دورهٔ ۵۱، شمارهٔ ۲، پاییز و زمستان ۱۴۰۰
صفحات ۵۰۳ تا ۵۲۱ (مقالهٔ پژوهشی)
DOI:10.22059/JQCLCS.2022.292559.1499

جستاری در پولشویی از طریق ارزهای رمزنگاری‌شده

مهدی مددی*
دانش‌آموخته کارشناسی ارشد گروه حقوق خصوصی، دانشکده حقوق، دانشگاه کاشان، اصفهان، ایران
سعید قماشی
دانشیار گروه حقوق خصوصی، دانشکده حقوق، دانشگاه کاشان، اصفهان، ایران
(تاریخ دریافت: ۱۳۹۸/۸/۲۴- تاریخ تصویب: ۱۴۰۰/۱۲/۲۲)

چکیده
مسئلهٔ پذیرش ارزهای رمزنگاری‌شده در داخل کشور همواره با چالش‌ها و نگرانی‌هایی همراه بوده است؛ یکی از چالش‌های اساسی در این زمینه مسئلهٔ «پولشویی» از طریق این ارزهاست، چراکه باور عمومی و حتی قانونگذار آن است که ارزهای مذکور اساساً به‌منظور انجام اعمال مجرمانه و به‌خصوص پولشویی پدید آمده‌اند و به همین منظور، نظر به ممنوع‌سازی مبادلات ارزهای رمزنگاری‌شده دارند. با این حال نمی‌توان از گسترش این ارزها در سطوح داخلی و بین‌المللی چشم فروبست و باید اقدام‌هایی در عرصهٔ کنترل مخاطرات ارزهای رمزنگاری‌شده داشت و با پذیرش کنترل‌شدهٔ این ارزها از محاسن آنها بهره گرفت. در همین زمینه پژوهش حاضر به واکاوی روش‌های مقابله با مهم‌ترین مخاطرهٔ ارزهای رمزنگاری‌شده -که همان پولشویی از طریق ارزهای رمزنگاری‌شده است- پرداخته است و رکن انتاجی آن را می‌توان چنین مختصر دانست که مقابله با پولشویی از طریق ارزهای رمزنگاری‌شده نیازمند «افزایش اقدام‌های نظارتی در سطوح داخلی و بین‌المللی»، «همکاری‌های مشترک بین‌المللی به‌منظور کشف تخلفات و مجازات متخلفان»، «بهره‌جویی از قوانین و راهکارهای مقابله با پولشویی و تروریسم مالی» که در سایر کشورها و یا در سطوح بین‌المللی اجرایی شده‌اند، «قانون‌مدار ساختن» این ارزها و استفاده از راهکارهایی چون «شناخت مشتری» است.

واژگان کلیدی
ارزهای رمزنگاری‌شده، بیت کوین، پولشویی، قانونمندسازی،FATF.

* mahdimadadi@grad.kashanu.ac.ir
ORCID iDs: https://orcid.org/0000-0002-5103-3051

مقدمه

پیشرفت و گسترش فناوری در عرصهٔ جهانی اگرچه سبب راحتی در زندگی انسان‌ها در عرصه‌های مختلف –اعم از کشف جرم برای ضابطان قضایی –شده است، لکن مجرمان نیز به‌عنوان بخشی از جامعهٔ جهانی از این پیشرفت‌ها در عرصه‌های مجرمانه بهره‌جویی کرده‌اند. برای مثال در سال‌های اخیر جرائم جدیدی چون جعل هویت از طریق صفحات مجازی پدید آمده یا سرقت و کلاه‌برداری مبالغ کلان با سهولت و دستاوردهای بزرگ‌تر همراه شده است و همین موضوع در نهایت در برخی موارد به صعوبت زندگی اجتماعی منتهی شده و سبب شده است تا پیشرفت فناوری واجد شرایط دوسویه‌ای باشد.

یکی از پیشرفت‌های فناوری در سال‌های اخیر را می‌توان پدیدهٔ ارزهای رمزنگاری‌شده دانست که اگرچه بیش از ده سال از پدیدآیی آن گذشته است، همچنان پدیده‌ای بدیع به‌شمار می‌آید که درک ابعاد مختلف آن به‌راحتی میسر نیست. علی ای حال این پدیده بدیع اگرچه در سطح بین‌المللی گسترش یافته است و جامعهٔ آماری زیادی به مبادله و استخراج آنها می‌پردازند، اما تاکنون دولت‌های مختلف اغلب به‌دلیل مخاطرات ناشناختهٔ آنها اقدامی در جهت قانونمندسازی این ارزها نداشته‌اند. از جمله مخاطراتی که سبب شک و تردید قانونگذاران در پذیرش رمزارزها شده است، مسئلهٔ ارتباط فی‌مابین پولشویی و ارزهای رمزنگاری‌شده است. موضوع مانحن فیه به دو قسم قابل رخ دادن است، نخست آنکه ارزهای رمزنگاری‌شده مورد پولشویی واقع شوند (به‌عبارت دیگر عملیات پولشویی بر خود رمزارزها حادث شود) و دوم آنکه پولشویی از طریق این ارزها به‌وقوع بپیوندد (به‌عبارتی رمزارزها به‌مثابهٔ ابزاری در عملیات پولشویی واقع شوند). پژوهش حاضر به‌دنبال بررسی قسم دوم این رویداد – که همان پولشویی از طریق ارزهای رمزنگاری‌شده است – خواهد بود.

مسئلهٔ اصلی پژوهش حاضر آن است که خطر پولشویی از طریق ارزهای رمزنگاری‌شده را به چه نحوی می‌توان مدیریت کرد؟ به‌عبارت دیگر یکی از موانع مهم بر سر راه پذیرش رمزارزها در نظام مالی – حقوقی ایران، مسئلهٔ قابلیت پولشویی از طریق این ارزهاست و قانونگذار به‌سبب رابطهٔ مجهول میان پولشویی و ارزهای رمزنگاری‌شده از پذیرش آنها اجتناب ورزیده است. در راستای این موضوع، مسئلهٔ این پژوهش نیز بررسی طرق رویارویی و کنترل مخاطرهٔ مذکور است. به‌منظور رویارویی با پدیدهٔ پولشویی از طریق ارزهای رمزنگاری‌شده باید شناخت مختصری از خصلت‌های این ارزها داشت و به‌عبارتی تبیین کرد که این ارزها واجد چه ویژگی‌هایی هستند که موضوع پولشویی از طریق آنها را نگران‌کننده ساخته است؟ (وجه معرفتی)، پس از این موضوع به

بررسی تجارب مقابله‌ای در سطوح داخلی و بین‌المللی پرداخته خواهد شد (وجه تقنینی) تا تبیین شود که نظام تقنینی چه ظرفیت‌ها و راهکارهایی را به‌منظور رویارویی با پولشویی از طریق رمزارزها می‌تواند اتخاذ کند؟ در نهایت نیز پیشنهادهایی در جهت طرق ممکنه و مؤثر در مقابله با پولشویی از طریق ارزهای رمزنگاری‌شده (وجه کاربردی) ارائه خواهد شد.

۲. واکاوی معرفتی ارزهای رمزنگاری‌شده

اهمیت سخن در خصوص تحلیل معرفتی ارزهای رمزنگاری‌شده از آن حیث است که باید ابتدا تصویر صریح و صحیحی از ارزهای رمزنگاری‌شده ترسیم شود و در پرتو چنین ترسیمی، با شناخت ابعاد مختلف، چالش‌ها و ظرفیت‌های این ارزها سعی شود با نگاهی کارامدگرا به پرسش‌ها در زمینهٔ چالش‌های مقابله با پولشویی از طریق ارزهای رمزنگاری‌شده پاسخ داده شود. به‌عبارت دیگر در واکاوی ماهیت ارزهای رمزنگاری‌شده مسئله آن است که این ارزها واجد چه خصوصیاتی هستند که آنها را از سایر ارزها متمایز می‌سازد و سبب شده است که رمزارزها به‌عنوان ابزاری مطلوب برای پولشویی شناخته شوند؟

۱. ۲. مشخص نبودن هویت و کاربرد جرم محور

رمزارزها برای ایجاد امنیت در شبکه از سازوکار رمزنگاری‌شده استفاده می‌کنند، ازاین‌رو هیچ فرستنده و گیرنده‌ای قابل شناسایی نیست و این مسئله می‌تواند به اقدام‌های مجرمانه منجر شود. به‌طور مثال اگر فردی از فروشگاهی توسط ارزهای رمزنگاری‌شده، کالایی را خریداری کرد و فروشنده پس از دریافت وجه از ارسال کالا امتناع ورزد، خریدار امکان پیگیری حقوقی از مراجع قضایی به‌دلیل فقدان مستندات لازم را ندارد، چراکه آدرس‌ها دربردارندهٔ هویت اصلی مالک نیستند و همچنین فروشنده می‌تواند در هر تراکنش از آدرس جدیدی استفاده کند (نوری، ۱۳۹۷: ۲۱). ریشهٔ این مسائل در امکان عدم تطابق مشخصات کاربری مالکان این ارزها با هویت حقیقی آنهاست. در واقع صاحبان این وجوه نه بی‌نام که گمنام هستند و ازاین‌رو زمینهٔ ارتکاب چنین تخلفات و جرائم برای آنها ساده‌تر است (میرزاخانی، ۱۳۹۶: ۵). گمنامی کاربران بیت‌کوین ممکن است به استفادهٔ بیت‌کوین در فعالیت‌های غیرقانونی‌ای از جمله پولشویی منجر شود، چراکه انجام عملیات پولشویی با هویت مجهول انتساب پول نامشروع به فرد خاصی را با صعوبت مواجه می‌کند و بدیهی است چنین موضوعی کمال مطلوب مجرمان پولشویی خواهد بود.

۲. ۲. نامشخص بودن مبدأ و مقصد تراکنش‌ها

یکی از ظرفیت‌های ارزهای رمزنگاری‌شده امکان پنهان‌سازی مبدأ و مقصد تراکنش‌هاست و

کاربران با بهره‌مندی از برخی ابزارها می‌توانند ارتباط میان مبدأ و مقصد را مختل سازند. از طرف دیگر حتی در صورت کشف ارتباط میان دو کیف پول، به‌دلیل هویت نامعلوم طرفین عملاً این ارتباط به‌دست‌آمده مبدأ و مقصد را مشخص نخواهد کرد. این موضوع در حالی است که به‌طور کلی قوانین مبارزه با پولشویی بر شفافیت تراکنش‌ها مالی و آشکارسازی مبدأ و مقصد پول‌های جابه‌جاشده تأکید دارند و از این طریق علاوه‌بر ایجاد بازدارندگی، امکان ره‌گیری تراکنش‌های مشکوک به پولشویی نیز فراهم می‌شود. به بیان دیگر در سیاست‌های مبارزه با پولشویی این نکته حائز اهمیت است که اگر مبدأ و مقصد یک تراکنش مالی مشخص نباشد، این تراکنش مشکوک تلقی شده و مظنون به پولشویی تلقی می‌شود و باید با دقت بیشتری رصد شود، درحالی‌که رصد این موضوع در رمزارزها امری دشوار تلقی می‌شود.

۳. ۲ . فقدان نهاد ناظر مرکزی

یکی از مهم‌ترین ویژگی‌های ارزهای رمزنگاری‌شده‌ای چون بیت کوین، «غیرمتمرکز»[1] بودن آنهاست. غیرمتمرکز بودن بدان مفهوم است که هیچ شخص یا نهاد خاصی سلطه‌ای بر اطلاعات ندارد و اطلاعات در سراسر شبکه پراکنده است و مجموعه‌ای از اعضای شبکه فعالیت در شبکه را به عهده دارند. بیت‌کوین یک ارز غیرمتمرکز است که با فناوری «نظیر به نظیر» مدیریت می‌شود و تمامی فعالیت‌ها مانند انتشار بیت‌کوین، پردازش و اعتبارسنجی معاملات توسط کاربران شبکه انجام می‌گیرد و هیچ واسطه یا مرجع مرکزی برای کنترل و دخالت در فرایند وجود ندارد. غیرمتمرکز بودن از دلایل بسیار مهم در مناسب بودن بیت کوین برای عملیات پولشویی است، چراکه در ساختار ارزهای این‌چنینی هیچ نهاد مرکزی‌ای وجود ندارد که به رصد و کنترل اطلاعات بپردازد، درحالی‌که در سیستم مالی رایج، فرد برای واریز کردن وجه به حساب خود باید اسناد مثبته‌ای را به بانک و سایر نهادهای مالی ارائه کند و تمامی اطلاعات مالی و گردش‌های مشکوک قابلیت رصد و رسیدگی دارند.

۴. ۲ . عدم محدودیت‌های زمانی، جغرافیایی، سیاسی

بیت‌کوین را می‌توان ارز فاقد محدودیت دانست، چراکه اولاً در بیت‌کوین محدودیت‌های «مکانی» فاقد وجاهت است و هر کسی در هر نقطهٔ جهان امکان دسترسی به آن و حضور در شبکهٔ بلاک‌چینی آن را دارد و به‌راحتی یک فرد می‌تواند در هر نقطه‌ای از دنیا، به انتقال این ارز به هر نقطه‌ای از دنیا که بخواهد مبادرت ورزد و این امر تنها چند دقیقه به طول خواهد انجامید. از طرف

1. Decentralize

دیگر محدودیت‌های «سیاسی» نیز در خصوص بیت‌کوین صدق نمی‌کند، چراکه اساساً دولت‌ها توانایی کنترل و دخالت در شبکهٔ بلاک‌چینی بیت‌کوین را ندارند و بر این اساس امکان اعمال علایق سیاسی حاکم در آنها غیرممکن است. محدودیت‌های «سرزمینی» نیز چنین است و بیت‌کوین یک دارایی جهان‌شمول است و به ملیت خاصی اختصاص ندارد و هر کس در هر نقطه از جهان می‌تواند از کاربرد آن منتفع شود. محدودیت دیگر اما محدودیت‌های «زمانی» است که جایی در عرصهٔ بیت‌کوین ندارد و افراد در هر زمان از شبانه‌روز و در تمامی ایام سال می‌توانند بدون نگرانی از تعطیلی بانک‌ها یا محدودیت‌های مشابه اقدام به تبادل وجوه خود کنند و چند دقیقه بعد تراکنش تأییدشدهٔ خود را مشاهده کنند.

ویژگی‌های مذکور به‌نوعی وجه تمایز و برتری رمزارزها نسبت به ارزهای فیات است که سبب می‌شود مجرمان پولشویی تمایل داشته باشند با رمزارزها عملیات خود را به ثمر برسانند. برای مثال با استفاده از ویژگی فرامرزی بودن بیت کوین، می‌توانند معاملات خارج از مرزی انجام دهند و مباحث مربوط به تعارض قوانین را پدید آورند و نظامات حقوقی مختلف را درگیر کنند؛ افزون‌بر این می‌توانند پیگیری و نظارت را سخت‌تر سازند، چراکه کشف این جرم نیازمند همکاری بین‌الدولی است که این مسئله کشف جرم را سخت‌تر و زمان‌بر می‌کند. در مثالی دیگر مجرمان پولشویی به‌علت نبود محدودیت‌های زمانی می‌توانند در تمامی ایام این عمل را انجام دهند و در فرایندهای مربوط به پاک کردن صبغهٔ پول‌ها دیگر با مشکلات مربوط به تعطیلات درون‌مرزی یا بین‌المللی مواجه نیستند که این امر به کوتاه شدن فرایند پولشویی و اتمام سریع‌تر آن کمک خواهد کرد.

۵. ۲. هزینهٔ عملیاتی پایین و سرعت بیشتر

یکی از معایب نظام‌های متعارف پرداخت در سطح بین‌المللی، هزینه‌های معاملاتی بالایی است که توسط نهادهای واسط دریافت می‌شود؛ اما در نظام نوین پرداخت ارزهای رمزنگاری‌شده، انتقالات به‌صورت فردبه‌فرد و به‌طور میانگین در کمتر از ۱۰ دقیقه صورت می‌پذیرد و به همین سبب و به‌علت فقدان نهادهای واسط، هزینه‌های معاملاتی بسیار اندک است و هر فردی بدون نیاز به پرداخت کارمزد مازاد می‌تواند وجه خود را انتقال دهد (ECB, 2015: 19). البته باید عنایت داشت که در صورت نیاز به سرعت بالاتر، هر فرد می‌تواند با تعریف کارمزدی برای تراکنش خود سرعت انتقال وجه خود را افزایش دهد. پایین بودن هزینهٔ عملیاتی نیز از آن حیث اهمیت دارد که در فرایند پولشویی، متعددا باید ارزها به ارزهای مختلف یا کالاهای متعدد تبدیل شوند و درصورتی‌که

این عملیات با کارمزد پایین‌تری همراه باشد، میزان استقبال از آن بیشتر خواهد بود؛ موضوعی که سبب می‌شود رمزارزها دارای مطلوبیت بیشتری باشند.

۶. ۲ . ناتوانی دولت‌ها در مصادره و بلوکه کردن

از معایب ارزهای رایج و پول‌های موجود در حساب‌های بانکی، امکان مصادره کردن آنها توسط دولت‌ها و برخی نهادهای صاحب قدرت بنابر دلایل متفاوت –اعم از اجرای احکام قانونی یا اعمال قدرت سیاسی– است، درحالی‌که این عدم امنیت در ساختار ارزهای رمزنگاری‌شده وجود ندارد و حقوق مالکیت اشخاص و دولت‌ها مورد تعرض و دخالت دیگران قرار نمی‌گیرد، چراکه ارزهای رمزنگاری‌شده نوعی ارز خصوصی محسوب می‌شوند و هیچ نهادی توانایی دخالت در تراکنش‌های آن را ندارد (نوری، ۱۳۹۷: ۱۷). به‌عبارت دیگر، به‌علت فقدان نهاد مرکزی صاحب قدرت امکان مصادره کردن رمزارزها وجود ندارد و دولت‌ها نمی‌توانند شخص را ممنوع‌المعامله کنند. البته در یک فرض چنین امکانی وجود دارد و آن در صورتی است که رمزارزهای یک شخص درون کیف پول یا صرافی‌ای باشد که تحت اعمال قدرت دولت‌هاست و از طریق مسدود کردن حساب کاربری شخص آنها را ضبط کنند که البته در چنین فرضی نیز در صورت عدم دسترسی به کلید خصوصی فرد مزبور، امکان انتقال رمزارزهای وی به شخص دیگر امکان‌پذیر نخواهد بود. ازاین‌رو این ویژگی می‌تواند برای مجرمان پولشویی امری بسیار مطلوب به‌حساب آید.

۷. ۲. فقدان قوانین و مقررات مشخص

ارزهای رمزنگاری‌شده به‌دلیل بدیع بودن و ساختار نسبتاً پیچیده‌ای که دارند، تاکنون به‌صورت جامع مورد تقنین واقع نشده‌اند و در این خصوص صرفاً تلاش‌های اندکی در برخی کشورها صورت پذیرفته است. این موضوع سبب شده است تا یک خلأ قانونی در این زمینه پدیدار شود و بعضاً افرادی که به حقوق ایشان در زمینهٔ ارزهای رمزنگاری‌شده تعرضی صورت‌گرفته است، در رجوع به نهادهای قضایی و درخواست رسیدگی خود با موانع بسیاری مواجه شوند و بعضاً به حق خود دست پیدا نکنند. افزون‌بر این خلأ قانونی سبب سوءاستفادهٔ مجرمان نیز شده است و ایشان با سوءاستفاده از این خلأ به ارتکاب جرائمی چون پولشویی، کلاه‌برداری و... می‌پردازند. به همین علت مسئلهٔ قانونمندسازی بیت‌کوین واجد اهمیت بسیاری است، لکن باید توجه داشت که چندوجهی بودن ارزهای رمزنگاری‌شده موجب می‌شود قانونمندسازی این ارزها، نهادهای مختلف اقتصادی و غیراقتصادی کشور را درگیر خود سازد که این موضوع سبب پیدایش چالش‌های جدی در عرصهٔ تنظیم‌گری ارزهای رمزنگاری‌شده خواهد شد.

۸ ۲. الکترونیکی بودن ارزهای رمزنگاری‌شده

بیت‌کوین اصولاً به‌صورت الکترونیکی وجود دارد و به‌منظور پول الکترونیکی بودن طراحی شده است، درحالی‌که پول سنتی اصولاً به‌صورت فیزیکی است و حساب‌هایی را که در بانک‌ها وجود دارد، می‌توان در صورت تمایل به‌سرعت به وجه نقد تبدیل کرد (سید حسینی، ۱۳۹۳: ۹). امکان مبادلات سریع از طریق رمزارزها یکی از دیگر دلایل تمایل مجرمان در استفاده از این ارزهاست، در حال حاضر بعضاً تراکنش‌های مالی پس از چند ساعت به ثمر می‌نشینند، درحالی‌که انجام پذیرفتن این امر در بیشتر رمزارزها کمتر از یک دقیقه و در بیت کوین در نهایت ۱۰ دقیقه زمان خواهد برد که این موضوع می‌تواند به کوتاه شدن فرایند پولشویی بینجامد.

یکی از چالش‌های موجود در پول‌های رایج در کشورها، جعل و چاپ تقلبی این پول‌هاست که مشکلاتی را برای سیستم مالی کشورها در دوره‌های مختلف ایجاد کرده است. ویژگی رمزنگاری و الکترونیکی بودن ارزهای رمزنگاری‌شده سبب شده که امکان جعل و چاپ تقلبی آنها وجود نداشته باشد که این امر مزیت مهمی برای این نوع از ارزها به‌حساب می‌آید (نوری، ۱۳۹۷: ۱۸)، چراکه در عرصهٔ ارزهای رمزنگاری‌شده به‌دلیل رمزنگاری پروتکل بیت‌کوین هیچ شخص یا سازمانی نمی‌تواند پروتکل‌های آن را کنترل یا دست‌کاری کند. الکترونیکی بودن از آن حیث حائز اهمیت است که امکان مبادلهٔ آنها کم‌هزینه‌تر است و مخاطرات مربوط به سرقت که در امور مادی وجود دارد، متوجه آنها نیست. عدم امکان جعل نیز اگرچه چندان حائز اهمیت در برای تمایل به رمزارزها به‌منظور پولشویی نیست، از آنجا که پولشویی فرایندی غیرقانونی است که به‌راحتی نمی‌تواند در معاملات رسمی وارد شود، این موضوع به افزایش خطر پولشویی می‌انجامد که تضمین اصالت وجه در پولشویی می‌تواند برای مجرمان این امر چندان بی‌اهمیت نیز نباشد.

۳. روش‌ها و بسترهای پولشویی از طریق ارزهای رمزنگاری‌شده

ارزهای رمزنگاری‌شده بنا به خصلت خود به‌نظر نقش مهمی در تسهیل عملیات پولشویی داشته است، چراکه مجرمان با احساس راحتی بیشتر و بدون آنکه وارد فرایندهای دست‌وپاگیر بانکی شوند، می‌توانند وجوه بزرگی را با سرعت و امنیت بیشتر و بدون نیاز به افشای هویت خود، در فرایند پولشویی داخل کنند. به نظر اما نقش ارزهای رمزنگاری‌شده صرفاً به‌عنوان یک تسهیل‌کنندهٔ پولشویی خلاصه نمی‌شود و آنها در گسترش و تنوع نیز دخیل بوده‌اند. در ابتدای زمانی‌که ارزهای رمزنگاری‌شده به‌عنوان رقیبی برای پول‌های رایج کنونی مطرح شدند، به‌علت پذیرش محدود و عدم مقبولیت کافی، دارای جذابیت کافی برای ورود به عملیات پولشویی نبودند، لکن امروزه با افزایش مقبولیت و امکان استفاده از ارزهای رمزنگاری‌شده برای معاملات تجاری و خریدهای

آنلاین فرامرزی، ارزهای رمزنگاری‌شده گزینه‌های جذاب برای پولشویی هستند. بر همین اساس در ذیل تأملی در خصوص «روش‌ها» و «بسترهای» پولشویی از طریق ارزهای رمزنگاری‌شده صورت خواهد پذیرفت، چراکه ارائهٔ راهکارهای مؤثر در جهت مقابله با امر مزبور نیازمند شناخت و درک صحیح از موارد چنینی است.

۱. ۳. روش‌های پولشویی از طریق ارزهای رمزنگاری‌شده

پولشویی از طریق ارزهای رمزنگاری‌شده، اگرچه دارای روش‌های متعدد و متنوع است، هدف از تمامی این روش‌ها پنهان ساختن هویت و ناشناس ماندن تراکنش‌هاست که در ذیل برخی از این روش‌ها بررسی خواهد شد.

۱. ۱. ۳. روش مخلوط‌سازی تراکنش‌ها

در روش «مخلوط کردن بیت‌کوین»[1]، ارزهای رمزنگاری‌شدهٔ افراد مختلف به واحدهای کوچک‌تری تبدیل شده و پس از ترکیب با یکدیگر و انجام تراکنش‌های متعدد به آدرس‌های موردنظر این افراد ارسال می‌شود.[2] به‌عبارت دیگر در این فرایند ارزهای رمزنگاری‌شدهٔ هر شخص به سرویس ناشناسی ارسال شده و با پول‌های اشخاص دیگر ترکیب شده و سپس به افراد بازگردانده می‌شود (Ruffing, 2014: 357). در این پروتکل تمامی شرکت‌کنندگان از طریق کانال‌های پرداختی بیت‌کوین‌های تحت مالکیت خود را به آدرس معینی ارسال کرده و مقدار برابری از بیت‌کوین‌های افراد دیگر در شبکه را دریافت می‌کنند. این فرایند مفهوم «ردپای مالکیت» را برای همه از بین می‌برد؛ به‌طوری‌که شرکت‌کنندگان و پایشگران از اینکه بیت‌کوین‌ها از چه کسانی و به چه کسانی منتقل شده است، مطلع نمی‌شوند.

۲. ۱. ۳. روش گمنام‌سازی آدرس

یکی از راه‌های کنترل دسترسی در فضای مجازی، پایش آدرس‌های IP مربوط به کاربران و تخمین محدودهٔ تقریبی جغرافیایی آنها و پیگیری اتصالات مشکوک است، چراکه IP در واقع یک شمارهٔ شناسایی یکتا برای برقراری یک ارتباط تحت شبکه هستند و از طریق آنها دستگاه‌های مختلف از هم بازشناخته می‌شوند. به‌منظور ناشناس‌سازی آدرس کاربران در شبکهٔ بیت‌کوین ابزارهایی چون

---

1. Bitcoin Mixing

۲. برای مثال شخصی که ۱۰ بیت‌کوین دارد، به‌جای ایجاد یک تراکنش ۱۰ واحدی، ۲۰ تراکنش نیم‌واحدی ایجاد می‌کند و با افزایش تعداد تراکنش‌ها و تکرار این موضوع ردیابی تراکنش‌ها بشدت دشوار خواهد شد.

مرورگر «Tor» [۱] و «vpn» استفاده می‌شود. ابزارهای مزبور به یک شخص امکان می‌دهد تا وانمود کند در مکان دیگری یا در قلمرو حقوقی دیگری اقامت دارد یا اینکه به فرد اجازه می‌دهد که چندین حساب کاربری بدون قابلیت انتساب به خود را ایجاد کند.

۳. ۱. ۳. استخراج انحصاری

روش استخراج انحصاری نوعی تبانی بین آغازکنندهٔ تراکنش و یک استخراجگر (یا یک استخر) است. در این روش تبهکاران مقداری بیت‌کوین را برای استخراجگر انحصاری خود (که کاملاً بر تمام فعالیت‌های آن کنترل دارند) ارسال می‌کنند و از آن استخراجگر می‌خواهند که هزینهٔ تراکنش بالایی را جهت تأیید این تراکنش تعیین کند. پس از استخراج تراکنش مزبور، هزینهٔ تراکنش تعیین‌شده به استخراجگر پرداخت می‌شود و به‌نوعی وجوه ناشی از پولشویی به وجوه ناشی از استخراج تغییر ماهیت می‌دهند و به یک دارایی کاملاً مشروع و قانونی بدل می‌شوند (Strehle, 2020: 6).

۴. ۱. ۳. روش مخلوط سازی غیرمتمرکز

مخلوط‌سازی غیرمتمرکز ایده‌ای است که مخلوط‌سازی توسط گروهی از کاربران انجام می‌گیرد و بدین‌ترتیب از خدمات مخلوط‌سازی و جاگذاری آن به‌جای پروتکل همتا به همتا رها می‌شود. این رویکرد بدیل عدم نیاز به اشخاص ثالث دارای سازگاری بیشتری با فلسفهٔ بیت‌کوین است. اصل کلیدی این روش برای گمنامی این‌گونه است که زمانی‌که تراکنش چندین ورودی از آدرس‌های مختلف دارد، همبستگی امضاهای آنها با هر ورودی، جدا از هم و مستقل از یکدیگرند؛ بنابراین این آدرس‌های متفاوت را می‌توان توسط افراد مختلف کنترل کرد. در این حالت به یک بخش برای جمع‌آوری کلیدهای خصوصی نیازی نیست. به این طریق گروهی از کاربران اجازه دارند تا سکه‌های خود را با یک تراکنش مخلوط کنند. هر کاربر یک آدرس ورودی و خروجی ایجاد می‌کند و این دو با هم، یک تراکنش با این آدرس‌ها تشکیل می‌دهند. آدرس‌های ورودی و

---

۱. مرورگر Tor سامانه‌ای است که برای ناشناس ماندن کاربران در محیط اینترنت به‌کار می‌رود و از نرم‌افزار کارخواه و شبکه‌ای از سرویسدهنده‌ها (سرورها) تشکیل شده است و می‌تواند داده‌هایی از کاربران مانند موقعیت مکانی و نشانی پروتکل اینترنت را پنهان کند. بهره‌گیری از این سامانه، ردگیری و شنود داده‌های کاربر را از سوی دیگران بسیار سخت می‌کند. این ردگیری و شنود می‌تواند در زمینهٔ بسیاری از فعالیت‌های کاربر، مثل وبگاه‌هایی که بازدید کرده، داده‌هایی که بارگیری و بارگذاری کرده، پیام‌هایی که از طریق نرم‌افزارهای پیام‌رسان ارسال یا دریافت کرده و هرگونه ارتباطاتی که در محیط اینترنت برقرار کرده است، صورت پذیرد؛ ازاین‌رو می‌توان گفت که این سیستم برای محافظت از آزادی کاربران و حفظ حریم خصوصی آنها در محیط اینترنت طراحی شده است. این نرم‌افزار، یک نرم‌افزار آزاد است و استفاده از شبکهٔ آن نیز رایگان است.

خروجی تصادفی است. در نتیجه مهاجم قادر به تشخیص ورودی و خروجی نیست. کاربران آدرس خروجی‌شان را در تراکنش بررسی می‌کنند تا درج شده باشد و همان مقدار بیت‌کوین ارسالی در ورودی را دریافت کرده باشند. پس از تأیید، تراکنش امضا می‌شود (عزیزی، ۱۳۹۸: ۷۹).

۲. ۳. بسترهای پولشویی از طریق ارزهای رمزنگاری‌شده

در پولشویی از طریق ارزهای رمزنگاری‌شده برخی از بسترها نیز وجود دارد که در ذیل به آنها پرداخته خواهد شد.

۱. ۲. ۳. صرافی‌های غیرقانونی

یکی از بسترهای پولشویی از طریق ارزهای رمزنگاری‌شده، «صرافی‌های غیرمجاز» هستند. در صرافی‌هایی که از مقررات مربوط به مقابله با پولشویی پیروی نمی‌کنند، فرایند احراز هویت کاربران چندان دقیق صورت نمی‌پذیرد که این مسئله سبب پنهان ماندن مشخصات معامله‌گر می‌شود. در پرتو عدم شناسایی هویت کاربران این امکان فراهم می‌آید که ارزهای رمزنگاری‌شده بارهاوبارها در بازارهای مختلف معامله شده و پس از واریز به صرافی‌های غیرقانونی، در خرید ارزهای دیگر از آنها استفاده شود.

۲. ۲. ۳. سایت‌های قمار و شرط‌بندی

قمار و بازی‌های آنلاین از طریق سایت‌هایی که بیت‌کوین یا سایر ارزهای رمزنگاری‌شده را قبول می‌کنند، یکی دیگر از روش‌هایی است که در طرح‌های پولشویی از طریق ارزهای رمزنگاری‌شده از آنها استفاده می‌شود، چراکه این سایت‌ها اصولاً از قوانین مقابله با پولشویی پیروی ندارند و نظارت خاصی نیز بر هویت افراد صورت نمی‌پذیرد و خلاف‌کاران می‌توانند به‌واسطهٔ فضای فراهم‌شده، پول‌های کثیف خود را به حساب سایت‌های شرط‌بندی انتقال دهند و سپس در بستری امن که این سایت‌ها فراهم کرده‌اند، پس از چند روز پول کثیف خود را از سایت قمار خارج و به‌حساب خود منتقل کنند.

۳. ۲. ۳. استفاده از دستگاه‌های خودپرداز ارزهای رمزنگاری‌شده

حدود ۸۰۰۰ دستگاه خودپرداز بیت‌کوین در سراسر جهان وجود دارد و امکان معاملهٔ بیت‌کوین را برای افراد فراهم آورده‌اند. دستگاه خودپرداز بیت‌کوین این امکان را فراهم آورده است که افراد با پول‌های رایج یا کارت‌های اعتباری، بیت‌کوین تهیه کنند. در این روش افراد پس از وارد کردن آدرس کیف پول خود (یا هر کس دیگری) و واریز کردن قیمت بیت‌کوین، می‌توانند بیت‌کوین

خریداری‌شده را در کیف پول خود مشاهده کنند. در این روش هویت خریدار نامشخص باقی می‌ماند و مجرمان می‌توانند از نقاط ضعف خودپردازهای ارزهای رمزنگاری‌شده برای سوءاستفاده از خطرهای مربوط به پولشویی سوءاستفاده کنند. چنانکه در یکی از مثال‌های پولشویی از طریق خودپردازها، پلیس اسپانیا اعلام کرد که یک عملیات پولشویی از طریق دستگاه‌های خودپرداز بیت‌کوین را کشف کرده و ۸ اسپانیایی و اهل آمریکای لاتین را در این جریان دستگیر کرده است. این ۸ نفر با استفاده از ۹ شرکت، ۹ میلیون یورو را برای قاچاقچیان مواد مخدر در کلمبیا و کشورهای دیگر منتقل کردند. عملیات پولشویی مذکور بدین‌شکل انجام می‌گرفته است که مواد مخدر کلمبیا در اروپا به فروش می‌رسیده و در قبال آن پول دریافت می‌شده است. در مرحلهٔ بعدی، یوروهای غیرقانونی دریافت‌شده، از طریق دستگاه‌های خودپرداز بیت‌کوین به ارزهای رمزنگاری‌شده تبدیل می‌شده است. در این عملیات به محض تبدیل پول نقد به ارزهای رمزنگاری‌شده، بیت‌کوین‌های ذخیره‌شده در کیف پول دیجیتالی به مؤسسهٔ دیگری ارسال می‌شد که به‌طور مستقیم تحت نظارت بزرگان مواد مخدر کلمبیایی قرار داشت. این تأمین‌کنندگان مواد مخدر نیز می‌توانستند با مراجعه به صرافی آنلاین ارزهای رمزنگاری‌شده، بیت‌کوین‌ها را به پول‌های دیگر تبدیل کنند (Castor, 2019).

۴. راهکارهای مقابله بر پولشویی از طریق ارزهای رمزنگاری‌شده

وفق تتبعات صورت‌گرفته در سیاست‌های اتخاذشده در سطوح داخلی و بین‌المللی به نظر بتوان راهکارهای مقابله‌ای با پولشویی از طریق ارزهای رمزنگاری‌شده را در موارد ذیل مختصر دانست.

۱. ۴. قانونمندسازی

قانونگذاری از مهم‌ترین راه‌ها در جهت کاستن از مخاطرات پدیده‌های نوین است. قانونگذاری مانند تحدید حدودی است که تا زمانی‌که رخ ندهد، امکان تجاوز به آن حریم، عمداً یا سهواً وجود دارد، بدون آنکه متجاوز مرتکب تخلفی شده باشد یا نگرانی برای ضمانت اجرای عمل خود داشته باشد. ارزهای رمزنگاری‌شده نیز تا زمانی‌که قانونگذاری نشود، می‌تواند محلی برای تجاوز به حقوق دیگران، تخلفات مالی و جرائم گسترده باشد، بدون آنکه عقوبتی را در پی داشته باشد (مددی، ۱۴۰۰: ۳۲۲). دولت‌ها باید با «قانونمند ساختن» ارزهای رمزنگاری‌شده بر پیامدهای اجتماعی، حقوقی، سیاسی، اقتصادی آن تسلط یابند. اگرچه در خصوص مفهوم قانونمندسازی برداشت واحدی وجود ندارد، نخستین معنایی که با شنیدن واژهٔ قانونی‌سازی متبادر می‌شود، «عدم ممنوعیت» و «جایز ساختن» است و از آن به «جرم‌زدایی» یا «کیفرزدایی» تعبیر می‌شود، لکن

مقصود از «قانونمندسازی» به مفهوم رفع ممنوعیت از ارزهای رمزنگاری‌شده نیست و مقصود قانون‌مدار کردن و تابع قانون قرارداد است. رسمیت بخشیدن به ارزهای رمزنگاری‌شده در کنار ترسیم چارچوبی جامع در جهت نظارت بر آن، بدین‌نحو به جرم‌یابی کمک می‌کند که از زیرزمینی شدن این‌گونه فعالیت‌ها پیشگیری کند و در نتیجه علاوه‌بر ایجاد بازدارندگی از طریق ایجاد شفافیت، مسیر کنترل و کشف جرم را نیز هموارتر می‌کند.

۲. ۴. بهره‌جویی از مقررات پیشنهادی بین‌المللی

یکی از راهکارهایی که در سطح داخلی و بین‌المللی می‌تواند در مقابله با پولشویی از طریق ارزهای رمزنگاری‌شده ثمربخش باشد، بهره‌جویی از دستورالعمل‌های صادره توسط «گروه ویژهٔ اقدام مالی»[1] است. این نهاد طی سال‌های اخیر دستورالعمل‌های متعددی را وضع کرده است و همواره در حال به‌روزرسانی آنهاست. برای مثال این نهاد در سال ۲۰۱۴ با انتظار گزارشی با عنوان «ارزهای مجازی: تعاریف کلیدی و ریسک‌های بالقوه ضدپولشویی و تأمین مالی تروریسم» به موضوع ارزهای مجازی پرداخت و آنها را به‌دلیل خطر ناشناسی مضر و آسیب‌رسان دانست، چراکه در این ارزها شناخت مشخصات مشتری (از جمله نام و نشانی آنها) امکان‌پذیر نیست و ساختار این ارزها فاقد نهاد نظارتی مرکزی است که بر تراکنش‌ها نظارت و آنها را ثبت کند (FATF, 2015: 10).

در سال ۲۰۱۵، گروه ویژهٔ اقدام مالی دستورالعمل خاصی برای ارزهای مجازی صادر کرد؛ دستورالعمل مزبور دربردارندهٔ مجموعه‌ای از توضیحات در خصوص کاربرد توصیه‌های گروه ویژهٔ اقدام مالی برای واحدهایی که با دارایی‌های مجازی و محصولات و خدمات پرداختی مرتبط با آنها سروکار دارند، است. گروه ویژهٔ اقدام مالی به کشورهایی که خدمات مبادله‌ای میان دارایی‌های مجازی و پول‌های رایج را عرضه می‌کردند، توصیه می‌کرد که در حوزه‌های قضایی مانند هر نهاد مالی دیگری ذیل «قوانین ضدپول‌شویی»[2] و «کنوانسیون بین‌المللی مقابله با تأمین مالی تروریسم»[3] قرار گرفته و نظارت‌های محتاطانه را اعمال کنند. در دستورالعمل سال ۲۰۱۵ اگرچه توصیه‌ای در خصوص ممنوعیت دارایی‌های مجازی و محصولات و خدمات پرداختی مرتبط با آنها نداشت (چراکه چنین ممنوعیتی می‌تواند به سوق پیدا کردن چنین فعالیت‌هایی به زیرزمین و ازبین‌رفتن کامل شفافیت و کنترل بر آنها منجر شود)، لکن بر این باور بود که واحدهای فعال در حوزهٔ دارایی‌های مجازی و محصولات و خدمات پرداختی مرتبط با آنها باید ذیل یک رویهٔ احراز

1. Financial Action Task Force (FATF)
2. Anti-Money Laundering (AML)
3. Countering Financing of Terrorism (CFT)

صلاحیت تشدیدشده قرار بگیرند، چراکه چنین فعالیت‌هایی بهسبب عنصر ناشناسی ذاتی و چالش‌هایی که در مسیر اجرای اقدامات تشخیصی لازم ایجاد می‌کنند، دارای ریسک بالاتری تلقی می‌شوند (FATF, 2015: 9).

گروه ویژهٔ اقدام مالی در سال ۲۰۱۸ اعلام کرد که استانداردهای خود را در خصوص ارزهای رمزنگاری‌شده و شرکت‌های فعال در زمینهٔ ارزهای رمزنگاری‌شده تغییر داده است و با ارائه تعاریف جدید دامنه واحدهای مشمول مقررات مربوط به قوانین ضدپولشویی و کنوانسیون بین‌المللی مقابله با تأمین مالی تروریسم را به‌طور چشمگیری نسبت به راهنمای سال ۲۰۱۵، توسعه داد. این سازمان در دستورالعمل‌های به‌روزشدهٔ خود، خاطرنشان کرده است که ارائه‌دهندگان خدمات ارزهای دیجیتال، باید تحت نظارت و بررسی قوانین سیاست‌های مبارزه با پولشویی و مقابله با تأمین مالی تروریسم قرار گیرند و انطباق فعالیت این شرکت‌ها با سازمان‌های مذکور، به‌دقت بررسی شود. مقررات قوانین ضدپولشویی به دو محور اساسی پیشگیری و اجرایی استوار است. پیشگیری بیشتر در چهار زمینهٔ شناسایی مشتری، گزارش‌دهی، مقررات‌گذاری و نظارت مورد تأمل واقع می‌شود و در مرحلهٔ اجرایی بیشتر بر مجازات متکی است. اینها مراحلی است که در عمل برای خود مؤسسات مالی نیز مفید است و می‌تواند از منافع آنها حمایت کند، اما به‌عنوان ضمانت اجرای غیرمستقیم این مقررات می‌توان به قرار گرفتن اسامی کشورهای متخلف در فهرست سیاه گروه ویژهٔ اقدام مالی اشاره کرد که در آن اسامی کشورهایی که الزامات مندرج در توصیه‌ها را برآورده نمی‌کنند، ذکر می‌شود. قرار گرفتن در این فهرست سبب می‌شود کشورهای دیگر به‌علت عدم عملکرد شفاف و افزایش مخاطرات از همکاری در سرمایه‌گذاری‌های مالی با این کشورها خودداری کنند (FATF, 2020: 130).

گروه ویژهٔ اقدام مالی در سال ۲۰۱۹ اقدام به انتشار دستورالعمل‌های مقدماتی در خصوص ارزهای رمزنگاری‌شده کرد که طی آن ارائه‌دهندگان دارایی دیجیتال موظف به کسب مجوز یا ثبت‌نام در مراکز قانونی‌ای که این گروه به‌وجود آورده بود، شدند و صاحبان این مراکز قانونی موظف به ارائهٔ اطلاعات هویتی مزبور به مقامات مربوطه شدند. همچنین این دستورالعمل‌ها دولت‌ها را وادار می‌سازد تا مقررات و نظارت کافی بر دارایی دیجیتال را شکل دهند و به‌منظور جلوگیری کامل از پولشویی و تأمین مالی تروریسم یک مرجع ذی‌صلاح را به‌جای یک نهاد خودتنظیم، عهده‌دار این امر کنند و مجازات‌های کیفری، مدنی یا اجرایی را برای نقض قوانین وضع کنند. در نهایت، گروه ویژهٔ اقدام مالی ارائه‌دهندگان دارایی دیجیتال را ملزم به اخذ و نگهداری سوابق فرستندگان و ذی‌نفعان نقل‌وانتقال ارزهای رمزنگاری‌شده و در صورت نیاز ارائهٔ این اطلاعات به مقامات بین‌المللی کرد. بر این اساس کشورهای عضو موظف‌اند هنگام انتقال وجه

میان مشاغل حوزهٔ ارزهای رمزنگاری‌شده، اطلاعات دقیق و ضروری شروع‌کنندهٔ عملیات (ارسال‌کننده) و اطلاعات ضروری ذی‌نفع (گیرنده) را دریافت و نگهداری کرده و در صورت وجود نهاد ذی‌نفع، این اطلاعات را به آن ارائه کنند. همچنین باید از وجود و نگهداری اطلاعات ضروری (نه لزوماً دقیق) فرستنده و اطلاعات ضروری و دقیق گیرنده، اطمینان حاصل کنند؛ بنابراین دستورالعمل جدید، اطلاعات مورد نیاز برای هر انتقال وجه شامل «نام شروع‌کنندهٔ عملیات (برای مثال مشتری ارسال‌کننده)؛ شماره‌حساب شروع‌کنندهٔ عملیات که از آن در انجام تراکنش استفاده شده است (به‌طور مثال حساب مربوط به افراد نظامی)، آدرس فیزیکی (جغرافیایی)، شمارهٔ شناسایی ملی یا شمارهٔ شناسایی مشتری (نه شماره تراکنش)، و یا تاریخ و محل تولد که منحصراً هویت شروع‌کنندهٔ تراکنش را برای نهاد ذی‌نفع مشخص می‌کند؛ نام گیرنده و شمارهٔ حساب گیرنده که از آن در انجام تراکنش استفاده شده است» است (FATF, 2020: 76).

۳. ۴. اجرای قوانین احراز هویت

اجرایی شدن مقررات مقابله با پولشویی و مبارزه با تروریسم مالی یا پشتوانه و غایت این قوانین با تصویب همین گزاره‌ها در نظامات حقوقی و استفاده از راهکارهایی چون «شناخت مشتری»[1] و «شناخت تراکنش»[2] می‌تواند در رفع مشکل و ایراد ناشناس بودن طرفین معامله ثمربخش باشد. به‌طور معمول سیاست‌های شناخت مشتری مبتنی بر چهار عنصر سیاست پذیرش مشتری، روش‌های شناسایی یا همان احراز هویت مشتری، نظارت تراکنش‌ها و مدیریت ریسک استوار است (ارجمندنژاد، ۱۳۸۴: ۱۵). در واقع این فرایند با احراز هویت مشتری شروع می‌شود؛ به‌عبارت دیگر یعنی بررسی شود که آیا مشتری همان کسی است که ادعا می‌کند یا نه و در بخش مالی، این کار شامل تأیید هویت مشتری[3] از طریق ارائهٔ یک‌سری مدارک از جمله کارت شناسایی ملی است. برای تأیید اصل بودن مدارک ارائه‌شده توسط مشتری به روش‌های بیومتریک مانند تشخیص چهره یا اثر انگشت استفاده می‌شود. موارد کنترلی شناخت مشتری به‌طور معمول شامل موارد چون جمع‌آوری و تجزیه‌وتحلیل اطلاعات هویتی مانند مدارک هویتی، تطبیق نام با فهرست احزاب شناخته‌شده (مانند چهره‌های سرشناس سیاسی)، تعیین ریسک مشتری در خصوص تمایل به انجام پولشویی، تأمین مالی تروریست یا سرقت هویت، ایجاد انتظارات از رفتار تراکنشی مشتری و

---

۱. Know Your Customer فرایندی است که کسب‌وکارها از آن برای شناسایی و تأیید مشتری‌های خود و بانک‌ها برای مبارزه با پولشویی استفاده می‌کنند؛ چراکه برای مؤسسات مالی، بانک‌ها و بیمه‌ها اینکه مشتریانشان جزئیات مربوط به عدم سوء پیشینه، پولشویی و رشوه‌خواری را بنویسند، امری الزامی تلقی می‌شود.

2. Know Your Transaction

3. Customer's Identity

نظارت بر انجام تراکنش‌های مشتری می‌شود. در عرصهٔ ارزهای رمزنگاری‌شده، مؤسسات ارائه‌دهندهٔ خدمات (اعم از صرافی‌های ارز دیجیتال و مؤسسات مربوط به خدمات کیف پول این ارزها) باید پیش از ارائهٔ خدمات به احراز هویت کاربران خود اقدام کنند، البته بدیهی است اطلاعات مزبور باید محرمانه بماند و ویژگی ناشناس بودن کاربران این ارزها مورد حمایت قرار گیرد.

یکی دیگر از لوازم مقابله با پولشویی از طریق ارزهای رمزنگاری‌شده، بحث «شناخت تراکنش‌ها» می‌باشد که عبارت است از فرایندی که طی آن ارزهای مجازی سیاه (غیرقانونی) را شناسایی می‌کند و به‌عبارتی آنها را به دو دستهٔ شناسایی‌شده و غیر شناسایی‌شده تقسیم می‌کند و این امکان را به شخص می‌دهد که متوجه شود ارزی که اکنون در حال انتقال به وی است، تحت چه شرایطی و از چه مجرایی به طرف مقابل وی منتقل شده است، ازاین‌رو نقش بسزایی در شفافیت مالی و جلوگیری از پولشویی ایفا خواهد کرد؛ بنابراین باید گفت که ارزهای دیجیتال نه‌تنها آلوده‌تر از ارزهای فیات نیستند که حتی بهتر نیز هستند، چراکه تفاوت ارزهای دیجیتال و ارزهای دیگر این است که به شکل بلادرنگ[1] به‌هنگام انتقال از فردی به فرد دیگر قابل پیگیری هستند (Quinlan, 2016: 24).

۴. ۴. همکاری‌های مشترک بین‌المللی

از آنجا که در ارزهای رمزنگاری‌شده مسئلهٔ «مرز» چندان مطرح نیست و هر فردی در هر نقطه‌ای از دنیا می‌تواند در شبکهٔ این ارزها حضور داشته باشد، موضوع همکاری‌های بین‌المللی در مقابله با جرائم مربوط به این ارزها بسیار حائز اهمیت است و در صورت فقدان چنین مشارکتی، مقابله با مجرمان امری سخت و بعضاً غیرممکن خواهد بود، البته مشارکت‌های مزبور نباید به محدودسازی استفادهٔ مشروع از این ارزها منتهی شود. در کنار مشارکت‌های عملیاتی در خصوص مقابله با پولشویی از طریق ارزهای رمزنگاری‌شده، این تقابل نیازمند همکاری‌های مشترک در عرصهٔ قوانین و مقررات نیز است و به نظر باید کشورها در این خصوص دست‌کم برخی از سیاست‌ها و مقررات مشابه و یکپارچه را نیز از طریق کنوانسیون‌های بین‌المللی و معاهدات دو یا چندجانبهٔ بین‌المللی وضع کنند.

1. real time

۵. ۴. افزایش اقدام‌های نظارتی

چنانکه گذشت، ساختار ارزهای رمزنگاری‌شده فاقد یک نهاد نظارتی مرکزی است و ثبت تراکنش‌های آن بدون نیاز به تأیید یک نهاد مرکزی صورت می‌پذیرد، با این حال اما به‌دلیل مسئلهٔ شفافیت، تمامی تراکنش‌ها روی شبکهٔ بلاک‌چینی بیت‌کوین قابل مشاهده است و نهادهای مربوطه بدون هیچ‌گونه محدودیت قانونی یا مانع از سوی نهادهای ثالث می‌تواند به زنجیرهٔ بلوکی به‌صورت آزادانه دسترسی داشته باشند و دست‌کم تاریخچهٔ تراکنش‌های مالی را دنبال کنند. پس هرچند عدم انجام تراکنش‌های مالی ارزهای رمزنگاری‌شده همچون بیت‌کوین خارج از سیستم بانکی است، اما وجود زنجیرهٔ بلوکی در مورد بیت‌کوین خود مزیت محسوب می‌شود و می‌توان از آن در مسیر جرم‌یابی استفاده کرد. در کنار نظارت بر تراکنش‌ها، کشورها باید بر مؤسسات ارائه‌دهندهٔ خدمات در حوزهٔ ارزهای رمزنگاری‌شده نیز نظارت داشته باشند و سعی کنند آنها را تابع مقررات و نظارت خود قرار دهند تا ضمن رعایت حریم خصوصی کاربران به شناسایی و رصد تراکنش‌های مشکوک بپردازند.[۱]

۶. ۴. اعطای مجوز به شرکت‌های ارائه‌کنندهٔ خدمات

در حال حاضر کارگزاری‌های معاملاتی مختلفی در سطح کشور بدون دریافت مجوزهای لازم، در حال ارائهٔ خدمات به معامله گران رمزارزها هستند. این موضوع در کنار آنکه خطر کلاه‌برداری از طریق ایجاد کارگزاری‌های متخلف را افزایش می‌دهد، با توجه به عدم اخذ مجوز و طبیعتاً عدم الزام این کارگزاری‌ها به رعایت قوانین می‌تواند زمینه‌ساز بروز جرائم تعددی باشد، ازاین‌رو دولت باید با ارائهٔ مجوز به کارگزاری‌های رمزارزها، آنها را به رعایت قوانین توسط خود کارگزاری‌ها و کاربرانشان ملزم کند تا از طریق افزایش نظارت، امکان بروز تخلفات را کاهش دهد. در کنار کارگزاری‌ها برخی دیگر از ارائه‌کنندگان خدمات – همانند ارائه‌کنندگان کیف پول رمز ارزها- نیز وجود دارند که باید به اخذ مجوز و رعایت قوانین ملزم شوند تا چنانکه پیشتر گفته شد، در صورت بروز تخلفات کاربران امکان الزام و اجبار قانونی آنها وجود داشته باشد.

نتیجه

از تتبع صورت‌گرفته در پژوهش حاضر دریافته می‌شود که اگرچه در نگاه اولیه ارزهای

۱. نشانه‌هایی در حوزهٔ تراکنش‌های مالی مربوط به ارزهای رمزنگاری‌شده از جمله بیت‌کوین وجود دارد که می‌تواند حاکی از فعالیت‌های مجرمانه باشد، از جمله اینکه ۱. مجرمان به‌دنبال انتقال هرچه بیشتر ارزهای رمزنگاری‌شده با مقادیر کم هستند؛ چراکه هرچه حجم پولی که در هر تراکنش انتقال می‌یابد پایین‌تر باشد، کمتر موجب جلب توسط نیروهای امنیتی می‌شود؛ ۲. تراکنش‌های مالی به‌طور مکرر با یک طرف معین صورت می‌گیرد؛ ۳. مجرمان در تلاش‌اند تا بیت‌کوین کمتری در حساب‌هایشان نگهداری کنند.

رمزنگاری‌شده به‌دلیل ویژگی‌هایی چون «غیرمتمرکز بودن»، «نبود نهاد ناظر مرکزی» و «ناشناسی کاربران» بهشت مجرمان پولشویی به‌نظر می‌آیند، لکن مسئلهٔ پولشویی از طریق ارزهای رمزنگاری‌شده به‌دلیل میزان جهان‌شمولی نسبتاً پایین این ارزها امری چندان شایع نیست. افرادی که اقدام به پولشویی از طریق ارزهای رمزنگاری‌شده می‌کنند، از روش‌هایی چون «مخلوط‌سازی تراکنش‌ها»، «گمان‌سازی آدرس‌ها»، «استخراج انحصاری» و «مخلوط سازی غیرمتمرکز» استفاده می‌کنند. وجه اشتراک این روش‌ها در مختل ساختن برقراری ارتباط میان مبدأ و مقصد تراکنش‌ها است و سعی دارد تا ردیابی این مبادلات را با مشکل مواجه سازد. اگرچه «صرافی‌های غیرقانونی»، «سایت‌های قمار و شرط‌بندی» و «دستگاه‌های خودپرداز ارزهای رمزنگاری‌شده» بستری مناسب برای پولشویی از طریق ارزهای رمزنگاری‌شده فراهم آورده‌اند، اما با وضع برخی مقررات امکان کاهش خطر این نوع پولشویی ممکن است.

به‌منظور مقابله با پولشویی طریق ارزهای رمزنگاری‌شده باید مقرراتی وضع کرد که صرافی‌های ارائه‌کنندهٔ خدمات و همچنین متولیان کیف پول‌های ارزهای دیجیتال اقدام به جمع‌آوری اطلاعات کاربران کنند و پس از احراز هویت کاربران به ارائهٔ خدمات به ایشان بپردازند. این اقدام سبب می‌شود تا موضوع ناشناسی ارزهای رمزنگاری‌شده تا حدودی تحت‌الشعاع قرار گیرد. از طرف دیگر از آنجا که مسئلهٔ مرزها در موضوع ارزهای رمزنگاری‌شده چندان مطرح نیست، مقابله با جرائم مربوط به این ارزها نیازمند همکاری مشترک در سطح بین‌المللی است. افزون‌بر همکاری‌های عملیاتی در سطح بین‌المللی، لازم است که کشورها در ذیل یک کنوانسیون، مقررات واحدی را در خصوص مقابله با پولشویی از طریق ارزهای رمزنگاری‌شده اتخاذ کنند. بدیهی است درصورتی‌که برخی کشورها در این موضوع همکاری‌های لازم را نداشته باشند، مجرمان تمایل خواهند داشت از خدمات ارائه‌شدهٔ ذیل قوانین آنها بهره‌مند شوند که این موضوع می‌تواند مقابله با پولشویی را سخت کند.

در خصوص ایران باید عنایت داشت از آنجا که ایران به کنوانسیون‌های پالرمو و تأمین مالی تروریسم نپیوسته است، لزومی به رعایت قوانین و مقررات این کنوانسیون‌ها در خصوص ارزهای رمزنگاری‌شده ندارد، لکن به نظر درصورتیکه ایران حتی تمایلی به پیوستن به این نهادها نداشته باشد نیز باید مقررات مربوط به پولشویی طریق ارزهای رمزنگاری‌شده را اجرا کند و مؤسسات ارائه‌کنندهٔ خدمات این ارزها را ملزم به اجرای این قوانین سازد. از منظر قوانین فعلی باید گفت که وفق بند «ب» مادهٔ ۱ این قانون مال عبارت است از «هر نوع دارایی اعم از مادی یا غیرمادی، منقول یا غیرمنقول، مشروع یا غیرمشروع و هر نوع منفعت یا امتیاز مالی و همچنین تمامی اسناد مبیّن حق اعم از کاغذی یا الکترونیکی نظیر اسناد تجاری، سهام یا اوراق بهادار». بر این اساس ارزهای

رمزنگاری‌شدهٔ مشمول تعریف این قانون از مال قرار خواهند گرفت. افزون‌بر این در بند «چ» این ماده معاملات و عملیات مشکوک شامل هر نوع معامله، دریافت یا پرداخت مال اعم از فیزیکی یا الکترونیکی یا شروع به آنهاست که براساس قرائن و اوضاع و احوالی مانند موارد زیر ظن وقوع جرم را ایجاد کند، دانسته شده است. بر این اساس غیرمادی بودن ارزهای رمزنگاری‌شده سبب نمی‌شود که معاملات آنها از دایرهٔ شمول این قانون خارج شود. البته براساس مادهٔ ۵ این قانون برخی اشخاص موظف به اجرای پاره‌ای از وظایف محوله توسط این قانون هستند. این در حالی است که عمده معاملات این ارزها در داخل کشور از طریق «صرافی‌های ارزهای دیجیتال» صورت می‌پذیرد که در فقدان قانون در خصوص ارزهای رمزنگاری‌شده به شکل غیررسمی به فعالیت اشتغال دارند و این مسئله سبب شده است که این مؤسسات اولاً تکلیفی در خصوص اجرای ضوابط این قانون نداشته باشند و ثانیاً مجوزی در جمع‌آوری اطلاعات مشتریان خود نیز نداشته باشند، ازاین‌رو با وجود چنین خلأ قانونی، اساساً احراز هویت کاربران (موضوع بند ۱ مادهٔ ۷) و حفظ اطلاعات مزبور توسط صرافی‌ها و ارائهٔ اطلاعات معامله‌گران مشکوک به نهادهای نظارتی (موضوع بندهای «ب» و «پ» مادهٔ ۷)، امکان‌پذیر نباشد، بر همین اساس لازم است که در خصوص قانون‌مدار کردن این ارزها اقدامات لازم صورت پذیرد.

منابع

الف) فارسی

۱. ارجمندنژاد، عبدالمهدی (۱۳۸۴). *شناسایی کافی مشتری از سوی بانک‌ها*، مدیریت کل نظارت بر بانک‌ها و مؤسسات اعتباری (ادارهٔ مطالعات و مقررات بانکی).

۲. سید حسینی، میرمیثم؛ دعایی، میثم (۱۳۹۳). *بیت‌کوین نخستین پول مجازی*، مدیریت پژوهش، توسعه و مطالعات سازمان بورس اوراق بهادار، گزارش تحقیقاتی ۹۳-۶-۲۰۱۴.

۳. عزیزی، فاطمه؛ سلیمانی، هادی (۱۳۹۸). «معرفی بیت‌کوین و چالش‌های امنیتی آن»، *پدافند غیرعامل*، ش ۴۰.

۴. مددی، مهدی؛ قائمی خرق، محسن؛ شفیعی، قاسم (۱۴۰۰). جستار فقهی حقوقی در مسئلهٔ قانونمندسازی «ارزهای رمزنگاری‌شده»، *مجلس و راهبرد*، دورهٔ ۲۸، ش ۱ (پیاپی ۱۰۵).

۵. میرزاخانی، رضا (۱۳۹۶)، *بیت‌کوین و ماهیت مالی - فقهی پول مجازی*، مرکز پژوهش، توسعه و مطالعات اسلامی سازمان بورس و اوراق بهادار، گزارش تحقیقاتی ۹۶-۲۰-۲۰۱۷.

۶. نوری، مهدی؛ نواب‌پور، علیرضا (۱۳۹۷). *مقدمه‌ای بر تنظیم‌گری رمزینهٔ ارزها در اقتصاد ایران*، شمارهٔ مسلسل ۱۵۹۳۲، مطالعات اقتصادی مجلس.

ب) انگلیسی

7. Castor, amy (2019). "Spanish authorities: bitcoin ATMs expose hole in AML laws" https://www.atmmarketplace.com/articles/spanish-authorities-bitcoin-atms-expose-loophole-in-aml-laws/

8. European Central Bank (E.C.B), (2012). "Virtual Currency Schemes." Technical Report, October. Available at https://www.ecb.europa.eu/pub/pdf/other/ virtualcurrencyschemes201210en.pdf
9. FATF (2014). "Virtual Currencies Key Definitions and Potential AML/CFT Risks".
10. FATF (2015). "GUIDANCE FOR A RISK-BASED APPROACH VIRTUAL CURRENCIES".
11. FATF (2020). "INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION The FATF Recommendations".
12. Quinlan, Benjamin & Kwan, Yvette (2016). From KYC to KYT, QUINLAN & ASSOCIATES, https://www.quinlanandassociates.com/wp-content/uploads/2018/03/Quinlan-Associates-From-KYC-to-KYT-new.pdf.
13. Ruffing T., Moreno-Sanchez P., Kate A. (2014). "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" In: Kutyłowski M., Vaidya J. (eds) Computer Security - ESORICS 2014. ESORICS 2014. Lecture Notes in Computer Science, Vol 8713. Springer, Cham
14. Strehle, Elias, & Ante, Lennart (2020). "Exclusive Mining of Blockchain Transactions" BRL Working Paper Series No. 13.