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

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - NĂM 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: Tiến sĩ Đặng Minh Tuấn

Phản biện 1: PGS.TS. Đỗ Trung Tuấn

Phản biện 2: TS. Phùng Văn Ổn

Luận văn đã được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày 20 tháng 06 năm 2020

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông.

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 ta 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 việc 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 blockchian. Trong chương này cũng giới thiệu về nền tảng blockchain Hyperleger Fabric và mô hình ứng dụng. 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

NỘI DUNG

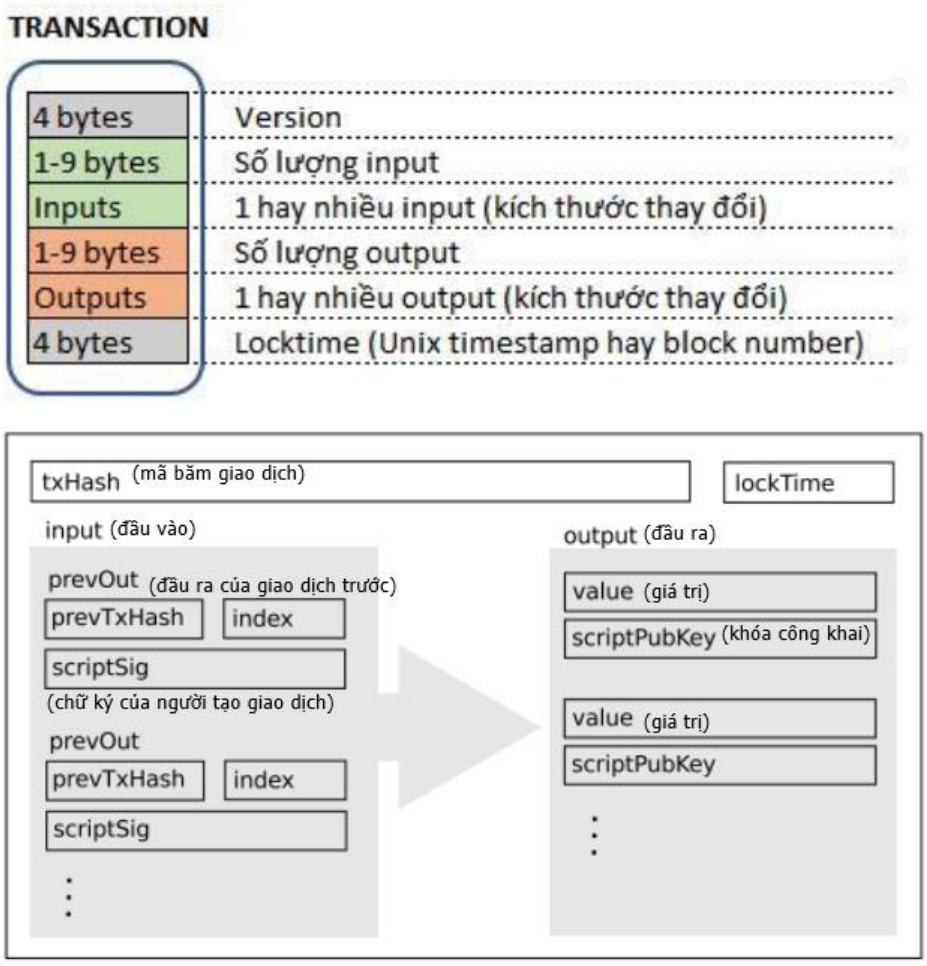
CHƯƠNG 1: TỔNG QUAN VỀ CÔNG NGHỆ BLOCKCHAIN

1.1. Giới thiệu tổng quan về công nghệ Bockchain

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. 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



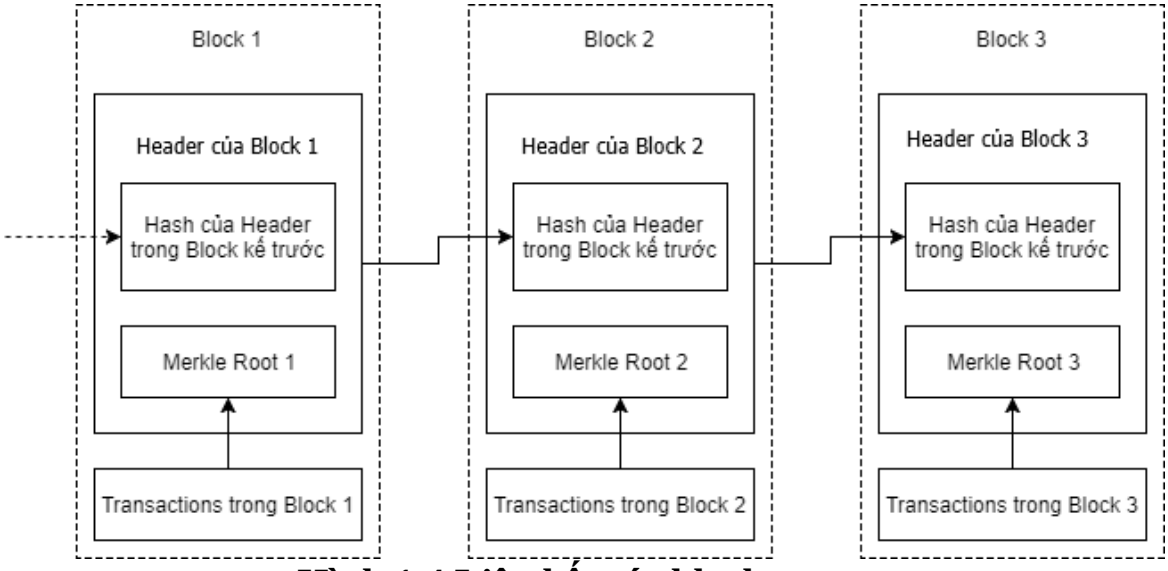
Hình 1.3 Cấu trúc giao dịch trong Blockchain

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

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 cũng tham chiếu đến một block trước đó gọi là block cha, thông qua một trường có tên "Block Hash trước" trong tiêu đề 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

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

1.2.4. Các cơ chế đồng bộ dữ liệu và xử lý đồng thuận trên blockchain

1.2.5. Sổ cái và quá trình hình thành block

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, được lưu trữ trên blockchain và được thực thi tự động như một phần của giao dịch

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 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 chung	Không	Một phần	Có
Quá trình đồng thuận	Không cần sự cho phép	Phải được cấp quyền	Phải được cấp quyền

1.4. Nền tảng Hyperledger Fabric

1.4.1. Giới thiệu về Hyperledger

Hyperledger là một dự án mã nguồn mở, nó xây dựng một hệ sinh thái các giải pháp và người dùng trên nền tảng công nghệ blockchain nhằm giải quyết các vấn đề trong ngành công nghiệp.

1.4.2. Hyperledger Fabric

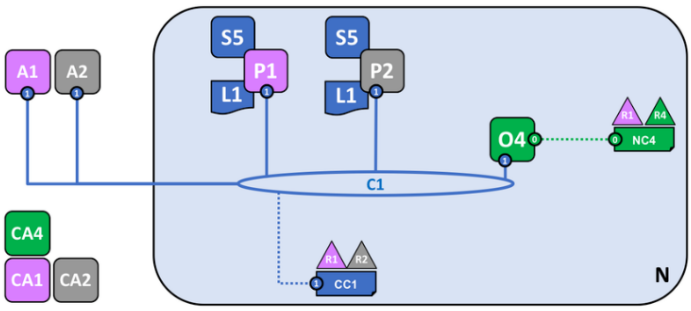
Hyperedger Fabric là một trong 5 Framework về Blockchain nằm trong chiến lược Hyperledger Umbrella của Linux Foundation.

Các khái niệm cơ bản

- ***Identity:*** Mỗi tác nhân trong HF bao gồm peers, orderer, client, admin, ... đều có 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 Blochain network bao gồm chủ yếu các peer. Peer là thành tố cơ bản của network.
- ***Ledger****:* Ở cấp độ đơn giản nhất, một blockchain bất biến ghi lại các giao dịch cập nhật kết quả thực hiện giao dịch trong một Ledger.
- ***The odering service****:* Hyperledger Fabric có một loại node được gọi là một orderer (hay còn được gọi "ordering node"), thực hiện nhiệm vụ "consensus", có thể là chỉ có 1 ordering node trong một network, hoặc có thể có nhiều node tạo nên 1 ordering service.

1.4.3. Kiến trúc của một mạng Hyperleger Fabric

Phần này sẽ phác thảo các tính năng thiết kế chính trong Hyperledger Fabric



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

N: (Netword) Mạng

NC: Network Configuration (Cấu hình của mạng)

C: Channel (Kênh)

CC: Channel Configuration (Cấu hình của kênh)

R: Organization (Tổ chức)

O: Orderer Node

P: Peer

S: Smart Contract (Chaincode)

L: Ledger (Sổ cái)

CA: Certificate Authority

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

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
- Mức độ tin cậy, khả năng mở rộng, hiệu suất
- Dữ liệu trên cơ sở cần biết (Data on need-to-know basis)
- Truy vấn phong phú trên một sổ cái phân tán bất biến
- Kiến trúc mô-đun hỗ trợ các thành phần plug-in
- Bảo vệ khóa kỹ thuật số và dữ liệu nhạy cảm

1.4.5. 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. Phần này cũng sẽ trình bày các ứng dụng của blockchain trong giáo dục, tình hình ứng dụng blockchain trong giáo dục trên thế giới và tiềm năng ứng dụng tại Việt Nam.

Kết luận chương

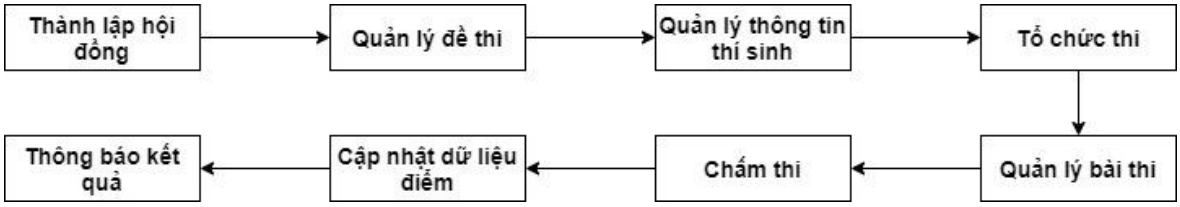
Trong chương 1, luận văn đã trình bày các kiến thức cơ bản nhất về hệ thống Blockchain và nền tảng Hyperleder Fabric. Các kiến thức được đề cập đến bao gồm: cấu trúc giao dịch, cấu trúc block, cấu trúc mạng, cơ chế đồng bộ dữ liệu và xử lý đồng thuận, kiến trúc của một mạng Hyperledger. Đồng thời trong 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 HYPERLEDGER FABRIC TRONG BÀI TOÁN PHÒNG CHỐNG GIAN LẬN THI CỬ

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

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

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

- 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 những gian lận có thể xảy ra trong kỳ thi, luận văn đề xuất giải pháp để giải quyết 1 số vấn đề 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 bỏa 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 với hình thức 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

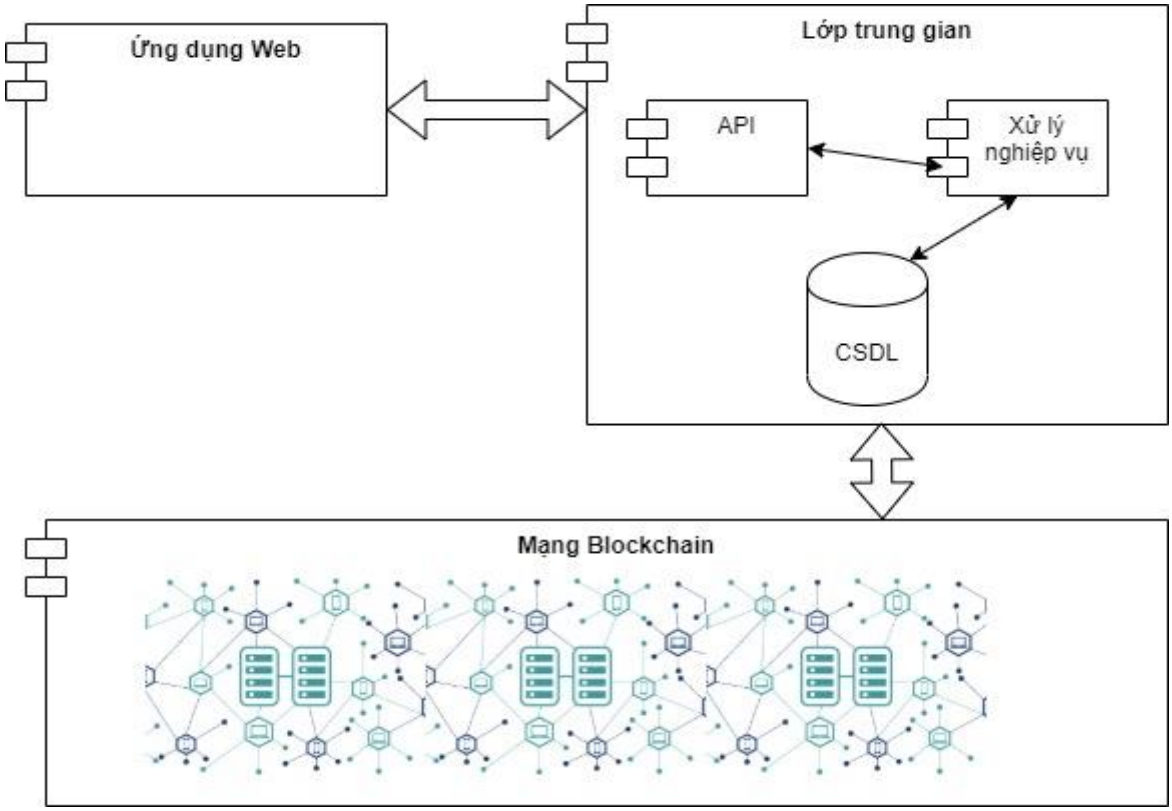
trên mạng blockchain. Khi thí sinh muốn biết điểm thì có thể tra cứu trên hệ thống, điểm sẽ được bảo đảm về tính toàn vẹn và minh bạch.

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 tập trung giải quyết cho hình thức thi trắc nghiệm, đối với hình thức thi tự luận thì cần xem xét và phát triển thêm.

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

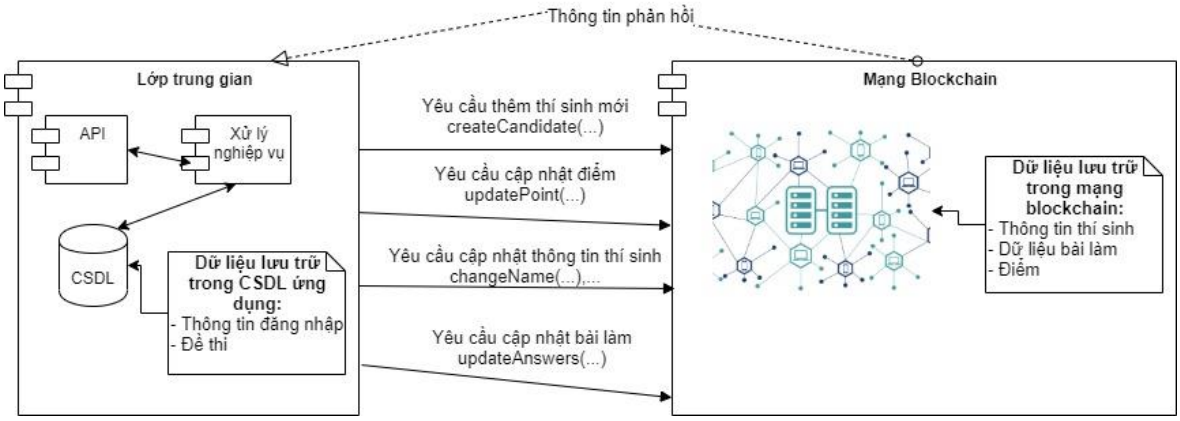
Lớp này cũng sẽ bao gồm CSDL lưu trữ thông tin người dùng (thí sinh, cán bộ) phục vụ đăng nhập hệ thống (chỉ lưu thông tin username, mật khẩu và một số thông tin khác phục vụ quản lý người dùng cho ứng dụng web), dữ liệu đề thi

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.

2.2.2. 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. 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



Hình 2.6 Luồng dữ liệu trao đổi giữa ứng dụng và mạng blockchain

Xây dựng các phương thức hoạt động trên chaincode

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.

2.2.4. Lớp trung gian

Đây là module có chức năng đảm bảo các nghiệp vụ chính của toàn bộ ứng dụng. Lớp này 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

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

2.4.1. Docker

2.4.2. Kubernetes

2.4.3. MongoDB

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

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, …

Thiết kết cơ sở dữ liệu

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

Xây dựng API Backend

Các API được xây dựng để cung cấp cho ứng dụng web

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.

3.2. Cài đặt và triển khai thử nghiệm

3.2.1. Mạng Blockchain

Các bước thực hiện như sau:

- Cài đặt Hyperledger Fabric
- Thiết lập network
- Cài đặt chaincode lên các node trong channel
- Khởi tạo ledger

3.2.2. Lớp trung gian

Backend được xây dựng dựa trên các bước cơ bản như sau:

- Viết dockerfile
- Viết file docker-compoe.yml để build thành image:
- Sau khi build thành image thì sẽ viết file config cho kubernetes để đẩy lên sever
- Sau khi tạo xong file thì có thể chạy lệnh *kubectl create* để chạy hai pod trên
- Cuối cùng là tạo file service để quy định xem service sẽ kết nốt tới pod nào

3.2.3. Ứng dụng web

Tạo service tương tự như lớp trung gian. Bên cạnh đó cần cấu hình thêm 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.

3.3. Phân tích và đánh giá kết quả

3.3.1. Kết quả thực nghiệm

Hệ thống được test thử nghiệm trên kỳ thi trắc nghiệm môn Tiếng Anh với kết quả như sau:

Bước 1: Thí sinh đăng nhập hệ thống

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

Bước 3: Sau khi xác thực thành công. Thí sinh lựa chọn môn thi và bắt đầu làm bài

Bước 4: Bắt đầu làm bài

Bước 5: Nộp bài, nếu hết thời gian hệ thống sẽ tự động nộp bài

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 log. 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 đã nêu. 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