New Research in Islamic Humanities Studies Online ISSN: 2980 - 8944
Homepage: //https: /api.lu.ac.ir
Lorestan University

Pathology and evaluation of a rational digital deterrence approach to counterfeiting and fraud crimes in the field of cryptocurrencies

Rasoul Shamsi[1], Ismail Abdollahi *[2], Maryam Safaei[3]

[1] PhD student, Department of Law, Bushehr Branch, Islamic Azad University, Bushehr, Iran, Email: rasoulshamsi41@yahoo.com

*[2.] Corresponding Author, Assistant Professor, Department of Law, Bushehr Branch, Islamic Azad University, Bushehr, Iran, Email: e.abdolahi@iaubushehr.ac.ir

[3.] Assistant Professor, Department of Law, Bushehr Branch, Islamic Azad University, Bushehr, Iran, Email: Maryamsafae@iaubushehr.ac.ir

Article Info

Article type:
Research Article

Article History:
Received 20 October 2023
Received in revised form 20 December 2023
Accepted 6 January 2024
Available online 25 March 2024

Keywords:
Cryptocurrency, technological prevention, counterfeiting, fraud, rational digital deterrence

ABSTRACT

Research Objective: This research aims to identify infrastructure vulnerabilities and legal gaps in the field of cryptocurrencies, as well as to examine the effects of related crimes on privacy, cybersecurity, and financial policies.

Research Method: The method used in this research is descriptive-analytical, which analyzes emerging crimes in the field of cryptocurrencies through data analysis and theoretical foundations.

Findings: The findings show that, based on the rational digital deterrence framework, criminals in the cryptocurrency space regulate their behavior based on calculating the profit and risk of crimes. In addition, the existence of legal gaps, ambiguity in the legal status of cryptocurrencies, and procedural difficulties in the Iranian criminal justice system are considered to be the main obstacles to combating these crimes.

Conclusion: This study suggests that amending and supplementing criminal laws, determining penalties commensurate with the proceeds of crime, establishing specialized oversight institutions, and utilizing preventive technologies and digital tracking should be considered as fundamental strategies in Iran's criminal policymaking. These measures can increase the cost of committing a crime and improve the likelihood of detection, reduce the motivation of criminals, and protect the rights of citizens and the stability of the financial system.

Cite this article: Shamsi, Abdollahi, Safaei, Rasoul, Esmaeil, Maryam (2025)., Pathology and Evaluation of the Rational Digital Deterrence Approach to Counterfeiting and Fraud Crimes in the Field of Cryptocurrencies, *New Research in Islamic Humanities Studies*, Volume 3, Number 6, 329-345 .http//doi.org/ 10.22034/api.2025.730436

DOI: http//doi.org/ 10.22034/api.2025.730436
Publisher: University of Lorestan.

1. Introduction

Money, as a fundamental tool for facilitating economic exchange, has a history as long as human civilization itself. Its evolution from valuable commodities and metal coins to gold-backed banknotes and, finally, fiat currency reflects the development of monetary systems at national and international levels. Following the collapse of the Bretton Woods system in the 1970s and the establishment of fiat money, the current monetary structure was solidified in most countries. While this system expanded global trade and economic capacity, its inherently inflationary nature and regulatory mismanagement have led to numerous economic crises, the burden of which has fallen disproportionately on the middle and lower classes. The 2008 financial crisis and the emergence of the novel technology "Bitcoin" as a decentralized payment system marked a turning point, starkly revealing the urgent need to re-evaluate existing legal frameworks. Virtual currencies, due to their unique characteristics, not only facilitate transactions but also create a potent environment for emerging crimes such as forgery and fraud. These crimes are intensified by a lack of transparency, the absence of centralized oversight, and challenges in identity verification and judicial pursuit. This paper examines these challenges and proposes a regulatory framework grounded in rational digital deterrence.

1.2. Research Questions

This article seeks to address the following primary questions:

- What are the fundamental legal and technical characteristics of virtual currencies that enable crimes like forgery and fraud?
- What are the substantive and procedural challenges that virtual currency crimes pose for domestic and international legal systems, particularly Iran's?
- How can a "Rational Digital Deterrence" theory, based on rational choice theory, inform effective criminal policy and novel preventive approaches to combat these crimes?

3. Literature Review

The literature on virtual currencies spans legal, economic, and criminological fields. Scholars have explored the legal nature of cryptocurrencies, classifying them as intangible property or digital assets rather than official currency in the absence of state recognition. Existing research highlights the regulatory dichotomy among nations, with approaches ranging from prescriptive (e.g., Japan) to prohibitive (e.g., China). Criminological studies apply theories like Rational Choice, Spatial Transfer, and Neutralization Techniques to explain criminal behavior in this domain. Previous works have documented the modus operandi of crimes such as Ponzi schemes, phishing, and the creation of fake tokens, emphasizing the challenges of anonymity and cross-border transactions. This article builds upon this foundation by synthesizing these perspectives and proposing the integrated theory of "Rational Digital Deterrence" to address the unique calculous of crime in the blockchain environment.

4. Methodology

This research employs a descriptive-analytical method. It relies on the analysis of primary sources, including Iranian laws, banking regulations, and international standards such as the FATF recommendations. Furthermore, it conducts a comparative review of the legal approaches adopted by various countries (e.g., South Korea, the United States, and the European Union). The study also integrates criminological theories to analyze the causes and

patterns of forgery and fraud in the virtual currency space, leading to the development of a novel theoretical framework for prevention.

5. Results

The analysis reveals several key findings:

- The decentralized, anonymous, and cross-border nature of virtual currencies creates significant substantive and procedural legal challenges, making it difficult to apply traditional laws on forgery and fraud.
- Iran's current legal framework suffers from ambiguities and gaps, lacking specific criminalization and clear procedures for investigating and prosecuting virtual currency-related crimes.
- From a criminological perspective, offenders operate based on a rational calculation where the potential for high profit and a low risk of discovery makes these crimes attractive.

6. Conclusion

The proliferation of virtual currencies presents a dual reality: they offer significant economic opportunities while simultaneously enabling sophisticated crimes like forgery and fraud. To effectively counter these threats, a multi-faceted approach is essential. This article concludes that Iran must move beyond absolute prohibition towards a comprehensive regulatory strategy. This strategy should be guided by the theory of "Rational Digital Deterrence," which aims to disrupt the criminal's cost-benefit calculus by increasing the costs of crime (through stricter penalties and transparent regulations) and the probability of detection (via digital tracking technologies and enhanced international judicial cooperation). Furthermore, the adoption of novel preventive measures—including smart contracts, biometric authentication, AI-driven analytics, and public education—is critical. Ultimately, a flexible, technology-informed, and internationally harmonized legal framework is the most viable path to securing the digital financial space, protecting users, and fostering sustainable innovation in the cryptocurrency industry.

Author Contributions

All authors contributed equally to the conceptualization of the article and writing of the original and subsequent drafts.

Data Availability Statement

Data available on request from the authors.

Acknowledgements

The authors would like to thank the anonymous reviewers for their insightful comments and constructive feedback, which significantly improved the quality of this manuscript. We also extend our gratitude to our colleagues for their valuable discussions and technical support throughout this research.

Ethical Considerations

The authors strictly adhered to the highest standards of research integrity. The authors avoided data fabrication, falsification, plagiarism, and any other form of scientific misconduct.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare no conflict of interest.

پژوهش های نوین در مطالعات علوم انسانی اسلامی شاپا الکترونیکی:۸۹۴۴-۲۹۸۰
Homepage: //https: /api.lu.ac.ir
دانشگاه لرستان

آسیب شناسی و ارزیابی رویکرد بازدارندگی دیجیتال عقلانی جرایم جعل و کلاهبرداری در حوزه رمز ارزها

رسول شمسی[۱]، اسماعیل عبدالهی*[۲]، مریم صفایی [۳]

[۱] دانشجوی دکتری گروه حقوق ، واحد بوشهر ، دانشگاه آزاد اسلامی ، بوشهر ایران، ایمیل:rasoulshamsi41@yahoo.com

[۲]* استادیار گروه حقوق ، واحد بوشهر ، دانشگاه آزاد اسلامی ، بوشهر، ایران، ایمیل: e.abdolahi@iaubushehr.ac.ir

[۳] استادیار گروه حقوق ، واحد بوشهر ، دانشگاه آزاد اسلامی ، بوشهر، ایران، ایمیل: Maryamsafae@iaubushehr.ac.ir

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی

تاریخ دریافت: ۱۴۰۳/۰۳/۱۰
تاریخ بازنگری: ۱۴۰۳/۰۶/۱۵
تاریخ پذیرش: ۱۴۰۳/۰۷/۱۵
تاریخ انتشار: ۱۲/۲۸ /۱۴۰۳

کلیدواژه‌ها:
رمز ارز، پیشگیری فناورانه، جعل، کلاهبرداری، بازدارندگی دیجیتال عقلانی

چکیده

هدف پژوهش: این پژوهش با هدف شناسایی آسیب‌پذیری‌های زیرساختی و خلأهای قانونی در حوزه رمزارزها و همچنین بررسی آثار جرایم مرتبط بر حریم خصوصی، امنیت سایبری و سیاست‌های مالی انجام شده است.

روش پژوهش: روش مورد استفاده در این تحقیق، توصیفی–تحلیلی است که از طریق تحلیل داده‌ها و مبانی نظری، به واکاوی جرایم نوظهور در حوزه رمزارزها پرداخته است.

یافته‌ها: یافته‌ها نشان می‌دهد که بر اساس چارچوب بازدارندگی دیجیتال عقلانی، مجرمان در فضای رمزارزها، رفتار خود را بر اساس محاسبه سود و خطر جرایم تنظیم می‌کنند. همچنین وجود خلأهای قانونی، ابهام در وضعیت حقوقی رمزارزها و دشواری‌های دادرسی در نظام عدالت کیفری ایران از موانع اصلی مقابله با این جرایم محسوب می‌شوند.

نتیجه‌گیری: این پژوهش پیشنهاد می‌کند که اصلاح و تکمیل قوانین کیفری، تعیین مجازات‌های متناسب با سود حاصل از جرم، ایجاد نهادهای نظارتی تخصصی و بهره‌گیری از فناوری‌های پیشگیرانه و ردیابی دیجیتال، به عنوان راهبردهای اساسی در سیاست‌گذاری کیفری ایران مورد توجه قرار گیرد. این اقدامات می‌تواند ضمن افزایش هزینه ارتکاب جرم و ارتقای احتمال کشف، انگیزه مجرمان را کاهش داده و از حقوق شهروندان و ثبات نظام مالی حفاظت کند.

استناد: شمسی، عبدالهی، صفایی، رسول، اسماعیل، مریم (۱۴۰۳). ، آسیب شناسی و ارزیابی رویکرد بازدارندگی دیجیتال عقلانی جرایم جعل و کلاهبرداری در حوزه رمز ارزها، *پژوهش های نوین در مطالعات علوم انسانی اسلامی*، جلد ۳ شماره ۶ ، ۳۲۹– ۳۴۵
http//doi.org/ 10.22034/api.2025.730436

ناشر: دانشگاه لرستان.

۱–مقدمه

پول به‌عنوان ابزاری بنیادین برای تسهیل مبادلات اقتصادی، سابقه‌ای هم‌پای تاریخ تمدن بشر دارد. سیر تحول آن از کالاهای ارزشمند و سکه‌های فلزی تا اسکناس‌های مبتنی بر پشتوانه طلا و در نهایت اسکناس‌های بدون پشتوانه، نشان‌دهنده تکامل نظام‌های پولی در سطح ملی و بین‌المللی است. پس از فروپاشی نظام «برتون وودز» در دهه ۱۹۷۰ و استقرار پول بدون پشتوانه، ساختار فعلی پولی در اغلب کشورها تثبیت شد. هرچند این نظام، ظرفیت‌های تجاری و اقتصادی را در اقتصاد جهانی گسترش داد، اما ماهیت تورمی آن و سوءمدیریت نهادهای ناظر، باعث بحران‌های اقتصادی متعددی شد که بیشترین بار آن بر دوش اقشار متوسط و ضعیف جامعه افتاد.ظهور بحران مالی ۲۰۰۸ و فناوری نوین «بیت‌کوین» به‌عنوان پول یا سامانه پرداخت غیرمتمرکز، نقطه عطفی در این مسیر بود و ضرورت بازنگری در نظام‌های حقوقی موجود را بیش از پیش آشکار ساخت. ارزهای مجازی به دلیل ویژگی‌های منحصربه‌فرد خود، علاوه بر تسهیل مبادلات، بستر بالقوه و بالفعل برای جرایمی نوظهور مانند جعل و کلاهبرداری را نیز فراهم کرده‌اند. این جرایم، به دلیل فقدان شفافیت، نبود نظارت متمرکز و چالش‌های شناسایی هویت و پیگیری قضایی، شدت و پیچیدگی بیشتری پیدا کرده‌اند. نمونه‌هایی از این جرایم شامل ایجاد توکن‌های جعلی، دستکاری داده‌ها در فرآیند تأیید تراکنش‌ها و کلاهبرداری‌های مبتنی بر فریب کاربران یا سوءاستفاده از آسیب‌پذیری‌های فنی و تبلیغات گمراه‌کننده در شبکه‌های اجتماعی است. از منظر بازدارندگی دیجیتال عقلانی، مجرمان در فضای رمزارزها بر اساس محاسبات عقلانی خود عمل می‌کنند و ارتکاب جرم زمانی محتمل است که سود بالقوه بالا و ریسک کشف پایین باشد. بنابراین، تدوین مقررات شفاف و جامع، افزایش هزینه ارتکاب جرم، ارتقای احتمال کشف آن و بهره‌گیری از فناوری‌های ردیابی دیجیتال، می‌تواند انگیزه ارتکاب جرایم را کاهش دهد. چنین رویکردی، هم حقوق افراد را حفاظت می‌کند و هم امنیت و پایداری نظام مالی را تضمین می‌نماید. در نتیجه، سیاست‌گذاری کیفری در حوزه رمزارزها باید با تمرکز بر کاهش جذابیت اقتصادی جرم و افزایش ریسک کشف، چارچوبی پیشگیرانه و متناسب با ویژگی‌های محیط غیرمتمرکز بلاکچین ایجاد کند.

۲–مفاهیم

تعریف مفاهیم جهت جلوگیری از ابهامات احتمالی در مورد ارزهای مجازی[۱] بسیار ضروری است. به دلیل آن که در این زمینه، از مفاهیم مرتبط گوناگونی مانند پول الکترونیک[۲]، پول دیجیتال[۳]، پول مجازی، رمز ارز، پول رمزنگاری[۴]، پول سایبری[۵] شده و... استفاده می شود. در برخی موارد، این مفاهیم به جای یکدیگر مورد استفاده قرار می گیرند. در این بخش تبیین مفاهیم مرتبط با ارزهای مجازی و تمیز میان آن ها، در حد ضرورت و جهت بیان مقصود نگارنده از ارز مجازی، صورت می گیرد.

۲-۱- مفهوم پول اعتباری

منظور از پول اعتباری یا پول بدون پشتوانه،[۶] پول دارای پشتوانه ی قانونی و یا دستوری است که توسط یک نهاد مرکزی صلاحیتدار قانونی مانند دولت و یا بانک مرکزی خلق و منتشر می شود. مطابق قانون پولی و بانکی کشور، پول رایج کشور به صورت اسکناس و سکه های فلزی قابل انتشار است و تعهد پرداخت هرگونه دین و یا بدهی فقط به پول رایج کشور انجام پذیر است. همچنین امتیاز انتشار پول رایج کشور در انحصار دولت است و این امتیاز با رعایت مقررات این قانون منحصراً به بانک مرکزی ج.ا.ایران واگذار می‌شود[۷]. بنابر تعریف شبکه مبارزه با جرایم مالی آمریکا:[۸] پول(اعتباری) به صورت سکه و اسکناس ایالات متحده یا هر کشور دیگری که به عنوان وجه رایج تعیین شده است و به صورت معمول مورد استفاده و پذیرش آن به عنوان وسیله مبادله در

1- Virtual Currency
2- Electronic Money
3- Digital Currency
4- cryptocurrency
5- cyber currency
6- Fiat Currency

۷- قانون پولی و بانکی کشور مصوب ۱۳۵۱/۴/۱۸ با آخرین اصلاحات تا ۱۳۹۶/۱۲/۲۸. مواد یک الی سه.

8- Financial Crimes Enforcemwnt Network (FINCEN)

کشور محل صدور، قرار می گیرد[۹]. نهاد مرکزی با وضع سیاست ها و مقررات پولی و مالی بر وضعیت اقتصادی و گردش پول، نظارت و آن را کنترل می کند. پول اعتباری به صورت اسکناس و یا سکه چاپ و ضرب می شود.

برخی ویژگی های پول های اعتباری عبارتند از: ظاهری یکسان (اندازه، رنگ، طرح، شکل، وزن، نوع کاغذ و...)، [۱۰]گمنام بودن (نمی توان دارنده آن را مشخص کرد و در صورتی که مفقود و یا سرقت شوند، یابنده و یا سارق می تواند از آن استفاده کند.)،[۱۱] عدم امکان خرج دوباره (دارنده آن پس از یک بار استفاده، دیگر نمی تواند از همان پول استفاده کند؛ زیرا از دارایی و مالکیت او خارج شده است)، محدودیت میزان در دسترس (میزان پول اعتباری محدود است و نهاد مرکزی با توجه به شاخص های پولی و مالی ممکن است اقدام به خلق و انتشار پول نماید).[۱۲] از پول اعتباری به عنوان ارز واقعی [۱۳]، پول واقعی[۱۴] و ارز ملی[۱۵]نیز نام می برند.

خلق پول پدیده‌ای اجتماعی است که فراتر از صرف ملاحظات حقوقی قابل بررسی است. در این میان، انقلاب فناورانه دولت‌ها و مقامات عمومی را ناگزیر ساخته تا در سطح بین‌المللی برای استفاده از آن مقررات‌گذاری کنند، به‌ویژه در زمینه‌هایی همچون پولشویی و تأمین مالی تروریسم .با توجه به ویژگی فرامرزی و چندجانبه عملکرد ارزهای دیجیتال، ضرورت هماهنگی و همگرایی در معیارهای نظارتی و حقوقی دولت‌ها بیش از پیش احساس می‌شود. در این راستا، توجه به جنبه فنی بلاکچین ضروری است؛ چراکه آنچه تغییر می‌یابد، شکل‌ها و شیوه‌های ارائه خدمات مالی است، نه ضرورت و ماهیت آن‌ها. با این حال، این موضوع نباید مانع از بررسی جامع‌تر وضعیت حقوقی خلق پول از منظرهای گوناگون شود. به‌ویژه دیدگاه‌های جامعه‌شناختی که پول را در اصل نه یک ابزار صرفاً اقتصادی یا حقوقی، بلکه نوعی توافق اجتماعی میان افراد و نهادها تلقی می‌کنند، می‌توانند افق‌های تازه‌ای در تحلیل این پدیده نوین بگشایند (سیاه بیدی کرمانشاهی و ثالث مؤید، ۱۳۹۶: ۱۷۳).

در واقع، حقوق به طور خاص از علم اقتصاد برای شناسایی قانونی آن چه امروز به عنوان پول قانونی شناخته می‌شود استفاده می کند. با این حال، در غیاب تعریف مثبت، هیچ مانعی وجود ندارد که بر اساس آن چه دیگر علوم به آن افزوده‌اند، دیگر اشکال پول نیز به‌طور قانونی شناخته شوند. در چنین ملاحظاتی، چارچوب‌های حقوقی اروپایی و فرانسوی به شناسایی غیرمستقیم تنوع پولی که به‌طور اجتماعی پذیرفته شده است اشاره دارند. ابزارهایی که در این متن تحلیل شده‌اند، به‌ویژه دستورالعمل (UE) 2018/843در سطح اروپا و همچنین قانون موسوم به PACTEدر فرانسه، وجود "نمایش‌های دیجیتال ارزش" را به‌عنوان انواعی متفاوت از پول قانونی به رسمیت می‌شناسند. این اقدامات حقوقی را می‌توان به‌عنوان اقدامات نظارتی از سوی دولت در نظر گرفت که هدف آن چارچوب بندی و هدایت یک بازار نوظهور از ارزهای دیجیتال و بازیگران آن است. به این ترتیب، امنیت حقوقی برای کاربران فراهم می‌شود و در حدی نظارت بر گردش و استفاده از ارزهای دیجیتال اعمال می‌گردد.

---

[9]- FINCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. FIN-2013-G001. March 18, 2013. P 1.

[۴]- همان قانون. بند و ماده دو: مبلغ اسمی، شکل، جنس، رنگ، اندازه، نقشه و سایر مشخصات اسکناس ها و سکه های فلزی رایج کشور به پیشنهاد رئیس کل بانک مرکزی ج.ا.ایران و تصویب وزیر امور اقتصادی و دارایی با رعایت مقررات این قانون تعیین خواهد گردید .

میزان سکه های فلزی به پیشنهاد رئیس کل بانک مرکزی ج.ا.ایران و تصویب وزیر امور اقتصادی و دارایی تعیین خواهد شد.

بند ز: اسکناس دارای امضاء وزیر امور اقتصادی و دارایی و رئیس کل بانک مرکزی ج.ا.ایران خواهد بود.

[۵]- همان قانون، بند ب ماده چهار: بانک مرکزی ج.ا.ایران در قبال سرقت یا فقدان یا از بین رفتن اسکناس ها و سکه های فلزی در دست اشخاص هیچ گونه تعهد و مسئولیتی نخواهد داشت.

[۶]- همان قانون. ماده ۱۰: بانک مرکزی ج.ا.ایران مسئول تنظیم و اجرای سیاست پولی و اعتباری، بر اساس سیاست کلی اقتصادی کشور می باشد.

ماده ۱۱: بانک مرکزی ج.ا.ایران به عنوان تنظیم کننده نظام پولی و اعتباری کشور موظف به انجام وظایف زیر می باشد:

الف- انتشار اسکناس و سکه هاست فلزی رایج کشور، طبق مقررات این قانون.

[13]-real currency

[14]- real money

[15]- national currency

۲-۲- مفهوم پول الکترونیک [۱۶]

با گسترش فنآوری اطلاعات، پول الکترونیکی پا به عرصه اقتصاد گشود که ماهیت آن همان اسکناس‌های کاغذی است اما از حالت فیزیکی و ملموس به یک سری اعداد و ارقام داخل کامپیوتر و شبکه تبدیل شده است؛ به عبارتی ؛ پول های الکترونیک یا دیجیتال، مکانیسمی جدید در پرداخت اسکناس های متداول بانکی هستند(نواب پور،۱۳۹۷:۲۱۸). در این حالت، هیچ وسیله فیزیکی ای در میان نیست و مبادله، تنها با انتقال و پردازش داده های رمزنگاری شده انجام می پذیرد؛ بدین صورت که رایانه های مرکزی بانک ها، حساب های افراد را طلبکار و بستانکار می کنند. لازم به ذکر است که در این نوع پول، امر مهم، قابلیت نقل و انتقال آن در فضای مجازی می باشد که موجب رونق این پول شده است اما از جهت ماهیتی، با کارت های بانکی، تفاوت زیادی ندارد؛ زیرا در هر دوحالت، آن چه مورد نقل و انتقال قرار می گیرد، نقل و انتقال واقعی پول به قبض و اقباض نمی باشد بلکه تنها با طلبکار و بستانکار کردن حساب مشتریان، میان آن ها نقل و انتقال واقع می شود. این نوع پول، شباهت بسیار زیادی با کارت های بانکی دارد؛ با این تفاوت که این حساب ها یا همراه با یک کارت بانکی است یا مستقل می باشد؛ به این نحو که مشتری در یک بانک، حسابی باز می کند و یک نام و رمز دریافت می دارد و می تواند به وسیله انتقالات اینترنتی، به خرید کالاهای خود بپردازد(سلطانی،۱۳۹۴:۴۸).

۲-۳- مفهوم جعل و کلاهبرداری در رمز ارزها

جعل در رمز ارزها، جعل معمولاً به معنای ایجاد امضای دیجیتال جعلی است که بدون دسترسی به کلید خصوصی، تراکنشی را به نام فرد دیگری معتبر نشان دهد. این شامل حملات مانند جعل امضای دیجیتال از طریق آسیب‌پذیری‌های خاص رمزنگاری، مانند حملات علیه رمزنگاری [۱۷]در سیستم‌هایRSA ، می‌شود. همچنین، حملات ۵۱ درصدی، که در آن کنترل اکثریت قدرت محاسباتی شبکه برای تغییر تاریخچه بلاکچین استفاده می‌شود، می‌تواند به‌عنوان نوعی جعل در نظر گرفته شود. کلاهبرداری شامل فعالیت‌هایی مانند طرح‌های پانزی (مانند OneCoin)، فیشینگ (فریب کاربران برای ارسال رمز ارز به آدرس‌های جعلی)، صرافی های جعلی، و وعده‌های سودهای کلان در سرمایه‌گذاری‌های غیرواقعی است. این جرایم اغلب از ویژگی‌های رمز ارزها، مانند ناشناس بودن نسبی و سرعت تراکنش‌ها، بهره می‌برند. ارز دیجیتال یکی از اقسام دارائی‌های دیجیتال می‌باشد که در سالیان اخیر بسیار مورد توجه قرارگرفته است(خلیلی پاجی، ۱۴۰۰:۲۵۱). رمز ارز پدیده نوینی است که بر بستر اینترنت و با استفاده از فناوری‌های نوین استخراج و منتقل می‌شوند. و یکی از انواع آن بنام بیت کوین توانسته نظام‌های مالی دنیا را تحت تاثیر قرار دهد. غیرمتمرکز بودن، فرامرزی بودن، گمنام بودن کاربران، رمزنگاری و برگشت ناپذیر بودن تراکنش‌ها، ویژگی–هایی است که بهره‌گیری از ارزهای مجازی در فعالیت‌های مجرمانه را مورد توجه بزهکاران قرار می‌دهد.

۳-موضوع شناسی حقوقی ارزهای مجازی

شناسایی ماهیت رمزارزها رابطهٔ تنگاتنگی با بازشناسی ساختار فنی هریک از اقسام آن دارد. لذا ارائهٔ ماهیتی واحد با وجود اقسام متنوع، امکان‌پذیر نبوده و قابل‌ایراد است. رمزارزها گونه‌ای از اموال غیرمادی و یا در صورت توسعه و تسری مفهوم عین به اموال ناملموس، از اعیان محسوب شده که دارای مالیت عرفی و شرعی نیز می‌باشند. رمزارزها اگرچه از لحاظ تئوریک و مبانی حقوقی و اقتصادی می‌توانند کارکردهای پول را ایفا نمایند و به‌عنوان واسطهٔ مبادله در میان مردم جهان نیز پذیرفته‌شده‌اند لکن بر اساس قوانین پولی، جهت صدق عنوان پول، نیازمند شناسایی دولت‌ها نیز می‌باشند؛ برخی از انواع رمزارزها همچون رمزارزهای ملی به‌واسطهٔ خلق توسط کشورها از این شناسایی برخوردار هستند لکن سایر اقسام آن، تا زمانی که در قوانین به رسمیت شناخته نشوند، پول تلقی نشده و صرفاً یک دارایی دیجیتال محسوب می‌شوند.ارزهای مجازی، به‌عنوان یکی از واقعیت‌های نوین در حوزه فناوری و اقتصاد، با ظهور بیت‌کوین در سال ۲۰۰۹ توسط یک شخص یا گروه ناشناس تحت عنوان "ساتوشی ناکاموتو" آغاز به‌وجود

---

[1]- Electronic Money/ e-money

[۱۷] حمله Bleichenbacher، که در سال ۱۹۹۸ توسط دانیل بلیشنباچر معرفی شد، یک حمله انتخابی متن رمز شده تطبیقی (CCA2) علیه رمزنگاری RSA با استفاده از استاندارد PKCS#1 v1.5 است. این حمله به‌ویژه در پروتکل‌های رمزنگاری مانند SSL/TLS که از RSA برای تبادل کلید استفاده می‌کنند، کاربرد دارد

آمدند. پس از مشخص شدن قابلیت‌های تبادلی و کاربردهای متنوع این رمزارز، دیگر ارزهای دیجیتالی مانند اتریوم ، ریپل ، مونرو و لایت‌کوین نیز به‌سرعت توسعه یافتند. این ارزها به دلیل ویژگی‌های منحصربه‌فرد خود، مانند غیرمتمرکز بودن، عدم نیاز به واسطه‌های مالی سنتی، و توانایی انجام تراکنش‌های سریع و کم‌هزینه، به‌سرعت در جهان گسترش یافتند(رحیمی و امینی نیا، ۸:۱۴۰۰).

موضوع بسیار حائز اهمیت در این خصوص، رویکرد کشورها در برابر پذیرش یا ممنوعیت این ارزها است. با توجه به نقش خاص ارزهای مجازی در تبادلات مالی و چالش‌های ناشی از آن‌ها در نظام‌های پولی و بانکی، کشورها سیاست‌ها و مقررات متفاوتی در این زمینه اتخاذ کرده‌اند. برخی کشورها با رویکرد تجویزکننده ، این ارزها را به‌عنوان بخشی از نظام مالی پذیرفته‌اند و مقرراتی برای حمایت از دادوستد و استفاده از آن‌ها وضع کرده‌اند. این کشورها، با تدوین قوانین شفاف و ایجاد چارچوب‌های حقوقی، به ترویج نوآوری و جذب سرمایه‌گذاری در این حوزه پرداخته‌اند. در مقابل، گروه دوم کشورها با رویکرد ممنوع‌کننده ، دادوستد و استفاده از ارزهای مجازی را به‌طور کامل ممنوع اعلام کرده‌اند. این کشورها، با تصویب مقررات سخت‌گیرانه، به دنبال جلوگیری از فعالیت‌های مرتبط با ارزهای دیجیتال هستند. این رویکرد معمولاً به دلیل نگرانی‌هایی مانند خطر پولشویی، تأمین مالی فعالیت‌های غیرقانونی، و تهدید به ثبات نظام بانکی و مالی اتخاذ می‌شود. بالاخره، گروه سوم کشورها، فاقد رویکرد مشخصی در قبال ارزهای مجازی هستند. این کشورها، به دلیل عدم وجود زیرساخت‌های حقوقی و فناوری لازم یا به دلیل عدم تصمیم‌گیری آشکار، هنوز به سیاست‌های واضحی در این حوزه دست نیافته‌اند. این وضعیت عدم قطعیت، گاهی زمینه‌ساز فعالیت‌های غیرقانونی مانند جعل و کلاهبرداری در فضای ارزهای دیجیتال می‌شود و نیاز به تدوین قوانین جامع و هماهنگ را بیش از پیش آشکار می‌سازد. تنوع در رویکردهای کشورها نسبت به ارزهای مجازی، نشان‌دهنده چالش‌های حقوقی، اقتصادی و امنیتی این حوزه است که نیازمند تحلیل دقیق و هماهنگی بین‌المللی برای مقابله مؤثر با جرایم مرتبط با این فناوری است(خداوردی و همکاران، ۴۳:۱۴۰۳).

٤-ابعاد شکلی و ماهوی جرایم جعل و کلاهبرداری مرتبط با ارزهای مجازی

سیاست‌گذاری عمومی در خصوص پدیده‌های اجتماعی طی دهه‌های اخیر به‌عنوان یکی از دغدغه‌های اصلی نظام‌های حاکم مطرح شده است. از جمله حوزه‌های چالش‌برانگیز در این زمینه، سیاست‌گذاری در قلمرو فناوری‌های نوین و نوظهور مرتبط با فضای مجازی/سایبری است. تنظیم‌گری و مقررات‌گذاری در این حوزه به دلیل ماهیت پویا و متغیر فضای مجازی، تأثیرات آن بر اقتصاد کلان، حساسیت‌های سیاسی و امنیتی موجود در این فضا و همچنین پیچیدگی‌های فنی، مستلزم توجه ویژه و برنامه‌ریزی دقیق است. این موضوع باتوجه به ظرفیت بالقوه فناوری‌های مزبور برای سوءاستفاده‌های بزهکارانه، به یکی از اولویت‌های تقنینی و کیفرگزینی جنایی تبدیل شده است. در این راستا، سیاست‌گذاران جنایی به‌عنوان بخشی از نظام حاکم، در چارچوب وظایف خود به تنظیم‌گری و مقررات‌گذاری در حوزه‌های مختلف بزهکاری، از جمله بزهکاری فناورانه، مبادرت می‌ورزند. این رویکرد سیاستی در قالب سیاست جنایی تقنینی شکل می‌گیرد که نقش راهبردی در تعیین برنامه‌های کلان پیشگیرانه و مقابله‌ای در برابر پدیده‌های مجرمانه ایفا می‌کند. سیاست جنایی به‌معنای طراحی الگوهای عملیاتی، برنامه‌ریزی دقیق و ارائه خط‌مشی‌های عملی برای کنشگران نظام عدالت کیفری است.

یکی از موضوعات نوین و نیازمند سیاست‌گذاری در حوزه فناوری، ارزهای مجازی است که به‌دلیل ویژگی‌های منحصربه‌فرد خود، ظرفیت بالقوه‌ای برای انواع فعالیت‌های بزهکارانه دارد. ارزهای مجازی به انواع مختلفی تقسیم می‌شوند که هر یک بر اساس ماهیت و کارکرد خاص خود، ویژگی‌های متمایزی نسبت به یکدیگر دارند. در این میان، بیت‌کوین به‌عنوان نمونه‌ای کامل از ارزهای مجازی، با ویژگی‌های خاصی که دارد، از سایر ارزهای مجازی مجزا شده و از اهمیت ویژه‌ای برخوردار است. این ویژگی‌ها شامل غیرمتمرکز بودن ، عدم نیاز به واسطه‌های مالی سنتی، و همچنین محرمانگی نسبی معاملات است که از یک سو مزایای فراوانی را به همراه دارد، اما از سوی دیگر، می‌تواند زمینه‌ساز سوءاستفاده‌های بزهکارانه باشد(مظلومان، ۷۶:۱۴۰۰).

در بعد ماهوی، جرایم جعل و کلاهبرداری مرتبط با ارزهای مجازی به دلیل پیچیدگی ذاتی این فناوری و نوظهور بودن آن، چالش‌های متعددی را در نظام حقوقی داخلی و خارجی ایجاد کرده‌اند. ارزهای مجازی که غالباً فاقد نظارت متمرکز هستند، زمینه‌ساز سوءاستفاده‌هایی از جمله فروش توکن‌های جعلی یا انجام معاملات کلاهبردارانه شده‌اند .این نوع جرایم معمولاً با استفاده از ظاهری

قانونی و تبلیغات گمراه‌کننده، افراد را به سرمایه‌گذاری در پروژه‌های فاقد ارزش واقعی ترغیب می‌کنند. از سوی دیگر، نقش عواملی مانند هوش مصنوعی و شبکه‌های اجتماعی در تسهیل این جرایم نیز قابل توجه است، به طوری که مجرمان از این ابزارها برای پنهان‌کردن هویت واقعی خود و افزایش دامنه فعالیت‌های مجرمانه استفاده می‌کنند. ابهام در وضعیت حقوقی ارزهای مجازی و عدم وجود قوانین روشن در بسیاری از کشورها، این مشکلات را تشدید کرده و تعقیب قضایی این نوع جرایم را با دشواری‌هایی همراه کرده است . از دیدگاه ماهوی، جرایم مرتبط با ارزهای مجازی به‌دلیل ماهیت نوظهور و پیچیده‌شان، چالش‌های خاصی را برای نظام حقوقی و قضایی کشورها، از جمله ایران، ایجاد کرده‌اند .ارزهای مجازی ، به‌ویژه بیت‌کوین، به‌عنوان یک فناوری نوین، ویژگی‌های منحصربه‌فردی دارند که شامل غیرمتمرکز بودن، عدم نیاز به واسطه‌های مالی سنتی، و مخفی‌ماندن هویت طرفین معامله است. این ویژگی‌ها زمینه‌ساز ظهور انواع جرایمی هستند که در چارچوب سنتی قانون مجازات اسلامی قابل تطبیق نیستند(خلیلی پاجی، ۱۳۲:۱۴۰۰).

به‌عنوان مثال، جعل در فضای ارزهای دیجیتال می‌تواند شامل ایجاد توکن‌های جعلی، دستکاری داده‌ها، و حتی جعل هویت در شبکه‌های بلاکچین باشد. این نوع جعل به‌دلیل پیچیدگی فناوری و نبود مقررات دقیق، تشخیص و تعقیب آن را دشوار می‌کند. از سوی دیگر، کلاهبرداری در این حوزه اغلب از طریق فریب کاربران برای سرمایه‌گذاری در پروژه‌های فاقد ارزش واقعی (مانند اسکم‌های اولیه سکه‌ها) یا سوءاستفاده از نقاط ضعف فناوری انجام می‌شود. این نوع کلاهبرداری‌ها معمولاً با استفاده از تبلیغات گمراه‌کننده و شبکه‌های اجتماعی تشدید می‌شوند.

در حوزه شکلی، این جرایم اغلب در قالب روش‌هایی مانند جعل رایانه‌ای، دستکاری داده‌ها و سوءاستفاده از نقاط ضعف فناوری اطلاعات اتفاق می‌افتند. سابقه قانون‌گذاری در حوزه جرایم رایانه‌ای در ایران به سال ۱۳۸۸ بازمی‌گردد، اما با ظهور ارزهای مجازی و تحولات فناوری، نیاز به به‌روزرسانی و تطبیق قوانین با محیط دیجیتال احساس می‌شود. از دیدگاه شکلی، جرایم مرتبط با ارزهای مجازی اغلب در قالب روش‌های نوین و ابزارهای فناورانه اتفاق می‌افتند. این جرایم معمولاً شامل استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی ، شبکه‌های اجتماعی ، و فناوری‌های رمزنگاری می‌شوند. به‌عنوان مثال، مجرمان ممکن است از الگوریتم‌های پیچیده برای پنهان‌کردن هویت واقعی خود استفاده کنند یا از شبکه‌های تور (Dark Web) برای انجام معاملات غیرقانونی بهره ببرند. ویژگی‌های منحصربه‌فرد این ارزها، از جمله غیرمتمرکز بودن، فرامرزی بودن، گمنامی کاربران، رمزنگاری و برگشت‌ناپذیری تراکنش‌ها، آنها را به ابزاری جذاب برای سوءاستفاده‌های بزهکارانه تبدیل کرده است. این ویژگی‌ها ضمن تسهیل فعالیت‌های غیرقانونی، چالش‌های جدی را در حوزه دادرسی جرایم مرتبط با ارزهای مجازی ایجاد کرده‌اند.

ویژگی‌های ذاتی ارزهای مجازی، به‌همراه ابهام در وضعیت قانونی و قلمرو فعالیت‌های مجرمانه، چالش‌های متعددی را برای نظام عدالت کیفری در حوزه دادرسی جرایم ایجاد کرده است. این چالش‌ها شامل نقص در چارچوب‌های حقوقی موجود، عدم تطبیق قوانین فعلی با ویژگی‌های ارزهای مجازی و مشکلات عملی در ردیابی و شناسایی بزهکاران است. برای مقابله با این چالش‌ها و بهبود فرآیند دادرسی جرایم مرتبط با ارزهای مجازی، راهکارهایی پیشنهاد می‌شود. از جمله این راهکارها می‌توان به تعریف دقیق قانونی از ارزهای مجازی و تعیین ماهیت حقوقی آنها اشاره کرد. همچنین، اصلاح قوانین موجود و تصویب قوانین جدید که به‌طور خاص به جرایم مرتبط با ارزهای مجازی می‌پردازد، ضروری است. در مواردی که امکان تطبیق جرایم مرتبط با ارزهای مجازی با قوانین فعلی وجود ندارد، تعیین عناوین مجرمانه جدید برای پوشش این نوع بزهکاری‌ها الزامی است(نبوی و صابر، ۲۰۷:۱۳۹۹).

همکاری با کشورهای خارجی و نهادهای بین‌المللی به‌منظور تبادل اطلاعات و ارتباطات مرتبط با ارزهای مجازی نیز از اهمیت ویژه‌ای برخوردار است. انعقاد تفاهم‌نامه‌های بین‌المللی برای مقابله با جرایم سایبری و بزهکاری‌های مرتبط با ارزهای مجازی می‌تواند به بهبود همکاری‌های بین‌المللی کمک کند. همچنین، انعقاد تفاهم‌نامه‌هایی بین بخش خصوصی (مانند صرافی‌های ارزهای مجازی) و دولت برای تسهیل ردیابی و شناسایی فعالیت‌های مجرمانه از دیگر راهکارهای موثر است. استفاده از کارشناسان متخصص در حوزه ارزهای مجازی برای کمک به پرونده‌های قضایی و ارائه دوره‌های آموزشی به دادرسان و ضابطان دادگستری نیز می‌تواند به افزایش آگاهی و توانایی آنها در مقابله با جرایم مرتبط با ارزهای مجازی کمک کند. این راهکارها به‌گونه‌ای طراحی شده‌اند که هم قابل اجرا باشند و هم با چالش‌های موجود در نظام عدالت کیفری سازگاری داشته باشند. ارزهای مجازی به‌دلیل

ویژگی‌های منحصربه‌فرد خود، نیازمند رویکردی دقیق و همه‌جانبه در حوزه سیاست‌گذاری حقوقی و جنایی هستند. تنظیم‌گری این حوزه مستلزم توجه ویژه به جنبه‌های حقوقی، فنی و بین‌المللی است تا بتواند به‌طور مؤثر به چالش‌های موجود پاسخ دهد و امنیت حقوقی و اجتماعی را تأمین کند(صادقی و ناصر،۲۸۱:۱۴۰۰).

از سوی دیگر، در مقایسه با قوانین خارجی، نظام حقوقی ایران هنوز با نارسایی‌هایی در تعریف دقیق جرائم مرتبط با رمزارزها و نحوه رسیدگی به آن‌ها مواجه است. این نارسایی‌ها شامل فقدان مقررات شفاف برای کشف، تعقیب و توقیف دارایی‌های دیجیتال و همچنین عدم هماهنگی بین نهادهای ذی‌ربط می‌شود. بنابراین، لزوم تدوین قوانین جامع و هماهنگ با استانداردهای بین‌المللی برای مقابله مؤثر با این جرایم بیش از پیش احساس می‌شود.

کشورهای مختلف با توجه به سیاست‌ها و نیازهای داخلی خود، رویکردهای متفاوتی در قبال جرایم ارزهای مجازی به کار گرفته‌اند. برخی کشورها با وضع قوانین دقیق و کارآمدتر، الگوهایی را برای دیگران ایجاد کرده‌اند. به عنوان مثال، کره جنوبی یکی از کشورهایی است که قوانین سخت‌گیرانه‌ای در حوزه مبادلات ارز دیجیتال دارد و این مقررات شامل شناسایی هویت کاربران، محدودیت‌های معاملاتی و نظارت دقیق بر صرافی‌ها می‌شود. این رویکرد نه تنها به کاهش فعالیت‌های غیرقانونی کمک کرده، بلکه به افزایش شفافیت و امنیت در بازار ارزهای دیجیتال منجر شده است. ژاپن نیز از جمله کشورهایی است که با تدوین مقررات جامع، به ویژه در حوزه مبارزه با پولشویی و فراهم کردن چارچوب قانونی برای فعالیت صرافی‌ها، گام‌های مؤثری برداشته است. این کشور با الزام صرافی‌ها به ثبت رسمی و رعایت استانداردهای امنیتی بالا، زمینه‌ساز اعتماد بیشتر کاربران و کاهش جرایم مرتبط با ارزهای دیجیتال شده است.

از سوی دیگر، برخی کشورها مانند چین با اتخاذ رویکرد ممنوعیت کامل، سعی در کنترل کامل این صنعت داشته‌اند؛ اما این رویکرد نه تنها به طور کامل موفقیت‌آمیز نبوده، بلکه باعث انتقال فعالیت‌های غیرقانونی به بازارهای خاکستری شده است. این تجربه نشان می‌دهد که ممنوعیت کامل ممکن است چالش‌هایی را در پی داشته باشد و به جای آن، تدوین قوانین هماهنگ و انعطاف‌پذیر می تواند راهکار مؤثرتری باشد. تجربه کشورهایی که در گذشته با محدودیت‌ها و تصویب قوانین نامناسب مواجه شده‌اند نیز قابل توجه است. این کشورها با بازنگری در رویکردهای خود و اصلاح قوانین، توانسته‌اند به تعادل بین نوآوری و کنترل قانونی دست یابند. بنابراین، تجربیات این کشورها نشان می‌دهد که انعطاف‌پذیری و به‌روزرسانی مداوم قوانین، به ویژه در محیط پویای فناوری ارزهای دیجیتال، ضروری است.

٤-١-آسیب شناسی نظری و عملی جرایم جعل و کلاهبرداری در حوزه رمز ارزها

در حوزه نظری، آسیب‌شناسی جرایم جعل و کلاهبرداری در فضای ارزهای مجازی به بررسی ریشه‌ها و علل این پدیده‌ها می‌پردازد. این حوزه با استفاده از نظریه‌های مختلف جرم‌شناسی، مانند نظریه انتقال فضایی، نظریه انتخاب عقلانی، نظریه جرم‌شناسی آنی، نظریه معاشرت ترجیحی و نظریه فنون خنثی‌سازی، تلاش می‌کند تا الگوها و مکانیزم‌های مؤثر در بروز این جرایم را شناسایی کند. به عنوان مثال، نظریه انتقال فضایی نشان می‌دهد که مجرمان چگونه با استفاده از شبکه‌های دیجیتال و مرزهای سیاسی، فعالیت‌های خود را از یک منطقه به منطقه دیگر منتقل می‌کنند تا از دسترس قانون فرار کنند. از سوی دیگر، نظریه انتخاب عقلانی تأکید می‌کند که مجرمان با محاسبه منافع و هزینه‌ها، تصمیم به انجام جرایم می‌گیرند؛ بنابراین، افزایش هزینه‌های جرم و کاهش فرصت‌های ارتکاب آن می‌تواند نقش مهمی در پیشگیری از این نوع جرایم داشته باشد. نظریه‌های دیگر نیز با رویکردهای خاص خود، به شناخت دقیق‌تر ابعاد روانشناختی و اجتماعی این جرایم کمک می‌کنند(مظلومان،۳۲:۱۴۰۰).

در زمینه عملی، آسیب‌شناسی جرایم ارزهای مجازی به کاربرد قوانین و مقررات داخلی و بین‌المللی می‌پردازد. این حوزه شامل جرم‌انگاری انحرافی، کنترل کیفری جهانی، گسترش دامنه جرم‌انگاری و تنظیم قوانین مرتبط با معاملات ارزهای دیجیتال است. جرم‌انگاری انحرافی به بررسی نحوه تعریف و دسته‌بندی این جرایم در قوانین مختلف می‌پردازد و تلاش می‌کند تا شکاف‌های موجود در قوانین داخلی و بین‌المللی را شناسایی کند.

کنترل کیفری جهانی نیز به همگرایی قوانین در سطح بین‌المللی می‌پردازد تا با هماهنگی بیشتر بین کشورها، مجرمان بین‌المللی را تحت پیگرد قانونی قرار دهد. علاوه بر این، گسترش دامنه جرم‌انگاری در زمینه جرایم اقتصادی با استفاده از ارزهای دیجیتال،

به تنظیم قوانینی می‌پردازد که مواردی مانند ورود یا خروج غیرقانونی ارز، معاملات بدون مجوز، معاملات فردایی و انجام کارگزاری بدون مجوز را تحت پوشش قرار دهد.(Hutchings, 2023) این موارد نه تنها به حفاظت از حقوق افراد کمک می‌کنند، بلکه به افزایش اعتماد عمومی به سیستم‌های مالی دیجیتال نیز کمک می‌کنند.

جرم‌انگاری و کیفرگذاری در حوزه ارزهای دیجیتال بیشتر بر اساس اهدافی مانند اجرای عدالت یا حفظ نظم اجتماعی توجیه می شود. در این زمینه، جرائم و مجازات‌ها دارای اهمیت بالایی هستند، زیرا عدم وجود قوانین دقیق می‌تواند به فقدان امنیت حقوقی و مالی منجر شود. به عنوان مثال، سرقت اطلاعات ورود به سیستم، جست‌وجوی کیف پول‌های دیجیتال، و کشف اشتراک‌های باز در شبکه، از جمله روش‌هایی هستند که مجرمان از آنها استفاده می‌کنند. از طرفی، فقدان جرم‌انگاری عناوین مجرمانه در حوزه رمزارزها، یکی از بزرگ‌ترین چالش‌های حقوقی است که باید مورد توجه قرار گیرد.از منظر فقهی نیز صحت و اباحه حاکم بر نقل‌وانتقال ارزهای مجازی مطرح است، اما ممنوعیت قانونی ممکن است منجر به بطلان معامله یا مجازات مرتکب نشود. این موضوع نیازمند بررسی دقیق‌تر در چارچوب قوانین فعلی و سیاست‌های کیفری است. آسیب‌شناسی نظری و عملی جرایم جعل و کلاهبرداری در حوزه ارزهای مجازی، دو رویکرد مکمل هستند که هر کدام به شیوه‌ای خاص به شناخت و مقابله با این چالش‌ها کمک می‌کنند.

٤-٢-آسیب شناسی قوانین در حقوق خارجی برای مقابله با جرایم جعل و کلاهبرداری ارزهای مجازی

قوانین موجود در کشورهای مختلف برای مقابله با جرایم ارزهای مجازی هنوز به طور کامل کافی نیستند و چالش‌های متعددی در این زمینه وجود دارد. یکی از دلایل اصلی این مشکل، تفاوت در رویکردها و مقررات بین کشورها است. به عنوان مثال، برخی کشورها برای فعالیت‌های مرتبط با ارزهای دیجیتال نیاز به دریافت لایسنس یا مجوز از مقامات دولتی دارند، در حالی که کشورهای دیگر ممکن است چنین الزامی نداشته باشند. این تفاوت‌ها باعث می‌شود مجرمان بتوانند از مرزهای سیاسی و قوانین ناهماهنگ بین کشورها استفاده کنند و به راحتی از دسترس قانون فرار کنند. علاوه بر این، وضعیت قانونی ارزهای مجازی در بسیاری از کشورها همچنان مبهم است. برای مثال، در ایران، استفاده از رمزارزها به عنوان یک روش پرداخت ممنوع است، اما معاملات ارزهای دیجیتالی به طور صریح جرم محسوب نمی‌شود و هیچ ممنوعیت قانونی مشخصی وجود ندارد .این مبهم بودن قوانین می تواند به سوءاستفاده و افزایش جرایم منجر شود. یکی دیگر از مشکلات مهم، فقدان جرم‌انگاری دقیق برای عناوین مجرمانه در حوزه رمزارزها است. به عنوان مثال، در برخی کشورها، حتی اگر جرمی مرتبط با ارزهای دیجیتال شناسایی شود، ممکن است مجازات مناسب یا قوانین کافی برای مقابله با آن وجود نداشته باشد. این موضوع می‌تواند به کاهش اثر بخشی قوانین و ضعف در اجرای عدالت منجر شود(خادمان و همکاران، ۳۵۲:۱۴۰۰).

قوانین ضد پولشویی و مقررات مربوط به تراکنش‌های ارز دیجیتال در برخی کشورها بسیار سخت‌گیرانه هستند، اما همچنان نیاز به به‌روزرسانی و هماهنگی بین‌المللی دارند. به عنوان مثال، در برخی کشورها، تراکنش‌های غیرقانونی ارز دیجیتال می‌تواند منجر به حبس طولانی‌مدت شود، اما این قوانین در کشورهای دیگر ممکن است به اندازه کافی سخت‌گیرانه نباشند. برای مقابله مؤثر با جرایم ارزهای مجازی، نیاز به هماهنگی بین‌المللی، به‌روزرسانی قوانین داخلی و تدوین سیاست‌های کیفری دقیق‌تر وجود دارد. بدون این اقدامات، قوانین موجود نمی‌توانند به طور کامل جرایم مرتبط با ارزهای دیجیتال را پوشش دهند.

٤-٣-هم افزایی قوانین ارزهای مجازی را در سطح بین‌المللی در مقابله با جعل و کلاهبرداری

در حوزه ارزهای دیجیتال، این دو جرم اغلب با یکدیگر همپوشانی دارند. به عنوان مثال، سودجویان ممکن است از روش‌های جعلی مانند پیامک‌های جعلی برای فریب افراد و تصاحب دارایی‌های آنها استفاده کنند. همچنین، جعل هویت و اسناد دیجیتالی در فضای ارزهای دیجیتال به منظور کلاهبرداری از افراد یا صرافی‌ها نیز رواج پیدا کرده است. برای مقابله با این جرایم، کشورها نیاز به قوانین دقیق و شفاف دارند که بتواند این نوع تهدیدات را پوشش دهد. با این حال، در بسیاری از کشورها، شکاف‌های قانونی در حوزه دارایی‌های رمز ارزی وجود دارد که منجر به افزایش کلاهبرداری و ضعف در محافظت از کاربران می‌شود. بنابراین، همکاری بین‌المللی، استفاده از فناوری‌های نوین برای ردیابی تراکنش‌ها و ایجاد چارچوب‌های حقوقی جامع، از جمله راهکارهای مؤثر برای مقابله با جعل و کلاهبرداری در این حوزه است.

برای هماهنگی قوانین ارزهای مجازی در سطح بین‌المللی، تشکیل نهادهای بین‌المللی متخصص یکی از راهکارهای اصلی است. این نهادها می‌توانند وظیفه نظارت، تنظیم و هماهنگی قوانین ارزهای دیجیتال را بر عهده گیرند و به عنوان مرجعی جهانی عمل کنند. این نهادها می‌توانند مشابه سازمان‌هایی مانند [۱۸]عمل کنند که در زمینه مبارزه با پولشویی و تأمین مالی تروریسم فعالیت می کند .این نهادها می‌توانند استانداردهای بین‌المللی تعیین کنند و کشورها را ترغیب به پیروی از این استانداردها کنند.یکی از مهم‌ترین زمینه‌ها برای هماهنگی بین‌المللی، تنظیم قوانین ضد پولشویی و تأمین مالی تروریسم است. ارزهای دیجیتال به دلیل ماهیت غیرشفاف و غیرمتمرکز خود، اغلب به عنوان ابزاری برای پولشویی و فرار از تحریم‌ها استفاده می‌شوند(زارع قاجاری و قائم مقامی، ۵۴:۱۳۹۲). بنابراین، کشورها می‌توانند با تدوین قوانین مشابه در این حوزه، به کاهش این نوع فعالیت‌ها کمک کنند. به عنوان مثال، الزام صرافی‌های ارز دیجیتال به شناسایی مشتریان (KYC) و گزارش تراکنش‌های مشکوک می‌تواند به عنوان یک استاندارد بین‌المللی تعریف شود.

همکاری قضایی و اطلاعاتی بین کشورها نیز ضروری است. این همکاری می‌تواند شامل تبادل اطلاعات درباره مجرمان بین‌المللی، تراکنش‌های مشکوک و فعالیت‌های غیرقانونی باشد(Higgins,2016). به عنوان مثال، وزارت دادگستری ایالات متحده با هماهنگی با سازمان‌های نظارتی مانند SEC وCFTC ، تلاش می‌کند تا از مصرف‌کنندگان محافظت کند و نظارت کارآمدتری داشته باشد. این مدل می‌تواند به عنوان الگویی برای همکاری بین‌المللی در دیگر کشورها مورد استفاده قرار گیرد(لارنت چیتن و همکاران، ۲۸۷:۱۴۰۱).

یکی دیگر از زمینه‌های مهم برای هماهنگی بین‌المللی، تنظیم قوانین مالی و مالیاتی در حوزه ارزهای دیجیتال است. برخی کشورها ارزهای دیجیتال را به عنوان دارایی مالی محسوب کرده و مالیات بر آن دریافت می‌کنند، در حالی که کشورهای دیگر ممکن است این رویکرد را نداشته باشند(Goldman et al.2017)

تدوین قوانین مشترک در این زمینه می‌تواند به کاهش فرار مالیاتی و افزایش شفافیت کمک کند.تشویق کشورها به منعقد کردن توافق‌های چندجانبه نیز برای رسیدن به هماهنگی بین‌المللی ضروری است. این توافق‌ها می‌توانند شامل تعهداتی برای هماهنگی قوانین داخلی، تبادل اطلاعات و همکاری قضایی باشند. به عنوان مثال، وزارت خزانه‌داری ایالات متحده بر نیاز فوری به قوانین ارزهای دیجیتال برای مبارزه با فعالیت‌های مجرمانه جهانی و داخلی تأکید کرده است(Ivantsov et al, 2019). این رویکرد می‌تواند به عنوان الگویی برای کشورهای دیگر مورد استفاده قرار گیرد. استفاده از فناوری‌های نوین مانند بلاک‌چین و هوش مصنوعی نیز می‌تواند به عنوان ابزاری برای نظارت و هماهنگی بین‌المللی مورد استفاده قرار گیرد. به عنوان مثال، استفاده از بلاک‌چین برای ردیابی تراکنش‌های غیرقانونی و اشتراک اطلاعات بین کشورها می‌تواند به کاهش جرایم کمک کند. علاوه بر این، توسعه پلتفرم‌های مشترک برای نظارت و گزارش‌دهی نیز می‌تواند به هماهنگی بین‌المللی کمک کند.

۵- رویکرهای نوین پیشگیرانه

رویکرهای نوین پیشگیرانه در برابر جعل و کلاهبرداری در حوزه ارزهای دیجیتال، مستلزم تلفیقی از راهکارهای حقوقی، فنی و آموزشی است. با توجه به پیچیدگی‌های فضای مجازی و ظهور روش‌های نوین کلاهبرداری، سیاست‌گذاران و متخصصان باید به‌صورت یکپارچه عمل کنند تا بتوانند از دارایی کاربران و سرمایه‌گذاران در برابر تهدیدات بالقوه محافظت کنند.تعیین وضعیت حقوقی ارزهای دیجیتال و صرافی‌ها به‌عنوان یک ضرورت در سیاست‌گذاری حقوقی مطرح است. این موضوع شامل تعیین مسئولیت‌های قانونی صرافی‌ها، ایجاد مکانیزم‌های نظارتی و الزامات شفافیت می‌شود. همچنین، با توجه به اینکه قوانین سنتی کیفری ممکن است توانایی پوشش جرایم نوین را نداشته باشند، تصویب قوانین خاصی که به‌طور مستقیم به جرایم مرتبط با ارزهای دیجیتال می‌پردازند، ضروری است.کاربران باید قبل از انجام معاملات، از اعتبار و اصالت صرافی‌ها اطمینان حاصل کنند. این امر مستلزم ایجاد نظام نظارتی قوی بر صرافی‌ها و ارائه مجوزهای قانونی به آنهاست. علاوه بر این، کلاهبرداران اغلب از تبلیغات

[۱۸] FATF

گمراه‌کننده استفاده می‌کنند؛ بنابراین، الزام صرافی‌ها و شرکت‌های مرتبط به رعایت اصول اخلاقی در تبلیغات و جلوگیری از استفاده غیرقانونی از نام‌های معتبر می‌تواند مؤثر باشد(رضا سلطان زاده و رفیعی، ۱۲:۱۴۰۲).

۵-۱- نظریه بازدارندگی دیجیتال عقلانی و سیاست‌گذاری نوین کیفری

تحلیل‌های جستار نشان می‌دهد که نظریه انتخاب عقلانی در فضای رمزارزها نیازمند تکمیل و انطباق با ویژگی‌های منحصربه‌فرد این محیط است. از این‌رو، نظریه‌ای نوین تحت عنوان «بازدارندگی دیجیتال عقلانی» ارائه می‌شود که تلفیقی از مبانی انتخاب عقلانی و ویژگی‌های خاص فناوری بلاکچین است. بر اساس این نظریه، رفتار مجرمانه در حوزه رمزارزها نتیجه محاسبات عقلانی مبتنی بر حداکثرسازی سود و حداقل‌سازی خطر است، اما این محاسبات تحت‌تأثیر عواملی چون گمنامی تراکنش‌ها، نبود نظارت متمرکز و پیچیدگی‌های فنی بلاکچین قرار دارد.

برای مثال، در پدیده ایجاد توکن‌های جعلی، مجرم با هزینه‌ای اندک می‌تواند یک دارایی دیجیتال تقلبی تولید کند و با تبلیغات گسترده در شبکه‌های اجتماعی، سرمایه‌گذاران ناآگاه را جذب نماید. سود چنین جرمی می‌تواند در عرض چند روز به میلیون‌ها دلار برسد، در حالی که ریسک شناسایی و مجازات به‌دلیل ساختار غیرمتمرکز فناوری پایین است. نظریه بازدارندگی دیجیتال عقلانی در پاسخ به این معضل پیشنهاد می‌کند که قوانین کیفری به‌گونه‌ای اصلاح شوند که هزینه ارتکاب جرم به‌طور چشمگیری افزایش یابد؛ برای مثال، اعمال جریمه‌های متناسب با کل سود حاصل از جرم یا حتی فراتر از آن. همچنین، افزایش احتمال کشف جرم از طریق توسعه ابزارهای ردیابی دیجیتال و همکاری‌های بین‌المللی می‌تواند معادله عقلانی مجرمان را بر هم بزند.

۵-۲- بهره‌گیری از نظریه انتخاب عقلانی در پیشگیری از جرایم رمزارزی

جستار حاضر با تمرکز بر جرایم جعل و کلاهبرداری در حوزه ارزهای رمزپایه، از نظریه انتخاب عقلانی به‌عنوان چارچوبی برای تحلیل و ارائه راهکارهای حقوقی استفاده می‌کند. بر اساس این نظریه، مجرمان رفتار خود را با محاسبه سود و زیان احتمالی تنظیم می‌کنند و ارتکاب جرم را زمانی برمی‌گزینند که خطر کشف و مجازات پایین و سود بالقوه بالا باشد. در فضای غیرمتمرکز رمزارزها، گمنامی تراکنش‌ها و فقدان نهاد مرکزی، ریسک ارتکاب جرم را به حداقل می‌رساند؛ در حالی که شیوه‌هایی مانند طرح‌های پانزی یا کلاهبرداری‌های مبتنی بر پامپ و دامپ، سودی سریع و چشمگیر به همراه دارند. (عیوضلو و همکاران،۵۹:۱۳۹۸). برای مثال، در یکی از پرونده‌های بین‌المللی، کلاهبرداران با طراحی یک پروژه سرمایه‌گذاری جعلی در حوزه رمزارز توانستند میلیون‌ها دلار از سرمایه‌گذاران خرد جمع‌آوری کنند و به‌دلیل پیچیدگی ردگیری تراکنش‌ها، پیگیری قضایی با دشواری جدی روبه‌رو شد. این نمونه نشان می‌دهد که محاسبه عقلانی مجرمان بر پایه سود بالا و خطر پایین شکل می‌گیرد. بر همین مبنا، جستار پیشنهاد می‌کند که قوانین کیفری ایران بازنگری شوند تا هزینه ارتکاب چنین جرایمی افزایش یابد. برای نمونه، در مورد کلاهبرداری‌های رمزارزی فرامرزی، افزایش حداقل مجازات حبس به بیش از هفت سال و الزام به رد مال همراه با جریمه‌ای دو برابر ارزش مال مسروقه، می‌تواند انگیزه مجرمان را از منظر عقلانی تضعیف کند. همچنین، به‌کارگیری ابزارهای ردیابی دیجیتال در فرایندهای قضایی موجب افزایش احتمال کشف جرم و برهم زدن معادله محاسباتی مجرمان می‌شود. تجربه اتحادیه اروپا نیز در این زمینه قابل‌توجه است؛ زیرا با تصویب مقررات ضدپولشویی و الزام صرافی‌های رمزارزی به شفافیت تراکنش‌ها، هزینه‌های انطباق بالا رفت و در نتیجه بسیاری از الگوهای مجرمانه در این فضا کاهش یافت

رویکردهای نوین پیشگیرانه در حوزه ارزهای دیجیتال باید به‌صورت چندبعدی و همه‌جانبه باشند. ترکیب قوانین دقیق، فناوری‌های امنیتی پیشرفته، آموزش کاربران و همکاری بین‌المللی می‌تواند به کاهش جعل و کلاهبرداری در این حوزه کمک کند. با این حال، به‌دلیل ماهیت پویا و نوین این تهدیدات، نیاز به به‌روزرسانی مستمر این رویکردها وجود دارد.یکی از تکنیک‌های نوین در پیشگیری از جرایم ارزهای دیجیتال، استفاده از قراردادهای هوشمند است که به‌صورت خودکار و تحت شرایط از پیش تعیین‌شده عمل می‌کنند. این نوع قراردادها با کاهش دخالت انسانی و افزایش شفافیت، احتمال سوءاستفاده و کلاهبرداری را کاهش می‌دهند. همچنین، فناوری‌های تحلیل داده‌ها و یادگیری ماشین نقش مهمی در شناسایی الگوهای مشکوک در معاملات ارزهای دیجیتال ایفا می‌کنند. این ابزارها قادرند با ترکیب داده‌های موجود در فضای حقیقی و مجازی، فعالیت‌های مجرمانه را زودتر شناسایی کنند(وراثی، ۶:۱۴۰۰).

از این جهت، برای پیشگیری از جعل و کلاهبرداری، فناوری‌های مختلفی وجود دارند که می‌توانند به شناسایی و مقابله با این جرایم کمک کنند. فناوری‌های بیومتریک مانند تشخیص چهره، اثر انگشت و اسکن شبکیه چشم، به دلیل قابلیت شناسایی دقیق هویت افراد، در جلوگیری از جعل هویت و سرقت اطلاعات مؤثر هستند. هوش مصنوعی و یادگیری ماشین نیز با تحلیل داده‌های حجیم و شناسایی الگوهای مشکوک، می‌توانند به پیش‌بینی و شناسایی رفتارهای مجرمانه کمک کنند.

استفاده از اسناد الکترونیکی و فناوری بلاک‌چین نیز به دلیل ماهیت غیرمتمرکز و رمزنگاری‌شده، از جعل اسناد و تراکنش‌ها جلوگیری می‌کند. هولوگرام‌های ضد جعل نیز به عنوان یک روش سنتی، در صنایع مختلف برای اطمینان از اصالت محصولات استفاده می‌شوند علاوه بر این، نرم‌افزارهای آنتی‌ویروس و ابزارهای امنیت سایبری می‌توانند از دسترسی غیرمجاز و حملاتی مانند IP Spoofing محافظت کنند. داده‌کاوی و تحلیل رفتاری نیز با شناسایی فعالیت‌های غیرعادی، به مقامات کمک می‌کنند تا زودتر از وقوع جرایم اطلاع پیدا کنند. قراردادهای هوشمند می‌توانند به‌طور مؤثری از تقلب در معاملات جلوگیری کنند، زیرا این قراردادها به‌صورت خودکار و بر اساس شرایط از پیش تعیین‌شده عمل می‌کنند و نیازی به دخالت انسانی ندارند(شاملو و خلیلی پاجی،۶۷:۱۳۹۹). قراردادهای هوشمند با تکیه بر بلاکچین و رمزنگاری، خطاهای انسانی و امکان تقلب را به‌طور چشمگیری کاهش می‌دهند و در حوزه‌هایی مانند زنجیره تأمین و رأی‌گیری الکترونیکی، شفافیت و امنیت را تقویت می‌کنند. بااین‌حال، آسیب‌پذیری‌های فنی و احتمال هک، ضرورت حسابرسی شخص ثالث و استانداردسازی امنیتی را برجسته می‌سازد. از منظر تحلیلی، این قراردادها با تغییر محاسبات عقلانی مجرمان—از طریق کاهش سود و افزایش خطر کشف—در چارچوب «بازدارندگی دیجیتال عقلانی» عمل کرده و به‌عنوان ابزاری کارآمد برای پیشگیری فناورانه از جرایم مالی و سایبری مطرح می‌شوند. (اکرمی۴۳:۱۱۳۹۵).

٦- نتیجه گیری

یکی از واقعیت‌های برجسته در دنیای معاصر، گسترش روزافزون استفاده از رمزارزها در مبادلات اینترنتی و تراکنش‌های مالی است. این فناوری نوین که بر پایه بلاکچین شکل گرفته، تحولات چشمگیری در نظام پولی جهان ایجاد کرده و به تدریج جایگاه سنتی پول‌های فیزیکی و حتی نظام‌های بانکی را تحت‌الشعاع قرار داده است. پیشرفت‌های فناوری، به‌ویژه در حوزه فناوری‌های مالی ، شیوه زندگی افراد، نحوه انجام معاملات و حتی ساختارهای مالی دولت‌ها را دگرگون ساخته است.

ارزهای دیجیتال با ویژگی‌هایی چون غیرمتمرکز بودن، حذف واسطه‌های مالی سنتی (تعامل نظیر به نظیر) و حفظ نسبی هویت طرفین معامله، فرصت‌های نوینی را در اقتصاد دیجیتال پدید آورده‌اند. با این حال، همین خصوصیات بستر شکل‌گیری چالش‌های حقوقی و امنیتی، به‌ویژه در زمینه جعل، کلاهبرداری و سایر جرایم سایبری را نیز فراهم کرده است.

در ایران، سیاست‌گذاران و نهادهای مقررات‌گذار رویکردی متحول نسبت به ارزهای مجازی داشته‌اند. در ابتدا، با توجه به مخاطرات بالقوه این فناوری و امکان استفاده از آن در جرایمی همچون پولشویی، رویکرد غالب بر ممنوعیت استفاده و مبادله رمزارزها استوار بود. این رویکرد بیانگر تمرکز جدی بر جنبه‌های جرم‌شناختی و نگرانی‌های امنیتی مرتبط با آن‌ها بود. اما به مرور، تغییراتی در این سیاست پدید آمد؛ انتشار پیش‌نویس سند »الزامات و ضوابط فعالیت در حوزه ارزهای مجازی «در تاریخ ۱۳۹۷/۱۱/۸ نشان‌دهنده فاصله گرفتن از ممنوعیت مطلق و حرکت به سوی تنظیم‌گری این حوزه بود. چنین تغییری، نشانه تلاش سیاست‌گذاران برای ایجاد تعادل میان کاهش تهدیدات امنیتی و حقوقی از یک سو و بهره‌برداری از فرصت‌های اقتصادی از سوی دیگر است.

با وجود این تحولات، همچنان مسائلی چون ایجاد رمزارزهای جعلی، کلاهبرداری از طریق فریب کاربران، و سوءاستفاده از خلأهای نظارتی و فنی، به دلیل نبود شفافیت کافی و دشواری شناسایی و ردیابی مجرمان، تهدیدی جدی برای نظام حقوقی و مالی کشور محسوب می‌شوند. رفع این چالش‌ها مستلزم تدوین قوانین جامع‌تر، شفاف‌تر و هماهنگ‌تر است تا ضمن تسهیل نوآوری و توسعه اقتصادی، از امنیت کاربران و سلامت فضای مالی دیجیتال نیز صیانت کند.

در این راستا، بهره‌گیری از رویکردهای نوین پیشگیرانه می‌تواند نقش تعیین‌کننده‌ای ایفا نماید. به‌کارگیری ابزارهای تحلیل داده‌ها و یادگیری ماشین برای شناسایی الگوهای مشکوک، توسعه سامانه‌های ردیابی تراکنش‌های بلاکچین برای مقابله با جرایمی چون پولشویی و هک کیف‌پول‌ها، و نیز آموزش عمومی برای افزایش آگاهی کاربران درباره روش‌های ایمن‌سازی دارایی‌های دیجیتال، همگی از جمله راهکارهای مؤثر در این زمینه‌اند.

علاوه بر این، همکاری‌های بین‌المللی و استفاده از تجربه کشورهای پیشرو می‌تواند زمینه‌ساز ارتقای سیاست‌های داخلی و تدوین چارچوب‌های حقوقی کارآمدتر شود. از این رو، با توجه به ماهیت پویا و در حال تحول ارزهای مجازی، ایجاد مقررات دقیق اما انعطاف‌پذیر همراه با راهکارهای فناورانه پیشگیرانه، بهترین مسیر برای کاهش جرایم مرتبط با رمزارزها و تقویت اعتماد عمومی به این فناوری خواهد بود. این رویکرد، نه‌تنها به امنیت کاربران کمک می‌کند، بلکه به توسعه پایدار صنعت رمزارزها در چارچوبی قانونی و مطمئن نیز منجر خواهد شد.

منابع و ماخذ

۱. اکرمی، سام؛ اکرمی، سعیده. (۱۳۹۵). پیشگیری غیرکیفری در جرائم اینترنتی . کنفرانس ملی چارسوی علوم انسانی . https://civilica.com/doc/721009/certificate/print/

۲. خادمان، محمود؛ کوشا، ابوطالب؛ نوری، فاطمه. (۱۴۰۰). شناسایی ماهیت حقوقی رمزارزها با تحلیل ساختاری آن‌ها در نظام حقوقی ایران. مجله حقوقی دادگستری ، ۸۵(۱۱۵)، ۳۴۹-۳۷۲ .

۳. خداوردی آرش، حسین؛ رضوی، محمد؛ پورزمانی، زهرا. (۱۴۰۳). رویکرد نظام حقوقی ایران در خصوص اعتبار رمز ارزهای مجازی. تعالی حقوق ، ۱۰(۳)، ۴۱-۷۹ .

۴. خلیلی پاجی، عارف. (۱۴۰۰). ارزیابی رویکرد پیشگیری ریسک‌مدار از مخاطرات جنایی ارزهای مجازی. حقوق فناوری های نوین ، ۲(۳)، ۲۴۷-۲۶۵ https://doi.org/10.22133/clj.2021.313012.1066 .

۵. خلیلی پاجی، عارف. (۱۴۰۰). ارزهای مجازی: جهانی شدن بزهکاری و سیاست جنایی . تهران: میزان.

۶. رحیمی، علی؛ امینی نیا، عاطفه. (۱۴۰۰). رمز ارزها، چالش‌ها و جرایم پیرامون آن. قانون یار ، ۵(۱۸)، ۰-۰ . https://sid.ir/paper/1023317/fa

۷. رضازاده سلطان آباد، محمد؛ رفیعی، علی. (۱۴۰۲). نقش هوشمندسازی قراردادها در پیشگیری از ارتکاب جرائم مرتبط با ارزهای دیجیتال. پژوهش‌های جرم‌شناسی کاربردی ، ۱(۱)، ۱-۲۲ .

۸. زارع قاجاری، فردوس؛ قائم مقامی، علی. (۱۳۹۲). استانداردهای بین‌المللی مبارزه با پولشویی و تأمین مالی تروریسم)توصیه‌های چهل‌گانه گروه ویژه اقدام مالی .تهران: نشر تاش.

۹. سلطانی، محمد؛ اسدی، حمید. (۱۳۹۴). ماهیت حقوقی پرداخت در پول الکترونیک. پژوهشنامه حقوق اسلامی ، ۱۶(۱)، ۷۹-۱۰۲.

۱۰. سیاه‌بیدی کرمانشاهی، سعید؛ ثالث مؤید، احمدعلی. (۱۳۹۶). حقوق کیفری اقتصادی «پولشویی» . چاپ اول، تهران: انتشارات میزان.

۱۱. سیاه‌بیدی کرمانشاهی، سعید؛ رحیمی‌نیت، ایمان؛ ملک‌زاده رودبنه، ریحانه. (۱۳۹۷). حقوق کیفری اقتصادی . چاپ اول، تهران: انتشارات جنگل.

۱۲. شاملو، باقر؛ خلیلی پاجی، عارف. (۱۳۹۹). مجازی شدن بزهکاری یقه سفیدی در پرتو ارزهای مجازی. حقوقی دادگستری ، ۸۴(۱۱۰)، ۶۷- ۹۹ . https://sid.ir/paper/402058/fa

۱۳. صادقی، محسن؛ ناصر، مهدی. (۱۴۰۰). مطالعه تطبیقی چالش‌ها و راهکارهای به‌کارگیری ارزهای رمزنگاری‌شده دیجیتالی در نظام حقوقی ایران و آمریکا. مطالعات حقوق خصوصی ، ۲۷۵-۲۹۳.

۱۴. عیوضلو، حسین؛ موسویان، سیدعباس؛ رضائی صدرآبادی، محسن؛ نوری، جواد. (۱۳۹۸). تحلیل فقهی اقتصادی استخراج ارزهای مجازی در نظام اقتصادی اسلام؛ (مطالعه موردی بیت کوین). معرفت اقتصاد اسلامی ، ۱۱(۱)، ۵۷-۷۲ . https://sid.ir/paper/359680/fa

۱۵. لارنت چیتن، پیتر و همکاران. (۱۴۰۱). پیشگیری از پولشویی و تأمین مالی تروریسم؛ راهنمای عملی برای ناظران بانکی (ترجمه مریم کشتکار). تهران: نشر تاش.

۱۶. مظلومان، حسین. (۱۴۰۰). جرایم و مجازات‌های بیت‌کوین و بلاک‌چین در حقوق ایران . تهران: مهرکلام.

۱۷. نبوی، سیدمهدی؛ صابر، محمود. (۱۳۹۹). مطالعه تطبیقی چالش‌های نظام عدالت کیفری ایران در دادرسی جرایم مرتبط با ارزهای مجازی. پژوهش‌های حقوق تطبیقی (مدرس علوم انسانی) ، ۲۴(۱)، ۱۷۹-۲۰۸ . https://sid.ir/paper/367562/fa

۱۸. وراثی، غزل. (۱۴۰۰). سیاست کیفری و ابعاد پیشگیری از جرایم در حوزه ارزهای دیجیتالی. قانون یار ، ۵(۱۹)، ۰-۰. https://sid.ir/paper/1023704/fa

19. FATF. (2019). VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS: GUIDANCE FOR A RISK-BASED APPROACH.
20. Goldman, Z., Maruyama, E., Rosenberg, E., Saravalle, E., & Solomon-Strauss, J. (2017). Terrorist use of virtual currencies . CNAS Publication, Washington.
21. Higgins, S. (2016, February 22). California bankruptcy judge says bitcoin is property, not currency. Coindesk . Retrieved April 2, 2018, from https://www.coindesk.com/bankruptcy-judge-bitcoin-property-currency
22. Hutchings, A. (2023). Cybercrime trajectories: An integrated theory of initiation, maintenance and desistance. In T. Holt (Ed.), Crime online: Correlates, causes, and context (3rd ed., pp. 117–140). Durham: Carolina Academic Press. https://www.cl.cam.ac.uk/~ah793/papers/2016trajectories.pdf
23. Ivantsov, S., Sidorenko, E., Spasennikov, B., Berezkin, Y., & Sukhodolov, Y. (2019). Cryptocurrency-related crimes: Key criminological trends. Russian Journal of Criminology, 13 (1), 85–93.