Extended Abstract

١. Title

An Impact Analysis of the "Lā Ḍarar" Rule in Cryptocurrency Transactions

٢. Author

Javad Soltani-Fard; Assistant Professor, Department of Fiqh and Private Law, Shahid Motahari University (RA), Tehran, Iran.

٣. Short Abstract

The "Lā Ḍarar" rule is one of the most important legal maxims in the Islamic legal system which, based on the Prophetic hadith "lā ḍarar wa lā ḍirār," prohibits any form of infliction of harm, including financial harm. When confronted with emerging economic phenomena such as cryptocurrencies, this rule acquires a new and noteworthy function. Adopting an analytical-descriptive approach, the present article examines the most significant challenges of cryptocurrency transactions—including extreme price volatility, market manipulation (pump and dump), organized fraudulent schemes, risks arising from sanctions, and losses resulting from user error—and classifies them into three general levels: behavioral harms, structural deficiencies, and user errors, assessing them on the basis of the "Lā Ḍarar" rule. The central research question is whether activity in the cryptocurrency market can constitute the infliction of harm upon contracting parties, society, and even the trader himself, and consequently be subject to Sharīʿa-based prohibition or restriction, or not.

The findings of the study indicate that the relationship between the risks in this field and the "Lā Ḍarar" rule is not uniform: behaviors such as market manipulation and fraudulent schemes, due to their direct infliction of harm upon others, fall more clearly within the scope of the rule's prohibition; by contrast, some harms, such as extreme price volatility or structural market risks, are less the product of harmful conduct by individuals and more attributable to the structural features of this space, and their juristic evaluation requires more precise considerations. Accordingly, the fiqh-based engagement with cryptocurrencies can be articulated neither as an absolute rejection nor as unconditional acceptance; rather, the function of the "Lā Ḍarar" rule in this domain is more properly explicable in terms of guiding appropriate regulation, strengthening oversight, and enhancing user awareness and prudence to reduce the grounds for harm. Nevertheless, until the aforementioned challenges are resolved, one cannot definitively claim that the "Lā Ḍarar" rule does not apply to cryptocurrency transactions.

٤. Keywords

"Lā Ḍarar rule," "negation of harm," "prohibition of inflicting harm," "transactions," "cryptocurrency," "coin"

٥. Introduction and Statement of the Problem

The "Lā Ḍarar" rule is one of the most fundamental rules of Islamic fiqh, which has been applied across a wide range of chapters in acts of worship and transactions and has acquired a pivotal status in both Imāmī and Sunnī jurisprudence. At the same time, the precise elucidation of the content of this rule and the scope of its application has consistently been a subject of debate and disagreement. In the contemporary world, the emergence of novel financial phenomena such as cryptocurrencies has posed the issue of "harm" on a new horizon and scale. Cryptocurrency transactions—due to extreme price volatility, the possibility of market manipulation, the spread of organized fraudulent schemes, risks stemming from sanctions and cross-border restrictions, as well as irreparable user errors—have created a highly risky environment for small investors and ordinary users; and this in a setting that is often devoid of centralized supervisory institutions and traditional legal protections. From the perspective of transactional fiqh, this situation poses a strategic question to the researcher: can cryptocurrency transactions, by virtue of their high-risk and harm-inducing nature, fall under the heading of "harm" and, pursuant to the "Lā Ḍarar" rule, be subject to a change or restriction in their legal ruling? And if the answer is affirmative, at what level and according to what logic and criteria should this change and restriction be implemented?

In the existing literature, most studies have either focused on the juristic and legal assessment of the process of cryptocurrency mining, or have separately addressed certain dimensions of risk and fraud in this market; however, a coherent analysis that employs the "Lā Ḍarar" rule as a systematic framework for distinguishing between different levels of harm and for determining its function in the regulation of cryptocurrency transactions is rarely encountered. The innovation of this study lies in the fact that, on the one hand, at the theoretical level, by critiquing the well-known view of the negation of harmful rulings and reinforcing the reading of the rule as a "prohibitory injunction against inflicting harm," it offers a clearer understanding of the "Lā Ḍarar" rule and, alongside the prohibition of harming others, re-examines its possible scope of application to self-harm; and, on the other hand, at the practical level, by articulating a three-layered typology of risks (fraudulent and harmful behaviors, structural and contextual deficiencies,

and user error), it makes possible a more precise relational assessment between the various types of cryptocurrency risks and the purport of the "Lā Ḍarar" rule. The research method is analytical-argumentative and is based on library study of fiqh and uṣūl sources, together with the use of reports and descriptive data regarding the risks of the cryptocurrency market.

٦. Research Findings

The findings of the study can be summarized on two levels: theoretical and practical. At the first level, a fiqh-uṣūl analysis of the hadith "lā ḍarar wa lā ḍirār" shows that interpreting the rule as "negation of the enactment of harmful rulings" faces serious linguistic and uṣūl-based difficulties. In contrast, construing the rule as a "prohibitory injunction against inflicting harm" enjoys stronger support and appears more consistent with the numerous instances in which the informative mode (khabar) is used for prescriptive purposes (inshāʾ) in the Qurʾān and the Sunna. On this basis, the purport of the "Lā Ḍarar" rule is not the negation of harmful rulings, but rather the prohibition of the realization of conduct involving harm to others (and, according to one view, harm to oneself); conduct that can be relevant both within the framework of private relations between individuals and at the level of macro-economic structures and policy-making.

At the practical level, the application of this foundation to cryptocurrency transactions shows that the risks in this field cannot be reduced in an undifferentiated way to a single generic heading of "harm." The findings of the research indicate that at least three distinct categories of risks can be identified: first, fraudulent and deceptive behaviors such as Ponzi schemes, pump-and-dump operations, and various types of organized scams, which directly entail unjust transfer of wealth and harm to small investors and constitute a clear instance of the prohibition enshrined in the "Lā Ḍarar" rule. Second, structural deficiencies and contextual conditions of the market, such as extreme price volatility, weak transparency, lack of effective oversight, and risks arising from sanctions and cross-border restrictions, which generally occur without any direct intention to inflict harm on the part of the contracting parties and whose source lies at the level of market design and policy-making. Third, harms arising from user error, such as sending to an incorrect address, losing a private key, or unknowingly entering into severe risks, which in principle do not count as harming others, but from the standpoint of certain doctrinal bases, can be included within the ambit of self-harm and negligence in the preservation of property.

On the basis of this typology, the key finding of the study is that, with respect to the first category, the "Lā Ḍarar" rule clearly serves as the basis for the declaratory prohibition (ḥurmat taklīfiyya) of such behaviors; with respect to the second category, it functions more as a foundation obliging the state and regulatory authorities to reform structures and enact protective rules; and with respect to the third category, it underscores the necessity of elevating user awareness and adopting rational precautionary measures.

٧. Conclusion

The overall conclusion of the study indicates that, although the "Lā Ḍarar" rule, as one of the central rules of Islamic fiqh, plays a decisive role in the Sharīʿa-based assessment of risks associated with cryptocurrency transactions, it does not, by itself, provide a basis for issuing a blanket ruling of prohibition regarding all types of such transactions. The three-level analysis of risks shows that what lies at the core of the rule's prohibition are fraudulent, deceptive, and harmful behaviors that manifest in the form of organized scams and market manipulation and must be explicitly prohibited within the legal system. By contrast, a significant segment of structural risks and user errors must be managed at the level of regulation, institutional design, public education, and strengthening rational precaution. On this basis, the strategic function of the "Lā Ḍarar" rule in the realm of cryptocurrencies is manifested less in a "general ban" and more in providing a normative framework for "multi-layered policy-making": a framework that, on the one hand, calls upon the state and regulatory bodies to enact protective regulations, enhance transparency, and oversee platforms, and, on the other hand, highlights users' responsibility to observe precaution and avoid high-risk behaviors. This conclusion opens up a new horizon for dialogue between fiqh and financial regulation in confronting modern technologies.

٨. Selected References

The Holy Qurʾān

Ansari, Morteza (١٣٧٧ [١٩٩٨/٩٩]). Farāʾid al-Uṣūl. Qom: Majmaʿ al-Fikr al-Islāmī.

Taftazani, Masʿud (n.d.). Mukhtaṣar al-Maʿānī. N.p.: Dār al-Fikr.

Hosseini-Maraghi, Seyyed Abd al-Fattah (١٤١٧ AH). al-ʿAnāwīn al-Fiqhiyya. Qom: Muʾassasat al-Nashr al-Islāmī al-Tābiʿa li-Jamāʿat al-Mudarrisīn.

Khuʾi, Seyyed Abul-Qasem (١٣٦٨ [١٩٨٩/٩٠]). Muḥāḍarāt fī Uṣūl al-Fiqh. Qom: Ansariyan.

Taftazani, Masʿud (n.d.). Mukhtaṣar al-Maʿānī. N.p.: Dār al-Fikr.

Shariʿat-Esfahani, Fathollah (n.d.). Qāʿidat Lā Ḍarar. Qom: Muʾassasat al-Nashr al-Islāmī al-Tābiʿa li-Jamāʿat al-Mudarrisīn.
Tusi, Mohammad b. Hasan (n.d.). al-Khilāf. Qom: Muʾassasat al-Nashr al-Islāmī al-Tābiʿa li-Jamāʿat al-Mudarrisīn.
Iraqi, Ḍiyāʾ al-Din (١٤١٨ AH). Qāʿidat Lā Ḍarar wa Lā Ḍirār. Qom: Maktab al-Iʿlām al-Islāmī.
Gharavi-Naʾini, Mohammad Hossein (١٣٧٣ AH). Munyat al-Ṭālib fī Ḥāshiyat al-Makāsib. Reported by Najafi-Khwansari. Tehran: al-Maktaba al-Mohammadiyya.
Mousavi-Bejnordi, Seyyed Hassan (١٣٧٧ [١٩٩٨/٩٩]). al-Qawāʿid al-Fiqhiyya. Qom: al-Hadi.
Mousavi-Khomeini, Seyyed Rouhollah (١٤٢٣ AH). Tahdhīb al-Uṣūl. Reported by Sobhani-Tabrizi. N.p.: Muʾassasat Tanzim wa Nashr Āthār al-Imam al-Khomeini (RA).
Najafi, Mohammad Hasan (١٣٦٢ [١٩٨٣/٨٤]). Jawāhir al-Kalām fī Sharḥ Sharāʾiʿ al-Islām. Beirut: Dār Iḥyāʾ al-Turāth al-ʿArabī.
Naraqi, Ahmad (١٤١٧ AH). ʿAwāʾid al-Ayyām fī Bayān Qawāʿid al-Aḥkām wa Muhimāt Masāʾil al-Ḥalāl wa al-Ḥarām. Qom: Daftar Tablīghāt Islāmī-ye Ḥawza-ye ʿIlmiyya-ye Qom.

۱. عنوان

تأثیرشناسی قاعده «لاضرر» در معاملات رمزارزها

۲. نویسنده

جواد سلطانی‌فرد؛ استادیار گروه فقه و حقوق خصوصی دانشگاه شهید مطهری(ره)، تهران، ایران

۳. چکیده مختصر

قاعده «لاضرر» از مهم‌ترین قواعد فقهی در نظام حقوق اسلامی است که با استناد به حدیث نبوی «لاضرر و لاضرار»، از هرگونه زیان‌رسانی، از جمله زیان‌های مالی، نهی می‌کند. این قاعده در مواجهه با پدیده‌های نوظهور اقتصادی همچون رمزارزها، کارکردی تازه و قابل‌توجه می‌یابد. مقاله حاضر با رویکردی تحلیلی-توصیفی، مهم‌ترین چالش‌های معاملات رمزارزها -از جمله نوسانات شدید قیمت، دستکاری بازار (پامپ و دامپ)، طرح‌های کلاهبرداری سازمان‌یافته، ریسک‌های ناشی از تحریم و نیز زیان‌های ناشی از خطای کاربر- را بررسی کرده و آن‌ها را در سه سطح کلی آسیب‌های رفتاری، نارسایی‌های ساختاری و خطاهای کاربری طبقه‌بندی و بر پایه قاعده لاضرر ارزیابی می‌کند. پرسش محوری پژوهش آن است که آیا فعالیت در بازار رمزارزها می‌تواند مصداق ورود ضرر به طرف‌های معامله، جامعه و حتی خود شخص معامله‌گر باشد و در نتیجه مشمول منع یا محدودیت شرعی قرار گیرد یا خیر؟

یافته‌های پژوهش نشان می‌دهد که نسبت مخاطرات این حوزه با قاعده لاضرر یکسان نیست: رفتارهایی مانند دستکاری بازار و طرح‌های کلاهبرداری، به دلیل زیان‌رسانی مستقیم به دیگران، آشکارتر در قلمرو منع این قاعده قرار می‌گیرند؛ در مقابل، بخشی از زیان‌ها مانند نوسانات شدید قیمت یا ریسک‌های ساختاری بازار، بیش از آنکه ناشی از رفتار زیان‌بار اشخاص باشند، به ویژگی‌های ساختاری این فضا بازمی‌گردند و ارزیابی فقهی آن‌ها نیازمند ملاحظات دقیق‌تری است. از این رو، مواجهه فقهی با رمزارزها نه در قالب ردّ مطلق و نه پذیرش بی‌قیدوشرط قابل تبیین است؛ بلکه کارکرد قاعده لاضرر در این حوزه بیشتر در جهت‌دهی به تنظیم‌گری مناسب، تقویت نظارت و ارتقای آگاهی و احتیاط کاربران برای کاهش زمینه‌های ورود ضرر قابل‌تبیین است. با این همه، تا زمان رفع چالش‌های یادشده، نمی‌توان با قطعیت از عدم شمول قاعده لاضرر نسبت به معاملات رمزارزها سخن گفت.

٤. کلمات کلیدی

"قاعده لاضرر"، "نفی ضرر"، "نهی از آسیب‌رسانی"، "معاملات"، "رمزارز"، "کوین"

۵. مقدمه و بیان مسأله

قاعده «لاضرر» از بنیادی‌ترین قواعد فقه اسلامی است که در گستره‌ای وسیع از ابواب عبادات و معاملات به‌کار گرفته شده و در فقه امامیه و اهل‌تسنن جایگاهی محوری یافته است. در عین حال، تبیین دقیق مفاد این قاعده و قلمرو کاربرد آن، همواره محل بحث و اختلاف‌نظر بوده است. در جهان معاصر، ظهور پدیده‌های نوین مالی مانند رمزارزها، مسأله «ضرر» را در افق و مقیاسی تازه مطرح کرده است. معاملات رمزارزها به‌دلیل نوسانات شدید قیمت، امکان دستکاری بازار، گسترش طرح‌های کلاهبرداری سازمان‌یافته، ریسک‌های ناشی از تحریم و محدودیت‌های برون‌مرزی و نیز خطاهای کاربری جبران‌ناپذیر، محیطی مملو از مخاطره برای سرمایه‌گذاران خرد و کاربران عادی ایجاد کرده‌اند؛ آن‌هم در بستری که غالباً از نهاد ناظر متمرکز و حمایت‌های حقوقی سنتی بی‌بهره است. این وضعیت، از منظر فقه معاملات، پرسشی راهبردی را پیش روی پژوهشگر قرار می‌دهد که آیا معاملات رمزارزها، به‌سبب ماهیت پرریسک و زمینه‌ساز ضرر، می‌تواند مشمول عنوان «ضرر» گردد و به‌موجب قاعده لاضرر، حکم آن‌ها تغییر یابد یا محدود شود؟ و اگر پاسخ مثبت است، این تغییر و تحدید در چه سطح و با چه منطق و معیاری باید اعمال گردد؟

در ادبیات موجود، غالب پژوهش‌ها یا بر ارزیابی ماهیت فقهی و حقوقی فرایند استخراج رمزارزها متمرکز بوده‌اند، یا به صورت مجزا به برخی ابعاد ریسک و کلاهبرداری در این بازار پرداخته‌اند؛ اما تحلیل منسجمی که قاعده لاضرر را به‌عنوان چارچوبی نظام‌مند برای تفکیک سطوح متفاوت ضرر و تعیین کارکرد آن در تنظیم‌گری معاملات رمزارزها به‌کار گیرد، کمتر دیده می‌شود. نوآوری این پژوهش در آن است که از یک سو، در سطح نظری، با نقد دیدگاه مشهور نفی حکم ضرری و تقویت قرائت «نهی تحریمی از آسیب‌رسانی»، فهم روشن‌تری از قاعده لاضرر به دست می‌دهد و در کنار منع از ضرر زدن به غیر، دامنه احتمالی شمول آن نسبت به ضرر به خود را نیز بازخوانی می‌کند؛ و از سوی دیگر، در سطح کاربردی، با صورت‌بندی سه‌لایه‌ای مخاطرات (رفتارهای متقلبانه و آسیب‌زا، نارسایی‌های ساختاری و شرایط پیرامونی، و خطای کاربر)، امکان نسبت‌سنجی دقیق‌تر میان انواع ریسک‌های رمزارزی و مفاد قاعده لاضرر را فراهم می‌آورد. روش پژوهش، تحلیلی-استدلالی و مبتنی بر مطالعه کتابخانه‌ای منابع فقهی و اصولی، همراه با بهره‌گیری از گزارش‌ها و داده‌های توصیفی درباره مخاطرات بازار رمزارزها است.

۶. یافته‌های پژوهش

یافته‌های پژوهش در دو سطح نظری و کاربردی قابل جمع‌بندی است. در سطح نخست، تحلیل فقهی-اصولی حدیث «لا ضرر و لا ضرار» نشان می‌دهد که تفسیر قاعده به‌عنوان «نفی تشریع حکم ضرری» با دشواری‌های ادبی و اصولی جدی مواجه است. در مقابل، قرائت قاعده به‌مثابه «نهی تحریمی از آسیب‌رسانی» از پشتوانه قوی‌تری برخوردار است و با نمونه‌های متعددی از کاربرد اسلوب خبر در مقام انشاء در قرآن و سنت سازگارتر می‌نماید. بر این اساس، مفاد قاعده لاضرر، نه نفی حکم ضرری، بلکه نهی از تحقق رفتارهای متضمن ضرر به غیر (و بنا بر یک دیدگاه، ضرر به خود) است؛ رفتاری که هم می‌تواند در قالب روابط خصوصی میان اشخاص و هم در سطح ساختارهای کلان اقتصادی و سیاست‌گذاری موضوعیت یابد.

در سطح کاربردی، تطبیق این مبنا بر معاملات رمزارزها نشان می‌دهد که مخاطرات این حوزه را نمی‌توان به صورت یکپارچه و در قالب یک عنوان کلی «ضرر» فروکاست. یافته‌های پژوهش حکایت از آن دارد که می‌توان دست‌کم سه دسته متمایز از مخاطرات را شناسایی کرد: نخست، رفتارهای متقلبانه و فریبکارانه مانند طرح‌های پانزی، عملیات پامپ و دامپ و انواع کلاهبرداری‌های سازمان‌یافته که به‌طور مستقیم متضمن انتقال ناعادلانه ثروت و آسیب‌رسانی به سرمایه‌گذاران خرد هستند و مصداق روشن نهی قاعده لاضرر به شمار می‌آیند. دوم، نارسایی‌های ساختاری و شرایط پیرامونی بازار، از قبیل نوسانات شدید قیمت، ضعف شفافیت، خلأ نظارت مؤثر و ریسک‌های ناشی از تحریم و محدودیت‌های برون‌مرزی که غالباً بدون قصد آسیب‌رسانی مستقیم از سوی متعاملین رخ می‌دهد و منشأ آن در سطح طراحی بازار و سیاست‌گذاری است. سوم، ضررهای ناشی از خطای کاربر، مانند ارسال به آدرس نادرست، از دست دادن کلید خصوصی یا ورود ناآگاهانه به ریسک‌های شدید، که در اصل، آسیب‌رسانی به غیر محسوب نمی‌شوند، اما از منظر برخی مبانی، می‌توانند در قلمرو ضرر به خود و تقصیر در حفظ مال قرار گیرند.

بر پایه این صورت‌بندی، یافته کلیدی پژوهش آن است که قاعده لاضرر در قبال دسته نخست، به‌روشنی مستند حرمت تکلیفی این رفتارها به شمار می‌آید؛ در قبال دسته دوم، بیشتر به‌مثابه مبنایی برای الزام دولت و نهادهای ناظر به اصلاح ساختارها و وضع قواعد صیانتی عمل می‌کند؛ و در قبال دسته سوم، بر لزوم ارتقای سطح آگاهی کاربران و اتخاذ تدابیر احتیاطی عقلایی تأکید دارد.

۷. نتیجه‌گیری

نتیجه کلی پژوهش نشان می‌دهد که قاعده لا ضرر، به‌عنوان یکی از قواعد محوری در فقه اسلامی، هرچند نقش تعیین‌کننده‌ای در ارزیابی شرعی مخاطرات مرتبط با معاملات رمزارزها دارد، اما به‌خودی‌خود مبنایی برای صدور حکم حرمت نسبت به همه انواع این معاملات نیست. تحلیل سه‌سطحی مخاطرات نشان می‌دهد که آنچه در قلب نهی قاعده قرار می‌گیرد، رفتارهای متقلبانه، فریبکارانه و زیان‌بار است که در قالب کلاهبرداری‌های سازمان‌یافته و دستکاری بازار نمود می‌یابد و باید به‌طور صریح در نظام حقوقی مورد منع قرار گیرد. در مقابل، بخش مهمی از ریسک‌های ساختاری و خطاهای کاربری را باید در سطح تنظیم‌گری، طراحی نهادی، آموزش عمومی و تقویت احتیاط عقلایی مدیریت کرد. بر این اساس، کارکرد راهبردی قاعده لاضرر در حوزه رمزارزها بیش از آنکه در «منع کلی» متجلی شود، در ارائه چارچوبی هنجاری برای «سیاست‌گذاری چندلایه» است: چارچوبی که از یک سو، دولت و نهادهای ناظر را به تدوین مقررات صیانتی، ارتقای شفافیت و نظارت بر پلتفرم‌ها فرا می‌خواند و از سوی دیگر، مسئولیت کاربران را در رعایت احتیاط و پرهیز از رفتارهای پرخطر برجسته می سازد. این نتیجه، افق تازه‌ای برای گفت‌وگو میان فقه و تنظیم‌گری مالی در مواجهه با فناوری‌های نوین می‌گشاید.

۸. گزیده منابع

قرآن کریم

انصاری، مرتضی (۱۳۷۷). فرائد الأصول. قم: مجمع الفکر الإسلامی.

تفتازانی، مسعود (بی‌تا). مختصر المعانی. بی‌جا: دار الفکر.

حسینی‌مراغی، سیدعبدالفتاح (۱٤۱۷ق). العناوین الفقهیة. قم: مؤسسة النشر الإسلامی التابعة لجماعة المدرسین.

خویی، سیدابوالقاسم (۱۳٦۸). محاضرات فی أصول الفقه. قم: انصاریان. تفتازانی، مسعود (بی‌تا). مختصر المعانی. بی‌جا: دار الفکر.

شریعت‌اصفهانی، فتح‌اللّه (بی‌تا). قاعدة لاضرر. قم: مؤسسة النشر الاسلامی التابعة لجماعة المدرسین.

طوسی، محمدبن‌حسن (بی‌تا). الخلاف. قم: مؤسسة النشر الإسلامی التابعة لجماعة المدرسین.

عراقی، ضیاءالدین (۱٤۱۸ق). قاعدة لاضرر و لاضرار. قم: مکتب الإعلام الإسلامی.

غروی‌نایینی، محمدحسین (۱۳۷۳ق). منیة الطالب فی حاشیة المکاسب. تقریر نجفی‌خوانساری. تهران: المکتبة المحمدیة.

موسوی‌بجنوردی، سیدحسن (۱۳۷۷). القواعد الفقهیة. قم: الهادی.

موسوی‌خمینی، سیدروح‌اللّه (۱٤۲۳ق). تهذیب الأصول. تقریر سبحانی‌تبریزی. بی‌جا: مؤسسة تنظیم و نشر آثار الإمام الخمینی(ره).

نجفی، محمدحسن (۱۳٦۲). جواهر الکلام فی شرح شرائع الإسلام. بیروت: دار إحیاء التراث العربی.

نراقی، احمد (۱٤۱۷ق). عوائد الأیام فی بیان قواعد الأحکام و مهمات مسائل الحلال و الحرام. قم: دفتر تبلیغات اسلامی حوزه علمیه قم.

۱. بیان مسأله

یکی از مشهورترین و بنیادی‌ترین قواعد فقهی، قاعده «نفی‌ضرر» یا همان «لاضرر» است که از حدیث مشهور نبوی «لاضرر و لاضرار» (کلینی، ۱٤۰۷، ج۵، صص۲۹۲و ۲۹۳) گرفته شده و در باب مفاد آن دیدگاه‌های متفاوتی مطرح شده است. این قاعده در بیشتر ابواب فقه اعم از عبادات و معاملات به کار می رود؛ مانند نفی وجوب وضو اگر انجام دادنش موجب ضرر شود و نفی حرمت تراشیدن ریش

اگر انجام ندادنش ضـــرر داشـــته باشـــد (ایروانی، ۱٤۳۲، ج۱، ص۸۷). نمونه دیگر، نفی لزوم بیع مشـــتمل بر غبن اســـت که در باب معاملات، بر اساس همین قاعده تحلیل می‌شود. شیخ طوسی در مبحث خیار غبن می نویسد:

«دلیلُنا ما رُوِیَ عن النبی(صلّی اللّه علیه و آله) أنه قال: لاضرر و لاضرار.» (طوسی، بی‌تا، ج۳، ص٤۲)

اهمیت این قاعده تا آنجاست که برخی از معاصران آن را تنها مستند برای بسیاری از مسائل فقهی دانسته و نوشته‌اند:

«هی مدرک الوحید لکثیر من المسائل.» (مکارم‌شیرازی، ۱۳۷۰، ج۱، ص۲۸)

شـهید اول این قاعده را جزو قواعد پنجگانه‌ای ذکر کرده اسـت که امکان دارد احکام شـرعی به آنها بازگردد (شـهیداول، ۱٤۰۰ق، ج ۱، صص۷٤ و ۱٤۰)؛ آنچنانکه برخی از دانشمندان اهل‌تسنن نیز گفته‌اند:

«فقه دائر مدار پنج حدیث اسـت، یکی از آنها حدیث لاضـرر و لاضـرار اسـت.» (نک: سـیوطی، ۱۳۸۹ق، ج۲، ص۱۲۲)

بر همین اسـاس، این قاعده از دیرباز مورد توجه و تدقیق فقها قرار گرفته و دیدگاه‌های متفاوتی در باب تبیین مفاد، دامنه شـمول و شـروط جریان آن شکل گرفته است. بسیاری از فقها در ادوار مختلف، در تألیفات و تقریرات خود رساله‌ای مستقل به آن اختصاص داده‌اند. ظاهراً شهید اول در کتاب القواعد و الفوائد نخ ستین فقیه امامی ا ست که قاعده لا ضرر را به صورت م ستقل و با عنوان «قاعدة الـ ضرر المنفیّ» مورد بحث قرار داده است (شهیداول، ۱٤۰۰ق، ج۱، ص۱٤۰).[1]

در دوره معاصر، با گسترش پدیده‌های نوین اقتصادی و فناوری‌های مالی، عرصه‌های تازه‌ای برای کاربست این قاعده بنیادین پدید آمده است. یکی از مهم‌ترین این پدیده‌ها، «رمزارزها» است که به عنوان یکی از پرچالش‌ترین نوآوری‌های مالی، توجه فقیهان و قانون‌گذاران اســلامی را به پرســش‌های اســاســی درباره مشــروعیت فعالیت‌های مرتبط با آن جلب کرده اســت. در میان ابعاد گوناگون این پدیده، «معاملات رمزارزها» جایگاهی ویژه دارد؛ زیرا بخش عمده‌ای از مواجهه عمومی با رمزارزها در همین بستر رخ می‌دهد. نوسانات شدید قیمت، دستکاری بازار، کلاهبرداری‌های سازمان‌یافته، مسدود شدن حساب‌ها بر اثر محدودیت‌های بین‌المللی و از دست رفتن دارایی به سبب خطای کاربر، در کنار نبودِ نهاد ناظر متمرکز از جمله عواملی است که این معاملات را مستعد ایجاد ضررهای مالی قابل توجه و گاه پیامدهای فردی و اجتماعی کرده و زمینه طرح این پر سش فقهی را فراهم می سازد که: آیا دادو ستد رمزارزها می‌تواند م شمول عنوان « ضرر» شده و به موجب قاعده لا ضرر، حکم آن تغییر یابد یا محدود گردد؟ این پر سش به ویژه با توجه به دیدگاهی که قاعده لا ضرر را ناظر به منع وارد ساختن هرگونه زیان و آسیب به فرد یا جامعه می‌داند[2]، ابعاد مهمی می‌یابد.

---

۱. برخی بر این باورند که سنت نگارش تک‌نگاری درباره این قاعده برای نخ ستین‌بار در قرن دوازدهم هجری در میان علمای شیعه شکل گرفت و آغاز آن با ر ساله‌ای از شیخ عبداللّه سماهیجی با عنوان الرسالة السلمانیة فی مسألة لاضرر و لاضرار بوده است (غفوری‌نژاد، ۱۳۹۹، ص۷۰).

۲. تعدادی از فقها واژه «ضـــرر» را به هرگونه نقص و کاســـتی در «مال»، «بدن» یا «آبرو» تعریف کرده‌اند (غروی‌اصـــفهانی، ۱٤۱٤ق، ج٤، ص٤۳٦؛ خویی، ۱٤۱۳ق، ج۱، ص٦۰٦؛ نک: ایروانی، ۱٤۳۲ق، ج۱، ص۱۱۲). با این حال، به نظر می‌ر سد دایره مفهوم ضرر مختص به این سه مورد نبا شد؛ بلکه به طور کلی هر امری که موجب از د ست رفتن یا کاهش یکی از منافع و مواهب متعارف زندگی انسان گردد، در قلمرو آن قرار می‌گیرد، خواه در مال باشد یا در جان، آبرو و مانند آن (مکارم‌شیرازی، ۱۳۷۰، ج۱، ص٥٥). از همین رو، برخی فقها آن را شامل هرگونه تعدّی به حقوق دیگران (همانند ماجرای سمرةبن‌جندُب) نیز دانسته‌اند (نک: عراقی، ۱٤۱۱ق، ج٤، ص۳۳۹؛ خویی، ۱٤۱۷ق، ج۳، ص٥۳۲).

بر این اســاس، نوشــتار حاضــر، پس از اشــاره‌ای اجمالی به مفاد و قلمرو قاعده لاضــرر، تمرکز خود را بر معاملات رمزارزها قرار داده، مهم‌ترین وجوه احتمالی ضرر در این حوزه را شنا سایی و بر پایه این قاعده تحلیل می‌کند. هدف نهایی، ارائه فهمی فقهی و من سجم از میزان تأثیر این قاعده در مشروعیت و حدود فعالیت معاملاتی رمزارزها و کمک به تبیین حکم این مسأله نوپدید است.

۲. مهم‌ترین دیدگاه‌ها درباره مفاد قاعده

با توجه به اینکه در حدیث نبوی «لاضــررَ و لاضــرارَ» -به‌عنوان مهم‌ترین مســتند قاعده (مکارم‌شــیرازی، ۱۳۷۰، ج۱، ص۳۰؛ نک: غروی‌نایینی، ۱۳۷۳ق، ج۲، ص۲۰۹)- در هر دو فقره «لاضرر» و «لاضرار»، اسم پس از حرف «لا» با حذف تنوین «تمکّن» (تمکّن) به صورت مفتوح آمده است، بی‌تردید «لا» در این حدیث از نوع «لای نفی جنس» -یا به تعبیر دقیق‌تر، «لای محموله بر إنّ» (سیوطی، ۱۴۳۰ق، ۱۳۱)- است. بر این اساس، حدیث یادشده در مقام نفی جنسِ «ضرر» و «ضرار» است.

لای نفی جنس بر سر هر جمله‌ای در آید، بیانگر آن است که آنچه پس از آن قرار گرفته، در خارج وجود ندارد. برای نمونه، در جمله «لا رجلَ فی الدار»، مقصود آن است که هیچ مردی در خانه وجود ندارد. اکنون این پرسش مطرح می شود که اگر گفته شود: «لا ضرر و لا ضرار»، آیا معنای آن این است که در عالم خارج هیچ‌گونه ضرر و ضراری وجود ندارد؟ بی‌تردید چنین برداشتی درست نیست؛ زیرا بدیهی اســت که ضــرر و ضــرار در خارج تحقق دارد و بســیاری از آدمیزادگان در زندگی روزمره به اشــکال گوناگون به یکدیگر زیان می‌رسانند. افزون بر این، شارع در مقام تشریع، بیان‌کننده احکام شرعی است، نه گزارشگر امور تکوینی و واقعیت‌های خارجی. با توجه به این اشــکال، فقیهان در صــدد تبیین مقصــود از هیأت ترکیبی «لاضــرر و لاضــرار» برآمده‌اند و در این باره دیدگاه‌های گوناگونی ارائه کرده‌اند. در ادامه، مهم‌ترین این دیدگاه‌ها بررسی می‌شود.

۲/۱. دیدگاه اول: نفی تشریع حکم ضرری. بر اساس این دیدگاه، مفاد قاعده آن است که هر حکمی که از سوی شارع صادر شود -اعم از حکم تکلیفی یا وضعی- اگر امتثال آن برای مکلّف مستلزم ضرر باشد، یا اصل تشریع آن موجب ورود زیان به مردم گردد، به موجب قاعده «لاضرر» در شریعت نفی می شود (انصاری، ۱۳۷۷، ج۲، ص٤٦٠). بر این اساس، «لا» در معنای حقیقی خود، یعنی نفی جنس، به کار رفته و دلالت بر نفی هرگونه حکم ضــرری دارد. برای نمونه، اگر اســتفاده از آب برای شــخصــی زیان‌آور باشــد، حکم تکلیفی وجوب وضو بر اساس این قاعده از او برداشته می شود. همچنین در معامله غبنی که یکی از طرفین متضرر می شود، اگر چنین معامله‌ای به حکم شارع لازم و غیرقابل فسخ تلقی شود، طرف مغبون دچار زیان خواهد شد؛ در حالی‌که بر پایه قاعده «لاضرر»، حکم وضعیِ لزوم در این مورد منتفی است و شخص مغبون حق فسخ معامله را خواهد داشت. بنابراین، قاعده «لاضرر» بر نفی جعل حکم ضرری دلالت دارد؛ خواه ضرر ناشی از خود حکم باشد (مانند لزوم بیع غبنی) یا ناشی از متعلق حکم باشد (مانند وضوی ضرری).

در قضیه سمره نیز، از آنجا که حکم به جواز ورود سمره به باغ مرد انصاری موجب ورود ضرر به مالک باغ می شود، نفی ضرر در این روایت به معنای نفی حکم جواز دخول دانسته می شود؛ زیرا این حکم، منشأ تحقق ضرر است. در نتیجه، با نفی حکم (سبب)، ضرر (مسبَّب) نیز منتفی خواهد شد. از این‌رو، هرچند معصوم(ع) به ظاهر فرموده‌اند «لاضرر»، مقصود آن است که سببیت حکم برای تحقق ضرر نفی شده است.

این دیدگاه، نظریه مشهور فقها و از جمله آنها محقق نراقی (نراقی، ۱٤۱۷ق، ص٥۱)، شیخ انصاری (انصاری، ۱۳۷۷، ج۲، ص٤٦٠)، محقق نایینی (غروی‌نایینی، ۱۳۷۳ق، ج۲، ص۲۲۰)، سید یزدی (طباطبایی‌یزدی، ۱۳۷۰، ج۲، ص۸۰)، سید حکیم (طباطبایی‌حکیم،

١٤١٦ق، ج١٤، ص٢٧٧)، محقق خویی (خویی، ١٤١٣ق، ج١، ص٦١٥) و محقق بجنوردی (موسوی‌بجنوردی، ١٣٧٧، ج١، ص٢١٨) است.

٢/٢. دیدگاه دوم: نهی تحریمی تکلیفی. بر اساس این دیدگاه، «لا» در حدیث «لاضرر و لاضرار» برای نفی جنس به کار نرفته، بلکه در معنای نهی و بازداشتن از اضرار به دیگران استعمال شده است.[1] مطابق این تفسیر، مفاد حدیث صرفاً بیانگر یک حکم فرعی تکلیفی، یعنی حرمت اضرار به غیر است، نه قاعده‌ای کلی که بتوان در ابواب مختلف فقه به آن استناد کرد. از همین رو، برخی بر این باورند که بر پایه این نظریه، «لاضرر» تنها حکمی فقهی دالّ بر عدم جواز آسیب‌رسانی به دیگران است و در شمار قواعد فقهی قرار نمی‌گیرد (هادوی‌تهرانی، درس خارج اصول، ١٤٠٢/٠٨/٢٠).

این نظریه بیش از همه با نام شیخ‌الشریعه اصفهانی شناخته می‌شود (شریعت‌اصفهانی، بی‌تا، صص ١٨و١٩؛ نک: خویی، ١٤١٣ق، ١، ٦١١)، هرچند پیش از او صاحب وسائل (حرعاملی، ١٤٠٩ق، ج٢٥، ص٤٢٧) و صاحب العناوین چنین دیدگاهی داشته‌اند (حسینی‌مراغی، ١٤١٧ق،ج١، ص٣١١). صاحب جواهر نیز به این دیدگاه تمایل نشان داده است (نجفی، ١٣٦٢، ج٥، ص٩٨).

٢/٣. نقد و بررسی

دیدگاه نخست قابل پذیرش به نظر نمی‌رسد و با اشکالات متعددی روبه‌رو است:

نخست. مخالفت با ظاهر روایت

تفسیر روایت «لا ضرر و لا ضرار» به نفی حکم ضرری مستلزم تقدیر گرفتن واژه «حکم» در روایت است؛ بدین معنا که روایت به دلالت اقتضا باید به صورت «لا حکمَ ضرریّاً» تفسیر شود. حال آنکه اصل، بر عدم تقدیر است و هرگاه بتوان بر پایه تفسیرهای دیگر، معنایی ارائه کرد که نیازمند تقدیر نباشد، عدول از ظاهر و گرایش به تقدیر موجه نخواهد بود (نک: عراقی، ١٤١٨ق، صص١٣٦ و ١٤٣). افزون بر این، مطابق این دیدگاه، واژه «ضرر» در روایت در مقام وصف و به صورت «ضرریّ» لحاظ شده است که با ظاهر لفظ سازگار نیست (نک: ایروانی، ١٤٣٢ق، ج١، ص١٢٤). ازهمین‌رو، امام خمینی تفسیر روایت به معنای نفی حکم ضرری را ناسازگار با فصاحت کلام دانسته است (موسوی‌خمینی، ١٤٢٣ق، ج٣، ص٥٣٧).

دوم. ناتمام بودن توجیه مجازیّت

اگر گفته شود که مقصود از «ضرر» از باب مجاز در کلمه و به علاقه مسببیّت، همان «حکم» است (سبحانی‌تبریزی، ١٤٢٠ق، ص٦٩)، این توجیه نیز از نظر عرفی چندان پذیرفتنی نیست؛ زیرا در جای خود ثابت شده است که صرف وجود علاقه برای اثبات مجازیّت کفایت نمی‌کند، مگر آنکه عرف و ذوق سلیم چنین استعمالی را بپذیرند (نک: تفتازانی، بی‌تا، ٢١٨)، و به نظر می‌رسد در این مورد چنین پذیرشی وجود ندارد. به علاوه، این مطلب را نیز نباید از نظر دور داشت که اصل در استعمالات، کاربرد لفظ در معنای حقیقی آن است، مگر آنکه دلیل محکمی برای گذر از معنای حقیقی به مجازی وجود داشته باشد.

سوم. خلط میان حکم شرعی و متعلَّق حکم

---

١. در ادامه، این مسئله بررسی خواهد شد که آیا قاعده نفی ضرر -افزون بر منع ضررسانی به دیگران- شامل بازداشتن از اضرار به خود نیز می‌شود یا خیر.

به نظر می‌رسد این تقریر از قاعده، مبتنی بر نوعی خلط میان حکم شرعی و متعلَّق حکم است. توضیح آنکه بر اساس این دیدگاه، جعل حکم ضـرری نفی شـده اسـت؛ حال آنکه احکام شـرعی -مانند وجوب و حرمت- به مثابه اموری اعتباری، ذاتاً فاقد آثار تکوینی‌اند و صرفاً نقش انگیز شی در جهت انبعاث مکلف به سوی انجام دادن یا ترک فعل دارند. از این رو، آنچه می‌تواند منشأ ضرر با شد، تحقق خارجیِ متعلَّق حکم -یعنی فعل مکلف در شـرایط خاص- اسـت، نه خود حکم. بنابراین، می‌توان گفت حکم (مانند وجوب روزه) فی‌نفسـه سـبب ضـرر نیسـت، بلکه متعلَّق حکم (مانند روزه گرفتن در شـرایطی خاص) اسـت که موجب ضـرر می‌شـود (برگرفته از نورمفیدی، درس خارج فقه، ۱۳۹۳/۱۱/۲۱).

چهارم. ناسازگاری این تفسیر با برخی نقل‌های دیگر از واقعه

این تفسیر با نقل دیگری از این واقعه که در برخی منابع اهل‌تسنن آمده است -«وقَضَی: أن لا ضرر و لا ضرار»- نیز سازگار به نظر نمی‌رسد؛ زیرا این تعبیر در مقام داوری و صدور حکم از سوی حاکم و پس از شکایت مظلوم از ظالم بیان شده است. ازاین‌رو، صرفِ إخبار از نفی حکم ضرری و عدم جعل آن با چنین مقامی تناسب ندارد (موسوی‌خمینی، ١٤٢٣ق، ج٣، صص٥٣٤ و ٥٣٧)؛ چراکه در چنین وضعیتی انتظار می‌رود حاکم حکمی در جهت رفع نزاع و جلوگیری از تحقق ضرر صادر کند، نه آنکه تنها از عدم تشریع حکم ضرری خبر دهد.

پنجم. استلزام محذور تخصیص اکثر

با کنار گذاشتن تفسیر «نفی حکم ضرری» از قاعده لاضرر، محذور تخصیص اکثر نیز برطرف می‌شود؛ زیرا در این صورت دیگر لازم نیست احکام متعددی که ممکن است در ظاهر متضمن نوعی ضرر باشند -مانند تشریع حدود، دیات، قصاص، تعزیرات، پرداخت خمس و زکات، کفارات و به‌ویژه وجوب جهاد- از شمول قاعده استثنا شوند و برای توجیه این استثناها به تحلیل‌ها و توجیهات پیچیده و پرمؤونه متوسل شد؛ توجیهاتی که در برخی منابع فقهی ارائه شده است (نک: نراقی، ١٤١٧ق، ص٥٦؛ انصاری، ١٣٧٧، ج٢، ص٤٦٥؛ حسینی‌سیستانی، بی‌تا، صص٢٢٠ـ٢٣٢).

به‌ویژه آنکه به نظر شماری از فقها، قاعده لاضرر -همانند حدیث «رفع» و قاعده «لاحرج»- در مقام امتنان بر بندگان وارد شده است؛ و هر حکمی که در مقام امتنان باشد، سیاق آن آبی از تخصیص است و اساساً تخصیص‌ناپذیر محسوب می‌شود، تا چه رسد به آنکه بحث از تخصیص اکثر، کثیر یا حتی قلیل درباره آن مطرح گردد (موسوی‌خمینی، ١٤٢٣ق، ج٣، ص٥١٣).

بر پایه این ملاحظات، تفسیر قاعده لاضرر به نفی تشریع حکم ضـرری با دشـواری‌های جدی روبه‌رو اسـت و نمی‌توان آن را تبیین قابل‌قبولی از مفاد روایت دانست. از این رو، لازم است مفاد حقیقی قاعده لاضرر را در دیدگاهی دیگر جستجو کرد.

٤/٢. تبیین و تقویت دیدگاه نهی تحریمی

به نظر می‌رسد آنچه با فضای صدور و سیاق حدیث سازگارتر است، دیدگاه دوم، یعنی برداشت نهی تکلیفی تحریمی از جمله «لاضرر و لاضرار» باشد؛ چنانکه شیخ‌الشریعه تصریح می‌کند آنچه از این روایت به ذهن متبادر می‌شود -البته برای ذهنی که از احتمالات دیگر خالی باشد- چیزی جز «نهی تکلیفی» نیست (شریعت‌اصفهانی، بی‌تا، ٢٦).

گفتنی است برداشت «نهی» از این روایت مستلزم آن نیست که «لا» لزوماً حرف نهی دانسته شود، تا این اشکال مطرح گردد که «لای نهی بر سر اسم وارد نمی شود». بر اساس دیدگاه برگزیده، «لا» در این حدیث لای نفی جنس است، اما مراد از آن معنای نهی است؛ یعنی مفاد جمله آن است که «نباید ضرر و ضراری وجود داشته باشد». برای تبیین این معنی، می‌توان به یکی از سه روش زیر ملتزم شد:

روش نخست. لای نفی جنس از باب مجاز در کلمه در معنای لای نهی به کار رفته است (ایروانی، ۱٤۳۲ق، ج۱، ص۱۱۹). وجه صحت این مجاز را می‌توان در تناسب معنایی میان این دو «لا» جست‌وجو کرد؛ زیرا هر دو در اصل معنی، یعنی نفی، مشترک‌اند؛ با این تفاوت که «لای نفی» ناظر به نفی در عرصه تکوین است، در حالی که «لای نهی» نفی در قلمرو اعتبار و انشاء به شمار می‌آید.

البته برخی اندیشمندان بر استفاده از معنای نهی در جمله «لاضرر و لاضرار» خرده گرفته‌اند، با این استدلال که چنین توجیهی متضمن مجاز است و تا زمانی که می‌توان جمله را به معنای حقیقی، یعنی نفی حمل کرد، هیچ مجوّزی برای عدول از معنای حقیقی به مجازی وجود نخواهد داشت (خویی، ۱۴۱۳ق، ج۱، ص۶۱۱).

پاسخ آن است که حتی اگر جمله «لا ضرر و لا ضرار» بر نفی جنس حمل شود، این حمل نیز نمی‌تواند حقیقی باشد؛ زیرا معنای حقیقی نفی جنس مستلزم آن است که در خارج هیچ مصداقی از ضرر و ضرار وجود نداشته باشد، در حالی که واقعیت خارجی خلاف آن را نشان می‌دهد (انصاری، ۱۳۷۷، ج۲، ص٤٦٠). از این‌رو، برای پرهیز از لغویت کلام و حفظ اعتبار گفتار شرعی، ناگزیر از توسل به مجاز هستیم؛ خواه این مجاز به سوی معنای «نهی» باشد یا به سوی «نفی حکم». در نتیجه، هر دو تفسیر در نهایت مجازی خواهند بود و از این جهت نمی‌توان یکی را بر دیگری ترجیح داد (نک: حسینی‌سیستانی، بی‌تا، صص۱۸۱و۱۸۲). افزون بر این، استنباط معنای نهی از حدیث «لاضرر و لاضرار» منحصر به مجازی بودن کاربرد «لا» نیست و راه‌های دیگری نیز برای توجیه آن وجود دارد.

روش دوم. لای نفی جنس بدون هیچ‌گونه مجازی در معنای حقیقی خود به کار رفته و برای نفی جنس ضرر و ضرار استعمال شده است، با این تفاوت که خبر آن –مانند «مشروعٌ» یا «جائزٌ»– محذوف در نظر گرفته می‌شود (حسینی‌مراغی، ۱٤۱۷ق، ج۱، ص۳۱۱). بر این اساس، مفاد جمله آن است که ضرر و ضرار در شریعت مشروع یا جایز نیست. روشن است که نفی جواز چیزی در وعاء تشریع، در عمل به معنای نهی از ارتکاب آن خواهد بود.

روش سوم. جمله در ظاهر إخبار از نفی است، اما به قصد انشای نهی به کار رفته است؛ مانند آنکه صاحب‌خانه به خدمتکار بگوید: «لیس فی بیتی الکذب و الخیانة» (در خانه من دروغ و خیانت وجود ندارد)، در حالی که مقصود او گزارش خبری نیست، بلکه دستوری انشایی است؛ یعنی «در این خانه هرگز دروغ مگو و خیانت مکن» (مکارم‌شیرازی، ۱۳۷۰، ج۱، ص٦١). این مطلب نظیر کاربرد جمله خبری «بِعتُ» (فروختم) است که به قصد انشای عقد بیع استعمال می شود (ایروانی، ۱٤۳۲ق، ج۱، ص۱۱۹؛ نک: خویی، ۱٤۱۷ق، ج۳، ص٥٣٦).

باید توجه داشت که استفاده از جمله خبری برای افاده نهی در کلام فصیحان امری شناخته شده است (موسوی‌خمینی، ۱٤۲۳ق، ج۳، ص٥٣٧) و در متون دینی، اعم از قرآن و سنت، نیز نمونه‌هایی از آن دیده می‌شود (خویی، ۱٤۱۷ق، ج۳، ص٥٣٧)؛ از جمله در قرآن کریم آمده است: «فَلَا رَفَثَ وَ لَا فُسُوقَ وَ لَا جِدَالَ فِي الْحَجِّ»[1] (بقره: ۱۹۷). این جمله به صورت خبری بیان شده است، اما در حقیقت معنایی انشایی و نهی‌گونه دارد؛ بدین معنی که حج‌گزاران از ارتکاب این امور منع شده‌اند. در روایات نیز نمونه‌هایی از این شیوه دیده

---

۱. در حج، آمیزش با زنان و گناه و جدال نیست.

می شود؛ چنانکه در حدیثی آمده ا ست: «لا طاعةَ لمخلوقٍ في معصيةِ الخالق»[1] (صدوق، ١٤١٣ق، ج٢، ص٦٢١)، که با وجود ظاهر خبری، در واقع حکمی انشایی را افاده می‌کند؛ یعنی در معصیت خداوند، نباید از هیچ مخلوقی اطاعت کرد.

افزون بر این، برداشت واژه شناسان -به‌ویژه لغویان متقدم- از دو جمله «لاضرر و لاضرار» و تفسیر آن در معنایی همسو با دیدگاه نهی تحریمی تکلیفی (ازهری، ١٤٢١ق، ج١١، ص٣١٤)، می‌تواند مؤید دیگری برای این دیدگاه به شمار آید.

٣. شمول قاعده نسبت به آسیب‌رسانی به خود

بر اساس مبنای اتخاذشده در تفسیر قاعده «لا ضرر و لا ضرار»، تردیدی نیست که این قاعده موارد آسیب‌رسانی به دیگران را دربرمی‌گیرد؛ اما در اینکه آیا شامل آسیب‌رسانی به خود نیز می‌شود یا نه، میان فقیهان اختلاف‌نظر وجود دارد. از آنجا که دو واژه «ضرر» و «ضرار» در این حدیث به صورت نکره در سیاق نفی به کار رفته‌اند، ظهور در عموم دارند و در نتیجه هر نوع ضرری را شامل می‌شوند؛ خواه ضرری که متوجه خود شخص شود (اضرار به نفس) و خواه ضرری که متوجه دیگران گردد (اضرار به غیر). شاید از همین روست که به تصریح شیخ انصاری، عالمان در استدلال به قاعده نفی ضرر میان «ضرر زدن به خود» و «ضرر زدن به دیگران» تفاوتی قائل نشده‌اند (انصاری، ١٤١١ق، ج٣، ص٣٤٤).

با این حال، شیخ انصاری با توجه به مبنای خاص خود در تفسیر قاعده «لاضرر»، دایره شمول آن را به مواردی محدود می‌داند که حکم شرعی منشأ پیدایش ضرر باشد؛ از این‌رو، قاعده را شامل ضرر به نفس نمی‌داند، زیرا در این موارد منشأ ضرر اراده خود مکلف است، نه حکم شرعی (انصاری، ١٤١١ق، ج٣، صص ٣٤٤ و ٣٤٩؛ نک: حائری، بی‌تا، ج٤، صص ٦٣٤و٦٣٥). بر همین اساس، وی معتقد است از قاعده «لاضرر» تنها حرمت اضرار به غیر استفاده می‌شود، در حالی که حرمت اضرار به نفس از ادله عقلی و نقلی دیگر به دست می‌آید (انصاری، ١٤١١ق، ج٣، ص٣٤٤). محقق خویی نیز تقریباً دیدگاهی نزدیک به همین نظر دارد (نک: خویی، ١٤١٣ق، ج١، ص٦١٩).

بر پایه دیدگاه برگزیده در این پژوهش، اگر قاعده «لاضرر» علاوه بر ضرر رساندن به دیگران، ضرر رساندن به خود را نیز دربرگیرد، دایره آن به نظریه مشهور، یعنی «نفی تشریع حکم ضرری»، نزدیک خواهد شد. در این صورت، قاعده افزون بر موارد مربوط به تعاملات میان افراد، مواردی مانند نهی از وضوی ضرری را نیز تحت پوشش قرار می‌دهد. از آنجا که بر اساس مبانی اصولی، نهی در عبادت مستلزم فساد آن است (خویی، ١٣٦٨، ج٥، ص٣)، در این دیدگاه نیز -همانند دیدگاه نخست- می‌توان نتیجه گرفت که وضوی ضرری باطل خواهد بود.

با این حال، در نقد این ادعا می‌توان گفت فضای صدور حدیث ـ یعنی ماجرای سمره و مرد انصاری ـ عمدتاً ناظر به تنظیم روابط میان افراد است و همین قرینه معنوی می‌تواند مانع از آن شود که دایره شمول قاعده به «ضرر رساندن به خود» نیز گسترش یابد. مؤید این نکته آن است که قدمای اصحاب، با وجود مهارت و تبحر در فهم مفاهیم عرفی کتاب و سنت، هرگز از این حدیث در موارد مربوط به عبادات ضرری استفاده نکرده و در چنین مواردی به آن استناد ننموده‌اند؛ بلکه کاربرد آن را عمدتاً در ابواب معاملات و در مسائل ناظر به روابط میان افراد -مانند خیار غبن- دانسته‌اند. برای نمونه، شیخ طوسی در کتاب الخلاف در مقام استدلال بر وجوب تیمم هنگام خوف از تلف

---

١. هیچ اطاعتی برای مخلوق در معصیت خالق وجود ندارد.

یا افزایش بیماری بر اثر استعمال آب، به آیه «مَا جَعَلَ عَلَيْكُمْ فِي الدِّينِ مِنْ حَرَجٍ» (حج: ۷۸) تمسک می‌کند و سپس به اجماع و برخی روایات استدلال می‌نماید، اما هیچ اشاره‌ای به قاعده نفی ضرر ندارد (طوسی، بی‌تا، ج۱، ص۱۵۸و۱۵۹).

شایان ذکر است که اگر مدرک اصلی قاعده «لاضرر» حکم عقل دانسته شود -نه حدیث «لا ضرر و لا ضرار»- (محقق‌داماد، ۱٤۰۱، ص۱۷۱)، با توجه به اینکه عقل به طور مستقل قبح ظلم را درک می‌کند، دایره شمول قاعده گسترده‌تر خواهد بود. از آنجا که عقل، قبح ظلم را امری مطلق و غیرمقید می‌داند، تفاوتی نمی‌کند که این ضرر رساندن متوجه دیگری باشد یا خود شخص؛ در هر صورت، هر فعل زیان‌باری می‌تواند مصداقی از ظلم تلقی شود و عقل به طور مستقل آن را قبیح و ناروا می‌شمارد.

٤. چالش‌های مرتبط با معاملات رمزارزها

پس از بررسی اجمالی قاعده «لاضرر» و تبیین مبنای مختار در مفاد آن، گام بعدی شناسایی مهم‌ترین چالش‌ها و مخاطرات موجود در معاملات رمزارزهاست؛ زیرا تنها در پرتو شناخت دقیق این مخاطرات می‌توان نسبت آن‌ها را با ممنوعیت آسیب‌رسانی ارزیابی کرد.

چالش‌های موجود در این حوزه عمدتاً از ویژگی‌های ساختاری این بازار ناشی می‌شود؛ از جمله غیرمتمرکز بودن شبکه‌ها، نوپا بودن فناوری، و فقدان چارچوب‌های نظارتی جامع و تثبیت‌شده. این ویژگی‌ها سبب شده است که حتی کاربران نسبتاً آگاه نیز در معرض خطرهای جدی قرار گیرند.

مهم‌ترین این ریسک‌ها که در ادامه به طور مستقل بررسی خواهند شد عبارت‌اند از:

۱- نوسانات شدید قیمت

۲- دستکاری بازار

۳- کلاهبرداری‌های سازمان‌یافته و پروژه‌های تقلبی

٤- مسدود شدن حساب‌ها و تحریم کاربران

۵- از دست دادن دارایی در اثر خطای کاربر

مجموع این عوامل سبب شده است که مسأله امنیت و قابلیت اعتماد به یکی از مهم‌ترین دغدغه‌های فعالان این حوزه تبدیل شود؛ دغدغه‌ای که نقش تعیین‌کننده‌ای در ارزیابی فقهی این معاملات و سنجش احتمال تحقق اضرار در آن‌ها خواهد داشت.

٤/۱. نوسانات شدید قیمت[۱]

یکی از مهم‌ترین مخاطرات بازار رمزارزها، نوسانات شدید قیمت است. این بازار به دلیل عواملی همچون حجم نسبتاً محدود، نقدینگی پایین‌تر نسبت به بازارهای مالی سنتی، و حضور گسترده معامله‌گران سفته‌باز، دچار بی‌ثباتی قیمتی قابل‌توجهی است. به‌عنوان‌مثال، بر اساس یافته‌های پژوهشی در سال ۲۰۲۴، نوسان‌پذیری بیت‌کوین به‌طور تاریخی چندین برابر شاخص‌های اصلی بازار سهام بوده است؛ به‌گونه‌ای که در دوره‌های مختلف، میزان نوسان آن به طور متوسط ۴ تا ۵ برابر شاخص‌هایی مانند S&P ۵۰۰ گزارش شده است (mdpi, ۲۰۲۳)[۲]. این امر نشان می‌دهد که ریسک از دست دادن سرمایه در بازار رمزارزها به مراتب بیشتر از بسیاری از بازارهای مالی متعارف

---

۱. Volatility

۲. Bitcoin versus S&P ۵۰۰ Index: Return and Risk Analysis

است. نمونه‌ای روشن از این بی‌ثباتی را می‌توان در تحولات قیمتی سال‌های اخیر مشاهده کرد. در سال ۲۰۲۲، قیمت بیت‌کوین از اوج تاریخی حدود ۶۹٬۰۰۰ دلار در نوامبر ۲۰۲۱ به کمتر از ۱۷٬۰۰۰ دلار در نوامبر ۲۰۲۲ سقوط کرد. در نتیجه این کاهش شدید، بسیاری از معامله‌گران خرد که در نزدیکی اوج قیمت وارد بازار شده بودند، بیش از ٪۷۵ از سرمایه خود را از دست دادند. برای مثال، سرمایه‌گذاری که ۱۰٬۰۰۰ دلار در قیمت حدود ۶۵٬۰۰۰ دلار خریداری کرده بود، با کاهش قیمت به محدوده ۱۷٬۰۰۰ دلار، ارزش دارایی او به حدود ۲٬۵۰۰ دلار تقلیل یافت. نمودار زیر، نوسانات قیمتی بیت‌کوین را به عنوان یکی از مهم‌ترین رمزارزها، در بازه‌ای حدوداً ده‌ساله (از سال ۲۰۱۵ تا ۲۰۲۵) نشان می‌دهد.

نمودار ۱. نوسانات قیمت بیت‌کوین در بازه ۲۰۱۵ تا ۲۰۲۵

این داده‌ها نشان می‌دهد که بیت‌کوین، با وجود ظرفیت بالقوه برای کسب سودهای چشمگیر، دارایی‌ای با سطح بالایی از بی‌ثباتی قیمتی است. از همین‌رو، برخی پژوهشگران (عابدیان‌کلخوران، ۱۴۰۲، ص. ۳۸۳) معتقدند نوسانات شدید قیمتی –به‌ویژه در مواردی که سرمایه‌های قابل‌توجه خانوارها را در معرض نابودی قرار می‌دهد– می‌تواند مصداق ضرر قابل‌توجه اقتصادی تلقی شود و از این‌رو قاعده «لاضرر» در این عرصه جریان می‌یابد.

۱/۱/۴. نقد و بررسی

اگرچه این اشکال به‌ویژه در مورد رمزارزهای پرنوسانی مانند بیت‌کوین صادق است، باید دانست که نوسانات شدید و دوره‌های ریزش قیمتی پدیده‌ای منحصر به بازار رمزارزها نیست؛ بلکه بازارهای مالی سنتی و تحت نظارت نیز از آن مصون نیستند. برای نمونه، بورس تهران در بازه زمانی ۱۳۹۹ تا ۱۴۰۲ با کاهش قابل‌ملاحظه شاخص کل مواجه شد. بر اساس داده‌های منتشرشده از سوی سازمان بورس و اوراق بهادار، ارزش پرتفوی شمار قابل‌توجهی از سرمایه‌گذاران خرد در این دوره بیش از ۵۰ درصد کاهش یافت و در برخی نمادها این کاهش حتی به حدود ۷۰ تا ۸۰ درصد نیز رسید.[۱] این واقعیت نشان می‌دهد که نوسانات شدید پدیده‌ای است که –با شدت‌های متفاوت– در سایر بازارهای مالی نیز مشاهده می‌شود.

---

۱. آمار یادشده در بخش «گزارش آماری وضعیت بازار سرمایه» در تارنمای رسمی «سازمان بورس و اوراق بهادار» به نشانی www.seo.ir قابل مشاهده و استناد است.

با این حال، باید به این نکته توجه داشت که کاهش قیمت‌ها لزوماً به معنای تحقق قطعی ضرر برای سرمایه‌گذار نیست؛ زیرا همان‌گونه که احتمال کاهش قیمت وجود دارد، امکان بازگشت آن به سطح‌های پیشین و حتی صعود به سطوح بالاتر نیز محتمل است. افزون بر این، از آنجا که رمزارزها دارایی‌های فاسدشدنی محسوب نمی‌شوند، افت موقتی قیمت را نمی‌توان لزوماً معادل ضرر قطعی دانست.

با وجود این، برای مواجهه با نوسانات بازار رمزارزها راهکارهای عملی متعددی پیشنهاد شده است که مهم‌ترین آنها عبارت‌اند از:

الف) سرمایه‌گذاری آگاهانه

سرمایه‌گذاران بهتر است تنها با سرمایه مازاد وارد این بازار شوند و از به‌کارگیری «اهرم مالی»[1] ـ که ریسک معاملات را به‌طور قابل‌توجهی افزایش می‌دهد ـ پرهیز کنند. همچنین، متنوع‌سازی سبد سرمایه‌گذاری[2] میان چند رمزارز مختلف می‌تواند ریسک ناشی از سقوط یک دارایی خاص را کاهش دهد.

ب) آموزش مالی

آشنایی با مفاهیم پایه‌ای مانند «ارزش ذاتی دارایی‌ها»، «تحلیل بنیادی» (بررسی اهداف، تیم و طرح پروژه) و «تحلیل تکنیکال» (بررسی نمودارها و روندهای قیمتی) به سرمایه‌گذاران کمک می‌کند تا به‌جای تصمیم‌های هیجانی، تصمیم‌های مبتنی بر تحلیل اتخاذ کنند.

ج) استفاده از استیبل‌کوین‌ها[3]

در دوره‌های نوسان شدید بازار، تبدیل دارایی‌ها به استیبل‌کوین‌های وابسته به ارزهای معتبر –مانند USDT یا USDC– می‌تواند راهکاری مؤثر برای حفظ ارزش سرمایه باشد. این رمزارزها به پشتوانه دارایی‌های سنتی مانند دلار آمریکا طراحی شده‌اند و از این‌رو نوسان قیمتی به‌مراتب کمتری دارند (investopedia, ۲۰۲۵)[4].

د) تعیین حدّ ضرر[5]

استفاده از ابزار «حدّ ضرر» در صرافی‌ها می‌تواند از زیان‌های سنگین جلوگیری کند. به‌عنوان مثال، اگر قیمت بیت‌کوین به زیر سطح از پیش تعیین‌شده‌ای برسد، دارایی کاربر به‌صورت خودکار فروخته می‌شود. نمونه‌ای از کارکرد این ابزار را می‌توان در ریزش تاریخی بیت‌کوین در سال ۲۰۲۲ مشاهده کرد؛ زمانی که قیمت از حدود ۶۹٬۰۰۰ دلار به کمتر از ۱۷٬۰۰۰ دلار سقوط کرد، سرمایه‌گذارانی که حدّ ضرر خود را در سطوحی مانند ۶۰٬۰۰۰ یا ۵۰٬۰۰۰ دلار تعیین کرده بودند، توانستند پیش از تشدید ریزش، دارایی خود را به‌طور خودکار بفروشند و از زیان‌های بسیار سنگین جلوگیری کنند.

هـ) سرمایه‌گذاری بلندمدت[6]

---

۱. «اهرم مالی» (Financial Leverage) به روشی از تأمین مالی گفته می‌شود که در آن اشخاص یا شرکت‌ها با استفاده از منابع استقراضی، سرمایه‌ای بیش از سرمایه واقعی خود را در معاملات به کار می‌گیرند. در این روش، معامله‌گر با ایجاد بدهی یا دریافت اعتبار از کارگزار یا صرافی، امکان خرید یا معامله دارایی‌هایی با ارزشی بیش از سرمایه اولیه خود را به دست می‌آورد. هدف از به‌کارگیری اهرم مالی افزایش میزان سود بالقوه است؛ هرچند در مقابل، ریسک زیان نیز به همان نسبت افزایش می‌یابد.

۲. Portfolio Diversification

۳. Stablecoins

٤. Stablecoins: Definition, How They Work, and Types

٥. Stop Loss

٦. HODLing

تجربه تاریخی بازار رمزارزها نشان می‌دهد که این بازار در افق‌های زمانی بلندمدت (حدود ۵ تا ۱۰ سال)، با وجود نوسانات کوتاه‌مدت، غالباً روندی صعودی داشته است. این راهبرد بر نگهداری دارایی و پرهیز از واکنش‌های شتاب‌زده به نوسانات کوتاه‌مدت تأکید دارد. اتخاذ چنین رویکردی نه‌تنها اثر نوسانات مقطعی را کاهش می‌دهد، بلکه با جلوگیری از تصمیم‌های هیجانی –مانند فروش در کف قیمت یا خرید در اوج– احتمال سودآوری را نیز افزایش می‌دهد.

در مجموع، هرچند نوسانات در بازار رمزارزها به‌طور کامل قابل‌حذف نیست، اما با به‌کارگیری مجموعه‌ای از راهکارهای یادشده می‌توان آثار منفی آن را بر سرمایه‌گذاران تا حد قابل‌توجهی کاهش داد.

۲/۱/٤. ملاحظات فقهی ناظر به «نوسانات شدید قیمت» و راهکارهای مدیریت آن

بر اساس تفسیر برگزیده از قاعده «لاضرر» به‌عنوان نهی از آسیب‌رسانی به دیگران، می‌توان گفت صرف نوسان شدید قیمت –مادامی که برآمده از سازوکار معمول عرضه و تقاضا و رفتار متعارف بازار باشد– به‌خودی‌خود، مصداق آسیب‌رسانی به غیر محسوب نمی‌شود. در مقابل، رفتارهایی مانند دستکاری عمدی قیمت، ایجاد حباب‌های مصنوعی، انتشار اطلاعات گمراه‌کننده یا سوءاستفاده از اطلاعات نهانی، با هدف انتقال زیان به دیگران، مصادیق روشن ضرر وارد کردن به غیر به شمار می‌رود و از این حیث، تحت منع شرعی قرار دارد.

در این چارچوب، اقداماتی چون افزایش شفافیت بازار، مقابله با دستکاری قیمت و محدودسازی سازوکارهای پرریسک، به‌منزله تدابیری است که به کاهش امکان اضرار به دیگران یاری می‌رساند.

از سوی دیگر، بر فرض توسعه مفاد قاعده لاضرر به «ضرر به خود»، ورود غیرآگاهانه یا نامتناسب با توان مالی به بازاری با نوسان شدید، دست‌کم در برخی موارد می‌تواند از مصادیق رفتارهای ممنوع شرعی بر پایه این قاعده تلقی شود. در این چارچوب، به‌کارگیری راهکارهایی مانند سرمایه‌گذاری با سرمایه مازاد، تنوع‌بخشی سبد دارایی، تعیین حدّ ضرر و اتخاذ افق زمانی بلندمدت، به‌عنوان تدابیری عقلایی برای پیشگیری از ورود ضرر قابل پیش‌بینی ارزیابی می‌شود.

۲/٤. دستکاری بازار[۱]

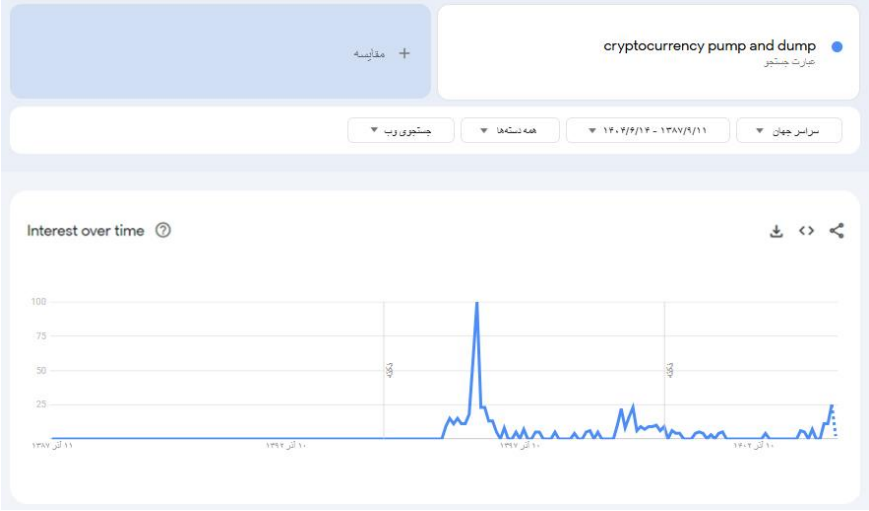
«دستکاری بازار» به‌ویژه در قالب طرح‌های «پامپ و دامپ»[۲]، از مصادیق بارز آسیب‌رسانی عمدی و برنامه‌ریزی‌شده در بازار رمزارزها است. بر اساس داده‌های گوگل‌ترندز[۳] مربوط به جستجوی عبارت «Cryptocurrency pump and dump» از سال ۱۳۸۷ (مصادف با ۲۰۰۸ میلادی، همزمان با تولد بیت‌کوین) تا ۱۴۰۴، می‌توان روندی رو به افزایش در توجه و نگرانی کاربران نسبت به این پدیده مشاهده کرد. این روند دست‌کم به دو نکته دلالت دارد: نخست آنکه با گسترش بازار رمزارزها و افزایش حضور سرمایه‌گذاران خرد، از حیث تعداد و تناوب، رویدادهای پامپ و دامپ نیز فزونی یافته است؛ دوم آنکه آگاهی عمومی نسبت به وجود چنین طرح‌های کلاهبردارانه و علاقه به شناخت سازوکار آنها به‌طور محسوس افزایش پیدا کرده است. اوج‌های متعدد نمودار، به‌ویژه در سال‌های اخیر، غالباً همزمان با رویدادهای مهم دستکاری بازار و افشاگری‌های رسانه‌ای بوده که توجه جامعه سرمایه‌گذاری را بیش از پیش به این موضوع جلب کرده است.

---

۱. Market Manipulation

۲. Pump and Dump

۳. Google Trends



نمودار ۲. روند جست‌وجوی گوگل در مورد پامپ و دامپ رمزارزها

در این طرح‌ها، گروه‌های سازمان‌یافته با در اختیار داشتن سرمایه قابل‌توجه، قیمت یک دارایی کم‌ارزش یا بی‌ارزش را از طریق تبلیغات دروغین در شبکه‌های اجتماعی (مانند تلگرام و توییتر) و انجام خریدهای هماهنگ، به‌صورت مصنوعی افزایش می‌دهند (پامپ). این فرایند، هیجان کاذب ایجاد کرده و سرمایه‌گذاران خردی را که از ماهیت واقعی ماجرا بی‌خبرند، به ورود در بازار ترغیب می‌کند. پس از آنکه این سرمایه‌گذاران وارد شده و قیمت به‌طور غیرواقعی رشد می‌کند، سازمان‌دهندگان اصلی، به‌صورت ناگهانی اقدام به فروش گسترده دارایی می‌نمایند (دامپ) و در نتیجه، قیمت با سقوط شدید مواجه شده و زیان‌های سنگینی بر سرمایه‌گذاران خرد تحمیل می‌شود (mdpi, ۲۰۲۳)[۱].

چنین سازوکاری، علاوه بر آنکه از منظر حقوقی در زمره کلاهبرداری‌های مالی قرار می‌گیرد، از حیث فقهی نیز مصداق روشن «آسیب‌رسانی عمدی» در چارچوب قاعده «لاضرر» است؛ زیرا در آن، انتقال آگاهانه و برنامه‌ریزی‌شده ضرر غیرمتعارف به دیگران، در قالب ظاهراً معاملاتی و مبتنی بر فریب و اغراء به جهل، رخ می‌دهد.

۱/۲/٤. نقد و بررسی

نخست باید توجه داشت که «دستکاری بازار» به هیچ‌وجه پدیده‌ای منحصر به رمزارزها نیست، بلکه سابقه‌ای طولانی در بازارهای سنّتی مالی، از جمله بورس سهام دارد. نمونه‌های کلاسیک طرح‌های پامپ و دامپ در سهام شرکت‌های کوچک، کم‌ارزش و فاقد بنیان‌های قوی، در ادبیات تاریخ بازارهای سرمایه به‌وفور گزارش شده است.

با این حال، ویژگی‌هایی مانند ساختار غالباً غیرمتمرکز، نوپا بودن بخش قابل‌توجهی از اکوسیستم رمزارزها، و ضعف یا عدم‌یکپارچگی نظارت مقرراتی در بسیاری از حوزه‌های قضایی، این بازار را به‌طور خاص مستعد و آسیب‌پذیر در برابر بروز و تکرار چنین رفتارهای مخرب

۱. A Survey on Pump and Dump Detection in the Cryptocurrency Market Using Machine Learning

ساخته است. با وجود این، راهکارهای متعددی برای مقابله و کاهش آثار این پدیده وجود دارد که به‌ویژه در صورت اتخاذ رویکردی ترکیبی و هماهنگ، می‌تواند کارآمد باشد. این راهکارها را می‌توان در سه سطح اصلی دسته‌بندی کرد:

الف) سطح فردی (کاربران و سرمایه‌گذاران)

در سطح فردی، ارتقای سواد مالی کاربران و آشنایی آنان با ماهیت کلاهبرداری‌های بازار، نقش محوری دارد. سرمایه‌گذاران با آموزش کافی درباره طرح‌های پامپ و دامپ و شناخت نشانه‌های هشداردهنده آن، از جمله وعده سودهای غیرمعمول و نجومی در بازه زمانی کوتاه، ایجاد فشار روانی برای خرید فوری و تأکید بر «فرصت تکرارناشدنی»، و تکیه بر تبلیغات هیجانی در کانال‌های غیررسمی و فاقد شفافیت، می‌توانند از تصمیم‌گیری‌های هیجانی و مبتنی بر ترس از دست دادن فرصت[۱] اجتناب کرده و به‌جای آن، بر تحلیل، منطق و اصول مدیریت ریسک تکیه نمایند. در این چارچوب، اقداماتی مانند تقسیم سرمایه[۲]، پرهیز از تمرکز سنگین بر یک دارایی خاص، و خودداری از به‌کارگیری بخش عمده دارایی در پروژه‌های ناشناخته و پرابهام، در کاهش آسیب‌پذیری نقش اساسی دارد. افزون بر این، بهره‌گیری از ابزارهای تحلیل On-Chain برای ردیابی فعالیت «نهنگ‌ها»[۳] و جریان‌های عمده مالی، می‌تواند امکان شناسایی زودهنگام الگوهای مشکوک و هماهنگ را برای کاربران آگاه فراهم سازد.

ب) سطح نهادی (صرافی‌ها و پروتکل‌ها)

در سطح نهادی، مسئولیت صرافی‌ها، پلتفرم‌های معاملاتی و پروتکل‌های غیرمتمرکز بسیار تعیین‌کننده است. این نهادها می‌توانند با پایش فعال معاملات و الگوهای قیمتی از طریق الگوریتم‌های پیشرفته، به‌ویژه ابزارهای مبتنی بر هوش مصنوعی[۴] و یادگیری ماشین، و با شناسایی و تعلیق معاملات مشکوک یا الگوهای غیرعادی حجم و قیمت، از گسترش طرح‌های دستکاری جلوگیری کنند. اجرای سیاست‌های سخت‌گیرانه احراز هویت و شناسایی مشتری، کاهش امکان فعالیت ناشناس مجرمان، انتشار گزارش‌های شفاف از حجم معاملات واقعی و عمق بازار، و اعلام هشدارهای عمومی به کاربران در صورت مشاهده رفتارهای مشکوک، از جمله اقداماتی است که هم امکان ارتکاب تخلف را کاهش می‌دهد و هم از حیث روانی و نهادی به تقویت اعتماد عمومی به بازار کمک می‌کند.

ج) سطح مقرراتی (حکمرانی و نهادهای ناظر)

در سطح مقرراتی، نهادهای ناظر مالی و تنظیم‌گران بازار سرمایه نیازمند وضع و اجرای قوانین شفاف، مشخص و قابل‌اجرا برای مقابله با دستکاری بازار هستند. تعریف دقیق مصادیق دستکاری، تعیین ضمانت‌اجراهای کیفری و مدنی متناسب، ایجاد سازوکارهای گزارش‌دهی و افشای به‌موقع، و فراهم‌سازی بسترهای حقوقی لازم برای همکاری با نهادهای خارجی، از ارکان این سطح به شمار می‌آید. با توجه به ماهیت ذاتاً فرامرزی رمزارزها، همکاری بین‌المللی نهادهای نظارتی برای تبادل اطلاعات، پیگیری فراسرزمینی مجرمان و مسدودسازی مسیرهای اصلی انتقال وجوه اهمیت ویژه‌ای دارد. همچنین، تأمین داده‌های قابل اعتماد و باکیفیت برای آموزش مدل‌های تشخیص دستکاری مبتنی بر هوش مصنوعی، از پیش‌نیازهای کارآمدسازی نظارت در این حوزه است.

---

۱. FOMO

۲. Diversification

۳. «نهنگ‌های رمزارزی» (Crypto Whales) به افراد یا نهادهایی (مانند صندوق‌های سرمایه‌گذاری) اطلاق می شود که مقدار بسیار زیادی از یک رمزارز خاص را در اختیار دارند. حجم دارایی آنها به حدی است که هر معامله بزرگ خرید یا فروش از سوی آنها می‌تواند به تنهایی موجب نوسانات قیمتی قابل توجهی در بازار شود، زیرا تأثیر مستقیمی بر توازن عرضه و تقاضا می‌گذارد.

٤. AI

در مجموع، هرچند حذف کامل پدیده «دستکاری بازار» –چه در رمزارزها و چه در سایر بازارهای مالی– واقع‌بینانه به نظر نمی‌رسد، اما با اجرای هم‌زمان و هماهنگ تدابیر یادشده در سطوح فردی، نهادی و مقرراتی، می‌توان به محیطی نسبتاً امن‌تر، شفاف‌تر و پاسخ‌گوتر دست یافت. بر این اساس، آموزش و توانمندسازی کاربران، تقویت نظارت فناورانه به‌ویژه با اتکا به ابزارهای هوش مصنوعی، و تدوین و اجرای قوانین مؤثر و متناسب با واقعیت فرامرزی رمزارزها، سه ضلع اصلی استراتژی مقابله با این چالش را تشکیل می‌دهد.

٤/٢/٢. ملاحظات فقهی ناظر به «دستکاری بازار» و راهکارهای مدیریت آن

در چارچوب مبنای مختار در قاعده لاضرر، دستکاری بازار در قالب طرح‌هایی مانند «پامپ و دامپ» از مصادیق روشن آسیب‌رسانی به دیگران به شمار می‌آید؛ زیرا در این سازوکارها، طراحان با ایجاد هیجان مصنوعی و انتشار اطلاعات گمراه‌کننده، زمینه انتقال آگاهانه زیان به سرمایه‌گذاران دیگر را فراهم می‌کنند. بنابراین چنین رفتارهایی، از جهت تکلیفی، تحت شمول نهی قاعده لاضرر قرار می‌گیرد و انجام دادن آن‌ها حرام است؛ هرچند بحث از صحّت یا بطلان معاملات واقع‌شده در این بستر و نیز مسئولیت‌های جبرانی (ضمان) نیازمند استناد به ادلّه و مبانی مستقل دیگری است. بر این اساس، راهکارهایی مانند ارتقای سواد مالی کاربران، نظارت فعال صرافی‌ها و تنظیم‌گری قانونی، در حکم مقدماتی است که برای کاهش امکان وقوع این نوع آسیب‌رسانی طراحی می‌شود.

همچنین، بر فرض شمول قاعده نسبت به ضرر به خود، ورود هیجانی و بدون بررسی به پروژه‌هایی که نشانه‌های آشکار دستکاری بازار دارند، می‌تواند زمینه تحقق عنوان ضرر و جریان یافتن منع شرعی مبتنی بر این قاعده را فراهم سازد. ازاین‌رو، آموزش مالی، هشدارهای نظارتی و محدودسازی دسترسی بی‌ضابطه به معاملات پرریسک، در جایگاه تدابیر پیشگیرانه‌ای قرار می‌گیرد که احتمال گرفتار شدن فرد در چنین ضررهایی را کاهش می‌دهد.

٤/٣. کلاهبرداری‌های سازمان‌یافته[1]

بر اساس پژوهشی که در سال ۲۰۲۳ در مجله تخصصی Risks منتشر شده است، بخش قابل‌توجهی از فضای رمزارزها توسط پروژه‌های کلاهبرداری احاطه شده که عمدتاً در دو قالب «طرح‌های پانزی»[2] و «تخلیه ناگهانی نقدینگی»[3] مشاهده می‌شوند. در طرح‌های پانزی، با وعده سودهای غیرواقعی (گاه در حدود ۲۰ تا ۳۰ درصد سالانه یا بیشتر) سرمایه افراد جذب می‌شود و سود سرمایه‌گذاران قدیمی از محل سرمایه‌های جدید تأمین می‌گردد، بدون آن‌که پشتوانه‌ای از فعالیت اقتصادی واقعی وجود داشته باشد. برای نمونه، شرکت «فینیکو»[4] در روسیه طی حدود ۱۹ ماه نزدیک به ۱/۵ میلیارد دلار از سرمایه‌گذاران را با وعده سود ماهانه ۳۰ درصد جذب کرد، در حالی‌که این طرح فاقد هرگونه پایه اقتصادی معتبر بود. همچنین، فروپاشی صرافی «اف‌تی‌ایکس»[5] در سال ۲۰۲۲ در بسیاری از تحلیل‌ها به‌عنوان یکی از بزرگ‌ترین کلاهبرداری‌های پانزی در حوزه رمزارزها معرفی شده است. در شیوه نوظهور تخلیه ناگهانی نقدینگی، توسعه‌دهندگان یک پروژه رمزارزی پس از جذب سرمایه کافی و ایجاد ظاهری از اعتماد و رشد، به‌طور ناگهانی نقدینگی را از پروژه خارج کرده و ناپدید

---

۱. Scams

۲. Ponzi Schemes

۳. Rug Pull

٤. Finiko

٥. FTX

می‌شوند؛ در نتیجه، ارزش توکن برای سرمایه‌گذاران عادی تقریباً به صفر می‌رسد. بر اساس گزارش شرکت تحلیل بلاک‌چین[1] «چینالیسیس»[2]، تنها در سال ۲۰۲۱ حدود ۲٫۸ میلیارد دلار (معادل حدود ۳۵ درصد از کل کلاهبرداری‌های رمزارزی) از این طریق به سرقت رفته است. شبکه‌های اجتماعی بستر اصلی گسترش این کلاهبرداری‌ها محسوب می‌شوند. طبق داده‌های این پژوهش، اینستاگرام (۳۲٪)، فیسبوک (۲۶٪)، واتس‌اپ (۹٪) و تلگرام (۷٪) به‌ترتیب بیشترین سهم را در تسهیل و ترویج این طرح‌ها داشته‌اند (mdpi, ۲۰۲۳)[3]. به عنوان نمونه‌ای دیگر، می‌توان به توکن «اسکوید گیم»[4] اشاره کرد که یک پروژه کلاهبرداری بود و با سوءاستفاده از محبوبیت سریال نتفلیکس و وعده سودهای کلان، سرمایه‌گذاران را فریب داد. در این پروژه، سرمایه‌گذاران پس از خرید توکن عملاً قادر به فروش آن نبودند و توسعه‌دهندگان با دستکاری عمدی قیمت تا ۲٬۸۶۱ دلار، در نهایت با خارج کردن حدود ۳٫۳۸ میلیون دلار از استخر نقدینگی فرار کردند؛ اقدامی که منجر به سقوط قیمت توکن به حدود ۰٫۰۰۳ دلار در عرض تقریباً ده دقیقه شد (wired, ۲۰۲۱)[5]. این نمونه، به‌روشنی ظرفیت بالای بازار رمزارزها برای شکل‌گیری کلاهبرداری‌های سازمان‌یافته و تحمیل ضررهای سنگین و ناگهانی بر سرمایه‌گذاران خرد را نشان می‌دهد.

۱٫۳٫٤. نقد و بررسی

این چالش، هرچند بسیار جدی است، اما به‌طور مطلق غیرقابل‌کنترل به نظر نمی‌رسد و از جهاتی شبیه مشکلاتی است که در ابتدای ظهور هر فناوری نوینی (مانند اینترنت در دهه ۱۹۹۰ میلادی) مشاهده شده است. هرچند ماهیت غیرمتمرکز و فرامرزی رمزارزها امکان ریشه‌کنی کامل کلاهبرداری را از میان نمی‌برد، اما تجربه نشان داده است که با ترکیبی از آموزش، مقررات‌گذاری و به‌کارگیری فناوری‌های امنیتی، می‌توان حجم این پدیده را به‌طور قابل‌توجهی کاهش داد.

افزون بر این، طرح‌های پانزی و کلاهبرداری‌های مشابه، اختصاص به رمزارزها ندارند و در بازارهای سنتیِ تحت نظارت، مانند سهام و حتی مسکن نیز به‌کرات مشاهده شده‌اند. این واقعیت نشان می‌دهد که ریشه اصلی این چالش‌ها را باید بیش از آنکه در ذات یک فناوری خاص جست‌وجو کرد، در سوءاستفاده از اعتماد افراد و خلأهای نظارتی و آموزشی دانست. در این راستا، مهم‌ترین اقدامات برای مقابله با این چالش عبارت است از:

الف) آموزش و افزایش آگاهی عمومی

بسیاری از کاربران به دلیل ناآگاهی از سازوکارهای کلاهبرداری، فریب وعده‌های سودهای وسوسه‌انگیز را می‌خورند. ازاین‌رو، برگزاری دوره‌های آموزشی، تولید محتوای ساده و قابل‌فهم درباره ریسک‌های رمزارزها و نیز هشدارهای رسمی نهادهای نظارتی درباره پروژه‌های بدون‌مجوز و غیرشفاف ضرورت دارد. همچنین، کاربران باید پیش از سرمایه‌گذاری، درباره پروژه، تیم توسعه‌دهنده، اهداف، نقشه راه و

---

۱. Blockchain

۲. Chainalysis

۳. Cryptocurrency Risks, Fraud Cases, and Financial Performance

٤. Squid Game Token

٥. How a Squid Game Crypto Scam Got Away With Millions

وایت‌پیپر[۱] آن تحقیق کافی انجام دهند. راه‌اندازی وب‌سایت آموزشی «HoweyCoin» توسط کمیسیون بورس و اوراق بهادار آمریکا[۲]، با هدف آموزش شناسایی پروژه‌های کلاهبرداری به سرمایه‌گذاران، از نمونه‌های قابل‌توجه این نوع اقدامات است.

ب) شفاف‌سازی مالی و حسابرسی مستمر

برای مقابله با پروژه‌های پانزی که مدعی ایجاد «سود واقعی» هستند، اما از ارائه گزارش‌های مالی شفاف خودداری می‌کنند، دو سازوکار بنیادی اهمیت می‌یابد: « شفاف سازی مالی» و «حسابرسی مستمر». این امر شامل الزام پروژه‌ها به ارائه گزارش‌های مالی منظم (مثلاً سه‌ماهه[۳]) و انجام حسابرسی‌های دوره‌ای[٤] توسط شرکت‌های مستقل است تا امکان ارزیابی و صحه‌گذاری بر سلامت مالی پروژه برای سرمایه‌گذاران و نهادهای ناظر فراهم شود. در کنار این سازوکارهای سنتی، به‌کارگیری خود فناوری بلاک‌چین می‌تواند نقشی تحول‌آفرین ایفا کند؛ زیرا این فناوری امکان ثبت تراکنش‌های شفاف، تغییرناپذیر و قابل‌ردیابی را فراهم می‌آورد و قابلیت پنهان‌کاری یا دستکاری در داده‌ها را به حداقل می‌رساند. نمونه روشن این رویکرد، استیبل‌کوین‌های معتبری مانند USDC است که به‌طور منظم توسط نهادهای مستقلی همچون شرکت حسابرسی «گرنت تورنتون»[٥] حسابرسی می‌شوند و گزارش‌های ماهانه یا سه‌ماهه از میزان دارایی‌های ذخیره‌شده خود منتشر می‌کنند (cointelegraph, ۲۰۲٥)[٦]. این سطح از شفافیت برای سرمایه‌گذاران اطمینان ایجاد می‌کند که به ازای هر توکن منتشرشده، پشتوانه واقعی وجود دارد. نمونه دیگر، برخی پروژه‌های خیریه مبتنی بر بلاک‌چین است که با ثبت تمامی کمک‌های مالی و مسیر هزینه‌ها در یک دفترکل[۷] عمومی، این امکان را برای اهداکنندگان فراهم می‌کنند که مسیر دقیق کمک خود را به صورت برخط و با درجه بالایی از اطمینان ردیابی کنند. این سطح از شفافیت، علاوه بر تقویت اعتماد در بخش خیریه، با کاهش نگرانی‌ها نسبت به سوءمدیریت مالی و تقلب، افراد را به مشارکت گسترده‌تر ترغیب می‌نماید (qlicnfp, ۲۰۲٥)[۸].

ج) قانون گذاری و نظارت فعال

فقدان یا ضعف چارچوب‌های قانونی جامع در بسیاری از کشورها، فضای مناسبی برای فعالیت کلاهبرداران در حوزه رمزارزها ایجاد کرده است. برای سامان‌دهی این حوزه پیچیده، دو اقدام مکمل یعنی «قانون‌گذاری» و «نظارت فعال» ضروری است. این اقدامات شامل تدوین مقررات مشخص برای ثبت‌نام اجباری و نظارت مستمر بر صرافی‌ها و پروژه‌های رمزارزی، و نیز ایجاد نهادهای ناظر تخصصی با اختیارات کافی برای رصد بازار، شناسایی فعالیت‌های مشکوک و واکنش سریع به تخلفات است. نمونه‌هایی از این رویکرد در سطح بین‌المللی در حال شکل‌گیری است. اتحادیه اروپا با تصویب «مقررات جامع بازار دارایی‌های رمزنگاری‌شده»[۹]، در جهت ایجاد یک چارچوب یکپارچه قانونی پیشگام شده است. این مقررات، پروژه‌ها و صرافی‌ها را ملزم می‌کند برای فعالیت در کشورهای عضو مجوز بگیرند،

---

۱. «وایت‌پیپر» (White Paper)، سندی است که معمولاً توسط تیم توسعه‌دهنده یا بنیان‌گذاران یک پروژه رمزارزی منتشر می‌شود و در آن اهداف پروژه، فناوری مورد استفاده، سازوکار فنی شبکه، مدل اقتصادی و نحوه توزیع توکن‌ها تشریح می‌گردد تا سرمایه‌گذاران و کاربران بتوانند درباره آن پروژه ارزیابی آگاهانه‌تری داشته باشند.

۲. SEC

۳. Quarterly Reports

٤. Periodic Audit

٥. Grant Thornton

٦. How to read a stablecoin attestation report and why it matters.

۷. Distributed Ledger

۸. Blockchain for Charity Donations Explained

۹. MiCA

اطلاعات شفاف و کافی منتشر کنند، ذخایر خود را به‌طور منظم افشا و حسابرسی کنند و تضمین‌های لازم برای حفاظت از دارایی سرمایه‌گذاران ارائه دهند؛ هدف اصلی آن نیز کاهش هرج‌ومرج و ارتقای امنیت و اعتماد در بازار است. در آمریکا نیز کمیسیون بورس و اوراق بهادار نمونه‌ای از نظارت فعال و قضایی است. این نهاد به‌طور مستمر از اختیارات خود برای پیگرد قانونی پروژه‌های متخلف بهره می‌گیرد. برای نمونه، پرونده علیه شرکت Ripple به دلیل عرضه XRP به‌عنوان اوراق بهادارِ ثبت‌نشده (investopedia, ۲۰۲۵)[۱]، و نیز تعقیب قضایی پروژه‌های کلاهبرداری بزرگ مانند BitConnect (justice, ۲۰۲۲)[۲] و Forsage (justice, ۲۰۲۳)[۳] که مجموعاً میلیاردها دلار از سرمایه‌گذاران کلاهبرداری کرده‌اند، نشان‌دهنده عزم این نهاد برای اعمال قانون و ایجاد اثر بازدارنده است.

د) فناوری‌های شناسایی و هشدار زودهنگام

یکی از مؤثرترین شیوه‌ها برای مقابله با کلاهبرداری در بازار رمزارزها، بهره‌گیری از فناوری‌های شناسایی و هشدار زودهنگام[۴] است. بسیاری از این کلاهبرداری‌ها –از جمله طرح‌های پانزی– الگوهای رفتاری و تراکنشی نسبتاً ثابتی دارند؛ مانند افزایش ناگهانی و غیرعادی حجم معاملات بدون پشتوانه خبری معتبر، گردش سرمایه میان تعداد معدودی کیف‌پول، یا الگوهای تکرارشونده در دستکاری عمدی قیمت. با استفاده از هوش مصنوعی و تحلیل پیشرفته داده‌های آن‌چین[۵]، می‌توان این الگوها را شناسایی و تراکنش‌های مشکوک را ردیابی کرد. چنین سامانه‌هایی قادرند به‌صورت خودکار به کاربران و پلتفرم‌ها هشدارهای فوری ارسال کنند و آن‌ها را از خطرهای احتمالی آگاه سازند. برای نمونه، شرکت «چینالیسیس» با ارائه ابزارهایی مانند Chainalysis Reactor به نهادهای قانونی و صرافی‌ها کمک می‌کند تا با ردیابی جریان وجوه و شناسایی ارتباط کیف‌پول‌ها، طرح‌های پانزی را شناسایی کنند. همچنین، پلتفرم‌های هشدار خودکار (مانند Pocket Universe) با تحلیل رفتار کاربران و تراکنش‌ها، در لحظه هشدارهای بصری برای جلوگیری از امضای تراکنش‌های مشکوک ارائه می‌دهند. ربات‌های نظارت بر جامعه[۶] در بسترهایی مانند تلگرام نیز با تحلیل محتوای گروه‌ها، تبلیغات پروژه‌های نامعتبر را شناسایی و حذف کرده و به کاربران هشدار می‌دهند. این مجموعه فناوری‌ها مانند یک «سیستم ایمنی خودکار» برای اکوسیستم رمزارزها عمل می‌کنند و با تبدیل داده‌های خام به اطلاعات قابل‌اقدام، از دارایی کاربران در برابر کلاهبرداری‌های سازمان‌یافته محافظت می‌نمایند.

۴/۳/۲. ملاحظات فقهی ناظر به «کلاهبرداری‌های سازمان‌یافته» و راهکارهای مدیریت آن

کلاهبرداری‌های سازمان‌یافته در بازار رمزارزها به‌دلیل اتکای آن‌ها بر فریب سرمایه‌گذاران و انتقال ناصحیح اموال ایشان به نفع طراحان پروژه، از مصادیق بارز آسیب‌رسانی به دیگران به شمار می‌آید. در این موارد، با ایجاد تصویر اغراق‌آمیز از سودآوری و پنهان‌سازی واقعیت اقتصادی پروژه، زیان قابل‌توجهی بر دیگران تحمیل می‌شود و چنین رفتارهایی، به‌طور روشن، تحت نهی قاعده لاضرر قرار دارد. در این

---

۱. SEC v. Ripple: Key Court Decision and Impact on Cryptocurrency

۲. BitConnect Founder Indicted in Global $۲/٤ Billion Cryptocurrency Scheme

۳. Forsage Founders Indicted in ۳٤۰$M DeFi Crypto Scheme

٤. **Early Detection and Warning Systems**

۵. «داده‌های روی زنجیره» (On-chain Data) به تمامی اطلاعات و تراکنش‌هایی اطلاق می‌شود که به صورت عمومی و تغییرناپذیر روی یک بلاک‌چین ثبت و ذخیره شده‌اند. این داده‌ها برای همه قابل مشاهده و تأیید هستند و امکان دستکاری یا حذف آنها وجود ندارد.

٦. Community Moderation Bots

چارچوب، اقداماتی مانند ارتقای شفافیت مالی، حسابرسی مستقل، نظارت نهادی و استفاده از فناوری‌های شناسایی تقلب، می‌تواند به‌عنوان ابزارهایی برای کاهش امکان تحقق چنین ضرری ارزیابی شود.

بر فرض شمول قاعده نسبت به ضرر به خود، ورود غیرآگاهانه به پروژه‌هایی که نشانه‌های واضح کلاهبرداری دارند -از قبیل وعده سودهای غیرمتعارف، نبود شفافیت مالی یا فقدان اطلاعات معتبر درباره تیم اجرایی- می‌تواند زمینه‌ساز ضرر به خویشتن تلقی شود. در این صورت، آموزش کاربران، هشدارهای عمومی درباره پروژه‌های مشکوک و توسعه ابزارهای فنی برای تشخیص الگوهای تقلب، نقش مهمی در کاستن از احتمال گرفتار شدن افراد در این‌گونه ضررها خواهد داشت.

٤/٤. مسدود شدن حساب‌ها به دلیل تحریم کاربران

یکی دیگر از چالش‌های مهمی که می‌تواند زمینه طرح قاعده فقهی «لاضرر» در بازار رمزارزها را فراهم سازد، مسدود شدن دارایی کاربران کشورهای تحت تحریم -از جمله ایران- در صرافی‌های خارجی است. بسیاری از صرافی‌های بین‌المللی به‌منظور تبعیت از مقررات مبارزه با پول‌شویی[١] و احراز هویت مشتریان[٢] و نیز در نتیجه فشارهای فزاینده نهادهای نظارتی، ممکن است حساب کاربرانی را که از IP یا مدارک متعلق به این کشورها استفاده می‌کنند مسدود کرده یا دسترسی آنان به دارایی‌هایشان را محدود سازند. نمونه‌ای از این وضعیت در مورد کاربران ایرانی صرافی بایننس[٣] گزارش شده است؛ به‌گونه‌ای که شماری از آنان با پیام خطای «عدم امکان استفاده از خدمات صرافی»[٤] مواجه شده و حساب‌هایشان مسدود گردید (arzdigital, ٢٠٢٠)[٥]. این تجربه نشان می‌دهد که احتمال تکرار چنین اقداماتی در سایر صرافی‌های بین‌المللی نیز وجود دارد و حتی ممکن است در آینده با شدت و گستردگی بیشتری رخ دهد. اخیراً نیز صرافی بینگ‌ایکس[٦] کاربران ایرانی را در بازه زمانی ١۴ تا ١٩ آذر ١۴٠٣ (۴ تا ٩ دسامبر ٢٠٢۴) ملزم به تکمیل فرآیند «احراز هویت پیشرفته»[٧] کرده و اعلام نموده است که در صورت عدم انجام این فرایند در موعد مقرر، محدودیت‌های جدی برای حساب‌ها اعمال خواهد شد (ompfinex, ٢٠٢٤)[٨]. چنین اقداماتی نشان می‌دهد که کاربران ایرانی همواره با خطر مسدود شدن دارایی‌های خود مواجه‌اند و دسترسی پایدار به حساب‌هایشان تضمین‌شده نیست.

شواهد بین‌المللی نیز از تشدید این روند حکایت دارد. برای نمونه، هشدار رئیس بانک مرکزی اروپا درباره استفاده روسیه از رمزارزها برای دور زدن تحریم‌های مرتبط با جنگ اوکراین، به واکنش سریع نهادهای بین‌المللی از جمله گروه هفت[٩] و اتحادیه اروپا انجامید. در همین راستا، اتحادیه اروپا مقرراتی را تصویب کرد که ارائه خدمات کیف پول رمزارزی به شهروندان روس با دارایی بیش از ١٠٬٠٠٠ یورو را

---

١. AML

٢. KYC

٣. Binance

٤. Apologies but we are unable to provide services to you as per our Terms of Use.

٥. کد خبر: ١٦٨٤٢٣.

٦. BingX

٧. KYC

٨. Iranian Investors at Risk

٩. Gv

ممنوع می‌سازد. هم‌زمان، صرافی‌های بزرگ جهانی مانند کوین‌بیس[۱] و بایننس[۲] نیز با مسدودسازی ده‌ها هزار حساب کاربری روسی و اعمال محدودیت‌های گسترده، پایبندی خود را به این تحریم‌ها نشان دادند. افزون بر این، رویکرد قضایی برخی کشورها -از جمله انگلیس- در صدور دستور مسدودسازی دارایی‌های رمزارزی، بیانگر رسمیت یافتن روزافزون این سازوکارهای تحریمی است (nortonrosefulbright, ۲۰۲۲)[۳]. چنین اقداماتی حتی در مواردی رخ می‌دهد که کاربر هیچ فعالیت غیرقانونی انجام نداده و صرفاً به دلیل تابعیت یا محل سکونت خود با محدودیت مواجه شده است؛ وضعیتی که می‌تواند او را بی‌آنکه تقصیری مرتکب شده باشد در معرض زیان قرار دهد.

۱/٤/٤. نقد و بررسی

این چالش در سطح فردی تا حدی قابل‌مدیریت است؛ با این حال، در سطح کلان، ماهیتی آشکارا سیاسی دارد و حل‌وفصل آن منوط به لغو تحریم‌ها یا دستیابی به توافق‌های بین‌المللی است؛ امری که دست‌کم در کوتاه‌مدت، دور از انتظار به نظر می‌رسد. ازاین‌رو، نمی‌توان این مسأله را به‌طور کامل حل‌شده تلقی کرد. با وجود این، مجموعه‌ای از راهکارهای عملی برای کاهش احتمال آسیب‌پذیری کاربران وجود دارد که مهم‌ترین آن‌ها عبارتند از:

الف) استفاده از کیف پول‌های شخصی (غیرامانی)[٤]

نگهداری دارایی‌های دیجیتال در کیف‌پول‌های غیرامانی نظیر متامسک[٥]، تراست‌ولت[٦] یا لجر[۷] -که در آن‌ها کلیدهای خصوصی[۸] (رمزهای دسترسی به دارایی) منحصراً در اختیار کاربر قرار دارد- موجب می‌شود دارایی، مادامی که روی بلاکچین نگهداری می‌شود، از دسترس نهادهای ثالث (مانند صرافی‌ها یا نهادهای نظارتی) خارج بوده و امکان مسدودسازی آن به‌سادگی وجود نداشته باشد (culbertellis, ۲۰۲۵)[۹]. این شرایط دقیقاً مشابه آن است که بخواهند پول نقد موجود در گاوصندوق شخصیِ یک فرد را مسدود کنند. با این حال، باید تأکید کرد که این سطح از کنترل، به معنای مصونیت مطلق نیست. مخاطراتی همچون از دست دادن کلید خصوصی یا عبارت بازیابی، آسیب‌پذیری در برابر بدافزارها و کلاهبرداری‌های سایبری، و نیز غیرقابل‌بازگشت بودن تراکنش‌های ارسال‌شده به آدرس‌های نادرست، همگی از تهدیدات جدی این روش محسوب می‌شوند. ازاین‌رو، رعایت اصول امنیتی در نگهداری کلیدهای خصوصی و دقت مضاعف در انجام تراکنش‌ها، از الزامات بنیادین این راهکار است.

ب) استفاده از صرافی‌های غیرمتمرکز

---

۱. Coinbase
۲. Binance
۳. Cryptoassets and sanctions
٤. Non-Custodial Wallets
٥. MetaMask
٦. Trust Wallet
۷. Ledger
۸. Private Keys
۹. Crypto & Blockchain Frozen Accounts

این راهکار، به‌عنوان مکمل استفاده از کیف‌پول‌های شخصی، نقش مهمی در کاهش ریسک تحریم ایفا می‌کند. صرافی‌های رمزارز، بر اساس ساختار مدیریتی، به دو دسته کلی «متمرکز»[۱] و «غیرمتمرکز»[۲] تقسیم می‌شوند. صرافی‌های غیرمتمرکز -که عملکرد آن به گونه‌ای است که هیچ نهاد مرکزی یا سازمان واسطی بر آن نظارت ندارد- با استفاده از قراردادهای هوشمند، امکان معامله مستقیم و بدون واسطه[۳] را فراهم می‌کند. در مقابل، صرافی‌های متمرکز عملکردی مشابه بانک‌های سنتی دارند؛ به‌گونه‌ای که نگهداری دارایی‌ها و اجرای عملیات مالی در یک ساختار متمرکز و تحت کنترل صرافی انجام می‌شود. در مدل غیرمتمرکز، دارایی‌ها هرگز به مالکیت یا کنترل صرافی منتقل نمی‌شوند و همین امر، ریسک مسدودسازی یا اعمال محدودیت‌های ناشی از تحریم را به‌طور قابل‌توجهی کاهش می‌دهد (hedera, ۲۰۲٤)[٤]. برای نمونه، کاربری می‌تواند با اتصال کیف‌پول متامسک خود به صرافی غیرمتمرکز یونی‌سواپ[٥]، توکن USDT را به اتریوم[٦] تبدیل کند، بی‌آنکه نیازی به افتتاح حساب یا طی فرایند احراز هویت در یک صرافی متمرکز داشته باشد. با وجود این، این راهکار نیز خالی از چالش نیست و پیچیدگی‌های فنی آن، به‌ویژه برای کاربران مبتدی، می‌تواند مانعی جدی در استفاده مؤثر از این بسترها باشد.

ج) استفاده از صرافی‌های داخلی معتبر

در کشورهای تحت تحریم، از جمله ایران، صرافی‌های داخلی نظیر نوبیتکس[۷] به دلیل عدم ارتباط مستقیم با شبکه بانکی جهانی و نگهداری دارایی کاربران در کیف‌پول‌های داخلی، به‌طور مستقیم و فوری تحت تأثیر تحریم‌های بانکی بین‌المللی (نظیر قطع دسترسی به سوئیفت[۸]) قرار نمی‌گیرند (nobitex, ۲۰۲۲)[۹]. برای مثال، یک کاربر ایرانی می‌تواند از طریق کارت بانکی داخلی، وجه ریالی خود را به حساب کاربری در صرافی نوبیتکس واریز کرده، با آن بیت‌کوین خریداری کند و پس از فروش دارایی، مجدداً ریال دریافت نماید. این چرخه به‌طور کامل در داخل کشور و با استفاده از پول ملی انجام می‌شود.

با این حال، این صرافی‌ها با محدودیت‌های قابل‌توجهی از جمله نقدشوندگی پایین، کارمزدهای نسبتاً بالا و ریسک‌های امنیتی (نظیر ضعف پروتکل‌ها یا احتمال کلاهبرداری) مواجه‌اند. افزون بر این، تأمین نقدینگی و سازوکار قیمت‌گذاری آن‌ها غالباً به‌صورت غیرمستقیم به بازارهای جهانی و صرافی‌های خارجی وابسته است. ازاین‌رو، هرچند صرافی‌های داخلی می‌توانند در کوتاه‌مدت دسترسی کاربران به بازار رمزارز را تسهیل کنند، اما به دلیل این وابستگی غیرمستقیم و ریسک شناسایی، نمی‌توان آن‌ها را راهکاری بلندمدت و کاملاً مطمئن برای مقابله با آثار تحریم‌ها دانست.

د) استفاده از معاملات OTC[۱۰]

---

۱. CEX
۲. DEX
۳. Peer-to-Peer
٤. The Ins and Outs of Decentralized Exchanges (DEXs).
٥. Uniswap
٦. Ethereum
۷. Nobitex
۸. SWIFT
۹. Nobitex's response to the allegations made in the Reuters report
۱۰. Over The Counter

معاملات OTC در حوزه رمزارز -که از حیث کارکرد، مشابه معاملات «فرابورس» در بازارهای سنتی هستند- به شبکه‌هایی غیررسمی و مبتنی بر اعتماد اشاره دارند که در آن‌ها خریداران و فروشندگان، بدون واسطه صرافی و به‌صورت مستقیم با یکدیگر معامله می‌کنند (osl, ۲۰۲۵)[۱]. این معاملات معمولاً از طریق انتقال بانکی یا پرداخت نقدی انجام می‌شود و برای تراکنش‌های با حجم بالا مناسب‌تر است.

با وجود انعطاف‌پذیری این روش، معاملات OTC با چالش‌هایی جدی همراه‌اند؛ از جمله ریسک بالای کلاهبرداری، ضرورت اعتماد متقابل در فضایی غالباً ناشناس، و قیمت‌های بالاتر که ناشی از ریسک‌پذیری فروشنده در این نوع معاملات است.

هـ) فعالیت در اکوسیستم های بسته

برخی پروژه‌ها، مانند بازی‌های درآمدزایی مانند Axie Infinity یا پلتفرم‌های متاورسی همچون Decentraland، دارای اقتصاد داخلی نسبتاً مستقلی هستند که کاربران می‌توانند بدون تعامل مستقیم با صرافی‌های بین‌المللی، توکن‌های خاص آن اکوسیستم را کسب کرده و در بازار داخلی همان پلتفرم معامله کنند. برای مثال، کاربر می‌تواند با مشارکت در بازی Axie Infinity، توکن SLP[۲] به دست آورد و آن را در بازار داخلی بازی به سایر کاربران بفروشد (dappradar, ۲۰۲۱)[۳]. بدین‌ترتیب، دارایی وی هرگز در معرض صرافی‌های بین‌المللی قرار نمی‌گیرد.

با این حال، این راهکار نیز با محدودیت‌های اساسی مواجه است؛ از جمله وابستگی شدید به موفقیت پروژه (به‌گونه‌ای که در صورت شکست پروژه، ارزش دارایی‌ها ممکن است به صفر میل کند)، نقدشوندگی پایین دارایی‌های درون‌اکوسیستمی، سودآوری محدود و نیاز به صرف زمان قابل‌توجه. بنابراین، این روش نمی‌تواند جایگزین راهکارهای اصلی -مانند استفاده از کیف‌پول‌های شخصی و صرافی‌های غیرمتمرکز- محسوب شود، بلکه صرفاً می‌تواند نقش مکمل را ایفا کند.

۲/٤/٤. ملاحظات فقهی ناظر به «مسدود شدن حساب‌ها به دلیل تحریم کاربران» و راهکارهای مدیریت آن

با توجه به **مفاد** قاعده «لاضرر» که ناظر به منع **آسیب‌رسانی** به دیگران است، مسدود شدن دارایی کاربران در صرافی‌های خارجی، در اصل ناشی از تصمیمات تحریمی و سیاست‌های نهادهای بیرونی است و به‌طور مستقیم، در زمره **آسیب‌رسانی** کاربران به یکدیگر قرار نمی‌گیرد. ازاین‌رو، صرف استفاده از بسترهای معاملاتی رمزارزی، از این جهت، عنوان **ضرر** به غیر را بر رفتار معمول کاربران منطبق نمی‌سازد.

با این حال، بر فرض شمول قاعده نسبت به ضرر به خود، قرار دادن حجم قابل‌توجهی از دارایی در بسترهایی که با توجه به وضعیت تحریم و مقررات حاکم، احتمال مسدود شدن یا از دسترس خارج شدن آن‌ها قابل ملاحظه است، می‌تواند در مواردی زمینه ورود ضرر به مال شخص را فراهم آورد و در صورت بی‌توجهی به هشدارها و راه‌حل‌های جایگزین، به‌عنوان رفتاری غیرعقلایی بر ضرر خویش تلقی شود. در این چارچوب، ا ستفاده از کیف‌پول‌های غیرامانی، بهره‌گیری از صرافی‌های غیرمتمرکز و کاهش وابستگی به صرافی‌های خارجی، تدابیری عقلایی برای کاهش احتمال تحقق این نوع ضررهاست و به کارگیری آن‌ها می‌تواند در راستای پرهیز از آسیب‌رسانی به خود ارزیابی گردد.

---

۱. A Comprehensive Guide to Over-the-Counter Crypto Transactions

۲. Smooth Love Potion

۳. Axie Infinity Sparks Debates with New SLP Rewards Requirements

٤/٥. از دست دادن دارایی در اثر خطای کاربر

ویژگی برگشت‌ناپذیربودن تراکنش‌ها در کنار ماهیت غیرمتمرکز فناوری بلاک‌چین سبب شده است که مسئولیت حفظ و مدیریت این دارایی‌های دیجیتال به طور کامل بر عهده کاربر قرار گیرد. برخلاف نظام‌های مالی سنتی که در آن‌ها نهادهای متمرکز امکان مداخله و بازگرداندن دارایی را دارند، در این اکوسیستم مرجع مرکزی‌ای (مانند بانک) برای اصلاح خطا یا جبران خسارت وجود ندارد. در چنین شرایطی، خطاهای انسانی می‌تواند به از دست رفتن دائمی دارایی منجر شود. مهم‌ترین این خطاها را می‌توان در دو دسته اصلی طبقه‌بندی کرد:

الف) ارسال دارایی به آدرس اشتباه

این خطا معمولاً در اثر اشتباه در کپی یا وارد کردن آدرس گیرنده، یا بی‌دقتی در بررسی جزئیات تراکنش رخ می‌دهد. با توجه به ماهیت غیرمتمرکز و برگشت‌ناپذیر شبکه بلاک‌چین، در صورت ثبت چنین تراکنشی عملاً امکان بازگرداندن دارایی وجود ندارد و سرمایه ارسال‌شده برای همیشه از دسترس خارج می‌شود.

ب) فراموشی «رمز عبور» یا گم کردن «کلید خصوصی»

هرچند «رمز عبور» و «کلید خصوصی» هر دو برای دسترسی به دارایی‌ها استفاده می‌شوند، اما ماهیت آن‌ها متفاوت است. رمز عبور رشته‌ای از حروف و نمادهاست که کاربر برای ورود به یک سرویس یا نرم‌افزار (مانند اپلیکیشن کیف‌پول یا صرافی) انتخاب می‌کند و در بسیاری از موارد از طریق سازوکارهای بازیابی، مانند تأیید ایمیل یا پیامک، قابل بازیابی است. در مقابل، «کلید خصوصی» رشته‌ای بسیار طولانی از اعداد و حروف است که به‌صورت رمزنگاری‌شده تولید می‌شود و در واقع تنها مدرک مالکیت دارایی در شبکه بلاک‌چین به شمار می‌آید. از دست رفتن این کلید -یا عبارت بازیابی مرتبط با آن- به معنای از دست دادن کامل دارایی است؛ زیرا هیچ مرجع مرکزی برای بازیابی آن وجود ندارد. در چنین حالتی، دسترسی به سرمایه‌های دیجیتال برای همیشه مسدود می‌شود[1] و حتی پس از مرگ مالک نیز امکان انتقال آن به وراث وجود نخواهد داشت و دارایی عملاً «از دست‌رفته» تلقی می‌گردد (نک: tejaratnews, ۲۰۲۳)[2].

در حالی‌که در نظام‌های مالی متمرکز امکان بازیابی دسترسی از طریق فرایندهای احراز هویت فراهم است، در اکوسیستم غیرمتمرکز رمزارزها تمامی مسئولیت حفظ دسترسی به دارایی‌ها بر عهده کاربر قرار دارد و سازوکاری نهادی برای جبران خطاهای انسانی پیش‌بینی نشده است. این ویژگی، هرچند از مداخله یا سوءاستفاده نهادهای متمرکز جلوگیری می‌کند، اما در صورت سهل‌انگاری کاربران می‌تواند خطر از دست رفتن دارایی را به‌طور قابل توجهی افزایش دهد. گزارش‌ها نشان می‌دهد که حدود ۲۰ درصد از کل بیت‌کوین‌های استخراج‌شده -معادل چندین میلیارد دلار- به دلیل گم شدن کلیدهای خصوصی برای همیشه غیرقابل دسترسی شده‌اند (rockitcoin, ۲۰۲٤)[3]. این آمار به روشنی نشان می‌دهد که خطای انسانی می‌تواند یکی از مهم‌ترین منابع بروز زیان در اکوسیستم رمزارزها باشد.

١/٥/٤. نقد و بررسی

---

۱. برای درک بهتر تفاوت «کلید خصوصی» و «رمز عبور» می‌توان از تشبیه گاوصندوق استفاده کرد: کلید خصوصی همانند کلید فیزیکی اصلی یک گاوصندوق است که مالکیت و امکان دسترسی به محتویات آن را فراهم می‌کند؛ در صورتی که این کلید گم شود، هیچ مرجع مرکزی قادر به جایگزینی آن نیست و محتویات گاوصندوق عملاً برای همیشه از دسترس خارج می شود. در مقابل، رمز عبور بیشتر به کد امنیتی درِ ورودی یک ساختمان یا سیستم دزدگیر شباهت دارد؛ به این معنا که اگر کاربر آن را فراموش کند، معمولاً می‌تواند با مراجعه به ارائه‌دهنده خدمات و طی فرایند احراز هویت، آن را بازیابی یا تغییر دهد.

۲. کد خبر: ۸۳۹۱۵۹.

۳. How Many Bitcoins Are Left to Mine?

هرچند غیرقابل‌برگشت بودن تراکنش‌ها و خطر از دست دادن کلید خصوصی در نگاه نخست چالش‌هایی جدی و حتی بازدارنده به نظر می‌رسند، اما بررسی دقیق‌تر نشان می‌دهد که این مسائل تا حد زیادی قابل مدیریت و کنترل هستند. جامعه بلاک‌چین به‌صورت مستمر در حال توسعه ابزارها و راهکارهایی برای کاهش این ریسک‌هاست و تجربه عملی نیز نشان می‌دهد که «خطای کاربر» بیش از آنکه ناشی از نقص فنی باشد، ریشه در کمبود آموزش و ضعف در تجربه کاربری دارد. با به‌کارگیری تدابیر مناسب، می‌توان احتمال بروز این خطاها را به حدی کاهش داد که برای بخش قابل توجهی از کاربران به مسئله‌ای نادر تبدیل شود. مهم‌ترین این راهکارها عبارت‌اند از:

الف) آدرس‌های هوشمند و تشخیص خطا[۱]

بسیاری از کیف‌پول‌های مدرن به قابلیت تشخیص آدرس‌های نامعتبر یا متعلق به شبکه‌ای دیگر مجهز شده‌اند. برای نمونه، اگر کاربر قصد ارسال دارایی در شبکه اتریوم را به آدرسی متعلق به شبکه بیت‌کوین داشته باشد، کیف‌پول به‌صورت خودکار هشدار صادر می‌کند (نک: tencentcloud, ۲۰۲۵)[۲]. این قابلیت، به‌عنوان یک لایه حفاظتی پیشگیرانه، نقش مؤثری در کاهش خطاهای انسانی ایفا می‌کند.

ب) استاندارد چکسام[۳] در آدرس‌ها

آدرس‌های مدرن رمزارزها معمولاً از سازوکار «چکسام» بهره می‌برند که امکان شناسایی خطاهای تایپی را فراهم می‌کند. هنگام وارد کردن آدرس، کیف‌پول اعتبار چکسام را بررسی می‌کند و در صورت وجود حتی یک کاراکتر اشتباه، از انجام تراکنش جلوگیری می‌شود (نک: learnmeabitcoin, ۲۰۲۵)[۴]. این مکانیزم ساده اما کارآمد، از بخش قابل توجهی از اشتباهات ناخواسته کاربران جلوگیری می‌کند.

ج) نام‌سرویس‌ها[۵]

سرویس‌های نام مانند «سرویس نام اتریوم» راه‌حلی ساده و کاربردی برای مشکل آدرس‌های طولانی و پیچیده ارائه می‌دهند. این سرویس‌ها امکان جایگزینی آدرس‌های معمولی -که ترکیبی طولانی و نامفهوم از حروف و اعداد هستند- را با یک نام خوانا و قابل به خاطرسپردن فراهم می‌کنند (ledger, ۲۰۲٤)[٦]. برای مثال، به جای استفاده از آدرس اصلی کیف پول: ۰x٤cbe٥٨c٥٠٤٨٠e٥٤١b٧c٤e٧a٦٧d٣c٥e٨b٩a٠f١d٢b می‌توان از نام ساده‌ای همچون john.eth استفاده کرد. بدیهی است که وارد کردن یک نام کوتاه، در مقایسه با یک رشته ۴۲ کاراکتری، احتمال خطا را به‌طور محسوسی کاهش می‌دهد.

د. کیف پول‌های امانی[۷]: کیف‌پول‌های رمزارزی بر اساس نحوه مدیریت کلید خصوصی به دو دسته «امانی» (حضانتی) و «غیرامانی» (غیرحضانتی) تقسیم می‌شوند. در کیف‌پول‌های امانی-مانند صرافی‌ها و برخی وب‌اپلیکیشن‌ها- کلید خصوصی توسط یک نهاد واسط نگهداری و مدیریت می‌شود. این مدل برای کاربران مبتدی مناسب‌تر است، زیرا مسئولیت حفاظت از کلید خصوصی بر عهده شخص

---

۱. Error Detection

۲. How to verify the address of a digital wallet?

۳. checksum

٤. Checksum, Simple error detection.

٥. Name Services

٦. Domain Name Service meaning

۷. Custodial Wallets

ثالث قرار دارد و امکان بازیابی حساب از طریق پشتیبانی فراهم است. در مقابل، در کیف‌پول‌های غیرامانی-مانند تراست‌ولت[1]- کلید خصوصی مستقیماً در اختیار کاربر قرار می‌گیرد و هیچ شخص یا نهاد دیگری به دارایی‌ها دسترسی ندارد. این رویکرد امنیت بالاتری در برابر نفوذ یا سوءاستفاده فراهم می‌کند، اما مسئولیت کامل نگهداری کلید خصوصی را نیز بر عهده کاربر می‌گذارد و در صورت از دست رفتن آن، امکان بازیابی وجود نخواهد داشت (crypto, ۲۰۲۲)[2].

از آنجا که کلید خصوصی رشته‌ای طولانی و پیچیده است، کیف‌پول‌های غیرامانی معمولاً آن را در قالب «عبارت بازیابی» ارائه می‌کنند؛ مجموعه‌ای متشکل از ۱۲، ۱۸ یا ۲۴ کلمه تصادفی که شکل قابل‌خواندن و قابل‌حفظ کلید خصوصی محسوب می‌شود. هر شخصی که به این عبارت دسترسی داشته باشد، قادر خواهد بود کلید خصوصی را بازسازی کرده و به دارایی‌ها دست یابد. ازاین‌رو، حفاظت از عبارت بازیابی اهمیتی هم‌سنگ با حفاظت از خود کلید خصوصی دارد. این عبارت در مواقعی مانند حذف اپلیکیشن کیف‌پول، خرابی یا تعویض دستگاه، یا انتقال کیف‌پول به دستگاه جدید، نقش حیاتی در بازیابی دارایی‌ها ایفا می‌کند.

بدین‌ترتیب، کاربران با یک انتخاب راهبردی مواجه‌اند: استفاده از کیف‌پول‌های امانی، که تجربه‌ای ساده‌تر و شبیه به نظام بانکی سنتی فراهم می‌کند و برای افراد کم‌تجربه مناسب‌تر است؛ یا استفاده از کیف‌پول‌های غیرامانی، که کنترل و استقلال کامل را در اختیار کاربر قرار می‌دهد، اما مستلزم پذیرش مسئولیت کامل نگهداری عبارت بازیابی است. این عبارت باید در مکانی کاملاً امن -ترجیحاً به‌صورت فیزیکی و خارج از فضای دیجیتال- نگهداری شود، زیرا افشا یا گم شدن آن به معنای از دست رفتن دائمی دارایی‌ها خواهد بود.

با وجود مزایای مدل امانی، این رویکرد به دلیل ماهیت متمرکز خود با ریسک‌های جدی همراه است؛ از جمله خطر هک شدن صرافی، مسدود شدن حساب‌ها به دلایل تحریمی یا سیاسی، بروز مشکلات نقدینگی، یا حتی ورشکستگی نهاد ارائه‌دهنده خدمات. نمونه شاخص این ریسک‌ها، ورشکستگی صرافی FTX در نوامبر ۲۰۲۲ بود که به دلیل سوءمدیریت، فقدان شفافیت و بحران نقدینگی رخ داد. در پی این حادثه، صدها هزار کاربر که دارایی‌های خود را در کیف‌پول‌های امانی این صرافی نگهداری می‌کردند، دسترسی به سرمایه‌هایشان را از دست دادند و میلیاردها دلار از دارایی‌ها بلوکه شد؛ به‌گونه‌ای که بسیاری از آن‌ها تاکنون تنها بخش اندکی از سرمایه خود را بازیابی کرده‌اند (investopedia, ۲۰۲٤)[3].

هـ) توسعه راهکارهای بازیابی[4]

برای کاهش ریسک گم شدن کلید خصوصی، برخی کیف‌پول‌های غیرمتمرکز مدرن به سمت پیاده‌سازی سازوکارهای بازیابی نسبتاً امن و بدون نیاز به اعتماد به نهاد متمرکز حرکت کرده‌اند. در این مدل‌ها، کاربر می‌تواند چند فرد مورد اعتماد یا دستگاه‌های شخصی امن خود را به‌عنوان «نگهبانان بازیابی»[5] تعیین کند. کلید بازیابی به‌صورت رمزگذاری‌شده میان این نگهبانان توزیع می‌شود و هیچ‌کدام به‌تنهایی به آن دسترسی ندارند. در صورت از دست رفتن دسترسی، کاربر با دریافت تأییدیه از تعداد مشخصی از نگهبانان (مثلاً ۳ نفر از ۵ نفر)

---

۱. Trust Wallet

۲. Custodial Wallets vs. Non-Custodial Wallets: What's the Difference?

۳. The Collapse of FTX: What Went Wrong With the Crypto Exchange?

٤. Recovery Solutions

٥. Recovery Guardians

می‌تواند کلید جدیدی ایجاد کرده و دارایی‌های خود را بازیابی کند. کیف‌پول «آرجنت»[1] در شبکه اتریوم نمونه‌ای شاخص از اجرای نسبتاً موفق این رویکرد است (نک: cryptonary, ۲۰۲۵)[2].

و) راهکارهای عملی و احتیاط‌های شخصی

در کنار راهکارهای فناورانه، رعایت برخی اصول ساده اما بنیادین توسط کاربران نقش تعیین‌کننده‌ای در کاهش خطاها دارد. از جمله:

نخست، دقت مضاعف در وارد کردن آدرس مقصد، شامل استفاده از قابلیت کپی-پیست و بررسی چند کاراکتر ابتدایی و انتهایی آدرس؛

دوم، نگهداری امن کلید خصوصی و عبارت بازیابی، ترجیحاً به‌صورت فیزیکی و دور از فضای دیجیتال؛

سوم، استفاده از کیف‌پول‌های سخت‌افزاری که با ذخیره کلید خصوصی در یک تراشه امن و جدا از اینترنت، بالاترین سطح حفاظت را در برابر حملات سایبری و بدافزارها فراهم می‌کنند؛

چهارم، ارسال تراکنش آزمایشی با مبلغ اندک برای آدرس‌های جدید یا ناشناخته، به‌منظور اطمینان از صحت آدرس و عملکرد شبکه پیش از انتقال مبالغ اصلی.

۲/۵/٤. ملاحظات فقهی ناظر به «از دست دادن دارایی در اثر خطای کاربر» و راهکارهای مدیریت آن

با توجه به مبنای قاعده «لاضرر» که متوجه منع آسیب‌رسانی به دیگران است، ویژگی‌هایی مانند برگشت‌ناپذیری تراکنش‌ها یا لزوم نگهداری شخصی کلید خصوصی، به خودی خود، مصداق ضرر زدن به غیر محسوب نمی‌شود؛ زیرا زیانی که در مواردی مانند ارسال اشتباه دارایی یا گم شدن کلید خصوصی رخ می‌دهد، غالباً نتیجه خطا یا سهل‌انگاری خود کاربر است و به شخص ثالثی تحمیل نمی‌شود. در عین حال، در مواردی که ارائه‌دهندگان خدمات رمزارزی –مانند صرافی‌ها یا توسعه‌دهندگان کیف‌پول– با بی‌توجهی به اصول طراحی ایمن، نادیده گرفتن استانداردهای متعارف امنیتی یا اطلاع‌رسانی ناکافی نسبت به ریسک‌ها، زمینه ورود ضرر قابل پیش‌بینی به کاربران را فراهم کنند، می‌توان این وضع را مصداقی از آسیب‌رسانی به غیر دانست و از این جهت، پرهیز از چنین کوتاهی‌هایی لازم خواهد بود.

از سوی دیگر، بر فرض توسعه مفاد قاعده به ضرر به خود، بی‌احتیاطی در نگهداری کلید خصوصی یا بی‌دقتی در انجام تراکنش‌ها –با توجه به احتمال از دست رفتن غیرقابل جبران دارایی– در برخی موارد می‌تواند تحت عنوان ضرر زدن به مال خویش قرار گیرد؛ به‌ویژه زمانی که مخاطرات برای کاربر شناخته‌شده و قابل‌اجتناب است. در این چارچوب، بهره‌گیری از ابزارهایی مانند سرویس‌های نام، سازوکارهای تشخیص خطا، نگهداری امن عبارت بازیابی، استفاده از کیف‌پول‌های سخت‌افزاری و انجام تراکنش آزمایشی، در شمار تدابیر عقلایی برای پیشگیری از ضرر قابل پیش‌بینی به خود قرار می‌گیرد.

۵. جایگاه رمزارز در منظومه علّی ضررهای معاملاتی

بررسی چالش‌های معاملات رمزارزها نشان می‌دهد که این حوزه با طیفی از ضررها همراه شده است؛ از نوسانات شدید قیمت و دست‌کاری بازار گرفته تا کلاهبرداری‌های سازمان‌یافته، مسدود شدن دارایی‌ها و از دست رفتن سرمایه‌ها در اثر خطاهای معاملاتی. با این حال، تحلیل فقهی این پدیده‌ها بدون تشخیص دقیق منشأ ضرر و تعیین جایگاه رمزارز در فرایند ایجاد یا تشدید آن‌ها کامل نخواهد

---

۱. Argent Vault

۲. How to Use Argent Wallet

بود. به‌ویژه با پذیرش این مبنا که قاعده «لا ضرر و لا ضرار» ناظر به نهی تحریمی از آسیب‌رسانی است، تبیین نسبت میان فاعل ضرر، رفتار زیان‌بار و بستر معاملاتی اهمیت می‌یابد؛ زیرا صرف همراهی یک فناوری با تحقق ضرر برای انتساب عنوان نهی به آن کافی نیست، مگر آنکه رفتار یا سازوکار مرتبط با آن عرفاً مصداق اضرار تلقی شود.

مطالعه آسیب‌های رایج در معاملات رمزارزی نشان می‌دهد که در بخش قابل توجهی از موارد، زیان‌ها ریشه در اختلال‌های پیشینی بازار دارد؛ از جمله فقدان شفافیت اطلاعاتی، ضعف نظارت، کاستی‌های آموزش مالی و اتکای معامله‌گران به منابع غیرحرفه‌ای. در چنین مواردی، رمزارز بیشتر به‌عنوان عاملی تقویت‌کننده برای ریسک‌های موجود عمل می‌کند، نه منشأ استقلالی ضرر. از این رو، مقتضای قاعده لاضرر در این سطح، معطوف به رفع موجبات اضرار در ساختار بازار، تقویت شفافیت و کاهش زمینه‌های سوءاستفاده است، به‌گونه‌ای که ارزیابی فقهی ناظر به رفتارهای زیان‌بار و شیوه‌های نادرست تعامل با این پدیده باشد، نه اصل وجود آن.

در مواردی دیگر، بخشی از خسارت‌ها ناشی از ناپختگی کاربران، خطاهای فنی و فقدان مهارت در استفاده از ابزارها و پلتفرم‌های معاملاتی است؛ مانند ارسال اشتباه تراکنش، استفاده از صرافی‌های غیرمعتبر یا اعتماد به پروژه‌های فاقد پشتوانه. این زیان‌ها غالباً ریشه در ضعف مهارت معاملاتی و نبود استانداردهای حداقلی دارد و رمزارز در این موارد بیشتر ظرف ظهور چنین رفتارهایی است. از منظر قاعده لاضرر، هرگاه این رفتارها عرفاً مصداق آسیب‌رسانی به دیگری یا حتی به خود فاعل تلقی شود، عنوان نهی بر آن مترتب می‌گردد؛ اما صرف احتمال خطا یا پذیرش ریسک‌های متعارف برای شمول قاعده کافی نیست.

در مقابل، در برخی حوزه‌ها –مانند طرح‌های پانزی مبتنی بر توکن، عرضه دارایی‌های فاقد پشتوانه، سیگنال‌فروشی‌های فریبکارانه و دست‌کاری عمدی قیمت– ساختار یا شیوه تعامل با رمزارز می‌تواند زمینه تحقق آسیب‌رسانی بالفعل را فراهم آورد. ویژگی‌هایی مانند سهولت ایجاد دارایی‌های غیرواقعی، نبود الزام به افشای اطلاعات یا امکان خروج ناگهانی سرمایه در مقیاس گسترده، می‌تواند وضعیتی پدید آورد که عرفاً عنوان آسیب‌رسانی بر آن صدق کند. در این موارد، قاعده لاضرر ناظر به منع یا محدودسازی رفتارها و سازوکارهایی است که وصف آسیب‌رسانی در آن‌ها تحقق یافته است؛ نه به اعتبار ماهیت رمزارز، بلکه به سبب شیوه‌های زیان‌بار بهره‌گیری از آن.

برآیند این تحلیل آن است که قاعده «لاضرر» حکم واحدی درباره همه معاملات رمزارزی ارائه نمی‌کند، بلکه چارچوبی فراهم می‌آورد که در آن هر رفتار یا سازوکار معاملاتی به میزان تحقق معیار آسیب‌رسانی موضوع نهی قرار می‌گیرد. بر این اساس، از یک سو باید زمینه‌های ساختاری مؤثر در ایجاد یا تشدید ضرر اصلاح شده و آموزش، شفافیت و نظارت تقویت گردد؛ و از سوی دیگر، مواردی که سازوکار خاص معامله عرفاً بستر آسیب‌رسانی به‌شمار می‌آید، مورد منع یا تنظیم‌گری متناسب قرار گیرد.

بنابراین، تحلیل پیش‌گفته به معنای نفی جریان قاعده لاضرر در معاملات رمزارزی نیست؛ بلکه شمول نهی تحریمی قاعده تابع تحقق عنوان «ضرر» است. هرجا رفتار یا سازوکار معاملاتی در این حوزه مصداق آسیب‌رسانی قابل‌اعتنا باشد، قاعده مقتضی منع یا کنترل آن خواهد بود؛ امری که بسته به نوع معامله و شرایط تحقق ضرر، نیازمند ارزیابی موردی خواهد بود.

نتایج و یافته‌ها

بررسی چالش‌های معاملاتی در حوزه رمزارز نشان می‌دهد که زیان‌های پدیدآمده در این عرصه، از خاستگاه واحدی نشأت نمی‌گیرند؛ بلکه در سطوح متفاوتی شکل می‌گیرند که هر یک نیازمند تبیین مستقل است. در پرتو قاعده «لاضرر» –که بر نهی از هرگونه آسیب‌رسانی دلالت دارد– می‌توان این گونه‌های اضرار را در سه سطح اصلی صورت‌بندی کرد:

۱. **سطح رفتارهای آسیب‌زا:** در این سطح، رفتارهایی قرار می‌گیرند که ماهیت آن‌ها مستقیماً متضمن آسیب‌رسانی به دیگران است؛ مصادیقی همچون دستکاری بازار، طرح‌های کلاهبرداری سازمان‌یافته (مانند پانزی) و سازوکارهای فریبنده‌ای که با هدف انتقال ناصحیح دارایی دیگران طراحی می‌شوند. در این موارد، عنصر «ضرر» به‌روشنی در فعل عامل حضور دارد و از همین رو، بی‌تردید مشمول نهی تحریمی قاعده لاضرر قرار می‌گیرد.

۲. **سطح نارسایی‌های ساختاری و شرایط پیرامونی:** این سطح شامل مخاطراتی است که از ویژگی‌های ساختاری بازار رمزارزها و شرایط بیرونی اثرگذار بر آن نشأت می‌گیرد؛ مواردی همچون نوسانات شدید قیمت، ضعف چارچوب‌های نظارتی، و محدودیت‌های برون‌مرزی (مانند انسداد حساب‌ها به دلیل تحریم). نکته کلیدی در این سطح آن است که زیان‌های احتمالی، بیش از آنکه ناشی از رفتار متعاملین نسبت به یکدیگر باشد، به ماهیت فنی بازار و عوامل محیطی بازمی‌گردد؛ با این حال، به نظر می‌رسد با توجه به جهت‌گیری قاعده لاضرر در رفع زمینه‌های بروز ضرر، این قاعده اقتضا دارد که دولت و نهادهای قانون‌گذار با تدوین مقررات صیانتی، تقویت نظارت بر پلتفرم‌ها و ارتقای شفافیت، در جهت رفع زمینه‌های ورود ضرر به شهروندان اقدام کنند.

۳. **سطح آسیب‌های ناشی از خطای کاربر:** در این سطح، زیان‌ها عمدتاً از رفتار و خطای خود کاربران ناشی می‌شود؛ مواردی مانند بی‌دقتی در تراکنش‌ها، نگهداری ناامن کلیدهای خصوصی یا ورود غیرآگاهانه به معاملات پرریسک. این سنخ از زیان‌ها غالباً متضمن آسیب‌رسانی به دیگران نیستند، هرچند در صورت پذیرش شمول قاعده لاضرر نسبت به «ضرر به خود»، می‌توانند از این حیث نیز موضوع تأمل فقهی قرار گیرند. در این وضعیت، آموزش عمومی و به‌کارگیری تدابیر احتیاطی، کارآمدترین راهکار پیشگیرانه خواهد بود.

نتیجه‌گیری راهبردی:

بر این اساس، تحلیل فقهی معاملات رمزارز بیش از آنکه متکی بر یک داوری کلی درباره اصل این پدیده باشد، نیازمند واکاوی منشأ و نحوه تحقق ضرر در هر مورد است. از منظر قاعده لاضرر، آنچه موضوع نهی قرار می‌گیرد، تحقق رفتارهای متضمن آسیب‌رسانی است که ارزیابی آن در هر یک از سطوح یادشده، نیازمند بررسی موردی خواهد بود.

در همین چارچوب، قاعده «لاضرر» را می‌توان نه صرفاً یک قاعده محدودکننده، بلکه راهنمایی برای «تنظیم‌گری» روابط اقتصادی تلقی کرد. مفاد این قاعده نشان می‌دهد که مواجهه با پدیده‌های نوظهوری همچون رمزارزها، لزوماً در قالب «منع کلی و تقلیل‌گرایانه» خلاصه نمی‌شود؛ بلکه می‌تواند به شکل یک سیاست‌گذاری چندلایه تجلی یابد؛ رویکردی که از سویی از حقوق اشخاص در امنیت دارایی حمایت کند و از سوی دیگر، مصالح عمومی جامعه نظیر ثبات اقتصادی و صیانت از نظم مالی را در برابر مخاطرات ساختاری حفظ نماید.

کتابنامه

قرآن کریم

ازهری، محمد (۱٤۲۱ق). ***تهذیب اللغة***. بیروت: دار إحیاء التراث العربی.

انصاری، مرتضی (۱۳۷۷). ***فرائد الأصول***. قم: مجمع الفکر الإسلامی.

انصاری، مرتضی (۱٤۱۱ق). ***کتاب المکاسب***. قم: دار الذخائر.

ایروانی، محمدباقر (۱٤۳۲ق). ***دروس تمهیدیّة في القواعد الفقهیّة***. قم: دار الفقه للطباعة و النشر.
تفتازانی، مسعود (بی‌تا). ***مختصر المعانی***. بی‌جا: دار الفکر.
حائری، سیدکاظم (بی‌تا). ***مباحث الأصول (القسم الثانی)***. بی‌جا: بی‌نا.
حرعاملی، محمد (۱٤۰۹ق). ***تفصیل وسائل الشیعة إلی تحصیل مسائل الشریعة***. قم: مؤسسة آل‌البیت علیهم‌السلام.
حسینی‌سیستانی، سیدعلی (بی‌تا). ***قاعدة لاضرر و لاضرار***. بی‌جا: مکتب آیة‌اللّه‌العظمی السید السیستانی.
حسینی‌مراغی، سیدعبدالفتاح (۱٤۱۷ق). ***العناوین الفقهیة***. قم: مؤسسة النشر الإسلامی التابعة لجماعة المدرسین.
خویی، سیدابوالقاسم (۱۳٦۸). ***محاضرات فی أصول الفقه***. قم: انصاریان. تفتازانی، مسعود (بی‌تا). مختصر المعانی. بی‌جا: دار الفکر.
خویی، سیدابوالقاسم (۱٤۱۳ق). ***مصباح الأصول***. قم: موسسة إحیاء آثار الإمام الخونی.
خویی، سیدابوالقاسم (۱٤۱۷ق). ***الهدایة فی الأصول***. تقریر صافی‌اصفهانی. قم: مؤسسه فرهنگی صاحب الأمر(عج).
سبحانی‌تبریزی، جعفر (۱٤۲۰ق). ***نیل الوطر من قاعدة لاضرر***. تقریر سبحانی. قم: مؤسسه امام صادق علیه‌السلام.
سیوطی، جلال‌الدین (۱۳۸۹ق). ***تنویر الحوالك شرح علی موطأ مالك***. مصر: المکتبة التجاریة الکبری.
سیوطی، جلال‌الدین (۱٤۳۰ق). ***البهجة المرضیة علی ألفیة ابن مالک***. قم: اسماعیلیان.
شریعت‌اصفهانی، فتح‌اللّه (بی‌تا). ***قاعدة لاضرر***. قم: مؤسسة النشر الاسلامی التابعة لجماعة المدرسین.
شهیداول، محمدبن‌مکی (۱٤۰۰ق). ***القواعد و الفوائد فی الفقه و الأصول و العربیة***. قم: مفید.
صدوق، محمدبن‌علی (۱٤۱۳ق). ***من لایحضره الفقیه***. قم: دفتر انتشارات اسلامی وابسته به جامعه مدرسین حوزه علمیه قم.
طباطبایی‌حکیم، سیدمحسن (۱٤۱٦ق). ***مستمسک العروة الوثقی***. قم: دار التفسیر.
طباطبایی‌یزدی، سیدمحمدکاظم (۱۳۷۰). ***حاشیة المکاسب***. قم: مؤسسة إسماعیلیان.
طوسی، محمدبن‌حسن (بی‌تا). ***الخلاف***. قم: مؤسسة النشر الإسلامی التابعة لجماعة المدرسین.
عابدیان‌کلخوران، سیدحسن؛ کریمی‌وردنجانی، مریم (۱٤۰۲). «م.شروعیت ا ستخراج بیت‌کوین با دقت در م.صادیق و قواعد فقهی آن». ***قانون‌یار***، سال۷، شماره۲۷، صص ۳٦۷-۳۸۷.
عراقی، ضیاءالدین (۱٤۱۱ق). ***منهاج الأصول***. بیروت: دار البلاغة.
عراقی، ضیاءالدین (۱٤۱۸ق). ***قاعدة لاضرر و لاضرار***. قم: مکتب الإعلام الإسلامی.
غروی‌اصفهانی، محمدحسین (۱٤۱٤ق). ***نهایة الدرایة في شرح الکفایة***. قم: مؤسسة آل‌البیت علیهم‌السلام لإحیاء التراث.
غروی‌نایینی، محمدحسین (۱۳۷۳ق). ***منیة الطالب فی حاشیة المکاسب***. تقریر نجفی‌خوانساری. تهران: المکتبة المحمدیة.
غفوری‌نژاد، محمد (۱۳۹۹). «مفهوم‌شناسی ضرر و ضرار». ***پژوهش‌های اصولی***. سال۷، شماره۲۵.
کلینی، محمدبن‌یعقوب (۱٤۰۷ق). ***الکافی***. تهران: دار الکتب الإسلامیة.
محقق‌داماد، سیدمصطفی (۱٤۰۱). ***قواعد فقه (بخش مدنی)***. تهران: مرکز نشر علوم اسلامی.
مکارم‌شیرازی، ناصر (۱۳۷۰). ***القواعد الفقهیة***. قم: مدرسة الإمام علی‌بن‌أبی‌طالب علیه‌السلام.
موسوی‌بجنوردی، سیدحسن (۱۳۷۷). ***القواعد الفقهیة***. قم: الهادی.
موسوی‌خمینی، سیدروح‌اللّه (۱٤۲۳ق). ***تهذیب الأصول***. تقریر سبحانی‌تبریزی. بی‌جا: مؤسسة تنظیم و نشر آثار الإمام الخمیني(ره).
نجفی، محمدحسن (۱۳٦۲). ***جواهر الکلام فی شرح شرائع الإسلام***. بیروت: دار إحیاء التراث العربی.
نراقی، احمد (۱٤۱۷ق). ***عوائد الأیام فی بیان قواعد الأحکام و مهمات مسائل الحلال و الحرام***. قم: دفتر تبلیغات اسلامی حوزه علمیه قم.
نورمفیدی، سیدمجتبی، ***درس خارج فقه***، دسترسی در ۱۳۹۳/۱۱/۲۱: https://www.m-noormofidi.com
هادوی‌تهرانی، مهدی، ***درس خارج اصول***، دسترسی در ۱٤۰۲/۰۸/۲۰: https://www.eshia.ir

https://www.arzdigital.com
https://www.cointelegraph.com
https://www.crypto.news

https://www.cryptonary.com
https://www.culbertellis.com
https://www.dappradar.com
https://www.hedera.com
https://www.investopedia.com
https://www.justice.gov
https://www.learnmeabitcoin.com
https://www.ledger.com
https://www.mdpi.com
https://www.nobitex.ir
https://www.nortonrosefulbright.com
https://www.ompfinex.com
https://www.osl.com
https://www.qlicnfp.com
https://www.rockitcoin.com
https://www.seo.ir
https://www.tejaratnews.com
https://www.tencentcloud.com
https://www.trends.google.com
https://www.wired.com