

چالش‌های نظام عدالت کیفری ایران در مواجهه با رمزارزها و راهکارها

نرگس فرزانه کندی^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 دادگستری‌ها به زیرساخت‌های فنی مناسب و آموزش تخصصی قضات و کارشناسان این حوزه را در کنار آگاهی‌افزایی 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 جرم‌شناسی و بازپرس دادرسی جرایم رایانه‌ای

a_tuysserkani@yahoo.com

درآمد

امروزه فناوری‌های جدید و پیشرفته 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 سهولت 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^۱ ایجاد شده است. اصطلاحاتی مانند ارز دیجیتال، ارز مجازی، رمزارز، ارز رمز پایه، رمزینه ارز، ارز رمزنگاری شده و غیره در زبان فارسی به کار می‌روند که اغلب به اصطلاح کریپتوکارنسی^۲ در زبان انگلیسی ارجاع داده می‌شوند و به معنای پول یا ارزی است که بر پایه علوم رمزنگاری ایجاد شده و می‌تواند با استفاده از علم ریاضیات، کدهای رمزنگاری شده را ایجاد نماید تا اطلاعات پنهان بماند و کسی قادر نباشد در روند تولید، انتشار و انجام مبادلات خللی وارد آورد (خادمان و دیگران، ۱۴۰۰: ۳۵۱).

ارزهای دیجیتال بدون نیاز به بانک مرکزی برای صدور ارز و یا بان‌کهای خصوصی برای ذخیره ارز عمل می‌کنند. آن‌ها بر اساس یک قطعه و زنجیره کد شکل می‌گیرند که قابل تکرار نیستند. به عنوان جایگزینی برای ارزهای سنتی، ارزش این ارزها، مبتنی بر تعداد کاربرانی است که آماده پذیرش پرداخت برای کالاها و خدمات با استفاده از ارز دیجیتال هستند. ارزش آن‌ها هم‌چنین از تمایل مبادلات ارز دیجیتال برای تبدیل آن‌ها به ارزهای دیگر ناشی می‌شود. در حال حاضر بیش از هزاران نوع ارز دیجیتال مانند بیت‌کوین^۳، دش^۴، اتریوم^۵، ریپل^۶ و زی‌کش^۷ 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 سرمایه‌گذاری استفاده می‌شوند. این ارز جایگزینی برای استاندارد طلا و پول کلایی (کلایی اقتصادی که به جای پول استفاده می‌شود) بوده است.

2. Crypto Currency

3. Bitcoin

4. Dash

5. Ethereum

6. Ripple

7. Zcash

(Duffy, 2019: 122). برخی معتقدند باید میان اصطلاحات «ارز دیجیتال»، «ارز مجازی» و «رمازز» تفاوت قائل شد. ارزهای دیجیتال ارزیابی را شامل می‌شوند که به صورت الکترونیکی ذخیره و منتقل می‌شوند و هرگونه پولی که بر مبنای صفر و یک باشد در این تعریف می‌گنجد؛ اعم از این که مبنای آن پول سستی و بانکی و یا ارزهای مجازی باشد. در واقع ارز دیجیتال به هر ارزش ایجاد شده در بستر دیجیتال اطلاق می‌گردد. ارز مجازی از این جهت که غیر ملموس است نوعی ارز دیجیتال محسوب می‌شود و وجه تمایز آن این است که پول دیجیتال، نماینده اسکناس‌های بانکی است که فقط سازکار آن غیر فیزیکی شده است؛ در حالی که ارز مجازی ارتباطی با پول بانکی ندارد و یک ارز جدید با سازکار منحصر به فرد است (نوری و نواب‌پور، ۱۳۹۷: ۴) و در نهایت رمازز (یا ارز رمز پایه) را گونه‌ای پول دیجیتال معرفی نموده‌اند که در آن تولید واحد پول و تأیید اصالت تراکنش پول با بهره‌گیری از الگوریتم‌های رمزگذاری شده کنترل می‌شود (Chohan, 2022: 2).

ارزهای غیر قابل تبدیل هرگز امکان تبدیل 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 سازنده بازی آن را منتشر نموده است و دفترکل را نزد خود نگاه می‌دارد. لیکن ارزهای مجازی قابل تبدیل، امکان تبدیل به پول‌های حقیقی و به عکس را دارند و از آن برای خرید کالا و خدمات حقیقی و مجازی می‌توان استفاده نمود. این نوع ارز به دو دسته متمرکز و غیر متمرکز تقسیم می‌شود؛ در دسته متمرکز، انتشار و کنترل ارز توسط یک نهاد مرکزی صورت می‌پذیرد؛ اما در ارز مجازی غیر متمرکز تمامی فرایندها از جمله انتشار و تأیید تراکنش‌ها به جای این که توسط نهادی مرکزی صورت گیرد به وسیله تمامی افراد با سازوکارهای رمزنگاری انجام می‌گیرد (نوری و نواب‌پور، ۱۳۹۷: ۶-۵). در تعریف رمازز می‌توان گفت، نوعی پول دیجیتال و ارز مجازی به حساب می‌آید که با شیوه‌های فناوری رمزنگاری (الگوریتم‌های رمزگذاری) و اغلب به صورت غیر متمرکز (بدون وابستگی به یک نهاد مرکزی) ایجاد و اداره می‌شود.

با امعان نظر به چالش‌ها و مشکلاتی که رمازرها 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 مطرح 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. موضوع 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 این که 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 ۵۸۱۴۴/ت/۵۵۶۳۷ 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 پردازی رمزنگاری شده) صرفاً با قبول مسئولیت 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 فناوریانه مربوط به تولید و واردات تجهیزات پردازش رمزارزها (ماینینگ) را تدوین و ابلاغ نماید. شایان ذکر است که در سال ۱۴۰۱ هیأت وزیران آیین‌نامه استخراج رمزارزایی‌ها^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 آیین‌نامه 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 مسئولیت 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 ۱۴۰۱/۵/۱۱ شورای عالی فضای مجازی؛ شایان ذکر است با استناد به سند مذکور اخیراً نظام‌نامه رمزارز اعم از ایجاد رمزارز ملی و ساماندهی کاربری رمزارزهای جهان‌روا در یکصد و پنجاه و هفتمین جلسه مورخ ۱۴۰۳/۱۰/۱۹ کمیسیون عالی تنظیم مقررات فضای مجازی کشور به تصویب رسیده است.

۲. آیین‌نامه استخراج رمزارزایی‌ها شماره ۱۵۱۴۵۵ مورخ ۱۴۰۱/۸/۲۲ هیأت وزیران.

به رسمیت شناخته نشده است. به هر حال غیرمجاز دانستن استفاده از رمزارزها (مزید بر ابهامات قانونی در خصوص ماهیت و شرایط استفاده از آن‌ها) در مبادلات داخل کشور تبعات و چالش‌هایی را در پی داشته است از جمله این که چون معامله ارزهای دیجیتال بر اساس مقررات بانک مرکزی و تصویب‌نامه شماره ۵۸۱۴۴/ت/۵۵۶۳۷ هـ مورخ ۱۳۹۸/۵/۶ هیأت وزیران در مبادلات داخلی رسمیت ندارد، لذا توقیف و فروش آن به وسیله اجرای احکام ممکن دانسته نشده است و در حکم مالی دانسته می‌شود که به آن دسترسی نیست و با توجه به ملاک ماده ۴۶ قانون اجرای احکام مدنی مصوب ۱۳۵۶، قیمت آن به تراضی طرفین و در صورت عدم تراضی، بهای آن به قیمت یوم‌الادا به وسیله کارشناس و خبره محاسبه و از محکوم علیه وصول و به محکوم له پرداخت می‌شود.

شاید اولین و مهم‌ترین چالش برای نظام‌های حقوقی کنونی مواجهه با پذیرش رمزارز به عنوان یک مال یا ابزار مالی باشد زیرا واکنش انفعالی در قبال این چالش، منشأ مشکلات بعدی خواهد بود. اگرچه برخی چالش‌های پیرامون ارزهای دیجیتال از کشوری به کشور دیگر متفاوت است، اما برخی موضوعات مشترک وجود دارند. تأثیر ارزهای دیجیتال بر قوانین مبارزه با پول‌شویی^۱ و جرائم مالی، دغدغه‌های ناشی از احراز هویت مشتری^۲ و قوانین اوراق بهادار در اکثر کشورها حائز اهمیت است؛ با این حال، هر کشوری با توجه به سیاست‌ها و مصالح خود به شیوه‌ای متفاوت با این چالش‌ها مواجه می‌شود (Hays & Kirilenko, 2021: 107). آمریکا حدود سه دهه است که در خصوص مقررات‌گذاری رمزارزها به 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 حساب می‌آید. تفاوت‌هایی در بحث صدور مجوزها، نظارت و کنترل رمزارزها در ایالات مختلف این کشور وجود دارد (محسنی‌طیب، ۱۳۹۹: ۹۹). رمزارز در این کشور به عنوان یک دارایی و مشابه یک کالا با ارزش مالی پذیرفته شده است. ارزهای دیجیتال مانند بیت‌کوین مشمول قوانین اخذ مالیات می‌شود و دارندگان آن‌ها در اقسام مختلف، 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 رمازها برای پول‌شویی و فرار مالیاتی توجه شده است (اسکات و موس و وندرروز و لارنت‌چتین و مک‌دوئل، ۱۳۹۵: ۱۲۳).

از فرانسه به عنوان اولین کشوری یاد می‌شود که با استفاده از فناوری بلاک چین امکان ثبت و انتقال اوراق بهادار ثبت نشده را فراهم نموده است (Christin, 2013: 213-224). در فرانسه نیز رمازها مجاز دانسته شده‌اند اما ذیل محدودیت‌ها و تدابیر قوانین و مقررات قرار گرفته‌اند و مالیات برای معاملات مربوط به آن‌ها در نظر گرفته شده است. رماز پول شناخته نمی‌شود اما دارایی دیجیتال در نظر گرفته شده است (Digital Assets, 2021). کانادا رماز را به مثابه دارایی نامشهود شناخته است و رویکرد پذیرش رماز در این کشور وجود دارد لیکن برای جلوگیری از اثرات مخرب رمازها، قوانین پول‌شویی و ضدتروریستی متناسب با آن‌ها تصویب شده است (Rabenfeld, 2014: 2). برای کسب و کارهای خرید و فروش رماز و هم‌چنین سرمایه‌گذاری در رمازها، مالیات وضع می‌شود و صرافی‌های بیت‌کوین به عنوان کسب‌وکارهای خدمات پولی در نظر گرفته می‌شوند (قائم‌مقامی، ۱۳۹۵: ۶۶). تا کنون چارچوب‌های قانونی گسترده‌ای در کانادا برای تنظیم مقررات دارایی‌های دیجیتال وضع شده‌اند که ضوابط کنترلی متعدد، قوانین و رویه‌های قضایی راجع به تنظیم‌کنندگان اوراق بهادار، تصویب قوانین انتقال، تدابیر مبارزه با پول‌شویی و تأمین مالی تروریسم، مقررات مربوط به پرداخت‌ها، مالیات، برنامه‌ریزی املاک، و ضوابط زیست‌محیطی برای عملیات استخراج ارزهای دیجیتال، از جمله آن‌ها می‌باشند (Clements, & Torrie, 2023: 350). دولت استرالیا نیز رمازها را به رسمیت شناخته است؛ بیت‌کوین و سایر ارزهای دیجیتال در استرالیا قانونی هستند و به عنوان دارایی تلقی می‌شوند. هم‌چنین در چارچوب قانون مبارزه با پول‌شویی و نیز مقابله با تروریسم، ارزهای دیجیتال در محدوده سیستم ضد پول‌شویی و ضد تأمین مالی تروریسم در استرالیا قرار گرفته است (اخوان، ۱۳۹۷: ۹۹)؛ با این حال در برخی کشورها از قبیل چین و روسیه نگاه بدبینانه و محتاطانه نسبت به رمازها وجود داشته و در چارچوب سیاست تقنینی، محدودیت حداکثری در قبال آن‌ها

اتخاذ شده است (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 سرمایه‌گذاری مورد پذیرش قرار گرفته است. با وجود این، از خرید و فروش 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 شده‌اند؛ با این حال 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: ۶۹).

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

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

با توجه به ابهامات و تردیدهایی که پیرامون انطباق اعمال زیان‌بار حیطه رمزارزها با عناوین مجرمانه وجود دارد، نیاز است که شیوه‌های ارتکاب جرم در حوزه رمزارزها و اهم دعاوی در این ارتباط مورد تحلیل و ارزیابی قرار گیرد. شیوه‌های ارتکاب جرم در رابطه با رمزارزها را می‌توان 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 است؛ اما حالت سومی نیز قابل تأمل است و آن این‌که فعالیت مرتبط با رمزارز موضوع جرم باشد.

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

با توجه به قوانین کنونی در نظام حقوقی داخلی، عمده جرائمی که متوجه دارایی‌های رمزارز هستند، دسترسی غیرمجاز، جعل اطلاعات و داده‌ها، ممانعت از دسترسی و کلاهبرداری رایانه‌ای در قانون جرائم رایانه‌ای مصوب ۱۳۸۸ است. بنابراین هرگونه مداخله در کیف پول رمزارز و داده‌های مربوط به آن، که مصداقاً

قابل انطباق با اعمال مزبور در قانون جرائم رایانه‌ای باشد، تحت عنوان یکی از جرائم مندرج در این قانون قابل تعقیب و مجازات خواهد بود. نظریه مشورتی شماره ۱۶۲۳/۱۴۰۰/۷ مورخ ۱۴۰۱/۰۸/۲۳ اداره کل حقوقی قوه قضاییه درباره کلاهبرداری رایانه‌ای که مال موضوع جرم ارز دیجیتال باشد، چنین آورده است: «اولاً، با عنایت به مقررات مربوط از جمله ماده ۳۱۲ قانون مدنی و ماده ۷۴۱ قانون مجازات اسلامی (ماده ۱۳ قانون جرائم رایانه‌ای مصوب ۱۳۸۸)، معادل آنچه از کیف پول الکترونیکی برده شده است، باید به مال‌باخته مسترد شود؛ از آن‌جا که مال موضوع سوال مثلی تلقی می‌شود، دادگاه باید حکم به پرداخت ارز دیجیتال صادر کند و در صورت امتناع، با عنایت به این‌که معامله ارزهای دیجیتال بر اساس مقررات بانک مرکزی و تصویب‌نامه شماره ۵۸۱۴۴/ت/۵۵۶۳۷ هـ مورخ ۱۳۹۸/۵/۶ هیأت وزیران در مبادلات داخلی رسمیت ندارد، لذا توقیف و فروش آن به وسیله اجرای احکام ممکن نیست؛ بنابراین در حکم مالی است که به آن دسترسی نیست و با توجه به ملاک ماده ۴۶ قانون اجرای احکام مدنی مصوب ۱۳۵۶ قیمت آن به تراضی طرفین و در صورت عدم تراضی، بهای آن به قیمت یوم‌الادا به وسیله کارشناس و خبره محاسبه 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 انگاشتن فعلیتی به واسطه این‌که در خصوص رمزارز (استخراج، بهره‌برداری و یا داد و ستد) انجام شده است، با عنایت به ماده ۲ قانون مجازات اسلامی و اصل قانونی بودن 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، پول‌شویی، اخلال در نظام اقتصادی و ...) هر نوع فعلیتی را که از استخراج 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 برداشت اشتباهی باشد چرا که بیشتر رمزارزها و معروف‌ترین آن‌ها چنین هستند. در حقیقت رمزارزها دارای خصیصه تمرکززدایی بوده و با رویکرد حذف

حاکمیت و نظارت ایجاد شده‌اند 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 مشخص کند برای آن‌که بتوان رمزارز حقیقی و غیر حقیقی یا فعالیت درست را از فعالیت نادرست در عرصه رمزارزها بازشناسد. بر اساس روند متعارف ایجاد و استفاده از رمزارزها، یک‌سری خصوصیات کلی و معیارها وجود دارد؛ نظیر این‌که رمزارزها بر مبنای استخراج و بر پایه رمزنگاری ایجاد می‌شوند ولی همین موارد هم با توجه به تنوع رمزارزها و تحولات در عرصه فناوری ممکن است دستخوش نقض و تغییر گردند. مکانیسم مقابله حقوق کیفری با جرائم ارتكابی حوزه رمزارزها در مراحل اولیه توسعه قرار دارد؛ در این مسیر، رسمیت یافتن دارایی‌های دیجیتال و ارزش و اعتبار آن در قانون جهت حمایت از افراد و تعلق سایر حقوق و تکالیف قانونی بسیار مهم است. در وهله بعدی لازم است مشخص شود که در دکرین حقوق کیفری در فرایند ارتكاب جرم جایگاه رمزارزها به عنوان موضوع جرم یا وسیله ارتكاب آن کجا است (Bokovny et al, 2020: 272). در کل، دادگاه‌ها نمی‌توانند در خصوص رمزارزها جرم خاصی را در نظر بگیرند بلکه باید ضمن شناخت ماهیت و آگاهی کافی از ابعاد فعالیت‌های مرتبط با آن‌ها، ارکان سایر 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 استفاده 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 رسیدگی کیفری مرتبط با

رمزارزها

با توجه به این‌که استخراج غیرقانونی رمزارز با بهره‌برداری و معاملات رمزارزها و استفاده از آن‌ها، دو طیف متفاوت هستند، در ادامه ضمن تفکیک این دو مورد به بررسی اهم عناوین مجرمانه کیفری مرتبط با آن‌ها و تحلیل شرایط 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 قوه قضاییه به آن اشاره شده است، ملاک تحقق بزه موضوع ماده ۷۴۱ 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^۱ 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 مخفی کردن 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^۲ 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 حیل 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/ت/۶۲۲۹۸ هـ مورخ ۱۴۰۳/۴/۴ هیات وزیران به مبلغ مذکور تعدیل شده است.

۲. جزای نقدی مندرج در این ماده به موجب مصوبه شماره ۵۶۲۶۱/ت/۶۲۲۹۸ هـ مورخ ۱۴۰۳/۴/۴ هیات 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 رماز بر مبنای ادعای اشخاصی که اقدام به ایجاد و واگذاری آن می‌کنند نباشد از جمله این که در ظاهر، پلتفرمی در یک سایت معتبر تأسیس شده و افتتاح کیف پول الکترونیک و معاملات راجع به یک رماز جدید انجام می‌شود اما در واقع این رماز ادعایی بر اساس فناوری بلاک چین تولید نشده است و عملاً رمازری که در کیف پول قرار دارد امکان مبادله با سایر رمازها را نیز نداشته باشد و کسی که این رماز را خریداری کرده نه امکان تبدیل آن را داشته باشد نه امکان برداشت؛ 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 شده است. با در نظر گرفتن این که امروزه ساخت و ایجاد رماز برای اشخاصی که دانش و مهارت فنی در این زمینه را دارند کاری سهل و سریع محسوب می‌شود و این، نفس رماز نیست که مبنای ارزش آن قرار می‌گیرد بلکه اعتباری است که اعتماد و اقبال عمومی و پذیرش در جامعه برای رماز ایجاد می‌کند و اگر افراد اقدام به ایجاد کیف پول و خریداری این رماز جدید نمایند تا اینجا می‌توان گفت همه چیز بر اساس عرف و رویه تولید و ارائه رمازها صورت گرفته و فعالیت متقلبان‌های نیز انجام نگرفته است. اما اگر عرضه کنندگان رماز به منظور افزایش ارزش و اعتبار و رسیدن به نقطه سودآوری اقداماتی انجام دهند که مبنای درست و واقعی نداشته باشد (برای مثال ارزش رماز را در سایت دستکاری کنند و یا وعده‌ای داده شود مثل این که با خریداری هر واحد رماز روزانه میزان مشخصی سود پرداخت می‌شود) تا این که در نتیجه با استفاده از امور واهی و وسایل متقلبان‌ه گرایش به رماز جدید را در جامعه و میان افراد افزایش دهند، در این حالت گرچه طراحی و عرضه رماز جرم نیست اما روشی که برای ترغیب و تشویق افراد به خریداری آن استفاده شده توأم با بهره‌گیری از ابزارهای متقلبان‌ه و جعل واقعیت بوده است؛ 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 کشور جرائمی که موضوع اخلال در نظام اقتصادی می‌باشند در دو ماده احصا شده

است که با توجه به ماده ۲۸۶ قانون مجازات اسلامی مصوب ۱۳۹۲، ارتکاب این جرائم که منجر به اخلال در نظام اقتصادی کشور شود؛ به گونه‌ای که رفتار مرتکب اختلال شدید در نظم عمومی جامعه و ورود خسارت عمده به اموال عمومی و خصوصی را موجب شود، افساد فی الارض محسوب می‌گردد (کمیلی، دانشور و گرایلی، ۱۴۰۰: ۱۳).

قانون مجازات اخلال‌گران در نظام اقتصادی کشور مصادیقی را مطرح نموده است که با برخی از فعالیت‌های زیان‌بار در حوزه رمزارزها قابل انطباق به نظر می‌رسد و عملاً نیز برخی قضات در جرائم مرتبط با رمزارزها به آن متمایل شده‌اند. بر اساس ماده یک این قانون، ارتکاب اعمال مذکور در بندهای الف تا ز، به عنوان مصادیق اخلال در نظام اقتصادی مشمول مجازات‌های مقرر در قانون شناخته شده است. دو بند «ه» و «ز» این ماده با فعالیت‌های مجرمانه در زمینه رمزارزها ارتباط برقرار می‌نماید. قانون‌گذار در بند هـ «وصول وجوه کلان به صورت قبول سپرده اشخاص حقیقی یا حقوقی تحت عنوان مضاربه و نظایر آن که موجب حیف و میل اموال مردم یا اخلال در نظام اقتصادی شود»، را مطرح نموده است. باید دقت داشت که مستفاد از بند هـ ماده یک قانون مجازات اخلال‌گران در نظام اقتصادی کشور فرض است که شخص به صورت واقعی اموال مردم را تحت عنوان عقود صحیح به صورت سپرده قبول می‌کند ولی عملاً موجب حیف و میل این اموال می‌شود (سمیعی زنور و حبیب‌زاده و صابر، ۱۳۹۵: ۳۱)؛ اما در فرضی که با استفاده از وسایل متقلبانه و فریبنده و امور واهی، افراد جلب سرمایه‌گذاری می‌شوند، عنوانی که انطباق بیشتر و بهتری با فعالیت حوزه رمزارز می‌یابد عنوان کلاهبرداری است. بند ز ماده یک قانون مجازات اخلال‌گران در نظام اقتصادی کشور، در خصوص شرکت‌های هرمی مطرح شده است و مشخصاً یکی از شقوق فعالیت‌های مجرمانه در حوزه رمزارزها استفاده از طرح‌های پانزی و هرمی در چارچوب فعالیت‌های مرتبط با رمزارزها است و زمینه‌های قبلی (نظیر خرید سکه و ...) در حال منسوخ شدن است. برای مثال یک کوین به صورت غیرواقعی و مزورانه یا حتی به طور واقعی و در بستر بلاک‌چین ایجاد می‌شود و برای جلب اعتماد مردم به آن و ایجاد زمینه گرایش تصاعدی و گسترش شبکه، از قالب شرکت‌های هرمی یا گلدکوئیست استفاده می‌شود و به طور

مثال برای افرادی که بتوانند زیرشاخه 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 عین حال از چارچوب شیوه‌های هر می 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 سعی بر قانونی جلوه دادن آن‌ها تعریف می‌شود رمزارزها را با توجه به ماهیت و خصایص آن‌ها، بستری مناسب برای ارتکاب جرم پول‌شویی محسوب کرده‌اند (مرادی قلعه، ۱۴۰۱: ۱۷۱). افزایش سرعت تراکنش‌ها و خصوصیات آن‌ها، پیچیدگی نظارت را افزایش داده و ترکیب استفاده از رمزارزها با سایر روش‌های نوین و سنتی پول‌شویی، کشف و تعقیب این جرم را بسیار دشوار کرده است. در نظام حقوقی داخلی، ماده ۲ قانون مبارزه با پول‌شویی مصوب ۱۳۸۶ (اصلاحی ۱۳۹۷)، مفهوم و مصادیق پول‌شویی را مورد توجه قرار داده است که در این میان به ویژه بند ب این ماده می‌تواند با فعالیت‌های مجرمانه در حوزه رمزارزها قابل انطباق باشد. یکی از مشکلاتی که در نظام داخلی منجر به دامن زدن به بحث پول‌شویی از طریق فعالیت‌های رمزارز می‌شود، وجود بستر مناسبی به نام صرافی‌های آنلاین است که در کشور ما بر اساس مجوز پایه ثبت شرکت‌ها فعالیت می‌کنند اما مجوزی از مراجع ذی‌ربط مالی و بانکی ندارند و از طرفی ممنوعیتی هم برای فعالیت آن‌ها در قوانین مصوب منظور نشده است که این امر نظارت بر کار آن‌ها را با دشواری مواجه می‌نماید. در چنین شرایطی این صرافی است که باید حسن‌نیت خود را ثابت کند زیرا این صرافی‌ها باید ریسک معاملات خود را بپذیرند و احتیاط‌های لازم را به عمل آورند. در این زمینه استفاده از ملاک مواد ۵ و ۷ قانون مبارزه با پول‌شویی و الزاماتی که برای صرافی‌ها (در کنار سایر اشخاص موضوع قانون) می‌توان در نظر گرفت راهگشا خواهد بود. ضمن این‌که می‌توان به تبصره یک ماده ۹ قانون مبارزه با پول‌شویی نیز استناد جست از آن حیث که طبق این تبصره «چنانچه عواید حاصل

از جرم به اموال دیگری تبدیل یا تغییر یافته باشد همان اموال و در صورت انتقال به ثالث با حسن نیت، معادل آن از اموال مرتکب ضبط می شود؛ و مفهوم مخالف این مقرر این است که اگر ثالث حسن نیت نداشت می توان مال مزبور نزد او را نیز ضبط نمود؛ در نتیجه اگر صرافی آنلاین در انجام معامله حسن نیت نداشته باشد، هم می توان ریال پرداخت شده به صرافی را توقیف نمود و هم او را به اتهام پول شویی تحت پیگرد قرار داد.

۳. نگاهی انتقادی به رویه قضایی

در جهت تبیین بیشتر موضوع، در این قسمت صرفاً به معرفی دو پرونده مهم و کثیرالشاکی در حوزه حقوق کیفری رمزارز خواهیم پرداخت. پرونده نخست موسوم به کینگ مانی^۱ با بیش از دو هزار و یکصد نفر شاکی و هشت نفر متهم با عنوان مشارکت در کلاهبرداری شبکه ای منجر به اخلال در نظام اقتصادی کشور از طریق ایجاد رمزارز جعلی به اسم کینگ مانی و توزیع ارز جعلی بین مردم (سایر اتهامات به دلیل عدم ارتباط با حوزه رمزارز محل بحث نخواهد بود) و پرونده دوم موسوم به کریپتولند^۲ با بیش از بیست و شش هزار و پانصد نفر شاکی و هشت نفر متهم با عناوین تشکیل، سردهستگی و مشارکت شبکه سازمان یافته اخلال کلان در نظام اقتصادی (ارزی و پولی) کشور از طریق تصدی به عملیات صرافی غیرمجاز و معاملات غیرمجاز رمزارزی و همچنین مباشرت 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 سپرده های مردمی (سایر اتهامات به 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^۳.

رویکرد قضایی در این حوزه نشان دهنده چالش های ناشی از درک پیچیدگی های فنی رمزارزها و نوسان سیاست جنایی در انطباق صحیح فعالیت های مرتبط با این

1. King Money

2. Cryptoland

۳. دادنامه شماره ۱۴۰۳۶۸۳۹۰۰۰۳۲۳۹۸۹ مورخ ۱۴۰۳/۱/۲۱ صادره از شعبه دوم دادگاه انقلاب اسلامی تهران ویژه رسیدگی به جرائم اقتصادی؛ و دادنامه شماره ۱۴۰۲۶۸۳۹۰۰۱۱۸۴۲۹۱۹ مورخ ۱۴۰۲/۸/۹ صادره از شعبه پنجم دادگاه انقلاب اسلامی تهران ویژه رسیدگی به جرائم اقتصادی تهران.

حوزه با عناوین مجرمانه است. به عنوان نمونه، تأکید بر جعلی بودن رمزارز و صرافیه‌های ساختگی در آرای قضایی، با وجود متنفی بودن فرض جعل در مورد رمزارزها و احراز معیارهای فنی اولیه، بیانگر ضعف شناخت صحیح مفاهیم مرتبط در رویه قضایی است. 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.

افزون بر این، انتساب عنوان «اخلال کلان در نظام اقتصادی» به معاملات رمزارزی، با توجه به ضرورت تطابق عناصر قانونی این جرم با رفتارهای ارتكابی، یکی از نقاط چالش برانگیز در این آرا به شمار می‌رود. در کنار جرم اخلال در نظام اقتصادی، استناد به عناوینی نظیر کلاهبرداری و تحصیل مال از طریق نامشروع نیز با توجه به ملاحظات از جمله فقدان منع قانونی در خصوص معاملات رمزارزی، عدم امکان جرم‌انگاری صرفاً بر مبنای مصوبات دولتی، خروج رمزارزها از تعریف سنتی پول و ارز، عدم شمول قوانین حوزه پولی و ارزی بر رمزارزها، تشکیک در تحقق عنصر «بردن مال» در فرض وجود توکن‌ها^۱ و هم‌چنین ضرورت تفسیر مضیق در حقوق کیفری، با انتقادات جدی مواجه است.

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

۱. توکن‌ها (Token)، واحدهای رمزنگاری‌شده‌ای هستند که بر بستر فناوری بلاک‌چین ایجاد می‌شوند و می‌توانند نمایان‌گر دارایی، حق مالکیت یا دسترسی به یک خدمت دیجیتال باشند. در دنیای فناوری اطلاعات و به ویژه در حوزه رمزنگاری (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.

۴. 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 این گونه 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 جرائم 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.

۴-۱. 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 هیچ گونه 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 مشاهده تمامی تراکنش‌های رمازرها وجود دارد و نهادهای نظارتی و مجری قانون قادرند اقدام به رصد آن‌ها نمایند؛ اما مشکل اصلی چگونگی تعیین و تشخیص تراکنش‌های مشکوک در رمازرها و شناسایی طرفین آن است؛ زیرا هر تراکنش به یک کد رمزنگاری شده، که کلید عمومی خواننده می‌شود، متصل است و تنها راه ممکن جهت کشف هویت کاربران، استفاده از روش‌های پیچیده فنی تحلیل شبکه و استفاده از منابع اطلاعاتی است و امکان کشف جرائم مرتبط با آن‌ها بدون استفاده از شیوه‌های فنی پیشرفته وجود ندارد (Kethineni and Dodg, 2018: 145). علاوه بر این که باید در نظر داشت که اشخاص می‌توانند از آدرس‌های متعدد (کلید عمومی) استفاده کنند که فرایند کشف و ردیابی را بسیار پیچیده و غیرممکن می‌سازد. با توجه به این که میزان گمنامی اشخاص، بستگی به میزان مهارت آن‌ها در استفاده از روش‌ها و ابزارهای گمنام‌کننده مضاعف دارد، لذا کشف و شناسایی مجرمان حرفه‌ای به مراتب سخت‌تر و هزینه برتر از اشخاص عادی خواهد بود (نبوی و صابر، ۱۳۹۹: ۱۹۷).

به رغم پیچیدگی‌ها و موانعی که در این زمینه وجود دارد و با توجه به این که کشف و تعقیب جرائم مرتبط با حوزه رمازرها امری محال نیست و در بسیاری از موارد قابلیت پیگیری دارد، بنابراین نباید مانع رسیدگی تا حد امکان و بضاعت با بهره‌گیری از نیروی متخصص و کارآمد باشد؛ هم‌چنین باید موجب تدوین قوانینی گردد که ساماندهی معاملات بر رمازرها و امکان نظارت و کنترل بعدی آن‌ها به منظور تأمین حقوق شهروندان را فراهم آورد.

۴-۲. تحقیقات مقدماتی و مسائل مربوط به دادرسی

پیرامون دادرسی‌ها راجع به جرائم مرتبط با سامانه‌های رایانه‌ای و الکترونیکی و به ویژه بحث استفاده و بهره‌گیری از ادله الکترونیک، آیین دادرسی جرائم رایانه‌ای (مواد ۶۶۴ به بعد قانون آیین دادرسی کیفری) در کنار قانون تجارت الکترونیک، قانون جرائم رایانه‌ای و مقررات مربوطه به ویژه آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی، منابع قانونی قابل استفاده و تطبیق در رابطه با دادرسی پیرامون رمازرها نیز به شمار 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^۱ 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^۲.

باید افزود که ادله الکترونیک به ویژه در مورد رمزارزها، در معرض تغییر قرار دارند و به میزان قابل توجهی فرار هستند؛ کدهای مربوط به رمزارزها شامل تعدادی شماره هستند که میزان حجمی که در فضای مجازی اشغال می‌کنند بسیار ناچیز محسوب می‌شود، بنابراین به راحتی 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^۳ 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 صورتی که شخص مجرم دارای مهارت و تخصص بالایی باشد، می‌تواند با استفاده از نرم‌افزارهای خاص، در بازه‌های زمانی

۱. ماده ۱۱ قانون تجارت الکترونیک 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 ۳ 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».

مشخص 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 انتساب امضای الکترونیک گمنام به شخص متهم، لازم است اطلاعات جمع‌آوری شده مطابق با اصول کلی مربوط به دلیل و روش تحصیل آن در امور کیفری و هم‌چنین مطابق با استنادپذیری ادله الکترونیک باشد. این موضوع برای ضابطان قضایی و دیگر نهادهای مجری قانون حائز اهمیت است، زیرا باید از تدابیر فنی و روش‌های تخصصی برای کسب دلایل، نگهداری و ارائه آن‌ها در موارد لازم، استفاده گردد (همان: ۲۰۳).

ملاحظه شد که کارشناسان امور کیفری در حیطه رمازرها نظریات واحد و یکسانی راجع به کفایت قوانین شکلی و از جمله ادله دادرسی الکترونیک برای رسیدگی به جرائم رمازرها ندارند و برخی طی فرایند دادرسی ادله اثبات الکترونیکی را کافی می‌دانند و در این میان به قابلیت مواد ۶۶۴ به بعد آیین دادرسی کیفری بخش جرائم رایانه‌ای و به خصوص ظرفیت ماده ۶۷۱ به بعد (که بحث توقیف و تفتیش داده‌ها را مطرح ساخته است)، استناد می‌جویند و در مقابل برخی اعتقاد دارند که قواعد دادرسی در حوزه بلاک‌چین و رمازرها باید به طور کلی دگرگون شود. آنچه مسلم است این‌که بسیاری از مواد کنونی در رابطه با دادرسی و جمع‌آوری ادله الکترونیکی در فرایند تحقیقات و دادرسی کیفری پرونده‌های مرتبط با رمازرها قابل بهره‌گیری هستند و در عین حال در این زمینه با ملاحظه خصایص و ویژگی‌های رمازرها نیازمند بروزرسانی قوانین شکلی هستیم.

۴-۳. مشکلات پیرامون توقیف، مصادره و اجرای حکم

بحث توقیف و اجرای حکم در حیطه رمازرها از اهمیت بسیاری بالایی برخوردار است. در بسیاری از جرائم اعم از کلاهبرداری، پول‌شویی، اخلاف در نظام اقتصادی و تأمین مالی تروریسم و غیره، برای آن‌که پرونده به سرانجام برسد نیاز به توقیف یا مصادره دارایی‌ها از جمله رمازر و وسایل مرتبط سخت‌افزاری و نرم‌افزاری مرتبط با آن می‌باشد؛ برای مثال در خصوص کلاهبرداری رایانه‌ای و هم‌چنین کلاهبرداری سنتی، یا موارد توقیف در جرم پول‌شویی و مصادره مال (بر اساس ماده ۹ قانون مبارزه با پول‌شویی)، نیاز به توقیف یا مصادره رمازر بر اساس

سازوکاری مشخص با امعان نظر به ویژگی نامحسوس بودن و حریم خصوصی و امنیت مبادلات در بستر بلاک چین احساس می شود.

حال اگر دادیار یا بازپرس بخواهد در موردی که کلاهبرداری صورت گرفته است نسبت به توقیف رمزارز اقدام نماید با چالش های عدیده ای مواجه است؛ این که 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 توقیف شده به فروش برسد این معضل وجود دارد که چه سازوکاری برای فروش و یا انتقال رمزارز پیش بینی شده است؛ و این در حالی است که رمزارزها هنوز آن گونه که بایسته و شایسته است در نظام حقوقی مورد پذیرش قرار نگرفته و رسمیت نیافته اند. حال چگونه می توان 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 داشته اند که در بسیاری از موارد نیازمند استفاده از روش های منحصر به فردی برای رسیدگی به پرونده های رمزارز نظیر توقیف فوری گوشی متهم و بررسی داده های آن تا پیش از ایجاد تغییرات و امحای ادله و هم چنین 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 نه تنها از حیث حفظ حقوق طرفین دعوا و جلوگیری از تضییع اموال اهمیت دارد، بلکه در مواردی که مال توقیفی ماهیت غیرملموس یا فناورانه دارد، پیچیدگی های مضاعفی را نیز به همراه می آورد. در خصوص اموالی مانند داده های دیجیتالی، دارایی های مبتنی بر فناوری بلاک چین و به ویژه ارزهای مجازی، مسأله نگهداری و صیانت از مال توقیفی، با چالش های فنی، امنیتی و حقوقی قابل توجهی روبه روست. فقدان چارچوب های مدون قانونی، کمبود تخصص فنی در میان ضابطان و خطر بالای از بین رفتن، سرقت یا تغییر ارزش این نوع دارایی ها، عدم تطابق شیوه های 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، چالش های منحصر به فردی

به همراه دارد. در صورتی که ارز مجازی توقیف گردد، نگهداری آن دارای الزاماتی مخصوص به خود خواهد بود؛ اساساً ضابطان دادگستری باید ارز مجازی را به یک کیف پول دیجیتال متعلق به دادگستری و یا پلیس انتقال دهند تا در آن ذخیره شود؛ کیف پول متعلق به نهادهای قانونی و کلید خصوصی آن باید با استفاده از روش‌های فنی مورد حفاظت قرار گیرد تا سرقت نشود و از هرگونه دست‌کاری محفوظ باشد. بدیهی است با توجه به تنوع گسترده ارزهای مجازی و کیف پول‌های مجازی، نحوه انتخاب بهترین و امن‌ترین کیف پول باید توسط 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 مسائلی نظیر توقیف و مصادره و اجرای حکم ضمن استفاده از ظرفیت قوانین فعلی توأم با پذیرش و رسمیت یافتن رمازرها، نیازمند تحول و بروزرسانی در قوانین موجود هستیم زیرا ملاحظه مواد ۶۷۱ به بعد قانون آیین دادرسی کیفری در بخش جرائم رایانه‌ای و مسائل مطروحه در رابطه با تفتیش و توقیف داده‌ها، حاکی از آن است این مقررات علی‌رغم آن‌که می‌توانند در زمینه رسیدگی شکلی به پرونده‌های رمازرها قابل استفاده باشند اما در برخی زمینه‌ها نیز که پیشتر عرض شد با مقتضیات جرائم مرتبط با رمازرها هماهنگ و هم‌راستا به نظر نمی‌رسند و این امر توسعه قوانین و مقررات موجود در این خصوص را امری اجتناب‌ناپذیر می‌سازد.

برآمد

۱- نخستین و مهم‌ترین چالش پیش‌روی نظام عدالت کیفری در مواجهه با رمازرها، 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 ارتكابی 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 سختی و پیچیدگی ردیابی و کشف ادله در پرونده‌های رمزارزها رسیدگی به آن‌ها را با دشواری مواجه می‌کند؛ در حالی که ساختار کنونی رسیدگی‌های قضایی متناسب با این شرایط تجهیز نشده است. از طرفی بحث توقیف و اجرای حکم در جرائم مرتبط با رمزارزها چالش عمده دیگر را تشکیل می‌دهد. مسائلی نظیر توقیف یا مصادره دارایی‌های رمزنگاری شده و وسایل و تجهیزات مورد استفاده مظنونین یا مجرمین و امکان انجام این اقدامات و سازوکارها و نهاد مسئول 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 زیرساخت‌های لازم چون کیف پول مختص دادگستری یا متخصصینی که با نظارت آن‌ها انتقال دارایی و یا فروش و تبدیل رمزارز به پول رایج انجام شود، ولو این که رسیدگی به جرائم ارتكابی در زمینه رمزارزها و اصدار حکم میسر باشد، اجرای آن‌ها را متعسر می‌نماید. در آخرین اقدامات صورت گرفته پیرامون حوزه رمزارزها در کشور مقرر گردید تا از ظرفیت کمیسیون اصل نودم قانون اساسی برای ایجاد هماهنگی میان دستگاه‌های متولی اجرایی و نظارتی استفاده شود که با دعوت از تمامی دستگاه‌ها و نهادهای مرتبط، همه ابعاد موضوع بررسی شد 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، پیمان (۱۳۹۷)، ارزشهای دیجیتال؛ بیت کوین، بلاک چین و مفاهیم پایه، تهران: نشر آتی‌نگر.
- * چتین، پیر-لارنت و مک دونل، جان و موسست، سدريک 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.
- * سمیعی زنور، حسین و حبیب‌زاده، محمدجعفر و صابر، محمود (۱۳۹۵)، «تحلیل جرم اخلاص در نظام اقتصادی کشور از طریق قبول سپرده اشخاص در حقوق ایران». آموزه‌های حقوق کیفری، شماره ۱۱، تابستان، ۲۷-۵۲.
- * قربان وطن، داود و یاری، محسن و شمسعلی‌نیا، سپیده (۱۳۹۸)، ارزش دیجیتال و کارکردهای آن، چاپ نخست، تهران: امیران.
- * جدمه‌یر، الجوشا و استیفت، نیکلاس و کرومبولز، کاترینا و واپیل، ادگار (۱۳۹۷)، بلاک‌ها و زنجیره‌ها مقدمه‌ای بر بیت کوین ارزشهای دیجیتالی و مکانیزم‌های سازمان‌دهی آنها، برگردان: امید خیاط و ابوالفضل آدرسی، چاپ نخست، تهران: روزنه.
- * خادمان، محمود و کوشا، ابوطالب و نوری، فاطمه (۱۴۰۰)، «شناسایی ماهیت حقوقی رمزارزها با تحلیل ساختاری 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، مارک (۱۳۹۷)، توضیح بیت کوین توضیح بلاک‌چین، برگردان: مرتضی شانی، تهران: شرکت چاپ و نشر بازرگانی.
- * قائم‌مقامی، علی (۱۳۹۵)، استانداردهای 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 کشور». مطالعات فقه اسلامی و مبانى حقوق، دوره ۱۵، شماره ۴۳.

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

* مرادی قلعه، سهیلا (۱۴۰۱)، «پولشویی از طریق ارزهای دیجیتال (تجزیه و تحلیل پدیده و اقدامات پیشگیرانه مناسب)». تحقیقات حقوق قضایی، شماره ۵.

* نبوی، سید مهدی و صابر، محمود (۱۳۹۹)، «مطالعه تطبیقی چالش‌های نظام عدالت کیفری ایران در دادرسی جرائم مرتبط با ارزهای مجازی»، پژوهش‌های حقوق تطبیقی، دوره ۲۴، 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 O'Farrell 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).