فصلنامه رهیافت پیشگیری/ دورهٔ دوم، شمارهٔ اول، بهار ۱۳۹۸
Prevention Approach Quarterly
Vol. 2, No.1, (Spring 2019)

تاریخ دریافت: ۱۳۹۸/۰۲/۱۰
تاریخ پذیرش: ۱۳۹۸/۰۴/۰۲

مقاله مروری

پیشگیری از جرائم پولشویی و کلاهبرداری در بستر استفاده از رمزارزهای جهانی

زهرا ایزدی[۱] و نسترن ارزانیان[۲]

چکیده

زمینه و هدف: جمهوری اسلامی ایران با ساحتی به نام رمزارزها مواجه شده است که از سویی از ویژگی‌های مثبتی نظیر دور زدن تحریم‌های ظالمانه و جایگزینی به عنوان ارز بین‌المللی در مبادلات جهانی برخوردار است و از دیگر سو در پسِ استفاده از آن، بستر ارتکاب جرم‌هایی همچون، کلاهبرداری و پولشویی فراهم شده است. درخور توجه است که پدیده رمزارزها از بستری مشهور به زنجیره‌های بلوکی متولد شده که برای تولید و انتشار وامدار آن هستند. تاکنون قانون‌گذاری در این راستا صورت نپذیرفته و آخرین اقدام مقنن تنها سند الزامات و ضوابط حوزه رمزارزهای بانک مرکزی در بهمن ماه ۱۳۹۷ است که کافی نیست زیرا بانک مرکزی، رمزارز جهانی نظیر بیت‌کوین و آلت‌کوین را از موضوع سند یادشده خارج کرده است. همچنین در فضای سایبر و فناوری رمزارز، نظارت، رصد حاکمیتی و صیانت از حقوق شهروندان مستلزم وجود قوانین و سازوکارهایی بروز و کارآمد است.

روش: پژوهش حاضر از نظر هدف کاربردی و گردآوری اطلاعات آن به صورت کتابخانه‌ای است که بر اساس نظرات حقوقی و فنی بوده و تمام این موارد از میان کتب، مقالات علمی و مراجعه به پایگاه‌های اینترنتی قابل دسترس انجام شده است.

یافته‌ها و نتایج: مصادیق متعددی از جرائم کلاهبرداری و پولشویی در بستر استفاده از رمزارزها قابلیت ارتکاب دارند. به طور نمونه سایت‌های جعلی با استفاده از تبلیغات گسترده در فضای مجازی سعی در کسب اعتماد مردم می‌کنند تا آن‌ها با پرداخت مبالغی، برای آنها حساب کاربری و کیف پول دیجیتالی ایجاد کنند. بنابراین شیوه‌های پیشگیری وضعی و اجتماعی، برای مقابله با جرائم کلاهبرداری و پولشویی در مبادلات رمزارزها قابل طرح است؛ پیشنهاداتی نیز ازجمله آگاه‌سازی کاربران از گذر برگزاری کلاس‌های آشنایی با رمزارزها و همچنین فیلترینگ سایت‌های مشکوک به ارتکاب فعل مجرمانه مطرح شد.

کلیدواژه‌ها: رمزارز، جرم پولشویی، جرم کلاهبرداری، پیشگیری از جرم، صرافی‌های رمزارز.

❑ **استناد:** ایزدی، زهرا و ارزانیان، نسترن. (۱۳۹۸). پیشگیری از جرائم پولشویی و کلاهبرداری در بستر استفاده از رمزارزهای جهانی. *فصلنامه رهیافت پیشگیری*، ۲(۱)، صص ۳۷-۵۶.

۱. کارشناس ارشد حقوق. دانشگاه علوم قضایی و خدمات اداری تهران. (نویسنده مسئول). رایانامه: zahraa.izadii@gmail.com
۲. کارشناس ارشد حقوق. دانشگاه علوم قضایی و خدمات اداری تهران. رایانامه: arzanian72@gmail.com

مقدمه

رمزارزها[1] مفهومی بدیع در ادبیات فنی حقوقی ایران و حتی جهان به شمار می آیند که از فناوری رمزنگاری بهره برده و در سال ۲۰۰۹ مدل اولیه آن، با نام بیت کوین طراحی و به جهان معرفی شد. رمزارزها به عنوان مفاهیم بدیع و نو در کنار ویژگی‌های برتری همچون دور زدن تحریم‌های ظالمانه و جایگزینی به عنوان ارز بین المللی در مبادلات جهانی، از نقطه ضعف ایجاد بستر ارتکاب جرائم مختلف به علت ناشناخته بودن نیز برخوردارند. از این رو پیشگیری از وقوع جرائمی که در بستر تبادلات آن ممکن است رخ بدهد، بکارگیری رویکردی جامع را اقتضاء می کند تا حاکمیت با به کارگیری تدابیر ویژه‌ای مبتنی بر پیشگیری، ضمن مجازات و اصلاح، به تقابل با هنجارشکنان این حوزه بپردازد. مبرهن است که مبادلات رمزارزها در مرزهای حاکمیتی گسترش یافته است؛ مانند درگاه‌های پرداخت اینترنتی در کشور که گاهی در کنار پرداخت از طریق کارت‌های اعتباری بانک‌های مختلف روش پرداخت به وسیله بیت کوین نیز اضافه شده است. بنابراین ضرورت دارد تا مفاهیم بدیع که نیازمند تبیین مفهومی و همراه با آن بررسی تقنینی و جرم انگاری جرائم مرتبط با این حوزه هستند، بررسی شوند. بر این اساس، پرسش پژوهش حاضر این است که دو جرم پولشویی و کلاهبرداری در بستر استفاده از رمزارزها چگونه انجام می گیرند و راهکار پیشگیری از وقوع آن‌ها چیست؟

پیشینه: با عنایت به موضوع پژوهش، با وجود فراوانی پژوهش‌های فنی در این حوزه، پژوهشی جامع و کامل در حوزه حقوقی و کیفری به چشم نمی‌خورد. شایسته است که در این میان به مقاله روشن و همکاران (۱۳۹۷) اشاره کرد که پس از بررسی ویژگی‌ها و وضعیت فقهی و حقوقی بیت کوین به این نتیجه رسیده است که کارکردهای پول سنتی را داراست و با تصویب قوانینی کارآمد می‌توان آن را در جامعه اقتصادی جمهوری اسلامی ایران به رسمیت شناخت. افزون بر آن مقاله ارزانیان (۱۳۹۶) نیز پس از بررسی ابعاد فنی رمزارزها به نتایجی دست یافته که شرح آن بدین مضمون است: رمزارزها مطابق با مواد دو تا چهار قانون تجارت الکترونیک مصوب ۱۳۸۱ قابل تطبیق با مصادیق قانون نامبرده خواهد بود و پژوهش دوریس[2] (۲۰۱۶) به بررسی رمزارزها به ویژه بیت کوین پرداخته و آینده اقتصادی آن را با آمار و

1. Cryptocurrency
2. Devries

ارقام مورد بررسی قرار داده است. همچنین پژوهش موبوندا[1] (۲۰۱۸) رمزارزها را مورد بررسی قرار داده و درصدد اثبات اینکه رمزارزها ابزار تسهیل کننده جرم به ویژه پولشویی هستند، برآمده است. در نتایج این پژوهش آمده است که بیت کوین و فضای سایبر به گونه‌ای عمل کرده است که جرم پولشویی روند رو به رشد داشته باشد. بنابراین پژوهش حاضر از نظر بررسی رمزارزها به عنوان ابزار ارتکاب جرم به صورت موردی جرائم پولشویی و کلاهبرداری درخور توجه است.

مبانی نظری: زنجیره بلوکی[2] فناوری رمزنگاری شده است که هسته مرکزی سوابق الکترونیکی رمزارزها، را راهبری می‌کند. برخی بر این باورند که زنجیره بلوکی به عنوان بستر رمزارزها، ابتکاری است که در سال ۱۹۹۱ میلادی توسط استوارت هابر و اسکات استورنتا از آن رونمایی شد و پس از آن ویدای در سال ۱۹۹۸ در تارنمای خود از ایده‌ای به نام رمزارزها با هدف تسهیل کارها و حذف پول فیزیکی سخن می‌گوید (سلیمانی پور و سلطانی‌نژاد و پورمطهر، ۱۳۹۶، ص ۱۷۰)، اما جرقه نهایی ایده نامبرده به وسیله شخصی نامعلوم به نام ساتوشی ناکاماتو در سال ۲۰۰۸ کلید خورد (ارزانیان، ۱۳۹۶، ص ۲).

بلاک‌چین دفتر کل توزیع شده است که سوابق کلیه تراکنش‌های مالی و غیر مالی را در خود جای داده و از آنها صیانت می‌کند (آذرنیوار، ۱۳۹۷، ص ۱۱). اطلاعات اعم از اسناد مالکیت، بیمه‌نامه‌ها، بارنامه‌ها و هر داده اطلاعات دیگری می‌توانند باشند (بالفنون، ۱۳۹۶، ص ۴). این فناوری از ویژگی‌هایی چون عدم تصرف داده‌ها و غیر متمرکز بودن، بهره می‌برد. غیر متمرکز بودن به این معنی است که داده‌ها در یک پایگاه مرکزی و کانونی نگهداری نمی‌شوند (لیخوتا[3]، ۲۰۱۷، ص ۳۰). زیرا اطلاعات تراکنش رمزارز در دسترس عموم بوده و پس از تأیید جمیع کاربران زنجیره بلوکی، در دسترس همگان قرار خواهد گرفت (امری[4]، ۲۰۱۵، ص ۳۹). به همین دلیل است که تعامل با بانک به طور کامل حذف شده است. تراکنش‌های رمزارزها به پرداخت نظیر به نظیر یا همتا به همتا، به عنوان تراکنش بی‌واسطه نیز شهرت دارد و نقش بانک‌ها در چنین فناوری بسیار کمرنگ شده است. بنابراین رمزارز، پولی بدون پشتوانه و بر پایه پروتکل رمزنگاری شده است که توسط هیچ نهاد یا سازمانی مانند بانک مرکزی تولید و منتشر

1. Mabunda
2. Blockchain
3. Likhuta
4. Omri

نمی‌شود و تنها با حل معادلات پیچیده ریاضی یا با عملیات استخراج (ماینینگ)[1] به منصه ظهور رسیده است (سلیمانی پور و سلطانی‌نژاد و پورمطهر، ۱۳۹۶، ص ۱۷۰)[2]. طرفین در زمان انتقال و معامله رمزارز نیازی به افشای هویت واقعی خود ندارند و این مسئله اولین زنگ خطر ارتکاب جرم در اینگونه معاملات خواهد بود. با عنایت به ماده ۲ قانون تجارت الکترونیک مصوب ۱۳۸۱ بند ز این قانون، سیستم اطلاعاتی، سیستمی برای تولید (اصل سازی)، ارسال، دریافت، ذخیره یا پردازش داده پیام است. در خصوص سیستم اطلاعاتی مطمئن، در بند ح ماده یادشده به چهار ویژگی محفوظ بودن در برابر سوءاستفاده و نفوذ، قابلیت دسترسی و تصدی صحیح و پیکربندی و سازماندهی متناسب اشاره شده است.

بنابراین فناوری بلاک‌چین در قالب حقوقی، همان سیستم اطلاعاتی مطمئن در قانون تجارت الکترونیک است. در ادامه ماده [2] طبق تعریفی که از سیستم اطلاعاتی و سیستم اطلاعاتی مطمئن شده است، دامنه وسیعی از ابزارهای فنی برای ارسال، دریافت و ذخیره اطلاعات و سوابق الکترونیکی را شامل می‌شود، که این ابزارهای فنی، پست الکترونیکی یا ماشین فکس می تواند باشد (حبیب‌زاده، ۱۳۹۰، ص ۲۱۰). بند الف این ماده داده پیام[3] را تعریف می کند و آن را هر نمادی از واقعه، اطلاعات یا مفهوم می‌داند که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود. با عنایت به تعریف قانون تجارت الکترونیک آنسیترال[4] و تجارت الکترونیک ایران، داده پیام علاوه بر اطلاعات، شامل سوابقی که از طریق ابزارهای رایانه‌ای تولید شده نیز می‌شود (حبیب‌زاده، ۱۳۹۰، ص ۲۲۲). بنابراین یکی از مصادیق داده پیام‌ها در این بند، همان رمزارزها هستند.

جرم کلاهبرداری: در کتب لغت کلاهبرداری به معنای فریب دادن یا ربودن پول و مال کسی از طریق حیله معنا شده است (معین، ۱۳۷۵، ص ۳۰۲۳-۳۰۲۴). عنصر قانونی جرم کلاهبرداری سنتی در ماده اول قانون تشدید مجازات مرتکبان ارتشاء و کلاهبرداری آمده است، اما مقنن تعریفی از جرم یادشده ارائه نکرده و تنها به بیان تعدادی از مصادیق کلاهبرداری اکتفا کرده است. به طور کلی می توان آن را توسل به حیله یا وسایل متقلبانه برای اغفال فرد و بردن مالش دانست (میرمحمد صادقی، ۱۳۹۵، ص ۵۶). در ضمن

---

1. Mining

۲. برای مطالعه بیشتر بنگرید به: نوری، مهدی و نواب پور، علیرضا. (۱۳۹۷). طراحی چارچوب مفهومی سیاستگذاری ارزهای مجازی در اقتصاد ایران. فصلنامه سیاستگذاری عمومی دانشگاه تهران، ۳(۴)، صص ۵۱-۷۸.

3. Data Message

4. Uncitral

رکن قانونی جرم کلاهبرداری رایانه‌ای در ماده ۶۷ قانون تجارت الکترونیک و همچنین ماده ۱۳ قانون جرائم رایانه‌ای آمده است که آن را می‌توان، به دست آوردن متقلبانه مال دیگران با استفاده از ابزار رایانه دانست. با بررسی دو تعریف ارائه شده می‌توان گفت؛ از جمله تفاوت‌های کلاهبرداری سنتی و رایانه‌ای محیط ارتکاب این دو است. البته ناگفته نماند که کلاهبرداران می‌توانند از رایانه هم برای کلاهبرداری سنتی و هم برای کلاهبرداری رایانه‌ای بهره ببرند.

جرم پولشویی: رکن قانونی جرم پولشویی ماده ۲ قانون مبارزه با پولشویی مصوب ۱۳۹۷/۷/۳ است که مطابق آن: «پولشویی عبارت است از: الف) تحصیل، تملک، نگهداری یا استفاده از عواید حاصل از ارتکاب جرائم با علم به منشأ آن؛ ب) تبدیل، مبادله یا انتقال عوایدی به منظور پنهان یا کتمان کردن منشأ مجرمانه آن با علم به این که به‌طور مستقیم یا غیر مستقیم از ارتکاب جرم به دست آمده یا کمک به مرتکب جرم منشأ به نحوی که مسئول آثار و تبعات قانونی ارتکاب آن جرم نشوند و پ) پنهان کردن یا کتمان کردن منشأ و منبع، محل، نقل و انتقال، جابه‌جایی یا مالکیت عوایدی که به طور غیر مستقیم یا مستقیم در نتیجه ارتکاب جرم تحصیل شده باشد». به عبارت دیگر پولشویی جرمی است که در آن مرتکب منشأ درآمدهای ناشی از جرم را پاک می‌کند و با پاک وانمود کردن آن، یافتن منبع اصلی آن را بسیار دشوار یا غیرممکن می‌سازد. نکته آخر اینکه در نوع سایبری پولشویی، از اینترنت برای مخفی کردن یا قانونی جلوه دادن پول حاصل از روش‌های نامشروع استفاده می‌شود.

پولشویی و کلاهبرداری در بستر استفاده از رمزارزها: در عصر حاضر فضای سایبر ابزار تسهیل کننده جرم پولشویی قرار گرفته و با وجود آن به گسترش چشمگیر و روزافزون پدیده نامبرده کمک شایانی کرده است. پولشویی سایبری به ترفندی جدید برای مختل کردن نظام ارزی، نفوذ در کشورها، اختلال در امنیت و مرزهای حاکمیتی، جابه‌جایی دارایی‌های نامشروع و تأمین مالی گروهک‌های تروریستی تبدیل شده است (عباسی، ۱۳۹۶، ص ۵۰).

روش‌های ارتکاب جرم پولشویی در مبادلات رمزارزها: رمزارزها که بر روی بستر زنجیره‌ای بلوکی فعالیت می‌کنند؛ برای نقل و انتقال و هر فعل دیگری نیازمند وجود کیف پول دیجیتال[1] است (کیبین[2]،

1. Digital Wallet
2. Kibin

۲۰۱۶، ص ۵۰)[۱]. کیف پول دیجیتال دارای کلید عمومی و خصوصی است و کلید خصوصی تنها راه ورود به حساب کاربری و کیف پول دیجیتال است. گفته شده است که تراکنش‌های مالی رمزارزها بر روی کیف پول دیجیتال نامعلوم بوده و تنها به صورت سوابقی از اعداد، حروف و علامت‌های نامعلوم قابل مشاهده است که امکان شناسایی هویت اشخاص و تراکنش‌هایشان غیر قابل پیگیری است (ساورایی و پورمسجدیان، ۱۳۹۳، ص ۱۵۴)؛ بنابراین بهترین ابزار برای جرم پول‌شویی و تأمین مالی گروهک‌های تروریستی است (سلیمانی پور و سلطانی‌نژاد و پورمطهر، ۱۳۹۶، ص ۱۷۵)؛ باید گفت استفاده از اعداد، حروف و علامت‌ها برای نمایه‌سازی حساب‌ها و اکانت‌ها در فضای سایبری امری بدیع و نو نیست و آدرس‌ها و سوابق تراکنش‌ها نیز قابل پیگیری و شناسایی است؛ مانند نام دامنه‌های اینترنتی که در آن آدرس‌ها مجموعه‌ای از حروف و اعداد هستند (ساورایی و پورمسجدیان، ۱۳۹۳، ص ۱۵۵). در پاسخ به استدلال اخیر خاطرنشان می‌شود که با استفاده از ابزاری چون TOR[۲] و سرویس ترکیب تراکنش بیت کوین می‌توان ردیابی و رصد تراکنش‌ها و سوابق مالی را غیر ممکن ساخت (مابوندا، ۲۰۱۸، ص ۲ و سات[۳]، ۲۰۱۶، ص ۸۴). بنابراین همانطور که پیشتر اشاره شد، ناشناسی و نامعلوم بودن هویت طرفین در این مبادلات، اولین زنگ خطر ارتکاب جرائم است. افزون بر این‌ها رمزارزهایی ناشناس نیز وجود دارند که امکان پیگیری و رصد آن‌ها به هیچ طریقی امکان‌پذیر نیست (لمیوکس[۴]، ۲۰۱۶، ص ۳۰). از جمله رمزارزهای ناشناس می‌توان به مونرو اشاره کرد که به نسبت بیت کوین و آلت کوین قیمت پایین‌تری نیز دارد. این رمزارز ناشناس از فناوری امضای حلقوی کریپتوگرافیک[۵] بهره می‌برد که ضمن ناشناس ماندن سوابق و تراکنش‌ها؛ بر کیف پول دیجیتال آن نیز نمی‌توان نظارت کرد (سات، ۲۰۱۶، ص ۹۰). برخی از صاحبان حساب‌های کاربری نیز با اجاره دادن حساب خود برای مدت معینی به اشخاص نامعلوم، بستر جرم پولشویی را فراهم می‌سازند. در این میان گسترش فعالیت صرافی‌های زیرزمینی و

---

۱. کیف پول دیجیتال کلیدی‌ترین نقش را در مبادلات رمزارزها ایفا کرده و دارندگان آن با داشتن کلید خصوصی دارایی مجازی خود را مدیریت می‌کنند.

2. The Inion Router

3. Sat

4. Lemieux

5. Cryptography

غیر مجاز رمزارزها به افزایش جرائم مالی همچون پولشویی، سرقت و کلاهبرداری کمک شایانی می کند (کریستین[1]، ۲۰۱۳، ص ۲۹). بدیهی است که هویت نامعلوم و ناشناس صرافی‌های زیرزمینی، عاملی اساسی و تعیین‌کننده، برای فعالیت‌های این چنینی خواهد بود. همچنین دیده شده است که افرادی با تأسیس شرکت‌های خدماتی و استخدام اشخاص در شرایطی خاص مبادرت به پولشویی می کنند، بدین صورت که اشخاصی را به استخدام شرکت در می‌آوردند تا آن‌ها در فضای سایبری اقدام به ایجاد حساب کاربری و رمزارز کنند و کلید خصوصی حساب مربوطه را در اختیار صاحبان شرکت قرار دهند (دینتو[2]، ۲۰۱۸، ص ۲). صاحبان شرکت اقدام به عملیات پولشویی و تطهیر دارایی‌های نامشروع کرده و یا حساب‌های مورد نظر را به مرتکبان حرفه‌ای پولشویی تقدیم می کنند. همین مسئله چالشی است برای افزایش جرم پولشویی و تطهیر دارایی‌هایی که از طریق نامشروع تحصیل می‌شوند. کشف نشدن هویت واقعی، انجام جرم پولشویی را تسهیل می کند و با توجه به آنچه بیان شد؛ در رمزارزها ظرفیت بی‌هویتی بسیار بالاست. لذا افزایش مبادلات بر پایه رمزارزها، گسترش چشمگیر ساحت جرم پولشویی را به دنبال خواهد داشت (بومه[3]، ۲۰۱۵، ص ۲۲۷). به عنوان نمونه رمزارز بیت کوین در راه ابریشم که به صورت بازارچه‌ای در وب‌سایت بلک برای مبادلات غیرقانونی و پولشویی استفاده می‌شد، توسط دولت آمریکا مسدود شد (آنه[4]، ۲۰۱۵، ص ۳۴). البته نهادهای نظارتی و رصدگر تنظیم مقررات و قواعد ضد پولشویی در جهان همانند کشور روسیه، چین، کره شمالی هشدارهای لازم را در راستای پدیده رمزارزها داده و به دنبال تصویب مقررات سختگیرانه در حوزه نامبرده هستند. در ایران سند الزامات و ضوابط حوزه رمزارزهای بانک مرکزی در بهمن ماه ۱۳۹۷ نیز تصویب و انتشار ارزهای جهان‌روا نظیر بیت کوین و آلت کوین به عنوان ابزار پرداخت، در داخل کشور ممنوع است. اما برخی از سایت‌ها در کنار درگاه‌های پرداخت بانکی، از بیت کوین نیز به عنوان ابزار پرداخت به هنگام خرید بهره می‌برند. البته استخراج رمزارز جهان‌روا به عنوان صنعت مطابق با دستورالعملی مبنی بر صدور جواز تأسیس و پروانه بهره‌برداری برای استخراج رمزارز به شماره ۱۰/۵۰۰۹ به تاریخ ۱۳۹۸/۸/۲۹ توسط وزیر صنعت و معدن و تجارت مورد

1. Chiristin
2. Dyntu
3. Bomhe
4. Anne

تصویب قرار گرفت.

در پولشویی سنتی درآمدهای ناشی از فعالیت‌های مجرمانه، ابتدا به بانک‌ها انتقال پیدا می کند تا سالم‌سازی پول ناشی از پولشویی انجام گیرد. پولشویی طی سه مرحله صورت می پذیرد که عبارت‌اند از: مکان‌یابی یا جایگزینی، طبقه‌بندی یا لایه‌بندی کردن و در نهایت یکپارچه‌سازی یا ادغام کردن، که مکان‌یابی با هدف وارد کردن وجه غیر قانونی به گردش مالی انجام می گیرد. در طبقه‌بندی نیز مجرم با تبدیل اموال ناشی از جرم به شکل‌های دیگر سعی در مخفی ساختن یا مبهم جلوه دادن منبع دارد و در آخرین مرحله پول شسته شده توسط مجرم با هدف شناسایی نشدن توسط سازمان‌های صلاحیت‌دار وارد سیستم مالی کشور می‌شود (عباسی، ۱۳۹۶، ص ۱۰۰). یکی از روش‌هایی که به منظور کشف جرم پولشویی سنتی ممکن است صورت بگیرد گزارش واریز نقدی وجوه بیشتر از سقف مقرر است که براساس دستورالعمل مصوب شورای عالی پولشویی تاریخ ۱۳۸۹/۱۱/۲۰ به تصویب رسیده است. با این توضیح که افراد با حضور در بانک‌ها و در صورت پرداخت یا واریز وجوه نقدی بیشتر از سقف مقرر باید فرم گزارش واریز وجوه به صورت نقد را تکمیل و امضا کنند؛ در این فرم اطلاعاتی مانند شناسه ملی، علت پرداخت وجوه به صورت نقد، منشأ پول واریزکننده و صاحب حساب دریافت می‌شود و بانک اطلاعات این فرم را با مدارک مراجعه کننده تطبیق داده و سپس اقدام به واریز یا انتقال وجوه می کند. تمام مؤسسه‌های مالی و بانک‌ها موظف‌اند اطلاعات حساب‌های مشکوک به پولشویی را در اختیار واحدی به نام واحد اطلاعات مالی قرار دهند، تا نسبت به بررسی آن اقدامات لازم انجام گیرد. پرواضح است چنین اقدامی نسبت به مبادلات رمزارزها محال است؛ زیرا چنین سیستمی در استفاده از رمزارزها به‌علت نبود بانک‌ها و سیستم نظارتی، وجود ندارد. بنابراین استفاده از فضای سایبر به علت سرعت بالایی که دارد؛ شست‌وشوی پول را آسان‌تر می کند و پولشویان می‌توانند بدون حسابرسی مالی و قانون‌گذاری، فعالیت‌های مدنظر را انجام دهند.

همچنین یکی از نهادهای صالح برای مبارزه با پولشویی و مفاسد اقتصادی بانک مرکزی است که ناظر بر فعالیت بانک‌ها و مؤسسه‌های مالی اعتباری مجاز است؛ مطابق بند الحاقی سه تبصره ۱۶ ماده واحده بودجه سال ۱۳۹۸ به‌منظور شفافیت تراکنش‌ها و مبارزه با پولشویی و فرار مالیاتی بانک مرکزی مجاز شناخته شده تا ظرف مدت یک ماه پس از اجرایی شدن این قانون حساب‌های بانکی اشخاص حقیقی

فاقد شماره ملی و افراد حقوقی بدون شناسه ملی را مسدود کند. اما در استفاده از رمزارزها مبادلات به صورت همتا به همتا یا نظیر به نظیر است و وجود واسطه به عنوان بانک از این چرخه مالی حذف شده است که وقوع جرم پولشویی را هموار می‌سازد. البته مطابق با سند الزامات و ضوابط فعالیت در حوزه رمزارزهای بانک مرکزی آمده است که صرافی‌های رمزارز ملی ملزم به رعایت قوانین مبارزه با پولشویی و شناسایی مشتریان (KYC) خواهند بود. خرید و فروش رمزارز ملی به صورت فردی تنها در صورت احراز کامل هویت و ردوبدل شدن اطلاعات هویتی و اسناد و اطلاعات مربوط به منشأ منابع مالی یا رمزارز ملی مجاز است و همچنین صرافی‌های رمزارز ملی موظف هستند تا کلیه اطلاعات مربوط به خرید و فروش، مشتریان و همچنین دلایل و منشأ معاملات را ثبت و در صورت درخواست در اختیار بانک مرکزی قرار دهند. اما همانطور که اشاره شد، این مشکل در ارتباط با رمزارزهای جهانی همچنان پابرجاست و به صرف غیر قانونی اعلام کردن این معاملات، از شیوع و گسترش آن در کشور کاسته نخواهد شد و الزامات ارائه شده به وسیله بانک مرکزی در ارتباط با رمزارزهای جهانی متناسب با ماهیت آن، نیز بهتر است صورت پذیرد. زیرا پیش‌بینی می‌شود رمزارز ملی، توفیقات رمزارز جهانی چون بیت کوین را نداشته باشد، درنتیجه مشکلات و بحران‌های پیش رو بیشتر بر روی رمزارزهای جهانی و مشهوری چون بیت کوین و آلت کوین است و مقنن در ارتباط با رمزارزهای جهانی باید کوشش و اهتمام بیشتری انجام دهد.

روش‌های کلاهبرداری در بستر مبادلات رمزارزها: همان‌طور که پیشتر در جرم کلاهبرداری سنتی گفته شد این جرم از کلیدواژه‌های مانور متقلبانه برای اغفال فرد و بردن مال وی تشکیل شده است. کلاهبرداری یکی از جرائم در عصر ارتباطات و فضای سایبر قلمداد شده است. در راستای استفاده از رمزارزها نیز به نظر می‌رسد که می‌توان مرتکب این جرم مالی شد؛ زیرا در فضای سایبر می‌توان به راحتی عملیات متقلبانه انجام داد و از ناآگاهی و نداشتن اطلاعات درست افراد از فناوری‌های نوظهور، سوء استفاده کرد و برای اغفال و بردن اموال آن‌ها گام برداشت. یکی از متداول‌ترین روش‌های کلاهبرداری در رابطه با استفاده از رمزارزها مربوط به عملیات کیف پول دیجیتال است. به طور نمونه سایت‌های جعلی با استفاده از تبلیغات گسترده در فضای مجازی سعی در کسب اعتماد مردم می‌کنند تا با دریافت مبالغ و اطلاعات لازم، برای این افراد اقدام به ایجاد حساب کاربری و کیف پول دیجیتالی کنند؛ سپس صاحبان این سایت‌ها با دریافت پول ناپدید شده و کیف پولی نیز تحویل داده نمی‌شود یا درصورت تحویل کیف

پول، با استفاده از کلید خصوصی که در اختیار دارند در اولین واریز رمزارز به کیف پول مزبور، اقدام به برداشت خودکار آن می کنند.

روش مشابه دیگری نیز وجود دارد که سایت‌های کلاهبرداری ادعا می کنند که در ازای دریافت وجه، آن‌ها به استخراج رمزارزها پرداخته و درصد بسیار کمی از رمزارز تولید شده را به عنوان حق‌الزحمه دریافت می کنند. از فعالیت‌های مشابه می توان به گروه پشتیبانی جعلی در فضای سایبری اشاره کرد که با ارسال پیامی اعلام می کنند که در صورتی که شما در حساب کاربری خود یا در سایت‌های رمزارزها فعالیت می کنید؛ گروه پشتیبانی سایت آماده خدمت‌رسانی به شماست که بیشتر این پیام‌ها دارای مقاصد منفی هستند. همچنین نام‌دامنه‌هایی جعلی با آدرس‌های تقریباً مشابه نام‌دامنه‌های استخراج رمزارزها به وجود آمده‌اند تا بیشترین سوءاستفاده را از کاربران این حوزه کنند. رواج سایت‌هایی با محتوای مجرمانه بیگ والت با دامنه ri از جمله سایت‌های ایرانی پرطرفدار است و بیشتر محتویات آن در رابطه با رمزارزها مجرمانه است (گروه نقد و بررسی، سایت ارز دیجیتال).

همچنین عملیات ماینینگ یا استخراج رمزارزها که پیشتر به آن اشاره شد نیازمند هزینه‌های سرسام‌آوری چون قیمت برق مصرفی بسیار بالا و سیستم‌های پردازشی پیشرفته و قدرتمند است (نوری و نواپ پور، ۱۳۹۷، ص ۳۰)؛ بنابراین کلاهبرداران حرفه‌ای فرصت و ناآگاهی افراد را غنیمت شمرده و تبلیغات گسترده‌ای چون استخراج رمزارزها را با سودهای کلان و تضمینی اعلام می کنند. در این میان طرح‌هایی با نام طرح درمی و پانزی نیز در حال گسترش هستند که طرح‌هایی با مقاصد کلاهبردارانه در سرمایه‌گذاری بازار رمزارزها محسوب می‌شوند (مابوندا، ۲۰۱۸، ص ۸)؛ با این توضیح که در آن‌ها بالاترین نرخ سود و کمترین میزان خطر و چالش برای کاربران پیشنهاد داده می‌شود که این ضمانت با دریافت هزینه از کاربران جدید برای کاربران قدیمی محسوب می‌شود. طرح پانزی و درمی سرمایه‌گذاری فریبکارانه است. به این صورت که سودی که به سرمایه‌گذاران پرداخت می کند را از پول ایشان یا از پول دیگر سرمایه‌گذاران تأمین می کنند؛ بنابراین سود یادشده حاصل از فعالیت اقتصادی واقعی نخواهد بود.

روش

پژوهش حاضر از نظر هدف کاربردی است و گردآوری اطلاعات آن به صورت کتابخانه‌ای است. بدین

شرح که نگارش این مقاله با تکیه بر نظرات حقوقی و همچنین آموزه‌های علمی و فنی مربوط رمزارزها و زنجیره بلوکی انجام شد و تبیین آن با مراجعه به مطالب تخصصی و مهندسی مربوط به این حوزه و کتب، مقالات علمی و مراجعه به پایگاه‌های اینترنتی قابل دسترس، انجام شد.

یافته‌ها

تدابیر پیشگیرانه از وقوع جرائم پولشویی و کلاهبرداری: ارتکاب جرم پولشویی و کلاهبرداری در حوزه جرائم مالی همانند دیگر جرائم نیازمند پیشگیری است. واژه پیشگیری در لغت به معنای ممانعت کردن و اقدامات احتیاطی برای جلوگیری از رخدادهای بد و ناخواسته است و در معنای عام آن هر عملی که نتیجه آن جلوگیری از ارتکاب جرم است، را می‌توان پیشگیری به شمار آورد (نیازپور، ۱۳۹۳، ص ۹۲). در معنای خاص منظور از پیشگیری، مجموعه اقداماتی است بجز اقدامات کیفری که هدف غایی آن جلوگیری از ارتکاب جرم است (فرزین‌راد و محمدی‌فرد، ۱۳۹۵، ص ۱۱۴). این مفهوم هم شامل اقدامات کیفری و هم اقدامات غیر کیفری است؛ زیرا هدف اصلی آن مقابله با جرم است. آنچه امروزه به پیشگیری در جرم‌شناسی شناخته شده است، پیشگیری قبل از ارتکاب جرم و غیر کیفری است، بدین جهت که قاعده پیشگیری بهتر از درمان است، مورد قبول صاحب‌نظران بسیاری از علوم قرارگرفته و برای جامعه نیز به‌صرفه‌تر به نظر می‌رسد (ابراهیمی، ۱۳۹۰، ص ۲۰). تردیدی نیست که با پیشرفت وسایل ارتباطی، امکان وقوع جرائم، پیوسته رو به افزایش است؛ بنابراین باید برای نیل به جامعه سالم در کنار اصلاح، به پیشگیری نیز پرداخته شود (ابراهیمی، ۱۳۹۰، ص ۲۰). از آنجایی که پیشگیری اولیه در رابطه با استفاده صحیح از فضای سایبر اهمیت دارد، در پژوهش نیز به پیشگیری غیر کیفری پرداخته شده است. پیشگیری غیر کیفری از گذر کاهش پدیده‌های مجرمانه، نامناسب نشان دادن موقعیت‌های ارتکاب بزه، آموزش افراد در دو حیطه پیشگیری اجتماعی و وضعی مطرح است.

پیشگیری اجتماعی: پیشگیری اجتماعی در اندیشه‌های روسو شکل گرفته است. بنا بر اعتقاد او انسان به طور طبیعی نیکوسیرت بوده و این جامعه است که او را به دامان ارتکاب جرائم می کشاند (صبح‌دل، ۱۳۹۶، ص ۹۵). این نوع از پیشگیری به دنبال علت‌شناسی جرم است؛ یعنی براین باور است که عوامل مختلفی بر ارتکاب جرم تأثیر دارد و پیشگیری اجتماعی باید این عوامل را ازطریق مداخله در محیط اجتماعی عمومی و شخصی خنثی کند. محیط اجتماعی عمومی مانند محیط های فرهنگی، اقتصادی،

سیاسی که نسبت به عموم مشترک است (صبح‌دل، ۱۳۹۶، ص ۹۶) و محیط اجتماعی شخصی مانند محله و خانواده است (نیازپور، ۱۳۸۹، ص ۶۱). در پیشگیری اجتماعی هدف، ایجاد تغییرات و اصلاحات در فرد و جامعه است تا جرم به‌صورت پایدار وقوع نیابد. در این راستا پیشگیری اجتماعی تعدادی از نهادهای جامعه را در برمی گیرد که کج‌روی را تحت نظم و قاعده درمی‌آورد (قماشی و عارفی، ۱۳۹۶، ص ۸۷). از جمله این نهادهای مهم آموزش و پرورش و رسانه‌های گروه هستند که افراد جامعه با کمک این وسایل به انجام رفتارهای قاعده‌مند هدایت می‌شوند (علمداری، ۱۳۸۹، ص ۷۸).

به دیگر سخن پیشگیری اجتماعی سعی دارد که علل و عوامل اجتماعی خطرزای بزهکاری و بزه‌دیدگی را هدف گیری کند و درنهایت سبب جلوگیری از بروز جرائم به صورت پایدار و همیشگی شود (ابرندآبادی، ۱۳۹۱، ص ۵۰۹) و هدف هماهنگ کردن افراد با هنجارهای جامعه است. پیشگیری اجتماعی خود به وسیله راهکارهای مهم پیشگیری جامعه‌مدار و فردمدار از ارتکاب جرم پیشگیری می کند. این نوع از پیشگیری نسبت به پیشگیری وضعی هزینه‌های کمتری در برداشته و اثر بلندمدت آن بیشتر است.

پیشگیری اجتماعی جامعه‌مدار: این نوع پیشگیری با به‌کارگیری اقدامات غیر قهرآمیز اجتماعی، فرهنگی و اقتصادی در محیط‌های مختلف درصدد از بین بردن یا کاهش تأثیر عوامل محیطی جرم‌زا بر افراد است (نجفی ابرندآبادی، ۱۳۹۱، ص ۵۷۰). در پیشگیری اجتماعی از نوع جامعه‌مدار هدف از بین بردن یا کاهش تأثیرات مخرب عوامل محیطی جرم‌زا و بستر ارتکاب جرائم بر افراد است (قماشی و عارفی، ۱۳۹۶، ص ۸۹). از بهترین عوامل پیشگیرانه جامعه‌مدار می‌توان به تقویت بنیان خانواده، فرهنگ و آموزش آن، اصلاح نگرش و باورهای دینی، افزایش آگاهی‌های عمومی و بهبود شرایط اقتصادی اشاره داشت.

خانواده: امروزه به جهت افزایش جرائم و ناکارآمدی مجازات‌ها، گرایش به شناسایی روش‌های پیشگیری از جرم بسیار زیاد شده است ناگفته نماند که پیشگیری از جرم امر تازه‌ای نیست، بلکه از اموری است که بشر و احکام الهی همواره به دنبال آن بوده‌اند. از جمله شیوه‌های پیشگیری که می‌تواند کاربرد داشته باشد توجه به نحوه تربیت است، از این رو می‌توان چنین گفت که مجرم یا منحرف از یک سری اصول تربیتی استوار و صحیح که لازم بوده از کودکی در وی القا می‌شد برخوردار نبوده است (ساریخانی، ۱۳۹۵، ص ۲۱۰). پرواضح است که در این راه نهاد خانواده نقش بسیار مهمی را برعهده دارد. ضمن این که اجرا و رعایت قوانین باید توسط خانواده به فرزندان آموزش داده شود. در واقع انسان‌های سالم در خانواده‌های سالم رشد می یابند و آسیب‌های

اجتماعی گوناگون نیز می‌تواند از خانواده سرچشمه بگیرد (ساریخانی، ۱۳۹۵، ص ۲۰۸).

اصلاح نگرش و باورهای دینی: مسلم است که نقش دین در ایجاد علقه و تکالیف مذهبی، تقویت فرهنگ صبر و استقامت در برابر وسوسه‌های مجرمانه و تعامل اجتماعی غیر قابل انکار است (لطفی و حاجی ده‌آبادی، ۱۳۹۱، ص ۱۷۰). در جامعه‌ای که باورهای دینی و اعتقاد به خداوند حاکمیت دارد، افراد جامعه خداوند را بر رفتار خود ناظر دیده و به جهت ترس از ناخشنودی خداوند از آنان دست به ارتکاب جرائم مختلف نخواهند زد. بنابراین انضباط اجتماعی، عدالت و آرامش جامعه برقرار خواهد بود و همگان خود را در مقابل صیانت و پاسداری از ارزش‌ها مسئول می‌دانند (لطفی و حاجی ده‌آبادی، ۱۳۹۱، ص ۱۷۲). از جمله راهکارهای افزایش و اصلاح نگرش و باورهای مذهبی در جامعه، انجام امر به معروف و نهی از منکر که از فروع دین اسلام است (حاجی‌تبار فیروزجائی، ۱۳۹۸، ص ۵۲). همان‌طور که خداوند متعال در آیات ۱۱۰ و ۱۱۴ سوره مبارکه آل عمران، ۱۵۷ و ۱۶۵ سوره مبارکه اعراف و ۶۵ سوره مبارکه توبه مسلمانان را از منکر نهی و آنان را به سوی معروف امر کرده است. وارد کردن رمزارزها در کشور بدون تدابیر پیشگیرانه‌ای مانند افزایش باورهای دینی و تقویت فرهنگ قناعت، منجر به حرص و طمع در افراد سودجو شده و شرایط را برای رفتارهای مجرمانه هموار می‌کند.

ارتقای آگاهی‌های عمومی: طیفی از مردم جوامع همواره به دنبال خدعه و نیرنگ بوده و به وسیله ابزاری چون فضای سایبر از ناآگاهی مردم سوء استفاده می‌کنند (شاه جهان پور، ۱۳۹۶، ص ۶۳). عموم جامعه به جهت ناآشنا بودن به ماهیت، چیستی و عملکرد فناوری‌های نوظهوری چون زنجیره‌های بلوکی و رمزارزها، قربانی اهداف مجرمانه این افراد می‌شوند. به دلیل گوناگونی فرهنگ و اقوام متعدد در کشور جمهوری اسلامی ایران، همواره ناآگاهی و اطلاع غیر دقیق عموم مردم از فناوری‌های نوظهور و گاهی فضای سایبر، تهدیدآمیز است. بنابراین به نظر می‌رسد که نهادهای مرتبط همچون معاونت اجتماعی و پیشگیری از وقوع جرم قوه قضاییه، پلیس فتا، شورای عالی فضای مجازی، کمیته تعیین مصادیق محتوای مجرمانه، صدا و سیما جمهوری اسلامی ایران و مانند آنها، می‌توانند با برگزاری کلاس‌هایی در مناطق محروم‌تر و برای اقشار ضعیف‌تر، آنان را نسبت به خطرهای این جرائم آگاه کنند. از دیگر تدابیر پیشگیری اجتماعی از نوع جامعه‌مدار در این بخش می‌توان به نیاز مبرم کشور به حقوق‌دانان آشنا به فضای سایبر به ویژه رمزارزها اشاره داشت. زیرا حقوق‌دانان اعم از اساتید، قضات و وکلای دادگستری آشنا به این امر می‌توانند

به اعمال تدابیر پیشگیرانه و آگاهی‌های مردمی کمک شایانی کنند. آگاه‌بخشی می‌تواند زمینه‌های افزایش جهل به فناوری‌های نوظهور و قواعد و مقررات حقوقی را از بین برده یا حداقل کاهش دهد (شاه جهان پور، ۱۳۹۶، ص ۶۹).

بهبود شرایط اقتصادی: شرایط ضعیف اقتصادی و معیشتی مانند فقر، بیکاری و درآمد کم، بر ارتکاب جرم به ویژه جرائم مالی نظیر پولشویی و کلاهبرداری در حوزه رمزارزها تأثیر بسزایی دارد. بنابراین بهبود وضعیت اقتصادی و عنایت مسئولان به این مهم بسیار ضروری است. یکی از برنامه‌های دین مبین اسلام مبارزه با فقر است. به همین جهت به نظر برخی از صاحب‌نظران، حل مشکلات اقتصادی کلید حل معضل ارتکاب جرائم است (ربیعی و صادق‌زاده، ۱۳۹۰، ص ۱۹۲). بنابراین به نظر می‌رسد که کارآفرینی و ایجاد اشتغال برای جوانان و افرادی که در حوزه فضای سایبر متخصص هستند؛ در کاهش جرائم این حوزه به ویژه پولشویی و کلاهبرداری تأثیرگذار است. به عنوان نمونه جذب جوانان در مشاغل امنیتی و حفاظت از داده‌ها در فضای سایبر و ارائه آموزش لازم به آنان در رفع این معضل بسیار کلیدی است. زیرا با استفاده از اشخاص ضمن ایجاد شغل و دغدغه کاری برای آنان می‌توان از نیرو و خلاقیت آنان برای صیانت از ارزش‌های جامعه بهره‌مند شد و تعهد آنان را افزایش داد. ضمن اینکه مطابق با بیانات مقام معظم رهبری لازم است بر نیروی خلاق و ایده‌پرداز جوانان تکیه شود و از کشف این استعدادها تا بهره‌وری از آنان در رشد و رونق تولید داخلی بهرمند شد (بیانات مقام معظم رهبری، ۱۳۹۸).

پیشگیری اجتماعی رشدمدار: پیشگیری رشدمدار بر آن است تا با شناسایی عوامل مخاطره‌آمیز، تقویت عوامل حمایتی و مداخله زودرس، از پایداری افراد در بزهکاری جلوگیری کند (متولی زاده نایینی، ۱۳۸۷، ص ۱۲۸). لازم به ذکر است که اقدامات یادشده باید پیش از بروز و در سنین کم در رابطه با کودکانی که در معرض آن هستند انجام شود. بنابراین پیشگیری رشدمدار در رابطه با کودکان و نوجوانان صورت می‌پذیرد که به منظور پیشگیری از ارتکاب جرم در آینده انجام می‌شود (نیازپور، ۱۳۹۱، ص ۱۸۹). مؤلفه‌های این پیشگیری فردی هستند. بنابراین با استفاده از راهبردها و اقدامات ناظر بر شخصیت فرد می‌توان زمینه‌های بروز بزهکاری و کج‌روی را در شخص کاهش داد. این نوع از پیشگیری با رشد، آموزش، رفتار و سلامت زیستی کودکان ارتباط بسیاری دارد و کم هزینه‌ترین نوع پیشگیری در میان جوامع مختلف به شمار می‌آید (فرانس و هامل، ۱۳۹۳، ص ۲۹۸). برنامه‌های این نوع از پیشگیری در خانواده و

مدرسه قابل پیاده‌سازی است تا با ارائه آموزش و تربیت لازم از بزهکار شدن کودکان و نوجوانان در سنین پایین‌تر جلوگیری و ممانعت شود (نیازپور، ۱۳۹۳، ص ۹۵). با استفاده از راهکارهای پیشگیری رشدمدار می‌توان اقدام به برگزاری کلاس‌های آموزشی به منظور افزایش آمادگی والدین نسبت به فضای سایبر به ویژه رمزارزها کرد تا والدینی آگاه‌تر، فرزندانی هوشمندتر و داناتر تربیت شوند. همچنین با گنجاندن و پیاده‌سازی واحدهای درسی درباره آشنایی با فضای سایبر متناسب با سن کودکان و نوجوانان، می‌توان در مدارس نیز رسالت یادشده را دنبال کرد.

پیشگیری وضعی: پیشگیری وضعی اقداماتی است که بر اداره، طراحی و کنترل محیط فیزیکی متکی است تا فرصت‌های ارتکاب جرم را کاهش دهد و یا این که در صورتی که ارعاب مؤثر واقع نشد، خطر تعقیب را افزایش دهد (صفاری، ۱۳۸۰، ص ۲۸۰). همچنین اقدامات پیشگیرانه در پیشگیری وضعی با دو هدف دنبال می‌شوند؛ نخست، دشوار یا غیر ممکن ساختن وقوع جرم با آن که قصد و انگیزه مجرمانه موجود است و دوم، منصرف کردن مجرم از رفتار مجرمانه و ممانعت از پیدایش و تشدید ارتکاب جرم (میرخلیلی، ۱۳۸۸، ص ۶۷). تدوین و ساخت آنتی ویروس‌های قوی و برنامه‌های قدرتمند ساخت کلید خصوصی و کیف پول دیجیتالی ایرانی، زیر نظر سازمان‌های مربوطه، کلاهبرداری و پولشویی از این دریچه را به حداقل خواهد رساند. همچنین آگاه‌سازی مردم نسبت به حفظ کلیدهای خصوصی خود و عواقب بعدی ناشی از مراقبت نکردن از آن نیز بسیار مهم است (مابوندا، ۲۰۱۳، ص ۱۰). همچنین لازم است تدوین مقررات و تنظیم قوانین مربوط به استخراج و انتقال رمزارزها به عنوان پیشگیری وضعی تقنینی در دستور کار قرار گیرد؛ بدین شرح که کارگروه یا کمیته‌ای در این خصوص تأسیس و بر روند و عملکرد صرافی‌های موجود در حوزه رمزارزها نظارت و بازرسی داشته باشد. ممنوعیت یا از دسترس خارج کردن سایت‌های مشکوک به عملیات مجرمانه رمزارزها و کانال‌هایشان در فضای مجازی، یکی از بهترین تدابیر پیشگیرانه از جرائم پولشویی و کلاهبرداری محسوب می‌شوند. اعلام شماره برای معرفی سایت‌ها یا کانال‌های مشکوک به جرائم پولشویی و کلاهبرداری و تأسیس سامانه‌ای ملی که هرگونه خرید و فروش و نقل و انتقال مربوط به رمزارزها در آن ثبت شده و در غیر این صورت تخلف از مقررات و اعمال مجازات درپی داشته باشد، از دیگر اقدامات پیشگیری وضعی است.

بحث و نتیجه‌گیری

با وجود ویژگی‌های مثبت رمزارزهای جهانی نظیر دور زدن تحریم‌های ظالمانه، کاهش بوروکراسی، پیاده‌سازی دولت الکترونیک و جایگزینی به عنوان ارز بین‌المللی در مبادلات، به نظر می‌رسد استفاده از رمزارزها به علت نبود امکان شناسایی و کشف هویت مبادلات در برخی از انواع آن، همچنین آشنایی غیر صحیح و غیر کامل مردم و کاربران با این فناوری نوظهور، موجب افزایش سرعت و تسهیل ارتکاب جرائمی چون کلاهبرداری و پولشویی می‌شود. بنابراین بکارگیری تدابیر پیشگیرانه برای جلوگیری از وقوع این جرائم، ضروری است. در همین راستا به دو شیوه پیشگیری وضعی و اجتماعی اشاره شده است. از آن جایی که در پیشگیری وضعی هدف ایجاد تغییرات در فرد و اجتماع به طور همزمان است تا از وقوع جرم ممانعت به عمل آید، دو شیوه پیشگیری جامعه‌مدار و پیشگیری رشدمدار مورد واکاوی قرار گرفت. در پیشگیری جامعه‌مدار به ارزش و جایگاه خانواده، اصلاح نگرش و باورهای دینی و همچنین بهبود شرایط اقتصادی برای اصلاح وضع موجود در رابطه با وقوع جرائم اشاره شد و همراه با آن بر نقش بی‌بدیل جایگاه خانواده و مدرسه از خاستگاه پیشگیری رشدمدار تأکید شد. همچنین در پیشگیری وضعی نیز می‌توان با کنترل محیط فیزیکی از فرصت‌های ارتکاب جرم کاست. شایان توجه است که رمزارز ملی به جهت وجود سند الزامات و ضوابط فعالیت در حوزه رمزارزها در کشور که در بهمن ماه سال ۱۳۹۸ توسط بانک مرکزی تدوین شده است، از تقنین و راهکارهای مناسبی برخوردار است که همچنان کافی به نظر نمی‌رسد. اما به جهت شیوع و محبوبیت رمزارزهای جهانی نظیر بیت کوین نیاز است که نسبت به تقنین و ارائه راهکارهای پیشگیرانه دقت نظر بیشتری شود. در ادامه پیشنهادهایی در هر دو حوزه پیشگیری از وقوع جرائم کلاهبرداری و پولشویی در راستای استفاده از رمزارزهای جهانی ارائه می‌شود:

- محدودیت و فیلترینگ سایت‌های مشکوک به پولشویی و کلاهبرداری؛
- به رسمیت شناختن برخی از صرافی‌های رمزارزها و استفاده از مدارک شناسایی هویت افرادی که مبادرت به انتقال رمزارزهای جهانی می کنند تا در صورت وقوع جرم از مدارک و سوابق تراکنش‌ها به مرتکبان دسترسی پیدا شود. ناگفته نماند که چنین راهکاری در راستای پیشگیری از جرائم یادشده در رابطه با رمزارز ملی در سند بانک مرکزی گنجانده شده است؛
- تدوین و تصویب قانون کارآمد برای کنترل استخراج رمزارزها و صرافی‌های مجاز به عنوان تدابیر

پیشگیرانه وضعی تقنینی؛

- طراحی و ساخت نرم‌افزارهای ایرانی قدرتمند ساخت کلید خصوصی برای کیف پول دیجیتال؛
- ارائه شماره تماس اعلام جرم به عموم جامعه در رابطه با مبادلات مشکوک رمزارزها و ارتکاب جرم و تشکیل کمیته رسیدگی به شکایات مردمی؛
- برگزاری کلاس‌های آشنایی با رمزارزها و مهارت کار با آن برای پیشگیری از بزه‌دیدگی افراد، با همکاری نهادهای ذی‌ربطی چون شورای عالی فضای مجازی، پلیس فتا، کارگروه تعیین مصادیق محتوای مجرمانه و معاونت اجتماعی و پیشگیری از وقوع جرم قوه قضاییه؛
- جذب و استعدادیابی جوانان متخصص در فضای سایبر به ویژه در زمینه رمزارزها برای مشاغل حفاظت از داده‌ها و مدیریت کنترل مبادلات نامبرده؛
- تأسیس سامانه‌ای ملی که هرگونه نقل و انتقال مربوط به رمزارزها در آن ثبت شده و در غیر این‌صورت تخلف از مقررات و اعمال مجازات درپی داشته باشد؛
- استفاده از گروه‌های حفاظتی و گشت‌های پلیس در فضای سایبر به ویژه سایت‌هایی که در انتقالات نقش بسزایی ایفا می‌کنند.

فهرست منابع

آذرنیوار، محمد. (۱۳۹۷). بررسی جامع فقه بیت کوین ارزهای دیجیتال و بلاک‌چین. گروه تخصصی ارز دیجیتال، صص ۱-۲۹. قابل بازیابی از:https://arzdigital.com/shariah-analysis-of-bitcoin-cryptocurrency-and-blockchain/

ابراهیمی، شهرام. (۱۳۹۰). جرم‌شناسی پیشگیری. جلد اول، تهران: انتشارات میزان.

ارزانیان، نسترن. (۱۳۹۶). بلاک‌چین و ارز دیجیتالی در ایران، قانوگذاری چالش‌ها و راهکارها. اولین کنفراس رگولاتوری بلاک‌چین و رمزارزها، تهران، صص ۱-۱۳. قابل بازیابی از:http://regublock.ir

ارزانیان، نسترن. (۱۳۹۸). تحلیل تطبیقی نهاد بیلمنت در نظام حقوقی کامن‌لا: با تأکید بر احکام تصرف در اموال مجازی. فصلنامه حقوق و فناوری اطلاعات، کانون سردفتران و دفتریاران، ۱(۱)، صص ۱-۱۸. قابل بازیابی از: http://www.notary.ir/

بابایی، محمدعلی و نجیبیان، علی. (۱۳۹۰). چالش‌های پیشگیری وضعی از جرم. مجله حقوقی دادگستری، ۷۵(۷۵)، صص ۱۴۷-۱۷۲. قابل بازیابی از:http://www.jlj.ir/article_11079_abbfad760dcc4719fc721ea4e8d853aa.pdf

بالفنون، حسین. (۱۳۹۶). فراتر از زنجیره بلوک، زیست بوم‌های خودانتظام، اولین کنفرانس رگولاتوری بلاک‌چین و رمز ارزها. تهران.

بیانات مقام معظم رهبری. (۱۳۹۸). دیدار با والیبالیست‌های جوان و نفرات برتر المپیادهای علمی، قابل بازیابی از: .Khamenei.ir

حاجی‌تبار فیروزجایی، حسن. (۱۳۹۸). نقش نهادهای مذهبی در پیشگیری از جرم: چالش‌ها و راهکارهای مقابله با آن. فصلنامه

پژوهش‌های فقه و حقوق اسلامی، ۱۵(۵۶)، صص ۴۴-۶۸، قابل بازیابی از:
http://ijrj.baboliau.ac.ir/article_666893_bd313ef0a328c3a078cced378ee51fbc.pdf

حبیب‌زاده، طاهر. (۱۳۹۰). حقوق فناوری اطلاعات. جلد اول. تهران: نشر مرکز پژوهش های مجلس شورای اسلامی.

ربیعی، علی و صادق‌زاده، حکیمه. (۱۳۹۰). بررسی رابطه سرمایه اجتماعی بر کارآفرینی. فصلنامه رفاه اجتماعی، ۱۱(۴۱)، صص ۱۹۱-۲۲۱. قابل بازیابی از: http://refahj.uswr.ac.ir/article-1-717-fa.pdf

روشن، محمد؛ مظفری، مصطفی و میرزایی، هانیه. (۱۳۹۷). بررسی وضعیت فقه و حقوقی بیت کوین. فصلنامه تحقیقات حقوقی، ۲۲(۸۷). قابل بازیابی از:http://lawresearchmagazine.sbu.ac.ir/article_82656.html

ساریخانی، عادل. (۱۳۹۵). سبک‌های تربیتی و پیشگیری از جرم. حقوق جزا و سیاست جنایی، ۴، صص ۲۰۷-۲۲۴، قابل بازیابی از:https://journals.ut.ac.ir/article_60840_38761d4feb1260c47637f23e2356c691.pdf

ساورایی، پرویز؛ پورمسجدیان، فاطمه. (۱۳۹۳). تبیین ماهیت حقوقی و اختلافات نام دامنه‌های اینترنتی. دانشنامه حقوق و سیاست، ۱۰(۲۲)، صص ۱۴۹-۱۸۴. قابل بازیابی از:
https://www.sid.ir/fa/journal/ViewPaper.aspx?id=259305

سلیمانی‌پور، محمدمهدی؛ سلطانی‌نژاد، حامد و پورمطهر، مهدی. (۱۳۹۶). بررسی فقه پول مجازی. دوفصلنامه تحقیقات مالی اسلامی، ۶(۲)، صص ۱۶۷-۱۹۲. قابل بازیابی از:
http://ensani.ir/file/download/article/1540363174-9982-75.pdf

شاه‌جهان‌پور، سعید. (۱۳۹۶). نقش فرهنگ در پیشگیری از جرم. فصلنامه علمی حقوقی قانون یار، ۴(۱۰)، صص ۶۱-۷۲. قابل بازیابی از:https://www.sid.ir/fa/journal/ViewPaper.aspx?id=313778

صبح‌دل، محمد. (۱۳۹۶). جایگاه حقوقی قوه قضاییه در پیشگیری اجتماعی، فصلنامه قانون‌یار، دوره۴، صص ۹۳-۱۰۸، قابل بازیابی از:https://www.sid.ir/fa/journal/ViewPaper.aspx?id=313782

صفاری، علی. (۱۳۸۰). مبانی نظری پیشگیری از جرم. مجله تحقیقات دانشگاه شهید بهشتی حقوقی. (۳۳-۳۴)، صص ۲۶۷-۳۲۱. قابل بازیابی از:http://ensani.ir/file/download/article/20100912152628

عباسی، اصغر. (۱۳۹۶). حقوق کیفری اقتصادی پولشـویی مبارزه با پول‌شویی در اسناد بین‌المللی و نظام حقوقی ایران، تهران: انتشارات میزان.

علمداری، علی. (۱۳۸۹). پیشگیری در جرائم سایبری. مطالعات بین‌المللی پلیس، (۲)، صص ۷۳-۹۱، قابل بازیابی از:
https://www.noormags.ir/view/fa/articlepage/987811/

فرانسس، آلن و هامل، راس. (۱۳۹۳). پیشگیری رشدمدار از جرم (مجموعه مقالات). باقر شاملو و مهدی مقیمی، مترجمان. تهران: انتشارات میزان.

فرزین‌راد، رویا و محمدی‌فرد، بشری. (۱۳۹۵). رویکردی بر مقوله پیشگیری از جرم در پرتو نظام قانونی ایران. فصلنامه تحقیقات حقوق خصوصی و کیفری، (۲۷)، صص ۱۱۳-۱۳۸.

قماشی، سعید و عارفی، مرتضی. (۱۳۹۶). موانع سیاسی و اقتصادی پیشگیری از جرم. آموزه‌های حقوق کیفری، (۱۳)، صص ۸۵-۱۱۳. قابل بازیابی از:http://ensani.ir/file/download/article/20180416093217-9835-92.pdf

لطفی، نسرین و حاجی‌ده‌آبادی، محمدعلی. (۱۳۹۱). بررسی نقش مذهب در پیشگیری از وقوع جرائم از دیدگاه افراد عادی و مجرم. فصلنامه دانش انتظامی، ۱۵(۴)، صص ۱۶۷-۱۸۶. قابل بازیابی از:http://ensani.ir/fa/article/360823/

متولی‌زاده نایینی، نفیسه. (۱۳۸۷). پیشگیری رشدمدار، فصلنامه مطالعات پیشگیری از جرم، ۲(۲)، صص ۱۲۳-۱۴۲، قابل بازیابی از:https://www.noormags.ir/view/fa/articlepage/972709

معین، محمد. (۱۳۷۵). فرهنگ معین. تهران: انتشارات امیرکبیر.

میرخلیلی، محمود. (۱۳۸۸). پیشگیری وضعی از بزهکاری با نگاه به سیاست جنایی اسلام. تهران: انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی.

میرزاخانی، رضا. (۱۳۹۶). بیت کوین و ماهیت مالی فقهی. مرکز پژوهش توسعه و مطالعات اسلامی، سازمان بورس و اوراق بهادار.

میرمحمد صادقی، حسین. (۱۳۹۵). حقوق جزا اختصاصی ۲؛ جرائم علیه اموال و مالکیت. تهران: نشر میزان.

نجفی ابرندآبادی، علی‌حسین. (۱۳۹۱). تقریرات مباحثی در علوم جنایی. ویرایش ۷. تهران: دانشگاه شهید بهشتی.

نوری، مهدی و نواب‌پور، علیرضا. (۱۳۹۷). طراحی چارچوب مفهومی سیاستگذاری ارزهای مجازی در اقتصاد ایران. فصلنامه سیاستگذاری عمومی دانشگاه تهران، ۳(۴)، صص ۵۱-۷۸. قابل بازیابی از:
https://www.sid.ir/Fa/Journal/ViewPaper.aspx?id=355692

نیازپور، امیرحسن. (۱۳۸۹). پاسخ‌های عدالت کیفری ایران، فصلنامه مطالعات پیشگیری از جرم، ۵(۱۴)، صص ۵۵-۷۷. قابل بازیابی از:/https://www.noormags.ir/view/fa/articlepage/1041948

نیازپور، امیرحسن. (۱۳۹۱). گفتمان پیمان حقوق کودک در زمینه پیشگیری از بزهکاری. مجله پژوهشنامه حقوق کیفری، ۵(۶)، صص ۱۸۷-۲۰۴. قابل بازیابی از:https://www.noormags.ir/view/fa/articlepage/934408

نیازپور، امیرحسن. (۱۳۹۳). اساسی‌سازی حقوق پیشگیری از جرم در ایران. مجله پژوهش حقوق کیفری، ۲(۶)، صص ۹۱-۱۱۲. قابل بازیابی از:https://www.noormags.ir/view/fa/articlepage/1097543

Anne, Elizabeth. (2015). Cryptocurrencies and the Anonymous Nature of Transactions on the Internet, Oregon State University.

Bomhe, R, Chiristin, N, Edelman, B, Moore, T. (2015). Bitcoin: Economics Technology, And Governance. The Journal of Economic Prespectives, 29(2), pp 213-238. Retrieved from: http://dx.doi.org/10.1257/jep.29.2.213.

Chiristin, N. (2013). Traveling The Silk Road: A Measurement Analysis of A Large Anonymous Online Marketplace, In Proceedings of The 22nd International Conference on Word Wide Web, pp 213-224,Retrievedfrom:https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab12018.pdf

Devries, Peter D. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future, International Journal of Business Management and Commerce, 1(2), pp 1-10, Retrieved from: https://www.academia.edu/35155833/An_Analysis_of_Cryptocurrency_Bitcoin_and_the_Future

Dyntu, Valeriia. (2018). Cryptocurrency As A Means of Money Laundering, Odessa Law Academy Press.

Kibin, Lee; James, Joshua I.; Ejeta, Tekachew G.; and Kim, Hyoung J. (2016). Electronic Voting Service Using Block-Chain, Journal of Digital Forensics, Security and Law, 11(2). Retrieved from: https://commons.erau.edu/jdfsl/vol11/iss2/8/

Lemieux Louise. (2016). Trusting Records: Is Block chain Technology the Answer?, Records Management Journal, 26(02). Retrieved from: https://www.emerald.com/insight/content/doi/10.1108/RMJ-12-2015-0042/full/

Likhuta, Vlad. (2017). Bitcoin Regulation: Global Impact, National Lawmaking, fork log research. Retrieved from: https://about.nvestlegal.com/bitcoin_regulation_en.pdf

Mabunda, Sagwadi. (2018). Cryptocurrency: The New Face of Cyber Money Laundering,

International Conference on Advances in Big Data, Computer and Data Communication Syste South Africa.
Omri Y, Marian. (2015). A Conceptual Framework for The Regulation of Cryptocurrencies, UF L Faculty Publications.
Sat, Krylov. (2016). Investigation of Money Laundering Methods Through Cryptocurrency, Vol