

کارکردهای مجرمانه ارزشهای مجازی: تحلیل جرم‌شناختی و راهکارهای پیشگیرانه*

علی صفاری^۱

دانشیار گروه حقوق جزا و جرم‌شناسی،
دانشکده حقوق دانشگاه شهید بهشتی

راضیه صابری^۲

دکتری حقوق جزا و جرم‌شناسی دانشکده
حقوق دانشگاه شهید بهشتی، پژوهشگر موسسه
پژوهشی حقوقی شهر دانش

عارف خلیلی پاجی^۳

دانشجوی دکتری حقوق جزا و جرم‌شناسی
دانشکده حقوق دانشگاه شهید بهشتی

تاریخ پذیرش: ۱۳۹۹/۱۰/۱

تاریخ دریافت: ۱۳۹۹/۳/۱۸

چکیده

پول در معنای ابزاری جهت مبادله قدمتی به اندازه تاریخ بشر دارد. استفاده از پول‌های کالایی تا ضرب سکه‌های فلزی و چاپ اسکناس‌های با پشتوانه طلا و در نهایت شکل‌گیری اسکناس‌های بدون پشتوانه را می‌توان خلاصه‌ای از سیر تکوین پول در نظام‌های پولی ملی و فراملی دانست. نظام موجود پولی، پس از گذر از نظام «برتون وودز» و شکل‌گیری «پول بدون پشتوانه» در تمامی کشورها استقرار یافت. با وجود توسعه ظرفیت‌های تجاری و اقتصادی در پهنه نظم نوین برآمده از اقتصاد جهانی شده، این نظم همواره

* - مقاله پژوهشی

1- alisaffary2020@gmail.com

2- نویسنده مسئول: raziehsaberi@yahoo.com

3- Arefkhalilipaji@gmail.com

DOI: 10.22067/lowecon.2020.48879.0

کانون انتقاداتی بنیادین از سوی منتقدان وضع موجود به سبب آسیب‌رسان بودن آن بوده است. ویژگی تورمی آن و تبدیل شدن پول به عنوان ابزاری در دست حکومت‌ها در راستای تحمیل سیاست‌هایی که نتایج زیان‌بار برای قشر متوسط و ضعیف در پی دارد و سوء‌مدیریت ناظران نظم موجود و در نتیجه ایجاد بحران‌های اقتصادی که پیامدهای منفی آن نیز بر دوش قشر مذکور است محور انتقادات به نظم نوین پولی است. از این رو، ارائه مدل‌های تعدیل‌کننده وضع موجود یا جایگزینی برای آن، حداقل در سطح دانشگاهی، مباحثی را به خود اختصاص داده است. امری که با وقوع بحران اقتصادی ۲۰۰۸ و معرفی فن‌آوری نوین «بیت‌کوین» به عنوان یک ارز یا پول مجازی، با کارکرد پول یا سامانه پرداخت وارد ابعاد نوینی شد که یک سال بعد با آغاز فعالیت، بیش از پیش نظرها را در ضرورت تغییر وضعیت فعلی به خود جلب کرد. در این چارچوب، ارزش‌های مجازی به دلیل برخورداری از ویژگی‌های منحصر به فرد همواره از ابعاد گوناگون مورد تحلیل و بررسی قرار گرفته‌اند. ویژگی‌هایی که افزون بر تسهیل مبادلات و کاربست‌های متعارف، می‌تواند قابلیت‌های احتمالی و واقعی مجرمانه‌ای را نیز در پی داشته باشد و بدین سان مطالعه ابعاد جرم‌شناختی این ابزار فن‌آورانه را اجتناب‌ناپذیر نماید. از این رو، در پژوهش پیش‌رو، با روشی توصیفی-تحلیلی و استفاده از منابع معتبر، علل تمایل بزهکاران به جایگزینی ارزش‌های مجازی به جای ارزش‌های رایج در ارتکاب فعالیت‌های مجرمانه در پرتو برخی نظریه‌های جرم‌شناسی و راه‌های پیشگیری از آن‌ها بررسی خواهد شد.

کلیدواژه‌ها: ارز مجازی، بیت‌کوین، بررسی جرم‌شناختی، قانون‌گذاری، پیشگیری.

طبقه بندی JEL: K14

مقدمه

ارز مجازی (Virtual Currency) عنوانی عام برای برخی ابزارهای فن‌آورانه با ویژگی‌ها و کارکردهای پولی یا ابزارهای مبادله است. برخی از مصادیق ارزش‌های مجازی را می‌توان ارزش‌های مبتنی بر فن‌آوری رمزنگاری دانست که با عناوینی چون رمزارز (Crypto-currency)، ارز رمزپایه و رمزینه در ادبیات فارسی مورد استفاده قرار می‌گیرد. این فن‌آوری برآمده از فضای مجازی است و در بستر این فضا معنا می‌یابد (Soleimani poor, et al., 2017: 173). در مقام مقایسه ارزها یا

پول‌های مجازی با ارزها یا پول‌های واقعی چند نکته قابل توجه است.^۱ نخست آنکه، خلق و ایجاد ارزهای مجازی وابسته به شخص یا گروه خاصی نیست و تمامی کاربران شبکه می‌توانند با استفاده از سازوکارهایی مشخص اقدام به خلق ارز نمایند؛ برخلاف ارزهای رایج فعلی/فیات (Fiat Currency) که بر اساس ضوابطی مشخص خلق و ایجاد آن جز وظایف ذاتی حکومت‌ها محسوب می‌شود و عموم مردم در این زمینه وظیفه‌ای ندارند. دوم آنکه مانند فیات، ارزهای مجازی نیز بدون پشتوانه مادی هستند. در واقع، همان‌گونه که دهه‌ها است پول‌های رایج بدون پشتوانه توسط دولت‌ها ایجاد می‌شوند ارزهای مجازی نیز فاقد هرگونه پشتوانه‌ای هستند.^۲ با این حال، اگر اعتبار دولت‌ها و میزان تولید کالا و خدمات را بتوان به‌نوعی پشتوانه پول‌های موجود دانست می‌توان این‌طور استدلال کرد که در این مفهوم ارزهای مجازی نیز از پشتوانه‌ای در معنای اعتماد عمومی برخوردار هستند. افزون بر موارد مذکور، باید دانست که از حیث حمایت قانونی نیز وضعیت ارزهای مجازی نسبت به فیات متفاوت است. فیات از حمایت کامل قانونی برخوردار است و ارزهای مجازی نه تنها به عنوان پول مورد شناسایی قرار نگرفته، بلکه رویه رسمی دولت‌ها تقلیل اعتبار آن از نوعی پول به سمت نوعی کالا است.

با این حال مزایای ارزهای مجازی نسبت به سامانه‌های مالی سنتی تلاش‌های رسمی برای به حاشیه کشاندن آن را تا حدودی ناکام کرده است. از جمله مزایای ارزهای مجازی را می‌توان

۱. در این زمینه مصداق بارز ارزهای مجازی یعنی بیت کوین به عنوان رمزارزی جهان‌روا مدنظر است؛ زیرا برخی رمزارها از قابلیت‌های محدودتری برخوردار هستند. در خصوص ارزهای مجازی از حیث تاریخی باید سابقه آن را از سال ۱۹۹۸ بررسی کرد. در این سال، به منظور تسهیل انجام امور مالی و ایجاد پولی بدون واسطه بانک‌ها و توسط افراد یک جامعه، گام نخست توسط وی دای (Wei Dai) برداشته شد. او پیشنهاد نوع جدیدی از پول الکترونیک را ارائه داد که از روش رمزگذاری رایانه-ای برای کنترل تولید پول و انجام معاملات بدون واسطه و مرجع مرکز استفاده شود (Raskin, 2013). با این حال، ایده «وی دای» تا سال ۲۰۰۹-۲۰۰۸ تنها در حد یک نظریه باقی ماند تا اینکه در این سال یک واحد پول مجازی به نام بیت کوین (Bit coin) به عنوان نمونه عملیاتی و موفق این ایده پدیدار شد (Seyed Hosseini & Doaei, 2014: 10). بیت کوین از زمان پیدایش، به عنوان یک ارز مجازی الهام‌بخش و باعث انتشار تعداد زیادی ارزهای رمزپایه همچون Acebucks, Linden Dollars, WoW Gold, QBCoin شده است (Liu, et al., 2020:299).

۲. با این وجود در سطح ملی و منطقه‌ای برخی کشورها در صدد ایجاد رمزارهایی با پشتوانه‌های مادی، از جمله طلا، نفت یا پول‌های ملی خود، هستند.

کاهش هزینه معاملات، دسترسی آسان و تسهیل مبادلات، افزایش حریم خصوصی و کاهش فشار تورمی دانست که تمایل به استفاده از آن را افزایش داده است (Miri؛ Doguet, 2013:1119).^۱ مواردی که در کنار دلایلی چون بی‌اعتمادی عمومی نسبت به نظام پولی موجود در سطح ملی و فراملی، گریز از دخالت مقامات و نهادهای مرکزی، مانند سیستم بانکی یا دولت‌ها و دخالت کشورهای صاحب نفوذ و قدرت همچون آمریکا در سطح بین‌المللی دانست، زمینه‌ساز توسعه این فن آوری شده است (Wood & Buchanan, 2015:392).

مزایای مذکور در کنار تمامی کارکردهای مثبت، در بردارنده چالش‌هایی پیش روی متولیان و کنشگران نظام عدالت کیفری بوده است. در این چارچوب جذابیت‌های ارزشهای مجازی فرصتی را برای بزهکاران ایجاد کرده است تا فعالیت‌های مجرمانه خود را با سهولت و امنیت بیشتر انجام دهند. افرادی که به عنوان اشخاص خطرناک یا با ریسک بالا در جامعه شناخته می‌شوند غالباً از خدمات و ابزار مالی سنتی استفاده نمی‌کنند و برای انتقال وجوه غیرقانونی یا خرید کالا و خدمات از بازارهای مجرمانه، تمایل به استفاده از ابزارهایی با ضریب امنیت بالا دارند (Brenig, et al., 2015: 8)؛ بنابراین، علی‌رغم تمام مزایای استفاده از ارزشهای مجازی نباید خطرات احتمالی مرتبط با آن و خصوصاً موارد مجرمانه را فراموش کرد؛ زیرا رمز ارزها با داشتن برخی مزایا به‌طور فعال در انجام اعمال مجرمانه هم کاربرد دارند. از این رو، جنبه‌های مجرمانه رمز ارزها را می‌توان تهدیدی

۱. علی‌رغم این مزایا، در ابتدا بسیاری از دولت‌ها نسبت به پذیرش این نوع ارزها مقاومت و برخوردهای متناقضی نشان دادند؛ اما پس از مدتی، ارزشهای مجازی توجه سیاست‌مداران و مردم را شدیداً به خود جلب کرد. در سال‌های اخیر دولت‌هایی مانند ونزوئلا، ایران، روسیه و کره شمالی که موضوع تحریم‌های ظالمانه از سوی سازمان‌ها و کشورهای مختلف به ویژه آمریکا قرار گرفته‌اند، به منظور دور زدن این تحریم‌ها و مقابله با بی‌ثباتی مالی ناشی از تحریم‌های تجاری، به عنوان یک راه جایگزین، تلاش خود را بر روی توسعه ارزشهای مجازی متمرکز کرده‌اند (Kirkpatrick, et al., 2019:40-42). به عنوان مثال، دولت ونزوئلا در اوایل سال ۲۰۰۸ ارز مجازی به نام پترو (Petro) را تحت حمایت خود توسعه داد (Panda, 2018)؛ زیرا برای بسیاری از این کشورها ارزشهای مجازی راهی برای رهایی از تسلط ایالت متحده و رهایی از اتکا به پول رایج این کشور و همچنین وسیله‌ای برای ملت‌ها جهت به دست آوردن مجدد حاکمیتشان است (O'Keeffe, 2018)؛ Naderi & Shahir, 2018: 89). علاوه بر دولت‌های تحت تحریم، شهروندان آن‌ها نیز ترجیح می‌دهند پول خود را برای خرید ارزشهای مجازی مبادله کنند، زیرا مبادله و خرید دلار آمریکا بسیار دشوار است (Turpin, 2014: 352). تلاش‌هایی نیز در ایران جهت ایجاد رمز ارز منطقه‌ای با مشارکت برخی کشورهای منطقه آغاز شده که مراحل تحقیقاتی خود را سپری می‌کند.

علیه نظام عدالت کیفری دانست.^۱

بدین ترتیب، با وجود برخی پژوهش‌ها که از ابعاد فقهی، حقوقی و کیفری به تحلیل ارزشهای مجازی پرداخته‌اند (Kheradmand, 2019؛ Mahmoudi, 2019؛ Roshan, et al., 2019؛ Shamloo & Khalili Paji, 2020)، اهمیت روز افزون این ارزشها از منظر جنایی، بررسی ابعاد جرم‌شناختی آن را اجتناب‌ناپذیر کرده است. بدین سان در نوشتار حاضر، گستره فعالیت‌های مجرمانه مرتبط با ارزشهای مجازی، ویژگی‌های جذاب بزهکارانه این فن‌آوری و تحلیل علت‌شناسی جرم‌شناختی و ارائه راهکارهای پیشگیرانه در برابر مخاطرات جنایی ارزشهای مجازی بر مبنای برخی نظریه‌های موجود با روشی توصیفی و تحلیلی مورد بررسی قرار گرفته است تا بدین وسیله نگاهی جامع از حیث جرم‌شناختی، به عنوان یکی از ابعاد مهم ارزشهای مجازی، حاصل شود.

الف: گستره فعالیت‌های مجرمانه مرتبط با ارزشهای مجازی

طیف گسترده‌ای از جرائم با استفاده از ارزشهای مجازی قابل ارتکاب هستند که در این قسمت برخی از رایج‌ترین آن‌ها توضیح داده شده است. لازم است تأکید گردد که این نمونه‌ها انحصاری نبوده و شاید بتوان موارد دیگری را نیز به آن‌ها افزود. پول‌های مجازی در زمینه صنعت فیلم‌های مستهجن، قاچاق غیرقانونی داده‌های شخصی، فروش اسناد جعلی، قاچاق غیرقانونی مواد مخدر و حتی برای قتل‌های نیابتی^۲ با استخدام قاتلان حرفه‌ای پرداخت می‌شود؛ اما در عین حال، قاچاق غیرقانونی مواد مخدر و روان‌گردان گسترده‌ترین بخش فعالیت‌های مجرمانه با استفاده از رمزارزها

۱. ارزشهای مجازی از حیث خرید کالاها و خدمات غیرقانونی و به طور کلی انجام فعالیت‌های مجرمانه از ظرفیت‌های بالقوه بسیاری برخوردارند. در این میان، هرچه مشاغل ارزشهای مجازی را بیشتر بپذیرند، فرصت بیشتری برای بزهکاران فراهم می‌شود تا تجارت مجرمانه خود را به صورت برخط انجام دهند. برای مثال، در پژوهشی در روسیه مشخص شده در پایان سال ۲۰۱۸، بازار فعالیت‌های غیرقانونی با استفاده از فن‌آوری رمزارزها از جمله بیت‌کوین تقریباً ۷۶ میلیارد دلار بوده است که تقریباً با حجم بازارهای قاچاق مواد مخدر در آمریکا و اروپا برابری می‌کند (www.group-ib.ru/media/gib-cryptosummary). تاکنون کشورهای مختلفی اقدام به ارائه گزارش در خصوص وقوع جرم با استفاده از ارزشهای مجازی پرداخته‌اند؛ هند (۱۰ مورد)، کره جنوبی (۸ مورد)، ژاپن (۵ مورد) و تایلند (۴ مورد). در میان کشورهای اروپایی، انگلستان با (۶ مورد) و در میان کشورهای آمریکای شمالی نیز، کانادا با (۵ مورد) بیش‌ترین تعداد را گزارش داده‌اند (Kethineni & Cao, 2019:10).

۲. منظور قتل‌هایی است که شخصی به دیگری پول داده و اصطلاحاً او را اجیر می‌کند تا شخص ثالثی را بکشد.

است (Ivantsov, et al., 2019: 87). در حقیقت، امروزه در کنار روش‌های سنتی فروش مواد مخدر، روش‌های جنایی جدید برای فروش این مواد، یعنی فروش از راه دور و با استفاده از ارزهای مجازی روز به روز در حال افزایش است. براساس داده‌های مربوط به اوایل سال ۲۰۱۹ در روسیه اکثر اقدامات مجرمانه با رمزارزها در حیطه خرید و فروش مواد مخدر و روان‌گردان بوده و در ردیف بعدی خرید محتوای مستهجن قرار می‌گیرد.^۱

بعد از قاچاق و فروش مواد مخدر، دومین حوزه مهم در استفاده مجرمانه از ارزهای رمزپایه، پولشویی منافع حاصل از جرم است. با توجه به افزایش حجم ارزهای رمزپایه در فضای مجازی، برای کسانی که فعالیت پولشویی را انجام می‌دهند سازوکارهای کیفی جدیدی برای تطهیر درآمدهای مجرمانه در اختیارشان قرار می‌گیرد (Ivantsov, et al., 2019: 89). اگر روند استفاده از ارزهای مجازی در فرایند پولشویی همچنان ادامه یابد آینده خوبی پیش‌بینی نمی‌شود، زیرا درنهایت استفاده غیر قانونی و غیر اخلاقی از ارزهای مجازی می‌تواند ثبات اقتصاد جهانی را تضعیف کند (Albrecht, et al., 2019: 214).

بعد دیگر استفاده از ارزهای مجازی در عملیات مجرمانه، استفاده از آن در فعالیت ناظر به طرح پونزی (Ponzi Schemes) است (Simser, 2015: 165).

استفاده از ارزهای مجازی در فعالیت‌های مربوط به قمار و شرط‌بندی نیز در حال افزایش است. برای مثال، بررسی‌های قوه قضاییه و بازجویی از فعالان بازداشت‌شده در حوزه شرط‌بندی، به ویژه در فضای مجازی، حاکی از آن است که بسیاری از سایت‌های شرط‌بندی و قمار که توسط برخی اشخاص معروف در نرم‌افزار اینستاگرام و فعالان حوزه شرط‌بندی هدایت می‌شود، از ارزهای مجازی در پیشبرد فعالیت مجرمانه خود، یعنی شرط‌بندی استفاده می‌کنند.^۳

1. www.inhope.org/tns/resources/statistics

۲. طرح پونزی یک سرمایه‌گذاری فریبکارانه است. در این طرح سودهایی که به سرمایه‌گذاران برگردانده می‌شود از بهره‌های متعارف به طور غیرعادی بالاتر است. این طرح بجای آن که سودی از فعالیت‌های اقتصادی واقعی به سرمایه‌گذاران پرداخت کند از پول خودشان یا از پول دیگر سرمایه‌گذاران به آن‌ها سود پرداخت می‌کند (بنگرید: www.iranhoshdar.ir).

۳. Pouyan Mokhtari arrested / Interpol will extradite Pouyan Mokhtar to Iran after his arrest
?, News ID: 78885, dated 10/5/2020. In: www.saednews.com

افزون بر موارد فوق، یکی دیگر از فعالیت‌های مجرمانه‌ای که با استفاده از ارزشهای مجازی صورت می‌گیرد تأمین مالی فعالیت‌های تروریستی است، اگرچه در حال حاضر در این حوزه رمزارزها کاربرد زیادی ندارند و همچنان این دسته از مجرمان بیشتر از ارزشهای واقعی و رایج استفاده می‌کنند (Khalili Paji, 2019: 115)؛ با این وجود، با توسعه روز افزون رمزارزها، پول-های مجازی هم می‌تواند به‌طور فزاینده‌ای برای تأمین مالی تروریسم مورد استفاده قرار بگیرد (Goldman, et al., 2017: 22-24). در این خصوص دولت اندونزی ادعا کرده که شبه‌نظامیان اسلامی از ارزشهای مجازی برای تأمین مالی فعالیت‌های تروریستی خود استفاده می‌کنند (Lester, 2017). همچنین گزارش شده که ارسال پول به گروه‌های تروریستی در سوریه به صورت ارزشهای مجازی انجام می‌شود (Naheem, 2018: 571). علاوه بر این، مدارک و شواهدی دال بر استفاده گروه تروریستی داعش از ارزشهای مجازی وجود دارد. گروه رایانه‌ای و ضد تروریستی هکتیویست (Hacktivist) در سال ۲۰۱۵ اعلام کرد زنجیره‌ای از معاملات بیت‌کوین را که گفته می‌شود توسط داعش اداره می‌شود به ارزش میلیون‌ها دلار شناسایی کرده است (Kfir, 2020:119).

بنابراین، رمزارزها یا به‌طور مستقیم برای دستیابی به یک نتیجه مجرمانه، همانند خرید اقلام ممنوعه استفاده می‌شوند و یا در تسهیل ارتکاب جرم مورد استفاده قرار می‌گیرند؛ مانند پول‌شویی. گاهی اوقات هم‌ارزهای مجازی می‌توانند به عنوان موضوع جرم باشند، مانند استفاده از رمزارزها در جرم دادن و دریافت رشوه و واسطه‌گری در دریافت رشوه. با توجه به ناشناس بودن معاملات با استفاده از رمزارزها این شکل از پرداخت غیرقانونی پاداش یا همان دادن و دریافت رشوه بسیار جذاب است.

در برخی موارد دیگر رمزارزها موضوع جرم سرقت قرار گرفته‌اند. اگرچه از حیث شناسایی قانونی و به تبع آن به رسمیت شناختن ماهیتی مشخص برای ارزشهای مجازی بسیاری از کشورها اقدامات مؤثری انجام نداده‌اند، اما نمی‌توان ارزشمندی این فن‌آوری را نادیده انگاشت و با ایجاد ابهام در مالیت داشتن آن امکان انتساب جرم سرقت را علیه ربایندگان آن کتمان کرد (Mahmoudi, 2019: 512؛ Korennaya & Tydykova, 2019: 412-413).

ارزهای مجازی همچنین می‌توانند به عنوان هدف یا ابزاری برای ارتکاب جرائم مربوط به ورشکستگی مورد استفاده قرار بگیرند. با توجه به اینکه در حال حاضر معاملات و خرید رمزارزها

توسط نهادهای دولتی کنترل نمی‌شود، بنابراین شخص قبل از آغاز ورشکستگی خود این حق را دارد تا با پول خویش ارزشهای مجازی خریداری کند و پس از آن این پول را تبدیل به ارز رایج و واقعی نماید یا مالکیت مال خاصی را به دست آورد (Sereda, 2017:60).

علاوه بر ارتکاب جرائم از طریق رمزارزها در فضای مجازی، امروزه بسیاری از جرائم مربوط به این نوع ارزها در حال گسترش و انتقال از فضای مجازی به فضای حقیقی هستند. اخاذی و درخواست پول بعد از آدم‌ربایی از جمله جرائمی هستند که در فضای حقیقی ارتکاب می‌یابند، اما بزهکار ممکن است بزه‌یده را مجبور به انتقال پول به صورت ارز مجازی نماید. در واقع از آنجاکه تعداد و تنوع ارزشهای مجازی در دنیای واقعی در حال افزایش هستند و همچنین با توجه به افزایش سریع قیمت رمزارزها، این نوع ارزشهای مجازی نه تنها در دنیای مجازی، بلکه در دنیای واقعی نیز برای بزهکاران جذاب هستند (Kethineni & Cao, 2019:12).

حال سؤال مهم این است، چه ویژگی‌های جذابی در ارزشهای مجازی وجود دارد که سبب می‌شود بزهکاران در انجام فعالیت‌های مجرمانه، تمایل به استفاده از این گونه ارزها داشته باشند. امری که در ادامه مورد بررسی قرار می‌گیرد.

ب: ویژگی‌های جذاب بزهکارانه ارزشهای مجازی

پیش از تحلیل جرم‌شناختی کارکرد مجرمانه ارزشهای مجازی، شناخت ویژگی‌های جذاب آن برای بزهکاران در اولویت قرار دارد. برخی از این ویژگی‌ها مربوط به ذات ارزشهای مجازی و برخی دیگر مربوط به ملاحظات حقوقی پیرامون این فن‌آوری است.

۱. جذابیت‌های ذاتی ارزشهای مجازی

به‌طور سنتی پژوهش‌های صورت گرفته پیرامون فضای مجازی از حیث حقوقی و جرم‌شناختی بیان‌گر وجود ویژگی‌هایی است که این فضا را همواره بستری مناسب برای ارتکاب جرم قرار داده است. ارزشهای مجازی به عنوان یک ابزار فن‌آورانه در بستر فضایی مجازی مورد استفاده قرار می‌گیرند. در این راستا، ویژگی‌های منحصر به فرد این فن‌آوری و ترکیب آن با برخی فن‌آوری‌های دیگر در بستر فضای مجازی موجب ایجاد جذابیت‌های مضاعفی شده که توجه بزهکاران را بیش از پیش به خود جلب کرده است. بر این اساس، از حیث ذاتی ارزشهای مجازی از ویژگی‌های ذیل

برخوردار هستند:

- نخست؛ انعطاف‌پذیری در هویت. انعطاف‌پذیری هویت از جذاب‌ترین عواملی است که سبب جلب توجه مجرمان به ارزهای مجازی می‌گردد. امری که اگرچه جزئی از ویژگی‌های ذاتی فضای مجازی است اما در چارچوب ارزهای مجازی تشدید شده است. بررسی انعطاف‌پذیری هویت از چند بعد قابل توجه است. نخست اینکه تمام بزهکاران برخلاف از هویت جعلی استفاده می‌کنند. امری که در پرونده مشهور ارزهای مجازی، یعنی پرونده جاده ابریشم نیز به وضوح دیده می‌شود. برای مثال، دانشگاه فروشنده مواد مخدر در این پرونده از نام «XX» و «Xanax king» و فیلا، فروشنده بیت‌کوین از عنوان «BTC King» به عنوان هویتی برای خود استفاده می‌کردند. دوم، بزهکاران با به کار بستن ارزهای مجازی می‌توانند از بیش از دو هویت استفاده کنند. به عنوان مثال، رأس اولبریچ، مالک جاده ابریشم، از هویت‌های «DPR»، «Pirate Dread Roberts» یا «Silk Road» به عنوان نام کاربری خود استفاده می‌کرد؛ و سوم، ارزهای مجازی این امکان را برای بزهکاران فراهم می‌کند تا مکرراً هویت خود را تغییر دهند. انعطاف‌پذیری در هویت باعث سردرگمی مأموران مجری قانون در شناسایی و کشف بزهکاران دخیل در تشکیلات مجرمانه مربوط به ارزهای مجازی می‌شود. در کنار ویژگی انعطاف‌پذیری هویت، عامل دیگری که باعث می‌شود کاربران مجرم ارزهای مجازی را بیش از پیش از دسترس کنشگران نظام عدالت کیفری دور کند، افزایش مشارکت کنندگان برخوردار از هویت‌های چندگانه و جعلی است (Shamloo & Khalili Paji, 2020: 59-63).

- دوم؛ ناشناختگی هویت. دلیل دیگر گرایش بزهکاران برای انتخاب ارزهای مجازی، ناشناس بودن معاملات مبتنی بر رمزارزها است؛ چراکه شناسایی طرفین معامله غیر قانونی بسیار دشوار است. دشوار بودن شناسایی معاملات مبتنی بر ارزهای مجازی به سه علت است. اول اینکه ارزهای مجازی ماهیت فراملی دارند و معاملات مبتنی بر این گونه ارزها محدود به مرزهای دولتی و ابزارهای کنترل مالی نیست (Brown, 2016: 336). دوم اینکه، ارزهای مجازی تنها یک شماره دیجیتال دارند و نیازی به نگهداری آن‌ها در فضای حقیقی نیست. هنگامی که این رمزارزها از پرداخت کنندگان به متقاضیان منتقل شود، اگرچه اطلاعات مربوط به فرستنده، گیرنده و مبلغ معامله برای عموم قابل مشاهده است اما هویت واقعی کاربران در

دسترس قرار ندارد و ناشناخته باقی می ماند (Kethineni, et al., 2018: 150). عامل دیگری که چنین دشواری را سبب می شود، وجود نداشتن یک هسته یا نهاد مرکزی کنترل کننده بر روی ارزشهای مجازی است. تلاش‌ها برای ایجاد چنین هسته کنترلی هم تا به امروز بی نتیجه بوده است (Brown, 2016: 336). ناشناس بودن معاملات مبتنی بر ارزشهای مجازی، ردیابی این نوع معاملات را پیچیده کرده، اثبات منشأ ارزشهای مجازی را بسیار چالش برانگیز می کند و امنیت بالایی در انتقال و خرید ارزشهای مجازی برای بزهکاران ایجاد می کند. بدین ترتیب، هزینه ارتکاب جرم کاهش می یابد و با کاهش خطر برای بزهکاران، امکان وقوع جرم در این بستر افزایش خواهد یافت.

– سوم؛ سهولت شرکت در عملیات مجرمانه. برای انجام فعالیت‌ها و معاملات با ارزشهای مجازی به هیچ نهاد مرکزی یا بانکی که معاملات را مدیریت کند، نیاز نیست و صدور آن به صورت جمعی و توسط شبکه انجام می شود. طراحی ارز مجازی عمومی است و هیچ کس صاحب یا کنترل کننده آن نیست و همه می توانند با آن کار کنند. معاملات مبتنی بر ارز مجازی امن و برگشت ناپذیر است و اطلاعات حساس یا شخصی مشتری را ذخیره نمی کند. نتیجه این سهولت در استفاده از ارز مجازی در فعالیت‌ها، امکان اتحاد فراملی برای ارتکاب جرم است. بزهکاران می توانند در کشورهای مختلف زندگی کنند و یک تجارت مجرمانه را از طریق ارزشهای مجازی اداره نمایند. در حقیقت، ارزشهای مجازی برخلاف ارزشهای رایج و سنتی برخوردار از ویژگی پویایی فضایی هستند. چنان که بررسی‌ها نشان داده متهمان برخی پرونده‌های مربوط به ارزشهای مجازی در کشورهای مختلف مانند آمریکا و تایلند ساکن بودند و از راه دور در انجام فعالیت‌های مجرمانه با استفاده از ارزشهای مجازی با یکدیگر مشارکت داشتند (Kethineni, et al., 2018:149). همچنین، در نمونه‌ای دیگر، شخصی به نام علی شکری امین (United States of America v. Ali Shukri Amin, 2015)، با استفاده از رسانه‌های اجتماعی مجازی، برای تأمین مالی داعش از افراد درخواست ارز مجازی می کرد.^۱ بدین سان، پویایی فضایی و امکان بزه دیده نمودن اشخاص از راه دور و

1 . www.extremism.gwu.edu

به‌طور کلی سهولت شرکت در عملیات مجرمانه با استفاده از ارزشهای مجازی باعث شده که این نوع ارزشها به عنوان جایگزینی مطمئن برای نظام‌های مالی و سامانه‌های پرداخت سنتی مطرح شوند. پدیده‌ای که در عمل ارتکاب جرم را تسریع می‌کند و ریسک کشف آن را برای بزهکاران کاهش می‌دهد.

۲. خلأهای حقوقی و ایجاد جذابیت‌های مضاعف

ارزشهای مجازی از حیث حقوقی در بردارنده ملاحظاتی هستند که عدم توجه و پاسخ‌دهی مناسب به آن می‌تواند در نهایت منجر به تقویت جنبه‌های جنایی این فن‌آوری و افزایش جذابیت آن برای بزهکاران شود.

بعد نخست این موضوع مربوط به رویکرد حقوقی کلان نسبت به ارزشهای مجازی است که تاکنون توسط بسیاری کشورها بدون پاسخ گذاشته شده است. برخلاف برخی کشورها که اقدام به ممنوعیت استفاده یا مجاز دانستن استفاده از ارزشهای مجازی در ساختارهای پولی و مالی ملی نموده‌اند و از منظر حقوقی تکلیف را برای تابعان آن مشخص کرده‌اند، اما همچنان یکی از مهم‌ترین چالش‌های حقوقی ارزشهای مجازی مشخص نبودن وضعیت قانونی استفاده از آن است. این امر زمانی از اهمیت بیشتری برخوردار می‌شود که ویژگی فرامرزی و جهانی ارزشهای مجازی را مدنظر قرار دهیم. بر این اساس، قابلیت استفاده از آن برای ارتکاب جرائم فراملی به گونه‌ای که هر قسمت از جرم در نقطه و کشوری خاص اتفاق افتد، چنانچه با روشن نبودن وضعیت حقوقی در برخی مناطق همراه شود بیش از پیش می‌تواند منجر به ایجاد مانع در اقدامات تعقیبی و تحقیقی شود.

اقدامات غالب کشورها در حال حاضر بدون ایجاد ساختار حقوقی مناسبی جهت پاسخ‌دهی به تمامی ابعاد ارزشهای مجازی، به اعلام توصیه‌هایی توسط بانک‌های ملی در خصوص معاملات مشتریان با استفاده از ارزشهای مجازی محدود شده است. بانک‌ها به مردم توصیه می‌کنند که رمزارزها را به عنوان ابزار مالی پرخطر در نظر بگیرند (Dorofeeva, et al., 2019: 887). برای مثال، بانک مرکزی ایران در دی ماه ۱۳۹۶، موضوع ممنوعیت به کارگیری ارزشهای مجازی را، با توجه به اینکه این نوع ارزشها از این قابلیت برخوردار هستند که به ابزاری برای پول‌شویی و تأمین

مالی تروریسم و به‌طور کلی، جابه‌جایی منابع پولی مجرمان بدل شوند، به بانک‌ها ابلاغ کرد. به دنبال این دستورالعمل، بانک‌ها، مؤسسات اعتباری و صرافی‌ها از خرید و فروش ارزهای مجازی منع شدند و هیچ اقدامی از سوی آن‌ها در جهت تبلیغ ارزهای مجازی نباید انجام می‌شد.^۱

بعد دوم این امر این است که با وجود تعیین تکلیف حقوقی از حیث مجاز یا غیرمجاز بودن استفاده از ارزهای مجازی، در بسیاری از کشورها تاکنون در خصوص ماهیت حقوقی ارزهای مجازی تعیین تکلیف نشده است. به‌طور کلی ارزهای مجازی را می‌توان پول، سامانه پولی، ارز خارجی یا کالا دانست. طبیعی است شناسایی هر یک از موارد مذکور در مشخص شدن سایر ابعاد حقوقی و قابلیت شمول قوانین موجود بر آن یا لزوم وضع قوانین جدید ضروری است. برای مثال از حیث قوانین مالیاتی مهم است که مشخص شود توصیف قانون‌گذار از ارزهای مجازی چیست؛ آن‌ها را کالا می‌داند یا پول؛ زیرا در هر یک از فروض احکام مالیاتی متفاوتی بر این فن‌آوری بار خواهد شد. با این حال، از آنجاکه ارزهای مجازی در بسیاری از کشورها به دلیل فقدان قوانین و مقررات مربوط، دارایی محسوب نمی‌شوند، معاملات مبتنی بر آن‌ها مشمول قوانین مالیاتی قرار نمی‌گیرد. عدم وجود مقررات مالیاتی در معاملات، سبب عدم کنترل و نظارت می‌شود و این عدم کنترل منجر به افزایش احتمال استفاده از رمزارزها به عنوان وسیله‌ای مناسب و کم‌خطر برای پول-شویی می‌شود (Apriliani, 2019: 37).

بدین سان، به رسمیت شناخته نشدن ارزهای مجازی همانند پول و ارزهای واقعی در قوانین مدنی، پولی و بانکی اکثر کشورها، به عنوان یک‌کشی و دارایی ارزشمند می‌تواند چالش‌هایی را به همراه داشته باشد. این امر موجب می‌شود آن‌ها تحت نظارت نظام بانک‌داری قرار نگیرند و چون تحت نظارت قرار نمی‌گیرند معاملات غیرقانونی در چارچوب استفاده از آن‌ها نیز از پایش‌های موجود؛ مانند ارائه گزارشات عملیات مشکوک، خارج می‌شود (Dyson, et al., 2019:1). در حقیقت، به دلیل ماهیت مالی نداشتن و ساختار غیرمتمرکز ارزهای مجازی، هیچ‌گونه وظیفه نظارتی و گزارشگری مربوط به نظام ارزهای مجازی وجود ندارد و هر فردی به‌طور مستقیم و بدون نظارت شخص ثالث یا بانک مرکزی معاملات خود را انجام می‌دهد. درحالی‌که بانک‌ها

1 . www.cbi.ir/showitem

باید به مقامات گزارش دهند و عملیات بانکی آن‌ها از نزدیک تحت نظارت باشد (Boehm & Pesch, 2014: 47).

همچنین، در مواردی که معاملات غیر قانونی یا تحقق جرمی با استفاده از ارزهای مجازی کشف شود متهم می‌تواند ادعا نماید که جرم اتهامی واقع نشده، چراکه ارزهای مجازی از منظر قانونی دارای ماهیت مالی نیستند؛ بنابراین، همان‌گونه که با جرائم ارتكابی از طریق ارزهای رایج و سنتی برخورد می‌شود، در برابر جرائم ارتكابی از طریق ارزهای مجازی نمی‌توان واکنش کیفی نشان داد. برای مثال در پرونده آلبرشت (In the united states of America v. Ulbricht) در سال ۲۰۱۴ در ایالت متحده آمریکا، متهم ادعا کرد که ارزهای مجازی همچون (BTC) پول نیستند و بنابراین معاملات با آن هم شامل پول‌شویی و قوانین مربوط به آن نمی‌شود. با این وجود، قضات متهم را محکوم به جرم پول‌شویی کردند (Higgins, 2016). قضات این پرونده و همچنین برخی حقوقدانان معتقدند برای جلوگیری از این امر، یعنی فرار اشخاصی که از ارزهای مجازی برای فعالیت‌های مجرمانه همچون پول‌شویی استفاده می‌کنند، ارزهای مجازی باید مشمول قوانین ناظر به پول‌شویی باشند؛ زیرا چارچوب حقوقی قوانین ناظر به پول‌شویی به اموال ناشی از فعالیت‌های مجرمانه باز می‌گردد. چنین اموالی به هر نوع دارایی اعم از مادی یا غیرمادی، منقول یا غیرمنقول، ملموس یا غیرملموس و اسناد حقوقی در هر شکلی از جمله الکترونیکی و دیجیتال اطلاق می‌گردد. براساس این تعریف گسترده از مال در قوانین و اسناد مربوط به پول‌شویی معلوم می‌شود چارچوب حقوقی پول‌شویی صرفاً بر روی پول به معنای دقیق کلمه، یعنی اسکناس‌های سنتی متمرکز نیست، بلکه ارزهای مجازی هم می‌توانند به عنوان دارایی غیرقانونی در نظر گرفته شوند. اگر از این تفسیر پیروی شود این چارچوب قانونی می‌تواند برای ارزهای مجازی حاصل از فعالیت‌های مجرمانه نیز اعمال شود (Vandezande, 2017: 349).

بدین‌سان، خلأ قانونی مربوط به ارزهای مجازی منجر به افزایش خطرات استفاده از آن‌ها و در نتیجه عدم تمایل ساختارهای صنعتی و مالی بزرگ برای معرفی این فناوری در فرآیندهای تجاری خود می‌شود. برخی محققان استدلال می‌کنند که به رسمیت نشناختن رمزارزها در نظام حقوقی موجب نقض منافع دولتی و عمومی می‌شود؛ زیرا به شرکت‌کنندگان بی‌پروا و بی‌توجه نسبت به درست و نادرست بودن عملیات اقتصادی آنان، این اجازه را می‌دهد تا معاملات غیرقانونی انجام دهند و دارایی‌های خود را مخفی کنند (Korennyaya & Tydykova, 2019).

409)؛ بنابراین، به رسمیت نشناختن رمز ارزها در نظام حقوقی و خلأ قانونی باعث شده که ارزهای مجازی به عنوان ابزارهای مالی جدید بیشترین محبوبیت خود را در حوزه جنایی همانند فساد، قاچاق مواد مخدر و مواد روان گردان به دست آورد. این امر، یعنی خلأ قانونی عمدتاً به دلیل عدم درک اهمیت ارزهای مجازی از حیث اقتصادی و ظرفیت‌های جنایی این گونه ارزها توسط برخی کارشناسان داخلی و بین‌المللی است (Ivantsov, et.al, 2019: 86-87) که زمینه را برای بزهکاران و ارتکاب فعالیت‌های مجرمانه گوناگون همچون پول‌شویی، قاچاق مواد مخدر و دیگر جرائم سازمان‌یافته با استفاده از ارزهای مجازی فراهم می‌کند (Lockett, 1999: 239).

پ: ارزهای مجازی و جرم؛ تحلیل جرم‌شناختی و راهکارهای پیشگیرانه

به‌طور کلی و در چارچوب برخی نظریات جرم‌شناسی می‌توان به تحلیل علت‌شناسانه بزهکاری در پرتو ارزهای مجازی و ارائه راهکارهایی پیرامون پیشگیری از آن پرداخت. در این زمینه برخی نظریه‌های سنتی مانند نظریه معاشرت ترجیحی^۱ و نظریه فنون خنثی‌سازی^۱ می‌توانند از کارکردهایی

۱. نظریه معاشرت‌های ترجیحی ساترلند نشان می‌دهد که رفتارهای بزهکارانه، صرف نظر از فنون یا انگیزه‌های آن، از طریق تعامل با گروه‌های شخصی صمیمی آموخته می‌شود (Wald, et al., 2009: 252). این نظریه در توجیه جرائم رایانه‌ای نیز کاربرد دارد، به ویژه که هم‌نشینی و تبادل اطلاعات بین افراد آشنا و حتی ناآشنا از طریق فضای مجازی خیلی ساده‌تر و گسترده‌تر انجام می‌شود و تأثیرگذاری آن بر دیگران نیز بیشتر می‌شود. به عنوان مثال، هکرهای رایانه‌ای ممکن است به صورت آنلاین یا تلفنی باهم ارتباط برقرار کنند و انگیزه و رفتارهای مجرمانه را از یکدیگر یاد بگیرند (Kethineni, et al., 2018: 145). در مورد ارزهای مجازی نیز بزهکارانی که از این نوع ارزها برای ارتکاب فعالیت‌های مجرمانه خود استفاده کرده و به سهولت و امنیت استفاده از آن‌ها نسبت به ارزهای واقعی در انجام فعالیت‌های مجرمانه پی برده‌اند، با گروه‌های دوستان در فضای مجازی یا حقیقی از مزیت استفاده از ارزهای مجازی سخن می‌گویند و همین امر باعث می‌شود تا دیگران که در ارتباط با آن‌ها هستند به آغاز و یا استمرار فعالیت‌های مجرمانه با استفاده از رمزارزها تشویق شوند؛ زیرا در نتیجه ارتباط و معاشرت آن‌ها با یکدیگر متوجه می‌شوند علاوه بر سهولت و امنیت، احتمال ردیابی فعالیت‌های مجرمانه با استفاده از ارزهای مجازی نیز کمتر از پول رایج و سود آن فراوان است. برای مثال، بررسی‌ها و تحقیقات انجام شده در پرونده تجارت آنلاین جاده ابریشم نشان داد وقتی بزهکاران اعم از بالفعل یا بالقوه به صورت آنلاین با دوستان ملاقات می‌کردند، تکنیک‌های خاص استفاده از ارزهای مجازی در فعالیت‌های مجرمانه و همچنین یافتن توجیه برای جرائم خود را از یکدیگر در فضای مجازی یاد می‌گرفتند و یکدیگر را در تصمیم‌گیری‌ها و ادامه فعالیت‌های مجرمانه با استفاده از ارزهای مجازی ترغیب می‌کردند (Kethineni, et al., 2018:153).

برخوردار باشند؛ با این حال، آنچه بیشتر در تحلیل‌های جرم‌شناختی به‌طور تخصصی‌تر می‌تواند مورد استفاده قرار گیرد نظریه انتقال فضایی (Space transition theory) و نظریه انتخاب عقلانی است. بدین‌سان، در چارچوب دو نظریه اخیر به تحلیل علت‌شناسی جنایی در پرتو ارزشهای مجازی و راهکارهای پیشگیرانه آن خواهیم پرداخت.

۱. تحلیل جرم‌شناختی ارزشهای مجازی

تحلیل جرم‌شناختی ارتکاب جرم در چارچوب ارزشهای مجازی از دو بعد قابل بررسی است. نخست در خصوص اشخاصی که در خارج از فضای مجازی به عنوان اشخاص قانون‌مدار شناخته می‌شوند ولی ویژگی‌های منحصربه‌فرد فضای مجازی کشش‌های درونی بزهکارانه و غالباً سرکوب شده آن‌ها را برمی‌انگیزد و در نتیجه در بستر فضای مجازی مرتکب جرم می‌شوند. چنین اعمال مجرمانه‌ای در فضای مجازی، بیش از هر نظریه دیگری، در چارچوب نظریه «انتقال فضایی» قابل تحلیل است و به تبع آن ارزشهای مجازی، به عنوان یک ابزار فن‌آورانه مجازی، نیز تحت شمول

۱. نظریه فنون خنثی‌سازی سایکس (Sykes) و ماتزا (Matza) بر این مبنا استوار است که بزهکاران یک مجموعه متمایز از توجیهات را برای رفتارهای غیر قانونی‌شان به کار می‌برند. این روش‌های خنثی‌سازی به آن‌ها اجازه می‌دهد به‌طور موقت از قوانین متعادل جامعه دور شوند و در رفتارهای مجرمانه مشارکت کنند (Siegel, 2006: 391). در خصوص مجرمان فضای مجازی هم گفته می‌شود که تمایل به خنثی کردن انگیزه رفتار جنایی خود با عنوان کنجکاوی فکری و تمایل به گسترش مرزهای دانش دارند. حتی در یک مطالعه میدانی در خصوص رفتار مجرمانه هک کردن در بین دانشجویان نشان داده شده که فنون خنثی‌سازی با اشکال خاصی از هک رایانه‌ای ارتباط قابل توجهی دارد (Hutchings, 2016: 126). در مورد جرائم ارتكابی از طریق ارزشهای مجازی نیز می‌توان براساس فنون خنثی‌سازی این گونه جرائم را تا حدودی تحلیل کرد. همان‌طور که قبلاً اشاره شد در مورد ماهیت مالی داشتن و دارایی محسوب شدن یا نشدن ارزشهای مجازی هنوز توافقی حاصل نشده است. این نقطه ضعف ارزشهای مجازی، یعنی منطقه خاکستری وضعیت حقوقی رمزارزها، باعث تشویق بزهکاران به استفاده از این نوع ارزها در انجام فعالیت‌های مجرمانه خویش می‌شود. بزهکاران پس از انجام رفتار مجرمانه مورد نظر، همانند پول‌شویی با استفاده از ارزشهای مجازی این‌گونه خود را توجیه کرده و در دادگاه دفاع می‌کنند که چون ارزشهای مجازی ماهیت مالی ندارند و دارایی به‌شمار نمی‌آیند، پس آن‌ها جرمی در معنای واقعی کلمه را انجام نداده‌اند. ضمن بازجویی از مجرمان پرونده جاده ابریشم نیز مشخص شده که توجیه بزهکاران پرونده این بوده است که به پول‌شویی مشغول نبودند و اصلاً رفتارهای آن‌ها غیرقانونی نبوده است، زیرا رمزارزها پول به رسمیت شناخته شده نیستند و به همین دلیل فرستنده پول هم نبوده‌اند (Kethineni, et al., 2018: 153).

آن قرار می‌گیرد.

دومین بعد، مربوط به ارتکاب جرائم توسط بزهکاران حرفه‌ای است که در تلاش‌اند از تمامی ابزارهای موجود به‌نوعی در راستای ارتکاب اعمال مجرمانه خود بهره ببرند. در این راستا، گسترش فضای مجازی موجب ایجاد تحول در مفهوم و مصداق جرائم و دایره ارتکاب جرم مجرمان حرفه‌ای شده است. با این حال، یکی از چالش‌های این دسته بزهکاران همواره تطهیر و وارد کردن درآمدهای مجرمانه به نظام مالی-اقتصادی رسمی است تا افرون بر گم کردن رد مجرمانه این درآمدها بتوانند از مزایای آن کمال بهره را ببرند. در این راستا می‌توان به‌نوعی کوچ بزهکارانه و شکل‌گیری مفهوم «بزهکاران یقه مجازی» اشاره کرد که در چارچوب «نظریه انتخاب عقلانی» عملکرد آن‌ها تحلیل‌پذیر است.

۱-۱. ارزش‌های مجازی در پرتو نظریه انتقال فضایی

نظریه انتقال فضایی در سال ۲۰۰۸ توسط جیشانکار ارائه شد. این نظریه یکی از نظریات تأثیرگذار در ادبیات جرم‌شناسی و شاید امروزه متداول‌ترین نظریه در زمینه جرائم فضای مجازی باشد. این نظریه ظهور فضای مجازی را به عنوان مکان جدید فعالیت‌های مجرمانه تلقی می‌کند و علت جرائم موجود در فضای مجازی را توضیح می‌دهد (Jaishankar, 2007: 7).

جیشانکار در نظریه انتقال فضایی هفت فرضیه را مطرح کرده که براساس آن‌ها به توضیح جرائم ارتكابی در فضای مجازی می‌پردازد. این هفت فرضیه عبارتند از: ۱- افراد دارای رفتارهای سرکوب شده جنایی در فضای حقیقی تمایل به ارتکاب جرائم در فضای مجازی دارند. ۲- انعطاف‌پذیری هویت، ناشناس بودن و عدم بازدارندگی عوامل تسهیل‌کننده انگیزه مجرمان برای ارتکاب جرائم فضای مجازی هستند. ۳- رفتار مجرمانه احتمالاً از فضای مجازی به فضای حقیقی و برعکس از فضای حقیقی به فضای مجازی وارد می‌شود. ۴- پویایی فضایی در جرائم فضای مجازی به مجرمان اجازه می‌دهد تا از یک سرور یا پروکسی به سرور یا پروکسی دیگر بروند و از راه دور به بزه‌دیده حمله کنند. ۵- احتمال تبانی در فضای مجازی برای ارتکاب جرم در فضای حقیقی وجود دارد. ۶- این احتمال هست که افراد در جامعه بسته نسبت به یک جامعه آزاد بیشتر دست به ارتکاب جرائم مربوط به فضای مجازی بزنند. ۷- تضاد هنجارها و ارزش‌ها در فضای مجازی ممکن است منجر به جرائم سایبری شود (Jaishankar, 2008: 101; Jaishankar, 2019: 101).

(285-295).

در این چارچوب یکی از اساسی‌ترین برداشت‌ها از نظریه مذکور این است: «شخصی که در دنیای واقعی قانون‌مدار است و وضعیت موجود مانعی درونی و بیرونی برای ارتکاب جرم توسط وی فراهم می‌سازد فضای مجازی را بستری مناسب برای به فعلیت رساندن کشش‌های منحرفانه/بزهکارانه خود شناسایی می‌کند و برخلاف دنیای واقعی، در فضای مجازی مرتکب برخی انحرافات/بزهکاری‌ها می‌شود». امری که اگرچه ویژگی نظریه عمومی ارتکاب جرم در فضای مجازی است اما به‌طور خاص در خصوص ارزش‌های مجازی نیز قابل بررسی است.

بدین‌سان آنچه در نظریه انتقال فضایی، پیش از سایر مؤلفه‌ها اهمیت دارد، تمایل و کشش برای ارتکاب جرم است. شخص اگرچه تمایل به ارتکاب جرم دارد اما موقعیت‌های اجتماعی، خانوداگی و... مانع از بروز تمایلات انحرافی می‌شود؛ اما ورود به فضای مجازی به واسطه انعطاف‌پذیری هویت، ناشناس بودن و فقدان بازدارندگی می‌تواند موجب تحقق کشش بزهکارانه شود. براین اساس، ارزش‌های مجازی به واسطه ویژگی‌های منحصربه‌فردی که در چارچوب ناشناختگی و انعطاف هویت ایجاد می‌کنند زمینه را برای ارتکاب جرم فراهم می‌سازند. در واقع شخص با وجود تمایلات مجرمانه خود را بدور از هرگونه کنترل و بازدارندگی ناشی از موقعیت‌های اجتماعی و خانوادگی می‌بیند و رفتار مجرمانه خود را به جای فضای حقیقی، در فضای مجازی مرتکب می‌شود. امری که به واسطه پویایی فن‌آوری ارزش‌های مجازی از چند بعد تسهیل‌کننده ارتکاب جرم است. از سویی، غالب این بزهکاران تمایلی به مواجهه حضوری با بزه‌دیدگان ندارند. براین اساس، ماهیت مجازی این ابزارها زمینه را برای ارتکاب جرائم بدون مواجهه حضوری با بزه‌دیده فراهم می‌سازد. از سوی دیگر، تسهیل ارتکاب جرم یا «ارتکاب جرم از راه دور» می‌تواند زمین‌ساز افزایش گستره جرائم ارتکابی توسط این دسته از بزهکاران باشد.

۱-۲. ارزش‌های مجازی در پرتو نظریه انتخاب عقلانی

برخلاف برخی نظریه‌های جرم‌شناسی که در چارچوب نگاه افتراقی و غیرطبیعی به بزهکار در تلاش‌اند تا او را شخصی متفاوت از سایر اشخاص جامعه نشان دهند، گرایشی در برخی نظریه‌ها وجود دارد که با تأکید بر عدم تفاوت بزهکار از غیربزهکار، سازوکار ارتکاب جرم را متفاوت از سازوکار سایر اعمال نمی‌داند. انسان‌ها مرتکب جرم می‌شوند، به همان دلیل که تحصیلات خود را

ادامه می‌دهند، کار می‌کنند، ازدواج می‌کنند و یا شغل خود را تغییر می‌دهند؛ از این منظر، رفتار مجرمانه، همانند رفتارهای غیرمجرمانه، مبتنی بر عقلانیت و حسابگری انسان و میل او به بهبود وضعیت زندگی خود است و عقل انسان گاهی به وی فرمان ارتکاب جرم می‌دهد، همان‌طور که گاه فرمان به رفتاری غیرمجرمانه می‌دهد (Saboorigour, 2019: 5). بدین سان مطابق این دیدگاه، انتخاب جرم متفاوت از سایر انتخاب‌های انسان نیست و مبتنی بر همان انگیزه‌ها و دلایلی است که سایر رفتارهای انسان را توجیه پذیر می‌کند.

نظریه انتخاب عقلانی کورنیش و کلارک (Cornish & Clarke) بر نوعی عقلانیت در انتخاب آماج مجرمانه قابل دسترس و بی‌خطر از سوی بزهکار برای ارتکاب جرم استوار است. این عقلانیت فرایند تصمیم‌گیری است که فرصت‌ها را برای رفع نیازها، هزینه‌های بالقوه عمل و سودهای پیش‌بینی شده، تعیین می‌نماید. امری که با حرفه‌ای شدن جرم بیش از پیش مدنظر بزهکاران قرار می‌گیرد. بدین ترتیب و در مقام سنجش و ارزیابی فن‌آوری ارزشهای مجازی دلایل ترجیح ارتکاب جرم بر اساس آن را به شرح ذیل می‌توان مورد بررسی قرار داد.

نخست؛ وضعیت قانون‌گذاری پیرامون ارزشهای مجازی همچنان نامشخص و ناقص است. بر این اساس عدم شمول قوانین نظارتی و جرم‌انگار بر این فن‌آوری جذابیت منطقی استفاده از آن را برای بزهکار افزایش می‌دهد؛ زیرا شخص همواره در مقام دفاع می‌تواند از توجیه فقدان قانون برای عملکرد خود استفاده کند.

دوم؛ فقدان نهاد مرکزی و نظارت‌کننده و دور بودن اعمال مبتنی بر ارزشهای مجازی از ثبت سابقه و نماندن ردپایی در یک سامانه نظارتی مشخص دلیل دیگری است که استفاده از ارزشهای مجازی را عقلانی‌تر می‌کند؛ بنابراین، در مقام جمع دو مورد نخست، مجرمان با انگیزه و عدم حضور نگهبانان توانا (یعنی فقدان قوانین و مقررات، عدم نظارت توسط یک نهاد مرکزی)، بزهکاران را به حرکت از استفاده از ابزار مالی سنتی به سوی این ابزار مالی جدید، یعنی ارزشهای مجازی سوق می‌دهد (Kethineni & Cao, 2019:7).

سوم؛ نبودن فن‌آوری و عدم شناخت مناسب بسیاری از کاربران استفاده‌کننده می‌تواند زمینه و فرصتی مناسب برای ارتکاب بزهکاری باشد. بر این اساس، عقلانیت حکم می‌کند تا در انتخاب آماج، ضعف آن مورد توجه قرار گیرد تا افزون بر کاهش ریسک ارتکاب بزه برای بزهکار، شانس موفقیت در آن نیز افزایش یابد. در این چارچوب، فن‌آوری نوظهور ارزشهای مجازی، از

حیث فنی، نه تنها برای بسیاری از افراد جامعه شناخته شده نیست، بلکه برای ماموران اجرای قانون نیز دشواری‌های زیادی برای کشف و شناسایی جرم و مجرم وجود دارد. ضمن آنکه اساساً برخی ویژگی‌های فنی ارزشهای مجازی در عمل مانع از کشف سیستمی جرم می‌شود و تنها راه استفاده از راهبردهای سنتی در کشف جرائم است. برای نمونه در پرونده جاده ابریشم، به عنوان معروف‌ترین پرونده در زمینه ارزشهای مجازی، با وجود آنکه FBI سال‌ها در تلاش بود تا هویت مؤسسان و اعضای بزهکار این بازار برخط مجرمانه را شناسایی کند، ویژگی‌های فنی این فضا به خصوص به دلیل استفاده از ارزشهای مجازی، مانع از تحقق چنین امری می‌شد. تا زمانی که بی‌احتیاطی مؤسس این سازمان مجرمانه و انتشار آدرس ایمیل واقعی وی در یکی از گروه‌ها موجب شناسایی او و سایر بزهکاران مرتبط با این بازار مجرمانه شد (Kethineni, et al., 2018:150-151).

بدین‌سان، عقلانیت بزهکار مانند هر انسانی حکم می‌کند که همواره با استفاده از بهترین، پرثمرترین و کم‌ریسک‌ترین روش‌ها اقدام نماید. از این‌رو، ارزشهای مجازی و ویژگی‌های ذاتی و وضعیت شکل گرفته پیرامون آن، شرایط مناسبی را برای ارتکاب جرم پدید آورده‌اند.

۲. راهکارهای پیشگیری

با توجه به اینکه امروزه بسیاری از جرائم از وصف جهانی و فراملی برخوردار شده‌اند، پیشگیری از ارتکاب جرائم نیز در بعد جهانی و فراملی باید مورد توجه قرار گیرد. این امر به ویژه در خصوص جرائم ارتكابی در بستر فضای مجازی و ابزارهای فن‌آورانه این فضا، مانند ارزشهای مجازی، صادق است. در این چارچوب در گام نخست پیش از اتخاذ هر اقدامی، باید در پی تدوین مدلی فراملی جهت پیشگیری از ارتکاب جرم با استفاده از ارزشهای مجازی بود. امری که در چارچوب مبانی «جرم‌شناسی آبی»^۱ نیز مورد تأکید قرار گرفته است.

۱. جرم‌شناسی آبی در واقع جرم‌شناسی سازمان ملل است. این جرم‌شناسی به دنبال همکاری چشمگیر در خصوص جنبه‌های جدیدی از همکاری‌های بین‌المللی در زمینه پیشگیری از جرم و عدالت کیفری است. جرم‌شناسی آبی یا جرم‌شناسی سازمان ملل بر روی اهمیت یک سیستم عدالت کیفری انسانی و کارآمد تأکید دارد و به طور مؤثر به جرائم سازمان‌یافته فراملی، پول‌شویی، دزدی دریایی، تروریسم و فساد مالی می‌پردازد (Redo, 2012: 46).

با جهانی شدن جرم و اهمیت مباحث اقتصادی برای ادامه حیات گروه‌های سازمان‌مند مجرمانه، که غالباً از دامنه‌ای با وسعت جهانی برای ارتکاب جرم استفاده می‌کنند، ارزش‌های مجازی می‌تواند جایگزینی مطمئن و قابل استفاده باشد؛ زیرا همان‌طور که بیان شد ویژگی‌های منحصر به فرد این فن‌آوری بسیاری از مخاطرات را برای این گروه‌ها کاهش و شانس ارتکاب موفق جرم را افزایش می‌دهد. بر این اساس و مطابق رویکرد جرم‌شناسی آبی، گسترش و تسهیل فعالیت‌های مجرمانه با استفاده از ارزش‌های مجازی از ظرفیت زیادی برای ایجاد آسیب به نظام اقتصادی در سطح ملی و فراملی برخوردار است؛ لذا جهت پیشگیری از چنین مخاطراتی و ایجاد ثبات اقتصادی و سیاسی و به تبع آن ایجاد صلح در سطح جهانی ضروری است اقدامات لازم برای پیشگیری از مخاطرات مجرمانه ارزش‌های مجازی، با هماهنگی در سطح فراملی و سپس با بومی شدن چارچوب‌های پیشنهادی در سطح ملی صورت پذیرد. در نهایت، لازم است کشورها در چارچوب سیاست پیشگیرانه متحدالشکل، برای مقابله با استفاده از ارزش‌های مجازی در فعالیت‌های مجرمانه مختلف همکاری مؤثر نمایند (Andrianov, 2019:22-25).

جهت اتخاذ هر مدل یا سیاست پیشگیرانه جامع، توجه به ملاحظات جرم‌شناختی از اهمیت بسیاری برخوردار است تا بتوان با گزینش اقداماتی مناسب زمینه‌های ارتکاب جرم را از بین برد. بررسی جرم‌شناختی ارزش‌های مجازی از منظر نظریه انتقال فضایی و نظریه انتخاب عقلانی، بیان‌گر ویژگی‌هایی است که هر مدلی پیشنهادی باید با توجه به آنها ارائه شود.

در این راستا، ابتدا باید وضعیت قانونی و ماهیت ارزش‌های مجازی مشخص شود، دوم، چارچوب تنظیم‌گری، مقررگذاشته‌ای و جرم‌انگاری ابعاد گوناگون آن ترسیم شود، سوم، راهبردهای فنی/سایبری لازم برای تقویت سامانه‌های پیشگیرانه مورد مطالعه قرار گیرد و در نهایت تدوین شود، چهارم، این فن‌آوری به‌طور مستمر مورد پایش و بررسی قرار گیرد تا مطابق با ویژگی پویایی آن اقدامات ضروری با سرعتی معقول اتخاذ و عملیاتی شود و پنجم، ارزش‌های مجازی که خارج از حیطه نظارت‌های رسمی قرار دارند تضعیف شوند و ارزش‌های جدید برای جایگزینی آنها وارد بازار شود.

با توجه به موارد مذکور و بررسی برخی اسناد در سطح فراملی و تلاش‌های صورت گرفته پیرامون کاهش مخاطرات مجرمانه ارزش‌های مجازی به نظر می‌رسد تمامی ملاحظات مذکور را بتوان در چارچوب «رویکرد ریسک‌مدار سیاست جنایی در برابر مخاطرات مجرمانه ارزش‌های

مجازی» که توسط گروه ویژه اقدام مالی FATF تجویز شده است (FATF, 2019) و برخی کشورها نیز در چارچوب آن اقدام به بومی‌سازی رهنمودها نموده‌اند، توجه داشت.

بر این اساس، ابتدا ارزهای مجازی به عنوان یک کالا یا دارایی مورد شناسایی قرار می‌گیرند. در واقع، جهت تضعیف جایگاه این فن‌آوری، به ویژه اشکال خارج از حیطه نظارتی دولت‌ها و با قابلیت ایجاد توسط عموم مردم، جایگاه آن از مفهوم پول به مفهوم مال تقلیل می‌یابد. سپس ارائه‌دهندگان خدمات مربوط به این دارایی‌ها ملزم به ثبت نام و دریافت مجوزهای ضروری می‌گردند. در نهایت با شمول قوانین و مقررات مربوط به پولشویی، فعالیت‌های مرتبط با ارزهای مجازی در چارچوب برنامه‌های ضد پولشویی به عنوان سامانه‌ای جامع مورد رصد و بررسی قرار می‌گیرد.

در این مفهوم پیشگیری وضعی محور قرار دارد و با توجه به مدیریت ریسک، پیشگیری اجتماعی از جایگاه خاصی برخوردار نیست. سامانه ضدپولشویی از دو کارکرد برخوردار است. به عنوان کارکرد اول تلاش می‌شود با چینش صحیح و مطلوب برخی اجزا، وضعیت پیش‌جنایی به گونه‌ای مدیریت شود تا از وقوع جرم پیشگیری شود. بر این اساس، ارائه‌دهندگان خدمات مربوط به ارزهای مجازی؛ اعم از خرید و فروش و ... ملزم به دریافت مجوز و ثبت هویت مشتریان و اطلاعات مربوط به مبادلات و ارائه گزارش‌های ضروری، مانند گزارش عملیات مشکوک، می‌شوند. تا از این طریق با ایجاد یک فضای نسبتاً شفاف امکان رهگیری مبادلات و معاملات تا حدودی فراهم شود و کفه به سمت کاهش تمایل به ارتکاب جرم با افزایش ریسک ارتکاب برای بزهکاران سنگین شود. در کارکرد دوم نیز تلاش بر کشف سریع جرائم ارتكابی معطوف می‌شود. بر این اساس، شکل‌گیری سامانه‌های مختلف با هدف ثبت و ضبط سوابق و ایجاد ردپای کاربران، زمینه را برای کشف جرائم ارتكابی در اسرع وقت فراهم می‌سازد.

با این حال، مدل مذکور با وجود برخی از اقسام ارزهای مجازی، مانند بیت‌کوین، از کارآمدی کاملی برخوردار نیست. به نظر می‌رسد برای حل این امر اتخاذ برخی سیاست‌های فراحقوقی و فراجرم‌شناختی جهت کاهش اقتدار «شاه رمزارزها» (King of Crypto currencies) در بازار ارزهای مجازی ضرورت داشته باشد.

در نهایت، راهکارهای پیشگیرانه‌ای که الهام گرفته از نظریه‌های مختلف جرم‌شناسی است در قالب جدول ذیل نمایه می‌شود.

جدول (۱): راهکارهای پیشگیرانه در برابر جرائم ارتكایی با ارزشهای مجازی

پیشگیری کیفری	پیشگیری وضعی	پیشگیری اجتماعی	
	فیلتر کردن سایت‌ها و یا مسدود نمودن شبکه‌های اینستاگرامی مشوق استفاده از ارزشهای مجازی در فعالیت‌های مجرمانه	دور کردن بزهکاران از محیط‌های مجازی یا حقیقی مشوق استفاده از ارزشهای مجازی در فعالیت‌های مجرمانه	نظریه معاشرت‌های ترجیحی
تعریف جرم، مسئولیت کیفری و تعیین کیفر برای اشخاص سوء- استفاده‌کننده از ارزشهای مجازی در فعالیت‌های مجرمانه			نظریه فنون خنثی‌سازی
	۱- تعیین چهارچوب نظارتی دقیق ۲- تعیین مدل مالیاتی صحیح ۳- ارائه آموزش و اطلاعات کافی در مورد ارزشهای مجازی به مردم و پلیس جهت انجام اقدامات آگاهانه در برابر بزهکاران سوء‌استفاده‌کننده از ارزشهای مجازی		نظریه انتخاب عقلانی
	۱- به رسمیت شناختن قانونی و اجتماعی ارزشهای مجازی و وضع قواعد برای این نوع ارزشها ۲- تعیین الزاماتی برای شناسایی اجباری صاحبان ارزشهای مجازی ۳- افزایش نظارت نهادهای رسمی، همچون بانک مرکزی و یا وزارت اطلاعات و ارتباطات بر روی ارزشهای مجازی		نظریه انتقال فضایی
الزام دولت‌ها به تصویب قوانین برای مقابله با بزهکاران سوء- استفاده‌کننده از ارزشهای مجازی	تدوین سیاست پیشگیرانه متحد الشکل جهت افزایش نظارت ملی و بین‌المللی بر ارزشهای مجازی		نظریه جرم‌شناسی آبی

نتیجه‌گیری

ارز مجازی از مظاهر ورود فناوری مجازی به عرصه اقتصاد و زندگی واقعی است. زمان زیادی از طرح ایده ارزشهای مجازی و عملیاتی شدن آن نمی‌گذرد. در ابتدای ظهور ارزشهای مجازی، مقاومت‌هایی از سوی حاکمیت‌ها و مؤسسات مالی به عنوان واسط و ناظر بازار، در مقابل این نوع ارزشها صورت گرفت. پس از مدتی دولت‌ها به ویژه دولت‌های تحت تحریم، جذب مزایای مختلف ارزشهای مجازی شدند؛ به خصوص از آن جهت که ارزشهای مجازی وسیله‌ای برای دور زدن تحریم‌ها و رهایی از فشارهای اقتصادی ناشی از این تحریم‌ها بودند. با وجود این مزایا،

پیامدهای منفی ارزشهای مجازی، به ویژه پیامدهای تسهیل جرم آن، قابل انکار نیست و هنگام تصمیم‌گیری و سیاست‌گذاری در خصوص این نوع ارزشها، باید در کنار استدلال‌های حقوقی و فقهی در بستر حقوق خصوصی برای پذیرش یا عدم پذیرش این نوع ارزشها در عرصه اقتصاد، به امکان مقابله کیفری و پیشگیری از جرائم ارتكابی با استفاده از جذابیت‌های ارزشهای مجازی نیز اندیشید.

گستره ارتكاب جرم با استفاده از ارزشهای مجازی، علل جذابیت و بررسی جرم‌شناختی کارکردهای مجرمانه آن در چارچوب برخی نظریات جرم‌شناسی، بیان‌گر آن است که در اتخاذ هر مدلی برای پیشگیری از مخاطرات مجرمانه این فن‌آوری، توجه به ابعاد فراملی آن اجتناب‌ناپذیر است. بر این اساس، کشورها باید در چارچوب برنامه‌های اقدام خود با بومی‌سازی مدل‌هایی مربوط، افزون بر استفاده از ظرفیت‌های مثبت ارزشهای مجازی، زمینه را برای کاهش مخاطرات مجرمانه این ارزشها فراهم سازند.

بر این اساس و با توجه به دستاورد این پژوهش پیشنهادات زیر با هدف پیشگیری از ارتكاب جرم با استفاده از ارزشهای مجازی قابل طرح است:

- به رسمیت شناختن قانونی و تعیین ماهیت ارزشهای مجازی به عنوان یک دارایی؛ این امر منجر به خارج شدن ارزشهای مجازی از نقطه کور قانون‌گذاری خواهد شد. در واقع، ضرورت تنظیم‌گری و ارائه مدل‌های سیاست‌گذاری پیرامون پدیده‌های گوناگون که از آثار گسترده-ای برخوردارند مداخله دولت‌ها را با استفاده از ابزارهای حقوقی اجتناب‌ناپذیر کرده است. بر این اساس، ورود دولت‌ها و تدوین مقررات مناسب می‌تواند تا حد زیادی به مدیریت مخاطرات مجرمانه پدیده‌ها کمک کند.
- پیش‌بینی الزاماتی جهت ثبت نام و اخذ مجوز توسط ارائه‌دهندگان خدمات مربوط به ارزشهای مجازی و مکلف نمودن آنها به ثبت هویت مشتریان و سابقه معاملات؛ بدیهی است ارزشهای مجازی مانند هر ابزار مالی دیگر در دو سطح بازارهای قانونی و بازارهای غیرقانونی قابلیت استفاده دارند. پیشنهاد مذکور به عنوان مکملی برای پیشنهاد اول، می‌تواند منجر به ایجاد نظم در بازار مبادلات قانونی ارزشهای مجازی شود. از این‌رو، پس از شناسایی قانونی، تنظیم‌گری ابعاد گوناگون ارزشهای مجازی ضرورتی اجتناب‌ناپذیر است.
- تعیین مدل مالیاتی مشخص برای ارزشهای مجازی؛ بدون شک یکی از مهم‌ترین کارکردهای

ارزهای مجازی جنبه تجارتي و اقتصادي آن است که آن را در کاربردهای مشروع و نامشروع مورد توجه قرار می‌دهد. از این رو، ضرورت برخورد برابر با چنین ارزشی، تدوین مقررات لازم از حیث مالیاتی است. این پیشنهاد نیز به عنوان مکملی برای دو پیشنهاد اول زمینه را برای ایجاد نظم در مرادوات اقتصادی فراهم خواهد کرد.

- توسعه زیرساخت‌های سخت‌افزاری و نرم‌افزاری لازم برای حضور ایمن و کنترل شده فعالان ارزهای مجازی؛ برخلاف سه پیشنهاد اول که به‌طور مشخص می‌تواند زمینه را پس از شناسایی قانونی، برای ایجاد انتظام در بازار قانونی ارزهای مجازی فراهم سازد، پیشنهاد فوق افزون بر بازارهای قانونی، برای کاهش مخاطرات مجرمانه نیز از کارایی برخوردار است. در برخورد با فن‌آوری ارزهای مجازی باید این نکته اساسی را به‌خاطر سپرد که ویژگی‌های ذاتی این ابزار در کنار سایر ابزارهای فن‌آورانه موجود در فضای مجازی، چالش‌های جدی و گاهی غیرقابل حل را برای کنش‌گران نظام عدالت کیفری به‌ویژه در مرحله کشف جرم و شناسایی مجرمان ایجاد می‌کند. در حال حاضر زمانی که از ارزهای جهان‌روایی چون بیت-کوین در فضای تاریک وب؛ یعنی دارکنت، برای اهداف مجرمانه استفاده می‌شود در عمل هیچ راهکار فنی برای شناسایی مرتکبان اعمال مجرمانه وجود ندارد. این امر با توجه به پرونده‌های کیفری موجود در سطح فراملی به وضوح قابل مشاهده است که در آنها مأموران اجرای قانون در کشف جرم و شناسایی مرتکبان با چالش‌های جدی رو به رو بوده‌اند و صرفاً توانستند با استفاده از راهکارهای سنتی کشف و شناسایی، برخی پرونده‌ها را به سرانجام برسانند. از این رو، تلاش جهت توسعه زیرساخت‌ها اگرچه شاید برطرف‌کننده تمامی مشکلات موجود در این زمینه نباشد اما می‌تواند توانمندی مأموران اجرای قانون را در انجام وظایف خود افزایش دهد.

- رصد مستمر، اطلاع‌رسانی، هشداردهی و افزایش آگاهی عمومی نسبت به مخاطرات مجرمانه ارزهای مجازی؛ باید توجه داشت که دنیای ارزها و دارایی‌های مجازی به شدت در حال توسعه، تغییر و پیشرفت است. چنین فضای پویایی با وجود مزیت‌ها و کاربردهای بی‌بدیل، در بردارنده ریسک‌هایی نیز برای عموم شهروندان، کاربران، بخش‌های پولی، مالی و بانکی و دولت‌ها است. از این رو، رصد مستمر این فضا، به روزرسانی دانش و آگاهی نسبت به ویژگی‌ها و تحولات دوره‌ای این فن‌آوری جهت اطلاع‌رسانی، هشداردهی و افزایش آگاهی تمامی

اشخاص و نهادهایی که در معرض این فن‌آوری قرار دارند می‌توانند تا حد قابل توجهی کاهش دهنده مخاطرات ارزهای مجازی، به ویژه مخاطرات مجرمانه آنها، باشد.

References

- [1]: Albrecht, Chad; Duffin, Kristopher; Hawkins, Steven & Rocha, Victor. (2019). The use of cryptocurrencies in the money laundering process, *Journal of Money Laundering Control*, Vol. 22, No.2, pp. 210-216.
- [2]: Apriliani, Muttaqim1. (2019). Analysis of The Probability of Money Laundering Crimes toward the Development of Crypto-currency Regulations in Indonesia, *Indonesian journal of criminal law studies*, 4(1). pp. 29-40.
- [3]: Boehm, Franziska & Pesch, Paulina. (2014). Conference Paper, International Conference on Financial Cryptography and Data Security, pp. 43-56. Available in: <https://www.tib.eu/en/search/id/BLSE%3ARN363392476/>.
- [4]: Brenig, C., Rafael, A., & Muller, G. (2015). Economic analysis of cryptocurrency backed money laundering. ECIS 2015 Completed Research Papers. Paper 20. Retrieved October 25, 2018, from http://aisel.aisnet.org/ecis2015_cr/20-
- [5]: Brown, David. (2016). Cryptocurrency and criminality: The Bitcoin opportunity, *The Police Journal: Theory, Practice and Principles*, Vol. 89(4). PP. 327–339.
- [6]: Doguet, Joshua. (2013). The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System, *Louisiana Law Review*, vol. 73, pp. 1119-1153.
- [7]: Dyson, Simon; Buchanan, William & Bell, Liam. (2019). The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime, pp.1-6. Available in: <https://arxiv.org/pdf/1907.12221.pdf>
- [8]: FATF (2019). VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, GUIDANCE FOR A RISK-BASED APPROACH.
- [9]: Goldman, Zachary; Maruyama, Ellie; Rosenberg, Elizabeth; Saravalle, Edoardo & Solomon-Strauss, Julia. (2017). Terrorist use of virtual currencies, CNAS Publication, Washington.
- [10]: Higgins, S. (2016, February 22). California bankruptcy judge says bitcoin is property, not currency. *Coindesk*. Retrieved April 2, 2018, from <https://www.coindesk.com/bankruptcy-judge-bitcoin-property-currency/>
- [11]: Hutchings, Alice. (2016). Cybercrime trajectories: An integrated theory of initiation, maintenance and desistance. In T. Holt (Ed.). *Crime online: Correlates, causes, and context* (3rd ed., pp. 117–140). Durham: Carolina Academic Press. Available in: <https://www.cl.cam.ac.uk/~ah793/papers/2016trajectories.pdf>

- [12]: Ivantsov, Sergey; Sidorenko, Elina; Spasennikov, Boris; Berezkin, Yuri & Sukhodolov, Yakov. (2019). Cryptocurrency-related crimes: key criminological trends, *Russian Journal of Criminology*, vol. 13, no. 1, pp. 85–93.
- [13]: Jaishankar, Karuppanan. (2007). Establishing a Theory of Cyber Crimes, *International Journal of Cyber Criminology*, Vol 1, Issue 2, pp. 7-9.
- [14]: Jaishankar, Karuppanan. (2008). Space Transition Theory of Cyber Crimes, In book: *Crimes of the Internet*, Publisher: Pearson, Editors: Frank Schmalleger, Michael Pittaro, pp.283-301. Available in: <https://www.researchgate.net/publication/321716315>.
- [15]: Jaishankar, Karuppanan. (2019). Cyber Criminology and Space Transition Theory: Contribution and Impact, pp. 101-110. In: Chapter 3. Cybercrimes, cybercriminals and cybervictims. Available in: <https://www.researchgate.net/publication/332550803>.
- [16]: Kheradmand, Mohsen. (2019). Jurisprudential study of extraction and exchange of cryptocurrencies with focus on bitcoin network, *Journal of Islamic Economic Knowledge*, 10th year, No. 2, pp. 109-124. (In Persian)
- [17]: Kethineni, S., Cao, Y., & Dodge, C. (2018). Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes. *American Journal of Criminal Justice*, 43, pp. 141–157.
- [18]: Kethineni, Sessa & Cao, Ying. (2019). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity, *International Criminal Justice Review*, pp.1-20. Available in: <https://doi.org/10.1177/1057567719827051>.
- [19]: Kfir, Isaac. (2020). Cryptocurrencies, national security, crime and terrorism, *Comparative strategy*, vol. 39, NO. 2, pp.113–127.
- [20]: Khalili Paji, Aref. (2019). Feasibility Study of Terrorist Financing in the Light of Virtual Currencies, *Collections of the International Conference on the Legal Dimensions of the Terrorism Criminological*, First Edition, Tehran, Allameh Tabatabai University Press, pp. 113-134. (In Persian)
- [21]: Kirkpatrick, Katherine; Savage, Christine; Johnston, Russell & Hanson, Matthew (2019). Virtual currency in sanctioned jurisdictions: stepping outside of SWIFT, *Journal of Investment compliance*, vol. 20, no. 2, pp.39-44.
- [22]: Korennaya, Anna & Tydykova, Nadezhda. (2019). Crypto currency as an object and instrument of committing crime, *Russian Journal of Criminology*, vol. 13, no. 3, pp. 408–415.
- [23]: Lester, C. (2017, January 9). Terrorists use bitcoin and PayPal in Indonesia, AML official claims. *CCN.com*. Retrieved September 30, 2018, from <https://www.ccn.com/terrorists-use-bitcoin-and-paypal-in-indonesiaagency-official-claims/>
- [24]: Liu, Weiyi; Liang, Xuan & Cui, Guowei. (2020). Common risk factors in the

- returns on cryptocurrencies, *Economic Modelling Journal*, vol. 86, pp. 299-305.
- [25]: Lockett, Nick(1999). Legal perspectives on digital money in Europe, *European Business Review*, Volume 99, Number 4, pp. 235-241.
- [26]: Mahmoudi, Asghar. (2019). Analysis of Virtual Currencies in the Light of Jurisprudence, *Law and Comparative Studies*, *Quarterly Journal of Private Law Studies*, Volume 49, Number 3, pp. 503-522. (In Persian)
- [27]: Miri Lavasani, Somaieh Sadat؛ Heidary, Bahareh؛ Razmjoo, Ali Akbar & Razmjoo, Mohadeseh. (2019). A Study of the Legal Status of the National Digital Currency, *Journal of New Achievements in Humanities Studies*, Second Year, No. 13, pp. 72-81. (In Persian)
- [28]: Naderi, Ebrahim & Shahir, Leili. (2018). Market and Capital Analysis from the Conversion of Digital Currencies: Digital Currencies Are the End to the Sovereignty of the Dollar, No. 96, pp. 88-90. (In Persian)
- [29]: Naheem, Mohammed Ahmad. (2018). Regulating virtual currencies—the challenges of applying fiat currency laws to digital technology services, *Journal of Financial Crime*, Vol. 25, No. 2, pp. 562-575.
- [30]: O’Keeffe, D. (2018, July 19). The pointlessness of state-backed cryptocurrencies. *Crypto disrupt*. Retrieved October 15, 2018, from <https://cryptodisrupt.com/the-pointlessness-of-state-backed-cryptocurrencies/>
- [31]: Panda, A. (2018, February 28). Cryptocurrencies and national security. *Council on Foreign Affairs*. Retrieved September 30, 2018, from <https://www.cfr.org/background/cryptocurrencies-and-national-security>.
- [32]: Pouyan Mokhtari arrested / Interpol will extradite Pouyan Mokhtar to Iran after his arrest ?, News ID: 78885, dated 10/5/2020. In: www.saednews.com(In Persian)
- [33]: Raskin, Max. (2013). Meet the Bitcoin Millionaires, *Bloomberg Businessweek*, Available in: <https://www.realcrapolitics.com/2013/04/15>.
- [34]: Redo, Slawomir. (2012). *Blue criminology (The power of the United Nations ideas to counter crime globally)*. HEUNI Publication.
- [35]: Roshan, Mohammad؛ Mozafari, Mostafa & Mirzaie, Hanieh. (2019). A Study of the Jurisprudential and Legal Status of Bitcoin, *Journal of Legal Research*, Volume 22, Number 87, pp. 49-78. (In Persian)
- [36]: Sabooripour, Mehdi. (2019). *Rationality in committing a crime*, Tehran, Mizan, first edition. (In Persian)
- [37]: Sereda A.V. (2017). Settlements using virtual currencies in the Russian Federation: analysis of the first law enforcement experience, *Modern Lawyer*,

- No. 2, pp. 57-64.
- [38]: Seyed Hosseini, Mir Meysam & Doaei, Meysam. (2014). Bitcoin, the first virtual money, Tehran, published by the Stock Exchange Organization. (In Persian)
- [39]: Shamloo, Baqir & Khalili Paji, Aref. (1399). Virtualization of white-collar delinquency in the light of virtual currencies, Legal Journal of Justice, Volume 84, Number 110, pp. 41-73. (In Persian)
- [40]: Siegel, Lari. (2006). Criminology, translated by Yashar Seif Elahi, first edition, Law Enforcement Publications of the Islamic Republic of Iran. (In Persian)
- [41]: Soleimanipoor, Mohammad Mehdi; Soltaninejad, Hamed & Pourmotahar, Mehdi (2017). Jurisprudential study of virtual money, Islamic Financial Research Quarterly, Year 6, Number 2, pp. 167-192. (In Persian)
- [42]: Turpin, J. B. (2014). Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework. Indiana Journal of Global Legal Studies, 21, pp. 335-368.
- [43]: Vandezande, Niels. (2017). Virtual currencies under EU anti-money laundering law, computer law & security review, vol. 33, pp. 341-353.
- [44]: Wald, George; Bernard, Thomas & Snipes, Jeffrey. (2009). Theoretical Criminology, translated by Ali Shojaei, third edition, Samat Publications. (In Persian)
- [45]: Wood, G., & Buchanan, A. (2015). Advancing egalitarianism. In D. L. K. Chuen (Ed.). Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data (pp. 385-402). New York, NY: Elsevier.
- [46]: www.group-ib.ru/media/gib-cryptosummary مراجعه در ۱۳۹۹/۱/۱۷
- [47]: www.inhope.org/tns/resources/statistics مراجعه در ۱۳۹۹/۲/۵
- [48]: www.iranhoshdar.ir مراجعه در ۱۳۹۹/۲/۲۸
- [49]: www.cbi.ir/showitem/ مراجعه در ۱۳۹۹/۱/۲۱
- [50]: www.alef.ir/news مراجعه در ۱۳۹۹/۲/۱۵
- [51]: www.extremism.gwu.edu مراجعه در ۱۳۹۹/۳/۷