یازدهمین همایش سالانه
بانکداری نوین و
نظام‌های پرداخت
پژوهشکده پولی و بانکی
بانک مرکزی جمهوری اسلامی ایران
بانک مرکزی جمهوری اسلامی ایران
شرکت ملی انفورماتیک
زیست بوم بانکداری هوشمند؛ حکمرانی دیجیتال و نظارت فنّاورانه
تهران، مرکز همایش‌های بین‌المللی برج میلاد ـ ۵ و ۶ آذر ۱۴۰۳ ISC

هوشمندسازی و کاهش مخاطرات مبارزه با پول‌شویی در حوزه رمزارزها

مهدی حجتی نیا[۱]

چکیده

در شروع هزاره سوم فناوری اطلاعات به عنوان عمده‌ترین محور تحول و توسعه در جهان مطرح شده و دستاوردهای ناشی از آن نیز به گونه‌ای با زندگی مردم عجین گردیده که روی‌گردانی و بی‌توجهی به آن اختلالات عظیمی را در جامعه به وجود می‌آورد. تغییر در فناوری پتانسیل ایجاد نوآوری را دارد از سوی دیگر فرصت‌های جدیدی را برای مجرمان و تروریست‌ها مهیا می‌کند تا از آن طریق درآمدهای غیرقانونی خود را مشروع جلوه دهند یکی از برجسته‌ترین پیشرفت‌های فناوری در دهه گذشته، راه‌اندازی دارایی‌های مجازی بوده است که به شکل ارزهای دیجیتال غیرمتمرکز با ارزهای مجازی در فضای معاملاتی خرد و کلان ایجاد شده است. هدف اصلی پژوهش حاضر، کشف و شناسایی مخاطرات حوزه پول‌شویی در زمینه رمزارزها در کشور ایران است. این پژوهش در دسته پژوهش‌های کاربردی قرار دارد و به صورت توصیفی انجام شده است. با بررسی ادبیات داخلی و بین‌المللی تعدادی از مخاطرات از قبیل باج افزار صرافی ارز، مجازی دارک نت جرایم مالی غیرمتمرکز، پل، دستگاه‌های خودپرداز رمزارز و فنتانیل شناسایی شده‌اند نتایج به دست آمده از این پژوهش پیشنهادهایی کارآمد برای کاهش مخاطرات حوزه مبارزه با پول‌شویی در بستر معاملات دیجیتال می‌باشد که از طریق به کارگیری عوامل شناسایی شده در آن، در فرایند خط‌مشی گذاری قانون‌گذاری در زمینه، رمزارزها فناوری اطلاعات و ارتباطات می‌تواند موجب بهبود وضعیت کشور از منظر گروه ویژه اقدام مالی به عنوان اصلی‌ترین نهاد سیاست‌گذار بین‌المللی در این حوزه گردد و به رعایت توصیه شماره ۱۵ و ۱۶ گروه ویژه اقدام مالی کمک شایانی نماید.

واژه‌های کلیدی: رمزارز، ارز دیجیتال، هوشمند سازی، مخاطرات مبارزه با پول‌شویی
طبقه‌بندی JEL: G28 ،G21

[۱] رئیس اداره کل مبارزه با پول‌شویی و تأمین مالی تروریسم بانک سپه؛ hojatinia@banksepah.ir

۱ مقدمه

پول یکی از مهم‌ترین ابزارها برای برطرف کردن نیازهای جوامع تا به امروز بوده است زیرا کلیه فعالیت‌های روزمره بشر به وسیله آن صورت می‌گیرد و دارای ویژگی‌های منحصربه‌فردی می‌باشد از آنجایی که امروزه ارز دیجیتال در حال طی کردن پله‌های ترقی می‌باشد به زودی شاهد جایگزین شدن این ارزها به عنوان پول در مبادلات خواهیم بود (سارانی و دیگران ۱۳۹۹).

از زمان ایجاد اینترنت در اوایل دهه ۱۹۸۰، کالاها و معاملات به طور فزاینده‌ای دیجیتالی شده‌اند و تأثیرات آن تقریباً در تمام بخش‌های زندگی بشر از جمله، ارتباطات مراقبت‌های بهداشتی زیرساخت‌ها، انرژی و بخش‌های مالی نفوذ پیدا کرده است. در بخش مالی ارزهای نامشهود و دیجیتال به عنوان جایگزینی برای پول سنتی و ملموس قرار گرفته است (فلتچر[1] و دیگران، ۲۰۲۱، ۲).

به موازات تحولات و پیشرفت‌های اقتصاد جهانی در سده‌های اخیر، جرایم اقتصادی جدیدی نیز به فهرست جرایم افزوده شده‌اند آثار مخرب این جرایم به ویژه بر امنیت اقتصادی و سیاسی نهادهای تقنینی، اجرایی و قضایی را به تأمل و تدبیر راهکارهایی برای مبارزه با این جرایم سوق داده است. پول‌شویی از جمله مهم‌ترین این جرایم است که جامعه بین‌المللی با درک تهدیدهای در پیش رو اقدامات متعددی را برای الزام به مبارزه با این جرایم و پیشگیری از آنها در پیش گرفته است جمهوری اسلامی ایران نیز همگام با جامعه بین‌المللی، ضمن جرم انگاری پدیده پول‌شویی، اقدامات پیشگیرانه و ضمانت اجراهای لازم را وضع کرده است تا از این طریق پاسخی مقتضی به جرایم پول‌شویی داده باشد (طغیانی، ۱۴۰۱، ۴).

بر اساس ماده ۲ قانون مبارزه با پول‌شویی مصوب سال ۱۳۸۶، پول‌شویی فرایند مشروعیت بخشیدن به پول‌های حاصل از فعالیت غیرقانونی است؛ به عبارت دیگر پول‌های به اصطلاح کثیف حاصل از جرایمی مانند قاچاق مواد مخدر، اسلحه انسان و مواردی همچون رشوه، اختلاس فرار مالیاتی و غیره با روش‌های مختلفی تطهیر می‌گردند و هدف از آن پنهان کردن منبع غیرقانونی پول‌ها به نحوی است که بتوان به راحتی و بدون ترس در هر جایی از آنها استفاده کرد.

بر اساس توصیه شماره ۱۵ ـ فناوری‌های جدید گروه ویژه اقدام مالی[2] کشورها ملزم به شناسایی و ارزیابی خطرات پول‌شویی مربوط به توسعه محصولات و شیوه‌های تجاری اخیر از جمله مکانیسم‌های تحویل نوین و استفاده از محصولات جدید می‌باشند (راهنمای گروه ویژه اقدام مالی با رویکرد مبتنی بر ریسک ارزهای مجازی، ۲۰۱۵، ۱۲) کشورهایی مانند ایتالیا (از سال ۲۰۱۷)، فنلاند (از ماه می سال ۲۰۱۹)، ژاپن (از سال ۲۰۱۶)، مکزیک (از ماه مارس سال ۲۰۱۸)، و نروژ (از ۱۵ اکتبر سال ۲۰۱۸) این توصیه را با رویکرد مبتنی بر ریسک در دستور کار قرار داده‌اند (راهنمای به‌روز شده گروه ویژه اقدام مالی با رویکرد مبتنی بر ریسک دارایی‌های مجازی و ارائه‌دهندگان

---

[1] Fletcher

[2] سازمانی بین دولتی است که در سال ۱۹۸۹ با اجلاس گروه ۷ با نگرش به سیاست‌های توسعه برای مبارزه با پول‌شویی تأسیس شده است. دبیرخانه این سازمان مستقر در مقر سازمان همکاری و توسعه اقتصادی در پاریس است. این نهاد ۴۰ توصیه را با هدف ایجاد واکنش هماهنگ جهانی برای جلوگیری از پول‌شویی و تأمین مالی تروریسم منتشر کرده است.

خدمات دارایی‌های مجازی ۸۹/۲۰۲۱). مجدد در سال ۲۰۲۲، گروه ویژه اقدام مالی بر اجرای توصیه شماره ۱۵ تأکید و نحوه ارزیابی آن را توضیح داده است (به‌روزرسانی هدفمند در مورد اجرای استانداردهای گروه ویژه اقدام مالی در دارایی‌های مجازی و ارائه‌دهندگان خدمات دارایی‌های مجازی، ۲۰۲۲، ۹).

بر اساس توصیه شماره ۱۶ ـ نقل‌وانتقال الکترونیکی وجوه ـ قانون انتقال اطلاعات[1] که به عنوان توصیه ۱۶ گروه ویژه اقدام مالی نیز شناخته می‌شود، مجموعه‌ای از دستورالعمل‌هایی است که برای جلوگیری از پول‌شویی و تأمین مالی تروریسم طراحی شده است. این قانون مستلزم آن است که کشورها اطلاعات شناسایی ذینفعان نقل و انتقالات داخلی و برون‌مرزی برای ایجاد یک مسیر حسابرسی مناسب مبارزه با پول‌شویی و تأمین مالی تروریسم جمع‌آوری کنند. براساس ماهیت فرامرزی فعالیت‌های دارایی مجازی و فعالیت‌های ارائه‌دهندگان خدمات دارایی مجازی برای همه نقل‌وانتقالات دارایی‌های مجازی اعمال می‌شود (به‌روزرسانی هدفمند در مورد اجرای استانداردهای گروه ویژه اقدام مالی در دارایی‌های مجازی و ارائه‌دهندگان خدمات دارایی‌های مجازی، ۴/۲۰۲۲). با توجه به اینکه در خصوص مواجهه با مقوله‌های مرتبط با ارزهای دیجیتال و فرایندهای وابسته به آن قوانین و مقررات با رویکرد بازدارندگی از تخلفات به ویژه، پول‌شویی، تأمین مالی تروریسم و ... در کشور وجود ندارد از این رو مجرمان می‌توانند از این خلأ قانونی در راستای انجام اعمال مجرمانه بدون امکان کشف و مجازات بهره‌مند شوند.

لذا پژوهش پیش رو با توجه به این اولویت‌ها و در جهت بررسی زوایای مختلف نحوه انجام مخاطرات شناسایی شده حوزه مبارزه با پول‌شویی و بهره‌مندی از فناوری‌های نوین و هوشمندسازی فرایندهای شناسایی نظارت و اقدام پیشگیرانه با هدف خودکارسازی بررسی‌ها و حذف عامل انسانی در جهت تسریع در فرایند کشف و عدم دخالت نظرات شخصی افراد و بالابردن سطح محرمانگی اطلاعات انجام شده است. در مبانی نظری به بررسی ادبیات موضوع پرداخته‌اند در پیشینه پژوهش به صورت موجز به برخی از پژوهش‌های انجام شده اشاره شده است، سپس جنبه نوآوری پژوهش روش‌شناسی، پژوهش مخاطرات شناسایی شده در حوزه مبارزه با پول‌شویی و تأمین مالی تروریسم جمع‌بندی و نتیجه‌گیری مطرح و در نهایت به پیشنهادهای کاربردی ختم شده است.

۲ مبانی نظری

موضوع ارزهای دیجیتال توسط سیاست‌گذاران و سازمان‌های بین‌المللی مختلف از جمله بانک مرکزی اروپا[2]، صندوق بین‌المللی پول[3]، کمیته پرداخت‌ها و زیرساخت‌های بازار[4]، سازمان بانکداری اروپا[5]، سازمان بازارهای اوراق بهادار اروپا[6] و بانک جهانی[7] مورد بررسی قرار گرفته است که هر کدام به شیوه‌ای متفاوت به این موضوع پرداخته‌اند.

---

[1] Travel Rule

[2] European Central Bank

[3] International Monetary Fund

[4] Committee on Payments and Market Infrastructures

[5] European Banking Authority

[6] European Securities and Markets Authority

[7] World Bank

از آنجایی که گروه ویژه اقدام مالی[1] در حال حاضر اصلی‌ترین نهاد سیاست‌گذار در حوزه مبارزه با پول‌شویی و تأمین مالی تروریسم می‌باشد و در این خصوص استانداردهایی را وضع کرده است. در این پژوهش نیز تعاریف مورد استفاده مطابق با تعاریف ارائه شده از طرف گروه ویژه اقدام مالی است.

دارایی مجازی[2]: دارایی مجازی یک نمایش دیجیتالی از ارزش است که می‌تواند به صورت دیجیتالی معامله شود، یا منتقل شود و می‌تواند برای اهداف پرداخت یا سرمایه‌گذاری استفاده شود دارایی‌های مجازی شامل نمایش دیجیتالی ارزهای، فیات اوراق بهادار و سایر دارایی‌های مالی نمی‌شود (گزارش گروه ویژه اقدام مالی، بررسی ۱۲ ماهه استانداردهای بازنگری شده گروه ویژه اقدام مالی در مورد دارایی‌های مجازی و ارائه‌دهندگان خدمات دارایی مجازی، ۲۰۲۰، ۲۵).

ارائه‌دهنده خدمات دارایی مجازی[3]: به معنای هر شخص حقیقی یا حقوقی است که به عنوان یک کسب‌وکار یک یا چند مورد از فعالیت‌ها یا عملیات زیر را برای یا از طرف شخص حقیقی یا حقوقی دیگری انجام می‌دهد.

- مبادله بین دارایی‌های مجازی و ارزهای فیات؛
- مبادله بین یک یا چند نوع دارایی مجازی؛
- انتقال دارایی‌های مجازی؛
- حفاظت و یا مدیریت دارایی‌های مجازی یا ابزارهایی که امکان کنترل بر دارایی‌های مجازی را فراهم می‌کند؛ و
- مشارکت و ارائه خدمات مالی مربوط به پیشنهاد ناشر و یا فروش یک دارایی مجازی گزارش گروه ویژه اقدام مالی، (بررسی ۱۲ ماهه استانداردهای بازنگری شده گروه ویژه اقدام مالی در مورد دارایی‌های مجازی و ارائه‌دهندگان خدمات دارایی مجازی، ۲۰۲۰، ۲۵).

شایان ذکر است در چند سال گذشته موضوع دارایی مجازی و استفاده از قابلیت‌های آن مورد استقبال و استفاده افراد زیادی قرار گرفته است و شرکت‌هایی نیز نسبت به ارائه بستر مورد نیاز در خصوص انجام فرایندهای خرید، فروش انتقال و ... شروع به فعالیت نموده‌اند.

ارز دیجیتال[4]: می‌تواند به معنای نمایش دیجیتال ارز مجازی (غیر فیات) یا پول الکترونیکی (فیات) باشد و بنابراین اغلب به جای واژه «ارز مجازی» استفاده می‌شود (گزارش گروه ویژه اقدام مالی ارزهای مجازی، تعاریف کلیدی و خطرات بالقوه مبارزه با پول‌شویی و تأمین مالی تروریسم، ۲۰۱۴، ۴).

---

[1] Financial Action Task Force (FATF)

[2] Virtual Asset

[3] Virtual Asset Service Provider (VASP)

[4] Digital Currency

ارز فیات[1]: (معروف به «ارز واقعی[2]»، «پول واقعی[3]» یا «پول ملی[4]») متمایز می‌شود که سکه و پول کاغذی کشوری است که به عنوان ارز قانونی آن تعیین شده است گردش می‌کند؛ و معمولاً به عنوان وسیله مبادله در کشور صادرکننده استفاده و پذیرفته می‌شود (گزارش گروه ویژه اقدام، مالی ارزهای مجازی تعاریف کلیدی و خطرات بالقوه مبارزه با پول‌شویی و تأمین مالی تروریسم، ۲۰۱۴، ۴).

ارز مجازی قابل‌تبدیل[5] (باز): دارای ارزشی معادل با ارز واقعی است و می‌توان آن را به صورت رفت‌وبرگشت با ارز واقعی مبادله کرد (گزارش گروه ویژه اقدام، مالی ارزهای مجازی تعاریف کلیدی و خطرات بالقوه مبارزه با پول‌شویی و تأمین مالی تروریسم، ۲۰۱۴، ۴)

ارز مجازی غیرقابل‌تبدیل[6] (بسته): برای اختصاص به یک دامنه یا دنیای مجازی خاص، مانند یک بازی نقش‌آفرینی آنلاین انبوه چند نفره در نظر گرفته شده است و طبق قوانین حاکم بر استفاده از آن نمی‌توان با ارز فیات مبادله می‌شود گزارش (گروه ویژه اقدام، مالی ارزهای مجازی تعاریف کلیدی و خطرات بالقوه مبارزه با پول‌شویی و تأمین مالی تروریسم، ۲۰۱۴، ۴).

ارزهای مجازی متمرکز[7]: همه ارزهای مجازی غیرقابل‌تبدیل متمرکز هستند طبق تعریف، آنها توسط یک مرجع مرکزی صادر می‌شوند که قوانینی را ایجاد می‌کند که آنها را غیرقابل‌تبدیل می‌کند (گزارش گروه ویژه اقدام مالی، ارزهای مجازی، تعاریف کلیدی و خطرات بالقوه مبارزه با پول‌شویی و تأمین مالی تروریسم، ۲۰۱۴، ۵).

ارزهای مجازی غیرمتمرکز[8]: ارزهای مجازی قابل‌تبدیل ممکن است یکی از دو نوع فرعی متمرکز یا غیرمتمرکز باشند. ارزهای مجازی غیرمتمرکز (معروف به ارزهای رمزنگاری‌شده)[9] ارزهای مجازی همتا به همتای توزیع شده، منبع باز و مبتنی بر ریاضی هستند که هیچ اختیار مدیریت و نظارت مرکزی ندارند (گزارش گروه ویژه اقدام مالی، ارزهای مجازی، تعاریف کلیدی و خطرات بالقوه مبارزه با پول‌شویی و تأمین مالی تروریسم، ۲۰۱۴، ۵).

ارزهای رمزنگاری‌شده: به یک ارز مجازی غیرمتمرکز مبدل مبتنی بر ریاضی اطلاق می‌شود که توسط رمزنگاری محافظت می‌شود این ارز دیجیتال از دو عبارت به معنای رمزارز تشکیل شده است (گزارش گروه ویژه اقدام مالی، ارزهای مجازی، تعاریف کلیدی و خطرات بالقوه مبارزه با پول‌شویی و تأمین مالی تروریسم، ۲۰۱۴، ۵).

---

[1] Fiat Currency
[2] Real Currency
[3] Real Money
[4] National Currency
[5] Convertible (or open) Virtual Currency
[6] Non-convertible (or closed) Virtual Currency
[7] Centralized Virtual Currencies
[8] Decentralized Virtual Currencies
[9] Cryptocurrency

بیت‌کوین: بیت‌کوین که در سال ۲۰۰۹ راه‌اندازی شد اولین ارز مجازی غیرمتمرکز قابل‌تبدیل و اولین ارز دیجیتال و رهبر فعلی بازار ارزهای دیجیتال است (مسلمی، ۱۳۹۷).

نکته قابل‌توجه این است که همچنان پس از گذشت سال‌ها از حضور این رمزارز پیشرو در حوزه رمزنگاری، هویت مبتکر و مبدع آن در هاله‌ای از ابهام قرار دارد.

مبادله گر[1]: (که گاهی اوقات صرافی ارز مجازی نیز نامیده می‌شود) شخص یا نهادی است که به عنوان یک تجارت مشغول مبادله ارز مجازی با ارز، واقعی وجوه یا سایر اشکال ارز مجازی و همچنین فلزات گران‌بها و بالعکس، در ازای پرداخت هزینه (کمیسیون) است (گزارش گروه ویژه اقدام مالی ارزهای مجازی، تعاریف کلیدی و خطرات بالقوه مبارزه با پول‌شویی و تأمین مالی تروریسم، ۲۰۱۴، ۷).

کاربر[2]: شخص/ نهادی است که ارز مجازی را به دست می‌آورد و از آن برای خرید کالاها یا خدمات واقعی یا مجازی یا ارسال نقل‌وانتقالات به صورت شخصی به شخص دیگری (برای استفاده شخصی) استفاده می‌کند، یا اینکه ارز مجازی را به عنوان یک سرمایه‌گذاری (شخصی) در اختیار دارد (گزارش گروه ویژه اقدام مالی، ارزهای مجازی، تعاریف کلیدی و خطرات بالقوه مبارزه با پول‌شویی و تأمین مالی تروریسم، ۲۰۱۴، ۷).

کیف پول ارز مجازی[3]: وسیله‌ای سخت‌افزاری یا محلی نرم‌افزاری برای نگهداری، ذخیره و انتقال بیت کوین یا سایر ارزهای مجازی است. کیف پول‌ها در انواع دسکتاپ، آنلاین، آفلاین، موبایل، سخت‌افزاری و کاغذی وجود دارند (گزارش گروه ویژه اقدام مالی ارزهای مجازی تعاریف کلیدی و خطرات بالقوه مبارزه با پول‌شویی و تأمین مالی تروریسم، ۲۰۱۴/۷)

زنجیره بلوک یا بلاک چین: فهرست یا پایگاه داده‌ای عمومی از همه تراکنش‌هایی است که تاکنون انجام پذیرفته‌اند و فرستاده شده‌اند با این فهرست هر کسی می‌تواند بداند که کدام بیت کوین از چه کسی است (صیاد معروف و همکاران،۱۳۹۴).

شاخص اعلان قرمز (پرچم قرمز)[4]: مفهوم اعلان قرمز ابزار مفیدی جهت استفاده مؤسسات مالی برای انجام فعالیت‌های مبارزه با پول‌شویی و تأمین مالی تروریسم است. این مفهوم برای شناسایی، گزارش فعالیت‌های مشکوک، شناسایی هرگونه معامله، فعالیت یا رفتار مشتری و مرتبط کردن آن با سطح معینی از ریسک استفاده می‌شود؛ این ابزار شناسایی و گزارش فعالیت مشکوک را برای مؤسسات مالی آسان‌تر می‌کند (گزارش گروه ویژه اقدام مالی، شاخص‌های اعلان قرمز برای مبارزه با پول‌شویی و تأمین مالی تروریسم، سپتامبر ۲۰۲۰، ۵).

توانمندسازی بانک‌ها و مؤسسات مالی در استفاده از ابزارهای هوشمند نظیر شاخص یاد شده در راستای نظارت مؤثر و مستمر بر مراودات مالی افراد/نهادها؛ شناسایی موارد محتمل عدم انطباق با قوانین و مقررات مبارزه با پول‌شویی و تأمین مالی تروریسم تأثیر به سزایی خواهد داشت.

---

[1] Exchanger

[2] User

[3] Virtual Currency Wallet

[4] Red Flag Indicators

۱.۲ پیشینه پژوهش

در ادامه به شرحی کوتاه از برخی پژوهش‌های انجام شده در این زمینه اشاره می‌شود.

مافی و رامشی (۱۴۰۱) در پژوهشی با عنوان ماهیت حقوقی دارایی‌های مجازی به بررسی رویکردها به پذیرش دارایی‌های مجازی پرداخته‌اند. چنین اظهار داشتند: در نظام حقوقی ایران به دارایی مجازی توجه نشده است.

قربانی و موسوی (۱۴۰۰) در پژوهشی با عنوان تأثیر رمزارز، بیت کوین و ارز دیجیتال در مراودات مالی کسب‌وکارهای امروز به بررسی، تعاریف مزایا و معایب بیت کوین و همچنین جایگاه و تأثیر آن در مراودات مالی پرداخته‌اند.

شاملو و خلیلی پاجی (۱۳۹۹) در پژوهشی با عنوان سیاست‌گذاری جنایی ریسک مدار در برابر فناوری ارزهای مجازی، با روش توصیفی — تحلیلی به مطالعه رویکردهای سیاست‌گذاری برخی کشورهای پیشرو پیرامون ارزهای مجازی پرداخته‌اند.

پادارین[1] (۲۰۲۲) در پژوهشی با عنوان چالش‌ها و فرصت‌های قانون‌گذاری دارایی مجازی در جزایر ویریجین بریتانیا، اظهار داشتند جزایر ویرجین بریتانیا چارچوب نظارتی خاصی برای دارایی‌های مجازی یا ارزهای دیجیتال ندارد اگرچه انتظار می‌رود که این حوزه قضایی به مرور زمان همانند سایر حوزه‌های قضایی، چارچوب نظارتی ویژه‌ای برای دارایی‌های مجازی ایجاد کند.

کود[2] (۲۰۲۰) در پژوهشی با عنوان پدیده دارایی‌های مجازی جنبه‌های اقتصادی و حقوقی از روش‌های نظری تحلیل و ترکیب، مقایسه، تعمیم، نظام‌مندسازی و تفسیر نتایج استفاده نموده است؛ همچنین طبقه‌بندی از دارایی مجازی معرفی و اظهار داشتند («ارائه‌دهندگان خدمات» و «کاربران خدمات») با یکدیگر ارتباط تعامل دارند.

کوربل[3] و دیگران (۲۰۱۹) در پژوهشی با عنوان نقش دارایی مجازی در توزیع کالاها و محصولات، اشاره داشتند انتشار فناوری واقعیت مجازی و واقعیت افزوده منجر به افزایش ارتباط دارایی‌های مجازی برای شرکت‌های سازنده و خرده‌فروشی به عنوان پایه و مرکز خرید می‌شود برای ارائه نمای کلی از نقشی که اشیای مجازی در توزیع کالاها و محصولات ایفا می‌کنند این مطالعه با هدف تمایز و طبقه‌بندی رخدادها و وابستگی‌های مختلف اشیاء مجازی در حوزه بازار و تحلیل هم‌افزایی و امکان‌های همکاری بین هر دو صنعت انجام شد. در نتیجه، نه نوع، دارایی کالا و محصول مختلف شناسایی و توصیف گردیدند. یافته‌ها حاکی از آن است که فرصت‌های تجاری مورد استفاده قرار نمی‌گیرند در حالی که دارایی‌های مجازی را می‌توان به عنوان محور همکاری بین صنعتی در نظر گرفت.

۲.۲ جنبه نوآوری پژوهش

در مقایسه این پژوهش با پژوهش‌های انجام شده، باید اذعان کرد که پژوهش حاضر با نگاهی تخصصی از گزارش‌هایی استفاده شده است که مبتنی بر تجزیه‌وتحلیل اطلاعات بلاک چین است بر مخاطرات حوزه پول‌شویی

---

[1] Padarin

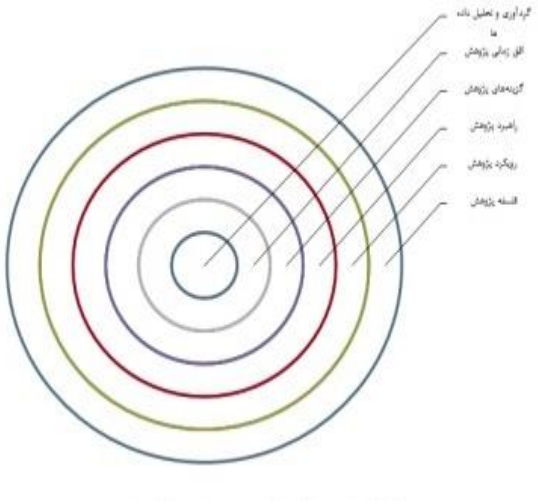
[2] Kud

[3] Korbel

با تمرکز بر تقلیل این خطرات به وسیله هوشمندسازی تأکید دارد. در حالی‌که به نظر می‌رسد سایر پژوهش‌ها از توجه به این مورد غافل مانده‌اند با توجه به اینکه موضوع بررسی رمزارزها از منظر مخاطرات پول‌شویی در ایران، به طور جامع تبیین نشده و با توجه به خلأ تحقیقاتی به نظر می‌رسد نتایج حاصل از این پژوهش می‌تواند خلأ موجود در این حوزه تخصصی در کشور را اندکی جبران کند.

۳.۲ روش‌شناسی پژوهش

روش پژوهش بر اساس مدل پیاز پژوهش ساندرز[1] (۲۰۰۹، ۱۳۸) می‌باشد.



شکل ۱ . مدل پیاز پژوهش ساندرز

مأخذ: ساندرز، ۲۰۰۹، ۱۳۸

بر اساس این مدل یک پژوهش از لایه‌های مختلفی تشکیل می‌شود که در آن هر لایه متأثر از لایه بالاتر است. آن‌ها عبارت‌اند از:

- لایه فلسفه‌های پژوهش: در این لایه حوزه پارادایم پژوهش مطرح می‌شود با توجه به اینکه در این پژوهش هدف شناسایی و کاهش مخاطرات حوزه مبارزه با پول‌شویی در مبادلات رمزارزها با بهره‌مندی از فناوری‌های نوین و هوشمندسازی است در نتیجه پژوهش حاضر با پارادایم تفسیرگرایی انجام شده است.
- لایه رویکردهای پژوهش: از آنجایی که نظریه‌های علمی باید به صورت تجربی نیز آزمایش پذیر باشند در این لایه قیاسی با استقرایی بودن پژوهش باید مشخص شود. با توجه به اینکه رویکرد استقرایی از یک نمونه خاص به بیانی عمومی می‌رسد لذا رویکرد این پژوهش استقرایی است.
- لایه راهبردهای پژوهش این پژوهش در دسته پژوهش‌های کاربردی قرار دارد و به صورت توصیفی انجام شده است.

---

[1] Saunders

- لایه گزینه‌های پژوهش پژوهش‌ها از جهت کمیت‌پذیری و کمیت‌ناپذیری به دو دسته پژوهش‌های کمی و کیفی تقسیم می‌شوند پژوهش کیفی پژوهشی است که یافته‌هایی تولید می‌کند که با توسل به عملیات آماری یا سایر روش‌های شمارشی حاصل نیامده است (استراوس و کربین[1]، ۱۳۹۴) پژوهش حاضر در دسته پژوهش کیفی قرار دارد.
- لایه افق زمانی پژوهش: به این دلیل که داده‌های مربوط تنها یک مرتبه گردآوری شده است، لذا در این پژوهش افق مقطعی است.
- لایه شیوه گردآوری داده‌ها: شیوه گردآوری داده در این پژوهش مطالعات کتابخانه‌ای است. لازم به ذکر است در این پژوهش از نمونه‌گیری هدفمند به دلیل تازگی و پیچیدگی مفهوم رمزارز استفاده شده است. از آنجایی که هدف، فهم عمیق پدیده مورد بررسی و کشف نظرات است؛ ملاک انتخاب نمونه مورد بررسی را تسلط و دسترسی به داده‌های مربوط به حوزه رمزارز قرار دادیم؛ سایفر تریس[2] جزو اولین تیم‌های بررسی تخصصی بلاک چین و یکی از اعضای اتاق تجارت دیجیتال و تیم این مجموعه شامل مدیران ارشد ارزهای دیجیتال، پرداخت، امنیت و همچنین مهندسان و محققان داده، در سطح جهانی است. چین الیسیس[3] اولین شرکت استارت آپی است که به تجارت ردیابی بیت کوین اختصاص یافته و نرم‌افزار اختصاصی تحقیق جرایم مالی را توسعه داده است. الیپتیک[4] سال ۲۰۱۳ تأسیس شد و پیشگام استفاده از تجزیه‌وتحلیل بلاک چین برای انطباق با جرایم مالی و ارائه‌دهنده پیشرو راه‌حل‌های انطباق رمزنگاری در سطح جهان هست، لذا به بررسی گزارش‌های تهیه شده توسط گروه ویژه اقدام مالی، سایفر تریس، چین الیسیس و الیپتیک در راستای شناسایی مخاطرات پول‌شویی حوزه رمزارزها به شرح جدول ذیل پرداخته‌اند.

---

[1] Strauss, Corbin

[2] CipherTrace

[3] Chainalysis

[4] ELLIPTIC

جدول ۱

گزارش‌های استفاده شده

نام سازمان	عنوان گزارش	سال تهیه گزارش
گروه ویژه اقدام مالی	ارزهای مجازی، تعاریف کلیدی و خطرات بالقوه مبارزه با پولشویی و تأمین مالی تروریسم	ژوئن ۲۰۱۴
	شاخص‌های اعلان قرمز برای مبارزه با پولشویی و تأمین مالی تروریسم	سپتامبر ۲۰۲۰
	راهنمای به‌روز شده گروه ویژه اقدام مالی با رویکرد مبتنی بر ریسک دارایی‌های مجازی و ارائه‌دهندگان خدمات دارایی‌های مجازی	اکتبر ۲۰۲۱
	به‌روزرسانی هدفمند در مورد اجرای استانداردهای گروه ویژه اقدام مالی در دارایی‌های مجازی و ارائه‌دهندگان خدمات دارایی‌های مجازی	ژوئن ۲۰۲۲
	پولشویی از طریق فنتانیل و مواد مخدر صنعتی	نوامبر ۲۰۲۲
	مقابله با تأمین مالی باج افزار	مارس ۲۰۲۳
سایفر تریس	جرایم ارزهای دیجیتال و مبارزه با پولشویی	آگوست ۲۰۲۱
	جنایات ارزهای دیجیتال و مبارزه با پولشویی	مارس ۲۰۲۳
چین‌الیسیس	جنایات رمزنگاری ۲۰۲۲	فوریه ۲۰۲۲
	جنایات رمزنگاری ۲۰۲۳، هر آنچه باید در مورد جرم و جنایت مبتنی بر ارزهای دیجیتال بدانید	فوریه ۲۰۲۳
الیپتیک	جلوگیری از جرایم مالی در دارایی‌های رمزنگاری شده، با استفاده از تحلیل بلاک چین برای کاهش ریسک	۲۰۲۳
	کریپتو و تجارت جهانی فنتانیل	۲۰۲۳
	چشم‌انداز نظارتی الیپتیک، سیاست رمزگذاری و مقررات گسترش به مرزهای دیجیتال جدید مشاهده خواهد شد	۲۰۲۳
	انطباق با تحریم‌ها در ارزهای دیجیتال. استفاده از تجزیه‌وتحلیل بلاک چین برای کاهش ریسک	۲۰۲۳

در این پژوهش به پشتوانه ادبیات نظری مورد بررسی در حوزه دارایی‌های مجازی (رمزارزها)، مبارزه با پول‌شویی و تأمین مالی تروریسم و با تأکید بر داده‌های به دست آمده از بررسی گزارش‌های یاد شده در جدول بالا؛ مخاطرات به شرح زیر شناسایی شده‌اند.

۴.۲ مخاطرات شناسایی شده حوزه مبارزه با پول‌شویی و تأمین مالی تروریسم

۱.۴.۲ باج افزار[1]

استفاده تقریباً انحصاری از دارایی‌های مجازی در پول‌شویی مربوط به باج افزار اهمیت تسریع در اجرای توصیه ۱۵ گروه ویژه اقدام مالی را تقویت می‌کند که از مراجع قضایی می‌خواهد اقداماتی را برای کاهش خطرات مرتبط با دارایی‌های مجازی و تنظیم بخش ارائه‌دهنده خدمات دارایی مجازی انجام دهند این تلاش‌ها برای جلوگیری از آسان مجرمان به ارائه‌دهندگان خدمات دارایی‌های مجازی مستقر در حوزه‌های قضایی با کنترل‌های ضعیف یا غیرقابل

[1] Ransomware

وجود مبارزه با پول‌شویی و تأمین مالی تروریسم برای شست و شوی سود حاصل از جرایم بسیار مهم است (گزارش گروه ویژه اقدام، مالی مقابله با تأمین مالی باج افزار، مارس ۲۰۲۳، ۵).

باج افزار نوعی نرم‌افزار مخرب (بدافزار) است که مجرمان برای ممانعت از دسترسی به داده‌ها، سیستم‌ها یا شبکه‌ها در ازای تقاضای باج توسعه داده یا استفاده می‌کنند؛ روش‌های رایج حمله شامل رمزگذاری داده‌ها، داده‌ها استخراج داده و اختلال در عملیات شخص قربانی است. حملات اغلب شامل بیش از یک روش است و ممکن است تهدیدی برای انتشار داده‌های قربانی، باشد قربانیان یا اشخاص ثالث مرتبط با قربانیان، اغلب از ارائه‌دهندگان خدمات دارایی مجازی برای پرداخت باج استفاده می‌کنند (گزارش گروه ویژه اقدام مالی، مقابله با تأمین مالی باج افزار، مارس ۲۰۲۳، ۸). مجرمان باج افزار همچنین از ارائه‌دهندگان خدمات دارایی مجازی برای تطهیر وجوه غیرقانونی و مبادله عواید با ارز فیات استفاده می‌کنند که می‌تواند راحت‌تر با کالاها و خدمات مبادله شود و ذخیره ارزش پایدارتری دارد. از سال ۲۰۱۸ گروه ویژه اقدام مالی دستورالعمل‌های مختلفی را برای کمک به حوزه‌های قضایی و بخش خصوصی برای نظارت و کاهش خطرات از جمله شاخص‌های اعلان قرمز پول‌شویی و تأمین مالی تروریسم در این بخش صادر کرده است (گزارش گروه ویژه اقدام مالی، مقابله با تأمین مالی باج افزار، مارس ۹، ۲۰۲۳).

اگرچه تاکنون تلاش‌هایی برای شناسایی و جلوگیری از فعالیت نرم‌افزارها ربات‌ها یا کدهای دستوری مخرب در برنامه‌های کاربردی یا شبکه‌های وب داخلی و بین‌المللی صورت پذیرفته است اما در بیشتر موارد عملکرد موفقی از آنها مشاهده نشده است به عنوان مثال افزونه کد کپچا[1] که برای جلوگیری از تکرار یک فرایند توسط ربات‌ها طراحی گردیده ولی از نقاط ضعفی نیز برخوردار است.

۲.۴.۲ صرافی ارز مجازی

در مبانی نظری به تعریف ارائه‌دهنده خدمات دارایی مجازی صرافی ارز مجازی اشاره گردید، در این بخش به مواردی از قبیل ریسک ذاتی صرافی ارز مجازی آسیب‌پذیری‌های کلیدی و عوامل پرخطر و خطرات خاص صرافی ارز مجازی پرداخته‌اند. صرافی ارز مجازی به دلیل دسترسی آسان و گستردگی جغرافیایی گسترده از ریسک ذاتی بالایی برخوردار است. آسیب‌پذیری‌های کلیدی و عوامل پرخطر شامل فناوری پرداخت جدید، ناشناس بودن و پیچیدگی عدم آگاهی از پول‌شویی و تأمین مالی تروریسم پرداخت‌های بین‌المللی مشتریان/ حوزه قضایی با ریسک بالا و افراد در معرض ریسک سیاسی می‌باشد.

۳.۴.۲ دارک نت[2]

دارک‌نت اغلب با دیپ‌وب[3] اشتباه گرفته می‌شود — دیپ‌وب بخشی از وب است که توسط موتورهای جستجو نمایه نمی‌شود و بنابراین قابل جستجو نیست دارکنت زیر بخش کوچکتری از دیپ‌وب است که برای میزبانی و بازدید از صفحات وب در آن به نرم‌افزار خاصی نیاز دارد (کوین مارکت).

---

[1] Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)

[2] Dark net

[3] Deep web

دارک مارکت[1] شامل آدرس‌های رمزنگاری مرتبط با افراد و سازمان‌هایی است که انسان‌ها، اسلحه‌های غیرقانونی، ارزهای تقلبی اسناد جعلی، داروهای مخدرغیرقانونی و روان‌گردان‌ها، داروهای غیرمجاز یا استروئیدها و تقلبی را می‌فروشند یا قاچاق می‌کنند (گزارش سایفر، تریس جنایات ارزهای دیجیتال و مبارزه با پول‌شویی مارس ۱۴/۲۰۲۳).

حجم قابل‌توجهی از معاملات مجرمانه مربوط به ارزهای رمزنگاری‌شده به دلیل ماهیت ناشناس، دیجیتالی و بدون مجوزشان، در دارکنت انجام می‌شود بازارهای جنایی انجمن‌ها فروشگاه‌ها وبلاگ‌های باج‌افزار و غیره معمولاً در دارکنت میزبانی می‌شوند. مهم‌ترین شبکه دارکنت (مسیریابی پیاز[2]) که دسترسی ناشناس را فراهم می‌کند و دیگری (پروژه اینترنت نامرئی[3]) که امکان میزبانی ناشناس وب‌سایت‌ها را فراهم می‌کند، هستند (گزارش سایفر تریس، جنایات ارزهای دیجیتال و مبارزه با پول‌شویی مارس ۲۰۲۳، ۱۴).

چهار بازار پردرآمد دارکنت در سال ۲۰۲۲ بازارهای دارکنت متمرکز بر مواد مخدر بودند، در حالی که تنها، برایان دامپس[4] یک فروشگاه کلاهبرداری[5] بود (گزارش چین‌الیسیس جنایات رمزنگاری ۲۰۲۳ ـ هر آنچه باید در مورد جرم و جنایت مبتنی بر ارزهای دیجیتال بدانید ـ فوریه ۲۰۲۳، ۷۱).

۴.۴.۲ جرایم مالی غیرمتمرکز

جرایم مالی غیرمتمرکز[6] را می‌توان به طور کلی به دو دسته تقسیم کرد هک یک پروتکل مالی غیرمتمرکز توسط عوامل خارجی یا یک راگ پول[7] که توسط افراد داخلی انجام می‌شود. راگ پول یک کلاهبرداری است که در آن یک توسعه‌دهنده ارز دیجیتال پروژه‌ای را برای جذب پول سرمایه‌گذار تبلیغ می‌کند اما به طور ناگهانی تعطیل یا ناپدید می‌شود و دارایی‌های سرمایه‌گذار را با خود می‌برد. یکی دیگر از روندهای رایج موجود در تجزیه‌وتحلیل هک‌های مالی غیرمتمرکز، استفاده از وام‌های فلش است که در اکثر حملات پروتکل مالی غیرمتمرکز استفاده شده است. از آنجایی که وام‌های فلش نیازی به وثیقه یا شناسایی مشتری ندارند دستگیر کردن بازیگران بدی که از آنها برای تأمین مالی حملات خود استفاده می‌کنند، دشوارتر می‌شود با این حال اصل مشکل در پلتفرم‌هایی نیست که وام‌های فلش[8] را ارائه می‌دهند، بلکه در قراردادهای هوشمند حسابرسی نشده‌ای است که وام‌ها به آنها ارسال می‌شوند و بعداً مورد بهره‌برداری قرار می‌گیرند (گزارش سایفر تریس، جرایم ارزهای دیجیتال و مبارزه با پول‌شویی، آگوست ۲۰۲۱، ۱۰).

---

[1] Dark Market

[2] Tor (The Onion Routing)

[3] 12P (The Invisible Internet Project)

[4] Brian Dumps

[5] Fraud Shop

[6] DeFi (Decentralized Finance)

[7] rug pull

[8] وام فلش نوعی وام بدون وثیقه است که به کاربر اجازه می‌دهد تا زمانی که دارایی‌های وام گرفته شده در همان تراکنش بلاک چین بازپرداخت شود دارایی‌هایی را بدون وثیقه اولیه قرض کند.

۵.۴.۲ پل

پل‌های زنجیره‌ای متقاطع یا به طور ساده پل‌ها خدمات یا قراردادهایی هستند که دو بلاک چین متفاوت از لحاظ اقتصادی و فناوری را به هم متصل می‌کنند و به کاربران امکان می‌دهند تا ارزش را به توکن‌ها مبادله کنند و سپس آن ارزش را به زنجیره‌ای دیگر منتقل کنند. پل‌ها عمدتاً توسط سرمایه‌گذاران رمزنگاری استفاده می‌شوند که می‌خواهند دارایی‌های دیجیتال را از یک زنجیره بگیرند و آن دارایی‌ها را در بلاک چین دیگری خرج، مبادله یا سرمایه‌گذاری کنند. با این حال مانند هر فناوری جدید پل‌ها اغلب مورد سوءاستفاده مجرمان قرار می‌گیرند تا منشأ ارزهای دیجیتال به سرقت رفته را پنهان کنند و از مسدود شدن یا ردیابی وجوه آنها جلوگیری کنند. این سوءاستفاده‌ها می‌توانند به اشکال مختلفی از جمله دستکاری کد قرارداد، هوشمند سرقت دارایی‌های دیجیتال یا تغییر داده‌های تراکنش‌ها، رخ دهند (گزارش سایفر تریس، جنایات ارزهای دیجیتال و مبارزه با پول‌شویی، مارس ۲۰۲۳، ۹ و ۱۰).

قبل از ظهور، پل‌ها کاربران رمزارز نمی‌توانستند به راحتی در میان بلاک‌چین‌ها حرکت کنند تا به خدمات مالی غیرمتمرکز دسترسی داشته باشند؛ اما با پل‌ها خدمات مالی غیرمتمرکز می‌توانند به عنوان بخشی از یک اکوسیستم زنجیره‌ای متقابل در هم تنیده رشد کنند (گزارش الیپتیک، انطباق با تحریم‌ها در ارزهای دیجیتال. استفاده از تجزیه‌وتحلیل بلاک چین برای کاهش ریسک ۸/۲۰۲۳).

گروه ویژه اقدام مالی هشدار داد که استفاده روزافزون از پل‌های زنجیره‌ای متقاطع، مجرمان را قادر می‌سازد تا در فرآیند پول‌شویی پرش زنجیره‌ای[1] انجام دهند (گزارش چشم‌انداز نظارتی، الیپتیک، سیاست رمزگذاری و مقررات گسترش به مرزهای دیجیتال جدید مشاهده خواهد شد ۸/۲۰۲۳). پرش زنجیره‌ای به عنوان راهی برای پنهان کردن جریان وجوه با جابجایی بین بلاک‌چین‌ها است، برای نمونه شامل استفاده از حساب‌های متعدد در چندین صرافی دارایی‌های رمزنگاری شده برای مبادله وجوه با چندین دارایی رمزنگاری می‌شود (گزارش الیپتیک، جلوگیری از جرایم مالی در دارایی‌های رمزنگاری شده با استفاده از تحلیل بلاک چین برای کاهش ریسک، ۲۰۲۳، ۵۷ و ۶۰).

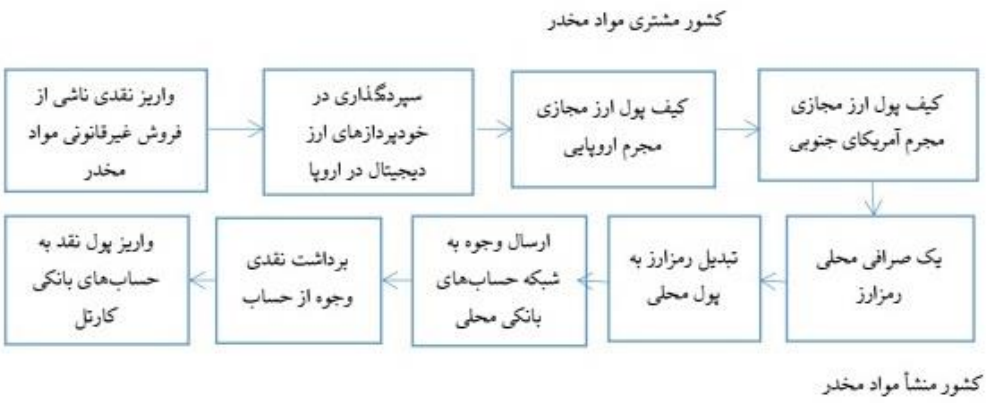
۶.۴.۲ دستگاه‌های خودپرداز رمزارز

دستگاه‌های خودپرداز دارایی رمزنگاری نقش مهمی در اکوسیستم دارایی دیجیتال ایفا کرده‌اند. آنها یک روش قابل‌اعتماد برای انتقال سریع دارایی‌های دیجیتال به فیات ارائه می‌دهند یا بالعکس دستگاه‌های خودپرداز رمزنگاری یک راه مفید برای انتقال پول نقد از یک همتای خود به یک کیف پول به شخص دیگری که در جای دیگری قرار دارد ارائه می‌دهد طرفداران آن‌ها را نقش مهمی در پیشبرد شمول مالی و پذیرش گسترده‌تر دارایی‌های رمزنگاری می‌دانند. متأسفانه، برخی از ارائه‌دهندگان دستگاه‌های خودپرداز رمزنگاری عمداً از رعایت مقررات اجتناب کرده و در برخی موارد این خدمات ناسازگار با قوانین و مقررات ممکن است از فعالیت غیرقانونی کاربران خود آگاه باشند یا حتی در آن شریک باشند.

[1] chain hopping

در دسترس بودن این سرویس‌های غیر منطبق که کاربران می‌توانند بدون کنترل‌های مبارزه با پول‌شویی و تأمین مالی تروریسم، پول نقد را با رمزارز مبادله کنند منجر به سوءاستفاده شبکه‌های مجرمانه سازمان یافته از این خدمات برای اهدافی مانند قاچاق مواد مخدر شده است حالت‌های زیر ممکن است اتفاق بیفتد:

- اعضای یک شبکه مجرمانه حجم زیادی از پول نقد غیرقانونی به دست آمده از فروش مواد مخدر را به دستگاه‌های خودپرداز دارایی‌های رمزنگاری شده واریز می‌کنند.
- وجوه فیات به دارایی‌های رمزنگاری شده تبدیل می‌شود و به کیف پول‌های متعلق به سایر اعضای همان شبکه جنایی منتقل می‌شود.
- اعضای شبکه به عنوان دریافت‌کننده نهایی نقل‌وانتقالات وجوه را در یک صرافی، نقد، یا وجوه را به صورت نقدی در سایر دستگاه‌های خودپرداز دارایی رمزنگاری برداشت می‌کنند.
- وجوه فیات بیشتر از طریق سپرده‌های نقدی در بانک‌ها و سایر مؤسسات مالی تطهیر می‌شوند (گزارش الیپتیک، جلوگیری از جرایم مالی در دارایی‌های رمزنگاری شده با استفاده از تحلیل بلاک‌چین برای کاهش ریسک، ۶۸/۲۰۲۳ و ۶۹).



شکل ۲ . تلاش مجرمان برای تطهیر وجوه از طریق خودپردازهای دارایی‌های رمزنگاری شده

مأخذ. (گزارش الیپتیک جلوگیری از جرایم مالی در دارایی‌های رمزنگاری شده، با استفاده از تحلیل بلاک چین برای کاهش ریسک، ۷۱/۲۰۲۳).

۷.۴.۲ غیرمستقیم در معرض قرار گرفتن از طریق روابط کارگزاری بانکی

بانک‌ها همچنین می‌توانند از طریق روابط کارگزاری خود با ریسک‌های مرتبط با دارایی‌های رمزنگاری شده به طور غیرمستقیم مواجه شوند هنگامی که یک بانک تسویه ارز را تسهیل می‌کند یا خدمات دیگری را از طرف مؤسسات مالی طرف مقابل ارائه می‌دهد ممکن است در معرض خطراتی قرار گیرد که آن مؤسسات مالی با ارائه‌دهندگان خدمات دارایی مجازی یا سایر مشاغل دارایی رمزنگاری شده ارتباط برقرار می‌کنند. حالت‌های زیر متصور است:

بانک A ـ که در ایالات‌متحده مستقر است ـ درخواستی از بانک B در اروپا برای تسهیل انتقال دلار آمریکا به بانک C در آسیا دریافت می‌کند.

جزئیات پرداخت درج شده در پیام پرداخت نشان می‌دهد که مشتری بانک B، یک صرافی دارایی مجازی کوچک است[۱].

تکرار تراکنش‌های پردازش شده از طریق یک حساب کارگزاری به نفع یک ارائه‌دهنده خدمات دارایی مجازی یا سایر کسب‌وکارهای دارایی‌های دیجیتال؛

تراکنش‌هایی که شامل ارائه‌دهندگان خدمات دارایی‌های مجازی یا سایر کسب‌وکارهای دارایی‌های رمزنگاری با ویژگی‌های پرخطر هستند، مانند ثبت‌نام در حوزه‌های قضایی پرخطر و فقدان فرایند و کنترل شناسایی مشتری. ارائه‌دهندگان خدمات دارایی‌های مجازی یا سایر کسب‌وکارهای دارایی‌های دیجیتالی که در تراکنش‌ها نشان داده می‌شوند، ممکن است نام‌های قانونی داشته باشند که به وضوح نشان‌دهنده دخالت آنها در دارایی‌های رمزنگاری نباشد که تنها پس از بررسی بیشتر آشکار می‌شود (گزارش الیپتیک جلوگیری از جرایم مالی در دارایی‌های رمزنگاری شده با استفاده از تحلیل بلاک‌چین برای کاهش ریسک، ۲۰۲۳، ۸۷ و ۸۹).

۸.۴.۲ فنتایل

گروه‌های جنایت سازمان یافته به بحران مواد مخدر صنعتی دامن می‌زنند که در دهه گذشته باعث مرگ صدها هزار نفر بر اثر مصرف بیش از حد شده است تنها در کانادا و ایالات‌متحده قاچاق فنتانیل به یک اپیدمی اوردوز دامن می‌زند و سالانه جان حدود ۸۰۰۰۰ نفر را می‌گیرد (گزارش گروه ویژه اقدام مالی، پول‌شویی از طریق فنتانیل و مواد مخدر صنعتی نوامبر ۲۰۲۲، ۵)

فنتانیل یک مخدر قوی است که به عنوان عامل اصلی مرگ‌ومیر مواد مخدر صنعتی افزایش یافته است. طبق گزارش مؤسسه ملی سوءمصرف مواد مخدر، فنتانیل بین ۵۰ تا ۱۰۰ برابر قوی‌تر از مورفین است (گزارش الیپتیک کریپتو و تجارت جهانی فنتانیل ۲۰۲۳، ۳).

گروه‌های جنایت سازمان یافته که مواد مخدر صنعتی را قاچاق می‌کنند از طیف وسیعی از روش‌ها برای انتقال عواید غیرقانونی به آن سوی مرزها استفاده می‌کنند، عبارتند از قاچاق پول نقد، پیک نقدی؛ پول‌شویی مبتنی بر تجارت؛ خدمات غیرمجاز انتقال پول یا ارزش یا سیستم بانکی؛ و دلالان پول گروه‌های مجرم نیز از سایت‌های فروشندگان دارکنت برای بازاریابی محصولات خود استفاده می‌کنند.

و در برخی موارد پرداخت را از طریق دارایی‌های مجازی انجام می‌دهند که باعث افزایش ناشناس بودن می‌شوند این دارایی‌های مجازی اغلب به سرعت به ارز فیات تبدیل می‌شوند قاچاقچیان از شرکت‌های پوسته‌ای برای تطهیر عواید استفاده و با عواید آن دارو، مواد شیمیایی پیش ساز و تجهیزات تولید تهیه می‌کنند (گزارش گروه ویژه اقدام مالی، پول‌شویی از طریق فنتانیل و مواد مخدر صنعتی، نوامبر ۲۰۲۳/۵).

بیشتر درآمدهای حاصل از قاچاق مواد مخدر صنعتی در کشور مصرف‌کننده انباشته می‌شود و گروه‌های جنایتکار سازمان یافته از فروش محلی مواد مخدر مانند فنتانیل یا ترامادول سود می‌برند با این حال زمانی که وجوه به سمت

---

[۱] ABC Limited ـ یک صرافی دارایی‌های دیجیتال کوچک است که در حوزه قضایی پرخطر ثبت‌شده و حجم زیادی از تراکنش‌های بیت‌کوین را از طرف مجرمان سایبری پردازش کرده است.

این گروه‌های جنایتکار که محموله‌های بزرگتر را مدیریت می‌کنند، حرکت می‌کند، عواید و کالاها می‌توانند از هم جدا شوند و عواید ممکن است از طریق طرح‌های پیچیده‌تر پول‌شویی منتقل شوند.

از نظر مراحل، پول‌شویی قرار دادن اغلب در داخل کشور مصرف‌کننده صورت می‌گیرد. لایه‌گذاری و یکپارچه‌سازی احتمالاً از طریق قاچاق پول نقد، انبوه شرکت‌های پیشخوان خدمات انتقال ارزش پول (از جمله حواله) یا پول‌شویی مبتنی بر تجارت یا از طریق روابط کارگزاری بانکی (از جمله برای نقل‌وانتقالات مالی مرتبط با تجارت) رخ می‌دهد. طیف متنوع روش‌های لایه‌گذاری و متعاقب آن یکپارچه‌سازی نشان می‌دهد که مدل کسب‌وکار یکسانی وجود ندارد اما سازمان‌های جنایی بر اساس کشور به کشور و دارو به دارو از طیف وسیعی از طرح‌های پول‌شویی استفاده می‌کنند (گزارش گروه ویژه اقدام مالی، پول‌شویی از طریق فنتانیل و مواد مخدر صنعتی، نوامبر ۲۰۲۲، ۱۷).

۳ جمع‌بندی و نتیجه‌گیری

با بررسی موارد فوق این موضوع کاملاً مشهود می‌باشد که کلیه فرآیندهای مطروحه براساس استفاده از فناوری‌های نوظهور و گسترش آن در تمامی سطوح زندگی افراد می‌باشد و مجرمان همواره در حال بهره‌برداری از جنبه‌های ناشناخته آن برای عموم مردم و حتی دولت‌ها می‌باشند. اگرچه تصویب و اجرای قوانین و مقررات ضد پول‌شویی، و ایجاد فضایی ناامن برای مجرمان عضویت در معاهدات پولی و مالی بین‌المللی و برداشتن موانع بر سر راه همکاری‌های بین‌المللی، اصلاح ساختار مالیاتی کشور، کنترل و نظارت بر ارزهای خارجی و به ویژه راه‌های مبادله و انتقال آن فاصله گرفتن از اقتصاد مطلقاً، دولتی ایجاد دستگاه و تشکیلاتی مقتدر و با سطح اختیارات بالا برای مبارزه با پول‌شویی ارائه گزارشات آماری دوره‌ای اجرای عملیات بانکداری اسلامی و بازسازی و اصلاح سیستم بانکی و مؤسسات اعتباری و برخی دیگر از موارد تا حدی فضا را برای این گروه از مجرمان ناامن نموده است ولی از آنجایی که در هیچ زمانی امکان جلوگیری از گسترش فناوری‌ها به ویژه در فضای مجازی و همچنین در حوزه‌های نرم‌افزاری وجود ندارد؛ به‌گونه‌ای که در حال حاضر نیز امکان پرداخت رمزارز جهت خرید کالا یا خدمات در وب‌سایت‌های داخلی وجود دارد پس می‌بایست سازوکاری در جهت افزایش توان شناسایی و مقابله هرگونه مصادیق مجرمانه‌ای به صورت ویژه مدنظر قرار گیرد.

با استناد به برخی گزارش‌ها و اخبار استفاده از باج‌افزار در جرایم سایبری جهانی ۸۲ درصد افزایش یافته است و از ایران جزو بزرگترین کاربران باج‌افزار در جهان یاد شده که شرکت‌های ایرانی و جهانی را هدف قرار داده است. ایران متهم به انجام عملیات قفل و نشت[1] شده است ـ جایی که مهاجمان با استفاده از باج‌افزار، یک سیستم را قفل می‌کنند و متعاقباً اطلاعات حساس شرکت را از طریق کانال‌های خود در دارکوب افشا می‌کنند.

متأسفانه خلأ قانونی در این زمینه باعث ایجاد ریسک شهرت در سطح جهانی و آسیب به ساختار اقتصادی کشور می‌شود. در تعدادی از گزارش‌های اشاره شده قسمت روش‌شناسی از جمله چین‌الیسیس فصلی مجزا به حوزه‌های قضایی با ریسک بالا اختصاص پیدا کرده است همچنین عملکرد صرافی‌های رمزارز در ایران در کنار کره شمالی و روسیه مورد بررسی قرار گرفته است. همان‌طور که در مبانی نظری اشاره شده است یکی از اقداماتی که ارائه‌دهندگان

[1] lock and leak

خدمات دارایی مجازی صرافی رمزارز انجام می‌دهند مبادله بین دارایی‌های مجازی و ارزهای فیات می‌باشد، از آنجایی که این صرافی‌ها به صورت مستقل در حال فعالیت هستند و نظارتی بر آنها وجود ندارد پس از انتقال ریال به کیف پول رمزارزی عملاً ارز فیات (پول) از شبکه بانکی و مالی رسمی خارج می‌شود و در فضایی وارد می‌شود که توسط ناظران قابل‌مشاهده و ردگیری نمی‌باشد، لذا این شرایط بستر مناسبی برای مجرمانی که مایل به سوءاستفاده از دارایی‌های مجازی برای مقاصد غیرقانونی هستند، می‌توانند به سادگی از حوزه‌های قضایی با چارچوب نظارتی ضعیف یا بدون چارچوب نظارتی؛ جهت انجام پول‌شویی تأمین مالی تروریسم و حتی تأمین مالی اشاعه فراهم آورد.

نتایج هم‌راستا با پژوهشی که مافی و رامشی در سال ۱۴۰۱ انجام دادند در نظام حقوقی ایران به دارایی مجازی توجه نشده است می‌باشد.

لذا خلأ موجود در مقررات اجرایی و کنترلی و از آن مهم‌تر قوانین بازدارنده از وقوع تخلفات احتمالی و مجازات‌های مربوطه باعث گردیده تا کلیه معاملات در حال انجام در کشور مورد نقد و بررسی شرکت‌ها و نهادهای ناظر بین‌المللی قرار گرفته و با توجه به عدم وجود صورت‌های مالی بین‌المللی شفاف و گزارش‌های دوره‌ای مربوطه در این خصوص، فعالین بازار رمزنگاری در ایران همواره در مظان اتهام قرار گیرند. این مورد در کاهش درجه اعتبار، افراد نهادها و معاملات بازار نیز تأثیرگذار بوده و تبعات خاص خود را به دنبال دارد. شایان ذکر است فضای سیاسی حاکم بر جوامع بین‌المللی به ویژه در برابر جمهوری اسلامی ایران، با تأثیرپذیری از تحریم‌ها و اعمال فشارهای مختلف همچنین غرض‌ورزی‌های متداول و ناعادلانه از یک‌سو و همچنین طرح موضوعات با رویکرد منفی در گزارشات فصلی و سالانه مختلف موجبات تخریب وجهه بین‌المللی کشور فراهم می‌آورند.

ماحصل پژوهش به عمل آمده بیانگر این موضوع است که با اقدامات مؤثر در خصوص تعیین متولی در حوزه رمزارز، تدوین دستورالعمل‌های مربوطه طراحی و راه‌اندازی سامانه‌های هوشمند پایش و شناسایی معاملات مشکوک به کمک فاکتورها و مؤلفه‌های از پیش تعیین شده در ابزار اعلان قرمز به صورت کاملاً. سیستمی و به صورت ۷/۲۴، علاوه بر نظم دهی به فرایندهای اجرایی سالم در سطح کشور موجبات جلوگیری از سوءاستفاده‌های احتمالی از روش‌هایی مانند باج‌افزار، صرافی ارز مجازی، راگ پول، پل و... در آینده صورت پذیرد؛ که این امر می‌تواند موجبات ایجاد جایگاهی مناسب از منظر گروه ویژه اقدام مالی به عنوان اصلی‌ترین نهاد سیاست‌گذار در حوزه مبارزه با پول‌شویی و سایر نهادهای بین‌المللی را برای کشور به ارمغان آورد.

۴ پیشنهادهای کاربردی

- از آنجایی که طراحی باج افزارها و عواید ناشی از استفاده از آنها به نوعی اخاذی محسوب می‌شود، لذا در راستای توصیه شماره ۳ گروه ویژه اقدام مالی پول‌شویی از طریق باج‌افزار جرم انگاری شود.
- با افزایش آگاهی و ایجاد کانال‌های، امن قربانیان به ارائه گزارش داوطلبانه حوادث تشویق شوند.
- در سند ارزیابی ریسک، ملی خطرات ناشی از انجام پول‌شویی از طریق باج افزارها شناسایی و ارزیابی شود.
- دارایی مجازی به عنوان یک دارایی توسط نهادهای ناظر پذیرفته شود همچنین لازم است نهادهای ناظر (بانک مرکزی ج.ا.ا و مرکز اطلاعات مالی) قوانین نظارتی بخشنامه‌ها و دستورالعمل‌هایی را توسعه دهند تا نظارت بر

فعالیت همه ارائه‌دهندگان خدمات دارایی مجازی از جمله صادرکنندگان متولیان، پلتفرم‌های معاملاتی و فروشندگان محقق شود. در این راستا یادداشت تفسیری توصیه شماره ۱۵ گروه ویژه اقدام مالی با رویکرد مبتنی بر ریسک و اجرای استانداردهای مبارزه با پول‌شویی و تأمین مالی تروریسم قابل‌استفاده است. ارائه‌دهندگان خدمات دارایی مجازی (صرافی ارز مجازی) باید قوانین نظارتی را که در حوزه کاری آنان تعریف خواهد شد را بیاموزند و از آنها پیروی کنند.

- در گام بعدی ارائه‌دهندگان خدمات دارایی مجازی ملزم شوند که اطلاعات مالک اولیه و ذینفع نهایی را در مورد کلیه نقل‌وانتقالات دارایی‌های مجازی در راستای اجرای مقررات مبارزه با پول‌شویی ذخیره و نگهداری کنند. آنچه که سال‌ها مؤسسات مالی ملزم بودند هنگام کارگزاری حواله‌های بانکی و نقل‌وانتقال الکترونیکی وجوه در بستر سوئیفت به اشتراک بگذارند، حال تحت قانون انتقال اطلاعات توسط گروه ویژه اقدام مالی در خصوص نقل‌وانتقالات دارایی مجازی مورد تأکید قرار گرفته است؛ زیرا آدرس‌های ارزهای دیجیتال می‌توانند توسط چندین مشتری ذینفع استفاده شوند به عنوان مثال برخی از صرافی‌ها از یک آدرس واحد برای ارسال تمام تراکنش‌ها استفاده می‌کنند.
- مراکز تصمیم‌گیری و سیاست‌گذاری در حوزه مبارزه با پول‌شویی در کشور و یا ایجاد کارگروه‌های مشترک با هدف جلوگیری از موازی کاری کاهش یابد اشتراک‌گذاری اطلاعات با رویکرد شناسایی و قانون‌گذاری در خصوص آسیب‌های فناوری‌های نوین تسریع گردد.
- نظارت دقیق‌تر بر فرآیندهای پولی مشتریان بانک‌ها و مؤسسات مالی در جهت اجرای کامل قوانین و مقررات ابلاغی از سوی بانک مرکزی ج.ا.ا توسط واحدهای مبارزه با پول‌شویی به کمک اعلان قرمز صورت پذیرد.
- کارگروه‌های بررسی مشترک دستورالعمل‌ها اطلاعیه‌ها و ... صادره از سوی نهادهای متولی داخلی با حضور نمایندگان بانک‌ها و مؤسسات مالی با هدف جلوگیری از برداشت‌های سلیقه‌ای از متن دستورالعمل‌ها، اطلاعیه‌ها و ... ایجاد شود.
- سازوکارهای مناسب جهت احراز هویت طرفین مبادلات و همچنین تعیین سقف مجاز انتقال ریال به کیف پول‌های دیجیتال جهت تبدیل رمزارزهای گوناگون در راستای جلوگیری از سوءاستفاده‌های انجام شده از حساب‌های بانکی افراد طراحی و اجرا گردد.
- سامانه‌های هوشمند نظارت بر مراودات مالی اشخاص حقیقی و حقوقی در بازار ارزهای دیجیتال به ویژه شرکت‌های ارائه‌دهنده خدمات دارایی مجازی داخلی طراحی و عملیاتی گردند.
- از انجام تبلیغات رسانه‌ای یا فضای مجازی در خصوص رمزارزها بدون پشتوانه علمی خاص و معتبر جلوگیری شود.
- یک منبع رسمی در داخل کشور برای بررسی و به اشتراک گذاشتن اطلاعات مالی پروژه‌های حوزه کریپتو و بیان توضیح روشن و شفافی از عملکرد، هویت سازندگان و توکنومیکس (بررسی ابعاد اقتصادی یک توکن) معرفی شود.

- تعیین سقف مبادلات برای دستگاه‌های خودپرداز خود دریافت جهت عملیات منتهی به خرید/فروش و انتقال رمزارزها، صورت پذیرد، هر چند این موضوع هم اکنون در کشور موضوعیت ندارد، در آینده می‌تواند ملحوظ نظر قرار گیرد.
- آموزش‌ها و هشدارهای لازم در خصوص خطرات استفاده یا حضور در فضاهایی همچون دارک نت و ... به صورت مفاد درسی در مقاطع مختلف تحصیلی قرار گیرد.

فهرست منابع

شاملو، ب، خلیلی پاجی ع (۱۳۹۹) سیاست‌گذاری جنایی ریسک مدار در برابر فناوری ارزهای مجازی فصلنامه مجلس و راهبرد، سال بیست و هفتم شماره یک‌صد و سوم پاییز ۱۳۹۹

صیاد معروف، م، طوفان زاده مژدهی، ع رشیدی، ح. (۱۳۹۴) واحد پول دیجیتالی بیت کوین و نقش آن در تجارت الکترونیک. دومین کنفرانس بین‌المللی پژوهش در علوم و تکنولوژی ترکیه استانبول موسسه سرآمد همایش کارین.

طغیانی، ا. (۱۴۰۱). فصلنامه رخدادها و اخبار بین‌المللی حوزه مبارزه با پول‌شویی و تأمین مالی تروریسم، سال اول، شماره ۱، پاییز ۱۴۰۱

قانون مبارزه با پول‌شویی (۱۳۸۶) مجلس شورای اسلامی

قربانی، ف، موسوی ز. (۱۴۰۰) تأثیر، رمزارز بیت کوین و ارز دیجیتال در مراودات مالی کسب‌وکارهای امروز نهمین کنفرانس بین‌المللی پژوهش‌های مدیریت و علوم انسانی در ایران

مافی، ه، رامشی م. (۱۴۰۱) ماهیت حقوقی دارایی‌های مجازی فصلنامه تحقیقات حقوقی دانشگاه شهید بهشتی.

مسلمی. م (۱۳۹۷) نقش ارزهای دیجیتالی در اقتصاد و معاملات بازرگانی اولین همایش ملی مدیریت با تاکید بر حمایت از کالا و خدمات ایرانی، آباده.

Chainalysis, (February 2022). The 2022 Crypto Crime Report.

Chainalysis, (February 2023). The 2022 Crypto Crime Report.

Ciphertrace, (August 2021). Cryptocurrency crime and anti-money laundering Report.

Ciphertrace, (March 2023). Cryptocurrency crime and anti-money laundering Report-

coinmarketcap.com/academy/glossary/dark-web

ELLIPTIC, (2023). Crypto and the Global Fentanyl Trade.

ELLIPTIC, (2023). Preventing Financial Crime in Crypto assets, Using Block Chain Analysis to Mitigate Risk.

ELLIPTIC, (2023). Regulatory Outlook Report 2023.

ELLIPTIC, (2023). Sanctions Compliance in Cryptocurrencies.

FATF, (June 2014). Virtual Currencies Key Definitions and Potential AML/CFT Risks

FATF, (September 2020). Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing Report.

FATF, (October 2021). Updated Guidance for A Risk-Based Approach Virtual Assets and Virtual Asset Service Providers.

FATF, (June 2022). Targeted Update on Implementation of The FATF Standards on Virtual Assets and Virtual Asset Service Providers.

FATF, (November 2022). Money Laundering from Fentanyl and Synthetic Opioids Report.

FATF, (March 2023). Countering Ransomware Financing Report.

Fletcher, E. Larkin, Ch. Corbet, Sh. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation, Research in International Business and Finance 56

Holloway, I. & Wheeler, S. (2002). Qualitative Research for Nurses, 2nd Edit. Oxford, Black Well Science.

Kud, A. A. (2020). The Phenomenon of Virtual Assets: Economic and Legal Aspects, International Journal of Education and Science, 3(4), 13-24

Korbel, JJ. Blankenhagel, K. J. Zarnekow, R. (2019). The Role of the Virtual Asset in the Distribution of Goods and Products. Twenty-fifth Americas Conference on Information Systems, Cancun

Padarin, M. (2022). Virtual assets regulation in BVI: Challenges and opportunities, Asia Law Business Journal.

Sarani, Mo and Kahdavi, A and Shafieianpour, A. (1399) Recognition of Digital Currency and Bitcoin, Fifth National Conference on Economics, Management and Accounting, Shirvan

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research Methods for Business Students.

Strauss, A, Corbin, J. (1394). Basics of qualitative research: techniques and stages of production of grounded theory. Translation: Ebrahim Afshar. Tehran