

BLOCKCHAIN - GIẢI PHÁP TRUY XUẤT NGUỒN GỐC BẰNG CẤP

Nguyễn Mậu Hân

Khoa Công nghệ Thông tin, Trường Đại học Khoa học, Đại học Huế

Email: nmhan@hueuni.edu.vn

Ngày nhận bài: 17/3/2020; ngày hoàn thành phản biện: 23/4/2020; ngày duyệt đăng: 02/7/2020

TÓM TẮT

Blockchain là một công nghệ cho phép truyền tải dữ liệu một cách an toàn dựa vào hệ thống mã hoá vô cùng phức tạp, tương tự như cuốn sổ cái kế toán của một công ty, nơi mà mọi hoạt động liên quan đến tiền của công ty được giám sát rất chặt chẽ. Việc quản lý phôi văn bằng hiện nay để cấp cho người học rất khó kiểm soát. Nói cách khác là khó có thể phân biệt được tính thật giả của văn bằng, ảnh hưởng không ít đến vấn đề tổ chức và trật tự trong xã hội. Bài báo này đề xuất mô hình quản lý thông tin trên các văn bằng bằng công nghệ blockchain nhằm lưu trữ, quản lý, tra cứu và xác thực thông tin thật giả về văn bằng đã cấp phát.

Từ khóa: blockchain, văn bằng, xác thực thông tin.

1. MỞ ĐẦU

Công nghệ blockchain không phải là một phát minh mới lạ mà là sự kết hợp giữa 3 loại công nghệ đã tồn tại qua nhiều năm: lý thuyết mật mã [2], mạng ngang hàng và lý thuyết trò chơi [6]. Blockchain được sử dụng trong việc lưu trữ thông tin trong các khối thông tin được liên kết với nhau và được quản lý bởi tất cả mọi người tham gia hệ thống. Blockchain được tạo ra để chống lại sự thay đổi dữ liệu trong hệ thống, không thể làm giả, không thể phá hủy sự liên kết giữa các khối thông tin. Thông tin khi được nhập vào trong chuỗi khối blockchain thì sẽ không thể thay đổi bởi một cá nhân nào đó và chỉ được bổ sung thêm thông tin khi có sự chấp thuận của tất cả mọi người trong hệ thống [7]. Các loại công nghệ được sử dụng trong blockchain là:

Mật mã học: Sử dụng public key trong chữ ký số và giá trị băm của hash function để đảm bảo tính minh bạch, toàn vẹn và riêng tư.

Mạng ngang hàng: Một hệ thống mạng mà mỗi một nút trong mạng có vai trò như nhau, tự quản lý tài nguyên của mình. Một nút được xem như một client và cũng là server để lưu trữ bản sao dữ liệu.

Lý thuyết trò chơi: Tất cả các nút tham gia vào hệ thống đều phải tuân thủ luật chơi đồng thuận (PoW, PoS) và được thúc đẩy bởi động lực xác định trước [7].

Công nghệ blockchain đóng vai trò giống như một cuốn sổ cái ghi lại tất cả các giao dịch xảy ra trong hệ thống và có các đặc điểm chính có thể kể đến như:

Không thể làm giả: Các chuỗi blockchain gần như không thể bị phá hủy [5]. Theo lý thuyết thì chỉ có máy tính lượng tử mới có thể can thiệp vào và giải mã chuỗi blockchain và nó chỉ bị phá hủy hoàn toàn khi không còn Internet trên toàn cầu.

Tính bất biến: Dữ liệu trong blockchain gần như không thể sửa đổi được (chỉ có thể sửa đổi được bởi chính người đã tạo ra nó, nhưng phải được sự đồng thuận của các nút trên mạng) và các dữ liệu đó sẽ lưu giữ mãi mãi [7].

Bảo mật dữ liệu: Các thông tin, dữ liệu trong các blockchain được phân tán và độ an toàn cao, chỉ có người nắm giữ private key mới có quyền truy xuất dữ liệu đó [1].

Tính minh bạch: Có thể theo dõi được đường đi của dữ liệu trong blockchain từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.

Hợp đồng thông minh: Blockchain không cần bên thứ ba tham gia vào hệ thống, và nó bảo đảm rằng tất cả các bên tham gia đều biết được chi tiết hợp đồng và các điều khoản sẽ được tự động thực hiện một khi các điều kiện được bảo đảm [6].

2. PHƯƠNG PHÁP NGHIÊN CỨU

Trên cơ sở các khối kiến thức đã có như lý thuyết mật mã, mạng ngang hàng và lý thuyết trò chơi, phương pháp nghiên cứu được sử dụng trong bài báo là tìm hiểu nguyên tắc hoạt động, đặc điểm và kiến trúc của blockchain để xây dựng một hệ thống lưu trữ, quản lý, tra cứu và xác thực thông tin văn bằng nhằm đảm bảo nhanh, kịp thời, an toàn, chuẩn xác và minh bạch.

Để có thể dễ dàng tiếp cận và sử dụng hệ thống chúng tôi sẽ tạo ra một hệ thống lưu trữ thông tin tốt nghiệp dựa trên nền tảng công nghệ blockchain. Sau đó, xây dựng trang web cho phép người dùng tra cứu thông tin tốt nghiệp đã được lưu trong hệ thống.

3. CÁC CÔNG NGHỆ SỬ DỤNG TRONG BLOCKCHAIN

2.1. Hàm băm (hash function)

Hàm băm dùng để chuyển đổi từ một thông tin sang một đoạn mã [2]. Bất kỳ nỗ lực gian lận nào để thay đổi bất kỳ phần nào của Blockchain sẽ bị phát hiện ngay lập tức vì giá trị băm mới sẽ không phù hợp với thông tin cũ trên blockchain. Hàm

băm là hàm một chiều (one-way hash), theo nghĩa giá trị của hàm băm là duy nhất, và từ giá trị băm này, “khó” có thể suy ngược lại được nội dung hay độ dài ban đầu của thông điệp gốc.

2.2. Chữ ký số (digital signature)

Về mặt công nghệ, chữ ký số là một thông điệp dữ liệu đã được mã hóa gắn kèm theo một thông điệp dữ liệu khác nhằm xác thực người gửi thông điệp đó. Quá trình ký và xác nhận chữ ký như sau: Người gửi muốn gửi thông điệp cho bên khác thì sẽ dùng một hàm băm, băm thông điệp gốc thành một “thông điệp tóm tắt” (Message Digest). Người gửi mã hoá bản tóm tắt thông điệp bằng khóa bí mật của mình (sử dụng phần mềm bí mật được cơ quan chứng thực cấp) để tạo thành một chữ ký số. Sau đó, người gửi tiếp tục gắn kèm chữ ký số này với thông điệp dữ liệu ban đầu và gửi thông điệp đã gắn kèm với chữ ký một cách an toàn qua mạng cho người nhận. Sau khi nhận được, người nhận sẽ dùng khoá công khai của người gửi để giải mã chữ ký số thành bản tóm tắt thông điệp. Người nhận cũng dùng hàm băm giống hệt như người gửi đã làm đối với thông điệp nhận được để biến đổi thông điệp nhận được thành một bản tóm tắt thông điệp. Người nhận so sánh hai bản tóm tắt thông điệp này, nếu chúng giống nhau tức là chữ ký số đó là xác thực và thông điệp đã không bị thay đổi trên đường truyền [2]. Ngoài ra, chữ ký số có thể được gắn thêm một “nhãn” thời gian với mục đích sau một thời gian nhất định quy định bởi nhãn đó, chữ ký gốc sẽ không còn hiệu lực, đồng thời nhãn thời gian cũng là công cụ để xác định thời điểm ký.

4. NHỮNG ĐẶC ĐIỂM CHÍNH CỦA BLOCKCHAIN

4.1 Một cơ sở dữ liệu phân tán

Thông tin tổ chức trên một blockchain được tồn tại dưới dạng cơ sở dữ liệu (CSDL) phân tán. CSDL blockchain không được lưu trữ ở duy nhất một vị trí nào mà được lưu trữ trên các block của hệ thống nhưng có liên kết logic với nhau một cách công khai, dễ kiểm chứng [1]. Không có một phiên bản tập trung nào của CSDL này tồn tại, nên hacker cũng chẳng có cơ hội nào để tấn công nó. Về mặt vật lý, CSDL của blockchain được lưu trữ bởi hàng triệu máy tính cùng lúc, dữ liệu của nó có thể truy cập bởi bất cứ người nào trên Internet.

4.2 Tính bền vững của blockchain

Bằng cách lưu trữ những khối thông tin giống nhau trên mạng lưới của mình, do đó blockchain không thể:

- Bị kiểm soát bởi bất kỳ một thực thể nào;
- Không có điểm thiếu sót hoặc lỗi duy nhất nào.

4.3 Minh bạch và không thể bị phá vỡ

Mạng lưới blockchain tồn tại trong trạng thái của sự thỏa thuận, tự động kiểm tra 10 phút một lần. Một loại hệ sinh thái tự kiểm soát giá trị kỹ thuật số, mạng lưới sẽ điều hòa mọi giao dịch xảy ra trong khoảng 10 phút. Mỗi nhóm giao dịch này được gọi là khối. Hai đặc tính quan trọng được rút ra từ đây:

- Minh bạch: Dữ liệu được nhúng trong mạng như một khối, công khai;
- Không thể bị hỏng: Khi thay đổi bất kỳ đơn vị thông tin nào trên blockchain có nghĩa là phải sử dụng một số lượng lớn máy tính để ghi đè thông tin lên toàn bộ mạng.

4.4 Một mạng lưới các nút

Một mạng lưới các nút tính toán tạo thành blockchain là các máy tính được kết nối với mạng với nhau, sử dụng client để thực hiện nhiệm vụ xác nhận và chuyển tiếp các giao dịch. Nút sẽ nhận được một bản sao của blockchain, được tải tự động khi tham gia mạng lưới blockchain.

Các nút này cùng nhau tạo ra một mạng lưới cấp 2 mạnh mẽ, một góc nhìn hoàn toàn khác về cách mà Internet có thể hoạt động. Mỗi nút là một “quản trị viên” của mạng blockchain và tự động tham gia vào mạng.

4.5 Ý tưởng về phân quyền

Theo thiết kế, blockchain là một công nghệ được phân quyền. Bất cứ điều gì xảy ra trên đó đều là chức năng của mạng. Nhờ tạo ra cách mới để xác nhận giao dịch mà những khía cạnh của thương mại truyền thống có thể trở nên không cần thiết. Ví dụ như những giao dịch trên thị trường chứng khoán có thể thực hiện cùng lúc trên Blockchain, hoặc có thể lưu trữ tài liệu giống như sổ đỏ, hoàn toàn công khai. Và sự phân quyền đã trở thành hiện thực.

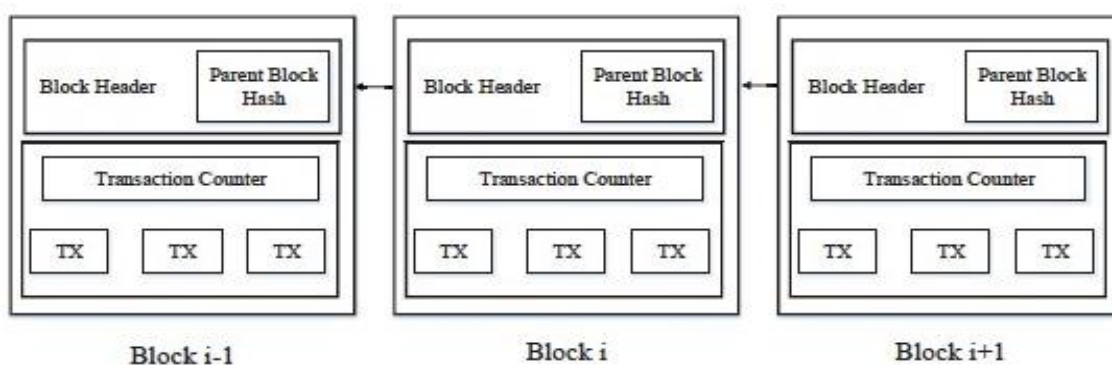
4.6 Tăng cường bảo mật

Nhờ lưu trữ dữ liệu trên mạng của mình, blockchain loại bỏ những rủi ro đi kèm với dữ liệu được tổ chức tập trung. Trên Internet thì chúng ta dựa vào hệ thống username/password để bảo vệ danh tính và tài sản của mình trên mạng, nhưng với cách làm này hệ thống vẫn có nhiều khả năng bị rủi ro. Còn phương pháp bảo mật của blockchain sử dụng công nghệ mã hóa với cặp khóa public/private. Khóa public (một chuỗi dài các số ngẫu nhiên) là địa chỉ của người dùng trên blockchain. Khóa private giống như mật khẩu, cho phép chủ sở hữu truy cập vào giao dịch hoặc các tài sản kỹ thuật số khác.

5. CẤU TRÚC CỦA BLOCKCHAIN

Để hiểu blockchain một cách sâu sắc chúng ta cần nắm được các khái niệm sau: chuỗi khối (block chain), cơ chế đồng thuận phi tập trung (decentralized consensus), tính toán tin cậy (trusted computing), hợp đồng thông minh (smart contracts) và bằng chứng công việc (proof of work). Mô hình tính toán này là nền tảng của việc tạo ra các ứng dụng phân tán trên nền tảng blockchain.

Blockchain có cấu trúc phi tập trung. Nghĩa là, CSDL của nó không dựa vào các tổ chức thứ ba để quản lý và xác thực, không có kiểm soát trung tâm, tất cả các nút nhận được thông tin tự kiểm tra, truyền tải, và quản lý, đặt sự tin tưởng vào các nút, cho phép các nút lưu trữ các giao dịch trong một khối (block). Các block được ghép nối với nhau tạo nên một chuỗi khối (blockchain). Cấu trúc phi tập trung là đặc điểm nổi bật và quan trọng nhất của blockchain [5].



Hình 1: Cấu trúc dữ liệu của blockchain

Mỗi block trong blockchain bao gồm các thành phần sau:

- Index (Block#): Thứ tự của block (block gốc có thứ tự 0)
- Hash: Giá trị băm của block
- Previous Hash: Giá trị băm của block trước.
- Timestamp: Thời gian tạo của block;
- Data: Thông tin lưu trữ trong block;
- Nonce: Giá trị biến thiên để tìm ra giá trị băm thỏa mãn yêu cầu của mỗi Blockchain;

🏆 Genesis Block	
🔗 Previous Hash	0
📅 Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
📄 Data	Welcome to Blockchain CLI!
🔥 Hash	0000018035a828da0...
🔑 Nonce	56551

Hình 2: Cấu trúc của block gốc

Giá trị băm (Hash) sẽ băm toàn bộ các thông tin cần thiết như timestamp, previous hash, index, data, nonce.

Khi có một block được thêm vào, block mới sẽ có giá trị “Previous Hash” là giá trị băm của block được thêm trước nó. Blockchain tìm kiếm block được thêm vào gần nhất để lấy giá trị index và previous hash. Block tiếp theo sẽ được tính như sau:

- Index: 0+1 = 1; - Previous Hash: 0000018035a828da0... 9;
- Timestamp: thời gian block được tạo ra; - Data: dữ liệu lưu trữ trong block;
- Hash: ??; - Nonce: ???;

Ta cần tìm giá trị “nonce” phù hợp để có giá trị băm Hash thỏa mãn điều kiện của blockchain. Số lượng số 0 ở đầu được gọi là “difficulty”.

Bằng cách lưu trữ dữ liệu trên tất cả các nút của mình, mạng blockchain loại bỏ các rủi ro đi kèm với dữ liệu được tổ chức lưu trữ tập trung. Trong mạng không có các điểm tập trung dễ bị tổn thương cho hệ thống, không có các điểm trung tâm làm cho hệ thống dừng hoạt động. Bất kỳ nút nào trong mạng khi dừng hoạt động sẽ không ảnh hưởng đến sự vận hành của hệ thống.

6. ỨNG DỤNG BLOCKCHAIN VÀO QUẢN LÝ VĂN BẢN

6.1 Bài toán đặt ra

Hiện nay việc lưu trữ, quản lý, tra cứu và xác thực văn bằng cho người học gặp nhiều khó khăn trong khi số lượng người học ngày càng tăng. Việc quản lý phôi văn bằng để cấp cho người học có nhiều sự thay đổi dẫn đến văn bằng cấp cho người học khó kiểm soát. Nói cách khác, khó có thể phân biệt được văn bằng đã cấp cho người học là thật hay giả.

Với thực trạng trên, bài báo đề xuất một mô hình để xây dựng một hệ thống lưu trữ, quản lý, tra cứu và xác thực thông tin văn bằng dựa vào công nghệ blockchain nhằm đảm bảo tính kịp thời, an toàn, chuẩn xác, minh bạch. Đồng thời, xây dựng một công cụ hỗ trợ người dùng có thể tìm hiểu đầy đủ thông tin của một tấm bằng tốt nghiệp một cách nhanh chóng, chính xác và tin cậy.

6.2 Cách tiếp cân và giải quyết bài toán

Tạo ra một hệ thống lưu trữ thông tin tốt nghiệp dựa trên nền tảng công nghệ blockchain. Sau đó, xây dựng trang web cho phép người dùng tra cứu thông tin tốt nghiệp đã được lưu trong hệ thống và cài đặt một mô đun trên điện thoại thông minh phục vụ cho việc xác thực thông tin thông qua quét mã QR. Không mất tính tổng quát của vấn đề trình bày, chúng ta giả sử rằng hệ thống được xây dựng cho một cơ sở giáo dục cao nhất ở một tỉnh X nào đó, chẳng hạn Sở Giáo dục và Đào tạo Tỉnh (SGD). SGD sẽ quản lý các Phòng giáo dục thuộc các huyện, thị xã, ... ; đồng thời cùng với Sở, đây

là các đơn vị được phép cấp văn bằng, chứng chỉ cho người học. Để việc tổ chức quản lý dữ liệu, tra cứu và xác thực thông tin hệ thống cần đảm bảo:

a. Dữ liệu tốt nghiệp cần được lưu trữ đồng thời cả ở SGD và tất cả các đơn vị; dữ liệu này phải đảm bảo tính thống nhất về cả cấu trúc và cả về thông tin.

b. Từ CSDL đã có, xây dựng trang web dùng quản lý, tra cứu thông tin văn bằng tốt nghiệp gồm các chức năng sau:

- Quản trị hệ thống:
 - ✓ Thiết lập các nút cơ sở, cho phép/không cho phép các nút cập nhật dữ liệu.
 - ✓ Các nút cơ sở: Cập nhật dữ liệu vào hệ thống (nếu được phép); tự động đồng bộ dữ liệu khi có một nút cập nhật dữ liệu.
- Trang tra cứu thông tin:
 - ✓ Người dùng nhập số hiệu của văn bằng hoặc số vào sổ cấp bằng hoặc các thông tin khác của người muốn tra cứu.
 - ✓ Thông tin tốt nghiệp chi tiết của người đó sẽ được hiển thị trên màn hình.
 - ✓ Người dùng có thể xem một số thông tin khác có liên quan đến thông tin trong văn bằng của người được cấp như: Trường cấp bằng, kết quả thi...
 - ✓ Ngoài các thông tin hiển thị sau khi tra cứu còn có phần hiển thị mã QR về thông tin người học để người dùng có thể xác thực; ngoài ra, người dùng có thể trực tiếp đăng ký cấp lại bản sao văn bằng qua hệ thống nếu có nhu cầu.

c. Song song với việc tổ chức lưu trữ, tra cứu, một mô đun cài đặt trên điện thoại thông minh cho phép đọc mã QR được hiển thị trên trang web khi tra cứu, mô đun này sẽ hiển thị thông tin sau khi đọc mã QR để người dùng có thể đối chiếu xác thực với thông tin được hiển thị trên web.

d. Ứng dụng công nghệ blockchain trong việc lưu trữ, quản lý, tìm kiếm và xác thực thông tin văn bằng của người học là công cụ giúp cho các tổ chức giáo dục và các nhà tuyển dụng có thể dễ dàng kiểm chứng tính chính xác về thông tin của một tấm bằng nào đó một cách tin cậy và nhanh chóng. Không những vậy, người dùng có thể nhanh chóng truy cập vào trang web, nhập số hiệu của bằng vào hệ thống để tìm kiếm và đối chiếu xem chiếc bằng đó có phải là giả hay không.

7. KIẾN TRÚC HỆ THỐNG

7.1 Thiết kế hệ thống

Do đặc thù của việc quản lý, truy xuất và xác minh bằng cấp hệ thống sẽ được xây dựng theo mô hình Private Blockchain. Nghĩa là, các nút có thể cập nhật các block

vào blockchain khi được phép của người quản trị và tất cả người dùng đều có quyền truy cập vào hệ thống để tra cứu thông tin nhưng không thể thêm hoặc thay đổi thông tin trong blockchain của hệ thống.

7.2 Thiết kế cơ sở dữ liệu

Hệ thống được chia làm 3 phần chính:

- *Blockchain*: Mỗi block sẽ chứa thông tin tốt nghiệp của một người học và sẽ được liên kết với nhau để tạo nên một blockchain. Trong mỗi block còn chứa các thông tin khác liên quan như: Thông tin về khóa thi, trường theo học, kết quả thi,... các thông tin được tổ chức lưu trữ trong các bảng với cấu trúc như sau:

TT	Trường	Kiểu dữ liệu	Khóa	Ghi chú
1	index	bigint	x	Index của block
2	ngaytao	date		Ngày tạo block
3	dulieu	json		Dữ liệu văn bản
4	hashtruoc	text		Hash của block ngay trước block này
5	hash	text		Hash của block này
6	nonce	bigint		Độ phức tạp của block

Khóa thi:

TT	Trường	Kiểu dữ liệu	Khóa	Ghi chú
1	khoathiid	bigint	x	Index của khóa thi
2	ten	text		Tên khóa thi
3	khoangay	date		Ngày tổ chức khóa thi
4	namhoc	text		Năm học
5	mon1	text		Môn thi 1
...	...	...		...
...	monn	text		Môn thi n
...	trangthai	bigint		Trạng thái của khóa thi

Tài khoản:

TT	Trường	Kiểu dữ liệu	Khóa	Ghi chú
1	taikhoanid	bigint	x	Index của tài khoản
2	truonghocid	text		Index trường học của tài khoản
3	matruonghoc	text		Mã quản lý trường học của tài khoản
4	tendangnhap	text		Tên đăng nhập vào hệ thống
5	matkhau	text		Mật khẩu đăng nhập hệ thống
6	hoten	text		Họ tên người dùng
7	email	text		Email của người dùng
8	sodienthoai	text		Số điện thoại của người dùng
9	nhomquyen	text		Nhóm quyền trên hệ thống
10	trangthai	bigint		Trạng thái của tài khoản

Trường học:

TT	Trường	Kiểu dữ liệu	Khóa	Ghi chú
1	truonghocid	bigint	x	Index của trường học
2	matruonghoc	text		Mã quản lý của trường học
3	tentruonghoc	text		Tên trường học
4	diachi	text		Địa chỉ
5	hieutruong	text		Tên hiệu trưởng hiện tại
6	dtht	text		Số điện thoại của hiệu trưởng
7	dtpv	text		Số điện thoại của văn phòng
8	email	text		Email của trường học
9	n1718	text		Tên của trường năm học 2017-2018
10	n1819	text		Tên của trường năm học 2018-2019
...	...	...		...

Văn bằng:

TT	Trường	Kiểu dữ liệu	Khóa	Ghi chú
1	id	bigint	x	Index của văn bằng
2	matruong	text		Mã trường
3	hoten	text		Họ tên thí sinh
4	gioitinh	bigint		Giới tính của thí sinh
5	ngaysinh	date		Ngày sinh của thí sinh
6	noisinh	text		Nơi sinh của thí sinh
7	dantoc	text		Dân tộc của thí sinh
8	hoidong	text		Hội đồng thi
9	d1	float		Điểm thi môn 1
...	...	...		...
...	dn	float		Điểm thi môn n
...	hocluc	bigint		Học lực của thí sinh
...	hanhkiem	bigint		Hạnh kiểm của thí sinh
...	daccach	bigint		Đặc cách
...	mienthi	bigint		Miễn thi
...	sovaoso	text		Số vào sổ của văn bằng
...	sohieu	text		Số hiệu của văn bằng
...	cmnd	text		Số chứng minh nhân dân
...	loai	bigint		Loại văn bằng
...	khoathi	bigint		Index của khóa thi
...	nguoitao	bigint		Người nhập thông tin văn bằng
...	ngaytao	date		Ngày nhập văn bằng
...	trangthai	bigint		Trạng thái của văn bằng

- *Các Server*: Mỗi node là một Server, trong đó Server trung tâm (Sở Giáo dục) làm nhiệm vụ lưu trữ dữ liệu gốc và phục vụ cho việc truy xuất, tra cứu thông tin của người dùng. Các Server khác (mỗi đơn vị thuộc SGD đặt một server) tương ứng với các node. Dữ liệu trong blockchain được cập nhật, tự động đồng bộ và được lưu trữ đồng thời tại các node. Khi một node cập nhật một block mới, các node còn lại sẽ tự động

Blockchain - giải pháp truy xuất nguồn gốc bằng cấp

kiểm tra dữ liệu đã có với dữ liệu trên hệ thống và tiến hành cập nhật lại dữ liệu nếu dữ liệu đã có đảm bảo là chính xác.

- *Quá trình đồng bộ dữ liệu giữa các node được thực hiện như sau:* Khi một node cập nhật một block mới, block đó sẽ được thêm vào blockchain trên node đó. Định kỳ, Server trung tâm sẽ tiến hành kiểm tra tính hợp lệ của các block trong blockchain trung tâm so với các block trong blockchain của các node. Nếu blockchain ở các node dài hơn và các block đầu là hợp lệ thì tiến hành cập nhật các block ở các node vào blockchain trên Server. Ngược lại, các node cũng tiến hành kiểm tra tính hợp lệ giữa các block trên các node với các block trên Server để tiến hành cập nhật dữ liệu.

- *Client:* Thực hiện tìm kiếm và hiển thị thông tin truy xuất được Server gửi về lên trang web cho người dùng xem.

- Một số hình ảnh minh họa của hệ thống:

Thứ 2, ngày 2 tháng 09 năm 2019

Đăng nhập

TRA CỨU THÔNG TIN TỐT NGHIỆP

Khóa thi:

--Chọn khóa thi--

Số hiệu:

Nhập số hiệu của văn bằng

Số vào sổ:

Nhập số vào sổ của văn bằng

Trường học:

--Chọn trường học--

Họ và tên:

Nhập họ và tên

Số CMND:

Nhập số chứng minh

Reset

Tìm kiếm

STT	SỐ HIỆU	SỐ VÀO SỔ	HỌ VÀ TÊN	NGÀY SINH	GIỚI TÍNH	TRƯỜNG HỌC
-----	---------	-----------	-----------	-----------	-----------	------------

Màn hình tra cứu thông tin văn bằng

BẢNG TỐT NGHIỆP THPT

Họ tên:

Nguyễn Như Hoàng Anh

Ngày sinh:

01/10/2000

Giới tính:

Nam

Dân tộc:

Kinh

Nơi sinh:

Đắc Lắc

Số CMND:

197392536

Số hiệu:

B.2752418

Số vào sổ:

00001/2018

Hội đồng:

Sở GD&ĐT Quảng Trị

Hình thức:

Giáo dục phổ thông

Loại bằng:

Trung học phổ thông

Khóa ngày:

25/06/2018

Thông tin khóa thi

Thông tin trường học

Chi tiết điểm thi

Chia sẻ thông tin bằng:



Chi tiết thông tin văn bằng

3. KẾT LUẬN

Trong bài báo này, chúng tôi đã đề xuất mô hình quản lý thông tin trên các văn bằng bằng công nghệ blockchain nhằm lưu trữ, quản lý, tra cứu và xác thực thông tin thật giả về văn bằng đã cấp phát. Song song với việc đề xuất mô hình này, chúng tôi đã

xây dựng một trang web để người sử dụng có thể dễ dàng thao tác với hệ thống và xây dựng một mô đun cài đặt trên điện thoại thông minh cho phép đọc mã QR được hiển thị trên trang web khi tra cứu để người dùng có thể đối chiếu xác thực với thông tin được hiển thị.

TÀI LIỆU THAM KHẢO

- [1]. Nguyễn Mậu Hân (2012), *Cơ sở dữ liệu phân tán*, NXB Đại Học Huế.
- [2]. Phan Đình Diệu (2002). *Lý thuyết mật mã và an toàn thông tin*, NXB ĐHQG Hà Nội.
- [3]. Đoàn Ngọc Sơn (2017), *Nghiên cứu, ứng dụng công nghệ blockchain trong thanh toán di động*, luận văn thạc sĩ chuyên ngành HT Thông tin, trường Đại học Công nghệ, ĐHQG Hà Nội.
- [4]. Bashir I. (2017). *Mastering Blockchain*, Published by Packt Publishing Ltd. Livery Place, 35 Livery Street, Birmingham.
- [5]. Gates M. (2017). *Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money*. Wise Fox Publishings and Mark Gates.
- [6]. Tapscott D. and Tapscott A. (2018). *Blockchain Revolution*. <http://blockchain-revolution.com/>
- [7]. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" *2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017*, pp. 557-564.
- [8]. Bitcoin Vietnam News (2019). <https://bitcoinvietnamnews.com/blockchain-la-gi> (truy cập ngày 07/12/2019).
- [9]. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," <https://bitcoin.org/bitcoin.pdf>

BLOCKCHAIN – A SOLUTION OF EXTRACT ORIGINAL DIPLOMAS

Nguyen Mau Han

Faculty of Information Technology, University of Sciences, Hue University

Email: nmhan@hueuni.edu.vn

ABSTRACT

Blockchain, a technology that allows the transmission of data based on an extremely complex encryption system, is similar to a company's ledger, in which all activities involved public money will be very closely monitored. It is very difficult to manage the diplomas to issue to learners. In other words, it is not easy to distinguish the authenticity of diplomas, which greatly affects the organization and order in society. This paper proposes a model for managing information on diplomas by using blockchain technology to store, manage, look up and validate the fake information about issued diplomas.

Keywords: Blockchain, diploma, fake information.



Nguyễn Mậu Hân sinh năm 1957 tại Thừa thiên Huế. Năm 1981, ông tốt nghiệp cử nhân toán tại Trường Đại học Tổng hợp Huế. Năm 1998, ông nhận bằng thạc sĩ Khoa học máy tính tại Trường Đại học Bách khoa Hà Nội. Năm 2003, ông nhận bằng tiến sĩ Khoa học Máy tính tại Viện Công nghệ Thông tin Hà Nội. Hiện ông là Phó Giáo sư, Giảng viên cao cấp tại Trường Đại học Khoa học, Đại học Huế.

Lĩnh vực nghiên cứu: Công nghệ phần mềm, Cơ sở dữ liệu, Xử lý song song và phân tán.