

KINH NGHIỆM PHÒNG, CHỐNG RỬA TIỀN ĐỐI VỚI TÀI SẢN MÃ HÓA TẠI MỘT SỐ QUỐC GIA VÀ HÀM Ý VỚI VIỆT NAM

● NGUYỄN NGỌC HÀ¹ - TRẦN THỊ MINH THU^{1*} - TRẦN THU QUỲNH¹
- VŨ MINH TIẾN¹ - ĐINH NGUYỄN BẢO NGỌC¹ - NGUYỄN HỮU NHẬT MINH¹

¹Trường Đại học Ngoại thương
* Email: k62.2312450128@ftu.edu.vn

TÓM TẮT:

Bài báo nghiên cứu kinh nghiệm của Liên minh châu Âu và Singapore trong hoạt động phòng, chống rửa tiền đối với tài sản mã hóa, từ đó rút ra bài học kinh nghiệm cho Việt Nam. Những bài học đề xuất trong nghiên cứu gồm: hoàn thiện khung pháp lý và ban hành văn bản hướng dẫn chi tiết, đánh giá rủi ro toàn diện và tăng cường kiểm soát khách hàng, tăng cường minh bạch và khả năng truy vết giao dịch tài sản số, thiết lập cơ chế giám sát và thực thi hiệu quả.

Từ khóa: tài sản số, tài sản mã hóa, phòng chống rửa tiền, AML/CFT, pháp luật.

1. Đặt vấn đề

Sự phát triển nhanh chóng của công nghệ số đang tạo ra những thay đổi sâu rộng trên thế giới, trong đó tài sản số và các hoạt động giao dịch số đang trở thành một xu hướng toàn cầu. Bên cạnh những cơ hội về đổi mới sáng tạo và tăng trưởng kinh tế, tài sản số cũng đặt ra nhiều thách thức lớn đối với công tác phòng, chống rửa tiền, do đặc tính ẩn danh, phi biên giới và tốc độ giao dịch gần như tức thời. Nhiều quốc gia đã sớm xây dựng khung pháp lý và cơ chế giám sát đối với tài sản số, coi đây là lĩnh vực rủi ro cao cần quản lý chặt chẽ.

Tại Việt Nam, theo Báo cáo "Chỉ số Chấp nhận Tiền mã hóa Toàn cầu năm 2025" của Chainalysis, Việt Nam xếp thứ 4 thế giới về tỷ lệ chấp nhận tiền mã hóa, với khối lượng giao dịch on-chain đạt trên 200 tỷ USD trong giai đoạn khảo sát, cùng khoảng 17

triệu người dùng (Chainalysis, 2025; VBA, 2024). Tuy nhiên, sự phát triển nhanh của thị trường lại diễn ra trong bối cảnh khung pháp lý còn thiếu đồng bộ, cơ chế giám sát chưa theo kịp, và các giao dịch phi chính thức như P2P hay ví tự lưu ký vẫn nằm ngoài phạm vi quản lý. Việc Việt Nam bị đưa vào Danh sách Xám của FATF từ năm 2023 càng cho thấy yêu cầu cấp bách phải hoàn thiện hệ thống phòng, chống rửa tiền, đặc biệt trong lĩnh vực tài sản số với rủi ro ngày càng gia tăng và phức tạp.

Trong bối cảnh Chính phủ đang triển khai thí điểm thị trường tài sản mã hóa và từng bước xây dựng hành lang pháp lý, việc nghiên cứu kinh nghiệm quốc tế về phòng chống rửa tiền đối với tài sản số cho Việt Nam là cần thiết nhằm học hỏi các mô hình quản trị hiệu quả, bảo đảm an ninh tài chính và tạo nền tảng pháp lý an toàn cho đổi mới sáng tạo trong nền kinh tế số.

2. Kinh nghiệm phòng, chống rửa tiền đối với tài sản mã hóa của một số quốc gia

Hệ thống tài chính đóng một vai trò then chốt trong việc định hướng dòng vốn. Trong bối cảnh Việt Nam chưa có khung pháp lý đầy đủ về phòng, chống rửa tiền đối với tài sản mã hóa và đang chịu áp lực cải thiện tuân thủ do nằm trong Danh sách Xám của FATF, việc tham chiếu kinh nghiệm quốc tế là vô cùng cần thiết. Trong đó, Liên minh châu Âu và Singapore là 2 đại diện tiêu biểu. EU là khu vực tiên phong xây dựng bộ khung pháp lý AML/CFT toàn diện cho tài sản mã hóa thông qua Gói cải cách AML và MiCA. Singapore là trung tâm tài chính châu Á với mức độ tuân thủ cao, tích hợp quản lý tài sản mã hóa chặt chẽ thông qua quy trình hóa cụ thể bằng Hướng dẫn thực hiện Thông báo PSN02 về phòng, chống rửa tiền và tài trợ khủng bố đối với dịch vụ token thanh toán kỹ thuật số. Do vậy, việc nghiên cứu kinh nghiệm của EU và Singapore là cơ sở tham khảo quan trọng cho quá trình hoàn thiện công tác phòng, chống rửa tiền của Việt Nam.

2.1. Kinh nghiệm của Singapore

Singapore là một trong những trung tâm tài chính quốc tế có mức độ tuân thủ và hiệu quả thực thi phòng, chống rửa tiền (AML/CFT) thuộc nhóm cao tại châu Á. Theo Basel AML Index 2025, Singapore đạt 4,29 điểm, thuộc nhóm quốc gia có mức rủi ro rửa tiền thấp hơn đáng kể so với mức trung bình toàn cầu (khoảng 5,25 điểm), phản ánh chất lượng khung pháp lý và năng lực thực thi hiệu quả. Năm 2023, Singapore đã triệt phá vụ rửa tiền xuyên quốc gia lớn nhất trong lịch sử, với tổng tài sản bị phong tỏa và tịch thu lên tới hơn 3 tỷ SGD (khoảng 2,2 tỷ USD), trong đó có khoảng 38 triệu SGD tài sản mã hóa bị thu giữ (APNews, 2023). Bên cạnh đó, các chiến dịch thực thi AML chuyên biệt đối với crypto cũng được triển khai; điển hình là một cuộc truy quét trên toàn quốc đã điều tra 49 đối tượng liên quan đến việc sử dụng tài khoản tiền mã hóa để chuyển tiền bất hợp pháp và thu giữ hơn 200.000 SGD tài sản mã hóa (The Straits Times, 2025). Những con số này cho thấy, Singapore không chỉ xây dựng khung pháp lý phù hợp chuẩn mực FATF mà còn duy trì cường độ

thực thi mạnh mẽ, góp phần củng cố tính minh bạch và toàn vẹn của hệ thống tài chính quốc gia.

Cụ thể, Singapore không lựa chọn cách ban hành một đạo luật “riêng” cho tài sản mã hóa ngay từ đầu, mà tích hợp nghĩa vụ AML/CFT đối với dịch vụ token thanh toán số (DPT) vào khuôn khổ pháp luật tài chính hiện hành thông qua Payment Services Act và MAS Notice PSN02 (Khan và cộng sự, 2024). Trọng tâm đáng chú ý nằm ở Hướng dẫn thực hiện Thông báo PSN02 về phòng, chống rửa tiền và tài trợ khủng bố đối với dịch vụ token thanh toán kỹ thuật số: các nguyên tắc AML/CFT ở tầm khuyến nghị FATF được MAS chuyển hóa thành quy trình tác nghiệp có thể kiểm tra theo từng bước, từ đánh giá rủi ro cấp doanh nghiệp, phân loại khách hàng, kiểm soát giao dịch không gặp mặt, xác minh quyền kiểm soát ví, đến giám sát giao dịch on-chain và chuẩn hóa trường dữ liệu cho báo cáo STR liên quan DPT (MAS, 2025). Cách tiếp cận này cho thấy, AML/CFT được thiết kế như một hệ thống vận hành đồng bộ và liên kết chặt chẽ với nhau, thay vì chỉ là nghĩa vụ báo cáo “hậu kiểm”.

Thứ nhất, đánh giá rủi ro cấp toàn doanh nghiệp (Enterprise-wide Risk Assessment - EWRA). Guidelines PSN02 yêu cầu tổ chức cung cấp dịch vụ DPT thực hiện EWRA bao phủ toàn bộ mô hình kinh doanh (sản phẩm - dịch vụ, kênh phân phối, nhóm khách hàng, phạm vi địa lý), bao gồm cả chi nhánh/công ty con ở nước ngoài. Đáng chú ý, MAS yêu cầu doanh nghiệp xác định và đưa vào đánh giá các yếu tố rủi ro đặc thù của tài sản mã hóa, bao gồm: sử dụng công cụ ẩn danh (VPN/TOR), công nghệ làm mờ dấu vết giao dịch (mixers/tumblers), mức độ phức tạp của token/giao thức, giao dịch xuyên biên giới với khu vực AML yếu, và đặc biệt là giao dịch không có trung gian được quản lý. Ngoài ra, EWRA cũng phải được cập nhật định kỳ tối thiểu 2 năm 1 lần, hoặc sớm hơn khi có sự thay đổi trọng yếu trong mô hình kinh doanh, như triển khai sản phẩm mới, mở rộng thị trường hoặc áp dụng công nghệ mới. Điều này phản ánh nhận thức của Singapore có rủi ro rửa tiền trong crypto là động và tiến hóa nhanh, không thể kiểm soát hiệu quả nếu chỉ dựa vào đánh giá rủi ro tĩnh.

Thứ hai, kiểm soát khách hàng và quản lý giao dịch không gặp mặt (non-face-to-face). Do giao dịch DPT chủ yếu diễn ra non-face-to-face, nguy cơ mạo danh và sử dụng tài khoản trung gian (mule accounts) tăng lên. Singapore giải quyết thách thức này bằng cơ chế CDD/KYC theo hướng phân tầng theo rủi ro, kết hợp giấy tờ/nguồn xác minh khó làm giả (ID/hộ chiếu, registry độc lập, báo cáo kiểm toán...) với mức độ thẩm tra tương ứng hồ sơ rủi ro của khách hàng (MAS, 2025). Đáng chú ý, MAS khuyến nghị biện pháp bổ sung mang tính kỹ thuật là xác minh quyền kiểm soát ví (proof of wallet control): yêu cầu khách hàng thực hiện một giao dịch DPT giá trị nhỏ theo chỉ định để chứng minh quyền kiểm soát địa chỉ ví. Với nhóm rủi ro cao, các biện pháp thẩm tra nâng cao (Enhanced Due Diligence - EDD) được áp dụng, bao gồm thu thập thêm thông tin về nguồn tiền, mục đích giao dịch, bên thụ hưởng thực sự, và tăng cường giám sát giao dịch.

Thứ ba, giám sát giao dịch on-chain. Theo Hướng dẫn thực hiện Thông báo PSN02 của MAS đặt giám sát giao dịch liên tục ở vị trí trung tâm của hệ thống AML trong lĩnh vực tài sản mã hóa: tổ chức phải có năng lực truy vết lịch sử giao dịch DPT trên sổ cái phân tán ở mức phù hợp với rủi ro để nhận diện mô hình bất thường/dấu hiệu rửa tiền. MAS khuyến nghị sử dụng công cụ phân tích sổ cái phân tán (distributed ledger analytics tools) tương xứng quy mô và mức độ phức tạp của tổ chức, nhằm hỗ trợ phát hiện, đánh giá ra quyết định STR và phối hợp cơ quan thực thi pháp luật (MAS, 2025). Đồng thời, các tham số cảnh báo/giám sát phải được tài liệu hóa và thẩm định độc lập, nhằm bảo đảm “hiệu lực thực chất”, tránh tình trạng hệ thống chỉ tồn tại về mặt kỹ thuật.

Thứ tư, Travel Rule và giao dịch với ví tự lưu ký. Một đóng góp quan trọng của kinh nghiệm Singapore là cách xử lý giao dịch liên quan đến ví tự lưu ký (self-hosted wallets). MAS (2025) thừa nhận các yêu cầu chuyển thông tin theo Travel Rule không thể áp dụng một cách máy móc trong mọi trường hợp, đặc biệt khi bên gửi hoặc bên nhận không phải là một tổ chức được quản lý. Thay vì loại trừ hoàn toàn hoặc áp

dụng cứng nhắc, Singapore lựa chọn cách tiếp cận coi các giao dịch này là rủi ro cao và yêu cầu áp dụng các biện pháp giảm thiểu rủi ro tăng cường, như xác minh quyền kiểm soát ví bằng chuyển khoản dịch vụ token thanh toán số lượng được chỉ định, xác minh bên thứ ba bằng cách thực hiện xác minh bổ sung của non-face-to-face, xác định chủ sở hữu hưởng lợi và tăng cường giám sát. Cách tiếp cận này cho phép duy trì tính khả thi của quy định, đồng thời vẫn bảo đảm mục tiêu AML.

Thứ năm, báo cáo giao dịch đáng ngờ (Suspicious Transaction Reports - STRs) và cơ chế thực thi. Singapore chuẩn hóa mạnh mẽ hoạt động STR cho DPT bằng hướng dẫn chi tiết về trường thông tin cần khai báo, đặc biệt liên quan địa chỉ ví/dữ liệu định danh của dịch vụ token thanh toán số. Các chỉ dấu đáng ngờ điển hình gồm: truy cập tài khoản qua VPN/TOR; đăng ký bằng email mã hoá/ẩn danh/tạm thời; thay đổi thường xuyên thông tin định danh (địa chỉ, IP, bank/wallet liên kết); sử dụng bên thứ ba để che giấu người gửi/nhận; thiếu thông tin nguồn tiền/nguồn DPT... Trong trường hợp liên quan danh sách trừng phạt, MAS yêu cầu báo cáo trong thời hạn rất ngắn (không quá 1 ngày làm việc), cho thấy mức độ nghiêm khắc trong thực thi. Cơ chế giám sát kết hợp giữa giám sát từ xa (off-site supervision) và thanh tra tại chỗ (on-site inspection) tạo áp lực tuân thủ thực chất đối với tổ chức cung cấp dịch vụ DPT.

2.2. Kinh nghiệm của EU

EU là một trong những khu vực đi đầu trong việc xây dựng hệ thống quản lý tài sản mã hóa gắn với phòng chống rửa tiền. Để tạo ra khuôn khổ thống nhất có hiệu lực trực tiếp trên toàn khối, EU đã triển khai Gói cải cách AML năm 2021 (EU AML Package), gồm 3 trụ cột chính: (i) Quy định về Phòng chống Rửa tiền (AMLR - Regulation (EU) 2024/1624); (ii) Quy định thành lập Cơ quan Phòng chống Rửa tiền Châu Âu (AMLA - Regulation (EU) 2024/1620); và (iii) Quy định Chuyển tiền sửa đổi (TFR Recast - Regulation (EU) 2023/1113).

Thứ nhất, EU đã thành lập Cơ quan Phòng chống Rửa tiền châu Âu (Anti-Money Laundering Authority - AMLA) theo Regulation (EU)

2024/1620, một cơ quan có thẩm quyền tập trung và độc lập, chịu trách nhiệm điều phối và giám sát toàn bộ hoạt động phòng, chống rửa tiền trong khối. Cụ thể, AMLA đã thiết lập cơ chế giám sát trực tiếp tới đa 40 thực thể rủi ro cao nhất (Selected Obligated Entities - SOEs), tạo ra một “vùng trọng điểm” để tập trung nguồn lực, thay vì dàn trải như trước. Selected obliged entities là các tổ chức được FATF xác định phải tuân thủ đầy đủ nghĩa vụ AML/CFT vì thuộc nhóm có rủi ro rửa tiền cao. Đây là nhóm đối tượng báo cáo (reporting entities) được pháp luật chỉ định phải thực hiện các nghĩa vụ như: nhận biết khách hàng (KYC), lưu trữ hồ sơ, giám sát giao dịch, báo cáo giao dịch đáng ngờ (STR), báo cáo giao dịch giá trị lớn, và áp dụng các biện pháp kiểm soát rủi ro. Nhóm này thường bao gồm: ngân hàng, tổ chức tài chính, công ty chứng khoán, bảo hiểm, kế toán - kiểm toán, luật sư, công chứng, bất động sản, casino, tổ chức kinh doanh vàng, và trong bối cảnh mới là VASP. Chính vì vậy, EU đã hình thành được một hệ sinh thái giám sát thống nhất, giảm đáng kể khoảng trống pháp lý giữa các quốc gia.

Thứ hai, Quy định Phòng chống Rửa tiền của Liên minh châu Âu (AMLR - Regulation 2024/1624) là văn bản trung tâm trong gói cải cách mới của EU. Điểm đổi mới quan trọng nhất là đưa nhà cung cấp dịch vụ tài sản mã hóa (Crypto-Asset Service Provider - CASP) vào nhóm “đối tượng báo cáo” ngang hàng với các định chế tài chính truyền thống, buộc họ tuân thủ đầy đủ các nghĩa vụ như quản trị rủi ro, kiểm toán độc lập, báo cáo giao dịch đáng ngờ và thẩm định khách hàng. Song song đó, AMLR tăng cường mạnh mẽ minh bạch chủ sở hữu hưởng lợi (Beneficial Ownership - BO) thông qua yêu cầu xác thực thông tin về chủ sở hữu hưởng lợi bởi cơ quan nhà nước và kết nối dữ liệu về chủ sở hữu hưởng lợi với các cơ sở dữ liệu trọng yếu như thuế và đăng ký doanh nghiệp, nhằm ngăn chặn việc sử dụng công ty vỏ bọc để che giấu dòng tiền. Không chỉ cơ quan nhà nước, AMLR còn mở rộng quyền truy cập dữ liệu chủ sở hữu hưởng lợi cho các tổ chức có nghĩa vụ báo cáo (Obligated Entities) và những chủ thể có lợi ích hợp pháp (như nhà báo điều

tra hay các tổ chức dân sự), nhằm hỗ trợ họ đánh giá rủi ro và phát hiện giao dịch đáng ngờ. Việc mở rộng này tạo thêm một lớp giám sát xã hội bên cạnh giám sát nhà nước, qua đó tăng cường minh bạch và khả năng truy vết trong toàn bộ hệ thống tài chính. Bên cạnh đó, Quy định AMLR còn bao gồm một số biện pháp bổ trợ: (i) thiết lập trần thanh toán tiền mặt 10.000 EUR để giảm giao dịch không truy vết và thúc đẩy hình thành “dấu vết giao dịch” điện tử; (ii) tiến hành thẩm định khách hàng (CDD/EDD) thống nhất trên toàn EU, trong đó giao dịch tài sản số không bao giờ được phép áp dụng thẩm định đơn giản; và (iii) cấm tuyệt đối các đồng tiền mã hóa ẩn danh (privacy coins) như Monero, Zcash hay Dash đối với mọi CASP được cấp phép, do đặc tính không thể truy vết giao dịch.

Thứ ba, Quy định về Chuyển tiền sửa đổi (TFR Recast - Regulation (EU) 2023/1113) là công cụ kỹ thuật cốt lõi bảo đảm tính minh bạch cho mọi giao dịch tài sản số trong EU. Quy định TFR chuyển hóa Travel Rule của FATF thành nghĩa vụ pháp lý bắt buộc, yêu cầu thông tin định danh của người khởi tạo và người thụ hưởng phải đi kèm với mọi giao dịch tài sản số - khắc phục hạn chế của blockchain vốn chỉ hiển thị địa chỉ ví ẩn danh. Theo TFR và hướng dẫn của EBA, CASP của người gửi phải thu thập và truyền ngay cho CASP thụ hưởng bộ dữ liệu tối thiểu gồm tên đầy đủ, địa chỉ hoặc mã địa lý quốc gia, địa chỉ ví, cùng thông tin pháp lý và giấy phép của CASP gửi và nhận (EBA, 2024). Các trường dữ liệu này được chuẩn hóa theo 2 bộ tiêu chuẩn IVMS101 (chuẩn dữ liệu theo ISO 20022 dùng cho CASP - ngân hàng) và IVMS400 (chuẩn JSON dùng cho CASP - CASP), bảo đảm mọi hệ thống có thể trao đổi dữ liệu thống nhất.

Thông tin Travel Rule không được ghi lên blockchain mà được truyền off-chain thông qua API mã hóa để bảo mật, sau đó được liên kết với giao dịch on-chain bằng transaction hash nhằm phục vụ truy vết. CASP thụ hưởng có trách nhiệm kiểm tra tính đầy đủ và đối chiếu với dữ liệu KYC; nếu phát hiện thiếu thông tin, sai lệch hoặc rủi ro cao, họ có quyền yêu cầu bổ sung, tạm giữ giao dịch hoặc từ chối. TFR

cũng đặt ra thời hạn xử lý nghiêm ngặt: giao dịch thiếu thông tin phải bị tạm giữ trong 24 giờ và bị từ chối sau 14 ngày nếu không được bổ sung.

Ngoài ra, một trong những điểm nổi bật trong Quy định TFR là áp dụng “ngưỡng zero” (zero threshold) - tức là yêu cầu thu thập và truyền tải thông tin định danh cho mọi giao dịch tài sản số, không phân biệt giá trị lớn hay nhỏ. Trong khi Khuyến nghị số 16 của FATF chỉ yêu cầu áp dụng Travel Rule đối với các giao dịch chuyển tiền có giá trị trên 1.000 USD/EUR, TFR của EU loại bỏ hoàn toàn ngưỡng này và yêu cầu áp dụng cho mọi giao dịch chuyển tài sản số, nhằm vô hiệu hóa kỹ thuật chia nhỏ giao dịch (smurfing/structuring) vốn cho phép tội phạm phân tán dòng tiền thành hàng nghìn giao dịch nhỏ để tránh bị phát hiện. Cuối cùng, TFR thiết lập cơ chế “áp lực ngang hàng” (peer pressure) giữa các CASP. Nếu CASP thụ hưởng phát hiện CASP gửi thường xuyên cung cấp thông tin thiếu hoặc sai, họ phải báo cáo cho cơ quan giám sát và có thể đưa CASP vi phạm vào danh sách cảnh báo hoặc từ chối giao dịch trong tương lai.

Thứ tư, bên cạnh Gói cải cách mới của EU, Quy định về Thị trường Tài sản Mã hóa (MiCA) được xem là khung pháp lý toàn diện đầu tiên trên thế giới điều chỉnh hoạt động phát hành và cung cấp dịch vụ liên quan đến tài sản số. MiCA thiết lập một cơ chế cấp phép nghiêm ngặt đối với các CASP, và việc được cấp phép là điều kiện tiên quyết để hoạt động hợp pháp trong toàn EU thông qua cơ chế “passporting”. Trong quá trình thẩm định, cơ quan quản lý quốc gia không chỉ đánh giá năng lực tài chính, kỹ thuật và quản trị của doanh nghiệp, mà còn tiến hành đánh giá “tính Thích hợp và Đúng đắn” (Fit and Proper Assessment) đối với ban quản lý cấp cao và các cổ đông lớn. Việc đánh giá này bao gồm kiểm tra lý lịch tư pháp, xem xét liệu họ có từng liên quan đến các hành vi như rửa tiền, gian lận hay tham nhũng, và đánh giá năng lực chuyên môn của họ trong quản trị rủi ro.

Bên cạnh đó, MiCA yêu cầu hồ sơ xin cấp phép phải chứng minh CASP đã xây dựng một hệ thống kiểm soát nội bộ toàn diện để đáp ứng các nghĩa vụ

phòng ngừa rủi ro từ ngày đầu hoạt động. Điều này bao gồm: quy trình định danh và thẩm định khách hàng (KYC/CDD/EDD); hệ thống giám sát giao dịch nhằm phát hiện mẫu hình bất thường; quy trình báo cáo giao dịch đáng ngờ; chương trình đào tạo nhân viên; và một bộ phận tuân thủ độc lập với Giám đốc Tuân thủ có đủ thẩm quyền và nguồn lực. Cơ quan cấp phép có thể tham vấn cơ quan chuyên trách và Đơn vị Tình báo Tài chính (FIU) để xác minh liệu doanh nghiệp có đang bị xem xét hoặc điều tra về các hành vi rủi ro hay không. Quan trọng hơn, MiCA quy định việc duy trì các biện pháp kiểm soát rủi ro hiệu quả là điều kiện để giữ giấy phép, chứ không chỉ là yêu cầu tại thời điểm xin phép. Do đó, CASP có thể bị áp dụng biện pháp cưỡng chế hoặc thu hồi giấy phép nếu không duy trì được hệ thống kiểm soát phù hợp trong quá trình hoạt động.

Có thể thấy, EU đã xây dựng một mô hình quản lý tài sản số mang tính hệ thống, trong đó phòng chống rửa tiền được tích hợp đồng bộ vào mọi cấu phần của thị trường. Nhờ sự kết hợp này, EU hình thành một hệ sinh thái quản lý khép kín, nơi chỉ những thực thể có năng lực tuân thủ thực chất mới có thể tham gia và vận hành trong thị trường tài sản số.

3. Hàm ý với Việt Nam

Từ kinh nghiệm quản lý AML/CFT đối với tài sản mã hóa của Singapore và Liên minh Châu Âu (EU), có thể rút ra một số hàm ý với Việt Nam như sau:

- Hoàn thiện khung pháp lý và ban hành văn bản hướng dẫn chi tiết: Từ kinh nghiệm của EU, Việt Nam cần xây dựng hệ thống văn bản pháp lý xác định rõ các đối tượng có nghĩa vụ tuân thủ trong lĩnh vực tài sản mã hóa, điển hình như các tổ chức cung cấp dịch vụ tài sản số (VASP/CASP) và các tổ chức tài chính có liên quan. Đồng thời, cần ban hành các hướng dẫn tác nghiệp cụ thể cho doanh nghiệp từ đánh giá rủi ro cho đến giám sát và báo cáo giao dịch đáng ngờ.

- Đánh giá rủi ro toàn diện và tăng cường kiểm soát khách hàng: Từ kinh nghiệm của Singapore, Việt Nam cần yêu cầu các tổ chức cung cấp dịch vụ tài sản mã hóa thực hiện đánh giá rủi ro toàn diện trên nhiều khía cạnh như sản phẩm, khách hàng, kênh giao dịch

và phạm vi địa lý. Đồng thời, cần tăng cường cơ chế KYC/CDD theo hướng phân tầng rủi ro thông qua thu thập hồ sơ định danh đáng tin cậy và áp dụng thẩm tra nâng cao đối với khách hàng hoặc giao dịch có mức độ rủi ro cao.

- Tăng cường minh bạch và khả năng truy vết giao dịch tài sản số: Thông qua Travel Rule, các giao dịch tài sản số phải kèm theo thông tin định danh của người gửi và người nhận, đồng thời tăng cường minh bạch về chủ sở hữu hưởng lợi. Từ kinh nghiệm này của EU và Singapore, Việt Nam có thể xem xét xây dựng cơ chế bảo đảm các thông tin nhận diện quan trọng - như danh tính khách hàng, địa chỉ ví, mã giao dịch và dữ liệu kỹ thuật liên quan - được ghi nhận và truyền tải đồng bộ cùng giao dịch tài sản số, qua đó hỗ trợ cơ quan chức năng theo dõi dòng tiền, phân

tích rủi ro và phát hiện các mô hình giao dịch bất thường bằng các công cụ phân tích dữ liệu blockchain.

- Thiết lập cơ chế giám sát và thực thi hiệu quả: Kinh nghiệm của EU và Singapore cho thấy hiệu quả phòng, chống rửa tiền trong lĩnh vực tài sản mã hóa phụ thuộc rất lớn vào năng lực giám sát và thực thi. Chính vì vậy, Việt Nam cần xây dựng một cơ chế giám sát tích hợp và liên tục, kết hợp giám sát kỹ thuật từ xa bằng công cụ phân tích blockchain, thanh tra tại chỗ, và hệ thống báo cáo giao dịch đáng ngờ với dữ liệu kỹ thuật được chuẩn hóa để kịp thời xử lý. Đồng thời, cần tăng cường phối hợp liên ngành giữa các bên liên quan để chia sẻ dữ liệu, phân tích dòng tiền on-chain và hỗ trợ điều tra các hành vi rửa tiền liên quan đến tài sản số ■

TÀI LIỆU THAM KHẢO:

VBA (2024). Báo cáo thị trường blockchain Việt Nam 2024.

APNews (2023). Gold, watches and other luxury items totaling \$1.75B seized in Singapore money laundering scheme. <https://apnews.com/article/singapore-money-laundering-asset-seizure-7640db7f784c05ac9024ef877aba1045>.

Chainalysis (2025). The 2025 Global Adoption Index: India and the United States Lead Cryptocurrency Adoption. <https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/>.

EBA (2024). Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113. <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countermeasures/financing-terrorism/guidelines-information-requirements-relation-transfers-funds-and-certain-crypto-assets-transfers>.

EUR-Lex (2023a). Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance). <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng>.

EUR-Lex (2023b). Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance).

EUR-Lex.(2024a). Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (Text with EEA relevance). <https://eur-lex.europa.eu/eli/reg/2024/1620/oj/eng>.

EUR-Lex (2024b). Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Text with EEA relevance). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1624>.

Khan A., Jillani M. A. H. S., Ullah M., & Khan M. (2025). Regulatory strategies for combatting money laundering in the era of digital trade. *Journal of Money Laundering Control*, 28(2), 408-423. <https://doi.org/10.1108/JMLC-07-2024-0113>.

MAS (2025). Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service. <https://www.mas.gov.sg/regulation/guidelines/guidelines-to-notice-psn02-on-aml-and-cft---dpt>.

Statbase (2025). Basel AML index | Singapore [Dataset].

The StraitsTimes (2025). 49 under probe for suspected money laundering involving crypto accounts; over \$200k seized. <https://www.straitstimes.com/singapore/49-under-investigation-for-suspected-money-laundering-involving-crypto-accounts-over-200k-seized>.

Ngày nhận bài: 20/01/2026

Ngày phản biện đánh giá và sửa chữa: 06/02/2026

Ngày chấp nhận đăng bài: 26/02/2026

COMPARATIVE APPROACHES TO COMBATING MONEY LAUNDERING THROUGH CRYPTO-ASSETS: INTERNATIONAL EXPERIENCES AND IMPLICATIONS FOR VIETNAM

- **NGUYEN NGOC HA¹**
- **TRAN THI MINH THU¹**
- **TRAN THU QUYNH¹**
- **VU MINH TIEN¹**
- **DINH NGUYEN BAO NGOC¹**
- **NGUYEN HUU NHAT MINH¹**

¹Foreign Trade University

ABSTRACT:

This study examines the regulatory experiences of the European Union and Singapore in combating money laundering through crypto-assets, with a view to deriving lessons for Vietnam. Through a comparative analysis, the study identifies key approaches adopted by these jurisdictions, including the development of comprehensive legal frameworks accompanied by detailed implementing guidelines, the conduct of systematic risk assessments alongside strengthened customer due diligence measures, the enhancement of transparency and traceability in digital asset transactions, and the establishment of robust monitoring and enforcement mechanisms. Overall, the findings provide a structured basis for understanding effective regulatory responses to the risks of money laundering in the evolving crypto-assets.

Keywords: digital assets, crypto-assets, anti-money laundering, AML/CFT, law.