University of Tehran Press

Public Law Studies Quarterly

Homepage: http://jplsq.ut.ac.ir

Online ISSN: 2423-8139

Volume: --, **Issue:** --
-- --

Anonymity;
A Prominent Factor in Cryptocurrencies for Terrorist Financing

Amir Famil Zavar Jalali[1]✉ | Abbas Ali Kadkhodaei[2]

1. Corresponding Author; P.h.D in Public International Law, Faculty of Law and Political Sciences, University of Tehran, Tehran, Iran. Email: azjalali@ut.ac.ir
2. Professor, Faculty of Law and Political Sciences, University of Tehran, Iran. Email: kadkhoda@ut.ac.ir

Article Info

Article Type:
Research Article

Pages: 1-28

Received:
2023/09/28
Received in Revised form:
2024/05/27
Accepted:
2024/09/15
Published online:

Keywords:
Cryptocurrencies, Blockchain, Anonymity, Terrorist Financing.

Abstract

Cryptocurrencies or encrypted assets have been introduced as the latest example of a digital display of value that can perform the functions of money as a means of payment. These types of assets, which are protected by cryptography, operate based on the agreement between the user community and in a decentralized manner. Cryptocurrencies, provided a suitable platform for committing financial crimes. Among the international financial crimes related to cryptocurrencies is the financing of terrorism, which has increased its scope in the last decade with the use of cryptocurrencies. One of the prominent features of cryptocurrencies that makes them attractive for terrorist financing is the anonymity of their transactions. In this article, we are trying to answer this question by using descriptive and analytical method, how anonymity as a feature of cryptocurrency can be effective in the use of this model of assets by terrorists. According to the studies done, considering that concealing the identity and preventing the blocking of financial resources is one of the most important concerns of terrorist groups and their sponsors, it can be acknowledged that anonymity is an important and key factor for terrorists to turn to the market of new assets, including cryptocurrencies.

How To Cite	Famil Zavar Jalali, Amir; Kadkhodaei, Abbas Ali (2025). Anonymity; A Prominent Factor in Cryptocurrencies for Terrorist Financing. *Public Law Studies Quarterly*, -- (--), 1-28. DOI: https://doi.com/10.22059/jplsq.2024.365889.3400
DOI	10.22059/jplsq.2024.365889.3400
Publisher	The University of Tehran Press.

انتشارات دانشگاه تهران

فصلنامه مطالعات حقوق عمومی

Homepage: http://jplsq.ut.ac.ir

شاپا الکترونیکی: ۸۱۳۹-۲۴۲۳

دوره: -- شماره: --

گمنامی؛ عاملی بارز در رمزارزها برای تأمین مالی تروریسم

امیر فامیل زوار جلالی[۱]✉ | عباسعلی کدخدایی[۲]

۱. دانش‌آموختهٔ دکتری حقوق بین‌الملل عمومی، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران. رایانامه: azjalali@ut.ac.ir

۲. استاد دانشکدهٔ حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران. رایانامه: kadkhoda@ut.ac.ir

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۱-۲۸

تاریخ دریافت:
۱۴۰۲/۰۷/۰۶

تاریخ بازنگری:
۱۴۰۳/۰۳/۰۷

تاریخ پذیرش:
۱۴۰۳/۰۶/۲۵

تاریخ انتشار برخط:

کلیدواژه‌ها:
بلاکچین، تأمین مالی تروریسم، رمزارزها، گمنامی.

چکیده

رمزارزها یا همان دارایی‌های رمزنگاری‌شده به‌عنوان جدیدترین نمونه از نمایش دیجیتالی ارزش معرفی شده‌اند که می‌توانند کارکردهای پول به‌عنوان وسیله پرداخت را ایفا کنند. این نوع دارایی‌ها که به‌وسیلهٔ رمزنگاری محافظت می‌شوند، بر اساس توافق میان جامعهٔ کاربران و به‌صورت غیرمتمرکز عمل می‌کنند. رمزارزها با وجود تمام مزایای خود بستر مناسبی را نیز جهت ارتکاب جرائم مالی فراهم کرده است. از جمله جرائم مالی بین‌المللی مرتبط با رمزارزها، تأمین مالی تروریسم است که در دههٔ اخیر دامنهٔ آن با استفاده از رمزارزها افزایش یافته است. یکی از ویژگی‌های بارز رمزارزها که آنها را برای ارتکاب تأمین مالی تروریسم، مستعد و جذاب می‌سازد، بحث گمنامی یا ناشناس بودن تراکنش‌های آنهاست. در پژوهش حاضر با استفاده از روش توصیفی- تحلیلی درصدد پاسخگویی به این سؤال هستیم گمنامی به‌عنوان یک ویژگی رمزارز تا چه اندازه می‌تواند در استفادهٔ تروریست‌ها از این مدل دارایی‌ها، مؤثر باشد. با توجه به مطالعات صورت‌گرفته، نظر به اینکه پنهان‌سازی هویت و جلوگیری از بلوکه شدن منابع مالی، از مهم‌ترین دغدغه‌های گروه‌های تروریستی و حامیان مالی آنهاست، می‌توان گفت گمنامی عاملی بسیار مهم و کلیدی برای تروریست‌ها در جهت روی آوردن به بازار دارایی‌های جدید از جمله رمزارزهاست.

استناد

فامیل زوار جلالی، امیر؛ کدخدایی، عباسعلی (۱۴۰۴). گمنامی؛ عاملی بارز در رمزارزها برای تأمین مالی تروریسم. *مطالعات حقوق عمومی*، -- (--)، ۱-۲۸.
DOI: https://doi.com/10.22059/jplsq.2024.365889.3400

DOI 10.22059/jplsq.2024.365889.3400

ناشر مؤسسهٔ انتشارات دانشگاه تهران.

۱. مقدمه

وقتی صحبت از تأمین مالی تروریسم می‌شود ابتدا شایسته است تا به هدف این جرم یعنی ایجاد رعب و وحشت اشاره‌ای نمود. تروریسم به معنای استفادهٔ سازماندهی‌شده و سیستماتیک از ترس و وحشت برای رسیدن به مقاصد سیاسی است. تروریسم در هر دو شکل داخلی و بین‌المللی آن، پدیده‌ای قدیمی است که اهداف آن در دامنه‌ای از کسب قدرت و نبرد برای آزادی ملی تا سرکشی و عمل به دستورهای ایدئولوژیکی و مذهبی قرار می‌گیرد (کوهن، ۱۳۸۷: ۱۸۴). صرف‌نظر از حوادث تروریستی در گذشته‌های دور، پدیدهٔ تروریسم حداقل پیش از آغاز جنگ جهانی اول منشأ بسیاری از درگیری‌ها و خصومت‌ها در روابط بین‌الملل بوده است (میرعباسی و فامیل زوار جلالی، ۱۳۹۵: ۲۶۸). بعد از جنگ جهانی دوم و به‌ویژه با رویداد ۱۱ سپتامبر، اهمیت این قضیه دوچندان شد و از آن زمان بود که جامعهٔ جهانی بر هدف خود یعنی مبارزه با تروریسم بیشتر مصمم گردید. بهترین شیوه برای حذف تروریسم، بهبود شرایط نامطلوب اجتماعی، اقتصادی و سیاسی به منظور پیشگیری از روی آوردن افراد به ارتکاب اعمال مبتنی بر ترور است که البته این امر مستلزم تلاش‌های جامع و بلندمدت می‌باشد. نظر به اینکه حملات تروریستی هزینه‌های اجتناب‌ناپذیری دارند که قابل اغماض نیست، مسدود کردن کانال‌های تأمین مالی و مقابله با روش‌های سرمایه‌افزایی سازمان‌های تروریستی، یک راه مستقیم و کوتاه برای پیشگیری از آن محسوب می‌شود (Shacheng & Zhu, 2021: 2331). منابع مالی، مهم‌ترین بُعد در تحقق یک عملیات تروریستی است. ازاین‌رو با قطع این منابع می‌توان به‌صورت محسوس با تروریسم مبارزه کرد. از همین رو، جامعهٔ بین‌المللی و در رأس آن سازمان ملل متحد همواره به‌دنبال ایجاد سازوکارهایی برای قطع منابع مالی تروریست‌ها اعم از منابع مالی مشروع و نامشروع بوده است (کدخدایی و فامیل زوار جلالی، ۱۴۰۲: ۳).

اما منظور از تأمین مالی تروریسم چیست. در ساده‌ترین تعریف، تأمین مالی تروریسم اقدامی آگاهانه جهت فراهم ساختن دارایی[1] برای افراد و گروه‌های درگیر در فعالیت‌های تروریستی است (دسوزا، ۱۳۹۶: ۶۰). بدون تردید پول، به مثابهٔ «خون حیاتی» است که در رگ‌های گروه‌های تروریستی جهان جریان دارد و بدون داشتن منابع مالی، برای گروه‌های تروریستی دشوار است که عملیات خود را به‌صورت گسترده و سازمان‌یافته طراحی و سپس وارد فاز عملیاتی کنند. سازمان‌های بین‌المللی و کشورهای جهان، برای تعریف تأمین مالی تروریسم بر هنجارهای اجرایی و روش‌های مالی خود، متمرکز شده‌اند. برای مثال مطابق مادهٔ ۲ کنوانسیون مبارزه با تأمین مالی تروریسم مصوب ۱۹۹۹، فردی متهم به جرم تأمین مالی تروریسم است که با هر وسیله، مستقیم یا غیرمستقیم، قانونی و یا غیرقانونی، وجوهاتی را فراهم و یا گردآوری کند، به قصد اینکه کل وجوهات مذکور و یا بخشی از آن را مصروف فعالیت‌های مرتبط با

1. Asset

جرائم تروریستی مندرج در کنوانسیون‌های ضمیمه‌شده، نماید (CFT, 1999, Article 2).[1] صندوق بین‌المللی پول نیز تأمین‌مالی تروریسم را به جمع‌آوری و تهیهٔ وجوه برای پشتیبانی از فعالیت‌های تروریستی یا سازمان‌های تروریستی تعریف می‌کند. همچنین از نظر یکی از پژوهشگران، «تأمین مالی تروریسم عبارت است از جریان پول و حمایت مالی دولت‌ها، سازمان‌ها یا اشخاص حقیقی از گروه‌های تروریستی به‌نحوی که آنها را برای انجام فعالیت‌هایشان توانمند سازد» (Dalyan, 2008: 139). البته باید توجه داشت تأمین مالی تروریسم، تنها تأمین بودجهٔ یک عملیات تروریستی خاص نیست، بلکه تأمین گسترده‌تر هزینه‌های سازمانی، توسعه، حفظ سازمان‌های تروریستی و ایجاد محیطی برای تقویت فعالیت‌های آنهاست که با اینکه ممکن است محسوس نباشد، اما بخش شایان توجهی از مخارج سازمان‌های تروریستی را دربرمی‌گیرد. بدین‌ترتیب هزینه‌های سازمان‌های تروریستی را می‌توان به دو بخش تقسیم کرد. دستهٔ اول، هزینه‌های سازمانی است؛ یعنی هزینه‌هایی که برای تداوم و مدیریت گروه‌های تروریستی به‌کار می‌رود. منابع مالی برای ترویج ایدئولوژی، آموزش اعضای جدید و مخارج زندگی از این دست هستند. البته نیازهای مالی، بسته به نوع گروه‌های تروریستی، متغیرند و گروه‌هایی که سلسله‌مراتب فراملی دارند، نسبت به گروه‌های کوچک‌تر و مستقل، بی‌شک هزینه‌های سازمانی بیشتری خواهند داشت. دستهٔ دوم نیز هزینه‌های عملیاتی است؛ یعنی مخارجی که برای انجام یک حملهٔ تروریستی باید هزینه شود. خرید تسلیحات و مهمات، دستمزد عاملان عملیات، تدارک سفرها و سازماندهی حملات از این دست از مخارج هستند.

حال باید دانست که گروه‌های تروریستی از دو طریق شیوه‌های قانونی و غیرقانونی منابع مالی خود را تأمین می‌کنند که البته در دستهٔ اخیر حوزهٔ اشتراک پول‌شویی و تأمین مالی تروریسم افزایش می‌یابد و این گروه‌ها برای در امان ماندن از هرگونه بلوکه شدن وجوه و دارایی، ناگزیر به تطهیر منابع مالی خود می‌شوند. برای مثال از زمان شیوع بیماری کووید ۱۹ در سال ۲۰۲۰ و طبق گزارش‌های مرتبط گروه ویژهٔ اقدام مالی[2]، سازمان‌های تروریستی از این بحران جهانی نیز برای سودآوری غیرقانونی استفاده

---

۱. کنوانسیون‌های ضمیمه به کنوانسیون مبارزه با تأمین مالی تروریسم عبارت‌اند از: «کنوانسیون سرکوب تصرف غیرقانونی هواپیما ۱۹۷۰، کنوانسیون سرکوب رفتارهای غیرقانونی ضد هواپیمایی غیرنظامی ۱۹۷۱، پیشگیری و مجازات جرائم علیه افراد تحت حمایت بین‌المللی از جمله دیپلمات‌ها ۱۹۷۳، کنوانسیون بین‌المللی ضد گروگان‌گیری ۱۹۷۹، کنوانسیون حمایت فیزیکی از مواد هسته‌ای ۱۹۸۰، پروتکل سرکوب رفتارهای خشونت‌آمیز غیرقانونی در فرودگاه‌های مورد استفادهٔ هوانوردی بین‌المللی غیرنظامی ۱۹۸۸، کنوانسیون سرکوب اقدامات غیرقانونی ضد امنیت پروازهای غیرنظامی ۱۹۸۸، پروتکل سرکوب اقدامات غیرقانونی ضد تأسیسات ثابت در فلات قاره ۱۹۸۸ و کنوانسیون بین‌المللی سرکوب بمب‌گذاری‌های تروریستی ۱۹۹۷».

2. Financial Action Task Force (FATF)

کرده‌اند که تولید تجهیزات پزشکی تقلبی یکی از آن نمونه‌هاست (Shacheng & Zhu, 2021: 139). حمایت دولت‌ها از تروریسم نیز از جمله شیوه‌های بارز تأمین مالی تروریسم است. استفاده از منابع مالی دولت‌ها برای سازمان‌های تروریستی یک امتیاز عمده محسوب می‌شود، زیرا منابع مالی غیرقابل تصوری را در اختیار آنها قرار می‌دهد که به‌طور مستقیم از درآمدهای ملی کشور سرچشمه می‌گیرد (الهویی نظری و فامیل زوار جلالی، ۱۳۹۶: ۷۳۱). البته تأمین مالی تروریسم در این مرحله به پایان نمی‌رسد، بلکه نگهداری، انتقال و جابه‌جایی دارایی و وجوه نیز خود مسئلهٔ مهمی است. به این ترتیب که وجوه به‌دست‌آمده باید به‌نحوی نگهداری شود و برای تبدیل به یک حمله یا سرمایه‌گذاری بلندمدت انتقال یابد. شیوه‌های متفاوتی نیز برای انتقال دارایی وجود دارد، از نقل و انتقال چمدانی گرفته تا استفاده از تجارت کالا و خدمات. شایان ذکر است موفقیت در شیوه‌های مقابله با تأمین مالی تروریسم که به کاهش دسترسی تروریست‌ها به منابع مالی سنتی و به‌ویژه ارزهای فیات[1] منجر می‌شود و از طرفی مسدود شدن کانال‌های رسمی انتقال وجه مانند حساب‌های بانکی این نگرانی را ایجاد می‌کند که گروه‌های تروریستی برای تأمین مالی فعالیت‌های خود، به‌دنبال روش‌های دیگری برای سرمایه‌افزایی، نگهداری و انتقال منابع مالی خود باشند که این امر به افزایش روزافزون استفاده از روش‌های انتقال غیرقابل ره‌گیری منجر می‌شود؛ یعنی روش‌هایی که در خارج از چارچوب مالی رسمی مرسوم اتفاق می‌افتند که به آن روش‌های غیررسمی انتقال ارزش یا نظام پرداخت جایگزین[2] می‌گویند.

منظور از نظام پرداخت جایگزین، یک روش غیررسمی برای انتقال پول و ارزش است که بدون دخالت دولت و از کانال‌های غیررسمی قابل انجام بوده و می‌تواند به شکل سنتی یا مدرن باشد. مطابق تعریف گروه ویژهٔ اقدام مالی، نظام پرداخت جایگزین عبارت است از «هر سازوکاری که به‌منظور انتقال وجه از مکانی به مکان دیگر خارج از چارچوب رسمی بانکی عمل نماید» (الهویی نظری و همکاران، ۱۴۰۱: ۱۲۳۰). این روش‌های غیررسمی مبادلات مالی، به اشکال مختلف از جمله انتقال وجه به‌صورت فیزیکی یا چمدانی، حواله و امثال آن صورت می‌گیرد که نمونهٔ جدید آن رمزارزها[3] هستند که موضوع پژوهش حاضر است. رمزارزها به‌عنوان یک دارایی‌های نامحسوس، از این حیث می‌توانند برای تروریست‌ها جذاب باشد که هم وسیله‌ای برای تولید درآمد و هم ابزاری برای انتقال دارایی خواهد بود. به‌عبارت دیگر هر دو جنبهٔ تأمین مالی تروریسم را در خود دارد. همچنین این دارایی‌های رمزنگاری‌شده، با ویژگی‌های خاصی از جمله گمنامی، تراکنش آسان، عدم محدودیت فیزیکی و عدم تمرکز می‌توانند

---

۱. ارز فیات، پولی است که فی‌نفسه ارزش مالی ندارد، بلکه ارزش آن وابسته به دولت است، یعنی دولت به آن ارزش می‌دهد تا در معاملات به‌کار رود. برای مثال ریال ایران نوعی ارز فیات است.

2. Alternative Remittance System

3. Cryptocurrency

ابزاری مناسب‌تر از شیوه‌های سنتی تأمین مالی تروریسم باشد. از میان این ویژگی‌ها، «گمنامی» یا «ناشناس بودن» نقش مهمی در استفاده از این نوع دارایی‌ها در تأمین مالی تروریسم خواهد داشت. در پژوهش حاضر مترصد بررسی این موضوع هستیم که گمنامی به‌عنوان یکی از ویژگی‌های مهم رمزارزها، تا چه حد می‌تواند عاملی مهم برای استفاده از این نوع دارایی‌ها در راستای تأمین مالی تروریسم باشد.

۲. رمزارزها

دارایی‌های رمزنگاری‌شده[1]، ارزهای مجازی[2]، رمزارزها[3] و به‌طور کلی دارایی‌های مجازی، همگی واژگان جدید و نمایانگر شکل جدیدی از ارزش[4] هستند و انتقال سریع و بی‌واسطهٔ وجوه را توصیف می‌کنند. اگرچه بیشتر دارایی‌های رمزنگاری‌شده به‌عنوان محصولی نوآورانه در راستای پیشرفت‌های فناوری و با نیات بشردوستانه ایجاد شدند، اما سوءاستفاده از این فناوری‌ها نیز روی دیگر سکه است که نباید از آن غافل شد. رمزارزها، به عنوان یکی از نمونه‌های نظام پرداخت جایگزین، که حوزهٔ عملیاتی آن فضای مجازی[5] است، از یک سو می‌تواند با پشت سر گذاشتن نهادهای نظارتی و ایجاد شفافیت و از سوی دیگر با ایجاد لایه‌های امنیتی به یک کارگزار بی‌نقص برای تراکنش‌های بی‌نام و نشان و غیرقابل ره‌گیری و ابزاری جدی برای تأمین مالی فعالیت‌های غیرقانونی از جمله تأمین سازمان‌های تروریستی تبدیل شود.

مطابق تعریف گروه ویژهٔ اقدام مالی، رمزارزها به هر نمایش دیجیتالی از ارزش گفته می‌شود که قابلیت معامله به‌صورت مجازی را دارد و می‌تواند به‌عنوان وسیلهٔ پرداخت و نیز ذخیرهٔ ارزش و سرمایه‌گذاری عمل کند و در کنار این دو، یک نوع واحد حساب نیز محسوب می‌شود (FATF, 2014: 4)، یعنی می‌توان کالاها و خدمات را بر اساس آن قیمت‌گذاری کرد. این نوع ارزها توسط هیچ مرجع قانونی صادر و تضمین نمی‌شود و تمامی ویژگی‌ها و وظایف آن بر اساس توافق میان جامعهٔ کاربران این نوع دارایی‌های مجازی صورت می‌گیرد.[6]

رمزارزها با توجه به ویژگی‌های خود، مزایای بالقوه زیادی را به ارمغان آورده‌اند که گمنامی[7] یا همان ناشناس ماندن و شفافیت از ویژگی‌ها و امکانات مهم آنهاست؛ به این معنا که در تراکنش‌های رمزارز،

---

1. Crypto Asset
2. Virtual Currency
3. Crypto currency
4. Value
5. Cyber Space

۶. شایان اشاره است که رمزارزها را نمی‌توان به‌مثابهٔ E-Money یا همان پول الکترونیک که نمایشی دیجیتال از پول فیات است، دانست، زیرا E-Money تنها نوعی مکانیزم دیجیتالی برای انتقال الکترونیکی پولی است که از آن به‌عنوان ارز ملی و پول رسمی یک کشور یاد می‌شود (FATF, 2019: 59).

7. Anonymity

هویت فروشندگان و خریداران کاملاً محرمانه می‌ماند. هرچند به هر خریدار و فروشنده، یک آی‌دی کیف پول یا شناسهٔ کیف پول[1] اختصاص داده می‌شود، اما این آی‌دی‌ها به‌آسانی و با هر تراکنش تغییرپذیرند. البته به هر میزان که رمزارزها با ویژگی گمنامی شناخته می‌شوند، از طرفی واجد ویژگی شفافیت نیز هستند (Cynthia Dion, 2019: 24-25). بزرگ‌ترین مزیت ارائه‌شده برای رمزارزها و بسترهای آن که همان بلاکچین است، این است که در قالب یک سیستم کاملاً شفاف معامله‌گری ظاهر می‌شوند. شفافیت به این معناست که تمام تراکنش‌ها در دفتر کل عمومی یا همان بلاکچین ثبت می‌شود و از سوی تمامی کاربران قابل مشاهده است، اما هویت دو طرف تراکنش ناشناس و پنهان است.[2] به‌عبارت دیگر فناوری مبتنی بر بلاکچین، سبب شفافیت برای تمامی افراد شبکه می‌شود و تراکنش‌ها برای تمامی رایانه‌های متصل قابل رؤیت هستند و این همان ماهیت خاص پلتفرم رمزارزها یعنی بلاکچین است.[3]

در بین ویژگی‌های متعدد رمزارزها، آنچه بیش از همه در حوزهٔ تأمین مالی تروریسم کاربرد دارد، ویژگی گمنامی است، زیرا در حوزهٔ جرائم مالی و به‌خصوص در تأمین مالی تروریسم، پنهان ماندن و عدم رهگیری، نقش بسیار مهمی در به سرانجام رساندن عملیات مجرمانه دارد. ازاین‌رو شایسته است ویژگی گمنامی، عوامل تقویت یا ضعف این ویژگی و نقش آن در تأمین مالی تروریسم در حوزهٔ رمزارزها بررسی شود.

۳. گمنامی

گمنامی[4] یا همان ناشناس ماندن از مشخصه‌های مهم دارایی‌های مجازی از جمله رمزارزهاست. همان‌طورکه یاد شد، اگرچه تراکنش‌ها را می‌توان در دفاتر ثبت عمومی پیدا کرد، اما هویت فروشندگان و خریداران کاملاً محرمانه می‌ماند. برای مثال رمزارز بیت کوین دارای دو کلید عمومی و خصوصی است که از تعدادی حروف الفبا و عدد تشکیل می‌شود. کلید عمومی مانند شماره حسابی می‌ماند که برای سایر کاربران نمایش داده می‌شود، اما کلید خصوصی فقط در اختیار صاحب حساب و برای تأیید هویت وی قبل از انجام مبادله ضروری است (ماتسورا، ۱۳۹۷: ۱۵۲). وجوه به کلیدهای خصوصی رمزنگاری‌شده ارسال می‌شوند و هر فردی که این کلیدها را در اختیار

---

1. Wallet ID

۲. برای مطالعهٔ بیشتر در خصوص مباحث فنی ر.ک:

Salami, Iwa, (2017): Terrorism Financing with Virtual Currencies – Can Regulatory Technology Solutions Combat this? Studies in Conflict & Terrorism, 2017, p.27, Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston, Terrorist use of cryptocurrency, Published by the RAND Corporation, 2019, pp. 24- 30

۳. «سیستم‌های مبتنی بر بلاک‌چین، در مقایسه با بایگانی‌ها و دفاتر کل موجود، شفافیت بیشتری دارند، زیرا تمام افراد شبکه قادر به دیدن تغییرات در دفاتر کل هستند و تراکنش‌ها، پس از وارد شد به بلاک‌چین، دیگر قابل تغییر یا حذف نیستند» (Gates, Mark, 2017: 23)

4. Anonymous

داشته باشد، می‌تواند رمزارزها را کنترل کند. به همین دلیل، بیت‌کوین را ناشناس می‌نامند، زیرا اگرچه کلیدهای عمومی کاربران می‌تواند از طریق تاریخچهٔ معامله پیگیری شود، اما هویت خریداران و فروشندگان پنهان باقی می‌ماند (Dion, 2013: 166). گمنامی رمزارزها نه‌تنها به نفع تروریست‌هاست، بلکه خطر تعقیب سازمان‌ها یا افراد حامی تروریسم را که در پی کمک مالی به آنها هستند، کاهش می‌دهد (Shacheng & Zhu, 2021: 2333). البته باید گفت که این میزان از اغراق در خصوص گمنامی و ناشناس بودن رمزارزها صحیح نیست. شاید توصیف بهتر برای رمزارزها، ویژگی «شبه‌گمنامی»[1] باشد. توضیح آنکه کاربران رمزارز، با آدرس‌های الفبا–عددی که مرتبط با کیف پول آنهاست، روی بلاک‌چین نمایش داده می‌شوند. بنابراین هویت واقعی یک کاربر، روی بلاک‌چین قابل رؤیت نیست، اما اطلاعات مربوط به تراکنش‌های آنها مانند تاریخ، میزان انتقال و آدرس‌های طرف‌های مقابل همگی به‌صورت عمومی ثبت می‌شود. افزون بر این از آنجا که بلاک‌چین، یک آرشیو زمانی از تراکنش‌ها را داراست، می‌تواند مسیر جابه‌جایی‌های رمزارز را نیز حکایت کند. بنابراین، اگر مشخص باشد که مالک یک آدرس عمومی بیت‌کوین، چه شخصی است، می‌توان دربارهٔ فعالیت آنها در شبکه، مقادیر شایان توجهی اطلاعات جمع‌آوری کرد (Wallace, 2011). برای مثال اگر فردی بخواهد برای تمام تراکنش‌هایش، فقط از یک جفت کلید عمومی یا خصوصی استفاده کند (استفادهٔ مجدد از کلید)، مشاهدهٔ هویت آنها برای یک ناظر نسبتاً آسان خواهد بود. برای مثال شخصی که در ۲۲ می ۲۰۱۰، ده هزار بیت‌کوین از کلید عمومی «1XPTgDRhN8RfnzniWCddobD9iKZatrvH4» را صرف خرید دو عدد پیتزای معروف کرده (Mack, 2013)، همان شخصی است که در ۱۵ نوامبر ۲۰۱۰، هزار و سیصد بیت‌کوین را به کلید عمومی «1DvSvCnRsHdrA76PnD1j58wAeUFnhTauxJ» فرستاده است (Wallace, 2011). گره خوردن نخستین تراکنش به هویت حقیقی شخص، به این معناست که تراکنش دوم نیز به احتمال زیاد با هویت حقیقی او مرتبط است و این یکی از نقایص عملی ویژگی گمنامی است.

در زمینهٔ «شناسایی کاربران گمنام»، روش‌های مختلفی به‌کار گرفته شده است و با توجه به قابلیت‌هایی که در آینده خواهد آمد، حتی تراکنش‌هایی که فعلاً قابل شناسایی نیستند نیز ممکن است در معرض شناسایی قرار گیرند. به‌ویژه آنکه امروزه برخی شرکت‌های خصوصی، در زمینهٔ گمنامی‌زدایی از تراکنش‌های رمزارزها و توسعهٔ ابزارهایی برای تحلیل فعالیت‌های غیرقانونی آنها به‌صورت تخصصی فعالیت می‌کنند (Jamie, 2018). این شرکت‌های جرم‌شناسی بلاک‌چین، راه‌حل‌هایی را برای نهادهای مجری قانون و صرافی‌های رمزارز ارائه می‌کنند تا بتوانند تراکنش‌های مشتریان خود را شناسایی و آنها را از نظر علائم مشکوک بررسی کنند.

نقطهٔ اتصال میان رمزارزها و ارزهای حقیقی نیز از دیگر چالش‌هایی است که از میزان ناشناس بودن

1. Pseudo-Anonymous

این‌گونه دارایی‌ها می‌کاهد، زیرا در گام نخست، لازمهٔ ارسال رمزارز برای یک تروریست، تبدیل ارز حقیقی به ارز مجازی است. ازاین‌رو ابتدا باید از یک صرافی یا یک شخص حقیقی در قبال پرداخت ارز فیات، رمزارز موردنظر خریداری شده و سپس رمزارز خریداری‌شده به مقصد موردنظر ارسال شود. در اینجا ممکن است با ره‌گیری مقصد نهایی تا نقطهٔ اولیه به سرنخ‌هایی دست یافت؛ یعنی تا زمانی‌که کیف پول ارزهای مجازی فرد با اطلاعات واقعی وی در ارتباط نباشد، وی تماماً ناشناس است. اما به محض اینکه ارزهای مجازی خود را از کیف پول الکترونیکی خود به حساب بانکی خود انتقال دهد یا از یک صرافی متمرکز استفاده کند که اطلاعات هویتی وی را ثبت کرده، ناشناس بودن خود را در واقع از بین برده است.

به‌طور کلی قابلیت ردیابی ارزهای مجازی، سودمندی آن برای بازیگران تروریستی را کم می‌کند (Berg & McCarthy, 2016: 84). در واقع، همان‌طورکه در خصوص کمپین سرمایه‌گذاری جمعی «جاهِزونا»[1] اتفاق افتاد، تحلیلگران امنیتی توانستند جابه‌جایی رمزارز توسط تروریست‌ها را رصد کنند. یک تحلیلگر نیز از طریق یک بات توییتر[2] موسوم به «Neonazi BTC Tracker» فعالیت بیت‌کوینی افراط‌گرایان را رصد کرد. افراط‌گرایان از سیزده آدرس بیت‌کوین استفاده کرده بودند و این بات، هر تراکنش از این آدرس‌ها را به‌طور خودکار توییت کرد (Keatinge *et al*., 2018: 32). اما می‌توان گفت همین میزان از شبه‌ناشناسی نیز برای گروه‌های مجرمانه و به‌خصوص تروریست‌ها کفایت می‌کند. به هر حال ارسال آدرس عمومی کیف پول یک رمزارز در یک شبکهٔ اجتماعی به‌مراتب بهتر و امن‌تر از تبلیغ شمارهٔ حساب بانکی در یک بانک یا مؤسسهٔ مالی معتبر است (کدخدایی و نوروزپور، ۱۳۹۹: ۱۶). مضافاً اینکه کاربران و در بحث ما تروریست‌ها می‌توانند با استفاده از یک سری روش‌ها و تکنیک‌ها، برخی از این تهدیدات فنی برای گمنامی را کاهش دهند و در نتیجه آن را برای تأمین مالی فعالیت‌های مجرمانه خود مناسب کنند. استفادهٔ گسترده از این روش‌های ناشناس‌ساز سبب شده است که گروه ویژهٔ اقدام مالی طی گزارشی در سپتامبر ۲۰۲۰، تحت عنوان شاخصه‌های خطر دارایی‌های مجازی، بر موضوع

---

۱. یحیی فانوسی، پژوهشگر بنیاد دفاع از دموکراسی، در جولای ۲۰۱۶، یک مدل از کمپین‌های جمع‌آوری سرمایه را شناسایی کرد که توسط مرکز رسانهٔ «تیمیه» اداره می‌شد. این مرکز، واحد رسانه‌ای آنلاین شورای مجاهدین در حومهٔ اورشلیم بود. این شورا که مجموعه‌ای از گروه‌های سَلَفی جهادی هستند و ایالات متحده آن را یک سازمان تروریستی خارجی نامیده بود، در جولای ۲۰۱۵ آغاز به کار کرد و از ژوئن ۲۰۱۶، گزینهٔ پرداخت با بیت‌کوین را نیز برای کمک‌کنندگان اضافه کرد. تا آگوست ۲۰۱۶، این کمپین توانست از طریق دو تراکنش که به فاصلهٔ شش روز از هم در جولای ۲۰۱۶ انجام شده بودند، حدوداً ۹۲۹. ۰ بیت‌کوین (حدوداً ۵۴۰ دلار) جمع کند. این مرکز رسانه‌ای با راه‌اندازی کمپین آنلاین خود تحت عنوان «جاهزونا» به معنای «ما را تجهیز کنید»، و با انتشار دستورالعمل‌های استفادهٔ آنلاین از این فناوری، امکان جمع‌آوری کمک‌های بیت‌کوین را برای خود فراهم کرد (United States Department of Justice, 2015).

2. Twitter-bot

کارکردهای فنی گمنامی و نقش آن در تأمین مالی تروریسم تأکید کند (FATF, 2020). در مجموع راه‌های متعددی برای لایه‌بندی[1] و بالا بردن ویژگی گمنامی و پنهان‌سازی هویت در تراکنش‌های رمزارزی وجود دارد که در ادامه بررسی می‌شوند.

۴. روش‌های گمنام‌سازی در حوزهٔ رمزارزها

همان‌طورکه اشاره شد، اگرچه تراکنش‌های رمزارزها را نمی‌توان واجد ویژگی تماماً ناشناس تلقی کرد، اما روش‌هایی در حوزهٔ رمزارزها و بلاکچین وجود دارد که از آن می‌توان برای گمنامی هرچه بیشتر تراکنش‌های رمزارز استفاده و در نتیجه آن را برای فعالیت‌های مجرمانه مناسب کرد. از جملهٔ این روش‌ها می‌توان به ناشناس‌سازها، دارک‌وب[2] و آلت‌کوین‌های حریم محور[3] اشاره کرد که در ادامه هریک بررسی می‌شود.

۴. ۱. ناشناس سازها[4]

مجرمان برای مخفی‌سازی منشأ پول، ممکن است از سرویس‌ها و فناوری‌های ناشناس‌ساز استفاده کنند. ابزاری که برای ناشناس‌سازی تراکنش‌های رمزارز به‌کار می‌رود به این صورت است که در یکی از مراحل انتقال رمزارز، یک تراکنش جمعی انجام می‌شود و جمعی بودن این تراکنش، به معنای از بین رفتن برقراری تناظر یک به یک میان رمزارزها و ارسال‌کنندگان آنهاست. بنابراین، با استفاده از فناوری‌های ناشناس‌ساز، مجرمان می‌توانند بدون ترس از افشای هویت خود، اقدام به انتقال رمزارز کنند.

میکسرها[5] (مخلوط‌کن‌ها) و پشتک‌زن‌ها[6] از انواع شاخص ناشناس‌سازها هستند که زنجیرهٔ تراکنش‌های یک بلاکچین را پنهان می‌کنند. به این ترتیب که همهٔ تراکنش‌ها را به یک آدرس رمزارز یکسان ربط می‌دهد، اما همهٔ آنها را با هم و به‌گونه‌ای ارسال می‌کند که گویی، هر کدام از یک آدرس متفاوت ارسال شده‌اند (FATF, 2014: 6). ارسال تراکنش‌ها در یک میکسر، با یک رشتهٔ پیچیده و نیمه‌تصادفی از تراکنش‌های ساختگی انجام می‌شود. به این ترتیب، ربط دادن رمزارزهای خاص (آدرس‌ها) به یک تراکنش خاص، دشوار می‌شود. سرویس‌های میکسر، به محض دریافت دستورالعمل‌های یک کاربر، فعال می‌شوند و وجوه را به یک آدرس رمزارز خاص، ارسال می‌کنند.

---

1. Layering
2. Dark Web
3. Privacy Coins
4. Anonymizer
5. Mixer
6. یعنی چرخاندن، غلت زدن، میکس کردن Tumbling

سرویس میکسر سپس این تراکنش را با سایر تراکنش‌ها مخلوط می‌کند، طوری که مشخص نشود که کاربر قصد هدایت وجوه به چه کسی را داشته است (FATF, 2014: 6). برای مثال الف می‌خواهد به ب یک بیت‌کوین پرداخت کند. ج هم می‌خواهد به د یک بیت‌کوین ارسال کند. برای گمراه کردن ناظران قانونی که این تراکنش‌ها را دنبال می‌کنند، شخص الف و ج که ارسال‌کننده هستند، می‌توانند بیت‌کوین خود را به میکسری به نام خ ارسال کنند و به آن دستور دهند تا یک بیت‌کوین به شخص ب و یک بیت‌کوین به شخص د انتقال دهد. در این حالت ناظر تنها جریان تراکنش از الف و ج به خ و نیز از خ به ب و د را می‌بیند، ولی نمی‌تواند حدس بزند که کدام‌یک از الف یا ج بیت‌کوین را به شخص ب یا د فرستاده است. به‌عبارت دیگر، حتی اگر به‌طور قطع مشخص شود که خرید و فروش بیت‌کوین به‌منظور پول‌شویی یا تأمین مالی تروریسم صورت گرفته و تراکنش‌ها نیز رصد شود، اما به‌دلیل عدم امکان انتساب این نقل و انتقال به شخص معینی، جرم‌یابی با مشکل روبه‌رو می‌شود (Kethineni *et al*., 2017: 43). سرویس‌های مخلوط‌کن مانند بیت‌میکس[۱]، مانی میکسر[۲]، کوین جوین[۳] و دارک والِت[۴] از معروف‌ترین و رایج‌ترین سرویس‌های ناشناس‌ساز در حوزهٔ رمزارزها هستند.

اهمیت استفاده از ناشناس‌سازها از چشم نهادهای بین‌المللی نظیر گروه ویژهٔ اقدام مالی نیز دور نمانده است. گروه ویژهٔ اقدام مالی در ژوئن ۲۰۱۹ در سند راهنمایی تحت عنوان «رویکردهای ریسک‌محور برای دارایی‌های مجازی و خدمات‌دهندگان این دارایی‌ها»، تأکید کرد که کشورها و ارائه‌دهندگان خدمات مربوط به رمزارزها، هنگام شناسایی، ارزیابی و نحوهٔ کاهش خطرهای مرتبط با فعالیت‌های دارایی‌های مجازی یا هنگام فراهم‌سازی محصولات یا خدمات مرتبط، باید به این نکته توجه داشته باشند که ناشناس‌سازهای پروتکل اینترنتی (IP) مانند مسیریاب آنیون (تور TOR) یا پروژهٔ اینترنت

---

۱. این سرویس که یکی از متداول‌ترین مخلوط‌کن‌ها محسوب می‌شود، به تمام رمزارزهای ورودی، یک برچسب یکتا اختصاص می‌دهد و امکان دریافت مجدد رمزارز ارسالی توسط کاربر را از بین می‌برد.

۲. ویژگی کلیدی این میکسِر، مخلوط‌کنندگی سرویس، همراه با تعامل آن با صرافی‌های جهانی است. بنابراین، پس از یک اختلاط کلاسیک، کوین‌ها به یکی از صرافی‌های بزرگ ارسال می‌شوند و در آنجا، با کوین‌های سایر معامله‌گران، تعویض می‌شوند (Goriacheva *et al*, 2018: 48).

۳. کاربرانی که قصد استفاده از سرویس کوین‌جوین را دارند، اَعمال خود را همگام کرده، یک تراکنش مشترک با ورودی و خروجی‌های متعدد ایجاد کرده و نتیجهٔ نهایی را امضا می‌کنند. وجوهی که از مبدأهای مختلف آمده‌اند، در یک بستهٔ مشترک ادغام شده و سپس به آدرس‌های دیگر ارسال می‌شوند (Goriacheva *et al*., 2018: 48).

۴. دارک‌والِت نیز نوعی کیف پول مبتنی بر وب و در واقع سرویسی است که ویژگی‌های میکسینگ را در کیف پول کاربر ادغام می‌کند. دارک‌والت با ترکیب تراکنش‌های تصادفی همزمان و سپس رمزگذاری اطلاعات گیرندگان برای ظاهر نشدن اطلاعات در بلاک‌چین، تشخیص هویت را با اختلال مواجه می‌کند (Greenberg, 2014, A).

نامرئی (I2P) می‌توانند با افزایش ابهام تراکنش‌ها، توانایی خدمات‌دهنده در شناخت مشتریانش و اجـرای مؤثر اقدامات ضدپول‌شویی و ضد تأمین مالی تروریسم سلب کنند (FATF, 2019: 13). در ادامه شـیوهٔ دیگر گمنامی یعنی وب پنهان بررسی می‌شود.

۴. ۲. وِب پنهان[1]

از دیگر فناوری‌هایی که می‌تواند در راستای گمنام کردن تراکنش‌های رمزارز برای تأمین مالی تروریسـم استفاده شود، حوزهٔ وب پنهان است. وِب پنهان، مجموعه‌ای از هزاران وبسایت با آدرس‌های IP مخفی و رمزگذاری‌شده است. وِب پنهان خود از دو بخش دیپ‌وِب[2] و دارک‌وب تشکیل مـی‌شـود. همـان‌طورکـه می‌دانیم اینترنت[3] به‌عنوان شبکهٔ بین‌المللی، مجموعهٔ گسترده‌ای[4] از رایانه‌های موجود در جهان است کـه از میلیون‌ها رایانهٔ شخصی و تجهیزات مخابراتی متصل به هم تشکیل شده که در بستر آن اطلاعات بـه اشتراک گذارده شده و با هم مرتبط می‌شوند (بابایی، ۱۴۰۰: ۲۸). عموم مردم، اینترنت را با سـایت‌هـایی مانند گوگل و یاهو و امثال آن می‌شناسند و از آن برای انجام امور روزانهٔ خود یا جست‌وجـوی اطلاعـات استفاده می‌کنند. این در حالی است که اینترنت روی تاریک‌تری نیز دارد. در واقع، فقط بخش کـوچکی از ترافیک اینترنت متعلق به این‌گونه سایت‌ها و امور است. طبق برخی معیارها، آنچه در گوگـل بـه عنـوان اینترنت نمایه‌گذاری می‌شود، حداکثر ۴۰ درصد اینترنت است. این در حالی است که میلیـون‌هـا وبسـایت وجود دارند توسط موتورهای جست‌وجو مانند گوگل نمایه نمی‌شوند، مگـر اینکـه کـاربر، آدرس پروتکـل اینترنتی (شمارهٔ خاصی که رایانه را در اینترنت معرفی می‌کند) آنها را بداند. این حـوزهٔ ناشـناخته، همـان «دیپ‌وِب» یا وب عمیق است (Singletary, 2015: 108). دیپ‌وب به‌سبب فلسـفهٔ ایجـاد و همچنـین ساختار و ویژگی‌های فنی خود، سطح بالایی از گمنامی و امنیت را بـه‌همـراه دارد کـه محیطـی مناسـبی برای ارتکاب جرائم در سطح بین‌المللی را ایجاد کرده است. مطابق برخی مطالعات، تنهـا تـا سـال ۲۰۱۰ حدود صد هزار وب‌سایت حاوی محتوای تروریستی و افـراط‌گـری در ایـن بخـش فعـال بـود (فیضـی و رنجبریان، ۱۴۰۱: ۸۸). بیشتر کلاه‌برداری‌ها، تهدیدات پیشرفته، بـدافزارها و مجرمـان مـالی ماننـد افـراد فعالی در حوزهٔ پول‌شویی و تأمین مالی تروریسم در دیپ‌وِب سکنی گزیده‌اند. البته دیپ‌وب، یـک بخـش عمیق‌تر نیز دارد که دارک‌وب[5] است.

---

1. Hidden Web
2. Deep Web

۳. Internet مخفف International Network است.

4. Wide Area Network, (WAN)
5. Dark Web

دارک‌وب یا دارک‌نِت، عمیق‌ترین بخش دیپ‌وِب و از لحاظ دسترسی نیز سخت‌ترین بخش آن است. دارک‌نِت سطحی از اینترنت است که تنها افراد آشنا به دانش روز رایانه در آن حضور دارند و محل رشد و فعالیت انواع هکرهاست. تفاوت اصلی میان دارک‌وب و دیپ‌وب، جدا از کیفیت و توانایی مجرمان حاضر در آن، نحوهٔ دسترسی به آن است. اما علت اینکه نگارنده به موضوع دارک‌وب اشاره کرد این است که این بخش می‌تواند به‌عنوان فضایی به‌کار رود تا بر ویژگی گمنامی تراکنش‌های رمزارزها بیفزاید و در نتیجه چراغ سبزی برای استفادهٔ پایدار تروریست‌ها از این‌گونه دارایی‌ها باشد. در دارک‌وب، امکان خرید اقلامی وجود دارد که برای فعالیت‌های تروریستی مناسب است و در واقع این محل به فضای مخفی برای انتشار محتواهای افراط‌گرایانه تبدیل شده‌اند (Moore *et al.*, 2016). بر اساس گزارش ۲۰۱۶ واحد اطلاعاتی مالی بلژیک، استفاده از ارزهای مجازی برای پرداخت تجارت غیرقانونی در دارک‌وب در حال افزایش است که از آن جمله می‌توان به خرید اسناد هویت جعلی و بلیت‌های هواپیمایی از سوی تروریست‌ها اشاره کرد (CTIF-CFI, 2016: 41). دارک‌وب همچنین می‌تواند بازار سودمندی برای خرید تسلیحات از سوی سلول‌های کوچک تروریستی باشد. در ارزیابی ملی ریسک‌های پول‌شویی و تأمین مالی تروریسم ۲۰۱۷ بریتانیا، به امکان خرید و فروش سلاح‌های گرم در دارک‌وب با استفاده از رمزارزها اشاره شده است (HM Treasury and the Home Office, 2017: 40-41). همچنین در گزارش ۲۰۱۸ مؤسسه Flemish Peace، اشاره شده است که تهیهٔ سلاح‌های گرم از دارک‌وِب، برای گروه‌های تروریستی بسیار محتمل است و بر اساس نظر «دفتر دادستان فدرال بلژیک»، این احتمال در میان گرگ‌های تنها[1] که به بازارهای شناخته‌شده و فیزیکی سلاح دسترسی ندارند، بسیار بیشتر خواهد بود (Duquet, 2017: 59).

مطابق گزارش تحلیلگران مستقل امنیت سایبری در ژانویهٔ ۲۰۱۵، یک هوادار داعش به هویت ابومصطفی با راه‌اندازی یک صفحهٔ جذب سرمایه در دارک‌وِب، توانست حدود ۱۰۰۰ دلار کمک جذب کند (Harman, 2015). همچنین طبق گزارش یکی از نهادهای نظارتی، برخی از افراط‌گرایان غربی، برای دسترسی به انواع سلاح، مواد منفجره و آشنایی کار با آنها، به‌صورت مداوم به دارک‌وِب مراجعه می‌کنند (Maxey, 2018). در سال ۲۰۱۶ نیز یک بلژیکی با این ادعا که می‌خواهد از خانواده‌اش در مقابل داعش محافظت کند، به اتهام سفارش سلاح گرم از دارک‌وب متهم شد (Duquet, 2017: 59). تحلیلگران مؤسسهٔ «راند» نیز به این نتیجه رسیدند که اگرچه مقیاس خرید و فروش سلاح در دارک‌وب، در مقایسه با بازارهای دارو، نسبتاً کوچک است، اما تأثیر بالقوه معناداری بر امنیت دارد (Judith & et.al,

---

۱. منظور از «گرگ‌های تنها» نوعی از تروریست‌ها هستند که اغلب به‌صورت انفرادی عملیات انجام می‌دهند، عموماً از یک گروه تروریستی مرکزی الهام می‌گیرند، اما هیچ‌گونه ارتباط رسمی با این گروه‌ها ندارند.

14 :2017). در واقع دارک‌وِب، با حذف موانع جغرافیایی که در گذشته بـر سـر راه تجـارت اسـلحه قـرار داشت، صرفاً با چند کلیک امکان خرید و فروش بین نقاط مختلف دنیا را فراهم کرده است (کدخـدایی و نوروزپور، ۱۳۹۹: ۱۹). حال استفاده از رمزارزها برای مبـادلات در بازارهـای دارک‌وب در راسـتای پنهـان سازی هویت و دشواری ره‌گیری به کمک آنها آمده است. مطابق تحقیقی از دارک‌وب برای پنهان کردن حمایت افراد و کشورهای معروف و برجسته از گروه‌های تروریستی استفاده شده است و اطلاعاتی وجـود دارد مبنی بر اینکه برخی کشورهای بزرگ از این طریق با پنهان کردن تراکنش‌های رمزارزی به داعـش کمک مالی کرده‌اند (Ozkaya & Islam, 2019: 43). همچنین کارگروه تبادل اطلاعات گروه اگمونت[1] در ژوئن ۲۰۲۳ سندی تحت عنـوان «سوءاسـتفاده از دارایـی‌هـای مجـازی بـرای اهـداف تـأمین مـالی تروریسم» منتشر کرد که در آن به‌طور خاص به نقش واحدهای اطلاعات مالی در مقابله با تـأمین مـالی تروریسم از طریق رمزارزها اشاره شده است. این پروژه در مورد سوءاستفاده از دارایی‌های مجـازی بـرای اهداف تأمین مالی تروریسم و همچنین معرفی بهترین شـیوهٔ ممکـن بـرای جلـوگیری از سوءاسـتفاده از دارایی‌های مجازی طراحی شده است. در این گزارش اشاره می‌شود که متـداول‌تـرین روش پرداخـت در برخی پلتفرم‌های دارک‌نت، رمزارزها و به‌خصوص محبوب‌ترین آنها، یعنی بیت‌کـوین اسـت (Egmont, 2023: 7-8). در ادامه سومین شیوهٔ ارتقای سطح گمنامی رمزارزهـا یعنـی اسـتفاده از آلـت کـوین‌هـای حریم‌محور بررسی می‌شود.

۴. ۳. آلت‌کوین‌های حریم محور[2]

اگر رمزارز بیت‌کوین را نخستین کوین یا سکه در حوزهٔ ارزهای مجازی بدانیم، منظور از آلت‌کوین تمامی رمزارزهایی است که بعد از بیت‌کوین به‌وجود آمده‌اند. به‌عبارت دیگر به هر رمـزارزی غیـر از بیـت‌کـوین به‌طور کلی آلت‌کوین گفته می‌شود و در این قسمت منظور از آلت‌کوین‌های حریم‌محور یـا خصوصـی آن دسته از رمزارزهایی است که با هدف مخفی نگه‌داشتن هویت کاربر و تراکنش‌های او طراحـی شـده‌انـد. به‌طور کلی، آلت کوین‌های حریم محور دسته‌ای از رمزارزها هستند که با پنهـان سـاختن مبـدأ و مقصـد تراکنش‌ها سعی دارند تراکنش‌های صورت‌گرفته در بلاک‌چین را ناشناس کنند. به‌عبارت دیگر این دسـته از کوین‌ها دارای دو ویژگی غیرقابل شناسایی و غیرقابل ردیابی هستند. در جنبـهٔ ناشـناس بـودن، اغلـب هویت فرد پشت تراکنش مخفی می‌ماند و در جنبهٔ غیرقابل ردیابی بودن نیز عمل ردگیری تراکنش‌ها بـا

---

۱. گروه اگمونت در سال ۱۹۹۵ در بروکسل با حضور ۲۴ کشور و ۸ سازمان بین‌المللی تشکیل شد. هدف این گروه، ایجاد یک محل اجتماع برای واحدهای اطلاعات مالی، جهت حمایت و پشتیبانی از برنامه‌های مبارزه با پول‌شویی و هماهنگی ابتکارعمل‌ها در امر مبارزه با پول‌شویی و تأمین مالی تروریسم است.

2. Privacy Coins

استفاده از اقداماتی نظیر تحلیل بلاکچین از سمت شخص ثالث غیرممکن می‌شود (آهنگری، ۱۴۰۰). رمزارزهای «مونرو»، «دَش» و «زِدکَش» شاخص‌ترین آلت‌کوین‌های حریم‌محور در دنیای امروزند.

مطابق پژوهش‌های جدید، آلت‌کوین‌های حریم‌محور، در حال کسب محبوبیت میان مجرمان هستند. در گزارش اکتبر ۲۰۱۷ یوروپُل در خصوص ارزیابی تهدیدات جرائم اینترنتی سازمان‌یافته[1]، شواهدی از استفادهٔ مجرمان از آلت‌کوین‌های حریم‌محور، به‌خصوص مونرو، ارائه شده و در یکی از مطالعات آکادمیک در ایالات متحده نیز تخمین زده شده است که حدود ۲۵ درصد از تمام فعالیت‌هایی که با رمزارز مونرو انجام می‌شود، غیرقانونی‌اند (Moser *et al.*, 2017: 1). یک نمونه از استفادهٔ مجرمانه از مونرو، در آگوست ۲۰۱۷ روی داد که در آن تدارک‌دهندگان حملهٔ باج‌افزار WannaCry از طریق صرافی رمزارز Shape Shift در سوئیس، بیت‌کوین غیرقانونی خود را با مونرو مبادله کردند. در میان افراط‌گرایان و تروریست‌ها نیز استفاده از رمزارزهای حریم‌محور سودمند تلقی می‌شود. مطابق تحقیقی، افراط‌گرایان برای غلبه بر ویژگی‌های قابلیت ردیابی در بیت‌کوین، استفاده از مونرو را افزایش داده‌اند (Suberg, 2017). بر اساس گزارشی دیگر، شواهدی وجود دارد که کمپین تروریستی «اَل‌صدقه»، از هواداران خود خواسته است که برای سرمایه‌گذاری در یک پروژهٔ ساخت تأسیسات در استان لاذقیه سوریه، کمک‌های خود را از طریق رمزارز و به‌طور گمنام و امن ارسال کنند (Fanusie, 2018: 6).[2] همچنین در اکتبر ۲۰۱۸، «بنیاد ابو احمد» که یک مؤسسهٔ خیریهٔ افراطی حامی گروه تروریستی تحریرالشام در اندونزی است، اقدام به جمع‌آوری سرمایه از طریق رمزارز می نمود و حامیان خود را تشویق به ارائهٔ کمک مالی از طریق رمزارزهای حریم‌محور مانند مونرو و دش می‌کرد (Wardhana & Nugroho, 2021: 5). در اوایل سال ۲۰۲۱ نیز یک کانال برجستهٔ تلگرامی که مطالب مرتبط با افراط‌گرایان خشونت‌آمیز را تبلیغ می‌کرد، تصویری گرافیکی همراه با متن را منتشر کرد که در آن استفاده از ارز دیجیتال مونرو را تبلیغ می‌کرد. همین کانال پیشتر راهنمای ۳۴ صفحه‌ای را با عنوان «ارز رمزنگاری‌شده؛ راهنمای عملی برای حریم خصوصی و امنیت» منتشر کرده بود (JCAT, 2021: 3). با این حال نتیجه‌گیری قطعی دربارهٔ حجم کلی فعالیت‌های تروریستی که ممکن است با آلت‌کوین‌های حریم‌محور انجام شوند، دشوار است.

در پایان این بخش باید گفت که دسترسی به رمزارزهای حریم‌محور و نقد کردن آنها همچنان دشوار است، زیرا صرافی‌های رمزارزی که این نوع کوین‌ها را به کاربران عرضه می‌کنند، محدودند. به‌علاوه اینکه، این صرافی‌ها با اعمال اقداماتی نظیر شناسایی کامل مشتری، ممکن است مزایای گمنامی

---

1. IOCTA

۲. از حساب توییتر این سازمان، مشخص است که در حال حاضر آلت‌کوین‌های حریم‌محور مونرو، دَش را قبول می‌کند.

این‌گونه ارزها را از بین ببرند. همچنین با توجه به عمومیت نداشتن این دسته از رمزارزها، در بیشتر موارد برای خرید و فروش آلت‌کوین‌ها و مبادلهٔ آنها با ارز واقعی، ابتدا باید آنها را به بیت‌کوین یا رمزارز معتبر دیگر تبدیل کرد و سپس دوباره رمزارز جدید دریافتی را مبادله کرد و این وابستگی سبب می‌شود که در نهایت برخی از مزایای گمنامی در مسیر تراکنش‌ها، کاهش یابند. در تأکید این گزاره، نمایندهٔ ویژهٔ سازمان مبارزه با مواد مخدر ایالات متحده طی مصاحبه‌ای اظهار کرد که رمزارزهای حریم‌محور مانند مونرو و زدکش می‌توانند جایگزین جذابی برای خلافکاران باشند، اما در حال حاضر گستردگی و نقدینگی آنها در حدی نیست که خیلی به‌کار روند (ناصر فلاح، ۱۳۹۸). با این حال کمیتهٔ ضدتروریسم شورای امنیت در دسامبر ۲۰۲۲ طی گزارشی که در آن به خلأهای اجرایی قطعنامه‌های شورای امنیت سازمان ملل در خصوص مبارزه با تأمین مالی تروریسم مرتبط پرداخته شده، در یکی از فصل‌های خود اشاره کرد که تروریست‌ها همچنان به سوءاستفاده از سیستم‌های پرداخت موبایلی، دارایی‌های مجازی از جمله بیت‌کوین و آلت‌کوین‌های حریم‌محور مشغول هستند، ازاین‌رو درک ماهیت و دامنهٔ دقیق این سوءاستفاده‌ها برای حوزه‌های قضایی ضروری است و نقش مهمی در گسترش مقررات مناسب دارد (Counter-Terrorism Committee Executive Directorate, 2022: 16). در ادامه ویژگی گمنامی در اسناد بین‌المللی مقابله با تأمین مالی تروریسم بررسی می‌شود.

۵. گمنامی در اسناد بین‌المللی و ضرورت مقابله با آن

همان‌طورکه توضیح داده شد، گمنامی، یک از فاکتورهای بارز در دارایی‌های مجازی محسوب می‌شود و از همین رو بسیاری از مجرمان مالی از جمله تروریست‌ها برای جذب، سرمایه‌گذاری و نقل و انتقال منابع مالی خود از رمزارزها استفاده می‌کنند تا حتی‌الامکان از ره‌گیری ناظران قانونی به دور باشند. به همین سبب سازمان‌ها و نهادهای بین‌المللی فعال در حوزهٔ مبارزه با پول‌شویی و تأمین مالی تروریسم به این مسئله توجه داشته و با وضع دستورالعمل‌هایی سعی دارند به مقابله با این پدیده و کنترل آن بپردازند که در ادامه اشاره می‌شود.

در ابتدا باید اشاره کرد که تا اواسط دههٔ ۱۹۹۰، تأمین مالی تروریسم جزو عناصر اصلی مقابله با تروریسم در نظر گرفته نمی‌شد. در سال ۱۹۹۶ برای نخستین بار بود که مجمع عمومی سازمان ملل با تصویب یک قطعنامه، منابع مالی مشروع و نامشروع سازمان‌های تروریستی را مشخص و اشاره کرد که گروه‌های تروریستی، مرتکب جرائم سازمان‌یافته با سوءاستفاده از سازمان‌های خیریه می‌شوند. پس از این اقدام، کنوانسیون بین‌المللی سازمان ملل برای سرکوب تأمین مالی تروریسم در سال ۱۹۹۹ به تصویب رسید که نخستین کنوانسیونی بود که بر موضوع تأمین مالی تروریسم متمرکز شد و در مورد نحوهٔ کمک به همکاری‌های بین‌المللی و سرمایه‌گذاری در زمینهٔ پیگرد اعمالی که در دستهٔ تأمین مالی تروریسم قرار

می‌گیرند، تأکید شد. شورای امنیت سازمان ملل نیز تا قبل از حوادث ۱۱ سپتامبر در ۱۲ قطعنامه، تروریسم را مورد توجه قرار داده بود. اما پس از حمله‌ای که در ۱۱ سپتامبر ۲۰۰۱ در ایالات متحده اتفاق افتاد، مقابله با تروریسم و تأمین‌مالی آن به یکی از اولویت‌ها تبدیل شد. گستردگی ابعاد حملات تروریستی ۱۱ سپتامبر و حجم امکانات و منابع تخصیص‌یافته برای اجرای آن نشان داد که تا چه اندازه نگرانی از تأمین و تقویت گروه‌ها و سازمان‌های تروریستی بجا و قابل درک است (زرنشان، ۱۳۸۶: ۷۹). پس از این حادثه، شورای امنیت با تصویب قطعنامهٔ ۱۳۷۳، کمیتهٔ مقابله با تروریسم را تشکیل داد و چندین موضوع به اقدامات موجود در مقابله با تأمین مالی تروریسم افزوده شد. این قطعنامه حکومت‌ها را به سرکوب تأمین مالی تروریسم و مسدودسازی همهٔ دارایی‌های تروریست‌ها فرا خواند و حکومت‌ها، سازمان‌ها یا افراد را از تأمین سرمایه برای گروه‌های تروریستی برحذر داشت و تمامی دولت‌ها را به جرم‌انگاری تأمین یا جمع‌آوری سرمایه به قصد استفادهٔ تروریستی، فرا خواند. همچنین طبق این قطعنامه، دول عضو باید وجوه و سایر دارایی‌های مالی یا منابع اقتصادی اشخاصی را که مرتکب، یا در تلاش برای ارتکاب اقدامات تروریستی هستند، یا در ارتکاب یا تسهیل این اقدامات شرکت دارند، بدون تأخیر مسدود سازند. در این قطعنامه، به همکاری بین‌المللی علیه تروریسم اشاره می‌شود و تمام دول عضو را به همکاری علیه تروریسم از طریق توافقات دو و چندجانبه و عضویت در کنوانسیون‌ها و پروتکل‌های بین‌المللی مرتبط با تروریسم، فرا می‌خواند (S/RES/1373). همچنین در بخشی از این قطعنامه آمده که تمامی دولت‌ها باید اتباع و ساکنان قلمرو حاکمیتی خود را از فراهم آوردن هرگونه تسهیلات سرمایه‌ای، تأمین اعتبار، تهیهٔ منابع مالی یا دیگر سازوکارهای مالی مرتبط در ارتباط با تأمین مالی تروریسم ممنوع سازند. به عقیدهٔ برخی نویسندگان عبارت «سایر سازوکارهای مالی مرتبط» قابل تعمیم به دارایی‌های مجازی و از جمله رمزارزهاست (Shah, 2007: 201). در ادامه شورای امنیت در قطعنامه‌های دیگری از جمله قطعنامه‌های ۱۹۶۳، ۲۱۶۰، ۲۱۶۱، ۲۳۷۰ بر اهمیت استفاده از اینترنت و فناوری‌های جدید به‌منظور تأمین مالی تروریسم تأکید کرد. اما اولین و تاکنون (مارس ۲۰۲۴) تنها قطعنامهٔ شورای امنیت که به‌صراحت به استفاده تروریست‌ها از رمزارزها اشاره و در خصوص آن ابراز نگرانی کرده است، قطعنامهٔ ۲۴۶۲ است که در مارس ۲۰۱۹ به تصویب رسید. در این قطعنامه، از کشورها درخواست شده تا استانداردهای گروه ویژهٔ اقدام مالی در خصوص مبارزه با تأمین مالی تروریسم و پول‌شویی را اجرا و تمام حوزه‌های اقتصادی را که می‌توانند بالقوه و غیرمستقیم به تأمین مالی تروریسم کمک کنند، بررسی کنند. بند ۱۵ اجرایی قطعنامه نیز از دولت‌ها می‌خواهد تا در سطح ملی چارچوبی ایجاد کنند که طی آن اشخاص ذی‌صلاح ملی و به‌طور مشخص واحدهای اطلاعات مالی، سرویس‌های اطلاعاتی، مجریان قانون، مقامات قضایی و کیفری بتوانند به جمع‌آوری و اشتراک اطلاعات در زمینهٔ تأمین مالی تروریسم در حوزهٔ رمزارزها بپردازند.[1]

1. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/090/16/PDF/N1909016.pdf?OpenElement

کمیتهٔ ضدتروریسم شورای امنیت نیز در دسامبر ۲۰۲۲ در جلسات کارشناسی که به همت دبیرخانهٔ اجرایی کمیتهٔ ضدتروریسم سازمان ملل[1] برگزار می‌شد، نمونه‌هایی از روش‌های جذب سرمایه برای مقاصد تروریستی را مورد بحث قرار داد. از جمله سوءاستفاده از شبکه‌های اجتماعی برای جذب کمک مالی، خدمات میزبانی محتوا، فروش آنلاین کالا و پلتفرم‌های سرمایه‌گذاری جمعی[2] که اغلب برای پنهان‌سازی کاربرد وجوه استفاده می‌شوند. کمیتهٔ ضدتروریسم در این گزارش خلأهای مهم در حوزهٔ دارایی‌های مجازی را شناسایی کرده که یکی از آنها روند کند معرفی و اجرای مقررات مقابله با پول‌شویی و تأمین مالی تروریسم و نظارت بر آن برای اطمینان از شمول تمام انواع خدمات‌دهندگان دارایی‌های مجازی است. از نظر کمیته، استفادهٔ رو به رشد از روش‌های غیرمتمرکز تأمین مالی، توکن‌های غیرقابل تعویض و کیف پول‌های بدون میزبان، پیاده‌سازی اقدامات مقابله‌ای را بیش از پیش چالش‌برانگیز ساخته است. در انتقال وجوه فرامرزی و گمنام که همتابه‌همتا بوده و هیچ خدمات‌دهنده‌ای در آنها مشارکت ندارد، خطرهای بیشتر نیز می‌شود. ازاین‌رو کمیته تأکید می‌کند که نیاز به مقررات جهانی و هماهنگ و اجرای منسجم «قانون حرکت دارایی‌های مجازی از مبدأ تا مقصد»[3] در حوزه‌های قضایی، احساس می‌شود تا بتوان به‌صورت دقیق این حوزه را کنترل و مدیریت کرد (Counter-Terrorism Committee Executive Directorate, 2022: 17). در جدیدترین اقدام، در صدوهجدهمین جلسهٔ کنگرهٔ آمریکا، مقرراتی برای رسیدگی به جنبه‌های خاصی از رمزارزها به تصویب رسید. برای مثال دو نسخه از قانون اختیارات دفاع ملی برای سال مالی ۲۰۲۴ (HR 2670 و S.2226)، ناظران بانکی و تنظیم‌کننده‌های فدرال را ملزم به ایجاد استانداردهای بررسی مبارزه با پول‌شویی و تأمین مالی تروریسم برای مؤسسات مالی مرتبط با دارایی‌های رمزنگاری می‌کنند. لوایح قانون اختیارات دفاع ملی، همچنین وزارت خزانه‌داری را ملزم می‌کند تا در خصوص خدمات ناشناس‌سازها مانند میکسرها به کنگره گزارش دهد و سیاست‌ها برای جلوگیری از استفاده از آنها توسط بازیگران غیرقانونی توصیه کند (Tierno *et al*., 2023: 3).

مجمع عمومی سازمان ملل متحد هم در جدیدترین اقدام خود در قطعنامهٔ شمارهٔ ۷۷/۲۹۸ مورخ ۲۲

---

1. CTED

۲. Crowdfunding یا سرمایه‌گذاری جمعی یا تأمین مالی جمعی روشی نوین در حوزهٔ تأمین مالی است. این روش که در جهان بسیار مورد توجه کسب‌وکارها و همچنین سرمایه گذاران قرار گرفته، روشی است که با مشارکت تعداد زیادی سرمایه‌گذار، تمام یا بخشی از سرمایهٔ مورد نیاز یک طرح، پروژه یا یک فعالیت مشخص جمع‌آوری می‌شود.

۳. Travel Rule یا قانون حرکت که از ابداعات گروه ویژهٔ اقدام مالی است، بدین‌معناست که هنگام انجام یک تراکنش مالی در یک صرافی، همزمان با انجام تراکنش، اطلاعات کاربر انتقال‌دهنده نیز باید همراه با مشخصات تراکنش انتقال پیدا کند و تمامی این اطلاعات در سامانهٔ یکپارچه به اشتراک گذارده شود.

جون ۲۰۲۳ به موضوع تأمین مالی تروریسم از طریق دارایی‌های مجازی پرداخت. در این قطعنامه ضمن تأکید مجدد بر تعهد کشورهای عضو برای جلوگیری و سرکوب تأمین مالی اقدامات تروریستی و خودداری از هرگونه حمایت از نهادها یا افراد درگیر در اقدامات تروریستی، نسبت به سوءاستفاده از اینترنت و سایر فناوری‌های اطلاعاتی و ارتباطاتی از جمله دارایی‌های مجازی و سیستم‌های پرداخت موبایلی ابراز نگرانی کرد و در این زمینه از همهٔ کشورهای عضو خواسته شد تا اقدامات بیشتری را برای مقابله با استفاده از این فناوری‌ها برای اهداف تروریستی در نظر بگیرند. در این قطعنامه همچنین بر چالش گمنامی و پنهان‌سازی هویت در حوزهٔ رمزارزها اشاره و از کشورهای عضو درخواست شد تا تلاش‌های خود را در مبارزه با تأمین مالی تروریسم از طریق رسیدگی به ناشناس بودن تراکنش‌ها و با ردیابی، شناسایی، تحریم و از بین بردن انتقال‌دهندگان غیرقانونی وجوه و مقابله با خطرهای مرتبط با استفاده از پول نقد و سیستم‌های حواله غیررسمی، افزایش دهند (UNDOC, 2023).

در اتحادیهٔ اروپا نیز اقدامات گسترده‌ای برای جلوگیری از سوءاستفادهٔ تروریستی از رمزارزها به‌ویژه در بخش گمنامی زدایی صورت گرفته است. انتشار گزارشی در خصوص ارزهای مجازی توسط بانک مرکزی اروپا (ECB)[1] در اکتبر ۲۰۱۲، نخستین تلاش کلی اتحادیهٔ اروپا برای پرداختن به مسئلهٔ رمزارزها بود. بانک مرکزی اروپا در واکنش به این پدیدهٔ نوظهور، میزان گمنامی فراهم‌شده توسط رمزارزها را از نظر تأمین مالی تروریسم، خطرآفرین دانست. طبق این گزارش، اگرچه تنظیم مقررات سرویس‌دهندگان ارزهای مجازی، راه‌حل کاملی برای مقابله با این ریسک‌ها نیست، اما تنظیم مقررات حداقل سبب کاهش انگیزهٔ تروریست‌ها، مجرمان و پولشویانی است که به‌دنبال استفاده از این طرح‌ها برای مقاصد غیرقانونی‌اند (European Central Bank, 2012). در جولای ۲۰۱۴، این نهاد با انتشار نظر رسمی خود در خصوص ارزهای مجازی، اعلام کرد که ارزهای مجازی، به‌سبب امکان پول‌شویی و تأمین مالی تروریسم، برای یکپارچگی مالی اتحادیهٔ اروپا بسیار خطرآفرین هستند، ازاین‌رو برای کاهش این ریسک‌ها، باید صرافی‌های ارز مجازی را به رعایت دستورالعمل‌های مبارزه با پول‌شویی اتحادیهٔ اروپا ملزم کرد (European Banking Authority, 2014). پس از حملهٔ تروریستی داعش در نوامبر ۲۰۱۵ در پاریس، کمیسیون اروپایی که در واقع مغز متفکر و طراح دستورالعمل‌ها و مقررات در سطح اتحادیهٔ اروپاست، در فوریهٔ ۲۰۱۶ قصد خود را برای اصلاح دستورالعمل چهارم مبارزه با پول‌شویی (4AMLD) و لحاظ کردن ریسک‌های مختلف تأمین مالی تروریسم نشان داد (Keatinge & Tom *et al.*, 2018: 24). کمیسیون، با ارائهٔ یک پیش‌نویس رسمی در جولای ۲۰۱۶، پیشنهادهای خود را مطرح کرد که از آن جمله شمول دستورالعمل، بر پلتفرم‌های مبادلات ارزهای مجازی و ارائه‌دهندگان خدمات کیف پول

1. The European Central Bank

امانی بود (فتحی‌زاده و اسماعیلی عطاآبادی، ۱۳۹۹: ۷۴). در نهایت در دسامبر ۲۰۱۷، پارلمان و شورای اروپا، بر سر متن پنجمین دستورالعمل مبارزه با پول‌شویی توافق کردند و در ۱۴ می ۲۰۱۸، شورای اتحادیهٔ اروپا این دستورالعمل را تصویب کرد (Council of the EU, 2018). در اصلاحیهٔ پنجم دستورالعمل، دایرهٔ نهادهای مالی مسئول در حوزهٔ دارایی‌های مجازی گسترش یافت و «ارائه‌دهندگان خدمات مالی در تبادل بین ارزهای مجازی و ارزهای فیات و همچنین ارائه‌دهندگان خدمات کیف پول امانی به‌عنوان نهادی که خدمات محافظت از کلیدهای رمزنگاری‌شدهٔ خصوصی مشتریانش را انجام می‌دهد و آنها را حفظ، نگهداری، ذخیره و انتقال می‌دهد نیز مشمول الزامات دستورالعمل قرار گرفتند. نحوه فعالیت ارائه‌دهندگان خدمات مبادلات ارزهای مجازی و کیف پول‌های امانی، تحت شمول الزامات قانونی قرار گرفته و مشابه بانک‌ها و مؤسسات مالی تلقی شدند و در نتیجه ملزم به پیروی از مقررات مربوط به مبارزه با پول‌شویی و تأمین مالی تروریسم هستند. ازاین‌رو نهادها یا مؤسساتی که خدمات مالی در خصوص ارزهای مجازی ارائه می‌دهند، باید نزد مراجع قانونی کشور متبوع به ثبت رسیده باشند و استانداردهای ناظر بر کنترل‌های مربوط به مشتریان و معاملات ارزهای مجازی را رصد کنند و در نهایت هنگام برخورد با موارد مشکوک به پول‌شویی و یا تأمین مالی تروریسم چنین مواردی را به نهادهای دولتی ذی‌ربط گزارش دهند (Houben & Snyers, 2018).

گروه ویژهٔ اقدام مالی نیز از جمله نهادهای بین‌المللی است به‌صورت مستمر و پویا، تحولات رمزارزها در حوزهٔ تأمین مالی تروریسم را مدنظر دارد و به‌طور خاص بر اهمیت شناخت و کنترل گمنامی این پدیده تأکید می‌کند. این کارگروه با انجام مطالعهٔ جامعی در سال ۲۰۱۰، اعلام کرد که استفادهٔ غیرقانونی از روش‌های پرداخت جایگزین در حال افزایش بوده و یکی از قابلیت‌های چالشی این فناوری‌های جدید، «گمنام ماندن کاربران» است (FATF, 2010). در ژوئن ۲۰۱۹ گروه ویژهٔ اقدام مالی «راهنمای رویکردهای ریسک‌محور برای دارایی‌های مجازی و خدمات‌دهندگان این دارایی‌ها» را منتشر کرد. در این راهنما تأکید شده است که کشورها و ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی (صرافی‌ها)، باید هنگام شناسایی، ارزیابی و نحوهٔ کاهش خطرهای مرتبط با فعالیت‌های دارایی‌های مجازی به موارد زیر توجه داشته باشند: از جمله اینکه خطرهای مرتبط با کسب‌وکار خدمات‌دهندگان دارایی‌های مجازی را شناسایی کنند و همچنین رمزارزهای گمنام‌تر، میکسرها یا پشتک‌زن‌های تعبیه‌شده، یا سایر محصولات و خدماتی را که پتانسیل مبهم‌سازی تراکنش‌ها یا تضعیف توانایی خدمات‌دهنده در شناخت مشتریانش و در نتیجه تضعیف احراز هویت مؤثر مشتری پرخطرتر محسوب می‌شوند، مدنظر قرار دهند. بر اساس این راهنما، کشورها باید بر رفتار یا فعالیت مالی مرتبط با دارایی‌های مجازی یا فناوری زیربنایی این فعالیت‌ها، تمرکز کنند و پس از تشخیص خطرهای پول‌شویی و تأمین مالی تروریسم آنها مانند افزایش گمنامی، مبهم‌سازی، حذف واسطه‌ها و کاهش شفافیت، یا فناوری، پلتفرم‌ها، یا دارایی‌های

مجازی که سبب تضعیف توانایی خدمات‌دهنده برای مقابله با پول‌شویی و تأمین‌مالی تروریسم می‌شوند، اقدامات متناسب را اِعمال کنند (FATF, 2019: 20). همچنین گروه ویژهٔ اقدام مالی در گزارش سپتامبر ۲۰۲۰ خود، بر ارزیابی بایستهٔ مشتری، به‌منظور جلوگیری از استفادهٔ سازمان‌های تروریستی از دارایی‌های مجازی تأکید کرد (FATF, 2020).

۶. راهکارهای کاهش گمنامی در تراکنش‌های رمزارز

در بخش پیشین به ضرورت مقابله با گمنامی تراکنش‌های رمزارزها در اسناد بین‌المللی اشاره شد. هریک از نهادهای بین‌المللی در راستای مبارزه با گمنامی حاصل از تراکنش در بلاکچین و به‌طور خاص رمزارزها راهکارهایی را ارائه داده‌اند. اما به‌طور خاص می‌توان به راهکارهای زیر برای رفع گمنامی تراکنش‌های رمزارزها و در نتیجه مقابله با تأمین مالی تروریسم از طریق رمزارزها اشاره کرد.

همان‌طورکه توضیح داده شد، شاید تمرکززدایی مهم‌ترین مزیت این نوع ارزها باشد. در رمزارزها، هیچ نهاد مرکزی یا واسطه‌ای میان طرفین تراکنش وجود ندارد. هیچ مرجع یا مرکزی وجود ندارد که بتواند مانع دستیابی یک فرد به شبکهٔ بلاکچین و رمزارز شود. این ویژگی باز بودن، انعطاف‌پذیری و مقاومت در برابر سانسور همان چیزی است که برای افرادی که دنبال دسترسی بلامانع به روش‌های جذب سرمایه یا جابه‌جایی وجوه هستند، بسیار جذاب است. اما باید به این واقعیت عملی اشاره کرد که شبکه‌های رمزارز پر از واسطه‌های متمرکزند که تبادل میان رمزارزها و ارزهای واقعی را تسهیل می‌کنند. صرافی‌های رمزارز، سرویس‌دهندگان کیف پول امانی و ارائه‌دهندگان خدمات دارایی‌های مجازی از جملهٔ این واسطه‌ها هستند که اغلب به‌صورت متمرکز فعالیت می‌کنند؛ به این معنا که برای تبادل رمزارز در بستر آنها، ابتدا می‌بایست احراز هویت صورت گیرد و سپس یک کیف پول امانی در آن صرافی برای کاربر ایجاد شود. در نتیجه هر مبادله‌ای که صورت می‌گیرد، ابتدا وارد کیف پول کاربر در همان صرافی می‌شود و در مرحلهٔ بعد است که کاربر می‌تواند آن را به کیف پول شخصی خود انتقال دهد یا تبدیل به ارز واقعی کند. استفادهٔ تروریست‌ها از رمزارزها برای تأمین مالی تروریسم نیز تقریباً به همین شکل است، زیرا باید دانست که اقدامات تروریستی در نهایت در دنیای واقعی و به‌صورت محسوس بروز پیدا می‌کنند، ازاین‌رو انجام هر رویداد تروریستی، نیازمند تهیهٔ تجهیزات مادی نظیر مواد منفجره و تسلیحات در دنیای واقعی و محسوس است. بنابراین می‌توان با نظارت بر نقطهٔ اتصال رمزارزها با ارزهای واقعی که همان واسطه‌های متمرکزند، وضعیت گمنامی را کاهش داد. به این ترتیب می‌توان گفت مؤثرترین راهبرد برای دستیابی به این هدف، متمرکزسازی قواعد و مقررات نظارتی بر نهادهایی است که دروازهٔ ورود به عرصهٔ دارایی‌های مجازی یا خروج به عرصهٔ ارزهای واقعی محسوب می‌شوند. این دروازه‌ها که گره‌های سیستم

مالی و نوعی واسطه متمرکزند، نقش مؤثری در شناسایی مشتریان یا فعالیت‌های مشکوک دارند. بنابراین با وضع مقررات مناسب برای این واسطه‌ها جهت احراز هویت کاربران در این نهادهای مالی، می‌توان جنبهٔ گمنامی رمزارزها را کاهش داد.

روش دیگر پیشنهادی برای کاهش گمنامی تراکنش‌های رمزارز، استفاده از فناوری در مقررات‌گذاری و نظارت است. با توجه به ماهیت پویا، در حال تکامل و فنی رمزارزها، دولت‌ها و سازمان‌های بین‌المللی نباید به‌تنهایی و به همان شیوهٔ مقررات‌گذاری سنتی به مدیریت این حوزه اقدام کنند، بلکه وضع مقررات و تنظیم‌گری باید به‌گونه‌ای صورت گیرد که متناسب با ماهیت تخصصی این حوزه باشد و بتواند همگام با آن خود را به‌روزرسانی کند تا مقررات‌گذاری از جنبهٔ صرف اعمال ضمانت اجرا خارج شود و جنبهٔ پیشگیرانه نیز به خود بگیرد و سوءاستفاده برای پول‌شویی و تأمین مالی تروریسم در این حوزه را کاهش دهد. در این زمینه برخی از فعالان حوزهٔ رمزارزها اقدام به توسعهٔ برنامه‌ها و نرم‌افزارهایی کردند که آنها را در احراز هویت و تشخیص و ره‌گیری تراکنش‌های مشکوک به پول‌شویی و تأمین مالی تروریسم یاری می‌رساند. برای مثال یکی از شرکت‌های کارگزاری تبادل رمزارز، در کنار استفاده از روش‌های سنتی تشخیص تراکنش‌های مشکوک که به کشف حساب‌های اجاره‌ای[1] منجر می‌شود، از یک سیستم هوشمند برای بررسی الگوهای رفتار کاربران خود نیز بهره برده است. در برنامهٔ تعبیه‌شده از سوی این شرکت که خود مبتنی بر یک فناوری جدید است، با رصد شبانه‌روزی کاربران، رفتار آنها در بازار رمزارز بررسی و سپس الگوی رفتاری آن کاربر مشخص می‌شود. در این مرحله اگر رفتار کاربر با الگوهای مشکوک از قبل تهیه‌شدهٔ سیستم، مطابقت کند، حساب آن کاربر مشکوک به حساب اجاره‌ای و در نتیجه پول‌شویی یا تأمین مالی تروریسم تشخیص داده می‌شود که اقدامات ضدپول‌شویی شرکت علیه آن کاربر را فعال می‌کند (مصاحبه با رئیس هیأت مدیرهٔ شرکت تبادل رمزارز بیت‌پین، ۱۴۰۲). این شیوه را می‌توان نوعی استفاده از فناوری برای تطبیق با مقررات دانست که باید در راستای توسعهٔ آنها اقدامات لازم صورت گیرد.

۷. نتیجه

با توجه به نقش کلیدی منابع مالی در زنده و پویا نگاه داشتن گروه‌های تروریستی، جامعهٔ بین‌المللی همواره به‌دنبال ایجاد سازوکارهایی برای قطع منابع مالی تروریست‌ها بوده است. از همین رو، تلاش‌ها

---

۱. حساب اجاره‌ای به معنای استفاده از حساب‌های دیگران جهت انجام کارهای مالی، تراکنش مالی و کسب سود با رضایت خودشان است. در این حالت مجرمان مالی به‌جای اینکه از حساب‌های خود برای پول‌شویی استفاده کنند، در قبال پرداخت وجهی، از افراد درخواست ایجاد حساب در بانک یا صرافی می‌کنند و سپس پول دارای منشأ مجرمانه را وارد آن حساب کرده و سپس آن را به کالا یا رمزارز تبدیل می‌کنند.

برای مقابله با تروریسم و تأمین مالی تروریسم اغلب بر قطع جریان پول در سیستم رسمی و حساب‌های بانکی که ممکن بود به حمایت مالی از عملیات تروریستی بینجامد متمرکز شد. اما موفقیت در راهبردهای مقابله با تأمین مالی تروریسم در کاهش دسترسی تروریست‌ها به منابع مالی و به‌ویژه ارزهای فیات، این نگرانی و تهدید را افزایش داد که گروه‌های تروریستی برای تأمین مالی فعالیت‌های خود، به استفاده از نظام‌های مالی جایگزین ترغیب شوند که نمونهٔ بارز و امروزی آن رمزارزها هستند. اگرچه هنوز بسیاری از منابع مالی گروه‌های تروریستی از طریق روش‌های سنتی مانند قاچاق مواد مخدر تأمین می‌شود و از سویی از سیستم‌های تراکنش سنتی مانند حواله یا سازوکارهای انتقال پول نقد محور استفاده می‌کنند، اما استفادهٔ تروریست‌ها از رمزارزها نیز دور از ذهن نبوده و حتی وارد مرحله عملی نیز شده است. امکانات و ویژگی‌هایی که رمزارزها با خود به‌همراه دارند می‌تواند باعث ایجاد انگیزه در آنها برای استفاده از این فناوری شود. یکی از ویژگی‌های بارز در رمزارزها که کاملاً منطبق با اهداف تروریست‌هاست، گمنامی و ناشناس بودن است. با اینکه رمزارزها به لحاظ فنی و ساختاری مقادیری از امنیت و پنهان‌سازی هویت را به‌همراه دارد، اما روش‌های متعددی نیز وجود دارد که می‌تواند این ویژگی رمزارزها را تقویت کرده و در نتیجه آنها را به ابزاری شایان توجه و مفید برای سرمایه‌گذاری، تأمین منابع مالی و انتقال وجوه برای گروه‌های تروریستی تبدیل کند که به آن به‌عنوان رویکردی پایدار بنگرند. از جملهٔ این روش‌ها که در مقاله به‌تفصیل بررسی شد، ناشناس‌سازها، دارک‌وِب و استفاده از رمزارزهای حریم‌محورند که با ارائهٔ امکانات متعددی که همه‌روزه در حال پیشرفت و افزایش کیفیت است، خود را ابزاری مناسب هم برای سرمایه‌افزایی و هم‌بستری برای انتقال امن و گمنام وجوه و منابع مالی معرفی می‌کنند. با توجه به مطالعات صورت‌گرفته، نظر به اینکه پنهان‌سازی هویت و جلوگیری از بلوکه شدن منابع مالی، از مهم‌ترین دغدغه‌های گروه‌های مجرمانه از جمله تروریست‌ها و حامیان مالی آنهاست، می‌توان اذعان داشت، گمنامی عاملی بسیار مهم و کلیدی برای تروریست‌ها در جهت روی آوردن به بازار دارایی‌های جدید از جمله رمزارزهاست. گزارش‌هایی که استفادهٔ رمزارزهای حریم‌محور و دارک‌وب از سوی تروریست‌ها را نشان می‌دهد، حکایت از اهمیت ویژگی گمنامی در این‌گونه نظام‌های پرداخت جایگزین است و از همین رو نهادهای بین‌المللی در دستورالعمل‌های خود بر این جنبه از ماهیت رمزارزها تأکید می‌کنند و یکی از راه‌های جلوگیری از سوءاستفاده در رمزارزها را تضعیف جنبهٔ گمنامی با اتخاذ یکسری راهکارها می‌دانند. از جمله راهکارهای مورد اشاره در این مقاله، مقررات‌گذاری و نظارت دقیق بر واسطه‌های متمرکز اکوسیستم رمزارزها یعنی صرافی‌ها و ارائه‌دهندگان خدمات دارایی مجازی است. همچنین استفاده از فناوری مقرراتی می‌توان نقش مهمی در کاهش گمنامی و کشف هویت طرفین تراکنش رمزارز داشته باشد.

منابع

۱. فارسی

الف) کتاب‌ها

۱. بابایی، جواد (۱۴۰۰). *جرائم رایانه‌ای و آیین دادرسی حاکم بر آن*. تهران: ادارهٔ کل آموزش قوهٔ قضاییه.

۲. برنارد کوهن، سائول (۱۳۸۷). *ژئوپلوتیک نظام جهانی*. ترجمهٔ عباس کاردان، تهران: ابرار معاصر.

۳. دسوزا، جاش (۱۳۹۶). *تأمین مالی تروریسم: پول‌شویی و فرار مالیاتی*. ترجمهٔ آزاد، معاونت پژوهش تولید علم، دانشگاه اطلاعات و امنیت ملی.

۴. فتحی‌زاده، امیرهوشنگ؛ اسماعیلی عطاآبادی، عقیل (۱۳۹۹). *حقوق بلاکچین*. تهران: شرکت چاپ و نشر بازرگانی.

ب) مقالات

۵. آهنگری، کارن (۱۴۰۰). «پرایوسی کوین چیست؟». قابل دسترس در: https://bitpin.ir/academy/privacy-coin/(Visited: 2022/03/27)

۶. الهویی نظری، حمید؛ فامیل زوار جلالی، امیر (۱۳۹۶). مسئولیت بین‌المللی دولت‌های تأمین مالی‌کننده تروریسم. *فصلنامهٔ مطالعات حقوق عمومی*، ۴۷(۳)، ۷۲۵- ۷۴۶.

۷. الهویی نظری، حمید؛ امیری، صالح؛ بی‌نیاز، زهرا (۱۴۰۱). استانداردهای نظام پرداخت جایگزین در جرائم پول‌شویی و تأمین مالی تروریسم. *فصلنامهٔ مطالعات حقوق عمومی*، ۵۲(۳)، ۱۲۲۷- ۱۲۵۲.

۸. زرنشان، شهرام (۱۳۸۶). شورای امنیت و تعهدات دولت‌ها برای مقابله با تروریسم. *مجلهٔ حقوقی*، (۳۶)، - ۹۴.

۹. فیضی، فریناز؛ رنجبریان، امیرحسین (۱۴۰۲). واکنش حقوق بین‌الملل به وب پنهان: چرایی و چگونگی. *فصلنامهٔ تحقیقات حقوقی*، ویژه‌نامهٔ حقوق فناوری.

۱۰. کدخدایی، عباسعلی؛ فامیل زوار جلالی، امیر (۱۴۰۲). ارزیابی پایبندی دولت‌ها به توصیه‌های گروه ویژه اقدام مالی در مبارزه با تأمین مالی تروریسم. *فصلنامهٔ مطالعات حقوق عمومی دانشگاه تهران*، آمادهٔ انتشار.

۱۱. کدخدایی، عباسعلی؛ نوروزپور، حسام (۱۳۹۹). چالش‌های ارزهای مجازی در مبارزه با پول‌شویی و تأمین مالی تروریسم با تأکید بر اقدامات و توصیه‌های کارگروه ویژهٔ اقدام مالی (FATF). *مجلهٔ حقوقی بین‌المللی*، (۶۲).

۱۲. ماتسورا، جفری اچ، (۱۳۹۷). بررسی اجمالی مقررات ارز دیجیتال و پیامدهای قانونی آن. ترجمهٔ سعید سیاه بیدی کرمانشاهی و حمیدرضا کناری‌زاده، *پژوهشنامهٔ حقوق فارس*، ۱(۱).

۱۳. میرعباسی، سیدباقر، فامیل زوار جلالی؛ امیر (۱۳۹۵). مسئولیت بین‌المللی دولت‌ها ناشی از مدارا و مماشات با گروه‌های دهشت افکن؛ با تأکید بر قضیهٔ افغانستان. *فصلنامهٔ مطالعات حقوق عمومی دانشگاه تهران*، ۴۶(۲)، ۲۷۱-۲۴۷.

۱۴. ناصر فلاح، بهزاد (۱۳۹۸). آیا تراکنش‌های ارزهای دیجیتال واقعا ناشناس است؟. قابل دسترس در: https://arzdigital.com/are-cryptocurrency-transactions-anonymous/(visited: 2023/09/09)

ج) مصاحبه

۱۵. مصاحبه با علی جهانی (۱۴۰۳). رئیس هیأت مدیرهٔ شرکت تبادل رمزارز بیت‌پین، منطقهٔ آزاد تجاری و اقتصادی انزلی.

۲. انگلیسی

A) Book

1. Duquet, N. (ed.), (2017). *Triggering Terror: Illicit Guns Markets and Firearms Acquisition of Terrorist Networks in Europe.* Flemish Peace Institute, Brussels
2. Gates, M. (2017). *Block Chain*. Wise fox pub
3. Ozkaya, E., & Islam, R. (2019). *Inside the Dark Web*. Taylor and Francis Group
4. B)Article
5. Greenberg, A, (2014). Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever. *Wired*, April 29, Available at: https://www.wired.com/2014/04/dark-wallet/. (A)
6. Greenberg, A (2014). Waiting for Dark: Inside Two Anarchists'Quest for Untraceable Money. *Wired*, July 11, Available at: https://www.wired.com/2014/07/inside-dark-wallet/. (B)
7. Benjamin, W (2011). The Rise and Fall of Bitcoin. *Wired*, November 23
8. Berg, S., & Killian J McCarthy, (2016). The Economics of ISIS — A Case of Theft or MoneyLaundering?. *Freedom from Fear*, (11), 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:08/10/2022).
9. Dalyan, S. (2008). Combating the financing of terrorism: Rethinking strategies for success, *Defense Against Terrorism Review*, 1.1.
10. Dion, D. (2013). I'll Gladly Trade you two bits on Tuesday for a Byte Today, Bitcoin, Regulating Fraud in the Economy of Hacker-Cash, *U. Ill. J. L. Tech and Policy*
11. Eric, M. (2013). The Bitcoin Pizza Purchase That's Worth $7 Million Today. *Forbes*, December 23
12. Fanusie, Y & Robinson, T. (2018). *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*, Foundation for Defense of Democracies and Elliptic, 12 January.
13. Fanusie, Y (2018). Survey of Terrorist Groups and Their Means of Financing, House Financial Services Committee, Available at: https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-yfanusie-20180907.pdf (visited: 2023/10/12)
14. Goriacheva, A, Jakubenko N, Pogodina, O & Silnov, D. (2018), Anonymization Technologies of Cryptocurrency Transactions as Money Laundering Instrument. in *III Network AML/CFT Institute International Scientific and Research Conference "FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies"*, KnE Social Sciences
15. Harman, D. (2015). U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests. *Haaretz*, 29 January, https://www.haaretz.com/.premium-isis-uses-bitcoin-

for-fundraising-1.5366305. (visited:2023/10/08)
16. Kethineni, S., Cao, Y., & Dodge, Cassandra (2017). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes, American Journal of Criminal Justice, 43(2), Available at: http://dx.doi.org/10.1007/s12103-017-9394-6
17. Maxey, L. (2018). Terrorists Stalk the Dark Web for Deadlier Weaponry. *The Cipher Brief*, 17 January, https://www.thecipherbrief.com/terrorists-stalk-dark-web-deadlier-weaponry.
18. Mixer. Money: Bitcoin Mixing Service. Available at: https://mixer.money
19. Redman, J. (2018). Chainalysis Raises $16Mn – Plans to Monitor Multiple Blockchains. *Bitcoin.com*, 6 April, retrieved from: https://news.bitcoin.com/chainalysis-raises-16mn-plans-to-monitor-multiple-blockchains. (visited:10/11/2018).
20. Salami, I. (2017). Terrorism Financing with Virtual Currencies – Can Regulatory Technology Solutions Combat this? *Studies in Conflict & Terrorism*, Available at: https://doi.org/10.1080/1057610X.2017.1365464
21. See Moore, D., & Rid, T. (2016). For a taxonomy of high-level categories of activity over the Dark Web, Cryptopolitik and the Darknet. *Survival*, 58:1, February-March.
22. Shacheng, W., & Xixi, Z (2021). Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing. *Policing*, 15(4).
23. Shah, A. (2007). The International Regulation of Informal Value Transfer System. *Utrecht Law Review*, 3(2).
24. Suberg, W. (2017). Bitcoin Exchange ShapeShift Helps Police as WannaCry Attacker Converts to Monero,' CoinTelegraph, 4 August. https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero.
25. Singletary, T, (2015). Dark Web and the Rise of Underground Networks, in *Evolution of Cyber Technologies and Operations to 2035*, Advances in Information Security 63, DOI 10.1007/978-3-319-23585-1_8
26. Wallace, B. (2011). The Rise and Fall of Bitcoin. *Wired*, November 23, Available at: https://www.wired.com/2011/11/mf-bitcoin/
27. Wardhana, A. T., & Nugroho, B. W. (2021). Abuse of Cryptocurrency to Funding International Terrorism Activities, *Proceedings University Muhammadiyah Yogyakarta Undergraduate Conference*, *1*(1), 353–362. Retrieved from https://prosiding.umy.ac.id/grace/index.php/pgrace/article/view/190

B) Instrument and Report

28. Aldridge, Judith; Paoli, Giacomo Persi; Ryan, Nathan; Warnes, Richard (2017). *Behind the curtain: the illicit trade of firearms, explosives and ammunition on the dark web*, RAND Corporation, Available at: https://www.rand.org/pubs/research_reports/RR2091.html.
29. Council of the EU (2018) 'Money laundering and terrorist financing: new rules adopted,' press release, 14 May, http://www.consilium.europa.eu/en/press/press-releases/2018/05/14/money-laundering-and-terrorist-financing-new-rules-adopted/.
30. Counter-Terrorism Committee Executive Directorate (2022). *Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of Security Council resolutions*, Available at:

https://www.un.org/securitycouncil/ctc/content/thematic-summary-assessment-gaps-implementing-key-countering-financing-terrorism-provisions, (Visited: 2024/01/04)
31. CTIF-CFI (2016). *23rd Annual Report.* Belgian Financial Intelligence Processing Unit (CTIF-CFI), Available at: http://www.ctifcfi.be/website/images/EN/annual_report/ar2016en.pdf
32. Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston, (2019), *Terrorist use of cryptocurrency*, Published by the RAND Corporation
33. Egmont (2023). *Report on Abuse of Virtual Assets for Terrorist Financing Purposes*. Information Exchange Working Group (IEWG), pp. 7-8, Available at: https://egmontgroup.org/wp-content/uploads/2023/12/2023-July-HoFIU-06-IEWG-Project-Abuse-of-VA-for-TF-Summary-1.pdf, (Visited: 2023/12/03)
34. European Banking Authority (2014) *EBA Opinion on Virtual Currencies*, 4 July, Available at: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-201408+Opinion+on+Virtual+Currencies.pdf.
35. European Central Bank (2012). *Virtual Currency Schemes*, Frankfurt, October, Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.
36. FATF (2010). Money Laundering Using New Payment Methods, FATF Report, Paris, October, Available at:https://www.fatfgafi.org/en/publications/Methodsandtrends/Moneylaunderingusingnewpaymentmethods.html (visited: 2023/10/11)
37. FATF (2014). *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, Paris, Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, (Visited: 2023/12/03)
38. FATF (2019). *Guidance for a Risk-Based Approach, Virtual Assets and Virtual Asset Service Providers*. Available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html (visited: 2024/01/15)
39. FATF (2020). *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html, (Visited: 2023/10/12)
40. HM Treasury and the Home Office (2017). *National risk assessment of money laundering and terrorist financing*, London
41. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/189/01/PDF/N2318901.pdf?OpenElement
42. Joint Counterterrorism Assessment Team (JCAT), (2021). Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists, Available at: https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/119s_First_Responders_Toolbox_-_Identifying_and_Preventing_Illicit_Use_of_Cryptocurrency_by_Terrorists.pdf , (visited: 2024/02/01)
43. Keatinge, Tom, Carlisle, David and Florence Keen (2018). *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, Policy Department for Citizens' Rights and Constitutional Affairs European Parliament

44. Möser, Malte; Soska, Kyle; Hellman, Ethan; Lee, Kevin; Heffan, Henry; Srivastava, Shastvat; Hogan, Kyle; Hennessey, Jason; Miller, Andrew; Narayanan, Arvind and Christin, Nicolas, (2017). *An Empirical Analysis of Traceability in the Monero Blockchain*. to appear in Privacy Enhancing Technologies Symposium (PETS)
45. Tierno, Paul, Miller, Rena S. and Liana W. Rosen, (2023). *Terrorist Financing: Hamas and Cryptocurrency Fundraising*, November 27, Available at: https://crsreports.congress.gov
46. United States Department of Justice, (2015). 'Virginia Teen Pleads Guilty to Providing Material Support to ISIS,' Justice News, 11 June, Available at: https://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil.
47. S/RES/1373 (2001). Available At: http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1373%282001%29
48. https://ripjar.com/blog/6amld-6th-money-laundering-directive/ (visited: 2023/07/10)
49. https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/digital-finance-council-adopts-new-rules-on-markets-in-crypto-assets-mica/ (visited: 2023/10/25)
50. Houben, R., & Snyers, A. (2018). *Cryptocurrencies and Blockchain: Legal context and Implications for Financial Crime, Money Laundering and Tax Evasion*, European Parliament, 2018, Available at: https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (visited: 2023/10/25)

References In Persian:

A) Book

1. Babayee, J. (2021). *Computer crimes and the procedure governing it*. Tehran: Publications of the General Department of Judicial Education (In Persian).
2. Bernard Cohen, S. (2008). *Geopolitics of the World System*. translated by Abbas Kardan, Tehran: Abrar Moaser (In Persian).
3. D'Souza, J. (2012). *Terrorist Financing, Money Laundering, and Tax Evasion*. The united states, CRC Press (In Persian).
4. Fathizadeh, A., & Esmaeili Attaabadi, A. (2019). *Blockchain Laws*. Tehran: Commercial Publishing Company (In Persian).

B) Articles

5. Feizi, F., & Ranjbarian, A. H. (2022). Reaction of International Law to the Hidden Web: Why and How. *Legal Research Quarterly*, Special issue of Technology Law, Winter (In Persian).
6. Kodkhodaei, A. A., & Famil Zavvar Jalali, A. (2023). Evaluation of Governments' Adherence to the Recommendations of the Financial Action Task Force in Combating the Financing of Terrorism. *Public Law Studies Quarterly*, ready to be published (In Persian).
7. Kodkhodaei, A. A., & Nowrozpour, H. (2019). Challenges of virtual currencies in the fight against money laundering and terrorist financing with an emphasis on the actions and recommendations of the Special Task Force on Financial Action (FATF). *International Legal Journal*, Spring and Summer, (62) (In Persian).
8. Matsuura, J. H. (2017). An Overview of Digital Currency Regulations and Its Legal Implications. traslated by Saeed Siah Bodi Kermanshahi and Hamidreza Konarizadeh, *Fars Law Research Journal*, 5(5), winter (In Persian).
9. Mir Abasi, S. B., & Famil Zavvar Jalali, A. (2016). International Responsibility of States due to Agreement with Terrorist Groups Emphasizing Afghanistan Issue. *Public Law Studies Quarterly*, University of Tehran, 46(2), 247-271 (In Persian).
10. Nasser Fallah, B. (2023). Are digital currency transactions really anonymous?. April 2018, *available at*: https://arzdigital.com/are-cryptocurrency-transactions-anonymous/ (visited: 2023/09/09) (In Persian).