

ĐẠI HỌC BÁCH KHOA HÀ NỘI

ĐỒ ÁN TỐT NGHIỆP

**DEducation - Nền tảng cập nhật và lưu trữ học bạ
dựa trên công nghệ Blockchain**

Đào Xuân An

an.dx190076@sis.hust.edu.vn

Ngành Công nghệ thông tin

Giảng viên hướng dẫn: PGS. TS. Trương Diệu Linh

Chữ kí GVHD

Khoa:

Kỹ thuật máy tính

Trường:

Công nghệ thông tin và Truyền thông

HÀ NỘI, 08/2023

LỜI CẢM ƠN

Trong thời gian làm đồ án tốt nghiệp, em đã nhận được nhiều sự giúp đỡ, đóng góp ý kiến và chỉ bảo nhiệt tình của thầy cô, gia đình và bạn bè.

Em xin gửi lời cảm ơn chân thành đến cô Trương Diệu Linh giảng viên Bộ môn Kỹ thuật máy tính - trường Công nghệ thông tin và truyền thông người đã tận tình hướng dẫn, chỉ bảo em trong suốt quá trình làm đồ án.

Em cũng xin chân thành cảm ơn các thầy cô giáo trong trường Công nghệ thông tin truyền thông - Đại học Bách Khoa Hà Nội nói chung, các thầy cô trong Bộ môn Kỹ thuật máy tính nói riêng đã dạy dỗ cho em kiến thức về các môn đại cương cũng như các môn chuyên ngành, giúp em có được cơ sở lý thuyết vững vàng và tạo điều kiện giúp đỡ em trong suốt quá trình học tập.

Cuối cùng, em xin chân thành cảm ơn gia đình và bạn bè, đã luôn tạo điều kiện, quan tâm, giúp đỡ, động viên em trong suốt quá trình học tập và hoàn thành đồ án tốt nghiệp.

TÓM TẮT NỘI DUNG ĐỒ ÁN

Hệ thống xác nhận dựa trên giấy tờ của ngày nay đã cho thấy một số những thiếu sót, chẳng hạn như văn bằng có thể dễ dàng bị đặt. Vấn đề bằng cấp giả luôn được cảnh báo trên khắp thế giới, thậm chí với sự phát triển của Internet ngày nay, những tài liệu như vậy đang được quảng cáo công khai và khai thác trong lực lượng lao động. Nếu người sử dụng lao động nghi ngờ trình độ của người lao động, họ không thể tự xác minh bằng cấp của người lao động. Điều này chỉ có thể được thực hiện bằng cách yêu cầu cơ quan cấp hồ sơ và thông thường phải mất vài ngày mới có kết quả. Ngoài ra, việc sử dụng chứng thư giấy còn đặt ra trách nhiệm bảo quản cẩn thận cho người cầm chứng.

Trong đồ án này, chúng ta tập trung vào việc tạo ra các tài liệu kỹ thuật số để thay thế các tài liệu giấy thông thường hiện tại nhằm loại bỏ bằng cấp giả và thông tin đăng nhập kỹ thuật số sẽ được cấp bằng cách sử dụng công nghệ Blockchain. Sinh viên sẽ nhận được chứng chỉ kỹ thuật số cho mỗi khóa học họ đã hoàn thành tại trường đại học và bằng tốt nghiệp kỹ thuật số được trao cho sinh viên khi họ hoàn thành chương trình của mình. Các tài liệu kỹ thuật số sẽ được đưa vào chuỗi khối - một nơi an toàn và không thể sửa đổi. Ngoài ra, việc thay thế văn bằng trên giấy bằng phiên bản kỹ thuật số cũng cho phép xác minh liên tục. Điều này sẽ giúp sinh viên và nhà tuyển dụng có thể chứng minh tính xác thực của các giấy tờ mà không cần gặp cán bộ của trường, gây tốn kém thời gian và công sức của cả hai bên. DEducation cung cấp cho chủ sở hữu khả năng sở hữu và chia sẻ tài liệu kỹ thuật số của họ một cách dễ dàng. Ngoài ra, hệ thống cũng cho phép sinh viên quyết định cách họ muốn chia sẻ bảng điểm học tập của mình với nhà tuyển dụng. Bảng điểm bao gồm thông tin về các khóa học đã hoàn thành của sinh viên với chứng chỉ kỹ thuật số đính kèm và cả bằng đại học kỹ thuật số của họ.

Sinh viên thực hiện
(Ký và ghi rõ họ tên)

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI.....	1
1.1 Đặt vấn đề.....	1
1.2 Mục tiêu và phạm vi đề tài.....	1
1.3 Định hướng giải pháp.....	2
1.4 Bố cục đồ án	3
CHƯƠNG 2. KHẢO SÁT VÀ PHÂN TÍCH YÊU CẦU.....	4
2.1 Khảo sát hiện trạng	4
2.2 Tổng quan chức năng	4
2.2.1 Biểu đồ ca sử dụng tổng quát	4
2.2.2 Biểu đồ ca sử dụng phân rã "Quản lý điểm theo lớp dạy"	6
2.2.3 Biểu đồ ca sử dụng phân rã "Quản lý bằng tốt nghiệp"	7
2.2.4 Biểu đồ ca sử dụng phân rã "Xem danh sách ứng viên"	8
2.2.5 Tổng quan về kiến trúc hệ thống	9
2.2.6 Quy trình nghiệp vụ	10
2.3 Đặc tả chức năng	11
2.3.1 Đặc tả ca sử dụng "Cập nhật bằng tốt nghiệp"	11
2.3.2 Đặc tả ca sử dụng "Xem bằng tốt nghiệp"	12
2.3.3 Đặc tả ca sử dụng "Cập nhật bằng điểm môn học"	13
2.3.4 Đặc tả ca sử dụng "Quản lý trạng thái công khai bằng điểm"	14
2.3.5 Đặc tả ca sử dụng "Xem danh sách sinh viên"	14
CHƯƠNG 3. NỀN TẢNG LÝ THUYẾT	16
3.1 Mật mã học	16
3.1.1 Mật mã bất đối xứng	16
3.1.2 Chữ kí điện tử	16

3.1.3 Hàm băm	18
3.2 Tổng quan về Blockchain.....	18
3.2.1 Công nghệ chuỗi khối là gì?.....	18
3.2.2 Công nghệ chuỗi khối có những đặc điểm gì?	19
3.2.3 Các thành phần chính của công nghệ chuỗi khối	19
3.2.4 Chuỗi khối hoạt động như thế nào?.....	20
3.3 Nền tảng Ethereum	21
3.3.1 Ví, khóa và địa chỉ	21
3.3.2 Giao dịch	21
3.3.3 Sự đồng thuận.....	22
3.3.4 Gasless Meta-Transactions	24
3.4 Nền tảng IPFS	24
3.4.1 IPFS cho tương lai.....	24
3.4.2 Cách IPFS hoạt động.....	25
CHƯƠNG 4. THỰC NGHIỆM VÀ ĐÁNH GIÁ	27
4.1 Thiết kế kiến trúc.....	27
4.1.1 Lựa chọn kiến trúc phần mềm	27
4.1.2 Thiết kế tổng quan.....	28
4.1.3 Thiết kế chi tiết gói	29
4.2 Thiết kế chi tiết.....	29
4.2.1 Thiết kế giao diện	29
4.2.2 Biểu đồ tuần tự mức nghiệp vụ	32
4.2.3 Thiết kế cơ sở dữ liệu	33
4.3 Xây dựng ứng dụng.....	37
4.3.1 Thư viện và công cụ sử dụng	37
4.3.2 Kết quả đạt được	39

4.3.3 Minh họa các chức năng chính	39
4.4 Kiểm thử.....	42
4.4.1 Kiểm thử API cập nhật	42
4.4.2 Kiểm thử tạo file PDF	43
4.4.3 Kiểm thử tương tác với Ethereum	43
4.4.4 Kiểm thử tính đúng đắn của đồ án	45
4.5 Triển khai	46
CHƯƠNG 5. CÁC GIẢI PHÁP VÀ ĐÓNG GÓP NỔI BẬT.....	47
5.1 Giảm thiểu tính khó tiếp cận cho người dùng khi sử dụng Ethereum trong hệ thống	47
5.1.1 Đặt vấn đề	47
5.1.2 Giải pháp	47
5.1.3 Hiệu quả	49
5.2 Giữ toàn vẹn tính bất biến với IPFS	50
5.2.1 Đặt vấn đề	50
5.2.2 Giải pháp	50
5.2.3 Hiệu quả	52
CHƯƠNG 6. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN	53
6.1 Kết luận.....	53
6.2 Hướng phát triển.....	53
6.3 Lời kết.....	53
TÀI LIỆU THAM KHẢO.....	54

DANH MỤC HÌNH VẼ

Hình 2.1	Sơ đồ ca sử dụng tổng quát	5
Hình 2.2	Ca sử dụng "Quản lý điểm theo lớp dạy"	6
Hình 2.3	Ca sử dụng "Quản lý bằng tốt nghiệp"	7
Hình 2.4	Ca sử dụng "Xem danh sách ứng viên"	8
Hình 2.5	Kiến trúc tổng quan	9
Hình 2.6	Quy trình nghiệp vụ "Xem kết quả học tập ứng viên"	10
Hình 2.7	Quy trình nghiệp vụ "Cập nhật bảng điểm theo lớp dạy"	11
Hình 4.1	Kiến trúc phần mềm tổng quan	27
Hình 4.2	Biểu đồ phụ thuộc gói	28
Hình 4.3	Thiết kế trang hiển thị thông tin cá nhân	29
Hình 4.4	Thiết kế cập nhật tài liệu số	29
Hình 4.5	Trang đăng nhập	30
Hình 4.6	Trang thông tin cá nhân sinh viên	31
Hình 4.7	Trang danh sách lớp	31
Hình 4.8	Trang danh sách trường	32
Hình 4.9	Trang danh sách học sinh	32
Hình 4.10	Biểu đồ tuần tự "Cập nhật bằng tốt nghiệp"	33
Hình 4.11	Biểu đồ tuần tự "Xác thực bằng tốt nghiệp"	33
Hình 4.12	Sơ đồ cơ sở dữ liệu	34
Hình 4.13	Màn hình đăng nhập	39
Hình 4.14	Xem bằng tốt nghiệp	40
Hình 4.15	Màn hình giao dịch on-chain	40
Hình 4.16	Màn hình danh sách lớp	41
Hình 4.17	Màn hình xem điểm	41
Hình 4.18	Màn hình danh sách sinh viên	42
Hình 4.19	Tài liệu không hợp lệ	45
Hình 4.20	Tài liệu hợp lệ	45
Hình 5.1	Gasless Station Network	47
Hình 5.2	Giao diện kí giao dịch của Metamask	48
Hình 5.3	Giao diện ghi lại giao dịch trên Metamask	49
Hình 5.4	Giao diện kết quả giao dịch trên Sepolia Etherscan	49
Hình 5.5	Cây Merkle [11]	50
Hình 5.6	Cây Multihash thực tế trong IPFS	51
Hình 5.7	Các "Peer" khi tham gia IPFS	52

DANH MỤC BẢNG BIỂU

Bảng 2.1	Đặc tả ca sử dụng "Cập nhật bằng tốt nghiệp"	12
Bảng 2.2	Đặc tả ca sử dụng "Xem bằng tốt nghiệp"	13
Bảng 2.3	Đặc tả ca sử dụng "Cập nhật bảng điểm môn học"	13
Bảng 2.4	Đặc tả ca sử dụng "Quản lý trạng thái công khai bảng điểm" .	14
Bảng 2.5	Đặc tả ca sử dụng "Xem danh sách sinh viên"	15
Bảng 4.1	Chi tiết bảng "User"	34
Bảng 4.2	Chi tiết bảng "AcademyTranscript"	35
Bảng 4.3	Chi tiết bảng "Diploma"	35
Bảng 4.4	Chi tiết bảng "Permission"	35
Bảng 4.5	Chi tiết bảng "School"	36
Bảng 4.6	Chi tiết bảng "StudentClass"	36
Bảng 4.7	Chi tiết bảng "PermissionRelationship"	36
Bảng 4.8	Chi tiết bảng "Role"	37
Bảng 4.9	Chi tiết bảng "Class"	37
Bảng 4.10	Chi tiết bảng "Semester"	37
Bảng 4.11	Chi tiết bảng "StudentSemester"	37
Bảng 4.12	Thư viện và công cụ sử dụng	38
Bảng 4.13	Kết quả đạt được	39
Bảng 4.14	Danh sách trường hợp kiểm thử cập nhật trạng thái công khai .	42
Bảng 4.15	Danh sách trường hợp kiểm thử cập nhật danh sách	43
Bảng 4.16	Danh sách trường hợp kiểm thử tạo bằng tốt nghiệp pdf	43
Bảng 4.17	Danh sách trường hợp kiểm thử tạo bằng bảng điểm pdf	43
Bảng 4.18	Danh sách trường hợp kiểm thử giao dịch cập nhật học bạ . .	44
Bảng 4.19	Danh sách trường hợp kiểm thử xác thực tài liệu số	44
Bảng 4.20	Danh sách trường hợp kiểm thử thời gian xác thực tài liệu số .	46

DANH MỤC THUẬT NGỮ VÀ TỪ VIẾT TẮT

Thuật ngữ	Ý nghĩa
API	Giao diện lập trình ứng dụng (Application Programming Interface)
CID	Xác định nội dung (Content Identifier)
DNS	Hệ thống phân giải tên miền (Domain name system)
HTTP	Giao thức Truyền tải Siêu Văn Bản (Hypertext Transfer Protocol)
IPFS	Mạng ngang hàng chia sẻ tệp để lưu trữ và chia sẻ dữ liệu trong một hệ thống tệp phân tán (InterPlanetary File System)
IPNS	InterPlanetary Name System

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI

1.1 Đặt vấn đề

Trong những năm gần đây, bằng giả, bằng cấp nổi lên như một vấn đề nhức nhối không duy nhất tại Việt Nam, những nội dung như vậy được quảng cáo và bán công khai trên Internet. Cả nước gần đây thôi đã rung động với thông tin một giám đốc trung tâm đăng kiểm lại không hề biết chữ [1]. Hay như một cựu bí thư Thành phố Đà Nẵng nhận bằng tiến sĩ "siêu tốc" của Trường Southern California University for Professional Studies (SCUPS) [2]. Với những bằng cấp giả này được lưu hành trên thị trường, nhà tuyển dụng không có cách nào để truy tìm lại tính xác thực của bằng cấp của nhân viên của họ ngoài để liên hệ với tổ chức phát hành. Tuy nhiên, có những trường hợp thậm chí công ty phát hành đã làm giả những tài liệu này với bàn tay của ban giám đốc trường đại học [3]. Chúng ta cần 1 hệ thống đồng bộ có khả năng tạo ra và lưu trữ những tấm bằng đại học, đồng thời những tấm bằng được tạo ra phải không thể chỉnh sửa.

Mặt khác, hệ thống quản lý sinh viên và chứng chỉ hiện tại ở hầu hết các trường đại học và học viện ở Việt Nam vẫn còn khá phức tạp, và nó gây phiền toái cho sinh viên khi họ phải giải quyết tất cả các thủ tục giấy. Ví dụ, khi một sinh viên mới tốt nghiệp trường Đại học Bách Khoa Hà Nội liên kết với một tổ chức giáo dục đại học ở nước ngoài, anh ta phải có được một bảng điểm học tập in từ trường Đại học Bách Khoa, in và gửi nó đến hội đồng tuyển sinh của tổ chức nước ngoài. Quá trình này bao gồm rất nhiều thủ công làm việc từ cả sinh viên và nhân viên của trường đại học, và thông thường anh ta có thể mất 3-5 ngày để có bảng điểm của mình trong tay. Rất nhiều sinh viên đang tìm kiếm việc làm sau khi tốt nghiệp và bộ phận tuyển dụng của các công ty sẽ muốn đánh giá kết quả học tập của họ như là một phần của quá trình tuyển dụng để chọn ứng cử viên tốt nhất cho họ. Sau đó, họ phải yêu cầu người nộp đơn cho thấy bằng cấp và bảng điểm từ thời đại học. Chúng ta cần 1 hệ thống có thể xác minh tài liệu chỉ bằng vài thao tác chuột đơn giản, qua đó tiết kiệm thời gian và nguồn nhân lực.

1.2 Mục tiêu và phạm vi đề tài

Từ năm học 2020 – 2021, Bộ Giáo dục và Đào tạo quyết định ứng dụng công nghệ trong việc lưu trữ văn bằng quốc gia. Theo đó, tất cả văn bằng được cấp bởi các đơn vị đào tạo thuộc Bộ Giáo dục và Đào tạo sẽ lần lượt được đưa vào hệ thống lưu trữ văn bằng quốc gia. Hệ thống truy xuất cho các bên có nhu cầu cũng sẽ được xã hội hoá [4]. Để đảm bảo tính an toàn dữ liệu, hệ thống này ứng dụng những công nghệ tiên tiến nhất, trong đó, nền tảng blockchain được triển khai bởi nhà phát triển