بررسی جرایم سایبری در حوزه ارزهای دیجیتال و طرح‌های کلاهبرداری مدرن

علی‌رضا قاسمی
وکیل پایه یک دادگستری

فصل‌نامه علمی- تخصصی / سال سوم، شماره ۸ / زمستان ۱۴۰۳

مقدمه

در سال‌های اخیر، رشد فناوری‌های نوین مالی و ظهور ارزهای دیجیتال، فرصت‌ها و چالش‌های متعددی را برای نظام‌های اقتصادی و حقوقی کشورها ایجاد کرده است. در کنار این فرصت‌ها، فعالیت‌های غیرقانونی نظیر شرکت‌های هرمی (مانند فیوچر، یونیک فایننس و موارد مشـــابه) که عمدتاً با پوشش سرمایه‌گذاری در حوزه ارزهای دیجیتال فعالیت می‌کنند، مشکلات جدی برای نظام حقوقی و اقتصادی کشور به وجود آورده‌اند. این مقاله به تحلیل وضعیت حقوقی این فعالیت‌ها در چارچوب قوانین و مقررات داخلی می‌پردازد.

مطالعه موردی:

پرونده کلاهبرداری موسوم به پروژه سرمایه‌گذاری "Filipping" در قم

چکیده

پیشـــرفت فناوری اطلاعات و ظهور ارزهای دیجیتال در سال‌های اخیر، فرصت‌های جدید اقتصادی را فراهم کرده است، اما هم‌زمان بستری مناسب برای شکل‌گیری جرایم

سایبری مانند کلاهبرداری‌های اینترنتی، پولشویی و طرح‌های هرمی مدرن نیز ایجاد کرده است. این مقاله با بررسی ابعاد مختلف این جرایم، به تحلیل‌های حقوقی و استناد به پرونده‌های واقعی پرداخته و خلأهای قانونی موجود در ایران را تشریح می‌کند.

دکتر عبدالحسین شیروی در کتاب جرایم رایانه‌ای و اینترنتی بیان می‌کند:

«ناشناس بودن کاربران و سهولت انجام تراکنش‌ها از طریق شبکه‌های غیرمتمرکز، چالش‌های بسیاری برای قانون‌گذاران و نظام قضایی کشورها ایجاد کرده است» (شیروی، ۱۳۹۹، ص ۸۷).

یکی از پرونده‌های مشهور در این زمینه، پرونده صرافی غیرقانونی MT.Gox در ژاپن است که منجر به سرقت ۸۵۰ هزار بیت‌کوین و نابودی سرمایه‌گذاران شد. این پرونده نشان می‌دهد که خلأ نظارت و امنیت در معاملات ارزهای دیجیتال، چگونه زمینه را برای کلاهبرداری‌های کلان فراهم می‌کند.

*****ماهیت شرکت‌های هرمی و تمایز آن از فعالیت‌های اقتصادی مشروع**

شرکت‌های هرمی مانند فیلیپینگ (Filipping) به طور کلی با هدف جذب سرمایه‌گذاران جدید به منظور پرداخت به سرمایه‌گذاران قبلی طراحی می‌شوند. در این سیستم‌ها، بیشتر درآمد افراد از جذب اعضای جدید به سیستم است تا از فروش محصولات یا خدمات واقعی. این گونه شرکت‌ها معمولاً پتانسیل کلاهبرداری دارند و در بسیاری از کشورهای جهان غیرقانونی محسوب می‌شوند. برخی از ویژگی‌های شرکت‌های هرمی عبارتند از:

۱. ورود به سیستم با پرداخت هزینه یا خرید محصول به قیمت بالاتر از ارزش واقعی آن.

۲. ایجاد شبکه‌ای از افراد جدید برای کسب درآمد از طریق جذب اعضای بیشتر به جای تمرکز بر فروش محصول واقعی.

۳. فقدان محصولات یا خدمات واقعی با ارزش در سیستم، یا اگر هم محصولی وجود داشته باشد، کیفیت آن معمولاً بسیار پایین است.

در مقابل، شـــرکت‌های مشروع و قانونی دارای ویژگی‌هایی هســـتند که آن‌ها را از شرکت‌های هرمی متمایز می‌کند:

۱. محصولات یا خدمات واقعی: شـــرکت‌های قانونی برای درآمد خود بر روی فروش محصولات یا خدمات با کیفیت تکیه می‌کنند. این محصولات باید دارای ارزش واقعی باشند و قابل استفاده یا مصرف برای مشتریان.

۲. مدل کســـب‌وکار مبتنی بر فروش: در شرکت‌های مشروع، درآمد از فروش واقعی محصولات یا خدمات حاصل می‌شود، نه از جذب سرمایه‌گذاران جدید.

۳. قانونی بودن و شفافیت: این شرکت‌ها معمولاً تحت نظارت مراجع قانونی و مقررات کسب‌وکار قرار دارند و فعالیت‌های آنها شفاف و ثبت شده است.

در نتیجه، تمایز اصلی بین شـــرکت‌های هرمی و شرکت‌های مشروع در نحوه کسب درآمد، مشروعیت، و وجود محصولات یا خدمات با ارزش است.

***** بررسی پرونده کلاهبرداری موسوم به سیستم هرمی "فلیپینگ" در ایران**

شرح پرونده

در این پرونده که بنده بعنوان وکیل شـــاکیه حضور دارم، خانم ف.آ، یکی از قربانیان در سراسر کشور، با تبلیغات گسترده در اینستاگرام از سوی شخصی به نام ا.ع ترغیب شد که در طرحی موسوم به فلیپینگ سرمایه‌گذاری کند. با تشویق‌های فرد کلاهبردار، موکله فریب خورده و تعداد ۱۵ واحد اتریوم (معادل ۵ میلیارد تومان در زمان سرمایه گذاری) را در این سیستم سرمایه‌گذاری می‌کند. نهایتاً، اتریوم‌های استیک‌شده موکل توســـط سیستم قفل شده و امکان دسترسی همیشگی به سرمایه از دست می‌رود. در همین حین، فرد معرف که موکل با ترغیب او وارد سیستم شده، ناپدید می‌شود.

مکانیسم این نوع کلاهبرداری بر پایه یک طرح هرمی است که در آن اعضای جدید مجبور به پرداخت مبلغی برای ورود شـــده و سود افراد قدیمی از محل سرمایه‌گذاری تازه واردها تأمین می‌شود. پس از مدتی، حساب کاربری قربانیان به بهانه‌های مختلف از جمله عدم دسترسی به استخر نقدینگی مسدود و دارایی‌های آنان ضبط می‌شود.

تحلیل مفهومی و فنی کلاهبرداری موضوع سیستم فلیپینگ

در این بخش، برای شفاف‌ســـازی موضوع سیســـتم هرمی فلیپینگ و تبیین مفهوم استیک کردن اتریوم و نحوه عملکرد کلاهبرداری، توضیحات زیر را به مرجع قضایی و در مقام دفاع ارائه نمودم:

- فلیپینگ چیست؟
- فلیپینگ (Flipping) در دنیای ارزهای دیجیتال معمولاً به خرید و فروش ســـریع ارزها برای کسب سود اشاره دارد.
- اما در این پرونده، فلیپینگ به عنوان یک پروژه هرمی یا پانزی ارائه شده است.
- مشتکی‌عنهم ادعا کرده‌اند که با خرید اتریوم و مشارکت در یک سیستم استیکینگ خاص، می‌توان در مدت کوتاهی سود کلانی کسب کرد.
- این پروژه بر اساس ساختار هرمی طراحی شده که سود افراد جدیدالورود، به حساب معرفان واریز می‌شود (نه از فعالیت واقعی یا سود سرمایه‌گذاری).
- استیک کردن اتریوم چیست؟
- استیکینگ (Staking) به معنای قفل کردن مقدار مشخصی از یک ارز دیجیتال در یک قرارداد هوشمند برای دریافت پاداش است.
- در این پرونده، کلاهبرداران ادعای دروغین مطرح کرده‌اند و به جای اتصال موکل به یک شبکه معتبر، اتریوم‌های استیک‌شده را به کیف پول خودشان منتقل کرده‌اند.

در نهایت از مرجع قضایی و در مقام تحقیقات خواســـته ام که دستورات مقتضی را جهت رهگیری ولت (آدرس کیف پول دیجیتال) متعلق به موکله و مشتکی عنهم انجام بدهد.

برای تسریع فرآیند بررسی و ره‌یابی تراکنش‌های مربوط به پرونده‌های کلاهبرداری ارزهای دیجیتال، همکاری دقیق با پلیس فتا از اهمیت بالایی برخوردار اســـت. در این راســـتا، ارائه مستندات و اطلاعات صحیح و جامع می‌تواند روند پیگیری را بهینه‌سازی کرده و امکان بازیابی وجوه ازدست‌رفته را افزایش دهد.

۱. اطلاعات دقیق کیف پول دیجیتال را در اختیار پلیس فتا قرار بدهید:

• آدرس کیف پول دیجیتال: اولین و مهم‌ترین مدرک، آدرس کیف پول (Wallet Address) موکل است. این آدرس باید بدون نقص در اختیار پلیس فتا قرار گیرد تا ره‌یابی تراکنش‌ها ممکن شود.

• آدرس‌های عمومی برای ارزهای دیجیتال مختلف: در صورتی که موکل از چند نوع ارز دیجیتال (مانند بیت‌کوین، اتریوم، تتر و ...) استفاده کرده، باید تمامی آدرس‌های مربوطه ارائه شود.

۲. اطلاعات مربوط به تراکنش‌ها

• تاریخ و زمان تراکنش‌ها: مشخص کردن دقیق زمان هر تراکنش به پلیس فتا کمک می‌کند تا بررسی‌های خود را در بازه مشخصی انجام دهد.

• مقدار ارز منتقل‌شده: حجم و ارزش تراکنش‌های مشکوک باید به تفکیک ذکر شود.

• شناسه تراکنش (TXID): ارائه TXID هر تراکنش به پلیس فتا امکان بررسی دقیق و ره‌یابی مبالغ را می‌دهد.

۳. اطلاعات سیستم و سرویس‌های مورد استفاده

• پلتفرم‌های مرتبط با کیف پول: نام و نوع کیف پول دیجیتال (مثلاً Metamask، Trust Wallet) یا صرافی‌های مورد استفاده (مانند Binance، Coinbase) باید مشخص شود.

• نام یا شناسه حساب‌های مرتبط: اگر از پلتفرم‌های دیفای یا پروژه‌های استیکینگ استفاده شده است، این اطلاعات به همراه نام حساب ارائه شود.

۴. اسناد و مدارک مرتبط با مالکیت کیف پول

• اثبات مالکیت کیف پول: مدارکی مانند ایمیل‌های مرتبط، کلید خصوصی (در صورت امکان)، یا گواهی صادرشده توسط سرویس‌دهنده کیف پول باید ارائه شود.

• مکاتبات مرتبط: هرگونه ایمیل یا چت مربوط به تراکنش‌ها که می‌تواند در شناسایی متهمان مفید باشد، به پرونده اضافه شود.

۵. استفاده از ابزارهای ره‌گیری تراکنش‌ها

• تحلیل بلاک‌چین: اســـتفاده از ابزارهای ره‌گیری مانند Etherscan (برای اتریوم) یا Blockchain Explorer (بـــرای بیت‌کوین) می‌تواند اطلاعات مفیدی درباره تراکنش‌ها ارائه دهد.

۶. شناسایی فعالیت‌های مشکوک

• گزارش فعالیت‌های غیرعادی: در صورت مشـــاهده رفتار مشکوک در کیف پول یا حساب‌های مرتبط، این موارد باید به‌طور مستند ارائه شوند.

۷. همکاری با پلیس فتا و کارشناسان فنی

• ارائه اطلاعات کارشناسی: در صورت نیاز، همکاری با تحلیل‌گران بلاک‌چین می‌تواند به ره‌یابی دقیق تراکنش‌ها کمک کند.

۸. ارائه شواهد فنی دیگر

• اسکرین‌شات‌های حساب‌ها و تراکنش‌ها: ثبت تصاویر از تراکنش‌ها، تاریخچه کیف پول و سوابق حساب‌های صرافی‌ها می‌تواند در تحقیقات کمک‌کننده باشد.

چگونه با پلیس فتا همکاری کنید؟

۱. تماس اولیه با پلیس فتا: گزارش جرم و ارائه اطلاعات اولیه.

۲. تحویل مستندات کامل: ارائه مدارک و اطلاعات مربوط به کیف پول، تراکنش‌ها و ارتباطات مالی.

۳. رصـــد وضعیت کیف پول: همـــکاری با پلیس در اســـتفاده از ابزارهای ره‌گیری بلاک‌چین.

۴. پیگیری و تعامل با کارشناسان: در برخی پرونده‌ها، همکاری متخصصان تحلیل بلاک‌چین ضروری اســـت.از قاضـــی بخواهید ضمن همکاری با پلیـــس فتا از کمک کارشناسان خبره دراین زمینه استفاده کند.

***** قوانین بین‌المللی موجود درباره ارزهای دیجیتال و جرایم مرتبط**

۱.مقررات FATF در خصوص مبارزه با پول‌شویی و تأمین مالی تروریسم

گروه ویژه اقدام مالی (FATF) که وظیفه نظارت بر جرایم مالی بین‌المللی را بر عهده دارد، در سال ۲۰۱۹ دستورالعمل‌هایی برای نظارت بر تراکنش‌های ارزهای دیجیتال صادر کرد. این دستورالعمل‌ها شامل موارد زیر است:

- الزام صرافی‌های ارز دیجیتال به احراز هویت مشتریان (KYC).
- ثبت و گزارش تراکنش‌های مشکوک به مراجع ذی‌صلاح.
- ایجاد سازوکار نظارتی برای جلوگیری از پول‌شویی و تأمین مالی تروریسم.

۲. مقررات اتحادیه اروپا (MiCA)

در سال ۲۰۲۳، اتحادیه اروپا قانونی به نام مقررات بازارهای دارایی‌های دیجیتال (MiCA) تصویب کرد که هدف آن تنظیم بازار ارزهای دیجیتال است.

۳. مقررات ایالات متحده (SEC و CFTC)

- کمیسیون بورس و اوراق بهادار آمریکا (SEC) بسیاری از عرضه‌های اولیه سکه (ICO) را تحت قوانین اوراق بهادار قرار داده و آنها را ملزم به ثبت کرده است.
- کمیسیون معاملات آتی کالا (CFTC) ارزهای دیجیتال را به عنوان کالا شناخته و مقررات خاصی برای معاملات آنها وضع کرده است.

*****تحلیل حقوقی جرایم سایبری در ایران**

۱. قوانین موجود و محدودیت‌ها

در ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ تنها به جرایم رایانه‌ای عمومی پرداخته است و هنوز قوانین جامعی برای مقابله با جرایم مرتبط با ارزهای دیجیتال وجود ندارد.

البته در مورد شرکت‌های هرمی معمولا قضات دادگاه طبق بند ز ماده یک قانون مجازات اخلالگران در نظام اقتصادی (الحاقی۱۳۸۴/۱۰/۱۴)- تأسیس، قبول نمایندگی و عضوگیری در بنگاه، موسسه، شرکت یا گروه به منظور کسب درآمد ناشی از افزایش اعضاء به نحوی که اعضاء جدید جهت منفعت، افراد دیگری را جذب نموده و توسعه زنجیره یا شبکه انسانی تداوم یابد.» که جرم‌انگاری شده است حکم صادر می‌نمایند.

*** تاکنون، بانک مرکزی ایران هنوز مجوز رسمی برای صرافی‌های ارز دیجیتال

صادر نکرده است. این امر به دلیل نبود چارچوب‌های قانونی مشخص در حوزه ارزهای دیجیتال است. با این حال، صرافی‌های معتبری در ایران فعالیت می‌کنند که با رعایت مقررات عمومی و دریافت مجوزهای لازم، خدمات خود را ارائه می‌دهند. برخی از این صرافی‌ها عبارت‌اند از: نوبیتکس، آبان تتر، تترلند، والکس، بیت‌پین، تبدیل، اکسیر، رمزینکس، او ام پی فینکس.

این صرافی‌ها با رعایت استانداردهای امنیتی و نظارتی، محیطی امن و شفاف را برای کاربران فراهم می‌کنند. با وجود عدم صدور مجوز رسمی، این صرافی‌ها با رعایت مقررات و استانداردهای موجود، به فعالیت خود ادامه می‌دهند و کاربران می‌توانند با اطمینان نسبی از خدمات آن‌ها استفاده کنند. لکن با این وجود، بانک مرکزی ایران استفاده از ارزهای دیجیتال به‌عنوان ابزار پرداخت ممنوع است. (بانک مرکزی جمهوری اسلامی ایران در تاریخ ۹ دی ۱۳۹۶، طی اطلاعیه‌ای به کارگیری بیت‌کوین و سایر ارزهای دیجیتال را در تمام مراکز پولی و مالی کشور ممنوع اعلام کرد.

همچنین، در مصوبه هیئت وزیران به شماره ۵۸۱۴۴/ت۵۵۶۳۷هـ مورخ ۱۳ مرداد ۱۳۹۸، تأکید شده است که استفاده از رمزارزها در مبادلات داخل کشور مجاز نیست و مسئولیت ریسک آن بر عهده متعاملین است.

این مصوبات نشان‌دهنده موضع رسمی بانک مرکزی و دولت در خصوص محدودیت استفاده از ارزهای دیجیتال به‌عنوان ابزار پرداخت در داخل کشور است.)

فلذا لازم است قانون‌گذار با شناخت دقیق جهت کشف و تعقیب جرایم سایبری و سیستم‌های هرمی قوانین و مقررات روزآمدی را تدوین نماید.

دکتر ابوالفضل طهری در مقاله تحلیل طرح‌های پانزی اشاره می‌کند:

«نبود قوانین شفاف و به‌روز در زمینه ارزهای دیجیتال و جرایم مرتبط با آن، فرصت‌های بسیاری برای مجرمان سایبری ایجاد کرده است» (طهری، ۱۴۰۰، ص ۱۲۰).

***خلأهای قانونی و راهکارهای پیشنهادی

۱. تدوین قوانین مشخص برای ارزهای دیجیتال و طرح‌های هرمی

۲. تشکیل دادگاه‌های تخصصی جرایم سایبری
۳. ایجاد نهادهای نظارتی برای ردیابی جرایم مالی دیجیتال
۴. عدم شفافیت در تعیین صلاحیت قضایی در جرایم بین‌المللی سایبری

*****پیشنهادات برای بهبود قانون‌گذاری**

- تدوین قوانین جامع برای ارزهای دیجیتال شـــامل تعاریف، مصادیق جرم و نحوه رسیدگی به آن‌ها.
- تقویت همکاری‌های بین‌المللی و امضای معاهدات همکاری در حوزه جرایم سایبری.
- ایجاد سازوکارهای نظارتی بر صرافی‌های ارز دیجیتال مانند الزام به گزارش‌دهی.
- توسعه ابزارهای پیش‌رفته ردیابی و تحلیل برای رهگیری تراکنش‌های مجرمانه.

نتیجه‌گیری

پرونده‌های مربوط به کلاهبرداری‌های ســـایبری و طرح‌های هرمی مانند فلیپینگ نشان می‌دهد که عدم وجود قوانین مشخص و نظارت دقیق بر ارزهای دیجیتال، بستری مناسب برای فعالیت‌های مجرمانه فراهم کرده است. برای مقابله با این تهدیدات، لازم اســـت که قانون‌گذاری دقیق‌تری انجام شـــود و نهادهای قضایی و انتظامی ابزارهای مناسبی برای پیگیری این جرایم داشته باشند.

برای اینکه پلیس فتا بتواند به‌ســـرعت سابقه تراکنش‌ها را بررسی کند، ارائه اطلاعات دقیق کیف پول، تراکنش‌ها، سوابق حساب‌ها و مدارک معتبر ضروری است. همچنین استفاده از ابزارهای تحلیلی مانند Etherscan می‌تواند در تسریع روند تحقیقات مؤثر باشد.

منابع

فارسی:
۱. شیروی، عبدالحسین (۱۳۹۹)، جرایم رایانه‌ای و اینترنتی، انتشارات سمت.
۲. طهری، ابوالفضل (۱۴۰۰)، "تحلیـــل طرح‌های پانزی و جرایم مرتبط با ارزهای

دیجیتال"، فصلنامه حقوق و فناوری، شماره ۲۵.
۳. موســـوی، رضا (۱۴۰۱)، "بررســـی قوانین ایران در حوزه رمزارزها"، مجله حقوق اقتصادی، شماره ۴۵.
۴. قانون جرایم رایانه‌ای ایران، مصوب ۱۳۸۸.
۵. قانون مبارزه با پول‌شویی، مصوب ۱۳۸۶ و اصلاحات بعدی آن.
انگلیسی:
۶. Nakamoto, S. (۲۰۰۸), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org
۷. Zohar, A. (۲۰۱۵), "Bitcoin: under the hood", Communications of the ACM, ۹)۵۸), pp. ۱۱۳-۱۰۴.
۸. Europol Report (۲۰۲۱), "Cryptocurrency and Criminal Activities", available at: www.europol.europa.eu
۹. Financial Action Task Force (FATF), "Guidance on Virtual Assets and Virtual Asset Service Providers" (۲۰۲۱), available at: www.fatf-gafi.org
۱۰. کتاب "Securities Regulation" (نوشتهٔ Jerry Markham)
وکتاب "Fraud and Abuse in the Investment Industry" (نوشتهٔ S.A. Knapp)
مقالات علمی Journal of Financial Economics و Journal of Business Ethics