

Legal Framework and International Efforts in Combating Digital Currency Crimes: An International Instruments Approach

**Mohadeseh
Ghavamipour Sereshkeh**

PhD Student in Criminal Law and Criminology,
Lahijan Branch, Islamic Azad University,
Lahijan, Iran (Corresponding author)
Email: mohadesehghavamipour@gmail.com

Amirreza Mahmoudi

Assistant Professor, Department of Law, Lahijan
Branch, Islamic Azad University, Lahijan, Iran
Email: amirreza.mahmodi@gmail.com



Abstract

With the proliferation of cryptocurrencies, new opportunities have emerged for committing financial crimes, including money laundering, terrorist financing, and other illegal activities. The unique features of these currencies—such as anonymity, decentralization, and transnationality—have posed significant challenges to traditional legal and regulatory systems. This article provides a comprehensive review of legal frameworks and international efforts to address these crimes, emphasizing the pivotal role of international documents such as the United Nations Convention against Transnational Organized Crime (Merida Convention), Financial Action Task Force (FATF) standards, and Group of 20 (G20) recommendations in regulating and mitigating the risks associated with digital currencies.

Journal of Research and
Development in Criminal Law and
Criminology

Iranian Law and Legal Research
Institute

Vol. 1 | No. 1 | Spring and
Summer 2024
(Original Article)

www.jclc.illrc.ac.ir

DOI:

[10.22034/jclc.2024.718662](https://doi.org/10.22034/jclc.2024.718662)

The present research employs a descriptive-analytical method to evaluate these frameworks and demonstrates that the Merida Convention, by establishing legal foundations to combat organized crimes and criminalizing money laundering, alongside the FATF, by developing specific standards and guidelines for preventing money laundering and terrorist financing, and the G20, by promoting regulatory recommendations and risk management related to digital currencies, have collectively contributed to fostering international coordination and cooperation in combating these crimes.

The findings of this research indicate that, in order to effectively address emerging crimes related to digital currencies, it is essential to utilize existing frameworks while also fostering transnational cooperation and continuously updating laws and regulations. This article underscores the necessity of developing regulatory and legal frameworks at the global level, strengthening international cooperation, and enhancing supervisory capabilities through the application of new technologies such as artificial intelligence and data analysis to combat digital currency crimes.

Keywords: *Crime, Digital Currency, International Instruments, Merida Convention, G20, Financial Action Task Force (FATF).*



چارچوب حقوقی و تلاش‌های بین‌المللی در مبارزه با جرایم ارزهای دیجیتال: رویکرد اسناد بین‌المللی

دانشجوی دکتری حقوق کیفری و جرم‌شناسی، واحد لاهیجان،
دانشگاه آزاد اسلامی، لاهیجان، ایران (نویسنده مسئول)
Email: mohadesehghavamipour@gmail.com

محدثه قوامی پور سرشکه

استادیار گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان،
ایران
Email: amirreza.mahmodi@gmail.com

امیررضا محمودی



دوفصلنامه تحقیق و توسعه در حقوق کیفری و
جرم‌شناسی

پژوهشکده حقوق و قانون ایران

دوره ۱ | شماره ۱ | بهار و تابستان ۱۴۰۳
(مقاله پژوهشی)

www.jclc.illrc.ac.ir

DOI:

[10.22034/jclc.2024.718662](https://doi.org/10.22034/jclc.2024.718662)

چکیده

با گسترش ارزهای دیجیتال و رمزنگاری شده، فرصت‌های جدیدی برای ارتکاب جرائم مالی از جمله پولشویی، تأمین مالی تروریسم، و سایر فعالیت‌های غیرقانونی پدید آمده است. ویژگی‌های منحصر به فرد این ارزها مانند ناشناس بودن، غیرمتمرکز بودن و فراملیتی بودن، چالش‌های جدی را برای سیستم‌های حقوقی و نظارتی سنتی به همراه داشته‌اند. این مقاله به بررسی جامع چارچوب‌های حقوقی و تلاش‌های بین‌المللی برای مقابله با این جرائم می‌پردازد و بر نقش کلیدی اسناد بین‌المللی همچون کنوانسیون سازمان ملل متحد علیه جرائم سازمان‌یافته فراملی (کنوانسیون مریدا)، استانداردهای گروه ویژه اقدام مالی (FATF)، و توصیه‌های گروه بیست (G20) در تنظیم‌گری و کاهش ریسک‌های مرتبط با ارزهای دیجیتال تأکید دارد.

پژوهش حاضر با استفاده از روش توصیفی-تحلیلی به ارزیابی دقیق این چارچوب‌ها پرداخته و نشان می‌دهد که کنوانسیون مریدا با ایجاد مبانی حقوقی برای مبارزه با جرائم سازمان‌یافته و جرم‌انگاری

پولشویی، گروه FATF با تدوین استانداردها و دستورالعمل‌های مشخص در زمینه پیشگیری از پولشویی و تأمین مالی تروریسم، و گروه G20 با ترویج توصیه‌های نظارتی و مدیریت ریسک‌های مرتبط با ارزهای دیجیتال، به ایجاد هماهنگی و همکاری بین‌المللی در مبارزه با این جرائم کمک کرده‌اند. یافته‌های این پژوهش حاکی از آن است که برای مقابله مؤثر با جرائم نوظهور مرتبط با ارزهای دیجیتال، علاوه بر بهره‌گیری از چارچوب‌های موجود، نیازمند همکاری‌های فراملیتی و به‌روزرسانی مستمر قوانین و مقررات هستیم. این مقاله بر ضرورت توسعه چارچوب‌های نظارتی و قانونی در سطح جهانی، تقویت همکاری‌های بین‌المللی، و همچنین ارتقای توانایی‌های نظارتی از طریق به‌کارگیری فناوری‌های نوین مانند هوش مصنوعی و تحلیل داده‌ها برای مقابله با جرائم ارزهای دیجیتال تأکید می‌کند.

کلیدواژه‌ها: جرائم مالی، ارزهای دیجیتال، اسناد بین‌المللی، کنوانسیون مریدا، گروه بیست (G20)، گروه ویژه اقدام مالی (FATF).

مقدمه:

در دنیای امروز که فناوری‌های نوین ارتباطی و اطلاعاتی نقش محوری در زندگی بشر ایفا می‌کنند، ارزش‌های دیجیتال و رمزنگاری شده به عنوان یکی از پدیده‌های جدید و تاثیرگذار در عرصه مالی و پرداخت‌ها مطرح شده‌اند. این ارزش‌های مجازی که بر پایه فناوری بلاکچین استوارند، با ویژگی‌هایی همچون عدم تمرکز، ناشناس بودن و رمزگیزی، ابعاد تازه‌ای را در تعاملات اقتصادی و مالی گشوده‌اند. علی‌رغم مزایای متعدد ارزش‌های دیجیتال، ماهیت فراسرمینی و غیرمتمرکز آنها می‌تواند زمینه‌ساز سوءاستفاده‌های گسترده از جمله پولشویی، تامین مالی تروریسم و سایر جرائم اقتصادی شود. نبود مرزهای سنتی در این عرصه، مقابله با چنین جرائمی را برای نظام‌های حقوقی و قضایی ملی با دشواری‌های فراوانی مواجه ساخته است. از این رو، ضرورت تدوین چارچوب‌های حقوقی بین‌المللی و هماهنگ‌سازی تلاش کشورها در این زمینه بیش از پیش احساس می‌شود.

در این راستا، کنوانسیون سازمان ملل متحد علیه جرائم سازمان یافته فراملی موسوم به کنوانسیون مریدا، به عنوان یکی از مهمترین اسناد حقوقی بین‌المللی در این حوزه شناخته می‌شود. این کنوانسیون ضمن ارائه تعاریف و الزامات قانونی، اصول و راهکارهایی را برای مبارزه با جرائم سازمان یافته فراملی از جمله پولشویی ارائه می‌دهد. در همین چارچوب، گروه ویژه اقدام مالی (FATF) نیز با تدوین استانداردها و توصیه‌هایی برای پیشگیری و مقابله با پولشویی و تامین مالی تروریسم، مکمل مناسبی برای اجرای کنوانسیون مریدا محسوب می‌شود. علاوه بر این، نهادهای بین‌المللی مانند گروه ۲۰ (G20) نیز توصیه‌هایی را در زمینه تنظیم‌گری و مدیریت ریسک‌های مربوط به حوزه رمزارزها ارائه داده‌اند. مقاله حاضر در صدد است تا با بررسی نقش و کارکرد این سه چارچوب حقوقی و بین‌المللی، راهکارها و الزامات مبارزه با جرائم ارزش‌های دیجیتال را مورد تحلیل قرار دهد.

۱. مفهوم ارز دیجیتال و جرائم آن

ارزهای دیجیتال یا رمزنگاری شده، دارایی‌های مجازی هستند که بر پایه فناوری رمزنگاری و زنجیره بلوکی (بلاکچین) بنا شده‌اند. برخلاف پول‌های سنتی و ارزهای قانونی که توسط بانک‌های مرکزی کنترل و منتشر می‌شوند، رمزارزها فاقد پشتوانه فیزیکی بوده و به صورت کاملاً غیرمتمرکز عمل می‌کنند. (Frankenfield, 2021: 1) این بدان معناست که انتشار، اعتبارسنجی و پردازش تراکنش‌های مرتبط با آنها به جای یک نهاد متمرکز، توسط شبکه‌ای گسترده و توزیع شده از کاربران و رایانه‌هایی در سراسر جهان انجام می‌شود (Chohan, 2021: 5-7).

یکی از مزایای اصلی رمزارزها، استفاده از رمزنگاری پیچیده و پیشرفته برای حفظ امنیت و جلوگیری از جعل است. همچنین ساختار منحصربفرد زنجیره بلوکی که پایه و اساس رمزارزها را تشکیل می‌دهد، باعث شده تا تراکنش‌های انجام شده در این شبکه‌ها غیرقابل تغییر، شفاف و دائمی باشند (Tasca, 2022: 111-112) به عبارت دیگر، هیچ نهاد یا فردی قادر به دستکاری یا حذف رکوردهای درج شده در زنجیره بلوکی نیست.

از ویژگی‌های جذاب دیگر رمزارزها، امکان انتقال سریع و کم‌هزینه آنها در سراسر جهان است. در حالی که انتقال پول‌های سنتی از طریق کانال‌های بانکی می‌تواند پرهزینه و زمان‌بر باشد، تراکنش‌های رمزارزی می‌توانند در عرض چند دقیقه و با هزینه‌های ناچیز در هر نقطه‌ای از جهان انجام شوند (Frankenfield, 2021: 3). (این امر، استفاده از رمزارزها را برای پرداخت‌های بین‌المللی و خریدهای آنلاین بسیار جذاب کرده است.

بیت‌کوین^۱ که در سال ۲۰۰۹ توسط فردی با نام مستعار ساتوشی ناکاموتو منتشر شد، نخستین و شناخته شده‌ترین رمزارز جهان است. اما امروزه حدود ۱۰ هزار رمزارز دیگر نیز وجود دارند که از فناوری مشابهی بهره می‌برند و برای اهداف گوناگونی مانند

1. Bitcoin

سرمایه‌گذاری، انجام پرداخت‌ها و اعتبارسنجی کاربرد دارند. (Vigna, 2022: 44) از جمله رمزارزهای معروف دیگر می‌توان به اتریوم، لایت‌کوین، ریپل، بیت‌کوین کش و تتر اشاره کرد.

گسترش سریع رمزارزها در یک دهه اخیر، ناشی از مزایا و ویژگی‌های منحصر به فرد آنها مانند غیرمتمرکز بودن، امنیت بالا و سرعت انتقال است. با این حال، این پدیده نوظهور با چالش‌ها و مسائل مختلفی نیز روبه‌رو است که از جمله می‌توان به فقدان تنظیم‌گری و نظارت قانونی کافی، حسابداری و مالیات‌ستانی پیچیده، کاربردهای غیرقانونی آن در پولشویی و خرید ارقام غیرمجاز، و مصرف انرژی بالا و مشکلات زیست‌محیطی ناشی از آن اشاره کرد (Chohan, 2021:16-17) این مسائل ضرورت تدوین چارچوب‌های حقوقی و نظارتی جامع را آشکار می‌سازد.

ارزهای دیجیتال دارای ویژگی بارز برگشت‌ناپذیری تراکنش‌ها هستند. این بدان معناست که پس از انجام یک تراکنش، حتی در صورت بروز خطا یا اشتباه، امکان بازگشت، برگرداندن یا لغو آن وجود ندارد. هیچ نهاد یا مرجع مرکزی نیز قادر به کنترل یا لغو تراکنش‌ها نیست. برای تأیید و ثبت هر تراکنش، ماینرها (افراد یا رایانه‌هایی که در فرآیند تأیید تراکنش‌ها و ایجاد بلاک‌های جدید در شبکه بلاکچین مشارکت دارند) تراکنش‌ها را در یک بلاک ثبت می‌کنند. این بلاک‌ها به صورت مستمر به زنجیره بلاک‌های قبلی اضافه می‌شوند و تاریخچه تمامی تراکنش‌ها در آنها ذخیره می‌گردد. پس از ثبت نهایی، تراکنش‌ها از لحاظ فنی غیرقابل تغییر یا حذف خواهند بود. همچنین، ارزهای دیجیتال بدون دخالت یا نظارت سازمان‌ها یا دولت‌ها فعالیت می‌کنند. این به معنای عدم وابستگی به نهادهای مالی متمرکز است و تراکنش‌ها در شبکه بلاکچین به صورت غیرمتمرکز انجام می‌شوند. نامشخص بودن هویت دقیق طرفین تراکنش نیز از دیگر ویژگی‌های ارزهای رمزنگاری شده است که می‌تواند حریم خصوصی کاربران را تضمین کند.

این ویژگی‌ها ارزشهای دیجیتال را به یک سیستم امن و قابل اعتماد برای انجام تراکنش‌های مالی تبدیل کرده است. اما از آنجا که تراکنش‌ها غیرقابل بازگشت هستند، کاربران باید با دقت و احتیاط بیشتری عمل کنند تا از بروز خطاها جلوگیری شود. (ریاضی مند، ۱۳۹۷: ۶۱)

با این حال، همین ویژگی‌ها می‌توانند ارزشهای دیجیتال را به بستری برای ارتکاب جرائم مالی مانند پولشویی تبدیل کنند. پولشویی فرایندی است که در آن، منشأ غیرقانونی اموال و پول‌ها پنهان می‌شود و اغلب به صورت سازمان‌یافته انجام می‌گیرد. مقابله با پولشویی همواره در دستور کار قانون‌گذاران و نهادهای مربوط به پیشگیری از جرائم مالی قرار دارد. (رهبر، ۱۳۸۲: ۴۲)

ارزشهای دیجیتال به دلیل ویژگی‌های منحصر به فردی مانند برگشت‌ناپذیری تراکنش‌ها و عدم افشای هویت طرفین معامله، می‌توانند بستر مناسبی برای فعالیت‌های پولشویی باشند. در ارزشهای دیجیتال، هویت افراد درگیر در تراکنش‌ها به صورت ناشناس و نامشخص است که این امر فرصت مناسبی برای انجام فعالیت‌های غیرقانونی مانند پولشویی فراهم می‌کند. علاوه بر این، برگشت‌ناپذیری تراکنش‌های ارزشهای دیجیتال نیز یکی دیگر از عواملی است که می‌تواند باعث سوءاستفاده از این فناوری برای پولشویی شود. زیرا امکان برگشت یا لغو تراکنش‌های انجام شده وجود ندارد و این موضوع، فرصت‌های بیشتری برای پنهان‌کاری و انتقال وجوه غیرقانونی فراهم می‌کند.

یکی دیگر از چالش‌های مهم در زمینه پولشویی با ارزشهای دیجیتال، فقدان نظارت و مقررات گذاری کافی در برخی کشورهاست. نبود یک نهاد مرکزی ناظر و قوانین و مقررات مشخص، نظارت بر فعالیت‌های پولشویی در حوزه ارزشهای دیجیتال را دشوار می‌سازد. با این حال، تلاش‌های زیادی در سطح ملی و بین‌المللی برای توسعه و اجرای قوانین و مقررات جلوگیری از پولشویی در ارزشهای دیجیتال صورت گرفته است. یکی از راهکارهای

اصلی در این زمینه، توسعه و اجرای قوانین و مقررات مناسب در سطح ملی و بین‌المللی است. این قوانین و مقررات باید به گونه‌ای طراحی شوند که امکان شناسایی و پیگیری فعالیت‌های پولشویی در ارزهای دیجیتال را فراهم کنند.

همچنین، همکاری میان نهادهای قانونی، نظارتی و اجرایی در سطح ملی و بین‌المللی برای تبادل اطلاعات و هماهنگی اقدامات ضروری است. این همکاری‌ها می‌تواند به شناسایی بهتر و پیشگیری موثرتر از فعالیت‌های پولشویی در ارزهای دیجیتال کمک کند. علاوه بر این، به‌کارگیری فناوری‌های پیشرفته مانند هوش مصنوعی و یادگیری ماشین می‌تواند در شناسایی و پیشگیری از فعالیت‌های پولشویی در ارزهای دیجیتال کمک شایانی کند. این فناوری‌ها قادر به تحلیل حجم عظیمی از داده‌ها و شناسایی الگوهای مشکوک هستند که می‌تواند در کشف فعالیت‌های پولشویی بسیار موثر باشد.

در نهایت، آموزش و آگاهی‌بخشی به کاربران، فعالان و سرمایه‌گذاران در حوزه ارزهای دیجیتال در خصوص خطرات پولشویی و راهکارهای پیشگیری از آن، می‌تواند نقش مهمی در مبارزه با این پدیده ایفا کند. افزایش آگاهی در این زمینه می‌تواند باعث افزایش هوشیاری و احتیاط بیشتر در معاملات ارزهای دیجیتال شود و در نتیجه، امکان سوءاستفاده از این فناوری برای فعالیت‌های غیرقانونی را کاهش دهد.

در مجموع، با وجود چالش‌های موجود در زمینه پولشویی با استفاده از ارزهای دیجیتال، راهکارهای متعددی برای مقابله با این پدیده وجود دارد که نیازمند تلاش‌های جهانی و هماهنگی در سطوح مختلف است. (بهره‌مند، عامری ثانی، ۱۳۹۸: ۵۹)

تامین مالی تروریسم به معنای جمع‌آوری، فراهم کردن یا انتقال وجوه با قصد استفاده آن برای انجام اعمال تروریستی یا حمایت از گروه‌های تروریستی است (Crimm & Majoor, 2019: 365) این جرم شامل «هرگونه رفتار که در آن فردی عمداً وجوه را جمع‌آوری یا فراهم می‌کند، با قصد استفاده از آنها برای ارتکاب یک عمل تروریستی» می‌شود

همچنین گزارش دفتر مبارزه با تروریسم وزارت خارجه آمریکا، تامین مالی تروریسم را «جمع‌آوری، ارائه یا انتقال وجوه برای حمایت از فعالیت‌های تروریستی» تعریف می‌کند. (U.S. Department of State, 2019) این جرم در سطح بین‌المللی، یک تهدید جدی محسوب می‌شود و نیازمند اقدامات قانونی و همکاری‌های فراگیر برای مقابله با آن است. گروه‌های تروریستی می‌توانند از ویژگی‌های منحصربه‌فرد ارزهای دیجیتال مانند ناشناس بودن، سرعت بالای انتقال وجوه و عدم نظارت کافی، برای تامین مالی فعالیت‌های خود به شیوه‌های مختلفی سوءاستفاده کنند. آنها قادرند «از انونیمیت و امکان انتقال سریع پول در ارزهای دیجیتال سوءاستفاده کنند تا فعالیت‌های تروریستی خود را تامین مالی کنند (FATF, 2022) بسیاری از ارزهای دیجیتال به دلیل ماهیت غیرمتمرکز خود، خارج از نظارت نهادهای مالی سنتی مانند بانک‌ها عمل می‌کنند و "عدم مقررات گذاری و نظارت کافی بر ارزهای دیجیتال، می‌تواند فرصت‌هایی برای تامین مالی تروریسم فراهم کند (Shalhoub & Qudsi, 2021: 47) از این‌رو، اهمیت جلوگیری از سوءاستفاده گروه‌های تروریستی از ارزهای دیجیتال برای تامین مالی فعالیت‌های خود، یک ضرورت جدی در سطح بین‌المللی محسوب می‌شود که نیازمند اقدامات قانونی، همکاری‌های فراگیر و تدوین مقررات نظارتی مناسب است.

ارزهای دیجیتال علاوه بر پولشویی و تامین مالی تروریسم، می‌توانند در ارتباط با جرائم دیگری نیز مورد سوءاستفاده قرار گیرند که نیازمند توجه و کنترل‌های بین‌المللی است. از جمله این جرائم می‌توان به موارد زیر اشاره کرد:

گروه‌های جنایتکار می‌توانند از ارزهای دیجیتال برای انتقال پول لازم جهت قاچاق کالا یا انسان استفاده کنند. «ویژگی‌های امنیتی بالای ارزهای دیجیتال، آنها را برای تراکنش‌های مرتبط با قاچاق، جذاب می‌کند» (UNODC, 2022) مجرمان می‌توانند در حوادث آدم‌ربایی و باج‌گیری، باج خواسته شده را از طریق ارزهای دیجیتال دریافت کنند

تا ردیابی آن‌ها را دشوارتر کند. (Europol, 2021) بازارهای زیرزمینی آنلاین اغلب از ارزشهای دیجیتال برای فروش غیرقانونی کالاها و خدمات مانند مواد مخدر، اسلحه و محتوای غیراخلاقی استفاده می‌کنند. (Chainalysis, 2022) همچنین، مجرمان سایبری می‌توانند از ارزشهای دیجیتال برای دریافت وجوه حاصل از جعل هویت، فیشینگ و سایر کلاهبرداری‌های آنلاین استفاده کنند. (Tiwari, 2020)

ارزهای دیجیتال به دلیل ماهیت فراملیتی و عدم وابستگی به مرزهای جغرافیایی، فرصت‌های جدیدی را برای فعالیت‌های مجرمانه فراهم می‌کنند که نیازمند همکاری بین‌المللی و ایجاد چارچوب‌های قانونی و نظارتی مشترک است. به طور مشخص:

۱. ماهیت فراملیتی: ارزهای دیجیتال می‌توانند به راحتی در سراسر مرزهای ملی منتقل شوند، که این امر تحقیقات پلیسی و قضایی را در یک کشور دشوار می‌کند. جرائم مرتبط با ارزهای دیجیتال اغلب بعد بین‌المللی دارند و نیازمند همکاری بین‌المللی هستند.

۲. نبود نظارت واحد: در حال حاضر، قوانین و مقررات ارزهای دیجیتال در کشورهای مختلف متفاوت است. این موضوع منجر به وجود حفره‌های قانونی و فضاهای نظارتی می‌شود که مجرمان می‌توانند از آن سوءاستفاده کنند.

۳. نیاز به همکاری و هماهنگی: برای مقابله موثر با جرائم مرتبط با ارزهای دیجیتال، نیاز به همکاری بین‌المللی در زمینه‌های تبادل اطلاعات، هماهنگی تحقیقات، استرداد مجرمان و توقیف دارایی‌ها وجود دارد.

۴. چارچوب‌های قانونی و نظارتی مشترک: ایجاد استانداردها و چارچوب‌های قانونی و نظارتی مشترک در سطح بین‌المللی می‌تواند به هماهنگی بهتر و پرکردن خلأهای قانونی کمک کند.

بنابراین، به دلیل ماهیت فراگیر و فراملیتی ارزهای دیجیتال، مبارزه موثر با جرائم مرتبط با آن‌ها نیازمند همکاری‌های بین‌المللی و ایجاد چارچوب‌های قانونی و نظارتی مشترک در سطح جهانی است.

۲. کنوانسیون مریدا

کنوانسیون مریدا از بدایع سازمان ملل متحد است که در ۲۹ سپتامبر ۲۰۰۳ در شهر مریدای مکزیک به تصویب مجمع عمومی سازمان ملل متحد رسید این کنوانسیون با مطرح کردن عنوان فساد در سطح بین‌الملل و ایجاد چهارچوبی ضد فساد به‌عنوان نخستین سند ضد فساد در جوامع بین‌المللی شناخته می‌شود که دارای ضمانت اجرا نیز هست. در حقیقت این کنوانسیون مبانی اخلاق تجاری را در سندی بین‌المللی اعلام کرده و مقامات دولتی را بر رعایت اخلاق حرفه‌ای ملزم می‌کند و دربندهای این قانون به مواردی از جمله مبارزه با فساد به‌وسیله‌ی ترغیب و تشویق کارمندان دولتی به صداقت، پیش‌بینی کدهای اخلاق در شرکت‌ها و سازمان‌ها، تنظیم راهکارهایی برای گزارش دهی کارمندان هنگام مشاهده فساد، تعیین ضمانت اجرا توسط دولت برای عدم اجرای مجموعه نظام رفتاری شده است.

همچنین در ماده ۱۲ با گسترش حیطة‌ی شمول، رعایت اصول اخلاقی درست‌والعمل علیه فساد شرکت‌های خصوصی را نیز مشمول ساخته.

در سال ۱۳۸۲ جمهوری اسلامی ایران به کنوانسیون مریدا پیوست. و در سال ۱۳۸۵ در مجلس شورای اسلامی ایران کنوانسیون مبارزه با فساد تصویب شد و در سال ۱۳۸۷ به تائید مجمع تشخیص مصلحت نظام رسید و در انتها در فرودین ماه سال ۱۳۸۸ جمهوری اسلامی ایران رسماً به عضویت کنوانسیون مریدا درآمد.

در اسفندماه سال ۱۳۸۸ هیئت وزیران با تعیین وزارت دادگستری به عنوان مرجع ملی کنوانسیون، برای مقابله فساد در کشور، اجرایی کردن مفاد کنوانسیون، و ضمانت حسن اجرای تعهداتی که جمهوری اسلامی ایران با پیوستن به کنوانسیون بر عهده دارد قدمی برداشت. و در جهت اعمال هماهنگی میان دستگاه اجرایی و قضایی برای اجرای تعهداتی که کشور مسئول آن است با شکل‌گیری شورای به نام کارگروه تخصصی مرجع ملی

کنوانسیون مبارزه با فساد در وزارت دادگستری با شرکت نمایندگانی از سازمان‌هایی مانند سازمان بازرسی کل کشور، دیوان محاسبات، ستاد مبارزه با مفاسد اقتصادی، نیروی انتظامی و... اقدامات خود را تکمیل نمود. (قوامی پور سرشکه، محمودی، ۱۴۰۲: ۸۶)

کنوانسیون مریدا ضمن ارائه تعاریف جامع از جرایم سازمان یافته، خط‌مشی‌ها، اقدامات پیشگیرانه، مقررات برای همکاری بین‌المللی و استرداد مجرمین را پیش‌بینی می‌کند. یکی از مهمترین موارد پوشش داده شده در این کنوانسیون، جرم پولشویی است که ارتباط نزدیکی با حوزه ارزهای دیجیتال دارد. بر اساس ماده ۶ کنوانسیون، تمامی کشورهای عضو موظف هستند پولشویی از طریق واسطه‌های مالی و سایر موسسات را جرم‌انگاری کنند (UNODC, 2004: 8). همچنین ماده ۷ کنوانسیون راهکارهایی برای مبارزه با پولشویی از جمله خشکاندن منابع مالی گروه‌های جنایتکار را ارائه می‌دهد. (UNODC, 2004: 10)

با توجه به اینکه ارزهای دیجیتال به دلیل ماهیت غیرمتمرکز و ناشناس خود، می‌توانند ابزاری برای پولشویی و فعالیت‌های مالی غیرقانونی باشند، الزامات و راهکارهای کنوانسیون مریدا در این زمینه اهمیت ویژه‌ای می‌یابد. کشورهای عضو این کنوانسیون باید تدابیر لازم را برای شناسایی، ردگیری و توقیف دارایی‌های حاصل از جرم اتخاذ کنند که شامل رمزارزها نیز می‌شود (FATF, 2022: 63)

کنوانسیون مریدا به طور مستقیم به ارزهای دیجیتال نپرداخته است، زیرا این کنوانسیون در سال ۲۰۰۳ به تصویب رسید، یعنی قبل از ظهور ارزهای دیجیتال مانند بیت‌کوین در سال ۲۰۰۹. با این حال، اصول و الزامات کلی کنوانسیون مریدا در زمینه مبارزه با پولشویی و تبادل اطلاعات می‌تواند به کنترل پولشویی با استفاده از ارزهای دیجیتال نیز کمک کند:

۱. الزام کشورها به جرم‌انگاری پولشویی عواید ناشی از فعالیت‌های مجرمانه به طور کلی، می‌تواند شامل پولشویی از طریق ارزهای دیجیتال نیز بشود.
۲. تأکید بر شفافیت مالی و الزام کشورها برای شناسایی مالکان واقعی دارایی‌ها، می‌تواند به شناسایی افراد درگیر در پولشویی با ارزهای دیجیتال کمک کند.

۳. همکاری بین‌المللی در تبادل اطلاعات و تحقیقات مشترک که در کنوانسیون پیش‌بینی شده، برای مقابله با پولشویی با استفاده از ارزش‌های دیجیتال که ماهیتی فراملیتی دارند، ضروری است.

۴. الزامات مربوط به نظارت مالی و استانداردهای حسابداری می‌تواند شامل نظارت بر تراکنش‌های ارزش‌های دیجیتال نیز بشود.

با این حال، به دلیل ماهیت نوظهور و ویژگی‌های منحصر به فرد ارزش‌های دیجیتال، نیاز به قوانین، مقررات و چارچوب‌های نظارتی جدید برای کنترل پولشویی با این ابزارها نیز ضروری است که می‌تواند براساس اصول کنوانسیون مریدا تدوین شود.

۳. گروه ۲۰

با آغاز دهه ۹۰ میلادی و اتمام جنگ سرد تحولات جدیدی در ساختارهای بین‌المللی شکل گرفت، که موجب رونق اقتصاد جهانی و افزایش همکاری‌های بین‌المللی شد از این تحولات می‌توان به تشکیل سازمان تجارت جهانی و همچنین پس از تشکیل گروه ۷ و ۸ که شامل همین تعداد کشورهای برتر صنعتی می‌شدند گروهی تحت عنوان G20 که دارای ۸۰ درصد ثروت جهان بودند اشاره کرد در واقع نشست مشترک اقتصادهای برتر جهان از اواخر دهه ۹۰ میلادی به شکل گروه ۲۰ تکامل یافت.

سعی و هدف این نهاد و فعالیت آن در راستای هدایت روندهای تأثیرگذار بر مناسبات اقتصادی جهان است. گروه ۲۰ مقامات اقتصادی و سران کشورهای صنعتی را در نشست‌های سالانه که در کشورهای عضو برگزار می‌گردد گرد هم می‌آورد تا تحت این عنوان به اتفاق نظری راجع به موضوعات مهم اقتصاد جهانی و بازار پول و سرمایه برسند.

از محورهای اعلام‌شده در دستور کار گروه ۲۰ می‌توان به‌طور خلاصه به مواردی همچون:

۱. به‌روزرسانی مؤسسات بین‌المللی برای انعکاس واقعیت‌های اقتصاد جهانی

۲. ایجاد یک نظام باز اقتصادی در جهان

۳. ایجاد چهارچوبی برای رشد پایدار و متوازن سرمایه

۴. تحکیم سیستم تنظیم مالی بین‌المللی

نخستین نشست گروه بیست در واشنگتن در سال ۲۰۰۸ تشکیل شد و در پی تشدید دامنه بحران مالی بین‌المللی و حساسیت شرایط اقتصاد جهانی سالانه حداقل یک نشست در سطح سران برگزار می‌شود. لازم به ذکر است علاوه بر اعضای گروه ۲۰ که شامل «آمریکا، انگلیس، فرانسه، آلمان، کانادا، استرالیا، ایتالیا، ژاپن، چین، هند، آرژانتین، برزیل، مکزیک، اندونزی، روسیه، عربستان، آفریقای جنوبی، کره جنوبی، ترکیه و اتحادیه اروپا» نمایندگان سازمان‌های مهم بین‌المللی مانند صندوق بین‌المللی پول، سازمان ملل و بانک جهانی و برخی کشورهای غیر عضو که توسط کشور میزبان نشست دعوت می‌شوند در نشست‌های سالانه‌ی سران حضور دارند.

گروه ۲۰ فاقد کارمند و دبیرخانه است و هر سال یکی از اعضا به ریاست آن انتخاب می‌شود و میزبانی دبیرخانه موقت و برگزاری نشست را بر عهده می‌گیرد. (موسوی، داوری، ۱۳۹۰، ۵۲۴-۵۲۳).

اعضای گروه ۲۰ با در اختیار داشتن بیشتر از ۸۰ درصد تولید ناخالص اسمی جهان و ۸۰ درصد تجارت جهانی و همچنین حدود دوسوم جمعیت جهان تأثیر قابل‌توجهی بر جهت‌گیری‌های اقتصادی دنیا دارد.

به اعتقاد برخی در حوزه‌ی اقتصاد و سیاست، این گروه قابلیت تبدیل شدن به مهم‌ترین نهاد بین‌المللی را دارد.

ایران علی‌رغم وجود ظرفیت‌های عظیم اقتصادی و سرمایه انسانی و به دلیل ملاحظات سیاسی همانند برخی دیگر از کشورهای با ظرفیت اقتصاد جهان از حضور و شرکت مستقیم در این گروه جامانده است.

مقامات گروه ۲۰ بعد از پیدایش ارزش‌های دیجیتال در نشست‌های سالیانه خود نظرات خود

در این راستا را اعلام کرده و همواره موجب ایجاد موجی در نرخ این بازار می‌شوند. در گزارش رسمی شورای ثبات مالی گروه ۲۰ این چنین آمده است: ارزیابی اولیه شورای ثبات مالی این است که ارزشهای رمز پایه در این زمان خطرانی برای ثبات مالی جهان ندارند، با این وجود این بازار همچنان به سرعت در حال رشد و تکامل است و این ارزیابی اولیه با توجه با اینکه ابزارهای رمز پایه به شکل قابل توجهی مورد استفاده قرار می‌گیرند یا با هسته‌ی سیستم مالی تنظیم شده ارتباط برقرار می‌کنند، ممکن است تغییر کند. گروه ۲۰ قوانین سخت‌گیرانه‌ای را در رابطه با رمز ارزها مقرر کرده است که کشورهایی مانند آمریکا و ژاپن به دلیل تقاضای بالای کاربران و پیشرو بودن آنان در این بستر بیشتر تن به اعمال این مقررات می‌دهند. مقامات گروه ۲۰ اعلام کرده‌اند که زمینه‌های قانونی برای پذیرش پرداخته‌ای دیجیتال را ایجاد خواهند کرد.

پیش‌بینی‌ها حاکی از این است که قبل از نشست بعدی گروه ۲۰ در سال جاری این نهاد قوانین و مقررات ناظر بر ارزشهای دیجیتال را ارائه دهد. (موسوی و داوری، ۱۳۹۰، ۵۲۷) گروه ۲۰ (G20) که شامل ۱۹ کشور و اتحادیه اروپا است، در سال‌های اخیر تلاش‌هایی را برای مقابله با جرائم مالی از طریق ارزشهای دیجیتال انجام داده است. برخی از اقدامات این گروه عبارتند از:

۱. تدوین اصول راهنمای سیاست‌گذاری برای ارزشهای دیجیتال: در اجلاس سران گروه ۲۰ در سال ۲۰۲۲ در اندونزی، اصول راهنمایی برای سیاست‌گذاری در زمینه ارزشهای دیجیتال تدوین شد. این اصول شامل تقویت همکاری و هماهنگی بین‌المللی در نظارت و اجرای قانون، مبارزه با جرائم مالی و افزایش شفافیت است. (G20,2022)
۲. همکاری با گروه ویژه اقدام مالی (FATF): گروه ۲۰ از اقدامات FATF برای مقابله با پولشویی و تأمین مالی تروریسم از طریق ارزشهای دیجیتال حمایت کرده است. FATF در سال ۲۰۱۹ راهنمایی‌هایی را برای نظارت بر ارزشهای دیجیتال و مقابله با جرائم مالی مرتبط منتشر کرد (FATF,2019).

۳. تشکیل کارگروه ارزش‌های دیجیتال: در سال ۲۰۲۰، گروه ۲۰ کارگروهی را برای بررسی چالش‌های ارزش‌های دیجیتال و ارائه راهکارهای سیاستی تشکیل داد. این کارگروه بر موضوعاتی مانند مقررات‌گذاری، نظارت و مبارزه با جرائم مالی تمرکز دارد.

۴. انتشار گزارش‌های مرتبط: گروه ۲۰ گزارش‌هایی را در زمینه چالش‌های ارزش‌های دیجیتال، از جمله جرائم مالی مرتبط، منتشر کرده است. از جمله می‌توان به گزارش «مسائل سیاست‌گذاری مرتبط با ارزش‌های دیجیتال» در سال ۲۰۲۲ اشاره کرد. (G20, 2022)

گروه ۲۰ تلاش می‌کند با همکاری سازمان‌های بین‌المللی و تدوین اصول راهنما، چارچوب‌های نظارتی و تبادل اطلاعات، از جرائم مالی مرتبط با ارزش‌های دیجیتال جلوگیری کند.

۴. کارگروه ویژه اقدام مالی

امروز فناوری با سرعت قابل توجهی در حال رشد و پیشرفت است همچنین مجرمین در سطح خرد یا کلان و چه در سطح داخلی و بین‌المللی و علی‌الخصوص گروه‌های تروریستی و تبهکاری هم به این درک رسیده‌اند که با توجه به ضرورت برای پیشبرد اهداف خود باید خود را با پیشرفت فناوری همگام کنند تا روش‌های مجرمانه خویش را در بسترهای تکنولوژی جدید فاقد ارزش نسازند.

با ظهور ارزش‌های مجازی به خصوص ارزی به نام بیت کوین که نشان‌دهنده‌ی فناوری جدیدی به دنیا بود مجرمین این امکان را پیدا کردند تا در چنین بستری که تأیید هویت دارنده ارز در اصل قرارداد ناشناختگی این بستر، ناشناس است تراکنش‌های مالی فراوانی انجام داده و به راحتی به ارتکاب پولشویی و جرائم دیگر در بستر وب عمیق و وب تاریک بپردازند.

بی‌قاعدگی و عدم توافق بر سر مقررات یکسان برای مقابله با این مسئله از دیگر دلایل به وجود آمدن یکی از ابزارهای اصلی تأمین مالی جرائم سازمان‌یافته‌ی فراملی و تروریسم است. این موضوع علاوه بر دولت‌ها توجه نهادها و سازمان‌های بین‌المللی از جمله سازمان

ملل و کارگروه ویژه اقدام مالی را به خود جلب کرده است. (کدخدایی و نوروزپور، ۱۳۹۹، ۸-۹)

گروه ویژه اقدام مالی ارز مجازی را این‌گونه تعریف نموده که: «ارز مجازی جلوه‌ی دیجیتالی یک ارزش است که توسط بانک مرکزی یا مقام صلاحیت‌دار صادر و تضمین نشده، الزاماً به ارز قانونی شناخته‌شده وابسته نبوده و واجد وضعیت حقوقی ارز یا پول نیست. اما به‌عنوان واسطه مبادله که قابلیت انتقال، ذخیره و تجارت در فضای الکترونیکی را دارد، توسط اشخاص حقیقی و حقوقی پذیرفته‌شده باشد.

ارز دیجیتال در بستری غیرمتمرکز و با ساختاری گمنام فعالیت می‌کند ارزش آن وابسته به عرضه و تقاضای کاربران است نه یک امر تعیینی توسط دولت‌ها یا سازمان‌های خاص. (کدخدایی، نوروزپور، ۱۳۹۹، ۱۳)

گروه ویژه اقدام مالی یک سازمان بین‌دولتی می‌باشد یعنی مشتق شده از چند سازمان بین‌المللی و چند کشور مستقل با بهره‌گیری از قوانین عمومی بین‌الملل.

وظیفه این نهاد بین‌المللی، بررسی وضعیت قوانین مبارزه با پول‌شویی در بازارهای مختلف مالی در سطح جهانی است که توسط کشورهای گروه هفت در سال ۱۹۸۹ شروع به فعالیت نمود البته در ادامه راه و به‌خصوص پس از حملات تروریستی ۱۱ سپتامبر آمریکا در سال ۲۰۰۱، حیثه‌ی وظایف این نهاد بزرگ‌تر و شامل نظارت و بررسی نظارت بازار هدف برای سرمایه‌گذاری فعالان مرتبط با اهداف تروریستی گشت و هدف این نهاد از بررسی چنین بازاری در جهت هرچه کمتر نمودن توان بهره‌برداری سودجویان است که با نظارت گروه ویژه اقدام مالی فعالیت آنان کاهش پیدا می‌کند. (فولادی، ۱۳۹۹، ۸۷-۸۸)

همچنین در سال ۲۰۰۸ با رشد تنش‌های هسته‌ای جمهوری اسلامی ایران یک مأموریت دیگر هم در راستای ممانعت از تأمین مالی اشاعه‌ی سلاح‌های کشتار جمعی به وظایف این نهاد اضافه گردید. (بایزیدی، ۱۴۰۰، ۳۶۶)

به‌طورکلی گروه ویژه اقدام مالی تمرکز فعالیت خود را بر روی مسئله‌ی شفافیت گردش‌های مالی در سرتاسر جهان گذاشته است. گروه ویژه اقدام مالی دارای اعضای از جمله بیش از ۳۰ کشور دو نهاد اتحادیه اروپا و شورای همکاری خلیج فارس و عضو ناظر می‌باشد همچنین گروه‌ها و نهادهایی مانند سازمان ملل، صندوق بین‌المللی پول و غیره در این سازمان دارای نماینده ناظر می‌باشند به‌طورکلی با توجه به حاکمیت اعضای گروه ویژه اقدام مالی این گروه شامل ۳۷ حوزه قضایی در سرتاسر جهان است. (فولادی، ۱۳۹۷، ۸۹) عضویت ایران گروه ویژه اقدام مالی دارای نتایج مختلفی می‌باشد که به‌طورکلی می‌توان آن را به دودسته‌ی مثبت و منفی تقسیم کرد نتایج مثبت عضویت عبارت است از:

۱. رفع تحریم و خروج از لیست سیاه .

۲. جذب سرمایه‌گذاری خارجی .

۳. آسان شدن روابط تجاری و معاملات تجار با خارج از کشور .

۴. افزایش شفافیت مالی و جلوگیری از انزوای اقتصادی .

و همچنین نتایج منفی عضویت عبارت است از :

۱. وجود ابهام در حوزه اجرا به دلیل دشواری اجرای قوانین گروه ویژه اقدام مالی در سطح بین‌المللی .

۲. تناقض با قانون اساسی و قاعده‌ی نفی سبیل که بیانگر حرمت تسلط سایرین بر مسلمانان است .

۳. امکان برخورد‌های گزینشی به دلیل فشار اقتصادی و سیاسی. (فولادی، ۱۳۹۷، ۹۰-۹۱).

گروه ویژه اقدام مالی طی سال‌های ۲۰۱۴ تاکنون پس از وقوع حوادثی در سطح جهان به دلیل بستر غیرمتمرکز ارزهای دیجیتال که باعث رشد جرمی در وب تاریک به‌عنوان مثال فروش اسلحه غیرمجاز و سفارش آدمکشی و فروش اعضای بدن و تأمین مالی برای گروه

داعش در سال ۲۰۱۸، تقویت گروه‌های قاچاقچی مواد مخدر و غیره همگی با بهره‌گیری از ارزش‌های دیجیتالی همچون بیت کوین با ارزش مالی بالا در این بستر اقدام به ارائه گزارش و اقدامات به‌طورکلی تحت دو عنوان ابتدایی و اقدام جدی‌تر نمود در این گزارش‌ها به‌طور خاص ارزش‌های دیجیتال را مدنظر قرار داده و تعاریفی نظیر «دسترسی جهانی به ارزش‌های مجازی موجب شده این ارزش‌ها در دنیای دیجیتال و خارج از اعمال نظر دولتی خاص به حیات خویش ادامه دهند» را به جامعه جهانی هشدار داد و در ادامه‌ی این گزارش‌ها ارزش‌های دیجیتال را «به‌صورت ویژه آسیب‌رسان» معرفی نمود.

در سال ۲۰۱۵ گزارشی مبسوط تحت عنوان «راهنمایی برای رویکرد مبتنی بر ریسک ارزش‌های مجازی» ارائه گشت. این گزارش یک روش عملی برای کشورهای در جهت مدیریت و مقابله با استفاده از ارز مجازی و تأمین مالی تروریسم و پولشویی تبدیل گردید.

در طول سال‌های ۲۰۱۷ و ۲۰۱۸ گروه ویژه اقدام مالی به‌طور پیوسته و مستمر توصیه و دستورالعمل‌هایی صادر کرده است همچنین در جهت نوآوری فناوری برای مقابله با تهدیدها، ابزارهای تشویقی قرار داده است و در همین راستا به سمت بازنگری در مقررات خود در باره‌ی ارزش‌های دیجیتال قدم برمی‌دارد. (کدخدایی، نوروزپور، ۱۳۹۹، ۲۱-۲۴)

از اقدامات گروه ویژه اقدام مالی از ابتدای تصویب گروه در سال ۱۹۸۹ تاکنون به‌صورت کلی می‌توان موارد ذیل را نام برد:

۱. تصویب و اصلاح توصیه‌ها
۲. آغاز اقدامات تقابلی علیه ترکیه و اتریش
۳. نظارت فرا نهادی و انتشار لیست سیاه
۴. تصویب کنوانسیون بین‌المللی مبارزه با تأمین مالی تروریسم
۵. تصویب کنوانسیون پالمو
۶. تصویب قطعنامه ۱۶۱۷ شورای امنیت سازمان ملل

با ظهور ارزش‌های دیجیتال و رشد سریع استفاده از آنها، نگرانی‌های جدی در خصوص سوءاستفاده از این ابزارهای نوین در جرائم مالی مانند پولشویی و تأمین مالی تروریسم به وجود آمده است. ویژگی‌های منحصر به فرد ارزش‌های دیجیتال از جمله غیرمتمرکز بودن، عدم وابستگی به نهادهای مرکزی و امکان انجام تراکنش‌های نسبتاً ناشناس، آنها را به ابزاری جذاب برای گروه‌های مجرمانه و تروریستی تبدیل کرده است.

با درک این تهدیدات، سازمان‌های بین‌المللی و نهادهای ناظر بر جریان‌های مالی، تلاش‌های گسترده‌ای را برای کنترل و نظارت بر فعالیت‌های مرتبط با ارزش‌های دیجیتال آغاز کرده‌اند. یکی از مهمترین این نهادها، گروه ویژه اقدام مالی (FATF) است که استانداردها و توصیه‌هایی را برای مبارزه با پولشویی و تأمین مالی تروریسم تدوین می‌کند.

در همین راستا، FATF در سال ۲۰۲۲ توصیه‌های جدیدی را برای مقابله با ریسک‌های مرتبط با دارایی‌های مجازی (ارزش‌های دیجیتال) و ارائه‌دهندگان خدمات مربوطه منتشر کرد. این توصیه‌ها بر افزایش شفافیت، نظارت و همکاری بین‌المللی در این حوزه تأکید دارند. در ادامه، به توضیح جزئیات این توصیه‌های مهم می‌پردازیم

۱. ریسک‌های جرم پولشویی و تأمین مالی تروریسم مرتبط با دارایی‌های مجازی باید شناسایی، ارزیابی و مدیریت شوند (توصیه ۱۵):

این توصیه کشورها را ملزم می‌کند تا نسبت به شناسایی و ارزیابی ریسک‌های ناشی از استفاده از دارایی‌های مجازی در فعالیت‌های پولشویی، تأمین مالی تروریسم و جرائم مالی اقدام کنند. همچنین باید برنامه‌ها و اقدامات لازم را برای مدیریت و کاهش این ریسک‌ها به اجرا بگذارند.

۲. مقررات مربوط به مبارزه با پولشویی و تأمین مالی تروریسم برای ارائه‌دهندگان خدمات دارایی‌های مجازی (توصیه ۱۵):

طبق این توصیه، کشورها باید قوانین و مقررات مربوط به مبارزه با پولشویی و تأمین مالی

تروریسم را برای شرکت‌ها و موسساتی که خدمات مرتبط با دارایی‌های مجازی (مانند صرافی‌های ارز دیجیتال) ارائه می‌دهند، به اجرا بگذارند. این شامل الزامات احراز هویت مشتری، نگهداری سوابق و گزارش دهی معاملات مشکوک است.

۳. الزامات شناسایی مشتری و نگهداری سوابق برای ارائه دهندگان خدمات دارایی‌های مجازی (توصیه‌های ۱۰ و ۱۱):

طبق این توصیه‌ها، ارائه دهندگان خدمات دارایی‌های مجازی باید تحت الزامات «شناسایی مشتری» (KYC) و نگهداری سوابق معاملات قرار گیرند. این امر به افزایش شفافیت و قابلیت ردیابی فعالیت‌های مرتبط با ارزهای دیجیتال کمک می‌کند.

۴. ردیابی و گزارش دهی تراکنش‌های مرتبط با دارایی‌های مجازی (توصیه ۱۶):
کشورها باید الزامات لازم را برای ردیابی تراکنش‌های مرتبط با دارایی‌های مجازی و گزارش دهی معاملات مشکوک در این حوزه وضع کنند. این امر به مقامات امکان می‌دهد تا فعالیت‌های مجرمانه احتمالی را شناسایی و پیگیری کنند.

۵. همکاری بین‌المللی و تبادل اطلاعات (توصیه‌های ۳۷ تا ۴۰):
این توصیه‌ها بر لزوم همکاری بین‌المللی و تبادل اطلاعات میان کشورها و نهادهای ذی‌ربط در زمینه نظارت بر دارایی‌های مجازی و ارائه دهندگان خدمات مربوطه تأکید دارد. این امر به دلیل ماهیت فراملیتی ارزهای دیجیتال و جرائم مرتبط با آن ضروری است. هدف اصلی این توصیه‌های جدید FATF، افزایش شفافیت، نظارت و کنترل بر فعالیت‌های مرتبط با ارزهای دیجیتال و جلوگیری از سوءاستفاده از این ابزارها در جرائم مالی مانند پولشویی و تأمین مالی تروریسم است.

نتیجه‌گیری

این پژوهش به بررسی تأثیر ظهور ارزهای دیجیتال بر حوزه مبارزه با جرائم مالی و نقش چارچوب‌های حقوقی بین‌المللی در مواجهه با این چالش‌ها پرداخته است. یافته‌های تحقیق نشان می‌دهد که ویژگی‌های منحصر به فرد ارزهای دیجیتال، از جمله ماهیت غیرمتمرکز، گمنامی نسبی و استقلال از نهادهای مرکزی، چالش‌های جدی را برای نظام‌های حقوقی و نظارتی سنتی ایجاد کرده است.

تحلیل عمیق سه چارچوب اصلی بین‌المللی - کنوانسیون میریدا، استانداردهای FATF و توصیه‌های گروه G20 نشان می‌دهد که این ابزارها، علی‌رغم ایجاد پایه‌ای برای مبارزه با جرائم مالی در حوزه ارزهای دیجیتال، نیازمند به‌روزرسانی و تطبیق با ماهیت پویای این فناوری هستند. کنوانسیون میریدا با ارائه چارچوبی برای همکاری‌های بین‌المللی در مبارزه با جرائم سازمان‌یافته فراملی، زمینه را برای گسترش این همکاری‌ها به حوزه ارزهای دیجیتال فراهم می‌کند. استانداردهای FATF، با تمرکز بر مبارزه با پولشویی و تأمین مالی تروریسم، راهنمایی‌های ارزشمندی برای تنظیم‌گری در این حوزه ارائه می‌دهند. توصیه‌های گروه G20 نیز با تأکید بر اهمیت نوآوری مالی و همزمان، مدیریت ریسک‌های مرتبط، چشم‌اندازی متوازن را ترسیم می‌کنند.

با این حال، ماهیت فراملیتی و سرعت تحول ارزهای دیجیتال، ضرورت همکاری و هماهنگی گسترده‌تر بین‌المللی را بیش از پیش آشکار می‌سازد. این پژوهش نشان می‌دهد که موفقیت در مبارزه با جرائم مالی مرتبط با ارزهای دیجیتال، مستلزم رویکردی جامع و چندوجهی است که فراتر از مرزهای ملی عمل کند.

بر اساس این یافته‌ها، پیشنهادها زیر برای بهبود اثربخشی مبارزه با جرائم مرتبط با ارزهای دیجیتال ارائه می‌شود:

۱. تدوین و اجرای چارچوب‌های قانونی و نظارتی یکپارچه در سطح بین‌المللی: این امر مستلزم همکاری نزدیک میان کشورها و سازمان‌های بین‌المللی برای ایجاد استانداردهای مشترک و قابل اجرا در سراسر جهان است. این چارچوب‌ها باید به گونه‌ای طراحی شوند که انعطاف‌پذیری لازم برای انطباق با تحولات سریع فناوری را داشته باشند.
۲. ایجاد نهادهای تخصصی مشترک بین‌المللی: این نهادها می‌توانند به عنوان مرکزی برای هماهنگی اقدامات، تبادل اطلاعات و انجام عملیات مشترک در مقیاس جهانی عمل کنند. همچنین، این نهادها می‌توانند به عنوان مرجعی برای به‌روزرسانی مداوم استراتژی‌های مبارزه با جرائم مالی در حوزه ارزهای دیجیتال عمل کنند.
۳. توسعه و اجرای برنامه‌های آموزشی جامع: این برنامه‌ها باید با هدف ارتقای دانش و مهارت‌های نیروهای انتظامی، قضایی و نظارتی در زمینه فناوری‌های نوین مالی و روش‌های پیشرفته مبارزه با جرائم مالی طراحی شوند. آموزش‌های بین‌المللی و تبادل تجربیات می‌تواند به افزایش کارایی این برنامه‌ها کمک کند.
۴. تقویت همکاری‌های بین‌بخشی: ایجاد پلتفرم‌هایی برای همکاری، میان بخش‌های دولتی، خصوصی و دانشگاهی می‌تواند به تولید دانش، نوآوری در روش‌های نظارتی و توسعه راهکارهای فناورانه برای مقابله با جرائم مالی منجر شود. این همکاری‌ها باید در سطح ملی و بین‌المللی گسترش یابند.
۵. توسعه سیستم‌های نظارتی هوشمند: با استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی و یادگیری ماشینی، می‌توان سیستم‌های نظارتی ایجاد کرد که قادر به شناسایی الگوهای مشکوک در تراکنش‌های ارزهای دیجیتال باشند. این سیستم‌ها باید قابلیت به‌روزرسانی مداوم برای مقابله با روش‌های جدید جرائم مالی را داشته باشند.
۶. ایجاد توازن میان نوآوری و امنیت: سیاست‌گذاران باید رویکردی متعادل اتخاذ کنند که ضمن تشویق نوآوری در حوزه فناوری‌های مالی، امنیت و ثبات سیستم مالی را نیز

تضمین کند. این امر مستلزم گفتگوی مستمر میان قانون‌گذاران، نهادهای نظارتی و فعالان صنعت ارزهای دیجیتال است.

در نهایت، این پژوهش تأکید می‌کند که موفقیت در مبارزه با جرائم مالی مرتبط با ارزهای دیجیتال، مستلزم اتخاذ رویکردی جامع، هماهنگ و انعطاف‌پذیر در سطح جهانی است. این رویکرد باید به طور مداوم با توجه به تحولات فناوری و روش‌های جدید جرائم مالی به‌روزرسانی شود.

پیشنهاد می‌شود پژوهش‌های آتی به بررسی تطبیقی اثربخشی این رویکردها در کشورهای مختلف، ارزیابی چالش‌های اجرایی آنها و همچنین تحلیل تأثیر فناوری‌های نوظهور مانند اینترنت اشیا و بلاکچین بر آینده مبارزه با جرائم مالی بپردازند. همچنین، مطالعه در مورد چگونگی ایجاد توازن میان حفظ حریم خصوصی کاربران ارزهای دیجیتال و نیازهای نظارتی برای مبارزه با جرائم مالی، می‌تواند زمینه‌ساز توسعه راهکارهای نوآورانه در این حوزه باشد

منابع و مأخذ

الف- منابع فارسی

بایزیدی، رحیم، (۱۴۰۰)، گروه ویژه اقدام مالی در اقتصاد جهانی و سیاست بین‌الملل-تحلیل الگوی رفتاری گروه ویژه در قبال ایران، فصلنامه‌ی سازمان‌های بین‌المللی، سال ۴، شماره ۳، ۳۹۶-۳۶۳.

بهره مند، حمید، عامری ثانی، امیرکیا، (۱۳۹۸)، چالش‌ها و راه کارهای جرم‌یابی پولشویی از طریق ارزهای رمزنگاری شده، فصلنامه کارآگاه، دوره ۱۲، شماره ۴۶، ۵۵-۷۳.

رهبر، فرهاد، (۱۳۸۲) پولشویی و آثار و پیامدهای آن، مجله تحقیقات اقتصادی، دوره ۳۸، شماره ۳، ۳۳-۵۵.

ریاضی مند، مهران، (۱۳۹۷)، بررسی ابعاد حقوقی ارزهای دیجیتال، انتشارات برتر اندیشان، تهران.

فولادی، مسعود، (۱۳۹۷)، بررسی گروه ویژه اقدام مالی FATF-پیامدهای عضویت ایران، مجله دستاوردهای نوین در مطالعات علوم انسانی، دوره ۱، شماره ۳، ۸۷-۹۲.

قوامی پور سرشکه، محدثه، محمودی، امیررضا (۱۴۰۲)، تاثیر اسناد بین‌المللی بر کنترل جرائم کسب و کار ایران با رویکردی بر ارزهای دیجیتال، انتشارات جهان سیاست، تهران.

کدخدایی، عباسعلی، نوروز پور، حسام، (۱۳۹۹)، چالش ارزهای مجازی در مبارزه با پولشویی و تامین مالی تروریسم با تاکید بر اقدامات و توصیه‌های کارگروه ویژه اقدام مالی FATF، مجله حقوق بین‌المللی، شماره ۶۲، ۲۸-۷.

موسوی، سیدعلی محمد، داوری، حسین، (۱۳۹۰)، نقش و جایگاه گروه ۲۰ در اقتصاد جهانی، فصلنامه سیاست خارجی، دوره ۲۵، شماره ۲، ۵۱۷-۵۳۸.

ب- منابع خارجی

Chainalysis (2022). The 2022 Crypto Crime Report.

Chohan, U. W. (2021). Cryptocurrency: A Theoretical Perspective. SSRN Electronic Journal.

Crimm, N. J., & Majoor, B. (2019). Financing of terrorism and emerging challenges. International & Comparative Law Quarterly, 68(2), 360-371

Europol (2021). Cryptocurrencies: Tracing the path in a crypto world.

FATF (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

FATF (2022). International Standards on Combating Money Laundering and the Financing

- of Terrorism & Proliferation: The FATF Recommendations.
- FATF (2022). Virtual Assets and Virtual Asset Service Providers Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/>
- FATF (2022). Money Laundering and Terrorist Financing Threat from Digital Currencies and Crypto Assets.
- Frankenfield,J(2021,).Cryptocurrency,Investopedia.<https://www.investopedia.com/terms/c/cryptocurrency.asp>
- FrankenfieldJ.(2022,).Decentralized.\Investopedia.<https://www.investopedia.com/terms/d/decentralized.asp>
- G20 (2022). Synthesis of the G20 Policy Principles on Crypto-Assets
- G20 (2020). G20 Finance Ministers and Central Bank Governors Meeting Communiqué
- G20 (2022). G20 Policy Principles on Crypto-Assets
- Shalhoub, Z., & Al-Qudsi, S. (2021). The role of anti-money laundering regulations in combating terrorist financing. *International Journal of Financial Crime*, 1(1), 45-67.
- Tasca, P. (2022). Digital Transformation and the Rise of Cryptocurrencies. In G. de Arcangelis & G. Ferri (Eds.), *Technological and Economic Impact of Digital Transformation* (pp. 101-128). Springer International
- Tiwari et al. (2020). Cyber Crimes and cryptocurrency. *Journal of Cyber Security Technology*, 4(2), 69-77.
- United Nations (1999). *International Convention for the Suppression of the Financing of Terrorism*.
- UNODC (2004). *United Nations Convention against Transnational Organized Crime and the Protocols Thereto*
- UNODC (2022). *The role of cryptocurrencies in human trafficking and migrant smuggling*.
- UNODC (2023). *United Nations Convention against Transnational Organized Crime*.
- U.S. Department of State (2019). *Terrorist Financing Report*.
- Vigna, P. (2022). *A Guide to Crypto's Industrial Revolution*. *The Wall Street Journal*.