

ĐẠI HỌC CẦN THƠ
TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG



LUẬN VĂN TỐT NGHIỆP

Đề Tài

**XÂY DỰNG HỆ THỐNG QUẢN LÝ DỮ LIỆU HỌC TẬP VÀ
CẤP PHÁT VĂN BẰNG SỐ DỰA TRÊN BLOCKCHAIN**

Cán bộ hướng dẫn
PGS. TS. Phan Thượng Cang

Sinh viên thực hiện
Họ tên: Lê Hải Đăng
MSSV: B2203716
Ngành: An Toàn Thông Tin
Khóa: 48

Học kỳ 1, năm học 2025 - 2026

ĐẠI HỌC CẦN THƠ
TRƯỜNG CÔNG NGHỆ THÔNG TIN
VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

**XÁC NHẬN CHỈNH SỬA LUẬN VĂN
THEO YÊU CẦU CỦA HỘI ĐỒNG**

Tên luận văn (tiếng Việt và tiếng Anh): **Xây dựng hệ thống quản lý dữ liệu học tập và cấp phát văn bằng số dựa trên Blockchain - Design and Implementation of a Blockchain-Enabled System for Learning Data and Digital Diploma Management**

Họ tên sinh viên: Lê Hải Đăng

MASV: B2203716

Mã lớp: DI22D2A1

Đã báo cáo với hội đồng ngành: An toàn thông tin

Ngày báo cáo: 23/12/2025

Luận văn đã được chỉnh sửa theo góp ý của hội đồng.

Cần Thơ, ngày ... tháng ... năm 2025

Giáo viên hướng dẫn

Phan Thượng Cang

LỜI CẢM ƠN

Để đạt được kết quả nghiên cứu như ngày hôm nay, em xin bày tỏ lòng biết ơn sâu sắc đến Thầy Phan Thượng Cang, giảng viên Khoa Mạng Máy Tính của Trường Công nghệ Thông tin và Truyền thông - Đại học Cần Thơ. Thầy đã tận tình hướng dẫn, định hướng và luôn đồng hành cùng em trong suốt quá trình thực hiện đề tài. Những góp ý quý báu và sự hỗ trợ của Thầy là nền tảng quan trọng giúp em hoàn thành tốt nhiệm vụ hoàng thành luận văn tốt nghiệp.

Em cũng xin chân thành cảm ơn quý Thầy Cô Trường Công nghệ thông tin - Đại học Cần Thơ đã nhiệt tình giảng dạy và truyền đạt cho em những kiến thức nền tảng lắn chuyên sâu trong suốt thời gian học tập tại trường. Những kiến thức ấy không chỉ giúp em hoàn thành đề tài mà còn là hành trang quý giá cho con đường học thuật và nghề nghiệp sau này.

Bên cạnh đó, em xin gửi lời tri ân đến gia đình và bạn bè, những người luôn ở bên động viên, khích lệ tinh thần và tạo điều kiện thuận lợi để em có thể tập trung nghiên cứu và hoàn thành tốt luận văn.

Mặc dù đã nỗ lực hết mình để hoàn thiện đề tài một cách chỉnh chu nhất, nhưng do giới hạn về thời gian, kinh nghiệm nghiên cứu còn hạn chế nên đề tài khó tránh khỏi những thiếu sót. Em rất mong nhận được sự góp ý của Quý Thầy Cô để đề tài được hoàn thiện hơn trong tương lai.

Em xin trân trọng cảm ơn và kính chúc Quý Thầy Cô luôn dồi dào sức khỏe, hạnh phúc và thành công trong sự nghiệp giáo dục.

Cần Thơ, ngày ... tháng ... năm 2025
Sinh viên thực hiện

Lê Hải Đăng

TÓM TẮT

Trong bối cảnh chuyển đổi số giáo dục, hầu hết các trường đại học đã triển khai hệ thống quản lý đào tạo trực tuyến nhưng vẫn dựa trên mô hình cơ sở dữ liệu tập trung, tiềm ẩn nguy cơ gian lận điểm số, chỉnh sửa trái phép kết quả học tập và làm giả văn bằng. Những hạn chế này đặt ra yêu cầu cấp thiết về một giải pháp công nghệ đảm bảo tính toàn vẹn dữ liệu, minh bạch và khả năng xác thực độc lập trong quản lý thông tin học tập và cấp phát văn bằng.

Đề tài “**Xây dựng hệ thống quản lý dữ liệu học tập và cấp phát văn bằng số dựa trên Blockchain**” tập trung nghiên cứu cơ sở lý thuyết về công nghệ blockchain (cấu trúc khối, cơ chế đồng thuận, Merkle Tree, hợp đồng thông minh), khảo sát các mô hình ứng dụng trong và ngoài nước, từ đó đề xuất mô hình hệ thống quản lý điểm và văn bằng trên nền tảng Ethereum (EVM). Trên cơ sở đó, luận văn thiết kế kiến trúc hệ thống, xây dựng các smart contract và phát triển một ứng dụng web prototype cho phép: quản lý chương trình đào tạo, tạo tài khoản sinh viên và cán bộ quản lý điểm, nhập và lưu trữ kết quả học tập, tự động xét tốt nghiệp, cấp phát và xác thực văn bằng số thông qua blockchain.

Hệ thống được triển khai và kiểm thử trên mạng blockchain cục bộ sử dụng Ganache và Truffle với dữ liệu mô phỏng. Kết quả cho thấy mô hình đề xuất có khả năng đảm bảo tính bất biến của dữ liệu điểm số, hỗ trợ xác thực văn bằng một cách nhanh chóng và công khai, đồng thời tạo điều kiện để sinh viên chủ động quản lý và chia sẻ hồ sơ học tập của mình. Luận văn đồng thời chỉ ra một số hạn chế về môi trường thử nghiệm và phạm vi chức năng, qua đó đề xuất hướng phát triển mở rộng trên các mạng Ethereum testnet/public và tích hợp thêm các nghiệp vụ đào tạo khác trong tương lai.

ABSTRACT

In the context of digital transformation in higher education, most universities have adopted online training management systems that still rely on centralized databases, which are vulnerable to grade manipulation, unauthorized modification of academic results, and diploma forgery. These limitations highlight the urgent need for a technological solution that ensures data integrity, transparency, and independent verification in managing academic records and issuing diplomas.

This thesis, entitled “**Design and Implementation of a Blockchain-Enabled System for Learning Data and Digital Diploma Management**”, investigates the theoretical foundations of blockchain technology (block structure, consensus mechanisms, Merkle Tree, smart contracts) and surveys related applications in Vietnam and worldwide. Based on this analysis, the thesis proposes a system model built on the Ethereum (EVM) platform for managing student grades and diplomas. The proposed architecture is then implemented through a set of smart contracts and a prototype web application that supports key processes such as training program management, account provisioning for students and academic staff, grade submission and on-chain storage, automatic graduation evaluation, as well as issuance and verification of digital diplomas via blockchain.

The system is deployed and tested on a local blockchain network using Ganache and Truffle with simulated data. Experimental results demonstrate that the proposed model can preserve the immutability of academic records, enable fast and publicly verifiable diploma authentication, and allow students to securely manage and share their learning achievements. The thesis also discusses current limitations regarding the test environment and functional scope, and outlines future directions such as deploying on Ethereum testnets or public networks and extending the model to additional academic processes.

DANH MỤC HÌNH

Hình 2.1 Lịch sử hình thành và phát triển của blockchain	9
Hình 2.2 Công nghệ blockchain	13
Hình 2.3 Cấu trúc khối của blockchain	14
Hình 2.4 Cơ chế liên kết thông qua hàm băm của blockchain	15
Hình 2.5 Cây Merkle	16
Hình 2.6 Hàm băm	17
Hình 2.7 Quy trình mã hóa và giải mã trong hệ mật mã khóa công khai	18
Hình 2.8 Quy trình ký số và xác thực chữ ký số	19
Hình 2.9 Kiến Trúc Phân Lớp Của Blockchain	20
Hình 2.10 Luồng hoạt động của Blockchain	24
Hình 2.11 Cơ chế Hash Block chống sửa đổi trong Blockchain	27
Hình 2.12 Hash Chaining: cơ chế chống sửa đổi dữ liệu trong blockchain	27
Hình 2.13 Phân loại blockchain theo quyền truy cập	31
Hình 2.14 Ethereum	34
Hình 2.15 Solidity	37
Hình 2.16 Truffle	38
Hình 2.17 Ganache	40
Hình 2.18 Ví Metamask	41
Hình 3.1 Mô hình kiến trúc tổng quan hệ thống	44
Hình 3.2 Luồng xử lý nghiệp vụ trong hệ thống quản lý dữ liệu học tập của sinh viên	45
Hình 3.3 Cấu trúc chuỗi block lưu trữ hồ sơ học tập của sinh viên	46
Hình 3.4 Cấu trúc dữ liệu cho các khối blockchain	47
Hình 3.5 Sơ đồ use case tổng quát	49
Hình 3.6 Sơ đồ use case của actor Admin	50
Hình 3.7 Sơ đồ use case của actor Cán bộ quản lí điểm	51
Hình 3.8 Sơ đồ use case của actor Sinh viên	52
Hình 3.9 Giao diện "Đăng nhập"	65
Hình 3.10 Giao diện upload chương trình đào tạo và gán chương trình đào tạo cho lớp	66
Hình 3.11 Giao diện xem danh sách chương trình đào tạo	66
Hình 3.12 Giao diện tạo tài khoản hàng loạt cho sinh viên	67
Hình 3.13 Giao diện cập nhật thông tin sinh viên	67
Hình 3.14 Giao diện xem danh sách sinh viên	68
Hình 3.15 Giao diện tạo tài khoản cán bộ quản lí điểm	69
Hình 3.16 Giao diện xem danh sách cán bộ quản lí điểm	69
Hình 3.17 Giao diện quản lí nhập điểm	70

Hình 3.18 Giao diện xem điểm đã nhập	70
Hình 3.19 Giao diện danh sách xét tốt nghiệp	71
Hình 3.20 Giao diện xem danh sách sinh viên tốt nghiệp	72
Hình 3.21 Giao diện trang sinh viên.....	73
Hình 3.22 Giao diện điểm một học kỳ của sinh viên	74
Hình 3.23 Bằng tốt nghiệp của sinh viên	75
Hình 3.24 Giao diện chia sẻ link xác thực bằng tốt nghiệp.....	75
Hình 3.25 Giao diện trang xác thực của doanh nghiệp	76
Hình 3.26 Thông tin xác thực văn bằng	76

DANH MỤC BẢNG

Bảng 2.1 So sánh một số cơ chế đồng thuận phổ biến trong blockchain	25
Bảng 2.2 So sánh giữa Ethereum và Hyperledger Fabric	33
Bảng 3.1 Danh sách các bảng dữ liệu trong hệ thống	48
Bảng 3.2 Bảng mô tả chức năng Đăng nhập	53
Bảng 3.3 Bảng mô tả chức năng Quản lý chương trình đào tạo	54
Bảng 3.4 Bảng mô tả chức năng Quản lý tài khoản sinh viên	56
Bảng 3.5 Bảng mô tả chức năng Quản lý tài khoản cán bộ quản lý điểm	58
Bảng 3.6 Bảng mô tả chức năng Cập nhật điểm	59
Bảng 3.7 Xem điểm sinh viên	60
Bảng 3.8 Bảng mô tả chức năng Quản lý sinh viên tốt nghiệp	61
Bảng 3.9 Bảng mô tả chức năng Xem thông tin cá nhân	62
Bảng 3.10 Bảng mô tả chức năng Xem hồ sơ học tập.....	62
Bảng 3.11 Bảng mô tả chức năng Đăng ký xét tốt nghiệp	63
Bảng 3.12 Bảng mô tả chức năng Xác thực bằng tốt nghiệp	64
Bảng 4.1 Bảng trường hợp kiểm thử Admin tạo mới chương trình đào tạo	79
Bảng 4.2 Bảng trường hợp kiểm thử Admin gán chương trình đào tạo với lớp	80
Bảng 4.3 Bảng trường hợp kiểm thử Admin tạo tài khoản sinh viên hàng loạt.....	81
Bảng 4.4 Bảng trường hợp kiểm thử Admin tạo tài khoản cho cán bộ quản lý điểm.....	82
Bảng 4.5 Bảng trường hợp kiểm thử Admin thu hồi tài khoản cán bộ quản lý điểm	82
Bảng 4.6 Bảng trường hợp kiểm thử Admin xem danh sách sinh viên, cán bộ đã tạo	83
Bảng 4.7 Bảng trường hợp kiểm thử Cán bộ quản lý điểm nhập điểm cho sinh viên	84
Bảng 4.8 Bảng trường hợp kiểm thử Cán bộ quản lý điểm xem điểm sinh viên đã nhập, xem danh sách sinh viên đã ra trường	85
Bảng 4.9 Bảng trường hợp kiểm thử Cán bộ quản lý điểm thu hồi văn bằng sinh viên	85
Bảng 4.10 Bảng trường hợp kiểm thử Sinh viên xem thông tin cá nhân, quá trình học tập	86
Bảng 4.11 Bảng trường hợp kiểm thử Sinh viên đăng ký xét tốt nghiệp.....	86
Bảng 4.12 Bảng trường hợp kiểm thử Sinh viên chia sẻ văn bằng cho doanh nghiệp.....	87
Bảng 4.11 Bảng trường hợp kiểm thử Cán bộ quản lý điểm cấp bằng cho sinh viên.....	87

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Từ đầy đủ	Nghĩa
UML	Unified Modeling Language	Ngôn ngữ mô hình hóa
DID	Decentralized Identifier	Định danh phi tập trung
API	Application Programming Interface	Giao diện lập trình ứng dụng
PoW	Proof of Work	Cơ chế đồng thuận Bằng chứng công việc
PoS	Proof of Stake	Cơ chế đồng thuận Bằng chứng cổ phần
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ
SHA	Secure Hash Algorithm	Thuật toán băm an toàn
BFT	Byzantine Fault Tolerance	Khả năng chịu lỗi Byzantine
TPS	Transactions Per Second	Số giao dịch xử lý mỗi giây
DApps	Decentralized Applications	Ứng dụng phi tập trung
ETH	Ether	Đồng tiền mã hóa của mạng Ethereum
DeFi	Decentralized Finance	Tài chính phi tập trung
NFT	Non-Fungible Token	Token không thể thay thế
DAO	Decentralized Autonomous Organization	Tổ chức tự trị phi tập trung
UI	User Interface	Giao diện người dùng
CLI	Command Line Interface	Giao diện dòng lệnh
RPC	Remote Procedure Call	Gọi thủ tục từ xa (cơ chế giao tiếp giữa các hệ thống/dịch vụ)

MỤC LỤC

CHƯƠNG 1: GIỚI THIỆU	1
I. TỔNG QUAN VỀ ĐỀ TÀI	1
II. NHỮNG NGHIÊN CỨU LIÊN QUAN	2
2.1. Nghiên Cứu Và Ứng Dụng Quốc Tế	2
2.2. Nghiên Cứu Và Thủ Nghiêm Trong Nước	3
2.3. Khoảng Trống Nghiên Cứu	3
III. MỤC TIÊU NGHIÊN CỨU	4
3.1. Mục Tiêu Tổng Quát	4
3.2. Mục Tiêu Cụ Thể	4
IV. ĐỐI TƯỢNG VÀ PHẠM VI NGHIÊN CỨU	5
4.1. Đối Tượng Nghiên Cứu	5
4.2. Phạm Vi Nghiên Cứu	5
V. PHƯƠNG PHÁP NGHIÊN CỨU	6
5.1. Phương Pháp Nghiên Cứu Lý Thuyết	6
5.2. Phân Tích Và Thiết Kế Hệ Thống	6
5.3. Thực Nghiệm Và Triển Khai:	7
5.4. Phương Pháp Đánh Giá	7
VI. Ý NGHĨA KHOA HỌC VÀ THỰC TIỄN	7
6.1. Ý Nghĩa Khoa Học	7
6.2. Ý Nghĩa Thực Tiễn	7
VII. KẾT CÂU LUẬN VĂN	8
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT	9
I. LỊCH SỬ HÌNH THÀNH VÀ PHÁT TRIỂN CỦA BLOCKCHAIN	9
1.1. Nền Tảng Tiền Thân Nhũng Ý Tưởng Khai Sinh Thập niên 1990 - 2008	9
1.2. Blockchain 1.0 Kỷ Nguyên Bitcoin và Tiền Tệ Kỹ Thuật Số (2008-2013)	10
1.3. Blockchain 2.0 Cuộc Cách Mạng Hợp Đồng Thông Minh (2013-2017)	10
1.4. Blockchain 3.0 Hướng Tới Sự Trưởng Thành (2017-Hiện tại)	11
1.5. Blockchain 4.0 Xu hướng tương lai	12
II. TỔNG QUAN VỀ CÔNG NGHỆ BLOCKCHAIN	12
2.1. Khái Niệm Về Công Nghệ Blockchain	12
2.2. Cấu Trúc Cốt Lõi Của Blockchain	14
2.3. Kiến Trúc Phân Lớp Của Blockchain	20
2.4. Các Tính Chất Của Blockchain	23
2.5. Nguyên Lý Hoạt Động Của Blockchain	23

2.6. Cơ Chế Đồng Thuận Của Blockchain	24
2.7. Cơ Chế Chống Sự Thay Đổi	26
III. ƯU VÀ NHƯỢC ĐIỂM CỦA BLOCKCHAIN.....	28
3.1. Ưu Điểm Của Công Nghệ Blockchain.....	28
3.2. Nhược Điểm Của Công Nghệ Blockchain.....	29
IV. ỨNG DỤNG CỦA BLOCKCHAIN CHIẾN LUỢC QUỐC GIA CỦA VIỆT NAM.....	29
V. PHÂN LOẠI BLOCKCHAIN	31
VI. CÁC NỀN TẢNG BLOCKCHAIN	32
VII. ETHEREUM	34
7.1. Giới Thiệu Tổng Quan Về Ethereum	34
7.2. Cấu Trúc Của Ethereum.....	35
7.3. Ứng Dụng Của Ethereum.....	35
7.4. Hợp Đồng Thông Minh.....	35
7.5. Công Cụ và Công Nghệ Hỗ Trợ.....	37
CHƯƠNG 3: XÂY DỰNG HỆ THỐNG QUẢN LÝ DỮ LIỆU HỌC TẬP VÀ CẤP PHÁT VĂN BẰNG SỐ.....	43
I. MÔ TẢ HỆ THỐNG.....	43
II. MỤC TIÊU CỦA HỆ THỐNG.....	43
III. MÔ HÌNH KIẾN TRÚC TỔNG QUAN HỆ THỐNG	44
IV. CẤU TRÚC CHUỖI BLOCK LUU TRỮ HỒ SƠ HỌC TẬP CỦA SINH VIÊN	45
V. THIẾT KẾ CẤU TRÚC DỮ LIỆU CHO CÁC KHỐI BLOCKCHAIN.....	47
VI. SƠ ĐỒ USE CASE VÀ MÔ TẢ CHỨC NĂNG.....	49
6.1. Sơ Đồ Use Case.....	49
6.2. Mô Tả Hệ Thống	53
VII. GIAO DIỆN CHỨC NĂNG	65
7.1. Giao Diện Trang Đăng Nhập	65
7.2. Giao Diện Quản Lý Chương Trình Đào Tạo	66
7.3. Giao Diện Quản Lý Tài Khoản Sinh Viên	67
7.4. Giao Diện Quản Lý Tài Khoản Cán Bộ Quản Lý Điểm	69
7.5. Giao Diện Quản Lý Nhập Điểm.....	70
7.6. Giao Diện Trang Sinh Viên.....	73
7.7. Giao Diện Xác Thực Bằng Tốt Nghiệp.....	76
CHƯƠNG 4: KIỂM THỬ MÔ HÌNH	77

I.	MỤC TIÊU KIÊM THỦ	77
II.	PHẠM VI KIÊM THỦ	77
III.	MÔI TRƯỜNG KIÊM THỦ	78
IV.	KỊCH BẢN KIÊM THỦ	79
4.1.	Trường hợp 1: Admin tạo mới chương trình đào tạo	79
4.2.	Trường hợp 2: Admin gán chương trình đào tạo với lớp.....	80
4.3.	Trường hợp 3: Admin tạo tài khoản sinh viên hàng loạt.	81
4.4.	Trường hợp 4: Admin tạo tài khoản cho cán bộ quản lí điểm	82
4.5.	Trường hợp 5: Admin thu hồi tài khoản cán bộ quản lí điểm.....	82
4.6.	Trường hợp 6: Admin xem danh sách sinh viên, cán bộ đã tạo.....	83
4.7.	Trường hợp 7: Cán bộ quản lí điểm nhập điểm học kỳ cho sinh viên	84
4.8.	Trường hợp 8: Cán bộ quản lí điểm xem điểm sinh viên đã nhập, xem danh sách sinh viên đã ra trường.....	85
4.9.	Trường hợp 9: Cán bộ quản lí điểm thu hồi văn bằng sinh viên.....	85
4.10.	Trường hợp 10: Sinh viên xem thông tin cá nhân, quá trình học tập	86
4.11.	Trường hợp 11: Sinh viên đăng ký xét tốt nghiệp.....	86
4.12.	Trường hợp 12: Sinh viên chia sẻ văn bằng cho doanh nghiệp.....	87
4.13.	Trường hợp 13: Cán bộ quản lí điểm cấp bằng cho sinh viên.....	87
	CHƯƠNG 5: KẾT QUẢ VÀ HƯỚNG PHÁT TRIỂN	88
I.	KẾT QUẢ ĐẠT ĐƯỢC.....	88
II.	ĐÁNH GIÁ HẠN CHẾ	89
III.	HƯỚNG PHÁT TRIỂN	90

CHƯƠNG 1: GIỚI THIỆU

I. TỔNG QUAN VỀ ĐỀ TÀI

Trong những năm gần đây, cùng với sự phát triển mạnh mẽ của công nghệ thông tin, các trường đại học ở Việt Nam đã đẩy mạnh ứng dụng hệ thống quản lý đào tạo trực tuyến nhằm nâng cao hiệu quả giảng dạy và quản lý. Tuy nhiên, việc quản lý điểm số và cấp phát văn bằng thông qua các hệ thống tập trung vẫn bộc lộ nhiều hạn chế. Thực tế cho thấy đã từng xuất hiện những trường hợp **sinh viên xâm nhập trái phép vào hệ thống để thay đổi kết quả học tập**, hoặc **giảng viên có thể điều chỉnh điểm số của sinh viên** vì những lý do chủ quan và khách quan. Bên cạnh đó, tình trạng sửa điểm thủ công trên sổ điểm điện tử, hoặc gian lận trong khâu nhập liệu, đã làm dấy lên nhiều lo ngại về tính minh bạch, công bằng và uy tín của cơ sở giáo dục.

Không chỉ dừng lại ở gian lận điểm số, tình trạng làm **giả văn bằng và chứng chỉ** cũng đang trở thành một vấn nạn nhức nhối. Trên thực tế, không ít trường hợp đã bị phát hiện sử dụng bằng giả để xin việc, thăng chức hoặc đi du học, gây tổn hại nghiêm trọng đến niềm tin của xã hội đối với hệ thống giáo dục. Theo thống kê của Bộ Giáo dục và Đào tạo, mỗi năm có hàng trăm vụ phát hiện liên quan đến văn bằng, chứng chỉ giả từ việc in ấn trái phép đến việc giả mạo thông tin trên văn bằng điện tử. Nhiều đường dây làm bằng giả quy mô lớn đã bị triệt phá, trong đó có những vụ liên quan đến cả cán bộ nhà nước và nhân viên giáo dục. Những vụ việc này không chỉ ảnh hưởng đến danh tiếng của các trường đại học mà còn đe dọa tính công bằng và minh bạch trong xã hội, đặc biệt trong tuyển dụng và đánh giá năng lực.

Chẳng hạn, năm 2014 tại Trường Đại học Quy Nhơn, một chuyên viên Phòng Đào tạo đã xâm nhập cơ sở dữ liệu để nâng điểm cho 71 sinh viên, thu lợi hơn 132 triệu đồng (Vietnamnet, 2014). Trên thế giới, năm 2012, một học sinh trung học ở bang New Hampshire (Mỹ) bị phát hiện hack hệ thống nhà trường để thay đổi điểm số (CBS News, 2012). Không chỉ dừng ở gian lận học tập, tình trạng làm giả văn bằng, chứng chỉ ở Việt Nam cũng ngày càng nghiêm trọng: Công an Quảng Trị triệt phá một đường dây sản xuất bằng cấp giả quy mô lớn, thu giữ hàng chục nghìn phôi và con dấu (VTV News, 2025), trong khi Công an Bắc Giang khởi tố 15 giáo viên vì mua bằng đại học và chứng chỉ giả để hợp thức hóa hồ sơ (Tuổi Trẻ, 2025). Những sự việc này cho thấy gian lận học tập và giả mạo văn bằng không chỉ diễn ra ở Việt Nam mà còn xuất hiện ở nhiều quốc gia khác, phản ánh nguy cơ hiện hữu trong các hệ thống quản lý tập trung, nơi dữ liệu dễ bị thao túng, chỉnh sửa và khó xác thực tính toàn vẹn một cách tuyệt đối.

Từ góc nhìn kỹ thuật, nguyên nhân cốt lõi của những vấn đề này bắt nguồn từ mô hình quản lý tập trung (Centralized Database), trong đó toàn bộ quyền kiểm soát dữ liệu tập

trung vào một máy chủ hoặc một nhóm người quản trị. Khi đó, chỉ cần một tài khoản có đặc quyền cao bị lộ hoặc bị lợi dụng, dữ liệu có thể bị chỉnh sửa, xóa bỏ, hay thay thế mà khó bị phát hiện. Các biện pháp hiện hành như sao lưu dữ liệu, ghi log, hoặc phân quyền truy cập chỉ mang tính phòng ngừa tương đối, không thể đảm bảo tính bất biến tuyệt đối (immutability) và không loại bỏ được điểm yếu quyền lực tập trung.

Trong khi đó, quá trình xác minh tính thật giả của văn bằng ở Việt Nam hiện nay vẫn chủ yếu thực hiện thủ công, dựa trên tra cứu công thông tin hoặc xác nhận qua văn bản hành chính, dẫn đến tốn thời gian và dễ bị giả mạo. Đặc biệt trong bối cảnh hội nhập quốc tế, việc công nhận văn bằng giữa các trường và quốc gia càng trở nên khó khăn do thiếu một cơ chế xác thực số thống nhất và tin cậy.

Từ những bất cập nêu trên, việc nghiên cứu và ứng dụng một công nghệ có khả năng đảm bảo tính toàn vẹn dữ liệu, tính minh bạch, phân tán và chống chỉnh sửa là yêu cầu cấp thiết. Công nghệ Blockchain, với đặc tính bất biến (immutability), phân tán (decentralization) và xác thực công khai (public verifiability), được xem là một hướng tiếp cận khả thi. Khi dữ liệu điểm số và văn bằng được lưu trữ và xác thực trên chuỗi khối, mọi hành vi thay đổi trái phép đều bị loại bỏ do không thể chỉnh sửa bản ghi đã xác nhận. Đồng thời, sinh viên có thể chủ động lưu giữ và chia sẻ hồ sơ học tập trong môi trường số an toàn, còn các bên liên quan (trường học, cơ quan quản lý, nhà tuyển dụng) có thể xác minh nhanh chóng mà không cần qua thủ tục hành chính rườm rà.

Không chỉ dừng lại ở việc phòng chống gian lận, giải pháp này còn mở ra tiềm năng xây dựng hệ sinh thái giáo dục số liên thông và minh bạch, hướng tới chuẩn hóa và công nhận văn bằng giữa các cơ sở giáo dục trong nước và quốc tế.

Xuất phát từ những yêu cầu thực tiễn và triển vọng ứng dụng nêu trên, đề tài “**Xây dựng hệ thống quản lý dữ liệu học tập và cấp phát văn bằng số dựa trên Blockchain**” được lựa chọn nhằm nghiên cứu, đánh giá tính khả thi và xây dựng thử nghiệm một mô hình ứng dụng, góp phần nâng cao tính minh bạch, công bằng và hiện đại hóa công tác quản lý giáo dục tại các trường đại học Việt Nam.

II. NHỮNG NGHIÊN CỨU LIÊN QUAN

Trong những năm gần đây, việc ứng dụng công nghệ Blockchain trong quản lý học tập và cấp phát văn bằng đã được nhiều tổ chức giáo dục, viện nghiên cứu và doanh nghiệp trên thế giới quan tâm triển khai dưới nhiều hình thức khác nhau.

2.1. Nghiên Cứu Và Ứng Dụng Quốc Tế

Trên thế giới, Viện Công nghệ Massachusetts (MIT, Hoa Kỳ) là đơn vị tiên phong triển khai dự án Blockcerts từ năm 2017, hợp tác cùng Learning Machine để cấp phát và

xác minh văn bằng điện tử trên Blockchain Bitcoin theo tiêu chuẩn mở. Mỗi văn bằng được mã hóa và lưu trữ bất biến, giúp người học có thể tự quản lý, chia sẻ và xác minh chứng chỉ của mình mà không cần qua trung gian.

Tại châu Á, Đại học Quốc gia Singapore (NUS) đã phát triển hệ thống OpenCerts, sử dụng Ethereum để xác thực văn bằng điện tử thông qua mã băm công khai. Ở châu Âu, Đại học Woolf cũng áp dụng mô hình tương tự, cấp phát văn bằng dưới dạng NFT và tích hợp định danh phi tập trung (DID) để đảm bảo quyền sở hữu và xác thực học tập.

2.2. Nghiên Cứu Và Thử Nghiệm Trong Nước

Tại Việt Nam, việc ứng dụng blockchain trong giáo dục đang ở giai đoạn nghiên cứu và triển khai thí điểm ban đầu. Nổi bật là chủ trương của Bộ Giáo dục và Đào tạo (GD&ĐT) về kế hoạch xây dựng một nền tảng quốc gia thông nhất để lưu trữ toàn bộ văn bằng, chứng chỉ.

Riêng tại **Trường Công nghệ Thông tin & Truyền thông - Đại học Cần Thơ**, đã có hai công trình nghiên cứu liên quan:

- Luận văn thạc sĩ: “Ứng dụng công nghệ Blockchain trong việc quản lý điểm sinh viên tại trường đại học” - Mai Nguyễn Thủy Trúc (Năm 2024)
- Luận văn đại học: “Xây dựng hệ thống quản lý sinh viên dựa trên công nghệ Blockchain” - Trần Thị Kim Oanh (K46)

Cả hai đề tài này đều được phát triển trên nền tảng **Hyperledger Fabric**, tập trung vào môi trường nội bộ của trường.

2.3. Khoảng Trống Nghiên Cứu

Ở quốc tế, các mô hình tiêu biểu như MIT Blockcerts tập trung mạnh vào xác thực văn bằng trên blockchain công khai, nhưng lại không giải quyết đầy đủ chuỗi dữ liệu học tập từ lúc sinh viên nhập học cho đến khi tốt nghiệp. Các giải pháp này thường chỉ lưu trữ chứng chỉ cuối cùng, không bao quát toàn bộ quá trình đào tạo hay quản lý dữ liệu học sinh, sinh viên.

Trong bối cảnh nghiên cứu trong nước, các hệ thống thử nghiệm chủ yếu lựa chọn Hyperledger Fabric, trong khi chưa có mô hình nào triển khai quản lý điểm và văn bằng dựa trên kiến trúc EVM như Ethereum, dù đây là nền tảng được sử dụng rộng rãi trong các ứng dụng blockchain quốc tế. Điều này tạo ra một khoảng trống rõ rệt: chưa có nghiên cứu nào kiểm chứng khả năng ứng dụng smart contract Solidity trong quản lý đào tạo, cũng như chưa có đánh giá so sánh ưu nhược điểm giữa Ethereum và Hyperledger trong môi trường giáo dục.

Đề tài này hướng đến việc xây dựng thử nghiệm một mô hình quản lý điểm và văn bằng trên Ethereum, qua đó làm rõ sự khác biệt về cơ chế thực thi, tính bất biến, phương thức xác minh dữ liệu và mức độ linh hoạt so với Hyperledger Fabric. Mô hình EVM cũng mang tính mở, có thể mở rộng triển khai trên mạng thật (public hoặc private Ethereum) mà không cần thay đổi kiến trúc lập trình, tạo nền tảng để các nghiên cứu sau tiếp tục phát triển, tối ưu hoặc so sánh hai hướng tiếp cận blockchain khác nhau trong giáo dục.

Vì vậy, khoảng trống nghiên cứu hiện tại nằm ở việc xây dựng một hệ thống quản lý học tập toàn diện dựa trên kiến trúc EVM như Ethereum, nơi không chỉ văn bằng được xác thực mà toàn bộ vòng đời dữ liệu của sinh viên từ thông tin ban đầu, kết quả học tập từng học kỳ cho đến quy trình xét tốt nghiệp được ghi nhận một cách minh bạch, bất biến và có thể xác minh độc lập. Hướng tiếp cận này khai thác smart contract để tự động hóa các nghiệp vụ liên quan đến quản lý điểm và cấp phát văn bằng, đồng thời cho phép mở rộng triển khai trên mạng Ethereum thật (public hoặc private) mà không cần thay đổi kiến trúc hệ thống. Đây chính là khoảng trống mà đề tài hướng đến bồi sung.

III. MỤC TIÊU NGHIÊN CỨU

3.1. Mục Tiêu Tổng Quát

Mục tiêu tổng quát của đề tài là nghiên cứu, thiết kế và xây dựng mô hình ứng dụng công nghệ Blockchain nhằm đảm bảo tính toàn vẹn, minh bạch và chống giả mạo trong quản lý điểm số và cấp phát văn bằng tại các trường đại học.

Hệ thống hướng đến việc chuyển đổi mô hình quản lý truyền thống sang nền tảng phi tập trung (decentralized), cho phép các bên liên quan (sinh viên, giảng viên, nhà trường và nhà tuyển dụng) có thể xác thực thông tin học tập và văn bằng một cách nhanh chóng, chính xác và công khai, qua đó nâng cao độ tin cậy, hiệu quả và hiện đại hóa công tác quản lý giáo dục trong bối cảnh chuyển đổi số.

3.2. Mục Tiêu Cụ Thể

Khảo sát và phân tích thực trạng quản lý điểm và cấp phát văn bằng tại các trường đại học Việt Nam, chỉ ra những hạn chế, rủi ro và lỗ hổng bảo mật của các hệ thống tập trung.

Tìm hiểu và hệ thống hóa cơ sở lý thuyết về công nghệ Blockchain, các đặc tính kỹ thuật (bất biến, phân tán, minh bạch, xác thực), cũng như các mô hình ứng dụng Blockchain trong lĩnh vực giáo dục trên thế giới.

Đề xuất mô hình ứng dụng Blockchain cho quản lý điểm và văn bằng phù hợp với điều kiện của Việt Nam, xác định phạm vi dữ liệu lưu trữ on-chain và off-chain, cũng như cơ chế xác minh và thu hồi văn bằng.

Xây dựng thử nghiệm (prototype) hệ thống quản lý điểm và cấp phát văn bằng dựa trên Blockchain, minh họa quy trình, thêm chương trình đào tạo, gán chương trình đào tạo cho một lớp, nhập điểm, cấp phát, xác minh và kiểm tra trạng thái văn bằng.

Đánh giá tính khả thi của mô hình thông qua các tiêu chí: mức độ bảo mật, tính minh bạch, hiệu quả xác minh, và khả năng mở rộng trong môi trường giáo dục đại học.

IV. ĐỐI TƯỢNG VÀ PHẠM VI NGHIÊN CỨU.

4.1. Đối Tượng Nghiên Cứu

Đối tượng nghiên cứu của đề tài là công nghệ Blockchain và khả năng ứng dụng của nó trong quản lý thông tin học tập và văn bằng điện tử tại các trường đại học.

Cụ thể, đề tài tập trung nghiên cứu các thành phần và cơ chế kỹ thuật cốt lõi của Blockchain, bao gồm: cấu trúc khối (block structure), cơ chế đồng thuận (consensus mechanism), chữ ký số và mã băm (digital signature & hash function), cấu trúc cây Merkle (Merkle Tree), và hợp đồng thông minh (smart contract).

Trên cơ sở đó, đề tài xem xét khả năng ứng dụng các thành phần này vào mô hình quản lý điểm số và cấp phát văn bằng, thông qua việc mã hóa, xác thực và lưu trữ dữ liệu học tập trên mạng Blockchain công khai (Ethereum - EVM).

Đối tượng hướng đến là hệ thống quản lý đào tạo của trường đại học, trong đó có các tác nhân tham gia chính: sinh viên, giảng viên, trưởng khoa, và nhà tuyển dụng, những người trực tiếp tương tác, kiểm tra và xác thực thông tin học tập thông qua nền tảng Blockchain.

4.2. Phạm Vi Nghiên Cứu

Phạm vi nghiên cứu của đề tài tập trung vào khía cạnh kỹ thuật và mô hình ứng dụng của công nghệ Blockchain trong quản lý điểm số và cấp phát văn bằng điện tử tại các trường đại học.

Phạm vi nghiên cứu cụ thể gồm:

- **Nghiên cứu lý thuyết:** Tìm hiểu các khái niệm, cấu trúc và cơ chế hoạt động của công nghệ Blockchain, bao gồm Ethereum, Smart Contract, Merkle Tree, làm nền tảng cho việc thiết kế hệ thống.
- **Phát triển ứng dụng mẫu:** Xây dựng một ứng dụng web đơn giản cho phép Admin có thể tạo chương trình đào tạo, gán chương trình đào tạo cho một lớp, cấp tài khoản cho sinh viên, cán bộ quản lý điểm, cán bộ quản lý điểm có thể nhập điểm cho sinh viên, xem danh sách sinh viên đã tốt nghiệp, Sinh viên có thể quản lý thông tin cá nhân,

xem toàn bộ quá trình học tập, đăng ký xét tốt nghiệp tự động, quản lý và chia sẻ văn bằng cho doanh nghiệp, doanh nghiệp có thể xác thực văn bằng thông qua Blockchain.

- **Môi trường thử nghiệm:** Triển khai và kiểm thử hệ thống trên mạng Blockchain cục bộ (local blockchain) bằng Ganache và Truffle, sử dụng dữ liệu mô phỏng (dữ liệu mẫu) để đánh giá tính khả thi, an toàn và minh bạch của mô hình.
- **Giới hạn phạm vi:** Đề tài chỉ tập trung vào quy trình quản lý chương trình đào tạo, quản lý thông tin sinh viên, quản lý điểm học phần và cấp bằng tốt nghiệp tự động dựa trên smart contract, chưa mở rộng sang các chức năng khác như đăng ký môn học, học phí.

V. PHƯƠNG PHÁP NGHIÊN CỨU.

Đề tài được thực hiện dựa trên sự kết hợp giữa nghiên cứu lý thuyết và thực nghiệm triển khai, nhằm đảm bảo tính khoa học, tính khả thi và tính ứng dụng thực tế.

5.1. Phương Pháp Nghiên Cứu Lý Thuyết

Thu thập và tổng hợp tài liệu: nghiên cứu các công trình khoa học, bài báo, báo cáo và tài liệu chính thống liên quan đến công nghệ Blockchain, các ứng dụng trong giáo dục và quản lý dữ liệu.

Tìm hiểu cơ sở lý thuyết về công nghệ Blockchain, bao gồm cấu trúc khối (Block Structure), cơ chế đồng thuận (Consensus Mechanism), mã băm (Hash Function), chữ ký số (Digital Signature), cây Merkle (Merkle Tree), hợp đồng thông minh (Smart Contract).

Nghiên cứu các mô hình, giải pháp tương tự đã được đề xuất trong và ngoài nước để rút kinh nghiệm và xác định khoảng trống nghiên cứu.

5.2. Phân Tích Và Thiết Kế Hệ Thống

Phân tích yêu cầu nghiệp vụ của bài toán quản lý điểm và cấp phát văn bằng, xác định các tác nhân tham gia (Admin, Cán bộ quản lý điểm, Sinh viên, doanh nghiệp).

Thiết kế mô hình kiến trúc hệ thống phi tập trung, Ethereum (EVM).

Thiết kế cấu trúc dữ liệu, hợp đồng thông minh (Smart Contract) và các quy trình nghiệp vụ (thêm chương trình đào tạo, gán chương trình đào tạo cho lớp học, cấp tài khoản cho cán bộ, sinh viên, nhập điểm, xem quá trình học tập, cấp bằng tự động, xác thực văn bằng).

Thiết kế hệ thống: Sử dụng các sơ đồ UML (như Use Case Diagram, ...) để mô hình hóa kiến trúc tổng thể, thiết kế luồng dữ liệu, và thiết kế chi tiết các Smart Contract.

5.3. Thực Nghiệm Và Triển Khai:

Xây dựng ứng dụng web mẫu (prototype) tích hợp với Blockchain thông qua Web3.js, cho phép admin tạo chương trình đào tạo, gán chương trình đào tạo cho lớp học, tạo tài khoản cho sinh viên, cán bộ, cán bộ nhập điểm, sinh viên đăng ký xét tốt nghiệp tự động và xác thực bằng tốt nghiệp.

Thử nghiệm hệ thống trên mạng Blockchain cục bộ (local) bằng Ganache và Truffle, triển khai trên linux, sử dụng dữ liệu mẫu để kiểm chứng hoạt động và đánh giá hiệu năng.

5.4. Phương Pháp Đánh Giá

Kiểm thử các chức năng của hệ thống theo các tiêu chí: tính chính xác, an toàn, minh bạch và khả năng xác thực dữ liệu.

Đánh giá ưu điểm, hạn chế của mô hình; từ đó đề xuất hướng mở rộng trong tương lai như triển khai trên mạng công khai Ethereum testnet (Sepolia, Goerli) hoặc mở rộng sang các nghiệp vụ giáo dục khác.

VI. Ý NGHĨA KHOA HỌC VÀ THỰC TIỄN

6.1. Ý Nghĩa Khoa Học

Đề tài có ý nghĩa khoa học ở việc nghiên cứu, tổng hợp và vận dụng các nguyên lý cốt lõi của công nghệ Blockchain vào lĩnh vực giáo dục, một hướng tiếp cận còn khá mới tại Việt Nam.

Thông qua quá trình tìm hiểu, phân tích và triển khai mô hình, đề tài góp phần:

- Làm rõ cơ chế hoạt động của Blockchain (bao gồm cấu trúc khối, cơ chế đồng thuận, Merkle Tree, hợp đồng thông minh).
- Chứng minh tính khả thi của việc áp dụng Blockchain công khai (Ethereum - EVM) trong quản lý học tập, qua đó mở rộng hiểu biết về khả năng xác thực dữ liệu phân tán và chống gian lận trong môi trường giáo dục số.
- Góp phần bổ sung tài liệu tham khảo cho hướng nghiên cứu về ứng dụng Blockchain trong lĩnh vực giáo dục, quản trị dữ liệu và chính phủ điện tử.

6.2. Ý Nghĩa Thực Tiễn

Về mặt thực tiễn, đề tài hướng đến xây dựng mô hình mẫu (prototype) của một hệ thống quản lý điểm và cấp phát văn bằng điện tử có khả năng xác thực công khai, chống chỉnh sửa và chống làm giả.

Khi được phát triển hoàn thiện, mô hình này có thể:

- Tăng tính minh bạch trong việc ghi nhận và quản lý điểm học tập.

- Ngăn ngừa gian lận và giả mạo văn bằng, giúp nâng cao uy tín và độ tin cậy của cơ sở giáo dục.
- Giảm tải thủ tục hành chính trong việc xác minh văn bằng, cho phép nhà tuyển dụng hoặc cơ quan kiểm định có thể kiểm tra nhanh chóng qua Blockchain.
- Định hướng cho việc chuyển đổi số trong giáo dục đại học Việt Nam, mở ra khả năng mở rộng sang các lĩnh vực khác như chứng chỉ nghề nghiệp, hồ sơ học tập suốt đời, và hệ thống quản lý đào tạo trực tuyến phi tập trung.

VII. KẾT CÁU LUẬN VĂN

Ngoài các phần mở đầu (Nhận xét của giảng viên, Lời nói đầu, Lời cảm ơn, Danh mục hình, bảng, từ viết tắt), luận văn được kết cấu thành 5 chương chính cùng phần Kết luận - Hướng phát triển, Phụ lục và Tài liệu tham khảo như sau:

Chương 1: Giới Thiệu

Trình bày bối cảnh và lý do chọn đề tài; mục tiêu nghiên cứu; đối tượng và phạm vi nghiên cứu; các nghiên cứu có liên quan; phương pháp nghiên cứu; ý nghĩa khoa học và thực tiễn; kết cấu luận văn.

Chương 2: Cơ sở lý thuyết

Trình bày tổng quan về công nghệ blockchain (khái niệm, cấu trúc, cơ chế đồng thuận và ứng dụng) và giới thiệu nền tảng Ethereum, hợp đồng thông minh cùng các công cụ phát triển, làm cơ sở cho việc thiết kế hệ thống ở các chương sau.

Chương 3: Xây dựng hệ thống thử nghiệm

Trình bày phân tích yêu cầu, thiết kế kiến trúc và triển khai hệ thống thử nghiệm quản lý dữ liệu học tập và cấp phát văn bằng số trên nền tảng blockchain, bao gồm các chức năng chính và mô hình dữ liệu của hệ thống.

Chương 4: Kiểm thử và đánh giá mô hình

Trình bày các kịch bản thử nghiệm (tạo chương trình đào tạo, cấp tài khoản, nhập điểm, cấp phát, xác minh, thu hồi); đánh giá hệ thống về các tiêu chí bảo mật, tính toàn vẹn, minh bạch và hiệu năng; so sánh với mô hình quản lý tập trung truyền thống; phân tích ưu điểm, hạn chế và khả năng mở rộng.

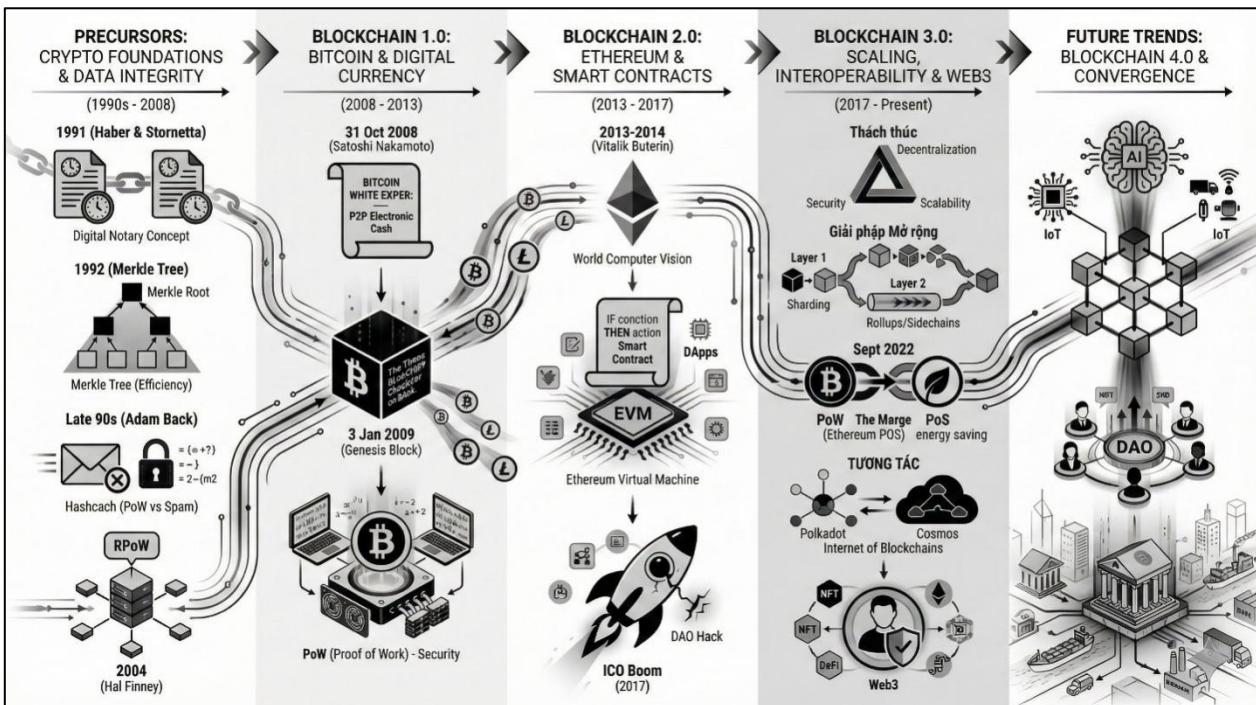
Chương 5: Kết luận và hướng phát triển

Tóm tắt kết quả đạt được, đóng góp khoa học và thực tiễn của đề tài; nêu những hạn chế còn tồn tại; đề xuất các hướng nghiên cứu, hoàn thiện và mở rộng hệ thống trong tương lai.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

I. LỊCH SỬ HÌNH THÀNH VÀ PHÁT TRIỂN CỦA BLOCKCHAIN

Sự ra đời của blockchain, thường được gắn liền với sự xuất hiện của Bitcoin vào năm 2008, trên thực tế là đỉnh cao của nhiều thập kỷ nghiên cứu trong lĩnh vực mật mã học và hệ thống phân tán. Công nghệ này không phải là một phát minh đột ngột mà là một quá trình tiến hóa, tổng hợp các ý tưởng đã có từ trước để giải quyết những vấn đề cơ bản về niềm tin và tính toàn vẹn trong thế giới kỹ thuật số. Phần này sẽ khám phá những nền tảng mật mã và các khái niệm tiền thân, chứng minh rằng blockchain là kết quả của một hành trình trí tuệ lâu dài, bắt nguồn từ những nỗ lực nhằm bảo vệ dữ liệu kỹ thuật số khỏi sự giả mạo.



Hình 2.1 Lịch sử hình thành và phát triển của blockchain

1.1. Nền Tảng Tiền Thân Nhũng Ý Tưởng Khai Sinh Thập niên 1990 - 2008

Sự ra đời của blockchain không phải là một khoảnh khắc bùng nổ mà là kết quả của nhiều thập kỷ nghiên cứu về mật mã và hệ thống phân tán. Năm 1991, Stuart Haber và W. Scott Stornetta giới thiệu một cơ chế đóng dấu thời gian cho tài liệu số bằng hàm băm mật mã, tạo ra một chuỗi hồ sơ liên kết tiền thân của cấu trúc blockchain. Mục tiêu của họ là đảm bảo tính toàn vẹn và chống sửa đổi dữ liệu, chứ không liên quan đến tài chính.

Năm 1992, Merkle Tree được tích hợp vào hệ thống, cho phép gom nhiều tài liệu vào một khối thông qua Merkle root, giúp xác minh nhanh và tối ưu lưu trữ.

Cuối thập niên 1990, Adam Back phát triển Hashcash cơ chế Proof of Work (PoW) chống spam bằng việc buộc người gửi email giải bài toán băm. Năm 2004, Hal Finney mở rộng ý tưởng này thành Reusable Proof of Work (RPoW), cho phép chuyển giao token PoW nhưng vẫn dựa vào máy chủ trung tâm, nên chưa đạt tính phi tập trung hoàn chỉnh.

Các công trình trên, cùng việc băng sáng chế của Haber & Stornetta hết hạn, tạo điều kiện để Satoshi Nakamoto kết hợp các thành phần rời rạc (hàm băm, Merkle Tree, PoW, hệ thống ngang hàng) thành một mô hình hoàn chỉnh, lần đầu tiên giải quyết được vấn đề chi tiêu hai lần mà không cần bên trung gian.

1.2. Blockchain 1.0 Kỷ Nguyên Bitcoin và Tiền Tệ Kỹ Thuật Số (2008-2013)

Ngày 31/10/2008, Satoshi công bố sách trắng Bitcoin: A Peer-to-Peer Electronic Cash System, mô tả một hệ thống tiền điện tử phi tập trung, hoạt động dựa trên mạng ngang hàng và cơ chế đồng thuận PoW để loại bỏ hoàn toàn nhu cầu về trung gian tin cậy.

Ngày 3/1/2009, khối nguyên thủy (Genesis Block) được khai thác, mở ra kỷ nguyên tiền mã hóa. Bitcoin sử dụng blockchain như một sổ cái công khai, nơi các khối được liên kết bằng giá trị băm. Cypher của PoW đảm bảo rằng muốn sửa một giao dịch cũ phải tái tính toán toàn bộ chuỗi sau nó - điều gần như không khả thi. Nhờ đó, Bitcoin giải quyết triệt để vấn đề chi tiêu hai lần và thiết lập mô hình tiền tệ kỹ thuật số an toàn, minh bạch, không chịu sự kiểm soát từ một thực thể duy nhất.

Sự mở mã nguồn của Bitcoin thúc đẩy nhiều altcoin xuất hiện (như Litecoin), đánh dấu Blockchain 1.0 giai đoạn công nghệ tập trung chủ yếu vào tiền tệ và thanh toán số.

1.3. Blockchain 2.0 Cuộc Cách Mạng Hợp Đồng Thông Minh (2013-2017)

Sự phát triển của Bitcoin cho thấy blockchain còn nhiều tiềm năng chưa khai phá. Cuối năm 2013, Vitalik Buterin đề xuất Ethereum một blockchain có ngôn ngữ lập trình tổng quát, cho phép chạy các chương trình phân tán thay vì chỉ xử lý giao dịch tiền tệ.

Ethereum giới thiệu hợp đồng thông minh (smart contract) các chương trình tự thực thi trên blockchain và Máy ảo Ethereum (EVM) môi trường tính toán phi tập trung thống nhất trên toàn mạng. Khái niệm “gas” được đưa vào để đo chi phí tính toán và bảo vệ mạng lưới khỏi lạm dụng tài nguyên.

Ethereum biến blockchain từ một hệ thống tài chính thành một nền tảng lập trình đa mục đích, mở ra kỷ nguyên DApps trong các lĩnh vực như tài chính, quản lý danh tính, trò chơi, và chuỗi cung ứng.

Tiêu chuẩn token ERC-20 tạo điều kiện cho sự bùng nổ của ICO vào năm 2017, khi hàng loạt dự án huy động vốn bằng token trên Ethereum. Dù mang lại đột phá cho mô hình

gọi vốn, giai đoạn này cũng cho thấy rủi ro bảo mật (như sự cố The DAO năm 2016) và sự cần thiết của cơ chế quản lý.

1.4. Blockchain 3.0 Hướng Tới Sự Trưởng Thành (2017-Hiện tại)

Blockchain 3.0 đánh dấu giai đoạn trưởng thành của công nghệ blockchain sau thời kỳ bùng nổ ICO, với trọng tâm chuyển từ thử nghiệm sang tối ưu hóa hạ tầng để sẵn sàng cho việc áp dụng ở quy mô lớn. Trọng tâm của giai đoạn này là giải quyết các hạn chế có hưu về khả năng mở rộng, hiệu quả năng lượng và khả năng tương tác giữa các chuỗi, trong bối cảnh “Bộ ba bất khả thi” (phi tập trung - bảo mật - mở rộng) khiến các hệ thống như Bitcoin, Ethereum khó có thể vừa đảm bảo an ninh cao, vừa duy trì tốc độ xử lý và chi phí thấp. Từ đó, nhiều hướng tiếp cận đã được phát triển, bao gồm mở rộng ở lớp nền tảng (Layer-1) như sharding, và mở rộng ở lớp thứ hai (Layer-2) với các cơ chế xử lý giao dịch ngoài chuỗi như state channel, sidechain và rollup (Optimistic Rollup, ZK-Rollup), trong đó Layer-1 giữ vai trò bảo mật cốt lõi, còn Layer-2 đảm nhận hiệu năng và chi phí.

Song song với bài toán mở rộng, cơ chế đồng thuận cũng trải qua bước chuyển quan trọng từ Proof of Work (PoW) sang Proof of Stake (PoS). PoS thay thế việc “đào” bằng sức mạnh tính toán bằng cơ chế đặt cọc tài sản số, chọn validator dựa trên lượng stake và áp dụng cơ chế phạt (slashing) khi gian lận, qua đó giảm tiêu thụ năng lượng và tăng hiệu quả vận hành. Sự kiện Ethereum chuyển đổi từ PoW sang PoS trong “The Merge” (2022) là cột mốc tiêu biểu, vừa cắt giảm hơn 99% năng lượng tiêu thụ, vừa tạo nền tảng kỹ thuật cho các chiến lược mở rộng tiếp theo như sharding. So với PoW, PoS sử dụng vốn (coin đặt cọc) làm tài nguyên chính thay vì phần cứng, mang lại hiệu quả năng lượng vượt trội, nhưng cũng đặt ra những quan ngại nhất định về mức độ tập trung và mức độ kiểm chứng theo thời gian.

Một trụ cột khác của Blockchain 3.0 là khả năng tương tác (interoperability), nhằm khắc phục tình trạng phân mảnh khi các blockchain hoạt động như những “hòn đảo” tách biệt. Các nền tảng như Polkadot và Cosmos đề xuất kiến trúc đa chuỗi với những triết lý khác nhau: Polkadot xây dựng mô hình Relay Chain – Parachain với bảo mật chia sẻ, nơi các parachain “thuê” bảo mật từ chuỗi trung tâm và giao tiếp thông qua giao thức XCM; trong khi Cosmos lựa chọn mô hình Hubs – Zones với tính chủ quyền cao hơn, mỗi Zone tự quản trị và tự bảo mật, kết nối với nhau thông qua giao thức IBC. Hai hướng tiếp cận này cùng hướng tới mục tiêu hình thành một “Internet của các blockchain”, nơi dữ liệu và tài sản có thể luân chuyển an toàn và linh hoạt giữa nhiều mạng lưới.

Trên nền tảng đó, blockchain thế hệ mới dần mở rộng khỏi phạm vi tài chính thuần túy và được ứng dụng vào nhiều lĩnh vực như y tế (lưu trữ hồ sơ bệnh án an toàn), giáo dục (quản lý bảng điểm và văn bằng phân tán), trò chơi, chính phủ điện tử, hay truy xuất nguồn gốc chuỗi cung ứng. Tuy nhiên, quá trình hiện thực hóa tầm nhìn này vẫn gặp nhiều rào

cản: khung pháp lý cho tài sản số và hợp đồng thông minh chưa hoàn thiện, rủi ro bảo mật trong DApp và cầu nối vẫn hiện hữu, trải nghiệm người dùng còn phức tạp do phụ thuộc vào quản lý khóa riêng. Trong bối cảnh đó, Web3 được xem là bước phát triển tiếp theo của Internet dựa trên blockchain, nơi dữ liệu, tài sản số và danh tính thuộc quyền sở hữu trực tiếp của người dùng, không phụ thuộc nền tảng trung gian. Blockchain 3.0 vì thế có thể được nhìn nhận như tầng hạ tầng cốt lõi của Web3, tập trung vào việc kết hợp hài hòa giữa phi tập trung, bảo mật, khả năng mở rộng và trải nghiệm người dùng để hướng tới ứng dụng thực tế ở quy mô đại chúng.

1.5. Blockchain 4.0 Xu hướng tương lai

Blockchain 4.0 được định hình như giai đoạn tiếp theo, nơi blockchain không còn đứng độc lập mà hội tụ với các công nghệ mới nổi khác như trí tuệ nhân tạo (AI) và Internet vạn vật (IoT) để hình thành các hệ thống tự động, thông minh và có khả năng ra quyết định gần thời gian thực. Trong mô hình này, IoT đảm nhiệm việc thu thập dữ liệu từ thế giới thực, blockchain cung cấp nền tảng ghi nhận và bảo đảm tính toàn vẹn, minh bạch của dữ liệu, trong khi AI phân tích và tối ưu hóa quá trình vận hành, từ đó mở ra các kịch bản ứng dụng như chuỗi cung ứng tự động, nhà máy thông minh, thành phố thông minh hay các hệ thống tài chính phi tập trung có khả năng tự điều chỉnh theo trạng thái thị trường.

Một xu hướng quan trọng khác là sự phát triển của các tổ chức tự trị phi tập trung (DAO), nơi cơ chế quản trị không còn phụ thuộc vào cấu trúc phân cấp truyền thống mà được mã hóa trong smart contract và vận hành thông qua biểu quyết của cộng đồng nắm giữ token. Mô hình này hứa hẹn mang lại mức độ minh bạch cao, giảm phụ thuộc vào cá nhân hay nhóm lợi ích và tạo điều kiện cho các cộng đồng toàn cầu cùng tham gia điều phối tài nguyên, đầu tư hoặc phát triển dự án. Song song đó, khu vực doanh nghiệp, đặc biệt là ngân hàng, tổ chức tài chính và các tập đoàn đa quốc gia ngày càng quan tâm đến việc ứng dụng blockchain trong thanh toán xuyên biên giới, số hóa và quản lý tài sản, truy xuất nguồn gốc và tối ưu vận hành chuỗi cung ứng. Trong bối cảnh đó, Việt Nam được đánh giá là một trong những thị trường năng động và giàu tiềm năng, với hệ sinh thái startup blockchain phát triển nhanh, lực lượng kỹ sư trẻ và các chính sách thúc đẩy chuyển đổi số, tạo tiền đề để năm bắt cơ hội từ làn sóng Blockchain 4.0 trong những năm tới.

II. TỔNG QUAN VỀ CÔNG NGHỆ BLOCKCHAIN

2.1. Khái Niệm Về Công Nghệ Blockchain

Blockchain là một công nghệ lưu trữ và truyền tải dữ liệu dạng sổ cái phân tán (Distributed Ledger Technology - DLT), trong đó dữ liệu được ghi lại dưới dạng các khối (blocks) liên kết với nhau bằng mã băm (hash) và đảm bảo tính bất biến, đồng nghĩa với

việc dữ liệu không thể bị can thiệp, sửa đổi hoặc xóa bỏ sau khi đã được xác thực bởi mạng lưới phi tập trung.

Công nghệ này cho phép mọi nút trong mạng cùng duy trì bản sao dữ liệu đồng nhất, tạo nên tính minh bạch và an toàn mà không cần phụ thuộc vào một máy chủ trung tâm hay tổ chức trung gian.

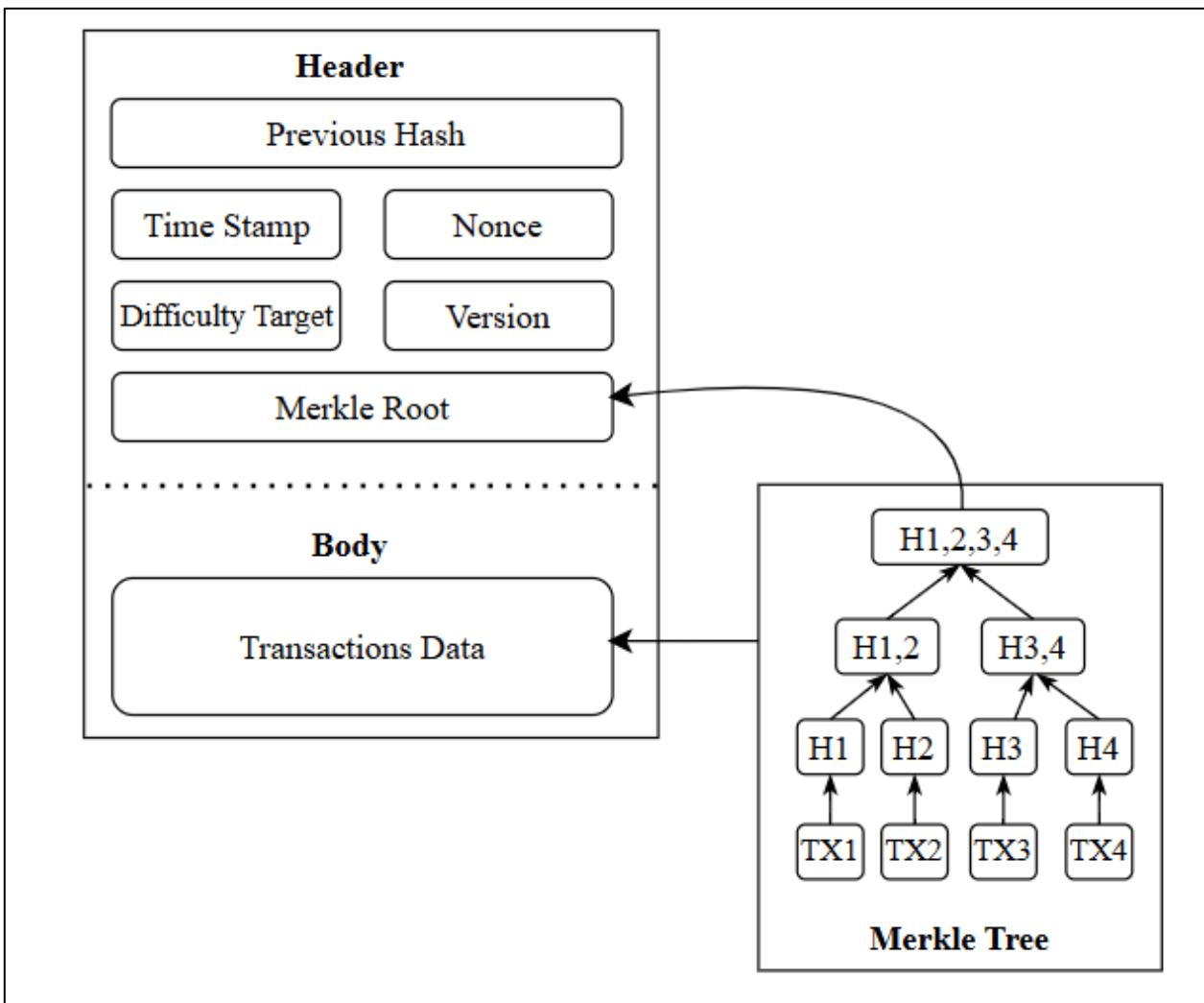
Mỗi giao dịch được xác thực bằng thuật toán đồng thuận giữa các nút (nodes) trong mạng, đảm bảo niềm tin không cần bên thứ ba.



Hình 2.2 Công nghệ blockchain

2.2. Cấu Trúc Cốt Lõi Của Blockchain

a. Khối (Block)



Hình 2.3 Cấu trúc khối của blockchain

1. Phần Header (phần đầu block)

- **Version (Phiên bản):** Xác định phiên bản quy tắc tạo và xử lý block mà mạng blockchain đang dùng.
- **Previous Hash:** mã băm của block liền trước. Giúp các block nối chuỗi với nhau. Nếu thay đổi dữ liệu trong block trước, hash sẽ khác, toàn bộ chuỗi sau đó bị “mất khớp”. Tính bất biến của blockchain bắt nguồn từ đây.
- **Merkle Root:** mã băm gốc của toàn bộ giao dịch trong block. Giúp kiểm tra tính toàn vẹn dữ liệu mà không cần đọc toàn bộ nội dung (sẽ nói kỹ ở phần sau).
- **Timestamp:** Ghi lại thời điểm block được tạo (tính bằng UNIX time số giây từ 01/01/1970). Giúp đồng bộ thời gian giữa các node, hỗ trợ tính hợp lệ của giao dịch.

- **Nonce:** giá trị mà các thợ đào (miner) thay đổi để tìm ra hash hợp lệ (trong hệ Proof of Work).
- **Difficulty Target:** Chỉ có trong các blockchain dùng cơ chế Proof of Work (PoW). Là giá trị mà hash của block mới phải nhỏ hơn thì mới hợp lệ. Điều này buộc miner phải thử nhiều giá trị nonce khác nhau cho đến khi tìm được hash đạt yêu cầu. Đây là cách mạng đảm bảo công sức thực sự (work) được bỏ ra để tạo block.

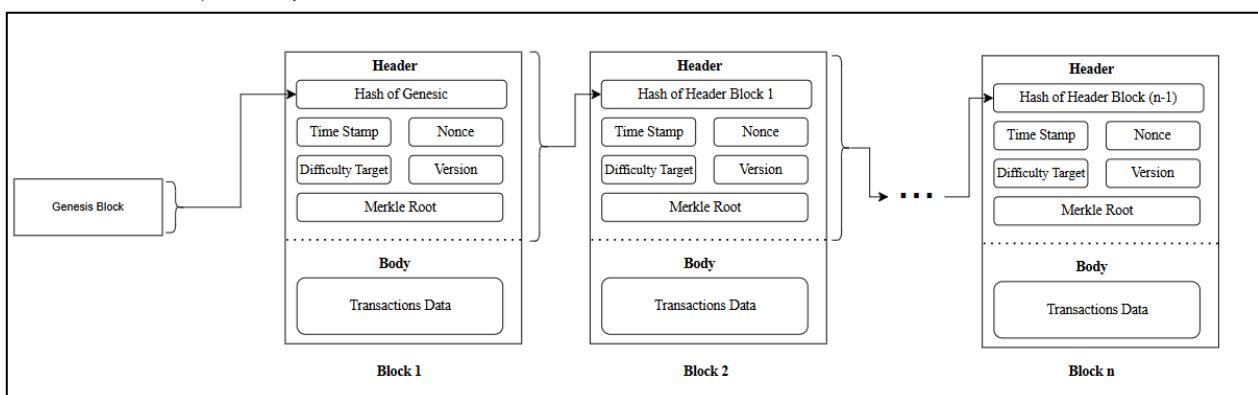
2. Phần Body (phần thân block)

Chứa danh sách các giao dịch (transactions), mỗi giao dịch bao gồm: Địa chỉ người gửi và người nhận (hoặc public key tương ứng), số lượng hoặc dữ liệu cần ghi nhận, chữ ký số của người gửi để xác thực rằng họ thật sự tạo ra giao dịch.

3. Hash của Block

Sau khi có Header, toàn bộ được băm lại bằng thuật toán mật mã học (hash) để tạo ra mã định danh duy nhất cho block đó, hash này có độ dài cố định (ví dụ 256 bit) và thay đổi nhỏ thì hash sẽ thay đổi toàn bộ, giúp phát hiện gian lận tức thì.

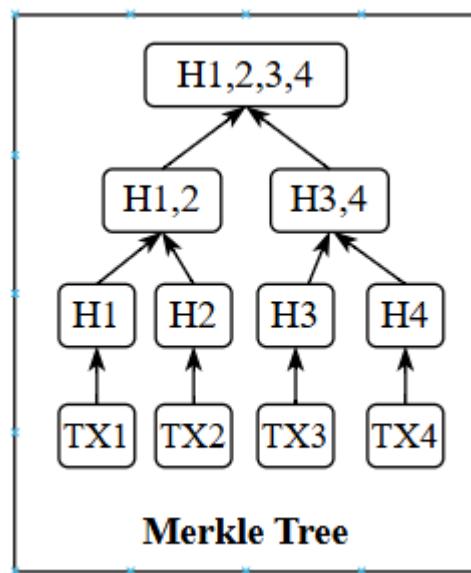
b. Chuỗi (Chain)



Hình 2.4 Cơ chế liên kết thông qua hàm băm của blockchain

- Blockchain hoạt động theo cơ chế “hash nối tiếp hash”:
- Mỗi block chứa PreviousHash, tức là mã hash của block trước.
- Nếu ai đó sửa dữ liệu trong block #100, hash của block #100 sẽ khác làm cho PreviousHash trong block #101 không còn đúng → toàn bộ chuỗi bị lỗi.
- Để giả mạo thành công, kẻ tấn công phải tính lại toàn bộ hash từ block đó trở đi trên hàng nghìn node, điều gần như không thể với blockchain công khai như Bitcoin.

c. *Merkle Tree*



Hình 2.5 Cây Merkle

Merkle Tree là cấu trúc cây nhị phân giúp tổng hợp và xác minh dữ liệu hiệu quả. Khi muốn kiểm tra 1 giao dịch trong block có hợp lệ hay không, chỉ cần vài hash trung gian (Merkle proof) mà không cần tải toàn bộ dữ liệu. Merkle Tree giảm tải dữ liệu, tăng tốc độ xác minh và cực kỳ quan trọng khi blockchain có hàng triệu giao dịch.

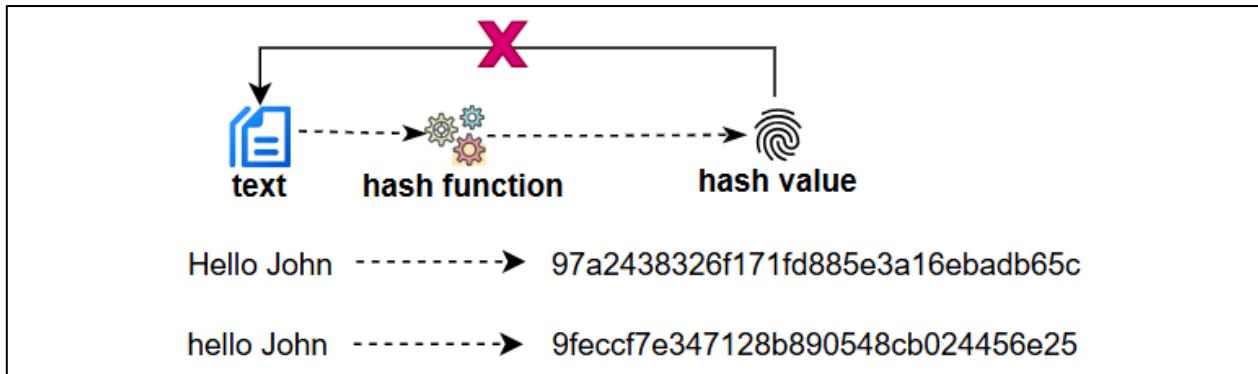
Cách hoạt động:

- Mỗi giao dịch được băm thành một nút lá (leaf).
 - Hai nút liền nhau được ghép và băm lại để tạo thành nút cha.
 - Tiếp tục như vậy cho đến khi chỉ còn một nút gốc duy nhất gọi là Merkle Root.

Ví dụ: Các giao dịch là TX1, TX2, TX3, TX4.

- $H1 = \text{Hash}(\text{TX1})$, $H2 = \text{Hash}(\text{TX2})$, $H3 = \text{Hash}(\text{TX3})$, $H4 = \text{Hash}(\text{TX4})$, $H12 = \text{Hash}(H1 + H2)$, $H34 = \text{Hash}(H3 + H4)$, $H1234 = \text{Hash}(H12 + H34)$
 - Nếu muốn kiểm tra TX3 có thật không, chỉ cần $H4$ và $H12$ để tính ra Root. Nếu trùng Merkle Root trong block, thì TX3 là thật.

d. Mã băm mật mã học (Hash Function)



Hình 2.6 Hàm băm

Hàm băm là cơ chế nén dữ liệu thành một chuỗi bit có độ dài cố định, dùng để tạo "dấu vân tay" duy nhất cho mỗi khối dữ liệu và liên kết các block thông qua việc lưu lại hash của block trước. Nhờ đó, cấu trúc blockchain đảm bảo tính toàn vẹn và chống sửa đổi: chỉ cần một thay đổi nhỏ trong dữ liệu cũng làm thay đổi hoàn toàn giá trị băm, khiến mọi hành vi chỉnh sửa trở nên dễ dàng bị phát hiện.

Các đặc tính quan trọng của hàm băm gồm:

- Tính xác định:** Cùng một chuỗi đầu vào được xử lý bởi cùng hàm băm, sẽ cho ra cùng một kết quả.
- Không thể đảo ngược:** không thể suy ngược lại dữ liệu ban đầu từ giá trị băm, ngay cả khi biết thuật toán băm.
- Độ nhạy cao với dữ liệu đầu vào:** chỉ cần thay đổi một ký tự trong thông điệp cũng tạo ra giá trị băm hoàn toàn khác (ví dụ: Abcde và abcde cho hai hash khác nhau hoàn toàn).
- Tính duy nhất:** Hai thông điệp khác nhau thì nhận về 2 chuỗi băm khác nhau.

e. Mật mã khóa công khai (Public-Key Cryptography)



Hình 2.7 Quy trình mã hóa và giải mã trong hệ mật mã khóa công khai

Hệ mật mã khóa công khai (Public Key Cryptography) sử dụng một cặp khóa có liên hệ toán học với nhau để đảm bảo tính an toàn và xác thực trong các hệ thống số.

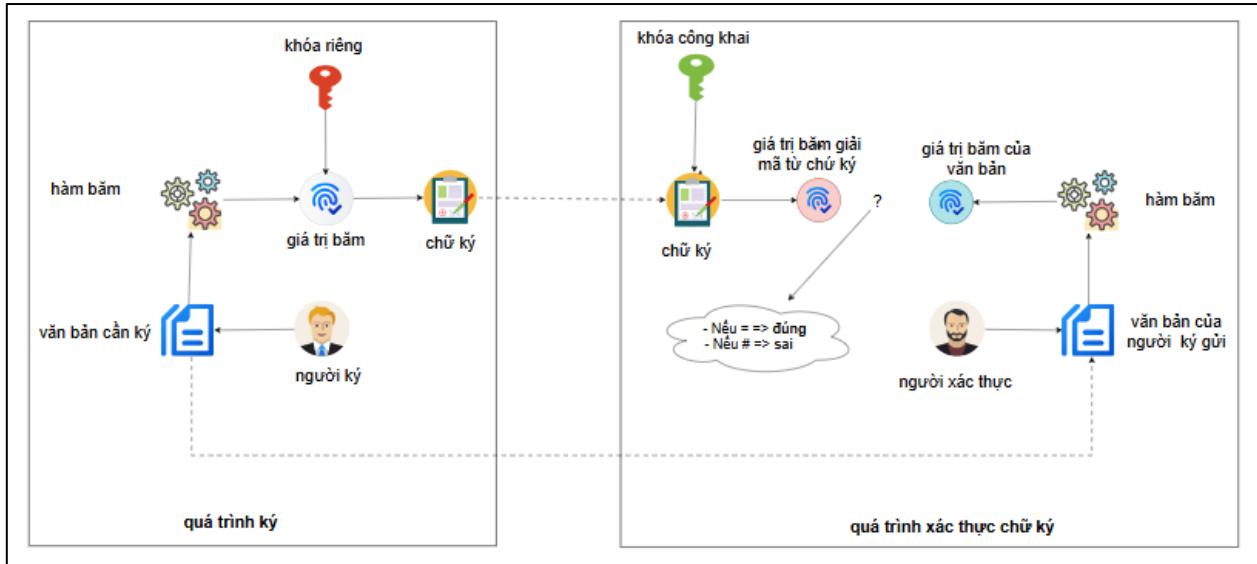
- **Khóa riêng (Private Key):** là một chuỗi số bí mật tuyệt đối, dùng để ký hoặc tạo bằng chứng sở hữu. Người dùng phải bảo mật khóa này và không được chia sẻ cho bất kỳ ai.
- **Khóa công khai (Public Key):** được sinh ra từ khóa riêng thông qua các phép toán một chiều; quá trình này không thể đảo ngược, nên không thể suy ra khóa riêng từ khóa công khai. Khóa công khai có thể chia sẻ rộng rãi để người khác kiểm tra hoặc xác minh.

Nguyên tắc hoạt động: Bất cứ thứ gì được mã hóa bằng Khóa riêng chỉ có thể được giải mã (xác minh) bằng Khóa công khai tương ứng và ngược lại.

Ứng dụng trong Blockchain:

- **Địa chỉ ví:** khóa công khai được băm (hash) để tạo thành địa chỉ ví, nơi người dùng có thể nhận tài sản số như Bitcoin hoặc Ether.
- **Xác thực quyền sở hữu:** chỉ người nắm giữ khóa riêng mới có khả năng ký giao dịch, chứng minh họ là chủ sở hữu hợp lệ của tài sản gắn với địa chỉ ví.
- **Xác minh phi tập trung:** toàn bộ mạng lưới có thể xác minh chữ ký giao dịch bằng khóa công khai mà không cần tin cậy bất kỳ bên trung gian nào, đảm bảo tính minh bạch và an toàn.

f. Chữ ký số (Digital Signature)



Hình 2.8 Quy trình ký số và xác thực chữ ký số

Chữ ký số là quy trình kết hợp hàm băm và mật mã khóa công khai nhằm xác thực giao dịch và đảm bảo tính toàn vẹn của dữ liệu. Cơ chế này đáp ứng ba yêu cầu quan trọng:

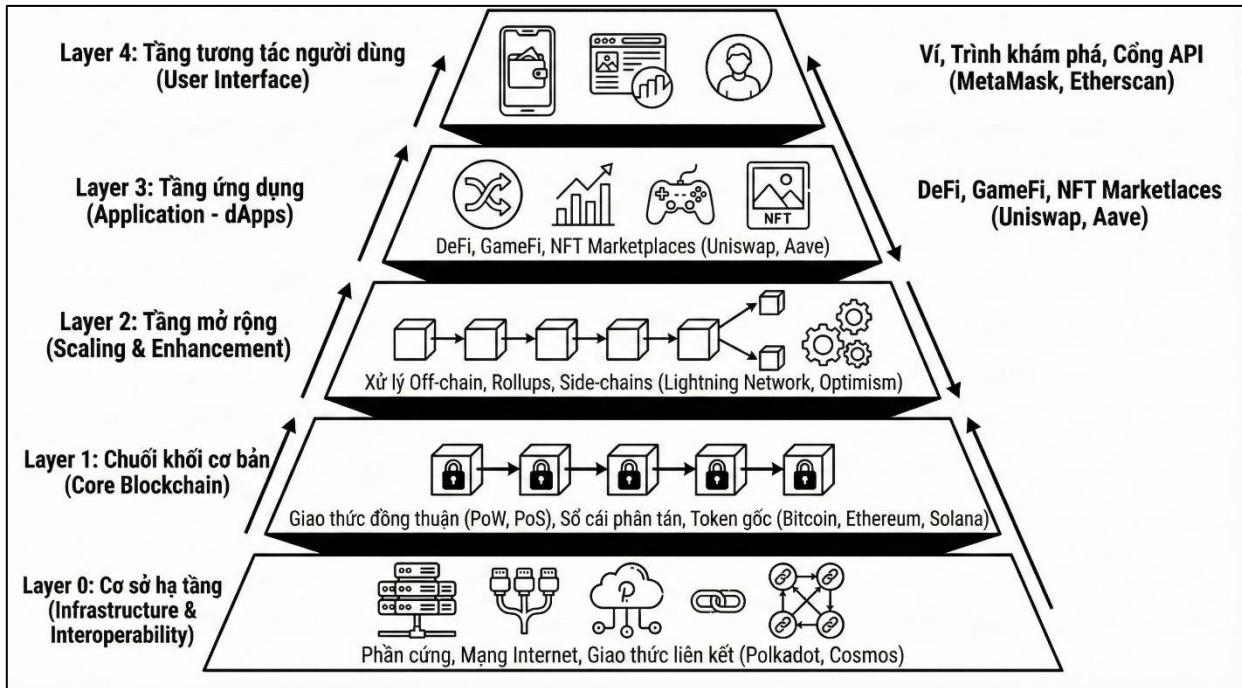
- **Tính xác thực (Authentication):** chỉ người sở hữu khóa riêng mới có thể tạo ra chữ ký hợp lệ.
- **Tính chống chối bỏ (Non-repudiation):** người đã ký giao dịch không thể phủ nhận việc mình đã tạo ra chữ ký đó.
- **Tính toàn vẹn (Integrity):** bất kỳ thay đổi nào trong dữ liệu đều làm chữ ký trở nên không hợp lệ.

Quy trình hoạt động:

- **Tạo giao dịch:** người dùng tạo thông điệp giao dịch (ví dụ: “gửi 1 BTC cho B”).
- **Băm giao dịch:** thông điệp được đưa qua hàm băm để tạo ra giá trị hash đại diện cho nội dung giao dịch.
- **Ký giao dịch:** người dùng sử dụng khóa riêng để ký lên hash, tạo thành chữ ký số.
- **Phát tán giao dịch:** gói dữ liệu gồm thông điệp gốc, chữ ký số và khóa công khai được gửi lên mạng.
- **Xác minh:**
 - ✓ Các nút trong mạng dùng khóa công khai để kiểm tra chữ ký số, thu được hash A.
 - ✓ Đồng thời, họ tự băm lại thông điệp gốc để tạo ra hash B.
 - ✓ Nếu hash A trùng với hash B, chữ ký hợp lệ và giao dịch được chấp nhận.

2.3. Kiến Trúc Phân Lớp Của Blockchain

Công nghệ blockchain có thể được hiểu như một hệ thống gồm nhiều tầng (layers) xếp chồng lên nhau, mỗi tầng đảm nhiệm một vai trò kỹ thuật và chức năng riêng biệt. Mô hình phân lớp này tương tự như nền móng và các tầng của một tòa nhà cao tầng, trong đó mỗi tầng thực hiện một chức năng cụ thể và xây dựng trên nền tảng của tầng bên dưới. Từ tầng hạ tầng cơ bản (Layer 0) cho đến tầng tương tác người dùng (Layer 4), tất cả cùng phối hợp để làm nên một hệ sinh thái blockchain hoàn chỉnh, đảm bảo các tiêu chí phi tập trung, bảo mật, mở rộng và thân thiện với người dùng.



Hình 2.9 Kiến Trúc Phân Lớp Của Blockchain

a. Layer 0: Tầng cơ sở hạ tầng (Foundation Layer)

Layer 0 là lớp cơ sở hạ tầng nền tảng cho phép các blockchain khác vận hành và tương tác với nhau. Về mặt kỹ thuật, Layer 0 bao gồm phần cứng, mạng lưới Internet, và các giao thức liên kết các blockchain độc lập. Đây là “nền đát” của tòa nhà blockchain, đóng vai trò giải quyết bài toán tương tác và kết nối giữa các chuỗi khối (interoperability) tức cho phép các blockchain riêng rẽ có thể giao tiếp và trao đổi dữ liệu với nhau một cách an toàn. Nhờ Layer 0, hệ sinh thái blockchain tránh được tình trạng cát cứ thông tin giữa các chuỗi khối riêng lẻ. Ví dụ: Polkadot và Cosmos là những nền tảng Layer 0 tiêu biểu, được thiết kế chuyên biệt để kết nối nhiều blockchain Layer 1 lại với nhau, cho phép truyền dữ liệu và giá trị xuyên chuỗi. Bên cạnh đó, Layer 0 còn bao gồm cơ sở hạ tầng phần cứng như máy chủ, nút mạng và thiết bị mạng internet đảm bảo cho các mạng blockchain vận hành liên tục.

b. Layer 1: Tầng chuỗi khối cơ bản (Core Blockchain Layer)

Layer 1 là lớp chuỗi khối cơ sở, nơi diễn ra mọi hoạt động cốt lõi của mạng blockchain. Tại tầng này, các giao dịch được xử lý, xác minh và ghi vào sổ cái phân tán; đây chính là “động cơ” vận hành của toàn bộ hệ thống. Về kỹ thuật, Layer 1 bao gồm các giao thức đồng thuận (như PoW của Bitcoin, PoS của Ethereum 2.0) để đảm bảo mọi nút mạng đồng thuận về trạng thái sổ cái. Nó cũng bao gồm các token gốc của mạng (VD: BTC trên Bitcoin, ETH trên Ethereum) và khả năng thực thi hợp đồng thông minh (trên các nền tảng như Ethereum). Layer 1 chịu trách nhiệm đảm bảo tính phi tập trung, bảo mật và bất biến của dữ liệu blockchain. Mọi giao dịch on-chain đều được xử lý tại đây, do đó hiệu năng Layer 1 ảnh hưởng trực tiếp đến tốc độ và chi phí giao dịch. Ví dụ: Bitcoin là blockchain Layer 1 đầu tiên tập trung vào tiền tệ số an toàn, phi tập trung; Ethereum là Layer 1 hỗ trợ thực thi hợp đồng thông minh và ứng dụng phi tập trung; Solana là Layer 1 hiệu năng cao nổi tiếng với tốc độ xử lý nhanh và thông lượng lớn.

c. Layer 2: Tầng mở rộng và tối ưu hiệu năng (Scaling & Enhancement Layer)

Layer 2 là lớp nằm trên Layer 1, cung cấp các giải pháp nhằm mở rộng khả năng xử lý và cải thiện hiệu suất cho blockchain cơ sở. Thay vì thay đổi trực tiếp giao thức của Layer 1, Layer 2 cho phép xử lý nhiều giao dịch ngoài chuỗi chính (off-chain) và chỉ đưa kết quả tổng hợp về Layer 1 khi cần thiết, nhờ đó giảm tải cho mạng chính. Về mặt kỹ thuật, Layer 2 bao gồm các giải pháp như kênh trạng thái (state channels), side-chains, và các giao thức rollups (ví dụ: Optimistic Rollup, zk-Rollup) – cho phép gộp hàng loạt giao dịch off-chain thành một giao dịch duy nhất trên Layer 1. Lợi ích chính của Layer 2 là tăng thông lượng, giảm phí giao dịch và cải thiện tốc độ mà vẫn thừa hưởng được tính bảo mật của Layer 1 (vì dữ liệu cuối cùng vẫn được ghi lên chuỗi chính). Ví dụ: Lightning Network trên Bitcoin là giải pháp Layer 2 giúp thực hiện thanh toán tức thời với phí rất thấp bằng cách mở các kênh giao dịch ngoài chuỗi. Trên Ethereum, các mạng như Optimism hay Arbitrum (sử dụng rollup) đóng vai trò như Layer 2 giúp giảm tải, giảm chi phí gas và tăng tốc độ xử lý cho Ethereum.

d. Layer 3: Tầng ứng dụng (Application Layer)

Layer 3 là lớp ứng dụng, nơi các ứng dụng phi tập trung (dApp) và dịch vụ blockchain trực tiếp tương tác với người dùng cuối. Đây là phần “mặt tiền” của thế giới blockchain, những gì mà người dùng thông thường nhìn thấy và sử dụng. Về bản chất, Layer 3 chính là nơi triển khai các hợp đồng thông minh để tạo ra ứng dụng thực tế như sàn giao dịch phi tập trung, giao thức tài chính phi tập trung (DeFi), trò chơi blockchain, mạng xã hội phi tập trung... Người dùng tương tác với Layer 3 tương tự như cách họ dùng ứng dụng web hoặc mobile truyền thống, tuy nhiên nền tảng bên dưới là các smart contract chạy trên Layer 1/Layer 2, đảm bảo tính minh bạch và phi tập trung. Tầm quan trọng: Layer 3

đem công nghệ blockchain đến gần với đời sống, ẩn đi những phức tạp kỹ thuật của các tầng dưới. Nhờ các ứng dụng ở tầng này, người dùng có thể hưởng lợi từ blockchain (bảo mật, minh bạch, không cần trung gian) mà không nhất thiết phải hiểu sâu về cách thức vận hành của các tầng kỹ thuật bên dưới.

Ví dụ: Uniswap là một ứng dụng (dApp) DeFi trên Ethereum cho phép người dùng hoán đổi token mà không cần sàn tập trung. Aave là một giao thức cho vay và đi vay phi tập trung. OpenSea là một chợ trực tuyến NFT cho phép mua bán các tài sản số độc nhất trên nền tảng Ethereum. Tất cả đều vận hành ở Layer 3, dựa trên các smart contract của Layer 1 Ethereum, mang lại trải nghiệm dịch vụ tài chính, sưu tầm số... ngay trong trình duyệt web của người dùng.

e. *Tầng tương tác người dùng (User Interface & Interaction Layer)*

Layer 4 là lớp giao diện và tiện ích người dùng, bao gồm các công cụ, phần mềm giúp người dùng kết nối và tương tác thuận tiện với các dịch vụ blockchain ở những tầng dưới. Có thể coi Layer 4 là “cầu nối” thân thiện giữa người dùng và thế giới blockchain. Về thành phần, Layer 4 bao gồm các ví blockchain, các cổng API dịch vụ, các bảng điều khiển/quản trị và các trình khám phá blockchain (block explorer) phục vụ việc tra cứu dữ liệu. Lớp này chịu trách nhiệm tối ưu trải nghiệm người dùng, giúp cho cả những người không có kỹ thuật vẫn có thể sử dụng blockchain một cách dễ dàng. Ví dụ: Ví MetaMask là ứng dụng ví phổ biến giúp người dùng tương tác với Ethereum và các dApp một cách trực quan (quản lý tài khoản, ký giao dịch...). Coinbase Wallet cũng cung cấp giao diện thân thiện để lưu trữ tài sản và kết nối với hệ sinh thái phi tập trung. Ngoài ra, các trang web block explorer như Etherscan cung cấp giao diện tra cứu thông tin giao dịch, hợp đồng, số dư ví... giúp người dùng theo dõi dữ liệu trên chuỗi một cách trực quan. Nhờ Layer 4, công nghệ blockchain trở nên dễ tiếp cận hơn với đại chúng, tương tự như cách trình duyệt web và giao diện đồ họa giúp người dùng phổ thông tiếp cận Internet mà không cần hiểu sâu về giao thức TCP/IP bên dưới.

Tóm lại, kiến trúc phân lớp từ Layer 0 đến Layer 4 giúp phân tách rõ ràng các chức năng trong hệ thống blockchain. Mỗi lớp đóng một vai trò riêng: Layer 0 tạo nền tảng hạ tầng và kết nối liên chuỗi; Layer 1 đảm trách vận hành chuỗi khỏi cơ bản và đảm bảo bảo mật, phi tập trung; Layer 2 mở rộng năng lực xử lý, giảm phí và tăng tốc độ; Layer 3 cung cấp các ứng dụng phi tập trung phục vụ nhu cầu thực tiễn; và Layer 4 mang đến giao diện thân thiện, giúp người dùng cuối tương tác dễ dàng với hệ sinh thái blockchain. Sự phối hợp nhịp nhàng của các tầng này là chìa khóa làm nên thành công kỹ thuật của blockchain, vừa duy trì các ưu điểm cốt lõi (bảo mật, phi tập trung) vừa không ngừng nâng cao hiệu năng và trải nghiệm sử dụng.

2.4. Các Tính Chất Của Blockchain

Theo các nghiên cứu từ Viện Tiêu chuẩn và Công nghệ Hoa Kỳ (NIST, 2018), Diễn đàn Kinh tế Thế giới (2018) và Melanie Swan (2015), công nghệ Blockchain có **năm đặc tính cốt lõi** như sau:

- **Phi tập trung (Decentralization):** Hệ thống không có máy chủ trung tâm; dữ liệu được sao chép và đồng bộ trên toàn mạng lưới, giúp giảm rủi ro mất mát hoặc giả mạo dữ liệu.
- **Bất biến (Immutability):** Khi dữ liệu đã được ghi nhận và xác nhận vào khối, gần như không thể thay đổi hoặc xóa bỏ.
- **Minh bạch và kiểm chứng (Transparency & Verifiability):** Mọi giao dịch đều có thể được kiểm tra công khai, bảo đảm tính minh bạch và khả năng truy xuất nguồn gốc.
- **Bảo mật bằng mật mã học (Cryptographic Security):** Mỗi giao dịch được mã hóa và xác thực bằng thuật toán mật mã (ví dụ: SHA-256, ECDSA), đảm bảo tính toàn vẹn và xác thực của dữ liệu.
- **Đồng thuận phân tán (Consensus Mechanism):** Các nút trong mạng phải đạt được sự đồng thuận (qua PoW, PoS, PBFT...) trước khi thêm giao dịch mới vào chuỗi khối.

Bên cạnh đó, những nghiên cứu gần đây chỉ ra ít **nhất hai đặc tính bổ sung** cần được đề cập nhằm phản ánh đúng khả năng và thách thức của blockchain thế hệ mới:

- **Hợp đồng thông minh (Smart Contracts):** Cho phép lập trình và tự động thực thi các điều kiện giao dịch mà không cần trung gian, mở rộng blockchain từ “sổ cái phân tán” thành “nền tảng vận hành phân quyền”.
- **Chống kiểm duyệt (Censorship Resistance):** Bảo vệ dữ liệu khỏi thao túng hoặc xoá bỏ bởi bất kỳ thực thể nào, nhờ cấu trúc phi tập trung và cơ chế đồng thuận bảo đảm tính toàn vẹn của toàn

2.5. Nguyên Lý Hoạt Động Của Blockchain

Quy trình xử lý giao dịch có thể mô tả như sau: Một giao dịch trên blockchain phải đi qua chuỗi bước chặt chẽ để đảm bảo tính xác thực, toàn vẹn và bất biến.

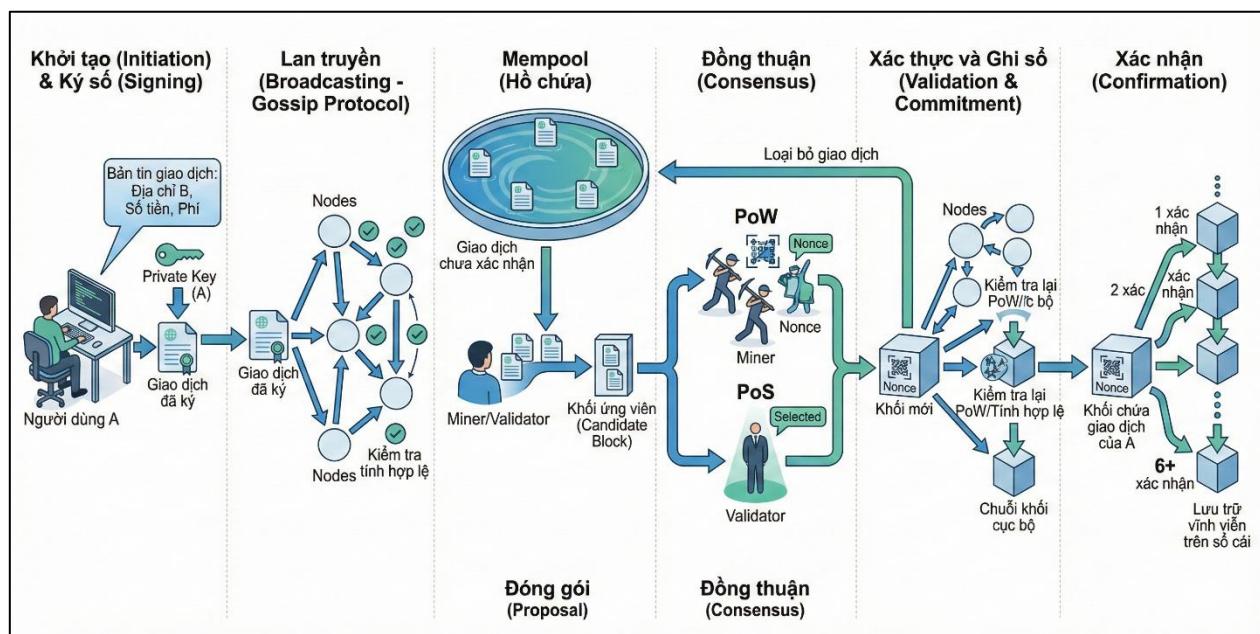
Trước hết, người dùng khởi tạo giao dịch bằng ví, nhập địa chỉ người nhận, số tiền và mức phí. Giao dịch sau đó được ký số bằng khóa riêng, tạo ra chữ ký mật mã chứng minh quyền sở hữu và ngăn mọi hành vi giả mạo. Bản giao dịch đã ký được phát tán lên mạng ngang hàng, nơi các nút nhanh chóng kiểm tra tính hợp lệ ban đầu và lan truyền nó theo cơ chế “gossip”.

Khi hợp lệ, giao dịch được đưa vào mempool, vùng đệm chứa các giao dịch chờ xử lý. Từ mempool, thợ đào (PoW) hoặc validator (PoS) chọn các giao dịch phù hợp và đóng gói vào một khối ứng viên, thường ưu tiên giao dịch có phí cao.

Khối này phải vượt qua cơ chế đồng thuận: PoW yêu cầu giải bài toán băm với độ khó nhất định; PoS dựa vào việc lựa chọn và xác thực của các nút đặt cọc. Khi khối qua được đồng thuận, mỗi node sẽ xác thực độc lập toàn bộ khối, kiểm tra bằng chứng đồng thuận và tính hợp lệ của từng giao dịch trước khi chấp nhận nó vào sổ cái cục bộ. Giao dịch tương ứng được loại khỏi mempool.

Sau khi khối được thêm vào chuỗi, giao dịch nhận xác nhận (confirmation) đầu tiên. Mỗi khối mới nối tiếp phía sau sẽ tăng thêm xác nhận, làm cho giao dịch ngày càng an toàn và gần như không thể đảo ngược. Khi đạt đủ số xác nhận (thường là 6), giao dịch được xem là cố định và bất biến.

Quy trình tổng thể này dựa trên mật mã, mạng phân tán và đồng thuận phi tập trung đảm bảo rằng mọi giao dịch đều được xác minh khách quan, ghi sổ an toàn và không thể bị chỉnh sửa sau khi xác nhận.



Hình 2.10 Luồng hoạt động của Blockchain

2.6. Cơ Chế Đồng Thuận Của Blockchain

Cơ chế đồng thuận (thuật toán đồng thuận) trong blockchain là tập hợp các quy tắc cho phép các node (nút) trong mạng phi tập trung đồng ý với nhau về trạng thái sổ cái tại mọi thời điểm. Nói cách khác, mặc dù không có trung gian tin cậy, tất cả các node đều phải thống nhất dữ liệu giao dịch và chuỗi khối cuối cùng. Cơ chế đồng thuận đảm bảo mọi giao

dịch được xác thực chính xác, minh bạch và được ghi nhận giống nhau trên toàn bộ các node. Nhờ đó, blockchain trở thành hệ thống chịu lỗi Byzantine (Byzantine Fault Tolerance - BFT), tức mạng vẫn hoạt động ngay cả khi một số node bị lỗi hoặc có ý gian lận, miễn là phần lớn các node tuân thủ giao thức.

Có nhiều thuật toán đồng thuận đã được phát triển, mỗi loại có nguyên lý hoạt động và ưu nhược điểm riêng. Tùy vào loại mạng (public/private/consortium), blockchain chọn cơ chế phù hợp để cân bằng giữa bảo mật - phi tập trung - hiệu suất (gọi là Blockchain Trilemma). Dưới đây, chúng ta sẽ trình bày chi tiết các cơ chế đồng thuận phổ biến nhất hiện nay:

Bảng 2.1 So sánh một số cơ chế đồng thuận phổ biến trong blockchain

Cơ chế đồng thuận	Nguyên lý hoạt động	Mức độ phi tập trung	Thông lượng (TPS) & Độ trễ	Chịu lỗi	Năng lượng tiêu thụ	Ví dụ tiêu biểu
Proof of Work (PoW) Bằng chứng công việc	Miner giải toán băm (hash) phức tạp để chọn người tạo khối kế tiếp; khối mới được thêm theo quy tắc “chuỗi dài nhất”.	Công khai, phân tán cao (permission less).	Thấp (~3–7 TPS); độ trễ cao (Bitcoin ~10 phút/khối).	Chịu được đến <50% công suất băm (ứng với tấn công 51% nếu chiếm đa số) (theo lý thuyết).	Rất cao (đào Bitcoin tiêu thụ năng lượng tương đương một quốc gia nhỏ).	Bitcoin, Litecoin, Ethereum (trước khi chuyển sang PoS)
Proof of Stake (PoS) Bằng chứng cổ phần	Validator được chọn dựa trên số lượng coin (stake) nắm giữ; node chỉ cần chứng minh quyền sở hữu tiền thay vì dùng sức mạnh tính toán.	Công khai; giảm năng lượng tiêu thụ nhưng dễ tập trung bình (người có nhiều token nắm quyền lực lớn).	Cao hơn PoW (ví dụ ~50–1000+ TPS); độ trễ trung bình (Ethereum ~6–12 giây/khối).	Chịu được <50% stake của kẻ xấu (tương tự PoW).	Rất thấp (không dùng đào); sau khi Ethereum chuyển sang PoS, tiêu thụ năng lượng giảm ~99.95%.	Ethereum 2.0 (Beacon Chain), Cardano, Polkadot, Algorand
DPoS Delegated Proof of Stake	Phát triển từ PoS: người sở hữu token bầu ra một nhóm nhỏ đại biểu (delegates) để xác thực khối.	Rất thấp (số đại biểu cố định ít, dễ tập trung quyền lực).	Rất cao (≥ 1000 TPS; thực tế có thể xử lý hàng ngàn TPS như EOS, Solana); độ trễ rất thấp (block ~giây).	Chịu theo cơ chế BFT của nhóm đại biểu (thường $f < n/3$ trong nhóm validator).	Thấp (như PoS).	EOS, TRON, Steem, Lisk

PBFT Practical Byzantine Fault Tolerance	Thuật toán BFT cổ điển: tất cả nút tin cậy trao đổi tin nhắn (prepare/commit) để đồng thuận; thường dùng cho mạng riêng hoặc consortium.	Hạn chế (thường triển khai trên mạng có quyền, chỉ vài chục nodes tin cậy).	Cao (~200–500 TPS); độ trễ rất thấp (đa phần dưới vài giây).	Chịu được $f < n/3$ Byzantine lý PBFT).	Rất thấp (không có khai thác, mức điện năng cơ bản).	Hyperledger Fabric, Tendermint (Cosmos), Quorum
PoA Proof of Authority	Các node có thẩm quyền (được xác thực danh tính) lần lượt tạo khối (không cần PoW/PoS).	Rất thấp (chỉ một nhóm nhỏ validator được quyền; rất tập trung).	Rất cao (>1500 TPS); độ trễ rất thấp (gần tức thì).	Giả định các authority hầu hết là thiện chí (nếu đa số authority xấu, hệ thống suy yếu).	Cực kỳ thấp (không đào, chỉ tiêu hao cho xác thực).	VeChain, POA Network, các chuỗi riêng dùng Ethereum
PoH Proof of History	Cơ chế tạo dấu thời gian phi tập trung: sinh một chuỗi hash lặp (Verifiable Delay Function) để xác minh thứ tự và khoảng thời gian giữa các giao dịch. PoH thường kết hợp với PoS (Solana) để đồng thuận.	Permissionless (ví dụ Solana) nhưng thường hạn chế node do yêu cầu phần cứng cao.	Rất cao (Solana tuyên bố khả năng ~710k TPS lý thuyết; thực tế hàng chục nghìn TPS); độ trễ rất thấp (~0.5 giây).	Phụ thuộc vào cơ chế PoS gắn với nó (ví dụ Solana cũng đáp ứng $f < n/3$).	Thấp (dựa trên PoS, không đào).	Solana (kết hợp PoH + PoS)

2.7. Cơ Chế Chống Sự Thay Đổi

Cơ chế chống thay đổi là nền tảng cốt lõi tạo nên mức độ an toàn và độ tin cậy vượt trội của blockchain. Một khi dữ liệu được ghi nhận và xác thực, việc sửa đổi nó gần như bất khả thi nếu không phá vỡ toàn bộ cấu trúc của chuỗi. Khả năng này không đến từ một kỹ thuật đơn lẻ, mà được hình thành bởi ba lớp bảo vệ hoạt động đồng thời: mã hóa và hàm băm mật mã; cấu trúc chuỗi liên kết giữa các khối; cơ chế đồng thuận phi tập trung.

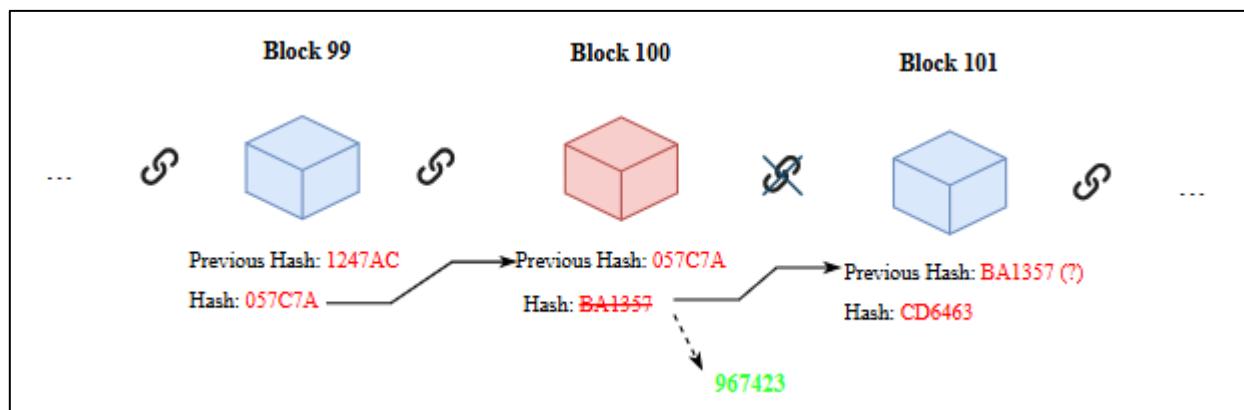
Có thể hình dung blockchain như một pháo đài nhiều tầng: lớp tường thành là hàm băm bảo vệ nội dung khối, hào nước sâu là chuỗi các block liên kết chặt chẽ với nhau, và đội cung thủ trên thành chính là mạng lưới các node đồng thuận, luôn sẵn sàng loại bỏ bất kỳ bản ghi bất hợp lệ nào. Nhờ ba tầng phòng thủ này, blockchain đạt được tính bất biến (immutability), làm cho mọi hành vi chỉnh sửa dữ liệu đều bị phát hiện và không thể đưa vào chuỗi hợp lệ.

a. Mã băm mật mã học

Mỗi khối trong blockchain chứa dữ liệu giao dịch, giá trị băm (hash) đại diện cho chính nó, hash của khối trước, nonce và một số tham số khác như độ khó (difficulty).

Hash là chuỗi ký tự duy nhất được tạo ra từ toàn bộ nội dung của khối; chỉ cần thay đổi một ký tự trong dữ liệu cũng làm giá trị hash thay đổi hoàn toàn.

Nhờ đó, nếu bất kỳ ai chỉnh sửa dữ liệu trong một khối (ví dụ: block 100), hash của khối này sẽ thay đổi và không còn khớp với hash được lưu trong block 101. Sự sai lệch này ngay lập tức phá vỡ chuỗi liên kết giữa các block, giúp phát hiện hành vi sửa đổi.

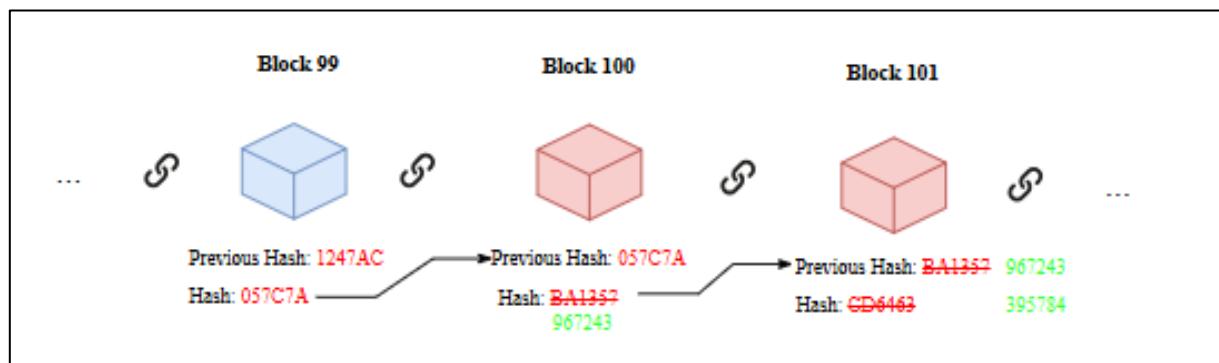


Hình 2.11 Cơ chế Hash Block chống sửa đổi trong Blockchain

b. Cấu trúc chuỗi liên kết (The "Chain")

Blockchain được cấu trúc như một chuỗi khói, nơi mỗi khói trỏ đến khói trước thông qua mã băm của nó. Điều này tạo ra một chuỗi liên kết mật mã an toàn. Để thay đổi dữ liệu trong block thứ 100, kẻ tấn công buộc phải: tính lại hash của block 100, sau đó tính lại hash của tất cả block phía sau (101, 102, ...) để khớp trở lại chuỗi.

Với các blockchain lớn như Bitcoin, điều này gần như bất khả thi vì việc tính toán lại toàn bộ chuỗi đòi hỏi lượng tài nguyên cực lớn.



Hình 2.12 Hash Chaining: cơ chế chống sửa đổi dữ liệu trong blockchain

c. Cơ chế đồng thuận phi tập trung

Ngay cả trong trường hợp giả định kẻ tấn công có đủ khả năng tính toán lại toàn bộ chuỗi băm, họ vẫn phải khiến phần lớn node trong mạng chấp nhận chuỗi mới là hợp lệ.

Các mạng blockchain phổ biến tuân theo quy tắc: “*Chuỗi hợp lệ nhất là chuỗi có tổng công sức (work) hoặc tổng cổ phần (stake) lớn nhất được đa số mạng xác nhận.*”

- Trong Proof of Work (PoW), kẻ tấn công cần hơn 50% **sức mạnh tính toán toàn mạng** → gọi là tấn công 51%.
- Trong Proof of Stake (PoS), kẻ tấn công cần sở hữu hơn 50% tổng lượng coin stake, điều này tối thiểu đến mức gần như phi thực tế.

Do đó, khả năng thay đổi lịch sử blockchain gần như bằng không nếu mạng đủ lớn và phân tán.

d. Sao chép phân tán

Số cái blockchain được sao chép và lưu trữ trên hàng nghìn node phân tán, nếu một node bị tấn công hoặc bị chỉnh sửa dữ liệu: các node khác sẽ so sánh bản ghi, phiên bản sai sẽ bị loại bỏ, toàn mạng đồng bộ theo bản được đa số xác nhận là đúng.

Không tồn tại “máy chủ trung tâm” để tấn công hoặc chiếm quyền kiểm soát, giúp hệ thống duy trì tính bền vững và khả năng kháng lỗi cao.

Cơ chế chống thay đổi của blockchain dựa trên: Liên kết băm mật mã giữa các khối, Đồng thuận phân tán giữa các node, Sao lưu toàn bộ dữ liệu trên nhiều bản sao độc lập. Nhờ ba yếu tố này, blockchain đạt được tính bất biến (immutability) — một khi dữ liệu được ghi nhận và xác nhận, không ai có thể chỉnh sửa mà không để lại dấu vết.

III. ƯU VÀ NHƯỢC ĐIỂM CỦA BLOCKCHAIN

3.1. Ưu Điểm Của Công Nghệ Blockchain

- **Tính minh bạch và toàn vẹn dữ liệu:** Mọi giao dịch đều được ghi vào khối (block), xác thực bởi mạng lưới phi tập trung và không thể chỉnh sửa. Điều này giúp đảm bảo dữ liệu không thể bị giả mạo hoặc xóa bỏ mà không để lại dấu vết.
- **Phi tập trung (Decentralization):** Không có máy chủ trung tâm. Mọi node trong mạng đều có bản sao dữ liệu giống nhau. Điều này giảm thiểu rủi ro bị tấn công hoặc gián đoạn do lỗi ở một điểm duy nhất (single point of failure).
- **Bảo mật cao:** Blockchain sử dụng các thuật toán mật mã học như SHA-256, ECDSA, và cơ chế chữ ký số để đảm bảo danh tính và tính toàn vẹn dữ liệu. Mỗi giao dịch phải được ký và xác thực trước khi ghi vào sổ cái.

- **Truy xuất nguồn gốc (Traceability):** Mỗi thay đổi đều được ghi lại, giúp dễ dàng truy vết lịch sử giao dịch hoặc chuỗi cung ứng.
- **Tự động hóa thông qua Smart Contract:** Hợp đồng thông minh giúp tự động hóa các quy trình (như xác nhận điểm, cấp chứng chỉ, chuyển quyền sở hữu tài sản) mà không cần trung gian.

3.2. Nhược Điểm Của Công Nghệ Blockchain

- **Khả năng mở rộng hạn chế (Scalability):** Các mạng blockchain công khai như Ethereum hay Bitcoin có tốc độ xử lý giao dịch thấp (chỉ vài chục TPS) so với hệ thống tập trung truyền thống có thể đạt hàng nghìn TPS.
- **Chi phí cao:** Phí giao dịch (gas fee) trên các mạng lớn có thể rất đắt, đặc biệt khi mạng bị tắc nghẽn.
- **Tiêu thụ năng lượng (đối với PoW):** Các blockchain dùng cơ chế Proof of Work (như Bitcoin) tiêu tốn năng lượng cực lớn để duy trì đồng thuận.
- **Khó tích hợp với hệ thống truyền thống:** Do tính phi tập trung và định dạng dữ liệu đặc thù, việc tích hợp blockchain với hệ thống cơ sở dữ liệu hoặc ứng dụng sẵn có thường phức tạp.
- **Quy định pháp lý chưa rõ ràng:** Nhiều quốc gia vẫn đang hoàn thiện khung pháp lý cho blockchain, đặc biệt trong các lĩnh vực nhạy cảm như tài chính, dữ liệu cá nhân hoặc giáo dục.

IV. ỨNG DỤNG CỦA BLOCKCHAIN CHIẾN LUỢC QUỐC GIA CỦA VIỆT NAM

Trong những năm gần đây, Chính phủ Việt Nam đã thể hiện sự quan tâm và cam kết mạnh mẽ đối với việc nghiên cứu, ứng dụng và phát triển công nghệ blockchain như một động lực của cuộc Cách mạng Công nghiệp 4.0. Đặc biệt, ngày 22/10/2024, Thủ tướng Chính phủ đã ban hành Quyết định số 1236/QĐ-TTg phê duyệt “Chiến lược quốc gia về ứng dụng và phát triển công nghệ chuỗi khối (blockchain) đến năm 2025, định hướng đến năm 2030” đây là văn bản chiến lược đầu tiên của Việt Nam dành riêng cho blockchain. Chiến lược quốc gia này đặt ra tầm nhìn, mục tiêu cụ thể cho từng giai đoạn, cùng các định hướng lớn nhằm thúc đẩy mạnh mẽ ngành công nghiệp blockchain trong nước, đưa Việt Nam bắt kịp xu hướng công nghệ toàn cầu.

Mục tiêu đến năm 2025: Chiến lược đề ra hai nhóm mục tiêu cụ thể cho giai đoạn đến 2025: (i) Thiết lập nền tảng phát triển công nghệ chuỗi khối, bao gồm việc hình thành Hạ tầng chuỗi khối Việt Nam phục vụ phát triển và quản lý các ứng dụng blockchain, tuân thủ các quy định về an toàn, an ninh mạng; thúc đẩy nghiên cứu phát triển ứng dụng

blockchain tại 03 trung tâm đổi mới sáng tạo quốc gia; xây dựng và nâng cấp 10 cơ sở nghiên cứu, đào tạo về blockchain, đưa nội dung công nghệ chuỗi khối vào chương trình đào tạo ở đại học, cao đẳng và dạy nghề. (ii) Thúc đẩy, tăng cường ứng dụng công nghệ chuỗi khối, với mục tiêu hình thành tối thiểu 01 trung tâm/đặc khu thử nghiệm về chuỗi khối (sandbox) làm hạt nhân cho mạng lưới blockchain quốc gia (ưu tiên tại những nơi đã có kinh nghiệm triển khai mạng lưới chuỗi khối) và hình thành hệ sinh thái “Blockchain+” thông qua việc ứng dụng công nghệ chuỗi khối trong các ngành/lĩnh vực như tài chính-ngân hàng, giao thông-vận tải, y tế, giáo dục, thương mại, logistics, bưu chính, sản xuất công nghiệp, năng lượng, du lịch, nông nghiệp, dịch vụ công, ...

Mục tiêu 2030: Trở thành nhóm dẫn đầu khu vực & có vị thế quốc tế về nghiên cứu, ứng dụng, phát triển; mở rộng Hạ tầng chuỗi khối quốc gia; phấn đấu ~20 thương hiệu blockchain uy tín tầm khu vực; duy trì ≥ 3 trung tâm/đặc khu sandbox; có đơn vị VN lọt Top 10 cơ sở đào tạo/nghiên cứu blockchain châu Á.

Chiến lược xác định các lĩnh vực ưu tiên triển khai blockchain, tiêu biểu gồm:

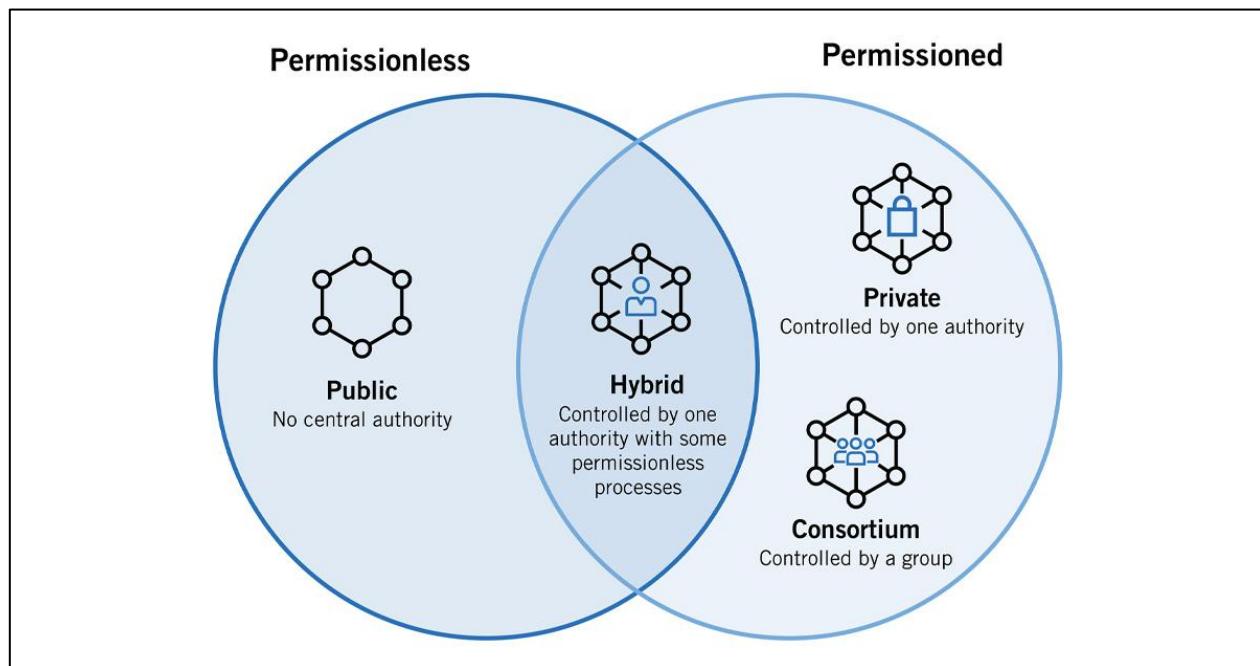
- **Tài chính - Ngân hàng:** Ứng dụng blockchain trong thanh toán, chuyển tiền, quản lý tài sản số, phát hành tiền số ngân hàng trung ương (CBDC), v.v. nhằm tăng cường minh bạch và hiệu quả.
- **Giao thông - Vận tải:** Triển khai blockchain để quản lý logistics, theo dõi chuỗi cung ứng, tối ưu hóa vận tải và chia sẻ dữ liệu giao thông một cách an toàn.
- **Y tế:** Lưu trữ và chia sẻ hồ sơ y tế bằng blockchain để bảo mật thông tin bệnh án, quản lý chuỗi cung ứng thuốc, và xác thực nguồn gốc thiết bị y tế.
- **Giáo dục và đào tạo:** Ứng dụng blockchain để quản lý văn bằng, chứng chỉ; xây dựng hồ sơ học tập số, qua đó chống làm giả và tạo sự tin cậy trong tuyển dụng, đào tạo.
- **Thương mại (bán lẻ, thương mại điện tử):** Dùng hợp đồng thông minh trong giao kết thương mại, truy xuất nguồn gốc hàng hóa, bảo vệ quyền lợi người tiêu dùng.
- **Logistics, Bưu chính - Chuyển phát:** Sử dụng blockchain để theo dõi hành trình vận chuyển, giảm giấy tờ thủ tục, minh bạch hóa quá trình giao nhận hàng.
- **Sản xuất công nghiệp:** Quản lý chuỗi cung ứng sản xuất, theo dõi linh kiện, hàng hóa trong nhà máy thông qua sổ cái phân tán, chống hàng giả.
- **Năng lượng:** Áp dụng blockchain trong quản lý lưới điện thông minh, giao dịch năng lượng ngang hàng (P2P energy trading), và chứng nhận nguồn gốc năng lượng tái tạo.
- **Du lịch:** Quản lý hồ sơ du khách, chương trình khách hàng thân thiết; xác thực đánh giá du lịch trên nền tảng blockchain để chống giả mạo.
- **Nông nghiệp:** Truy xuất nguồn gốc nông sản bằng blockchain, bảo đảm minh bạch thông tin về quá trình trồng trọt, chế biến, phân phối thực phẩm.

- **Dịch vụ công:** Ứng dụng chuỗi khối trong chính phủ điện tử, quản lý hồ sơ công dân, đăng ký đất đai, phiếu lý lịch tư pháp, bô phiếu điện tử... tăng tính minh bạch và tin cậy của dịch vụ công.

(Danh sách trên chỉ mang tính tiêu biểu; chiến lược quốc gia mở rộng sang nhiều lĩnh vực khác khi công nghệ chín muồi)

V. PHÂN LOẠI BLOCKCHAIN

Blockchain được phân loại theo nhiều tiêu chí khác nhau. Dưới đây là các cách phân loại phổ biến, Phân loại theo quyền truy cập.



Hình 2.13 Phân loại blockchain theo quyền truy cập

Blockchain công khai (Public Blockchain): Mạng blockchain mở, permissionless, cho phép bất kỳ ai tham gia đọc và ghi dữ liệu. Mọi nút (node) trong mạng có quyền bình đẳng trong xác thực giao dịch và duy trì sổ cái. Dữ liệu trên chuỗi công khai hoàn toàn minh bạch và bất biến - một khi đã ghi, dữ liệu không thể bị sửa hay xóa. Blockchain công khai phi tập trung hoàn toàn, không một cá nhân hay tổ chức nào kiểm soát mạng, ví dụ điển hình là Bitcoin và Ethereum. Nhờ tính phi tập trung và minh bạch, blockchain công khai được ưa chuộng trong các ứng dụng tiền mã hóa và hệ thống mở.

Blockchain riêng tư (Private Blockchain): Mạng blockchain giới hạn cho một tổ chức hoặc nhóm người dùng được cấp phép. Blockchain riêng tư thường do một thực thể duy nhất kiểm soát, vận hành trong môi trường khép kín (intranet), nên quy mô nhỏ và tốc độ xử lý nhanh hơn. Loại này còn gọi là blockchain được phép (permissioned blockchain)

hoặc blockchain doanh nghiệp. Chỉ các nút được ủy quyền mới có quyền đọc/ghi dữ liệu; điều này đảm bảo tính riêng tư cho tổ chức sử dụng. Blockchain riêng tư không cần token gốc để vận hành (không có cơ chế đào coin) do số lượng nút ít, nhờ vậy tiêu thụ ít năng lượng hơn so với chuỗi công khai. Ví dụ: Ripple là một mạng blockchain riêng tư tập trung vào thanh toán liên ngân hàng; Hyperledger Fabric do IBM phát triển cũng thuộc loại private blockchain cho doanh nghiệp.

Blockchain liên hợp (Consortium Blockchain): Còn gọi là blockchain liên minh, là mạng blockchain permissioned do một nhóm tổ chức cùng quản trị. Nhiều thực thể hợp tác vận hành các nút xác thực thay vì chỉ một bên duy nhất, giúp giảm rủi ro tập trung so với blockchain riêng tư. Các thành viên liên minh thỏa thuận về quy tắc, quyền hạn và quy trình đồng thuận chung. Blockchain liên hợp lý tưởng cho các chuỗi cung ứng phức tạp hoặc liên ngành, nơi nhiều bên cần chia sẻ dữ liệu một cách tin cậy. Ví dụ: Global Shipping Business Network (GSBN) - liên minh các hãng tàu biển áp dụng blockchain để số hóa vận tải; B3i - liên minh các công ty bảo hiểm ứng dụng blockchain; hay nền tảng IBM Food Trust - liên minh nhà bán lẻ và nhà cung cấp sử dụng Hyperledger Fabric để truy xuất nguồn gốc thực phẩm. Trong các hệ thống này, cơ chế đồng thuận được kiểm soát bởi tập hợp nút đã được chỉ định trước, đảm bảo hiệu suất cao mà vẫn giữ được tính phân tán giữa các tổ chức.

Blockchain lai (Hybrid Blockchain): Là mô hình kết hợp giữa blockchain công khai và riêng tư. Một phần mạng hoạt động công khai, cho phép mọi người kiểm chứng dữ liệu chung; phần còn lại hoạt động riêng tư, giới hạn truy cập đối với dữ liệu nhạy cảm. Điều này cho phép tổ chức vừa kiểm soát được dữ liệu bí mật, vừa tận dụng tính minh bạch của mạng công khai khi cần thiết. Ví dụ, một ngân hàng có thể vận hành sổ cái giao dịch nội bộ trên mạng riêng tư, nhưng dùng một blockchain công khai để ghi băm (hash) xác nhận giao dịch, công chúng có thể kiểm tra tính hợp lệ của giao dịch mà không thấy nội dung chi tiết. Trong blockchain lai, thông tin nhạy cảm được giữ kín nhưng vẫn có thể kiểm chứng qua cơ chế mật mã (ví dụ: tiết lộ có chọn lọc qua hợp đồng thông minh). Ưu điểm lớn của mô hình lai là an ninh cao, hacker bên ngoài rất khó tấn công 51% do hệ thống vận hành trong môi trường đóng, đồng thời đảm bảo quyền riêng tư và khả năng mở rộng tốt hơn mạng công khai. Nền tảng XinFin (kết hợp public Ethereum và private blockchain) hay Dragonchain là những ví dụ về blockchain lai.

VI. CÁC NỀN TẢNG BLOCKCHAIN

Blockchain khởi nguồn từ Bitcoin (2009), nhưng đến nay hệ sinh thái đã mở rộng thành nhiều nền tảng với kiến trúc và mục tiêu sử dụng khác nhau. Trong đó, Ethereum và Hyperledger Fabric là hai nền tảng được quan tâm và nghiên cứu rộng rãi nhất; bên cạnh

đó còn có các kiến trúc mới như Polkadot, Solana hay R3 Corda, mỗi nền tảng mang theo một định hướng công nghệ riêng. Các nghiên cứu gần đây chỉ ra rằng **Ethereum là “nền tảng blockchain phổ biến cho cả mạng công cộng lẫn mạng riêng tư”, trong khi Hyperledger Fabric được xem là “bộ công cụ blockchain doanh nghiệp phổ biến do Linux Foundation phát triển”**, với kiến trúc mô-đun cho phép tùy chỉnh linh hoạt các thành phần như đồng thuận, quản lý thành viên hay lớp lưu trữ dữ liệu.

Phản tiếp theo tổng hợp các kết quả chính từ những nghiên cứu và báo cáo kỹ thuật liên quan đến các nền tảng này, làm rõ đặc điểm cốt lõi, ưu điểm nổi bật, ứng dụng thực tế cũng như những khía cạnh công nghệ quan trọng như cơ chế đồng thuận, ngôn ngữ phát triển hợp đồng thông minh và công cụ hỗ trợ triển khai.

Bảng 2.2 So sánh giữa Ethereum và Hyperledger Fabric

Tiêu chí	Ethereum	Hyperledger Fabric
Kiến trúc	Blockchain công cộng, phi tập trung (permissionless), cho phép bất kỳ ai tham gia mà không cần giấy phép. Sử dụng Ethereum Virtual Machine (EVM) để chạy các hợp đồng thông minh (smart contract) trên mạng phân tán.	Nền tảng blockchain doanh nghiệp, permissioned (chỉ các bên đã xác thực được tham gia). Kiến trúc mô-đun (pluggable), cho phép tùy chỉnh thành phần (đồng thuận, lưu trữ, quản lý danh tính) và hỗ trợ các kênh riêng tư (channels) để bảo vệ dữ liệu kinh doanh.
Cơ chế đồng thuận	Sau “The Merge” (2022), Ethereum sử dụng cơ chế Proof of Stake (PoS) để xác nhận khối. Trước đó Ethereum dùng Proof of Work (PoW). PoS giúp tiết kiệm năng lượng và cải thiện bảo mật (token ETH được stake để đảm bảo tính trung thực).	Không dùng PoW/PoS công khai. Fabric có cơ chế đồng thuận linh hoạt (pluggable). Thông thường dùng thuật toán Raft (CFT) hoặc PBFT do các nút đã biết danh tính phối hợp, hoặc Kafka (trước đây). Cơ chế này không yêu cầu “đào” coin, tăng hiệu năng và giảm chi phí vận hành.
Ứng dụng thực tế	Phổ biến trong các ứng dụng công khai phi tập trung (DApp): tài chính phi tập trung (DeFi), NFT, game trên blockchain, ICO, crowdfund... Ethereum có hệ sinh thái rộng lớn với hàng nghìn hợp đồng và ứng dụng trực tuyến.	Tập trung cho doanh nghiệp: chuỗi cung ứng, tài chính, chăm sóc y tế, sản xuất... (các tổ chức như IBM, Walmart, ngân hàng sử dụng). Ví dụ: IBM Food Trust (quản lý nguồn gốc thực phẩm) dùng Fabric. Fabric tích hợp dễ với hệ thống CNTT hiện có nhờ smart contract viết bằng Java/Go/Node.js.
Hiệu năng (TPS, độ trễ)	Thông lượng thấp (~15–30 giao dịch/giây trên mạng chính) và độ trễ cao (thời gian tạo khối ~12 giây). Khi nhiều giao dịch, mạng có thể tắc nghẽn và phí gas tăng cao.	Thông lượng cao (thường vài trăm đến hàng nghìn TPS tùy cấu hình) và độ trễ thấp nhờ xử lý song song và mạng hạn chế node. Nghiên cứu cho thấy Fabric vượt trội hơn Ethereum về tốc độ xử lý và độ trễ. Fabric được thiết kế để xử lý khối lượng giao dịch lớn trong môi trường riêng tư.
Bảo mật	Bảo mật dựa vào tính phi tập trung và thuật toán PoS (mã hóa mạnh). Mọi node đều lưu bản sao sổ cái, giao dịch công khai minh bạch nên khó bị giả mạo. Tuy nhiên do cho phép	Mạng đóng (permissioned) nên bảo mật nhờ xác thực và quản lý danh tính. Chỉ các thành viên được phép mới xem và ghi giao dịch (bảo mật cao hơn). Fabric sử dụng TLS và kênh riêng để đảm

	ân danh, mạng có nguy cơ tấn công (51%) nếu kẻ xấu chiếm đa số stake.	bảo tính riêng tư, không có token nên tránh được các tấn công liên quan đến khai thác tiền mã hóa.
Điểm mạnh	<p>Phi tập trung & minh bạch: Mọi giao dịch đều công khai, không phụ thuộc bên thứ ba. Cộng đồng phát triển lớn, hệ sinh thái DApp không lồ.</p> <p>Tính linh hoạt: Hỗ trợ nhiều loại hợp đồng thông minh (Solidity) và turing-complete.</p>	<p>Hiệu năng cao: Mô-đun và tối ưu cho doanh nghiệp, throughput lớn, độ trễ thấp.</p> <p>Bảo mật, riêng tư: Quyền truy cập được kiểm soát, hỗ trợ kênh riêng tư cho giao dịch kinh doanh an toàn.</p> <p>Tùy chỉnh cao: Cấu hình linh hoạt (đồng thuận, lưu trữ, danh tính), dễ tích hợp với hệ thống hiện có. Không phải trả phí giao dịch (gas) mặc định.</p>
Điểm yếu	<p>Khả năng mở rộng hạn chế: Thông lượng thấp, độ trễ cao, dễ tắc nghẽn khi tăng tải.</p> <p>Phí giao dịch: Gas fee biến động, khiến chi phí giao dịch cao, khó dự đoán.</p> <p>Thiếu riêng tư: Dữ liệu minh bạch mọi người đều thấy, không phù hợp khi cần bảo mật thông tin.</p>	<p>Giới hạn người tham gia: Chỉ áp dụng trong mạng riêng, không mở rộng cho cộng đồng rộng rãi. Cần quản lý chặt thành viên, khó mở rộng khi có nhiều tổ chức kết nối.</p> <p>Tập trung: Có rủi ro tập trung điều hành (quyết định bởi tổ chức chủ quản).- Ecosystem: Ít ứng dụng và công cụ hỗ trợ so với Ethereum công khai. Không có token gốc (nếu cần phải xây dựng thêm).</p>

VII. ETHEREUM

7.1. Giới Thiệu Tổng Quan Về Ethereum



Hình 2.14 Ethereum

Ethereum là nền tảng blockchain phi tập trung thế hệ thứ hai, được đề xuất bởi Vitalik Buterin vào năm 2013 và chính thức ra mắt năm 2015 dưới sự phát triển của Ethereum Foundation. Khác với Bitcoin vốn chỉ tập trung vào chức năng chuyển giá trị, Ethereum được thiết kế như một “máy tính thế giới” (World Computer), cho phép thực thi hợp đồng thông minh (smart contracts) và triển khai ứng dụng phi tập trung (Decentralized Applications - DApps) trên cùng một hạ tầng chung.

Ethereum sở hữu môi trường tính toán hoàn chỉnh Turing (Turing-complete), giúp xử lý các logic phức tạp mà Bitcoin không hỗ trợ. Từ năm 2022, sau bản nâng cấp The Merge, Ethereum chuyển đổi cơ chế đồng thuận từ Proof of Work (PoW) sang Proof of Stake (PoS), giúp giảm tiêu thụ năng lượng, cải thiện khả năng mở rộng và nâng cao hiệu

quả xác thực giao dịch. Hệ sinh thái Ethereum ngày nay phát triển rộng với các mạng tương thích EVM (EVM-compatible) như BNB Chain, Polygon và Avalanche, hình thành một mạng lưới blockchain có khả năng tương tác cao.

7.2. Cấu Trúc Của Ethereum

- **Ethereum Virtual Machine (EVM):** Máy ảo thực thi hợp đồng thông minh. Tất cả hợp đồng Solidity đều được biên dịch thành bytecode và chạy trên EVM của mọi node đảm bảo tính xác định và đồng nhất.
- **Smart Contracts:** Các đoạn mã tự động thực thi khi điều kiện được thỏa mãn, đảm bảo minh bạch và không thể bị can thiệp.
- **Ether (ETH):** Đồng tiền gốc của hệ thống, được dùng để trả phí giao dịch (gas fee) và thưởng cho validator.
- **Blockchain Layer:** Chuỗi khối lưu trữ toàn bộ lịch sử giao dịch, trạng thái tài khoản và mã bytecode của hợp đồng.
- **Consensus Layer:** Lớp đồng thuận sử dụng PoS, đảm bảo tất cả các node đạt được sự nhất quán về trạng thái số cái.

7.3. Ứng Dụng Của Ethereum

Ethereum được ứng dụng rộng rãi trong nhiều lĩnh vực công nghệ và kinh tế số, bao gồm:

- **Tài chính phi tập trung (DeFi):** Các nền tảng như Uniswap, Aave, Compound cho phép vay, cho vay và giao dịch không cần trung gian.
- **Token hóa và NFT:** Biến tài sản số hoặc vật lý thành token có thể giao dịch (ERC-20, ERC-721).
- **Quản trị phi tập trung (DAO):** Tổ chức tự trị vận hành dựa trên hợp đồng thông minh.
- **Chuỗi cung ứng, giáo dục và nhận dạng số:** Ứng dụng blockchain Ethereum để xác thực nguồn gốc, bằng cấp, hoặc danh tính người dùng.

7.4. Hợp Đồng Thông Minh

Hợp đồng thông minh là chương trình máy tính được lưu trữ và thực thi trên blockchain. Khi các điều kiện được định nghĩa trước được thỏa mãn, hợp đồng tự động thực thi và cập nhật trạng thái mà không cần bên trung gian. Tất cả các nút trong mạng blockchain đều đồng thời xác thực và thực hiện hợp đồng, đảm bảo tính minh bạch, toàn vẹn và không thể bị can thiệp tùy tiện. Về bản chất, đây là cơ chế “thực thi thỏa thuận tự động trên nền tảng phi tập trung”.

Hợp đồng thông minh hoạt động như thế nào?

- **Triển khai (Deployment):** Lập trình viên viết hợp đồng bằng ngôn ngữ như Solidity và triển khai lên blockchain, tạo ra một địa chỉ hợp đồng cố định.
 - **Kích hoạt (Trigger):** Người dùng hoặc hệ thống gửi giao dịch kích hoạt các hàm trong hợp đồng khi điều kiện khớp.
 - **Thực thi (Execution):** Hợp đồng được thực thi trong Ethereum Virtual Machine (EVM), mọi nút đều tính toán cùng một kết quả và ghi lại trên blockchain dưới dạng dữ liệu bất biến.
- Kết quả chỉ được chấp nhận khi đạt đồng thuận (PoS/PoW tùy nền tảng).

Các nền tảng blockchain hỗ trợ hợp đồng thông minh

- **Ethereum:** Nền tảng phổ biến nhất, sử dụng EVM và ngôn ngữ Solidity. Hầu hết các ứng dụng DeFi, NFT và DAO đều chạy trên Ethereum.
- **Binance Smart Chain (BSC):** Là một bản “fork” của Ethereum, tương thích EVM. BSC ra đời để **giảm chi phí và tăng tốc độ xử lý** so với Ethereum, nên cũng được nhiều dự án DeFi sử dụng.
- **Solana:** Tốc độ rất cao, hợp đồng viết bằng Rust, phù hợp ứng dụng thời gian thực.
- **Các nền tảng khác:** Ngoài ra còn có **Polkadot, Avalanche, Tezos, Hyperledger Fabric, Cardano** (dành cho blockchain riêng tư) ... Mỗi nền tảng có đặc điểm riêng nhưng đều cho phép triển khai hợp đồng tự động theo các điều kiện đã định.

Lợi ích của hợp đồng thông minh

- **Tự động hóa:** Hợp đồng tự thực thi mà không cần giám sát thủ công.
- **Không cần trung gian:** Loại bỏ vai trò của ngân hàng, công chứng, môi giới... → giảm chi phí và rủi ro gian lận.
- **Minh bạch - Bất biến:** Mã nguồn và dữ liệu thực thi được ghi vĩnh viễn trên blockchain, không thể chỉnh sửa tùy tiện.
- **Độ tin cậy cao:** Quy tắc rõ ràng, kết quả có thể tự kiểm chứng.

Thách thức khi sử dụng hợp đồng thông minh

- **Rủi ro bảo mật:** Lỗi lập trình rất khó sửa vì blockchain bất biến (ví dụ sự cố The DAO năm 2016).
- **Chi phí và hiệu suất:** Gas fee cao và tốc độ chậm trên một số nền tảng như Ethereum.
- **Vấn đề pháp lý:** Khung pháp luật quốc tế chưa hoàn thiện, khó xác định trách nhiệm khi hợp đồng gây thiệt hại.
- **Độc quyền và linh hoạt:** Dữ liệu hợp đồng dễ bị lộ; việc cập nhật hợp đồng khó khăn.

Ứng dụng thực tế:

- **Tài chính phi tập trung (DeFi):** Toàn bộ ngành DeFi (cho vay, vay, sàn giao dịch phi tập trung) đều được xây dựng trên các hợp đồng thông minh.
- **NFT (Non-Fungible Token):** Mỗi NFT về cơ bản là một hợp đồng thông minh xác nhận quyền sở hữu một tài sản kỹ thuật số.
- **Chuỗi cung ứng:** Tự động theo dõi hàng hóa và thực hiện thanh toán khi hàng hóa đến đúng địa điểm.
- **Bỏ phiếu:** Tạo ra các hệ thống bỏ phiếu minh bạch, không thể gian lận.
- **Bất động sản:** Mua bán/thuê nhà đất tự động, Ví dụ: khi nhận đủ tiền → hợp đồng chuyển quyền sở hữu ngay trên blockchain.
- **Bảo hiểm, y tế, chứng nhận số:** Bảo hiểm tự động chi trả khi đủ điều kiện, Hồ sơ y tế bảo mật, Văn bằng, giấy tờ gắn với token blockchain để chống giả mạo.

Tóm lại, hợp đồng thông minh là thành phần cốt lõi giúp blockchain không chỉ lưu trữ dữ liệu mà còn vận hành các quy trình nghiệp vụ phức tạp một cách tự động, minh bạch và tin cậy.

7.5. Công Cụ và Công Nghệ Hỗ Trợ

a. Ngôn ngữ Solidity - Nền tảng của Hợp đồng Thông minh trên Ethereum



Hình 2.15 Solidity

Solidity là ngôn ngữ lập trình được Ethereum Foundation phát triển từ năm 2014 nhằm xây dựng hợp đồng thông minh cho Ethereum và các blockchain tương thích EVM. Với cú pháp gần gũi JavaScript/C++ và khả năng tích hợp sâu với Ethereum Virtual Machine, Solidity cho phép triển khai các ứng dụng phi tập trung có tính tự động, minh bạch và không cần bên trung gian.

Đặc trưng chính của Solidity:

- **Hướng đối tượng:** hỗ trợ kế thừa, đóng gói, hàm và cấu trúc dữ liệu.
- **Biên dịch sang bytecode EVM,** đảm bảo mọi node thực thi thống nhất.
- **Bảo mật & kiểm soát truy cập,** hạn chế rủi ro khi xử lý tài sản số.
- **Tính bất biến:** hợp đồng triển khai rồi không thể sửa đổi.
- **Cấu trúc hợp đồng rõ ràng:** state variables, functions, modifiers, events và các kiểu dữ liệu như mapping, struct, array.

Ứng dụng tiêu biểu:

- Xây dựng giao thức DeFi, phát hành token ERC-20 và NFT ERC-721.
- Triển khai hệ thống quản lý danh tính, văn bằng, chuỗi cung ứng, bô phiếu điện tử và các mô hình tự động hóa nghiệp vụ.

Solidity là công nghệ cốt lõi biến kiến trúc blockchain từ hệ thống lưu trữ thành một nền tảng tính toán phi tập trung, mở ra thế hệ ứng dụng Web3 nơi các thỏa thuận được thực thi bằng mã lệnh minh bạch và bất biến.

b. Truffle - framework phát triển ứng dụng blockchain (dApp)



Hình 2.16 Truffle

Truffle là một trong những môi trường phát triển, khung thử nghiệm và quy trình quản lý tài sản (asset pipeline) phổ biến và lâu đời nhất dành cho các blockchain tương thích với Máy ảo Ethereum (EVM). Về cơ bản, nó cung cấp cho các nhà phát triển một bộ công cụ toàn diện để đơn giản hóa toàn bộ vòng đời phát triển hợp đồng thông minh, từ việc viết mã cho đến triển khai và quản lý sau đó.

Đặc điểm và chức năng chính:

- Biên dịch hợp đồng: tự động biên dịch Solidity thành bytecode và ABI để triển khai trên EVM.
- Triển khai có kiểm soát: hệ thống migration scripts giúp triển khai theo từng bước, dễ quản lý phiên bản.
- Kiểm thử tích hợp: hỗ trợ unit test và integration test bằng JavaScript hoặc Solidity, giúp giảm rủi ro lỗi trước khi đưa lên mạng thật.
- Quản lý mạng linh hoạt: cho phép cấu hình nhiều môi trường như Ganache, testnet hoặc mainnet.
- Tương tác & gỡ lỗi: truffle console hỗ trợ tương tác trực tiếp với hợp đồng; truffle debug giúp phân tích giao dịch và truy vết lỗi.

Cấu trúc dự án tiêu chuẩn:

- **contracts/** - chứa mã Solidity
- **migrations/** - các script triển khai

- **test/** - bộ kiểm thử
- **truffle-config.js** - cấu hình mạng và compiler

Ưu điểm nổi bật:

- Tự động hóa toàn bộ quy trình phát triển hợp đồng.
- Tích hợp mượt với Ganache và các công cụ blockchain khác.
- Khả năng kiểm thử và gỡ lỗi mạnh, giảm thiểu rủi ro tài sản.
- Cộng đồng lớn, tài liệu phong phú, phù hợp cả người mới và chuyên gia.

Truffle đóng vai trò như bộ công cụ “tiêu chuẩn vàng” trong phát triển hợp đồng thông minh trên Ethereum, giúp rút ngắn thời gian xây dựng DApp, tăng độ an toàn và đảm bảo quy trình triển khai nhất quán.

c. Web3.js - Thư viện giao tiếp giữa ứng dụng và blockchain Ethereum



Hình 2.17 Web3.js

Web3.js là thư viện JavaScript mã nguồn mở do Ethereum Foundation phát triển nhằm giúp ứng dụng web tương tác trực tiếp với blockchain Ethereum thông qua giao thức JSON-RPC. Thư viện đóng vai trò cầu nối giữa frontend và mạng blockchain, cho phép gửi giao dịch, truy vấn dữ liệu và gọi hàm hợp đồng thông minh mà không cần lập trình viên thao tác trực tiếp với node Ethereum.

Thành phần và chức năng chính:

- **web3.eth:** quản lý tài khoản, giao dịch, tương tác với hợp đồng thông minh.
- **web3.utils:** cung cấp hàm tiện ích (chuyển đổi Ether/Wei, mã hóa, hashing).
- **web3.net:** kiểm tra trạng thái kết nối mạng.
- **Các module mở rộng:** hỗ trợ các giao thức phụ như Whisper (ít dùng).

Vai trò trong phát triển DApp:

- Kết nối frontend với smart contract thông qua ABI và địa chỉ triển khai.
- Cho phép người dùng ký giao dịch bằng ví Web3 như MetaMask.
- Hiển thị dữ liệu on-chain lên giao diện web theo thời gian thực.

Trong hệ sinh thái phát triển DApp, Web3.js là lớp giao tiếp frontend, hỗ trợ cho Truffle/Hardhat (backend) và Ganache (môi trường thử nghiệm).

Ưu điểm nổi bật:

- Dễ tích hợp với các framework web như React, Vue, Angular.
- Tương thích tốt với ví MetaMask và hầu hết các ví Web3.
- Tự động xử lý gas, nonce, ký giao dịch và quản lý luồng RPC.
- Cộng đồng lớn và tài liệu đầy đủ, phù hợp cả người mới và lập trình viên chuyên sâu.

Web3.js là thư viện tiêu chuẩn giúp ứng dụng web giao tiếp liền mạch với blockchain Ethereum. Kết hợp với Truffle và Ganache, Web3.js tạo thành nền tảng cốt lõi cho việc xây dựng ứng dụng phi tập trung (DApp) toàn diện từ triển khai hợp đồng đến tương tác người dùng.

d. Ganache



Hình 2.18 Ganache

Ganache là môi trường blockchain cá nhân do Truffle Suite phát triển, cho phép mô phỏng đầy đủ cơ chế hoạt động của mạng Ethereum ngay trên máy tính. Đây là công cụ quan trọng giúp triển khai, kiểm thử và gỡ lỗi hợp đồng thông minh nhanh chóng, an toàn và không tốn gas thật.

Đặc điểm và chức năng chính:

- **Mô phỏng mạng Ethereum:** tạo blockchain cục bộ hoạt động tương tự testnet/mainnet nhưng hoàn toàn offline.
- **Tài khoản ảo & Ether giả:** tự động tạo nhiều ví có sẵn ETH để thử nghiệm giao dịch và triển khai hợp đồng.
- **Theo dõi & gỡ lỗi giao dịch:** hiển thị block, gas, log và trạng thái giao dịch theo thời gian thực.
- **Hai phiên bản:**
 - ✓ **Ganache UI:** giao diện trực quan
 - ✓ **Ganache CLI:** công cụ dòng lệnh phục vụ automation và CI/CD.

Vai trò trong phát triển DApp:

- Cho phép triển khai hợp đồng nhiều lần mà không tốn chi phí.
- Hỗ trợ kiểm thử tự động, tái tạo kịch bản và phân tích lỗi smart contract.
- Là mạng mặc định của Truffle để chạy compile - migrate - test trước khi đưa lên testnet hoặc mainnet.

Ưu điểm nổi bật:

- Nhanh, miễn phí và không cần kết nối Internet.
- Quan sát dữ liệu blockchain trực quan qua UI.
- Tích hợp chặt chẽ với Truffle, MetaMask và các công cụ EVM khác.
- Phù hợp cho học tập, nghiên cứu và thử nghiệm chuyên sâu.

Ganache là “phòng thí nghiệm blockchain” dành cho nhà phát triển Ethereum, rút ngắn đáng kể vòng đời phát triển và đảm bảo hợp đồng thông minh hoạt động ổn định trước khi triển khai lên mạng thực.

e. Metamask



Hình 2.19 Ví Metamask

MetaMask là ví tiền mã hóa dạng phần mềm (hot wallet) và là công kết nối giữa người dùng và các blockchain tương thích EVM. Với mô hình ví phi lưu ký, MetaMask cho phép người dùng tự quản lý khóa riêng tư và seed phrase, đồng thời cung cấp giao diện đơn giản để tương tác với các ứng dụng phi tập trung (DApps).

Kiến trúc và cơ chế hoạt động:

- **Ví phi lưu ký:** khóa riêng được mã hóa và lưu cục bộ trên thiết bị, hoàn toàn do người dùng kiểm soát.
- **Tiêm mã Web3 (Web3 Injection):** MetaMask tích hợp web3.js/ethers.js vào trình duyệt, giúp ứng dụng web giao tiếp trực tiếp với blockchain.
- **Giao tiếp JSON-RPC:** các yêu cầu gửi giao dịch, đọc dữ liệu hoặc gọi hàm hợp đồng được chuyển qua RPC tới node Ethereum (thường thông qua Infura).
- **Nền tảng đa dạng:** hỗ trợ dưới dạng tiện ích mở rộng trình duyệt và ứng dụng di động.

Chức năng chính:

- **Quản lý danh tính Web3:** tạo, lưu trữ và sử dụng tài khoản blockchain mà không cần username/password.
- **Ký giao dịch:** người dùng phê duyệt các thao tác như chuyển ETH, tương tác smart contract thông qua chữ ký số sử dụng private key.
- **Quản lý mạng:** cho phép chuyển đổi giữa Ethereum Mainnet, Sepolia Testnet, các mạng Layer-2 và cả blockchain tùy chỉnh (custom RPC).
- **Tích hợp DApps:** MetaMask là ví được hỗ trợ rộng nhất trong hệ sinh thái Web3, đảm bảo kết nối liền mạch giữa người dùng và ứng dụng.

MetaMask là thành phần thiết yếu của hệ sinh thái Web3, đóng vai trò ví phi lưu ký và cầu nối giữa ứng dụng phi tập trung với blockchain. Nhờ khả năng quản lý khóa an toàn, ký giao dịch và tương tác RPC, MetaMask trở thành chuẩn phổ biến cho phát triển DApps trên Ethereum và các mạng tương thích EVM.

CHƯƠNG 3: XÂY DỰNG HỆ THỐNG QUẢN LÝ DỮ LIỆU HỌC TẬP VÀ CẤP PHÁT VĂN BẰNG SỐ

I. MÔ TẢ HỆ THỐNG

Hệ thống Quản lý Sinh viên trên Blockchain là một ứng dụng phi tập trung (DApp - Decentralized Application) được xây dựng nhằm quản lý toàn bộ quy trình đào tạo sinh viên từ khâu đăng ký, quản lý điểm số, đến cấp phát và xác thực bằng tốt nghiệp. Hệ thống được phát triển dựa trên nền tảng Ethereum Blockchain, kết hợp với công nghệ Smart Contract để đảm bảo tính minh bạch, bảo mật và không thể thay đổi của dữ liệu.

Khác với các hệ thống quản lý sinh viên truyền thống sử dụng cơ sở dữ liệu tập trung, hệ thống này tận dụng đặc tính phi tập trung của blockchain để loại bỏ điểm yếu duy nhất (single point of failure), tăng cường tính minh bạch trong quản lý học vụ, và đặc biệt là giải quyết vấn đề xác thực bằng cấp giả mạo - một thách thức lớn trong giáo dục hiện nay.

II. MỤC TIÊU CỦA HỆ THỐNG

- Số hóa toàn bộ quy trình quản lý sinh viên từ đăng ký đến tốt nghiệp
- Xây dựng cơ chế lưu trữ điểm số và bằng cấp trên blockchain đảm bảo tính bất biến
- Tạo ra hệ thống xác thực bằng tốt nghiệp nhanh chóng, chính xác và công khai
- Tự động hóa quy trình tính điểm trung bình và xét tốt nghiệp
- Giảm thiểu can thiệp thủ công, hạn chế sai sót và gian lận
- Tạo giao diện thân thiện, dễ sử dụng cho các đối tượng người dùng khác nhau
- Đảm bảo khả năng mở rộng cho số lượng sinh viên lớn

Yêu Cầu Giao Diện: Xây dựng giao diện thân thiện, dễ sử dụng cho admin, cán bộ quản lý điểm, sinh viên và doanh nghiệp bên ngoài, giao diện cung cấp đầy đủ chức năng như tìm kiếm, tra cứu thông tin, hiển thị thông báo lỗi, quản lý thông tin cá nhân, quản lý bằng cấp, chia sẻ bằng cho doanh nghiệp, thu hồi văn bằng.

Yêu cầu chức năng của Người sử dụng:

1. Admin

- Quản lý chương trình đào tạo
 - Quản lý tài khoản cán bộ quản lý điểm
 - Quản lý tài khoản sinh viên
- ### 2. Cán bộ quản lý điểm
- Nhập điểm cho sinh viên

- Quản lý điểm sinh viên
- Quản lý sinh viên tốt nghiệp

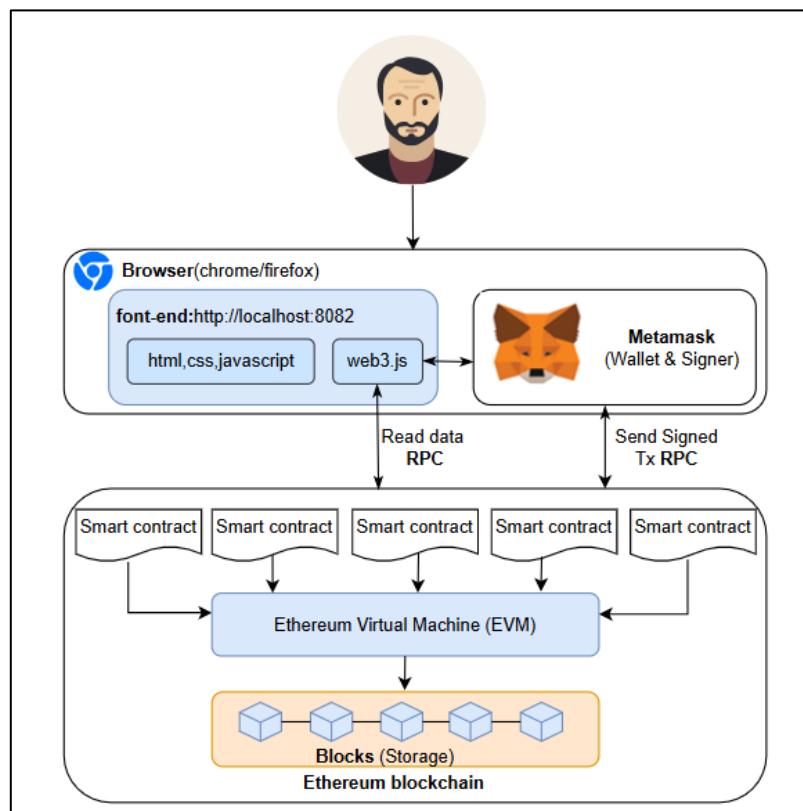
3. Sinh viên

- Quản lý thông tin cá nhân
- Quản lý hồ sơ học tập
- Xét tốt nghiệp tự động

4. Doanh nghiệp bên ngoài

- Xác thực văn bằng, xem quá trình học tập

III. MÔ HÌNH KIẾN TRÚC TỔNG QUAN HỆ THỐNG



Hình 3.1 Mô hình kiến trúc tổng quan hệ thống

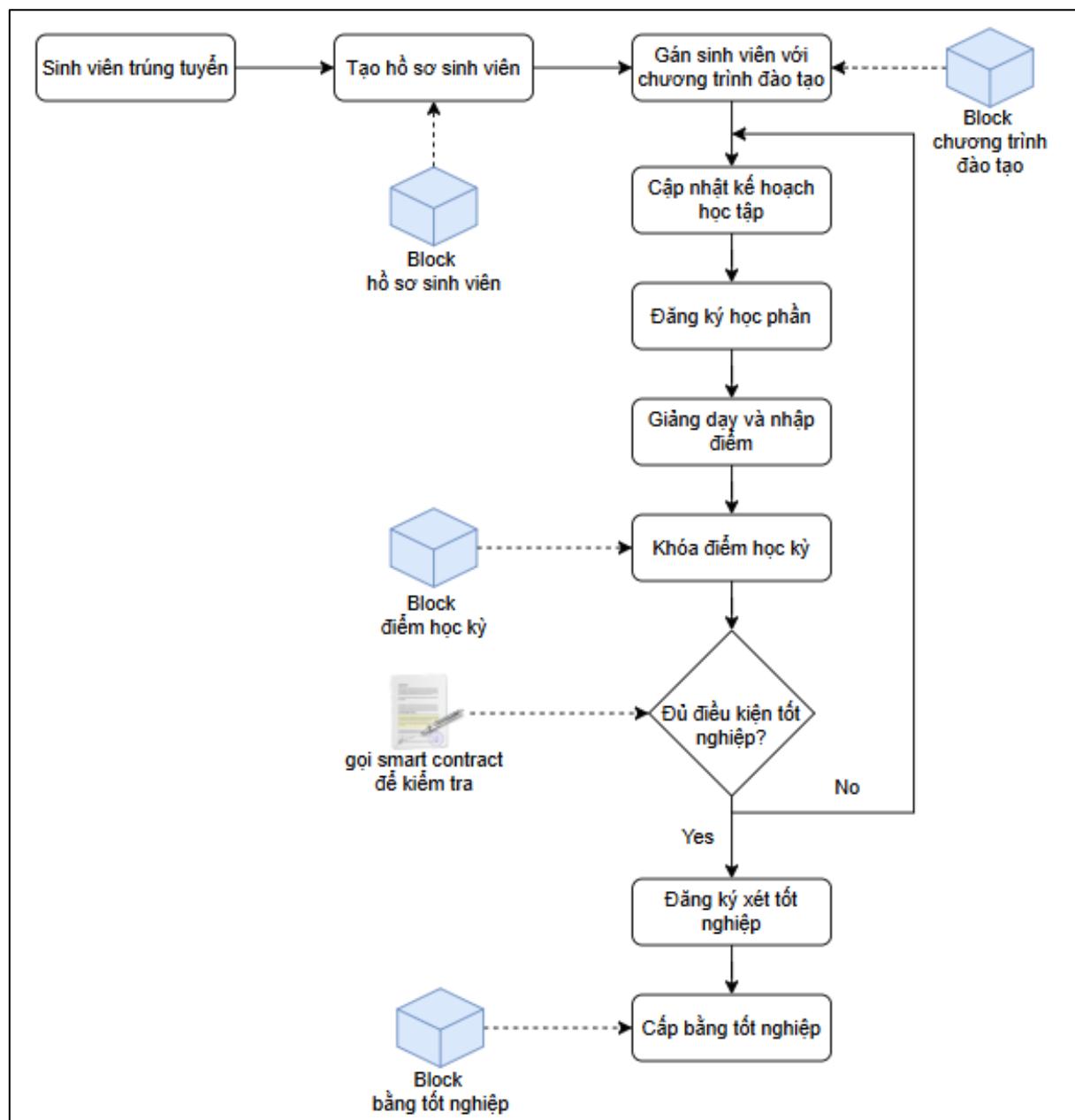
Người sử dụng (quản trị viên, cán bộ quản lý điểm, sinh viên và doanh nghiệp) tương tác với hệ thống thông qua trình duyệt web. Lớp giao diện người dùng được xây dựng bằng HTML, CSS và JavaScript, đảm nhiệm vai trò hiển thị thông tin và tiếp nhận thao tác của người dùng.

Ở tầng kết nối, thư viện web3.js đóng vai trò cầu nối giữa front-end và mạng Ethereum. Thông qua web3.js, ứng dụng có thể gửi yêu cầu đọc dữ liệu trên blockchain, gọi các hàm của hợp đồng thông minh hoặc khởi tạo giao dịch. Những giao dịch cần ch

ký số sẽ được chuyển cho ví MetaMask, nơi giữ khóa riêng tư và thực hiện quá trình ký trước khi phát tán lên mạng blockchain.

Bên dưới, Ethereum Virtual Machine (EVM) chịu trách nhiệm thực thi mã bytecode của hợp đồng thông minh, xử lý logic nghiệp vụ và ghi nhận các thay đổi trạng thái vào blockchain. Kết quả thực thi được lưu trữ trực tiếp trong cấu trúc dữ liệu của các block, đảm bảo tính bất biến và minh bạch của toàn hệ thống.

IV. CẤU TRÚC CHUỖI BLOCK LUU TRỮ HỒ SƠ HỌC TẬP CỦA SINH VIÊN

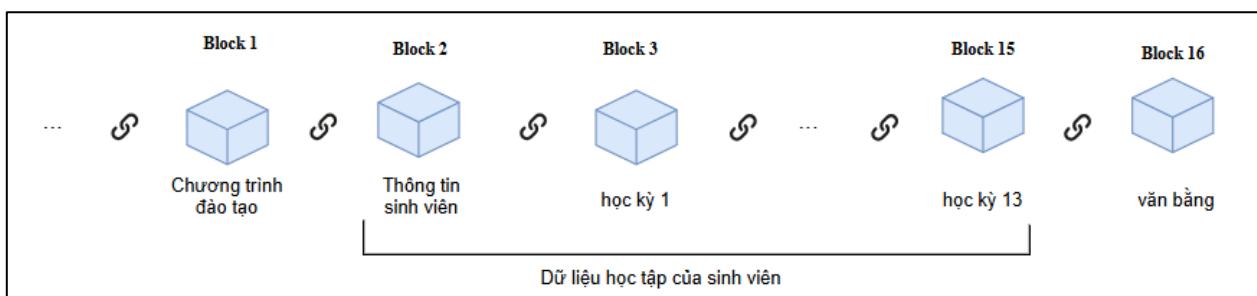


Hình 3.2 Luồng xử lý nghiệp vụ trong hệ thống quản lý dữ liệu học tập của sinh viên

Trong thiết kế hệ thống, không phải toàn bộ dữ liệu đều được đưa lên blockchain, bởi mọi thông tin được ghi lên chuỗi sẽ được lưu trữ vĩnh viễn trên toàn mạng lưới, dẫn đến chiếm dụng không gian bộ nhớ lớn. Vì vậy, hệ thống chỉ lựa chọn lưu trữ những dữ liệu có tính chất quyết định, cần bảo đảm tính toàn vẹn tuyệt đối và không được phép chỉnh sửa sau khi công bố.

Cụ thể, điểm số của sinh viên không được ghi on-chain ở từng lần nhập mà chỉ được lưu lại một bản ghi cuối cùng của mỗi học kỳ sau khi điểm đã được khóa. Cách tiếp cận này vừa giảm tải chi phí lưu trữ, vừa vẫn bảo đảm rằng kết quả học tập cuối cùng là bất biến và có thể kiểm chứng. Bên cạnh đó, các thông tin quan trọng khác như hồ sơ sinh viên, văn bằng tốt nghiệp và đặc biệt là chương trình đào tạo cũng được lưu trực tiếp trên blockchain. Việc đưa chương trình đào tạo lên chuỗi cho phép smart contract tự động đổi chiếu số tín chỉ, học phần bắt buộc, học phần tự chọn và các điều kiện tốt nghiệp khác, từ đó tự động quyết định việc cấp văn bằng cho sinh viên khi họ đạt đủ yêu cầu.

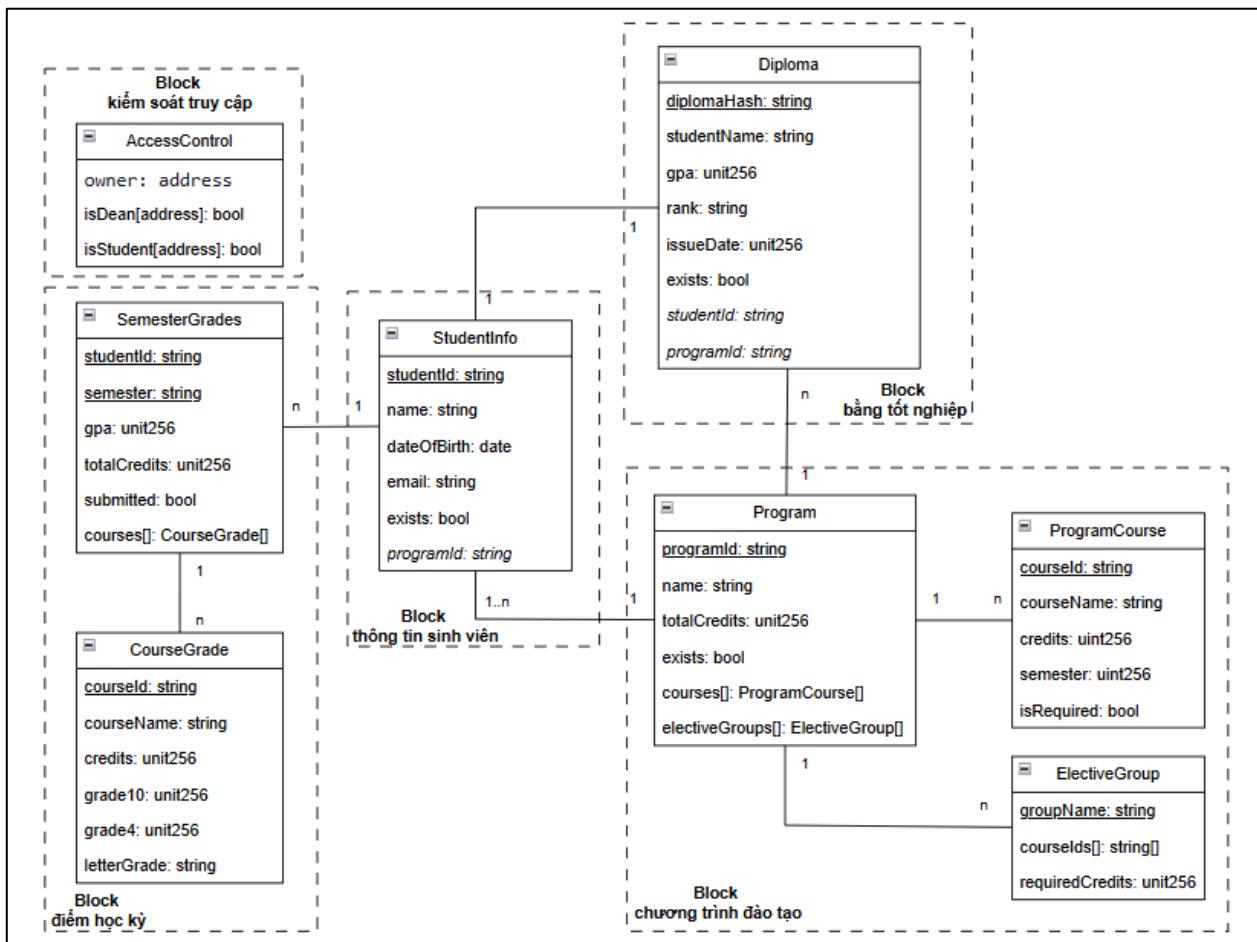
Cách tổ chức dữ liệu này cân bằng giữa tính bất biến của blockchain và hiệu quả sử dụng tài nguyên, đảm bảo rằng chỉ những thành phần dữ liệu mang giá trị pháp lý và kiểm chứng mới được lưu trữ vĩnh viễn trên chuỗi khôi. Đây là chiến lược phù hợp cho các hệ thống giáo dục sử dụng blockchain ở quy mô lớn, nơi tính toàn vẹn và khả năng xác thực phải được ưu tiên nhưng vẫn phải kiểm soát chi phí vận hành.



Hình 3.3 Cấu trúc chuỗi block lưu trữ hồ sơ học tập của sinh viên

Dữ liệu của một sinh viên bao gồm nhiều thành phần được ghi nhận xuyên suốt quá trình học tập. Cụ thể, hệ thống lưu lại chương trình đào tạo mà sinh viên theo học, thông tin cá nhân của sinh viên, dữ liệu của từng học kỳ (học phần và điểm số hoàn thành). Khi sinh viên đủ điều kiện tốt nghiệp và đăng ký xét tốt nghiệp, văn bằng tốt nghiệp được smart contract tạo tự động như phần dữ liệu cuối cùng. Tập hợp các thành phần này tạo nên toàn bộ hồ sơ học tập đầy đủ của một sinh viên.

V. THIẾT KẾ CÁU TRÚC DỮ LIỆU CHO CÁC KHỐI BLOCKCHAIN



Hình 3.4 Cấu trúc dữ liệu cho các khối blockchain

Mô tả các lớp: Các lớp trong mô hình này không phản ánh cấu trúc của một hệ quản trị cơ sở dữ liệu quan hệ (RDBMS), mà được xây dựng theo phong cách UML để biểu diễn các cấu trúc dữ liệu được lưu trực tiếp trên blockchain. Mục tiêu là giúp quan sát mối quan hệ giữa các thành phần một cách trực quan, trước khi triển khai thành các cấu trúc dữ liệu Solidity.

Bảng 3.1 Danh sách các bảng dữ liệu trong hệ thống

#	Tên bảng	Mô tả
1	AccessControl	Quản lý phân quyền trong hệ thống
2	Diploma	Thông tin sinh viên
3	Program	Chương trình đào tạo
4	SemesterGrades	Điểm từng học kỳ
5	Diploma	Bằng tốt nghiệp
6	CourseGrade	Điểm từng học phần
7	ProgramCourse	Học phần bắt buộc nằm trong chương trình đào tạo
8	ElectiveGroup	Nhóm môn tự chọn nằm trong chương trình đào tạo

Mô tả các Block dữ liệu lưu trên blockchain: Mặc dù mô hình được trình bày dưới dạng sơ đồ quan hệ để dễ theo dõi, dữ liệu thực tế được lưu trực tiếp dưới dạng các cấu trúc (struct) trong smart contract trên blockchain. Mỗi loại dữ liệu chính tương ứng với một “block logic”, phản ánh một tập thông tin bất biến theo thời gian.

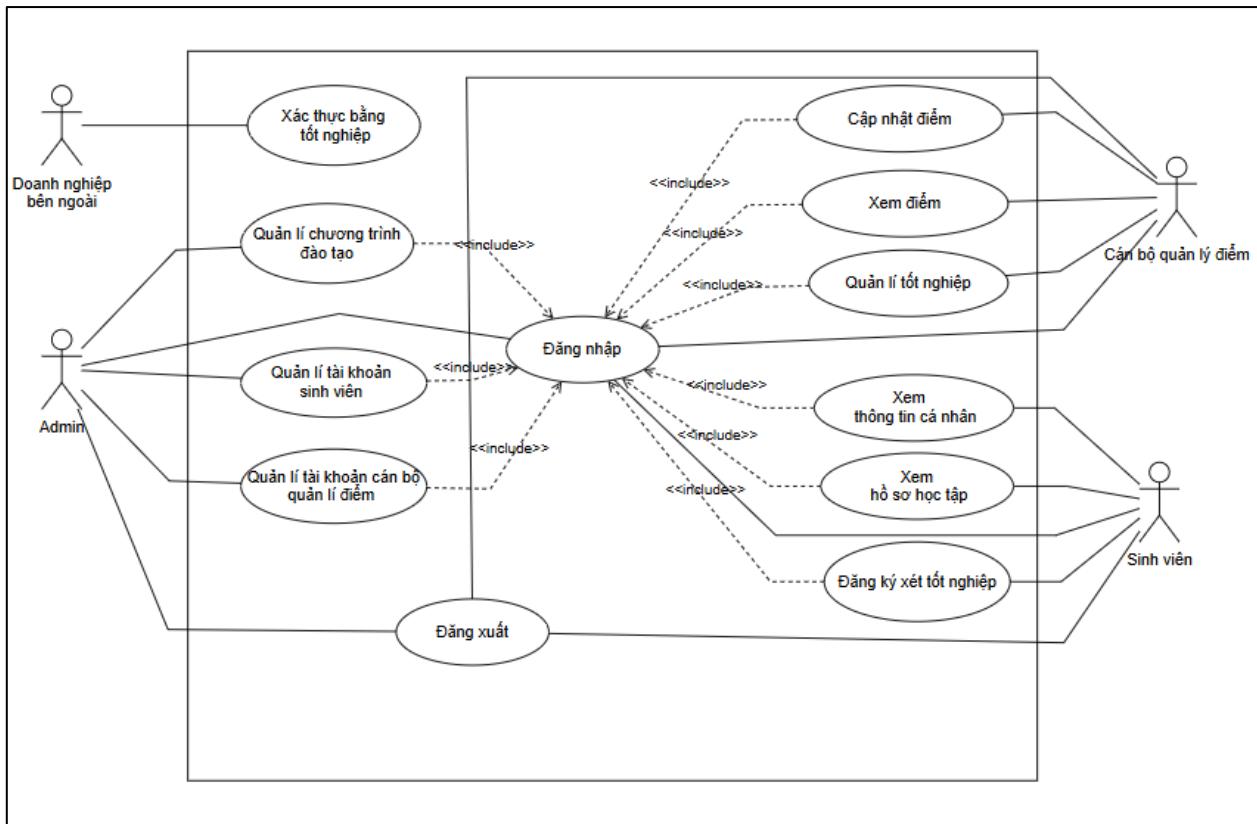
- **Block chương trình đào tạo:** Block này biểu diễn một chương trình đào tạo duy nhất, bao gồm danh sách các học phần bắt buộc và các nhóm học phần tự chọn với số tín chỉ yêu cầu. Toàn bộ dữ liệu được lưu trực tiếp lên blockchain nhằm bảo đảm tính minh bạch và hỗ trợ quá trình kiểm tra điều kiện tốt nghiệp một cách tự động, chính xác.
- **Block thông tin sinh viên:** Block này lưu trữ dữ liệu nhận diện của sinh viên như mã số sinh viên, họ tên, ngày sinh và email. Đây là lớp dữ liệu lõi liên kết với điểm học kỳ, chương trình đào tạo và văn bằng. Khi được ghi lên blockchain, các thông tin này trở nên bất biến và có thể xác thực bởi bất kỳ bên thứ ba nào.
- **Block điểm học kỳ:** Mỗi học kỳ của sinh viên được ghi thành một block riêng biệt, bao gồm danh sách điểm từng học phần, GPA và tổng số tín chỉ tích lũy trong kỳ. Khi học kỳ được khóa, toàn bộ dữ liệu không thể chỉnh sửa, đảm bảo tính toàn vẹn và minh bạch của kết quả học tập theo thời gian.
- **Block bằng tốt nghiệp:** Block văn bằng là kết quả cuối cùng của toàn bộ quá trình học tập, liên kết trực tiếp với dữ liệu sinh viên và chương trình đào tạo. Các thông tin như GPA tốt nghiệp, xếp loại và ngày cấp được lưu dưới dạng bất biến, phục vụ xác thực văn bằng một cách công khai và đáng tin cậy.

VI. SƠ ĐỒ USE CASE VÀ MÔ TẢ CHỨC NĂNG

6.1. Sơ Đồ Use Case

a. Sơ Đồ Tổng Quát

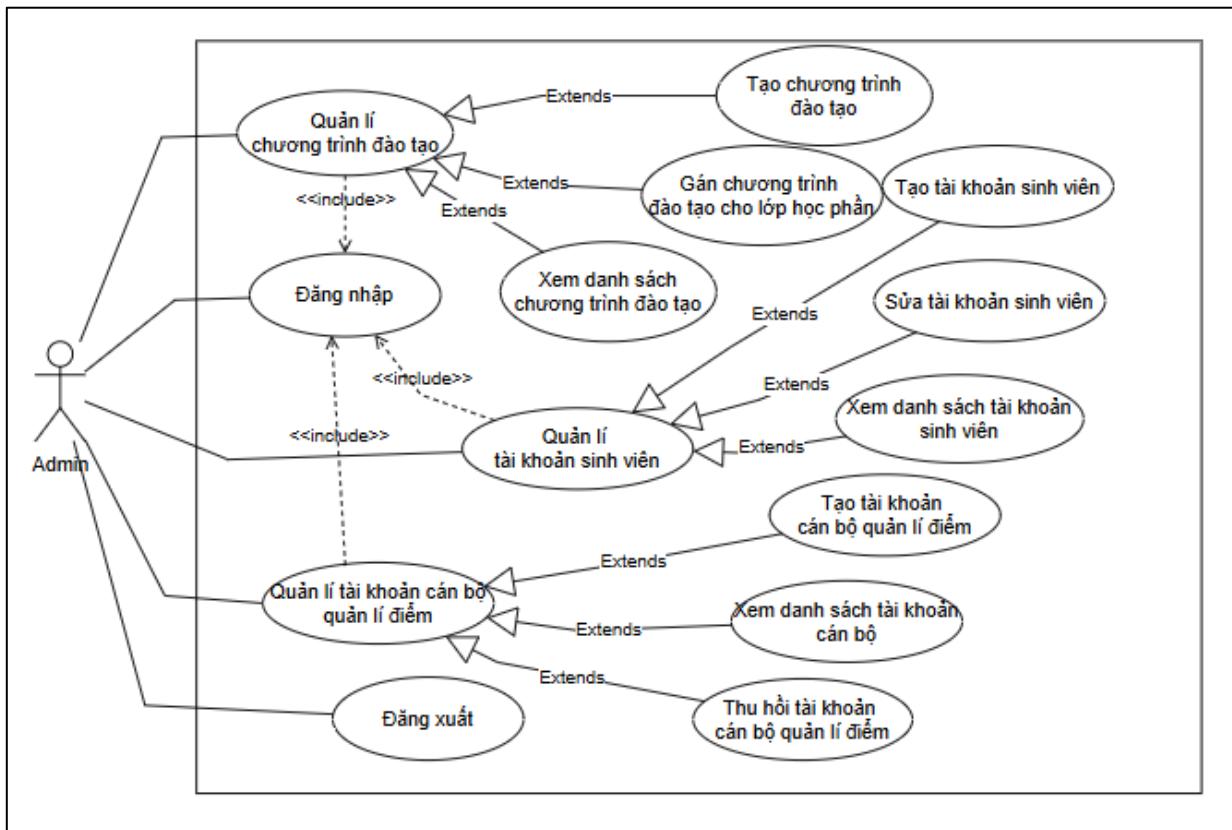
Sơ đồ use case tổng quát của hệ thống bao gồm các nhóm người dùng (actors) và các chức năng cơ bản của hệ thống được thể hiện như hình 3.5



Hình 3.5 Sơ đồ use case tổng quát

b. Chức năng của actor “Admin”

Admin là người quản lí hệ thống, cũng là người triển khai hợp đồng thông minh. Những chức năng của actor được mô tả như hình 3.6

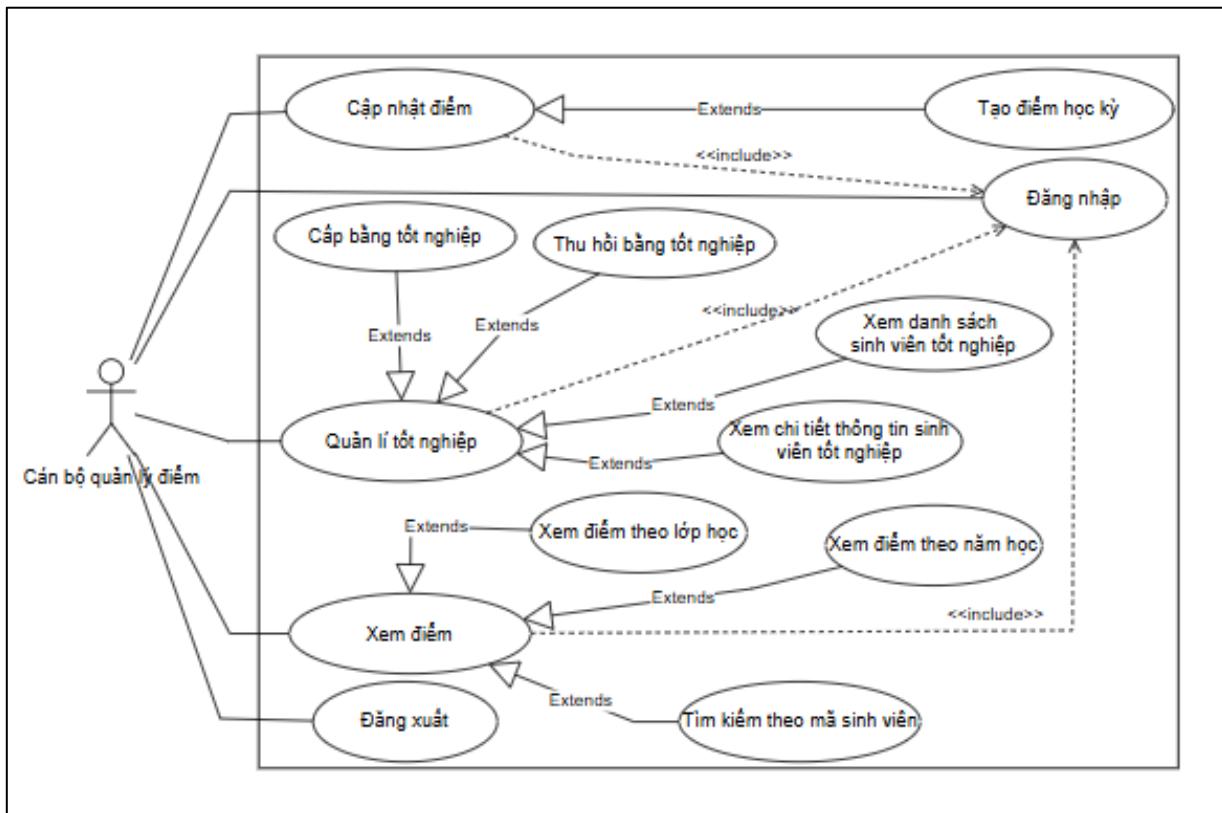


Hình 3.6 Sơ đồ use case của actor Admin

- **Chức năng Quản lý chương trình đào tạo:** cho phép Admin tạo chương trình đào tạo mới hoặc gắn những chương trình đào tạo đã tạo với một lớp học nào đó.
- **Chức năng quản lý tài khoản sinh viên:** cho phép Admin tạo tài khoản cho sinh viên, sửa đổi tài khoản nếu có sai sót hay cần sửa đổi, xem danh sách tài khoản sinh viên đã tạo.
- **Chức năng quản lý tài khoản cán bộ quản lý điểm:** cho phép Admin tạo tài khoản cho cán bộ quản lý điểm, xem danh sách tài khoản cán bộ, thu hồi tài khoản nếu cán bộ không còn thực hiện nhiệm vụ nữa.

c. Use case của cán bộ quản lý điểm

Cán bộ quản lý điểm là những nhân sự được cấp tài khoản để đăng nhập vào hệ thống. Những chức năng của Actor này được mô tả như hình 3.7

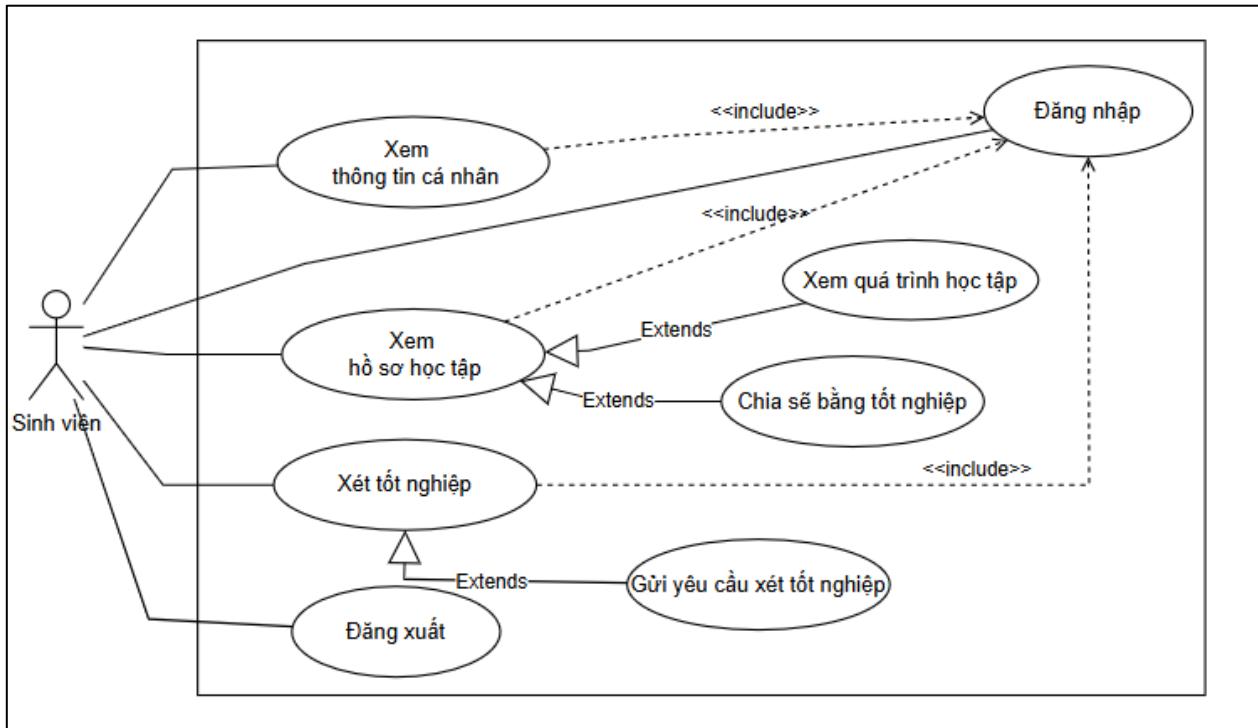


Hình 3.7 Sơ đồ use case của actor Cán bộ quản lý điểm

- **Chức năng cập nhật điểm:** cho phép cán bộ quản lý điểm gửi dữ liệu điểm ở cuối mỗi học kỳ lên blockchain (khóa điểm ở mỗi học kỳ), không cho phép sửa đổi điểm khi đã lưu trữ.
- **Chức năng xem điểm:** cho phép cán bộ có thể xem điểm vừa tạo, xem điểm theo từng lớp học, theo từng năm học hoặc có thể tìm kiếm theo mã số sinh viên, tên sinh viên.
- **Chức năng quản lý tốt nghiệp:** cho phép cán bộ có thể cấp bằng cho sinh viên đủ điều kiện và đã đăng ký xét tốt nghiệp, cho phép cán bộ có thể xem danh sách sinh viên nào đã tốt nghiệp (có thể tìm kiếm theo lớp học, năm tốt nghiệp hoặc mã sinh viên), cho phép cán bộ có thể xem chi tiết điểm và thông tin cá nhân của sinh viên đã tốt nghiệp hay thu bằng của sinh viên nếu phát hiện sai phạm.

d. Use Case Sinh Viên

Sinh viên là những người học được cấp tài khoản để đăng nhập vào hệ thống, những chức năng của actor được mô tả như hình 3.8



Hình 3.8 Sơ đồ use case của actor Sinh viên

- **Chức năng quản lý thông tin cá nhân:** sinh viên có thể xem thông tin cá nhân của mình.
- **Chức năng quản lý hồ sơ học tập:** cho phép sinh viên có thể xem điểm quá trình học tập của mình theo từng học kỳ, có thể quản lý và chia sẻ thông tin bằng tốt nghiệp của mình cho doanh nghiệp.
- **Chức năng xét tốt nghiệp:** cho phép sinh viên có thể gửi yêu cầu đến smart contract để xét tốt nghiệp tự động.

6.2. Mô Tả Hệ Thống

a. *Chức năng đăng nhập*

Chức năng “đăng nhập” là một trong những chức năng của actor trừ doanh nghiệp, cho phép người dùng đăng nhập vào hệ thống, các chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.2

Bảng 3.2 Bảng mô tả chức năng Đăng nhập

Tên chức năng	Đăng nhập
Tóm Tắt	Cho phép người dùng có tài khoản đăng nhập vào hệ thống.
Actor	Admin, Cán bộ quản lý điểm, sinh viên
Điều kiện tiên quyết	Người dùng đã có tài khoản, tài khoản hợp lệ và đăng nhập thành công vào hệ thống.
Kịch bản thường	<ol style="list-style-type: none"> 1. Người dùng tải ví metamask từ cửa hàng ứng dụng web. 2. Người dùng vào ví metamask nhập privatekey được cấp. 3. Người dùng vào trang web của hệ thống. 4. Hệ thống yêu cầu đăng nhập bằng ví metamask. 5. Người dùng cho phép kết nối metamask. 6. Người dùng nhấn nút đăng nhập 7. Hệ thống xác thực thông tin đăng nhập. <p><i>Có thể nhảy đến:</i></p> <p><i>A1: Người dùng nhập sai ví.</i></p> <ol style="list-style-type: none"> 8. Nếu thông tin đúng, hệ thống cho phép sử dụng, với quyền hạn tương ứng với quyền hạn của người dùng.
Kịch bản thay thế	<p><i>A1: Người dùng nhập sai ví.</i></p> <ol style="list-style-type: none"> 8. Hệ thống hiển thị bạn không có quyền sử dụng hệ thống.
Kết quả	Đăng nhập thành công và cho phép người dùng sử dụng các chức năng theo quyền hạn.

b. Chức năng quản lý chương trình đào tạo

Chức năng “quản lý chương trình đào tạo” là một chức năng của Admin, Cho phép Admin tạo chương trình đào tạo mới chương trình đào tạo, gắn những chương trình đào tạo đã tạo với một lớp học nào đó hoặc xem danh sách chương trình đào tạo, các chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.3

Bảng 3.3 Bảng mô tả chức năng Quản lý chương trình đào tạo

Tên chức năng	Quản lí chương trình đào tạo
Tóm Tắt	Cho phép Admin tạo chương trình đào tạo mới, gắn chương trình đào tạo đã tạo với một lớp học nào đó hoặc xem danh sách chương trình đào tạo.
Actor	Admin
Điều kiện tiên quyết	Đăng nhập thành công vào hệ thống.
Kịch bản thường	<p>1. Admin vào trang quản lí chương trình đào tạo.</p> <p>2. Admin chọn chức năng đăng nhập bằng ví metamask.</p> <p>2.1 Tạo chương trình đào tạo</p> <p>2.1.1 Admin click vào chọn file excel chương trình đào tạo</p> <p>2.1.2 Chọn file json của chương trình đào tạo cần tạo</p> <p>2.1.3 Hệ thống hiển thị chi tiết chương trình đào tạo.</p> <p>2.1.4 Admin chọn upload lên blockchain.</p> <p>2.1.5 Ví metamask hiện lên cho admin ký</p> <p>Có thể nhảy đến:</p> <p><i>A1 - Admin tắt extension ví metamask</i></p> <p>2.1.6 Hệ thống kiểm tra và upload lên blockchain.</p> <p>Có thể nhảy đến:</p> <p><i>A2 - Chương trình đã tồn tại.</i></p> <p><i>A3 - Không đủ phí gas.</i></p> <p>2.1.7 Hệ thống hiển thị thành công, kết thúc quá trình.</p> <p>2.2 Admin chọn gán chương trình đào tạo với lớp học.</p> <p>2.2.1 Admin chọn chương trình đào tạo trong danh sách</p> <p>2.2.2 Nhập mã lớp học phần cần gán</p> <p>2.2.3 Nhấn nút button gắn chương trình đào tạo cho lớp</p> <p>2.2.4 Ví metamask hiện lên cho admin ký</p> <p>Có thể nhảy đến:</p> <p><i>A4 - Admin tắt extension ví metamask</i></p> <p>2.2.5 Hệ thống kiểm tra và upload lên blockchain.</p> <p>Có thể nhảy đến:</p>

	<p><i>A5 - Lớp đã tồn tại</i> <i>A6 - Không đủ phí gas.</i></p> <p>2.2.6 Lớp đã gắn với chương trình đào tạo, kết thúc quá trình.</p>
Kịch bản thay thế	<p><i>A1 - Admin tắt extension ví metamask</i> <i>A1 bắt đầu ở bước 2.1.5</i></p> <p>2.1.6 Hiển thị lỗi ký, có thể quay lại bước 2.1.1</p> <p><i>A2 - Chương trình đã tồn tại.</i></p> <p><i>A2 bắt đầu ở bước 2.1.6</i></p> <p>2.1.7 Hiển thị lỗi chương trình đã tồn tại, có thể bắt đầu lại ở bước 2.1.1</p> <p><i>A3 - Không đủ phí gas.</i></p> <p><i>A3 bắt đầu ở bước 2.1.6</i></p> <p>2.1.7 Hiển thị lỗi không đủ phí gas, có thể thực hiện lại ở bước 2.1.1</p> <p><i>A4 - Admin tắt extension ví metamask</i></p> <p><i>A5 bắt đầu ở bước 2.2.4</i></p> <p>2.2.5 Hiển thị lỗi ký, có thể bắt đầu lại bước 2.2.1</p> <p><i>A5 - Lớp đã tồn tại.</i></p> <p><i>A5 bắt đầu ở bước 2.2.5</i></p> <p>2.2.6 Hiển thị lỗi lớp đã tồn tại, có thể bắt đầu lại ở bước 2.2.1</p> <p><i>A6 - Không đủ phí gas.</i></p> <p><i>A6 bắt đầu ở bước 2.2.5</i></p> <p>2.2.6 Hiển thị lỗi không đủ phí gas, có thể thực hiện lại ở bước 2.2.1</p>
Kết quả	Tạo thành công chương trình đào tạo, gán thành công chương trình với lớp học.

c. **Chức năng quản lý tài khoản sinh viên**

Chức năng “quản lý tài khoản sinh viên” là một chức năng của Admin, cho phép Admin tạo tài khoản cho sinh viên, sửa đổi tài khoản nếu có sai sót hay cần sửa đổi, xem danh sách sinh viên đã tạo, các chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.4

Bảng 3.4 Bảng mô tả chức năng Quản lý tài khoản sinh viên

Tên chức năng	Quản lý tài khoản sinh viên
Tóm Tắt	Chức năng quản lý tài khoản sinh viên: cho phép Admin tạo tài khoản cho sinh viên, sửa đổi tài khoản nếu có sai sót hay cần sửa đổi, xem danh sách sinh viên đã tạo
Actor	Admin
Điều kiện tiên quyết	Đăng nhập thành công vào hệ thống
Kịch bản thường	<p>1. Admin vào trang quản lý tài khoản đăng nhập bằng ví metamask</p> <p>2. Chức năng đăng ký sinh viên mới.</p> <p>2.1 Vào tab đăng ký từng sinh viên</p> <p>2.2 Nhập đầy đủ thông tin sinh viên</p> <p>2.3 Nhấn vào nút đăng ký sinh viên mới</p> <p>2.4 Ví metamask hiện lên cho admin ký</p> <p>Có thể nhảy đến:</p> <p><i>A1 - Admin tắt extension ví metamask</i></p> <p>2.5 Kiểm tra thông tin và upload lên blockchain</p> <p>Có thể nhảy đến:</p> <p><i>A2 - Sinh viên đã tồn tại.</i></p> <p><i>A3 - Không đủ phí gas.</i></p> <p>2.6 Upload thành công, kết thúc quá trình</p> <p>3. Đăng ký sinh viên - upload bằng file excel/csv</p> <p>3.1 Admin vào tab đăng ký sinh viên bằng file excel/csv.</p> <p>3.2 Chọn button “chọn file excel/csv”.</p> <p>3.3 Chọn file danh sách sinh viên cần upload.</p> <p>3.4 Hệ thống hiển thị danh sách sinh viên sắp đăng ký, tự động loại bỏ những sinh viên đã đăng ký trước đó (nếu có).</p> <p>3.5 Kiểm tra và nhấn vào button “upload lên blockchain”.</p> <p>3.6 Hệ thống hiển thị đăng ký thành công và hiển thị danh sách vừa đăng ký.</p> <p>3.7 Kết thúc quá trình</p> <p>4. Xem danh sách sinh viên</p>

	4.1 Admin vào tab xem danh sách sinh viên. 4.2 Hệ thống hiển thị tất cả sinh viên đã đăng ký. 4.3 Admin có thể chọn lọc theo khóa học, lớp học, tìm theo mã sinh viên 4.4 Hiển thị danh sách sinh viên theo khóa học, lớp học, mã sinh viên 4.5 Kết thúc quá trình
Kịch bản thay thế	<p><i>A1 - Admin tắt extension ví metamask</i> <i>A1 bắt đầu ở bước 2.4</i> 2.5 Hiển thị lỗi, quá trình kết thúc, có thể bắt đầu lại ở bước 2.1</p> <p><i>A2 - Sinh viên đã tồn tại.</i> <i>A2 bắt đầu ở bước 2.5</i> 2.6 Hiển thị sinh viên đã tồn tại, kết thúc quá trình.</p> <p><i>A3 - Không đủ phí gas.</i> <i>A3 bắt đầu ở bước 2.5</i> 2.6 hiển thị lỗi không đủ phí gas, kết thúc quá trình.</p>
Kết quả	Tạo được tài khoản sinh viên mới, sửa thông tin sinh viên hoặc xem danh sách sinh viên đã tạo.

d. Chức năng quản lý tài khoản cán bộ quản lý điểm

Chức năng “quản lý tài khoản cán bộ quản lý điểm” là một chức năng của Admin, cho phép Admin tạo tài khoản cho cán bộ quản lý điểm, xem danh sách cán bộ quản lý điểm, thu hồi tài khoản khi cán bộ không còn công tác nữa, các chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.5

Bảng 3.5 Bảng mô tả chức năng Quản lý tài khoản cán bộ quản lý điểm

Tên chức năng	Quản lý tài khoản cán bộ quản lý điểm
Tóm Tắt	Chức năng quản lý tài khoản: cho phép Admin tạo tài khoản cho cán bộ quản lý điểm, xem danh sách cán bộ quản lý điểm, thu hồi tài khoản khi cán bộ không còn công tác nữa.
Actor	Admin
Điều kiện tiên quyết	Đăng nhập thành công vào hệ thống
Kịch bản thường	<p>1. Admin vào trang quản lý tài khoản đăng nhập bằng ví metamask</p> <p>2. Đăng ký cán bộ quản lý điểm</p> <p>2.1 Admin vào tab đăng ký cán bộ quản lý điểm</p> <p>2.2 Admin nhập thông tin tài khoản của cán bộ</p> <p>2.3 Nhấn vào nút “đăng ký”</p> <p>2.4 Hiển thị ví metamask và ký</p> <p>Có thể nhảy đến:</p> <p><i>A1 - Admin tắt extension ví metamask</i></p> <p>2.5 Hệ thống kiểm tra hợp lệ</p> <p>Có thể nhảy đến:</p> <p><i>A2 - Cán bộ đã tồn tại.</i></p> <p>2.6 Hiển thị thành công, kết thúc quá trình.</p> <p>3. Xem danh sách cán bộ quản lý điểm</p> <p>3.1 Admin vào tab đăng ký cán bộ quản lý điểm.</p> <p>3.2 Đến mục danh sách cán bộ quản lý điểm.</p> <p>3.3 Kết thúc quá trình</p> <p>4. Thu hồi tài khoản cán bộ quản lý điểm</p> <p>4.1 Admin vào tab đăng ký cán bộ quản lý điểm.</p> <p>4.2 Đến mục danh sách cán bộ quản lý điểm</p> <p>4.3 Nhấn nút thu hồi.</p> <p>4.4 Ví metamask hiện lên và admin ký</p> <p>4.5 Hiển thị thành công, kết thúc quá trình</p>
Kịch bản thay thế	<i>A1 - Admin tắt extension ví metamask</i>

	<p>A1 bắt đầu ở bước 2.4</p> <p>2.5 Hiển thị lỗi, quá trình kết thúc, có thể bắt đầu lại ở bước 2.1</p> <p>A2 - Cán bộ đã tồn tại.</p> <p>A2 bắt đầu ở bước 2.5</p> <p>2.6 Hiển thị sinh viên đã tồn tại, kết thúc quá trình.</p>
Kết quả	Thêm, xem danh sách hoặc thu hồi tài khoản của cán bộ quản lý điểm

e. **Chức năng cập nhật điểm**

Chức năng “cập nhật điểm” là một chức năng của cán bộ quản lý điểm, cho phép cán bộ quản lý điểm gửi dữ liệu điểm ở cuối mỗi học kỳ lên blockchain (khóa điểm ở mỗi học kỳ), không cho phép sửa đổi điểm khi đã lưu trữ, các chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.6

Bảng 3.6 Bảng mô tả chức năng Cập nhật điểm

Tên chức năng	Cập nhật điểm
Tóm Tắt	Chức năng cập nhật điểm: cho phép cán bộ quản lý điểm gửi dữ liệu điểm ở cuối mỗi học kỳ lên blockchain (khóa điểm ở mỗi học kỳ), không cho phép sửa đổi điểm khi đã lưu trữ.
Actor	Cán bộ quản lý điểm
Điều kiện tiên quyết	Đăng nhập thành công vào hệ thống
Kịch bản thường	<ol style="list-style-type: none"> 1. Người dùng đăng nhập thành công vào trang quản lý nhập điểm 2. Vào tab nhập điểm. 3. Nhấn vào button chọn file excel 4. Chọn file excel điểm của học kỳ cần nhập 5. Hiển thị danh sách từng sinh viên/ từng học kỳ (có thể xem chi tiết điểm của từng sinh viên) 6. Nhấn vào nút upload lên blockchain 7. Hiển thị ví metamask, Cán bộ ký vào. <p>Có thể nhảy đến:</p> <p>A1: Tắt ví metamask</p> <ol style="list-style-type: none"> 8. Hiển thị thành công và hiện danh sách sinh viên đã được ghi, kết thúc quá trình
Kịch bản thay thế	<p>A1: Tắt ví metamask</p> <p>A1 bắt đầu ở bước 7</p> <p>7. Hiển thị lỗi, kết thúc quá trình</p>
Kết quả	Thành công upload điểm của sinh viên lên blockchain

f. Chức năng xem điểm

Chức năng “xem điểm” là một chức năng của cán bộ quản lý điểm, cho phép cán bộ có thể xem điểm vừa tạo, xem điểm theo từng lớp học, theo từng năm học hoặc có thể tìm kiếm theo mã số sinh viên, tên sinh viên, các chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.7

Bảng 3.7 Xem điểm sinh viên

Tên chức năng	Xem điểm của sinh viên
Tóm Tắt	Chức năng xem điểm: cho phép cán bộ có thể xem điểm vừa tạo, xem điểm theo từng lớp học, theo từng năm học hoặc có thể tìm kiếm theo mã số sinh viên, tên sinh viên.
Actor	Cán bộ quản lý điểm
Điều kiện tiên quyết	Đăng nhập thành công vào hệ thống
Kịch bản thường	<ol style="list-style-type: none"> 1. Người dùng đăng nhập thành vào trang quản lý nhập điểm 2. Vào tab xem điểm đã nhập 3. Hệ thống hiển thị danh sách điểm của sinh viên đã nhập 4. Cán bộ có thể lọc điểm theo lớp, năm, mã sinh viên 5. Hệ thống hiển thị điểm theo lớp, năm, mã sinh viên 6. Kết thúc quá trình
Kịch bản thay thế	-
Kết quả	Cán bộ quản lý điểm có thể xem điểm sinh viên theo lớp, năm, mã sinh viên.

g. Chức năng quản lý sinh viên tốt nghiệp

Chức năng “Quản lý sinh viên tốt nghiệp” là một chức năng của cán bộ quản lý điểm, cho phép cán bộ có thể cấp bằng cho sinh viên đủ điều kiện và đã đăng ký xét tốt nghiệp, xem danh sách sinh viên nào đã tốt nghiệp (có thể tìm kiếm theo lớp học, năm tốt nghiệp), cho phép cán bộ có thể xem chi tiết thông tin điểm và thông tin cá nhân của sinh viên đã tốt nghiệp, ngoài ra còn có thể thu hồi bằng tốt nghiệp của sinh viên, các chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.8

Bảng 3.8 Bảng mô tả chức năng Quản lý sinh viên tốt nghiệp

Tên chức năng	Quản lý sinh viên tốt nghiệp
Tóm Tắt	Chức năng quản lý sinh viên tốt nghiệp: cho phép cán bộ có thể cấp bằng tốt nghiệp cho sinh viên đủ điều kiện và đã đăng ký xét tốt nghiệp, xem danh sách sinh viên nào đã tốt nghiệp (có thể tìm kiếm theo lớp học, năm tốt nghiệp), cho phép cán bộ có thể xem chi tiết thông tin điểm và thông tin cá nhân của sinh viên đã tốt nghiệp, cán bộ có thể thu hồi bằng tốt nghiệp của sinh viên.
Actor	Cán bộ quản lý điểm
Điều kiện tiên quyết	Đăng nhập thành công vào hệ thống
Kịch bản thường	<ol style="list-style-type: none"> 1. Người dùng đăng nhập thành vào trang quản lý nhập điểm. 2. Vào tab sinh viên tốt nghiệp. <ol style="list-style-type: none"> 2.1. Hệ thống hiển thị danh sách sinh viên đã tốt nghiệp. 2.2. Cán bộ quản lý điểm có thể lọc sinh viên theo năm tốt nghiệp, lớp, hoặc mã sinh viên, ngoài ra có tùy chọn xuất file excel. 2.3. Hiển thị danh sách sinh viên (cán bộ có thể xem chi tiết từng sinh viên hoặc thu hồi bằng tốt nghiệp, ký xác nhận thu hồi) 2.4 Kết thúc quá trình 3. Vào tab danh sách xét tốt nghiệp. <ol style="list-style-type: none"> 3.1 Hệ thống hiển thị danh sách sinh viên đã đăng ký xét tốt nghiệp 3.2 Cán bộ quản lý điểm có thể lọc sinh viên theo năm tốt nghiệp, lớp, hoặc mã sinh viên 3.3 Hiển thị danh sách sinh viên (cán bộ có thể cấp bằng tốt nghiệp, ký xác nhận cấp bằng tốt nghiệp hoặc từ chối cấp bằng tốt nghiệp) 3.4 Kết thúc quá trình
Kịch bản thay thế	-
Kết quả	Xem thành công danh sách sinh viên hoặc thu hồi bằng.

h. Chức năng Xem thông tin cá nhân

Chức năng “Xem thông tin cá nhân” là một chức năng của cán sinh viên, cho phép sinh viên có thể xem thông tin cá nhân của mình, các chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.9

Bảng 3.9 Bảng mô tả chức năng Xem thông tin cá nhân

Tên chức năng	Xem thông tin cá nhân
Tóm Tắt	Chức năng quản lý thông tin cá nhân: sinh viên có thể xem thông tin cá nhân của mình.
Actor	Sinh viên
Điều kiện tiên quyết	Đăng nhập thành công vào hệ thống
Kịch bản thường	<ol style="list-style-type: none"> 1. Sinh viên đăng nhập thành công vào trang cổng sinh viên 2. Đến phần thông tin cá nhân 3. Kết thúc quá trình
Kịch bản thay thế	-
Kết quả	Sinh viên có thể xem thông tin cá nhân của mình.

i. Chức năng Xem hồ sơ học tập

Chức năng “Xem hồ sơ học tập” là một chức năng của sinh viên, cho phép sinh viên có thể xem điểm quá trình học tập của mình theo từng học kỳ, xem bằng tốt nghiệp và chia sẻ thông tin bằng tốt nghiệp của mình cho doanh nghiệp, các chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.10

Bảng 3.10 Bảng mô tả chức năng Xem hồ sơ học tập

Tên chức năng	Xem hồ sơ học tập
Tóm Tắt	Chức năng quản lý hồ sơ học tập: cho phép sinh viên có thể xem điểm quá trình học tập của mình theo từng học kỳ, có thể xem và chia sẻ thông tin bằng tốt nghiệp của mình cho doanh nghiệp.
Actor	Sinh viên
Điều kiện tiên quyết	Đăng nhập thành công vào hệ thống
Kịch bản thường	<ol style="list-style-type: none"> 1. Sinh viên đăng nhập thành công vào trang “cổng sinh viên” Có thể nhảy đến: <i>A1: Sinh viên đã tốt nghiệp</i> 2. Bấm vào button tải điểm tất cả học kỳ. 3. Hệ thống sẽ tải và hiển thị điểm của sinh viên theo từng học kỳ. 4. Kết thúc quá trình

Kịch bản thay thế	<p><i>A1: Sinh viên đã tốt nghiệp</i></p> <p>A1 bắt đầu ở bước 1</p> <p>2. hiển thị văn bằng tốt nghiệp</p> <p> 2.1 Tùy chọn: chia sẻ bằng tốt nghiệp</p> <p> 2.2 Tùy chọn: tải điểm tất cả học kỳ</p> <p>3. Kết thúc quá trình</p>
Kết quả	Sinh viên có thể xem điểm của mình theo từng học kỳ, sinh viên có thể chia sẻ văn bằng của mình cho doanh nghiệp

j. *Chức năng đăng ký xét tốt nghiệp*

Chức năng “Đăng ký xét tốt nghiệp” là một chức năng của sinh viên, cho phép sinh viên có thể đăng ký xét tốt nghiệp tự động dựa trên smart contract, kết quả tốt nghiệp sẽ được gửi đến trang cán bộ quản lý điểm, cán bộ quản lý điểm sẽ ký để cấp bằng tốt nghiệp cho sinh viên, các chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.11

Bảng 3.11 Bảng mô tả chức năng Đăng ký xét tốt nghiệp

Tên chức năng	Đăng ký xét tốt nghiệp
Tóm Tắt	Chức năng yêu cầu xét tốt nghiệp: cho phép sinh viên có thể gửi yêu cầu đến smart contract để xét tốt nghiệp tự động.
Actor	Sinh viên
Điều kiện tiên quyết	Đăng nhập thành công vào hệ thống
Kịch bản thường	<p>1. Sinh viên đăng nhập thành công vào trang “cổng sinh viên”</p> <p>2. Sinh viên nhấp vào button đăng ký xét tốt nghiệp</p> <p>3. Hệ thống sẽ kiểm tra điều kiện tốt nghiệp</p> <p> 4.1 Nếu sinh viên đủ điều kiện tốt nghiệp</p> <p> 4.1.1 Sinh viên nhấp vào nút đăng ký xét tốt nghiệp.</p> <p> 4.1.2 Ví metamask hiện lên cho sinh viên ký.</p> <p> 4.1.3 Hệ thống sẽ gửi đơn đăng ký đến cho cán bộ quản lý điểm.</p> <p> 4.1.4 Hệ thống hiển thị đã đăng ký thành công.</p> <p> 4.1.5 Kết thúc quá trình.</p> <p> 4.2 Nếu sinh viên chưa đủ điều kiện tốt nghiệp</p> <p> 4.2.1 Hệ thống hiển thị những điều kiện cần để tốt nghiệp, những môn sinh viên đã hoàn thành, những môn sinh viên chưa hoàn thành.</p> <p> 4.2.2 Kết thúc quá trình.</p> <p>5. Kết thúc quá trình.</p>

Kịch bản thay thế	-
Kết quả	Sinh viên có thể xét tốt nghiệp tự động, Hiển thị sinh viên đủ điều kiện tốt nghiệp hoặc chưa đủ điều kiện tốt nghiệp

k. Chức năng xác thực bằng tốt nghiệp

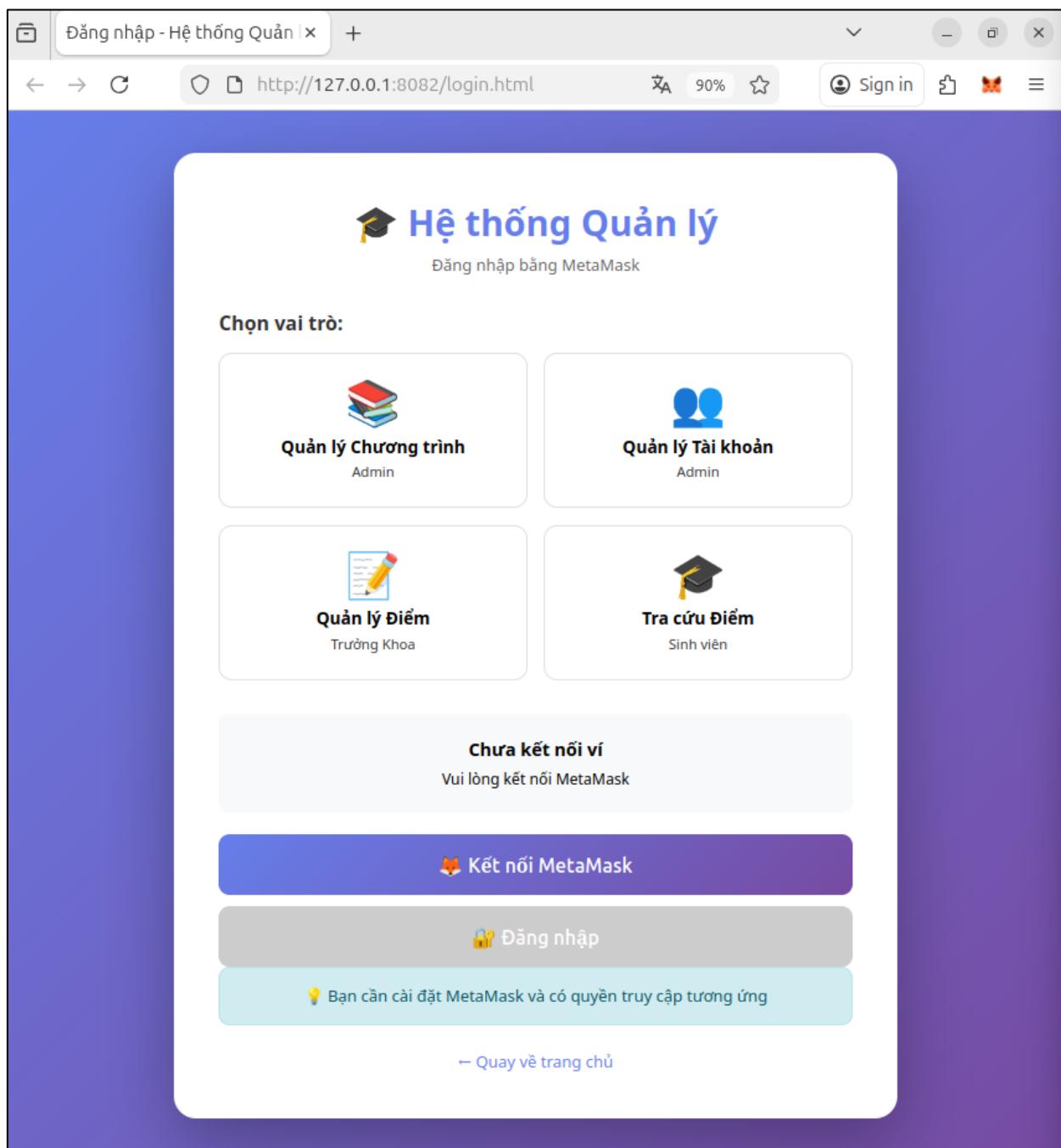
Chức năng “Xác thực bằng tốt nghiệp” là một chức năng của nhà tuyển dụng, doanh nghiệp hay bất kỳ bên thứ ba nào có thể xác thực văn bằng sinh viên, chức năng cụ thể và kịch bản của chức năng này được mô tả cụ thể trong bảng 3.12

Bảng 3.12 Bảng mô tả chức năng Xác thực bằng tốt nghiệp

Tên chức năng	Xác thực bằng tốt nghiệp
Tóm Tắt	Chức năng xác thực văn bằng tốt nghiệp: cho phép nhà tuyển dụng, doanh nghiệp hay bất kỳ bên thứ ba nào có thể xác thực văn bằng tốt nghiệp sinh viên.
Actor	Doanh nghiệp bên ngoài
Điều kiện tiên quyết	Sử dụng trình duyệt có kết nối mạng
Kịch bản thường	<ol style="list-style-type: none"> 1. Ấn nút liên kết do sinh viên gửi. 2. Hệ thống sẽ lấy văn bằng từ blockchain và hiển thị ra cho doanh nghiệp. 3. Doanh nghiệp xem bằng. 4. Doanh nghiệp có thể nhấp vào nút xem quá trình học tập. 5. Hệ thống hiển thị toàn bộ quá trình học tập của sinh viên. 6. Kết thúc quá trình
Kịch bản thay thế	-
Kết quả	Hiển thị quá trình học tập và văn bằng sinh viên hoặc hiển thị sinh viên chưa tốt nghiệp hoặc mã sinh viên không tồn tại

VII. GIAO DIỆN CHỨC NĂNG

7.1. Giao Diện Trang Đăng Nhập



Hình 3.9 Giao diện "Đăng nhập"

7.2. Giao Diện Quản Lý Chương Trình Đào Tạo

The screenshot shows the Admin Panel interface for managing programs. At the top, there's a header with a graduation cap icon, the title 'Quản lý Chương trình Đào tạo', a user profile for 'Admin' (with a hex ID), and a 'Đăng xuất' (Logout) button.

Upload Chương trình Đào tạo (CSV/Excel)

A dashed box highlights a central area where users can upload files. It features a yellow folder icon and the text 'Click để chọn file CSV hoặc Excel'. Below it, a note specifies the format: 'Format: programId, programName, description, minCredits, minGPA, requiredCourses'.

Gán Chương trình Đào tạo cho Lớp

This section allows linking classes to a program. It includes dropdown menus for 'Chọn chương trình:' (Choose program) and 'Tên lớp (Class):' (Class name), both marked with asterisks indicating they are required. A note says 'Khi gán class vào chương trình, mọi sinh viên có class đó sẽ tự động được gán vào chương trình này.' (When linking a class to a program, all students with that class will automatically be assigned to the program). A green button labeled 'Gán Class cho Chương trình' (Link Class to Program) with a checkmark icon is visible.

Hình 3.10 Giao diện upload chương trình đào tạo và gán chương trình đào tạo cho lớp

The screenshot displays the 'Danh sách Chương trình Đào tạo' (List of Programs) page. It lists two programs:

- TT&MMT2020 - Truyền thông và Mạng máy tính - Khóa 2020** (Status: Đang hoạt động)
 - Tổng tín chỉ: 156 TC | Tín chỉ tối thiểu: 0 TC | GPA tối thiểu: 2.00
 - Số môn học: 118
 - Tạo ngày: 24/11/2025
 - Các lớp: D122D2A1, D120T9A1
 - [Xem chi tiết](#)
- CNTT_2020 - Công Nghệ Thông Tin - Khóa 2020** (Status: Đang hoạt động)
 - Tổng tín chỉ: 156 TC | Tín chỉ tối thiểu: 0 TC | GPA tối thiểu: 2.00
 - Số môn học: 103
 - Tạo ngày: 24/11/2025
 - Các lớp: (Chưa có lớp nào)
 - [Xem chi tiết](#)

Hình 3.11 Giao diện xem danh sách chương trình đào tạo

7.3. Giao Diện Quản Lý Tài Khoản Sinh Viên

TÍNH NĂNG BATCH REGISTRATION:

- Gộp tất cả sinh viên vào MỘT transaction duy nhất
- Chỉ cần ký một lần thay vì ký nhiều lần
- Tiết kiệm gas fee và thời gian đăng ký
- Tất cả sinh viên vào cùng một block

MSSV	HoTen	NgaySinh	CCCD	SDT	Email	QueQuan	Lop	Nghanh	Khoa	Truong	HeDoanTao	WalletAddress	KhoaHoc
B2203710	Lê Hải Đăng	21/08/2004	093103002105	0374390243	dangb2203710@student.ctu.edu.vn	Kiên Giang	DI22D2A1	An toàn thông tin	CNTT&TT	Đại học Cần Thơ	Chinh quy	0x742d35Cc...f44e	2020

Chọn file Excel/CSV Chưa chọn file

Hình 3.12 Giao diện tạo tài khoản hàng loạt cho sinh viên

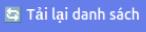
Lưu ý:

- Chức năng này chỉ cập nhật thông tin cá nhân/đào tạo của sinh viên
- KHÔNG ảnh hưởng đến điểm số đã submit
- Sinh viên phải đã được đăng ký trước đó

Mã số sinh viên (MSSV) để tìm kiếm *

Nhập MSSV cần cập nhật **Tìm kiếm**

Hình 3.13 Giao diện cập nhật thông tin sinh viên

Danh sách sinh viên đã đăng ký															
Lưu ý: Chức năng này hiển thị các sinh viên bạn đã đăng ký trong phiên làm việc hiện tại. Để xem tất cả sinh viên trong blockchain, cần query events hoặc lưu danh sách riêng.															
 Tải lại danh sách															
Khóa học:  Khóa 2022 Lớp học:  Lớp D122D2A1 Tìm kiếm:  MSSV hoặc tên...															
STT	MSSV	Họ tên	Ngày sinh	CCCD	SĐT	Email	Quê quán	Lớp	Ngành	Khoa	Trường	Hệ	Khóa	Đã lập học	
1	B2203716	Lê Hải Đăng	20/08/2003	093405993872	0357773838	lehaidang@gmail.com	Châu Thành, Kiên Giang	D122D2A1	An Toàn Thông Tin	Mạng Máy Tính	CNTT&TT	TT&MMT2020	2022	17:35 29/11	

Hình 3.14 Giao diện xem danh sách sinh viên

7.4. Giao Diện Quản Lý Tài Khoản Cán Bộ Quản Lý Điểm

Lưu ý:

- Cán bộ quản lý điểm có quyền submit điểm cho sinh viên và thu hồi bằng tốt nghiệp
- Chỉ Admin mới có quyền thêm/xóa cán bộ quản lý điểm
- Mỗi cán bộ cần có địa chỉ ví MetaMask riêng

Thêm Cán bộ quản lý điểm mới

Địa chỉ ví MetaMask *

0x...

Ví dụ: 0x1234567890123456789012345678901234567890

Họ và tên * TS. Nguyễn Văn A

Tên Khoa * Công nghệ thông tin và truyền thông

Email dean@ctu.edu.vn

Số điện thoại 0123456789

Ghi chú Thông tin bổ sung...

Hình 3.15 Giao diện tạo tài khoản cán bộ quản lý điểm

Danh sách Cán bộ quản lý điểm	
Tài lại danh sách	
Tổng số: 2 Trưởng khoa	
TS. Nguyễn Văn A <input checked="" type="checkbox"/> Active Khoa: Mạng Máy Tính Địa chỉ ví: 0xde0dA6007226B18a219cBECBA85AaF01223B60fe Email: nva@ctu.edu.vn SĐT: 0123456789 Thêm lúc: 19:21:19 24/11/2025	Xóa quyền
TS. Lê Thị B <input checked="" type="checkbox"/> Active Khoa: Công Nghệ Thông Tin Địa chỉ ví: 0xc27D92B6A6F4CF40e2d3481Fc704845457cA780f Email: ltb@ctu.edu.vn SĐT: 0123456789 Thêm lúc: 19:22:23 24/11/2025	Xóa quyền

Hình 3.16 Giao diện xem danh sách cán bộ quản lý điểm

7.5. Giao Diện Quản Lý Nhập Điểm

Hình 3.17 Giao diện quản lý nhập điểm

Hình 3.18 Giao diện xem điểm đã nhập

Quản Lý Nhập Điểm

TS. Nguyễn Văn A
0xde0da6007226b18a219cbebe85aaf01223b60fe

Đăng xuất

Hệ thống quản lý nhập điểm và xem thông tin sinh viên trên Blockchain

Nhập điểm Xem điểm đã nộp Danh sách xét tốt nghiệp Sinh viên tốt nghiệp

Bộ lọc đơn xét tốt nghiệp

Lọc theo Năm nộp đơn MSSV / Tên sinh viên

Tất cả Tất cả năm Nhập MSSV hoặc tên...

Tải lại dữ liệu Đặt lại bộ lọc Xuất Excel

Thống kê đơn xét tốt nghiệp

TỔNG ĐƠN: 2 ĐANG CHỜ DUYỆT: 2 ĐÃ DUYỆT: 0 ĐÃ TỪ CHỐI: 0 GPA TRUNG BÌNH: 3.04

Danh sách đơn xét tốt nghiệp

Tổng số: 2 đơn | Đang hiển thị: 2 đơn

STT	MSSV	Tên sinh viên	Lớp	GPA (4.0)	GPA (10)	Tín chỉ	Xếp loại	Ngày nộp	Trạng thái	Chi tiết	Thao tác
1	B2004742	Lê Hoàng Cường	DI20T9A1	3.06	7.65	156	KHÁ	10/12/2025	DANG CHOR	Chi tiết	✓ Duyệt ✗ Từ chối

Hình 3.19 Giao diện danh sách xét tốt nghiệp

Quản Lý Nhập Điểm

TS. Nguyễn Văn A
0xde0da6007226b18a219cbeba85aa01223b60fe

Đăng xuất

Hệ thống quản lý nhập điểm và xem thông tin sinh viên trên Blockchain

Nhập điểm Xem điểm đã nhập Danh sách xét tốt nghiệp Sinh viên tốt nghiệp

Bộ lọc sinh viên tốt nghiệp

Lọc theo Năm tốt nghiệp: 2025 MSSV / Tên sinh viên

Xuất Excel Tài lại dữ liệu

Thống kê tốt nghiệp

TỔNG SỐ TỐT NGHIỆP: 2 XUẤT SẮC: 0 GIỎI: 0 KHÁ: 2 GPA TRUNG BÌNH: 3.04

Danh sách sinh viên tốt nghiệp

Tổng số: 2 sinh viên | Đang hiển thị: 2 sinh viên

STT	MSSV	Tên sinh viên	Lớp	Ngành	GPA (4.0)	GPA (10)	Tín chỉ	Xếp loại	Năm TN	Thao tác
1	B2004742	Lê Hoàng Cường	DI20T9A1	Truyền thông và Mạng máy tính	3.06	7.65	156	Kha	2025	Chi tiết Thu hồi

Hình 3.20 Giao diện xem danh sách sinh viên tốt nghiệp

7.6. Giao Diện Trang Sinh Viên

Student Portal - Xem điểm Blockchain

Sinh viên (B2004742)
0x52cc688bc930f93d6a52b6e394434f1c760e38d9

Đăng xuất

Tra cứu điểm học tập và quá trình học tập từ Blockchain

Thông tin sinh viên

Họ và tên: Lê Hoàng Cường | MSSV: B2004742 | Ngày sinh: 23/08/2002 | Lớp: DI20T9A1
 Ngành học: Truyền thông và Mạng | Khoa: Mạng Máy Tính | Trường: CNTT&TT | Hệ đào tạo: TT&MMT2020
 Chương trình đào tạo: TT&MMT2020
 Email: b2004715@student.ctu.edu.vn | Điện thoại: 0901234569 | CCCD: 093202001236
 Quê quán: Sóc Trăng
 Đăng ký lúc: 20:25:25 10/12/2025

Tổng kết học tập

Thông tin tổng hợp toàn khóa học

GPA TÍCH LŨY 7.53 (Hệ 10) 3.06 (Hệ 4) Hệ 10 / Hệ 4	TÍN CHỈ TÍCH LŨY 156 100% Yêu cầu: 156 tín chỉ	TỔNG SỐ MÔN 52 52 PASS / 0 FAIL	SỐ HỌC KỲ 14 Đã hoàn thành
---	--	--	---

Phân bô điểm

10 môn A (9.0-10) | 28 môn B+/B (7.0-8.9) | 10 môn C+/C (5.5-6.9) | 4 môn D+/D (4.0-5.4) | 0 môn F (<4.0)

Xếp loại học lực: Khá

Trạng thái: Đủ điều kiện tốt nghiệp

Hình 3.21 Giao diện trang sinh viên

 **Học kỳ 20211**
Sinh viên: B2004742

Submit: 15:41:26 24/11/2025
Version: 1 | By: 0xde0dA600...

STT	Mã MH	Tên môn học	Tín chỉ	Điểm hệ 10	Điểm hệ 4	Điểm chữ
1	QP010	Giáo dục quốc phòng và An ninh 1 (*)	2	8.3	3.5	B+
2	QP011	Giáo dục quốc phòng và An ninh 2 (*)	2	8.4	3.5	B+
3	QP012	Giáo dục quốc phòng và An ninh 3 (*)	2	6.9	2.5	C+
4	QP013	Giáo dục quốc phòng và An ninh 4 (*)	2	7.5	3.0	B
5	TN010 *	Xác suất thống kê	3	3.0	0.0	F
6	CT100	Kỹ năng học đại học	2	8.2	3.5	B+

 **Tổng kết học kỳ 20211**

GPA HỌC KỲ
6.74
Thang điểm 10

TÍN CHỈ
13
6 môn học

KẾT QUẢ
5 Đạt
1 Trượt

Chú thích màu sắc:
■ Mầu xanh: Kết quả được công nhận (điểm cao nhất của môn học lại)
■ Mầu vàng: Môn học lại (không được tính vào kết quả)
* Ký hiệu môn học lại

Hình 3.22 Giao diện điểm một học kỳ của sinh viên



Hình 3.23 Bằng tốt nghiệp của sinh viên

Thông tin xác thực Blockchain

Thông tin bằng tốt nghiệp

Họ tên: Phạm Minh Đức
MSSV: B2004754
Ngành: Truyền thông và Mạng máy tính
Xếp loại: Khá
Năm tốt nghiệp: 2025

Blockchain Hash:
1cff95e146d63da314d33fc1ebdb6280262ef120...
Quét mã QR để xác thực trực tuyến →



Quét để xác thực

[Copy Link Xác Thực](#)

Hướng dẫn chia sẻ với nhà tuyển dụng

Doanh nghiệp có thể xác thực bằng 3 cách:

1. Quét QR Code: Sử dụng camera điện thoại quét mã QR trên bằng → Tự động xác thực
2. Click Link: Copy link xác thực (nút phía trên) và gửi cho nhà tuyển dụng → Tự động xác thực
3. Nhập MSSV: Truy cập verify_diploma.html và nhập MSSV: **B2004754**

Blockchain Hash:
1cff95e146d63da314d33fc1ebdb6280262ef120a0fa4fcab3b03401cda33370

Hình 3.24 Giao diện chia sẻ link xác thực bằng tốt nghiệp

7.7. Giao Diện Xác Thực Bằng Tốt Nghiệp

The screenshot shows a web-based application for blockchain verification. At the top, there's a header with a magnifying glass icon and the text "Xác thực Bằng Tốt Nghiệp". Below it, a sub-header reads "Hệ thống xác thực bằng tốt nghiệp trên Blockchain cho doanh nghiệp". A light blue sidebar on the left contains instructions:

- 💡 **Hướng dẫn sử dụng**
- Quét QR Code trên bằng tốt nghiệp → Tự động xác thực
- Click vào link mà ứng viên gửi → Tự động xác thực
- Nhập MSSV thủ công để tra cứu thông tin bằng

A note below says: "👉 Blockchain Verification: Tất cả thông tin được lấy trực tiếp từ blockchain, đảm bảo chính xác và không thể giả mạo."

The main area has a section titled "👉 Nhập MSSV để xác thực" with a text input field containing "B2004742". Two buttons are present: a green "Tra cứu & Xác thực" button and a red "Làm lại" button. A progress bar at the bottom indicates: "✓ Đang tự động xác thực từ QR Code...".

A large green box at the bottom right displays a checkmark and the text "✓ BẰNG TỐT NGHIỆP XÁC THỰC THÀNH CÔNG" and "✓ VERIFIED ON BLOCKCHAIN". Below this, a smaller text states: "Bằng tốt nghiệp này đã được xác thực trên Blockchain. Tất cả thông tin đã được mã hóa và không thể giả mạo."

Hình 3.25 Giao diện trang xác thực của doanh nghiệp

This screenshot shows a detailed view of the blockchain verification information. At the top, there's a header with a lock icon and the text "Thông tin Blockchain Verification". Below it is a table with the following data:

Thông tin kỹ thuật	Giá trị
SHA256 Hash	ef038d65e3783b59d9dd3f658129ea584c976f2876d8e2a5912ed5a7c66dc97
Smart Contract	0x0e068999591e59D0eAbff3491E2CD449B2B7D9f2
Timestamp	15:44:46 24/11/2025
Block Time	1763973886
Verification Status	✓ VERIFIED

Below the table, there's a section titled "Thông báo cho nhà tuyển dụng" with the following bullet points:

- **Bằng chính thức:** Đây là bằng tốt nghiệp được ghi nhận trên blockchain công nghệ cao
- **Không thể giả mạo:** Mọi thông tin đã được mã hóa và lưu trữ permanent
- **Đã xác thực:** Hệ thống đã kiểm tra và xác nhận tính hợp lệ 100%
- **Liên hệ trường:** Có thể liên hệ CNTT&TT để xác nhận thêm nếu cần

A blue button at the bottom right says "Xem quá trình học tập" (View learning process).

Hình 3.26 Thông tin xác thực văn bằng

CHƯƠNG 4: KIỂM THỦ MÔ HÌNH

I. MỤC TIÊU KIỂM THỦ

Phản kiểm thử mô hình được thực hiện nhằm đánh giá mức độ chính xác của cấu trúc dữ liệu, sự phù hợp của các mối quan hệ giữa các thực thể và khả năng đáp ứng đầy đủ các yêu cầu nghiệp vụ của hệ thống quản lý sinh viên trên nền tảng Ethereum. Mục tiêu của kiểm thử là xác định tính toàn vẹn của dữ liệu, tính hợp lý của các luồng xử lý và khả năng mở rộng của mô hình khi triển khai trong môi trường thực tế.

Bên cạnh đó, hoạt động kiểm thử còn giúp phát hiện và ngăn ngừa các sai sót tiềm ẩn trong quá trình phát triển hệ thống, đặc biệt là những lỗi có thể phát sinh trong giai đoạn lập trình smart contract. Việc kiểm thử mô hình góp phần đảm bảo tính minh bạch, nhất quán và an toàn của dữ liệu trong suốt vòng đời vận hành của hệ thống, đồng thời tạo nền tảng cho việc kiểm chứng độ tin cậy và tuân thủ của các quy trình nghiệp vụ trên blockchain.

II. PHẠM VI KIỂM THỦ

Các trường hợp kiểm thử sẽ tương ứng với các chức năng có trong tài liệu, kịch bản kiểm thử sẽ kiểm thử các chức năng chính sau:

- Admin tạo mới chương trình đào tạo.
- Admin gắn chương trình đào tạo với lớp.
- Admin tạo tài khoản sinh viên hàng loạt.
- Admin tạo tài khoản cho cán bộ quản lý điểm
- Admin thu hồi tài khoản cán bộ quản lý điểm
- Admin xem danh sách sinh viên, cán bộ đã tạo
- Cán bộ quản lý điểm nhập điểm học kỳ hàng loạt cho sinh viên
- Cán bộ quản lý điểm xem điểm sinh viên đã nhập, xem danh sách sinh viên tốt nghiệp
- Cán bộ quản lý điểm cấp bằng cho sinh viên
- Cán bộ quản lý điểm thu hồi văn bằng sinh viên
- Sinh viên xem thông tin cá nhân, quá trình học tập
- Sinh viên đăng ký xét tốt nghiệp
- Sinh viên chia sẻ văn bằng cho doanh nghiệp

III. MÔI TRƯỜNG KIỂM THỬ

Quá trình kiểm thử được thực hiện trên máy ảo **Ubuntu 24.04.3 LTS**, CPU đa nhân, RAM tối thiểu 8 GB, nhằm đảm bảo khả năng xử lý liên tục nhiều interactions trên blockchain mô phỏng.

Nền tảng thực hiện hợp đồng thông minh là **Ganache CLI** làm blockchain mô phỏng, cung cấp mạng Ethereum cục bộ với khả năng sinh khối nhanh, chi phí giao dịch thấp và cho phép quan sát chi tiết từng giao dịch, trạng thái lưu trữ và log sự kiện. Đây là môi trường phù hợp cho việc đánh giá tính đúng đắn của mô hình dữ liệu và các thao tác cập nhật trên smart contract.

Công cụ phát triển và biên dịch **Truffle Framework**, được sử dụng để biên dịch, triển khai và chạy các bài kiểm thử tự động. Bộ công cụ hỗ trợ truy vấn trạng thái blockchain, theo dõi luồng xử lý và phân tích các thay đổi trong cấu trúc dữ liệu sau mỗi giao dịch.

Máy chủ kiểm thử được cấu hình với **Node.js** phiên bản ổn định (**v20.x** hoặc tương đương), kết hợp các thư viện **Web3.js** để mô phỏng các hành vi tương tác của từng vai trò trong hệ thống (admin, cán bộ quản lý điểm, sinh viên, doanh nghiệp kiểm chứng).

Môi trường kiểm thử này giúp đảm bảo rằng các tình huống nghiệp vụ và thao tác trên smart contract có thể được tái hiện chính xác, từ đó hỗ trợ đánh giá độ tin cậy của mô hình dữ liệu, tính nhất quán của các quan hệ và khả năng vận hành của hệ thống trong các điều kiện triển khai thực tế.

IV. KỊCH BẢN KIỂM THỬ

4.1. Trường hợp 1: Admin tạo mới chương trình đào tạo

Điều kiện:

- Người dùng có vai trò là admin.
- Mã chương trình đào tạo chưa trùng với mã chương trình đào tạo nào khác.
- File json chương trình đào tạo phải phù hợp với file json mẫu.

Mô tả: admin tạo mới chương trình đào tạo

Bảng 4.1 Bảng trường hợp kiểm thử Admin tạo mới chương trình đào tạo

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là admin chọn đúng file json, mã chương trình đào tạo không trùng, ký bằng ví metamask đúng, chuẩn.	Thêm thành công chương trình đào tạo.	Thêm thành công chương trình đào tạo.	Đúng
2	Người dùng đúng vai trò là admin chọn đúng file json, mã chương trình đào tạo không trùng, không ký .	Hiển thị lỗi.	Hiển thị lỗi.	Đúng
3	Người dùng đúng vai trò là admin chọn file json sai định dạng , mã chương trình đào tạo không trùng, ký bằng ví metamask đúng, chuẩn.	Hiển thị lỗi, sai định dạng file.	Hiển thị lỗi, sai định dạng file.	Đúng
4	Người dùng đúng vai trò là admin chọn đúng file json, trùng mã chương trình đào tạo , ký bằng ví metamask đúng, chuẩn.	Hiển thị lỗi, trùng mã chương trình đào tạo.	Hiển thị lỗi, trùng mã chương trình đào tạo.	Đúng
5	Người dùng không phải vai trò là admin chọn đúng file json, mã chương trình đào tạo không trùng, ký bằng ví metamask đúng, chuẩn.	Lỗi, bạn không có quyền.	Lỗi, bạn không có quyền.	Đúng

4.2. Trường hợp 2: Admin gán chương trình đào tạo với lớp.

Điều kiện:

- Người dùng có vai trò là admin.
- Mã lớp chưa được gắn với chương trình đào tạo nào trước đó.

Mô tả: Admin gán chương trình đào tạo cho một lớp nào đó

Bảng 4.2 Bảng trường hợp kiểm thử Admin gán chương trình đào tạo với lớp

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là admin gán đúng chương trình đào tạo cho một lớp chưa được gán chương trình đào tạo nào, ký đúng, chuẩn.	Gán thành công lớp với chương trình đào tạo.	Gán thành công lớp với chương trình đào tạo.	Đúng
2	Người dùng đúng vai trò là admin, gán chương trình đào tạo cho lớp đã có chương trình đào tạo , ký đúng, chuẩn.	Lỗi, lớp đã được gán với một chương trình trước đó.	Lỗi, lớp đã được gán với một chương trình trước đó.	Đúng
3	Người dùng đúng vai trò là admin gán đúng chương trình đào tạo cho một lớp chưa được gán chương trình đào tạo nào, không ký .	Lỗi, gán chương trình đào tạo thất bại.	Lỗi, gán chương trình đào tạo thất bại.	Đúng

4.3. Trường hợp 3: Admin tạo tài khoản sinh viên hàng loạt.

Điều kiện:

- Người dùng có vai trò là admin.
- Mã sinh viên chưa được gán cho sinh viên nào trước đó.
- Mã lớp của sinh viên phải được gắn với chương trình đào tạo trước đó
- Files excel đúng form mẫu.

Mô tả: Admin tạo tài khoản cùng lúc cho nhiều sinh viên.

Bảng 4.3 Bảng trường hợp kiểm thử Admin tạo tài khoản sinh viên hàng loạt

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là admin, chọn file excel đúng chuẩn, đúng mẫu, mã sinh viên không trùng, ký bằng ví metamask đúng, chuẩn.	Thêm sinh viên thành công.	Thêm sinh viên thành công.	Đúng
2	Người dùng đúng vai trò là admin, chọn file excel không đúng chuẩn , mã sinh viên không trùng, ký bằng ví metamask đúng, chuẩn.	Lỗi tải file excel.	Lỗi tải file excel.	Đúng
3	Người dùng đúng vai trò là admin, chọn file excel đúng chuẩn, đúng mẫu, mã sinh viên đã được đăng ký trước đó , ký bằng ví metamask đúng, chuẩn.	Tự động loại bỏ sinh viên đã đăng ký trước đó, đăng ký những sinh viên chưa đăng ký.	Tự động loại bỏ sinh viên đã đăng ký trước đó, đăng ký những sinh viên chưa đăng ký.	Đúng
4	Người dùng đúng vai trò là admin, chọn file excel đúng chuẩn, đúng mẫu, mã sinh viên không trùng, không ký .	Thất bại.	Thất bại.	Đúng

4.4. Trường hợp 4: Admin tạo tài khoản cho cán bộ quản lý điểm

Điều kiện:

- Người dùng có vai trò là admin.
- Địa chỉ ví của cán bộ quản lý điểm không được trùng.
- Phải điền đủ địa chỉ ví, tên cán bộ quản lý và tên khoa.

Mô tả: admin tạo mới tài khoản cho cán bộ quản lý điểm

Bảng 4.4 Bảng trường hợp kiểm thử Admin tạo tài khoản cho cán bộ quản lý điểm

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là admin, nhập đủ khóa, tên cán bộ, tên khoa, ký bằng ví metamask đúng, chuẩn.	Thêm thành công cán bộ quản lý điểm.	Thêm thành công cán bộ quản lý điểm.	Đúng
2	Người dùng đúng vai trò là admin, nhập không đủ khóa, tên cán bộ hoặc tên khoa .	Không cho thêm.	Không cho thêm.	Đúng
3	Người dùng đúng vai trò là admin, nhập đủ khóa, tên cán bộ, tên khoa, không ký .	Lỗi ký.	Lỗi ký.	Đúng

4.5. Trường hợp 5: Admin thu hồi tài khoản cán bộ quản lý điểm

Điều kiện:

- Người dùng có vai trò là admin.

Mô tả: Admin thu hồi tài khoản cán bộ quản lý điểm

Bảng 4.5 Bảng trường hợp kiểm thử Admin thu hồi tài khoản cán bộ quản lý điểm

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là admin, ký bằng ví metamask đúng, chuẩn.	Xóa thành công tài khoản cán bộ quản lý điểm	Xóa thành công tài khoản cán bộ quản lý điểm	Đúng
2	Người dùng đúng vai trò là admin, không ký .	Lỗi ký.	Lỗi ký.	Đúng

4.6. Trường hợp 6: Admin xem danh sách sinh viên, cán bộ đã tạo

Điều kiện:

- Người dùng có vai trò là admin.

Mô tả: Admin xem danh sách sinh viên, cán bộ đã tạo

Bảng 4.6 Bảng trường hợp kiểm thử Admin xem danh sách sinh viên, cán bộ đã tạo

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là admin.	Hiển thị danh sách sinh viên, cán bộ quản lý điểm.	Hiển thị danh sách sinh viên, cán bộ quản lý điểm.	Đúng
2	Người dùng không có vai trò là admin.	Không hiển thị danh sách sinh viên, cán bộ quản lý điểm.	Không hiển thị danh sách sinh viên, cán bộ quản lý điểm.	Đúng

4.7. Trường hợp 7: Cán bộ quản lý điểm nhập điểm học kỳ cho sinh viên

Điều kiện:

- Người dùng có vai trò là cán bộ quản lý điểm.
- Năm học, học kỳ không được trùng, sinh viên phải được.
- Sinh viên phải được đăng ký tài khoản trước đó.
- Files excel điểm học kỳ của sinh viên phải đúng chuẩn.

Mô tả: Cán bộ quản lý điểm nhập điểm học kỳ hàng loạt cho sinh viên

Bảng 4.7 Bảng trường hợp kiểm thử Cán bộ quản lý điểm nhập điểm cho sinh viên

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là cán bộ quản lý điểm, file excel đúng chuẩn, sinh viên đã được đăng ký trước đó, năm học học kỳ không trùng, ký bằng ví metamask đúng, chuẩn.	Thêm thành công.	Thêm thành công.	Đúng
2	Người dùng đúng vai trò là cán bộ quản lý điểm, file excel đúng chuẩn, sinh viên chưa được đăng ký trước đó , năm học học kỳ không trùng, ký bằng ví metamask đúng, chuẩn.	Hiển thị lỗi sinh viên chưa được đăng ký.	Hiển thị lỗi sinh viên chưa được đăng ký.	Đúng
3	Người dùng đúng vai trò là cán bộ quản lý điểm, file excel sai chuẩn , sinh viên đã được đăng ký trước đó, năm học học kỳ không trùng, ký bằng ví metamask đúng, chuẩn.	Hiển thị lỗi tải file excel.	Hiển thị lỗi tải file excel.	Đúng
4	Người dùng đúng vai trò là cán bộ quản lý điểm, file excel đúng chuẩn, sinh viên đã được đăng ký trước đó, năm học học kỳ không trùng, không ký .	Lỗi ký	Lỗi ký	Đúng

4.8. Trường hợp 8: Cán bộ quản lý điểm xem điểm sinh viên đã nhập, xem danh sách sinh viên đã ra trường.

Điều kiện:

- Người dùng có vai trò là cán bộ quản lý điểm.

Mô tả: Cán bộ quản lý điểm xem điểm sinh viên đã nhập, xem danh sách sinh viên đã ra trường.

Bảng 4.8 Bảng trường hợp kiểm thử Cán bộ quản lý điểm xem điểm sinh viên đã nhập, xem danh sách sinh viên đã ra trường

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là cán bộ quản lý điểm.	Có thể xem danh sách	Có thể xem danh sách	Đúng
2	Người dùng không phải là cán bộ quản lý điểm.	Không thể xem danh sách	Không thể xem danh sách	Đúng

4.9. Trường hợp 9: Cán bộ quản lý điểm thu hồi văn bằng sinh viên

Điều kiện:

- Người dùng có vai trò là cán bộ quản lý điểm.

Mô tả: Cán bộ quản lý điểm thu hồi văn bằng sinh viên

Bảng 4.9 Bảng trường hợp kiểm thử Cán bộ quản lý điểm thu hồi văn bằng sinh viên

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là cán bộ quản lý điểm ký bằng ví metamask đúng, chuẩn.	Thu hồi thành công.	Thu hồi thành công.	Đúng
2	Người dùng đúng vai trò là cán bộ quản lý điểm, không ký .	Lỗi ký.	Lỗi ký	Đúng

4.10. Trường hợp 10: Sinh viên xem thông tin cá nhân, quá trình học tập

Điều kiện:

- Người dùng có vai trò là sinh viên (có ví).
- Sinh viên phải được đăng ký tài khoản trước đó.
- Người dùng nhập đúng mã số sinh viên

Mô tả: Sinh viên xem thông tin cá nhân, quá trình học tập

Bảng 4.10 Bảng trường hợp kiểm thử Sinh viên xem thông tin cá nhân, quá trình học tập

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là sinh viên, nhập đúng mã sinh viên.	Có thể xem thông tin cá nhân và quá trình học tập.	Có thể xem thông tin cá nhân và quá trình học tập.	Đúng
2	Người dùng không phải là sinh viên hoặc nhập sai mã số sinh viên.	Hiển thị lỗi, không thể xem thông tin hoặc điểm quá trình.	Hiển thị lỗi, không thể xem thông tin hoặc điểm quá trình.	Đúng

4.11. Trường hợp 11: Sinh viên đăng ký xét tốt nghiệp

Điều kiện:

- Người dùng có vai trò là sinh viên (có ví).
- Sinh viên phải được đăng ký tài khoản trước đó.
- Người dùng nhập đúng mã số sinh viên.
- Đủ điều kiện tốt nghiệp (đủ tín chỉ, hoàn thành các môn tự chọn và tất cả các môn bắt buộc, gpa trên 2.0...)

Mô tả: Sinh viên đủ điều kiện có thể đăng ký xét tốt nghiệp.

Bảng 4.11 Bảng trường hợp kiểm thử Sinh viên đăng ký xét tốt nghiệp

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là sinh viên, nhập đúng mã sinh viên, đủ điều kiện tốt nghiệp, ký bằng ví metamask đúng, chuẩn.	Đăng ký xét tốt nghiệp thành công, hiển thị trạng thái đang chờ duyệt.	Đăng ký xét tốt nghiệp thành công, hiển thị trạng thái đang chờ duyệt.	Đúng
2	Người dùng đúng vai trò là sinh viên, nhập đúng mã sinh viên, đủ điều kiện tốt nghiệp, không ký.	Hiển thị lỗi ký.	Hiển thị lỗi ký.	Đúng
3	Người dùng đúng vai trò là sinh viên, nhập đúng mã sinh viên, chưa đủ điều kiện tốt nghiệp, ký bằng ví metamask đúng, chuẩn.	Không thể xét tốt nghiệp.	Không thể xét tốt nghiệp.	Đúng

4.12. Trường hợp 12: Sinh viên chia sẻ văn bằng cho doanh nghiệp

Điều kiện:

- Người dùng có vai trò là sinh viên.
- Sinh viên đã tốt nghiệp.

Mô tả: Sinh viên chia sẻ văn bằng cho doanh nghiệp

Bảng 4.12 Bảng trường hợp kiểm thử Sinh viên chia sẻ văn bằng cho doanh nghiệp

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là sinh viên, nhập đúng mã sinh viên, đã tốt nghiệp.	Có thể chia sẻ bằng tốt nghiệp	Có thể chia sẻ bằng tốt nghiệp	Đúng
2	Người dùng đúng vai trò là sinh viên, nhập đúng mã sinh viên, chưa tốt nghiệp.	Không hiển thị bằng tốt nghiệp, chưa thể chia sẻ bằng tốt nghiệp	Không hiển thị bằng tốt nghiệp, chưa thể chia sẻ bằng tốt nghiệp	Đúng

4.13. Trường hợp 13: Cán bộ quản lý điểm cấp bằng cho sinh viên

Điều kiện:

- Người dùng có vai trò là cán bộ quản lý điểm
- Sinh viên đủ điều kiện tốt nghiệp
- Sinh viên đã đăng ký xét tốt nghiệp

Mô tả: Cán bộ cấp bằng tốt nghiệp cho sinh viên đủ điều kiện tốt nghiệp và đã đăng ký xét tốt nghiệp.

Bảng 4.13 Bảng trường hợp kiểm thử Cán bộ quản lý điểm cấp bằng cho sinh viên

STT	Kịch bản	Kết quả mong đợi	Kết quả thực tế	Kết quả
1	Người dùng đúng vai trò là cán bộ quản lý điểm, cấp bằng cho sinh viên đủ điều kiện tốt nghiệp và đã đăng ký xét tốt nghiệp, ký bằng ví metamask đúng, chuẩn.	Hiển thị trạng thái đã cấp bằng.	Hiển thị trạng thái đã cấp bằng.	Đúng
2	Người dùng đúng vai trò là cán bộ quản lý điểm, cấp bằng cho sinh viên đủ điều kiện tốt nghiệp và đã đăng ký xét tốt nghiệp, không ký .	Hiển thị lỗi ký.	Hiển thị lỗi ký.	Đúng
3	Người dùng đúng vai trò là cán bộ quản lý điểm, cấp bằng cho sinh viên đủ điều kiện tốt nghiệp và chưa đăng ký xét tốt nghiệp , ký bằng ví metamask đúng, chuẩn.	Không hiển thị sinh viên trong danh sách	Không hiển thị sinh viên trong danh sách	Đúng

CHƯƠNG 5: KẾT QUẢ VÀ HƯỚNG PHÁT TRIỂN

I. KẾT QUẢ ĐẠT ĐƯỢC

Luận văn đã xây dựng và triển khai thành công một mô hình thử nghiệm (prototype) hệ thống quản lý dữ liệu học tập và cấp phát văn bằng số dựa trên nền tảng Ethereum (EVM). Mô hình cho thấy khả năng ứng dụng công nghệ blockchain công khai vào bài toán quản lý điểm và văn bằng trong môi trường giáo dục đại học, đồng thời minh chứng tính khả thi của việc chuyển đổi từ mô hình cơ sở dữ liệu tập trung sang kiến trúc phi tập trung, bất biến và có thể xác thực công khai.

Về mặt kiến trúc và thiết kế hệ thống, đề tài đã đề xuất mô hình lưu trữ dữ liệu thuần on-chain, trong đó các thông tin mang tính quyết định như hồ sơ sinh viên, chương trình đào tạo, kết quả học tập cuối mỗi học kỳ sau khi khóa điểm và thông tin văn bằng tốt nghiệp được biểu diễn và quản lý trực tiếp trong các hợp đồng thông minh triển khai trên nền tảng Ethereum. Cách tiếp cận này giúp bảo đảm tính toàn vẹn và bất biến của dữ liệu quan trọng, mọi thao tác cập nhật đều phải đi qua giao dịch được ký số và ghi nhận trên sổ cái phân tán, từ đó tăng mức độ minh bạch và khả năng kiểm chứng công khai của hệ thống, dù phải đánh đổi với chi phí lưu trữ cao hơn khi triển khai ở môi trường thực tế.

Bên cạnh đó, các quy trình nghiệp vụ cốt lõi (thêm chương trình đào tạo, gán chương trình đào tạo cho lớp, cấp tài khoản, nhập điểm, xét tốt nghiệp, cấp phát và thu hồi văn bằng, xác thực văn bằng) đã được mô hình hóa thông qua các sơ đồ use case và hiện thực hóa bằng các hợp đồng thông minh trên EVM, với cơ chế phân quyền rõ ràng cho từng vai trò (quản trị viên, cán bộ quản lý điểm, giảng viên, sinh viên, doanh nghiệp), bảo đảm chỉ những tác nhân hợp lệ mới có thể kích hoạt các chức năng tương ứng trên chuỗi.

Về mặt triển khai và giao diện người dùng, luận văn đã xây dựng thành công một ứng dụng web mẫu tích hợp với blockchain thông qua Web3.js và ví MetaMask, cho phép các tác nhân khác nhau tương tác với hệ thống theo đúng vai trò: Admin quản lý chương trình đào tạo và tài khoản, cán bộ quản lý điểm nhập và tra cứu điểm, sinh viên theo dõi toàn bộ quá trình học tập, đăng ký xét tốt nghiệp tự động, quản lý và chia sẻ văn bằng, doanh nghiệp xác thực văn bằng trực tiếp trên chuỗi. Hệ thống cung cấp các giao diện trực quan cho các chức năng quản lý chương trình đào tạo, tài khoản sinh viên, tài khoản cán bộ, nhập điểm học kỳ, xem điểm, xem danh sách sinh viên tốt nghiệp, trang thông tin sinh viên, hiển thị bằng tốt nghiệp và trang xác thực văn bằng cho doanh nghiệp.

Về mặt kiểm thử và đánh giá, đề tài đã xây dựng bộ 12 kịch bản kiểm thử bao phủ các luồng nghiệp vụ chính của hệ thống, từ khâu tạo chương trình đào tạo, gán chương trình cho lớp, tạo và thu hồi tài khoản, nhập và tra cứu điểm, đến quy trình sinh viên xem quá

trình học tập, đăng ký xét tốt nghiệp và chia sẻ văn bằng cho doanh nghiệp. Kết quả kiểm thử cho thấy tất cả các trường hợp đều cho kết quả thực tế trùng khớp với kết quả mong đợi, bao gồm cả các tình huống hợp lệ (đủ điều kiện tốt nghiệp, có văn bằng để chia sẻ) và không hợp lệ (chưa đủ điều kiện tốt nghiệp, chưa có văn bằng, thiếu chữ ký giao dịch), qua đó khẳng định tính đúng đắn của logic nghiệp vụ và cơ chế kiểm soát điều kiện trong hợp đồng thông minh.

Từ góc độ khoa học, luận văn đã góp phần hiện thực hóa một mô hình ứng dụng blockchain trong giáo dục dựa trên kiến trúc EVM, bổ sung thêm một hướng tiếp cận khác biệt so với các mô hình trước đó chủ yếu sử dụng Hyperledger Fabric. Mô hình không chỉ dừng lại ở việc xác thực văn bằng cuối cùng mà còn bao quát được vòng đời dữ liệu học tập của sinh viên từ khi nhập học, tích lũy tín chỉ đến khi xét tốt nghiệp và cấp phát văn bằng, qua đó làm rõ hơn tiềm năng của smart contract trong tự động hóa các quy trình quản lý đào tạo.

Về mặt thực tiễn, kết quả của đề tài cho thấy việc áp dụng blockchain vào quản lý điểm và văn bằng có thể giúp tăng mức độ minh bạch, hạn chế nguy cơ chỉnh sửa trái phép dữ liệu, giảm phụ thuộc vào niềm tin đối với hệ thống quản trị tập trung, đồng thời rút ngắn thời gian và chi phí cho các bên liên quan trong quá trình xác minh văn bằng. Mặc dù mới dừng lại ở quy mô thử nghiệm trên mạng blockchain cục bộ với dữ liệu mô phỏng, mô hình đã chứng minh được tính khả thi để tiếp tục mở rộng triển khai trên các mạng Ethereum testnet hoặc mạng riêng trong tương lai, và có thể làm nền tảng tham khảo cho các nghiên cứu, ứng dụng tiếp theo trong lộ trình chuyển đổi số giáo dục đại học.

II. ĐÁNH GIÁ HẠN CHẾ

Mặc dù hệ thống đã chứng minh được tính khả thi trong việc áp dụng blockchain vào bài toán quản lý điểm và cấp phát văn bằng, đề tài vẫn tồn tại một số hạn chế nhất định cần được nhìn nhận khách quan để làm cơ sở cho các nghiên cứu và phát triển tiếp theo.

Thứ nhất, về môi trường triển khai, hệ thống mới chỉ được cài đặt và kiểm thử trên mạng blockchain cục bộ sử dụng Ganache, với dữ liệu mô phỏng và số lượng bản ghi còn hạn chế. Do đó, luận văn chưa đánh giá được đầy đủ hiệu năng, độ trễ giao dịch, khả năng chịu tải và chi phí vận hành khi triển khai trên các mạng thử nghiệm hoặc mạng công cộng với số lượng sinh viên, lớp học và giao dịch lớn hơn nhiều lần so với mô hình thử nghiệm.

Thứ hai, về phạm vi chức năng, đề tài tập trung vào các quy trình chính gồm quản lý chương trình đào tạo, thông tin sinh viên, điểm học phần và cấp bằng tốt nghiệp tự động dựa trên smart contract, chưa mở rộng sang các nghiệp vụ khác như đăng ký môn học, xử lý học phí, bảo lưu kết quả học tập, phúc khảo điểm hay các quy trình đặc thù khác của hệ

thống quản lý đào tạo đại học. Điều này giúp mô hình gọn hơn nhưng làm giảm mức độ bao phủ so với thực tế vận hành tại các trường đại học.

Thứ ba, về giao diện và trải nghiệm người dùng, ứng dụng web được xây dựng chủ yếu nhằm minh họa luồng nghiệp vụ và chức năng của smart contract nên giao diện còn đơn giản, chưa tối ưu cho nhiều loại thiết bị (đặc biệt là thiết bị di động), chưa chú trọng nhiều đến khả năng tùy biến, khả năng mở rộng về mặt giao diện, cũng như chưa đánh giá trải nghiệm người dùng thông qua khảo sát hoặc thử nghiệm với nhóm người dùng thực tế.

Thứ tư, việc lưu trữ dữ liệu học tập và thông tin cá nhân của sinh viên trực tiếp trên blockchain đặt ra nhiều thách thức liên quan đến bảo mật và tuân thủ quy định về bảo vệ dữ liệu cá nhân. Để tài chưa đi sâu vào các cơ chế ẩn danh hóa, mã hóa dữ liệu hay phân quyền truy cập chi tiết để giảm thiểu rủi ro rò rỉ thông tin nhạy cảm trong môi trường phi tập trung.

Thứ năm, về mô hình lưu trữ dữ liệu, hệ thống lựa chọn lưu trữ thuận on-chain cho hồ sơ sinh viên, chương trình đào tạo, kết quả học tập và văn bằng trên một mạng blockchain mô phỏng kiến trúc Ethereum với nhiều nút cùng duy trì số cái. Việc mỗi bản ghi đều được nhân bản và lưu trên tất cả các nút giúp dữ liệu bất biến và dễ kiểm chứng, nhưng đồng thời làm tổng dung lượng lưu trữ tăng rất nhanh khi số lượng sinh viên, năm học và nút tham gia tăng lên. Trong khuôn khổ luận văn, mô hình mới dừng ở mức minh họa, chưa phân tích định lượng chi tiết nhu cầu lưu trữ theo quy mô triển khai, cũng như chưa so sánh với các hướng tối ưu hơn như kết hợp on-chain/off-chain.

Nhìn chung, các hạn chế trên là khó tránh khỏi trong bối cảnh thời gian thực hiện luận văn có hạn và phạm vi đề tài chỉ dừng ở mức mô hình minh họa. Tuy nhiên, chính những hạn chế này mở ra nhiều hướng nghiên cứu tiếp theo, từ tối ưu chi phí lưu trữ và tài nguyên tính toán, mở rộng phạm vi nghiệp vụ, tăng cường cơ chế bảo vệ dữ liệu cá nhân, cho đến tích hợp hệ thống với hạ tầng quản lý đào tạo hiện hữu trong lộ trình chuyển đổi số giáo dục đại học.

III. HƯỚNG PHÁT TRIỂN

Thứ nhất, mở rộng môi trường triển khai và đánh giá hiệu năng. Hệ thống có thể được triển khai trên mạng nhiều nút hoặc các testnet để đo đặc thông lượng, độ trễ, khả năng chịu tải và nhu cầu tài nguyên khi số lượng sinh viên, lớp học và giao dịch tăng lên, làm cơ sở hiệu chỉnh kiến trúc cho quy mô thực tế.

Thứ hai, mở rộng phạm vi nghiệp vụ. Trong các nghiên cứu tiếp theo, hệ thống có thể tích hợp thêm các chức năng như đăng ký môn học, học phí, phúc khảo, bảo lưu kết

quả, khen thưởng, kỷ luật... nhằm bao phủ đầy đủ hơn vòng đời học tập của sinh viên và tiệm cận quy trình quản lý đào tạo thực tế.

Thứ ba, tối ưu mô hình lưu trữ và bảo vệ dữ liệu. Cần nghiên cứu các phương án kết hợp on-chain/off-chain, rút gọn hoặc nén dữ liệu, xây dựng mô hình ước lượng nhu cầu lưu trữ theo quy mô triển khai, đồng thời bổ sung các cơ chế mã hóa, ẩn danh hóa và phân quyền chi tiết hơn để đáp ứng yêu cầu bảo vệ dữ liệu cá nhân trong môi trường blockchain.

Thứ tư, cải thiện giao diện và tích hợp hệ thống. Ứng dụng web có thể được nâng cấp về trải nghiệm người dùng, hỗ trợ tốt hơn trên thiết bị di động và từng nhóm đối tượng, đồng thời xem xét tích hợp với các hệ thống quản lý đào tạo hiện hữu, tiến tới khả năng mở rộng thành mô hình liên trường phục vụ chia sẻ và xác thực văn bằng ở quy mô rộng hơn.

TÀI LIỆU THAM KHẢO

- [1] **Vietnamnet**, “Nhận 132 triệu đồng để nâng điểm cho 71 sinh viên,” Vietnamnet.vn, 2014. [Online]. Available: <https://vietnamnet.vn/nhan-132-trieu-dong-de-nang-diem-cho-71-sinh-vien-194052.html>
- [2] **CBS News**, “Students accused of hacking school computer system to change grades,” CBS News, 2012. [Online]. Available: <https://www.cbsnews.com/newyork/news/commack-high-school-grades-hacked/>
- [3] **VTV News**, “Triệt phá đường dây làm giấy tờ, bằng cấp giả quy mô lớn ở Quảng Trị,” VTV.vn, Oct. 28, 2025. [Online]. Available: <https://vtv.vn/triet-pha-duong-day-lam-giay-to-bang-cap-gia-quy-mo-lon-o-quang-tri-100251028051852442.htm>
- [4] **Tuổi Trẻ**, “Phát hiện giáo viên mua bằng, chứng chỉ giả của nhiều trường sư phạm,” Tuoitre.vn, Apr. 26, 2025. [Online]. Available: <https://tuoitre.vn/phat-hien-giao-vien-mua-bang-chung-chi-gia-cua-nhieu-truong-su-pham-20250426220514335.htm>
- [5] **Blockcerts**, “An open standard for blockchain-based certificates,” Blockcerts.org, 2017. [Online]. Available: <https://www.blockcerts.org>
- [6] **OpenCerts**, “The Singapore OpenCerts initiative,” opencerts.io, 2019. [Online]. Available: <https://www.opencerts.io>
- [7] **Woolf University**, “Woolf academic credentials on blockchain,” woolf.university, 2022. [Online]. Available: <https://woolf.university>
- [8] **D. Yaga, P. Mell, N. Roby, and K. Scarfone**, “Blockchain technology overview,” National Institute of Standards and Technology, Gaithersburg, MD, USA, NISTIR 8202, Oct. 2018.
- [9] **UK Government Office for Science**, “Distributed ledger technology: beyond blockchain,” London, UK, Rep. GS/16/1, 2016.
- [10] **D. Tapscott and A. Tapscott**, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York, NY, USA: Penguin, 2016.
- [11] **World Economic Forum**, “Blockchain beyond the hype: A practical framework for business,” Geneva, Switzerland, White Paper, Apr. 2018.
- [12] **M. Swan**, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015.

- [13] **Thủ tướng Chính phủ**, “Quyết định số 1236/QĐ-TTg phê duyệt Chiến lược quốc gia về ứng dụng và phát triển công nghệ chuỗi khối (blockchain) đến năm 2025, định hướng đến năm 2030,” Hà Nội, Việt Nam, Oct. 22, 2024. [Online]. Available: <https://vanban.chinhphu.vn>
- [14] **Deloitte**, “2021 Global blockchain survey: A new age of digital assets,” Deloitte Insights, Rep., 2021.
- [15] **Ngân hàng Nhà nước Việt Nam**, “Tiềm năng ứng dụng công nghệ Blockchain trong hoạt động ngân hàng,” Hà Nội, Việt Nam, Báo cáo, 2025.
- [16] **G. Kumar**, “Blockchain Transaction Lifecycle,” GeeksforGeeks, Aug. 2023. [Online]. Available: <https://www.geeksforgeeks.org/blockchain-transaction-lifecycle/>
- [17] **RockItCoin**, “What Is the Bitcoin Mempool? Transaction Delays Explained,” RockItCoin Bitcoin ATM Blog, Jul. 2022. [Online]. Available: <https://rockitcoin.com/what-is-the-bitcoin-mempool/>
- [18] **Bitget Academy**, “How to Verify Transactions in the Blockchain,” Bitget.com, Apr. 2023. [Online]. Available: <https://www.bitget.com/academy/crypto-basics/how-to-verify-transactions-in-the-blockchain>
- [19] **CodiesAlert**, “Bitcoin Transaction Life Cycle,” CodiesAlert Blog, Oct. 2022. [Online]. Available: <https://codiesalert.com/blog/bitcoin-transaction-life-cycle/>
- [20] **DeFi Education Fund**, “Public Blockchains: Consensus and Transaction Verification,” defieducationfund.org, 2023. [Online]. Available: <https://www.defieducationfund.org/public-blockchains-consensus>
- [21] **MemPool Space**, “The Mempool: Lifecycle of a Transaction (Key Stages),” mempool.webflow.io, 2022. [Online]. Available: <https://mem-pool.webflow.io/>
- [22] **Fireblocks**, “Understanding Transaction Flows: The Lifecycle of a Blockchain Transaction,” fireblocks.com, 2022. [Online]. Available: <https://www.fireblocks.com/blog/blockchain-transaction-lifecycle/>
- [23] **A. M. Antonopoulos**, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 2nd ed. Sebastopol, CA: O’Reilly Media, 2017. [Online]. Available: <https://masteringbitcoin.neocities.org/>
- [24] **V. Buterin**, “A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum Whitepaper, 2014. [Online]. Available: <https://ethereum.org/en/whitepaper/>

- [25] **N. Szabo**, “Smart Contracts,” 1994. [Online]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
- [26] **G. Wood**, “Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper),” Shanghai version, Feb. 2025. [Online]. Available: <https://ethereum.github.io/yellowpaper/paper.pdf>
- [27] **Ethereum Foundation**, “Ethereum Development Documentation,” ethereum.org, Aug. 2023. [Online]. Available: <https://ethereum.org/developers/docs/>
- [28] **Solidity Team**, “Solidity Documentation,” Version 0.8.x, docs.soliditylang.org. [Online]. Available: <https://docs.soliditylang.org/>
- [29] **Truffle Suite**, “Truffle Documentation,” archive.trufflesuite.com. [Online]. Available: <https://archive.trufflesuite.com/docs/truffle/>
- [30] **Truffle Suite**, “What is Ganache?,” Ganache Documentation, archive.trufflesuite.com. [Online]. Available: <https://archive.trufflesuite.com/docs/ganache/>
- [31] **Web3.js Core Team**, “Web3.js: Ethereum JavaScript API Documentation,” docs.web3js.org. [Online]. Available: <https://docs.web3js.org/>
- [32] **W3C**, “Decentralized Identifiers (DIDs) v1.0,” W3C Recommendation, did-core. [Online]. Available: <https://www.w3.org/TR/did-core/>
- [33] **W. Entriken, D. Shirley, J. Evans, and N. Sachs**, “EIP-721: ERC-721 Non-Fungible Token Standard,” Ethereum Improvement Proposal 721, Jan. 2018. [Online]. Available: <https://eips.ethereum.org/EIPS/eip-721>