

<http://doi.org/10.22133/MTLJ.2024.411998.1238>

## Bitcoin; A Revolution in Terrorist Financing

Amir Famil Zovar Jalali<sup>1\*</sup>, Abbas Ali Kodkhodaei<sup>2</sup>

<sup>1</sup> PhD in Public International Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran.

<sup>2</sup> Prof. Department of Public Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran.

### Article Info

### Abstract

#### Original Article

#### Received:

31-12-2023

#### Accepted:

17-08-2023

#### Keywords:

Financial Technologies

Blockchain

Virtual Currencies

Bitcoin

Terrorist Financing

The financing of terrorism is the most critical aspect in the growth of terrorism, and combating the financing of terrorism is the most crucial aspect to eliminating the roots of terrorism. Suppose the actions of governments and international financial and non-financial organisations successfully combat the traditional methods of financing terrorism. In that case, terrorists will move beyond conventional methods and turn to new financial technologies. Due to features such as anonymity, creation of security layers and decentralisation, virtual currencies, especially Bitcoin, are among the financial innovations that criminals, including terrorists, pay attention to for investment and financing. In this article, we will see in a detailed review how Bitcoin, regardless of whether it can be considered a valid currency in the future, by changing the financial systems, has become attractive to illegal networks and can create a revolution in financing terrorism.

#### \*Corresponding author

e-mail: [azjalali@ut.ac.ir](mailto:azjalali@ut.ac.ir)

#### How to Cite:

Famil Zovar Jalali, A., & Kodkhodaei, A.A. (2024). Bitcoin; A Revolution in Terrorist Financing. *Modern Technologies Law*, 5(9), 235-252.

Published by University of Science and Culture <https://www.usc.ac.ir>

Online ISSN: 2783-3836



# حقوق فناوری‌های نوین

<http://doi.org/10.22133/MTLJ.2024.411998.1238>

## بیت‌کوین؛ انقلابی در تأمین مالی تروریسم امیر فامیل زوار جلالی<sup>۱\*</sup>، عباسعلی کدخدایی<sup>۲</sup>

<sup>۱</sup> دکتری حقوق بین‌الملل عمومی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.  
<sup>۲</sup> استاد گروه حقوق عمومی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.

اطلاعات مقاله	چکیده
مقاله پژوهشی	
تاریخ دریافت:	تأمین مالی تروریسم مهم‌ترین بعد در رشد تروریسم و مبارزه با تأمین مالی تروریسم مهم‌ترین جنبه برای خشکاندن ریشه‌های تروریسم است. به هر میزان که اقدامات دولت‌ها و سازمان‌های بین‌المللی مالی و غیرمالی در مبارزه با شیوه‌های سنتی تأمین مالی تروریسم به موفقیت منجر شود، گذرکردن تروریست‌ها از شیوه‌های سنتی و روی آوردن به فناوری‌های جدید مالی بیشتر خواهد شد. ارزشهای مجازی و در رأس آن، بیت‌کوین با توجه به ویژگی‌هایی همچون گمنامی، ایجاد لایه‌های امنیتی و غیرمتمرکزبودن از جمله نوآوری‌های مالی هستند که مجرمانی مانند تروریست‌ها برای سرمایه‌گذاری و نیز تأمین مالی خود به آن نظر دارند. در این مقاله، با مطالعه‌ای دقیق خواهیم دید که بیت‌کوین صرف‌نظر از این‌که به منزله ارزی معتبر در آینده تلقی خواهد شد، چگونه با تغییر سیستم‌های مالی باعث جذابیت برای شبکه‌های غیرقانونی می‌شود و انقلابی در تأمین مالی تروریسم ایجاد می‌کند.
تاریخ پذیرش:	
واژگان کلیدی:	
فناوری‌های مالی	
بلاکچین	
ارزهای مجازی	
بیت‌کوین	
تأمین مالی تروریسم	
*نویسنده مسئول	
رایانامه: <a href="mailto:azjalali@ut.ac.ir">azjalali@ut.ac.ir</a>	

نحوه استناددهی:

فامیل زوار جلالی، امیر، و کدخدایی، عباسعلی (۱۴۰۳). بیت‌کوین؛ انقلابی در تأمین مالی تروریسم. حقوق فناوری‌های نوین، ۵(۹)، ۲۳۵-۲۵۲.

ناشر: دانشگاه علم و فرهنگ <https://www.usc.ac.ir>

شاپای الکترونیکی: ۲۷۸۳-۳۸۳۶

با گذر زمان و طی شدن ادوار تاریخی، شاهد پیشرفت بشر در حوزه‌های مختلف هستیم که غالب این پیشرفت‌ها در راستای ارتقای سطح امنیت، رفاه و بهبود زندگی انسان‌ها بوده است. اما در این میان، می‌توان از حوزه‌ی فناوری اطلاعات به‌منزله‌ی سریع‌ترین حوزه یاد کرد که با شاخه‌های متنوع خود، انقلابی عظیم در روابط میان بشر ایجاد کرده است. به‌اختصار، پیشرفت‌های حوزه‌ی فناوری اطلاعات را می‌توان به سه انقلاب تقسیم کرد. انقلاب اول را می‌توان در فراهم‌شدن بستر اینترنت و قرارگرفتن حجم بالای اطلاعات در اختیار مردمان جهان دانست؛ هرچند با وجود گذشت بیش از ۲۵ سال از این انقلاب، هنوز شاهد توزیع عادلانه‌ی جغرافیایی آن در سطح جهان نیستیم. انقلاب دوم را می‌توان در حوزه‌ی ارتباطات و پیدایش شبکه‌های اجتماعی دانست که تحولی شگرف در زمینه‌ی گذر مردم از پست و تلگراف به شیوه‌های نوین، آسان و کم‌هزینه‌تر به وجود آورد و اما انقلاب سوم را باید بی‌شک در حوزه‌ی بلاکچین و ظهور ارزش‌ها و دارایی‌هایی دانست که می‌توان آنها را دارایی‌های مجازی نامید (پژوهشکده آمار و فناوری اطلاعات قوه قضاییه، ۱۴۰۰، ص ۷). بلاکچین، دارایی‌های مجازی، ارزهای مجازی، رمزارزها، متاورس، ان‌اف‌تی‌ها<sup>۱</sup> همگی واژگان جدیدی هستند که نمایانگر شکل جدیدی از ارزش بوده و همچنین انتقال سریع و بی‌واسطه‌ی وجوه را توصیف می‌کنند. این حجم بالا از تولید، تحول، اختراع و اکتشاف در دارایی‌هایی که نام‌محسوس و ناملموس هستند، چنان جهان را فراگرفته که در زمان نگارش این سطور، ارزش کل بازار آن‌ها بیش از یک تریلیون دلار است.<sup>۲</sup> اگرچه بیشتر دارایی‌های مجازی به‌منزله‌ی محصولی نوآورانه در راستای پیشرفت‌های فناوری و با نیات بشردوستانه ایجاد شدند، اما سوء استفاده از این فناوری‌ها نیز روی دیگر سکه است که نباید از آن غافل شد. بیت‌کوین، ارزی که حوزه عملیاتی آن قلمرو سایبری است، می‌تواند از سویی با پشت‌سرگذاشتن نهادهای نظارتی و ایجاد شفافیت‌ها و از سوی دیگر با ایجاد لایه‌های امنیتی به یک کارگزار بی‌نقص برای تراکنش‌های بی‌نام‌ونشان تبدیل شود. هم‌زمان با افزایش نگرانی دولت‌ها درباره‌ی وضع مالیات و نبود کنترل بر این نوع ارزها، بیت‌کوین تبدیل به ابزاری جدی برای تأمین مالی فعالیت‌های غیرقانونی و از جمله تأمین مالی سازمان‌های تروریستی نیز شده است. حال سؤال این است که بیت‌کوین تا چه اندازه قابلیت تبدیل به یک ارز قابل اتکا برای تأمین مالی تروریسم را دارد و چگونه در این راستا توسعه می‌یابد؟ آیا می‌توان گفت که بیت‌کوین انقلابی در تأمین مالی تروریسم ایجاد کرده است؟

در مقاله حاضر، ابتدا توضیح مختصری از ارزهای مجازی و محبوب‌ترین گونه‌ی آن یعنی بیت‌کوین، ویژگی‌ها و کارکردهای آن ارائه می‌شود. سپس به مزایا، تهدیدها و آسیب‌های بالقوه‌ی آن از جمله در حوزه‌ی تروریسم سایبری و تأمین مالی تروریسم اشاره خواهد شد و در نهایت، چگونگی تأمین مالی تروریسم از طریق بیت‌کوین و نقش این دارایی در آینده‌ی حوزه‌ی تأمین مالی تروریسم بررسی می‌شود.

## ۱. ارزهای مجازی؛ نمونه‌ی تکامل‌یافته‌ی پول

از زمان مبادله‌ی کالا به کالا تا ایجاد روش‌های جایگزین آن، همواره بشر به دنبال ایجاد راه‌های آسان‌تر در انجام مبادلات بود. ایجاد و توسعه‌ی پول نیازی به دستاورد یا کشف مهمی نداشت، بلکه یک انقلاب ذهنی مطلق بود و به‌واسطه‌ی ایجاد یک حقیقت بین‌الذهانی جدید شکل گرفت که فقط در تصور مشترک افراد وجود داشت (هراری، ۱۳۹۸، ص ۲۱).

پول همواره به شکل امروزی نبوده و در طول تاریخ و در مناطق مختلف دنیا به اشکال مختلفی وجود داشته است؛ به طوری که تا به امروز از کالاهای مختلفی به‌مثابه‌ی پول استفاده شده است (آذرنژاد، ۱۴۰۱، ص ۱۴). پول در گذر زمان، ناملموس‌تر و مجازی‌تر شده و روند تکاملی چند هزارساله‌ای را طی کرده تا امروزه به مفهوم ارز مجازی رسیده است. با گسترش فناوری اطلاعات، پول الکترونیکی پا به عرصه‌ی اقتصاد گشود که ماهیت آن همان اسکناس‌های کاغذی است، اما از حالت فیزیکی و ملموس به مجموعه‌ای از اعداد و ارقام داخل شبکه‌های رایانه‌ای تبدیل شده که تحت عنوان سیستم بانکی الکترونیک شناخته می‌شود (عبادی لمر، ۱۳۹۹، ص ۱۲). بنابراین، امروزه بیشتر تراکنش‌های دنیا از طریق

1. Non-fungible tokens

2. <https://blog.bittestan.com/growth-total-market-value-digital-currencies>

انتقال داده‌های الکترونیکی از یک پوشه رایانه‌ای به پوشه دیگر (بدون هیچ‌گونه تبادل پول فیزیکی) انجام می‌شود (هراری، ۱۳۹۸، ص ۲۲)؛ اما در دهه اخیر پولی به وجود آمده که به طور کلی با اسکناس‌های بانکی و نمایش الکترونیکی آن‌ها متفاوت و یک واحد ارزش جدید با سازوکار منحصر به فرد به نام «ارز مجازی»<sup>۱</sup> یا «ارز رمزنگاری‌شده»<sup>۲</sup> است.

برای تعریف و آشنایی با ارزهای مجازی ابتدا باید با اصلاح ارزهای دیجیتال آشنا شد. ارز دیجیتال ارزی است که به شکل الکترونیک ذخیره شده و با استفاده از ابزارهایی مانند کامپیوتر، اینترنت و تلفن‌های هوشمند به‌عنوان وسیله پرداخت عمل می‌کند؛ لذا از این منظر ارزهای دیجیتال می‌تواند شامل ارزهای واقعی مانند پول الکترونیک باشد که در بالا توضیح داده شد یا شامل ارزهای جدیدی باشد که از آن به‌عنوان ارز مجازی یاد می‌شود.

ارز مجازی یکی از انواع ارز دیجیتال و نمایانگر ارزشی است که دارای پشتوانه بانک مرکزی یک دولت نیست (آذرزاد، ۱۴۰۱، ص ۴۳) و با سازوکار رمزنگاری در بستر خاص هوشمندی تولید شده و فعالیت می‌کند. مطابق تعریفی که گروه ویژه اقدام مالی (FATF)، اصطلاح ارزهای مجازی به هر نمایش دیجیتالی از ارزش گفته می‌شود که قابلیت معامله به‌صورت مجازی را دارد و می‌تواند هم به‌منزله وسیله پرداخت و هم به‌منزله ذخیره ارزش و سرمایه‌گذاری عمل کند و در کنار این سه، یک نوع واحد حساب نیز به‌شمار می‌رود؛ یعنی می‌توان کالاها و خدمات را براساس آن قیمت‌گذاری کرد<sup>۳</sup>. این نوع ارزها را هیچ مرجع قانونی صادر و تضمین نمی‌کند و کلیه ویژگی و وظایف آن براساس توافق میان جامعه کاربران این نوع دارایی‌های مجازی صورت می‌گیرد. همچنین این نوع دارایی را نمی‌توان به‌مثابه e-Money یا همان پول الکترونیک که نمایشی دیجیتال از پول فیات است دانست؛ زیرا e-Money تنها نوع مکانیزم دیجیتالی برای انتقال الکترونیکی پولی است که از آن به‌منزله ارز ملی و پول رسمی یک کشور یاد می‌شود<sup>۴</sup>. در ادامه به معرفی انواع ارزهای مجازی خواهیم پرداخت.

## ۱-۲. انواع ارزهای مجازی

ارزهای مجازی به دو دسته تقسیم می‌شوند که در ادامه شرح داده شده‌اند.

### ۱-۲-۱. ارزهای مجازی به‌لحاظ قابلیت تبدیل

ارزهای مجازی بر مبنای پاسخ به این سؤال که آیا قابلیت تبدیل شدن به پول واقعی را دارند یا خیر، به دو دسته قابل تبدیل و غیرقابل تبدیل تقسیم می‌شوند: ارزهای مجازی قابل تبدیل یا منبع باز ارزشی معادل ارز واقعی دارند و می‌توانند به‌صورت دادوستد با ارز واقعی مبادله شوند؛ اما ارزهای مجازی غیرقابل تبدیل یا منبع بسته امکان تبدیل به پول‌های بانکی را ندارند و فقط در یک برنامه خاص یا برای منظوری خاص استفاده می‌شوند. مثل پول‌های استفاده‌شده در بازی‌های آنلاین که فقط در همان سایت قابلیت مبادله دارند و اصطلاحاً به آن‌ها سکه‌های بازی<sup>۵</sup> می‌گویند و نمی‌توان آن‌ها را با ارز فیات مبادله کرد. این نوع ارزها صرفاً متمرکزند؛ یعنی نهادی مرکزی (برای مثال شرکت عرضه‌کننده بازی) آن را انتشار می‌دهد و دفتر کل<sup>۶</sup> آن را نزد خود نگه می‌دارد. گفتمی است همواره این فرضیه محتمل است که یک بازار سیاه غیررسمی فرصتی را برای تبدیل

1. Virtual Currency

2. Crypto Currency

3. FATF Report, June 2014, p. 4. <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

4. Financial Action Task Force (2019), Virtual Assets and Virtual Assets Service Providers, June 2019, retrieved from: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html>

5. Game Coin

6. منظور از دفتر کل، یک دفتر مجازی از سابقه تراکنش‌هاست که در ادامه با آن بیشتر آشنا خواهیم شد.

دارایی‌های مجازی غیرقابل تبدیل به ارز فیات یا سایر دارایی‌های محسوس را فراهم کند؛ اما این امر به تغییر ویژگی آن (غیرقابل تبدیل بودن) منجر نخواهد شد.<sup>۱</sup>

## ۱-۲-۲. ارزش‌های مجازی به لحاظ قابلیت نظارت

ارزش‌های مجازی به لحاظ قابلیت نظارت و تحت کنترل بودن به دو دسته ارزش‌های متمرکز و غیرمتمرکز تبدیل می‌شوند. متمرکزها مدیریتی واحد و متمرکز برای کنترل و تنظیم دارند. در این مدل دارایی، شخص ثالثی تحت عنوان مدیر، نوعی دارایی یا ارز را تولید می‌کند، قواعد استفاده از آن را تنظیم کرده و صلاحیت با خرید دارایی را نیز دارد.<sup>۲</sup> به اختصار این نوع ارزها به شخص یا نهادی خاص وابسته است که کنترل کامل آن ارز را برعهده دارد. ارزش‌های مجازی مانند وب مانی یا پرفکت مانی از این دسته هستند.

در نقطه مقابل ارزش‌های مجازی متمرکز، گونه‌ای دیگر وجود دارند که انتشار و کنترل آن‌ها فارغ از کنترل و مدیریت نهاد مرکزی بوده و از طریق کلیه افراد موجود در شبکه و با به کارگیری علم رمزنگاری مدیریت می‌شود (عبادی لمر، ۱۳۹۹، ص ۱۴). این نوع دارایی‌ها که با عنوان رمزارزها<sup>۳</sup> شناخته می‌شوند، به علت داشتن ویژگی‌هایی همچون نامتمرکز بودن، ناشناس بودن، قابلیت رهگیری نداشتن، بیشترین حجم بازار دارایی‌های مجازی را به خود اختصاص داده که نمونه شاخص آن رمزارز بیت‌کوین است که از آن با عنوان پادشاه ارزش‌های مجازی یاد می‌شود. در ادامه، به معرفی و بررسی این ارز مجازی و ویژگی‌های آن خواهیم پرداخت.

## ۲. بیت‌کوین

بیت‌کوین «ارز رمزنگاری شده قابل تبدیل غیرمتمرکز»<sup>۴</sup> است که در سال ۲۰۰۹ از طریق یک برنامه‌نویس یا گروهی با نام مستعار ساتوشی ناکاموتو<sup>۵</sup> آغاز به کار کرد (CNNMoney, 2014, p. 2). زمانی که ایده بیت‌کوین مطرح شد، هدفش این بود که به منزله عامل اصلی، نقش مهم تمرکززدایی را ایفا کند. تمرکززدایی یعنی همه افراد (کاربران) بخشی از اکوسیستم بیت‌کوین هستند و همگی به روش خود در آن مشارکت می‌کنند. بیت‌کوین به جای آن که به یک دولت یا بانک متکی باشد، در سیستمی که «همتابه‌همتا»<sup>۶</sup> نامیده می‌شود، به همه کاربران تعلق دارد و این کاربران هستند که شبکه بیت‌کوین را تشکیل می‌دهند (پریپتو، ۱۴۰۰، صص ۹-۱۰). این ارز و روش‌های تراکنش آن، با حذف واسطه‌ها، باعث رهایی از نهادهای سنتی مانند بانک‌ها می‌شوند و یک دنیای بدون مرز ایجاد می‌کنند که مشخصه آن، تراکنش‌های لحظه‌ای با هزینه پایین و به صورت گمنام است. امروزه بیت‌کوین بالاترین ارزش بازاری را در بین رمزارزها دارد که باعث علاقه‌مندی سرمایه‌گذاران و نیز سیاست‌سازان به این رمزارز شده است (Song et al, 2023, p. 1). در ادامه به مزایا و معایب بیت‌کوین اشاره خواهد شد.

## ۱-۲-۱. مزایا، معایب و آسیب‌پذیری‌ها

دارایی‌های مجازی و در رأس آن بیت‌کوین، مزایای بالقوه زیادی دارند. آن‌ها می‌توانند پرداخت‌ها را آسان‌تر، سریع‌تر و ارزان‌تر کنند و نوعی جایگزین برای آن دسته از افراد یا نهادهایی باشند که به خدمات مالی منظم و سنتی دسترسی ندارند؛ البته بدون تنظیم مقررات و سیستم نظارتی مناسب، این حوزه بستری مناسب برای سوءاستفاده مجرمان مالی است.<sup>۷</sup> در ادامه، ابتدا مزایای بیت‌کوین و سپس معایب و ریسک‌های فعلی و بالقوه آن بررسی می‌شود.

۱. رجوع کنید به: FATF Report, June 2014, p. 5

2. FATF Report, June 2014, p. 5

3. Cryptocurrency

4. Convertible Decentralized Cryptocurrency

5. Satoshi Nakamoto

6. Peer to Peer

7. [http://www.fatf-gafi.org/publications/virtualassets/documents/virtual\\_assets.html?hf=10&b=0&s=desc\(fatf\\_releasedate\)](http://www.fatf-gafi.org/publications/virtualassets/documents/virtual_assets.html?hf=10&b=0&s=desc(fatf_releasedate))

## ۲-۲. مزایای بیت‌کوین

ارزهای مجازی و در رأس آن، بیت‌کوین مشخصه‌هایی دارند که افراد، صنایع و بازارهای مالی را جذب می‌کنند. به نظر تمرکززدایی و آزادی مالی مهم‌ترین مزیت این نوع دارایی‌ها محسوب می‌شود. این آزادی مالی و عدم تمرکز با یک مثال ساده درک‌شدنی است: ارزش رایجی که ما در کیف پول یا در حساب بانکی خود داریم (همان ارزش فیات) نشان‌دهنده ارزش خاص است. برای مثال یک اسکناس ۲۰ هزار ریالی به میزان ۲ هزار تومان ارزش دارد. این همان چیزی است که بانک مرکزی به ما می‌گوید؛ چراکه روش دیگری وجود ندارد تا مصرف‌کننده عادی تأیید کند این قطعه کاغذ، که ماهیتاً بی‌ارزش است، به‌واقع چقدر می‌ارزد؛ اما در مقابل قیمت یک بیت‌کوین را بازار آزاد تعیین می‌کند. اگر بازار آزاد، که از کاربران بیت‌کوین در سراسر جهان تشکیل شده، تصمیم بگیرد قیمت جدید بیت‌کوین از ۲۰ هزار دلار به ۱۰۰ هزار دلار برسد، هیچ نهاد مرکزی وجود ندارد که از این اتفاق ممانعت کند.

یکی از مزایای فناوری بلاک‌چین در مقایسه با سیستم‌های موجود، توانایی حذف واسطه‌ها و امکان تراکنش‌های مستقیم بین افراد، بدون دخالت اشخاص ثالث، است. با تمرکززدایی، هزینه‌های خدمات پرداخت و انتقال وجوه به میزان درخور توجهی کاهش می‌یابد. گمنامی<sup>۱</sup> یا همان ناشناس ماندن از دیگر امکانات ارزهای مجازی از جمله بیت‌کوین است؛ به این معنا که می‌توان تراکنش‌ها را به‌صورت ناشناس انجام داد تا هویت طرفین معامله محرمانه باقی بماند؛ برای مثال رمزارز بیت‌کوین دارای دو کلید عمومی و خصوصی است که از تعدادی حروف الفبا و عدد تشکیل می‌شود. کلید عمومی مانند شماره حسابی است که برای سایر کاربران نمایش داده می‌شود، اما کلید خصوصی فقط در اختیار صاحب حساب و برای تأیید هویت صاحب حساب قبل از انجام مبادله ضروری است (ماتسورا، ۱۳۹۷، ص ۱۵۲). وجوه به کلیدهای خصوصی رمزنگاری شده (و مسلماً مخفی) ارسال می‌شوند و هر فردی که این کلیدها را در اختیار داشته باشد می‌تواند رمزارزها را کنترل کند. به همین دلیل، بیت‌کوین را ناشناس می‌نامند؛ زیرا اگرچه کلیدهای عمومی کاربران می‌تواند از طریق تاریخچه معامله پیگیری شوند، اما هویت خریداران و فروشندگان پنهان باقی می‌ماند. به هر میزان که بیت‌کوین با ویژگی گمنامی شناخته می‌شود از طرفی واحد ویژگی شفافیت نیز هست. شفافیت به این معناست که تمام تراکنش‌ها در دفتر کل عمومی یا همان بلاکچین ثبت شده و کلیه کاربران می‌توانند آن را مشاهده کنند، اما هویت دو طرف تراکنش ناشناس و پنهان است. این همان ماهیت خاص پلتفرم بیت‌کوین یعنی بلاکچین است.<sup>۲</sup> در عین این‌که همه چیز شفاف است، هویت کاربران و میزان دارایی آن‌ها پنهان باقی می‌ماند؛ شفافیت در عین محرمانگی و تمرکززدایی بلاک‌چین‌ها این است که داده‌ها به جای نگه‌داری در چند دفتر مجزا، روی یک دفتر اشتراکی منفرد نگه‌داری می‌شوند؛ بنابراین در صورت استفاده از بلاک‌چین، دیگر نیازی نیست مردم و شرکت‌ها، کنترل را به‌دست نهاد خاصی بسپارند. مصادیق بی‌شماری وجود داشته که در آن، نبود شفافیت دفاتر کل به پرونده‌های انبوهی از تقلب و کلاهبرداری منجر شده است. نبود شفافیت باعث شده که افراد بتوانند بدون اطلاع سایرین، ورودی‌ها یا همان مدخل‌ها را تغییر یا داده‌ها را دستکاری کنند. این درحالی است که فناوری مبتنی بر بلاک‌چین، باعث شفافیت برای همه افراد شبکه می‌شود و تراکنش‌ها برای تمامی رایانه‌های متصل مشاهده‌پذیر هستند.

## ۲-۳. معایب و آسیب‌پذیری بیت‌کوین

ارزهای مجازی از جمله بیت‌کوین در کنار تمامی مزایا و امکانات منحصر به فردی که دارند همچون فناوری‌های دیگر از معایب و خطرات دور نیستند. یکی از خطرات مهم مرتبط با ارزهای مجازی از جمله بیت‌کوین، برگشت‌ناپذیری تراکنش‌هاست. به‌عبارت‌دیگر، در صورت ارسال بیت‌کوین به یک آدرس کیف پول اشتباه هیچ سازوکاری برای برگشت مقادیر ارسالی وجود ندارد؛ هرچند که طرفین می‌توانند به‌صورت داوطلبانه

### 1. Anonymity

<sup>۱</sup> «سیستم‌های مبتنی بر بلاک‌چین، در مقایسه با بایگانی‌ها و دفاتر کل موجود، شفافیت بیشتری دارند. تمام افراد شبکه قادر به دیدن تغییرات در دفاتر کل هستند و تراکنش‌ها، پس از وارد شدن به بلاک‌چین، دیگر قابل تغییر یا حذف نیستند» (Gates, 2017, p. 23).

اشتباه در پروتکل بیت‌کوین را اصلاح کنند؛ اما سازوکاری برای عودت ارز با استفاده از ابزارهای قانونی وجود ندارد و دلیل اصلی این خلأ، ماهیت غیرمتمرکز بیت‌کوین است.

نبود بیمه یا تضمین نیز از دیگر معایب شبکه رمزارزها از جمله بیت‌کوین است. عمده شرکت‌های بیمه سرمایه‌گذاری در بیت‌کوین را تضمین نمی‌کنند. مشکل تضمین نکردن این است که به‌رغم تلاش‌های کاربران برای حفظ امنیت کلید خصوصی و استفاده از ویژگی‌هایی مانند گمنامی و کدگذاری امنیتی به‌منزله ابزارهای امنیتی، اکوسیستم بیت‌کوین هم‌چنان آسیب‌پذیر است و همیشه این احتمال هست که یک فرد کنجکاو بتواند با توجه به برخی عوامل مانند خطای اپراتور، نقص امنیتی یا بهره‌گیری از بدافزارهای جست‌وجوگر، اطلاعات کیف پول و رمز کلید خصوصی را به‌دست آورد. فضای سایبری و قلمرو سایبری همیشه در معرض حملات هکری هستند و بیت‌کوین هم با توجه به ماهیت ذاتی‌اش، پتانسیل سوء استفاده را دارد. برای نمونه، در فوریه ۲۰۱۵، صرافی «مت‌گوکس»<sup>۱</sup> که یکی از صرافی‌های برتر بیت‌کوین است، با ادعای هک شدن اطلاعات صدها میلیون بیت‌کوین، اعلام ورشکستگی کرد (US Defense Dept, 2014, p. 9). حملات طرد «خدمات»، فراموشی رمز کلید خصوصی کیف پول و نیز ویروس‌ها از دیگر خطرات فنی مرتبط با ارز مجازی محسوب می‌شوند.

یکی دیگر از حوزه‌هایی که ارزهای مجازی درگیر آن هستند، مقاصد غیرقانونی و مجرمانه است. مطابق تخمین برخی مطالعات، قریب ۲۵ درصد کاربران بیت‌کوین و ۴۴ درصد تراکنش‌های بیت‌کوین، در فعالیت‌های غیرقانونی دخیل هستند. براساس همین تخمین‌ها، ارزش کل تراکنش‌های بیت‌کوین غیرقانونی حدود ۷۲ میلیارد دلار در سال است؛ اما سایر مطالعات کمتر از ۱ درصد تراکنش‌های بیت‌کوین پردازش شده در سرویس‌های صرافی را غیرقانونی دانسته‌اند (Foley, 2019). بنابراین، درباره میزان استفاده از دارایی‌های مجازی برای اهداف مجرمانه اختلاف نظرها زیاد است. اگرچه اظهارنظر قطعی درباره میزان فعالیت غیرقانونی در حوزه ارزهای مجازی دشوار است؛ اما استفاده از این نوآوری برای مقاصد غیرقانونی و مجرمانه، یکی از مسائل بسیار حساس و جالب برای ناظران و مجریان قانون است؛ زیرا هم‌چنان که مراجع ذی‌ربط درگیر تنظیم مقررات برای فعالیت‌های مرتبط با فناوری هستند، روش‌های استفاده شده متخلفان برای استفاده غیرقانونی و مجرمانه از این فناوری‌ها نیز روزبه‌روز تکامل می‌یابد. پولشویی، خرید و فروش کالاها و خدمات غیرقانونی در دارک وب و تروریسم اصلی‌ترین فعالیت‌های غیرقانونی و مجرمانه مرتبط با ارزهای مجازی هستند.

از آنجاکه استفاده از رمزارزها و به‌ویژه بیت‌کوین در تأمین مالی فعالیت‌های تروریستی به یکی از نگرانی‌های فزاینده ناظران و تلاش‌های ضدتروریسم تبدیل شده است، در ادامه به بررسی نقش و تحول ارز مجازی بیت‌کوین در تأمین مالی تروریسم خواهیم پرداخت.

### ۳. بیت‌کوین و تأمین مالی تروریسم

در فرازهای پیشین توضیح داده شد که ارزهای مجازی وابسته به کشور یا ارگان خاصی نیستند و تجارت و خریدوفروش بیت‌کوین‌ها باعث سهولت در مبادلات شده؛ به‌گونه‌ای که صرفاً با دسترسی به اینترنت از هر گوشه دنیا می‌توان اقدام به تراکنش کرد. ویژگی‌هایی همچون نبود نظارت، متمرکز نبودن، گمنامی و تلقی آن به‌منزله روش جایگزین پرداخت سریع، آسان و ارزان می‌تواند ارزهای مجازی را برای بسیاری از مجرمان جرایم مالی از جمله تروریست‌ها جذاب کند (Goldman et al., 2017, p. 2)؛ زیرا امکان ناشناس ماندن هویت کاربر بیش از سیستم‌های پرداخت الکترونیک سنتی بوده و پولشویان و تروریست‌ها را قادر می‌سازد که ریشه غیرقانونی ارزهای به‌دست‌آمده را مخفی و کنترل و نظارت بر جریان وجوه را سخت‌تر کند. سازمان‌های تروریستی تلاش می‌کنند با درک فناوری‌های جدید و درحال تکامل دیجیتالی، از جمله رمزارزها از آن برای انتقال گمنام و امن وجوه به نواحی مدنظرشان استفاده کنند (Song et al., 2023, p. 5).

در این بخش، در راستای بررسی معایب رمزارزها در حوزه تأمین مالی تروریسم و این که چه عواملی به روی آوردن تروریست‌ها به استفاده از رمزارزها برای تأمین منابع مالی خود منجر می‌شود، لازم است ابتدا تروریسم سایبری بررسی شود و سپس به نقش بیت‌کوین در شکل نوین تأمین مالی تروریسم پرداخته شود.

### ۱-۳. تروریسم سایبری

تروریسم به معنای استفاده سازمان‌دهی شده و نظام‌ن از ترور برای رسیدن به مقاصد سیاسی در هر دو شکل داخلی و بین‌المللی آن پدیده‌ای قدیمی است که اهدافش در طیفی از کسب قدرت و نبرد برای آزادی ملی تا سرکشی و عمل به دستورات ایدئولوژیکی و مذهبی قرار می‌گیرد (کوهن، ۱۳۸۷، ص ۱۸۴). به لحاظ مفهومی، تروریسم تعاریف متفاوتی دارد و تاکنون هیچ تعریفی از تروریسم ارائه نشده که کل جامعه بین‌المللی بر سر آن توافق داشته باشد. مطابق یک گزارش، بین سال‌های ۱۹۶۳ تا ۱۹۸۱، حدود ۱۰۹ تعریف متفاوت از تروریسم ارائه شده بود که این حجم از تعریف، خود واضح‌ترین نشانه اختلاف در درک بین‌المللی از تروریسم است (Jongman & Schmid, 2005, pp. 5-6). در هر صورت، تروریسم یک ایدئولوژی دارد که با اعمال خشونت‌بار به دنبال گسترش آن است. این نقطه اشتراک همه گروه‌های تروریستی است که همه‌ی افعالشان یک پیش‌زمینه ایدئولوژیکی دارد و این گروه‌ها سعی دارند افراد را جذب ایدئولوژی خود کنند.

به هر روی، تروریسم مسئله‌ای است که از دیرباز تا کنون جامعه بین‌المللی را درگیر خود کرده و تروریست‌های امروزی حتی سازمان یافته‌تر، حرفه‌ای‌تر و مجهزتر از همتایانشان در تاریخ هستند. با پیشرفت جهان در ابعاد گوناگون فناوری، تروریسم نیز ابعادی جدید پیدا کرده است. تروریسم نوین قادر است که به جنگ‌های شبکه‌ای، سایبری، هسته‌ای و بیولوژیکی منجر شود و دامنه این گونه تهدیدات را به کشورهای که ظاهراً به لحاظ جغرافیایی از کانون بحران دورند نیز گسترش دهد (ناجی راد، ۱۳۸۷، ص ۹).

شاید بتوان گفت یکی از جدیدترین ابعاد تروریسم در عصر حاضر، تروریسم سایبری است که در دهه ۱۹۸۰ کالین باری، محقق ارشد حفاظت اطلاعات در کالیفرنیا، آن را مطرح کرد. این اصطلاح با تلفیق دو عبارت سایبر و تروریسم به یکی از اشکال نوین تروریسم بین‌المللی اشاره دارد و بدین معناست که شاید در حملات تروریستی دیگر از حمله‌های فیزیکی خبری نباشد؛ بلکه حملات علیه رایانه‌ها و اطلاعات ذخیره‌شده به منظور ترساندن یا وادار ساختن یک دولت یا اتباع آن برای اهداف سیاسی خاص صورت گیرد.

تروریسم سایبری عبارت است از اقدامات برنامه‌ریزی شده و هدفمند، که با اغراض سیاسی و غیرشخصی علیه رایانه‌ها، امکانات و برنامه‌های ذخیره‌شده در آن‌ها صورت می‌گیرد و هدف از چنین اقداماتی نابودی یا وارد آوردن آسیب‌های جدی به آن‌هاست (ابوذری، ۱۳۹۱، ص ۷۲). همچنین مارک پُلینت تروریسم سایبری را حمله عامدانه و مخرب با اهداف سیاسی علیه مدیریت سامانه‌های اطلاعاتی تعریف می‌کند. به عبارت دیگر، تروریسم سایبری را می‌توان اختلال از طریق دسترسی غیرمجاز به رایانه، انتشار ویروس، بمب‌های ایمیلی و غیره با هدف آسیب‌رساندن تعریف کرد (قاسمی و باقرزاده، ۱۳۹۴، ص ۲۲۸). تروریسم سایبری سعی دارد با ایجاد اختلال یا خراب‌کاری در سامانه‌ها، شبکه‌ها یا مؤلفه‌های اطلاعاتی رایانه‌ای و ایجاد رعب و وحشت در جوامع و همچنین ایجاد صدمه و خسارت فیزیکی یا اطلاعاتی به اموال و اشخاص در راستای رسیدن به اهداف سیاسی، اجتماعی و ایدئولوژیکی مدنظر خود گام بردارد (رزمنخواه، ۱۴۰۲، ص ۵).

تروریست‌ها جدا از این که می‌توانند از فضای سایبر برای حملات تروریستی استفاده کنند، پیشرفتشان در این حوزه، این امکان را برای آنها فراهم خواهد کرد تا از این فضا برای تأمین منابع مالی، تبلیغ ایدئولوژی و جذب هوادار و نیرو بهره ببرند. مطابق گزارش یوروپل، تروریست‌ها برای هماهنگی، تبلیغات و انتشار اطلاعات خود، از اینترنت، فضای مجازی و اپلیکیشن‌های ارتباطی آنلاین استفاده می‌کنند.<sup>۱</sup> همچنین مفهوم

1. Europol, (2017), EU Terrorism Situation and Trend Report (TE-SAT), The Hague, 2017, <https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017>.



جهاد سایبری<sup>۱</sup> که جیمز اسکات<sup>۲</sup> و درو اسپانیل<sup>۳</sup> ابداع کرده‌اند در حال رایج شدن است و موقعیتی را توصیف می‌کند که در آن، دنیای سایبری به عرصه معمول عملیات‌های تروریستی امروزی تبدیل می‌شود. از نظر آن‌ها، برای مثال گروه تروریستی داعش تهدیدی بالفعل در حوزه سایبری است؛ زیرا با هکرهای تنها یا گروه‌های هکری کار می‌کند و مطالب آنلاین را در دسترس همگان قرار می‌دهد (Ashok, 2016).

با پیشرفت فناوری، به‌ویژه در فناوری‌های مالی، حملات سایبری تروریست‌ها برای کسب درآمد به حوزه‌های نوین مالی یعنی رمزارزها نیز توسعه پیدا کرده است. پرونده تبعه کوزوو با نام مستعار هکر آلبانیایی یکی از نمونه‌های همگرایی فضای سایبر، تروریسم و رمزارزهاست و نشانه‌ای است از آنچه ممکن است در آینده اتفاق بیفتد. در آن ماجرا، اگرچه وی نتوانست هیچ‌گونه بیت‌کوینی اخاذی کند، اما در انجام جرم موفق بود؛ زیرا از توانایی بازیگران تروریستی در انجام هک و دستیابی به اطلاعات محرمانه حکایت می‌کرد.<sup>۴</sup>

درباره‌ی استفاده تروریست‌ها از رمزارزها در طرح‌های باج‌خواهی آنلاین نیز روایات زیادی وجود دارد؛ برای مثال طبق تحلیل‌های انجام‌شده، تروریست‌ها برای عدم افشای داده‌های یک شرکت، ۱۰۰۰ بیت‌کوین مطالبه کردند. در ژانویه ۲۰۱۶، مجرمان با استفاده از باج‌افزار، کنترل رایانه‌های گروه لینکلن را به دست گرفتند و یک باج بیت‌کوین به ارزش ۵۰۰ دلار آمریکا مطالبه کردند. همچنین در نوامبر ۲۰۱۵، سه بانک یونانی به باج‌خواهی تهدید شدند که مطالبه آن‌ها پرداخت صدها یورو به شکل بیت‌کوین بود (Wang & Xixi, 2021, p. 2330). در حملات باج‌افزاری، هکرها فایل‌ها یا داده‌های قربانیان را رمزگذاری و در ازای دسترسی دوباره به فایل‌ها یا داده‌ها، درخواست باج می‌کنند. این‌گونه حملات، از نظر سوددهی رشد در خورتوجهی داشته‌اند و برخی از انواع باج‌افزارها به‌تنهایی تا دومیلیون دلار برای گروه‌های جرایم سایبری سود داشته است.<sup>۵</sup> بیت‌کوین همچنان پرکاربردترین رمزارز در حملات باج‌افزارها و باج‌افزارهاست. همچنین مطابق یکی از گزارش‌های اخیر، ۹۸ درصد موارد مطالعه‌شده درباره‌ی باج‌افزارها و بدافزارها با بیت‌کوین انجام شده بودند، درحالی‌که رمزارز اتر فقط ۱ درصد از موارد را به خود اختصاص داده بود.<sup>۶</sup>

بنابراین دورنما را نمی‌توان نادیده گرفت، اشتراک جرایم سایبری و تروریسم می‌تواند جبهه‌ای جدید در توانایی‌های تروریست‌ها و فرصتی درخور ملاحظه برای تأمین مالی تروریسم باشد. همچنین با گذر زمان تروریست‌ها می‌توانند به فعالیت‌های آنلاین مختل‌کننده پیچیده‌تر با ارزش‌های مجازی مبادرت کنند. بنابراین باید با دقت بیشتری این اشتراکات را رصد و پیش از گسترده‌تر شدن، با آن مقابله کرد.

### ۲-۳. تأمین مالی تروریسم سایبری

تأمین مالی تروریسم را می‌توان به‌اختصار این‌گونه تعریف کرد: «تأمین مالی تروریسم عبارت است از جریان پول و حمایت مالی دولت‌ها، سازمان‌ها یا اشخاص حقیقی به گروه‌های تروریستی؛ به‌نحوی که آن‌ها را به انجام فعالیت‌هایشان قادر سازد» (Sener, 2008, p. 139). کنوانسیون مبارزه با تأمین مالی تروریسم در ماده ۲ خود، این‌گونه به تعریف تأمین مالی تروریسم می‌پردازد: «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 جرایم تروریستی مندرج در کنوانسیون‌های ضمیمه شده، کند».<sup>۷</sup> در قسمت ب بند اول

1. Cyber-Jihad  
2. James Scott  
3. Drew Spaniel

۴. در آگوست ۲۰۱۵، یک تبعه کزوویی به نام اردیت فریزی که با نام مستعار «هکر آلبانیایی» شناخته می‌شد، با نصب بدافزار، به اطلاعات شخصی کارکنان دولت و ارتش ایالات متحده دسترسی پیدا کرد و بعداً داعش، اسامی این اشخاص را که شامل ۱۳۵۱ نفر از پرسنل دولتی و نظامی ایالات متحده بود، به‌عنوان لیست ترور خود منتشر کرد. وی سپس در قبال حذف این بدافزار، درخواست باج از نوع بیت‌کوین کرد (Johnson, 2016).

5. True scale of Bitcoin extortion revealed (2018). MIT Technology Review

6. CipherTrace, Cryptocurrency Anti- MoneyLaundering Report, 2019 Q2, 2019, p. 4. <https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/>

۷. 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 ضدگروگان‌گیری ۱۹۷۹، کنوانسیون حمایت فیزیکی از مواد

ماده دو این کنوانسیون، مصرف کردن وجوهات در فعالیت‌هایی که به قصد کشتار یا ایراد صدمات جسمی شدید به شهروندان غیرنظامی و یا هر فرد دیگری که نقش فعالی در منازعات در زمان درگیری‌های نظامی ندارد؛ به‌ویژه حالاتی که هدف از این اعمال ترساندن یک گروه انسانی، اجبار یک دولت و یا یک سازمان بین‌المللی به انجام یا ترک یک عمل باشد، مصداق تأمین مالی تروریسم تلقی می‌شود. ماده یک کنوانسیون، در تعریف واژه‌ها به انواع عناوین نقدینگی و پول اشاره می‌کند و استفاده و یا انتقال آن‌ها به عوامل تروریستی را مصداق تأمین مالی تروریسم می‌داند و در این باره استفاده یا انتقال وجه نقد، اعتبار بانکی یا الکترونیکی، چک و تراول چک، کارت بانکی، سهام، گواهی اعتبار یا تمکن مالی، سفارش پول، پرداخت هزینه‌ها به نیابت از عوامل تروریستی از مصادیق تأمین مالی تروریسم بیان شده است. در همین ماده، کمک‌ها، اعانات و ارائه امکانات دولتی به عوامل تروریستی شامل هرگونه تسهیلات دائمی یا موقتی در هر شکل از سوی هر مقام دولتی در هر سطح، مصداق مساعدت دولتی به عوامل تروریستی تلقی شده است (CFT, 1999, Article 2).

هرچند گروه‌های تروریستی از حمایت برخی دولت‌ها برخوردارند، اما از قرن ۲۱ به بعد و با توجه به اعمال فشار مقررات و نهادهای ناظر بین‌المللی، که مانعی بر سر راه دریافت کمک‌های مالی از دولت‌ها بود، این گروه‌ها سعی کردند که از لحاظ منابع مالی به خود متکی شوند و شیوه‌های تولید درآمد داخلی را تجربه کنند. به همین منظور، گروه‌های تروریستی به روش‌ها و وسایل تولید درآمد بدون اتکا به دولت‌ها و حامیان مالی متوسل شدند.

البته باید توجه داشت که تأمین مالی تروریسم تنها تأمین بودجه یک عملیات تروریستی خاص نیست؛ بلکه تأمین گسترده‌تر هزینه‌های سازمانی، توسعه و حفظ سازمان‌های تروریستی و ایجاد یک محیط برای تقویت فعالیت‌های آن‌ها را نیز دربرمی‌گیرد با پیشرفت هرچه بیشتر تجهیزات ایمنی در سطح جهان، نقض امنیت نیز مستلزم هزینه بیشتر خواهد بود؛ از این رو گروه‌های تروریستی برای مقابله با چنین وضعیتی ناچار به صرف هزینه‌های بسیاری هستند تا بتوانند در نقض امنیت و ایجاد چالش موفقیت کسب کنند. به همین علت، این گروه‌ها به وسایل گوناگونی متوسل می‌شوند تا بتوانند هزینه‌های معیشتی و نیز عملیاتی خود را تأمین کنند. هر اقدام تروریستی مستلزم صرف هزینه است و این نکته بسیار مهم است که به هر میزان این گروه‌ها منابع مالی بهتری در اختیار داشته باشند، حملات بزرگ‌تر و موفق‌تری انجام خواهند داد (Acharya, 2009, p. 33). انجام یک اقدام تروریستی متضمن خرید وسایل لازم نظیر تفنگ، مواد منفجره، لوازم ارتباطی و غیره است که با توجه به تأمین آن‌ها از بازار سیاه، هزینه صرف شده برای تروریست‌ها را افزایش می‌دهد. علاوه بر این، سازمان‌ها و گروه‌های تروریستی همچون سازمان‌های عادی (غیرتروریستی) هزینه‌های بسیاری را صرف نگهداری از خود می‌کنند؛ برای نمونه هزینه عضوگیری جدید برای سازمان و ساختن کمپ‌های آموزشی برای اعضا، از جمله مواردی است که برای سازمان هزینه‌بردار است. در نتیجه پول را باید به‌مثابه خونی در رگ‌های سازمان‌های تروریستی دانست؛ به‌گونه‌ای که بدون وجود آن این سازمان‌ها قادر به ادامه حیات یا انجام فعالیت‌های خود برای مدت طولانی نیستند (کدخدایی و فامیل زوار جلالی، ۱۴۰۲، ص ۶).

با توجه به هزینه‌هایی که گروه‌های تروریستی در راستای سازمان‌دهی و به‌انجام‌رساندن حملات خود صرف می‌کنند، باید برای تأمین مالی خود فعالیت‌های گوناگونی انجام دهند که شامل فعالیت‌های قانونی و غیرقانونی می‌شود. توسل به اقدامات قانونی همچون تجارت، مؤسسات خیریه و حمایت دولت‌ها از شیوه‌های رایج گروه‌های تروریستی برای تأمین مالی است که از یک‌سو، گروه را در معرض پیگرد قانونی قرار نمی‌دهد و از این‌رو آسان‌تر می‌توانند اهداف سیاسی خود را پیگیری کنند و از سوی دیگر، در کنار انجام فعالیت‌های مشروع، فعالیت‌های مجرمانه بسیاری از جانب اعضای گروه‌ها برای کسب بودجه انجام می‌شود. قاچاق نفت و اسلحه، غارت آثار باستانی و آدم‌ربایی از بارزترین اقدامات محبوب سازمان‌های تروریستی برای کسب درآمد است (الهویی نظری و فامیل زوار جلالی، ۱۳۹۶، ص ۷۲۸).

هسته‌ای ۱۹۸۰، پروتکل سرکوب رفتارهای خشونت‌آمیز غیرقانونی در فرودگاه‌های مورد استفاده هواوردی بین‌المللی غیرنظامی ۱۹۸۸، کنوانسیون سرکوب اقدامات غیرقانونی ضدامنیت پروازهای غیرنظامی ۱۹۸۸، پروتکل سرکوب اقدامات غیرقانونی ضد تأسیسات ثابت در فلات قاره ۱۹۸۸ و کنوانسیون بین‌المللی سرکوب بمب‌گذاری‌های تروریستی ۱۹۹۷، ۱۱.

با پیشرفت فناوری‌های مالی از یک‌سو و با افزایش نظارت و کنترل نهادهای ناظر داخلی و بین‌المللی در راستای مسدودسازی منابع مالی گروه‌های تروریستی از سوی دیگر، این گروه‌ها نیز وارد شیوه‌های جدید تأمین مالی خواهند شد تا بتوانند از رهگیری مقامات ناظر در امان بمانند؛ در نتیجه موفقیت در راهبردهای مقابله با تأمین مالی تروریسم در کاهش دسترسی تروریست‌ها به منابع مالی و به‌ویژه ارزش‌های فیات این نگرانی را ایجاد می‌کند که گروه‌های تروریستی برای تأمین مالی فعالیت‌های خود، شیوه‌ها و فناوری‌های به‌روز را امتحان کنند. یکی از فناوری‌هایی که در زمینه پولشویی و تأمین مالی تروریسم امکانات فراوانی در اختیار تروریست‌ها قرار می‌دهد، رمزارزها هستند.

در نبود نظارت سیستم مالی جهانی و پایش دقیق، رمزارزها و در رأس آن، بیت‌کوین برای سازمان‌های تروریستی که برایشان گمنامی، سرعت و منابع درآمدی جهانی در اولویت است، جذابیت خاصی خواهد داشت. اجتناب از کانال‌های پولی رسمی و حتی دارایی‌های نقدی ملموس، که قابلیت مسدودشدن دارند، علت عمده استفاده از این سیستم برای تأمین مالی و جذب سرمایه از طریق سازمان‌های تروریستی است. با توجه به تکامل سازمان‌های تروریستی و استفاده آن‌ها از رویکردهایی شبیه به کسب‌وکار در ساختارهای مالی، احتمال تحولات و حتی انقلاب در تأمین مالی تروریسم از طریق ارزش‌های مجازی وجود دارد. اگرچه نفس عمل تروریستی نوعی ارائه خدمات در ازای کمک‌های مالی محسوب می‌شود، اما برخلاف کارت‌های مواد مخدر و سایر فعالیت‌های مجرمانه، حامیان مالی تروریست‌ها انتظار دریافت مستقیم یک کالا را ندارند؛ در نتیجه برای سازمان‌های تروریستی، رمزارزها گزینه مالی بسیار مهمی هستند؛ زیرا پتانسیل ادغام در چهارچوب تأمین مالی خود را دارند. در ادامه، به طور خاص به نقش بیت‌کوین در تأمین مالی تروریسم پرداخته می‌شود.

### ۳-۳. استفاده از بیت‌کوین در تأمین مالی تروریسم

همان‌گونه که سازمان‌های تروریستی در حال فاصله‌گرفتن از روش‌های سنتی نبرد و سازمان‌دهی هستند، تکامل رویه آن‌ها در تأمین مالی و جذب سرمایه نیز دور از انتظار به نظر نمی‌رسد. در حالی که تروریست‌های امروزی عمدتاً به حامیان مالی دولتی یا فردی متکی‌اند، فاصله‌گرفتن بازارها و سازمان‌های غیرقانونی بین‌المللی از دارایی‌های نقدی ملموس، باعث روی آوردن آن‌ها به ارزش‌های مجازی شده که با ویژگی‌هایی همچون گمنامی، رهگیری و مسدودسازی آن‌ها را غیرممکن یا دست‌کم دشوار و زمان‌بر می‌کند. با توجه به این که نخستین راهبرد ضد تروریسم هر کشوری، حذف تأمین مالی از طریق رهگیری و مسدودسازی دارایی‌هاست؛ بنابراین بیت‌کوین از نظر روش برخورد دولت‌ها و مؤسسات با فعالیت‌های تروریستی، تهدیدی مهم محسوب می‌شود. با افزایش شبکه‌های تروریستی، که تصمیم می‌گیرند از بیت‌کوین و سایر ارزش‌های مجازی در چهارچوب مالی خود استفاده کنند، سیاست‌های ملی و بین‌المللی ضد تروریسم نیز نیازمند یک خانه‌تکانی و انطباق چشمگیر با این رویداد هستند.

فرضیه استفاده تروریست‌ها از ارزش‌های مجازی نظیر بیت‌کوین نه تنها جدی است، بلکه به مرحله عملیاتی رسیده است. نمونه‌های متعددی وجود دارد که نشان‌دهنده ورود گروه‌های تروریستی در حوزه تأمین مالی تروریسم از طریق ارزش‌های مجازی است. در فوریه ۲۰۱۸، تحلیلگر تروریسم، مایکل اشمیت، از شرکت مشورتی امنیت ملی آمریکا،<sup>۱</sup> اعلام کرد که نشریه آنلاین القاعده تحت عنوان ال‌حقیقت مقاله‌ای را درباره کاربردهای بیت‌کوین منتشر کرده است که شامل بحث درباره مجاز بودن یا نبودن بیت‌کوین در شرع و چالش‌های آن است. در این مقاله، نتیجه‌گیری می‌شود که «می‌توان به شکل‌های مختلف از رمزارزها برای مقاصد خود استفاده کرد، اما موانع زیادی نیز در این راه وجود دارد».<sup>۲</sup> برخی افراط‌گرایان حتی کتابی با عنوان بیت‌کوین و صدقات‌الجهاد منتشر کرده‌اند که در آن، نحوه انتقال بیت‌کوین از آمریکای شمالی و غرب اروپا به جهادی‌ها به‌وضوح تشریح می‌شود. طبق گزارش‌ها، بحرین نعیم،<sup>۳</sup> طراح حملات تروریستی جاکارتا در سال ۲۰۱۶، برای پرداخت مجازی و انتقال وجوه به عناصر مسلح و تأمین مالی فعالیت‌های تروریستی آن‌ها از بیت‌کوین استفاده کرد (Wang & Xixi, 2021, p. 2330).

1. Kronos Advisory

2. <https://twitter.com/MichaelSSmithII/status/959293289823285248>

3. Bahrun Naim

همچنین گروه تروریستی داعش علناً پیشنهاد استفاده از بیت‌کوین‌ها برای تأمین مالی عملیات‌های خود در سراسر جهان را مطرح کرده است. در مقاله‌ای موسوم به «بیت‌کوین و کمک‌های خیریه برای مبارزه خشونت‌آمیز» به قلم تقی‌الدین ماتتیر، که از اعضای داعش است، آمده: «این سیستم [بیت‌کوین] پتانسیل زنده‌کردن سنت فراموش‌شده کمک مالی به مجاهدین را دارد؛ چون ساده و آسان است و پروردگار نیز اسباب استفاده سریع‌تر ما از آن را فراهم خواهد کرد» (Higgins, 2014, p. 3). وی در این مقاله استدلال می‌کند که داعش برای این‌که بتواند عملیات تروریستی خود را تأمین مالی کند، باید خارج از چهارچوب سیستم مالی مرسوم فعالیت کند (Nimmo, 2014, p. 5).

نمونه‌ای دیگر: در سال ۲۰۱۵ فردی به نام ابوالاحمد الرقه از هواداران داعش درخواست کرد که کمک‌های بیت‌کوینی خود را در دارکوب ارائه کنند. در ژانویه ۲۰۱۵ هآرتز نخستین مورد از استفاده یک سلول تروریستی داعش برای جذب سرمایه با بیت‌کوین از طریق دارکوب را گزارش کرد. جمع‌کننده سرمایه فردی به هویت ابومصطفی بود که از شماره حساب بیت‌کوین او مشخص شد که تا پیش از بسته‌شدن حساب وی از طریق افبی‌آی، پنج بیت‌کوین جمع‌آوری کرده بود (Ellis, 2016). همچنین از برخی بحث‌های صورت‌گرفته در انجمن‌های وبسایت‌های مرتبط با این گروه، مشخص بود که اعضای فنی در تلاشی گسترده‌تر به دنبال آموزش هم‌تایان خود برای استفاده از ارزهای مجازی هستند.<sup>۱</sup> شرکت‌کنندگان در این بحث‌های انجمنی، همچنین اشاره کردند که گاهی از ارزهای مجازی برای انتقال پول به کشورهای استفاده می‌شد که به علت نبود ظرفیت کافی شبکه یا رصد و مقررات سختگیرانه، انجام تراکنش‌های سنتی در آن‌ها دشوار است (European Parliamentary Research Service, 2015).

برخی سازمان‌های خیریه از جمله سازمان خیریه «الصدقه»، از نهادهای مرتبط با القاعده، نیز به استفاده از بیت‌کوین برای دریافت کمک‌های مالی روی آورده‌اند. این سازمان کمپین سرمایه‌گذاری جمعی است که در اواخر سال ۲۰۱۷ در کانال‌های تلگرامی مرتبط با القاعده راه‌اندازی شد. این کمپین در ابتدا از هواداران خواست که برای سرمایه‌گذاری در یک پروژه ساخت تأسیسات در استان لاذقیه سوریه، کمک‌های خود را به شکل گمنام و امن از طریق بیت‌کوین ارسال کنند. تا اول آوریل ۲۰۱۸، الصدقه برای جمع‌آوری کمک از طریق توییتر، از هوادارانش درخواست می‌کرد که به شکل گمنام و بدون هیچ‌گونه ردیابی، با ثروت خود از مجاهدین در سوریه پشتیبانی کنند (Fanusie, 2017). اما چه عواملی باعث می‌شود که گروه‌های تروریستی برای تأمین مالی و همچنین نقل و انتقالات مالی خود به بیت‌کوین نظر مثبت داشته باشند و هواداران خود را نیز به این کانال مالی رهنمود کنند. جدا از مزایایی که در بخش‌های ابتدایی مقاله اشاره شد، بیت‌کوین دارای ویژگی‌هایی است که استفاده از آن‌ها را برای تروریست‌ها جذاب می‌کند.

قابلیت تراکنش‌های گمنام و شبه‌گمنام بیت‌کوین شکلی از سرمایه را برای تروریست‌ها فراهم کرده که با اهداف حامیان مالی آن‌ها بسیار متناسب است. به این ترتیب، ماهیت بدون مرز بیت‌کوین، باعث افزایش وابستگی جهادی‌ها به حامیان آن‌ها می‌شود که به‌طور فزاینده‌ای خواهان کمک به تروریست‌ها از سراسر دنیا و احساس شراکت مستقیم در عملیات‌های این گروه‌ها هستند. نوع تشخیص هویت در بیت‌کوین تهدید امنیتی جدی است؛ زیرا ذاتاً اثر تلاش‌های ضدتروریسم جامعه بین‌المللی را خنثی می‌کند. در بُعد عملی، از آنجاکه بیت‌کوین و شبکه عملیاتی آن، قطع جریان تراکنش‌ها یا مسدودسازی دارایی‌ها را برای مراجع مالی ضدتروریسم دشوار می‌سازند، شاهد آن هستیم که این گروه‌ها در حال روی آوردن به بیت‌کوین و استفاده از آن برای پشتیبانی مالی عملیات‌های خود هستند؛ البته باید دانست که این میزان اغراق درباره‌ی گمنامی و ناشناس بودن در خصوص رمزارزها و به‌ویژه بیت‌کوین صحیح نیست. توصیف بهتر برای بیت‌کوین، «شبه‌گمنامی»<sup>۲</sup> است. چراکه اگرچه هویت واقعی یک کاربر روی بلاک‌چین مشهود نیست، اطلاعات مربوط به تراکنش‌های آن‌ها - مانند تاریخ‌ها، ارزش‌ها و آدرس‌های بیت‌کوین طرف‌های مقابل - همگی به‌طور عمومی ثبت می‌شوند. به‌علاوه، چون بلاک‌چین شامل آرشیو زمانی از تراکنش‌هاست، می‌توان به مجموعه‌ای از اطلاعات درباره‌ی جابه‌جایی‌های بیت‌کوین دست یافت. بنابراین، اگر مشخص باشد که مالک یک آدرس عمومی بیت‌کوین چه شخصی

1. Europol, (2017), EU Terrorism Situation and Trend Report (TE-SAT), The Hague, 2017, <https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017>.

2. Pseudonymous

است، می‌توان دربارهٔ فعالیت آن‌ها در شبکه، مقادیر درخور توجهی اطلاعات جمع‌آوری کرد؛ اما گفتنی است همین میزان از شبه‌ناشناسی نیز برای گروه‌های مجرمانه و به‌ویژه تروریست‌ها مفید است. به‌رحال ارسال آدرس عمومی کیف پول بیت‌کوین در یک شبکهٔ اجتماعی، به‌مراتب بهتر و امن‌تر از تبلیغ شماره‌حساب بانکی در یک بانک یا مؤسسهٔ مالی رسمی است (کدخدایی و نوروزپور، ۱۳۹۹، ص ۱۶).

یکی دیگر از ویژگی‌های جذاب بیت‌کوین برای گروه‌های تروریستی، قابلیت نقل و انتقال بین‌المللی آن‌ها بدون واسطه‌های قانونی است. همان‌گونه که اشاره شد، سیستم‌های مبتنی بر بلاک‌چین نه تنها باعث کاهش هزینه‌های دخیل در تراکنش‌ها می‌شوند، بلکه به افزایش شایان توجه سرعت انتقال نیز منجر می‌شوند. این ویژگی برای تروریست‌ها مفید خواهد بود؛ زیرا از این راه می‌توانند بدون مراجعه به یک بانک یا مؤسسهٔ مالی، از هواداران خود در سراسر دنیا کمک مالی دریافت کنند. تمرکززدایی نیز از دیگر مزیت این نوع دارایی است. در بیت‌کوین، هیچ نهاد یا مرکزی وجود ندارد که بتواند مانع دستیابی یک فرد به شبکهٔ بلاک‌چین یا بیت‌کوین شود و به‌عبارتی دارایی‌های او را مسدود و توقیف کند؛ البته باید به این واقعیت عملی اشاره کرد که شبکه‌های رمزارز پر از واسطه‌های متمرکزند. درست است که دو کاربر می‌توانند بیت‌کوین را به‌صورت همتابه‌همتا (P2P) و تقریباً به‌سادگی در شبکهٔ بیت‌کوین دادوستد کنند، اما انجام صفر تا صد این امر بدون کمک طرف ثالث معمولاً دشوار است؛ در نتیجه گروه‌های تروریستی برای فرار از هرگونه رهگیری، از صرافی‌های غیرمتمرکز استفاده می‌کنند.

ناتوانی نهادهای ناظر در رهگیری دقیق و جدی در حوزهٔ ارزهای مجازی نیز چراغ سبزی برای تروریست‌ها برای فعالیت در این حوزه از فتاوری است. اگرچه صندوق بین‌المللی پول، گروه ویژهٔ اقدام مالی و سایر سازمان‌های بین‌المللی سال‌هاست که مجموعه‌ای از برنامه‌های ضدپولشویی و ضدتروریسم را آغاز کرده‌اند، اما روند توسعهٔ نظارت قضایی در کشورهای مختلف، یکسان نیست و مشکل نظارت ناسازگار، که ناشی از تفاوت در میزان توسعه‌یافتگی سیستم‌های مالی کشورهای مختلف است، همچنان پابرجاست (Ponsford, 2015). برای مثال قوانین و مقررات رمزارزها در چین، آمریکا و استرالیا متفاوت است و همین امر باعث نظارت ناسازگار می‌شود و ناسازگاری در مقررات رمزارزها، تلاش‌ها برای جلوگیری از فعالیت‌های مجرمانه‌ای را که به قصد سوءاستفاده از فتاوری صورت می‌گیرند ناکام خواهد گذاشت. یکی از ارزیابی‌های مستند انجام‌شده که نشان‌دهندهٔ ناکارآمدی بخش نظارتی در حوزهٔ ارزهای مجازی است، ارزیابی و گزارشی است که گروه ویژه اقدام مالی انجام داده است. این کارگروه در ژوئن ۲۰۱۹ راهنمای رویکردهای ریسک‌محور دارایی‌های مجازی و خدمات‌دهندگان این دارایی‌ها را منتشر کرد و در جولای ۲۰۲۰، نتایج بررسی یک‌سالهٔ خود دربارهٔ پابندی به این راهنما را اعلام کرد. طبق این بررسی، ۱۹ حوزه از ۵۴ حوزهٔ قضایی گزارش‌دهنده هنوز نتوانسته‌اند استانداردهای لازم را در راهبردهای موجود در قوانین داخلی پیاده کنند که این آمار نسبت به کل جامعهٔ بین‌المللی ضعیف ارزیابی می‌شود.<sup>۱</sup> در سطح جهانی، اگرچه برخی کشورها مانند کشورهای حوزهٔ اتحادیهٔ اروپا دپارتمان‌های خاصی را برای تنظیم مقررات رمزارزها از جمله بیت‌کوین در نظر گرفته‌اند، بسیاری از کشورها همچنان اقدام خاصی دربارهٔ رمزارزها نکرده‌اند. این شکاف‌ها در سیستم نظارتی جهانی، باعث ایجاد خلأهای بزرگ در زمینهٔ رمزارزها و سوءاستفادهٔ تروریست‌ها از این خلأها می‌شود. در کشورهایی که نظام‌های مالی نسبتاً ضعیفی دارند و رژیم‌های مبارزه با تأمین مالی تروریسم آن‌ها نیز ناقص است، نظارت بر رمزارزها بسیار ضعیف یا صفر است. حتی در کشورهایی که نظارت سخت‌گیرانه‌ای نیز دارند، به علت ناسازگاری مقررات نظارتی میان کشورها یا مناطق مختلف نمی‌تواند مانع تأمین مالی تروریسم شود و این وضعیت، فرصتی مناسب برای استفادهٔ سازمان‌های تروریستی از رمزارزها فراهم می‌کند. بنابراین، مکانیسم‌های ضدپولشویی و ضدتروریسم موجود هنوز در حدی نیست که بخواهد با این‌گونه فتاوری‌های نوظهور مقابله کند و این مهم، یکی از دیگر دلایل تمرکز سازمان‌های تروریستی بر بیت‌کوین است.

عملی بودن استفاده از بیت‌کوین از منظر منتقدان نیز باید بررسی شود. برخی منتقدان معتقدند که بیت‌کوین بسیار نوسان‌پذیر است و برخی دیگر استدلال می‌کنند که شبکه‌های تروریستی به‌علت نداشتن قابلیت‌های استخراج بیت‌کوین قادر به ادغام آن در سیستم مالی خود نخواهند

1. Financial Action Task Force, (2020), 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs, FATF Report, retrieved from: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html>

بود. به علاوه، با توجه به مشخصات فعلی بسیاری از ارزش‌های مجازی، به ویژه آسیب‌پذیری بالا و چالش‌هایی که در استفاده این ارزش‌ها برای انتقال یا جابه‌جایی وجوه در حجم‌های بالا وجود دارد، احتمالاً روش مطمئنی برای گروه‌های تروریستی سازمان‌یافته نیستند. در پاسخ گفتنی است درست است که اغلب سازمان‌های تروریستی فاقد قابلیت‌های استخراج هستند (که البته غیرممکن نیست)، اما اراده لازم برای متنوع‌سازی منابع درآمدی خود را دارند که می‌تواند به استفاده از بیت‌کوین یا سایر دارایی‌های مجازی منجر شود. شبکه‌های تروریستی اصلاً نیاز مستقیم به استخراج ندارند. آن‌ها می‌توانند استخراج بیت‌کوین را برون‌سپاری کنند؛ یعنی مسئولیت تأمین و استخراج آن را در قالب قرارداد به افراد یا گروه‌های خارج از سیستم خود بسپارند. امروزه استفاده از بیت‌کوین به منزله مکانیزمی برای جذب سرمایه در حال انجام بوده و بیشتر مبتنی بر کمک‌های مالی هواداران سازمان است؛ هرچند هنوز به منبع اصلی تأمین سرمایه مبدل نشده است. در ادامه، از جایگاه بیت‌کوین در تأمین مالی تروریسم پیش‌بینی آینده‌نگرانه‌ای ارائه خواهد شد.

#### ۴. آینده بیت‌کوین در حوزه تأمین مالی تروریسم

چشم‌انداز اصلی برای ایجاد بیت‌کوین جایگزین کردن آن با ارزش‌های سنتی موجود به منظور استفاده به منزله ابزار مبادله در انجام تراکنش‌های روزمره و ذخیره آن به مثابه ارزش<sup>۱</sup> در غیاب نظارت و کنترل دولتی بود (آتوود، ۱۳۹۸، ص ۱۸۳). بیت‌کوین در بسیاری از نقاط جهان پذیرفته شده و رشد آن چشمگیر است. این رمزارز و رقبا آن از جمله اتریوم<sup>۲</sup> با تهیه برنامه‌های کاربردی در حال ادامه‌دادن به رشد خود هستند. از زمان ایجاد بیت‌کوین در دهه‌های گذشته، هر ساله ویژگی‌هایی جدید در استفاده از بیت‌کوین کشف شده که امکانات آن را برای استفاده گسترش می‌دهد. زمانی بیت‌کوین در یک دایره کوچک از علاقه‌مندان ارزش‌های دیجیتال قرار داشت، اما امروزه بیت‌کوین توسط هزاران کسب‌وکار در سراسر جهان پذیرفته شده است (آتوود، ۱۳۹۸، ص ۱۹۴).

اگرچه بیت‌کوین به شکل فوق‌العاده‌ای نوآورانه و جهانی شده است، اما همچنان بسیار نوسان‌پذیر است که این یکی از معایب مهم آن محسوب می‌شود و آن را به رقابت با سایر اشکال رمزارزها و حتی اشکال سنتی تأمین مالی مجبور می‌کند. عرضه بیت‌کوین محدود و تقاضا برای آن متغیر است. همین تغییرپذیری باعث شده که قیمت آن به شدت پیش‌بینی‌پذیر باشد. برخی اقتصاددانان استدلال می‌کنند که بیت‌کوین در نهایت با ویژگی‌های عالی خود، جای تمام رمزارزهای موجود را خواهد گرفت. این دسته معتقدند تازمانی که بازارهای دارک‌وب وجود دارند، بیت‌کوین به منزله ارز مطلوب دنیای دیپ‌وب<sup>۳</sup> به حیات خود ادامه خواهد داد. اگرچه ممکن است در جاهایی، ارزش‌های رقابتی تر و جذاب‌تری ظهور کنند، اما از نظر مسائل امنیتی فعلی در خصوص تأمین مالی تروریسم، بیت‌کوین فعلاً حرف اول را می‌زند (Prisco, 2014, p. 6). همچنین با وضع موجود که در آن، دولت‌ها و آژانس‌های امنیتی سراسر دنیا در حال نظارت سنگین بر بازارهای مالی قانونی هستند، شبکه‌های تروریستی و سایر بازیگران غیرقانونی، برای بقا مجبور به متنوع‌سازی چهارچوب مالی خود خواهند شد. این نیاز به متنوع‌سازی در کنار مزایایی همچون گمنامی، باعث سوق بیشتر شبکه‌های تروریستی به سمت ارزش‌های مجازی به خصوص بیت‌کوین می‌شود؛ البته بی‌شک به زودی شاهد فاصله گرفتن کامل از ارزش‌های سنتی در حوزه تأمین مالی تروریسم نخواهیم بود؛ بلکه توانایی بیت‌کوین در ایفای نقشی ثابت و مؤثر در تأمین مالی تروریسم، آن را به سلاحی تبدیل کرده که امروزه دولت‌ها برای رهگیری و مسدودسازی آن با مشکل مواجه‌اند.

#### 1. Value

۲. اتریوم (Ethereum): در سال ۲۰۱۴ با هدف افزایش هرچه بیشتر قابلیت توزیع‌شدگی ارزش‌های دیجیتال راه‌اندازی شد. این ارز از ساختاری مشابه ارزش‌های دیجیتال بهره می‌برد؛ اما با وجود الهام گرفتن از سیستم ارزش‌های دیجیتال، تفاوت‌های زیادی را می‌توان در این ارز مشاهده کرد (ریاضی‌مند، ۱۳۹۷، ص ۳۹).

۳. Deep Web: دیپ‌وب، که گاهی اوقات دیپ‌نت نیز نامیده می‌شود، سیستم‌های واسط عمومی تعریف می‌شوند که از طریق گوگل یا یاهو نمایه‌گذاری نشده‌اند و معمولاً به یک کوه یخ تشبیه می‌شود که بخش‌هایی از آن، قابل رؤیت هستند. دیپ‌وب پر است از محتواهای بدون لینک (صفحات وبی که فاقد لینک به سایر صفحات وب هستند)، صفحات وب خصوصی که بدون احراز هویت اجزای دسترسی به شما نمی‌دهند، محتواهای با دسترسی کنترل‌شده (با استفاده از ابزارهای فنی برای کنترل چیزهای نمایه‌گذاری شده، برای مثال فایل Robots.txt)، محتواهای اسکرپت‌شده که فقط از طریق جاوا اسکریپت قابل دسترسی هستند، محتواهای بدون HTTP(S) ها مانند سرورهای پروتکل Gopher و پروتکل انتقال فایل (FTP). برای مطالعه بیشتر رجوع کنید به: (Singletary, 2015, pp. 108- 109).

با توجه به این که سازمان‌های تروریستی نیازمند کمک مالی هواداران خود در سطح جهان هستند و با توجه به این که در صورت مسدود شدن منابع اصلی تأمین مالی این کمک نباید متوقف شود. بیت‌کوین‌ها توانایی تبدیل شدن به یک منبع جایگزین و نجات‌بخش برای سازمان‌های تروریستی را دارند.<sup>۱</sup> بیت‌کوین‌ها سلاح‌هایی هستند که قادر به منسوخ کردن سیاست‌های ضدتروریسم دولتی و بین‌المللی بوده و به این ترتیب می‌توانند یکی از قوی‌ترین ابزارها علیه تروریسم را به‌طور کامل بی‌اعتبار سازند. سرعت انطباق شبکه‌های تروریستی بسیار بیشتر از سیاست‌ها و راهبردهای ضدتروریسم است که این امر بیانگر شکست دولت‌ها و جامعه بین‌المللی در صحنه نبرد سایبری است. امروزه متنوع‌سازی چهارچوب‌های مالی، اقدام راهبردی بعدی گروه‌های تروریستی مانند داعش است؛ چون در حال پا گذاشتن به قلمروی هستند که دولت‌ها و جامعه بین‌المللی توان مقابله با آن را به نحو احسن ندارند. ماهیت بیت‌کوین و ارزهای مجازی به گونه‌ای است که مشوق‌های حرکت به سمت آن هم‌چنان بر خطرات و نوسان‌پذیری آن سنگینی می‌کنند. اگر بیت‌کوین خود را به شکل فرصتی امن و مؤثر برای توسعه نشان دهد، تردیدی نمی‌ماند که سازمان‌های تروریستی به استفاده و سرمایه‌گذاری در آن چشم خواهند دوخت.

### نتیجه‌گیری

با عنایت به مزایای بی‌شمار و معایب محدود ارزهای مجازی در حوزه تأمین مالی و تجارت، جای تردیدی باقی نمی‌ماند که این ارز، در حال تبدیل شدن به یک گزینه برای بازیگرانی است که با هدف رهگیری‌نشدن وجوه، به دنبال دورزدن موانع قانونی هستند. به نظر می‌رسد که ارزهای مجازی به‌خصوص بیت‌کوین با ویژگی‌هایی چون گمنامی، سرعت تراکنش و بازدهی بالا در حال بازی در صحنه یک تئاتر بسیار خطرناک یعنی بازارهای غیرقانونی بوده و پتانسیل انقلاب در حوزه تأمین مالی تروریسم را دارند. می‌توان ادعان کرد که بیت‌کوین باعث انقلاب در سیستم‌های پشتیبانی مالی شبکه‌های تروریستی خواهد شد و مؤثرترین سیاست‌های ضدتروریسم امروزی را منسوخ خواهد ساخت؛ زیرا باید به این نظریه معتقد بود که هرچه راهبرد مقابله با تأمین مالی تروریسم در کاهش دسترسی شبکه‌های تروریستی به ارز فیات و سیستم‌های مالی سنتی موفق عمل کند، احتمال روی آوردن این شبکه‌ها به استفاده از نوآوری‌های فناوری مالی از جمله ارزهای مجازی مثل بیت‌کوین را افزایش خواهد داد. ویژگی‌های ارزهای مجازی، همچون بیت‌کوین، گزینه جذابی برای شبکه‌های تروریستی هستند تا با ادغام آن در ساختار مالی خود، امکان رهگیری خود را بیش از پیش دشوار سازند؛ البته باید در نظر داشت که اگرچه سازمان‌های تروریستی در حال استفاده از بیت‌کوین هستند، بیت‌کوین فعلاً نمی‌تواند رقیبی برای استفاده مستقیم از دارایی‌های ملموس همانند ارزهای فیات محسوب شود و با توجه به نوسان‌پذیری و خطرات ادامه‌دار در استفاده از بیت‌کوین، نمی‌توان با قاطعیت استدلال کرد که سازمان‌های تروریستی کاملاً به ارزهای مجازی متکی خواهند شد و ارزهای فیات و شیوه‌های سنتی تأمین مالی را کنار خواهند گذاشت؛ اما می‌توان معتقد بود که بیت‌کوین راهی برای متنوع‌سازی سرمایه در آمدی است که به‌ویژه در صورت مسدودسازی یا قطع سایر دارایی‌ها در اقدامات ضدتروریسم، می‌تواند نفس موقت برای ادامه حیات سازمان باشد؛ بنابراین عقیده نگارندگان بر این است که امروزه بیت‌کوین بیشتر مکملی برای تأمین مالی این گونه شبکه‌ها در کنار پشتیبانی‌های مالی سنتی و سایر انواع کمک‌های مالی است. در پایان باید اشاره داشت که اگر واکنش دولت‌ها بی‌نتیجه یا کم‌اثر باشد، جامعه بین‌المللی در آینده با چالش‌های مهمی در حوزه تأمین مالی تروریسم مواجه خواهد شد. در عصر فناوری مالی امروز، که ما در آن زندگی می‌کنیم، نوآوری به قصد بهبود تجارت قطعاً ضروری است؛ اما ابزارهایی که بشر ایجاد می‌کند معمولاً به سلاح‌هایی تبدیل خواهند شد که خود بشر آمادگی مقابله با آن‌ها را ندارد. چگونگی مقابله با ریسک‌های فناوری‌های نوظهور نیازمند تصمیم‌گیری و اقدامی جامع در سطح بین‌المللی است که این چالش می‌تواند موضوع تحقیقات آینده قرار گیرد.

۱. با توجه به قهرمان‌بودن گروه‌های تروریستی از دیدگاه برخی افراد، این احساس همدردی برای طرفداران آن‌ها به وجود می‌آید که کمک‌هایی را برای آنان در نظر بگیرند. این امر به‌ویژه زمانی که عامل ارتباط‌دهنده گروه‌های تروریستی به حامیان، عاملی قوی باشد بیشتر به چشم می‌آید. مذهب و قومیت مشترک از جمله عوامل مؤثر و قدرتمندی هستند که می‌تواند در این باره نقش اساسی و مهمی را ایفا کند (کارگری، ۱۳۹۱، ص ۲۶۱ به نقل از فامیل زوار جلالی، ۱۳۹۵، ص ۸۸).

## منابع

- ابوذری، مهنوش (۱۳۹۱). تروریسم سایبری؛ ترور در دنیای صفر و یک. فصل‌نامه بین‌المللی شهر قانون، ۲۰(۳)، ۷۰-۷۲. آتوود، مارک (۱۳۹۸). توضیح بلاک چین + توضیح بیت‌کوین. ترجمه مرتضی شانی. تهران: شرکت چاپ و نشر بازرگانی. آذرنژاد، مهدی (۱۴۰۱). حقوق داری‌های رمزنگاری شده. تهران: مجلد.
- پژوهشکده آمار و فناوری اطلاعات قوه قضاییه (۱۴۰۰). پدیده‌شناسی رمزارزها و فناوری زنجیره بلوکی (بلاکچین). تهران: مرکز مطبوعات و انتشارات قوه قضاییه.
- رزمخواه، نجمه (۱۴۰۲). نقدی بر پیش‌نویس قانون اتحادیه اروپا در همسان‌سازی قوانین حاکم بر هوش مصنوعی از منظر مقابله با تروریسم سایبری. فصل‌نامه مطالعات حقوق عمومی، زودآیند.
- ریاضی‌مند، سیدمهران (۱۳۹۷). بررسی ابعاد حقوقی ارزشهای دیجیتال. تهران: انتشارات برتراندیشان.
- شرکت پریپتو (۱۴۰۰). بیت‌کوین. ترجمه بهروز خدارحمی. تهران: نشر آوند دانش.
- عبادی لمر، صالح (۱۳۹۹). سرمایه‌گذار در ارزشهای دیجیتال و جایگاه آن در ایران. تهران: مؤسسه فرهنگی هنری دیباگران.
- فامیل زوار جلالی، امیر (۱۳۹۵). مسئولیت بین‌المللی دولت‌ها ناشی از تأمین مالی تروریسم. تهران: نشر خرسندی.
- قاسمی، غلام‌علی و باقرزاده، سجاد (۱۳۹۴). جایگاه حقوق بشر در مبارزه با سایبر تروریسم. مجله حقوقی بین‌المللی، ۳۲(۵۲)، ۲۲۵-۲۵۴. <http://doi.org/10.22066/cilamag.2015.15764>
- کارگری، نوروز (۱۳۹۱). درون‌مایه‌های تروریسم. تهران: نشر میزان.
- کدخدایی، عباسعلی و فامیل زوار جلالی، امیر (۱۴۰۲). ارزیابی پایبندی دولت‌ها به توصیه‌های گروه ویژه اقدام مالی در مبارزه با تأمین مالی تروریسم. فصل‌نامه مطالعات حقوق عمومی دانشگاه تهران، زودآیند. <http://doi.org/10.22059/jplsq.2021.322979.2765>
- کدخدایی، عباسعلی و نوروزپور، حسام (۱۳۹۹). چالش‌های ارزشهای مجازی در مبارزه با پولشویی و تأمین مالی تروریسم با تأکید بر اقدامات و توصیه‌های کارگروه ویژه اقدام مالی. مجله حقوقی بین‌المللی، ۳۷(۶۲)، ۷-۲۹. <http://doi.org/10.22066/cilamag.2019.101998.1647>
- کوهن، برنارد سائول (۱۳۸۷). ژئوپولیتیک نظام جهانی. ترجمه عباس کاردان. تهران: ابرار معاصر.
- ماتسورا، جفری اچ. (۱۳۹۷). بررسی اجمالی مقررات ارز دیجیتال و پیامدهای قانونی آن. ترجمه سعید سیاه‌بیدی کرمانشاهی و حمیدرضا کناری‌زاده. پژوهشنامه حقوق فارس، ۱(۱)، ۱۴۹-۱۶۷.
- ناجیراد، محمدعلی (۱۳۸۷). جهانی‌شدن تروریسم. تهران: مرکز چاپ و انتشارات وزات امور خارجه.
- هراری، یووال نوح (۱۳۹۸). پول. ترجمه مهدی نمازیان. تهران: نشر نون.
- الهی‌نظری، حمید و فامیل زوار جلالی، امیر (۱۳۹۶). مسئولیت بین‌المللی دولت‌های تأمین‌کننده مالی تروریسم. فصل‌نامه مطالعات حقوق عمومی دانشگاه تهران، ۴۷(۳)، ۷۲۵-۷۴۶. <https://doi.org/10.22059/jplsq.2017.207526.1262>
- Acharya, A. (2009). *Targeting Terrorist Financing: international cooperation and new regimes*. Routledge.
- Ashok, I. (2016). The anatomy of a "Cyber Jihad" – analysing the future and evolution of terrorism in cyberspace, International Business Times, 20 June 2016, <https://www.ibtimes.co.uk/anatomy-cyber-jihad-analysing-evolution-future-terrorism-cyberspace-1566184>.
- CFT, United Nations, General Assembly, 1999, <https://treaties.un.org/doc/db/terrorism/english-18-11.pdf>



- Dalyan, S. (2008). Combating the financing of terrorism: rethinking strategies for success. *Defence Against Terrorism Review*, 1(1), 137-153.
- Ellis, C., Pantucci, R., Zuijdewijn, J., Bakker, E., Gomis, B., Palombi, S., & Smith, M. (2016). *Countering Lone Actor Terrorism Series No. 11: Lone Actor Terrorism, Final Report*, Royal United Services Institute, London, April 2016. [https://rusi.org/sites/default/files/201604\\_clat\\_final\\_report.pdf](https://rusi.org/sites/default/files/201604_clat_final_report.pdf)
- European Parliamentary Research Service (2015). 'Understanding Definitions of Terrorism,' November 2015, [http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/571320/EPRS\\_ATA\(2015\)571320\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/571320/EPRS_ATA(2015)571320_EN.pdf)
- Europol (2017). *EU Terrorism Situation and Trend Report (TE-SAT)*, The Hague. <https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017>.
- Fanusie, Y. (2017). Terrorist Networks Eye Bitcoin as Cryptocurrency's Price Rises, *The Cipher Brief*, 21 December 2017. <https://www.thecipherbrief.com/terrorist-networks-eye-bitcoin-cryptocurrencys-price-rises>, (last visited on: 10/06/2022).
- Financial Action Task Force (2014). *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, Financial Action Task Force (2018). *Financing of Terrorism for Recruitment Purposes*, FATF Report, January 2018, retrieved from: <http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>. (visited:10/10/2018).
- Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798-1853.
- Gates, M. (2017). *Block Chain, CreateSpace Independent Publishing Platform*. Volume 1 of Ultimate Cryptocurrency. CreateSpace Independent Publishing Platform.
- Goldman, Z. K., Maruyama, E., Rosenberg, E., Saravalle, E., & Solomon-Strauss, J. (2017). Terrorist use of virtual currencies. *Washington DC: Center for a New American Security, May 3*. Center for a New American Security.
- Higgins, S. (2014). ISIS-Linked blog: bitcoin can fund terrorist movements worldwide, *Coin Desk*. Web, <https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/>.
- Johnson, T. (2016). Computer hack helped feed an Islamic State death list. *McClatchy DC Bureau*, 20. <http://www.mcclatchydc.com/news/nation-world/national/article90782637.html>.
- Jongman, A. J., & Schmid, A. P. (2005), *Political terrorism, Frequency of Definitional Elements in 109 Definitions of Terrorism*, New Jersey: Transaction Publishers.

- Nimmo, K. (2014). Bitcoin dismissed as a currency for terrorists and drug dealers. Infowars, Web. 1 Dec 2014, <https://www.infowars.com/results/?query=Bitcoin%20dismissed%20as%20a%20currency%20for%20terrorists>.
- Ponsford, M. P. (2015). A comparative analysis of Bitcoin and other decentralised virtual currencies: legal regulation in the People's Republic of China, Canada, and the United States. *HKJ Legal Stud.*, 9, 29.
- Prisco, G. (2014). Bitcoin will be displaced by cryptocurrencies with superior features – Crypto Coins News, Cato Institute. Web. 20 Nov. <https://www.cato.org/search?query=Bitcoin+will+be+displaced+by+cryptocurrencies>
- Singletary, T. (2015). Dark web and the rise of underground networks. In *Evolution of Cyber Technologies and Operations to 2035* (pp. 107-126). Cham: Springer International Publishing.
- Song, Y., Chen, B., & Wang, X. Y. (2023). Cryptocurrency technology revolution: are Bitcoin prices and terrorist attacks related? *Financial innovation*, 9(1), 1-20. <https://doi.org/10.1186/s40854-022-00445-3>
- US Defense Dept. (2022), *Analyzing Bitcoin as Potential Terrorism Threat*, RT USA. RT USA. Web. 1 Dec 2014, <https://www.rt.com/usa/157552-defense-pentagon-bitcoin-terrorism/>, (last visited on : 20/09/2022)
- Wang, S., & Zhu, X. (2021). Evaluation of potential cryptocurrency development ability in terrorist financing. *Policing: A Journal of Policy and Practice*, 15(4), 2329-2340.