VIỆN KIỂM SÁT NHÂN DÂN TỐI CAO

VIỆN KIỂM SÁT NHÂN DÂN TỈNH BẮC GIANG

TÀI LIỆU HỘI NGHỊ TẬP HUẤN

THỰC HÀNH QUYỀN CÔNG TỐ, KIỂM SÁT ĐIỀU TRA VỤ ÁN HÌNH SỰ VỀ TỘI PHẠM CÔNG NGHỆ CAO LIÊN QUAN ĐẾN ĐỊA CHỈ IP VÀ TIỀN ẢO

(Lưu hành nội bộ)

Vũ Anh Tuấn-Phòng 2

Bắc Giang, tháng 8 năm 2024

TÀI LIỆU TẬP HUẤN

THỰC HÀNH QUYỀN CÔNG TỐ, KIỂM SÁT ĐIỀU TRA VỤ ÁN HÌNH SỰ VỀ TỘI PHẠM CÔNG NGHỆ CAO LIÊN QUAN ĐẾN ĐỊA CHỈ IP VÀ TIỀN ẢO

Phần 1
Thực hành quyền công tố, kiểm sát điều tra các vụ án hình sự về tội phạm công nghệ cao liên quan đến địa chỉ IP

I- KHÁI NIỆM, PHÂN LOẠI, PHIÊN BẢN, CẤU TRÚC, QUẢN LÝ VÀ VAI TRÒ CỦA ĐỊA CHỈ IP

1. Khái niệm và phân loại địa chỉ IP

1.1. Khái niệm địa chỉ IP

IP (Interner Protocol-giao thức Internet) là địa chỉ số được tập hợp theo tiêu chuẩn và quy tắc nhất định, có trên mọi thiết bị có chức năng kết nối mạng để định danh thiết bị điện tử khi kết nối mạng. IP là một địa chỉ duy nhất được thiết bị điện tử sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet. Tất cả các thiết bị, từ máy chủ (Server) đến máy khách (Client) đều sở hữu 01 địa chỉ IP riêng biệt, không trùng lặp với bất kỳ một địa chỉ IP nào khác. Địa chỉ IP giúp các thiết bị này có thể liên lạc và trao đổi dữ liệu với nhau qua mạng.

1.2. Phân loại địa chỉ IP

Tùy theo tiêu chí phân loại mà có nhiều cách phân loại địa chỉ IP, sau đây là 04 loại địa chỉ IP cơ bản và phổ biến sau:

- IP Public (IP cộng đồng): Là IP kết nối trực tiếp với Internet, sử dụng trong mạng gia đình, tổ chức hoặc doanh nghiệp cụ thể; sử dụng để truy cập, liên lạc trực tiếp với các thiết bị kết nối Internet khác. IP Public là yếu tố thiết yếu với bất kỳ phần cứng mạng có thể truy cập công khai nào.

- IP Private (IP nội bộ/riêng tư): Là IP chỉ được sử dụng cho những máy tính thuộc mạng nội bộ (mạng LAN) như nhà trường, công ty, tổ chức,...hỗ trợ các máy tính trong hệ thống kết nối với nhau, không kết nối trực tiếp với các máy tính bên ngoài hệ thống. IP nội bộ do người dùng thiết lập thủ công hoặc do bộ định tuyến (Router) gán thiết lập tự động.

- IP Static (IP tĩnh/thủ công): Là IP được định cấu hình thủ công cho thiết bị, nó cố định và không thể thay đổi, kết nối Internet nhanh chóng mà không cần đợi cấp phát. IP tĩnh thường được cấp cho 01 máy chủ với mục đích riêng như máy chủ mail, máy chủ Web,.... Khi 01 thiết bị điện tử gia nhập vào mạng, người sử dụng sẽ sử dụng DHCP để gán địa chỉ IP cho thiết bị của mình bằng cách thủ công, địa chỉ IP này sẽ không thay đổi cho đến khi tự mình thay đổi một cách thủ công.

- IP Dynamic (IP động/tự động): Là IP phổ biến và được ứng dụng rộng rãi, được gán tự động cho từng thiết bị khi kết nối vào mạng, nó có thể thay đổi sau mỗi lần sử dụng. IP động hoạt động bằng cách sử dụng phương thức DHCP (Dynamic Host Configuration Protocol-Giao thức cấu hình máy chủ), là giao thức tự động cấp phát địa chỉ IP đến các thiết bị trong mạng cho phép truy cập vào Internet.

Khi 01 thiết bị điện tử gia nhập vào mạng lần đầu tiên sẽ gửi yêu cầu được cấp địa chỉ IP, khi đó máy chủ DHCP sẽ trả lời với 01 đề nghị cung cấp 01 địa chỉ IP, sau đó thiết bị điện tử sẽ chấp nhận đề nghị và sử dụng địa chỉ IP này để truy cập mạng. Các ISP (Internet Service Provider-Nhà cung cấp dịch vụ Internet) sẽ chỉ cung cấp IP động cho khách hàng thông thường, tức là IP sẽ khác nhau sau mỗi lần kết nối hoặc trong một phiên kết nối sẽ đổi thành IP khác. Việc cấp IP động này nhằm tiết kiệm nguồn IP đang có hạn. Khi thiết bị không kết nối vào mạng thì ISP sẽ cấp IP đó cho người sử dụng khác.

2. Các phiên bản và cấu trúc của địa chỉ IP

2.1. IPv4 (Internet Protocol Version 4)

- IPv4 là phiên bản thứ 4 của giao thức Internet, còn gọi là TCP/IP. IPv4 được thiết kế gồm 04 nhóm số thập phân, phân cách nhau bằng dấu chấm. Bộ IPv4 có 32 bits dữ liệu, chia đều cho 04 nhóm số, mỗi nhóm gồm 08 bits dữ liệu (gọi là 01 octet), là các số nằm trong khoảng từ 0 đến 255. IPv4 gồm khoảng 4,29 tỉ địa chỉ khả dụng và đã cạn kiệt vào tháng 4/2014. Ví dụ: 172.16.254.1.

- Một cấu trúc địa chỉ IPv4 được tạo thành từ một bộ 04 số, mỗi số được ngăn cách bằng một dấu chấm (.) dưới dạng cấu trúc X1.X2.X3.X4. Mỗi X1, X2, X3, X4 có thể nằm trong khoảng từ 0-255. Do đó, cấu trúc của địa chỉ IPv4 nằm trong khoảng từ 0.0.0.0 đến 255.255.255.255.

- Một địa chỉ IPv4 được chia thành 02 thành phần:

+ ID mạng (Network Identification): ID mạng xác định mạng cụ thể nơi có thiết bị đích, tương ứng với bộ 3 số đầu tiên (X1.X2.X3). Ví dụ: Đối với địa chỉ

IP 192.158.1.38 thì phần 192.158.1 là ID mạng, bình thường bộ số cuối bằng 0, vì vậy ID mạng của thiết bị là 192.158.1.0.

+ ID máy chủ (Hosting Identification): Tương ứng với bộ số cuối cùng (X4). Nếu ID mạng xác định một mạng chứa thiết bị thì ID máy chủ xác định thiết bị cụ thể trong mạng đó. ID máy chủ là bộ số cuối cùng mà ID mạng không lấy. Ví dụ: Đối với địa chỉ IP 192.158.1.38 thì phần 38 là ID máy chủ trên mạng 192.158.1.0.

- Địa chỉ IPv4 được phân làm 5 lớp sau:

+ Lớp A: Gồm các địa chỉ IP từ 1.0.0.1 đến 126.0.0.0. Lớp A thường dành riêng cho địa chỉ IP của các tổ chức lớn trên thế giới.

+ Lớp B: Gồm các địa chỉ IP từ 128.1.0.0 đến 191.254.0.0. Lớp B thường dành cho địa chỉ IP của các tổ chức hạng trung trên thế giới.

+ Lớp C: Gồm các địa chỉ IP từ 192.0.1.0 đến 223.255.254.0. Lớp C thường dành cho địa chỉ IP của các tổ chức nhỏ, trong đó có cả thiết bị điện tử cá nhân.

+ Lớp D: Gồm các địa chỉ IP từ 224.0.0.0 đến 239.255.255.255. Lớp D được dành cho phát các thông tin, ứng dụng dạng truyền thông đa phương tiện. (Multicast/Broadcast).

+ Lớp E: Gồm các địa chỉ IP từ 240.0.0.0 đến 254.255.255.255. Lớp E được dùng trong thí nghiệm, nghiên cứu khoa học và dự phòng.

+ Ngoài ra, còn có 01 lớp có địa chỉ IP là 127.x.x.x và được dùng riêng để kiểm tra vòng lặp quy hồi (gọi là Loopback).

2.2. IPv6 (Internet Protocol Version 6)

- IPv6 là phiên bản thứ 6 phiên bản mới nhất của IP. IPv6 ra đời vì thiếu hụt địa chỉ IP trên IPv4 và để mở rộng không gian địa chỉ mạng, nâng cao tính an toàn và bảo mật, hỗ trợ các thiết bị kết nối mạng mới như IoT (Internet of Things-Internet vạn vật). IPv6 có 128 bits dữ liệu, gồm 08 nhóm số (từ số 0 đến số 9) và chữ cái (từ chữ A đến chữ F) dưới dạng các cụm số hexa, mỗi nhóm gồm 16 bits, phân cách nhau bằng dấu hai chấm (:). IPv6 gồm 2^{128} địa chỉ, cung cấp lượng địa chỉ khổng lồ cho hoạt động Internet của thế giới.

- IPv6 gồm 03 thành phần, phân tích 01 địa chỉ IPv6 theo ví dụ sau 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

+ Site Prefix: Là số được gán bằng một ISP nên đây chính là số để xác định ISP. Ví dụ: 2001:0db8:85a3.

+ Subnet ID: Định danh mặt nạ mạng con, là phần mô tả cấu trúc của mạng con khi chia mạng thành các cấu trúc nhỏ hơn. Ví dụ: 0000:0000.

+ Interface ID: Định danh giao diện, là phần định danh duy nhất của một thiết bị trong mạng, giúp xác định một thiết bị cụ thể truy cập mạng. Ví dụ: 8a2e:0370:7334.

3. Vai trò của địa chỉ IP trong điều tra tội phạm công nghệ cao

Khi một thiết bị điện tử kết nối với Internet hay với một mạng nào đó (LAN, 3G, 4G,...) thì bao giờ cũng có địa chỉ IP. Khi truy cập vào mạng Internet, thiết bị điện tử sẽ được cấp duy nhất 01 địa chỉ IP Public, được cấp phát cho Modem/Router bởi ISP (hoặc máy chủ DHCP Server trong mạng LAN). Khi sử dụng mạng di động 4G hay các băng tần mạng khác, thiết bị điện tử sẽ được cấp một địa chỉ IP Public tạm thời và duy nhất từ ISP để kết nối thiết bị với Internet và truy cập các dịch vụ trực tuyến. Địa chỉ IP là một thành phần cực kỳ quan trọng, cung cấp danh tính của các thiết bị được kết nối mạng, giúp các thiết bị trên mạng phân biệt và nhận ra nhau, kết nối, liên lạc giữa các thiết bị mạng với nhau trên Internet, cho phép truyền dữ liệu giữa chúng, cũng như cho phép truy cập vào các ứng dụng và dịch vụ mạng. Tính duy nhất của địa chỉ IP khi truy cập mạng Internet là một trong những căn cứ quan trọng trong điều tra tội phạm công nghệ cao. Do đó, để xác định các hoạt động trên Internet của thiết bị điện tử đó thì việc xác định địa chỉ IP là việc đầu tiên phải điều tra, xác minh.

Ngoài địa chỉ IP của các thiết bị điện tử, mỗi Website cũng có một địa chỉ IP riêng đã được đăng ký để có thể truy cập được trên Internet. Địa chỉ IP của Website thường được gọi là địa chỉ IP máy chủ (Server IP address). Tuy nhiên, địa chỉ IP của Website là một dãy số tự nhiên dài và khó nhớ, vì vậy cần có tên miền để thay thế cho địa chỉ IP. Khi nhập một tên miền Website vào thanh địa chỉ của trình duyệt, máy tính sẽ gửi yêu cầu tới máy chủ DNS để phân giải tên miền thành địa chỉ IP của Website đó. Sau đó, thiết bị điện tử sẽ sử dụng địa chỉ IP này để kết nối và tải nội dung từ Website. Hầu hết các Website đều giữ lại nhật ký hoạt động khi khách hàng khi truy cập, đây là nguồn thông tin quan trọng, hữu ích trong điều tra tội phạm công nghệ cao.

Như vậy, địa chỉ IP có thể có tiềm năng cung cấp các thông tin hữu ích sau trong điều tra tội phạm công nghệ cao: Nhà cung cấp dịch vụ Internet (IPS); tên máy chủ của địa chỉ IP có liên quan đến Website; tên khu vực/quốc gia/tỉnh/thành phố; vĩ tuyến và kinh tuyến của vị trí địa chỉ IP; mã bưu điện ; nhật ký truy cập mạng,...

Đối với tên miền, khi tiến hành điều tra, tên miền có thể cung cấp các thông tin hữu ích sau: Tính sẵn có của miền; địa chỉ IP; máy chủ tên miền và vị trí đặt máy chủ; ngày đăng ký/ngày tạo tên miền; ngày hết hạn tên miền; chủ sở hữu và

các thông tin về chủ sở hữu tên miền;...

4. Quản lý địa chỉ IP/tên miền trên thế giới và Việt Nam

Khi có địa chỉ IP hoặc thông tin tên miền thì các thông tin này chỉ đại diện cho thiết bị điện tử chứ không phải đại diện cho con người cụ thể. Các ISP thường được cấp phát các khối địa chỉ IP cụ thể nào đó và chúng được ghi lại trong cơ sở dữ liệu công cộng do các cơ quan đăng ký Internet của khu vực quản lý. Do đó, cơ quan điều tra cần tiến hành các hoạt động điều tra để có thêm thông tin để tìm ra danh tính của người truy cập, tức là phải tiến hành điều tra để xác định ISP nào đang sở hữu địa chỉ IP/tên miền đó. Địa chỉ IP/tên miền được quản lý theo RIR (Regional Internet Registry-Đăng ký Internet theo khu vực). Tổ chức quản lý RIR có trách nhiệm kiểm soát tất cả các địa chỉ IP và đăng ký tên miền trong khu vực hoạt động.

Ở phạm vi toàn cầu, ICANN (Internet Corporation for Assigned Names and Numbers-Tập đoàn Internet quản lý tên và số được gán) là tổ chức có nhiệm vụ giám sát các công việc liên quan đến Internet, thực hiện việc phân phối, ủy quyền cấp phát, quản lý không gian địa chỉ IP, quản lý cơ sở dữ liệu và hệ thống tên miền trên Internet. ICANN không kiểm soát nội dung xuất hiện trên Internet, không điều chỉnh quyền truy cập Internet, nhưng ICANN giúp giữ an toàn bằng cách phát triển và thực thi chính sách về mã số định danh duy nhất của Internet. ICANN có trụ sở tại Mỹ, website là icannn.org. ICANN là tổ chức quản lý website who.is là công cụ tìm kiếm địa chỉ IP, tên miền và Website công khai trên toàn thế giới và có độ chính xác, tin cậy cao, được thừa nhận trong hoạt động điều tra, truy tố, xét xử ở nhiều nước trên thế giới.

Ở phạm vi châu lục, trực thuộc ICANN có 05 tổ chức chịu trách nhiệm về việc đăng ký, quản lý dải IP, tên miền trong khu vực của mình, gồm: ARIN (American Registry for Internet Number-Cơ quan đăng ký số Internet Mỹ), trụ sở tại Mỹ, quản lý khu vực Bắc Mỹ, Website là arin.net. RIPE NCC (Réseaux IP Européens Network Coordination Centre-Cơ quan đăng ký Internet khu vực châu Âu), trụ sở tại Bỉ, quản lý khu vực châu Âu, Website là ripe.net. APNIC (Asia Pacific Network Information Centre-Trung tâm thông tin mạng châu Á-Thái Bình Dương), trụ sở tại Úc, Website là apnic.net. LACNIC (Latin American and Caribbean Internet Address Registry-Trung tâm an ninh mạng châu Mỹ La Tinh và Caribe), trụ sở tại Uruguay, Website là lacnic.net. AFRINIC (African Network Information Centre-Trung tâm thông tin mạng châu Á), trụ sở tại quốc đảo Mauritius, Website là afirinic.net.

Tại Việt Nam, VNNIC (Vietnam Internet Network Information Center-

Trung tâm Internet Việt Nam) là đơn vị sự nghiệp công lập, trực thuộc Bộ Thông tin và Truyền thông, là đơn vị quản lý địa chỉ IP và tên miền. VNNIC có địa chỉ tại 18 Nguyễn Du, Hà Nội; Website là vnnic.vn. Theo Quyết định số 48 ngày 18/01/2024 của Bộ trưởng Bộ Thông tin và Truyền thông, VNNIC có chức năng, nhiệm vụ, quyền hạn có liên quan đến địa chỉ IP, tên miền, gồm: Cấp, phân bổ, duy trì địa chỉ IP, số hiệu mạng (ASN), địa chỉ tiền miền quốc gia ".vn" cho các tổ chức, cá nhân. Thiết lập, quản lý, khai thác, cung cấp số liệu truy vấn, bảo đảm an toàn, bảo mật của hệ thống DNS quốc gia và Trạm trung chuyển Internet quốc gia (VNIX-Vietnam National Internet eXchange). Kiểm tra, giám sát việc đăng ký, sử dụng và thực hiện việc ngừng, tạm ngừng, thu hồi tài nguyên Internet Việt Nam. Thu thập, phân tích, đánh giá, công bố các thông tin, số liệu đăng ký, sử dụng tài nguyên Internet.

Việc xác định được tổ chức nào quản lý địa chỉ IP, tên miền sẽ định hướng cho các cơ quan pháp luật tiến hành điều tra, xác minh, thu thập thông tin đối với các vụ việc, vụ án về tội phạm công nghệ cao. Các thông tin về địa chỉ IP và tên miền do VNNIC cung cấp có ý nghĩa quan trọng để định hướng các hoạt động điều tra; truy vết, xác định các chứng cứ xác định tội phạm và người phạm tội liên quan đến công nghệ cao.

II- KIỂM TRA, XÁC ĐỊNH, TRUY VẾT ĐỊA CHỈ IP VÀ TÊN MIỀN

1. Kiểm tra, xác định địa chỉ IP

1.1. Đối với máy vi tính

Có nhiều cách để kiểm tra, xác định địa chỉ IP của máy tính, một số cách thường được sử dụng là:

- Sử dụng Command Prompt: Nhấn tổ hợp phím Windows+R để mở hộp thoại Run -> Nhập "cmd" vào hộp thoại Run -> Tại màn hình cmd.exe đánh lệnh "ipconfig" để tìm địa chỉ IP. Máy tính sẽ cung cấp địa chỉ IPv6 sau dòng Link-local IPv6 Addres và địa chỉ IPv4 sau dòng IPv4 Address. Nếu máy tính kết nối mạng có dây: Địa chỉ IP xuất hiện sau cụm từ "Wireless LAN adapter Local connection*1". Nếu máy tính kết nối mạng không dây: Địa chỉ IP xuất hiện sau cụm từ "Wireless LAN adapter Wi-Fi".

- Sử dụng Control Panel: Vào Start Menu -> Click chọn Control Panel -> Click vào View Network Status and Tasks (hoặc Network and Sharing Center, tùy hệ hiều hành) -> Nhấn vào phần mạng đang truy cập (Connections) -> Chọn Details.

- Sử dụng phần mềm TrueIP: Truy cập Website haztek-software.com để tải

về và tiến hành cài đặt phần mềm. Sau khi khởi động, phần mềm sẽ tự động đọc IP trên máy tính gồm:

+ Local Address: Là địa chỉ IP trong mạng nội bộ, hệ thống mạng LAN, thường là địa chỉ IPv4.

+ External Addres: Là địa chỉ IP được nhận dạng khi kết nối với các dịch vụ Internet, Website nước ngoài. Đây cũng là địa chỉ chung dành cho 01 hệ thống mạng máy tính.

- Sử dụng trình duyệt Internet: Có rất nhiều Website có chức năng kiểm tra, xác định địa chỉ IP. Một số Website được sử dụng phổ biến và có độ tin cậy cao gồm: who.is; whatismyip.com; whatismyipaddress.com.

Lưu ý: Sử dụng trình duyệt Internet sẽ kiểm tra, xác định được địa chỉ IP của máy tính trên hệ thống Internet toàn cầu chứ không phải là địa chỉ IP trong mạng LAN được cấp qua Router, Modem. Nếu muốn xem địa chỉ IP trong mạng LAN hoặc cấp bởi Router, Modem thì sử dụng phương pháp Command Prompt như đã nêu trên.

1.2. Đối với điện thoại di động thông minh

- Trường hợp điện thoại đang kết nối mạng Wi-Fi:

+ Đối với điện thoại cài đặt hệ điều hành IOS: Mở ứng dụng Cài đặt (Settings) -> Chọn Wi-Fi -> Nhấn vào tên mạng Wi-Fi đang kết nối để mở tuỳ chọn sẽ kiểm tra, xác định được địa chỉ IPv4 và cả IPv6 tại mục này.

+ Đối với điện thoại cài đặt hệ điều hành Android: Mở ứng dụng Cài đặt (Settings) -> Chọn Network & Internet -> Nhấn vào tên mạng Wi-Fi đang kết nối - > Chọn Advanced (Nâng cao) -> Xuất hiện màn hình có địa chỉ IP ở mục IP Address cùng với một số thông tin khác có liên quan.

- Trường hợp điện thoại kết nối mạng 4G:

+ Truy cập vào trình duyệt Internet của điện thoại: Trình duyệt Safari đối với hệ điều hành IOS, trình duyệt Chrome đối với hệ điều hành Android.

+ Sử dụng một số Website có chức năng kiểm tra, xác định địa chỉ IP được sử dụng phổ biến và có độ tin cậy cao gồm: iphey.com; whatismyip.com whatismyipaddress.com.

Kết quả sẽ kiểm tra, xác định được địa chỉ IP Public mà ISP cung cấp cho điện thoại đang sử dụng truy cập mạng 4G.

2. Truy vết địa chỉ IP

Sau khi kiểm tra, xác định và có được địa chỉ IP, bước tiếp theo cần phân tích và truy vết địa chỉ IP để có được các thông tin cần thiết định hướng cho các

hoạt động điều tra, xác minh tiếp theo cũng như truy vết, xác định các chứng cứ xác định tội phạm và người phạm tội. Có nhiều cách để truy vết địa chỉ IP, một số cách phổ biến và có độ tin cậy cao gồm:

- Sử dụng Website để truy vết địa chỉ IP, gồm:

+ Website who.is của ICANN: Nhập địa chỉ IP cần truy vết -> chọn Get IP Details -> Nhận kết quả truy vết trên trang (Địa chỉ IP) Address Profile.

+ Website whatismyipaddress.com: Chọn mục IP Lookup -> nhập địa chỉ IP cần truy vết -> chọn Get IP Details (thông tin chi tiết về địa chỉ IP).

+ Website ipinfor.io: Chọn mục Your IP -> Thông tin chi tiết về địa chỉ IP.

+ Website apnic.net (đối với khu vực châu Á, các khu vực khác truy cập vào Website của tổ chức đó): Nhập địa chỉ IP vào thanh tìm kiếm Whois & Website của giao diện -> Nhận được bản kết quả APNIC Whois Search với các thông tin chi tiết về địa chỉ IP cần truy vết.

Trên cơ sở truy vết địa chỉ IP từ các Website nêu trên có thể xác định được các thông tin cần quan tâm gồm: Tên máy chủ; địa chỉ máy chủ; nhà cung cấp dịch vụ Internet (ISP); địa chỉ ISP/Email/số điện thoại; tên mạng; quốc gia/khu vực/tỉnh/thành phố; dịch vụ tên miền của máy chủ (Hostname); tên/địa chỉ/ Email/số điện thoại của người quản trị (Admin); vĩ độ/kinh độ; trạng thái; giờ/ngày/tháng/năm sửa đổi;...và rất nhiều thông tin hữu ích khác định hướng cho các hoạt động điều tra, xác minh.

- Gửi yêu cầu cung cấp thông tin về địa chỉ IP cần điều tra, xác minh đến VNNIC. Kết quả trả lời của VNNIC sẽ trong trường hợp:

+ Nếu ISP ở trong nước (VNPT, Viettel, FPT, CMC,...): Tiến hành các hoạt động điều tra, xác minh tại ISP để có được thông tin khách hàng sử dụng và vị trí lắp đặt thiết bị điện tử sử dụng địa chỉ IP đó.

+ Nếu ISP ở nước ngoài: Điều tra, xác minh qua kênh ngoại giao hoặc tiến hành ủy thác tương trợ tư pháp để có được thông tin khách hàng sử dụng địa chỉ và vị trí lắp đặt thiết bị điện tử sử dụng IP đó.

3. Kiểm tra, xác định, truy vết tên miền

Bản chất của tên miền (Domain) chính là địa chỉ IP, nếu không có tên miền, muốn truy cập Website người ta phải gõ một dãy số IP khó nhớ. Do đó, tên miền là một chuỗi ký tự được dùng để định danh và truy cập vào các trang web trên Internet. Tên miền chính là tên của một Website hoạt động trên Internet, nó đóng vai trò là một địa chỉ IP tĩnh. Một Website hoạt động trên Internet cần ít nhất 02 thành phần là Web Server và tên miền để hoạt động bình thường. Web Server là

máy tính chứa File và Database (Hosting) tạo nên Website để hoạt động rồi gửi nó đi ra Internet mỗi khi có người truy cập vào Website từ máy chủ họ. Tên miền là tên mọi người gõ lên trình duyệt, sau đó vì tên miền đã trỏ về địa chỉ Web Server, nên trình duyệt có thể gửi yêu cầu truy cập Web Server đó.

Hiểu một cách đơn giản, chúng ta có thể xem Domain như tên của một cửa hàng, giúp khách hàng tìm đường đến nơi chúng ta kinh doanh. Trong khi Hosting giống như kho chứa, nơi bạn lưu trữ tất cả hàng hóa và dịch vụ của mình. Nếu không có Hosting, dù có Domain cũng không đem lại lợi ích gì cho Website. Vì vậy, khi hoạt động trên Internet, Website cần có cả Domain lẫn Hosting.

Sử dụng các Website để kiểm tra, xác định, truy vết tên miền, một số Website phổ biến và có độ tin cậy cao gồm:

- Đối với các tên miền không phải ".vn": who.is; whois.inet.vn; godaddy.com; whois.domaintools.com (lưu ý đến tiện ích IP đảo ngược-Reverse IP để chuyển đổi từ tên miền sang địa chỉ IP và ngược lại).

- Đối với các tên miền ".vn": vnnic.vn; tracuutenmien.gov.vn.

Trên cơ sở kiểm tra, xác định, truy vết tên miền từ các Website nêu trên có thể xác định được các thông tin hữu ích cho điều tra, xác minh gồm: Ngày đăng ký, ngày tạo tên miền, ngày cập nhật, ngày hết hạn; chủ sở hữu tên miền; nhà quản lý tên miền; Email và số điện thoại; trạng thái tên miền; tên máy chủ, địa chỉ IP của máy chủ; bản ghi DNS;...

- Đối với các tên miền đã bị xóa khỏi Internet:

+ Sử dụng website web.archive.org, đây là thư viện số phi lợi nhuận, lưu giữ nội dung các Website và các loại dữ liệu điện tử khác trên Internet (hiện đang lưu khoảng 866 tỷ Website theo thời gian). Đặc biệt, đây là Website có tính năng Wayback Machine dùng để kiểm tra, xác định, truy vết tên miền đã bị xóa khỏi Internet. Với Wayback Machine, người sử dụng có thể tái hiện nội dung của Website đã bị xóa khỏi Internet và lưu dữ liệu của chúng để phục vụ cho các hoạt động điều tra, xác minh.

+ Cách lưu nội dung của Website: Truy cập vào Website cần lưu thông tin -> Nhấn vào Tùy chỉnh (có biểu tượng 03 chấm hoặc 03 gạch ngang) -> Chọn In -> Tại Máy in đích, chọn Lưu dưới dạng PDF -> Nhấn Lưu -> Tại hộp thoại Save as (Lưu dưới dạng) chọn đường dẫn đến thư mục lưu tệp PDF - > Nhấn Save (lưu) và đặt tên File.

- Gửi yêu cầu cung cấp thông tin về địa chỉ tên miền cần điều tra, xác minh đến VNNIC. Kết quả trả lời của VNNIC sẽ trong các trường hợp:

+ Nếu tên miền ở trong nước: Tiến hành các hoạt động điều tra, xác minh tại tổ chức cung cấp tên miền để có được thông tin thông tin khách hàng sử dụng địa chỉ và vị trí lắp đặt thiết bị điện tử của tên miền đó.

+ Nếu tên miền ở nước ngoài: Điều tra, xác minh qua kênh ngoại giao hoặc tiến hành ủy thác tương trợ tư pháp để có được thông tin khách hàng sử dụng địa chỉ và vị trí lắp đặt thiết bị điện tử của tên miền đó.

Phần 2
Thực hành quyền công tố, kiểm sát điều tra các vụ án hình sự về tội phạm công nghệ cao liên quan đến tiền ảo

I- KHÁI NIỆM, ĐẶC ĐIỂM VÀ MỘT SỐ THUẬT NGỮ LIÊN QUAN ĐẾN TIỀN ẢO

1. Khái niệm, đặc điểm tiền ảo

1.1. Khái niệm tiền ảo

Hiện nay, chưa có khái niệm chung, thống nhất về tiền ảo mà tùy vào từng quốc gia, từng chủ thể và góc độ nghiên cứu mà tiền ảo được định nghĩa với nhiều cách khác nhau. Các thuật ngữ khác như tiền kỹ thuật số (Digital Currency) hay tiền mã hóa (Crypto Currency) thường được sử dụng để chỉ tiền ảo. Ngân hàng trung ương châu Âu (ECB) định nghĩa tiền ảo là một loại tiền kỹ thuật số, không được điều chỉnh bởi ngân hàng trung ương; được ban hành và kiểm soát bởi nhà phát triển, được sử dụng và chấp nhận giữa các thành viên của cộng đồng ảo nhất định. Văn phòng trách nhiệm Chính phủ Mỹ (GAO) định nghĩa tiền ảo là một đơn vị trao đổi số hóa, không được bảo đảm bởi một đồng tiền chính thức do Chính phủ phát hành. Liên minh châu Âu (EU) định nghĩa tiền ảo là một đại diện kỹ thuật số của giá trị, không được phát hành hoặc bảo đảm bởi một ngân hàng trung ương hoặc cơ quan nhà nước, không gắn với tiền pháp định hay mang giá trị pháp lý như tiền pháp định nhưng được cá nhân hoặc pháp nhân chấp nhận như một phương tiện trao đổi và có thể được chuyển giao, lưu trữ và giao dịch điện tử.

Theo nghĩa chung nhất, tiền ảo (Virtual Currency) là một loại tiền không vật lý, được tạo ra, mã hóa bằng công nghệ mã hóa và được quản lý, lưu trữ, vận hành trong hệ thống máy tính kết nối mạng Internet ngang hàng. Tiền ảo không phải là tiền tệ truyền thống được phát hành bởi ngân hàng trung ương hoặc cơ quan tài chính, thay vào đó, tiền ảo sử dụng các nền tảng công nghệ như Blockchain để tạo ra và xác nhận các giao dịch.

Tại Việt Nam, chưa có định nghĩa hay giải thích chính thức nào về tiền ảo được quy định trong các văn bản quy phạm pháp luật. Nhà nước ta thừa nhận tính pháp lý của tiền điện tử và giải thích thuật ngữ này tại Điều 3 Nghị định số 52 ngày 15/5/2024 của Chính phủ. Theo đó, tiền điện tử là giá trị tiền Việt Nam đồng lưu trữ trên các phương tiện điện tử, được cung ứng trên cơ sở đối ứng với số tiền được khách hàng trả trước cho ngân hàng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán cung ứng dịch vụ ví điện tử. Như vậy, phát sinh vấn đề đó là cần phân biệt tiền ảo (Virtual Currency) và tiền điện tử (E-Money).

- Sự khác biệt giữa tiền điện tử và tiền ảo ở những yếu tố:

+ Tiền điện tử (tiền pháp định) có sự bảo đảm từ phía Nhà nước (do ngân hàng Nhà nước phát hành), còn tiền ảo không được bảo đảm thực hiện bởi Nhà nước, đồng thời cũng không được bảo đảm thực hiện từ bất kỳ tổ chức nào.

+ Tiền điện tử có hình thức vật chất nhất định và tồn tại độc lập, còn tiền ảo luôn luôn phụ thuộc vào môi trường kỹ thuật số để tồn tại.

+ Tiền điện tử và tiền ảo tuy rằng cùng tồn tại và phụ thuộc vào môi trường kỹ thuật số, nhưng tiền điện tử là hình thức điện tử của tiền pháp định (ví điện tử, tài khoản thanh toán qua thiết bị điện tử,...).

+ Tiền ảo cũng có hình thức kỹ thuật số, nhưng nó hoàn toàn không gắn liền với đơn vị tiền tệ pháp định nào. Vì vậy, tiền ảo không được đảm bảo khả năng chuyển đổi thành tiền pháp định bởi các chủ thể phát hành hoặc quản lý nó và không có một tổ chức nào chịu trách nhiệm về những rủi ro cho một hoặc các bên chủ thể trong giao dịch liên quan đến tiền ảo.

1.2. Đặc điểm của tiền ảo

- Tính phi tập trung: Khác với tiền thật, là tiền do một tổ chức trung gian là ngân hàng phát hành và trực tiếp quản lý, hầu hết các loại tiền ảo hoạt động dựa trên công nghệ Blockchain, không cần tổ chức hoặc cá nhân trung gian.

- Tính biến động cao của giá trị: Giá trị của tiền ảo hoàn toàn phụ thuộc vào cung-cầu nên có tính biến động rất lớn. Trong khi đó, giá trị của tiền thật có tính ổn định cao hơn do phụ thuộc và sự quản lý của nhà nước và nhiều yếu tố khác.

- Khả năng giao dịch toàn cầu: Với tính chất kỹ thuật số và không phụ thuộc vào các giới hạn địa lý, tiền ảo có thể được giao dịch trên phạm vi toàn cầu một cách nhanh chóng và hiệu quả. Trong khi đó, tiền thật được chuyển bắt buộc phải qua các kênh trung gian là các ngân hàng. Các kênh trung gian này được điều chỉnh bởi pháp luật từng quốc gia và thỏa thuận giữa các quốc gia với nhau.

- Không có tính đại diện quốc gia: Với bản chất phi tập trung, không do tổ chức trung gian nào phát hành, quản lý và bảo đảm, tiền ảo khó có thể được xem là tiền của một quốc gia.

- Tính ẩn danh và không thể kiểm soát: Tiền ảo được tạo ra và hoạt động hoạt động dựa trên công nghệ blockchain trên mạng Internet ngang hàng nên có tính bảo mật cao và không thể kiểm soát. Tiền ảo cho phép người dùng giao dịch mà không cần tên, không cần đăng ký tài khoản ngân hàng hoặc tương tác với bên trung gian thứ ba.

Bản chất và các đặc điểm nêu trên của tiền ảo khiến chúng được lựa chọn và bị sử dụng cho các hoạt động bất hợp pháp. Giới tội phạm hiện nay thường "ziczac hóa" dòng tiền chiếm đoạt được bởi hành vi phạm tội để xóa dấu vết tội phạm, cản trở hoạt động điều tra. Chúng thường sử dụng mạng tối (Dark Web) để giao dịch tiền ảo và coi đó như một thứ công cụ hữu hiệu để hợp pháp hóa đồng tiền bất chính hoặc chuyển tiền bất hợp pháp ra nước ngoài.

2. Một số thuật ngữ cơ bản trong lĩnh vực tiền ảo

Trong lĩnh vực tiền ảo có rất nhiều thuật ngữ, liên quan đến nội dung tập huấn, cần nắm được một số thuật ngữ cơ bản sau:

2.1. Blockchain

- Khái niệm: Hiểu một cách đơn giản, Block nghĩa là khối, Chain là chuỗi, Blockchain nghĩa là chuỗi các khối kết nối với nhau, khối sau lấy thông tin của khối trước tạo thành một mắt xích. Blockchain là cấu trúc dữ liệu phân tán (phi tập trung) để lưu trữ thông tin dưới dạng các khối liên kết với nhau một cách an toàn và không thể thay đổi.

- Đặc điểm: Blockchain có các đặc điểm đó là nó có tính minh bạch và không thể thay đổi; phân quyền và phi tập trung; tính bảo mật cao; cho phép tạo và thực thi các hợp đồng thông minh (Smart Contracts), tự động hóa các quy trình và giao dịch mà không cần sự can thiệp của con người.

- Cơ chế hoạt động: Blockchain hoạt động như một sổ cái kỹ thuật số phân tán, nơi mỗi giao dịch được ghi chép lại một cách minh bạch và không thể thay đổi. Blockchain như một chuỗi gồm các khối, trong đó mỗi khối chứa dữ liệu về một giao dịch cụ thể. Khi một giao dịch mới được thực hiện, thông tin sẽ được ghi vào một khối mới và sau đó khối này được liên kết mật mã với khối trước đó, tạo thành một chuỗi liên tục. Điểm đặc biệt của Blockchain là tính phân quyền và không tập trung, không có một tổ chức nào quản lý sổ cái này. Thay vào đó, mỗi nút trong mạng lưới Blockchain sẽ giữ một bản sao của sổ cái, đảm bảo tính

minh bạch và khó bị tấn công hay gian lận. Mỗi khi một giao dịch mới được thêm vào, nó phải được xác nhận bởi một số lượng lớn các nút trong mạng, qua đó đảm bảo tính chính xác và an toàn của thông tin.

- Các loại Blockchain: Có 03 loại Blockchain là Public (công khai), Private (riêng tư) và Permissioned (có quyền hạn). Trong đó, Blockchain công khai được sử dụng phổ biến trong lĩnh vực tiền ảo. Đây là loại Blockchain mở, cho phép mọi người đều có thể tham gia, xác minh và thực hiện giao dịch, mọi giao dịch đều công khai và minh bạch, nhưng không ai có thể kiểm soát hoặc thay đổi dữ liệu đã được ghi vào Blockchain.

- Vai trò: Công nghệ Blockchain là chìa khóa khai sinh ra các loại tiền ảo, duy trì các giao dịch tiền ảo được bảo mật, an toàn và phi tập trung. Công nghệ Blockchain không chỉ giới hạn trong lĩnh vực tiền ảo, mà còn được sử dụng như "*sổ cái*" dữ liệu trong bất kỳ ngành nào để ngăn dữ liệu bị thay đổi hoặc gian lận.

2.2. Coin và Token

- Coin: Coin là đơn vị tiền tệ trong mạng lưới Blockchain, là giá trị của tiền ảo dựa trên công nghệ Blockchain của riêng chúng và có thể được sử dụng làm phương tiện thanh toán.

- Token: Token là một dạng chữ ký số hay chữ ký điện tử được mã hóa thành những con số trên thiết bị chuyên biệt. Mã Token tạo ra là dạng mã OTP nghĩa là mã sử dụng được một lần, tạo ngẫu nhiên cho mỗi giao dịch và bị giới hạn về thời gian hữu dụng. Token được sử dụng phổ biến trong lĩnh vực ngân hàng, mã OTP thường được cung cấp qua SMS hoặc máy Token do ngân hàng cung cấp.

- Phân biệt Coin và Token:

+ Coin có thể hoạt động một cách đơn lẻ dựa trên Blockchain riêng biệt của chính nó và được tích hợp trong các khối, còn Token hoạt động dựa trên sự liên kết với các Blockchain cụ thể nhưng không được tích hợp trong các khối.

+ Coin được xem như một loại tiền tệ có chức năng lưu trữ giá trị và giao dịch. Trong khi đó, Token được xem như là một dạng tài sản kỹ thuật số có chức năng thanh toán, có mục đích sử dụng rộng hơn Coin.

+ Mỗi loại Coin phải được lưu trữ trên một ví riêng, Token thì có thể lưu trữ nhiều Token trên cùng một ví nếu chúng được xây dựng trên cùng một nền tảng Blockchain. Coin có thể tự thực hiện giao dịch mà không mất phí, còn Token khi giao dịch phải trả phí cho nền tảng xây dựng của nó.

2.3. Ví (Wallet), Khóa (Key), Chuỗi từ hạt giống (Seed Phrase)

- Khái niệm: Ví tiền ảo là một chương trình phần mềm hoặc thiết bị được

thiết kế để tương tác với Blockchain của đồng tiền đó. Tiền ảo được lưu trữ trên Blockchain riêng của mỗi đồng tiền nên ví tiền ảo không lưu trữ tiền ảo mà nó lưu trữ khóa công khai và khóa riêng tư của chủ sở hữu cùng giao diện Blockchain giúp người dùng có thể dễ dàng thực hiện các giao dịch cũng như theo dõi biến động số dư từ ví. Khóa công khai và khóa riêng tư cũng chính là 02 thành phần cơ bản của ví tiền ảo.

- Phân loại:

+ Ví nóng (Hosted Wallet): Là ví Online kết nối trực tiếp với Internet, cho phép người dùng dễ dàng truy cập và sử dụng cho các giao dịch. Ví nóng có nhiều hình thức khác nhau, chẳng hạn như ví ứng dụng di động, ví dùng trên máy tính và ví trực tuyến.

+ Ví lạnh (Unhosted Wallet): Là thiết bị điện tử (bên trong chip bảo mật có tên là Secure Element) lưu trữ Offline (không kết nối với Internet), được dùng để lưu trữ khóa riêng tư để mở nơi chứa tiền ảo trên Internet.

- Khóa công khai (Public Key) và Khóa riêng tư (Private Key):

+ Đây là cặp khóa luôn gắn liền với nhau, nó là đoạn mã gồm chuỗi các ký tự được lưu trong ví tiền ảo. Khi giao dịch tiền ảo trên Internet sẽ khởi tạo ra cặp khóa này. Khoá riêng tư tạo ra khóa công khai, tiếp đó khóa công khai này lại tạo ra địa chỉ ví công khai, nhưng không thể làm ngược lại (mã hóa một chiều).

+ Khóa công khai được người dùng sử dụng như địa chỉ của mình để đưa cho người khác (tương đương số tài khoản ngân hàng) chuyển tiền ảo vào tài khoản của mình, khóa công khai chính là địa chỉ để bạn cho mọi người biết bạn đang ở đâu trên mạng. Trong khi đó, khóa riêng tư được người dùng sử dụng để truy cập ví tiền ảo và thực hiện giao dịch (tương đương mật khẩu).

- Chuỗi từ hạt giống (Seed Phrase):

+ Là một chuỗi các từ khóa ngẫu nhiên gồm 12, 18 hoặc 24 từ được tạo ra theo tiêu chuẩn BIP39 (Bitcoin Improvement Proposal 39-Đề xuất cải tiến Bitcoin 39) khi người dùng tạo một ví Blockchain mới.

+ BIP39 quy định trong chuỗi từ hạt giống có 02 quy tắc đó là: 04 chữ cái đầu tiên của mỗi từ là duy nhất và không có 2 từ nào trong danh sách này có 4 ký tự đầu tiên giống nhau.

+ Chuỗi từ hạt giống được coi là chìa khóa chính của ví tiền ảo vì nó hỗ trợ người dùng khôi phục ví tiền ảo khi họ quên mật khẩu của ví. Mất chuỗi từ hạt giống sẽ mất tiền ảo vĩnh viễn vì không thể khôi phục được ví tiền ảo khi không có chuỗi từ hạt giống.

2.4. Hàm băm giao dịch (Hashing)

- Băm là một hàm toán học chuyển đổi bất kỳ dữ liệu đầu vào có kích thước bất kỳ thành một chuỗi ký tự có kích thước cố định gọi là hàm băm. Hàm băm biến đoạn dữ liệu thành mã nhị phân (chỉ là 1 và 0). Sau đó, nó chia các con số thành các phần và liên tục áp dụng một hàm tính toán. Kết quả cuối cùng thường là một chuỗi gồm 64 kí tự gồm các chữ và số. Hàm băm là chức năng một chiều không thể đảo ngược, là duy nhất đối với dữ liệu đầu vào và bất kỳ thay đổi nào trong dữ liệu đầu vào sẽ dẫn đến một hàm băm khác.

- Hàm băm được mật mã hóa chính là cốt lõi của tiền ảo. Nhờ chúng mà Blockchain và các hệ thống phân tán khác có thể đạt được tính toàn vẹn và bảo mật của dữ liệu ở mức độ cao.

- Có nhiều thuật toán băm, trong đó thuật toán băm Hash 256 được sử dụng phổ biến nhất của công nghệ Blockchain. Thuật toán này tạo ra một hàm băm 256 bit có độ dài cố định, xác định duy nhất một khối hoặc giao dịch trên Blockchain.

- Mỗi giao dịch trong một Blockchain được biểu thị bằng một hàm băm duy nhất đóng vai trò là mã định danh. Hàm băm này được tạo bằng cách chạy dữ liệu giao dịch qua thuật toán băm, tạo ra hàm băm có độ dài cố định. Hàm băm này sau đó được đưa vào khối tiếp theo trong Blockchain, tạo ra một khối được bảo mật bằng hàm băm mật mã. Hầu hết hàm băm là sự kết hợp của các chữ số và chữ cái thường thể hiện bằng chứng rằng tiền ảo đã được giao dịch.

2.5. Hợp đồng thông minh (Smart Contracts)

- Khái niệm: Hợp đồng thông minh là một giao thức giao dịch được máy tính thực hiện dựa trên công nghệ Blockchain, đó là các chương trình tự động chạy khi thỏa mãn những điều kiện đã được xác định từ trước nhằm mục đích tự động hóa về mặt pháp lý việc thực hiện thỏa thuận. Hiểu một cách đơn giản, với các điều kiện xác định trước, một hợp đồng thông minh được chạy trên blockchain là nơi mà thông qua đó, người tham gia vào chương trình này chắc chắn về kết quả ngay lập tức mà không chịu tác động bởi các bên trung gian. Bản chất của hợp đồng thông minh là một hợp đồng kĩ thuật số chứa mã bảo mật của công nghệ Blockchain. Tiền ảo Etherium-loại tiền ảo phổ biến luôn luôn sử dụng hợp đồng thông minh trong giao dịch.

- Để hợp đồng thông minh có thể hoạt động, cần có các yếu tố sau: Chủ thể hợp đồng (các bên tham gia) được cấp quyền truy cập. Có các điều khoản của hợp đồng quy định ở dạng chuỗi, được lập trình đặc biệt mà các bên tham gia

phải đồng ý với các điều này. Có chữ ký số và phải thực hiện thao tác thông qua chữ ký số. Hợp đồng phải được tải lên Blockchain để phân phối dữ liệu về các node, mỗi node sẽ kiểm tra tính hợp lệ của hợp đồng và xác nhận nó vào một khối mới, không thể điều chỉnh.

- So với hợp đồng truyền thống, hợp đồng thông minh có ưu điểm đó là tự động, minh bạch, an toàn, có tính tùy biến cao, tiết kiệm thời gian và chi phí, giảm thiểu rủi ro cho các bên tham gia. Tuy nhiên, hợp đồng thông minh cũng có nhược điểm đó là khó khăn trong điều chỉnh dữ liệu, khó giải quyết tranh chấp, phụ thuộc vào công nghệ Blockchain, rủi ro về tính pháp lý và rò rỉ dữ liệu.

2.6. Danh tính khách hàng (Know Your Customer-KYC)

- Khái niệm: KYC quy trình mà sàn giao dịch tiền ảo và các tổ chức tài chính sử dụng để xác minh danh tính khách hàng khi khách hàng mở tài khoản. Mục đích của quy trình này nhằm đảm bảo toàn bộ khách hàng đăng ký đều là người thật, là chính chủ.

- Các loại KYC:

+ KYC thông thường sẽ thực hiện xác minh danh tính khách hàng thông qua việc điền thông tin cơ bản (như họ tên, ngày sinh, địa chỉ, số điện thoại, email,...) vào biểu mẫu giấy và cung cấp bản sao giấy tờ tùy thân hợp pháp (căn cước công dân, hộ chiếu, giấy phép lái xe,...).

+ KYC điện tử (Electronic Know Your Customer-eKYC) sẽ thực hiện xác minh danh tính khách hàng bằng kỹ thuật số thông qua việc điền thông tin vào biểu mẫu điện tử, chụp ảnh selfie (ảnh chân dung) hoặc quay video selfie theo hướng dẫn, chụp ảnh các giấy tờ tùy thân hợp pháp, dữ liệu sinh trắc học vân tay, giọng nói, nhận diện khuôn mặt, sau đó sẽ dùng công nghệ trí tuệ nhân tạo (AI) để định danh tự động.

- Vai trò của KYC: Giúp các sàn giao dịch tiền ảo và các tổ chức tài chính xác minh thông tin người dùng, xác định được những rủi ro liên quan đến khách hàng, nâng cao tính an toàn cho các giao dịch, góp phần phát hiện và ngăn chặn các hoạt động gian lận,.... Trong điều tra, truy tố các vụ việc, vụ án hình sự về tội phạm công nghệ cao liên quan đến tiền ảo, KYC thu giữ được từ các sàn giao dịch tiền ảo và các tổ chức tài chính là những thông tin, tài liệu rất quan trọng giúp các cơ quan thực thi pháp luật xác định được có hành vi phạm tội là ai, thu thập được các chứng cứ chứng minh hành vi phạm tội của họ.

2.7. Dịch vụ trộn và giao dịch trộn (Coin Mixer)

- Các giao dịch liên quan đến tiền ảo đều được ghi lại trên một sổ cái

Blockchain công khai, phi tập trung. Điều này có nghĩa là tất cả mọi người đều có thể truy cập được những hồ sơ này. Từ đó, phát sinh dịch vụ trộn và giao dịch trộn tiền ảo với mục đích che dấu danh tính, số lượng tiền giao dịch, đích đến của tiền để bảo vệ khách hàng khỏi hành vi trộm cắp hoặc gian lận tiềm ẩn.

- Dịch vụ trộn và giao dịch trộn là các dịch vụ được các sàn giao dịch tiền ảo cung cấp cho khách hàng để làm cho các giao dịch tiền ảo trở nên không theo dõi được bằng cách kết hợp các khoản tiền ảo từ nhiều nguồn khác nhau làm chúng trở nên không xác định được và không thể liên kết trở lại với người dùng ban đầu. Máy trộn Coin có thể được coi như một công ty phần mềm là người trung gian cung cấp cho người dùng khả năng kết hợp chuyển tiền qua các địa chỉ tiền ảo khác nhau, thu thập một số lượng lớn hơn của cùng một loại tiền ảo và sau đó phân tán nó đến địa chỉ đích được chỉ định. Khách hàng phải trả phí cho việc sử dụng dịch vụ trộn và giao dịch trộn.

- Dịch vụ trộn và giao dịch trộn tiền ảo là cách thức phổ biến mà tội phạm sử dụng để che dấu danh tính, che dấu hành vi phạm tội, rửa tiền, hợp thức hóa nguồn tiền. Đây là thách thức rất lớn đặt ra đối với các các cơ quan thực thi pháp luật trong việc xác định, truy vết tiền ảo để chứng minh hành vi phạm tội và người phạm tội.

2.8. Sàn giao dịch tiền ảo (Virtual Currency Exchange)

- Sàn giao dịch tiền ảo là nền tảng trực tuyến của tổ chức, doanh nghiệp cho phép khách hàng mua bán, trao đổi, lưu trữ, rút nhiều loại tiền ảo khác nhau thông qua Internet theo các quy tắc nhất định của sàn giao dịch. Sàn giao dịch tiền ảo hoạt động như một nhà môi giới, kết nối giữa người mua và người bán để thực hiện các giao dịch và thu phí.

- Về bản chất, sàn giao dịch tiền ảo là 01 ví nóng lớn, chứa nhiều địa chỉ tiền ảo khác nhau. Đây là đặc điểm rất quan trọng sàn giao dịch tiền ảo mà các cơ quan pháp luật cần lưu ý. Quá trình xác định, điều tra, truy vết tiền ảo; nếu đích đến của tiền ảo là các sàn giao dịch thì sẽ không dùng các công cụ truy vết tiền ảo để tiếp tục truy vết nữa mà cần sự hợp tác các cung cấp thông tin tiếp theo từ sàn giao dịch.

- Các sàn giao dịch có thể chấp nhận thanh toán bằng thẻ tín dụng, chuyển khoản ngân hàng hoặc các hình thức thanh toán khác để đổi lấy tiền ảo. Đây là thông tin quan trọng khi tiến hành truy vết qua tài khoản ngân hàng.

II- CHÍNH SÁCH, PHÁP LUẬT VIỆT NAM VỀ TIỀN ẢO

Từ năm 2013, tiền ảo Bitcoin bắt đầu len lỏi vào Việt Nam, kéo theo sự góp

mặt của hàng loạt đồng tiền ảo khác như Ethereum (ETH), Tether (USDT), Binance Coin (BNB),..., thu hút một lượng người quan tâm và tham gia đầu tư bởi sự hấp dẫn từ những quảng cáo về lợi nhuận thu được từ việc tăng giá của các loại tiền này khi đầu tư. Các hoạt động giao dịch ngầm, đầu tư, mua bán tiền ảo, huy động vốn qua phát hành tiền ảo (ICO) vẫn diễn ra khá sôi động, đặc biệt là hoạt động sử dụng tiền ảo để huy động vốn theo phương thức đa cấp ngày càng diễn biến phức tạp, điều này làm gia tăng các loại hình thức lừa đảo, đặc biệt trên môi trường điện tử.

1. Trong lĩnh vực pháp luật về tiền tệ, ngân hàng, thương mại

Dưới góc độ thanh toán, pháp luật Việt Nam hiện tại quy định tiền Đồng (VNĐ) là tiền tệ hợp pháp duy nhất, được dùng để thanh toán tại Việt Nam. Ngân hàng nhà nước là cơ quan duy nhất phát hành tiền VNĐ. Điều 17 Luật Ngân hàng nhà nước năm 2010 chỉ ghi nhận tiền giấy, tiền kim loại; không có quy định nào liên quan đến việc chấp nhận và phát hành tiền ảo. Do đó, tiền ảo không phải là phương tiện thanh toán hợp pháp tại Việt Nam.

Thông cáo báo chí ngày 27/02/2014, và văn bản gửi các cơ quan báo chí ngày 28/10/2017 của Ngân hàng nước khẳng định: Theo các quy định của pháp luật hiện hành về tiền tệ và ngân hàng, Bitcoin và các loại tiền ảo tương tự khác không phải là phương tiện thanh toán hợp pháp tại Việt Nam. Việc phát hành, cung ứng, sử dụng Bitcoin và các loại tiền ảo tương tự khác làm phương tiện thanh toán là hành vi bị cấm tại Việt Nam. Việc sử dụng Bitcoin và các loại tiền ảo tương tự khác làm phương tiện thanh toán không được pháp luật thừa nhận và bảo vệ. Các tổ chức tín dụng không được phép sử dụng Bitcoin và các loại tiền ảo tương tự khác như một loại tiền tệ hoặc phương tiện thanh toán khi cung ứng dịch vụ cho khách hàng. Công văn số 4486 ngày 20/7/2018 của Ủy ban Chứng khoán Nhà nước đề nghị các công ty đại chúng, công ty chứng khoán, công ty quản lý quỹ, quỹ đầu tư chứng khoán, không được thực hiện hoạt động phát hành, giao dịch và môi giới tiền ảo trái pháp luật.

Ngày 21/8/2017, Thủ tướng Chính phủ đã ban hành Quyết định số 1255 về phê duyệt Đề án hoàn thiện khung pháp lý để quản lý, xử lý đối với các loại tài sản ảo, tiền điện tử, tiền ảo. Ngày 11/04/2018, Thủ tướng Chính phủ ban hành Chỉ thị số 10 về tăng cường quản lý các hoạt động liên quan tới Bitcoin và các loại tiền ảo tương tự khác. Trên cơ sở đó, ngày 13/4/2018, Thống đốc Ngân hàng nhà nước đã ban hành Chỉ thị số 02 về các biện pháp tăng cường kiểm soát các giao dịch, hoạt động liên quan đến tiền ảo. Vào tháng 5/2020, Bộ trưởng Bộ Tài chính đã quyết định thành lập Tổ nghiên cứu về tài sản ảo, tiền ảo, nhằm triển

khai công tác nghiên cứu, đề xuất các nội dung chính sách, cơ chế quản lý theo chức năng, nhiệm vụ của Bộ, có liên quan đến tài sản ảo, tiền ảo.

Dưới góc độ hàng hóa, theo Nghị định số 52 ngày 16/05/2013 và Nghị định số 85 ngày 25/9/2021 (sửa đổi, bổ sung) của Chính phủ về thương mại điện tử thì Bitcoin và các loại tiền ảo tương tự khác không nằm trong danh mục hàng hóa kinh doanh bị cấm theo hình thức thương mại điện tử. Trong khi đó, Công văn số 334 ngày 12/8/2014 của Cục Thương mại điện tử Bộ Công Thương lại cho rằng Bitcoin không đáp ứng các đặc tính cơ bản của hàng hóa hay dịch vụ, do đó Bitcoin không phải là hàng hóa, hay dịch vụ. Công văn số 5612 ngày 28/12/2015 của Tổng cục Thuế, Bộ Tài chính cho rằng tiền ảo là tài sản (động sản) theo quy định của Bộ luật Dân sự nên là hàng hóa theo Luật Thương mại, hoạt động mua bán tiền ảo là hoạt động mua bán hàng hóa. Công văn số 2313 ngày 19/6/2016 của Viện kiểm sát nhân dân tối cao (Vụ 3) xác định hiện chưa có văn bản quy phạm pháp luật nào điều chỉnh về hành vi khai thác Bitcoin và các loại tiền ảo nên chưa có căn cứ pháp lý để xử lý loại hành vi này.

Như vậy, có thể thấy rằng, do chưa có khung pháp lý điều chỉnh rõ ràng về tiền ảo đã dẫn đến việc tồn tại nhiều cách hiểu khác nhau về tiền ảo, điều này tạo ra nhiều khó khăn, mâu thuẫn trong công tác kiểm soát và quản lý tiền ảo. Hơn nữa, đây cũng là cơ hội để các đối tượng lợi dụng để thực hiện các hành vi lừa đảo, trục lợi thông qua các hoạt động đầu tư, kinh doanh tiền ảo.

2. Trong lĩnh vực pháp luật dân sự, hình sự

Khoản 1 Điều 105 Bộ luật Dân sự 2015 quy định tài sản là vật, tiền, giấy tờ có giá và quyền tài sản. Theo quy định mang tính chất liệt kê này, tài sản chỉ tồn tại ở 04 dạng là gồm vật, tiền, giấy tờ có giá và quyền tài sản. Trong đó, tiền là phương tiện thanh toán do nhà nước phát hành, được nhà nước bảo hộ để định giá, trao đổi, thanh toán cho các loại tài sản khác (tiền pháp định). Tiền ảo không thuộc 01 trong 04 loại nêu trên nên không được coi là tài sản. Như vậy, trong lĩnh vực này, pháp luật dân sự không quy định tiền ảo là tài sản. Tuy nhiên, có quan điểm cho rằng, tiền ảo là một loại quyền tài sản theo quy định của Bộ luật Dân sự 2015 vì quyền tài sản là quyền trị giá được bằng tiền và không có giới hạn về loại tài sản này. Sự không thống nhất trong cách hiểu nêu trên là do quy định pháp luật, đặc biệt là các quy định pháp luật dân sự chưa có quy định nào khẳng định tiền ảo là một loại tài sản. Hơn nữa, chính việc chưa có văn bản pháp luật nào quy định cụ thể tiền ảo có phải là một loại tài sản hay không đã dẫn đến việc không thể thống nhất được trong việc xác định các nghĩa vụ, trách nhiệm liên quan đến tiền ảo cũng như việc điều chỉnh các quan hệ dân sự như sở hữu,

thừa kế, hợp đồng hay bồi thường thiệt hại liên quan đến tiền ảo cũng gần như rơi vào khoảng trống, không có một cơ chế để giải quyết một cách phù hợp.

Trong thực tiễn, các tranh chấp dân sự thường phát sinh liên quan đến tiền ảo gồm: Quyền sở hữu, mua bán, vay mượn, thừa kế tiền ảo, bồi thường thiệt hại trong giao dịch tiền ảo. Các giao dịch, tranh chấp liên quan đến tiền ảo chưa được pháp luật quy định và bảo hộ, dẫn đến thực trạng nhiều đương sự có đơn khởi kiện không được Tòa án thụ lý với nhiều lý do khác nhau, mặc dù Khoản 2 Điều 4 Bộ luật Tố tụng dân sự 2015 có quy định Tòa án không được từ chối giải quyết vụ việc dân sự vì lý do chưa có điều luật áp dụng.

Việc phát hành, cung ứng và sử dụng tiền ảo làm phương tiện thanh toán là không hợp pháp theo quy định tại Khoản 10, 11 Điều 3 Nghị định số 52 ngày 15/5/2024 của Chính phủ. Việc phát hành, cung ứng, sử dụng các phương tiện thanh toán không hợp pháp sẽ bị xử phạt hành chính theo quy định tại Khoản 6 Điều 26 Nghị định số 88 ngày 01/7/2016 của Chính phủ. Theo quy định tại Điểm h Khoản 1 Điều 206 Bộ luật Hình sự năm 2015 thì hành vi phát hành, cung ứng, sử dụng phương tiện thanh toán không hợp pháp (bao gồm cả Bitcoin và các loại tiền ảo tương tự khác) mà gây thiệt hại cho người khác về tài sản từ 100 triệu đồng đến dưới 300 triệu đồng là phạm tội hình sự. Theo các quy định pháp luật nêu trên, có thể thấy rằng, việc sử dụng tiền ảo làm phương tiện thanh toán tại Việt Nam là hành vi vi phạm pháp luật và có thể bị xử phạt vi phạm hành chính hoặc xử lý hình sự.

Trong thực tiễn, có nhiều vụ án hình sự liên quan đến việc lừa đảo, chiếm đoạt tiền ảo như: Nhận tiền ảo sau đó không trả lại cho người đầu tư hoặc nhận tiền đầu tư rồi chiếm đoạt, không giao lại tiền ảo cho nhà đầu tư. Cùng nhau hợp tác công sức để tạo lập tiền ảo, chia kết quả bằng tiền ảo nhưng người này lại chiếm đoạt tiền ảo của người kia khi giá tiền ảo lên cao, hoặc do mâu thuẫn với nhau trong làm ăn, kinh doanh. Điển hình là vụ án cướp Bitcoin xảy ra tại TP Hồ Chí Minh tháng 5/2020, sau 03 năm mới được đưa ra xét xử sơ thẩm vào tháng 5/2023. Tòa án cấp sơ thẩm đã bác các quan điểm của Luật sư khi cho rằng hiện pháp luật Việt Nam chưa công nhận tiền ảo là tài sản nên không có căn cứ để xử lý các bị cáo về hành vi cướp Bitcoin. Theo quan điểm của Tòa án, pháp luật Việt Nam chưa chấp nhận Bitcoin là tiền tệ và phương tiện thanh toán, nhưng Tòa không chỉ căn cứ vào kết luận định giá để kết tội các bị cáo. Tôi cướp tài sản có cấu thành hình thức, các bị cáo khai nhận ngay từ đầu đã lê kế hoạch để cướp 1.000 Bitcoin trị giá 200 tỷ đồng của bị hại. Thực tế, các bị cáo đã cướp được số Bítcoin quy đổi ra tiền VNĐ là hơn 37 tỷ đồng và bán để chia nhau hưởng lợi.

Từ thực trạng nêu trên nêu trên có thể thấy rằng, hiện nay tại Việt Nam chưa có khung pháp lý hoàn chỉnh và đầy đủ về tiền ảo. Việc điều chỉnh về tiền ảo dưới khía cạnh pháp lý mới dừng lại ở việc ban hành các thông cáo báo chí, công văn, chỉ thị mang tính chất khuyến cáo. Do thiếu khung pháp lý điều chỉnh nên việc hiểu và xác định các vấn đề pháp lý liên quan đến tiền ảo còn nhiều bất cập và chưa tạo được sự thống nhất. Điều đó đã gây ra nhiều khó khăn trong cách hiểu, cách tiếp cập về loại tiền này, đặt ra nhiều thách thức trong công tác quản lý, kiểm soát và xử lý các hành vi vi phạm về tiền ảo. Đặc biệt, với sự tồn tại những khoảng trống pháp luật về tiền ảo đã tạo cơ hội cho các chủ thể lợi dụng để thực hiện các hành vi lừa đảo, trục lợi gây thiệt hại nghiêm trọng cho người tham gia. Chính vì vậy, việc đẩy mạnh nghiên cứu hoàn thiện khung pháp lý về tiền ảo một cách đầy đủ tại Việt Nam là điều rất quan trọng và cấp thiết trước yêu cầu thực tiễn hiện nay. Khi khung pháp lý liên quan đến tiền ảo khi được hoàn thiện sẽ giúp hạn chế, ngăn chặn và kiểm soát hiệu quả các rủi ro, lạm dụng liên quan cũng như phòng ngừa được các hành vi phạm tội trong lĩnh vực này.

III- MỘT SỐ TIỀN ẢO CƠ BẢN VÀ PHỔ BIẾN

1. Bitcoin (BTC)

1.1. Tổng quan

- Bitcoin là tiền ảo được tạo ra từ công nghệ Blockchain, được sử dụng như một phương tiện thanh toán trực tuyến và có tính tiền tệ độc lập, không phụ thuộc vào ngân hàng trung ương hay chính phủ nào.

- BTC là một trong những loại tiền ảo phổ biến, dẫn đầu theo vốn hóa thị trường. BTC sử dụng mạng ngang hàng (peer-to-peer), cho phép người gửi giao dịch trực tiếp với người nhận mà không cần thông qua bên trung gian. BTC được cấp tới các máy tính đào BTC để trả công cho việc xác minh giao dịch BTC và ghi chúng vào cuốn sổ cái được phân tán trong mạng ngang hàng, thông qua công nghệ Blockchain, cuốn sổ cái này sử dụng BTCla đơn vị kế toán.

- Mỗi BTC có thể được chia nhỏ tới 100 triệu đơn vị nhỏ hơn gọi là Satoshi. 01 Satoshi tương đương với 0,00000001 BTC. Sự cung ứng Bitcoin là tự động, hạn chế, được phân chia theo lịch trình định sẵn dựa trên các thuật toán vì chỉ có tối đa 21 triệu BTC. Trang web của BTC là bitcoin.org.

1.2. Đặc tính

- Tính phi tập trung: Mạng lưới BTC được xây dựng dưới dạng không tập trung, không có máy chủ hoạt động, không do bất cứ một cơ quan nào kiểm soát do đó khó có thể bị thao túng hay bị đánh sập.

- Tính ẩn danh: Bất kỳ ai tham gia vào mạng lưới BTC cũng đều có quyền lợi như nhau và thực hiện giao dịch một cách ẩn danh. Người tham gia không cần phải xác minh danh tính hay bất cứ điều gì khác để vào được mạng lưới giao dịch BTC. Đây là đặc tính mà kẻ phạm tội lợi dụng BTC để thực hiện hành vi phạm tội.

- Tính minh bạch: Hệ thống BTC sẽ lưu lại chi tiết các thông tin giao dịch của người tham gia trên Bockchain. Người tham gia có thể biết được một địa chỉ chứa số lượng BTC nhưng không biết được người đang giữ nó là ai.

- Không thể bị hoàn trả: Khi BTC đã được chuyển đi thì sẽ không thể lấy lại được, trừ trường hợp được người nhận gửi. Bởi khi thông tin đã được ghi vào Blockchain, không ai có thể thay đổi hay chỉnh sửa thông tin đó được. Thông tin trong Blockchain chỉ được bổ sung thêm khi có sự đồng thuận của tất cả các node trong hệ thống.

1.3. Địa chỉ ví Bitcoin

- Là bộ định danh có từ 25 đến 36 ký tự chữ và số (có phân biệt chữ thường và chữ hoa) dùng để gửi BTC tới người khác hoặc nhận BTC từ người khác gửi tới. Các địa chỉ BTC và khóa riêng tư được quản lý trong ví, ví BTC lưu và chứa được nhiều cặp khóa, ví quản lý giao dịch và cho phép tiêu tài sản ảo. Ví có thể chỉ dùng riêng cho một loại tiền ảo hoặc có thể chứa nhiều loại tiền ảo khác nhau.

- Tùy theo phương pháp được tiêu chuẩn hóa để nhận BTC trên chuỗi Blockchain mà ví BTC bắt đầu với một trong các số, ký tự như sau:

+ Số 1: Sử dụng đối với giao thức P2PKH (Pay to public key hash-nhận BTC theo địa chỉ). Thay vì sử dụng địa chỉ, P2PK gửi BTC trực tiếp cho 01 khóa công khai.

+ Số 3: Sử dụng đối với giao thức P2SH (Pay to script hash-nhận BTC linh hoạt), tạo ra theo BIP13, có độ dài 34 ký tự, tạo được địa chỉ đa chữ ký. Người nhận xác định chi tiết đoạn mã và hướng dẫn về việc chi tiêu không được tiết lộ công khai cho đến khi BTC được chi tiêu khỏi địa chỉ.

+ Chuỗi ký tự bc1: Sử dụng đối với giao thức Bech32- Bitcoin Core. Bech32 không còn phân biệt chữ hoa và chữ thường. Các địa chỉ có chuỗi ký tự và số dài hơn nhưng lại ít sử dụng các ký tự khác nhau.

- Phân tích 01 địa chỉ ví BTC, cơ quan pháp luật sẽ có được các thông tin sau: Tổng số tiền đối tượng đã gửi và nhận. Tổng giá trị mà đối tượng đang nắm giữ. Các địa chỉ mà đối tượng đã gửi tiền tới. Các địa chỉ mà đối tượng đã nhận được tiền. Sàn giao dịch mà đối tượng đang sử dụng (có thể có KYC). Bản chất

thủ đoạn phạm tội của đối tượng. Các địa chỉ của nạn nhân. Số nạn nhân và tổng tiền nhận được từ nạn nhân. Các địa chỉ của đồng phạm và đối tượng khác có liên quan. Ví tiền của đối tượng. Dòng tiền mà đối tượng đã giao dịch,...

1.4. Giao dịch và chuỗi khối của Bitcoin

- Giao dịch là việc chuyển giá trị giữa các ví BTC được đưa vào chuỗi khối. 01 giao dịch BTC có các thành phần gồm: Hàm băm giao dịch; địa chỉ đầu vào; địa chỉ đầu ra; số lượng/giá trị giao dịch; khối; thời gian, kích cỡ, phí giao dịch, các xác nhận. Các giao dịch BTC thường có tiền thừa hoàn lại gọi là giao dịch UTXO (Unspent Transaction Output-đầu ra giao dịch chưa sử dụng) là một kỹ thuật dùng để theo dõi dịch chuyển số dư giữa các ví tiền mã hóa), đây là một trong nguồn căn cứ quan trọng để cơ quan pháp luật truy vết tiền ảo.

- Chuỗi khối là một sổ cái công khai được chia sẻ mà toàn bộ mạng lưới Bitcoin dựa vào. Tất cả các giao dịch đã xác nhận đều được đưa vào chuỗi khối, nó cho phép ví BTC tính toán số dư có thể chi tiêu của chúng để các giao dịch mới có thể được xác minh, đảm bảo rằng chúng thực sự thuộc sở hữu của người chi tiêu.

- Phân tích chuỗi khối của BTC sẽ có được các thông tin sau: Quan hệ giữa các địa chỉ; xây dựng được mạng lưới; xác định được đặc điểm sở hữu của địa chỉ; xác định, thay đổi quyền kiểm soát. Đặc biệt, cơ quan pháp luật sẽ điều tra bám theo dòng tiền từ nơi xuất phát cho đến điểm đích của dòng tiền.

1.5. Đào Bitcoin (Bitcoin Mining)

- Là quá trình tạo mới BTC thông qua việc xác nhận và ghi chép các giao dịch trên mạng lưới Blockchain. Đào Bitcoin được thực hiện bởi các máy tính chạy phần mềm đào, người tham gia quá trình này gọi là thợ đào BTC. 01 máy đào Bitcoin AntMiner S9 của Bitman giá 4.900 USD có thể đào 0,0018 BTC/01 ngày, nghĩa là để đào được 01 BTC thì máy phải hoạt động liên tục 556 ngày.

- Quá trình đào BTC tóm tắt như sau: Khi thực hiện giao dịch sẽ tạo ra khối mới, mạng lưới Blockchain sẽ tạo ra 01 hàm băm cho khối giao dịch -> Người đào (Miner) bắt đầu tạo ra các hàm băm bằng phần mềm đào -> Người đào đầu tiên tạo ra hàm băm sẽ được gắn khối mà mình đào được vào bản sao của chuỗi khối -> Những người đào khác và các nốt bảo mật kiểm tra xem khối có đúng không -> Xác nhận giao dịch và trở thành bản ghi vĩnh viễn -> Người đào nhận được tiền ảo BTC (tiền thưởng) từ khối, từ đó tạo ra BTC mới.

2. Ethereum (ETH)

2.1. Tổng quan

- ETH là tiền ảo không giới hạn số lượng, nó được xây dựng trên công nghệ Blockchain mã nguồn mở, quản lý phi tập trung, nó có khả năng thực thi hợp đồng thông minh, tức là điều khoản được ghi trong hợp đồng sẽ được thực thi một cách tự động khi các điều kiện trước đó được thỏa mãn, không ai có thể can thiệp vào. Về bản chất, ETH là một hệ thống phân bổ gồm các máy tính ghi lại tất cả các giao dịch tiền ảo. Trang Web của ETH là https://ethereum.org.

- Ethereum cung cấp một môi trường trong đó những người dùng có thể tạo ra các ứng dụng phi tập trung (DApps-Decentralized Application) và triển khai chúng trên mạng, cho phép người tham gia giao dịch với nhau mà không cần ngân hàng trung ương hay chính phủ nào. Nó khác với Bitcoin, nền tảng blockchain đầu tiên, bởi vì Ethereum cho phép thực hiện các chương trình phức tạp hơn thông qua hợp đồng thông minh.

- Khi thực hiện giao dịch hoặc tương tác với hợp đồng thông minh trên nền tảng Blockchain ETH, bắt buộc người dùng phải thanh toán khoản chi phí bắt buộc gọi là phí gas ETH (ETH gas fee). Gas là một đơn vị đặc biệt, là tài nguyên tính toán khi đáp ứng một nhiệm vụ nhất định. Nó đóng vai trò như "*nhiên liệu*" cung cấp năng lượng cho cỗ máy Blockchain hoạt động trơn tru.

2.2. Đặc tính

- ETH hoạt động thông qua mạng lưới các máy tính gọi là Nodes (là các nút dùng để lưu trữ, truyền tải và bảo quản dữ liệu trên Blockchain). Để tham gia vào mạng lưới này, các Nodes cài đặt phần mềm Ethereum Client. Sau khi cài đặt, Nodes sẽ chạy chương trình ảo thực hiện các hợp đồng thông minh gọi là EVM (Ethereum Virtual Machine-máy đào tiền ảo ETH).

- EVM thực hiện các hoạt động như thực thi các lệnh giao dịch và thực hiện các hợp đồng thông minh. Mỗi giao dịch và hoạt động trong EVM đều yêu cầu một lượng phí Gas được thanh toán bằng tiền ETH.

- Sau khi thực hiện giao dịch, các Nodes sẽ tiến hành xác minh tính hợp lệ của giao dịch này và dùng cơ chế Proof of Work (PoW-thuật toán đồng thuận) để chứng minh rằng họ đã hoàn thành công việc và thông báo kết quả này cho toàn bộ mạng (còn gọi là bằng chứng công việc, người đào chuyển năng lượng sang khối đào). Sau đó, các Nodes khác sẽ thực hiện việc xác nhận và kiểm tra tính hợp lệ của bằng chứng này.

- Một khối mới được tạo ra bằng cách giải mã với thuật toán Ethash, sau đó mạng lưới xác nhận các giao dịch thông qua PoW và dữ liệu giao dịch được ghi vào Blockchain của ETH và không thể thay đổi.

2.3. Ví ETH

- Ví ETH là một ứng dụng phần mềm hoặc phần cứng nơi lưu trữ ETH, cung cấp quyền truy cập vào ETH, giúp người dùng toàn quyền kiểm soát, mua bán, theo dõi số dư của ETH, thực thi hợp đồng thông minh và tương tác với các ứng dụng phi tập trung DApps trên mạng Ethereum. Ví ETH được kiểm soát thông qua khóa riêng tư chỉ có người tạo ra ví mới được biết, vì bất kỳ ai biết chúng đều có thể truy cập vào tài sản của họ. Ví ETH bao gồm 3 thành phần:

+ Địa chỉ ví (Address): Là địa chỉ định danh người dùng trên mạng lưới ETH, cho phép người dùng có thể chia sẻ công khai để nhận tiền mã hoá về ví của mình.

+ Khoá riêng tư (Private Key): Là chuỗi ký tự gồm chữ cái và số ngẫu nhiên, đóng vai trò là mật khẩu giúp người dùng truy cập vào địa chỉ ví và quản lý tài sản bên trong.

+ Cụm mật khẩu (Seed Phrase): Là tập hợp gồm 12 cụm từ tiếng Anh bất kỳ, cho phép người dùng bảo mật tài khoản và khôi phục ví trong trường hợp bị mất hoặc thay đổi thiết bị lưu trữ ví.

- Địa chỉ ví ETH: Địa chỉ Ethereum là một chuỗi ký tự hexa (hệ cơ số 16) dài 40 ký tự, bắt đầu bằng "**0x**", đại diện cho ví ETH của người dùng. Nó là định danh duy nhất được sử dụng để nhận và gửi các loại tiền ảo và thực hiện các giao dịch thông qua mạng Blockchain ETH. Số dư của mọi địa chỉ ETH có thể được nhìn thấy trên Blockchain, mặc dù không biết ai kiểm soát địa chỉ nào vì địa chỉ trên mạng được biểu thị thông qua một chuỗi số và chữ cái. Khác với địa chỉ BTC, địa chỉ ETH hỗ trợ nhiều tính năng tiên tiến hơn như hợp đồng thông minh và DApps.

IV- XÁC ĐỊNH, TRUY VẾT, THU GIỮ TIỀN ẢO TRONG ĐIỀU TRA, TRUY TỐ

1. Quy trình và một số vấn đề đặc trưng cần làm rõ

1.1. Quy trình xác định, truy vết tiền ảo

* *Bước 1*: Kiểm tra, phân tích nguồn dữ liệu sẵn có do người bị hại, người làm chứng cung cấp hoặc từ các nguồn khác, cụ thể:

- Thông tin địa chỉ ví, hàm băm giao dịch chuyển tiền, thời gian giao dịch, giá trị của giao dịch, thiết bị sử dụng để truy cập Internet.

- Những nội dung, vật chứng có liên quan đến khóa riêng tư, khóa công khai, cụm từ hạt giống và các dữ liệu, tài liệu khác có liên quan.

* *Bước 2*: Xác định, truy vết theo dòng tiền ảo, cụ thể:

- Xác định loại tiền ảo theo định dạng địa chỉ (BTC, ETH,...).

- Sử dụng các công cụ truy vết tiền ảo để theo dõi giao dịch chuyển đến các địa chỉ ví, dịch vụ trộn tiền, dịch vụ ẩn danh, phần tiền thừa hoàn lại, phí GAS.

- Kiểm tra các thông tin liên quan đến giao dịch (thời gian, giá trị,...), tiền pháp định được đối tượng rút ra. Từ đó xác định tính chất, mức độ, phương thức, thủ đoạn phạm tội nhằm định hướng điều tra, truy vết đối với các giao dịch tiên quan tới tài khoản gốc của tội phạm.

Lưu ý: Ngay khi phát hiện dòng tiền giao dịch được chuyển tới sàn giao dịch thì dừng truy vết để yêu cầu sàn giao dịch cung cấp dữ liệu về người dùng tài khoản đối với giao dịch đó.

* *Bước 3*: Thu thập hồ sơ và phân tích dữ liệu, cụ thể:

- Yêu cầu các cơ quan, tổ chức, doanh nghiệp, các sàn giao dịch liên quan cung cấp thông tin liên quan (KYC) tới tài khoản tình nghi để phục vụ điều tra.

- Đối chiếu các thông tin sẵn có và các thông tin được cơ quan, tổ chức, doanh nghiệp, các sàn giao dịch liên quan cung cấp để phát hiện các vấn đề chưa làm rõ, phát sinh, mâu thuẫn trong quá trình truy vết.

- Xác định có bao nhiêu chủ sở hữu ví tiền, bao nhiêu ví tiền trong tài khoản, bao nhiêu địa chỉ nhận/chuyển tiền, bao nhiêu loại tiền trong tài khoản, mã khôi phục tài khoản tiền điện tử;

- Khai thác các thông tin đăng nhập vào tài khoản, xác định danh tính, địa chỉ IP; chi tiết lịch sử giao dịch trên tài khoản; quá trình nạp/rút tiền trong tài khoản; thời gian, số lượng, loại tiền; cách thức chuyển dịch, giao dịch, chuyển đổi loại tiền trong tài khoản; địa chỉ ví tiền nhận.

* *Bước 4*: Tổng hợp, đánh giá kết quả thu thập

- Tổng hợp, đánh giá kết quả thu thập được từ 03 bước trên để xác định danh tính đối tượng và các đặc điểm định danh cá nhân khác.

- Tiến hành thu giữ tiền ảo (chi tiết ở phần sau).

- Xác định, đề xuất áp dụng các biện pháp tố tụng như: Khám xét thu giữ vật chứng, tài sản; áp dụng các biện pháp ngăn ngặn đối với đối tượng,...

1.2. Một số vấn đề đặc trưng cần làm rõ

- Thu thập chứng cứ chứng minh, làm rõ đối tượng chính là người quản lý, sử dụng tài khoản có chứa tiền ảo tham gia vào việc thực hiện tội phạm.

- Thu thập chứng cứ làm rõ chi tiết từng hành vi của đối tượng thông qua tài khoản, ví tiền ảo; cách thức quy đổi giữa tiền ảo thành tiền pháp định hoặc tiền VNĐ tại từng thời điểm nhất định.

- Xác định loại tiền ảo, địa chỉ tiền ảo; làm rõ quá trình mua bán, nạp, chuyển, nhận tiền ảo; các giao dịch mua bán tiền ảo trong nội bộ sàn giao dịch của đối tượng với người khác.

- Xác định thời gian, số lượng, mã giao dịch mua bán, nạp, chuyển, nhận tiền của đối tượng với người khác thông qua địa chỉ và ví của tiền ảo.

2. Các công cụ xác định, truy vết tiền ảo

2.1. Sử dụng Chainalysis

- Đây là công ty chuyên cung cấp các dịch vụ hỗ trợ điều tra tiền ảo và phải trả phí cho công ty. Cụ thể là cung cấp các giải pháp phân tích chuyên sâu về Blockchain và theo dõi, phân tích hoạt động tiền ảo. Có thể phân tích các hoạt động gian lận, rửa tiền, giao dịch không hợp lệ trên Blockchain.

- Trang Web của Chainalysis là chainalysis.com (khi truy cập có thể dùng email đăng ký sử dụng bản Demo để trải nghiệm).

2.2. Truy cập các Website

Một số trang Web có độ tin cậy cao, có nhiều chức năng, chứa đựng nhiều thông tin có giá trị trong việc xác định, tìm kiếm, truy vết tiền ảo gồm:

- Coinmarketcap.com; tokenmarket.com; icoalert.com: Thống kê tiền ảo.

- Coinmap.org: Mức độ chấp thuận tiền ảo theo từng khu vực địa lý.

- Blockchain.com; blockchair.com: Truy vết tiền ảo trên Blockchain.

- Mempool.space; walletexplorer.com; reactor.chainalysis.com: Truy vết BTC.

- Etherscan.io, Ethplorer.io, otx.me; explorer.binance.org: Truy vết ETH.

- Open2eppelin.com, tokensniffer.com: Truy vết hợp đồng thông minh.

- Trang Web của các sàn giao dịch, đặc biệt là Binance.

3. Thu giữ tiền ảo trong điều tra, truy tố

3.1. Quy trình thu giữ

** Giai đoạn chuẩn bị thu giữ:*

- Bước 1: Tạo tài khoản tiền ảo (thực hiện trên máy tính 1).

+ Sử dụng máy tính để tạo tài khoản với cặp khóa riêng tư và khóa công khai do cơ quan nhà nước quản lý.

+ Cài đặt, sử dụng hệ điều hành phù hợp hoặc các phần mềm, phần cứng cần thiết.

+ Lựa chọn loại ví tốt nhất cho từng loại tiền ảo cần thu giữ (ví Eletrum dành cho Bitcoin, ví Exodus dành cho ETH hoặc các loại tiền ảo khác).

+ Tạo một khóa chính và bất kỳ khóa bổ sung nào thêm.

+ Sử dụng trình khám phá Blockchain công khai để đảm bảo không có bản gi nào về các địa chỉ công khai ở trên chuỗi khối. Nếu bản ghi tồn tại, hãy xóa các cặp khóa và bắt đầu lại.

+ Sao chép các địa chỉ (không phải khóa riêng tư), xóa chúng khỏi máy tính 1, xác nhận các địa chỉ được sao chép là chính xác.

- ***Bước 2***: Bảo mật các khóa của cơ quan thu giữ, gồm:

+ Ghi lại và sao lưu các cặp khóa, các bản sao lưu trên giấy và kỹ thuật số.

+ Hợp nhất các bản sao lưu kỹ thuật số và giấy.

+ Lưu trữ các bản sao lưu ngoại tuyến ở 01 vị trí an toàn bằng cách niêm phong với các cá nhân có liên quan.

+ Xóa ví gốc, để an toàn có thể xóa sạch dữ liệu ở máy tính 1.

- ***Bước 3***: Cài đặt thiết bị chuyển tiền ảo (thực hiện trên máy tính 2).

+ Cài đặt, sử dụng hệ điều hành phù hợp hoặc các phần mềm, phần cứng cần thiết.

+ Sử dụng máy tính 2 kết nối với Internet để sử dụng cho việc chuyển tiền ảo.

+ Lựa chọn loại ví tốt nhất cho từng loại tiền ảo cần chuyển (ví Eletrum dành cho Bitcoin, ví Exodus dành cho ETH hoặc các loại tiền ảo khác).

+ Xác nhận ví được đồng bộ hóa với Blockchain.

* *Giai đoạn thu giữ*:

- ***Bước 4***: Xác định vị trí các khóa riêng tư và các ví

+ Tìm kiếm phần mềm ví và các tệp tin liên quan đến ví tiền ảo.

+ Tìm kiếm địa chỉ, khóa riêng tư và mật khẩu.

+ Tìm kiếm từ các phần mềm phục hồi.

- ***Bước 5***: Xuất các khóa riêng tư và các ví cần thu giữ.

+ Sử dụng các công cụ chuyên ngành kỹ thuật hình sự (nếu có).

+ Sử dụng chức năng xuất khóa (hoặc tương tự) trong phần mềm ví.

+ Sao chép toàn bộ tệp tin ví tiền ảo.

+ Sao chép bất kỳ khóa riêng tư nào được lưu trên giấy, trong tệp văn bản hoặc các tài liệu xử lý văn bản khác.

- ***Bước 6***: Nhập các khóa riêng tư tìm được vào máy tính 2

+ Sử dụng chức năng nhập khóa (hoặc tương tự) trong phần mềm ví.

+ Sao chép các tệp tin ví vào thư mục thích hợp.

- ***Bước 7***: Chuyển tiền ảo từ địa chỉ mục tiêu sang địa chỉ do cơ quan thu thu giữ thiết lập

+ Đảm bảo máy tính 2 kết nối với Internet, chuỗi khối được đồng bộ hóa.

+ Điều chỉnh cài đặt mặc định của ví.

+ Nhấp vào tùy chọn gửi trong ví.

+ Làm theo lời nhắc trên màn hình và điền thông tin vào trường bắt buộc.

+ Nhấp vào gửi.

* *Giai đoạn sau thu giữ*:

- ***Bước 8***: Xác nhận giao dịch

+ Tìm kiếm địa chỉ do nhà nước kiểm soát bằng trình khám phá Blockchain và xác nhận giao dịch.

+ Ghi lại quá trình thu giữ, bao gồm giá trị băm của giao dịch, số tiền ảo được gửi trong mỗi giao dịch và phí giao dịch.

+ Sử dụng công cụ định giá dựa trên giá tiền ảo để ước tính giá trị của tiền ảo vào ngày thu giữ.

3.2. Xử lý một số tình huống khi thu giữ

- Trường hợp đối tượng tự nguyện chuyển đổi tiền kỹ thuật số trong ví sang tiền pháp định để chuyển về tài khoản của đối tượng thì lập biên bản về việc này. Sau đó, tiến hành phong tỏa tài khoản ngân hàng (đây là trường hợp tối ưu phục vụ cho việc điều tra, truy tố, xét xử).

- Trường hợp đối tượng không đồng ý chuyển đổi tiền kỹ thuật số trong ví sang tiền pháp định mà chỉ đồng ý chuyển tiền kỹ thuật số sang ví khác: Tiến hành tạo ví mới (ví nóng hoặc ví lạnh, nên chọn ví lạnh vì bảo mật cao hơn), lưu giữ khóa bảo mật và các thông tin liên quan đến ví mới vừa tạo. Chuyển toàn bộ số tiền kỹ thuật số trong ví điện tử của đối tượng sang ví mới vừa tạo. Lập biên bản chi tiết về việc chuyển đổi tiền kỹ thuật số nêu trên. Giao ví mới vừa tạo cho cán bộ trực tiếp tạo ví quản lý và chịu trách nhiệm.

- Trường hợp đối tượng không cung cấp thông tin về ví điện tử hoặc không tự nguyện chuyển đổi tiền kỹ thuật số sang tiền pháp định thì cần lập biên bản ghi nhận lại sự việc thể hiện rõ các nội dung: Số lượng, giá quy đổi của tiền kỹ thuật số; địa chỉ ví, địa chỉ nhận mã OTP (One Time Password). Lý do đối tượng không hợp tác và yêu cầu đối tượng cam kết tự bảo toàn số tiền kỹ thuật số có trong ví, không được phát sinh giao dịch và tự chịu trách nhiệm về việc bị mất. Sau đó, tiến hành thu giữ, niêm phong vật chứng, thiết bị, phương tiện điện tử của đối tượng theo quy định.