مجله حقوقی بین‌المللی/ شماره ۶۲/ بهار ـ تابستان ۱۳۹۹/ صفحات ۲۸ ـ ۷

چالش ارزهای مجازی در مبارزه با پولشویی و تأمین مالی تروریسم با تأکید بر اقدامات و توصیه‌های کارگروه ویژه اقدام مالی(FATF)

عباسعلی کدخدایی *

حسام نوروزپور **

شناسه دیجیتال اسناد (DOI) : 10.22066/CILAMAG.2019.101998.1647

تاریخ دریافت: ۱۳۹۷/۱۰/۲۶ تاریخ پذیرش: ۱۳۹۸/۰۲/۲۳

چکیده

ابزارها و شیوه‌های پولشویی به‌عنوان اصلی‌ترین روش تسهیل‌کننده تأمین مالی تروریسم، با ظهور فناوری‌های نوین، چنان تنوع یافته است که دیگر نمی‌توان مبارزه با آن را به قالب‌های سنتی گذشته منوط کرد. تروریست‌ها و تبهکاران از فناوری‌های نوین چون اینترنت و ارزهای مجازی برای توسعه روش‌های مجرمانه خویش بسیار سود می‌جویند. ارزهای مجازی بر بستری غیرمتمرکز و در پوشش ناشناختگی عمل می‌کنند. این ارزها در اغلب موارد فاقد پشتوانه دولتی بوده و هیچ ضمانت یا نظارتی را بر خویش نمی‌بینند. هرچند ویژگی‌های خاص ارزهای مجازی، کار را برای مجرمین و تروریست‌ها تسهیل کرده، نباید در این امر مبالغه کرد. مطالعات نهادهای بین‌المللی چون کارگروه ویژه اقدام مالی در سال‌های اخیر، تا حدودی نقاط قوت مبارزه با اعمال مجرمانهٔ ارتکابی با توسل به این ابزارهای مجازی را آشکار کرده است.

این پژوهش بر آن است با تحلیل جنبه‌های مختلف ارزهای مجازی، تأثیر آن‌ها را بر اجرای قواعد ضدپولشویی (AML) و تأمین مالی تروریسم (CFT) بررسی کند. این موضوع، به‌ویژه در سال‌های اخیر علاوه بر کشورهای مختلف، توجه نهادهایی چون کارگروه ویژه اقدام مالی را نیز به خود جلب کرده است.

واژگان کلیدی

ارزهای مجازی، ناشناختگی، پولشویی، تأمین مالی تروریسم، کارگروه ویژه اقدام مالی

* استاد دانشکده حقوق‌وعلوم‌سیاسی دانشگاه تهران kadkhoda@ut.ac.ir

** نویسنده مسئول، دانشجوی دکتری حقوق فناوری دانشگاه هنگ‌کنگ hesam.norouzpour@ut.ac.ir

مقدمه

در سال‌های اخیر، مبارزه با جرایم سازمان‌یافته و تروریسم، هم در نهادهای بین‌المللی همچون کارگروه ویژه اقدام مالی (FATF) و سازمان ملل و هم در داخل کشورها بسیار بحث‌برانگیز شده است. واقعیت آن است که ابزارها و شیوه‌های پولشویی، به‌عنوان اصلی‌ترین عامل تأمین مالی جرایم مذکور، با ظهور و بروز فناوری‌های نوین چنان تنوع یافته است که دیگر نمی‌توان مبارزه با آن را به قالب‌های سنتی گذشته محدود کرد. امروزه فناوری با سرعتی شگرف پیش می‌تازد و بر خوشایند و عدم خوشایند بشر نیز تأمل نمی‌کند. تروریست‌ها و تبهکاران چه به‌صورت فردی و چه در قالب گروه‌های سازمان‌یافته نیز ضرورت همگام‌شدن با این پیشرفت را دریافته‌اند و از این فناوری‌های نوین برای توسعه روش‌های مجرمانه خویش بسیار سود می‌جویند.

در وهله نخست، گروه‌های تبهکاری با دقت فراوان از محصولات فناوری‌های مدرن از قبیل بانکداری مجازی و پول الکترونیکی برای ازبین‌بردن حلقه ارتباطی میان فعل مجرمانه و خویش استفاده می‌کردند که در واقع این فرصت را برای آن‌ها فراهم می‌کرد تا بدون نیاز به حضور فیزیکی به خرید و فروش کالا بپردازند. هرچند این واسطه‌های خدماتی از الگوهای دیجیتال برای شناسایی هویت فرستنده و گیرنده بهره می‌بردند، تبهکاران به روش‌هایی از قبیل هک‌کردن رایانه‌های دیگران و سرقت هویت دیجیتال آن‌ها متوسل شده و هویت واقعی خود را پنهان می‌کردند. با ظهور ارزهای مجازی بخصوص ارزی چون *بیت‌کوین* با فناوری خاص، مجرمان ابزار تازه‌ای یافتند که با اصل‌قراردادن ناشناختگی این فرصت را به دارندگان خود می‌دهند که بدون نیاز به تأیید یا معرفی هویت خویش، تراکنش‌های مالی نامحدودی انجام دهند. در دو سال گذشته، مجرمین به حدود ۱,۲ میلیارد ارز مجازی دست یافته‌اند و این رغم تنها در نیمه اول سال ۲۰۱۸ میلادی به سه‌برابر مجموع سال ۲۰۱۷ افزایش یافته است.[۱]

تا چند سال قبل تقریباً اغلب نویسندگان اتفاق‌نظر داشتند که ارزهای مجازی، ارزهایی دیجیتال مبتنی بر شبکه نظیر به نظیر (P2P)[۲] و محصول رمزنگاری هستند.[۳] اما دیگر اجماعی جهانی بر سر این تعریف وجود ندارد زیرا به‌رغم این واقعیت که از واژه «ارز» برای این پدیده نوظهور استفاده

1. Chavez-Dreyfuss, Gertrude, "About $1.2 Billion in Cryptocurrency Stolen Since 2017: Cybercrime Group, 2018", retrieved from: https://www.reuters.com/article/us-crypto-currency-crime/about-1-2-billion-in-cryptocurrency-stolen-since-2017-cybercrime-group-idUSKCN1IP2LU. (visited: 18/11/2018).

۲. شبکه نظیر به نظیر یا Peer to Peer به معنای ارتباط مستقیم و بدون نیاز به واسط (سرور) سامانه‌های رایانه‌ای با یکدیگر است و معماری آن به گونه‌ای است که تمام سامانه‌های درون شبکه دسترسی برابری دارند و هرکدام از سامانه‌ها، جزئی از منابع شبکه به حساب می‌آیند اما در واقع نکته مهم‌تر در این روش ارتباطی آن است که امکان نظارت مرجع بالادستی بر تبادلات اعضای شبکه وجود ندارد.

3. Bierer, Timothy, "Hashing Out: The Problems and Solutions Concerning Cryptocurrency Used as Article 9. Collateral", *Case W. Res. J.L. Tech. & Internet*, vol. 77,issue 1, 2016, p. 83.

می‌شود، امروزه نظر مخالف جدی وجود دارد که ارزهای مجازی را ارز یا پول نمی‌داند.[۴] اما آنچه تقریباً همگان امروزه بر آن توافق دارند این است که ویژگی‌های این ارزهای مجازی یا ارزرمزها[۵] نه‌تنها قالب‌های سنتی حاکمیتی پولی دولت‌ها و سازمان‌هایی چون صندوق بین‌المللی پول و بانک مرکزی اروپا و خزانه‌داری ایالات متحده را به چالش کشانده، بلکه همان طور که گفته شد، بی‌قاعدگی و عدم توافق بر سر مقرراتی یکسان در مواجهه با آن‌ها اندک اندک به سمت و سویی می‌رود که به یکی از ابزارهای اصلی تأمین مالی جرایم سازمان‌یافته فراملی و تروریسم بدل شود.

این پژوهش بر آن است با تحلیل جنبه‌های مختلف ارزهای مجازی، تأثیر آن‌ها را بر اجرای قواعد ضدپولشویی(AML)[۶] و تأمین مالی تروریسم (CFT)[۷] بررسی کند. این موضوع به‌ویژه در سال‌های اخیر علاوه بر کشورهای مختلف، توجه نهادها و سازمان‌های بین‌المللی چون سازمان ملل و کارگروه ویژه اقدام مالی را به خود جلب کرده است. در این مسیر ابتدا به بحث پولشویی که بستر پژوهش حاضر است، سپس ارزهای مجازی و ویژگی خاص این ارزها و اشکال شناخته‌شدهٔ پولشویی از طریق آن‌ها که باعث می‌شود کنترل و نظارت بر آن‌ها دشوارتر باشد، و در پایان به بررسی توصیه‌ها و اقدامات بین‌المللی که به شکل خاص از سوی کارگروه ویژه اقدام مالی صورت گرفته پرداخته خواهد شد.

۱. پولشویی و تأمین مالی تروریسم

تمرکز این مقاله بر پولشویی از طریق ارزهای مجازی است اما به هرحال این امر تابع پولشویی است و بنابراین در ابتدا باید به درکی از مفهوم پولشویی دست یافت. جرایم اقتصادی بسیاری به امید رسیدن به اهداف مالی از طریق اعمال غیرقانونی صورت می‌گیرد که از آن جمله می‌توان به قتل، قاچاق مواد مخدر، قاچاق سلاح و کلاهبرداری اشاره کرد. اما ارتکاب چنان جرایمی صرفاً مرتکب یا مرتکبین را منتفع نمی‌کند. عواقب این اعمال باعث بروز ناهنجاری‌های اجتماعی و خروج پول از چرخه مشروع و قانونی آن می‌شود. مجرمین برای بهره‌مندی از پول غیرقانونی ابتدا باید آن را از طریق نهادهای قانونی منشأ دارایی که از فعالیت‌های اقتصادی مشروع حاصل شده‌اند تطهیر کنند.[۸]

۱ـ۱. پیشینه و تعریف

ظاهراً یک گروه مافیایی در ایالات متحده مبدع اصطلاح «پولشویی» برای تطهیر مبالغ هنگفت

4. Prentis, Mitchell, "Digital Metal: Regulating Bitcoin as a Commodity", *Case W. Res. J.L. Tech. & Internet*, vol. 66,issue 2, 2015, p. 626.

5. Cryptocurrencies

6. Anti-Money Laundering

7. Combating the Financing of Terrorism

8. Pacleb, Calvin Lee, "International Money Laundering: A Comprehensive Review and General Theory of Corruption", 2003, p. 51. retrieved from: https://ttu-ir.tdl.org/ttu-ir/bitstream/handle/2346/14128/31295018735125.pdf. (Accessed:10/10/2018).

پول‌های ناشی از تجارت غیرقانونی بوده است. این گروه از رختشورخانه‌ها برای تطهیر پول‌های ناشی از اعمال غیرقانونی خود استفاده می‌کرد.[۹]

پولشویی جرمی قدیمی است اما به لحاظ وضع قوانین داخلی و اقدامات بین‌المللی جزو جرایم نوظهور طبقه‌بندی می‌شود. اینترپل، آن را این‌گونه تعریف کرده است: «پولشویی شامل اقدام برای مخفی‌کردن یا پنهان نگاه‌داشتن چگونگی کسب غیرقانونی پول است به منظور تظاهر به اینکه از منابع مشروع و قانونی حاصل شده است».[۱۰]

صندوق بین‌المللی پول (IMF) نیز این تعریف را کمابیش پذیرفته است: «پولشویی فرایندی است که منبع غیرقانونی دارایی‌های مکتسبه یا حاصل از فعالیت‌های مجرمانه را در جهت پنهان‌کردن ارتباط میان دارایی و منشأ مجرمانه پول به کار می‌برد».[۱۱]

اما کارگروه ویژه اقدام مالی (از این پس کارگروه) را می‌توان مهم‌ترین نهاد کنونی مبارزه با پولشویی و تأمین مالی تروریسم در سطح بین‌المللی دانست. این کارگروه هرچند به تعریف کوتاهی در خصوص پولشویی بسنده کرده و آن را «فرایندی در ادامه اعمال مجرمانه می‌داند که برای پنهان‌کردن منشأ غیرقانونی پول حاصله صورت می‌گیرد»،[۱۲] در ادامه آن را این‌گونه بیان می‌دارد: «نخست پول، چه به‌صورت رسمی و چه غیررسمی وارد نظام مالی داخلی می‌شود؛ سپس برای درهم‌آمیخته‌شدن با نظام مالی کشور مقصد به خارج از کشور ارسال و سرانجام در ظاهری مشروع به کشور فرستنده بازگردانده می‌شود».[۱۳]

۱ـ۲. رویکرد قانونگذار ایران

با توجه به اینکه در حال حاضر بحث‌های متعددی در خصوص رعایت الزامات کارگروه در ایران مطرح شده، بهتر است نگاهی هرچند گذرا به جرم‌انگاری پدیده پولشویی در قوانین داخلی نیز بشود. قانونگذار داخلی در ماده ۲ قانون مبارزه با پولشویی، مصوب ۱۳۸۶ در سه بند این جرم را تعریف کرده است: «الف) تحصیل، تملک، نگهداری یا استفاده از عواید حاصل از فعالیت‌های غیرقانونی با علم به اینکه به‌طور مستقیم یا غیرمستقیم در نتیجه ارتکاب جرم به دست آمده باشد. ب) تبدیل، مبادله یا انتقال عوایدی به منظور پنهان‌کردن منشأ غیرقانونی آن با علم به اینکه به‌طور مستقیم یا غیرمستقیم ناشی از

9. AL Hassan, Abdulaziz, "Money Laundering and Terrorism Financing: Does the Saudi Arabian Financial Intelligence Unit Comply with International Standards?", *Research Master Thesis, Victoria University*, 2011, p. 16. retrieved from: http://vuir.vu.edu.au/19945/1/Abdulaziz_Al-Hassan.pdf (visited: 18/11/2018).

10. https://www.interpol.int/Crime-areas/Financial-crime/Money-laundering.

11. IMF and the Fight against Money Laundering and the Financing of Terrorism, 2018. Retrieved from: https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/31/Fight-Against-Money-Laundering-the-Financing-of-Terrorism (visited: 13/11/2018).

12. http://www.fatf-gafi.org/faq/moneylaundering/.

13. FATF, "Report on Money Laundering Typologies, 2000-2001", p. 21. retrieved from: http://www.fatf-gafi.org/countries/s-t/spain/documents/fatfannualreport2000-2001.html (visited:10/10/2018).

ارتکاب جرم بوده یا کمک به مرتکب به نحوی که وی مشمول آثار و تبعات قانونی ارتکاب آن جرم نگردد. ج) اخفاء یا پنهان یا کتمان‌کردن ماهیت واقعی، منشأ، منبع، محل، نقل و انتقال، جابه‌جایی یا مالکیت عوایدی که به‌طور مستقیم یا غیرمستقیم در نتیجه جرم تحصیل شده باشد».

همان طور که در مقایسه با تعاریف بین‌المللی مشهود است، تعریف قانونگذار ایران از جرم پولشویی بسیار مفصل‌تر است اما به نظر می‌رسد این تفصیل با اشکالاتی نیز همراه است که به‌صورت خلاصه عبارت‌اند از: ۱ـ قانونگذار سه عنصر تحصیل، تملک، نگهداری یا استفاده از عواید حاصل از فعالیت‌های مجرمانه را بخشی از عناصر مادی جرم تعریف کرده است که اصولاً با توجه به اینکه جرم پولشویی انتقال عواید نامشروع به قصد تطهیر آن‌هاست، موارد مذکور، خارج از عناصر این جرم است. ۲ـ بندهای (ب) و (ج) دارای همپوشانی است زیرا اقدامات مندرج در بند (ب) اصولاً با هدف دست‌یافتن به موارد مندرج در بند (ج) صورت می‌گیرد؛ و در نهایت ۳ـ قانونگذار به یکی از مهم‌ترین عناصر جرم پولشویی که همانا «درآمیختن عواید نامشروع از جرم با عواید حاصل از منابع مشروع» است اشاره نکرده است.

علاوه بر این موارد، قانونگذار داخلی تا کنون در راستای ساماندهی ارزهای مجازی هیچ اقدامی نکرده و بانک مرکزی به‌عنوان متولی نظام پولی و مالی کشور، تنها به صدور چند دستورالعمل مختصر و متضاد با یکدیگر بسنده کرده است[۱۴] که بیشتر موجب سردرگمی شده و بدین وسیله نه‌تنها جامعه از فواید و منافع این ارزهای رمزی بی‌بهره مانده، بلکه در نبود قانون و نظارت، احتمال سواستفاده از آن‌ها در جرایمی چون پولشویی نیز قوت گرفته است.

۱ـ۳. رابطه پولشویی با تأمین مالی تروریسم

باید دانست که تروریست‌ها اصراری بر تطهیر عواید حاصل خود ندارند و اصولاً یکی از منابع عمده تأمین مالی تروریسم، تجارت قانونی و کمک‌های داوطلبانه است[۱۵] که نیازی به پولشویی ندارد. آنچه برای تروریست‌ها مهم‌تر است، مسئله تقسیم یا توزیع پول به نحوی است که نهادهای ناظر، قادر به کشف و ضبط آن نباشند و اینجاست که پولشویی به کمک تأمین مالی تروریسم می‌آید. در نتیجه می‌توان تأمین مالی را امر «ضرورتاً بایسته» برای بقای تروریسم دانست فارغ از اینکه منشأ آن مشروع

۱۴. بانک مرکزی پس از مدت‌ها سکوت، طی اطلاعیه‌ای در دوم اردیبهشت ۱۳۹۷ به‌کارگیری ابزار *بیت‌کوین* و سایر ارزهای مجازی را در تمام مراکز پولی و مالی کشور ممنوع اعلام کرد. متعاقب آن چند تن از مدیران این نهاد در مصاحبه‌های مختلفی بر لزوم استفاده از ارزهای دیجیتال (که اصطلاحی اشتباه برای ارزهای مجازی است) در کشور تأکید و در نهایت در هفتم بهمن ۱۳۹۷ بانک مرکزی پیش‌نویسی تحت عنوان «الزامات و ضوابط حوزه رمزارزها» منتشر و طی آن استفاده از این ارزها را برای مؤسسات مالی و بانکی تحت شرایطی مجاز اعلام کرد. لازم به ذکر است که پیش‌نویس مذکور نیز در موارد متعددی تناقضات فاحشی دارد.

15. Schneider, Friedrich, "Macroeconomics: The Financial Flows of Islamic Terrorism". In: Masciandaro D., (ed.) *Global Financial Crime: Terrorism, Money Laundering and Offshore Center*, Routledge, 2004, p. 120.

است یا نامشروع. در مواردی که منشأ عواید گروه تروریستی فعالیت‌های مجرمانه باشد، حوزه اشتراک پولشویی و تأمین مالی گسترش بیشتری می‌یابد و گروه تروریستی ناچار است برای انتقال مخفیانه وجوه از منبع به دریافت‌کننده، هویت واقعی هر دو طرف(فرستنده و گیرنده) را نیز پنهان کند.[۱۶]

در مجموع، پولشویی با پاکسازی ردّ پول آغاز و با مشروع‌سازی آن پایان می‌یابد در حالی که تأمین مالی تروریسم با کسب پول آغاز و با توزیع آن پایان می‌پذیرد. به‌رغم تفاوت در اهداف نهایی، وجه مشترک پولشویی و تأمین مالی تروریسم، دغدغه آن‌ها در پنهان‌کردن منبع پول است و همین است که مهارت‌های عامل پولشویی، ابزاری ضروری برای تروریست‌ها در جهت پنهان‌نگه‌داشتن جریان مالی در کنار حفظ منابع کسب این ثروت شده است.[۱۷] در نتیجه ابزارهای مبارزه با پولشویی از اهمیت ویژه‌ای برای سرکوب تأمین مالی تروریسم برخوردارند؛ هرچند همان طور که پیش‌تر عنوان شد، قسمت مهمی از تأمین مالی تروریسم، منشأ مجرمانه ندارد و لذا در همه حالات نمی‌توان با ابزارهای ضدپولشویی با آن مقابله کرد و به تلاش و ابزارهایی فراتر از آن نیاز است.

۲. ارزهای مجازی

در واقع هیچ تعریف جهان‌شمولی از «ارز مجازی» وجود ندارد و اصولاً بسیاری از کشورها بر سر استفاده از عنوان «ارز» نیز اختلاف دارند و برخی از آن‌ها در عوض از عبارت «دارایی‌های رمزی» استفاده می‌کنند.[۱۸] با این حال، برای پیشبرد بحث و امکان انطباق مقررات ضدپولشویی، ناگزیر باید ارزهای مجازی را تعریف کرد که از مقبولیت عام‌تری برخوردارند.

۲ـ۱. تعریف و دسته‌بندی کلی ارزهای مجازی

در گام نخست می‌توان ارزهای مجازی را «سامانه ارزی که از رمزنگاری برای انتقال امن و مبادله رمزهای دیجیتالی در یک بستر توزیع شده و غیرمتمرکز فعالیت می‌کند»[۱۹] تعریف کرد. اما به نظر می‌رسد برای نزدیک‌شدن به رویکردی که مبنای قواعد ضدپولشویی در این حوزه است ضرورت دارد تعاریفی رسمی‌تر را برگزید. شبکه اقدام علیه جرایم مالی[۲۰](Fin CEN) ایالات متحده این ارزها را با

16. Gunaratna, Rohan, *Inside Al Qaeda: Global Network of Terror*, Columbia University Press; First Printing Edition, 2002, pp. 88-89.

17. Kimberley L., Thachuk, "Terrorism's Financial Lifeline: Can It Be Severed?", *Strategic Forum, Institute for National Strategic Studies*, 2002, National Defense University, no. 191. retrieved from: https://www.hsdl.org/?view&did=515. (visited: 15/10/2018).

۱۸. مانند آلمان و فرانسه. ن.ک:

https://www.politico.eu/wp-%20content/%20uploads/2018/02/G20-Letter-on-crypto-assets-tokens.pdf

19. Dourado, Eli and Brito, Jerry, "Cryptocurrency", at: *The New Palgrave Dictionary of Economics*, Palgrave Macmillan, 2014, Number of Entry: 196. retrieved from: https://coincenter.org/entry/the-new-palgrave-dictionary-of-economics-cryptocurrency(visited:08/10/2018).

20. Financial Crimes Enforcement Network

مؤلفه‌های کارکردی (و نه ماهیت) آن‌ها تعریف کرده است: «ارز مجازی در برخی شرایط همانند ارز واقعی عمل می‌کند اما فاقد تمام ویژگی‌های ارز واقعی است؛ به‌ویژه آنکه ارز مجازی فاقد صلاحیت قانونی در نظام‌های حقوقی است».[۲۱] اما اتحادیه اروپا (EU) در تعریف خود، تعریف کارگروه را ملاک قرار داده است که بیان می‌دارد: «ارز مجازی جلوه دیجیتالی یک ارزش[۲۲] است که توسط بانک مرکزی یا مقام صلاحیت‌دار صادر و تضمین نشده، الزاماً به ارز قانونی شناخته‌شده وابسته نبوده و واجد وضعیت حقوقی ارز یا پول نیست اما به‌عنوان واسطه مبادله که قابلیت انتقال، ذخیره و تجارت در فضای الکترونیکی را دارد، توسط اشخاص حقیقی و حقوقی پذیرفته شده است».[۲۳]

در دسته‌بندی کلی می‌توان ارزهای مجازی را به دو دسته کلی تقسیم کرد:

الف) ارزهای مجازی متمرکز: این ارزها برخلاف ارزرمزها دارای مدیریتی متمرکز برای ایجاد ارزها (معادل ضرب سکه در پول واقعی) است که عموماً همانند واحد معینی از یک ارز مشخص (مانند ریال) عمل کرده و ابزار پرداخت در محیط برخط محدود، مثلاً روش پرداخت جایگزین برای پرداخت‌های درون شبکه‌ای و بازی‌های تحت شبکه است. نمونه این نوع ارزها، *وب مانی*،[۲۴] رابط خدمات پرداخت متعلق به روسیه و *پرفکت مانی*،[۲۵] رابط خدمات پرداخت متعلق به کشور پاناما است.[۲۶]

ب) ارزهای مجازی نامتمرکز: این دسته از ارزهای مجازی به مرکز صادرکننده یا مقام صلاحیت‌دار برای صدور مجوز ایجاد و تراکنش در درون شبکه نیازی ندارند. این نوع ارزها به «ارزرمزها» مشهورند که شناخته‌ترین مصداق آن *بیت‌کوین*[۲۷] است[۲۸] و از این پس در این مقاله هر جا به ارزهای مجازی اشاره می‌شود مقصود دسته اخیر است زیرا چنانچه در ادامه توضیح داده خواهد شد، ویژگی‌های خاص این نوع ارزهاست که امکان پولشویی را بیشتر فراهم می‌آورد.

21. Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, Fin. Crimes Enforcement Network, FIN-2014-R011, 2014, retrieved from: https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/request-administrative-ruling-application-0 (visited: 14/09/2018).

22. Value

23. Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FATF Report, June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. (visited: 10/10/2018).

24. Web Money

25. Perfect Money

26. European Central Bank, "Virtual Currency Schemes – A Further Analysis", 2015, p. 10. retrieved from: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (visited: 16/11/2018).

27. Bitcoin

28. Plessis, Paul du, "The Nature of Decentralized Virtual Currencies: Benefits, Risks and Regulations", *World Trade Institute*, 2014, p. 13. retrieved from: https://www.wti.org/media/filer_public/30/f0/30f00e05-e848-4c82-90fe-7e7842a7dbe4/paul_du_plessis_masters_thesis.pdf (visited:16/10/2018).

۲ـ۲. درک عملکرد ارزهای مجازی

همان طور که عنوان شد، ارزهای مجازی بر بستری غیرمتمرکز و به شکلی گمنام عمل می‌کنند. هیچ دولتی ارزش آن‌ها را تعیین نمی‌کند بلکه ارزش نهایی آن‌ها را عرضه و تقاضای کاربران تعیین می‌کند.[۲۹]

تراکنش ارزهای مجازی از زمانی آغاز می‌شود که فروشنده، مقدار مشخصی از ارز خود را از کیف پول دیجیتال[۳۰] خود و از طریق بسترهای الکترونیک خاصی به نشانی رمزداری که خریدار به‌عنوان کیف دیجیتال خود معرفی کرده است ارسال می‌کند.[۳۱] شبکه‌ای که این تراکنش بر بستر آن انجام می‌شود (عمدتاً *بلاکچین*)[۳۲] متوجه این نقل و انتقال شده و آن را ثبت می‌کند.

تراکنش معمول ارز مجازی ازجمله تراکنش‌های شامل پولشویی تقریباً پنج مرحله دارد: ۱ـ ارسال‌کننده تراکنشی را در شبکه ایجاد می‌کند که در اینجا همان پول کثیف است. ۲ـ دریافت‌کننده ارز که آن را می‌پذیرد که در اینجا شوینده پول است که به فرستنده کمک می‌کند تا منشأ پول کثیف را پنهان کند. ۳ـ استخراج‌کنندگان[۳۳] ارزهای مجازی که با کامل‌کردن بلوک‌های شبکه بستر تراکنش به‌عنوان تأییدکنندگان و پردازنده‌ها عمل می‌کنند و گاه ممکن است اندک مبلغی نیز از این بابت دریافت کنند. ۴ـ تیم اصلی توسعه‌دهنده ارز مجازی که در صورت ضرورت، کدهای پایه ارز مجازی را به‌روزرسانی می‌کنند و ۵ـ تبدیل ارزهای دیجیتال که تبدیل ارز مجازی به سایر ارزها و بالعکس را تسهیل می‌کند.

۲ـ۳. قانونمندکردن ارزهای مجازی؛ مطالعه ایالات متحده و اتحادیه اروپا

ارزهای مجازی به این دلیل که به‌عنوان ابزار خرید کالا، خدمات برخط، واحد سنجش و ابزار ذخیره ارزش نیز به کار می‌رود، دارای همه ویژگی‌های اقتصادی پول است. از همین رو برخی

---

29. "FAQ", Bitcoin Wiki, https://en.bitcoin.it/wiki/FAQ.

۳۰. کیف پول دیجیتال، یا کیف پول الکترونیکی، یک برنامه نرم‌افزاری است که به کاربر اجازه می‌دهد تا هم پول رایج و هم رمز ارزها را به‌صورت آنلاین ذخیره کند. پول‌های ذخیره‌شده در کیف پول الکترونیکی می‌تواند برای معاملات و خرید و فروش استفاده شود. برگرفته از:

https://payment24.ir/blog/everything-need-know-electronic-wallets/.

31. The user's addresses, transactions, preferences, etc. "Wallet", Bitcoin Wiki, https://en.bitcoin.it/wiki/Wallet.

۳۲. *بلاکچین* زنجیره بلوک‌هایی است برای ثبت اطلاعات(دفتر کل) تراکنش‌ها که میان تمام کاربران به اشتراک گذاشته می‌شود و به دلیل رمزنگاری عملاً امکان تغییر و دستکاری در آن غیرممکن است. ن.ک:

Kuo Chuen, David Lee, *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, Elsevier Inc., 2015, p. 49.

۳۳. استخراج ارز مجازی به معنای حل معماهای ریاضی است که به‌صورت خودکار ایجاد شده‌اند و حل هر قسمت از این معما توسط کاربر به منزله پیشروی در فرایند تراکنش‌های آن‌هاست. ن.ک:

Barski, Conrad and Wilmer, Chris, *Bitcoin for the Befuddled*, No Starch Press, 2015, p. 4.

معتقدند باید آن را همانند پول دانست.[۳۴] در مقابل، برخی دیگر بر کالابودن آن تأکید دارند.[۳۵] کمیسیون معاملات آتی کالای ایالات متحده(CFTC)[۳۶] نیز به علت تفسیر موسع خود از کالا، نظر اخیر را پذیرفته است.[۳۷] اما اشکال شناسایی ارزهای مجازی به‌عنوان کالا آن است که دیگر نمی‌توان مقررات ضدپولشویی را علیه آن‌ها اعمال کرد.

شبکه اقدام علیه جرایم مالی ایالات متحده (FinCEN) در سال ۲۰۱۳ نخستین گزارش خود را در خصوص ارزهای مجازی ارایه و اعلام کرد که مبادلات و فراهم‌آورندگان ارزهای مجازی مشمول قانون اسرار بانکی (BSA) هستند و باید خود را به‌عنوان تجارت خدمات مالی ثبت کنند.[۳۸] هدف از این اقدام، نظارت بر تراکنش‌های این ارزها و ممانعت از استفاده نامشروع از آن‌ها به‌ویژه در امر پولشویی بود. این گزارش‌ها در سال‌های بعد نیز منتشر شد. مقامات این نهاد در آخرین گزارش خود به سال ۲۰۱۸ اعلام کردند که به‌زودی طرحی جامع در خصوص ارزهای مجازی به کنگره ارایه خواهند کرد.[۳۹] همان طور که پیداست تا کنون مقررات جامعی در خصوص ایجاد، استفاده و مبادله ارزهای مجازی در ایالات متحده تصویب نشده و تنها برخی حوزه‌ها همچون مالیات، مقررات سرمایه‌گذاری فراساحلی و پیشگیری از به‌کارگیری ارزهای مجازی در معاملات غیرقانونی و آن‌هم در اغلب موارد توسط احکام دادگاه‌های فدرال تا حدودی مقرره‌هایی در این خصوص فراهم آورده‌اند.

در اتحادیه اروپا نیز در سطح منطقه‌ای هیچ مقررات جامعی در خصوص ارزهای مجازی وجود ندارد. در برخی دولت‌های عضو، مبادلات این ارزها قانونمند شده است. از این میان می‌توان به آلمان، فرانسه و ایتالیا اشاره کرد.[۴۰] تنها نقطه‌عطف در سطح اتحادیه اروپا را می‌توان مقرره پنجم اتحادیه اروپا (AML5) در ۲۰۱۸ دانست که تبدیل ارزهای مجازی به ارزهای واقعی را تحت مقررات مقابله با پولشویی قرار داد و بدین ترتیب، قاعده «شناسایی مشتری»[۴۱] بر این‌گونه مبادلات

34. Pacy, Eric P., "Tales from the Cryptocurrency: On Bitcoin, Square Pegs, and Round Holes", *NEW ENG. L. REV*. vol. 121, 2014, p. 49.

35. Mishkin, Fredrick S.**,** *The Economics of Money Banking and Financial Markets*, Pearson Education, 4th Edition, 2004, p. 44.

36. Commodity Futures Trading Commission

37. Customer Advisory: Understand the Risks of Virtual Currency Trading, p. 1, retrieved from: https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory_urvct121517.pdf (visited:10/10/2018).

38. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, March 18, 2013. retrieved from: https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (visited:10/10/2018).

39. Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference, August 09, 2018. retrieved from: https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block (visited:10/10/2018)

40. Bryanov, Kirill, "France and Germany: How Regulatory Traditions in Two Countries Could Affect EU Legislation", MAR 30, 2018. retrieved from: https://cointelegraph.com/news/france-and-germany-how-regulatory-traditions-in-two-countries-could-affect-eu-legislation(visited:13/10/2018)

41. Know Your Customer: KYC

حاکم خواهد بود.[۴۲]

۳. ویژگی‌های ریسک‌پذیری ارزهای مجازی در پولشویی و تأمین مالی تروریسم

اکنون باید دید کدام‌یک از ویژگی‌های ارزهای مجازی، مجرمین و تروریست‌ها را برای استفاده از آن‌ها به‌عنوان ابزار پولشویی ترغیب می‌کند.

۳ـ۱. ناشناختگی و شبه ناشناختگی

بسیاری از رسانه‌های خبری بر این نکته پافشاری دارند که ارزهای مجازی ویژگی «ناشناختگی» و «غیرقابل ردیابی» بودن دارند، اما این امر تاحدودی اغراق‌آمیز بوده و با بی‌دقتی همراه است. شاید بهترین عبارت برای ارزرمزهایی چون *بیت کوین*، «شبه ناشناختگی»[۴۳] است زیرا کاربران این نوع ارزها با نشانی‌های حرفی ـ عددی[۴۴] و کیف پول دیجیتال خود در *بلاکچین* حاضر می‌شوند در حالی‌که هویت واقعی کاربر در *بلاکچین* مشخص نیست اما اطلاعات مربوط به تراکنش‌ها ازجمله تاریخ، ارزش و نشانی رمزارزهای معامله‌گران به‌صورت عمومی ثبت می‌شود. به‌علاوه از آنجا که *بلاکچین* به ترتیب زمانی اقدام به ثبت تراکنش‌ها می‌کند این امکان وجود دارد که تصویری نسبتاً قابل اعتماد از حرکت ارزرمزها به دست آورد.

بنابراین هنگامی که هویت شخص حقیقی یا حقوقی دارنده نشانی عمومی ارز مجازی مشخص شود می‌توان حجم انبوهی از اطلاعات را در خصوص اقدامات وی در شبکه کسب کرد. امروزه برخی شرکت‌های خصوصی در افشای تراکنش‌های این ارزها و توسعه ابزارهای تحلیل فعالیت‌های غیرقانونی آن‌ها به‌صورت تخصصی فعالیت می‌کنند.[۴۵]

اما همین میزان از ناشناختگی یا «شبه‌ناشناختگی» نیز برای مجرمین و بخصوص تروریست‌هایی که از ارزهای مجازی استفاده می‌کنند، کاراست. در هرحال ارسال نشانی مثلاً *بیت‌کوین* به یک رسانه یا شبکه عمومی در قالب پیام صوتی و تصویری به‌مراتب بهتر و سودمندتر از تبلیغ برخط شماره حساب بانکی است. با این حال، امکان ردیابی ارزهای مجازی تا حدود زیادی فعالیت

42. Amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, 2018.retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN (visited:13/10/2018).

43. Pseudonymous

44. Alphanumeric

45. Redman, Jamie, "Chainalysis Raises $16Mn – Plans to Monitor Multiple Blockchains", *Bitcoin.com*, 6 April, 2018, retrieved from: https://news.bitcoin.com/chainalysis-raises-16mn-plans-to-monitor-multiple-blockchains. (visited:10/11/2018).

مجرمان را محدود می‌کند.[۴۶]

علی‌رغم آنچه در خصوص امکان ردیابی ارزهای مجازی گفته شد، روش‌های متعددی نیز برای حفظ ناشناختگی یا اصطلاحاً «لایه‌بندی»[۴۷] وجود دارد. یکی از این روش‌ها استفاده از خدمات «مخلوط‌کن‌ها»[۴۸] یا «پشتک‌زن‌ها»[۴۹]ست که ارزهای مجازی کاربران متعدد را جمع‌آوری و بازتوزیع و به این ترتیب مسیر تراکنش‌ها را پنهان می‌کنند. در این راستا سایت‌هایی چون *کوین جوین*[۵۰] و *دارک والت*،[۵۱] روش‌های ترکیبی چندگانه‌ای به‌کار می‌برند. هرچند بسیاری از اقدامات درآمیختن ارزها غیرقانونی نیست، تحقیقی جدید نشان می‌دهد که بسیاری از این خدمات عملاً در جهت پاک‌سازی پول‌های غیرقانونی است.[۵۲] در اواسط سال ۲۰۱۴ افراد وابسته به داعش از فناوری درهم‌آمیزی *بیت‌کوین* برای پنهان‌کردن مبادلات و تراکنش‌ها استفاده کردند.[۵۳]

در سال‌های اخیر، نوآوری‌هایی در به‌کارگیری ارزهای جایگزین[۵۴] با تأکید بر حفظ بیشتر حریم شخصی ظهور یافته‌اند که به‌مراتب بیشتر از *بیت‌کوین* از ویژگی ناشناختگی بهره می‌برند که عموماً از آن‌ها تحت عنوان «سکه‌های حریم خصوصی»[۵۵] یاد می‌کنند. هرچند این ارزها نیز همچون *بیت کوین* دارای منبع باز[۵۶] بوده و بر بستر *بلاکچین* عمومی قرار دارند، جزئیات شناسایی آن‌ها دیگر عمومی نیست. از آن میان می‌توان به *مونرو*[۵۷] *دش*[۵۸] و *زدکش*[۵۹] اشاره کرد. مطالعات متعددی در

46. Berg, Svenja and McCarthy, Killian J., "The Economics of ISIS — A Case of Theft or Money Laundering?", *Freedom from Fear*, vol. 11, 2016, p. 84. Retrieved from: https://www.un-ilibrary.org/human-rights-and-refugees/the-economics-of-isis-a-case-of-theft-or-money-laundering_c855eaf4-en (visited:08/10/2018).

47. Layering

48. Mixers

49. Tumblers

50. CoinJoin

51. DarkWallet

52. Fanusie, Yaya J. and Robinson, Tom, "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services", *Foundation for Defense of Democracies and Elliptic*, 12 January, 2018, p. 7. Retrieved from: http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf. (visited:03/10/2018).

53. Higgins, Stan, 'ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide,' CoinDesk, 7 July 2014. Retrieved from: https://www.coindesk.com/isis-bitcoin-donations-fund-jihadist-movements/. (visited:08/10/2018)

۵۴. ارزهای جایگزین یا Altcoins بعد از موفقیت *بیت‌کوین* و با هدف ارتقای عملکرد نسبت به این ارز پدیدار شدند. ن.ک: https://www.investopedia.com/terms/a/altcoin.asp

55. Privacy coins

56. Open source

57. Monero

58. Dash

59. Zcash

سال‌های اخیر حکایت از استفاده گسترده از سکه‌های حریم خصوصی در اعمال مجرمانه دارد.[۶۰]

در هر صورت هر روز بر تعداد و قابلیت این سکه‌های حریم خصوصی افزوده می‌شود و قوانین ضدپولشویی را با چالش‌های جدیدتری مواجه می‌کند. به‌عنوان مثال، اصلاحیه پنجم اتحادیه اروپا تنها بر آن دسته از ارزهای مجازی قابل اعمال است که ارز مجازی را به پول واقعی تبدیل می‌کند و صراحتاً شامل مبادله یک ارز مجازی با نوع دیگری از ارز مجازی نمی‌شود؛ واقعیتی که کار را برای کاربران جهت تبدیل *بیت‌کوین* به سکه‌های حریم خصوصی بدون اینکه شامل قاعده «شناسایی مشتری» یا سایر قواعد رصد تراکنش‌های ارزهای مجازی شوند به‌مراتب ساده‌تر می‌کند.[۶۱]

۳ـ۲. شبکه تاریک و پیام‌رسان‌ها

علاوه بر ویژگی ناشناختگی در ارزهای مجازی، آنچه ریسک پولشویی را بسیار بالاتر می‌برد، استفاده از این ارزها با سایر فناوری‌های ناشناسایی همچون شبکه تاریک[۶۲] است. شبکه تاریک زیرمجموعه *دیپ وب* یا وب عمیق[۶۳] و مجموعه‌ای از هزاران وب سایت عرضه خدمات و محصولات غیرقانونی است که از خدماتی همچون *پروتکل تور*[۶۴] برای پنهان‌کردن نشانی‌های *آی پی* و رمزنگاری ارتباطات استفاده می‌کند.[۶۵] پرداخت‌ها در شبکه تاریک عموماً از طریق ارزهای مجازی صورت می‌گیرد.

شبکه تاریک، خدماتی را برای دسترسی به کالاهایی که معمولاً تروریست‌های استفاده می‌کنند، عرضه می‌دارند. واحد اطلاعات مالی بلژیک در گزارش سال ۲۰۱۶ خود اعلام کرد که ارزهای مجازی به‌صورت گسترده‌ای برای پرداخت تجارت غیرقانونی پنهان در وب تاریک به کار می‌رود که از آن جمله می‌توان به خرید اسناد جعلی هویت و بلیط خطوط هوایی اشاره کرد.[۶۶]

60. Europol, *Internet Organised Threat Assessment (IOCTA Report 2017)*, 2017, p. 13. Retrieved from: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 (visited:08/10/2018)

61. Amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, 2018.retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN (visited:13/10/2018)

62. Dark Web

۶۳. برخلاف آنچه عموماً این دو اصطلاح را یکسان می‌دانند، در واقع شبکه عمیق (deep web) صرفاً قسمتی از اینترنت است که از طریق موتورهای جستجوی معمول همچون *گوگل* و *یاهو* قابل دسترسی نیست اما شامل وب‌سایت‌های عادی و غیرمجرمانه متعددی نیز هست.

64. Tor Protocol

65. Torpey, Kyle, "AlphaBay Comments on Bitcoin Congestion, Monero Adoption and Zcash Possibilities," *Bitcoin Magazine*, 21 December 2016. Retrieved from: https://bitcoinmagazine.com/articles/alphabay-comments-on-bitcoin-congestion-monero-adoption-and-zcash-possibilities-1482345512/. (visited:08/12/2018)

66. CTIF-CFI, *23rd Annual Report*, Belgian Financial Intelligence Processing Unit (CTIF-CFI), 2016, p. 41. Retrieved from: http://www.ctif-cfi.be/website/images/EN/annual_report/ar2016en.pdf. (visited:08/10/2018).

گزارش اخیر یکی از مراکز نظارتی نشان می‌دهد که امروزه افراط‌گراهای غیرسازمان‌یافته در غرب از طریق شبکه تاریک به‌مراتب سهل‌تر از گذشته به سلاح مواد منفجره و تجهیزات مشابه دیگر دسترسی دارند.[۶۷] در واقع شبکه تاریک موانع تاریخی، جغرافیایی را که پیش‌تر محدویت‌های جدی بر سر راه خرید اسلحه و مواد منفجره ایجاد کرده بود به اندازه چند حرکت *موس* و اشاره بر صفحه *مانیتور* کاهش داده است. اما از سوی دیگر نباید در این امر مبالغه کرد زیرا هرچند خرید این ادوات و تجهیزات تسهیل شده، همچنان مانع بزرگی به نام تحویل فیزیکی این مواد وجود دارد که همچنان وسعت تجارت واقعی آن‌ها را محدود نگه داشته است.

تمام استفاده مجرمین/تروریست‌ها از شبکه تاریک فقط خرید کالاها و پولشویی نیست و به‌ویژه تروریست‌ها از این فضای پنهانی برای تبلیغ عقاید خویش و جذب نیرو نیز استفاده می‌کنند چنان‌که تحقیق اخیر در یکی از دانشگاه‌های انگلستان از گرایش بسیار افراد دارای سوءسابقه جنایی در اروپا به اقدامات تروریستی با انگیزه مذهبی «جهاد» حکایت دارد.[۶۸]

اپلیکیشن‌های پیام‌رسان و رسانه‌های جمعی دیگر، کانال‌هایی هستند که تروریست‌ها و مجرمین سازمان‌یافته می‌توانند به‌واسطه آن‌ها مخفی بمانند. در پویش‌های جمع‌آوری کمک گروه‌های افراطی و تروریستی که تا به امروز شناسایی شده‌اند، عموماً کمک‌های مالی مستقیماً از طریق *توییتر* و *فیسبوک* یا پیام‌رسان‌های رمزنگاری‌شده‌ای همچون تلگرام صورت گرفته است. فواید بالقوه اتخاذ این رویکرد توسط تروریست‌ها بسیار روشن است: پویش‌های جمع‌آوری کمک به هواداران اجازه می‌دهد که از «هدف‌شان حمایت» کنند بدون آنکه از خانه بیرون بزنند، ضمن اینکه یک لایه اضافی ناشناختگی نیز از ارتباطات‌شان حفاظت می‌کند.[۶۹]

۳ـ۳. انتقال فرامرزی از طریق شبکه نظیر به نظیر و قابلیت جابه‌جایی

دیگر ویژگی ارزهای مجازی که برای مجرمین و تروریست‌ها جذابیت دارد، امکان انتقال فرامرزی آن‌ها بدون توسل به واسطه‌های قانونی است. هرچند باید اذعان کرد که ارزهای مجازی قابلیت انتقال در حجم وسیع و بسیار سریع را ندارند، ابزاری مؤثر برای انتقال ارزش از طریق فناوری نظیر

67. Maxey, Levi, "Terrorists Stalk the Dark Web for Deadlier Weaponry", *The Cipher Brief*, 17 January, 2018. Retrieved from: https://www.thecipherbrief.com/terrorists-stalk-dark-web-deadlier-weaponry. (visited:08/10/2018).

68. Neumann, Richard and Basra, Rajan, "Crime as Jihad: Developments in the Crime-Terror Nexus in Europe, CTC Sentinel", October 2017, vol. 10,issue 9, *Combatting Terrorism Center*, Retrieved from: https://ctc.usma.edu/crime-as-jihad-developments-in-the-crime-terror-nexus-in-europe/. (visited:19/10/2018).

69. Authors: Tom Keatinge, David Carlisle, Florence Keen; Responsible Research Administrator: Kristiina Milt, "Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses", *Policy Department for Citizens' Rights and Constitutional Affairs*, European Parliament, 2018, p. 38. http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

به نظیر به‌صورت فرامرزی هستند. این قابلیت به‌ویژه برای باج‌گیران اینترنتی که در قبال اعاده اطلاعات کاربران مورد حمله، اخاذی می‌کنند جذابیت خاصی دارد زیرا می‌توانند از هر نقطه جهان مبالغ مورد نظر خود را بدون نیاز به ارایه اطلاعات حساب بانکی دریافت کنند.

علی‌رغم جستجوها در میان منابع متعدد، تا کنون هیچ گزارشی مبنی بر استفاده تروریست‌ها از شبکه نظیر به نظیر برای انتقال ارزهای مجازی دریافت نشده است. اما این به معنای نبود این امر نیست. شاید بتوان یکی از علل این امر را فقدان امکان تبدیل ارزهای مجازی به ارزهای ملموس در مناطق مورد مخاصمه و درگیری تروریست‌ها دانست. همان طور که محققین مرکز امنیت امریکای نوین (CNAS) اعلام کرده‌اند: «اگر امکان انتقال و تبدیل ارزهای مجازی آسان‌تر شود ... و اگر گروه‌های تروریستی در مکان‌هایی همچون زیر صحرای آفریقا، یمن و شاخ آفریقا به زیرساخت‌های فنی لازم برای حمایت از فعالیت ارزهای مجازی دست یابند، با تهدید بالفعل مواجه خواهیم بود».[۷۰]

ارزهای مجازی قابلیت جابه‌جایی سریع و راحت را دارند و مشکل محدودیت جابه‌جایی حمل پول نقد را ندارند. شخص می‌تواند ارزهای مجازی خود را به‌راحتی با به‌همراه‌داشتن برگه یا کیف سخت‌افزاری یا حتی ساده‌تر، با همراه‌داشتن اپلیکیشن کیف نرم‌افزاری در گوشی، تبلت یا سایر وسایل قابل حمل از مرز عبور دهد. کارت‌های اعتباری ارزهای مجازی می‌توانند همانند ابزار مشابه ایفای نقش کنند زیرا می‌توان آن‌ها را به‌صورت برخط با مقدار دلخواه ارزهای مجازی شارژ و از مکانی به مکان دیگر انتقال داد. در آوریل ۲۰۱۸ مقامات اسپانیایی عملیاتی را علیه یک شبکه جرایم سایبری صورت دادند که از کارت‌های اعتباری *بیت‌کوین* برای پولشویی درآمدهای خود استفاده می‌کرد.[۷۱]

۳ـ۴. غیرمتمرکزبودن

طبیعی است که مجرمین و تروریست‌ها تمایل بیشتری به استفاده از ارزهای غیرمتمرکز داشته باشند. این نوع ارزها که منبع باز و رابط‌های غیرمتمرکز دارند ارزهای «بدون مجوز» نام دارند زیرا دسترسی به آن‌ها محدودیتی ندارد. هیچ مرکز صلاحیت‌دار واحد برای ممانعت از دسترسی به شبکه این نوع ارزها وجود ندارد. نمی‌توان این شبکه‌ها را تعلیق، مجازات یا همانند سامانه‌های متمرکز کاملاً مسدود کرد.[۷۲]

70. Zachary Goldman, Ellie Maruyama, Elizabeth Rosenberg, Eduardo Saravalle, Julia Solomon-Strauss, "Terrorist Use of Virtual Currencies: Containing the Potential Threat", *Center for New American Security*, Washington, 3 May, 2017, Retrieved from: https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies. (visited:14/11/2018).

71. Europol, "Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain", *Europol Press Release*, 26 March, 2018, Retrieved from: https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain. (visited:03/10/2018).

72. Decentralization in Bitcoin and Ethereum, retrieved from: http://hackingdistributed.com/ 2018/01/15/ decentralization-bitcoin-ethereum/ (visited:10/10/2018).

هرچند شبکه‌های ارزهای مجازی از نظام غیرمتمرکز برخوردارند، واسطهای آن‌ها عمدتاً از شبکه‌ای متمرکز استفاده می‌کنند. این واسطها کار مبادله ارزهای مجازی و کیف پول را فراهم می‌کنند. در حالی که دو کاربر می‌توانند به‌آسانی و از طریق شبکه نظیر به نظیر در درون شبکه *بیت‌کوین*، نقل و انتقال این نوع ارز را انجام دهند، ثابت شده که انتقال میان شبکه *بیت‌کوین* به سایر ارزهای مجازی یا واقعی، اغلب با مشکلاتی همراه است که بدون کمک شخص ثالث قابل حل نیست. واسطه‌های مبادلاتی همچون *بینانس*[۷۳] و *کوین بیس*[۷۴] این خلأ را پر می‌کنند.

واسطها می‌توانند همانند بانک‌ها دسترسی کاربر را به خدمات محدود کنند. در خلال ناآرامی‌های *شارلوت ویل* امریکا، انتقال ارز به شبکه *دیلی استورمر*[۷۵] توسط *کوین بیس* بسته شد. این واسطه در توضیح علت اقدام خود، آن را به دلیل «جلوگیری از سوءاستفاده حساب کاربری، تقلب در ایجاد ارز، تهدید یا ترویج خشونت علیه دیگران» اعلام و عنوان کرد «این سیاست محدودسازی را تا آرامش اوضاع» ادامه خواهد داد.[۷۶]

این جنبه متمرکز از یک زیست‌بوم غیرمتمرکز، «گلوگاهی» طبیعی برای وضع مقررات و اعمال نظارت فراهم می‌آورد. در واقع مشکل تبدیل ارز مجازی به ارز واقعی مشکلاتی را به‌طور گسترده برای مجرمین فراهم آورده است. واسطه‌های تبدیلی چون *کوین بیس* معمولاً محدودیت‌هایی برای فعالیت کاربران ایجاد می‌کنند، مثل محدودیت‌هایی برای میزان تراکنش در یک هفته یا ماه.[۷۷] بنابراین اگرچه عدم تمرکز و منبع باز ارزهای مجازی، تسهیل‌کنندهٔ اعمال غیرقانونی است، در عمل محدودیت‌های تبدیل این ارزها توانایی آن‌ها را تا حدود زیادی تعدیل می‌کند.

۴. رویکرد کارگروه ویژه اقدام مالی در قبال فناوری‌های نوین

از دهه ۱۹۹۰ و اوایل ۲۰۰۰ میلادی که کارگروه، توصیه‌های ضد پولشویی و تأمین مالی تروریسم را آغاز و تشدید کرده است تا کنون نوآوری‌های فناوری به‌شدت بخش مالی را تحت تأثیر خود قرار داده است. توسعه و همه‌گیری کاربرد اینترنت، رایانه‌های شخصی، تلفن‌های همراه و نرم‌افزارها و خدمات مربوطه، آثار بسیاری بر تعاملات اجتماعی ازجمله تجارت و مبادلات مالی داشته است.

در سال ۲۰۰۶ کارگروه با انتشار گزارشی در خصوص روش‌های نوین پرداخت، قدم در راه

73. Binance

74. Coinbase

75. Daily Stormer

76. Burns, Janet, "Cut Off from Big Fintech, White Nationalists Are Using Bitcoin to Raise Funds", *Forbes*, 3 January 2018, retrieved from:https://www.forbes.com/sites/janetwburns/2018/01/03/cut-off-from-big-fintech-white-supremacists-are-using-bitcoin-to-raise-funds/#49f5334633b3. (visited:10/12/2018).

77. Gilbert, David, "Criminals Are Racing to Cash Out Their Bitcoin. Here's How They're Doing It", *Vice*, 19 March 2018. retrieved from: https://news.vice.com/en_ca/article/7xdzqa/criminals-are-racing-to-cash-out-their-bitcoin-heres-how-theyre-doing-it (visited:12/11/2018).

درک این پیشرفت‌های فناورانه نهاد.[۷۸] این گزارش با اشاره به قابلیت‌های نوآوری‌های مالی همانند کارت‌های اعتباری و بسترهای پرداخت برخط و موبایلی، عنوان کرد که این نوآوری‌ها موجب تسریع در تراکنش‌های فرامرزی شده و در نتیجه ریسک‌های تأمین مالی تروریسم را افزایش داده است. متعاقب این ارزیابی در سال ۲۰۱۰ مطالعه دقیق‌تری توسط این نهاد صورت گرفت که عنوان می‌داشت اعضای کارگروه با رشد فزاینده تعداد موارد استفاده غیرقانونی از روش پرداخت‌های نوین مواجه‌اند. این گزارش به قابلیت فناوری‌های نوین در ایجاد امکان دسترسی‌های از راه دور که باعث ناشناختگی کاربران می‌شود اشاره می‌کند. از همه مهم‌تر اینکه گزارش سال ۲۰۱۰ کارگروه بر پیاده‌سازی ابزارهای پایگاه حفظ دامنه (CDD)[۷۹] در نقطه دسترسی کاربران که می‌تواند موجب کاهش ریسک‌های تأمین مالی شود تأکید دارد.[۸۰]

۴ـ۱. کارگروه ویژه اقدام مالی و ارزهای مجازی؛ اقدامات ابتدایی

در سال ۲۰۱۴ کارگروه با انتشار گزارشی تحت عنوان «ارزهای مجازی: تعاریف کلیدی و ریسک‌های بالقوه ضدپولشویی/ تأمین مالی تروریسم»[۸۱] به‌صورت خاص موضوع ارزهای مجازی را مدنظر قرار داد. این گزارش اشعار می‌دارد: «دسترسی جهانی به ارزهای مجازی موجب شده این ارزها در دنیای دیجیتال و خارج از اعمال نظر دولتی خاص به حیات خویش ادامه دهند».[۸۲] کارگروه در این گزارش، ارزرمزها را «به‌صورت ویژه آسیب‌رسان» به دلیل خطر ناشناختگی ارزیابی می‌کند زیرا شناخت مشخصات مشتری ازجمله نام و نشانی آن‌ها به دلیل عدم درج‌شان در نشانی کاربر ارز و همچنین به دلیل فقدان ارائه‌دهنده خدمات‌دهنده مرکزی که بر تراکنش‌ها نظارت داشته و آن‌ها را ثبت کند امکان‌پذیر نیست. مطابق ارزیابی کارگروه، به این ترتیب نه‌تنها شناسایی فعالیت مشکوک به‌مراتب سخت‌تر می‌شود، بلکه شناخت منبع آن نیز در قیاس با کارت‌های اعتباری و نقدی یا نظام‌های پرداختی چون *پی پال*[۸۳] و *وسترن یونیون*[۸۴] مبهم‌تر شده است.

78. Financial Action Task Force, *Report on New Payment Methods*, FATF Report, Paris, 13 October, 2006. retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Report on New Payment Methods.pdf. (visited:10/10/2018).

79. Conserved Domains Database

80. Financial Action Task Force, *Money Laundering Using New Payment Methods*, FATF Report, Paris, October 2010. Last visited on 25/09/2019 from: fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingusingnewpaymentmethods.html.

81. Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential* AML/CFT Risks, FATF Report, Paris, June 2014. retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. (visited:10/10/2018).

82. *Ibid.*, p. 10.

83. PayPal

84. Western Union

۴ـ۲. کارگروه ویژه اقدام مالی و ارزهای مجازی؛ اقدامات جدی‌تر

گزارش سال ۲۰۱۴ کارگروه، اندکی پس از دو قضیه پرسروصدا در خصوص استفاده از ارزهای مجازی در فعالیت‌های غیرقانونی منتشر شد. نخستین مورد قضیه *سیلک رود*[۸۵] بود. در این قضیه، یک وبسایت خرید و فروش کالاهای غیرقانونی همچون مواد مخدر و اعضای انسان و ارایه خدماتی چون گروگان‌گیری و آدم‌کشی بود که در شبکه تاریک فعالیت می‌کرد. مقامات ایالات متحده در سال ۲۰۱۴ و سه سال پس از فعالیت این وبسایت، بنیانگذار آن را دستگیر کرده و متوجه شدند که عمده تراکنش‌های این وبسایت غیرقانونی از طریق *بیت‌کوین* صورت می‌گرفت.[۸۶] این قضیه قابلیت فناوری‌های غیرمتمرکز فناوری‌های نوین را که باعث ظهور طیف جدیدی از بازار غیرقانونی می‌شود برجسته‌تر کرد.

دومین قضیه مربوط به *لیبرتی رزرو*،[۸۷] یک مرکز خدمات برخط انتقال پول ثبت‌شده در کاستاریکا بود که از ارز مجازی خاص خود به نام لیبرتی دلار[۸۸] استفاده می‌کرد و از این راه با حفظ ناشناختگی، امکان انتقال وجه میان کاربران را فراهم می‌کرد. مطابق اعلام مقامات امریکایی، این مرکز، تراکنش فعالان غیرقانونی شامل کلاهبرداران، مجرمان سایبری و قاچاقچیان مواد مخدر را تسهیل می‌کرد. جمع تراکنش‌های این مرکز تا هنگام تعطیلی به ۸ میلیارد دلار رسیده شده بود.[۸۹]

در سال ۲۰۱۵ کارگروه، گزارش مبسوط‌تری با عنوان «راهنمایی برای رویکرد مبتنی بر ریسک: ارزهای مجازی» ارایه کرد که راهنمایی عملی برای کشورها در خصوص چگونگی مدیریت مقابله با پولشویی و تأمین مالی تروریسم با استفاده از ارزهای مجازی بود.[۹۰] این راهنما شامل دو قاعده اصلی بود: الف) برای مدیریت ارزهای مجازی، رویکرد مبتنی بر ریسک امکان‌پذیر است و کشورها می‌توانند برای ارزیابی ریسک‌های ناشی از ارزهای مجازی توصیه‌های کاهش ریسک کارگروه را به‌کار ببندند. ب) ریسک ارزهای مجازی در مقطع قابلیت تبدیل‌شوندگی آن‌ها به سایر ارزهای باارزش به اوج خود می‌رسد و تمرکز عمده کشورهایی که رویکرد مبتنی بر ریسک را برای مواجهه با پولشویی/تأمین مالی اتخاذ می‌کنند باید بر نقطه تبدیل ارزهای مجازی و ارزهای واقعی قرار گیرد.[۹۱]

85. Silk Road

86. Greenberg, Andy, "End of the Silk Road: FBI Says It's Busted the Web's Biggest Anonymous Drug Market", *Forbes*, 2 October 2013. retrieved from: https://www.forbes.com/sites/andygreenberg/ 2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/ - 1190f0dc5b4f. (visited 10/11/2018).

87. Liberty Reserve

88. Liberty Dollar

89. United States Department of Justice, "Liberty Reserve Founder Sentenced to 20 Years for Laundering Hundreds of Millions of Dollars", *Justice News*, 6 May 2016. retrieved from: https://www.justice.gov/opa/pr/liberty-reserve-founder- sentenced-20-years-laundering-hundreds-millions-dollars. (visited 03/11/2018)

90. Financial Action Task Force, *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF Guidance, Paris, June 2015. retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. (visited:10/10/2018).

91. *Ibid.*, p. 19.

کارگروه همچنین مطالعاتی را نیز برای درک وسعت بالقوه و ماهیت ریسک‌های خاص تأمین مالی تروریسم مربوط به ارزهای مجازی در دستور کار قرار داده است. گزارش سال ۲۰۱۵ این نهاد تحت عنوان «ریسک‌های در حال ظهور تأمین مالی تروریسم» عنوان می‌دارد که کشورهای عضو به شکل فزاینده‌ای نگران استفاده از ارزهای مجازی توسط سازمان‌های تروریستی هستند و این امر مستند به وب‌سایت‌های مرتبط با سازمان‌های تروریستی است که به دنبال دریافت کمک‌ها به شکل *بیت‌کوین* یا فراهم‌آوردن شرایطی برای خرید سلاح با استفاده از *بیت‌کوین* هستند.[۹۲] در گزارش ماه ژانویه ۲۰۱۸ کارگروه به سایتی با محتوای تبلیغ اندیشه‌های داعش با مدیریتی نامعلوم اشاره شده که درخواست کمک از طریق *بیت‌کوین* بوده و برخی از *بیت‌کوین*‌های اهدایی را نیز برای تأمین هزینه خدمات میزبانی وب پرداخت کرده است.[۹۳]

در سال‌های اخیر، کارگروه فعالیت‌های خود را در خصوص برآورد و مدیریت ریسک‌های فناوری نوین مالی (FinTech) تا حدود زیادی تشدید کرده است. در طول سال‌های ۲۰۱۷ و ۲۰۱۸ این نهاد به‌طور مستمر توصیه‌ها و دستورالعمل‌هایی صادر کرده است.[۹۴] کارگروه تصریح کرده است که نوآوری‌های مسئولانه را در حوزه مالی ازجمله ارزهای مجازی که مطابق با استانداردهای کارگروه باشد تشویق می‌کند. این نهاد همچنین مایل است قابلیت‌های فناوری‌های نوین را برای ارتقای اجرای ابزارهای ضدپولشویی و تأمین مالی تروریسم به‌کار گیرد و در همین راستا در فوریه سال ۲۰۱۸ اعلام کرد به‌زودی در مقررات خود درباره ارزهای مجازی بازنگری خواهد داد.[۹۵]

نتیجه

ارزهای مجازی همانند سایر پدیده‌های نوظهور به‌رغم جنبه‌های بسیار مثبت و کارآمد به‌ویژه برای کشورهایی چون ایران،[۹۶] نیازمند تبیین عمومی ماهیت این ارزها، فرهنگ‌سازی صحیح و در نهایت، تعیین چارچوب‌های قانونی و نظارت دقیق هستند و نادیده‌گرفتن آن صرفاً موجب ایجاد فضای

92. Financial Action Task Force, *Emerging Terrorist Finance Risks*, FATF Report, October 2015, p. 36. retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf. (visited:10/10/2018).

93. Financial Action Task Force, *Financing of Terrorism for Recruitment Purposes*, FATF Report, January 2018, p. 20. retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf. (visited:10/10/2018).

94. Financial Action Task Force, "FATF FinTech and RegTech Initiative", website of the FATF: http://www.fatf-gafi.org/fintech-regtech/?hf=10&b=0&s=desc(fatf_releasedate). (visited:10/10/2018)

95. Financial Action Task Force, *FATF Report to G20 Finance Ministers and Central Bank Governors*, Paris, March 2018. retrieved from: http://www.fatf-gafi.org/media/fatf/documents/FATF-G20-FM-CBG-March-2018.pdf. (visited:10/10/2018).

۹۶. ازجمله این مزایا و با لحاظ ریسک‌های احتمالی می‌توان به کاهش هزینه انتشار پول واقعی، توسعه واسطه‌های مالی مبتنی بر اینترنت، کاهش نیاز به ارزهایی چون دلار در مبادلات بین‌المللی و تضعیف تحریم‌های بین‌المللی و افزایش میزان ذخایر ارزی کشور اشاره کرد.

آشفتگی مالی و در نهایت، فعالیت بی‌دغدغه مجرمین در آن خواهد بود.

ارزهای مجازی بر بستر غیرمتمرکز (ارزرمزها) در عمل (هرچند در قیاس با ارزهای واقعی به‌صورت محدود) فناوری مختل‌کننده نظام مالی سنتی را عرضه داشته‌اند که بسیاری از قواعد ضدپولشویی و تأمین مالی تروریسم را به چالش کشیده و ناتوانی آن‌ها را در عرصه دنیای مجازی برجسته ساخته‌اند. ارزهای مجازی روند عادی ارزهای مادی دارای پشتوانه دولتی را برهم زده‌اند و حقوق را در جایی نحیف گذاشته‌اند که نه هر سال بلکه هر ماه و شاید هر روز روشی نوین و ابزاری جدید را به منظور ناشناختگی بیشتر به‌کار می‌گیرد

شبکه ارزهای مجازی با برخورداری از ویژگی‌هایی چون ناشناختگی و غیرمتمرکزبودن، این امکان را برای مجرمین و تروریست‌ها فراهم می‌آورد که به پولشویی و تأمین مالی خود بپردازند. دو ویژگی مذکور به همراه دو ویژگی دیگر، یعنی عدم نظارت از سوی مرجع صلاحیت‌داری چون بانک‌های مرکزی (چنان‌که در ارزهای سنتی وجود دارد) و امکان انتقال آسان این ارزها به‌صورت فرامرزی بر بستر سامانه نظیر به نظیر، در کنار فقدان تشتت و گاه حتی تضاد قوانین کشورهای مختلف، دست مجرمان را بیشتر باز گذاشته است، هرچند تلاش برای ایجاد رویه‌های واحد از سوی نهادهای بین‌المللی چون کارگروه ویژه اقدام مالی می‌تواند تا حدودی این خلأ را پر کند.

ارزهای مجازی در عملکرد خود مشکلاتی نیز دارند، ازجمله اینکه ارزش این ارزها بسیار متغیر بوده و این امر ریسک اقدام را برای مجرمین بالا می‌برد، ضمن اینکه هزینه انتقال، هرچند در قیاس با ارزهای واقعی بسیار اندک است، بر مورد قبلی اضافه شده و هزینه پولشویی را بالا می‌برد. همان طور که اشاره شد، بزرگ‌ترین مشکل ارزهای مجازی برای مجرمین به هنگام تبدیل این ارزها به یکدیگر و تبدیل آن‌ها به ارزهای واقعی است.

کارگروه ویژه اقدام مالی در سال‌های اخیر و به‌طور خاص از سال ۲۰۱۴ بر موضوع استفاده از فناوری‌های نوین مالی و ارزهای مجازی در خصوص تأمین مالی تروریسم و پولشویی متمرکز شده و در طی این مدت نزدیک به هفت گزارش، دستورالعمل و راهنما در این خصوص صادر کرده است و هربار ضمن شناسایی شیوه‌های نوین در به‌کارگیری مجرمانه این ابزارهای مجازی، توصیه‌هایی در خصوص چگونگی مقابله با آن ارایه می‌کند.

به نظر می‌رسد با توجه به آنچه گفته شد، راه‌حل مبارزه با پولشویی و تأمین مالی تروریسم، حمایت از سامانه مالی داخلی کشورها، وضع قوانین دقیق و سخت‌گیرانهٔ داخلی، تمرکز بر گلوگاه تبدیل ارزهای مجازی به یکدیگر و تبدیل ارزهای مجازی به ارزهای واقعی به‌ویژه در مورد تأمین مالی تروریسم و در نهایت، اتخاذ رویه‌های یکسان در سطح بین‌المللی و همکاری‌های پلیسی و معاضدت‌های قضایی است زیرا قضایای متعدد نشان از آن دارد که مجرمین از خلأهای قضایی و قانونی بین‌المللی نهایت استفاده را برای ارتکاب اعمال غیرقانونی خود می‌برند.

منابع:

- Books

- Barski, Conrad and Wilmer, Chris, *Bitcoin for the Befuddled*, No Starch Press, 2015.
- Gunaratna, Rohan, *Inside Al Qaeda: Global Network of Terror*, Columbia University Press; First Printing Edition, 2002.
- Kuo Chuen, David Lee, *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, Elsevier Inc., 2015.
- Mishkin, Fredrick S., *The Economics of Money Banking and Financial Markets*, Pearson Education, 4th Edition, 2004.

- Articles

- AL Hassan, Abdulaziz "Money Laundering and Terrorism Financing: Does the Saudi Arabian Financial Intelligence Unit Comply with International Standards?", *Research Master Thesis*, Victoria University, 2011.
- Berg, Svenja and McCarthy, Killian J., "The Economics of ISIS — A Case of Theft or Money Laundering?", *Freedom from Fear*, vol. 11, 2016.
- Bierer, Timothy, "Hashing Out: The Problems and Solutions Concerning Cryptocurrency Used as Article 9 Collateral", *Case W. Res. J. L. Tech. & Internet*, vol. 77,issue 1, 2016.
- Bryanov, Kirill, "France and Germany: How Regulatory Traditions in Two Countries Could Affect EU Legislation", *CoinTelegraph.com*, March 30, 2018.
- Burns, Janet, 'Cut Off from Big Fintech, White Nationalists Are Using Bitcoin to Raise Funds", *Forbes*, 3 January 2018.
- Chavez-Dreyfuss, Gertrude, "About $1.2 Billion in Cryptocurrency Stolen Since 2017", *Cybercrime Group*, 2018.
- Dourado, Eli and Brito, Jerry, "Cryptocurrency", at: *The New Palgrave Dictionary of Economics*, Palgrave Macmillan, 2014. retrieved from: https://coincenter.org/entry/the-new-palgrave-dictionary-of-economics-cryptocurrency (visited:08/10/2018).
- Europol, "Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain", *Europol Press Release*, 26 March 2018.
- Gilbert, David, "Criminals are Racing to Cash Out Their Bitcoin. Here's How They're Doing It", *Vice*, 19 March 2018.
- Goldman, Zachary; Maruyama, Ellie; Rosenberg, Elizabeth; Saravalle, Eduardo; Solomon-Strauss, Julia, "Terrorist Use of Virtual Currencies: Containing the Potential Threat", *Center for New American Security*, Washington, 3 May, 2017.
- Greenberg, Andy, "End of the Silk Road: FBI Says It's Busted the Web's

Biggest Anonymous Drug Market", *Forbes*, 2 October, 2013.
- Higgins, Stan, 'ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide", *CoinDesk*, 7 July, 2014.
- Kimberley, Thachuk, "Terrorism's Financial Lifeline: Can It Be Severed?", *Strategic Forum, Institute for National Strategic Studies*, National Defense University, no. 191. 2002.
- Maxey, Levi, "Terrorists Stalk the Dark Web for Deadlier Weaponry", *The Cipher Brief*, 17 January, 2018.
- Authors: Tom Keatinge, David Carlisle, Florence Keen; Responsible Research Administrator: Kristiina Milt, "Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses", *Policy Department for Citizens' Rights and Constitutional Affairs*, European Parliament, 2018.
- Neumann, Richard and Basra, Rajan, "Crime as Jihad: Developments in the Crime-Terror Nexus in Europe", *CTC Sentinel*, vol. 10, issue 9, *Combatting Terrorism Center*, October 2017.
- Pacleb, Calvin Lee, "International Money Laundering: A Comprehensive Review and General Theory of Corruption", 2003, https://ttu-ir.tdl.org/handle/2346/141282003.
- Pacy, Eric P., "Tales from the Cryptocurrency: On Bitcoin, Square Pegs, and Round Holes", *New Eng. L. Rev.* vol. 49, 2014.
- Plessis, Paul du, "The Nature of Decentralized Virtual Currencies: Benefits, Risks and Regulations", *World Trade Institute*, 2014.
- Prentis, Mitchell, "Digital Metal: Regulating Bitcoin as a Commodity", *Case W. Res. J.L. Tech. & Internet*, vol. 66,issue 2, 2015.
- Redman, Jamie, "Chainalysis Raises $16Mn – Plans to Monitor Multiple Blockchains", *Bitcion.com*, 6 April, 2018.
- Schneider, Friedrich, "Macroeconomics: The Financial Flows of Islamic Terrorism". In: Masciandaro D. (ed.) *Global Financial Crime: Terrorism, Money Laundering and Offshore Center*, CRC Press Book, 2004.
- Torpey, Kyle, "AlphaBay Comments on Bitcoin Congestion, Monero Adoption and Zcash Possibilities", *Bitcoin Magazine*, 21 December, 2016.

- Reports and Recommendations
- Amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, 2018.
- Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, March 18, 2013.
- CTIF-CFI, *23rd Annual Report*, Belgian Financial Intelligence Processing Unit (CTIF-CFI), 2016.

- Customer Advisory: Understand the Risks of Virtual Currency Trading, 2018.
- European Central Bank, Virtual Currency Schemes – A Further Analysis, 2015.
- Europol, *Internet Organised Threat Assessment (IOCTA Report 2017)*, 2017.
- FATF, *Report on Money Laundering Typologies*, 2000-2001.
- FATF, *Emerging Terrorist Finance Risks*, 2015.
- FATF, *Report to G20 Finance Ministers and Central Bank Governors*, Paris, 2018.
- FATF, *Financing of Terrorism for Recruitment Purposes*, 2018.
- FATF, *Guidance for a Risk-Based Approach: Virtual Currencies*, Paris, 2015.
- FATF, *Money Laundering Using New Payment Methods*, Paris, 2010.
- FATF, *Report on New Payment Methods*, Paris, 2006.
- FATF, *Virtual Currencies: Key Definitions and Potential* AML/CFT Risks, Paris, 2014.
- IMF and the Fight against Money Laundering and the Financing of Terrorism, 2018.
- Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference, 2018.
- Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, Fin. Crimes Enforcement Network, Fin-2014-R011, 2014.

- Websites

- https://www.interpol.int/Crime-areas/Financial-crime/Money-laundering
- http://www.fatf-gafi.org/faq/moneylaundering/
- https://www.politico.eu/wp-%20content/%20uploads/2018/02/G20-Letter-on-crypto-assets-tokens.pdf
- https://en.bitcoin.it/wiki/FAQ
- https://payment24.ir/blog/everything-need-know-electronic-wallets/
- https://en.bitcoin.it/wiki/Wallet
- https://www.investopedia.com/terms/a/altcoin.asp
- http://hackingdistributed.com/2018/01/15/decentralization-bitcoin-ethereum/.