



## فصلنامه علمی مطالعات پیشگیری از جرم

doi: 10.22034/CPS.2022.211339.1365

سامانه: cps.jrl.police.ir

## پیشگیری وضعی از جرایم در بستر رمز ارزها

تاریخ دریافت: ۱۴۰۰/۰۸/۱۳

تاریخ پذیرش: ۱۴۰۱/۰۳/۲۹

نوع مقاله: پژوهشی

هادی کرامتی معز<sup>۱</sup>✉مجید بهاری غازانی<sup>۲</sup>

## چکیده

**زمینه و هدف:** تکامل رمز ارزها همراه با ارتکاب جرم همراه بوده و استفاده از این فناوری نوین برای مقاصد غیرقانونی نه تنها فعالیت مجرمانه را در سراسر جهان تسهیل می‌کند، بلکه امنیت افرادی را که از رمز ارزها برای مقاصد قانونی استفاده می‌کنند را نیز تضعیف می‌کند، به دلیل که مجرمان برای پنهان کردن منشأ غیرقانونی وجوه خود از طرق مختلفی وارد عمل می‌شوند ولی یکی از راحت‌ترین و جدیدترین این روش‌ها آن است که این پول‌های کثیف تحت عنوان رمز ارزها معامله شوند. لذا این مسأله مطرح است که چه اقدامات پیشگیرانه وضعی می‌تواند در خصوص جرائم مرتبط با رمز ارزها موثر باشد؟

**روش:** این پژوهش به صورت توصیفی-تحلیلی مورد تجزیه و تحلیل قرار گرفته است.

**یافته‌ها و نتایج:** جهت اتخاذ سیاست پیشگیرانه وضعی، توجه به تئوری‌های جرم‌شناختی از اهمیت بسیاری برخوردار است و از تئوری‌های مرتبط در زمینه بررسی‌های جرم‌شناختی رمز ارزها، می‌توان به نظریه‌های انتخاب عقلانی، الگوی جرم و سبک زندگی برخط، گذار از فضا و جرم‌شناسی آبی اشاره نمود. همچنین می‌توان نتیجه گرفت که راهکارهای پیشگیری وضعی از جرایم در بستر رمز ارزها در دو محور الف) تدابیر نظارتی (نصب و راه‌اندازی سیستم‌های KYC، محدودیت دسترسی به رمز ارزها و قرار گرفتن در لیست سیاه، نظارت بر صرافی‌های آنلاین و نظارت مؤثر در ارائه‌دهندگان خدمات رمز ارزها)؛ ب) تدابیر افزایش دشواری ارتکاب جرم (استفاده از داده‌های بلاک‌چین عمومی، طبقه‌بندی بازیگران حقیقی و حقوقی شبکه رمز ارزها، حفاظت از داده‌های شخصی) قرار می‌گیرد.

**کلیدواژه‌ها:** رمز ارزها، پیشگیری وضعی، تدابیر نظارتی، افزایش دشواری ارتکاب جرم.

\* استناددهی (APA): کرامتی معز، هادی؛ بهاری غازانی، محمد. (۱۴۰۱). پیشگیری وضعی از جرایم در بستر رمز ارزها. *مطالعات پیشگیری از جرم*، ۱۷(۶۳)، ۱۸۹-۱۶۷.

[http://cps.jrl.police.ir/article\\_98908.html](http://cps.jrl.police.ir/article_98908.html)

۱. گروه حقوق، موسسه آموزش عالی طلوع مهر، قم، ایران. نویسنده مسئول. رایانامه: keramatihadi@ut.ac.ir

۲. کارشناسی ارشد حقوق جزا و جرم‌شناسی، موسسه آموزش عالی طلوع مهر، قم، ایران. رایانامه: majidbaharighazani@gmail.com

## مقدمه

رمز ارزها به دلیل مفاهیم فناوری نوآورانه خود، سؤالات حقوقی جدیدی را مطرح می‌کنند. یکی از چالش مهم در حوزه ارزهای دیجیتال روند رو به گسترش آنها می‌باشد به نحوی که با توجه به تعداد زیاد (و به طور مداوم در حال رشد) سیستم‌های به اصطلاح «ارز رمزنگاری» با ویژگی‌های فناوری متفاوت، ارائه تعریف اصطلاح «ارز دیجیتال» کار آسان نیست. آنچه در بیان تعریف ارز دیجیتال اهمیت دارد این است که چه ویژگی ارز دیجیتال را از پول بانکی مجزا می‌سازد (بارج<sup>۱</sup>، ۲۰۱۶: ۵۴۹).

سیستم ارزهای دیجیتال مانند سیستم‌های ارز سنتی عمل نمی‌کند. در سیستم‌های ارزی در دنیای حقیقی، دولت‌ها، بانک‌های مرکزی و مؤسسات بانکی خصوصی به عنوان واحدهای اداری و کنترل مرکزی پول عمل می‌کنند. برعکس، در سیستم ارز دیجیتال، کاربران قدرت پردازشی را تحت یک «شبکه همتا به همتا»<sup>۲</sup> که برنامه‌ای را برای پیگیری مانده حساب‌های همه کاربران اجرا می‌کند، اعمال می‌کنند. به طور مثال بیت کوین اساساً یک مسیر تراکنش بین چندین کلید عمومی در بلاک چین است. از این رو، «نگهداری» بیت کوین به معنای کنترل کلید عمومی (آدرس بیت کوین) است که آخرین تراکنش ثبت شده را دریافت کرده است. یک کاربر بیت کوین با در اختیار داشتن کلید خصوصی مربوطه، قدرت را روی یک کلید عمومی اعمال می‌کند (بریتو<sup>۳</sup> و همکاران، ۲۰۱۴: ۱۳۴).

افزودن یک بلوک داده (که شامل تراکنش‌های کاربران است) به بلاک چین، استخراج نامیده می‌شود. ماینرهای بیت کوین کاربرانی هستند که قدرت CPU خود را برای فرآیند استخراج فراهم می‌کنند. یک ماینر موفق با بیت کوین‌های تازه استخراج شده (علاوه بر کارمزد تراکنش‌های ارائه شده توسط طرفین تراکنش) پاداش می‌گیرد تا به کاربران انگیزه دهد تا قدرت محاسباتی را برای عملیات شبکه فراهم کنند. حتی اگر بلاک چین عمومی باشد، شرکت کنندگان در شبکه بیت کوین (در صورت تمایل به انجام این کار) با نام مستعار باقی می‌مانند. این امکان‌پذیر است؛ زیرا هر مشتری می‌تواند تعداد بی‌نهایت کلید عمومی منحصر به فرد و مستقل ایجاد کند. بنابراین، هیچ کاربری مجبور نیست خود را به یک واحد اداری معرفی کند (برخلاف افتتاح حساب بانکی). معمولاً فقط دارنده کلید خصوصی می‌داند که کلید عمومی با چه کسی مرتبط است (بریتو و همکاران، ۲۰۱۴: ۱۳۵).

1. Burge  
2. peer-to-peer network  
3. Brito



از آنجا که جرایم مرتبط با رمز ارزها، به سرعت توسعه آنها رو به افزایش است، هم‌زمان دولت‌ها شروع به تنظیم صریح ارزهای دیجیتال از نظر مبارزه با پول‌شویی<sup>۱</sup> و شفاف‌سازی یا تقویت مبنای قانونی برای تعقیب جرایم در زمینه رمز ارزها می‌کنند. علاوه بر این، تحقیقات جنایی در زمینه رمز ارزها با افزایش تعداد جرایم مرتبط با این حوزه تشدید می‌شود. علاوه بر این، دولت‌ها باید پیشگیری از بزهکاری را در این زمینه‌ها در نظر بگیرند، به نحوی که به حقوق اساسی شهروندان آسیب نرساند (موزر<sup>۲</sup> و همکاران، ۲۰۱۴: ۱۱). هرچند جرایم ارتكابی از طریق این گونه رمز ارزها در مقیاسی وسیع صورت می‌گیرد، اما پول‌شویی و تأمین مالی تروریسم به دلیل ارتباطش با سایر جرایم و اینکه اصولاً به نحو سازمان یافته انجام می‌گیرد؛ اهمیت دوچندانی دارد. با این وصف، نگارندگان در این مقاله به دنبال پاسخ‌گویی به این سؤالات هستند که راهکارهای پیشگیری وضعی از جرایم در بستر رمز ارزها چیست؟ چه نظریه‌های جرم‌شناسی در زمینه بررسی‌های جرم‌شناختی رمز ارزها در راستای سیاست‌های جرم‌شناسی پیشگیرانه وضعی مرتبط هستند؟

## پیشینه و مبانی نظری

### پیشینه

عبداللهی قهفرخی و همکاران (۱۴۰۰)، در پژوهشی با عنوان «پیشگیری از پول‌شویی الکترونیکی: رویکرد دفاعی و رویکرد هجومی» به این نتیجه رسیده‌اند که پیشگیری از پول‌شویی الکترونیکی از دو منظر، جنبه دفاعی دارد. یکی از منظر بستر ارتكاب جرم یعنی فضای سایر که صیانت از موضوع جرم نسبت به پیشگیری از جرم اولویت دارد و تدابیر پیشگیرانه در مقام حفاظت از ارزش‌های رایانه‌ای‌اند تا دست مرتکب به آنها نرسد. برخلاف پیشگیری از جرم در فضای سنتی، اختیار عمل در دست متصدیان پیشگیری است، ولی در فضای سایر، اختیار عمل در دست مرتکبان است و متصدی پیشگیری بیشتر نگرهبانی می‌کند تا برهم زدن فرصت ارتكاب جرم، دوم از منظر مبادلات مالی الکترونیکی که بر پایه ویژگی‌هایی چون سرعت، انبوهی و تنوع مکانی در عمل از دسترس تدابیر پیشگیرانه به دور است.

صفاری و همکاران (۱۳۹۹)، در پژوهشی با عنوان «کارکردهای مجرمانه ارزهای مجازی: تحلیل جرم‌شناختی و راهکارهای پیشگیرانه» به این نتیجه رسیده‌اند که گستره ارتكاب جرم با استفاده از ارزهای مجازی، علل جذایت و بررسی جرم‌شناختی کارکردهای مجرمانه آن در چارچوب برخی نظریات جرم‌شناسی، بیانگر آن است که در اتخاذ هر مدلی برای

1. Anti-money-laundering (AML)

2. Moeser

پیشگیری از مخاطرات مجرمانه این فناوری، 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 ارزهای مجازی، زمینه را برای کاهش مخاطرات مجرمانه این ارزها فراهم سازند.

بهره‌مند و همکاران (۱۳۹۳)، در پژوهشی با عنوان «**راهبردهای وضعی پیشگیری از جرایم سایبری**» به این نتیجه رسیده‌اند که پیشگیری از جرم، نخستین گام برای تحقق عدالت کیفری است. فضای سایبر به اقتضای ویژگی‌های خاصی که دارد، برای پیشگیری وضعی بسیار مساعد است. رهایی بستر، گمنامی کاربران، آسیب‌پذیری آماج، دشواری شناسایی بزه‌کاران، سهولت ارتکاب جرم، گستردگی خسارت، کثرت بزه‌دیدگان و کم سن بودن اغلب کاربران، ضرورت پیشگیری وضعی از این جرایم را دو چندان ساخته است، لذا با اعمال شیوه‌های فنی پیشگیری از جرم، می‌توان تا حد مطلوبی از این جرایم پیشگیری نمود.

## مبانی نظری

جهت اتخاذ سیاست جرم‌شناسی پیشگیرانه وضعی، توجه به تئوری‌های جرم‌شناختی از اهمیت بسیاری برخوردار است تا بتوان با گزینش اقداماتی مناسب زمینه‌های ارتکاب جرم را از بین برد. از تئوری‌های مرتبط در زمینه بررسی‌های جرم‌شناختی رمز ارزها، می‌توان به نظریه‌های انتخاب عقلانی، الگوی جرم و سبک زندگی برخط، گذار از فضا و جرم‌شناسی آبی اشاره نمود.

### ۱. تئوری انتخاب عقلانی<sup>۱</sup>

یکی از مهم‌ترین مبانی پیشگیری وضعی از جرایم در بستر رمز ارزها را می‌توان در نظریه‌های انتخاب عقلانی مشاهده کرد که تحلیلی اقتصادی از ارتکاب بزه را ارائه می‌دهند. بنیان نظریه‌ی انتخاب عقلانی را می‌توان در آثار سزار بکاریا و جرمی بنتام جستجو نمود. دغدغه‌ی آن‌ها تحلیل رفتار مجرمانه نبود، بلکه؛ در صدد انتخاب مجازاتی مناسب با بزه ارتكابی بودند (فرهادی آلاشتی، ۱۳۹۵: ۳۲). نظریه انتخاب عقلانی بیشتر به واسطه تحقیقات «درک کورنیش»<sup>۲</sup> و «رونالد کلارک»<sup>۳</sup> شناخته شده است. این رویکرد یک اصل محوری دارد و آن این است که رفتار انسان‌ها، هدفدار و سنجیده است، انسان‌ها در دوراهی‌ها، راهی را که با اهدافشان موافق است انتخاب می‌کنند و برای رفتن به هر راهی سود و زیانش را محاسبه می‌کنند؛ بنابراین، رفتار منحرفانه نیز نوعی تصمیم‌گیری

1. Rational Choice Theory  
2. Derek Cornish  
3. Ronald Clarke



فردی و انتخاب عقلانی منفعت گرایانه است که پس از سنجش پیامدهای مثبت و منفی آن صورت می گیرد (کرامتی معزز، ۱۳۹۹: ۹۱).

جرم شناسان معاصر بر پایه این آموزه های کلاسیک، استدلال می کنند که «بزهکارانی احتمالی»<sup>۱</sup> با یک حسابگری خرد بنیاد در فرصت های ارتکاب جرم عمل می کنند؛ بنابراین، همیشه افرادی وجود دارند که اگر فرصتی بیابند، مرتکب جرم می شوند. نظریه انتخاب عقلانی را زیربنای نظریه های فرصت جرم باید دانست؛ زیرا فرض می کند که بزهکاران احتمالی همواره پیش از تصمیم به ارتکاب جرم، فرصت های خطر آن را ارزیابی می کنند و احتمال هایی مانند دیده شدن، آسانی ورود به محل ارتکاب جرم و امکان فرار را، بی آنکه شناسایی شوند، در نظر می گیرند (رایجیان اصلی، ۱۴۰۱: ۲۴۴-۲۴۳).

این قاعده به زبان جرم شناسی از این قرار است: جرم به عنوان یک شکل از رفتار، زمانی رخ می دهد که فردی که دارای انگیزه های مجرمانه است، با یک فرصت یا موقعیت مجرمانه مواجه شود؛ به عبارت دیگر، هم انگیزه مجرمانه و هم موقعیت جرم زا، برای وقوع جرم ضروری هستند. تمرکز کلارک بر تأثیر موقعیت ها در شکل گیری جرم، موجب سوق پیدا کردن وی به سمت پیشگیری وضعی و احیای آن گردید (عبدالهی، ۱۴۰۱: ۱۲۷). از آنجایی که نظریه انتخاب عقلانی بر آن است که پرسه زنان فضای مجازی، پیش از ارتکاب یک جرم به محاسبه میزان مخاطرات آن می پردازند، لذا اگر مخاطرات یاد شده افزایش یافته و مجازات، چهره ای شدید به خود بگیرد، می توان مانع از بروز این رفتارها شد، در حال حاضر، هیچ بازدارنده ای واقعی در مقابل این رفتارها در فضای مجازی وجود ندارد (جیشانکار، ۱۳۹۴: ۴۰۳).

با توجه به مطالبی که بیان شد و در راستای انطباق تئوری انتخاب عقلانی با رمز ارزها و جرایم مرتبط با آن، می توان این گونه استنباط نمود که نو بودن فناوری رمز ارزها و عدم آگاهی مناسب بسیاری از کاربران، ظرفیت و فرصتی ایده آل برای ارتکاب جرم است. از این رو، تئوری انتخاب عقلانی ایجاب می کند تا در انتخاب آماج، ضعف آن مورد توجه قرار گیرد تا افزون بر کاهش ریسک ارتکاب جرم برای مرتکبین، شانس موفقیت در آن نیز افزایش یابد.

## ۲. تئوری الگوی جرم و سبک زندگی برخط<sup>۲</sup>

این نظریه به گات فردسن<sup>۳</sup> و هیندلانگ<sup>۴</sup> منسوب است و طبق آن، هر قدر یک فرد شیوه زندگی بازتری داشته باشد؛ یعنی فعالیت های شغلی و تفریحی و اوقات فراغت وی بیشتر باشد احتمال

1. potential offenders/criminals  
2. Online Lifestyle  
3. Gottfredson  
4. Hindelang

بزه دیده شدن او بیشتر است (کرامتی معز و میرخلیلی، ۱۳۹۹: ۶). لذا عادت‌ها و سبک زندگی افراد در احتمال بزه دیدگی آنان تأثیر گذار است. لذا بسیاری از افراد از اینکه عادت‌های فردی‌شان و الگوی استفاده از کامپیوتر، فضای مجازی و رمز ارزها می‌تواند به امنیت و حریم اطلاعات شخصی‌شان تأثیر گذارد، ناآگاه هستند. این امر می‌توان ضریب بزه دیدگی آنان را بالا ببرد (ابوذری، ۱۳۹۵: ۱۳۸).

نظریه سبک زندگی در فضای سایر نیز قابلیت اعمال داشته و می‌توان از آن عنوان سبک زندگی برخط تعبیر کرد. امروزه گروهی از کاربران، زمان زیادی را در فضای سایبری می‌گذرانند و از تدابیر موقعیت‌مدار به روز نیز استفاده نمی‌نمایند؛ حال، چنانچه آنان در فضاهای پرمخاطره سایبری فعالیت نمایند و یا خود را در معرض فضاهای ناشناخته مستعد بزه قرار دهند، احتمال بزه دیدگی آنان افزایش خواهد یافت (فرهادی آلاشتی، ۱۳۹۵: ۳۹). فرض بر این است که سبک زندگی بر خط یک کاربر، عاملی اساسی در به حداقل رسانی بزه دیدگی رایانه‌ای/ مجازی است (جیشانکار، ۱۳۹۴: ۳۴۳).

در حال نیز به‌ویژه با گسترش یافتن رمز ارزها و ناشناختگی و گمنامی را برای کاربران به ارمغان آورده و همچنین به عبارتی انتقال وجه در این نوع ارزها غیرقابل تشخیص و امکان رهگیری آن به راحتی میسر نیست و منجر شده احتمال بزه دیدگی اشخاص در انجام معاملات رمز ارزها بالا باشد.

### ۳. تئوری گذار از فضا<sup>۱</sup>

کی. جایشانکار- جرم‌شناس هندی<sup>۲</sup>، «نظریه گذار از فضا» را در مقاله «نظریه گذار از فضا درباره جرم‌های سایبری» (۲۰۰۸)<sup>۳</sup> سازمان‌دهی کرده است که به موجب آن، افراد در فرآیند گذار از فضای فیزیکی به فضای مجازی و یا برعکس، متفاوت رفتار می‌کنند (رایجیان اصلی، ۱۴۰۱: ۴۳۵-۴۳۴).

1. space transition theory

۲. جیشانکار، جرم‌شناس هندی، International Journal of Cyber Criminology مجله بین‌المللی جرم‌شناسی سایبری را تأسیس و نخستین شماره آن را در ژانویه ۲۰۰۷ برابر با دی ۱۳۸۹ منتشر کرده است. مراجعه کنید به سایت <https://www.cybercrimejournal.com> (کرامتی معز، ۱۳۹۹: ۲۴).

همچنین جرم‌شناسی سایبری یک شاخه میان‌رشته‌ای است که محققان رشته‌های مختلفی مانند جرم‌شناسی، بزه دیده شناسی، جامعه‌شناسی، علوم اینترنت و علوم کامپیوتر را در برمی‌گیرد. جایشانکار (۲۰۰۷) بنیانگذار رشته دانشگاهی جرم‌شناسی سایبری است و جرم‌شناسی سایبری را به عنوان «مطالعه علل جرایمی که در فضای مجازی رخ می‌دهد و تأثیر آن در فضای فیزیکی» ابداع و تعریف کرد. با این اوصاف جرم‌شناسی مجازی را به عنوان مطالعه علت شناسی جرایمی که در فضای مجازی اتفاق می‌افتد و تأثیر آن در فضای واقعی و فیزیکی تا ارائه راهکارهای پیشگیرانه می‌دانیم (کرامتی معز، ۱۳۹۹: ۲۵).

3. Jaishankar, K. (2008); Space Transition Theory of Cyber Crimes, in: Schmallerger, F. & Pittaro, M. (eds.). Crimes of the Internet. Upper Saddle River, NJ: Prentice Hall, pp. 283-301. <http://www.cybercrimejournal.com/Editoriaijccjuly.pdf>



بدین سان 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، خانوادگی 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. بر این اساس، ارزش‌های مجازی به واسطه ویژگی‌های منحصربه‌فردی که در چارچوب ناشناختگی و انعطاف هویت ایجاد می‌کنند؛ زمینه را برای ارتکاب جرم فراهم می‌سازند (صفاری و همکاران، ۱۳۹۹: ۲۳۹). عموم مجرمان مرتبط با رمز ارزها تمایلی به مواجهه حضوری با کاربران ندارند. از این‌رو معاملات آنلاین زمینه را برای ارتکاب این جرایم فراهم می‌سازد.

#### ۴. تئوری جرم‌شناسی آبی

دامنه مطالعات و تحقیقات رشته‌های تخصصی علوم جنایی نیز در پرتو تحولات جهانی شدن متحول شده و گسترش فرآیند جهانی شدن در حوزه‌های مختلف علوم اجتماعی به حوزه بزهکاری نیز تسری پیدا کرده است. حقوق کیفری با جهانی شدن معضل جرم، تدابیر متعددی را در سطح ملی و بین‌المللی توصیه نموده است، ولی جرم‌شناسی با چند دهه تأخیر به اندیشه و فرآیند جهانی شدن توجه نموده است. بدین ترتیب، در حال حاضر با توجه به تحول متغیرهای مطالعات جرم‌شناسی، ناکارآمدی مطالعات جرم‌شناختی در سطح ملی، ضرورت استقلال علمی در قبال ملاحظات سیاسی و اجتماعی دولت‌ها و کمک به توسعه فعالیت‌های علمی جرم‌شناسی در سطح بین‌المللی، ایجاب می‌کند که این علم نیز جهانی شده و ضمن انجام تحقیقات و مطالعه در سطح بین‌المللی، راهکارهای بین‌المللی نیز برای جامعه جهانی در قبال پدیده بزهکاری ارائه نماید (بابایی، ۱۳۹۰: ۱۱۵).

با توجه به اینکه امروزه بسیاری از جرایم از وصف جهانی و فراملی برخوردار شده‌اند، پیشگیری از ارتکاب جرایم نیز در بعد جهانی و فراملی باید مورد توجه قرار گیرد.<sup>۱</sup> این امر به ویژه در خصوص جرایم ارتكابی در بستر فضای مجازی و ابزارهای فناورانه 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

۱. جرم‌شناسی جهانی یک رشته نوظهور است که جنایات بین‌المللی و فراملی را پوشش می‌دهد (جیشانکار و رونل، ۲۰۱۳)، پیشگیری از نوع کیفری آن، در اسانامه دیوان و اسناد بین‌المللی دیگر مورد توجه قرار گرفته است و در مقابل، تدابیر پیشگیری غیرکیفری روی هم رفته مورد غفلت واقع شده است. مطالعات جرم‌شناسی فراملی می‌تواند خلأهای موجود راهبردهای پیشگیری جرم‌شناسانه یعنی پیشگیری اجتماعی - فرهنگی، پیشگیری موقعیت مدار فنی - فناورانه و پیشگیری بالینی را نیز در سیاست جنایی بین‌المللی پر کند (نجفی ابرندآبادی، ۱۳۹۶: ۲۳-۲۲).

چارچوب مبانی «جرم‌شناسی آبی»<sup>۱</sup> نیز مورد تأکید قرار گرفته است (صفاری و همکاران، ۱۳۹۹: ۲۴۱).

اصطلاح «جرم‌شناسی آبی» را اسلاومیر مارک ردو<sup>۲</sup> از کارشناسان باسابقه سازمان ملل متحد در کتاب «جرم‌شناسی آبی: قدرت اندیشه‌های سازمان ملل متحد برای مقابله با جرم در سطح جهانی: یک مطالعه تک نگارانه» (۲۰۱۲) به کار برد<sup>۳</sup>. این گرایش نوین جرم‌شناختی عبارت است از مطالعه آن دسته از فعالیت‌ها، نوشتگان و رویدادهایی که سازمان ملل متحد در زمینه جرم، بزهکاران و چگونگی پیشگیری از آنها یا کنترل و مبارزه با آنها، بر پایه مفهومی‌ها و نظریه‌های جرم‌شناسانه، در قالب هنجارها، مقرره‌ها و یا رهنمودهایی به تصویب رسانده است (رایجیان اصلی، ۱۴۰۱: ۴۷۰-۴۶۹). به عبارتی جرم‌شناسی آبی بیانگر رهنمودهای جرم‌شناسی سازمان ملل است. این جرم‌شناسی به دنبال همکاری‌های بین‌المللی در زمینه پیشگیری از جرم به ویژه جرایم سازمان‌یافته فراملی، پول‌شویی، دزدی دریایی، تروریسم و فساد مالی است (ردو، ۲۰۱۲: ۴۶). با توجه به مطالب فوق و در راستای انطباق تئوری جرم‌شناسی آبی با رمز ارزها و جرایم مرتبط با آن، می‌توان انتظار تدوین سیاست پیشگیرانه وضعی متحدالشکل جهت افزایش نظارت ملی و بین‌المللی بر رمز ارزها داشت.

## یافته‌ها

### ۱. تدابیر نظارتی

یکی از مهم‌ترین راهبردهای پیشگیری وضعی تدابیری است که سعی در کنترل و نظارت دارد. در ابتدای امر لازم به ذکر است که این نوع نظارت به معنای ورود به حریم خصوصی زندگی افراد و همچنین دخالت در آن نیست (کرامتی معز، ۱۳۹۹: ۱۵۰)، بلکه منظور از آن به کارگیری تدابیری حمایتی و نظارتی است که سعی در جلوگیری از ارتکاب جرم دارد (منصورآبادی و همکاران، ۱۴۰۰: ۳۳). از این‌رو نظارت همواره به عنوان عاملی برای پیشگیری از جرم مد نظر بوده و توانسته تا حدودی در این خصوص کارا باشد. بهره‌گیری از این ابزار برای پیشگیری از جرایم مرتبط با رمز ارزها به صورت‌های مختلفی امکان‌پذیر است که در ذیل به مطالعه آنها خواهیم پرداخت.

1. blue criminology

2. Slawomir Redo

3. Redo. Slawomir (2012). Blue Criminology, The Power of United Nations Ideas to Counter Crime Globally: A Monographic Study, European Institute for Crime Prevention and Control, Affiliated with the United Nations



## ۱-۱. نصب و راه اندازی سیستم های KYC

به طور سنتی مفهوم مبارزه با پول شویی (AML) با سیستم «مشتري خود را بشناسيد» (KYC)، سیستم های انطباق و نظارت و گزارش دهی بانک ها و سایر ارائه دهندگان خدمات مالی متکی است. بسته به مقیاس معاملات، محل اقامت شریک تجاری و به ویژه در روابط قراردادی با افراد متعرض سیاسی، ارائه دهندگان خدمات مالی باید هویت شرکای قراردادی خود را بررسی کنند، اطلاعاتی را در مورد هدف و نوع رابطه تجاری مورد نظر جمع آوری کنند. ارزیابی ریسک انجام دهند و نظارت مداوم بر رابطه خود نمایند (توصیه های FATF شماره ۲۳-۱۰).

در زمینه ارزش های سنتی و «واقعی»، این مفهوم مسلماً مؤثر است؛ زیرا شخص فقط می تواند با یک حساب بانکی در سیستم پول سپرده مشارکت کند. برخلاف آن، در سیستم ارزش های دیجیتال، کاربران می توانند «حساب» (کیف پول) خود را در سیستم خود ایجاد کنند و هر تعداد جفت کلید را که می خواهند بدون دخالت هیچ ارائه دهنده خدمات مالی ایجاد نمایند (گوآداموز<sup>۱</sup> و مارسدن<sup>۲</sup>، ۲۰۱۹: ۲۳).

برای پیشگیری از جرایم مرتبط با رمز ارزها چندین دولت و سازمان فراملی در حال برنامه ریزی برای نصب و راه اندازی سیستم های KYC برای پلتفرم های مبادله هستند. به طور مثال می توان به قانون بیت لایسنس نیویورک<sup>۳</sup>، قانون خدمات پرداخت ژاپن<sup>۴</sup>، لایحه کانادا موسوم به سی ۳۱<sup>۵</sup> و قانون ارائه دهندگان مبادلات ارز دیجیتال در قانون مبارزه با پول شویی و مبارزه با تأمین مالی تروریسم در استرالیا<sup>۶</sup> نام برد. به عنوان یک مرحله مقدماتی ضروری برای KYC و بررسی دقیق، دولت ها شروع به قرار دادن مجوز تجارت با ارزش های دیجیتال و مبادله آنها تحت حق شرط تأیید نظارتی مطابق قوانین مذکور کردند (گوآداموز و مارسدن، ۲۰۱۹: ۳۴).

## ۱-۲. محدودیت دسترسی به رمز ارزها و قرار گرفتن در لیست سیاه

رمز ارزها با طراحی متفاوت باید بسته به ویژگی های تکنولوژیکی آنها به طور متفاوتی نظام مند شوند. به طور مثال طراحی فناوری سیستم بیت کوین به نحوی است که فرصت های زیادی را برای تنظیم کنندگان فراهم می کند. بر این اساس در درجه اول، مقامات می توانند دسترسی به رمز ارزها را محدود کنند. محدود کردن دسترسی به نرم افزار بیت کوین (به عنوان مثال مشتریان بیت کوین، کیف پول های آنلاین) یک رویکرد نظارتی قابل تصور است، هرچند به سختی قابل اجرا است. در

1. Guadamuz

2. Marsden

3. BitLicense Law of the State of New York, section 200.15 (e) (1).

4. Payment Services Act of Japan from April 2017

5. Canada's Bill C-31

6. the inclusion of Digital Currency Exchange Providers in the Anti-Money Laundering and Counter Terrorism Financing Act in Australia 2018

درجه دوم، مقامات دولتی می‌توانند با مشارکت در استخراج دولتی یا با تنظیم کردن تولید یا دسترسی به سخت‌افزار استخراج، تلاش کنند تا فرآیند استخراج را کنترل یا حداقل تحت تأثیر قرار دهند. در درجه سوم، مبادله ارز دیجیتال با پول و کالاهای واقعی می‌تواند توسط مقامات محدود و یا کنترل شود، مانند چین و هند که در حال حاضر انجام می‌دهند (تراتمن<sup>۱</sup> و هارل<sup>۲</sup>، ۲۰۱۷: ۲۱).

ویژگی غیرمتمرکز شبکه بیت کوین یک استدلال قوی برای اجرای مفاهیم پیشگیری است که به سمت حفاظت از دروازه که در مرز بین ارزهای دیجیتال و دنیای واقعی عمل می‌کنند، هدایت می‌شود. یک مثال قابل توجه از چنین رویکردهایی، فهرست سیاه تراکنش‌ها است. هدف از این مفهوم، فهرست سیاه تراکنش‌هایی است که ناشی از جرایمی مانند کلاهبرداری و پول‌شویی است. بازیگران سیستم بیت کوین مانند پلتفرم‌های صرافی و بازرگانانی که بیت کوین‌ها را برای پرداخت می‌پذیرند، مجاز به پذیرش تراکنش‌های لیست سیاه یا تراکنش‌هایی نیستند که می‌توانند در قالب تراکنش‌های فهرست سیاه ردیابی شوند. مزیت چنین رویکردی این است که پلتفرم‌های مبادله‌ای و بازرگانانی برای سازمان‌های مجری قانون ملموس هستند؛ زیرا در دنیای واقعی فعالیت می‌کنند (کارلا<sup>۳</sup>، ۲۰۱۶: ۱۹۳).

مزیت دیگر در حداقل کاهش جزئی ارزش بیت کوین از تراکنش‌های لیست سیاه نهفته است که این کاهش ارزش هم به دلیل یک اثر اقتصادی و هم اثر قانونی ایجاد می‌شود. کاربران بیت کوین قیمت بیت کوین‌های لیست سیاه را به همان قیمت بیت کوین‌های لیست نشده پرداخت نمی‌کنند؛ زیرا نمی‌توانند از آنها استفاده کنند. اگر لیست سیاه تراکنش عمومی بود (حداقل کاربران می‌توانستند درخواست کنند که آیا بیت کوین‌های ارائه شده از یک تراکنش فهرست شده منشأ می‌گیرند یا خیر)، کاربران مجبور می‌شدند برای جلوگیری از پیگرد کیفری، لیست را بررسی کنند. برای پول‌شویی این امر باعث می‌شود که فعالیت‌های مجرمانه با هدف به دست آوردن بیت کوین جذابیت کمتری داشته باشد. لازم به ذکر است که کاهش ارزش بیت کوین‌های لیست سیاه می‌تواند سیستم بیت کوین را با مشکل مواجه کند، گفته شده است که قرار گرفتن در لیست سیاه منجر به از دست دادن ارزش چشم‌گیر بیت کوین می‌شود (کارلا، ۲۰۱۶: ۱۹۵).

امکان ردیابی تک‌تک ارزهای دیجیتال به مبدأ خود فرصت دیگری را برای تنظیم‌کننده‌ها فراهم می‌کند، حتی اگر به‌طور مثال چندین بیت کوین در کیف پول یک کاربر ذخیره شده باشد (دقیقاً کلیدهای خصوصی در آن ذخیره می‌شوند) از این‌رو، برخلاف سیستم‌های بانکداری کلاسیک، خروجی‌های تراکنش واحد در هر زمان از یکدیگر جدا می‌شوند و بنابراین می‌توانند

1. Trautman  
2. Harrell  
3. Carla



بدون «مسموم کردن» تمام بیت کوین‌های مربوط به کلید عمومی مربوطه در لیست سیاه قرار گیرند (بومه<sup>۱</sup> و همکاران، ۲۰۱۵: ۲۳۲).

چالش اصلی این است که اگر کاربران مجبور نباشند هنگام باز کردن حساب خود را شناسایی کنند، سیستم‌های استاندارد (KYC<sup>۲</sup>) کار نمی‌کنند. علاوه بر این، نام مستعار ارزهای رمزنگاری شده مانع شناسایی هر مفهومی می‌شود که به دانش هویت کاربران بستگی دارد، همان‌طور که توسط سازمان‌های مجری قانون نظارت بر یک فرد لازم است. از سوی دیگر، سابقه تراکنش‌های عمومی رویکردهای نظارتی جدیدی را امکان‌پذیر می‌کند. به عنوان مثال، در مقایسه با بازیابی پول نقد دزدیده شده از گردش، امکان جداسازی و کاهش ارزش بیت کوین از طریق فهرست سیاه تراکنش وجود دارد. همین امر در مورد سود سایر فعالیت‌های غیرقانونی مانند قاچاق مواد مخدر نیز صدق می‌کند (موزر و همکاران، ۲۰۱۴: ۱۱).

علی‌رغم پیشرفت‌هایی که فهرست سیاه تراکنش‌ها در تنظیم ارزهای دیجیتال به همراه دارد، این مفهوم دارای کاستی‌هایی نیز می‌باشد. اول از همه، یک لیست سیاه که توسط مقامات دولتی نگهداری می‌شود، نمی‌تواند معاملات خارج از زنجیره را پوشش دهد؛ بنابراین مقامات دولتی به همکاری ارائه‌دهندگان خدماتی که تراکنش‌های خارج از زنجیره را انجام می‌دهند، وابسته خواهند بود. با این حال، در صورت لزوم، آنها می‌توانند با قوانین و تحریم‌های مربوطه مجبور به همکاری شوند. علاوه بر این، سیستم فهرست سیاه تراکنش‌ها باید در سرتاسر جهان اجرا شود تا اثربخشی کامل آن توسعه یابد.

با این حال، در حال حاضر بعید به نظر می‌رسد که همه دولت‌ها بتوانند در مورد یک لیست سیاه مشترک به توافق برسند، به‌ویژه به این دلیل که فعالیت‌های متفاوت در دولت‌های مختلف به عنوان «فعالیت‌های غیرقانونی» طبقه‌بندی می‌شوند. البته به نظر می‌رسد، توافق در اتحادیه اروپا ممکن باشد، اما یک لیست سیاه صرفاً اروپایی احتمالاً با مقررات سایر دولت‌ها تضاد دارد. برای حل این مناقشات، باید توافقات بین‌المللی مناسبی با این کشورها منعقد شود و در نهایت، یک سیستم کارآمد فهرست سیاه می‌تواند توسط رژیم‌های اقتدارگرا مورد سوء استفاده قرار گیرد تا مخالفان سیاسی خود را از این امکانات تا حد زیادی محروم کند. به عنوان مثال می‌توان به سوء استفاده دولت‌های مستبد از ابزار حکم بازداشت بین‌المللی برای بازداشت منتقدان رژیم اشاره کرد (پونزفورد<sup>۳</sup>، ۲۰۱۵: ۳۸).

1. Boehme

2. Know-Your-Customer

3. Ponsford

### ۳-۱. نظارت بر صرافی‌های آنلاین

با وجود امنیت ارائه شده توسط ارزهای دیجیتال، باید به این نکته توجه کنیم که در بسیاری از مواقع آنها، ابزاری برای ارتکاب کلاهبرداری هستند و برای فرار مالیاتی (اغلب به دلیل ناآگاهی از مقررات مالیاتی)، انجام معاملات غیرقانونی یا پولشویی مورد استفاده قرار می‌گیرند. مطالعه‌ای بر روی مجموعه داده‌ای از ۴۶۸۱ حساب شبکه اتریوم انجام شد و مشخص شد که ۲۱۷۹ حساب غیرقانونی بودند (فاروژیا<sup>۱</sup> و همکاران، ۲۰۲۰: ۵۶).

گزارش جغرافیای ارزهای دیجیتال نشان می‌دهد که بیت‌کوین ریسک پایینی برای پولشویی دارد یا همچنین نشان می‌دهد که از یک بازار ۵۰۰ میلیارد دلاری، تنها ۱۰ میلیارد دلار در کلاهبرداری و سایر فعالیت‌های غیرقانونی (دو درصد از کل) استفاده می‌شود (ناوارو کاردوسو<sup>۲</sup>، ۲۰۱۹: ۱۷).

در نظام بانکداری سنتی، واسطه، بانک و نظارت مقامات دولتی وجود دارد، ولی در رمز ارزها، این بازیگران ناپدید می‌شوند و به دلیل عدم وجود نهادی واسطه‌گر همچون بانک، ایجاد حساب برای هیچ‌یک از طرفین که منجر به افشای هویت آنها می‌شود نیز ضروری نیست، بلکه ساخت کیف پول می‌تواند به صورت کاملاً محرمانه و بدون افشای مشخصات فردی انجام گیرد (منصورآبادی و همکاران، ۱۴۰۱: ۱۰).

علاوه بر این، صرافی‌ها (به‌ویژه در ایران)، بنگاه اصلی خرید و فروش بیت‌کوین سایر ارزهای مجازی هستند و باید الزامات لازم الرعایه در خصوص بانک‌ها در زمینه شفافیت مبادلات مالی در مورد صرافی‌ها نیز به‌دقت اعمال شود. همان‌طور که ملاحظه می‌شود در ماده (۵) اصلاحیه قانون مبارزه با پولشویی مصوب ۱۳۹۷ نیز موظف به رعایت مفاد قانون مبارزه با پولشویی و قانون مبارزه با تأمین مالی تروریسم هستند (قاسمی و بیاتی، ۱۴۰۰: ۱۰۱).

با ارزهای دیجیتال، ابزارها و خدماتی توسعه یافته‌اند که می‌توانند برای مقاصد غیرقانونی نظیر تأمین مالی تروریسم و پولشویی استفاده شوند. ناشناس بودن یا شبه ناشناس بودن (بسته به بلاک‌چین مورد استفاده) در مالکیت ارز دیجیتال، با استفاده از روش‌های مختلف مانند «میکسر»<sup>۳</sup> و «صرافی»<sup>۴</sup>، می‌تواند در برخی موارد مانع از بررسی و ردیابی عملیات شود. برای پولشویی ویژگی‌های اصلی ارزهای دیجیتال امنیت، سرعت، مبتنی بر رمزنگاری، ناشناس بودن، غیرمتمرکز بودن، حذف واسطه‌ها و تسهیل در معاملات بین‌المللی قابل توجه است. همه این ویژگی‌ها،

1. Farrugia  
2. Navarro Cardoso  
3. mixers  
4. exchanges



ارزهای دیجیتال را به محصولی جذاب و مفید برای برخی جرایم مانند پول‌شویی تبدیل می‌کند (بارویلِت<sup>۱</sup>، ۲۰۱۹).

در اتحادیه اروپا، در ۳۰ می ۲۰۱۸، دستورالعمل، همچنین به عنوان «دستورالعمل پنجم»<sup>۲</sup>، در مورد جلوگیری از استفاده از سیستم مالی به منظور پول‌شویی، به تصویب رسید و منتشر شد. در این دستورالعمل برای اقدامات پیشگیرانه از جرایم در بستر رمز ارزها به موضوع نظارت بر صرافی‌های آنلاین و تعیین دستورالعمل فعالیت آنها اشاره دارد. همچنین FATF در سال ۲۰۱۹ راهنمای دارایی‌های مجازی و ارائه‌دهندگان خدمات را منتشر کرد که بر مبنای آن نظارت دولت بر فعالیت صرافی‌های آنلاین را مورد توجه قرار داده است. این دستورالعمل‌ها جنبه‌های متعددی از جنبه نحوه فعالیت صرافی‌های آنلاین را شامل می‌شود که یکی از هدف آن این است که ارائه‌دهندگان را وادار کند تراکنش‌های مشکوک را گزارش کنند.

#### ۱-۴. نظارت مؤثر در ارائه‌دهندگان خدمات رمز ارزها

در اکتبر ۲۰۱۸، کارگروه ویژه اقدام مالی<sup>۳</sup> تغییراتی در توصیه‌ها و واژه‌نامه‌های خود اعمال کرد تا صریحاً روشن کند که این توصیه‌ها در مورد فعالیت‌های مالی شامل دارایی‌های مجازی اعمال می‌شود. کارگروه ویژه اقدام مالی از اصطلاح «دارایی‌های مجازی» استفاده می‌کند که به صورت دیجیتالی قابل معامله با انتقال است و می‌تواند برای مقاصد پرداخت با سرمایه‌گذاری استفاده شود که شامل اشکال تبدیل‌پذیر، تبدیل‌ناپذیر و متمرکز و غیرمتمرکز و همچنین ICO است. اینها فقط به دارایی‌هایی که به رمزنگاری تکیه می‌کنند، محدود نمی‌شود، مطابق با توصیه اصلاح شده این کارگروه، لازم است ارائه‌دهندگان خدمات دارایی‌های مجازی به دلیل پول‌شویی و مبارزه با تأمین مالی تروریسم (CFT)، دارای مجوز باشند یا ثبت شوند و مشمول سیستم‌های مؤثر برای نظارت قرار گیرند. این کارگروه با بیان دقیق‌تر الزامات اجرای دقیق برای نظارت مؤثر در ارائه‌دهندگان خدمات دارایی مجازی را ارائه می‌دهد. طبق دستورالعمل کارگروه ویژه اقدام مالی، ارائه‌دهندگان سرویس‌های مرتبط با ارزهای دیجیتال باید اطلاعات مشتریان خود را با یکدیگر به اشتراک بگذارند و اطلاعات را درون تراکنش‌ها روی بلاک‌چین عمومی قرار دهند تا از دید عموم مخفی نباشند. همچنین، به تمامی کشورهای عضو این گروه توصیه شده تا سیستم کسب و کار خودشان را مشابه با بانکداری تجاری پیش ببرند (منصورآبادی و همکاران، ۱۴۰۱: ۱۶).

1. Barroilhet.

2. (EU) 2018/843

3. Financial Action Task Force (FATF)

## ۲. تدابیر افزایش دشواری ارتکاب جرم

یکی از تدابیر پیشگیری وضعی که کلارک معرفی کرد، تدبیر و افزایش دشواری ارتکاب جرم است (صفاری، ۱۳۸۰: ۲۹۳). در این روش به راهبردهایی که به تغییر وضعیت، فرصت و موقعیت اشاره دارد مانند کنترل ورودی‌ها و خروجی‌ها، ایجاد فضای قابل دفاع، جمع‌آوری ابزار و لوازم ارتکاب جرم، ایجاد مانع برای خرابکاران، مصونیت بخشی به آماج‌ها و... که جملگی منجر به ناتوان کردن فاعل از محقق ساختن نیت مجرمانه خود می‌شود می‌پردازد (میرخلیلی و همکاران، ۱۳۹۷: ۱۱۶). اگر بتوان با استفاده از تکنیک‌هایی زحمت فردی را که قصد ارتکاب جرم دارد، در راه رسیدن به هدف مورد نظرش افزایش داد، می‌توان انتظار داشت که از انجام جرم منصرف شود. حال باید دید که در مورد جرم شکنجه چگونه می‌توان این تدبیر را به کار گرفت (شیدائیان و همکاران، ۱۳۹۷: ۹۴).

دولت‌ها باید مفاهیم نظارتی و روش‌های تحقیق جدیدی را توسعه دهند و یا روش‌های سنتی را تعدیل کنند. هر دو روش می‌تواند بر نیازها و منافع چندین شخص حقیقی و حقوقی در داخل و اطراف سیستم رمز ارزها مؤثر باشد.

## ۲-۱. استفاده از داده‌های بلاک چین عمومی

ساختار غیرمتمرکز شبکه بیت کوین و نام مستعار کاربران مشکلاتی را برای دادستان‌ها و دستگاه تعقیب کیفری ایجاد می‌نماید. به طور سنتی، مسئولان مرتبط با تحقیقات مقدماتی در زمینه جرایم مالی، هنگام ردیابی پول، به جستجو و ضبط اسناد و پرونده‌های بانکی، بازجویی از کارمندان بانک به عنوان شاهد و بررسی خودکار حساب‌های بانکی متکی هستند. بدون مدیریت مرکزی و توانایی هر کاربر برای ایجاد تعداد نامحدودی از حساب‌ها توسط خودش، این روش‌های سنتی تحقیقات، محکوم به شکست است. آنها فقط زمانی موفق هستند که مظنون از یک حساب ارائه شده توسط یک ارائه‌دهنده خدمات استفاده کند که دارای سیستم KYC اجباری است. اگرچه تعداد سیستم‌های KYC با مقررات دولتی افزایش می‌یابد، اما محققین باید راه‌هایی برای شناسایی کاربران بیت کوین که تحت پوشش سیستم‌های KYC نیستند، بیابند (سوکرمن<sup>۱</sup>، ۲۰۱۵: ۷۲).

برای مقابله با این چالش، پژوهشگران می‌توانند از داده‌های بلاک چین عمومی استفاده کنند. به این ترتیب که هر تراکنش را از طریق بلاک چین تا پیدایش بیت کوین‌های منتقل شده ردیابی کرد. به این ترتیب محققین قادر به نتیجه‌گیری در مورد اشخاص حقیقی و حقوقی درگیر خواهند بود. این رویکرد می‌تواند با پیاده‌سازی پایگاه‌های اطلاعاتی کاربران رمز ارز مرکزی برای واحدهای



اطلاعات مالی مانند پیشنهاد شده در پنجمین دستورالعمل AML اتحادیه اروپا پشتیبانی شود (سوکرمن، ۲۰۱۵: ۷۳).

## ۲-۲. طبقه‌بندی بازیگران حقیقی و حقوقی شبکه رمز ارزها

شناسایی بازیگران حقیقی و حقوقی شبکه ارز دیجیتال به منظور بررسی حقوق اساسی که باید در نظر گرفته شوند، ضروری است. در نظام پولی و بانکی سنتی، دولت‌ها، بانک‌های مرکزی، بانک‌های خصوصی و سایر پردازشگرهای پرداخت، بازیگران اصلی هستند. در واقع دولت‌ها ارزها را ایجاد می‌کنند و بانک‌ها سیستم را اجرا می‌کنند و تابع قوانین دولتی هستند. سایر اشخاص حقیقی و حقوقی مانند مشتریان و بازرگانان بانک‌ها تنها مجاز به فعالیت در قالب این شرایط می‌باشند.

به عنوان مثال، هر مشتری بانک باید هنگام افتتاح حساب بانکی، خود را با یک سند رسمی معرفی کند. در مقابل، به طور مثال هر کاربر بیت کوین می‌تواند با ارائه قدرت محاسباتی به سیستم، بیت کوین ایجاد کند و سیستم توسط شبکه همتا به همتا، به عبارت دیگر، توسط همه کاربران - که قدرت CPU را تأمین می‌کنند - اداره می‌شود. از این رو، رویکردهای نظارتی و روش‌های تحقیق نمی‌توانند (فقط) روی بانک‌ها تمرکز کنند، بلکه آنها باید انواع مختلفی از اشخاص حقیقی و حقوقی را در داخل و اطراف سیستم بیت کوین در نظر بگیرند. بر این مبنا افراد داخل و اطراف شبکه رمز ارزها را می‌توان به سه گروه تقسیم کرد: افراد «داخل» سیستم، افراد به اصطلاح اکوسیستم و افرادی که در دنیای واقعی اقتصاد فعالیت می‌کنند. دسته بعدی شامل چندین گروه از اشخاص حقیقی و حقوقی در اقتصاد دنیای واقعی مانند بانک‌ها، تراست‌ها، بازرگانان و ارائه‌دهندگان خدمات است که واحدهای ارزهای دیجیتال را خرید و فروش می‌کنند یا ارزهای دیجیتال را برای پرداخت می‌پذیرند (هکر<sup>۱</sup> و تومال<sup>۲</sup>، ۲۰۱۸: ۵).

امروزه اکثر کاربران رمز ارزها دیگر خودشان ارزهای دیجیتال خود را مدیریت نمی‌کنند (کلید خصوصی آدرس‌های بیت کوین خود را خودشان در کیف پول ذخیره نمی‌کنند)، بلکه مدیریت کلیدهای خصوصی را به طور کامل به یک ارائه‌دهنده خدمات واگذار می‌کنند (به عنوان مثال ارائه‌دهنده کیف پول)؛ بنابراین، این افراد به معنای محدودتر کاربران بیت کوین نیستند، بلکه فقط مشتریان «بانک‌های سایه» هستند؛ بنابراین، آنها وضعیت حقوقی مشابهی با مشتریان عادی بانک دارند (هکر و تومال، ۲۰۱۸: ۶).

1. Hacker  
2. Thomale

درست است که افرادی که صرفاً ادعایی علیه ارائه دهنده خدمات بیت کوین دارند، مانند سایر دارندگان ادعاهای خارج از سیستم های ارزشهای دیجیتال، از حمایت حقوق اساسی (مانند حق مالکیت) برخوردارند. با این حال، این موضوع ارتباط اظهارات زیر در مورد حقوق اساسی را برای آن دسته از کاربرانی که کلیدهای خصوصی خود را به تنهایی مدیریت می کنند، تغییر نمی دهد و بنابراین در واقع خودشان به عنوان «مالک» بیت کوین ها در نظر گرفته می شوند. البته، هیچ مطالعه تجربی در مورد این مسأله منتشر نشده است که چه تعداد از کاربران بیت کوین واقعاً بیت کوین های خود را مدیریت می کنند، چه تعداد از کاربران از ارائه دهنده خدمات استفاده می کنند و چگونه این ارائه دهنده گان خدمات دقیقاً بیت کوین ها را برای مشتریان خود مدیریت می کنند. علاوه بر این، رفتار کاربران در بیت کوین یا سایر سیستم های ارزشهای دیجیتال می تواند در هر زمان تغییر کند، به طوری که ملاحظات اساسی در مورد حمایت از حقوق اساسی همچنان در آینده مهم خواهد بود و در نهایت، مفاهیم نظارتی باید آن دسته از کاربرانی را پوشش دهد که به عمد از ارائه دهنده گان خدمات تنظیم شده برای دور زدن مقررات سنتی AML استفاده نمی کنند (کریستوفر<sup>۱</sup>، ۲۰۱۴: ۶).

## ۲-۳. حفاظت از داده های شخصی

مفهوم «داده های شخصی» همزمان با داده های عمومی و در نقطه مقابل آن پدید آمده است، ولی در گذر زمان، به عنوان مفهوم مستقل مورد توجه قرار گرفته و به ویژه از نظر تجاری، اهمیتی بیش از داده های عمومی پیدا کرده است؛ به گونه ای که اکنون، هر جا از احکام حقوقی داده صحبت می شود بلافاصله، داده های شخصی به ذهن مخاطبان متبادر می شود و نه سایر انواع داده. همچنین در حال حاضر این اصطلاح در اروپا در برابر اصطلاح «داده های غیر شخصی» به کار می رود نه داده های عمومی (انصاری و همکاران، ۱۴۰۰: ۹۰).

تعریف مقررات اتحادیه اروپا درباره حمایت از داده های شخصی که اکنون مورد الهام قوانین و رویه های مختلف در دنیاست، به شرح زیر است: «داده های شخصی عبارت است از هر گونه اطلاعات مربوط به یک شخص حقیقی با هویت مشخص یا قابل شناسایی (شخص موضوع داده)؛ شخص حقیقی قابل شناسایی کسی است که مستقیم یا غیرمستقیم، به ویژه از طریق ارجاع به یک شناسه مانند نام، شماره شناسایی، داده های مکانی، یک شناسه برخط یا یک یا چند عامل خاص درباره هویت جسمی، روانی، ژنتیک، ذهنی، اقتصادی، فرهنگی یا اجتماعی آن شخص، قابل شناسایی است».

اهمیت روزافزون و کلیدی داده های شخصی برای انواع فعالیت های تجاری و غیر تجاری موجب شده است که در سه سطح بین المللی، ملی و سازمانی یا شرکتهای، قواعد و ضوابطی در زمینه

1.Christopher



نحوه جمع آوری و استفاده از داده‌های شخصی وضع شود. این قواعد و ضوابط را بر حسب رویکردهایی که دنبال کرده‌اند حداقل می‌توان به سه دسته تقسیم کرد: رویکرد آمریکایی مبتنی بر جریان آزاد داده‌های شخصی و آزادی استفاده تجاری از آنها، رویکرد اروپایی مبتنی بر حمایت از حقوق افراد و حق کنترل آنها بر سرنوشت داده‌های مرتبط با خود و رویکردهای مختلط که عمدتاً از سوی دولت‌های چین، روسیه و برخی دیگر از دولت‌ها اتخاذ شده است.

حق حفظ حریم خصوصی داده‌ها زمانی مطرح می‌شود که مقامات داده‌های مربوط به یک شخص حقیقی (حقوقی) را جمع آوری، ذخیره، به اشتراک بگذارند یا پردازش کنند و از این طریق «زندگی خصوصی» شخص تحت تأثیر قرار گیرد. برخلاف محدوده آزادی ارتباطات از راه دور، دامنه حریم خصوصی داده‌ها می‌تواند شامل حفاظت از داده‌های عمومی باشد که سازمان‌های دولتی داده‌های عمومی را به طور سیستماتیک جمع آوری و ذخیره می‌کنند. بسیار مهم است که روشن شود که «سیستماتیک» لزوماً به معنای جمع آوری، ذخیره یا پردازش داده‌ها در مقیاس وسیع نیست. به کارگیری این اصول در داده‌های عمومی اینترنتی (مانند داده‌های موجود در بلاک چین) به طبقه‌بندی خاصی منجر می‌شود. بدین ترتیب که صرف مرور و جستجوی داده‌ها در بلاک چین تداخلی در حق تلقی نمی‌شود (بولن<sup>۱</sup>، ۲۰۱۳: ۹۸).

حفاظت از داده‌های شخصی با این حال، زمانی که سازمان‌های مجری قانون، دادستان‌ها یا تنظیم‌کننده‌ها به طور سیستماتیک داده‌ها را از زنجیره بلوکی جمع آوری، ذخیره یا پردازش می‌کنند، مداخله در حق حفاظت از داده‌های شخصی قابل تصور است. برای مثال، پیاده‌سازی پایگاه‌های داده کاربران رمز ارز مرکزی تداخل جدی و گسترده‌ای با حق حفاظت از داده‌های شخصی خواهد بود. علاوه بر این، استفاده از ابزارهای جستجویی که داده‌ها را از زنجیره بلاک توسط مقامات جمع آوری و ذخیره می‌کنند تا زمانی که مقامات به داده‌های ذخیره‌شده دسترسی داشته باشند یا به این دلیل که داده‌ها در حوزه کنترل مقامات ذخیره می‌شوند، می‌تواند به عنوان تداخل تلقی شود، به عنوان مثال هنگامی که بازرسان جنایی از ابزارهای جستجوی ویژه‌ای استفاده می‌کنند که به‌طور خاص برای سازمان‌های مجری قانون طراحی شده‌اند که داده‌ها را برای ارائه یا بهبود سرعت جستجو یا نتایج ذخیره می‌کنند (داکونا<sup>۲</sup>، ۲۰۱۶: ۴۵).

مطابق با ماده «۲» (الف) دستورالعمل EC/۴۶/۹۵ داده‌های شخصی «به هر گونه اطلاعات مربوط به یک شخص حقیقی شناسایی شده یا قابل شناسایی است»، البته لازم نیست که داده‌ها حاوی اطلاعات یک شخص حقیقی (حقوقی) باشند. اطلاعات می‌تواند به یک شیء مربوط باشد تا زمانی که این شیء به یک شخص حقیقی (حقوقی) مربوط باشد. بند (۲۶) این دستورالعمل بیان

1 . Bollen  
2 . DaCunha

می‌کند که «همه ابزارهایی که احتمالاً به طور منطقی (...) برای شناسایی شخص مذکور مورد استفاده قرار می‌گیرند» باید هنگام تعیین اینکه آیا یک شخص قابل شناسایی است در نظر گرفته شود. از سوی دیگر، حق حفاظت از داده‌ها زمانی قابل اعمال نیست که داده‌ها «ناشناس ارائه شوند به گونه‌ای که موضوع داده دیگر قابل شناسایی نباشد».

داده‌های تراکنش در بلاک‌چین توسط حق حفاظت از داده‌ها در ماده ۷ و ۸ ECHR محافظت می‌شود. مشابه بحث در مورد آدرس‌های IP باید در نظر گرفت که دانستن کلیدهای عمومی که بخشی از یک تراکنش هستند، لزوماً منجر به شناسایی نهادهای شرکت کننده نمی‌شود؛ بنابراین، لزوماً «مالک قانونی» کلید عمومی نیست که باعث تراکنش بیت کوین می‌شود. علاوه بر این، باید در نظر گرفت که داده‌های تراکنش در بلاک‌چین دارای نام مستعار هستند. از این رو، نمی‌توان آن را صرفاً برای شناسایی کاربر بیت کوین استفاده کرد. با این وجود، داده‌های بلاک‌چین را می‌توان با مجموعه داده‌هایی از منابع دیگر (مانند تالارهای گفتگوی وب، سوابق تحقیق و غیره) ترکیب کرد تا کاربر مربوطه را شناسایی کند؛ بنابراین، کاربران بیت کوین را می‌توان به عنوان افرادی که به طور غیرمستقیم قابل شناسایی هستند طبقه‌بندی کرد. به دنبال بخش (۲۶) دستورالعمل EC/۴۶/۹۵، صرف امکان شناسایی کاربران برای گنجاندن داده‌های زنجیره بلوکی در محدوده حفاظت از داده‌های شخصی کافی است.

حق مالکیت در ماده ۱۷ CFR و ماده ۱ از پروتکل ECHR مقرر شده است این امر شامل «کلیه حقوق با ارزش دارایی ایجاد یک موقعیت قانونی تثبیت شده تحت سیستم حقوقی است که دارنده را قادر می‌سازد تا از آن حقوق به طور مستقل و به نفع خود استفاده کند؛ بنابراین، دامنه، محدود به اشیاء فیزیکی متحرک و غیرقابل حرکت نیست.

چندین موقعیت غیرمادی تحت حمایت مانند سهام شرکت یا حقوق مالکیت معنوی (ماده ۱۷ CFR (۲) یا حتی «حسن نیت» یک شرکت (پروتکل شماره ۱ بند ۴) در نظر گرفته شد. با این حال، حقوق باید «به اندازه کافی ایجاد شود تا قابل اجرا باشد» (بند ۵۹) و در محدوده حق مالکیت قرار گیرد (پروتکل شماره ۱ بند ۳ بند ۲۲). در نتیجه، «منافع یا فرصت‌های تجاری صرف» محافظت نمی‌شوند.

به نظر می‌رسد تعیین اینکه آیا نگهداری رمز ارزها در محدوده حق مالکیت قرار می‌گیرد یا خیر، دشوار است. از یک سو، وضعیت حقوقی رمز ارزها یکی از بحث‌برانگیزترین بحث‌ها در این زمینه است. با توجه به فقدان مادی بودن، واحدهای ارزشی رمزنگاری شده دارایی نیستند. علاوه بر این، آنها نه حق هستند و نه بدهی؛ زیرا مستلزم متعهد (حداقل یکی) از یک طرف و متعهد (حداقل یکی) از طرف دیگر است. حتی مقوله «مالکیت فکری» هم مناسب نیست؛ زیرا بر



خلق فکری متکی است و بیت کوین ها به صورت «مکانیکی» از طریق استخراج بدون هیچ دستاورد فکری ایجاد می شوند (ارلانک<sup>۱</sup>، ۲۰۱۶: ۶۵).

از سوی دیگر، واحدهای ارزشهای دیجیتال تمام معیارها را برای موقعیت ها و دارایی های محافظت شده توسط حق مالکیت برآورده می کنند. اول، بیت کوین ها دارای ارزش بازار هستند. این یک استدلال قوی برای گنجاندن بیت کوین در محدوده حق مالکیت است؛ زیرا اساساً حق مالکیت از واحدهای ارزش قابل تعریف به عنوان مبنایی برای آزادی محافظت می کند. دوم، بیت کوین ها را می توان به عنوان یک «حق انحصاری» نه بر اساس قانون، بلکه بر اساس ماهیتشان دید. تازمانی که کاربر مطمئن شود که تنها کسی است که کلید خصوصی را می داند و ذخیره می کند، دسترسی انحصاری به بیت کوین های اختصاص داده شده است. برخلاف سایر کالاهای مجازی مانند Linden-Dollar یا WoW-Gold، بیت کوین ها را نمی توان به سادگی توسط یک دستگاه حذف کرد، حتی مدیر سیستم؛ زیرا حتی یک نفر با این قدرت وجود ندارد (ارلانک، ۲۰۱۶: ۶۶).

همچنین واحدهای ارزش دیجیتال قابل تعریف هستند. دقیقاً می توان گفت که در هر مقطع زمانی چند بیت کوین با کلید عمومی مربوطه مرتبط است؛ بنابراین، به طور خلاصه، می توان گفت که بیت کوین ها تمام معیارهای «مالکیت مجازی» را برآورده می کنند: رقابت، پایداری، قابلیت اتصال، قابلیت تعریف و ارزش بازار. لذا به طور خلاصه، می توان بیان کرد که نگهداری واحدهای ارزی مانند بیت کوین باید توسط حق مالکیت محافظت شود؛ بنابراین، حق مالکیت باید به سمت یک مفهوم حفاظتی فراگیر برای دارایی های مجازی توسعه یابد. معیارهای فوق را می توان به عنوان تعریفی از «مالکیت مجازی» در محدوده حق مالکیت استفاده کرد. این موضوع این سؤال را ایجاد می کند که چه نوع تداخلی در حق مالکیت دارندگان ارزش دیجیتال قابل تصور است. به طور سنتی، مداخله در حق مالکیت به چند دسته تقسیم می شود: سلب مالکیت (مصادره)، مقررات استفاده از اموال و سایر مداخلات با پیامدهای واقعی و محرومیت از تصرفات را می توان به سلب مالکیت های قانونی و واقعی طبقه بندی کرد. نمونه ای از سلب مالکیت، کاهش کامل ارزش بیت کوین از طریق مفهوم فهرست سیاه تراکنش ها است. لازم به ذکر است آن دسته از کاربران بیت کوین که بیت کوین های خود را توسط یک ارائه دهنده خدمات (به عنوان مثال ارائه دهندگان کیف پول) اداره می کنند و فقط طبق قانون تعهدات علیه ارائه دهنده ادعا می کنند، از حمایت حق مالکیت مانند سایر دارندگان برخوردارند.

1 . Erlank

## بحث و نتیجه گیری

رمز ارزها به عنوان یک ارز مجازی غیر متمرکز، توزیع شده و قابل تبدیل که از نظر ریاضی بر اساس یک الگوریتم پیچیده است و از یک سیستم رمزنگاری برای اطمینان از یکپارچگی تراکنش‌های سیستمی که بر آن مبتنی است، استفاده می‌کند، درک می‌شود؛ اما چالش اصلی در این خصوص آن است که اگر کاربران مجبور نباشند هنگام باز کردن حساب خود را شناسایی کنند، سیستم‌های استاندارد (KYC) کار نمی‌کنند. علاوه بر این، نام مستعار ارزهای رمزنگاری شده مانع شناسایی هر مفهومی می‌شود که به دانش هویت کاربران بستگی دارد.

یافته‌های تحقیق حاکی از این است جهت اتخاذ سیاست پیشگیرانه وضعی، توجه به تئوری‌های جرم‌شناختی از اهمیت بسیاری برخوردار است و از تئوری‌های مرتبط در زمینه بررسی‌های جرم‌شناختی رمز ارزها، می‌توان به نظریه‌های انتخاب عقلانی، الگوی جرم و سبک زندگی برخط، گذار از فضا و جرم‌شناسی آبی اشاره نمود.

با توجه به خصوصیات رمز ارزها مداخله حقوق کیفری در این زمینه قابل توجیه نیست و مداخله حقوق کیفری باید به عنوان راه‌حل آخر گزینش شود؛ زیرا توسل به حقوق کیفری وقتی ضروری است که هیچ گزینه دیگری که فاقد وصف مداخله‌آمیز و تعدی‌گرا باشد در دسترس قرار ندارد. در این خصوص اقدامات پیشگیرانه می‌تواند مانعی مهم در خصوص ارتکاب جرایم مرتبط با رمز ارزها باشد.

پیشگیری وضعی از انواع روش‌های پیشگیری غیر کیفری (جرم‌شناسی پیشگیرانه) است که می‌تواند مبتنی بر روش‌های موقعیت مدار باشد. از جمله اقدامات پیشگیرانه وضعی نظارت است. نظارت همواره به عنوان عاملی برای پیشگیری از جرم مد نظر بوده و توانسته تا حدودی در این خصوص کارا باشد. یکی از موارد نظارت، نصب و راه‌اندازی سیستم‌های KYC می‌باشد. (KYC) بر سیستم‌های انطباق و نظارت و گزارش‌دهی بانک‌ها و سایر ارائه‌دهندگان خدمات مالی متکی است. محدودیت دسترسی به ارزهای دیجیتال شیوه دیگری برای پیشگیری وضعی از ارتکاب جرایم مرتبط با رمز ارزهاست. نظارت بر صرافی‌های آنلاین نیز اقدام مؤثر دیگری در این خصوص است. در اتحادیه اروپا، در ۳۰ می ۲۰۱۸، دستورالعمل (EU) 2018/843 (EU)، همچنین به عنوان «دستورالعمل پنجم»، در مورد جلوگیری از استفاده از سیستم مالی به منظور پول‌شویی، به تصویب رسید و منتشر شد. در این دستورالعمل برای اقدامات پیشگیرانه از جرایم ناشی از رمز ارزها به موضوع نظارت بر صرافی‌های آنلاین و تعیین دستورالعمل فعالیت آنها اشاره دارد. تدابیر افزایش دشواری ارتکاب جرم مانند استفاده از داده‌های بلاک چین عمومی، طبقه‌بندی بازیگران حقیقی و حقوقی شبکه رمز ارزها و حق حفاظت از داده‌های شخصی عامل دیگری است که می‌تواند در این خصوص مؤثر باشد.



## منابع

- ابوذری، مهنوش. (۱۳۹۵). جرم‌شناسی جرایم سایبری. چاپ اول. بنیاد حقوقی میزان.
- انصاری، باقر؛ عطار، شیماء؛ صالحی، امیرحسین. (۱۴۰۰). حقوق داده‌ها و هوش مصنوعی: مفاهیم و چالش‌ها. چاپ اول. شرکت سهامی انتشار.
- بابایی، محمدعلی. (۱۳۹۰). جهانی شدن جرم: ضرورتی پیش روی مطالعات و تحقیقات جرم‌شناسی آموزه‌های حقوق کیفری، ۸(۱)، ۱۱۵-۱۳۶.
- [https://cld.razavi.ac.ir/article\\_846.html](https://cld.razavi.ac.ir/article_846.html)
- بهره‌مند، حمید؛ محمد کوره‌پز، حسین؛ سلیمی، احسان. (۱۳۹۳). راهبردهای وضعی پیشگیری از جرایم سایبری. آموزه‌های حقوق کیفری، ۱۱(۷)، ۱۷۶-۱۴۷.
- [https://cld.razavi.ac.ir/article\\_770.html](https://cld.razavi.ac.ir/article_770.html)
- جیشانکار، کی. (۱۳۹۴). جرم‌شناسی فضای مجازی: کشف جرایم اینترنتی و رفتار مجرمانه. چاپ اول. بنیاد حقوقی میزان.
- شیدائیان، مهدی؛ اسحاقی، سید جعفر؛ رجایی، زهرا. (۱۳۹۷). پیشگیری وضعی تقنینی از جرم شکنجه. پژوهش حقوق کیفری، ۷(۲۵)، ۸۹-۱۲۳.
- [https://jclr.atu.ac.ir/article\\_9406.html](https://jclr.atu.ac.ir/article_9406.html)
- رایجیان اصلی، مهرداد. (۱۴۰۱). کلیات جرم‌شناسی: محتوا و تحول؛ از دیروز تا امروز. چاپ اول. انتشارات نگاه معاصر.
- صفاری، علی؛ صابری، راضیه؛ خلیلی پاچی، عارف. (۱۳۹۹). کارکردهای مجرمانه ارزشهای مجازی: تحلیل جرم‌شناختی و راهکارهای پیشگیرانه. دانشنامه حقوق اقتصادی، ۲۷(۱۸)، ۲۵۰-۲۲۳.
- [https://lowecon.um.ac.ir/article\\_39480.html](https://lowecon.um.ac.ir/article_39480.html)
- صفاری، علی. (۱۳۸۰). مبانی نظری پیشگیری از وقوع جرم، مجله تحقیقات حقوقی، ۴(۳۴ و ۳۳)، ۳۲۱-۲۶۷.
- [https://lawresearchmagazine.sbu.ac.ir/article\\_56568.html](https://lawresearchmagazine.sbu.ac.ir/article_56568.html)
- عبدالهی، سامان. (۱۴۰۱). از علت شناسی قربانیان جرایم جنسی تا کارآمدی پلیس تخصصی. کارآگاه، ۱۶(۵۹)، ۱۴۷-۱۲۳.
- [http://det.jrl.police.ir/article\\_98630.html](http://det.jrl.police.ir/article_98630.html)
- عبدالهی قهفرخی، شهیار؛ پاکزاد، بتول؛ عالی‌پور، حسن؛ الهی منش، محمدرضا. (۱۴۰۰). پیشگیری از پول‌شویی الکترونیکی: رویکرد دفاعی و رویکرد هجومی، پژوهش‌های حقوق جزا و جرم‌شناسی، ۹(۱۸)، ۴۰۶-۳۸۵.
- [https://jclac.sdil.ac.ir/article\\_141514.html](https://jclac.sdil.ac.ir/article_141514.html)
- فرهادی آلاشتی، زهرا. (۱۳۹۵). پیشگیری وضعی از جرایم سایبری: راهکارها و چالش‌ها. چاپ اول. بنیاد حقوقی میزان.
- قاسمی، ناصر؛ بیاتی، مجید. (۱۴۰۰). ارزشهای دیجیتال از نگاه سیاست جنایی تقنینی ایران و فقه امامیه، چاپ اول. انتشارات دانشگاه علوم قضائی و خدمات اداری.
- کرامتی معز، هادی. (۱۳۹۹). نبردهای جرم‌شناسی کودکان در شبکه‌های مجازی. چاپ اول. نشر دادگستر.

- کرامتی معز، هادی؛ میرخلیلی، سید محمود. (۱۳۹۹). پیشگیری رشدمدار از بزه دیدگی کودکان در شبکه‌های اجتماعی مجازی (مطالعه موردی معلمان منطقه پنج شهر تهران. *مطالعات پیشگیری از جرم*، ۱۵(۵۶)، ۲۱-۱.

[http://cps.jrl.police.ir/article\\_95006.html](http://cps.jrl.police.ir/article_95006.html)

- منصورآبادی، عباس؛ میرخلیلی، سید محمود؛ کرامتی معز، هادی. (۱۴۰۰). پیشگیری از بزه دیدگی کودکان در شبکه‌های اجتماعی مجازی با تأکید بر نقش نظارتی شورای عالی فضای مجازی و پلیس فتا. *مطالعات بین‌المللی پلیس*، ۱۲(۴۶)، ۵۲-۲۹.

[http://interpol.jrl.police.ir/article\\_95912.html](http://interpol.jrl.police.ir/article_95912.html)

- منصورآبادی، عباس؛ کرامتی معز، هادی؛ بهاری غازی، مجید. (۱۴۰۱). پول شویی در بستر رمز ارزها (خصوصیات ریسک‌پذیری رمز ارزها و ارائه راهکارهای مقابله‌ای). *کارآگاه*، ۱۶(۶۰)، ۲۲-۱.

[http://det.jrl.police.ir/article\\_98637.html](http://det.jrl.police.ir/article_98637.html)

- میرخلیلی، سید محمود؛ چاووشی، محمدصادق؛ کرامتی معز، هادی. (۱۳۹۷). پیشگیری از پدیده ریزومیک شدن جرایم در فضاهای شهری ایرانی اسلامی با تأکید بر سرمایه اجتماعی. *مطالعات شهر ایرانی اسلامی*، ۸(۳۱)، ۲۴-۱۵.

<https://www.magiran.com/paper/citation?ids=2200183>

- نجفی ابرندآبادی، علی حسین. (۱۳۹۶). جنایات بین‌المللی و جرم‌شناسی، دیپاچه در: جرم‌شناسی فراملی (به‌سوی جرم‌شناسی جنایات بین‌المللی). به کوشش حمیدرضا نیکوکار. چاپ اول. بنیاد حقوقی میزان.

- Barroilhet, A. (2019). *Doctrina Cryptocurrencies, economy and law*, REVISTA CHILENA DE DERECHO Y TECNOLOGÍA, Vol 8, Num 1.

<https://rchdt.uchile.cl/index.php/RCHDT/article/view/51584/56575>

- Brito, J., Shadab, H., & Castillo, A. (2014). Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling. *Colum. Sci. & Tech. L. Rev.*, 16, 144.

<http://dx.doi.org/10.2139/ssrn.2423461>

- Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of economic Perspectives*, 29(2), 213-38.

<https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213>

- Bollen, R. (2016). *The Legal Status of Online Currencies – Are Bitcoins the Future?*. Melbourne Business School, 2016 Financial Institutions, Regulation & Corporate Governance (FIRCG) Conference.

<https://ssrn.com/abstract=2736021> or <http://dx.doi.org/10.2139/ssrn.2736021>

- Burge, M. E. (2015). Apple pay, bitcoin, and consumers: The ABCs of future public payments law. *Hastings LJ*, 67, 1493.

[https://repository.uchastings.edu/hastings\\_law\\_journal/vol67/iss6/1](https://repository.uchastings.edu/hastings_law_journal/vol67/iss6/1)

- Reyes, C. L. (2016). Moving beyond Bitcoin to an endogenous theory of decentralized ledger technology regulation: An initial proposal. *Vill. L. Rev.*, 61, 191. Available at: <https://digitalcommons.law.villanova.edu/vlr/vol61/iss1/5>

- Christopher, C. M. (2014). Whack-A-Mole: Why prosecuting digital currency exchanges won't stop online money laundering. *Lewis & Clark L. Rev.*, 18, 1

[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2312787](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312787)

- DeCunha, N. (2010). Virtual property, real concerns. *Akron Intell. Prop. J.*, 4, 35.

<https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss1/2>

- Erlank, W. (2015). Introduction to virtual property: lex virtualis ipsa loquitur. *PELJ*. (18)7:2559-2525.

<https://perjournal.co.za/article/view/1142>



- Jaishankar, K., & Ronel, N. (Eds.). (2013). *Global criminology: Crime and victimization in a globalized era*. CRC Press.
- Jaishankar, K. (2008). *Space Transition Theory of Cyber Crimes*, in: Schmallager, F., & Pittaro, M. (eds.), *Crimes of the Internet*, Upper Saddle River, NJ: Prentice Hall, pp. 283-301.  
<http://www.cybercrimejournal.com/Editoriaijccjuly.pdf>
- Farrugia, S., Ellul, Joshua., & Azzopardi, G. (2020). *Detection of illicit accounts over the Ethereum blockchain*. Expert systems with applications, 150,  
<https://doi.org/10.1016/j.eswa.2020.113318>
- Guadamuz, A., & Marsden, C. (2015). Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. *First Monday*, 20(12-7).  
<https://ssrn.com/abstract=2704852>
- Guadamuz, A., & Marsden, C. (2015). *Blockchains and Bitcoin: Regulatory responses to cryptocurrencies*. *First Monday*, 20(12-7).  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2704852](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2704852)
- Hacker, P., & Thomale, C. (2018). Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. *European Company and Financial Law Review*, 15(4), 645-696.  
<https://doi.org/10.1515/ecfr-2018-0021>
- Moeser, M, Boehme, R, Breuker, D. (2014). *Towards risk scoring of Bitcoin transactions*. In: Boehme R, Brenner M, Moore T et al. (eds), *Financial Cryptography and Data Security*. Heidelberg: Springer.  
[https://informationsecurity.uibk.ac.at/pdfs/MBB2014\\_BitcoinRiskScoring.pdf](https://informationsecurity.uibk.ac.at/pdfs/MBB2014_BitcoinRiskScoring.pdf)
- Navarro Cardoso, F. C. (2019). Criptomonedas (en especial, bitcoin) y blanqueo de dinero. *Revista electrónica de ciencia penal y criminología*.  
<http://criminnet.ugr.es/recpc/21/recpc21-14.pdf>
- Ponsford, M. P. (2015). A comparative analysis of bitcoin and other decentralised virtual currencies: legal regulation in the People's Republic of China, Canada, and the United States. *HKJ Legal Stud.*, 9,  
<https://ssrn.com/abstract=2554186> or <http://dx.doi.org/10.2139/ssrn.2554186>
- Redo. S. (2012). *Blue Criminology, The Power of United Nations Ideas to Counter Crime Globally: A Monographic Study*, European Institute for Crime Prevention and Control, Affiliated with the United Nations.
- Trautman, L. and Harrell, A. (2017). *Bitcoin versus Regulated Payment Systems: What Gives?*, 38 *Cardozo Law Review* 1041.  
<https://ssrn.com/abstract=2730983> or <http://dx.doi.org/10.2139/ssrn.2730983>
- Tsukerman, M. (2015). The block is hot: A survey of the state of Bitcoin regulation and suggestions for the future. *Berkeley Technology Law Journal*, 30(4), 1127-1170.  
<https://www.jstor.org/stable/26377750>