Research Journal on Business Law and Investment
پژوهشنامه حقوق کسب و کار و سرمایه گذاری

Criminal Protection for Victims of Cryptocurrency Crimes: Legal Challenges and Legislative Solutions

Mostafa Kafi [1], **Yaser Abasi** [2]✉

1. Department of Law, Isf. C., Islamic Azad University, Isfahan, Iran. (Corresponding Author). E-mail: kafi64@iau.ac.ir

2.Department of Governance, Isf.C., Islamic Azad University, isfahan, Iran. E-mail: 1271853450@iau.ir

Received: 2025-07-10	**How to cite this article:**
Revised: 2025-09-07	Kafi, M., & Abasi, Y. (2025). Criminal Protection for Victims of Cryptocurrency Crimes: Legal Challenges and Legislative Solutions. Research Journal on Business Law and Investment, 1(1) (1): 128-145.
Accepted: 2025-09-12	
Available Online: 2025-09-23	

Introduction

The emergence of cryptocurrencies as one of the defining elements of the digital economy has given rise to a new form of victimization known as technological victimization. This phenomenon has presented the Iranian criminal justice system with unprecedented legislative, institutional, and judicial challenges. Features such as the anonymity of perpetrators, the decentralized nature of blockchain platforms, the absence of a legal infrastructure compatible with blockchain technology, and the inherent technical complexities have created serious obstacles to identifying offenders, restoring victims' rights, and establishing criminal liability.

Accordingly, this study seeks to examine the deficiencies of the Iranian criminal justice system in protecting victims of cryptocurrency crimes and to propose legislative measures to address these shortcomings. The main objective is to analyze the legal and legislative challenges faced by such victims within Iran's criminal framework and to develop practical legal solutions to enhance their protection. The subsidiary objectives include:

- Identifying the distinct characteristics of cryptocurrency victims;
- Examining Iran's legislative criminal policy regarding these victims;
- Analyzing the challenges related to criminalization, judicial jurisdiction, digital evidence, and supportive institutions;
- Proposing legislative reforms based on a victim-centered approach.

Method

This research adopts a descriptive-analytical approach, relying on legislative sources, judicial documents, existing procedures, and academic literature. Data were collected through the examination of criminal laws, executive bylaws, Persian scholarly sources, and specialized materials on blockchain technology and cryptocurrencies. The analysis is grounded in logical reasoning and comparative assessment between current legal frameworks and the distinctive features of cryptocurrency crimes and their victims' protective needs.

Findings

The findings reveal that the Iranian criminal justice system faces significant structural challenges in addressing the situation of cryptocurrency crime victims. The key issues include:

Lack of a legal definition for cryptocurrency victims. The absence of formal recognition for this category of victims deprives them of essential rights such as the ability to effectively file complaints, access legal aid, and seek compensation.

Inefficiency of existing criminalization. Many acts specific to cryptocurrency-related offenses—such as private key forgery, sophisticated phishing schemes, and the exploitation of smart contracts—remain outside the scope of explicit criminal definitions.

Difficulties in identifying perpetrators and establishing jurisdiction. Anonymity in transactions, the cross-border nature of digital assets, and the lack of mandatory identity verification on trading platforms hinder the identification of offenders and complicate jurisdictional determinations.

Weaknesses in the system of digital evidence. Technical evidence such as transaction hashes and public keys lacks recognized evidentiary weight in traditional courts, and no clear mechanisms exist for their authentication or evaluation.

Lack of specialized support institutions and compensation mechanisms. The absence of entities such as compensation funds or specialized advisory centers leaves victims in a passive and disadvantaged position.

To address these issues, the following legislative solutions are proposed:

- Enhancing judicial jurisdiction and mandating information disclosure by platforms;
- Designing compensation mechanisms, including the establishment of a national victims' fund;
- Creating specialized judicial authorities and dedicated support institutions;
- Defining the criminal liability of cryptocurrency service providers.

Conclusion

The Iranian criminal justice system currently lacks the necessary capacity to provide effective protection for victims of cryptocurrency crimes. The absence of a coherent legal framework, deficiencies in criminalization, weaknesses in support institutions, and challenges related to digital evidence collectively undermine victims' rights and public confidence in criminal justice. Achieving effective criminal protection requires the adoption of a victim-centered approach through the enactment of specific legislation, reform of criminal policy, and the establishment of specialized institutions. Only through these measures can the principles of digital justice and judicial security be realized in the age of emerging technologies.

English Keywords: Crypto-Crime Victims, Criminal Policy, Penal Protection, Blockchain Technology, Legal Reform.

پژوهشنامه حقوق کسب و کار و سرمایه گذاری
Research Journal on Business Law and Investment

حمایت کیفری از بزه‌دیدگان جرایم رمزارزی: چالش‌های حقوقی و راهکارهای تقنینی

مصطفی کافی[1]✉، یاسر عباسی[2]

۱. استادیار، گروه حقوق، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران. (نویسنده مسئول). رایانامه: m.kafi64@iau.ac.ir

۲. دانشجوی کارشناسی ارشد، گروه حقوق، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران. رایانامه: 1271853450@iau.ir

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی

تاریخ دریافت: ۱۴۰۴/۰۴/۱۹

تاریخ بازنگری: ۱۴۰۴/۰۶/۱۶

تاریخ پذیرش: ۱۴۰۴/۰۶/۲۱

تاریخ انتشار: ۱۴۰۴/۰۷/۰۱

چکیده

ظهور رمزارزها به‌عنوان یکی از نمودهای اقتصاد دیجیتال، زمینه‌ساز شکل‌گیری نوعی بزه‌دیدگی فناورانه شده که نظام حقوق کیفری ایران را با چالش‌های نوظهوری در سطوح تقنینی و نهادی مواجه ساخته است. مختصاتی نظیر ناشناسی فاعل، تمرکززدایی بستر ارتکاب و فقدان زیرساخت‌های حقوقی هم‌ساز با فناوری بلاک‌چین، فرآیند شناسایی مرتکب، استیفای حقوق بزه‌دیده و احراز مسئولیت کیفری را با موانع پیچیده‌ای روبه‌رو کرده است. پژوهش حاضر با روش توصیفی ـ تحلیلی و با استناد به منابع تقنینی، اسناد قضایی و رویه‌های موجود، به بررسی نارسایی‌های ساختاری نظام کیفری ایران در مواجهه با جرائم رمز ارزی و چالش‌های ناشی از آن در حمایت از بزه‌دیدگان می‌پردازد. یافته‌ها مؤید آن است که خلأ جرم‌انگاری اختصاصی، فقدان تعریف قانونی از بزه‌دیده رمز ارزی، ضعف در تعیین صلاحیت قضایی و فقدان نهادهای تخصصی جبرانی، از جمله موانع بنیادین در تحقق حمایت کیفری مؤثر محسوب می‌شوند. در پایان، راهکارهایی با رویکرد بزه‌دیده‌محور جهت اصلاح سیاست جنایی پیشنهاد می‌گردد.

کلیدواژه‌ها: بزه‌دیده رمز ارزی، سیاست جنایی افتراقی، حمایت کیفری، فناوری بلاک‌چین.

استناد: کافی، مصطفی و عباسی، یاسر (۱۴۰۴). حمایت کیفری از بزه‌دیدگان جرایم رمزارزی: چالش‌های حقوقی و راهکارهای تقنینی. *حقوق کسب و کار و سرمایه‌گذاری*، ۱(۱) (پیاپی ۱)، ۱۴۵-۱۲۸.

ناشر: دانشگاه آزاد اسلامی.

http/http//doi.org//10.82466/jbli.2025.1210387

مقدمه

با ظهور فناوری‌های نوین مالی در دهه‌های اخیر، ساختار سنتی تبادلات اقتصادی دچار تحولاتی بنیادین شده است. در این میان، رمزارزها به‌عنوان جلوه‌ای برجسته از فناوری بلاک‌چین، با فراهم‌سازی امکان انتقال سریع، ناشناس و فرامرزی دارایی، بسیاری از قواعد تثبیت‌شده در نظام‌های مالی و کیفری را به چالش کشیده‌اند. ویژگی‌هایی چون عدم تمرکز، گمنامی نسبی کاربران و پیچیدگی فنی تراکنش‌ها، این دارایی‌های دیجیتال را در جایگاهی مبهم و آسیب‌پذیر از منظر حقوق کیفری قرار داده‌اند (رحمان‌زاده، محمودی و ابافت، ۱۴۰۲ :۸۵۲؛ تاج‌لنگرودی و دهدار، ۱۴۰۳ :۹۰). در کنار مزایای اقتصادی و فناورانه رمزارزها، بُعد تاریک آن نیز به‌سرعت بروز یافته است؛ جرائمی نظیر کلاهبرداری پیچیده، پول‌شویی، اخاذی دیجیتال و جعل هویت در بستر بلاک‌چین، با دشواری‌هایی جدی در شناسایی مرتکب و جبران خسارت برای بزه‌دیدگان همراه است. در نظام کیفری ایران، علی‌رغم برخی تلاش‌ها، هنوز چارچوب قانونی مستقل و کارآمدی برای مواجهه با این وضعیت شکل نگرفته است (تاج‌الدینی و مختاری افراکتی، ۱۴۰۳ :۲۷). علاوه بر خلأهای تقنینی، سازوکارهای سنتی حمایت از بزه‌دیده نیز پاسخ‌گوی وضعیت خاص جرائم مبتنی بر فناوری نیست. فقدان تعریف قانونی از بزه‌دیده رمز ارزی، ضعف در تعیین صلاحیت قضایی و نبود نهادهای تخصصی حمایتی، موجب شده بزه‌دیدگان نه‌تنها از حیث مالی متضرر شوند، بلکه در فرآیند دادرسی نیز در موقعیتی غیرمتوازن قرار گیرند.

مسئله اصلی این پژوهش آن است که نظام کیفری ایران چگونه می‌تواند با اصلاح قوانین و توسعه نهادهای حمایتی، حمایت مؤثر از بزه‌دیدگان جرائم رمز ارزی را تضمین نماید. مقاله حاضر با روش توصیفی ـ تحلیلی و با تکیه بر منابع تقنینی و اسناد قضایی، ضمن تبیین خلأهای ساختاری، راهکارهایی را با رویکرد بزه‌دیده‌محور و مبتنی بر اصولی چون عدالت کیفری، جبران خسارت و دسترسی مؤثر به فرآیند دادرسی ارائه می‌دهد.

۱. ویژگی‌های متمایز بزه‌دیدگان جرائم رمزارزمحور

۱-۱. چالش شناسایی مرتکب برای بزه‌دیده در بسترهای ناشناس رمز ارزی

یکی از مهم‌ترین موانع پیش روی بزه‌دیدگان در فضای تبادلات رمز ارزی، دشواری در شناسایی مرتکب جرم و انتساب دقیق رفتار مجرمانه به شخص معین است. این مشکل ناشی از ویژگی‌های فنی ذاتی بسیاری از رمزارزهاست که تراکنش‌ها را بدون اتصال به داده‌های هویتی شفاف مانند نام، شناسه ملی یا اطلاعات بانکی انجام می‌دهند (تاج لنگرودی و دهدار، ۱۴۰۳ :۹۲). در اغلب رمزارزها از جمله بیت‌کوین، تنها آدرس عمومی کیف پول دیجیتال[1] در معرض دید قرار دارد که به خودی خود، هیچ پیوندی با هویت حقیقی یا حقوقی کاربران ندارد. در رمزارزهای با تمرکز ویژه بر حفظ حریم خصوصی مانند مونرو یا زاش، حتی همین میزان از شفافیت نیز وجود ندارد و ساختار تراکنش‌ها به‌گونه‌ای طراحی شده است که ردیابی فنی و حقوقی آنها، حتی برای مراجع رسمی نیز عملاً ناممکن می‌گردد (ربیع پور و نوروی، ۱۴۰۰ :۲۱).

در چنین شرایطی، بزه‌دیده با مانعی اساسی در مسیر استیفای حقوق خود مواجه می‌شود؛ زیرا بدون امکان شناسایی دقیق بزهکار، فرآیند تعقیب کیفری، مطالبه ضرر و زیان و حتی توقیف مال دیجیتال غیرممکن یا فاقد اثربخشی لازم خواهد بود. در نتیجه، ناشناس بودن مرتکب نه تنها ابزار ارتکاب جرم را فراهم می‌سازد، بلکه از منظر حقوقی، جایگاه بزه‌دیده را نیز متزلزل کرده و وی را از بهره‌مندی مؤثر از سازوکارهای عدالت کیفری محروم می‌سازد.

[1] Crypto Wallet

۱-۲. آسیب‌پذیری ناشی از ضعف آگاهی مالی و امنیتی

در بسیاری از موارد، قربانیان جرائم رمز ارزی افرادی هستند که دانش کافی نسبت به مبانی فناوری بلاک‌چین، امنیت اطلاعات یا مفاهیم مالی نوین ندارند. این ناآگاهی، آن‌ها را در معرض طرح‌های اغواگرایانه‌ای نظیر سرمایه‌گذاری‌های رمز ارزی کاذب، توکن‌های جعلی یا نرم‌افزارهای فیشینگ[1] قرار می‌دهد (آذرنژاد، ۱۴۰۱: ۵۱). تبلیغات فریبنده در فضای مجازی که سودهای هنگفت و سریع را وعده می‌دهند، اغلب با استقبال همین دسته از کاربران ناآگاه مواجه می‌شود. در نبود آموزش عمومی یا هشدارهای منسجم از سوی نهادهای مسئول، بزه‌دیدگان نه‌تنها به‌راحتی فریب می‌خورند، بلکه در ادامه نیز به دلیل احساس شرم یا خودسرزنش‌گری، از گزارش‌دهی به نهادهای قضایی خودداری می‌ورزند. این چرخه پنهان ماندن بزه، نه‌تنها مانع تحقق عدالت می‌شود، بلکه زمینه‌ساز تکرار بزهکاری توسط همان مجرمان خواهد بود.

۱-۳. ناتوانی بزه‌دیدگان در پیگیری کیفری در سطح فراملی

یکی از دشوارترین موانع پیش روی بزه‌دیدگان جرائم رمز ارزی، فقدان امکان پیگیری مؤثر در عرصه بین‌المللی است. در بسیاری از موارد، مرتکبان با هویت‌های جعلی و بهره‌گیری از زیرساخت‌های اینترنتی برون‌مرزی، بزه خود را علیه کاربران داخلی مرتکب می‌شوند و پس از آن، عملاً از دسترس نظام قضایی ایران خارج می‌گردند (تاج لنگرودی و دهدار، ۱۴۰۳: ۹۴). عدم عضویت ایران در برخی از کنوانسیون‌های کلیدی مبارزه با جرائم سایبری نظیر «کنوانسیون بوداپست»، ضعف شدید در همکاری‌های قضایی بین‌المللی و محدودیت‌های ناشی از تحریم‌ها، موجب شده است که حتی در موارد شناسایی عامل جرم، مسیر استرداد، محاکمه یا توقیف اموال وی در خارج از کشور مسدود یا به‌شدت پیچیده باشد (قوامی پور سرشکه و محمودی، ۱۴۰۲ :۸۱). نتیجه آن، محرومیت بزه‌دیدگان از دسترسی به سازوکارهای مؤثر جبران خسارت در سطح فرامرزی است.

۱-۴. دشواری در ارائه و جمع‌آوری ادله اثبات و احراز بزه در مرجع قضایی

اثبات وقوع جرم در فضای رمز ارزی، یکی از دشوارترین مراحل برای بزه‌دیدگان محسوب می‌شود؛ زیرا برخلاف جرائم سنتی که غالباً با ادله محسوس و متعارف نظیر شهادت شهود، قراردادهای مکتوب یا شواهد فیزیکی قابل پیگیری‌اند، جرائم مبتنی بر رمزارز در بستری صورت می‌گیرند که بسیاری از ادله سنتی در آن یا اساساً قابل تحقق نیستند یا اعتبار حقوقی محدودی دارند (رحمان‌زاده و همکاران،۱۴۰۲ :۸۵۶). در نظام حقوقی ایران نیز ساختار اثبات جرم، عمدتاً بر پایه ادله معنوی همچون اقرار، بینه و سوگند بنا شده که در بستر دیجیتال و رمز ارزی یا وجود ندارند یا کاربرد عملی بسیار اندکی دارند.

از سوی دیگر، هرچند ممکن است بزه‌دیده در اختیار داشتن داده‌هایی چون هش تراکنش[2]، آدرس عمومی کیف پول، یا سابقه فعالیت در شبکه بلاک‌چین را به‌عنوان ادله ارائه کند، اما این داده‌ها اغلب نزد مراجع قضایی سنتی به‌عنوان دلیل مستقل تلقی نمی‌شوند، مگر آنکه در کنار سایر قرائن و تحت ضوابط دقیق کارشناسی، بتوانند موجبات علم قاضی را فراهم سازند. ضعف زیرساخت کارشناسی رسمی در حوزه رمزارز نیز موجب شده است این داده‌ها در اغلب موارد یا نادیده گرفته شوند یا فاقد تحلیل فنی معتبر باقی بمانند.

در نتیجه، فقدان سازوکار روشن و قابل‌اتکا برای ارائه، تحلیل و پذیرش ادله دیجیتال، یکی از مهم‌ترین موانع در مسیر تحقق عدالت کیفری و حمایت مؤثر از بزه‌دیدگان در جرائم رمز ارزی است.

[1] Phishing
[2] Transaction Hash

۱-۵. فقدان نهادهای حمایتی مؤثر برای قربانیان رمزارز

در نظام حقوقی ایران، برای قربانیان برخی از جرائم سنتی نهادهایی مانند صندوق تأمین خسارت بدنی، دفاتر معاضدت حقوقی یا سازوکارهای بیمه‌ای پیش‌بینی شده است؛ اما در مواجهه با بزه‌دیدگان جرائم رمز ارزی، فقدان کامل یک نهاد تخصصی حمایتی به چشم می‌خورد. نه دولت، نه قوه قضاییه و نه نهادهای مالی، هیچ‌کدام تاکنون چارچوب مشخصی برای رسیدگی به نیازهای قربانیان رمزارز، همراهی اولیه، آموزش، جبران خسارت یا حتی ارجاع به مرجع صالح ارائه نداده‌اند. این وضعیت، حس رهاشدگی و بی‌اعتمادی را در میان بزه‌دیدگان تقویت کرده و آن‌ها را در موقعیتی انفعالی و آسیب‌پذیر قرار داده است.

این خلأ تنها به اشخاص حقیقی محدود نمی‌شود؛ شرکت‌های دانش‌بنیان، استارت‌آپ‌ها و نهادهای عمومی نیز در بسیاری موارد قربانی تخلفات رمز ارزی شده‌اند، اما ساختارهای موجود، ظرفیت پوشش‌دهی حمایتی برای این گروه‌ها را نیز ندارند. در واقع، طیف گسترده‌ای از بزه‌دیدگان بالقوه، از حمایت‌های کیفری و حقوقی نهادینه‌شده بی‌بهره‌اند و این امر، چالش جدی برای کارآمدی عدالت کیفری در حوزه فناوری‌های نوین به وجود آورده است (تاج‌الدینی و مختاری افراکتی، ۱۴۰۳ :۳۵).

مجموعه‌ای از ویژگی‌های خاص ـ از دشواری شناسایی مرتکب، ضعف در آگاهی فنی، ناتوانی در پیگیری بین‌المللی تا مشکلات اثباتی و نبود نهادهای پشتیبان ـ بزه‌دیدگان جرائم رمز ارزی را در موقعیتی به‌مراتب شکننده‌تر از قربانیان جرائم سنتی قرار داده است. این شرایط، نظام تقنینی و قضایی کشور را با ضرورتی فوری برای بازاندیشی در سیاست‌گذاری کیفری مواجه می‌سازد؛ ضرورتی که بدون اصلاحات ساختاری، تدوین قوانین اختصاصی و تقویت ظرفیت‌های حمایتی، نمی‌توان به تحقق آن امید داشت.

۲. بررسی سیاست جنایی تقنینی ایران در حمایت از بزه‌دیدگان جرائم رمزارزمحور

نظام تقنینی ایران در مواجهه با جرائم نوپدید مرتبط با رمزارزها، هنوز از جامعیت و انسجام لازم برای حمایت مؤثر از بزه‌دیدگان برخوردار نیست. اگرچه برخی از این جرائم تحت عناوین کیفری موجود مانند کلاهبرداری، سرقت داده[1] یا جعل قابل پیگیری‌اند، اما در عمل، فقدان قوانین خاص و روزآمد موجب شده است که حقوق بزه‌دیدگان در مراحل مختلف تعقیب، اثبات جرم، استرداد اموال و جبران خسارت با موانع جدی مواجه گردد (زارع و امین نژاد، ۱۴۰۴: ۳۶).

در این بخش، سیاست جنایی تقنینی ایران در قبال بزه‌دیدگان جرائم رمزارزمحور مورد تحلیل قرار می‌گیرد. هدف، شناسایی ظرفیت‌های قانونی موجود، بررسی ناکارآمدی‌ها و نارسایی‌ها و ارزیابی تطابق قوانین فعلی با نیازهای حمایتی خاص این دسته از قربانیان است. تمرکز اصلی بر قوانین کیفری، آیین دادرسی کیفری، قانون جرائم رایانه‌ای[2] و سایر مقررات پراکنده خواهد بود که به‌طور مستقیم یا غیرمستقیم در فرآیند حمایت از بزه‌دیدگان نقش دارند.

با توجه به ویژگی‌های خاص جرائم رمز ارزی، انتظار می‌رود قانون‌گذار با بازاندیشی در ساختار موجود، به سمت طراحی سازوکارهای حمایتی نوین، متناسب با چالش‌های فنی و ساختاری این نوع جرائم حرکت کند. تحلیل حاضر، پایه‌ای برای تبیین ضرورت این اصلاحات و زمینه‌ساز پیشنهادهای راهبردی در بخش‌های بعدی مقاله خواهد بود.

۱-۲. حمایت تقنینی از بزه‌دیدگان کلاهبرداری رمز ارزی

در نظام تقنینی ایران، جرم کلاهبرداری به‌عنوان یکی از ابزارهای حمایتی از بزه‌دیدگان رفتارهای متقلبانه در فضای رمزارزها قابل‌اعمال است. ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری، استفاده از وسایل متقلبانه برای بردن مال غیر را جرم‌انگاری کرده و امکان تعقیب کیفری بزهکاران این حوزه را فراهم ساخته است.

---

[1] Data theft
[2] Cybercrimes

همچنین ماده ۷۴۱ قانون مجازات اسلامی (تعزیرات)، ناظر به کلاهبرداری رایانه‌ای[1] بوده و دربرگیرنده رفتارهایی چون ورود متقلبانه به سامانه‌های رایانه‌ای و فریب سیستم‌های اطلاعاتی با هدف تحصیل مال می‌باشد. این ماده ظرفیت قانونی مناسبی برای پیگرد کیفری کلاهبرداری‌های مبتنی بر رمزارزها از جمله وعده‌های دروغین و صرافی‌های جعلی فراهم کرده است.

بر این اساس، نظام قانون‌گذاری ایران از طریق جرم‌انگاری رفتارهای فریبکارانه در فضای دیجیتال، امکان حمایت کیفری از بزه‌دیدگان رمز ارزی را در قالب عناوین مصرح قانونی فراهم آورده است.

۲-۲. حمایت تقنینی از بزه‌دیدگان سرقت رمزارز و داده‌های دیجیتال

قوانین کیفری ایران در حوزه سرقت فیزیکی و دیجیتال، قابلیت استفاده در حمایت از بزه‌دیدگان رفتارهایی چون ربایش رمزارز، دسترسی غیرمجاز به کیف پول‌های دیجیتال و تخریب اطلاعات مربوط به دارایی‌های رمز ارزی را دارا می‌باشند (تاج‌الدینی و مختاری افراکتی، ۱۴۰۳ :۲۹).

مطابق ماده ۷۴۰ قانون مجازات اسلامی (تعزیرات)، دسترسی غیرمجاز به داده‌های رایانه‌ای جرم تلقی شده و در حوزه رمزارزها نیز قابل تطبیق با رفتارهایی مانند استخراج غیرمجاز کلیدهای خصوصی[2] یا نفوذ به حساب‌های کاربری رمز ارزی است.

همچنین ماده ۲۶۷ قانون مجازات اسلامی، ناظر به سرقت فیزیکی بوده و در مواردی چون ربایش کیف پول‌های سخت‌افزاری یا تجهیزات استخراج رمزارز قابل استناد می‌باشد. ماده ۷۳۶ همین قانون نیز امکان حمایت از بزه‌دیدگان در برابر حذف یا تخریب اطلاعات رمز ارزی را فراهم می‌سازد.

در نتیجه، مجموعه مقررات کیفری موجود، سازوکارهایی برای حمایت از بزه‌دیدگان جرائم مبتنی بر سرقت فیزیکی یا دیجیتال در بستر رمزارزها پیش‌بینی کرده‌اند.

۲-۳. حمایت تقنینی از بزه‌دیدگان جعل رایانه‌ای[3] و تحریف اطلاعات رمز ارزی

بر اساس ماده ۷۳۴ قانون مجازات اسلامی (تعزیرات)، هرگونه تغییر، ورود، حذف یا توقف داده‌های رایانه‌ای با قصد تقلب، تحت عنوان جعل رایانه‌ای جرم‌انگاری شده است. این حکم در فضای رمز ارزی، پوشش‌دهنده رفتارهایی نظیر جعل هش تراکنش، تغییر داده‌های کیف پول دیجیتال یا تحریف اطلاعات پلتفرم‌های معاملاتی است.

جرم جعل رایانه‌ای به‌عنوان یکی از ابزارهای قانونی برای حمایت از بزه‌دیدگان رفتارهای متقلبانه و تحریف اطلاعات دیجیتال در حوزه رمزارز، این امکان را فراهم ساخته است که دادگاه‌ها در مواجهه با شکایات مربوط به تغییرات غیرمجاز در داده‌های رمز ارزی، از مقررات موجود بهره گیرند (کرمی‌پور و رجب زاده باغی، ۱۴۰۲ :۲۳۲).

به این ترتیب، سیاست جنایی تقنینی ایران از طریق شمول مفاد قانونی در حوزه جعل رایانه‌ای، ظرفیت مناسبی برای حمایت از بزه‌دیدگان در برابر تحریف‌های فنی و داده‌ای در بستر رمزارز فراهم آورده است.

۲-۴. مقررات اجرایی و آیین‌نامه‌های مرتبط

افزون بر قوانین کیفری، شماری از مقررات اجرایی و آیین‌نامه‌های تخصصی نیز به‌طور غیرمستقیم به موضوع رمزارزها پرداخته‌اند. از جمله، سیاست‌نامه بانک مرکزی در سال ۱۳۹۸ که دستورالعمل‌هایی را درباره نحوه فعالیت در این حوزه صادر کرده، یا آیین‌نامه‌هایی که به موضوعاتی چون مصرف برق ماینرها یا واردات با رمزارز پرداخته‌اند.

---

[1] Cyber Fraud
[2] Private Keys
[3] Computer Forgery

این مقررات، هرچند اغلب ناظر به جنبه‌های اقتصادی یا فناورانه‌اند، اما از حیث تقنینی و نظام حقوقی رمزارزها، بخشی از بستر حقوقی موجود تلقی می‌شوند و در داوری حقوقی دادگاه‌ها نقش ایفا می‌کنند.

۲-۵. آیین‌نامه اجرایی ماده ۱۴ الحاقی قانون مبارزه با پول‌شویی

یکی از مهم‌ترین مقررات تکمیلی در این زمینه، آیین‌نامه اجرایی ماده ۱۴ الحاقی قانون مبارزه با پول‌شویی (مصوب ۱۳۹۸) است. این آیین‌نامه، شامل ۱۵۸ ماده، با هدف کنترل نقل‌وانتقال غیرقانونی دارایی‌های مجازی، به‌ویژه رمزارزها، تدوین شده و تکالیفی را برای مؤسسات مالی در زمینه شناسایی و گزارش تراکنش‌های مشکوک مقرر داشته است.

در ماده ۳۷ این آیین‌نامه، مسئولیت روشنی برای واحدهای مبارزه با پول‌شویی در خصوص رمزارزها تعیین شده و بانک مرکزی نیز به‌موجب مصوبات شورای عالی مبارزه با پول‌شویی، دامنه فعالیت مؤسسات مالی در این حوزه را به رمزارزهای استخراج‌شده داخلی محدود ساخته است. گرچه تمرکز این آیین‌نامه بر بزه‌کاری مالی است و نه بزه‌دیدگی، اما به‌عنوان سند راهبردی، نقش مهمی در تنظیم ساختار قانونی حوزه رمزارز دارد.

۲-۶. مسئولیت کیفری اشخاص حقوقی در بستر رمزارز

در ساختار تقنینی ایران، موضوع مسئولیت کیفری اشخاص حقوقی در جرائم رایانه‌ای نیز مورد توجه قرار گرفته است. مطابق مواد ۷۴۷ و ۷۴۸ قانون مجازات اسلامی (بخش تعزیرات)، چنانچه ارتکاب جرم در بستر رایانه‌ای توسط مدیر یا با اطلاع وی صورت گیرد، شخص حقوقی نیز تحت شرایطی مسئول شناخته می‌شود. همچنین، مواد ۷۵۱ و ۷۵۲ این قانون، بر وظایف ارائه‌دهندگان خدمات اینترنتی در زمینه پالایش محتوای مجرمانه تأکید کرده‌اند.

در فضای رمز ارزی، این احکام می‌توانند ناظر بر پلتفرم‌هایی مانند صرافی‌های دیجیتال، کیف پول‌های آنلاین یا درگاه‌های ارائه‌دهنده خدمات مبتنی بر بلاک‌چین باشند. چنانچه این بسترها با سهل‌انگاری یا بی‌توجهی نسبت به الزامات قانونی، زمینه وقوع جرم را فراهم سازند یا نسبت به هشدارهای قضایی بی‌اعتنا باشند، در چارچوب مسئولیت کیفری قابل تعقیب خواهند بود. با این حال، نبود معیارهای دقیق در تمایز میان فعل و ترک فعل مؤثر، موجب ابهام در اجرای مؤثر این مقررات شده است (عمرانی فر و بیرنگ، ۱۴۰۳ :۵۲).

۲-۷. ظرفیت‌های آیین دادرسی کیفری در مواجهه با جرائم رمز ارزی

مواد ۶۶۴ تا ۶۸۲ قانون آیین دادرسی کیفری، به‌طور خاص به نحوه رسیدگی به جرائم رایانه‌ای اختصاص یافته‌اند. در این بخش از قانون، مواردی چون نحوه بازرسی سیستم‌های رایانه‌ای، شنود قانونی، حفظ داده‌ها، تحلیل دیجیتال و قواعد جمع‌آوری و اعتبارسنجی ادله الکترونیکی تشریح شده است.

در مواجهه با جرائم رمز ارزی که به‌طور ذاتی بر بستری فنی و دیجیتال رخ می‌دهند، این مقررات می‌توانند ابزارهایی اولیه برای کشف جرم و شناسایی مرتکب فراهم سازند. با این حال، فقدان دستورالعمل‌های جزئی‌تر در حوزه خاص رمزارز و نیز کمبود نیروی انسانی متخصص در تحلیل فنی ادله، موجب شده است کارایی این مقررات در عمل با چالش‌هایی همراه باشد (کرمی‌پور و رجب زاده باغی، ۱۴۰۲: ۲۳۴).

مرور قوانین کیفری و مقررات آیین دادرسی نشان می‌دهد که نظام حقوقی ایران، به‌ویژه در سال‌های اخیر، در تلاش بوده است تا بخشی از مصادیق جرائم رمز ارزی را در قالب عناوین کیفری موجود جای دهد. مقرراتی چون کلاهبرداری رایانه‌ای، جعل دیجیتال، سرقت داده، مسئولیت اشخاص حقوقی و دستورالعمل‌های آیین دادرسی، در ظاهر قابلیت‌هایی برای مداخله کیفری ایجاد کرده‌اند (حسینی، ۱۴۰۳ :۷۵).

بااین‌حال، این چارچوب حقوقی بیش از آنکه مبتنی بر فهم دقیق از ماهیت رمزارزها و اقتضائات فناوری بلاک‌چین باشد، بیشتر نوعی تطبیق منفعلانه با مفاهیم موجود کیفری به نظر می‌رسد. در نتیجه، در بسیاری از موارد، بزه‌دیدگان جرائم رمز ارزی یا در قالب مفاهیم سنتی جای نمی‌گیرند، یا در اثبات بزه و بازیابی حقوق خود با موانع جدی مواجه می‌شوند. همین مسئله، ضرورت بازنگری جدی در قوانین موجود و تدوین مقررات اختصاصی برای حمایت مؤثر از بزه‌دیدگان را تقویت می‌کند.

۳. چالش‌های تقنینی حمایت از بزه‌دیدگان جرائم رمز ارزی

با توجه به ماهیت پیچیده و فناورانه رمزارزها، ساختار فعلی نظام کیفری ایران در حمایت مؤثر از بزه‌دیدگان این حوزه با چالش‌های بنیادین روبروست. بسیاری از مقررات موجود یا اساساً ناظر به چنین بسترهایی تدوین نشده‌اند، یا کوشیده‌اند با توسعه تفسیری مفاهیم کلاسیک، پاسخ‌گوی موقعیت‌های نوظهور باشند. (عباس پور ایکدر، رمضانی و ملکی،۱۴۰۲ :۴۸) با این حال، تجربه‌های عملی در رسیدگی به پرونده‌های رمز ارزی، نشان می‌دهد که این تلاش‌ها کافی نبوده و خلأهای جدی در حوزه تقنین و اجرا باقی مانده است (کرمی‌پور و رجب زاده باغی، ۱۴۰۲ :۲۳۵). در این بخش، مهم‌ترین چالش‌های تقنینی ناظر بر بزه‌دیدگان جرائم رمز ارزی مورد تحلیل قرار می‌گیرند.

۳-۱. ابهام در شناسایی بزه‌دیده و فقدان تعریف قانونی از آن

در حال حاضر، هیچ تعریف خاص و روشنی از «بزه‌دیده رمز ارزی» در قوانین کیفری ایران ارائه نشده است. ویژگی‌هایی نظیر ناشناسی تراکنش‌ها، ناپایداری روابط قراردادی و اختفای هویت طرفین، شناسایی قربانیان را با ابهام مواجه ساخته‌اند. همین امر موجب می‌شود در بسیاری از موارد، امکان بهره‌مندی از حقوق قانونی مانند طرح شکایت مؤثر، مطالبه خسارت یا استفاده از وکیل معاضدتی از بزه‌دیدگان سلب شود (دالوندی، موسوی و غضنفری، ۱۴۰۴: ۲۴۸)

این خلأ نه‌فقط موجب کاهش اثربخشی فرآیند رسیدگی کیفری، بلکه به تضعیف اعتماد عمومی نسبت به توان نظام حقوقی در پاسخ‌گویی به تحولات فناوری منجر شده است. نبود چنین تعریفی در نهایت به حذف تدریجی بزه‌دیده از مرکز توجه عدالت کیفری می‌انجامد.

۳-۲. ناکارآمدی در جرم‌انگاری رفتارهای خاص رمز ارزی

بخش قابل‌توجهی از جرائم مرتبط با رمزارزها در قالب مفاهیم سنتی نظیر کلاهبرداری، جعل یا سرقت داده مورد بررسی قرار می‌گیرند. با این حال، رفتارهایی چون فیشینگ رمز ارزی[1]، جعل کلید خصوصی، سوءاستفاده از باگ‌های قراردادهای هوشمند[2]، یا هک کیف پول‌های غیرمتمرکز، خارج از شمول دقیق این عناوین قرار می‌گیرند (آذرنژاد، ۱۴۰۱ :۷۲).

این فقدان عناوین کیفری خاص، موجب دوگانگی در تشخیص جرم، تشتت آراء و سردرگمی در مرحله تعقیب کیفری شده است. در نتیجه، برخی از مراجع قضایی به دلیل اصل تفسیر مضیق در حقوق کیفری، از اعمال عنوان مجرمانه امتناع می‌ورزند و همین امر امکان حمایت کیفری از بزه‌دیده را تضعیف می‌کند.

۳-۳. دشواری شناسایی و ردیابی مرتکب

ساختار فناورانه رمزارزها، به‌ویژه در رمزارزهایی با تمرکز بر حفظ حریم خصوصی به‌گونه‌ای طراحی شده است که امکان شناسایی مرتکب را به‌شدت محدود می‌کند. کاربران می‌توانند بدون افشای هویت واقعی، در شبکه‌هایی فعالیت کنند که نه تحت نظارت قانونی‌اند و نه تابع مقررات احراز هویت[3] (زررخ، ۱۳۸۹: ۷۱).

---

[1] Crypto Phishing
[2] Smart Contracts
[3] Identity Verification

در کنار این ویژگی فنی، خلأ قانونی نیز مزید بر علت شده است؛ به‌گونه‌ای که در نظام حقوقی ایران هیچ الزام صریحی برای صرافی‌ها یا پلتفرم‌های رمز ارزی داخلی در زمینه ثبت هویت کاربران یا نگهداری تراکنش‌های مشکوک مقرر نشده است. این وضعیت، فرآیند شناسایی بزه‌کار و اثبات عنصر انتساب را در عمل دشوار و بعضاً غیرممکن می‌سازد.

۳-۴. فقدان نظام حمایتی برای جبران خسارت

بزه‌دیدگان جرائم رمز ارزی، در فقدان سازوکارهای جبرانی مؤثر، عملاً امکان بازیابی دارایی خود را از دست می‌دهند. نه صندوقی برای جبران خسارت در این حوزه وجود دارد، نه سازوکار بیمه‌ای و نه نهادی برای ارائه معاضدت حقوقی و پیگیری تخصصی (میرزاخانی و دعائی، ۱۴۰۲: ۱۸).

در بسیاری از موارد، حتی با اثبات وقوع جرم، به دلیل عدم شناسایی مرتکب یا فرار دارایی دیجیتال از قلمرو ملی، اجرای حکم جبرانی عملاً امکان‌پذیر نیست. در غیاب نهادهای مکمل حمایت از بزه‌دیده، این وضعیت به‌نوعی «بزه‌دیدگی مضاعف» منجر شده و احساس بی‌پناهی در میان قربانیان تقویت می‌شود.

۳-۵. ضعف ساختاری در تعیین صلاحیت قضایی

تراکنش‌های رمز ارزی در ذات خود ماهیتی فرامرزی دارند. کاربر می‌تواند از داخل ایران با پلتفرمی در کشور دیگر تعامل داشته باشد و مرتکب جرم نیز ممکن است در حوزه قضایی متفاوتی اقامت داشته باشد. در چنین شرایطی، تعیین مرجع صالح برای رسیدگی کیفری، به یکی از چالش‌های جدی بدل شده است (قوامی پور سرشکه و محمودی، ۱۴۰۲ :۹۲).

نظام حقوقی ایران که عمدتاً بر اصل صلاحیت سرزمینی استوار است، در مواجهه با چنین جرائمی، فاقد انعطاف لازم برای اعمال صلاحیت مؤثر است. از سوی دیگر، نبود توافق‌نامه‌های همکاری قضایی با بسیاری از کشورها و عدم عضویت در کنوانسیون‌های بین‌المللی مبارزه با جرائم سایبری، مسیر احقاق حق بزه‌دیده را در سطح بین‌المللی مسدود ساخته است.

۳-۶. چالش‌های اعتبارسنجی و نگهداری ادله دیجیتال

در پرونده‌های مرتبط با جرائم رمز ارزی، ادله اثباتی عمدتاً در قالب داده‌های فنی و تخصصی ارائه می‌شوند؛ نظیر هش تراکنش‌ها، لاگ کیف پول‌ها و داده‌های ثبت شده در شبکه‌های بلاک‌چین. این نوع ادله، برخلاف شواهد سنتی، نیازمند سازوکارهای خاص برای جمع‌آوری، تحلیل، نگهداری و پذیرش در فرآیند قضایی هستند (رحمان‌زاده و همکاران، ۱۴۰۲ :۸۵۴).

اگرچه آیین‌نامه جمع‌آوری ادله الکترونیکی چارچوبی ابتدایی برای پذیرش این داده‌ها پیش‌بینی کرده، اما در عمل، این مقررات فاقد جزئیات کافی برای پاسخ‌گویی به اقتضائات فنی جرائم رمز ارزی هستند. به‌ویژه در مواردی مانند اعتبارسنجی هش تراکنش‌ها، ذخیره‌سازی امن کلیدهای رمزنگاری‌شده یا ثبت زنجیره زمانی داده‌ها، ضعف‌های جدی در دستورالعمل‌های اجرایی احساس می‌شود (محمدی، میرزایی و صعیدی، ۲۴۵:۱۴۰۳).

علاوه بر این، عدم وجود کارشناسان رسمی متخصص در حوزه رمزارز و بلاک‌چین در فهرست رسمی کارشناسان دادگستری، موجب شده است که بسیاری از داده‌های دیجیتال با تردید یا عدم پذیرش در فرآیند رسیدگی مواجه شوند. این خلأ، نه‌تنها موجب تضییع حقوق بزه‌دیده در مرحله اثبات می‌شود، بلکه زمینه فرار بزه‌کار از پاسخ‌گویی کیفری را نیز فراهم می‌سازد.

مجموعه چالش‌هایی که در این بخش مورد بررسی قرار گرفت، گویای آن است که قوانین کیفری و رویه‌های موجود در نظام قضایی ایران، از منظر حمایت مؤثر از بزه‌دیدگان جرائم رمز ارزی، با نارسایی‌های ساختاری روبه‌رو هستند. فقدان تعریف روشن از بزه‌دیده رمز ارزی، عدم جرم‌انگاری دقیق برای رفتارهای نوظهور، دشواری در شناسایی مرتکب، خلأ نهادهای حمایتی و

ناکارآمدی در تعیین صلاحیت قضایی، همگی نشان از آن دارند که ساختار تقنینی کنونی، برای مواجهه با پیچیدگی‌های فناوری بلاک‌چین و جرائم مرتبط با آن کفایت نمی‌کند.

در غیاب اصلاحات حقوقی بنیادین، این خلأها می‌توانند موجب بی‌اعتمادی گسترده نسبت به‌نظام عدالت کیفری، گسترش بزه‌کاری دیجیتال و حذف تدریجی بزه‌دیدگان از فرآیند قضایی شوند. ازاین‌رو، بازنگری تقنینی و نهادسازی تخصصی، ضرورتی انکارناپذیر در مسیر تحقق عدالت دیجیتال است.

۴. پیشنهادهای تقنینی برای تقویت حمایت کیفری از بزه‌دیدگان جرائم رمز ارزی

۴-۱. پیشنهاد اصلاح و تکمیل قواعد شکلی و ماهوی حمایت کیفری از بزه‌دیدگان رمز ارزی

۴-۱-۱. جرم‌انگاری اختصاصی و تعریف قانونی بزه‌دیده رمز ارزی

تحقق حمایت کیفری مؤثر از بزه‌دیدگان جرائم رمز ارزی، مستلزم تدوین مقرراتی اختصاصی (با تدوین سیاست جنایی افتراقی) است که به‌روشنی متناسب با ویژگی‌های فنی و ساختاری این دسته از جرائم طراحی شده باشند. در وضعیت فعلی، رفتارهایی نظیر جعل کلید خصوصی، فیشینگ رمز ارزی، بهره‌برداری از آسیب‌پذیری‌های فنی در قراردادهای هوشمند یا پول‌شویی در پلتفرم‌های فاقد احراز هویت، در قالب مفاهیم سنتی مانند کلاهبرداری یا جعل به‌سختی قابل انطباق‌اند. این ناهماهنگی سبب سردرگمی در مراجع قضایی و تضعیف جایگاه حقوقی بزه‌دیدگان شده و در مواردی نیز به صدور قرار منع تعقیب به استناد اصل تفسیر مضیق انجامیده اس. (عمرانی فر و بیرنگ، ۱۴۰۳: ۷۳).

افزون بر این، در نظام تقنینی ایران، تعریف روشن و مستقلی از «بزه‌دیده رمز ارزی» وجود ندارد. تعاریف عمومی بزه‌دیده پاسخ‌گوی وضعیت خاص قربانیان جرائم مبتنی بر بلاک‌چین نیستند؛ کسانی که در معرض آسیب‌هایی چون گمنامی مرتکب، فرامرزی بودن بستر ارتکاب جرم و نبود امکان انتساب هویت فنی قرار دارند. همین خلأ موجب سلب امکان بهره‌مندی از حقوقی چون پیگیری قضایی مؤثر، مطالبه خسارت و دسترسی به حمایت‌های معاضدتی برای شمار زیادی از آسیب‌دیدگان شده است (محمدی و همکاران،۱۴۰۳ :۲۴۸).

در راستای رفع این نارسایی‌ها، پیشنهاد می‌شود بخشی مستقل تحت عنوان «جرائم مرتبط با رمزارز و دارایی‌های دیجیتال» به قانون مجازات اسلامی یا قانون جرائم رایانه‌ای افزوده شود. در این بخش، مفاهیم کلیدی نظیر رمزارز، کیف پول دیجیتال، قرارداد هوشمند، کلید خصوصی و تراکنش بلاک‌چینی[1] باید به‌صورت دقیق تعریف و رفتارهای نوپدید مانند جعل دیجیتال رمز ارزی، فیشینگ بلاک‌چینی، سوءاستفاده از نقص‌های فنی، اخاذی رمز ارزی و پول‌شویی در بسترهای غیرمتمرکز، به‌طور مستقل جرم‌انگاری شود.

همچنین، تعریف بزه‌دیده رمز ارزی باید شامل سه عنصر اساسی باشد: اول، وقوع خسارت مستقیم در قالب دارایی دیجیتال؛ دوم، امکان انتساب فنی یا عرفی زیان حتی در صورت ناشناسی مرتکب؛ و سوم، ارتباط ذاتی بزه با ماهیت فناورانه رمزارز. (دالوندی و همکاران، ۱۴۰۴ :۲۶۰) در کنار آن، باید حقوقی همچون امکان شناسایی رسمی بزه‌دیده، اولویت در توقیف دارایی‌های دیجیتال مشکوک، الزام دستگاه‌های ذی‌ربط به ثبت و پیگیری شکایات و بهره‌مندی از وکیل معاضدتی برای بزه‌دیدگان جرائم مهم پیش‌بینی شود.

چنین اصلاحی، ضمن ارتقای جایگاه بزه‌دیده در فرآیند دادرسی، زمینه تدوین یک سیاست جنایی افتراقی و متناسب با چالش‌های اقتصاد دیجیتال را نیز فراهم می‌آورد و چهره‌ای فعال‌تر و روزآمدتر از نظام کیفری در مقابله با جرائم فناورانه به نمایش خواهد گذاشت.

[1] Blockchain Transaction

۴-۱-۲. تقویت صلاحیت قضایی و الزامات قانونی افشای داده در جرائم رمز ارزی با بُعد فرامرزی

فناوری بلاک‌چین با ویژگی‌هایی همچون تمرکززدایی و ناشناسی، امکان شناسایی بزه‌کار در بسیاری از جرائم رمز ارزی را دشوار ساخته است (تاج لنگرودی و دهدار، ۱۴۰۳ :۱۰۰). در غیاب الزامات حقوقی روشن و زیرساخت‌های فنی لازم، بزه‌دیدگان این جرائم در مسیر احقاق حق با بن‌بست‌های جدی مواجه می‌شوند. عدالت کیفری اقتضا دارد که قربانی بتواند به‌صورت مؤثر اقدام به طرح شکایت کند و از اطلاعات لازم برای شناسایی مرتکب برخوردار شود، اما نبود الزام قانونی برای همکاری پلتفرم‌های داخلی با مراجع قضایی، در کنار فقدان سامانه‌ای برای ثبت تراکنش‌های مشکوک، تحقق این هدف را با مانع مواجه کرده است (عباس پور ایکدر و همکاران،۱۴۰۲ :۴۹).

برای رفع این نقیصه، پیشنهاد می‌شود مقرره‌ای الزام‌آور برای پلتفرم‌های فعال در حوزه رمزارزها وضع شود که آن‌ها را ملزم به اجرای فوری دستورات قضایی، افشای اطلاعات کاربران و ارائه لاگ تراکنش‌ها و آدرس‌های کیف پول نماید. تدوین آیین‌نامه‌ای تخصصی جهت تعیین «حد آستانه» برای تراکنش‌هایی که مستلزم احراز هویت دقیق هستند، از دیگر اقدامات ضروری است. علاوه بر آن، ایجاد سامانه‌ای متمرکز در سطح ملی برای ثبت و پایش تراکنش‌های مشکوک با دسترسی محدود مقام قضایی و نیز الزام به استقرار واحدهای پاسخ‌گویی کیفری در صرافی‌های داخلی، از جمله ابزارهایی است که می‌تواند فرآیند شناسایی مرتکب و حفاظت از حقوق بزه‌دیدگان را تسهیل کند.

اجرای این اصلاحات، نه‌تنها موجب افزایش قابلیت تعقیب مجرمان در بستر رمزارز خواهد شد، بلکه اعتماد عمومی به ظرفیت‌های نظام کیفری در برخورد با تهدیدات نوین دیجیتال را نیز تقویت می‌کند.

۴-۱-۳. طراحی سازوکار جبران خسارت و ارتقاء استنادپذیری ادله دیجیتال در حمایت از بزه‌دیدگان رمز ارزی

از ارکان بنیادین حمایت کیفری، تضمین جبران خسارت برای بزه‌دیده است؛ امری که در بستر رمزارز به دلیل پیچیدگی‌های فنی، فقدان شفافیت هویتی و فرامرزی بودن تراکنش‌ها، با موانع متعدد روبه‌روست. در بسیاری از موارد، قربانیان نه تنها توانایی شناسایی و پیگیری مرتکب را از دست می‌دهند، بلکه حتی در صورت شناسایی نیز، به علت فقدان سازوکارهای مؤثر برای توقیف دارایی دیجیتال یا نبود نهاد جبران خسارت، به‌حق خود نمی‌رسند. این وضعیت موجب بروز بزه‌دیدگی مضاعف می‌شود (کرمی‌پور و رجب زاده باغی، ۱۴۰۲ :۲۳۶).

برای پاسخ به این خلأ، تشکیل یک صندوق ملی جبران خسارت برای بزه‌دیدگان جرائم سایبری و رمز ارزی پیشنهاد می‌شود. این صندوق می‌تواند از محل جرائم مکشوفه، جرائم نقدی، یا منابع عمومی تأمین اعتبار شود. همچنین لازم است مسئولیت مدنی و کیفری صرافی‌ها و ارائه‌دهندگان خدمات رمز ارزی در قبال نقص امنیتی یا عدم همکاری با مراجع قضایی، به‌صراحت در قانون پیش‌بینی شود. از سوی دیگر، پیش‌بینی امکان صدور فوری دستور توقیف دارایی دیجیتال، ثبت آن در سامانه‌های پیگیری و رهگیری رمزارزها و طراحی سازوکار بیمه‌گذاری برای تراکنش‌های رمز ارزی با مشارکت بیمه‌گران داخلی، از جمله راهکارهایی است که می‌تواند جبران خسارت و استیفای حقوق بزه‌دیدگان را محقق سازد.

این مجموعه اقدامات، زیرساختی کارآمد برای تحقق عدالت جبرانی در نظام کیفری دیجیتال فراهم خواهد ساخت و جایگاه بزه‌دیده را در سیاست جنایی مرتبط با رمزارز، به‌طور بنیادین ارتقاء می‌دهد.

۴-۲. چالش‌های مربوط به نهادهای حمایتی از بزه‌دیدگان رمز ارزی

۴-۲-۱. پیشنهاد تأسیس نهاد تخصصی حمایت کیفری از بزه‌دیدگان رمز ارزی

فقدان یک نهاد تخصصی با توانایی فنی و حقوقی برای حمایت از بزه‌دیدگان جرائم رمز ارزی، از خلأهای آشکار در نظام کیفری ایران است. با توجه به ماهیت پیچیده و فرامرزی فناوری بلاک‌چین و ناشناس بودن مرتکبان، بسیاری از بزه‌دیدگان قادر

به پیگیری مؤثر حقوق خود نیستند. عدم دسترسی به مشاوره، ناتوانی در تشخیص نوع جرم، تحلیل فنی تراکنش‌ها و مستندسازی ادله، موجب حذف تدریجی آنان از فرآیند عدالت کیفری شده است (زارع و امین نژاد، ۱۴۰۴ :۴۱).

برای رفع این کاستی، پیشنهاد می‌شود نهادی مستقل با عنوان «مرکز ملی حمایت کیفری از بزه‌دیدگان جرائم سایبری و رمز ارزی» تأسیس شود. این مرکز دارای شخصیت حقوقی مستقل، بودجه اختصاصی و صلاحیت اختصاصی باشد. وظایف آن شامل دریافت اولیه شکایات، ارائه مشاوره رایگان، تحلیل کیف پول و ادله، تنظیم شکایات کیفری و تعامل مؤثر با مراجع تخصصی مانند پلیس فتا، دادسراهای فضای مجازی، صرافی‌ها و نهادهای بین‌المللی خواهد بود.

ترکیب مرکز باید از تیم‌های تخصصی در حوزه وکالت کیفری، امنیت رمزارز، بلاک‌چین و روان‌شناسی تشکیل شود. همچنین تدوین دستورالعمل‌های فنی و قضایی برای مستندسازی ادله دیجیتال در حوزه رمزارز نیز در صلاحیت آن باشد. این مرکز می‌تواند ابتدا ذیل شورای عالی فضای مجازی یا مرکز توسعه عدالت الکترونیکی قوه قضائیه مستقر شود و سپس به نهادی مستقل تبدیل گردد.

۴-۲-۲. پیشنهاد طراحی نظام الزام‌آور احراز هویت کیفری در فضای رمزارز

احراز هویت کیفری کاربران، شرط بنیادین برای شناسایی مرتکب، تعقیب کیفری و جبران ضرر بزه‌دیده در جرائم رمز ارزی است؛ اما ویژگی‌هایی مانند ناشناسی تراکنش‌ها و استفاده از کیف پول‌های غیرمتمرکز، این امکان را به‌شدت محدود کرده‌اند. در وضعیت فعلی، نبود الزام قانونی صریح برای پلتفرم‌های رمز ارزی در خصوص ثبت هویت کاربران، موجب شده است بزه‌دیدگان علیرغم اثبات وقوع جرم، امکان معرفی فاعل قابل تعقیب را نداشته باشند (ربیع پور و نوروزی، ۱۴۰۰ :۵۸).

برای رفع این خلأ، ضروری است «نظام احراز هویت کیفری رمز ارزی» در قالب قانون جامع حمایت از بزه‌دیدگان فضای مجازی طراحی شود. این نظام باید شامل الزام کلیه پلتفرم‌های داخلی به ثبت دقیق اطلاعات هویتی) مانند شماره ملی، IP، شناسه بانکی و تصویر شناسنامه(، ایجاد «سامانه ملی هویت کیفری رمز ارزی» با نظارت مرکز ملی فضای مجازی یا پلیس فتا و پیش‌بینی دسترسی محدود مقام قضایی به اطلاعات این سامانه باشد.

همچنین، برای اجرای مؤثر این نظام، باید ضمانت اجراهای کیفری و انضباطی برای پلتفرم‌های متخلف و الزام به انطباق با استانداردهای بین‌المللی نیز در نظر گرفته شود. این اقدامات، پیش‌نیاز تحقق عدالت کیفری در حوزه رمزارز و عاملی کلیدی در توانمندسازی بزه‌دیده برای احقاق حق در برابر فناوری‌های نوپدید و پُر ریسک است (قوامی پور سرشکه و محمودی، ۱۴۰۲: ۹۵).

۴-۲-۳. طراحی نظام صلاحیت قضایی اختصاصی برای جرائم رمز ارزی

نبود ساختار مشخص برای تعیین صلاحیت قضایی در جرائم رمز ارزی، یکی از موانع اساسی در حمایت کیفری از بزه‌دیدگان این حوزه است. ویژگی‌های فناورانه رمزارزها نظیر غیرمتمرکز بودن، ناشناسی کاربران و ماهیت فرامرزی تراکنش‌ها، موجب شده‌اند که بزه‌دیدگان در همان مراحل ابتدایی طرح شکایت، با ابهام در مرجع صالح، اطاله دادرسی و حتی صدور قرار منع تعقیب مواجه شوند (کرمی‌پور و رجب زاده باغی، ۱۴۰۲ :۲۳۷).

ماده ۱۱۸ قانون آیین دادرسی کیفری که ملاک صلاحیت را محل کشف ادله می‌داند، پاسخگوی شرایط خاص فضای رمز ارزی نیست؛ چراکه در بسیاری از موارد، نه محل وقوع جرم قابل‌تعیین است و نه ادله فیزیکی وجود دارد. این وضعیت، موجب سردرگمی مراجع رسیدگی و سلب حق بزه‌دیدگان در پیگیری مؤثر می‌شود؛ درحالی‌که اصول ۳۴ و ۱۵۹ قانون اساسی بر حق دادخواهی در دادگاه صالح تأکید دارند.

برای رفع این خلأ، پیشنهاد می‌شود:

الف) ماده‌ای مستقل در قانون آیین دادرسی کیفری افزوده شود که معیارهایی مانند اقامتگاه بزه‌دیده، محل برداشت رمزارز، IP مبدأ یا مقصد، محل کشف کیف پول یا ادله دیجیتال را به‌عنوان محل وقوع جرم بپذیرد؛ ب) دادسرای تخصصی جرائم رمز ارزی با صلاحیت کشوری تأسیس شود، با حضور قضاتی آشنا به فناوری‌های دیجیتال؛ ج) اعمال صلاحیت فراسرزمینی درصورتی‌که بـزه‌دیده ایرانی باشد یا بخشی از جـرم در داخل کشور رخ دهد، بـا استناد به اصول حمایتی و شخصی حقوق بین‌الملل کیفری؛ د) تنظیم موافقت‌نامه‌های قضایی با کشورهایی که زیرساخت رمز ارزی فعال دارند، برای همکاری فرامرزی در تعقیب و استرداد مرتکبان.

این اقدامات با تمرکز بر حمایت فعال از بزه‌دیده، می‌تواند نظام قضایی را در برابر جرائم رمز ارزی توانمند ساخته و از اطاله و انفعال در روند دادرسی پیشگیری کند

۴-۳. راهکارهای تقنینی برای جبران خسارت و حمایت مؤثر از بزه‌دیدگان در مرحله پس از جرم

۴-۳-۱. لزوم تأسیس صندوق جبران خسارت برای بزه‌دیدگان جرائم رمز ارزی

در عدالت کیفری نوین، حمایت از بزه‌دیده صرفاً به مجازات مرتکب محدود نیست، بلکه شامل جبران خسارت و ترمیم آسیب نیز می‌شود. تأسیس صندوق جبران خسارت در جرائم رمز ارزی، از جمله سازوکارهای ترمیمی است که حتی در فرض ناشناس بودن یا ناتوانی مالی مجرم، حقوق بزه‌دیده را تأمین می‌نماید و نقش مهمی در ارتقای کارآمدی نظام کیفری ایفا می‌کند (حسینی، ۱۴۰۳: ۱۰۲).

الف) در وضعیت فعلی، به دلیل عدم شناسایی مرتکب، پیچیدگی فنی تراکنش‌ها و نبود نهاد حمایتی، اجرای احکام مالی در این حوزه اغلب با شکست مواجه می‌شود. این امر بزه‌دیدگان را از جبران خسارت محروم کرده و اعتماد عمومی به عدالت کیفری را تضعیف نموده است.

ب) پیشنهاد می‌شود با تصویب قانونی مستقل یا ذیل قانون جامع رمزارز، «صندوق جبران خسارت بزه‌دیدگان جرائم سایبری و رمز ارزی» تأسیس گردد. این صندوق می‌تواند تحت نظارت قوه قضائیه یا وزارت دادگستری، از منابع زیر تغذیه شود:

۱. بخشی از جرائم نقدی محکومان سایبری؛
۲. بودجه عمومی؛
۳. وجوه حاصل از ضبط رمزارزهای غیرقانونی؛
۴. مشارکت داوطلبانه پلتفرم‌ها و شرکت‌ها.

ج) فعالیت صندوق باید تحت نظارت هیئتی متشکل از نمایندگان دادستانی کل، بانک مرکزی، سازمان فناوری اطلاعات و سازمان بازرسی انجام شود. همچنین، امکان بازیافت مبالغ پرداختی در صورت شناسایی مرتکب، در قانون پیش‌بینی گردد.

چنین نهادی می‌تواند خلأ جدی در جبران خسارت بزه‌دیدگان را پر کرده و عدالت کیفری را به معنای واقعی، محقق سازد.

۴-۳-۲. تعیین مسئولیت قانونی ارائه‌دهندگان خدمات رمز ارزی در قبال بزه‌دیدگان

یکی از الزامات تقنینی در راستای حمایت کیفری از بزه‌دیدگان رمز ارزی، وضع مقررات صریح پیرامون مسئولیت قانونی ارائه‌دهندگان خدمات رمز ارزی، اعم از صرافی‌های دیجیتال، کیف پول‌های آنلاین، پلتفرم‌های معاملات غیرمتمرکز و ارائه‌دهندگان واسط انتقال دارایی‌های رمزنگاری‌شده است. در حال حاضر، بسیاری از این فعالان، به‌ویژه در بسترهای غیررسمی داخلی یا پلتفرم‌های خارجی بدون مجوز، بدون شفافیت در مقررات ناظر بر تعهدات کیفری و مدنی نسبت به کاربران، به فعالیت

مشغول‌اند. این وضعیت سبب شده در مواردی که جرائمی نظیر فیشینگ، جعل کلید خصوصی، سرقت رمز ارزی یا انتقال غیرمجاز دارایی‌ها از طریق این پلتفرم‌ها صورت می‌گیرد، بزه‌دیدگان راه مشخصی برای پیگیری مؤثر و مطالبه خسارت نداشته باشند (چراغی، ۱۴۰۲ :۱۹۵).

در همین راستا، ضروری است قانون‌گذار، ارائه‌دهندگان خدمات رمز ارزی را به‌عنوان بازیگران دارای مسئولیت قانونی در فرآیند مبارزه با جرائم رمز ارزی شناسایی کرده و مجموعه‌ای از الزامات مشخص را بر ایشان تحمیل کند. مهم‌ترین این الزامات، ایجاد سامانه‌های احراز هویت چندمرحله‌ای، ثبت سوابق تراکنش‌ها، همکاری با مراجع قضایی در تحلیل زنجیره تراکنش‌ها و اعلام موارد مشکوک به بزهکاری است. فقدان چنین الزامی، نه‌تنها روند شناسایی مرتکب را برای ضابطان و قضات دشوار می‌سازد، بلکه زمینه گسترش بسترهای بی‌هویت و آسیب‌پذیر را نیز فراهم می‌آورد.

بنابراین، پیشنهاد می‌شود قانونی مستقل یا فصلی مجزا در قوانین موجود، به‌صورت خاص به تعیین حدود مسئولیت کیفری و مدنی ارائه‌دهندگان خدمات رمز ارزی اختصاص یابد. در این مقررات باید الزام به احراز هویت کاربران، ثبت کامل و قابل بازیابی تراکنش‌ها، نگهداری امن کلیدهای خصوصی (در کیف پول‌های امانی) و همکاری با مراجع نظارتی و قضایی به‌روشنی پیش‌بینی شود. تنها در چنین شرایطی می‌توان از این نهادهای فنی، انتظار ایفای نقش مؤثر در تحقق عدالت کیفری و حمایت فعال از بزه‌دیدگان را داشت.

۴-۳-۳. تأسیس مرجع قضایی تخصصی برای رسیدگی به جرائم رمز ارزی: ضرورتی بنیادین در حمایت کیفری از بزه‌دیدگان

تحقق عدالت کیفری بزه‌دیده‌محور در گرو طراحی فرآیندهای تخصصی، منسجم و کارآمد در رسیدگی قضایی است. جرائم رمز ارزی به دلیل ویژگی‌هایی چون پیچیدگی فنی، ساختار غیرمتمرکز و فرامرزی، در چارچوب دادرسی‌های سنتی پاسخ مناسبی نمی‌یابند و همین امر منجر به حذف تدریجی بزه‌دیده از چرخه حمایت کیفری مؤثر شده است (کرمی‌پور و رجب زاده باغی، ۱۴۰۲: ۲۳۸). در وضعیت موجود، نظام قضایی ایران فاقد مرجع اختصاصی برای رسیدگی به این دسته از جرائم است و با آنکه برخی پرونده‌ها به دادسرای ویژه جرائم رایانه‌ای ارجاع می‌شوند، اما عدم شمول صلاحیتی جامع، فقدان آموزش تخصصی میان قضات و ضابط ، و پراکندگی در فرایند رسیدگی، بزه‌دیدگان را با اطاله دادرسی و سردرگمی مواجه می‌سازد. از این‌رو، پیشنهاد می‌شود با اصلاح قانون آیین دادرسی کیفری یا در قالب قانون خاص رمزارزها، نهادی با عنوان «شعبه تخصصی جرائم رمز ارزی» تأسیس گردد که کلیه جرائم مرتبط با رمزارزها، از جمله کلاهبرداری، جعل، پول‌شویی، اخاذی، استخراج غیرمجاز و فیشینگ رمز ارزی، در صلاحیت انحصاری آن قرار گیرد. قضات و ضابطان این مرجع باید آموزش‌های لازم در حوزه فناوری بلاک‌چین، رمزنگاری و تحلیل تراکنش‌ها را گذرانده باشند و بهره‌گیری از کارشناسان رسمی دادگستری در حوزه رمزارز، الزامی تلقی شود (چراغی، ۱۴۰۲ :۱۹۷).

همچنین طراحی سامانه‌ای الکترونیکی برای ثبت، پیگیری و توقیف دارایی‌های رمز ارزی با قابلیت تعامل با صرافی‌ها و بسترهای بین‌المللی ضروری است. مشارکت فعال بزه‌دیده از طریق مشاوره رایگان، دسترسی به اطلاعات پرونده و پیگیری هوشمند روند دادرسی باید در این ساختار پیش‌بینی شود. ایجاد چنین مرجعی، ضمن ارتقاء کارایی سیاست جنایی، اعتماد عمومی به‌نظام قضایی را افزایش داده و موجب بازگشت بزه‌دیده به جایگاه حقوقی فعال خود خواهد شد.

۵. نتیجه‌گیری

تحلیل ساختاری نظام عدالت کیفری ایران در مواجهه با جرائم مبتنی بر رمزارز، نشان‌دهنده ضعف بنیادی در پاسخ‌دهی به اشکال نوظهور بزه‌دیدگی فناورانه است. یافته‌های این پژوهش گویای آن است که سیاست جنایی ایران در قلمرو رمزارزها، فاقد جامعیت تقنینی، انسجام نهادی و کارآمدی اجرایی در تأمین حقوق بزه‌دیدگان است. در بُعد ماهوی، عدم جرم‌انگاری اختصاصی

برای رفتارهای مجرمانه خاص رمز ارزی نظیر جعل کلید خصوصی، فیشینگ بلاک‌چینی، سوءاستفاده از آسیب‌پذیری‌های فنی قراردادهای هوشمند و پول‌شویی در بسترهای غیرمتمرکز، موجب تزلزل در مبانی مسؤولیت کیفری و ممانعت از شناسایی رفتارهای قابل تعقیب شده است.

در سطح شکلی نیز خلأ در تعریف مفهومی و قانونی از «بزه‌دیده رمز ارزی»، فقدان مکانیزم‌های مؤثر در احراز هویت کیفری کاربران، ضعف در استنادپذیری ادله رمزنگاری‌شده و دشواری در تعیین صلاحیت قضایی، به حذف تدریجی بزه‌دیده از فرآیند عدالت کیفری انجامیده است. همچنین، غیبت نهادهای جبرانی و حمایتی تخصصی و عدم پیش‌بینی مسئولیت قانونی برای ارائه‌دهندگان خدمات رمز ارزی در قبال ارتکاب بزه یا امتناع از همکاری قضایی، نظام حمایت کیفری را در وضعیت انفعالی قرار داده است.

پیشنهادهای ارائه‌شده در این مقاله، با رویکرد بزه‌دیده‌محور و متکی بر اصول کارآمدی، تناسب و تخصص‌گرایی در سیاست جنایی، بر محورهایی چون جرم‌انگاری مستقل رمزارزمحور، تأسیس نهادهای جبرانی از جمله صندوق حمایت از بزه‌دیدگان، وضع الزام قانونی برای پلتفرم‌ها در ارائه داده و احراز هویت و طراحی مراجع قضایی با صلاحیت اختصاصی مبتنی بر فناوری بلاک‌چین متمرکز بوده است.

بر این اساس، تحقق حمایت کیفری مؤثر از بزه‌دیدگان جرائم رمز ارزی، مستلزم تدوین یک نظم حقوقی افتراقی است که با گسست از ساختارهای سنتی، بتواند با تکیه بر اصول حاکم بر جرم‌انگاری نوین و عدالت ترمیمی دیجیتال، کارآمدی نظام کیفری را در بستر اقتصاد رمزنگاری‌شده تضمین کند. بی‌تردید، تداوم وضعیت موجود، نه‌تنها موجب افزایش بزه‌دیدگی مضاعف و ناکارآمدی رویه قضایی خواهد شد، بلکه به بی‌اعتمادی عمومی نسبت به صلاحیت نظام عدالت کیفری در مدیریت مخاطرات نوپدید منجر می‌گردد.

ملاحظات اخلاقی

نویسندگان اصول اخلاقی را در انجام و انتشار این پژوهش علمی رعایت نموده‌اند و این موضوع مورد تأیید همه آنهاست.

تعارض منافع

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

حامی مالی

این مقاله حامی مالی ندارد.

سپاسگزاری

از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.

منابع

آذرنژاد، مهدی (۱۴۰۱). *حقوق دارایی‌های رمز نگاری شده (مبانی، مقدمات، قواعد، مقررات)*. تهران: مجد.

عباس پور ایکدر، نازنین؛ رمضانی، احمد و ملکی، محمدامین (۱۴۰۲). طراحی و اعتبار سنجی مدل مطلوب در برابر جرائم مخاطره‌آمیز مرتبط با رمز ارز در حقوق کیفری ایران. *مدیریت مخاطرات محیطی*، ۱۱(۱)، ۵۵-۴۳.

تاج‌الدینی، علی و مختاری افراکتی، نادر (۱۴۰۳). قانون‌گذاری در حوزه رمز ارزها در ایران، *ضرورت‌ها و پیشنهادها. رهیافت انقلاب اسلامی*، ۱۸(۶۶)، ۲۳-۴۲.

تاج لنگرودی، محمدحسن و دهدار، فرزین (۱۴۰۳). چالش‌های استفاده از رمز ارزها در نظام حقوقی جمهوری اسلامی ایران. *حقوق فناوری‌های نوین*، ۵(۹)، ۸۷-۱۰۶.

چراغی، محمدجواد (۱۴۰۲). کلاهبرداری به‌واسطه توکن سازی در رمز ارزها. *فصلنامه بین‌المللی قانون یار*، ۲۸، ۱۸۹-۲۰۸.

حسینی، سید علی (۱۴۰۳). *رمز ارزها (ماهیت حقوقی و صلاحیت در آیین دادرسی ایران)*. تهران: میراث فرهیختگان.

دالوندی، محمدرضا؛ موسوی، سید ابراهیم و غضنفری، هنگامه (۱۴۰۴). بررسی کارکردهای رمز ارزها از منظر حقوقی و نظم اجتماعی. *پژوهش‌های اخلاقی*، ۱۵(۳)، ۲۴۵-۲۶۷.

ربیع پور، علی‌اصغر و نوروزی، نیما (۱۴۰۰). *حقوق در عصر فناوری‌های پویا و غیرمتمرکز با نگاهی به رمز ارزها و فناوری بلاک چین*. تهران: گنجور.

زارع، محمدکاظم و امین نژاد، محمد صادق (۱۴۰۴). *جرائم رمز ارزها در پرتو رویه قضایی*. تهران: دوراندیشان.

زررخ، احسان (۱۳۸۹). بزه دیده شناسی سایبری. *مجلس و راهبرد*، ۶۴، ۱۲۷.

عمرانی فر، عدنان و بیرنگ، یگانه (۱۴۰۳). *جرم انگاری رمز ارزها در حقوق ایران*. تهران: گیتی قلم.

قاطعی، مهرداد (۱۴۰۳). رهیافت‌های فقهی خرید و فروش رمز ارزها. *پژوهشنامه مطالعات راهبردی علوم انسانی و اسلامی*، ۵(۶۴).

قوامی پور سرشکه، محدثه و محمودی، امیررضا (۱۴۰۲). *جرم انگاری حوزه کسب و کار ارز دیجیتال در اسناد بین‌المللی*. کرج: انتشارات جهان سیاست.

کرمی‌پور، مصطفی و رجب زاده باغی، مونا (۱۴۰۲). نقش سیاست کیفری ایران در مدیریت رمز ارزها. *تمدن حقوقی*، ۱۶(۱۵)، ۲۲۵-۲۴۰.

محمدی، امیرحسین؛ میرزایی، فرهاد و صعیدی، یاسین (۱۴۰۳). سیاست جنایی حاکم بر رمز ارزها با چشم‌انداز به‌نظام حقوق کیفری اقتصادی. تحولات سیاست اجتماعی معاصر ایران، ۳(۱)، ۲۴۴-۲۵۸.

رحمان‌زاده، زهرا؛ محمودی، اصغر و ابافت، رسول (۱۴۰۲). بررسی ماهیت و آثار حقوقی رمز ارزها در نظام حقوقی ایران. *مطالعات حقوق*، دوره جدید (۳۲)، ۸۴۳-۸۶۰.

میرزاخانی، رضا و دعائی، میثم (۱۴۰۲). راهکارها و چالش‌های استفاده از رمز ارزها در بازار سرمایه نگرش فقهی حقوقی. *نشریه اقتصاد و بانکداری اسلامی*، ۱۲(۴۵)، ۷-۲۸.

References

Abbas Pour-Ikdar, N., Ramezani, A., & Maleki, M.A. (2023). Design and validation of the optimal model against risky crimes related to cryptocurrency in Iranian criminal law. *Environmental Risk Management*, 11(1), 43-55. (In Persian)

Azarnejad, M. (2022). *Crypto Asset Law (Basics, Prerequisites, Rules, Regulations)*. Tehran: Majd. (In Persian)

Babak, M., Haji Mollamirzaei, H., & Najafi Jazeh, H. (2024). Dimensions of the Cryptocurrency Policy-Making Pattern in the Islamic Republic of Iran. *Interdisciplinary Studies in Strategic Knowledge*, 14(56), 223-245. (In Persian)

Cheraghi, M.J. (2023). Cryptocurrency tokenization fraud. *Qanon Yar Magazine*, 28, 189-208. (In Persian)

Dalvandi, M.R., Mousoui, S.E., & Ghazanfari, H. (2025). Examining the functions of cryptocurrencies from a legal and social order perspective. *Ethics and Islamic Education*, 15(3), 245-267. (In Persian)

Ghatei, M. (2024). Jurisprudential approaches to buying and selling cryptocurrencies. *Journal of Strategic Studies in Humanities and Islamic Sciences*, 5(64). (In Persian)

Ghavamipour Sarsheke, M., & Mahmoudi, A.R. (2023). Book on the Criminalization of the Digital Currency Business in International Documents, Karaj: World Politics Publications. (In Persian)

Hoseini, S.A. (2024). *Cryptocurrencies (Legal Nature and Jurisdiction in Iranian Procedure)*. Tehran: Heritage of the Educated. (In Persian)

Karami Pour, M., & Rajabzade Baghi, M. (2023). The Role of Iran's Criminal Policy in the Management of Cryptocurrencies. *Fares Law Research*, 6(15), 225-240. Doi: 10.22034/lc.2023.401114.1356. (In Persian)

Mirzakhani, R., Doaei, M. (2023). Solutions and challenges of using crypto-currencies in the capital market: jurisprudential-legal perspective. *Journal of Islamic Economics and Banking*, 12(45), 7-28. (In Persian)

Mohammadi, A.H., Mirzaei, F., & Saeidi, Y. (2024). Legislative criminal policy governing the codes of conduct with a perspective on the economic criminal law system. *Contemporary Socio-Political Developments in Iran*, 3(1), 244-258. Doi: 10.30510/pscci.2024.490077.1139. (In Persian)

Omranifar, A., & Birang, Y. (2024). *Criminalization of cryptocurrencies in Iranian law*. Tehran: Giti Qalam. (In Persian)

Rabipour, A.A., & Norouzi, N. (2022). *Law in the era of dynamic and decentralized technologies with a look at cryptocurrencies and blockchain technology*. Tehran: Ganjur. (In Persian)

RahmanzadehE, Z., Mahmoudi, A., & Abafat, R. (2023). Examining the nature and legal effects of cryptocurrencies in the Iranian legal system. *Journal of Legal Studies*, 3(320, 843-860. (In Persian)

Taj Aldini, A., & Mokhtari Afrakti, N. (2024). Legislation in the field of cryptocurrencies in Iran: necessities and suggestions. *The Islamic Revolution Approach*, 18(66), 23-42. (In Persian)

Taj Langerudi, M.H., & Dehdar, F. (2024). The challenges of using cryptocurrencies in the legal system of Islamic Republic of Iran. *ModernTechnologies Law*, 5(9), 87-106. Doi: 10.22133/mtlj.2023.401446.1216. (In Persian)

Zare, M.K., & Aminnejad, M.S. (2025). *Cryptocurrency Crimes in the Light of Judicial Practice*. Tehran: Doorandishann. (In Persian)

Zarrokh, E. (2010). Cyber victimology. *Majles and Strategy Magazine*, 64, 127. (In Persian)