Jurisprudential Principles of Islamic
Biannual journal of jurisprudential principles of Islamic law
Vol.۱۷● no.۱● spring and summer ۲۰۲٤● Issue ۳۳

Research Article

The role of cryptocurrencies in creating black business and juridical and legal mechanisms to prevent it

Qasim Ali Sabouri[۱], Atefeh Aminia[۲], Maryam Afshari[۳]

Received: ۲۰۲۴/۰۹/۰۴ Accepted: ۲۰۲۴/۱۱/۱۴

Abstract

Cryptocurrencies are often portrayed as a major challenger to the current financial system, promising security, speed, transparency, increasing financial transactions and creating a fairer economy, preserving privacy, and eliminating red tape. Assuming we accept all these things, but the crypto world does not always have positive aspects. Governments, regulatory agencies, central banks and other financial institutions are struggling to consider the prospect of cryptocurrency decentralization in terms of the legal and forensic challenges it has created; But there are still many important challenges such as committing crimes such as: money laundering, terrorism financing, drug trafficking through the use of these cryptocurrencies. The main question of this research is what role do cryptocurrencies play in creating black business and what mechanisms are there to prevent this business? The results of the research indicate that in order to prevent black trade, solutions such as the use of smart contracts, the need to legalize cryptocurrencies, monitoring exchanges and banks, etc. can be used. The research method in this research is descriptive-analytical.

Keywords: *Cryptocurrency, black business, challenges, mechanisms.*

[۱] - PhD student, Department of Law, Emirates Branch, Islamic Azad University, Dubai, United Arab Emirates.

[۲]- Assistant Professor, Department of Law, Varamin Branch, Islamic Azad University, Varamin, Iran. (corresponding author) jahanbakhsh@skiff.com

[۳] - Assistant Professor, Department of Law, Damavand Branch, Islamic Azad University, Damavand, Iran.

دوفصلنامه علمی- تخصصی مبانی فقهی حقوق اسلامی
سال۱۷● شماره۱● بهار و تابستان ۱۴۰۳● شماره پیاپی۳۳

مقاله پژوهشی

نقش رمزارزها در ایجاد تجارت سیاه و سازوکارهای فقهی و حقوقی پیشگیری از آن

قاسمعلی صبوری[۴] ، عاطفه امینی نیا[۵]، مریم افشاری[۶]

چکیده

رمزارزها اغلب به عنوان رقیب بزرگ برای سیستم مالی فعلی به تصویر کشیده می‌شوند که وعدهٔ امنیت، سرعت، شفافیت، افزایش تراکنش‌های مالی و ایجاد اقتصادی عادلانه‌تر، حفظ حریم خصوصی و حذف تشریفات اداری را می‌دهند. بر فرض اینکه همهٔ این موارد را بپذیریم، اما همیشه دنیای کریپتو واجد جنبه‌های مثبت نیست. دولت‌ها، سازمان‌های نظارتی، بانک‌های مرکزی و سایر مؤسسات مالی به سختی تلاش می‌کنند تا چشم انداز غیرمتمرکز بودن رمزارز را ازنقطه‌نظر چالش‌های حقوقی و جرم‌شناختی که ایجاد کرده است، مدنظر قرار دهند؛ اما همچنان چالش‌های مهم و متعددی نظیر ارتکاب جرایمی مانند: پول‌شویی، تأمین مالی تروریسم، قاچاق مواد مخدر به‌واسطهٔ استفاده از این رمزارزها وجود دارد. پرسش اصلی این پژوهش آن است که رمزارزها چه نقشی در ایجاد تجارت سیاه دارند و چه سازوکارهایی جهت پیشگیری از این تجارت وجود دارد؟ نتایج تحقیق حاکی از آن است جهت جلوگیری از تجارت سیاه می‌توان از راهکارهایی نظیر استفاده از قراردادهای هوشمند، لزوم قانونی‌سازی رمزارزها، نظارت بر صرافی‌ها و بانک‌ها و... استفاده نمود. روش پژوهش در این تحقیق از نوع توصیفی – تحلیلی می‌باشد.

واژگان کلیدی: رمزارز، تجارت سیاه، چالش‌ها، سازوکارها.

---

[۴]– دانشجوی دکتری، گروه حقوق، واحد امارات، دانشگاه آزاد اسلامی، دبی، امارات متحده عربی.
[۵]– استادیار، گروه حقوق، واحد ورامین، دانشگاه آزاد اسلامی، ورامین، ایران. (نویسنده مسئول) jahanbakhsh@skiff.com
[۶]– استادیار، گروه حقوق، واحد دماوند، دانشگاه آزاد اسلامی، دماوند، ایران.

مقدمه

پیشرفت روزافزون فناوری اطلاعات و افزایش کاربری آن در زندگی روزمره علاوه بر بهبود کیفیت حیات از طریق استفاده مشروع گاهی موجب آسیب‌دیدن جامعه نیز می‌شود. فضای سایبری که از دستاوردهای فناوری اطلاعات است، بستری را برای تحولات مختلف حقوقی و مالی فراهم آورده است. در عصر حاضر، ارزهای رمزنگاری شده در خط مقدم توسعه اقتصادی و مالی جهان قرار دارند. این امر، فرصت‌ها و تهدیدهای متعددی را در بازارهای مالی سراسر جهان به وجود آورده و در سال‌های اخیر سبب جلب‌توجه شمار قابل‌توجهی از شهروندان و فعالان اقتصادی به خود شده است. بر همین اساس، تعداد بازیگران درگیر در تجارت ارزهای رمز پایه در سال‌های اخیر افزایشی چشمگیر یافته است (قاسمی، ۱۴۰۰، ۱۹۶).

یکی از فرضیه‌های باورپذیر دربارۀ رمزارزها بر این تأکید دارد که خالق اصلی پرکاربردترین ارز رمزنگاری شده در واقع نهادهای اطلاعاتی و امنیتی هستند و هدف از ایجاد آنها تأمین مالی و تسهیل پرداخت ناشناس برای شبکه بین‌المللی عوامل مخفی و جاسوسی است. این فرضیه با توجه به چشمگیر بودن کاربری رمزارزها برای پروژه‌های مخرب مبتنی بر وب سیاه، همانند باج‌گیری اینترنتی، پول‌شویی و فروش مواد مخدر بیشتر تقویت می‌گردد. پیچیدگی، ابهام و عدم قطعیت به دلیل اتخاذ قریب‌الوقوع یک رویکرد رسمی از سوی قانون‌گذاران سبب گردیده است تا در این نوشتار به بررسی عمیق‌تر تناقض‌ها و تضادهای موجود و نیز آگاه‌سازی ذی‌نفعان از زوایای مختلف پرداخته شود. در این راستا از دو ابزار پرکاربرد آینده‌پژوهی تحت عنوان "چرخ آینده" و همچنین "نگاشت مفهومی حلقه‌های سیستمی" استفاده گردیده است. از این طریق ابعاد تحلیلی این موضوع در قالب سناریوی تجارت سیاه بررسی می‌شود. حلقه‌های بازخوردی شناسایی شده در سناریوی تجارت سیاه شامل الف) تروریسم، پاشنه آشیل رمزارزها، ب)هکرها مانع توسعه‌یافتگی و پ)شکاف تخصص امنیت فناوری اطلاعات با نیازهای بازار می‌باشد. با توجه به مطالبی که در فوق عنوان گردید، هدف این پژوهش، بررسی نقش رمزارزها در تشکیل و ایجاد تجارت سیاه، مصادیق آن و راهکارها و سازوکارهای پیشگیری از ایجاد تجارت سیاه با استفاده از ظرفیت رمزارزها پرداخته خواهد شد.

۲- مفاهیم

۲-۱- مفهوم ارزهای رمزنگاری شده

رمزارز یا ارز رمزنگاری شده یکی از انواع ارزهای دیجیتالی است. در این نوع از ارزهای دیجیتالی سوابق تراکنش‌ها و مالکیت دارایی به‌وسیلۀ الگوریتم‌های رمزنگاری قوی برای اطمینان از سوابق معاملات و داده‌ها تبدیل به کد شده و به‌وسیلۀ فناوری زنجیرۀ بلوکی ثبت و نگهداری می‌شوند. این نوع از ارزهای دیجیتالی معمولاً به صورت یک سازمان خودگردان مدیریت می‌شوند و این بدین معنی است که کاربران ارز رمزنگاری شده می – توانند بدون وجود یک واسطه همانند مؤسسه اعتباری یا بانک و بدون داشتن یک حساب بانکی یا کارت اعتباری اقدام به پرداخت‌های خرد یا مبادلۀ ارزی با دیگران نمایند و این امر تهدیدی برای روش‌های مرسوم مدیریت مالی محسوب می‌شود و می‌تواند نقش سازمان‌های مالی همچون بانک مرکزی را بی‌اثر نماید. با توجه به اینکه ارزهای رمزنگاری شده به و صورت نامتمرکز و خودگردان مدیریت می‌شوند، نقطۀ مقابل مدیریت مالی متمرکز مرسوم در جهان محسوب می‌شوند. ازاین‌رو در اغلب

کشورهای جهان دولت‌ها و بانک‌های مرکزی در مقابل استفاده از این رمزارزها مقاومت نموده و یا استفاده از آن را در کشور خود ممنوع اعلام نموده‌اند.

۲-۲- مفهوم تجارت سیاه

تردیدی در این نیست که مکانیسم‌های پرداخت ناشناس و دیجیتال به ویژه رمزارزها موجب تسهیل و رشد بازرهای وب سیاه شده است که در آن تبادلات کالاها و خدمات غیرقانونی صورت می‌گیرد. معروف‌ترین اتفاق در این حوزه دستگیری گردانندگان سایت سلیک رود[۷] بوده است که در این پرونده مبلغی بالغ بر ۴ میلیون دلار بیت‌کوین مصادره شده است. همچنین افراد مجرم توانسته‌اند با استفاده از تبادلات رمزارزها یک میلیارد و دویست میلیون دلار در طی سال‌های ۲۰۱۷ تا ۲۰۱۸ جابجا کنند. همچنین گزارشFBI حاکی از آن است که در سال ۲۰۱۸ ثبت شکایت‌های مرتبط با جرایم انجام شده از طریق رمزارزها در مقایسه با سال ۲۰۱۵ شش برابر شده است (Malwa ,۲۰۱۸, ٦٨).

از جمله مصادیق جرایم ناشی از تجارت سیاه که با استفاده از رمزارزها در بستر مجازی ارتکاب می‌یابند می – توان به فعالیت‌های پول‌شویی، قاچاق مواد مخدر، باج‌گیری‌های اینترنتی، قاچاق انسان و اعضای بدن، تأمین مالی تروریسم و فعالیت شبکه‌های اطلاعاتی و جاسوسی اشاره نمود.

۳- مصادیق تجارت سیاه با استفاده از رمزارزها

۳-۱ پول‌شویی الکترونیکی با استفاده از رمزارزها

پول‌شویی جرم مهمی است که مجموعه اقتصاد را تحت‌تأثیر قرار می‌دهد و مانع توسعه اقتصادی، اجتماعی و فرهنگی جوامع در تمام جهان می‌شود. در دهه‌های اخیر، جهانی‌شدن به همراه رشد اقتصادهای زیر زمینی فرامرزی، محرک فعالیت‌های غیرقانونی بوده است. فعالیت‌های مجرمانه مانند تجارت و قاچاق مواد مخدر، تجارت و قاچاق اسلحه، تروریسم، قاچاق مهاجران، تجارت انسان و فحشا، تجارت اعضای بدن انسان، کلاهبرداری اخاذی، رشوه و... سودهای کلانی را خلق کرده که افزایش تقاضا برای پول‌شویی را به دنبال داشته است. مبارزه با پول‌شویی شامل پیشگیری از باز بکار گیری عواید حاصل از فعالیت‌های مجرمانه و فراهم‌کردن ابزارهایی برای شناسایی جرم پس از ارتکاب آن است (چتین و دیگران، ۱۳۹۲، ۷).

جرم پول‌شویی قبل از پیدایش ارزهای رمزنگاری شده نیز سیستم عدالت کیفری را با چالش‌های جدی مواجه می‌کرد؛ تبدیل شدن این ارزها به عنوان یک ابزار مجرمانه در دست بزهکاران، این چالش‌ها را چندین برابر می‌کند. به بیان دیگر، رمزارزها هم سبب ایجاد روش‌های نوین در جرم پول‌شویی شدند و هم ترکیب ویژگی‌های آنها با روش‌های سنتی پول‌شویی، کشف و تعقیب مجرمان این جرایم را دشوارتر کرده است. از جمله مهم‌ترین ویژگی‌های این ارزها که سبب تسهیل ارتکاب جرم پول‌شویی می‌شود، می‌توان تراکنش‌های سریع ارزهای رمزنگاری شده و تبدیل آنها به سایر وجوه

---

[۷] Slik Road

(نبوی و صابر، ۱۳۹۹، ۱۸۶)، ناشناس ماندن هویت اشخاص، مبادلات همتا به همتا و ماهیت غیرمتمرکز این ارزها را نام برد. در این نوشتار به تشریح روش‌های ارتکاب جرم پول‌شویی در بستر ارزهای رمزنگاری شده پرداخته می‌شود.

یکی از روش‌های پول‌شویی با استفاده از ارزهای رمزنگاری شده می‌تواند این باشد که شخص عواید مجرمانه‌ای را که به دست آورده است با روش اس مورفینگ و با ایجاد چندین حساب گوناگون اقدام به خرید ارز رمزنگاری شده مانند بیت‌کوین کند (مرحلهٔ جای‌گذاری). (منطق پشت اس مورفینگ این است که چندین نفر که تراکنش‌های کوچک را در مکان‌های مختلف انجام می‌دهند، بسیار کمتر مشکوک هستند و توجه کمتری را نسبت به یک نفر که یک تراکنش فردی با مقدار قابل‌توجهی پول انجام می‌دهند، جلب می‌کنند. اس مورفینگ مطمئناً طرح جدیدی نیست، اما به دلیل سهولت و سرعت انتقال ارزهای رمزنگاری شده در یک شهر یا سراسر جهان، به یک مشکل جهانی تبدیل شده است) (Forgang,۲۰۱۹: ۱٤). در مرحله دوم، شخص بیت‌کوین‌ها را با سایر آلت‌کوین‌ها مبادله می‌کند (مرحلهٔ لایه‌گذاری) و سرانجام در مرحله آخر آلت‌کوین‌ها را به پول رایج تبدیل می‌کند (مرحلهٔ ادغام). مجرم در چنین شرایطی مبالغ هنگفت را سود ناشی از سرمایه‌گذاری معرفی می‌کند.

سایت‌های قمار ارزهای رمزنگاری شده نیز اغلب به عنوان تسهیلات پول‌شویی استفاده می‌شوند. (سایت‌های قمار متعددی در اینترنت وجود دارند که بر این نوع ارزها تمرکز کرده‌اند. حتی بیشتر این ارزها در فضای دارک نت فعالیت می‌کنند). مجرمان می‌توانند در این سایت‌ها حساب باز کنند، سپس وجوه پول‌شویی را به آن سایت ها منتقل کنند. آنها شرط‌بندی‌هایی انجام می‌دهند، یا حتی در برخی موارد وجوه را بدون هیچ شرطی به آدرس جدید منتقل می‌کنند. این امر به ایجاد شکاف در ردیابی جریان وجوه کمک می‌کند و در بسیاری از جهات مانند یک مخلوط‌کننده. از آن جا که سایت‌ها مقررات مربوط به «شناسایی مشتری»[۸] در سطح پایینی قرار دارد، برای مجریان قانون دشوار است که اطلاعاتی در مورد انتقال وجه به داخل و یا خارج از این خدمات به دست آورند (Cipher,۲۰۱۸, ۸-۹). انجام مبادلات ارزی در صرافی‌ها و تأسیس شرکت‌های صوری و پیشرو (پوشش یا شرکت‌های پیشرو؛ یک شرکت پیشرو یک کسب کسب‌وکار که درآمدهای حاصل از فروش را با درآمد حاصل از فروش محصولات یا سرویس‌های غیرقانونی مخلوط می‌کند. مجرمان از شرکت‌های پیشرو برای شست‌وشوی پول‌های غیرقانونی با دادن وجوه با ظاهری که منبع آن مشروع جلوه کند، استفاده می‌کنند) (رنگریز، ۱۳۹۷، ۴) از دیگر مواردی هستند که با ظهور ارزهای رمزنگاری شده شکل پیچیده‌تری از پول‌شویی را به خود گرفتند که مجرمان به این روش‌ها نیز متوسل می‌شوند.

۳-۲ تأمین مالی تروریسم با استفاده از رمزارزها

تروریسم پدیده‌ای است که همواره امنیت جهانی را تهدید می‌کند. با اینکه مخاطب، هدف و سبیل مرتکب اقدامات تروریستی حاکمیت و دولت‌ها می‌باشد، لیکن تروریست‌ها از طریق جنایت علیه اشخاص و اموال مردم سعی در ارسال پیام وحشت به حاکمیت را دارند. به‌عبارت‌دیگر، هر چند که بزه‌دیدگان قانونی این جرایم حاکمیت و دولت‌ها هستند؛ اما بزه‌دیدگان واقعی، عینی و ملموس جرایم تروریستی افراد عادی و بی‌گناه جامعه هستند که جان و مال خود را از دست می‌دهند (نجفی ابرندآبادی،۱۳۸۶، ۲۵۶۲)؛ لذا می‌توان گفت که تروریسم یک مشکل جهانی است و راه رسیدن به یک

[۸] Know Your Custumer (KYC).

امنیت و آسایش جهانی و مقابله مؤثر با این جرم نیاز به یک عزم ملی و همکاری جهانی دارد. دولت‌ها دریافتند که مهم‌ترین و مؤثرترین راهکار مبارزه با تروریسم؛ مبارزه با تأمین مالی آن است. تأمین مالی تروریسم از جمله جرایمی است که بیشتر جنبه سازمان‌یافته دارد و در بستری فراملی و جهانی رخ می‌دهد.

استمرار و تداوم حیات سازمان‌های تروریستی برای ارتکاب جرایم و تأمین بودجهٔ اعضای خود وابستگی شدیدی به تأمین منابع مالی دارد. در نتیجه کشورهای جهانی در وهلهٔ نخست شروع به مسدودکردن راه‌های ارتباطی تروریست‌ها با منابع مالی آنها پرداختند. با این حال، ظهور ارزهای رمزنگاری شده می‌تواند در این مبارزه کشورها را با دشواری مواجه کند، چرا که جامهٔ جهانی بر این باورند که این ارزها می‌تواند تأمین مالی گروه‌های تروریستی و ارسال پول به آنها را تسهیل بخشد. در این نوشتار به بررسی جرم تأمین مال تروریسم و نقش رمزارزها در ارتکاب این جرم پرداخته می‌شود.

FATF یکی دیگر از نهادهای مهم در راستای مبارزه با تأمین مالی تروریسم است. در واقع هدف اولیه این نهاد بین‌دولتی مبارزه با پول‌شویی بود، اما با افزایش حملات تروریستی و ارتباط تنگاتنگی که تأمین مالی تروریسم با پول‌شویی دارد، مبارزه با تأمین مالی تروریسم نیز در دستور کار این سازمان قرار گرفت. به‌طوری‌که در بیشتر توصیه‌های ارائه شده توسط این نهاد، در کنار پول‌شویی به تأمین مالی تروریسم نیز اشاره شده است. (اخیراً مقابله با تأمین مالی اشاعه سلاح‌های کشتارجمعی نیز به عنوان سومین رکن اساسی FATF به وظایف این نهاد اضافه شده است). ظهور ارزهای رمزنگاری شده توجه FATF را نیز به عنوان یک ابزار پرداخت تسهیل‌کننده برای تأمین مالی تروریسم به خود جلب کرده است. به‌طوری‌که در سال ۲۰۱۵ طی گزارشی تحت عنوان «خطرات نوظهور تأمین مالی تروریسم»[۹] ؛از ارزهای مجازی نیز در بخشی از این گزارش، به عنوان یک خطر جدی برای تأمین مالی تروریسم یاد کرده است. FATF در توصیه دیگری تحت عنوان «راهنمای بروز شده برای رویکرد مبتنی بر ریسک به دارایی‌های مجازی و ارائه‌دهندگان خدمات دارایی مجازی»[۱۰] روشن می‌کند که کشورها باید رویکرد مبتنی بر ریسک را به کار گیرند تا اطمینان حاصل شود که اقدامات برای جلوگیری یا کاهش خطرات پول‌شویی، تأمین مالی تروریسم یا خطرات شناسایی شده در حوزه قضایی مربوطه آنها است. تحت رویکرد مبتنی بر ریسک کشورها باید الزامات را برای موقعیت‌های پر خطر یا فعالیت‌های مرتبط با دارایی‌های مجازی تقویت کنند. [۱۱]

ناشناس ماندن هویت و امکان انتقال ناشناس وجوه رمزنگاری در سطح بین‌الملل (هر چند که این ناشناس بودن گاهی اوقات نسبی باشد)، سهولت انجام تراکنش، ماهیت غیرمتمرکز و دشواری در ردیابی اشخاص از جمله ویژگی‌هایی است که تأمین مالی تروریسم را نیز همانند سایر جرایم می‌تواند در بستر ارزهای رمزنگاری شده تسهیل بخشد. شاید ذکر این مهم ضروری باشد که گروه‌های تروریستی از راه‌های گوناگون دیگری همچون کاشت، فروش و قاچاق مواد مخدر، اخاذی، آدم‌ربایی برای باج‌گیری و بسیاری از روش‌های دیگر تأمین مالی می‌شوند، و هر شیوه و روش نیز چالش‌های

---

[۹] FATF Report, Emerging Terrorist Financing Risks, FATF, Paris, October ۲۰۱۵. (www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financingrisks.html.)

[۱۰] FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, October ۲۰۲۱. (http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBAVA-VASP.html).

[۱۱] Ibid, p: ۱۹.

خاص خود را دارد که بررسی تمامی این چالش‌ها خارج از موضوع این پژوهش می‌باشد. بسیاری از رسانه‌های خبری بر این نکته پافشاری دارند که ارزهای مجازی ویژگی «ناشناختگی» و «غیرقابل‌ردیابی» بودن دارند، اما این امر تا حدودی اغراق‌آمیز بوده و با بی‌دقتی همراه است شاید بهترین عبارت برای رمزارزهایی چون بیت‌کوین، «شبه ناشناختگی»[۱۲]است؛ زیرا کاربران این نوع ارزها با نشانی‌های حرفی – عددی و کیف پول دیجیتال خود در بلاک‌چین حاضر می‌شوند. درحالی‌که هویت واقعی کاربر در بلاک‌چین مشخص نیست؛ اما اطلاعات مربوط به تراکنش‌ها ازجمله تاریخ، ارزش و نشانی رمزارزهای معامله‌گران به صورت عمومی ثبت می‌شود. به‌علاوه ازآنجاکه بلاک‌چین به ترتیب زمانی اقدام به ثبت تراکنش‌ها می‌کند این امکان وجود دارد که تصویری نسبتاً قابل‌اعتماد از حرکت رمزارزها به دست آورد.

بنابراین، هنگامی که هویت شخص حقیقی یا حقوقی دارنده نشانی عمومی ارز مجازی مشخص شود می‌توان حجم انبوهی از اطلاعات را در خصوص اقدامات وی در شبکه کسب کرد. امروزه برخی شرکت‌های خصوصی در افشای تراکنش‌های این ارزها و توسعه ابزارهای تحلیل فعالیت‌های غیرقانونی آنها به صورت تخصصی فعالیت می‌کنند (Redman,۲۰۱۸: ٦). اما همین میزان از ناشناختگی یا «شبه ناشناختگی» نیز برای مجرمین و به‌خصوص تروریست‌هایی که از ارزهای مجازی استفاده می‌کنند، کاراست.

درهرحال ارسال نشانی؛ مثلاً بیت‌کوین به یک رسانه یا شبکه عمومی در قالب پیام صوتی و تصویری به‌مراتب بهتر و سودمندتر از تبلیغ برخط شماره‌حساب بانکی است. بااین‌حال، امکان ردیابی ارزهای مجازی تا حدود زیادی فعالیت مجرمان را محدود می‌کند. (Berg and McCarthy,۲۰۱٦, ۸٤).

یکی دیگر از ویژگی ارزهای مجازی که برای مجرمین و تروریست‌ها جذابیت دارد، امکان انتقال فرامرزی آنها بدون توسل به واسطه‌های قانونی است. هرچند باید اذعان کرد که ارزهای مجازی قابلیت انتقال در حجم وسیع و بسیار سریع را ندارند، ابزاری مؤثر برای انتقال ارزش از طریق فناوری نظیر به نظیر به صورت فرامرزی هستند. این قابلیت به ویژه برای باج‌گیران اینترنتی که در قبال اعاده اطلاعات کاربران مورد حمله، اخاذی می‌کنند جذابیت خاصی دارد زیرا می‌توانند از هر نقطه جهان مبالغ موردنظر خود را بدون نیاز به ارائه اطلاعات حساب بانکی دریافت کنند.

علی‌رغم جستجوها در میان منابع متعدد، تا کنون هیچ گزارشی مبنی بر استفاده تروریست‌ها از شبکه نظیر به نظیر برای انتقال ارزهای مجازی دریافت نشده است. اما این به معنای نبود این امر نیست. شاید بتوان یکی از علل این امر را فقدان امکان تبدیل ارزهای مجازی به ارزهای ملموس در مناطق مورد مخاصمه و درگیری تروریست‌ها دانست. همان‌طور که محققین مرکز امنیت امریکای نوین(CNAS) اعلام کرده‌اند: «اگر امکان انتقال و تبدیل ارزهای مجازی آسان‌تر شود... و اگر گروه‌های تروریستی در مکان‌هایی همچون زیر صحرای آفریقا، یمن و شاخ آفریقا به زیرساخت‌های فنی لازم برای حمایت از فعالیت ارزهای مجازی دست یابند، با تهدید بالفعل مواجه خواهیم بود» (Goldman and other,۲۰۱۷, ۳۵). یکی دیگر از ویژگی‌های رمزارزها غیرمتمرکز بودن آنها می‌باشد. طبیعی است که مجرمین و تروریست‌ها تمایل بیشتری به استفاده از ارزهای غیرمتمرکز داشته باشند. این نوع ارزها که منبع‌باز و رابطه‌ای غیرمتمرکز دارند ارزهای «بدون مجوز» نام دارند؛ زیرا دسترسی به آنها محدودیتی ندارد. هیچ مرکز صلاحیت‌دار واحد برای ممانعت

[۱۲] Pseudonymous.

از دسترسی به شبکه این نوع ارزها وجود ندارد. نمی‌توان این شبکه‌ها را تعلیق، مجازات یا همانند سامانه‌های متمرکز کاملاً مسدود کرد. [۱۳]

۳-۳- قاچاق سازمان یافتهٔ مواد مخدر با استفاده از رمزارزها

آثار شوم و بسیار خطرناک مواد مخدر همانند آفتی تاروپود جوامع بشری را فراگرفته است و علی‌رغم رویکردها و سیاست جنایی دولت‌ها در مبارزه با جرایم ناشی از مواد مخدر متأسفانه روزبه‌روز بر تعداد و میزان این جرایم افزوده می‌شود. ظهور ارزهای رمزنگاری شده و ایجاد روش‌های پرداخت نوین و تبادل ارزش در این مجراها، راه مجرمان این عرصه را هموارتر کرده است. در نتیجه بزهکاران می‌توانند عواید مجرمانهٔ حاصل از خریدوفروش، ارسال و قاچاق مواد مخدر را خیلی راحت‌تر جابه‌جا کنند. در نتیجه اگر جرایم مواد مخدر با همین سرعت پیش برود جامعهٔ جهانی با یک اپیدمی (همه‌گیری) مواجه خواهد شد.

چند سال است که ارزهای رمزنگاری شده به بازارهای دارک نت متصل شده‌اند، جایی که این بازارها به عنوان «آمازون» برای انواع کالاهای قاچاق که مهم‌ترین آنها مواد مخدر، روان‌گردان و افیونی هستند؛ تبدیل شده‌اند. دلیل اینکه ارزهای رمزنگاری شده به این طریق به دارک نت متصل می‌شوند، این است که بسیاری از بازارها و وب‌سایت‌های دارک نت که مواد مخدر می‌فروشند، همهٔ کاربران خود (اعم از مصرف‌کنندگان و فروشندگان) را ملزم می‌کنند که از گونهٔ خاصی رمزارز برای انجام تراکنش و معاملات استفاده کنند. این امر برای محافظت از هویت خریدار و فروشنده از شناسایی شخصی است (Durrant,۲۰۱۸,۲۸).

بازارها و وب‌سایت‌های دارک نت به فروشندگان مواد مخدر اجازه می‌دهند تا پایگاه (بازار) مصرف‌کننده‌ای گسترده‌تر از زمانی که قرار بود مواد مخدر را به صورت محلی بفروشند، داشته باشند. به‌عبارت‌دیگر، با دارک نت، فروشندگان می‌توانند مواد مخدر غیرقانونی خود را هم در بازار داخلی کشور متبوع خودشان داخل و هم در سطح بین‌الملل توزیع کنند، و به مردم سراسر جهان دسترسی داشته باشند (Ibid,٥٤).

بازارهای ناشناس آنلاین یک توسعهٔ فناوری نسبتاً جدید هستند که فروشندگان و خریداران را قادر می‌سازند تا با ضمانت‌های ناشناس بودن بسیار قوی نسبت به پلتفرم‌های تجارت الکترونیک سنتی، به صورت آنلاین معامله کنند. برای نشان‌دادن وسعت جهانی‌شدن خرید مواد مخدر، در ذیل به بررسی و مطالعهٔ موردی یکی از پرونده‌های مواد مخدر که در فضای دارک نت و ارزهای رمزنگاری شده رخداده است می‌پردازیم.

یکی از بازارهای مربوط به خریدوفروش مواد مخدر، بازار آلفابای[۱۴] بود که بین دسامبر ۲۰۱۴ و جوالی ۲۰۱۷ فعالیت می‌کرد، و ظاهراً در آن زمان به بازار پیشرو تبدیل شده بود (Christin,۲۰۱۷,۲). در واقع آلفابای یک وب‌سایت مارکت بود که در دارک نت روی شبکهٔ ناشناس TOR راه‌اندازی شده بود و برای فروش داروهای غیرقانونی مرگ‌بار، اسناد هویتی سرقت شده و جعلی (مانند شناسنامه و گذرنامه)، کالاهای تقلبی، بد افزارها و سایر ابزارهای هک رایانه،

---

[۱۳] Decentralization in Bitcoin and Ethereum, retrieved from: http://hackingdistributed.com/ ۲۰۱۸/۰۱/۱۵/ decentralization-bitcoin-ethereum/ (visited: ۱۰/۱۰/۲۰۱۸).

[۱۴] Alphabay.

سلاح گرم و مواد شیمیایی سمی در سراسر جهان استفاده می‌شد و از ارزهای رمزنگاری شده از جمله بیت‌کوین، اتریوم و مونرو برای پرداخت و مخفی‌کردن مکان سرورهای زیربنایی خود و هویت مدیران، ناظران و کاربران خود استفاده می‌کرد. [۱۵] از بین این جرایم، رایج‌ترین و شاید پرسودترین جرم مربوط به فروش مواد مخدر و افیونی بود. به‌طوری‌که مدتی بعد از راه‌اندازی سایت، لیستی از مواد مخدر ارائه کردند که بیش از صدها گونهٔ مواد مخدر در این سایت‌ها دسته‌بندی و به فروش گذاشته شد.

پس از مدتی آلفابای به یک بازار بسیار بزرگ تبدیل شد. طبق اطلاعات عمومی موجود در آلفابای قبل از حذف آن، یکی از کارکنان آلفابای ادعا کرد که بیش از ۲۰۰۰۰۰ کاربر و ۴۰۰۰۰ هزار فروشنده در این وب‌سایت ارائه خدمات کرده است[۱۶]. علاوه بر این مبلغ فروش کل روزانهٔ آن در اوایل سال ۲۰۱۷ به بیش از ۶۰۰۰۰۰ یورو رسید. این مبلغ فروش روزانه و تعداد کاربران و فروشندگان یک وب‌سایت مارکت در دارک نت که خدمات مجرمانه ارائه می‌کرده است، به‌تنهایی بیانگر ابعاد تاریک و پنهان جرایم ارتکابی در این بستر را بیان می‌کند.

در نتیجه افزایش تعداد و مقدار جرایم ارتکابی در آلفابای، این وب‌سایت مجرمانه توجه نظام عدالت کیفری کشورهای مختلف را به خود جلب کرد و سرانجام یک عملیات بین‌المللی برای تصرف زیر ساخت‌های آلفابای توسط ایالات متحده رهبری شد و با همکاری آژانس‌های مجری قانون بین‌المللی در عملیات من‌جمله پلیس سلطنتی تایلند، پلیس ملی هلند، اداره پلیس جنایی لیتوانی، پلیس سواره سلطنتی کانادا، آژانس جنایی ملی بریتانیا، پلیس ملی فرانسه و یوروپل همراه بود. در ۵ جوالی ۲۰۱۷ الکساندر کازِز[۱۷] که یک شهروند ۲۵(بنابه برخی منابع ۲۶) ساله کانادایی ساکن تایلند بود، توسط مقامات تایلندی از طرف ایالات متحده به دلیل نقش خود به عنوان مؤسس و مدیر آلفابای دستگیر شد. در ۱۲ جولای کازِز ظاهراً زمانی که در تایلند در بازداشت بود، جان خود را از دست داد[۱۸]. در ۱۹ جولای دفتر دادستانی ایالات متحده در ناحیهٔ شرقی کالیفرنیا، شکایتی را علیه الکساندرکازِز و دارایی‌های همسرش که در سراسر جهان، از جمله در تایلند، قبرس، لیختن اشتاین و آنتیگوآ و باربودا واقع شده‌اند به ثبت رساند.

کازز و همسرش دارایی‌های بسیار با ارزش از جمله وسایل نقلیهٔ لوکس، اقامتگاه‌ها و یک هتل در تایلند جمع‌آوری کردند. کازِز همچنین میلیون‌ها دلار ارز رمزنگاری شده در اختیار داشت که توسط FBI و ادارهٔ مبارزه با مواد مخدر ضبط شده است[۱۹].

۳-۴- فرار مالیاتی با استفاده از رمزارزها

---

[۱۵] United States, Department of Justice Office of Public Affairs, Alphabay, The Largest Online 'Dark Market,' Shut Down, ۲۰ July ۲۰۱۷.

[۱۶] https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down, (accessed: ۱۶ December ۲۰۲۱).

[۱۷] Alexandre Cazes.

[۱۸] United States, Department of Justice Office of Public Affairs, Alphabay, The Largest Online 'Dark Market,' Shut Down, ۲۰ July ۲۰۱۷.

[۱۹] Law Library of Congress, U.S... Global Legal Research Directorate. Regulation of Bitcoin in Selected Jurisdictions, Washington, D.C.: Law Library of Congress, ۲۰۱۴. Pdf. https://www.loc.gov/item/۲۰۱۴۴۲۷۳۶۰/.

بزرگ‌ترین عیب رمزارزها مشخص نبودن هویت طرفین معامله است؛ بنابراین، می‌توان از این فرصت استفاده کرد و بسیاری از فعالیت‌های غیرقانونی از جمله فرار مالیاتی را محقق ساخت، مثلاً مواردی وجود دارد که نشان می – دهد چندین پزشک برای فرار از مالیات، درآمد خود را در قالب رمزارزها پنهان می‌کرده‌اند. کافی است شخص صرفاً با ذخیرهٔ یک کلید خصوصی بیت‌کوین، به صورت آنلاین و ناشناس، به‌راحتی سرمایهٔ خود را پنهان کند، مقادیر زیادی ارز را بدون برخورد با منطقه‌های بازرسی مرزی به کشور وارد یا خارج کند. (Blockchain,۲۰۲۲,۲۰)

در فقدان مقررات قانونی و جلوگیری از فرار مالیاتی، در بعضی از کشورها مانند ایالات متحده، رمزارزها به عنوان دارایی‌های سرمایه‌ای مشمول مالیات طبقه‌بندی می‌شوند، نه ارز. در ۲۵ مارس ۲۰۱۴، ادارهٔ خدمات درآمد داخلی ایالات متحده دستورالعملی صادر کرد که بیت‌کوین نه به عنوان ارز، بلکه به‌مثابه دارایی در نظر گرفته شود (Sapovadia, ۲۰۱۵, ۲۵۳-۲٦٦). برخی از نویسندگان معتقدند که تعیین نرخ مالیات بر درآمد یا دارایی حاصل از رمزارزها، به‌خودی‌خود به آنها مشروعیت قانونی نمی‌بخشد (Sayantani,۲۰۲۱,۵۷). درهرصورت مالیات‌دهندگان ایالات متحده موظف‌اند تراکنش‌های مربوط به ارزهای دیجیتال را به دلار آمریکا در اظهارنامهٔ مالیاتی سالانهٔ خود گزارش دهند. این الزام به این معنی است که مالیات‌دهندگان باید معادل ارزش دلاری رمزارزهای خود را در تاریخ معامله معین کنند. البته گزارش صحیح ارزش دلاری رمزارزها به دولت برای مالیات‌دهندگان بسیار سخت است؛ زیرا آنها باید قیمتی را که ارزهای رمزنگاری شدهٔ خود را خریده و فروخته‌اند، ثبت کنند. اما وقتی نرخ رمزارزها به‌شدت در حال نوسان است، چگونه می‌توان مالیات را با نرخ صحیح پرداخت کرد؟!.

اتحادیه اروپا بیان کرده است که مالیات بر ارزش‌افزوده برای کالاها و خدمات در خصوص تبدیل بیت‌کوین به ارز سنتی قابل‌اعمال نیست. البته مالیات بر ارزش‌افزوده برای کالاها و خدمات و سایر مالیات‌ها (مانند مالیات‌بردرآمد) همچنان برای تراکنش‌های انجام شده با استفاده از بیت‌کوین برای کالاها و خدمات اعمال می‌شود.

طبق گزارش بانک مرکزی اروپا، مقررات سنتی در بخش مالی برای بیت‌کوین قابل‌اجرا نیست؛ زیرا فاقد ارکان و بازیگران معاملات سنتی است (Szczepański,۲۰۱٤,۹). دیوان دادگستری اتحادیه اروپا در اکتبر ۲۰۱۵ چنین رأی داده است: «تبادل ارزهای سنتی برای واحدهای ارز مجازی بیت‌کوین از مالیات بر ارزش افزوده معاف است». به گفتهٔ قضات، نظر به این که بیت‌کوین به عنوان وسیله پرداخت تلقی می‌گردد، لذا مالیات به آن تعلق نمی‌گیرد (Bodoni,۲۰۱۵, ۳٤). در ژوئیه ۲۰۱۴، سازمان بانکداری اروپا به بانک‌های اروپایی توصیه کرد تا زمانی که یک رژیم نظارتی برقرار نشده است، با ارزهای مجازی مانند بیت‌کوین معامله نکنند[۲۰]. در سال ۲۰۱۶ پیشنهاد پارلمان اروپا برای تشکیل کارگروهی برای نظارت بر ارزهای مجازی برای مبارزه با پول‌شویی و تروریسم تصویب و برای بررسی به کمیسیون اروپا ارسال کرد[۲۱].

---

[۲۰] European Central Bank (October ۲۰۱۲). Virtual Currency Schemes (PDF). Frankfurt am Main: European Central Bank. ISBN ۹۷۸-۹۲-۸۹۹-۰۸٦۲-۷.
https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes۲۰۱۲۱۰en.pdf/ "EBA Opinion on 'virtual currencies'" (PDF). European Banking Authority. ٤ July ۲۰۱٤. p. ٤٦. Retrieved ۸ July ۲۰۱٤.

[۲۱] "MEPs call for virtual currency watchdog to combat money laundering and terrorism - News - European Parliament". Europarl.europa.eu. ۲۶ May ۲۰۱۶. https://www.europarl.europa.eu/news/en/press-room/۲۰۱۶۰۵۲۴IPR۲۸۸۲۱/meps-call-forvirtual-currency-watchdog-to-combat-money-laundering-and-terrorism.

۳-۵- کلاهبرداری با استفاده از رمزارزها

افزایش روزافزون کاربران ارزهای رمزنگاری شده از دیدگاه مجرمان، افزایش قربانیانی هستند که می‌توانند مورد بزه‌دیدگی واقع شوند؛ چرا که بسیاری از این اشخاص، کسانی هستند که اطلاعات کافی در خصوص کارکرد این ارزها ندارند و صرفاً این پدیدهٔ نوظهور را یک موقعیت اقتصادی تلقی می‌کنند تا بتوانند سرمایهٔ خود را افزایش دهند، غافل از این که یک غفلت و ناآگاهی می‌تواند تمام سرمایهٔ آنها را از بین ببرد. چرا که درآمیخته شدن ویژگی‌های منحصر به فردی که ارزهای رمزنگاری شده دارند با فضای سایبر؛ امکان انجام عملیات متقلبانهٔ گوناگون را به بزهکاران فرآهم می‌آورد تا با فریب و اغفال اشخاص، اموال و دارایی آنها را تصاحب کنند. متداول‌ترین و رایج‌ترین روش‌هایی که بزهکاران برای ارتکاب جرم کلاهبرداری در بستر ارزهای رمزنگاری شده به آن متوسل می‌شوند عبارت اند از: کلاهبرداری در سرمایه‌گذاری، کلاهبرداری از طریق طرح‌های پمپ و تخلیه و کلاهبرداری از طریق طرح‌های پانزی، هرمی و پرامیدی که در ذیل به تجزیه و تحلیل این موارد پرداخته می‌شود. با افزایش محبوبیت بیت‌کوین و موفقیت کلی آن در تبدیل شدن به یک ارز جهانی، اشخاص بیشتری به سمت استفاده از ارزهای رمزنگاری شده کشیده شدند. با وجود اینکه در حال حاضر بیت‌کوین شناخته شده‌ترین رمزارز است، لیکن به دلیل قیمت بالای آن بسیاری از کاربران قادر به سرمایه‌گذاری بر بیت‌کوین نیستند، همین امر موجب شده است تا عده‌ای در صدد آزمایش رمز ارزهای جدید و کمتر شناخته شده باشند، تا شاید در آینده همانند بیت‌کوین ارزش آن افزایش پیدا کند و در نتیجه سرمایه‌شان چند برابر شود. این موضوع از دید افراد سود جو پنهان نمانده است، لذا به ایجاد ارزهای رمزنگاری شدهٔ جدید روی آورده‌اند. سازندگان این ارزها با اطلاعات واهی و تغییر در داده‌های ارزها (مثلاً با صعودی نشان دادن سیر ارزش رمزارز)، آنها را ارز آینده معرفی می‌کنند و با ارزش تر از آن چیزی که هستند جلوه می‌دهند. کاربران عادی که قصد سرمایه‌گذاری در بستر مبادلات ارزهای رمزنگاری شده را دارند چنین ارزها را به مثابه یک فرصت سرمایه‌گذاری تلقی می‌کنند و به این امید که در آینده این ارزها نیز به ارزشی مشابه ارزش بیت‌کوین خواهد رسید، اقدام به خرید سهام می‌نمایند. پس از به دام افتادن کا ربران، بنیان‌گذاران ارز رمزنگاری شده با اعمال نقشه‌های متفاوت اقدام به خارج کردن تمام پول سرمایه گذاران می‌کنند. آنگاه ارزش سهام ارزهای خریداری شده توسط کاربران به صفر می‌رسد. در نتیجه سرمایه گذاران می‌مانند و سهام فاقد ارزش و پولی که توسط کلاهبرداران فاقد هویت واقعی، از دست رفته! در این روش گاهاً سرمایه گذار تا مدت‌ها متوجه نمی‌شود که بزه دیده واقع شده است و مدت‌ها منتظر می‌ماند تا سهام ارز رمزنگاری شده‌ای که خریده است با ارزش شود.

روش دیگر کلاهبرداری در رابطه با سرمایه‌گذاری در ارزهای رمزنگاری شده مربوط به عملیات کیف پول دیجیتال است. به‌عنوان‌مثال سایت‌های جعلی با استفاده از تبلیغات گسترده در وسایل ارتباط‌جمعی و فضای سایبر سعی می‌کنند که اعتماد مردم را کسب کنند تا با دریافت مبالغ و اطلاعات لازم، برای این اشخاص اقدام به ایجاد حساب کاربری کنند؛ سپس بنیان‌گذاران و گردانندگان این سایت‌های جعلی با دریافت پول ناپدید شده و کیف پولی نیز تحویل داده نمی‌شود یا در صورت تحویل کیف پول دیجیتال، اطلاعات مربوط به کیف پول خصوصی را در اختیار خود نگه می‌دارند و در اولین واریز ارز به کیف پول مزبور، اقدام به هک یا برداشت خودکار مبالغ موجود در کیف پول می‌نمایند (ایزدی و ارزانیان، ۱۳۹۸، ۴۵-۴۶).

روش دیگر کلاهبرداری، کلاهبرداری با وعدهٔ سرمایه‌گذاری است. در این روش برخی اشخاص خود را متخصص در موضوع ارزهای رمزنگاری شده معرفی کرده و ادعا می‌کنند که می‌توانند نبض بازار ارزهای رمزنگاری شده را در دست بگیرند و کنترل کنند؛ لذا از مرم دعوت می‌کنند تا پول‌هایشان را برای سرمایه‌گذاری به آنها بسپارند؛ و بعد از مدت معینی (مثلاً شش ماه) سه برابر پولشان را سود کنند. کلاهبرداران در ابتدا در قبال این کار درصدی از سود را به عنوان پورسانت طلب می‌کنند؛ اما بعد از گرفتن پول سرمایه گذاران، کل سرمایه آنها را به تاراج می‌برند.

۴- روش‌های بازدارندگی از تجارت سیاه با استفاده از رمزارزها

پس از بررسی مصادیق تجارت سیاه و جرائمی که با استفاده از رمزارزها ارتکاب می‌یابند، در این نوشتار به بررسی برخی از روش‌های بازدارنده در زمینهٔ تجارت سیاه با استفاده از رمزارزها که شامل مواردی نظیر: استفاده از قراردادهای هوشمند، لزوم قانونی رمزارزها در نظام‌های داخلی، لزوم پیشگیری از جرایم ارتکابی در بستر ارزهای رمزنگاری شده، تقویت همکاری‌های بین‌المللی و تقویت سازوکارهای گزارش دهی و شفافیت در بانک‌ها و صرافی‌ها می‌گردد، خواهیم پرداخت.

۴-۱- استفاده از قراردادهای هوشمند

بیت‌کوین، بلاک‌چین و قراردادهای هوشمند اصطلاحاتی هستند که با افزایش فزاینده در مطبوعات بانکی و مالی مواجه شده‌اند. فناوری بلاک‌چین که مبنای ارز دیجیتال بیت‌کوین می‌باشد، به طور گسترده‌ای برای حل برخی از مشکلات دیرینه و به‌ظاهر قابل‌حل، مانند کاهش هزینه‌های معامله، سرعت پردازش، گسترش خدمات مالی و توانمندسازی مصرف‌کنندگان مورداستفاده قرار می‌گیرد (Tapscott Tapscott and , ۲۰۱۷, ۲۰-۱۷).

انعقاد قراردادهای هوشمند از لحظه انجام مذاکرات مقدماتی تا امضای قرارداد توسط طرفین، تحت نظارت هوش مصنوعی انجام می‌گیرد. هوش مصنوعی مطابق با دستورالعمل داده شده، مفاد قرارداد را تجزیه و تحلیل و در صورت مطابقت مفاد قرارداد با پروتکل‌های داده شده، آنها را تأیید می‌کند. تأیید قرارداد توسط هوش مصنوعی به منزله نهایی‌شدن قرارداد است. درصورتی‌که مفاد قرارداد با دستورالعمل داده شده به هوش مصنوعی تطابق نداشته باشد، امکان انعقاد قرارداد نیست. تشریفات امکان انعقاد قراردادهای هوشمند تحت نظارت شدید مراجع صلاحیت‌دار انجام می‌گیرد. متقاضی انعقاد قراردادهای هوشمند باید دو مجوز امضای دیجیتالی و امکان تملک ارزهای رمزنگاری شده دیجیتالی را داشته باشد .

از سال ۲۰۱۷ پس از وجود نوسانات شدید قیمت ارز بیت‌کوین در بازارهای جهانی، کمیسیون حقوق تجارت بین‌الملل سازمان ملل مبادرت به تصویب کنوانسیون یکنواخت سازی معاملات مبتنی بر ارزهای مجازی[۲۲] در جوالی ۲۰۱۷ کرده است. مطابق با مفاد ماده ۲ این کنوانسیون، تخصیص ارزهای رمزنگاری شده به افراد منوط به شناسایی هویت، مایملک

[۲۲] Uniform Regulation Virtual Currency Business Act, July ۲۰۱۷.

و وضعیت حقوقی و حقیقی افراد است. متقاضیان باید نسبت به تقدیم مدارک حاکی از وضعیت حقوقی و ورشکستگی و سوابق حقوقی و کیفری خود به سازمان‌های صلاحیتدار اقدام کنند.

این سازمان‌ها نیز پس از بررسی مدارک و انجام استعلامات لازم نسبت به تخصیص یا عدم تخصیص مجوز به متقاضیان اقدام می‌کنند. این فرایند می‌تواند از وقوع بسیاری از جرایم مانند پول‌شویی دیجیتالی نیز جلوگیری کند (Kiviatt۲۰۱۵, ٥٦)؛ چرا که هویت مالک حقیقی هر ارز و مالکانی که آن را مبادله کرده‌اند مشخص است. امکان تحصیل این ارزها از راه‌های غیرقانونی وجود ندارد؛ چراکه ارز دیجیتالی تا زمانی که از کشور مستخرج یا تولیدکننده آن مجوز ورود به بازارهای جهانی پیدا نکرده و مالک آن مشخص نشده باشد، امکان مبادله نخواهد داشت؛ بنابراین وقوع جرایم مرتبط با این ارزها از جمله پول‌شویی منتفی است.

تشریفات تخصیص امضائات دیجیتالی در کشورهای توسعه‌یافته نیز همین قدر حساس است. افراد در صورتی می‌توانند مجوز استفاده از امضائات دیجیتالی را دریافت کنند که وضعیت حقوقی و سوابق حقوقی و کیفریشان توسط دولت بررسی شده باشد. از این رو، پس از تخصیص این مجوز به افراد، دولت ضامن صحت مبادلات انجام شده توسط دارندگان امضائات دیجیتالی است. این امر یکی از دلایل توسعه امنیت مبادلاتی محسوب می‌شود.

نکتهٔ دیگر اینکه، قراردادهای هوشمند خود اجرا هستند. این ویژگی باعث می‌شود پس از انعقاد قرارداد، قرارداد به صورت خودکار توسط هوش مصنوعی در قالب کدهای رمزنگاری شده به صورت منظم در بلاک‌های زنجیره ذخیره شود. ذخیره این داده‌ها در بستر بلاک‌چین و ارسال رونوشت به رایانه‌های متصل به بستر، متعاملین را از ثبت معاملات خود بی‌نیاز می‌کند. به‌عبارت‌دیگر، ثبت اطلاعات قراردادهای منعقده در این بستر در هر بلاک، در حقوق امریکا به منزله ثبت این اطلاعات در سیستم ثبت است. رونوشت اطلاعات چاپ شده توسط هر رایانه‌ای نیز سندی تلقی می‌شود که رسمیت آن به جهت ثبت در بستر بلاک‌چین رخ می‌دهد.

همچنین، نامتمرکز بودن بستر بلاک‌چین و بهره‌مندی آن از ارزهای رمزنگاری شده، نقل‌وانتقال این ارزها را در انعقاد قراردادهای هوشمند بدون نیاز به واسطه‌های مالی فراهم کرده است (Savelyev,۲۰۱۸,٥٥١)؛ بنابراین برخلاف سایر قراردادهای الکترونیکی که نقل‌وانتقال وجوه باید از طریق واسطه‌های مالی؛ مانند بانک‌ها و مؤسسات مالی (از بانک به حساب فرد) انجام گیرد، انتقال ارزهای رمزنگاری شده از طریق کیف پول دیجیتالی یا ارزهای ذخیره شده در همان بستر بلاک‌چین انجام می‌گیرد. نتیجه این امر، تأثیر نپذیرفتن این قراردادها از ورشکستگی‌های بانکی و انجام سریع‌تر مبادلات تجاری است. همچنین وجوه ذخیره شده در بلاک‌چین امکان سرقت توسط سارقان الکترونیکی را نداشته، از هرگونه تجاوز مصون است. این امر می‌تواند از جمله موارد توسعه امنیت مبادلاتی نیز تلقی گردد (Raskin,۲۰۱۷, ۸۳۳).

مسئلهٔ دیگر این که، انعقاد قراردادهای هوشمند در بستر بلاک‌چین منجر به افزایش امنیت مبادلاتی می‌شود. این بستر متشکل از بلوک‌هایی است که تحت الگوریتم‌های توابع هش ایجاد شده‌اند. ایجاد اخلال در هر بلوک می‌تواند منجر به وجود اخلال در سیستم و شناسایی سریع عامل مخل گردد. ذخیره اطلاعات در هر بلوک در قالب کدهای رمزنگاری شده انجام می‌گیرد. چنین فرایندی منجر می‌شود تا اطلاعات ذخیره شده در هر بلوک غیرقابل‌تغییر باشند (Savelyev,۲۰۱۸,٥٥١)؛ بنابراین امکان انجام حملات سایبری نیز به حداقل می‌رسد. ذخیره هر داده در بلاک‌چین منجر به ارسال رونوشتی از آن به هریک از رایانه‌های متصل به این بستر می‌گردد. این امر نه‌تنها در افزایش شفافیت

مؤثر است؛ بلکه از وقوع تقلب و سوءاستفاده‌های مالی تجار و تبانی در معاملات جلوگیری می‌کند. در شبکه‌های نامتمرکز مانند بلاک‌چین یک هکر نمی‌داند به کدام بلاک برای تغییر محتوای آن ضربه بزند؛ بنابراین اگر به یک بلاک حمله سایبری شود، چون رونوشت محتوای آن به‌تمامی رایانه‌های متصل به شبکه ارسال شده است، محتوا ایمن بوده و عامل مخل نیز به‌سرعت شناسایی و حذف می‌شود (Guegan, ۲۰۱۸, ۵).

۴-۲- لزوم قانونی‌سازی رمزارزها در نظام‌های داخلی

سرقت، کلاهبرداری، قماربازی، خرید و فروش اقلام ممنوعه و نظیر آن از جرایمی هستند که اگر قانونی‌سازی و جرم انگاری صورت نگیرد، امکان ارتکاب آنها در زمینه معامله بیت‌کوین و سایر رمزارزها وجود دارد. با توجه به اصل قانونی بودن جرم و مجازات و دیگر قواعد از جمله اصل برائت و قاعده قبح عقاب بلابیان، در وهله نخست باید جرایم ناشی از ارزهای دیجیتال جرم انگاری شوند (بهره مند و عامری ثانی، ۱۳۹۸، ۱۲۰).

از منظر حقوق‌دانان، قانونی‌سازی، فرایندی است سه‌مرحله‌ای که شامل نظارت بر چگونگی تأسیس بانک یا یک مؤسسه مالی، نظارت بر شیوه فعالیت و بالاخره اعمال اقدامات اصلاحی برای بهبود وضعیت، حمایت یا مجازات بانک متخلف از قبیل تذکر کتبی، تغییر اعضای هیئت‌مدیره و اجبار به تزریق سرمایه توسط سهام‌داران است.

هر چند هزینه نظارت سنگین است، ضعف در نظارت به‌مراتب، هزینه سنگین‌تری خواهد داشت. مهم‌ترین رکن نظارت، حفظ ثبات و اعتبار نظام مالی است؛ زیرا وجود این عوامل سبب کاهش خطر ضرر سپرده‌گذاران و دیگر بستانکاران است. در این زمینه، ناظران در اجرای وظایف خود باید نظم و انضباط بازار را با اعمال حاکمیت شرکتی، از طریق ساختار مناسب و تنظیم قواعد مربوط به مسئولیت هیئت‌مدیره و مدیران ارشد و ارتقای سطح شفافیت مستحکم و تقویت کنند (منظور و بادی پور، ۱۳۸۷، ۸).

۴-۳- لزوم پیشگیری از جرایم ارتکابی در بستر ارزهای رمزنگاری شده

برای مبارزه با جهانی‌شدن جرایم ارتکابی در بستر ارزهای رمزنگاری شده صرف دستگیری مجرمان مانند، دستگیری گردانندگان سایت‌هایی که در قبال بیت‌کوین یا هر نوع ارز رمزنگاری شده دیگر خدمات مجرمانه ارائه می‌دهند کافی نیست؛ چرا که این عمل در مواردی می‌تواند نتیجهٔ عکس بدهد و باعث شناخته‌شدن و افزایش محبوبیت پلتفرم ارائه‌دهندهٔ خدمات مجرمانه شود.

بازار جاده ابریشم که در فوریه سال ۲۰۱۱ (۱۳۸۹) تأسیس شد، این سایت به عنوان محبوب‌ترین برند در بین بازارهای دارک نت محسوب می‌شد (Afilipoaie and Shortis,۲۰۱۵,۱). جاده ابریشم، با سامانهٔ فروش آنلاین از فروشنده تا درب (منزل)، به بزرگ‌ترین بازار تاریک آنلاین تبدیل شد (Ibid). این سایت در قبال بیت‌کوین، خدمات مجرمانه‌ای از قبیل فروش مواد مخدر و سایر محصولات غیرقانونی را ارائه می‌داد (Kethineni and other,۲۰۱۷, ۱۱).

نحوهٔ کار این سایت بدین شرح بود که در گام نخست همهٔ فروشندگان (که غالباً فروشندگان محصولات غیرقانونی بودند) یک فروشگاه در جادهٔ ابریشم راه‌اندازی می‌کردند. این فروشنده برای دسترسی به جاده ابریشم باید خدمات Tor

را دارا می‌بود. جاده ابریشم سیستم رتبه‌بندی پنج‌ستاره برای فروشندگان ایجاد کرد و به مشتریان اجازه داد تا نظرات خود را بنویسند. در این قسمت، مشتریان نظرات خود را در مورد خدمات، تراکنش و ارسال بیان می‌کردند (Ibid).

از آنجایی که بیت‌کوین تنها پرداخت پذیرفته شده در جاده ابریشم بود؛ لذا در مرحلهٔ دوم خریداران باید بیت‌کوین تهیه کرده و نشانی‌ای را برای تحویل آماده می‌کردند. چنانچه اگر خریداران بیت‌کوین نداشتند، می‌توانستند از یک سرویس مبادلهٔ بیت‌کوین برای تبدیل واحد پولی خود به بیت‌کوین استفاده کنند. دو نفر با نام‌های رابرت فایال و چارلی شرم که از فروشندگان بیت‌کوین در جاده ابریشم بودند سرویس انتقال و تبدیل پول را اداره می‌کردند. هنگامی که رابرت فایال سپرده نقدی را از مشتری دریافت می‌کرد، آنها را با بیت‌کوین مبادله می‌کرد و بیت‌کوین‌ها را به حساب مشتری در جاده ابریشم منتقل می‌کرد. او برای نقش خود به عنوان صرافی حق کمیسیون دریافت می‌کرد. خریداران همچنین باید آدرسی را برای دریافت کالای خریداری شده آماده کنند. بسیاری از آنها یک سرویس صندوق پستی را با استفاده از شناسهٔ جعلی انتخاب می‌کردند (Ibid).

مرحلهٔ سوم، مرحلهٔ تحویل و پرداخت است. برای جلوگیری از تحویل کنترل شده، جاده ابریشم دستورالعمل‌های دقیقی را برای کمک به مشتریان خود برای جلوگیری از تحقیقات ارائه کرد. برای اجتناب از (کشف محصولات غیرقانونی ارسالی) در تحقیقات معمول پستی با سگ موادیاب، فروشندگان از کیسه‌های خلأ مهروموم شده و زیپ‌دار استفاده می‌کردند. همچنین جاده ابریشم از یک سیستم امانی خاص استفاده می‌کرد. تحت این سیستم، خریداران بیت‌کوین را از کیف پول خود (به‌وسیلهٔ وب‌سایت) به حساب خود در جاده ابریشم منتقل می‌کردند. زمانی که فروشندگان متوجه می‌شدند که پرداخت انجام شده است، تحویل صورت می‌گرفت. هنگامی که خریداران کالا یا خدمات را دریافت می‌کردند، معامله را تأیید کرده و فروشندگان پرداخت نهایی را دریافت می‌کردند. برای جلوگیری از پرداخت مستقیم خریداران به فروشندگان، اولبریخت و کلارک (راجر توماس کلارک که کارمند اولبریخت بود) قوانینی را تدوین کردند که پرداخت‌های امانی شخص ثالث را ممنوع می‌کرد (Ibid).

تفاوت عمده بین جاده ابریشم و بازارهای دیگر (علی الخصوص بازارهای سنتی) این است که جاده ابریشم بر تضمین ناشناس ماندن فروشندگان و خریداران تا حد امکان تمرکز داشت (Christin,۲۰۱۲,۳). این سایت در طول دوسال و نیم فعالیت خود به فروش ۱,۲ میلیارد دلاری (آن طور که از برخی منابع بر می‌آید در ماهانهٔ جاده ابریشم ۱,۲ میلیون دلار بود) (Ibid). و ادعای ۸۰ میلیون دلار کمیسیون برای صاحب و ناظر خود کسب کرد[۲۳].

FBI در اواسط سال ۲۰۱۱ از وجود این سایت‌ها مطلع شد و تحقیقات خود را آغاز کرد. همچنین سایر آژانس‌های مجری قانون نیز در پایان سال ۲۰۱۱ کار خود را آغاز کردند. در مارس ۲۰۱۲، یک جوان ۲۹ ساله به نام راس اولبریخت در وب سایتی از نام واقعی خود استفاده کرد، تا از او بپرسند که چگونه با استفاده از curl در php می‌توان به یک سرویس مخفی Tor متصل شد؟ او از نام واقعی خود در این پست استفاده کرده بود، اگر چه بعداً نام و آدرس ایمیل خود را نیز تغییر داد. با این حال از طریق این آدرس ایمیل، مجریان قانون بعداً توانستند آن را به کلید رمز گذاری سرور جاده ابریشم متصل کنند. لذا FBI توانست سایت بازار جاده ابریشم را تصرف و مصادره کند. این پایان کار بازار مجرمانهٔ جاده

[۲۳] Global Drug Policy Observatory (GDPO) Situation Analysis, Silk Road and Bitcoin, December ۲۰۱۳, P.۱.

ابریشم نبود و کمی بیش از یک ماه از بسته شدن جاده ابریشم ۱,۰، در تاریخ ۶ نوامبر ۲۰۱۳، جاده ابریشم ۲,۰، راه‌اندازی شد. این سایت جدید توسط اعضای انجمن – های جاده ابریشم ۱,۰ساخته شده است، که FBI در زمان از بین رفتن بازار آن را تصرف نکرد. تا اکتبر ۲۰۱۴، جاده ابریشم ۲,۰، هر ماه ۸ میلیون دلار فروش داشت (Afilipoaie and Shortis,۲۰۱۵,۲-۳).

باید توجه داشت که علی‌رغم عملیات های موفقیت آمیزی که توسط مجریان قانون صورت گرفت، باید به این مهم اشاره کرد که اگر چه این عملیات ها امری ضروری است اما به‌تنهایی کافی نیست و نمی‌توان با صرف دستگیری عاملان و گردانندگان سایت‌ها این ایده و روش مجرمانه را از بین برد. چرا که جرایم ارتکابی در بازارهای آنلاین دارک نت و بستری که ارزهای رمزنگاری شده مهیا ساخته‌اند، همانند تمام بازارها و بسترهای دیگر تابع شرایط عرضه و تقاضا است، و تا زمانی که تقاضا وجود داشته باشد مجرمان به هر روش ممکن عرضه را مهیا می‌کنند. در نتیجه مدیران جدید شکاف‌هایی را که مجریان قانون در بازارهای مجرمانهٔ قبلی شناسایی و نفوذ کرده بودند را دریافته و با نوآوری و تکنولوژی‌های جدید در سایت‌های جدیدی که راه‌اندازی می‌کنند این شکاف‌ها را بسته و راه ورود مجریان قانون را دشوارتر می‌کنند.

همان‌طور که در تمام جنبه‌های دیگر اجرای قانون علیه بازارهای غیرقانونی مواد مخدر نشان‌داده‌شده است، (البته باید گفت که این امر فقط به مواد مخدر محدود نمی‌شود و سایر خدمات مجرمانه را نیز از قبیل فروش اسلحه، فروش بد افزارها و ارائهٔ خدمات هک و... را نیز شامل می‌شود) پیشرفت در ممنوعیت و تعطیلی

بازیگران کلیدی تنها به تکه‌تکه کردن فعالیت‌های پویای بازار کمک می‌کند (Afilipoaie and Shortis,۲۰۱۵,۲-۳)، لذا پس از گذشت مدتی، بازیگران کوچک سعی می‌کنند که بزرگ‌تر شوند و جای آکتورهای اصلی و بزرگ را پر کنند.

نقطه‌ضعف دیگری که در اکتفای صرف به مبارزهٔ کیفری، وجود دارد این است که در چنین روشی مجریان قانون همواره در حالت انفعالی و تدافعی قرار دارد، یعنی همواره یک گام از بزهکاران عقب هستند؛ بدین شرح که باید ابتدا یک بازار مجرمانه تشکیل شود؛ به فروش کالاهای ممنوعه در طیف گسترده‌ای از مناطق جغرافیایی بپردازد، نهایتاً مجریان قانون از وجود این سایت‌ها باخبر شده و در راستای شناسایی عاملان این سایت‌ها قدم بردارند. که این عمل به مثابه نوش داروی بعد از مرگ سهراب می‌ماند. پس ضرورت ایجاب می– کند که در راستای مبارزهٔ جدی‌تر با جرایم ارتکابی در این بستر مجریان قانون حالت تهاجمی‌تر به خود بگیرند. این حالت تحقق نمی‌یابد مگر با اقدامات پیشگیرانه. در واقع اقدامات پیشگیرانه تنها روشی است که می‌تواند مجریان قانون را در قبال بزهکاران یک قدم جلو بیندازد.

۴-۴- تقویت همکاری‌های بین‌المللی

یکی از چالش‌های اصلی پیش روی، جرم‌یابی و تعقیب جرایم ناشی از رمزارزها می‌باشد. عدم سهولت در تعیین حوزهٔ قضایی ای است که جرم در آن واقع شده است. هر چند این مشکل اصولاً در جرایم سایبری وجود دارد، بدین صورت که فرد با استفاد از رایانه و اینترنت می‌تواند در نطقه ای آن سوی کرهٔ زمین مرتکب جرم شود. به عبارت دیگر، فعل مجرمانه در یک حوزهٔ قضایی رخ داده و نتیجه جرم در حوزه ای‌دیگر تحقق می‌یابد. این امر تحقیق و تفحص، تحصیل

دلیل و در نهایت تشخیص دادگاه صالح جهت رسیدگی به جرم را با مشکلات جدی مواجه می‌سازد. به منظور حل این معضل، با توجه به اینکه تراکنش‌های مالی مشکوک به پول‌شویی و یا دلایل و شواهد موجود ممکن از در خارج از قلمرو کشوری باشد که در حال جرم‌یابی می‌باشد، همکاری بین‌المللی اجتناب ناپریر است. رویکرد جهانی به ارزهای رمزنگاری شد لزوماً منفی نبود بلکه آن را دارای فواید اقتصادی زیادی می‌دانند، اما محدودیت‌هایی که در سطح ملی برای یک کشور به‌تنهایی وجود دارد، نیاز به همکاری بین‌المللی را در جهت کاهش استفاده از ارزهای رمزنگاری شده به عنوان ابزاری برای پول‌شویی ضروری می‌سازد، این همکاری‌ها نباید محدودیتی در مسیر استفاد مشروع از این ارزها ایجاد نماید. همکاری های بین‌المللی می‌تواند از مجاری گوناگونی صورت پذیرد که از جمله آنها معاهدات دو یا چند جانبه بین‌المللی و همین طور پیروی از چارچوب‌های پیشنهادی توسط پلیس بین‌الملل به منظور ایجاد هماهنگی و ایجاد وحدت رویه در امر مبارزه با جرایمی که از طریق ارزهای رمزنگاری شده ارتکاب می‌یابند می‌باشد.

۵-۱-۳ تقویت سازوکارهای گزارش دهی و شفافیت در بانک‌ها و صرافی‌ها

هویت طرفین، و مبدأ و مقصد، مهم‌ترین عناصر در مظنون به پول‌شویی قلمدادشدن یک تراکنش مالی هستند. کار گرو اقدام مالی (FATF)، در توصیه‌های چهل‌گانه خود به دنبال ایجاد چهارچوبی به‌منظور ایجاد تعادل میان جلوگیری از ارائه خدمات به مجرمین و از طرف دیگر، جذب مشتری می‌باشد. از سوی دیگر، در خصوص بانک‌ها الزاماتی در کشورهای مختلف وجود دارد که شفافیت تراکنش‌ها را تضمین کرده و مانعی بر سر راه ارتکاب جرایم ناشی از رمزارزها ایجاد می‌نماید.

اما نکته قابل‌توجه اینکه، تبادل ارزهای رمزنگاری شده خارج از سیستم بانکی و در نتیجه دور از دسترس سازوکارهای نظارتی که در این زمینه وجود دارد صورت می‌گیرد. بااین‌حال، با توجه به اینکه زنجیرهٔ بلوکی در دسترس عموم نهادهای ذی‌ربط در امر مبارزه با پول‌شویی است، برخلاف تراکنش‌های صورت‌گرفته از طریق بانک، دستگاه‌های متولی امر، نیازمند همکاری نهادی ثالث همچون بانک نبوده و مستقیماً می‌توانند تبادلات مالی را رصد نمایند. در واقع نهادهای مربوطه بدون هیچ‌گونه محدودیت قانونی و یا مانع از سوی نهادهای ثالث می‌تواند به زنجیرهٔ بلوکی به صورت آزادانه دسترسی داشته باشند و دست‌کم تاریخچه تراکنش‌های مالی را دنبال کنند.

پس هرچند عدم انجام تراکنش‌های مالی ارزهای رمزنگاری شده همچون بیت‌کوین خارج از سیستم بانکی است، اما وجود زنجیرهٔ بلوکی در مورد بیت‌کوین خود یک مزیت محسوب شده و می‌تواند از آن در مسیر جرم‌یابی استفاده کرد. علاوه بر این، صرافی‌ها، بنگاه اصلی خریدوفروش بیت‌کوین است و باید الزامات لازم‌الرعایه در خصوص بانک‌ها در زمینه شفافیت مبادلات مالی در مورد صرافی‌ها نیز به‌دقت اعمال شود.

در ایالات متحد آمریکا یکی از الزاماتی که در خصوص استفاده از فناوری پیشرفته رمزنگاری شده در نظر گرفته شده است این است که باید کلید رمزگشای آن به پلیس فدرال آمریکا ارائه شود (شاملو و خلیلی پاجی، ۱۳۹۹، ۸۵).

۵- نتیجه‌گیری

ارزهای رمزنگاری شده یا دیجیتال که از عمر آنها چند سالی بیش نمی‌گذرد، به صورت گسترده استفاده می‌شوند. امروزه با مطرح‌شدن رمزارزهایی نظیر بیت‌کوین در کشورهای مختلف و استفاده گسترده مردم از آنها، ابهام‌های متعددی در

مورد ماهیت آنها مطرح شده و پذیرش رمزارزها و پول مجازی، موافقان و مخالفانی داشته است که هر یک برای اثبات نظر خود به دلایل متعددی اشاره می‌کنند. از جمله مهم‌ترین تأثیرات ارزهای دیجیتال می‌توان به ماهیت به‌هم‌پیوسته پرداخت‌های صورت‌گرفته به واسطه ارزهای دیجیتال اشاره کرد که ارزهای دیجیتال تحت حمایت دولت می‌توانند برای فعالیت‌های خارج از سیستم‌های جهانی از طرف آن کشور مورداستفاده قرار گیرند. ردیابی فعالیت‌های خارج از نظارت بین‌المللی که از همان کیف پول بیت‌کوین یا هر ارز دیجیتال دیگری سرچشمه می‌گیرد، نشان می‌دهد که چگونه یک بازیگر خارجی می‌تواند از ارز دیجیتالی ملی توسعه‌یافته برای دورزدن تحریم، خریدوفروش تسلیحات نظامی و ایجاد روابط کاملاً دوطرفه بدون دخالت دولت‌های ثالث بهره ببرد. ارزهای دیجیتال البته به گروه‌های تروریستی نیز اجازه افزایش فعالیت‌های غیرقانونی خود را می‌دهند که این موضوع می‌تواند ماهیت منازعات بین‌المللی را تغییر دهند. پول‌شویی، خرید سلاح‌های کشتارجمعی و باج‌گیری از جمله موارد آسیب‌پذیری‌های امنیتی در حوزه ارز دیجیتال هستند.

مصادیق جرایمی که به واسطهٔ رمزارزها و در بستر فضای دیجیتال ارتکاب می‌یابند می‌توان به مواردی نظیر: پول‌شویی، تأمین مالی تروریسم، فرار مالیاتی، باج‌گیری اینترنتی، کلاهبرداری اینترنتی و... اشاره نمود. از جمله مهم‌ترین راهکارها و سازوکارهای مقابله با این قبیل جرایم که با استفاده از رمزارزها ارتکاب می‌یابند می‌توان به مواردی نظیر: استفاده از قراردادهای هوشمند، لزوم قانونی‌سازی رمزارزها در نظام‌های داخلی، لزوم پیشگیری از جرایم ارتکابی در بستر ارزهای رمزنگاری شده و استفاده از راهبردهای پیشگیرانه در این زمینه، تقویت همکاری‌های بین‌المللی و بین دولی توسط کشورها و تقویت سازوکارهای گزارش دهی و شفافیت در بانک‌ها و صرافی‌ها در زمینهٔ مبادلات ارزهای رمزنگاری شده اشاره نمود.

فهرست منابع

۱. ایزدی، زهرا و ارزانیان، نسترن (۱۳۹۸)، پیشگیری از جرائم پول‌شویی و کلاهبرداری در بستر استفاده از رمزارزهای جهانی، فصلنامه رهیافت پیشگیری، دوره دوم، شماره اول.

۲. بهره‌مند، حمید و امیرکیا عامری ثانی (۱۳۹۸)، چالش‌ها و راهکارهای جرم‌یابی پول‌شویی از طریق ارزهای رمزنگاری شده، مجله کارگاه، شماره ۴۶.

۳. چتین، پی یِر لارنت و دیگران (۱۳۹۲)، پیشگیری از پول‌شویی و تأمین مالی تروریسم: راهنمای عملی برای ناظران بانکی، مترجم: مریم کشتکار، چاپ اول، تهران: نشر تاش.

۴. رنگریز، وحید (۱۳۹۷)، خطر پول‌شویی و حمایت مالی تروریسم در ارزهای مجازی، کنفرانس ملی مطالعات نوین اقتصاد، مدیریت و حسابداری در ایران.

۵. شاملو، باقر و خلیلی پاجی، عارف (۱۳۹۹)، سیاست‌گذاری جنایی ریسک مدار در برابر فناوری ارزهای مجازی، فصلنامهٔ مجلس و راهبرد، سال بیست و هفت، شمارهٔ ۱۰۳.

۶. قاسمی، ناصر، فرصت‌ها و تهدیدات ارزهای دیجیتال: مطالعه موردی کشورهای منتخب شرق آسیا، مجله سیاست جهانی، ۱۴۰۰، دوره دهم، شماره ۳.

۷. منظور، داوود و مهدی بادی پور (۱۳۸۷)، نظارت در سیستم بانکی با تکیه بر اصول نظارتی کمیته بال به عنوان ناظر بین‌الملل، نشریه راهبرد، شماره ۱۳.

۸. نجفی ابرندآبادی، علی حسین (۱۳۸۶)، تقریرات درس جرم شناسی (جرم شناسی تروریسم)، دانشکدهٔ حقوق دانشگاه تهران (پردیس قم)، گرد آورنده: امیر باستانی، مهدی نوروزیان، بازبینی: کریم صالحی.

۹. نبوی، سید مهدی و صابر، محمود (۱۳۹۹)، مطالعه تطبیقی چالش‌های نظام عدالت کیفری ایران در دادرسی جرایم مرتبط با ارزهای مجازی، فصلنامهٔ پژوهش‌های حقوق تطبیقی، دوره ۲۴، شماره ۱.