

TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC TP. HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

KHOÁ LUẬN TỐT NGHIỆP

**TÌM HIỂU CÔNG NGHỆ VÀ ỨNG
DỤNG BLOCKCHAIN QUẢN LÝ XÁC
THỰC CHỨNG CHỈ SINH VIÊN**

GIẢNG VIÊN HƯỚNG DẪN ThS. LÝ ĐOÀN DUY KHÁNH
SINH VIÊN THỰC HIỆN:

PHẠM NGỌC PHÚ - 19DH110266
TRẦN THANH LONG - 19DH110248

TP. HỒ CHÍ MINH – THÁNG 6 - NĂM 2023

LỜI CẢM ƠN

Để hoàn thành khóa luận này, chúng em xin gửi lời cảm ơn chân thành đến:

Thầy hướng dẫn ThS. Lý Đoàn Duy Khánh, thầy đã đồng hành và hướng dẫn chúng em trong quá trình học tập cũng như trong việc hoàn thành luận văn.

Thầy, cô Khoa Công Nghệ Thông Tin và Trường Đại học TPHCM đã tận tình giảng dạy cho chúng em trong thời gian học tập.

Xin cảm ơn Ban Giám hiệu Trường Đại học Ngoại Ngữ Tin Học TPHCM 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 PM1902 VÀ PM1906 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 chúng em 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, để 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 để 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 đạt được, 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.

LỜI CAM ĐOAN

Chúng em là Phạm Ngọc Phú và Trần Thanh Long, là học viên ngành Công Nghệ Thông Tin, khóa 2019-2023. Chúng em xin cam đoan luận văn này là công trình nghiên cứu khoa học thực sự của bản thân chúng em và được sự hướng dẫn của ThS. Lý Đoàn Duy Khánh.

Các thông tin được sử dụng tham khảo trong đề tài luận văn được thu thập từ các nguồn đáng tin cậy, đã được kiểm chứng, được công bố rộng rãi và được chúng em trích dẫn nguồn gốc rõ ràng ở phần danh mục, tài liệu tham khảo. Các kết quả nghiên cứu được trình bày trong luận văn này là do chính chúng em thực hiện một cách nghiêm túc, trung thực và không trùng lặp với các đề tài khác đã được công bố trước đây.

Chúng em lấy danh dự và uy tín của bản thân để đảm bảo cho lời cam đoan này.

TPHCM, ngày ... tháng ... năm 2023

Tác giả 1

Tác giả 2

Trần Thanh Long

Phạm Ngọc Phú

MỤC LỤC

MỤC LỤC	i
MỤC LỤC BẢNG.....	iv
MỤC LỤC HÌNH VẼ.....	v
CHƯƠNG 1. MỞ ĐẦU	1
1.1 Giới thiệu	1
1.2 Lý do chọn đề tài.....	2
1.3 Mục tiêu nghiên cứu	3
1.4 Đối tượng và phạm vi nghiên cứu	3
1.5 Phương pháp nghiên cứu	3
1.6 Ý nghĩa của đề tài	4
CHƯƠNG 2. CƠ SỞ LÝ THUYẾT	5
2.1 Quản lý văn bằng chứng chỉ.....	5
2.1.1 Khái niệm	5
2.1.2 Cấp phát chứng chỉ	6
2.1.3 Xác minh chứng chỉ.....	7
2.2 Kỹ thuật mật mã.....	9
2.2.1 Khái niệm	9
2.2.2 Phân loại mật mã	9
2.2.3 Hàm băm.....	11
2.2.4 Chữ ký số	12
2.2.5 Nguyên lý ký số và xác thực chữ ký số.....	13
2.2.6 Chức năng của chữ ký số và tiêu chí an toàn thông tin	14
2.2.7 Chứng thư số.....	14
2.2.8 Chứng thư số dưới dạng PEM và JSON	15
2.2.9 Dịch vụ chứng thực số	17
2.2.10 Hạ tầng khóa công khai	17
2.3 Công nghệ Blockchain	18
2.3.1 Khái niệm	18
2.3.2 Phân loại Blockchain	18
2.3.3 Sổ cái phân tán	18
2.3.4 Bitcoin - Nền tảng Blockchain	19
2.3.5 Ethereum.....	21
2.3.6 Hyperledger Fabric	23
2.3.7 Merkle Tree	30
2.4 Công nghệ sử dụng.....	32
2.4.1 Hyperledger Fabric	32
2.4.2 NodeJS	32
2.4.3 Docker	34
2.4.4 NextJS	35
2.4.5 Mongoddb.....	36
2.4.6 Jenkins	37

CHƯƠNG 3. XÂY DỰNG ỨNG DỤNG VĂN BẰNG CHỨNG CHỈ TÍCH HỢP BLOCKCHAIN	38
3.1 Mô tả bài toán	38
3.2 Tổng quan giải pháp.....	39
3.3 Mối quan hệ trong quy trình xác minh VBCC.....	39
3.4 Quy trình cấp VBCC.....	40
3.5 Thuật toán xác minh VBCC.....	40
3.5.1 Đưa VBCC lên Blockchain	41
3.5.2 Tạo proof xác minh VBCC.....	41
3.5.3 Xác minh VBCC.....	42
3.6 Usecase.....	43
3.6.1 Tổng quát use case.....	43
3.6.2 Trường và sở giáo dục	44
3.6.3 Sinh viên	44
3.6.4 USE CASE 01. ĐĂNG NHẬP	47
3.6.5 USE CASE 02. Đăng Xuất	48
3.6.6 USE CASE 04. Xem trường	49
3.6.7 USE CASE 05. Đăng ký trường	50
3.6.8 USE CASE 06. Quản lý năm tốt nghiệp.....	52
3.6.9 USE CASE 11. Quản lý hồ sơ người nhận VBCC.....	53
3.6.10 USE CASE 12. Ban hành số hiệu.....	55
3.6.11 USE CASE 13. Ban hành số vào sổ	56
3.6.12 USE CASE 10. Quản lý năm tốt nghiệp.....	57
3.6.13 USE CASE 18. Quản lý loại VBCC.....	58
3.6.14 USE CASE 23. Quản lý khóa tốt nghiệp.....	60
3.6.15 USE CASE 28. Quản lý sinh viên	61
3.6.16 USE CASE 33. Quản lý VBCC.....	62
3.6.17 USE CASE 34. Cấp VBCC	63
3.6.18 USE CASE 36. Quản lý VBCC của riêng Sinh viên.....	65
3.6.19 USE CASE 37. Tùy chọn thông tin VBCC	66
3.6.20 USE CASE 39. Xác thực VBCC	67
3.7 Sequence Diagram.....	68
3.7.1 Đăng nhập.....	68
3.7.2 Đăng ký thông tin trường	69
3.7.3 Đăng ký sinh viên	69
3.7.4 Quản lý năm tốt nghiệp	70
3.7.5 Quản lý loại VBCC	72
3.7.6 Quản lý khóa tốt nghiệp	73
3.7.7 Quản lý hồ sơ người nhận.....	75
3.7.8 Ban hành số hiệu.....	76
3.7.9 Ban hành số vào sổ	76
3.7.10 Phát hành VBCC	77
3.7.11 Quản lý sinh viên	78

3.8 Tổng quan hệ thống	80
3.8.1 Kiến trúc tổng quan hệ thống	80
3.8.2 Cơ sở dữ liệu.....	81
3.8.3 Cân bằng tải server	82
3.8.4 Mạng Blockchain.....	83
3.8.5 Các thành phần của một chứng thư số trong hệ thống VBCC	83
3.8.6 PKI trong HyperLedge Fabric	84
3.8.7 Cơ sở dữ liệu & Blockchain	85
3.8.8 Mô tả Cơ sở dữ liệu	85
3.8.9 Thiết kế Blockchain.....	91
CHƯƠNG 4. KẾT QUẢ ĐẠT ĐƯỢC	93
4.1 Mạng Blockchain	93
4.2 Ứng dụng Web	93
4.2.1 Chức năng nhập excel cho tài khoản sinh viên, tài khoản trường, hồ sơ người nhận	94
4.2.2 Quản lý đơn vị đào tạo	94
4.2.3 Trường	102
4.2.4 Sinh viên	107
4.2.5 Chức năng tra cứu văn bằng/ chứng chỉ	110
CHƯƠNG 5. KẾT LUẬN	112
TÀI LIỆU THAM KHẢO.....	113

MỤC LỤC BẢNG

Bảng 2.1 So sánh số cái phân tán.....	18
Bảng 2.2 So sánh Hyperledger Fabric về một số nền tảng khác.....	30
Bảng 3.1 Các tác nhân.....	45
Bảng 3.2 Danh sách Usecase	45
Bảng 3.3 USE CASE 01. ĐĂNG NHẬP	47
Bảng 3.4 USE CASE 02. Đăng Xuất	48
Bảng 3.5 USE CASE 04. Xem trường	49
Bảng 3.6 USE CASE 05. Đăng ký trường	50
Bảng 3.7 USE CASE 06.Quản lý năm tốt nghiệp.....	52
Bảng 3.8 Quản lý hồ sơ người nhận VBCC.....	53
Bảng 3.9 USE CASE 12. Ban hành số hiệu.....	55
Bảng 3.10 USE CASE 13. Ban hành số vào sổ	56
Bảng 3.11 USE CASE 10. Quản lý năm tốt nghiệp.....	57
Bảng 3.12 USE CASE 18. Quản lý loại VBCC.....	58
Bảng 3.13 USE CASE 23. Quản lý khóa tốt nghiệp.....	60
Bảng 3.14 USE CASE 28. Quản lý Sinh viên	61
Bảng 3.15 USE CASE 33. Quản lý VBCC	62
Bảng 3.16 USE CASE 34. Cấp VBCC	63
Bảng 3.17 USE CASE 36. Quản lý VBCC của riêng Sinh viên.....	65
Bảng 3.18 USE CASE 37. Tùy chọn thông tin VBCC	66
Bảng 3.19 Cơ sở dữ liệu 01.Bảng User.....	85
Bảng 3.20 Cơ sở dữ liệu 02. Info User	86
Bảng 3.21 Cơ sở dữ liệu 03.Bảng Graduation Course.....	87
Bảng 3.22 Cơ sở dữ liệu 04.Bảng Graduation Year	87
Bảng 3.23 Cơ sở dữ liệu 05.Bảng Certificate Type	88
Bảng 3.24 Cơ sở dữ liệu 06.Bảng Level	88
Bảng 3.25 Cơ sở dữ liệu 07. Bảng Diploma And Certificate	89
Bảng 3.26 Danh sách đối tượng Blockchain.....	91
Bảng 3.27 Blockchain 01.Certificate	91
Bảng 3.28 Blockchain 02.Schema	92
Bảng 3.29 Blockchain 03.University	92

MỤC LỤC HÌNH VẼ

Hình 2.1 Quy trình xác minh chứng chỉ.....	8
Hình 2.2 Sơ đồ hệ mật mã Khóa đối xứng.....	10
Hình 2.3: Sơ đồ ký số và xác thực chữ ký số.....	13
Hình 2.4 Sơ đồ ký số và xác thực chữ ký số với hàm băm.....	13
Hình 2.5 Cấu trúc chứng thư số X.509 phiên bản 3.....	15
Hình 2.6 Khóa công khai RSA trong định dạng PEM	16
Hình 2.7 Chứng thư số dạng JSON.....	16
Hình 2.8: Mô tả cấu trúc một khối	20
Hình 2.9 Mô tả một giao dịch Blockchain	20
Hình 2.10 Mô tả cây mã hóa Merkle trong Bitcoin	21
Hình 2.11 Mô tả cách thực thi máy EVM.....	22
Hình 2.12 Mô tả cách thực thi máy EVM.....	22
Hình 2.13 Mô tả cách thực thi máy EVM.....	23
Hình 2.14 Dự án Hyperledger.....	24
Hình 2.15 Kiến trúc mạng Hyperledger Fabric	24
Hình 2.16 Docker container	27
Hình 2.17 Sơ đồ ứng dụng Blockchain Hyperledger Fabric.....	27
Hình 2.18 Merkle Tree	30
Hình 2.19 Tạo multiproof của A,C và xác minh dữ liệu A, C	31
Hình 2.20 Hyperledeger fabric.....	32
Hình 2.21 ExpressJS	33
Hình 2.22 Docker	34
Hình 2.23 So sánh giữa container và máy ảo	35
Hình 2.24 NextJS	35
Hình 2.25 MongoDB.....	36
Hình 2.26 Jenkins.....	37
Hình 3.1 Mối quan hệ trong quy trình xác minh VBCC.....	39
Hình 3.2 Quy trình cấp VBCC.....	40
Hình 3.3 Thuật toán xác minh VBCC	41
Hình 3.4 Tạo proof xác minh VBCC	41
Hình 3.5 Xác minh VBCC	42
Hình 3.6 Tổng quát usecase	43
Hình 3.7 Usecase Trường và Sở giáo dục	44
Hình 3.8 Usecase sinh viên	44
Hình 3.9 Usecase người xác thực	45
Hình 3.10 Sequence Diagram Đăng nhập	68
Hình 3.11 Sequence Diagram Đăng ký thông tin trường	69
Hình 3.12 Sequence Diagram Đăng ký sinh viên	69
Hình 3.13 Sequence Diagram Tạo năm tốt nghiệp	70
Hình 3.14 Sequence Diagram Sửa năm tốt nghiệp	71
Hình 3.15 Sequence Diagram Xóa năm tốt nghiệp	71
Hình 3.16 Sequence Diagram Tạo loại VBCC	72
Hình 3.17 Sequence Diagram Xóa loại VBCC	72
Hình 3.18 Sequence Diagram Sửa loại VBCC	73
Hình 3.19 Sequence Diagram Tạo khóa tốt nghiệp	73

Hình 3.20 Sequence Diagram Sửa khóa tốt nghiệp	74
Hình 3.21 Sequence Diagram Xóa khóa tốt nghiệp.....	74
Hình 3.22 Sequence Diagram Tạo danh sách hồ sơ người nhận	75
Hình 3.23 Sequence Diagram Sửa thông tin người nhận.....	75
Hình 3.24 Sequence Diagram Xóa hồ sơ người nhận.....	76
Hình 3.25 Sequence Diagram Ban hành số hiệu.....	76
Hình 3.26 Ban hành số vào sổ.....	77
Hình 3.27 Phát hành VBCC	77
Hình 3.28 Sửa thông tin sinh viên.....	78
Hình 3.29 Sequence Diagram Chia sẻ thông tin VBCC	79
Hình 3.30 Sequence Diagram Xác minh VBCC.....	79
Hình 3.31 Tổng quan hệ thống.....	80
Hình 3.32 Cache trong cơ sở dữ liệu	81
Hình 3.33 Cân bằng tải server.....	82
Hình 3.34 Kiến trúc thử nghiệm được cài đặt trong môi trường hệ thống VBCC	83
Hình 3.35 Các thành phần một chứng thư số (JSON)	83
Hình 3.36 Lược đồ CSDL	85
Hình 4.1 Giao diện trang chủ	93
Hình 4.2 Nhập dữ liệu từ excel	94
Hình 4.3 Màn hình quản lý tài khoản theo trường / sinh viên	95
Hình 4.4 Màn hình quản lý tài khoản trường.....	95
Hình 4.5 Màn hình tạo/sửa trường	96
Hình 4.6 Màn hình quản lý tài khoản sinh viên	96
Hình 4.7 Màn hình quản lý tạo / chỉnh sửa tài khoản sinh viên	97
Hình 4.8 Màn hình chọn trường đại học	97
Hình 4.9 Màn hình hồ sơ người nhận của một trường đại học	98
Hình 4.10 Màn hình tạo/chỉnh sửa hồ sơ người nhận	98
Hình 4.11 Màn hình nhập số hiệu	99
Hình 4.12 Màn hình quản lý loại bằng.....	99
Hình 4.13 Màn hình tạo / chỉnh sửa loại bằng	100
Hình 4.14 Màn hình quản lý năm tốt nghiệp	100
Hình 4.15 Màn hình tạo năm tốt nghiệp	101
Hình 4.16 Màn hình quản lý văn bằng chứng chỉ	101
Hình 4.17 Màn hình văn bằng chứng chỉ của một trường	102
Hình 4.18 Màn hình quản lý tài khoản sinh viên	102
Hình 4.19 Màn hình tạo/ chỉnh sửa tài khoản sinh viên	103
Hình 4.20 Màn hình quản lý hồ sơ người nhận	104
Hình 4.21 Màn hình tạo/chỉnh sửa hồ sơ người nhậnMàn hình cấp số vào sổ	104
Hình 4.22 Màn hình cấp số vào sổ.....	105
Hình 4.23 Màn hình cấp văn bằng / chứng chỉ	105
Hình 4.24 Màn hình quản lý khóa tốt nghiệp	106
Hình 4.25 Màn hình tạo / chỉnh sửa khóa tốt nghiệp	106
Hình 4.26 Màn hình quản lý văn bằng chứng chỉ đã cấp.....	107
Hình 4.27 Màn hình danh sách văn bằng.....	107
Hình 4.28 Màn hình chi tiết văn bằng.....	108
Hình 4.29 Màn hình chọn thông tin chia sẻ văn bằng	108
Hình 4.30 Màn hình chia sẻ văn bằng thông qua file PDF, đường dẫn hoặc mã QR	109

Hình 4.31 Màn hình sau khi xác thực thành công thông qua mã QR đường dẫn hoặc mã QR trên file PDF	109
Hình 4.32 Màn hình sau khi xác thực thất bại thông qua mã QR đường dẫn hoặc mã QR trên file PDF	110
Hình 4.33 Màn hình nhập thông tin tra cứu	110
Hình 4.34 Màn hình tra cứu thành công	111

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
HF	Hyperledger Fabric

CHƯƠNG 1. MỞ ĐẦU

1.1 Giới thiệu

Đề tài nghiên cứu trong việc xây dựng hệ thống quản lý và xác thực 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.

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. Các giải pháp hiện nay như là 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 [2] 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.

Công nghệ Blockchain có tiềm năng lớn trong việc quản lý và xác thực thông tin văn bằng, chứng chỉ. Áp dụng Blockchain trong lĩnh vực giáo dục có thể cải thiện tính tin cậy, minh bạch và hiệu quả của quá trình quản lý. Tuy nhiên, việc triển khai thực tế cần được đánh giá kỹ lưỡng để đảm bảo sự thành công và chấp nhận từ các bên liên quan.

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 tồn 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.

Số gốc cấp VBCC theo quy định tại Điều 19 thông tư số 21/2019/TT-BGDĐT [4] 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. Số 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 số gốc còn làm thủ công trong những trường hợp như sau:

- Nhân viên phát VBCC cho người nhận chứng chỉ đến trực tiếp và có giấy tờ khớp thông tin với số gốc thì nhân viên phát cho người đó và cập nhật số

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.

- 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:

- 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.
- Xây dựng hệ thống website tương tác với người sử dụng, giao diện trực quan và phản hồi nhanh.
- 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 trình quản lý VBCC theo định pháp luật Phạm vi nghiên cứu:
- Quy trình cấp phát chứng chỉ của Trường Đại học Ngoại Ngữ Tin Học TPHCM

• Xây dựng hệ thống quản lý xác thực VBCC ứng dụng công nghệ Blockchain
Phạm vi nghiên cứu :

- Đơn vị cấp VBCC
- Người xác minh VBCC
- Sinh viên

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 khôi.

- 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 khôi. Ngoài việc triển khai với bài toán cụ thể tại Trường Đại học Ngoại Ngữ Tin Học TPHCM 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 khôi 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 khôi có thể mở rộng ứng dụng trong nhiều lĩnh vực như nông nghiệp, y tế, ngân hàng, vận tải.

CHƯƠNG 2. CƠ SỞ LÝ THUYẾT

2.1 Quản lý văn bằng chứng chỉ

2.1.1 Khái niệm

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 đat. 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.” [3]

Điều 3 Thông tư 21/2019/TT-BGDDĐT 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.[4]

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.[5]

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.[6]

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.

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 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 là triển khai các ban hành, phổ biến thông tin, tiếp nhận yêu cầu, thực hiện và lưu giữ hồ sơ được quy định. 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 [7]. 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.

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. Nhân viên dựa vào hệ thống quản lý và sổ gốc cấp chứng chỉ để kiểm tra thông tin chứng chỉ. 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. Nhân viên phát chứng chỉ cho người nhận. 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:

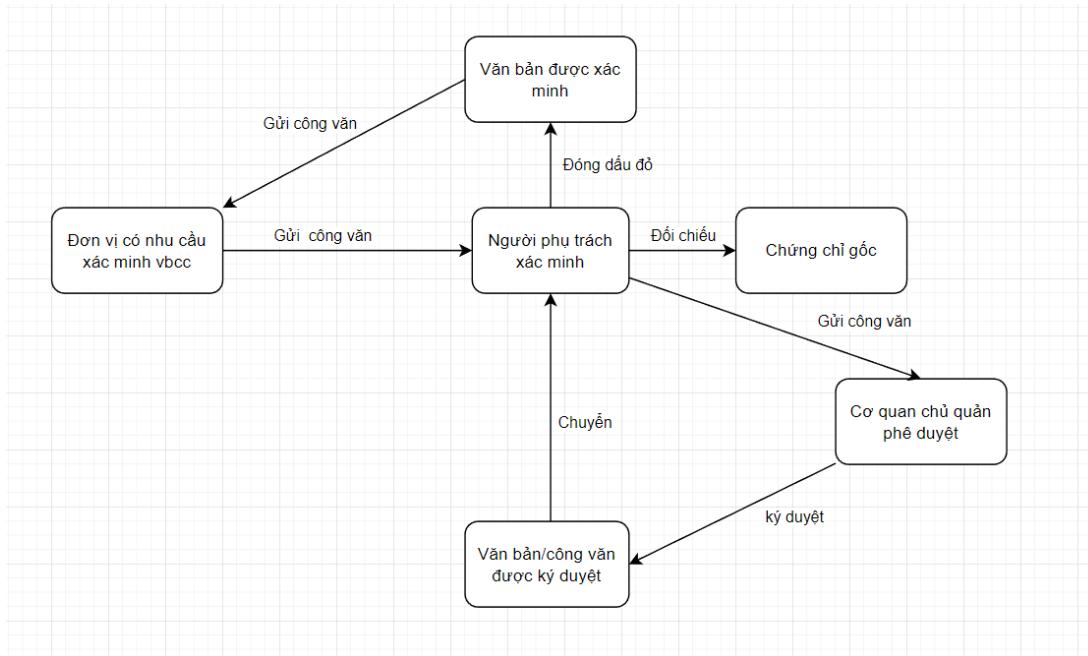
Bước 1. Đơn vị có nhu cầu xác minh các VBCC cần gửi công văn đến cơ sở đào tạo. Đơn vị có thể cử người có giấy giới thiệu đến trực tiếp phòng ban để bắt đầu làm thủ tục xác minh. Trong quá trình gửi công văn, đơn vị phải chịu trách nhiệm với hồ sơ được bàn giao.

Bước 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.

Bước 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.

Bước 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.

Bước 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).



Hình 2.1 Quy trình xác minh chứng chỉ

Có 3 cách xác minh:

- Việc xác minh chứng chỉ dựa trên các tính năng bảo mật được xây dựng trong chính chứng chỉ: có thể bao gồm các biện pháp như kiểm tra xác thực của ký hiệu, giấy chuyên dụng, chữ ký,...
- Xác minh dựa trên đơn vị phát hành: Bên thứ ba gửi yêu cầu kiểm tra tới đơn vị phát hành chứng chỉ để xác nhận việc phát hành chứng chỉ. Đơn vị phát hành sẽ kiểm tra trong cơ sở dữ liệu hoặc kiểm tra chức năng bảo mật của chứng chỉ.
- Xác minh dựa trên cơ sở dữ liệu tập trung: Bên thứ ba truy vấn cơ sở dữ liệu tập trung của nhà phát hành để kiểm tra thông tin về chứng chỉ đã phát hành và so sánh với chứng chỉ hiện tại. 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, đổi 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

Phản 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 Khái niệm

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).[8]

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 Phân loại mật mã

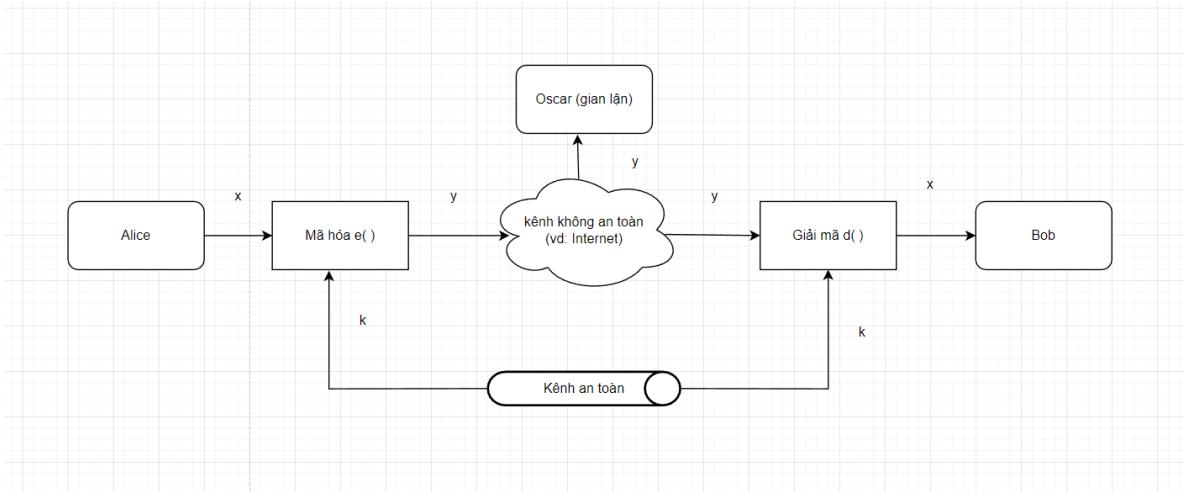
Có thể phân loại mật mã theo đặc điểm phụ thuộc vào loại khóa:

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

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

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

Cryptosystems).



Hình 2.2 Sơ đồ hệ mật mã Khóa đối xứng

Sơ đồ 2.2 minh họa một ứng dụng mật mã Khóa đối xứng trong thực tế [9]. 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 nén liên lạc được, chỉ Oscar thiếu duy nhất khóa để giải mật nén không thể hiểu thông tin.

Các ký hiệu trong sơ đồ 2.2:

- x là bản rõ: bản tin được sinh ra bởi bên gửi
- y là bản mật: bản tin che giấu thông tin của bản rõ, được gửi tới bên nhận qua một kênh không bí mật
- k là khóa: Nó là giá trị ngẫu nhiên và bí mật được chia sẻ giữa các bên trao đổi thông tin và được tạo ra từ:
 - Bên thứ 3 được tin cậy tạo và phân phối tới bên gửi và bên nhận
 - Hoặc, bên gửi tạo ra và chuyển cho bên nhận

Mật mã Khóa bắt đôi 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 [9].

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.

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

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

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

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

2.2.4 Chữ ký số

Chữ ký số là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng 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. Chữ ký số cung cấp một cách để xác thực tính đúng đắn của một tài liệu hoặc giao dịch, bằng cách cho phép người nhận xác minh rằng nó đã được ký bởi người gửi và rằng nó không đã bị sửa đổi sau khi được ký. Chữ ký số cũng được sử dụng rộng rãi trong các giao dịch điện tử và giao dịch tiền điện tử.

Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa. Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

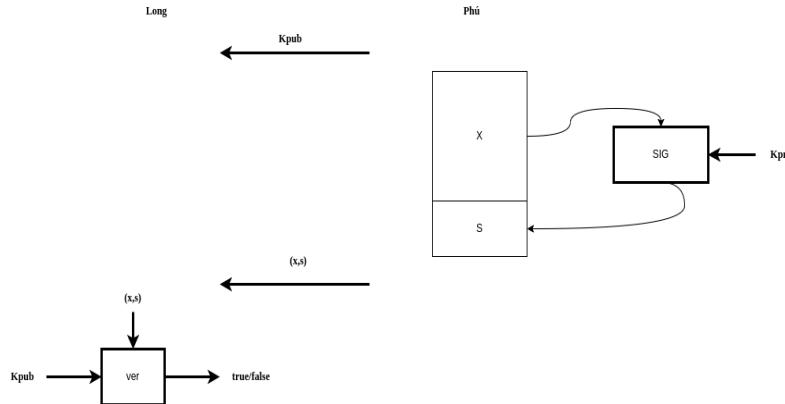
Chữ ký số xử lý vấn đề xác thực và chống chối bỏ trong mật mã học. Nói cách khác, để đảm bảo cho một người/thiết bị đã gửi một bản tin, nó cần được ký điện tử cũng giống như những bức thư tay được niêm phong và được ký bằng tay bởi chính người gửi. Chữ ký số là một phương pháp ký dữ liệu điện tử, nó đảm bảo tính định danh hơn so với chữ ký trên thư viết tay. Nó xác thực bản tin được gửi đi, đảm bảo rằng người gửi không thể chối bỏ được hành vi gửi đi của mình và danh tính của người gửi.

Trong thuật toán chữ ký số, có hai loại: một loại sử dụng nội dung của tin nhắn làm đầu vào cho thuật toán xác minh, một loại khác sẽ sử dụng chữ ký của tin nhắn để khôi phục lại nội dung tin nhắn. Loại đầu tiên được sử dụng rộng rãi hơn và dựa trên thuật toán băm để tránh các tấn công giả mạo. Loại thứ hai không cần thông tin về nội dung tin nhắn để xác minh, nên phù hợp hơn khi gửi nội dung tin nhắn ngắn.

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.

2.2.5 Nguyên lý ký số và xác thực chữ ký số

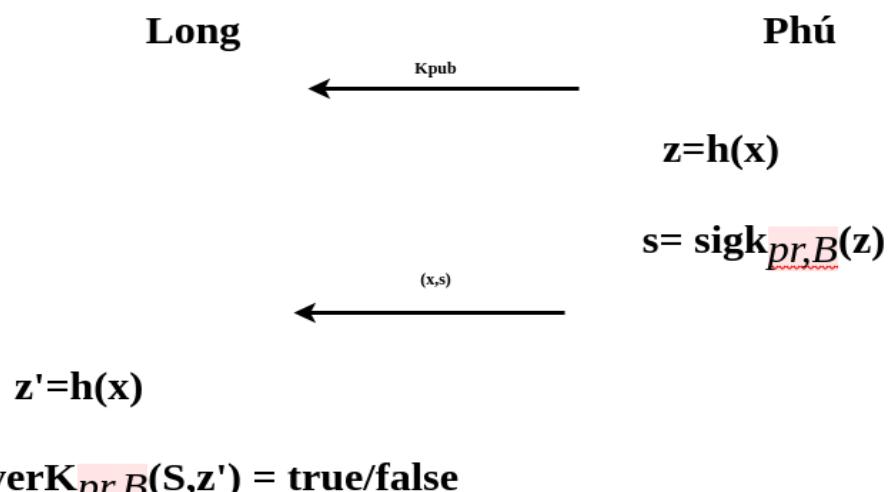


Hình 2.3: Sơ đồ ký số và xác thực chữ ký số

Sơ đồ nguyên lý ký số và xác thực chữ ký số [9] được mô tả ở hình 2.3. Quy trình bắt đầu khi Phú ký thông điệp x . Thuật toán ký số (sig) có tham số thứ nhất là khóa bí mật của Phú, k_{pr} . Khóa bí mật được Phú 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 bắn chữ ký s sẽ thêm vào thông điệp x tạo một cặp (x,s) gửi cho Long.

Tiếp theo Long 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 Phú. Nếu x do Phú 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 2.4 Sơ đồ ký số và xác thực chữ ký số với hàm băm

Sơ đồ 2.4 mô tả nguyên lý ký số và xác thực chữ ký số với hàm băm [9]. Phú 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, Long sẽ tính giá trị băm z' của thông điệp x : $z' = h(x)$. Long sẽ

xác thực chữ ký s với khóa công khai Kpub,B và z'.

2.2.6 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:

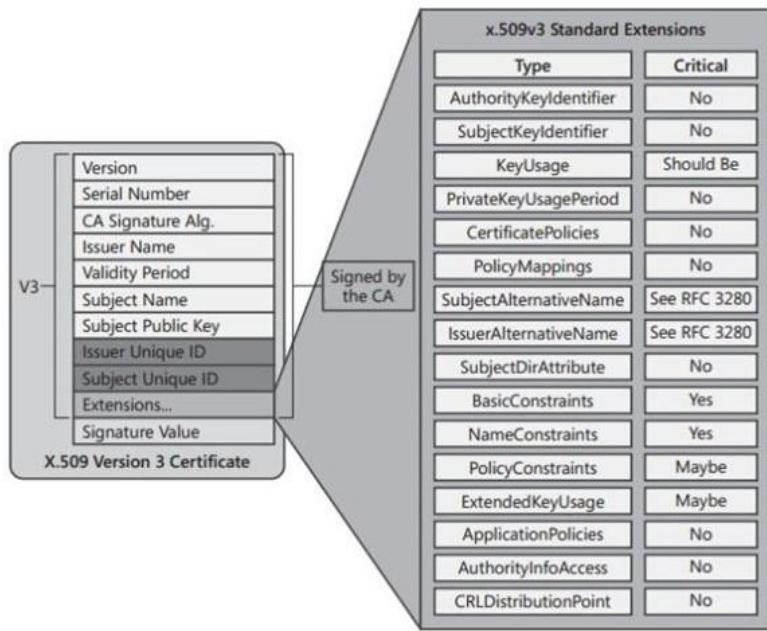
- Tính toàn vẹn thông tin: khi có sự thay đổi bất kỳ lên thông điệp thì giá trị hàm băm sẽ bị thay đổi; nghĩa là thông điệp không toàn vẹn.
- Tính không chối bỏ hay chống thoái thác trách nhiệm: vì chỉ có chủ thông điệp mới có khóa bí mật để ký lên thông điệp nên người ký không thể chối bỏ thông điệp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

2.2.7 Chứng thư số

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

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

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



Hình 2.5 Cấu trúc chứng thư số X.509 phiên bản 3

(*Nguồn: Các phiên bản của chứng chỉ số X.509. <https://cer.vn/news/kien-thuc/cac-phien-ban-cua-chung-chi-so-x-509/>*)

2.2.8 Chứng thư số dưới dạng PEM và JSON

Chứng thư số dạng PEM (Privacy Enhanced Mail) là một định dạng chuẩn để lưu trữ và truyền tải các chứng thư số trong môi trường công cộng. PEM được sử dụng rộng rãi trong các ứng dụng bảo mật như mạng riêng ảo (VPN), giao thức truyền tải lớp bảo mật (TLS/SSL), chứng thực người dùng và mã hóa email.

Định dạng PEM sử dụng cú pháp văn bản ASCII để lưu trữ khóa công khai, khóa riêng tư và chứng chỉ trong các tệp tin PEM. PEM thường chứa các thành phần sau:

1. Header: Bắt đầu bằng chuỗi "-----BEGIN" và mô tả loại đối tượng được lưu trữ trong PEM file (ví dụ: RSA Private Key, X.509 Certificate).
2. Dữ liệu: Dữ liệu thực tế của đối tượng, có thể là khóa công khai, khóa riêng tư hoặc chứng chỉ.
3. Footer: Kết thúc bằng chuỗi "-----END" theo cùng loại với header.

Ví dụ, một khóa công khai RSA trong định dạng PEM có thể trông như sau:

```

-----BEGIN PUBLIC KEY-----
MIIBIjANBqkqhkiG9w0BAQEAAQ8AMIIIBCgKCAQEAmXSR4krXgbKByZU0axMP
f0POMrGVRpXzx17GgQX5ysnRVoShbIxI9atJS1L7WTWZhu7Scbc/V3q7WSH6ZG4
2lgBwkY8ZDn+8/dTxp8tiXI+bNv1bj/BmESe+Ep3ctGUcfnDQq92VyEzSy6uoN10
2UJUw/v1uGYIDmtvcSeszPpF5nFZ8uAcygRN54x/pPz4orZNIu+ge9RYf0bVXHW
U6ZfUJ2Wx6IWuYXWbxSx7DtNdkkdN2FZ2zCXgD8rkLZZQV/u0uqxLTrah56eQgVN
akLuX+Pq+dm0vukq+oo2tuPlqIpFBaifygThbkk/EksZLZV4SOR/3W+39tB3e5CG
oQIDAQAB
-----END PUBLIC KEY-----

```

Hình 2.6 Khóa công khai RSA trong định dạng PEM

Chứng thư số dạng PEM cung cấp tính tương thích và dễ đọc với các hệ thống và công cụ hỗ trợ. Để sử dụng chứng thư số PEM trong các ứng dụng, chúng ta thường phải đọc và phân tích cú pháp PEM để trích xuất thông tin cần thiết, chẳng hạn như khóa công khai hoặc khóa riêng tư.

Chứng thư số dạng JSON là một loại chứng thư số (digital certificate) được lưu trữ dưới dạng đối tượng JSON (JavaScript Object Notation). JSON là một định dạng dữ liệu phổ biến được sử dụng để truyền tải dữ liệu giữa các ứng dụng web và máy chủ.

Ví dụ, một khóa công khai RSA trong định dạng JSON có thể trông như sau:

```

{
  "type": "certificate",
  "subject": {
    "commonName": "example.com",
    "organization": "Example Organization",
    "country": "US"
    // Thêm thông tin khác về người nhận chứng chỉ (subject)
  },
  "issuer": {
    "commonName": "Certificate Authority",
    "organization": "Example CA",
    "country": "US"
    // Thêm thông tin khác về cơ quan phát hành chứng chỉ (issuer)
  },
  "validFrom": "2022-01-01",
  "validTo": "2023-01-01",
  "fingerprint": "AB:CD:EF:...",
  "publicKey": {
    "algorithm": "RSA",
    "key": "-----BEGIN PUBLIC KEY-----\n..."
    // Thêm thông tin khác về khóa công khai
  },
  // Thêm thông tin khác về chứng chỉ, chẳng hạn như extensions, signature, v.v.
}

```

Hình 2.7 Chứng thư số dạng JSON

- "type": Loại chứng thư số, trong ví dụ này là "certificate" để chỉ rằng đây là một chứng thư số.
- "subject": Đối tượng chứng thư số, chứa thông tin về người nhận chứng chỉ (subject). Trong ví dụ, có các trường thông tin như "commonName" (tên thông thường), "organization" (tổ chức), "country" (quốc gia).

- "issuer": Đối tượng phát hành chứng thư số, chứa thông tin về cơ quan phát hành chứng chỉ (issuer). Ví dụ này bao gồm các trường thông tin tương tự như "subject".
- "validFrom" và "validTo": Thời gian bắt đầu và kết thúc của chứng thư số, chỉ ra khoảng thời gian mà chứng thư số được coi là hợp lệ.
- "fingerprint": Dấu vân tay của chứng thư số, một giá trị duy nhất được tạo ra từ chứng thư số để xác định tính toàn vẹn của nó.
- "publicKey": Thông tin về khóa công khai trong chứng thư số, bao gồm thuật toán mã hóa (algorithm) và chuỗi khóa công khai (key).

Lưu ý rằng cấu trúc JSON có thể khác nhau tùy thuộc vào mục đích và nhu cầu của ứng dụng. Bạn có thể tùy chỉnh cấu trúc JSON theo yêu cầu của mình.

2.2.9 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 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.

2.2.10 Hạ tầng khóa công khai

Hạ tầng khóa công khai (Public Key Infrastructure) là cơ chế cho 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. Là hệ thống vừa mang tính tiêu chuẩn, vừa mang tính công nghệ cho phép người dùng trong một mạng công cộng không bảo mật (như Internet), có thể trao đổi thông tin một cách an toàn thông qua việc sử dụng một cặp khóa bí mật và công khai được chứng nhận bởi một nhà cung cấp chứng nhận số CA (Certificate Authority) được tín nhiệm. Nền tảng khóa công khai cung cấp một chứng chỉ số, dùng để xác minh một cá nhân hoặc một tổ chức, và các dịch vụ danh mục có thể lưu trữ và khi cần có thể thu hồi các chứng chỉ số.

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 Khái niệm

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.

2.3.2 Phân loại Blockchain

Mạng Blockchain có thể được phân loại thành: Blockchain công khai, Blockchain riêng tư [8] và Blockchain phân quyền. 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,..., việc tham gia mạng Blockchain được kiểm soát chặt chẽ, xác định rõ danh tính của thành viên. Loại thứ 3 Cũng là 1 dạng private nhưng người dùng được cung cấp 1 số tính năng đặc quyền khác tùy thuộc bên thứ 3 cung cấp.

Nghiên cứu và so sánh mạng Blockchain dựa trên 4 khái niệm chính của Blockchain: sổ cái phân tán, cơ chế đồng thuận, bảo mật, smart contract

2.3.3 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, có các 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

2.3.4 Bitcoin - Nền tảng Blockchain

Công nghệ Blockchain bắt nguồn từ tài liệu của Nakamoto năm 2009 – tài liệu chỉ ra đồng tiền kỹ thuật số Bitcoin được xây dựng như thế nào. Bitcoin giải quyết một vấn đề rất quan trọng trong lĩnh vực tiền điện tử được gọi là double-spending. Ví dụ sử dụng cùng một đồng điện tử thanh toán cho 12 người khác. Thông thường điều này được xử lý thông qua một cơ quan kiểm soát ví dụ như ngân hàng hoặc bên thứ ba được tin tưởng nhưng Nakamoto

Đưa ra một máy chủ dấu thời gian (time-stamp server) đảm bảo tất cả giao dịch xuất hiện theo thứ tự thời gian trong cơ sở dữ liệu. Tác giả đã đưa ra thuật toán Proof-of-Work để thiết lập sự đồng thuận để biết được chuỗi nào là chuỗi đúng. Thuật toán cũng thúc đẩy động lực cho người giao dịch đúng thông qua phần thưởng. Về bản chất, nó làm cho một giao dịch giả có chi phí tốn kém hơn rất nhiều so với việc xác nhận một giao dịch đúng. Nếu không có thuật toán đồng thuận thì sẽ mất đi sự tin tưởng vào hệ thống Blockchain của Bitcoin vì khi đó ai cũng có quyền truy cập vào lịch sử các giao dịch (tất cả các node) và có thể viết lại lịch sử sau đó công bố nó như một chuỗi đúng.

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

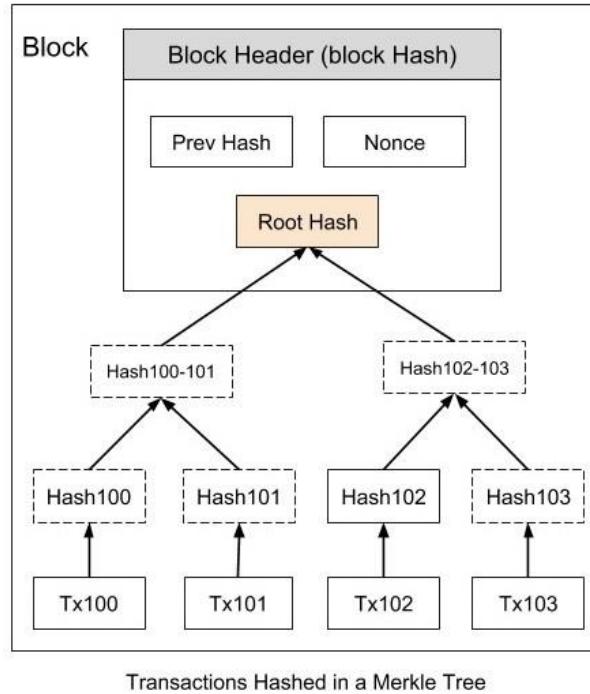
Một dữ liệu giao dịch gồm có nhiều giao dịch thành phần được ký số bởi các bên tham gia như hình 2.9

Dữ liệu A, B, C, D, E được tính giá trị băm, sau đó gộp 2 giá trị băm của dữ liệu 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 2.10

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

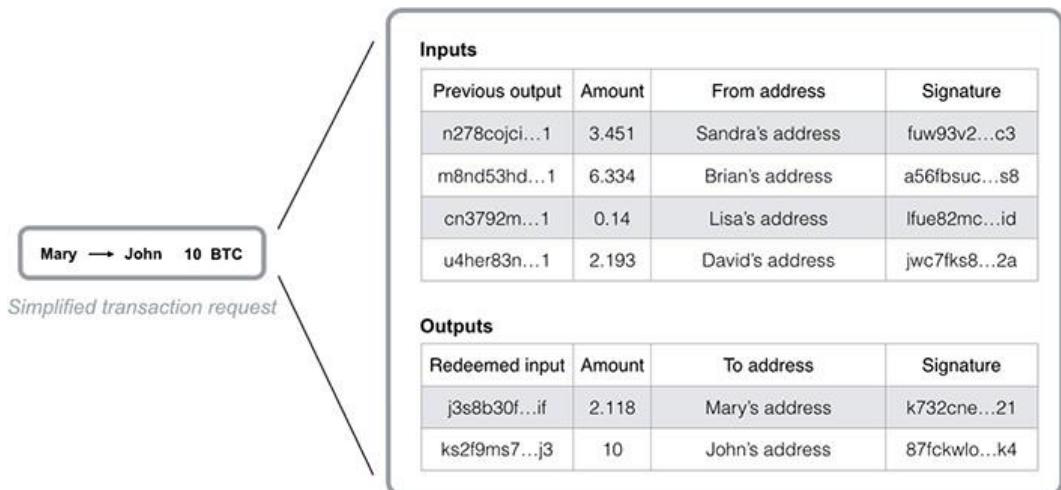
- Giao dịch thuộc về khối đầu tiên của Blockchain sẽ được xác định sẵn trong mã nguồn của Blockchain tại khối đầu tiên của Blockchain. Các loại tiền số có quy định số lượng tiền giới hạn trong hệ thống.
- Giao dịch thường cho những người tạo ra khối mới: hệ thống Blockchain tự tạo tự động và sẽ chuyển tiền thưởng cho người tạo ra khối mới.

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

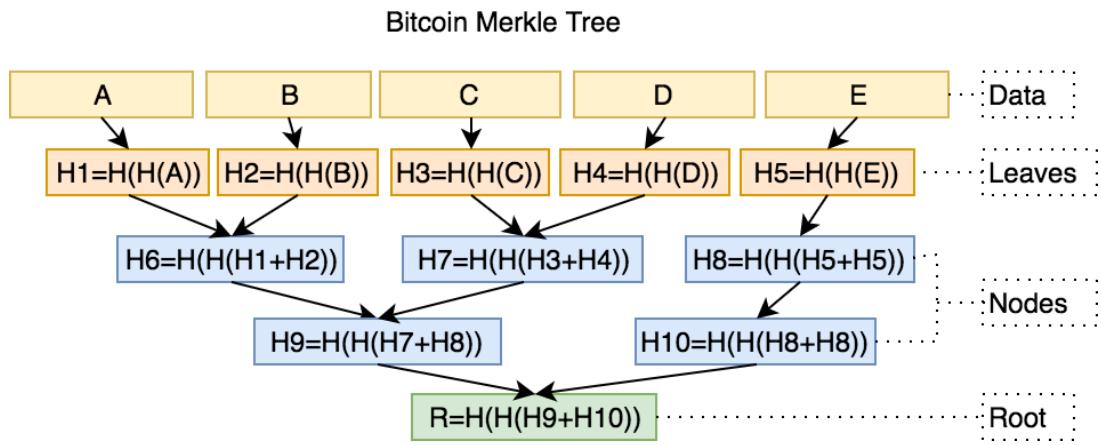


Hình 2.8: Mô tả cấu trúc môt khôi

(Nguồn: *merkletreejs npm*. <https://www.npmjs.com/package/merkletreejs?activeTab=readme>)



Hình 2.9 Mô tả một giao dịch Blockchain



Hình 2.10 Mô tả cây mã hóa Merkle trong Bitcoin

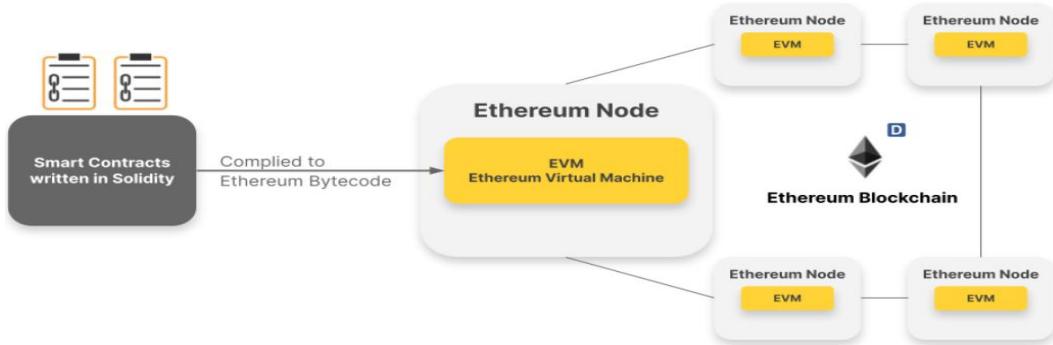
(*Nguồn: merkletreejs npm. <https://www.npmjs.com/package/merkletreejs?activeTab=readme>*)

2.3.5 Ethereum

Ethereum là mạng Blockchain của ứng dụng đồng coin ETH (Chú ý về sự khác biệt về đồng coin và token). 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. Là một nền tảng thực thi smart contract một hệ thống thực hiện những hợp đồng có sẵn một cách tự động mà không cần phải thông qua một trung gian.

Cơ chế đồng thuận của ethereum hiện tại là Proof of Stake Để thực thi smart contract thì phải cần đến EVM(Ethereum Virtual Machine). EVM (Ethereum Virtual Machine) là máy ảo Ethereum. Ví dụ: Giống như việc Software Developers phải dùng các IDE (Integrated Development Environment - Môi trường tích hợp như là Microsoft Visual Studio hoặc Xcode dùng để viết code và đóng gói ứng dụng. Sau đó, các IDE này sẽ dịch code sang ngôn ngữ mà máy tính có thể hiểu được.

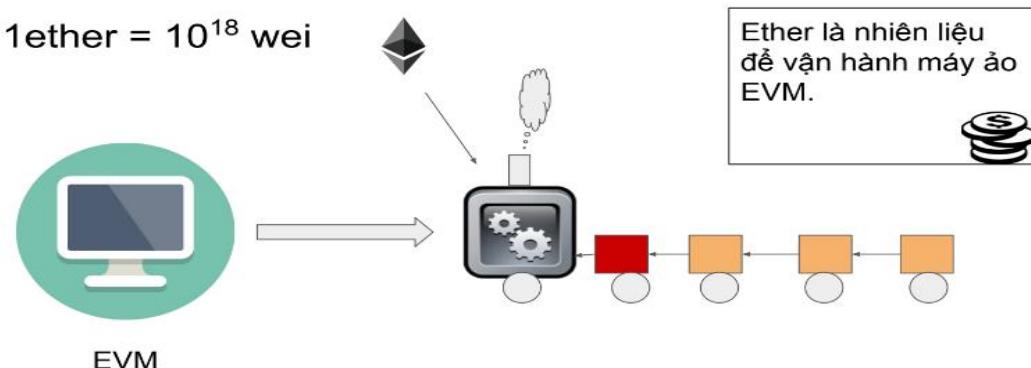
➔ Có thể hiểu đơn giản và dựa vào hình 2.11 là các EVM sẽ đóng vai trò trung gian trong việc thực thi các smart contract (hợp đồng thông minh) ở trên mạng lưới Ethereum. Mỗi một Ethereum node được trang bị một EVM riêng, điều này sẽ đảm bảo tính bảo mật và phi tập trung của mạng lưới.



Hình 2.11 Mô tả cách thực thi máy EVM

(*Nguồn: EVM [Etherum Virtual Machine] <https://haimanh.vn/evm--ethereum-virtual-machine--la-gi--tim-hieu-crypto-2022-380-newsdt.aspx>*)

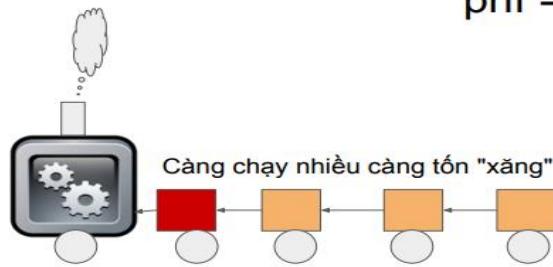
Để vận hành được cỗ máy này chúng ta phải cần nguyên liệu đó chính là ether đơn vị nhỏ nhất của 1 ether = 10^{18} wei. Máy đào sẽ thực hiện cơ chế proof of stake để đào ra ether và sản xuất là không giới hạn so với bitcoin vì bitcoin có giới hạn để tăng độ khan hiếm đẩy giá coin lên nhưng ethereum với sứ mệnh là phát triển mạng Blockchain nên các ether được đào không giới hạn.



Hình 2.12 Mô tả cách thực thi máy EVM

Để tính toán được nguyên liệu cho động cơ thì ethereum có sinh ra cái gọi là gas. Dựa vào hình 2.11 ta có thể thấy gas là chi phí phải trả cho EVM khi hoạt động bất kì trên Blockchain. Gas price là số ether phải trả cho 1 gas và số giá gas tùy thuộc về độ thanh khoản trên thị trường tác động đến và các vấn đề khác ví dụ: Như chúng ta chạy xe thì phải cần có xăng, xăng thì giá biến động dữ dội. Phí vận hành = gas cần phải trả * giá gas

$$\text{phí} = \text{gas} \times \text{gas price}$$



- **gas là chi phí phải trả cho EVM khi làm một điều gì đó.**
- **gas price là số ether phải trả cho 1 gas.**

Hình 2.13 Mô tả cách thực thi máy EVM

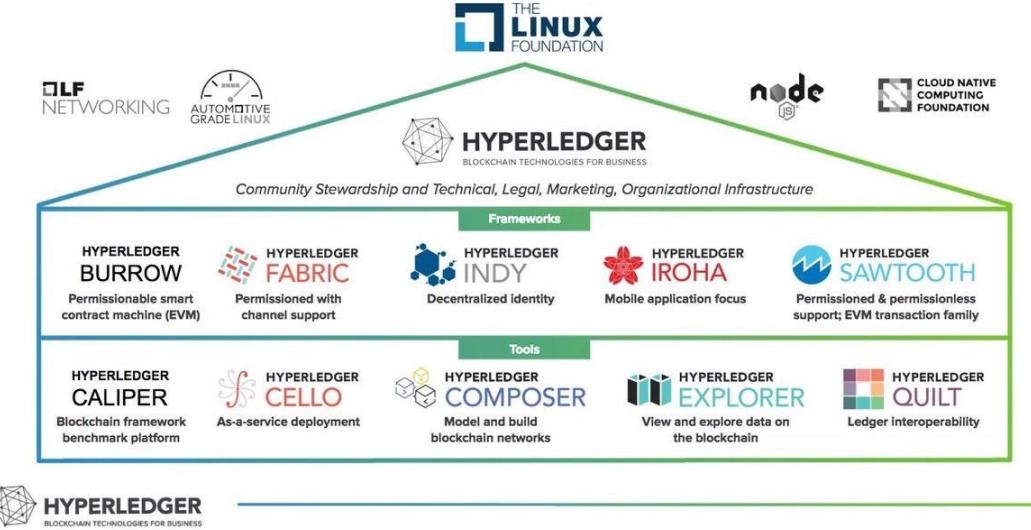
Để lưu trữ dữ liệu Ethereum sử dụng cấu trúc dữ liệu cây trie. Ethereum Patricia tree (còn được gọi là Trie) là một cấu trúc dữ liệu được sử dụng trong Blockchain Ethereum để lưu trữ và truy xuất dữ liệu trong khối lưu trữ. Nó cho phép truy xuất dữ liệu một cách hiệu quả và nhanh chóng bằng cách sử dụng cấu trúc cây Merkle.

Cây Patricia được tạo ra từ cấu trúc cây Merkle, nó sẽ tạo ra một hash giống như Merkle Tree nhưng sẽ giảm số lượng các hash cần để lưu trữ. Nó sẽ lưu trữ các hash của giá trị tại các node chứ không lưu trữ giá trị trực tiếp. Điều này giúp giảm đáng kể dung lượng lưu trữ cần thiết cho khối lưu trữ và tăng tốc độ truy xuất dữ liệu. Nó cũng được sử dụng để lưu trữ các smart contract trong Ethereum và các thông tin về tài sản giao dịch trong Ethereum.

2.3.6 Hyperledger Fabric

Hyperledger Fabric (HF) [10] 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 Buror. Hình 2.16 mô tả các thành phần của dự án Hyperledger.

HF là phần mềm mã nguồn mở. Công ty IBM đã 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 hóa cho nhiều ứng dụng. Các ứng dụng phổ biến như : tài chính, y tế, giáo dục, chuỗi cung ứng, ...



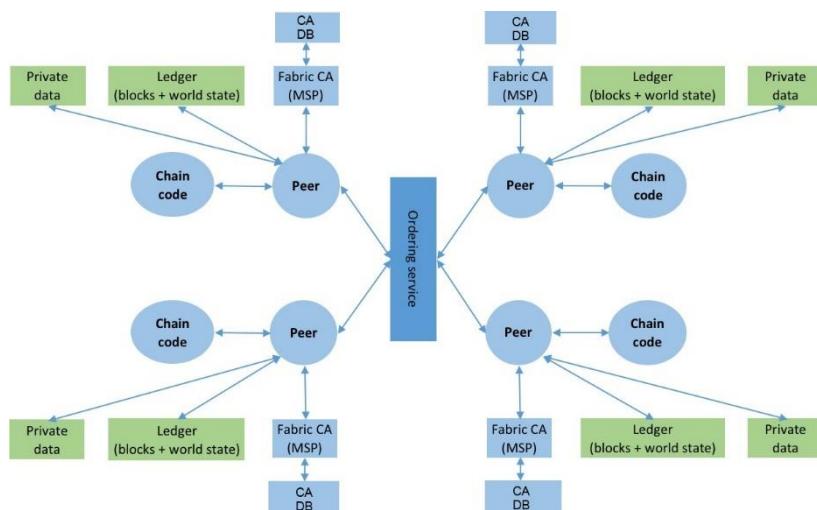
Hình 2.14 Dự án Hyperledger

(*Nguồn: Comprehensive Blockchain Hyperledger Developer Guide from Beginner to Advance Level*
<https://gbaglobal.org/blog/2019/07/03/comprehensive-blockchain-hyperledger-developer-guide-from-beginner-to-advance-level/>)

2.3.6.1 Kiến trúc của Hyperledger Fabric

Kiến trúc HF có các kênh bảo mật riêng kết nối trong mạng Blockchain, giúp các số 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 2.17



Hình 2.15 Kiến trúc mạng Hyperledger Fabric

(*Nguồn: Hyperledger Fabric architecture* <https://subscription.packtpub.com/book/web-development/9781838649982/11/ch11lvl1sec76/hyperledger-fabric-architecture>)

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 hiện nay 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 số 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 sẻ 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 khói bất động bộ, phân trang chaincode,....

HF gồm các thành phần trong hình 2.15 được mô tả như sau:

- Ledger: Quyền sở cái kỹ thuật số bao gồm 2 thành phần có liên quan nhau là “chuỗi khói” và “cơ sở dữ liệu trạng thái”. Khi các giao dịch làm thay đổi các tài sản trong mạng Blockchain, dữ liệu sẽ được ghi nhận tất cả lên “chuỗi khói” 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 sở cái được lưu trên các nút Peer trong cùng kênh, đồng thời sở 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

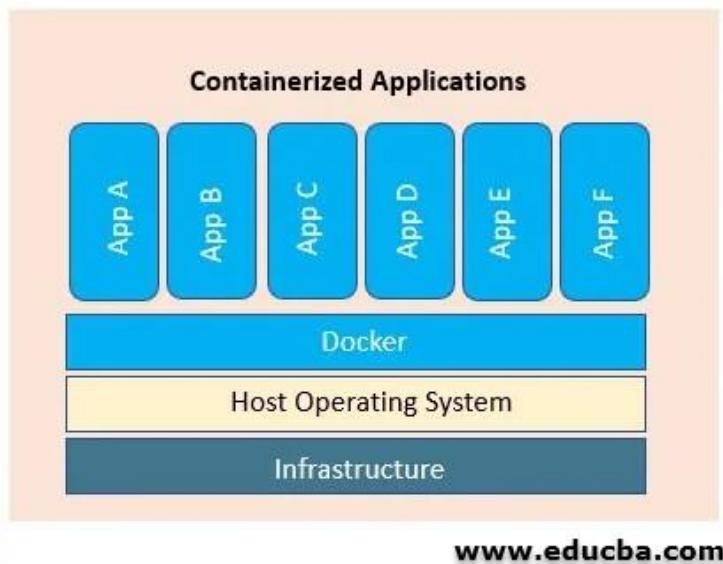
Sở cái và thực thi Hợp đồng thông minh. Các nút peer được quản lý và duy trì bởi các dịch vụ thành viên trong mạng. Nút Peer được chia làm hai dạng:

- 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 sở 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.

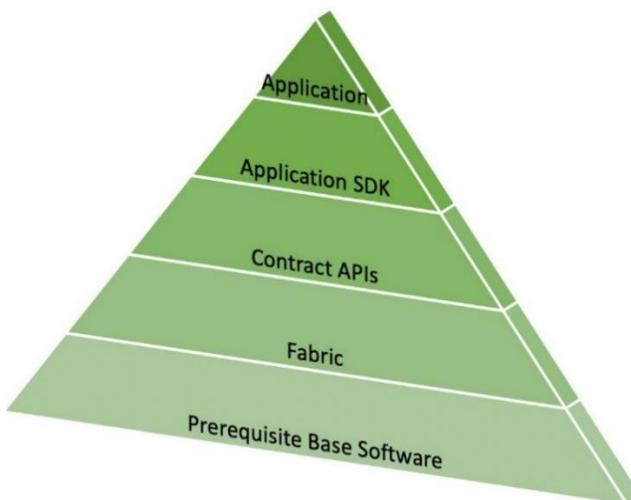
Docker Engine tạo các container hoạt động từ các file cấu hình Dockerfile. Một máy vật lý, máy ảo sẽ cần cài đặt Docker Engine. Sau đó các docker containers sẽ chạy trên Docker Engine. Các ứng dụng chạy trên Docker Engine được minh họa như hình 2.16



Hình 2.16 Docker container

(Nguồn: <https://www.docker.com/resources/what-container/>)

Ứng dụng Blockchain HF sẽ chạy trong các docker container. Sơ đồ ứng dụng Blockchain được minh họa ở hình 2.17.



Hình 2.17 Sơ đồ ứng dụng Blockchain Hyperledger Fabric

(Nguồn: HypderLedger document https://hyperledger-fabric.readthedocs.io/en/release-2.5/getting_started.html)

Để triển khai kiến trúc mạng Fabric, nghiên cứu để xuất sử dụng công cụ Minifabric (<https://labs.hyperledger.org/labs/minifabric.html>). Minifabric được thiết kế để đơn giản hóa quá trình triển khai mạng HF. Công cụ chỉ yêu cầu Docker Engine và hoạt động trên các hệ điều hành Windows 10, Linux và MacOS. Quá trình thiết lập mạng HF bằng một lệnh duy nhất. Sau khi mạng HF được thiết lập và chạy bằng Minifabric, Minifabric cung cấp lệnh để hoạt động với chuỗi khôi, kênh và ứng dụng

Blockchain Hyperledger Fabric. Minifabric cung cấp các chức năng chính sau:

- Thiết lập và mở rộng mạng HF, chẳng hạn như thêm các tổ chức mới thông qua tập tin cấu hình spec.yaml
- Các chức năng với kênh như tạo, cập nhật, đưa các peer vào, cập nhật kênh và truy vấn kênh
- Các chức năng với chaincode như cài đặt, nâng cấp, phê duyệt, khởi tạo, gọi, truy vấn.
- Hỗ trợ tập dữ liệu riêng tư trong mạng.
- Truy vấn kích thước số cái và khôi.
- Tạo hồ sơ kết nối và các tập tin ví cho SDK của các ngôn ngữ go, node, python và các extensions để tích hợp vào VSCode.
- Tích hợp Hyperledger Explorer và Caliper
- Giám sát, kiểm tra trạng thái và giám sát các nút bên trong mạng Blockchain.
- Minifabric sử dụng tập tin cấu hình thông số mạng spec.yaml trong thư mục làm việc để thiết lập mạng Fabric. Trong đó, cho phép định nghĩa các tên tổ chức khác nhau, tên nút, số lượng tổ chức, để thiết lập mạng Fabric.

2.3.6.2 Các đặc điểm chính

- Tính mô-đun
 - Hyperledger Fabric được đội ngũ phát triển thiết kế kiến trúc dưới dạng mô-đun. Từ các thuận toán đồng thuận, giao thức quản lý danh tính, quản lý danh tính đến các thư viện mật mã đều có thể triển khai dưới dạng mô-đun (pluggable). Do đó, bên triển khai công nghệ sẽ có nhiều tùy chọn, cách cấu hình hệ thống cho phù hợp với từng mục đích khác nhau.
- Ở mức độ trừu tượng cao, Hyperledger Fabric gồm những mô-đun sau:
 - Ordering service là thành phần thiết lập sự đồng thuận trên mạng và chuyển các khối (block) đã được xác minh đến các nút trong mạng.
 - Nhà cung cấp dịch vụ thành viên (membership service provider) là thành phần liên kết các thực thể trong mạng với một định danh riêng được mã hóa.
 - Thành phần cung cấp chức năng kết nối mạng ngang hàng giữa các nút trong hệ thống.
 - Hợp đồng thông minh (chaincode) chạy trên môi trường ảo hóa (như Docker) chứa logic nghiệp vụ của hệ thống.
 - Sổ cái (Ledger) là thành phần lưu trữ dữ liệu các khối trong chuỗi, sổ cái sử dụng các hệ cơ sở quản trị dữ liệu NoSQL.
 - Chứng thực, chính sách đối với quyền của các thực thể trên mạng.
 - Nền tảng Blockchain riêng tư (private Blockchain hay permissioned Blockchain)

Trong một nền tảng Blockchain công khai, bất cứ ai cũng có thể tham gia và mọi tác nhân tham gia đều ẩn danh. Hơn nữa, mọi dữ liệu được lưu vết trên cơ sở dữ liệu Blockchain hoàn toàn được công khai, bất cứ ai cũng có thể truy vấn và đọc được dữ liệu. Đối với môi trường doanh nghiệp, dữ liệu cần có sự riêng tư cũng như bảo mật sẽ

không phù hợp để ứng dụng các nền tảng Blockchain công khai vào hệ thống của mình.

Mặt khác, các nền tảng Blockchain riêng tư như Hyperledger Fabric giúp thiết lập một hệ thống chỉ có thể tham gia khi đã được cho phép, các tác nhân tham gia vào hệ thống đều được xác định danh tính và kiểm duyệt hoạt động

Ngoài ra, việc người dùng thực thi các hành động xấu nhằm trực lợi cũng sẽ bị hạn chế. Những người tham gia vào hệ thống đều được định danh, những người khác hoàn toàn có thể nắm bắt được các hành động trên hệ thống của người khác như gửi giao dịch, sửa đổi cấu hình mạng hay triển khai hợp đồng thông minh. Các hành động đều được lưu vết lại trên cơ sở dữ liệu Blockchain. Các hành động mờ ám sẽ hoàn toàn không che dấu được hệ thống cũng như các người dùng khác trong mạng.

2.3.6.3 Smart Contract

Smart contract là một chương trình máy tính chứa các điều khoản logic được các bên tham gia vào hệ thống chấp nhận. Hợp đồng thông minh cho phép thực hiện các giao dịch đáng tin cậy giữa nhiều bên mà không cần bên thứ ba làm trung gian. Trong Hyperledger Fabric, hợp đồng thông minh được gọi với cái tên mã chuỗi (chaincode). Chaincode trong Hyperledger Fabric được viết bằng một trong ba ngôn ngữ lập trình là Go, Java hoặc Javascript.

Có ba điểm chính áp dụng cho hợp đồng thông minh:

- Nhiều hợp đồng thông minh có thể chạy trên cùng một hệ thống.
- Hợp đồng thông minh có thể được triển khai một cách linh hoạt (trong nhiều trường hợp và bởi bất cứ ai).

Mã nguồn của hợp đồng nên được coi là không đáng tin cậy hay thậm chí là độc hại. Cho nên việc thực thi các hợp đồng thông minh được diễn ra trong các môi trường ảo hóa, độc lập.

Tính riêng tư và bảo mật

Như chúng ta đã thảo luận, trong một mạng Blockchain công khai, các giao dịch được thực hiện trên mọi nút trong mạng ngang hàng. Điều này đồng nghĩa rằng việc bảo mật dữ liệu về các giao dịch là bất khả thi. Mọi giao dịch và dữ liệu liên quan đều hiển thị cho mọi nút trong mạng.

Những hạn chế kể trên sẽ là vấn đề rất lớn nếu áp dụng vào các hệ thống doanh nghiệp, kinh doanh. Lấy ví dụ với một hệ thống chuỗi cung ứng, một số bên do một lý do nào đó chẳng hạn như đối tác chiến lược hay khách hàng thân thiết được hưởng ưu đãi hơn so với phần còn lại. Nhưng mọi thành phần tham gia vào mạng đều nhìn thấy được giao dịch, việc áp dụng các chính sách ưu tiên đó sẽ là không thể vì mọi người cũng muốn được hưởng mức ưu đãi đó.

Hyperledger Fabric giải quyết vấn đề riêng tư và bảo mật thông qua tính năng

kênh (channel) và dữ liệu riêng tư (private data). Trong các kênh, các bên tham gia mạng Hyperledger Fabric sẽ thiết lập một mạng con nơi nút thành viên có thể tham gia kênh và chỉ có họ mới nhìn thấy các giao dịch diễn ra trên kênh. Do đó, chỉ những nút tham gia và kênh mới có quyền truy cập vào dữ liệu giao dịch trên kênh đó. Dữ liệu riêng tư ở mức độ thấp hơn, giúp các thành viên trên một kênh có thể trao đổi dữ liệu riêng tư với các thành viên khác trong kênh mà không cần tạo một kênh mới.

Hiệu suất và khả năng mở rộng

Hiệu suất và khả năng mở rộng đang là vấn đề nan giải với các nền tảng Blockchain công khai sử dụng thuật toán đồng thuận bằng chứng công việc (Proof of work). Bitcoin và Ethereum chỉ đạt hiệu suất trong khoảng vài chục giao dịch mỗi giây, kém xa so với các hệ thống truyền thống lên đến hàng ngàn giao dịch mỗi giây. Nổi tiếng nhất là sự kiện mạng Ethereum bị nghẽn do quá nhiều người chơi trò chơi Crypto Kitties vào năm 2017.

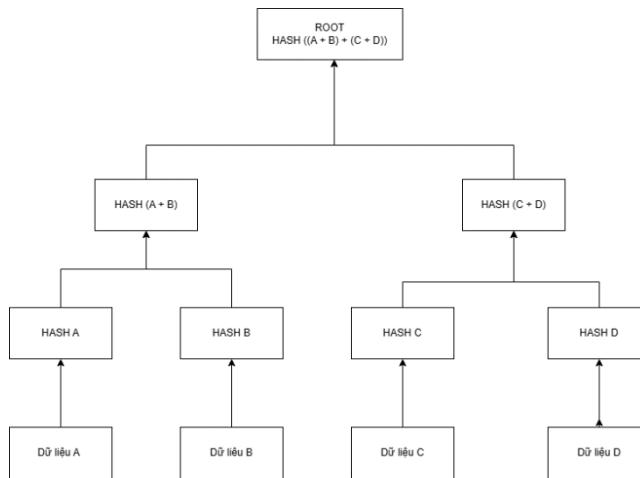
Hyperledger Fabric là một nền tảng Blockchain riêng tư và không sử dụng thuật toán đồng thuận bằng chứng công việc nên hiệu suất so với các nền tảng như Bitcoin hay Ethereum là tốt hơn đáng kể. Một số tài liệu nghiên cứu đã được xuất bản về việc thử nghiệm hiệu suất của Hyperledger Fabric. Hyperledger Fabric khả năng đạt tới 20.000 giao dịch mỗi giây.

Bảng 2.2 So sánh Hyperledger Fabric về một số nền tảng khác

	Bitcoin	Ethereum	Hyperledger Fabric
Cơ chế đồng thuận	Proof Of Work	Proof Of Stack	PBFT
Truy cập dữ liệu	Công Khai	Công Khai	Riêng Tư
Thực thi HĐTM	Thuộc ứng dụng	EVM	Docker
Ngôn ngữ	Go, C++	Solidity,Serpent,LLL, C++	Go, Java, JavaScript
Tiền tệ	Bitcoin	Ether	Không có

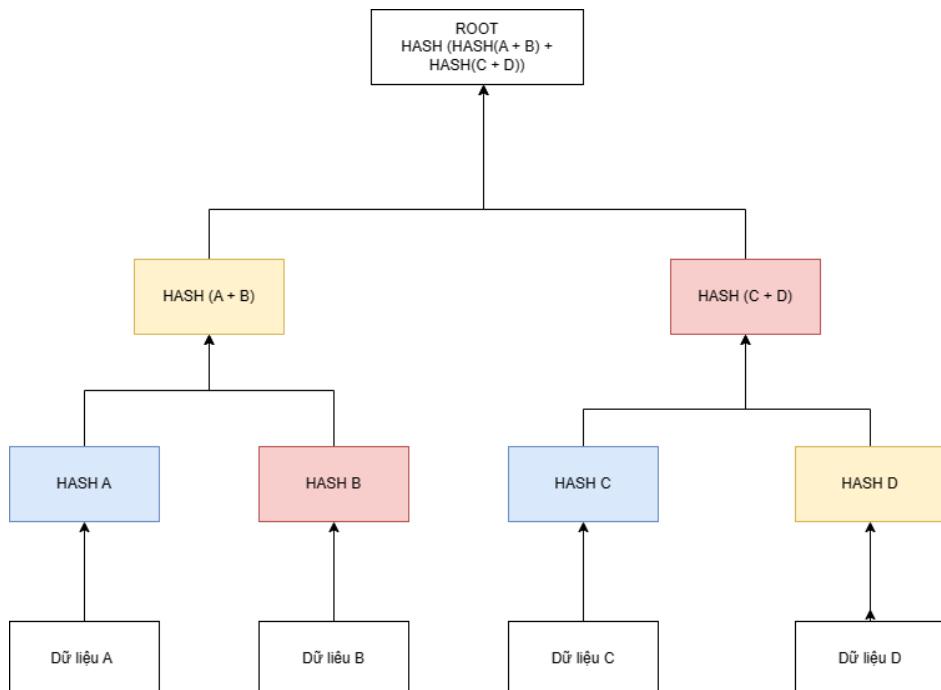
2.3.7 Merkle Tree

2.3.7.1 Cấu trúc dữ liệu merkle root



Hình 2.18 Merkle Tree

Ví dụ về bốn dữ liệu trong một khối: A, B, C và D. Mỗi dữ liệu được băm và hàm băm được lưu trữ trong mỗi nút lá, dẫn đến các cặp Hash A, B, C và D. Liên tiếp các nút lá sau đó được tóm tắt trong một nút cha bằng cách băm Hash A và Hash B, dẫn đến Hash AB và băm riêng Hash C và Hash D, dẫn đến Hash CD. Hai băm (Hash AB và Hash CD) sau đó được băm lại để tạo Root Hash (Root Merkle). Quá trình này có thể được tiến hành trên các tập dữ liệu lớn hơn: các khối liên tiếp có thể được băm cho đến khi chỉ có một nút ở trên cùng.



Hình 2.19 Tạo multiproof của A,C và xác minh dữ liệu A, C

Để tạo multi-proof cho giá trị hash của nút A và C, ta cần biết vị trí của chúng trong Merkle Tree [11]. Giả sử rằng nút A có vị trí là 0 (tức là nó là nút lá đầu tiên), và nút C có vị trí là 2.

Sau đó, ta sẽ tạo multi-proof cho nút A và C bằng cách xác định đường dẫn từ mỗi nút cần chứng thực lên đến nút gốc của Merkle Tree. Đường dẫn này sẽ bao gồm các cặp giá trị hash của các nút cha trên đường từ nút lá chứa giá trị cần chứng thực lên đến nút gốc.

Đối với A:

Proof cho A sẽ bao gồm Hash B và Hash CD, vì A là nút lá đầu tiên và nó được tổng hợp với B để tạo ra Hash AB, sau đó Hash AB và Hash CD được tổng hợp để tạo ra Root Hash.

Merkle proof cho A là: [Hash B, Hash CD]

Đối với C:

Proof cho C sẽ bao gồm Hash AB và Hash D, vì C là nút lá thứ ba và nó được tổng hợp với D để tạo ra Hash CD, sau đó Hash AB và Hash CD được tổng hợp để tạo ra Root Hash.

Merkle proof cho C là: [Hash AB, Hash D]

Vì vậy, để xác minh dữ liệu A và C, ta cần sử dụng Merkle proof tương ứng cho từng giá trị hash và kiểm tra chúng bằng cách tính toán lại Root Hash. Nếu Root Hash tính toán được khớp với Root Hash được lưu trữ, điều đó có nghĩa là dữ liệu đã được chứng thực và không bị thay đổi.

2.4 Công nghệ sử dụng

2.4.1 Hyperledger Fabric



Hình 2.20 Hyperledeger fabric

(Nguồn: *Conducting Data with Concerto and Hyperledger Fabric*
<https://www.hyperledger.org/blog/2018/11/28/conducting-data-with-concerto-and-hyperledger-fabric>)

a) Giới thiệu chung

Hyperledger Fabric là một nền tảng Blockchain mã nguồn mở thuộc dự án Hyperledger do tổ chức Linux Foundation khởi động vào năm 2015. Hyperledger Fabric được duy trì và phát triển chính bởi tập đoàn IBM và Digital Asset. Hyperledger Fabric là một nền tảng Blockchain riêng tư (private Blockchain hay permissioned Blockchain) khác với Bitcoin hay Ethereum là các nền tảng Blockchain công khai (public Blockchain hay permissionless Blockchain). Hyperledger Fabric được thiết kế để giải quyết các vấn đề doanh nghiệp (enterprise), nghiệp vụ (business) như chuỗi cung ứng, y tế, giáo dục, bảo hiểm.

2.4.2 NodeJS

a) Giới thiệu chung

Node.js [12] là một môi trường thực thi Javascript độc lập, mã nguồn mở và đa nền tảng. Được xây dựng dựa trên engine google chrome v8, Node.js cho thấy khả năng xử lý các tác vụ ở phía backend một cách hiệu quả với đặc trưng bất đồng bộ của mình.

Ngoài khả năng xử lý các tác vụ backend, Node.js cũng được sử dụng phổ biến trong lĩnh vực Blockchain. Cụ thể, Node.js có thể được sử dụng để phát triển các ứng dụng Blockchain trên nền tảng Hyperledger Fabric. Hyperledger Fabric là một nền tảng Blockchain do Linux Foundation phát triển, cung cấp một cách tiếp cận modul và linh hoạt cho việc phát triển các ứng dụng Blockchain doanh nghiệp. Với Node.js, các nhà phát triển có thể tận dụng các tính năng bất đồng bộ để phát triển các ứng dụng Blockchain có khả năng xử lý các giao dịch và thực hiện các tác vụ phức tạp một cách nhanh chóng và hiệu quả.

b) Framework Express



Hình 2.21 ExpressJS

(*Nguồn:Introduction to ExpressJS. <https://geekflare.com/introduction-expressjs/>*)

Express [13] là một framework rất phổ biến trong việc xây dựng các API cho các ứng dụng web và mobile. Với Express, người dùng có thể dễ dàng tạo các endpoint cho API, điều hướng yêu cầu đến các xử lý tương ứng và trả về các phản hồi. Việc xử lý các yêu cầu và phản hồi được thực hiện một cách đơn giản và linh hoạt nhờ vào sự hỗ trợ của các middleware.

Ngoài ra, Express cũng được sử dụng trong việc phát triển các ứng dụng Blockchain bằng Node.js. Ví dụ, trong việc phát triển các ứng dụng Blockchain trên nền tảng Hyperledger Fabric, Express có thể được sử dụng để xây dựng các API để kết nối và tương tác với các nút (nodes) trên Blockchain. Việc sử dụng Express trong việc phát triển các ứng dụng Blockchain giúp cho việc triển khai các API trở nên đơn giản hơn và giúp cho người dùng tập trung vào việc xây dựng logic nghiệp vụ của ứng dụng.

2.4.3 Docker



Hình 2.22 Docker

(Nguồn: Docker In Action. <https://labs.flinters.vn/wp-content/uploads/2021/07/docker-logo.png>)

Docker [14] là một nền tảng cho developers và sysadmin để develop, deploy và run application với container. Nó cho phép tạo các môi trường độc lập và tách biệt để khởi chạy và phát triển ứng dụng và môi trường này được gọi là container. Khi cần deploy lên bất kỳ server nào chỉ cần run container của Docker thì application của bạn sẽ được khởi chạy ngay lập tức.

a) Giới thiệu về container

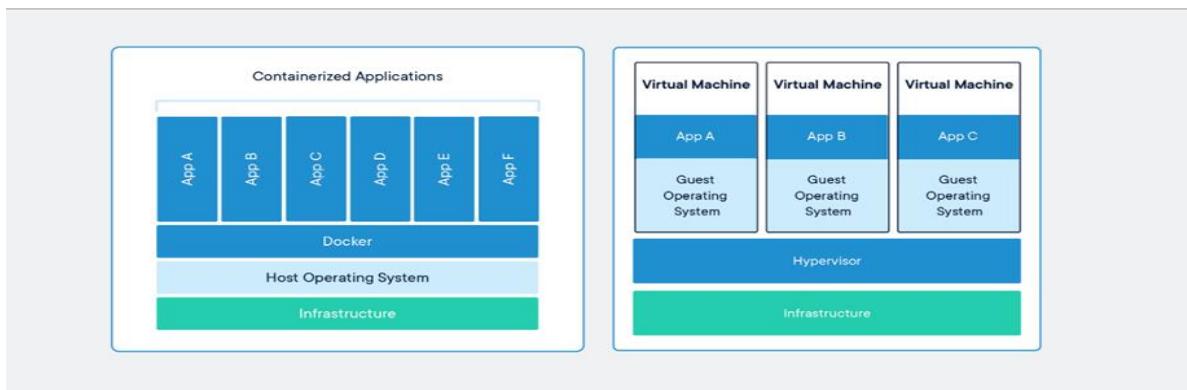
Container là một đơn vị phần mềm tiêu chuẩn đóng gói mã nguồn và các thành phần phụ thuộc. Đặc điểm của container là nhẹ, độc lập, có thể thực thi.

b) So sánh giữa container và máy ảo

Container và máy ảo đều là các môi trường ảo hóa có đặc điểm chung đó là tài nguyên được phân tách độc lập, khác nhau ở chỗ container ảo hóa hệ điều hành thay vì ảo hóa phần cứng như máy ảo. Container được đánh giá có tính linh hoạt và hiệu quả hơn máy ảo.

Nhiều container có thể chạy trên cùng một máy vật lý và chia sẻ chung nhân của hệ điều hành với các container khác.

Nhiều máy ảo cũng có thể chạy trên một máy vật lý. Tuy nhiên, khác với container chia sẻ chung nhân của hệ điều hành với các container khác, mỗi máy ảo điều có một hệ điều hành riêng, ứng dụng, các tệp nhị phân và thư viện cần thiết. Điều đó làm cho kích thước bộ nhớ mỗi máy ảo chiếm dụng lên đến hàng chục GB thay vì MB như container.



Hình 2.23 So sánh giữa container và máy ảo

(Nguồn:

https://www.researchgate.net/publication/343764931_Optimizing_Virtual_Resources_Management_Using_Docker_on_Cloud_Applications)

2.4.4 NextJS



Hình 2.24 NextJS

(Nguồn: *Why NextJS ?*. <https://articles.wesionary.team/why-nextjs-in-2020-8c2f76973cbf>)

Next.js [15] cung cấp cho người dùng một số tính năng và công cụ để giúp tối ưu hoá trải nghiệm người dùng và hiệu năng ứng dụng web. Một trong số đó là hỗ trợ cho Server Side Rendering (SSR) và Static Site Generation (SSG). SSR cho phép người dùng render các trang web trực tiếp trên máy chủ trước khi trả về cho trình duyệt, điều này giúp giảm thời gian tải trang và tăng khả năng tương tác của người dùng. SSG cho phép người dùng tạo ra các trang web tĩnh (static) trước đó và lưu chúng trên máy chủ, điều này giúp cải thiện hiệu năng của ứng dụng bằng cách giảm tải cho máy chủ và tăng tốc độ tải trang.

Ngoài ra, Next.js còn hỗ trợ các tính năng như Code splitting, Dynamic Importing, Automatic Code Optimization và Image Optimization, giúp giảm thiểu thời gian tải trang và cải thiện hiệu năng ứng dụng. Next.js cũng cung cấp các công cụ để hỗ trợ SEO và phát triển các ứng dụng web tiện ích như tích hợp với các công cụ như Google Analytics và các tính năng như Hot Module Replacement (HMR) để tăng năng suất lập trình viên.

2.4.5 Mongodb



Hình 2.25 MongoDB

(*Nguồn: MongoDB: The Developer Data Platform.*
https://webimages.mongodb.com/_com_assets/cms/kuzt9r42or1fxvlq2-Meta_Generic.png)

MongoDB [16] là một hệ quản trị cơ sở dữ liệu NoSQL, được thiết kế để hỗ trợ cho các ứng dụng có tính mở rộng cao và phục vụ cho các truy vấn dữ liệu phức tạp. Trong MongoDB, các tài liệu được lưu trữ dưới dạng các bản ghi tài liệu (document records), được lưu trữ dưới dạng JSON (JavaScript Object Notation) hoặc BSON (Binary JSON). BSON là một định dạng nhị phân của JSON, cung cấp tính năng mã hóa thêm cho các kiểu dữ liệu phức tạp như các kiểu ngày tháng, số thực và ObjectId.

MongoDB cũng hỗ trợ các tính năng như sharding (phân tán dữ liệu), replica sets (bản sao dữ liệu), và index hóa để giúp tối ưu hóa hiệu suất truy vấn dữ liệu

a) Đặc điểm chính

MongoDB cũng hỗ trợ các tính năng như replica set (bộ đôi sao chép) và sharding (phân mảnh) để tăng tính sẵn sàng và khả năng mở rộng của cơ sở dữ liệu.

Các tài liệu trong MongoDB có thể chứa các trường nhị phân (binary) và các trường lồng nhau (nested fields) giúp tăng tính linh hoạt và hiệu quả trong việc lưu trữ và truy vấn dữ liệu.

MongoDB cung cấp các API hỗ trợ truy vấn và xử lý dữ liệu linh hoạt như aggregation framework, MapReduce, và các phương pháp truy vấn đa dạng.

MongoDB cũng hỗ trợ các tính năng an ninh và quản lý người dùng để bảo vệ dữ liệu của ứng dụng.

2.4.6 Jenkins



Hình 2.26 Jenkins

(Nguồn: Jenkins – An Open Source for Continuous Integration Server
<https://blog.ntechdevelopers.com/jenkins-an-open-source-for-continuous-integration-server/>)

Jenkins [17] là một opensource dùng để thực hiện chức năng tích hợp liên tục (gọi là **CI – Continuous Integration**) và xây dựng các tác vụ tự động hóa.

Nó tích hợp các source code của các members trong team lại nhanh chóng một cách liên tục, theo dõi sự thực thi và trạng thái thông qua các bước kiểm thử (**Integration test, units test**). Tất nhiên là nhằm giúp sản phẩm chạy ổn định.

CHƯƠNG 3. XÂY DỰNG ỦNG DỤNG VĂN BẰNG CHỨNG CHỈ TÍCH HỢP BLOCKCHAIN

3.1 Mô tả bài toán

Hiện nay, việc quản lý VBCC được quy định cụ thể riêng theo từng Trường, nhằm để hướng dẫn quy trình thực hiện, báo cáo, lưu trữ hồ sơ và phân cấp chịu trách nhiệm của các cá nhân và đơn vị liên quan trong khi thực hiện công việc. Tuy nhiên, công việc quản lý VBCC có nhiều hồ sơ, quy trình như bàn giao, in phôi VBCC, trình ký và đóng dấu, rà soát thông tin in lên phôi VBCC, lập sổ gốc, quản lý phát VBCC, xác minh VBCC, còn thủ công nên ảnh hưởng đến chất lượng hiệu quả công việc. Chẳng hạn như VBCC phát cho sinh viên dễ sai sót, do VBCC phải được in thông tin, ký tên, đóng dấu. Thông tin VBCC gồm có: số hiệu phôi, số vào sổ gốc, họ tên, ngày sinh, giới tính, nơi sinh, kết quả, ngày cấp, người cấp.

Thủ tục cấp VBCC giấy phải qua nhiều công đoạn, tốn thời gian và chi phí: Trường làm đề nghị cấp phôi chứng chỉ: cần 2 ngày chờ phê duyệt, làm hồ sơ quản lý và lưu trữ phôi chứng chỉ.... Ngoài ra, hiện trạng in VBCC giấy gây tốn công sức và ngân sách:

- Đối với Trường: với số lượng lớn VBCC được cấp như hiện nay và phải cấp cho từng sinh viên sẽ làm tốn chi phí in ấn và thời gian nhận chứng chỉ. Giá phôi chứng chỉ xê dịch khoảng 5.000 đồng/phôi chứng chỉ.
- Đối với cơ quan quản lý: nếu có xảy ra sai sót thì việc truy tìm hồ sơ xử lý sẽ gây khó khăn cho cơ quan quản lý.
- Dễ làm giả chứng chỉ giấy.

Do đó, bài toán đặt ra nhu cầu cải tiến trong 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.

Sau khi thực hiện công tác tổ chức thi chứng chỉ ứng dụng Công Nghệ Thông Tin, Hội đồng thi công bố kết quả thí sinh thi đạt, Trường sẽ ban hành quyết định cấp VBCC kèm theo danh sách thí sinh được cấp VBCC. Danh sách thí sinh được cấp VBCC gồm có thông tin như số báo danh, họ tên, ngày sinh, giới tính, dân tộc, điểm thi lý thuyết, điểm thi thực hành. Tiếp theo Trường lập đề nghị cấp phôi chứng chỉ và tiếp nhận, quản lý phôi chứng chỉ.

Khi Trung tâm in và cấp chứng chỉ cho sinh viên, Trung tâm tiến hành ghi nhận thông tin VBCC vào CSDL, những thông tin cần tính minh bạch sẽ được lưu trữ vào hệ thống Blockchain.

Khi sinh viên nhận chứng chỉ, sinh viên sẽ quản lý xem danh sách chứng chỉ được cấp, thông tin trên chứng chỉ có thể chia sẻ theo lựa chọn trong các thông tin cá nhân

được lưu trên CSDL. Khi Đơn vị xác minh nhận thông tin VBCC được chia sẻ từ sinh viên, thông tin VBCC xác thực với dữ liệu trong Blockchain.

Khi phát hành VBCC cho sinh viên: Thông tin VBCC của sinh viên được kết hợp lưu trên CSDL và trên hệ thống Blockchain để đảm bảo tính an toàn và tin cậy. Ứng dụng ký số các thông tin VBCC của sinh viên nhằm bảo vệ tính minh bạch trên môi trường điện tử.

Cung cấp thông tin xác minh VBCC: Sinh viên có thể sở hữu một hoặc nhiều VBCC của Trường cấp. Khi cần xác minh VBCC thì chỉ cần gửi thông tin VBCC, có thể lựa chọn thông tin cá nhân như giới tính, dân tộc... khi chia sẻ cho đơn vị xác minh

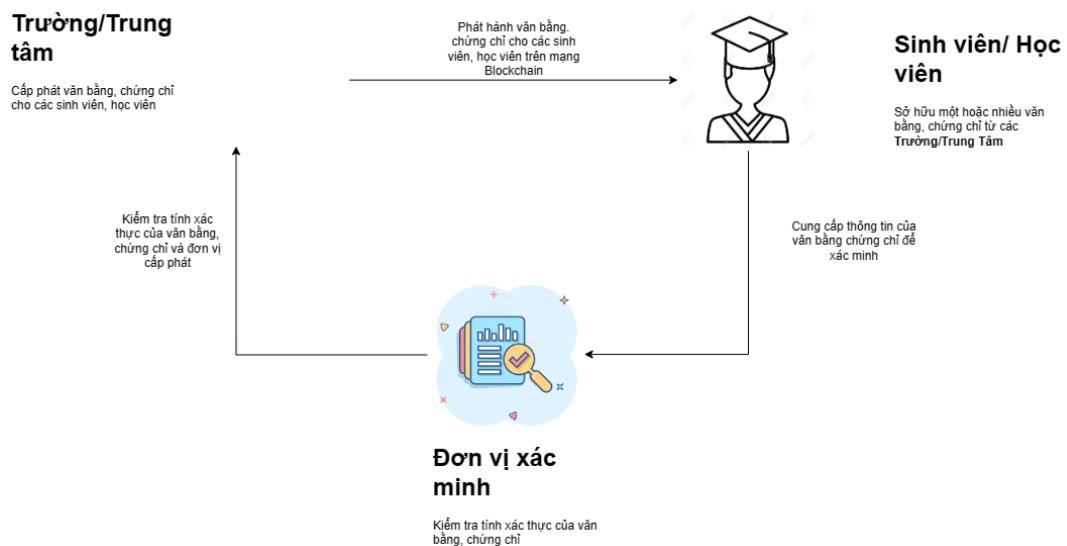
Kiểm tra xác minh VBCC: Đơn vị xác minh nhận thông tin VBCC được chia sẻ từ sinh viên, và có thể xác thực thông tin VBCC với dữ liệu trong Blockchain.

3.2 Tổng quan giải pháp

Nghiên cứu đề xuất hệ thống quản lý VBCC 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 các chức năng chính: ký số lên thông tin VBCC, lưu chữ ký số vào Blockchain, đồng thời lưu thông tin VBCC vào Blockchain và CSDL, từ đó truy vấn dữ liệu trong Blockchain để xác thực VBCC.

- Phần ứng dụng web: Nodejs, Express và giao diện TailwindCSS và MUI để giao tiếp với người dùng, truy vấn, cập nhật dữ liệu vào Blockchain, CSDL
- Phần CSDL: Hệ CSDL MongoDB lưu thông tin VBCC và các thông tin không được lưu trong Blockchain.
- Phần Blockchain: Nền tảng Hyperledger Fabric và CA quản lý định danh người dùng và ứng dụng bằng mật mã khóa công khai.

3.3 Mối quan hệ trong quy trình xác minh VBCC



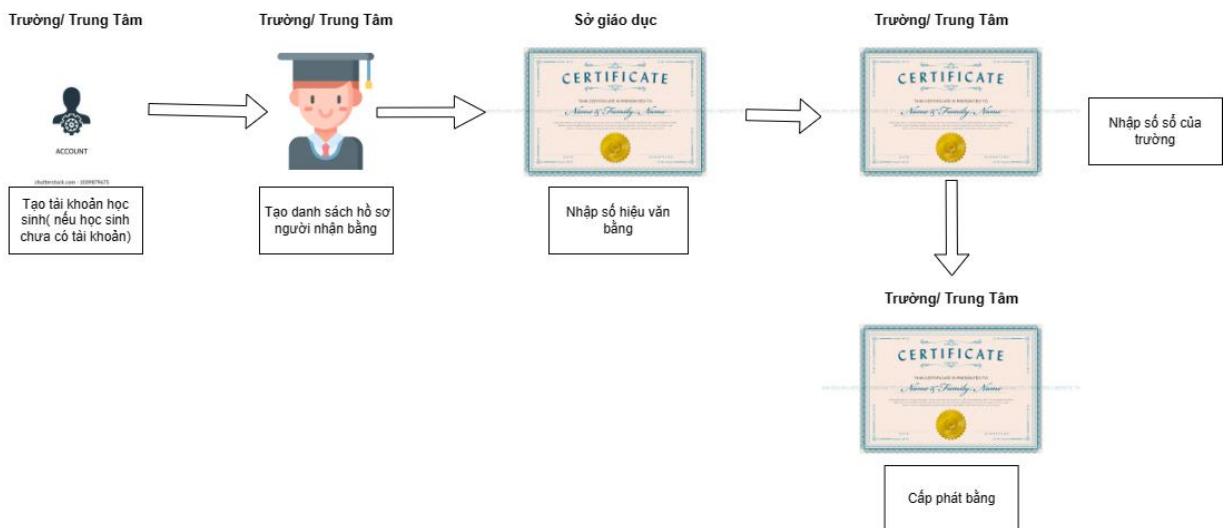
Hình 3.1 Mối quan hệ trong quy trình xác minh VBCC

- Trường/Trung tâm: Sẽ là người cấp phát văn bằng, chứng chỉ cho sinh viên và

những văn bằng chứng chỉ này được đưa lên Blockchain

- Sinh viên: Người được nhận văn bằng chứng chỉ từ trường và có thẻ quản lý văn bằng, chứng chỉ của mình. Có thể chia sẻ thông tin văn bằng, chứng chỉ và bằng chứng là văn bằng, chứng chỉ của mình (Có thể không cần phải chia sẻ nếu sinh viên muốn).
- Đơn vị xác minh: Người cần xác minh VBCC của sinh viên có chính xác không sẽ đưa thông tin cho đơn vị xác minh để xác minh VBCC

3.4 Quy trình cấp VBCC



Hình 3.2 Quy trình cấp VBCC

Quy trình gồm 5 bước cấp phát VBCC trong hệ thống

Bước 1. Trường sẽ tạo tài khoản cho sinh viên nếu sinh viên chưa có tài khoản

Bước 2. Trường sẽ tạo danh sách hồ sơ người nhận VBCC

Bước 3. Sở giáo dục sẽ vào hệ thống và nhập số hiệu cho từng VBCC

Bước 4. Sau đó trường sẽ vào ban phát số vào sổ

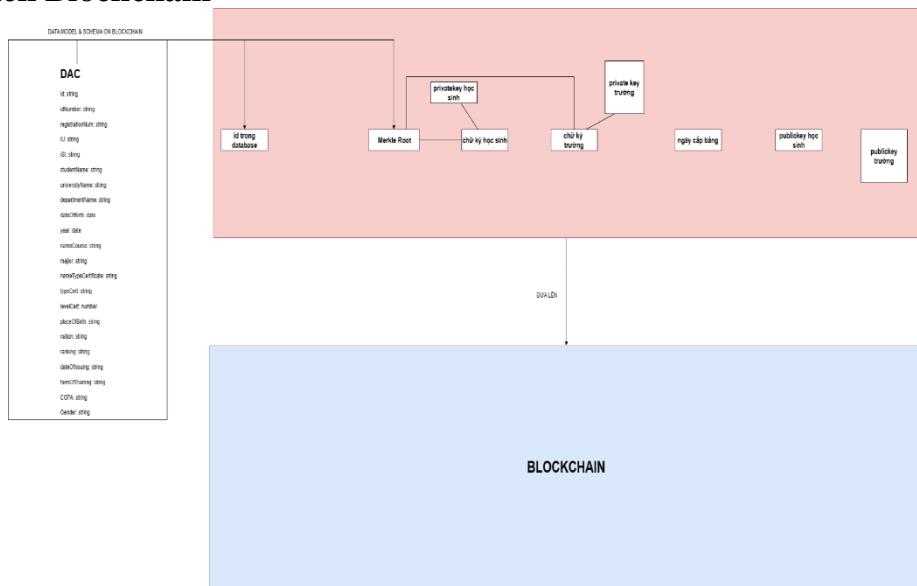
Bước 5. Trường đem hồ sơ người nhận chọn loại văn bằng và cấp phát

3.5 Thuật toán xác minh VBCC

Thuật toán để xác minh VBCC áp dụng cấu trúc dữ liệu cây merkle tree.

Việc đầu tiên để có thể nhìn toàn vẹn cách áp dụng thuật toán ta sẽ gồm 3 quy trình:

3.5.1 Đưa VBCC lên Blockchain

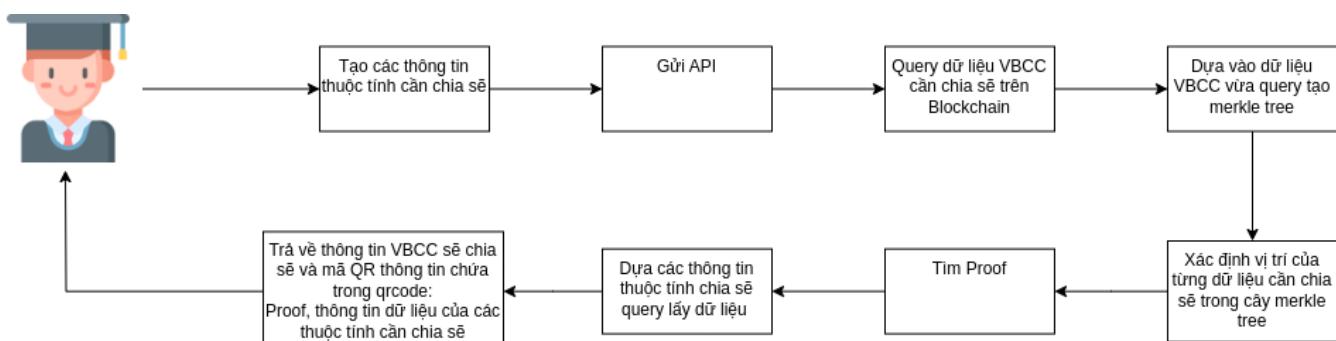


Hình 3.3 Thuật toán xác minh VBCC

Để đưa dữ liệu 1 VBCC lên Blockchain ta sẽ cần có: ID của VBCC trong cơ sở dữ liệu, merkle root, chữ ký sinh viên, chữ ký trưởng, ngày cấp bằng, publicKey sinh viên và pulicKey trưởng, dữ liệu VBCC

- ID của VBCC trong cơ sở dữ liệu: là id của VBCC trong cơ sở dữ liệu.
- Merkle root: là 1 dãy chuỗi hash được lấy từ root của Merkle tree.(Merkle tree được tạo dựa trên dữ liệu của VBCC)
- Chữ ký sinh viên: được tạo ra bởi merkle root và private key của sinh viên được nhận VBCC
- Chữ ký trưởng: được tạo bởi merkle root và private key của trưởng phát hành VBCC.
- publicKey sinh viên: publicKey của người nhận VBCC
- publicKey trưởng: publicKey của người phát hành VBCC
- Chú ý:
- privateKey: là khóa bí mật chỉ được biết bởi chủ sở hữu. Nó được sử dụng để tạo chữ ký.
- publicKey: khóa công khai là mã định danh duy nhất có thể được chia sẻ với những người tham gia khác trên mạng. Nó được sử dụng để xác minh chữ ký số được tạo bằng khóa riêng tư tương ứng.

3.5.2 Tạo proof xác minh VBCC



Hình 3.4 Tạo proof xác minh VBCC

Bước 1. Để tạo thông tin VBCC cần chia sẻ và sinh viên sẽ chọn thông tin

mình muốn chia sẻ nhưng sẽ có một số thông tin là phải bắt buộc có: tên, nơi sinh, ngày sinh, chứng minh nhân dân,...

Bước 2. Sau đó giao diện của người dùng tương tác sẽ gửi đến API xử lý

Bước 3. Truy vấn dữ liệu VBCC trên Blockchain

Bước 4. Dựa vào dữ liệu VBCC vừa truy vấn tạo merkle tree

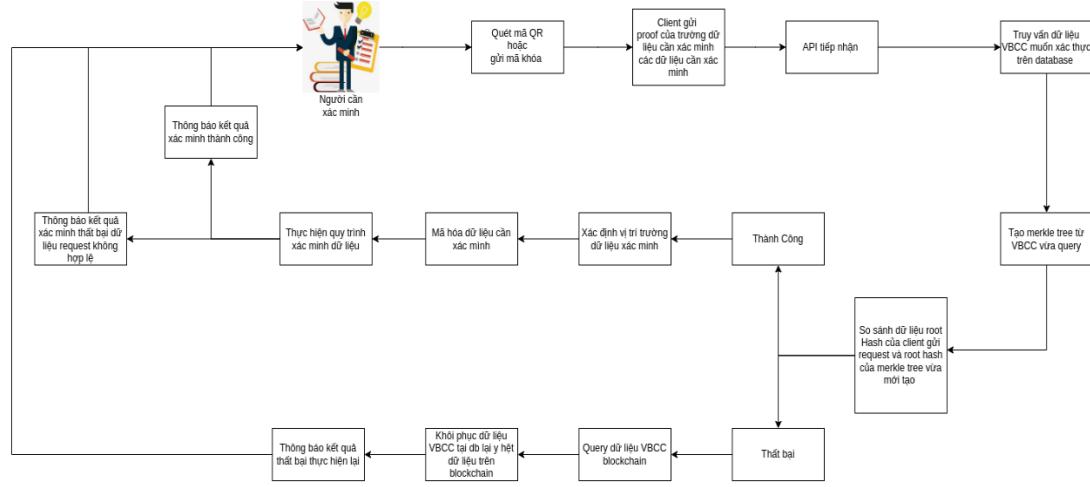
Bước 5. Xác định vị trí của thuộc tính mà sinh viên đã gửi bằng cách ta sẽ truy vấn schema trong schema gồm các thuộc tính trên Blockchain. Sau đó lấy thuộc tính sinh viên cần chia sẽ so sánh và lấy vị trí dựa vào schema gồm có các thuộc tính trên Blockchain. Và ứng với mỗi thuộc tính ta sẽ có 1 vị trí cụ thể cho nó. Mục đích để có thể xác định dữ liệu cần xác minh.(Có thể xem thuật toán merkle tree chúng em đã nghiên cứu)

Bước 6. Khi có được vị trí của dữ liệu cần xác minh thì ta cần tìm proof của từng dữ liệu đó. Khi dùng proof đó ta có thể chứng minh dữ liệu cần xác minh là đúng

Bước 7. Thông tin thuộc tính dữ liệu cần chia sẽ nó dùng để chứng minh dữ liệu chia sẽ này là 1 phần của cây merkle tree => những dữ liệu này chính xác

Bước 8. Sau đó client sẽ trả về thông tin cần chia sẻ và mã QR

3.5.3 Xác minh VBCC



Hình 3.5 Xác minh VBCC

Bước 1. Khi người cần xác minh VBCC đầu tiên họ sẽ phải cần đưa proof của dữ liệu cần xác minh/dữ liệu cần xác minh thì những dữ liệu này có thể được lưu trong cơ sở dữ liệu hoặc mã QR.

Bước 2. Nếu xác thực mã QR sẽ được lưu dưới dạng QR hoặc xác thực qua tra cứu sẽ được lưu trong cơ sở dữ liệu

Bước 3. API tiếp nhận và truy vấn dữ liệu VBCC muốn chứng thực ở database

Bước 4. Tạo merkle tree từ VBCC vừa truy vấn dữ liệu

Bước 5. So sánh root hash của merkle tree vừa mới tạo và root hash người cần xác minh gửi

Bước 6. Thành công

Bước 7. Xác định vị trí từng trường dữ liệu cần xác minh

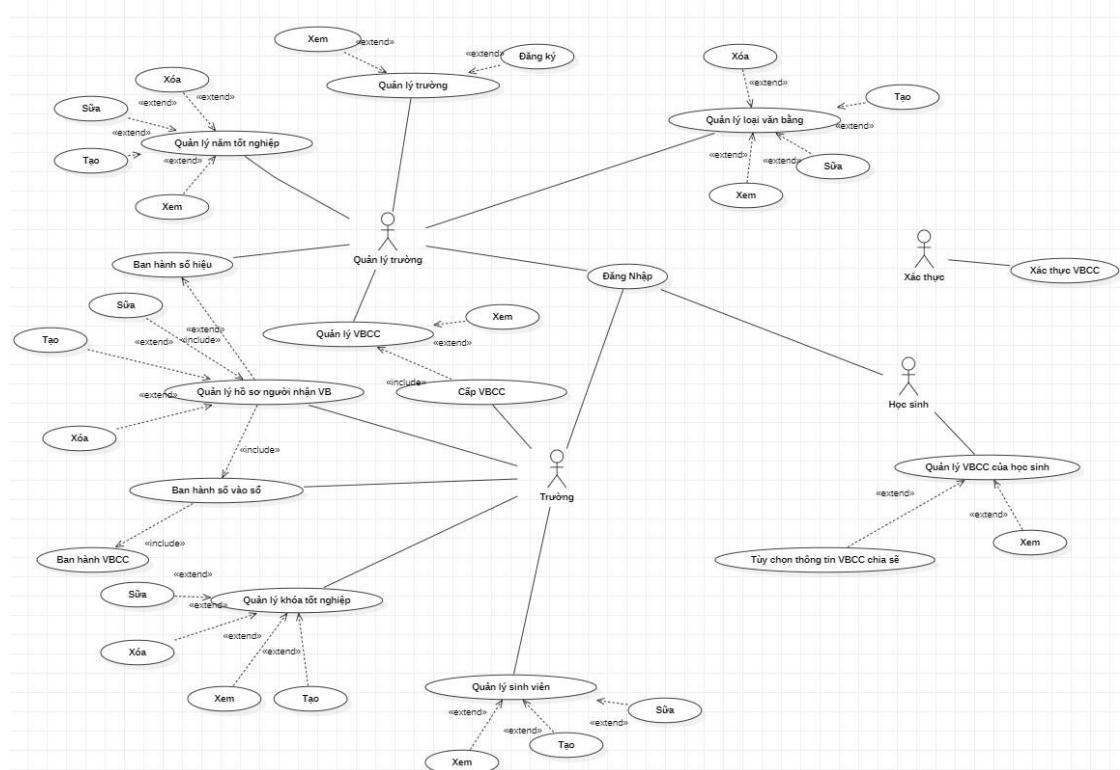
Bước 8. Băm dữ liệu cần xác minh

Bước 9. Thực hiện quy trình xác minh dữ liệu dựa vào mã hóa dữ liệu cần xác minh và proof được người dùng đưa

Bước 10. Thông báo kết quả thành công hoặc thất bại

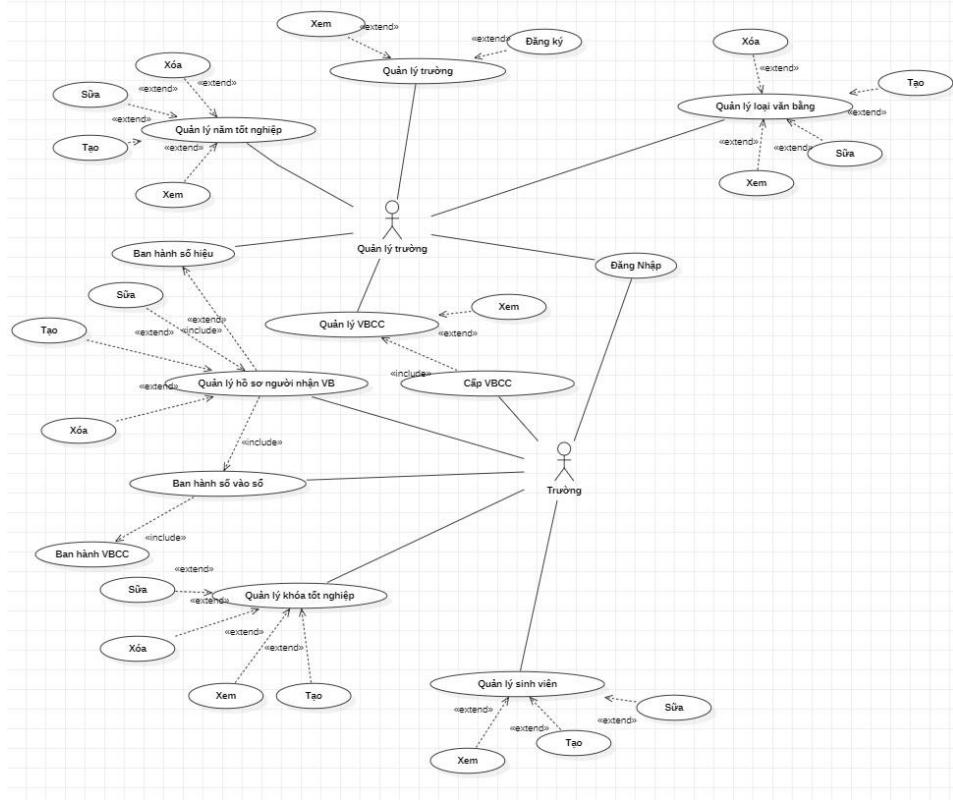
3.6 Usecase

3.6.1 Tổng quát use case



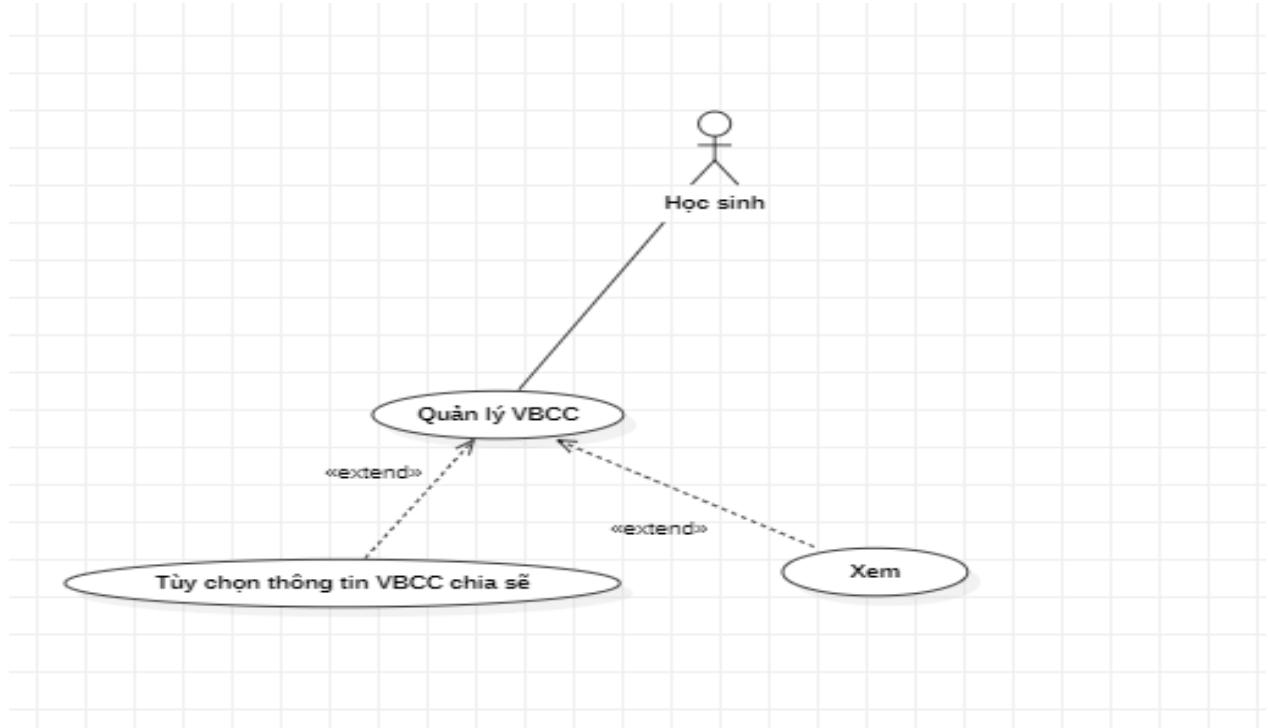
Hình 3.6 Tổng quát usecase

3.6.2 Trường và sở giáo dục



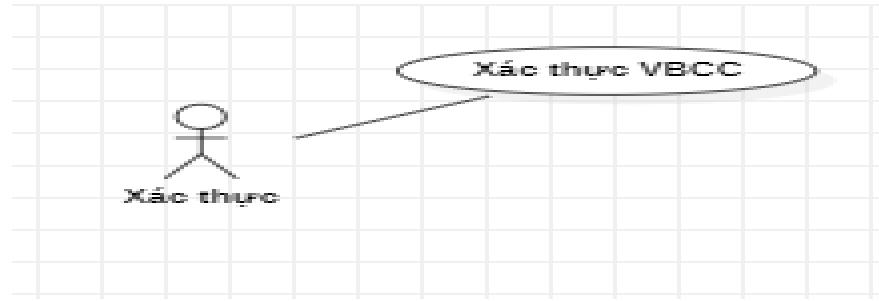
Hình 3.7 Usecase Trường và Sở giáo dục

3.6.3 Sinh viên



Hình 3.8 Usecase sinh viên

- Người xác thực



Hình 3.9 Usecase người xác thực

Bảng 3.1 Các tác nhân

#	Tên Actor	Mô tả
1	Sở giáo dục	Đơn vị quản lý trường đại học và ban hành quyết định cấp phát văn bằng chứng chỉ cho Sinh viên
2	Sinh viên	Sinh viên người đang học ở trường và nhận văn bằng chứng chỉ
3	Trường	Đơn vị dưới sự quản lý của trường và cấp phát văn bằng chứng chỉ cho sinh viên
4	Xác Thực	Đơn vị xác thực văn bằng chứng chỉ

Bảng 3.2 Danh sách Usecase

#	Code	Name	Brief Description
1	UC01	Đăng nhập	Cho phép actor đăng nhập vào hệ thống
2	UC02	Đăng xuất	Cho phép actor đăng xuất khỏi hệ thống
3	UC03	Quản lý trường	Cho phép actor quản lý các trường có trong hệ thống
4	UC04	Xem trường	Cho phép actor xem trường có trong hệ thống
5	UC05	Đăng ký trường	Cho phép actor đăng ký trường có trong hệ thống
6	UC06	Quản lý năm tốt nghiệp	Cho phép actor quản lý năm tốt nghiệp của VBCC khi được phát hành
7	UC07	Tạo năm tốt nghiệp	Cho phép actor tạo năm tốt nghiệp
8	UC08	Sửa năm tốt nghiệp	Cho phép actor sửa năm tốt nghiệp
9	UC09	Xóa năm tốt nghiệp	Cho phép actor xóa năm tốt nghiệp
10	UC10	Xem năm tốt nghiệp	Cho phép actor xem năm tốt nghiệp
11	UC11	Quản lý hồ sơ người nhận VB	Cho phép actor quản lý hồ sơ

			người nhận VBCC
12	UC12	Ban hành số hiệu	Cho phép actor ban hành số hiệu vào hồ sơ người nhận
13	UC13	Ban hành số vào sổ	Cho phép actor ban hành số vào sổ vào hồ sơ người nhận bắt buộc trước đó đã có số hiệu
14	UC14	Tạo danh sách hồ sơ người nhận VB	Cho phép actor tạo danh sách hồ sơ người nhận
15	UC15	Sửa hồ sơ người nhận VBCC	Cho phép actor sửa hồ sơ người nhận VBCC
16	UC16	Xóa hồ sơ người nhận VBCC	Cho phép actor xóa hồ sơ người nhận
17	UC17	Xem hồ sơ người nhận	Cho phép actor xem 1 hồ sơ người nhận VBCC
18	UC18	Quản lý loại VBCC	Cho phép actor quản lý các loại VBCC trong VBCC
19	UC19	Thêm loại VBCC	Cho phép actor thêm loại VBCC
20	UC20	Sửa loại VBCC	Cho phép actor sửa loại VBCC
21	UC21	Xóa loại VBCC	Cho phép actor xóa loại VBCC
22	UC22	Xem loại VBCC	Cho phép actor xem loại VBCC
23	UC23	Quản lý khóa tốt nghiệp	Cho phép actor quản lý khóa tốt nghiệp của sinh viên trong VBCC
24	UC24	Thêm khóa tốt nghiệp	Cho phép actor thêm khóa tốt nghiệp
25	UC25	Sửa khóa tốt nghiệp	Cho phép actor sửa khóa tốt nghiệp
26	UC26	Xóa khóa tốt nghiệp	Cho phép actor xóa khóa tốt nghiệp
27	UC27	Xem khóa tốt nghiệp	Cho phép actor xem khóa tốt nghiệp
28	UC28	Quản lý sinh viên	Cho phép actor quản lý sinh viên đang và đã học tại trường
29	UC29	Tạo danh sách sinh viên	Cho phép actor tạo danh sách Sinh viên
30	UC30	Sửa thông tin sinh viên	Cho phép actor sửa sinh viên
31	UC31	Xóa sinh viên	Cho phép actor xóa thông tin sinh viên
32	UC32	Xem thông tin sinh viên	Cho phép actor xem sinh viên
33	UC33	Quản lý VBCC	Cho phép actor quản lý VBCC của actor đã được nhận từ phía trường cấp phát
34	UC34	Cấp VBCC	Cho phép actor cấp VBCC
35	UC35	Xem VBCC	Cho phép actor xem VBCC
36	UC36	Quản lý VBCC của riêng sinh	Cho phép actor quản lý VBCC

		viên	của riêng mình
37	UC37	Tùy chọn thông tin VBCC	Cho phép actor chia sẻ thông tin VBCC của bản thân và mã QR code xác thực bằng
38	UC38	Xem VBCC	Cho phép actor xem chi tiết VBCC
39	UC39	Xác thực VBCC	Cho phép actor xác thực văn bằng chứng chỉ từ thông tin VBCC và mã QR Code

3.6.4 USE CASE 01. ĐĂNG NHẬP

Bảng 3.3 USE CASE 01. ĐĂNG NHẬP

Name	Đăng Nhập	Code	UC02
Description	Người dùng đăng nhập hệ thống Blockchain		
Actor	Trường, Sinh viên, Sở giáo dục	Trigger	Trong trang chủ xác thực VBCC chọn nút đăng nhập
Pre-condition	Người dùng chưa đăng nhập tài khoản		
Post-condition	Người dùng đã đăng nhập thành công và truy cập vào hệ thống.		
Error situations	<ul style="list-style-type: none"> – Người dùng nhập sai thông tin tài khoản hoặc mật khẩu. – Hệ thống gặp lỗi kết nối hoặc lỗi phần mềm. – Lỗi trong quá trình xử lý thông tin đăng nhập. – Lỗi trong quá trình xác thực thông tin trên Blockchain. 		
System state in error situations	<ul style="list-style-type: none"> – Trong trường hợp người dùng nhập sai thông tin tài khoản hoặc mật khẩu, hệ thống sẽ yêu cầu người dùng nhập lại thông tin tài khoản hoặc mật khẩu. – Trong trường hợp hệ thống gặp lỗi kết nối hoặc lỗi phần mềm, hệ thống sẽ hiển thị thông báo lỗi và yêu cầu người dùng thử lại sau. – Trong trường hợp xảy ra lỗi trong quá trình xử lý thông tin đăng nhập, hệ thống sẽ hiển thị thông báo lỗi và yêu cầu người dùng thử lại sau. – Trong trường hợp xảy ra lỗi trong quá trình xác thực thông tin trên Blockchain, hệ thống sẽ hiển thị thông báo lỗi và yêu cầu người dùng thử lại sau. 		

Standard flow/process	<ul style="list-style-type: none"> - Người dùng truy cập vào trang đăng nhập của hệ thống. - Người dùng nhập thông tin tài khoản và mật khẩu. - Hệ thống kiểm tra thông tin đăng nhập của người dùng. - Hệ thống sử dụng thông tin tài khoản để xác thực trên Blockchain. - Nếu thông tin đăng nhập và xác thực chính xác, hệ thống cho phép người dùng truy cập vào hệ thống. - Nếu thông tin đăng nhập hoặc xác thực không chính xác, hệ thống yêu cầu người dùng nhập lại thông tin đăng nhập hoặc xác thực trên Blockchain.
Alternative Flow 1 Người dùng truy cập vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống không thể kết nối với cơ sở dữ liệu. 2. Hệ thống hiển thị thông báo lỗi kết nối và yêu cầu người dùng thử lại sau.
Alternative Flow 2 Người dùng truy cập vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống xử lý thông tin đăng nhập bị lỗi 2. Hệ thống hiển thị thông báo lỗi xử lý và yêu cầu người dùng thử lại sau.

3.6.5 USE CASE 02. Đăng Xuất

Bảng 3.4 USE CASE 02. Đăng Xuất

Name	Đăng Xuất	Code	UC02
Description	Đăng xuất tài khoản		
Actor	Trường, Sinh viên, Sở giáo dục	Trigger	Trong trang chủ người dùng chọn nút đăng xuất
Pre-condition	Người dùng chọn chức năng "Đăng xuất" trên giao diện của hệ thống.		
Post-condition	Người dùng đã được đăng xuất khỏi hệ thống và không thể truy cập vào các tính năng của hệ thống.		
Error situations	<ul style="list-style-type: none"> - Không thể kết nối đến Blockchain để xác nhận quá trình đăng xuất. - Lỗi hệ thống khi thực hiện quá trình đăng xuất. 		
System state in error situations	<ul style="list-style-type: none"> - Hệ thống sẽ hiển thị thông báo lỗi cho người dùng. - Người dùng sẽ không được đăng xuất và vẫn có thể truy cập vào các tính năng của hệ thống. 		

Standard flow/process	<ol style="list-style-type: none"> Người dùng chọn chức năng "Đăng xuất" trên giao diện của hệ thống. Hệ thống hiển thị thông báo xác nhận đăng xuất và yêu cầu người dùng xác nhận. Người dùng xác nhận yêu cầu đăng xuất. Hệ thống gửi yêu cầu đăng xuất đến Blockchain và cơ sở dữ liệu để xác nhận. Blockchain xác nhận quá trình đăng xuất và trả về kết quả cho hệ thống. Hệ thống đăng xuất người dùng và hiển thị thông báo thành công.
Alternative Flow 1 Người dùng đăng xuất hệ thống.	<ol style="list-style-type: none"> Người dùng không chọn chức năng "Đăng xuất" trên giao diện của hệ thống. Use case kết thúc
Alternative Flow 2 Người dùng đăng xuất hệ thống.	<ol style="list-style-type: none"> Hệ thống gửi yêu cầu đăng xuất đến Blockchain để xác nhận. Không thể kết nối đến Blockchain hoặc cơ sở dữ liệu để xác nhận quá trình đăng xuất. Hệ thống hiển thị thông báo lỗi cho người dùng. Người dùng không được đăng xuất và vẫn có thể truy cập vào các tính năng của hệ thống. Use case kết thúc.

3.6.6 USE CASE 04. Xem trường

Bảng 3.5 USE CASE 04. Xem trường

Name	Xem trường	Code	UC04
Description	xem thông tin về một trường học trong hệ thống		
Actor	Sở giáo dục	Trigger	Người dùng chọn chức năng "Xem trường" trên giao diện của hệ thống.
Pre-condition	Người dùng đã đăng nhập thành công vào hệ thống.		
Post-condition	Người dùng đã xem được thông tin về trường học trong hệ thống.		
Error situations	<ul style="list-style-type: none"> Không thể kết nối đến Blockchain hoặc cơ sở dữ liệu để lấy thông tin về trường học. Trường học không tồn tại trong hệ thống. 		
System state in error situations	<ul style="list-style-type: none"> Hệ thống sẽ hiển thị thông báo lỗi cho người 		

	<p>dùng.</p> <ul style="list-style-type: none"> – Người dùng sẽ không xem được thông tin về trường học.
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng "Xem trường" trên giao diện của hệ thống. 2. Hệ thống hiển thị form tìm kiếm trường học cho người dùng nhập thông tin. 3. Người dùng nhập thông tin tìm kiếm (tên trường hoặc mã số trường). 4. Hệ thống gửi yêu cầu tìm kiếm đến Blockchain và cơ sở dữ liệu để lấy thông tin về trường học. 5. Blockchain và cơ sở dữ liệu trả về thông tin về trường học cho hệ thống. 6. Hệ thống hiển thị thông tin về trường học cho người dùng.
Alternative Flow 1	<ol style="list-style-type: none"> 1. Hệ thống không tìm thấy thông tin về trường học trong Blockchain. 2. Hệ thống hiển thị thông báo cho người dùng biết trường học không tồn tại trong hệ thống. 3. Quay lại bước 2 trong standard flow.

3.6.7 USE CASE 05. Đăng ký trường

Bảng 3.6 USE CASE 05. Đăng ký trường

Name	Đăng ký trường		Code	UC05
Description	Đăng ký trường học mới trong hệ thống			
Actor	Sở Giáo Dục	Trigger	Người dùng chọn chức năng "Đăng ký trường" trên giao diện của hệ thống.	
Pre-condition	Người dùng đã đăng nhập thành công vào hệ thống.			
Post-condition	Hệ thống đã lưu thông tin về trường học mới trong Blockchain.			
Error situations	<ul style="list-style-type: none"> – Không thể kết nối đến Blockchain để lưu thông tin về trường học mới. – Thông tin về trường học đã tồn tại trong hệ thống. 			
System state in error situations	<ul style="list-style-type: none"> – Hệ thống sẽ hiển thị thông báo lỗi cho người dùng. – Người dùng sẽ không thực hiện được đăng ký trường học mới. 			

Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng "Đăng ký trường" trên giao diện của hệ thống. 2. Hệ thống hiển thị form nhập thông tin về trường học mới. 3. Người dùng nhập thông tin về trường học mới (tên trường, địa chỉ, số điện thoại, email, mã số trường, thông tin người đại diện trường,...). 4. Hệ thống kiểm tra xem thông tin vừa nhập có hợp lệ hay không (trường hợp thông tin bị trùng lặp với trường học đã có trong hệ thống). 5. Hệ thống lưu thông tin về trường học mới vào Blockchain. 6. Hệ thống hiển thị thông báo thành công cho người dùng và chuyển về trang chủ của hệ thống.
Alternative Flow 1 Người dùng không nhập đầy đủ thông tin yêu cầu	<ol style="list-style-type: none"> 1. Người dùng không nhập đầy đủ thông tin yêu cầu. 2. Hệ thống không thực hiện lưu thông tin và hiển thị thông báo yêu cầu nhập đầy đủ thông tin. 3. Quay lại bước 2 trong standard flow.
Alternative Flow 2 Thông tin về trường học đã tồn tại trong hệ thống	<ol style="list-style-type: none"> 1. Hệ thống kiểm tra xem thông tin vừa nhập có trùng lặp với trường học đã có trong hệ thống hay không. 2. Hệ thống hiển thị thông báo cho người dùng biết thông tin về trường học đã tồn tại trong hệ thống. 3. Quay lại bước 2 trong standard flow.

3.6.8 USE CASE 06.Quản lý năm tốt nghiệp

Bảng 3.7 USE CASE 06.Quản lý năm tốt nghiệp

Name	Quản lý năm tốt nghiệp	Code	UC06
Description	Quản lý năm tốt nghiệp của sinh viên trong hệ thống có tích hợp Blockchain.		
Actor	Sở giáo dục	Trigger	Người dùng chọn chức năng thêm hoặc sửa hoặc xóa hoặc xem trên giao diện của hệ thống.
Pre-condition	Người dùng đã đăng nhập vào hệ thống và có quyền truy cập vào chức năng quản lý năm tốt nghiệp.		
Post-condition	Thông tin năm tốt nghiệp được thêm, xóa, sửa hoặc xem trên hệ thống		
Error situations	<ul style="list-style-type: none"> - Người dùng không đăng nhập được vào hệ thống. - Người dùng không có quyền truy cập vào chức năng quản lý năm tốt nghiệp. - Không thể thêm, xóa, sửa hoặc xem thông tin năm tốt nghiệp trên hệ thống. 		
System state in error situations	<ul style="list-style-type: none"> - Hệ thống yêu cầu người dùng đăng nhập hoặc đăng nhập lại. - Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng quản lý năm tốt nghiệp. - Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 		
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý năm tốt nghiệp trên hệ thống. 2. Hệ thống hiển thị danh sách thông tin năm tốt nghiệp hiện có của người dùng. 3. Người dùng chọn thêm, xóa, sửa hoặc xem thông tin năm tốt nghiệp. 4. Nếu người dùng chọn thêm, hệ thống yêu cầu người dùng nhập thông tin năm tốt nghiệp mới. 5. Nếu người dùng chọn xóa hoặc sửa, hệ thống yêu cầu người dùng chọn thông tin năm tốt nghiệp muốn xóa hoặc sửa. 6. Nếu người dùng chọn xem, hệ thống hiển thị chi 		

	<p>tiết thông tin năm tốt nghiệp.</p> <ol style="list-style-type: none"> 7. Người dùng xác nhận thực hiện thao tác. 8. Hệ thống lưu trữ thông tin được thêm, xóa, sửa hoặc hiển thị thông tin năm tốt nghiệp
Alternative Flow 1 Người dùng không đăng nhập được vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng đăng nhập lại. 2. Quay trở lại bước 1 của Standard flow.
Alternative Flow 2 Người dùng không có quyền truy cập vào chức năng quản lý năm tốt nghiệp.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng này. 2. Quay trở lại bước 1 của Standard flow.
Alternative Flow 3 Không thể thêm, xóa, sửa hoặc xem thông tin năm tốt nghiệp trên hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 2. Quay trở lại bước 3 của Standard flow.
Alternative Flow 4 Không thể lưu trữ thông tin trên cơ sở dữ liệu.	<ol style="list-style-type: none"> 1. Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 2. Quay trở lại bước 7 của Standard flow.

3.6.9 USE CASE 11. Quản lý hồ sơ người nhận VBCC

Bảng 3.8 Quản lý hồ sơ người nhận VBCC

Name	Quản lý hồ sơ người nhận VBCC	Code	UC011
Description	Quản lý hồ sơ người nhận văn bằng chứng chỉ		
Actor	Sở giáo dục, Trường	Trigger	Người dùng chọn chức năng thêm hoặc sửa hoặc xóa hoặc xem trên giao diện của hệ thống.
Pre-condition	Người dùng đã đăng nhập vào hệ thống và có quyền truy cập vào chức năng quản lý năm tốt nghiệp.		
Post-condition	Thông tin người nhận văn bằng được thêm, xóa, sửa hoặc xem trên hệ thống		

Error situations	<ul style="list-style-type: none"> – Không thể kết nối với mạng Blockchain. – Người dùng không có quyền truy cập vào hồ sơ.
System state in error situations	<ul style="list-style-type: none"> – Người dùng không đăng nhập được vào hệ thống. – Người dùng không có quyền truy cập vào chức năng quản lý hồ sơ người nhận – Không thể thêm, xóa, sửa hoặc xem thông tin hồ sơ người nhận trên hệ thống.
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý hồ sơ người nhận VB trên hệ thống. 2. Hệ thống hiển thị danh sách thông tin người nhận VBCC hiện có của người dùng. 3. Người dùng chọn thêm, xóa, sửa hoặc xem thông tin người nhận VBCC 4. Nếu người dùng chọn thêm, hệ thống yêu cầu người dùng nhập thông tin người nhận VBCC 5. Nếu người dùng chọn xóa hoặc sửa, hệ thống yêu cầu người dùng chọn thông tin năm tốt nghiệp muốn xóa hoặc sửa. 6. Nếu người dùng chọn xem, hệ thống hiển thị chi tiết thông tin người nhận VB 7. Người dùng xác nhận thực hiện thao tác. 8. Hệ thống lưu trữ thông tin được thêm, xóa, sửa hoặc hiển thị thông tin người nhận VB
Alternative Flow 1 Người dùng không đăng nhập được vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng đăng nhập lại. 2. Quay trở lại bước 1 của Standard flow.
Alternative Flow 2 Người dùng không có quyền truy cập vào chức năng quản lý hồ sơ người nhận VB	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng này. 2. Quay trở lại bước 1 của Standard flow.
Alternative Flow 3 Không thể thêm, xóa, sửa hoặc xem thông tin hồ sơ người nhận VB trên hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 2. Quay trở lại bước 3 của Standard flow.

3.6.10 USE CASE 12. Ban hành số hiệu

Bảng 3.9 USE CASE 12. Ban hành số hiệu

Name	Ban hành số hiệu	Code	UC12
Description	Ban hành số hiệu cho hồ sơ người nhận VBCC		
Actor	Sở giáo dục	Trigger	Chọn excel và nhập hồ sơ người nhận kèm thông tin số hiệu
Pre-condition	Người dùng đã truy cập hệ thống và có quyền truy cập		
Post-condition	Thông tin hồ sơ người nhận VB được cập nhật số hiệu		
Error situations	<ul style="list-style-type: none"> - Không thể cập nhật số hiệu - Hồ sơ người nhận không tồn tại 		
System state in error situations	<ul style="list-style-type: none"> - Người dùng không đăng nhập được vào hệ thống. - Người dùng không có quyền truy cập vào chức năng quản lý hồ sơ người nhận - Không thể cập nhật số hiệu thông tin hồ sơ người nhận trên hệ thống. 		
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý hồ sơ người nhận VB trên hệ thống. 2. Hệ thống hiển thị danh sách thông tin người nhận VBCC hiện có của người dùng. 3. Người dùng chọn cập nhật số hiệu 4. Người dùng xác nhận thực hiện thao tác. 5. Hệ thống lưu trữ thông tin, hiển thị thông tin người nhận VB 		
Alternative Flow 1 Người dùng không đăng nhập được vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng đăng nhập lại. 2. Quay trở lại bước 1 của Standard flow. 		
Alternative Flow 2 Người dùng không có quyền truy cập vào chức năng quản lý hồ sơ người nhận VB	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng này. 2. Quay trở lại bước 1 của Standard flow. 		
Alternative Flow 3 Không thể cập số hiệu hồ sơ người nhận VB trên hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 2. Quay trở lại bước 3 của Standard flow. 		

3.6.11 USE CASE 13. Ban hành số vào sổ

Bảng 3.10 USE CASE 13. Ban hành số vào sổ

Name	Ban hành số vào sổ	Code	UC13
Description	Ban hành số vào sổ cho hồ sơ người nhận VBCC		
Actor	Trường	Trigger	Chọn nút cập nhật số vào sổ và excel nhập hồ sơ người nhận kèm thông tin số vào sổ
Pre-condition	Người dùng đã truy cập hệ thống và có quyền truy cập		
Post-condition	Thông tin hồ sơ người nhận VB được cập nhật số vào sổ		
Error situations	<ul style="list-style-type: none"> - Không thể cập nhật vào sổ - Hồ sơ người nhận không tồn tại 		
System state in error situations	<ul style="list-style-type: none"> - Người dùng không đăng nhập được vào hệ thống. - Người dùng không có quyền truy cập vào chức năng quản lý hồ sơ người nhận - Không thể cập nhật số vào sổ hồ sơ người nhận trên hệ thống. 		
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý hồ sơ người nhận VB trên hệ thống. 2. Hệ thống hiển thị danh sách thông tin người nhận VBCC hiện có của người dùng. 3. Người dùng chọn cập nhật số vào sổ 4. Người dùng xác nhận thực hiện thao tác. 5. Hệ thống lưu trữ thông tin, hiển thị thông tin người nhận VB 		
Alternative Flow 1 Người dùng không đăng nhập được vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng đăng nhập lại. 2. Quay trở lại bước 1 của Standard flow. 		
Alternative Flow 2 Người dùng không có quyền truy cập vào chức năng quản lý hồ sơ người nhận VB	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng này. 2. Quay trở lại bước 1 của Standard flow. 		
Alternative Flow 3 Không thể cập nhật số vào sổ hồ sơ người nhận VB trên hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 2. Quay trở lại bước 3 của Standard flow. 		

3.6.12 USE CASE 10. Quản lý năm tốt nghiệp

Bảng 3.11 USE CASE 10. Quản lý năm tốt nghiệp

Name	Quản lý năm tốt nghiệp	Code	UC06
Description	Quản lý năm tốt nghiệp của sinh viên trong hệ thống có tích hợp Blockchain.		
Actor	Sở giáo dục	Trigger	Người dùng chọn chức năng thêm hoặc sửa hoặc xóa hoặc xem trên giao diện của hệ thống.
Pre-condition	Người dùng đã đăng nhập vào hệ thống và có quyền truy cập vào chức năng quản lý năm tốt nghiệp.		
Post-condition	Thông tin năm tốt nghiệp được thêm, xóa, sửa hoặc xem trên hệ thống		
Error situations	<ul style="list-style-type: none"> – Người dùng không đăng nhập được vào hệ thống. – Người dùng không có quyền truy cập vào chức năng quản lý năm tốt nghiệp. – Không thể thêm, xóa, sửa hoặc xem thông tin năm tốt nghiệp trên hệ thống. 		
System state in error situations	<ul style="list-style-type: none"> – Hệ thống yêu cầu người dùng đăng nhập hoặc đăng nhập lại. – Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng quản lý năm tốt nghiệp. – Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 		
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý năm tốt nghiệp trên hệ thống. 2. Hệ thống hiển thị danh sách thông tin năm tốt nghiệp hiện có của người dùng. 3. Người dùng chọn thêm, xóa, sửa hoặc xem thông tin năm tốt nghiệp. 4. Nếu người dùng chọn thêm, hệ thống yêu cầu người dùng nhập thông tin năm tốt nghiệp mới. 5. Nếu người dùng chọn xóa hoặc sửa, hệ thống yêu cầu người dùng chọn thông tin năm tốt nghiệp muốn xóa hoặc sửa. 6. Nếu người dùng chọn xem, hệ thống hiển thị 		

	<p>chi tiết thông tin năm tốt nghiệp.</p> <ol style="list-style-type: none"> 7. Người dùng xác nhận thực hiện thao tác. 8. Hệ thống lưu trữ thông tin được thêm, xóa, sửa hoặc hiển thị thông tin năm tốt nghiệp
Alternative Flow 1 Người dùng không đăng nhập được vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng đăng nhập lại. 2. Quay trở lại bước 1 của Standard flow.
Alternative Flow 2 Người dùng không có quyền truy cập vào chức năng quản lý năm tốt nghiệp.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng này. 2. Quay trở lại bước 1 của Standard flow.

3.6.13 USE CASE 18. Quản lý loại VBCC

Bảng 3.12 USE CASE 18. Quản lý loại VBCC

Name	Quản lý loại VBCC	Code	UC18
Description	Quản lý loại Văn bằng chứng chỉ để cập nhật thông tin, thêm, sửa, xóa, xem thông tin loại văn bằng chứng chỉ.		
Actor	Sở giáo dục	Trigger	Người dùng chọn chức năng thêm hoặc sửa hoặc xóa hoặc xem trên giao diện của hệ thống.
Pre-condition	Đã truy cập vào hệ thống và có quyền quản lý		
Post-condition	<ul style="list-style-type: none"> – Thông tin loại VBCC được thêm, xóa, sửa hoặc xem trên hệ thống 		
Error situations	<ul style="list-style-type: none"> – Người dùng không đăng nhập được vào hệ thống. – Người dùng không có quyền truy cập vào chức năng quản lý loại VBCC. – Không thể thêm, xóa, sửa hoặc xem thông tin loại VBCC trên hệ thống. 		
System state in error situations	<ul style="list-style-type: none"> – Hệ thống yêu cầu người dùng đăng nhập hoặc đăng nhập lại. – Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng quản lý loại VBCC – Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 		

Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý trên VBCC hệ thống. 2. Hệ thống hiển thị danh sách thông tin loại VBCC hiện có của người dùng. 3. Người dùng chọn thêm, xóa, sửa hoặc xem thông tin loại VBCC 4. Nếu người dùng chọn thêm, hệ thống yêu cầu người dùng nhập thông tin loại VBCC. 5. Nếu người dùng chọn xóa hoặc sửa, hệ thống yêu cầu người dùng chọn thông tin loại VBCC muốn xóa hoặc sửa. 6. Nếu người dùng chọn xem, hệ thống hiển thị chi tiết thông tin loại VBCC 7. Người dùng xác nhận thực hiện thao tác. 8. Hệ thống lưu trữ thông tin được thêm, xóa, sửa hoặc hiển thị thông tin loại VBCC.
Alternative Flow 1 Người dùng không đăng nhập được vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng đăng nhập lại. 2. Quay trở lại bước 1 của Standard flow.
Alternative Flow 2 Người dùng không có quyền truy cập vào chức năng quản lý loại VBCC	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng này. 2. Quay trở lại bước 1 của Standard flow.
Alternative Flow 3 Không thể thêm, xóa, sửa hoặc xem thông tin loại VBCC trên hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 2. Quay trở lại bước 3 của Standard flow.

3.6.14 USE CASE 23. Quản lý khóa tốt nghiệp

Bảng 3.13 USE CASE 23. Quản lý khóa tốt nghiệp

Name	Quản lý khóa tốt nghiệp	Code	UC23
Description	Quản lý khóa tốt nghiệp để cập nhật thông tin, thêm, sửa, xóa, xem thông tin khóa tốt nghiệp.		
Actor	Trường	Trigger	Người dùng chọn chức năng thêm hoặc sửa hoặc xóa hoặc xem trên giao diện của hệ thống.
Pre-condition	Đã truy cập vào hệ thống và có quyền quản lý		
Post-condition	<ul style="list-style-type: none"> – Thông tin khóa tốt nghiệp được thêm, xóa, sửa hoặc xem trên hệ thống 		
Error situations	<ul style="list-style-type: none"> – Người dùng không đăng nhập được vào hệ thống. – Người dùng không có quyền truy cập vào chức năng quản lý khóa tốt nghiệp – Không thể thêm, xóa, sửa hoặc xem thông tin khóa tốt nghiệp. 		
System state in error situations	<ul style="list-style-type: none"> – Hệ thống yêu cầu người dùng đăng nhập hoặc đăng nhập lại. – Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng quản lý khóa tốt nghiệp – Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 		
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý khóa tốt nghiệp trên hệ thống. 2. Hệ thống hiển thị danh sách thông tin khóa tốt nghiệp hiện có của người dùng. 3. Người dùng chọn thêm, xóa, sửa hoặc xem thông tin khóa tốt nghiệp 4. Nếu người dùng chọn thêm, hệ thống yêu cầu người dùng nhập thông tin khóa tốt nghiệp. 5. Nếu người dùng chọn xóa hoặc sửa, hệ thống yêu cầu người dùng chọn thông tin khóa tốt nghiệp muốn xóa hoặc sửa. 6. Nếu người dùng chọn xem, hệ thống hiển thị chi tiết thông tin khóa tốt nghiệp 		

	<p>7. Người dùng xác nhận thực hiện thao tác.</p> <p>8. Hệ thống lưu trữ thông tin được thêm, xóa, sửa hoặc hiển thị thông tin khóa tốt nghiệp</p>
Alternative Flow 1 Người dùng không đăng nhập được vào hệ thống.	<p>1. Hệ thống yêu cầu người dùng đăng nhập lại.</p> <p>2. Quay trở lại bước 1 của Standard flow.</p>
Alternative Flow 2 Người dùng không có quyền truy cập vào chức năng quản lý khóa tốt nghiệp	<p>1. Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng này.</p> <p>2. Quay trở lại bước 1 của Standard flow.</p>
Alternative Flow 3 Không thể thêm, xóa, sửa hoặc xem thông tin khóa tốt nghiệp trên hệ thống.	<p>1. Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác.</p> <p>2. Quay trở lại bước 3 của Standard flow.</p>

3.6.15 USE CASE 28. Quản lý sinh viên

Bảng 3.14 USE CASE 28. Quản lý Sinh viên

Name	Quản lý sinh viên	Code	UC028
Description	Quản lý sinh viên để cập nhật thông tin, thêm, sửa, xóa, xem thông tin sinh viên		
Actor	Trường	Trigger	Người dùng chọn chức năng thêm hoặc sửa hoặc xóa hoặc xem trên giao diện của hệ thống.
Pre-condition	Đã truy cập vào hệ thống và có quyền quản lý		
Post-condition	<ul style="list-style-type: none"> – Thông tin sinh viên được thêm, xóa, sửa hoặc xem trên hệ thống 		
Error situations	<ul style="list-style-type: none"> – Người dùng không đăng nhập được vào hệ thống. – Người dùng không có quyền truy cập vào chức năng quản lý sinh viên – Không thể thêm, xóa, sửa hoặc xem thông tin sinh viên. 		

System state in error situations	<ul style="list-style-type: none"> - Hệ thống yêu cầu người dùng đăng nhập hoặc đăng nhập lại. - Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng quản lý sinh viên - Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác.
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý sinh viên trên hệ thống. 2. Hệ thống hiển thị danh sách thông tin sinh viên hiện có của người dùng. 3. Người dùng chọn thêm, xóa, sửa hoặc xem thông tin sinh viên 4. Nếu người dùng chọn thêm, hệ thống yêu cầu người dùng nhập thông tin sinh viên. 5. Nếu người dùng chọn xóa hoặc sửa, hệ thống yêu cầu người dùng chọn thông tin sinh viên xóa hoặc sửa. 6. Nếu người dùng chọn xem, hệ thống hiển thị chi tiết thông tin sinh viên 7. Người dùng xác nhận thực hiện thao tác. 8. Hệ thống lưu trữ thông tin được thêm, xóa, sửa hoặc hiển thị thông tin sinh viên
Alternative Flow 1 Người dùng không đăng nhập được vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng đăng nhập lại. 2. Quay trở lại bước 1 của Standard flow.
Alternative Flow 2 Người dùng không có quyền truy cập vào chức năng quản lý sinh viên	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng này. 2. Quay trở lại bước 1 của Standard flow.

3.6.16 USE CASE 33. Quản lý VBCC

Bảng 3.15 USE CASE 33. Quản lý VBCC

Name	Quản lý VBCC	Code	UC33
Description	Quản lý VBCC có thể xem thông tin chi tiết hoặc một vài chức năng tiện lợi tìm kiếm, tạo		
Actor	Trường	Trigger	Người dùng chọn chức năng xem chi tiết hoặc tìm kiếm, tạo

Pre-condition	Đã truy cập vào hệ thống và có quyền quản lý
Post-condition	<ul style="list-style-type: none"> - Thông tin VBCC xem trên hệ thống
Error situations	<ul style="list-style-type: none"> - Người dùng không đăng nhập được vào hệ thống. - Người dùng không có quyền truy cập vào chức năng quản lý VBCC - Không thể xem thông tin VBCC - Không đủ quyền xem VBCC
System state in error situations	<ul style="list-style-type: none"> - Hệ thống yêu cầu người dùng đăng nhập hoặc đăng nhập lại. - Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng quản lý VBCC - Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác.
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý VBCC trên hệ thống. 2. Hệ thống hiển thị danh sách thông tin VBCC hiện có của người dùng. 3. Người dùng chọn xem thông tin VBCC hoặc tìm kiếm 4. Nếu người dùng chọn xem, tạo, hệ thống lưu hoặc hiển thị chi tiết thông tin VBCC 5. Người dùng xác nhận thực hiện thao tác. 6. Hệ thống hiển thị thông tin VBCC
Alternative Flow 1 Người dùng không đăng nhập được vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng đăng nhập lại. 2. Quay trở lại bước 1 của Standard flow.
Alternative Flow 2 Người dùng không có quyền truy cập vào chức năng quản lý VBCC	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng này. 2. Quay trở lại bước 1 của Standard flow.

3.6.17 USE CASE 34. Cấp VBCC

Bảng 3.16 USE CASE 34. Cấp VBCC

Name	Cấp VBCC	Code	UC34
Description	Trường cấp VBCC từ hồ sơ người nhận VBCC trên hệ thống		
Actor	Trường	Trigger	Người dùng chọn chức năng cấp VBCC
Pre-condition	Sinh viên đã hoàn thành tất cả các yêu cầu cần thiết cho văn		

	bằng hoặc chứng chỉ.
Post-condition	Sinh viên nhận được văn bằng hoặc chứng chỉ đã được cấp.
Error situations	Hồ sơ người nhận không đủ điều kiện để cấp VBCC <ul style="list-style-type: none"> – Hồ sơ người nhận VB cung cấp thông tin không chính xác hoặc không đầy đủ. – Lỗi hệ thống khi xử lý yêu cầu cấp văn bằng chứng chỉ.
System state in error situations	<ul style="list-style-type: none"> – Nếu hồ sơ người nhận không đủ điều kiện để nhận văn bằng chứng chỉ, hệ thống sẽ thông báo lỗi và không cấp văn bằng. – Nếu hồ sơ người nhận sang cấp thông tin không chính xác hoặc không đầy đủ, hệ thống sẽ thông báo lỗi và yêu cầu cung cấp lại thông tin. – Nếu hệ thống gặp lỗi kỹ thuật, trạng thái hệ thống có thể bị treo, không thể xử lý yêu cầu cấp văn bằng chứng chỉ.
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng cấp quản lý hồ sơ người nhận 2. Hệ thống hiển thị danh sách thông tin hồ sơ người nhận VB hiện có của người dùng. 3. Người dùng chọn cấp phát bằng VBCC 4. Người dùng xác nhận thực hiện thao tác. 5. Hệ thống hiển thị thông tin VBCC
Alternative Flow 1 Sinh viên không đủ điều kiện để nhận văn bằng chứng chỉ.	<ol style="list-style-type: none"> 1. Trường kiểm tra và phát hiện rằng sinh viên không đủ điều kiện để nhận văn bằng chứng chỉ. 2. Trường thông báo cho sinh viên biết về việc không cấp văn bằng chứng chỉ và giải thích lý do. 3. Quá trình kết thúc.
Alternative Flow 2 Sinh viên cung cấp thông tin không chính xác.	<ol style="list-style-type: none"> 1. Trường kiểm tra và phát hiện thông tin cung cấp bởi sinh viên không chính xác hoặc không đầy đủ. 2. Trường thông báo cho sinh viên về lỗi và yêu cầu cung cấp lại thông tin chính xác và đầy đủ. 3. Quá trình tiếp tục từ bước 2 trong Standard flow.

3.6.18 USE CASE 36. Quản lý VBCC của riêng Sinh viên

Bảng 3.17 USE CASE 36. Quản lý VBCC của riêng Sinh viên

Name	Quản lý VBCC của riêng sinh viên	Code	UC36
Description	Quản lý VBCC của riêng sinh viên có thể xem thông tin chi tiết hoặc một vài chức năng tiện lợi tìm kiếm của VBCC thuộc mỗi sinh viên đó.		
Actor	Sinh viên	Trigger	Người dùng chọn chức năng xem chi tiết hoặc tìm kiếm, tạo
Pre-condition	Đã truy cập vào hệ thống và có quyền quản lý		
Post-condition	Thông tin VBCC xem trên hệ thống		
Error situations	<ul style="list-style-type: none"> – Người dùng không đăng nhập được vào hệ thống. – Người dùng không có quyền truy cập vào chức năng quản lý VBCC – Không thể xem thông tin VBCC – Không đủ quyền xem VBCC 		
System state in error situations	<ul style="list-style-type: none"> – Hệ thống yêu cầu người dùng đăng nhập hoặc đăng nhập lại. – Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng quản lý VBCC – Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 		
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý VBCC trên hệ thống. 2. Hệ thống hiển thị danh sách thông tin VBCC hiện có của người dùng. 3. Người dùng chọn xem thông tin VBCC hoặc tìm kiếm 4. Nếu người dùng chọn xem, hệ thống hiển thị chi tiết thông tin VBCC 5. Hệ thống hiển thị thông tin VBCC 		
Alternative Flow 1 Người dùng không đăng nhập được vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng đăng nhập lại. 2. Quay trở lại bước 1 của Standard flow. 		
Alternative Flow 2	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng có quyền truy 		

Người dùng không có quyền truy cập vào chức năng quản lý VBCC	cập vào chức năng này. 2. Quay trở lại bước 1 của Standard flow.
---	---

3.6.19 USE CASE 37. Tùy chọn thông tin VBCC

Bảng 3.18 USE CASE 37. Tùy chọn thông tin VBCC

Name	Tùy chọn thông tin VBCC	Code	UC37
Description	Tùy chọn thông tin VBCC người dùng có thể tùy chỉnh thông tin chia sẻ VBCC với bên thứ 3		
Actor	Sinh viên	Trigger	Người dùng chọn chức năng chia sẻ thông tin VBCC
Pre-condition	Đã truy cập vào hệ thống và có quyền quản lý		
Post-condition	Thông tin VBCC được chia sẻ		
Error situations	<ul style="list-style-type: none"> – Người dùng không đăng nhập được vào hệ thống. – Người dùng không có quyền truy cập vào chức năng quản lý VBCC – Không thể xem thông tin VBCC – Không đủ quyền xem VBC – Không thể chia sẻ thông tin VBCC 		
System state in error situations	<ul style="list-style-type: none"> – Hệ thống yêu cầu người dùng đăng nhập hoặc đăng nhập lại. – Hệ thống yêu cầu người dùng có quyền truy cập vào chức năng quản lý VBCC – Hệ thống thông báo lỗi và yêu cầu người dùng thực hiện lại thao tác. 		
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng chọn chức năng quản lý VBCC trên hệ thống. 2. Hệ thống hiển thị danh sách thông tin VBCC hiện có của người dùng. 3. Người dùng chọn thông tin chia sẻ 4. Người dùng chọn nút chia sẻ VBCC 5. Người dùng xác nhận thực hiện thao tác 6. Hệ thống hiển thị VBCC và mã QR 		
Alternative Flow Người dùng không đăng nhập được vào hệ thống.	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng đăng nhập lại. 2. Quay trở lại bước 1 của Standard flow. 		
Alternative Flow 2	<ol style="list-style-type: none"> 1. Hệ thống yêu cầu người dùng có quyền truy 		

Người dùng không có quyền truy cập vào chức năng quản lý VBCC	cập vào chức năng này. 2. Quay trở lại bước 1 của Standard flow.
---	---

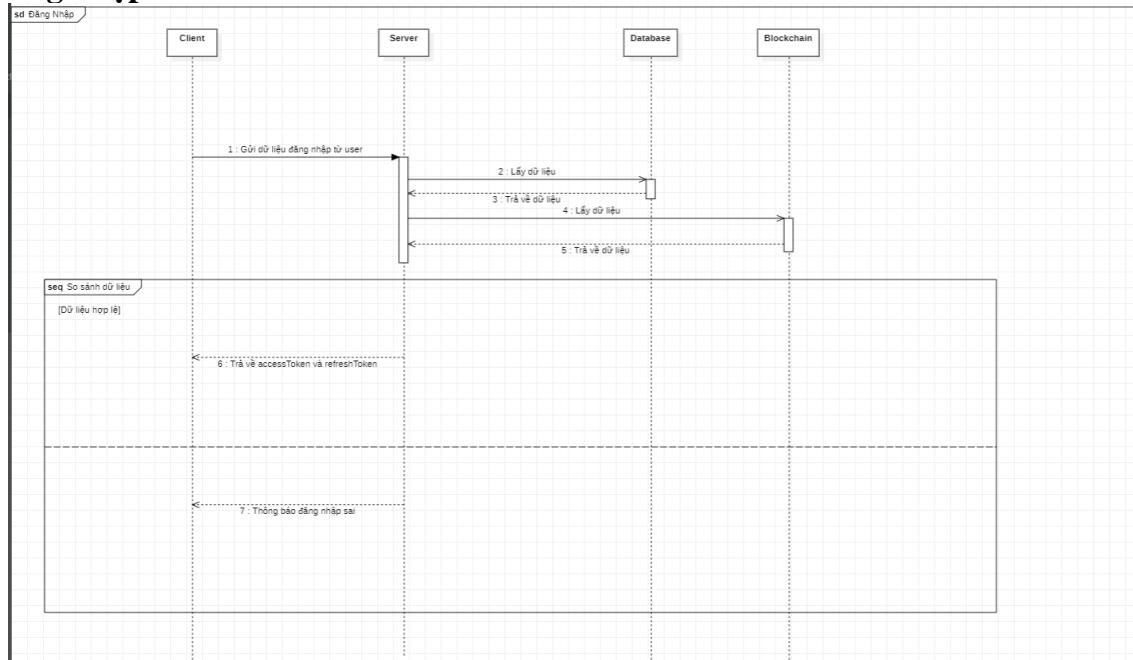
3.6.20 USE CASE 39. Xác thực VBCC

Name	Xác Thực VBCC	Code	UC39
Description	Xác thực VBCC		
Actor	Người Xác Minh	Trigger	Quét mã QR hoặc hình thực paste chuỗi mã hóa và điền thông tin
Pre-condition	Có mã QR hoặc thông tin có trong VB		
Post-condition	Xác minh văn bằng hoàn tất		
Error situations	<ul style="list-style-type: none"> - Mã chứng chỉ không hợp lệ - Chứng chỉ hết hạn - Chứng chỉ bị chỉnh sửa - Lỗi hệ thống 		
System state in error situations	<ul style="list-style-type: none"> - Mã chứng chỉ không hợp lệ: Hệ thống hiển thị thông báo lỗi cho người dùng, cho biết mã chứng chỉ không hợp lệ. - Chứng chỉ hết hạn: Hệ thống thông báo cho người dùng biết chứng chỉ đã hết hạn và không thể xác thực được. - Chứng chỉ bị chỉnh sửa: Hệ thống phát hiện chứng chỉ đã bị chỉnh sửa và cảnh báo người dùng. - Lỗi hệ thống: Hệ thống hiển thị thông báo lỗi cho người dùng, cho biết có vấn đề xảy ra với máy chủ và không thể hoàn tất xác thực. 		
Standard flow/process	<ol style="list-style-type: none"> 1. Người dùng nhập mã chứng chỉ hoặc mã QR VBCC. 2. Hệ thống kiểm tra tính hợp lệ của mã chứng chỉ. 3. Nếu mã chứng chỉ không hợp lệ, hệ thống hiển thị thông báo lỗi và kết thúc quy trình. 4. Nếu mã chứng chỉ hợp lệ, hệ thống kiểm tra ngày hết hạn của chứng chỉ. 5. Nếu chứng chỉ đã bị chỉnh sửa, hệ thống cảnh báo người dùng rằng chứng chỉ đã bị sửa đổi. 6. Nếu chứng chỉ hợp lệ và không bị chỉnh sửa, hệ thống xác nhận tính chính xác của chứng chỉ VBCC. 7. Hệ thống hiển thị thông tin liên quan về chứng chỉ đã được xác thực. 		
Alternative Flow 1 Mã chứng chỉ không	<ol style="list-style-type: none"> 1. Người dùng nhập một mã chứng chỉ VBCC không hợp lệ. 		

hợp lệ	<ol style="list-style-type: none"> 2. Hệ thống phát hiện mã không hợp lệ. 3. Hệ thống hiển thị thông báo lỗi cho biết mã chứng chỉ không hợp lệ. 4. Quy trình kết thúc.
Alternative Flow 2 Lỗi Hệ thống	<ol style="list-style-type: none"> 1. Hệ thống gặp lỗi trong quá trình xử lý yêu cầu xác thực. 2. Hệ thống hiển thị thông báo lỗi cho biết có lỗi xảy ra trên máy chủ. 3. Quy trình kết thúc và người dùng được khuyến nghị thử lại sau hoặc liên hệ với bộ phận hỗ trợ để được giúp đỡ.

3.7 Sequence Diagram

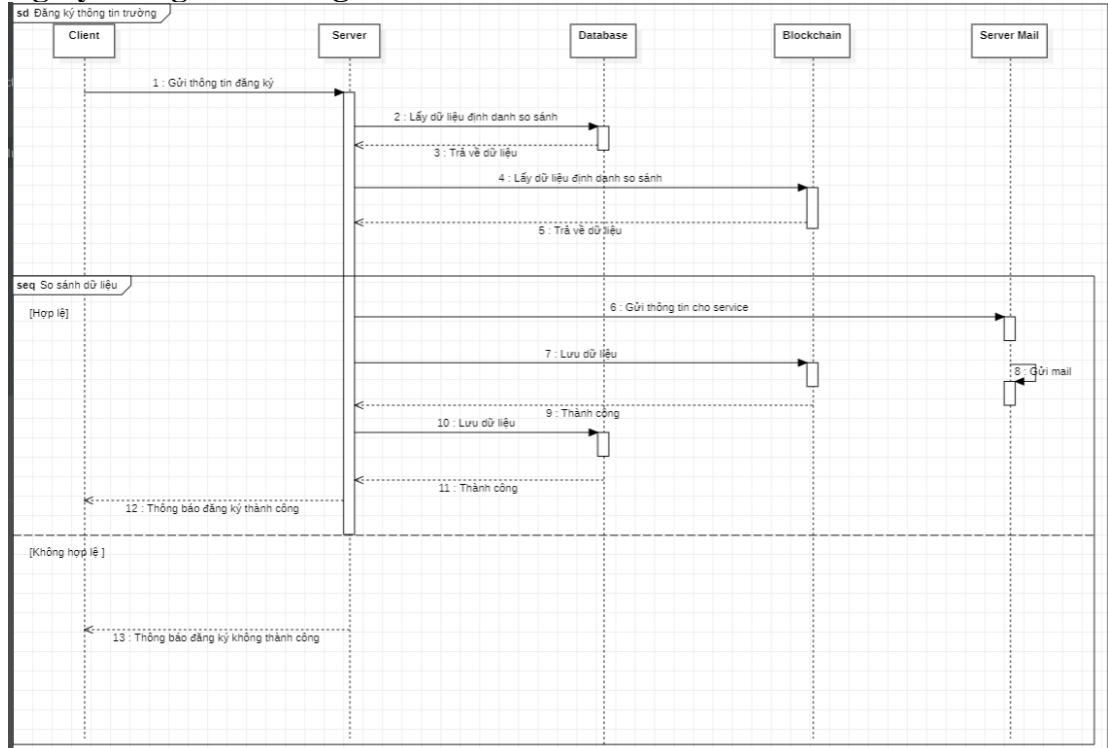
3.7.1 Đăng nhập



Hình 3.10 Sequence Diagram Đăng nhập

Khi client gửi thông tin đăng nhập server sẽ tiếp nhận và truy vấn cơ sở dữ liệu, Blockchain xem dữ liệu có đồng nhất không. Nếu không đồng nhất thì trả về thông báo đăng nhập không thành công. Ngược lại trả về accessToken và refreshToken cho client

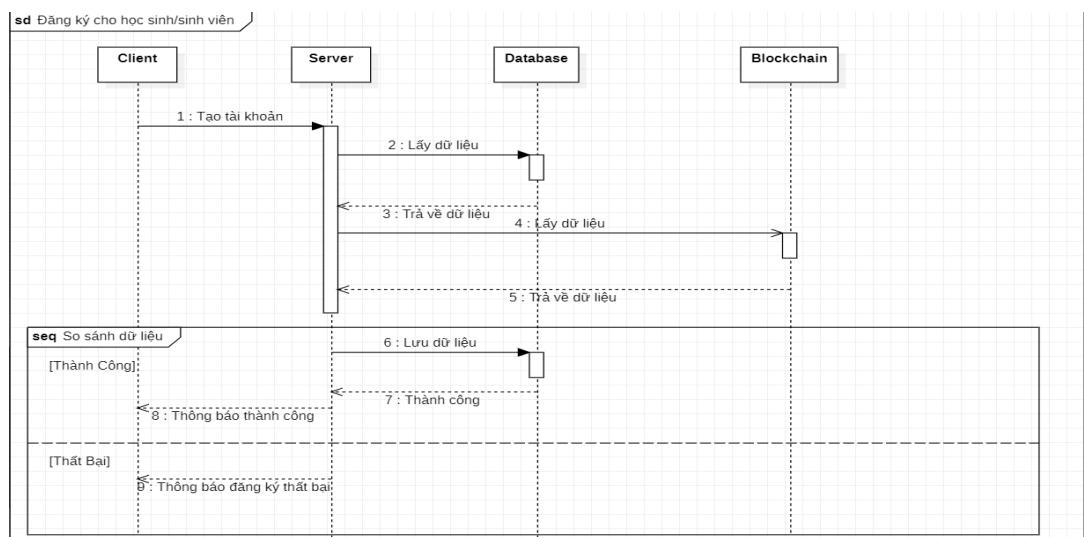
3.7.2 Đăng ký thông tin trường



Hình 3.11 Sequence Diagram Đăng ký thông tin trường

Khi client gửi thông tin đăng ký trường học, server tiếp nhận và truy vấn cơ sở dữ liệu, Blockchain kiểm tra có hợp lệ hay không còn nếu không hợp lệ trả về thông báo đăng ký không hợp lệ. Ngược lại lưu dữ liệu vào cơ sở dữ liệu và Blockchain ban hành chứng thư số và lưu dữ liệu đồng thời gửi cho service bên thứ 3 là gửi mail đến người dùng đăng ký

3.7.3 Đăng ký sinh viên

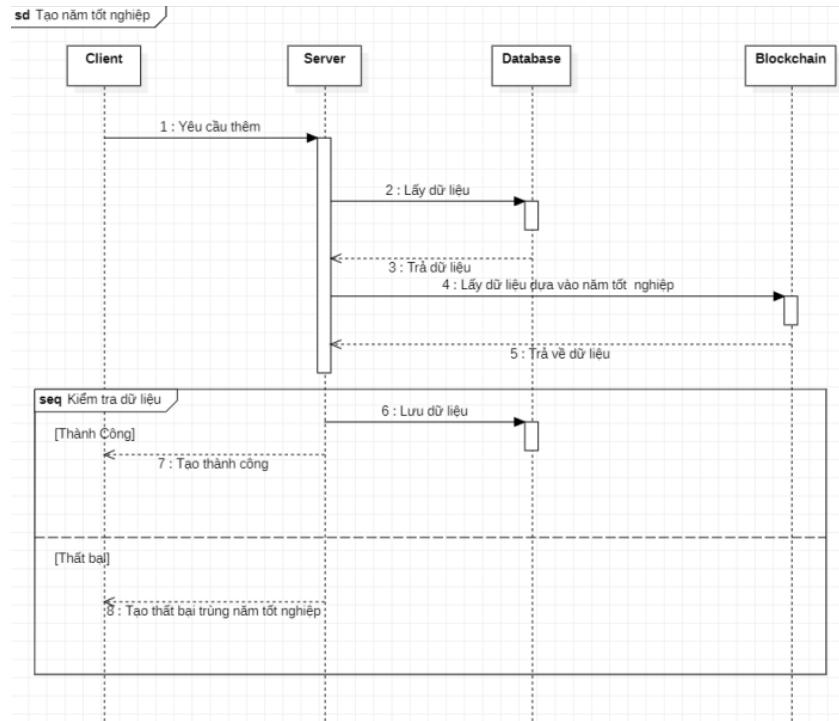


Hình 3.12 Sequence Diagram Đăng ký sinh viên

Khi client gửi thông tin đăng ký sinh viên, server tiếp nhận và truy vấn cơ sở dữ liệu, Blockchain kiểm tra có hợp lệ hay không còn nếu không hợp lệ trả về thông báo đăng ký không hợp lệ. Ngược lại lưu dữ liệu vào cơ sở dữ liệu và Blockchain ban hành chứng thư số đồng thời gửi cho service bên thứ 3 là gửi mail đến người dùng đăng ký

3.7.4 Quản lý năm tốt nghiệp

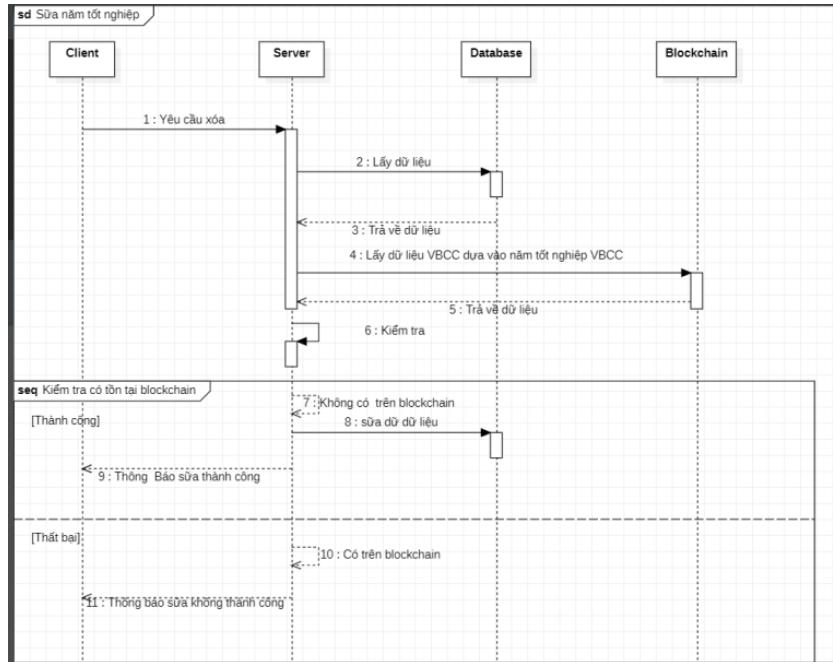
3.7.4.1 Tạo năm tốt nghiệp



Hình 3.13 Sequence Diagram Tạo năm tốt nghiệp

Khi client yêu cầu tạo thông tin năm tốt nghiệp server truy vấn cơ sở dữ liệu, Blockchain kiểm tra thông tin có tồn tại hay không. Nếu không tồn tại sẽ tạo . Ngược lại thông báo tạo không thành công

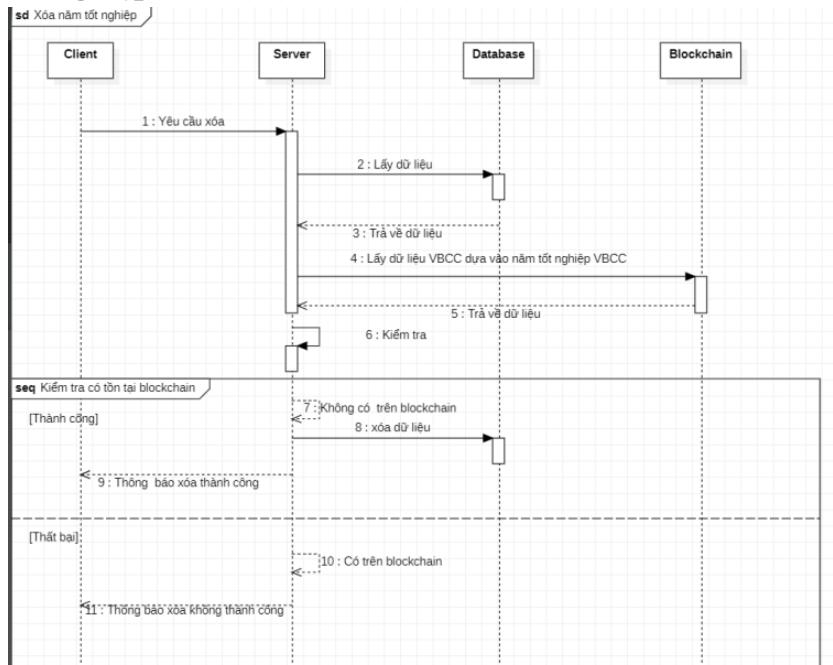
3.7.4.2 Sửa năm tốt nghiệp



Hình 3.14 Sequence Diagram Sửa năm tốt nghiệp

Khi client yêu cầu sửa thông tin năm tốt nghiệp server truy vấn cơ sở dữ liệu, Blockchain kiểm tra dữ liệu đã được có trên Blockchain nếu không có sửa thành công. Ngược lại sửa không thành công

3.7.4.3 Xóa năm tốt nghiệp



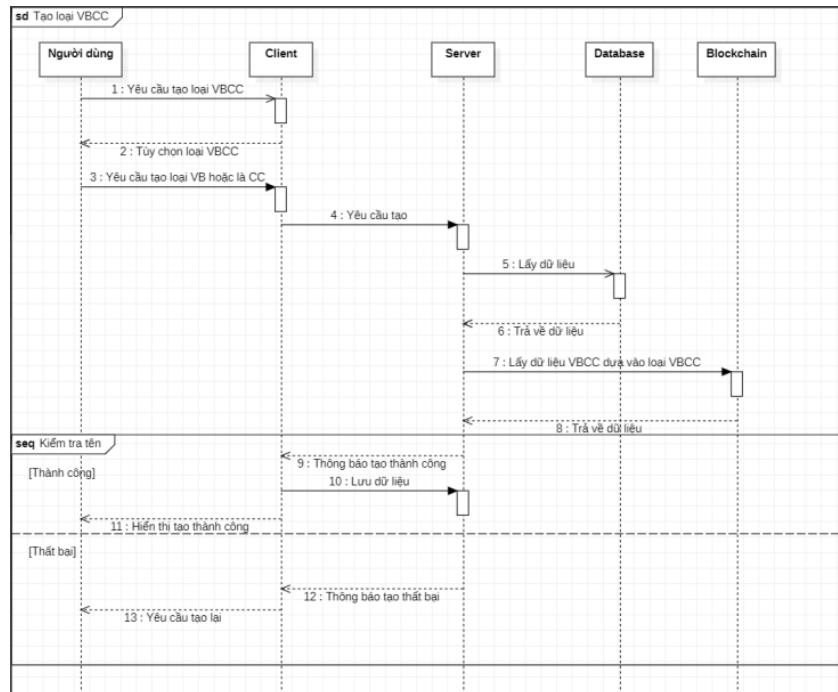
Hình 3.15 Sequence Diagram Xóa năm tốt nghiệp

Khi client yêu cầu xóa thông tin năm tốt nghiệp server truy vấn cơ sở dữ liệu, Blockchain kiểm tra dữ liệu đã được có trên Blockchain nếu không có xóa thành công.

Ngược lại xóa không thành công

3.7.5 Quản lý loại VBCC

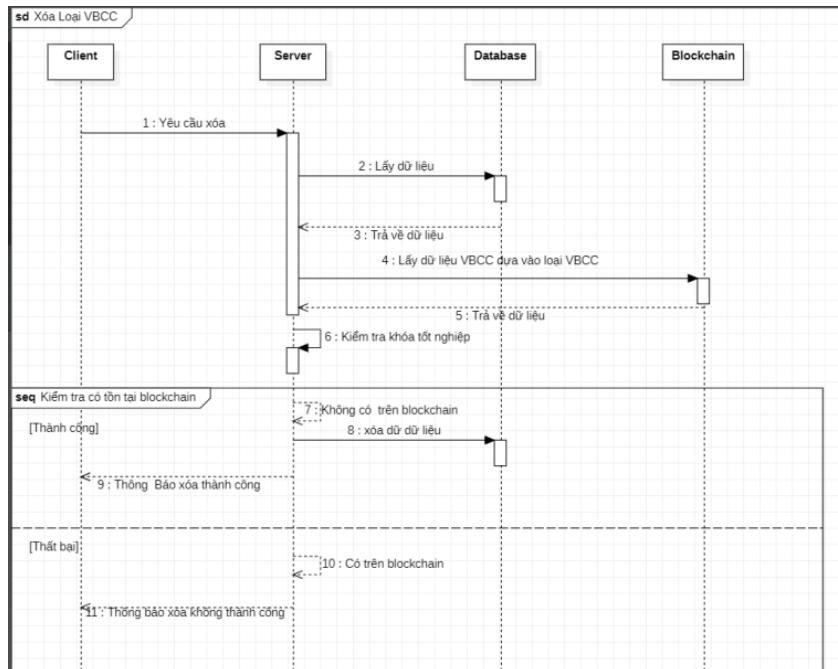
3.7.5.1 Tạo VBCC



Hình 3.16 Sequence Diagram Tạo loại VBCC

Khi client yêu cầu tạo loại VBCC server truy vấn cơ sở dữ liệu, Blockchain kiểm tra thông tin có tồn tại hay không. Nếu không tồn tại sẽ tạo . Ngược lại thông báo tạo không thành công

3.7.5.2 Xóa loại VBCC

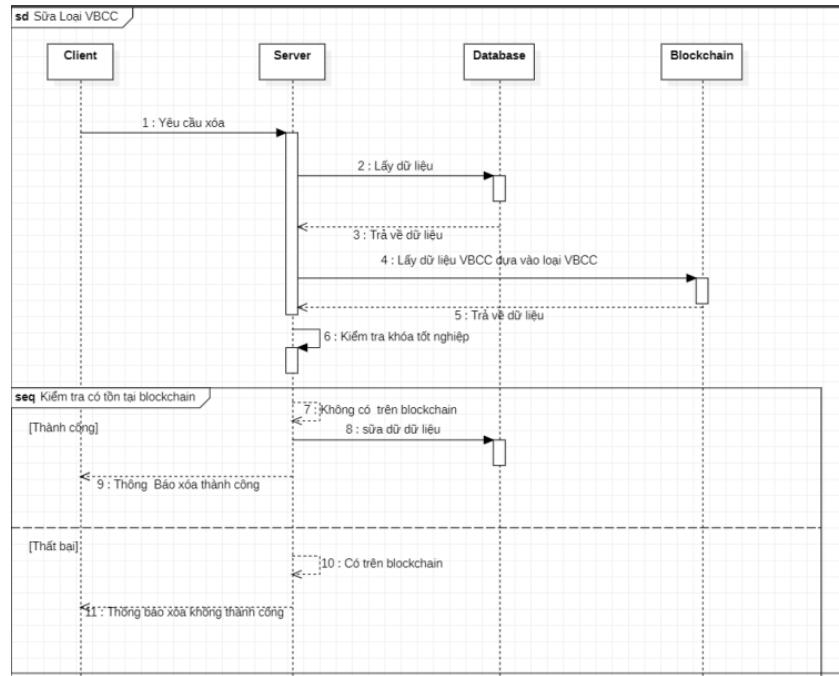


Hình 3.17 Sequence Diagram Xóa loại VBCC

Khi client yêu cầu xóa loại VBCC server truy vấn cơ sở dữ liệu, Blockchain kiểm

tra dữ liệu đã được có trên Blockchain nếu không có xóa thành công. Ngược lại xóa không thành công

3.7.5.3 Sửa loại VBCC

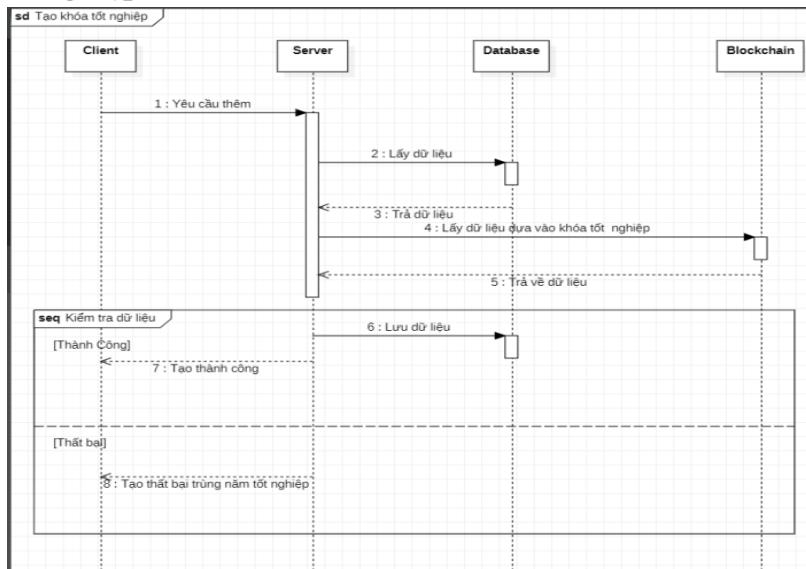


Hình 3.18 Sequence Diagram Sửa loại VBCC

Khi client yêu cầu sửa loại VBCC server truy vấn cơ sở dữ liệu, Blockchain kiểm tra dữ liệu đã được có trên Blockchain nếu không có sửa thành công. Ngược lại sửa không thành công

3.7.6 Quản lý khóa tốt nghiệp

3.7.6.1 Tạo khóa tốt nghiệp

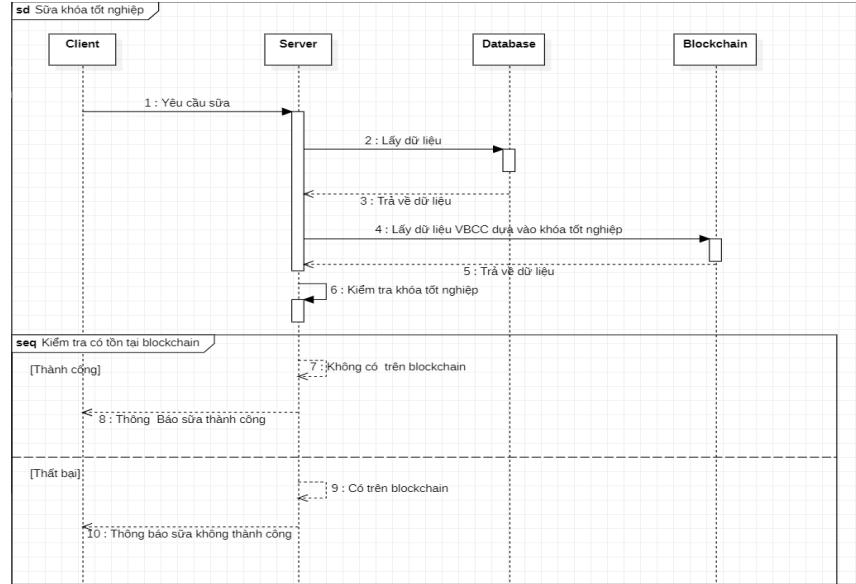


Hình 3.19 Sequence Diagram Tạo khóa tốt nghiệp

Khi client yêu cầu tạo khóa tốt nghiệp server truy vấn cơ sở dữ liệu, Blockchain kiểm tra thông tin có tồn tại hay không. Nếu không tồn tại sẽ tạo . Ngược lại thông báo

tạo không thành công

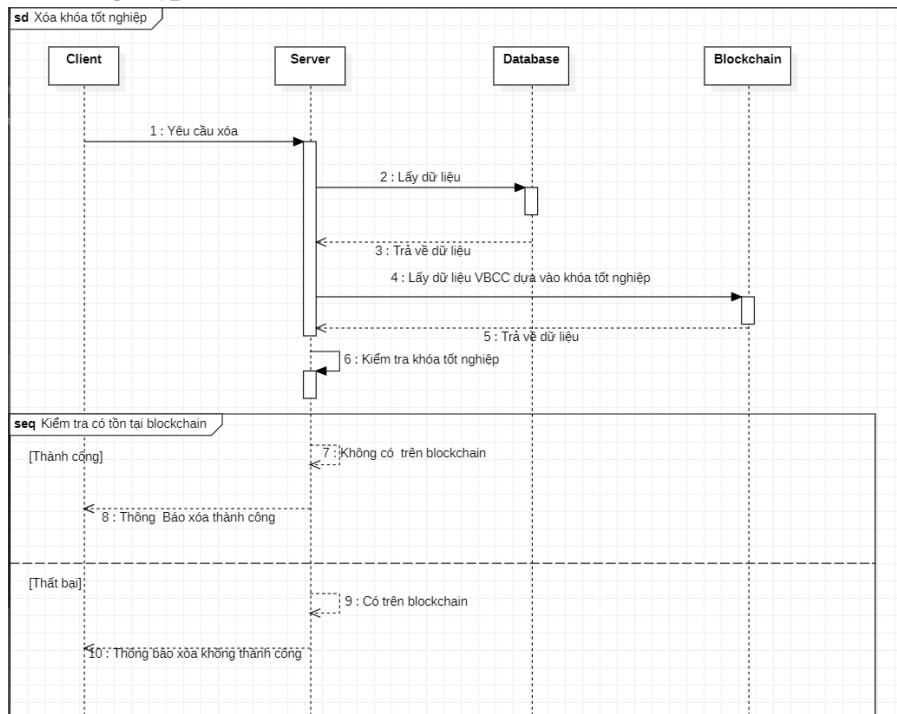
3.7.6.2 Sửa khóa tốt nghiệp



Hình 3.20 Sequence Diagram Sửa khóa tốt nghiệp

Khi client yêu cầu sửa khóa tốt nghiệp server truy vấn cơ sở dữ liệu, Blockchain kiểm tra dữ liệu đã được có trên Blockchain nếu không có sửa thành công. Ngược lại sửa không thành công

3.7.6.3 Xóa khóa tốt nghiệp

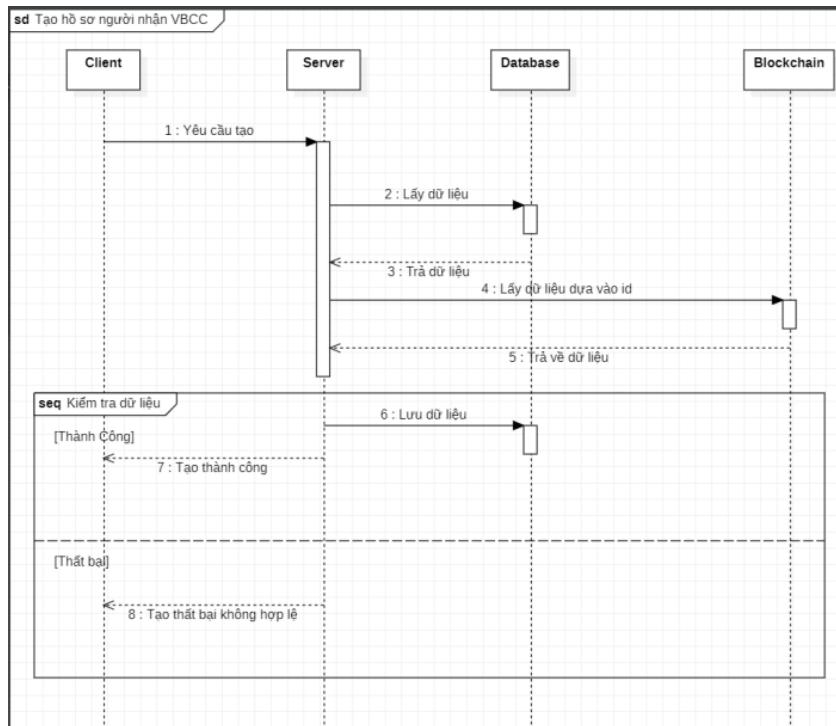


Hình 3.21 Sequence Diagram Xóa khóa tốt nghiệp

Khi client yêu cầu xóa khóa tốt nghiệp server truy vấn cơ sở dữ liệu, Blockchain kiểm tra dữ liệu đã được có trên Blockchain nếu không có xóa thành công. Ngược lại xóa không thành công

3.7.7 Quản lý hồ sơ người nhận

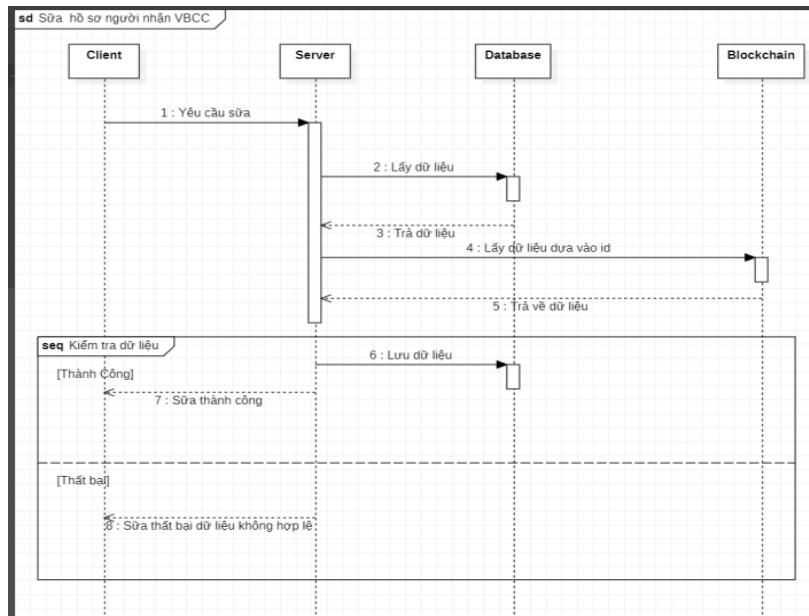
3.7.7.1 Tạo danh sách hồ sơ người nhận



Hình 3.22 Sequence Diagram Tạo danh sách hồ sơ người nhận

Khi client yêu cầu tạo hồ sơ người nhận VBCC server truy vấn cơ sở dữ liệu, Blockchain kiểm tra thông tin có tồn tại hay không. Nếu không tồn tại sẽ tạo . Ngược lại thông báo tạo không thành công

3.7.7.2 Sửa thông tin hồ sơ người nhận

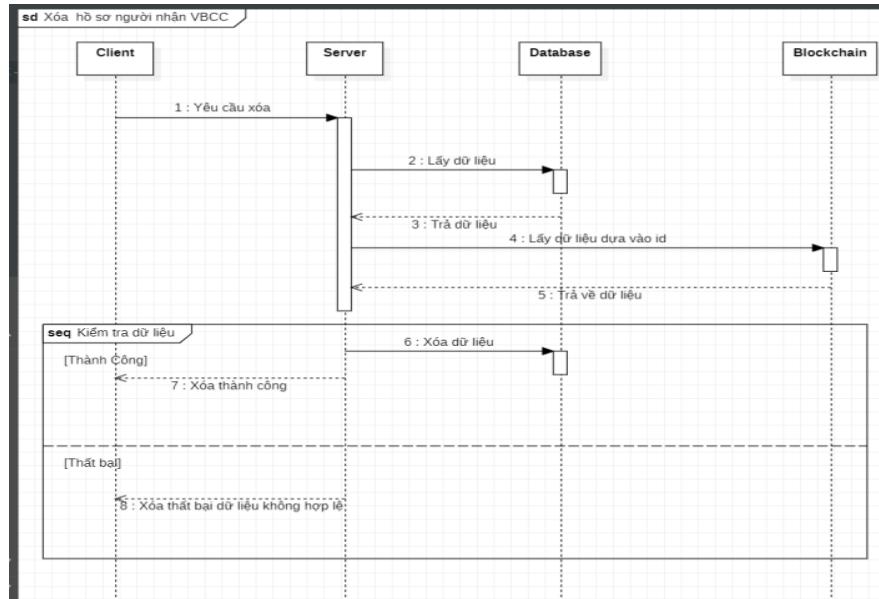


Hình 3.23 Sequence Diagram Sửa thông tin người nhận

Khi client yêu cầu sửa hồ sơ người nhận VBCC server truy vấn cơ sở dữ liệu, Blockchain kiểm tra dữ liệu đã được cung cấp trên Blockchain nếu không có sửa thành công.

Ngược lại sửa không thành công

3.7.7.3 Xóa hồ sơ người nhận

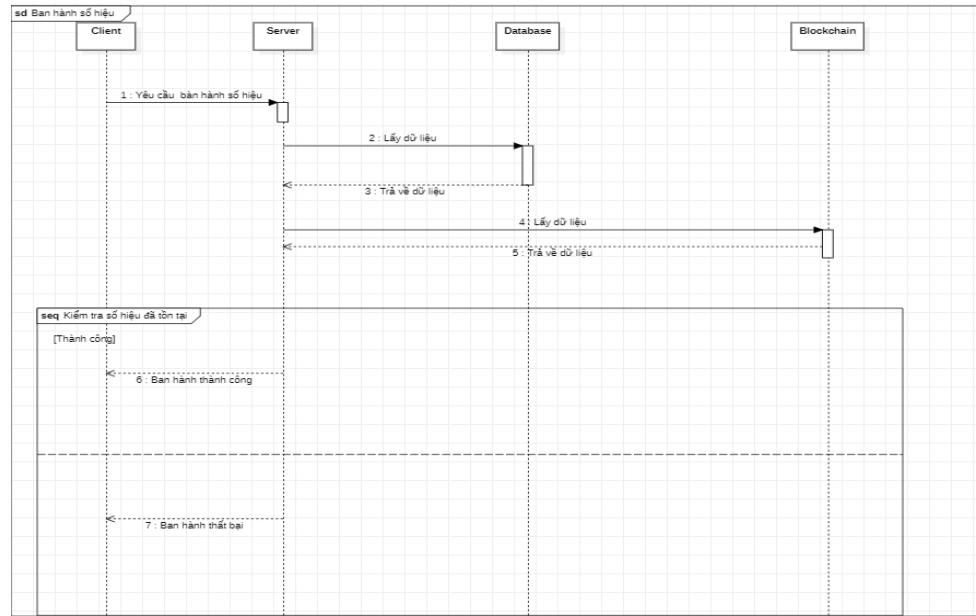


Hình 3.24 Sequence Diagram Xóa hồ sơ người nhận

Khi client yêu cầu xóa hồ sơ người nhận VBCC server truy vấn cơ sở dữ liệu, Blockchain kiểm tra dữ liệu đã được có trên Blockchain nếu không có xóa thành công.

Ngược lại xóa không thành công

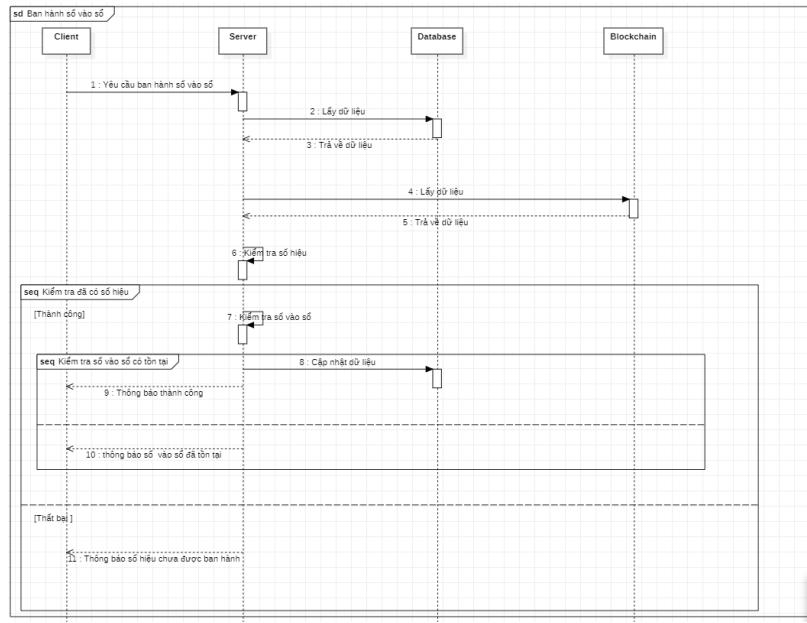
3.7.8 Ban hành số hiệu



Hình 3.25 Sequence Diagram Ban hành số hiệu

Khi client yêu cầu ban hành số hiệu tốt nghiệp server truy vấn cơ sở dữ liệu, Blockchain kiểm tra thông tin có tồn tại số hiệu đó trên Blockchain hay không. Nếu không tồn tại sẽ tạo . Ngược lại thông báo tạo không thành công

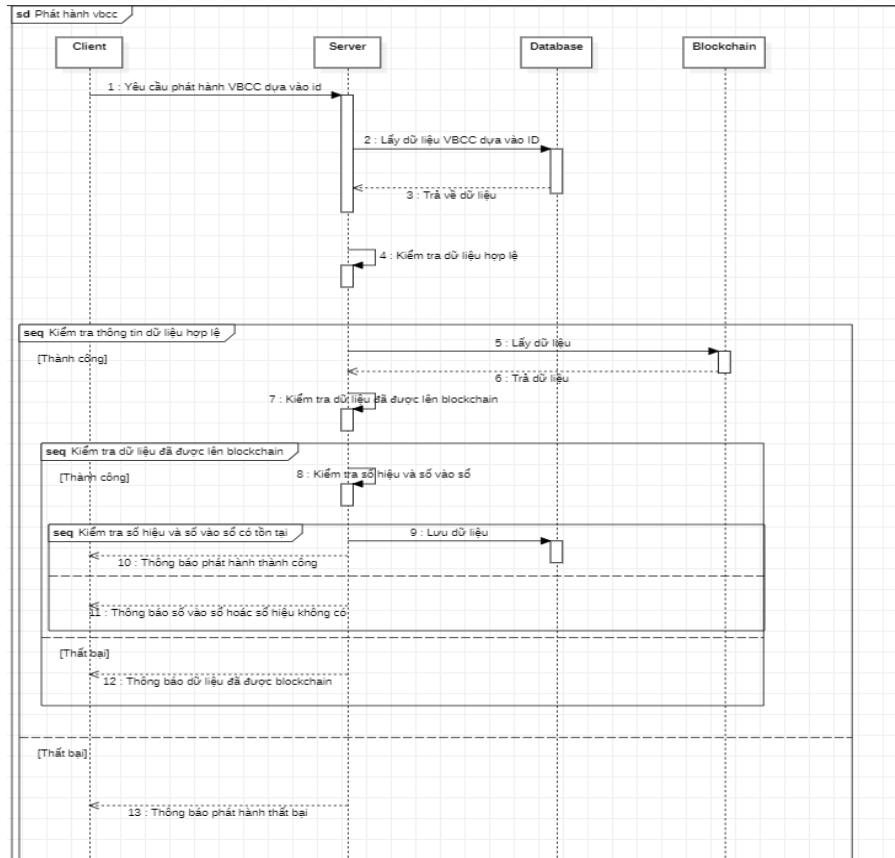
3.7.9 Ban hành số vào sổ



Hình 3.26 Ban hành số vào sổ

Khi client yêu cầu ban hành số vào sổ tốt nghiệp server truy vấn cơ sở dữ liệu, Blockchain kiểm tra thông tin có tồn tại số vào sổ đó trên Blockchain hay không. Nếu không tồn tại sẽ tạo. Ngược lại thông báo tạo không thành công

3.7.10 Phát hành VBCC



Hình 3.27 Phát hành VBCC

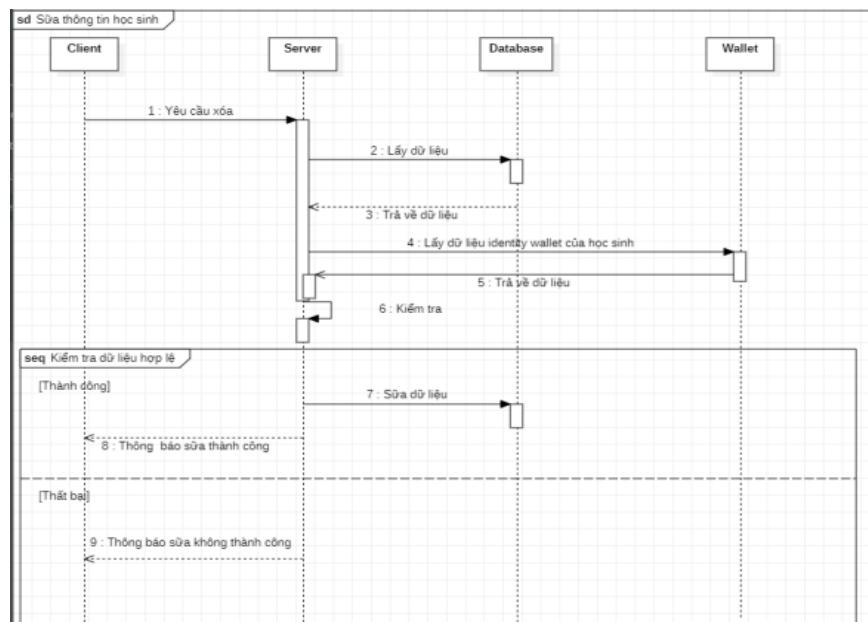
Khi client yêu cầu phát hành VBCC server truy vấn cơ sở dữ liệu, Blockchain.

Kiểm tra dữ liệu hợp lệ hay không. Ngược lại nếu không hợp lệ thông báo cho client

Kiểm tra dữ liệu có trên Blockchain hay chưa. Nếu không hợp lệ thông báo phát hành VBCC không thành công. Nếu dữ liệu hợp lệ. Kiểm tra dữ liệu số vào sổ và số hiệu thêm lần nữa. Nếu chưa tồn tại thì tạo. Ngược lại thông báo phát hành VBCC không thành công.

3.7.11 Quản lý sinh viên

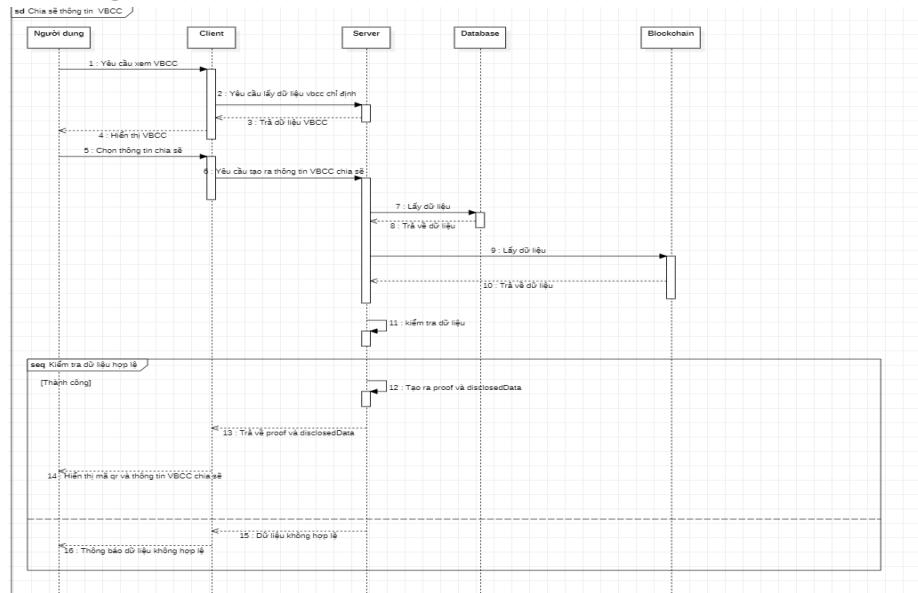
3.7.11.1 Sửa thông tin sinh viên



Hình 3.28 Sửa thông tin sinh viên

Khi client yêu cầu sửa thông tin sinh viên server truy vấn cơ sở dữ liệu, Blockchain kiểm tra dữ liệu đã được có trên Blockchain nếu không có sửa thành công. Ngược lại sửa không thành công

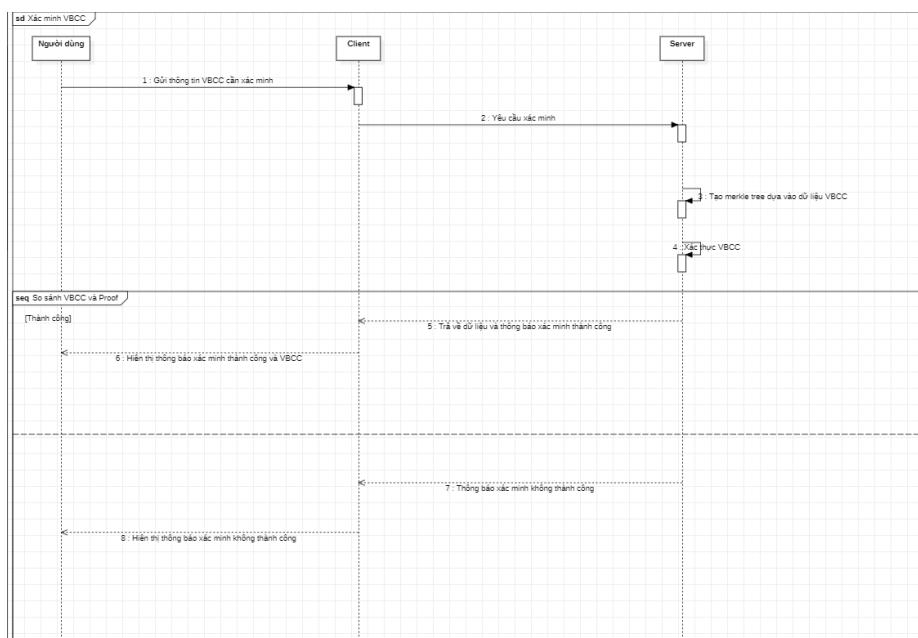
3.7.11.2 Chia sẻ thông tin VBCC



Hình 3.29 Sequence Diagram Chia sẻ thông tin VBCC

Khi người dùng yêu cầu xem VBCC. Client gửi thông tin VBCC chỉ định đến server. Server truy vấn dữ liệu và trả về dữ liệu VBCC chỉ định. Client hiển thị thông tin VBCC. Người dùng sẽ chọn thông tin nào cần chia sẻ sau đó gửi lên client. Client gửi lên server. Server xử lý lấy dữ liệu Blockchain, cơ sở dữ liệu kiểm tra dữ liệu. Nếu dữ liệu hợp lệ tạo ra proof và disclosedData trả về cho client. Client trả về cho người dùng thông tin và mã QR

3.7.11.3 Xác minh VBCC



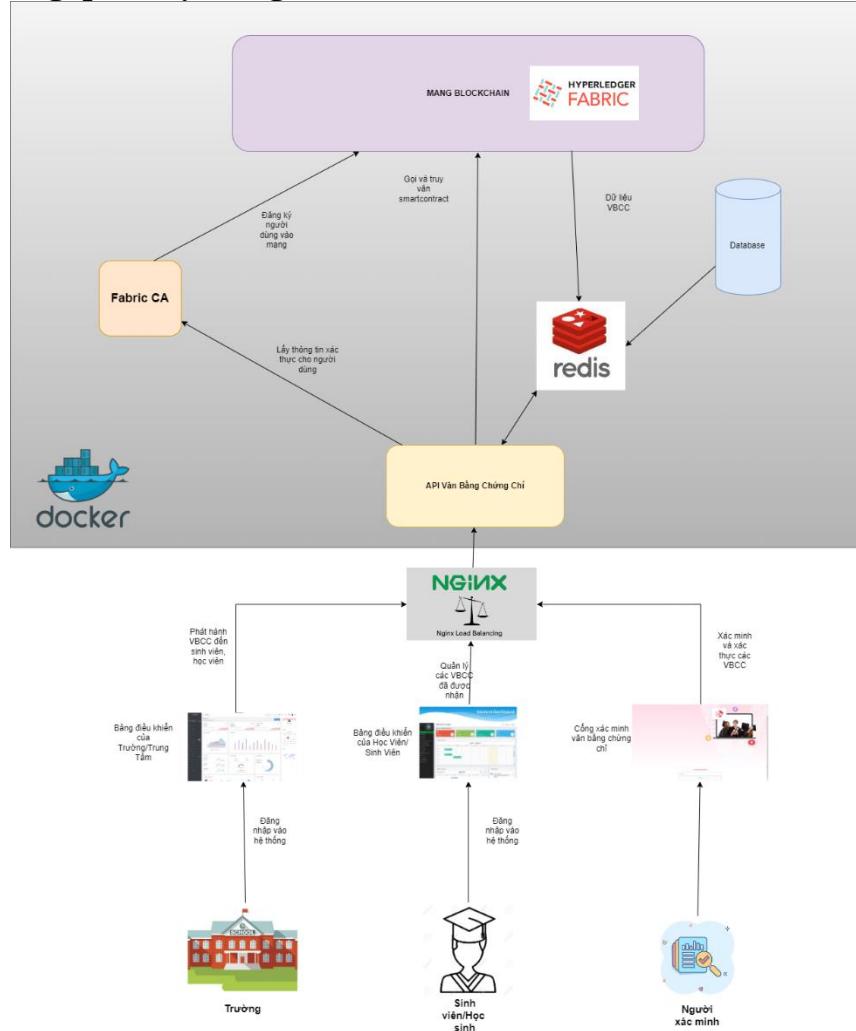
Hình 3.30 Sequence Diagram Xác minh VBCC

Khi người gửi thông tin cần xác minh gồm proof và disclosedData. Client tiếp

nhận và gửi đến server. Server thực hiện xác minh dữ liệu bằng thuật toán xác minh multiproof của cấu trúc dữ liệu merkle tree. Sau đó trả về kết quả cho client. Client thông báo cho người dùng

3.8 Tổng quan hệ thống

3.8.1 Kiến trúc tổng quan hệ thống



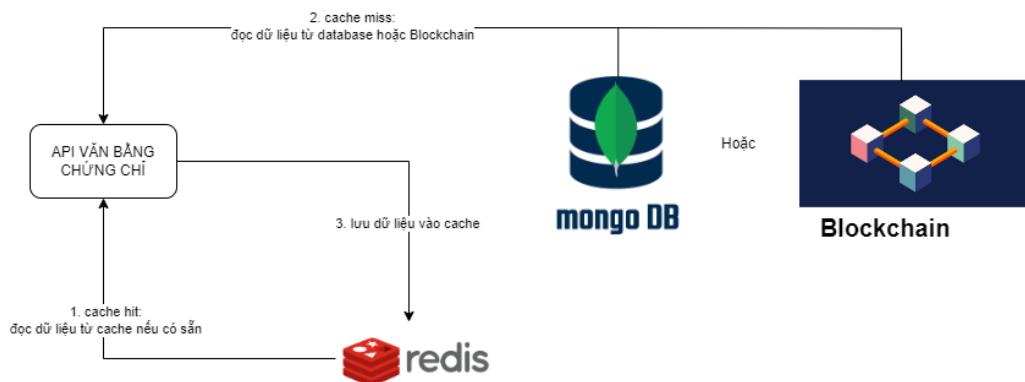
Hình 3.31 Tổng quan hệ thống

Đây là sơ đồ tổng quan hệ thống VBCC

- Chúng ta sẽ có 3 đối tượng trong hệ thống:
 - Trường
 - Sinh viên
 - Người xác minh
- Những đối tượng sẽ tương tác với giao diện web phù hợp với từng hành động nhiệm vụ của mỗi đối tượng
- Giao diện sẽ thực hiện yêu cầu của đối tượng đến API VBCC và API chứng chỉ sẽ xử lý yêu cầu và trong quy trình xử lý sẽ tiếp xúc với 4 thành phần trong hệ thống:
 - Fabric CA

- Cơ sở dữ liệu
- Mạng Blockchain
- Redis
- Khi API request lên Blockchain sẽ cần Fabric CA là gác cổng kiểm tra quyền request lên Blockchain có phù hợp và được có quyền truy cập vào smartcontract chức năng đó hay không. Nếu không hợp lệ sẽ phản hồi lại cho API và API sẽ báo lỗi cho client
- Mạng Blockchain là nơi là chứa các dữ liệu VBCC và trường nhưng nó có tính bất biến không thể nào thay đổi
- Cơ sở dữ liệu cũng là nơi chứa các dữ liệu và các dữ liệu khác để tạo ra VBCC nhưng những dữ liệu ở đây có thể thay đổi được. Khi đi sâu vào cách giải quyết hệ thống ta sẽ thích sâu về vấn đề này.
- Redis là nơi để cache dữ liệu giúp hệ thống tối ưu và có hiệu suất cao

3.8.2 Cơ sở dữ liệu



Hình 3.32 Cache trong cơ sở dữ liệu

- Trong hệ thống cơ sở dữ liệu vì để đảm bảo về mặt hiệu suất, đỡ tốn tài nguyên nên chúng em đã áp dụng thêm redis là nơi cache dữ liệu và áp dụng chiến lược cache là Cache aside.
- Cache aside là một mô hình thiết kế cache phổ biến trong các hệ thống phân tán, được sử dụng để cải thiện hiệu suất truy xuất dữ liệu từ cơ sở dữ liệu. Mô hình này tận dụng sự hiệu quả của cache để giảm thời gian truy cập vào cơ sở dữ liệu chậm.
- Trong mô hình cache aside, dữ liệu được lưu trữ trong hai nơi: cache và cơ sở dữ liệu chính (thường là một cơ sở dữ liệu ổn định như hệ quản trị cơ sở dữ liệu SQL). Khi ứng dụng cần đọc dữ liệu, quá trình truy xuất dữ liệu diễn ra theo các bước sau:

3.8.2.1 Cache hit (truy cập thành công):

- Ứng dụng truy vấn dữ liệu từ cache.
- Nếu dữ liệu có sẵn trong cache, được gọi là cache hit, dữ liệu được trả về cho ứng dụng mà không cần truy xuất cơ sở dữ liệu chính.
- Quá trình này nhanh chóng và giảm bớt tải cho cơ sở dữ liệu chính.

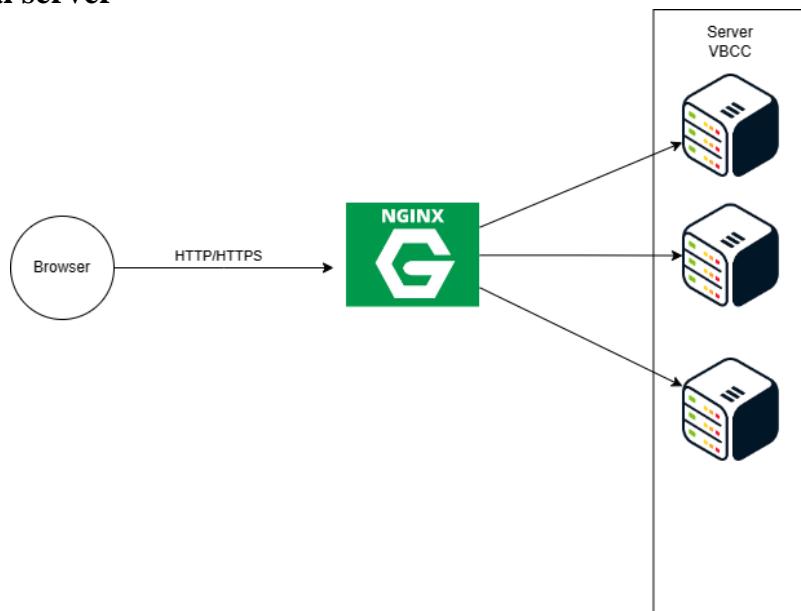
3.8.2.2 Cache miss (truy cập không thành công):

- Nếu dữ liệu không tồn tại trong cache, được gọi là cache miss, ứng dụng sẽ truy xuất dữ liệu từ cơ sở dữ liệu chính.
- Truy xuất cơ sở dữ liệu chính sẽ tốn nhiều thời gian hơn so với cache hit, nhưng nó chỉ xảy ra khi dữ liệu không có sẵn trong cache.
- Sau khi truy xuất cơ sở dữ liệu chính thành công, dữ liệu sẽ được đọc và trả về cho ứng dụng.
- Đồng thời, dữ liệu này cũng sẽ được lưu vào cache để các truy vấn sau có thể tận dụng cache hit.

3.8.2.3 Lưu dữ liệu vào cache:

- Sau khi đọc dữ liệu từ cơ sở dữ liệu chính trong quá trình cache miss, dữ liệu sẽ được lưu vào cache để sử dụng cho các truy vấn tương lai.
- Lưu trữ dữ liệu vào cache tùy thuộc vào chiến lược được xác định, như là việc đặt thời gian sống (time-to-live) hoặc sử dụng kỹ thuật khác để xác định xem khi nào dữ liệu cần được xóa khỏi cache.
- Tác dụng của cache aside cải thiện hiệu suất khi dữ liệu được lưu trong cache, việc truy cập lần tiếp theo có thể được thực hiện

3.8.3 Cân bằng tải server

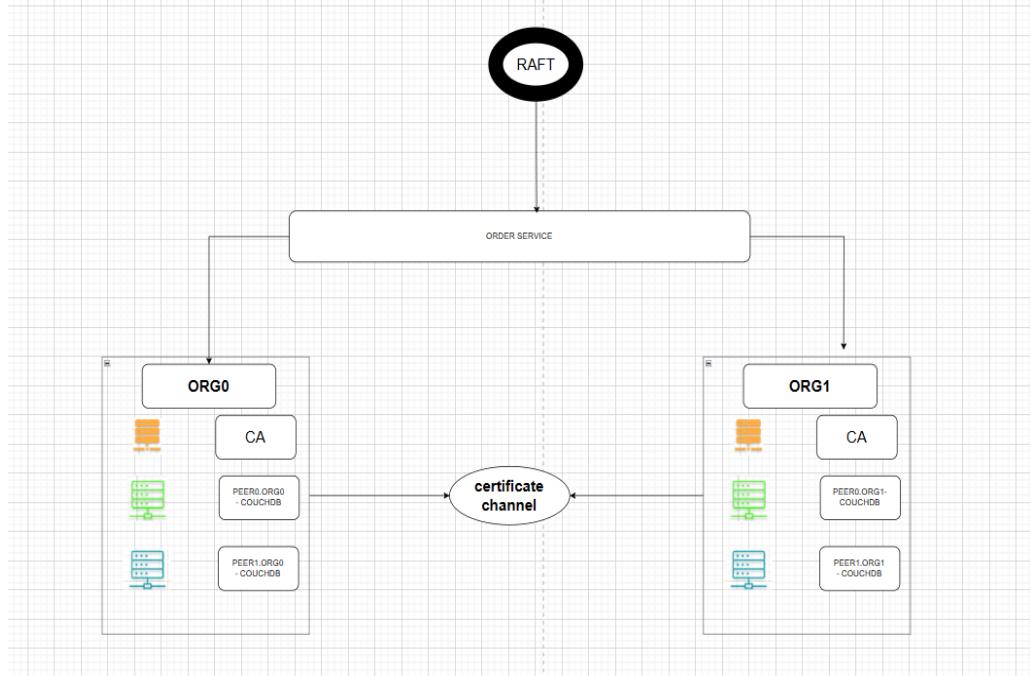


Hình 3.33 Cân bằng tải server

Khi lượng user sử dụng request ngày càng nhiều để tránh trường hợp bị sập server chúng ta sẽ sử dụng loadbalancing để cân bằng tải. Nó sẽ giúp server chạy cân bằng không để server chịu đựng 1 lượng request cao

Ví dụ: Khi một lượng user lớn request khi không có NGINX thì lượng user request đến sẽ request đến server 1 lượng lớn khiến server sập. Nhưng khi ta đặt NGINX đồng nghĩa cùng với việc bật thêm bản sao server thì nginx sẽ là người cân bằng lượng request điều chuyển request đến từng server không để 1 server chịu hết tất cả request

3.8.4 Mạng Blockchain



Hình 3.34 Kiến trúc thử nghiệm được cài đặt trong môi trường hệ thống VBCC

- Mạng HF được triển khai gồm có 02 tổ chức (ORG0, ORG1), mỗi ORG được cài đặt trên một máy chủ ảo riêng. Mỗi ORG bao gồm các thành phần:

1. 1 CA

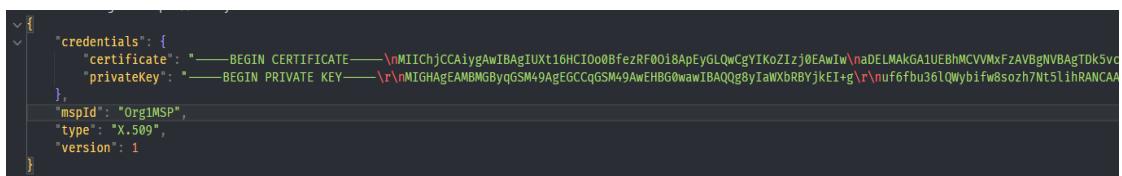
2. 2 Peer sử dụng CSDL couchdb

- Ngoài ra trong mạng HF cũng được cài đặt Ordering Service, nút Orderer dùng cơ chế đồng thuận RAFT.

- Tất cả các tổ chức sẽ cùng tham gia vào kênh certificate channel

3.8.5 Các thành phần của một chứng thư số trong hệ thống VBCC

Khi người dùng tạo tài khoản trong hệ thống VBCC thì những tài khoản này sẽ được phát hành chứng thư số từ Hyperledger Fabric



Hình 3.35 Các thành phần một chứng thư số (JSON)

Dưới đây là giải thích chứng trong đoạn mã JSON :

- "credentials": Chứa thông tin về chứng thư số và khóa riêng tư.
- "certificate": Đây là phần chứa chứng thư số dạng PEM. Bạn có thể thấy chuỗi bắt đầu từ "-----BEGIN CERTIFICATE-----" và kết thúc bằng "-----END CERTIFICATE-----". Đây là một chứng thư số X.509.

- "privateKey": Đây là phần chứa khóa riêng tư dạng PEM. Tương tự như chứng thư số, nó bắt đầu bằng "-----BEGIN PRIVATE KEY-----" và kết thúc bằng "-----END PRIVATE KEY-----". Đây là khóa riêng tư tương ứng với chứng thư số.
- "mspId": Là mã nhận dạng (ID) của tổ chức (Membership Service Provider) mà chứng thư số thuộc về. Trong trường hợp này, mspId là "Org1MSP".
- "type": Xác định loại chứng thư số. Trong trường hợp này, nó là "X.509", cho biết đó là một chứng thư số X.509.
- "version": Xác định phiên bản của chứng thư số.

Tổng quan, đoạn mã JSON chứa thông tin về chứng thư số dạng X.509 và khóa riêng tư tương ứng, cùng với các thông tin khác như mã nhận dạng và phiên bản.

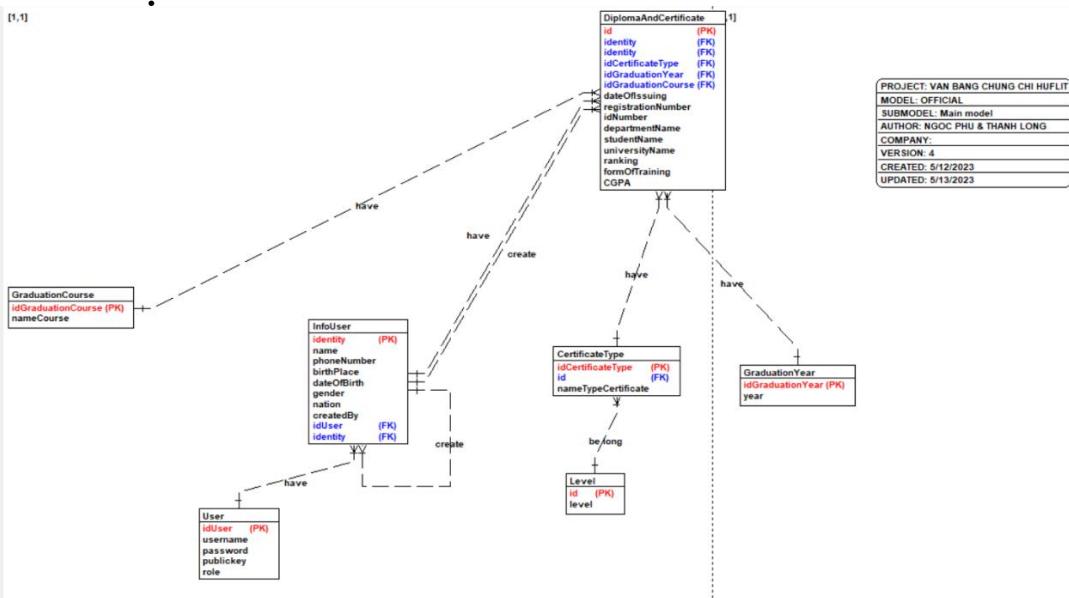
3.8.6 PKI trong HyperLedge Fabric

Trong Hyperledger Fabric, Public Key Infrastructure (PKI) cũng đóng vai trò quan trọng trong việc xác thực và bảo mật các thành viên và giao dịch trong mạng Blockchain. PKI trong Hyperledger Fabric được sử dụng để tạo, quản lý và xác thực chứng chỉ số và khóa công khai cho các thành viên tham gia vào mạng.

Các thành phần chính của PKI trong Hyperledger Fabric bao gồm:

- Certificate Authority (CA): Hyperledger Fabric sử dụng CA để phát hành và quản lý chứng chỉ số cho các thành viên trong mạng. CA được sử dụng để xác thực danh tính của các thành viên và tạo ra chứng chỉ số cho họ. CA có thể được triển khai dưới dạng một CA độc lập hoặc bằng cách sử dụng Hyperledger Fabric Certificate Authority (Fabric CA), một thành phần cung cấp sẵn trong Hyperledger Fabric.
- Enrollment Process: Quá trình đăng ký (enrollment process) trong Hyperledger Fabric là quá trình mà một thành viên mới trong mạng được xác thực và được phát hành chứng chỉ số. Trong quá trình này, thành viên mới sẽ cung cấp thông tin xác thực và yêu cầu chứng chỉ từ CA. CA sẽ xác minh thông tin và sau đó tạo ra chứng chỉ số cho thành viên.
- X.509 Certificates: Hyperledger Fabric sử dụng định dạng chứng chỉ X.509 cho việc xác thực và bảo mật. Chứng chỉ X.509 chứa thông tin về danh tính của thành viên và được sử dụng để xác thực và mã hóa dữ liệu trong mạng.
- MSP (Membership Service Provider): MSP trong Hyperledger Fabric quản lý các chứng chỉ và khóa công khai của các thành viên trong mạng. Nó định nghĩa các quy tắc và chính sách xác thực và ủy quyền trong mạng.
- PKI trong Hyperledger Fabric đảm bảo tính toàn vẹn, bảo mật và xác thực của các thành viên và giao dịch trong mạng Blockchain. Nó giúp đảm bảo rằng chỉ có các thành viên được xác thực mới có thể tham gia vào mạng và thực hiện các giao dịch an toàn và bảo mật.

3.8.7 Cơ sở dữ liệu & Blockchain



Hình 3.36 Lược đồ CSDL

3.8.8 Mô tả Cơ sở dữ liệu

1. Bảng User

Bảng 3.19 Cơ sở dữ liệu 01.Bảng User

Id	Tên	Kiểu dữ liệu	Ràng buộc	Mô tả
id	Mã người dùng	String	PK	Đây là trường dữ liệu đại diện cho một giá trị duy nhất để xác định mỗi bản ghi trong bảng dữ liệu. Trường này thường được sử dụng để xác định một đối tượng duy nhất trong hệ thống.
username	Tên người dùng	String	NOT NULL	Trường này chứa tên người dùng hoặc tên đăng nhập của người dùng trong hệ thống. Nó thường được sử dụng để xác định một người dùng cụ thể và có thể được sử dụng cho mục đích xác thực và phân quyền.
password	Mật khẩu người dùng	String	NOT NULL	Trường này chứa vai trò hoặc quyền hạn của người dùng trong hệ thống. Vai trò này có thể được sử dụng để quản lý phân quyền và kiểm soát truy cập của người dùng vào các tài nguyên và chức năng trong hệ thống.
Publickey	Khóa công khai	String	NOT NULL	Trường này chứa khóa công khai của người dùng, được sử dụng trong các cơ chế mã hóa và xác thực. Nó có thể được sử dụng

				trong các hệ thống mật mã công khai để đảm bảo tính bí mật và xác thực của dữ liệu.
--	--	--	--	---

3.8.8.1 Bảng Info User

Bảng 3.20 Cơ sở dữ liệu 02. Info User

Id	Tên	Kiểu dữ liệu	Ràng buộc	Mô tả
identity	CMND	String	PK	<p>Đây là trường dữ liệu đại diện cho một giá trị duy nhất để xác định mỗi bản ghi trong bảng dữ liệu.</p> <p>Trường này thường được sử dụng để xác định một đối tượng duy nhất trong hệ thống</p>
idUser	Mã người dùng	String	FK	Trường này liên kết với trường id trong bảng User và được sử dụng để xác định một người dùng cụ thể trong hệ thống.
createdBy	Được tạo bởi	String	FK	Trường này liên kết với trường id trong bảng User và chỉ ra người dùng đã tạo bản ghi.
name	Tên người dùng	String	NOT NULL	Trường này chứa tên của người sở hữu
phoneNumber	Số điện thoại	String	NOT NULL	Trường này chứa số điện thoại
birthPlace	Nơi Sinh	String	NOT NULL	Trường này chứa địa điểm sinh
dateOfBirth	Ngày sinh	String	NOT NULL	Trường này chứa ngày tháng năm sinh

gender	Giới tính	String	NOT NULL	Trường này chứa giới tính. Thông thường, giá trị của trường này có thể là "Nam" hoặc "Nữ", nhưng cũng có thể được mở rộng để hỗ trợ các giá trị khác nếu cần thiết.
nation	Dân tộc	String	NOT NULL	Trường này chứa quốc tịch.

3.8.8.2 Bảng Graduation Course

Bảng 3.21 Cơ sở dữ liệu 03.Bảng Graduation Course

Id	Tên	Kiểu dữ liệu	Ràng buộc	Mô tả
idGraduationCourse	Mã định danh khóa học	String	PK	Đây là trường dữ liệu đại diện cho một giá trị duy nhất để xác định mỗi bản ghi trong bảng dữ liệu. Trường này thường được sử dụng để xác định một đối tượng duy nhất trong hệ thống
nameCourse	Tên khóa học	String	NOT NULL	Trường này chứa học tốt nghiệp.

3.8.8.3 Bảng Graduation Year

Bảng 3.22 Cơ sở dữ liệu 04.Bảng Graduation Year

Id	Tên	Kiểu dữ liệu	Ràng buộc	Mô tả
idGraduationYear	Mã định danh năm học	String	PK	Trường này chứa quốc tịch.
nameYear	năm	String	NOT NULL	Trường này chứa năm tốt nghiệp.

3.8.8.4 Bảng Certificate Type

Bảng 3.23 Cơ sở dữ liệu 05.Bảng Certificate Type

Id	Tên	Kiểu dữ liệu	Ràng buộc	Mô tả
idCertificateType	Mã định danh khóa học	String	PK	Đây là trường dữ liệu đại diện cho một giá trị duy nhất để xác định mỗi bản ghi trong bảng dữ liệu. Trường này thường được sử dụng để xác định một đối tượng duy nhất trong hệ thống
idLevel	Mã định danh level	String	NOT NULL	Trường này liên kết với trường idLevel trong bảng Level và được sử dụng để xác định cấp bậc loại VBCC dùng cụ thể trong hệ thống.
nameCertificate	Tên khóa học	String	NOT NULL	Trường này chứa loại VBCC

3.8.8.5 Bảng Level

Bảng 3.24 Cơ sở dữ liệu 06.Bảng Level

Id	Tên	Kiểu dữ liệu	Ràng buộc	Mô tả
idLevel	Mã định danh cấp bậc	String	PK	Đây là trường dữ liệu đại diện cho một giá trị duy nhất để xác định mỗi bản ghi trong bảng dữ liệu. Trường này

				thường được sử dụng để xác định một đối tượng duy nhất trong hệ thống
level	Cấp bậc	String	NOT NULL	Trường này chưa cấp bậc

3.8.8.6 Bảng Diploma And Certificate

Bảng 3.25 Cơ sở dữ liệu 07. Bảng Diploma And Certificate

Id	Tên	Kiểu dữ liệu	Ràng buộc	Mô tả
idDiplomaAndCertificate	Mã định danh VBCC	String	PK	Đây là trường dữ liệu đại diện cho một giá trị duy nhất để xác định mỗi bản ghi trong bảng dữ liệu. Trường này thường được sử dụng để xác định một đối tượng duy nhất trong hệ thống
identityStudent	Mã định danh người dùng là sinh viên	String	FK	Trường này liên kết với trường trong bảng InfoUser và được sử dụng để xác định sinh viên nhận VBCC cụ thể trong hệ thống.
identityUniversity	Mã định danh người dùng là trường	String	FK	Trường này liên kết với trường trong bảng InfoUser và được sử dụng để xác định trường phát VBCC cụ thể trong hệ thống.
idCertificateType	Mã định danh loại VBCC	String	FK	Trường này liên kết với trường trong bảng

				InfoUser và được sử dụng để xác định sinh viên nhận VBCC cụ thể trong hệ thống.
idGraduationYear	Mã định danh tốt nghiệp năm	String	FK	Trường này liên kết với trường trong bảng GraduationYear và được sử dụng để xác định năm tốt nghiệp trong VBCC.
idGraduationCourse	Mã định danh tốt nghiệp khóa học	String	FK	Trường này liên kết với trường trong bảng GraduationCourse và được sử dụng để xác định khóa học tốt nghiệp trong VBCC.
dateOfIssuing	Ngày ban hành	DateTime	NOT NULL	Trường này chứa người phát hành VBCC.
registrationNumber	Số hiệu	String	NOT NULL	Trường này chứa số hiệu VBCC.
idNumber	Số vào sổ	String	NOT NULL	Trường này chứa số vào sổ VBCC.
departmentName	Tên VBCC	String	NOT NULL	Trường này chứa tên VBCC.
studentName	Tên sinh viên	String	NOT NULL	Trường này chứa tên sinh viên nhận VBCC.
universityName	Tên trường	String	NOT NULL	Trường này chứa tên trường phát hành VBCC.
ranking	Xếp hạng	String	NOT NULL	Trường này chứa loại học lực trong VBCC.
formOfTraining	Hình thức đào tạo	String	NOT NULL	Trường này chứa hình thức đào tạo.
CGPA	Điểm	String	NOT NULL	Trường này chứa số điểm.

3.8.9 Thiết kế Blockchain

3.8.9.1 Danh sách đối tượng

Bảng 3.26 Danh sách đối tượng Blockchain

STT	Tên đối tượng	Mô tả
1	certificate	VBCC
2	schema	Loại VBCC
3	university	Trường cấp VBCC

3.8.9.2 Bảng mô tả các thuộc tính của đối tượng certificate

Bảng 3.27 Blockchain 01.Certificate

STT	Tên trường	Kiểu dữ liệu	Mô tả	Ràng buộc
1	certHash	String	Lưu giá trị băm của VBCC gồm những thông tin:studentEmail, studentName, universityName, universityEmail,number, regNo,major,birthday, cgpa, dateOfIssuing	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	NOT NULL
4	dateOfIssuing	String	Ngày cấp	NOT NULL
5	certNumber	String	Số hiệu VBCC	NOT NULL
6	certRegNo	String	Số vào sổ gốc	NOT NULL
7	certNumber	String	Số hiệu VBCC	NOT NULL
8	certUUID	String	Mã số VBCC	NOT NULL
9	universityPK	String	Khóa công khai của Trường cấp VBCC	NOT NULL
10	Properties	String	Dữ liệu JSON của VBCC	NOT NULL
11	studentPK	String	Khóa công khai của sinh viên nhận VBCC	NOT NULL

Bảng 3.28 Blockchain 02.Schema

STT	Tên trường	Kiểu dữ liệu	Mô tả	Ràng buộc
1	certificateType	String	Loại VBCC	NOT NULL
2	id	String	Mã loại	NOT NULL
3	ordering	String	Thứ tự của từng trường dữ liệu	NOT NULL

Bảng 3.29 Blockchain 03.University

STT	Tên trường	Kiểu dữ liệu	Mô tả	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	NOT NULL
4	description	String	Thông tin mô tả	NOT NULL

CHƯƠNG 4. KẾT QUẢ ĐẠT ĐƯỢC

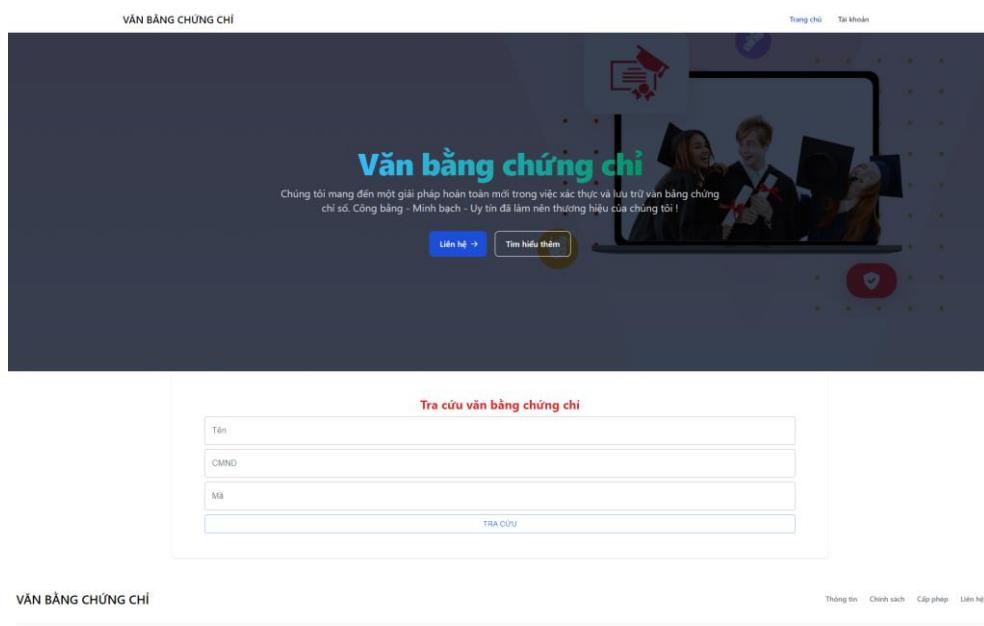
4.1 Mạng Blockchain

Đè tài đã tìm hiểu và thử nghiệm mạng Blockchain: cài đặt trên máy tính cá nhân, sau đó cài đặt và triển khai hệ thống Blockchain trên các máy chủ ảo. Trên máy tính cá nhân, mạng HF được thiết lập và cấu hình như sau:

1. Vào link [huflit-blockchain-certification/backend](https://github.com/huflit-blockchain-certification/backend) (github.com)
2. Clone source github
3. Sau khi clone đứng ở thư mục đã clone cd /backend/blockchain/fabric
4. Bật command line nhập lệnh ./startfabric.sh javascript

4.2 Ứng dụng Web

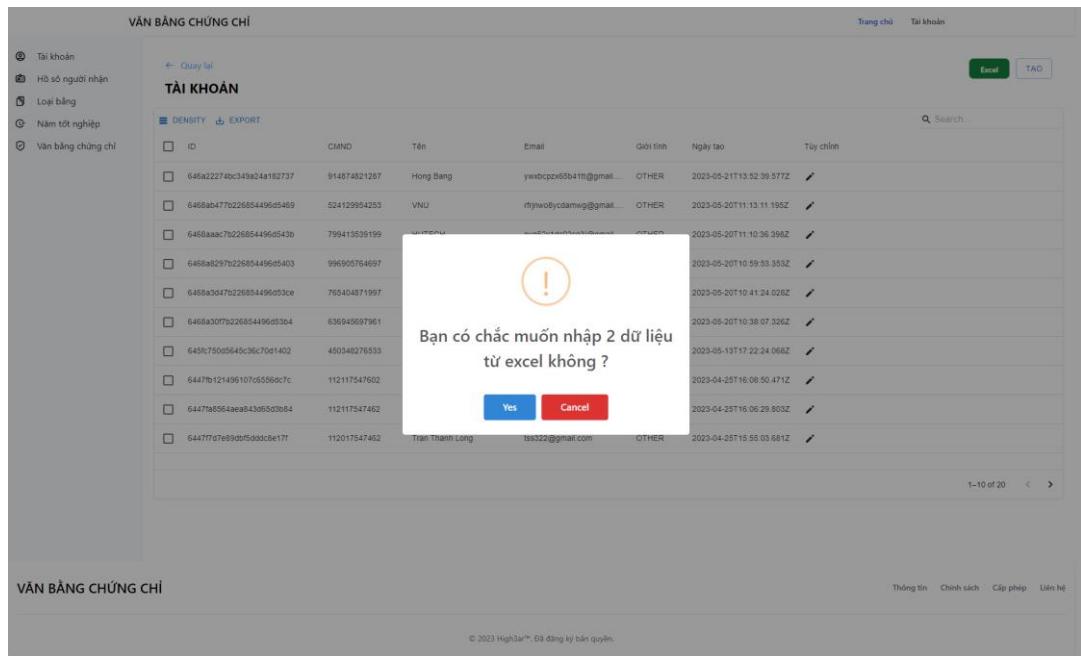
Giao diện ứng dụng web hoạt động tại địa chỉ <https://vbcc.high3ar.club/> như hình 4.1



Hình 4.1 Giao diện trang chủ

4.2.1 Chức năng nhập excel cho tài khoản sinh viên, tài khoản trường, hồ sơ người nhận

Chức năng cho phép người dùng nhanh chóng nhập nhiều dữ liệu từ file excel có sẵn và lưu ý cần phải đúng định dạng có sẵn từ bảng dữ liệu



Hình 4.2 Nhập dữ liệu từ excel

4.2.2 Quản lý đơn vị đào tạo

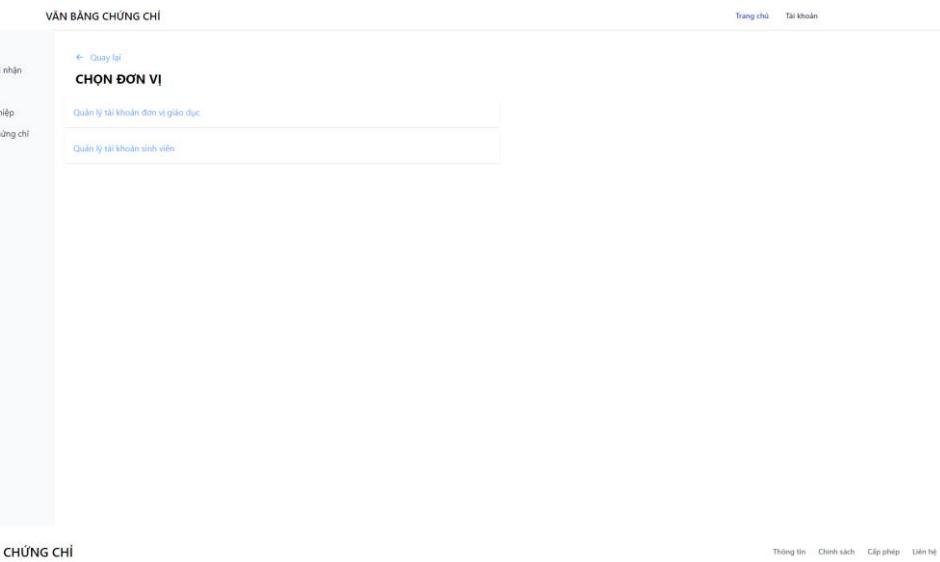
Quản lý đơn vị đào tạo trường đóng vai trò thiết yếu trong hệ thống như nhập số hiệu, tạo tài khoản cho trường cũng như quản lý năm học, các văn bằng có thể cấp, xem thông tin sinh viên

4.2.2.1 Quản lý tài khoản trường

Quản lý đơn vị đào tạo có thể quản lý các tài khoản của trường (trường học / sinh viên) ở trang tài khoản

4.2.2.1.1 Màn hình quản lý tài khoản theo trường / sinh viên

Quản lý đơn vị đào tạo chọn đối tượng để quản lý



Hình 4.3 Màn hình quản lý tài khoản theo trường / sinh viên

4.2.2.1.2 Màn hình quản lý tài khoản trường

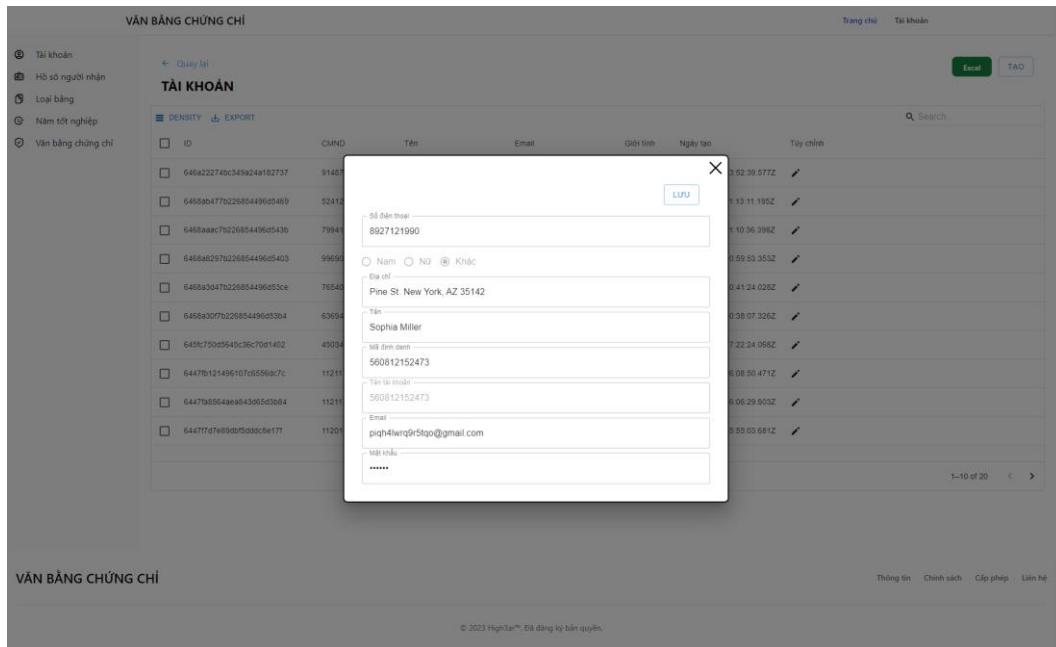
Quản lý đơn vị đào tạo có tạo hoặc nhập thông tin từ excel để thực hiện tạo nhiều tài khoản.

TÀI KHOẢN						
ID	CMND	Tên	Email	Giới tính	Ngày tạo	Tùy chỉnh
646a22274bc349a24a182707	914874821287	Hong Bang	yvxtcpzx8tba4tt@gmail...	OTHER	2023-05-21T13:52:39.07Z	
646ab0477b226854496d5469	524129954253	VNU	itjywoleyctamvg@gmail...	OTHER	2023-05-20T11:13:11.19Z	
6468aacb7226854496d543b	799413539199	HUTECH	nyg52x1dd02cp3ij@gmail...	OTHER	2023-05-20T11:10:36.39Z	
6468a8297b226854496d5403	996905764697	TSA	id2oeQiu70dyvs@gmail...	OTHER	2023-05-20T10:59:53.35Z	
64693d47b226854496d53ce	765404871997	ENU	mcx7ymspjekhs@gmail...	OTHER	2023-05-20T10:41:24.02Z	
6469a30ff7b226854496d53b4	636945697961	HUPI	luwchetchtfsl@gmail.c...	OTHER	2023-05-20T10:38:07.32Z	
645fc750d5645c36c7091402	450348276533	HUFLIT	maq1rltdby5y9g@gmail...	OTHER	2023-05-13T11:22:24.06Z	
6447fb121496107c6556dc7c	112117547602	Tran Thanh Long	tss3222@gmail.com	OTHER	2023-04-25T16:08:50.47Z	
6447fa8564ea843d65d3b64	112117547462	Tran Thanh Long	tss3222@gmail.com	OTHER	2023-04-25T16:06:29.80Z	
64477fd7e89dbf5ddc8e17f	112017547462	Tran Thanh Long	tss322@gmail.com	OTHER	2023-04-25T15:55:03.68Z	

Hình 4.4 Màn hình quản lý tài khoản trường

4.2.2.1.3 Màn hình tạo/ chỉnh sửa trường

Dữ liệu trường đại học sau khi được tạo không thể sửa vì dữ liệu này cần tính đúng đắn trên Blockchain



Hình 4.5 Màn hình tạo/sửa trường

4.2.2.2 Quản lý tài khoản sinh viên

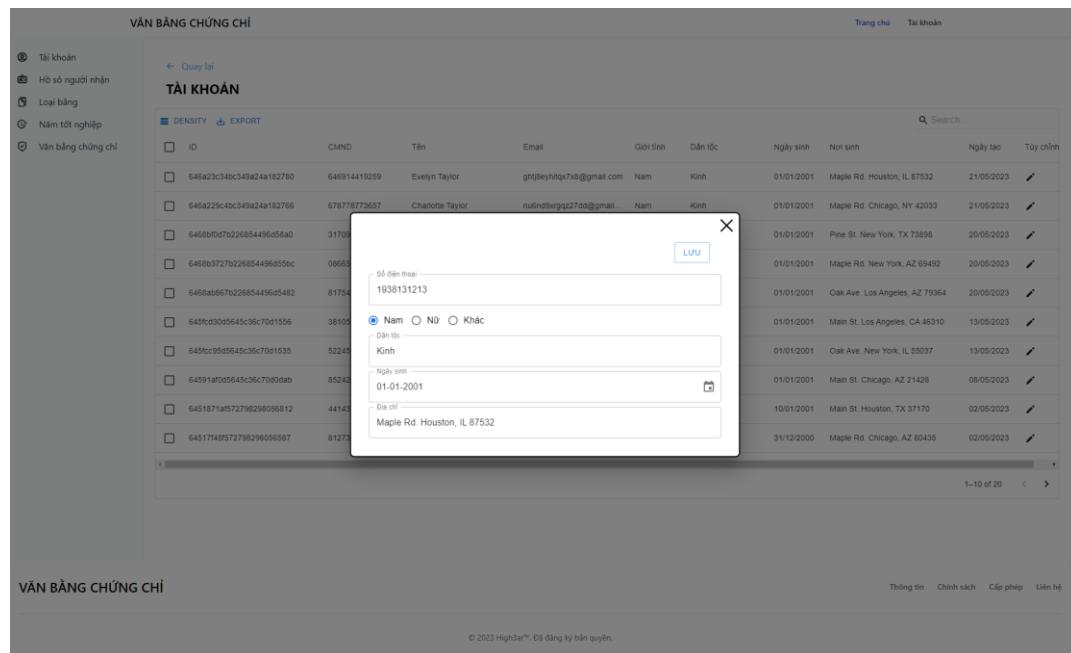
4.2.2.2.1 Màn hình quản lý tài khoản sinh viên

VĂN BẰNG CHỨNG CHỈ										Trang chủ	Tài khoản		
TÀI KHOẢN										Search			
		ID	CMND	Tên	Email	Giới tính	Đến	Nơi sinh	Ngày tạo	Tùy chỉnh			
<input type="checkbox"/>	6468aaac7b025654496d543b	911871											
<input type="checkbox"/>	6468aa477b025654496d5469	524121											
<input type="checkbox"/>	6468aaac7b025654496d543b	79941		Số điện thoại 8927121990	Lưu								
<input type="checkbox"/>	6468aa297b025654496d5400	99909		<input type="radio"/> Nam <input type="radio"/> Nữ <input checked="" type="radio"/> Khác									
<input type="checkbox"/>	6468aa347b025654496d53ce	78540		Địa chỉ Pine St. New York, AZ 35142									
<input type="checkbox"/>	6468aa397b025654496d53b4	63694		Tên Sophia Miller									
<input type="checkbox"/>	6468a75065641c36c70d1400	40034		Mật khẩu 560812152473									
<input type="checkbox"/>	6447fb121496107d6556e7c	11211		Tên và ngày 560812152473									
<input type="checkbox"/>	6447fb8954ae8a63965d384	11211		Email piqht4wqrq@stgo@gmail.com									
<input type="checkbox"/>	6447fb776795d95d8c61f	11201		Mật khẩu *****									
1-10 of 20													
© 2023 High3ar™. Đã đăng ký bản quyền.													
VĂN BẰNG CHỨNG CHỈ										Thông tin	Chỉnh sửa	Cấp phép	Liên hệ

Hình 4.6 Màn hình quản lý tài khoản sinh viên

4.2.2.2.2 Màn hình quản lý tạo chỉnh sửa tài khoản sinh viên

Quản lý đơn vị đào tạo có thể xem tài khoản sinh viên, sửa nếu như tài khoản sinh viên chưa được đưa lên hồ sơ người nhận.



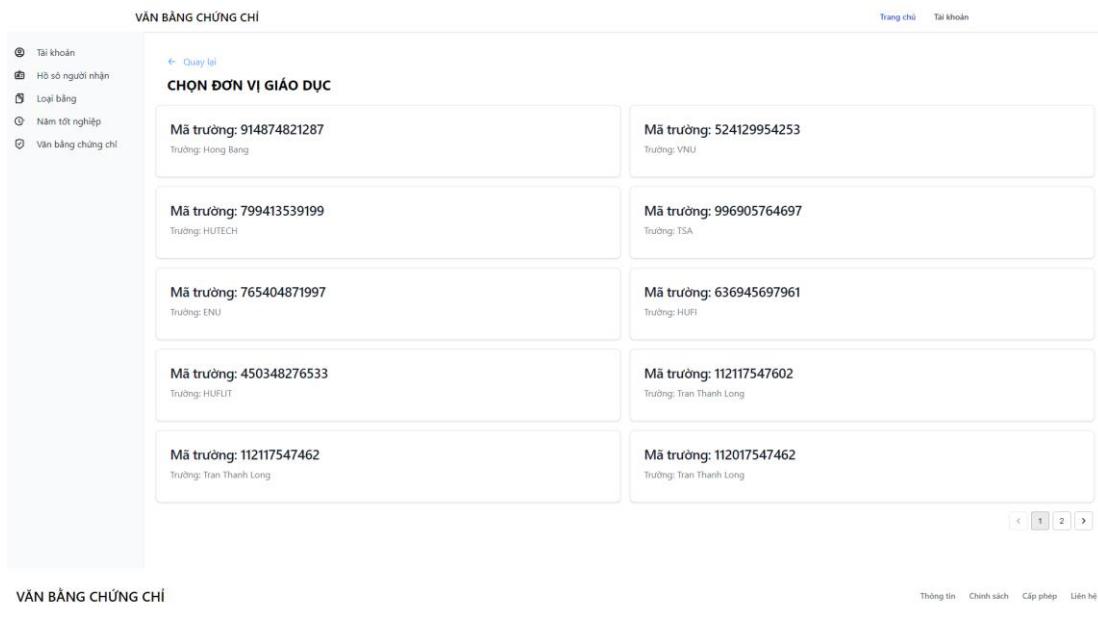
Hình 4.7 Màn hình quản lý tạo / chỉnh sửa tài khoản sinh viên

4.2.2.3 Quản lý hồ sơ người nhận

Hồ sơ người nhận là trang quản lý thông tin của sinh viên được trường nhập vào yêu cầu các bên liên quan như trường / quản lý đơn vị đào tạo nhập số hiệu / số vào sổ trước khi được cấp phát văn bằng lên Blockchain

4.2.2.3.1 Màn hình chọn trường đại học

Quản lý đơn vị đào tạo sẽ phải chọn trường đại học để quản lý hồ sơ người nhận theo trường



Hình 4.8 Màn hình chọn trường đại học

4.2.2.3.2 Màn hình hồ sơ người nhận của một trường đại học

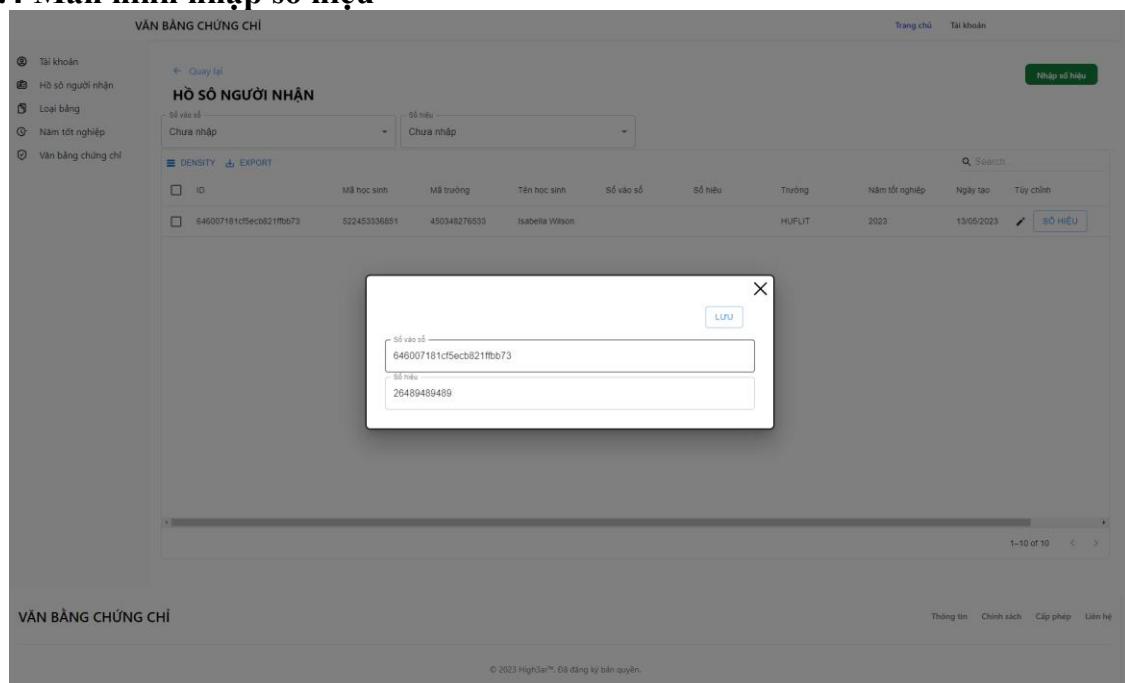
Ngoài nút nhập số hiệu cho từng Sinh viên sẽ có nút nhập số hiệu bằng excel cho phép nhập nhiều dữ liệu số hiệu tương ứng cho sinh viên.

Hình 4.9 Màn hình hồ sơ người nhận của một trường đại học

4.2.2.3.3 Màn hình tạo/chỉnh sửa hồ sơ người nhận

Hình 4.10 Màn hình tạo/chỉnh sửa hồ sơ người nhận

4.2.2.3.4 Màn hình nhập số hiệu



Hình 4.11 Màn hình nhập số hiệu

4.2.2.4 Quản lý loại bằng

Quản lý đơn vị đào tạo quản lý các loại bằng có thể cấp phát cho sinh viên từ trường đại học

4.2.2.4.1 Màn hình quản lý loại bằng

ID	Tên	Type	Cấp bậc	Ngày tạo	Tùy chỉnh
646a21894bc349a24a162718	Bằng cử nhân Công nghệ...	Văn bằng	0	21/05/2023	
6468ae977b226854496d5566	Bằng cử nhân Hóa học Ủ...	Văn bằng	0	20/05/2023	
64523490f5727982980572e4	Bằng cử nhân QTKD	Văn bằng	0	03/05/2023	
6452347f5727982980572df	Bằng cử nhân HHUD	Văn bằng	0	03/05/2023	
6452346f5727982980572c4	Bằng cử nhân CNSH	Văn bằng	0	03/05/2023	
6452345c15727982980572bf	Bằng cử nhân QHQT	Văn bằng	0	03/05/2023	
64523446f5727982980572a4	Bằng cử nhân NNA	Văn bằng	0	03/05/2023	
6452349f57279829805729f	Bằng cử nhân CNTT	Văn bằng	0	03/05/2023	
644d55046ae0f930f78151d	Bằng Cử Nhân Nhan	Văn bằng	1	29/04/2023	
644d54e98ae0f930f78150f	Bằng Cử Nhân Nhan	Văn bằng	0	29/04/2023	

Hình 4.12 Màn hình quản lý loại bằng

4.2.2.4.2 Màn hình tạo / chỉnh sửa loại bằng

ID	Tên	Type	Cấp bậc	Ngày tạo	Tùy chỉnh
645a218940c349a24a182718	Bằng cử nhân Công nghệ	văn bằng	0	21/05/2023	
645bae977f2265d4496d5d568	Bằng cử nhân Hóa học U...	văn bằng	0	20/05/2023	
645234905727982980572a4	Bằng cử nhân QTKD	văn bằng	0	03/05/2023	
6452347f57279802980572df	Bằng cử nhân Luật	văn bằng	0	03/05/2023	
64523466f727982980572c4	Bằng...	bằng	0	03/05/2023	
6452345cf727982980572f	Bằng...	bằng	0	03/05/2023	
64523440f727982980572a4	Bằng...	bằng	0	03/05/2023	
64523439f7279829805729f	Bằng...	bằng	0	03/05/2023	
64405f90548aeab95077b151d	Bằng Cửu Nhan	văn bằng	1	29/04/2023	
64405f495aeab95077b150f	Bằng Cửu Nhan	văn bằng	0	29/04/2023	

Hình 4.13 Màn hình tạo / chỉnh sửa loại bằng

4.2.2.5 Quản lý năm tốt nghiệp

Năm tốt nghiệp cũng được quản lý trường quản lý

4.2.2.5.1 Màn hình quản lý năm tốt nghiệp

ID	Năm	Ngày tạo
646a21924bc349a24a182724	2019	21/05/2023
644d2e54e9e9498095148065	2026	29/04/2023
6447e91e19fd8e42a4c4d2c8	2025	25/04/2023
64416c42c01d51205a2f7cd	2024	20/04/2023
6420a1134295959e902030c9	2030	05/04/2023
6429706d90acedf12d6519be	2023	02/04/2023

Hình 4.14 Màn hình quản lý năm tốt nghiệp

4.2.2.5.2 Màn hình tạo/chỉnh sửa năm tốt nghiệp

The screenshot shows a modal dialog box in the center of a web application. The dialog has a title bar with 'Hàm tốt nghiệp' and a close button 'X'. It contains a single input field with the value '2023' and two buttons: 'LƯU' (Save) and a small icon. In the background, there is a table listing graduation years (ID, Năm, Ngày tạo). The table includes rows for 2019, 2026, 2025, 2024, 2030, and 2023. The row for 2023 is highlighted. The application header includes 'Trang chủ' and 'Tài khoản'.

Hình 4.15 Màn hình tạo năm tốt nghiệp

4.2.2.6 Quản lý văn bằng chứng chỉ

Quản lý đơn vị đào tạo chọn trường để có thể xem các văn bằng đã cấp của từng trường

4.2.2.6.1 Màn hình quản lý văn bằng chứng chỉ

The screenshot shows a grid of certificate details. Each row contains a card with 'Mã trường' and 'Trường'. The cards are arranged in three columns. Row 1: Mã trường 914874821287 (Trường: Hồng Bang), Mã trường 524129954253 (Trường: VNU). Row 2: Mã trường 799413539199 (Trường: HUTECH), Mã trường 996905764697 (Trường: TSA). Row 3: Mã trường 765404871997 (Trường: ENU), Mã trường 636945697961 (Trường: HUFI). Row 4: Mã trường 450348276533 (Trường: HUFLIT), Mã trường 112117547602 (Trường: Trần Thành Long). Row 5: Mã trường 112117547462 (Trường: Trần Thành Long), Mã trường 112017547462 (Trường: Trần Thành Long). The application header includes 'Trang chủ' and 'Tài khoản'.

Hình 4.16 Màn hình quản lý văn bằng chứng chỉ

4.2.2.6.2 Màn hình văn bằng chứng chỉ của một trường

The screenshot shows a search interface for degree certificates. On the left, there are filters for 'Tài khoản', 'Hồ sơ người nhận', 'Loại bằng', 'Năm tốt nghiệp', and 'Văn bằng chứng chỉ'. The main area displays a table titled 'VĂN BẰNG CHỨNG CHỈ' with columns: ID, Mã học sinh, Mã trường, Tên học sinh, Số vào sổ, Số hiệu, Trường, Năm tốt nghiệp, Ngày tạo, and a search bar. Two certificates are listed:

ID	Mã học sinh	Mã trường	Tên học sinh	Số vào sổ	Số hiệu	Trường	Năm tốt nghiệp	Ngày tạo
646a31b440c349a24a182a38	678778773657	914874821287	Charlotte Taylor	0	0	Hong Bang	2023	21/05/2023
646a300548bc349a24a1829ee	646914419259	914874821287	Evelyn Taylor	0	0	Hong Bang	2023	21/05/2023

At the bottom right, there is a page number '1-10 of 10' and navigation arrows.

Hình 4.17 Màn hình văn bằng chứng chỉ của một trường

4.2.3 Trường

Trường đóng vai trò cấp phát, nhập số vào sổ, cũng như tạo tài khoản cho sinh viên và quản lý khóa tốt nghiệp trong hệ thống.

4.2.3.1 Quản lý tài khoản sinh viên

4.2.3.1.1 Màn hình quản lý tài khoản sinh viên

The screenshot shows a search interface for student accounts. On the left, there are filters for 'Tài khoản', 'Hồ sơ người nhận', 'Khóa tốt nghiệp', and 'Văn bằng chứng chỉ'. The main area displays a table titled 'TÀI KHOẢN' with columns: ID, CMND, Tên, Email, Giới tính, Dân tộc, Ngày sinh, Nơi sinh, Ngày tạo, and Tùy chỉnh. A 'Search' bar is also present. A large number of student accounts are listed, each with a unique ID and personal details.

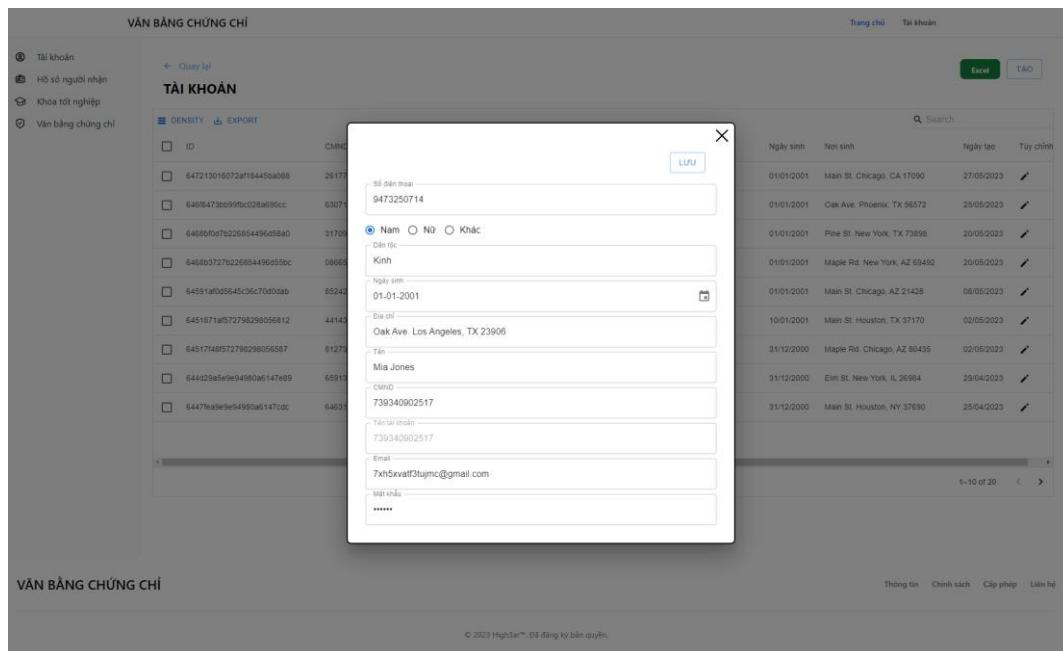
ID	CMND	Tên	Email	Giới tính	Dân tộc	Ngày sinh	Nơi sinh	Ngày tạo	Tùy chỉnh
646f8473b059fb028a690cc	630712645411	Mia Wilson	08vnvnfdwqe276g@gmail...	Nam	Kinh	01/01/2001	Oak Ave, Phoenix, TX 56572	25/05/2023	
6468bf0d7b226854496d58a0	317097422195	Amelia Johnson	yfew4xehobtib@gmail...	Nam	Kinh	01/01/2001	Pine St. New York, TX 73898	20/05/2023	
6468b372b226854496d58bc	086659937506	Olivia Miller	8bn2ip61jr4vqt2@gmail...	Nam	Kinh	01/01/2001	Maple Rd. New York, AZ 69492	20/05/2023	
64591af055645c06c770d0ab	852420756980	Olivia Moore	4wst0nfguvvg4c@gmail...	Nam	Kinh	01/01/2001	Main St. Chicago, AZ 21428	08/05/2023	
6451871af572798298056812	4411431717267	Ava Brown	j0gmi0opkv4l2bf@gmail.c...	Nam	Kinh	10/01/2001	Main St. Houston, TX 37170	02/05/2023	
64517148f572798298056587	812732153442	Isabella Wilson	17ngvum7o4ll7p@gmail...	Nam	Kinh	31/12/2000	Maple Rd. Chicago, AZ 80435	02/05/2023	
644d29a5e9e94980a6147e89	659138251720	Ava Jones	nxz2rhjyz8k1ku@gmail.c...	Nam	Kinh	31/12/2000	Em St. New York, IL 26984	29/04/2023	
6447fea9e9e94980a6147cdc	646317346612	Mia Williams	b54xd909twsg@gmail...	Nam	Kinh	31/12/2000	Main St. Houston, NY 37690	25/04/2023	

At the bottom right, there is a page number '1-10 of 20' and navigation arrows.

Hình 4.18 Màn hình quản lý tài khoản sinh viên

4.2.3.1.2 Màn hình tạo/ chỉnh sửa tài khoản sinh viên

Dữ liệu sinh viên sau khi đã có hồ sơ người nhận sẽ không thể chỉnh sửa để giữ tính đúng đắn trên Blockchain



Hình 4.19 Màn hình tạo/ chỉnh sửa tài khoản sinh viên

4.2.3.2 Quản lý hồ sơ người nhận

Hồ sơ người nhận sẽ được tạo bởi trường.

Hồ sơ người nhận được quản lý đơn vị đào tạo cấp số hiệu sau đó trường sẽ cấp số vào sổ

Khi hồ sơ người nhận đã có đủ số hiệu và số vào sổ thì hồ sơ có thể được trường cấp phát thành văn bằng / chứng chỉ trên Blockchain

4.2.3.2.1 Màn hình quản lý hồ sơ người nhận

Trường có thể nhập hồ sơ người nhận hoặc nhập dữ liệu từ excel để tạo nhiều hồ sơ người nhận

VĂN BẰNG CHỨNG CHỈ

Tài khoản
Hồ sơ người nhận
Khóa tốt nghiệp
Văn bằng chứng chỉ

[← Quay lại](#)

HỒ SƠ NGƯỜI NHẬN

Số vào sổ	Số hiệu
Chưa nhập	Chưa nhập

DENSITY EXPORT

ID	Mã học sinh	Mã trường	Tên học sinh	Số vào sổ	Số hiệu	Trường	Năm tốt nghiệp	Ngày tạo	Tùy chỉnh
647213616072af18445ba0bc	261774782210	592560749767	Isabella Miller			HUFLIT	2023	27/05/2023	<input checked="" type="checkbox"/> SỐ VÀO SỔ

Search:

1-10 of 10 < >

Nhập hồ sơ Nhập số vào sổ TẠO

VĂN BẰNG CHỨNG CHỈ

Thông tin Chính sách Cấp phép Liên hệ

© 2023 High3ar™. Đã đăng ký bản quyền.

Hình 4.20 Màn hình quản lý hồ sơ người nhận

4.2.3.2.2 Màn hình tạo/chỉnh sửa hồ sơ người nhận

VĂN BẰNG CHỨNG CHỈ

Tài khoản
Hồ sơ người nhận
Khóa tốt nghiệp
Văn bằng chứng chỉ

[← Quay lại](#)

HỒ SƠ NGƯỜI NHẬN

Số vào sổ	Số hiệu
Chưa nhập	Chưa nhập

DENSITY EXPORT

ID	Mã hồ sơ	Mã trường	Năm tốt nghiệp	Ngày tạo	Tùy chỉnh
647213616072af18445ba0bc	DAC527780	HUFLIT	2023	27/05/2023	<input checked="" type="checkbox"/> SỐ VÀO SỔ

© 2023 High3ar™. Đã đăng ký bản quyền.

Lưu

Mã hồ sơ: DAC527780

Giới tính: Nam

Tên học sinh:

Mã học sinh:

Mã tài khoản đại học: 592560749767

Trường đại học:

Ngày sinh: DD-MM-YYYY

Nơi sinh:

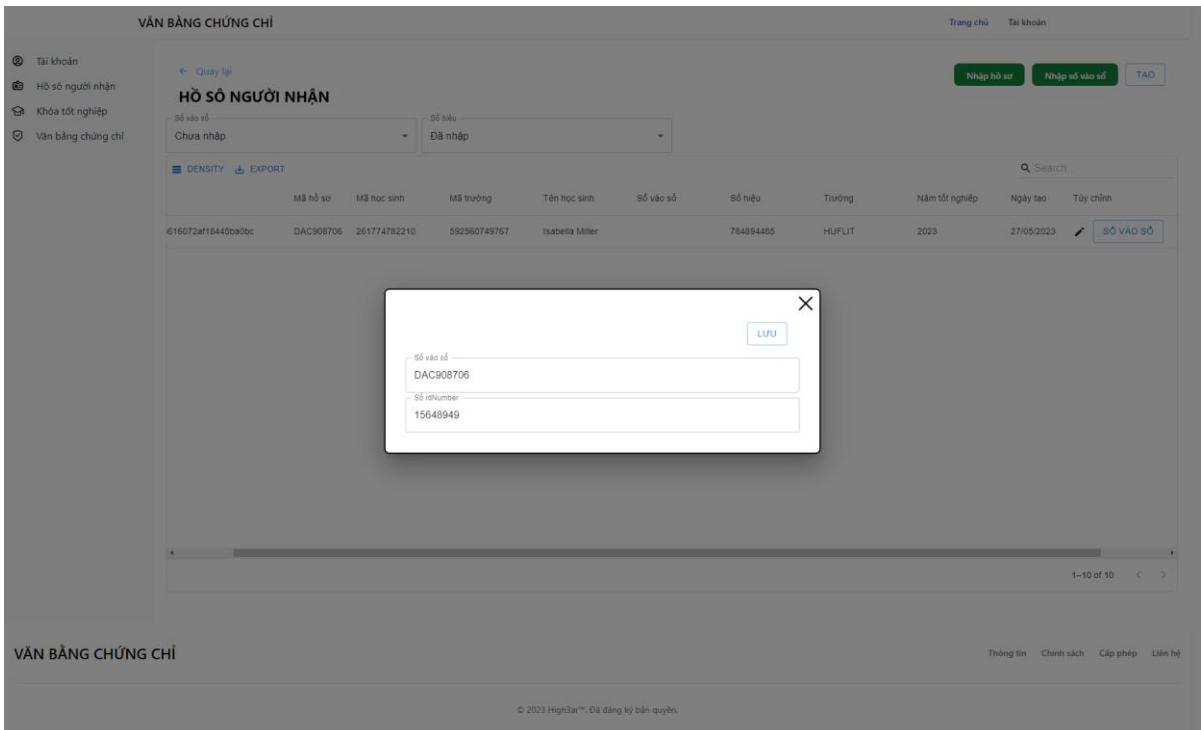
Dân tộc: Kinh

Khoa:

Ngành:

Thông tin Chính sách Cấp phép Liên hệ

Hình 4.21 Màn hình tạo/chỉnh sửa hồ sơ người nhậnMàn hình cấp số vào sổ

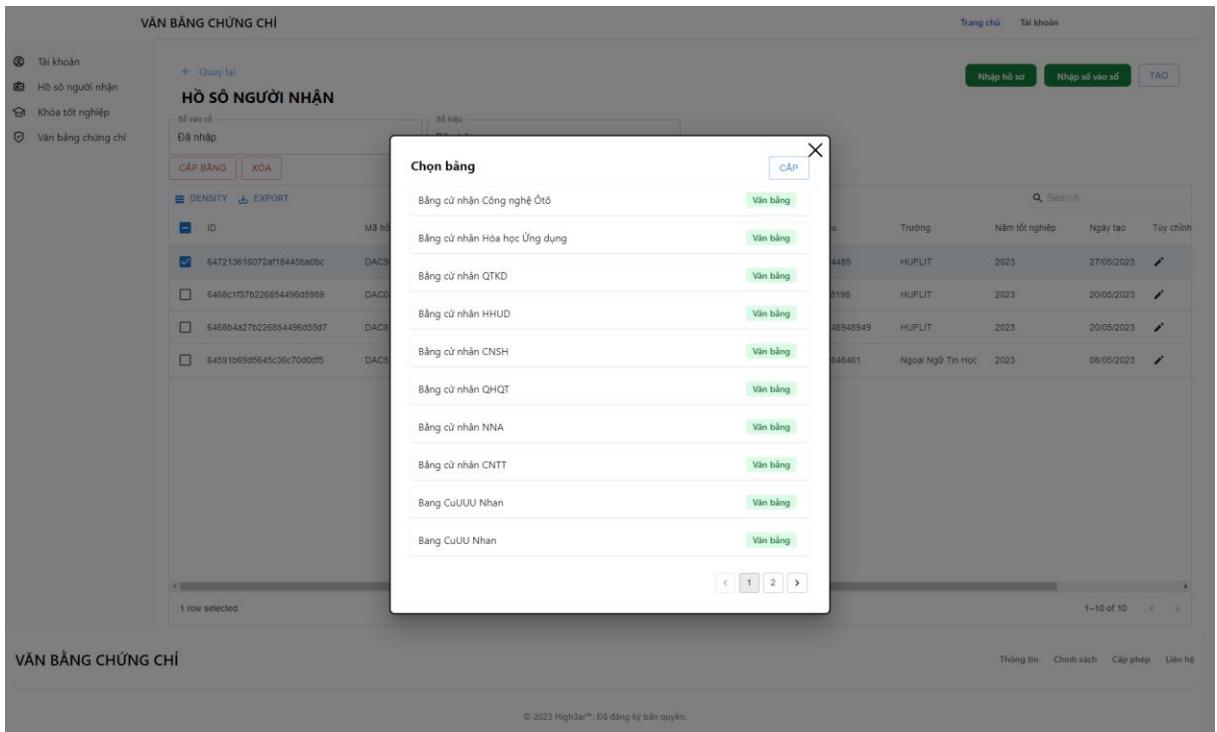


Hình 4.22 Màn hình cấp số vào sổ

4.2.3.2.3 Màn hình cấp văn bằng / chứng chỉ

Văn bằng được quản lý đơn vị đào tạo tạo và quản lý.

Trường thực hiện cấp phát bằng cho Sinh viên



Hình 4.23 Màn hình cấp văn bằng / chứng chỉ

4.2.3.3 Quản lý khóa tốt nghiệp

Trường trực tiếp quản lý khóa tốt nghiệp của chính đơn vị đây.

4.2.3.3.1 Màn hình quản lý khóa tốt nghiệp

ID	Tên	Ngày bắt đầu	Ngày kết thúc	Ngày tạo	Tùy chỉnh
646a22694bc349a24a182753	Khóa tốt nghiệp 2019-2023	21/05/2019	21/05/2023	21/05/2023	<input checked="" type="checkbox"/>
64ad2917e9e94980a6147df7	Khóa tốt nghiệp 2023-2024	29/04/2023	30/04/2023	29/04/2023	<input checked="" type="checkbox"/>
6447f4ee9e94980a6147d3e	Khóa tốt nghiệp 2018-2021	12/10/2012	12/12/2013	25/04/2023	<input checked="" type="checkbox"/>
6447f41e9e94980a6147d2f	Khóa tốt nghiệp 2019-2021	12/10/2012	12/12/2013	25/04/2023	<input checked="" type="checkbox"/>

Hình 4.24 Màn hình quản lý khóa tốt nghiệp

4.2.3.3.2 Màn hình tạo / chỉnh sửa khóa tốt nghiệp

Hình 4.25 Màn hình tạo / chỉnh sửa khóa tốt nghiệp

4.2.3.3.3 Màn hình quản lý văn bằng chứng chỉ đã cấp

Trường có thể xem các văn bằng chứng chỉ đã cấp cho sinh viên

VĂN BẰNG CHỨNG CHỈ

Trang chủ Tài khoản

- Tài khoản
- Hồ sơ người nhận
- Khóa tốt nghiệp
- Văn bằng chứng chỉ

[← Quay lại](#)

VĂN BẰNG CHỨNG CHỈ

DENSITY EXPORT

Search

<input type="checkbox"/>	ID	Mã học sinh	Mã trường	Tên học sinh	Số vào số	Số hiệu	Trường	Năm tốt nghiệp	Ngày tạo
<input type="checkbox"/>	647213616072af18445ba0bc	261774782210	592560749767	Isabella Miller	0	0	HUFLIT	2023	27/05/2023
<input type="checkbox"/>	6468c1f57b225854496d5989	317097422195	592560749767	Amelia Johnson	0	0	HUFLIT	2023	20/05/2023
<input type="checkbox"/>	64680fa27b226854496d55a7	086659837506	592560749767	Olivia Miller	0	0	HUFLIT	2023	20/05/2023
<input type="checkbox"/>	64591b69d9645c36c70d0df5	852420756980	592560749767	Olivia Moore	0	0	Ngoại Ngữ Tin Học	2023	08/05/2023
<input type="checkbox"/>	645236a1f57279629805744f	441431717267	592560749767	Ava Brown	0	0	Ngoại Ngữ Tin Học	2023	03/05/2023
<input type="checkbox"/>	645188f8f57279829605679	812732153442	592560749767	Isabella Wilson	0	0	Ngoại Ngữ Tin Học	2023	02/05/2023
<input type="checkbox"/>	644e51ecf64b14fb4b974e72	646317346612	592560749767	Mia Williams	0	0	HUFLIT	2023	30/04/2023
<input type="checkbox"/>	644e0fedf64b14fb4b974e81	6591382511720	592560749767	Ava Jones	0	0	HUFLIT	2023	30/04/2023

1-10 of 10 < >

VĂN BẰNG CHỨNG CHỈ

Thông tin Chính sách Cấp phép Liên hệ

© 2023 High3ar™. Đã đăng ký bản quyền.

Hình 4.26 Màn hình quản lý văn bằng chứng chỉ đã cấp

4.2.4 Sinh viên

Sinh viên có thể xác thực văn bằng ở trang chủ hoặc tải PDF, gửi đường dẫn liên kết để xác thực văn bằng hoặc gửi cho các bên yêu cầu xác thực văn bằng.

4.2.4.1 Danh sách văn bằng

4.2.4.1.1 Màn hình danh sách văn bằng

VĂN BẰNG CHỨNG CHỈ

Trang chủ Tài khoản

Danh sách văn bằng

Bảng cử nhân CNTT
Khóa tốt nghiệp 2023-2024
Chia sẻ 
Ngày cập: 27-05-2023

 Đã xác nhận

VĂN BẰNG CHỨNG CHỈ

Thông tin Chính sách Cấp phép Liên hệ

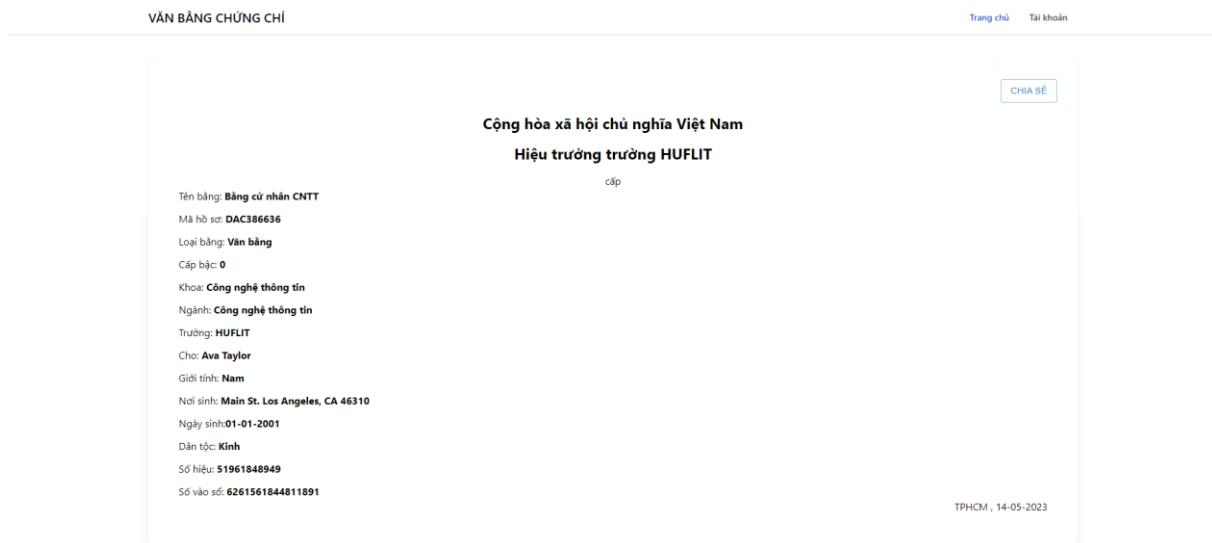
© 2023 High3ar™. Đã đăng ký bản quyền.

Hình 4.27 Màn hình danh sách văn bằng

4.2.4.2 Chi tiết văn bằng

4.2.4.2.1 Màn hình chi tiết văn bằng

Chia sẻ văn bằng gồm 2 bước



VĂN BẰNG CHỨNG CHỈ

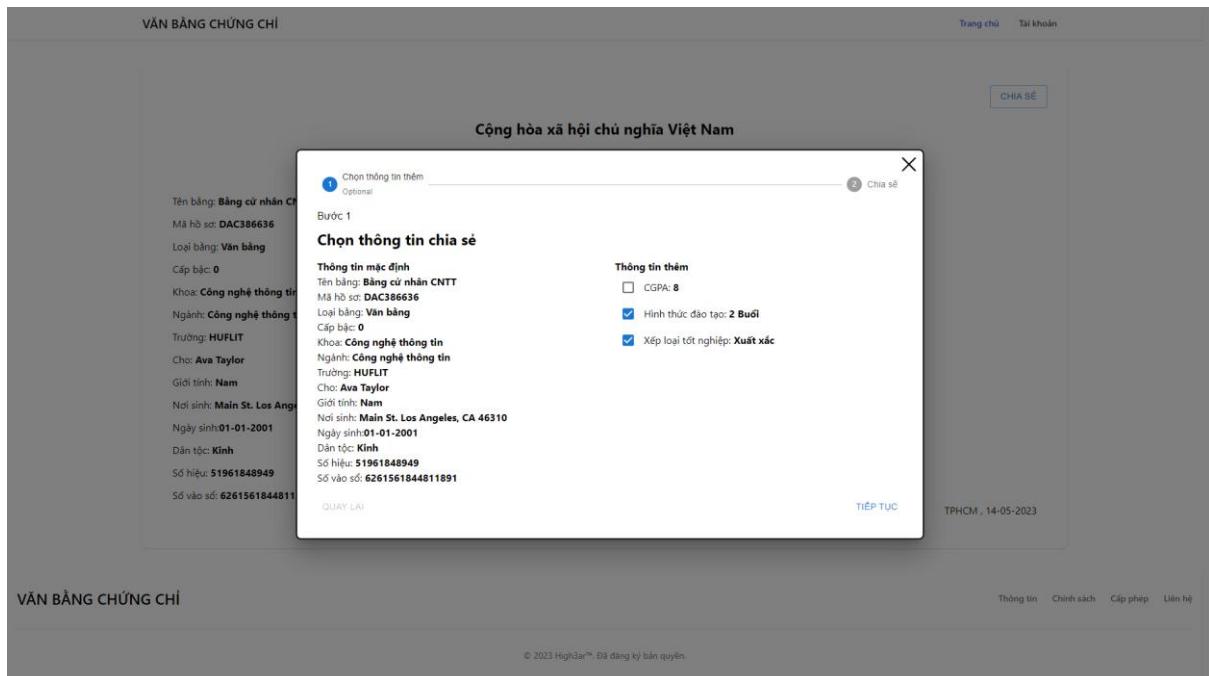
Thông tin Chính sách Cấp phép Liên hệ

© 2023 High3ar™. Đã đăng ký bản quyền.

Hình 4.28 Màn hình chi tiết văn bằng

4.2.4.2.2 Màn hình chọn thông tin chia sẻ văn bằng

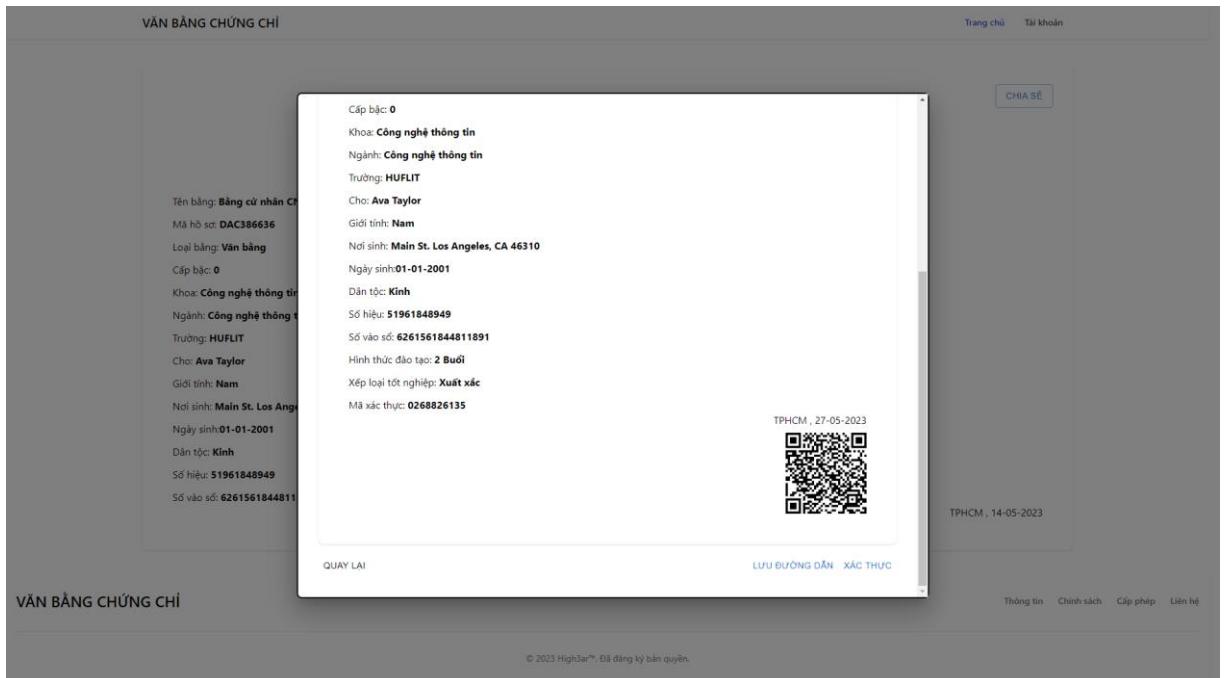
- Bước 1: Chọn thông tin thêm



Hình 4.29 Màn hình chọn thông tin chia sẻ văn bằng

4.2.4.2.3 Màn hình chia sẻ văn bằng thông qua file PDF, đường dẫn hoặc mã QR

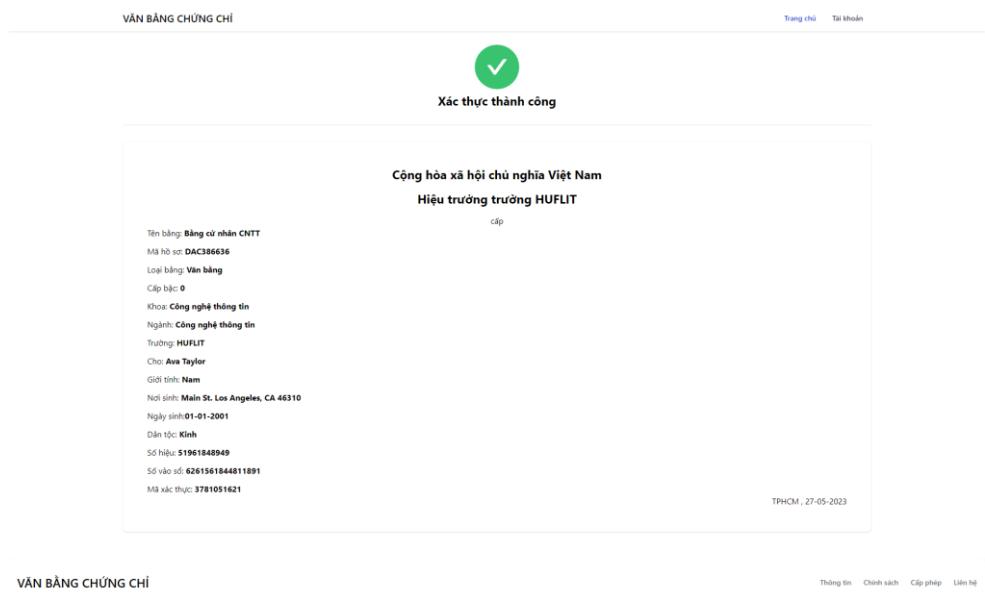
- Bước 2: Sinh viên chọn cách để chia sẻ văn bằng (Mã QR, gửi đường dẫn, Gửi PDF hoặc trang chủ văn bằng chứng chỉ) cho bên thứ 3 xác thực



Hình 4.30 Màn hình chia sẻ văn bằng thông qua file PDF, đường dẫn hoặc mã QR

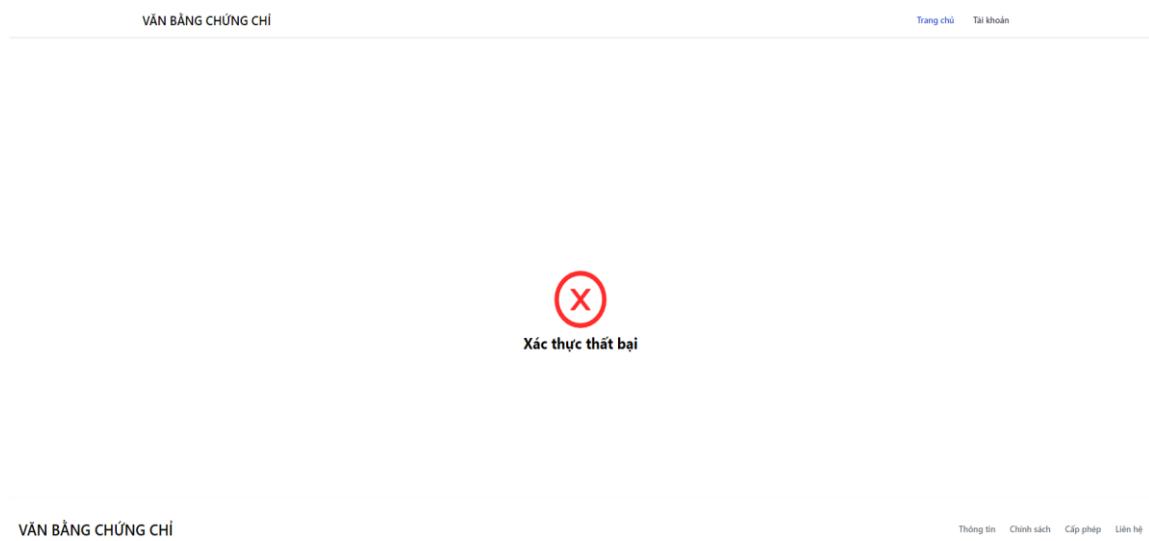
4.2.4.2.4 Màn hình sau khi xác thực thành công thông qua mã QR đường dẫn hoặc mã QR trên file PDF

Nếu thông tin văn bằng chứng chỉ của sinh viên đó được xác thực thành công sẽ hiện màn hình như sau



Hình 4.31 Màn hình sau khi xác thực thành công thông qua mã QR đường dẫn hoặc mã QR trên file PDF

4.2.4.2.5 Màn hình sau khi xác thực thất bại thông qua mã QR đường dẫn hoặc mã QR trên file PDF



Hình 4.32 Màn hình sau khi xác thực thất bại thông qua mã QR đường dẫn hoặc mã QR trên file PDF

4.2.5 Chức năng tra cứu văn bằng/ chứng chỉ

4.2.5.1 Màn hình tra cứu văn bằng chứng chỉ

Chức năng tra cứu văn bằng/ chứng chỉ giúp người dùng có thể nhanh chóng xác thực văn bằng/ chứng chỉ của sinh viên ngay trên trang chủ

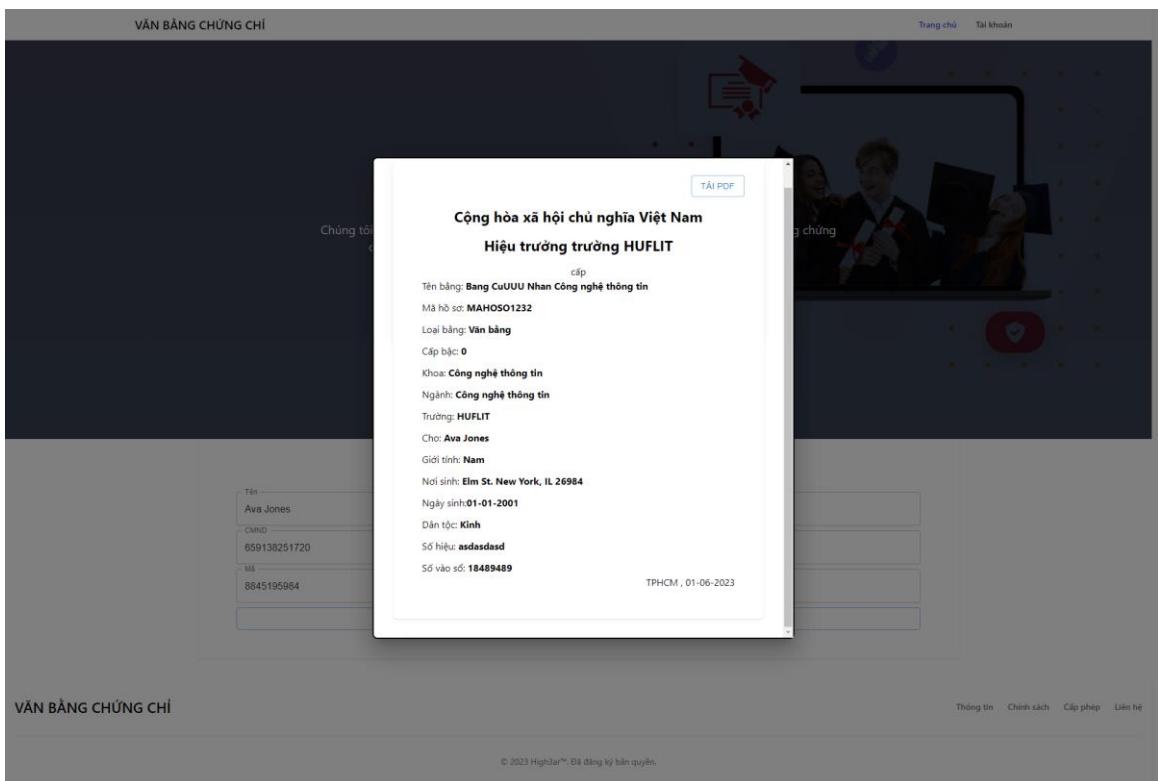
a) Nhập thông tin tra cứu

The screenshot shows a search interface for document verification. At the top, there is a banner with the text 'Văn bằng chứng chỉ' and a subtext: 'Chúng tôi mang đến một giải pháp hoàn toàn mới trong việc xác thực và lưu trữ văn bằng chứng chỉ số. Công bằng - Minh bạch - Uy tín đã làm nên thương hiệu của chúng tôi !'. Below the banner are two buttons: 'Liên hệ' and 'Tìm hiểu thêm'. The main area is titled 'Tra cứu văn bằng chứng chỉ' and contains input fields for 'Tên' (Name), 'CMND' (ID Card), and 'MS' (MSSV). The 'Tên' field contains 'Ava Jones', the 'CMND' field contains '659138251720', and the 'MS' field contains '8845195984'. A large 'TRA CỨU' button is located at the bottom of the input area. The bottom of the screen has a footer with links for 'Thông tin', 'Chính sách', 'Cấp phép', and 'Liên hệ'.

Hình 4.33 Màn hình nhập thông tin tra cứu

b) Xác thực thành công

Sau khi xác thực thành công người dùng có thể tải pdf cũng như xem chi tiết văn bằng/ chứng chỉ



Hình 4.34 Màn hình tra cứu thành công

CHƯƠNG 5. KẾT LUẬN

Qua quá trình nghiên cứu, cùng với sự giúp đỡ tận tình của giáo viên hướng dẫn thầy Khánh, khóa luận của chúng em 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. Nghiên cứu tổng quan cơ sở lý thuyết 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. Mật hạn chế của đè tài chúng em là chỉ dùng dịch vụ chứng thư số của Hyperledger Fabric và chứng thư số tự cấp trong hệ thống.
3. Ứng dụng thuật toán merkle tree vào xác thực VBCC đồng thời giảm đi lượt request nhờ vào thuật toán xác minh.

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. 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.

Đè tài còn hạn chế là hệ thống Blockchain triển khai trên một máy, chưa đề xuất được mô hình mạng Blockchain phù hợp yêu cầu phân tán. Định hướng nghiên cứu tiếp theo ngoài những hạn chế trên, chắc chắn đè tài của chúng chúng em còn có nhiều thiếu sót.

Do đó, đè 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 liên quan đến cấp chứng chỉ.
- (3) Cải tiến hệ thống thành microservice giúp hệ thống mạnh mẽ không bị phụ thuộc lẫn nhau.

TÀI LIỆU THAM KHẢO

- [1] Ralph Charles Merkle (1979), “Secrecy, authentication, and public key systems”.
Báo cáo kỹ thuật. <http://www.ralphmerkle.com/papers/Thesis1979.pdf>
- [2] 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.<https://www.sciencedirect.com/science/article/pii/S2096720921000075>.
- [3] Luật giáo dục 2019. <https://luatvietnam.vn/giao-duc/luat-giao-duc-2019-so-43-2019-qh14-175003-d1.html#:~:text=%C4%90i%E1%BB%81u%2012.&text=b%E1%BA%B1ng%2C%20ch%E1%BB%A9ng%20ch%E1%BB%89-,1.,2>
- [4] Điều 3 Thông tư 21/2019/TT-BGDDT <https://thuvienphapluat.vn/van-ban/Giao-duc/Thong-tu-21-2019-TT-BGDDT-quan-ly-bang-tot-nghiep-trung-hoc-trung-cap-su-pham-bang-cao-dang-430050.aspx>
- [5] Điều 5 Nghị định số 30/2020/NĐ-CP <https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Nghi-dinh-30-2020-ND-CP-cong-tac-van-thu-436532.aspx>
- [6] Nghị định Số 45/2020/NĐ-CP <https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-45-2020-ND-CP-thuc-hien-thu-tuc-hanh-chinh-tren-moi-truong-dien-tu-426372.aspx>
- [7] Điều 17 của Quy chế và Điều 19 Thông tư 21/2019/TT-BGDDT.
<https://thuvienphapluat.vn/van-ban/Giao-duc/Thong-tu-21-2019-TT-BGDDT-quan-ly-bang-tot-nghiep-trung-hoc-trung-cap-su-pham-bang-cao-dang-430050.aspx#:~:text=%C4%90i%E1%BB%81u%2019.&text=Tr%C6%B0%E1%BB%9Dng%20h%E1%BB%A3p%20v%C4%83n%20b%E1%BA%B1ng%2C%20ch%E1%BB%A9ng,c%E1%BB%A7a%20v%C4%83n%20b%E1%BA%B1ng%2C%20ch%E1%BB%A9ng%20ch%E1%BB%89>
<https://thuvienphapluat.vn/van-ban/Giao-duc/Thong-tu-21-2019-TT-BGDDT-quan-ly-bang-tot-nghiep-trung-hoc-trung-cap-su-pham-bang-cao-dang-430050.aspx#:~:text=%C4%90i%E1%BB%81u%2019.&text=Tr%C6%B0%E1%BB%9Dng%20h%E1%BB%A3p%20v%C4%83n%20b%E1%BA%B1ng%2C%20ch%E1%BB%A9ng,c%E1%BB%A7a%20v%C4%83n%20b%E1%BA%B1ng%2C%20ch%E1%BB%A9ng%20ch%E1%BB%89>
- [8] 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.

- [9] Christof Paar và Jan Pelzl (2009), Understanding Cryptography: A Textbook for Students and Practitioners (Springer Publishing Company, Incorporated), 1st edition, ISBN 3642041000.<https://link.springer.com/book/10.1007/978-3-642-04101-3>
- [10] Hyperledger Fabric: Blockchain with Hyperledger Fabric - Second Edition by Nitin Gaur, Anthony O'Dowd, Petr Novotny, Luc Desrosiers, Venkatraman Ramakrishna, Salman A. Baset
<https://www.oreilly.com/library/view/Blockchain-with-hyperledger/9781839218750/>
- [11] Merkle Tree: Compact Merkle Multiproofs by Lum Ramabaja and Arber Avdullahu
https://www.researchgate.net/publication/339350196_Compact_Merkle_Multiproofs
- [12] NodeJS: Beginning NodeJS
<https://edu.anarchocopy.org/Programming%20Languages/Node/BEGINNING%20NODEJS.pdf>
- [13] ExpressJS: Beginning Node.js, Express & MongoDB by Greg Lim
- [14] Docker: THE DOCKER & CONTAINER ECOSYSTEM by Itarun Pitimon
https://www.academia.edu/18830429/The_Docker_and_Container_Ecosystem
- [15] NextJS: The Next.js Handbook by Flavio Copes.<https://flaviocopes.com/nextjs/>
- [16] MongoDB: MongoDB Fundamentals: A hands-on guide to using MongoDB and Atlas in the real world - by Amit Phaltankar, Juned Ahsan, Michael Harrison, Liviu Nedov
<https://www.perlego.com/book/2059687/mongodb-fundamentals-a-hands-on-guide-to-using-mongodb-and-atlas-in-the-real-world-pdf>
- [17] Jenkins: Jenkins: The Definitive Guide by John Ferguson