ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA TOÁN – CƠ – TIN HỌC

Nguyễn Ngọc Dũng

BLOCKCHAIN VÀ ỨNG DỤNG TRONG XÁC THỰC THÔNG TIN

Khóa luận tốt nghiệp đại học hệ chính quy
Ngành Toán tin
(Chương trình đào tạo chuẩn)

Hà Nội - 2025

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA TOÁN – CƠ – TIN HỌC

Nguyễn Ngọc Dũng

BLOCKCHAIN VÀ ỨNG DỤNG TRONG XÁC THỰC THÔNG TIN

Khóa luận tốt nghiệp đại học hệ chính quy
Ngành Toán tin
(Chương trình đào tạo chuẩn)

Cán bộ hướng dẫn: PGS.TS. Phó Đức Tài

Hà Nội - 2025

LỜI CẢM ƠN

Trước khi trình bày nội dung chính của khóa luận, em xin bày tỏ lòng biết ơn sâu sắc tới PGS.TS. Phó Đức Tài, người đã tận tình hướng dẫn để em có thể hoàn thành khóa luận này. Em cũng xin bày tỏ lòng biết ơn chân thành tới toàn thể các thầy cô giáo trong khoa Toán - Cơ - Tin học, Đại học Khoa Học Tự Nhiên, Đại Học Quốc Gia Hà Nội đã dạy bảo em tận tình trong suốt quá trình học tập tại khoa. Nhân dịp này em cũng xin được gửi lời cảm ơn chân thành tới gia đình, bạn bè đã luôn bên em, cổ vũ, động viên, giúp đỡ em trong suốt quá trình học tập và thực hiện khóa luận tốt nghiệp.

Hà Nội, ngày 20 tháng 5 năm 2025

Sinh viên

Dũng

Nguyễn Ngọc Dũng

BẢNG KÝ HIỆU, CHỮ VIẾT TẮT

a rightrotate b là phép xoay bit sang phải, sẽ đưa các bit bị đẩy ra ngoài trở lại đầu.

a rightshift b là phép dịch bit sang phải, đẩy các bit ra ngoài và thay bằng số 0 ở đầu.

Blockchain: Chuỗi khối.

Block Header: Tiêu đề khối.

ECC (Elliptic Curve Cryptography): Hệ mật mã đường cong elliptic.

ECDSA (Elliptic Curve Digital Signature Algorithm): Thuật toán chữ ký số đường cong Elliptic.

gcd(a,b) – Ước chung lớn nhất của a và b.

h: $\{0,1\}^* \rightarrow \{0,1\}^n$: là hàm h nhận đầu vào là chuỗi nhị phân có độ dài bất kỳ, và trả về chuỗi nhị phân độ dài n.

IPFS (InterPlanetary File System): Hệ thống tệp liên hành tinh.

Merkle Root: Nút gốc của một cây Merkle.

PoW (Proof of Work): Bằng chứng công việc.

PoS (Proof of Stake): Bằng chứng cổ phần.

xor: Phép loại trừ 2 xâu bit.

MỤC LỤC

DANH MỤC HÌNH VẼ

MỞ ĐẦU

Trong thời đại số hóa hiện nay, việc xác thực thông tin đang trở thành một vấn đề mang tính cấp thiết và đóng vai trò then chốt trong nhiều lĩnh vực như giáo dục, y tế, tài chính, quản lý công dân, và đặc biệt là quản lý văn bằng, chứng chỉ. Tuy nhiên, hệ thống xác thực thông tin truyền thống vẫn còn tồn tại nhiều bất cập như: phụ thuộc vào bên trung gian, nguy cơ làm giả tài liệu, quy trình xác minh phức tạp và tốn thời gian. Những hạn chế này không chỉ làm giảm hiệu quả trong công tác quản lý mà còn ảnh hưởng đến tính minh bạch và độ tin cậy của dữ liệu.

Trong bối cảnh đó, công nghệ blockchain đã và đang nổi lên như một giải pháp đầy tiềm năng giúp giải quyết bài toán xác thực thông tin một cách minh bạch, an toàn và không thể thay đổi. Với đặc điểm phi tập trung, minh bạch, và bất biến, blockchain mở ra hướng đi mới trong việc xây dựng các hệ thống xác thực đáng tin cậy, không cần đến sự can thiệp của bên thứ ba.

Việc ứng dụng công nghệ blockchain vào xác thực thông tin, đặc biệt trong xác minh văn bằng, chứng chỉ, có thể giúp loại bỏ gian lận, rút ngắn thời gian xác thực và tăng cường niềm tin giữa các bên liên quan. Đây chính là động lực thúc đẩy em lựa chọn đề tài: "*Blockchain và ứng dụng trong xác thực thông tin*" làm chủ đề cho khóa luận tốt nghiệp. Mục tiêu của đề tài là nghiên cứu và ứng dụng công nghệ blockchain vào quá trình xác thực thông tin, cụ thể là xác thực văn bằng, chứng chỉ. Thông qua việc triển khai một mô hình thử nghiệm, đề tài hướng tới:

- Hiểu rõ nguyên lý hoạt động và các đặc điểm nổi bật của blockchain.
- Khảo sát thực trạng và các giải pháp hiện tại trong xác thực thông tin.
- Xây dựng ứng dụng cho phép tương tác giữa trường học và người dùng trong quá trình cấp phát và xác minh bằng cấp sử dụng công nghệ blockchain.

CHƯƠNG 1

GIỚI THIỆU VỀ BLOCKCHAIN

1.1 Thực trạng và các giải pháp hiện tại trong xác thực thông tin

Trong nhiều năm qua, việc xác thực thông tin, đặc biệt là bằng cấp và chứng chỉ, chủ yếu được thực hiện thông qua hình thức bằng giấy truyền thống. Mỗi khi cần xác minh, người dùng buộc phải cung cấp bản sao hoặc bản gốc của chứng chỉ, và bên xác thực phải liên hệ với cơ sở cấp bằng để kiểm tra. Cách làm này tồn tại nhiều bất cập:

- Dễ bị thất lạc hoặc hư hỏng: Bằng giấy là dạng vật lý, rất dễ bị rách, mờ chữ, hoặc mất do thiên tai, hỏa hoạn hay sơ suất cá nhân. Khi bị thất lạc, việc cấp lại thường mất nhiều thời gian và quy trình phức tạp, đặc biệt nếu đơn vị cấp bằng đã thay đổi cơ cấu tổ chức hoặc ngừng hoạt động.
- Khó xác minh nguồn gốc: Khi muốn xác minh, các đơn vị tiếp nhận phải liên hệ trực tiếp với nơi cấp chứng chỉ. Việc này không chỉ mất thời gian mà còn dễ gặp khó khăn nếu cơ sở dữ liệu không đồng bộ hoặc không còn lưu giữ bản ghi rõ ràng. Các quy trình xác minh thường thủ công, dẫn đến độ trễ và nguy cơ sai sót cao.
- Có thể bị làm giả: Công nghệ in ấn ngày càng tinh vi khiến cho việc làm giả bằng cấp trở nên phổ biến. Nhiều tổ chức, cá nhân sử dụng bằng cấp giả để gian lận trong học thuật hoặc tuyển dụng, gây ảnh hưởng nghiêm trọng đến chất lượng nguồn nhân lực và uy tín của các tổ chức giáo dục.
- Không có tính minh bạch và toàn vẹn dữ liệu: Một chứng chỉ được in ra không có cơ chế để kiểm tra xem nội dung đã bị chỉnh sửa hay chưa. Điều này khiến việc phát hiện gian lận hoặc sai lệch trở nên khó khăn, đồng thời gây ra sự thiếu tin tưởng trong quá trình xác minh giữa các bên liên quan.

Khi quá trình chuyển đổi số diễn ra mạnh mẽ, nhiều đơn vị đã tiến hành số hóa bằng cấp nhằm khắc phục những nhược điểm nêu trên bằng một số giải pháp công nghệ như:

- Hệ thống quản lý tập trung (cơ sở dữ liệu tập trung): Các trường đại học, tổ chức nghề nghiệp xây dựng hệ thống cơ sở dữ liệu riêng để lưu trữ và kiểm tra chứng chỉ.
- Mã QR trên chứng chỉ: Một số đơn vị in mã QR để liên kết đến hồ sơ chứng chỉ trên website, tuy nhiên tính bảo mật không cao nếu hệ thống bị can thiệp.
- Chữ ký số và chứng thực điện tử: Các tổ chức sử dụng chữ ký số do cơ quan chứng thực cấp, đảm bảo tính hợp lệ của văn bản điện tử.
- Dịch vụ trung gian xác thực: Một số đơn vị cung cấp dịch vụ xác minh trung gian, đóng vai trò cầu nối giữa người xác minh và tổ chức cấp phát.

Tuy nhiên, việc số hóa cũng đặt ra nhiều thách thức:

- Đòi hỏi hệ thống định danh và quy trình xác thực đồng bộ, bảo mật cao: Các cơ quan cần xây dựng cơ sở hạ tầng công nghệ và chính sách quản lý định danh điện tử chặt chẽ. Quy trình xác thực phải được thống nhất, đáng tin cậy và có thể mở rộng khi tích hợp liên ngành hoặc liên tổ chức.
- Nguy cơ rò rỉ dữ liệu cá nhân, mất mát dữ liệu do lỗ hổng bảo mật hoặc hệ thống chưa hoàn thiện: Nhiều tổ chức chưa có đủ nguồn lực để đảm bảo an toàn thông tin, dẫn đến nguy cơ các dữ liệu nhạy cảm bị lộ lọt, bị tấn công hoặc bị xóa nhầm.
- Khả năng giả mạo vẫn tồn tại nếu thuật toán mã hóa hoặc quá trình xác thực còn lỏng lẻo: Nếu chỉ áp dụng các phương pháp mã hóa đơn giản, thiếu kiểm tra chéo hoặc thiếu nhật ký giao dịch rõ ràng, dữ liệu vẫn có thể bị sửa đổi hoặc bị đánh cắp mà không bị phát hiện.

Do đó, việc tìm kiếm một giải pháp mới trong lĩnh vực xác thực thông tin là điều cần thiết trong xã hội mà số hóa đang là tiên phong như hiện nay. Blockchain nổi lên như là một trong những giải pháp đầy tiềm năng để cải tiến quy trình xác thực thông tin, đặc biệt là trong thời đại chuyển đổi số với những đặc tính vượt trội như:

- Dữ liệu không thể bị thay đổi hoặc xóa bỏ: Một khi thông tin đã được ghi vào blockchain, gần như không thể chỉnh sửa hoặc xóa mà không để lại dấu vết. Điều này đảm bảo tính toàn vẹn và lâu dài cho dữ liệu chứng chỉ.
- Mọi hành động đều được ghi lại một cách minh bạch: Mỗi thao tác ghi dữ liệu, xác thực hay cập nhật đều được ghi nhận công khai trong chuỗi khối, tạo ra một hệ thống minh bạch và có thể kiểm tra lại bất cứ lúc nào.

- Có thể xác thực nguồn gốc thông tin dễ dàng và nhanh chóng: Thông qua mã hash và địa chỉ ví lưu trữ, các tổ chức và cá nhân có thể kiểm chứng tức thì thông tin bằng cấp mà không cần phải liên hệ với đơn vị cấp.

Thực tế hiện nay, nhiều trường đại học và tổ chức giáo dục tại Việt Nam đã tiên phong trong việc áp dụng công nghệ blockchain vào quy trình xác thực và cấp phát văn bằng, chứng chỉ. Một ví dụ điển hình là Đại học Hoa Sen, đơn vị đầu tiên tại Việt Nam triển khai hệ thống xác thực bằng tốt nghiệp thông qua blockchain từ năm 2021. Khi sinh viên tốt nghiệp, thông tin về bằng cấp sẽ được mã hóa, gắn mã hash và lưu trữ trên nền tảng blockchain. Nhà tuyển dụng hoặc bất kỳ bên liên quan nào chỉ cần truy cập vào hệ thống công khai để xác minh tính xác thực của bằng chỉ với vài thao tác đơn giản, không cần giấy tờ bản cứng hay phải liên hệ trực tiếp với trường. Việc ứng dụng blockchain không chỉ giúp trường tiết kiệm quản lý văn bằng, mà còn nâng cao uy tín trong việc chống gian lận học thuật. Mô hình này đã và đang được xem xét nhân rộng trong nhiều trường đại học khác như Đại học Quốc gia TP.HCM, Đại học FPT, cũng như các tổ chức quốc tế có nhu cầu xác minh bằng cấp của sinh viên Việt Nam một cách nhanh chóng và minh bạch. Từ thực tiễn đó có thể thấy, xu hướng số hóa và xác thực thông tin bằng blockchain không còn là lý thuyết mà đã bước vào giai đoạn triển khai thực tế, góp phần hiện đại hóa hoạt động giáo dục và tuyển dụng. Do vậy, việc xây dựng và đánh giá một hệ thống xác thực văn bằng dựa trên blockchain không chỉ mang tính nghiên cứu học thuật mà còn có khả năng ứng dụng cao, đặc biệt trong bối cảnh nhu cầu minh bạch hóa thông tin cá nhân ngày càng được quan tâm.

1.2 Tổng quan về blockchain

1.2.1 Giới thiệu chung về blockchain

Blockchain là một công nghệ lưu trữ và truyền tải dữ liệu theo hình thức chuỗi khối, trong đó các khối dữ liệu được liên kết với nhau bằng các thuật toán mã hóa, đảm bảo rằng dữ liệu một khi đã được ghi nhận thì không thể thay đổi hoặc xóa bỏ. Công nghệ này hoạt động theo nguyên tắc phi tập trung, tức là không có một máy chủ trung tâm điều phối mà toàn bộ các nút trong hệ thống đều có quyền ngang nhau và cùng tham gia xác thực giao dịch.

Hình 1-1 Giới thiệu về blockchain

Từ khi công nghệ blockchain ra đời cùng với đồng tiền kỹ thuật số Bitcoin vào năm 2008, công nghệ này đã nhanh chóng thu hút sự quan tâm từ nhiều lĩnh vực. Không chỉ dừng lại ở tài chính và tiền mã hóa, blockchain ngày nay đã được nghiên cứu và áp dụng trong nhiều lĩnh vực, tiêu biểu như:

- Lĩnh vực y tế: Blockchain được ứng dụng để quản lý hồ sơ bệnh án điện tử một cách an toàn và đáng tin cậy. Mỗi bệnh án khi được ghi lại sẽ không thể bị chỉnh sửa hoặc xóa bỏ, đảm bảo toàn vẹn dữ liệu y tế trong suốt quá trình điều trị. Ngoài ra, bệnh nhân có thể kiểm soát quyền truy cập vào hồ sơ cá nhân, từ đó nâng cao tính riêng tư và bảo mật trong ngành y.
- Lĩnh vực logistics và chuỗi cung ứng: Nhờ khả năng ghi nhận dữ liệu không thể thay đổi và truy xuất theo thời gian thực, blockchain cho phép các doanh nghiệp theo dõi chính xác hành trình của hàng hóa từ nơi sản xuất đến tay người tiêu dùng. Điều này giúp nâng cao hiệu quả quản lý chuỗi cung ứng, giảm thiểu gian lận, hàng giả, đồng thời tăng tính minh bạch trong thương mại toàn cầu.
- Lĩnh vực giáo dục: Công nghệ blockchain được sử dụng để lưu trữ và xác thực văn bằng, chứng chỉ học thuật nhằm chống lại tình trạng làm giả giấy tờ. Khi bằng cấp được ghi nhận trên blockchain, bất kỳ tổ chức hoặc nhà tuyển dụng nào cũng có thể dễ dàng kiểm tra độ xác thực thông qua mã băm và thông tin liên kết, mà không cần liên hệ trực tiếp với cơ sở đào tạo.
- Chính phủ điện tử: Nhiều quốc gia đang nghiên cứu và triển khai các hệ thống bỏ phiếu điện tử dựa trên blockchain, với mục tiêu tăng cường tính

minh bạch, bảo mật và chống gian lận bầu cử. Nhờ vào cơ chế đồng thuận và ghi nhận không thể chỉnh sửa, các lá phiếu được đảm bảo không bị thay đổi hoặc làm sai lệch trong suốt quá trình bầu cử.

- Xác thực thông tin: Một trong những ứng dụng tiềm năng của blockchain là giúp xác thực tính chính xác và nguồn gốc của các dữ liệu quan trọng như giấy tờ pháp lý, hồ sơ công dân, hợp đồng điện tử, hoặc bằng cấp. Thông qua mã hóa và lưu trữ phân tán, blockchain giúp loại bỏ nguy cơ làm giả, chỉnh sửa trái phép, đồng thời tạo niềm tin giữa các bên liên quan khi trao đổi thông tin.

Sự phổ biến và tính ứng dụng rộng rãi của công nghệ blockchain đã mở ra nhiều cơ hội mới trong lĩnh vực nghiên cứu và phát triển công nghệ thông tin. Từ một sáng kiến ban đầu phục vụ cho hệ thống tiền mã hóa Bitcoin, blockchain đã nhanh chóng chứng minh được giá trị cốt lõi của mình và trở thành một trong những công nghệ nền tảng quan trọng trong kỷ nguyên số. Đặc biệt, việc ứng dụng blockchain vào xác thực thông tin đang nổi lên như một xu hướng đầy tiềm năng, không chỉ giúp nâng cao hiệu quả quản lý dữ liệu mà còn mang lại giá trị thực tiễn cao trong nhiều lĩnh vực như giáo dục, hành chính, tài chính và y tế. Những đặc tính kỹ thuật nổi bật đã làm nên sức mạnh của blockchain, có thể kể đến như:

- Tính minh bạch: Mọi giao dịch và thao tác dữ liệu trên blockchain đều được ghi nhận công khai vào một sổ cái phân tán, cho phép tất cả các bên liên quan đều có thể truy cập và kiểm chứng. Điều này giúp nâng cao độ tin cậy và hạn chế tối đa nguy cơ thao túng dữ liệu hoặc gian lận.
- Tính bất biến: Một khi thông tin đã được ghi vào blockchain thì gần như không thể bị thay đổi hoặc xóa bỏ. Các khối dữ liệu mới được gắn kết với khối trước đó thông qua mã băm, tạo thành một chuỗi liên tục. Việc thay đổi bất kỳ thông tin nào trong một khối sẽ làm thay đổi toàn bộ chuỗi sau đó, điều này đòi hỏi một khối lượng tính toán khổng lồ và là điều gần như bất khả thi trong thực tế.
- Tính phi tập trung: Blockchain không chịu sự kiểm soát của bất kỳ tổ chức hay cá nhân đơn lẻ nào. Thay vào đó, mạng lưới được duy trì bởi nhiều nút mạng phân tán, mỗi nút đều lưu giữ một bản sao đầy đủ của sổ cái. Điều này không chỉ giúp loại bỏ điểm yếu về rủi ro tập trung mà còn gia tăng tính minh bạch và khả năng chống giả mạo trong toàn bộ hệ thống.

- Tính bảo mật cao: Thông tin trong blockchain được mã hóa bằng các thuật toán mật mã hiện đại như SHA-256, đồng thời mọi thay đổi hoặc bổ sung dữ liệu đều cần đạt được sự đồng thuận của phần lớn các nút trong mạng lưới thông qua các cơ chế như Proof of Work (PoW), Proof of Stake (PoS), hoặc các thuật toán đồng thuận khác. Nhờ vậy, blockchain có khả năng chống lại các cuộc tấn công độc hại từ bên ngoài và đảm bảo tính toàn vẹn, bảo mật cho dữ liệu.

Nhờ những đặc tính trên, blockchain không chỉ đáp ứng các yêu cầu kỹ thuật khắt khe trong quản lý dữ liệu mà còn phù hợp với các mục tiêu chiến lược về minh bạch hóa, số hóa và bảo vệ thông tin trong thời đại công nghệ 4.0. Do đó, việc triển khai công nghệ này vào xác thực thông tin, đặc biệt là thông tin có tính pháp lý hoặc học thuật như văn bằng, chứng chỉ, hợp đồng hứa hẹn sẽ tạo nên những bước tiến quan trọng trong quá trình chuyển đổi số toàn diện. Với những đặc điểm trên, blockchain không chỉ được ứng dụng trong lĩnh vực tiền mã hóa mà còn đang dần thâm nhập vào nhiều lĩnh vực khác, đặc biệt là trong việc xây dựng các hệ thống xác thực đáng tin cậy, giúp tiết kiệm chi phí và thời gian.
Một số loại blockchain có thể kể tới như:

- Public Blockchain: Bất kỳ ai cũng có thể tham gia xác thực và xem dữ liệu (ví dụ: Bitcoin, Ethereum,..).
- Private Blockchain: Chỉ những tổ chức được cấp quyền mới có thể truy cập và vận hành.
- Consortium Blockchain: Một nhóm tổ chức cùng vận hành và kiểm soát mạng lưới blockchain.

Một khối điển hình trong blockchain bao gồm các thành phần:

- Block Header: Chứa thông tin như mã băm của block trước, thời gian tạo, nonce, và root của cây Merkle.
- Transaction List: Danh sách các giao dịch đã được xác thực và đưa vào khối.
- Hash: Giá trị mã hóa đại diện cho toàn bộ nội dung của khối, dùng để kiểm tra tính toàn vẹn.

Nhắc tới blockchain thì không thể không nói tới các giao thức đồng thuận trong blockchain. Giao thức đồng thuận là cơ chế giúp các nút trong mạng blockchain thống nhất về trạng thái hiện tại của sổ cái. Hiện nay có 2 cơ chế phổ biến nhất là:

- Proof of Work (PoW): Các nút cạnh tranh giải bài toán mật mã để xác thực giao dịch và tạo block mới. Được dùng trong Bitcoin.
- Proof of Stake (PoS): Các nút được chọn xác thực giao dịch dựa trên lượng coin nắm giữ.

Tùy vào mục tiêu của hệ thống xác thực, có thể sử dụng các nền tảng hỗ trợ PoW hoặc PoS nhằm tiết kiệm năng lượng và tối ưu hiệu suất. Hiện nay, có rất nhiều nền tảng blockchain khác nhau nhưng phổ biến có thể kể tới như:

- Ethereum: Hỗ trợ smart contract và là nền tảng phổ biến nhất cho các ứng dụng phi tập trung (dApp).
- Hyperledger Fabric: Hướng đến doanh nghiệp, hỗ trợ blockchain permissioned (có quyền kiểm soát).
- Polygon (MATIC): Nền tảng mở rộng Ethereum, có phí giao dịch thấp và tốc độ cao.
- BNB Chain: Hỗ trợ smart contract và có hệ sinh thái lớn, phí giao dịch thấp.

Trong đề tài này, Ethereum sẽ được sử dụng hợp đồng thông minh kết hợp với IPFS để xây dựng hệ thống xác thực thông tin.

1.2.2 Hợp đồng thông minh

Hợp đồng thông minh là một thành phần then chốt trong hệ sinh thái của các nền tảng blockchain hiện đại, tiêu biểu là Ethereum. Về bản chất, hợp đồng thông minh là một đoạn mã được lập trình sẵn và được triển khai trên blockchain để tự động thực hiện các điều khoản, hành động hoặc quy trình nhất định khi các điều kiện đầu vào được đáp ứng. Điều này giúp loại bỏ sự phụ thuộc vào các bên trung gian truyền thống như luật sư, công chứng viên hoặc tổ chức trung gian thứ ba, từ đó không chỉ giảm chi phí giao dịch mà còn nâng cao hiệu suất, tốc độ và tính minh bạch trong quá trình thực thi. Khác với hợp đồng truyền thống dưới dạng văn bản giấy hoặc tài liệu điện tử cần người chứng thực và giám sát thực thi, hợp đồng thông minh hoạt động hoàn toàn tự động và phi tập trung. Khi được triển khai lên blockchain, mỗi hợp đồng thông minh tồn tại dưới dạng một địa chỉ hợp đồng cố định và có thể được truy cập, tương tác bởi bất kỳ ai trên mạng lưới thông qua các giao dịch blockchain. Mỗi lần hợp đồng được gọi để thực hiện chức năng nào đó, toàn bộ quá trình xử lý và dữ liệu liên quan sẽ được ghi lại vĩnh viễn trong sổ cái phân tán và không thể chỉnh sửa. Trong bối cảnh hệ thống xác thực chứng chỉ học thuật, hợp đồng thông minh đóng vai trò như một cơ chế kiểm soát và xác minh

trung tâm, đảm bảo cho các bước cấp phát, lưu trữ và tra cứu chứng chỉ diễn ra một cách tự động, chính xác và không thể bị giả mạo. Ví dụ, khi một sinh viên hoàn thành đầy đủ các yêu cầu của một chương trình học, hệ thống có thể sử dụng hợp đồng thông minh để xác nhận điều kiện này và tự động phát hành chứng chỉ tương ứng. Thông tin chứng chỉ sẽ được mã hóa, lưu trữ trên một nền tảng lưu trữ phi tập trung như IPFS, đồng thời một bản ghi chứa địa chỉ IPFS và các dữ liệu nhận dạng được ghi vĩnh viễn vào blockchain. Việc xác minh sau đó chỉ cần truy cập vào hợp đồng thông minh để kiểm tra thông tin gốc, không cần phải liên hệ với trường học hoặc tổ chức cấp phát ban đầu.

Các đặc điểm nổi bật của hợp đồng thông minh:

- Tự động hóa: Hợp đồng thông minh có khả năng tự động thực thi khi các điều kiện đã được định nghĩa từ trước được thoả mãn, giúp loại bỏ hoàn toàn sự can thiệp thủ công và giảm thiểu sai sót con người.
- Không thể thay đổi: Một khi hợp đồng được triển khai lên blockchain, mã nguồn của nó trở nên bất biến, không thể bị chỉnh sửa hay can thiệp từ bên ngoài. Điều này đảm bảo tính toàn vẹn của quy trình và loại bỏ nguy cơ sửa đổi thông tin vì mục đích xấu.
- Minh bạch: Toàn bộ mã hợp đồng và các lần thực thi đều được lưu trữ công khai trên blockchain. Bất kỳ ai cũng có thể kiểm tra logic hoạt động và lịch sử giao dịch liên quan của hợp đồng, qua đó nâng cao sự tin cậy và minh bạch trong toàn hệ thống.

Trong lĩnh vực phát triển hợp đồng thông minh, ngôn ngữ lập trình phổ biến và được sử dụng rộng rãi nhất hiện nay là Solidity, ngôn ngữ chính thức cho Ethereum — nền tảng blockchain đầu tiên hỗ trợ hợp đồng thông minh. Bên cạnh Ethereum, có nhiều nền tảng blockchain khác cũng hỗ trợ triển khai smart contract với đa dạng ngôn ngữ, bao gồm:

- Binance Smart Chain (BSC): Hỗ trợ Solidity, tương thích với Ethereum Virtual Machine (EVM).
- Polygon: Một giải pháp mở rộng lớp 2 của Ethereum, cũng hỗ trợ Solidity.
- Solana: Sử dụng ngôn ngữ Rust hoặc C để phát triển hợp đồng thông minh, với tốc độ xử lý giao dịch cao và phí thấp.
- Hyperledger Fabric: Một nền tảng blockchain dành cho doanh nghiệp, hỗ trợ nhiều ngôn ngữ như Go và Java.

Không chỉ giới hạn trong lĩnh vực xác thực học thuật, hợp đồng thông minh ngày nay đã được triển khai rộng rãi trong nhiều lĩnh vực công nghệ và đời sống:

- Tài chính phi tập trung: Tự động hóa các giao dịch vay mượn, trao đổi tài sản, bảo hiểm và nhiều dịch vụ tài chính khác mà không cần ngân hàng.
- Quản lý chuỗi cung ứng: Theo dõi, xác minh nguồn gốc và trạng thái hàng hóa tại từng điểm trong chuỗi cung ứng.
- Chứng nhận học thuật: Quản lý, lưu trữ và xác minh các chứng chỉ học tập một cách minh bạch, phi tập trung.
- Bỏ phiếu điện tử: Tổ chức bầu cử minh bạch và bảo mật, đảm bảo mỗi lá phiếu chỉ được ghi nhận một lần và không thể bị thay đổi.
- Quản lý bản quyền số: Bảo vệ quyền sở hữu trí tuệ và quản lý việc phân phối nội dung số như âm nhạc, hình ảnh, video...

Trong khuôn khổ đề tài này, hợp đồng thông minh giữ vai trò trung tâm trong kiến trúc hệ thống xác thực thông tin chứng chỉ học thuật. Nó không chỉ đảm nhiệm chức năng xác minh mà còn đóng vai trò phát hành, lưu trữ, và kiểm tra thông tin một cách tự động và minh bạch. Mọi chứng chỉ được cấp phát sẽ trở thành một phần của blockchain bất biến, có thể xác minh mọi lúc, và không phụ thuộc vào một tổ chức tập trung nào. Nhờ đó, người học, nhà tuyển dụng và các bên liên quan đều có thể tra cứu và xác thực thông tin chứng chỉ một cách nhanh chóng và tin cậy, góp phần nâng cao hiệu quả và minh bạch cho quá trình quản lý học thuật trong thời đại số.

1.2.3 Hệ thống tệp liên hành tinh – IPFS

Trong các hệ thống blockchain truyền thống, việc lưu trữ dữ liệu có dung lượng lớn như tài liệu PDF, hình ảnh, video hoặc các tệp nhị phân phức tạp thường gặp nhiều hạn chế do hai yếu tố chính: chi phí cao và giới hạn kỹ thuật về dung lượng lưu trữ trên blockchain. Blockchain được thiết kế để lưu trữ dữ liệu một cách minh bạch, bất biến và bảo mật, nhưng điều này đồng nghĩa với việc mỗi byte dữ liệu được ghi vào blockchain đều có chi phí tương đối cao và tốn tài nguyên tính toán của toàn mạng lưới. Chính vì vậy, một giải pháp thay thế nhằm mở rộng khả năng lưu trữ, nhưng vẫn đảm bảo tính toàn vẹn và không thể sửa đổi của dữ liệu, là một yếu tố cần thiết trong các hệ thống ứng dụng blockchain thực tế.

Một trong những giải pháp nổi bật và hiệu quả nhất hiện nay là InterPlanetary File System (IPFS) – một giao thức mạng phân tán được thiết kế để lưu trữ và chia sẻ dữ liệu theo cơ chế phi tập trung. IPFS không lưu trữ dữ liệu theo

địa chỉ truyền thống (như đường dẫn URL hoặc IP), mà lưu theo nội dung của tệp. Điều này có nghĩa là mỗi tệp được lưu trữ trên IPFS sẽ được ánh xạ thành một mã băm duy nhất đại diện cho nội dung của chính nó. Bất kỳ sự thay đổi nào trong nội dung, dù là nhỏ nhất, đều dẫn đến thay đổi hoàn toàn mã băm – qua đó đảm bảo tính toàn vẹn của dữ liệu. Nhờ đó, IPFS có thể cung cấp một lớp lưu trữ linh hoạt, hiệu quả và bảo mật, đồng thời bổ trợ lý tưởng cho các ứng dụng blockchain.

Quá trình lưu trữ tệp trên IPFS diễn ra qua các bước cơ bản sau:

- Phân mảnh dữ liệu: Mỗi tệp lớn sẽ được chia thành nhiều phần nhỏ (blocks), giúp dễ dàng phân phối và tối ưu truy xuất.
- Sinh mã băm cho từng khối: Mỗi phần nhỏ của tệp sẽ được mã hóa thành một mã băm riêng biệt, đảm bảo tính toàn vẹn cho từng đơn vị dữ liệu.
- Tạo ra một mã đại diện duy nhất (root hash): Toàn bộ cấu trúc các khối sẽ được ánh xạ lại thành một cây Merkle DAG, từ đó sinh ra một mã hash đại diện duy nhất cho toàn bộ tệp.
- Truy xuất dữ liệu theo nội dung: Người dùng chỉ cần mã hash để truy xuất và tải lại toàn bộ tệp từ bất kỳ nút nào đang lưu trữ nó trên mạng IPFS.

Khác với hệ thống lưu trữ tập trung (như Google Drive, Dropbox hay cơ sở dữ liệu truyền thống), IPFS cho phép bất kỳ ai cũng có thể lưu trữ và chia sẻ dữ liệu thông qua việc chạy một node IPFS. Khi người dùng khác yêu cầu tệp bằng mã hash, IPFS sẽ tìm kiếm các node có khối dữ liệu phù hợp và tải về nhanh chóng theo mô hình phân phối đồng cấp, tương tự cơ chế của các mạng chia sẻ torrent.

Những ưu điểm nổi bật của IPFS có thể kể đến như:

- Tính phi tập trung cao: IPFS không có máy chủ trung tâm, mọi dữ liệu được phân phối và lưu trữ trên hàng nghìn nút khác nhau, giúp tăng khả năng chống chịu lỗi và giảm phụ thuộc vào một thực thể duy nhất.
- Tiết kiệm chi phí lưu trữ: Thay vì lưu trữ toàn bộ nội dung lên blockchain (gây tốn kém), chỉ cần lưu mã hash của tệp – một chuỗi ký tự ngắn – lên blockchain. Điều này giảm tải cho mạng lưới và tối ưu chi phí.
- Đảm bảo toàn vẹn và chống giả mạo: Do dữ liệu được truy xuất theo mã hash duy nhất, bất kỳ thay đổi nào dù nhỏ cũng sẽ làm hash thay đổi hoàn toàn. Điều này giúp phát hiện mọi hành vi sửa đổi nội dung.
- Hiệu suất cao: IPFS cho phép tải dữ liệu từ nhiều nguồn khác nhau cùng lúc, cải thiện tốc độ truyền tải dữ liệu, đặc biệt là với các tệp lớn.

- Khả năng mở rộng: Với bản chất phân tán, IPFS có thể mở rộng quy mô mà không bị giới hạn bởi một máy chủ hoặc trung tâm dữ liệu.

Trong khuôn khổ đề tài này, IPFS được lựa chọn làm nền tảng lưu trữ cho các chứng chỉ học tập dưới dạng tệp PDF. Quy trình vận hành cơ bản như sau:

- Cấp phát chứng chỉ:
  - Khi một người học hoàn thành khóa học và được cấp chứng chỉ, hệ thống sẽ sinh ra tệp PDF đại diện cho chứng chỉ.
  - Tệp PDF sẽ được tải lên IPFS và nhận về một mã hash duy nhất đại diện cho tệp.
  - Mã hash này được lưu trữ trong hợp đồng thông minh trên blockchain, đóng vai trò như "chứng thư số" xác nhận sự tồn tại và tính toàn vẹn của chứng chỉ.
- Xác minh chứng chỉ:
  - Khi một bên thứ ba (ví dụ: nhà tuyển dụng hoặc tổ chức kiểm định) cần xác minh tính hợp lệ của chứng chỉ, họ chỉ cần truy xuất hợp đồng thông minh để lấy mã hash IPFS.
  - Sau đó, sử dụng mã hash để tải tệp từ IPFS, so sánh nội dung với chuẩn (hoặc các trường thông tin cần thiết) để xác thực rằng chứng chỉ không bị sửa đổi.
- Đảm bảo tính minh bạch và chống gian lận:
  - Vì tệp PDF không thể bị chỉnh sửa mà không thay đổi mã hash tương ứng, mọi hành vi giả mạo hoặc can thiệp nội dung đều có thể dễ dàng phát hiện.
  - Bên xác minh không cần tin tưởng vào bên phát hành chứng chỉ, mà có thể xác thực một cách độc lập thông qua dữ liệu trên blockchain và IPFS.

Tóm lại, việc kết hợp blockchain và IPFS tạo thành một mô hình lưu trữ và xác thực dữ liệu hiệu quả, vừa tối ưu hóa chi phí, vừa đảm bảo tính bảo mật, minh bạch và bất biến. Trong hệ thống xác thực chứng chỉ học thuật được đề xuất trong khóa luận này, IPFS đóng vai trò không thể thiếu trong việc lưu trữ các tệp chứng chỉ, còn blockchain và hợp đồng thông minh đảm nhận vai trò kiểm chứng, theo dõi và xác minh sự tồn tại của chúng. Mô hình này không chỉ mang tính khả thi cao trong thực tiễn, mà còn có thể mở rộng sang các lĩnh vực khác như y tế, pháp lý, chứng nhận nghề nghiệp và quản lý tài liệu số.

CHƯƠNG 2

CƠ SỞ TOÁN HỌC TRONG BLOCKCHAIN

2.1 Cây Merkle

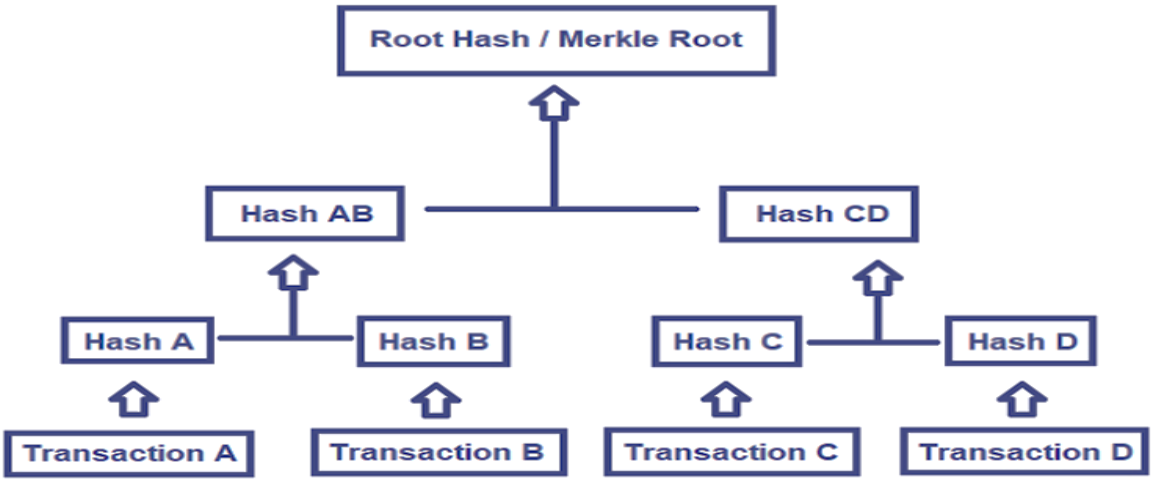
2.1.1 Sơ lược về hàm băm

Một hàm băm mật mã là một hàm toán học chuyển đổi một chuỗi bit có độ dài tùy ý thành một chuỗi bit có độ dài cố định. Hàm này phải đảm bảo các tính chất sau để được coi là an toàn trong mật mã:

- Khó đảo ngược: dễ dàng tính toán giá trị băm từ dữ liệu đầu vào, nhưng rất khó để tìm lại dữ liệu ban đầu từ giá trị băm.
- Khó tìm hai thông điệp khác nhau có cùng giá trị băm: khó tìm hai chuỗi dữ liệu khác nhau sao cho chúng có cùng giá trị băm.
- Khó tìm thông điệp khác có cùng giá trị băm với một thông điệp đã biết: khi đã biết một thông điệp và giá trị băm của nó, rất khó để tìm một thông điệp khác có cùng giá trị băm.

Các hàm băm mật mã được sử dụng rộng rãi trong các ứng dụng như chữ ký số, mã xác thực tin nhắn, và trong các hệ thống blockchain để đảm bảo tính toàn vẹn và xác thực của dữ liệu. Một số hàm băm mật mã phổ biến có thể kể đến như: SHA-256, SHA-2, MD5,…

2.1.2 Sơ lược về cây Merkle



Hình 2-1 Cấu trúc của một cây Merkle

Khái niệm cây Merkle được đặt theo tên của Ralph C. Merkle – người đã cấp bằng sáng chế cho nó vào năm 1979.

Trong mật mã học và khoa học máy tính, cây Merkle là một cây nhị phân hoàn chỉnh trong đó mỗi nút lá là một băm của một khối dữ liệu, và mỗi nút không phải lá (hay còn gọi là nhánh, nút trong) là một băm được tính từ phép nối của các giá trị băm của hai nút con.

Gọi hàm băm là h: $\{0,1\}^* \rightarrow \{0,1\}^n$
Gọi $D_1, D_2, \dots, D_k$ là các khối dữ liệu đầu vào.

- Nút lá: L_i=$h(D_i)$.
- Nút trong P: Nếu A, B là hai nút con, thì $P = h(A \parallel B)$ trong đó $\parallel$ là phép nối chuỗi.
- Merkle root: $R = h(h(\dots) \parallel h(\dots))$ là giá trị của Merkle root.

Merkle root là đại diện duy nhất cho toàn bộ tập dữ liệu đầu vào và được dùng để kiểm tra tính toàn vẹn dữ liệu một cách hiệu quả. Vì với mỗi thay đổi dù là nhỏ nhất trên nút con D_i thì tương ứng $h(D_i)$ sẽ thay đổi dẫn đến gốc Merkle cũng thay đổi theo. Chính vì vậy, cây Merkle có thể được sử dụng để xác minh bất kỳ loại dữ liệu nào được lưu trữ, xử lý và chuyển giao trong và giữa các máy tính. Chúng có thể giúp đảm bảo rằng các khối dữ liệu nhận được từ các đối tác khác trong mạng ngang hàng được nhận mà không bị hư hỏng và không bị thay đổi, và thậm chí để kiểm tra xem các đối tác khác có nói dối và gửi các khối giả không.

2.1.3 Bằng chứng Merkle

Bên cạnh tính toàn vẹn dữ liệu của mình, cây Merkle còn có một ưu điểm nữa chính là khả năng chứng minh. Tức là dù độ phức tạp khi xây cây là O(n) thì ta chỉ cần một phương pháp với độ phức tạp O(log$n$) để xác minh một phần tử có thuộc cây Merkle hay không. Phương pháp này được gọi là bằng chứng Merkle.

Bằng chứng Merkle là một chuỗi các giá trị băm cần thiết được cung cấp để chứng minh rằng một phần tử dữ liệu cụ thể thuộc về một cây Merkle nhất định. Merkle Proof bao gồm:

- Giá trị băm của phần tử cần chứng minh
- Danh sách các giá trị băm của các nút anh em (danh sách cho phép tính toán lại gốc Merkle trên đường đi từ phần tử cần chứng minh tới Merkle root).

- Thông tin về cấu trúc cây Merkle (gồm: chiều cao của cây Merkle, vị trí của phần tử cần chứng minh, cách thức kết hợp các giá trị băm, merkle root dùng để so sánh).

Cách thức hoạt động của bằng chứng Merkle

- Bắt đầu từ phần tử cần chứng minh: Lấy giá trị băm của phần tử D_i, gọi là $h(D_i)$
- Lần lượt kết hợp với các giá trị băm của các nút anh em: Sử dụng danh sách các giá trị băm của các nút anh em để tính toán lại giá trị băm của gốc Merkle. Cách kết hợp phụ thuộc vào cấu trúc cây Merkle (trái-phải hoặc phải-trái).
- So sánh với băm của root đã biết: Sau khi tính toán lại giá trị băm này, so sánh với giá trị băm của Merkle root đã biết. Nếu chúng khớp, phần tử D_i là một phần của cây Merkle.

Ví dụ minh họa:

Giả sử bạn có một cây Merkle với các phần tử dữ liệu D_1, D_2, D_3, D_4. Các bước để kiểm tra xem D_3 là một phần của cây Merkle hay không có thể thực hiện như sau:

- Thay vì cần toàn bộ các nút trong cây Merkle thì ta chỉ cần các nút anh em của D_3 gồm: $D_4, h(D_1||D_2)$, merkle root $h(D_1||D_2||D_3||D_4)$.
- Tính giá trị băm của D_3, gọi là $h(D_3)$.
- Lấy giá trị băm của nút anh em của D_3, gọi là $h(D_4)$
- Kết hợp $h(D_3)$ và $h(D_4)$ theo cấu trúc cây Merkle để tính toán giá trị băm của nút cha $h(D_3||D_4)$.
- Tiếp tục kết hợp với các giá trị băm của các nút cha cho đến khi đạt được giá trị băm của Merkle root.
- So sánh giá trị băm của gốc Merkle tính toán được với giá trị băm đã biết để xác minh tính hợp lệ.

2.2 Nguyên lý của thuật toán RSA

2.2.1 Sơ lược về hàm băm SHA-256

SHA-256 là một hàm băm mật mã thuộc họ SHA-2, được phát triển bởi Cơ quan An ninh Quốc gia Hoa Kỳ (NSA) và công nhận bởi Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) trong tiêu chuẩn FIPS PUB 180-2 vào năm 2002.

SHA-256 có các đặc tính chính như:

- Độ dài đầu ra cố định: nó nhận đầu vào có độ dài tùy ý và luôn trả về giá trị băm cố định 256 bit.
- Hàm một chiều (tính không thể đảo ngược): Rất khó hoặc gần như không thể phục hồi dữ liệu gốc từ giá trị băm.
- Hiệu ứng "tuyết lở": Một thay đổi nhỏ trong đầu vào dẫn đến giá trị băm hoàn toàn khác biệt.
- Khả năng kháng va chạm: Khó tìm hai đầu vào khác nhau tạo ra cùng một giá trị băm, đảm bảo tính toàn vẹn dữ liệu.

Một số ứng dụng của thuật toán SHA-256 có thể kể đến như:

- Chữ ký số và chứng chỉ số: SHA-256 được sử dụng trong các giao thức bảo mật như TLS/SSL, PGP, và S/MIME để đảm bảo tính toàn vẹn và xác thực của dữ liệu.
- Blockchain và tiền điện tử: Bitcoin sử dụng SHA-256 trong cơ chế "bằng chứng công việc" để xác thực giao dịch và tạo khối mới.
- Xác thực phần mềm: SHA-256 được dùng để xác thực các gói phần mềm, đảm bảo rằng chúng không bị thay đổi hoặc giả mạo.
- Lưu trữ mật khẩu: Nhiều hệ thống sử dụng SHA-256 để băm mật khẩu trước khi lưu trữ, giúp bảo vệ mật khẩu khỏi việc bị lộ khi cơ sở dữ liệu bị xâm nhập

2.2.2 Các bước thực hiện hàm băm SHA-256

Bước 1: Bước xử lý (thêm padding)

Mục đích của padding là làm cho dữ liệu đầu vào có độ dài chia hết cho 512 bit.

- Chuyển dữ liệu đầu vào thành một chuỗi nhị phân gốc.
- Sau đó thêm bit "1" vào sau chuỗi nhị phân gốc.
- Tiếp theo ta sẽ thêm đủ số lượng bit "0" để độ dài cuối cùng là bội số của 512 (Rồi trừ đi 64 bit cuối)
- Cuối cùng là thêm 1 chuỗi 64 bit biểu diễn độ dài của chuỗi dữ liệu ban đầu.

Sau khi được thêm padding thành các khối, mỗi khối có kích thước 512 bit.

Bước 2: Khởi tạo các giá trị ban đầu

SHA-256 sử dụng 8 giá trị khởi tạo cố định là 8 giá trị băm. Đây là các hằng số được mã hóa cứng đại diện cho 32 bit đầu tiên của phần phân số của căn bậc hai của 8 số nguyên tố đầu tiên: 2, 3, 5, 7, 11, 13, 17, 19.

H0 = 0x6a09e667 (căn bậc hai của 2)
H1 = 0xbb67ae85 (căn bậc hai của 3)
H2 = 0x3c6ef372 (căn bậc hai của 5)
H3 = 0xa54ff53a (căn bậc hai của 7)
H4 = 0x510e527f (căn bậc hai của 11)
H5 = 0x9b05688c (căn bậc hai của 13)
H6 = 0x1f83d9ab (căn bậc hai của 17)
H7 = 0x5be0cd19 (căn bậc hai của 19)

Các bước để tạo ra các giá trị này: tính căn bậc hai của 8 số nguyên tố đầu tiên, sau đó lấy phần thập phân của căn bậc hai này, tiếp theo nhân giá trị này với 2^{32} rồi lấy phần nguyên, và cuối cùng chuyển sang hệ thập lục phân.

Bước 3: Nén dữ liệu

Mỗi khối 512 bit sẽ được xử lý qua 64 vòng lặp

- Mở rộng khối dữ liệu
  - Khởi tạo Hằng số tròn (k).

Một số giá trị (k) được tính như sau: Tính căn bậc ba của 64 số nguyên tố đầu tiên, sau đó lấy phần thập phân của căn bậc 3 này, tiếp theo nhân giá trị này với với 2^{32} rồi lấy phần nguyên, và cuối cùng chuyển thành hệ thập lục phân.Dưới đây là 64 hằng số sau khi đã tính toán

```
0x428a2f98 0x71374491 0xb5c0fbcf 0xe9b5dba5 0x3956c25b 0x59f111f1 0x923f82a4 0xab1c5ed5
0xd807aa98 0x12835b01 0x243185be 0x550c7dc3 0x72be5d74 0x80deb1fe 0x9bdc06a7 0xc19bf174
0xe49b69c1 0xefbe4786 0x0fc19dc6 0x240ca1cc 0x2de92c6f 0x4a7484aa 0x5cb0a9dc 0x76f988da
0x983e5152 0xa831c66d 0xb00327c8 0xbf597fc7 0xc6e00bf3 0xd5a79147 0x06ca6351 0x14292967
0x27b70a85 0x2e1b2138 0x4d2c6dfc 0x53380d13 0x650a7354 0x766a0abb 0x81c2c92e 0x92722c85
0xa2bfe8a1 0xa81a664b 0xc24b8b70 0xc76c51a3 0xd192e819 0xd6990624 0xf40e3585 0x106aa070
0x19a4c116 0x1e376c08 0x2748774c 0x34b0bcb5 0x391c0cb3 0x4ed8aa4a 0x5b9cca4f 0x682e6ff3
0x748f82ee 0x78a5636f 0x84c87814 0x8cc70208 0x90befffa 0xa4506ceb 0xbef9a3f7 0xc67178f2
```

Hình 2-2 Các hằng số được làm tròn

- Tạo lịch trình nhắn tin (w)

Mỗi khối 512 bit được chia thành 16 từ ban đầu (W_0 đến W_{15}), mỗi từ có kích thước 32 bit. Sau đó mở rộng thành 64 từ (W_0 đến W_{63}) bằng cách sử dụng phép toán logic:

for i from 16 to 63

s0 := (w[i-15] rightrotate 7) xor (w[i-15] rightrotate 18) xor (w[i-15] rightshift 3)

s1 := (w[i- 2] rightrotate 17) xor (w[i- 2] rightrotate 19) xor (w[i- 2] rightshift 10)

w[i] := w[i-16] + s0 + w[i-7] + s1

Khởi tạo các biến thành giá trị băm hiện tại:

a := h0, b := h1, c := h2, d := h3, e := h4, f := h5, g := h6, h := h7

– Nén vòng lặp chính:

Quá trình nén thực hiện theo vòng lặp sau:

for i from 0 to 63

S1 := (e rightrotate 6) xor (e rightrotate 11) xor (e rightrotate 25)

ch := (e and f) xor ((not e) and g)

temp1 := h + S1 + ch + k[i] + w[i]

S0 := (a rightrotate 2) xor (a rightrotate 13) xor (a rightrotate 22)

maj := (a and b) xor (a and c) xor (b and c)

temp2 := S0 + maj

h := g

g := f

f := e

e := d + temp1

d := c

c := b

b := a

a := temp1 + temp2

– Thêm đoạn đã nén vào giá trị băm hiện tại:

h0 := h0 + a, *h4 := h4 + e*

h1 := h1 + b, *h5 := h5 + f*

h2 := h2 + c, *h6 := h6 + g*

h3 := h3 + d, *h7 := h7 + h*

Bước 4: Tạo giá trị băm cuối cùng

$$digest := hash := h0 \,||\, h1 \,||\, h2 \,||\, h3 \,||\, h4 \,||\, h5 \,||\, h6 \,||\, h7$$

Với || là phép nối chuỗi.

Chuyển digest sang dạng thập lục phân để dễ đọc hơn.

2.2.3 Hệ mật mã khóa công khai

Trước khi đi vào tìm hiểu về mật mã khóa công khai, ta sẽ đến với khái niệm về mật mã học cũng như mật mã đối xứng và bất đối xứng.

Đầu tiên, mật mã học là ngành khoa học nghiên cứu các phương pháp toán học để mã hóa giữ mật thông tin bao gồm mã hóa và giải mã.

- Mã hóa là biến đổi cách thức biểu diễn thông tin từ dạng bản rõ (chúng ta có thể đọc được) sang dạng bản mã (chỉ người giải mã mới hiểu được), nó giúp chúng ta che giấu, giữ mật thông tin trong khi lưu trữ cũng như truyền thông tin đi.
- Giải mã là quá trình ngược lại đó là biến bản mã thành bản rõ.

Các chức năng cơ bản của mật mã đó là:

- Tính bí mật: nó đảm bảo tính bí mật của dữ liệu mà mình gửi đi và chỉ những người liên quan mới biết được nội dung.
- Tính toàn vẹn : đảm bảo dữ liệu không thể bị mất mát hoặc chỉnh sửa trong qua trình gửi và nhận mà không bị phát hiện.
- Tính xác thực: đảm bảo danh tính của thực thể được xác minh.
- Tính không thể chối từ: đảm bảo người gửi không thể chối cãi với thông tin mình gửi đi

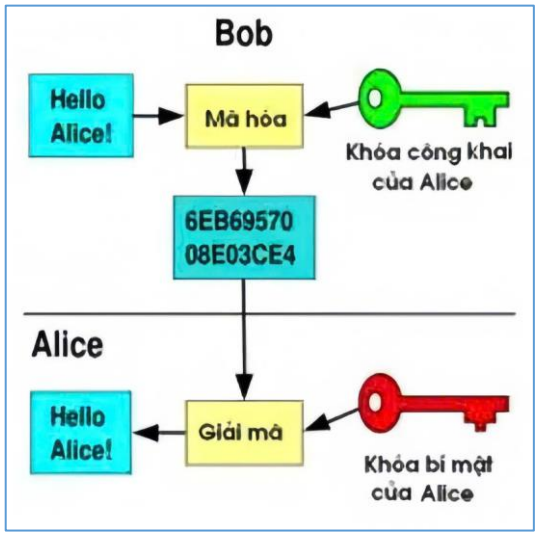
Tiếp theo là hệ mật mã khóa đối xứng. Đó là những hệ mật được sử dụng chung một khóa trong quá trình mã hóa và mã hóa. Tức là người gửi sử dụng khóa chung để mã hóa thông tin rồi gửi cho nguời nhận. Và người nhận nhận được thông tin đó sẽ dùng chính khóa chung đó để giải mã. Do đó khóa phải được giữ bí mật tuyện đối. Một số hệ mật mã khóa đối xứng hiện đại mà mình thấy hay được sử dụng là DES, AES, RC4, RC5,.. Mặc dù có nhiều ưu điểm như hiệu suất cao và đơn giản trong triển khai, nhưng phương pháp này cũng tồn tại một số nhược điểm đáng lưu ý như:

- Vấn đề phân phối khóa: Vì cùng một khóa được sử dụng cho cả mã hóa và giải mã, việc phân phối khóa một cách an toàn giữa các bên là một thách thức lớn. Nếu khóa bị rò rỉ hoặc bị đánh cắp trong quá trình truyền tải, toàn bộ hệ thống bảo mật sẽ bị đe dọa.
- Khả năng mở rộng kém: Trong một hệ thống với nhiều người dùng, mỗi cặp người dùng cần một khóa riêng biệt. Điều này dẫn đến số lượng khóa cần

quản lý tăng theo cấp số nhân, gây khó khăn trong việc duy trì và bảo vệ chúng.

- Quản lý khóa phức tạp: Việc tạo, lưu trữ và thay đổi định kỳ các khóa một cách an toàn là một công việc phức tạp, đặc biệt trong các tổ chức lớn. Nếu không quản lý tốt, khóa có thể bị lộ hoặc sử dụng sai mục đích.
- Thiếu xác thực: Mã hóa đối xứng không cung cấp cơ chế xác thực người gửi hoặc đảm bảo tính toàn vẹn của dữ liệu. Điều này có thể dẫn đến việc người gửi phủ nhận hành động gửi tin nhắn.

Việc giữ bí mật khóa đồng nghĩa với việc giữ bí mật thông tin nên việc trao đổi khóa chỉ diễn ra trên kênh mật thì mới đảm bảo được, thế nhưng việc trao đổi này cung không phải dễ để đảm bảo độ an toàn cao. Từ đây hình thành nên ý tưởng của mật mã công khai, tức là không cần phải trao đổi khóa qua kênh mật nữa.Và từ ý tưởng đó cũng như để khắc phục những nhược điểm của hệ mật mã đối xứng thì hệ mật mã khóa bất đối xứng (hay còn gọi là hệ mật mã khóa công khai) đã ra đời. Ở hệ mật này thay vì người dùng dùng chung một khóa như ở hệ mật mã khóa đối xứng thì ở đây sẽ dùng một cặp khóa có tên là khóa công khai và khóa riêng tư. Hệ mật mã khóa bất đối xứng mình thấy được dùng nhiều nhất là hệ mật RSA, do Rivest, Shamir và Adleman đưa ra đầu tiên năm 1977. Sơ đồ của hệ mã công khai được cho ở hình sau:



Hình 2-3 Sơ đồ mật mã khóa công khai

Về cơ bản thì hệ mã công khai sử dụng hai khóa có quan hệ toán học với nhau, tức là một khóa này được hình thành từ khóa kia: Người muốn nhận bản mã (Alice) tạo ra một khóa bí mật và từ khóa bí mật tính ra khóa công khai với một thủ tục không phức tạp, còn việc tìm khóa mật khi biết khóa công khai là bài toán khó

giải được. Khóa công khai sẽ đưa đến cho người gửi bản tin (Bob) qua kênh công cộng. Và bản tin được Bob mã hóa bằng khóa công khai này. Bản mã truyền đến Alice, và nó được giải mã bằng khóa bí mật Alice.

2.2.4 Thuật toán RSA

Thuật toán RSA (hay còn gọi là hệ mật RSA) là một thuật toán dựa trên độ khó của bài toán phân tích một số thành nhân tử và bài toán tính căn bậc e modulo n (hay có thể phát biểu là tìm số m sao cho:

$$c = m^e \ (mod\ n)$$

trong đó (e, n) chính là khóa công khai và c là bản mã.

Trước hết thì ta sẽ nói về quá trình tạo khóa. Ta lấy luôn ví dụ đã nói ở trên: Alice là người nhận và Bob là người gửi. Khi đó, Alice sẽ tạo một cặp khóa công khai và khóa bí mật với các bước như sau:

- Bước 1: Chọn ngẫu nhiên 2 số nguyên tố rất lớn khác nhau p và q.
- Bước 2: Tính tích của 2 số này $n = p * q$.
- Bước 3: Tính giá trị hàm $\varphi(n) = (p-1) * (q-1)$.
- Bước 4: Chọn một số nguyên d: $d < \varphi(n)$ và $\gcd\big(d, \varphi(n)\big) = 1$ (tức là d và $\varphi(n)$ nguyên tố cùng nhau).
- Bước 5: Tính giá trị e thỏa mãn: $e * d \equiv 1\ mod(\varphi(n))$.

Từ đây, ta được một cặp khóa (e,d) với e là khóa công khai và d là khóa bí mật. Tiếp theo là quá trình mã hóa. Sau khi Alice tạo ra cặp khóa, Bob muốn gửi đi thông điệp m cho Alice sẽ sử dụng khóa công khai của Alice để tiến hành mã hóa:

$$c = m^e \ (mod\ n)$$

Và gửi cho Alice. Cuối cùng Alice nhận c từ Bob và sử dụng khóa bí mật d của bản thân mình để giải mã được m từ c theo công thức:

$$m = c^d \ (mod\ n)$$

Ta hoàn toàn có thể chứng minh được tính đúng đắn của biểu thức này nhưng trước tiên ta sẽ tìm hiểu về hai định lí sử dụng trong quá trình chứng minh. Đó là:

Định lý Fermat nhỏ: khẳng định rằng nếu p là một số nguyên tố, thì với số nguyên a bất kỳ, $a^p - a$ sẽ chia hết cho p. Bằng kí hiệu đồng dư, ta có:

$$a^p \equiv a \ (mod\ p)$$

Định lý phần dư trung hoa: Giả sử có các số nguyên dương $n_1, n_2, \dots, n_k$ đôi một nguyên tố cùng nhau $\gcd(n_i, n_j) = 1$ với mọi $i \neq j$.

Cho hệ phương trình:

$$\begin{cases} x \equiv a_1 \, mod \, n_1 \\ x \equiv a_2 \, mod \, n_2 \\ \quad \ldots . \\ x \equiv a_k \, mod \, n_k \end{cases}$$

Khi đó, tồn tại duy nhất một số nguyên x thỏa mãn tất cả các đồng dư trên trong modulo $N = n_1 * n_1 * \ldots * n_k$.

Giờ ta sẽ chứng minh tính đúng đắn của :

$$c^d = (m^e)^d \, (mod \, n) = m^{e*d} \, (mod \, n)$$

Do $e * d \equiv 1 \, mod(\varphi(n))$ nên $e * d \equiv 1 \, mod(p-1)$ và $e * d \equiv 1 \, mod(q-1)$. Theo định lý Fermat nhỏ, ta có:

$$m^{e*d} \equiv m(mod \, p) \text{ và } m^{e*d} \equiv (mod \, q)$$

Do p và q là hai số nguyên tố khác nhau nên chúng cũng đồng thời là hai số nguyên tố cùng nhau, áp dụng định lý phần dư trung hoa, ta có:

$$m^{e*d} \equiv m(mod \, pq)$$

Hay

$$c^d \equiv m(mod \, n)$$

Biểu thức này tương đương với biểu thức:

$$m = c^d \, (mod \, n)$$

2.3 ECC trên trường hữu hạn F_P

2.3.1 ECC trên trường số thực

Mật mã đường cong elliptic là một phương pháp mật mã khóa công khai dựa trên lý thuyết về đường cong elliptic trên các trường hữu hạn. ECC cho phép tạo ra các khóa mật mã nhanh hơn, nhỏ gọn hơn và hiệu quả hơn so với các hệ thống mật mã truyền thống như RSA và ElGamal, đồng thời vẫn đảm bảo mức độ bảo mật tương đương.

Trước hết, ta nói về nhóm abel (tạm kí hiệu là $\{G,\bullet\}$). Đây là một tập hợp các phần tử có một phép toán nhị phân được kí hiệu là •, ánh xạ mỗi cặp có thứ tự (a,b) các phần tử trong G thành một phần từ (a,b) trong G, sao cho thỏa mãn điều kiện:

- Đóng: Nếu a, b thuộc G thì a • b cũng thuộc G.
- Kết hợp: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$, với mọi a, b, c trong G.
- Phần tử đơn vị: Tồn tại một phần tử đơn vị e trong G sao cho: $a \bullet e = e \bullet a = a$, với mọi a trong G.

– Phần tử nghịch đảo: Với mỗi phần tử a trong G, tồn tại một phần tử a' trong G sao cho $a \bullet a' = a' \bullet a = e$.
– Giao hoán: $a \bullet b = b \bullet a$, với mọi a, b trong G.

Một đường cong elliptic trên trường số thực là một tập hợp các điểm (x, y) thỏa mãn phương trình:

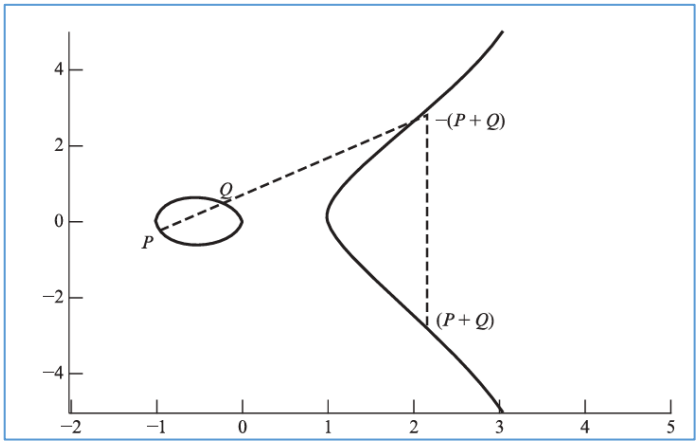
$$y^2 = x^3 + ax + b \qquad (với\ 4a^3 + 27b^2 \neq 0)$$

Trong đó, a và b là các hằng số xác định đường cong, và các phép toán trên nhóm các điểm này được định nghĩa theo lý thuyết nhóm abel.
Từ đây, ta có tập hợp tất cả các điểm thuộc được cong elliptic kí hiệu:

$$E(a,b) = \{(x,y) \in R: y^2 = x^3 + ax + b\}\, U\, \{O\}$$

Với a và b thỏa mãn điều kiện:

$$4a^3 + 27b^2 \neq 0$$



Hình 2-4 Đường cong elliptic

Trên đường cong elliptic, để xác định một nhóm, ta cần định nghĩa một phép toán, gọi là phép cộng và ký hiệu là + cho tập E(a, b). Về mặt hình học, quy tắc cộng có thể được phát biểu như sau: Nếu ba điểm trên đường cong elliptic nằm trên một đường thẳng thì tổng của chúng là O (điểm vô cực). Từ định nghĩa này, ta có thể xây dựng các quy tắc cộng trên đường cong elliptic:

– Đóng vai trò là phần tử đơn vị cộng. Do đó $O = -O$, với mọi điểm P trên đường cong elliptic, ta có $P + O = P$.

Giả xử có hai điểm $P, Q \neq O$,

– Phần tử đối của một điểm P là điểm có cùng hoành độ x nhưng tung độ y đối dấu, tức là $P = (x, y)$ thì $-P = (x, -y)$. Lưu ý: hai điểm này có thể được nối bởi một đường thẳng đứng (chỉ cắt đường cong elliptic tại hai điểm) thì $P + (-P) = P - P = O$.

- Để cộng 2 điểm P và Q có hoành độ khác nhau, ta vẽ một đường thẳng đi qua chúng và tìm điểm thứ ba R mà đường thẳng đó cắt đường cong. Ta dễ dàng thấy rằng tồn tại duy nhất điểm R là giao điểm (trừ trường hợp đường thẳng tiếp xúc với đường cong tại P và Q, khi đó lấy $R = P$ hoặc $R = Q$). Ta định nghĩa phép cộng $P + Q = -R$ (là điểm đối xứng qua trục hoành của giao điểm thứ 3 của đường thẳng đi qua P, Q với đường cong elliptic).
- Để nhân đôi điểm Q (tức là tính 2Q), thực chất là ta đang thực hiện phép cộng điểm đó nhiều lần. Tức là $2Q = Q + Q$.

Từ những quy tắc cộng này, ta có thể tìm được tọa độ của điểm R = P + Q là

$$x_R = \Delta^2 - x_P - x_Q$$

$$y_R = -y_p + \Delta(x_P - x_R)$$

Với $P = (x_P, y_P), Q = (x_Q, y_Q)$ và $\Delta = \frac{y_Q - y_P}{x_Q - x_P}$.

Ta hoàn toàn có thể chứng minh tính đúng đắn của 2 biểu thức trên.

Gọi đường cong Elliptic E: $y^2 = x^3 + ax + b$

Với 2 điểm $P = (x_P, y_P), Q = (x_Q, y_Q) \neq O$.

Đường thẳng d qua P, Q có phương trình:

$$y - y_P = \Delta(x - x_P)$$

Hay

$$y = y_P + \Delta(x - x_P)$$

Với hệ số góc $\Delta = \frac{y_Q - y_P}{x_Q - x_P}$ (mọi (x, y) thuộc d).

Gọi giao điểm thứ 3 là điểm $R(x_R, y_R)$.

Xét phương trình hoành độ giao điểm giữa d và E, ta có:

$$(y_P + \Delta(x - x_P))^2 = x^3 + ax + b$$

Khai triển phương trình và chuyển vế, ta được:

$$x^3 - \Delta^2 x^2 - (2\Delta(y_P - \Delta x_P) - a)x - (y_P - \Delta x_P)^2 + b = 0$$

Theo định lý Vi-et:

Tổng ba nghiệm: $x_P + x_Q + x_R = \frac{-b}{a} = \Delta^2$

Suy ra, $x_R = \Delta^2 - x_P - x_Q = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - (x_P + x_Q)$

Ta đã tìm được hoành độ của (P + Q) là x_R.

Từ đây, ta có thể tìm được tung độ của (P + Q) là

$$-y_R = -(\Delta(y_R - y_P) + y_P) = -y_p + \Delta(x_P - x_R).$$

Tương tự với phép nhân 2P = P + P = R ($y_R \neq O$) với:

$$x_R = (\frac{3{x_P}^2 + a}{2y_P})^2 - 2x_P$$

$$y_R = (\frac{3{x_P}^2 + a}{2y_P})(x_P - x_R) - y_P$$

2.3.2 ECC trên trường hữu hạn F_P

Các tham số miền đường cong elliptic trên trường hữu hạn F_P là một bộ sáu:

$$T = (p, a, b, G, n, h)$$

Bao gồm:

- một số nguyên p xác định trên trường hữu hạn F_P.
- hai phần tử $a, b \in F_P$ xác định một đường cong elliptic $E(F_P)$ được cho bởi phương trình:
  E: $y^2 = x^3 + ax + b$ (mod p)
- một điểm cơ sở G(x_G, y_G) trên $E(F_P)$. Đây là một điểm cụ thể trên đường cong elliptic sao cho nếu ta lặp lại phép cộng điểm G với chính nó, ta sẽ tạo được một tập hợp các điểm gọi là nhóm con tuần hoàn sinh từ G.
- một số nguyên tố n là bậc của G (tức là nếu ta nhân điểm G với n, ta sẽ quay về điểm vô cùng O hay $nG = O$).
- một số nguyên h là hệ số đồng cấu $h = \frac{\#E(F_P)}{n}$. Trong đó:

$$\#E(F_P) = \{(x, y) \in F_P : y^2 = x^3 + ax + b \ (mod\ p)\} \cup \{O\}$$

2.3.3 Mật mã đường cong elliptic

Trước khi tìm hiểu về mật mã đường cong elliptic, ta sẽ nói về trao đổi khóa ECC Diffie-Hellman. Về bản chất, phương pháp này vẫn dựa trên trao đổi khóa Diffie-Hellman nhưng áp dụng với đường cong elliptic. Cụ thể như sau:

- Các thông tin công khai như là $E_P(a, b), G$.
- User A tạo khóa với khóa bí mật $d_A < n$. Sau đó tính toán khóa công khai $P_A = d_A G$.
- User B tạo khóa với khóa bí mật $d_B < n$. Sau đó tính toán khóa công khai $P_B = d_B G$.
- User A nhận khóa công khai P_B và tính khóa chia sẻ bí mật $K_A = d_A P_B = d_A d_B G$.

- User B nhận khóa công khai P_A và tính khóa chia sẻ bí mật $K_B = d_B P_A = d_B d_A G$.

Ta thấy $K_A = K_B$. Không cần chia sẻ khóa bí mật, 2 user vẫn có thể tính được khóa chung.

Nguyên lý của mật mã đường cong elliptic cũng tương tự như vậy. Ta sẽ lấy một ví dụ để dễ hình dung cách thức hoạt động của nó:

Alice muốn gửi trao đổi thông điệp m với Bob trên cơ sở mật mã đường cong elliptic, thì Alice chọn đường cong $E_p(a, b)$ với số nguyên tố p, điểm cơ sở G có bậc n. Đầu tiên, Bob có khóa bí mật $d_B < n$ và khóa công khai $Q_B = d_B G$. Alice biết khóa công khai Q_B của Bob.

Alice mã hóa thông điệp:

- Tạo một số ngẫu nhiên $k < n$. Tính điểm $R = kG$.
- Sau đó tính $P_m \in E(F_P)$ tương ứng với thông điệp m
- Cuối cùng, Alice sẽ gửi cho Bob thông tin C = (C_1, C_2) = (R, $P_m + kQ_B$).

Bob nhận (R, c) từ Alice và tiến hành giải mã:

- Bob tiến hành giải mã lấy $C_2 - d_B C_1 = (P_m + kQ_B) - d_B kG = P_m$. Và từ P_m có thể lấy được thông điệp m.

Điểm an toàn của phương pháp này là dù cho kẻ tấn công biết được R, Q_B, G, $R = kG$ và $Q_B = d_B G$ nhưng không biết k, d_B nên không thể tính được khóa chia sẻ để giải mã. Độ an toàn của phương pháp này dựa trên độ khó tính toán của bài toán logarit rời rạc đường cong elliptic (ECDLP) trong khoa học máy tính được định nghĩa như sau: Đường cong elliptic trên trường hữu hạn F_P và điểm sinh G trên đường cong, với $P \in E(F_P)$, tìm số nguyên k sao cho $P = kG$.

2.4 Thuật toán ECDSA và ứng dụng trong chữ ký số

2.4.1 Sơ lược về thuật toán ECDSA

ECDSA là viết tắt của Elliptic Curve Digital Signature Algorithm - thuật toán sinh chữ ký số dựa trên đường cong Elliptic, là thuật toán mã hoá bất đối xứng được sử dụng để tạo chữ kí số cho dữ liệu, giúp chống lại sự giả mạo cũng như làm sai lệch dữ liệu, cung cấp một phương pháp xác thực mà không ảnh hưởng đến tính bảo mật của dữ liệu gốc. ECDSA được ứng dụng rộng rãi trong rất nhiều lĩnh vực cần tính bảo mật và sự riêng tư dữ liệu, đặc biệt như trong blockchain.

Thuật toán ECDSA hoạt động như sau:

Với đường cong elliptic $E(F_P)$: $y^2 = x^3 + ax + b$ (mod p) trên trường hữu hạn F_P với p là một số nguyên tố và điểm cơ sở G có bậc n. Bob sẽ tiến hành ký số thông điệp m để gửi cho Alice và Alice sẽ nhận và xác thực lại thông tin theo các bước:

Bước 1: Bob tiến hành tạo cặp khóa công khai – khóa riêng tư:

- Chọn khóa riêng tư $d < n$.
- Tính khóa công khai $Q = dG$.

Bước 2: Bob tạo chữ ký, chữ ký sẽ được biểu diễn bởi một cặp (r, s).

- Chọn một số bí mật $k < n$.
- Chọn một điểm $P(x, y) = kG$. Và tính $r = x \bmod n$, nếu $r = 0$ thì ta lặp lại bước chọn k.
- Tính $t = k^{-1} \bmod n$.
- Tính $e = H(m)$ – một hàm băm thông điệp m.
- Tính $s = k^{-1}(e + dr) \bmod n$. Nếu $s = 0$ thì ta lặp lại từ bước chọn k
- Ta thu được chữ ký của thông điệp m là cặp khóa (r, s).

Bước 3: Alice nhận thông tin từ Bob và xác thực lại chữ ký.

- Xác thực r và s là các số nguyên bé hơn n.
- Tính $e = H(m)$
- Tính $w = s^{-1} \bmod n$. Sau đó tính $u_1 = ew$ và $u_2 = rw$.
- Tính điểm $X = (x_1, y_1) = u_1G + u_2G$.
- Nếu X = O, từ chối chữ ký, ngược lại, tính $v = x_1 \bmod n$
- Chấp nhận chữ ký của Bob nếu $v = r$.

2.4.2 Vai trò của ký số ECDSA

- Trước khi ký: Giao dịch chỉ là một tập hợp dữ liệu, ai cũng có thể tạo ra.
- Sau khi ký: Giao dịch mang dấu ấn duy nhất của người sở hữu private key. Không ai khác có thể giả mạo.
- Nếu không ký: Bất kỳ ai cũng có thể gửi giao dịch lên blockchain, gây mất an toàn.
- Ký xong: Blockchain xác thực được đúng người gửi, đảm bảo tính toàn vẹn và xác thực của dữ liệu.

CHƯƠNG 3

XÂY DỰNG ỨNG DỤNG SỬ DỤNG BLOCKCHAIN TRONG XÁC THỰC THÔNG TIN BẰNG CẤP

3.1 Phân tích thiết kế ứng dụng xác thực thông tin bằng cấp sử dụng blockchain

3.1.1 Cấu trúc một khối trong hệ thống

Một khối sẽ bao gồm các thông tin như sau:

- Số thứ tự của khối trong chuỗi (khối đầu tiên là 0).
- Tiêu đề khối (Block Header):
  - Version: Phiên bản phần mềm hoặc định dạng block.
  - Timestamp: Thời gian block được tạo.
  - Previous Hash: Mã hash của khối trước (liên kết khối với chuỗi).
  - Merkle Root (nếu có nhiều chứng chỉ trong một khối): là mã băm tổng hợp từ tất cả các dữ liệu trong khối thông qua cây Merkle.
  - Difficulty/Target: Mức độ khó của bài toán hash (nếu dùng PoW)
  - Nonce (nếu dùng PoW): Một số để tìm ra hash hợp lệ. (tuy nhiên với ứng dụng mẫu xây dựng trên môi trường local không đào, có thể bỏ qua hoặc đặt mặc định).
  - Hash của chính block: Hash SHA-256 được tính từ toàn bộ nội dung block (ngoại trừ trường hash này).
- Dữ liệu khối:
  - Thông tin chứng chỉ: Bao gồm tên sinh viên, loại văn bằng, ngày cấp,...
  - Mã hash của tài liệu PDF (lưu trên IPFS).

3.1.2 Mục tiêu và yêu cầu hệ thống

Hệ thống ứng dụng blockchain trong xác thực thông tin có các mục tiêu chính:

- Đảm bảo tính toàn vẹn và nguồn gốc của chứng chỉ (bằng đại học).
- Lưu trữ mã hash của bằng trên blockchain kèm theo tham chiếu tới tài liệu thật trên IPFS.

- Cung cấp giao diện tạo chứng chỉ cho phía nhà trường và giao diện xác thực chứng chỉ.

Các bên liên quan:

- Tổ chức giáo dục (Institute)
  - Phát hành chứng chỉ
  - Quản lý và theo dõi chứng chỉ đã phát hành
  - Có thể thu hồi chứng chỉ và cấp phát lại nếu cần
- Người xác thực (Verifier)
  - Kiểm tra tính hợp lệ của chứng chỉ
  - Xem thông tin chi tiết của chứng chỉ

Yêu cầu chức năng:

- Tạo chứng chỉ PDF từ giao diện.
- Lưu hash của chứng chỉ PDF trên IPFS.
- Lưu mã hash và CID (Content Identifier) - một mã định danh duy nhất trong hệ thống IPFS vào blockchain.
- Cho phép truy vấn và xác thực chứng chỉ.

Yêu cầu phi chức năng:

- Bảo mật.
- Minh bạch.
- Dễ sử dụng và xác thực nhanh.

3.1.3 Công nghệ sử dụng

- Front-end: Streamlit (Framework Python đơn giản để tạo giao diện web: giao diện người dùng, xử lý tương tác người dùng, hiển thị thông tin chứng chỉ).
- Back-end: Python (giúp xử lý logic nghiệp vụ, tương tác với blockchain, quản lý dữ liệu) và Firebase (giúp lưu thông tin, hỗ trợ xác thực người dùng và truy vấn dữ liệu phụ trợ).
- Smart Contract: ngôn ngữ Solidity (giúp lưu trữ thông tin chứng chỉ, xác thực tính hợp lệ, quản lý quyền truy cập), triển khai trên mạng Ethereum testnet (ganache-cli) (giúp lưu trữ dữ liệu phi tập trung, đảm bảo tính minh bạch, bảo mật thông tin).

- Lưu trữ bản PDF chứng chỉ: IPFS (Pinata – hệ thống lưu trữ phân tán, trả về CID duy nhất cho mỗi tệp)
- Xác thực và tương tác với blockchain: Web3.py – thư viện Python giúp tương tác với Ethereum và smart contract.

3.1.4 Giao diện người dùng

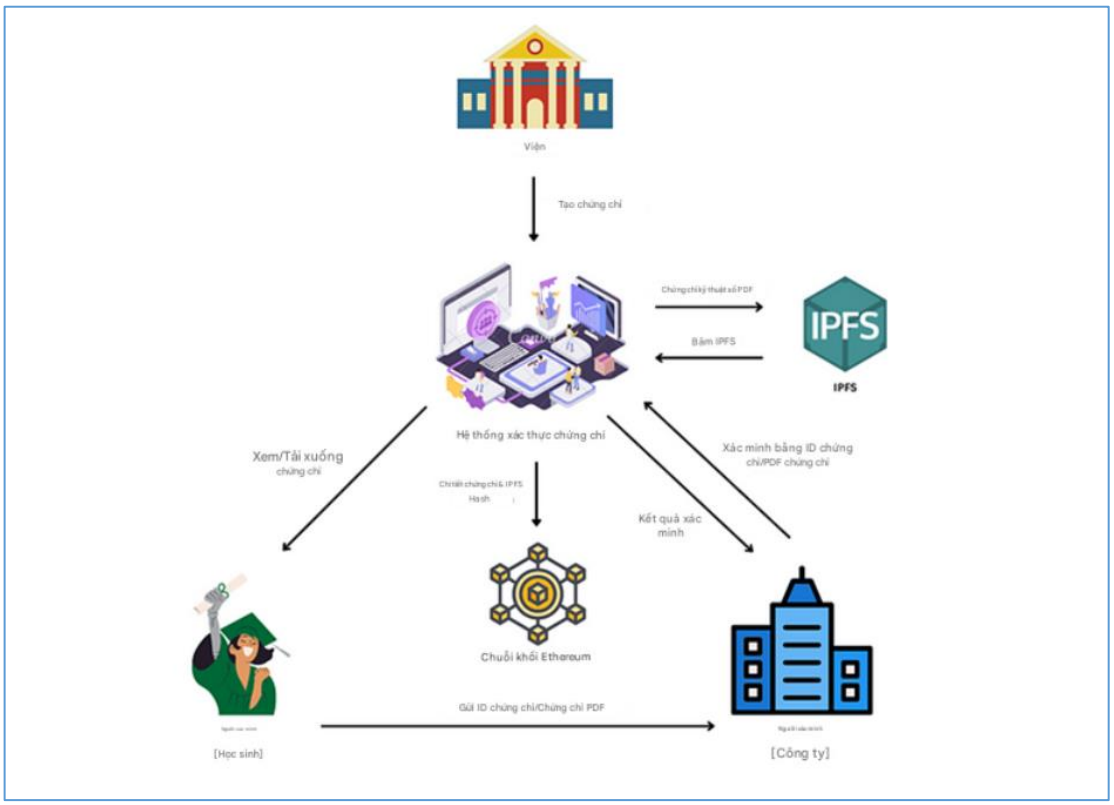
Ứng dụng được thiết kế với giao diện người dùng thân thiện, trực quan và dễ sử dụng, hướng đến trải nghiệm mượt mà cho cả hai nhóm người dùng chính: Institute (tổ chức phát hành chứng chỉ) và Verifier (đơn vị xác thực chứng chỉ). Giao diện được phân chia rõ ràng theo vai trò, giúp người dùng dễ dàng truy cập các chức năng tương ứng. Ngay từ trang chủ, người dùng có thể lựa chọn vai trò của mình để truy cập vào không gian làm việc phù hợp.

- Đối với vai trò Institute, sau khi đăng nhập, người dùng có thể thực hiện đầy đủ các nghiệp vụ liên quan đến quản lý chứng chỉ, bao gồm phát hành chứng chỉ mới, quản lý danh sách chứng chỉ hiện có, thu hồi, cấp phát lại hoặc xem thông tin chi tiết của từng chứng chỉ. Các thao tác được trình bày theo dạng biểu mẫu và danh sách, dễ theo dõi và thao tác.
- Với vai trò Verifier, người dùng không cần đăng nhập mà vẫn có thể truy cập nhanh vào chức năng xác thực chứng chỉ thông qua mã định danh hoặc mã QR. Hệ thống sẽ hiển thị đầy đủ thông tin liên quan đến chứng chỉ và người sở hữu để phục vụ quá trình kiểm tra, xác minh. Giao diện Verifier được tối ưu cho thao tác nhanh, phù hợp với nhu cầu xác thực tại chỗ hoặc trong các tình huống kiểm tra thực tế.

Tổng thể, giao diện người dùng của ứng dụng đảm bảo sự rõ ràng, đơn giản nhưng đầy đủ chức năng, giúp người dùng thực hiện công việc hiệu quả mà không gặp trở ngại về mặt thao tác hay điều hướng.

3.2 Phân tích sơ đồ luồng chức năng của ứng dụng

3.2.1 Sơ đồ luồng hoạt động của ứng dụng



Hình 3-1 Mô hình luồng hoạt động của ứng dụng

Tạo chứng chỉ (ở phía trường):

- Nhập thông tin chứng chỉ: Trường nhập thông tin: tên sinh viên, khóa học, tổ chức, v.v.
- Sinh file PDF chứng chỉ: Hệ thống tạo file PDF chứa thông tin trên.
- Upload file PDF lên IPFS: File PDF được upload lên IPFS (một hệ thống lưu trữ phi tập trung). Sau khi upload, IPFS trả về một hash (ví dụ: QmXyz...), gọi là IPFS hash. Hash này là duy nhất cho nội dung file PDF đó.
- Tạo mã định danh chứng chỉ (certificate_id): Hệ thống sẽ băm (hash) các thông tin như UID, tên, khóa học, tổ chức... để tạo ra một mã định danh duy nhất cho chứng chỉ (thường dùng SHA256).
- Chuẩn bị dữ liệu để ghi lên blockchain: Dữ liệu gồm: certificate_id, UID, tên, khóa học, tổ chức, IPFS hash.

Gửi giao dịch lên blockchain:

- Gọi hàm generateCertificate trên smart contract: Hệ thống gọi hàm này, truyền vào các thông tin ở trên.
- Ký số giao dịch bằng ECDSA: Trước khi gửi lên blockchain, giao dịch này sẽ được ký số bằng ECDSA: Web3 lấy private key của tài khoản trường (admin). Tạo một bản hash của nội dung giao dịch (gồm dữ liệu, địa chỉ contract, gas, v.v.). Dùng private key để ký bản hash này bằng thuật toán ECDSA, tạo ra chữ ký số.
- Giao dịch + chữ ký số được gửi lên mạng Ethereum.
- Node blockchain xác thực chữ ký. Node nhận giao dịch, kiểm tra chữ ký ECDSA. Nếu đúng là private key của trường đã ký, giao dịch hợp lệ và được ghi vào blockchain. Nếu không đúng, giao dịch bị từ chối.
- Giao dịch được ghi vào blockchain. Thông tin chứng chỉ (bao gồm IPFS hash) được lưu vĩnh viễn trên blockchain. Không ai có thể sửa/xóa thông tin này, trừ khi thực hiện giao dịch mới (ví dụ: thu hồi).

Xác thực chứng chỉ:

- Người kiểm tra nhập mã chứng chỉ: Hệ thống truy vấn smart contract bằng certificate_id.
- Smart contract trả về thông tin: Trả về thông tin chứng chỉ, trạng thái (đã thu hồi hay chưa), IPFS hash.
- Kiểm tra file PDF gốc: Dùng IPFS hash để lấy lại file PDF gốc từ IPFS. So sánh thông tin trên blockchain và file PDF.

3.2.2 Thiết kế hợp đồng thông minh

Trong hệ thống xác thực chứng chỉ sử dụng blockchain, hợp đồng thông minh (smart contract) đóng vai trò trung tâm trong việc lưu trữ, quản lý và xác minh các chứng chỉ điện tử. Hợp đồng thông minh được lập trình bằng ngôn ngữ Solidity và triển khai trên nền tảng Ethereum hoặc các blockchain tương thích như Binance Smart Chain hoặc Polygon, cho phép hệ thống hoạt động một cách minh bạch, an toàn và không thể sửa đổi.

Hợp đồng thông minh được thiết kế để lưu trữ các thông tin cơ bản liên quan đến chứng chỉ, bao gồm:

- ID chứng chỉ: Mã định danh duy nhất của mỗi chứng chỉ.
- Tên người nhận: Họ và tên của người được cấp chứng chỉ.

- Ngành học, hình thức, xếp loại: Thông tin học thuật liên quan đến nội dung chứng chỉ.
- Ngày cấp: Thời điểm chứng chỉ được phát hành.
- Tên tổ chức cấp: Tên trường hoặc tổ chức chịu trách nhiệm phát hành chứng chỉ.
- Mã hash IPFS: Giá trị băm đại diện cho tệp chứng chỉ lưu trữ trên hệ thống IPFS để đảm bảo tính toàn vẹn và có thể truy cập công khai.

Để đáp ứng các chức năng quản lý chứng chỉ, hợp đồng thông minh sẽ triển khai các hàm sau:

- generateCertificate(): Được sử dụng khi nhà trường tạo mới một chứng chỉ. Hàm này sẽ nhận các tham số đầu vào là thông tin chi tiết của chứng chỉ và lưu trữ chúng vào blockchain. Chỉ tài khoản có quyền (admin) mới có thể thực hiện hành động này.
- revokeCertificate(): Được sử dụng để thu hồi một chứng chỉ đã cấp trong trường hợp có sai sót hoặc lý do khác. Hệ thống sẽ đánh dấu chứng chỉ tương ứng là "đã thu hồi" nhưng vẫn lưu lại lịch sử trên blockchain để đảm bảo tính minh bạch.
- reissueCertificate(): Cho phép cấp phát lại một chứng chỉ mới dựa trên chứng chỉ cũ đã bị thu hồi. Thông tin mới sẽ được lưu dưới một ID mới hoặc cập nhật lại bản ghi hiện tại tùy theo chính sách triển khai.
- getCertificate(): Cho phép bất kỳ người dùng nào (verifier) truy cập thông tin chứng chỉ dựa trên mã ID. Hàm trả về toàn bộ dữ liệu liên quan đến chứng chỉ.
- isVerified(): Hàm này cho phép kiểm tra tính xác thực và trạng thái hiện tại của chứng chỉ (còn hiệu lực hay đã thu hồi). Hàm này hỗ trợ các đơn vị tuyển dụng, tổ chức kiểm tra độ tin cậy của thông tin.

Để đảm bảo an toàn cho hệ thống, hợp đồng thông minh được thiết kế với cơ chế phân quyền, trong đó:

- Chỉ admin (trường cấp) mới có quyền gọi các hàm như generateCertificate(), revokeCertificate() và reissueCertificate().
- Các verifier (người kiểm chứng) chỉ có quyền gọi các hàm đọc như getCertificate() và isVerified().

Việc áp dụng hợp đồng thông minh trong hệ thống giúp đảm bảo tính minh bạch, chống giả mạo và dễ dàng xác minh, đồng thời tận dụng tính bất biến và phi tập trung của blockchain để tăng độ tin cậy trong quá trình xác thực chứng chỉ.

CHƯƠNG 4

TRIỂN KHAI THỰC NGHIỆM VÀ ĐÁNH GIÁ KẾT QUẢ

4.1 Triển khai thực nghiệm

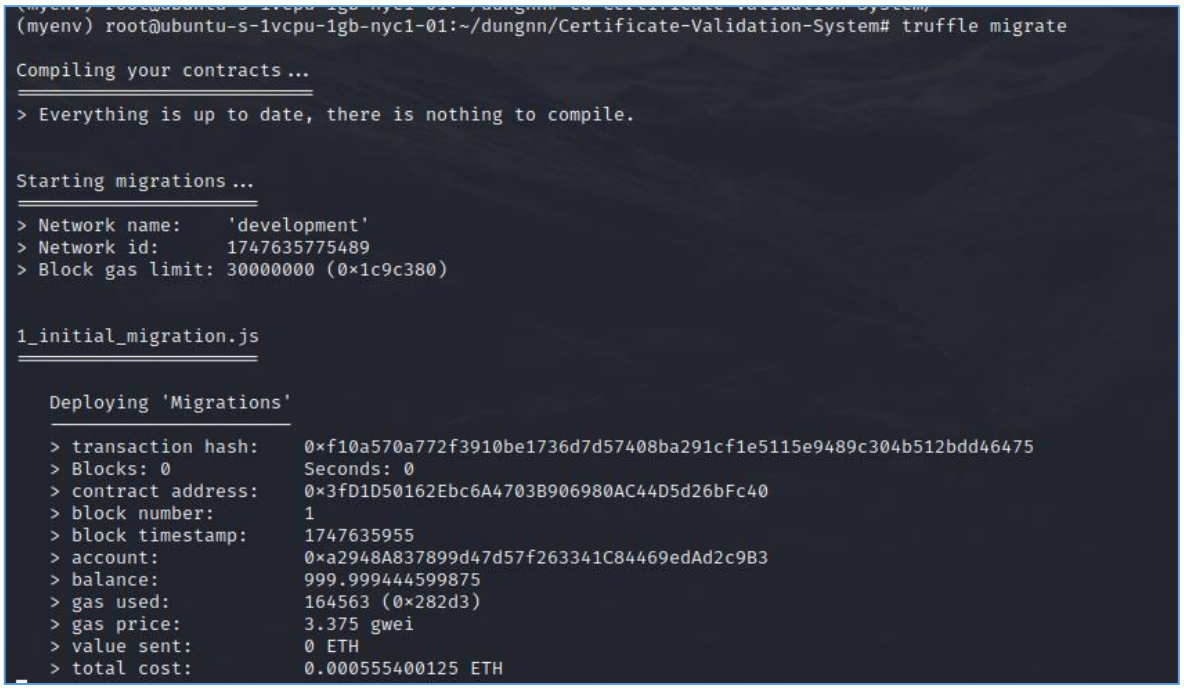
Ta tạo một con máy ảo ubuntu trên DigitalOcean để có thể thực hiện public website. Sau khi cài đặt và cấu hình dự án trên máy ảo này, ta thực hiện các bước để khởi chạy dự án bằng ba câu lệnh như sau:

– Đầu tiên khởi động mạng blockchain Ethereum testnet bằng ganache-cli:

```
(myenv) root@ubuntu-s-1vcpu-1gb-nyc1-01:~/dungnn/Certificate-Validation-System# ganache-cli -h 127.0.0.1 -p 8545
ganache v7.9.2 (@ganache/cli: 0.10.2, @ganache/core: 0.10.2)
Starting RPC server

Available Accounts
==================
(0) 0x2948A837899d47d57f263341C84469edAd2c9B3 (1000 ETH)
(1) 0xCC9087A9A721e48b00e958e5362503b8a7Ff4816 (1000 ETH)
(2) 0x3C9de663FfD2525F35d242a12EF9c0F9c6C9a707 (1000 ETH)
(3) 0xf07A97414fECBb15A2d5887871CE0139BDe6aBb8 (1000 ETH)
(4) 0x7eb91f0ad24abf9310398709fe8f21475C2ea0f0 (1000 ETH)
(5) 0x64De1D95aD60D03fBf5a4bBAa9A5Bb3F164D803d (1000 ETH)
(6) 0xb2f8082b60768c3A8E5E8306360d033143f2ba4b (1000 ETH)
(7) 0x43eEDB1f066F26B901e9bb0D34294cebaa99A6fA (1000 ETH)
(8) 0x2A2ee43A8370eb86D17e2d2EE460fc248E59dB00 (1000 ETH)
(9) 0x9EB93D94a39A10454CE6Ea9b0c05c9Bd7C52Fd95 (1000 ETH)

Private Keys
==================
(0) 0x1e26e8c7a9774977113c899981e2587b29f795cf6574eba3672f806c2bc01b38
(1) 0x7df5478a8328e0a99da834c8577cbb7a72ffa9cf7130967dc1ca98744b4b6e6a
(2) 0xeb53b6d563b9a8b38f96ed18f7014433e96f4e7888764adfea5889c5b3c20ad9
(3) 0xdbdfb5d56ddcb1b7a8cca7b3e60c924c1c9584021abc1b20c4d6745402b0ed08
(4) 0xd92e9d0f3f5fa86163dda8873d92710c19e96460d389d2d33c7212aadde3040a
(5) 0xcbe541c039e100e8cd265e5b030959bfc14639cee6c532d3dc5e7e849f44c37d
(6) 0x66962add132dd5f9beee1a61a9b07719de6b7feffc6c06676f39e2030f949133
(7) 0xa2f22b7d31dd73fa94ab6f93fc10a720a01703f9701d20fadad4ccf0f5a2d2fa
(8) 0xf513e8b304addd6f9b1967ce87a53ea758031516ccd97ee978cbb70d355ab9f5
(9) 0x378bfea571e9fb00f80bc34ed7ebd0f795f49541445a3c4f5959e6ffa185031c

HD Wallet
==================
Mnemonic:      alarm else lottery fork uncover broom problem combine churn capital bean borrow
Base HD Path:  m/44'/60'/0'/0/{account_index}

Default Gas Price
==================
2000000000
```

Hình 4-1 Khởi động ganache-cli

– Sau đó thực hiện deploy hợp đồng thông minh bằng truffle:

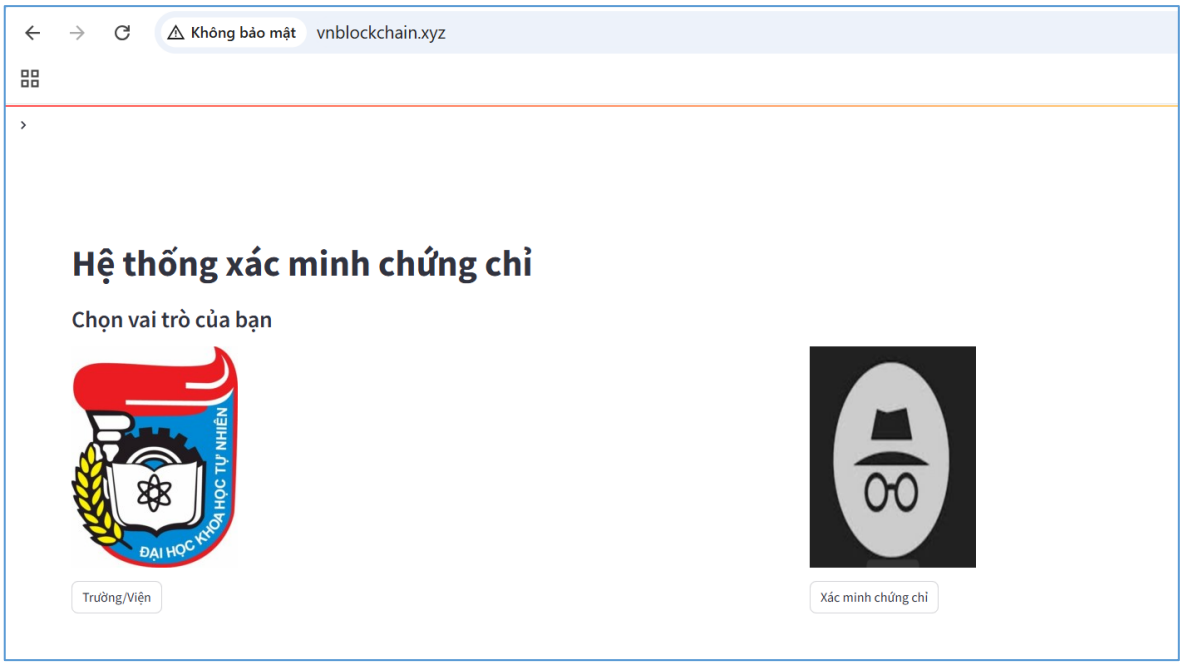


Hình 4-2 Triển khai hợp đồng thông minh lên mạng blockchain

– Cuối cùng thực hiện khởi chạy webGUI bằng streamlit:

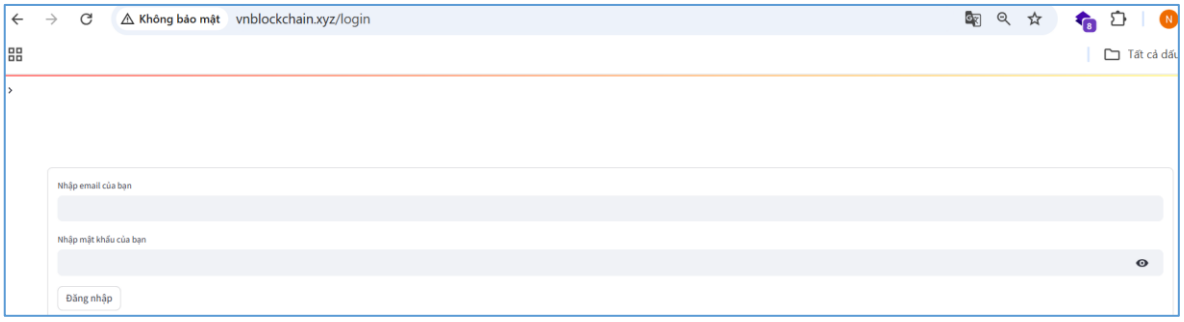
Hình 4-3 Khởi chạy ứng dụng webGUI

Vậy là ta đã thực hiện triển khai thành công website, giờ ta sẽ có thể truy cập dự án thông qua domain http://vnblockchain.xyz/. Source code của dự án được gắn trong đường dẫn: https://github.com/nguyenngocdung18/KLTN. Sau khi khởi chạy dự án thành công sẽ truy cập tới giao diện webGUI của ứng dụng, tại đây ta sẽ tiến hành chọn vai trò là nhà trường hay người xác minh.



Hình 4-4 Màn hình giao diện chính

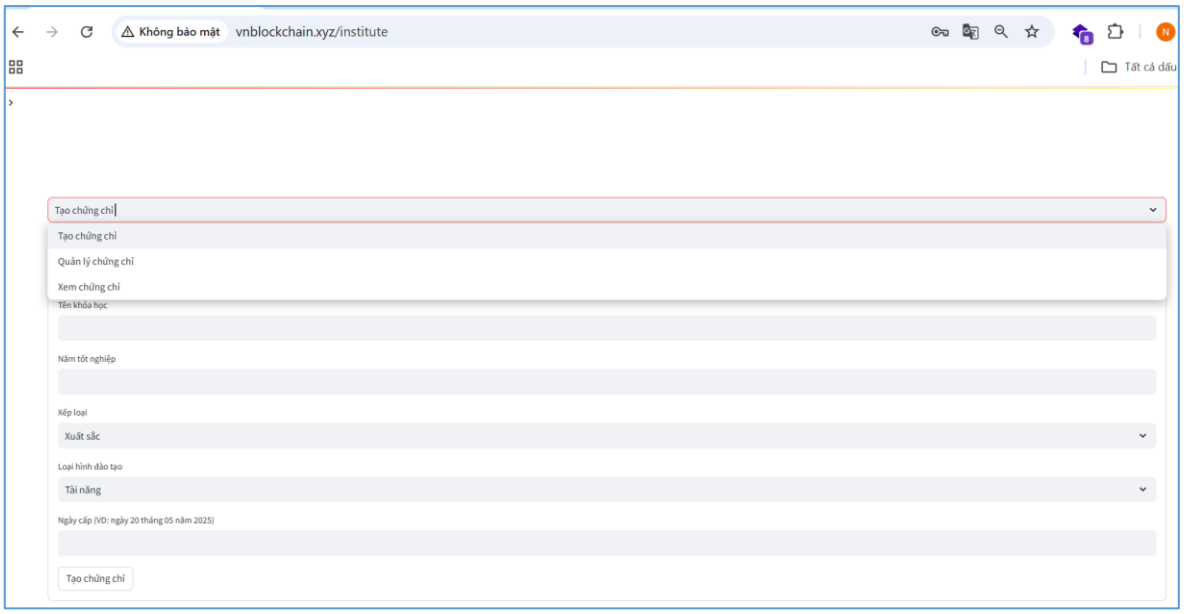
Với vai trò là nhà trường, ta sẽ được điều hướng tới trang đăng nhập



Hình 4-5 Màn hình đăng nhập với vai trò là nhà trường

Sau khi đăng nhập thành công, người dùng được chuyển hướng tới giao diện quản trị có 3 chức năng chính đó là:

- Tạo, phát hành chứng chỉ.
- Quản lý chứng chỉ.
- Xem chứng chỉ.



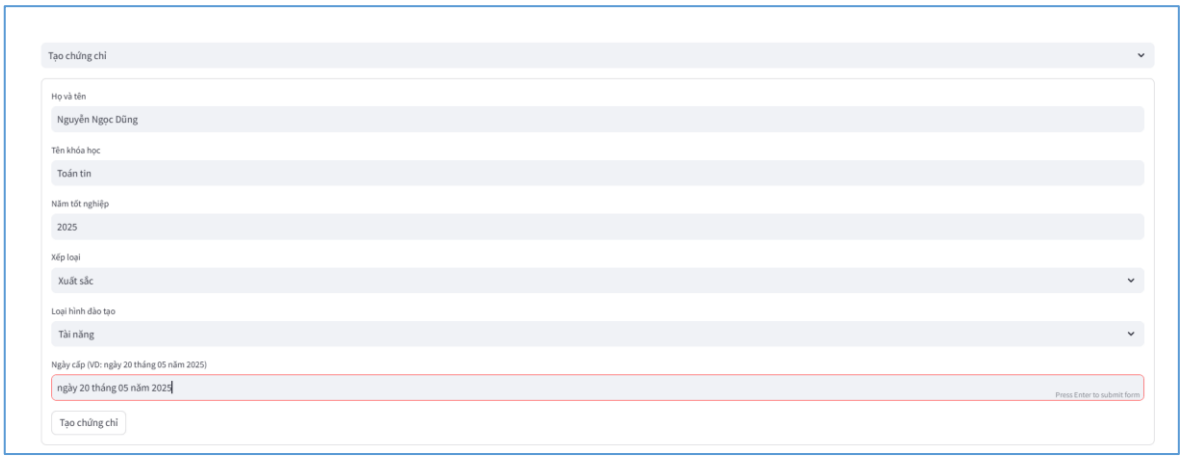
Hình 4-6 Giao diện quản trị của nhà trường

4.2 Đánh giá kết quả thực nghiệm

4.2.1 Xây dựng các kịch bản để kiểm tra.

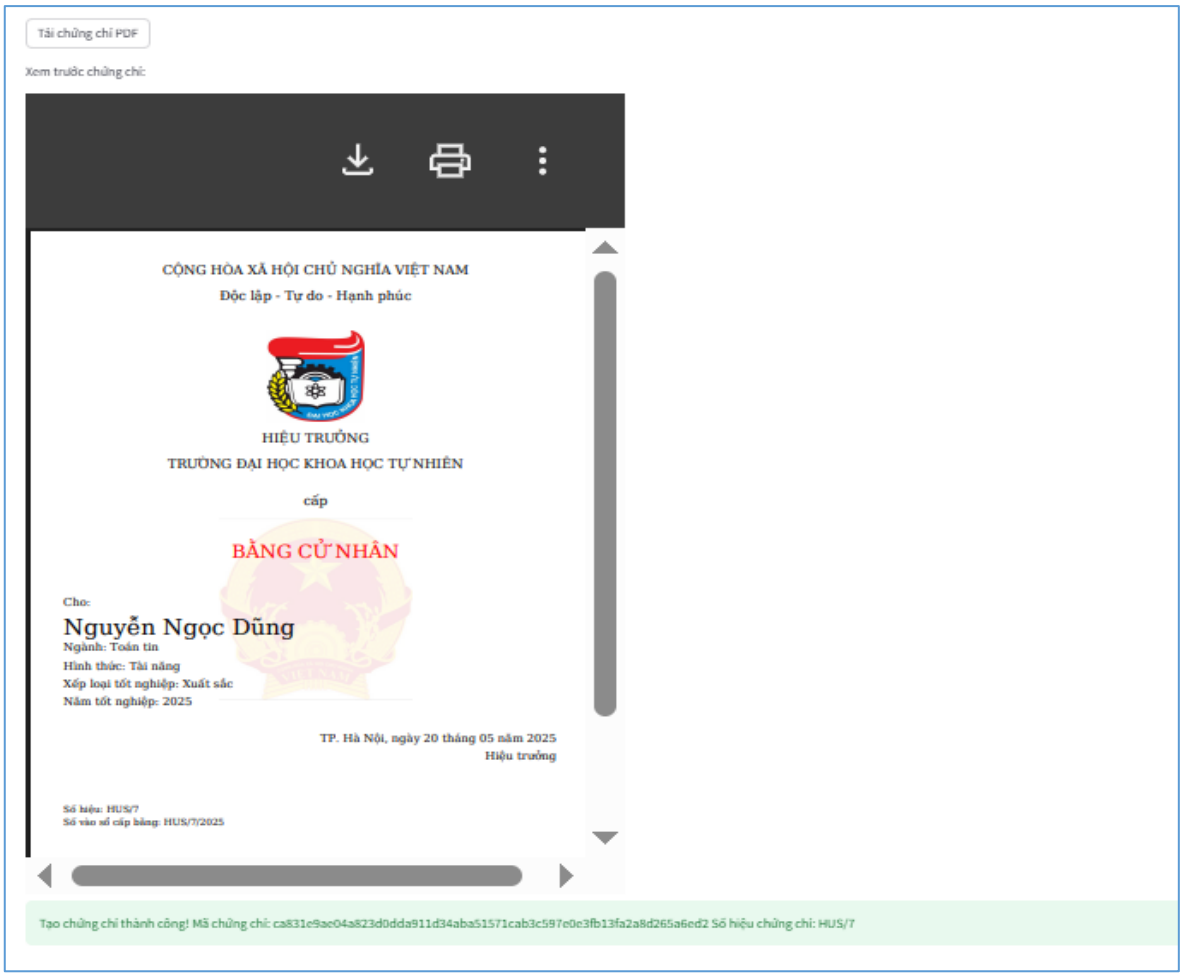
- Kịch bản 1: Nhà trường thực hiện cấp bằng cho cử nhân mới.

Tại chức năng tạo, phát hành chứng chỉ: Sau khi điền đây đủ thông tin gồm họ và tên, ngành học, năm tốt nghiệp, xếp loại bằng, hình thức, ngày tốt nghiệp. Sau đó ấn "Tạo chứng chỉ" để tạo.



Hình 4-7 Nhà trường tạo và cấp phát chứng chỉ

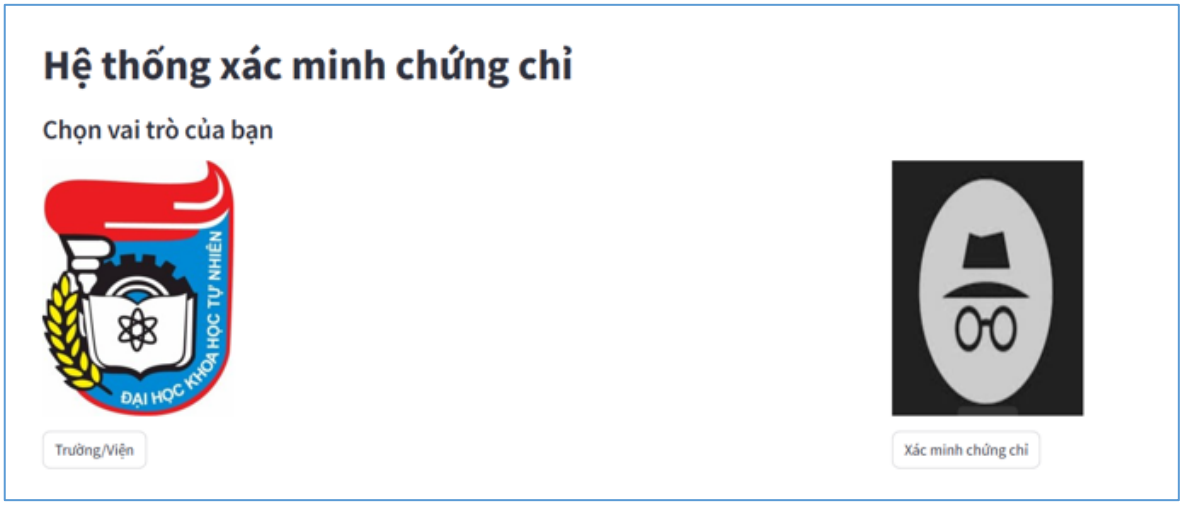
Sau khi tạo thành công, hệ thống sẽ tạo một bản PDF chứng chỉ và hiển thị trên màn hình giao diện cùng với số hiệu chứng chỉ. Ngoài ra cũng có kèm thêm cả chức năng tải xuống bản PDF đó.



Hình 4-8 Cấp phát chứng chỉ thành công

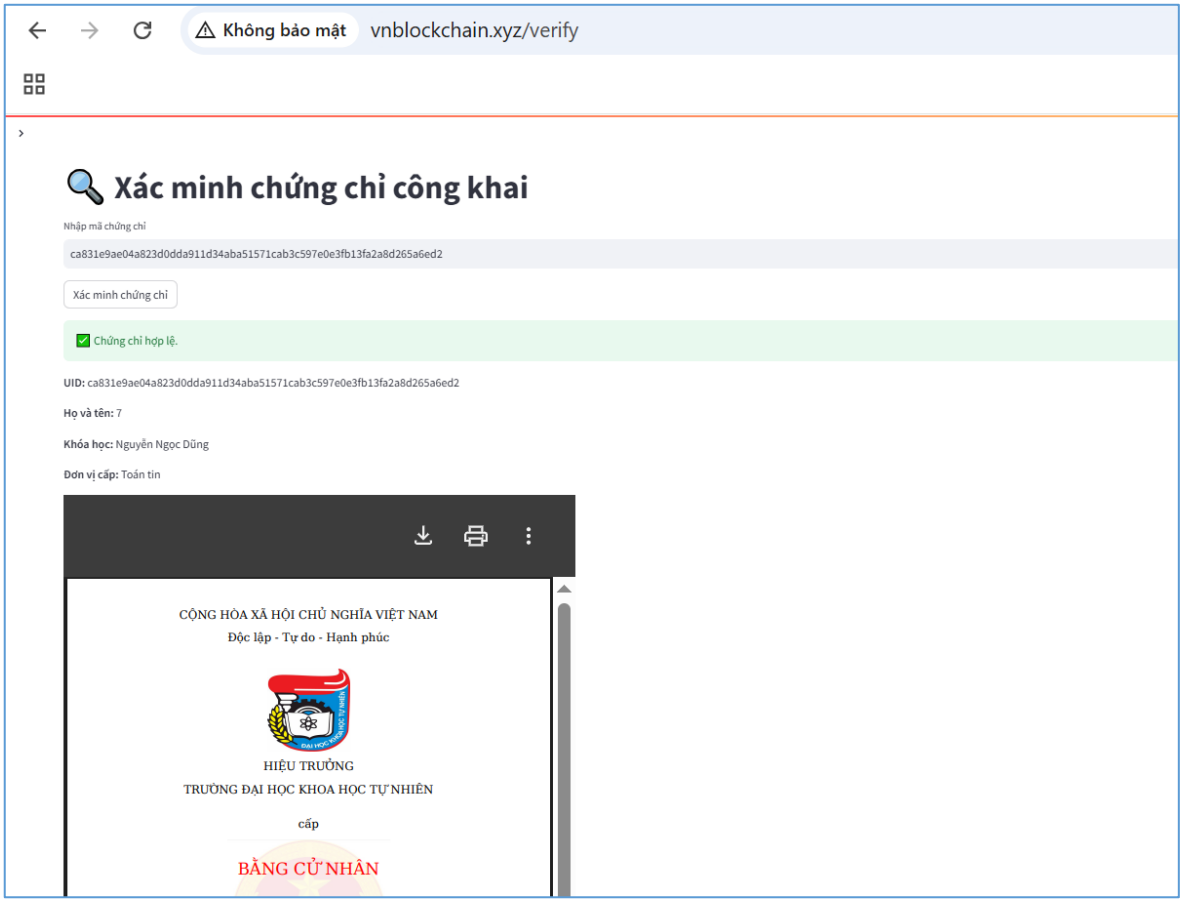
– Kịch bản 2: Người xác minh thực hiện xác minh chứng chỉ

Trong trường hợp mọi người muốn xác minh, kiểm tra lại chứng chỉ đó. Chọn vai trò "Xác minh chứng chỉ".



Hình 4-9 Màn hình giao diện chính để chọn vai trò

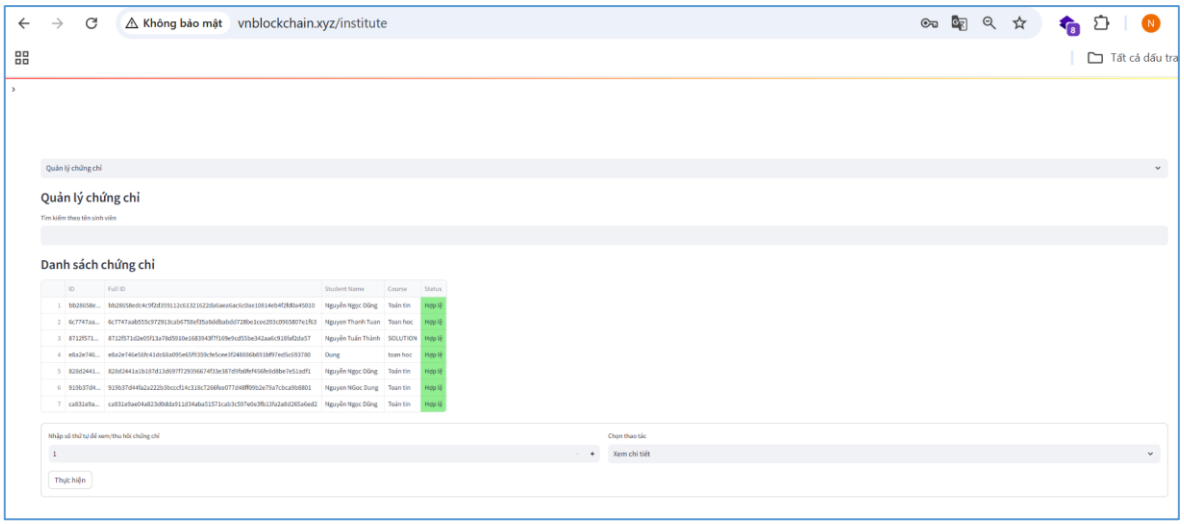
Sau đó nhập vào id của chứng chỉ và thực hiện ấn "Xác minh chứng chỉ". Nếu chứng chỉ hợp lệ, thông tin chi tiết cũng như bản PDF của chứng chỉ sẽ hiện ra.



Hình 4-10 Người xác minh thực hiện xác minh chứng chỉ thành công

– Kịch bản 3: Nhà trường quản lí chứng chỉ.
  - Kịch bản 3.1: Xem danh sách các chứng chỉ đã được cấp phát.

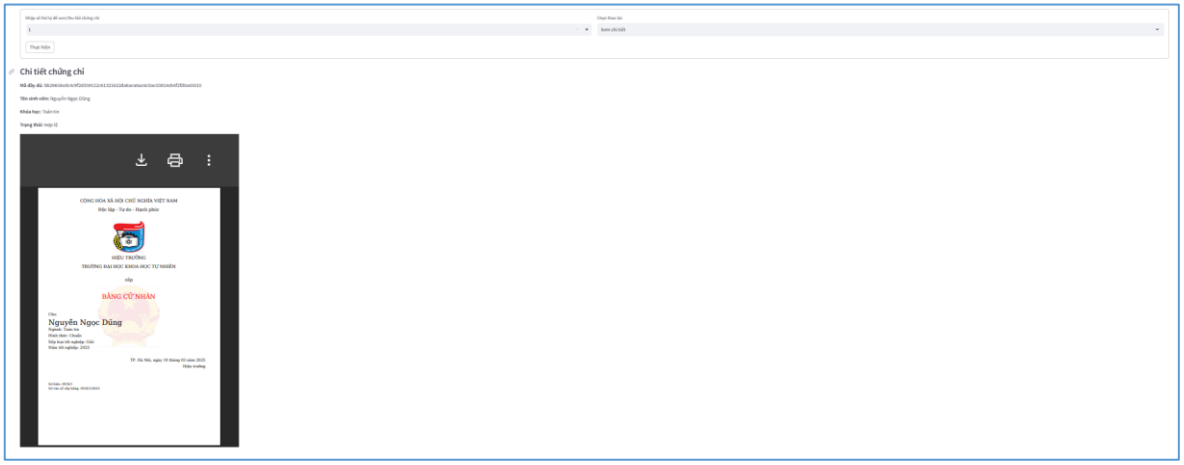
Truy cập vào chức năng quản lí chứng chỉ. Tại đây, người quản lí có thể xem được danh sách chứng chỉ đã cấp phát cũng như thực hiện xem chi tiết, hủy bỏ và cấp phát lại bằng cấp, chứng chỉ.



Hình 4-11 Giao diện quản lí các chứng chỉ đã được cấp phát

- Kịch bản 3.2: Xem chi tiết thông tin chứng chỉ.

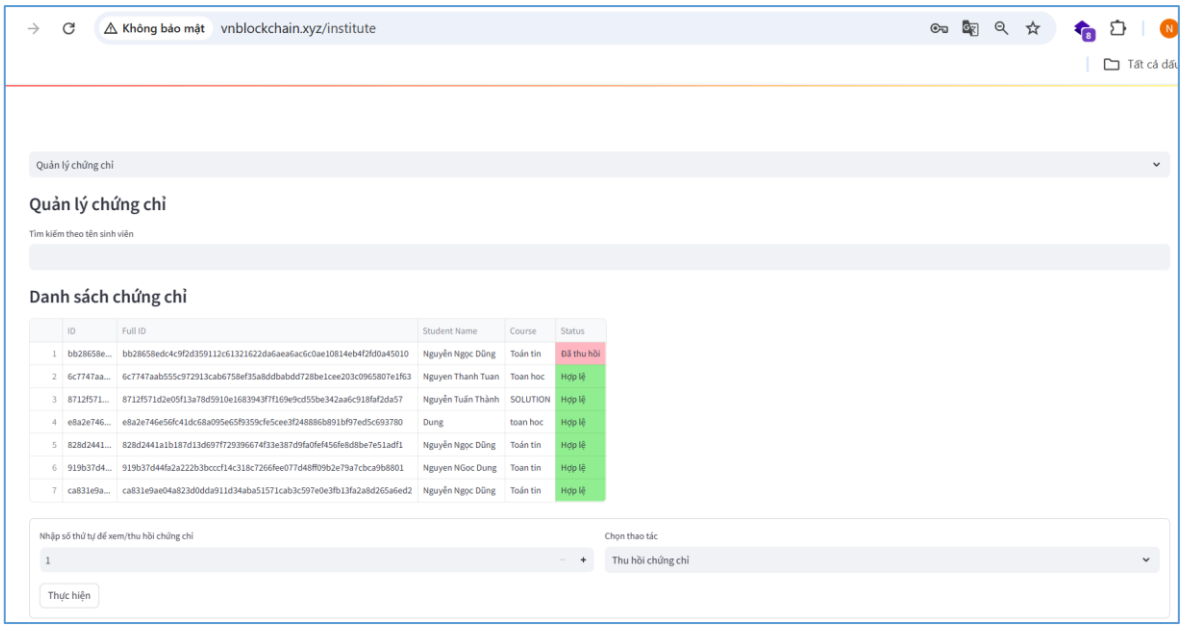
Thực hiện chọn số thứ tự dòng của chứng chỉ muốn xem chi tiết, chọn hành động "Xem chi tiết" và ấn "Thực hiện". Thông tin chi tiết về tình trạng chứng chỉ và bản PDF của chứng chỉ sẽ hiện ra.



Hình 4-12 Xem thông tin chi tiết của chứng chỉ

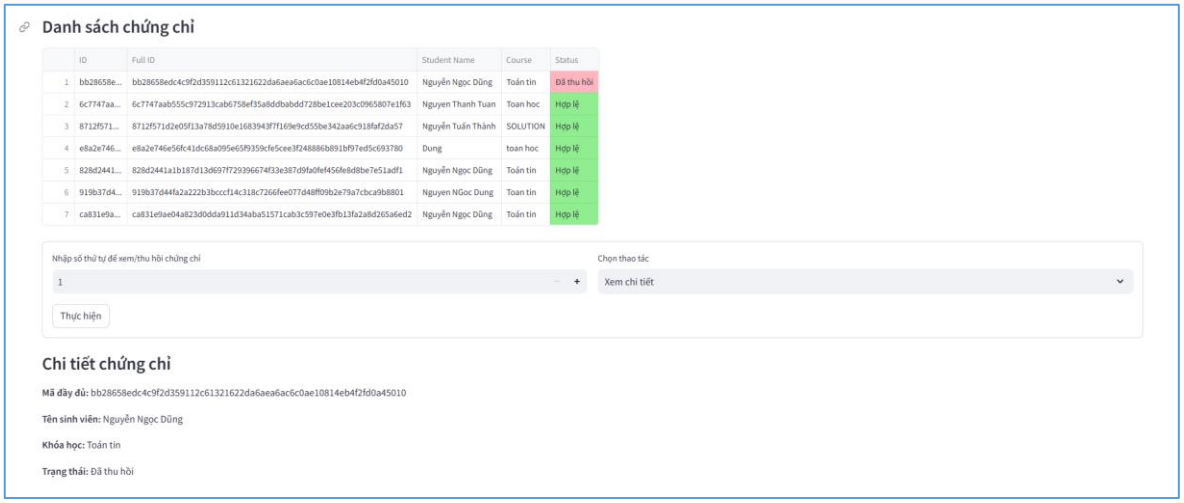
- Kịch bản 3.3: Nhà trường thực hiện hủy bằng cấp.

Với trường hợp nhà trường muốn thực hiện thu hồi lại bằng cấp, chứng chỉ. Chọn số dòng của chứng chỉ muốn thu hồi và hành động "Thu hồi chứng chỉ" rồi ấn "Thực hiện".



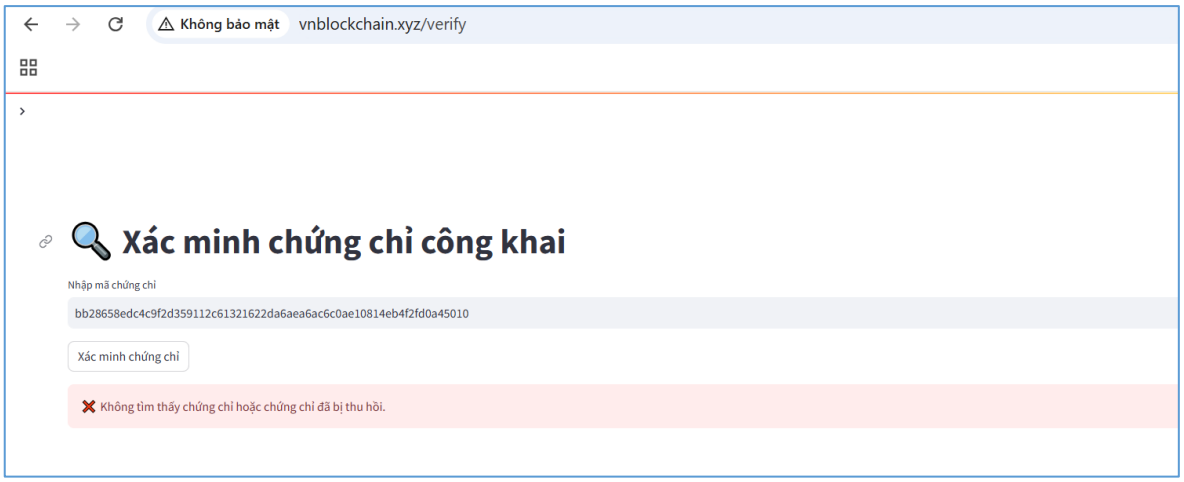
Hình 4-13 Nhà trường thực hiện thu hồi chứng chỉ

Trạng thái của chứng chỉ sẽ chuyển từ "Hợp lệ" về "Đã thu hồi". Khi đó không thể thực hiện truy vấn cũng như xem thông tin của chứng chỉ nữa.



Hình 4-14 Chứng chỉ bị thu hồi thành công

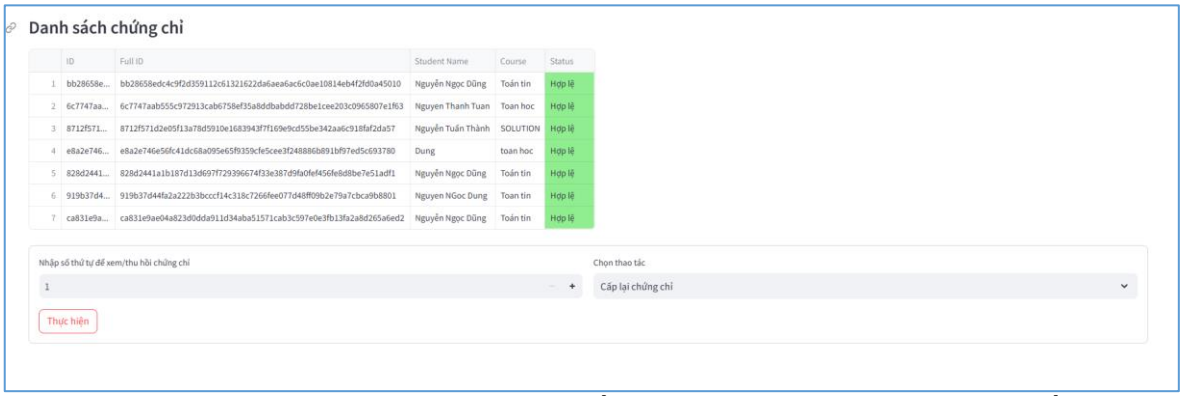
Từ phía của những người xác minh chứng chỉ cũng sẽ không hiển thị thông tin về chứng chỉ nữa.



Hình 4-15 Chứng chỉ bị thu hồi sẽ không hiển thị khi xác minh

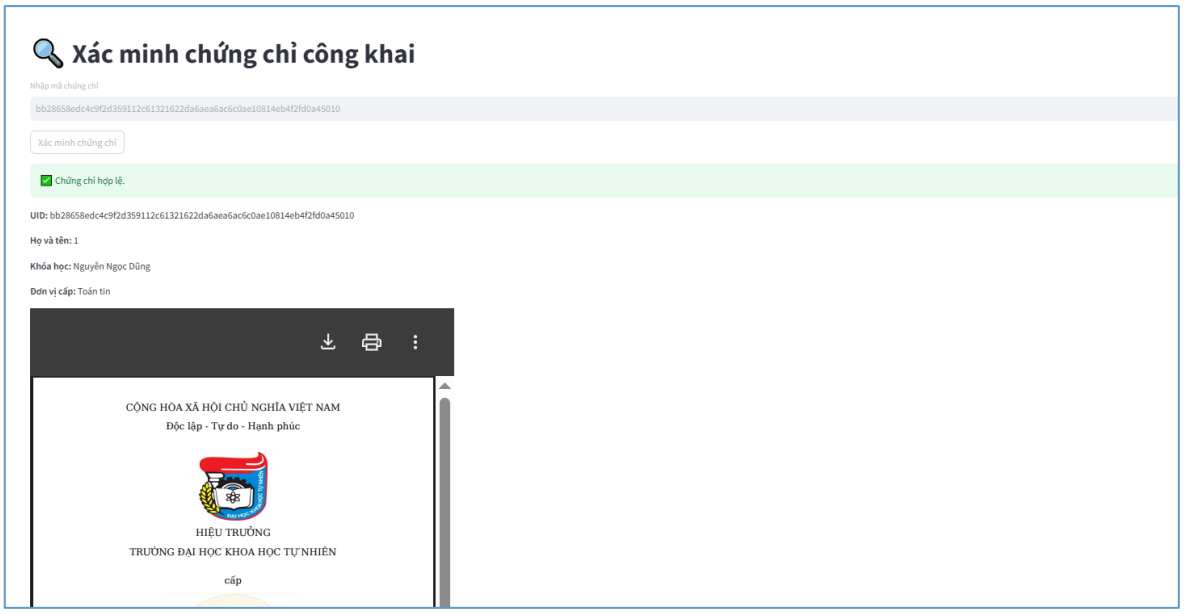
- Kịch bản 3.4: Nhà trường thực hiện cấp phát lại chứng chỉ.

Trong trường hợp nhà trường muốn cấp phát lại chứng chỉ đã bị thu hồi trước đó. Thực hiện chọn số dòng của chứng chỉ đã bị thu hồi và chọn hành động "Cấp phát lại chứng chỉ" và ấn "Thực hiện". Sau đó, trạng thái của chứng chỉ sẽ chuyển từ "Đã thu hồi" về "Hợp lệ".



Hình 4-16 Nhà trường thực hiện cấp phát lại chứng chỉ đã bị thu hồi

Sau khi cấp phát lại chứng chỉ thành công, người xác minh hoàn toàn có thể xem được thông tin chi tiết của chứng chỉ một cách bình thường.



Hình 4-17 Chứng chỉ được cấp phát lại đã hoạt động bình thường

4.2.2 Đánh giá và so sánh với hình thức xác thực truyền thống

Trong quá trình thực nghiệm, hệ thống xác thực chứng chỉ dựa trên công nghệ blockchain kết hợp với IPFS và hợp đồng thông minh đã được triển khai thành công và cho thấy nhiều ưu điểm vượt trội so với các phương pháp xác thực truyền thống. Hệ thống được xây dựng với chức năng cấp phát và xác thực chứng chỉ học tập dưới dạng tệp PDF thông qua các bước chính:

- Chứng chỉ được tạo dưới dạng file PDF, sau đó được tải lên hệ thống IPFS.
- Mã hash IPFS được ghi vào blockchain thông qua một hợp đồng thông minh viết bằng ngôn ngữ Solidity.
- Khi cần xác thực, người dùng hoặc bên thứ ba chỉ cần tra cứu mã hash từ blockchain để truy xuất và kiểm tra chứng chỉ từ IPFS.

Kết quả cho thấy:

- Dữ liệu được lưu trữ một cách phi tập trung, đảm bảo không phụ thuộc vào một máy chủ trung tâm.
- Tính toàn vẹn của dữ liệu được bảo đảm tuyệt đối do mã hash IPFS thay đổi nếu nội dung tệp thay đổi.
- Quá trình xác thực diễn ra nhanh chóng, chỉ cần nhập địa chỉ hoặc mã hash.

So sánh với hình thức xác thực bằng cấp truyền thống:

Tiêu chí	Hệ thống truyền thống	Hệ thống dựa trên blockchain
Tính toàn vẹn dữ liệu	Dễ bị chỉnh sửa hoặc giả mạo chứng chỉ nếu không có biện pháp bảo mật tốt	Dữ liệu đã ghi trên blockchain và IPFS không thể thay đổi, đảm bảo tính toàn vẹn
Tốc độ xác minh	Phụ thuộc vào con người, phải liên hệ nhà trường hoặc tổ chức cấp chứng chỉ	Xác minh nhanh chóng, chỉ cần truy cập blockchain và IPFS
Khả năng xác thực từ xa	Giới hạn – cần qua các bước xác minh qua email, công văn, hoặc gọi điện	Có thể xác minh mọi lúc, mọi nơi, chỉ cần có internet
Chi phí vận hành	Tốn nhân lực, thời gian và tài nguyên để lưu trữ và kiểm tra hồ sơ	Giảm chi phí nhờ tự động hóa và phân tán lưu trữ
Độ tin cậy	Có thể bị giả mạo hoặc lưu trữ sai lệch	Rất cao do không thể chỉnh sửa và tất cả thông tin đều công khai, minh bạch

Bảng so sánh giữa hệ thống truyền thống và hệ thống dựa vào blockchain

Tuy hệ thống xác thực bằng cấp sử dụng công nghệ blockchain đã cho thấy nhiều ưu điểm nhưng vẫn còn một vài điểm hạn chế như:

- Việc sử dụng blockchain và IPFS yêu cầu hạ tầng kỹ thuật và hiểu biết nhất định từ phía người triển khai.
- Hệ thống hiện tại mới chỉ đáp ứng nhu cầu cơ bản về lưu trữ và xác thực chứng chỉ, chưa tích hợp đầy đủ các chức năng khác như tra cứu lịch sử học tập, học phí, điểm số,...

4.3 Hướng phát triển

Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ trong ngành giáo dục, việc chỉ dừng lại ở xác thực chứng chỉ sau khi tốt nghiệp là chưa đủ để đáp ứng nhu cầu quản lý toàn diện và hiện đại hóa hệ thống học tập. Một trong những hướng

phát triển tiềm năng và có tính ứng dụng cao là xây dựng hồ sơ sinh viên điện tử dựa trên nền tảng blockchain, có thể theo dõi toàn bộ quá trình học tập của sinh viên từ khi nhập học đến khi tốt nghiệp, đồng thời đảm bảo tính minh bạch, bất biến và dễ xác minh ở mọi thời điểm.

Hồ sơ sinh viên là một tập hợp các thông tin học tập, hành chính và tài chính được ghi nhận xuyên suốt trong quá trình đào tạo. Nếu được triển khai trên nền tảng blockchain kết hợp IPFS, các thông tin này sẽ có thể được lưu trữ và truy xuất một cách minh bạch, an toàn, không thể sửa đổi và có thể kiểm chứng bởi bất kỳ bên thứ ba nào được ủy quyền.

Các thông tin có thể tích hợp vào hồ sơ sinh viên bao gồm:

- Thông tin cá nhân: Mã số sinh viên, ngày nhập học, chuyên ngành, thông tin liên hệ, giấy tờ tùy thân (được mã hóa).
- Lịch sử học tập:
  - Kết quả từng môn học theo từng học kỳ.
  - Bảng điểm học phần và điểm trung bình tích lũy.
  - Kết quả rèn luyện, điểm thi lại (nếu có).
- Thông tin tài chính:
  - Lịch sử đóng học phí, khoản nợ học phí còn tồn đọng.
  - Các khoản học bổng đã nhận.
- Chứng chỉ, bằng cấp nội bộ:
  - Chứng chỉ ngoại ngữ, tin học.
  - Chứng nhận tham gia các hoạt động, khóa học kỹ năng mềm, hội thảo học thuật...
- Trạng thái học tập: Đang học, bảo lưu, tốt nghiệp, buộc thôi học...

Tất cả những dữ liệu này có thể được lưu mã băm trên blockchain để đảm bảo tính toàn vẹn, còn nội dung chi tiết sẽ lưu trữ trên hệ thống phân tán như IPFS. Điều này không chỉ giúp tiết kiệm chi phí, mà còn đảm bảo dữ liệu không thể bị chỉnh sửa ngầm bởi bất kỳ cá nhân hay bộ phận nào.Mô hình này mang lại rất nhiều lợi ích như:

- Tính đồng bộ cao giữa các đơn vị trong trường: Phòng đào tạo, phòng công tác sinh viên, phòng kế toán… đều có thể truy xuất dữ liệu theo phân quyền, đảm bảo cập nhật tức thời, chính xác và thống nhất.

- Tiện lợi cho sinh viên và cựu sinh viên: Sinh viên có thể truy cập hồ sơ cá nhân của mình mọi lúc, mọi nơi, phục vụ cho việc xin việc, du học, chuyển tiếp hoặc kiểm chứng bằng cấp.
- Tăng tính minh bạch trong quản lý: Mọi hành vi gian lận điểm số, sửa bảng điểm, cấp chứng chỉ giả đều có thể được loại bỏ nhờ tính bất biến của blockchain.
- Hỗ trợ nhà tuyển dụng và đối tác giáo dục: Có thể dễ dàng xác minh thông tin học tập và bằng cấp thông qua một địa chỉ duy nhất, không cần phải liên hệ thủ công với trường học.
- Mở rộng sang hệ sinh thái giáo dục quốc gia.

Nếu được chuẩn hóa và triển khai ở quy mô lớn, mô hình này có thể trở thành một phần của cơ sở dữ liệu giáo dục quốc gia, liên thông giữa các trường đại học, cao đẳng, cơ sở đào tạo và thậm chí là với Bộ Giáo dục & Đào tạo. Hệ thống này có thể:

- Đồng bộ hóa quá trình chuyển trường hoặc học song song nhiều chương trình.
- Tạo nền tảng cho việc cấp hộ chiếu học tập – một hồ sơ học tập điện tử chuẩn hóa, dùng được ở trong nước và quốc tế.
- Làm tiền đề để xây dựng hồ sơ công dân số trong lĩnh vực giáo dục, phục vụ quản lý công dân toàn diện trong thời đại số.

KẾT LUẬN

Trong thời đại chuyển đổi số mạnh mẽ hiện nay, việc đảm bảo tính xác thực, minh bạch và toàn vẹn của dữ liệu là một trong những thách thức quan trọng trong nhiều lĩnh vực, đặc biệt là giáo dục. Khóa luận này đã đi sâu tìm hiểu công nghệ blockchain – một trong những công nghệ đột phá với tiềm năng to lớn trong việc giải quyết vấn đề xác thực thông tin một cách hiệu quả, an toàn và phi tập trung.

Chương 1 đã trình bày tổng quan về công nghệ blockchain, từ khái niệm đến các đặc điểm nổi bật như minh bạch, bất biến, bảo mật và phi tập trung. Đồng thời, chương này cũng làm rõ lý do tại sao blockchain lại phù hợp với các bài toán xác thực, trong đó có xác thực bằng cấp, chứng chỉ học thuật.

Chương 2 đi vào phân tích các cơ sở toán học của blockchain như cây Merkle, hàm băm SHA-256, đường cong ECC và thuật toán ký số ECDSA, nhằm lý giải bản chất kỹ thuật giúp blockchain đạt được tính toàn vẹn và không thể giả mạo dữ liệu. Những nền tảng toán học này là cơ sở để đảm bảo rằng các thông tin được ghi lên blockchain là đáng tin cậy và không thể bị can thiệp.

Chương 3 là trọng tâm của đề tài, tập trung vào việc phân tích và thiết kế một hệ thống ứng dụng blockchain kết hợp với IPFS và hợp đồng thông minh để xác thực chứng chỉ đại học. Giải pháp được đề xuất cho phép lưu trữ nội dung chứng chỉ dưới dạng tệp PDF trên IPFS, trong khi mã hash của chứng chỉ được ghi nhận trong smart contract trên blockchain. Qua đó, hệ thống không chỉ đảm bảo tiết kiệm chi phí lưu trữ mà còn đạt được tính bảo mật và minh bạch cao.

Chương 4 đã đánh giá hiệu quả của mô hình thông qua thực nghiệm triển khai hợp đồng thông minh trên mạng thử nghiệm Ethereum, kết hợp lưu trữ IPFS. Kết quả cho thấy hệ thống có khả năng hoạt động ổn định, xác thực thông tin nhanh chóng, đồng thời không phát sinh chi phí cao như khi lưu trữ trực tiếp trên blockchain. Qua đó, đề tài đã chứng minh được tính khả thi và tiềm năng ứng dụng của blockchain trong xác thực thông tin trong lĩnh vực giáo dục.

Trong tương lai, mô hình có thể được mở rộng để quản lý toàn bộ hồ sơ sinh viên điện tử, tích hợp các thành phần như bảng điểm, lịch sử học phí, chứng chỉ kỹ năng mềm, và trạng thái học tập. Ngoài ra, giải pháp có thể được liên thông với các hệ thống giáo dục khác trong nước hoặc quốc tế, tạo nên một nền tảng xác thực học thuật thống nhất và đáng tin cậy. Hơn thế nữa, hướng ứng dụng tương tự có thể triển khai trong nhiều lĩnh vực khác như y tế, pháp lý, hay quản lý hành chính công.

TÀI LIỆU THAM KHẢO

1. Đoàn Ngọc Sơn (2017), *Nghiên Cứu, Ứng Dụng Công Nghệ Blockchain Trong Thanh Toán Di Động*, Luận văn thạc sỹ Công Nghệ Thông Tin, Trường Đại học Công Nghê, Đại học Quốc gia Hà Nội.

2. Drescher D. (2017), "Blockchain Basics: A Non-Technical Introduction in 25 Steps ", *Apress,* New York.

3. Nakamoto S. (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System", *(nguồn: https://bitcoin.org/bitcoin.pdf).*

4. Stallings W. (2016), "Cryptography and Network Security: Principles and Practice (7th edition)", *Pearson Education*.