Khả năng ứng dụng công nghệ blockchain trong việc lưu trữ chứng cứ hỗ trợ điều tra số

Vũ Quang Minh[a], Lê Thị Anh[b*]

Tóm tắt:

Hiện nay, chứng cứ số đã được chấp nhận, sử dụng thường xuyên bởi các cơ quan tư pháp trên toàn cầu. Bằng chứng kỹ thuật số hay chứng cứ số ngày càng thể hiện vai trò quan trọng trong việc truy tìm, đánh giá và kết luận tội phạm. Trong chứng cứ số, tính toàn vẹn, tính xác thực và khả năng được chấp nhận luôn là những ưu tiên cao nhất. Điều này đặt ra nhu cầu về việc cần có một nhật ký ghi lại quá trình xử lý chứng cứ số, có thể dùng để xác minh sự giả mạo chứng cứ, những vi phạm trong quá trình xử lý chứng cứ số, đồng thời đảm bảo những dấu vết giả mạo này không thể bị xóa bởi các bên liên quan. Công nghệ blockchain với những tính năng của nó có thể làm cho quy trình theo dõi, quản lý việc xử lý chứng cứ số hiệu quả và đáng tin cậy hơn. Bài báo này đánh giá khả năng ứng dụng công nghệ blockchain và đề xuất mô hình lưu trữ, quản lý chứng cứ số, tận dụng các lợi thế của công nghệ chuỗi khối, giúp các bên liên quan theo dõi các giao dịch chứng cứ số trong suốt quá trình xử lý hợp pháp, đồng thời đảm bảo tính toàn vẹn và không thể giả mạo của chứng cứ số.

Từ khóa: *blockchain, chứng cứ số, không thể giả mạo, tính toàn vẹn, tính xác thực*

---

[a] Phòng Thí nghiệm trọng điểm an toàn thông tin; 03 ngõ Phan Chu Trinh, Hoàn Kiếm, Hà Nội, Việt Nam. e-mail: vuquangminh2631990@gmail.com

[b] Phòng Thí nghiệm trọng điểm an toàn thông tin; 03 ngõ Phan Chu Trinh, Hoàn Kiếm, Hà Nội, Việt Nam. e-mail: leanh41@gmail.com

[*] Tác giả chịu trách nhiệm chính.

Tạp chí Khoa học Đại học Đông Á, Tập 1, Số 4, Tháng 12.2022, tr. 2-13

ISSN: 2815 - 5807

Blockchain Technology in Evidence Storage Supporting for Digital Forensic

Vu Quang Minh, Le Thi Anh

Abstract:

Digital evidence (DE) has been accepted and often used by judicial authorities worldwide due to its role in tracing, evaluating, and concluding crimes. In digital forensics, integrity, authenticity, and the admissibility of the digital proofs are always the highest priorities leading to the need for a log to record DE processing processes, and verify evidence tampering. Additionally, in handling of the digital proofs, violation, and tampering traces cannot be erased by the involved stakeholders. Blockchain technology (BC) can make the process of tracking and managing the handling of digital evidence more efficient and reliable. This article evaluates the applicability of Blockchain technology, and proposes a model for storing and managing the digital proofs. Moreover, BC will assist stakeholders in tracking DE transactions during the legal process while ensuring the integrity, and no tampering of DE.

Key words: *authenticity, blockchain, digital evidence, no tampering, integrity*

Received: 27.09.2022; Accepted: 23.11.2022; Published: 31.12.2022

ISSN: 2815 - 5807

Dong A University Journal of Science, Vol. 1, No. 4, Dec 2022, pp. 2-13

Giới thiệu

Tầm quan trọng của chứng cứ số

Sự phát triển mạnh mẽ của công nghệ số, công nghệ thông tin hiện nay kéo theo sự bùng nổ của tội phạm công nghệ cao với nhiều hình thức, kỹ thuật tinh vi và quy mô ngày càng mở rộng. Khi các thiết bị kỹ thuật số như máy tính, điện thoại di động và thiết bị định vị toàn cầu GPS (Global Positioning System) trở nên phổ biến, việc phân tích bằng chứng kỹ thuật số ngày càng trở nên quan trọng đối với việc điều tra và truy tố nhiều loại tội phạm vì nó có thể tiết lộ thông tin về tội ác đã thực hiện, sự di chuyển của nghi phạm và các đồng phạm, giúp xác định những gì đã xảy ra làm ảnh hưởng tới hệ thống, giúp phát hiện, điều tra nguyên nhân sự cố, các hành vi, nguồn gốc của các vi phạm xảy ra đối với hệ thống,… Nếu được xác định, thu thập và phân tích một cách hợp lý, chứng cứ số góp phần quan trọng trong việc kết luận điều tra số, áp dụng các chế tài xử phạt với các hành vi phạm pháp.

Chứng cứ số có thể là email, tin nhắn, các tệp tin, văn bản, hình ảnh của các ổ cứng vật lý… được trích xuất từ ổ đĩa, các giao dịch, các tệp tin âm thanh, hình ảnh. Những nơi có thể tìm thấy chứng cứ số trong một hệ thống thường là các thiết bị như: router, firewall, server, các thiết bị máy tính, điện thoại cầm tay, thiết bị nhúng, các phần mềm ứng dụng, các phần mềm giám sát, nhật ký hệ thống, lịch sử truy cập internet, các giao dịch trong cơ sở dữ liệu, lưu lượng mạng, các bản sao lưu, bản nén (Ćosić, 2010),…

Đặt vấn đề

Một trong những vấn đề chung của mọi cuộc điều tra, trong đó có điều tra số, là việc bảo vệ chứng cứ trong suốt quá trình điều tra. Trong quá trình điều tra, chứng cứ số được chuyển giao cho nhiều cơ quan tiến hành phân tích pháp y, xử lý,… Việc bảo vệ chứng cứ bằng tất cả các biện pháp có thể ngày càng trở nên quan trọng, đảm bảo chứng cứ số không bị giả mạo, đáng tin và được chấp nhận tại các phiên tòa.

Chứng cứ số chỉ được xem là hợp lệ, được chấp nhận nếu đáp ứng đầy đủ các tiêu chí sau: *tính toàn vẹn, tính xác thực, độ tin cậy*.

Ngoài ra, hai khía cạnh chính để bằng chứng được xem là hợp lệ:

- Đầu tiên là *khía cạnh pháp lý, hợp lệ của bằng chứng, độ chính xác và tính toàn vẹn của bằng chứng như thế nào*.

- Thứ hai, *khía cạnh kỹ thuật của bằng chứng, tính minh bạch, khả năng giải thích chuỗi xử lý bằng chứng*, ví dụ như những ai đã truy cập vào chứng cứ trước khi nó được xem xét tại các phiên tòa.

So với chứng cứ vật lý thì chứng cứ số khó nắm bắt và lưu trữ hơn vì những đặc tính như dễ giả mạo, dễ truyền dẫn, chia sẻ,…

Chuỗi xử lý chứng cứ là việc ghi lại mọi thao tác, hành động liên quan tới chứng cứ số và tài liệu hóa lịch sử lưu trữ các chứng cứ số kể từ khi nó được tạo ra. Chuỗi xử lý chứng cứ là bước quan trọng, giúp xác minh xem chứng cứ được tìm ra và bảo quản đúng quy trình đến khi nó được xem xét tại các phiên tòa. Điều tối quan trọng là phải chứng minh được, chứng cứ số không bị thay đổi trong suốt quá trình điều tra.

Chứng cứ số sau khi được thu thập cần được ghi lại, mã hóa bằng các thuật toán băm mật mã SHA256 để đảm bảo tính toàn vẹn chứng cứ, sau đó chứng cứ được lưu trữ trong một môi trường an toàn để phục vụ công tác điều tra, phân tích sau này. Đây là việc làm rất quan trọng bởi vì nó phải đảm bảo được rằng những chứng cứ thu được ban đầu cần phải đảm bảo được tính toàn vẹn. Trước khi bắt đầu điều tra thì người thực hiện nhiệm vụ phân tích điều tra sẽ kiểm tra độ tin cậy của chứng cứ dựa vào thông tin mà các chuỗi SHA256 cung cấp nhằm tránh việc gian lận và cài đặt, làm giả các chứng cứ đánh lạc hướng điều tra.

Trong quá trình điều tra, bằng chứng và dữ liệu số được xử lý theo nghiệp vụ qua nhiều giai đoạn, dễ dẫn đến khả năng chứng cứ số không giữ được tính toàn vẹn, tính xác thực, thậm chí có thể bị giả mạo. Việc đảm bảo tính bảo mật, tính toàn vẹn, xác thực của chứng cứ số đóng vai trò vô cùng quan trọng trong công tác điều tra số. Những dự đoán, kết luận của cơ quan điều tra, tòa án,… sẽ bị ảnh hưởng nghiêm trọng nếu như chứng cứ số bị thay đổi, giả mạo. Điều này đặt ra bài toán cần có một giải pháp công nghệ đảm bảo cho việc lưu trữ bảo mật, theo dõi và quản lý chứng cứ để hỗ trợ hiệu quả công tác điều tra số, đảm bảo tính toàn vẹn, xác thực của chứng cứ số.

Trong bài báo này, chúng tôi sẽ xem xét khả năng ứng dụng và đề xuất mô hình lưu trữ, quản lý chứng cứ số, tận dụng các lợi thế của công nghệ chuỗi blockchain, một trong những công nghệ mới nổi với những đặc điểm phù hợp cho bài toán lưu trữ bảo mật chứng cứ số.

Những lợi thế của công nghệ blockchain trong việc lưu trữ, theo dõi và quản lý chứng cứ số

Một số yêu cầu cần được đáp ứng của chứng cứ số

Trước tiên, chúng ta cần biết rằng, chứng cứ số phục vụ quá trình điều tra cần đáp ứng được một số đặc tính sau:

Tính toàn vẹn: Chứng cứ số cần phải đảm bảo tính toàn vẹn, không bị mất mát, thay đổi trong quá trình điều tra. Chứng cứ số có thể đến từ nhiều nguồn khác nhau như ổ cứng máy tính, email, nhật ký chat, nhật ký sử dụng internet, thẻ nhớ, camera,… Quy trình bảo quản tính toàn vẹn của chứng cứ số là một nhiệm vụ quan trọng mà các điều tra số phải xem xét và luôn đặt lên ưu tiên hàng đầu.

Tính xác thực: Các thực thể tương tác với chứng cứ số cần chứng minh được định danh của mình. Tùy vào định danh của các bên liên quan mà quyền truy cập, xử lý chứng cứ số được xác định tương ứng.

Khả năng theo dõi được: Từ khi được thu thập, lưu trữ đến khi được đưa ra như một bằng chứng trong tòa án hoặc kết luận điều tra số, chứng cứ số trải qua nhiều bước xử lý. Quá trình này cần được theo dõi, giám sát để đảm bảo tính hợp pháp, bảo mật của dữ liệu. Lý do là vì trong quá trình điều tra, chứng cứ có thể được ngụy tạo, làm giả, thay đổi hoặc xóa… bởi tác nhân nào đó bị thao túng bởi các tổ chức tội phạm,… Ngoài ra, trong quá trình điều tra, không phải tất cả các bên liên quan đều được quyền truy cập, xử lý chứng cứ số. Vì vậy, khả năng theo dõi quy trình xử lý chứng cứ số giúp đảm bảo tính pháp lý và phát hiện các sai phạm trong quá trình điều tra số.

Tính bảo mật: Chứng cứ số cần được lưu trữ an toàn, đảm bảo yếu tố bí mật, tránh để lộ lọt thông tin ra ngoài, dẫn đến tội phạm có thể phát hiện, đề cao cảnh giác, xóa dấu vết hoặc bỏ trốn,…

Đặc điểm của công nghệ blockchain

Vậy tại sao công nghệ blockchain lại phù hợp trong việc lưu trữ, theo dõi và quản lý chứng cứ số?

Bản chất của blockchain là một công nghệ lưu trữ dữ liệu theo dạng chuỗi khối được liên kết với nhau, dựa trên công nghệ sổ cái phân tán, được lập trình để ghi lại và theo dõi các giá trị dữ liệu. Điểm khác biệt của blockchain so với việc lưu trữ dữ liệu thông thường ở chỗ, thay vì chỉ ghi thông tin vào một cuốn sổ cái, hoặc một hệ thống duy nhất do một người, một nhóm người hoặc một tổ chức nào đó nắm giữ, thì công nghệ blockchain sẽ giúp cho cuốn sổ cái này được công khai và nhiều người có thể cùng giám sát những thông tin được ghi và sửa đổi trên cuốn sổ cái. Điều này giúp cho dữ liệu được lưu trữ minh bạch và chính xác hơn.

Quan trọng hơn, công nghệ blockchain sở hữu những đặc điểm hoàn toàn phù hợp với các đặc tính và yêu cầu lưu trữ của chứng cứ số.

- Đầu tiên là do *tính bất biến và tin cậy của dữ liệu* trong công nghệ blockchain

Blockchain được thiết kế để chống lại việc thay đổi của dữ liệu. Một khi dữ liệu đã được mạng lưới chấp nhận thì sẽ không thể nào xóa hoặc thay đổi được. Đó chính là tính bất biến của dữ liệu. Sự thay đổi chỉ có thể xảy ra bằng cách lưu trữ một khối mới, chỉ ra rằng dữ liệu X đã chuyển thành Y vào thời gian nào đó. Mọi sự thay đổi, mọi tiến trình, hoạt động đều được ghi lại trong blockchain. Ngoài ra, sự thay đổi đó còn phải thỏa mãn các hợp đồng thông minh và cơ chế đồng thuận phi tập trung trong blockchain. Tính chất

này của công nghệ blockchain đáp ứng tiêu chí *tính toàn vẹn* của chứng cứ số và *khả năng theo dõi được* của quy trình xử lý chứng cứ số.

Mỗi khi một khối được tạo thành, dữ liệu được mã hóa bằng cách kết hợp giữa hàm băm và các thuật toán mã hóa bất đối xứng nên dữ liệu không thể thay đổi hay giả mạo được. Việc kết hợp giữa các thuật toán mã hóa và xác thực bởi nhiều máy tính thông qua các hợp đồng thông minh và cơ chế đồng thuận đảm bảo rằng, chúng ta có thể tin tưởng tuyệt đối vào từng khối trong chuỗi. Đó là tính đáng tin cậy của dữ liệu trong blockchain, phù hợp với tiêu chí *tính xác thực, chống giả mạo* của chứng cứ số.

Tính phân tán của dữ liệu: Khác với phương pháp sổ cái truyền thống, tệp cơ sở dữ liệu trong blockchain được lưu trữ trong một hệ thống được thiết kế phân quyền và phân tán đồng đẳng trong mạng lưới. Việc phân quyền thông tin này làm giảm khả năng giả mạo dữ liệu và tạo ra sự tin tưởng vào dữ liệu. Tất cả máy tính tham gia vào khối đều có một bản sao hợp lệ của chuỗi, vì vậy nếu sự thay đổi chỉ diễn ra trên một máy tính thì không có ý nghĩa gì. Hacker phải thực hiện giả mạo đồng loạt trên tối thiểu 51% các máy trong một khoảng thời gian ngắn, đó là một điều gần như không thể với một hệ thống lớn. Việc kết hợp giữa việc lưu trữ dữ liệu phân tán, mã hóa dữ liệu bằng hàm băm và thuật toán mã hóa bất đối xứng, hợp đồng thông minh và cơ chế đồng thuận đảm bảo *tính bảo mật* tuyệt đối cho dữ liệu nói chung và chứng cứ số nói riêng.

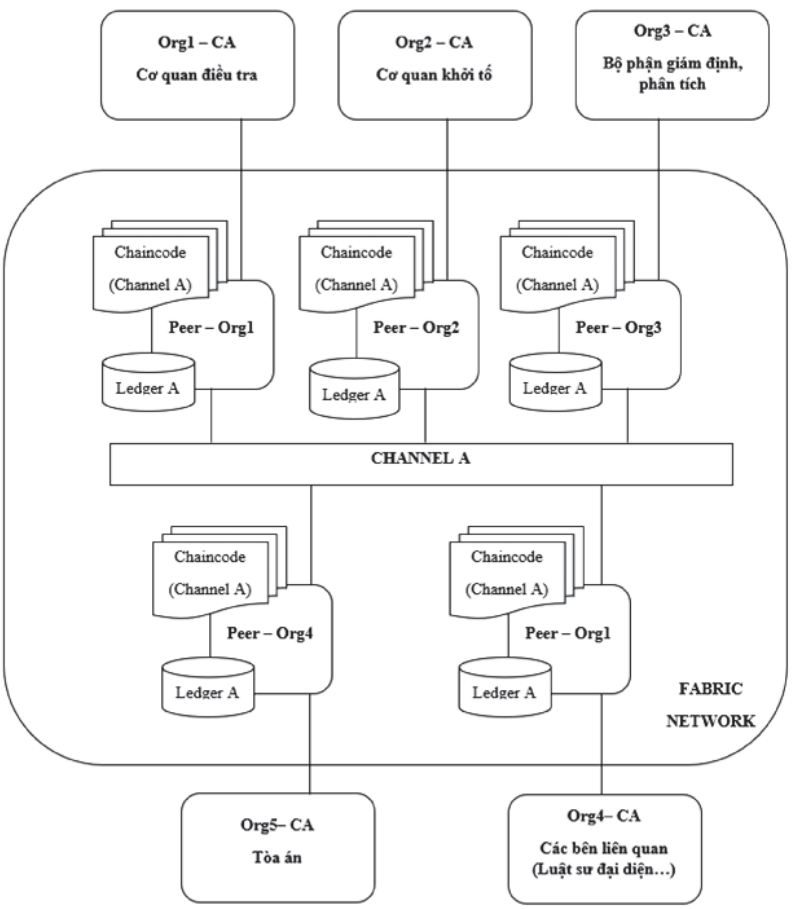
Tính minh bạch và bảo mật: blockchain là sự kết hợp hoàn hảo giữa tính minh bạch và bảo mật. Vì sao có thể nói như vậy? *Tính minh bạch* của blockchain thể hiện ở việc trong mạng lưới blockchain, khi một giao dịch diễn ra, mọi thành viên của mạng blockchain đều biết về việc giao dịch đó được thực hiện và phải có sự đồng thuận phi tập trung của mọi người về tính hợp lệ của giao dịch. Điều đó có nghĩa là trong mạng blockchain, khi bên A muốn chuyển chứng cứ số cho bên B, để giao dịch thành công, phải được sự đồng ý của tất cả các thành viên trong cơ chế đồng thuận phi tập trung, các thành viên của mạng lưới blockchain đều biết và xác nhận tính hợp lệ của giao dịch mà A chuyển cho B chứng cứ số nhưng thông tin cụ thể về giao dịch, về chứng cứ số đó là gì thì chỉ có A và B biết. A và B sử dụng cặp khóa công khai - riêng tư của mình để xem chi tiết thông tin giao dịch, các thành viên còn lại đều không thể xem chi tiết thông tin giao dịch. Vì vậy, giao dịch trong blockchain vẫn đảm bảo tính riêng tư, bảo mật. *Tính bảo mật* trong blockchain được tạo nên từ việc kết hợp giữa thuật toán mã hóa bất đối xứng sử dụng cặp khóa công khai - riêng tư và hàm băm cùng cơ chế đồng thuận phi tập trung để xác thực tính đúng đắn của giao dịch, cho phép giao dịch diễn ra. Thông tin về việc giao dịch đã diễn ra giữa A và B được lưu trữ phân tán và mãi mãi trong blockchain ở tất cả các node thành viên. Chính vì thế, chứng cứ số được lưu trữ trong blockchain vừa minh bạch vì các thành viên đều biết về việc xảy ra giao dịch nhưng cũng vừa đảm bảo yếu tố bí mật vì chỉ các bên liên quan trực tiếp đến giao dịch mới xem được thông tin cụ thể của chứng cứ số trong giao dịch.

- Phù hợp để giải quyết vấn đề

Như đã phân tích ở trên, công nghệ blockchain hoàn toàn phù hợp để lưu trữ, theo dõi và quản lý chứng cứ phục vụ công tác điều tra số. Công nghệ blockchain có những thuộc tính quan trọng, thiết yếu, cần thiết trong việc lưu trữ chứng cứ số. Chứng cứ số được lưu trữ bằng công nghệ blockchain có thể chứng minh được khả năng theo dõi trong quá trình điều tra. Tính xác thực của chứng cứ số được lưu trữ thông thường hoàn toàn dựa trên lòng tin vào các bên liên quan, còn công nghệ blockchain theo một mô hình chính xác tuyệt đối, loại bỏ sự tin tưởng cần thiết vào một bên thứ ba. Mô hình công nghệ blockchain dựa trên các hành động, giao dịch xảy ra đối với chứng cứ số. Mỗi một và mọi giao dịch, hành động đều được ghi lại vào sổ cái phân tán và được lưu trữ vĩnh viễn. Điều này giúp các bên tin tưởng tuyệt đối vào việc chứng cứ số được theo dõi chặt chẽ trong quá trình xử lý, đảm bảo đúng tính pháp lý và quy trình xử lý nghiệp vụ.

Mô hình đề xuất

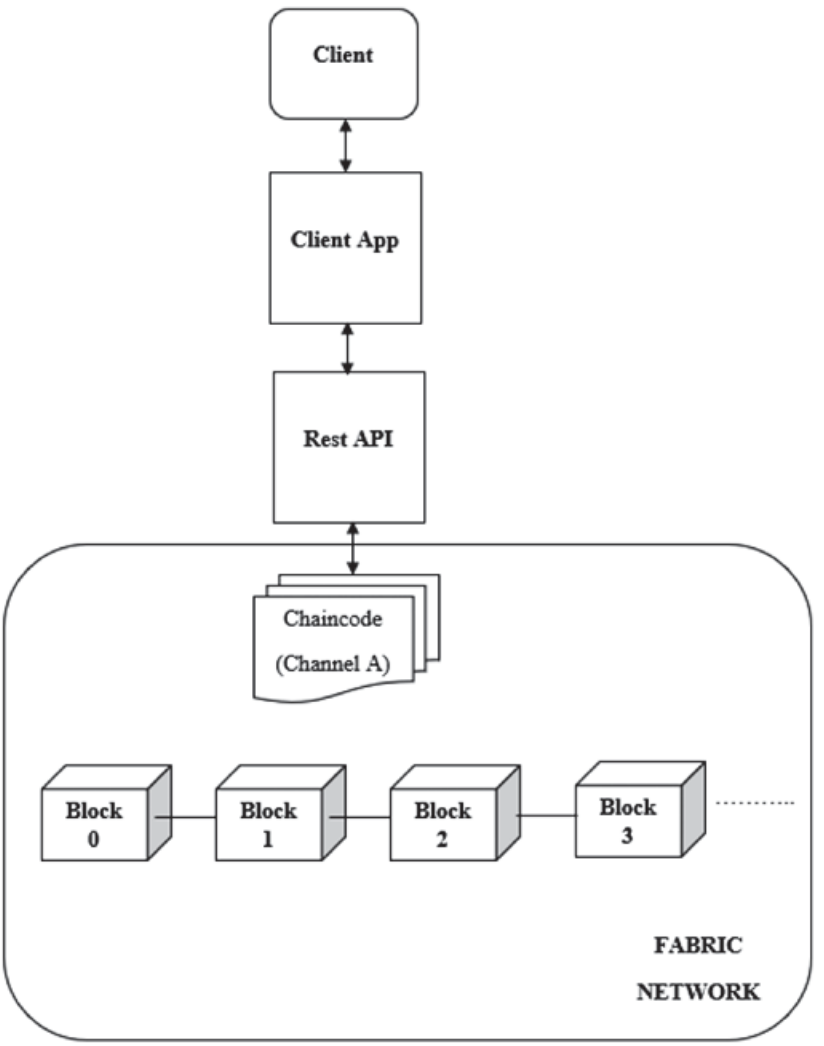
Quá trình điều tra, chuỗi xử lý pháp y số được thực hiện trong một môi trường an toàn, được kiểm soát chặt chẽ. Trong môi trường này, các chứng cứ số là các tài sản cần được bảo quản, bảo vệ, tránh mất mát, hỏng dữ liệu hoặc bị thay đổi, sửa, xóa, can thiệp trái phép từ các tác nhân không được phép. Chúng tôi đề xuất cấu trúc mô hình Hyperledger Fabric, giúp lưu trữ các thông tin cần thiết của chứng cứ số và chuỗi xử lý chứng cứ số.



Hình 1. Mô hình cấu trúc mạng Fabric lưu trữ, quản lý chứng cứ số

Mạng Hyperledger Fabric bao gồm nhiều tổ chức (org) như: cơ quan điều tra; cơ quan khởi tố; bộ phận giám định, phân tích;

các bên liên quan; tòa án;… tương tác lẫn nhau trong mạng. Mỗi tổ chức có cơ quan cấp chứng chỉ CA (Certificate Authority) giúp định danh tổ chức trong mạng và một hoặc nhiều nút ngang hàng Peer. Một mạng Fabric cũng có một Ordering Service được chia sẻ với tất cả các tổ chức trong mạng và thành phần này giúp xử lý, sắp xếp thứ tự giao dịch cho mạng lưới. Một tổ chức cũng tạo ra một node hoặc nhiều node (peer) để thay mặt thực hiện các hoạt động (transaction) cho tổ chức đó. Cụ thể, một peer node xác nhận các giao dịch được đề xuất trên mạng, lưu trữ và thực thi hợp đồng thông minh (chaincode) và lưu trữ bản sao cục bộ của sổ cái (ledger) để truy cập.



Hình 2. Mô hình tương tác giữa client và Fabric Network

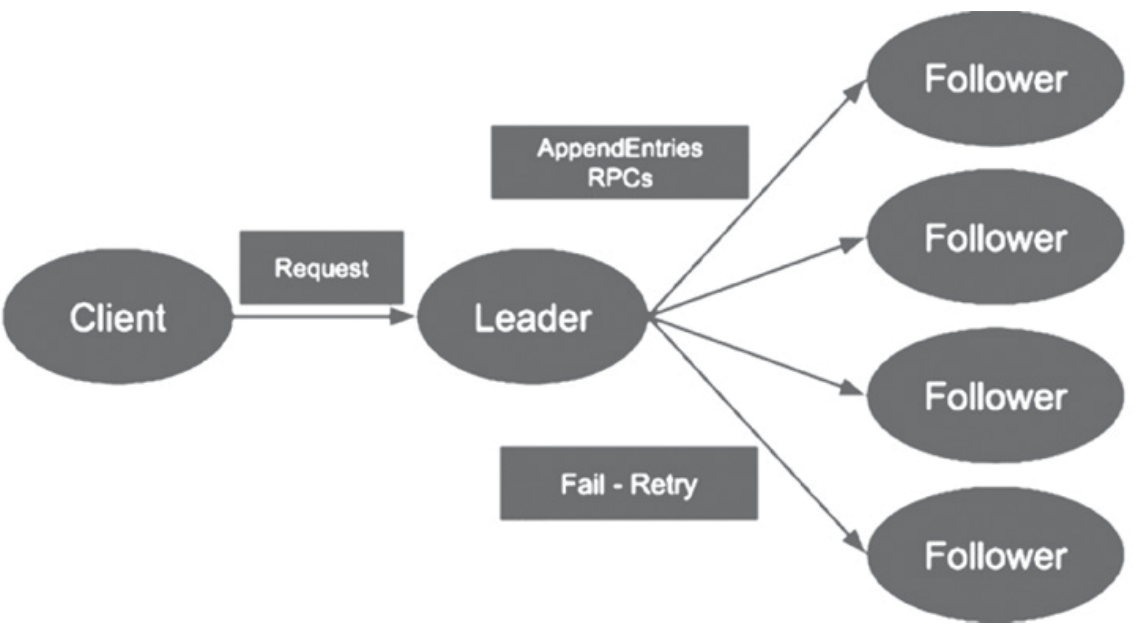
Các thành viên kết nối và tương tác với chuỗi điều tra, pháp y như đã chỉ ra trong hình 2 bên trên, sử dụng ứng dụng chuỗi điều tra số (Sadiku, 2017). Dữ liệu được chia sẻ thông qua các kênh xác định của Hyperledger Fabric. Fabric client tương tác với peer

node đọc sổ cái, thêm chaincode mới vào mạng hoặc đề xuất giao dịch mới. Một peer node thường chạy trên chính máy tính của nó.

Khi một chứng cứ số được tạo ra, nó có thể được chuyển đến cho nhiều node tham gia vào mạng lưới blockchain trong quy trình xử lý như nhân viên điều tra, nhân viên giám định, quan tòa,… Hợp đồng thông minh (Chaincode) được tạo ra dựa trên cơ chế đồng thuận để xử lý tự động các hành động giao dịch liên quan đến chứng cứ số trong mạng lưới blockchain và đảm bảo không có sự giả mạo chứng cứ. Mỗi một khối Block chứa một giao dịch của một chứng cứ số xác định.

Cơ chế đồng thuận phi tập trung mà chúng tôi đề xuất trong mô hình Hyperledger Fabric là cơ chế đồng thuận Raft. Raft là thuật toán đồng thuận được ra đời để giải quyết bài toán sao lưu log trong hệ thống phân tán, đảm bảo tính an toàn và nhất quán.

Cơ chế đồng thuận Raft dựa trên cơ chế Leader - Follower. Trong đó, để điều phối và thống nhất các bản sao lưu của sổ cái phân tán ở các node trong mạng lưới blockchain, Raft bầu ra một node làm Leader. Một node trở thành Leader nếu nhận được đa số vote từ các node còn lại. Sau khi hệ thống chọn ra được Leader, node này sẽ chịu trách nhiệm xử lý các request từ phía client và sao lưu dữ liệu dưới dạng log sang các node còn lại trong mạng blockchain. Trong trường hợp một node trong hệ thống gặp sự cố (crash, network,…) thì Leader sẽ gửi lại request cho đến khi tất cả các node Follower trong hệ thống thực hiện xong quá trình sao lưu log. Các node trong cụm Raft giao tiếp với nhau thông qua việc gửi các request sử dụng giao thức RPCs.



Hình 3. Cơ chế Leader-Follower trong thuật toán đồng thuận Raft

Trong mô hình được đề xuất, tùy vào các hành động giao dịch mà cơ chế đồng thuận cũng như vai trò của các bên trong cơ chế đồng thuận Raft sẽ được cấu hình trước để phù hợp về mặt pháp lý với từng trường hợp.

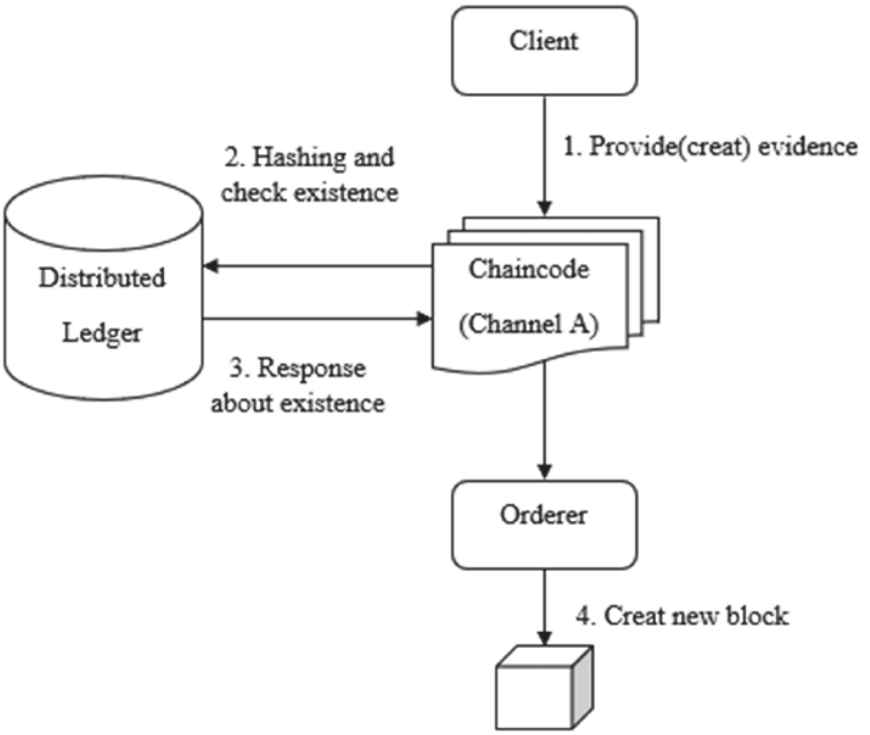
Ví dụ, đối với trường hợp cung cấp thêm chứng cứ số vào mạng blockchain, luật sư của bên A sẽ gửi request muốn cung cấp thêm chứng cứ số. Lúc này, một trong các bên cơ quan điều tra, cơ quan khởi tố và tòa án (vì theo tính pháp lý, chỉ một trong ba bên này mới đủ quyền công nhận tính hợp lệ của chứng cứ số) sẽ được chọn làm Leader khi có đủ số vote trong mạng. Các thành viên còn lại sẽ đóng vai trò Follower, theo quyết định của Leader.

Request của A sẽ được gửi đến Leader, ví dụ là cơ quan điều tra, sau khi cơ quan điều tra xác thực tính đúng đắn của chứng cứ số mới được cung cấp, cơ quan điều tra chấp nhận chứng cứ số đó và thêm chứng cứ số đó vào trong mạng lưới blockchain. Cơ quan điều tra đóng vai trò Leader sẽ sao lưu dữ liệu dưới dạng log sang các node Follower còn lại trong mạng lưới blockchain. Quá trình đồng thuận hoàn tất khi Leader hoàn tất quá trình sao lưu dữ liệu log của Leader sang các Follower.

Tóm lại, trong cơ chế đồng thuận Raft, khi một giao dịch muốn diễn ra, một trong các bên sẽ được chọn làm Leader để nhận request từ client và chịu trách nhiệm sao lưu log dữ liệu sang các log của Follower để đảm bảo tính nhất quán, thống nhất của sổ cái phân tán.

Hệ thống có các chức năng chính như tạo ra chứng cứ số, di chuyển, truyền nhận và hiển thị dữ liệu chứng cứ số từ mạng blockchain. Tùy theo chính sách phân quyền được cấu hình mà các thành viên trong mạng lưới có thể có những hành động nhất định đối với chứng cứ số.

- *Tạo chứng cứ số*: Là một hàm lấy hai tham số đầu vào, sau đó tạo ra một chứng cứ số mới trong chuỗi điều tra (Borse, 2021). Hai tham số đầu vào là số ID (định danh của chứng cứ) và description (mô tả chứng cứ). Hàm tạo chứng cứ số sẽ tạo ra mã băm của chứng cứ số, giúp thuận tiện trong quá trình kiểm tra tính toàn vẹn của chứng cứ số trong suốt quá trình điều tra. Sau đó tiến hành kiểm tra chứng cứ số đó đã tồn tại trong hệ thống hay chưa? Nếu đã tồn tại, việc tạo mới chứng cứ số sẽ không được xem xét. Ngược lại, một khối block mới được tạo ra lưu trữ chứng cứ đó và đăng ký vào trong chuỗi xử lý của mạng blockchain.



Hình 4. Luồng dữ liệu của hàm cung cấp (tạo) chứng cứ

- *Chuyển chứng cứ*: Hàm sử dụng khi các bên muốn chuyển/chuyển giao chứng cứ cho các bên liên quan, hàm lấy hai tham số đầu vào là ID của chứng cứ và địa chỉ người nhận. Trước khi chuyển, hệ thống sẽ kiểm tra xem chứng cứ đó đã tồn tại trong hệ thống hay chưa và người gửi/nhận có quyền sở hữu chứng cứ đó hay không?

- *Xem chứng cứ*: Hệ thống sẽ kiểm tra xem chứng có tồn tại trên hệ thống hay không và người gọi hàm xem chứng cứ có quyền đó hay không? Nếu người gọi hàm đó không có quyền xem chứng cứ, hệ thống sẽ từ chối hiển thị chứng cứ.

Kết luận

Lĩnh vực pháp y, điều tra số đang được mở rộng từng ngày và có rất nhiều điểm khác biệt trong việc quản lý chứng cứ số so với quản lý chứng cứ vật lý. Công nghệ blockchain có khả năng cung cấp những đặc tính quan trọng, cần thiết trong việc quản lý chứng cứ số như tính xác thực, tính toàn vẹn, minh bạch và bảo mật. Vì vậy, công nghệ blockchain có lợi thế về việc lưu trữ, bảo quản, theo dấu chuỗi xử lý chứng cứ số so với các phương pháp thông thường. Để tránh việc không chấp nhận chứng cứ số tại các buổi kết luận điều tra hoặc tòa án, công nghệ blockchain là giải pháp khả thi trong việc duy trì, lưu trữ bằng chứng cũng như chuỗi xử lý chứng cứ số, phục vụ hiệu quả cho quá trình điều tra số.

Bài báo đã cung cấp, giới thiệu ứng dụng công nghệ blockchain trong việc lưu trữ chứng cứ số, phân tích các đặc trưng cơ bản của blockchain và chỉ ra khả năng phù hợp, tương thích của công nghệ blockchain trong việc lưu trữ chứng cứ số. Bên cạnh đó, chúng tôi cũng đề xuất mô hình Hyperledger Fabric lưu trữ và theo dõi quá trình xử lý chứng cứ số với các bên tham gia như cơ quan điều tra, cơ quan khởi tố, tòa án, các bên liên quan cũng như giới thiệu vai trò của các bên trong cơ chế đồng thuận.

Tài liệu tham khảo

Ćosić, J., & Ba a, M. (2010, May). "(Im) proving chain of custody and digital evidence integrity with time stamp". The 33rd International Convention MIPRO, 1226-1230, IEEE.

Sadiku, M. N., Shadare, A. E., & Musa, S. M. (2017). "Digital chain of custody. Int. J. Adv. Res". Comput. Sci. Softw. Eng, 7(7), 117.

Borse, Y., Patole, D., Chawhan, G., Kukreja, G., Parekh, H., & Jain, R. (2021, May). "Advantages of blockchain in Digital Forensic Evidence Management". Proceedings of the 4th International Conference. Advances in Science & Technology (ICAST2021).