Nhận 23/11, 2017, duyệt 29/12, 2017, công bố ngày 05/1, 2018, ngày hiệu lực 28/2, 2018.
Đối tượng định danh số 10.1109/ACCESS.2018.2789929

EduCTX: Nền tảng tín chỉ giáo dục đại học dựa trên Blockchain

EduCTX: A Blockchain-Based Higher Education Credit Platform

MUHAMED TURKANOVIC®, MARKO HOLBL®, KRISTJAN KOSIC,
MARJAN HERICKO, AND AIDA KAMISALIC®
Khoa Kỹ thuật điện và khoa học máy tính, Đại học Maribor, 2000 Maribor, Slovenia

Công trình này được Cơ quan Nghiên cứu Slovenia hỗ trợ (Kinh phí nghiên cứu cơ bản) theo Grant P2-0057.

Sưu tầm và dịch thuật: Ts. Mai Văn Tỉnh, Cố vấn Viện Công nghệ OFE Việt Nam

Lời giới thiệu của người dịch: *Công nghệ Blockchain (BC) mới xuất hiện hơn 1 thập kỷ qua với 3 thế hệ: BC1.0 liên quan tiền ảo Bitcoin; BC2.0 liên quan Etherium với khái niệm Hợp đồng thông minh; và mới nhất là BC 3.0 có thế mạnh xuất sắc của xa lộ thông tin tốc độ cao, tự động hóa và bảo mật cao nhằm chống các hành vi gian lận. Nền tảng CSE30 của các nhà khoa học Việt Nam được thế giới chính thức công nhận đã và đang làm thay đổi mọi phong cách sống và làm việc của chúng ta trong mọi lĩnh vực cuộc sống. Công trình nghiên cứu EduCTX: nền tảng tín chỉ đào tạo đại học của các nhà khoa học trường đại hoc Maribor Slovenia đã mô tả khái quát hiện trạng xu thế ứng dụng BC vào giáo dục ở châu Âu và một số nước trên thế giới. Mặc dù mới chỉ dừng ở mức độ ứng dụng BC1.0 và BC 2.0, kết hợp sử dụng phần mềm mã nguồn mở trên GitHub, bài học kinh nghiệm của Slovenia sẽ giúp chúng tôi - các nhà nghiên cứ ứng dụng công nghệ BC trong giáo dục đại học (GDĐH) ở Việt Nam, hiểu được rõ hơn bức tranh ứng dung công nghệ BC vào hệ thống kết nối nút mạng để chuyển đổi số, công nhận giá trị tín chỉ học thuật giữa các cơ sở GDĐH ở các nước Đông Âu cũ và khu vực châu Âu. Xin trân trọng giới thiệu cùng bạn đọc.*

TÓM TẮT

Công nghệ Blockchain cho phép tạo ra một môi trường phi tập trung, nơi các giứ ba nào. Bất kỳ giao dịch nào đã từng được hoàn thành đều được ghi lại ao dịch và dữ liệu không nằm dưới sự kiểm soát của bất kỳ tổ chức bên thtrong sổ cái công khai theo cách có thể xác minh và vĩnh viễn. Dựa trên công nghệ blockchain, chúng tôi đề xuất một nền tảng tín chỉ giáo dục đại học toàn cầu, có tên là EduCTX. Nền tảng này dựa trên khái niệm của Hệ thống Tích lũy và Chuyển đổi Tín chỉ Châu Âu (ECTS). Nó tạo thành một hệ thống tín chỉ giáo dục đại học phi tập trung và đáng tin cậy trên toàn cầu, có thể đưa ra quan điểm thống nhất toàn cầu cho sinh viên và các cơ sở giáo dục đại học (HEI), cũng như cho các bên liên quan tiềm năng khác, chẳng hạn như các công ty, nhà trường và tổ chức. Như một bằng chứng về khái niệm, chúng tôi trình bày một triển khai nguyên mẫu của môi trường, dựa trên Nền tảng chuỗi khối Ark mã nguồn mở. Dựa trên mạng đồng đăng được phân phối toàn cầu, EduCTX sẽ xử lý, quản lý và kiểm soát các mã thông báo ECTX, đại diện cho các khoản tín chỉ mà sinh viên đạt được cho các khóa học đã hoàn thành, chẳng hạn như ECTS. HEI là các đồng đẳng của mạng blockchain. Nền tảng này là bước đầu tiên hướng tới một hình thức hệ thống giáo dục đại học minh bạch hơn và công nghệ tiên tiến hơn. Nền tảng EduCTX đại diện cho cơ sở của sáng kiến EduCTX, dự đoán rằng các cơ sở GDĐH khác nhau sẽ hợp lực để tạo ra một môi trường hiệu quả, đơn giản hóa và phổ biến trên toàn cầu nhằm tránh các rào cản về ngôn ngữ và hành chính. Do đó, chúng tôi mời và khuyến khích các cư sở GDĐH tham gia sáng kiến EduCTX và mạng lưới blockchain EduCTX.

• **Từ khóa:** Blockchain, giáo dục đại học, ECTS, mã thông báo.

I. GIỚI THIỆU

Dựa trên khái niệm của Hệ thống tích lũy và chuyển đổi tín chỉ châu Âu (ECTS), chúng tôi đề xuất một nền tảng tín chỉ giáo dục đại học dựa trên blockchain toàn cầu, có tên là EduCTX. Hệ thống được đề xuất sẽ khai thác các lợi ích của blockchain, như một kiến trúc phi tập trung, cung cấp bảo mật, ẩn danh, tuổi thọ, tính toàn vẹn, minh bạch, bất biến và đơn giản hóa hệ sinh thái toàn cầu, để tạo ra một hệ thống chấm điểm và tín chỉ giáo dục đại học đáng tin cậy trên toàn cầu. Như một bằng chứng về khái niệm, chúng tôi sẽ trình bày một bản mẫu thử nghiệm của nền tảng, dựa trên Nền tảng chuỗi khối Ark nguồn mở [1].

Đóng góp khoa học là cung cấp một mô hình kiến trúc phân tán và liên thông cho hệ thống tín chỉ giáo dục đại học nhằm giải quyết quan điểm thống nhất toàn cầu cho sinh viên và các tổ chức nhà trường. Các nhà tuyển dụng tiềm năng có thể hưởng lợi từ hệ thống được đề xuất.

Sinh viên có thể tận dụng lợi thế của việc xem lịch sử khóa học đã hoàn thành của họ trong một chế độ xem duy nhất và minh bạch, cũng như các trường đại học có dữ liệu này có thể truy cập và cập nhật, bất kể nguồn gốc học vấn của sinh viên. Mặt khác, các tổ chức khác nhau (chẳng hạn như nhà tuyển dụng, đơn vị học nghề, v.v.) với tư cách là người dùng tiềm năng của hệ thống, có thể xác thực thông tin được cung cấp sau khi được sự cho phép của sinh viên.

Cấu trúc của văn bản như sau. Phần hiện tại trình bày chi tiết về động lực và những đóng góp của bài báo. Các công trình liên quan trình bày các dự án và nghiên cứu quan trọng trong lĩnh vực liên quan đến nghiên cứu này, trong khi phần Cơ sở giới thiệu nền tảng và sơ lược của công trình. Đóng góp chính của bài báo được trình bày trong các phần triển khai Nền tảng EduCTX Pro¬posed và Nguyên mẫu. Phần Nền tảng EduCTX được đề xuất sẽ trình bày chi tiết khái niệm được đề xuất của nền tảng, trong khi việc triển khai Nguyên mẫu bao gồm các phần kỹ thuật, ví dụ như áp dụng, hoạt động, ví dụ thực tế, v.v. Một số phản ánh và vấn đề của công việc được mô tả chi tiết trong phần Thảo luận. Cuối cùng, phần Kết luận và công việc Tương lai cung cấp một bản tóm tắt về giải pháp được đề xuất và một số kế hoạch trong tương lai.

A. ĐỘNG LỰC

Phần lớn các cơ sở GDĐH (HEI) lưu giữ hồ sơ khóa học mà sinh viên của họ đã hoàn thành trong theo các định dạng thích hợp. Các cơ sở dữ liệu này được cấu trúc để nhân viên của tổ chức truy cập độc quyền và trong các hệ thống trực tuyến chuyên dụng, do đó có rất ít hoặc không có khả năng tương tác. Hơn nữa, phần lớn các nhà trường có hệ thống chuyên biệt của riêng họ để lưu giữ hồ sơ khóa học đã hoàn thành của sinh viên, hệ thống này bảo vệ trước cấu trúc dữ liệu độc quyền của cơ sở dữ liệu. Nói chung, các cơ sở dữ liệu này được lưu trữ trong một trung tâm dữ liệu bên trong cơ sở GDĐH, với quyền truy cập hạn chế đối với các chuyên gia CNTT của nó. Sinh viên có thể có quyền truy cập bên ngoài vào dữ liệu của họ theo cách hạn chế, được bảo vệ bằng mật khẩu, chỉ để xem hoặc in hồ sơ khóa học đã hoàn thành của họ (một số hệ thống cho phép và ghi lại các bài kiểm tra đăng ký và trả phòng trực tuyến của sinh viên). Có một số điểm quan trọng liên quan đến các hệ thống như vậy, bao gồm chuẩn hóa dữ liệu, vị trí lưu trữ, an toàn và cách lọc, phân tích và chia sẻ dữ liệu đó một cách an toàn. Liên quan đến những vấn đề này, các cơ sở GDĐH duy trì hồ sơ khóa học đã hoàn thành của sinh viên vô thời hạn. Điều này là bắt buộc vì lý do pháp lý, tùy thuộc vào chính sách của quốc gia. Cũng trong phần lớn các trường hợp, các cơ sở giáo dục không chia sẻ dữ liệu học viên của họ, thậm chí không chia sẻ hồ sơ khóa học đã hoàn thành. Do đó, sinh viên có thể gặp khó khăn khi chuyển sang Trường khác, trong khi vẫn bảo toàn và chứng minh sự hoàn thành của các khóa học từ cơ sở trước đó. Vấn đề này thậm chí còn sống động hơn trong trường hợp một sinh viên muốn chuyển đến một quốc gia khác, nơi tồn tại rào cản ngôn ngữ, chữ viết và hành chính. Hơn nữa, những hồ sơ này thường được lưu trữ theo các chuẩn khác nhau, điều này gây khó khăn

cho việc trao đổi hồ sơ giữa các cơ sở GDĐH.Trong trường hợp sinh viên nộp đơn cho một vị trí công việc và phải chứng minh bằng cấp học tập của mình ở nước ngoài, các xác suất phát sinh từ việc lưu trữ tập trung toàn bộ hồ sơ khóa học của sinh viên do không thể truy cập, thiếu tiêu chuẩn hóa, v.v.

Sinh viên phải dịch và viết chứng chỉ học tập của họ, đây có thể là một quá trình phức tạp và tốn nhiều thời gian. Quá trình xác minh bao gồm việc dịch tất cả các tài liệu chính thức sang ngôn ngữ của tổ chức nhà trường lưu trữ, quá trình này phải xem xét và xác thực mọi khía cạnh của tài liệu để kiểm tra nội dung phù hợp hoặc khác biệt.

Hơn nữa, sau khi hoàn thành chương trình học, sinh viên đôi khi không có quyền truy cập vào hệ thống chấm điểm học tập trực tuyến. Trong trường hợp như vậy, nếu một sinh viên bị mất chứng chỉ học tập của mình, họ cần phải đến tận cơ sở GD DH tại quê nhà của họ và yêu cầu một bản sao mới, đây có thể là một quá trình tốn kém và mất thời gian.

Mặc dù có một số chuẩn hợp nhất cho hệ thống tín chỉ học thuật như ECTS, việc áp dụng và triển khai một nền tảng tín chỉ an toàn, đáng tin cậy và phi tập trung toàn cầu là một thách thức. Nhiều trở ngại đến từ thực tế là học bạ của học sinh rất nhạy cảm và có nhiều quy định quản lý phức tạp.

B. **SỰ ĐÓNG GÓP**

Chúng tôi đề xuất một nền tảng tín chỉ giáo dục đại học phi tập trung dựa trên blockchain, có tên là EduCTX. Nó được xây dựng trên hệ thống mạng đồng đẳng (P2P) được phân bổ. Các hệ thống này linh hoạt, an toàn và có khả năng phục hồi vì khả năng lưu trữ và chia sẻ tài nguyên trên quy mô toàn cầu [2]. Nền tảng EduCTX chuyển hệ thống chấm điểm và tín chỉ giáo dục đại học từ thế giới tương tự và vật lý sang một phiên bản phổ biến, đơn giản hóa, hiệu quả trên toàn cầu, dựa trên công nghệ blockchain. Nền tảng EduCTX là nền tảng của sáng kiến EduCTX của chúng tôi (có thêm thông tin tại: eductx.org), dự kiến một hệ thống chấm điểm và tín chỉ giáo dục đại học thống nhất, đơn giản hóa và phổ biến trên toàn cầu. Thông qua sáng kiến này, chúng tôi có kế hoạch tiến xa hơn và phát triển khái niệm EduCTX.

II. **CÁC CÔNG TRÌNH LIÊN QUAN**

Công nghệ chuỗi khối nhằm mục đích tạo ra một môi trường phi tập trung, nơi không có bên thứ ba nào kiểm soát các giao dịch và dữ liệu [3]. Nó được sử dụng trong một số lĩnh vực do lợi ích của nó trong việc lưu trữ dữ liệu phân tán và khả năng kiểm tra các dấu vết.Trong lĩnh vực chăm sóc sức khỏe, một số phương pháp tiếp cận đã được giới thiệu trong lĩnh vực hồ sơ sức khỏe điện tử (EHR) [4] - [10]. Thử nghiệm lâm sàng hoặc truy cập dữ liệu và quản lý quyền là những lĩnh vực mà công nghệ có thể được áp dụng [7], [10]. Có liên quan mật thiết đến EHRs là khả năng tương tác, nơi các blockchains cũng đã được sử dụng [6], [8]. Một số tác giả thậm chí còn tuyên bố rằng nó có thể cách mạng hóa lĩnh vực chăm sóc sức khỏe [9]. Họ đưa ra các ví dụ như quản lý chăm sóc sức khỏe cộng đồng và thông minh, có thể mang lại lợi ích cho bệnh nhân, bằng cách sử dụng công nghệ blockchain để chống thuốc giả trong ngành dược phẩm.

Tuy nhiên, chăm sóc sức khỏe chỉ là một trong những lĩnh vực ứng dụng blockchain khả thi. Do tính minh bạch của công nghệ, các lĩnh vực chính phủ và doanh nghiệp cũng cố gắng áp dụng công nghệ và thu được lợi ích của nó [11] - [15]. Blockchain được áp dụng trong các kịch bản chính phủ điện tử [11], chính phủ thông minh [13], v.v. Trong lĩnh vực kinh doanh nảy sinh các khái niệm và hệ thống mới (ví dụ: hệ thống tiền điện tử, quy trình kinh doanh, v.v.) [16] - [18].

Ngay cả trong lĩnh vực hậu cần và vận chuyển, công nghệ blockchain cũng có thể được áp dụng

[19], [20]. Bằng cách này, các hệ thống giao thông thông minh mới được phát triển. Ngoài ra, sản xuất, quản lý và kinh doanh năng lượng có thể thúc đẩy các lợi ích của blockchain [21] - [23]. Lưới thông minh và các công nghệ thông minh khác nhau có thể sử dụng công nghệ để tối ưu hóa hoạt động của chúng [23] và các cơ hội kinh doanh mới có thể được phát triển [22].

Ngay cả trong lĩnh vực mới nổi của Internet of Things (IoT), công nghệ blockchain có thể được sử dụng trong các kịch bản và hình thức khác nhau [15], [17], [24] - [28]. Chúng bao gồm việc quản lý quyền riêng tư và bảo mật của IoT [26], [28], cũng như sự phát triển của các kịch bản và cơ hội kinh doanh mới [25].Bản chất linh hoạt của công nghệ bockchain được chứng minh bằng các ứng dụng linh hoạt trong nhiều lĩnh vực [29] - [31].

Công nghệ blockchain cũng có thể được áp dụng trong GDĐH. Một số cơ sơ GDĐH đã sử dụng công nghệ blockchain để thiết kế các giải pháp và phương pháp tiếp cận khác nhau liên quan đến giáo dục đại học. Phần lớn các giải pháp sử dụng chuỗi khối Bitcoin [32], [33]. NazarAf và cộng sự. đã đề xuất một nền tảng để tạo, chia sẻ và xác minh chứng chỉ giáo dục dựa trên blockchain trong phạm vi của Dự án chứng chỉ kỹ thuật số. Dự án ươm tạo này dựa trên chuỗi khối Bitcoin và được dẫn dắt bởi Sáng kiến Học tập Phòng thí nghiệm Truyền thông tại Viện Công nghệ Massachusetts (MIT). Cách tiếp cận này giải quyết các vấn đề về số hóa chứng chỉ học thuật và không điều tra khả năng blockchain được sử dụng trong nền tảng chấm điểm và tín chỉ giáo dục đại học toàn cầu.

Đại học Quốc gia La Plata (UNLP) đã bắt đầu phát triển một khung để xác minh dựa trên blockchain về thành tích học tập [32], [34], [35], nhưng không có chi tiết nào khác được tiết lộ cho đến ngày hôm nay [33]. Phương pháp tương tự cũng được trường Cao đẳng Argentina CESYT áp dụng [36]. Cả hai giải pháp đều sử dụng công nghệ blockchain và mật mã (nghĩa là chữ ký số, tem thời gian, v.v.) để cấp bằng tốt nghiệp cho sinh viên. Tuy nhiên, cách tiếp cận của họ không giải quyết vấn đề các khoản tín chỉ được tích lũy cho các thành tích học tập nhiều hơn. Cách tiếp cận chỉ tập trung vào việc cấp văn bằng chứng chỉ bằng cách sử dụng blockchain bitcoin (BC1.0- ND nhấn).

Vào năm 2016, Trường Kỹ thuật Leonardo da Vinci ở Paris (ESILV) đã thông báo rằng họ sẽ chứng nhận các văn bằng trên blockchain bitcoin [37]. Họ đã hợp tác với công ty khởi nghiệp Bitcoin Paymium của Pháp, nhưng không có thêm chi tiết hoặc mẫu thử nghiệm nào được công bố cho đến nay. Ngoài ra còn có các cơ sở GDĐH khác, có hoặc có ý định sử dụng công nghệ blockchain. Vào năm 2015, một trường kỹ thuật phần mềm ở San Francisco, Holberton School, đã công bố sử dụng công nghệ này để giúp các nhà tuyển dụng xác minh văn bằng học thuật [38].

Hầu hết các dự án nói trên trong lĩnh vực GDĐH dựa trên các khái niệm hoặc ý tưởng khép kín và thường không thảo luận chi tiết hoặc thậm chí chỉ dừng lại ở mức độ ý tưởng. Một số dự án liên quan được cung cấp độc quyền cho một vòng kết nối khép kín của các thực thể. Ngược lại, ý tưởng được trình bày trong bài báo này dựa trên các công nghệ mã nguồn mở (tức là mã nguồn mở công khai của việc triển khai) và nó nhằm mục đích kết hợp các bên liên quan toàn cầu vào sáng kiến EduCTX, và do đó, nó được mở cho sự tham gia và đưa vào bất kỳ cơ sở GDĐH nào thông qua một nền tảng có sẵn công khai và sự hiện diện trên web. Nền tảng được trình bày dựa trên công nghệ blockchain ARK và việc triển khai nguyên mẫu có sẵn thông qua nền tảng phát triển phần mềm GitHub. Do đó, nền tảng blockchain EduCTX được đề xuất là cơ sở của sáng kiến EduCTX, được mở trên toàn cầu cho tất cả các cơ sở GDĐH để xây dựng một giải pháp hiệu quả, đơn giản, phổ biến cho việc cấp tín chỉ đào tạo cho sinh viên, đồng thời loại bỏ các trở ngại về ngôn ngữ và hành chính.

III. **BỐI CẢNH**
A. HỆ THỐNG CHUYỂN ĐỔI VÀ TÍCH LŨY TÍN CHỈ CHÂU ÂU

Hệ thống chuyển đổi và tích lũy tín chỉ châu Âu (ECTS) là một khung cho hệ thống chấm điểm GD ĐH do Ủy ban châu Âu phát triển và được các nước thành viên EU đồng ý chấp nhận. Nó được thành lập vào năm 1989 trong chương trình Erasmus (trao đổi sinh viên). Mục tiêu của hệ thống lấy người học làm trung tâm này là tạo điều kiện thuận lợi cho việc lập kế hoạch, phân phối và đánh giá các chương trình học cũng như tạo điều kiện thuận lợi cho việc di chuyển của sinh viên bằng cách công nhận thành tích học tập, trình độ, kinh nghiệm và thời gian học tập trước đó [39]. Tín chỉ ECTS thể hiện khối lượng học tập dựa trên kết quả học tập xác định và khối lượng công việc liên quan đến việc học. Kết quả học tập được thể hiện dưới dạng kiến thức của một cá nhân (những gì họ biết, hiểu và có thể làm), trong khi khối lượng công việc là thời gian ước tính mà một cá nhân cần để hoàn thành tất cả các hoạt động học tập. Kết quả học tập và khối lượng công việc liên quan của một năm học toàn thời gian được đánh giá bằng 60 tín chỉ ECTS. Tín chỉ được thể hiện bằng số nguyên. Xem xét kết quả học tập dự kiến và khối lượng công việc ước tính, số lượng tín chỉ khác nhau được chỉ định cho các cấu phần giáo dục khác nhau (các khóa học). Một tín chỉ tương ứng với 25 đến 30 giờ làm việc [39].

B**. BLOCKCHAIN - CÔNG NGHỆ LEDGER PHÂN TÁN**

Một Blockchain có thể được coi là một cơ sở dữ liệu phân tán, lưu trữ theo thứ tự thời gian một chuỗi dữ liệu được đóng gói thành các khối niêm phong [4] một cách an toàn và bất biến. Chuỗi khối, còn được gọi là sổ cái (ledger), không ngừng phát triển, do đó các khối mới đang được nối vào cuối sổ cái, theo đó mỗi khối mới giữ một tham chiếu (chính xác hơn là giá trị băm) cho nội dung của khối trước đó [40]. Nội dung của các khối có thể được xác định trước hoặc được tạo ngẫu nhiên bởi người dùng của blockchain. Tuy nh ớc của blockchain và được niêm phong bằng đồ họa tiền điện tử [41]. Tuy nhiên, dữ liệu được cấu trúc thành các giao dịch được gọi là theo cấu trúc được xác định trước của blockchain và được niêm phong bằng đồ họa tiền điện tử [41].

Có ba loại blockchain chính: (1) công khai - không được phép, (2) riêng tư - được cấp phép và (3) chuỗi khối kết hợp. Loại blockchain không được phép nhấn mạnh vào phần công khai, do đó tất cả dữ liệu blockchain đều có thể truy cập và hiển thị cho công chúng. Tuy nhiên, một số phần của blockchain có thể được mã hóa để bảo vệ tính ẩn danh của người tham gia [43]. Hơn nữa, trong các loại blockchain công khai này, mọi người đều có thể tham gia mạng với tư cách là một nút mạng. Ví dụ về một chuỗi khối như vậy là chuỗi khối Bitcoin và Ethereum. Ngược lại, một blockchain riêng tư chỉ cho phép các nút được chọn tham gia vào mạng, do đó được coi là một dạng của mạng phân tán nhưng vẫn tập trung [43]. Chuỗi khối liên hợp là sự kết hợp của cả hai và chỉ cho phép một nhóm các nút được chọn tham gia vào quá trình đồng thuận phân tán [43].

1) **SỰ ĐỒNG THUẬN ĐƯỢC PHÂN TÁN**

Vì blockchain là một cơ sở dữ liệu giống sổ cái phân tán nằm trên mạng P2P, nên mỗi mạng ngang hàng giữ một bản sao của trạng thái sổ cái đã xác nhận và một nhóm dữ liệu chưa được xác nhận cần được đóng gói thành các khối và thêm vào sổ cái. Để mạng lưới blockchain duy trì hoạt động, các đồng nghiệp cần đồng ý về một trạng thái nhất định của nội dung sổ cái và về cách đóng gói dữ liệu thành các khối. Điều này đạt được bằng một giao thức đồng thuận phân tán, giao thức này xác nhận thứ tự thời gian của dữ liệu được tạo ra [43]. Giao thức đồng thuận phân tán đảm bảo rằng một số lượng lớn các đồng nghiệp mạng blockchain đồng ý về trạng thái chính xác của sổ cái được chia sẻ, do đó thứ tự các khối mới được thêm vào sổ cái [41]. Một số thuật toán đồng thuận phân tán được sử dụng là bằng chứng công việc (PoW), bằng chứng cổ phần (PoS), bằng chứng cổ phần được ủy quyền (DPoS), bằng chứng quan trọng, bằng chứng hoạt động, bằng chứng - của cháy, bằng

chứng ký gửi, v.v. [41], [43], [45]. Tiếp theo, chúng tôi trình bày chi tiết về PoW và PoS, các cách tiếp cận được sử dụng phổ biến nhất để đạt được sự đồng thuận trong một chuỗi khối.Ý tưởng cơ bản của các giao thức đồng thuận phân tán là thống nhất về một người đồng đẳng/ngang hàng sẽ chuẩn bị và niêm phong khối mới nhất với dữ liệu vẫn chưa được xác nhận và chưa được giải nén. Có một số cách về cách quyết định hoặc lựa chọn đồng nghiệp đó. Cách đơn giản nhất là xác định nó một cách ngẫu nhiên, nhưng cách tiếp cận như vậy không hiệu quả về tuổi thọ mạng và thậm chí có thể gây nguy hiểm cho mạng, vì các đồng nghiệp có thể quyết định tấn công toàn bộ mạng [43]. Ý tưởng đằng sau PoW, PoS và những cái khác là thực tế rằng những người ngang hàng/đồng đẳng được chọn phải đóng góp một cái gì đó có giá trị, điều này sẽ dẫn đến sự cạnh tranh và người giỏi nhất sẽ nhận được phần thưởng, do đó giảm thiểu nguy cơ tấn công có thể xảy ra.

PoW là một giao thức đồng thuận được sử dụng trong mạng Bitcoin và nó sử dụng sức mạnh tính toán như một cơ chế để xác định đồng đẳng được chọn [3], [43], [46]. Sự cạnh tranh giữa các công ty ngang hàng dựa trên việc băm các giao dịch - dữ liệu chưa được xác nhận, do đó, cơ hội được chọn của một người ngang hàng phụ thuộc vào sức mạnh tính toán của nó. Mỗi khi một người ngang hàng chiến thắng, nó sẽ nhận được phần thưởng, về mặt mạng Bitcoin là 12,5 bitcoin mới được tạo ra được thêm vào tài khoản của nó [41]. Cạnh tranh băm (tức là khai thác) dựa trên việc tính toán một khối, chứa các giao dịch chưa được xác nhận và một số ngẫu nhiên. Yêu cầu rằng kết quả của băm phải bằng một giá trị được xác định trước. Trong trường hợp một máy ngang hàng (tức là người khai thác) đạt đến giá trị cần thiết, nó sẽ phát khối mới được tạo ra cho các máy ngang hàng khác, nhờ đó nó được xác nhận và trong trường hợp tính đúng đắn của nó sẽ được tất cả các máy ngang hàng nối vào bản sao của sổ cái phân tán [43].

Giao thức đồng thuận PoS dựa trên cổ phần của giá trị mạng mà một người ngang hàng có quyền kiểm soát (tức là tài sản của họ). Trong trường hợp này, cơ hội của một người ngang hàng được chọn trở thành người ký kết mới của một khối tương ứng với sự giàu có của khối đó, tức là cổ phần. Trên thực tế, điều này được thực hiện dưới hình thức một người ngang hàng gửi một số lượng tài sản tối thiểu được xác định trước, do đó mua một vé để nằm trong nhóm những người ngang hàng sẽ được chọn theo cách giả ngẫu nhiên xác định làm người ký khối mới. Vì sự cạnh tranh trong PoS không dựa trên sức mạnh tính toán của các công ty ngang hàng, nên sẽ không tiêu tốn năng lượng như trong trường hợp của PoW, nhưng cách tiếp cận như vậy giống như một tập đoàn cổ đông, nơi người giàu có lợi thế hơn [45]. Hơn nữa, khả năng một máy ngang hàng sẽ tấn công mạng cũng ít hơn, vì trong trường hợp này, nó sẽ tấn công tài sản của chính nó [43]. Có nhiều phiên bản của giao thức đồng thuận PoS, theo đó mỗi phiên bản giới thiệu một cách tiếp cận khác nhau về cách chọn người ký để đảm bảo tính công bằng. Một trong những phiên bản này là DPoS, theo đó sự khác biệt giữa hệ thống PoS thông thường và hệ thống DPoS có thể được so sánh với sự khác biệt giữa dân chủ trực tiếp và dân chủ đại diện, vì các bên liên quan bỏ phiếu để quyết định người ký, tức là đại biểu [43].

2) **NÚT MẠNG BLOCKCHAIN**

Để có một mạng blockchain đầy đủ chức năng, cần phải có một tập hợp các nút mạng, vì chúng là xương sống của blockchain. Vì mạng blockchain là loại mạng P2P, một nút có thể được coi là một mạng ngang hàng/đồng đẳng khi nó bắt đầu kết nối và giao tiếp với các nút khác trong mạng, do đó tên thích hợp sẽ là một nút đồng đẳng. Để thuận tiện, chúng tôi sẽ ký hiệu nó là một nút. Nói về mặt kỹ thuật, nút blockchain là bất kỳ máy tính nào được cài đặt ứng dụng khách blockchain cốt lõi và vận hành một bản sao đầy đủ của sổ cái blockchain [43], [47], [48].

Khi người dùng của một blockchain cụ thể tương tác với blockchain, họ thực sự kết nối với mạng thông qua một nút [47]. Cái gọi là thợ đào của khái niệm PoW là một tập hợp con của các nút, vì tất cả các thợ đào cũng phải vận hành một nút đầy đủ chức năng, do đó mỗi người khai thác là một nút,

nhưng không phải nút nào cũng là một thợ đào. Thực tế này cũng hiển nhiên đối với các phiên bản blockchain khác, nơi các loại đồng thuận phân tán khác được giới thiệu và không cần khai thác, ví dụ: PoS [3]. Do đó, chúng ta có thể tuyên bố rằng các nút xác định phối hợp phân tán, do đó đồng ý về một quy tắc cụ thể và blockchain hoạt động như một cơ chế đồng thuận để đảm bảo rằng các nút luôn đồng bộ [48]. Hơn nữa, trong blockchain loại PoW, một nút đơn giản không nhận được bất kỳ phần thưởng nào như một người khai thác, do đó lợi ích duy nhất khi chạy một nút là giúp bảo vệ mạng [48]. Các nhiệm vụ cơ bản của một nút blockchain là: (1) kết nối với mạng blockchain, (2) lưu trữ sổ cái cập nhật, (3) lắng nghe các giao dịch, (4) chuyển các giao dịch hợp lệ vào mạng, (5) lắng nghe các khối mới được niêm phong, (6) xác nhận các khối mới được niêm phong - xác nhậngiao dịch, và (7) tạo và chuyển các khối mới [43], [47], [48].

C. GIAO THỨC ĐA CHỮ KÝ

Giao thức đa chữ ký là một khái niệm nổi tiếng trong thế giới mật mã khóa công khai [42], [49]. Nó cho phép nhiều bên cùng ký kỹ thuật số vào một tin nhắn đã thỏa thuận, mỗi bên có khóa riêng của mình. Lựa chọn như vậy là mong muốn trong trường hợp nhiều bên phải đồng ý thống nhất, như trong trường hợp tài khoản ngân hàng chung. Ví dụ như một tài khoản ngân hàng là Số tài khoản ngân hàng quốc tế (IBAN), trong trường hợp có giao dịch đến, không yêu cầu bất kỳ hành động nào từ chủ tài khoản và hơn thế nữa, nó còn ẩn danh tính của chủ tài khoản. Ngược lại, khi thực hiện giao dịch gửi đi, mỗi chủ tài khoản phải chấp thuận trước khi ngân hàng xử lý giao dịch. Khái niệm như vậy đã là một thực tế phổ biến trong thế giới tiền điện tử, theo đó ví blockchain M-to-N có thể được tạo ra [50]. Ở đây M biểu thị số lượng người ký yêu cầu tối thiểu của một giao dịch và N biểu thị số lượng địa chỉ đầy đủ có thể có (chủ tài khoản). Một ví dụ sẽ là địa chỉ có 2-3 chữ ký, bao gồm ba bên (khóa công khai của họ) và ít nhất hai trong số đó phải ký một giao dịch từ địa chỉ nhiều chữ ký này để được xử lý. Trong thế giới tiền điện tử, việc sử dụng cách tiếp cận như vậy để thực hiện giao dịch được gọi là pay-to-script-hash (P2SH), trái ngược với các giao dịch pay-to-public-key-hash (P2PKH) thông thường, tạo điều kiện cho địa chỉ không có nhiều chữ ký.

VI. NỀN TẢNG EduCTX ĐÃ ĐỀ XUẤT

Phần này phác thảo nền tảng được đề xuất EduCTX, một tín chỉ GDĐH dựa trên blockchain và biểu mẫu chấm điểm. Mô tả trừu tượng về nền tảng ở cấp độ cao hơn được trình bày trong Hình 1. Nền tảng blockchain EduCTX được hình dung để xử lý, quản lý và kiểm soát mã thông báo ECTX dưới dạng tín chỉ học tập và nằm trên mạng P2P được đánh giá cao trên toàn cầu, nơi các đồng nghiệp của blockchain mạng là cơ sở GDĐH và người dùng nền tảng là sinh viên và các tổ chức (ví dụ: các công ty là nhà tuyển dụng tiềm năng).

Mã thông báo ECTX tương đương với giá trị tín chỉ của sinh viên cho các khóa học đã hoàn thành, cũng như với các tín chỉ ECTS mà sinh viên Châu Âu đạt được (xem phần Hệ thống tích lũy và chuyển đổi tín chỉ Châu Âu). Mỗi sinh viên sẽ giữ một ví blockchain EduCTX đã được khấu trừ, nơi họ sẽ thu thập các mã thông báo ECTX, tức là giá trị của các khoản tín chỉ được cơ sở GDĐH chỉ định cho các khóa học đã hoàn thành của họ. Mỗi khi sinh viên hoàn thành khóa học, cơ sở GDĐH tại quê nhà của họ sẽ chuyển số lượng mã thông báo ECTX thích hợp đến địa chỉ blockchain của họ. Thông tin người chuyển được lưu trữ trên blockchain, nơi dữ liệu tiếp theo được lưu trữ: (1) người gửi được xác định là trường ĐH liên quan với tên chính thức của nó, (2) người nhận - sinh viên được trình bày ẩn danh, (3) mã thông báo - giá trị tín chỉ khóa học, và (4) nhận dạng khóa học. Hơn nữa, bằng cách sử dụng địa chỉ blockchain của mình, sinh viên với tư cách là người nhận mã thông báo ECTX, sẽ có thể chứng minh toàn cầu các khóa học đã hoàn thành của mình mà không gặp bất kỳ trở ngại nào về quản trị, tập lệnh hoặc ngôn ngữ bằng cách gửi trước địa chỉ blockchain của mình. Vì lợi ích bảo mật, sinh viên sẽ được cơ sở GDĐH tại quê nhà của họ chỉ định một địa chỉ đa chữ ký 2-2, do đó họ sẽ không thể chuyển bất kỳ mã thông báo ECTX nào đạt được đến các

địa chỉ khác (xem phần Giao thức đa chữ ký). Quá trình chỉ định sinh viên có mã thông báo ECTX và khả năng chứng minh quyền sở hữu của họ sẽ được xử lý thông qua ứng dụng khách API blockchain EduCTX đơn giản để sử dụng, do đó làm cho việc sử dụng nền tảng EduCTX trực quan nhất có thể.

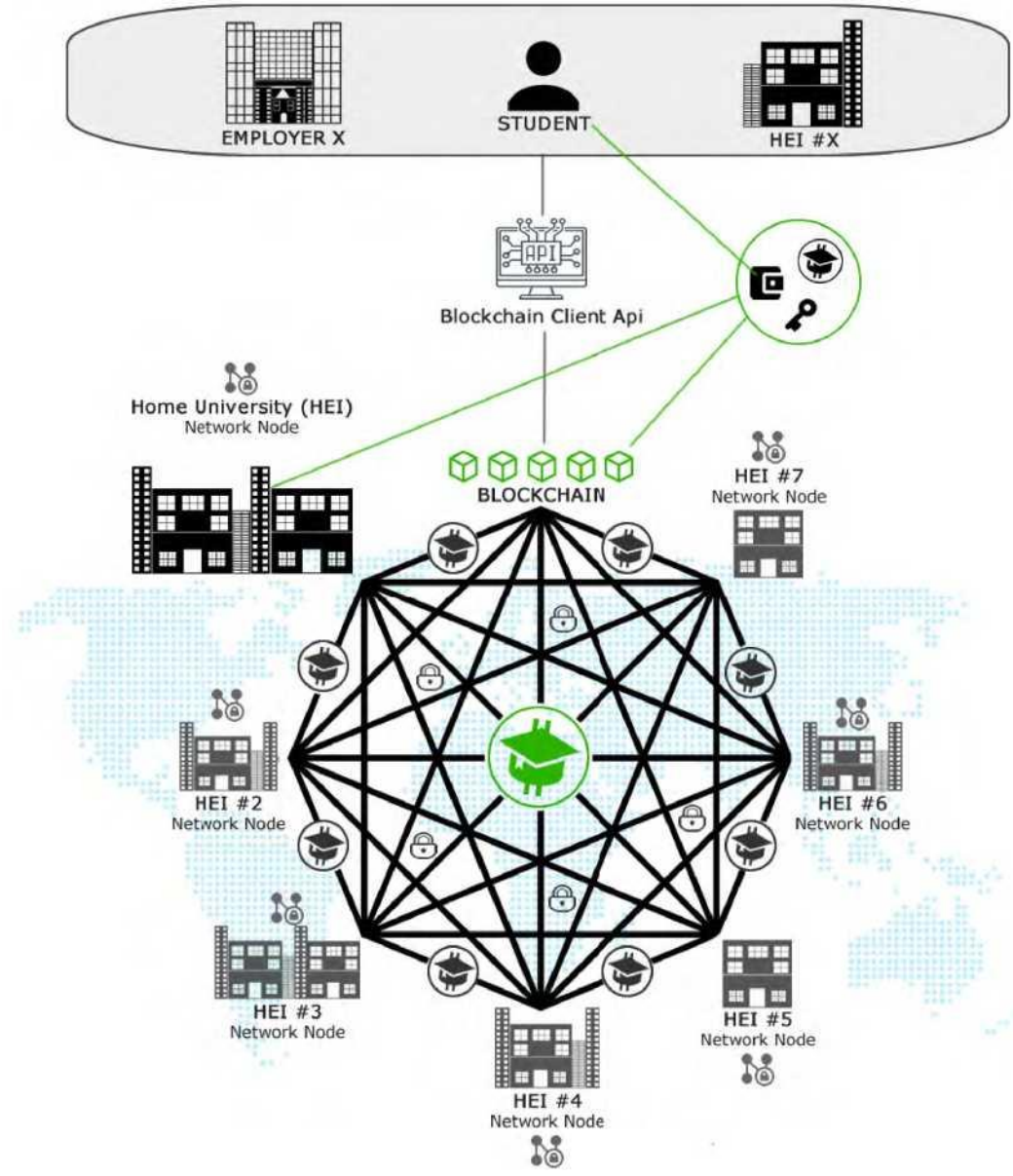
Bất kỳ cơ sở GDĐH nào cũng được kiểm định công nhận và các thành viên của họ sẽ có thể tham gia mạng lưới. Trong khi tham gia mạng, cơ sở GDĐH sẽ phải thiết lập một nút mạng (xem phần Nút mạng chuỗi khối) để duy trì cơ sở hạ tầng toàn cầu và mạng an toàn. Một nút đầy đủ chức năng sẽ phát các thông báo trên toàn mạng, đây là bước đầu tiên trong quá trình giao dịch dẫn đến xác nhận khối, do đó xác nhận chuyển tín chỉ ECTX cho các khóa học đã hoàn thành cho sinh viên. Nút cơ sở GDĐH cũng sẽ có ứng dụng khách blockchain EduCTX cốt lõi trên phiên bản máy chủ của nó với bản sao của sổ cái blockchain hoàn chỉnh. Điều này làm tăng thêm tính bảo mật, vì càng có nhiều nút, mạng càng an toàn. Cơ sở GDĐH và các nút do đó, sẽ không phải khai thác các giao dịch chuyển tiếp, vì nền tảng blockchain EduCTX sẽ dựa trên giao thức đồng thuận DPoS (xem phần Đồng thuận phân tán). Do đó, nút cơ sở GDĐH không cần đến sức mạnh tính toán. Cách tiếp cận như vậy cũng phù hợp từ khía cạnh bảo mật cho mạng EduCTX, vì các đồng nghiệp ngẫu nhiên không thể tham gia mạng và tạo mã thông báo ECTX mới bằng cách khai thác chúng. Như vậy, blockchain EduCTX có thể được xem như một phiên bản liên hợp của một blockchain (xem phần Blockchain - Công nghệ sổ cái phân tán). Mỗi cơ sở GDĐH mới tham gia mạng và được các cơ sở GDĐH thành viên khác xem xét, sẽ được gán mã thông báo ECTX và được yêu cầu thiết lập một nút mạng. Vì chúng tôi đề xuất phiên bản đồng thuận phân tán DPoS của blockchain, nên mỗi thành viên cơ sở GDĐH sẽ có thể đăng ký làm đại biểu trong nền tảng blockchain EduCTX và cộng đồng cơ sở GDĐH EduCTX sẽ bỏ phiếu cho một đại biểu, từ đó sẽ xác nhận các giao dịch và niêm phong các khối. Điều này ngụ ý rằng cộng đồng sẽ bỏ phiếu cho cơ sở GDĐH đó sẽ là người khẳng định và liên tục nhất trong công việc của mình. Để đảm bảo một phiên bản được phép của nền tảng blockchain và một cộng đồng dân chủ và phi lợi nhuận, chúng tôi dự định giảm phần thưởng giả mạo xuống 0. Trong các phần phụ sau đây, chúng tôi mô tả chi tiết bốn tình huống quan trọng sẽ diễn ra trong EduCTX. Mỗi kịch bản được sao lưu bằng biểu diễn sơ đồ Quản lý quy trình nghiệp vụ (BPM).

A. **CƠ SỞ GDĐH THAM GIA MẠNG EduCTX**

Một cơ sở GDĐH mới (sau đây gọi là cơ sở Mới) cố gắng tham gia vào mạng lưới blockchain EduCTX bằng cách sử dụng API của chúng tôi để tạo ví và địa chỉ blockchain chứa các khóa công khai và riêng tư. Cơ sở mới nên lưu trữ một cách an toàn khóa riêng. Sau khi tạo địa chỉ, nó liên hệ với một trong các cơ sở GDĐH hiện có, các thành viên của mạng blockchain EduCTX (sau đây gọi là cơ sở thành viên). Cơ sở thành viên nhận được yêu cầu đăng ký (tham gia) cơ sở GDĐH mới. Trước tiên, nó xác minh thông tin chính thức của cơ sở GDĐH mới và sau đó chuyển 1 mã thông báo ECTX đến địa chỉ blockchain của cơ sở mới. Giao dịch sau đó được xử lý thông qua mạng blockchain (để biết chi tiết tham khảo Hình 2).

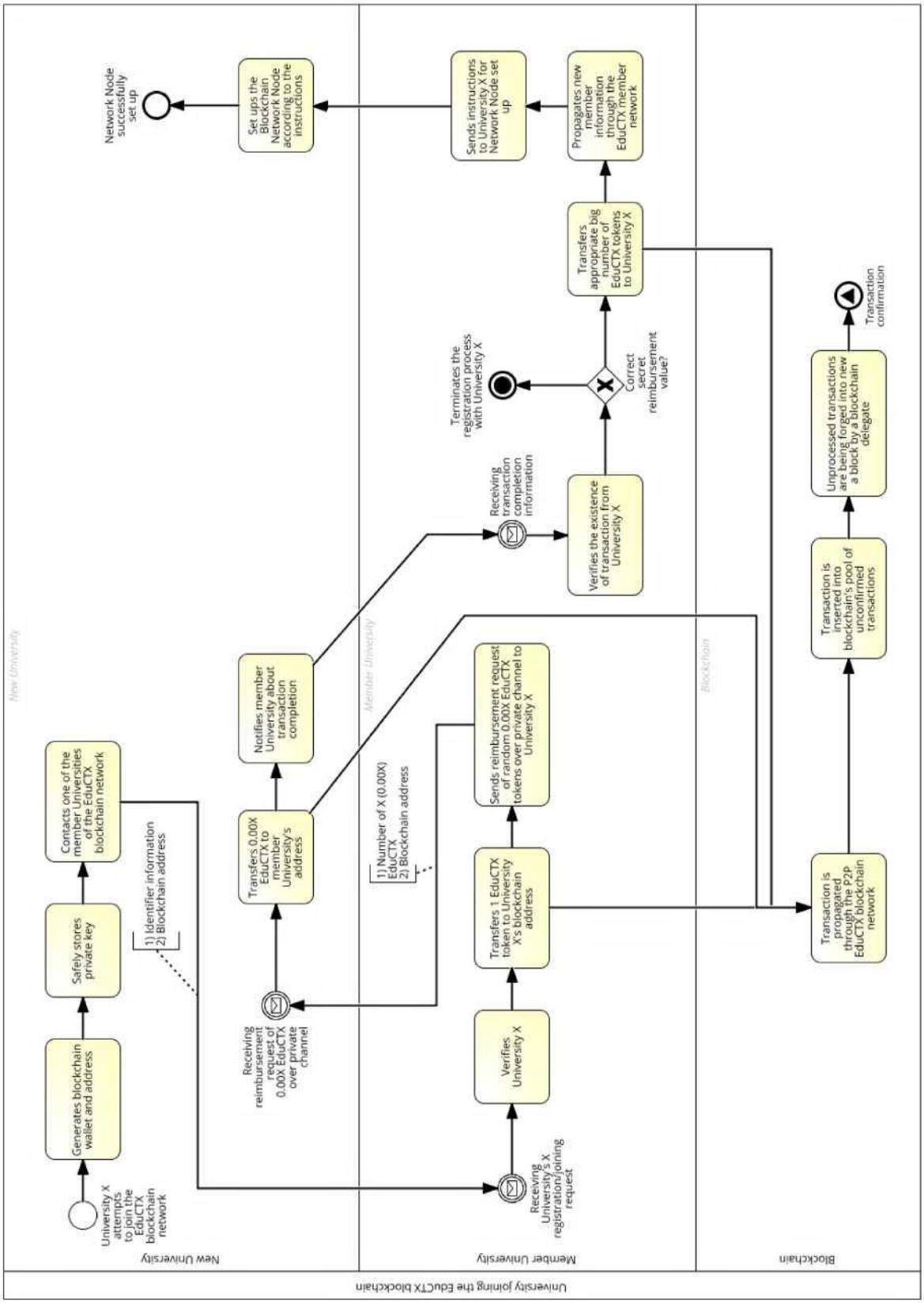
Khi giao dịch được xác nhận, cơ sở thành viên sẽ gửi yêu cầu hoàn tiền gồm các mã thông báo ECTX 0,00X ngẫu nhiên qua một kênh riêng tư tới cơ sở mới. Nó bao gồm (1) số lượng X (0,00X) EduCTX (ví dụ: 235781- nghĩa là 0,00235781 EduCTX) và (2) Địa chỉ chuỗi khối. Khi cơ sở GDĐH mới nhận được yêu cầu bồi hoàn qua một kênh riêng tư, nó chuyển 0,00X EduCTX sang địa chỉ của cơ sở thành viên (giao dịch được xử lý thông qua mạng blockchain). Sau đó, cơ sở Mới thông báo cho cơ sở thành viên sau khi giao dịch hoàn tất. Cơ sở thành viên xác minh sự tồn tại của giao dịch từ cơ sở Mới. Nếu giá trị hoàn trả bí mật không chính xác, cơ sở thành viên sẽ chấm dứt quá trình đăng ký. Nếu không, nó sẽ chuyển số lượng thích hợp Mã thông báo ECTX sang cơ sở Mới (giao dịch đang được xử lý thông qua mạng blockchain). Cơ sở thành viên tuyên truyền thông tin về cơ sở GDĐH mới thông qua mạng thành viên EduCTX và gửi hướng dẫn đến cơ sở Mới về Nút mạng

thiết lập. Cư sở GDĐH mới thiết lập nút mạng blockchain theo hướng dẫn. Sau khi nút mạng là-nghĩa là 0,00235781 EduCTX) và (2) địa chỉ chuỗi khối. Khi cơ sở GDĐH mới nhận được yêu cầu bồi hoàn qua một kênh riêng tư, nó chuyển 0,00X EduCTX sang địa chỉ của cơ sở thành viên (giao dịch được xử lý thông qua mạng blockchain). Sau đó, cơ sở Mới thông báo cho cơ sở thành viên sau



Hình 1. Mô tả mức độ cao của EduCTX platform được đề xuất.

khi giao dịch hoàn tất. Cơ sở thành viên xác minh sự tồn tại của giao dịch từ cơ sở Mới. Nếu giá trị hoàn trả bí mật không chính xác, cơ sở thành viên sẽ chấm dứt quá trình đăng ký. Nếu không, nó sẽ chuyển số lượng thích hợp Mã thông báo ECTX sang cơ sở Mới (giao dịch đang được xử lý thông qua mạng blockchain). Cơ sở thành viên tuyên truyền thông tin về cơ sở Mói thông qua mạng thành viên EduCTX và gửi hướng dẫn đến cơ sở Mới về Nút mạng thiết lập. Cơ sở Mới thiết lập nút mạng blockchain theo hướng dẫn. Sau khi nút mạng được thiết lập thành công, quá trình cơ sở Mới tham gia EduCTX blockchain đã hoàn thành. Thông tin chi tiết về mô hình quy trình cho kịch bản được mô tả được đưa ra trong Hình 2 trong BPM khóa cá nhân biểu diễn theo sơ đồ. Sau khi tạo địa chỉ, nó liên hệ với một trong các cơ sở GDĐH hiện có, thành viên của mạng blockchain EduCTX.



Hình 2. Mô hình quá trình của một cơ sở GD ĐH tham gia mạng blockchain EduCTX .

B. ĐĂNG KÝ CỦA SINH VIÊN

Khi một sinh viên đăng ký vào cơ sở GDĐH (thành viên của mạng lưới blockchain EduCTX), nó sẽ cấp thẻ sinh viên và tạo một địa chỉ blockchain mới cho sinh viên, có chứa khóa công khai và riêng tư. Ngoài ra, cơ sở GDĐH tạo một địa chỉ blockchain đa chữ ký 2-2 mới với khóa công khai và khóa công khai của sinh viên mới được tạo. Địa chỉ đa chữ ký này kết hợp với thẻ sinh viên được lưu trữ trong cơ sở dữ liệu của cơ sở GDĐH. Cơ sở GDĐH chuyển 0,1 mã thông báo ECTX đến địa chỉ blockchain đa chữ ký 2-2 của sinh viên và qua một kênh riêng cung cấp cho sinh viên thông tin cần thiết để thiết lập ví đa chữ ký blockchain. Thông tin được cung cấp bao gồm (1) hướng dẫn thiết lập ví blockchain EduCTX, (2) địa chỉ blockchain của sinh viên chứa các khóa công khai và riêng tư, (3) khóa công khai của cơ sở GDĐH và (4) tập lệnh đổi. Với thông tin nhận được, sinh viên thiết lập ví blockchain của mình và một địa chỉ duy nhất bằng cách sử dụng các khóa công khai và riêng tư nhận được từ cơ quan quản lý cơ sở GDĐH. Anh ấy/cô ấy cũng thiết lập một địa chỉ blockchain đa chữ ký 2-2 bằng cách sử dụng khóa công khai của anh ấy / cô ấy và khóa công khai của cơ sở GDĐH. Dữ liệu ví phải được lưu trữ an toàn. Sử dụng ví đa chữ ký 2-2 của mình, sinh viên tạo và ký một giao dịch gồm 0,1 mã thông báo ECTX tới địa chỉ blockchain của cơ sở GDĐH. Sau đó, cơ sở GDĐH ký giao dịch bằng khóa riêng của nó. Giao dịch được xử lý thông qua mạng blockchain. Khi giao dịch được xác nhận, cơ sở GDĐH lưu trữ thông tin trong cơ sở dữ liệu của mình, xác nhận việc tạo ví thành công của sinh viên. Hình 3 mô tả một mô hình quy trình cho kịch bản được mô tả bằng cách sử dụng biểu đồ BPM HỌC VIÊN HOÀN THÀNH KHÓA HỌC

Sau khi sinh viên làm bài kiểm tra, giáo sư cần xác minh kết quả. Anh ấy / cô ấy công bố kết quả kỳ thi. Nếu sinh viên đã thành công và nếu giáo sư có thể đăng ký từng cá nhân hoàn thành nghĩa vụ khóa học của sinh viên, thì kết quả được lưu trữ trong cơ sở dữ liệu tập trung. Nếu không, giáo sư sẽ thông báo cho văn phòng quản lý để thực hiện thủ tục cần thiết để đăng ký tình trạng nghĩa vụ của sinh viên. Các kết quả có thể được lưu trữ đồng thời trong cơ sở dữ liệu tập trung trong trường hợp cơ sở GDĐH cần giữ một hệ thống song song được điều chỉnh bởi các quy định pháp luật quốc gia và cũng như một bản sao lưu cho đến khi hệ thống blockchain EduCTX không tự chứng minh là đã được triển khai đầy đủ và chưa chạy/vận hành. Giáo sư hoặc văn phòng quản lý tìm địa chỉ blockchain của sinh viên trong cơ sở dữ liệu trung tâm, tìm số lượng ECTS mà khóa học đã đặt và sử dụng ví blockchain để chuyển lượng mã thông báo ECTX thích hợp đến địa chỉ blockchain đa chữ ký 2-2 của sinh viên. Giao dịch được xử lý thông qua mạng blockchain. Khi giao dịch được xác nhận, giáo sư hoặc văn phòng quản trị ghi lại việc chuyển mã thông báo ECTX thành công vào cơ sở dữ liệu trung tâm. Mô hình quy trình cho kịch bản được mô tả được mô tả trong Hình 4, sử dụng biểu diễn dạng sơ đồ BPM.

C. TỔ CHỨC XÁC NHẬN HỒ SƠ TÍN CHỈ CỦA SINH VIÊN

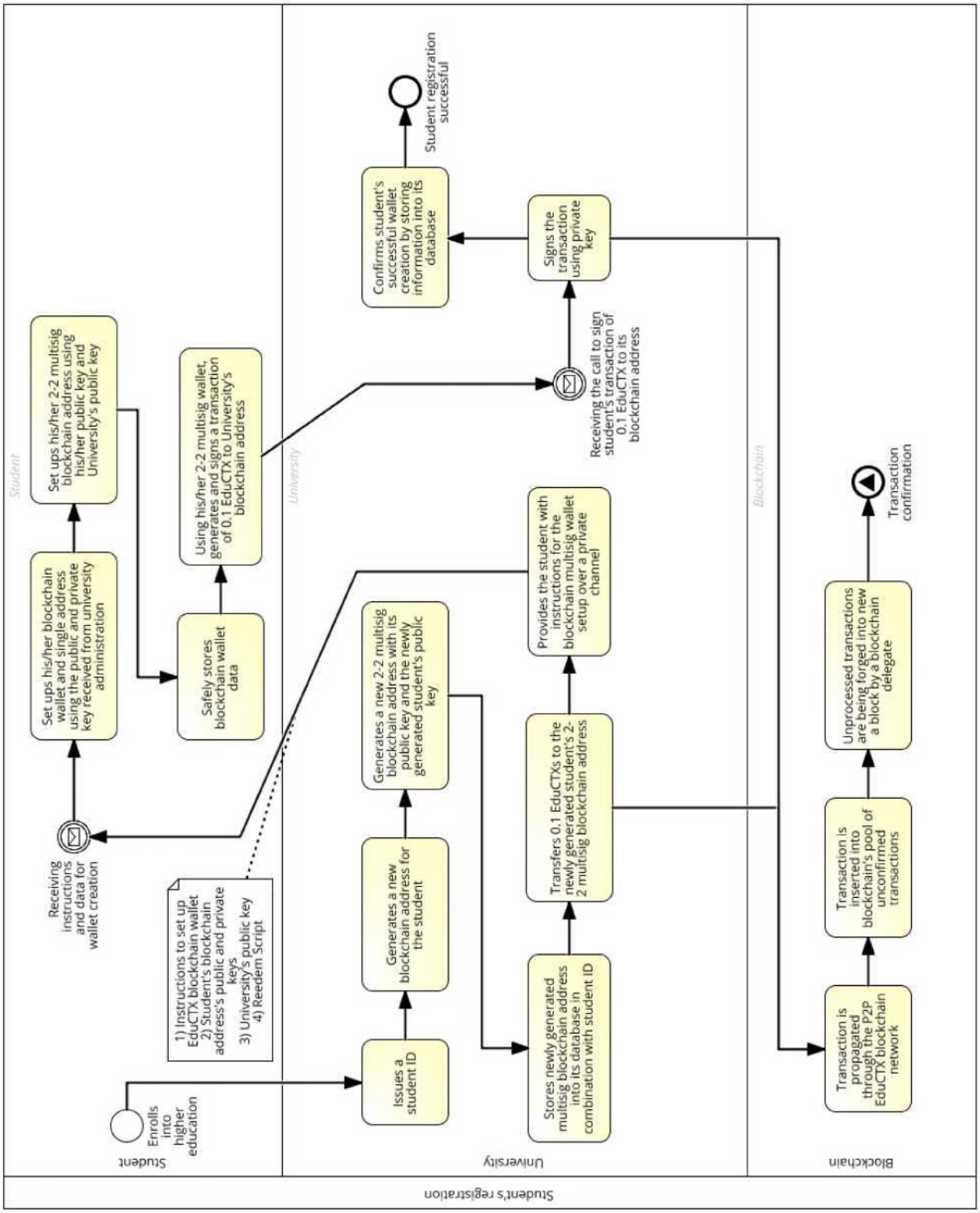
Khi một tổ chức (ví dụ: nhà tuyển dụng, trường đại học, v.v.) muốn xác minh việc hoàn thành nghĩa vụ khóa học của sinh viên, sinh viên phải gửi địa chỉ blockchain của mình, địa chỉ blockchain đa chữ ký 2-2 của mình và đổi tập lệnh cho người xác minh - tổ chức. Tổ chức kiểm tra tập lệnh đổi để xác minh địa chỉ của sinh viên và địa chỉ đa chữ ký 2-2. Sử dụng API web blockchain để truy cập dữ liệu blockchain, tổ chức kiểm tra số lượng mã thông báo ECTX trong địa chỉ đa chữ ký 2-2, đại diện cho thành tích tín chỉ học tập của sinh viên. Sau đó, thông qua một kênh riêng tư, tổ chức yêu cầu sinh viên ký một tin nhắn (ví dụ: "XYZ") với địa chỉ của mình để xác minh danh tính của mình. Khi sinh viên, sử dụng API web blockchain, ký vào thư bằng địa chỉ và khóa cá nhân của mình, anh / cô ấy sẽ thông báo cho tổ chức, người kiểm tra thư đã ký. Nếu tin nhắn đã ký được xác thực, tổ chức có thể tin tưởng rằng địa chỉ blockchain được trình bày và giá trị mã thông báo ECTS của nó thực sự là của sinh viên. Mô hình quy trình cho kịch bản được mô tả được miêu tả trong Hình 5, sử dụng biểu diễn dạng sơ đồ BPM.

V. **TRIỂN KHAI PHƯƠNG TIỆN (*PROTOTYPE*)**

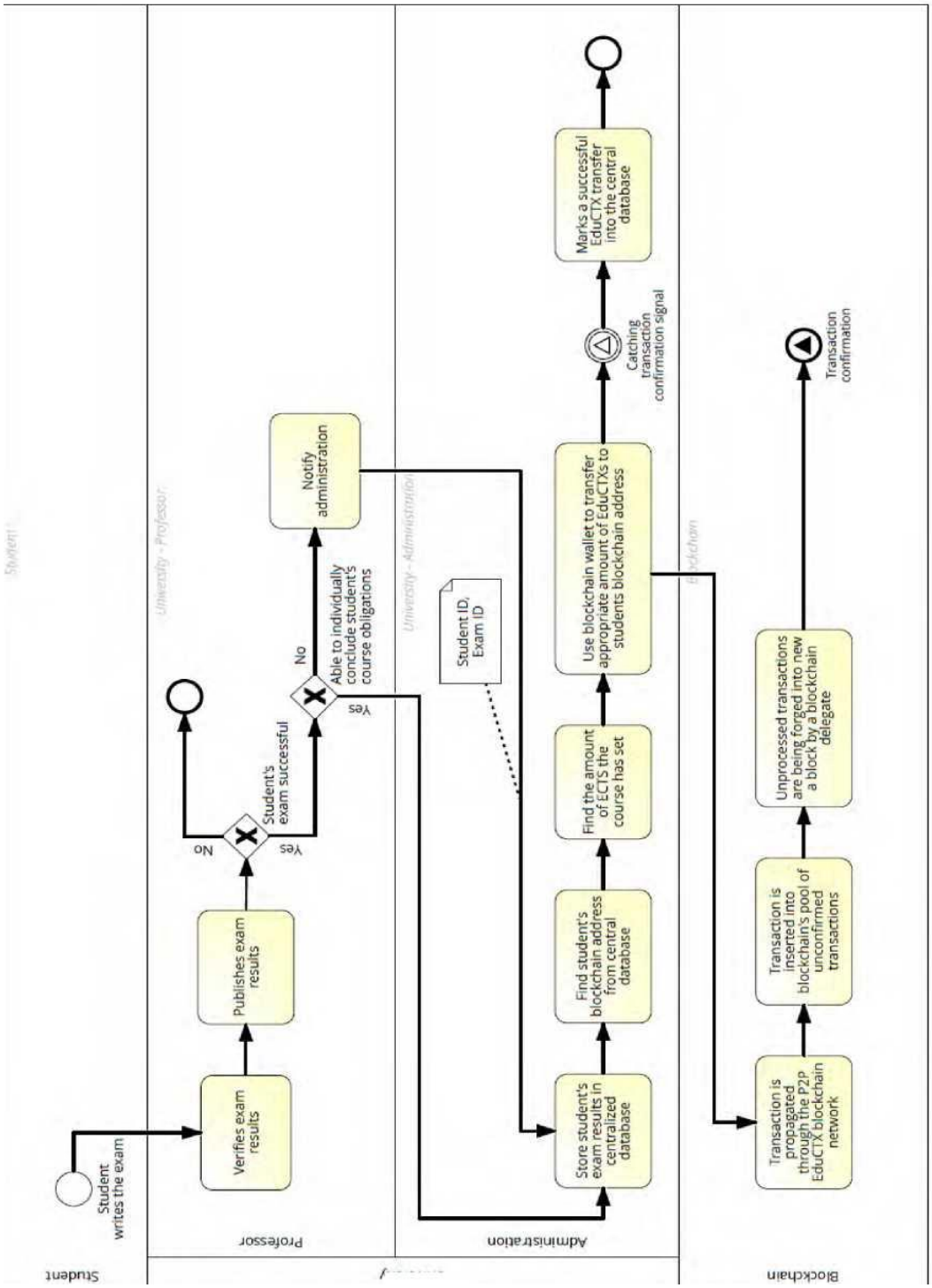
Chúng tôi đã chọn ARK Blockchain [1] làm công nghệ cơ bản của nền tảng EduCTX của chúng tôi. ARK không chỉ là một loại tiền điện tử, mà còn là một hệ sinh thái dành cho việc áp dụng hàng loạt blockchain. Bằng cách xây dựng nền tảng EduCTX trên nền tảng blockchain lõi ARK nhanh và an toàn cao, tích hợp các công nghệ phi tập trung quan trọng, nền tảng trở thành một hệ sinh thái thân thiện với người dùng ở trường đại học để tăng cường áp dụng toàn bộ công nghệ blockchain. Các lý do chính để chọn công nghệ ARK làm cơ sở mã là tính linh hoạt và nguồn mở của nó cũng như tính khả dụng tổng thể của các triển khai API ứng dụng khách. Tại thời điểm viết bài, ARK cung cấp hơn 12 ngôn ngữ lập trình khác nhau để triển khai ứng dụng khách, do đó cho phép các tác nhân khác (cơ sở GDĐH, sinh viên, nhà tuyển dụng) tham gia nền tảng bằng ngôn ngữ lập trình mà họ chọn.

A. **CÁC KHỐI XÂY DỰNG HỆ SINH THÁI EduCTX**

ARK được xây dựng để sử dụng cơ chế đồng thuận được gọi là DPoS. Mặc dù DPoS (xem phần Đồng thuận phân tán) đã được biết đến từ khá lâu, nhưng nó đã không nhận được mức độ phơi nhiễm tương tự như PoW và PoS [51]. Mô hình đồng thuận DPoS có một số khác biệt lớn khi so sánh với các mô hình PoW và PoS truyền thống. DPoS có thể được xem như một nền dân chủ đại diện, nơi người dùng cá nhân (trong trường hợp sử dụng của chúng tôi là cơ sở GDĐH) sử dụng cổ phần của họ (cổ phần, niềm tin) để đề cử các đại diện (cơ sở GDĐH khác) tham gia mạng lưới EduCTX gồm các nút đáng tin cậy (đại biểu). Các đại biểu có trách nhiệm xác thực các giao dịch và bảo mật mạng. Nếu người được ủy quyền (cơ sở GDĐH thành viên của EduCTX) thực hiện nhiệm vụ của họ kém hoặc sử dụng quyền hạn theo cách không đại diện. ARK cũng được chọn vì tính linh hoạt của nó. Nó là một blockchain không được phép, nghĩa là bất kỳ ai cũng có thể tham gia. Chúng tôi đã thích nghichuỗi khối ARK đến một chuỗi khối liên hợp bằng cách thay đổi các thông số đồng thuận DPoS của mạng.



Hình 3. **Mô hình quá trình về việc sinh viên đăng ký vào mạng blockchain EduCTX**



Hình 4. Mô hình quá trình về nghĩa vụ hoàn thành khóa học của sinh viên đã đăng ký vào mạng blockchain EduCTX

Hình 5. Mô hình quá trình của một tổ chức thẩm tra xác minh hồ sơ tín chỉ của sinh viên.

Các thành viên mạng mới chỉ có thể tham gia dựa trên thỏa thuận trước, bằng cách chứng minh danh tính của họ trong các hệ thống tập trung hiện có (ví dụ: một tuyên bố đã ký từ trưởng khoa của cơ sở GDĐH). Về tính bảo mật và tính hợp lệ của hồ sơ EduCTX trên blockchain, chúng tôi đã xác định một số quy tắc, để đảm bảo tính an toàn và hợp lệ của hồ sơ hoàn thành khóa học của sinh viên.

• Mọi sinh viên đều ẩn danh. Một sinh viên được cung cấp địa chỉ blockchain duy nhất của mình và địa chỉ này sẽ lưu trữ và nhận mã thông báo ECTX, do đó giá trị tín chỉ giống như ECTS, sẽ xác nhận việc hoàn thành các khóa học khác nhau của sinh viên.

• Sinh viên không thể gửi mã thông báo ECTX đã nhận, do đó, các khoản tín dụng giống như ECTS, đến một địa chỉ khác. Đây là địa chỉ đa chữ ký 2-2 sẽ yêu cầu chữ ký thứ hai để cho phép các giao dịch gửi đi của mã thông báo ECTX (xem Phần Giao thức chữ ký đa dạng). Một bản ký tên thứ hai được yêu cầu bởi một tổ chức được ủy quyền, nơi đã cấp địa chỉ của sinh viên, tức là cơ sở GDĐH quê nhà của họ.

• Mặc dù một sinh viên hoàn toàn ẩn danh, chúng tôi đã triển khai hệ thống chữ ký thư, có thể được sử dụng để chứng minh danh tính (quyền sở hữu) của các mã thông báo ECTX.

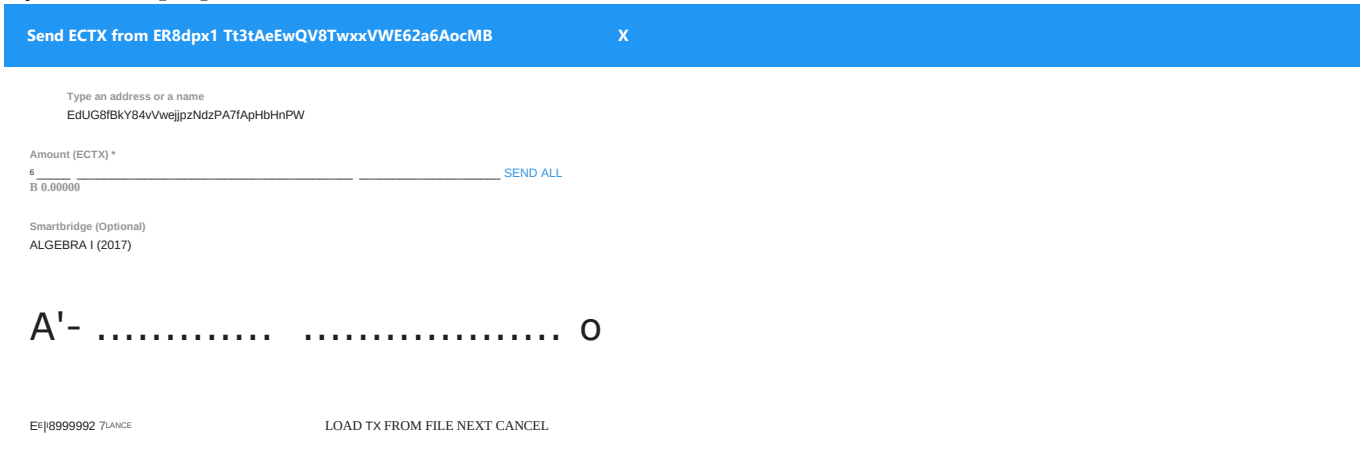
Trình khám phá blockchain EduCTX công khai đã có sẵn tại http://eductx.um.si. Trình khám phá khối EduCTX là một trình duyệt blockchain trực tuyến, hiển thị trạng thái tổng thể của mạng EduCTX (các nút ủy quyền, tính khả dụng, nội dung của các khối riêng lẻ, giao dịch, lịch sử giao dịch và số dư EduCTX của các địa chỉ).

B. THAM GIA HỆ SINH THÁI ECOSYX EduCTX

Mã EduCTX được xuất bản trên GitHub [52] và được cấp phép theo Giấy phép MIT [53]. Bất kỳ ai cũng có thể xem xét và điều chỉnh mã theo nhu cầu của riêng mình, do đó cũng đóng góp vào toàn bộ hệ sinh thái EduCTX, bằng cách chia sẻ các tính năng mới cho tất cả người dùng - đây cũng là khái niệm cơ bản của các dự án nguồn mở và sáng kiến EduCTX của chúng tôi. Chúng tôi khuyến khích và mời các cơ sở GDĐH khác tham gia, đóng góp và mở rộng khái niệm EduCTX hơn nữa.

Chúng tôi đã thiết kế EduCTX theo cách thức mô-đun (dựa trên các khối xây dựng của hệ sinh thái blockchain ARK). EduCTX có thể được tích hợp liền mạch với các hệ thống thông tin hiện có của cơ sở GDĐH. Điểm cuối của blockchain là các API REST có thể được sử dụng bởi các API ứng dụng khách đã được xuất bản và có sẵn (xem github EduCTX để biết thêm chi tiết). Để cho phép chuyển đổi suôn sẻ sang một nền tảng mới hơn, nền tảng EduCTX trước tiên có thể cùng tồn tại với các hệ thống thông tin cơ sở GDĐH hiện có. Nó không nhằm mục đích thay thế chúng hoàn toàn, vì nó cũng có thể là một vấn đề lập pháp ở các quốc gia khác nhau, nhưng cùng tồn tại và cung cấp bằng chứng hoàn thành khóa học hiệu quả, đáng tin cậy và trên hết là minh bạch và tức thì.

Là giao diện người dùng đầu tiên của hệ sinh thái EduCTX, ứng dụng khách (ví) ECTX có sẵn (xem Hình 6). Sử dụng ví, các trường đại học có thể đăng ký người dùng mới (địa chỉ dành cho sinh viên), chuyển các khoản tín chỉ EduCTX cho sinh viên (được đại diện bởi một địa chỉ) và thực hiện đăng ký ban đầu của cơ sở GDĐH đang áp dụng (đăng ký đại diện). Ví cung cấp giao diện an toàn cho hệ sinh thái blockchain bằng cách tận dụng API REST được cung cấp bởi các nút mạng blockchain. Để thuận tiện, ví cũng cho phép bảo mật phần cứng - bằng cách tích hợp ví phần cứng Ledger Nano S (HW). Ledger Nano S là một ví HW, dựa trên các tính năng an toàn mạnh mẽ để lưu trữ tài sản mật mã và đảm bảo thanh toán kỹ thuật số [54].



Hình 6. Giáo sư chỉ định số tín chỉ sử dụng ví khách ECTX.

Để tham gia hệ sinh thái EduCTX, cơ sở GDĐH đang áp dụng phải cung cấp cơ sở kỹ thuật (chạy ít nhất một nút mạng chính, cung cấp ứng dụng ví cho người đăng ký) và chứng minh danh tính của mình. Các bước cơ bản bao gồm: (1) chuẩn bị một nút EduCTX, (2) tham gia mạng EduCTX và (3) trở thành thành viên EduCTX được cấp phép. Sau khi đánh giá danh tính cẩn thận, cơ sở GDĐH mới có thể được chấp nhận làm đại diện hợp pháp và đáng tin cậy của mạng EduCTX. Cơ sở GDĐH mới được bỏ phiếu vào mạng đại biểu bởi các cơ sở GDĐH đáng tin cậy khác (các nút đại biểu). Hướng dẫn chi tiết có tại trang web chính thức của Sáng kiến EduCTX, eductx.org.

Để tham gia hệ sinh thái EduCTX, cơ sở GDĐH đang áp dụng phải cung cấp cơ sở kỹ thuật (chạy ít nhất một nút mạng chính, cung cấp ứng dụng ví cho người đăng ký) và chứng minh danh tính của mình. Các bước cơ bản bao gồm: (1) chuẩn bị một nút EduCTX, (2) tham gia mạng EduCTX và (3) trở thành thành viên EduCTX được cấp phép. Sau khi đánh giá danh tính cẩn thận, cơ sở GDĐH mới có thể được chấp nhận làm đại diện hợp pháp và đáng tin cậy của mạng EduCTX. Cơ sở GDĐH mới được bỏ phiếu vào mạng đại biểu bởi các cơ sở GDĐH đáng tin cậy khác (các nút đại biểu). Hướng dẫn chi tiết có tại trang web chính thức của Sáng kiến EduCTX, eductx.org.

Hệ sinh thái EduCTX đã được thiết kế để chạy hiệu quả, an toàn và không xâm phạm. Việc tích hợp với các hệ thống thông tin hiện có sẽ được tiến hành dựa trên các yêu cầu của chúng bằng cách sử dụng các API REST. Có rất nhiều lợi ích cho người dùng cuối (hồ sơ hoàn thành đáng tin cậy, xác nhận khóa học xuyên biên giới, giao dịch nhanh, xác minh nhân viên), sẽ được cung cấp thông qua các ứng dụng hiện có và ứng dụng mới dựa trên API REST. Khái niệm tổng thể của hệ sinh thái blockchain là chạy nền và cung cấp xương sống toàn cầu, đáng tin cậy và chống giả mạo cho một hệ thống tín chỉ học thuật tiềm năng.

VI. **THẢO LUẬN**

Phần sau đây phác thảo bối cảnh rộng hơn, các giả định và xác định các hạn chế và thách thức của nền tảng blockchain được đề xuất.Với bằng chứng về khái niệm đã được trình bày và việc triển khai nguyên mẫu của nền tảng EduCTX, chúng tôi cũng đã giới thiệu sáng kiến EduCTX và dự đoán rằng cộng đồng xung quanh nó sẽ phát triển hơn nữa. Tất cả các bên liên quan được xác định (tức là cơ sở GDĐH, sinh viên, công ty) đều có thể hưởng lợi từ hệ thống chấm điểm và tín chỉ giáo dục đại học phi tập trung, đáng tin cậy trên toàn cầu, dễ sử dụng và không gặp bất kỳ trở ngại nào về quản trị, kịch bản và ngôn ngữ, do đó, giới thiệu sự rõ ràng dễ hiểu về chương trình cho một quy trình thường xuyên cao, được phổ biến trên toàn thế giới.

Cần lưu ý rằng mục đích của sáng kiến EduCTX không phải là thay đổi và chuyển đổi hoàn toàn các hệ thống tín chỉ và chấm điểm hiện tại được thiết lập ở các quốc gia khác nhau, mà là để cải thiện nó bằng cách thêm tính minh bạch và tự động hóa để tối ưu hóa các quy trình hành chính liên quan đến hệ thống GDĐH trên phạm vi toàn cầu. Đây thậm chí còn là một trường hợp đúng đắn hơn khi xem xét các quy tắc lập pháp khác nhau ở các quốc gia khác nhau và xem xét các hệ thống tín chỉ và phân loại khác nhau trên quy mô toàn cầu. Trên thực tế, do các lý do pháp lý (luật pháp và quy tắc quốc gia hoặc xuyên quốc gia), sự tồn tại chung của cả hai hệ thống ngay từ đầu là một kịch bản rất có thể xảy ra. Do đó, chúng tôi khuyến khích các cơ sở GDĐH tham gia sáng kiến EduCTX và sử dụng nền tảng EduCTX đồng thời với việc quản lý quy trình hiện tại của họ, đồng thời đóng góp các ý tưởng, nhận xét và đề xuất mới về nền tảng EduCTX. Tính mở của cả nền tảng và khái niệm cũng cho phép tiến bộ và phát triển hơn nữa khái niệm ở những người nghiện công nghệ hoặc có những sửa đổi tích cực đối với khái niệm.

Có một số lợi thế cho các bên liên quan khác nhau khi sử dụng một nền tảng như EduCTX. Về nguyên

tắc, biểu mẫu EduCTX cho phép các tổ chức có thể sử dụng lao động trong tương lai khả năng kiểm tra hồ sơ học tập của những người được tuyển dụng tiềm năng một cách minh bạch. Các cơ sở GDĐH có một cách thức mở, phi tập trung và minh bạch trong việc xác nhận hồ sơ cho sinh viên và nghĩa vụ của họ. Nền tảng được đề xuất hỗ trợ các cơ sở GDĐH trong các hoạt động của họ liên quan đến sinh viên và cung cấp khả năng phát hiện và ngăn chặn gian lận. Do đó, có thể tránh được nhu cầu về một quy trình kiểm tra phức tạp hơn liên quan đến hồ sơ học tập của sinh viên. Ngoài ra, sinh viên được cung cấp khả năng minh bạch và tổng quan về nghĩa vụ học tập của họ trong phạm vi chương trình học của họ. Một sinh viên có thể kiểm tra ngay lập tức hồ sơ khóa học đã hoàn thành của mình. Một lợi thế rõ ràng cho tất cả các bên liên quan có liên quan là khả năng có một dấu vết kiểm toán. Bằng cách này, gian lận có thể được ngăn chặn.

Sáng kiến và nền tảng được đề xuất trước tiên sẽ được áp dụng trên một số ít co sở GDĐH và tổ chức, do đó cho phép giai đoạn đầu tiên có thể được loại bỏ bất kỳ sự không hoàn hảo nào trong cả phần kỹ thuật và khái niệm. Nền tảng này được mở để sử dụng cho bất kỳ bên quan tâm nào, mà chúng tôi dự đoán sẽ thu hút các cơ sở GDĐH trên khắp Châu Âu và cả trên toàn cầu.

Nghiên cứu cũng bao gồm các giả định và gợi ý cụ thể. Việc triển khai nền tảng đầu tiên sẽ được thực hiện bởi cơ sở GDĐH tại quê nhà của chúng tôi, Đại học Maribor. Nền tảng cần các cơ sở GDĐH khác và các bên liên quan tham gia bắt chước để phát triển thịnh vượng. Nền tảng được đề xuất cũng có những vấn đề và sự không hoàn hảo cụ thể của nó. Lúc đầu, chỉ một vài nút sẽ là một phần của mạng và đây có thể được coi là một rủi ro bảo mật. Tuy nhiên, chúng tôi dự đoán số lượng các nút trường đại học sẽ tăng lên và bằng cách này, mối lo ngại về bảo mật sẽ giảm thiểu kịp thời. Hơn nữa, khi một số lượng nút cơ sở GDĐH thích hợp trở thành một phần của mạng, vấn đề sẽ hoàn toàn không xảy ra. Một vấn đề bổ sung liên quan đến việc lưu trữ và bảo vệ đầy đủ các khóa cá nhân cho tất cả các thực thể tham gia (ví dụ: sinh viên, nhà trường). Người ta cho rằng tất cả những người tham gia sẽ bảo vệ và sao lưu khóa cá nhân của họ, như mong đợi khi xử lý dữ liệu nhạy cảm. Những thực hành và khía cạnh như vậy là bình thường trong các xã hội cho phép một người ký các tài liệu điện tử bằng chữ ký số của họ, do các tổ chức chính phủ ban hành và được bảo vệ bằng khóa cá nhân và mật khẩu [55]. Hơn nữa, người tham gia cũng yêu cầu phải bảo vệ và bảo vệ thông tin của họ trong thế giới thực, nơi chúng tôi mong đợi từ các cơ quan đáng tin cậy (trong trường hợp này là cơ sở GDĐH) để bảo vệ và sao lưu tất cả các con dấu, chữ ký chính thức của họ, v.v.

Tuy nhiên, một trường hợp có thể xảy ra khi sinh viên mất khóa riêng của mình, do đó không thể chứng minh quyền sở hữu địa chỉ blockchain EduCTX và mã thông báo ECTX. Trong trường hợp này, sinh viên có thể đích thân về thăm cơ sở GDĐH tại quê nhà của mình và yêu cầu cấp một địa chỉ blockchain mới cho anh ta / cô ta. Cơ sở GDĐH tại nhà của anh ấy / cô ấy sẽ xác minh hồ sơ của anh ấy / cô ấy và lại chuyển số lượng mã thông báo ECTX thích hợp đến địa chỉ blockchain mới của anh ấy / cô ấy. Thay vào đó, địa chỉ cũ của sinh viên có thể bị hủy bỏ bằng nhiều cách khác nhau. Đề xuất cải tiến sẽ được thảo luận thêm trong chương trình Sáng kiến EduCTX. Hơn nữa, các khóa dữ liệu ví blockchain (công khai và riêng tư) của sinh viên có thể bị đánh cắp bởi kẻ thù, kẻ có thể cố gắng mạo danh sinh viên và yêu cầu thành tích học tập của họ. Có thể tránh được trường hợp này bằng cách thêm một mức bảo vệ bổ sung cho dữ liệu ví blockchain của sinh viên, tức là mã hóa dữ liệu ví bằng mật khẩu hoặc sử dụng ví Ledger Nano HW đã được tích hợp. Để bảo mật bổ sung, mỗi bên liên quan đến nền tảng có liên quan có thể được cấp một địa chỉ chữ ký đa cấp (ví dụ: 2-8, theo đó tất cả các khóa được giao cho chủ sở hữu ban đầu và được lưu trữ ở những nơi bí mật và an toàn khác nhau), kèm theo đó là một địa chỉ vẫn hoạt động ngay cả khi một trong các chìa khóa bị mất.

VII. KẾT LUẬN VÀ CÔNG VIỆC TƯƠNG LAI

EduCTX được đề xuất như một nền tảng tín chỉ giáo dục đại học dựa trên blockchain toàn cầu. Nền tảng được đề xuất tận dụng lợi thế của blockchain để tạo ra một hệ thống chấm điểm và tín chỉ giáo dục đại

học đáng tin cậy trên toàn cầu. Như một bằng chứng về khái niệm, chúng tôi đã trình bày một bản triển khai nguyên mẫu của nền tảng EduCTX dựa trên nền tảng blockchain Ark mã nguồn mở. Nền tảng EduCTX được đề xuất giải quyết quan điểm thống nhất toàn cầu cho sinh viên và tổ chức. Sinh viên được hưởng lợi từ một cái nhìn duy nhất và minh bạch về các khóa học đã hoàn thành của họ, trong khi các cơ sở GDĐH có quyền truy cập vào dữ liệu cập nhật bất kể nguồn gốc giáo dục của sinh viên. Những người thụ hưởng khác của hệ thống được đề xuất là những nhà tuyển dụng tiềm năng, những người có thể xác nhận trực tiếp thông tin do sinh viên cung cấp.

Giải pháp được đề xuất dựa trên hệ thống mạng làm việc P2P phân tán. Nó chuyển hệ thống chấm điểm giáo dục đại học từ các hồ sơ vật lý trong thế giới thực hiện tại hoặc các hồ sơ kỹ thuật số truyền thống (ví dụ: cơ sở dữ liệu) sang một phiên bản hiệu quả, đơn giản, phổ biến, dựa trên công nghệ blockchain. Người ta dự đoán rằng một hệ thống như vậy có thể phát triển thành một hệ thống chấm điểm và tín chỉ giáo dục đại học thống nhất, đơn giản hóa và phổ biến trên toàn cầu.

Chúng tôi đặc biệt khuyến khích, kêu gọi và mời tất cả các cơ sở GDĐH liên hệ với chúng tôi và từ đó tham gia sáng kiến EduCTX.

Trong tương lai, chúng tôi có kế hoạch thử nghiệm nguyên mẫu trong môi trường thực tế, bao gồm các cơ sở GDĐH, sinh viên và công ty. Bằng cách này, khái niệm được trình bày có thể tiếp tục được xác thực. Ngoài ra, chúng tôi có kế hoạch điều chỉnh chuỗi khối EduCTX để mỗi khóa học sẽ được chỉ định với một địa chỉ blockchain duy nhất và một nhóm các mã thông báo. Sau khi hoàn thành các nghĩa vụ của khóa học, sinh viên sẽ nhận được mã thông báo từ địa chỉ khóa học chứ không phải trực tiếp từ tổ chức nhà trường. Địa chỉ khóa học sẽ là một địa chỉ có nhiều chữ ký giữa một tổ chức nhà trường và một giáo sư.

Hiện tại, nền tảng được đề xuất dựa trên hệ thống chấm điểm ECTS, nhưng có thể được mở rộng và điều chỉnh cho phù hợp với bất kỳ hệ thống tín chỉ hoặc chứng chỉ nào hiện có và do đó kết hợp các khía cạnh khác của chứng chỉ giáo dục.

Chúng tôi còn có kế hoạch mở rộng công việc của mình và nền tảng EduCTX để dựa trên các hợp đồng thông minh và phiên bản thích hợp của công nghệ blockchain.

LỜI MỜI sáng kiến EduCTX

Nền tảng blockchain EduCTX dựa trên ý tưởng rằng tất cả cáccơ sở GD ĐH được phân tán trên toàn cầu hợp lực với nhau để xây dựng một giải pháp hiệu quả, đơn giản hóa, phổ biến cho việc chuyển đổi tín chỉ của sinh viên, đồng thời loại bỏ các trở ngại về ngôn ngữ và quản trị phát sinh khi xử lý chuyển khoản tín dụng và chứng nhận trên phạm vi rộng hơn hoặc toàn cầu. Do đó, chúng tôi mời bất kỳ ai quan tâm tham gia sáng kiến EduCTX (có thêm thông tin tại eductx.org), để ý tưởng EduCTX có thể được thảo luận và phát triển thêm. Chúng tôi cũng khuyến khích tất cả các cơ sỏ GDĐH, đặc biệt là những cơ sở GDĐH đã có hệ thống được công nhận ECTS, tham gia vào mạng lưới blockchain EduCTX, do đó giúp lan rộng và tăng thêm tính bảo mật của mạng. Để biết thêm thông tin, vui lòng liên hệ với chúng tôi theo địa chỉ: eductx@um.si.

Hà Nội, ngày 29-8-2020

REFERENCES

[1] (2016). *Ark: All-in-One Blockchain Solutions.* [Online]. Available: http://www.ark.io

[2] G. Coulouris, J. Dollimore, T. Kindberg, and G. Blair, *Distributed Systems: Concepts and Design,* 5th ed. Reading, MA, USA: Addison-Wesley, 2011.

[3] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review,'' *PLoS ONE,* vol. 11, no. 10, p. e0163477, Oct. 2016. [Online]. Available: https://doi.org/10.1371/journal.pone.0163477

[4] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records,'' *J. Biomed. Inform.,* vol. 71, pp. 70-81, Jul. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1532046417301089

[5] O. S. Kemkar and P. Kalode, "Formulation of distributed electronic patient record (DEPR) system using openemr concept,'' *Int. J. Eng. Innov. Res.,* vol. 4, pp. 85-89, 2012. [Online]. Available: http://www.ijeir.org/index.php/issue?view=publication&task=show&id=418

[6] C. He, X. Fan, and Y. Li, "Toward ubiquitous healthcare services with a novel efficient cloud platform,'' *IEEE Trans. Biomed. Eng.,* vol. 60, no. 1, pp. 230-234, Jan. 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6324392/

[7] Z. Shae and J. J. P. Tsai, "On the design of a blockchain platform for clinical trial and precision medicine,'' in *Proc. Int. Conf. Dis- trib. Comput. Syst.,* Jun. 2017, pp. 1972-1980. [Online]. Available: http://ieeexplore.ieee.org/document/7980138/

[8] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, andM. Guizani, "MeD-Share: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access,* vol. 5, pp. 14757-14767, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7990130/

[9] M. Mettler, "Blockchain technology in healthcare: The revolution starts here,'' in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom),* Sep. 2016, pp. 1-3. [Online]. Available: http://ieeexplore.ieee.org/document/7749510/

[10] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management,'' in *Proc. 2nd Int. Conf. Open Big Data (OBD),* Aug. 2016, pp. 25-30. [Online]. Available: http://ieeexplore.ieee.org/document/7573685/

[11] H. Hou, "The application of blockchain technology in E-government in China,'' in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN),* Jul./Aug. 2017, pp. 1-4. [Online]. Available: http://ieeexplore.ieee.org/document/8038519/

[12] S. 0lnes and A. Jansen, *Blockchain Technology as s Support Infrastructure in e-Government.* Cham, Switzerland: Springer, Sep. 2017, pp. 215-227. [Online]. Available: http://link.springer.com/10.1007/978-3- 319-64677-0_18

[13] S. 0lnes, *Beyond Bitcoin Enabling Smart Government Using Blockchain Technology.* Cham, Switzerland: Springer, Sep. 2016, pp. 253-264. [Online]. Available: http://link.springer.com/10.1007/978-3-319-44421- 5_20

[14] V. Morabito, "Blockchain Governance," in *Business Innovation Through Blockchain*. Cham, Switzerland: Springer, 2017, pp. 41-59. [Online]. Available: http://link.springer.com/10.1007/978-3-319-48478-5_3

[15] R. Qi, C. Feng, Z. Liu, and N. Mrad, *Blockchain-Powered Internet of Things, E-Governance and E-Democracy.* Singapore: Springer, 2017, pp. 509-520. [Online]. Available: http://link.springer.com/10.1007/978- 981-10-4035-1_17

[16] J. Sidhu, "Syscoin: A peer-to-peer electronic cash system with blockchain-based services for E-business,'' in *Proc. 26th Int. Conf. Comput. Com- mun. Netw. (ICCCN),* Jul./Aug. 2017, pp. 1-6. [Online]. Available: http://ieeexplore.ieee.org/document/8038518/

[17] S. Huckle, R. Bhattacharya, R. White, and N. Beloff, "Internet of Things, blockchain and shared economy applications,'' *Procedia Comput. Sci.,* vol. 98, pp. 461-466, Jan. 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050916322190

[18] P. Rimba, A. B. Tran, I. Weber, M. Staples, A. Ponomarev, and X. Xu, "Comparing blockchain and cloud services for business process execution,'' in *Proc. IEEE Int. Conf. Softw. Archit. (ICSA),* Apr. 2017, pp. 257-260. [Online]. Available: http://ieeexplore.ieee.org/document/ 7930226/

[19] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems,'' in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC),* Nov. 2016, pp. 2663-2668. [Online]. Available: http://ieeexplore.ieee.org/document/7795984/

[20] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems,'' *IEEE Internet Things J.,* vol. 4, no. 6, pp. 1832-1843, Dec. 2017.

[21] F. Imbault, M. Swiatek, R. de Beaufort, and R. Plana, "The green blockchain: Managing decentralized energy production and consumption,'' in *Proc. 17th IEEE Int. Conf. Environ. Elect. Eng., 1st IEEE Ind. Commercial Power Syst. Eur. (EEEIC/I CPS Eur.),* Jun. 2017, pp. 1-5. [Online]. Available: http://ieeexplore.ieee.org/document/7977613/

[22] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,'' *IEEE Trans. Depend. Sec. Comput.,* to be published. [Online]. Available: http://ieeexplore.ieee.org/document/7589035/

[23] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets,'' in *Computer Science—Research and Development.* Berlin, Germany: Springer, Aug. 2017, pp. 1-8. [Online]. Available: http://link.springer.com/10.1007/s00450-017-0360-9

[24] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review,'' in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. (AICCSA),* Nov. 2017, pp. 1-6. [Online]. Available: http://ieeexplore.ieee.org/document/7945805/

[25] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things,'' *Peer-Peer Netw. Appl.,* vol. 10, no. 4, pp. 983-994, Jul. 2017. [Online]. Available: http://link.springer.com/10.1007/s12083-016-0456-1

[26] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, *Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT.* Cham, Switzerland: Springer, 2017, pp. 523-533. [Online]. Available: http://link.springer.com/10.1007/978-3-319-46568-5_53
[27] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68-72, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8012302/
[28] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618-623. [Online]. Available: http://ieeexplore.ieee.org/document/7917634/
[29] J. Sun, J. Yan, and K. Z. K. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," *Financial Innov.*, vol. 2, no. 1, p. 26, Dec. 2016. [Online]. Available: http://jfin-swufe.springeropen.com/articles/10.1186/s40854-016-0040-y
[30] Z. Chen and Y. Zhu, "Personal archive service system using blockchain technology: Case study, promising and challenging," in *Proc. IEEE Int. Conf. AIMobile Services (AIMS)*, Jun. 2017, pp. 93-99. [Online]. Available: http://ieeexplore.ieee.org/document/8027275/
[31] M. Fukumitsu, S. Hasegawa, J. Iwazaki, M. Sakai, and A. Takahashi, "A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain," in *Proc. IEEE 31st Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2017, pp. 803-810. [Online]. Available: http://ieeexplore.ieee.org/document/7920990/
[32] Media Lab Learning Initiative. *Digital Certificates Project.* [Online]. Available: http://certificates.media.mit.edu/
[33] *Universidad Nacional De la Plata.* [Online]. Available: https://www.unlp.edu.ar/
[34] A. Third, J. Domingue, M.Bachler, and K. Quick, "Blockchains and the Web position paper," in *Proc. W3C Workshop Distrib. Ledgers Web*, Cambridge, U.K., 2016. [Online]. Available: https://www.w3.org/2016/04/blockchain-workshop/interest/third.html
[35] F Bond, F. Amati, and G. Blousson, "Blockchain, academic verification use case," Tech. Rep., 2015. [Online]. Available: https://s3.amazonaws.com/signatura-usercontent/blockchain_academic_verification_use_case.pdf
[36] F Amati. (2015). *First Official Career Diplomas on Bitcoin's Blockchain.* [Online]. Available: https://blog.signatura.co/first-official-career- diplomas-on-bitcoin-s-blockchain-69311acb544d
[37] S. Das. (2016). *Parisian Engineering School Will Certify Diplomas on the Blockchain—CryptoCoinsNews.* [Online]. Available: https://www.cryptocoinsnews.com/parisian-engineering-school-will-certify-diplomas-blockchain/
[38] L. Coleman. (2015). *Engineering School Simplifies Verifying Certificates Using the Blockchain—CryptoCoinsNews*. [Online]. Available: https://www.cryptocoinsnews.com/engineering-school-simplifies-verifying-certificates-using-block-chain/
[39] European Commission. (2015). *ECTS Users' Guide.* [Online]. Available: https://ec.europa.eu/education/sites/education/files/ects-users-guide_en.pdf
[40] M. D. Sleiman, A. P Lauf, and R. Yampolskiy, "Bitcoin message: Data insertion on a proof-of-work cryptocurrency system," in *Proc. Int. Conf. Cyberworlds (CW)*, Oct. 2015, pp. 332-336. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7398436
[41] T. Aste, P. Tasca, andT. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18-28, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8048633/
[42] Y. G. Desmedt, *Public Key Cryptography—PKC: 6th International Workshop on Theory and Practice in Public Key Cryptography*. Miami, FL, USA: Springer, 2003, pp. 1-266.
[43] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557-564. [Online]. Available: http://ieeexplore.ieee.org/document/ 8029379/
[44] NIST Technology. (2012). *Secure Hash Standard (Shs), Federal Information Processing Standards Publication*. [Online]. Available: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
[45] M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "Proof-of-personhood: Redemocratizing permissionless cryptocurrencies," in *Proc. IEEE Eur Symp. Secur Privacy Workshops (EuroS PW)*, Apr. 2017, pp. 23-26. [Online]. Available: http://ieeexplore.ieee.org/document/7966966/
[46] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* [Online]. Available: https://bitcoin.org/bitcoin.pdf
[47] G. Greenspan. (2016). *Blockchains vs Centralized Databases.* [Online]. Available: https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/
[48] A. Lewis. (2015). *A Gentle Introduction to Blockchain Technology*. Available: https://bitsonblocks.net/2015/09/09/a-gentle-introduction- to-blockchain-technology/
[49] N. Gilboa, "Two party RSA key generation," in *Proc. 19th Annu. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO)*, London, U.K., 1999, pp. 116-129. [Online]. Available: http://dl.acm.org/citation.cfm?id=646764.703977
[50] X. Zhou, Q. Wu, B. Qin, X. Huang, and J. Liu, "Distributed bitcoin account management," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 105-112.
[51] (2017). *ARK Whitepaper: A Platform for Consumer Adoption.* [Online]. Available: https://ark.io/Whitepaper.pdf
[52] (2017). *Github: EduCTX Platform Initiative.* [Online]. Available: https://github.com/eductxplatform
[53] *The MIT License*. [Online]. Available: https://opensource. org/licenses/MIT
[54] *Ledger Wallet—Ledger Nano S—Cryptocurrency Hardware Wallet*. Accessed: Dec. 3, 2017. [Online]. Available: https://www.ledgerwallet.com/products/ledger-nano-s
[55] L. M. Batten, "Digital Signatures," in *Public Key Cryptography: Applica tions and Attacks.* Hoboken, NJ, USA: Wiley, 2013,pp. 103-131. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber =6482707

MUHAMED TURKANOVIC received the B.Sc. degree and the Ph.D. degree in computer science and informatics from the University of Maribor in 2011 and 2016, respectively. His Ph.D. thesis was on authentication protocols for the Internet of Things. He has authored several highly cited scientific articles, published in renowned journals with an impact factor in the field of computer science. He was a Managing Director and a CTO of an IT company from 2013 to 2016. In 2017, he joined the Faculty of Electrical Engineering and Computer Science, University of Maribor, as an Assistant Professor of information technology. His current research interests include advanced database technologies, big data, blockchain technology, Internet of Things, cryptography, wireless sensor networks, and quantum cryptography.

MARKO HOLBL received the Ph.D. degree in computer science from the University of Maribor in 2009. He is currently an Assistant Professor with the Institute of Informatics. His main research interests include all aspect of computer security, cryptography, network and Internet security, users' perception of security, security awareness, and the blockchain technology. He has been involved in several applied and international projects. He has authored or coauthored several articles in peer- erence impact factor, and in international conferences.

reviewed scientific journals, four in journals with the journal citation ref-

KRISTJAN KOSIC is currently pursuing the Ph.D. degree in computer science with the University of Maribor. He has more than ten years of experience in research, pedagogical, and project work. He is currently a Senior Researcher in computer science with the University of Maribor, where he helps to deliver various courses of different study programs. He has authored or coauthored several peer-reviewed scientific journals. His current research interests include blockchain technology and challenges related to its mass adoption and human-computer interaction related to quality user experience design with enabling contact-free humancomputer sensors and supportive technologies, all in the context of contemporary information system interfaces and improving efficiency for the end user. His current certifications include a Certified Cloud Computing Engineer and an Internal Auditor for Medical Software Quality Systems (EN-ISO-13485).

AIDA KAMISALIC received the Ph.D. degree in computer science in 2014. She is currently a Teaching Assistant and a Researcher with the Faculty of Electrical Engineering and Computer Science, University of Maribor. Her research interests include database technologies, big data, blockchain technology medical procedures modeling for chronic patients, and time knowledge acquisition for medical procedures.

MARJAN HERICKO received the Ph.D. degree in computer science and informatics from the University of Maribor in 1998. He is currently a Full Professor with the Faculty of Electrical Engineering and Computer Science, University of Mari- bor, where he is also the Head of the Institute of Informatics. His main research interests include all aspects of IS development with emphasis on software and service engineering, software process improvement, data, and process modeling.