



Australian Government



**GLOBAL
INITIATIVE**
AGAINST TRANSNATIONAL
ORGANIZED CRIME

KHU VỰC MEKONG GIÁM SÁT RỦI RO



ẤN PHẨM SỐ 1
THÁNG 12, 2025



Australian Government

TUYÊN BỐ MIỄN TRỪ TRÁCH NHIỆM

Ấn phẩm này được xây dựng với sự tài trợ của Chính phủ Australia thông qua Bộ Ngoại giao và Thương mại. Các quan điểm được trình bày trong ấn phẩm này là quan điểm riêng của các tác giả và không nhất thiết phản ánh quan điểm của Chính phủ Australia.

© 2025 Sáng kiến Toàn cầu chống Tội phạm có Tổ chức xuyên quốc gia.
Mọi quyền được bảo lưu.

Không một phần nào của ấn phẩm này được phép sao chép hoặc truyền tải dưới bất kỳ hình thức hay phương tiện nào khi chưa có sự cho phép bằng văn bản của Sáng kiến Toàn cầu.

Mọi thắc mắc xin vui lòng gửi tới:
Sáng kiến Toàn cầu chống Tội phạm có Tổ chức xuyên quốc gia
Avenue de France 23
Geneva, CH-1202
Thụy Sĩ
www.globalinitiative.net



GIÁM SÁT RỦI RO KHU VỰC MEKONG

Chào mừng bạn đến với số đầu tiên của Giám sát Rủi ro khu vực Mekong. Ấn phẩm này là bản tin định kỳ của Mạng lưới Mekong chống tội phạm xuyên quốc gia (MNET-CTC), một chương trình hợp tác được triển khai theo mô hình đối tác giữa Sáng kiến Toàn cầu chống Tội phạm có Tổ chức xuyên quốc gia (GI-TOC) và Chính phủ Australia. Ấn phẩm theo dõi các diễn biến trong các nền kinh tế phi pháp tại Campuchia, Lào, Myanmar, Thái Lan và Việt Nam, cũng như mối liên hệ của chúng với các vấn đề về phát triển khu vực, quản trị và an ninh. Nội dung được xây dựng dựa trên cả nguồn thông tin sơ cấp và thứ cấp, bao gồm phỏng vấn các bên liên quan chủ chốt như nhà báo và quan chức nhà nước, đóng góp từ xã hội dân sự, cùng việc theo dõi các nguồn tài liệu mở, nhằm cung cấp các phân tích dựa trên bằng chứng về những mối đe dọa và hiểm họa tồn tại đang nổi lên.

Mỗi số ấn phẩm báo cáo về các xu hướng và trọng tâm trong các thị trường tội phạm của các quốc gia này, đồng thời đặt các diễn biến tại địa phương trong bối cảnh rộng hơn của những động lực khu vực và toàn cầu, qua đó

Nội dung ấn phẩm

Ấn phẩm đầu tiên tập trung phân tích năm yếu tố có mối liên hệ chặt chẽ với nhau, vốn định hình các nền kinh tế trong khu vực. Bài viết thứ nhất theo dõi việc sử dụng tài sản tiền mã hóa trong các hoạt động tội phạm tài chính tại Việt Nam, phân tích sự gia tăng của các hình thức lừa đảo liên quan đến tài sản số và các mô hình rửa tiền, đồng thời chỉ ra những khoảng trống trong cơ chế giám sát và quản lý mà các đối tượng tội phạm vẫn đang lợi dụng. Bài viết thứ hai xem xét những diễn biến gần đây của các hoạt động lừa đảo trên không gian mạng tại Đặc khu Kinh tế Tam giác Vàng ở Lào, đánh giá các biện pháp ứng phó mới nhất của chính phủ, đồng thời thảo luận những tác động tiềm tàng của các động thái này đối với tương lai của khu vực. Bài viết thứ ba tập trung vào phụ nữ Campuchia có nguy cơ cao bị bóc lột; điều tra tình trạng buôn bán cô dâu sang Trung Quốc vốn đã tồn tại từ lâu

góp phần nâng cao hiểu biết về tội phạm có tổ chức tại khu vực Mekong. Ấn phẩm này hướng tới việc hỗ trợ hoạch định chính sách và triển khai các chương trình dựa trên bằng chứng, qua đó nâng cao khả năng phục hồi và thúc đẩy hợp tác giữa chính phủ, xã hội dân sự và các đối tác quốc tế. Nội dung tập trung vào bốn thị trường tội phạm chính: lợi dụng và xâm hại tình dục phụ nữ và trẻ em gái, các hoạt động lừa đảo trực tuyến, buôn bán ma túy và tội phạm tài chính. Mục tiêu của ấn phẩm là làm rõ cách những thay đổi về chính trị, kinh tế và công nghệ tạo ra cơ hội cho tội phạm có tổ chức, cũng như cách các chính phủ, cộng đồng và xã hội dân sự ứng phó với những thách thức này.

Chúng tôi khuyến khích độc giả và các cộng tác viên chia sẻ phản hồi, dữ liệu hoặc ý tưởng cho các số ấn phẩm trong tương lai, nhằm làm nổi bật các xu hướng mới, bổ sung bằng chứng thực tiễn hoặc đặt các diễn biến hiện tại trong bối cảnh thị trường tội phạm của khu vực. Vui lòng liên hệ đội ngũ MNET-CTC tại: ioannis.vlassis@globalinitiative.net.

nhưng vẫn chưa chấm dứt; đồng thời làm rõ vai trò tiếp tay của các bên trung gian và một bộ phận quan chức trong việc duy trì hoạt động mua bán người này. Bài viết thứ tư phân tích cách các dịch vụ giao hàng dựa trên ứng dụng tại Thái Lan bị các mạng lưới buôn bán ma túy lợi dụng cho hoạt động phân phối, qua đó làm mờ ranh giới giữa dịch vụ hợp pháp và hệ thống hậu cần phục vụ các mục đích tội phạm. Bài viết cuối cùng đánh giá tình trạng vận chuyển tiền mặt trái phép ra vào Lào, làm rõ vai trò trung tâm của tiền mặt trong nền kinh tế tội phạm địa phương, cũng như cách các đường biên giới lỏng lẻo và những hạn chế về năng lực quản lý đã tạo điều kiện cho các dòng tiền xuyên biên giới. Tổng thể, các bài viết này làm nổi bật những rủi ro mà tội phạm có tổ chức gây ra đối với cộng đồng, các thiết chế nhà nước và nền kinh tế địa phương trong khu vực Mekong.

DIỄN BIẾN VIỆC SỬ DỤNG TÀI SẢN TIỀN MÃ HÓA TRONG TỘI PHẠM TÀI CHÍNH TẠI VIỆT NAM

Vào tháng 2 năm 2025, Công an Hà Nội đã bắt giữ một người đàn ông Việt Nam, 32 tuổi, với cáo buộc là chủ mưu của một mô hình Ponzi hoạt động trên phạm vi toàn quốc, liên quan đến một nền tảng tiền mã hóa giả mạo mang tên CrossFi. Hơn 1.900 nhà đầu tư đã bị dụ dỗ đầu tư tổng cộng hơn 2.000 tỷ đồng (hơn 75 triệu USD) vào một dự án mà họ tin là ứng dụng công nghệ blockchain tiên tiến. Theo thông tin từ Công an Thành phố Hà Nội, các đối tượng đứng sau vụ lừa đảo đã ngưng trang hoạt động của mình dưới vỏ bọc các dự án kinh doanh hợp pháp và dự án tiền ảo, đưa ra những cam kết lợi nhuận cực kỳ cao. Bị hấp dẫn bởi các mức lợi nhuận này, nhiều nhà đầu tư đã trở thành nạn nhân của vụ lừa đảo, trong đó có một trường hợp được cho là đã chịu thiệt hại lên tới 13 tỷ đồng (hơn 490.000 USD).¹

Đây không phải là một vụ việc riêng lẻ. Từ đầu năm 2024 đến giữa năm 2025, Việt Nam đã chứng kiến sự gia tăng chưa từng có của các hoạt động tội phạm liên quan đến tiền mã hóa, đặc biệt là các vụ lừa đảo đầu tư quy mô lớn và hoạt động rửa tiền xuyên quốc gia. Mặc dù các cơ quan thực thi pháp luật và cơ quan quản lý đã tăng cường cảnh báo tới công chúng, làn sóng tội phạm này vẫn bộc lộ rõ các lỗ hổng nghiêm trọng trong kiểm soát pháp lý, năng lực điều tra và cơ chế giám sát tài chính xuyên quốc gia.

Hàng chục vụ bắt giữ với quy mô lớn, các đợt tịch thu tài sản và những bước đột phá trong điều tra tại hơn một chục tỉnh, thành cho thấy Việt Nam đã trở thành một “điểm nóng” của các vụ lừa đảo tiền mã hóa kết hợp – những thủ đoạn pha trộn giữa mô hình Ponzi truyền thống với thao túng token (mã thông báo) và các kỹ thuật tấn công tâm lý. Các vụ lừa đảo này thường liên quan đến việc xây dựng các nền tảng đầu tư giả mạo, phát hành các loại tiền mã hóa không được niêm yết hoặc giả mạo (ví dụ: MTC, PAYN, MPX, CBP), và kèm theo các cam kết về trả lãi hàng ngày. Để tạo dựng uy tín, các đối tượng thường tổ chức các hội nghị xa hoa tại khách sạn năm sao, phô trương sự giàu có trên các nền tảng mạng xã hội,

đồng thời áp dụng các chiến thuật tiếp thị đa cấp nhằm nhanh chóng mở rộng mạng lưới nạn nhân.

Vụ việc khét tiếng nhất có thể kể đến là vụ lừa đảo Matic Chain. Hiện vụ việc đã được cơ quan chức năng khởi tố. Các đối tượng trong vụ án này sử dụng nền tảng quyền chọn nhị phân – một hình thức giao dịch trực tuyến trong đó người tham gia dự đoán giá của một tài sản sẽ tăng hay giảm trong một khoảng thời gian nhất định. Tuy nhiên, kết quả giao dịch đã bị các đối tượng thao túng, qua đó thu hút hơn 138.000 tài khoản nhà đầu tư và gây thiệt hại với ước tính gần 10.000 tỷ đồng (khoảng 394 triệu USD).² Trong vụ PaynetCoin, hiện vẫn đang trong quá trình điều tra, các đối tượng đã lừa đảo hơn 500.000 nhà đầu tư trên phạm vi cả nước, với tổng thiệt hại ước tính lên tới hàng nghìn tỷ đồng. Trong giai đoạn đầu điều tra, cơ quan chức năng đã thu giữ khoảng 800 tỷ đồng tiền mặt (tương đương hơn 30 triệu USD).³

Trước đó, nhiều vụ lừa đảo lớn đã bị truy tố, như vụ CrossFi, Cashback Pro và Toptrade1. Các vụ này đều sử dụng thủ đoạn tương tự, và gây thiệt hại từ 2.000 tỷ đến hơn 5.000 tỷ đồng mỗi vụ (tương đương khoảng 80 triệu đến hơn 200 triệu USD). Những nền tảng này thường sụp đổ chỉ sau 6 đến 12 tháng hoạt động, người dùng không thể rút tiền và toàn bộ dữ liệu lưu trữ cũng bị xóa sạch.

Trong vụ việc gần đây nhất, xảy ra vào tháng 8 năm 2025, Công an tỉnh Lào Cai đã bắt giữ 25 đối tượng liên quan đến một đường dây lừa đảo tiền mã hóa hoạt động trên cả nước. Nhóm này sử dụng các nền tảng đầu tư giả mạo để dụ dỗ hơn 10.000 nhà đầu tư, gây thiệt hại ước tính lên tới hàng chục nghìn tỷ đồng.⁴ Các vụ việc tương tự và quá trình điều tra liên quan được tổng hợp trong Hình 1.

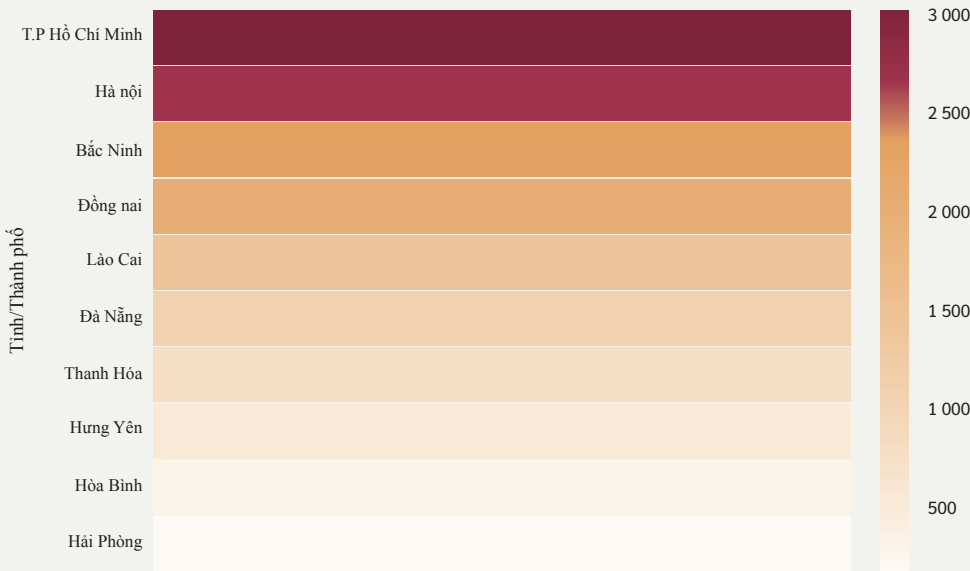
Tên vụ	Địa điểm	Loại hình lừa đảo/tội phạm	Thiệt hại ước tính (VND)	Phương thức, thủ đoạn chính
Matrix Chain	Toàn quốc	Lừa đảo kết hợp Ponzi và kinh doanh đa cấp	~ 10 nghìn tỷ	Xây dựng ứng dụng DeFi phát hành token và dàn dựng các hội thảo nhằm tạo lòng tin
Cashback Pro	Hà Nội, TP. Hồ Chí Minh	Mô hình đa cấp kim tự tháp	~ nghìn tỷ	Lợi nhuận phi thực tế, marketing trên mạng xã hội
PaynetCoin	Toàn quốc	Lừa đảo token và rửa tiền ngoài sàn (OTC)	~ nghìn tỷ	Phát hành coin giả, sử dụng môi giới ngoài sàn (OTC)
CrossFi	TP. Hồ Chí Minh	Rửa tiền và token giả mạo	~ 2 nghìn tỷ	Chuyển dòng USDT qua Binance
Madam Ngo case	Phạm vi khu vực	Rửa tiền xuyên quốc gia	~ 7.9 nghìn tỷ	Thuê tài khoản ngân hàng, chuyển đổi sang USDT
Naga Kingdom	Lào Cai	Lừa đảo dựa trên trò chơi	~ 200 tỷ	Xây dựng game NFT lừa đảo và dàn dựng các sự kiện nhằm tạo lòng tin

HÌNH 1 Các vụ lừa đảo và rửa tiền liên quan đến tiền mã hóa đáng chú ý tại Việt Nam, 2024–2025.

NGUỒN: Phân tích GI-TOC dựa trên dữ liệu phân bố vụ án theo tỉnh, trích từ các báo cáo của CAND Online¹¹

Để minh họa rõ hơn quy mô thiệt hại không đồng đều, Hình 2 tổng hợp mức thiệt hại ước tính từ các vụ lừa đảo và rửa tiền liên quan đến tiền mã hóa đáng chú ý được ghi nhận tại Việt Nam trong giai đoạn 2024–2025. Dù các vụ việc mới vẫn tiếp tục xuất hiện, phần lớn thiệt hại tài chính được ghi nhận lại đến từ một số ít vụ lừa đảo quy mô lớn, cho thấy tác động ngày càng lan rộng của loại hình tội phạm này đối với nạn nhân trên cả nước.

Phần lớn các vụ việc tập trung tại những khu vực đô thị phát triển, có mức độ kết nối cao như Thành phố Hồ Chí Minh, Hà Nội và Bắc Ninh – nơi tập trung nhiều hoạt động fintech (công nghệ tài chính) và đông đảo nhà đầu tư. Tuy nhiên, một số tỉnh nông thôn như Hòa Bình, Đắk Nông và Nghệ An cũng ghi nhận thiệt hại đáng kể, cho thấy các mạng lưới này đã lan rộng ra các đô thị nhỏ và khu vực vùng ven.



HÌNH 2 Thiệt hại liên quan đến tội phạm tiền mã hóa theo tỉnh (Việt Nam, 2024–2025).

NGUỒN: Phân tích của GI-TOC dựa trên phân bố các vụ án theo tỉnh/thành từ các báo cáo CAND online

Mặc dù tiền mã hóa thường được xem là một công cụ phục vụ các hành vi lừa đảo thông qua token (mã thông báo) giả hoặc các nền tảng đầu tư trá hình, nhưng theo cơ quan công an Việt Nam loại hình này hiện nay dần biến tướng và liên quan đến nhiều hình thức tội phạm nghiêm trọng khác. Một số vụ tham ô và trộm cắp, như trường hợp một kế toán nhà nước chiếm đoạt hàng tỷ đồng,¹³ một nhân viên cửa hàng điện tử lấy cắp gần 140 chiếc iPhone, được cho là xuất phát từ những khoản thua lỗ trước đó liên quan đến tiền mã hóa.¹⁴ Trong một vụ việc tại Hưng Yên, bốn người đàn ông đã dàn dựng một giao dịch USDT giả trực tiếp, sau đó dùng vũ lực cướp 3 tỷ đồng (hơn 113.000 USD) từ người bán tiền mã hóa.¹⁵ Những vụ việc này cho thấy tiền mã hóa, với mức độ ẩn danh cao, khả năng sinh lợi lớn và sự giám sát còn hạn chế đối với các nền tảng giao dịch, có thể bị lợi dụng cho nhiều hành vi sai phạm, từ che giấu nguồn tiền phạm pháp đến lôi kéo người khác tham gia các mạng lưới tội phạm xuyên quốc gia, dù với vai trò nạn nhân hay người tham gia vô tình.

Từ thụ động trong quản lý đến sự tham gia thận trọng

Cho đến gần đây, Việt Nam vẫn giữ thái độ thận trọng đối với tài sản tiền mã hóa, chưa công nhận chính thức và chưa xây dựng khung pháp lý rõ ràng cho loại hình này. Chẳng hạn, năm 2017, Ngân hàng Nhà nước Việt Nam khẳng định tiền ảo không được coi là phương tiện thanh toán hợp pháp,

đồng thời khuyến cáo các tổ chức tài chính không tham gia các giao dịch liên quan đến tiền mã hóa.¹⁶ Tuy nhiên, như minh chứng từ sự gia tăng các vụ án hình sự trong giai đoạn 2024–2025, điều này không ngăn cản các đối tượng tham gia vào các hoạt động liên quan đến tiền mã hóa. Thực tế tại Việt Nam cho thấy các vụ việc này không chỉ tăng về số lượng mà còn về quy mô và mức độ phức tạp.

Cho đến nay, pháp luật Việt Nam vẫn cấm việc sử dụng tiền mã hóa như một phương tiện thanh toán hợp pháp, đồng thời cho phép truy tố các hành vi phạm tội liên quan theo các quy định chung của Bộ luật Hình sự (như lừa đảo, kinh doanh đa cấp trái phép hoặc rửa tiền). Một bước chuyển quan trọng trong công tác quản lý diễn ra vào tháng 3 năm 2025, khi Chính phủ ban hành Nghị quyết số 05/2025/NQ-CP, thiết lập cơ chế thử nghiệm (sandbox) cho việc thí điểm phát triển thị trường tài sản kỹ thuật số.¹⁷ Văn kiện này lần đầu tiên đưa ra các định nghĩa pháp lý về “tài sản kỹ thuật số”, “tài sản tiền mã hóa” và “nhà cung cấp dịch vụ tài sản kỹ thuật số”. Nghị quyết cũng vạch ra lộ trình triển khai theo từng giai đoạn đối với việc tham gia có quản lý, bao gồm các điều kiện áp dụng cho nhà đầu tư trong và ngoài nước, yêu cầu cấp phép đối với các nhà cung cấp dịch vụ tài sản ảo (VASP), cùng các nghĩa vụ về phòng, chống rửa tiền và tài trợ khủng bố (AML/CFT).

Song song, Việt Nam ban hành Luật Công nghiệp công nghệ số năm 2025 vào ngày 14 tháng 6 năm 2025, đặt ra khung pháp lý đối với tiền mã hóa trong bối cảnh chiến lược kinh tế số và công nghệ tài. ¹⁸ Chính phủ Việt Nam cũng đã thông qua Nghị định số 94/2025/NĐ-CP, quy định các nguyên tắc thử nghiệm trong môi trường sandbox nhằm triển khai các giải pháp công nghệ tài chính, bao gồm chấm điểm tín dụng, chia sẻ dữ liệu thông qua giao diện lập trình ứng dụng mở và cho vay ngang hàng. ¹⁹ Mặc dù những bước đi này cho thấy một xu hướng chính trị rõ ràng trong việc quản lý thị trường tiền mã hóa, nhưng vẫn còn tồn tại những khoảng trống pháp lý đáng kể.

Báo cáo theo dõi và đánh giá lần thứ ba của Nhóm châu Á – Thái Bình Dương, công bố vào tháng 2 năm 2025, tiếp tục đánh giá Việt Nam chưa tuân thủ Khuyến nghị số 15 của Lực lượng Đặc nhiệm Tài chính (FATF) về tài sản ảo và các nhà cung cấp dịch vụ tài sản ảo (VASP). Báo cáo cũng nhận định rằng Việt Nam chưa có quy định về quản lý, cấp phép hoặc đăng ký đối với VASP nhằm phục vụ công tác phòng, chống rửa tiền và tài trợ khủng bố (AML/CFT), đồng thời chưa áp dụng đầy đủ các biện pháp giám sát và phòng ngừa cần thiết. ²⁰ Trong thời gian qua, các cơ quan chức năng đã ban hành một số văn bản mới bao gồm Luật phòng, chống rửa tiền 2022²¹ và Nghị định 19/2023/NĐ-CP,²² cũng như triển khai Thông tư 27/2025/TT-NHNN,²³ nhằm tiếp cận từng bước với Khuyến nghị 15 của FATF. Tuy nhiên, các chuyên gia nhận định rằng những văn bản này vẫn còn chưa rõ ràng trong việc công nhận tài sản ảo hoặc VASP là đối tượng phải báo cáo, đồng thời chưa đủ để xử lý những lỗ hổng phức tạp đang tồn tại trên thực tế. ²⁴ Bên cạnh đó, cho đến nay vẫn chưa có hoạt động giám sát hay biện pháp xử phạt nào được áp dụng đối với VASP, và Việt Nam cũng chưa tiến hành đánh giá rủi ro quốc gia riêng đối với các nguy cơ rửa tiền và tài trợ khủng bố phát sinh từ tài sản ảo. Những hạn chế này được đánh giá là một lỗ hổng đáng kể, ảnh hưởng đến tính toàn vẹn của hệ thống tài chính Việt Nam và khiến quốc gia này dễ bị lợi dụng bởi các luồng tài sản mã hóa chưa được quản lý.

Hệ quả là một khung pháp lý còn phân mảnh, trong đó chính sách về tiền mã hóa dường như đang được xây dựng song song, nhưng chưa thực sự được tích hợp vào khung pháp lý phòng, chống rửa tiền (AML) của Việt Nam. Vấn đề này không chỉ giới hạn trong lĩnh vực AML, mà còn phản ánh tổng quan sự thiếu đồng bộ trong cách tiếp cận và quản lý các công nghệ mới nổi tại Việt Nam. Trong bối cảnh cơ chế sandbox được triển khai theo Nghị quyết 05 và Nghị định 94, hiệu quả phối hợp thể chế giữa Bộ Tài chính, Ngân hàng Nhà nước và các cơ quan thực thi pháp luật sẽ là yếu tố then chốt để chuyển hóa ý chí chính trị thành thực tiễn quản lý hiệu quả.

Các hạn chế về mặt thể chế và giới hạn của các biện pháp nghiêm cấm

Các cơ quan chức năng Việt Nam đã đạt được nhiều kết quả đáng kể trong việc triệt phá các đường dây tội phạm, phong tỏa tài sản và cảnh báo người dân về rủi ro của các tài sản số chưa được quản lý. Tuy nhiên, khi khung pháp lý chưa được hoàn thiện và cơ chế quản lý còn thiếu rõ ràng, những nỗ lực này vẫn còn mang tính rời rạc. Các biện pháp như tịch thu tài sản có giá trị lớn, phong tỏa tài khoản ngân hàng hay dẫn độ các nghi phạm nước ngoài là cần thiết, nhưng mới chỉ xử lý phần ngọn, chưa giải quyết được nguyên nhân gốc rễ.

Cần có một cách tiếp cận quản trị mang tính định hướng dài hạn, theo đó cho phép hợp pháp hóa một số hoạt động tiền mã hóa nhất định dưới các yêu cầu tuân thủ nghiêm ngặt (bao gồm đăng ký, kiểm toán, thuế và giám sát phòng, chống rửa tiền), đồng thời hình sự hóa các mô hình phát hành token gian lận và các sản phẩm giao dịch không được cấp phép. Một số quốc gia láng giềng trong khu vực, như Thái Lan, Singapore và Philippines, hiện đã và đang thử nghiệm các mô hình quản lý song song theo hướng này.

Việc khắc phục ba khoảng trống thể chế then chốt có thể nâng cao đáng kể năng lực ứng phó của các cơ quan chức năng. Thứ nhất, cần triển khai một khung cấp phép toàn diện đối với các nền tảng tiền mã hóa. Một số mô hình lừa đảo với quy mô lớn, như Matrix Chain, PaynetCoin và Cashback Pro, đã hoạt động tại Việt Nam mà không có bất kỳ giấy phép chính thức nào, thay vào đó dựa vào ứng dụng di động, mạng xã hội và việc phát hành token không chịu sự giám sát. Bên cạnh đó, vụ Exness năm 2023 cho thấy các nền tảng này có thể sử dụng tên miền tiếng Việt và hệ thống ngân hàng trong nước để nhận tiền gửi, dù không hề có giấy phép hợp pháp. ²⁵ Ngay cả sau khi bị các cơ quan quản lý internet quốc gia chặn truy cập, nền tảng này vẫn nhanh chóng xuất hiện trở lại dưới tên miền mới và tiếp tục thu hút tiền từ các nhà đầu tư Việt Nam. ²⁶ Vì vậy, trong thời gian tới, việc triển khai khung cấp phép đối với các nền tảng tiền mã hóa — hiện đang được xây dựng theo lộ trình nêu trong Nghị quyết 05 và các công cụ pháp lý liên quan — là hết sức then chốt. Trước khi các quy định này chính thức có hiệu lực, các đối tượng lừa đảo vẫn có thể lợi dụng những kẽ hở pháp lý bằng cách đăng ký công ty bình phong ở nước ngoài, tổ chức sự kiện trong nước và triển khai các ứng dụng không được quản lý, trong khi mức độ trách nhiệm pháp lý tại Việt Nam vẫn rất hạn chế.

Thứ hai, các cơ quan thực thi pháp luật cần tăng cường phối hợp xuyên biên giới, đồng thời đẩy mạnh hợp tác khu vực kinh tế tư nhân. Cho đến nay, các cơ quan chức năng thường phản ứng khá bị động trước những vụ việc thu hút sự chú ý rộng rãi của truyền thông, trong khi mức độ phối hợp liên tỉnh và hợp tác quốc tế vẫn còn hạn chế. Điều này khiến việc nhận diện đầy đủ cấu trúc của các mạng lưới lừa đảo tiền mã hóa gặp nhiều khó khăn. Bên cạnh đó, cơ chế chia sẻ thông tin tình báo tài chính với các sản phẩm giao dịch lớn hoặc các nhà cung cấp dịch vụ phân tích blockchain hiện vẫn chưa được phát triển đầy đủ.

Cuối cùng, các nhà hoạch định chính sách cần xác định rõ một cơ quan quản lý chịu trách nhiệm giám sát tài sản tiền mã hóa. Cho đến nay, Ngân hàng Nhà nước Việt Nam cho rằng lĩnh vực này không thuộc thẩm quyền quản lý của mình, trong khi các cơ quan quản lý chứng khoán lại coi phần lớn các token nằm ngoài phạm vi thị trường vốn. Điều này tạo ra một “khoảng trống pháp lý”, trong đó không có cơ quan nào trực tiếp giám sát các hoạt động ví đáng ngờ, thực thi các quy định về nhận diện khách hàng (KYC) trên các sản phẩm giao dịch, hay theo dõi các đợt phát hành token trong nước.

Số lượng lớn các vụ việc liên quan đến tiền mã hóa cho thấy cách tiếp cận thực thi pháp luật mang tính phản ứng đơn thuần không còn đủ hiệu quả. Quy mô thiệt hại được báo cáo – hơn 20.000 tỷ đồng (khoảng 800 triệu USD) trên nhiều tỉnh thành chỉ trong hai năm – cho thấy rủi ro từ tiền mã hóa đã trở thành một vấn đề mang tính hệ thống. Trong bối cảnh Việt Nam đang triển khai khung thí điểm đối với tài sản kỹ thuật số, đây là thời điểm then chốt để khép lại các khoảng trống giám sát và củng cố việc quản lý tiền mã hóa một cách chặt chẽ hơn trong khuôn khổ phòng, chống rửa tiền (AML), qua đó bảo đảm tính toàn vẹn chung của hệ thống tài chính. ■