

مطالعه تطبیقی چالش های نظام عدالت کیفری ایران در دادرسی جرایم مرتبط با ارزش های مجازی

سید مهدی نبوی^۱، دکتر محمود صابری^۲*

۱. دانشجوی کارشناسی ارشد حقوق جزا و جرم شناسی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران

۲. استادیار حقوق جزا و جرم شناسی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران

پذیرش: ۱۳۹۹/۰۱/۲۸

دریافت: ۱۳۹۸/۰۹/۱۰

چکیده

ارزش های مجازی پدیده نوینی است که بر بستر اینترنت و با استفاده از فناوری های نوین استخراج و منتقل می شوند. غیرمتمرکز بودن، فرامرزی بودن، گمنام بودن کاربران، رمزنگاری و برگشت ناپذیر بودن تراکنش ها، ویژگی هایی است که بهره گیری از ارزش های مجازی در فعالیت های مجرمانه را مورد توجه بزهکاران قرار می دهد. پژوهش حاضر با استفاده از روش توصیفی تحلیلی و با استفاده از منابع کتابخانه ای به صورت تطبیقی با کشورهای ژاپن و آمریکا، ضمن تشریح روش کارکرد ارزش های مجازی و گونه شناسی آنها، به این سوال اصلی پرداخته است که فرآیند رسیدگی به پرونده های فعالیت های مجرمانه مرتبط با ارزش های مجازی با چه چالش هایی رو به رو است. یافته های تحقیق نشان می دهد ویژگی های ارزش های مجازی به همراه ابهام در وضعیت قانونی و قلمرو فعالیت های مجرمانه، چالش هایی برای نظام عدالت کیفری در حوزه دادرسی جرایم، بوجود آورده است.

تعریف دقیق قانونی از ارزهای مجازی و تعیین ماهیت حقوقی آن‌ها، اصلاح قوانین مرتبط با ارزهای مجازی و تصویب قوانین جدید با در نظر گرفتن ویژگی‌های منحصر به فرد ارزهای مجازی در مواردی که قانون وجود ندارد، تعیین عناوین مجرمانه مرتبط با ارزهای مجازی در جایی که امکان تطبیق با قوانین فعلی وجود ندارد، همکاری با کشورهای خارجی و نهادهای بین‌المللی در زمینه تبادل اطلاعات و ارتباطات مرتبط با ارزهای مجازی، انعقاد تفاهم‌نامه میان بخش خصوصی و دولتی، استفاده و بکارگیری کارشناسان ارزهای مجازی و آموزش دادرسان و ضابطان دادگستری، از جمله راهکارهای پیشنهادی در زمینه رفع چالش‌های دادرسی جرایم مرتبط با ارزهای مجازی است.

واژگان کلیدی: ارز مجازی، پول الکترونیکی، زنجیره بلوک، پولشویی، تأمین مالی تروریسم، دادرسی جرایم سایبری.

۱. مقدمه

در سال ۲۰۰۸ شخص یا گروهی با نام مستعار ساتوشی ناکاماتو با انتشار متنی در فضای مجازی نحوه کارکرد ارز مجازی بیت‌کوین را تشریح کرد (Nakamoto 2008).

اولین بیت‌کوین در سال ۲۰۰۹ بر پایه فناوری دفتر کل توزیع شده و زنجیره بلوک

تولید شد. بیت‌کوین نمونه ابتدایی ارز مجازی غیرمتمرکز است که پس از بحران مالی

سال ۲۰۰۸ مورد اقبال گسترده قرار گرفت (Kethineni, Cao & Dodge, 2017, p.142). غیرمتمرکز بودن، فرامرزی بودن، گمنام بودن کاربران، رمزنگاری و برگشت‌ناپذیر بودن تراکنش‌ها از ویژگی‌های ارزهای مجازی است که موجب افزایش حریم خصوصی کاربران، امنیت شبکه، کاهش هزینه تراکنش‌ها و افزایش سرعت انتقال پول شده است.



ویژگی‌های فوق به همراه خلاءها و عدم اعمال الزامات و نظارت‌های قانونی، عدم شناخت و درک صحیح قانونگذاران، عدم تخصص و آشنایی ضابطان قضایی و قضات از ماهیت و چگونگی کارکرد ارزش‌های مجازی (J Kim 2016, p.75)، استفاده از دیگر فناوری‌های نوین از قبیل اینترنت تاریک (تاریک (Martin 2014:2) و نرم افزارهای افزایش دهنده گمنامی کاربران^۱ در فضای مجازی (Kethineni, Cao & Dodge 2017, p.145)، موجب می‌شود تا بهره‌گیری از ارزش‌های مجازی در فعالیت‌های مجرمانه مورد توجه بزهکاران واقع شود و امکان شناسایی، تعقیب و رسیدگی به جرایم مرتبط با ارزش‌های مجازی بسیار سخت و پیچیده شود (Romeo 2016, p.76).

در حال حاضر وضعیت قانونی ارزش‌های مجازی مبهم است. استناد به قوانین موجود در مواجهه با ارزش‌های مجازی با توجه به ویژگی‌های منحصر به فردی که دارند، ابهامات و چالش‌هایی را در مراحل کشف، تعقیب، توقیف و مصادره و دادرسی ارزش‌های مجازی به وجود می‌آورد. در ادامه ابتدا ارزش‌های مجازی و جرایم مرتبط با آنها توصیف، سپس چالش‌های نظام حقوقی ایران در دادرسی جرایم مرتبط با ارزش‌های مجازی و راهکارهای پیشنهادی ارائه خواهد شد.

۲. مفاهیم

تعریف مفاهیم جهت جلوگیری از ابهامات احتمالی در مورد ارزش‌های مجازی^۲ بسیار ضروری است. به دلیل آن‌که در این زمینه، از مفاهیم مرتبط و مشابه گوناگونی مانند پول الکترونیک^۳، پول دیجیتال^۴، پول مجازی، رمزارز^۵، رمزینه ارز، پول رمزنگاری

۱. برای مثال: Tumbler software و PGP (pretty good privacy) software

۲. Virtual Currency

۳. Electronic Money / e-money

۴. Digital Currency

۵. cryptocurrency

شده و... استفاده می‌شود. در این بخش تبیین مفاهیم مرتبط با ارزشهای مجازی و تمیز میان آنها، جهت بیان مقصود از ارز مجازی، صورت می‌گیرد.

۱-۲. مفهوم پول الکترونیک

پول‌های الکترونیک یا دیجیتال، مکانیسمی جدید در پرداخت اسکناس‌های متداول بانکی هستند (نواب پور، یوسفی، طالبی ۱۳۹۷:۲۱۸). در این حالت، هیچ وسیله فیزیکی‌ای در میان نیست و مبادله، تنها با انتقال و پردازش داده‌های رمزنگاری شده انجام می‌پذیرد؛ بدین صورت که رایانه‌های مرکزی بانک‌ها، حساب‌های افراد را طلبکار و بستانکار می‌کنند (سلطانی، اسدی ۱۳۹۴:۸۳-۸۴).

پول الکترونیکی که پول دیجیتال نیز نامیده می‌شود، ساز و کار انتقال دیجیتالی برای پول واقعی است. پول الکترونیکی ارزش پول رایج را به صورت دیجیتال منتقل می‌کند؛ به عبارت دیگر پول الکترونیکی شکل دیجیتال پول است که تحت نظارت نهاد مرکزی خلق می‌شود و مشمول مقررات پولی و بانکی است.

۲-۲. مفهوم ارزشهای مجازی

ارز مجازی برخلاف پول الکترونیک، بازنمایی دیجیتال پول اعتباری^۱ نیست و خلق و انتشار آن دارای ساز و کاری متفاوت از پول الکترونیک و به صورت منحصر به فرد است. سازمان خدمات درآمد داخلی ایالات متحده آمریکا ارزشهای مجازی را به این صورت تعریف می‌کند: «بازنمایی دیجیتالی ارزش که در جایگاه واسط مبادله، سنجش ارزش یا ذخیره ارزش کار می‌کند» (مرکز پژوهش‌ها ۱۳۹۷، ص ۳). طبق تعریف بانک مرکزی اتحادیه اروپا، ارزشهای مجازی عبارت‌اند از: بازنمایی دیجیتالی

۱ . digital representation of fiat currency



ارزش که توسط یک بانک مرکزی یا نهاد عمومی منتشر نشده است و ضرورتاً مبتنی بر یک پول اعتباری نیست اما بوسیله اشخاص حقیقی یا حقوقی به عنوان وسیله مبادله مورد استفاده قرار می‌گیرند و می‌توانند به صورت الکترونیکی منتقل، ذخیره و یا مبادله شوند (EBA, 2015, p4).

۲-۳. دسته بندی ارزهای مجازی

به طور کلی ارزهای مجازی را می‌توان با توجه به وجود نهاد مرکزی و قابلیت تبدیل آن‌ها به ارزهای دیگر و ترکیب این ویژگی‌ها به سه دسته اصلی ارز مجازی متمرکز قابل تبدیل، ارز مجازی غیر متمرکز قابل تبدیل و ارز مجازی غیر متمرکز قابل تبدیل تقسیم کرد. هر چند دسته بندی‌های دیگری نیز ممکن است صورت گرفته باشد^۱، اما دسته بندی موجود با توجه به ویژگی‌های مذکور، انتخاب شده است.

ارز مجازی متمرکز^۲ قابل تبدیل^۳ ارزی است که دارای یک نهاد مرکزی مدیریت است، که کنترل سیستم را به عهده دارد، و به دیگر ارزهای مجازی و یا پول‌های واقعی مانند دلار، یورو و... و بالعکس قابل تبدیل است. نهاد مرکزی ارز مجازی را منتشر می‌کند و قوانین مربوط به چگونگی استفاده از آن را وضع می‌نماید. نهاد مرکزی پشتیبانی از دفتر کل مرکزی را به عهده دارد. مانند: E-gold; Liberty Reserve; Perfect Money and Web Money.

ارز مجازی غیر متمرکز قابل تبدیل^۴ ارزی است که توسط یک نهاد مرکزی مانند یک وب سایت و یا بازی رایانه‌ای تولید شده است و فقط در همان محیط قابل

۱ . see: European Central Bank, Virtual Currency Schemes, October 2012.

۲ . Centralised Virtual Currency

۳ . Convertible

۴ . Non-convertible

استفاده‌اند و امکان تبدیل آنها به پول اعتباری وجود ندارد مانند: Q Coins and Project Entropia Dollars. تمام ارزهای مجازی غیرقابل تبدیل متمرکز هستند. ارز مجازی غیر متمرکز^۱ قابل تبدیل، فاقد یک نهاد مرکزی همانند دولت و یا بانک مرکزی است. ارزش این ارز بر پایه اعتماد میان کاربران است و هیچ پشتوانه‌ای اعم از فلزات گران بها مانند طلا و یا کالا ندارد و مانند پول واقعی عمل می‌کند و به وسیله آنها می‌توان کالا و خدمات خریداری کرد. منظور از قابل تبدیل بودن امکان تبدیل این نوع ارز مجازی به پول‌های واقعی مانند دلار، یورو و... و بالعکس است (UNODC, 2014, p.12). ارز مجازی غیرمتمرکز قابل تبدیل با استفاده از فرمول‌های ریاضی، الگوریتم‌های رمزنگاری و یک معماری هم‌تا به هم‌تا عمل می‌کند که به آن رمزارز یا پول رمزنگاری شده نیز می‌گویند. مانند: Bitcoin; LiteCoin; and Ripple.

۳. روش کار ارزهای مجازی

ارزهای مجازی بر خلاف پول الکترونیکی فاقد نهاد مرکزی هستند (Kim, 2016, p.77). این بدان معنا است که در این سامانه هیچ شخصی نسبت به صحت عملکرد و تضمین کارکرد مؤثر آن مسئولیتی ندارد. از طرف دیگر با توجه به ماهیت ارز مجازی غیرملموس و یک سری شماره است، امکان استفاده مجدد از آنها وجود دارد که به آن پرداخت دوباره^۲ می‌گویند. با توجه به این‌که کاربران شبکه به صورت گمنام و هم‌تا به هم‌تا اقدام به پرداخت و یا دریافت ارز مجازی می‌نمایند (Hoyer, 2017, p.86)، جهت ایجاد اعتماد میان کاربران، تضمین صحت عملکرد سامانه و تراکنش‌ها و جلوگیری از پرداخت دوباره، از فناوری نوین زنجیره بلوک استفاده می‌شود.

۱ . Non-centralised Virtual Currency

۲ . Duple-Spending



زنجیره بلوک فناوری است که بیت‌کوین^۱ و برخی دیگر از ارزهای مجازی بر پایه آن کار می‌کنند. این فناوری گونه‌ای از دفترکل توزیع شده است. زنجیره بلوک به سه دسته عمومی، خصوصی و نیمه خصوصی تقسیم می‌شود (درشر ۱۳۹۷: ۲۶۴) که در این نوشتار مقصود از آن، زنجیره بلوک عمومی است.

۴. فعالیت‌های مجرمانه مرتبط با ارزهای مجازی

ارزهای مجازی می‌توانند به همراه دیگر فناوری‌ها در فعالیت‌های مجرمانه مورد استفاده قرار گیرند و یا می‌تواند به عنوان نوعی دارایی، موضوع جرم واقع شوند. در ادامه مهمترین جرایمی که امکان وقوع آنها در این حوزه وجود دارد به اختصار ذکر می‌شود.

۴-۱. سرقت ارز مجازی

ارز مجازی می‌تواند مانند پول نقد، سرقت و یا مفقود شود. سختی نگهداری ارز مجازی به صورت برخط آن‌ها را در معرض سرقت قرار می‌دهد. سارقان با استفاده از بدافزار و یا با هک کردن می‌توانند ارزهای مجازی را از رایانه و یا حساب شخصی افراد سرقت کنند. سرقت ارزهای مجازی تنها از رایانه‌های شخصی و کیف پول مجازی صورت نمی‌گیرد، بلکه بزهکاران می‌توانند کسب و کارهای مرتبط مانند صرافی‌های ارز مجازی را نیز مورد هدف قرار دهند. در این زمینه می‌توان به سرقت از صرافی‌های Mt.Gox^۲ و Flexcoin^۳ اشاره کرد.

۱ . Bitcoin.

2 . see: The Troubling Holes in MtGox's Account of How It Lost \$600 Million in Bitcoins, MIT TECH. REV. <http://www.technologyreview.com/view/526161/the-troubling-holes-in-mtgoxs-account-of-how-it-lost-600-million-in-bitcoins/>; Takashi Mochizuki & Eleanor Warnock, Mt. Gox Finds 200,000 Missing Bitcoins, WALL ST. J., Mar. 21, 2014, at C2; Dylan Love, \$500 Million Worth of Bitcoin Has Been Stolen Since 2010, BUS. INSIDER, <http://www.businessinsider.com/how-many-bitcoins-have-been-stolen-2014-3>; L. Kate, 'The Rise and Fall of Mt Gox, Everything You Need to Know' (25 March 2014) <https://coinreport.net/editorial-rise-fall-mtgox/>.

3 . see: Warner T. Huston, A Second Bitcoin Exchange Goes Bankrupt, BREITBART.COM (Mar. 4, 2014), <http://www.breitbart.com/Big-Government/2014/03/04/A-Second-Bitcoin-Exchange-Goes-Bankrupt>; FlexCoin Is Shutting Down, FLEXCOIN.COM (Mar. 3, 2014) <http://www.flexcoin.com/>.

۲-۴. کلاهبرداری

ارزهای مجازی دارای خطر بالای کلاهبرداری هستند. افزایش قابل توجه قیمت برخی از ارزهای مجازی، می‌تواند سرمایه‌گذاران را به راحتی اغوا کند و اشخاص بزهکار با وعده خرید ارز مجازی، دارایی افراد را ببرند. روش دیگر خرید با ارزهای مجازی است که فروشنده پس از دریافت ارز، از فرستادن کالا و یا ارائه خدمات خودداری می‌کند. نمونه دیگر عرضه اولیه سکه^۱ است که اشخاص با ادعای خلق ارز مجازی جدید، اقدام به جمع آوری پول می‌کنند و سپس متواری می‌شوند.

۳-۴. پولشویی^۲

تراکنش‌های سریع از طریق ارزهای مجازی، موجب شده است تا برداشت پول و یا تبدیل آن به سایر وجوه، بسیار سریع‌تر از راه‌های سنتی صورت گیرد. افزایش سرعت تراکنش‌ها، پیچیدگی نظارت بر آن‌ها را افزایش داده و ترکیب استفاده از ارزهای مجازی با سایر روش‌های نوین و سنتی پولشویی، کشف و تعقیب این جرم را بسیار دشوار کرده است. مجرمان از این طریق می‌توانند منافع حاصل از جرم را به مناطقی که قوانین و نظارت کم‌تری در مورد پولشویی دارند منتقل کنند و در آن کشورها اقدام به تبدیل ارز مجازی به پول نقد و... نمایند. استفاده از ارزهای مجازی در پولشویی، نگرانی اصلی بسیاری از کشورها است ((Verduyn, 2018). در این

۱. ICO

۲. مطابق ماده ۲ قانون مبارزه با پولشویی، پولشویی عبارت است از: «الف- تحصیل، تملک، نگهداری یا استفاده از عواید حاصل از ارتکاب جرایم با علم به منشاء مجرمانه آن. ب- تبدیل، مبادله یا انتقال عوایدی به منظور پنهان یا کتمان کردن منشاء مجرمانه آن با علم به اینکه به طور مستقیم یا غیر مستقیم از ارتکاب جرم به دست آمده یا کمک به مرتکب جرم منشاء به نحوب که وی مشمول آثار و تبعات قانونی ارتکاب آن جرم نشود. پ- پنهان یا کتمان کردن منشاء، منبع، محل، نقل و انتقال، جابه‌جایی یا مالکیت عوایدی که به طور مستقیم یا غیرمستقیم در نتیجه جرم تحصیل شده باشد.»

خصوص می‌توان به سایت Liberty Reserve اشاره کرد که به عنوان بزرگ‌ترین پولشویی تاریخ مشهور شده است.^۱

۴-۴. تأمین مالی تروریسم^۲

تأمین مالی تروریسم یکی از نگرانی‌هایی است که بسیاری از دولت‌ها و سازمان‌های بین‌المللی را به خود مشغول کرده است. فعالیت‌های گروه‌های تروریستی صرفاً شامل حمله به یک نقطه خاص و یا عملیات نظامی نیست بلکه گسترش فعالیت‌های سازمانی گروه‌های تروریستی مانند تبلیغ، تهیه اقلام مورد نیاز و... نیازمند پشتیبانی مالی است. از این رو، امروزه گروه‌های تروریستی ابزارها و روش‌های نوین را، جهت تأمین منابع مالی خود، به کار می‌برند. شبکه اینترنت یکی از ابزارهای نوین در اختیار گروه‌های تروریستی است. فرامرزی بودن و گمنام بودن ارزهای مجازی درکنار فقدان نظارت بر تراکنش‌های آنها، می‌تواند به عنوان روشی جهت تأمین مالی گروه‌های تروریستی مورد استفاده قرار گیرد (FATF 2008).

۴-۵. تسهیل سایر جرایم

گمنامی و نامتمرکز بودن و نبود نظارت نهاد مرکزی و الزامات قانونی موجب شده است تا تراکنش‌های صورت گرفته از شبکه بیت‌کوین به راحتی قابل شناسایی نباشد.

۱. see: "Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A \$6 Billion Money Laundering Scheme", US Department of Justice, May 2013. (Source: <http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php?print=1>).

۲. مطابق ماده ۱ قانون مبارزه با تأمین مالی تروریسم: «تهیه یا جمع‌آوری وجوه یا اموال به هر طریق چه دارای منشأ قانونی باشد یا نباشد و یا مصرف تمام یا بخشی از منابع مالی حاصله از قبیل قاچاق ارز، جلب کمک‌های مالی و پولی، اعانه، انتقال پول، خرید و فروش اوراق مالی و اعتباری، افتتاح مستقیم یا غیرمستقیم حساب یا تأمین اعتبار یا انجام هرگونه فعالیت اقتصادی اشخاص توسط خود یا دیگری برای انجام اعمال زیر یا جهت ارائه به افراد تروریست یا سازمان‌های تروریستی، تأمین مالی تروریسم است.»

این ویژگی‌ها اشخاص را به استفاده از ارزش‌های مجازی در فعالیت‌های مجرمانه ترغیب کرده است. به گونه‌ای که برخی از جرایم مرتبط با بیت‌کوین^۱ سخن به میان آورده‌اند (Rev, 2014, p.513).

استفاده از ارزش‌های مجازی در ایالات متحده آمریکا، برای فرار از مالیات‌های دولتی، بوسیله تبدیل درآمد به ارزش مجازی و انتقال آنها به حساب‌های خارجی^۲ (گزارش شده است (Valeriane 2016: 865). بهره‌گیری از ارزش‌های مجازی در فعالیت‌هایی نظیر قاچاق انسان، بهره‌کشی جنسی (Hoyer 2017: 90) به عنوان یکی از نگرانی‌های دولت‌ها و نهادهای بین‌المللی مطرح است. ارزش‌های مجازی به تبهکاران این امکان را می‌دهند تا از طریق سایت‌هایی که در آن‌ها تبلیغات به صورت گمنام و بدون نظارت کافی صورت می‌گیرد، با استفاده از ارزش‌های مجازی فعالیت‌های مجرمانه‌شان را با سرعت و سهولت بیشتری انجام دهند.

ویژگی‌ها و قابلیت‌های ارزش‌های مجازی به خصوص در زمانی که هنوز پلیس و نهادهای مجری قانون آشنایی زیادی با این پدیده ندارند می‌تواند زمینه تسهیل بسیاری از جرایم را فراهم نماید. ترکیب چند فناوری گمنام‌کننده در بستر اینترنت و استفاده از اینترنت تاریک و بیت‌کوین، فروشگاه‌های اینترنتی را بوجود آورده است که در آن‌ها اقلام ممنوعه و غیرقانونی از جمله مواد مخدر و روان‌گردان، سلاح، انواع نرم‌افزارهای هک و... به راحتی خرید و فروش می‌شود.^۳

یکی دیگر از جرایمی که در آن از ارزش‌های مجازی استفاده می‌شود، باج‌افزارهایی است که در فضای مجازی، پس از آن‌که دسترسی کاربران و اشخاص را به اطلاعات و سیستم‌هایشان با محدودیت و مانع مواجه می‌کنند، از آن‌ها مبالغی را مطالبه

۱ . bitcoin-related crime

۲ . Offshore account

۳ . See: Dune Lawrence, Silk Road 2.0 Shut Down by FBI, Just Like Its Black Market Predecessor, Bloornburg Business Week, Nov.

می‌کنند. در برخی از این باج افزارها از اشخاص خواسته می‌شود تا ارز مجازی بپردازند.

در حال حاضر در ایران استفاده غیر مجاز از برق جهت استخراج ارزهای مجازی مشکلاتی را ایجاد کرده است. با توجه به مصرف زیاد برق، برخی از مزارع استخراج بیت کوین توسط پلیس توقیف شده‌اند. در حال حاضر استفاده غیر مجاز از برق که در بسیاری از موارد انشعاب کارگاه‌ها و یا مکان‌های صنعتی و تولیدی است، مطابق با قانون مجازات استفاده کنندگان غیرمجاز از آب، برق، تلفن، فضا و گاز جرم انگاری شده است و دارای ضمانت اجرای کیفری می‌باشد.

۵. چالش‌های ناظر بر دادرسی جرایم مرتبط با ارزهای مجازی

ارزهای مجازی در حال حاضر فاقد یک تعریف قانونی یکسان هستند (Hoyer 2017, p.85) و وضعیت حقوقی آنها در هاله‌ای از ابهام قرار دارد. هر چند تعاریف مختلفی از ارز مجازی صورت گرفته است، اما تعریفی که مشخص کننده ماهیت ارز مجازی باشد و شکل قانونی به خود گرفته باشد می‌تواند وضعیت حقوقی ارزهای مجازی را برای قضات و نهادهای قانونی تعیین کند. فقدان تعریف دقیق قانونی توسط قانون‌گذار، امکان تفاسیر و تعاریف متعدد را فراهم خواهد کرد. در نتیجه در مراجع قضایی و مراکز اجرایی، با آرای متشکست و تصمیمات متناقض مواجه خواهیم شد. سازمان‌ها و نهادهای پولی و بانکی با توجه به اولویت‌ها و دیدگاه‌های خود، اقدام به تعریف ارز مجازی می‌کنند و بر اساس همان تعریف، مقررات و دستورالعمل‌هایی صادر خواهند کرد. در نظر گرفتن ارز مجازی به عنوان پول یا نوعی از روش‌های نوین پرداخت و یا دارایی، هر کدام دارای آثار متفاوتی است. به طور مثال، تصدیق به عملیات بانکی بدون مجوز، در برخی کشورها از جمله ایران دارای ضمانت اجرای

کیفری است.^۱ آیا در حال حاضر می‌توان مدیریت و تصدی به فعالیت‌های مرتبط با ارمجازی را مصداق تصدی به عملیات بانکی در نظر گرفت؟ و یا در صورت انجام فعالیت مجرمانه از طریق ارزهای مجازی چه کسی را می‌توان مسئول شناخت؟ در حال حاضر نظام‌های پولی و بانکی دارای قوانین و مقررات بسیار گسترده، جهت کنترل فعالیت‌های مالی هستند. اعمال این قوانین در خصوص ارزهای مجازی مستلزم این است که قانون‌گذار ارمجازی را به عنوان پول رایج، مورد پذیرش قرار دهد و یا به اعمال قوانین خاص، در مورد ارزهای مجازی تصریح کند.

در همین رابطه می‌توان به یک پرونده کلاهبرداری که در سال ۲۰۱۳ در ایالت تگزاس مطرح و مورد رسیدگی قرار گرفته است اشاره کرد. در این پرونده متهم در دفاع از خود استدلال می‌کند که بیت کوین‌ها پول نیستند و بنابر این هرگونه تقاضای سرمایه‌گذاری در رابطه با آن‌ها و قبول این درخواست‌ها توسط متهم، نمی‌تواند شامل قوانین مرتبط باشد. اما در نهایت دادگاه بیت‌کوین را به عنوان پول و یا شکلی از پول مورد پذیرش قرار داد و متهم را محکوم کرد.^۲

۱. ماده یک قانون تنظیم بازار غیر متشکل پولی: «اشتغال به عملیات بانکی توسط اشخاص حقیقی و یا حقوقی تحت هر عنوان و تاسیس و ثبت هرگونه تشکل برای انجام عملیات بانکی بدون دریافت مجوز از بانک مرکزی جمهوری اسلامی ایران ممنوع است. عملیات بانکی در این قانون به امر واسطه‌گری بین عرضه‌کنندگان و متقاضیان وجوه و اعتبار به صورت دریافت انواع وجوه، سپرده، ودیعه و موارد مشابه تحت هر عنوان و اعطاء وام، اعتبار و سایر تسهیلات و صدور کارتهای الکترونیکی پرداخت و کارت‌های اعتباری اطلاق می‌شود. تبصره ۱- بانک‌ها و صندوق‌هایی که قبلاً به موجب قوانین خاص تاسیس شده‌اند بر اساس مفاد همان قوانین ادامه فعالیت خواهند داد. تبصره ۲- اشخاص حقیقی یا حقوقی دیگری که بدون دریافت مجوز از بانک مرکزی جمهوری اسلامی ایران به عملیات بانکی مبادرت دارند موظفند ظرف یک ماه از تاریخ لازم‌الاجرا شدن این قانون برای اخذ مجوز به بانک مرکزی جمهوری اسلامی ایران مراجعه و مدارک مورد نیاز را ارائه نمایند. در غیر این صورت بنا به درخواست بانک مرکزی جمهوری اسلامی ایران ادامه فعالیت این قبیل اشخاص توسط نیروی انتظامی جمهوری اسلامی ایران متوقف خواهد شد.»

۲. see: SEC v. Shavers, No. 4:13-cv-00416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 6, 2013) and Complaint at 1-2, SEC v. Shavers, No. 4:13-cv-00416 (E.D. Tex. July 23, 2013).



۵-۱. ابهام در ماهیت حقوقی ارزشمجازی

در قوانین مرتبط با نظام پولی و بانکی، ارز و پول به صورت مشخصی تعریف شده است. مطابق بند پ ماده ۱ قانون مبارزه با قاچاق کالا و ارز و بند الف ماده ۴۲ و ماده ۲ قانون پولی و بانکی کشور، ارز، پول رایج کشورهای خارجی، اعم از اسکناس، مسکوکات، حوالجات ارزی و سایر اسناد مکتوب یا الکترونیکی است که در مبادلات مالی کاربرد دارد و خرید و فروش ارز و هرگونه عملیات بانکی که موجب انتقال ارز یا تعهد ارزی گردد یا ورود یا خروج ارز یا پول رایج کشور بدون رعایت مقررات بانک مرکزی ج.ا.ایران ممنوع است و قاچاق محسوب می‌شود. همچنین مطابق ماده ۵ آئین نامه مستند سازی جریان وجوه در کشور مصوب ۱۳۸۶/۱۱/۲۲ هیئت وزیران: «خرید و فروش ارز به هر صورت از جمله پرداخت ریال در داخل و دریافت ارز در خارج کشور و بالعکس، تنها در سیستم بانکی و صرافی‌های مجاز با رعایت قوانین و مقررات مجاز است و در غیر این صورت خرید و فروش ارز غیرمجاز محسوب و مشمول قانون نحوه اعمال تعزیرات حکومتی راجع به قاچاق کالا و ارز مصوب سال (۱۳۷۴) مجمع تشخیص مصلحت نظام است.» از طرفی، وجوه نقد مطابق بند ۳۱ ماده یک آیین‌نامه اجرایی ماده ۱۴ قانون مبارزه با پولشویی مصوب ۱۳۹۸/۷/۲۱ «هرگونه مسکوک و اسکناس و انواع چک‌هایی که نقل و انتقال آن‌ها مستند نشده و غیرقابل ردیابی باشد؛ از قبیل چک‌های عادی در وجه حامل و سایر چک‌هایی که دارنده آن غیر از ذی نفع اولیه باشد (مانند چک‌های پشت نویسی شده توسط اشخاص ثالث، انواع چک پول و چک مسافرتی) و کارت‌های پرداخت بی‌نام و موارد مشابه. وجوه نقد شامل وجوه نقد ریالی و ارزی است» عنوان شده است. مطابق ماده ۲۶ دستورالعمل اجرایی تأسیس، فعالیت و نظارت بر صرافی‌ها مصوب ۱۳۸۹/۹/۶ بانک مرکزی ج.ا.ایران «صرافی‌ها مجاز به انجام معامله با کلیه ارزها می‌باشند مگر اینکه بانک مرکزی معامله یک یا چند ارز را ممنوع اعلام کرده باشد.» طبق ماده ۲۸ همان دستورالعمل، «صرافی‌ها در قبال دریافت هرگونه وجه اعم از پول داخلی، ارز و یا

ابزارهای پولی مشابه مجاز و... ملزم به ارائه رسید... می‌باشند». با توجه به تعریف ارز در قوانین مورد اشاره، آیا ارزهای مجازی را می‌توان به عنوان ارز و یا پول و یا ابزارهای پولی مشابه در نظر گرفت؟ بانک مرکزی ج.ا.ی. در پیش‌نویس الزامات و ضوابط فعالیت در حوزه رمز ارزها، رمز ارز را یک نوع دارایی مالی که می‌تواند در شرايطی کارکرد پولی به‌خود بگیرد تعریف کرده است (بانک مرکزی ج.ا.ی. ۱۳۹۷). از سوی دیگر در همان پیش‌نویس استفاده از رمز ارزهای جهان‌روا را به عنوان ابزار پرداخت در داخل کشور، ممنوع اعلام کرده است. در بخش الزامات عمومی کیف پول رمز ارزی، نگهداری رمز ارزها توسط اشخاص حقیقی و حقوقی تابع مقررات عمومی قوانین ارزی آورده شده است. همان‌گونه که مشهود است، تعریف دقیق و روشنی از سوی بانک مرکزی ارائه نشده و علی‌رغم معرفی ارزهای مجازی به عنوان دارایی، رعایت قوانین ارزی در خصوص آنها الزامی دانسته شده است. بانک مرکزی ضمن سلب مسئولیت نظارتی از خود، استفاده از ارزهای مجازی را به عنوان ابزار پرداخت، که مهم‌ترین جنبه کارکردی ارزهای مجازی است، عملاً ممنوع اعلام کرده است. در حال حاضر براساس اعلامیه‌ای مورخ ۱۳۹۶/۱۰/۹ شورای عالی مبارزه با پولشویی^۱، هرگونه به‌کارگیری ارزهای مجازی توسط موسسات مالی و پولی کشور ممنوع است. همچنین مطابق با ماده یک تصویب نامه مورخ ۱۳۹۸/۵/۱۳ هیأت وزیران: «استفاده از رمز ارزها صرفاً با قبول مسئولیت خطرپذیری (خطر) از سوی متعاملین صورت می‌گیرد و مشمول حمایت و ضمانت دولت و نظام بانکی نبوده و استفاده از آن در مبادلات داخل کشور مجاز نیست»^۲.

قانون پولی ژاپن، پول را سکه‌ها و یا پول‌های کاغذی‌ای که توسط بانک ژاپن منتشر می‌شوند و اختیار صدور و ضرب آن‌ها به دولت داده شده است، تعریف کرده است. در حالی که ارزهای مجازی بوسیله اشخاص خصوصی منتشر می‌شوند و به

۱. تارنمای بانک مرکزی ج.ا.ی. ایران؛ پیوند خبر <https://www.cbi.ir/showitem/17722.aspx>

۲. تصویب نامه شماره ۵۸۱۴۴/ت/۵۵۶۳۷ ه ابلاغی مورخ ۱۳۹۸/۵/۱۳.



این علت با تعریف قانون ارزی ژاپن منطبق نیستند. از سوی دیگر امکان اعمال قانون کنترل سهام‌هایی که مشابه با اسکناس هستند، درباره ارزشهای مجازی وجود ندارد. زیرا این قانون تنها بر سهام که دارای یک مفهوم قانونی خاص است و شامل اسناد الکترونیکی یا مغناطیسی نمی‌شود و برای اعمال این قوانین هم زمینه‌های قانونی وجود ندارد (Ishikawa 2017, p.126).

نبود تعریف قانونی از ارزشهای مجازی در عرصه داخلی و بین‌المللی، موجب سوء استفاده مجرمان می‌شود. لذا ضروری است قانون‌گذار نسبت به ارایه تعریفی دقیق از ارزشهای مجازی و تعیین نهاد متولی نظارت بر این ارزشها، اقدام کند.

۲-۵. چالش چگونگی اعمال قوانین و مقررات بر ارزشهای مجازی

در نظام پولی و بانکی، قوانین و الزامات بسیاری ناشی از تعهدات، بخش‌نامه‌ها و دستورالعمل‌های گوناگون بین‌المللی^۱، منطقه‌ای و ملی وجود دارد تا نظام اقتصادی کشور بتواند محیطی امن و سالم برای سرمایه‌گذاران داخلی و خارجی فراهم نماید و صاحبان سرمایه از مصونیت دارایی خویش اطمینان حاصل کنند. بانکها، موسسات مالی و اعتباری و اشخاص حقیقی و حقوقی ارائه‌کننده خدمات پولی، بانکی و یا هرگونه واسطه‌گری وجوه، باید مطابق قوانین و ویژه‌ای اقدام نمایند^۲. تاسیس یک نهاد مالی همراه با اخذ مجوز و بررسی صلاحیت‌های مختلف است^۳ و تصدی به عملیات

۱. نگاه کنید: استانداردهای بین‌المللی مبارزه با پول‌شویی و تامین مالی تروریسم (توصیه‌های چهل گانه گروه ویژه اقدام مالی FATF). ترجمه و تالیف: زارع قاجاری، فردوس؛ قائم مقامی، علی. چاپ اول. تهران، نشر تاش. ۱۳۹۲.

۲ - نگاه کنید: لایحه قانونی اداره امور بانکها مصوب ۱۳۵۷/۷/۳ شورای انقلاب اسلامی و لایحه متمم لایحه قانونی اداره بانکها مصوب ۱۳۵۸/۹/۲۸ همان شورا و قانون تسری امتیازات خاص بانکها به موسسات اعتباری بانکی مجاز مصوب ۱۳۸۱/۱/۲۱ مجلس. ش.ا و قانون تنظیم بازار غیرمتمثل پولی مصوب ۱۳۸۳/۱۰/۲۲ و قانون پولی و بانکی کشور مصوب ۱۳۵۱/۱/۱۸ با آخرین اصلاحات.

۳. نگاه کنید: قانون اجازه تاسیس بانکهای غیردولتی مصوب ۱۳۷۹/۱/۲۱ مجلس شورای اسلامی.

بانکی بدون مجوز، گاه ضمانت اجرای کیفری دارد.^۱ در مورد افتتاح حساب و ارائه خدمات به اشخاص حقیقی و حقوقی، موسسات پولی و بانکی باید ضوابط ویژه‌ای را رعایت کنند که عدم رعایت این مقررات، حسب مورد جریمه‌های مالی، انتظامی و در برخی موارد لغو مجوز موسسه متخلف را به همراه دارد.^۲ دستورالعمل‌های شناسایی مشتری^۳ (KYC) و شناسایی کافی مشتریان^۴ (CDD)، نگهداری سوابق و اطلاعات تراکنش‌ها و گزارش معاملات مشکوک^۵ (STR) از جمله مواردی است که جهت پیشگیری و همچنین سهولت و تسریع در کشف و تعقیب جرایم، باید صورت گیرد. مطابق ماده ۵ قانون مبارزه با پول‌شویی، کلیه صاحبان مشاغل غیرمالی و موسسات غیرانتفاعی و همچنین اشخاص حقیقی و حقوقی مکلفند نسبت به احراز هویت و شناسایی مراجعان، ارائه گزارش معاملات یا عملیات مشکوک بانکی، ثبتی، سرمایه‌گذاری، صرافی، کارگزاری و مانند آن‌ها، نگهداری سوابق مربوط به شناسایی ارباب رجوع، مالک، سوابق حساب‌ها، عملیات و معاملات داخلی و خارجی اقدام کنند. علی‌رغم قوانین و مقررات مذکور و بسیاری از قوانین مشابه دیگر، در ارزش‌های مجازی به دلیل فقدان نهاد مرکزی متولی و ناظر و معماری هم‌تا به هم‌تا، اجرای هیچ

۱. تبصره ۴ ماده ۳ قانون تنظیم بازار غیر متشکل پولی مصوب ۱۳۸۳/۱۰/۲۲: «اشخاص حقیقی یا حقوقی موضوع این ماده که به عملیات بانکی اشتغال دارند در صورتی که موفق به اخذ مجوز فعالیت تحت عنوان موجود یا عنوان مناسب دیگر ظرف شش ماه از تاریخ لازم‌الاجرا شدن این قانون نشوند بنا به اعلام بانک مرکزی جمهوری اسلامی ایران حق ادامه فعالیت نخواهند داشت. متخلفین از اجرای حکم در صورت شکایت بانک یادشده از طریق مقامات قضایی صلاحیتدار به مجازات حبس تا شش ماه محکوم خواهد شد.»

۲. ماده ۴۵ دستورالعمل اجرایی تأسیس، فعالیت و نظارت بر صرافی‌ها مصوب ۱۳۸۹/۶/۹ بانک مرکزی: «عدم رعایت مفاد این دستورالعمل و قوانین و ضوابط مقرر، علاوه بر ابطال مجوز فعالیت صرافی، حسب مورد موجب اقدامات قضایی و انتظامی و تعقیب کیفری مسئولین صرافی از سوی بانک مرکزی و مراجع ذیربط طبق قانون پولی و بانکی کشور، قانون تنظیم بازار غیرمتشکل پولی و سایر قوانین و مقررات مربوط می‌گردد.»

۳. know your customer

۴. customer due diligence

۵. suspicious transaction report



یک از موارد مذکور، مقدور نیست. اشخاص بدون نیاز به مراجعه حضوری به بانک و یا موسسه مالی و ثبت اطلاعات و مشخصات هویتی خود، می‌توانند از هرکجای دنیا حساب کاربری ایجاد نمایند. هیچ شخصی موظف به احراز هویت و بررسی صلاحیت و صحت اطلاعات کاربران نیست. اصولاً در ارزشهای مجازی، بدلیل آنکه عملیات صحت سنجی تراکنش‌ها بر اساس فرمول‌های ریاضی و الگوریتم‌های رمز نگاری صورت می‌گیرد و هدف از آن حفظ حریم خصوصی و گم‌نام بودن اشخاص است، احراز هویت اشخاص موضوعیتی ندارد.

از سوی دیگر امکان اعمال نظارت و محدودیت‌هایی نظیر بررسی تابعیت اشخاص، میزان مجاز وجوه جهت انتقال یا واریز و برداشت^۱، کشور مبدا و یا مقصد^۲، گزارش دهی معاملات مشکوک^۳ و مسدود نمودن حساب اشخاص^۴، وجود ندارد؛ زیرا تمامی عملیات مالی از نظام پولی و بانکی رسمی به عنوان نقطه حیاتی خارج است و هیچ سامانه اطلاعاتی مربوط به سوابق تراکنش‌ها^۵، کد رهگیری یا شناسایی و مشخصات نمایان‌گر هویت اشخاص، جهت بررسی و کنترل آن‌ها در دسترس نهادهای ناظر قرار

۱. طبق بند ۱۳ ماده یک آئین نامه اجرایی قانون مبارزه با پول‌شویی: «سقف مقرر: مبلغ سقف مقرر در قانون برگزاری مناقصات جهت انجام معاملات خرد، به صورت وجه نقد یا معادل آن به سایر ارزها و کالاهای گران بها که هرساله توسط هیات وزیران به استناد تبصره (۱) ماده (۳) قانون برگزاری مناقصات تصویب می‌گردد.»
۲. بند ۵ تبصره ماده ۷ ق.مبارزه با پول‌شویی: «معاملات یا عملیات مالی که اقامتگاه قانونی هریک از طرفین در مناطق پر خطر (از نظر پول‌شویی) واقع شده است. فهرست این مناطق توسط شورا مشخص می‌شود.»
۳. تبصره ماده ۷ همان قانون: «معاملات و عملیات مشکوک شامل هر نوع معامله، دریافت یا پرداخت مال اعم از فیزیکی یا الکترونیکی یا شروع به آنها است که بر اساس اوضاع و احوالی مانند ارزش، موضوع یا طرفین آن برای انسان به طور متعارف ظن وقوع جرم را ایجاد کند.»
۴. نگاه کنید: آئین‌نامه تعیین ضوابط و مقررات مربوط به محرومیت اشخاص از افتتاح حساب جاری و چگونگی پاسخ استعلام بانک‌ها، مصوب ۱۳۷۳/۸/۲۵ هیات وزیران.
۵. بند ۵ تبصره ماده ۶ قانون مبارزه با پول‌شویی: «نگهداری سوابق مربوط به شناسایی ارباب رجوع، مالک، سوابق حساب‌ها، عملیات و معاملات داخلی و خارجی حداقل به مدت پنج سال پس از پایان رابطه کاری یا انجام معامله موردی است که شیوه آن به موجب آئین نامه اجرایی این قانون تعیین می‌شود.»

ندارد. به عبارت دیگر، ارزشهای مجازی قوانین مرتبط با نظام بانکی و مبارزه با پولشویی را کنار گذاشته‌اند.

در حال حاضر کشور ژاپن اقدام به تدوین مقرراتی جهت فراهم کنندگان خدمات صرافی ارزشهای مجازی نموده است. طبق این قوانین اعمال خرید و فروش ارزشهای مجازی و یا تبدیل آن‌ها به ارزشهای مجازی دیگر؛ واسطه‌گری، دلالی و یا کارگزاری ارزشهای مجازی جهت خرید، فروش و یا تبدیل آن‌ها؛ مدیریت پول و یا ارزشهای مجازی کاربران در رابطه با خرید، فروش و یا تبدیل آن‌ها، همچنین واسطه‌گری، دلالی و یا کارگزاری برای ارزشهای مجازی کاربران، به عنوان خدمات صرافی ارزشهای مجازی شناخته می‌شود و باید جهت انجام آن‌ها مجوز اخذ شود. زندان و جریمه نقدی، همچنین ابطال و یا تعلیق تمام یا بخشی از فعالیت صرافی، ضمانت اجرایی است که در صورت تخلف از مقررات مربوطه نسبت به اشخاص مرتبط اعمال خواهد شد (Ishikawa 2017, p.129).

ایالت نیویورک جهت اعمال قوانین خود بر ارزشهای مجازی، اقدام به گسترش تنظیم‌گری ویژه بیت‌کوین نموده است. در این ایالت مجوز مخصوصی جهت ارزشهای مجازی با عنوان BitLicense در نظر گرفته شده است. با اجرای این مقررات، علاوه بر نظارت بر فروشندگان ارزشهای مجازی توسط نهادهای تنظیم‌گر و فراهم نمودن زمینه لازم جهت اجرای مقاصد نهادهای مجری قانون، امکان حفاظت از مشتریان نیز فراهم می‌شود (Ramasastry 2014).

۳-۵. چالش‌های شناسایی و کشف جرایم مرتبط با ارزشهای مجازی

کشف و تعقیب جرایم که به وسیله ضابطان دادگستری و تحت نظارت و تعلیمات مقام قضایی صورت می‌گیرد از مهم‌ترین مراحل دادرسی فعالیت‌های مجرمانه محسوب می‌شود. دقت، سرعت و صحت عملکرد ضابطان می‌تواند پیشرفت مراحل بعدی



اجرای قانون و رسیدگی قضایی را تند و یا کند نماید. ارزش‌های مجازی ماهیتی کاملاً دیجیتالی دارند و هیچ‌گونه اثر و نشانه حقیقی و فیزیکی خارج از فضای مجازی ندارند. ضمن آن‌که به دلیل جدید بودن این پدیده، ضابطان دادگستری نسبت به نحوه کار و ظرافت‌های فنی ارزش‌های مجازی آگاهی لازم را ندارند. همین مسئله موجب می‌شود تا در مراحل کشف و تعقیب جرایم، چالش‌های جدیدی نمایان شود.

به دلیل شفافیت ناشی از فن‌آوری دفتر کل توزیع شده (زنجیره بلوک عمومی)، امکان مشاهده تمامی تراکنش‌های ارزش‌های مجازی وجود دارد و نهادهای نظارتی و مجری قانون می‌توانند اقدام به رصد آن‌ها نمایند. اما چالش اصلی چگونگی تعیین و تشخیص تراکنش‌های مشکوک در ارزش‌های مجازی و شناسایی طرفین آن است. همان‌گونه که پیش‌تر بیان شد، هر تراکنش به یک کد رمزنگاری شده، که کلید عمومی خوانده می‌شود، متصل است. تنها راه ممکن جهت کشف هویت کاربران، استفاده از روش‌های پیچیده فنی تحلیل شبکه و استفاده از منابع اطلاعاتی است و امکان کشف جرایم مرتبط با آن‌ها بدون استفاده از شیوه‌های فنی پیشرفته وجود ندارد (Kethineni & Cao 2017, p.153). ضمن آنکه باید در نظر داشت اشخاص می‌توانند از آدرس‌های متعدد (کلید عمومی) استفاده کنند که فرآیند کشف و ردیابی را بسیار پیچیده و عملاً غیرممکن می‌سازد (UNODC 2014, p.45). با توجه به اینکه میزان گمنامی اشخاص، بستگی به میزان مهارت آن‌ها در استفاده از روش‌ها و ابزارهای گمنام‌کننده مضاعف دارد، لذا کشف و شناسایی مجرمان حرفه‌ای بسیار سخت‌تر و هزینه‌بر تر از اشخاص عادی است.

یکی دیگر از چالش‌های مرتبط در این زمینه، فقدان رابطه چهره به چهره در به‌کارگیری ارزش‌های مجازی است. با توجه به این‌که در برخی روش‌های نوین پرداخت، کاربر به صورت گمنام عمل می‌کند، ترکیب استفاده از ارزش‌های مجازی و روش‌های نوین پرداخت، امکان شناسایی، ردیابی و تعقیب متهم را دشوار می‌سازد (UNODC, 2014, p.55).

موارد مذکور از جمله چالش‌هایی است که مقامات قضایی و ضابطان دادگستری در مرحله شناسایی و کشف جرم مرتبط با ارزش‌های مجازی با آن‌ها مواجه هستند.

۴-۵. چالش‌های توقیف و مصادره ارزش‌های مجازی

در مواردی که ارزش‌های مجازی به عنوان وسیله و یا موضوع جرم باشد، باید مطابق قوانین توقیف یا مصادره شوند. مطابق تبصره ۲ ماده ۳ قانون مبارزه با پول‌شویی: «کلیه آلات و ادواتی که در فرآیند جرم‌پولشویی وسیله ارتکاب جرم بوده یا در اثر جرم تحصیل شده یا حین ارتکاب، استعمال و یا برای استعمال اختصاص یافته و در هر مرحله از مراحل تعقیب و رسیدگی به دست آید در صورت احراز اطلاع مالک از قصد مجرمانه مرتکب توقیف می‌شود...» وفق ماده ۹ همان قانون: «اصل مال و درآمد و عواید حاصل از ارتکاب جرم منشا و جرم پولشویی (واگر موجود نباشد مثل یا قیمت آن) مرتکبین جرم پولشویی مصادره می‌شود» و در ادامه تبصره همان ماده: «چنانچه عواید حاصل از جرم به اموال دیگری تبدیل یا تغییر یافته همان اموال و در صورت انتقال به ثالث با حسن نیت، معادل آن از اموال مرتکب ضبط می‌شود.» وفق ماده ۵ قانون مبارزه با تأمین مالی تروریسم: «مراجع قضایی و ضابطان دادگستری تحت نظارت و تعلیمات و یا دستور مقام قضایی حسب مورد مکلفند اقدامات زیر را انجام دهند: الف- شناسایی، کشف و مسدود کردن وجوه استفاده شده یا تخصیص داده شده برای تأمین مالی تروریسم و عواید به‌دست آمده از آن‌ها. ب- شناسایی و توقیف اموال موضوع جرایم مذکور در این قانون و عواید آن‌ها که به طور کامل یا جزئی تبدیل به اموال دیگری شده و تغییر وضعیت یافته است. پ- توقیف اموال و عواید موضوع جرم که با اموال قانونی امتزاج یافته به نحوی که اموال مزبوره به اندازه تخمین زده شده قابل توقیف باشد. -تبصره: اشخاص موضوع این ماده موظفند حسب دستور مقام قضایی نسبت به مسدود کردن وجوه و توقیف اموال و

دارایی‌های افراد، گروه‌ها و سازمان‌های تروریستی و همچنین افراد موضوع قانون مبارزه با پولشویی... اقدام نمایند.»

ارزهای مجازی به دلیل گم‌نامی که فراهم کرده‌اند، می‌توانند برای پنهان کردن منشاء پول از طریق تبدیل به و یا خرید ارزهای مجازی و واقعی دیگر، مورد استفاده قرار گیرند. همین‌طور سرمایه‌گذاری در ارزهای مجازی می‌تواند عواید بیش‌تری را به سبب افزایش قیمت ارز مجازی و یا استخراج ارز جدید بوجود آورد. در کشف و تعقیب جرایم مرتبط با ارزهای مجازی به‌خصوص پولشویی و تامین مالی تروریسم، تفکیک این‌که ارز مجازی به عنوان وسیله ارتکاب جرم و یا عواید حاصل از جرم باید توقیف شود، امری دشوار به نظر می‌رسد. هر چند در عمل، این موضوع تاثیر چندانی بر چگونگی و روش‌های توقیف و مصادره آن‌ها ندارد.

از سوی دیگر ماهیت ارزهای مجازی به گونه‌ای است که تصویر دیگری از خود ارائه داده‌اند. برای مثال بیت‌کوین به خودی خود، در هیچ شکلی، حتی به صورت یک فایل دیجیتالی وجود ندارد؛ در واقع آن‌ها فقط ثبت تراکنش‌های مختلف میان آدرس‌های متفاوت هستند که افزایش و کاهش موجودی حساب‌ها را تنظیم می‌کنند. بنابر این اگر ارز مجازی به عنوان وسیله ارتکاب جرم و یا عواید حاصل از جرم در نظر گرفته شود، نمی‌تواند به صورت فیزیکی بر روی یک وسیله و یا محل خاص وجود داشته باشد. با توجه به این‌که ارز مجازی رابطه بی‌واسطه‌ای با آدرس خاصی دارد که کنترل موثر آن‌ها را در اختیار دارد، تنها می‌توان با دسترسی به کیف پول و یا کد رمزنگاری آن، ارز مجازی را توقیف کرد.

ارزهای مجازی فاقد مکان مشخصی هستند. برخلاف شبکه‌های رایانه‌ای متمرکز که دارای یک سرور مرکزی هستند، ارزهای مجازی برپایه شبکه‌ای توزیع شده عمل می‌کنند، که از توان محاسباتی و نرم‌افزاری گره‌ها استفاده می‌کند. برخلاف شبکه‌های متمرکز که امکان متوقف کردن آن‌ها از طریق اجبار نهاد مرکزی مدیریت‌کننده و یا

دسترسی فیزیکی به محل سخت افزار مرکزی ممکن است، در ارزش‌های مجازی بدلیل ساختار توزیع شده، چنین امری مقدور نیست. نکته دیگری که باید به آن توجه داشت این است که امکان مسدود کردن و یا جلوگیری از نقل و انتقال ارزش‌های مجازی به دلیل غیرمتمرکز بودن و فقدان نهاد مسؤول، وجود ندارد.

۵-۵. چالش چگونگی نگهداری ارزش‌های مجازی

یکی از مشکلات ضابطان دادگستری و دادرسان، نگهداری اموال توقیف شده است. ارزش‌های مجازی به صورت فیزیکی موجود نیستند و نگهداری آن‌ها چالش‌های منحصر به فردی به همراه دارد. در صورتی که ارز مجازی توقیف شود، نگهداری آن دارای الزامات مخصوص خود است. ضابطان دادگستری باید ارز مجازی را به یک کیف پول دیجیتالی متعلق به دادگستری و یا پلیس انتقال دهند تا در آن ذخیره شود. کیف پول متعلق به نهادهای قانونی و کلید خصوصی آن باید با استفاده از روش‌های فنی مورد حفاظت قرار گیرد تا مورد سرقت واقع نشود و از هرگونه دستکاری محفوظ باشد.^۱ بدیهی است با توجه به تنوع گسترده ارزش‌های مجازی و کیف پول‌های مجازی، نحوه انتخاب بهترین و امن‌ترین کیف پول باید توسط کارشناسان این عرصه تعیین شود.^۲ همچنین باید تدابیری اندیشیده شود تا امکان سوء استفاده احتمالی اشخاص مسؤول نیز از بین برود.^۱

۱. بند د ماده یک آئین نامه جمع‌آوری و استناد پذیری ادله الکترونیکی: «زنجیره حفاظتی: مجموعه اقداماتی است که ضابط دادگستری و سایر اشخاص ذی صلاح به منظور حفظ صحت، تمامیت، اعتبار و انکار ناپذیری ادله الکترونیکی با به کارگیری ابزارها و روش‌های استاندارد در مراحل شناسایی، کشف، جمع‌آوری، مستند سازی، تجزیه و تحلیل و ارائه آنها به مرجع مربوط به اجرا درآورده و ثبت می‌کنند؛ به نحوی که امکان رد یابی آنها از مبدا تا مقصد وجود داشته باشد.»

۲. ماده ۳۶ آئین نامه جمع‌آوری و استنادپذیری ادله الکترونیکی: «ضابطان و اشخاصی که حسب قانون مأمور جمع‌آوری، تفتیش، نگهداری، حفظ و انتقال داده‌ها و سامانه‌های رایانه‌ای یا مخابراتی می‌شوند باید علاوه بر



تغییر قیمت ارزهای مجازی در مدت نگهداری و نحوه فروش ارزهای مجازی
مصادره شده نیز از موضوعاتی اند که نیاز به بررسی دارند.

۵-۶. چالش استفاده از ادله الکترونیک

برخلاف ادله سنتی و فیزیکی که در یک فعالیت مجرمانه فراهم می‌شود و می‌تواند شامل اسناد و مدارک فیزیکی، شهادت شهود، فیلم، عکس و... باشد، ادله الکترونیکی در فضای مجازی شکل می‌گیرند و باید آنها را در این محیط و با ابزارهای الکترونیکی مانند رایانه و دستگاه‌های مرتبط با آن، بدست آورد. سیستم‌ها و وسائل سخت افزاری و نرم‌افزاری الکترونیکی برحسب فن‌آوری به‌کار گرفته شده، می‌تواند طیف گسترده‌ای از شبکه‌های رایانه‌ای، تلفن‌های همراه، وسائل ذخیره داده، فضاهای ذخیره سازی ابری^۲، اینترنت و... را شامل شود. تمامی موارد فوق در فرآیند ایجاد و ذخیره اطلاعاتی که می‌تواند به عنوان دلیل مورد استناد قرار گیرند، ممکن است مورد استفاده واقع شوند. (UNODC 2014, p.60).

ارزهای مجازی اصولاً در فضای برخط^۳ عمل می‌کنند و تمامی تراکنش‌ها بر بستر شبکه رایانه‌ها و داده‌ها قرار دارد. بنابر این در جرایم مرتبط با ارزهای مجازی بیش‌تر دلایل مرتبط به صورت الکترونیک است و هیچ سند فیزیکی در دسترس نیست؛ مگر در موارد محدودی که ارزهای مجازی از طریق یک نهاد قانونی که ملزم به ثبت و نگهداری سوابق باشد، به پول واقعی تبدیل شده‌اند یا برعکس.

داشتن شرایط لازم از قبیل تخصص و توانایی فنی و آموزش کافی، تجهیزات و وسایل لازم را در اختیار داشته باشند».

۱. ماده ۲۰ همان: «از زمان ارائه داده‌ها به ضابطان قضایی یا دیگر اشخاص ذی‌ربط، مسئولیت حفظ داده‌های مذکور با شخص یا اشخاص تحویل گیرنده خواهد بود.»

۲. Cloud storage

۳. Online

سختی ردیابی و کشف ادله در ارزش‌های مجازی (Greenemeier 2015) به گونه‌ای است که تنها از عهده اشخاص متخصص برمی‌آید. در صورتی که متهم از ابزارهای گم‌نام کننده و یا ماشین‌های مجازی^۱ استفاده کرده باشد، کشف و شناسایی ارزش‌های مجازی و یا استفاده از آن را نمی‌توان به راحتی مستند سازی کرد. هر چند تراکنش‌های ثبت شده در زنجیره بلوک، تغییر ناپذیر و در نتیجه قابل استناد هستند^۲، اما مسئله اصلی باتوجه به گم‌نام بودن کاربران و تراکنش‌ها، نحوه اثبات و انتساب آنها به یک شخص معین^۳ می‌باشد.

ادله الکترونیک بخصوص در مورد ارزش‌های مجازی، در معرض تغییر قرار دارند و به میزان زیادی^۴ فرار هستند. زیرا کدهای مربوط به ارزش‌های مجازی تعدادی شماره‌اند که میزان حجمی که در فضای مجازی اشغال می‌کنند بسیار ناچیز محسوب می‌شود، بنابر این به راحتی می‌توانند در کوچک‌ترین فضای ذخیره سازی، پنهان شوند. اگر رایانه شخص مظنون و یا متهم توقیف شود، باید اقدامات لازم جهت کسب دلایل، به صورت فوری^۵ صورت گیرد. ممکن است اطلاعات ذخیره شده به جهت بروز رسانی نرم‌افزارها و یا حذف داده‌های قبلی و ثبت داده‌های جدید در سیستم‌های رایانه‌ای، از دست بروند. در صورتی که شخص مجرم دارای تخصص

۱ . Virtual Machines

۲. ماده ۱۱ قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۲۴: «سابقه الکترونیکی مطمئن عبارت است از داده است که

با رعایت شرایط یک سیستم اطلاعاتی مطمئن ذخیره شده و به‌هنگام لزوم در دسترس و قابل درک است.»

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

۴ . High volatility

۵. بند د ماده ۱ همان آیین نامه: «جمع‌آوری ادله الکترونیکی: فرآیندی است که طی آن ادله الکترونیکی به تنهایی یا به همراه سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده، نگهداری، حفظ فوری، تفتیش و توقیف و شنود می‌شوند.»



بالایی باشد، می‌تواند با استفاده از نرم‌افزارهای خاص، در بازه‌های زمانی مشخص داده‌های موجود در رایانه را حذف کند تا دسترسی به آن‌ها ممکن نباشد. با توجه به لزوم حفظ صحت و تمامیت ادله الکترونیک و جهت انتساب امضای الکترونیک گم‌نام به شخص متهم، باید اطلاعات جمع‌آوری شده مطابق با اصول کلی مربوط به دلیل و روش تحصیل آن در امور کیفری و همچنین مطابق با استناد پذیری ادله الکترونیک باشد. این موضوع برای ضابطان قضایی و سایر نهادهای مجری قانون دارای اهمیت است، زیرا باید از تدابیر فنی و روش‌های تخصصی برای کسب دلایل، نگهداری و ارائه آن‌ها در موارد لازم، استفاده شود.^۱

۵-۷. چالش تعیین قلمرو صالح قضایی

ارزهای مجازی در یک محیط برخط عمل می‌کنند که مرزهای ملی را از بین برده است و تجارت الکترونیک را به یک پدیده جهانی تبدیل کرده است. یکی از چالش‌های اساسی در این رابطه، تعیین قلمرو صالح قضایی جهت بازیابی عواید حاصل از جرایم مرتبط با ارزهای مجازی است. همین طور در خصوص تمهیداتی که باید جهت همکاری‌های بین‌المللی صورت گیرد، تعیین حوزه قضایی صالح ضروری است. مطابق ماده ۱۱۸ قانون آیین دادرسی کیفری: «هرگاه آثار و ادله وقع جرمی در حوزه قضایی محل مأموریت بازپرس کشف شود، اما محل وقوع آن معلوم نباشد، بازپرس ضمن انجام تحقیقات، سعی در کشف محل وقوع جرم می‌کند و اگر محل وقوع جرم تا ختم تحقیقات مشخص نشود، بازپرس در خصوص موضوع، اظهار عقیده می‌کند». یکی از مواردی که می‌تواند محل وقوع جرم نامعلوم باشد، جرایم مرتبط با ارزهای مجازی است که در محیط سایبری و بدون وجود مکان فیزیکی و مرکزیتی معلوم ارتکاب می‌یابد. در این موارد در صورتی که امکان شناسایی و تعیین

۱. ماده ۷ همان: «داده‌های محتوا و ترافیک و اطلاعات کاربران باید مطابق مقررات این آئین نامه به نحوی نگهداری، حفاظت، توقیف و ارائه شود که صحت و تمامیت، محرمانگی، اعتبار و انکار ناپذیری آنها محفوظ بماند.»

موقعیت جغرافیایی سخت افزار حامل کیف پول مجازی وجود داشته باشد، می‌توان محل نگهداری کیف پول را به عنوان مکان وقوع جرم در نظر گرفت. زیرا کنترل ارزشهای مجازی از طریق کیف پول صورت می‌گیرد.

۶. نتیجه و پیشنهاد

ارزشهای مجازی به عنوان پدیده‌ای نو در فضای مجازی، همراه با سود و زیان‌هایی است. افزایش سرعت، کاهش هزینه، افزایش حریم خصوصی و سهولت استفاده از این ارزشها موجب محبوبیت و رونق آنها شده است. گم‌نامی و فقدان نهاد مرکزی برای نظارت و اعمال قوانین موجب شده است تا امکان استفاده از این پدیده در فعالیت‌های مجرمانه فراهم شود. ویژگی‌های مذکور به همراه ابهام در وضعیت قانونی و عدم شناخت کافی مردم، سیاستگذاران و نهادهای مجری قانون از این پدیده، چالش‌هایی را پیش روی نظام عدالت کیفری در دادرسی جرایم مرتبط با آنها قرار داده است. ابهام در ماهیت ارزشهای مجازی، چگونگی اعمال قوانین و مقررات بر ارزشهای مجازی، چگونگی شناسایی و کشف جرایم، توقیف و مصادره و نگهداری ارزشهای مجازی، استفاده از ادله الکترونیک و تعیین قلمرو صالح قضایی از چالش‌های اصلی در دادرسی جرایم مرتبط با ارزشهای مجازی است.

بررسی‌های پژوهش نشان می‌دهد ویژگی‌های گم‌نامی کاربران و غیر متمرکز

بودن ارزشهای مجازی به همراه ابهام در ماهیت ارزشهای مجازی، چالش‌های جدیدی



در رسیدگی به دعاوی کیفری بوجود آورده است. به گونه‌ای که در کلاهبرداری که ارز مجازی موضوع جرم است، مطابق قانون، بزهار به رد مال و پرداخت جزای نقدی معادل مالی که برده است محکوم می‌شود؛ در حالی که بازگرداندن ارزهای مجازی در موارد بسیاری امکان پذیر نیست و برای تعیین قیمت مال برده شده، مرجع قانونی وجود ندارد. کشف و تعقیب جرایم این حوزه بدلیل فقدان نهاد مرکزی و مسؤول در ارزهای مجازی و عدم دسترسی به اطلاعات نهادهای واسط مانند سایت‌های کیف پول ارز مجازی، نهادهای مجری قانون و قضات را با مشکلاتی مواجه کرده است.

نتایج پژوهش بیانگر آن است که رفع ابهام از ماهیت ارزهای مجازی و به تبع تعیین نهاد متولی ناظر توسط قانونگذار، آن استفاده از روش‌های فنی در نظارت و سازماندهی صرافی‌ها و مراکز خدمات‌دهی به ارزهای مجازی و الزام آن‌ها به اعمال قوانین و مقررات پولی و مالی، مبارزه با پولشویی و تأمین مالی تروریسم، آموزش ضابطان قضایی و دادرسان، تبادل اطلاعات میان بخش‌های خصوصی و دولتی در عرصه داخلی و بین المللی از جمله اقداماتی است که می‌تواند چالش‌های پیش‌گفته را از میان بردارد.

موارد ذیل به عنوان راهکاری در برابر چالش‌های دادرسی جرایم مرتبط با ارزهای مجازی، پیشنهاد می‌شود:

۱. با توجه به ابهام در وضعیت حقوقی ارزهای مجازی و عدم انطباق آن‌ها با تعریف فعلی از ارز، قانونگذار نسبت به اصلاح بند پ ماده یک قانون مبارزه با قاچاق کالا و ارز، از طریق افزودن تعریف ارزهای مجازی و قراردادن آن‌ها در حکم ارز، اقدام کند.

۲. ضمن به رسمیت شناختن استفاده از ارزش‌های مجازی، نهادهای مسئول در زمینه سیاست‌گذاری، نظارت و کنترل آن‌ها توسط قانون‌گذار تعیین شود.
۳. آیین‌نامه‌ی نحوه تاسیس و اخذ مجوز جهت صرافی‌های ارزش‌های مجازی و ارائه دهندگان خدمات اینترنتی به منظور اعمال قوانین و مقررات بر خرید، فروش و نگهداری ارزش‌های مجازی، با همکاری بانک مرکزی جمهوری اسلامی ایران و وزارت ارتباطات و فن‌آوری اطلاعات تدوین شود.
۴. آئین‌نامه‌ی نحوه اعمال مقررات مقابله با پولشویی و تامین مالی تروریسم در ارزش‌های مجازی با همکاری بانک مرکزی جمهوری اسلامی ایران، وزارت ارتباطات و فن‌آوری اطلاعات، وزارت اطلاعات، پلیس فتا و وزارت دادگستری تدوین شود.
۵. شیوه‌نامه نحوه همکاری و تعامل میان بخش خصوصی و بخش دولتی در زمینه تبادل اطلاعات مرتبط با ارزش‌های مجازی، در سطوح ملی، منطقه‌ای و بین‌المللی با همکاری وزارت خانه‌های ذی ربط تدوین شود.
۶. آئین‌نامه چگونگی کشف، توقیف، انتقال و نگهداری ارزش‌های مجازی، با همکاری پلیس فتا، وزارت دادگستری و وزارت ارتباطات و فن‌آوری اطلاعات تدوین شود.
۷. وفق بند ۱۳ ماده ۳۸ آئین‌نامه اجرایی ماده (۱۴) الحاقی قانون مبارزه با پولشویی، دوره‌های آموزشی تخصصی برای دادرسان، ضابطان دادگستری و کارشناسان نهادها و سازمان‌هایی که مکلف به اجرای قوانین ضد پولشویی و تامین مالی تروریسم هستند، طراحی و برگزار شود.
۸. با توجه به ویژگی جهان‌شولی ارزش‌های مجازی و برای تسهیل کشف جرایم و تعقیب مجرمین، مقررات داخلی با قواعد بین‌المللی جهت همکاری با کشورهای خارجی و نهادهای بین‌المللی در زمینه تبادل اطلاعات، انتقال تجربیات، استرداد مجرمین، توقیف و مصادره ارزش‌های مجازی هماهنگ شود.

۷. منابع



۱-۷. فارسی

۱. بانک مرکزی ج.ا.ایران، پیش‌نویس الزامات و ضوابط حوزه رمز ارزها، معاونت فن‌آوری‌های نوین، ۱۳۹۷.
۲. درشر، دنیل، مبانی بلاکچین، مقدمه ای غیرفنی در ۲۵ گام، ترجمه: سیاوش تفضلی. چاپ اول. تهران؛ صفحه سفید، ۱۳۹۷.
۳. سلطانی، محمد؛ اسدی، حمید، ماهیت حقوقی پرداخت در پول الکترونیک. پژوهشنامه حقوق اسلامی، سال شانزدهم، شماره اول (پیاپی ۴۱)، بهار و تابستان، ۱۳۹۴.
۴. محمد رضا داوری، مجید داوری، پول‌شویی الکترونیکی و راهکارهای فنی و بین‌المللی دفاع در برابر آن. فصلنامه پدافند غیرعامل، سال اول، شماره ۴، پاییز، ۱۳۸۹.
۵. مرکز پژوهش‌های مجلس شورای اسلامی، ارزش مجازی: قانونگذاری در کشورهای مختلف و پیشنهادها برای ایران، ۱۳۹۷.
۶. نواب پور، علیرضا؛ یوسفی، احمد علی؛ طالبی، محمد، تحلیل فقهی کارکردهای پول‌های رمزنگاری شده (مورد مطالعه بیت کوین)، فصلنامه علمی پژوهشی اقتصاد اسلامی، سال هجدهم، شماره ۷۲، زمستان، ۱۳۹۷.

۲-۷. انگلیسی

7. Anita, Ramasastry, Bitcoin: If You Can't Ban It, Should You Regulate It? The Merits of Legalization, JUSTIA.COM, Feb. 25, 2014.
8. A. Dominick Romeo, *Hidden Threat: The Dark Web Surrounding Cyber Security*, 43 N. Ky. L. Rev. 73, 2016.
9. Charleston L. Rev, *Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation*, 8 Charleston L. Rev. 511, 2014.
10. EBA, *Opinion on virtual currencies*, European Banking Authority, 2014.

11. Elizabeth M. Valeriane, *IRS, Will You Spare Some Change: Defining Virtual Currency for the FATCA*, 50 Val. U. L. Rev. 863, 2016.
12. Ethan D. Jeans, *Funny Money or the Fall of Fiat: Bitcoin and Forward-Facing Virtual Currency Regulation*, 13 J. on Telecomm. & High Tech. L.99, 2015.
13. FATF, REPORT, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, 2014.
14. Financial Action Task Force: *Money Laundering & Terrorist Financing Vulnerabilities Of Commercial Websites And Internet Payment Systems*, 2008.
15. James Martin), *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs*, First published, UK: Palgrave Macmillan, 2014.
16. Jessica Hoyer, *SEX TRAFFICKING IN THE DIGITAL AGE: THE ROLE OF VIRTUAL CURRENCY-SPECIFIC LEGISLATION IN KEEPING PACE WITH TECHNOLOGY*; 63 Wayne L. Rev. 83, 2017.
17. Jonathan Lane., *Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation*, 8 Charleston L. Rev. 511, 2014.
18. Hak J. Kim, *Virtual Currency Is Becoming Reality: Is It Opportunity or Disaster*, 16 J. Int'l Bus. & L. 75, 2016.
19. Malcolm Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance*; Springer Science+Business Media B.V., part of Springer Nature, 2018.
20. Mai Ishikawa(, *Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case*; Journal of Financial Regulation, 2017.
21. Larry Greenemeier, *Human Traffickers Caught on Hidden Internet*, Sci. AM., 2015.
22. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.
23. Sesha, Kethineni; Ying, Cao; Cassandra, Dodge, *Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes*; Southern Criminal Justice Association, 2017.

24. UNODC, *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, 2014.