Kỷ yếu Hội nghị KHCN Quốc gia lần thứ XII về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR); Huế, ngày 07-08/6/2019
DOI: 10.15625/vap.2019.00022

GIẢI PHÁP QUẢN LÝ TÀI SẢN NGĂN CHẶN BẰNG CÔNG NGHỆ BLOCKCHAIN

Trương Minh Tuyền[1], Nguyễn Hoàng Tùng[2], Huỳnh Phước Hải[2], Lê Hoàng Anh[2], Nguyễn Văn Hòa[2]

[1] Trung tâm Tin học, Trường Đại học An Giang
[2] Khoa Công nghệ thông tin, Trường Đại học An Giang

{tmtuyen, nhoangtung, hphai, lhanh, nvhoa}@agu.edu.vn

***TÓM TẮT**: Công nghệ blockchain mới xuất hiện trong một vài năm gần đây nhưng đã có rất nhiều nghiên cứu để hoàn thiện công nghệ cũng như các nghiên cứu triển khai ứng dụng trong nhiều lĩnh vực như tài chính, y tế, giáo dục và đặc biệt là chính phủ số. Đặc tính nổi trội của công nghệ blockchain là bảo mật thông tin dựa trên nền tảng dữ liệu phi tập trung và cấu trúc lưu trữ theo dạng chuỗi khối. Đây chính là cơ sở để chống giả mạo thông tin và nâng cao hiệu suất xác thực dựa trên kiến trúc phi tập trung và chia sẻ thông tin sổ cái. Công nghệ blockchain có thể tạo ra một hệ sinh thái an toàn, linh hoạt và thích hợp trong lĩnh vực dịch vụ công. Công nghệ này cũng mang đến sự minh bạch bằng cách tạo ra bằng chứng số, hợp đồng giao dịch về tài sản. Trong bài báo này, chúng tôi đề giải pháp quản tài sản ngăn chặn bằng công nghệ blockchain thông qua nền tảng Hyperledger Fabric. Giải pháp đề xuất góp phần nâng cao hiệu quả công tác quản lý, điều hành và đơn giản thủ tục công chứng tại các phòng công chứng và cơ quan quản lý nhà nước. Kết quả thử nghiệm giải pháp đề xuất có hiệu suất cao và có khả năng ứng dụng rộng rãi trong lĩnh vực công chứng.*

***Từ khóa**: blockchain, sổ cái, chaincode, Hyperledger Fabric, công chứng, tài sản ngăn chặn.*

I. GIỚI THIỆU

Được ra đời trong vài năm gần đây nhưng blockchain được xem là một trong các ý tưởng mang tính đột phá nhất trong việc thay đổi tư duy và cuộc sống của con người kể từ sau sự ra đời của Internet. Về cơ bản, blockchain là công nghệ được dùng để xây dựng một cấu trúc dữ liệu (cuốn sổ cái) với mục đích ghi lại các giao dịch một cách công khai trên một hệ thống máy tính ngang hàng theo phương thức mã hóa các giao dịch theo chuỗi thời gian. Từ đó có thể loại bỏ các bên trung gian và tạo ra vô vàn ứng dụng giúp tăng cường sự tin tưởng, tính trách nhiệm và sự minh bạch với chi phí và quy trình thủ tục được giảm thiểu đáng kể. Công nghệ blockchain đã thu hút rất nhiều nghiên cứu để hoàn thiện kiến trúc mạng, cơ chế vận hành cũng như là triển khai ứng dụng ngoài tiền mã hóa và hợp đồng thông minh như các sản phẩm dịch vụ trong công nghệ tài chính, y tế, giáo dục và các hệ thống chia sẻ dữ liệu có tính chất pháp lý như dịch vụ công.

Ở Việt Nam, xã hội hóa hoạt động công chứng là một trong những chủ trương lớn của Đảng và Nhà nước ta. Chủ trương này đã được cụ thể hóa thông qua khung pháp lý của Luật Công chứng 2006 (Quốc hội khóa 11, 2006). Và khung pháp lý này tiếp tục được hoàn thiện trong Luật Công chứng 2014 (Quốc hội khóa 13, 2014). Một trong những thành công của chủ trương xã hội hóa hoạt động công chứng là số lượng phòng công chứng đã tăng rất nhanh. Đến tháng 6 năm 2018, số phòng công chứng trong cả nước tăng hơn nhiều lần so với năm 2007, là năm bắt đầu cho thành lập các văn phòng công chứng. Hiện nay, hầu hết các địa phương cấp huyện hoặc tương đương đều có phòng công chứng nhằm đáp ứng nhu cầu ngày càng cao của xã hội.

Luật Công chứng hiện hành quy định rất chặt chẽ các hành vi bị cấm đối với tổ chức và công chứng viên (Quốc hội khóa 13, 2014). Chẳng hạn, một phòng công chứng chỉ được công chứng hợp đồng, giao dịch về bất động sản trong phạm vi tỉnh, thành phố trực thuộc trung ương nơi tổ chức hành nghề công chứng đặt trụ sở tại tỉnh, thành phố trực thuộc trung ương nơi có bất động sản. Ngoài ra, khi một bất động sản đã được thế chấp để bảo đảm thực hiện một nghĩa vụ và hợp đồng thế chấp đã được công chứng mà sau đó được tiếp tục thế chấp để bảo đảm cho một nghĩa vụ khác trong phạm vi pháp luật cho phép thì các hợp đồng thế chấp tiếp theo phải được công chứng tại tổ chức hành nghề công chứng đã công chứng hợp đồng thế chấp lần đầu. Tuy nhiên, hiện nay hoạt động công chứng hợp đồng, giao dịch bất động sản vẫn còn một số tồn tại, một trong số đó là tình trạng tranh chấp, khiếu kiện liên quan đến giao dịch về bất động sản ngày càng gia tăng và phức tạp. Tồn tại này xuất phát nhiều nguyên nhân trong đó có sự gian dối, lừa đảo của một số đối tượng khi tham gia giao dịch. Để khắc phục tồn tại trên, Bộ Tư pháp có nhiều các giải pháp đã được đưa ra (Bộ Tư pháp, 2014). Trong đó có đề xuất xây dựng cơ sở dữ liệu công chứng bao gồm các thông tin về nguồn gốc tài sản, tình trạng giao dịch của tài sản và các thông tin về biện pháp ngăn chặn được áp dụng đối với tài sản có liên quan đến hợp đồng, giao dịch đã được công chứng. Cơ sở dữ liệu này được vận hành bởi Ủy ban nhân dân cấp tỉnh và các tổ chức hành nghề công chứng trên địa phương đó cùng khai thác với yêu cầu bảo mật và tính tường minh.

Công nghệ blockchain có thể tạo ra một hệ sinh thái an toàn và linh hoạt thích hợp trong lĩnh vực công chứng (Casinoa, 2019). Công nghệ này mang đến tính minh bạch bằng cách tạo ra bằng chứng cho các loại tài liệu như giấy tờ, hợp đồng giao dịch công chứng về nhà đất và tài sản cần ngăn chặn các giao dịch. Theo hiểu biết của chúng tôi thì ở Việt Nam chưa có một nghiên cứu nào về ứng dụng blockchain trong quản lý hợp đồng công chứng và tài sản ngăn chặn được công bố. Trong báo cáo này, chúng tôi đề xuất giải pháp quản lý tài sản ngăn chặn cho các phòng công

chứng bằng công nghệ blockchain trên nền tảng Hyperledger Fabric. Chúng tôi đánh giá hiệu suất của giải pháp thông qua hoạt động phân tích hiệu suất của kiến trúc mạng blockchain đề xuất.

Trong phần tiếp theo của bài viết sẽ giới thiệu các nghiên cứu có liên quan có sử dụng công nghệ blockchain. Phần III sẽ trình bày mô kiến trúc đề xuất của mạng blockchain và mô hình tổng thể của giải pháp quản lý hợp đồng công chứng, giao dịch và tài sản ngăn chặn. Kết quả của giải pháp và phân tích hiệu suất của kiến trúc mạng blockchain được đề xuất trong phần IV trước phần kết luận và hướng phát triển trong phần V.

II. CÁC NGHIÊN CỨU CÓ LIÊN QUAN

Hiện nay, hệ thống blockchain được chia làm 3 loại (Zheng, 2017): (a) hệ thống public cho phép bất kỳ ai cũng có quyền ghi và đọc dữ liệu trên blockchain như Bitcoin (Nakamoto, 2008), Ethereum (Wood, 2014)…; (b) hệ thống private chỉ cho phép người dùng quyền đọc dữ liệu mà không có quyền ghi vì điều này thuộc về bên thứ ba tuyệt đối tin cậy như Ripple (Armknecht, 2015); (c) hệ thống phân quyền (hay còn được gọi là consortium) là dạng của private nhưng có sự kết hợp giữa "niềm tin" khi tham gia vào public và "niềm tin tuyệt đối" khi tham gia vào private như blockchain riêng của các tổ chức trên nền tảng Hyperledger (Cachin, 2016; Androulaki, 2018). Từng loại hệ thống blockchain có những điểm mạnh và hạn chế của nó và được sử dụng trong từng lĩnh vực cụ thể, trong đó Hyperledger là nền tảng rất phù hợp để triển khai hệ thống blockchain phân quyền.

Ngoài những ứng dụng về tiền mã hóa và hợp đồng thông minh, blockchain còn được ứng dụng trong rất nhiều lĩnh vực khác như y tế, giáo dục, quản lý dữ liệu (data management) và chính phủ số (digital government). Trong lĩnh vực y tế, công nghệ blockchain được sử dụng trong các ứng dụng về chăm sóc sức khỏe cộng đồng, tiếp nhận bệnh trực tuyến, chia sẻ dữ liệu bệnh nhân mới mục tiêu minh bạch hóa thông tin và đảm bảo an toàn dữ liệu (Kleinaki, 2018; Mettler, 2016; Peterson, 2016; Patel, 2018); các giải pháp này sử dụng nền tảng Ethereum để lưu dữ liệu và các giao dịch.

Còn trong lĩnh vực giáo dục, blockchain có thể giải quyết các vấn đề về lỗ hổng bảo mật và quyền riêng tư trong không gian học tập (Bdiwi et al., 2017); hoặc blockchain có thể được sử dùng để lưu trữ hồ sơ, minh chứng về các phần thưởng hoặc danh hiệu (Turkanović, 2018); lưu trữ các kết quả học tập của sinh viên (Devine, 2015); blockchain giúp cải thiện bảo mật và niềm tin về văn bằng/chứng chỉ của các cơ sở đào tạo (Duc-Hiep Nguyen, 2018; Xu, 2017); Cộng đồng châu Âu cũng đã sử dụng blockchain trong việc quản lý tín chỉ trong đào tạo khi thực hiện trao đổi sinh viên đang học tại các trường của họ (Turkanović, 2018).

Trong quản lý dữ liệu, blockchain phát huy thế mạnh là tính không thể chối bỏ với nhiều ứng dụng như quản lý tập tin chia sẻ trên nền tảng Hyperledger Fabric khi xây dựng giao thức NFB dựa trên giải pháp lưu trữ tập trung được gọi là OKORO (Magrahi, 2018). Christidis và cộng sự đề xuất giải pháp bảo mật tập tin chia sẻ qua mạng bằng giao thức bảo mật telehash (Christidis, 2016), hoặc sử dụng trực tiếp hệ thống file P2P như IPFS (IPFS, 2016).

Trong chính phủ số, nhiều ứng dụng được triển khai trên nền tảng blockchain như quản lý định danh công dân, bầu cử số và dịch vụ công. Trong quản lý định danh công dân, các thông tin cá nhân như họ tên, địa chỉ, thông tin ngân hàng và những thông tin cá nhân khác được lưu trên hệ thống blockchain (Lemieux, 2016; Leiding, 2017; Augot, 2017; Buchmann, 2017). Blockchain trở thành công cụ khả thi để xây dựng hệ thống dữ liệu công dân toàn cầu thông qua bằng chứng minh có tính xác thực cao (Roberts 2017; Riera, 2017). Đối với bầu cử số thì các giải pháp trước đó đã được phát triển phát triển nền dữ liệu tập trung tiềm ẩn nhiều rủi ro bảo mật và những quan ngại về tính riêng tư. Tuy nhiên với các giải pháp bầu cử số trên nền tảng blockchain như BitCongress (Deitz, 2014) và Liquid Democracy (Schiener, 2014), cử chi có thể kiểm tra được tình trạng phiếu bầu của mình đồng thời vẫn đảm bảo tính riêng tư và bảo vệ danh tính từ đó giúp tăng cường tỷ lệ bỏ phiếu.

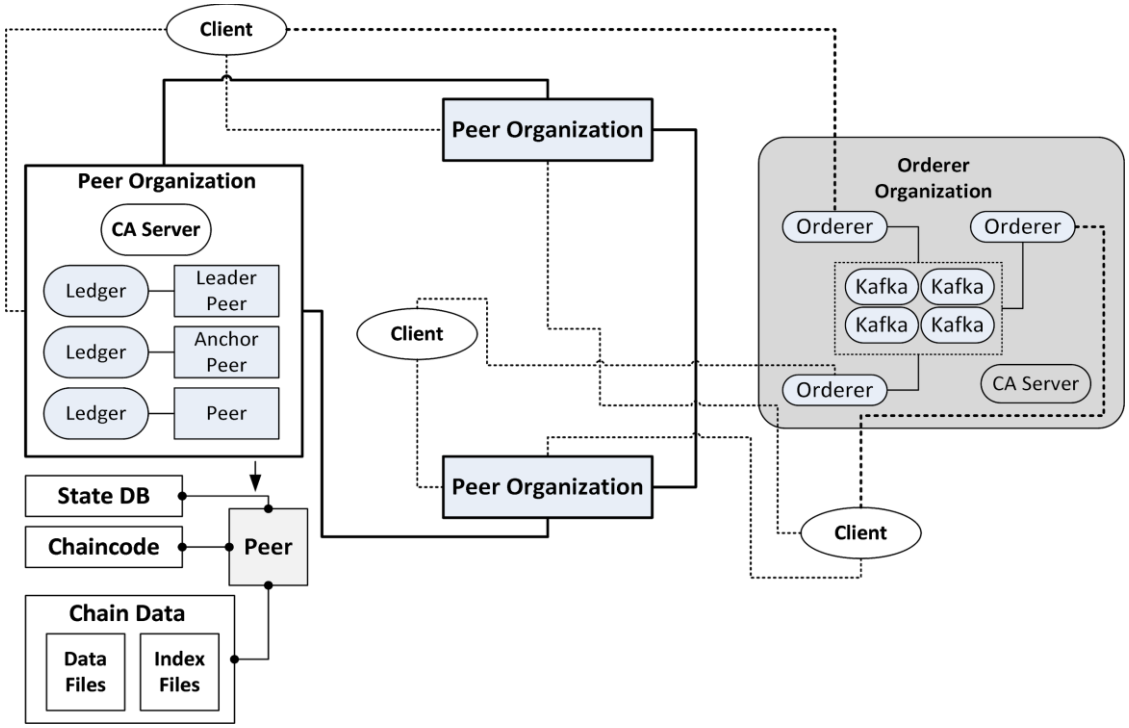
Trong dịch vụ công (public service), các dịch vụ công chứng ảo (virtual notary), xác minh sự tồn tại (proof-of-existence - PoE), xác minh sở hữu (proof-of-ownership - PoO), xác minh proof-of-integrity (PoI), và giải quyết tranh chấp là các loại dịch vụ có thể được dành cho công dân mà không có sự tham gia của các cơ quan công quyền. PoE, PoO và PoI có liên quan chặt chẽ với nhau và dễ dàng kiểm chứng trong một nền tảng blockchain. Các cơ quan chính phủ của các quốc gia trên thế giới đang tìm kiếm cơ hội để triển khai ứng dụng công nghệ blockchain trong khu vực công (Deloitte Development LLC, 2017; Chiang, 2018), đặc biệt là sử dụng công nghệ cơ sở dữ liệu an toàn, phân tán, nguồn mở để giảm chi phí đầu tư và chi phí vận hành đồng thời tăng hiệu hiệu quả và xác thực nhiều loại tài liệu dài hạn (Ølnes, 2016; Nordrum, 2017; Ølnes, 2017; Ølnes, 2017). Ngoài ra còn phải kể đến các ứng dụng blockchain khác như xác minh tài liệu (document verification), giải pháp về cư trú điện tử (Sullivan, 2017), giải pháp về minh bạch hóa về thuế (Pokrovskaia, 2017; Wijaya, 2017).

III. MÔ HÌNH KIẾN TRÚC HỆ THỐNG

Hyperledger Fabric

Hyperledger Fabric là một nền tảng blockchain phân quyền nguồn mở, được thiết kế cho các ứng dụng riêng trong môi trường doanh nghiệp. Hyperledger Fabric cung cấp kiến trúc mô đun có sự phân định vai trò giữa các nút trong kiến trúc mạng, cho phép tích hợp và thực thi hợp đồng thông minh (Chaincode). Mạng Fabric bao gồm các nút

ngang hàng với vai trò thực thi các chaincode, truy cập dữ liệu sổ cái (Ledger), xác nhận giao dịch và cũng là giao diện cho phép các ứng dụng (Client) kết nối. Ngoài ra, trong mạng còn có các nút đóng vai trò sắp xếp thứ tự các giao dịch nhằm đảm bảo tính nhất quán của mạng blockchain sau đó phân phát lại các giao dịch được chứng thực cho các nút ngang hàng của mạng. Các nút này được gọi là Orderer, chúng sẽ vận hành các cơ chế đồng thuận như Solo, Kafka, Raft. Tất cả các thành phần trong mạng được xác thực và phân cấp các vai trò bằng hệ thống cung cấp dịch vụ gọi là Membership Service Provider (MSP). Hình 1 cho thấy các thành phần cơ bản của một mạng Hyperledger Fabric bao gồm các Peer, Ledger, Orderer, Client, Kafka và CA server.



Hình 1. Các thành phần của mạng Hyperledger Fabric, mô hình kết nối giữa các peer và cấu trúc lưu trữ

Các thành phần của mạng Fabric

Peer: Một mạng blockchain bao gồm một tập hợp các nút ngang hàng (Peer). Peer là thành phần cơ bản của mạng vì nó lưu trữ sổ cái và hợp đồng thông minh. Sổ cái ghi lại tất cả các giao dịch được tạo bởi các hợp đồng thông minh. Hợp đồng thông minh và sổ cái được sử dụng để đóng gói các thông tin, các nghiệp vụ xử lý và được chia sẻ giữa tất cả các nút ngang hàng trong mạng.

Ledger: Trong mạng Hyperledger Fabric, sổ cái bao gồm hai thành phần riêng biệt là cơ sở dữ liệu lưu trạng thái hiện tại (State DB) và chuỗi khối (blockchain) như hình 1. Cơ sở dữ liệu trạng thái hiện tại sẽ cung cấp giá trị hiện tại của dữ liệu thay vì phải tính toán bằng cách duyệt qua toàn bộ nhật ký giao dịch. Chúng được lưu trữ dưới dạng các cặp khóa-giá trị (Key-Value - KV). Chuỗi khối ghi lại tất cả các nhật ký giao dịch dẫn đến thay đổi trên dữ liệu trạng thái hiện tại. Các giao dịch được tập hợp thành các khối sau đó được liên kết vào blockchain từ đó cho phép truy vết được các thay đổi đã dẫn đến trạng thái hiện tại.

Orderer: khác với blockchain public, Hyperledger Fabric yêu cầu phải có các nút chuyên biệt để vận hành các cơ chế đồng thuận. Hyperledger Fabric dựa trên các thuật toán đồng thuận xác định (deterministic) nên khi bất kỳ khối nào được đưa vào chuỗi đều phải đảm bảo chính xác và cuối cùng. Việc tách biệt chức năng chứng thực các chaincode ra khỏi orderer giúp loại bỏ các tắc nghẽn từ đó gia tăng hiệu suất và khả năng mở rộng mạng. Hiện tại mạng Fabric hỗ trợ ba cơ chế đồng Solo, Raft và Kafka.

Membership Service (MSP): MSP cung cấp tất cả các cơ chế và giao thức mã hóa, cũng như là cấp phát và quản lý các chứng chỉ đồng thời xác thực (Certificate Authority - CA) các thành phần (tổ chức) tham gia bên trong mạng. Trong một mạng blockchain Fabric có thể tồn tại nhiều hơn một MSP.

Chanel: Chanel (kênh) là một mạng con riêng, giao tiếp giữa hai hoặc nhiều thành viên trong mạng, với mục đích thực hiện các giao dịch riêng tư và bí mật. Một kênh được xác định bởi các thành viên, nút đại diện ngang hàng cho mỗi thành viên, sổ cái, chaincode, và các nút orderer.

Nghiệp vụ quản lý tài sản ngăn chặn

Theo Luật Công chứng 2014 (Quốc hội khóa 13, 2014), khi một công dân (được gọi là khách hàng) có nhu cầu thực hiện giao dịch dân sự về công chứng như mua bán, chuyển nhượng, thế chấp, tặng cho... có liên quan đến tài sản

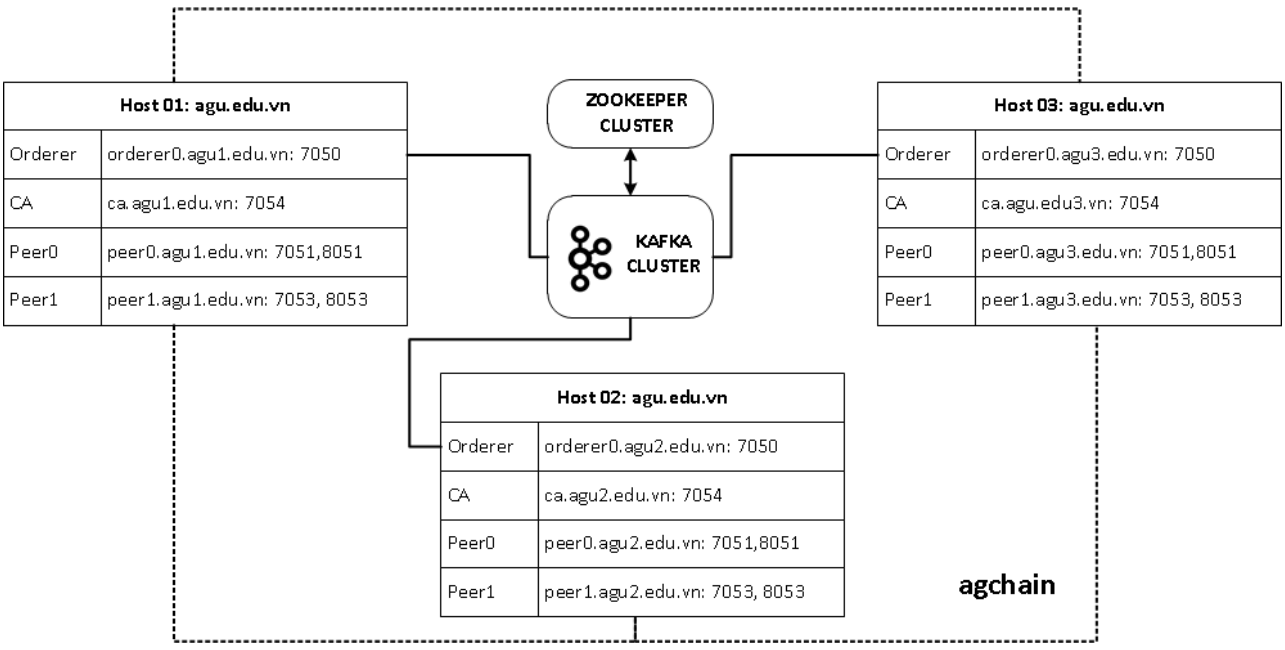
do mình đứng tên chủ sở hữu, khách hàng này cần thực hiện công chứng hợp đồng, giao dịch tại một trong các phòng công chứng trong phạm vi tỉnh/thành phố. Sau khi trao đổi với khách hàng, nhân viên phòng công chứng xác nhận loại hình giao dịch và yêu cầu xuất trình các loại chứng từ kèm theo giao dịch. Nếu các chứng từ hợp pháp, nhân viên tiến hành thực hiện giao dịch với các bước như là soạn hợp đồng, sao lưu các chứng từ kèm theo... Sau khi các bên tham gia hợp đồng kiểm tra thông tin, hợp đồng sẽ được chuyển đến công chứng viên để công chứng viên ra lời chứng và xác nhận lời chứng. Trước kết thúc giao dịch, các bên tham gia hợp đồng xác nhận thông tin, công chứng viên sẽ cấp số công chứng cho hợp đồng giao dịch để hoàn tất quy trình giao dịch.

Trong các bước thực hiện giao dịch, công chứng viên phải kiểm tra tài sản đang giao dịch có bị ngăn chặn hay không. Tài sản ngăn chặn là tài sản không được thực hiện các giao dịch dân sự bởi một trong các lý do như sau: tài sản được kê biên để đảm bảo thi hành án; tài sản đang có tranh chấp; tài sản đang trong giai đoạn báo mất giấy chứng nhận sở hữu và đang xin cấp lại giấy chứng nhận sở hữu. Theo quy định hiện hành, các thông tin về tài sản ngăn chặn để đảm bảo thi hành án được chuyển đến sở Tư pháp dưới thức văn bản pháp lý. Các phòng công chứng sẽ cập nhật thông tin về tài sản này thông qua nhiều hình thức khác nhau như thông qua cổng thông tin của sở Tư pháp hoặc thông qua bản sao từ thư điện tử nếu sở Tư pháp chưa có cổng thông tin về dữ liệu này. Còn đối với các tài sản được chủ sở hữu báo mất với văn phòng đăng ký đất thì văn phòng đăng ký đất nơi tiếp nhận hồ sơ sẽ phát hành thông báo về tình trạng mất giấy chứng nhận đến các phòng công chứng để cập nhật thông tin tài sản. Các thông tin về tài sản ngăn chặn bao gồm thông tin về chủ sở hữu, thông tin về hiệu lực ngăn chặn và các thông tin về thuộc tính tài sản được quy định Luật Công chứng 2014 (Quốc hội khóa 13, 2014) dưới dạng hệ thống cơ sở dữ liệu chia sẻ thông tin về nguồn gốc tài sản, tình trạng giao dịch của tài sản và các nghiệp vụ liên quan tài sản ngăn chặn do Ủy ban nhân dân cấp tỉnh xây dựng, vận hành và các tổ chức hành nghề công chứng khai thác.

Mô hình kiến trúc đề xuất

Quản lý tài sản ngăn chặn cần quản lý được thông tin của tài sản ngăn chặn, tài sản giải tỏa và tài sản giao dịch. Thông tin tài sản ngăn chặn như là thông tin về việc ngừng, tạm ngừng giao dịch, do các cơ quan quản lý nhà nước cấp thông tin bằng văn bản. Tài sản giải tỏa là các thông tin về chấm dứt, chấm dứt tạm ngừng giao dịch do tòa án nhân dân các cấp thông tin bằng văn bản đối với các tài sản ngăn chặn. Tài sản giao dịch là các thông tin về tài sản đã tham gia vào giao dịch tại các đơn vị công chứng trên địa bàn bao gồm động sản và bất động sản.

Dựa trên các yêu cầu về nghiệp vụ và yêu cầu minh bạch hóa và an toàn thông tin, chúng tôi đề xuất mô hình quản lý tài sản ngăn chặn dựa trên nền tảng một mạng blockchain Hyperledger Fabric như hình 2. Mạng blockchain được xây dựng dựa trên 3 host, mỗi host là một tổ chức riêng biệt, bao gồm các thành phần sau: 2 peer, 1 CA, 1 orderer. Trên mạng này chúng tôi thiết lập một kênh duy nhất với tên là agchain và sử dụng cơ chế đồng thuận Kafka.



Hình 2. Mô hình kiến trúc mạng blockchain Hyperledger Fabric đề xuất

Chúng tôi biểu diễn các nghiệp vụ quản lý tài sản ngăn chặn thông qua ngôn ngữ mô hình hóa (Modeling language) trong tập tin CTO theo định dạng của Hyperledger Composer. Tập tin CTO này bao gồm các định nghĩa dữ liệu (concept), các thành phần tham gia (participant), các tài sản (asset) và các giao dịch (transaction). Ba thành phần quan trọng nhất trong tập tin CTO là các thành phần tham gia, các tài sản và các giao dịch. Chúng tôi định nghĩa 2 thành phần tham gia chính là người dùng đến từ sở Tư pháp và người dùng đến từ phòng công chứng. Về tài sản, chúng tôi khai báo các tài sản sau đây: (a) tài sản là bất động sản hoặc động sản bao gồm các thông tin như mã tài sản, tên tài

sản, thông tin mô tả tài sản, trạng thái tài sản, phòng công chứng thực hiện giao dịch…; (b) tài sản ngăn chặn bao gồm các thông tin mã tài sản, người dùng thực hiện giao dịch ngăn chặn, đơn vị ban hành quyết định ngăn chặn, thông tin về thời gian ngăn chặn…; (c) tài sản giải tỏa cùng các thông tin mã tài sản, người dùng thực hiện giao dịch giải tỏa, đơn vị ban hành quyết định giải tỏa, số quyết định giải tỏa…; (d) các hợp đồng giao dịch tại các phòng công chứng bao gồm các thông tin như luật định. Chúng tôi cũng định nghĩa 3 giao dịch chính là thêm tài sản, thêm tài sản ngăn chặn và giao dịch giải tỏa tài sản ngăn chặn như hình 3.

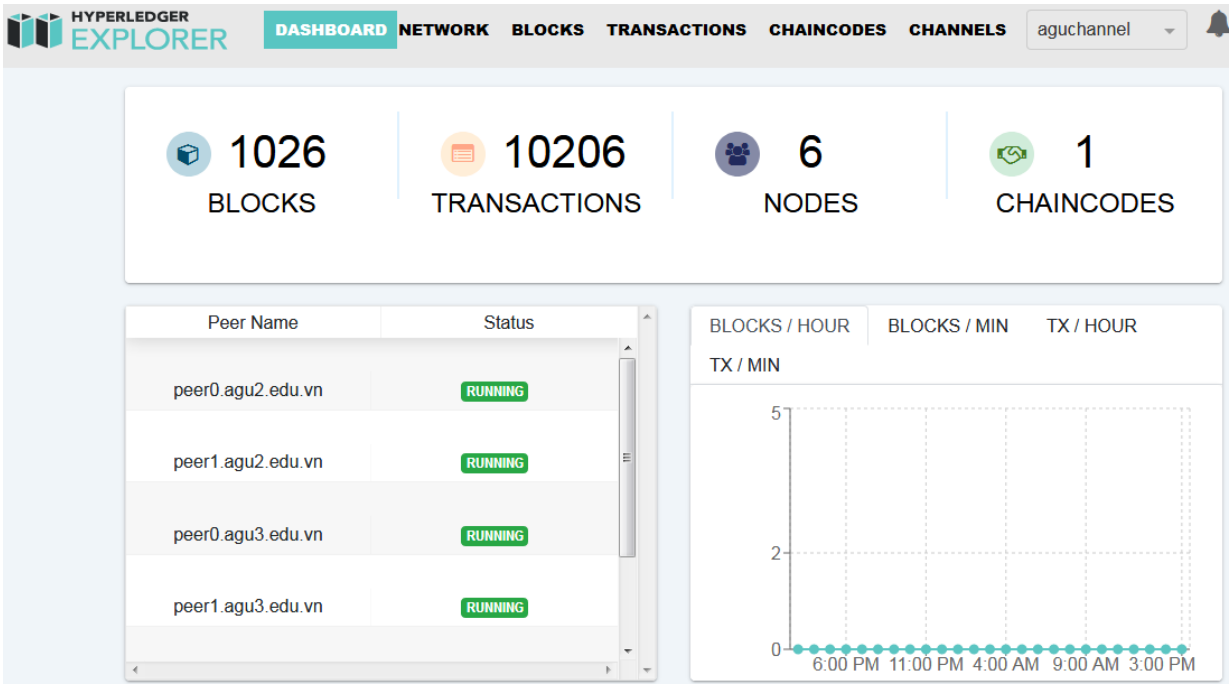
(a) các bước thực hiện giao dịch thêm tài sản ngăn chặn

(b) các bước thực hiện giao dịch giải tỏa tài sản ngăn chặn

Hình 3. Các bước thực hiện giao dịch thêm và giải tỏa tài sản ngăn chặn

IV. KẾT QUẢ THỰC NGHIỆM

Để xây dựng mạng blockchain Hyperledger Fabric như hình 2, chúng tôi sử dụng 3 chủ máy ảo. Cấu hình của mỗi máy chủ ảo như sau: 6 vCPU Intel Xeon 3.07GHz, 8G RAM. Băng thông kết nối 3 máy chủ áo là 10 Gbps. Mỗi máy chủ ảo được sử dụng để chạy 2 peer, 1 orderer, 1 zookeeper, 1 kafka, 1CA. Mạng blockchain được quản lý thông qua giao diện Hyperledger Explorer như hình 4.



Hình 4. Giao diện quản lý mạng blockchain đề xuất bằng Hyperledger Explorer

Trước khi triển khai mô hình nghiệp vụ quản lý tài sản ngăn chặn trên hệ thống mạng blockchain Fabric, chúng tôi tiến hành đánh giá hiệu suất mạng blockchain đề xuất theo quy trình đề xuất của Thakkar (2018). Để đánh giá hiệu suất mạng, một hợp đồng thông minh (chaincode) mẫu được triển khai với hai giao dịch cơ bản ghi và đọc dữ liệu vào sổ cái. Các thông số cấu hình mạng blockchain mà chúng tôi sử dụng để đánh giá như ở bảng 1.

Bảng 1. Các thông số cấu hình thực nghiệm đánh giá hiệu suất mạng blockchain

Số kênh	Độ phức tạp của giao dịch	Tên CSDL trạng thái	Tài nguyên của Host	Endorserment Policy	Kích thước của khối	Block Timeout
1	1 KV write	CouchDB	6 vCPU, 10 Gbps link	3-of	99MB	2s

Trong kịch bản mà chúng tôi sử dụng số giao dịch là 1000 (tx =1000), hai giao dịch ghi (open) và đọc (query) dữ liệu trên chuỗi khối được đánh giá hiệu suất. Chúng tôi sử dụng công cụ đánh giá hiệu suất Caliper tương tự như nghiên cứu của Thakkar để phân tích số lượng giao dịch được thực hiện thành công trong 1 giây (Throughput), độ trễ tối đa (Max Delay), độ trễ tối thiểu (Min Delay), độ trễ trung bình (Avg Delay), Số lượng giao dịch thành công (Succ), số lượng giao dịch thất bại (Fail), tốc độ gửi (Send Rate). Kết quả đánh giá hiệu suất được thể hiện trong bảng 2.

Bảng 2. Kết quả đánh giá hiệu hiệu của giao dịch ghi và đọc trên sổ cái với 1000 giao dịch

Test	Name	Succ	Fail	Send Rate	Max Delay	Min Delay	Avg Delay	Throughput
1	open	1000	0	50.1 tps	1.03 s	0.23 s	0.48 s	49.4 tps
2	query	1000	0	101.0 tps	0.13 s	0.01 s	0.02 s	100.0 tps

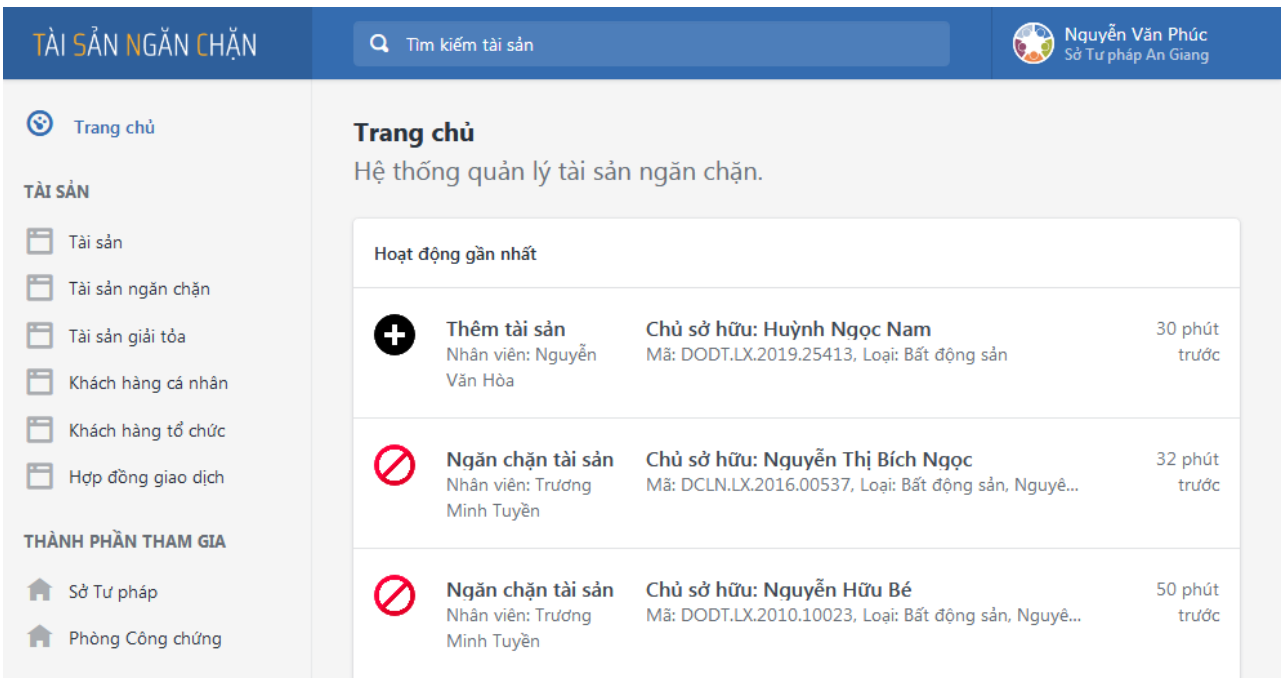
Ngoài ra, công cụ Caliper cũng phân tích mức độ sử dụng tài nguyên phần cứng như bộ nhớ, bộ xử lý, băng thông mạng và ghi và đọc đĩa cứng được sử dụng khi tiến hành thực hiện kịch bản đã đưa ra. Kết quả phân tích về sử dụng tài nguyên của kịch bản thử nghiệm được trình bày trong bảng 3.

Bảng 3. Kết quả phân tích về sử dụng tài nguyên của kịch bản thử nghiệm với 1000 giao dịch

Name	Memory (max)	Memory (avg)	CPU (max)	CPU (avg)	Traffic In	Traffic Out	Disc Read	Disc Write
peer1	102.0MB	87.7MB	30.61%	25.57%	750.4KB	732.8KB	0B	6.9MB
peer0	100.0MB	86.7MB	32.42%	25.68%	751.6KB	735.4KB	0B	6.9MB
couchdb1	178.8MB	173.2MB	69.55%	54.82%	116B	0B	0B	2.3MB
couchdb0	180.2MB	175.0MB	76.71%	49.81%	116B	0B	0B	2.2MB
ca	22.2MB	22.2MB	0.00%	0.00%	116B	0B	0B	0B
orderer	70.4MB	58.7MB	13.92%	10.19%	2.4MB	738.8KB	0B	5.4MB
kafka	466.7MB	441.8MB	225.75%	68.25%	116B	0B	0B	24.0KB
zookeeper	105.9MB	104.2MB	2.28%	0.43%	116B	0B	0B	0B

Kết quả đánh giá hiệu suất mạng blockchain và yêu cầu về sử dụng tài nguyên phần cứng cho thấy mạng blockchain đề xuất đáp ứng tốt yêu cầu về quy mô của hệ thống quản lý tài sản ngăn chặn cho nhiều tỉnh thành vì theo tìm hiểu của chúng tôi thì trừ 2 thành phố lớn là Hà Nội và TP. HCM, trung bình mỗi tỉnh thành có khoảng từ 20 đến 30 phòng công chứng.

Các nghiệp vụ quản lý tài sản ngăn chặn đã được xây dựng cho 2 loại người dùng chính ở các phòng công chứng và sở Tư pháp. Nghiệp vụ chính của 2 loại người dùng này là quản lý các tài sản, tài sản ngăn chặn, tài sản giải tỏa thông qua thao tác thêm và chuyển đổi trạng thái tài sản. Ngoài ra hệ thống còn cho phép quản lý các văn phòng công chứng, các hợp đồng giao dịch tài sản… Hệ thống được phát triển dưới dạng ứng dụng web và thực hiện các giao dịch trên trên chuỗi khối thông qua các lời gọi web API. Giao diện chính của ứng dụng như ở hình 5.



Hình 5. Giao diện chính của hệ thống quản lý tài sản ngăn chặn

V. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Chúng tôi vừa trình bày giải pháp quản lý tài sản ngăn chặn trong nghiệp vụ công chứng trên nền tảng công nghệ blockchain. Chúng tôi xây dựng mạng blockchain phân quyền với Hyperledger Fabric với 6 peer, 3 CA, 3 orderer và một chaincode trên 3 máy chủ ảo. Chúng tôi cũng đã tiến hành đánh giá hiệu suất mạng blockchain và tần suất sử dụng tài nguyên phần cứng trước khi tiến hành xây dựng giải pháp quản lý tài sản ngăn chặn. Giải pháp này cũng được triển khai thử nghiệm tài các phòng công chứng. Trong tương lai chúng tôi sẽ cải tiến hiệu suất mạng blockchain để có thể mở rộng quy mô sử dụng giải pháp cho nhiều phòng công chứng.

TÀI LIỆU THAM KHẢO

[1] Quốc hội khóa 11, Luật Công chứng 2006.

[2] Quốc hội khóa 13, Luật Công chứng 2014.

[3] Bộ Tư pháp (2014), Công văn 500/BTP-BTTP V/v phối hợp thực hiện một số giải pháp nâng cao hiệu quả hoạt động của công chứng.

[4] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" In 2017 IEEE International Congress on Big Data, 2017.

[5] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[6] G. Wood, Ethereum: A secure decentralised generalised transaction ledger.," Ethereum Project Yellow Paper, 2014.

[7] Frederik Armknecht, Ghassan O. Karame, Avikarsha Mandal, Franck Youssef, and Erik Zenner, "Ripple: Overview and Outlook" In Trust and Trustworthy Computing. pp: 163-180, 2015.

[8] C. Cachin. Architecture of the hyperledger blockchain fabric, 2016.

[9] Kleinaki A. S, Mytis-Gkometh P, Drosatos G, Efraimidis PS, Kaldoudi E., "A blockchain based notarization service for biomedical knowledge retrieval," in Comput Struct Biotechnol Journal, 2018; pp: 288-297.

[10] George Drosatos, Eleni Kaldoudi, "Blockchain Applications in the Biomedical Domain: A Scoping Review," in Comput Struct Biotechnol Journal, 2019; pp: 229-240.

[11] Wolfgang Gräther, Sabine Kolvenbach, Rudolf Ruland, "Blockchain for Education: Lifelong Learning Passport," in Proceedings of 1st ERCIM Blockchain Workshop, 2018.

[12] Duc-Hiep Nguyen, Dinh-Nghia Nguyen-Duc, Nguyen Huynh-Tuong, Hoang-Anh Pham, "CVSS: A Blockchainized Certificate Verifying Support System," in Proceedings of the 9th International Symposium on Information and Communication Technology (SoICT), 2018

[13] Haikel Magrahi, Nouha Omrane, Olivier Senot, Rakia Jaziri, "NFB: A Protocol for Notarizing Files over the Blockchain," in Proceedings of the 9th International Conference on New Technologies, Mobility and Security, 2018.

[14] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in Proc. 13th EuroSyst. Conf., 2018.

[15] Mettler, M., "Blockchain technology in healthcare: The revolution starts here," In: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) IEEE, 2016, pp. 1-3.

[16] Peterson, K., Deeduvanu, R., Kanjamala, P., Boles, K., "A blockchain-based approach to health information exchange networks," In: Proc. NIST Workshop Blockchain Healthcare, vol. 1. pp. 1-10.

[17] Patel, V., A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Inf, 2018.

[18] Chiang, C. W., Betanzos, E., Savage, S., 2018. Blockchain for trustful collaborations between immigrants and governments. In: Proceedings - Conference on Human Factors in Computing Systems.

[19] Fran Casinoa, Thomas K. Dasaklisb, Constantinos Patsakisa. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics 36 (2019) 55-81.

[20] Bdiwi, R., De Runz, C., Faiz, S., Cherif, A. A., Towards a New Ubiquitous Learning Environment Based on Blockchain Technology. In: Proceedings - IEEE 17th International Conference on Advanced Learning Technologies, ICALT 2017, pp. 101-102.

[21] Turkanović, M., Holbl, M., Košič, K., Heričko, M., Kamišalić, A., EduCTX: A blockchain-based higher education credit platform. IEEE Access 6, 2018, 5112-5127.

[22] Devine, P., Blockchain learning: can crypto-currency methods be appropriated to enhance online learning? ALT Online Winter Conference, 2015.

[23] Xu, Y., Zhao, S., Kong, L., Zheng, Y., Zhang, S., Li, Q., ECBC: a high-performance educational certificate blockchain with efficient query. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10580 LNCS, pp. 288-304, 2017.

[24] Christidis, K., Devetsikiotis, M., Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292-2303, 2016.

[25] IPFS: a new peer-to-peer hypermedia protocol, 2016.https://ipfs.io.

[26] Lemieux, V. L., Trusting records: is blockchain technology the answer? Records Manage. J. 26 (2), 110-139, 2016.

[27] Leiding, B., Norta, A., Mapping requirements specifications into a formalized lockchain-enabled authentication protocol for secured personal identity assurance. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10646 LNCS, pp. 181-196, 2017.

[28] Augot, D., Chabanne, H., Chenevier, T., George, W., Lambert, L., A user-centric system for verified identities on the bitcoin blockchain. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10436 LNCS, pp. 390-407, 2017.

[30] Buchmann, N., Rathgeb, C., Baier, H., Busch, C., Margraf, M., Enhancing breeder document long-term security using blockchain technology. In: 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), vol. 2, ISSN 0730-3157, 744-748, 2017.

[31] Roberts, J. J., Microsoft and Accenture Unveil Global ID System for Refugees, http://fortune.com/2017/06/19/id2020-blockchain-microsoft/.

[32] Deitz, J., Decentralized Governance Whitepaper, 2014, http://distributed-autonomous-society.quora.com/Decentralized-Governance-Whitepaper.

[33] Schiener, D., Liquid Democracy: True Democracy for the 21st Century, 2014, https://medium.com/organizer-sandbox/liquid-democracy-true-democracy-for-the-21stcentury-7c66f5e53b6f.

[34] Deloitte Development LLC, Will blockchain transform the public sector? Blockchain basics for government, 2017.

[35] Chiang, C. W., Betanzos, E., Savage, S., Blockchain for trustful collaborations between immigrants and governments. In: Proceedings - Conference on Human Factors in Computing Systems, 2018.

[36] Olnes, S., Jansen, A., Blockchain technology as s support infrastructure in e-government. In: International Conference on Electronic Government Springer, pp. 215-227, 2017.

[37] Sullivan, C., Burger, E., E-residency and blockchain. Computer Law Secur. Rev. 33 (4), 470-481, 2017.

[38] Pokrovskaia, N. N., Tax financial and social regulatory mechanisms within the knowledge-driven economy. Blockchain algorithms and fog computing for the efficient regulation. In: Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017, pp. 709-712, 2017.

[39] Wijaya, D. A., Liu, J. K., Suwarsono, D. A., Zhang, P., A new blockchain-based value-added tax system. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10592. LNCS, pp. 471-486, 2017.

[40] Parth Thakkar, Senthil Nathan, Balaji Viswanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," in 26th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, pp 264-276, 2018.

A SOLUTION TO MANAGE BLOCKED ASSET ON TECHNOLOGY BLOCKCHAIN

Minh Tuyen Truong, Hoang Tung Nguyen, Hoang Anh Le, Van Hoa Nguyen

***ABSTRACT**: Blockchain technology has been developed in recent years and there are many researches to improve this technology as well as to build applications in many areas such as finance, health, education and especially digital government. Blockchain technology has an outstanding feature in securing information based on decentralized data platforms and storage structures in blockchains. This is the basis to combat information fraud and improve authentication performance based on decentralized architecture and shared ledger. Blockchain technology can create a safe and flexible ecosystem that is suitable for public services. This technology also provides transparency by creating digital evidence, asset trading contracts. In this article, we propose solutions to manage blocked asset on blockchain technology through Hyperledger Fabric platform. Our solution contributes to improving the effectiveness of management, administration and simple notarization procedures in notary offices and state management agencies. Experiences shows that our solution hase high efficiency and has potential to deploy in notary offices.*