

<http://doi.org/10.30510/pscci.2026.570950.1400>

Criminal analysis of digital currencies in the Iranian and German criminal systems

Seyed Mohammad Hadi Masoumi¹
Amir Hossein Rahgoshah^{2*}
Mehdi Hoshyar³

Received: 26 April 2025

Reception: 6 September 2025

Abstract:

Cryptocurrencies, as a new phenomenon in the global financial system, with features such as decentralized nature, anonymity of transactions, and cross-border exchangeability, have provided the basis for a diverse range of economic and financial crimes. This study, with an analytical-comparative approach, examines how the criminal systems of Iran and Germany deal with crimes resulting from the use of cryptocurrencies. The research method is descriptive-analytical and, using legal sources, judicial decisions, and official documents, various dimensions of criminalization, criminal policy, and preventive measures in the two countries have been examined. The main objective of the research is to identify the challenges, legal gaps, and legislative differences between the two legal systems in dealing with crimes such as money laundering, digital fraud, tax evasion, and terrorist financing through cryptocurrencies. The findings show that in the Iranian criminal system, due to the lack of specific laws and a codified legal framework, dealing with cryptocurrency crimes is mainly based on broad interpretations of general laws. In contrast, Germany has taken a more coherent approach by reforming legal structures, recognizing cryptocurrencies as financial assets, and setting explicit regulations in laws such as the German Banking Act (KWG) and the Anti-Money Laundering Act (GwG). In the final section, the study emphasizes the need to formulate a comprehensive criminal policy in Iran and suggests that in order to effectively combat cryptocurrency abuse, it is necessary to put transparent legal frameworks, specialized supervisory institutions, and coordination with international documents such as the FATF guidelines on the agenda

¹PhD Student in Criminal Law and Criminology, Department of Criminal Law and Criminology, Islamic Azad University, Shiraz Branch, Shiraz, Iran
²Professor, Department of Criminal Law and Criminology, Islamic Azad University, Shiraz Branch, Shiraz, Iran (Corresponding Author)
³Professor, Department of Criminal Law and Criminology, Islamic Azad University, Shiraz Branch, Shiraz, Iran

<http://doi.org/10.30510/pssci.2026.570950.1400>

تحلیل کیفری رمز ارزهای دیجیتال در نظام کیفری ایران و آلمان

سید محمد هادی معصومی^۱امیرحسین رهگشا^۲*مهدی هوشیار^۳

تاریخ دریافت: ۱۴۰۴/۰۲/۰۶

تاریخ پذیرش: ۱۴۰۴/۰۳/۱۵

چکیده

رمزارزهای دیجیتال به عنوان پدیده‌ای نوین در نظام مالی جهانی، با ویژگی‌هایی چون ماهیت غیرمتمرکز، ناشناس بودن تراکنش‌ها، و قابلیت تبادل فرامرزی، بستر بروز طیف متنوعی از جرایم اقتصادی و مالی را فراهم ساخته‌اند. این مطالعه با رویکرد تحلیلی — تطبیقی، به بررسی نحوه مواجهه نظام‌های کیفری ایران و آلمان با جرایم ناشی از کاربرد رمزارزها می‌پردازد. روش پژوهش به صورت توصیفی-تحلیلی است و با بهره‌گیری از منابع قانونی، آراء قضایی و اسناد رسمی، ابعاد مختلف جرم‌انگاری، سیاست کیفری، و اقدامات پیشگیرانه در دو کشور بررسی شده است.

هدف اصلی پژوهش، شناسایی چالش‌ها، شکاف‌های قانونی و تفاوت‌های تقنینی میان دو نظام حقوقی در مواجهه با جرایمی نظیر پول‌شویی، کلاهبرداری دیجیتال، فرار مالیاتی و تأمین مالی تروریسم از طریق رمزارزها می‌باشد. یافته‌ها نشان می‌دهند که در نظام کیفری ایران، به دلیل فقدان قوانین اختصاصی و چارچوب حقوقی مدون، مواجهه با جرایم رمزارزی عمدتاً بر اساس تفسیرهای موسّع از قوانین عام صورت می‌گیرد. در مقابل، آلمان با اصلاح ساختارهای قانونی، شناسایی رمزارزها به عنوان دارایی مالی و تنظیم مقررات صریح در قالب قوانین مانند قانون بانکی آلمان (KWG) و قانون مبارزه با پول‌شویی (GWG)، رویکرد منسجم‌تری در پیش گرفته است.

در بخش پایانی، پژوهش با تأکید بر ضرورت تدوین سیاست کیفری جامع در ایران، پیشنهاد می‌کند که جهت مقابله مؤثر با سوءاستفاده‌های رمزارزی، لازم است چارچوب‌های قانونی شفاف، نهادهای نظارتی تخصصی، و هماهنگی با اسناد بین‌المللی همچون دستورالعمل‌های FATF در دستور کار قرار گیرد. واژگان کلیدی: تحلیل کیفری، رمزارز، بلاکچین، ارز مجازی، سیاست

جنایی تطبیقی

^۱دانشجوی دکتری حقوق جزا و جرم‌شناسی، گروه حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد شیراز، شیراز، ایران^۲استاد، گروه حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد شیراز، شیراز، ایران (نویسنده مسئول)^۳استاد، گروه حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد شیراز، شیراز، ایران

پس از بحران مالی سال ۲۰۰۹ و کاهش اعتماد عمومی به نهادهای مالی سنتی، بازارهای جهانی با پدیده‌ای نوظهور به نام ارزهای مجازی یا رمزارزها مواجه شدند. این ارزهای دیجیتال طی مدت کوتاهی توانستند جایگاه قابل توجهی در مبادلات اقتصادی و نظام‌های پرداخت نوین به دست آورند؛ به گونه‌ای که علی‌رغم تردیدها و مقاومت اولیه برخی نهادهای حاکمیتی، توسعه‌دهندگان فناوری و فعالان اقتصادی با تکیه بر ظرفیت‌های فناوری بلاکچین، زمینه گسترش و پذیرش روزافزون این ابزارهای مالی را فراهم کردند (Nakamoto, 2008). رمزارزها نوعی نشان رقومی ارزش هستند که قابلیت انتقال و معامله الکترونیکی داشته و می‌توانند در نقش ابزار مبادله، واحد محاسبه یا ذخیره ارزش مورد استفاده قرار گیرند؛ هرچند در اغلب نظام‌های حقوقی، فاقد جایگاه پول رسمی بوده و ارزش اقتصادی آن‌ها مبتنی بر پذیرش و توافق کاربران شبکه است (European Central Bank, 2019).

ویژگی‌هایی همچون تمرکززدایی، انجام تراکنش‌های همتا به همتا، حذف واسطه‌های مالی سنتی، امکان انتقال سریع و فرامرزی دارایی‌ها و سطح بالای حفظ حریم خصوصی، رمزارزها را به یکی از مهم‌ترین جلوه‌های تحول دیجیتال در عرصه اقتصاد تبدیل کرده است. از این منظر، برخی رمزارزها مانند بیت‌کوین و اتریوم ماهیتی غیرمتمرکز داشته و بدون کنترل مستقیم یک نهاد مرکزی فعالیت می‌کنند، در حالی که برخی دیگر تحت نظارت نهادهای مشخص یا در قالب دارایی‌های دیجیتال تنظیم‌شده توسعه یافته‌اند (Blandin et al., 2019). با وجود فرصت‌های اقتصادی ناشی از این فناوری، ویژگی‌های ساختاری رمزارزها، به‌ویژه ناشناس بودن نسبی کاربران، دشواری ردیابی تراکنش‌ها و ماهیت فرامرزی آن‌ها، زمینه سوءاستفاده در ارتکاب جرایمی مانند پول‌شویی، کلاهبرداری سایبری، فرار مالیاتی، تأمین مالی فعالیت‌های غیرقانونی و جرایم سازمان‌یافته را نیز فراهم کرده است (FATF, 2019).

گسترش جرایم مرتبط با رمزارزها، نظام‌های عدالت کیفری را با چالشی نوین تحت عنوان **جرم‌انگاری فناوری محور** مواجه ساخته است. در این رویکرد، قانونگذار با پدیده‌هایی روبه‌رو است که ماهیت مجرمانه آن‌ها نه صرفاً ناشی از رفتار انسانی، بلکه مرتبط با استفاده از فناوری‌های پیچیده و نوظهور است. ویژگی اصلی این دسته از جرایم، سرعت تحول فناوری و ناتوانی نسبی قواعد کیفری سنتی در پاسخ‌گویی سریع به اشکال جدید بزهکاری است. در چنین شرایطی، نظام کیفری باید میان ضرورت حمایت از نظم عمومی و حفظ اصول بنیادین حقوق کیفری، از جمله اصل قانونی بودن جرم و مجازات، تعادل برقرار کند؛ زیرا توسعه تفسیرهای موسع از قوانین موجود برای پوشش رفتارهای مرتبط با رمزارزها ممکن است با اصل پیش‌بینی‌پذیری قوانین کیفری و ضرورت تعیین دقیق رفتار مجرمانه در تعارض قرار گیرد (Ashworth, 2013).

اصل قانونی بودن جرم و مجازات اقتضا دارد که هیچ رفتاری بدون وجود نص قانونی روشن، جرم تلقی نشده و هیچ مجازاتی بدون حکم صریح قانون اعمال نشود. در حوزه رمزارزها، فقدان مقررات اختصاصی در برخی نظام‌های حقوقی، از جمله ایران، موجب شده است که مراجع قضایی ناگزیر از استفاده از ظرفیت قوانین عام مانند مقررات مربوط به کلاهبرداری، پول‌شویی، جرایم رایانه‌ای و جرایم اقتصادی برای مواجهه با رفتارهای مجرمانه مرتبط با این فناوری شوند. اگرچه استفاده از قوانین موجود در کوتاه‌مدت می‌تواند خلأهای حقوقی را کاهش دهد، اما در بلندمدت ممکن است موجب ابهام در تعیین حدود مسئولیت کیفری، تفاوت در رویه‌های قضایی و کاهش امنیت حقوقی شهروندان شود (شاملو و خلیلی پاجی، ۱۳۹۹).

از سوی دیگر، سیاست جنایی در حوزه رمزارزها با تعارضی اساسی میان حمایت از نوآوری‌های فناورانه و ضرورت کنترل کیفری مخاطرات ناشی از آنها مواجه است. اتخاذ رویکرد کیفری شدید و محدودکننده ممکن است موجب جلوگیری از بهره‌برداری مشروع از ظرفیت‌های فناوری بلاکچین و اقتصاد دیجیتال شود؛ در مقابل، فقدان نظارت و مقررات‌گذاری نیز می‌تواند زمینه افزایش جرایم مالی و آسیب‌های اقتصادی را فراهم کند. بنابراین، سیاست کیفری مطلوب در این حوزه باید از رویکرد صرفاً سرکوبگر فاصله گرفته و به سمت سیاست جنایی متوازن، تنظیم‌گر و پیشگیرانه حرکت کند. در این چارچوب، ابزارهایی مانند نظارت تخصصی، الزام به احراز هویت کاربران، آموزش عمومی، ارتقای توان فنی نهادهای قضایی و استفاده از فناوری‌های تحلیل تراکنش‌های بلاکچینی، در کنار ضمانت اجرای کیفری، نقش مهمی در پیشگیری از جرم ایفا می‌کنند. (FATF, 2019)

تحقیقات انجام‌شده در حوزه رمزارزها عمدتاً بر ابعاد اقتصادی، مالی و فناوری متمرکز بوده‌اند. برخی پژوهش‌ها آثار رمزارزها بر نظام پولی، سیاست‌های مالی و بازار سرمایه را بررسی کرده‌اند، در حالی که مطالعات دیگری به نقش این فناوری در ارتکاب جرایم سایبری، پول‌شویی و فعالیت‌های اقتصادی غیرقانونی پرداخته‌اند. بررسی پیشینه پژوهش نشان می‌دهد که در نظام کیفری ایران، علی‌رغم تصویب برخی قوانین مرتبط با پول‌شویی، جرایم رایانه‌ای و تأمین مالی تروریسم، هنوز چارچوب جامع و مستقلی برای تنظیم مسئولیت کیفری ناشی از فعالیت‌های رمزارزی وجود ندارد و این امر موجب شکل‌گیری چالش‌های تقنینی و قضایی شده است (حسینی مقدم و فرزین‌فر، ۱۳۹۸). در مقابل، آلمان با اتخاذ رویکردی تنظیم‌گرایانه، شناسایی رمزارزها به‌عنوان دارایی مالی و توسعه مقرراتی مانند قانون بانکداری آلمان (KWG) و قانون مبارزه با پول‌شویی (GwG)، تلاش کرده است میان حمایت از نوآوری دیجیتال و کنترل مخاطرات کیفری تعادل ایجاد کند. (BaFin, 2021)

بر این اساس، نوآوری پژوهش حاضر در تحلیل تطبیقی سیاست کیفری ایران و آلمان در مواجهه با جرایم مرتبط با رمزارزها و ارائه راهکارهایی برای اصلاح چارچوب حقوقی

ایران است. پرسش اصلی پژوهش آن است که نظام کیفری ایران چگونه می‌تواند با بهره‌گیری از تجربیات حقوقی آلمان، ضمن رعایت اصول بنیادین حقوق کیفری، چارچوبی مؤثرتر برای پیشگیری، کنترل و مقابله با جرایم مرتبط با رمزارزها ایجاد کند؟ در این راستا، مقاله ابتدا به مفهوم‌شناسی رمزارزها و بررسی ویژگی‌های حقوقی و فنی آن‌ها می‌پردازد؛ سپس مبانی کیفری و سیاست جنایی ایران و آلمان در مواجهه با جرایم رمزارزی مورد تحلیل قرار می‌گیرد. در ادامه، چالش‌های موجود در نظام کیفری ایران بررسی شده و سازوکارهای قانونی و نظارتی آلمان تبیین می‌شود. در پایان، با بهره‌گیری از یافته‌های تطبیقی، پیشنهادهایی برای ایجاد نظام کیفری کارآمدتر در حوزه رمزارزها ارائه خواهد شد.

بیان مسئله

تحولات شتابان فناوری اطلاعات و ارتباطات در دهه‌های اخیر، نظام‌های حقوقی و کیفری را با پدیده‌هایی مواجه ساخته است که ماهیتی متفاوت از اشکال سنتی رفتارهای مجرمانه دارند. یکی از مهم‌ترین جلوه‌های این تحول، ظهور رمزارزهای دیجیتال مبتنی بر فناوری زنجیره بلوکی (Blockchain) است که با ایجاد امکان انتقال ارزش بدون نیاز به واسطه‌های مالی سنتی، ساختارهای متعارف نظام پولی و مالی را دستخوش تغییر کرده است. رمزارزها به دلیل ویژگی‌هایی همچون غیرمتمرکز بودن، سرعت بالای انتقال، امکان انجام تراکنش‌های فرامرزی و سطح بالای ناشناسی، علاوه بر ایجاد فرصت‌های اقتصادی و فناورانه، زمینه‌های جدیدی برای ارتکاب جرایم مالی و سایبری نیز فراهم کرده‌اند (Nakamoto, 2008).

در سال‌های اخیر، استفاده مجرمانه از رمزارزها در حوزه‌هایی مانند پول‌شویی، کلاهبرداری اینترنتی، فرار مالیاتی، تأمین مالی فعالیت‌های غیرقانونی، اخاذی سایبری و جرایم سازمان‌یافته افزایش یافته است. ماهیت فنی و پیچیده این فناوری موجب شده است که روش‌های سنتی کشف جرم، تعقیب کیفری و نظارت مالی با چالش‌های جدی مواجه شوند؛ زیرا در بسیاری از موارد، شناسایی هویت واقعی مرتکبان، تعیین محل وقوع جرم، کشف مسیر انتقال دارایی و توقیف اموال دیجیتال با دشواری‌های فراوان همراه است. (FATF, 2019) از این رو، رمزارزها نه تنها یک موضوع اقتصادی، بلکه مسئله‌ای مهم در حوزه سیاست جنایی و حقوق کیفری محسوب می‌شوند.

یکی از مهم‌ترین چالش‌های نظام‌های کیفری در مواجهه با رمزارزها، مسئله **جرم‌انگاری فناوری‌محور** است. در این حوزه، قانونگذار با رفتارهایی مواجه است که پیش از ظهور فناوری‌های نوین وجود نداشته‌اند و در نتیجه، قوانین کیفری سنتی همواره پاسخگوی تمامی ابعاد آن‌ها نیستند. این وضعیت، ضرورت بازنگری در شیوه‌های جرم‌انگاری و طراحی سیاست کیفری متناسب با تحولات فناوری را مطرح می‌کند. با این حال، هرگونه توسعه قلمرو حقوق کیفری در این زمینه باید با رعایت اصل قانونی بودن جرم و مجازات همراه باشد؛ زیرا تفسیر موسع قوانین موجود برای پوشش رفتارهای جدید ممکن است

موجب کاهش پیش‌بینی‌پذیری حقوق کیفری و ایجاد ناامنی حقوقی برای شهروندان شود. (Ashworth, 2013)

در نظام حقوقی ایران، اگرچه برخی قوانین مانند قانون مبارزه با پول‌شویی، قانون مبارزه با تأمین مالی تروریسم و قانون جرایم رایانه‌ای ظرفیت‌هایی برای برخورد با برخی سوءاستفاده‌های مرتبط با رمزارزها فراهم کرده‌اند، اما هنوز قانون جامع و مستقلى که ماهیت حقوقی رمزارزها، حدود مسئولیت کیفری کاربران، وظایف ارائه‌دهندگان خدمات رمزارزی و سازوکارهای نظارتی را مشخص کند، وجود ندارد. این خلأ قانونی موجب شده است که مواجهه کیفری با جرایم رمزارزی عمدتاً بر تفسیر قوانین عام استوار باشد؛ رویکردی که می‌تواند موجب اختلاف در رویه قضایی، ابهام در تعیین عناوین مجرمانه و دشواری در تعقیب مؤثر مرتکبان شود (حسینی مقدم و فرزین‌فر، ۱۳۹۸).

در مقابل، نظام حقوقی آلمان تلاش کرده است با اتخاذ رویکردی تنظیم‌گرایانه، میان حمایت از نوآوری‌های فناورانه و کنترل مخاطرات کیفری تعادل برقرار کند. این کشور با شناسایی رمزارزها به عنوان دارایی‌های مالی و توسعه مقرراتی مانند قانون بانکداری آلمان (KWG)، قانون مبارزه با پول‌شویی (GwG) و الزامات ناشی از مقررات اتحادیه اروپا، چارچوب مشخص‌تری برای نظارت بر فعالیت‌های مرتبط با دارایی‌های دیجیتال ایجاد کرده است. همچنین، الزام ارائه‌دهندگان خدمات رمزارزی به رعایت الزامات احراز هویت مشتری (KYC)، گزارش معاملات مشکوک و رعایت استانداردهای مبارزه با پول‌شویی، نشان‌دهنده حرکت این کشور از سیاست کیفری صرفاً سرکوبگر به سمت سیاست جنایی پیشگیرانه و ریسک‌محور است. (BaFin, 2021)

مسئله اساسی پژوهش حاضر آن است که نظام کیفری ایران در مواجهه با جرایم ناشی از استفاده از رمزارزها تا چه اندازه توانایی پاسخگویی به این پدیده نوظهور را دارد و آیا می‌توان با بهره‌گیری از تجربه نظام حقوقی آلمان، الگویی کارآمد برای تنظیم‌گری کیفری و پیشگیری از جرایم رمزارزی ارائه کرد؟ به عبارت دیگر، چالش اصلی صرفاً جرم‌انگاری رفتارهای مرتبط با رمزارزها نیست، بلکه ایجاد تعادل میان سه ضرورت اساسی است: نخست، حفظ اصول بنیادین حقوق کیفری مانند اصل قانونی بودن جرم و مجازات؛ دوم، حمایت از ظرفیت‌های اقتصادی و فناورانه رمزارزها؛ و سوم، ایجاد سازوکارهای مؤثر برای پیشگیری و مقابله با سوءاستفاده‌های مجرمانه.

بر این اساس، پژوهش حاضر با رویکردی توصیفی — تحلیلی و تطبیقی، ضمن بررسی مبانی کیفری و سیاست جنایی ایران و آلمان در حوزه رمزارزها، درصدد شناسایی نقاط ضعف نظام حقوقی ایران و ارائه پیشنهادهایی برای ایجاد چارچوبی جامع‌تر، شفاف‌تر و هماهنگ با تحولات فناوری است. اهمیت این مطالعه از آن جهت است که عدم تدوین سیاست کیفری مناسب در برابر رمزارزها می‌تواند از یک سو موجب گسترش جرایم مالی نوین و از سوی دیگر، موجب محدود شدن بی‌دلیل نوآوری‌های فناورانه شود.

مبانی نظری :

تحلیل تطبیقی سیاست‌های جنایی ایران و آلمان

سیاست‌های کیفری ایران و آلمان در مقابله با جرایم رمز ارزی تفاوت‌های قابل توجهی دارند. در حالی که آلمان به دلیل برخورداری از چارچوب‌های قانونی محکم و نظارت دقیق‌تر، با استفاده از قوانین AML و FATF به مبارزه با جرایم مرتبط با رمز ارزها می‌پردازد، سیاست‌های کیفری ایران در این زمینه به صورت جامع و کارآمد اجرا نمی‌شود. این تفاوت‌ها به دلیل تفاوت در ساختارهای قانونی و نحوه اجرای سیاست‌های جنایی در دو کشور است (Feldman, 2021: 55).

در تحلیل تطبیقی سیاست‌های جنایی ایران و آلمان در مقابله با جرایم مرتبط با رمز ارزها، به وضوح می‌توان تفاوت‌های بنیادی در نگرش و اجرای سیاست‌ها مشاهده کرد. کشور آلمان، به عنوان یکی از پیشگامان اروپا در حوزه فناوری و مقررات‌گذاری، برخورداری از چارچوب‌های قانونی محکم را با بهره‌گیری از قوانین مبارزه با پول‌شویی (AML) و سیاست‌های نظارتی سختگیرانه‌تر مرتبط با گروه ویژه اقدام مالی (FATF) ترکیب کرده است. این امر به آلمان امکان می‌دهد تا تراکنش‌های مالی و رمز ارزی را با دقت بیشتری رصد کرده و از فعالیتهای مشکوک یا مجرمانه جلوگیری کند. نهادهایی مانند BaFin (مرجع نظارت بر امور مالی فدرال) نیز به طور جدی با نظارت بر تبادلات رمز ارزی، باعث تقویت کارایی و امنیت در نظام مالی کشور می‌شوند (Feldman, 2021: 55).

در مقابل، در ایران، با وجود رشد روزافزون استفاده از رمز ارزها، همچنان سیاست‌های کیفری و چارچوب‌های قانونی مشخص و جامعی در این زمینه وجود ندارد. این کمبود، منجر به ایجاد خلأ قانونی شده و راه را برای بهره‌برداری‌های مجرمانه در حوزه رمز ارزها هموار کرده است. قوانین فعلی ایران به طور کامل نمی‌توانند با پیچیدگی‌های جرایم سایبری و مالی که از رمز ارزها به عنوان ابزار استفاده می‌کنند، همخوانی داشته باشند. به عنوان مثال، نبود چارچوب‌های اجرایی برای سیاست‌های AML و KYC در تراکنش‌های رمز ارزی، چالشی جدی در کنترل و پیگیری جرایم مرتبط با رمز ارزها ایجاد کرده است، که این خلأها می‌تواند به افزایش فعالیتهای غیرقانونی از جمله پول‌شویی و فرار مالیاتی منجر شود (Levi, 2018: 310).

از سوی دیگر، در آلمان، نقش همکاری‌های بین‌المللی و تبادل اطلاعات با دیگر کشورها در زمینه تراکنش‌های رمز ارزی بسیار پررنگ است. آلمان، به عنوان عضوی از FATF و اتحادیه اروپا، به الزامات بین‌المللی مبارزه با پول‌شویی و تأمین مالی تروریسم پایبند است و به طور منظم پروتکل‌های خود را برای انطباق با سیاست‌های جهانی به‌روز می‌کند. این تعاملات بین‌المللی به آلمان امکان می‌دهد که به صورت مؤثرتری با تهدیدات سایبری و مالی مرتبط با رمز ارزها مقابله کند. در ایران اما، نبود همکاری‌های موثر بین‌المللی و

محدودیت در تبادل اطلاعات، یکی از موانع اساسی در کنترل جرایم فرامرزی و جرایم سایبری مرتبط با رمز ارزها است (Gottschalk, 2019: 122).

همچنین، آلمان در زمینه آموزش و آگاه‌سازی عمومی نیز گام‌های مهمی برداشته و اطلاعات مربوط به امنیت و خطرات بالقوه رمز ارزها را به جامعه انتقال می‌دهد. این در حالی است که در ایران، این بعد از سیاست‌گذاری همچنان جای خالی دارد و بسیاری از افراد بدون اطلاع کافی از خطرات، وارد معاملات رمز ارزی می‌شوند. این امر موجب افزایش جرایمی نظیر کلاهبرداری‌های دیجیتال می‌شود که نیازمند یک سیاست جنایی جامع و مؤثر است.

در مجموع، می‌توان گفت که تفاوت در سیاست‌های کیفری ایران و آلمان در زمینه جرایم رمز ارزی نه تنها به تفاوت در چارچوب‌های قانونی و نظارتی بازمی‌گردد، بلکه به شدت وابسته به عوامل ساختاری نظیر تعاملات بین‌المللی، آگاهی عمومی و نحوه اجرای سیاست‌ها نیز هست. در ایران، چالش‌های فقهی و حقوقی بسیاری پیرامون استفاده و مشروعیت رمز ارزها وجود دارد. از دیدگاه فقهی، برخی از کارشناسان استفاده از رمز ارزها را به دلیل نبود پشتوانه فیزیکی و احتمال ایجاد اختلال در نظم مالی و تورم‌زا بودن آن‌ها، دارای شبهه می‌دانند (نواب‌پور و همکاران، ۱۳۹۷: ۱۲). از سوی دیگر، مراجع مذهبی و حقوق‌دانان در تلاش‌اند تا از منظر فقه حکومتی، راهکارهایی برای مشروعیت‌بخشی به رمز ارزها تدوین کنند، به شرطی که این ابزارها به کاهش وابستگی به ارزهای خارجی و تقویت استقلال اقتصادی کمک کنند.

از دیدگاه حقوقی، عدم وجود قوانین شفاف و جامع درباره رمز ارزها در ایران موجب شده که حوزه‌ای مبهم و پرابهام برای کاربران و سرمایه‌گذاران این حوزه ایجاد شود. با وجود تلاش‌ها برای وضع مقررات در این زمینه، همچنان چارچوب قانونی مدونی برای کنترل، نظارت و پیشگیری از سوءاستفاده‌های احتمالی از رمز ارزها در جرایمی نظیر پول‌شویی و قاچاق مالی وجود ندارد (حسینی مقدم و فرزین‌فر، ۱۳۹۸: ۲۲). این چالش‌ها نشان‌دهنده نیاز فوری به سیاست‌گذاری‌های دقیق و شفاف در این زمینه است تا امکان بهره‌برداری قانونی و مدیریت‌شده از ظرفیت‌های رمز ارزها در اقتصاد کشور فراهم شود. با توجه به مباحث مطرح‌شده، مرور ادبیات نظری این فصل نشان‌دهنده اهمیت و ضرورت تحلیل دقیق ویژگی‌ها و چالش‌های مرتبط با رمز ارزها و نیز نقش قوانین و مقررات در بهینه‌سازی استفاده و مقابله با سوءاستفاده‌های احتمالی از آن‌هاست.

تحلیل تطبیقی سیاست‌های جنایی ایران و آلمان در قبال رمز ارزها

در حوزه تنظیم‌گری رمز ارزها، ایران و آلمان رویکردهای متفاوتی اتخاذ کرده‌اند. در آلمان، چارچوب‌های نظارتی تحت نظارت BaFin (مرجع نظارتی مالی فدرال) شامل مقررات مرتبط با AML (مبارزه با پول‌شویی) و KYC (احراز هویت مشتری) است که توانسته تا حدود زیادی امنیت تراکنش‌ها را تضمین کند. در ایران، عدم وجود یک نهاد

مشخص برای نظارت بر رمز ارزها موجب ضعف در پیگیری قانونی جرایم و اجرای سیاست‌های پیشگیرانه شده است. مقایسه این دو رویکرد می‌تواند به شناسایی راهکارهای بهبود سیاست‌های جنایی و نظارتی در ایران کمک کند (ماتسورا و همکاران، ۲۰۲۱: ۸۴). در نتیجه، تدوین سیاست‌های جنایی مؤثر برای تنظیم و کنترل حوزه رمز ارزها در ایران، با توجه به ماهیت فرامرزی و سایبری این فناوری و تجربه کشورهای پیشرفته‌تر، ضرورت بسیاری دارد.

در ایران، سیاست‌گذاری در زمینه رمز ارزها همچنان در حال تکامل است و چارچوب قانونی و مقررات خاصی در این حوزه به طور کامل اجرایی نشده است. در حالی که برخی از نهادهای رسمی، استفاده از رمز ارزها را مجاز دانسته‌اند، معاملات و تبادلات این ارزها همچنان در فضای قانونی کاملاً شفاف قرار ندارد. به عنوان مثال، هرچند که استخراج رمز ارزها در ایران قانونی شده، تبادل و معاملات آن با ابهاماتی همراه است و این موضوع باعث شده که فرصت‌های بزهکارانه و جرایم مالی مرتبط با رمز ارزها افزایش یابد (Tahmasebi & Esmaeili, 2020: 93).

در مقابل، آلمان با رویکردی تنظیم‌گراانه‌تر و شفاف‌تر نسبت به ایران، سعی کرده است از طریق مقررات دقیق در خصوص معاملات و استخراج رمز ارزها، زمینه سوءاستفاده و جرایم مرتبط با رمز ارزها را کاهش دهد. در این کشور، تمامی نهادهای مالی که به خدمات رمز ارزی می‌پردازند، باید مجوزهای لازم را از BaFin دریافت کرده و تحت نظارت دقیق باشند. چنین مقرراتی در راستای رویکرد پیشگیرانه و کنترلی آلمان است که هدف آن جلوگیری از جرایم مالی و حفاظت از مصرف‌کنندگان است (Gottschalk, 2019: 127).

در نتیجه، می‌توان گفت که سیاست‌های کیفی آلمان در قبال رمز ارزها به دلیل نظارت قوی‌تر و چارچوب شفاف‌تر، نسبت به سیاست‌های ایران کارآمدتر است. این رویکرد می‌تواند الگویی برای ایران در جهت تدوین مقررات جامع‌تر و مؤثرتر باشد. با تدوین سیاست‌های تنظیم‌گراانه و اجرای دقیق آنها، ایران نیز می‌تواند ضمن کنترل جرایم مرتبط با رمز ارزها، از فرصت‌های اقتصادی این فناوری بهره‌برداری کند.

تفاوت‌های سیاست‌های کیفی ایران و آلمان در مواجهه با رمز ارزها را می‌توان به چند محور اصلی تقسیم کرد.

۱. شفافیت و سازوکار قانونی: در آلمان، رمز ارزها به‌عنوان دارایی‌های مالی و ابزارهایی با ارزش اقتصادی تعریف شده‌اند که این تعریف پایه‌ای برای سیاست‌گذاری و قانون‌گذاری ایجاد کرده است. چنین دسته‌بندی مشخصی به نهادهای اجرایی و قضایی کمک می‌کند که در برخورد با جرایم مالی مرتبط با رمز ارزها چارچوب روشنی داشته باشند. در ایران اما به دلیل عدم تعریف دقیق قانونی برای رمز ارزها و نبود قوانین جامع در این زمینه، نظارت و کنترل بر معاملات و استخراج این دارایی‌ها با چالش مواجه است.

نبود شفافیت و تعریف دقیق باعث شده است که تخلفات مالی و سایبری مرتبط با رمز ارزها در ایران به درستی کنترل نشود (Feldman, 2021: 58).

۲. نظارت و تنظیم‌گری در حوزه‌های مالی: آلمان از طریق نظارت گسترده با محوریت BaFin بر تمامی نهادهای مالی فعال در حوزه رمز ارز، توانسته است سیستمی کارآمد برای ردیابی و نظارت بر معاملات رمز ارزها ایجاد کند. این سازمان با ملزم کردن شرکت‌ها به رعایت مقررات ضدپول‌شویی و شناخت مشتری (KYC)، محیطی امن‌تر برای معاملات رمز ارزها فراهم کرده است. در مقابل، ایران علی‌رغم قانونی بودن استخراج رمز ارزها، هنوز چارچوب مشخصی برای نظارت بر تبادل و معاملات رمز ارزها به‌ویژه در صرافی‌های آنلاین ندارد. این خلأ قانونی سبب شده است که بسیاری از معاملات رمز ارزها از نظر مالی و امنیتی کنترل‌نشده باقی بمانند، و این وضعیت می‌تواند زمینه‌ساز جرایم مالی نظیر پول‌شویی باشد (Tahmasebi & Esmaeili, 2020: 97).

۳. همکاری‌های بین‌المللی و مقابله با جرایم سایبری: آلمان با عضویت در نهادهایی همچون FATF و همکاری نزدیک با سایر کشورها در اجرای دستورالعمل‌های ضدپول‌شویی و مقابله با تأمین مالی تروریسم، در سطح بین‌المللی اقدامات مؤثری انجام داده است. این همکاری‌ها سبب شده‌اند که آلمان بتواند در مقابله با جرایم بین‌المللی مرتبط با رمز ارزها گام‌های بلندی بردارد. در ایران اما به دلیل عدم همکاری رسمی با برخی نهادهای بین‌المللی نظیر FATF و محدودیت‌های ناشی از تحریم‌ها، تعاملات بین‌المللی برای پیگیری جرایم مالی در حوزه رمز ارزها محدود است. این محدودیت‌ها پیگیری و شناسایی جرایم سایبری مرتبط با رمز ارزها را دشوار می‌کند و باعث می‌شود که مجرمان بین‌المللی بتوانند با کمترین ریسک از شبکه‌های مالی ایران بهره‌برداری کنند (Brenner, 2019: 89).

۴. سیاست‌های پیشگیرانه و آموزش عمومی: آلمان به‌عنوان بخشی از سیاست‌های پیشگیرانه، برنامه‌های آموزشی برای آگاهی‌بخشی عمومی در مورد خطرات رمز ارزها و کلاهبرداری‌های مرتبط با آنها اجرا می‌کند. آموزش عمومی و آگاهی‌رسانی در این کشور به عنوان یکی از مؤثرترین ابزارهای پیشگیری از جرایم مالی و سایبری شناخته شده است. در ایران، اگرچه افزایش استفاده از رمز ارزها، جامعه را با خطرات مرتبط با این فناوری آشنا کرده است، اما هنوز برنامه‌های رسمی و جامعی برای آموزش عمومی در مورد استفاده ایمن و مخاطرات احتمالی رمز ارزها وجود ندارد. این وضعیت به‌ویژه برای افرادی که دانش کافی در مورد رمز ارزها ندارند، زمینه‌ساز ریسک‌های زیادی می‌شود و احتمال وقوع جرایم مالی را افزایش می‌دهد (Gottschalk, 2019: 132).

در نتیجه، تطبیق سیاست‌های ایران با کشورهای پیشرو در این حوزه همچون آلمان، می‌تواند در توسعه چارچوب‌های قانونی و مقرراتی جامع برای رمز ارزها در ایران مؤثر باشد. بهره‌گیری از تجربه‌های بین‌المللی و توسعه ابزارهای نظارتی، آموزشی و پیشگیرانه

نه تنها به کنترل جرایم مالی مرتبط با رمز ارزها کمک می‌کند بلکه موجب ارتقای ایمنی و شفافیت اقتصادی در این حوزه می‌شود.

قانون‌گذاری ایران و آلمان در رابطه با قوانین ضد پول‌شویی (AML) و مبارزه با تأمین مالی تروریسم (CFT)

قانون‌گذاری ایران در زمینه مبارزه با پول‌شویی و تأمین مالی تروریسم، تحت تأثیر عوامل داخلی و بین‌المللی، روندی تدریجی و متحول را طی کرده است. با توجه به اینکه پول‌شویی و تأمین مالی تروریسم می‌تواند ثبات اقتصادی کشور را به خطر بیندازد و همچنین موجب ایجاد فساد در نظام مالی شود، ایران در سال‌های اخیر اقدامات متعددی را برای تدوین و اصلاح قوانین مرتبط با این موضوع انجام داده است. قانون مبارزه با پول‌شویی در ایران ابتدا در سال ۱۳۸۶ به تصویب مجلس شورای اسلامی رسید. این قانون، بانک‌ها و مؤسسات مالی را ملزم به شناسایی دقیق مشتریان و گزارش فعالیت‌های مشکوک به مراجع نظارتی کرد. همچنین، بر اساس این قانون، شورای عالی مبارزه با پول‌شویی به عنوان نهاد مرکزی نظارت بر اجرای قوانین ضد پول‌شویی تشکیل شد. با این حال، با توجه به تحولات بین‌المللی و فشارهای گروه ویژه اقدام مالی (FATF)، قانون مبارزه با پول‌شویی در سال ۱۳۹۷ مورد بازنگری قرار گرفت و اصلاحاتی در آن اعمال شد. مهم‌ترین تغییرات این قانون شامل تقویت نظارت بر مؤسسات مالی، تعریف دقیق‌تر جرایم مرتبط با پول‌شویی و ارائه سازوکارهایی برای همکاری‌های بین‌المللی در زمینه تبادل اطلاعات مالی بود. مبارزه با تأمین مالی تروریسم نیز به دلیل ارتباط مستقیم آن با ثبات امنیت ملی و روابط بین‌المللی، اهمیت زیادی در سیاست‌های قضایی و اقتصادی ایران دارد. قانون مبارزه با تأمین مالی تروریسم در سال ۱۳۹۵ به تصویب رسید. این قانون، تأمین مالی گروه‌های تروریستی را جرم‌انگاری کرده و مجازات‌هایی برای افرادی که به هر نحوه به تأمین مالی اقدامات تروریستی کمک می‌کنند، در نظر گرفته است. یکی از چالش‌های مهم در این حوزه، تعریف گروه‌های تروریستی است. ایران بر اساس سیاست‌های داخلی و منطقه‌ای خود، برخی گروه‌ها را سازمان‌های مقاومت می‌داند، در حالی که نهادهای بین‌المللی آن‌ها را به عنوان گروه‌های تروریستی قلمداد می‌کنند. این اختلاف دیدگاه موجب شده است که ایران با مشکلاتی در پذیرش کامل توصیه‌های FATF مواجه شود. ایران برای همگام شدن با استانداردهای بین‌المللی، عضویت موقت خود را در FATF اعلام کرد و تعهداتی برای اصلاح قوانین مرتبط با پول‌شویی و تأمین مالی تروریسم ارائه داد. از جمله این تعهدات، تصویب لوایح الحاق ایران به کنوانسیون‌های بین‌المللی مربوط به تأمین مالی تروریسم و اصلاح برخی قوانین داخلی بود. با این حال، این موضوع در فضای سیاسی داخلی، مخالفت‌هایی را به دنبال داشت و برخی از نهادهای سیاسی و امنیتی، اجرای کامل توصیه‌های FATF را تهدیدی برای امنیت ملی کشور دانستند. این اختلافات باعث شد که برخی از لوایح مرتبط با

FATF در شورای نگهبان و مجمع تشخیص مصلحت نظام به چالش کشیده شود و روند اصلاحات قانونی با کندی مواجه گردد. نهادهای نظارتی و اجرایی مسئول مبارزه با پول‌شویی و تأمین مالی تروریسم در ایران شامل بانک مرکزی، واحد اطلاعات مالی (FIU)، شورای عالی مبارزه با پول‌شویی، نیروی انتظامی و دستگاه قضایی هستند. بانک مرکزی نقش مهمی در تدوین مقررات ناظر بر شفافیت تراکنش‌های مالی دارد و واحد اطلاعات مالی وظیفه جمع‌آوری و تجزیه و تحلیل اطلاعات مربوط به فعالیت‌های مشکوک را بر عهده دارد. همچنین، قوه قضاییه و نیروی انتظامی به عنوان نهادهای اجرایی، مسئولیت برخورد با متخلفان و پیگیری قضایی پرونده‌های مرتبط را دارند. یکی از مشکلات عمده در اجرای قوانین ضد پول‌شویی و مبارزه با تأمین مالی تروریسم در ایران، فقدان زیرساخت‌های لازم برای نظارت مؤثر بر فعالیت‌های مالی است. برخی از بانک‌ها و مؤسسات مالی به دلیل عدم دسترسی به سیستم‌های نظارتی پیشرفته، قادر به شناسایی دقیق تراکنش‌های مشکوک نیستند. همچنین، محدودیت‌های بین‌المللی و تحریم‌ها موجب شده است که سیستم بانکی ایران نتواند ارتباطات مؤثری با نهادهای مالی جهانی داشته باشد و تبادل اطلاعات در این زمینه با مشکلاتی روبه‌رو شود. ایران با سرمایه‌گذاری در زیرساخت‌های نظارتی، تدوین قوانین شفاف‌تر، و افزایش همکاری‌های بین‌المللی، بتواند مبارزه با پول‌شویی و تأمین مالی تروریسم را به شیوه‌ای مؤثرتر اجرا کند. همچنین، اصلاح فرایندهای قضایی و بانکی، ارائه آموزش‌های تخصصی به کارکنان مؤسسات مالی، و تصویب قوانین مکمل می‌تواند نقش مهمی در بهبود وضعیت اجرایی این قوانین داشته باشد. تطبیق استانداردهای داخلی با قوانین بین‌المللی در این حوزه، نه تنها به افزایش اعتبار نظام مالی ایران کمک می‌کند، بلکه موجب بهبود روابط اقتصادی و کاهش موانع تعاملات بین‌المللی نیز خواهد شد. با وجود موانع سیاسی و اقتصادی، اتخاذ رویکردهای نوین در قانون‌گذاری و اجرای مقررات ضد پول‌شویی و مبارزه با تأمین مالی تروریسم، می‌تواند زمینه‌ساز تحولات مثبت در نظام مالی و قضایی ایران باشد.

قوانین ضد پول‌شویی (AML) و مبارزه با تأمین مالی تروریسم (CFT) در آلمان به عنوان بخشی از سیاست‌های امنیت مالی و اقتصادی این کشور، تحت نظارت دقیق و اجرای دقیق قرار دارند. این کشور به‌دقت دستورالعمل‌های اتحادیه اروپا، مانند بخشنامه‌های چهارم، پنجم و ششم ضد پول‌شویی (AMLD) را اجرا می‌کند و به عنوان عضوی از گروه ویژه اقدام مالی (FATF)، به اجرای سیاست‌های بین‌المللی در این زمینه متعهد است (FATF, 2019: 33). رویکرد آلمان در قانون‌گذاری و اجرای مقررات AML و CFT بر مبنای رویکرد ریسک‌محور (RBA) بوده و اصول شناسایی و ارزیابی خطرات، مشتریان پرریسک و رویکردهای مبتنی بر دقت کافی (CDD) را شامل می‌شود (European Commission, 2020: 14). طبق قانون بانک‌داری آلمان (KWG)، صرافی‌های ارزهای دیجیتال و سایر ارائه‌دهندگان خدمات مالی مرتبط با ارزهای دیجیتال

به عنوان مؤسسات مالی محسوب شده و ملزم به رعایت الزامات AML و CFT هستند (BaFin, 2021: 58). این الزامات شامل تعهدات زیر می‌شوند:

تعیین مأمور گزارش تخلفات پول‌شویی: مؤسسات مالی موظفند فردی را به عنوان مسئول گزارش‌دهی تخلفات پول‌شویی و جرایم مالی منصوب کنند که مسئول شناسایی و گزارش هرگونه فعالیت مشکوک به واحدهای نظارتی و اطلاعات مالی مربوطه است (BaFin, 2021: 59).

احراز هویت مشتریان (KYC): یکی از اصول اساسی AML و CFT در آلمان، احراز هویت مشتریان (KYC) و بررسی صلاحیت آنها است. این فرایند شامل جمع‌آوری اطلاعات هویتی مشتریان و بررسی دقیق وضعیت مالی آنها می‌شود. برای مشتریان پریسک، ارزیابی صلاحیت مشتری (EDD) الزامی است (European Commission, 2020: 15).

شناسایی افراد دارای منصب سیاسی و مشتریان پریسک: مؤسسات مالی ملزم به شناسایی مشتریانی هستند که در معرض دید سیاسی یا دارای ریسک بالای جرایم مالی هستند. این افراد به عنوان «افراد دارای منصب سیاسی» (PEPs) شناخته می‌شوند و نیاز به بررسی‌های دقیق‌تری دارند (FATF, 2019: 35).

ثبت و ذخیره‌سازی اطلاعات و سوابق تراکنش‌ها: مؤسسات مالی موظفند اطلاعات هویتی مشتریان و سوابق تراکنش‌های آنها را ثبت کرده و برای مدت معینی ذخیره کنند. این الزام برای تسهیل در ارزیابی دقیق و پیگیری تراکنش‌های مالی است (BaFin, 2021: 61).

گزارش‌دهی فعالیت‌های مشکوک: بر اساس قانون پول‌شویی آلمان (GWG)، مؤسسات مالی موظفند فعالیت‌های مشکوک شامل پول‌شویی و تأمین مالی تروریسم را به واحد اطلاعات مالی آلمان (FIU) گزارش کنند. این گزارش‌ها شامل فعالیت‌هایی است که احتمال وقوع جرایم مالی دارند (FIU Germany, 2021: 45).

علاوه بر صرافی‌ها و متولیان، کارگزاری‌های معاملات ارزهای دیجیتال (OTC)، ارائه‌دهندگان خدمات بیمه‌ای مرتبط و شرکت‌های ارائه‌دهنده کیف پول دیجیتال نیز ملزم به رعایت این قوانین هستند (BaFin, 2021: 62). مقررات AML و CFT آلمان کلیه مؤسسات مرتبط با ارزهای دیجیتال را تحت پوشش قرار می‌دهد تا از فعالیت‌های غیرقانونی جلوگیری کرده و امنیت مالی کاربران را تأمین کند.

این قوانین سخت‌گیرانه به‌ویژه در زمینه ارزهای دیجیتال، برای حفاظت از سرمایه‌گذاران و جلوگیری از فعالیت‌های غیرقانونی طراحی شده‌اند و هم‌راستا با مقررات اتحادیه اروپا و FATF اجرا می‌شوند. این سیاست‌ها می‌توانند نقش مهمی در پایداری اقتصادی و ثبات مالی کشور ایفا کنند (European Commission, 2020: 20).

قوانین AML و CFT در آلمان نه تنها برای محافظت از سیستم مالی این کشور، بلکه برای مقابله با تهدیدات مالی و اقتصادی ناشی از ارزهای دیجیتال و جلوگیری از سوءاستفاده

از این ابزارها در فعالیتهای غیرقانونی تدوین شده‌اند. با توجه به اینکه ارزشهای دیجیتال می‌توانند به دلیل ناشناس بودن و سهولت تراکنش‌های بین‌المللی مورد استفاده قرار گیرند، قوانین AML و CFT اهمیت ویژه‌ای در پیشگیری از پول‌شویی و تأمین مالی تروریسم دارند (European Commission, 2020: 24).

روش تحقیق

پژوهش حاضر از نظر روش، توصیفی — تحلیلی و تطبیقی است. در این پژوهش، با استفاده از روش توصیفی — تحلیلی، مفاهیم، مبانی حقوقی و چالش‌های کیفری مرتبط با رمزارزهای دیجیتال بررسی شده و مقررات موجود در نظام حقوقی ایران در زمینه مقابله با جرایم ناشی از استفاده از رمزارزها مورد تحلیل قرار گرفته است. همچنین، با بهره‌گیری از روش تطبیقی، رویکرد نظام کیفری آلمان در زمینه جرم‌انگاری، تنظیم‌گری، پیشگیری و مقابله با جرایم مرتبط با دارایی‌های دیجیتال مطالعه و با وضعیت حقوقی ایران مقایسه شده است.

داده‌های مورد استفاده در این پژوهش به شیوه کتابخانه‌ای و از طریق مطالعه منابع معتبر حقوقی شامل قوانین و مقررات داخلی ایران، قوانین کیفری و مالی آلمان، اسناد بین‌المللی مرتبط با مبارزه با پول‌شویی و تأمین مالی تروریسم، مقالات علمی، کتب تخصصی و پژوهش‌های انجام‌شده در حوزه حقوق فناوری و جرایم سایبری گردآوری شده است. جامعه مورد مطالعه در این پژوهش شامل مجموعه قوانین، مقررات، اسناد حقوقی و منابع علمی مرتبط با سیاست کیفری ایران و آلمان در حوزه رمزارزهای دیجیتال است. تحلیل داده‌ها نیز با استفاده از شیوه استدلال حقوقی و بررسی تطبیقی انجام گرفته تا نقاط قوت و ضعف هر یک از دو نظام حقوقی مشخص و راهکارهای مناسب برای اصلاح سیاست کیفری ایران ارائه شود.

از نظر هدف، این پژوهش کاربردی محسوب می‌شود؛ زیرا یافته‌های آن می‌تواند در فرآیند قانون‌گذاری، تدوین سیاست جنایی مناسب، ایجاد سازوکارهای نظارتی و اصلاح رویکردهای کیفری در مواجهه با جرایم ناشی از فناوری‌های نوین، به‌ویژه رمزارزهای دیجیتال، مورد استفاده قرار گیرد.

یافته‌ها و تجزیه و تحلیل یافته‌ها

یافته‌های پژوهش حاضر نشان می‌دهد که ظهور رمزارزهای دیجیتال، نظام‌های کیفری معاصر را با نوع جدیدی از چالش‌های حقوقی و جرم‌شناختی مواجه ساخته است. برخلاف نظام مالی سنتی که گردش وجوه در آن از طریق نهادهای واسطه‌ای مانند بانک‌ها، مؤسسات اعتباری و سایر ارائه‌دهندگان خدمات مالی کنترل می‌شود، در نظام مبتنی بر فناوری بلاکچین، انتقال دارایی می‌تواند بدون دخالت یک نهاد مرکزی انجام گیرد. این ویژگی اگرچه از منظر افزایش سرعت، کاهش هزینه‌های مبادلات و توسعه نوآوری‌های مالی دارای اهمیت است، اما از دیدگاه سیاست جنایی، موجب کاهش نقاط

کنترل رسمی و افزایش دشواری در شناسایی و تعقیب رفتارهای مجرمانه می‌شود (Nakamoto, 2008). بنابراین، یافته‌های این پژوهش بیانگر آن است که مسئله اصلی در مواجهه کف‌ری با رمزارزها، صرفاً جرم‌انگاری رفتارهای جدید نیست، بلکه ایجاد سازوکاری است که بتواند میان حفظ امنیت اقتصادی، رعایت اصول حقوق کف‌ری و حمایت از نوآوری‌های فناورانه تعادل برقرار کند.

بررسی قوانین و مقررات نظام مالی ایران نشان می‌دهد که قانونگذار برای مقابله با جرایم مالی، مجموعه‌ای از الزامات نظارتی را بر مؤسسات مالی و اشخاص فعال در حوزه پولی و بانکی تحمیل کرده است. مطابق ماده ۵ قانون مبارزه با پول‌شویی مصوب ۱۳۸۶ با اصلاحات بعدی، بانک‌ها، مؤسسات مالی و اعتباری، صرافی‌ها، شرکت‌های سرمایه‌گذاری و سایر اشخاص مشمول مکلف به اجرای مقررات مربوط به مبارزه با پول‌شویی و تأمین مالی تروریسم هستند. همچنین مطابق ماده ۷ همین قانون، شناسایی مراجعان، احراز هویت مالکان واقعی، ثبت و نگهداری اطلاعات معاملات و گزارش فعالیت‌های مشکوک از جمله تکالیف اصلی اشخاص مشمول محسوب می‌شود. این الزامات در واقع بخشی از سیاست جنایی پیشگیرانه نظام مالی ایران برای جلوگیری از ورود منابع مالی نامشروع به چرخه اقتصادی رسمی است (قانون مبارزه با پول‌شویی، ۱۳۸۶).

همچنین قانون مبارزه با تأمین مالی تروریسم مصوب ۱۳۹۴، در راستای تکمیل سازوکارهای پیشگیرانه، تمامی اشخاص و نهادهای مشمول قانون مبارزه با پول‌شویی را مکلف کرده است تا ضمن شناسایی مشتریان، سوابق معاملات و عملیات مالی را نگهداری کرده و موارد مشکوک را به مراجع ذی‌صلاح گزارش دهند. این مقررات نشان می‌دهد که در نظام مالی سنتی، اصل «شناخت مشتری (KYC)» و ثبت اطلاعات مالی، ابزارهای اساسی برای پیشگیری و کشف جرایم اقتصادی محسوب می‌شوند (قانون مبارزه با تأمین مالی تروریسم، ۱۳۹۴).

با این حال، یافته‌های پژوهش نشان می‌دهد که اجرای این الزامات در حوزه رمزارزهای دیجیتال با محدودیت‌های اساسی مواجه است؛ زیرا ساختار فنی رمزارزها بر پایه حذف واسطه‌های سنتی و انجام تراکنش‌های مستقیم میان کاربران شکل گرفته است. در بسیاری از شبکه‌های رمزارزی، کاربران به جای استفاده از حساب بانکی مبتنی بر هویت واقعی، از نشانی‌های دیجیتال استفاده می‌کنند و همین موضوع موجب می‌شود ارتباط میان تراکنش انجام‌شده و شخص واقعی دارنده دارایی همواره به‌صورت مستقیم قابل شناسایی نباشد (Böhme et al., 2015). در نتیجه، ابزارهای سنتی مبارزه با پول‌شویی مانند احراز هویت مشتری، کنترل منشأ وجوه و گزارش‌دهی معاملات مشکوک، در محیط رمزارزی نیازمند بازطراحی و سازگارسازی با ویژگی‌های فناوری بلاکچین هستند.

یکی از مهم‌ترین یافته‌های این پژوهش، نقش تعیین‌کننده مسئله ناشناس بودن نسبی کاربران در افزایش فرصت‌های ارتکاب جرم است. برخلاف تصور عمومی، تراکنش‌های بلاکچین کاملاً ناشناس نیستند، زیرا اطلاعات مربوط به انتقال دارایی‌ها در بسیاری از

شبکه‌ها ثبت عمومی و دائمی می‌شود؛ اما چالش اصلی، ارتباط دادن یک نشانی دیجیتال با هویت واقعی یک فرد مشخص است. این ویژگی سبب شده است که برخی مرتکبان جرایم مالی بتوانند از رمزارزها برای پنهان‌سازی منشأ وجوه، انتقال عواید حاصل از جرم و دشوار کردن فرآیند کشف جرم استفاده کنند. (FATF, 2019) از این رو، یافته‌های تحقیق نشان می‌دهد که سیاست کیفری مناسب در این حوزه نباید بر ممنوعیت کلی رمزارزها متمرکز شود، بلکه باید بر ایجاد سازوکارهای نظارتی هوشمند و متناسب با ویژگی‌های این فناوری استوار باشد.

در نظام حقوقی ایران، فقدان قانون جامع درباره ماهیت حقوقی رمزارزها و مسئولیت کیفری فعالان این حوزه موجب شده است که برخورد با جرایم مرتبط عمدتاً بر اساس قوانین عمومی کیفری صورت گیرد. برای مثال، در مواردی مانند کلاهبرداری‌های رمزارزی، طرح‌های سرمایه‌گذاری جعلی یا سرقت دارایی‌های دیجیتال، ممکن است از ظرفیت عناوین کیفری موجود مانند کلاهبرداری، خیانت در امانت یا جرایم رایانه‌ای استفاده شود؛ اما در موارد پیچیده‌تر مانند استفاده از خدمات ناشناس‌کننده تراکنش‌ها، انتقال بین‌المللی دارایی‌های دیجیتال یا فعالیت در بسترهای غیرمتمرکز، انطباق رفتار با عناوین کیفری موجود با دشواری بیشتری همراه است. این وضعیت با اصل قانونی بودن جرم و مجازات ارتباط مستقیم دارد؛ زیرا توسعه قلمرو کیفری از طریق تفسیر موسع قوانین موجود ممکن است موجب کاهش پیش‌بینی‌پذیری حقوق کیفری شود (Ashworth, 2013).

از منظر جرم‌انگاری فناوری‌محور، یافته‌های پژوهش نشان می‌دهد که رمزارزها نمونه‌ای از تحولاتی هستند که نظام کیفری را ناگزیر از بازنگری در شیوه‌های سنتی مقابله با جرم کرده‌اند. در جرایم سنتی، رفتار مجرمانه معمولاً در فضای فیزیکی رخ داده و امکان شناسایی مرتکب و محل وقوع جرم آسان‌تر است؛ اما در جرایم مرتبط با فناوری‌های غیرمتمرکز، مرزهای جغرافیایی، هویت مرتکب و حتی مفهوم مال موضوع جرم با پیچیدگی‌های جدیدی مواجه شده است. (Wall, 2017) بنابراین، پاسخ کیفری مؤثر نیازمند ترکیبی از قانونگذاری تخصصی، توسعه توان فنی نهادهای کشف جرم و استفاده از ظرفیت‌های فناوری برای ردیابی فعالیت‌های مجرمانه است.

بررسی تطبیقی نظام حقوقی آلمان نشان می‌دهد که این کشور تلاش کرده است به جای اتخاذ رویکرد محدودکننده، چارچوبی تنظیم‌گر برای مدیریت مخاطرات رمزارزها ایجاد کند. در آلمان، رمزارزها به‌عنوان نوعی دارایی مالی شناسایی شده‌اند و ارائه‌دهندگان خدمات مرتبط با دارایی‌های دیجیتال، تحت الزامات نظارتی قانون بانکداری و مقررات مبارزه با پول‌شویی قرار گرفته‌اند. همچنین نهاد نظارت مالی فدرال آلمان (BaFin) نقش مهمی در صدور مجوز، کنترل فعالیت ارائه‌دهندگان خدمات رمزارزی و تضمین رعایت الزامات شفافیت مالی ایفا می‌کند. (BaFin, 2021) این رویکرد نشان می‌دهد که

سیاست جنایی مؤثر در حوزه فناوری‌های نوین، الزاماً مبتنی بر جرم‌انگاری گسترده نیست، بلکه می‌تواند از طریق تنظیم‌گری پیشگیرانه و کنترل هوشمند خطرات تحقق یابد. مقایسه وضعیت ایران و آلمان نشان می‌دهد که تفاوت اساسی میان دو نظام حقوقی، در نحوه مواجهه با پدیده رمزارزهاست. در حالی که نظام حقوقی ایران هنوز عمدتاً در مرحله مواجهه با آثار منفی و پیامدهای کیفری رمزارزها قرار دارد، نظام حقوقی آلمان تلاش کرده است با شناسایی حقوقی این دارایی‌ها و ایجاد الزامات نظارتی، زمینه استفاده مشروع از فناوری را فراهم کرده و هم‌زمان فرصت‌های ارتکاب جرم را کاهش دهد. تجربه آلمان نشان می‌دهد که حمایت از نوآوری و کنترل کیفری دو هدف متعارض نیستند، بلکه می‌توان از طریق سیاست جنایی متوازن میان آن‌ها هماهنگی ایجاد کرد (European Central Bank, 2019).

بر اساس یافته‌های پژوهش، مهم‌ترین راهکار برای نظام کیفری ایران، حرکت از سیاست کیفری واکنشی به سمت سیاست جنایی پیشگیرانه و فناوری‌محور است. این امر مستلزم تدوین مقررات اختصاصی درباره وضعیت حقوقی رمزارزها، تعیین مسئولیت ارائه‌دهندگان خدمات رمزارزی، ایجاد نظام رسمی احراز هویت کاربران، الزام به گزارش‌دهی معاملات مشکوک و تقویت همکاری میان نهادهای مالی، قضایی و انتظامی است. همچنین آموزش تخصصی قضات و ضابطان دادگستری در زمینه فناوری بلاکچین و جرایم مرتبط با دارایی‌های دیجیتال، یکی از الزامات اساسی برای افزایش کارآمدی نظام عدالت کیفری خواهد بود. (FATF, 2019)

در مجموع، یافته‌های این پژوهش نشان می‌دهد که رمزارزها نه صرفاً یک ابزار مالی جدید، بلکه پدیده‌ای چندبعدی با آثار اقتصادی، اجتماعی و کیفری هستند. بنابراین، مواجهه مؤثر با جرایم رمزارزی نیازمند ایجاد تعادل میان سه عنصر اساسی شامل حفظ اصول بنیادین حقوق کیفری، حمایت از توسعه فناوری و ایجاد سازوکارهای نظارتی پیشگیرانه است. تجربه آلمان نشان می‌دهد که تنظیم‌گری هوشمند و سیاست جنایی مبتنی بر مدیریت خطر می‌تواند الگویی مناسب برای اصلاح نظام کیفری ایران در مواجهه با این فناوری نوظهور باشد.

نتیجه‌گیری

ظهور و گسترش رمزارزهای دیجیتال، یکی از مهم‌ترین تحولات فناورانه در حوزه نظام‌های مالی و اقتصادی معاصر محسوب می‌شود که آثار آن فراتر از حوزه اقتصاد بوده و عرصه‌های حقوقی، کیفری و سیاست جنایی را نیز تحت تأثیر قرار داده است. ویژگی‌هایی همچون غیرمتمرکز بودن، امکان انجام تراکنش‌های فرامرزی، حذف واسطه‌های مالی سنتی و استفاده از فناوری رمزنگاری، از یک سو فرصت‌های قابل توجهی برای توسعه اقتصاد دیجیتال، تسهیل مبادلات مالی و افزایش کارایی نظام پرداخت ایجاد کرده است و از سوی دیگر، زمینه‌های جدیدی برای ارتکاب جرایمی مانند

پول‌شویی، کلاهبرداری، فرار مالیاتی، تأمین مالی فعالیت‌های غیرقانونی و جرایم سازمان‌یافته فراهم آورده است (Nakamoto, 2008)؛ (FATF, 2019).

یافته‌های این پژوهش نشان داد که مهم‌ترین چالش نظام‌های کیفری در مواجهه با رمزارزها، صرفاً جرم‌انگاری رفتارهای جدید نیست، بلکه ایجاد تعادل میان سه ضرورت اساسی شامل حمایت از نوآوری‌های فناورانه، رعایت اصول بنیادین حقوق کیفری و ایجاد سازوکارهای مؤثر پیشگیرانه است. ماهیت فناورانه و غیرمتمرکز رمزارزها موجب شده است که بسیاری از ابزارهای سنتی کنترل مالی، از جمله احراز هویت مشتریان، نظارت بر جریان وجوه و گزارش معاملات مشکوک، با محدودیت‌هایی مواجه شوند. از این رو، سیاست کیفری در این حوزه باید از رویکرد صرفاً واکنشی فاصله گرفته و به سمت سیاست جنایی پیشگیرانه و مبتنی بر مدیریت خطر حرکت کند (Böhme et al., 2015).

بررسی تطبیقی نظام کیفری ایران و آلمان نشان داد که تفاوت اصلی میان دو نظام حقوقی، در نحوه مواجهه با ماهیت رمزارزها و میزان توسعه سازوکارهای تنظیم‌گری است. در ایران، علی‌رغم وجود قوانینی مانند قانون مبارزه با پول‌شویی، قانون مبارزه با تأمین مالی تروریسم و قانون جرایم رایانه‌ای، هنوز چارچوب جامع و مستقلى برای تعیین وضعیت حقوقی رمزارزها، مسئولیت کیفری ارائه‌دهندگان خدمات رمزارزی و نحوه نظارت بر فعالیت‌های مرتبط با آن وجود ندارد. این خلأ قانونی موجب شده است که برخورد کیفری با بسیاری از رفتارهای مرتبط با رمزارزها بر اساس تفسیر قوانین عمومی صورت گیرد؛ موضوعی که می‌تواند با چالش‌هایی از منظر اصل قانونی بودن جرم و مجازات و ضرورت پیش‌بینی‌پذیری مقررات کیفری همراه باشد (Ashworth, 2013).

در مقابل، نظام حقوقی آلمان با اتخاذ رویکردی تنظیم‌گرایانه، تلاش کرده است میان حمایت از فناوری‌های نوین مالی و کنترل مخاطرات ناشی از آن تعادل برقرار کند. این کشور با شناسایی رمزارزها به عنوان دارایی‌های مالی، اعمال نظارت بر ارائه‌دهندگان خدمات دارایی‌های دیجیتال و الزام رعایت مقررات مبارزه با پول‌شویی، توانسته است چارچوب حقوقی منسجم‌تری ایجاد کند. نقش نهادهایی مانند سازمان نظارت مالی فدرال آلمان (BaFin) در کنترل فعالیت‌های مرتبط با رمزارزها، نشان‌دهنده حرکت این کشور از سیاست کیفری صرفاً سرکوبگر به سمت سیاست جنایی پیشگیرانه و تنظیم‌محور است (BaFin, 2021).

با این حال، تجربه آلمان نیز نشان می‌دهد که تنظیم‌گری رمزارزها فرآیندی پویا و مستمر است؛ زیرا سرعت تحول فناوری موجب می‌شود مقررات موجود همواره نیازمند بازنگری و اصلاح باشند. بنابراین، حتی نظام‌های حقوقی پیشرفته نیز برای مقابله با جرایم رمزارزی نیازمند توسعه همکاری‌های بین‌المللی، استفاده از فناوری‌های نوین کشف جرم و تقویت ظرفیت‌های تخصصی نهادهای نظارتی هستند (European Central Bank, 2019).

بر اساس نتایج حاصل از پژوهش، می‌توان بیان کرد که ایران برای مواجهه مؤثر با جرایم مرتبط با رمزارزها باید از رویکرد محدودکننده یا صرفاً کیفری فاصله گرفته و به سمت ایجاد یک نظام حقوقی جامع حرکت کند؛ نظامی که ضمن پذیرش ظرفیت‌های اقتصادی فناوری بلاکچین، امکان کنترل سوءاستفاده‌های مجرمانه از آن را نیز فراهم سازد. در این مسیر، بهره‌گیری از تجربه کشورهای پیشرو مانند آلمان می‌تواند زمینه اصلاح سیاست جنایی ایران را فراهم کند، هرچند این الگو باید با توجه به شرایط اقتصادی، حقوقی و نهادی کشور بومی‌سازی شود.

در نهایت، می‌توان نتیجه گرفت که آینده تنظیم‌گری رمزارزها وابسته به ایجاد تعادل میان آزادی نوآوری و ضرورت حفظ امنیت اقتصادی و اجتماعی است. اتخاذ سیاست‌های هوشمندانه، تدوین قوانین شفاف، تقویت همکاری میان نهادهای داخلی و بین‌المللی و توسعه دانش تخصصی در حوزه فناوری‌های مالی، می‌تواند زمینه استفاده ایمن‌تر از رمزارزها و کاهش آثار کیفری ناشی از سوءاستفاده از این فناوری را فراهم کند.

پیشنهادهای

با توجه به یافته‌های پژوهش، پیشنهادهای زیر برای ارتقای کارآمدی نظام کیفری ایران و بهبود سیاست جنایی در حوزه رمزارزهای دیجیتال ارائه می‌شود:

۱. تدوین قانون جامع و تخصصی درباره رمزارزها

ضروری است قانونگذار ایران با تدوین مقررات جامع، وضعیت حقوقی رمزارزها، ماهیت مالی آن‌ها، حقوق و تکالیف کاربران، مسئولیت ارائه‌دهندگان خدمات رمزارزی و حدود مسئولیت کیفری اشخاص فعال در این حوزه را مشخص کند. وجود قانون خاص می‌تواند از پراکندگی مقررات، اختلاف رویه قضایی و تفسیرهای متفاوت جلوگیری کرده و اصل قانونی بودن جرم و مجازات را تقویت کند.

۲. ایجاد نظام رسمی نظارت و احراز هویت ارائه‌دهندگان خدمات رمزارزی

با توجه به نقش احراز هویت در پیشگیری از پول‌شویی و جرایم مالی، پیشنهاد می‌شود فعالیت صرافی‌ها و ارائه‌دهندگان خدمات رمزارزی تحت نظام مجوزدهی و نظارت مشخص قرار گیرد. این نهادها باید همانند مؤسسات مالی سنتی، مکلف به اجرای الزامات شناخت مشتری (KYC)، ثبت اطلاعات معاملات و گزارش فعالیت‌های مشکوک باشند. (FATF, 2019)

۳. تقویت آموزش تخصصی قضات، ضابطان و کارشناسان حقوقی

پیچیدگی فنی فناوری بلاکچین موجب شده است که رسیدگی به پرونده‌های مرتبط با رمزارزها نیازمند دانش تخصصی باشد. بنابراین، آموزش قضات، کارشناسان رسمی، پلیس فتا و سایر نهادهای مرتبط درباره نحوه عملکرد رمزارزها، روش‌های کشف جرم و تحلیل تراکنش‌های بلاکچینی ضروری است.

۴. توسعه همکاری میان نهادهای داخلی

مبارزه مؤثر با جرایم رمزارزی نیازمند هماهنگی میان بانک مرکزی، قوه قضاییه، پلیس فتا، مرکز اطلاعات مالی و سایر نهادهای مرتبط است. ایجاد سازوکار مشترک تبادل اطلاعات می‌تواند موجب افزایش سرعت کشف جرم و کاهش امکان سوءاستفاده از خلأهای نظارتی شود.

۵. بهره‌گیری از فناوری‌های نوین در کشف و پیشگیری از جرم

با توجه به اینکه تراکنش‌های بلاکچینی دارای قابلیت ثبت و ردیابی هستند، استفاده از ابزارهای تحلیل داده و فناوری‌های ردیابی تراکنش می‌تواند نقش مهمی در کشف جرایم ایفا کند. بنابراین، سرمایه‌گذاری در فناوری‌های تحلیل بلاکچین و ایجاد واحدهای تخصصی در این زمینه پیشنهاد می‌شود.

۶. توسعه همکاری‌های بین‌المللی

با توجه به ماهیت فرامرزی رمزارزها، مقابله با جرایم مرتبط با آن بدون همکاری بین‌المللی امکان‌پذیر نیست. همکاری با نهادهای بین‌المللی، تبادل تجربیات حقوقی و هماهنگی با استانداردهای جهانی مبارزه با پول‌شویی می‌تواند نقش مهمی در افزایش کارآمدی نظام کیفری کشورها داشته باشد. (FATF, 2019)

۷. حرکت به سمت سیاست جنایی متوازن

سیاست‌گذاری در حوزه رمزارزها نباید صرفاً مبتنی بر ممنوعیت یا جرم‌انگاری گسترده باشد؛ زیرا چنین رویکردی ممکن است موجب محدود شدن نوآوری‌های اقتصادی شود. پیشنهاد می‌شود سیاست جنایی ایران بر پایه تنظیم‌گری هوشمند، مدیریت خطر و ایجاد تعادل میان توسعه فناوری و حفظ امنیت اقتصادی طراحی شود.

منابع

الف) منابع فارسی

- آذر، عادل). ۱۳۹۹. (آمار و کاربرد آن در مدیریت (جلد اول). تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).
- امامی، علیرضا، زارع، علی و تقی‌خانی، علی. (۱۴۰۱). «تبیین ماهیت فقهی و حقوقی استخراج و بیع رمز ارزها در حقوق ایران». «ماهنامه جامعه‌شناسی سیاسی ایران».
- اخوان‌فرد، مسعود، صفاریان‌زاده، مجید و قاسم‌زاده، محمد. (۱۳۹۲). «جایگاه پول الکترونیکی در حقوق شهروندان شهرهای الکترونیکی». «مجموعه مقالات دومین کنفرانس شهر الکترونیکی».
- احمدی جشفقانی، حسینعلی و میرزائیان، مهدی. (۱۳۹۱). «ماهیت حقوقی پرداخت در پول الکترونیک». «پنجمین کنفرانس ملی پژوهش‌های کاربردی در مدیریت و حسابداری».
- ارغوانی، فریبرز و میراحمدی، سعید. (۱۳۹۸). «جهانی‌شدن ارزهای مجازی و حکمرانی اقتصادی دولت». «دوفصلنامه سیاست و روابط بین‌الملل»، ۳(۶)، ۶۱-۲۹.
- امیری، مرتضی. (۱۳۹۸). «چالش‌های حقوقی ارزهای دیجیتال با نگاهی به قوانین آلمان و آمریکا». پرتال جامع علوم انسانی.
- جعفری، میثم). ۱۳۹۱. (چالش‌های جرم‌انگاری پول‌شویی الکترونیکی در اسناد بین‌المللی. پایان‌نامه کارشناسی ارشد.
- خادمان، محمود، کوشا، ابوطالب و نوری، فاطمه. (۱۴۰۰). «شناسایی ماهیت حقوقی رمزارزها با تحلیل ساختاری آن‌ها در نظام حقوقی ایران». «مجله حقوقی دادگستری»، ۱۵(۱۱۵)، ۳۷۲-۳۴۹.
- خردمند، محسن. (۱۳۹۸). «بررسی فقهی استخراج و مبادله رمز ارزها با تمرکز بر شبکه بیت‌کوین». «معرفت اقتصاد اسلامی»، ۱۰(۲)، ۱۰۹-۱۲۴.
- حسینی مقدم، سیدحسن و فرزین‌فر، به‌آرا. (۱۳۹۸). «تحلیل وضعیت زنجیره‌های بلوکی و معاملات ارزهای دیجیتال از منظر حقوق ایران و فقه امامیه». «تمدن حقوقی»، ۲(۵)، ۴۵-۲۷.
- حسینی، علیرضا، نوح‌امانی و عاشوری، امیر. (۱۳۹۱). «بررسی حقوقی جایگاه پول مجازی در نظام حقوقی ایران و کنوانسیون بیع بین‌المللی کالا». «اولین کنفرانس حقوق و امور قضایی».
- سیدحسینی، میرمیثم و دعایی، میثم. (۱۳۹۳). «بیت‌کوین، نخستین پول مجازی». «ماهنامه بورس، شماره ۱۱۴».

- سلطانی، محمد). ۱۳۹۱. (حقوق بانکی. تهران: انتشارات میزان.
- سلیمانی پور، محمد مهدی، سلطانی نژاد، حامد و پورمطهر، مهدی. (۱۳۹۶). «بررسی فقهی پول مجازی». «دوفصلنامه تحقیقات مالی اسلامی، ۲۶(۲).
- شاملو، باقر و خلیلی پاچی، عارف. (۱۳۹۹). «سیاستگذاری جنایی ریسک‌مدار در برابر فناوری ارزهای مجازی». «مجلس و راهبرد، ۲۷(۱۰۳)، ۲۷۸-۲۴۷.
- شعبانی، امیرمحسن، محسنی دهکلانی، محمد و ابراهیمی، سعید. (۱۳۹۹). «بررسی تطبیقی قانونی‌سازی بیت‌کوین». «پژوهشنامه حقوق تطبیقی، ۴(۱)، ۲۳۸-۲۰۹.
- صفاری، علی، صابری، راضیه و خلیلی پاچی، عارف. (۱۳۹۹). «کارکردهای مجرمانه ارزهای مجازی: تحلیل جرم‌شناختی و راهکارهای پیشگیرانه». «دانشنامه حقوق اقتصادی، ۲۷(۱۸)، ۲۲۳-۲۵۰.
- نواب‌پور، علیرضا، یوسفی، احمدعلی و طالبی، محمد. (۱۳۹۷). «تحلیل فقهی کارکردهای پول‌های رمزنگاری‌شده (مطالعه موردی بیت‌کوین)». «اقتصاد اسلامی، ۱۸(۷۲)، ۲۴۳-۲۱۳.
- نوری، مهدی و نواب‌پور، علیرضا. (۱۳۹۶). «طراحی چارچوب مفهومی سیاستگذاری ارزهای دیجیتال در اقتصاد ایران». «فصلنامه علمی پژوهشی سیاستگذاری عمومی.
- نبوی، سیدمهدی و صابر، محمود. (۱۳۹۹). «مطالعه تطبیقی چالش‌های نظام عدالت کیفری ایران در دادرسی جرایم مرتبط با ارزهای مجازی». «پژوهش‌های حقوق تطبیقی، ۲۴(۱)، ۲۰۸-۱۸۳.
- فرقان‌دوست حقیقی، کامبیز و نداف، رضوانه. (۱۳۹۷). «مروری بر رمز ارزها، فرصت‌ها و تهدیدها». «رویکردهای پژوهشی نوین در مدیریت و حسابداری، ۹(۳)، ۷۴-۶۱.
- میرزاخانی، رضا و سعدی، حسینعلی. (۱۳۹۷). «بیت‌کوین و ماهیت مالی-فقهی پول مجازی». «جستارهای اقتصادی، ۱۵(۳۰)، ۹۲-۷۱.
- مرکز پژوهش‌های مجلس). ۱۳۹۶. (بیت‌کوین، ابزاری نوین در نظام پرداخت‌های الکترونیکی. تهران: معاونت پژوهش‌های زیربنایی و امور تولیدی.

ب) منابع انگلیسی

- Ashworth, A. (2013). *Principles of Criminal Law*. Oxford University Press.
- BaFin. (2021). *Guidelines for Cryptocurrency Regulation and Risks*. Federal Financial Supervisory Authority, Germany.
- BaFin. (2022). *Digital Assets and Regulatory Challenges in Germany*. Federal Financial Supervisory Authority.
- Blandin, A., Cloots, A., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., & Zhang, B. (2019). *Global Cryptoasset Regulatory Landscape Study*.
- Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29(2), 213–238.
- Bundesministerium der Finanzen (BMF). (2022). *Tax Regulations for Digital Assets and Cryptocurrencies in Germany*. Federal Ministry of Finance, Germany.
- Bundesregierung. (2019). *Blockchain Strategy for Germany*. Federal Government of Germany.

- European Central Bank. (2019). *Crypto-Assets: Implications for Financial Stability, Monetary Policy, and Payments*.
- European Commission. (2020). *Markets in Crypto-Assets Regulation (MiCA) Proposal*.
- European Council. (2017). *Fourth Anti-Money Laundering Directive*. Official Journal of the European Union.
- European Council. (2019). *Fifth Anti-Money Laundering Directive*. Official Journal of the European Union.
- FATF. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*.
- Murphy, E. V. (2015). *Bitcoin: Questions, Answers, and Analysis of Legal Issues*. Congressional Research Service.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- Wall, D. S. (2017). *Cybercrime: The Transformation of Crime in the Information Age*.