

چالش‌های دادرسی عادلانه در جرایم مالی ناشی از رمز ارزها

(تاریخ دریافت ۱۴۰۲/۰۵/۱۵، تاریخ تصویب ۱۴۰۲/۰۶/۱۰)

مریم سنجابی

چکیده

روند جهانی و تجربیات دیگر کشورهای جهان نشان می‌دهد که نظام قضایی در معرض مسائلی خواهد بود که به جهت مستحدثه بودن آن‌ها دور از انتظار نیست که تمهیدات تقنینی، ساختاری و انسانی لازم برای مواجهه با چنین مسائلی وجود نداشته باشد. با توجه به رشد و گسترش فناوری‌های ارتباطی و رایانه‌ای، یکی از مهم‌ترین این پدیده‌ها، ظهور پول‌های مجازی در جامعه ایران است. این ارزها چالش‌های حقوقی و اقتصادی بسیاری را برای نظام‌های سیاسی ایجاد می‌نمایند. ویژگی‌هایی نظیر غیرمتمرکز بودن و فرامرزی بودن این قبیل ارزها سبب شده است تا این حوزه به منظور انجام فعالیت‌های مجرمانه، مورد توجه بزهکاران قرار گیرد. این مقاله با روش توصیفی و تحلیلی و از طریق جستجو در پی پاسخ به این سؤال است که دادرسی عادلانه برای رسیدگی به جرایم مالی ناشی از رمز ارزها با چه چالش‌هایی مواجه می‌باشد. در یافته‌های به دست آمده از تحقیق، نمایان می‌گردد که فارغ از خصوصیات اختصاصی ارزهای مجازی، مبهم بودن وضعیت قانونی و به ویژه قلمروی فعالیت‌های مجرمانه در حوزه دادرسی این قبیل جرایم از مهم‌ترین چالش‌های نظام عدالت کیفری می‌باشد. از مهم‌ترین راهکارهای پیشنهادی می‌توان ابتدا به اصلاح و وضع قوانین مرتبط و تعریف دقیق قانونی از ارزهای مجازی و سپس تعیین ماهیت حقوقی آن‌ها اشاره نمود.

واژگان کلیدی: ارزهای مجازی، ارزهای الکترونیکی، دادرسی عادلانه، جرایم مالی،

چالش‌های دادرسی، پولشویی

بخش اول: تحلیل و واکاوی اولیه موضوع

ارزهای رمزآنگاری شده یا «رمزارزها» به ارزیابی گفته می‌شود که بر اساس فناوری رمزآنگاری^۱ شده، ذیل عنوان کلی «ارزهای مجازی» به تضمین امنیت و صحت مبادلات در غالب عملکردی مشخص می‌پردازند. پرداخت ارزهای مجازی، شکلی از پرداخت هستند که به شکل الکترونیکی خلق و ذخیره می‌گردند.^۲

رمزارز یا ارز رمز، پایه یا کریپتوکارنسی یک مسئله جهانی است. این روزها رمزارز، مورد توجه افراد زیادی در جهان و کشور ما قرار گرفته است و از حقایقی می‌باشد که بروز آن در جامعه، قابل انکار نیست و هر روزه بر دامنه بستر مبادلات اینترنتی افزوده می‌گردد. ظهور این ارزها به اختراع بیت کوین^۳ در سال ۲۰۰۹ برمی‌گردد که عنوان معروف‌ترین ارز مجازی را نیز به خود اختصاص داده است. بیش از ۱۵۰۰ ارز مجازی وجود دارد که تنها تعداد کمی از آنها معروف‌اند و مبادله با آنها صورت می‌گیرد. این ارزها عبارت‌اند از مونرو، بایت بال، لایت کوین، ریپل، اتریوم و بیت کوین.

از سال ۲۰۰۸، بیت کوین به صورت یک سامانه پرداخت نوین، توسط شخص یا اشخاصی با نام «ساتوشی ناکاموتو» به عنوان یک ارز مجازی جایگزین برای پرداخت‌های سنتی و به ویژه پول به جهان معرفی شد. دامنه پایگاه Bitcoin.org در ماه اوت همان سال در شبکه اینترنت به ثبت رسید. در اکتبر سال ۲۰۰۸ مؤسسين آن در خبرنامه رمزگذاری شده‌ای به نام metzdowd اعلام کردند که ما در حال کار روی سامانه پول الکترونیکی جدیدی هستیم که کاملاً شخصی بوده و عاری از دخالت هر شخص ثالثی است. این رمزارز در نهایت در سال ۲۰۰۹ عملیاتی شد و جریان تازه‌ای را در دنیای داد و ستد به صورت پرداخت غیرمتمرکز و شخص به شخص رقم زد، بدون آنکه نیازمند وجود شخص یا صرافی و بانک و نظایر آنها باشد. بیت کوین را باید به عنوان نخستین ارز مجازی غیرمتمرکز معرفی نمود که با گذر از

^۱. Cryptography

^۲. Dibrova, Alina. . "Virtual currency: new step in monetary development", ۴۲-۴۹.

^۳. بیت کوین با حرف اول بزرگ (Bitcoin)، دربردارنده نرم‌افزار منبع باز است که هم به ایجاد رمزارز بیت کوین و هم شبکه شخص به شخص (p2p) اشاره دارد. بیت کوین با حروف کوچک (bitcoin) به معنی واحدهای ارزش رمزارز بیت کوین است.

بحران مالی سال ۲۰۰۸ توجه عموم را به خود معطوف ساخت.^۱ قدرت حقیقی این شبکه به کاربران آن برمی گردد و نیازی به مرجع مرکزی و واسطه‌ای برای مدیریت و دخل و تصرف در آن نیست. بهره‌گیری از ارزهای مجازی به عنوان روشی برای پرداخت جهت خرید و فروش محصولات و خدمات تحت نام «روش برخط و پنهان»، از دلایل جذابیت این ارزهای رمزنگاری شده برای کاربران آن است. تا سال ۲۰۱۶ چیزی حدود ۱۶ میلیون بیت کوین جریان داشت و مورد استفاده شرکت‌ها و کاربران آن قرار گرفت (Greenfield, ۲۰۱۶) و تا اوایل سال ۲۰۲۰ میزان آن به ۱۸/۵ میلیون بیت کوین رسید.^۲

از زمانی که این رمزارزها و ارزهای دیجیتال مطرح گردید، ابعاد کیفری و جرم‌شناسی آن برای نظام عدالت کیفری اهمیت یافت و بررسی ابعاد جنایی آن قوت گرفت.^۳ بهره‌گیری از فناوری‌های پیچیده و تثبیت خصوصیات نظیر ناشناختگی هویت از مهم‌ترین خصوصیات است که ارزهای مجازی را برای تبهکاران این عرصه، جذاب و آینده‌دار کرده است.^۴ همین امر سبب می‌شود تا مجرمان با استفاده از قابلیت‌های این پدیده و با توجه به ناشناختگی آن برای همگان، به ارتکاب جرایم مالی و اقتصادی در این عرصه پردازند و کشف جرم و رسیدگی به آن را با چالش‌های جدی روبه‌رو سازند. ارزهای مجازی به جهت مبهم بودن کاربران آن‌ها، عدم آشنایی قضات و دادرسان و ضابطین قضایی در رسیدگی به جرایم حاصل از آن‌ها و نحوه کارکرد آن‌ها، با وضعیت قانونی مبهمی مواجه می‌گردد. قوانین موجود برای کشف، تعقیب و دادرسی ارزهای مجازی با استناد به خصوصیات ویژه آن با چالش‌هایی روبه‌رو است. به منظور شناسایی و ارائه راهکارهایی در حد بضاعت، در ابتدا به واکاوی مفهومی ارزهای مجازی و تعیین مصادیق آن پرداخته می‌شود، با این هدف که از گذر آن، چالش‌های حقوقی-اقتصادی ارزهای مجازی در سیستم عدالت کیفری ایران به درستی شناخته شود و پس از آن، چالش‌ها و

^۱. Sessa, Kethineni, Ying, Cao, Cassandra, & Dodge. "Use of bit coin in dark net markets: examining facilitative factors on bit coin-related crimes", ۱۴۲

^۲. <https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined>

^۳. شاملو، باقر، و خلیلی پاجی عارف. «چالش‌های حقوقی اقتصادی ارزهای مجازی برای نظام‌های سیاسی در پرتو نظریه جایگزینی»، ۱۲۸.

^۴. خلیلی پاجی، عارف. امکان‌سنجی تأمین مالی تروریسم در پرتو ارزهای مجازی، ص ۱۱۳-۱۱۴.

خلاءهای نظام حقوقی ایران در دادرسی عادلانه جرایم ناشی از رمزارزها مورد مذاقه قرار می‌گیرد. در پایان، با بیان ضرورت‌های جرم‌انگاری در حوزه رمزارزها با هدف حمایت از امنیت اقتصادی، مقابله با خطرات این جرم و احتیاط‌انگاری سیاست جنایی ایران، راهکارهایی جهت رفع خلاءها و چالش‌های موجود پیشنهاد می‌گردد. هدف پژوهش حاضر، کاربردی می‌باشد و امید است برای محققان و علاقه‌مندان این حوزه، منبع تحقیقی مفیدی باشد و در رفع چالش‌های عدالت کیفری در رسیدگی به جرایم مالی رمزارزها مفید واقع گردد.

بخش دوم: بررسی کلی مفاهیم کلیدی

در هر تحقیقی ارائه تعاریف دقیق از مفاهیم کلیدی آن به منظور جلوگیری از ابهامات احتمالی ضروری است. ارز در اصطلاح، معادل فارسی «Currency» می‌باشد و ریشه لاتین آن «Currens» به معنی در گردش است.^۱ ارز مجازی^۲ با عبارات متعدد اما در معنا تا حدودی یکسان نظیر ارز مخفی، رمزینه پول، ارز رمزپایه و ارز دیجیتال نیز شناخته می‌شود.

در تعریفی از ارز مجازی آمده است که این ارز، نماینده دیجیتالی ارزش می‌باشد که نهاد صادر کننده آن، بانک مرکزی یا سایر نهادهای دولتی نیستند و فاقد هرگونه ارتباطی با پول‌های رایج ملی و نحوه صدور آنها هستند. این ارزها به وسیله اشخاصی به صورت روش پرداخت مقبول واقع گردیده و قادر است منتقل یا از طرق الکترونیکی مبادله گردد.^۳

گروهی دیگر، ارزهای مجازی را نماد دیجیتالی ارزشی معرفی می‌نمایند که قادر است به صورت دیجیتال معامله گردد و به شکل ابزاری برای تبادل یا واحد حساب یا ذخیره ارزش عمل کنند، بدون آنکه در هر کشوری، جایگاه پول رایج قانونی را با پشتوانه‌های مرسوم آن

^۱. قربانی، احمد. پول و ارز و بانکداری، قابل دسترس در <http://poolvbank.com>

^۲. Virtual Currency

^۳. Dabrowski, Marek, & Janikowski, Lukasz. Virtual currencies and central banks monetary policy: challenges ahead. European Parliament's Committee on Economic and Monetary Affairs. ۹.

دارا باشند. جالب توجه است که دولت‌ها اقدام به صدور آن نکرده و آن را تضمین نمی‌کنند و این ارزها، کارکرد و مقبولیت خود را مدیون توافق میان کاربران هستند.^۱

در تعریفی که توسط بانک مرکزی اروپا از ارز مجازی ارائه شده است، این ارز، نوعی از پول دیجیتال و غیرقانونی خوانده می‌شود که از طریق گسترش دارندگان آن، اصدار یافته و تحت کنترل در می‌آید و در فضایی مجازی به وسیله عضویت اشخاص و میزان به کارگیری آن‌ها مقبولیت پیدا می‌کند.^۲

صندوق بین‌المللی پول در ارائه تعریفی از پول مجازی، آن را نشانگر دیجیتال ارزش می‌خواند که توسط توسعه‌دهندگان خصوصی تأسیس گردیده است و در میان آنان، به عنوان واحد ارزش در نظر گرفته می‌شود.^۳

در تعریفی دیگر، گروه ویژه اقدام مالی^۴، تمامی اوصاف اساسی پول فیزیکی را به این قبیل ارزها نیز سرایت داده‌اند و تنها وجه تمایز این ارزها را با پول در این می‌دانند که پول مجازی، تحت سیطره و نفوذ قواعد کشورها در نمی‌آید. به موجب این تعریف، ارزهای مجازی، به شکل اینترنتی و مجازی، به عنوان وسیله‌ای برای مبادله واحد سنجش ارزش یا ذخیره ارزش، موضوع تجارت قرار گرفته‌اند، اما هیچ نظام قانون‌گذاری، آن را نمی‌پذیرد.^۵

رمزارزها یا همان کریپتوکارنسی (Cryptocurrency) از تجمع دو لغت «Crypto» به معنای رمزی، سری، پنهانی و «Currency» به معنای پول رایج یا ارز به وجود آمده است و معنای جمعی آن، پول یا ارزی است که بر مبنای علوم رمزنگاری ایجاد شده است و می‌تواند

^۱. Financial Action Task Force. Virtual Currencies – Key Definitions and Potential AML/CFT Risks, ۴.

^۲. European Central Bank. Virtual Currency Schemes, available at: <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes20110en>

^۳. Dong, He, Karl, Habermeier, Ross, Leckow, Vikram, Kyriakos-Saad, Hiroko, Oura, Tahsin Saadi Sedik, Natalia, Stetsenko. Virtual Currencies and Beyond: Initial Considerations, Initial Considerations. v

^۴. Financial Action Task Force (FATF)

^۵. Financial Crimes Enforcement Network guidance. available at: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G-001.pdf>

با استفاده از علم ریاضیات، کدهای رمزنگاری شده‌ای را به وجود آورد تا داده‌ها، هویت و... پنهان شود و کسی نتواند در روند تولید، انتشار و صورت دادن مبادله‌ها اختلالی ایجاد نماید. در بیانی دقیق، ارزهای دیجیتال^۱ ارزیابی هستند که به شکل الکترونیکی ذخیره و انتقال داده می‌شوند. این تعریف، شامل هر پولی است که بر اساس صفر و یک تعریف گردد؛ فارغ از اینکه بر مبنای پول سنتی و بانکی قرار گیرد یا بر پایه ارزهای مجازی واقع گردد.^۲

ارز مجازی از این جهت که غیر ملموس است، نوعی ارز دیجیتال شناخته می‌شود و از آن جهت متمایز می‌گردد که پول دیجیتال، نماینده اسکناس‌های بانکی است که فقط سازوکار آن غیر فیزیکی است، حال آنکه ارز مجازی، فاقد هرگونه ارتباطی با پول بانکی است و ارز جدیدی شناخته می‌شود که تأسیسی انحصاری دارد.^۳ ارزهای مجازی تقسیماتی دارند که دقت نظر در تأسیس نهادی به نام «نهاد مرکزی» یا عدم وجود آن و امکان مبدل ساختن آنان به ارزهای دیگر و مزج این خصوصیات سه نوع برای آنان قابل تصور می‌باشد که عبارت‌اند از: ارز مجازی متمرکز قابل تبدیل، ارز مجازی غیر قابل تبدیل و ارز مجازی غیر متمرکز قابل تبدیل. ارزهای مجازی غیر قابل تبدیل^۴ را نمی‌توان به هیچ صورتی به پول‌های بانکی تبدیل نمود، چرا که این ارزها دارای خصیصه متمرکز بودن می‌باشند و خالق آن، نهاد منتشر کننده‌ای است که دفتر کل را نزد خود محفوظ می‌دارد.

ارز مجازی متمرکز قابل تبدیل^۵، ارزی است که می‌شود آن را به وجه رایج و ملموس حقیقی کشورها مبدل ساخت و از آن برای مبادلات به هر شکل بهره جست. در این نوع ارز مجازی،

^۱. Wikipedia: *Digital currency* (digital money, electronic money or electronic currency) is a type of currency available in digital form (in contrast to physical, such as banknotes and coins)

^۲. Wagner, Andrew. Digital vs. Virtual Currencies, ۳. <https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-۱۴۰۸۷۳۵۵۰۷>

^۳. نواب‌پور، علیرضا، یوسفی، احمدعلی، و طالبی، محمد. تحلیل فقهی کارکردهای پول‌های رمزنگاری شده، مطالعه

موردی بیت کوین،^۴.

^۴. Non-convertible

^۵. Convertible

یک نهاد مرکزی، مدیریت آن و کنترل سیستم را بر عهده دارد و به دیگر ارزهای مجازی و یا پول‌های واقعی مانند دلار، یورو و... و بالعکس قابل تبدیل است.^۱

این گروه به دو دسته متمرکز و غیرمتمرکز قابل تقسیم است. در ارزهای متمرکز، نهاد مرکزی بر انتشار و کنترل ارز نظارت دارد، حال آنکه در دسته غیرمتمرکز، کلیه فرآیندها نظیر انتشار و تأیید تراکنش‌ها به وسیله اشخاصی و با بهره‌گیری از سازوکارهای علوم ریاضی رمزنگاری می‌گردد و این کار توسط نهاد مرکزی انجام نمی‌شود. الگوهای مقرر شده حاوی رمز، صحت معاملات را مورد تأیید قرار می‌دهند و کاربران قادر به ایجاد تغییر در این الگوها نیستند.^۲ رمزارزها در گروه ارزهای مجازی غیرمتمرکز^۳ جای می‌گیرند و مصادیق گوناگونی دارند که در ابتدای امر ممکن است آن‌ها را نتوان رمزارز به معنای حقیقی دانست، اما از جمله ارزهای مجازی متمرکز به شمار می‌روند.

بخش سوم: مزایا و معایب رمزارزها

بند اول: مزایا

- آزادی در پرداخت و دسترسی بین‌المللی: با این پول می‌توان وجه دلخواه را به سرعت به هر کسی در هر جای دنیا بدون کارمزد و وجود نهاد واسطه منتقل نمود. در کشورهایی که به دلایل تحریمی، مبادلات با دشواری‌هایی روبه‌روست، رمزارزها می‌توانند امتیازات ویژه‌ای را برای تعاملات مالی در ابعاد بین‌المللی فراهم آورند.^۴

- سرعت انتقال در این روش پرداخت، بسیار بالا است، به نحوی که در دقایقی اندک، انتقال صورت می‌گیرد. حتی کاربر و صاحب حساب این امکان را دارند که در صورت نیاز، با تعریف کارمزد برای تراکنش خود، سرعت تراکنش را بالا برده و آن را تعیین کنند.

^۱. UNODC. Basic Manual on the detection and investigation of the laundering of crime proceeds using virtual currencies, ۱۲

^۲. همان، صص ۵ و ۶.

^۳. Non-centralised Virtual Currency

^۴. Chuen, D. L. K. *Handbook of digital currency: Bitcoin, Innovation, financial instrument, and big data*, ۲۰۱۵.

- به علت غیر قابل شناسایی بودن گیرنده و فرستنده برای کشورهای که مورد تحریم واقع می‌شوند، نظیر ایران، این روش فرصت مناسبی برای آن‌ها است تا تعاملات مالی خود را به سرانجام رسانده و دریافت و پرداخت غیر قابل کنترل داشته باشند. بنابراین تحریم‌ها فاقد قدرت لازم برای اعمال فشار خواهند بود.

- قابلیت رهگیری: هر ارز دیجیتال در تمامی ابعاد خود، قابلیت رهگیری را داراست و تمامی مسیرهای آن از ابتدا تا انتهای امر مشخص است.

- از معایب نظام‌های متعارف پرداخت در سطح بین‌المللی، هزینه‌های معاملاتی بالایی است که واسطه، آن را دریافت می‌کند، اما در نظام‌هایی نظیر بیت کوین به دلیل عدم وجود واسطه‌ها از هزینه‌های معاملاتی کاسته می‌شود و این امکان برای هر شخص فراهم می‌گردد تا بتواند بدون نیاز به پرداخت پول اضافه، وجه خود را منتقل نماید. ویژگی منحصر به فرد دیگر آن نیز عدم امکان مصادره و بلوکه کردن آن توسط دولت‌ها است.^۱

بند دوم: معایب

به عنوان مهم‌ترین ایراد باید از ابهام در ماهیت ارزهای مجازی نام برد که برخی کشورها آن را جزو کالا، برخی دیگر به عنوان دارایی نامشهود و برخی آن را به عنوان یک پل می‌شناسند و روشن است که رویه واحدی در این خصوص وجود ندارد. این قبیل تراکنش‌ها فاقد نظارت روزانه هستند و سیاست‌های پولی، امکان اعمال پیدا نمی‌کنند، زیرا در این گونه داد و ستدها، نهاد واسطه حذف گردیده است. از سوی دیگر، ایجاد مشکلات امنیتی، دور از ذهن نیست، چرا که الکترونیکی بودن پول‌های مجازی، آن را با دشواری‌هایی همچون گم شدن، هک شدن حساب کاربر و سرقت مواجه کرده است. برگشت‌ناپذیری وجه در این سیستم، اشکال عمده بعدی این قبیل ارزها و تراکنش‌های مربوط به آن‌ها می‌باشد.

لازم به ذکر است فقدان مستند قانونی، از جمله معایب بسیار مهم دیگر ارزهای مجازی است، زیرا زمانی که کالا به صورت اینترنتی خریداری گردید، اما ارسال نشد، اثبات واریز وجه، با دشواری‌های بسیاری مواجه خواهد بود.

۱. فرقان‌دوست حقیقی، کامبیز، و نداف، رضوانه. «مروری بر رمزارزها، فرصت‌ها و تهدیدها»، ۶۱-۷۴.

بخش چهارم: لزوم جرم‌انگاری در حوزه رمزارزها

اهمیت روزافزون ارزهای مجازی از منظر جرایم مالی، بررسی جرم‌شناختی آن را اجتناب‌ناپذیر کرده است. بخش وسیعی از جرایم، از طریق رمزارزها امکان تحقق می‌یابند که در زیر به رایج‌ترین آن‌ها پرداخته می‌شود. این جرایم، جنبه حصری نداشته‌اند و در مواردی این امکان وجود دارد که بتوان مصادیق دیگری را نیز با توجه به شرایط برای آن در نظر گرفت. رمزارزها در زمینه‌هایی همچون سرقت، قاچاق، پول‌شویی، فروش اسناد جعلی، قاچاق مواد مخدر، کلاهبرداری و تأمین مالی تروریسم پرداخت می‌گردند، اما گسترده‌ترین بخش فعالیت‌های مجرمانه در استفاده از رمزارزها، استفاده از آن‌ها برای پرداخت‌های مربوط به مواد مخدر و روان‌گردان است.^۱ رمزارزها نیز امکان به سرقت رفتن را دارند و می‌توانند موضوع جرم سرقت واقع شوند. با وجود اینکه کشورها تمهیدات مؤثری در جهت شناسایی قانونی و رسمیت‌بخشی به ماهیت رمزارزها نیاندیشیده‌اند، اما نمی‌توان مالیت داشتن و ارزشمندی آن را انکار نمود و انتساب عنوان سرقت به آن را در پرتوی ابهام در مالیت داشتن آن ممکن ندانست.^۲ بی‌تردید ارزهای مجازی، با وجود اینکه فاقد ماهیت فیزیکی و ملموس هستند، شیء دانسته می‌شوند. همچنین در صورت قرار گرفتن در ید شخصی، معنای ملک می‌یابند و بدون رضایت مالک، امکان تصرف آن‌ها وجود ندارد. بدیهی است خارج کردن ارزهای مجازی از تصرف دارنده، بدون رضایت شخص، سبب مسئولیت می‌گردد. قانون مبارزه با پول‌شویی مصوب سال ۱۳۸۶ اولین قانون در زمینه مبارزه با پول‌شویی در کشور ایران محسوب می‌شود. در مواد ۴، ۵ و ۶ این قانون، کلیه اشخاص حقیقی و حقوقی، به خصوص بانک‌ها و مؤسسات مالی و اعتباری موظف‌اند آیین‌نامه‌های این قانون را رعایت نمایند. شورای عالی مبارزه با پول‌شویی به ریاست و مسئولیت وزیر امور اقتصادی و دارایی، مسئولیت تدوین آیین‌نامه‌ها و اجرای مفاد این قانون را برعهده دارد. به نظر می‌رسد با توجه به تجربیات جهانی دبیرخانه شورای عالی مبارزه با پول‌شویی، تکلیف قانونی لازم برای کنترل مراکز مبادله پول مجازی با

^۱. Ivantsov, Sergey; Sidorenko, Elina; Spasennikov, Boris; Berezkin, Yuri & Sukhodolov, Yakov. "Cryptocurrency-related crimes: key criminological trends", ۸۷.

^۲ Korennaya, Anna, & Tydykova, Nadezhda. "Crypto currency as an object and instrument of committing crime", ۴۱۲-۴۱۳.

پول رایج کشور برعهده این شورا می‌باشد. این امکان وجود دارد که این شورا به منظور حکمرانی بهتر، نیازمند اختیارات وسیع‌تری باشد که این امر در حدود هیئت وزیران قابل اعمال می‌گردد، اما در جلسه شورای عالی مبارزه با پول‌شویی در تاریخ ۹ دی‌ماه سال ۱۳۹۶، ممنوعیت به‌کارگیری ابزار بیت کوین و سایر رمزارزها در تمامی مراکز پولی و مالی کشور اعلام گردید. واحدهای مربوطه باید از انجام هرگونه خرید و فروش ارزهای مذکور و یا انجام هرگونه اقدامی که به تسهیل و یا ترویج ارزهای یاد شده بینجامد، به‌طور جدی دوری نمایند. تجربه‌های کشورهای دیگر و مقایسه آن‌ها با قوانین ایران آشکار می‌سازد که قانون مالیات‌های مستقیم مصوب سال ۱۳۹۴ مجلس شورای اسلامی در زمینه مالیات‌های بر درآمد در زمینه رمزارزها، امکان اعمال در کشور را یافته است و مسئولیت این امر بر عهده سازمان امور مالیاتی جهت تولید اجرای قانون فوق است.

ماده ۹۳ این قانون بیان می‌دارد درآمدهای که شخص حقیقی از طریق اشتغال به مشاغل یا به عناوین دیگر غیر از موارد مذکور در سایر فصل‌های این قانون در ایران تحصیل کند، پس از کسر معافیت‌های مقرر در این قانون، مشمول مالیات بر درآمد مشاغل است. از این ماده چنین استنباط می‌گردد که درآمدهای ناشی از خرید ارزهای مجازی نیز می‌تواند مشمول حکم این ماده شود. تجربه دیگر کشورها در زمینه فروش ارز مجازی به عنوان فروش کالا، درآمدهای را به وجود می‌آورد که از آن می‌توان به عنوان درآمد مشمول مالیات شخص حقیقی نام برد. در ماده ۹۷ از این قانون، مدیریت نحوه اخذ مالیات از ارزهای مجازی بر عهده سازمان امور مالیاتی خواهد بود.

بخش پنجم: مصادیق جرایم مرتبط با رمزارزها

بند اول: سرقت

ارز مجازی نیز امکان سرقت و یا مفقود شدن را دارد. نگهداری رمزارزها نیز با دشواری‌هایی روبه‌رو است و برخط بودن، آن‌ها را در معرض سرقت قرار می‌دهد. روش سارقان، به‌کارگیری بدافزارها یا هک کردن رایانه یا حساب شخصی افراد است که به دنبال آن، رمزارزها را به سرقت می‌برند. رمزارزهایی نظیر بیت کوین تنها از کیف پول‌های مجازی به

سرقت نمی‌روند، بلکه کسب و کار صرافیهایی نظیر Flexcoin^۱ نیز مورد حمله قرار می‌گیرند.

بند دوم: کلاهبرداری

کلاهبرداری عنوان دیگری است که باید به آن اشاره کرد. رمزارزهای مجازی، دارای خطر بالای کلاهبرداری هستند. در عصر حاضر، فضای سایبر، ابزار تسهیل کننده جرم پول‌شویی شده و با وجود آن، کمک شایانی به گسترش چشمگیر و روزافزون این پدیده کرده است. در جرم کلاهبرداری سستی، مانور متقلبانه برای اغفال فرد و بردن مال وی صورت می‌گیرد. در خصوص استفاده از رمزارزها نیز این طور به نظر می‌رسد که می‌توان مرتکب این جرم مالی گردید، زیرا در فضای سایبر می‌توان به راحتی مرتکب عملیات متقلبانه شد؛ از ناآگاهی و عدم کفایت اطلاعاتی افراد در برخورد با فناوری‌های نوین، سوء استفاده و برای اغفال و بردن اموال آن‌ها اقدام کرد. شایع‌ترین روش‌های کلاهبرداری در رابطه با استفاده از رمزارزها، مربوط به عملیات کیف پول دیجیتال است. به طور مثال، سایت‌های جعلی با به کارگیری تبلیغات گسترده در فضای مجازی، برای کسب اعتماد مردم تلاش می‌کنند تا با دریافت مبالغ و اطلاعات لازم از این افراد، اقدام به ایجاد حساب کاربری و کیف پول دیجیتال کنند و پس از آن، صاحبان این سایت‌ها با دریافت پول ناپدید می‌شوند و کیف پولی توسط صاحبان اصلی حساب دریافت نمی‌گردد یا اینکه با استفاده از کلید خصوصی که دارند، در اولین واریز رمزارز به کیف پول مربوطه، اقدام به برداشت خود کار آن می‌کنند.

^۱. See: The Troubling Holes in MtGox's Account of How It Lost ۶۰۰ Million in Bitcoins, MIT TECH. REV. <http://www.technologyreview.com/view/۵۲۶۱۶۱/the-troubling-holes-inmtgoxs-account-of-how-itlost-۶۰۰-million-in-bitcoins/>; Takashi Mochizuki & Eleanor Warnock, Mt. Gox Finds ۲۰۰,۰۰۰ Missing Bitcoins, WALL ST. J., Mar. ۲۱, ۲۰۱۴, at C۲; Dylan Love, ۵۵۰۰ Million Worth of Bitcoin Has Been Stolen Since ۲۰۱۰, BUS. INSIDER, <http://www.businessinsider.com/how-many-bitcoins-have-beenstolen-۲۰۱۴-۳>. L Kate, 'The Rise and Fall of Mt Gox, Everything You Need to Know' (۲۵ March ۲۰۱۴) <https://coinreport.net/editorial-risefall-mtgox/>

راه های دیگری نیز وجود دارد. حملات فیشینگ در واقع با سوء استفاده از ضعف های امنیتی یک سایت صورت می گیرند. اجرای آن ها به این شکل است که ایمیل یا پیامی با مضامین مهم از سوی فرد کلاه بردار به قربانی ارسال می شود که او را وادار می کند اطلاعات بسیار مهمی از جمله رمز عبور، رمز دوم کارت بانکی و اطلاعاتی از این قبیل را در یک وبسایت جعلی وارد کند با این خیال که مشغول تکمیل اطلاعات خود در سایتی مهم و آشنا است. در واقع، فیشینگ، نوعی عملیات مهندسی اجتماعی- روانی است که با استفاده از غفلت، ساده انگاری و اشتباهات سهوی افراد، دارایی آن ها را به سرقت می برد. عرصه ارز دیجیتال از فضاهایی است که فیشرها به آن بسیار علاقه مند هستند و یکی از ترفندهای رایج کلاه برداری صرافی های آنلاین ارز دیجیتال این است که با جعل کیف پول و یا وبسایت خاصی کاربران را می فریبند با خیال اینکه مشغول انجام عملیات مالی برای دریافت خدمات معمولی و معتبر هستند. افراد اطلاعات کلیدی خود را در محل دلخواه کلاه برداران وارد می کنند و به سادگی مورد سرقت قرار می گیرند. در شرایط دیگری، سایت کلاه بردار ادعا می کند که درصد ناچیزی از رمزارز تولید شده را به عنوان حق الزحمه خود برمی دارند. اولین و مهم ترین اصل در حفاظت از سرمایه در بازارهای مالی دیجیتال، احتیاط، دقت کامل و پرهیز از سهل انگاری است. استخراج ارزهای دیجیتال یا ماینینگ معمولاً بسیار هزینه بر بوده و تجهیزات ویژه ای می طلبد و همین امر، این موضوع را تبدیل به راهی برای کلاه برداری صرافی های آنلاین ارز دیجیتال نموده است. تبلیغات گسترده ای با عناوین کسب درآمد عالی با استخراج ارز و اجاره دستگاه استخراج بیت کوین در فضای مجازی وجود دارد^۱.

بند سوم: پول شویی سایبری

پول شویی سایبری به روش هایی گفته می شود که با هدف ایجاد اختلال در نظام ارزی، نفوذ در کشورها، اختلال در امنیت و مرزهای حاکمیتی، جابه جایی دارایی های نامشروع و تأمین

^۱ نوری، مهدی، و نواب پور، علیرضا، «طراحی چارچوب مفهومی سیاست گذاری ارزهای مجازی در

مالی گروهک‌های تروریستی برنامه‌ریزی و انجام می‌شوند.^۱ رمزارزها که بر روی بستر زنجیرهای بلوکی فعالیت می‌نمایند جهت نقل و انتقال و هر فعل دیگری، نیازمند وجود کیف پول دیجیتال است.^۲ کیف پول دیجیتال، دارای کلید عمومی و خصوصی می‌باشد و کلید خصوصی تنها راه ورود به حساب کاربری و کیف پول دیجیتال خواهد بود. 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 شناسایی هویت اشخاص و تراکنش‌های مربوط به آن قابل پیگیری نیست.^۳ هویت نامعلوم و ناشناس صرافی‌های زیرزمینی، عاملی اساسی و تعیین کننده برای فعالیت‌های این چنینی خواهد بود. همچنین افرادی با تأسیس شرکت‌های خدماتی و استخدام اشخاص در شرایطی خاص مبادرت به پول‌شویی می‌کنند، بدین شرح که اشخاصی را استخدام می‌کنند تا آن‌ها در فضای سایبری اقدام به ایجاد حساب کاربری و رمزارز کنند و کلید خصوصی حساب مربوطه را به صاحب شرکت تحویل دهند.^۴ بنابراین ناشناسی و نامعلوم بودن هویت طرفین در این گونه داد و ستدها اولین زنگ خطر ارتکاب جرایم است. علاوه بر این، رمزارزهای ناشناسی نیز وجود دارند که امکان پیگیری و رصد آن‌ها به هیچ طریقی مقدور نیست.^۵ تراکنش‌های سریع از طریق ارزهای مجازی موجب شده است تا برداشت پول و یا تبدیل آن به سایر وجوه، با سرعت بیشتری نسبت به راه‌های سنتی آن صورت گیرد. سرعت بالای تراکنش‌ها و همچنین ترکیب استفاده از ارزهای مجازی با سایر روش‌های نوین و سنتی پول‌شویی سبب شده است تا نظارت، کشف و تعقیب آن‌ها با دشواری‌هایی روبه‌رو باشد. مجرمان این عرصه با مهارت در این حوزه و اجرای آن، سود حاصل از جرم را به کشورهای

^۱ عباسی، اصغر. حقوق کیفری اقتصادی پول‌شویی مبارزه با پول‌شویی در اسناد بین‌المللی و نظام حقوقی ایران، ۵۰.

^۲ Kibin, Lee, James, Joshua I, Ejeta, Tekachew G, & Kim, Hyoungh, J. "Electronic voting service using block-chain", ۵۰.

^۳ ساورایی، پرویز، و پورمسجدیان، فاطمه. «تبیین ماهیت حقوقی و اختلافات نام دامنه‌های اینترنتی»، ۱۵۰.

^۴ Dyntu, Valeriia. *Cryptocurrency As A Means of Money Laundering*, ۲.

^۵ Lemieux, Louise. "Use of bit coin in dark net markets: examining facilitative factors on bit coin-related crimes".

که قوانین و نظارت کمتری در مورد پول‌شویی اعمال می‌نماید منتقل می‌کنند و در آنجا روند تبدیل رمزارزها را به پول نقد و... پی می‌گیرند.

بند چهارم: تأمین مالی تروریسم

تأمین مالی تروریسم از دیگر چالش‌های کشورها در استفاده از رمزارزها است. اقدامات تروریست‌ها تنها شامل حملات انتحاری و جنگی نمی‌گردد و فعالیت‌های تبلیغی و تهیه کالاهای مورد نیاز آن‌ها نیازمند پشتوانه مالی است. به همین جهت، سرعت زیاد، غیر قابل شناسایی بودن و فقدان نظارت بر رمزارزها سبب شده است تا روش امنی برای آنان باشد و به عنوان طریقه‌ای برای تأمین مالی تروریست‌ها به حساب آید.

بند پنجم: فرار مالیاتی

فرار مالیاتی نیز از دیگر جرایمی است که از طریق رمزارزها قابلیت تحقق دارند. رمزارزها در جهان امروز در حال خروج از حاشیه و مبدل گشتن به جریان اصلی اقتصاد هستند. این امر، هرچند سرمایه‌گذاری بیشتری با خود به همراه دارد، اما نیازمند تأمین امنیت، بازارهای قوی‌تر و توجه بیشتر به سازمان مالیاتی خواهد بود. برقراری و افزایش مالیات بر رمزارزها نمایانگر اقبال آن‌ها است. چنانچه شرایط به صورت حال ثابت گردد، ضروری است که سرمایه‌گذاران رمزارزها در چهارچوب‌های مالیاتی و قوانین آن اقدام نمایند و مالیات بپردازند، اما با وجود نوسان زیاد رمزارزها، پیگیری کلیه داده‌ها و تنظیم مالیات، از دشواری‌های دولت‌هاست. کدهای مالیاتی رمزارزها ضمن اینکه پیچیدگی‌های بسیاری دارند، در کشورهای مختلف متفاوت هستند. هرچند در تراکنش‌های رمزارزهایی نظیر بیت کوین یا اتریوم، هویت دریافت کننده و ارسال کننده ناشناس باقی می‌ماند، اما این امر، غیرقابل ردیابی بودن تراکنش‌های مذکور را تأیید نمی‌کند، زیرا کلیه تراکنش‌ها در بلاک‌چین، به صورت عمومی و برای همیشه قابل دسترسی است و جز در مواردی ویژه، دستیابی به هویت واقعی اشخاص امکان‌پذیر می‌باشد. بنابراین با وجود راه‌های فرار مالیاتی، دولت‌ها باید تدابیری برای فعالان حوزه رمزارزها جهت انجام ایمن معاملات‌شان اتخاذ نمایند تا شرایط را برای معامله و پرداخت مالیات رمزارزها با ریسک کم فراهم کنند.

بخش ششم: چالش‌های دادرسی در جرایم مالی ناشی از رمزارزها

از مهم‌ترین چالش‌های این حوزه باید بر عدم وجود تعریف یکسان قانونی نام برد و خاطرنشان ساخت همچنان بعد از گذشت سال‌ها وضعیت حقوقی رمزارزها با ابهام مواجه است. با وجود تعاریف مختلف صورت گرفته، اما تعریفی که کامل و جامع بوده و قالب قانونی نیز یافته باشد همچنان وجود ندارد. این امر، بالتبع سبب سردرگمی قضات و تشتت آرای قضایی خواهد شد. تعاریف ارائه شده از بخش‌های مختلف جامعه، هر یک به سبب قوانین و دستورالعمل‌های درون‌سازمانی خود ارائه می‌گردند و همین امر موجب می‌شود تا آثار متفاوت قانونی را از خود بر جای گذارند. از سوی دیگر، در مقررات نظام پولی و بانکی ایران، تعریف مشخصی از پول و ارز ارائه گردیده است.^۱ در پیش‌نویس الزامات و ضوابط فعالیت در حوزه رمزارزها، بانک مرکزی جمهوری اسلامی، رمز ارز را یک نوع دارایی مالی که قادر است در شرایطی کارکرد پولی داشته باشد، اعلام می‌نماید. از سوی دیگر، در پیش‌نویس مذکور، به کار بردن این رمزارزها برای پرداخت که مهم‌ترین خصیصه این ارزها می‌باشد را در کشور ممنوع نموده است. شورای عالی مبارزه با پول‌شویی به موجب اعلامیه‌ای (مورخ ۱۳۹۶/۱۰/۹)،^۲ هر گونه به کارگیری ارزهای مجازی توسط مؤسسات مالی و پولی کشور را با ممنوعیت مواجه کرده است. همچنین مطابق با ماده یک تصویب‌نامه مورخ ۱۳۹۸/۵/۱۳^۳ استفاده از رمزارزها صرفاً با قبول مسئولیت خطرپذیری از سوی متعاملین صورت می‌گیرد و مشمول حمایت و ضمانت دولت و نظام بانکی نیست و استفاده از آن در مبادلات داخل کشور مجاز نمی‌باشد. قانون‌گذار ایران با هدف برقراری دادرسی عادلانه و پیشتر از آن، پیشگیری از وقوع این جرایم و تسهیل و تسريع در کشف و تعقیب این جرایم، قوانین و الزامات بسیار ناشی از تعهدات، دستورالعمل‌ها و قوانین گوناگون را برای حفظ سلامت نظام اقتصادی کشور و برقراری امنیت جهت ترغیب به جذب سرمایه‌گذاران داخلی و خارجی در نظر گرفته است. ضروری است اشخاص مرتبط

^۱. برای اطلاعات بیشتر رک: ماده ۱ قانون مبارزه با قاچاق کالا و ارز و بند الف ماده ۴۲ و ماده ۲ قانون پولی و بانکی

کشور و همچنین ماده ۵ آیین‌نامه مستندسازی جریان و جوه در کشور مصوب ۱۳۸۶ هیئت وزیران.

^۲. تارنمای بانک مرکزی ج.ا.ایران؛ پیوند خبر <http://www.cbi.ir/showitem/۱۷۷۲۲>

^۳. تصویب‌نامه شماره ۵۱۴۴/ت: ۵۵۶۹ ه ابلاغی مورخ ۱۳۹۸/۵/۱۳

با رمزارزها، نظیر بانک‌ها، مؤسسات مالی و اعتباری و اشخاص حقیقی و حقوقی ارائه‌کننده خدمات پولی بانکی، مطابق با این مقررات و دستورالعمل‌ها اقدام نمایند. به موجب تبصره ۴ ماده ۳ قانون تنظیم بازار غیرمتشکل پولی مصوب ۱۳۸۳/۱۰/۲۲، تصدی به عملیات بانکی فاقد مجوز حتی می‌تواند ضمانت اجرای کیفری را به همراه داشته باشد. در برخی موارد به موجب ماده ۴۵ دستورالعمل اجرایی تأسیس، فعالیت و نظارت بر صرافی‌ها مصوب ۱۳۸۹/۶/۹ بانک مرکزی، افتتاح حساب و ارائه خدمات به اشخاص حقیقی و حقوقی و مؤسسات پولی و بانکی با ضوابط ویژه‌ای همراه است که در صورت تخطی از آن، جرمه‌های مالی، انتظامی و حتی لغو جواز مؤسسه متخلف را در پی داشته باشد. ماده ۵ قانون مبارزه با پول‌شویی، کلیه صاحبان مشاغل غیرمالی و مؤسسات غیرانتفاعی و همچنین اشخاص حقیقی و حقوقی را موظف می‌سازد تا هویت ارباب رجوع، صاحبان حساب‌ها، معاملات داخلی و خارجی را محفوظ بدارند؛ معاملات یا عملیات مشکوک بانکی، ثبتی، سرمایه‌گذاری، صرافی، کارگزاری و مانند آن‌ها را گزارش کنند و در نگهداری سوابق علی‌رغم قوانین و مقررات مذکور و بسیاری از قوانین مشابه دیگر، در ارزش‌های مجازی به دلیل فقدان اهتمام ورزد. با وجود تمامی قوانین و دستورالعمل‌های موجود و به سبب فقدان نهاد مرکزی ناظر، اجرای موارد فوق‌الذکر در عمل با شکست مواجه گردیده است، زیرا اشخاص نیازی به مراجعه حضوری به بانک و یا مؤسسه مالی و ثبت اطلاعات و مشخصات هویتی خود ندارند و قادرند در هر زمان و مکانی نسبت به ایجاد حساب کاربری اقدام کنند و هیچ تکلیفی برای احراز هویت و بررسی صلاحیت و صحت اطلاعات کاربران وجود ندارد. همچنین با توجه به خصیصه ذاتی رمزارزها که مبتنی بر علم ریاضی و الگوریتم‌ها می‌باشد، احراز هویت اشخاص، فاقد موضوعیت است. علاوه بر این، همان‌طور که پیشتر بیان گردید، دولت‌ها قادر به نظارت و ایجاد محدودیت‌های مورد نظر خود همچون بررسی صلاحیت اشخاص، کنترل وجوه جهت انتقال یا واریز و برداشت، کشور مبداء و یا مقصد، توقیف و مسدود نمودن حساب اشخاص، سوابق تراکنش‌ها^۱ و بررسی صحت

معاملات مشکوک نیستند^۱. دادرسی جرایم مرتبط با رمزارزها، در اولین مرحله با کشف و تعقیب جرایم مرتبط با رمزارزها آغاز می‌گردد که همچون سایر جرایم، توسط ضابطان دادگستری و تحت نظارت و تعلیمات مقام قضایی انجام می‌شود. اصول دادرسی منصفانه در این جرایم نیز همچون سایر جرایم، مبتنی بر قانونی بودن، سرعت و صحت عملکرد ضابطان است. ماهیت مجازی رمزارزها، از عدم وجود ملموس و فیزیکی در خارج از فضای مجازی حکایت دارد. علاوه بر این، جرایم این حوزه، از جمله جرایم نوپیدا تلقی می‌گردند و نیازمند تخصص و علم مربوط به آن هستند که در برخورد با این امر، ضابطان دادگستری نسبت به اصول فنی و عملکرد آن‌ها فاقد اطلاعات و آگاهی لازم هستند که همین امر، رسیدگی به آن را با دشواری روبه‌رو می‌سازد.

روند دادرسی با چالش‌های دیگری نیز مواجه است که از آن جمله می‌توان به فقدان رابطهٔ چهره به چهره در به‌کارگیری ارزشهای مجازی نام برد. در پاره‌ای از جدیدترین روش‌های پرداخت، کاربران با بهره‌گیری از ارزشهای مجازی و روش‌های نوین، به صورت کاملاً گمنام و غیر قابل ردیابی عمل می‌کنند و این امر، شناسایی، ردیابی و تعقیب متهم متخصص در این فناوری را برای ضابطان ناآگاه، دشوار می‌نماید.

مطابق تبصرهٔ ۲ مادهٔ ۳ قانون مبارزه با پول‌شویی و همچنین مادهٔ ۹ همین قانون، هنگامی که رمزارزها وسیله یا موضوع جرم واقع شوند، لازم است که بر اساس قوانین مذکور، توقیف یا مصادره گردند. این قانون، ضابطان دادگستری و مراجع قضایی را مکلف می‌سازد تا اقدامات لازم را در خصوص شناسایی، کشف و مسدود کردن وجوه استفاده شده یا تخصیص داده شده برای تأمین مالی تروریسم، عواید به‌دست آمده از آن‌ها، شناسایی و توقیف اموال موضوع جرایم مذکور در این قانون و عواید آن‌ها که به طور کامل یا جزئی به اموال دیگری تبدیل شده و تغییر وضعیت یافته‌اند و توقیف اموال و عواید موضوع جرم که با اموال قانونی امتزاج یافته است به نحوی که اموال مزبور به اندازهٔ تخمین زده شده قابل توقیف باشد، انجام دهند. در تبصرهٔ این ماده آمده است که اشخاص موضوع این ماده، موظف‌اند حسب دستور مقام

^۱. رک: بند ۱۹ مادهٔ یک آیین‌نامهٔ اجرایی قانون مبارزه با پول‌شویی، و تبصرهٔ مادهٔ ۷ قانون مبارزه با پول‌شویی و بند ۵ تبصرهٔ این ماده.

قضایی، نسبت به مسدود کردن وجوه و توقیف اموال و دارایی‌های افراد و سازمان‌های ترویرستی و همچنین افراد موضوع قانون مبارزه با پول‌شویی اقدام کنند. تشخیص اینکه رمزارزها در جرایمی نظیر پول‌شویی و تأمین مالی تروریسم به چه عنوانی باید توقیف شوند دشوار به نظر می‌رسد، چرا که روشن نیست در کشف و تعقیب این جرایم، رمزارزها، تحت عنوان وسیله ارتکاب جرم توقیف می‌گردند یا عواید حاصل از جرم. از سوی دیگر به سبب عدم وجود نهاد متمرکز، مسئول قوای حاکمه بر کشور، توان انسداد یا ممانعت از نقل و انتقال رمزارزها را ندارد و برعکس، شبکه‌های متمرکز که امکان توقیف آن‌ها به وسیله ایجاد تکلیف بر نهاد مرکزی مدیریت کننده وجود دارد در رمزارزها این امر امکان‌پذیر نیست. این چالش‌ها معطوف به موارد گفته شده نیست و در نگهداری آن‌ها نیز دشواری‌هایی وجود دارد، زیرا نگهداری رمزارزها مشکلاتی را برای ضابطان دادگستری به همراه دارد. در صورت توقیف رمزارزها توسط ضابطان باید رمزارزها به کیف پول دیجیتال دادگستری یا پلیس منتقل و در آن ذخیره گردد، اما مشکل اصلی، روش‌های فنی حفاظت از آن است تا از سرقت و دخل و تصرف حفاظت گردد. با وجود گستردگی ارزش‌های مجازی، پیش از هر چیز باید ضابط متخصص در این عرصه معین گردد و پس از آن، امن‌ترین و بهترین کیف پول توسط متخصصین این حوزه انتخاب شود.^۱ دستیابی به ادله قانونی در فضای مجازی در خصوص رمزارزها نیز از دیگر مواردی می‌باشد که فرآیند دادرسی را با دشواری روبه‌رو می‌سازد، زیرا ردیابی رمزارزها و توانایی کشف ادله، تنها توسط متخصصین امکان‌پذیر است و آنگاه که متهم، ابزارهای خاص گمنام‌سازی را به کار برده باشد، فرآیند کشف و شناسایی رمزارزها جهت مستندسازی بسیار دشوار می‌گردد. با وجود اینکه تراکنش‌های ثبت شده در زنجیره بلوک، غیر قابل تغییر می‌باشند و می‌توان به آن‌ها استناد نمود، اما با توجه به نامشخص بودن کاربر و تراکنش‌های وی، نحوه اثبات و انتساب این تراکنش‌ها به شخصی معین است که چالش ایجاد می‌کند. سرعت و تخصص ضابط دادگستری در دستیابی به ادله الکترونیک از اهمیت زیادی برخوردار است، زیرا این ادله به دلیل به‌روزرسانی و یا حذف داده‌های قبلی و تثبیت اطلاعات جدید در معرض تغییر هستند و امکان از بین رفتن آن‌ها در مدت زمانی کوتاه

۱. ماده ۳۶ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی. | ۳۱۲

وجود دارد. بنابراین آن گاه که مجرم، متخصص باشد، با بهره گیری از نرم افزارهایی این داده‌ها را محدود به زمان‌های از پیش تعیین شده می‌کند و پس از آن با حذف آن‌ها، دسترسی به ادله جرم، غیرممکن می‌گردد و در نهایت به سبب فقدان دلیل یا عدم کفایت آن، دادرسی خاتمه خواهد یافت. اما با وجود تمام موارد گفته شده، سؤالی که مطرح می‌گردد این است که قلمروی صالح قضایی برای رسیدگی به جرایم مالی مربوط به رمزارزها کجاست؟

رمزارزها اختصاص به قلمروی مشخصی نداشته و از جمله مواردی است که محل وقوع جرم مشخص نیست. به موجب ماده ۱۱۸ قانون آیین دادرسی کیفری، آن گاه که آثار و ادله وقوع جرم در حوزه قضایی محل مأموریت بازپرس کشف شود، اما محل وقوع آن معلوم نباشد، بازپرس ضمن انجام تحقیقات، سعی در کشف محل وقوع جرم می‌نماید و اگر محل وقوع جرم تا ختم تحقیقات مشخص نشود، بازپرس در خصوص موضوع، اظهار عقیده خواهد کرد. این ماده، بر رمزارزها که فاقد محدوده جغرافیایی مشخصی هستند، دلالت نموده و چنانچه تعیین قلمروی جغرافیایی به هر نحوی ممکن باشد، نظیر اینکه محل نگهداری کیف پول مجازی، مشخص گردد، همان محل به عنوان محل وقوع جرم شناخته می‌شود و مطابق با آن، رسیدگی خواهد شد، زیرا رمزارزها از طریق کیف پول مدیریت می‌گردند.

نتیجه گیری

رمزارز، مفهومی می‌باشد که در زندگی مردم جهان راه یافته و ایران نیز از این امر مستثنی نگردیده است. رمزارزها با وجود ویژگی‌های مثبتی نظیر دور زدن تحریم‌ها و جانشینی ارزهای بین‌المللی در مبادلات برای مصون ماندن از تحریم‌ها علیه ایران، بستر ارتکاب جرایم مالی بسیاری را نیز فراهم آورده است. به کارگیری رمزارزها، امکان ارتکاب جرایمی نظیر پولشویی، سرقت و کلاهبرداری را افزایش می‌دهد، زیرا عدم امکان شناسایی و کشف هویت طرفین و ناآگاهی عموم مردم از نحوه کارکرد این فناوری، موجبات تسریع و تسهیل ارتکاب این قبیل جرایم را فراهم می‌سازد و در نتیجه، رجوع مال‌باخته به سیستم قضایی کشور، امری اجتناب‌ناپذیر است. همین ویژگی‌ها روند دادرسی عادلانه را با چالش‌هایی مواجه می‌نماید. وضع مقررات در حوزه رمزارزها با توجه به ویژگی‌های فناوری آن‌ها به تدریج در حال تکامل است؛ هرچند هنوز در ابتدای این امر قرار دارد و قوانین مختص به آن نیز وجود ندارد.

افزایش استفاده از رمزارزها در ایران، ضرورت کنشگری حقوقی در خصوص جنبه‌های مختلف این پدیده را نمایان می‌سازد، اما شناسایی رمزارزها بیش از هر چیز دارای اولویت است، زیرا دستیابی به شناخت دقیق در ماهیت حقوقی آن سبب می‌گردد تا مقررات کارآمد و کاربردی تدوین شود. رمزارزها گونه‌ای از اموال غیرفیزیکی و ناملموس هستند که در میان مردم، دارای ارزش مبادله‌ای بوده، بنابراین در مال بودن آن تردیدی روا نیست. خصوصیات گمنامی و غیرمتمرکز بودن رمزارزها در رسیدگی به دعاوی ناشی از آن، دشواری‌های بسیاری ایجاد نموده است. به طور مثال، آن گاه که رمزارزها، موضوع جرم کلاهبرداری واقع می‌گردند، بر اساس قوانین موجود، بزهدکار بر رد مال و پرداخت جزای نقدی معادل مال برده شده محکوم می‌گردد، حال آنکه برای تعیین مال برده شده، نهادی قانونی وجود ندارد و بازگرداندن آن‌ها نیز در عمل امکان‌پذیر نیست. کشف و تعقیب جرایم این حوزه به سبب نبود نهاد مسئول، عدم تمرکز در رمزارزها، تخصص بالای مرتکبان این قبیل جرایم، اهمیت سرعت ضابطان قضایی در بررسی داده‌ها، دادرسان این قبیل جرایم را با چالش‌هایی مواجه نموده است. به عنوان نتایج حاصل از این پژوهش، پیشنهادات زیر به منظور رفع چالش‌های دادرسی عادلانه در رسیدگی به جرایم مالی مرتبط با رمزارزها ارائه می‌گردد:

- ✓ شناخت ماهیت رمزارزها و ارائه تعریف قانونی از آن؛
- ✓ رفع ابهام از وضعیت حقوقی رمزارزها؛
- ✓ رسمیت‌بخشی به رمزارزها و نهادهای مسئول در خصوص وضع سیاست‌های مقرر شده توسط نهاد قانون‌گذاری؛
- ✓ تدوین قوانین اختصاصی صرافی‌های ارزهای مجازی و ارائه دهندگان خدمات اینترنتی با هدف اعمال نظارت و حاکمیت قانون بر معاملات و وضع مالیات بر آن؛
- ✓ وضع قوانین به‌روز در خصوص مقابله با پول‌شویی و تأمین مالی تروریسم در این قبیل ارزها با همکاری نهادهای گوناگونی نظیر بانک مرکزی، پلیس فتا، نهاد دادگستری و...

- ✓ وضع قوانین و آیین‌نامه‌های مربوط به نحوه کشف، دادرسی، حقوق متهم و زیان‌دیده در برخورد با جرایم مرتبط با رمزارزها در نظام قضایی ایران؛
- ✓ اتخاذ تمهیدات متناسب جهت توقیف، انتقال و نگهداری رمزارزها به عنوان وسیله ارتکاب جرم یا عواید حاصله از جرم و برگزاری دوره‌های آموزشی لازم برای ضابطان دادگستری، قضات و سازمان‌هایی که به هر نحو، موظف به اجرای قوانین می‌باشند؛
- ✓ به کارگیری متخصصین در حوزه ارزهای مجازی با هدف حفاظت از داده‌ها؛
- ✓ انتقال صحیح آن‌ها و بررسی رایانه‌های مکشوفه از متهمان به جهت حفظ سرعت و دقت لازمه این جرایم.

منابع و مآخذ

الف) منابع فارسی

۱. خلیلی پاجی، عارف. امکان‌سنجی تأمین مالی تروریسم در پرتو ارزشهای مجازی. مجموعه مقالات همایش بین‌المللی ابعاد حقوقی - جرم‌شناختی تروریسم، تهران، دانشگاهی علامه طباطبائی، ۱۳۹۸.
۲. ساورایی، پرویز، پورمسجدیان، فاطمه. «تبیین ماهیت حقوقی و اختلافات نام دامنه‌های اینترنتی». دانشنامه حقوق و سیاست ۱۰(۱۳۹۳): ۱۴۹-۱۸۴.
۳. شاملو، باقر، خلیلی پاجی، عارف. «چالش‌های حقوقی اقتصادی ارزشهای مجازی برای نظام‌های سیاسی در پرتو نظریه جایگزینی». فصلنامه رهیافت‌های سیاسی و بین‌المللی ۱۲(۱۳۹۹): ۱۲۵-۱۵۲.
۴. فرقان‌دوست حقیقی و کامبیز، نداف، رضوانه. «مروری بر رمزارزها، فرصت‌ها و تهدیدها». مجله علمی تخصصی رویکردهای پژوهشی نوین در مدیریت و حسابداری، ۱(۱۳۹۷): ۶۱-۷۴.
۵. نواب‌پور، علیرضا، یوسفی، احمدعلی طالبی، محمد. «تحلیل فقهی کارکردهای پول‌های رمزنگاری شده، مطالعه موردی بیت کوین». فصلنامه اقتصاد اسلامی، ۱۸(۱۳۹۷): ۲۱۳-۲۴۳.
۶. نوری، مهدی و نواب‌پور، علیرضا. «طراحی چارچوب مفهومی سیاست‌گذاری ارزشهای مجازی در اقتصاد ایران». فصلنامه سیاست‌گذاری عمومی دانشگاه تهران، ۳(۱۳۹۷): ۵۱-۷۸.

ب) منابع لاتین

۷. Dibrova, Alina. ۲۰۱۶. "Virtual currency: New step in monetary development. " *Procedia - Social and Behavioral Sciences* ۲۲۹(۲۰۱۶): ۴۲-۴۹.

۸. Dong, He, Karl, Habermeier, Ross, Leckow, Vikram, Kyriakos-Saad, Hiroko, Oura, Tahsin Saadi Sedik, Natalia, Stetsenko. *Concepcion Verdugo-Yepes, Virtual Currencies and Beyond: Initial Considerations, Initial Considerations, IMF Discussion Note SDN/ ۱۶/۰۳. European Central Bank, Virtual Currency Schemes*, ۲۰۱۶.
۹. Dyntu, Valeriia. *Cryptocurrency as a means of money laundering*. Odessa Law Academy Press (۲۰۱۸).
۱۰. European Central Bank, *Virtual Currency Schemes*, available at :<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes> ۲۰۱۲۱۰en Oct. ۲۰۱۲.
۱۱. Financial Action Task Force. *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, ۲۰۱۴, available at: www.fatf-gafi.org.
۱۲. Financial Crimes Enforcement Network guidance. available at: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.
۱۳. <https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined>
۱۴. Ivantsov, Sergey; Sidorenko, Elina; Spasennikov, Boris; Berezkin, Yuri & Sukhodolov, Yakov. "Cryptocurrency-related crimes: key criminological trends". *Russian Journal of Criminology* ۱۲(۲۰۱۹): ۸۵-۹۳.
۱۵. Kibin, Lee, James, Joshua I, Ejeta, Tekachew G, & Kim, Hyoung, J. "Electronic voting service using block-chain". *Journal of Digital Forensics, Security and Law*, ۱۱(۲۰۱۸): ۸.
۱۶. Korennaya, Anna, & Tydykova, Nadezhda. "Cryptocurrency as an object and instrument of committing crime". *Russian Journal of Criminology*, ۱۲(۲۰۱۹): ۴۰۸-۴۱۵.

۱۷. Lemieux, Louise. "Trusting Records: Is Block chain Technology the Answer? Records Management Journal, ۲۶(۲۰۱۶).
۱۸. Sesha, Kethineni, Ying, Cao, Cassandra, & Dodge. "Use of bit coin in dark net markets: examining facilitative factors on bit coin-related crimes". Southern Criminal Justice Association, ۴۳(۲۰۱۷): ۱۴۱-۱۵۷.
۱۹. UNODC. Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies, ۲۰۱۴
۲۰. Wagner, Andrew. Digital vs. Virtual Currencies. <https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-۱۴۰۸۷۳۵۵۰۷>, ۲۰۱۴.
۲۱. Wikipedia: Digital currency (digital money, electronic money or electronic currency) is a type of currency available in digital form (in contrast to physical, such as banknotes and coins)