مجله حقوقی دادگستری

مقاله پژوهشی/ دوره ۸۹/ شماره ۱۳۰/ صفحات: ۲۲۰-۱۹۳
تاریخ دریافت: ۱۴۰۳/۰۸/۰۵ تاریخ پذیرش: ۱۴۰۳/۱۲/۱۴

چالش‌های نظام عدالت کیفری ایران در مواجهه با رمزارزها و راهکارها

نرگس فرزانه کندری[۱]، محمدمتین ارجمندفر[۲]، امین تویسرکانی[۳]

چکیده

تحول فناوری‌های نوین مالی و گسترش به‌کارگیری رمزارزها، چالش‌هایی را برای نظام‌های حقوقی و به ویژه دستگاه عدالت کیفری ایجاد نموده و اغلب نظام‌های حقوقی به جای مقابله مطلق و نفی رمزارزها، به رویکرد مقررات‌گذاری و تنظیم فعالیت‌های مرتبط با آن‌ها در دو طیف تجویز حداکثری و حداقلی متمایل شده‌اند. پرسش محوری این مقاله آن است که رمزارزها چه چالش‌هایی را در عرصه‌های ماهوی، شکلی و اجرایی برای نظام عدالت کیفری به‌وجود آورده‌اند و راهکارهای رفع چالش‌ها در چارچوب قوانین موجود چیست.

این تحقیق که با رویکرد توصیفی تحلیلی و بهره‌گیری از منابع کتابخانه‌ای و مصاحبه نیمه‌ساختاریافته با برخی قضات و بازپرسان فعال در حوزه جرائم رایانه‌ای انجام شده است، مهم‌ترین چالش‌های نظام عدالت کیفری در مواجهه با این جرائم را شامل: ابهام در رسمیت و مالیت رمزارزها و اعتبار حقوقی آن‌ها، نبود قوانین و مقررات نظارتی و پیشگیرانه شفاف، مشکلات دادرسی در جرائم مرتبط با رمزارزها به واسطه پیچیدگی‌های ناشی از تمرکززدایی و ناشناس بودن فناوری بلاک‌چین، چالش‌های مرتبط با توقیف و اجرای احکام و نارسایی‌های فنی، فرهنگی و آموزشی در حیطه پیشگیری و رسیدگی به دعاوی مرتبط با این حوزه، شناسایی کرده و برای رفع این چالش‌ها، لزوم تدوین مقررات جامع و متناسب برای رسیدگی، تجهیز ضابطان قضایی و دادگستری ها به زیرساخت‌های فنی مناسب و آموزش تخصصی قضات و کارشناسان این حوزه را در کنار آگاهی افزایی عمومی نسبت به مخاطرات رمزارزها، پیشنهاد می‌دهد.

واژگان کلیدی: رمزارز، نظام عدالت کیفری، بلاک‌چین، جرائم مرتبط با رمزارزها

---

۱. عضو هیأت علمی پژوهشکده قوه قضائیه (نویسنده مسئول)
n.farzaneh@jri.ac.ir

۲. کارشناسی ارشد حقوق مالکیت فکری دانشگاه علامه طباطبائی
matinarjmand3@gmail.com

۳. دکتری حقوق جزا و جرم شناسی و بازپرس دادسرای جرایم رایانه‌ای
a_tuysserkani@yahoo.com

درآمد

امروزه فناوری‌های جدید و پیشـــرفته از جمله علم رمزنگاری باعث تغییراتی در ساختار اقتصادی جهان و روابط تجاری شده‌اند که از مهم‌ترین آن‌ها، پدیده جدید ارزهای مجازی یا رمزارزها است. رمزارز یا ارز مجازی سیستمی خصوصی است که جهت ســـهولت انجام مبادلات بین افراد بدون حضور واسطه و نهاد مرکزی، استفاده می‌شود. در واقع رمزارز پولی است که در فضای مجازی و بدون مقام ناظر و پشتوانه قانونی مانند پول فیات[1] ایجاد شده است. اصطلاحاتی مانند ارز دیجیتال، ارز مجازی، رمزارز، ارز رمز پایه، رمزینه ارز، ارز رمزنگاری شـــده و غیره در زبان فارســـی به‌کار می‌روند که اغلب به اصطلاح کریپتوکارنســـی[2] در زبان انگلیسی ارجاع داده می‌شوند و به معنای پول یا ارزی اســـت که بر پایه علوم رمزنگاری ایجاد شـــده و می‌تواند با اســـتفاده از علم ریاضیات، کدهای رمزنگاری شـــده را ایجاد نماید تا اطلاعات پنهان بماند و کســـی قادر نباشد در روند تولید، انتشـــار و انجام مبادلات خللی وارد آورد (خادمان و دیگران، ۱۴۰۰: ۳۵۱).

ارزهای دیجیتـــال بدون نیاز به بانک مرکزی برای صـــدور ارز و یا بآن‌کهای خصوصی برای ذخیره ارز عمل می‌کنند. آن‌ها بر اساس یک قطعه و زنجیره کد شکل می‌گیرند که قابل تکرار نیســـتند. به عنوان جایگزینی برای ارزهای سنتی، ارزش این ارزها، مبتنی بر تعداد کاربرانی است که آماده پذیرش پرداخت برای کالاها و خدمات با اســـتفاده از ارز دیجیتال هستند. ارزش آن‌ها هم‌چنین از تمایل مبادلات ارز دیجیتال برای تبدیل آن‌ها به ارزهای دیگر ناشـــی می‌شود. در حال حاضر بیش از هزاران نوع ارز دیجیتال مانند بیت‌کوین[3]، دش[4]، اتریوم[5]، ریپل[6] و زی‌کش[7] وجود دارد (Latimer

---

۱. ارز فیات هیچ ارزش فیزیکی ندارد و یک تکه کاغذ یا سکه است. این ارزها که همان اسکناس‌ها و سکه‌های رایج امروزی هستند؛ در سراسر جهان برای مبادلات اقتصادی و تجاری، خرید و فروش کالا و ســـرمایه‌گذاری استفاده می‌شوند. این ارز جایگزینی برای استاندارد طلا و پول کالایی (کالایی اقتصادی که به‌جای پول استفاده می‌شود) بوده است.

2. Crypto Currency
3. Bitcoin
4. Dash
5. Ethereum
6. Ripple
7. Zcash

& Duffy, 2019: 122). برخی معتقدنـــد باید میان اصطلاحات «ارز دیجیتال»، «ارز مجازی» و «رمزارز» تفاوت قائل شـــد. ارزهای دیجیتال ارزهایی را شامل می‌شوند که به صورت الکترونیکی ذخیره و منتقل می‌شـــوند و هرگونه پولی که بر مبنای صفر و یک باشـــد در این تعریف می‌گنجد؛ اعم از این‌که مبنای آن پول ســـنتی و بانکی و یا ارزهای مجازی باشـــد. در واقع ارز دیجیتال به هر ارزش ایجاد شده در بستر دیجیتال اطلاق می‌گـــردد. ارز مجازی از این جهت که غیرملموس اســـت نوعی ارز دیجیتال محسوب می‌شـــود و وجه تمایز آن این است که پول دیجیتال، نماینده اسکناس‌های بانکی اســـت که فقط ســـازِکار آن غیر فیزیکی شده اســـت؛ در حالی‌که ارز مجازی ارتباطی با پول بانکی ندارد و یک ارز جدید با ســـازِکار منحصربه‌فرد است (نوری و نواب‌پـــور، ۱۳۹۷: ٤) و در نهایت رمزارز (یا ارز رمـــز پایه) را گونه‌ای پول دیجیتال معرفـــی نموده‌اند که در آن تولید واحد پول و تأیید اصالت تراکنش پول با بهره‌گیری از الگوریتم‌های رمزگذاری شده کنترل می‌شود (Chohan, 2022: 2).

ارزهـــای غیرقابل تبدیل هرگز امکان تبدیـــل به پول‌های بانکی را ندارند نظیر پول‌هایی که در بازی‌های رایانه‌ای کسب می‌شود. این ارزها به صورت متمرکز هستند و یک نهاد مرکزی برای مثال ســـازنده بازی آن را منتشر نموده است و دفترکل را نزد خود نگاه می‌دارد. لیکن ارزهای مجازیِ قابل تبدیل، امکان تبدیل به پول‌های حقیقی و به‌عکـــس را دارنـــد و از آن برای خرید کالا و خدمـــات حقیقی و مجازی می‌توان استفاده نمود. این نوع ارز به دو دسته متمرکز و غیر متمرکز تقسیم می‌شود؛ در دسته متمرکز، انتشـــار و کنترل ارز توســـط یک نهاد مرکزی صـــورت می‌پذیرد؛ اما در ارز مجازی غیرمتمرکز تمامی فرایندها از جمله انتشـــار و تأیید تراکنش‌ها به جای این‌که توســـط نهادی مرکزی صورت گیرد به وسیله تمامی افراد با سازوکارهای رمزنگاری انجـــام می‌گیرد (نوری و نواب‌پـــور، ۱۳۹۷: ٦-٥). در تعریف رمزارز می‌توان گفت، نوعی پول دیجیتال و ارز مجازی به حساب می‌آید که با شیوه‌های فناوری رمزنگاری (الگوریتم‌های رمزگذاری) و اغلب به صورت غیرمتمرکز (بدون وابستگی به یک نهاد مرکزی) ایجاد و اداره می‌شود.

با امعان نظر به چالش‌ها و مشـــکلاتی که رمزارزها به واسطه ویژگی‌های خود در نظام‌های حقوقی و قضایی ایجاد کرده‌اند، در تحقیق حاضر بر آن شدیم که ضمن

شناسایی این چالش‌ها در نظام عدالت کیفری ایران با تأکید بر نظریات متخصصان قضایی که به نوعی درگیر پرونده‌های مرتبط با رمزارزها هستند، ضمن ارائه تصویری از واقعیت موجود، پیشنهادهایی متناظر با چالش‌های فعلی ارائه نماییم.

این تحقیق با استفاده از روش توصیفی تحلیلی و به‌کارگیری منابع کتابخانه‌ای و هم‌چنین استفاده از ابزار مصاحبه با شش متخصص این حوزه از مقامات قضایی و بازپرسان دادسرای جرائم رایانه‌ای انجام شد، اما به لحاظ محدود بودن شمار متخصصان این حوزه در نظام قضایی ایران که مصاحبه با تعداد بیشتری از قضات را غیر ممکن می‌ساخت، تحقیق پیش‌رو را باید یک تحقیق نظری دانست که در عین حال، استفاده از روش مصاحبه و تحلیل چالش‌های عملی و ارائه پیشنهادهایی در این زمینه آن را واجد وصف کاربردی نیز نموده است.

پرسش اصلی تحقیق حاضر این است که جرائم مرتبط با رمزارزها چه چالش‌هایی را در عرصه‌های ماهوی و شکلی برای نظام عدالت کیفری ایجاد نموده است و راهکارهای رفع چالش‌های موجود در رسیدگی به جرائم مرتبط با رمزارزها که در چارچوب نظام عدالت کیفری کنونی قابل ارائه است، چیست. در جهت پاسخ به این پرسش، ابتدا واکنش نظام حقوقی کنونی در مواجهه با رمزارزها را تبیین می‌نماییم؛ سپس شیوه‌های ارتکاب جرم و هم‌چنین اهم دعاوی کیفری مرتبط با رمزارزها را بررسی می‌کنیم. پس از آن ضمن نگاهی به رویه قضایی، مشکلات شکلی رسیدگی به دعاوی مرتبط با رمزارزها در چارچوب نظام عدالت کیفری ایران را مطمح نظر قرار خواهیم داد. در انتهای مقاله نیز با تکیه بر یافته‌های حاصل از مصاحبه با کارشناسان و مطالعات نظری به ارائه نتایج تحقیق و پیشنهاداتی در خصوص موضوع مبادرت خواهیم نمود.

۱. موضع تقنینی و اجرایی نظام حقوقی ایران در قبال رمزارزها با نگاهی به رویکرد سایر کشورها

تاکنون قانون خاصی در مورد رمزارزها در ایران تصویب نشده است. مصوبه شورای عالی فضای مجازی، طراحی نظام «رمزارز» اعم از رمزارز ملی و ساماندهی کاربری رمزارزهای جهان‌روا را به وزارت امور اقتصادی و دارایی واگذار کرده

است[۱]. علاوه بر بانک مرکزی که همکار وزارت اقتصاد در این امر است، قوه قضاییه، وزارت صنعت، معدن و تجارت، وزارت نیرو، وزارت اطلاعات، فرماندهی انتظامی جمهوری اسلامی و سازمان اطلاعات سپاه نیز از دیگر سازمان‌های همکار برای پیشبرد برنامه‌های رمزارز در کشور می‌باشند.

به رغم این‌که قانون خاصی در حوزه رمزارزها مصوب نشده لیکن در سال‌های اخیر مصوباتی از مراجع دولتی پیرامون رمزارزها صادر شده است. هیأت وزیران در تصویب‌نامه شماره ٥٨١٤٤/ت ٥٥٦٣٧ هـ مورخ ۱۳۹۸/۵/۱۳، آیین‌نامه فرایند ماینینگ ارزهای دیجیتال را تصویب و معاون اول رئیس‌جمهور آن را ابلاغ نمود که بر اساس بند یک آن رمزارزها (فراورده‌های پردازشی رمزنگاری شده) صرفاً با قبول مسؤولیت خطرپذیری آن از سوی طرفین، معامله می‌شود و مشمول حمایت و ضمانت دولت و نظام بانکی نبوده و استفاده از آن در مبادلات داخل کشور مجاز نیست. سازمان ملی استاندارد ایران موظف شده است با همکاری وزارت‌خانه‌های نیرو، ارتباطات و فناوری اطلاعات، برچسب انرژی و استانداردهای کیفیت توان الکترونیکی و استانداردهای فناورانه مربوط به تولید و واردات تجهیزات پردازش رمزارزها (ماینینگ) را تدوین و ابلاغ نماید. شایان ذکر است که در سال ١٤٠١ هیأت وزیران آیین‌نامه استخراج رمزدارایی‌ها[۲] را تصویب نمود و بر اساس ماده ۱۲ آن، آیین‌نامه فوق را لغو نمود. آیین‌نامه اخیر شرایط و ضوابط اخذ مجوز و استفاده از برق، گاز و سوخت مایع و دیگر مسائل راجع به استخراج رمزارزها را مورد توجه قرار داده است. نکته مهم در این آیین نامه آن است که بند یک مصوبه سال ۱۳۹۸ را پابرجا نهاده است، لذا در حال حاضر با توجه به مقررات جاری کشور استفاده از رمزارزها صرفاً با قبول مسؤولیت ریسک آن از سوی متعاملین خواهد بود و مشمول حمایت و ضمانت دولت و نظام بانکی نبوده و استفاده از آن در مبادلات داخل کشور غیرمجاز اعلام شده و لذا از نظر دولت استفاده از رمزارزها در مبادلات داخلی

---

۱. سند راهبردی جمهوری اسلامی ایران در فضای مجازی مصوب هشتاد و چهارمین جلسه مورخ ١٤٠١/٥/١١ شورای عالی فضای مجازی؛ شایان ذکر است با استناد به سند مذکور اخیرا نظام‌نامه رمزارز اعم از ایجاد رمزارز ملی و ساماندهی کاربری رمزارزهای جهان‌روا در یکصد و پنجاه و هفتمین جلسه مورخ ١٤٠٣/١٠/١٩ کمیسیون عالی تنظیم مقررات فضای مجازی کشور به تصویب رسیده است.

۲. آیین‌نامه استخراج رمزدارایی‌ها شماره ١٥١٤٥٥ مورخ ١٤٠١/٨/٢٢ هیأت وزیران.

به رسمیت شناخته نشده است. به هر حال غیرمجاز دانستن استفاده از رمزارزها (مزید بر ابهامات قانونی در خصوص ماهیت و شـــرایط استفاده از آن‌ها) در مبادلات داخل کشور تبعات و چالش‌هایی را در پی داشته است از جمله این‌که چون معامله ارزهای دیجیتال بر اســـاس مقررات بانک مرکزی و تصویب‌نامه شـــماره ٥٨١٤٤/ت ٥٥٦٣٧ هـ مورخ ١٣٩٨/٥/٦ هیأت وزیران در مبادلات داخلی رســـمیت ندارد، لذا توقیف و فروش آن به وســـیله اجرای احکام ممکن دانسته نشده است و در حکم مالی دانسته می‌شـــود که به آن دسترسی نیســـت و با توجه به ملاک ماده ٤٦ قانون اجرای احکام مدنی مصوب ١٣٥٦، قیمت آن به تراضی طرفین و در صورت عدم تراضی، بهای آن به قیمت یوم‌الادا به وســـیله کارشـــناس و خبره محاسبه و از محکوم‌علیه وصول و به محکوم‌له پرداخت می‌شود.

شاید اولین و مهم‌ترین چالش برای نظام‌های حقوقی کنونی مواجهه با پذیرش رمزارز به عنوان یک مال یا ابزار مالی باشـــد زیرا واکنش انفعالی در قبال این چالش، منشـــأ مشکلات بعدی خواهد بود. اگرچه برخی چالش‌های پیرامون ارزهای دیجیتال از کشـــوری به کشور دیگر متفاوت است، اما برخی موضوعات مشترک وجود دارند. تأثیر ارزهای دیجیتال بر قوانین مبارزه با پول‌شویی[1] و جرائم مالی، دغدغه‌های ناشی از احراز هویت مشتری[2] و قوانین اوراق بهادار در اکثر کشورها حائز اهمیت است؛ با این‌حال، هر کشـــوری با توجه به سیاست‌ها و مصالح خود به شیوه‌ای متفاوت با این چالش‌ها مواجه می‌شـــود (Hays & Kirilenko, 2021: 107). آمریکا حدود سه دهه اســـت که در خصوص مقررات‌گذاری رمزارزها بـــه آزمون و خطا پرداخت و تجربه حائز توجهی در این حوزه گرد آورده است (Ibid). می‌توان گفت این کشور پیشگام قانون‌گذاری و تدوین مقررات در حوزه رمزارزها به حســـاب می‌آید. تفاوت‌هایی در بحث صدور مجوزها، نظارت و کنترل رمزارزها در ایالات مختلف این کشـــور وجود دارد (محســـنی‌طیب، ١٣٩٩: ٩٩). رمزارز در این کشور به عنوان یک دارایی و مشابه یک کالا با ارزش مالی پذیرفته شـــده است. ارزهای دیجیتال مانند بیت‌کوین مشمول قوانین اخذ مالیات می‌شـــود و دارندگان آن‌ها در اقســـام مختلـــف، ملزم به پرداخت

1. Anti-Money Laundering (AML)
2. Know Your Customer (KYC)

مالیات می‌باشند. بر اساس الزامات قوانین فدرال برای مؤسسات مالی، به مسائلی نظیر نگهداری از سوابق تراکنش‌ها، گزارش تراکنش‌ها و ارزیابی ریسک مشتریان، با هدف ممانعت استفاده از رمزارزها برای پول‌شویی و فرار مالیاتی توجه شده است (اسکات و موست و وندرروز و لارنت‌چتین و مک‌دوئل، ۱۳۹۵: ۱۲۳).

از فرانسه به عنوان اولین کشوری یاد می‌شود که با استفاده از فناوری بلاک‌چین امکان ثبت و انتقال اوراق بهادار ثبت نشـــده را فراهم نموده است (Christin, 2013: 213-224). در فرانســـه نیز رمزارزها مجاز دانســـته شـــده‌اند اما ذیل محدودیت‌ها و تدابیر قوانین و مقررات قرار گرفته‌اند و مالیات برای معاملات مربوط به آن‌ها در نظر گرفته شده است. رمزارز پول شناخته نمی‌شود اما دارایی دیجیتال در نظر گرفته شده اســـت (Digital Assets, 2021). کانادا رمزارز را به مثابه دارایی نامشـــهود شناخته اســـت و رویکرد پذیرش رمزارز در این کشـــور وجود دارد لیکن برای جلوگیری از اثرات مخرب رمزارزها، قوانین پول‌شـــویی و ضدتروریستی متناسب با آن‌ها تصویب شـــده است (Rabenfeld, 2014: 2). برای کسب و کارهای خرید و فروش رمزارز و هم‌چنین سرمایه‌گذاری در رمزارزها، مالیات وضع می‌شود و صرافی‌های بیت‌کوین به عنوان کســـب‌وکارهای خدمات پولی درنظر گرفته می‌شوند (قائم‌مقامی، ۱۳۹۵: ٦٦). تا کنون چارچوب‌های قانونی گســـترده‌ای در کانـــادا برای تنظیم مقررات دارایی‌های دیجیتال وضع شـــده‌اند که ضوابط کنترلی متعدد، قوانیـــن و رویه‌های قضایی راجع بـــه تنظیم‌کنندگان اوراق بهادار، تصویب قوانین انتقال، تدابیر مبارزه با پول‌شـــویی و تأمین مالی تروریســـم، مقـــررات مربوط به پرداخت‌ها، مالیـــات، برنامه‌ریزی املاک، و ضوابط زیســـت‌محیطی برای عملیات اســـتخراج ارزهای دیجیتـــال، از جمله آن‌ها می‌باشـــند (Clements, & Torrie, 2023: 350). دولت اســـترالیا نیز رمزارزها را به رسمیت شناخته اســـت؛ بیت‌کوین و سایر ارزهای دیجیتال در استرالیا قانونی هستند و به عنوان دارایی تلقی می‌شـــوند. هم‌چنین در چارچوب قانون مبارزه با پول‌شویی و نیز مقابله با تروریسم، ارزهای دیجیتال در محدوده سیستم ضد پول‌شویی و ضدتأمین مالی تروریســـم در اســـترالیا قرار گرفته اســـت (اخوان، ۱۳۹۷: ۹۹)؛ با این حال در برخی کشـــورها از قبیل چین و روســـیه نگاه بدبینانه و محتاطانه نسبت به رمزارزها وجود داشـــته و در چارچوب سیاســـت تقنینی، محدودیـــت حداکثری در قبال آن‌ها

اتخاذ شده اســـت (Huang, & Mayer, 2022: 325). برای مثال در روسیه، پذیرش رمزارز به شکل رسمی اعلام نشده است. رمزارز به عنوان وسیله پرداخت ممنوع شده لیکن برای ســـرمایه‌گذاری مورد پذیرش قرار گرفته اســـت. با وجود این، از خرید و فـــروش ارز دیجیتال در صرافی‌های معتبر و مجاز به عنوان دارایی‌های مالی دیجیتالی حمایت شده است. در چین اساساً رمزارزهای دولتی به عنوان رمزارز معتبر شناسایی شـــده‌اند؛ با این‌حال رمزارزها به عنوان دارایی مجازی شناخته شده و نگهداری و نقل و انتقال آن‌ها جرم محسوب نمی‌شود، اما عرضه اولیه رمزارز ممنوع اعلام شده است. ممنوعیت‌ها و محدودیت‌های شدیدی از سوی بانک خلق چین برای تجارت ارزهای مجازی و عرضه اولیه کوین در نظر گرفته شده است (اتوود، ۱۳۹۷: ٦٩).

با توجه به رویکرد این کشورها لازم است ابتدا ماهیت این پدیده شفاف شده و از ســـوی حاکمیت ایران مورد پذیرش واقع گردد و در گام اول مالیت و تبادل و داد و ســـتد آن‌ها توسط مراجع رســـمی مجاز اعلام گردد و سپس همانند کانادا و فرانسه حداقل به مقرره‌گذاری و حداکثر قانون‌گذاری بپردازیم.

۲. شیوه‌های ارتکاب جرم و تحلیل اهم دعاوی کیفری در خصوص رمزارزها

بـــا توجه به ابهامـــات و تردیدهایی که پیرامون انطباق اعمـــال زیان‌بار حیطه رمزارزها با عناوین مجرمانه وجود دارد، نیاز اســـت که شـــیوه‌های ارتکاب جرم در حـــوزه رمزارزهـــا و اهم دعاوی در ایـــن ارتباط مورد تحلیـــل و ارزیابی قرار گیرد. شـــیوه‌های ارتکاب جرم در رابطـــه با رمزارزها را می‌تـــوان از حیث نقش و کارکرد رمزارز در شکل‌گیری و وقوع جرم، به سه دسته تقسیم نمود؛ به این صورت که گاهی رمزارز صرفاً وسیله‌ای برای ارتکاب یک جرم است و گاهی خود رمزارز مال موضوع جرم بوده که جرم بر آن واقع گردیده اســـت؛ اما حالت ســـومی نیز قابل تأمل است و آن این‌که فعالیت مرتبط با رمزارز موضوع جرم باشد.

۲-۱. استفاده از رمزارز به مثابه وسیله ارتکاب جرم

بـــا توجه به قوانین کنونی در نظام حقوقی داخلـــی، عمده جرائمی که متوجه دارایی‌های رمزارز هســـتند، دسترســـی غیرمجاز، جعل اطلاعـــات و داده‌ها، ممانعت از دسترســـی و کلاه‌برداری رایانه‌ای در قانون جرائم رایانه‌ای مصوب ۱۳۸۸ اســـت. بنابرایـــن هرگونه مداخله در کیف پول رمزارز و داده‌هـــای مربوط به آن، که مصداقاً

قابـــل انطباق با اعمال مزبـــور در قانون جرائم رایانه‌ای باشـــد، تحت عنوان یکی از جرائم مندرج در این قانون قابل تعقیب و مجازات خواهد بود. نظریه مشورتی شماره ۱۶۲۳/۱۴۰۰/۷ مـــورخ ۱۴۰۱/۰۸/۲۳ اداره کل حقوقی قوه قضاییه درباره کلاه‌برداری رایانه‌ای که مال موضوع جرم ارز دیجیتال باشـــد، چنین آورده است: «اولاً، با عنایت به مقررات مربوط از جمله ماده ۳۱۲ قانون مدنی و ماده ۷۴۱ قانون مجازات اســـلامی (ماده ۱۳ قانون جرائم رایانه‌ای مصوب ۱۳۸۸)، معادل آنچه از کیف پول الکترونیکی برده شـــده است، باید به مال‌باخته مسترد شـــود؛ از آن‌جا که مال موضوع سوال مثلی تلقـــی می‌شـــود، دادگاه باید حکم به پرداخت ارز دیجیتال صـــادر کند و در صورت امتناع، با عنایت به این‌که معامله ارزهای دیجیتال بر اســـاس مقررات بانک مرکزی و تصویب‌نامه شماره ۵۸۱۴۴/ت ۵۵۶۳۷ هـ مورخ ۱۳۹۸/۵/۶ هیأت وزیران در مبادلات داخلی رســـمیت ندارد، لذا توقیف و فروش آن به وسیله اجرای احکام ممکن نیست؛ بنابراین در حکم مالی اســـت که به آن دسترسی نیســـت و با توجه به ملاک ماده ۴۶ قانـــون اجرای احکام مدنی مصوب ۱۳۵۶ قیمـــت آن به تراضی طرفین و در صورت عدم تراضی، بهای آن به قیمت یوم‌الادا به وســـیله کارشـــناس و خبره محاســـبه و از محکوم‌علیه وصول و به محکوم‌له پرداخت می‌شود».

۲-۲. رمزارز به مثابه موضوع جرم، تحلیل عناصر

در حال حاضر جرم بودن عمل به واسطه رمزارز بودن موضوع آن یا به عبارت دیگر به ذاته جرم انگاشـــتن فعالیتی به واسطه این‌که در خصوص رمزارز (استخراج، بهره‌برداری و یا داد و ســـتد) انجام شـــده اســـت، با عنایت به ماده ۲ قانون مجازات اسلامی و اصل قانونی‌بودن جرائم و مجازات‌ها، محل اشکال است. با توجه به این‌که در خصوص رمزارز جرم‌انگاری صریحی صورت نگرفته است نمی‌توان بدون احراز عناصر دیگر جرائم (نظیر قاچاق، کلاه‌برداری، پول‌شـــویی، اخلال در نظام اقتصادی و ...) هر نوع فعالیتی را که از اســـتخراج رمزارز تا استفاده از آن صورت می‌پذیرد جرم پنداشت. در برخی مواقع ممکن است تصور شود که رمزارز جدید بدون پشتوانه است و لذا ابزار فریبنده تلقی شود بنابراین ممنوع و مجرمانه بوده و کلاه‌برداری است؛ این می‌تواند برداشـــت اشتباهی باشد چرا که بیشـــتر رمزارزها و معروف‌ترین آن‌ها چنین هســـتند. در حقیقت رمزارزها دارای خصیصـــه تمرکززدایی بوده و با رویکرد حذف

حاکمیت و نظارت ایجاد شـــده‌اند و اکثریت آن‌ها هیچ‌گونه پشتوانه مالی و اقتصادی ندارند. کنار گذاشتن حاکمیت یک چالش اساسی در این زمینه ایجاد کرده است و آن این‌که هیچ مقرره خاصی در این زمینه وجود ندارد که خط‌کش و معیاری مشـــخص کنـــد برای آن‌که بتوان رمـــزارز حقیقی و غیرحقیقی یا فعالیت درســـت را از فعالیت نادرســـت در عرصه رمزارزها بازشناسد. بر اســـاس روند متعارف ایجاد و استفاده از رمزارزها، یک‌ســـری خصوصیات کلی و معیارها وجود دارد؛ نظیر این‌که رمزارزها بر مبنای اســـتخراج و بر پایه رمزنگاری ایجاد می‌شوند ولی همین موارد هم با توجه به تنوع رمزارزها و تحولات در عرصه فناوری ممکن اســـت دســـتخوش نقض و تغییر گردند. مکانیســـم مقابله حقوق کیفری با جرائم ارتکابـــی حوزه رمزارزها در مراحل اولیه توســـعه قرار دارد؛ در این مســـیر، رسمیت یافتن دارایی‌های دیجیتال و ارزش و اعتبار آن در قانون جهت حمایت از افراد و تعلق سایر حقوق و تکالیف قانونی بسیار مهم اســـت. در وهله بعدی لازم است مشخص شود که در دکترین حقوق کیفری در فرایند ارتکاب جرم جایگاه رمزارزها به عنوان موضوع جرم یا وسیله ارتکاب آن کجا اســـت (Bokovny et al, 2020: 272) . در کل، دادگاه‌هـــا نمی‌تواننـــد در خصوص رمزارزهـــا جرم خاصی را در نظر بگیرند بلکه باید ضمن شـــناخت ماهیت و آگاهی کافی از ابعاد فعالیت‌های مرتبط با آن‌ها، ارکان ســـایر جرائم مربوطه در قوانین کیفری و انطباق با فعالیت‌های صورت گرفته را مطمح نظر قرار دهند. بنابراین بحث از جرم رمزارز جعلی یا تقلبی در این شرایط محلی از اعراب نخواهد داشت و باید دید که آیا اســـتفاده از رمزارزها می‌توانسته عناصر جرائم دیگری چون کلاه‌برداری و پول‌شویی و غیره را فراهم نماید یا خیر.

۳-۲. تحلیل اهم دعاوی و تطبیق عناصر جرم در رســـیدگی کیفری مرتبط با رمزارزها

با توجه بـــه این‌که اســـتخراج غیرقانونی رمزارز با بهره‌بـــرداری و معاملات رمزارزها و اســـتفاده از آن‌ها، دو طیف متفاوت هستند، در ادامه ضمن تفکیک این دو مورد به بررســـی اهم عناوین مجرمانه کیفری مرتبط با آن‌ها و تحلیل شـــرایط انطباق فعالیت‌های پیرامون رمزارزها با این عناوین کیفری، خواهیم پرداخت.

۱-۳-۲. دعاوی مرتبط با استخراج غیرقانونی رمزارزها

اگر شخصی بدون داشتن شرایط لازم و یا اخذ مجوز مربوطه در مقررات، اقدام به عملیات استخراج رمزارز نماید، نمی‌توان عمل او را بر اساس مبانی حقوقی جرم دانست زیرا هیأت وزیران و اساساً قوه مجریه در هر سطحی صلاحیت جرم‌انگاری و تهدید حقوق شهروندی را ندارد و مواردی مانند توقیف و ضبط دستگاه‌های ماینینگ (در فرض وجود مجوز گمرکی) یا پلمپ واحد صنفی و توقیف بیت‌کوینی که استخراج شده است، که به عنوان مجازات تلقی می‌شود و باید در قوانین مصوب مجلس پیش‌بینی شده باشد، قابل اعمال نخواهد بود.

۲-۳-۲. دعاوی مرتبط با استفاده از رمزارزها

از حیث ارتباط و انطباق با عناصر دیگر جرائم و مبتلابه بودن می‌توان به طور کلی اعمال زیان‌باری که در رابطه با رمزارزها انجام می‌شوند را به دسته‌های زیر تقسیم کرد:

الف. جرائم رایانه‌ای

جرم کلاه‌برداری رایانه‌ای از مهم‌ترین عناوینی است که در خصوص اعمال مرتبط با رمزارزها مورد توجه قرار می‌گیرد. اطلاق جرم کلاه‌برداری رایانه‌ای یا کلاه‌برداری سنتی حسب مورد بسته به نوع ارتکاب جرم و امکان تطبیق آن با مواد قانونی مربوطه است. همان‌طور که در نظریه مشورتی اداره کل حقوقی قوه‌قضاییه به آن اشاره شده است، ملاک تحقق بزه موضوع ماده ۷٤۱ قانون مجازات اسلامی مصوب ۱۳۷۵ الحاقی ۱۳۸۸/۳/۵ (ماده ۱۳ قانون جرائم رایانه‌ای مصوب ۱۳۸۸) این است که «وجه یا مال یا منفعت یا خدمات یا امتیازات» با استفاده غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی و با ارتکاب اعمالی از قبیل واردکردن، تغییر، محو، ایجاد، متوقف کردن داده‌ها یا مختل کردن سامانه‌ها تحصیل گردد؛ وگرنه اگر کسی بدون ارتکاب چنین اعمالی ولی با استفاده از سامانه‌های رایانه‌ای یا مخابراتی موجب فریب فرد یا افرادی گردد و مالی از آنان تحصیل نماید، موضوع از مصادیق کلاه‌برداری ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاه‌برداری خواهد بود. ماده ۷۲۹ قانون مجازات اسلامی (ماده ۱ قانون جرائم رایانه‌ای) مقرر می‌دارد: «هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به

وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی) از شصت و شش میلیون ریال تا دویست و شصت و چهار میلیون ریال[1] یا هر دو مجازات محکوم خواهد شد». هم‌چنین ماده ۷۳۸ الحاقی به قانون مجازات اسلامی (ماده ۱۰ قانون جرائم رایانه‌ای) مقرر می‌دارد: «هرکس به طور غیرمجاز با اعمالی از قبیل مخفی‌کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از شصت و شش میلیون ریال تا دویست و شصت و چهار میلیون ریال[2] یا هر دو مجازات محکوم خواهد شد».

ب. جرم کلاه‌برداری

رمزارزها به دلیل در معرض سوءاستفاده قرار گرفتن با روش‌های کلاه‌برداری ریسک بالایی دارند. با توجه به ملاک‌ها و معیارهای قانون و شیوه‌های مجرمانه‌ای که در خصوص رمزارزها وجود دارد، رفتارهای متقلبانه در این زمینه که منجر به بردن مال دیگری می‌شود بیش از هر چیز در چارچوب جرم کلاه‌برداری سنتی قابل تطبیق و تفسیر است. ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاه‌برداری، مقرر می‌دارد: «هرکس از راه حیله و تقلب مردم را به وجود شرکت‌ها یا تجارتخانه‌ها یا کارخانه‌ها یا موسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیرواقع امیدوار نماید یا از حوادث و پیشامدهای غیرواقع بترساند و یا اسم و یا عنوان مجعول اختیار کند و به یکی از وسایل مذکور و یا وسایل تقلبی دیگر وجوه و یا اموال یا اسناد یا حوالجات یا قبوض یا مفاصاحساب و امثال آن‌ها تحصیل کرده و از این راه مال دیگری را ببرد کلاه‌بردار محسوب و علاوه بر رد اصل مال به صاحبش، به حبس از یک تا هفت سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می‌شود».

به صرف تولید و ارائه رمزارز بدون پشتوانه که مورد اقبال عمومی نیز قرار نمی‌گیرد و ارزش آن کاهش می‌یابد، نمی‌توان گفت از ابزار متقلبانه برای بردن مال

---

۱. جزای نقدی مندرج در این ماده به موجب مصوبه شماره ۵۶۲۶۱/ت۶۲۲۹۸هـ مورخ ۱۴۰۳/۴/۴هیات وزیران به مبلغ مذکور تعدیل شده است.

۲. جزای نقدی مندرج در این ماده به موجب مصوبه شماره ۵۶۲۶۱/ت۶۲۲۹۸هـ مورخ ۱۴۰۳/۴/۴هیات وزیران به مبلغ مذکور تعدیل شده است.

دیگران استفاد شده و نتیجتاً جرم کلاه‌برداری محقق شده است، اما اگر تمامی اقدامات راجع به تولید و ارائه رمزارز بر مبنای ادعای اشـــخاصی که اقدام به ایجاد و واگذاری آن می‌کنند نباشـــد از جمله این‌که در ظاهر، پلتفرمی در یک سایت معتبر تأسیس شده و افتتاح کیف پول الکترونیک و معاملات راجع به یک رمزارز جدید انجام می‌شـــود اما در واقع این رمزارز ادعایی بر اســـاس فناوری بلاک‌چین تولید نشده است و عملاً رمزارزی که در کیف پول قرار دارد امکان مبادله با سایر رمزارزها را نیز نداشته باشد و کســـی که این رمزارز را خریداری کرده نه امکان تبدیل آن را داشته باشد نه امکان برداشـــت؛ در چنین موردی با فعالیتی فریبنده مواجه هستیم که مبتنی بر ادعایی واهی و تقلبی، منجر به بردن مال دیگران و تحقق ارکان جرم کلاه‌برداری شـــده است. با در نظر گرفتن این‌که امروزه ســـاخت و ایجاد رمزارز برای اشخاصی که دانش و مهارت فنی در این زمینه را دارند کاری ســـهل و سریع محسوب می‌شود و این، نفس رمزارز نیســـت که مبنای ارزش آن قرار می‌گیرد بلکه اعتباری است که اعتماد و اقبال عمومی و پذیـــرش در جامعه برای رمزارز ایجـــاد می‌کند و اگر افراد اقدام به ایجاد کیف پول و خریداری این رمزارز جدید نمایند تا اینجا می‌توان گفت همه چیز بر اســـاس عرف و رویـــه تولید و ارائه رمزارزها صورت گرفتـــه و فعالیت متقلبانه‌ای نیز انجام نگرفته اســـت. اما اگر عرضه کنندگان رمزارز به منظور افزایش ارزش و اعتبار و رســـیدن به نقطه ســـودآوری اقداماتی انجام دهند که مبنای درســـت و واقعی نداشته باشد (برای مثال ارزش رمزارز را در ســـایت دستکاری کنند و یا وعده‌ای داده شود مثل این‌که با خریداری هر واحد رمزارز روزانه میزان مشـــخصی سود پرداخت می‌شود) تا این‌که در نتیجه با اســـتفاده از امور واهی و وســـایل متقلبانه گرایش به رمزارز جدید را در جامعـــه و میان افراد افزایش دهند، در این حالت گرچه طراحی و عرضه رمزارز جرم نیســـت اما روشی که برای ترغیب و تشـــویق افراد به خریداری آن استفاده شده توأم بـــا بهره‌گیری از ابزارهای متقلبانه و جعل واقعیت بوده اســـت؛ لذا در این خصوص کلاه‌برداری محرز خواهد بود.

پ. جرم اخلال در نظام اقتصادی کشور

در نظام حقوقی ایران با تصویب قانون مجازات اخلال‌گران در نظام اقتصادی کشـــور جرائمی که موضوع اخلال در نظام اقتصادی می‌باشند در دو ماده احصا شده

اســـت که با توجه به ماده ۲۸۶ قانون مجازات اســـلامی مصوب ۱۳۹۲، ارتکاب این جرائم که منجر به اخلال در نظام اقتصادی کشـــور شود؛ به گونه‌ای که رفتار مرتکب اختلال شـــدید در نظم عمومی جامعه و ورود خســـارت عمده بـــه اموال عمومی و خصوصی را موجب شـــود، افساد فی الارض محســـوب می‌گردد (کمیلی، دانشور و گرایلی، ۱۴۰۰: ۱۳).

قانون مجازات اخلال‌گران در نظام اقتصادی کشـــور مصادیقی را مطرح نموده است که با برخی از فعالیت‌های زیان‌بار در حوزه رمزارزها قابل‌انطباق به نظر می‌رسد و عملاً نیز برخی قضات در جرائم مرتبط با رمزارزها به آن متمایل شده‌اند. بر اساس مـــاده یک این قانون، ارتکاب اعمال مذکور در بندهـــای الف تا ز، به عنوان مصادیق اخلال در نظام اقتصادی مشـــمول مجازات‌های مقرر در قانون شـــناخته شده است. دو بنـــد «هـ» و «ز» این ماده با فعالیت‌هـــای مجرمانه در زمینه رمزارزها ارتباط برقرار می‌نماید. قانون‌گذار در بند هـ «وصول وجوه کلان به صورت قبول ســـپرده اشخاص حقیقی یا حقوقی تحت عنوان مضاربه و نظایر آن که موجب حیف و میل اموال مردم یا اخلال در نظام اقتصادی شـــود»، را مطرح نموده است. باید دقت داشت که مستفاد از بند هـ ماده یک قانون مجازات اخلالگران در نظام اقتصادی کشـــور فرض اســـت که شـــخص به صـــورت واقعی اموال مردم را تحت عنـــوان عقود صحیح به صورت ســـپرده قبول می‌کند ولی عملاً موجب حیف و میل این اموال می‌شود (سمیعی زنور و حبیب‌زاده و صابر، ۱۳۹۵: ۳۱)؛ اما در فرضی که با اســـتفاده از وســـایل متقلبانه و فریبنده و امور واهی، افراد جلب ســـرمایه‌گذاری می‌شوند، عنوانی که انطباق بیشتر و بهتری با فعالیت حوزه رمزارز می‌یابد عنوان کلاه‌برداری اســـت. بند ز ماده یک قانون مجازات اخلالگران در نظام اقتصادی کشـــور، در خصوص شرکت‌های هرمی مطرح شـــده است و مشخصاً یکی از شقوق فعالیت‌های مجرمانه در حوزه رمزارزها استفاده از طرح‌هـــای پانزی و هرمـــی در چارچوب فعالیت‌های مرتبط با رمزارزها اســـت و زمینه‌های قبلی (نظیر خرید ســـکه و ...) در حال منسوخ شدن است. برای مثال یک کویـــن به صورت غیرواقعی و مزورانه یا حتی به طور واقعی و در بســـتر بلاک‌چین ایجاد می‌شـــود و بـــرای جلب اعتماد مردم به آن و ایجـــاد زمینه گرایش تصاعدی و گســـترش شبکه، از قالب شرکت‌های هرمی یا گلدکوئیست استفاده می‌شود و به طور

مثال برای افرادی که بتوانند زیرشـــاخه ایجاد کنند ارزش سهم بیشتر یا تخفیف بالاتر در هنگام خرید رمزارز و مانند این‌ها منظور می‌شود. در واقع، اگر شخصی در تولید و عرضه رمزارز اقدامات متقلبانه انجام دهد و در عین‌حال از چارچوب شیوه‌های هرمی برای افزایش طیف خریداران و فزونی اعتبار برای رمزارز استفاده نماید، در اینجا، هم جرم کلاه‌برداری و هم جرم اخلال در نظام اقتصادی از طریق عضوگیری محقق شده است و لذا جرم، تعدد مادی دارد.

ت. جرم پول‌شویی

پول‌شویی به عنوان تلاش یا اقدام در پنهان کردن هویت درآمدهای غیرقانونی و ســـعی بر قانونی جلوه دادن آن‌ها تعریف می‌شـــود رمزارزها را با توجه به ماهیت و خصایص آن‌ها، بســـتری مناســـب برای ارتکاب جرم پول‌شویی محسوب کرده‌اند (مرادی قلعه، ۱٤۰۱: ۱۷۱). افزایش سرعت تراکنش‌ها و خصوصیات آن‌ها، پیچیدگی نظـــارت را افزایش داده و ترکیب اســـتفاده از رمزارزها با ســـایر روش‌های نوین و ســـنتی پول‌شویی، کشـــف و تعقیب این جرم را بسیار دشـــوار کرده است. در نظام حقوقـــی داخلی، ماده ۲ قانون مبارزه با پول‌شـــویی مصوب ۱۳۸٦ (اصلاحی ۱۳۹۷)، مفهوم و مصادیق پول‌شـــویی را مورد توجه قرار داده اســـت که در این میان به ویژه بنـــد ب این ماده می‌تواند بـــا فعالیت‌های مجرمانه در حـــوزه رمزارزها قابل انطباق باشـــد. یکی از مشـــکلاتی که در نظام داخلی منجر به دامن زدن به بحث پول‌شویی از طریق فعالیت‌های رمزارز می‌شـــود، وجود بســـتر مناسبی به نام صرافی‌های آنلاین اســـت که در کشور ما بر اساس مجوز پایه ثبت شرکت‌ها فعالیت می‌کنند اما مجوزی از مراجـــع ذی‌ربط مالی و بانکی ندارنـــد و از طرفی ممنوعیتی هم برای فعالیت آن‌ها در قوانین مصوب منظور نشـــده اســـت که این امر نظارت بر کار آن‌ها را با دشواری مواجه می‌نماید. در چنین شـــرایطی این صرافی است که باید حسن‌نیت خود را ثابت کند زیرا این صرافی‌ها باید ریســـک معاملات خـــود را بپذیرند و احتیاط‌های لازم را به عمل آورند. در این زمینه اســـتفاده از ملاک مواد ۵ و ۷ قانون مبارزه با پول‌شـــویی و الزاماتی که برای صرافی‌ها (در کنار ســـایر اشخاص موضوع قانون) می‌توان در نظر گرفت راهگشـــا خواهد بود. ضمن این‌که می‌توان به تبصره یک ماده ۹ قانون مبارزه با پول‌شـــویی نیز استناد جست از آن حیث که طبق این تبصره «چنانچه عواید حاصل

از جـــرم به اموال دیگری تبدیل یا تغییر یافته باشـــد همان اموال و در صورت انتقال به ثالث با حســـن‌نیت، معادل آن از اموال مرتکب ضبط می‌شـــود»؛ و مفهوم مخالف این مقرره این اســـت که اگر ثالث حسن‌نیت نداشت می‌توان مال مزبور نزد او را نیز ضبط نمود؛ در نتیجه اگر صرافی آنلاین در انجام معامله حســـن‌نیت نداشته باشد، هم می‌توان ریال پرداخت شـــده به صرافی را توقیف نمود و هم او را به اتهام پول‌شویی تحت پیگرد قرار داد.

۳. نگاهی انتقادی به رویه قضایی

در جهت تبیین بیشـــتر موضوع، در این قســـمت صرفاً بـــه معرفی دو پرونده مهم و کثیرالشـــاکی در حوزه حقوق کیفری رمزارز خواهیم پرداخت. پرونده نخست موســـوم به کینگ‌مانی[1] با بیش از دو هزار و یکصد نفر شـــاکی و هشـــت نفر متهم با عنوان مشـــارکت در کلاه‌برداری شـــبکه‌ای منجر به اخلال در نظام اقتصادی کشور از طریق ایجاد رمزارز جعلی به اســـم کینگ مانی و توزیع ارز جعلی بین مردم (ســـایر اتهامات بـــه دلیل عدم ارتباط با حوزه رمزارز محل بحث نخواهد بود) و پرونده دوم موســـوم به کریپتولند[2] با بیش از بیســـت و شش هزار و پانصد نفر شاکی و هشت نفر متهم با عناوین تشـــکیل، سردستگی و مشارکت شبکه ســـازمان‌یافته اخلال کلان در نظام اقتصادی (ارزی و پولی) کشـــور از طریق تصـــدی به عملیات صرافی غیرمجاز و معاملات غیرمجاز رمزارزی و هم‌چنین مباشـــرت در اخلال کلان در نظام ارزی و پولی کشور از طریق خیانت در امانت و برداشت غیرمجاز از نقدینگی کاربران صرافی غیرمجاز کریپتولند و تحصیل مال از طریق نامشروع سپرده‌های مردمی (سایر اتهامات بـــه دلیل عدم ارتباط با حوزه رمزارز محل بحث نخواهد بود) که نهایتاً هر دو پرونده منجر به صدور رأی قطعی و محکومیت به عناوین اتهامی مذکور گردید[3].

رویکرد قضایی در این حوزه نشان‌دهنده چالش‌های ناشی از درک پیچیدگی‌های فنی رمزارزها و نوســـان سیاســـت جنایی در انطباق صحیح فعالیت‌های مرتبط با این

---

1. King Money
2. Cryptoland

۳. دادنامه شـــماره ۱۴۰۳۶۸۳۹۰۰۰۰۳۲۳۹۸۹ مورخ ۱۴۰۳/۱/۲۱ صادره از شعبه دوم دادگاه انقلاب اسلامی تهران ویژه رســـیدگی به جرائم اقتصادی؛ و دادنامه شماره ۱۴۰۲۶۸۳۹۰۰۱۱۸۴۲۹۱۹ مورخ ۱۴۰۲/۸/۹ صادره از شـــعبه پنجم دادگاه انقلاب اســـلامی تهران ویژه رســـیدگی به جرایم اقتصادی تهران.

حـــوزه با عناوین مجرمانه اســـت. به عنـــوان نمونه، تأکید بر جعلـــی بودن رمزارز و صرافی‌های ســـاختگی در آرای قضایی، با وجود منتفی بـــودن فرض جعل در مورد رمزارزها و احراز معیارهای فنی اولیه، بیانگر ضعف شـــناخت صحیح مفاهیم مرتبط در رویه قضایی اســـت. این امر منجر به انتساب عناوین مجرمانه‌ای مانند کلاه‌برداری و اخلال در نظام اقتصادی شده است که از لحاظ مبنای حقوقی محل تردید محسوب می‌شود.

افـــزون بر این، انتســـاب عنوان «اخلال کلان در نظـــام اقتصادی» به معاملات رمـــزارزی، با توجه به ضرورت تطابق عناصـــر قانونی این جرم با رفتارهای ارتکابی، یکی از نقاط چالش‌برانگیز در این آرا به شـــمار می‌رود. در کنار جرم اخلال در نظام اقتصادی، اســـتناد به عناوینی نظیر کلاه‌برداری و تحصیل مال از طریق نامشروع نیز با توجـــه به ملاحظاتی از جمله فقدان منع قانونی در خصوص معاملات رمزارزی، عدم امکان جرم‌انگاری صرفاً بر مبنای مصوبات دولتی، خروج رمزارزها از تعریف ســـنتی پول و ارز، عدم شـــمول قوانین حوزه پولی و ارزی بر رمزارزها، تشـــکیک در تحقق عنصـــر «بردن مال» در فرض وجود توکن‌ها[1] و هم‌چنین ضرورت تفســـیر مضیق در حقوق کیفری، با انتقادات جدی مواجه است.

طی مطالعه آرای فـــوق مشاهده می‌گردد که انطباق عناوین مجرمانه با رفتار مجرمین و اوضاع و احوال پرونـــده‌ها دارای ابهامات و انتقاداتی است. رویه قضایی باید به ســـمتی حرکت نماید که ضمن درک جامـــع و مانع از مباحث فنی رمزارز (و توجه به این‌که در حـــال حاضر قانون خاصی در این حوزه وجود ندارد) بتواند فارغ از اهمیـــت پرونده نزد عموم جامعه، با عناوین مجرمانـــه موجود، عنوان صحیحی را بـــه رفتارهای مختص حوزه بلاک‌چین انطبـــاق داده و عدالت کیفری در این حوزه را حفظ نماید.

---

۱. توکن‌ها (Token)، واحدهای رمزنگاری‌شـــده‌ای هســـتند که بر بســـتر فناوری بلاک‌چین ایجاد می‌شـــوند و می‌توانند نمایان‌گر دارایی، حق مالکیت یا دسترســـی به یک خدمت دیجیتال باشند. در دنیـــای فناوری اطلاعات و به ویژه در حوزه رمزنـــگاری (Cryptography) و ارزهای دیجیتال، یک توکن یک واحد دیجیتال ارزش یا یک دارایی است که بر روی یک بلاک‌چین از پیش موجود ایجاد شده و عمل می‌کند.

٤. مشکلات رسیدگی شکلی به دعاوی رمزارزها از منظر آیین دادرسی کیفری

گسترش مبادلات مبتنی بر رمزارزها و افزایش جرائم مرتبط با این حوزه، نظام عدالت کیفری را با چالش‌هایی نوظهور در زمینه آیین رسیدگی به این‌گونه دعاوی دست به گریبان نموده است. ماهیت غیر متمرکز، ناشناخته و فناورانه رمزارزها، سبب شده تا سازکارهای سنتی آیین دادرسی کیفری در حوزه‌هایی چون کشف جرم، تعقیب متهم، گردآوری ادله، و اجرای احکام کیفری کارایی لازم را در این زمینه نداشته باشند. نبود قوانین صریح و دستورالعمل‌های فنی برای نحوه توقیف، نگه‌داری و ارزش‌گذاری دارایی‌های دیجیتال نیز بر پیچیدگی این روند افزوده است. از این رو، بررسی دقیق چالش‌های شکلی در فرایند رسیدگی به جرایم مرتبط با رمزارزها، به ویژه در مراحل کشف و تعقیب جرم، تحقیقات مقدماتی و اجرای احکام، می‌تواند زمینه‌ساز اصلاح رویه‌های موجود و تدوین چارچوبی منطبق با واقعیت‌های حقوقی و فناورانه عصر دیجیتال باشد.

٤-١. کشف و تعقیب جرم

یکی از چالش‌هایی که در رابطه با رسیدگی به رمزارزها وجود دارد و برخاسته از خصایص آن‌ها است بحث امکان ردیابی و کشف جرم است. در واقع در رمزارزها به واسطه آن‌که با هدف محرمانه ماندن اطلاعات و هویت اشخاص، عملیات صحت‌سنجی تراکنش‌ها از طریق فرمول‌های ریاضی و الگوریتم‌های رمزنگاری صورت می‌پذیرد شناخت هویت اشخاص می‌تواند فاقد موضوعیت باشد. این مسأله در مورد نظارت بر معاملات رمزارز که خارج از حیطه صرافی‌های داخلی و به صورت بین‌المللی انجام شده است امکان رهگیری و رسیدگی را با مانع مواجه می‌سازد.

از سوی دیگر رمزارزها ماهیتی کاملاً دیجیتالی دارند و هیچ‌گونه اثر و نشانه حقیقی و فیزیکی خارج از فضای مجازی ندارند و همین امر تعقیب جرم را از جهات مختلف با مشکل مواجه می‌کند؛ ضمن آن‌که به دلیل جدید بودن این پدیده، ضابطان دادگستری اشرافی کامل نسبت به نحوه کار و ظرافت‌های فنی رمزارزها ندارند و همین امر موجب می‌گردد تا در مراحل کشف و تعقیب جرائم، چالش‌های جدیدی

نمایان شود. البته به علت شفافیت ناشی از فناوری دفترکل توزیع شده (زنجیره بلوک عمومی)، امکان مشـــاهده تمامی تراکنش‌های رمزارزها وجود دارد و نهادهای نظارتی و مجری قانون قادرند اقدام به رصد آن‌ها نمایند؛ اما مشـــکل اصلی چگونگی تعیین و تشـــخیص تراکنش‌های مشکوک در رمزارزها و شناسایی طرفین آن است؛ زیرا هر تراکنش به یک کد رمزنگاری شـــده،که کلید عمومی خوانده می‌شود، متصل است و تنها راه ممکن جهت کشـــف هویت کاربران، استفاده از روش‌های پیچیده فنی تحلیل شـــبکه و استفاده از منابع اطلاعاتی اســـت و امکان کشف جرائم مرتبط با آن‌ها بدون استفاده از شـــیوه‌های فنی پیشـــرفته وجود ندارد (Kethineni and Dodg, 2018: 145). علاوه بر این‌که باید در نظر داشـــت که اشخاص می‌توانند از آدرس‌های متعدد (کلید عمومی) اســـتفاده کنند که فرایند کشف و ردیابی را بسیار پیچیده و غیرممکن می‌ســـازد. با توجه به این‌که میزان گمنامی اشخاص، بســـتگی به میزان مهارت آن‌ها در اســـتفاده از روش‌ها و ابزارهای گمنام‌کننده مضاعف دارد، لذا کشـــف و شناسایی مجرمان حرفه‌ای به مراتب سخت‌تر و هزینه برتر از اشخاص عادی خواهد بود (نبوی و صابر، ۱۳۹۹: ۱۹۷).

بـــه رغم پیچیدگی‌ها و موانعی که در این زمینه وجود دارد و با توجه به این‌که کشـــف و تعقیب جرائم مرتبط با حوزه رمزارزها امری محال نیست و در بسیاری از مـــوارد قابلیت پیگیری دارد، بنابراین نباید مانع رســـیدگی تا حد امکان و بضاعت با بهره‌گیری از نیروی متخصص و کارآمد باشـــد؛ هم‌چنین باید موجب تدوین قوانینی گردد که ســـاماندهی معاملات بر رمزارزها و امکان نظـــارت و کنترل بعدی آن‌ها به منظور تأمین حقوق شهروندان را فراهم آورد.

۲-٤. تحقیقات مقدماتی و مسائل مربوط به دادرسی

پیرامون دادرسی‌ها راجع‌به جرائم مرتبط با سامانه‌های رایانه‌ای و الکترونیکی و به ویژه بحث اســـتفاده و بهره–گیری از ادله الکترونیک، آیین دادرسی جرائم رایانه‌ای (مواد ٦٦٤ به بعد قانون آیین دادرســـی کیفری) در کنار قانـــون تجارت الکترونیک، قانون جرائم رایانه‌ای و مقررات مربوطه به ویژه آیین‌نامه جمع‌آوری و اســـتنادپذیری ادلـــه الکترونیکی، منابع قانونی قابل اســـتفاده و تطبیق در رابطه با دادرســـی پیرامون رمزارزها نیز به شـــمار می‌روند. اما مسأله این است که آیا مفاد قوانین مزبور می‌تواند

با توجه به خصوصیات رمزارزها اقتضائاتی که رسیدگی به آن‌ها به طور ویژه ایجاب می‌کند را فراهم آورند.

سختی و پیچیدگی ردیابی و کشف ادله مربوط به پرونده‌های رمزارزها به نحوی است که تنها از عهده اشخاص متخصص و زبده برمی‌آید؛ اگر متهم از وسایل گمنام‌کننده و یا ماشین‌های مجازی استفاده کرده باشد، ایجاد سابقه الکترونیکی مطمئن مختل می‌شود[1] و کشف و شناسایی رمزارز و یا استفاده از آن را نمی‌توان به راحتی مستندسازی کرد. هر چند تراکنش‌های ثبت شده در زنجیره بلوک، تغییرناپذیر و در نتیجه قابل استناد می‌باشند لیکن مسأله اصلی این است که با توجه به گمنام بودن کاربران و تراکنش‌ها در برخی مواقع، نحوه اثبات و انتساب آن‌ها به یک شخص معین با صعوبت مواجه است[2].

باید افزود که ادله الکترونیک به ویژه در مورد رمزارزها، در معرض تغییر قرار دارند و به میزان قابل‌توجهی فرار هستند؛ کدهای مربوط به رمزارزها شامل تعدادی شماره هستند که میزان حجمی که در فضای مجازی اشغال می‌کنند بسیار ناچیز محسوب می‌شود، بنابراین به‌راحتی می‌توانند در کوچکترین فضای ذخیره‌سازی، پنهان شوند.

اگر رایانه شخص مظنون و یا متهم توقیف شود، باید اقدامات لازم جهت کسب دلایل، به صورت فوری[3] صورت پذیرد زیرا ممکن است اطلاعات ذخیره شده به دلیل بروزرسانی نرم‌افزارها و یا حذف داده‌های قبلی و ثبت داده‌های جدید در سیستم‌های رایانه‌ای، از دست بروند. در صورتی‌که شخص مجرم دارای مهارت و تخصص بالایی باشد، می‌تواند با استفاده از نرم‌افزارهای خاص، در بازه‌های زمانی

---

۱. ماده ۱۱ قانون تجارت الکترونیکی مصوب ۱۳۸۲: «سابقه الکترونیکی مطمئن عبارت از «داده پیام»ی است که با رعایت شرایط یک سیستم اطلاعاتی مطمئن ذخیره شده و به هنگام لزوم در دسترس و قابل درک است».

۲. ماده ۱۰ همان قانون: «امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد: الف – نسبت به امضاء کننده منحصر به فرد باشد. ب– هویت امضاء کننده «داده پیام» را معلوم نماید. ج– به وسیله امضاء کننده و یا تحت اراده انحصاری وی صادر شده باشد. د– به نحوی به یک «داده پیام» متصل شود که هر تغییری در آن «داده پیام» قابل تشخیص و کشف باشد».

۳. بند د ماده ۱ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی مقرر می‌دارد: «جمع‌آوری ادله الکترونیکی، فرایندی است که طی آن ادله الکترونیکی به تنهایی یا به همراه سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده، نگهداری، حفظ فوری، تفتیش و توقیف و شنود می‌شوند».

مشـــخص داده‌های موجود در رایانه را حذف نماید تا دسترسی به آن‌ها ممکن نباشد (نبوی و صابر، ۱۳۹۹: ۲۰۲). با توجه به لزوم حفظ صحت و تمامیت ادله الکترونیک و جهت انتســـاب امضای الکترونیک گمنام به شـــخص متهم، لازم اســـت اطلاعات جمع‌آوری‌شـــده مطابق با اصـــول کلی مربوط به دلیـــل و روش تحصیل آن در امور کیفـــری و هم‌چنین مطابق با اســـتنادپذیری ادله الکترونیک باشـــد. این موضوع برای ضابطان قضایی و دیگر نهادهای مجری قانون حائز اهمیت اســـت، زیرا باید از تدابیر فنی و روش‌های تخصصی برای کســـب دلایل، نگهداری و ارائه آن‌ها در موارد لازم، استفاده گردد (همان: ۲۰۳).

ملاحظه شـــد که کارشناســـان امور کیفری در حیطه رمزارزها نظریات واحد و یکســـانی راجع به کفایت قوانین شـــکلی و از جمله ادله دادرسی الکترونیک برای رسیدگی به جرائم رمزارزها ندارند و برخی طی فرایند دادرسی ادله اثبات الکترونیکی را کافی می‌دانند و در این میان به قابلیت مواد ٦٦٤ به بعد آیین دادرسی کیفری بخش جرائـــم رایانه‌ای و به خصوص ظرفیت مـــاده ٦٧١ به بعد (که بحث توقیف و تفتیش داده‌ها را مطرح ســـاخته است)، اســـتناد می‌جویند و در مقابل برخی اعتقاد دارند که قواعد دادرســـی در حوزه بلاک‌چین و رمزارزها باید به طور کلی دگرگون شود. آنچه مســـلم است این‌که بســـیاری از مواد کنونی در رابطه با دادرســـی و جمع‌آوری ادله الکترونیکی در فرایند تحقیقات و دادرسی کیفری پرونده‌های مرتبط با رمزارزها قابل بهره‌گیـــری هســـتند و در عین‌حال در این زمینه با ملاحظـــه خصایص و ویژگی‌های رمزارزها نیازمند بروزرسانی قوانین شکلی هستیم.

۳-٤. مشکلات پیرامون توقیف، مصادره و اجرای حکم

بحث توقیف و اجـــرای حکم در حیطه رمزارزها از اهمیت بســـیاری بالایی برخوردار اســـت. در بســـیاری از جرائم اعم از کلاه‌برداری، پول‌شـــویی، اخلال در نظام اقتصادی و تأمین مالی تروریســـم و غیره، برای آن‌که پرونده به ســـرانجام برسد نیاز به توقیف یا مصادره دارایی‌ها از جمله رمزارز و وســـایل مرتبط ســـخت‌افزاری و نرم‌افزاری مرتبط با آن می‌باشـــد؛ برای مثال در خصـــوص کلاه‌برداری رایانه‌ای و هم‌چنین کلاه‌برداری ســـنتی، یا موارد توقیف در جرم پول‌شـــویی و مصادره مال (بر اســـاس ماده ۹ قانون مبارزه با پول‌شویی)، نیاز به توقیف یا مصادره رمزارز بر اساس

سازوکاری مشخص با امعان نظر به ویژگی نامحسوس بودن و حریم خصوصی و امنیت مبادلات در بستر بلاک‌چین احساس می‌شود.

حال اگر دادیار یا بازپرس بخواهد در موردی که کلاه‌برداری صورت گرفته است نسبت به توقیف رمزارز اقدام نماید با چالش‌های عدیده‌ای مواجه است؛ این‌که چه سازوکار و چه نهادی برای توقیف و نگهداری از رمزارزها وجود دارد محل چالش و اشکال جدی هستند. در مقوله اجرای حکم نیز برای مثال اگر قرار بر این باشد که رمزارز توقیف‌شده به فروش برسد این معضل وجود دارد که چه سازوکاری برای فروش و یا انتقال رمزارز پیش‌بینی شده است؛ و این در حالی است که رمزارزها هنوز آن‌گونه که بایسته و شایسته است در نظام حقوقی مورد پذیرش قرار نگرفته و رسمیت نیافته‌اند. حال چگونه می‌توان رمزارزی را توقیف نمود و به فروش رساند یا در اختیار شکات و زیان دیدگان قرار داد. بر این اساس برخی کارشناسان به این مهم تصریح داشته‌اند که در بسیاری از موارد نیازمند استفاده از روش‌های منحصر به فردی برای رسیدگی به پرونده‌های رمزارز نظیر توقیف فوری گوشی متهم و بررسی داده‌های آن تا پیش از ایجاد تغییرات و امحای ادله و هم‌چنین ایجاد کیف پول دیجیتال مخصوص دادگستری جهت اجرای احکام توقیف، نگهداری از رمزارز و اجرای نهایی حکم خواهیم بود.

در واقع، یکی دیگر از معضلات فراروی ضابطان دادگستری و دادرسان، نگهداری اموال توقیف شده است. این موضوع نه‌تنها از حیث حفظ حقوق طرفین دعوا و جلوگیری از تضییع اموال اهمیت دارد، بلکه در مواردی که مال توقیفی ماهیت غیرملموس یا فناورانه دارد، پیچیدگی‌های مضاعفی را نیز به همراه می‌آورد. در خصوص اموالی مانند داده‌های دیجیتالی، دارایی‌های مبتنی بر فناوری بلاک‌چین و به ویژه ارزهای مجازی، مسأله نگهداری و صیانت از مال توقیفی، با چالش‌های فنی، امنیتی و حقوقی قابل توجهی روبه‌روست. فقدان چارچوب‌های مدون قانونی، کمبود تخصص فنی در میان ضابطان و خطر بالای از بین رفتن، سرقت یا تغییر ارزش این نوع دارایی‌ها، عدم تطابق شیوه‌های سنتی و معمول توقیف و نگهداری اموال را در این حیطه به وضوح نمایان می سازد. به عبارت دیگر ارزهای مجازی به صورت فیزیکی موجود نیستند و نگهداری از آن‌ها، چالش‌های منحصر به فردی

به همـــراه دارد. در صورتی که ارز مجازی توقیف گردد، نگهداری آن دارای الزاماتی مخصوص به خود خواهد بود؛ اساســاً ضابطان دادگستری باید ارز مجازی را به یک کیف پول دیجیتالی متعلق به دادگســتری و یا پلیس انتقال دهند تا در آن ذخیره شود؛ کیف پول متعلق به نهادهای قانونی و کلید خصوصی آن باید با اســتفاده از روش‌های فنی مورد حفاظت قرار گیرد تا ســرقت نشود و از هرگونه دست‌کاری محفوظ باشد. بدیهی اســت با توجه به تنوع گسترده ارزهای مجازی و کیف پول‌های مجازی، نحوه انتخاب بهترین و امن‌ترین کیف پول باید توســط کارشناسان این عرصه تعیین شود و نیاز است تدابیری اندیشیده شود تا امکان سوء استفاده احتمالی اشخاص مسؤول نیز از بین برود (نبوی و صابر، ۱۳۹۹: ۲۰۰). تغییر قیمت ارزهای مجازی در مدت نگهداری و نحوه فروش ارزهای مجازی مصادره شده نیز از موضوعاتی هستند که در این رابطه نیاز به بررسی و تأمل بیشتری دارند(همان: ۲۰۱).

در رابطه با مســائلی نظیــر توقیف و مصادره و اجرای حکم ضمن اســتفاده از ظرفیــت قوانین فعلی توأم با پذیرش و رســمیت یافتــن رمزارزها، نیازمند تحول و بروزرســانی در قوانین موجود هســتیم زیرا ملاحظه مواد ٦٧١ به بعد قانون آیین دادرســی کیفری در بخش جرائم رایانه‌ای و مســائل مطروحــه در رابطه با تفتیش و توقیــف داده‌ها، حاکی از آن اســت این مقررات علی‌رغم آن‌کــه می‌توانند در زمینه رســیدگی شکلی به پرونده‌های رمزارزها قابل استفاده باشند اما در برخی زمینه‌ها نیز که پیشــتر عرض شــد با مقتضیات جرائم مرتبط با رمزارزها هماهنگ و هم‌راستا به نظر نمی‌رسند و این امر توســعه قوانین و مقررات موجود در این خصوص را امری اجتناب‌ناپذیر می‌سازد.

برآمد

۱- نخستین و مهم‌ترین چالش پیش‌روی نظام عدالت کیفری در مواجهه با رمزارزها، ابهامات قانونی پیرامون پذیرش رمزارز به عنوان یک مال یا ابزار مالی و هم‌چنین ماهیت و شرایط فعالیت‌های مجاز حوزه رمزارز است؛ زیرا واکنش‌های انفعالی در برابر این چالش می‌تواند زمینه‌ساز مشکلات حقوقی و قضایی آتی و سرگردانی در انطباق مواد قانونی بر رفتار ارتکابی گردد.

۲- قانون‌گذاری در حوزه رمزارزها با استفاده از برشمردن معیارها و شرایط کلی و سپردن جزئیات به آیین‌نامه‌هایی که بنا بر اقتضا صادر می‌شوند، می‌تواند ضمن رسمیت بخشی به آن‌ها و تمیز خصایص و ماهیت حقوقی و شرایط فعالیت‌های قانونی در این رابطه، منجر به زدودن ابهامات و نظریات متفاوتی که در رویه قضایی شکل گرفته است، گردد. برای تشخیص ماهیت و معیارهای فعالیت قانونی در رابطه با رمزارزها نیازمند تحرکات تقنینی از سوی قانون‌گذاران از طریق تبیین صریح شرایط فنی و حقوقی اعتبار و رسمیت ارزها و فعالیت‌های مرتبط با آن‌ها هستیم که البته این امر می‌تواند از طریق صدور آیین‌نامه‌ها و مقررات مصوب و موسع قوانین عادی صورت پذیرد؛ هرچند پذیرفته باشیم لزوماً جرم‌انگاری خاصی برای رمزارزها ضرورت ندارد؛ زیرا ادبیات کنونی حقوق کیفری و جرم‌انگاری‌های عمومی و عناوینی که در قوانین جزایی از جمله قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاه‌برداری مصوب ۱۳۶۷ و قانون جرائم رایانه‌ای مصوب ۱۳۸۸ مورد توجه بوده است، در حال حاضر برای انطباق‌پذیری با اقدامات مجرمانه در این خصوص کافی به نظر می‌رسد.

۳- بخش قابل توجهی از چالش‌ها در حوزه رمزارزها، معطوف به بعد شکلی و فرایند رسیدگی و صدور و اجرای حکم است. انجام عملیات صحت‌سنجی تراکنش‌ها از طریق فرمول‌های ریاضی و الگوریتم‌های رمزنگاری در رمزارزها و محرمانه ماندن اطلاعات و هویت اشخاص، نظارت بر معاملات رمزارز که خارج از حیطه صرافی‌های داخلی و به صورت بین‌المللی انجام شده است را با مانع جدی مواجه می‌کند. هم‌چنین استفاده از حساب‌های کاربری گوناگون و آدرس‌های متعدد (کلید عمومی) فرایند کشف و ردیابی را بسیار پیچیده و در مواردی غیرممکن می‌سازد؛

بنابراین سـخـتی و پیچیدگی ردیابی و کشـف ادله در پرونده‌های رمزارزها رسیدگی به آن‌ها را با دشـواری مواجه می‌کند؛ در حالی‌که ساختار کنونی رسیدگی‌های قضایی متناسـب با این شرایط تجهیز نشده اسـت. از طرفی بحث توقیف و اجرای حکم در جرائم مرتبط با رمزارزها چالش عمده دیگر را تشـکیل می‌دهد. مسائلی نظیر توقیف یا مصادره دارایی‌های رمزنگاری شـده و وسایل و تجهیزات مورد استفاده مظنونین یا مجرمین و امکان انجام این اقدامات و سـازوکارها و نهاد مسؤول آن، محل چالش و اشکال جدی هستند. مسائلی چون رد مال و توقیف زمانی که موضوع آن رمزارز باشد با توجه به فقدان امکانات و زیرسـاخت‌های لازم چون کیف پول مختص دادگستری یـا متخصصینی که با نظارت آن‌ها انتقال دارایـی و یا فروش و تبدیل رمزارز به پول رایج انجام شود، ولو این‌که رسـیدگی به جرائم ارتکابی در زمینه رمزارزها و اصدار حکم میسـر باشد، اجرای آن‌ها را متعسر می‌نماید. در آخرین اقدامات صورت گرفته پیرامـون حوزه رمزارزها در کشـور مقرر گردید تا از ظرفیت کمیسـیون اصل نودم قانون اساسی برای ایجاد هماهنگی میان دستگاه‌های متولی اجرایی و نظارتی استفاده شـود که با دعوت از تمامی دسـتگاه‌ها و نهادهای مرتبط، همه ابعاد موضوع بررسی شـد و تشکیل کارگروه مشترک «رمزارزها» برای بررسی همه جانبه موضوع و تحلیل آسیب‌ها و فرصت‌ها و نیل به سندی جامع و واحد برای تنظیم قواعد و مقررات مرتبط در دستور کار قرار گرفت.

فهرست منابع

الف. فارسی

* اخوان، پیمـــان (۱۳۹۷)، **ارزهای دیجیتال؛ بیت کوین، بلاک‌چین و مفاهیم پایه**، تهران: نشر آتی‌نگر.

* چتین، پیر-لارنت و مک دوئل، جان و موســـت، سدریک و اسکات، پل آلن و ون در دوز دی ویلبویس، امیل (۱۳۹۵)، **پیشگیری از پول‌شویی و تامین مالی تروریسم؛ راهنمای عملی برای ناظران بانکی**، برگردان: مریم آقایی و محسن نوری، چاپ دوم، تهران: نشر تاش.

* ســـمیعی زنور، حسین و حبیب‌زاده، محمدجعفر و صابر، محمود (۱۳۹۵)، «**تحلیل جرم اخلال در نظام اقتصادی کشـــور از طریق قبول ســـپرده اشخاص در حقوق ایران**». آموزه‌های حقوق کیفری، شماره ۱۱، تابستان، ۲۷-۵۲.

* قربان وطن، داود و یاری، محســـن و شمسعلی‌نیا، سپیده (۱۳۹۸)، **ارز دیجیتال و کارکردهای آن**، چاپ نخست، تهران: امیران.

* جدمه‌یر، الجوشـــا و استیفتر، نیکلاس و کرومبولز، کاترینا و وایپل، ادگار (۱۳۹۷)، **بلاک‌ها و زنجیره‌هـــا مقدمه‌ای بر بیت کوین ارزهـــای دیجیتالی و مکانیزم‌های ســـازمان‌دهی آن‌ها**، برگردان: امید خیاط و ابوالفضل آدرسی، چاپ نخست، تهران: روزنه.

* خادمان، محمود و کوشـــا، ابوطالب و نوری، فاطمه (۱۴۰۰)، «**شناســـایی ماهیت حقوقی رمزارزها با تحلیل ســـاختاری آن‌ها در نظام حقوقی ایران**»، مجله حقوقی دادگستری، شماره ۱۱۵.

* دهقان، محمدحسین (۱۳۹۸)، **مبارزه با تامین مالی تروریسم**، چاپ نخست، تهران: پژوهشکده پولی و بانکی.

* اتوود، مـــارک (۱۳۹۷)، **توضیح بیت کوین توضیح بلاک‌چین**، برگردان: مرتضی شانی، تهران: شرکت چاپ و نشر بازرگانی.

* قائم‌مقامی، علی (۱۳۹۵)، **اســـتانداردهای بین‌المللی مبارزه با پولشویی و تامین مالی تروریسم**، چاپ نخست، تهران: نشر تاش.

* کمیلی، محمدرضا و دانشور ثانی، رضا و گرایلی، محمدباقر (۱۴۰۰)، «**ماهیت جرم**

اخلال در نظام اقتصادی کشـــور». مطالعات فقه اسلامی و مبانی حقوق، دوره ۱۵، شماره ٤۳.

* محسنی‌طیب، سید امیررضا (۱۳۹۹)، **تاثیر اف ای تی اف بر سیاست جنایی تامین مالی تروریسم**، چاپ نخست، تهران: مجد.

* مرادی قلعه، سهیلا (۱٤۰۱)، «**پولشویی از طریق ارزهای دیجیتال (تجزیه و تحلیل پدیده و اقدامات پیشـگیرانه مناسـب)**». تحقـیقات حـقوق قضایی، شماره ۵.

* نبوی، ســید مهدی و صابر، محمود (۱۳۹۹)، «**مطالعـــه تطبیقی چالش‌های نظام عدالت کیفری ایران در دادرســـی جرائم مرتبط با ارزهای مجازی**»، پژوهش‌های حقوق تطبیقی، دوره ۲٤، شماره ۱.

* نوری، مهدی و نواب‌پور، علی‌رضا (۱۳۹۷)، **مقدمه‌ای بر تنظیم‌گری رمزینه ارزها در اقتصاد ایران**، تهران: دفتر مطالعات اقتصادی مجلس شورای اسلامی.

ب. انگلیسی

* **Blockchain & Cryptocurrency Laws and Regulations, United Kingdom**, Available at: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/united-kingdom

* Bokovnya AY, Shutova AA, Zhukova TG, Ryabova LV (2020), **Legal measures for crimes in the field of cryptocurrency billing**, Utopía y Praxis Latinoamericana, 25(7).

* Chohan, Usman W. (2022), **Cryptocurrencies: A brief thematic review**, Economics of Networks Journal Available at: SSRN 3024330.

* **Digital assets: the AMF amends its General Regulation and updates its policy** (2021), Available at: ww.amf-france.org/en/news-publications/news/digital-assets-amf-amends-its-general-regulation-and-updates-its-policy

* Juan M. and Diehl Moreno (2023), **A general introduction to the regulation of virtual currencies in Argentina**, Marval OFarrell Mairal, Available at: https://www.lexology.com/library/

❋ Kethineni, Sesha; Ying Cao and Cassandra Dodge (2018), **Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes**, American Journal of Criminal Justice, 43.

❋ Latimer, Paul; Duffy, Michael (2019), **Deconstructing Digital Currency and Its Risks: Why ASIC Must Rise to the Regulatory Challenge**, Federal Law Review, Vol. 47(1).

❋ Rabenfeld, S. (2014), **Canada Enacts Bitcoin Regulation**, Risk and Compliance Journal, 2.

❋ Hays, D. and Kirilenko, A. (2021), **Cryptocurrency regulation and enforcement in the US and Europe**, Fostering FinTech for Financial Transformation, 26.

❋ Huang, Y., & Mayer, M. (2022). **Digital currencies, monetary sovereignty, and US–China power competition**. Policy & Internet, 14(2), 324-347.

❋ Christin, N. (2013), **Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace**, In Proceedings of the 22nd international conference on World Wide Web.

❋ Clements, R. and Torrie, V. (2023), **Crypto Asset Regulation in Canada: Developments and Governance Considerations**, Banking & Finance Law Review, 39(3).