MỘT SỐ BIỆN PHÁP ĐIỀU TRA HOẠT ĐỘNG RỬA TIỀN QUA KHÔNG GIAN MẠNG VÀ KINH NGHIỆM CHO VIỆT NAM

TRẦN NGỌC LAN TRANG
Khoa Luật Hình sự, Trường Đại học Luật TP. Hồ Chí Minh
Faculty of Criminal Law, Ho Chi Minh City University of Law
Email: tnltrang@hcmulaw.edu.vn

Tóm tắt

Trong những năm gần đây, việc sử dụng tiền mã hóa (hay tiền kỹ thuật số) (cryptocurrency) đã trở thành một phần trong cuộc sống của nhiều người trên toàn thế giới. Tiền mã hóa là bất kỳ dạng tiền tệ nào tồn tại dưới dạng kỹ thuật số và sử dụng mật mã để bảo mật các giao dịch. Tiền mã hóa không có cơ quan quản lý hoặc phát hành trung tâm, thay vào đó là sử dụng hệ thống phi tập trung để ghi lại các giao dịch và phát hành các đơn vị mới. Tiền mã hóa được phát triển trên cơ sở dữ liệu quản lý thông qua mạng ngang hàng, được gọi là chuỗi khối (blockchain). Việc sử dụng Internet, kết hợp với sự phát triển của tiền mã hóa và chuỗi khối, đã cho phép những kẻ rửa tiền mở rộng hoạt động của chúng sang không gian mạng. Hoạt động rửa tiền qua không gian mạng cung cấp các giao dịch ẩn danh nhanh chóng, dễ dàng, chi phí thấp và phá vỡ các kỹ thuật phát hiện truyền thống được chính quyền sử dụng. Ngược lại với hoạt động rửa tiền truyền thống, hoạt động rửa tiền qua không gian mạng tương đối mới, tiền mã hóa và chuỗi khối khiến hoạt động này trở nên phức tạp về mặt kỹ thuật. Trong bài viết, tác giả phân tích đặc điểm nổi bật của công nghệ chuỗi khối blockchain và tiền mã hóa Bitcoin (i) nêu ra một số phương thức rửa tiền qua không gian mạng (ii), thực tiễn công tác điều tra phát hiện hoạt động rửa tiền (iii) và bài học kinh nghiệm cho Việt Nam.

Từ khóa: *tiền mã hóa, chuỗi khối, rửa tiền qua không gian mạng*

Abstract

Cryptocurrency, sometimes called crypto-currency or crypto, is any form of currency that exists digitally or virtually and uses cryptography to secure transactions. Cryptocurrencies don't have a central issuing or regulating authority, instead a decentralized system to record transactions and issue new units is used. Cryptocurrencies run on a distributed public ledger called blockchain, a record of all transactions updated and held by currency holders. The use of the Internet, combined with cryptocurrency and blockchain development, has enabled money launderers to expand their activities into cyberspace. Cyber money laundering provides quick, easy, low-cost, anonymous transactions and circumvents traditional detection techniques used by the authorities. In contrast to traditional money laundering, cyber money laundering is relatively new, and cryptocurrency and the blockchain make it technically complex. In this article, the author analyzes the outstanding features of blockchain technology and Bitcoin cryptocurrency (i); Outlines a number of money laundering methods through cryptocurrency transactions (ii), experiences in investigating and detecting this cyber money laundering (iii) and experience for Vietnam.

Keywords: *cryptocurrency, blockchain, cyber money laundering*
Ngày nhận bài: 17/12/2023 **Ngày duyệt đăng: 12/01/2024**

Theo Báo cáo thị trường crypto Việt Nam năm 2022, "Việt Nam hiện có hơn 16,6 triệu người sở hữu tiền mã hóa (trong đó có khoảng 31% sở hữu Bitcoin). Trong đó, báo cáo nhấn mạnh, Việt Nam là quốc gia đứng đầu thế giới về việc chấp nhận tiền mã hóa trong hai năm liên tiếp 2021 và 2022. Ngoài ra, Việt Nam còn là quốc gia có tỷ lệ người

nắm giữ tiền mã hóa lớn thứ hai ASEAN sau Thái Lan."[1] Như vậy, việc nghiên cứu đặc tính của tiền mã hóa đặt ra thách thức cho các nhà khoa học và Nhà nước trong công tác xây dựng pháp luật nhằm điều chỉnh phương thức giao dịch, hoạt động kinh doanh.

Các công trình nghiên cứu tại Việt Nam về tiền mã hóa cũng chưa nhiều. Trong đó, sách chuyên khảo "Xây dựng và hoàn thiện khung pháp lý về tiền ảo trong bối cảnh hội nhập và phát triển" của tác giả Nguyễn Minh Oanh (năm 2019), Nxb. Tư Pháp, đã nghiên cứu các vấn đề pháp lý về tiền ảo tại Việt Nam và thực trạng pháp luật tại một số quốc gia ở châu Âu, châu Mỹ và châu Á với mục đích học hỏi kinh nghiệm cũng như đề xuất một số chính sách phù hợp cho việc hoàn thiện chính sách, pháp luật về tiền ảo tại Việt Nam. Bài viết: "Hoàn thiện khung pháp lý về tiền ảo trong thời đại công nghiệp 4.0" của tác giả Đoàn Thị Ngọc Hải (năm 2019) đăng trên Tạp chí điện tử của Toà án nhân dân nêu định nghĩa tiền ảo tại một số quốc gia như Nhật Bản, Mỹ, Thụy Điển, Liên minh châu Âu nói chung và định nghĩa về tiền ảo trong Bộ luật Dân sự Việt Nam năm 2015 và các quy định về giao dịch pháp lý liên quan đến tiền ảo trong các văn bản pháp luật của Việt Nam như: Luật giao dịch điện tử năm 2005, Pháp luật tín dụng – ngân hàng năm 2005 và Luật Ngân hàng nhà nước Việt Nam năm 2010. Đề tài nghiên cứu khoa học "Khung pháp lý về Bitcoin và các loại tiền ảo trong pháp luật một số nước trên thế giới - kinh nghiệm cho Việt Nam" của nhóm nghiên cứu Phạm Hải Trà My (năm 2019) phân tích một số vấn đề lý luận và khung pháp lý của Bitcoin và các loại tiền ảo, tình hình thực hiện pháp luật ở Mỹ, Singapore, Pháp và Trung Quốc, qua đó nêu bài học kinh nghiệm và một số định hướng xây dựng khung pháp lý về Bitcoin và các loại tiền ảo trong bối cảnh cụ thể của Việt Nam. Luận văn thạc sĩ chuyên ngành luật kinh tế "Những nội dung pháp lý về tiền ảo – thực tiễn pháp luật nước ngoài và kinh nghiệm cho Việt Nam" của tác giả Nguyễn Trần Phương Dung (năm 2022), Trường ĐH Luật TP. Hồ Chí Minh, phân tích khái quát chung, hoạt động giao dịch, đầu tư tiền ảo tại Việt Nam và một số vấn đề pháp lý về tiền ảo trong các luật dân sự, thuế, doanh nghiệp, chứng khoán, hình sư, qua đó tác giả đề xuất một số kinh nghiệm cho Việt Nam. Bài viết "Bàn về tiền mã hóa và vấn đề phải chứng minh trong giải quyết vụ án hình sự" của tác giả Nguyễn Thị Phương Hoa (năm 2023), Hội thảo cấp trường, Trường ĐH Luật TP. Hồ Chí Minh phân tích đặc điểm của tiền mã hóa và chính sách, quy định hiện hành của Việt Nam, đồng thời tác giả phân tích những vấn đề phải chứng minh trong bản án điển hình cướp

1 Nhịp sống kinh tế Việt Nam và Thế giới, "Việt Nam có hơn 16,6 triệu người sở hữu tiền mã hóa, đứng thứ hai ASEAN sau Thái Lan", https://vneconomy.vn/viet-nam-co-hon-16-6-trieu-nguoi-so-huu-tien-ma-hoa-dung-thu-hai-asean-sau-thai-lan, truy cập ngày 25/10/2023.

Bitcoin, qua đó kiến nghị khung pháp lý liên quan đến tài sản mã hóa. Bài viết "Tiền mã hóa và những vấn đề đặt ra với hoạt động quản lý nhà nước của lực lượng an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao" của tác giả Đinh Thành An (năm 2023) đăng trên Tạp chí Dân chủ và pháp luật, đưa ra quan niệm về tiền ảo, tiền điện tử, tiền mã hóa, tiền kỹ thuật số, đồng thời nêu khó khăn, vướng mắc trong hoạt động quản lý nhà nước, thực trạng hoạt động xây dựng hệ thống pháp luật và giải pháp nâng cao hiệu quả quản lý nhà nước đối với tiền mã hóa.

Trong bài viết tác giả sử dụng phương pháp nghiên cứu so sánh (*comparative research method*) nhằm phân tích đặc điểm nổi bật của công nghệ chuỗi khối Blockchain và tiền mã hóa Bitcoin ở mục 1 và nêu một số phương thức rửa tiền qua không gian mạng ở mục 2. Tính ẩn danh trong giao dịch tiền mã hoá gây khó khăn cho việc phát hiện hoạt động rửa tiền qua không gian mạng. Vì vậy, ở mục 3 của bài viết, tác giả nêu một số kinh nghiệm điều tra hoạt động rửa tiền này từ kết quả nghiên cứu thực nghiệm của một số tác giả khác với mục đích tìm ra bài học kinh nghiệm cho Việt Nam trong mục 4.

1. Đặc điểm nổi bật của công nghệ chuỗi khối Blockchain và tiền mã hóa Bitcoin

Công nghệ chuỗi khối blockchain là một cơ sở dữ liệu công cộng phi tập trung, loại bỏ việc quản lý, can thiệp của các tổ chức tập trung (gồm nhà nước, ngân hàng, tổ chức tài chính).

Công nghệ blockchain tạo sổ cái không thể thay đổi hoặc bất biến để theo dõi đơn đặt hàng, thanh toán, tài khoản và các giao dịch khác. Hệ thống được tích hợp sẵn các cơ chế ngăn chặn các mục nhập giao dịch trái phép và tạo sự nhất quán trong cách nhìn chung về các giao dịch này (tính bất biến). Công nghệ này giảm thiểu những vấn đề như vậy bằng cách tạo ra một hệ thống phi tập trung, chống giả mạo để ghi lại các giao dịch. Trong quá trình giao dịch tài sản, Blockchain tạo ra một sổ cái cho mỗi người mua và người bán. Tất cả các giao dịch phải được cả hai bên chấp thuận và được tự động cập nhật vào sổ cái của cả hai bên theo thời gian thực. Bất kỳ sai sót nào trong các giao dịch lịch sử sẽ làm sai lệch toàn bộ sổ cái. Những đặc tính này của công nghệ blockchain đã dẫn đến việc sử dụng nó trong nhiều lĩnh vực khác nhau, bao gồm cả việc tạo ra loại tiền mã hóa như Bitcoin.[2]

Bitcoin (ký hiệu: BTC, XBT, ₿) là một loại tiền mã hóa dựa trên sự phân cấp, không cần được quản lý bởi bất kỳ ngân hàng hoặc người quản lý nào, áp dụng mạng ngang hàng và sáng kiến đồng thuận, mã nguồn mở

2 Amazon, "What is blockchain technology?", https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc, truy cập ngày 01/10/2023.

và sử dụng blockchain làm công nghệ cơ bản.[3] Tiền mã hóa Bitcoin có các đặc điểm nổi bật là tính phi tập trung, ẩn danh và hoạt động theo cơ chế đồng thuận. Trong đó, bằng việc sử dụng công nghệ blockchain, sự cung ứng Bitcoin là tự động, trao đổi trực tiếp bằng thiết bị kết nối internet mà không cần thông qua một tổ chức tài chính trung gian. Mạng giao dịch là cấu trúc liên kết ngang hàng (P2P), là công nghệ không có máy chủ trung tâm và mỗi người dùng đều có khả năng trao đổi thông tin như nhau với người khác. Cấu trúc giống như chuỗi khiến chủ sở hữu sổ cái không thể thay đổi dữ liệu giao dịch trong quá khứ.[4]

Trong giao dịch Bitcoin, mức độ ẩn danh được cung cấp bởi các địa chỉ chữ và số, do đó, không có tổ chức hoặc quốc gia tập trung nào sở hữu thông tin của chủ sở hữu ví Bitcoin. Vì tính chất ẩn danh, người phạm tội có thể sử dụng loại tiền mã hóa này cho các hoạt động bất hợp pháp, cụ thể có một số nhóm sau:[5]

- Tội phạm lừa đảo: Bitcoin là một khái niệm và công nghệ tiền tệ mới nổi và cơ cấu hoạt động của nó rất phức tạp đối với nhiều người. Trong những năm gần đây, giá trị của Bitcoin đã tăng vọt và nó trở thành mục tiêu đầu tư mới nổi. Nhiều tội phạm lợi dụng sự thiếu hiểu biết hoặc tâm lý theo đuổi lợi nhuận cao của các nhà đầu tư để thực hiện hành vi lừa đảo chiếm đoạt Bitcoin;

- Tội phạm trộm cắp: Bitcoin được lưu trữ trong ví Bitcoin và ví Bitcoin thực sự là một chuỗi mã kỹ thuật số (khóa riêng), chỉ cần khóa riêng được truyền ra ngoài, người giữ khóa riêng sẽ có tất cả các quyền của chủ sở hữu ví bitcoin. Vì vậy nhiều tin tặc sẽ sử dụng kỹ thuật nhằm xâm nhập để giành quyền kiểm soát ví bitcoin này.

- Giao dịch bất hợp pháp: Bitcoin được nhiều tội phạm sử dụng như một cách để nhận được khoản thanh toán tiền chuộc từ nạn nhân nhằm tránh nguy cơ rút tiền trực tiếp hoặc rút tiền bị truy tìm. Bitcoin thường được sử dụng làm công cụ thanh toán cho vũ khí, ma túy hoặc buôn người trên web đen như một loại tiền tệ toàn cầu.

3 Bitcoin là một loại tiền mã hóa, được phát minh bởi một cá nhân hoặc tổ chức vô danh dùng tên Satoshi Nakamoto dưới dạng phần mềm mã nguồn mở từ năm 2009. Mỗi bitcoin có thể được chia nhỏ tới 100 triệu đơn vị nhỏ hơn gọi là satoshi. Đơn vị nhỏ nhất của tiền mã hóa Bitcoin (BTC) được đặt theo tên của cá nhân hoặc tổ chức sáng lập là "satoshi". Một satoshi, thường được viết tắt là 'sats', tương đương với một phần trăm triệu của một bitcoin (0,00000001 BTC), cho phép đo lường và giao dịch số lượng nhỏ bitcoin. Khả năng phân chia này là chìa khóa cho chức năng của Bitcoin vì nó cho phép các giao dịch vi mô và tính phí giao dịch. Nguồn: Sam Cooling, "What is satoshi?", https://www.techopedia.com/definition/satoshi, truy cập ngày 04/10/2023.

4 Chang-Yi Lin, Hsiang-Kai Liao, Fu-Ching Tsai, "A Systematic Review of Detecting Illicit Bitcoin Transactions", *ScienceDirect*, Procedia Computer Science 207, 2022, tr. 3211–3219, https://www.sciencedirect.com/science/article/pii/S1877050922012698, truy cập ngày 26/9/2023.

5 Chang-Yi Lin, Hsiang-Kai Liao, Fu-Ching Tsai, *tlđd,* tr. 3213.

- Rửa tiền: Mức độ ẩn danh được cung cấp bởi các địa chỉ chữ và số được sử dụng trong giao dịch Bitcoin. Vì vậy, Bitcoin đã trở thành một kênh rửa tiền mới nổi của tội phạm về khủng bố, buôn người, buôn bán vũ khí, ma túy.

Như vậy, Bitcoin là một loại tiền mã hóa có ưu điểm vượt trội là tính phi tập trung, minh bạch, phí giao dịch thấp và thực hiện giao dịch xuyên quốc gia một cách nhanh chóng, thuận tiện.[6] Quan trọng hơn, vì Bitcoin không thuộc thẩm quyền quản lý của bất kỳ quốc gia nào nên nó thường được sử dụng cho các tội phạm xuyên biên giới.

2. Một số phương thức rửa tiền qua không gian mạng

Theo CoinMarketCap,[7] tính đến tháng 9/2023, trên thế giới hiện có hơn 23.000 loại tiền mã hóa.[8] Các loại tiền mã hóa không phải Bitcoin được gọi chung là "altcoin" để phân biệt chúng với bản gốc.[9]

Tính phi tập trung của tiền mã hóa đã khiến nó trở thành công cụ yêu thích của nhiều tội phạm. Động cơ chính thúc đẩy việc sử dụng tiền mã hóa (gồm cả Bitcoin và altcoin) trong hoạt động bất hợp pháp là mức độ ẩn danh được cung cấp bởi các địa chỉ chữ và số được sử dụng trong giao dịch. Với đặc điểm này và phạm vi tiếp cận toàn cầu, tiền mã hóa đã cung cấp một phương thức để các tổ chức tội phạm chuyển hoạt động rửa tiền truyền thống sang lĩnh vực rửa tiền qua không gian mạng. Các tổ chức tội phạm và khủng bố quan tâm đến tiền mã hóa vì các cơ quan thực

---

6 Nguyễn Thị Phương Hoa, "Bàn về tiền mã hóa và vấn đề phải chứng minh trong giải quyết vụ án hình sự", *Kỷ yếu Hội thảo Chứng cứ và chứng minh trong giải quyết vụ án hình sự,* do Khoa Luật Hình sự tổ chức tại Trường Đại học Luật TP. Hồ Chí Minh, 2023, tr. 302-332.

7 CoinMarketCap là trang web được tham khảo nhiều nhất để theo dõi giá về các loại tiền mã hóa trên thế giới trên thị trường tiền mã hóa đang phát triển nhanh chóng. Nhiệm vụ của họ là làm cho tiền mã hóa có thể khám phá được và có hiệu quả trên toàn cầu bằng cách trao quyền cho người dùng bán lẻ thông tin không thiên vị, chất lượng cao và chính xác để đưa ra kết luận sáng suốt của riêng họ. Được thành lập bởi Brandon Chez vào tháng 5 năm 2013, CoinMarketCap đã nhanh chóng phát triển để trở thành nguồn đáng tin cậy nhất bởi người dùng, tổ chức và phương tiện truyền thông để so sánh hàng nghìn loại tiền mã hóa và thường được trích dẫn bởi CNBC, Bloomberg và các hãng tin tức lớn khác (ngay cả Chính phủ Hoa Kỳ cũng sử dụng dữ liệu của CoinMarketCap trong nghiên cứu và các báo cáo). Xem: CoinMarketCap, "About CoinMarketCap" https://coinmarketcap.com/about/, truy cập ngày 10/10/2023.

8 Tuy nhiên, tốc độ tăng trưởng đáng kinh ngạc đó không hoàn toàn là tin tốt. Nhiều loại tiền mã hóa mới có rất ít mục đích ngoài việc kiếm tiền cho các nhà phát triển của chúng. Nhìn chung, đây vẫn là một thị trường rất phức tạp, nặng nề bởi một số lượng nhỏ tiền mã hóa nhưng chiếm phần lớn tổng giá trị của thị trường. Xem: Lyle Daly, "How Many Cryptocurrencies Are There?", 2023, https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/how-many-cryptocurrencies-are-there/, truy cập ngày 15/10/2023.

9 Trần Ngọc Lan Trang, "Một số cách thức điều tra hoạt động rửa tiền qua không gian mạng và kinh nghiệm cho Việt Nam", *Kỷ yếu Hội thảo Chứng cứ và chứng minh trong giải quyết vụ án hình sự*, do Khoa Luật Hình sự tổ chức tại Trường Đại học Luật TPHCM, ngày 08/11/2023, tr. 333-350. Phụ lục: Một số loại tiền mã hóa quan trọng và có ảnh hưởng nhất, tr. 349-350.

thi pháp luật và các chuyên gia chống khủng bố có thể gặp khó khăn hơn trong việc theo dõi tài sản tiền mã hóa. Ngay từ đầu, các tổ chức tội phạm đã chuyển sang sử dụng tiền mã hóa Bitcoin như một cách thức thực hiện thanh toán ẩn danh.[10]

Những kẻ rửa tiền sử dụng rất nhiều công cụ và kỹ thuật để che giấu các giao dịch bất hợp pháp, thậm chí tạo ra các nhật ký đáng tin cậy. Một số phương thức rửa tiền qua không gian mạng thường được sử dụng là:

- Phần mềm ẩn danh *The Onion Router* (TOR) là một ứng dụng ẩn danh, miễn phí, dễ truy cập, sử dụng nhiều nút TOR để định tuyến lưu lượng truy cập qua Internet trong khi mã hóa lưu lượng giữa các nút. Do máy tính kết nối chỉ có thể phát hiện được địa chỉ IP[11] của nút trước đó nên phần mềm sẽ ẩn địa chỉ IP gốc và dấu vết tiếp theo.[12] Tiêu chí của phần mềm TOR là cung cấp quyền riêng tư trực tuyến cho tất cả những ai cần sử dụng.[13]

- Hoạt động rửa tiền vi mô là chia số lượng tiền mã hóa đáng kể thành số tiền nhỏ hơn, sau đó đổi chúng lấy tiền tệ và gửi chúng vào tài khoản hợp pháp. Đây được xem là cách đơn giản để làm xáo trộn và làm cho việc chuyển tiền mã hóa vào hệ thống tài chính trông ít đáng ngờ hơn. Kết hợp hoạt động rửa tiền vi mô với các dịch vụ trộn/đánh cắp tiền mã hóa sẵn có và các công cụ bảo vệ quyền riêng tư, những kẻ rửa tiền có thể ẩn danh hơn nữa các giao dịch, bảo vệ quyền riêng tư và tránh bị chính quyền phát hiện.[14]

- Các dịch vụ trộn lẫn (*mixing/tumbling services*) nhằm chuyển đổi hợp pháp tiền mã hóa "bẩn" thành tiền mã hóa "sạch" và che giấu lịch sử giao dịch trên blockchain. Tiền mã hóa "sạch" được lấy từ những người dùng hợp pháp khác của dịch vụ. Do đó, số lượng người đăng ký hợp pháp

10 Bitcoin là phương thức thanh toán tiêu chuẩn để mua ma túy bất hợp pháp trên nền tảng web đen khét tiếng Silk Road, mà Ross Ulbricht đã đưa ra vào tháng 7 năm 2010.15 Silk Road đã xử lý doanh số bán hàng trị giá 9,5 triệu Bitcoin trong tổng số 12 triệu Bitcoin đang lưu hành từ năm 2010 đến năm 2012.16 Tin tặc đã sử dụng Bitcoin trong các cuộc tấn công ransomware như WannaCry, trong đó phần mềm độc hại như CryptoLocker mã hóa tất cả dữ liệu trên các máy tính bị xâm nhập. Sau đó, tin tặc đưa ra khóa mã hóa để đổi lấy một lượng Bitcoin nhất định. Xem Armin Krishnan, "Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations", *Journal of Strategic Security*, Vol. 13, Apr. 2020, tr. 44-45, https://www.academia.edu/47089198/Blockchain_Empowers_Social_Resistance_and_Terrorism_Through_Decentralized_Autonomous_Organizations, truy cập ngày 17/10/2023.

11 Địa chỉ IP - *Internet Protocol - giao thức Internet*, hiểu là một địa chỉ đơn nhất mà những thiết bị điện tử hiện nay đang sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính. Xem: https://vi.wikipedia.org/wiki/Địa_chỉ_IP, truy cập ngày 03/10/2023.

12 Xem: https://en.wikipedia.org/wiki/Tor_(network), truy cập ngày 01/10/2023.

13 Xem: https://www.torproject.org, truy cập ngày 01/10/2023.

14 Rolf van Wegberg, Jan-Jaap Oerlemans, and Oskar van Deventer, "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin", *Journal of Financial Crime*, ISSN: 1359-0790, Article publication date: 8 May 2018, https://www.emerald.com/insight/content/doi/10.1108/JFC-11-2016-0067/full/html, truy cập ngày 17/10/2023.

càng cao sẽ làm tăng hiệu quả của việc trộn/xáo trộn. Bộ trộn cung cấp cho tiền mã hóa đã được làm sạch một địa chỉ công khai mới từ một trong những địa chỉ công khai "sạch" của bộ trộn không liên quan đến quá trình trộn/xáo trộn. Dịch vụ trộn sẽ khấu trừ phí giao dịch từ số tiền mới được "rửa sạch" của khách hàng và nạp tiền mã hóa dự trữ vào các địa chỉ công cộng, góp phần vào quá trình trộn.[15]

- Dịch vụ trực tuyến (*online services*) đề cập đến các dịch vụ được cung cấp bởi các ngân hàng trực tuyến và các trung gian tài chính ảo khác. Đây là những công cụ rửa tiền hấp dẫn vì nó dễ dàng khai thác những khác biệt về quy định và bỏ qua các yêu cầu, chẳng hạn như mở tài khoản ngân hàng Internet ở các khu vực pháp lý khác nhau. Các tài khoản có thể được mở dưới tên của một công ty vỏ bọc cung cấp các dịch vụ và sản phẩm giả hoặc thật để che giấu danh tính và tạo thêm vẻ ngoài hợp pháp. Bằng cách cung cấp các dịch vụ hoặc sản phẩm thực, khách hàng hợp pháp vô tình cung cấp số tiền thu được hợp pháp được trộn lẫn với số tiền thu được bất hợp pháp, khiến cho việc phân biệt và theo dõi những khoản sau này khó bị phát hiện hơn. Các sàn giao dịch này thường xuyên sử dụng các kỹ thuật trộn/ lật đổ và thậm chí cả những người chuyển tiền (*money couriers/money mules*) để tăng thêm tính ẩn danh và che giấu giao dịch. Giao dịch có thể thực hiện giữa khách hàng và sàn giao dịch bằng cách sử dụng ATM tiền mã hóa. [16]

- Đấu giá trực tuyến (*online auctions*) thường được sử dụng để chuyển tiền bất hợp pháp vào tài khoản ngân hàng của các công ty hợp pháp (thường là các công ty vỏ bọc). Một đại diện của công ty vỏ bọc đóng vai trò là công ty bán vật phẩm trong cuộc đấu giá và những kẻ rửa tiền (*smurfs*) đóng vai trò là người mua, đẩy giá bán của vật phẩm đó lên cao nhất có thể. Vì các cuộc đấu giá không có giới hạn về giá nên kẻ rửa tiền đưa ra mức giá cắt cổ so với giá trị của món hàng được đấu giá. Giao dịch được hoàn tất khi người có giá thắng cao nhất (kẻ rửa tiền) gửi tiền bất

15 Rolf van Wegberg, Jan-Jaap Oerlemans, and Oskar van Deventer, *tlđd,* tr. 425. Nghiên cứu của nhóm tác giả dựa trên việc sử dụng kỹ thuật TNO Dark Web để truy cập, thu thập dữ liệu trên internet không được công khai và không thể truy cập thông qua các công cụ tìm kiếm thông thường. *TNO Dark Web MoniTOR là một công cụ tương tác được thiết kế để lập chỉ mục và hiển thị dữ liệu Dark Web được thu thập thông tin. Sử dụng kỹ thuật này, nhóm nghiên cứu đã phát hiện ra hơn 25.000 dịch vụ* ẩn, tức là các trang web Dark Web. Bằng cách sử dụng TNO Dark Web Monitor, chúng tôi đã có được cái nhìn tổng quan chắc chắn về tổng nguồn cung dịch vụ Dark Web cung cấp việc trộn và trao đổi bitcoin từ bitcoin sang loại tiền không ảo khác thông qua nhiều nền tảng đầu ra ẩn danh. Tổng quan này cho phép chúng tôi thấy một số điểm khác biệt đáng chú ý trong các dịch vụ được cung cấp. Mục đích của chiến lược rút tiền là cung cấp số tiền có thể chi tiêu được từ tội phạm mà không thể truy nguyên nguồn gốc của nó.

16 Michael W. Calafos and George Dimitoglou, "Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency", first online: 04 July 2022, In book: Kevin Daimi, Ioanna Dionysiou (ed.), *Principles and Practice of Blockchains*, Nour EI Madhoun, Springer, 2023, tr. 271-300, https://www.researchgate.net/publication/365641007_Cyber_Laundering_Money_Laundering_from_Fiat_Money_to_Cryptocurrency, truy cập ngày 10/10/2023.

hợp pháp vào tài khoản ngân hàng của công ty vỏ bọc và công ty này vận chuyển vật phẩm đấu giá. Quá trình này mang lại cho giao dịch vẻ ngoài hợp pháp khi có sự tham gia của một công ty uy tín (mặc dù chỉ là vỏ bọc).[17]

- Rửa tiền ảo (*Virtual money laundering*) là một kỹ thuật tương đối mới sử dụng các tổ chức từ thiện trên internet và các trò chơi nhập vai trực tuyến nhiều người chơi (*massive multiplayer online role-playing games* - MMORPG). Những kẻ rửa tiền qua không gian mạng quyên góp tiền bẩn cho các công ty vỏ bọc có vẻ hợp pháp, được thành lập như các tổ chức từ thiện dựa trên internet, thực hiện rất ít hoặc không làm từ thiện. Mặt khác, với MMORPG, người chơi rửa tiền hầu như có thể mua tiền mã hóa bằng cách sử dụng tiền tệ pháp định (*fiat*) với tỷ giá hối đoái cố định trước khi chơi và sau đó kiếm thêm tiền mã hóa khi chơi trò chơi. Sau đó, người chơi có thể trao đổi ảo tiền mã hóa với người khác hoặc mua hoặc bán các vật phẩm ảo. Người chơi cũng có thể chuyển đổi tiền mã hóa thành tiền pháp định và sau đó gửi tiền pháp định vào một hoặc nhiều tài khoản. Sau khi tiền tệ được gửi, người chơi có thể rút tiền từ bất kỳ máy ATM nào. Đôi khi, người chơi nhận được thẻ ghi nợ có thể nạp lại để chơi một trò chơi cụ thể, điều này cũng cho phép người chơi rút tiền pháp định từ máy ATM.[18]

- Cờ bạc trực tuyến (*online gambling*) cũng như cờ bạc trong thế giới thực, cờ bạc trực tuyến là một cách nhanh chóng và hiệu quả khác để hợp pháp hóa các khoản tiền bất hợp pháp và trốn thuế. Thông thường, các sòng bạc ở nước ngoài ở những địa điểm có quy định lỏng lẻo được chọn và chúng có thể được sử dụng để rửa và phân phối số tiền lớn. Một phương pháp điển hình là khai thác các dịch vụ cờ bạc hợp pháp trên Internet hoặc thành lập các doanh nghiệp cờ bạc bất hợp pháp. Dù bằng cách nào, cờ bạc trực tuyến là một phương pháp rửa tiền qua không gian mạng hiệu quả vì hầu hết các giao dịch đều sử dụng thẻ tín dụng hoặc thẻ trả trước.[19]

- Thẻ (*cards*) gồm thẻ tín dụng (*credit cards*) và thẻ trả trước (*prepaid cards*), còn được gọi là thẻ "thông minh", là những công cụ có giá trị được lưu trữ. Các tổ chức tội phạm sử dụng các loại thẻ bị đánh cắp hoặc giả mạo để mua sản phẩm và dịch vụ trực tuyến nhằm che giấu hoạt động rửa

17 Danton Bryans, "Bitcoin and money laundering: mining for an effective solution", *Indiana Law Journal*, Vol. 89:144, 2014, SSRN: https://ssrn.com/abstract=2317990, truy cập ngày 17/10/2023.

18 Danton Bryans, *tlđd*.

19 Danton Bryans, *tlđd*. See Pim Verschuuren, "Money laundering, sports betting and gambling", in K. J. Mc Carthy (ed.), *The Money Laundering Market: Regulating the criminal economy*, Agenda Publishing, 2018, tr. 113–136, https://www.unodc.org/res/safeguardingsport/grcs/section-9_html/SPORTS_CORRUPTION_2021_S9.pdf, truy cập ngày 20/10/2023.

tiền của mình. Phương thức thanh toán ưa thích là thẻ trả trước gồm cả hệ thống mở và đóng vì tính dễ sử dụng trong việc chuyển tiền xuyên biên giới. Trong đó, thẻ hệ thống mở là thẻ ghi nợ (*debit cards*) có thể sử dụng ở hầu hết mọi nơi như máy rút tiền tự động thông thường - *automated teller machines* (ATMs), kiosk có thể đổi tiền ảo - *convertible virtual currency (CVC) kiosks*, hoặc ATM tiền mã hóa - *crypto ATMs*. Còn thẻ hệ thống khép kín là thẻ điện thoại trả trước (*prepaid telephone cards*) có thể được mua và bán lại.[20]

- Dịch vụ thanh toán di động (*mobile payment services* - MPS) được cung cấp bởi các tổ chức phi ngân hàng và không yêu cầu người dùng phải có tài khoản ngân hàng hoặc thẻ tín dụng. MPS được giao dịch qua điện thoại di động hoặc thiết bị liên lạc khác, kết nối với internet thông qua truy cập giọng nói, nhắn tin văn bản hoặc giao thức ứng dụng không dây để thực hiện thanh toán. Thanh toán qua điện thoại di động đã thay thế tài khoản ngân hàng ở nhiều quốc gia và thanh toán thông qua các công cụ ngân hàng (ví dụ: tiền mặt, séc, chuyển tiền). Đặc biệt ở những quốc gia có hệ thống ngân hàng kém phát triển hoặc hoạt động kém, MPS là cách nhanh nhất để tiến hành kinh doanh. Những kẻ rửa tiền sử dụng điện thoại di động cho các giai đoạn phân lớp và dàn dựng (còn được gọi là lướt web kỹ thuật số). Theo đó, họ hướng dẫn những người trong đường dây rửa tiền sử dụng điện thoại di động và tiền tệ pháp định bất hợp pháp để chuyển tiền mã hóa vào tài khoản chính hoặc một số địa chỉ khác.[21]

- Chiến dịch mã độc tống tiền (*ransomware*): Chiến dịch ransomware chống lại các mục tiêu được chọn là một phương pháp rửa tiền tiêu chuẩn khác trên mạng. Kiểu tấn công này dựa trên mã độc, một loại phần mềm độc hại lây nhiễm vào hệ thống máy tính để lấy hoặc xóa dữ liệu và giữ dữ liệu làm con tin nhằm chặn quyền truy cập vào dữ liệu yêu cầu thanh toán tiền chuộc để giải phóng dữ liệu, thường ở dạng tiền mã hóa. Nhằm thực hiện chiến dịch ransomware, các tổ chức tội phạm thường thuê nhân tài (có thể là một tin tặc riêng lẻ hoặc một nhóm hoạt động độc lập). Sau khi nhận tiền chuộc từ mục tiêu, các tổ chức này nắm giữ tiền mã hóa "sạch".[22]

Như vậy, với một số phương thức, kỹ thuật như trên, về cơ bản, tiền mã hóa (gồm cả Bitcoin và altcoin) có thể cho phép những kẻ rửa tiền chuyển tiền bất hợp pháp nhanh hơn, rẻ hơn và kín đáo hơn bao giờ hết. Tiền mã hóa có khả năng cho phép bất kỳ người dùng nào (gồm cả người dùng hợp pháp hoặc tội phạm) chuyển tiền với tốc độ gần như tức thời với chi phí thấp hoặc miễn phí, với rào cản gia nhập rất thấp, trong khi

20 Michael W. Calafos and George Dimitoglou, *tlđd*.
21 Michael W. Calafos and George Dimitoglou, *tlđd*.
22 Michael W. Calafos and George Dimitoglou, *tlđd*.

vẫn hầu như ẩn danh mà không cần có dấu vết giấy tờ công khai.

3. Kết quả nghiên cứu về các biện pháp điều tra hoạt động rửa tiền qua không gian mạng tại một số quốc gia trên thế giới

Hoạt động rửa tiền qua không gian mạng có thể được thực hiện trực tuyến một phần hoặc hoàn toàn, với việc chuyển tiền và rửa tiền mã hóa xuyên biên giới và xuyên khu vực pháp lý được thực hiện một cách bí mật, liền mạch và thực tế là ngay lập tức.[23] Do đó, hoạt động rửa tiền qua không gian mạng hiện nay đặt ra một số thách thức sau:

Thứ nhất, về khung pháp lý liên quan đến tiền mã hóa và rửa tiền qua không gian mạng, đặc biệt ở cấp độ quốc tế, các kế hoạch quản lý và chính sách pháp lý liên quan hầu như đều bị phân mảnh và không giải quyết thỏa đáng thị trường tiền mã hóa. Sự phân mảnh này bao gồm từ một số khu vực pháp lý cấm hoàn toàn việc sử dụng tiền mã hóa do mối đe dọa được nhận thấy của nó đối với các khu vực pháp lý khác không có bất kỳ luật nào vì họ không coi tiền mã hóa là tiền tệ và do đó không phải tuân theo các quy định chống rửa tiền. Ngay cả định nghĩa pháp lý và tiền tệ của tiền mã hóa cũng khác nhau giữa các khu vực pháp lý và đôi khi ngay cả giữa các cơ quan trong cùng khu vực pháp lý. Những biến thể này trong việc xác định, công nhận và điều chỉnh tiền mã hóa trong bối cảnh pháp lý cho phép các hoạt động tiền mã hóa bất hợp pháp phát triển mạnh và cản trở quy định quốc tế hiệu quả và thực thi hoạt động rửa tiền qua không gian mạng.[24]

Thứ hai, đặc tính ẩn danh và phi tập trung của tiền mã hóa gây khó khăn trong việc phát hiện, truy vết tội phạm rửa tiền qua không gian mạng. Điều thú vị là, không giống như tiền pháp định, tiền mã hóa có thể được sử dụng làm tài sản đầu vào và đầu ra và có thể tham gia hoặc thoát khỏi quá trình rửa tiền ở bất kỳ giai đoạn nào. Người nắm giữ tiền mã hóa có thể sử dụng các sàn giao dịch chưa đăng ký hoặc các trung gian tài chính khác, bỏ qua hệ thống tài chính và ngân hàng đã được thiết lập, cùng với bất kỳ cơ quan quản lý yêu cầu xác minh khách hàng. Tương tự, những kẻ rửa tiền qua không gian mạng sử dụng các sàn giao dịch chưa đăng ký để chuyển đổi tiền pháp định và thậm chí cả kim loại quý và đá quý thành tiền mã hóa để tránh sự giám sát của cơ quan quản lý.[25] Khả năng của người dùng trong việc trao đổi tiền mã hóa trực tiếp lấy các loại tiền tệ khác, chuyển qua vô số địa chỉ khác nhau để che giấu và giao dịch với những người dùng khác để lấy hàng hóa vật chất, gây khó khăn trong việc phát hiện, truy vết tội phạm.

23 Rolf van Wegberg, Jan-Jaap Oerlemans, and Oskar van Deventer, *tlđd*.
24 Michael W. Calafos and George Dimitoglou, *tlđd*. See 5.2 Cyber Laundering Legislation and Regulations.
25 Michael W. Calafos and George Dimitoglou, *tlđd*.

Thứ ba, việc sử dụng nhiều mã hóa để hỗ trợ tính ẩn danh và ứng dụng của nó với ví kỹ thuật số làm tăng đáng kể thách thức cho các nhà điều tra trong việc xác định những người liên quan đến giao dịch. Mặc dù khóa công khai của người dùng có thể được truy tìm thông qua lịch sử giao dịch, nhưng sự tồn tại của nhiều khóa công khai tiềm ẩn liên quan đến một cá nhân khiến nhiệm vụ điều tra chỉ trở nên phức tạp hơn. Ngay cả khi thông tin nhận dạng được yêu cầu xác nhận danh tính người dùng và mở tài khoản, người dùng vẫn có thể cung cấp thông tin lừa đảo. Người dùng cũng có thể che giấu danh tính của mình bằng cách sử dụng nhiều địa chỉ công khai từ các ví tiền mã hóa khác nhau hoặc kết nối với các máy tính khác trong mạng không dây mở.[26]

Thứ tư, các cuộc điều tra rửa tiền rất phức tạp và tốn thời gian mà thông thường, chỉ những cơ quan điều tra lớn nhất với đội ngũ nhân viên am hiểu kỹ thuật và lành nghề nhất mới có đủ nguồn lực để theo đuổi với bất kỳ mức độ thành công nào. Các nhà điều tra phải hiểu kỹ về chuỗi khối blockchain và tiền mã hóa cũng như các phương thức và thuật toán giao dịch phức tạp mà chúng hỗ trợ. Họ cũng phải theo kịp tốc độ đổi mới nhanh chóng trong thị trường tiền mã hóa, nơi liên tục giới thiệu các loại tiền tệ khác nhau với hệ thống thanh toán và ẩn danh khác nhau.

Với những thách thức trên, hoạt động điều tra hành vi rửa tiền qua không gian mạng cần có cách thức riêng. Các nhà điều tra cũng nhận ra rằng mặc dù ẩn danh nhưng hồ sơ giao dịch Bitcoin chứa nhiều thông tin đặc trưng (*features*) như thời gian giao dịch (*transaction time*), địa chỉ ví đầu vào (*input wallet address*), địa chỉ ví đầu ra (*output wallet address*). Với những thông tin đặc trưng này, kèm với tính bất biến nên chủ sở hữu ví Bitcoin không thể thay đổi dữ liệu giao dịch trong quá khứ. Do đó, cách chọn thông tin đặc trưng này để phân tích, điều tra sẽ giúp phát hiện các giao dịch bất hợp pháp, chẳng hạn như gửi tiền mặt tại các chi nhánh ngân hàng khác nhau trong một khung thời gian ngắn, chuyển khoản vào các tài khoản không có giao dịch nào khác hoặc hối phiếu ngân hàng đổi thành ngoại tệ, được áp dụng để phát hiện hành vi rửa tiền.[27]

Trong nghiên cứu "Đánh giá có hệ thống về việc phát hiện các giao dịch Bitcoin bất hợp pháp" của các tác giả Chang-Yi Lin, Hsiang-Kai Liao, Fu-Ching Tsai từ Cục Điều tra tội phạm thuộc Đại học Cảnh sát Đài Loan, nhóm tác giả đã thu thập được 25 tác phẩm, tài liệu (từ các bài báo,

26 Michael W. Calafos and George Dimitoglou, *tlđd;* Investigating, regulating and prosecuting cyber laundering; S. Middlebrook and S. Hughes, "Regulating Cryptocurrencies in the United States: Current Issues and Future Directions", *William Mitchell Law Review*, Vol. 40, Jan. 2014, https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1567&context=wmlr, truy cập ngày 10/10/2023.

27 Chang-Yi Lin, Hsiang-Kai Liao, Fu-Ching Tsai, *tlđd, tr. 3212.*

hội thảo của các tác giả)[28] liên quan đến việc xác định các hoạt động bất hợp pháp trong mạng lưới giao dịch Bitcoin. Để xác định các hoạt động bất hợp pháp trong mạng Bitcoin, việc phân tích giao dịch Bitcoin là cần thiết. Tuy nhiên, lượng dữ liệu trong các giao dịch Bitcoin quá lớn, các tính năng liên quan và các biến thể của chúng quá phức tạp cần được nghiên cứu. Vì vậy, công nghệ máy học (*machine learning*) đang bắt đầu được áp dụng rộng rãi trong lĩnh vực này. Máy học là một loại trí tuệ nhân tạo, cho phép máy học từ dữ liệu lớn và đưa ra các tiêu chí phân biệt, cuối cùng đạt được mục đích dự đoán dữ liệu chưa nhìn thấy. Công nghệ máy học có thể được chia thành học có giám sát (*supervised learning*), học không giám sát (*unsupervised learning*), học bán giám sát (*semi-supervised learning*) và học tăng cường (*reinforcement learning*) theo chế độ hoạt động của nó. Tiền mã hóa có đặc điểm là phân cấp, minh bạch và bất biến. Số lượng người dùng và các ứng dụng liên quan đến tiền mã hóa sẽ ngày càng trở nên phổ biến hơn. Tuy nhiên, xu hướng này cũng khuyến khích tội phạm thực hiện các giao dịch bất hợp pháp trên web đen hoặc rửa tiền. Mặt khác, bản chất của sổ cái công khai tiền mã hóa mở ra một cánh cửa khác xác định hoạt động bất hợp pháp. Bằng cách tóm tắt các thuật toán và nghiên cứu việc ứng dụng công nghệ máy học trong việc phát hiện giao dịch bất hợp pháp trên wed đen và có hoạt động rửa tiền, nhóm tác giả tin rằng các nhà nghiên cứu trong tương lai có thể hiểu rõ hơn về dòng Bitcoin.[29]

Trong nghiên cứu "*Phát hiện hoạt động bất hợp pháp trong giao dịch Bitcoin bằng kỹ thuật phân tích chuỗi thời gian*" của các tác giả Rohan Maheshwari, Sriram Praveen V A, Shobha G, Jyoti Shetty, Arjuna Chala, Hugo Watanuki, nhóm tác giả cho rằng động cơ chính thúc đẩy việc sử dụng tiền mã hóa như bitcoin trong hoạt động bất hợp pháp là mức độ ẩn danh được cung cấp bởi các địa chỉ chữ và số được sử dụng trong giao dịch. Tuy nhiên, điều này không có nghĩa là tính ẩn danh được tích hợp vào hệ thống vì các giao dịch được thực hiện vẫn phụ thuộc vào yếu tố con người. Ngoài ra, có khoảng 400 Gigabyte dữ liệu thô có sẵn trong chuỗi khối Bitcoin, khiến nó trở thành một vấn đề về dữ liệu lớn. Hệ thống tính toán và truyền thông hiệu năng cao (*high performance computing and communication*, HPCC) được sử dụng trong nghiên cứu này, đây là một nền tảng dữ liệu lớn, nguồn mở, chuyên sâu về dữ liệu. Trong nghiên cứu, nhóm tác giả cố gắng sử dụng dữ liệu thời gian được tạo ra bằng cách lấy khoảng thời gian giữa các giao dịch liên tiếp được thực hiện bởi một địa chỉ và xác định bản chất của địa chỉ đó (gồm cả hợp pháp và bất hợp pháp). Nghiên cứu cho thấy dữ liệu chuỗi thời gian có thể được sử dụng để có thể xác định các địa chỉ khác nhau có

28 Chang-Yi Lin, Hsiang-Kai Liao, Fu-Ching Tsai, *tlđd, tr. 3214-3215*. Xem Table 2. The reference list: các bài báo, hội thảo từ năm 2018 đến năm 2022.

29 Chang-Yi Lin, Hsiang-Kai Liao, Fu-Ching Tsai, *tlđd*.

nguồn gốc từ cùng một người dùng hoặc những người dùng tham gia vào hoạt động tương tự. Trên cơ sở phân tích, bài viết đưa ra bằng chứng mạnh mẽ cho thấy người dùng tham gia vào hoạt động bất hợp pháp có thể bị phát hiện bằng cách sử dụng các địa chỉ bất hợp pháp đã biết trước đó. Tuy nhiên, nhóm tác giả cũng chỉ ra rằng khuyết điểm của phương pháp này là thiếu dữ liệu về các giao dịch và địa chỉ bất hợp pháp. Do đó, nhóm tác giả đề xuất cần nghiên cứu sâu hơn và có bộ dữ liệu toàn diện hơn để cải thiện độ chính xác và độ tin cậy của việc phát hiện địa chỉ bất hợp pháp trong các giao dịch Bitcoin.[30]

Trong nghiên cứu "Rửa tiền trên không gian mạng: từ tiền pháp định đến tiền mã hóa" của các tác giả Michael W. Calafos and George Dimitoglou, nhóm tác giả tập trung phân tích Chiến dịch chống rửa tiền (*U.S. anti-money laundering (AML) regime*) của Hoa Kỳ. Là một trung tâm tài chính và kinh tế toàn cầu quan trọng, Hoa Kỳ dễ bị ảnh hưởng về an ninh và khủng bố do khối lượng giao dịch tài chính lớn. Chiến lược này bắt đầu từ những năm cuối 1970 đã dẫn đến việc xây dựng các khuôn khổ pháp lý toàn diện nhằm phát hiện và ngăn chặn các hoạt động tội phạm qua trung gian hệ thống tài chính. Từ đó đến nay, Hoa Kỳ liên tục cập nhật, thắt chặt khuôn khổ AML và giám sát chặt chẽ các tổ chức tài chính để đảm bảo tuân thủ pháp luật.[31] Với việc phân tích Chiến dịch AML, nhóm tác giả cho rằng các biện pháp kiểm soát phi kỹ thuật và kỹ thuật cụ thể có thể can thiệp, làm gián đoạn hoặc ngăn cản các hoạt động rửa tiền qua không gian mạng. Trong đó: một số biện pháp kiểm soát phi kỹ thuật gồm:[32]

- Thấu hiểu (*Know-Your-Customer*, KYC) và thẩm định khách hàng (*Customer Due Diligence,* CDD): các biện pháp kiểm soát được áp dụng để ngăn chặn cả hoạt động rửa tiền và tài trợ khủng bố. Các biện pháp kiểm soát của họ được pháp luật quy định đối với các công ty trong ngành dịch vụ tài chính, yêu cầu các công ty phải chứng minh bất kỳ người nào nắm giữ hoặc niêm yết trên một tài khoản. Các biện pháp kiểm soát này xuất hiện ở các giai đoạn khác nhau của mối quan hệ với khách hàng, mỗi giai đoạn yêu cầu một biện pháp kiểm soát khác nhau. Khi danh tính đã được xác nhận và thiết lập, cần phải đánh giá rủi ro và giám sát tài khoản

30 Rohan Maheshwari, Sriram Praveen V. A., Shobha G., Jyoti Shetty, Arjuna Chala, Hugo Watanuki, "Illicit Activity Detection in Bitcoin Transactions using Timeseries Analysis", *International Journal of Advanced Computer Science and Applications*, Vol. 14, No. 3, 2023, https://thesai.org/Downloads/Volume14No3/Paper_2-Illicit_Activity_Detection_in_Bitcoin_Transactions.pdf, truy cập ngày 23/10/2023.

31 Sanctions Canner, "Anti-Money Laundering (AML) in United States of America", https://sanctionscanner.com/aml-Guide/anti-money-laundering-aml-in-united-states-of-america-80 , truy cập ngày 18/01/2024.

32 Michael W. Calafos and George Dimitoglou, *tlđd*.

liên tục. Bất kỳ giao dịch đáng ngờ sẽ được chuyển đến cơ quan có thẩm quyền để điều tra.

- Giảm tính ẩn danh của các sàn giao dịch bằng cách kiểm soát việc xác định danh tính khách hàng;

- Theo dõi hoạt động của các sàn giao dịch đã đăng ký: Mặc dù danh tính của chủ sở hữu hoặc người dùng sàn giao dịch có thể không bị phát hiện, nhưng cơ quan chức năng có thể sử dụng công nghệ và vẫn thu giữ hoặc đình chỉ bất kỳ tài khoản đáng ngờ nào trong sàn giao dịch hoặc đóng toàn bộ sàn giao dịch. Trong khi sử dụng một sàn giao dịch chưa đăng ký, những sai sót hoặc thiếu kinh nghiệm của chủ sở hữu hoặc người dùng trong quá trình rút tiền có thể dẫn đến rò rỉ dữ liệu và cung cấp cho cơ quan chức năng bằng chứng dấu vết. Những lỗi như vậy có thể đơn giản như sử dụng cùng một địa chỉ hoặc mật khẩu cho nhiều mục đích hoặc tài khoản, không sử dụng các công cụ bảo vệ quyền riêng tư;

- Quản lý tiền mã hóa bằng hệ thống pháp luật toàn diện của quốc gia, khu vực: Quy định này có thể bao gồm từ lệnh cấm hoàn toàn đối với tiền mã hóa đến việc công nhận hợp pháp tiền mã hóa. [33]

Ngoài các biện pháp nêu trên, nhóm tác giả cũng phân tích một số biện pháp kiểm soát kỹ thuật có thể được triển khai để ngăn chặn những kẻ rửa tiền, nhưng trên thực tế, chúng đều gặp khó khăn cả về mặt kỹ thuật và thực tế khi triển khai trên quy mô lớn, như:[34]

- Theo dõi địa chỉ IP: Ngay cả khi kẻ phạm pháp sử dụng ứng dụng bảo vệ quyền riêng tư, chẳng hạn như trình duyệt TOR, nhà chức trách vẫn có thể theo dõi một phần địa chỉ IP. Mặc dù địa chỉ IP ban đầu vẫn không thể tìm thấy nhưng cơ quan chức năng có thể xem liệu địa chỉ IP đáng ngờ đang được điều tra có khớp với bất kỳ địa chỉ IP nào được liệt kê trong danh sách chuyển tiếp thoát của công cụ.

- Theo dõi chuỗi khối blockchain: Các giao dịch chuỗi khối có thể theo dõi, bất biến và không thể đảo ngược cho phép các cơ quan chức

33 Khoảng 111 quốc gia áp dụng cách tiếp cận sau trong khi một số quốc gia áp dụng cách tiếp cận trước. Nhìn chung, các quốc gia dường như thuộc hai loại, hiện đang phát triển các khuôn khổ tiền mã hóa hợp pháp hoặc đang chờ xem sự phát triển của nó. Đồng thời, không phải tất cả các quốc gia công nhận hợp pháp tiền mã hóa đều có luật chống rửa tiền nghiêm ngặt đối với việc sử dụng tiền mã hóa trong hoạt động rửa tiền. Hoa Kỳ, Canada, Anh, Úc và các quốc gia thành viên của Liên minh Châu Âu (E.U.) có luật chống rửa tiền áp dụng cho tiền mã hóa. Liên minh châu Âu cấm các quốc gia thành viên tạo và giới thiệu tiền mã hóa của riêng họ, trong khi các sàn giao dịch tiền mã hóa được khuyến khích duy trì tính hợp pháp bằng cách tuân thủ các quy định. Tại Hoa Kỳ, chính phủ liên bang có thể viện dẫn Điều khoản Thương mại (Điều I, Mục 8, Khoản 3) của Hiến pháp để điều chỉnh thị trường tiền mã hóa một cách rõ ràng. Một số quốc gia, chẳng hạn như Canada, Trung Quốc, Nga, Singapore, Hàn Quốc và Vương quốc Anh và các ngân hàng trung ương của họ đang xem xét phát triển và triển khai tiền mã hóa nhà nước được chính phủ hỗ trợ để cạnh tranh hoặc thay thế tiền mã hóa hiện có bằng nghị định. Xem Michael W. Calafos and George Dimitoglou, *tlđd*.

34 Michael W. Calafos and George Dimitoglou, *tlđd*.

năng sử dụng chuỗi khối và lịch sử giao dịch của nó cho mục đích điều tra, phát hiện hoạt động bất hợp pháp hoặc suy ra mối quan hệ xã hội giữa người dùng. Để làm như vậy, việc kiểm tra giao dịch blockchain bằng cách sử dụng khai thác dữ liệu rộng rãi và phân tích định tính và định lượng là cần thiết. Một dấu vết kiểm tra bất biến có thể được thiết lập bằng cách kiểm tra cẩn thận dữ liệu giao dịch trong quá khứ và hiện tại của blockchain, đồng thời thông tin cần thiết và các mẫu quan trọng có thể được suy ra, dẫn đến địa chỉ IP hoặc giao dịch của người dùng bị ẩn danh. Bằng cách liên kết các khóa công khai cụ thể với các giao dịch, các cặp khóa công khai/giao dịch có thể được phát triển trên các bộ dữ liệu và mạng cho phép ánh xạ cụm các mẫu hành vi và dẫn đến khả năng phát hiện ra những người dùng mạng cụ thể. Những mô hình này có thể tạo nên một bức tranh về thói quen mua sắm và chi tiêu cũng như tần suất giao dịch của người dùng, đồng thời xác định các vị trí địa lý.

4. Bài học kinh nghiệm cho Việt Nam về điều tra hoạt động rửa tiền qua không gian mạng

Theo báo cáo của Bộ Công an, trong khoảng 8 tháng đầu năm 2022, lực lượng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao toàn quốc đã phát hiện, khởi tố 474 vụ án, 1.071 bị can liên quan các loại tội phạm sử dụng công nghệ cao xâm phạm trật tự an toàn xã hội, đặc biệt là tội phạm đánh bạc, lừa đảo, chiếm đoạt tài sản, cho vay nặng lãi, tội phạm liên quan đến "tín dụng đen"… Trong đó, tội phạm lừa đảo, chiếm đoạt tài sản tăng mạnh trên không gian mạng với thủ đoạn tinh vi, chuyên nghiệp thông qua hoạt động của các sàn đầu tư chứng khoán, giao dịch vàng trên thị trường ngoại hối (*forex*), quyền chọn nhị phân (BO), giao dịch tiền "ảo", vàng "ảo", ngoại tệ "ảo", dự án bất động sản... hoặc hoạt động kinh doanh đa cấp trái phép.[35]

Tại Hội nghị tổng kết công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao năm 2023 do Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao (A05)[36] thuộc Bộ Công an tổ chức, một trong các kết quả đạt được là A05 phối hợp cơ quan điều tra các cấp khởi tố 46 vụ án, hơn 230 bị can trong các đường dây, ổ nhóm tội phạm quy mô lớn, hoạt động phức tạp, xuyên quốc gia, như: tổ chức

35 Văn Chúc, "Bộ Công an triển khai nhiều giải pháp xử lý nghiêm tội phạm công nghệ cao", *Báo Nhân dân*, 10/08/2022, https://nhandan.vn/bo-cong-an-trien-khai-nhieu-giai-phap-xu-ly-nghiem-toi-pham-cong-nghe-cao-post709689.html, truy cập ngày 18/01/2024.

36 Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) trực thuộc Bộ Công an Việt Nam là cơ quan đầu ngành về công tác bảo đảm an ninh và an toàn mạng, và các biện pháp phòng ngừa, phát hiện, điều tra xử lý tội phạm sử dụng công nghệ cao. Trong cơ cấu tổ chức, A05 gồm các phòng Phòng, chống tội phạm, phòng Nghiên cứu, phát triển giải pháp và phục hồi dữ liệu chứng cứ điện tử và Tổng công ty Công nghệ - Viễn thông Toàn Cầu (GTEL).

đánh bạc, đánh bạc, lừa đảo chiếm đoạt tài sản qua mạng; tội phạm cho vay tín dụng đen qua mạng quy mô lớn tại nhiều tỉnh thành do đối tượng người nước ngoài cầm đầu; hoạt động tấn công, chiếm đoạt, mua bán, trao đổi dữ liệu cá nhân nhằm mua bán, thực hiện hành vi vi phạm pháp luật...[37]

Với phương thức đa dạng về hoạt động rửa tiền qua không gian mạng (mục 2) và thách thức khi điều tra tội phạm này (mục 3), bài học kinh nghiệm cho Việt Nam gồm bốn vấn đề cơ bản là:

Thứ nhất là xây dựng khung pháp lý liên quan đến tiền mã hóa. Trước hết, Việt Nam cần thừa nhận tiền mã hóa là một loại tiền tệ và là phương tiện thanh toán hợp pháp. Vào giai đoạn đầu khi tiền mã hóa phát triển (khoảng thời gian từ năm 2011-2016), Ngân hàng Nhà nước Việt Nam khẳng định tiền ảo nói chung và Bitcoin, Litecoin nói riêng không phải là tiền tệ và không phải là phương tiện thanh toán hợp pháp theo quy định của pháp luật Việt Nam.[38] Tuy nhiên, với tình hình thực tế và xu hướng chung của thế giới, Việt Nam đang hoàn thiện dần về khung pháp lý liên quan đến tiền mã hóa. Trong đó, nghiên cứu, xây dựng và thí điểm sử dụng tiền ảo dựa trên công nghệ chuỗi khối (blockchain) là một trong những giải pháp để thực hiện Chiến lược phát triển Chính phủ điện tử.[39] Ngoài ra, Chính phủ cũng xem xét một trong những nhiệm vụ giải pháp nhằm thực hiện Kế hoạch Phát triển kinh tế - xã hội là tiếp tục rà soát, hoàn thiện khung pháp lý về hạ tầng thương mại điện tử; cơ chế thử nghiệm có kiểm soát; cơ chế quản lý tài sản ảo, tiền mã hóa, tiền ảo.[40]

Thứ hai, nâng cao năng lực của đội ngũ cán bộ công tác trong lực lượng an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao

37 Xuân Mai, "Nâng cao hiệu quả đấu tranh với tội phạm an ninh mạng và công nghệ cao", *Báo Công an Nhân dân*, 02/01/2024, https://cand.com.vn/lanh-dao-bo-cong-an/nang-cao-hieu-qua-dau-tranh-voi-toi-pham-an-ninh-mang-va-cong-nghe-cao-i719047/, truy cập ngày 20/01/2024.

38 Theo Công văn 5747/NHNN-PC của Ngân hàng Nhà nước Việt Nam ngày 21/07/2017 gửi Văn phòng Chính phủ đã khẳng định: "Tiền ảo nói chung và Bitcoin, Litecoin nói riêng không phải là tiền tệ và không phải là phương tiện thanh toán hợp pháp theo quy định của pháp luật Việt Nam. Việc phát hành, cung ứng và sử dụng tiền ảo nói chung và Bitcoin, Litecoin nói riêng (phương tiện thanh toán không hợp pháp) làm tiền tệ hoặc phương tiện thanh toán là hành vi bị cấm. Chế tài xử lý hành vi này đã được quy định tại Nghị định 96/2014/NĐ-CP của Chính phủ về xử phạt vi phạm hành chính trong lĩnh vực tiền tệ và ngân hàng và Bộ luật Hình sự 2015 (đã sửa đổi, bổ sung)".

39 Phần VI mục 5 điểm c, đ của Quyết định 942/QĐ-TTg ngày 15/6/2021 quyết định phên duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021-2025, định hướng đến năm 2030: "cụ thể, Thủ tướng giao Ngân hàng Nhà nước chủ trì nghiên cứu, xây dựng và thí điểm sử dụng tiền ảo dựa trên công nghệ chuỗi khối blockchain."

40 Phần II Mục 6 điểm đ của Nghị quyết 01/NQ-CP về nhiệm vụ, giải pháp chủ yếu thực hiện Kế hoạch phát triển kinh tế - xã hội, Dự toán ngân sách nhà nước và cải thiện môi trường kinh doanh, nâng cao năng lực cạnh tranh quốc gia năm 2023 do Chính phủ ban hành ngày 06/01/2023.

của Bộ Công An. Do đó, mỗi cán bộ, chiến sĩ phải nâng cao khả năng tự học hỏi, tự nghiên cứu kết hợp với việc đào tạo, tập huấn thông qua chương trình liên kết đào tạo với cơ quan an ninh, cảnh sát các nước và tổ chức an ninh mạng. Ngoài ra, theo một số thực tiễn công tác điều tra hoạt động rửa tiền (mục 3), lực lượng An ninh mạng phối hợp với Cơ quan điều tra các cấp cần theo dõi địa chỉ IP, lịch sử giao dịch tiền mã hóa, chuỗi khối blockchain.[41]

Thứ ba, các biện pháp kiểm soát phi kỹ thuật có thể làm gián đoạn hoặc ngăn cản các hoạt động rửa tiền qua không gian mạng như xác định danh tính khách hàng; theo dõi hoạt động của các sàn giao dịch đã đăng ký. Do đó, về mặt pháp luật, cần bổ sung những quy định chi tiết hoá trình tự, thủ tục thu thập, bảo quản, phục hồi, giải mã, chuyển hoá, kiểm tra, đánh giá và sử dụng nguồn chứng cứ là dữ liệu điện tử ngay trong Bộ luật Tố tụng hình sự năm 2015 hoặc văn bản hướng dẫn thi hành.[42] Ngoài ra, trong việc thu thập chứng cứ điện tử bằng các biện pháp điều tra tố tụng đặc biệt, cần bảo đảm quyền con người.[43]

Thứ tư, cần ứng dụng các kỹ thuật về công nghệ chuỗi khối blockchain nhằm phát hiện giao dịch đáng ngờ, bất hợp pháp. Một trong những kỹ thuật được sử dụng phổ biến nhất hiện nay là ứng dụng công nghệ máy học, một loại trí tuệ nhân tạo, cho phép máy học từ dữ liệu lớn và đưa ra các tiêu chí phân biệt, cuối cùng đạt được mục đích dự đoán dữ liệu chưa nhìn thấy. Tuy nhiên, khi sử dụng kỹ thuật này, người điều tra cần dữ liệu về các giao dịch và địa chỉ bất hợp pháp, để máy học có thể theo dõi. Công việc này gặp nhiều khó khăn bởi những kẻ rửa tiền sử dụng rất nhiều công cụ và kỹ thuật để che giấu các giao dịch (mục 2).

Kết luận

Động cơ chính thúc đẩy việc sử dụng tiền mã hóa (gồm cả Bitcoin và altcoin) trong hoạt động bất hợp pháp là mức độ ẩn danh

41 Phát biểu tại buổi họp báo thông báo tình hình kết quả công tác 6 tháng đầu năm 2023, về đồng tiền ảo Pi, A05 đang phối hợp với công an địa phương điều tra hoạt động kinh doanh lợi nhuận cao bất thường, có dấu hiệu lôi kéo, đa cấp. Xem Danh Trọng, "Cục An ninh mạng điều tra hoạt động liên quan giao dịch tiền ảo Pi", Báo Tuổi trẻ, 30/06/2023, https://tuoitre.vn/cuc-an-ninh-mang-dieu-tra-hoat-dong-lien-quan-giao-dich-tien-ao-pi-20230630112938412.htm, truy cập ngày 20/01/2023.

42 Lê Huỳnh Tấn Duy, "Xác định xu hướng phát triển của pháp luật Việt Nam về chứng cứ và chứng minh trong tố tụng hình sự", *Kỷ yếu Hội thảo Chứng cứ và chứng minh trong giải quyết vụ án hình sự,* do Khoa Luật Hình sự tổ chức tại Trường Đại học Luật TP. Hồ Chí Minh, 2023, tr. 34.

43 Lê Nguyên Thanh, "Chứng cứ điện tử và thu thập chứng cứ điện tử trong Tố tụng hình sự Việt Nam", *Kỷ yếu Hội thảo Chứng cứ và chứng minh trong giải quyết vụ án hình sự,* do Khoa Luật Hình sự tổ chức tại Trường Đại học Luật TP. Hồ Chí Minh, 2023, tr. 159-180.

được cung cấp bởi các địa chỉ chữ và số được sử dụng trong giao dịch. Với đặc điểm này và phạm vi tiếp cận toàn cầu, tiền mã hóa đã cung cấp một phương thức để các tổ chức tội phạm chuyển hoạt động rửa tiền truyền thống sang lĩnh vực rửa tiền qua không gian mạng. Với phương thức đa dạng, hoạt động rửa tiền qua không gian mạng thực hiện xuyên biên giới và xuyên khu vực pháp lý một cách bí mật, liền mạch và thực tế là ngay lập tức. Sẽ là một sai lầm nếu coi thường các thuật toán và công nghệ mới hỗ trợ khai thác, lưu trữ và trao đổi tiền mã hóa này. Giống như bất kỳ công nghệ đang phát triển nào, tiền mã hóa và chuỗi khối blockchain là những công nghệ mang lại lợi ích cho cả mục đích hợp pháp và bất hợp pháp. Chúng có thể góp phần cách mạng hóa cách thức tiến hành kinh doanh và tác động tích cực cũng như biến đổi nền kinh tế quốc gia và quốc tế nếu được quản lý và sử dụng phù hợp. Do đó, việc ghi nhận tiền ảo là một loại tài sản và ban hành quy định pháp luật toàn diện điều chỉnh loại tiền này là hướng đi phù hợp với tình hình thực tế của Việt Nam hiện nay cũng như bắt kịp xu thế chung của thế giới. Điều này cũng đặt ra thách thức về nỗ lực hợp tác quốc tế để thực hiện tính thống nhất quy định giữa các khu vực pháp lý khác nhau về hoạt động rửa tiền qua không gian mạng. ●

Tài liệu tham khảo

[1] Danton Bryans, "Bitcoin and money laundering: mining for an effective solution", *Indiana Law Journal*, Vol. 89:144, 2014

[2] K. J. Mc Carthy (ed.), *The Money Laundering Market: Regulating the criminal economy*, Agenda Publishing, 2018

[3] Kevin Daimi, Ioanna Dionysiou (ed.), *Principles and Practice of Blockchains*, Nour EI Madhoun, Springer, 2023

[4] Khoa Luật Hình sự, *Kỷ yếu Hội thảo Chứng cứ và chứng minh trong giải quyết vụ án hình sự*, Trường Đại học Luật TP. Hồ Chí Minh, 2023 [trans: Faculty of Criminal Law, *Proceedings of the Conference on Evidence and Proof in Resolving Criminal Cases*, Ho Chi Minh City University of Law, 2023]

[5] Armin Krishnan, "Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations", *Journal of Strategic Security*, Vol. 13, 2020

[6] Chang-Yi Lin, Hsiang-Kai Liao, Fu-Ching Tsai, "A Systematic Review of Detecting Illicit Bitcoin Transactions", *ScienceDirect*, Procedia Computer Science 207, 2022

[7] Rohan Maheshwari, Sriram Praveen V. A., Shobha G., Jyoti Shetty, Arjuna Chala, Hugo Watanuki, "Illicit Activity Detection in Bitcoin Transactions using Timeseries Analysis", *International Journal of Advanced Computer Science and Applications*, Vol. 14, No. 3, 2023

[8] S. Middlebrook and S. Hughes, "Regulating Cryptocurrencies in the United States: Current Issues and Future Directions", *William Mitchell Law Review*, Vol. 40, 2014

[9] Rolf van Wegberg, Jan-Jaap Oerlemans, and Oskar van Deventer, "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin", *Journal of Financial Crime*