XÂY DỰNG MÔ HÌNH ỨNG DỤNG BLOCKCHAIN VÀ CHỮ KÝ SỐ TRONG QUẢN LÝ VĂN BẰNG VÀ CHỨNG CHỈ Ở VIỆT NAM

Nguyễn Quỳnh Chi*
*Học viện Công nghệ Bưu chính Viễn thông

Tóm tắt: Vấn đề buôn bán, sử dụng văn bằng, chứng chỉ giả đã và đang là một vấn nạn của xã hội trong bối cảnh khoa học công nghệ phát triển mạnh mẽ. Các cơ quan, tổ chức đều đang phải đối mặt với bài toán nan giải này trong những thời điểm như tuyển dụng, tổ chức các kỳ thi nâng cao trình độ hoặc xét duyệt đi du học. Điều đáng báo động chỉ trong vài năm trở lại đây, đã có hàng chục nghìn văn bằng, chứng chỉ giả đã được các cơ quan chức năng phát hiện, xử lý. Vấn đề này được giải quyết bằng cách sử dụng công nghệ blockchain với khả năng phi tập trung, phân tán, bảo mật, xử lý nhanh, minh bạch và không thể sửa đổi. Những đặc tính ưu việt hơn so với các công nghệ hiện nay để chống lại gian lận và giả mạo văn bằng, chứng chỉ. Tuy nhiên. hạn chế lớn ở Việt Nam hiện nay là blockchain không được pháp luật quy định rõ ràng nên ngày càng có áp lực để đảm bảo tính pháp lý và tính xác thực của các văn bằng, chứng chỉ. Trong bài báo này, nhóm nghiên cứu trình bày mô hình giải pháp xác thực văn bằng, chứng chỉ dựa trên ứng dụng công nghệ Blockchain và chữ ký số để giải quyết vấn đề trên. Mô hình đề xuất được thực nghiệm trên dữ liệu văn bằng, chứng chỉ của Học viện Công nghệ Bưu chính Viễn thông để đánh giá hiệu năng của mô hình và các kết quả đạt được cho thấy hiệu quả khả quan và mô hình có thể ứng dụng trong thực tiễn quản lý văn bằng, chứng chỉ.

Từ khóa: Blockchain; Chữ ký số; Chứng chỉ; Văn bằng.

I. GIỚI THIỆU

Blockchain có thể được xem như cuốn sổ cái ghi lại mọi giao dịch một cách công khai trên một hệ thống máy tính đồng đẳng dựa trên phương thức mã hóa theo chuỗi thời gian. Blockchain cho phép loại bỏ các bên trung gian, giảm thiểu nguy cơ bị tấn công mạng, thay đổi cách thức kiến tạo, lưu trữ và xử lý thông tin. Theo ước tính vào năm 2025, 10% GDP của thế giới (khoảng 100 tỷ đô la Mỹ) sẽ được kiểm soát bằng việc sử dụng các công nghệ blockchain [1]. Do các khả năng độc đáo của blockchain là bảo mật, phân quyền, minh bạch, truy xuất nguồn gốc và bất biến, blockchain đã được sử dụng trong nhiều lĩnh vực khác nhau như tài chính [2], chính phủ [3], giáo dục [4], y tế [5], năng lượng [6], ngân hàng [7] và tạo ra nhiều ứng dụng giúp tăng cường độ tin cậy, tính trách nhiệm và minh bạch của giao dịch với chi phí tối thiểu và quy trình thủ tục tối giản.

Theo báo cáo của Viện thống kê UNESCO (UIS) [8], hơn 235 triệu sinh viên theo học các chương trình giáo dục đại học trên thế giới vào năm 2020, tăng hơn gấp đôi so với 100 triệu sinh viên đăng ký vào năm 2000 (theo cơ sở dữ liệu UIS). Do vậy, việc ứng dụng blockchain vào giáo dục đào tạo là vô cùng tiềm năng và cần thiết bởi hầu hết các văn bằng, chứng chỉ đều ở dạng giấy hoặc điện tử và rất khó bảo quản, tra cứu và sử dụng khi được yêu cầu. Không dễ để kiểm tra tính xác thực của văn bằng, chứng chỉ bởi trong bối cảnh khoa học công nghệ phát triển việc làm văn bằng, chứng chỉ giả rất tinh vi. Theo [9], trong năm 2004, Bộ Giáo dục và Đào tạo Việt Nam đã phát hiện hơn 10.000 chứng chỉ giả cùng các tài liệu liên quan khác được rao bán công khai trên Internet, mạng xã hội và các sàn giao dịch tinh vi [10]. Bên cạnh đó, không phải cơ quan, tổ chức nào cũng có một bản sao các văn bằng, chứng chỉ đó để xác thực từng tài liệu, nên tính nguyên gốc của văn bằng, chứng chỉ phải được xác minh với tổ chức phát hành (nếu vẫn còn). Các trường đại học có thể cung cấp một số hình thức xác minh hoặc dựa vào các dịch vụ khác cho nhiệm vụ này để giảm thiểu vấn đề. Mặc dù vậy, các sáng kiến như vậy bị thiếu tiêu chuẩn hóa và thống nhất [11], và điều này thường tốn thời gian và nguồn lực, đồng thời trong quá trình thực hiện có thể phát sinh những vấn đề quan liêu.
Như vậy có thể thấy những tồn tại, hạn chế công tác quản lý văn bằng, chứng chỉ hiện nay tập trung vào việc ký văn bằng chứng chỉ chưa đúng thẩm quyền; lập và quản lý sổ gốc cấp văn bằng chứng chỉ, sổ cấp bản sao văn bằng chứng chỉ, việc nhận thay văn bằng chứng chỉ dễ dẫn đến thất lạc; việc in, quản lý, cấp phát phôi văn bằng, chứng chỉ trong tình trạng tự chủ in, quản lý phôi văn bằng chứng chỉ; công khai thông tin văn bằng chứng chỉ trên trang điện tử của các đơn vị; tra cứu, xác minh với người có văn bằng chứng chỉ, với cơ quan quản lý và các tổ chức liên quan

Tác giả liên hệ: Nguyễn Quỳnh Chi,
Email: chinq@ptit.edu.vn
Đến tòa soạn: 10/2022, chỉnh sửa: 11/2022, chấp nhận đăng: 12/2022.

[12].

Với những tồn tại trên, trong thực tế hiện nay chữ ký số (là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng, theo đó, người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác) hướng tới khắc phục được vấn đề về người có thẩm quyền ký văn bằng, chứng chỉ; đảm bảo tính toàn vẹn của văn bằng chứng chỉ trong môi trường điện tử ở góc độ người nhận văn bằng, chứng chỉ đã có ký số mới có thể mở được văn bằng, chứng chỉ đó chứ chưa giải quyết được vấn đề tính toàn vẹn của văn bằng chứng chỉ để đảm bảo cho việc tra cứu, xác minh. Để giải quyết vấn đề này blockchain được coi là một giải pháp tiềm năng để cải thiện quy trình, tăng tính minh bạch, mang lại hiệu quả bổ sung, đạt được sự phân quyền và do đó giảm gian lận văn bằng, chứng chỉ. Nó cũng có thể được sử dụng để xây dựng một hệ sinh thái xác thực chứng chỉ toàn cầu (xuyên quốc gia) [13], giúp chống giả mạo và phi tập trung, để dữ liệu có thể được truy xuất ngay cả khi tổ chức hoặc toàn bộ hệ thống của cơ quan phát hành văn bằng, chứng chỉ ngừng hoạt động. Đặc tính bất biến của nó có thể nâng cao uy tín và giảm nguy cơ mất thông tin. Nhiều nghiên cứu đã khai thác đặc điểm này của blockchain để ứng dụng trong lĩnh vực giáo dục ở trong và ngoài nước như [14], [15], [16], [17], [18]. Tuy nhiên, theo hiểu biết của nhóm tác giả thì tại Việt Nam việc quản lý văn bằng chứng chỉ mặc dù ứng dụng công nghệ blockchain nhưng phải tuân thủ theo Thông tư 21/2019/TT-BGDĐT [19] và Việt Nam đang hướng tới hoàn thiện hệ thống pháp luật, xây dựng thể chế, chính sách tạo hành lang pháp lý cho các hoạt động liên quan đến công nghệ blockchain. Do đó tính pháp lý của việc quản lý văn bằng, chứng chỉ ứng dụng công nghệ blockchain mới chỉ dừng ở nghiên cứu mang tính lý thuyết, chưa thực tế nên việc cần hệ thống xác thực và có tính pháp lý đối văn bằng, chứng chỉ là yêu cầu cấp thiết hiện nay.

Dựa trên mục đích của công việc này, các câu hỏi nghiên cứu sau đây đã được đưa ra:

Câu hỏi nghiên cứu 1. Công nghệ blockchain có thể mang lại những lợi ích gì cho quản lý văn bằng, chứng chỉ?

Câu hỏi nghiên cứu 2. Giải pháp nào để đảm bảo tính pháp lý trong quản lý văn bằng, chứng chỉ?

Phần còn lại của bài báo được cấu trúc như sau. Phần 2 trình bày kiến thức nền tảng của blockchain, lợi ích của blockchain trong quản lý văn bằng, chứng chỉ và những nghiên cứu liên quan. Phần 3 giới thiệu mô hình giải pháp đề xuất đảm bảo tính xác thực và tính pháp lý trong quản lý văn bằng, chứng chỉ. Tiếp đó, cung cấp môi trường, dữ liệu thử nghiệm để đánh giá, phân tích sâu và thảo luận về kết quả tại Phần 4. Cuối cùng, Phần 5 kết thúc bài báo và đưa ra định hướng nghiên cứu tương lai.

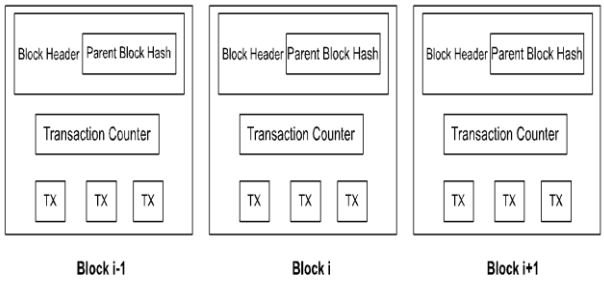
II. KIẾN THỨC CƠ BẢN LIÊN QUAN

Phần này trình bày nền tảng cần thiết cho những người đọc không chuyên về kỹ thuật có thể hiểu những điều cơ bản về công nghệ blockchain. Sau đó là trình bày về một số nghiên cứu cùng hướng nghiên cứu trong thời gian gần đây.

A. Kiến thức cơ bản

Công nghệ chuỗi khối (blockchain) là một công nghệ có nguồn gốc liên quan đến tiền điện tử bitcoin và công nghệ cơ bản do Satoshi Nakamoto đề xuất vào năm 2008 [20]. Theo Gatteschi và cộng sự [21], sự phát triển của các ứng dụng dựa trên blockchain có thể được chia thành ba giai đoạn chính: Blockchain 1.0, 2.0 và 3.0. Ngay từ khi ra đời, công nghệ này đã được liên kết với các giao dịch và sử dụng để phát triển các đồng tiền điện tử, đây được gọi là Blockchain 1.0. Sự ra đời của các hợp đồng thông minh (smart contracts) bổ sung quyền riêng tư, đại diện cho sự bùng nổ của Blockchain 2.0, với sự phát triển của một loạt các ứng dụng mới trong các lĩnh vực tài chính. Với các đặc tính cơ bản của blockchain là phân cấp, bất biến và minh bạch nên đã thu hút được sự quan tâm ngày càng tăng của trong các lĩnh vực như y tế, chuỗi cung ứng, chính phủ, giáo dục, đây được gọi là giai đoạn Blockchain 3.0 [22]. Hiện nay, blockchain 4.0 hướng tới trí tuệ nhân tạo (AI), hỗ trợ ra quyết định dựa trên AI phi tập trung và dữ liệu đáng tin cậy của blockchain mà không cần sự can thiệp trực tiếp của con người.

Blockchain có thể được xem như một cuốn sổ cái công khai, chống giả mạo và tất cả các giao dịch được lưu trữ trong một danh sách các khối (block). Các chuỗi này được ghép nối với nhau tạo thành một chuỗi khối. Chuỗi này liên tục được phát triển khi các khối mới được thêm vào. Với hàm mật mã bất đối xứng và cơ chế đồng thuận phân tán đã làm cho blockchain bảo mật, nhất quán hơn các cuốn sổ cái truyền thống.



Hình 1: *Cấu trúc dữ liệu của blockchain*

Mỗi chuỗi trong blockchain gồm các thành phần sau:

- Index (block#): thứ tự của chuỗi (chuỗi gốc có thứ tự 0)
- Hash: giá trị băm của chuỗi
- Previous hash: giá trị băm của chuỗi trước
- Timestamp: nhãn thời gian khởi tạo của chuỗi
- Data: thông tin lưu trữ trong chuỗi
- Nonce: giá trị biến thiên để tìm ra giá trị băm thỏa mãn yêu cầu của mỗi blockchain

Giá trị băm sẽ băm toàn bộ các thông tin cần thiết gồm Index, Previous hash, Timestamp, Data và Nonce. Khi có một chuỗi được thêm vào, chuỗi mới sẽ có giá trị "Previous Hash" là giá trị băm của chuỗi được thêm trước nó. Blockchain tìm kiếm chuỗi được thêm vào gần nhất để lấy giá trị index và previous hash. 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. Trên thực tế, ngay cả những thay đổi nhỏ nhất trong bản ghi dữ liệu cũng sẽ thay đổi đáng kể hàm băm khối, điều này sẽ thể hiện truy cập sửa đổi cơ sở dữ liệu. Về loại hàm băm, mạng Bitcoin sử dụng thuật toán SHA-256 và RIPEMD-160, trong khi Ethereum sử dụng thuật toán KECCAK-256, không tuân theo chính xác tiêu chuẩn FIPS, còn được gọi là SHA-3 thuật toán. Bên cạnh tính giá trị băm, công nghệ blockchain triển khai các chức năng mã hóa để cung cấp bảo mật và chữ ký số cho các giao dịch. Thuật toán mã hóa chính là thuật toán mã hóa đường cong Elliptic, sử dụng đường cong elliptic (EC) $y^2 = x^3 + ax + b$ trên trường Galois hữu hạn được xác định với một số nguyên tố p.

Có ba loại blockchain chính [23] gồm:

- Blockchain công khai là một dạng blockchain mà ở đó tất các mọi người tham gia đều có quyền như nhau, tất cả mọi người tham gia có thể đọc, ghi. Ưu điểm của loại blockchain này là độ tin cậy cao, an toàn và bảo mật hệ thống cao. Nhưng hạn chế là tốc độ xử lý giao dịch chậm, tiêu tốn nhiều tài nguyên điện để hoạt động và dữ liệu cá nhân có khả năng bị công khai. Bitcoin và Ethereum là loại blockchain này.
- Blockchain riêng tư là một blockchain có sự phân quyền, không phải ai cũng được quyền tham gia vào hệ thống này, chỉ những người được cho phép mới tham gia vào được. Ưu điểm của loại blockchain này là tốc độ xử lý giao dịch nhanh, tốn ít tài nguyên, khả năng mở rộng dễ dàng nhưng hạn chế về độ tin cậy, bảo mật thấp và tính phi tập trung kém bởi việc xây dựng và duy trì private blockchain được thực hiện chỉ bởi vài tổ chức. Hyperledger là một loại blockchain này.
- Consortium Blockchain là sự kết hợp của 2 loại blockchain trên. Giống như trong một blockchain riêng tư, người tham gia chỉ có thể tham gia nếu được mời, tuy nhiên, không có tổ chức nào kiểm soát mạng lưới mà thay vào đó là một nhóm. Từ góc độ quản trị, chúng duy trì bản chất phi tập trung của một blockchain công khai, mặc dù chúng được kiểm soát và quản lý chặt chẽ hơn. Do đó, khối lượng giao dịch, tốc độ và việc sử dụng tài nguyên cũng tốt hơn.

Hợp đồng thông minh (smart contracts) [24] được đề xuất vào những năm 1990, là các điều khoản có thể được mô tả bằng ngôn ngữ lập trình và được thực thi bởi máy tính. Ethereum đã giới thiệu các hợp đồng thông minh trong mã nguồn cốt lõi của nó, làm cho blockchain có thể lập trình được và do đó, cho phép các nhà phát triển viết một bộ ứng dụng đa dạng [25]. Ngoài ra, hợp đồng thông minh có thể được xem như một đối tượng có trạng thái, thuộc tính và chức năng hoặc phương thức có thể được gọi để thay đổi trạng thái, gọi các chức năng khác hoặc các hợp đồng thông minh khác [26]. Tất cả các hoạt động đều chống giả mạo và được ghi lại trong blockchain để tăng thêm độ tin cậy.

Các tính năng cơ bản của blockchain như sau [27]:

- Phi tập trung: blockchain là một bản ghi mở phổ biến, trong đó tất cả các nút được liên kết với nhau trong một mạng.
- Tính minh bạch: tất cả các giao dịch trên blockchain được lập chỉ mục theo thứ tự tuần tự và một khối được liên kết với hai khối liền kề bằng một hàm băm mật mã, các giao dịch được lưu lại và có thể kiểm tra các giao dịch này.
- Cơ chế đồng thuận: cơ chế chịu lỗi là cơ chế đồng thuận được sử dụng trong các máy tính và blockchain để đạt được thỏa thuận về một dữ liệu duy nhất của trạng thái mạng giữa các quy trình phân tán.
- Tính bí mật: chỉ người giữa khóa riêng tư mới có thể truy cập các dữ liệu bên trong blockchain.
- Tích hợp hợp đồng thông minh: hợp đồng thông minh là một giao thức blockchain cần thiết cho phép các nhà phát triển mã hóa thỏa thuận các điều khoản, các điều khoản sẽ được thực thi bởi các bên liên quan mà không thể ngăn cản hoặc hủy bỏ.
- Tính bất biến: Một khi dữ liệu đã được ghi vào trong block của blockchain thì nó không thể bị thay đổi hoặc sửa chữa.

Với những tính năng cơ bản trên của blockchain thì trong quản lý văn bằng, chứng chỉ giáo dục đào tạo các tính năng của Blockchain mang lại một số lợi ích sau:

- Tính bảo mật: gồm bảo vệ dữ liệu, quyền riêng tư và tính toàn vẹn của dữ liệu liên quan đến văn bằng, chứng chỉ người học như bảng điểm, thông tin cá nhân, chương trình đào tạo.
- Tính kiểm soát: kiểm soát tốt về cách truy cập vào dữ liệu liên quan đến văn bằng, chứng chỉ của người học bởi ai.
- Tính giải trình và minh bạch: bất kỳ thay đổi nào trong blockchain cũng sẽ bị ghi nhận từ đó giảm thiểu nguy cơ chỉnh sửa dữ liệu học tập, văn bằng, chứng chỉ
- Nâng cao niềm tin: khi văn bằng, chứng chỉ được triển khai trên blockchain thì sẽ đảm bảo thiết lập được sự tin cậy giữa tất cả các bên và cũng dễ dàng truyền tải thông tin giữa các bên.
- Giảm chi phí: giảm chi phí phát sinh trong in ấn, bảo quản văn bằng, chứng chỉ; giảm chi phí trong tra cứu, xác minh văn bằng, chứng chỉ
- Xác thực: văn bằng, chứng chỉ của người học được lưu trữ trong mỗi cơ sở giáo dục và một phần được chia sẻ với các cơ quan quản lý (cơ sở giáo dục đại học, đơn vị quản lý và các đơn vị sử dụng lao động). Không dễ để các bên liên quan khác có thể tiếp cận được những thông tin này. Sự đồng thuận phân tán cho phép các tổ chức cộng tác và lưu trữ thông tin giống nhau trên một nền tảng duy nhất và do đó, dễ dàng cung cấp thông tin đó cho những bên quan tâm.
- Tính liên thông và hỗ trợ ra quyết định: với dữ liệu học tập của người học được lưu trữ bền vững, minh bạch và toàn vẹn giữa các hệ thống, người học có thể có dữ liệu tham khảo chính xác để lựa chọn ngành nghề phù hợp với năng lực bản thân.

Nội dung này đã trả lời cho câu hỏi nghiên cứu 1 là công nghệ blockchain có thể mang lại những lợi ích gì cho quản lý văn bằng, chứng chỉ.

B. Các nghiên cứu liên quan

Ý tưởng trong quản lý văn bằng, chứng chỉ (từ cấp phát đến tra cứu, xác minh) bằng cách sử dụng blockchain đã được quan tâm mạnh mẽ trên toàn cầu, từ châu Á, châu Âu

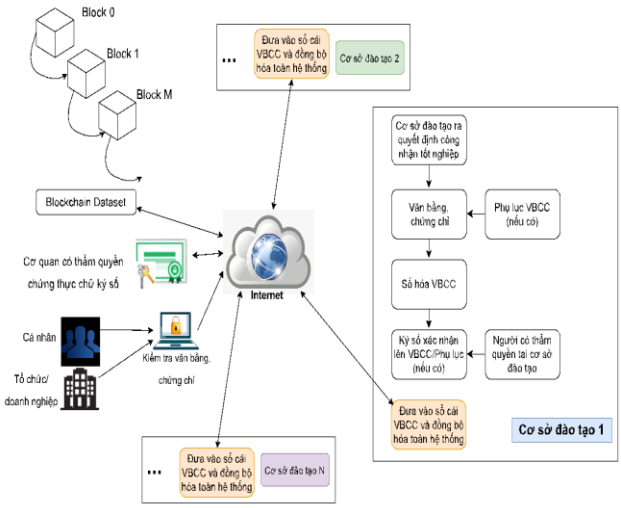
đến châu Mỹ [28]. Một số nghiên cứu tiêu biểu như Kumutha và cộng sự [17] trình bày phân tích, đánh giá về ứng dụng của blockchain trong lĩnh vực giáo dục đào tạo. Kết quả nghiên cứu cho thấy việc triển khai công nghệ blockchain trong các hệ thống giáo dục, đào tạo dựa trên chuỗi khối Ethereum. Điều này cho thấy rõ ràng rằng sự cần thiết của blockchain riêng tư Hyperledger fabric [29] trong lĩnh vực giáo dục đào tạo để xác thực văn bằng, chứng chỉ. Cùng hướng tiếp cận, Vidal và cộng sự [16] đã trình bày kết quả thảo luận việc sử dụng công nghệ blockchain nhằm đánh giá những lợi ích mà công nghệ blockchain mang lại đối với văn bằng, chứng chỉ. Ngoài ra, Nguyễn Đức Hiệp và cộng sự [14] đã giới thiệu giải pháp CVSS, là hệ thống hỗ trợ phát hành chứng chỉ kỹ thuật số bền vững. Hệ thống bao gồm 4 thành phần như quy trình đăng ký KYC, cấp chứng chỉ, xác minh và truy xuất. CVSS cho phép người dùng bao gồm tổ chức phát hành (ví dụ: tổ chức đào tạo) và người xác minh (ví dụ: nhà tuyển dụng) thực hiện các hoạt động một cách chính xác, nhanh chóng, tiết kiệm chi phí và hiệu quả trong quản lý chứng chỉ số. Hệ thống đã được thử nghiệm tại tại Trung tâm Kỹ thuật Máy tính, Đại học Bách khoa – Đại học quốc gia Thành phố Hồ Chí Minh, kết quả đạt được cho thấy tính thích hợp khi áp dụng hệ thống trong quản lý văn bằng và chứng chỉ. Tuy nhiên, nghiên cứu này sử dụng công nghệ blockchain của Ethereum để phát hành các chứng chỉ kỹ thuật số bất biến, nên nó cần được cải tiến liên tục vì những thiếu sót của Ethereum như khả năng mở rộng và chi phí hoạt động, ngoài ra hệ thống này không cung cấp tốc độ và đánh giá sự dễ dàng cần thiết cho việc cung cấp dữ liệu kịp thời.

Bên cạnh đó, Nguyễn Bình Minh và cộng sự [15] trình bày giải pháp quản lý chứng chỉ sinh viên tại Việt Nam, gọi là VECefblock, là hệ thống xác thực chứng chỉ đảm bảo độ tin cậy của dữ liệu và cung cấp các ưu điểm như ngăn chặn văn bằng, chứng chỉ giả mạo, hỗ trợ tính năng toàn vẹn cho dữ liệu được lưu trữ. Hệ thống bao gồm các quy trình nghiệp vụ, cấu trúc ánh xạ dữ liệu và ứng dụng phi tập trung, theo cách đáp ứng yêu cầu cụ thể của Việt Nam. Hệ thống được phát triển trên nền tảng Hyperledger Fabric blockchain, được định cấu hình và triển khai trên dịch vụ Amazon EC2, trong đó sử dụng chứng minh nhân dân là duy nhất đại diện cho danh tính của sinh viên. Tuy nhiên nghiên cứu này không đánh giá, phân tích khả năng thử tải, thời gian phản hồi tối đa và thời gian phản hồi tối thiểu. Theo hướng tiếp cận này, Đỗ Bá Lâm và cộng sự [18] đã trình bày nghiên cứu về ứng dụng công nghệ blockchain riêng tư cho giáo dục đào tạo nhằm xác minh và quản lý dữ liệu học tập suốt đời, gọi là B4E (Blockchain for Education). B4E không chỉ lưu trữ chứng chỉ mà còn lưu trữ dữ liệu đào tạo của người học vĩnh viễn như bảng điểm, chương trình đào tạo để tạo ra hồ sơ đầy đủ về quá trình học tập suốt đời của mỗi người dùng, cũng như xác minh các chứng chỉ mà họ đã đạt được. Ngoài ra, B4E cung cấp thêm một lớp xác thực thông qua mối liên kết giữa lịch sử đào tạo và văn bằng, chứng chỉ đạt được của người học.

Qua đánh giá những nghiên cứu trên có thể thấy, các nghiên cứu, giải pháp đã hướng tới ứng dụng blockchain trong quản lý văn bằng, chứng chỉ nhưng mới chỉ dừng ở việc bảo đảm các tính năng của blockchain hiệu quả trong quản lý văn bằng, chứng chỉ theo Thông tư 21/2019/TT-BGDĐT. Tuy nhiên, yếu tố pháp lý được quan tâm nghiên cứu hoặc chưa được thể hiện rõ ràng đối với văn bằng, chứng chỉ thì cần đảm bảo theo Nghị định 30/2020/NĐ-CP [30]. Bên cạnh đó, liên quan đến giao dịch số thì ngoài chữ ký số còn có thể kể đến hợp đồng thông minh (Smart Contract), nhưng hiện nay về mặt pháp luật thì hình thức hợp đồng thông minh chưa được thừa nhận về giá trị pháp lý. Do vậy, điểm khác biệt trình bày trong đề xuất của nhóm nghiên cứu là mô hình giải pháp quản lý văn bằng, chứng chỉ ứng dụng công nghệ blockchain và chữ ký số chính là tích hợp chữ ký số được cung cấp bởi Ban cơ yếu Chính phủ vào toàn bộ quy trình quản lý văn bằng, chứng chỉ. Phương pháp đề xuất được giới thiệu trong phần tiếp theo của bài báo.

III. GIẢI PHÁP ĐỀ XUẤT

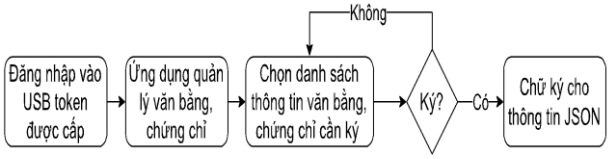
Để giải quyết các vấn đề nêu trên, bài báo đề xuất mô hình ứng dụng Blockchain và chữ ký số trong quản lý văn bằng, chứng chỉ. Mô hình quản lý văn bằng, chứng chỉ được minh họa cụ thể trong hình 2. Mô hình đề xuất bao gồm các bước sau:



Hình 2: *Tổng quan mô hình đề xuất quản lý văn bằng, chứng chỉ*

Bước 1. Ký số sao y bản scan văn bằng, chứng chỉ:

Để đảm bảo tính toàn vẹn và chống chối bỏ của dữ liệu trước khi đưa lên blockchain, hay còn gọi là tính pháp lý trong công tác xác thực theo đúng Nghị định số 30/2020/NĐ-CP của Chính phủ thì hệ thống cung cấp giải pháp ký số vào bản scan văn bằng, chứng chỉ và dữ liệu thông tin văn bằng, chứng chỉ dạng JSON (JavaScript Object Notation). Để thực hiện ký số, người dùng sẽ được cung cấp một ứng dụng ký số sử dụng chữ ký số của Ban Cơ yếu Chính phủ để lựa chọn chứng thực thư và tệp tin cần thực hiện ký. Ứng dụng được xây dựng dựa trên các công cụ, trình điều khiển và trình tự tuân thủ theo tài nguyên được cung cấp chính thức của Ban Cơ yếu Chính phủ.



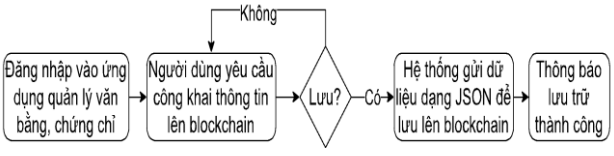
Hình 3: *Ký số bản sao chụp văn bằng, chứng chỉ*

Bước 2. Ký số với thông tin dữ liệu của văn bằng dạng JSON

Việc ký số với thông tin dữ liệu văn bằng dạng JSON được thực hiện tương tự như với ký số tệp tin. Chuẩn ký số được sử dụng là JWS (JSON Web Signature) [31]. JWS là sản phẩm của nhóm chuyên viên kỹ thuật Internet (IETF) và hoàn thành vào tháng 05 năm 2015 trong RFC 7515. Tài liệu được đánh giá công khai và được phê duyệt đề xuất bản bởi khối chỉ đạo kỹ thuật Internet (IESG). JWS hay JSON Web Signature là một dạng chữ ký có tác dụng xác minh chính trong JWT được viết với ngôn ngữ JavaScript Object Notation (JSON) trên nền tảng web. Về mặt kỹ thuật JWS đại diện cho nội dung được ký số hoặc MACed bằng cách sử dụng cấu trúc dữ liệu JSON và mã hóa base64url. Các cấu trúc dữ liệu JSON này có thể chứa khoảng trắng hoặc ngắt dòng trước hoặc sau bất kỳ giá trị JSON hoặc ký tự cấu trúc nào, phù hợp với định dạng dữ liệu của JSON được viết chi tiết trong RFC 7159 [RFC7159]. JWS đại diện cho các giá trị logic này: JOSE Header, JWS Payload, JWS Signature.

Bước 3. Lưu trữ trên Blockchain

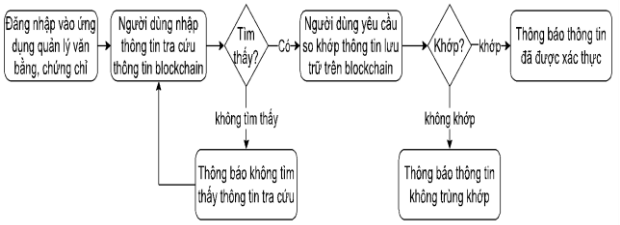
Để đảm bảo tính công khai, minh bạch của thông tin văn bằng, tất cả các nội dung bản scan văn bằng, chứng chỉ và thông tin dữ liệu sau khi ký số đều trên được lưu trữ dựa trên công nghệ Blockchain và cho phép tra cứu công khai. Mô hình giải pháp đề xuất sử dụng công nghệ Hyperledger Fabric blockchain để xây dựng mạng lưới blockchain, chạy các hợp đồng thông minh. Fabric CA được sử dụng để kết nạp thành viên trong mạng. Explorer để cho phép người dùng theo dõi hoạt động trên mạng. Hệ thống cho phép tiếp nhận dữ liệu dưới dạng JSON để đảm bảo hỗ trợ được bất kỳ các dạng biểu mẫu thông tin văn bằng, chứng chỉ nào do cơ sở đào tạo cấp. Để đưa thông tin lên blockchain khi có yêu cầu từ quản trị hệ thống, hệ thống quản lý văn bằng sẽ thực hiện giao tiếp với blockchain thông qua API. Sau khi dữ liệu được đưa lên thành công, người dùng có thể theo dõi, tra cứu công khai thông tin văn bằng theo ID và các giao dịch liên quan đến văn bằng trên mạng. Khi có bất kỳ thay đổi nào đến liên quan đến thông tin văn bằng, chứng chỉ dẫn đến không trùng khớp dữ liệu đã lưu trên blockchain thì hệ thống sẽ đưa ra cảnh báo các giao dịch này đều được ghi lại để đảm bảo tính minh bạch. Luồng lưu trữ thông tin lên blockchain được mô tả như hình 4.



Hình 4: *Sơ đồ lưu thông tin JSON lên blockchain*

Bước 4. Tra cứu văn bằng, chứng chỉ

Khi tra cứu thông tin quá trình phát hành văn bằng được thể hiện bằng giao dịch (tx) cụ thể kèm ngày giờ và tham chiếu trong sổ cái Explore, bảo đảm tính toàn vẹn và không sửa, xóa lịch sử cấp phát văn bằng chứng chỉ bằng blockchain. Sinh viên, ứng viên và các nhà tuyển dụng lao động có thể kiểm tra, tìm kiếm bằng QR Code hay bằng họ tên, mã văn bằng. Thông tin tìm được bảo đảm tính pháp lý bằng chữ ký số và bảo đảm tính toàn vẹn của lịch sử cấp phát văn bằng chứng chỉ bằng blockchain. Ngoài ra bản lưu trữ này có thể xác thực bằng các phần mềm của nước ngoài như Acrobat, Foxit… Ngoài ra, một trong những điểm mới của mô hình đề xuất giải pháp là việc phát triển hệ thống ký số trực tiếp theo lô và trên dữ liệu dạng JSON theo chuẩn thế giới RFS7515 mà hiện tại Việt Nam chưa đưa vào sử dụng. Việc sử dụng chuẩn thế giới RFS7515 trong ký số JSON giúp các cơ sở đào tạo có thể xác thực cả nội dung các phụ lục của văn bằng.



Hình 5: *Sơ đồ tra cứu thông tin trên blockchain*

Với phương nêu trên đã trả lời được câu hỏi nghiên cứu 2 là giải pháp nào để đảm bảo tính pháp lý trong quản lý văn bằng, chứng chỉ. Kết quả thử nghiệm mô hình đề xuất được trình bày trong phần tiếp theo.

IV. THỬ NGHIỆM VÀ ĐÁNH GIÁ

Mục đích của phần này là thử nghiệm, đánh giá và cho thấy tiềm năng của việc ứng dụng công nghệ blockchain và chữ ký số trong việc xác thực, tra cứu văn bằng, chứng chỉ. Do đó các kết quả thử nghiệm được triển khai trên cluster gồm 02 máy tính, trong đó máy tính thực hiện quản lý văn bằng, chứng chỉ cài đặt hệ điều hành Ubuntu 18.04, có cấu hình CPU 24 vCPU, RAM 64GB, HDD 250 GB với Bandwidth 200MBs; máy tính thực hiện blockchain có cấu hình CPU 12 core 24 thread, RAM 16GB, HDD 317GB. Để đơn giản, chúng tôi giả định tất cả các thực thể đều có cấu hình giống nhau cho tất cả PC.

Trước hết, chúng tôi đánh giá hiệu suất tính toán bằng cách triển khai các thuật toán mật mã, cụ thể là hàm băm và lược đồ chữ ký số. Chúng tôi sử dụng SHA256 để triển khai hàm băm có đầu ra thông báo có độ dài 32 bytes và tóm tắt kết quả hiệu suất trong Bảng 1.

Bảng 1. *Hiệu suất băm*

Kích thước mục dữ liệu (Kilobyte)	0.5	1	10	100	1000
Băm một mục dữ liệu (ms)	0.012	0.025	0.24	1.7225	8.679

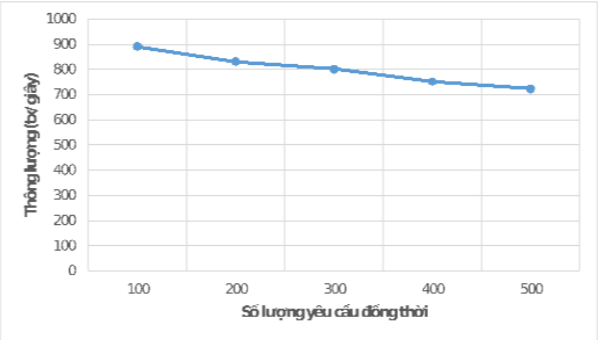
Để tính toán chi phí cho giải pháp đề xuất, chúng tôi giả sử có 100 văn bằng, chứng chỉ được xử lý và mỗi văn bằng chứng chỉ có 22 thuộc tính. Chúng tôi giả sử rằng mỗi thuộc tính có thể được biểu thị với 10 Kilobyte dữ liệu và mỗi giá trị salt có độ dài 32 bytes. Chúng tôi đánh giá chi phí cho từng giai đoạn và tóm tắt kết quả cuối cùng trong Bảng 2.

Bảng 2. *Tổng hợp hiệu suất tính toán (ms)*

	Cấp phát văn bằng	Xác thực văn bằng	Người dùng
Tạo văn bằng	25.21	0	13.54
Sử dụng văn bằng	0	1.15	1.32
Xác thực văn bằng	0	9.87	0

- Sinh văn bằng, chứng chỉ: với mỗi văn bằng, chứng chỉ cấp phát cần 1.32 ms để chuẩn bị cho dữ liệu văn bằng, chứng chỉ và cần 13.54 ms để ký văn bằng, chứng chỉ. Với người dùng, cần 13.54 ms để ký văn bằng, chứng chỉ của họ.
- Xác minh văn bằng, chứng chỉ. Trong giai đoạn này, trình xác minh văn bằng, chứng chỉ cần tính giá trị băm cho nút gốc của cây thuộc tính văn bằng, chứng chỉ. Chi phí tính toán này được giới hạn trên 1.32 ms. Hơn nữa, người phát hành văn bằng, chứng chỉ cần xác minh chữ ký, bằng cách dành 8.55 ms.

Bên cạnh đó, chúng tôi tiến hành thử nghiệm khác nhau để tính toán tốc độ và thời gian phản hồi của mạng blockchain đối với các hoạt động đọc dữ liệu (hay gọi là quá trình xác thực). chúng tôi sử dụng công cụ JMeter để đo khả năng đọc dữ liệu trên mạng blockchain. Trong thử nghiệm này, chúng tôi tạo đồng thời yêu cầu đọc các giao dịch trong vòng một phút. Thử nghiệm được lặp lại 10 lần để nhận các giá trị trung bình. Hình dưới mô tả rằng TPS giảm nhẹ từ 890 xuống 721 tx/s khi số lượng yêu cầu đồng thời tăng từ 100 lên 500. Tốc độ đọc đồng thời giảm do dung lượng của mỗi nút mạng bị hạn chế; do đó yêu cầu đến sau sẽ phải xếp hàng đợi để được phục vụ.



Hình 6: *Thông lượng cho đọc dữ liệu*

V. KẾT LUẬN

Có thể nói, việc làm giả văn bằng, chứng chỉ không phải là một vấn đề mới và các văn bằng, chứng chỉ giả đang là một trong những vấn nạn gây bức xúc trong dư luận xã hội, ảnh hưởng nghiêm trọng đến người sử dụng lao động. Để góp phần ngăn chặn, hỗ trợ hiệu quả với hình thức vi phạm này, bên cạnh sự vào cuộc quyết liệt của các lực lượng chức năng trong công tác kiểm tra, quản lý thì người dân cần nâng cao ý thức, không mua bán, sử dụng các loại giấy tờ, bằng cấp giả. Tuy nhiên, nếu chỉ mong chờ vào việc nâng cao ý thức của người dân thì sẽ khó đạt được hiệu quả triệt để, do đó việc ứng dụng công nghệ chuỗi khối và chữ ký số vào quản lý văn bằng, chứng chỉ là cần thiết. Bài báo này đã trình bày mô hình ứng dụng hiệu quả blockchain và chữ ký số trong giáo dục đào tạo, cụ thể là quản lý văn bằng, chứng chỉ. Bên cạnh đó, kết quả thử nghiệm với cơ sở đào tạo lớn như Học viện Công nghệ Bưu chính viễn thông đã cho thấy khả năng hoạt động và tính khả thi của mô hình đề xuất trong thực tế. Trong tương lai, chúng tôi sẽ tiếp tục đánh giá các thành phần dựa trên blockchain để kiểm tra hiệu suất của blockchain và khả năng hoạt động của các dịch vụ blockchain với quy mô nhiều cơ sở giáo dục đào tạo trong việc quản lý văn bằng, chứng chỉ cũng như các tác vụ khác (quản lý thông tin cá nhân, sơ yếu lý lịch khoa học, …).

TÀI LIỆU THAM KHẢO

[1] W.D.Patrick, Natural sciences citations and references. “Tapscott, A., & Tapscott, D. (2017). How blockchain is changing finance. Harvard Business Review, 1(9), 2-5.”

[2] “Hyvärinen, H., Risius, M., & Friis, G. (2017). A blockchain-based approach towards overcoming financial fraud in public sector services. Business & Information Systems Engineering, 59(6), 441-456.”

[3] “Alketbi, A., Nasir, Q., & Talib, M. A. (2018, February). Blockchain for government services—Use cases, security benefits and challenges. In 2018 15th Learning and Technology Conference (L&T) (pp. 112-119). IEEE.”

[4] “Mahankali, S., & Chaudhary, S. (2020). Blockchain in education: a comprehensive approach–utility, use cases, and implementation in a university. In Blockchain Technology Applications in Education (pp. 267-293). IGI global.”

[5] “Mettler, M. (2016, September). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom) (pp. 1-3). IEEE.”

[6] “Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and sustainable energy reviews, 100, 143-174.”

[7] “Rajnak, V., & Puschmann, T. (2021). The impact of blockchain on business models in banking. Information Systems and e-Business Management, 19(3), 809-861.”

[8] “UNESCO, 2022, Higher education global data report (Summary). A contribution to the World Higher Education Conference 18-20 May 2022.”

[9] “Ngăn chặn nạn bằng giả và tình trạng ‘chạy’ bằng cấp. Nhân Dân. Truy cập tại: http:// nhandan.com.vn/ giaoduc/tin-tuc/item/ 33377202-ngan-chan-nan-bang-gia-va-tinh-trang-chay-bangcap.html (ngày truy cập 20/8/2022).”

[10] “Bằng đại học giả tung hoành, người bán kẻ mua nhộn nhịp. Truy cập tại: https://laodong.vn/ phong-su/ bang-dai-hoc-gia-tung-hoanh-nguoi-ban-ke-mua-nhon-nhip-613842.ldo (truy cập ngày 20/8/2022).”

[11] “Gresch, J., Rodrigues, B., Scheid, E., Kanhere, S. S., & Stiller, B. (2018, July). The proposal of a blockchain-based architecture for transparent certificate handling. In International Conference on Business Information Systems (pp. 185-196). Springer, Cham.”

[12] "Serranito, D., Vasconcelos, A., Guerreiro, S., & Correia, M. (2020, September). Blockchain ecosystem for verifiable qualifications. In 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) (pp. 192-199). IEEE."
[13] "Nguyen, D. H., Nguyen-Duc, D. N., Huynh-Tuong, N., & Pham, H. A. (2018, December). CVSS: a blockchained certificate verifying support system. In Proceedings of the Ninth International Symposium on Information and Communication Technology (pp. 436-442)."
[14] "Nguyen, B. M., Dao, T. C., & Do, B. L. (2020). Towards a blockchain-based certificate authentication system in Vietnam. PeerJ Computer Science, 6, e266."
[15] "Vidal, F. R., Gouveia, F., & Soares, C. (2020). Blockchain application in higher education diploma management and results analysis. Adv. Sci. Technol. Eng. Syst, 5, 871-882."
[16] "Kumutha, K., & Jayalakshmi, S. (2021). The Impact of the Blockchain on Academic Certificate Verification System-Review. EAI Endorsed Transactions on Energy Web, 8(36), e11-e11."
[17] "Do, B. L., Nguyen, V. T., Dinh, H. N., Dao, T. C., & Nguyen, B. (2022). Blockchain for Education: Verification and Management of Lifelong Learning Data. COMPUTER SYSTEMS SCIENCE AND ENGINEERING, 43(2), 591-604.".
[18] "Ban hành quy chế quản lý bằng tốt nghiệp trung học cơ sở, bằng tốt nghiệp trung học phổ thông, bằng tốt nghiệp trung cấp sư phạm, bằng tốt nghiệp cao đẳng sư phạm, văn bằng giáo dục đại học và chứng chỉ của hệ thống giáo dục quốc dân. Truy cập tại: https://moet.gov.vn/van-ban/vanban/Pages/chi-tiet-van-ban.aspx?ItemID=1328."
[19] "Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260."
[20] "Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? Future internet, 10(2), 20."
"Kamišalić, A., Turkanović, M., Mrdović, S., & Heričko, M. (2019, April). A preliminary review of blockchain-based solutions in higher education. In International workshop on learning technology for education in cloud (pp. 114-124). Springer, Cham."
[21]
[22] "Delgado-von-Eitzen, C., Anido-Rifón, L., & Fernández-Iglesias, M. J. (2021). Blockchain Applications in Education: A Systematic Literature Review. Applied Sciences, 11(24), 11811."
[23] "Swan, M. (2015). Blockchain: Blueprint for a New Economy. 'O'Reilly Media, Inc.'."
[24] "Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2018, April). Blockchain and smart contract for digital certificate. In 2018 IEEE international conference on applied system invention (ICASI) (pp. 1046-1051). IEEE."
[25] "Capece, G., Levialdi Ghiron, N., & Pasquale, F. (2020). Blockchain technology: redefining trust for digital certificates. Sustainability, 12(21), 8952."
[26] "Hameed, B., Khan, M. M., Noman, A., Ahmad, M. J., Talib, M. R., Ashfaq, F., ... & Yousaf, M. (2019). A review of Blockchain based educational projects. International Journal of Advanced Computer Science and Applications, 10(10)."
[27] "Castro, R. Q., & Au-Yong-Oliveira, M. (2021). Blockchain and higher education diplomas. European Journal of Investigation in Health, Psychology and Education, 11(1), 154-167."
[28] "Ghani, R. F., Salman, A. A., Khudhair, A. B., & Aljobouri, L. (2022). Blockchain-based student certificate management and system sharing using hyperledger fabric platform. Periodicals of Engineering and Natural Sciences (PEN), 10(2), 207-218."
[29] "Nghị định về công tác văn thư. Truy cập tại https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Nghi-dinh-30-2020-ND-CP-cong-tac-van-thu-436532.aspx (ngày 20/9/2022)."
[30] "Jones, M., Bradley, J., & Sakimura, N. (2015). JSON web signature (JWS) (No. rfc7515)."

BUILDING AN APPLICATION MODEL OF BLOCKCHAIN AND DIGITAL SIGNATURES IN THE MANAGEMENT OF DIPLOMAS AND CERTIFICATES IN VIETNAM

Abstract: Trading and using fake diplomas and certificates has been a problem of the society in the context of strong development of science and technology. Agencies and organizations are all facing this dilemma in times of recruitment, holding exams to improve qualifications or considering studying abroad. It is alarming that just in the past few years, there have been tens of thousands of fake diplomas and certificates that have been detected and handled by the authorities. This problem is solved by using blockchain technology with the ability to be decentralized, distributed, secure, fast processing, transparent and unmodifiable. The features are superior to current technologies to combat fraud and forgery of diplomas and certificates. However the major limitation in Vietnam today is that blockchain is not clearly regulated by law, so there is increasing pressure to ensure the legality and authenticity of diplomas and certificates. In this paper, the research team presents a model of a diploma and certificate authentication solution based on the application of Blockchain technology and digital signatures to solve the above problem. The proposed model is experimented on data of diplomas and certificates of the Institute of Posts and Telecommunications Technology to evaluate the performance of the model and the obtained results show positive efficiency and the model can be applied in the management of diplomas and certificates.

Keywords: *Blockchain; Digital signatures; Certificate; Diploma.*

Nguyễn Quỳnh Chi tốt nghiệp đại học chuyên ngành Công nghệ thông tin loại giỏi tại đại học Bách Khoa, Hà nội, Việt nam năm 1999, nhận bằng Thạc sĩ chuyên ngành Khoa học máy tính tại Đại học California, Hoa Kỳ năm 2004 và nghiên cứu sinh Tiến sĩ Khoa học máy tính từ năm 2004 đến 2008, cũng tại Đại học California, Hoa Kỳ. Lĩnh vực nghiên cứu liên quan tới kho dữ liệu và ứng dụng các phương pháp học máy và khai phá dữ liệu để giải quyết các bài toán trong thực tế