

TRƯỜNG ĐẠI HỌC CẦN THƠ
TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG



LUẬN VĂN TỐT NGHIỆP - TT&MMT
MÃ HỌC PHẦN: CT555

XÂY DỰNG HỆ THỐNG
CHỨNG THỰC BẰNG CẤP CỦA TRƯỜNG ĐẠI HỌC
SỬ DỤNG CÔNG NGHỆ BLOCKCHAIN
VỚI NỀN TẢNG ETHEREUM

CÁN BỘ HƯỚNG DẪN
ThS. Nguyễn Trọng Nghĩa

SINH VIÊN THỰC HIỆN
Họ tên: Dương Trúc Mai
MSSV: B2004790 – Khóa 46
Lớp: DI20T9A2

Tháng 5/2024

TRƯỜNG ĐẠI HỌC CẦN THƠ
TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG



LUẬN VĂN TỐT NGHIỆP - TT&MMT
MÃ HỌC PHẦN: CT555

XÂY DỰNG HỆ THỐNG
CHỨNG THỰC BẰNG CẤP CỦA TRƯỜNG ĐẠI HỌC
SỬ DỤNG CÔNG NGHỆ BLOCKCHAIN
VỚI NỀN TẢNG ETHEREUM

CÁN BỘ HƯỚNG DẪN
ThS. Nguyễn Trọng Nghĩa

SINH VIÊN THỰC HIỆN
Họ tên: Dương Trúc Mai
MSSV: B2004790 – Khóa 46
Lớp: DI20T9A2

Tháng 5/2024

TRƯỜNG ĐẠI HỌC CẦN THƠ
TRƯỜNG CNTT&TT

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: Xây dựng hệ thống chứng thực bằng cấp của trường đại học sử dụng công nghệ Blockchain với nền tảng Ethereum

Họ tên sinh viên: Dương Trúc Mai

MASV: B2004790

Mã lớp: DI20T9A2

Đã báo cáo tại hội đồng khoa: Mạng máy tính và truyền thông dữ liệu

Ngày báo cáo: 14/05/2024

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

Cần Thơ, ngày ... tháng 05 năm 2024

Giáo viên hướng dẫn

(Ký và ghi họ tên)

LỜI CẢM ƠN

Với Đề tài luận văn tốt nghiệp chuyên ngành Mạng máy tính và truyền thông dữ liệu “Xây dựng hệ thống chứng thực bằng cấp của trường đại học sử dụng công nghệ Blockchain với nền tảng Ethereum” là kết quả của quá trình cố gắng không ngừng nghỉ của chúng em và được sự giúp đỡ tận tình, động viên khích lệ của thầy cô và người thân. Qua đây, em xin gửi lời cảm ơn chân thành đến những người đã giúp đỡ em trong thời gian học tập - nghiên cứu vừa qua.

Em xin trân trọng gửi đến thầy **ThS. Nguyễn Trọng Nghĩa** - Người đã trực tiếp tận tình hướng dẫn cũng như cung cấp tài liệu, thông tin cần thiết cho đề tài luận văn này cho em và những nhận xét quý báu để em có thể hoàn thành tốt đề tài một lời cảm ơn chân thành và sâu sắc nhất.

Em cũng xin gửi lời cảm ơn chân thành đến quý Thầy Cô trường Công nghệ thông tin và truyền thông - Đại học Cần Thơ và khoa Mạng máy tính và truyền thông đã tạo điều kiện cho em hoàn thành tốt đề tài luận văn và truyền đạt vốn kiến thức quý báu cho chúng em trong suốt thời gian học tập trên giảng đường đại học. Cuối cùng, em cảm ơn quý Thầy, Cô hội đồng phản biện luận văn đã nhận xét, góp ý cho đề tài của em.

Bằng tất cả sự cố gắng để thực hiện đề tài một cách hoàn chỉnh nhất, nhưng với vốn kiến thức và thời gian hạn chế nên không thể tránh khỏi những thiếu sót cũng như những hạn chế. Rất mong nhận được sự góp ý của quý Thầy, Cô và bạn bè để đề tài được hoàn thiện hơn.

Em xin trân trọng cảm ơn!

Cần Thơ, tháng 05 năm 2024

Sinh viên

DƯƠNG TRÚC MAI

LỜI CAM ĐOAN

Em xin cam đoan luận văn “Xây dựng hệ thống chứng thực bằng cấp của trường đại học sử dụng công nghệ Blockchain với nền tảng Ethereum” được hoàn thành hoàn toàn dựa trên kết quả nghiên cứu của em dưới sự hướng dẫn của ThS. Nguyễn Trọng Nghĩa, các nguồn tài liệu tham khảo đã được ghi rõ trong danh mục tài liệu tham khảo.

Cần Thơ, ngày ... tháng 05 năm 2024
Sinh viên thực hiện

DƯƠNG TRÚC MAI

NHẬN XÉT CỦA CÁN BỘ HƯỚNG DẪN

Sinh viên **Dương Trúc Mai**, MSSV: B2004790 có tinh thần trách nhiệm, siêng năng, chịu khó đọc sách, tài liệu trong quá trình thực hiện luận văn, viết code tốt, rõ ràng, kỹ năng lập trình tốt, chủ động liên hệ với giảng viên hướng dẫn để báo cáo tiến độ của luận văn và đã hoàn thành tốt luận văn tốt nghiệp của mình.

Cần Thơ, ngày ... tháng 05 năm 2024
Cán bộ hướng dẫn

ThS. Nguyễn Trọng Nghĩa

[illegible]

Cần Thơ, ngày ... tháng 05 năm 2024
Hội đồng phản biện

MỤC LỤC

LỜI CẢM ƠN	4
LỜI CAM ĐOAN	5
NHẬN XÉT CỦA CÁN BỘ HƯỚNG DẪN	6
NHẬN XÉT CỦA HỘI ĐỒNG PHẢN BIỆN	7
MỤC LỤC	8
DANH MỤC HÌNH ẢNH.....	11
DANH MỤC BẢNG	12
DANH MỤC CÁC TỪ VIẾT TẮT.....	13
ABSTRACT	14
TÓM TẮT	15
CHƯƠNG 1: TỔNG QUAN.....	16
I. ĐẶT VẤN ĐỀ	16
II. ĐỐI TƯỢNG, PHẠM VI NGHIÊN CỨU	16
III. MỤC TIÊU ĐỀ TÀI.....	17
IV. NỘI DUNG NGHIÊN CỨU	17
1.4.1 Quy trình nghiên cứu	17
1.4.2 Bố cục luận văn.....	17
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT	19
I. GIỚI THIỆU BLOCKCHAIN	19
2.1.1 Khái niệm Blockchain	19
2.1.2 Các giai đoạn của Blockchain.....	19
2.1.3 Đặc điểm của Blockchain	19
2.1.4 Phân loại Blockchain	20
2.1.5 Cấu trúc của Blockchain.....	22
2.1.6 Cách Blockchain hoạt động	23
2.1.7 Ứng dụng của Blockchain	23
II. MẠNG ETHEREUM	25
2.2.1 Giới thiệu mạng Ethereum.....	25
2.2.2 Ưu điểm và nhược điểm của Ethereum	26
2.2.3 Ứng dụng của Ethereum	27
III. NGÔN NGỮ SOLIDITY VÀ SMART CONTRACT	27
2.3.1 Giới thiệu về ngôn ngữ Solidity	27
IV. HỢP ĐỒNG THÔNG MINH.....	28

Mục lục

2.4.1 Giới thiệu về hợp đồng thông minh.....	28
2.4.2 Cách hoạt động của hợp đồng thông minh	29
2.4.3 Ưu điểm và nhược điểm hợp đồng thông minh	29
V. VÍ METAMASK	30
VI. GANACHE VÀ TRUFFLE	31
2.6.1 Ganache	31
2.6.2 Truffle	32
VII. MONGODB.....	33
2.7.1 MongoDB	33
VIII. THUẬT TOÁN ĐỒNG THUẬN.....	33
CHƯƠNG 3: GIẢI QUYẾT VẤN ĐỀ.....	35
I. ĐẶC TẢ ĐỀ TÀI.....	35
II. SƠ ĐỒ CHỨC NĂNG CỦA HỆ THỐNG.....	35
3.2.1 Sơ đồ Use Case đối với Admin.....	35
3.2.2 Sơ đồ Use Case đối với Trường Đại học	35
3.2.3 Sơ đồ Use Case đối với Người dùng	36
III. ĐẶC TẢ YÊU CẦU CHỨC NĂNG.....	36
3.3.1 Đăng nhập	36
3.3.2 Tạo tài khoản cho Trường Đại học	37
3.3.3 Xóa tài khoản của Trường Đại học.....	37
3.3.4 Thêm thông tin sinh viên	38
3.3.5 Xóa thông tin sinh viên.....	39
3.3.6 Xem Bảng tốt nghiệp	39
IV. ĐẶC TẢ YÊU CẦU PHI CHỨC NĂNG.....	40
3.4.1 Yêu cầu thực thi	40
3.4.2 Yêu cầu bảo mật	40
3.4.3 Đặc điểm hệ thống	41
3.4.4 Môi trường vận hành	41
3.4.5 Mô hình tổng quan hệ thống.....	41
V. CÀI ĐẶT HỆ THỐNG.....	42
3.5.1 Cấu trúc hợp đồng thông minh	42
3.5.2 Cài đặt hợp đồng thông minh	43
VI. GIAO DIỆN CÁC CHỨC NĂNG.....	46
3.6.1 Giao diện Trang chủ	46

Mục lục

3.6.2 Giao diện Đăng nhập	47
3.6.3 Giao diện Thêm Username	48
3.6.4 Giao diện Danh sách Username	48
3.6.5 Giao diện Sửa Username.....	49
3.6.6 Giao diện Xóa Username	49
3.6.7 Giao diện Thêm thông tin	50
3.6.8 Giao diện Danh sách thông tin.....	50
3.6.9 Giao diện Xóa thông tin.....	51
3.6.10 Giao diện Tra cứu	51
3.6.11 Giao diện bằng tốt nghiệp (kết quả tra cứu)	52
3.6.12 Giao diện Xác thực	52
3.6.13 Giao diện Kết quả xác thực.....	53
CHƯƠNG 4: KẾT LUẬN - ĐÁNH GIÁ.....	54
I. KẾT QUẢ ĐẠT ĐƯỢC	54
II. HẠN CHẾ.....	54
III. HƯỚNG PHÁT TRIỂN	55
TÀI LIỆU THAM KHẢO	56

DANH MỤC HÌNH ẢNH

Hình 1. Cấu trúc của Blockchain	23
Hình 2. Ứng dụng của Blockchain trong y tế	25
Hình 3. Giao diện tương tác ví Metamask	31
Hình 4. Giao diện Ganache và các ví điện tử.....	32
Hình 5. Sơ đồ Use case Admin	35
Hình 6. Sơ đồ Use case Trường Đại học.....	36
Hình 7. Sơ đồ Use case Người dùng	36
Hình 8. Mô hình tổng quan hệ thống	42
Hình 9. Cấu trúc sinh viên trong hợp đồng thông minh.....	42
Hình 10. Các biến trong hợp đồng thông minh.....	43
Hình 11. Nội dung file cấu hình mạng truffle-config.js.....	43
Hình 12. Thêm Workspace cho Ganache.....	44
Hình 13. Viết Migrations	44
Hình 14. Kết quả khi chạy lệnh truffle migrate –reset.....	45
Hình 15: Kết quả Transactions.....	46
Hình 16. Giao diện Trang chủ.....	47
Hình 17. Giao diện Đăng nhập.....	47
Hình 18. Giao diện Thêm Username	48
Hình 19. Giao diện Danh sách Username	48
Hình 20. Giao diện Sửa Username.....	49
Hình 21. Giao diện Xóa Username	49
Hình 22. Giao diện Thêm thông tin	50
Hình 23. Giao diện Xem danh sách	50
Hình 24. Giao diện Xóa thông tin	51
Hình 25. Giao diện Tra cứu.....	51
Hình 26. Giao diện bằng tốt nghiệp	52
Hình 27. Giao diện Xác thực.....	52
Hình 28. Giao diện Hiện thị khi kết quả xác thực là Bằng thật	53
Hình 29. Giao diện Hiện thị kết quả xác thực khi Bằng không tồn tại trong hệ thống	53

DANH MỤC BẢNG

Bảng 1: Một số thuật toán đồng thuận	34
Bảng 2: Đặc tả chức năng Đăng nhập	37
Bảng 3: Đặc tả chức năng Tạo tài khoản cho Trường Đại học	37
Bảng 4: Đặc tả chức năng Xóa tài khoản của Trường Đại học	38
Bảng 5: Đặc tả chức năng Thêm thông tin	39
Bảng 6: Đặc tả chức năng Xóa thông tin	39
Bảng 7: Đặc tả chức năng Xem bằng tốt nghiệp	40

DANH MỤC CÁC TỪ VIẾT TẮT

STT	Tên viết tắt	Tên đầy đủ	Giải thích
1		Blockchain	Chuỗi khối
2	DApp	Decentralized Application	Ứng dụng phi tập trung
3	DPoS	Delegated Proof of Stake	Bằng chứng cổ phần được ủy quyền
4	DEX	Decentralized Exchange	Sàn giao dịch phi tập trung
5	ETH	Ethereum	
6	EVM	Ethereum Virtual Machine	Máy ảo Ethereum
7	NFT	Non-fungible token	Token không thể thay thế
8	PoS	Proof of Stake	Bằng chứng cổ phần
9	PoW	Proof of Work	Bằng chứng công việc

ABSTRACT

Currently at Vietnamese Universities, when completing a program, students will be given a paper diploma by the University with their information on the diploma. Then, to apply for a job, students will often photocopy their university degree and submit it to the employer.

With that, the employer may encounter situations such as difficulty verifying the authenticity of the degree and the risk that the degree may be faked. Because buying, selling, and using fake diplomas has been a problem in the context of strongly developing information technology in today's society. Agencies and organizations are facing this difficult problem in times such as recruitment, organizing qualifications improvement exams or approval to study abroad.

To overcome the above disadvantages, if there is a system to authenticate degrees, those degrees can be processed conveniently, quickly and especially transparently, and cannot be modified. At this time, Blockchain technology is considered suitable with many outstanding advantages such as: basis to prove falsification, transparency...

The topic "Building an authentication system of university degree using Blockchain technology with Ethereum platform" will help verification become more transparent, clear and time-saving.

This thesis includes 2 main tasks for degree authentication:

- Learn about Blockchain as well as how Blockchain and Ethereum network work.
- Deploying a university degree authentication system based on blockchain technology with the Ethereum platform

Basically, the system has provided full functionality for Admin, University and users. But it is expected that if developed later, additional functions can be added for Admin and the University or develop more mobile platforms.

TÓM TẮT

Hiện nay ở các Trường Đại học Việt Nam, khi hoàn thành một chương trình học thì sinh viên sẽ được Trường Đại học cấp cho mình một tấm bằng tốt nghiệp bằng giấy với các thông tin của họ ở trên tấm bằng. Sau đó, để xin việc, sinh viên thường sẽ photo công chứng tấm bằng đại học và nộp cho bên nhà tuyển dụng.

Với đó, bên nhà tuyển có thể có khả năng sẽ gặp phải những trường hợp như khó khăn khi xác minh được tính xác thực của tấm bằng đó và rủi ro khi tấm bằng đó có thể làm giả. Do việc mua bán, sử dụng văn bằng giả đã và đang là một vấn nạn trong bối cảnh công nghệ thông tin phát triển mạnh mẽ trong xã hội hiện nay. Các cơ quan, tổ chức đều đang phải đối mặt với bài toán nan giải này trong những thời điểm như tuyển dụng, tổ chức các kỳ thi nâng cao trình độ hoặc xét duyệt đi du học.

Để khắc phục các nhược điểm trên, nếu có hệ thống chứng thực bằng cấp thì những bằng cấp đó có thể xử lý một cách tiện lợi, nhanh chóng và đặc biệt là minh bạch, không thể bị sửa đổi được. Lúc này, công nghệ Blockchain được xem là phù hợp với nhiều ưu điểm vượt trội như: cơ sở để chứng minh tính giả mạo, tính minh bạch...

Đề tài “Xây dựng hệ thống chứng thực bằng cấp của trường đại học sử dụng công nghệ Blockchain với nền tảng Ethereum” sẽ giúp việc chứng thực trở nên minh bạch, rõ ràng và tiết kiệm thời gian hơn.

Luận văn này bao gồm 2 công việc chính để cho việc thực hiện chứng thực bằng cấp:

- Tìm hiểu về Blockchain cũng như cách hoạt động của Blockchain và mạng Ethereum.
- Triển khai hệ thống chứng thực bằng cấp của trường đại học dựa trên công nghệ blockchain với nền tảng Ethereum.

Về cơ bản, hệ thống đã cung cấp đầy đủ chức năng cho Admin, Trường Đại học và người dùng. Nhưng dự kiến nếu phát triển về sau, có thể bổ sung thêm các chức năng cho Admin và Trường Đại học hay phát triển thêm nền tảng mobile.

CHƯƠNG 1: TỔNG QUAN

I. ĐẶT VẤN ĐỀ

Công nghệ chuỗi khối (Blockchain) là một công nghệ đặc biệt hứa hẹn và mang tính cách mạng vì nó giúp giảm thiểu rủi ro bảo mật, loại bỏ gian lận và mang lại sự minh bạch ở quy mô chưa từng thấy trước đây. Giữa cuộc khủng hoảng tài chính trong khoảng năm 2007 - 2008, đồng tiền ảo Bitcoin đã được thế giới biết khi Satoshi Nakamoto cho ra mắt whitepaper Bitcoin - mạng lưới phục vụ việc chuyển tiền giữa hai bên mà không bị ảnh hưởng hay cần phải thông qua bên thứ ba như ngân hàng. Và công nghệ mà Satoshi áp dụng vào mạng lưới Bitcoin đó là Chain of Blocks. Sau đó, ông đã thay đổi thuật ngữ “Chain of Blocks” thành thuật ngữ “blockchain” dễ nhớ hơn. Ban đầu nó được liên kết với tiền điện tử và token không thể thay thế (Non-fungible token - NFT) vào những năm 2010, nhưng công nghệ chuỗi khối kể từ đó đã phát triển thành một giải pháp quản lý cho tất cả các loại ngành công nghiệp toàn cầu. Với công nghệ Blockchain, chúng ta sẽ rất thuận tiện khi có thể mang lại sự minh bạch cho chuỗi cung ứng thực phẩm, bảo mật dữ liệu chăm sóc sức khỏe và nói chung là thay đổi cách xử lý dữ liệu và quyền sở hữu. Sử dụng công nghệ chuỗi khối, tiền điện tử (như Bitcoin) và thông tin kỹ thuật số khác có thể di chuyển tự do từ người này sang người khác mà không cần sự tham gia của bên thứ ba. Bất kỳ ai có máy tính đều có thể tham gia mạng và tham gia vào quá trình xác thực giao dịch.

Bên cạnh những điều đó, công nghệ Blockchain cũng phát sinh ra những vấn đề như chi phí để duy trì một số Blockchain là cực kỳ tốn kém đối với những cá nhân hoặc những tổ chức nhỏ và rất chậm trong việc xử lý các giao dịch. Chính vì vậy, công nghệ Blockchain chỉ thích hợp khi triển khai những vấn đề có những yếu tố như xác định tính minh bạch, nghĩa là giảm nguy cơ gian lận, vì tất cả dữ liệu được ghi trong khối không thể thay đổi hoặc xóa, điều này làm cho công nghệ Blockchain trở thành một hệ thống hoàn toàn đáng tin cậy. Vận dụng các ưu điểm của công nghệ Blockchain, chúng tôi đã ứng dụng công nghệ này để xây dựng hệ thống chứng thực bằng tốt nghiệp của trường đại học trên nền tảng mạng lưới private Blockchain Ethereum.

II. ĐỐI TƯỢNG, PHẠM VI NGHIÊN CỨU

Đối tượng:

- Đối tượng nghiên cứu chính của đề tài: công nghệ Blockchain, mạng Ethereum.

- Đối tượng sử dụng hệ thống gồm: Admin, Nhà trường, Người dùng khác: Sinh Viên, Nhà tuyển dụng.

Phạm vi nghiên cứu đề tài được tập trung vào việc nghiên cứu xác minh chứng thực bằng tốt nghiệp của trường đại học ở Việt Nam.

III. MỤC TIÊU ĐỀ TÀI

- Nghiên cứu về công nghệ Blockchain: Hiểu rõ các kiến thức về Blockchain, ứng dụng, cách thức hoạt động cũng như áp dụng công nghệ Blockchain vào trong thực tế.
- Xây dựng một hệ thống có khả năng chứng thực và lưu trữ thông tin về bằng tốt nghiệp trên mạng Ethereum, sử dụng hợp đồng thông minh để triển khai. Hệ thống sẽ cung cấp một cách an toàn và minh bạch để xác minh tính hợp lệ của các bằng tốt nghiệp, giúp người dùng dễ dàng chia sẻ và xác thực thông tin về bằng tốt nghiệp.

IV. NỘI DUNG NGHIÊN CỨU

1.4.1 Quy trình nghiên cứu

Quy trình nghiên cứu được thực hiện như sau:

- Nghiên cứu về Blockchain, Ethereum, Solidity, Ganache, Truffle.
- Cài đặt các công nghệ và cấu hình để kết nối (MongoDB, MetaMask,...).
- Vẽ UseCase.
- Thiết kế hệ thống.
- Xây dựng và viết chức năng cho hệ thống.
- Tổng hợp tài liệu và viết báo cáo.

1.4.2 Bố cục luận văn

Bố cục của quyền luận văn ngoài phần mục lục, danh mục hình, danh mục bảng, danh mục từ viết tắt thì nội dung của quyền luận văn còn bao gồm các phần như sau:

Phần tổng quan: Nêu ra lý do thực hiện đề tài. Xác định mục tiêu của đề tài và nêu lên những nội dung cần phải nghiên cứu.

Phần cơ sở lý thuyết: Tìm hiểu những khái niệm, ưu điểm và nhược điểm cũng như các ứng dụng của các công nghệ được sử dụng trong hệ thống.

Phần giải quyết vấn đề: Bao gồm việc đặc tả đề tài, đặc tả các yêu cầu chức năng và giao diện các chức năng của hệ thống.

Chương 1: Tổng quan

Phần kết luận – đánh giá: Trình bày các kết quả hoàn thành, nêu lên những mặt hạn chế mà hệ thống cần phải cải thiện hoặc chưa thể khắc phục ngay, từ đó định hình hướng phát triển của hệ thống trong tương lai.

Tài liệu tham khảo: Đưa ra các nguồn nghiên cứu và tham khảo trong quá trình thực hiện luận văn.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

I. GIỚI THIỆU BLOCKCHAIN

2.1.1 Khái niệm Blockchain

Blockchain (chuỗi khối) là một cơ sở dữ liệu phân cấp, thông tin được lưu trữ trong các khối và liên kết với nhau. Thông tin trong khối, được liên kết với nhau bằng mã hóa đồng thời có thể mở rộng theo thời gian. Mỗi khi một thông tin hoặc giao dịch mới xảy ra, thông tin cũ sẽ không bị mất đi mà thay vào đó, thông tin mới sẽ được lưu vào một khối mới và lần lượt được nối vào khối cũ để tạo thành một chuỗi mới. Có thể ví chuỗi khối Blockchain như một cuốn sổ cái ghi lại toàn bộ dữ liệu trong hệ thống. Blockchain khác với các dữ liệu thông thường ở cấu trúc lưu trữ dữ liệu. Blockchain sẽ thu thập thông tin dữ liệu và nhóm chúng thành các khối chứa tập hợp nhiều thông tin.

2.1.2 Các giai đoạn của Blockchain

Blockchain bao gồm 4 giai đoạn:

Blockchain 1.0 (tiền tệ): Blockchain hỗ trợ mọi giao dịch liên quan đến chuyển đổi tiền tệ, kiều hối và tạo lập hệ thống thanh toán kỹ thuật số trong phạm vi tiền điện tử

Blockchain 2.0 (hợp đồng thông minh): Các giao dịch sẽ được minh bạch, rõ ràng nhất, giảm mạnh các chi phí xác thực.

Blockchain 3.0 (DApps - Ứng dụng phi tập trung): các phần mềm được triển khai độc lập, không nằm trên một máy chủ duy nhất mà lưu trữ một cách phân tán trên các kho lưu trữ phi tập trung và có thể được viết bằng bất kỳ ngôn ngữ nào. Blockchain 3.0 hỗ trợ khả năng mở rộng, giao diện người dùng tốt, trải nghiệm người dùng và các ứng dụng có khả năng tương tác.

Blockchain 4.0 (Ứng dụng vào thực tiễn): mô tả các giải pháp và phương pháp tiếp cận giúp công nghệ blockchain có thể sử dụng được cho nhu cầu kinh doanh và công nghiệp.

2.1.3 Đặc điểm của Blockchain

Các đặc điểm của Blockchain:

- Phân quyền: Được định nghĩa là lưu trữ các khối trên một mạng lưới các nút chứ không phải ở bất kỳ vị trí trung tâm nào. Nội dung của mỗi khối trong chuỗi khối công khai có thể được truy cập bởi bất kỳ nút nào trên mạng
- Thúc đẩy sự đồng thuận: Một mô hình đồng thuận xác minh độc lập từng khối trên blockchain và cung cấp các quy tắc nhất định để xác thực một khối. Ví dụ: liên quan đến Bitcoin, đây được gọi là quy trình khai thác.
- Tính bất biến: Một blockchain có thể được coi là một bản ghi giao dịch không thể thay đổi và không thể đảo ngược. Do đó, khi một khối được hoàn tất, đó là thời điểm mà các bên liên quan đến giao dịch đó đồng ý và do đó giao dịch không thể bị đảo ngược hoặc thay đổi theo bất kỳ cách nào, sau đó nó sẽ được thêm vào chuỗi khối.
- Tính minh bạch: Về bản chất, một blockchain công khai cung cấp tính minh bạch mở hoàn toàn. Bất kỳ bên nào cũng có thể xem toàn bộ lịch sử giao dịch vì nó thực chất là một tệp mở. Do đó, một lợi thế rất có lợi khác là blockchain tạo ra nguồn gốc xuất xứ, vì tất cả các giao dịch có thể được kiểm tra dễ dàng từ lần nhập đầu tiên đến lần nhập cuối cùng.
- Ẩn danh: Mọi giao dịch đều minh bạch và công khai, nhưng những người thực tế được giữ ẩn danh thông qua các địa chỉ. Ví dụ: giả sử một người gửi một khoản tiền, người nhận sẽ biết rằng người gửi được liên kết với địa chỉ bitcoin, nhưng họ sẽ không biết địa chỉ thực tế, đảm bảo quyền riêng tư của người gửi.

2.1.4 Phân loại Blockchain

Có bốn loại chính: Public, Private, Hybrid và Consortium.

- Public Blockchain: Một blockchain phi tập trung và mở, nơi bất kỳ ai cũng có thể tham gia.
 - + Cách hoạt động: Trong một public blockchain, các giao dịch được cộng đồng xác thực thông qua một quá trình được gọi là khai thác, tuân theo cơ chế đồng thuận như Proof of Work (PoW) hoặc Proof of Stake (PoS). Sau khi được xác thực, các giao dịch được thêm vào một khối, sau đó được thêm vào blockchain.
 - + Ưu điểm của Public Blockchain:
 - Phân cấp: Không một thực thể nào có quyền kiểm soát, dẫn đến tăng tính minh bạch và công bằng.
 - Bảo mật: Các Public Blockchain được bảo mật do tính chất phi tập trung và các biện pháp bảo mật mã của chúng.

- Khả năng truy cập: Bất kỳ ai, ở bất cứ đâu, đều có thể tham gia, thực hiện giao dịch hoặc xác thực giao dịch trên Public Blockchain
- + Nhược điểm của Public Blockchain
 - Khả năng mở rộng: Các Public Blockchain thường phải vật lộn với các vấn đề về khả năng mở rộng do thiết kế của chúng.
 - Quyền riêng tư: Vì tất cả các giao dịch đều minh bạch, có rất ít quyền riêng tư trong các Public Blockchain.
 - Hiệu quả: Quá trình đồng thuận có thể chậm và tiêu tốn năng lượng đáng kể.
- Private Blockchain: Một blockchain được phép với một mạng lưới tập trung.
 - + Cách hoạt động: Trong một Private Blockchain, một tổ chức hoặc thực thể duy nhất quản lý mạng. Chỉ các thành viên được ủy quyền mới có thể xác thực các giao dịch, sau đó được thêm vào blockchain.
 - + Ưu điểm của Private Blockchain
 - Hiệu quả: Các Private Blockchain nhanh hơn và hiệu quả hơn vì chúng không yêu cầu khai thác hoặc cơ chế đồng thuận phức tạp.
 - Quyền riêng tư: Các giao dịch là riêng tư, chỉ hiển thị cho các thành viên mạng.
 - Khả năng mở rộng: Khi ít nút tham gia xác thực giao dịch hơn, các Private Blockchain có khả năng mở rộng hơn.
 - + Nhược điểm của Private Blockchain
 - Tập trung: Một thực thể duy nhất có quyền kiểm soát mạng, điều này có thể dẫn đến lạm dụng quyền lực.
 - Khả năng tiếp cận: Nhu cầu xin phép có thể hạn chế khả năng tiếp cận và đổi mới.
- Hybrid Blockchain: là một loại mạng tích hợp các tính năng của cả Public Blockchain và Private Blockchain. Sự pha trộn sáng tạo này cung cấp một giải pháp linh hoạt và có thể tùy chỉnh, cung cấp tính minh bạch và toàn diện của các Public Blockchain trong khi vẫn duy trì tính bảo mật và kiểm soát vốn có trong các Private Blockchain. Nó đảm bảo rằng các tổ chức có thể kiểm soát ai truy cập thông tin, nhưng vẫn cho phép một số dữ liệu nhất định được công khai, tạo ra sự cân bằng hoàn hảo giữa tính minh bạch, bảo mật và kiểm soát. Dragonchain là một ví dụ đáng chú ý về Hybrid Blockchain.

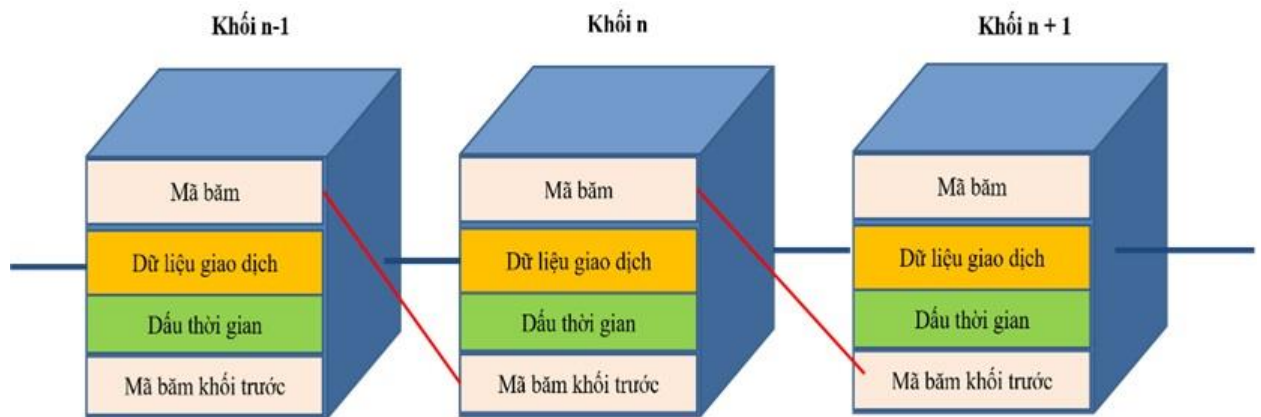
- + Ưu điểm của Hybrid Blockchain
 - Tính linh hoạt: Các Hybrid Blockchain có thể hoạt động cả công khai và riêng tư, mang lại sự linh hoạt cao hơn.
 - Bảo mật: Các giao dịch được bảo mật khi chúng xảy ra trong một mạng được phép.
 - Khả năng tương tác: Các blockchain này có thể tương tác với nhiều blockchain khác.
 - Nhược điểm của Hybrid Blockchain
 - Độ phức tạp: Bản chất kép của các Hybrid Blockchain có thể dẫn đến sự phức tạp.
 - Thách thức thực hiện: Họ có thể phải đối mặt với những thách thức trong việc áp dụng do các vấn đề pháp lý và kỹ thuật.
- Consortium Blockchain: Một blockchain liên kết được quản lý bởi nhiều tổ chức. Các Consortium Blockchain là các mạng bán riêng được kiểm soát bởi một nhóm các nút hoặc tổ chức, thay vì một thực thể duy nhất, cung cấp sự cân bằng giữa tính minh bạch của các Public Blockchain và tính bảo mật của các Private Blockchain.
 - + Ưu điểm của Consortium Blockchain
 - Cộng tác: Nhiều tổ chức có thể cộng tác hiệu quả.
 - Kiểm soát và quyền riêng tư: Mặc dù không được phân cấp hoàn toàn, quyền kiểm soát vẫn được phân phối giữa nhiều thực thể.
 - Hiệu quả: Xác thực giao dịch nhanh hơn so với các Public Blockchain.
 - + Nhược điểm của Consortium Blockchain
 - Ít phi tập trung hơn: Các Consortium Blockchain ít phi tập trung hơn các blockchain công khai.
 - Sự tham gia hạn chế của công chúng: Công chúng nói chung không thể tham gia vào quá trình đồng thuận.

2.1.5 Cấu trúc của Blockchain

Như khái niệm Blockchain ở trên thì Blockchain gồm 2 phần chính đó là:

- Chuỗi: các khối liên kết với nhau tạo thành chuỗi.
- Khối: các khối chứa dữ liệu. Với mỗi khối chứa những thông tin sau:
 - + Data (dữ liệu): các bản ghi dữ liệu đã được xác minh được bảo vệ bằng các thuật toán mã hóa phụ thuộc vào mỗi loại khác nhau của blockchain.

- + Timestamp: nhãn thời gian khởi tạo của chuỗi
- + Hash (Mã hàm băm): Một chuỗi ký tự và số được tạo ngẫu nhiên không hoàn toàn giống nhau, được sử dụng một thuật toán mã hóa để mã hóa. Mã này được sử dụng để phát hiện các thay đổi trong khối, ví như dấu vân tay của chúng ta, là duy nhất, không trùng nhau.
- + Hash of previous block (mã Hash khối trước đó): Để các khối liên kết đúng về việc khối nào ở phía trước và khối nào ở sau. Và khối đầu tiên được gọi là Genesis block (khối gốc) do mã hash của nó là một chuỗi số 0.



Hình 1. Cấu trúc của Blockchain

2.1.6 Cách Blockchain hoạt động

Đầu tiên, bản ghi hồ sơ sẽ được tạo ra sau khi hệ thống ghi lại thông tin giao dịch. Công nghệ blockchain hoạt động dựa trên hệ thống mạng ngang hàng P2P, tất cả máy tính (node) tham gia sẽ đóng vai trò như một máy chủ của hệ thống xác minh xem bản ghi có hợp lệ hay là không theo thuật toán đồng thuận trên blockchain.

Tiếp theo, các bản ghi và một loạt các bản ghi khác đã được xác minh có giá trị sẽ được nhóm lại thành một khối.

Cuối cùng, khối (block) mới được tạo sẽ kết nối khối trước đó bằng cách kết nối với hash of previous block (mã Hash khối trước đó) của khối được thêm vào và một blockchain sẽ được tạo thành.

2.1.7 Ứng dụng của Blockchain

- **Trong giáo dục:**

Blockchain trong hệ thống giáo dục có thể dễ dàng lưu trữ lượng dữ liệu giáo dục đa dạng do hồ sơ sinh viên là vô tận. Với công nghệ blockchain thì bằng cấp,

chúng chỉ, điểm danh, khóa học, khoản thanh toán học phí, điểm số, bài tập có thể được lưu trữ và không thể bị xóa. Vì vậy, chúng góp phần bảo mật dữ liệu bằng cách không thay đổi. Đó cũng là tài sản của sinh viên chứ không phải của nhà trường. Không ai có thể giả mạo bản ghi một khi đã được ghi trên blockchain.

- **Trong thương mại điện tử**

Blockchain mang lại lợi ích đôi bên cùng có lợi cho cả thương hiệu và người mua, nó giúp giao dịch an toàn hơn và nhanh hơn. Nhưng nó cũng mang lại nhiều lợi ích khác, bao gồm cắt giảm chi phí, cải thiện quy trình kinh doanh, thực hiện giao dịch nhanh hơn và cải thiện trải nghiệm tổng thể của khách hàng, cải thiện quy trình kinh doanh. Công nghệ blockchain trong thương mại điện tử đảm bảo độ tin cậy và độ chính xác của dữ liệu. Nó cũng cho phép phát triển các sản phẩm hấp dẫn và cá nhân hóa hơn. Ví dụ: khách hàng có thể thiết kế sản phẩm của riêng họ, mã hóa sở thích của họ và trao đổi chúng với người dùng hoặc nhà cung cấp khác thông qua các ứng dụng blockchain

- **Đối với ngành tài chính:**

Các giao dịch tài chính luôn là mục tiêu của hacker và lừa đảo. Ngoài ra, họ có nguy cơ bị đánh cắp thông tin khi giao dịch đi qua bộ xử lý thanh toán hoặc bên trung gian thứ ba. Nhiều doanh nghiệp tận dụng blockchain để tạo ra một hệ thống ủy thác phi tập trung, sử dụng thuật toán mật mã để xử lý và ghi lại các giao dịch mà không can thiệp vào bên thứ ba. Điều này hạn chế khả năng gian lận và các nỗ lực khai thác. Giao dịch cũng phải đáp ứng tất cả các điều kiện của hợp đồng thông minh, nếu không chúng sẽ bị từ chối.

Tự động hóa hợp đồng thông minh là chìa khóa của blockchain. Họ đủ thông minh để tự động hóa các điều kiện được xác định trước nhằm thực hiện hợp đồng giữa các bên. Bên cạnh việc cải thiện tính bảo mật của các giao dịch, hợp đồng thông minh còn loại bỏ nguồn nhân lực và tránh sự chậm trễ trong việc thực hiện các hợp đồng tài chính. Quản lý tài sản là một trong những ứng dụng lớn nhất của blockchain đối với ngành tài chính. Quản lý tài sản liên quan đến việc quản lý và trao đổi các tài sản khác nhau thuộc sở hữu của cá nhân. Quy trình giao dịch truyền thống trong quản lý tài sản có thể cực kỳ tốn kém, đặc biệt khi các giao dịch liên quan đến thanh toán qua nhiều quốc gia và biên giới. Trong những tình huống như vậy, blockchain có thể rất hữu ích vì nó loại bỏ sự cần thiết của các bên trung gian như người môi giới, người giám sát và người thanh toán. Thay vào đó, blockchain cung cấp một quy trình đơn giản và minh bạch giúp loại bỏ khả năng xảy ra lỗi.

- **Đối với lĩnh vực y tế:**

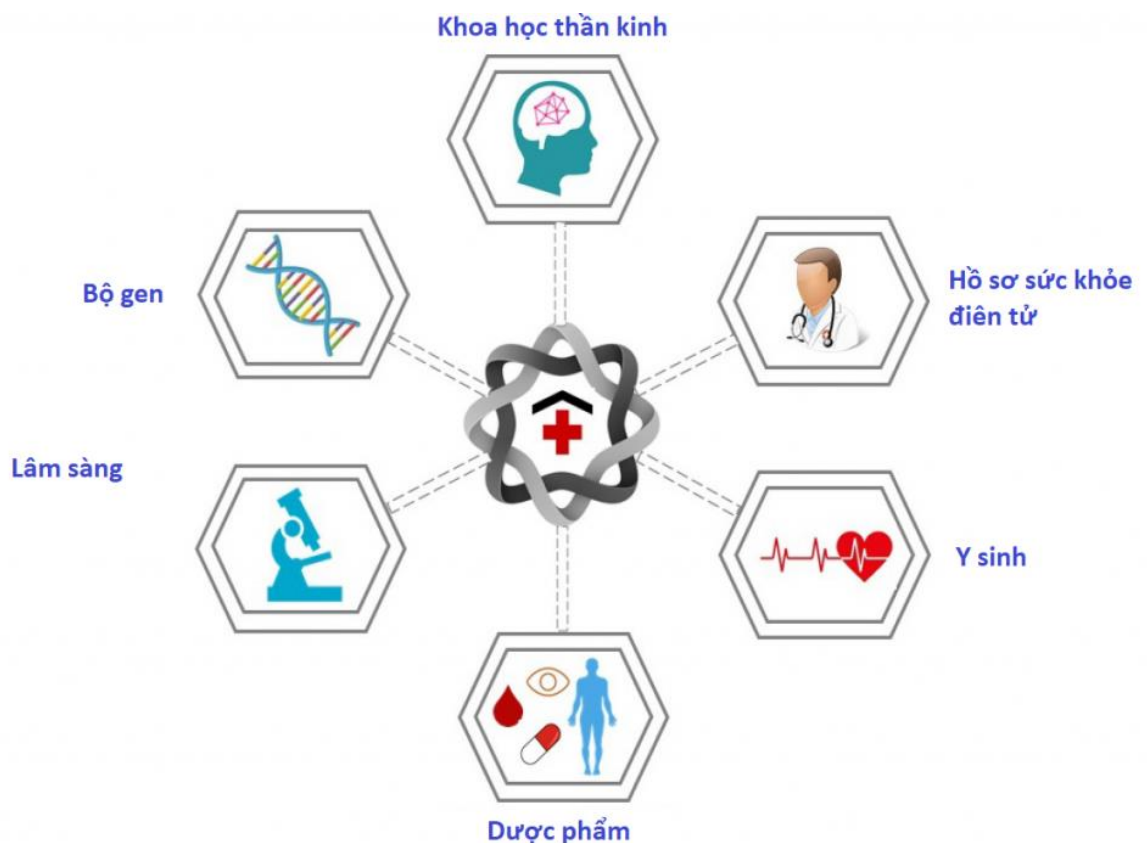
Blockchain có thể tạo ra một hệ thống duy nhất để lưu trữ, cập nhật liên tục các bản ghi sức khỏe để người dùng được ủy quyền có thể truy xuất nhanh chóng và

Chương 2: Cơ sở lý thuyết

an toàn giúp việc chăm sóc bệnh nhân nhanh hơn, rẻ hơn, tốt hơn, có thể ngăn ngừa được vô số sai sót, để bác sĩ chẩn đoán và can thiệp nhanh hơn cũng như có thể cá nhân hóa việc chăm sóc cho từng bệnh nhân.

Bởi các ứng dụng y tế di động ngày càng trở nên quan trọng hơn với công nghệ tiên tiến. Trong bối cảnh này, hồ sơ y tế điện tử (EMR) được phát hiện là được giữ an toàn trong mạng blockchain và dữ liệu có thể được gửi đến nhân viên y tế một cách nhanh chóng, cũng như có sẵn để tự theo dõi và chăm sóc tại nhà.

Ngoài ra các khả năng độc đáo của blockchain có thể giúp báo cáo bệnh theo thời gian thực và khám phá các mô hình bệnh có thể giúp xác định nguồn gốc và các thông số lây truyền của nó.



Hình 2. Ứng dụng của Blockchain trong y tế

II. MẠNG ETHEREUM

2.2.1 Giới thiệu mạng Ethereum

Ethereum (ETH) là nền tảng điện toán phân tán, mã nguồn mở dựa trên công nghệ chuỗi khối (blockchain) có khả năng thực thi hợp đồng thông minh (smart contract), là một mạng lưới các máy tính trên toàn thế giới tuân theo một bộ quy tắc gọi là giao thức Ethereum. Mạng Ethereum đóng vai trò là nền tảng cho cộng đồng,

ứng dụng, tổ chức và tài sản kỹ thuật số mà bất kỳ ai cũng có thể xây dựng và sử dụng. Bao bao gồm một máy ảo gọi là Ethereum Virtual Machine (EVM), có nhiệm vụ xử lý việc triển khai và thực thi trên smart contract

Ethereum là loại tiền điện tử phổ biến thứ hai sau Bitcoin. Được thành lập bởi Vitalik Buterin và Gavin Wood vào năm 2015, ngày nay vốn hóa thị trường của Ethereum chiếm khoảng 20% trong thị trường tiền điện tử toàn cầu. Ethereum có đồng tiền điện tử gốc là ether (ETH). Ether là một loại cryptocurrency (tiền điện tử kỹ thuật số) được xây dựng vào năm 2013 bởi Vitalik Buterin, thường được gọi là cryptocurrency 2.0.

Nói theo cách riêng của tiền điện tử, Ethereum là “một nền tảng toàn cầu, phi tập trung dành cho tiền và các loại ứng dụng mới”, với hàng nghìn trò chơi và ứng dụng tài chính chạy trên chuỗi khối Ethereum. Tiền điện tử này phổ biến đến mức ngay cả các loại tiền điện tử khác cũng chạy trên mạng của nó.

Trọng tâm của Ethereum là mạng blockchain của nó. Blockchain là một sổ cái công khai, phân tán, phi tập trung, nơi các giao dịch được xác minh và ghi lại. Ethereum cũng là blockchain đầu tiên khám phá và triển khai hợp đồng thông minh.

2.2.2 Ưu điểm và nhược điểm của Ethereum

- Ưu điểm:
 - + Cộng đồng phát triển lớn mạnh: Ethereum sở hữu cộng đồng lập trình viên và nhà phát triển sôi động, không ngừng đóng góp vào việc cải tiến và mở rộng hệ sinh thái. Nhờ vậy, nền tảng liên tục được cập nhật với các tính năng mới, ứng dụng đa dạng và giải pháp sáng tạo.
 - + Rất nhiều nhà đầu tư lớn, nổi tiếng ủng hộ Ethereum như Microsoft, Intel, Red Hat
 - + Hỗ trợ đa dạng: Ethereum được hỗ trợ bởi nhiều ví tiền, sàn giao dịch và ứng dụng tiền điện tử, giúp người dùng dễ dàng truy cập và sử dụng.
- Nhược điểm:
 - + Chi phí giao dịch tăng cao. Sự phổ biến ngày càng tăng của Ethereum đã dẫn đến chi phí giao dịch cao hơn. Phí giao dịch Ethereum, còn được gọi là “gas”, có thể dao động liên tục và khá tốn kém.
 - + Tiềm năng lạm phát tiền điện tử: Mặc dù Ethereum có giới hạn phát hành hàng năm là 18 triệu Ether mỗi năm, nhưng không có giới hạn trọn đời về số lượng tiền tiềm năng. Điều này có thể có

nghĩa là với tư cách là một khoản đầu tư, Ethereum có thể hoạt động giống đô la hơn và có thể không được đánh giá cao bằng Bitcoin, loại tiền có giới hạn nghiêm ngặt suốt đời đối với số lượng xu.

2.2.3 Ứng dụng của Ethereum

- Các thỏa thuận: Với hợp đồng thông minh Ethereum, các thỏa thuận có thể được duy trì và thực hiện mà không có bất kỳ sự thay đổi nào. Vì vậy, trong một ngành công nghiệp có những người tham gia phân tán, có tranh chấp và yêu cầu phải có hợp đồng kỹ thuật số, Ethereum có thể được sử dụng như một công nghệ để phát triển hợp đồng thông minh và để ghi lại kỹ thuật số các thỏa thuận và giao dịch dựa trên chúng.
- Hệ thống ngân hàng: Ethereum đang được áp dụng rộng rãi trong các hệ thống ngân hàng. Nó cho phép thanh toán trên mạng dựa trên Ethereum, vì vậy các ngân hàng cũng đang sử dụng Ethereum như một kênh để thực hiện chuyển tiền và thanh toán, đồng thời gây nên thách thức đối với tin tặc khi truy cập trái phép.
- Vận chuyển: Triển khai Ethereum trong vận chuyển giúp theo dõi hàng hóa và ngăn hàng hóa bị thất lạc hoặc làm giả.

Ngoài các hợp đồng thông minh, Ethereum còn tạo ra các sản phẩm sau:

- Ứng dụng phi tập trung (DApps): DApps là các ứng dụng phi tập trung có thể phục vụ bất kỳ mục đích nào mà các ứng dụng truyền thống có thể làm được, chúng được phi tập trung hóa, thiên về quyền riêng tư và không có cơ quan trung ương nào kiểm soát các ứng dụng này.
- Tài chính phi tập trung (DeFi): DeFi là tên gọi chung của một dự án tiền điện tử cung cấp dịch vụ ngân hàng phi tập trung. Các dự án DeFi là cách để người dùng kiếm thu nhập thụ động bằng cách cho vay phi tập trung, đặt cược, khai thác năng suất, khai thác thanh khoản,...
- Sàn giao dịch phi tập trung (DEX): Sàn giao dịch phi tập trung nổi lên như một giải pháp thay thế cho các nền tảng tập trung. Các sàn giao dịch phi tập trung cũng thường có mức phí sử dụng rẻ hơn và có thể hoàn thành giao dịch hoán đổi của bạn ngay lập tức.

III. NGÔN NGỮ SOLIDITY VÀ SMART CONTRACT

2.3.1 Giới thiệu về ngôn ngữ Solidity

Solidity là một ngôn ngữ lập trình cấp cao, được thiết kế đặc biệt để viết các hợp đồng thông minh (smart contract). Nó được lấy cảm hứng từ các ngôn ngữ như C ++, Python và JavaScript cũng như sử dụng sự kết hợp lý giữa chữ cái và số. Solidity giúp các nhà phát triển quen thuộc với các ngôn ngữ này dễ dàng tiếp cận.

IV. HỢP ĐỒNG THÔNG MINH

2.4.1 Giới thiệu về hợp đồng thông minh

Hợp đồng thông minh là các chương trình máy tính được lưu trữ và thực thi trên mạng blockchain. Mỗi hợp đồng thông minh bao gồm mã xác định các điều kiện được xác định trước mà khi đáp ứng sẽ kích hoạt kết quả. Bằng cách chạy trên blockchain phi tập trung thay vì máy chủ tập trung, hợp đồng thông minh cho phép nhiều bên đi đến kết quả chung một cách chính xác, kịp thời và chống giả mạo.

Hợp đồng thông minh là một cơ sở hạ tầng mạnh mẽ để tự động hóa vì chúng không được quản trị viên kiểm soát và không dễ bị tấn công bởi các thực thể độc hại. Khi áp dụng cho các thỏa thuận kỹ thuật số nhiều bên, các ứng dụng hợp đồng thông minh có thể giảm rủi ro đối tác, tăng hiệu quả, giảm chi phí và cung cấp mức độ minh bạch mới cho các quy trình.

Hợp đồng thông minh lần đầu tiên được nhà khoa học máy tính người Mỹ Nick Szabo đặt ra vào năm 1994. Trong bài viết chuyên đề của mình, ông đã đưa ra định nghĩa rộng rãi về hợp đồng thông minh như sau: “một giao thức giao dịch được vi tính hóa thực hiện các điều khoản của hợp đồng” với mục tiêu chung là thỏa mãn các yêu cầu chung, điều kiện hợp đồng, giảm thiểu các trường hợp ngoại lệ cả cố ý và vô tình, đồng thời giảm thiểu nhu cầu về các bên trung gian đáng tin cậy.

Chuỗi khối Bitcoin sau đó đã phát triển để cung cấp một loại hợp đồng thông minh chính thức khác vào năm 2012 được gọi là giao dịch đa chữ ký. Giao dịch nhiều chữ ký yêu cầu một số lượng người xác định (khóa chung) để ký giao dịch bằng khóa riêng của họ trước khi giao dịch được coi là hợp lệ. Điều này làm tăng tính bảo mật cho tiền của người dùng bằng cách giảm thiểu một điểm lỗi duy nhất như khóa riêng bị đánh cắp hoặc bị mất.

Để hợp đồng thông minh được hình thành, cần 04 điều kiện sau:

- + Chủ thể hợp đồng: Các bên tham gia thực hiện giao kết hợp đồng, trong đó có những bên được cấp quyền truy cập, theo dõi tình hình xử lý và nội dung hợp đồng.
- + Điều khoản hợp đồng: Các điều khoản quy định ở dạng chuỗi, được lập trình đặc biệt mà các bên tham gia phải đồng ý với các điều này.

- + Chữ ký số: Các bên tham gia Smart Contract đồng thuận triển khai thỏa thuận về chữ ký số và phải thực hiện thao tác thông qua chữ ký số.
- + Nền tảng phân quyền: Bước vào giai đoạn hoàn tất, Smart Contract cần được tải lên Blockchain. Chuỗi Blockchain tiếp tục phân phối dữ liệu về các node và lưu lại, không thể điều chỉnh.

2.4.2 Cách hoạt động của hợp đồng thông minh

Hợp đồng thông minh là các chương trình chống giả mạo trên blockchain với logic sau: “nếu/khi sự kiện x xảy ra, thì thực hiện hành động y”. Một hợp đồng thông minh có thể có nhiều điều kiện khác nhau và một ứng dụng có thể có nhiều hợp đồng thông minh khác nhau để hỗ trợ một tập hợp các quy trình được kết nối với nhau. Ngoài ra còn có nhiều ngôn ngữ hợp đồng thông minh để lập trình, trong đó Solidity của Ethereum là ngôn ngữ phổ biến nhất.

Cách hoạt động của Smart Contract được cụ thể qua 4 bước sau:

- Bước 1: Lập trình sẵn hợp đồng: Các câu điều kiện của thỏa thuận trong hợp đồng như: “If / When...” được đưa vào Blockchain thành mã code.
- Bước 2: Chuỗi hoạt động: Nếu điều kiện thỏa mãn, hợp đồng thông minh sẽ được thực hiện.
- Bước 3: Thực hiện & chuyển giao giá trị: Một khi thực hiện chuyển giao, các điều khoản của hợp đồng sẽ tự động mã hóa và chuyển giao cho các bên liên quan.
- Bước 4: Hoàn tất: Giao dịch hoàn tất sẽ được cập nhật trên blockchain và không thể thay đổi. Chỉ các bên đã được cấp quyền mới có thể xem kết quả.

2.4.3 Ưu điểm và nhược điểm hợp đồng thông minh

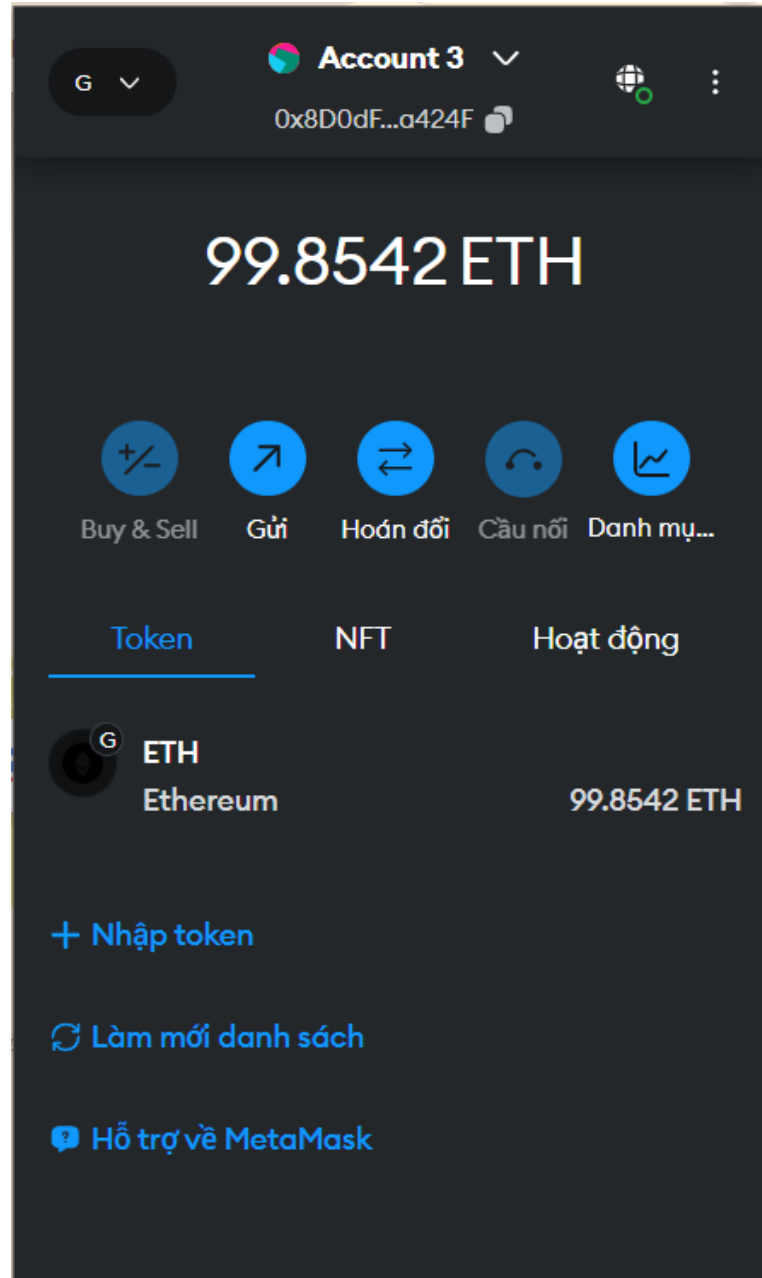
- Ưu điểm:
 - + Hiệu quả: Tăng tốc độ thực hiện hợp đồng.
 - + Độ chính xác: Không thể có lỗi do con người gây ra.
 - + Tính bất biến: Chương trình không thể thay đổi.
- Nhược điểm:
 - + Vĩnh viễn: Chúng không thể thay đổi nếu có sai sót.
 - + Lỗi hồng: Có thể có lỗi hồng trong mã hóa, cho phép các hợp đồng được thực hiện một cách thiếu thiện ý.

V. VÍ METAMASK

Ra mắt vào năm 2016 bởi Consensys như một tiện ích mở rộng trình duyệt cho trình duyệt web Chrome và Firefox, MetaMask nhanh chóng thu hút được sự chú ý của các nhà phát triển và người dùng Ethereum.

MetaMask là một plugin trình duyệt đóng vai trò như một ví Ethereum và được cài đặt giống như bất kỳ plugin trình duyệt nào khác. Sau khi được cài đặt, nó cho phép người dùng lưu trữ Ether và các mã thông báo ERC-20 khác, cho phép họ giao dịch với bất kỳ địa chỉ Ethereum nào.

Bằng cách kết nối với MetaMask với các ứng dụng phi tập trung dựa trên Ethereum, người dùng có thể chi tiêu tiền của họ trong các trò chơi, đặt cược mã thông báo trong các ứng dụng cờ bạc và giao dịch chúng trên các sàn giao dịch phi tập trung (DEX). Nó cũng cung cấp cho người dùng một điểm vào thế giới tài chính phi tập trung mới nổi, hoặc DeFi, cung cấp một cách để truy cập các ứng dụng DeFi như Compound và PoolTogether.



Hình 3. Giao diện tương tác ví Metamask

VI. GANACHE VÀ TRUFFLE

2.6.1 Ganache

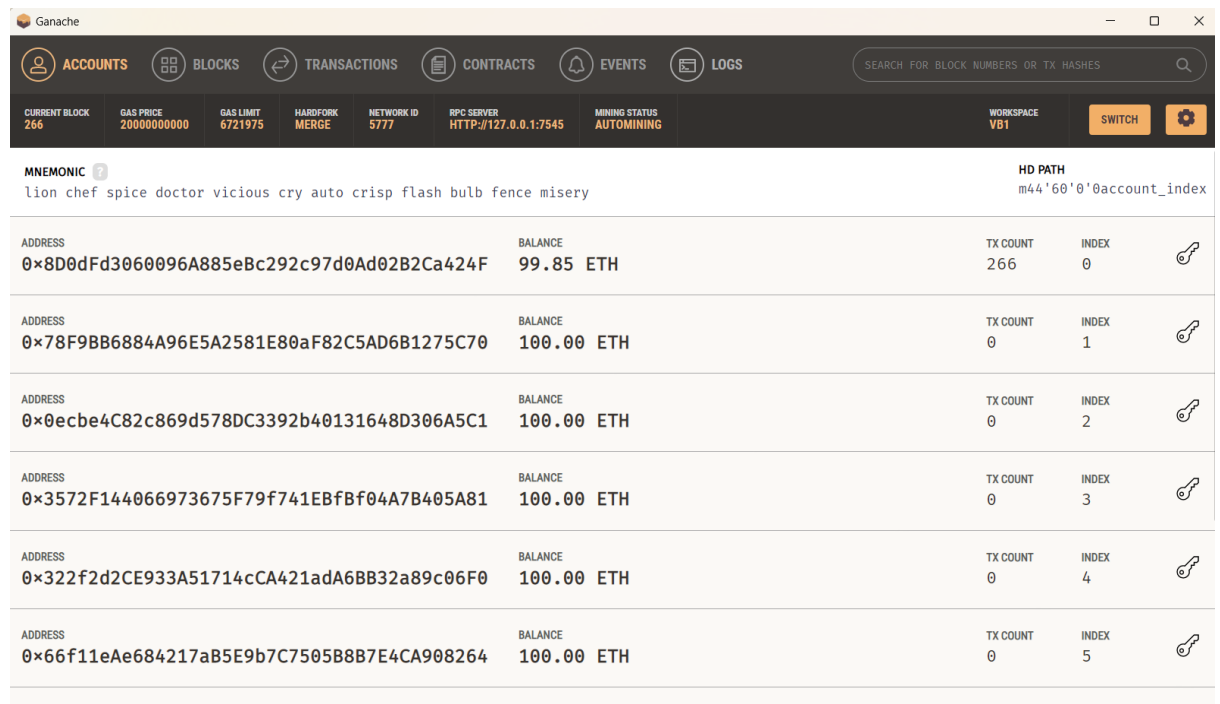
Ganache là một công cụ phát triển cao cấp được sử dụng để chạy blockchain cục bộ và cho cả việc phát triển Ethereum và Corda DApp. Ganache rất hữu ích trong tất cả các phần của quá trình phát triển. Chuỗi cục bộ cho phép phát triển, triển khai và thử nghiệm các dự án và hợp đồng thông minh của mình trong một môi trường xác định và an toàn. Ganache còn tạo sẵn 10 địa chỉ ví (wallet) trong đó

Chương 2: Cơ sở lý thuyết

mỗi wallet có sẵn 100 Ether để hỗ trợ trong quá trình phát triển các ứng dụng DApp.

Ganache là một phần của hệ sinh thái Truffle Suite. Cụ thể, Truffle Suite bao gồm Ganache và một cặp công cụ bổ sung: Truffle và Drizzle

Có hai "phiên bản" khác nhau của Ganache, một ứng dụng máy tính để bàn và một công cụ dòng lệnh. Ứng dụng dành cho máy tính để bàn được gọi là Ganache UI và nó hỗ trợ phát triển cho cả Ethereum và Corda. Trong khi đó, công cụ dòng lệnh được gọi là ganache-CLI, chỉ hỗ trợ phát triển Ethereum.



Hình 4. Giao diện Ganache và các ví điện tử

2.6.2 Truffle

Như đã nói ở trên, Truffle là thành phần cốt lõi của Truffle Suite, đóng vai trò là khung phát triển toàn diện cho các DApp Ethereum. Nó cung cấp cho các nhà phát triển các công cụ, bao gồm trình biên dịch hợp đồng thông minh, kiểm tra tự động và các tập lệnh triển khai sử dụng EMV (Máy ảo Ethereum). Với Truffle, các nhà phát triển có thể viết và quản lý hiệu quả các hợp đồng thông minh bằng ngôn ngữ lập trình Solidity. Nó đơn giản hóa quá trình phát triển bằng cách cung cấp các tính năng như di chuyển hợp đồng, quản lý mạng và gỡ lỗi.

Truffle cũng tích hợp với các khung thử nghiệm phổ biến và cho phép các nhà phát triển mô phỏng các kịch bản trong thế giới thực, đảm bảo độ tin cậy và bảo mật của các hợp đồng thông minh của họ trước khi triển khai.

VII. MONGODB

2.7.1 MongoDB

MongoDB là một phần mềm mã nguồn mở dùng để quản trị cơ sở dữ liệu NoSQL. NoSQL (Not only SQL) được sử dụng thay thế cho cơ sở dữ liệu quan hệ (Relational Database – RDB) truyền thống. Cơ sở dữ liệu NoSQL khá hữu ích trong khi làm việc với các tập dữ liệu phân tán lớn.

MongoDB là một công cụ có thể quản lý thông tin hướng document cũng như lưu trữ hoặc truy xuất thông tin. Trong khi đó, ngôn ngữ truy vấn có cấu trúc (SQL) là ngôn ngữ lập trình được tiêu chuẩn hóa, dùng để quản lý cơ sở dữ liệu quan hệ. Dữ liệu được chuẩn hóa SQL dưới dạng schema và table và mọi table đều có cấu trúc cố định.

VIII. THUẬT TOÁN ĐỒNG THUẬN

Thuật toán đồng thuận được sử dụng để đạt được sự thống nhất về một giá trị dữ liệu duy nhất giữa các quy trình hoặc hệ thống phân tán. Các thuật toán này được thiết kế để đạt được độ tin cậy trong mạng có nhiều người dùng hoặc nút. Việc giải quyết vấn đề đồng thuận rất quan trọng trong các hệ thống điện toán phân tán và đa tác nhân, chẳng hạn như các hệ thống được thấy trong các mạng chuỗi khối tiền điện tử.

Blockchain là ứng dụng phổ biến nhất của thuật toán đồng thuận. Với mục tiêu là đảm bảo tồn tại duy nhất một lịch sử giao dịch và lịch sử giao dịch đó không chứa các giao dịch không hợp lệ hoặc các giao dịch có mâu thuẫn.

STT	Tên thuật toán	Cơ chế hoạt động	Ví dụ
1	Proof of Work (PoW): Bằng chứng công việc	Các thợ đào (miner) phải chứng minh rằng công việc họ đã thực hiện và gửi cho họ quyền thêm giao dịch mới vào chuỗi khối. Họ phải giải một bài toán phức tạp bằng cách tìm hàm băm mật mã của một khối cụ thể.	Bitcoin (BTC), Ethereum (ETH).

2	Proof of Stake (PoS): Bằng chứng cổ phần	PoS yêu cầu ít tài nguyên phần cứng hoặc phần mềm chuyên dụng để khai thác tiền điện tử vì nó không liên quan đến việc giải quyết các vấn đề tính toán phức tạp. Người xác thực nhận được phần thưởng hoặc số tiền đặt cược (stake) của họ tăng lên tương ứng với số tiền đặt cược của họ dựa trên các khối được thêm vào chuỗi khối.	Binance Coin (BNB), Ontology (ONT).
3	Delegated Proof of Stake (DPoS): Bằng chứng cổ phần được ủy quyền	Thuật toán này dựa trên hệ thống bỏ phiếu trong đó các đại biểu hoặc nhân chứng bỏ phiếu cho người xác nhận yêu thích của họ để đạt được sự đồng thuận trong quá trình tạo và xác thực các khối. Bên cạnh việc xác thực các giao dịch, các đại biểu còn giúp duy trì tính toàn vẹn, độ tin cậy và tính minh bạch của mạng blockchain.	Bitshares (BTS)

Bảng 1: Một số thuật toán đồng thuận

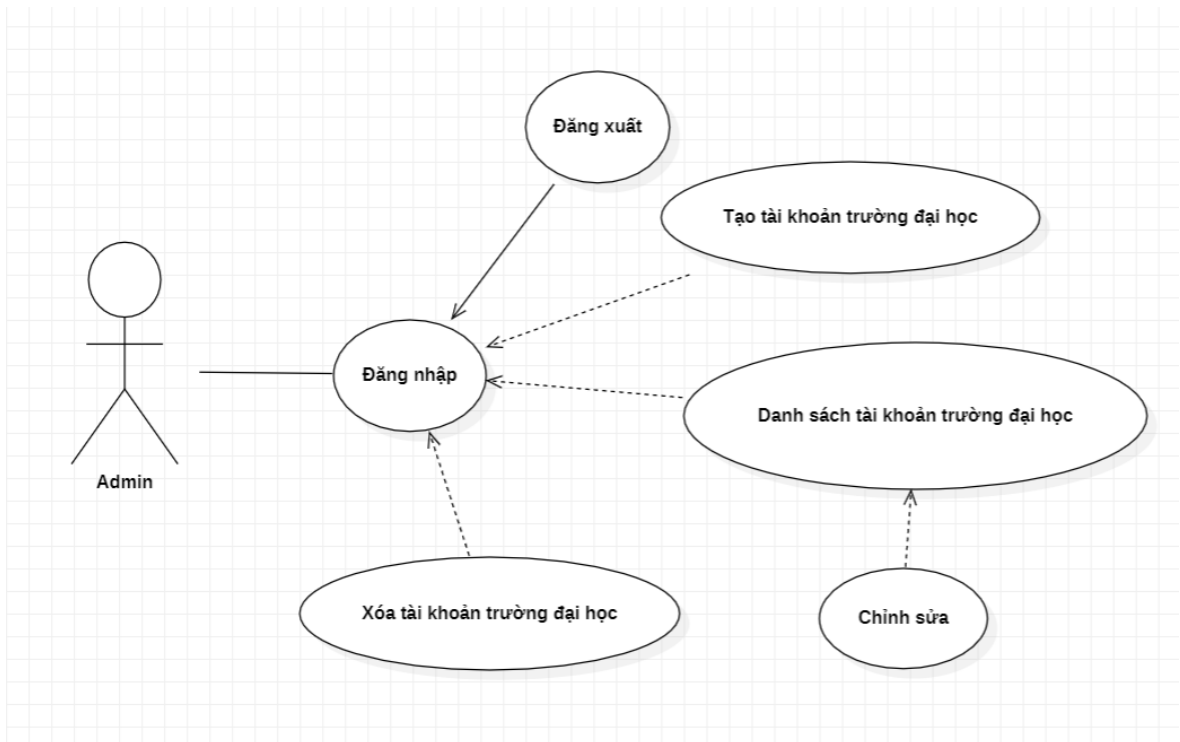
CHƯƠNG 3: GIẢI QUYẾT VẤN ĐỀ

I. ĐẶC TẢ ĐỀ TÀI

Hệ thống chứng thực bằng cấp sử dụng blockchain được xây dựng và cài đặt nhằm mục đích giúp người dùng dễ dàng nhận và chứng thực văn bằng tốt nghiệp, khiến cho việc phát hành và chứng thực bằng tốt nghiệp của trường đại học trở nên chính xác, minh bạch, thuận lợi và tiết kiệm thời gian hơn. Tăng độ tin cậy cho hệ thống khi người dùng chỉ có thể xem nhưng không thể thêm, sửa, xóa và công tác tạo và phát hành bằng tốt nghiệp sẽ nhanh hơn do vấn đề buôn bán, sử dụng văn bằng, chứng chỉ giả đã và đang là một vấn nạn của xã hội. Các cơ quan, tổ chức đều đang phải đối mặt với bài toán nan giải này trong những thời điểm như tuyển dụng, tổ chức các kỳ thi nâng cao trình độ hoặc xét duyệt đi du học.

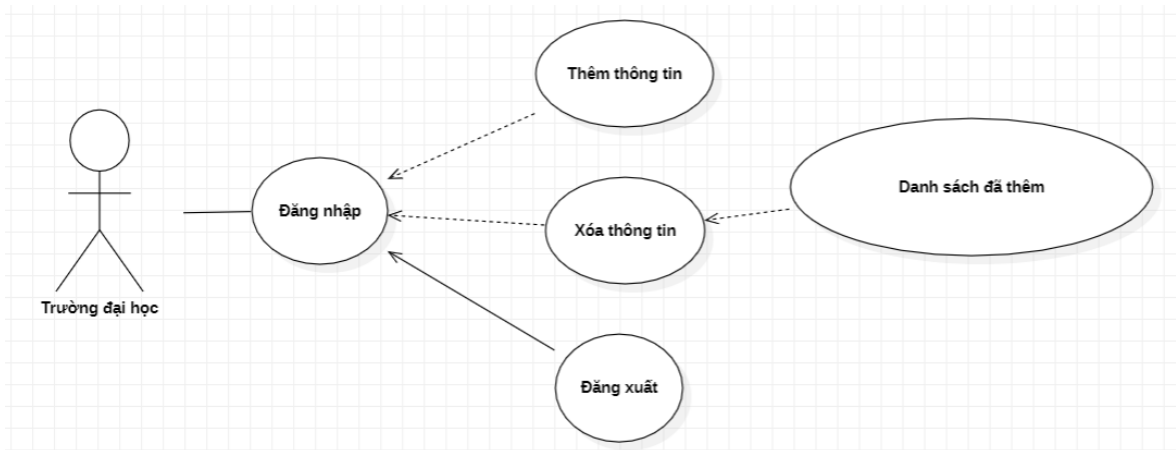
II. SƠ ĐỒ CHỨC NĂNG CỦA HỆ THỐNG

3.2.1 Sơ đồ Use Case đối với Admin



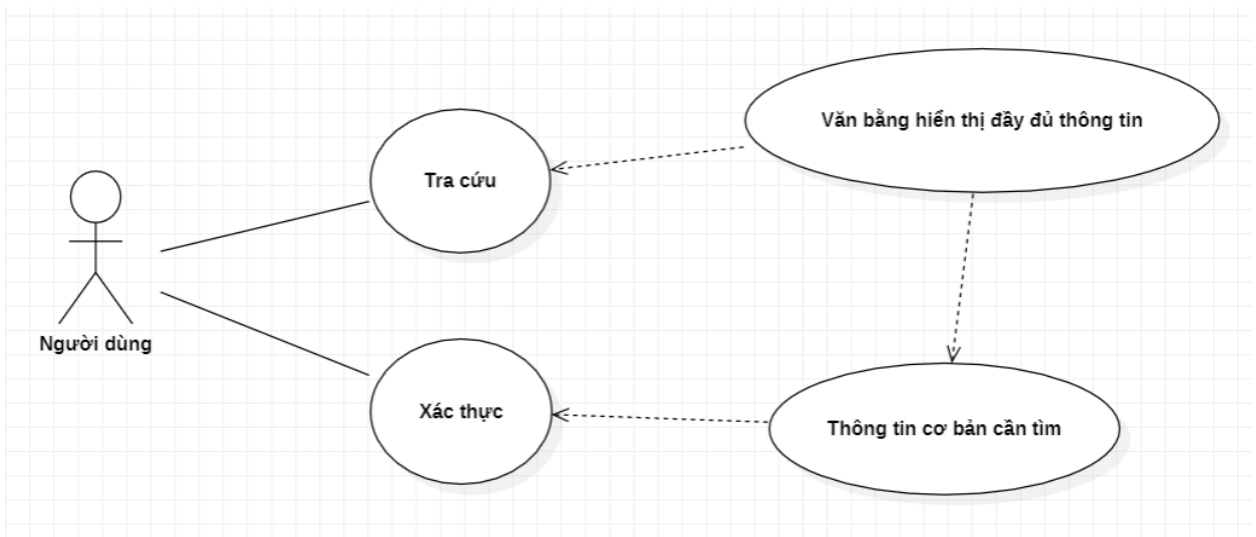
Hình 5. Sơ đồ Use case Admin

3.2.2 Sơ đồ Use Case đối với Trường Đại học



Hình 6. Sơ đồ Use case Trường Đại học

3.2.3 Sơ đồ Use Case đối với Người dùng



Hình 7. Sơ đồ Use case Người dùng

III. ĐẶC TẢ YÊU CẦU CHỨC NĂNG

3.3.1 Đăng nhập

Tên chức năng	Đăng nhập
Đối tượng sử dụng	Admin, Trường Đại học
Tiền điều kiện	Mở được trang chủ hệ thống, có tài khoản trên hệ thống.

Chương 3: Giải quyết vấn đề

Cách xử lý	Bước 1: Mở trang chủ và chọn nút Đăng nhập. Bước 2: Sau khi chuyển sang trang Đăng nhập: nhập username và mật khẩu. Bước 3: Chọn nút “Đăng nhập”: <ul style="list-style-type: none">• Nếu username và mật khẩu đúng thì đăng nhập thành công.• Ngược lại, thông báo đăng nhập thất bại.
Kết quả	Đăng nhập tài khoản username, admin thành công.
Ghi chú	Phải nhập đầy đủ và chính xác: username và mật khẩu.

Bảng 2: Đặc tả chức năng Đăng nhập

3.3.2 Tạo tài khoản cho Trường Đại học

Tên chức năng	Tạo tài khoản cho Trường Đại học
Đối tượng sử dụng	Admin
Tiền điều kiện	Mở được trang chủ hệ thống, đăng nhập thành công tài khoản Admin
Cách xử lý	Bước 1: Mở trang chủ hệ thống và tiến hành đăng nhập. Bước 2: Sau khi đăng nhập thành công sẽ chuyển hướng đến trang Tạo tài khoản Nhà trường. Nhập thông tin (Username, Trường, tên hiệu trưởng, mật khẩu) Bước 3: Nhấn nút “Tạo tài khoản user cho Trường Đại học”
Kết quả	Tạo thành công.
Ghi chú	Chỉ Admin mới có thể tạo tài khoản cho user cho Trường Đại học

Bảng 3: Đặc tả chức năng Tạo tài khoản cho Trường Đại học

3.3.3 Xóa tài khoản của Trường Đại học

Chương 3: Giải quyết vấn đề

Tên chức năng	Xóa tài khoản của Trường Đại học
Đối tượng sử dụng	Admin
Tiền điều kiện	Mở được trang chủ hệ thống, đăng nhập thành công tài khoản Admin
Cách xử lý	Bước 1: Mở trang chủ hệ thống và tiến hành đăng nhập. Bước 2: Sau khi đăng nhập thành công sẽ chuyển hướng đến trang Tạo tài khoản cho Trường Đại học. Bước 3: Chọn mục Xóa tài khoản. Nhập thông tin (Username, Trường, Mật khẩu) Bước 4: Nhấn nút “Xóa tài khoản”
Kết quả	Xóa thành công.
Ghi chú	Chỉ Admin mới có thể xóa tài khoản của Trường Đại học

Bảng 4: Đặc tả chức năng Xóa tài khoản của Trường Đại học

3.3.4 Thêm thông tin sinh viên

Tên chức năng	Thêm thông tin sinh viên
Đối tượng sử dụng	Trường Đại học
Tiền điều kiện	Mở được trang chủ hệ thống, đăng nhập thành công tài khoản Trường Đại học được cấp
Cách xử lý	Bước 1: Mở trang chủ hệ thống và tiến hành đăng nhập. Bước 2: Sau khi đăng nhập thành công sẽ chuyển hướng đến trang Thêm thông tin, nhập thông tin (Họ tên, MSSV, ngày sinh, tên trường, ngành học,...). Bước 3: Nhấn nút “Thêm thông tin”
Kết quả	Thêm thông tin thành công.
Ghi chú	- Chỉ Trường Đại học mới có thể thêm thông tin.

Chương 3: Giải quyết vấn đề

	- Nhằm tăng tính an toàn và bảo mật, khi Nhà trường thực hiện các chức năng khác, muốn quay về chức năng thêm cần đăng nhập lại.
--	--

Bảng 5: Đặc tả chức năng Thêm thông tin

3.3.5 Xóa thông tin sinh viên

Tên chức năng	Xóa thông tin sinh viên
Đối tượng sử dụng	Trường Đại học
Tiền điều kiện	Mở được trang chủ hệ thống, đăng nhập thành công tài khoản mà Trường Đại học được cấp
Cách xử lý	Bước 1: Mở trang chủ hệ thống và tiến hành đăng nhập. Bước 2: Sau khi đăng nhập thành công sẽ chuyển hướng đến trang Thêm thông tin. Bước 4: Chọn mục Xóa thông tin, nhập các thông tin cần thiết (Mssv, trường, Mật khẩu của tài khoản Trường Đại học đó) Bước 3: Nhấn nút “Xóa thông tin”
Kết quả	Xóa thông tin thành công.
Ghi chú	Chỉ Trường Đại học mới có thể thêm thông tin.

Bảng 6: Đặc tả chức năng Xóa thông tin

3.3.6 Xem Bằng tốt nghiệp

Tên chức năng	Xem bằng tốt nghiệp
Đối tượng sử dụng	Người dùng
Tiền điều kiện	Mở được trang chủ hệ thống
Cách xử lý	<u>Cách 1: Tra cứu (chủ sở hữu văn bằng)</u> Bước 1: Mở trang chủ hệ thống và chọn

	<p>nút “Tra cứu”.</p> <p>Bước 2: Sau khi chuyển sang trang Tra cứu, nhập MSSV, tên Trường Đại học và Mật khẩu trường cấp.</p> <p>Bước 3: Chọn nút “Tra cứu”.</p> <ul style="list-style-type: none"> • Nếu số thông tin vừa nhập đúng thì chuyển hướng xem bằng tốt nghiệp. • Ngược lại, thông báo thông tin không trùng khớp. <p><u>Cách 2: Xác Thực (truy xuất văn bằng)</u></p> <p>Bước 1: Mở trang chủ hệ thống và chọn nút “Xác thực”.</p> <p>Bước 2: Sau khi chuyển sang trang Xác thực, nhập MSSV, tên Trường Đại học và Số hiệu văn bằng</p> <p>Bước 3: Chọn nút “Xác thực”.</p> <ul style="list-style-type: none"> • Nếu thông tin hợp lệ sẽ hiển thị cỡ bản các thông tin (MSSV, Ngành, Hình thức đào tạo, Năm tốt nghiệp, Loại tốt nghiệp). • Ngược lại, thông báo thông tin không tồn tại. <p>Bước 5: Bấm vào nút “Xem chi tiết”</p>
Kết quả	Xem được bằng tốt nghiệp.
Ghi chú	<p>Phải nhập đầy đủ và chính xác thông tin yêu cầu</p> <p>Không xem được thông tin của những người khác nếu không nhập đúng các thông tin yêu cầu.</p>

Bảng 7: Đặc tả chức năng Xem bằng tốt nghiệp

IV. ĐẶC TẢ YÊU CẦU PHI CHỨC NĂNG

3.4.1 Yêu cầu thực thi

Chạy được trên hệ điều hành Window và hỗ trợ sử dụng trên các trình duyệt như: Chrome, Microsoft Edge, Fire Fox,...

3.4.2 Yêu cầu bảo mật

Hệ thống sẽ phân quyền người dùng. Người dùng chỉ có thể thực hiện được một vài chức năng nhất định.

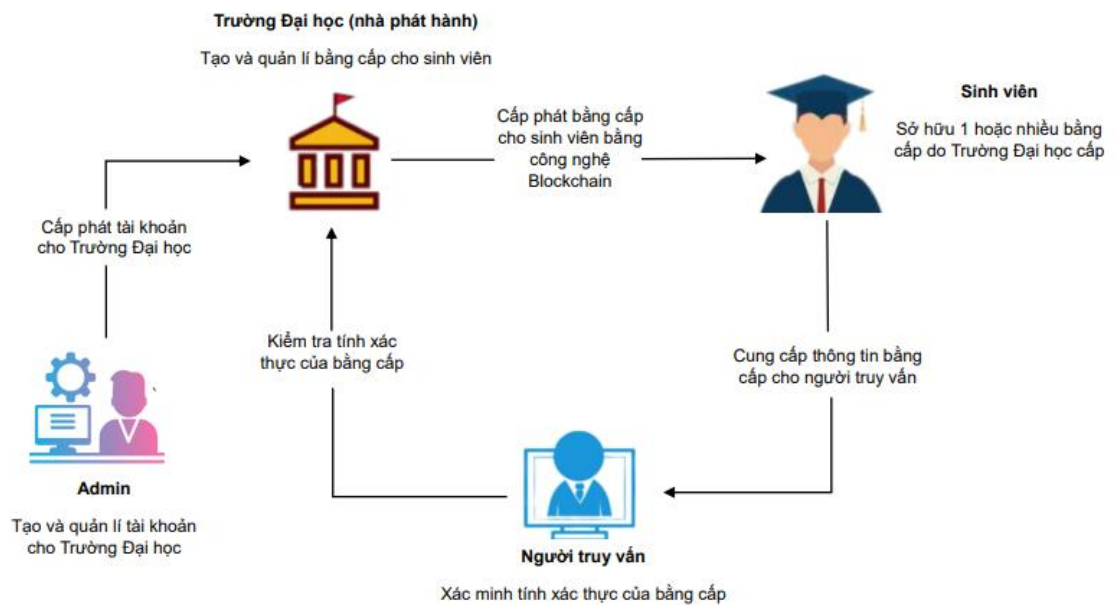
3.4.3 Đặc điểm hệ thống

- Giao diện thân thiện, dễ sử dụng.
- Từ ngữ đơn giản, dễ hiểu.
- Chứng thực văn bằng tốt nghiệp nhanh chóng.
- Đảm bảo việc tuân thủ quy định của pháp luật và an toàn an ninh mạng.

3.4.4 Môi trường vận hành

- Phần cứng: Máy tính
- Phần mềm:
 - + Hệ điều hành: Window
 - + Trình duyệt: Chrome, Microsoft Edge, Fire Fox,...
 - + Visual Code Studio
 - + Có kết nối: MetaMask, Ganache, MongoDB.

3.4.5 Mô hình tổng quan hệ thống



Hình 8. Mô hình tổng quan hệ thống

V. CÀI ĐẶT HỆ THỐNG

3.5.1 Cấu trúc hợp đồng thông minh

Trong hợp đồng thông minh sẽ có một struct đại diện cho sinh viên, cấu trúc thông tin của sinh viên.

```
struct Student {  
    string truong; // Tên trường  
    string msvv; // Mã số sinh viên  
    string bang; // Bằng cấp  
    string fullName; // Họ và tên  
    string ngaySinh; // Ngày sinh  
    string ngành; // Ngành học  
    string nam; // Năm sinh  
    string loai; // Loại bằng cấp  
    string hìnhThuc; // Hình thức đào tạo  
    string soHieu; // Số hiệu sinh viên  
}
```

Hình 9. Cấu trúc sinh viên trong hợp đồng thông minh

Tiếp theo, hợp đồng thông minh này sẽ có 4 kiểu mapping lưu trữ địa chỉ đã đã thêm sinh viên, danh sách sinh viên đã được thêm, địa chỉ đã thực hiện xác thực và địa chỉ đã tra cứu. Kiểu dữ liệu mapping trong Solidity là kiểu dữ liệu dạng key value tương tự như kiểu dữ liệu dictionary ở các ngôn ngữ khác.

```
address private owner; // Địa chỉ của chủ sở hữu hợp đồng (trường đại học)
mapping(bytes32 => bool) studentAdded; // Lưu trữ địa chỉ đã thêm sinh viên
mapping(bytes32 => Student) students; // Lưu trữ danh sách sinh viên đã được thêm
mapping(bytes32 => address) verifiedAddresses; // Lưu trữ địa chỉ đã thực hiện xác thực
mapping(bytes32 => address) lookupAddresses; // Lưu trữ địa chỉ đã tra cứu
```

Hình 10. Các biến trong hợp đồng thông minh

3.5.2 Cài đặt hợp đồng thông minh

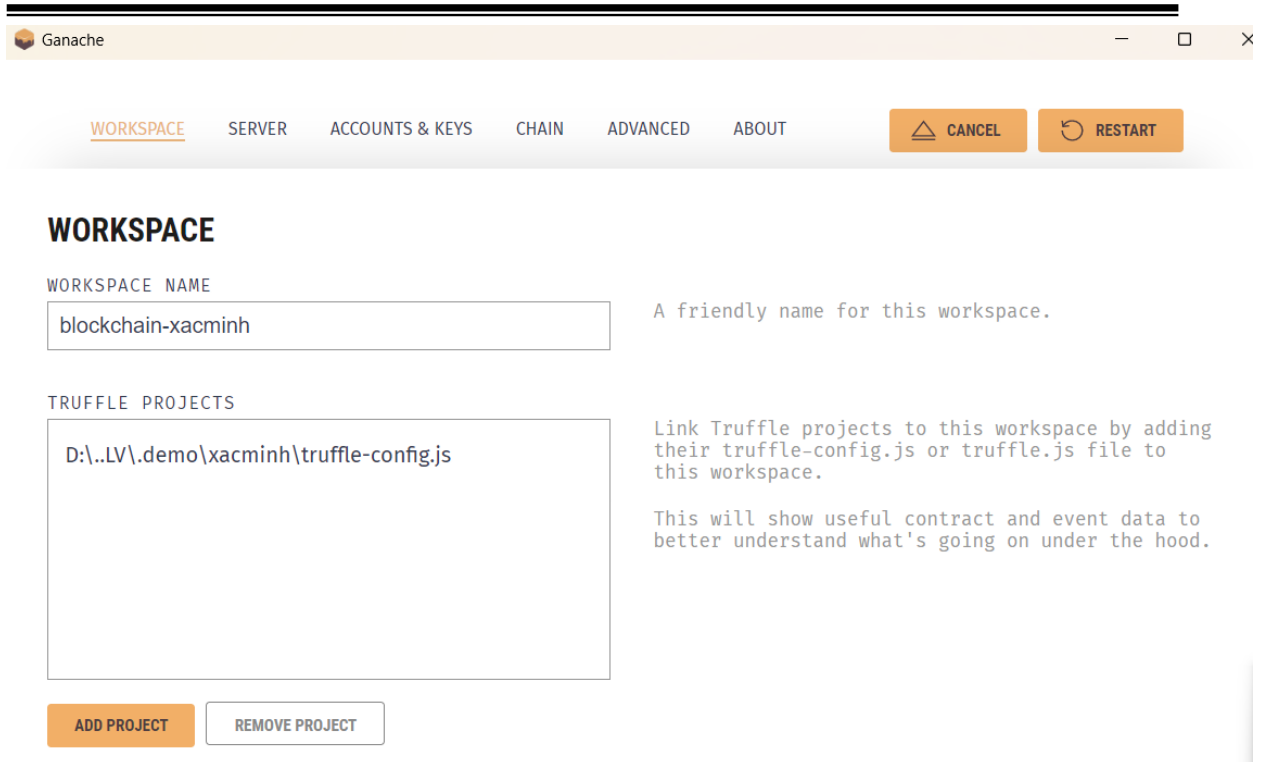
- Chuẩn bị:
 - + Cài đặt Nodejs
 - + Cài đặt Truffle: `npm install -g truffle`
 - + Khởi tạo Truffle project
 - + Cấu hình mạng trong file “truffle-config.js”

```
module.exports = {
  // See <http://truffleframework.com/docs/advanced/configuration>
  networks: {
    development: {
      host: "127.0.0.1",
      port: 7545,
      network_id: "*" // Match any network id
    },
    develop: {
      port: 8545
    }
  }
};
```

Hình 11. Nội dung file cấu hình mạng truffle-config.js

Cài đặt Ganache, khởi chạy Ganache và dẫn file truffle-config.js vào Ganache.

Chương 3: Giải quyết vấn đề



Hình 12. Thêm Workspace cho Ganache

- Viết và đẩy hợp đồng thông minh vào project.
- Compile hợp đồng thông minh: `truffle compile`.
Lệnh này tạo ra một file `build/contracts`. Các file này là bản tóm tắt của Smart Contract và chứa thông tin sau:
 - + Contract name.
 - + ABI (danh sách tất cả các hàm cùng với các giá trị tham số và giá trị trả về của chúng).
 - + Bytecode.
 - + Deployed bytecode.
 - + Compiler name và phiên bản của nó.
 - + Danh sách các networks mà hợp đồng được deploy.
 - + Địa chỉ của contract đối với từng mạng mà contract được deploy.
- Viết Migrations

```
var xacminh = artifacts.require("./xacminh.sol");

module.exports = function(deployer) {
  deployer.deploy(xacminh);
};
```

Hình 13. Viết Migrations

Chương 3: Giải quyết vấn đề

- Sau đó chạy lệnh: `truffle migrate --reset`

```
Starting migrations...
=====
> Network name:      'development'
> Network id:        5777
> Block gas limit: 6721975 (0x6691b7)

1_initial_migration.js
=====

Replacing 'xacminh'
-----
> transaction hash:  0x165511d1309146029a70f73b8fc7c39d0ebae32c06697d92a5437727a0ffd3d9
> Blocks: 0         Seconds: 0
> contract address: 0x0bC13c671772f3B017dE82dfb397D9AAA487C9c5
> block number:     389
> block timestamp:  1714035362
> account:          0x8D0dFd3060096A885eBc292c97d0Ad02B2Ca424F
> balance:          99.755830069994445119
> gas used:         890710 (0xd9756)
> gas price:        2.500000008 gwei
> value sent:       0 ETH
> total cost:       0.00222677500712568 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost:       0.00222677500712568 ETH

Summary
=====
> Total deployments: 1
> Final cost:       0.00222677500712568 ETH
```

Hình 14. Kết quả khi chạy lệnh `truffle migrate --reset`

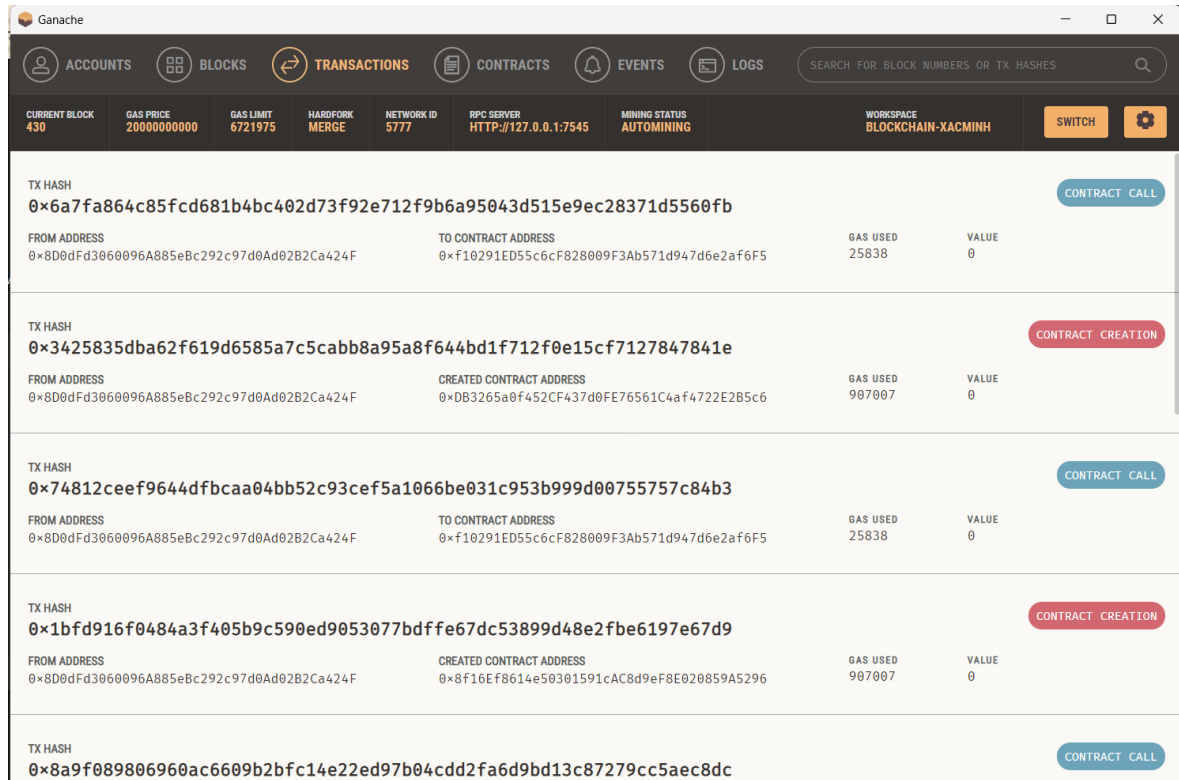
- Truy vấn thông tin trên Blockchain – Transactions

Hiển thị danh sách các giao dịch trên chuỗi khối Ethereum. Các giao dịch được liệt kê theo số khối, hàm băm giao dịch, địa chỉ hợp đồng, từ địa chỉ này đến địa chỉ khác, lượng gas được sử dụng và giá trị.

- **Số khối** là số khối trong đó giao dịch được bao gồm.
- **Băm giao dịch** là mã định danh duy nhất cho giao dịch.
- **Địa chỉ hợp đồng** là địa chỉ của hợp đồng thông minh mà giao dịch đang tương tác.
- **Địa chỉ người gửi** là địa chỉ của tài khoản đã gửi giao dịch.
- **Địa chỉ** là địa chỉ của tài khoản đã nhận giao dịch.

Chương 3: Giải quyết vấn đề

- **Gas được sử dụng** là lượng gas đã được sử dụng để thực hiện giao dịch.
- **Giá trị** là lượng ether được chuyển trong giao dịch.



TX HASH	FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE	
0x6a7fa864c85fcd681b4bc402d73f92e712f9b6a95043d515e9ec28371d5560fb	0x8D0dFd3060096A885eBc292c97d0Ad02B2Ca424F	0xf10291ED55c6cF828009F3Ab571d947d6e2af6F5	25838	0	CONTRACT CALL
0x3425835dba62f619d6585a7c5cabb8a95a8f644bd1f712f0e15cf7127847841e	0x8D0dFd3060096A885eBc292c97d0Ad02B2Ca424F	0xDB3265a0f452CF437d0FE76561C4af4722E2B5c6	907007	0	CONTRACT CREATION
0x74812ceef9644dfbcaa04bb52c93cef5a1066be031c953b999d00755757c84b3	0x8D0dFd3060096A885eBc292c97d0Ad02B2Ca424F	0xf10291ED55c6cF828009F3Ab571d947d6e2af6F5	25838	0	CONTRACT CALL
0x1bfd916f0484a3f405b9c590ed9053077bdf67dc53899d48e2f6e6197e67d9	0x8D0dFd3060096A885eBc292c97d0Ad02B2Ca424F	0x8f16EF8614e50301591cAC8d9eF8E020859A5296	907007	0	CONTRACT CREATION
0x8a9f089806960ac6609b2bfc14e22ed97b04cdd2fa6d9bd13c87279cc5aec8dc					CONTRACT CALL

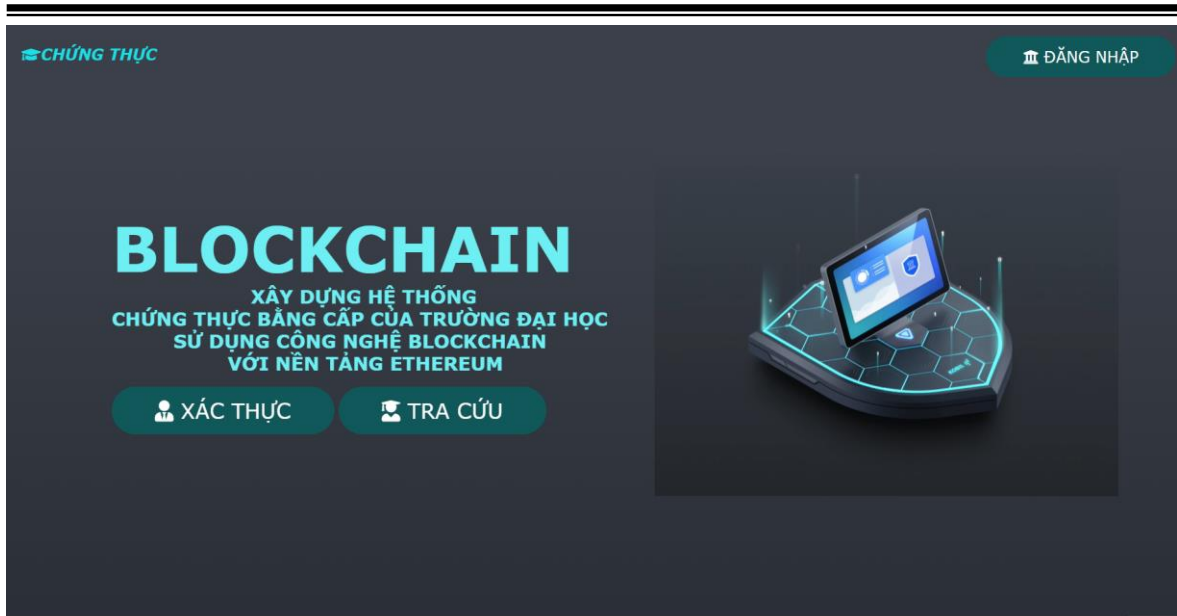
Hình 15: Kết quả Transactions

VI. GIAO DIỆN CÁC CHỨC NĂNG

3.6.1 Giao diện Trang chủ

Trang chủ là giao diện đầu tiên khi chúng ta vào trang web. Với 3 chức năng chủ yếu: đăng nhập, xác thực và tra cứu.

- Chức năng đăng nhập: Admin và Trường Đại học đã được cấp tài khoản có thể sử dụng chức năng đăng nhập này
- Chức năng xác thực: người dùng là sinh viên hay các nhà tuyển dụng,... có thể vào để xác thực khi có họ tên và mã văn bằng của sinh viên
- Chức năng tra cứu: sinh viên với tài khoản đã được cấp có thể vào để tra cứu thông tin văn bằng của mình



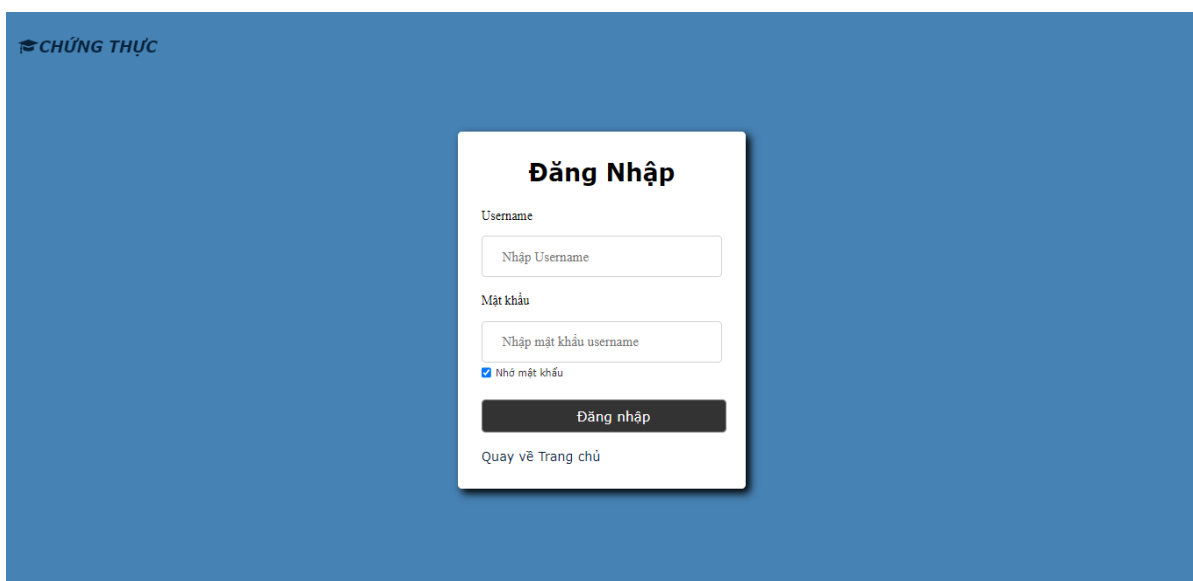
Hình 16. Giao diện Trang chủ

3.6.2 Giao diện Đăng nhập

Chức năng được sử dụng cho các Trường Đại học đã được cấp tài khoản, các tài khoản này sẽ được Admin tạo và cấp cho Trường Đại học. Đồng thời Admin sẽ đăng nhập tài khoản mặc định để truy cập.

Mục đích: đăng nhập tài khoản để thực hiện các chức năng nhất định

Đối tượng người dùng: Admin, Trường Đại học



Hình 17. Giao diện Đăng nhập

3.6.3 Giao diện Thêm Username

Chỉ Admin mới có quyền truy cập vào trang này, Admin có nhiệm vụ tạo tài khoản cho các Trường Đại học gồm các thông tin user, tên trường Đại học, tên Hiệu trưởng và tạo mật khẩu cho Trường Đại học đó

Nhập thông tin để tạo tài khoản

Username

Nhập tên username muốn tạo

Tên trường

Nhập tên Trường Đại học

Hiệu trưởng

Nhập tên Hiệu trưởng của Trường Đại học

Mật khẩu

Tạo mật khẩu cho username

Tạo tài khoản

Hình 18. Giao diện Thêm Username

3.6.4 Giao diện Danh sách Username

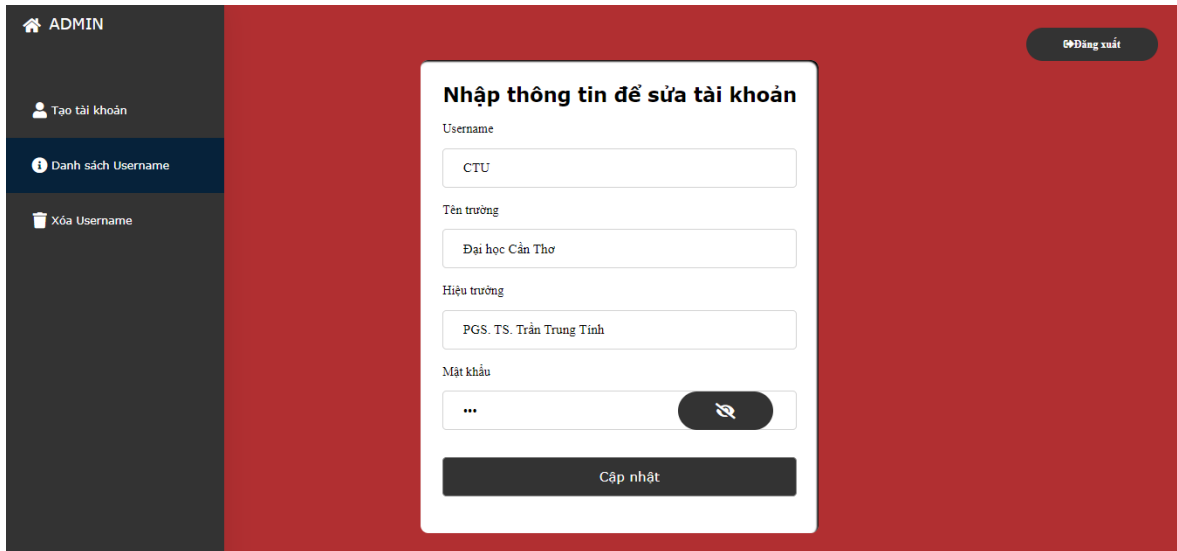
Ngoài việc tạo tài khoản, Admin có thể xem danh sách các tài khoản của Trường Đại học mà Admin đã tạo.

STT	Username	Trường	Hiệu trưởng	
1	CTU	Đại học Cần Thơ	PGS. TS. Trần Trung Tính	Sửa
2	CTUMP	Đại học Y Dược Cần Thơ	GS. TS. BS. Nguyễn Trung Kiên	Sửa
3	CTUET	Đại học Kỹ thuật - Công nghệ Cần Thơ	NGƯT. PGS. TS. Huỳnh Thanh Nhă	Sửa
4	NCTU	Đại học Nam Cần Thơ	TS. Nguyễn Văn Quang	Sửa
5	TDU	Đại học Tây Đô	GS.TS.TTƯT. Trần Công Luận	Sửa
6	FPTU	Đại học FPT Cần Thơ	TS. Nguyễn Khắc Thành	Sửa
7	Admin			Sửa

Hình 19. Giao diện Danh sách Username

3.6.5 Giao diện Sửa Username

Khi một Hiệu trưởng trong Trường Đại học nào đó đã hết nhiệm kỳ, Admin có thể vào sửa tên của Hiệu trưởng trường đó. Ngoài ra, Admin cũng có quyền sửa mật khẩu của Trường Đại học đó nếu cần.

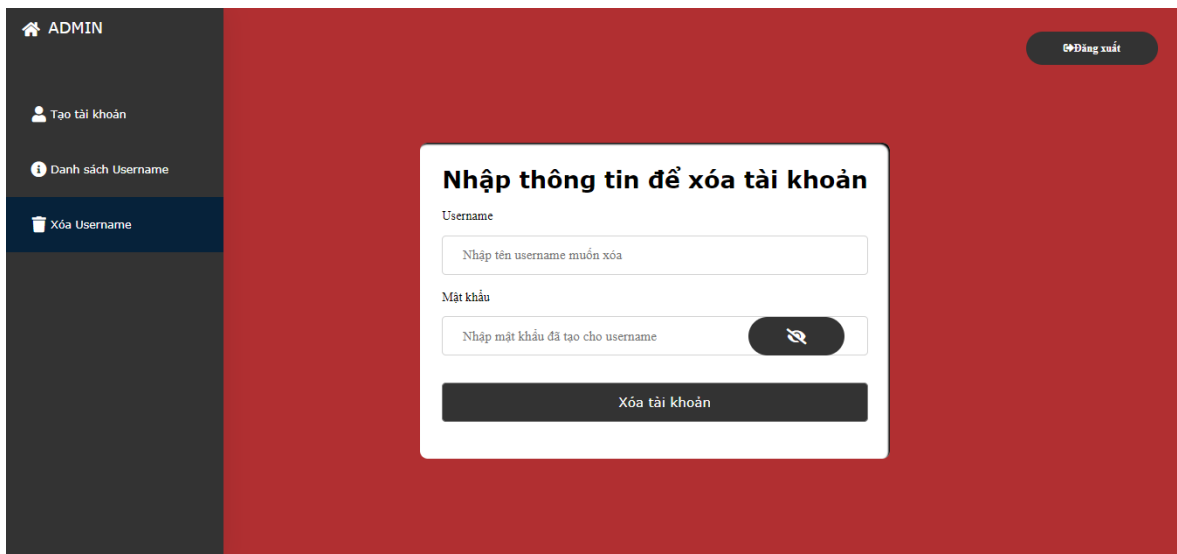


The screenshot shows the Admin interface with a sidebar on the left containing links: ADMIN, Tạo tài khoản, Danh sách Username, and Xóa Username. The main content area has a red background and a 'Đăng xuất' button in the top right. A white form titled 'Nhập thông tin để sửa tài khoản' is centered. It contains four input fields: 'Username' (with 'CTU'), 'Tên trường' (with 'Đại học Cần Thơ'), 'Hiệu trưởng' (with 'PGS. TS. Trần Trung Tính'), and 'Mật khẩu' (with a masked input and a toggle icon). A 'Cập nhật' button is at the bottom of the form.

Hình 20. Giao diện Sửa Username

3.6.6 Giao diện Xóa Username

Trường hợp có một trường đại học nào đó ngưng hoạt động, admin có thể xóa tài khoản của nhà trường đó.



The screenshot shows the Admin interface with the same sidebar as Figure 20. The main content area has a red background and a 'Đăng xuất' button in the top right. A white form titled 'Nhập thông tin để xóa tài khoản' is centered. It contains two input fields: 'Username' (with placeholder 'Nhập tên username muốn xóa') and 'Mật khẩu' (with placeholder 'Nhập mật khẩu đã tạo cho username' and a toggle icon). A 'Xóa tài khoản' button is at the bottom of the form.

Hình 21. Giao diện Xóa Username

Chương 3: Giải quyết vấn đề

3.6.7 Giao diện Thêm thông tin

Trường Đại học sẽ nhập các thông tin cũng như mật khẩu để tạo thông tin cho bằng tốt nghiệp và cấp tài khoản tra cứu để sinh viên có thể tra cứu bằng tốt nghiệp. Các thông tin như tên Trường Đại học và tên Hiệu trưởng sẽ được mặc định, và tên Hiệu trưởng sẽ thay đổi theo mỗi nhiệm kỳ tùy vào từng Trường Đại học.

TRƯỜNG ĐẠI HỌC Đăng xuất

Thêm thông tin

Xóa thông tin

Hãy thêm các thông tin sau

Họ và Tên	Mã số sinh viên
<input type="text" value="Ghi rõ Họ và Tên"/>	<input type="text" value="Nhập MSSV"/>
Ngày sinh:	Trường
<input type="text" value="dd/mm/yyyy"/>	<input type="text" value="Đại học Cần Thơ"/>
Ngành học	Năm tốt nghiệp
<input type="text" value="Nhập Ngành học"/>	<input type="text" value="Nhập Năm Tốt nghiệp"/>
Xếp loại tốt nghiệp	Loại Bằng Tốt nghiệp
<input type="text" value="Chọn xếp loại tốt nghiệp"/>	<input type="text" value="Chọn loại bằng"/>
Hình thức tốt nghiệp	Số hiệu
<input type="text" value="Chọn hình thức tốt nghiệp"/>	<input type="text" value="VÍ DỤ: VBXXXX"/>
Mật khẩu	Hiệu trưởng
<input type="text" value="Tạo mật khẩu cho sinh viên"/>	<input type="text" value="PGS. TS. Trần Trung Tĩnh"/>

Tạo thông tin

Hình 22. Giao diện Thêm thông tin

3.6.8 Giao diện Danh sách thông tin

Danh sách thông tin sẽ hiển thị các thông tin mà Trường Đại học đã thêm như ở trên.

TRƯỜNG ĐẠI HỌC Đăng xuất

Thêm thông tin

Danh sách

Xóa thông tin

STT	MSSV	Tên	Ngành học	Hình thức đào tạo	Năm Tốt nghiệp	Xếp loại tốt nghiệp
1	B2002307	Uchiha Sasuke	Công nghệ thông tin	Chính quy	2024	Xuất sắc
2	B2002605	SEVENTEEN	Hệ thống thông tin	Chính quy	2024	Xuất sắc
3	B2001010	Sesshomaru	Khoa học máy tính	Chính quy	2024	Xuất sắc
4	B2004790	Dương Trúc Mai	Mạng máy tính và truyền thông dữ liệu	Chính quy	2024	Giỏi

Hình 23. Giao diện Xem danh sách

3.6.9 Giao diện Xóa thông tin

Với trường hợp Trường Đại học vô tình nhập sai thông tin về bằng, thì Trường Đại học có thể nhập thông tin để xóa tài khoản. Mọi trường hợp khác, thì Trường Đại học hoàn toàn không được tùy tiện xóa thông tin.

The screenshot shows a web interface for a university system. On the left is a dark sidebar with a home icon and the text 'TRƯỜNG ĐẠI HỌC'. Below it are two menu items: 'Thêm thông tin' (Add information) and 'Xóa thông tin' (Delete information), with the latter being highlighted. On the right, a white modal form titled 'Nhập thông tin để xóa tài khoản' (Enter information to delete account) is displayed. The form contains four input fields: 'Mssv' (Student ID) with placeholder 'Nhập tên mssv muốn xóa', 'Trường' (School) with placeholder 'Nhập tên trường', 'Số hiệu văn bằng' (Degree number) with placeholder 'Nhập số hiệu văn bằng', and 'Password' with placeholder 'Nhập password username' and a toggle icon. A dark 'Xóa tài khoản' button is at the bottom of the form. A 'Đăng xuất' (Logout) button is in the top right corner of the page.

Hình 24. Giao diện Xóa thông tin

3.6.10 Giao diện Tra cứu

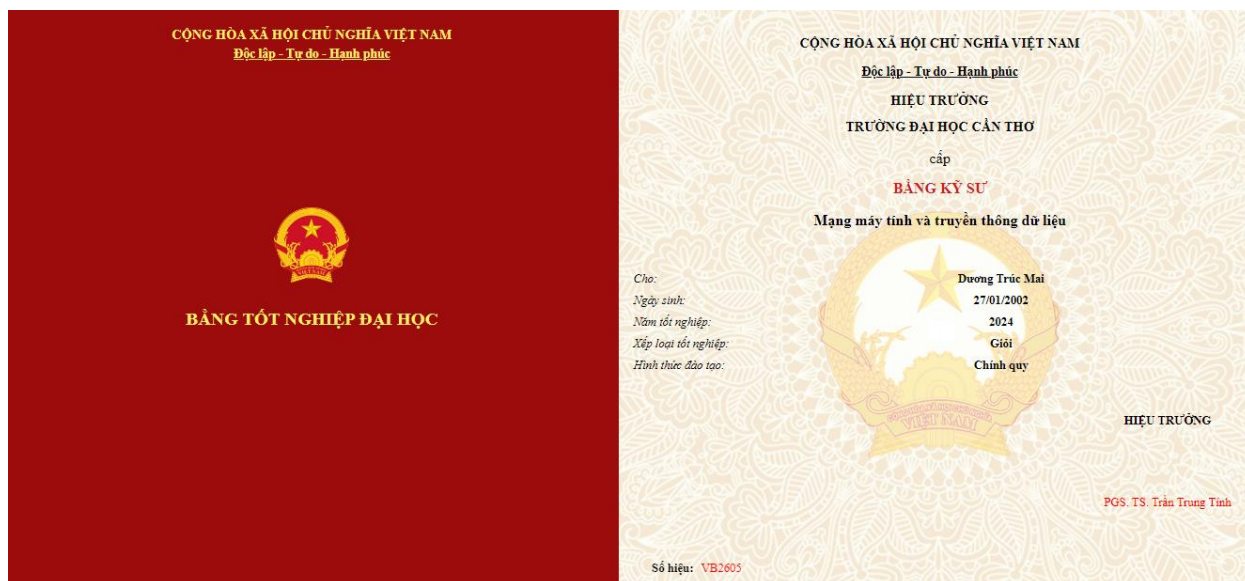
Khi sinh viên có nhu cầu tra bằng tốt nghiệp, sinh viên phải nhập đúng các thông tin mà Trường Đại học đã cung cấp để có thể tra.

The screenshot shows a web interface for a university system. At the top left is a logo and the text 'CHỨNG THỰC'. In the center, a white modal form titled 'Nhập thông tin bạn muốn tra' (Enter information you want to search) is displayed. The form contains three input fields: 'Mã số sinh viên' (Student ID) with placeholder 'Nhập MSSV', 'Trường' (School) with placeholder 'Nhập tên trường', and 'Mật khẩu' (Password) with placeholder 'Tạo mật khẩu cho username'. A dark 'Tra cứu' button is at the bottom of the form. Below the button is a link 'Quay về Trang chủ' (Return to Home page).

Hình 25. Giao diện Tra cứu

3.6.11 Giao diện bằng tốt nghiệp (kết quả tra cứu)

Sau khi tra cứu bằng tốt nghiệp, giao diện bằng tốt nghiệp sẽ được hiển thị.



Hình 26. Giao diện bằng tốt nghiệp

3.6.12 Giao diện Xác thực

Người dùng khi muốn xác thực bằng cấp phải nhập đầy đủ thông tin của bằng tốt nghiệp mà người dùng muốn tra.

CHỨNG THỰC

Nhập thông tin bạn muốn xác thực

Mã số sinh viên

Trường

Mã Văn Bằng

Xác thực

[Quay về Trang chủ](#)

Hình 27. Giao diện Xác thực

3.6.13 Giao diện Kết quả xác thực

- Nếu là Bằng thật: hiển thị thông tin cơ bản của của bằng, nếu muốn xem toàn bộ thông tin bằng cấp thì người dùng bấm vào xem chi tiết.



Hình 28. Giao diện Hiển thị khi kết quả xác thực là Bằng thật

- Trường hợp không có thông tin về bằng đó: Hiển thị giao diện thông báo thông tin vừa nhập là bằng không tồn tại trong hệ thống.



Hình 29. Giao diện Hiển thị kết quả xác thực khi Bằng không tồn tại trong hệ thống

CHƯƠNG 4: KẾT LUẬN - ĐÁNH GIÁ

I. KẾT QUẢ ĐẠT ĐƯỢC

- Về lý thuyết:

Cơ bản nắm được kiến thức về Blockchain và mạng Ethereum cũng như những lợi ích và ứng dụng đã đem lại cho chúng ta.

Sau thời gian nghiên cứu, tìm hiểu các công nghệ, và kiến thức chuyên môn để thực hiện đề tài, thì đã hiểu biết rõ hơn về các quy trình phát triển hệ thống, từ lập kế hoạch đến các bước thiết kế, lập trình và cuối cùng là vận hành một hệ thống. Nâng cao tư duy sáng tạo, khả năng phân tích vấn đề, học hỏi được những công nghệ mới giúp nâng cao kinh nghiệm cho bản thân.

Sử dụng và hiểu được những lợi ích cũng như các ứng dụng về công nghệ Blockchain, mạng Ethereum,... và công cụ hỗ trợ lập trình như Visual Studio Code. Điều đang được sử dụng rộng rãi trong thực tế.

- Về chương trình demo:

Cơ bản hệ thống đã ứng dụng được công nghệ Blockchain và đã được xây dựng tương đối hoàn chỉnh và đáp ứng được các thông tin yêu cầu về chức năng đã đề ra để tạo nên và chứng thực bằng tốt nghiệp. Hệ thống cho phép Admin tạo và quản lý tài khoản cho các Trường Đại học để các Trường Đại học có thể tạo bằng tốt nghiệp, đồng thời giúp cho sinh viên cũng như các nhà tuyển dụng có thể chứng thực bằng cấp một cách dễ dàng.

Xây dựng được một hệ thống đáp ứng nhu cầu chứng thực bằng cấp của người dùng với giao diện đầy đủ chức năng, dễ thao tác.

Ngoài ra hệ thống còn cho phép chứng thực không cần tạo tài khoản, chỉ cần có các thông tin như mã văn bằng để chứng thực, điều này sẽ tạo cảm giác liền mạch khi sử dụng.

II. HẠN CHẾ

Trong quá trình thực hiện đề tài do một số yếu tố khách quan, đề tài vẫn còn một số hạn chế chưa thực hiện được như sau:

Giao diện chưa thực sự thu hút người dùng.

Code chưa tối ưu và clean.

Chưa responsive cho nhiều thiết bị.

Chưa thể đưa vào thực tiễn do vẫn chưa đáp ứng được các yêu cầu để tạo cũng như chứng thực bằng cấp.

III. HƯỚNG PHÁT TRIỂN

Tối ưu thêm nhiều chức năng cho Admin và Trường Đại học.

Phát triển hệ thống với ứng dụng di động.

Responsive giao diện website thân thiện mọi thiết bị.

Tương lai của công nghệ blockchain có thể được sử dụng để ngăn chặn giả mạo, bảo mật dữ liệu và cho phép người dùng xác minh tính xác thực của dữ liệu do bây giờ thách thức đang diễn hiện nay là giả mạo dữ liệu. Vì vậy, an ninh mạng là một trong những lĩnh vực hứa hẹn nhất về tăng trưởng dự kiến cho blockchain.

TÀI LIỆU THAM KHẢO

- [1] **Brooke Becher.** *Blockchain: What It Is, How It Works, Why It Matters.* 2024.
<https://builtin.com/blockchain>

- [2] **THE INVESTOPEDIA TEAM.** *What Are Smart Contracts on the Blockchain and How Do They Work?.* 2024.
<https://www.investopedia.com/terms/s/smart-contracts.asp>

- [3] Solidity — Solidity 0.8.25 documentation, ngày truy cập 16/01/2024.
<https://docs.soliditylang.org/en/v0.8.25/>

- [4] **Nguyễn Thị Hồng Hà.** *Blockchain có thật là giải pháp cho vấn đề về hồ sơ giáo dục điện tử?.* 2023.
<https://caodang.fpt.edu.vn/tin-tuc-poly/blockchain-co-that-la-giai-phap-cho-van-de-ve-ho-so-giao-duc-dien-tu.html>

- [5] **Rahul Awati.** *Consensus Algorithm.* 2022.
<https://www.techtarget.com/whatis/definition/consensus-algorithm>

- [6] **Nguyễn Quỳnh Chi.** *Xây Dựng Mô Hình Ứng Dụng Blockchain Và Chữ Ký Số Trong Quản Lý Văn Bản Và Chứng Chỉ Ở Việt Nam.* Tạp Chí Khoa Học Công Nghệ Thông Tin Và Truyền Thông, 2022.

- [7] **Vatshayan, S.** *Fake-Product-Identification-Using-blockchain: Fake Product Identification by QR Code Using Blockchain Project with Source Code, Documents and YouTube Video Implementation.* 2022
<https://github.com/Vatshayan/Fake-Product-Identification-Using-Blockchain?tab=readme-ov-file>

- [8] **W3Schools .com.** *W3Schools online web tutorials.*2022
<https://www.w3schools.com/>

- [9] *Web3.Js - ethereum JavaScript API — web3.Js 1.0.0 documentation.* 2022
<https://web3js.readthedocs.io/en/v1.8.1/>

- [10] **Johnnybui.** *Smart Contracts là gì? Cơ chế hoạt động của Smart Contract.* 2021.

<https://gfiblockchain.com/smart-contracts-la-gi.html>

[11] **Dr. Liji Thomas, MD.** *Blockchain Applications in Healthcare*. 2021.

<https://www.news-medical.net/health/Blockchain-Applications-in-Healthcare.aspx>

[12] **Bộ nội vụ.** *Bộ Giáo dục và Đào tạo chuẩn bị lưu trữ văn bằng quốc gia trên blockchain*. 2020

<https://moha.gov.vn/tintuc/Pages/lists.aspx?ItemID=44761>