**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**BÁO CÁO TỔNG KẾT**

**ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN**

**NĂM 2022**

**Nghiên cứu công nghệ blockchain phát triển ứng dụng quản lý văn bằng, chứng chỉ**

**Sinh viên thực hiện**

**Phạm Anh Quân Lớp: CNTT VA Khoa: QT**

Bùi Huy Tú Lớp: CNTT VA Khoa: QT

Dương Tuấn KhangLớp: CNTT VA Khoa: QT

Trần Trung KiênLớp: CNTT VA Khoa: QT

Kiều Hồng QuànLớp: CNTT VA Khoa: QT

**Người hướng dẫn:** TS. Hoàng Văn Thông

**Hà Nội, 2021**

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**BÁO CÁO TỔNG KẾT**

**ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN**

**NĂM 2022**

**Nghiên cứu công nghệ blockchain phát triển ứng dụng quản lý văn bằng, chứng chỉ**

**Sinh viên thực hiện**

**Phạm Anh Quân Giới Tính: Nam Dân tộc: Kinh**

**Lớp:CNTTVA Khoa: Quốc Tế Năm thứ:2/4**

Bùi Huy Tú Giới Tính: Nam Dân tộc: Kinh

Lớp:CNTTVA Khoa Quốc Tế Năm thứ:2/4

Dương Tuấn Khang Giới Tính: Nam Dân tộc: Kinh

Lớp:CNTTVA Khoa Quốc Tế Năm thứ:2/4

Kiều Hồng Quang Giới Tính: Nam Dân tộc: Kinh

Lớp:CNTTVA Khoa Quốc Tế Năm thứ:2/4

Trần Trung Kiên Giới Tính: Nam Dân tộc: Kinh

Lớp:CNTTVA Khoa: Quốc Tế Năm thứ:2/4

**Người hướng dẫn:** TS. Hoàng Văn Thông

**Hà Nội, 2021**

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**THÔNG TIN KẾT QUẢ NGHIÊN CỨU CỦA ĐỀ TÀI**

**1. Thông tin chung:**

**-** Tên đề tài: Nghiên cứu công nghệ blockchain phát triển ứng dụng quản lý văn bằng, chứng chỉ

- Sinh viên thực hiện:

1. Phạm Anh Quân

2. Bùi Huy Tú

3. Dương Tuấn Khang

4. Trần Trung Kiên

5. Kiều Hồng Quang.

- Lớp: CNTTVA Khoa: Đào tạo quốc Tế Năm thứ: 2 Số năm đào tạo: 4

- Người hướng dẫn: TS. Hoàng Văn Thông

**2. Mục tiêu đề tài:**

Nghiên cứu về công nghệ Blockchain, Xây dựng website quản lý văn bằng đại học dựa trên 1 số nguyên lý của blockchain

**3. Tính mới và sáng tạo:**

Phát triển một website hoàn toàn mới để quản lý, tra cứu văn bằng được cấp bởi các trường đại học với các công nghệ tổ chức dữ liệu dựa trên nguyên lý chuỗi khối, hàm băm.

**4. Kết quả nghiên cứu:**

Nhóm đã xây dựng được website quản lý văn bằng được cấp bởi các trường đại học ứng dụng 1 số nguyên lý của blockchain.

**5. Đóng góp về mặt kinh tế - xã hội,** **giáo dục và đào tạo, an ninh, quốc phòng và khả năng áp dụng của đề tài:**

Kết quả của đề tài nếu được áp dụng sẽ làm giảm tệ nạn sử dụng bằng đại học giả của người xin việc, hỗ trợ các cơ quan, doanh nghiệp tra dễ dàng kiểm tra bằng cấp của nhân viên mà không phải nhờ các trường đại học xác minh. Các giảm công việc xác mình bằng cấp cho các cơ quan, doanh nghiệp của các nhân viên quản lý bằng của các trường đại học.

**6.** **Công bố khoa học của sinh viên từ kết quả nghiên cứu của đề tài** *(ghi rõ họ tên tác giả, nhan đề và các yếu tố về xuất bản nếu có)* hoặc nhận xét, đánh giá của cơ sở đã áp dụng các kết quả nghiên cứu *(nếu có)*:

Ngày 10 tháng 06 năm 2022

|  |  |
| --- | --- |
|  | **Sinh viên chịu trách nhiệm chính**  **thực hiện đề tài**  *(ký, họ và tên)*  Phạm Anh Quân |

**Nhận xét của người hướng dẫn về những đóng góp khoa học của sinh viên thực hiện đề tài** *(phần này do người hướng dẫn ghi):* *Sinh viên đã hiểu được nguyên lý hoạt động của công nghệ blockchain, áp dung nguyên lý này vào tổ chức dữ liệu lưu trữ bằng cấp giảm thiểu rủi ro sửa đổi trên hệ thống. Với đóng góp mới này sẽ giúp làm giảm bớt tệ nạn sử dụng bằng giả hiện nay.*

Ngày 13 tháng 06 năm 2022

|  |  |
| --- | --- |
|  | **Người hướng dẫn**  *(ký, họ và tên)* |

Mục lục

[LỜI MỞ ĐẦU 7](#_Toc105797440)

[1. Tổng quan tình hình nghiên cứu thuộc lĩnh vực đề tài 7](#_Toc105797441)

[2. Lý do lựa chọn đề tài 8](#_Toc105797442)

[3. Mục tiêu, nội dung, phương pháp nghiên cứu của đề tài 8](#_Toc105797443)

[4. Đối tượng và phạm vi nghiên cứu 8](#_Toc105797444)

[CHƯƠNG I: GIỚI THIỆU BLOCKCHAIN 9](#_Toc105797445)

[1. Vì sao ra đời Blockchain 9](#_Toc105797446)

[Hạn chế trong giao dịch thời xưa: 9](#_Toc105797447)

[2. Lịch sử ra đời blockchain 9](#_Toc105797448)

[3. Blockchain (chuỗi khối) 10](#_Toc105797453)

[3.1. Blockchain là gì? 10](#_Toc105797454)

[3.2. KHỐI VÀ DỮ LIỆU KHỐI 11](#_Toc105797455)

[3.3. HÀM BĂM (HASH FUNCTION) 12](#_Toc105797456)

[3.5. Phi tập trung 13](#_Toc105797458)

[3.6. Phân tán 13](#_Toc105797459)

[3.7. Mạng ngang hàng (p2p) 14](#_Toc105797460)

[3.8. Validator 14](#_Toc105797461)

[3.9. Miner 14](#_Toc105797462)

[3.10. Nút (node) 14](#_Toc105797463)

[3.11. Blockchain giải quyết vấn đề gì? 15](#_Toc105797464)

[4.1. Cơ chế đồng thuận (blockchain consencus) là gì? 15](#_Toc105797465)

[4.2. Bằng chứng công việc – Proof of Work (PoW) 16](#_Toc105797466)

[4.3. Bằng chứng cổ phần – Proof of Stake (PoS) 17](#_Toc105797467)

[5. Ứng dụng của blockchain 18](#_Toc105797468)

[6. Ứng dụng Blockchain vào bài toán quản lý văn bằng 18](#_Toc105797469)

[1. Khảo sát bài toán 19](#_Toc105797470)

[2. Thiết kế hệ thống 20](#_Toc105797471)

[2.1. Thiêt kế chức năng 20](#_Toc105797472)

[2.2. Thiết kế cơ sở dữ liệu 20](#_Toc105797473)

[3. Thiết kế website 21](#_Toc105797474)

[3.1. Giao diện đăng nhập 21](#_Toc105797475)

[3.2. Giao diện quản trị người dùng 23](#_Toc105797476)

[3.3. Giao diện cập nhật văn bằng chứng chỉ 24](#_Toc105797477)

[3.4. Giao diện tra cứu 25](#_Toc105797478)

[3.5. Đăng kí thông tin trường 26](#_Toc105797479)

[KẾT LUẬN 27](#_Toc105797480)

[TÀI LIỆU THAM KHẢO 28](#_Toc105797481)

# LỜI MỞ ĐẦU

## 1. Tổng quan tình hình nghiên cứu thuộc lĩnh vực đề tài

Có thể khẳng định rằng, với việc sử dụng bằng giả, bằng không hợp lệ đã gây ảnh hưởng lớn đến uy tín của các cơ quan, tổ chức Nhà nước; gây bất công bằng trong cán bộ, công chức, viên chức và ảnh hưởng lớn đến chất lượng của công việc.

Tình trạng sử dụng bằng giả ngày càng lan rộng, gây nguy hiểm cho xã hội. Đặc biệt, nguy hại hơn khi vấn nạn này tồn tại trong ngành giáo dục, khi để cho các giáo viên “dỏm” đứng lớp sẽ để lại những hậu quả nặng nề. Trước hết, học sinh sẽ không được trang bị những kiến thức đầy đủ, do hầu hết các trường hợp giáo viên này mua bằng sẽ không có kiến thức cũng như nghiệp vụ sư phạm nếu tham gia giảng dạy.

Ngoài ra, còn ảnh hưởng nhiều đến hình thành nhân cách, đạo đức của người học. Ông Nguyễn Văn Biên, Trưởng phòng Nội vụ huyện Sơn Tây (Quảng Ngãi) cho rằng, những trường hợp sử dụng bằng giả để vào trong ngành giáo dục sẽ khiến chất lượng giáo dục không hiệu quả, ảnh hưởng nghiêm trọng đến chất lượng giáo dục…

Hiện nay Bộ giáo dục và đào tạo vẫn chưa có một phần mềm thống nhất hỗ trợ việc quản lý văng bằng và cho phép người dùng có thể tra cứu một văn bằng đó là thật hay giả.

## 2. Lý do lựa chọn đề tài

Với sự phát triển của internet nói chung và công nghệ blockchain nói riêng. Cuộc sống con người đã và đang ngày càng trở nên tiện ích hơn. Qua sự phát triển vượt bậc ấy, nhóm em đã cùng thảo luận và nhận thấy vấn đề về việc tra cứu văn bằng dùng phương pháp thủ công khá mất thời gian, việc lưu trữ thủ công cũng tốn nhiều không gian, hơn thế nữa văn bằng bằng giấy dễ làm giả nên nhà trường còn phải mất thời gian xác thực văn bằng. Do đó nhóm chúng em đã cố gắng tìm tòi và nghiên cứu dựa trên cách hoạt động của công nghệ blockchain, đưa ra giải pháp về tính minh bạch thông tin văn bằng chứng chỉ giúp cho sinh viên và các nhà tuyển dụng tra cứu nhanh thông tin về văn bằng đã được cấp mà các trường đại học không tốn nhiều công sức vào những vấn đề xác minh bằng cấp cho các cơ quan, doanh nghiệp.

## 3. Mục tiêu, nội dung, phương pháp nghiên cứu của đề tài

**Mục tiêu của đề tài**: Dựa theo bối cảnh trên, căn cứ nhu cầu thực tế, đề tài nghiên cứu và phát triển một website nhằm lưu trữ và tra cứu văn bằng của các trường Đại học một cách nhanh chóng.

**Nội dung nghiên cứu:** Nghiên cứu tổng quan các khái niệm cơ bản của blockchain và xây dựng website tra cứu văn bằng

**Phương nghiên cứu:** Phương pháp luận được sử dụng trong trong nghiên cứu này là nghiên cứu lý thuyết, thiết kế hệ thống, thử nghiệm và đánh giá.

## 4. Đối tượng và phạm vi nghiên cứu

**Đối tượng nghiên cứu:**

Công tác quản lý, xác minh văn bằng, chứng chỉ của các trường

Công nghệ blockchain

Các thuật toán băm, các thuật toán đồng thuận

**Phạm vi nghiên cứu:**

Những kiến thức cơ bản về blockchain

Các công nghệ phát triển ứng dụng web

# CHƯƠNG I: GIỚI THIỆU BLOCKCHAIN

## Vì sao ra đời Blockchain

## **Hạn chế trong giao dịch thời xưa:**

Ngày xưa, khi giao dịch tiền tệ, vay tiền, trả nợ, người ta sẽ thỏa thuận với nhau (giữa A và B) và ghi lại các thông tin giao dịch đó vào 1 cuốn sổ để lưu trữ nó - gọi là sổ cái. Sau đó đưa sổ này cho 1 người trung gian C uy tín nắm giữ. Và tất nhiên người C này phải đều được A và B tin tưởng.

**Hạn chế trong giao dịch qua hệ thống ngân hang**

Tới khi xã hội phát triển, chúng ta có hệ thống ngân hàng thay thế cho người C thứ 3 trung gian kể trên. Và cuốn sổ cái làm bằng giấy được thay thế bằng hệ thống máy tính của ngân hàng.

**Nguy cơ dữ liệu bị đe dọa:** Do máy chủ ngân hàng chứa rất nhiều thông tin quan trọng nên luôn là mục tiêu tấn công của nhiều kẻ xấu. Dữ liệu vẫn có thể bị đánh cắp hoặc thay đổi.

## Lịch sử ra đời blockchain

## ****Blockchain 1.0****

[Bitcoin](https://hocviendaututaichinh.com.vn/bitcoin-danh-gia-crypto-tiem-nang/) được coi là tiên phong trong hệ thống trao đổi tài sản số (tiền số, tiền ảo) qua internet. Theo thời gian hệ thống mạng lưới bitcoin vẫn làm tốt công việc của mình tuy nhiên cộng đồng cần có thêm điều khác biệt. Bitcoin là đại diện cho blockchain thế hệ đầu.

## ****Blockchain 2.0****

## Để tiếp tục cuộc hành trình [Ethereum](https://hocviendaututaichinh.com.vn/ether-danh-gia-crypto-tiem-nang/) ra đời và tạo ra sự khác biệt hơn so với Bitcoin đó là vẫn giữ đầy đủ tính chất của hệ thống trao đổi tài sản số nhưng thêm 1 tính năng mới đó là tự phân sử online.

Với tư tưởng cho phép trao đổi tiền ảo và loại bỏ vai trò của nhân viên thống kê, kế toán và bảo mật mà bitcoin là đại diện cho blockchain thế hệ thứ nhất ra đời.

## ****Blockchain 3.0****

Như vậy hệ thống mang lưới blockchain thứ 2 mang đến cho cộng đồng ngoài khả năng trao đổi tiền số online thì còn cung cấp nền tảng cho người dùng tự định nghĩa các trường hợp phán sử/phán xét và quyết định khi có các yếu tố sảy ra (Smart-contract).

Blockchain thế hệ thứ 3 kế thừa khái niệm của 2 thế hệ trước và đưa thêm một khả năng mới đó là ứng dụng phân tán (Dapp viết tắt của **decentralized application**).

## 3. Blockchain (chuỗi khối)

### **3.1. Blockchain là gì?**

Blockchain là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối (block) được liên kết với nhau bằng mã hóa và mở rộng theo thời gian để tạo thành một chuỗi (chain). Mỗi khối trong Blockchain sẽ được liên kết với khối trước đó, chứa thông tin về thời gian khởi tạo khối đó kèm một mã thời gian và dữ liệu giao dịch.

* **Các tính chất của blockchain**

**Tính phi tập trung (Decentralized):**Blockchain hoạt động độc lập theo các thuật toán máy tính, hoàn toàn không bị bất kỳ một tổ chức nào nắm quyền kiểm soát. Chính vì vậy blockchain tránh được rủi ro từ bên thứ 3.

**Tính phân tán (Distributed):**Các khối chứa dữ liệu giống nhau nhưng được phân tán ở nhiều nơi khác nhau. Nên chẳng may 1 nơi bị mất hoặc hỏng thì dữ liệu vẫn còn trên Blockchain.

**Không thể thay đổi:**Một khi dữ liệu đã được ghi vào trong block của blockchain thì nó không thể bị thay đổi hoặc sửa chữa, bởi đặc tính của thuật toán đồng thuận và mã hash (mình sẽ trình bày chi tiết ở phần dưới).

**Tính bảo mật:**Chỉ có người nắm giữ [**Private Key**](https://coin98.net/private-key-passphrase-la-gi) (khóa riêng tư) mới có thể truy cập các dữ liệu bên trong Blockchain.

**Tính minh bạch:**Các giao dịch trong blockchain được lưu lại và mọi người có thể check các giao dịch này. Dựa vào đó, ta có thể kiểm tra và truy xuất lịch sử giao dịch. Thậm chí người ta có thể phân quyền để cho phép người khác truy cập một phần thông tin trên Blockchain.

**Tích hợp Smart contract (hợp đồng thông minh):**Dựa vào đó các điều khoản được ghi trong hợp đồng thông minh sẽ được thực thi khi các điều kiện trước đó được thỏa mãn, không ai có thể ngăn cản hoặc hủy nó.

### **3.2. KHỐI VÀ DỮ LIỆU KHỐI**

A group of different colored squares

Description automatically generated with low confidence

A picture containing diagram

Description automatically generated

Diagram

Description automatically generated

**Hình 1.1** Mô tả cấu trúc của Blockchain

### **3.3. HÀM BĂM (HASH FUNCTION)**

A picture containing timeline

Description automatically generated

**Hình 1.2** Sơ đồ hàm băm

### Hashing là quá trình biến một dữ liệu đầu vào có độ dài bất kỳ thành một chuỗi đầu ra đặc trưng có độ dài cố định. Hashing được thực hiện thông qua hàm băm.

**Tính chất:**

* Tất định: cùng input thì ra 1 output
* Hiệu quả: tính giá trị băm nhanh chóng
* Table

  Description automatically generatedNhạy cảm: một thay đổi nhỏ tại input cũng đem lại thay đổi cực lớn trên giá trị băm.
* Một chiều: từ giá trị băm sẽ rất khó tìm được đầu vào.

**3.4. Sổ cái (legder):**

* Sổ cái là nơi các giao dịch tài chính và tiền tệ được ghi lại và lưu trữ
* Sổ cái này được công khai cho tất cả mọi người.
* Mỗi node trong blockchain đều lưu trữ 1 bản sao sổ cái.

**Hình 1.3** Mô hình sổ cái

### **3.5. Phi tập trung**

Một hệ thống phi tập trung là hệ thống đó có các hoạt động lập kế hoạch và ra quyết định được phân phối hoặc ủy thác thay vì tập trung vào một vị trí hoặc một nhóm nào đó.

### **3.6. Phân tán**

Một hệ thống phân tán là một hệ thống bao gồm nhiều thành phần hoạt động độc lập, trao đổi và làm việc với nhau (qua mạng) để giải quyết một vấn đề cụ thể.

Một hệ thống phân tán nhưng vẫn có thể không phi tập trung.

### **3.7. Mạng ngang hàng (p2p)**

Diagram

Description automatically generated

**Hình 1.4** Sơ đồ mạng ngang hàng

Mạng ngang hàng là một mạng máy tính trong đó hoạt động của mạng chủ yếu dựa vào khả năng tính toán và băng thông của các máy tham gia.

Các máy tính trong mạng có vai trò như nhau

### **3.8. Validator**

Validator: là Node được Blockchain chọn ngẫu nhiên theo thuật toán POS, được phép xác thực và tạo block mới.

Xác thực là quá trình xác minh các giao dịch trước khi được thêm vào blockchain (thu thập dữ liệu giao dịch, xác định xem giao dịch có đáp ứng các yêu cầu giao thức và không có các thao tác độc hại hay không).

### **3.9. Miner**

Miner (thợ đào) là người đóng góp sức mạnh tính toán của mình để giải quyết các bài toán phức tạp nhằm xác nhận giao dịch và ghi lại nó trên Blockchain.

Blockchain sử dụng thuật toán đồng thuận PoW

### **3.10. Nút (node)**

Là một máy tính chạy các ứng dụng blockchain, kết nối với máy tính cùng chạy ứng dụng đó thành một mạng ngang hàng.

Mỗi nút đều lưu trữ toàn bộ dữ liệu các khối.

Khi một máy gia nhập mạng đều nhận được một bản sao lưu đẩy đủ của blockchain

### **3.11. Blockchain giải quyết vấn đề gì?**

Vấn đề tập trung hóa: blockchain sẽ loại bỏ những bên trung gian trong giao dịch, không một bên nào quản lý blockchain.

Dữ liệu bị sửa đổi: Trong blockchain thì bất cứ thay đổi nào về dữ liệu cũng đều được ghi lại và không thể thay đổi.

Minh bạch hóa: mọi giao dịch đều được công khai cho toàn bộ người tham gia blockchain.

**4. Thuật toán đồng thuận**

### PoW là gì? Tìm hiểu cơ chế hoạt động của PoW**4.1. Cơ chế đồng thuận (blockchain consencus) là gì?**

**Hình 1.5.** Cơ chế đồng thuận POS

Cơ chế đồng thuận của mỗi blockchain có nhiệm vụ đảm bảo cho trạ

ng thái hiện thời của blockchain đó đạt được sự thỏa thuận thống nhất giữa những người tham gia. Cơ chế [đồng thuận](https://academy.binance.com/vi/articles/what-is-a-blockchain-consensus-algorithm) sẽ quyết định ai là người được phép thêm các block giao dịch mới, và một trong các mục đích cơ bản của nó là để bảo đảm việc chuỗi sẽ không bị ghi đè

### **4.2. Bằng chứng công việc – Proof of Work (PoW)**

Là thuật toán đồng thuận đầu tiên xuất hiện và cho đến nay vẫn là thuật toán thống trị. Nó được giới thiệu bởi [Satoshi Nakamoto](https://academy.binance.com/en/glossary/satoshi-nakamoto) trong sách trắng [Bitcoin](https://academy.binance.com/vi/articles/what-is-bitcoin) năm 2008, nhưng bản thân công nghệ này đã được hình thành [từ lâu trước đó](https://academy.binance.com/vi/articles/history-of-blockchain).

Proof of Work tập hợp các thợ đào (hay còn gọi là node) tham gia cạnh tranh xác thực các giao dịch, sau đó đưa giao dịch và các block trong Blockchain để nhận phần thưởng tùy theo mạng lưới.

Bản chất của PoW là xác nhận bằng chứng làm việc của ai đó là hợp lệ đến toàn bộ mạng lưới blockchain, thông qua việc tiêu tốn tài nguyên trong thế giới thực (máy đào, năng lượng điện và thời gian).

Cơ chế đồng thuận cho phép thợ đào xác thực giao dịch và tạo block mới dựa vào phần cứng máy tính và năng lượng điện để chạy máy tính đó.

**Cơ chế hoạt động:**

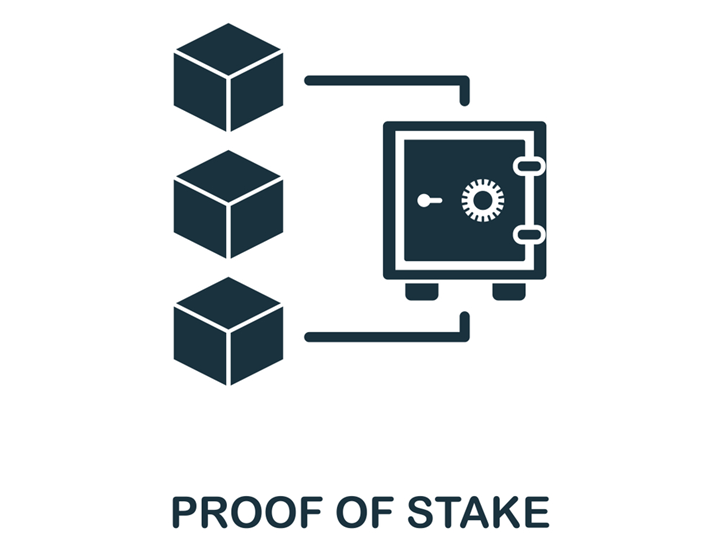
Khi thực hiện giao dịch trên Blockchain, nó sẽ được gom vào một Block cùng một số giao dịch khác. Các thợ đào sẽ sử dụng hệ thống máy đào gồm nhiều máy tính mạnh để xác minh giao dịch.

Một câu đố toán học phức tạp sẽ được hệ thống đưa ra. Nhiệm vụ của thợ đào là sử dụng sức mạnh của hệ thống đào tìm ra câu trả lời, sau khi tìm được sẽ thông báo cho các thợ đào còn lại. Khi phần lớn thành viên xác nhận đó là câu trả lời đúng, Block mới sẽ được tạo ra, giao dịch được xác nhận.

Khi hoàn thành, thợ đào sẽ nhận được phần thưởng là phí giao dịch và phần thưởng khối. Tuy nhiên, đây là quá trình sử dụng rất nhiều tài nguyên, điện, thời gian.

Nếu câu đố quá khó, sẽ mất rất nhiều thời gian để tìm ra câu trả lời, khiến Block mới không được tạo ra, hệ thống sẽ bị tắc nghẽn, giao dịch không thể thực hiện. Nhưng nếu câu đố quá dễ, hệ thống sẽ dễ bị tấn công, các giao dịch có khả năng bị làm giả. PoW giải quyết vấn đề này bằng một thuật toán điều chỉnh độ khó phù hợp với tốc độ khai thác của các thợ đào, sao cho Block mới sẽ sinh ra trong một khoảng thời gian cố định.

### **4.3. Bằng chứng cổ phần – Proof of Stake (PoS)**



**Hình 1.6.** Mô tả bằng chứng cổ phần

[Thuật toán đồng thuận](https://academy.binance.com/vi/articles/what-is-a-blockchain-consensus-algorithm) Bằng chứng cổ phần (Proof of Stake) được giới thiệu vào năm 2011 tại diễn đàn Bitcointalk để giải quyết các vấn đề của thuật toán phổ biến nhất khi đó - [Proof of Work](https://academy.binance.com/vi/articles/proof-of-work-explained). Mặc dù cả hai thuật toán có cùng mục tiêu đạt đến sự đồng thuận trong blockchain, nhưng quy trình để đạt được mục tiêu của hai thuật toán là khác nhau.

**Cơ chế hoạt động:**

PoS yêu cầu người tham gia phải đóng góp một lượng tài sản để xác nhận đồng thuận cho block. Khi xác nhận thành công, phần thưởng của block sẽ xuất hiện và được chia cho những người đã đóng góp. Mỗi người tham gia sẽ nhận theo mức họ đã đóng góp trước đó.

Bất kì ai muốn tham gia vào quá trình đặt cổ phần này đều phải sở hữu số lượng tài sản trong blockchain. Sau khi staking thành công, tài sản sẽ bị khóa để làm tài sản thế chấp của mạng lưới.

Nhưng không đơn thuần là bỏ tài sản vào và nhận coin mà còn có những quy tắc nhất định. Để nhận được lãi một cách cao nhất và chiếm được block nhanh nhất, người dùng phải cạnh tranh với các staker (người đặt cọc) khác.

Phương thức lựa chọn các node trong PoS: dựa trên các node ngẫu nhiên, dựa trên thời gian nắm giữ tài sản.

## 5. Ứng dụng của blockchain

**Tiền mã hóa** – tiền kỹ thuật số là một phương tiện trao đổi giá trị cực kỳ mạnh mẽ mà không có sự hư hỏng tại một điểm, không cần đến người gác cổng và người trung gian. Người dùng có thể gửi và nhận tiền cho những người dùng khác trên toàn cầu trong một khoảng thời gian chỉ bằng một phần nhỏ thời gian (và thường bằng một phần nhỏ chi phí) mà họ sẽ mất khi chuyển qua ngân hàng.

**Dữ liệu phân tán** – các blockchain phải đối mặt với một số vấn đề về khả năng mở rộng, nhưng chúng có thể tích hợp với các phương tiện lưu trữ phân tán để quản lý tệp. Kiểm soát truy cập có thể được quản lý thông qua hợp đồng thông minh, trong khi dữ liệu được lưu trữ trong bộ chứa ngoài chuỗi.

**Chứng khoán** – mặc dù chúng bao gồm một số rủi ro về việc các đối tác có thể không hoàn thành các nghĩa vụ của mình, các token chứng khoán dựa trên blockchain được cho là một cải tiến rất cần thiết cho lĩnh vực tài chính. Chúng bơm nguồn tiền giúp tăng tính thanh khoản và tính di động cho không gian chứng khoá ngày nay và cho phép token hóa tài sản (như bất động sản hoặc vốn chủ sở hữu).

**6. Ứng dụng Blockchain vào bài toán quản lý văn bằng**

Lí do ứng dụng công nghệ Blockchain: để minh bạch thông tin về văn bằng, tránh được vấn nạn bằng giả đang tràn lan hiện nay.

Ứng dụng blockchain vào quản lý văn bằng: Các văn bằng sau khi được gửi lên trên mạng lưới Blockchain sẽ được nhóm vào các khối và mỗi 1 văn bằng là 1 khối (block). Để được thêm vào Blockchain, mỗi khối phải chứa một đoạn mã đóng vai trò như một đáp án cho một vấn đề toán học phức tạp được tạo ra bằng**hàm mã hóa băm không thể đảo ngược**.

**CHƯƠNG 2: PHÁT TRIỂN WEBSITE QUẢN LÝ VĂN BẰNG ỨNG DỤNG BLOCKCHAIN**

1. **Khảo sát bài toán**

Hiện nay, vấn nạn buôn bán và sử dụng văn bằng, chứng chỉ giả vẫn đã và đang là những vấn đề nhức nhối đối với xã hội. Mọi cơ quan, tổ chức, cá nhân đều đang phải đối mặt với bài toán nan giải này trong quá trình tuyển dụng; và điều đáng báo động là hàng chục nghìn bằng cấp, chứng chỉ giả đã được các cơ quan chức năng triệt phá trong vài năm gần đây.

Nhằm đáp ứng mục tiêu kép là xác thực được nguồn gốc văn bằng, chứng chỉ và đảm bảo tính pháp lý của việc xác thực, nhóm nghiên cứu của lớp CNTT Việt Anh đã được sự hướng dẫn của Thầy Hoàng Văn Thông và có tham gia một số buổi hội thảo Blockchain do khoa CNTT tổ chức từ đó nghiên cứu và xây dựng website xác thực văn bằng, chứng chỉ dựa trên ứng dụng công nghệ Blockchain

Yêu cầu bài toán: Xây dựng website để lưu trữ và tra cứu văn bằng của các trường ĐH.

Các thông tin cần lưu trữ: Lưu trữ văn bằng, các tài khoản người dùng, các trường.

Thông tin văn bằng gồm có: Mã Ngành, Tên Ngành, Mã SV, Họ và tên, Ngày sinh, Nơi sinh, Giới tính, Hạng TN, Lớp, Khóa học, Mã Ngành, Tên Ngành, Số Quyết định tốt nghiệp, Số vào sổ, Số hiệu bằng, Năm.

Những đối tượng người dùng tham gia vào hệ thống: sinh viên, giảng viên, nhà tuyển dụng, cơ quan quản lý, chuyên viên quản lý văn bằng của trường đại học, nhóm người quản lý hệ thống

|  |  |
| --- | --- |
| **Người tham gia** | **Chức năng được phép thực hiện** |
| Sinh viên, Giảng viên, Nhà tuyển dụng, … | Tra cứu, xác thực văn bằng |
| Chuyên viên được giao quản lý văn bằng của Phòng đào tạo các Trường ĐH | Cập nhật thông tin văn bằng |
| Người quản trị hệ thống | Cấp 1 tài khoản cho mỗi trường ĐH để cập nhật văn bằng |

1. **Thiết kế hệ thống** 
   1. **Thiêt kế chức năng**

**Người dùng:**

Tìm kiếm, kiểm tra văn bằng xem có tồn tại trong hệ thống không

**Chuyên viên phòng được giao quản lý văn bằng của trường đại học:**

Thêm được văn bằng của trường mình mà không thể thêm của trường khác theo 2 cách đó là nhập form và Excel.

Tìm kiếm được văn bằng của trường mình quản lý mà không thể tìm được của người khác.

Đăng xuất.

**Admin:**

Tìm kiếm văn bằng.

Đăng ký tài khoản các trường cần quản lý văn bằng.

Đăng ký thông tin các trường.

Quản lý các tài khoản đang sử dụng hệ thống.

Quản lý các trường có trong hệ thống.

Đăng xuất.

### **2.2. Thiết kế cơ sở dữ liệu**

A picture containing table

Description automatically generated

**Hình 2.1** Sơ đồ quan hệ thực thể

## 3. Thiết kế website

### **3.1. Giao diện đăng nhập**

Graphical user interface

Description automatically generated with medium confidence

**Hình 3.1.** Đăng nhập chung cho chuyển viên quản lý văn bằng và admin

Graphical user interface, text

Description automatically generated

**Hình 3.2.** Đăng nhập cho chuyên viên quản lý văn bằng

Text

Description automatically generated

**Hình 3.3.** Đăng nhập thành công cho admin

### **3.2. Giao diện quản trị người dùng**

Table

Description automatically generated

**Hình 3.4.** Quản lý các trường

Table

Description automatically generated

**Hình 3.5.** Quản lý người dùng hệ thống

### **3.3. Giao diện cập nhật văn bằng chứng chỉ**

A picture containing graphical user interface

Description automatically generated

**Hình 3.6.** Phương thức cập nhật bằng cấp

A picture containing text

Description automatically generated

**Hình 3.7.** Thêm bằng excel

Graphical user interface, text, application, email

Description automatically generated

**Hình 3.8.** Thêm bằng form

### **3.4. Giao diện tra cứu**

A picture containing timeline

Description automatically generated

**Hình 3.9.** Tra cứu

### **3.5. Đăng kí thông tin trường**

Logo

Description automatically generated with low confidence

**Hình 3.10.** Thêm trường mới

# KẾT LUẬN

1. Kết quả đạt được

Tuy ứng dụng còn khá sơ sài, nhưng chức năng chính nhất của ứng dụng là giúp người dùng có thể thuận tiện trong việc tra cứu văn bằng, chuyễn viên quản lý văn bằng có thể them và tìm kiếm văn bằng của trường mình, Admin có thể đăng kí thông tin, tài khoản của các trường và có thể quản lý thông tin tài khoản của các trường.

1. **Hạn chế**

Do mới chỉ là sinh viên năm 2 nên lượng kiến thức để làm nên một ứng dụng blockchain hoàn chỉnh là chưa đủ nên nhóm em đã xây dựng rat rang web ứng dụng 1 số nguyên lý cơ bản của blockchain để quản lý văn bằng.

1. **Hướng phát triển trong tương lai**

Trong tương lai, website sẽ là 1 website chạy trên nền tảng blockchain. Giao diện sẽ được thiết kế lại cho bắt mắt và gọn hơn.  
 Phần backend trong đó cơ sở dữ liệu sẽ được mở rộng, code gọn gàng hơn

**TÀI LIỆU THAM KHẢO**

[1]. [Blockchain Là Gì? Cách Hiểu Đơn Giản Nhất Về Blockchain (viblo.asia)](https://viblo.asia/p/blockchain-la-gi-cach-hieu-don-gian-nhat-ve-blockchain-aWj53p38K6m)

[2]. <https://viblo.asia/p/nhung-khai-niem-co-ban-cua-blockchain-WAyK8MQEZxX>

[3]. [Giải thích cơ chế đồng thuận hỗn hợp PoW/PoS | Binance Academy](https://academy.binance.com/vi/articles/hybrid-pow-pos-consensus-explained)

[4]. https://www.youtube.com/watch?v=auMA7jIHYvQ&t=209s