Legal Studies in Cyberspace

مطالعات حقوقی فضای مجازی

Received: 2024/12/10
Accepted: 2025/04/15
Publish: 2025/09/09
Pages: 50-64

ISSN: 2821-126X
وبگاه مجله: https://sanad.iau.ir/journal/cyberlaw

Volume 4, Issue 14, Summer 2025
Article Type: **Research**
DOI: 10.71488/cyberlaw.2025.1217497

Assessing the Feasibility of Penal Sanctions for Digital Currency

Sadegh Khezri-Nia
Department of Criminal Law and Criminology, Cha.C., Islamic Azad University, Chalus, Iran
Jafar Koosha
Associate Professor of Criminal Law and Criminology, Shahid Beheshti University, Tehran, Iran (Corresponding Author). Email: jkoosha@yahoo.com
Parviz Zakaiyan
Department of Jurisprudence and Law, Cha.C., Islamic Azad University, Chalus, Iran

Abstract
The possibility or impossibility of criminalizing and attributing criminal liability to activities arising from digital currencies is accompanied by significant challenges. Users frequently resort to such currencies for various purposes, including tax evasion, and, given the difficulty of tracing these currencies, they provide a platform for crimes such as money laundering, tax evasion, and related offenses. Within the Iranian criminal justice system, various regulations and circulars have been issued to criminalize and penalize activities associated with digital currencies, one of which is the resolution of banks and financial institutions prohibiting any use, purchase, or sale of Bitcoin and other digital currencies within banks, licensed financial institutions, and exchange offices authorized by the Central Bank. Although this prohibition existed previously, no formal directive had been issued; consequently, any attempt to introduce criminalization and penal measures must consider both the risks arising from the lack of regulatory frameworks for digital currencies and, simultaneously, their rapid domestic and international expansion and the serious threats they pose to internal and international security through the financing of terrorist and sabotage groups. From a security-oriented criminal policy perspective, it appears feasible to criminalize and penalize threatening activities in this domain. Moreover, the confiscation and forfeiture of assets obtained through such means in favor of the state may serve as an optimal approach. The findings of this research, conducted through a library-based method and note-taking tools, underscore this conclusion as a key scientific contribution of the study.

Keywords: Digital Currency, Penalization, Differentiated Criminal Policy, Economic Crimes, Criminalization

❋Citation (APA): Khezri-Nia, S.; Koosha, J.; Zakaiyan, P. (2025). Assessing the Feasibility of Penal Sanctions for Digital Currency. *Cyberspace legal studies, 4(14), 50-64.*

مطالعات حقوقی فضای مجازی
Legal Studies in Cyberspace
ISSN: 2821-126X
ویگاه مجله: https://sanad.iau.ir/journal/cyberlaw
تاریخ دریافت: ۱۴۰۳/۰۹/۲۰
تاریخ پذیرش: ۱۴۰۴/۰۱/۲۶
تاریخ انتشار: ۱۴۰۴/۰۶/۱۸
صفحه: ۵۰ الی ۶۴
دوره ۴ / شماره ۱۴ / تابستان ۱۴۰۴
نوع مقاله: پژوهشی
DOI: 10.71488/cyberlaw.2025.1217497

امکان‌سنجی کیفرگذاری در قبال ارز دیجیتال

صادق خضری‌نیا
گروه حقوق جزا و جرم شناسی، واحد چالوس، دانشگاه آزاد اسلامی، چالوس، ایران
جعفر کوشا
دانشیار حقوق جزا و جرم شناسی، دانشگاه شهید بهشتی، تهران، ایران
(نویسنده مسئول) پست الکترونیک: jkoosha@yahoo.com
پرویز ذکائیان
گروه فقه و حقوق ، واحد چالوس، دانشگاه آزاد اسلامی، چالوس، ایران

چکیده

امکان یا عدم امکان جرم‌انگاری و القای وصف جرایم کیفری به فعالیت‌های ناشی از ارز دیجیتال با چالش‌های زیادی همراه می‌باشد. معمولاً کاربران این‌گونه ارزها را برای موارد متعددی از جمله فرار مالیاتی استفاده می‌نمایند و به دلیل اینکه این‌گونه ارزها قابل پیگیری نمی‌باشد، بستری است برای جرایمی از جمله پولشویی و فرار مالیاتی و مانند آن. در نظام کیفری ایران مقررات و اطلاعیه‌های مختلفی در جهت جرم‌انگاری و کیفرگذاری در خصوص ارزهای دیجیتالی صادر شده است که یکی از آنها مصوبه‌ی بانک‌ها و مؤسسات مالی است. طبق این اطلاعیه، هرگونه استفاده و خرید و فروش بیت‌کوین و سایر ارزهای دیجیتال در بانک‌ها، مؤسسات مالی و صرافی‌های دارای مجوز بانک مرکزی رسماً ممنوع اعلام شد. این ممنوعیت از گذشته نیز وجود داشت، اما برای آن بخشنامه رسمی صادر نشده بود، که اگر بخواهیم برای این موضوع جرم‌انگاری و کیفرگذاری نماییم، با توجه به مخاطرات ناشی از عدم قاعده‌مندی ارزهای دیجیتال از یک سو و گسترش روزافزون آنها در سطح داخلی و بین‌المللی از سوی دیگر و تهدید جدی امنیت داخلی و بین‌المللی از طریق تأمین گروه‌های تروریستی و خرابکاری، با مراجعه به یک سیاست جنایی امنیت‌گرا، می‌توان اقدامات تهدیدآمیز در این حوزه را جرم‌انگاری و کیفرگذاری نمود. به نظر می‌رسد رد و مصادره اموالی که از این طریق کسب می‌شود به نفع دولت می‌تواند بهترین گزینه باشد، که یافته‌های مقاله بطور اجمالی با روش کتابخانه‌ای با ابزار فیش‌برداری موضوع مورد بررسی قرار گرفته و نهایتاًرا می‌توان از یافته‌های علمی این پژوهش دانست.

واژگان کلیدی: ارز دیجیتال، کیفرگذاری، سیاست کیفری افتراقی، جرایم اقتصادی، جرم‌انگاری

❋ استناددهی (APA): خضری‌نیا، صادق؛ کوشا، جعفر؛ ذکائیان، پرویز؛ (۱۴۰۴). امکان‌سنجی کیفرگذاری در قبال ارز دیجیتال. *مطالعات حقوقی فضای مجازی*، ۴(۱۴)، ۶۴-۵۰.

مقدمه

از آغاز تاکنون، پول به عنوان یکی از ابزارهای اصلی در معاملات و مبادلات به کار می‌رود و سیر تکوینی آن از پول‌های کالایی شروع شده است و تا تولید سکه‌های فلزی، اسکناس‌های کاغذی با پشتوانه طلا و بدون پشتوانه ادامه یافت. در حال حاضر نسل جدیدی از پول در بستر اینترنت ایجاد شده است تحت عنوان ارزهای دیجیتالی، که به وسیله فناوری‌های نوین مبادله می‌شود. دعاوی مربوط به ارزهای دیجیتالی در دسته جرائم ارزهای دیجیتالی و رایانه‌ای قرار گرفته است. ارز دیجیتالی مصادیق مختلفی مانند بیت‌کوین، نانو، لایت‌کوین و... را در برمی‌گیرد و با پول سنتی متفاوت است. به عنوان نمونه، برای ایجاد ارزهای دیجیتالی، شاهد انحصار خلق پول در دست یک شخص یا گروه خاصی نیستیم، بلکه هر فرد با استفاده از یک روش مشخصی می‌تواند ارزهای دیجیتالی را تولید کند. برخلاف پول‌ها و ارزهای واقعی، ارزهای دیجیتالی در تعداد محدودی از کشورهای جهان به صورت قانونی به رسمیت شناخته شده است و تحت حمایت آنها قرار دارد در حالیکه در بسیاری از کشورها هنوز این ارزها به رسمیت شناخته نشده‌اند؛ به همین دلیل جرائم مربوط به این ارزها روز به روز در حال افزایش است.

ارزدیجیتالی به دو بخش تقسیم می‌شود: ۱. ارزهای دیجیتالی قابل تبدیل؛ ۲. ارزهای دیجیتالی غیرقابل تبدیل. ارزهای دیجیتالی قابل تبدیل، قابلیت تبدیل شدن به پول‌ها و ارزهای واقعی را دارند، بنابراین از این‌گونه ارزهای برای خرید کالاها، خدمات حقیقی و یا مجازی استفاده می‌شوند. ارزهای دیجیتالی قابل تبدیل به دو قسمت متمرکز و غیر متمرکز تقسیم می‌شوند. انتشار پول و همچنین کنترل آن در ارزهای دیجیتالی متمرکز برعهده نهادی مرکزی قرار دارد که آزادی[۱]، ذخیره[۲]و... نمونه‌هایی از این ارزها هستند. ولی در ارزهای دیجیتالی قابل تبدیل غیرمتمرکز، برخلاف ارزهای متمرکز تمامی فرایندهای مربوط به آنها از جمله، انتشار ارزها، گزارش تراکنش‌ها و... توسط خود افراد از طریق رمزنگاری صورت می‌گیرد. که لایت‌کوین و بیت‌کوین نمونه‌های از این‌گونه ارزها هستند.

علاوه بر اینها، ذکر این نکته خالی از اهمیت نیست که بیان شود به دلیل غیرقابل پیگیری بودن ارزهای دیجیتالی در بسیاری از موارد، امکان رهگیری و آمار و ارقام درست و دقیقی از آن در دست نیست و همین امر سبب می‌شود در مقوله‌ی قانونگذاری، قانونگذار نتواند به درستی قانونگذاری نماید که برای قابل پیگیری بودن ارزهای دیجیتال و فعالیت‌هایی در این زمینه، راههای مختلفی وجود دارد که یکی از آنها، داد و ستد ارزهای دیجیتالی در غالب قراردادهایی مشخص و معین است که عموماً اشخاص از این راهها استفاده نمی‌کنند، چرا که ارزهای دیجیتالی را وسیله‌ای در جهت پولشویی و فرار مالیاتی قرار می‌دهند و همانگونه که در مقررات پارلمان و شورای اروپا و در بند ۴ به آن اشاره شده، خلاء قانونی (بجز مقررات راجع به پولشویی) می‌تواند تهدیدی علیه دارایی‌های اعضا شده و و آنها را از این فرصت جهت جایگزینی در مبادلات و خلق سرمایه‌های جدید بی‌بهره سازد. با توجه به موارد فوق پرسش اصلی تحقیق پیش‌رو از امکان‌سنجی کیفرگذاری در خصوص جرایم مرتبط با ارزهای دیجیتال می‌باشد و فرضیه تحقیق امکان جرم‌انگاری و کیفرگذاری براساس مراجعه به سیاست کیفری مبتنی بر امنیت و نظم عمومی می‌باشد. مطالب پژوهش نیز در دو بخش ارائه شده است: در بخش اول به شناسایی مصادیق جرایم نوظهور و توسعه یافته در پهنه بارزهای دیجیتالی پرداخته شد و موضوع بخش دوم نیز بررسی امکان-سنجی جرم‌انگاری و بکارگیری سیاست کیفری افتراقی در زمینه جرایم مربوط به ارزهای دیجیتالی می‌باشد.

۱. مصادیق جرایم نوظهور و مرتبط با فعالیت‌های ارزهای دیجیتالی

۱. Liberty

۲. Reserve

ارزهای دیجیتال توانسته‌اند نوآوری‌های چشمگیری در سیستم‌های برداشت به وجود بیاورند و منافع چنین نوآوری‌هایی بسیار فراتر از نقاط ضعف احتمالی آن‌هاست (David LEE Kuo Chuen, 2015, 285). با توجه به روند رو به رشد جرایم مرتبط با ارزهای دیجیتال و استفاده تبهکاران بین المللی از این فرصت[1]، ضرورت داشت که قانونگذار در خصوص این حوزه، رویکردی افتراقی و سخت‌گیرانه اتخاذ نماید. علی رغم اهمیت موضوع و حیاتی بودن آن در برخی موارد (همانند تامین مالی گروه‌های تروریستی) قانون-گذار موضوع را به سکوت واگذار نموده است. حال در این قسمت تلاش می‌شود تا جرایم مرتبط به ارزهای دیجیتال مورد بررسی قرار گیرد:

۱-۱. پولشویی در خلال ارز دیجیتالی

یکی از بهترین روش‌های ارتکاب جرم پولشویی، استفاده از بیت کوین و سایر ارزهای دیجیتال در مبادلات می باشد (فراتی و همکاران، ۱۳۹۸: ۵۶). چرا که گمنامی و عدم لزوم احراز هویت کاربران در بسیاری از صرافی‌ها (خصوصا صرافی های خارجی)، مجرمین را بر آن داشته تا برای تطهیر عواید ناشی از ارتکاب جرایم از طریق ارزهای دیجیتال اقدام کنند. بدین نحو که اموال تحصیل شده از طرق نامشروع، صرف خرید بیت کوین و هزاران ارز دیگر و در نهایت انتقال آن به شخص ثالث و یا مبادلات تجاری می‌شود. تعریفی که در خصوص پولشویی با ارز دیجیتال ارائه می‌گردد این هست که در این روش پول نقد به صورت غیرقانونی به دست آمده و به صورتی رد این پول را دچار تغییر می‌کنند تا مثلاً به نظر آید که از روش مجازی کسب شده است. امروزه قانونگذاران بیش از بیش نگران مجرمان و فعالیت آنها می‌باشند که از ارز دیجیتال برای فعالیت‌های غیرمجاز خود مثل پولشویی، تأمین مالی تروریسم و فرار مالیاتی استفاده می-کنند.

یکی از دلایل پولشویی در بیت‌کوین، گمنامی شخص صاحب حساب در حساب‌های ارزهای دیجتالی است و مکانیزم آن به این صورت است که در هر تراکنشی، نشانی فرستنده و گیرنده بیت‌کوین ثبت می‌شود (غلام‌پور، ۱۴۰۲: ۶۵) که این نشانی متعلق به فرد هست و برای به‌دست آوردن اطلاعات نیازی به ارائه‌ی هویت فرد نیست. بنابراین هر فردی به راحتی می‌تواند برای انجام تراکنش‌های خود، به کمک یکی از برنامه‌های کیف پول یک یا چندین نشانی به دست بیاورد و با این حساب‌ها اقدام به مبادله‌ی بیت‌کوین کند؛ و تنها زمانی هویت فردی مشخص می‌گردد که آن فرد در صرافی‌ها اقدام به مبادله‌ی بیت‌کوین‌ها کرده باشد یا یکی از طرف‌های معامله هویت آن فرد را درخواست کند. در غیر این‌صورت فرد می‌تواند در هر معامله‌ای شرکت کند، بدون اینکه هویتش مشخص شود (خردمند، ۱۳۹۸: ۱۲۶). بنابراین اگر صرافی‌ها در مبادلات بیت‌کوین براساس قانون عمل نکنند و از روش‌های ضدپولشویی استفاده نکنند و همچنین در حین مبادله‌ی بیت‌کوین هویت افراد را شناسایی نکنند، می‌توان از طریق این صرافی‌ها، برای تمیز کردن بیت‌کوین-های کثیف و غیرقانونی استفاده کرد (وایزی و جمشیدی، ۱۳۹۶: ۱۰۲). که در چنین مواردی ممکن است در صورت تبانی فرد با صرافی، موضوع مشارکت در جرم نیز مطرح شود. ممکن است فرد از هویت مجعول و یا مدارک دیگری برای احراز هویت و ایجاد حساب کاربری استفاده کرده باشد که در اینجا مسئولیت صرافی صرفا نسبت به تخلفات صورت گرفته در خصوص نقض مقررات می-باشد.

علاوه بر بیت‌کوین‌ها، در سایر ارزهای دیجیتالی هم مانند بیت‌کوین کَش، اتریوم، ریپل و... امکان پولشویی وجود دارد. مثلاً در معاملات ارزهای دیجیتالی مونرو، زی‌کش و دَش امکان ردگیری هویت افراد وجود ندارد (حسینی و دعائی، ۱۳۹۳: ۸۷). در بیت‌کوین، علاوه بر ویژگی گمنامی آن برای ایجاد امکان پولشویی، سرویس‌های رد اثر در بیت‌کوین نیز پولشویی انجام می‌دهند. این سرویس‌ها از طریق انتقال بیت‌کوین‌ها بین آدرس‌های گوناگون، آنها را تمیز می‌کنند. این‌گونه سرویس‌ها هزینه‌بر هم هستند و معمولاً ۱ تا۳ درصد از ارز

---

۱ – از این رو است که کارگروه ویژه اقدام مالی در چارچوب توجه به ریسک های مجرمانه در ارتباط با پولشویی، با نگاهی ویژه به حوزه فن آوری های نوظهور تلاش کرده است تا به پوشش آن ها در چارچوب رویکرد ریسک مدار بپردازد (خلیلی پاچی و نیازپور، ۱۴۰۰: ۱۷۷).

دیجیتالی را که رد اثر می‌کنند، هزینه‌هایی در بر دارد و همچنین استفاده از این سرویس‌ها از ریسک بالایی برخوردار است (میرزاخانی و سعدی، ۱۳۹۷: ۷۳). در کنار همه خطرات و سختی‌های موجود در این روش، همچنان بواسطه دشواری در رهگیری و شناسایی، می تواند بستر مطلوبی برای مرتکبان پولشویی محسوب شود.

در عین حال از آنجایی که تمامی تراکنش‌های ارز دیجیتال در دفتر حساب توزیع‌شده ثبت می‌شوند و همچنین به دلیل وجود فرآیند شناسایی کاربر و وجود روش‌های پیشرفته برای ردگیری مجرم روی بستر رمز ارزها، با وجود آنکه بیشتر رمزارزها شبه‌گمنام یا گمنام هستند و هویت افراد به نشانی حسابشان متصل نشده و همچنین به‌دلیل این که همه‌ی صرافی‌ها براساس مقررات عمل نمی‌کنند و وجود سرویس‌های رد اثر، می‌توان ادعا کرد به لطف بلاک چین، ارزهای رمزنگاری شده در مقایسه با پول‌های واقعی به طور کل ظرفیت کم‌تری برای پولشویی دارند. اما همچنان از طریق رمز ارزها پولشویی انجام می‌شود که به بدنبال قوانین سفت و سختی در جهت پیشگیری از آن می‌باشیم (رجبی، ۱۳۹۷: ۸۹). بنابراین ضرورت دارد هم در زمینه پیشگیری از طریق وضع مقررات و قاعده‌مند نمودن فعالیت در این بستر و هم در زمینه رصد مستمر این فضا و کشف فعالیت‌های مجرمانه از طریق رسمیت شناسی[۱]، تدابیر لازم اتخاذ شود. چرا که ماهیت دارای ریسک رمز ارزها، نقش مؤثری در شکل‌گیری این نوع از جرم‌انگاری داشته باشد و قانون‌گذار با انتخاب راهبرد پیش‌دستی اقدام به توسعه قلمرو مداخله کیفری کند (خلیلی پاچی و شاملو، ۱۴۰۰: ۳۳). در واقع حوزه رمز ارزها می-تواند یکی از موارد جرم‌انگاری پیش‌دستانه باشد.

۱-۲. کلاهبرداری از طریق ارزهای دیجیتالی

انواع کلاهبرداری ارز دیجیتال به شرح زیر می‌باشد:
به دلیل گستردگی فضای دیجیتال، روش‌های بسیار زیادی برای کلاهبرداری از افراد وجود دارد که عبارتند از:

الف: طرح پانزی، هرمی و شبکه‌ای:

کلاهبرداری به روش پانزی با اندکی تفاوت، همان روش قدیمی بازاریابی شبکه‌ای یا هرمی است. در این روش، فرد با نشان دادن دستگاه‌های استخراج رمز ارز و یا نشان دادن کیف پول دیجیتال خود و موجودی آن، افراد را به سرمایه‌گذاری برای استخراج یا خرید رمز ارز تشویق می‌کند. پرداخت سود معمولاً در این روش منوط به ورود افراد جدید و آشنایان و بستگان فرد خواهد بود. سودی به عنوان سود تضمینی در این طرح‌ها در نظر گرفته می‌شود که غالباً وسوسه‌کننده بوده و فرد با وعده سرمایه‌گذاری در بورس‌های بزرگ دنیا و خرید رمزارزهای معروف، اقدام به معرفی افراد جدید به این مجموعه می‌کند. با ورود افراد جدید، سود افراد قدیمی‌تر با استفاده از سرمایه ورودی جدید پرداخت می‌شود. این کار تا جایی ادامه دارد که کلاهبردار به حد معینی از اموال دست یابد و امکان حفظ شبکه برای کسب سود بیشتر وجود نداشته باشد. باید توجه داشت که گاهی ممکن است در این نوع از کلاهبرداری، اجناسی نیز به عنوان بازاریابی برای فروش در اختیار اعضا قرار بگیرد (نواب‌پور و همکاران، ۱۳۹۷: ۳۲). مرز میان کلاهبرداری عادی و کلاهبرداری از طریق ارز دیجیتال در این روش ظریف می‌باشد، چرا که در مقام عمل و قضاوت فعالیت‌هایی این‌گونه را که نوعی وسیله متقلبانه محسوب می‌شود را کلاهبرداری از طریق بازاریابی شبکه‌ای ناسالم محسوب می‌کنند. آنچه که این شیوه را متمایز می‌سازد، سودهای کلان ناشی از رشد ناگهانی می‌باشد که معمولاً افراد را سریعتر جذب و منافع قابل توجهی را نصیب افراد مشخصی می نماید.

ب: استخراج ابری[۲]:

---

[۱]. رسمیت بخشیدن به ارزهای دیجیتال و تقنین آنها می‌تواند نقش مهمی در پیشگیری از جرایم مالی داشته باشد. این اقدام با قرار دادن زیرساخت‌های قانونی و پذیرش ارزهای دیجیتال همانند بیت‌کوین در حوزه حقوق عمومی، به شفافیت و جلوگیری از فعالیت‌های زیرزمینی یاری می‌رساند. این امر می‌تواند به تشخیص و مبارزه با جرایم مالی کمک کرده و از انتفاع مجرمانه غیرقانونی جلوگیری کند (Boehm, Pesch, 2014, 8438).

[۲]. cloud mining

این نوع استخراج از هر نظر ریسکی می‌باشد که فرد از طریق یک سیستم ساده عضو یک استخر دیجیتالی شده که به شکل پورسانتی کار می‌کند، ولی در نهایت فرد محکوم به شکست است. در مورد این نوع استخراج در اینترنت ملی و بین‌المللی هشدارهای زیادی داده شده است؛ پس اگر فرد ورود کند از قبل به ایشان اطلاع‌رسانی شده است (محمودی، ۱۳۹۸: ۵۱۰). با وجود آگاهی قبلی و احیاناً پذیرش خطرات احتمالی، نمی‌توان مسئولیت مرتکب را در چنین مواردی منتفی دانست. چرا که در چنین مواردی جنبه عمومی جرم و خطرات این اقدام برای اقتصاد و مبادلات تجاری همچنان مبنای تعقیب خواهد بود.

تب استخراج رمز ارزها در کشورمان به دلیل انرژی ارزان قیمت بسیار داغ است. اما در بسیاری از موارد، افراد با تبلیغاتی مواجه می‌شوند که بدون نیاز به دستگاه، اقدام به استخراج کنند. در این نوع کلاهبرداری معمولاً با این عناوین تبلیغاتی مواجه می‌شوید: «استخراج ابری»، «استخراج بدون دستگاه درآمد میلیونی از استخراج بیت کوین»، اجاره دستگاه استخراج در این روش معمولاً فرد در یک سایت و یا ربات تلگرامی ثبت‌نام کرده و با هدف سرمایه‌گذاری در استخراج رمز ارز، اقدام به پرداخت می‌کند (نواب‌پور و همکاران، ۱۳۹۷: ۱۲).

در واقع در این روش شما بدون این که نیاز به خرید دستگاه استخراج داشته باشید، قدرت استخراج و محاسبه را از یک مزرعه استخراج رمز ارز خریداری یا اجاره می‌کنید. به دلیل گران بودن دستگاه‌های استخراج، فرد تهییج می‌شود تا با سرمایه‌گذاری مشترک دست به استخراج بزند. اما در واقع خبری از استخراج نیست. یعنی شما تصور می‌کنید که بابت اجاره قدرت پردازش و استخراج پول می‌دهید، اما در واقعیت چنین چیزی وجود خارجی نداشته و این پرداخت، بازگشتی نخواهد داشت.

در این روش شرکت‌ها برای برداشت شما سقف خاص از سرمایه‌گذاری را تعیین می‌کنند و تا به آن میزان نرسید، امکان برداشت سود برای شما ممکن نیست. مثلاً کف سرمایه لازم برای برداشت، ۵۰ میلیون تومان بوده و شما حساب کاربری خود را ۵ میلیون تومان شارژ می‌کنید. در حساب کاربری خود مدام مشاهد می‌کنید که مثلاً برای همان ۵ میلیون تومان، ماهانه ۲ میلیون تومان حساب شما شارژ شده است. اما امکان برداشت ندارید. طبیعتاً تهییج خواهید شد تا ۵ میلیون را به ۵۰ میلیون برسانید تا از سودهای سرشار منتفع شوید. درحالی‌که تمام این امور فریبی بیش نیست. البته در این نوع کلاهبرداری نیز ممکن است به شکل ترکیبی از روش هرمی استفاده شود و مبالغ اندکی به فرد پرداخت شود. اما غالباً پرداخت‌ها تا زمان برداشت ادامه دارد و در هنگام برداشت، فرد مکلف به خرید از ربات شده و یا ربات به شکلی کاملاً از پیش تعیین‌شده دچار خطا می‌شود تا عدم برداشت از ربات کاملاً عادی جلوه کند. این در حالی است که اصلاً قرار نیست پرداختی صورت بگیرد (میرزاخانی و سعدی، ۱۳۹۷: ۷۸). در چنین مواردی فعالت گسترده در فضای مجازی و جلب نظر افراد زیاد به سرمایه‌گذاری در چنین فعالیت‌هایی منجر به ایجاد مخاطرات اجتماعی و امنیتی خواهد شد و معمولاً مالباختگان چنین پروژه‌هایی با تجمع و اعتراض، تعقیب جرم را مطالبه نموده و عدم نظارت مسئولین را علت جرم می‌دانند. بنابراین سلب امنیت و آسایش عمومی وجه افتراقی جرم در چنین مواردی نسبت به جرم کلاهبرداری ساده و در فضای حقیقی می‌باشد.

ج: تبلیغ برای توکن‌های بی‌ارزش:

معمولاً مبلغین توکن‌های بی‌ارزش با سونیت قبلی تبلیغ به توکن‌هایی می‌کنند که قرار است بی‌ارزش شوند. به نوعی تبلیغ برای توکنی بی‌پشتوانه که خود می‌تواند رفتاری مجرمانه تلقی شود تحت عنوان مبلغین توکن بی‌ارزش.مبلغین اول شرایطی را مهیا می‌کنند و در آن شرایط راجب به ارزی که ممکن است در بازه زمانی سقوط کند، تبلیغ می‌کنند و امکان این رفتار مبلغین تحت عنوان تبلیغ برای توکن-های بی‌ارزش قابلیت جرم‌انگاری می‌تواند داشته باشد.

کلاهبرداران در این روش، پروژه تولید یک رمز ارز را کلید می‌زنند و ضمن لیست کردن آن در صرافی به تبلیغ آن می‌پردازند. با توجه به این که رمز ارزها معمولاً در آغاز ارزش بسیار پایینی داشته و ممکن است پس از مدتی ارزشی تا چند هزار برابر را نیز تجربه کنند،

افراد مشتاق خرید این توکن‌ها می‌شوند خصوصاً در جایی که سازندگان با انجام مبادلات صوری، اقدام به اعتبارزایی برای توکن می-نمایند. پس از مدتی که مقادیر بالایی از این توکن فروخته شد، پروژه متوقف شده و توکن‌ها ارزش خود را از دست می‌دهند (محمودی، ۱۳۹۸: ۵۱۴).به نظر نگارنده، برای اطلاع‌رسانی در مورد خرید و فروش ارزهای دیجیتال ضمن نظام‌مند کردن این فضای فعالیت، مبلغین در قلمرو ارزهای دیجیتال باید دارای صلاحیت باشند و تعیین صلاحیت آنها در واقع توسط مرجعی تایید گردد که به نظر وزارت اقتصاد و دارایی صالح به تأیید این موضوع است. در این راستا افرادی هستند که با تشویق افراد در رسانه باعث فروش گسترده‌ای از این ارزهای دیجیتالی می‌شوند که در نهایت با دست به یکی کردن با سانده‌ی ارز باعث فروپاشی ارز شده و از ضرر مردم پول به دست می‌آورند که به نوعی رفتار آنها می‌تواند مصداق بارز مباشر معنوی در توکن‌های بی‌ارزش شود.

۱-۳. جعل و تقلب در ارزهای دیجیتالی

امروزه برای خرید و فروش رمز ارزها صرافی‌های جعلی به وجود می‌آیند که از عباراتی مانند «کارمزد صفر»، «امکان پرداخت به ریال با کارت شتابی»، «بدون تحریم»، «بدون نیاز به احراز هویت» و... استفاده می‌کنند. سایت‌های جعلی به عنوان این صرافی‌های جعلی ساخته می‌شود که ادعا می‌کنند برای خرید و فروش رمز ارزها، کارمزدشان صفر است ولی در واقع، از طریق دریافت کارمزد برای فهرست کردن هر توکنی (از جمله عرضه‌های اولیه کوین تقلبی) در پلتفرم خود کسب درآمد می‌کنند، بدون این که نقدینگی معاملاتی لازم برای معامله‌گران را به‌منظور خرید و فروش آزادانه توکن ایجاد کنند. این توکن‌ها معمولاً در این صرافی‌های جعلی مسدود می‌شوند و معامله‌گران با «توکن‌های بی‌ارزش» خود درگیر می‌شوند، بدون این‌که بتوانند آنها را بفروشند و یا نقد کنند (نواب‌پور و همکاران، ۱۳۹۷: ۱۴).به نظر نگارنده، گاهی اوقات در صحنه‌ی وب صرافی‌هایی درست می‌شوند که کاملاً فیک هستند که می‌توانند توسط برنامه‌نویسان درست شده باشند. رسیدگی به این صرافی‌ها فاقد نظارت کافیست و باعث کلاهبرداری می‌شوند در واقع صرافی حتماً باید از نظر بین‌المللی شناخته شده و معتبر باشد که آگاهی از آن با یک سرچ ساده در صفحه‌ی اصلی همان سایت به دست بیاید. این اعتبار از لحاظ علامت تنظیم[۱] هست که از سامانه‌های بین‌المللی به صرافی‌ها اعطا می‌شود.

جعل وقتی دیجیتالی می‌شود، فضای آن متفاوت و فضای دیجیتالی را دچار چالش عدم امنیت و موجب سلب اعتماد و آسایش عمومی و گسترش قربانیان در فضای دیجیتالی می‌شود؛ اینجاست که مداخله‌ی کیفری متفاوت می‌طلبد تا آحاد مردم بتوانند با طیب خاطر وارد سایت‌ها و شبکه‌های دیجیتالی شوند. این سلب آسایش عمومی نیازمند جرم‌انگاری متفاوت از دنیای عادی است.

۱-۴. خیانت در امانت در ارزهای دیجیتالی

یکی دیگر از جرائم مربوط به ارزهای دیجیتال، جرم خیانت در امانت است. در این روش، اشخاص با ادعای داشتن تخصص و همچنین پرداخت سودهای کلان در مبادلات ارزهای دیجیتالی، اقدام به خیانت در امانت می‌کنند. شخص بزه‌دیده به واسطه‌ی تبلیغات و دیدن سودهای پرداختی، اموال خود را با رضایت کامل بدست این‌گونه افراد می‌سپارند، ولی بعد از گذشت مدت زمانی، نه تنها سودی به افراد پرداخت نمی‌گردد، بلکه سرمایه اولیه آنها نیز برگردانده نمی‌شود و اینجاست که خیانت در امانت به وقوع می‌پیوندد (کوشا، ۱۳۸۸: ۳۴). ممکن است در چنین مواردی گفته شود که کلاهبرداری به وقوع پیوسته است اما باید اشاره داشت که در این موارد معمولا ابتدا سرمایه‌ای بعنوان امانت در اختیار فرد قرار می گیرد و سپس خائن اقدام به ارتکاب جرم می‌نماید.

اگرچه احراز جرم خیانت در امانت و تحقق ارکان این جرم یا جرائم دیگری از قبیل تحصیل مال از طریق نامشروع کمی دشوار و پیچیده می‌باشد، لکن بدلیل نوسانات موجود در این نوع از معاملات و امکان ورود ضرر همیشه نمی‌توان عنوان مجرمانه در این نوع از

۱. Regulation Mark

روابط مالی لحاظ نمود. از طرفی باید در نظر داشت که در سرمایه‌گذاری‌هایی با مبالغ بالا امکان هک کردن کیف پول و سرقت محتویات آن نیز قابل تصور است. این مسأله را می‌توان در زیر شاخه رسانه‌های فیک دانست که با تشویق و ترغیب اشخاص می‌شوند (رجبی، ۱۳۹۷: ۸۸). بنابراین با توجه به اینکه فرد امین، خود در بسیاری از موارد در معرض مالباختگی قرار دارد، احراز سونیت فرد در چنین مواردی ضروری می باشد.

از سوی دیگر، مالک صرافی که در مبادلات ارز دیجیتال بعنوان واسطه عمل می‌کند، ممکن است ارزهایی را که بعنوان امانت در اختیار او قرار گرفته و بنابراین بوده که تبدیل به ارز سنتی یا ارز دیجیتال دیگری نماید یا آن را به مصرف معینی برساند، به ضرر مالک آن، ارز مزبور را تصاحب یا به مصرف دیگری برساند. در شرایط فعلی بسیاری از صرافی‌ها به بهانه مقررات تحریم، پرداخت و یا تبدیل ارزهای دیجیتال شهروندان داخلی را متوقف نموده و یا در اختیار دیگران قرار داده‌اند، گرچه طبق مقررات بین‌المللی استناد آنها به احکام راجع به تحریم موجه می‌باشد و امکان پیگیری در محاکم را سلب می‌نماید اما می‌توان طبق مقررات داخلی با توجه به اینکه قربانی رفتار یکی از شهروندان ایرانی می‌باشد، مقررات مربوط به صلاحیت منفعل را توسعه داد و ضمن جرم‌انگاری، اقدام به تعقیب مرتکب نمود.

۲. امکان‌سنجی جرم‌انگاری جرایم مربوط به ارزهای دیجیتالی

پولشویی فرآیندی است که در آن درآمدهای غیرقانونی به نظر قانونی و مشروع جلوه داده می‌شوند(خضری نیا، ۱۳۹۸، ج۱: ۷۹). در این فرآیند امکان بهره‌گیری از هر دو نوع ارز، یعنی سنتی و دیجیتال، امکان‌پذیر است اما با تفاوت‌هایی همراه می‌باشد. پولشویی با ارز سنتی اغلب از طریق سیستم‌های بانکی انجام می‌شود، جایی که مجرمان می‌توانند با استفاده از شرکت‌های صوری و تراکنش‌های پیچیده، منشأ پول‌ها را پنهان کنند.

از حیث شیوه، ارتکاب جرم پولشویی از طریق ارزهای دیجیتال معمولاً نیاز به واسطه‌های مالی مانند بانک‌ها دارد و مرزهای ملی و همچنین قوانین بانکی می‌توانند فرآیند را کند یا پیچیده کند. در خصوص کشف جرم نیز شناسایی و ردیابی تراکنش‌ها از طریق سیستم‌های مالی موجود با سهولت بیشتری امکان‌پذیر است در مقابل، در پولشویی با ارزهای دیجیتال، امکان انجام تراکنش‌های ناشناس یا نیمه‌ناشناس وجود دارد و از حیث قلمرو نیز محدودیت‌های جغرافیایی کمتری برای انتقال وجوه وجود دارد. در خصوص کشف و ردیابی تراکنش‌ها می‌تواند کار برای نظام رسیدگی دشوار باشد، به خصوص اگر از رمزارزهایی استفاده شود که برای حفظ حریم خصوصی طراحی شده‌اند.

از آنجایی که جرایمی که در حوزه‌ی رمز ارزها به وقوع می‌پیوندند غالباً مجازی بوده و در فضای حقیقی صورت نمی‌پذیرند، لذا برای جرم‌انگاری و کیفرگذاری در این خصوص می‌بایست رویکردی افتراقی در این حوزه بکار برد، چرا که باید منافع عموم در آن در نظر گرفته شود و از آنجایی که این نوع جرایم بطور غالب، نوظهور محسوب می‌گردند، جرم‌انگاری نوینی در این راستا مورد نظر می‌باشد (حسینی و دعائی، ۱۳۹۳: ۹۸). بنابراین لازم است که قانون‌گذار با لحاظ ویژگی‌های این جرایم، وسعت و آثار ارتکاب بر امنیت اقتصادی کشور و مبادلات تجاری، چه در حیث تعریف جرایم و چه در حیث شرایط و نهایتاً در زمینه مجازات، رویکرد متناسب با آن را اتخاذ نماید. با همین رویکرد می‌توان رفتارهایی را که خارج از هنجارهای قواعد دنیای بلاکچین باشد، جرم منشأ شناخت و دامنه آن را به تخلفات نیز بعنوان مقدمه جرم تسری داد. در نتیجه هر تغییر و تحولی که منجر به لایه‌گذاری، ادغام و تطهیر ارزهای دیجیتال را پولشویی در ارزهای دیجیتال شناسایی نمود. در نتیجه بستر جرم پولشویی در ارزهای دیجیتال گسترده خواهد شد.

۲-۱. امکان‌سنجی جرم‌انگاری در پولشویی از طریق ارز دیجیتالی

به نظر نگارنده، پولشویی بدلیل غایت آن که همان عدم امکان رهگیری ست، رایج‌ترین جرم حاصل از فالعیت‌های مرتبط با ارزهای دیجیتالی می‌باشد. در واقع افرادی که می‌خواهند اقدام به پولشویی نمایند ارزهای دیجیتال را ساده‌ترین راه می‌دانند. با افزایش استفاده از ارزهای دیجیتال، قوانین و مقررات نیز در حال تکامل هستند تا از پولشویی جلوگیری کنند و شفافیت بیشتری را ایجاد کنند. در هر دو حالت، نظام‌های قضایی داخلی و سازمان‌های نظارتی تلاش می‌کنند تا با استفاده از فناوری‌های جدید و همکاری‌های بین‌المللی، فعالیت‌های پولشویی را شناسایی و با آن مقابله کنند. این تلاش‌ها شامل تبادل اطلاعات و به‌کارگیری ابزارهای تحلیلی پیشرفته برای ردیابی و شناسایی الگوهای مشکوک است[۱]. البته ناگفته نماند که در برخی از مصادیق بدلیل نوظهور بودن و نوعی سردرگمی قانون‌گذار داخلی و بین‌المللی در این‌خصوص هم در قوانین داخلی و همچنین مقررات بین‌المللی دچار ضعف‌ها و چالش‌ها و ناکارآمدی‌های بسیاری می‌باشیم که همه‌ی اینها لازمه‌ی این امر می‌باشد که قانونگذاری و جرم‌انگاری درستی در این راستا انجام شود.

در خصوص پولشویی باید اذعان کنیم که در حوزه‌ی رمز ارزها هیچ‌گونه نظارت و مقررات مشخصی وجود ندارد و یا قرارداد یا برنامه کاربردی که کاربران رمز ارزها بتوانند با استفاده از آنها به داد و ستد در این حوزه بپردازند نیز وجود ندارد. به همین خاطر است که اکثر پولشویی‌ها از فیلتر رمز ارزها عبور می‌کند (خضری‌نیا، ۱۳۹۸، ج۱: ۱۲۵). توانایی کاربر ارز دیجیتال برای تبادل آن به دلیل مهم بودن انتقال آن از طریق تعداد بیشمار آدرس ها، و سرعت انتقال آن در مقایسه با پول های منتشره توسط دولت، بیشتر تلاش های ضد پولشویی را خنثی می‌کند (Darfon Bryans, 2014, 441).

بنابراین در راستای ساماندهی این عرصه لذا و در راستای سیاست‌های کیفری افتراقی در حوزه‌ی جرم‌انگاری، می‌توان هرگونه کسب و کاری که مجرم در کنار استفاده از ارزهای دیجیتالی بکار می‌گیرد (اعم از تأسیس شرکت‌های صوری، خرید و فروش ماشین و زمین و بطور کلی اموال منقول و غیرمنقول) به نوعی در جهت تطهیر پولشویی بوده که می‌بایست هر یک از آنها جرم تلقی شود که البته با وصف استفاده از روش‌های تطهیر ارز. به طور کلی دو نوع تریدر در قلمرو ارزهای دیجیتال وجود دارد:

۱) تریدر مجرم که باعث فریب افراد می‌شود؛ پولشویی و تبلیغات فیک و در نهایت درآمد از این روش‌های مجرمانه دارد.
۲) تریدر واقعی که فردی تحصیل کرده اقتصاددان؛ این افراد دارای توانایی تحلیل‌های خبری و معامله‌گری در چهارچوب قانون هستند و درآمد ایشان در قلمروی ارزهای دیجیتال دارای صلاحیت علمی و فنی و تخصصی می‌باشد.

به نظر بعضی از نویسندگان هرگونه اقدام به نصب بدافزار و یا نرم‌افزارهایی که منجر به استفاده از آنها در جهت نیل به اهداف پولشویی‌گری می‌باشد، می‌بایست جرم تلقی گردد و وصف مجرمانه‌ی مخصوص به خود را داشته باشند. در واقع نرم‌افزارهای اصلی این بازار انگشت شمار بوده و قابل ذکر است که نوع استفاده‌ی فرد است که منتهی به عمل مجرمانه می‌شود یا خیر.

بکارگیری نیروهای کاری انسانی و به بیانی چنانچه در خلال فعالیت‌های پولشویی از طریق بکارگیری ارزهای دیجیتالی نیروهای انسانی نیز بکار گرفته شوند هر یک از آنها عملشان دارای وصف کیفری بوده و مستلزم مجازات خواهند بود.

همچنین القای وصف مجازات جرایم اقتصادی به جرایم پولشویی در حوزه‌ی رمز ارزها (چرا که پولشویی از طریق رمز ارزها از آنجایی که معمولاً قابل پیگیری نمی‌باشد، تعادل و بالانس بازار اقتصادی را برهم زده و مشکلات عدیده‌ای در این خصوص بوجود می‌آورد). راهکار دیگری در این حوزه می باشد. مجازات‌های مالی مشدد در خصوص کاربران ارزهای دیجیتالی که از این طریق پولشویی کرده و موجب بروز ضرر و زیان‌هایی در حوزه‌ی تولید داخلی شده‌اند (مجازات مالی از این حیث می‌بایست مشدد باشد که هم کاربر با پولشویی مرتکب یک جرم و با رد گم کنی از طریق ارزهای دیجیتالی مرتکب دو جرم شده است). نیز می‌تواند به تقویت موضوع کمک

[۱]. بعنوان نمونه قانون کنترل و اعلام الزامی سال ۱۹۸۴ در آمریکا موسسات مالی را موظف کرده است که هر گونه عملیاتی بالغ بر ده هزار دلار را به مقامات خاصی اعلام کنند (بوسورث، ۱۳۷۶، ۹۷).

کند. با توجه به اینکه تحصیل منافع مالی یکی از اهداف مرتکبان در این حوزه می‌باشد، مصادره نمودن تمامی عواید و فواید حاصل از پولشویی از طریق بکارگیری رمز ارزهای دیجیتالی به نفع ارگان‌های دولتی ذیربط اعم از اداره مالیات[1] و اداره صنعت و معدن و تجارت راهکار دیگر مقابله خواهد بود ؛چرا که بیشترین ضررها از این عمل متوجه این دو نهاد دولتی می‌باشد (خضری‌نیا، ۱۳۹۸، ج۱: ۱۵۳).

در نهایت ابطال نمودن تمامی معاملات به قصد فرار از مصادره پس از تاریخ شروع به جرم پولشویی از طریق ارزهای دیجیتالی اثر حقوقی دیگر مترتب بر فعالیت‌های مجرمانه این گروه به قصد حمایت از فعالیت‌های سالم اقتصادی خواهد بود. بنابراین به نظر می رسد به جای ممنوعیت کلی ارز دیجیتال، بهتر است تبادلات کلان آن با تکنولوژی پیشرفته تحت کنترل قرار گیرد؛ به گونه‌ای که ریسک چنین مبادلاتی برای پولشویان افزایش یابد و به این ترتیب از استفاده این روش برای پولشویی، صرف نظر کند. برخی از صاحب نظران حفرق نیز معتقدند سرکوب جرایم سازمان یافته از طریق قوانین ضد پولشویی چندان موثر نیست و اگر مزیت اندکی هم داشته باشد در برابر حفظ حریم خصوصی سایر افراد جامعه کم اهمیت است (Darfon Bryans, 2014, 65).

۲-۲. امکان‌سنجی جرم‌انگاری کلاهبرداری از طریق ارزهای دیجیتال

به نظر نگارنده، موارد و مصادیقی هستند که استفاده از آنها و یا ارتکاب آنها از لحاظ سیاست کیفری مدرن در مواجهه با جرایم نوظهوری همچون کلاهبرداری در ارزهای دیجیتالی جرم محسوب می‌گردد. از یک منظر هرگونه خرید و فروشی که کاربران ارزهای دیجیتالی در فضای دیجیتال انجام می‌دهند، به نوعی مستلزم جرم محسوب شدن می‌باشد چرا که هیچ‌گونه اعتبار و اعتمادسازی قانونی در فضای ارزهای دیجیتالی وجود ندارد و چه بسا بسیاری از افراد که قراردادهایی را در عرصه‌ی ارز دیجیتال منعقد می‌نمایند که صرفاً از آن طریق کلاهبرداری نمایند و در پی سوء استفاده از این خلاء قانونی (جرم محسوب نشدن ارزهای دیجیتالی) می‌باشند. با این وجود همچنان عنصر اغفال بعنوان یکی از اجزا مهم جرم کلاهبرداری در رابطه میان خریدار و فروشنده مخدوش می‌باشد. اما انتشار محتواهای تبلغیاتی از طریق صفحات افراد معروف در فضای مجازی در جهت ترغیب افراد علی‌الخصوص افراد فاقد شغل و یا افرادی که سرمایه اندکی دارند در جهت پیوستن به عرصه‌ی ارزهای دیجیتالی و سرمایه‌گذاری در این زمینه که در واقع در اصل سرمایه‌گذاری معتبری وجود ندارد، می‌تواند تشکیل‌دهنده اغفال باشد و همگی کلاهبرداری محسوب شود.

نصب بدافزارها و نرم‌افزارها بر روی تلفن همراه افراد مختلف علی‌الخصوص سرمایه‌داران با گردش مالی و حساب بانکی بالا به نحوی که چنانچه فرد بدافزار را باز کرده، کلیه اطلاعات حساب علی‌الخصوص حساب کیف پول ارزهای دیجیتالی بین‌المللی وی افشا شده و به حساب شخص کلاهبردار منتقل می‌گردد نیز نوع دیگری از کلاهبرداری در این حوزه می باشد.

کلاهبرداری از طریق ارز دیجیتال ممکن است مشمول کلاهبرداری ساده و یا کلاهبرداری اینترنتی شود. کلاهبرداری ارز دیجیتال زمانی اتفاق می‌افتد که عملیات متقلبانه حول محور ارز دیجیتال رخ دهد (کوشا، ۱۳۸۸: ۳۵). با توجه به عمومیت و واجد جنبه دولتی بودن جرم بعنوان یکی از معیارهای افتراقی[2]، در خصوص مجازات این جرم به شکل افتراقی براساس سیاست‌های کیفری نوین در حوزه‌ی جرایم نوظهور و مرتبط باید بیان کرد که هر کس به طور غیرمجاز از سامانه‌های رایانه‌ای و مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، مرتکب کلاهبرداری اینترنتی شده و علاوه بر رد مال به صاحب آن، می‌بایست به حبس از ۱ تا ۵ الی ۶ سال یا

---

[1]. امروزه ارز دیجیتال مشکلاتی را در سیستم مالیاتی ایجاد کرده است. زیرا برای انجام کارکردهای پولی طراحی شده است؛ ولیکن با درک سنتی از پول متناسب نیست. علاوه بر این، بسیاری از مردم از آن برای سرمایه‌گذاری و نه صرفا برای خرید و فروش کالا و خدمات استفاده می کنند. (Adam Chodorow, 2016, 373) در مجموع کسانی که ارزهای مجازی را برای خرید استفاده می‌کنند در حال حاضر وضعیت مالیاتی نامطمئن و نامشخصی دارند (Ball Aleksandra, 2014, 162).

۲ –ر.ک سماواتی پیروز، ۱۳۸۸، ص۱۳۶

جزای نقدی معادل مبلغ کلاهبرداری شده یا هر دو مجازات محکوم شود (فراتی و همکاران، ۱۳۹۸: ۶۵). در عین حال باید اشاره کرد که بر خلاف کلاهبرداری معمول که مبنای آن حمایت از منافع افراد می‌باشد، در اینجا مبنا صیانت از مصالح عمومی خواهد بود.

بنابراین در این نوع از کلاهبرداری، این شخص نیست که فریب می‌خورد و در واقع سیستم رایانه‌ای فریب می‌خورد. در این روش، فرد مجرم، سیستم‌های مرتبط با رمز ارزها مانند کیف پول دیجیتال را دستکاری کرده و رمز ارزها را به حساب خود منتقل می‌کند. همچنین فرد می‌تواند با ایجاد اختلال در هنگام انتقال رمز ارز از حسابی به حساب دیگر، رمز ارز را به کیف پول خود منتقل کند. لذا ضروری است تا وصف مجرمانه و مجازات دیگری نیز در غالب هک سیستم‌های رایانه‌ای متوجه مجرم باشد (سلطانی و اسدی، ۱۳۹۴: ۱۷۷). با تفسیر و تعمیم ماده ۱قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری، به کلاهبرداری دیجیتالی در حوزه‌ی رمز ارزها می‌توان اینگونه مجازات تعیین نمود که: هر کس از راه حیله و تقلب مردم را به وجود شرکت‌ها یا تجارت‌خانه‌ها یا کارخانه‌ها یا مؤسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیرواقع امیدوار نماید یا از حوادث و پیش‌آمدهای 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 حواله‌جات یا قبوض یا مفاصاحساب و امثال آنها تحصیل کرده و از این راه مال دیگری را ببرد، کلاهبردار محسوب شده و علاوه بر رد اصل مال به صاحبش، به حبس از ۱ تا ۷ سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است، محکوم می‌شود (کوشا، ۱۳۸۸: ۳۶). نباید از نظر دور داشت که ویژگی‌های مرتکب، نحوه ارتکاب و گستردگی جرم بطور معمول، می‌تواند ضمن تفاوت در نوع مجازات، از کیفیات مشدده این جرم محسوب شود.

۲-۳. امکان‌سنجی جرم‌انگاری خیانت در امانت از طریق ارز دیجیتالی

خیانت در امانت نیز جرم دیگری است که در فضای مجازی و بخصوص در حوزه‌ی ارزهای دیجیتال بسیار اتفاق می‌افتد. به نظر نگارنده، در یک‌سری از حالات شخص با وعده‌ی سرمایه‌گذاری در حوزه‌ی ارز دیجیتال شخص یا موسسه‌ی دیگری را ترغیب به سرمایه‌گذاری می‌کند و شرایط آن را نیز به این شکل در نظر می‌گیرد که شخص می‌بایست سند یا سفته یا چکی را در شروع کار به عنوان وثیقه برای شراکت در سود نزد طرف اول وثیقه قرار دهد و پس از آن اقدام به فروش و یا به اجرا گذاشتن چک یا سفته می‌کند که این عمل مستلزم جرم‌انگاری می‌باشد.

نوع دیگری از اقداماتی که می‌تواند خیانت در امانت در ارزهای دیجیتالی جرم محسوب گردد، حالتی است که خائن پس از آنکه دیگری را ترغیب به سرمایه‌گذاری می‌کند با وعده‌ی سرشاخه بودن خود به عنوان سرگروه و با توجیه اینکه سرگروه می‌بایست رمز ورود تمامی زیر شاخه‌ها را داشته باشد رمزها از افراد گرفته و پس از سوددهی از طریق ورود با رمز عبور اشخاص سود را گرفته و به والت خود منتقل کرده و از این حیث خیانت در امانت کرده و وصف مجرمانه دارد و از امانت و اعتماد سایرین سوء استفاده نموده است.

از حیث مجازات نیز از آنجایی که جرایم حوزه‌ی ارزهای دیجیتالی غالباً مدرن و نوظهور هستند و لذا سیاست‌های کیفری افتراقی می‌بایست برای آنها در نظر گرفته شود، به نظر می‌رسد از لحاظ قانونی و قانون‌گذاری ضعف‌هایی در این خصوص دیده می‌شود.

در نظر گرفتن رد مال و سود عاید از سرمایه‌گذاری‌هایی که مجرم با رمز مشترک آنها را دریافت نموده و به حساب خویش انتقال داده است که این رد مال می‌بایست متناسب با نرخ روز باشد. برای مثال اگر شخصی در سال ۱۴۰۰ اقدام به خیانت در امانت در این خصوص نموده باشد و در سال ۱۴۰۲ محکوم گردد به رد سود و عواید آن می‌بایست براساس نرخ روز در سال ۱۴۰۲ اقدام به رد نماید، چرا که تورم طی این دو سال نیز باید لحاظ گردد

نتیجه‌گیری

رمزارزها نوعی ارز دیجیتالی غیرمتمرکز می‌باشند که با فناوری جدیدی ارائه شده‌اند. شناسایی ماهیت رمزارزها رابطهٔ تنگاتنگی با بازشناسی ساختار فنی هریک از اقسام آن دارد. از حیث حقوقی؛رمزارزها گونه‌ای از اموال غیرمادی و یا در صورت توسعه و تسری مفهوم عین به اموال ناملموس، از اعیان محسوب شده که دارای مالیت عرفی و شرعی نیز می‌باشند. با توسعه روزافزون در مبادلات تجاری و فواید و کارکردهای آن برای اقتصاد جوامع و علی‌الخصوص جوامع تحت تحریم بدلیل ایجاد فرصت دور زدن تحریم‌ها، ضمن غنیمت شمردن فرصت استفاده از آنها، باید نسبت به خطرات احتمالی و پیش‌بینی جرایم احتمالی و کیفر مجرمان این عرصه چاره‌اندیشی کرد و با لحاظ ابعاد مالی آن، می‌توان قواعد مرتبط با جرایم مالی را در خصوص جرایم مرتبط با آنها از قبیل کلاهبرداری، سرقت و دیگر جرایم از این سنخ اعمال، و مرتکب را تحت تعقیب قرار داد.

در شرایط کنونی وجود خلاءهای قانونی و فقدان چارچوب مدون برای فعالیت‌های در این حوزه، در کنار خسارات مالی، می‌تواند خسارات جبران ناپذیری را متوجه مصالح عمومی نماید. چرا این که فرصت ممکن است منجر به تهدید از سنخ از دست دادن سرمایه ملی در سطح گسترده شود. بنابراین گشودن بابی در بخش جرایم علیه امنیت و آسایش عمومی نیز می‌تواند خلا موجود را مرتفع نماید. می‌توان با اتخاذ رویکرد مبتنی بر سیاست جنایی امنیت‌گرا، دو شناسایی جرایم مرتبط با آن بعنوان تهدیدی علیه امنیت و آسایش عمومی و بعنوان اقدامی مخرب نسبت به امنیت اقتصادی جامعه و اعتماد عمومی به مبادلات تجاری و ابزارهای مبادله، از وقوع جرایمی همچون پولشویی از طریق تطهیر درآمدهای ناشی از فعالیت های نامشروع با ارز دیجیتال، تبلیغ برای توکن‌های بی ارزش، خیانت در امانت، کلاهبرداری، جعل و ورود و ترید بدون مجوز، اقدام به جرم انگاری و کیفرگذاری کرد. همچنین از آنجایی که اینگونه جرایم جملگی نوظهور و جدید می‌باشند، سیاست جنایی و کیفری افتراقی و جدید را می‌طلبد تا بتوان با آنها به صورت کارآمد مواجهه نمود.

با توجه با یافته‌های پژوهش می‌توان پیشنهاد نمود:

۱. قانون‌گذار در ذیل فصل مربوط به جرایم رایانه‌ای، بخشی را به جرایم مرتبط با ارزهای دیجیتال اختصاص دهد و مجازات‌هایی متناسب با آن همچون مصادره اموال را بعنوان کیفر مرتکبان پیش‌بینی نماید.

۲. ماهیت این سیستم عامل‌های محاسباتی و قلمرو برنامه‌های کاربردی (اپلیکیشن‌های) آن، مسائل مهمی در زمینه انطباق با قانون ایجاد می‌کند. بسیاری از حوزه‌های قضایی در سراسر دنیا در حال بررسی این موضوع هستند که سیستم‌های ارز دیجیتال تا چه میزان تحت تأثیر قوانین و مقررات موجود هستند و برای پاسخگویی به رشد پول‌های دیجیتال، چه میزان از قوانین و مقررات موجود باید اصلاح شوند یا قوانین جدید وضع گردد. با این‌حال، در حال حاضر روشن است که در عالم واقع در هر حوزه قضایی طیف متنوعی از قوانین و مقررات قابل اعمال بر پول‌های دیجیتال و برنامه‌های کاربردی (اپلیکیشن‌های) آن وجود دارد. در این شرایط، توسعه‌دهندگان، توزیع-کنندگان و کاربران پول‌های دیجیتال و سیستم‌های مرتبط با آن، با مسائل مهم مربوط به انطباق با قانون مواجه هستند. شناخت این الزامات قانونی موجود و بالقوه برای استفاده موفقیت‌آمیز از سیستم عامل‌های ارز دیجیتال و برنامه‌های کاربردی (اپلیکیشن‌های) آن ضروری است.

۳. ضرورت دارد که علاوه بر شناسایی رفتارهای مجرمانه و مجازات آنهادر قلمروی ارزهای دیجیتال در راستای بهینه‌کردن و جا انداختن ترید در حوزه‌ی ارزهای دیجیتال از این مقوله حمایت کرد و بسته به نوع استفاده‌ی فرد در این قلمرو را ارزیابی کرد و به محض کشف نشانه‌های مجرمانه و پیش‌زمینه‌هایی به عنوان رفتار مجرمانه جرم‌انگاری کرد، زیرا در آینده‌ای نه چندان دور ارزهای دیجیتال نوعی انس جهانی به حساب می‌آیند و با جرم دانستن آنها و بستن راه‌های استفاده از آنها نوعی ضربه‌ی مهلک به امنیت و اقتصاد کشور خواهد بود.

۴. لازم است که با ایجاد یک سامانه‌ی الکترونیکی زیر نظر یک واحد مرجع، تمامی افرادی که در این زمینه فعالیت دارند، عضو شده و هرگونه فعالیت آنها و تبلیغات زیر نظر این سامانه باشد و لذا افرادی که در این سامانه عضو نیستند و به تشویق و ترغیب افراد در رسانه فعالیت دارند یا از نوع معاملات ثبت نشده بهره می‌برند، بازخواست شود واز پشتیبانی قانون محروم گردند و می‌توان از افراد ثبت این سامانه به صورت سالانه مالیات کسب گردد که کمکی جدی به اقتصاد و امنیت کشور شده که در نهایت سرمایه ملی حفظ می‌شود.

۵. ورود بدون مجوز به شبکه بلاکچین و متعاقب آن ترید بدون مجوز جرم‌انگاری شود و چنین فعالیت‌هایی دارای ساختار و مقررات مدون جهت هرگونه فعالیت و ورود به آن شود و رعایت رفتار مطابق با مقررات در طول دوره مجوز، زمینه تمدید فعالیت او برای دوره‌های بعدی و تمدید مجوز قرار گیرد.

۶. استفاده از فناوری‌های نوین مانند هوش مصنوعی، بررسی تراکنش‌های با مبالغ بالا و ایجاد سوال‌هایی جهت پاسخ راجع به منشا و علت انتقال و تحلیل بلاکچین برای شناسایی الگوهای مشکوک و مبارزه با پولشویی برای به حداقل رساندن ارتکاب جرم از طریق مبادلات مرتبط با کیف‌های پول چرا که در بسیاری از موارد، مبادله صرفا میان کیف‌های پول است.

در مقام تقنین با توجه به اینکه صرافی‌ها نقش مهم و کلیدی در مبادلات ارزهای دیجیتال ایفا می‌کنند و نقش واسطه را بازی می‌کنند و کلیه مبادلات از این طریق صورت می‌گیرد، ضرورت دارد که فرایند احراز صلاحیت، اخذ تضامین لازم، نظارت مستقیم و برخط و همچنین مقررات مربوط به دریافت نشانه اعتماد با حساسیت کامل و با وضع مقررات سخت‌گیرانه صورت گیرد چرا که می‌تواند منجر به پیشگیری از جرایم و تخلفات بعدی شود. همچنین مقرراتی وضع شود تا بانک‌ها نیز صرفا مجاز به انتقال پول به صرافی‌های مجاز باشند. همچنین از حیث قانونی لازم است که با ایجاد یک سامانه‌ی الکترونیکی زیر نظر یک واحد مرجع، تمامی افرادی که در این زمینه فعالیت دارند، عضو شده و هرگونه فعالیت آنها و تبلیغات زیر نظر این سامانه باشد و لذا افرادی که در این سامانه عضو نیستند و به تشویق و ترغیب افراد در رسانه فعالیت دارند یا از نوع معاملات ثبت نشده بهره می‌برند، بازخواست شود واز پشتیبانی قانون محروم گردند و می‌توان از افراد ثبت این سامانه به صورت سالانه مالیات کسب گردد که کمکی جدی به اقتصاد و امنیت کشور شده که در نهایت سرمایه ملی حفظ می‌شود.

باتوجه به ماهیت ارزهای دیجیتال جرایم مرتبط با آن محدود می‌باشد وعلی القاعده نسبت به بسیاری از جرایم ارتکاب آنها سالب به انتقاع موضوع می‌باشد مانند جرایم علیه اشخاص بنابراین در این مقاله تلاش شده است که در حد یک مقاله به مهم‌ترین و رایج‌ترین این جرایم پرداخته شود و در مراتب بعدی جرائم دیگری نیز متصور می‌باشد.

همچنین کستردگی، شیوه ارتکاب، نوظهور بودن آنها اثراتی که ممکن است در سطح داخلی و بین اللمللی به جای گذارد اقتضا می‌کند تا قانونگذار سیاست کیفری افتراقی راجب به آنها اتخاذ کند مقررات فعلی نمی‌تواند پاسخ‌گویی آنها باشد.

منابع

۱. بوسورث، روون؛ سالت‌مارش، گراهام. (۱۳۷۶). پولشویی، مترجم: نصرالله امیر بشیری، اداره کل آموزش نیروی انتظامی.

۲. حسن‌زاده، علی؛ مجتهد، احمد؛ بغدادی، پویا؛ تقی‌زاده حصاری، فرهاد. (۱۳۹۶). پول و بانکداری نوین، چاپ دوم، تهران، انتشارات جنگل (جاودانه).

۳. خضری‌نیا، صادق. (۱۳۹۸). *پول‌شویی جرم اقتصادی یا مالی*، جلد اول، تهران، انتشارات عدلیه.

۴. خلیلی پاجی، عارف؛ نیازپور، امیرحسین. (۱۴۰۰). *بایسته‌های شمول قانون مبارزه با پولشویی بر دارایی‌های مجازی؛ در پرتو توصیه‌های گروه ویژه اقدام مالی FATF*، دوفصلنامه دانشنامه حقوق اقتصادی، شماره ۲۰.

۵. خلیلی پاجی، عارف؛ نیازپور، امیرحسین؛ شاملو، باقر. (۱۴۰۰). *جرم‌انگاری در حوزه رمز ارزها، آموخته‌های حقوق کیفری*، دانشگاه علوم اسلامی رضوی، دوره ۱۸، شماره ۲۱.

۶. خردمند، محسن. (۱۳۹۸). *بررسی فقهی استخراج و مبادله‌ی رمز ارزها با تمرکز بر شبکه‌ی «بیت کوین»*، معرفت اقتصاد اسلامی، شماره ۱۰و ۱۲.

۷. رجبی، ابوالقاسم. (۱۳۹۷). *ارز مجازی: قانونگذاری در کشورهای مختلف و پیشنهادها برای ایران*، تهران: مرکز پژوهش‌های مجلس شورای اسلامی.

۸. روشن، محمد؛ مظفری، مصطفی؛ میرزایی، هانیه. (۱۳۹۸). *بررسی وضعیت فقهی و حقوقی بیت کوین*، فصلنامه تحقیقات حقوقی، شماره ۸۷.

۹. فراتی، مریم؛ شاملو، باقر؛ گلدوزیان، ایرج. (۱۳۹۸). *راهکارهای مقابله با پولشویی از طریق بیت‌کوین*، فصلنامه علمی تحقیقات حقوقی آزاد، دوره ۱۳.

۱۰. سماواتی پیروز، امیر. (۱۳۸۸). *مؤلفه‌های افتراقی جرایم اقتصادی در تقابل با جرایم مالی*، رهنمون، شماره ۲۵و۲۶.

۱۱. سبحانی، حسن؛ قائمی‌نیا، علی‌اصغر. (۱۳۹۷). *تأملی در منشا ارزش بیت‌کوین از منظر اعتباریات علامه طباطبایی(ره)*، پژوهشنامه اقتصادی، دوره۱۸، شماره ۷۰.

۱۲. سلطانی، محمد؛ اسدی، حمید. (۱۳۹۴). *ماهیت حقوقی پرداخت در پول الکترونیک*، پژوهشنامه حقوق اسلامی، شماره ۴۱.

۱۳. سیدحسینی، میرمیثم؛ دعائی، میثم. (۱۳۹۳). *بیت کوین نخستین پول مجازی*، ماهنامه بازار سرمایه ایران، شماره ۱۱۴ و ۱۱۵، ۸۴-۸۸.

۱۴. عبدی‌پور، ابراهیم. (۱۳۸۹). *تحلیل حقوقی ماهیت پول الکترونیکی*، مجله حقوق خصوصی، دوره ۷، شماره۱۶.

۱۵. *غلام‌پور، امین. (۱۴۰۲). پولشویی با ارز دیجیتال، برگرفته شده از سایت:*

۱۶. *کاشیان، عبدالحمید؛ بهرامی، زهرا؛ قلی‌پور، فهیمه؛ شهروی، زهرا. (۱۳۹۸). درک ماهیت پول‌های رمزپایه و تعیین برخی از الزامات قانون‌گذاری آن در ایران از منظر اقتصاد اسلامی، فصلنامهٔ سیاستهای مالی و اقتصادی، شماره ۲۶.*

۱۷. *کوشا، جعفر (۱۳۸۸). امنیت اقتصادی با تاکید بر پیشگیری و مبارزه با قاچاق کالا و پیشگیری، مجله تحقیقات حقوقی، نشریه دانشکده حقوق دانشگاه شهید بهشتی.*

۱۸. *وایزی، بهار؛ جمشیدی، علیرضا. (۱۳۹۶). سیاست‌جنایی ایران در قبال جرم پولشویی، کنفرانس ملی تحقیقات علمی جهان در مدیریت، حسابداری، حقوق و علوم اجتماعی.*

۱۹. *محمدی، پژمان؛ اسدی، روح‌الله. (۱۳۹۱). ماهیت انتقال مالکیت اموال غیرمادی غیرفکری، نشریه دانش و پژوهش حقوقی، شماره ۱.*

۲۰. *محمودی، اصغر. (۱۳۹۸). تحلیل ارزهای مجازی در پرتو فقه، حقوق و مطالعات تطبیقی، نشریه مطالعات حقوق خصوصی (حقوق)، شماره ۳.*

۲۱. *میرزاخانی، رضا؛ سعدی، حسین‌علی. (۱۳۹۷). بیت‌کوین و ماهیت مالی- فقهی پول مجازی، جستارهای اقتصادی ایران با رویکرد اقتصادی اسلامی، شماره ۳۰.*

۲۲. *نواب‌پور، علیرضا؛ یوسفی، احمدعلی؛ طالبی، محمد. (۱۳۹۷). تحلیل فقهی کارکردهای پول‌های رمزنگاری شده (مطالعه موردی بیت کوین)، فصلنامهٔ علمی پژوهشی اقتصاد اسلامی، شماره۷۲.*

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

24. Chodorow, A. (2016). Bitcoin And The Definition Of Foreign Currency. *Florida Tax Review*, Vol 19.
25. Boehm, F. & Pesch, P. (2014). Bitcoin: A First Legal Analysis. In: Böhme R. ،Brenner M. ،Moore T. ، Smith M. (Eds) Financial Cryptography and Data Security. FC. *Lecture Notes in Computer Science*, Vol 8438. Springer ،Berlin ،Heidelberg ،n. d.
26. David, L.E.E. Chuen, K. (2015). Handbook of Digital Clarency Bitcoin. Innovation. *Financial Instruments, and Big Data*. *Elsevier Science*.
27. Darfon, B. (2014). Bitcom and Money Laundering Mixing for an Effective Solution. *89 Indiana Law Joumal*.