HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Lưu Quang Đạt

NGHIÊN CỨU BLOCKCHAIN VÀ ỨNG DỤNG VÀO BÀI TOÁN PHÒNG CHỐNG GIAN LẬN THI CỬ

LUẬN VĂN THẠC SĨ KỸ THUẬT

(*Theo định hướng ứng dụng*)

HÀ NỘI – NĂM 2020

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Lưu Quang Đạt

NGHIÊN CỨU BLOCKCHAIN VÀ ỨNG DỤNG VÀO BÀI TOÁN PHÒNG CHỐNG GIAN LẬN THI CỬ

Chuyên ngành: Hệ thống thông tin

Mã số: 8.48.01.04

LUẬN VĂN THẠC SĨ KỸ THUẬT

(*Theo định hướng ứng dụng*)

NGƯỜI HƯỚNG DẪN KHOA HỌC:

TS. Đặng Minh Tuấn

HÀ NỘI – NĂM 2020

LỜI CẢM ƠN

Lời đầu tiên, em xin được gửi lời cảm ơn sâu sắc tới TS. Đăng Minh Tuấn - người thầy đã luôn tận tình giúp đỡ em định hướng nghiên cứu trong suốt quá trình làm luận văn. Đồng thời, thầy cũng là người truyền đạt cho em rất nhiều những kiến thức bổ ích về các lĩnh vực chuyên môn cũng như các kỹ năng, phương pháp nghiên cứu khoa học.

Em xin được cảm ơn các thầy, cô đang công tác giảng dạy tại Khoa Sau đại học – Học viện công nghệ bưu chính viễn thông. Trong suốt quá trình học cao học, em đã được các thầy, cô truyền đạt rất nhiều tri thức quí báu.

Em cũng xin được cảm ơn gia đình, người thân và bạn bè của em đã giúp đỡ và hỗ trợ cho em rất nhiều trong suốt thời gian qua.

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn thạc sĩ với đề tài: "**NGHIÊN CỨU BLOCKCHAIN VÀ ỨNG DỤNG VÀO BÀI TOÁN PHÒNG CHỐNG GIAN LẬN THI CỬ**" là công trình nghiên cứu của riêng tôi. Các kết quả nghiên cứu trong luận văn là trung thực và chưa từng được công bố trong bất kỳ một công trình nào khác.

Hà nội, ngày 25 tháng 06 năm 2020

Học viên

Lưu Quang Đạt

MỤC LỤC

DANH SÁCH CÁC THUẬT NGỮ TIẾNG ANH VÀ VIẾT TẮT

Từ viết tắt/Thuật ngữ	**Thuật ngữ tiếng Anh/Giải thích**	**Thuật ngữ tiếng Việt/Giải thích**
Block/Khối	Block	Chỉ các khối trong blockchain
BlockHeader		Chỉ tiêu đề của Block
CSS	Cascading Style Sheets	Các kỹ thuật phục vụ cho việc thêm style cho các thành phần của trang web
CSDL	Database	Cơ sở dữ liệu
Hash		Mã băm
HTML5	HTML version 5	Phiên bản mới nhất của HTML, có hỗ trợ một số công nghệ đặc biệt
NodeJS		Nền tảng cung cấp môi trường thực thi ngôn ngữ Javascript phía server
Peer/Node	Peer/Node	Chỉ các nốt mạng trong blockchain
Smart contract	Smart contract	Hợp đồng thông minh
Transaction/Giao dịch	Transaction	Chỉ giao dịch trong blockchain
VueJS	Javascript framework	Đây là 1 khung làm việc Javascript (ngôn ngữ kịch bản phía người dùng) giúp cho việc phát triển các ứng dụng web một cách nhanh chóng, thuận tiện
Web/Website	Web/Website	Là loại ứng dụng chạy trên nền các trình duyệt, được viết bằng ngôn ngữ HTML, ngôn ngữ kịch bản Javascript, …

DANH MỤC CÁC BẢNG BIỂU

DANH MỤC CÁC HÌNH VẼ

LỜI MỞ ĐẦU

Tính cấp thiết của đề tài:

Trong những năm gần đây cùng với sự bùng nổ của Internet, cuộc cách mạng công nghiệp lần thứ 4 đang lan tỏa tới mọi lĩnh vực của đời sống, ứng dụng công nghệ thông tin dần thay thế và hỗ trợ con người trong một số công việc mang lại hiệu suất cao hơn, tỉ lệ chính xác cao hơn. Nhiều nên tảng công nghệ mới được công bố và ứng dụng vào thực tế như trí tuệ nhân tạo (Artificial Intelligence - AI), chuỗi khối (Blockchain), … Với mục tiêu đảm bảo tính an toàn, giảm thiểu chi phí, đảm bảo tính minh bạch và xa hơn nữa là cách mạng hóa về các giải pháp bảo mật, nền tảng Blockchain đã được ra đời.

Blockchain được định nghĩa là công nghệ xử lý và lưu trữ dữ liệu một cách phi tập trung và an toàn dựa vào hệ thống mã hoá vô cùng phức tạp. Blockchain đang được ứng dụng ngày càng mở rộng trong các lĩnh vực tài chính ngân hàng, logistics, điện tử viễn thông, kế toán kiểm toán ... với những ưu điểm nổi bật. Công nghệ Blockchain có các đặc điểm như không thể làm giả, bất biến, bảo mật, minh bạch, phù hợp để áp dụng vào trong lĩnh vực giáo dục như cấp văn bằng chứng chỉ, tổ chức các kỳ thi quan trọng.

Tại Việt Nam, trước thực trạng tình hình gian lận trong thi cử diễn ra vô cùng phức tạp, đặc biệt là trong các kỳ thi quan trọng mang tính chất quyết định như kỳ thi Trung học phổ thông quốc gia. Việc gian lận xảy ra từ chính những người làm công tác tổ chức thi và chấm thi với những thủ đoạn hết sức tinh vi. Điều này đòi hỏi phải có các giải pháp nhằm hạn chế tối đa những sai sót cũng như việc can thiệp trái phép vào kết quả của bài thi, trong đó bao gồm cả những giải pháp nghiệp vụ cũng như cần có các giải pháp công nghệ mang tính đột phát nhằm hạn chế tối đa những gian lận này. Việc đảm bảo tính minh bạch và tin cậy trong kỳ thi là vấn đề vô cùng quan trọng, đây cũng chính là giá trị cốt lõi mà blockchain mang lại. Dựa trên những đặt tính nổi bật của mình, công nghệ Blockchain có thể được áp dụng từ khâu xây dựng ngân hàng câu hỏi, tạo đề thi, thi, nhận kết quả, chấm và công bố

điểm thông qua các hợp đồng thông minh (smart contract). Để làm rõ hơn những điểm mà Blockchain có thể áp dụng được, tôi đã chọn đề tài "Nghiên cứu Blockchain và ứng dụng vào bài toán phòng chống gian lận trong thi cử " cho luận văn của mình.

Mục đích nghiên cứu:

Mục đích nghiên cứu của đề tài là nghiên cứu tổng quan về công nghệ blockchain, nghiên cứu về nguyên tắc hoạt động, ứng dụng của blockchain đối với các hoạt động kinh tế và khoa học của xã hội. Nghiên cứu một mô hình, hệ thống Blockchain có khả năng hạn chế tiêu cực trong các kỳ thi. Từ đó xây dựng kịch bản mô phỏng của hệ thống đề xuất nhằm hạn chế tiêu cực trong các kỳ thi.

Nội dung nghiên cứu:

- Nghiên cứu tổng quan về công nghệ blockchain, các ứng dụng cơ bản trong công nghệ blockchain.
- Nghiên cứu về sổ cái, block, giao dịch trong blockchain.
- Nghiên cứu nền tảng Blockchain Hyperledger Fabric và smart contract.
- Nghiên cứu và xây dựng mô hình kỳ thi có khả năng hạn chế tiêu cực dựa trên công nghệ Blockchain.

Phương pháp nghiên cứu:

Tham khảo các công trình nghiên cứu, bài báo, tài liệu chuyên ngành, từ đó đưa ra các kiến thức cơ bản về blockchain. Sử dụng các kiến thức nghiên cứu được để đề xuất mô hình hình ứng dụng. Cài đặt và thử nghiệm thông qua các thực nghiệm để làm rõ các vấn đề cần đạt được trong luận văn.

Ý nghĩa khoa học và thực tiễn:

Về mặt khoa học, luận văn đã cung cấp các kiến thức cơ bản về blockchain: cấu trúc mạng, block, giao dịch, sổ cái, phân loại các hệ thống blockchain, đi sâu vào phân tích nền tảng Hyperledger Fabric

Về mặt thực tiễn, đề tài có đưa ra các hướng ứng dụng blockchain trong đời sống thực tiễn, đặc biệt là khả năng ứng dụng trong lĩnh vực giáo dục. Việc áp dụng blockchain vào lĩnh vực giáo dục sẽ góp phần tạo ra một một kỳ thi minh bạch, an toàn và tin cậy luận văn, mang lại niềm tin cho mọi người vào kết quả của kỳ thi.

Nội dung chính của luận văn

Chương 1

Trong chương này sẽ trình bày các kiến thức cơ bản về Blockchain như cấu trúc giao dịch, cấu trúc block và mô hình tính toán đồng thuận trên mạng P2P. Nghiên cứu cơ chế đồng bộ và xử lý đồ thuận, quá trình hình thành block và vào sổ, phân loại các mô hình blockchain. Giới thiệu mô hình private blockchain Hyperleger Fabric và mô hình ứng dụng. Trong chương này cũng nêu ra các ứng dụng của Blockchain trong thực tiễn, khả năng áp dụng trong bài toán phòng chống gian lận thi cử.

Chương 2

Chương này, luận văn tập trung phân tích quy trình tổ chức thi và phân tích các gian lận, tiêu cực có thể xảy ra trong một kỳ thi, từ đó xác định các vấn đề cần giải quyết, đồng thời đề xuất mô hình ứng dụng để giải quyết các vấn đề đặt ra.

Chương 3

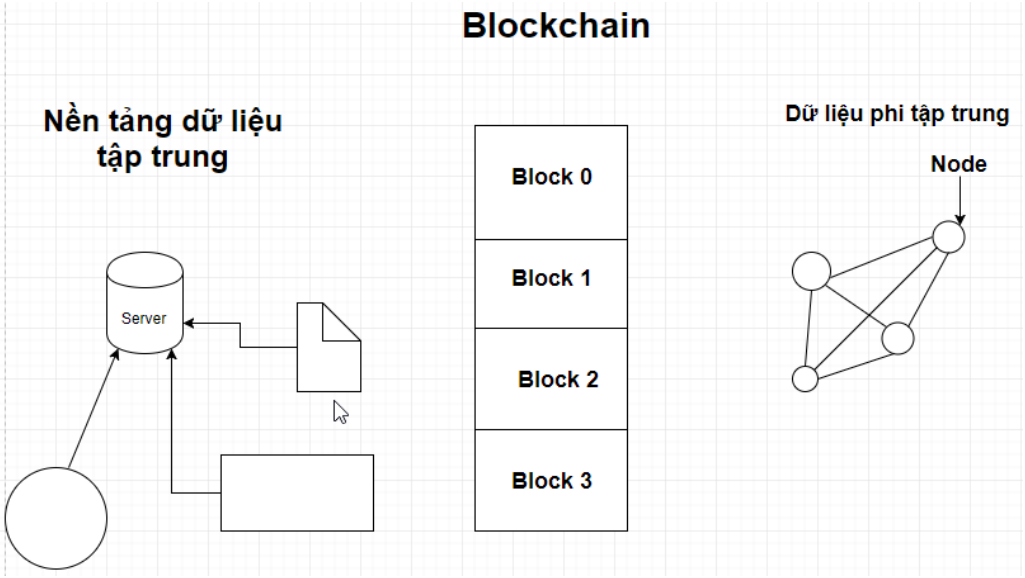
Cuối cùng, chương 3 sẽ tập trung vào vào phân tích và trình bày việc triển khai mô hình ứng dụng blockchain đề xuất vào một kỳ thi cụ thể, đưa ra đánh giá kết quả thực nghiệm.

CHƯƠNG 1: TỔNG QUAN VỀ CÔNG NGHỆ BLOCKCHAIN

1.1. Giới thiệu tổng quan về công nghệ Bockchain

Blockchain ban đầu được phát minh và thiết kế bởi Satoshi Nakamoto vào năm 2008 và được thực hiện hóa vào năm sau đó với Bitcoin [3]

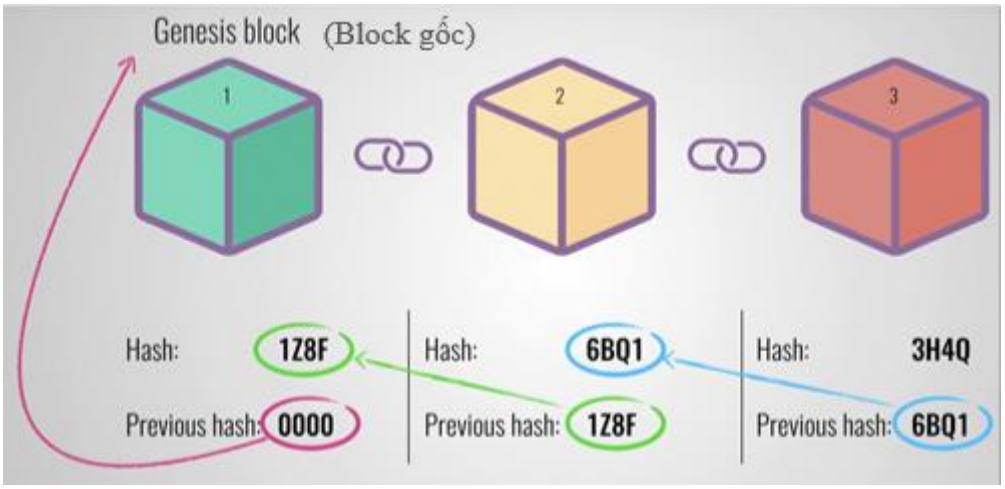
Blockchain là mô hình tính toán mạng lưới, tổ chức theo mô hình phi tập trung, các nút mạng nối nhau từng nhóm. Blockchain có dữ liệu ghi dưới dạng sổ cái phân tán, đồng bộ nhờ cơ chế đồng thuận. Blockchain được đảm bảo an ninh bằng hàm băm mật mã, chữ ký số và cấu trúc lưu trữ móc xích các khối dữ liệu. Mỗi block chứa đựng các thông tin về thời gian khởi tạo, các thông tin giao dịch và được liên kết với các khối trước đó thông qua con trỏ hash. Blockchain được thiết kế để chống lại sự thay đổi dữ liệu do được thiết kế trên *nền tảng dữ liệu phi tập trung*. Thông tin các block trong blockchain được đảm bảo toàn vẹn bằng hàm hash và lưu trữ trên tất cả các nút, mỗi nút sẽ chứa thông tin không thể bị thay đổi và chỉ được bổ sung thêm khi có sự đồng thuận của tất cả các nút trong hệ thống. Ngay cả khi nếu một phần của hệ thống blockchain sụp đổ, những máy tính và nút khác sẽ tiếp tục hoạt động để bảo vệ thông tin.



Hình 1.1 Mô hình Blockchain

Đặc biệt blockchain có khả năng truyền tải dữ liệu mà không đòi hỏi trung gian để xác nhận thông tin. Hệ thống blockchain bao gồm nhiều nút độc lập có khả năng xác thực thông tin mà không đòi hỏi "dấu hiệu của niềm tin". Về cơ bản blockchain là một chuỗi các máy tính (mỗi máy tính là một node) mà tất cả các nút này phải chấp thuận một giao dịch (nếu giao dịch đó là hợp lệ) trước khi nó có thể được xác nhận và ghi lại.

Với blockchain, ngoài việc có thể trỏ tới block trước đó, mỗi block còn có thể lưu giá trị digest (giá trị hash) của khối được trỏ tới. Thông qua việc kiểm tra giá trị hash, chúng ta có thể nhận dạng khối được trỏ tới có bị thay đổi hay không. Cấu trúc blockchain như vậy cho phép chúng ta chỉ cần lưu giá trị của con trỏ chỉ tới khối cuối cùng, đồng thời vẫn kiểm soát được nội dung của các khối còn lại không bị thay đổi.



Hình 1.2 Các block trong Blockchain

(Nguồn internet)

Trong hình trên, hash là mã băm của block hiện tại, previous hash là mã băm của block trước.

Ví dụ điển hình cho Blockchain đó là Bitcoin. Bitcoin là một tập hợp các khái niệm và công nghệ tạo nên nền tảng của một mạng lưới tiền mật mã.

Tính chất của blockchain

Về cơ bản, blockchain có các tính chất dưới đây [6]:

Không lặp: Cơ chế đồng thuận phi tập trung của bitcoin đảm bảo rằng không có giao dịch nào bị trùng lặp.

Tính bất biến: Một khi giao dịch được ghi lại trong blockchain và gắn vào các block tiếp theo thì giao dịch trở nên bất biến. Tính bất biến được đảm bảo bởi sức mạnh của năng lực tính toán vì việc viết lại dữ liệu blockchain đòi hỏi chi phí rất lớn cho việc tính toán để tạo ra "Bằng chứng công việc".

Tính trung lập: Mạng bitcoin phi tập trung lan truyền các giao dịch hợp lệ bất kể nguồn gốc hay nội dung của các giao dịch đó. Điều này có nghĩa là bất cứ ai cũng có thể tạo ra một giao dịch hợp lệ với mức chi phí và độ tin cậy phù hợp, giao dịch có thể lan truyền và đưa vào blockchain bất cứ lúc nào.

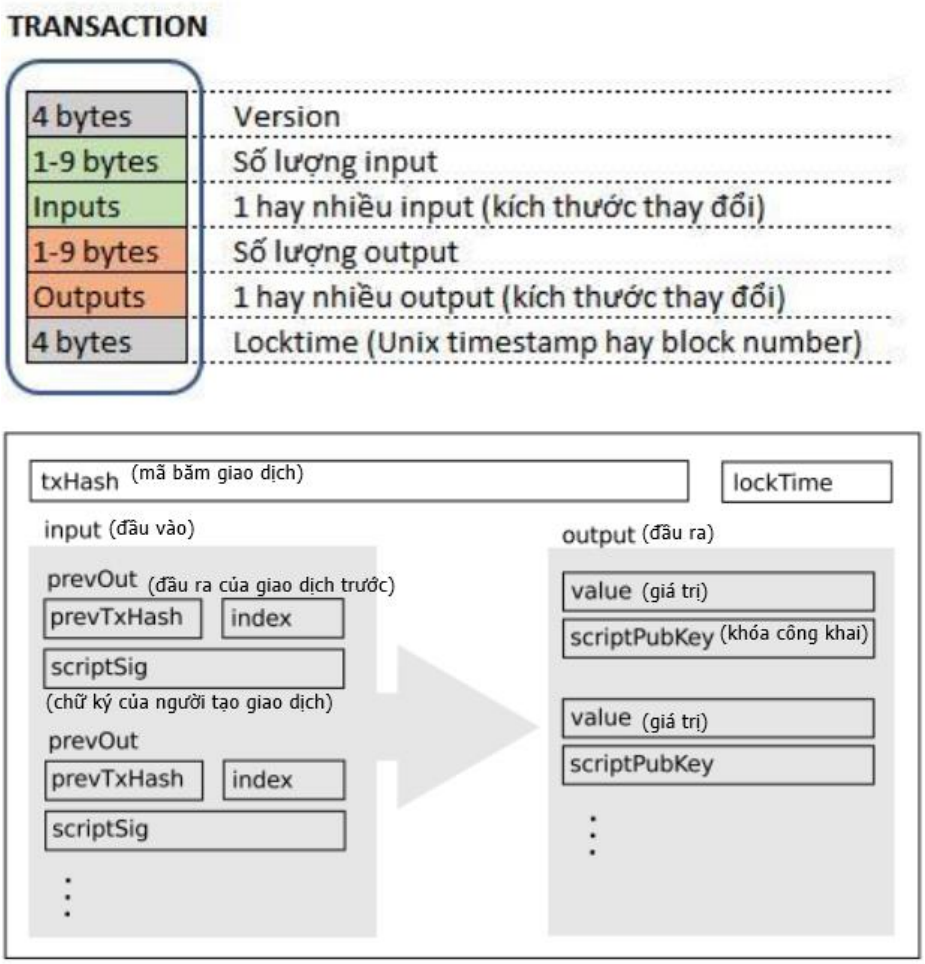
Ngưỡng thời gian an toàn: Các cơ chế đồng thuận từ chối bất kỳ block nào có nhãn thời gian quá xa trong quá khứ hoặc tương lai. Điều này đảm bảo rằng nhãn thời gian trên các block có thể tin cậy được. Nhãn thời gian của một block có ý nghĩa đảm bảo các giao dịch trong block đó.

Tính toàn vẹn: Một giao dịch sẽ được ký bởi SIGHASH_ALL hoặc các phần của giao dịch được ký không thể bị sửa đổi mà không có chữ ký, chính vì vậy đảm bảo giao dịch không bị thay đổi trong quá trình truyền đi

1.2. Nguyên lý cấu tạo của Blockchain

1.2.1. Cấu trúc giao dịch

Giao dịch (Transaction) là một thành phần quan trọng trong Blockchain – Bitcoin. Mọi thành phần khác đều được thiết kế nhằm đảm bảo rằng các giao dịch có thể được tạo ra, lan truyền trên mạng, xác thực và ghi vào sổ cái (blockchain). Giao dịch là cấu trúc dữ liệu mã hóa hóa sự chuyển giao giá trị giữa các đối tượng trong Blockchain. Mỗi giao dịch là một mục ghi chép công khai trong Blockchain – còn được gọi là sổ cái [4]



Hình 1.3 Cấu trúc giao dịch trong Blockchain

(Nguồn dựa trên hình ảnh tại website readthedocs.io)

Khi một node hình thành một giao dịch, node đó sẽ gửi giao dịch này tới các node lân cận, từng node trong đó sẽ kiểm tra tính hợp lệ (validate) giao dịch nhận được nếu hợp lệ nó sẽ lưu vào bộ nhớ cục bộ (mempool) và chuyển tiếp giao dịch đó cho những node lân cận của mình, các node lân cận đó lại tiếp tục kiểm tra hợp lệ- lưu vào mempool và chuyển tiếp, cứ như vậy giao dịch được lan truyền đi toàn mạng. Cuối cùng giao dịch sẽ được đóng trong một block nào đó và được đào bởi thợ đào (miner) lúc đó giao dịch mới được xác thực và lưu lại trong sổ cái blockchain. Giao dịch có kích thước khoảng 300-400 bytes (với hệ thống bitcoin).

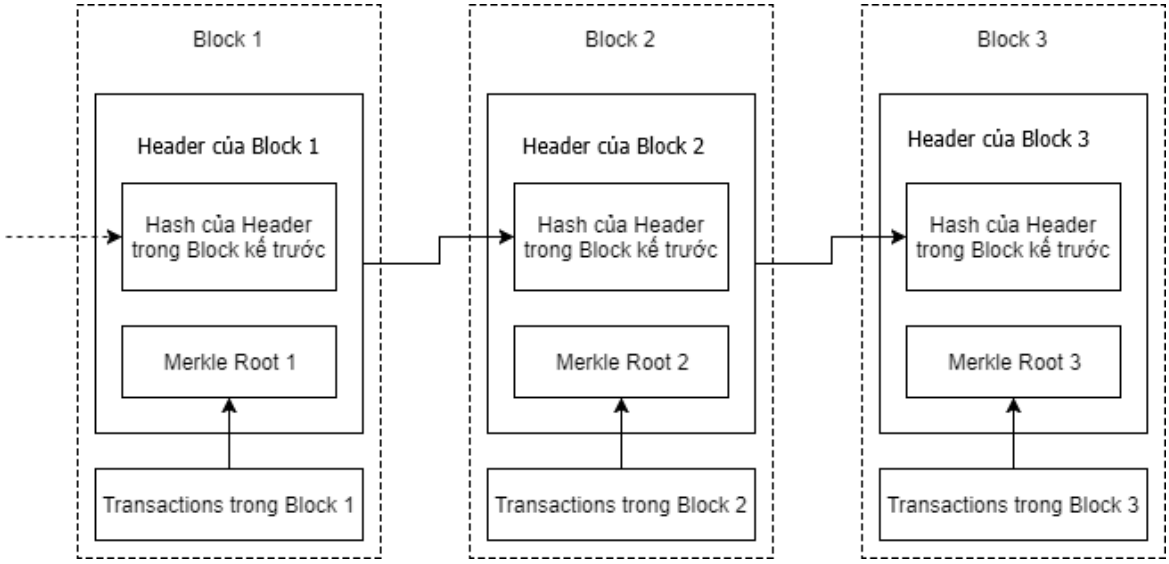
Mỗi một nút trong Blockchain đều phải kiểm tra tính hợp lệ của giao dịch, việc kiểm tra này nhằm nâng cao tính xác thực của chủ sở hữu, tăng tính an toàn cho giao

dịch. Thường trong blockchain sẽ có 2 loại giao dịch đó là Coinbase Transaction và Regular Transaction.

1.2.2. Cấu trúc của Block

Mỗi block trong blockchain được xác định bằng một mã băm do thuật toán băm mật mã SHA256 tạo ra trong tiêu đề block (block header). Mỗi block đều chứa mã băm của block trước đó trong tiêu đề của chính nó. Chuỗi các mã băm liên kết từng block tới block trước tạo thành một chuỗi mắt xích đi ngược trở về cho tới block được tạo ra đầu tiên, gọi là block gốc (genesis block).

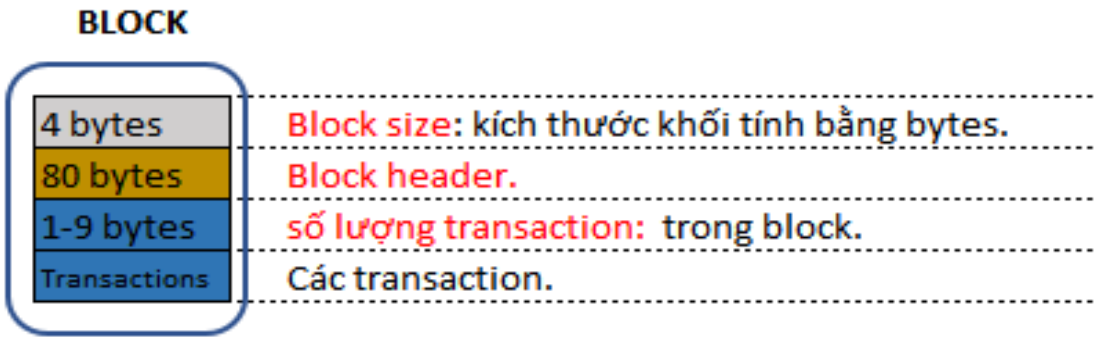
Mỗi block chỉ có một block trỏ đến, có thể có trường hợp rẽ nhánh, 2 block cùng trỏ đến 1 block trước nhưng đến một thời điểm có 1 nhánh dài hơn và khi đó nhánh ngắn hơn sẽ phải xóa bỏ và dữ liệu trên nhánh này phải rollback trở lại.



Hình 1.4 Liên kết các block

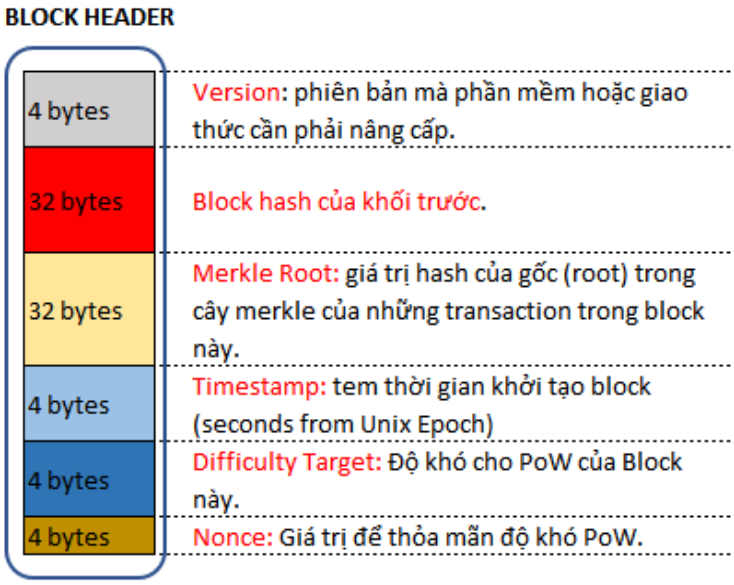
Block bao gồm một tiêu đề để chứa dữ liệu, theo sau là một danh sách giao dịch. Tiêu đề block có kích thước cố định 80 byte, trong khi một giao dịch trung bình chứa

tối thiểu 250 byte và block trung bình chứa hơn 500 giao dịch.



Hình 1.5 Cấu trúc block

a. Tiêu đề của Block



Hình 1.6 Block header

Tiêu đề của block bao gồm 3 bộ dữ liệu mô tả. Đầu tiên là một tham chiếu tới một mã băm của block kế trước, liên kết block này với block kế trước trong một mạng blockchain. Bộ siêu dữ liệu thứ hai, được đặt tên là độ khó (difficulty), nhãn thời gian (timestamp), và số nonce (số dùng một lần), số này chính là thông số quan trọng của quá trình miner (đào). Phần dữ liệu thứ 3 là gốc cây merkle, một cấu trúc dữ liệu được sử dụng để ánh xạ toàn bộ giao dịch trong một block.

b. Định danh block:

Định danh block chính là mã băm mật mã của nó, là một vân tay số được tạo ra bằng cách băm tiêu đề của block hai lần qua thuật toán SHA256. Mã băm 32 byte kết quả được gọi là mã băm block – mã băm tiêu đề block. Mã băm của một block luôn luôn xác định một block đơn lẻ duy nhất và rõ ràng, có thể được tạo ra một cách độc lập bởi bất kỳ nút nào đơn giản bằng cách băm tiêu đề block.

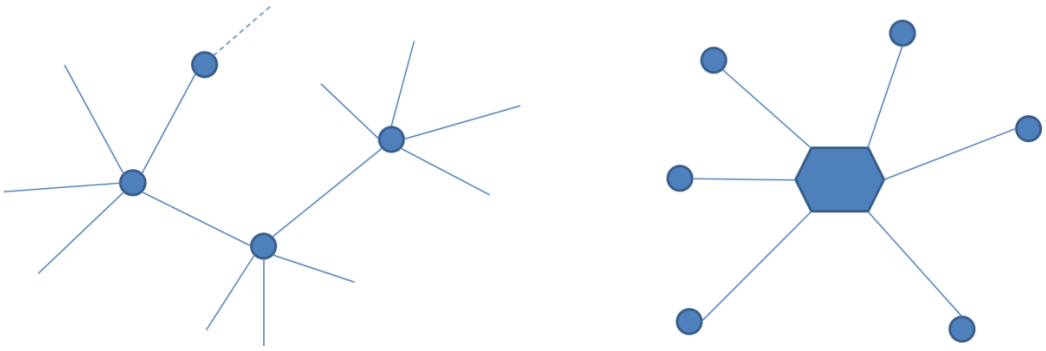
Một cách thứ hai để xác định một block là bằng vị trí của nó trong blockchain, được gọi là chiều cao block. Block đầu tiên từng được tạo ra có chiều cao là 0.

1.2.3. Cấu trúc mạng blockchain và mô hình mạng ngang hàng P2P

a. Mô hình ngang hàng P2P:

Mạng ngang hàng Peer-2-peer bao gồm rất nhiều các nút mạng liên kết trực tiếp với nhau, trong đó mỗi nút mạng có vai trò và vị trí như nhau. Một ví dụ về ứng dụng của mô hình này là Bittorrent, giao thức chia sẻ dữ liệu qua Internet ngày nay, hoặc Napster ứng dụng chia sẻ nhạc trực tuyến những năm 1990

Mạng ngang hàng cho phép hàng triệu người sử dụng có thể kết nối với nhau, hình thành một khối khổng lồ với khả năng tính toán và băng thông của tất cả các mạng gộp lại.



Hình 1.7 Mô hình tính toán P2P

Trong mạng P2P, do không tồn tại một đơn vị trung tâm kiểm soát thông tin, độ tin cậy của mạng này phụ thuộc vào độ tin cậy của từng nốt mạng. Do đó, vấn đề đặt ra phải có một giải pháp chia sẻ thông tin đảm bảo được tính bền vững của các giao dịch và quản lý dữ liệu ngay cả khi không có được sự trung thực của tất cả các nốt mạng. Blockchain được đề cập đến như một giải pháp giải quyết việc triển khai mô

hình ngang hàng kết hợp với các giải pháp ký số nhằm hướng tới khả năng chia sẻ khổng lồ và xác thực.

b. Cấu trúc mạng Blockchain:

Mô hình tính toán P2P trong công nghệ blockchain được ứng dụng một cách khoa học. Bất cứ máy tính nào kết nối với blockchain Bitcoin được coi là một node. Bất kỳ các node nào thực thi đầy đủ các quy tắc của Bitcoin được gọi là "full nodes" (nút đầy đủ). Hầu hết các nodes trên mạng là các nodes nhỏ, nhưng các nút đầy đủ mới là xương sống của mạng lưới. Nút đầy đủ tải về mọi khối và giao dịch, kiểm tra chúng theo nguyên tắc đồng thuận cốt lõi của Blockchain.

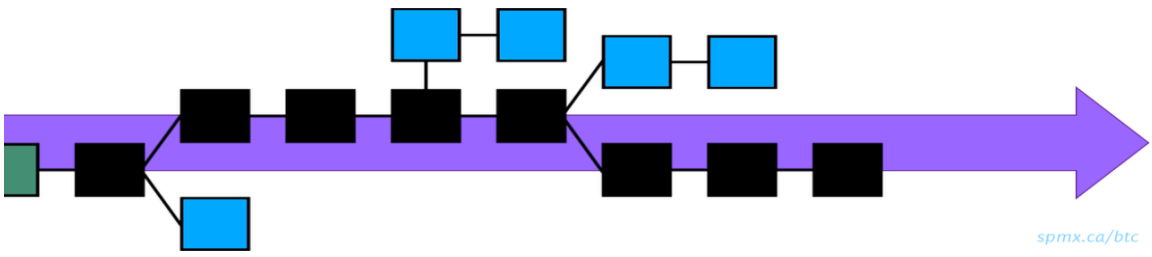
Mỗi node xác minh mỗi giao dịch và mỗi khối nó nhận được trước khi chuyển nó sang các node khác.

Nếu một giao dịch hoặc một khối vi phạm các quy tắc đồng thuận (có nghĩa là giao dịch hoặc khối đó được 1 node xác minh là không hợp lệ), nó hoàn toàn bị từ chối khỏi mạng, ngay cả khi mọi node khác trên mạng cho rằng nó là hợp lệ. Đây là một đặc tính quan trọng nhất của các nodes: Chúng thực hiện đúng nguyên tắc dù có bất cứ chuyện gì xảy ra.

Nếu giao dịch (hoặc khối) là hợp lệ, node sẽ lưu trữ chúng lại và chuyển đi tất cả các node khác trong mạng lưới kết nối với node đó. Bằng cách này, mọi node sẽ thực thi tất cả các quy tắc đồng thuận, và ngăn không cho bất cứ nội dung nào được đưa vào phá vỡ các quy tắc đó.

1.2.4. Các cơ chế đồng bộ đồng thuận trên blockchain

Để đảm bảo tính bất biến của dữ liệu, blockchain sử dụng cơ chế đồng thuận. Có 2 cơ chế đồng thuận trong blockchain là PoW(Proof of Work- Bằng chứng công việc) và PoS (Proof of Stake - Bằng chứng cổ phần)



Hình 1.8 Xử lý đồng thuận

PoW trong khai thác mỏ của Bitcoin lấy một đầu vào bao gồm Merkle Root (về cơ bản là một hàm băm nhị phân của tất cả các giao dịch trong khối), timestamp (dấu thời gian), khối băm trước đó và một số thông tin khác cộng với nonce là số ngẫu nhiên hoàn toàn (0->2^31). Nếu đầu ra kết quả trong băm nhỏ hơn so với target (mục tiêu băm) thì miner sẽ nhận được phần thưởng và sự đồng thuận (khối mới được tạo ra sẽ được thông báo cho toàn hệ thống).

Mỗi nút đều có quyền hình thành block và gửi lên mạng, khi hai trạm đào cùng hình thành block thì sẽ có hiện tượng Fork. Từ một gốc sổ chính xuất hiện hai nhánh khác nhau, như một phần của sự đồng thuận, phần mềm phía máy trạm blockchain sẽ chọn nhánh dài nhất là nhánh an toàn nhất. Các block nằm trên nhánh phụ được gọi là slate block.

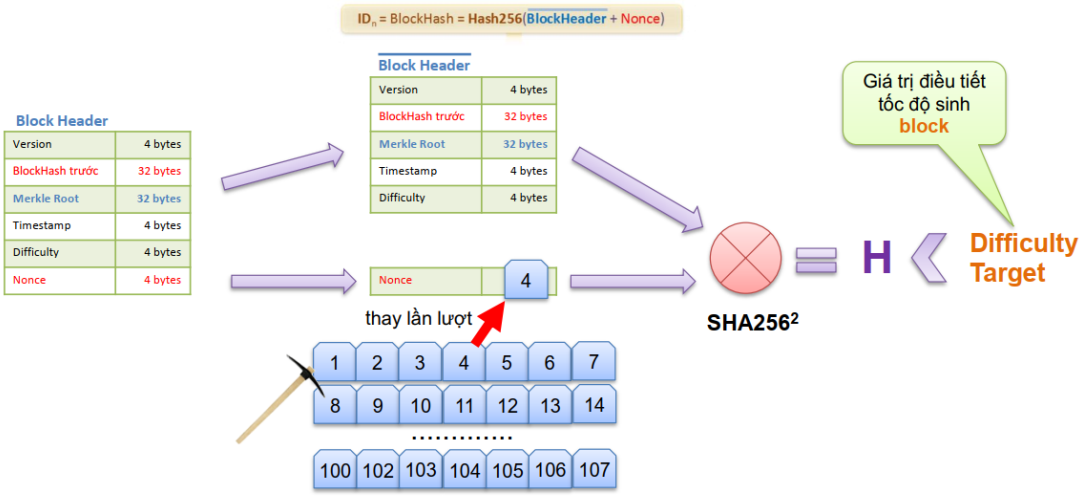
Với việc PoW tiêu tốn quá nhiều năng lượng thì được đề xuất để giảm đáng kể chi phí. PoS được áp dụng lần đầu trong Peercoin vào 08/2012. Giống như PoW, PoS cũng phải tìm ra đáp án của một câu đố mã hóa nhưng độ khó ở đây lại tỷ lệ nghịch so với số tài sản đặt cược của nút trong mạng [5]. Cổ phần ở đây là một tài khoản bị khóa với số dư nhất định thể hiện cam kết của nút đó để giữ cho mạng an toàn.

1.2.5. Sổ cái và quá trình hình thành block

Trong blockchain, sổ cái là một danh sách các giao dịch. Sổ cái khác với cơ sở dữ liệu truyền thống (CSDL). Với sổ cái, chúng ta chỉ có thể thêm giao dịch mới vào, trong khi với CSDL, chúng ta có thể thêm, tùy chỉnh hoặc xóa giao dịch. Có thể dùng CSDL để tạo một sổ cái. Sổ cái có những đặc điểm sau:

- Lưu trữ dữ liệu phân tán.
- Người dùng ẩn danh.
- Gắn với thời gian.
- Các nút lưu trữ với nhau đồng thuận về nguyên tắc chia sẻ.
- Sổ cái không thể đảo ngược, điều này có nghĩa là giao dịch không thể xóa được.
- Sổ cái được bảo mật.
- Có thể lập trình được.

Quá trình hình thành các block là quá trình mà các miner (node khai thác), còn gọi là quá trình tìm Nounce sẽ thực hiện. Trong quá trình này giao dịch sẽ được các miner xếp vào trong hàng đợi gọi là mempool, giao dịch sẽ được gom lại (khoảng 300-500 giao dịch). Giao dịch sẽ được gom theo một mức độ ưu tiên (ví dụ như khoản phí hoặc các giao dịch lâu chưa được xử lý) tạo thành một khối gọi là block. Các miner sẽ phát tán toàn mạng các block mới được tạo, thưởng và phí sẽ được nhận được sau khi có 100 xác nhận. Các block sẽ được đào – là quá trình tính toán mã hash hợp lệ cho block (hashBlock< Target).



Hình 1.9 Quá trình khai thác (mining) [3]

Quá trình xác nhận một block mới được diễn ra như sau: nút sẽ nhận block mới, kiểm tra tính xác thực và đúng đắn thì phát tán toàn mạng, nếu không hợp lệ thì không phát tán. Tiếp theo xóa các giao dịch trong hàng đợi đã được xác thực trong block mới nhận được. Từng thành viên sẽ nối block này như một giao dịch được công nhận trong sổ cái blockchain của mọi thành viên. Xác nhận chính là quá trình đào (mining), việc xác nhận cũng xác định số lượng giao dịch đang chứa. Cụ thể:

0 confirmation: Giao dịch đã được lan truyền trên mạng nhưng chưa vào bất kỳ block nào điều đó có khả năng giao dịch không thành công hoặc tiêu trùng lặp.

1 confirmation: Giao dịch được chứa trong block mới nhất, nguy cơ tiêu trùng lặp ít đi đáng kể tuy khó xảy ra.

2 confirmation: Giao dịch nằm ít nhất trong 2 block gần đây, việc tấn công trở nên đắt đỏ (mất nhiều tài nguyên tính toán để phân nhánh).

6 confirmation: Mạng blockchain đã mất gần 1h đồng hồ để bảo vệ giao dịch chống lại hiện tượng tiêu trùng. Giao dịch đã nằm ở độ sâu 6 block và khả năng nó bị thay thế là rất thấp.

1.2.6. Hợp đồng thông minh

Smart contracts (Hợp đồng thông minh) là một thỏa thuận hoặc tập hợp các quy tắc chi phối việc thực hiện giao dịch; nó được lưu trữ trên blockchain và được thực thi tự động như một phần của giao dịch [6]

Hầu như tất cả các mô hình blockchain đều có hợp đồng thông minh được tích hợp trong các giao dịch. Ví dụ trong các loại tiền mã hóa, hợp đồng thông minh xác minh các giao dịch đầu vào bằng cách kiểm tra chữ ký của chúng. Sau đó, xác minh số dư của các địa chỉ gửi có khớp với địa chỉ nhận không. Cuối cùng, hợp đồng thông minh sẽ áp dụng các thay đổi tới các trạng thái. Người dùng cũng có thể viết các hợp đồng thông minh thực thi trong giao dịch.

```
car contract:

 query(car):
  get(car);
  return car;

 transfer(car, buyer, seller):
  get(car);
  car.owner = buyer;
  put(car);
  return car;

 update(car, properties):
  get(car);
  car.colour = properties.colour;
  put(car);
  return car;
```

Hình 1.10 Ví dụ hợp đồng thông minh trong mạng blockchain fabcar [10]

1.3. Phân loại Blockchain

Các hệ thống blockchain hiện tại có thể được phân thành ba loại: Blockchain công cộng (public blockchain), blockchain riêng tư (private blockchain) và blockchain liên kết (consortium blockchain). Trong blockchain công cộng, tất cả dữ

liệu được hiển thị công khai và bất kỳ ai cũng có thể trở thành một nút trong hệ thống. Đối với blockchain liên kết thì chỉ một nhóm các nút được chọn mới được tham gia vào hệ thống. Với blockchain riêng tư thì chỉ bao gồm các nút từ các tổ chức cụ thể mới có thể tham gia. Để phân biệt rõ được sự khác nhau của ba loại blockchain, Bảng dưới đây liệt kê các tiêu chí được sử dụng để đưa ra so sánh:

Bảng 1.1 So sánh các loại blockchain

Tiêu chí	**Blockchain công cộng**	**Blockchain liên kết**	**Blockchain riêng tư**
Xác định sự đồng thuận	Tất cả thợ đào	Các nút được chọn	Một tổ chức
Quyền đọc	Công khai	Có thể công khai hoặc bị hạn chế	Có thể công khai hoặc bị hạn chế
Tính bất biến	Gần như không thể giả mạo	Có thể bị giả mạo	Có thể bị giả mạo
Tính hiệu quả	Thấp	Cao	Cao
Tính tập trung	Không	Một phần	Có
Quá trình đồng thuận	Không cần sự cho phép	Phải được cấp quyền	Phải được cấp quyền

Xác định sự đồng thuận: Trong blockchain công cộng, mỗi nút đều có thể tham gia vào quá trình đồng thuận. Với blockchain liên kết thì chỉ có một tập hợp các nút được chọn mới có thể xác nhận tính hợp lệ của khối trong hệ thống. Ở blockchain riêng tư, một tổ chức kiểm soát hoàn toàn để xác định sự đồng thuận cuối cùng.

Quyền đọc: Các giao dịch trong một blockchain công cộng được hiển thị cho bất cứ ai, nhưng ở blockchain riêng tư và blockchain liên kết thì điều đó có thể cấu hình được.

Tính bất biến: Do có số lượng lớn các nút tham gia quá trình xác nhận nên dữ liệu trong blockchain công cộng gần như không thể sửa đổi trái phép. Trong khi ở blockchain riêng tư và liên kết thì dữ liệu có thể bị giả mạo vì số lượng nút tham gia đồng thuận hạn chế.

Tính hiệu quả: Trong blockchain công cộng do số lượng nút tham gia vào mạng lưới nên phải mất nhiều thời gian để lan truyền các giao dịch và các khối cho toàn hệ thống. Điều này gây ra độ trễ cao và thông lượng của giao dịch bị giới hạn. Ngược lại, với số lượng nút xác nhận ít hơn nên blockchain riêng tư và liên kết có thể hiệu quả hơn.

Tính tập trung: Ở blockchain công cộng các nút tham gia đồng thuận là phi tập trung, blockchain liên kết tập trung một phần, blockchain riêng tư vì được kiểm soát bởi một nhóm duy nhất.

Quá trình đồng thuận [6]: Bất kỳ ai cũng có thể tham gia vào quá trình đồng thuận trong blockchain công cộng. Ở blockchain riêng tư và liên kết thì chỉ những ai được cấp phép mới được tham gia quá trình đồng thuận.

Bảng 1.2 So sánh giữa mô hình Bitcoin, Ethereum và Hyperledger **Fabric** sẽ đưa ra so sánh một số nền tảng blockchain điển hình tương ứng với các loại blockchain đã nêu ở trên

Bảng 1.2 So sánh giữa mô hình Bitcoin, Ethereum và Hyperledger Fabric[5]

Thuộc tính	Bitcoin	Ethereum	Hyperledger Fabric
Mô hình	Công cộng	Công cộng hoặc riêng tư	Riêng tư
Mật mã học	ECDSA, SHA256, RIPEMD160, Base58, Merkle tree	ECDSA, Keccak256, Patricia Merkle tree	ECDSA, SHA256, Bucket tree
Khả năng truy cập dữ liệu	Công khai	Công khai (hệ thống công cộng) hoặc bị hạn chế (hệ thống riêng tư)	Bị hạn chế

1.4. Nền tảng Hyperledger Fabric

1.4.1. Giới thiệu về Hyperledger

Hyperledger là một dự án mã nguồn mở, cung cấp một hệ sinh thái các giải pháp và người dùng trên nền tảng công nghệ blockchain nhằm giải quyết các vấn đề đặc thù của từng doanh nghiệp.

Hyperledger thuộc tổ chức Linux Foundation. NodeJs, Alljoyn, Dronecode là một số dự án nổi tiếng của Linux Foundation. Mục đích của Linux Foundation là tạo ra một cộng đồng các nhà phát triển làm việc trên các dự án nguồn mở, nhằm duy trì sự phát triển của các dự án, trong đó, mã nguồn dự án luôn được nâng cấp, sửa đổi và phân phối lại. Tư tưởng của Hyperledger là thế giới sẽ gồm nhiều kênh thanh toán (private chain) riêng biệt với các thị trường khác nhau. Mỗi doanh nghiệp có những đặc trưng riêng, nên các ứng dụng cho các doanh nghiệp sẽ cần phát triển với các quy tắc được cá nhân hóa. Dự án Hyperledger bắt đầu với một số ít các nhà phát triển vào

cuối năm 2015. Dự án được bắt đầu với các thử nghiệm tương tác giữa ứng dụng và một mạng blockchain an toàn.

Cách hoạt động của Hyperledger

Trên mạng Hyperledger, các peer liên kết trực tiếp với nhau và chỉ có sổ cái của riêng họ được cập nhật về thỏa thuận giao dịch. Các bên giúp thực hiện giao dịch chỉ được biết một lượng thông tin đủ để họ cần để chuyển tiếp và cho phép giao dịch trên mạng. Sau khi đã được xác thực, hai peer sẽ được kết nối và kết quả được trả về. Trong thỏa thuận hai bên này, cả hai kết quả trả về phải giống nhau để giao dịch có thể được xác nhận. Trong các giao dịch khác với nhiều bên, nhiều quy tắc hơn có thể được áp dụng.

Những đặc điểm của Hyperledger

Trong kiến trúc này, những đăc điểm đáng chú ý nhất được thể hiện trong các peer của mạng. Các peer đã được chia thành ba vai trò riêng biệt, đó là:

- *Endorser*: Các endorser là những peer thực thi các giao dịch trong chaincode (hợp đồng thông minh) container và đề xuất giao dịch lên mạng dựa trên kết quả của hợp đồng thông minh. Tất cả các endoser peer phải được cài đặt chaincode.
- *Committer*: Đây là những peer không nhất thiết phải cài đặt chaincode, chúng lưu trữ sổ cái đầy đủ (full ledger). Sự khác biệt chính giữa committer peer và endoser peer là việc committer peer không thể gọi chaincode hoặc chạy các hàm trong hợp đồng thông minh.
- *Consenters*: Các nút này chịu trách nhiệm điều hành sự đồng thuận của mạng. Consenters có trách nhiệm xác nhận các giao dịch và quyết định các giao dịch sẽ được đưa vào sổ cái.

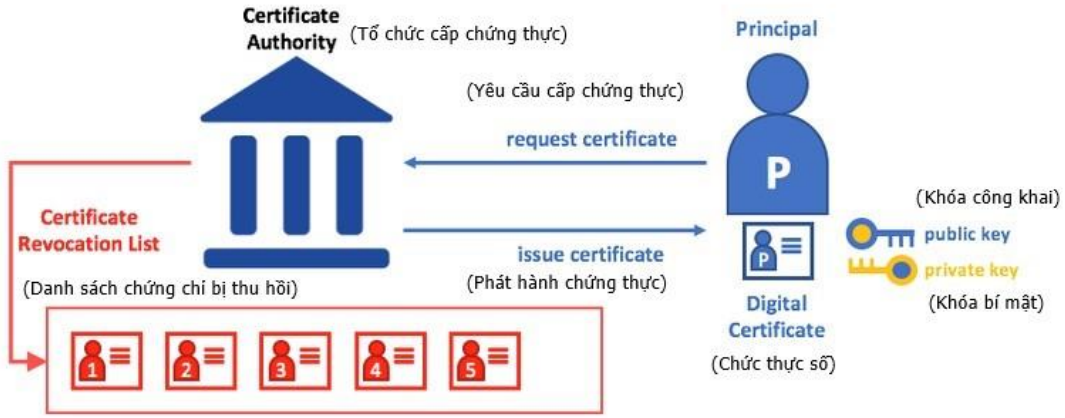
1.4.2. Hyperledger Fabric

Hyperedger Fabric là một trong 5 Framework về Blockchain nằm trong chiến lược Hyperledger Umbrella của Linux Foundation gồm: Hyperledger Indy, Hyperledger Fabric, Hyperledger Iroha, Hyperledger Sawtooth, Hyperledger Burror. Hyperledger Fabric được xây dựng và hỗ trợ bởi công ty lớn như IBM. Hyperledger

Fabric có modularity (tính mô đun) khá cao nên nó cho phép các doanh nghiệp dễ dàng plug and play để xây dựng một ứng dụng Private Blockchain phù hợp các yêu cầu nghiệp vụ của mình.

Các khái niệm cơ bản trong Hyperledger Fabric [10]

- *Identity:* Mỗi tác nhân trong Hyperledger Fabric bao gồm peers, orderer, client, admin, ... đều có một identity. Các tác nhân này sẽ sử dụng identity của mình để tương tác với mạng, identity đó được cấp dưới dạng một X.509 digital certificate. Các identity rất quan trọng vì nó còn giúp hệ thống xác định tác nhân có thể thực hiện những hành động nào, có quyền truy cập vào những tài nguyên nào của network.

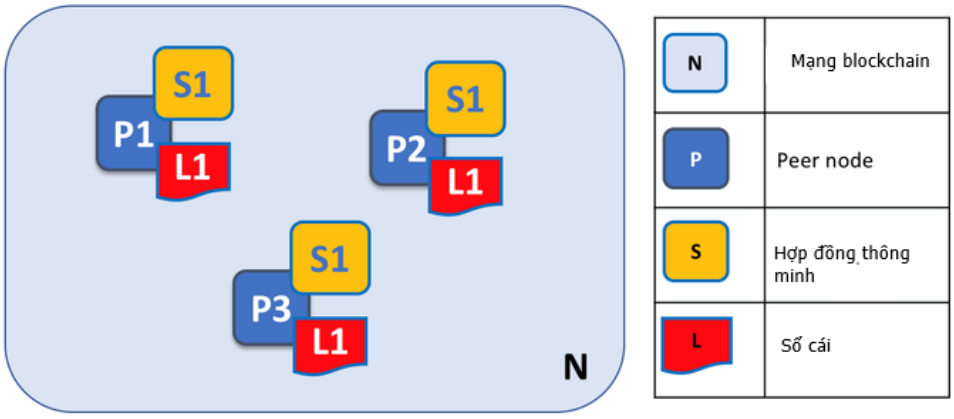


Hình 1. 11 Identity trong Hyperledger Fabric

Một Public key Infrastructue **(**PKI**)** là tập hợp các internet technologies cung cấp sự liên lạc an toàn trong network. Trong mạng Hyperledger Fabric, PKI là tập hợp các Certificate Authorities của các tổ chức. Các Certificate Authorities này sẽ cấp cho mỗi tác nhân muốn tham gia vào vào mạng một identity.

- *Membership:* Membership Service Provider (MSP) của một tổ chức tham gia - xác định CA nào được ủy quyền cấp identity hợp lệ cho các thành viên của tổ chức đó.

- *Peer:* Một mạng Blockchain bao gồm chủ yếu các peer. Peer là thành tố cơ bản của network vì nó lưu trữ bản sao của Smart Contract (Chaincode) và bản sao của Ledger. Các peer có thể được tạo, start, stop, tái cấu hình, thậm chí là xóa.



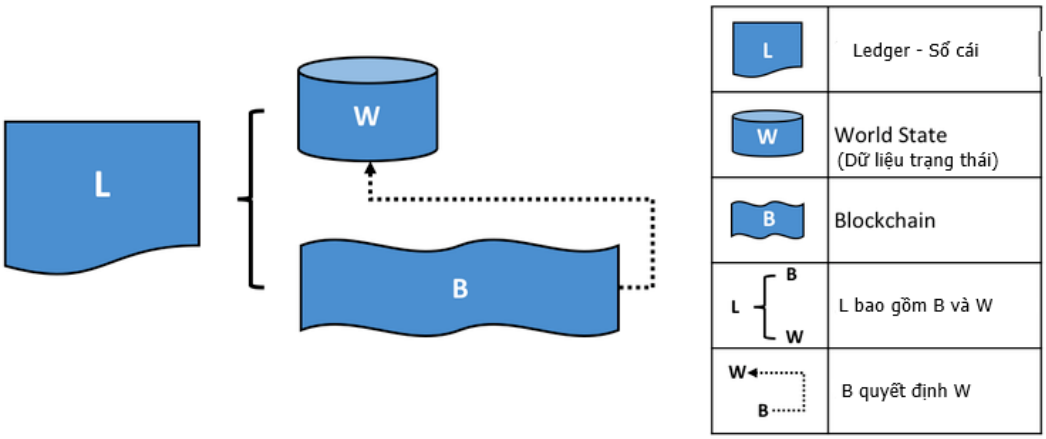
Hình 1. 12 Peers trong Hyperledger Fabric

- *Smart contract và chaincode:* Smart Contract xác định các quy tắc giữa các tổ chức khác nhau trong các hành động. Các ứng dụng gọi một smart contract để tạo ra các giao dịch được ghi lại kết quả trên Ledger.

Hình 1. 13 Prototype đơn giản của một chaincode

Một smart contract định nghĩa các logic giao dịch, sau đó smart contract được đóng gói thành chaincode

- *Ledger:* Trong mạng Hyperledger Fabric, mỗi kênh có một ledger bao gồm các thành phần như sau:

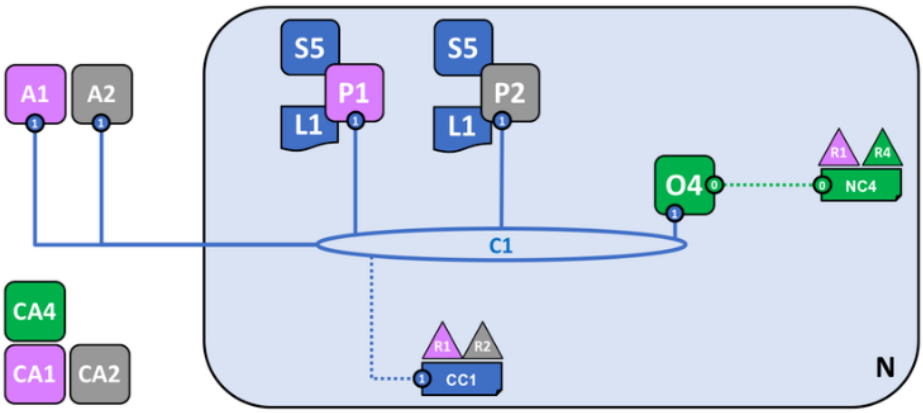


Hình 1. 14 Ledger trong Hyperledger Fabric

- *The odering service:* Hầu hết các mạng Public Blockchain, chẳng hạn như Ethereum và Bitcoin, bất kỳ node nào cũng có thể tham gia vào quá trình đồng thuận (consensus). Hyperledger Fabric thì khác, nó có một loại node được gọi là orderer (hay còn được gọi "ordering node"), thực hiện nhiệm vụ "consensus", có thể là chỉ có một ordering node trong một network, hoặc có thể có nhiều node tạo nên một ordering service. Bởi vì thiết kế Hyperledger Fabric là dựa trên các thuật toán "deterministic consensus ", nên bất kỳ block nào đã được các peer validates và được tạo bởi ordering service thì đều được đảm bảo là chính xác. Ledger sẽ không thể xảy ra tình trạng rẽ nhánh như các blockchain khác. Ngoài vai trò trên, ordering service còn lưu trữ các thông tin khác như tổ chức nào được phép tạo channel, ai có thể thay đổi các cấu hình channel, và tất cả hành động thay đổi cấu hình đó đều phải đi qua orderer.

1.4.3. Kiến trúc của một mạng Hyperleger Fabric

Một mạng Hyperledger Fabric đơn giản bao gồm các thành phần như sau:



Hình 1.15 Kiến trúc đơn giản của một mạng Hyperledger Fabric [10]

N: (Networld) Mạng

NC: Network Configuration (Cấu hình của mạng)

C: Channel (Kênh), tập hợp các tổ chức có vai trò nhất định trong cùng một quy trình kinh doanh. Ví dụ, trong một channel về mua bán xe hơi sẽ gồm có 2 tổ chức là: Nhà sản xuất xe hơi, Nhà phân phối xe hơi.

CC: Channel Configuration (Cấu hình của kênh)

R: Organization (Tổ chức)

O: Orderer Node: Nếu như trong Publuc Blockchain, tất cả các node của mạng đều tham gia vào quá trình đồng thuận, thì ở Hyperledger Fabric chỉ có Orderer tham gia vào quá trình đó.

P: Peer, là điểm tương tác giữa các thành viên trong tổ chức tương ứng với kênh, mọi hành động của người dùng đều phải đi qua peer.

S: Smart Contract (Chaincode) được cài đặt trên kênh, định nghĩa rõ các struct, các hành động mà người dùng có thể thực hiện để tương tác trạng thái của struct được lưu trong sổ cái.

L: Ledger (Sổ cái), lưu trữ trạng thái của các đối tượng.

CA: Certificate Authority, phát hành identity cho người dùng hoặc node của tổ chức tương ứng. Ví dụ, người dùng A là thành viên của Tổ chức R1, khi muốn tham gia vào mạng thì sẽ gửi yêu cầu đến CA1, sau đó CA1 sẽ tạo ra một identity gồm

private-key, public-key và các đặc tính liên quan khác, sau đó trả về cho người dùng A, từ đó về sau A dùng identity đó để thực hiện các tương tác với mạng, mạng sẽ tự động biết đó là người dùng A đến từ tổ chức R1.

A: Application, ứng dụng hay giao diện (web, mobile app) giúp người dùng tương tác với hệ thống dễ dàng hơn.

Tất cả cả thành phần ở trên hoặc là chạy trên docker hoặc là chúng ta có thể định nghĩa chúng trong code.

1.4.4. Ưu điểm của Hyperledger

Theo IBM, Hyperledger có một số ưu điểm nổi bật so với một số nền tảng blockchain khác [7]. Cụ thể như sau:

Thành viên được cấp phép

Hyperledger Fabric là một khung cho các mạng được phép (permissioned networks), nơi tất cả những người tham gia có danh tính đã biết.

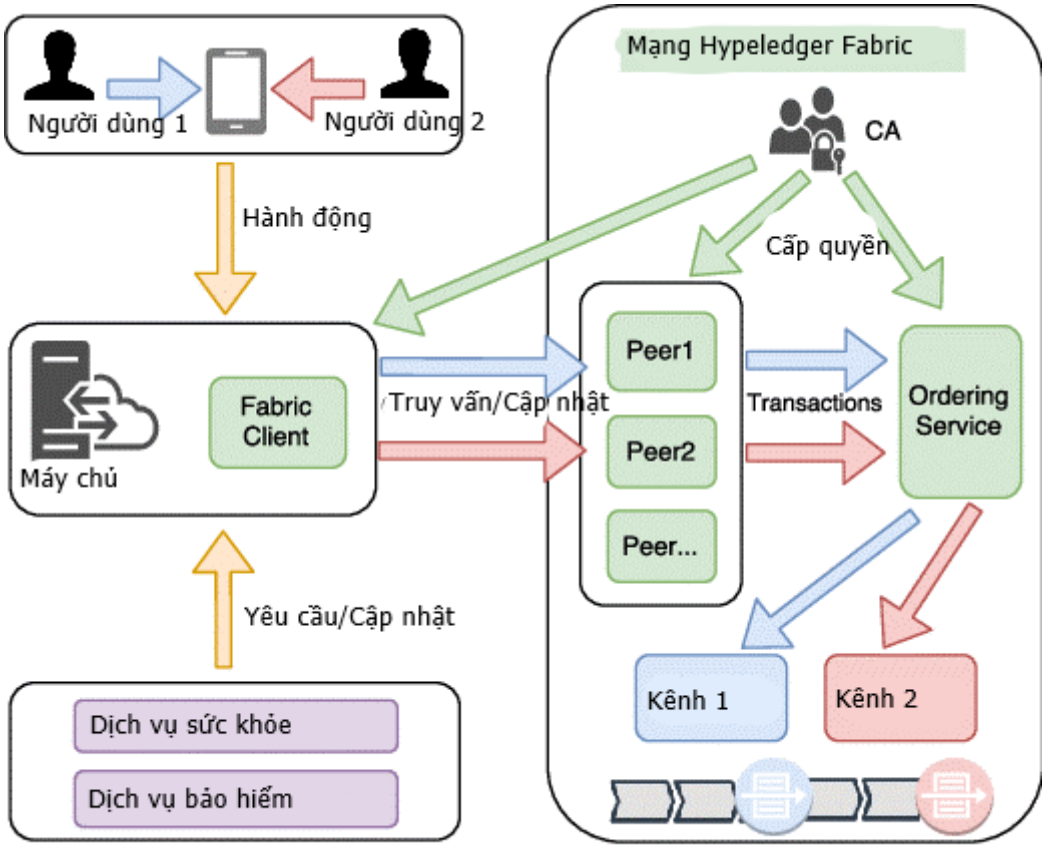
Mức độ tin cậy, khả năng mở rộng, hiệu suất

Hyperledger Fabric được xây dựng trên một kiến trúc mô đun, phân tách xử lý giao dịch thành ba giai đoạn: xử lý và thỏa thuận logic phân tán (chuỗi chuỗi mã hóa), đặt hàng giao dịch, và xác nhận giao dịch và cam kết. Sự tách biệt này tạo ra một số lợi thế: Mức độ tin cậy và xác minh ít hơn được yêu cầu trên các loại nút, và khả năng mở rộng và hiệu suất của mạng được tối ưu hóa.

Dữ liệu trên cơ sở cần biết (Data on need-to-know basis)

Các kênh được hỗ trợ trong Hyperledger Fabric cho phép dữ liệu chỉ đến các bên cần biết, đảm bảo tính bảo mật của dữ liệu.

Truy vấn phong phú trên một sổ cái phân tán bất biến



Hình 1. 16 Mô hình truy vấn thông tin trong Fabric [7]

(Trong hình trên, Fabric client là các node cung cấp dịch vụ, Ordering Service cung cấp dịch vụ phê duyệt các block)

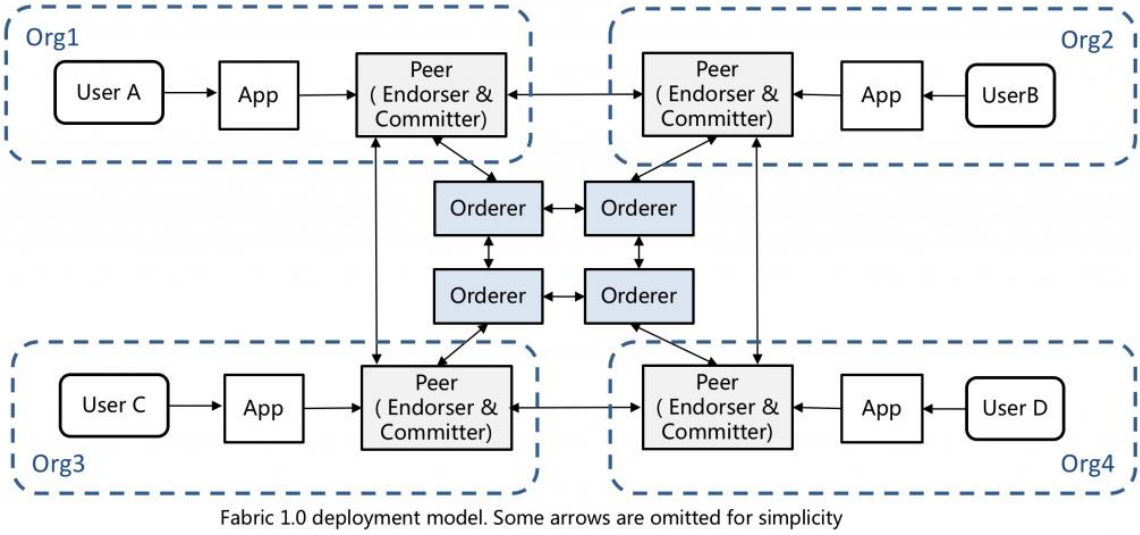
Sổ cái là bản ghi tuần tự các chuyển đổi trạng thái cho ứng dụng blockchain. Mỗi giao dịch dẫn đến một tập hợp các cặp giá trị khóa tài sản được cam kết với sổ cái khi tạo, cập nhật hoặc xóa.

Kiến trúc mô-đun hỗ trợ các thành phần plug-in

Tính mô-đun của kiến trúc Hyperledger Fabric cho phép các nhà phát triển dễ dàng tích hợp, bổ sung thêm các thành phần vào mạng blockchain. Một số mạng đa công ty đã có quản lý danh tính và muốn sử dụng lại thay vì xây dựng lại. Các thành phần khác của kiến trúc có thể dễ dàng cắm vào bao gồm cơ chế đồng thuận hoặc mã hóa, trong đó một số quốc gia có các tiêu chuẩn mã hóa riêng.

Bảo vệ khóa kỹ thuật số và dữ liệu nhạy cảm

Hỗ trợ HSM (Module bảo mật phần cứng) là rất quan trọng để bảo vệ và quản lý các khóa kỹ thuật số để xác thực mạnh mẽ. Hyperledger Fabric cung cấp PKCS11 được sửa đổi và không sửa đổi để tạo khóa, hỗ trợ các trường hợp như quản lý danh tính cần được bảo vệ nhiều hơn. Đối với các tình huống liên quan đến quản lý danh tính, HSM tăng khả năng bảo vệ khóa và dữ liệu nhạy cảm.



Hình 1. 17 Mô hình triển khai Fabric [7]

Mô tả các thành phần trong mô hình trên:

- Org 1, 2, 3, 4 là các tổ chức tham gia mạng blockchain
- User A, user B, user C, user D là người dùng trong các tổ chức tương ứng
- App: Ứng dụng tương tác với mạng blockchain
- Peer (Endorser & Commiter): Các node trong mạng làm nhiệm vụ phê duyệt các giao dịch
- Oderer: Các node trong mạng làm nhiệm vụ hình thành các block

1.5. Ứng dụng của blockchain

Với những ưu điểm của mình, Blockchain nói chung và Hyperledger Fabric nói riêng có thể ứng dụng vào nhiều lĩnh vực khác nhau trong cuộc sống như: hệ thống quản lý Chứng minh nhân dân, bầu cử, hồ sơ y bạ, hợp đồng thông minh, chuỗi cung ứng, dịch vụ tài chính, …[8]

Ứng dụng blockchain trong giáo dục

Blockchain có thể được ứng dụng để lưu trữ dữ liệu bảng điểm, quá trình đào tạo, kinh nghiệm thực tế, lịch sử tuyển dụng của từng cá nhân. Trong thực tế, khi đăng ký tuyển dụng hoặc xin học bổng nhiều, thường xuyên xảy ra tình huống ứng viên đã cung cấp thông tin của mình không chính xác, đa phần là kê khai thông tin cao hơn so với năng lực, trình độ, kinh nghiệm thực tế bản thân nhằm đáp ứng đủ điều kiện xét/thi tuyển.

Ngoài ra, blockchain còn có thể được ứng dụng để thực thi tự động các điều khoản trong quy chế đào tạo thông qua hình thức hợp đồng thông minh của blockchain. Hợp đồng thông minh giúp xử lý vấn đề "không giữ lời hứa. Khác biệt với hợp đồng truyền thống, trong hợp đồng thông minh, một khi điều kiện được đáp ứng, việc đã thoả thuận được tự động kích hoạt mà không một bên nào có thể tác động cản trở, ngăn chặn để hợp đồng không thực hiện được. Ví dụ nếu sinh viên vi phạm một số điều trong nội quy, hệ thống sẽ ghi nhận và ban hành các biện pháp kỷ luật mà không có trường hợp ngoại lệ. Hoặc trong việc đánh giá chất lượng giảng dạy, nếu đa số sinh viên có ý kiến đánh giá môn học không mang lại kiến thức thiết yếu, thì môn học đó sẽ được tổ chức, cải tiến lại hoặc sinh viên tham gia môn học đó sẽ được đăng ký học môn học khác mà không phải nộp thêm tiền học phí.

Blockchain cũng cung cấp một cách thức đơn giản, bảo mật để đánh giá năng lực của một cá nhân dựa trên các yêu cầu tuyển sinh đầu vào. Với đặc tính bất biến, sẽ rất khó để giả mạo thông tin, ví dụ như ứng viên tuyển sinh khai đã tham gia một khoá học nhưng thực tế lại không như vậy; các nhà tuyển sinh sẽ dễ dàng xác thực được thông tin này qua công nghệ blockchain. Trong việc tuyển dụng giáo viên, blockchain cũng là công cụ cho phép tính minh bạch để lựa chọn giáo viên trong các trường học, nhằm bảo đảm rằng giáo viên sẽ được lựa chọn phù hợp với tính chất, nội dung môn học cũng như cung cấp một danh sách các môn học phù hợp với năng lực, phẩm chất của mỗi giáo viên.

Blockchain cũng có thể ứng dụng để tạo ra một cơ sở dữ liệu bảo mật về dữ liệu học tập và điểm số cho các hệ thống học trực tuyến. Công nghệ chuỗi khối sẽ cho

phép bảo đảm an toàn thông tin đối với đủ mọi loại đối tượng từ học viên, cha mẹ, giáo viên đến các trường học, doanh nghiệp.

Thực tế ứng dụng blockchain trong giáo dục trên thế giới

Nhiều trường đại học trên thế giới đã bắt đầu triển khai công nghệ blockchain để theo dõi và lưu trữ bảng điểm và bằng cấp của sinh viên và thông tin của các đơn vị đào tạo. Ví dụ có thể kể tới là dự án "Blockcerts" do Phòng nghiên cứu truyền thông MIT thuộc Viện Công nghệ Massachusetts, Hoa Kỳ phát triển vào năm 2017; Blockcerts cung cấp bằng chứng nhận cho các học viên hoàn thành một số chương trình của MIT dưới dạng số hóa trên nền bảo mật của blockchain. Trường đại học Nicosia của Cộng hòa Síp cung cấp thông tin xác thực đầy đủ cho toàn bộ chương trình của họ trên nền tảng công nghệ blockchain. Hay như cơ sở đào tạo toàn cầu của Sony (Sony Global Education) đã công bố việc phát triển chuỗi khối mới để lưu trữ các bản ghi thông tin học tập.[9]

Xu hướng nghiên cứu, triển khai công nghệ blockchain trong lưu trữ bảng điểm và đánh giá học sinh trong giáo dục phổ thông cũng nhận được nhiều quan tâm của nhiều nước trên thế giới. Công ty Learning is Earning đã đưa ra một phát kiến về "edublock", các khối dữ liệu về giáo dục gồm các thông tin về lịch sử học tập của cá nhân, các môn học, bài giảng, chủ đề, … mà cá nhân đó đã từng tham gia và kết quả, điểm số học tập của họ. Các khối edublock này được thu thập bởi các học viện, các trung tâm cộng đồng, … để xem xét cá nhân/ứng viên có phù hợp với công việc giảng dạy hay không, từ đó đưa ra quyết định mời cá nhân đó làm việc cho họ. Phát kiến về edublock được đánh giá có tiềm năng rất lớn, nếu dự án thành công sẽ mang lại tác động to lớn cho ngành giáo dục – đào tạo toàn cầu, và chính con người sẽ có thể sử dụng học vấn của mình làm token (thẻ xác thực) trong thế giới số.

Blockchain như một hệ thống quản lý mức độ đánh giá sự uy tín trong nghiên cứu khoa học. Trong lĩnh vực giáo dục – đào tạo, việc công bố một công trình nghiên cứu khoa học chưa đủ để đánh giá chất lượng nghiên cứu, mà còn phụ thuộc vào số lượng trích dẫn. Nhà khoa học sẽ có nhiều cơ hội thăng tiến và tuyển dụng nếu công trình của họ được trích dẫn nhiều lần và đánh giá cao bởi các nhà chuyên môn có uy

tín. Ví dụ, trường đại học sẽ kéo dài thời gian cấp học bổng cho nghiên cứu viên nếu quá trình nghiên cứu của người đó đạt kết quả tốt. Ví dụ khác, khi cơ sở đào tạo trao giải thưởng về nghiên cứu hoặc công nhận bằng cấp cho nhà khoa học, thì tương ứng với việc chuyển một phần chỉ số uy tín của mình sang cho nhà khoa học. Trường hợp nhà khoa học khi giảng dạy có thể chuyển chỉ số uy tín của mình sang học viên khi hoàn thành tốt khóa học. Cơ chế hợp đồng thông minh cho phép chi trả chỉ số uy tín khi thực hiện trích dẫn từng phần các kết quả nghiên cứu. Bất cứ ai cũng có thể đăng các thông tin trí tuệ trên chuỗi khối giáo dục và nếu thông tin trí tuệ này được trích dẫn hoặc xác nhận đồng nghĩa với người đó sẽ nhận được các chỉ số uy tín từ người trích dẫn/xác nhận.

Tiềm năng ứng dụng blockchain trong giáo dục - đào tạo của Việt Nam

Trong những năm gần đây, giáo dục – đào tạo luôn là chủ đề nóng hổi được trao đổi trong những diễn đàn về cải cách giáo dục, và đặc biệt trong những phiên Đại biểu quốc hội chất vấn các thành viên Chính phủ, giáo dục – đào tạo được đặt rất nhiều câu hỏi đòi hỏi Chính phủ đưa ra những phương án giải quyết kịp thời. Những vấn đề trong ngành giáo dục - đào tạo Việt Nam gặp phải gồm:

- Tỷ lệ thất nghiệp cao, sinh viên ra trường ngày một tăng tuy nhiên khó khăn trong tìm kiếm công việc

- Thiếu minh bạch trong hệ thống thi cử, điển hình là những vụ gian lận thi cử trong kỳ thi trung học phổ thông quốc gia năm 2018

- Năng lực của một bộ phận giáo viên chưa đáp ứng được yêu cầu.

- Ngoài ra còn có một số vấn đề khác nữa, tuy nhiên chúng ta tập trung vào các vấn đề có khả năng ứng dụng được công nghệ blockchain.

Blockchain giúp quản lý quá trình đào tạo. Với mỗi học sinh/sinh viên, toàn bộ các thông tin về quá trình đào tạo của mình sẽ được lưu trữ trên hệ thống blockchain, quản lý từ bảng điểm, thành tích, kết quả các kỳ thi. Các dữ liệu thông tin này được lưu trữ an toàn, chuẩn xác và có thể là vĩnh viễn. Đối với các nhà tuyển dụng, họ chỉ cần truy cập và xác minh dữ liệu thông tin về ứng viên trên hệ thống, công việc tuyển dụng sẽ rất dễ dàng; thậm chí một số công ty headhunter (các công ty nhân sự chuyên

đi săn tìm các ứng viên tiềm năng theo yêu cầu của các công ty khách hàng) cũng có thể sử dụng dữ liệu được công khai trên hệ thống này để "săn tìm" những ứng viên phù hợp. Điều này cho thấy blockchain có khả năng giúp kết nối giữa các nhà tuyển dụng và các sinh viên ra trường, từ đó góp phần giảm tỷ lệ thất nghiệp của nước ta.

Để giải quyết sự thiếu minh bạch trong hệ thống thi cử, điều này hoàn toàn nằm trong khả năng ứng dụng của blockchain đã được nhiều chuyên gia nhận định từ trước tới giờ. Với cơ chế chống thay đổi thông tin, dữ liệu của blockchain, thì việc sửa điểm hay gian lận thi cử dường như đã có giải pháp cụ thể.

Cơ chế hợp đồng thông minh của blockchain cho thấy khả năng ứng dụng giúp nhà trường đánh giá năng lực của đội ngũ giáo viên đang làm việc, từ đó đưa ra những phương án cải cách phù hợp.

Kết luận chương

Trong chương 1, luận văn đã trình bày các kiến thức cơ bản nhất về hệ thống Blockchain và nền tảng Hyperleder Fabric. Các kiến thức được đề cập đến bao gồm: cấu trúc giao dịch, cấu trúc block, cấu trúc mạng, cơ chế đồng bộ dữ liệu và xử lý đồng thuận, kiến trúc của một mạng Hyperledger. Đồng thời trong chương này luận văn cũng trình bày các ưu điểm của nền tảng Hyperledger Fabric, về các ứng dụng của Hyperledger Fabric trong thực tế.

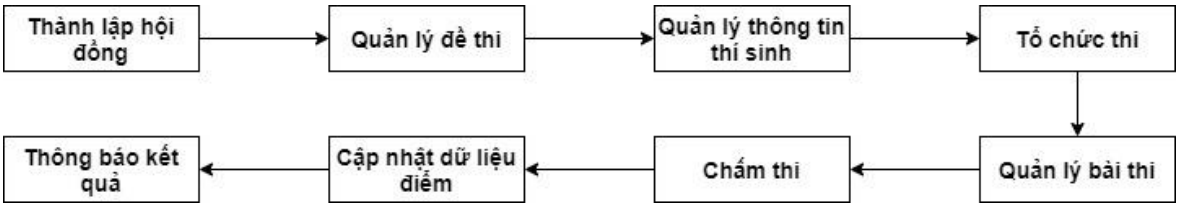
CHƯƠNG 2: ỨNG DỤNG HYPERLEDER FABRIC TRONG BÀI TOÁN PHÒNG CHỐNG GIAN LẬN THI CỬ

Trên cơ sở những ưu điểm và khả năng ứng dụng trong lĩnh vực giáo dục đã nêu trong chương trước. Chương này luận văn sẽ đi sâu vào phân tích bài toán phòng chống gian lận trong thi cử, đồng thời chỉ ra khả năng ứng dụng blockchain, cụ thể hơn là nền tảng Hyperledger Faric nhằm hạn chế các gian lận có thể xảy ra.

2.1. Bài toán phòng chống gian lận trong thi cử

2.1.1. Quy trình tổ chức thi

Trong thực tế, một kỳ thi có thể bao gồm quy trình phức tạp, gồm nhiều khâu khác nhau. Tuy nhiên trong phạm vi của luận văn, một kỳ thi giả định có thể diễn ra với quy trình như sau:

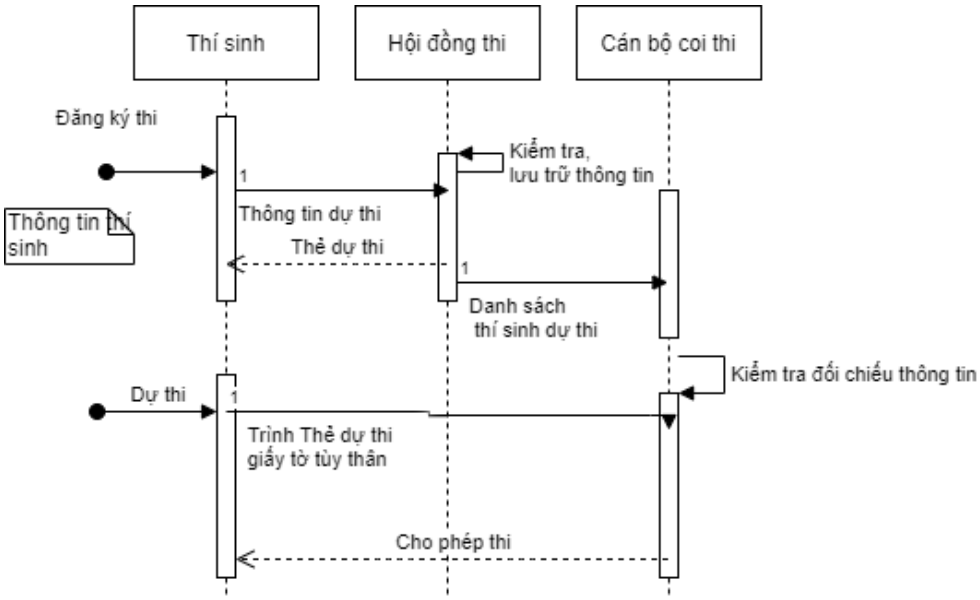


Hình 2. 1 Quy trình tổ chức thi

- Thành lập hội đồng: Thành lập và quản lý hội đồng thi
- Quản lý đề thi: Biên soạn, lưu trữ, quản lý ngân hàng câu hỏi/đề thi
- Quản lý thông tin thí sinh: Lập danh sách thí sinh dự thi
- Tổ chức thi: Sắp xếp phòng thi, xác thực thông tin thí sinh, giám sát thi, cấp phát đề
- Quản lý bài thi: Quản lý bài làm của thí sinh, quản lý phách
- Chấm điểm: Thực hiện chấm điểm bài bài làm của thí sinh
- Cập nhật kết quả thi: Quản lý phách, cập nhật điểm số cho bài làm của thí sinh, phê duyệt kết quả thi
- Thông báo kết quả thi: Thông báo kết quả thi cho thí sinh, hội đồng

Luồng thông tin trao đổi chủ yếu trong suốt quá trình thi bao gồm: thông tin thí sinh, đề thi, bài làm của thí sinh, kết quả thi.

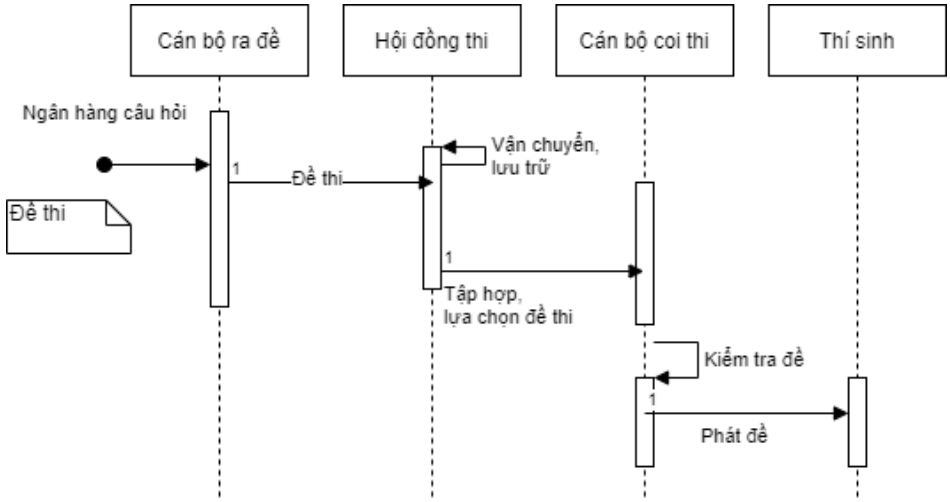
Đầu tiên thông tin thí sinh dự thi cần được kiểm tra, lưu trữ, đối chiếu trong quá trình tổ chức thi. Luồng thông tin thí sinh được mô tả trong sơ đồ dưới đây:



Hình 2. 2 Luồng dữ liệu thông tin thí sinh

Trong sơ đồ trên, thông tin thí sinh được hình thành khi thí sinh đăng ký dự thi. Các thông tin về họ tên, ngày tháng năm sinh, quê quán, trường, lớp, giới tính, ảnh chân dung được thí sinh cung cấp cho hội đồng thi để thực hiện làm thẻ dự thi và lưu trữ hồ sơ. Sau khi kiểm tra, nếu thông tin hợp lệ thí sinh sẽ được cấp thẻ dự thi, đồng thời thông tin thí sinh và phòng thi cũng được gửi cho cán bộ coi thi để thực hiện kiểm tra đối chiếu. Khi tham gia thi, thí sinh cần cung cấp thẻ dự thi và hoặc giấy tờ tùy thân để phục vụ việc đối chiếu, xác thực thí sinh. Nếu xác thực thành công, thí sinh sẽ được phép dự thi.

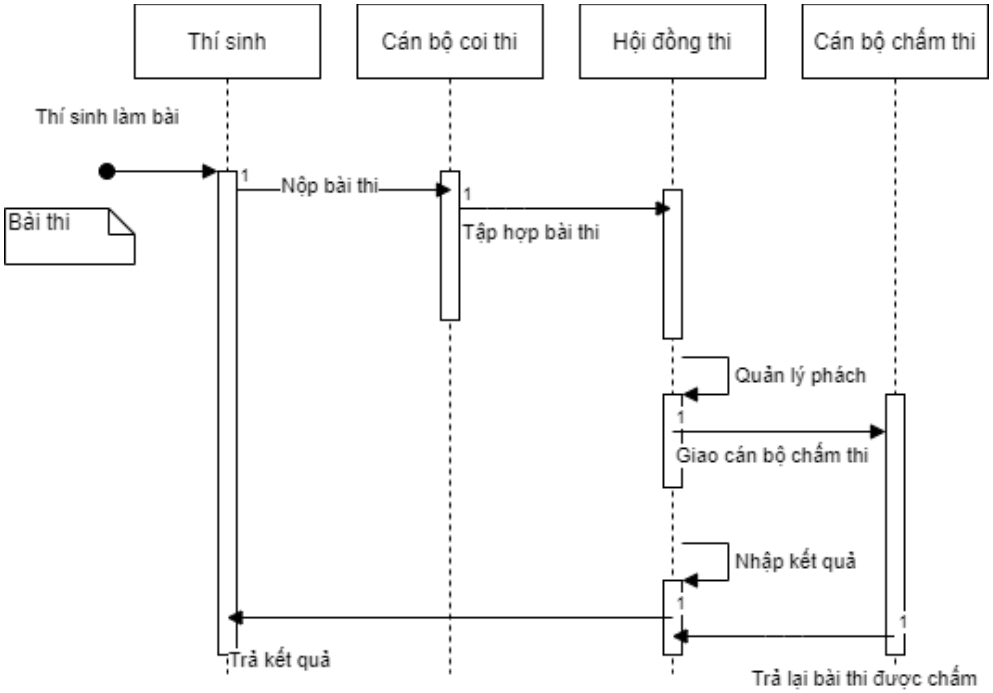
Bên cạnh thông tin thí sinh, đề thi cũng là một trong những dữ liệu quan trọng trong kỳ thi. Luồng dữ liệu cơ bản của đề thi có thể được minh họa như sau:



Hình 2.3 Luồng dữ liệu đề thi

Dữ liệu đề thi được hình thành bởi cán bộ ra đề. Sau đó được hội đồng thi lựa chọn, lưu trữ, vận chuyển đến nơi tổ chức thi. Tiếp đó, đề thi được cán bộ coi thi kiểm tra và phát cho thí sinh để thực hiện làm bài.

Dữ liệu quan trọng nhất là bài thi (bài làm) của thí sinh. Luồng thông tin dữ liệu bài thi được mô tả trong hình dưới đây:



Hình 2.4 Luồng dữ liệu bài thi

Trong sơ đồ trên dữ liệu bài thi được hình thành sau khi thí sinh nộp bài cho cán bộ coi thi. Sau đó cán bộ coi thi tập hợp các bài thi của thí sinh và nộp về hội

đồng thi. Tiếp theo, hội đồng thi sẽ bảo quản, lưu trữ bài thi, thực hiện xử lý phách và giao cán bộ chấm thi thực hiện việc chấm thi. Cán bộ chấm thi thực hiện chấm và trả lại kết quả chấm thi cho hội đồng. Hội đồng kiểm tra, lưu trữ kết quả thi và thông báo kết quả cho thí sinh.

2.1.2. Đánh giá các nguy cơ gian lận có thể xảy ra trong thi cử

Với nhiều khâu tổ chức đã nêu trong phần trước, đặc biệt trong đó có nhiều khâu có sự tham gia của con người nên hoàn toàn có thể xảy ra tiêu cực.[1]

- Đối với đề thi: Có thể xảy ra lộ, lọt đề thi từ cán bộ ra đề, vận chuyển, ...
- Đối với khâu xác thực thông tin thí sinh: Có thể xảy ra nguy cơ thi hộ do xảy ra sai sót trong quá trình xác thực thông tin thí sinh dự thi với thông tin trên thẻ dự thi.
- Quá trình làm bài: Có thể xảy ra quay cóp.
- Quá trình vận chuyển và lưu trữ bài thi: Có thể xảy ra gian lận can thiệp vào dữ liệu bài làm nhằm thay đổi đáp án.
- Quá trình quản lý phách: Có thể để lộ lọt thông tin phách dẫn tới việc lộ thông tin thí sinh.
- Quá trình chấm thi: Có thể xảy ra sai sót, tiêu cực dẫn đến điểm số không đúng với kết quả bài làm.
- Quá trình cập nhật kết quả: Có thể xảy ra gian lận cập nhật sai kết quả như nâng điểm.

Thực tế cho thấy, tại kỳ thi THPT quốc gia năm 2018 của Việt Nam [2], các tỉnh Hà Giang, Sơn La, Hòa Bình đã phát hiện hơn 200 thí sinh được nâng điểm. Trước đó, báo chí trong nước cũng đã nhiều lần phản ánh tình trạng gian lận trong các kỳ thi tại các địa phương.

2.1.3. Đề xuất giải pháp nhằm hạn chế gian lận trong thi cử

Để hạn chế tình trạng gian lận trong thi cử, trong nước cũng đã có nhiều chuyên gia đề xuất các giải pháp cho vấn đề này như tăng cường chế tài pháp luật để xử lý vi phạm; thay đổi các hình thức kiểm tra, thi cử; cho phép hệ thống kiểm định đánh giá độc lập; áp dụng các biện pháp bảo vệ nghiêm ngặt; sử dụng các công nghệ hỗ trợ

như camera giám sát, ứng dụng trí tuệ nhân tạo… Tuy nhiên hiện đang dừng ở mức ý tưởng và đề xuất hoặc chưa hoàn toàn triệt để, vẫn còn nhiều khâu quan trọng có sự tham gia của con người, đối tượng chính tạo ra gian lận, tiêu cực.

Từ những nguy cơ gian lận như đã phân tích ở trên, luận văn xác định mốt số vấn đề cần giải quyết như sau:

- Bảo mật đề thi và đáp án
- Xác thực thông tin thí sinh
- Xác thực thông tin cán bộ
- Đảm bảo toàn vẹn dữ liệu bài thi
- Bảo mật thông tin phách
- Tránh can thiệp dữ liệu điểm số

Để giải quyết các vấn đề trên, luận văn đề xuất giải pháp như sau:

- Đối với đề thi: Đề thi sẽ được khởi tạo, lưu trữ và quản lý bằng cơ sở dữ liệu tập trung. Có cơ chế bảo vệ chống sao chép, khai thác trái phép.

- Đối với dữ liệu thí sinh: Dữ liệu thí sinh sẽ được lưu trữ số hóa. Việc xác nhận thông tin thí sinh được thực hiện tự động, có sự trợ giúp của máy tính và công nghệ nhận dạng.

- Đối với dữ liệu bài thi: Thí sinh sẽ thực hiện làm bài trên máy tính. Ngay sau khi thí sinh nhấn nộp bài, hệ thống tự động mã hóa và lưu trữ dữ liệu bài làm, đảm bảo rất khó hoặc không thể bị can thiệp nhằm thay đổi nội dung. Trong trường hợp thi trắc nghiệm, bài làm của thí sinh sẽ được chấm tự động. Kết quả bài làm của thí sinh cũng được tự động lưu trữ, hạn chế sự can thiệp trái phép từ các yếu tố con người.

Việc đảm bảo tính minh bạch và tin cậy trong kỳ thi là vấn đề vô cùng quan trọng, đây cũng chính là giá trị cốt lõi mà blockchain mang lại. Giải pháp sử dụng blockchain với các kỹ thuật mã hóa và mô hình ứng dụng áp dụng vào việc quản lý bài thi. Các dữ liệu này sẽ được niêm phong bằng việc mã hóa với tem thời gian. Để can thiệp và sửa đổi, người can thiệp cần phải bóc tem thời gian này ra. Nếu mất tem thời gian chúng ta có thể dễ dàng nhận biết dữ liệu đã bị thay đổi.

2.1.4. Phạm vi bài toán

Bài toán ứng dụng blockchain trong công tác thi cử có nhiệm vụ chính là tổ chức một kỳ thi trắc nghiệm trên máy tính, các thí sinh sẽ là bài thi trên trang web, kết quả sẽ được chấm một cách tự động và sau đó lưu lên trên mạng blockchain. Khi thí sinh muốn biết điểm thì có thể tra cứu trên hệ thống, điểm sẽ được bảo đảm về tính toàn vẹn và minh bạch.

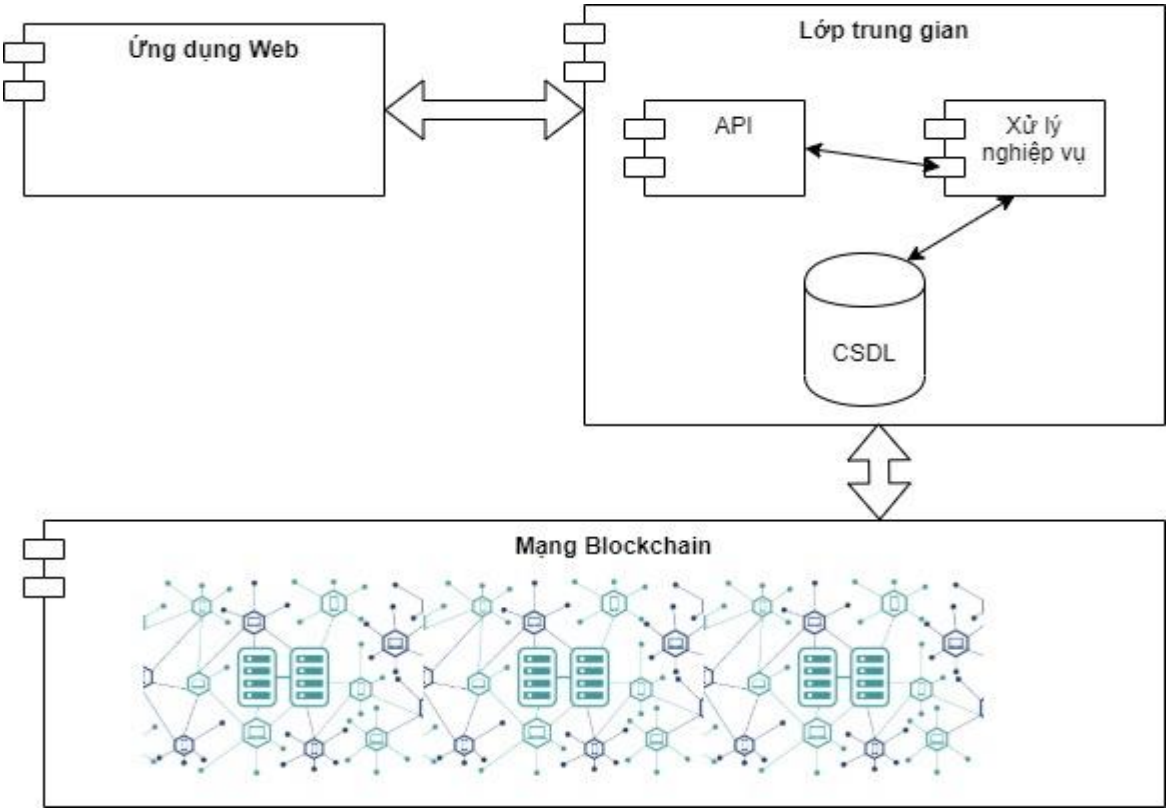
Với đặc điểm của các kỳ thi là bảo mật điểm của thí sinh chỉ có cá nhân thí sinh và những người có thẩm quyền mới xem được điểm vì vậy trong bài toán này sẽ sử dụng mạng private blockchain. Trong đó, Hyperledger Fabric là một mạng private blockchain điển hình, được sinh ra để phục vụ cho mục đích giao dịch riêng tư giữa các doanh nghiệp và có thể áp dụng trong bài toán này. Luận văn sẽ tập trung giải quyết đối với hình thức thi trắc nghiệm, đối với hình thức thi trắc nghiệm sẽ cần phải xem xét và phát triển thêm. Bên cạnh đó, ứng dụng thi sẽ được thiết kế để có thể cho phép một lượng lớn các thí sinh thi cùng lúc bằng việc sử dụng biện pháp cân bằng tải và các biện pháp đảm bảo tính khả dụng khác.

Việc giới hạn phạm vi bài toán là cơ sở cần thiết cho việc lựa chọn các phương pháp phù hợp để giải quyết bài toán.

2.2. Đề xuất mô hình ứng dụng Blockchain vào bài toán phòng chống gian lận thi cử

2.2.1. Mô hình tổng thể

Mô hình ứng dụng dự kiến sẽ bao gồm 02 khối: Khối ứng dụng (gồm ứng dụng web và lớp trung gian) và khối mạng Blockchain



Hình 2.5 Mô hình tổng thể ứng dụng

Ứng dụng web:

Cung cấp giao diện dạng Web cho người sử dụng cuối là thí sinh, giám thị, hội đồng thi. Bên cạnh đó bao gồm một số chức năng của hệ thống.

Lớp trung gian:

Xử lý các nghiệp vụ chính của hệ thống (xử lý thông tin thí sinh, thông tin đề thi, …), cung cấp các API cho ứng dụng web và giao tiếp với mạng blockchain thông qua các API.

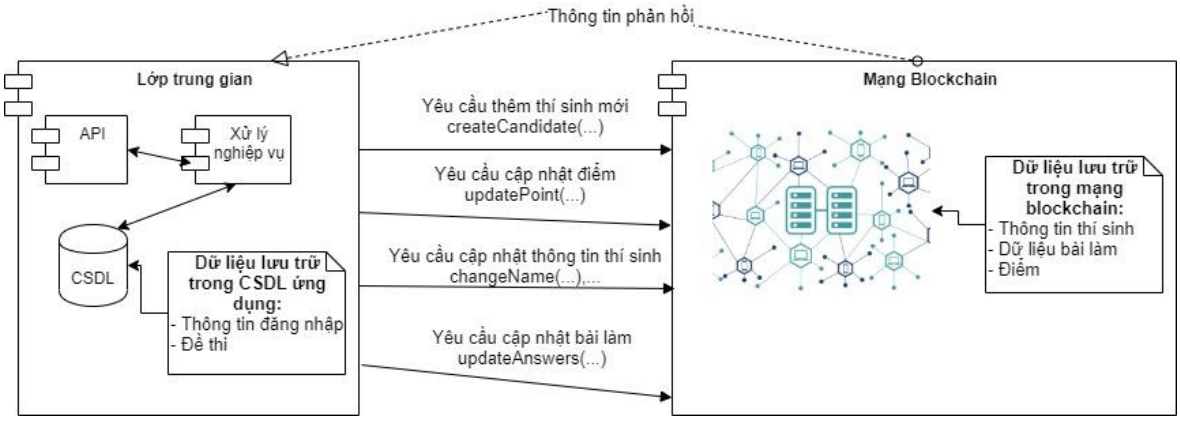
Lớp này cũng sẽ bao gồm CSDL lưu trữ thông tin người dùng (thí sinh, cán bộ) phục vụ đăng nhập hệ thống (chỉ lưu thông tin username, mật khẩu và một số thông tin khác phục vụ quản lý người dùng cho ứng dụng web), dữ liệu đề thi.

Mạng blockchain:

Sử dụng nền tảng hyperledger fabric để lưu trữ thông tin thí sinh, dữ liệu bài làm và điểm số của thí sinh.

Trong mô hình trên, ứng dụng web sẽ nằm trên một mạng riêng để tránh truy cập từ bên ngoài và chỉ có lớp trung gian có thể truy cập ra được bên ngoài để gửi điểm lên mạng blochain. Quá trình trao nhận dữ liệu phải sử dụng phương thức HTTPS để đảm bảo dữ liệu trên đường truyền.

Dữ liệu thí sinh liên kết giữa ứng dụng và mạng blockchain là một mã khóa riêng được sinh tương ứng với từng thí sinh khi thêm mới thông tin thí sinh. Mã khóa này sẽ sử dụng để cập nhật thông tin bài làm, điểm số, thông tin thí sinh, truy vấn thông tin từ ứng dụng vào mạng blockchain. Luồng dữ liệu chủ yếu trao đổi giữa ứng dụng và mạng blockchain được mô tả trong hình dưới đây:



Hình 2. 6 Luồng dữ liệu trao đổi giữa ứng dụng và mạng blockchain

Đối với kỳ thi thực tế, số lượng thí sinh tham gia đồng thời có thể lớn. Để đảm bảo tính khả dụng của hệ thống cần phải tính đến phương án cân bằng tải (load balancer). Đề xuất sử dụng công nghệ Kubernetes (sẽ được làm rõ thêm trong phần sau) để cân bằng tải, cụ thể mô hình như sau: máy chủ ứng dụng web và lớp trung gian cần được triển khai lên nhiều máy chủ và load balancer.

2.2.2. Mạng blockchain

Mô hình mạng blockchain sẽ bao gồm các tổ chức Orgx tương ứng với các tổ chức/đơn vị có quyền tổ chức kỳ thi. Mỗi tổ chức sẽ bao gồm các node ngang hàng(peer), các oderer tương ứng với các đơn vị trong tổ chức có quyền thực hiện phê duyệt kết quả thi. Thực tế triển khai sẽ cần dựa vào khả năng sẵn sàng về cơ sở hạ tầng của các tổ chức.

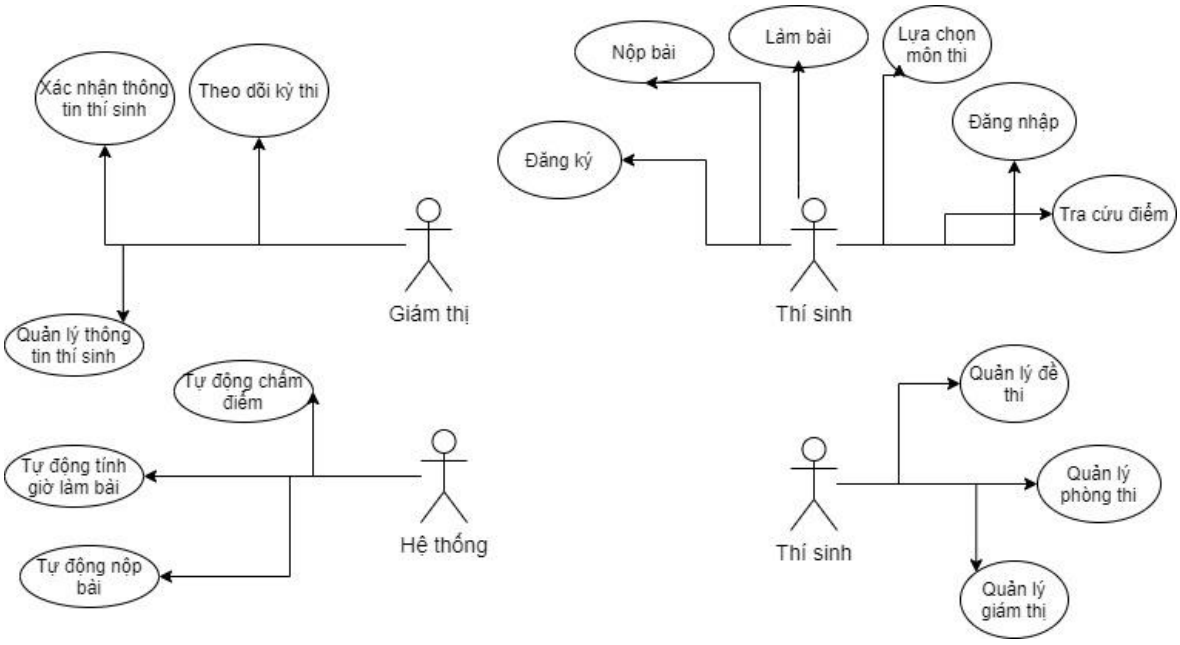
Cơ sở dữ liệu thí sinh, bài thi, điểm thi sẽ được lưu trữ trong mạng blockchain sử dụng cơ sở dữ liệu CouchDB (theo đề xuất của IBM đối với nền tảng Hyperledger Fabric).

Xây dựng các phương thức hoạt động trên chaincode:

- Truy vấn tất cả bản ghi thí sinh trên sổ cái
- Truy vấn thí sinh theo ID
- Thêm mới một bản ghi vào sổ cái
- Truy vấn tất cả bản ghi thí sinh trên sổ cái để xem bản ghi vừa được thêm mới
- Thay đổi điểm của một thí sinh bất kỳ nào đó
- Truy vấn lại sổ cái và xem sự thay đổi

2.2.3. Ứng dụng web

Cung cấp giao diện cho người sử dụng cuối, bao gồm quản trị hệ thống, hội đồng thi, giám thị, thí sinh. Các chức năng chính của hệ thống phân chia theo đối tượng tác động vào hệ thống bao gồm:



Hình 2. 7 Chức năng chính của Ứng dụng web

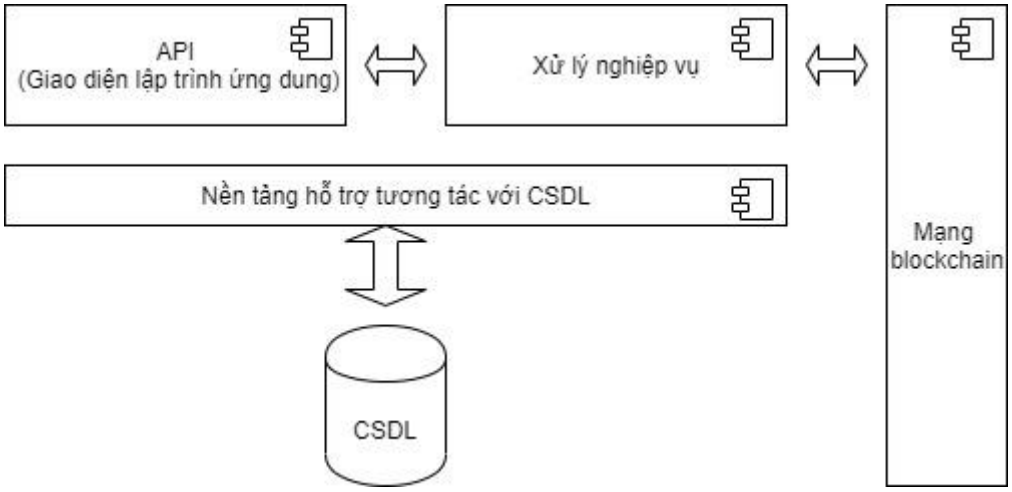
- Giám thị: Quản lý thông tin thí sinh, xác nhận thí sinh dự thi, theo dõi kỳ thi.
- Thí sinh: Đăng ký, đăng nhập, lựa chọn môn thi, làm bài, nộp bài, tra cứu điểm.
- Hội đồng thi: Quản lý đề thi, quản lý giám thị, quản lý và thiết lập phòng thi.

- Hệ thống: Cung cấp các chức năng cho quản trị hệ thống, các chức năng tự động như tự động làm bài, nộp bài, chấm điểm.

Ứng dụng web sẽ giao tiếp với lớp trung gian thông qua API do lớp này cung cấp

2.2.4. Lớp trung gian

Đây là module có chức năng đảm bảo các nghiệp vụ chính của toàn bộ ứng dụng. Lớp trung gian sẽ tiếp nhận các yêu cầu xử lý từ ứng dụng web để thực hiện các nghiệp vụ tương ứng, đảm nhận nhiệm vụ giao tiếp với mạng blockchain để thực hiện các cập nhật, truy vấn thông tin. Module này sẽ có kiến trúc như sau:



Hình 2. 8 Kiến trúc lớp trung gian

- API: Đây là cung cấp các giao diện lập trình tương tác với module Ứng dụng web để thực hiện xử lý các nghiệp vụ liên quan

- Xử lý nghiệp vụ: Thực hiện các nghiệp vụ của kỳ thi như: xử lý thông tin thí sinh, đề thi, giao tiếp với mạng Blockchain

2.3. Đề xuất một số công nghệ khác sử dụng để tăng tính khả dụng của ứng dụng

2.3.1. Docker

Docker là 1 framework (khung làm việc) hỗ trợ việc tạo môi trường ảo trên máy chủ linux (1 loại hệ điều hành) nhanh gọn và đơn giản. Docker được thiết kế để tạo mới, chạy các tứng dụng bằng cách sử dụng các container. Container là phương pháp

ảo hóa ở mức hệ điều hành, cho phép chạy một ứng dụng cùng các thư viện mà ứng dụng đó phụ thuộc trong các tiến trình có tài nguyên được cách ly. Container giúp đóng gói mã, công cụ hệ thống, các cấu hình ... của ứng dụng vào trong một khối duy nhất gọi là ảnh container. Container giúp đảm bảo ứng dụng có thể triển khai một cách nhanh chóng, độ tin cậy cao và nhất quán.

Dokerfile

Docker sử dụng Dockerfile để mô tả các lớp ảnh, các câu lệnh cần thực hiện cho việc build ảnh container. Dockerfile chứa tập hợp các lệnh để docker có thể đọc hiểu và thực hiện để đóng gói thành một ảnh (image) theo yêu cầu của người phát triển. Dockerfile là một tệp văn bản chứa tất cả các câu lệnh để chỉ dẫn cho docker xây dựng ảnh. Bằng cách sử dụng câu lệnh *docker build,* docker sẽ tự động thực thi các câu lệnh mà người phát triển soạn thảo trong dockerfile.

Dockercompose

Docker compose là một công cụ dùng để quản lý và liên kết nhiều containers, mỗi container chạy 1 service riêng biệt nhưng phục vụ chung một ứng dụng. Docker-compose có định dạng giống các tệp yaml (key – value hay khóa – giá trị), chứa các chỉ dẫn để khởi động, liên kết các container với nhau

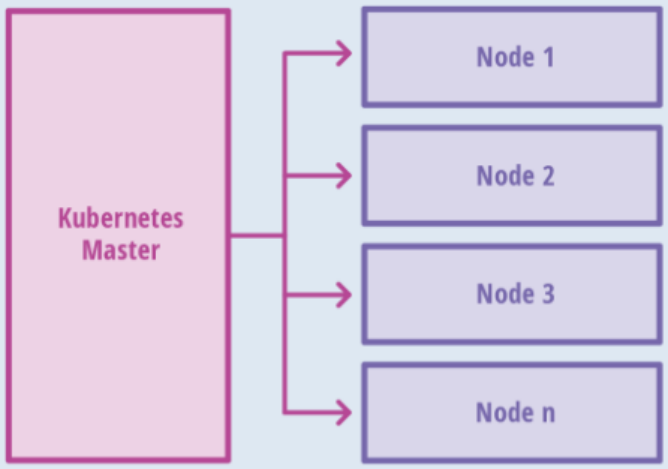
2.3.2. Kubernetes

Kubernetes (còn gọi là K8s) là một nền tảng điều phối mã nguồn mở được phát triển sau hơn một thập kỷ chạy các ứng dụng container của Google. K8s dùng để tự động hoá việc quản lý, co giãn (scaling) và triển khai ứng dụng dưới dạng container hoá.[12]

Các khái niệm trong Kubernetes

Kubernetes Cluster

Một cluster là một tập các máy vật lý hay máy ảo được sử dụng bởi Kubernetes để chạy các ứng dụng. Một cluster bao gồm một *master node* (chủ) và các *worker nodes* (thực thi), ngoài ra còn có các thành phần khác *etcd* cung cấp chức năng lưu trữ phân tán các giá trị dạng key – value, …

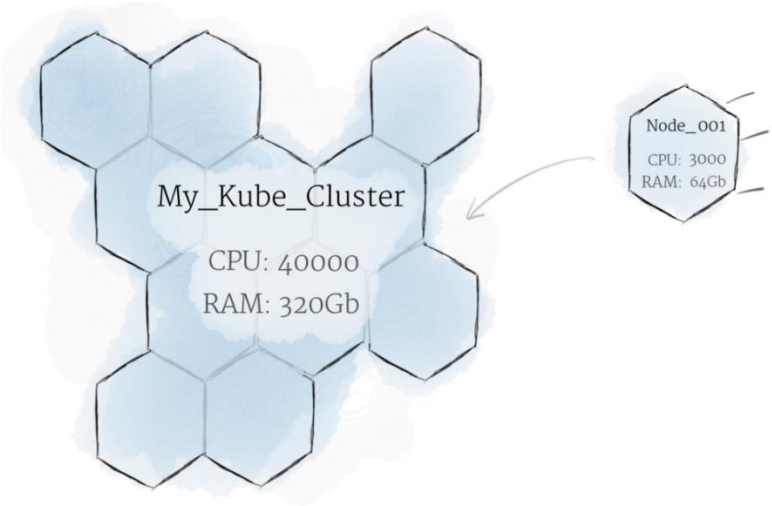


Hình 2.9 Mô hình node trong kubernetes

Nodes

Một node là một máy ảo hoặc máy vật lý chạy Kubernetes. Nodes hay còn gọi là docker host

Kubernetes cho phép dễ dàng kết hợp các node đơn lẻ với nhau tạo thành các cụm máy tính (Kube cluster) với sức mạnh xử lý lớn hơn, tang khả năng chịu tải.



Hình 2.10 Kết hợp các node trong kubernetes

Pods

Trong kubernetes, Pod là một tập hợp các container được triển khai và quản lý cùng nhau nhằm thực hiện một mục đích nào đó. Nhóm này chia sẻ không gian lưu trữ, địa chỉ IP với nhau. Pod thì được tạo ra hoặc xóa tùy thuộc vào yêu cầu của dự

án. Đơn vị nhỏ nhất của ứng dụng chạy Kubernetes đó là container, nhưng đơn vị quản lý cơ bản nhất thì là Pods. Trong Kubernetes, các pod có thể xuất hiện hoặc biến mất trên mỗi máy tùy thuộc vào tài nguyên hiện tại.

Deployment

Deployment trong Kubernetes dùng để phân phối các pods cho các nodes cụ thể, mang tính dự phòng.

Với đặc điểm kể trên, K8s phù hợp đề triển khai cho mô hình ứng dụng thi, đảm bảo khả năng triển khai nhanh chóng, đáp ứng tính khả dụng của hệ thống.

2.3.3. MongoDB

MongoDB là một hệ quản trị cơ sở dữ liệu mã nguồn mở được thiết kế theo kiểu hướng đối tượng trong đó các bảng được cấu trúc một cách linh hoạt cho phép các dữ liệu lưu trên bảng không cần phải tuân theo một dạng cấu trúc nhất định nào. Chính do cấu trúc linh hoạt này nên MongoDB có thể được dùng để lưu trữ các dữ liệu có cấu trúc phức tạp và đa dạng và không cố định (hay còn gọi là Big Data).[11]

Lợi thế của mongodb so với các cơ sở dữ liệu dạng quan hệ

Cấu trúc của một đối tượng là rõ rang (Dữ liệu được lưu trong các tài liệu kiểu JSON)

- Khả năng mở rộng dễ dàng
- Các truy vấn đa dạng.
- Cập nhật nhanh hơn.

Do đề thi có cấu trúc đa dạng (nhiều dạng câu hỏi, nhiều phương án trả lời khác nhau) nên đề xuất sử dụng mongodb để lưu thông tin đề thi để đảm bảo tính linh hoạt về cấu trúc.

Kết luận chương

Trong chương 2, luận văn đã trình bày tổng quan bài toán phòng chống gian lận trong thi cử. Cụ thể hơn, luận văn đã phân tích quy trình tổ chức một kỳ thi, đánh giá

các nguy cơ gian lận có thể xảy ra. Từ đó luận văn cũng đề xuất giải pháp để hạn chế các nguy cơ này. Chương này cũng xác định phạm vi bài toán, từ đó đề xuất mô hình ứng dụng blockchain, cụ thể là nền tảng Hyperledger Fabric vào giải quyết bài toán đã đặt ra. Ngoài ra chương này cũng giới thiệu và đề xuất một số công nghệ được phối hợp sử dụng để tang tính khả dụng của ứng dụng.

CHƯƠNG 3: TRIỂN KHAI THỬ NGHIỆM VÀ ĐÁNH GIÁ KẾT QUẢ

Trên cơ sở mô hình đã đề xuất trong chương trước, chương này luận văn sẽ trình bày mô hình triển khai thử nghiệm trong thực tế và đánh giá kết quả đạt được. Tuy nhiên trong khuôn khổ luận văn này, hệ thống thử nghiệm chỉ mang tính chất demo, mô phỏng hoạt động của hệ thống.

3.1. Mô hình triển khai thử nghiệm

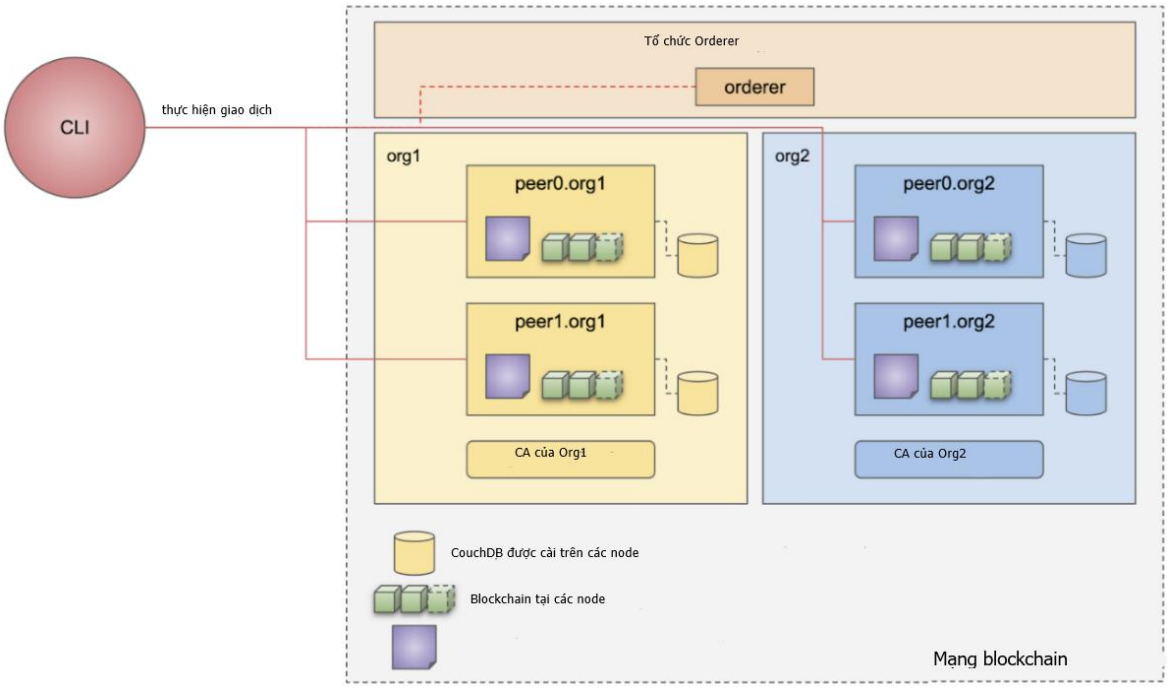
3.1.1. Môi trường thử nghiệm

Trên thực tế để triển khai mạng blockchain cần nhiều node tham gia để đảm bảo tính phi tập trung của mạng, đối với ứng dụng cũng cần triển khai trên hạ tầng có khả năng co giãn dễ dàng để đảm bảo tính khả dụng của hệ thống. Tuy nhiên trong khuôn khổ của luận văn, hệ thống được thử nghiệm trên môi trường giả lập, sử dụng 01 máy server có cấu hình bộ nhớ 32 GB, chip xử lý 2.5 GHz (8 nhân), ổ cứng SSD 512 GB. Máy chủ được cài đặt nền tảng docker và kubenetes để phục vụ việc triển khai các ứng dụng web cũng như các thành phần trong hạ tầng mạng blockchain

3.1.2. Xây dựng mạng blockchain dựa trên nền tảng Hyperledger Fabric

Mạng blockchain giả lập bao gồm 2 tổ chức: Tổ chức giáo dục 1(Org1) và tổ chức giáo dục 2 (Org2), mỗi tổ chức có hai node peer0 và peer1. Một tổ chức quản lý thi đóng vai trò orderer bao gồm một node orderer.

Mỗi node ngang hàng sử dụng cơ sở dữ liệu CouchDB để lưu trữ thông tin trong sổ cái. Tất cả các thành phần được triển khai dưới dạng các Container và chạy trên một máy chủ như đã đề cập ở phần trên



Hình 3. 1 Mô hình mạng blockchain sử dụng Hyperledger Fabric

Phần này sẽ trình bày thiết kế cơ sở dữ liệu lưu trữ thông tin thí sinh, chaincode, các API để tương tác với mạng blockchain

Cơ sở dữ liệu

Thông tin được lưu trữ trong dữ liệu sổ cái của mạng blockchain bao gồm thông tin thí sinh, thông tin bài làm của thí sinh, điểm số. Dữ liệu này có định dạng như sau:

```
{
   HoTen: Lưu Quang Đạt,
   DiaChi: Hà Nội,
   MaDuThi: M18IS000128,
   Cmnd: 123456789,
   MaDe: WKJH,
   BaiLam:1-A; 2-B; 3-C; 4-D
   Diem: 8
}
```

Chaincode

Chaincode được xây dựng dựa trên SDK do IBM cung cấp cho nền tảng NodeJS. Một chaincode sẽ phải thực thi các giao diện bao gồm 2 hàm: *Init* và *Invoke*

Hàm *Init* sẽ được gọi mỗi khi chaincode được *instantiate* hoặc *upgrade* trong channel. Nó có dạng như sau:

```
func(t*SimpleChaincode) Init(stubshim.ChaincodeStubInterface) pb.Response{}
shim.ChaincodeStubInterface) pb.Response {}
```

Hàm *Invoke* sẽ được gọi mỗi khi cần truy vấn dữ liệu hoặc tạo transaction trong Fabric.

```
func (t *SimpleChaincode) Invoke(stub shim.ChaincodeStubInterface) pb.Response {}
```

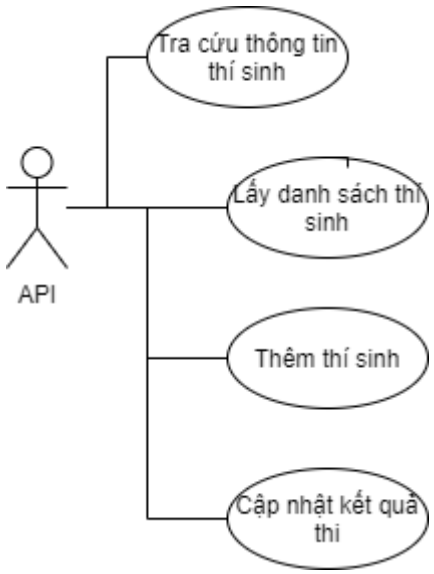
Ngoài ra, Chaincode sẽ có các hàm để tương tác với dữ liệu được lưu trữ trong sổ cái bao gồm:

- *async getCandidate(ctx, candidateId){…}*
- *async createCandidate(ctx, candidateId, HoTen, GioiTinh, DiaChi, MaDuThi, NgaySinh, CMT, KT, BaiLam, Diem) {…}*
- *async getAllCandidates(ctx){…}*
- *async changePoint(ctx, CandidateId, newPoin){…}*
- *async changeName(ctx, CandidateId, newName){…}*
- ...

Ngoài ra ta cần lập trình các API tương tác với mạng blockchain để cung cấp cho lớp trung gian. Cụ thể các tệp query.js và invoke.js thực hiện tương tác với các hàm trong chaincode nhằm truy vấn hoặc thay đổi trạng thái của sổ cái trong kênh.

Xây dựng bộ API để tương tác với mạng blockchain

Để tương tác được với mạng blochain, hệ thống xây dựng một số API như sau:



Hình 3. 2 API tương tác với mạng blockchain

- API lấy thông tin một thí sinh:

Url: https://domain/api/query/id trong đó id là mã dự thị của thí sinh

Method: Get

Header: Authorization: ‘mã bí mật được cấp’

Respone: {"CMND":"123456788","DiaChi":"Thái Nguyên", "Diem":"5", "HoTen":"Mai Thu Nga", "MaDe":"MVIK", "MaDuThi":"M18IS000199", "NgaySinh":"01/01/1996"}

- API lấy danh sách thí sinh:

Url: https://domain/api/queryall

Method: Get

Header: Authorization: ‘mã bí mật được cấp

Respone: Chuỗi JSON chứa danh sách thí sinh

- API thêm thí sinh:

Url: https://domain/api/create

Method: POST

Param:{"CMND":"123456788","DiaChi":"Thái Nguyên","Diem":"5","HoTen":"Mai Thu Nga", "MaDe":"MVIK", "MaDuThi":"M18IS000199", "NgaySinh":"01/01/1996"}

Header: Authorization: ‘mã bí mật được cấp’

Respone: {status: True, mss: ‘Thêm thành công’}

- API cập nhật điểm cho thí sinh:

Url: https://domain/api/updatePoint

Method: POST

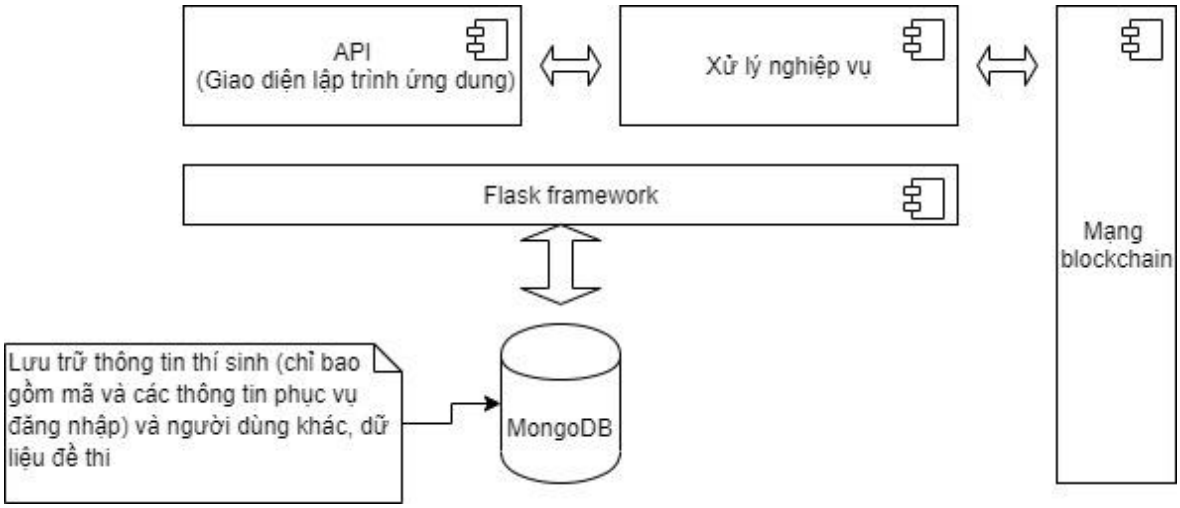
Param: {“MaDuThi”: “M18IS000199”, “Diem”: “5”}

Header: Authorization: ‘mã bí mật được cấp’

Respone: {status: True, mss: ‘Cập nhật thành công’}

3.1.3. Xây dựng Lớp trung gian

Lớp trung gian sẽ bao gồm phần xử lý các logic nghiệp vụ như kiểm tra thông tin thí sinh, kiểm tra quyền, quản lý thông tin đề thi, quản lý người dùng, … Lớp trung gian được xây dựng sử dụng ngôn ngữ Python với Flask framework với đặc điểm đơn giản, linh hoạt, dễ dàng triển khai.



Hình 3. 3 Kiến trúc lớp trung gian

Thiết kết cơ sở dữ liệu

Theo mô hình đề xuất, lớp trung gian sẽ sử dụng hệ quản trị cơ sở dữ liệu Mongodb để lưu trữ thông tin đăng nhập của thí sinh và người dùng khác, dữ liệu đề thi, …

Mô hình cơ sở dữ liệu gồm hai bảng là user (chứa thông tin đăng nhập của thí sinh và dethi (chứa thông tin đề thi).

Bảng user có cấu trúc như sau:

```
{
   Username: M18IS000199
   Password: 20fb05713e46ca7ed1b1e3675f35a52b
   Secret_key: BHGFSEAYDHETDJSY
   Create_time: 157337509
   Token: udfadfafa-adfasdf-fasdfasdf-ddwdw (Token được cấp sau khi đăng nhập)
```

Token_otp: jfdqwr-rrwxgawrf-fawfv (Token opt được cấp sau khi nhập đúng mật khẩu dùng 1 lần)

}

Các trường thông tin trong bảng user:

- Username: Tên đăng nhập là mã dự thi
- Password: Mật khẩu đã mã hóa md5 sẽ được cấp khi vào phòng thi
- Secret_key: Mã bí mật để tạo mã xác thực
- Token: mã được cấp khi đăng nhập thành công để có thể gọi được api
- Token_otp: mã được cấp sau khi xác thực mật khẩu một lần thành công, sử dụng cùng với mã Token để có thể gọi API

Bảng dethi có cấu trúc như sau:

{

Id: Id của đề thi

Exam: [

{Question: Nội dung câu hỏi, AnsA: Phương án A, AnsB: Phương Án B, AnsC: phương án C, AnsD: phương án D, TrueAns: Đáp án},{…}, …]

}

Các trường thông tin trong bảng dethi:

- Id: mã đề, sau khi đăng nhập thành công thì hệ thống sẽ lấy thông tin mã đề của thí sinh trên mạng blockchain và truy vấn dữ liệu đề thi cho thí sinh
- Exam: Đề thi

Xây dựng API cho ứng dụng Web

Các API này được xây dựng để cung cấp cho ứng dụng web gồm một số API sau:

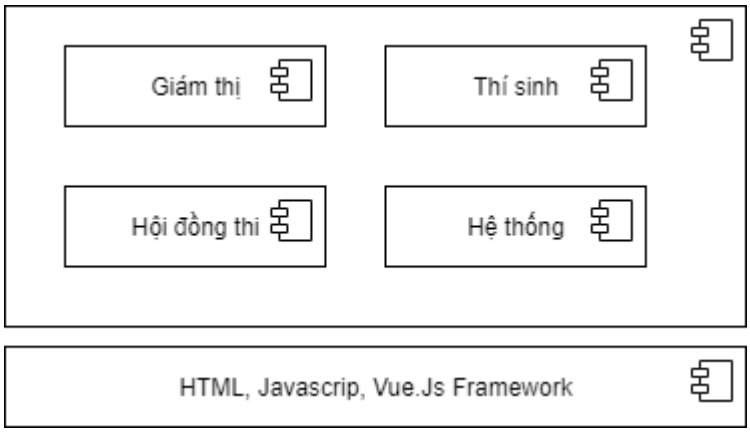
- Xác thực thông tin người dùng
- Lấy thông tin đề thi
- Nộp bài

- Thêm/cập nhật thông tin thí sinh

3.1.4. Xây dựng ứng dụng web

Trong phạm vi hệ thống thử nghiệm, ứng dụng web được xây dựng dựa trên nền tảng Vue.js framework, cùng với một số công nghệ hỗ trợ như Boostrap (công nghệ hỗ trợ tạo và quản lý giao diện dựa trên CSS). Các công nghệ này giúp cho việc triển khai ứng dụng một cách nhanh chóng, dễ dàng tiếp cận và sử dụng. Ứng dụng web sẽ giao tiếp với lớp trung gian thông qua bộ API do lớp này cung cấp.

Kiến trúc của ứng dụng web sẽ như sau:



Hình 3. 4 Kiến trúc ứng dụng web

3.2. Cài đặt và triển khai thử nghiệm

3.2.1. Mạng Blockchain

Cài đặt Hyperledger Fabric:

curl -sSL http://bit.ly/2ysbOFE | bash -s -- 1.4.2 1.4.2 0.4.15

Thiết lập network:

echo y | ./byfn.sh down

echo y | ./byfn.sh up -a -n -s couchdb

Cài đặt chaincode lên các node trong channel:

```
echo  "Installing smart contract on peer0.org1.example.com"
docker exec \
    -e CORE_PEER_LOCALMSPID=Org1MSP \
    -e CORE_PEER_ADDRESS=peer0.org1.example.com:7051 \
    -e CORE_PEER_MSPCONFIGPATH=${ORG1_MSPCONFIGPATH} \
    -e CORE_PEER_TLS_ROOTCERT_FILE=${ORG1_TLS_ROOTCERT_FILE} \
    cli \
    peer chaincode install \
        -n fabcar \
        -v 1.0 \
        -p "$CC_SRC_PATH" \
        -l "$CC_RUNTIME_LANGUAGE"
```

Hình 3. 5 Triển khai chaincode lên các node

Khởi tạo sổ cái

```
echo "Submitting initLedger transaction to smart contract on mychannel"
echo "The transaction is sent to the two peers with the chaincode installed
(peer0.org1.example.com and peer0.org2.example.com) so that chaincode is built before receiving the following requests"
docker exec \
  -e CORE_PEER_LOCALMSPID=Org1MSP \
  -e CORE_PEER_MSPCONFIGPATH=${ORG1_MSPCONFIGPATH} \
  cli \
  peer chaincode invoke \
    -o orderer.example.com:7050 \
    -C mychannel \
    -n fabcar \
    -c '{"function":"initLedger","Args":[]}' \
    --waitForEvent \
    --tls \
    --cafile ${ORDERER_TLS_ROOTCERT_FILE} \
    --peerAddresses peer0.org1.example.com:7051 \
    --peerAddresses peer0.org2.example.com:9051 \
    --tlsRootCertFiles ${ORG1_TLS_ROOTCERT_FILE} \
    --tlsRootCertFiles ${ORG2_TLS_ROOTCERT_FILE}
```

Hình 3.6 Khởi tạo sổ cái

3.2.2. Lớp trung gian

Khởi tạo tệp dockerfile

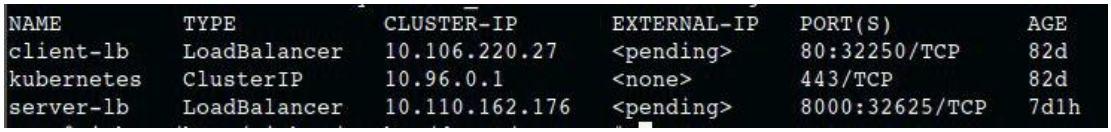
```
FROM python:3.7-alpine
#RUN echo "deb http://ftp.us.debian.org/debian/ jessie main non-free contrib" > /etc/apt/sources.list && \
#       echo "deb http://security.debian.org/ jessie/updates main non-free contrib" >> /etc/apt/sources.list
#
#RUN apt-get update && \
#    apt-get clean && \
#    rm -rf /var/lib/apt/lists/*
# Cài code API
RUN mkdir /code
RUN mkdir /code/api
COPY api/ /code/api/
```

```
COPY api/requirements.txt /code/api/
WORKDIR /code/api
#RUN mkdir /code
#RUN mkdir /code/api
#COPY api/ /code/api/
RUN pip install --trusted-host pypi.python.org -r requirements.txt
#RUN apt-get update && apt-get install net-tools && apt-get install -y iputils-ping
RUN pip install -r requirements.txt
CMD ["python", "run.py"]
```

Khởi tạo tệp docker-compoe.yml để build thành image:

```
version: '3'
services:
  api:
    container_name: api_flask
    build:
      context: ../
      dockerfile: docker/Dockerfile
    ports:
      - "0.0.0.0:8000:8000"
    environment:
      FLASK_ENV: development
    restart: unless-stopped
```

Sau khi đóng thành ảnh, khởi tạo tệp cấu hình để đẩy lên máy chủ. Chạy lệnh *kubectl create –f* để tạo service. Kết quả thu được như hình dưới đây:



NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
client-lb	LoadBalancer	10.106.220.27	<pending>	80:32250/TCP	82d
kubernetes	ClusterIP	10.96.0.1	<none>	443/TCP	82d
server-lb	LoadBalancer	10.110.162.176	<pending>	8000:32625/TCP	7d1h

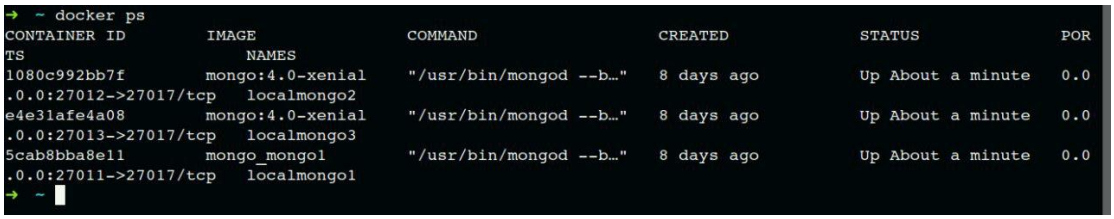
Hình 3. 7 Kết quả tạo service lớp trung gian

Triển khai cơ sở dữ liệu

Như đã đề xuất, cơ sở dữ liệu sẽ sử dụng mongodb và dùng mongo replication để đảm bảo tính khả dụng của CSDL. Mô hình thử nghiệm sẽ tạo 3 cơ sở dữ liệu trên 3 docker, 1 CSDL làm master (CSDL chủ) còn 2 CSDL còn lại sẽ làm slave (cơ sở dữ liệu thứ cấp/lệ thuộc). Khi master mất thì lập tức một trong 2 docker còn lại sẽ

chuyển thành master thay thế. Kỳ thi thực tế có thể triển khai nhiều hơn 3 docker tùy vào số lượng thí sinh tham dự đồng thời.

Sau khi triển khai, kết quả thu được như hình sau:



Hình 3. 8 Kết quả replication mongodb

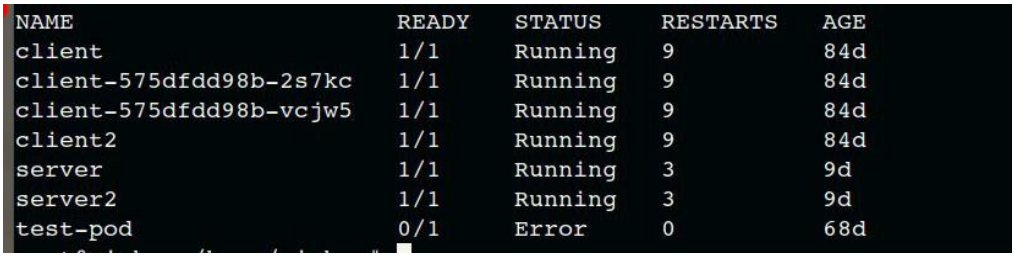
3.2.3. Ứng dụng web

Tương tự với lớp trung gian, ứng dụng web cũng được tổ chức thành các docker (chi tiết quá trình tạo docker và triển khai tương tự như lớp trung gian). Bên cạnh đó cần cấu hình thêm máy chủ web (web server) (đề xuất sử dụng ngnix, ứng dụng web server được đánh giá có nhiều ưu điểm để triển khai trên nền linux, khả năng co giãn dễ dàng. Nội dung tệp cấu hình nginx.conf:

```
server {
   listen 8080;
   root /code;
   index index.html;
   location / {
      include  /etc/nginx/mime.types;
      try_files $uri $uri/ @rewrites;
   }
   location @rewrites {
      include  /etc/nginx/mime.types;
      rewrite ^(.+)$ /index.html last;
   }
   location ~ \.css {
```

```
        include  /etc/nginx/mime.types;
        add_header Content-Type text/css;
    }
    location ~ \.js {
        include  /etc/nginx/mime.types;
        add_header  Content-Type    application/x-javascript;
    }
    location ~* \.(jpg|jpeg|png|gif|ico|css|js)$ {
        include  /etc/nginx/mime.types;
        expires 1M;
    }
}
```

Kết quả sau khi triển khai như sau:



NAME	READY	STATUS	RESTARTS	AGE
client	1/1	Running	9	84d
client-575dfdd98b-2s7kc	1/1	Running	9	84d
client-575dfdd98b-vcjw5	1/1	Running	9	84d
client2	1/1	Running	9	84d
server	1/1	Running	3	9d
server2	1/1	Running	3	9d
test-pod	0/1	Error	0	68d

Hình 3. 9 Các pods của ứng dụng web sau khi tạo

Giải thích các tham số trong hình trên:

- NAME: Tên của pod
- READY: Trạng thái sẵn sàng
- STATUS: Trạng thái hiện tại (Running là đang chạy, Error là có lỗi)
- RESTARTS: Số lần khởi động lại
- AGE: Ngày được tạo

Các dịch vụ (services) sau khi tạo:

```
NAME          TYPE           CLUSTER-IP       EXTERNAL-IP   PORT(S)          AGE
client-lb     LoadBalancer   10.106.220.27    <pending>     80:32250/TCP     84d
kubernetes    ClusterIP      10.96.0.1        <none>        443/TCP          84d
server-lb     LoadBalancer   10.110.162.176   <pending>     8000:32625/TCP   9d
```

Hình 3. 10 Service sau khi tạo bằng kubernetes

Giải thích các tham số:

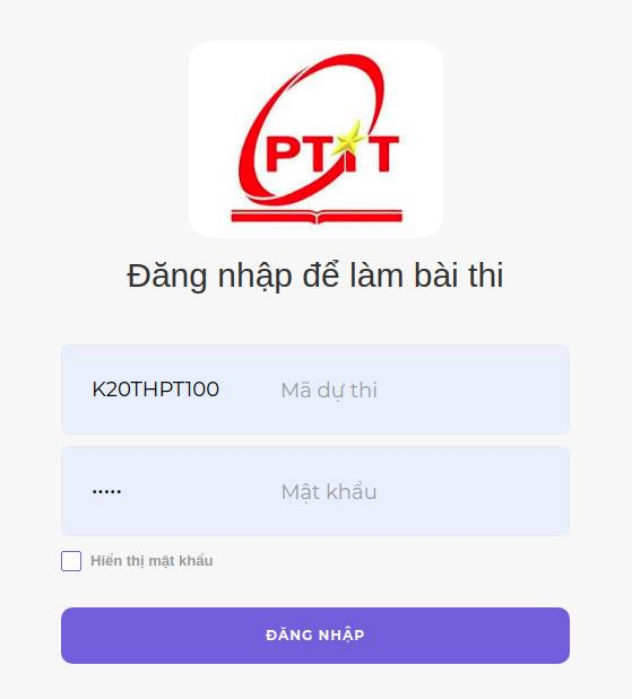
- NAME: Tên dịch vụ
- TYPE: Loại dịch vụ (ở đây là loadbalancer)
- CLUSTER_IP: địa chỉ của cụm
- EXTERNAL-IP: địa chỉ mạng ngoài
- PORT: cổng mạng ngoài
- AGE: ngày được tạo

3.3. Phân tích và đánh giá kết quả

3.3.1. Kết quả thực nghiệm

Hệ thống được chạy thử nghiệm với kỳ thi trắc nghiệm môn tiếng Anh cho kết quả như sau:

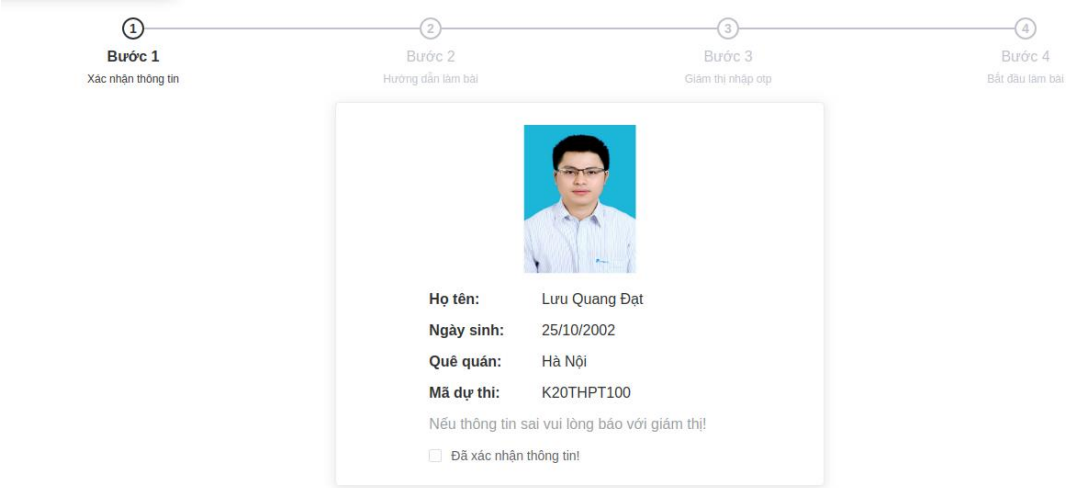
Bước 1: Thí sinh đăng nhập hệ thống và xác thực thông tin



Hình 3.11 Giao diện chức năng đăng nhập

Bước 2: Sau khi đăng nhập thành công, hệ thống yêu cầu thí sinh xác nhận thông tin và hướng dẫn làm bài. Giám thị thực hiện xác thực thí sinh dự thi

- Xác nhận lại thông tin thí sinh nếu có sai sót báo lại cho giám thị

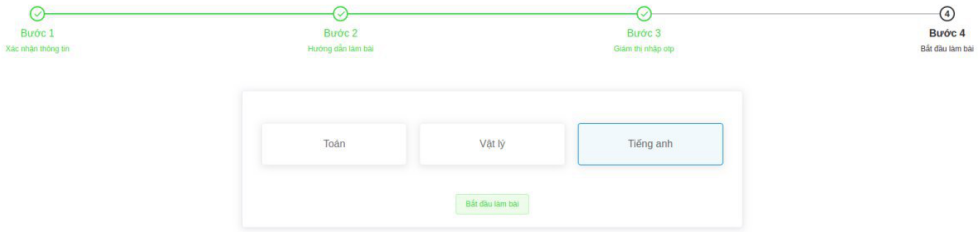


Hình 3.12 Giao diện chức năng xác thực thông tin

- Đọc quy định và hướng dẫn làm bài thi

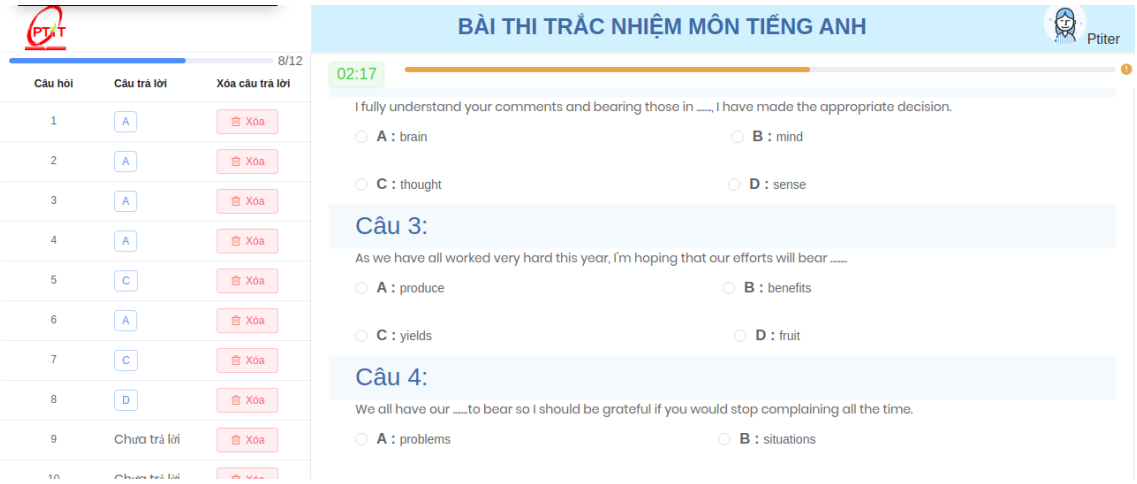
Hình 3.13 Giao diện hướng dẫn làm bài thi

Bước 3: Chọn môn thi và bắt đầu làm bài (trong trường hợp được lựa chọn)



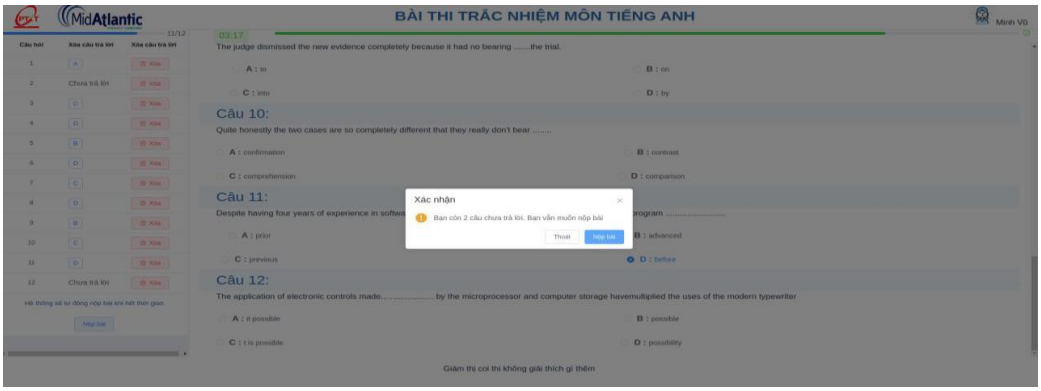
Hình 3.14 Giao diện chọn môn thi

Bước 4: Bắt đầu làm bài



Hình 3.15 Giao diện làm bài thi

Bước 5: Nộp bài (trường hợp hết thời gian quy định mà thí sinh chưa nộp bài, hệ thống sẽ tự động nộp)



Hình 3.16 Giao diện nộp bài thi

3.3.2. Đánh giá

Kết quả đạt được:

Hệ thống thử nghiệm đã giải quyết được một số vấn đề đặt ra như:

- Đối với đề thi: Đề thi được khởi tạo và lưu trữ trong CSDL, chỉ những người dùng có quyền mới được truy cập vào hệ thống. Mọi thao tác truy vấn, cập nhật đều được ghi nhật ký. Chính vì vậy hạn chế được việc lộ lọt thông tin đề thi

- Đối với dữ liệu thí sinh: Dữ liệu thí sinh được lưu trữ trong cơ sở dữ liệu. Khi thí sinh tham dự hệ thống yêu cầu phải thực hiện xác thực. Điều này sẽ hạn chế tình trạng thi hộ.

- Đối với dữ liệu bài thi: Với phạm vi là kỳ thi trắc nghiệm, thí sinh sẽ thực hiện làm bài trên máy tính. Ngay sau khi thí sinh nhấn nộp bài, hệ thống tự động mã hóa và lưu trữ dữ liệu bài làm của thí sinh vào mạng blockchain, đảm bảo rất khó hoặc không thể bị can thiệp nhằm thay đổi nội dung. Khi hết giờ hệ thống tự động nộp bài nên thí sinh không thể gian lận về thời gian thi.

Ưu điểm

Hệ thống thử nghiệm đã thực hiện được các chức năng cơ bản của một kỳ thi trắc nghiệm. Đảm bảo quản lý được việc xác thực thông tin thí sinh, quản lý thời gian làm bài, đặc biệt là việc lưu trữ được thông tin thí sinh và kết quả làm bài vào mạng blockchain đã thiết kế. Hệ thống đã giải quyết được một số vấn đề gian lận đặt ra.

Hệ thống cũng đã tính toán đến khả năng số lượng lớn thí sinh tham gia đồng thời. Hệ thống cũng đã áp dụng được một số công nghệ tương đối mới tại thời điểm hiện tại như vue.js, docker, kubernetes, ...

Nhược điểm

Chức năng trên hệ thống còn đơn giản nên cần nghiên cứu bổ sung thêm nhiều chức năng để đảm bảo đáp ứng được nhiều kịch bản và quy trình tổ chức thi trong thực tế.

Kết luận chương

Trong chương này luận văn đã trình bày quá trình cài đặt, triển khai ứng dụng thử nghiệm. Trên cơ sở kết quả thu được, chương này cũng đưa ra đánh giá các ưu nhược điểm của hệ thống thử nghiệm.

KẾT LUẬN

Sau khi nghiên cứu công nghệ blockchain và ứng dụng vào bài toán phòng chống gian lận trong thi cử, luận văn đã đạt được kết quả và hạn chế sau:

Kết quả:

- Trình bày về sự hình thành và phát triển của công nghệ blockchain.
- Trình bày về các khái niệm, thuật ngữ, đặc điểm kỹ thuật tính chất của blockchain.
- Trình bày các thuận toán đồng thuận trong blockchain như: bằng chứng cổ phần, bằng chứng công việc.
- Trình bày về nền tảng Hyperledger Fabric và chaincode
- Trình bày các nguy cơ gian lận có thể xảy ra trong kỳ thi.
- Trình bày được mô hình đề xuất ứng dụng blockchain để giải quyết bài toán.
- Trình bày được việc xây dựng và triển khai ứng dụng thi trắc nghiệm dựa trên nền tảng Hyperledger Fabric

Hạn chế cần khắc phục:

- Ứng dụng còn đơn giản, chưa bao quát được các nghiệp vụ của một kỳ thi
- Quy mô ứng dụng mới chỉ dừng ở việc thử nghiệm trên hình thức thi trắc nghiệm, cho một bộ môn.
- Số tổ chức, số node trong mô hình blockchain thử nghiệm còn ít

Hướng phát triển trong thời gian tới:

- Nghiên cứu các giải pháp cho phép thực hiện toàn trình từ khẩu tổ chức thi, quản lý hội đồng, quản lý phách, công bố kết quả, ...
- Nghiên cứu mở rộng giải pháp cho hình thức thi tự luận
- Mở rộng giải pháp cho việc cung cấp dịch vụ tra cứu, truy xuất thông tin kết quả thi cử.
- Mở rộng giải pháp cho việc cấp văn bằng chứng chỉ tốt nghiệp sau kỳ thi nhằm hạn chế tình trạng bằng giả, đồng thời giảm chi phí lưu trữ

TÀI LIỆU THAM KHẢO

[1] Trọng Đạt (2018). *Tiến sĩ Blockchain hiến kế xóa bỏ gian lận thi cử tại Hà Giang, Sơn La*, VietNamNet. https://vietnamnet.vn/vn/cong-nghe/tin-cong-nghe/tien-si-blockchain-hien-ke-xoa-bo-gian-lan-thi-cu-tai-ha-giang-son-la-466498.html. Truy cập ngày 26/10/2019.

[2] Hà Đức Minh (2019). *Vì sao gian lận thi cử ngày càng trầm trọng*, Báo Thanh niên online. https://thanhnien.vn/giao-duc/vi-sao-gian-lan-thi-cu-ngay-cang-tram-trong-1139597.html. Truy cập ngày 25/10/2020.

[3] Antonopoulos Andreas M, Farnham B., Tokyo S. và cộng sự (2017), *Mastering Bitcoin Mastering Bitcoin Revision History for the Second Edition.*

[4] Crosby Michael, Nachiappan, Pattanayak Pradhan và cộng sự (2016), *Blockchain Technology - BEYOND BITCOIN*, Berkley Eng.

[5] D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen (2018), "Untangling Blockchain: A Data Processing View of Blockchain Systems, " *IEEE Trans. Knowl. Data Eng* 4347: 1-20.

[6] Gupta, M. (2017), *Blockchain for Dummies,IBM Limited Edition.* John Wiley & Sons, Inc.

[7] Sharon Cocco, Gari Sing (2018). *IBM Developer - Top 6 technical advantages of Hyperledger Fabric for blockchain networks*, IBM. Truy cập tháng 12/2019. https://developer.ibm.com/.

[8] Toshendra, Kumar Sharma (2019). *Hyperledger Fabric – Top use cases,* Blockchain Council. Available: https://www.blockchain-council.org/.

[9] *Use cases of blockchain in education*. Available: https://www.blockchain-council.org/. Truy cập ngày 20/12/2019

[10] Website **https://hyperledger-fabric.readthedocs.io/en/release-2.0/key_concepts.html**. IBM. Truy cập tháng 11/2019

[11] Website https://docs.mongodb.com/manual/tutorial/ MongoDB inc. Truy cập tháng 12/2019

[12] Website https://kubernetes.io/ Linux Foundation. Tuy cập tháng 12/2019