Legal Research, Vol 29, Issue 115, 2026: 243-260 Print ISSN: 1024-0772 Online ISSN: 3060-5911

Journal of Legal Research
https://lawresearchmagazine.sbu.ac.ir/

Orginal Article

The Impact of Metaverse Technology on the Rate of Financial Crimes

Mahmoud Mahdavi[1], Mohammad Rouhollahi[2], Seyyed Mahyar Morovati[3]

Highlights

- Within the metaverse, due to the decentralized nature of blockchain and user anonymity, criminals can convert vast sums into assets such as NFTs, virtual land, or related cryptocurrencies to engage in money laundering.
- Unlike bank transfers, which are traceable, the origin of illicit funds in the metaverse is easily concealed; consequently, this technology has become a convenient channel for laundering proceeds derived from both traditional and crypto-related crimes.
- The metaverse is an attractive platform for terrorist financing and support, as it lowers training costs, enables anonymous funding through cryptocurrencies, and diminishes the effectiveness of financial blacklists.

ABSTRACT

Introduction

With the development of science, various technologies have also grown rapidly or new technologies have emerged. One of these new technologies, which is known as a revolution in the field of information and communication technology (ICT), is metaverse technology. As a new emerging technology, this technology is a world consisting of virtual spaces in which people can communicate with each other in the virtual world instead of being physically together, a world that provides its inhabitants with the possibility of communication and gaining various experiences regardless of the limitations of the Internet. Since this technology is still growing and has not reached the stage of development, it has faced challenges such as deficiencies in regulations, technical security, and privacy, which have led to the emergence of some crimes in this context. But one of the less studied aspects of this technology is its impact on financial crimes, because the metaverse is becoming a vast world there is a huge financial turnover in it, and on the other hand, people in it can communicate like in the physical and material world. One of the social phenomena in the real world is also crime, and since a large amount of wealth is circulating in this technology, metaverse is likely to be a suitable platform for committing some financial crimes, and this can lead to challenges in cybersecurity and e-commerce. Therefore, this research examines the impact of metaverse

How to Cite: Mahdavi, Mahmoud, Rouhollahi, Mohammad, Morovati, Seyyed Mahyar, "The Impact of Metaverse Technology on the Rate of Financial Crimes", Legal Research, Vol. 29, No. 115, 2026, pp: 243-260.

DOI: https://doi.org/10.48308/jlr.2025.239696.2889 Received: 29/04/2025-Accepted: 20/10/2025

1. Assistant Professor, Faculty of Law & Political Science, University of Tehran, Tehran, Iran
2. L.L.M., Faculty of Law & Political Science, University of Tehran, Tehran, Iran
Corresponding Author Email: mhmdrwhallhy00@gmail.com
3. L.L.M Student, Faculty of Law & Political Science, University of Tehran, Tehran, Iran

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

technology on increasing the rate of financial crimes, because this question is very important. metaverse technology today has a significant impact on individuals' economic and social relations.

Methods
The research is conducted using a descriptive-analytical method and uses library- based researches such as books and scholary articles.

Results and Discussions
The findings of the study show that metaverse technology, using its capacity, is a suitable platform for committing crimes, especially financial crimes. This technology is suitable for committing financial crimes due to its capabilities. One of the crimes that can be committed using this ability is fraud, which can be done both in a computerized way, which is done by deceiving a computer system, and traditionally, which is done by creating fraudulent data with the intention of deceiving the audience. Another crime that may be committed through the metaverse platform is money laundering. Metaverse technology is a good option for money laundering, due to the anonymity of its users, and people can launder their dirty money by buying and selling NFTs and make their money obtained from illegal methods appear clean. Theft is also one of the other crimes that can be committed from the metaverse space. In the metaverse, since data is obtained from various sources, the possibility of theft also increases. Data and information theft can occur at any stage of data collection, storage, and processing. For example, someone in the metaverse may steal an existing object that is visible to the naked eye, has been paid for, and has value. Another financial crime that can be committed in the metaverse, and perhaps one of the most important financial crimes committed in this space, is the financing of terrorism. metaverse can facilitate terrorism in two ways. First, it reduces its costs; for example, this technology facilitates the training of people for terrorist purposes. In fact, terrorists use various online platforms to train attackers. Through the metaverse and augmented reality or virtual reality, they can teach how to make the manufacture of chemical weapons, the construction of explosive devices, and how to attack infrastructure or conduct cyber-attacks. without all of them being present in a specific location. In the second step, individuals can finance terrorists and terrorist groups by donating valuable NFTs to them without being identified.

Conclusion
Significant advances in the field of information and communication technology have led to the emergence of new technologies, one of which is the metaverse. This growing technology has the ability to collect and analyze a vast amount of data and has affected various areas such as economics, politics, and social relations. This technology is rapidly expanding and becoming widespread due to its advantages, but since metaverse is still being completed and has shortcomings, it faces challenges such as lack of adequate regulations, deficiencies in supervision, the inability of security systems to detect and prevent crimes, privacy, technical security, and the possibility of fraud, and provides the ground for committing crimes. Due to the unprecedented opportunities in the field of financial activities, one of the categories of crimes that the metaverse provides a suitable platform for committing is financial crimes, and metaverse technology, as an emerging phenomenon, may have a significant impact on increasing the commission of financial crimes. this study finds that the use of metaverse technology, which is an emerging technology under development and itself uses other technologies such as virtual reality, blockchain and other technologies, can create conditions that increase the commission of financial crimes such as fraud, theft, money laundering or even terrorist financing. In other words, it creates conditions for its users to commit these crimes. Or, due to the challenges it faces, it causes users to be victims of financial crimes. This result shows that we need a comprehensive and broad view of the social and economic impacts of metaverse technology.

Keywords: New Crimes, Financial Crimes, Information Technology, Metaverse.

فصلنامه تحقیقات حقوقی
https://lawresearchmagazine.sbu.ac.ir/

مقاله علمی-پژوهشی

تأثیر فناوری متاورس بر میزان ارتکاب جرائم مالی

محمود مهدوی[۱]، محمد روح اللهی[۲]، سید مهیار مروتی[۳]

نکات برجسته

- در بستر متاورس به‌دلیل ماهیت غیرمتمرکز بلاک‌چین و ناشناس بودن کاربران، مجرمان می‌توانند مبالغ هنگفت را به دارایی‌هایی مثل NFT ، زمین مجازی یا رمزارزهای مرتبط تبدیل کنند و مرتکب پولشویی شوند.
- برخلاف انتقال بانکی که قابل ردیابی است، در متاورس مبدأ وجوه غیرقانونی به‌راحتی پنهان می‌ماند و این فناوری به کانالی مناسب برای تطهیر پول‌های حاصل از جرایم واقعی یا رمزارزی تبدیل شده است.
- متاورس برای تأمین مالی و پشتیبانی تروریسم جذاب است چراکه هم هزینه آموزش را کاهش می‌دهد و هم با ارزهای رمزنگاری‌شده، تأمین مالی ناشناس را ممکن می‌سازد و فهرست‌های سیاه مالی را کم‌اثر می‌کند.

چکیده

با پیشرفت علم و تکنولوژی شاهد گسترش فناوری‌ها در تمام شاخه‌های علوم هستیم. یکی از فناوری‌های نوپدید در علوم اطلاعات و ارتباطات، فناوری متاورس است که به‌دلیل ظرفیت‌ها و امکاناتی که در اختیار کاربران خود قرار می‌دهد به‌سرعت درحال‌گسترش و همه‌گیر شدن است و از آنجایی که این فناوری همچنان درحال‌رشد بوده و به مرحله تکامل نرسیده با چالش‌هایی از قبیل نقص در مقررات، امنیت فنی و حریم خصوصی مواجه شده که سبب بروز برخی جرائم در این بستر شده است و سؤالی را که به ذهن متبادر می‌کند این است که این فناوری چه تأثیری بر میزان جرائم مالی دارد؟ به‌دلیل گستردگی امکاناتی که متاورس در اختیار کاربران خود در حوزه‌های مختلف قرار می‌دهد، در رابطه با این فناوری در حوزه‌های مختلف مانند علم روان‌شناسی و پزشکی تحقیقاتی نیز صورت گرفته است، اما در حوزه علم حقوق در کشور ما آن‌طور که باید به این فناوری پرداخته نشده است. ازاین‌رو پژوهش ذیل به روش توصیفی - تحلیلی به ارتباط فناوری متاورس و میزان جرائم مالی پرداخته است و نتایج نشان می‌دهد، فناوری متاورس که یک فناوری درحال‌توسعه است، با توجه به ویژگی‌هایش مانند غیرمتمرکز بودن، عدم احراز هویت کاربران، نبود نهاد ناظر و ناآگاهی برخی کاربران سبب افزایش جرائمی مانند سرقت، کلاهبرداری، پول‌شویی و تأمین مالی تروریسم می‌شود و به‌منظور پیشگیری از این جرائم می‌شود اقداماتی از قبیل معرفی نهاد ناظر مانند پلیس فتا را انجام داد.

کلید واژگان: جرائم نوین، جرائم مالی، فناوری اطلاعات، متاورس.

استناد به این مقاله: مهدوی، محمود، روح‌اللهی، محمد، مروتی، سید مهیار، « تأثیر فناوری متاورس بر میزان ارتکاب جرائم مالی»، فصلنامه تحقیقات حقوقی، دوره ۲۹، شماره ۱۱۵، مهر ۱۴۰۵، صص: ۲۴۳-۲۶۰.

تاریخ دریافت: ۱۴۰۴/۰۲/۰۹ - تاریخ پذیرش: ۱۴۰۴/۰۷/۲۸ DOI: https://doi.org/10.48308/jlr.2025.239696.2889

۱. استادیار، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران
۲. کارشناس‌ارشد، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران
ایمیل نویسنده مسئول: mhmdrwhallhy00@gmail.com
۳. دانشجوی کارشناسی‌ارشد، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

مقدمه

با گسترش علم، فناوری‌های مختلف نیز به همراه آن به‌سرعت رشد کرده یا فناوری‌های جدید به وجود می‌آیند. یکی از این فناوری‌های جدید که به‌عنوان انقلابی در حوزه فناوری اطلاعات و ارتباطات (ICT) شناخته شده است، فناوری متاورس است. این فناوری به‌عنوان یک تکنولوژی نوظهور، دنیایی را به تصویر می‌کشد که از فضاهای مجازی تشکیل شده است. در این دنیا، افراد می‌توانند بدون حضور فیزیکی در کنار یکدیگر، از طریق محیط‌های مجازی باهم ارتباط برقرار کنند. جهانی که فارغ از محدودیت‌های اینترنت، فرصت برقراری ارتباط و کسب تجربیات متنوع را برای کاربران خود فراهم می‌سازد. در دنیای مجازی متاورس هرچیز که افراد بخواهند در دسترسشان قرار می‌گیرد و می‌توانند شخصیت خود را در آن بسازند و مانند دنیای واقعی در آن زندگی کنند و هرچیز را در آن به‌صورت غیرمتمرکز کنترل کنند بدون اینکه مدیریت آن‌ها در دست نهاد دولتی خاصی باشد[۱]. متاورس که با امکانات گسترده‌اش ازجمله واقعیت افزوده[۲]، واقعیت مجازی[۳] که به‌سرعت درحال‌گسترش است، به‌طور قابل‌توجهی بر روابط اجتماعی و تجاری افراد تأثیر گذاشته و حتی بازارهای مختلف را تحت تأثیر خود قرار داده است. به‌طوری‌که بنا بر گزارش بلومبرگ[۴] تا سال ۲۰۲۴، متاورس به بازار اقتصادی با سرمایه ۸۰۰ میلیارد دلاری مبدل خواهد شد[۵]. در همین راستا شرکت‌های بزرگ تجاری مانند گوچی[۶] با خریداری زمین‌های مجازی در فضای متاورس به تأسیس فروشگاه‌هایی اقدام کرده‌اند که امکان حضور و خرید در فضای متاورس را به کاربران می‌دهد[۷]. اما یکی از جنبه‌های کمتر مورد بررسی این تکنولوژی، تأثیر آن بر جرائم مالی است؛ چراکه متاورس درحال تبدیل شدن به دنیایی گسترده است و گردش مالی هنگفتی نیز در آن وجود دارد و از طرفی افراد در آن می‌توانند مانند دنیای فیزیکی و مادی ارتباط بر قرار کنند، یکی از پدیده‌های اجتماعی در دنیای واقعی نیز جرم است و از آنجایی که حجم زیادی از ثروت در این فناوری در گردش است، احتمال آن می‌رود که بستری مناسب برای انجام برخی جرائم مالی باشد و این امر می‌تواند منجر به ایجاد چالش در امنیت سایبری و همچنین تجارت الکترونیک باشد. ازاین‌رو این مقاله بر آن است تا با روش توصیفی - تحلیلی به بررسی این مسئله بپردازد و تأثیر فناوری متاورس را بر افزایش ضریب جرائم مالی مورد مطالعه قرار دهد؛ چراکه این سؤال بسیار مهم است که این فناوری به‌روز و مهم در روابط اجتماعی و اقتصادی و ... چه تأثیری می‌تواند بر میزان ارتکاب جرائم مالی داشته باشد؟

۱. تبیین مفهوم فناوری متاورس و تکنولوژی‌های مرتبط

برای مشخص کردن ماهیت فناوری متاورس ابتدا به معنای خود واژه می‌پردازیم. واژه متاورس از دو عبارت متا که ریشه‌ای یونانی دارد و در مفهوم به ماورای چیزی گفته می‌شود[۸] و عبارت یونیورس[۹] که به‌معنای جهان و کائنات است، تشکیل

---

۱. محمودی، محسن و سالار صادقی، «متاورس و تأثیر آن بر سبک زندگی»، *مطالعات حقوقی فضای مجازی*، شماره ۲، ۱۴۰۱، ص ۴۶.

2. Augmented Reality

3. Virtual Reality

4. Bloomberg

5. Intelligence, Bloomberg. 2021. Metaverse may be $800 billion market, next tech platform. 12 01. https://www.bloomberg.com/professional/blog/metaverse-may-be-800-billion-market-next-tech-platform/

6. Gucci

۷. محمد باقری، زهرا و سیدمجتبی سیدباقری، «مد سریع در جهان مادی و متاورس»، *فصلنامه مطالعات حقوقی فضای مجازی*، دوره ۱، شماره ۴، ۱۴۰۱، ص ۷۱.

8. Donaldson, Tara. "Year in Review: What Exactly Is the Metaverse? The Simplest Explanation of What It Means for Fashion". 2021, pp 12- 22. https://wwd.com/business-news/business-features/what-is-metaverse-simple-explainermeta-zuckerberg-digital-fashion-1235015619/

9. Universe

شده است. لذا متاورس به‌طور یکپارچه به مفهوم ماورای جهان است. این عبارت نخستین بار در یک رمان در سال ۱۹۹۲ به نام *تصادف برفی*[۱] در مفهوم جهان مجازی به‌موازات جهان فیزیکی به کار رفته است که اهالی آن به وسیله آواتارهای مجازی با یکدیگر به تعامل می‌پرداختند[۲]. اما در عرصه تکنولوژی متاورس بسیار پیچیده‌تر و گسترده است. درابتدای امر به نظر می‌رسد متاورس، پلتفرم‌های دیجیتال در زمان حال یا آینده با تمرکز بر واقعیت افزوده و واقعیت مجازی است. پلتفرم‌هایی نظیر هدست‌های واقعیت مجازی، تلفن‌های هوشمند و مانند این‌ها که این امکان را به افراد می‌دهند تا با دسترسی به محیط سه‌بعدی واقعیت مجازی یا واقعیت افزوده به فعالیت و تعامل با سایر افراد بپردازند[۳]. اما متاورس نه‌فقط به محتوا و تجربه کاربردی در یک دنیای مجازی اطلاق می‌شود، بلکه اهداف و کاربردهای این فناوری بسیار گسترده‌تر از آن است و شامل تعاملات اجتماعی، اقتصادی، فرهنگی و حتی سیاستی افراد با یکدیگر نیز می‌شود. این مفهوم به دنیایی از جهان‌های مجازی که می‌تواند از سکوهای مختلف فناوری ایجاد شود، اشاره دارد. برای مثال، روبلاکس یکی از پلتفرم‌های متاورس است که گیمرها می‌توانند بازی‌های تولید شده توسط کاربر را براساس آن انجام دهند. همچنین این پلتفرم به کاربران اجازه می‌دهد تا اقلام مجازی بخرند و از راه دور در رویدادها، ازجمله کنسرت، مراسم دسته‌جمعی و مهمانی‌ها شرکت کنند. اما طیف وسیع‌تری از کاربردها و فرصت‌هایی فراتر از بازی که متاورس را در حوزه‌های مختلف جذاب می‌کند، وجود دارد[۴]. متاورس در اصل شبکه‌ای گسترده از جهان‌ها و شبیه‌سازی‌های سه‌بعدی پایدار است که به‌طور هم‌زمان و لحظه‌ای پردازش می‌شوند. در این فضا، هویت افراد، اشیای فیزیکی، تاریخ بشر و حتی سیستم‌های پرداخت، انسجام و ارتباط خود را حفظ می‌کنند. این مجموعه می‌تواند هم‌زمان تعداد زیادی از افراد را به‌طور مجازی درون خود جای دهد، بدون اینکه افراد در یک مکان فیزیکی حضور داشته باشند. هرکدام از اعضای کاربر دراین دنیای مجازی در قالب بدن‌های دیجیتالی پیکربندی شده که به آن‌ها آواتار[۵] می‌گویند، نمود مادی پیدا می‌کنند[۶]. متاورس در حقیقت به‌عنوان یک شبکه جهانی مجازی فعالیت می‌کند که در آن کاربران می‌توانند با یکدیگر و همچنین با عناصر مختلف محیط اطراف خود تعامل داشته باشند. در این میان، ارتباط هماهنگ و یکپارچه‌ای میان هویت افراد و ماهیت اشیا وجود دارد که اهمیت ویژه‌ای دارد. در حقیقت انگار افراد به دنیای واقعی اما در شکل مجازی وارد شده‌اند. به عبارتی دیگر، در دنیای متاورس افراد به‌صورت برخط و مجازی به ایفای نقش خود می‌پردازند. این دنیای مجازی، جنبه‌های مختلف تکنولوژی نظیر شبکه‌های اجتماعی، بازی‌های ویدئویی، فناوری واقعیت مجازی (VR) و واقعیت افزوده (AR) و در نهایت بلاک‌چین[۷] را با یکدیگر ادغام می‌کند. به همین دلیل متاورس را می‌توان به دنیایی که توسط واقعیت‌های مجازی و واقعیت‌های افزوده ساخته می‌شود هم نسبت داد و یکی از راه‌های ورود به این دنیای مجازی داشتن هدست

---

1. Snow Crash

۲. عاکفی قاضیانی، موسی، سیدمصطفی میلانی و وحید عاکفی قاضیانی، «متاورس و چالش‌های حقوقی در حوزه حقوق اموال»، *مجله حقوق فناوری‌های نوین*، دوره ۳، شماره ۶، ۱۴۰۱، صص۱۴۴-۱۴۵.

3. Neuburger Jeffrey D., "Proskauer Rose LLP, In the Coming 'Metaverse', There May Be Excitement but There Certainly Will Be Legal Issues", *National Law Review*, Friday, December 3, 2021. https://newmedialaw.proskauer.com/2021/12/03/in-the-coming-metaverse-there-may-be-excitement-but-there-certainly-will-be-legal-issues/ (last visited on: 20/8/2024).

4. Weimann, Gabriel & Dimant, Roy, "The Metaverse and Terrorism: Threats and Challenges". *Perspective on Terrorism. Issue XVII*, Volume 17, Issue 2, 2023, P 93.

5. Avatar

6. Dionisio, J.D.N.; Burns, W.G., III; Gilbert, R., "3D Virtual worlds and the metaverse". *ACM Comput.Surv*, Volume 45, Issue 3, 2013, p 35.

7. Block Chain

واقعیت مجازی و عینک هوشمند واقعیت مجازی در کنار اینترنت پرسرعت است[1].

۱.۱. واقعیت مجازی(VR)

یکی از فناوری‌هایی که متاورس بر آن تمرکز دارد، واقعیت مجازی است. واقعیت مجازی یکی از فناوری‌های نوین در حوزه فناوری‌های اطلاعاتی و ارتباطی است که تغییر عادت در زندگی مردم، گونه‌های مختلف تجارت و راهبردها را در پی داشته است. این فناوری به کاربران اجازه می‌دهد تا به یک محیط مجازی سه‌بعدی وارد شوند که نشانه‌های موجود در یک محیط واقعی را فراهم می‌کند. محققان این ورود به محیط مجازی را با تجربه ذهنی در زمینه‌های مختلف بررسی و مشاهده کردند که این ورود و غوطه‌ور شدن در فضای مجازی سبب می‌شود که افراد خود را به‌طور واقعی حاضر در آن فضا حس کنند و توجه خود را به اشیا و محیط پیرامونی معطوف نمایند[2]. در واقع هنگامی‌که فرد هدست واقعیت مجازی را روی سر خود می‌گذارد، محیطی را مشاهده می‌کند که براساس تغییر موقعیت بدنش تغییر می‌کند و فرد بعد از گذشت زمان اندکی می‌پذیرد که در یک محیط واقعی قرار گرفته است. یک محیط واقعیت مجازی در پلتفرم‌های خاص خود مانند هدست‌های واقعیت مجازی به وجود می‌آید. علاوه‌بر آن به وسیله ابزارهای دیگر می‌شود حواس پنج‌گانه فرد را در آن محیط مجازی تحت تأثیر خود قرار داد تا با ادغام حواس تجربه نزدیک‌تری به واقعیت را به فرد بدهد[3]. با توجه به ساختار متاورس که پیش‌تر گفته شد و تعریف واقعیت مجازی، می‌توان این‌گونه گفت که واقعیت مجازی یکی از المان‌های اصلی متاورس است. زیرا در فضای متاورس، ما انتظار داریم که افراد به‌طور فعال در دنیای مجازی شرکت و از آن استفاده کنند و فناوری واقعیت مجازی می‌تواند یکی از راه‌های ایجاد و ورود به این دنیای مجازی باشد.

۱.۲. واقعیت افزوده (AR)

به‌موازات فناوری واقعیت مجازی، فناوری واقعیت افزوده وجود دارد. در این فناوری دنیای واقعی و تصاویر مجازی با هم ادغام می‌شوند. در واقعیت افزوده ارزش اولیه واقعیت موجود حفظ می‌شود و اطلاعات حساس و مهم آن توسط تولیدات، نرم‌افزارها و سخت‌افزارهای کامپیوتری پوشش داده می‌شوند. به این صورت، یک نمای فیزیکی زنده به دنیای واقعی افراد اضافه می‌شود. عناصر پیرامون همانند داده به وسیله سنسورها دریافت می‌شود و توسط کامپیوتر پردازش می‌شوند. سپس تولیدات کامپیوتری با یک رابطه تعاملی با عناصر محیطی آمیخته می‌شوند؛ به‌طوری‌که به‌صورت اجسام واقعی درک می‌شوند. بنابراین، همان‌طور که اشاره شد، واقعیت افزوده همانند واقعیت مجازی مبتنی‌بر تصاویر ایجاد شده توسط کامپیوتر است و درحالی‌که نمای فیزیکی دارد واقعیت فیزیکی ندارد[4]. این فناوری مبتنی‌بر سه بخش است: بخش اول آن وظیفه دریافت اطلاعات محیطی را برعهده دارد؛ به‌عبارت‌دیگر این بخش مربوط به ورودی داده‌هاست؛ بخش دوم آن وظیفه دریافت اطلاعات از بخش اول و پردازش آن‌ها و تهیه اطلاعات مورد نیاز جهت اضافه کردن به تصویر واقعی است

---

[1]. محمودی و صادقی، منبع پیشین، ص ۴۸.

[2]. Schultze, U.; Brooks, J. A. M.; "An interactional view of social presence: Making the virtual other 'real'", *Information Systems Journal*, Volume 29, Issue 3, pp 710-712.

[3]. Vidal-Balea, A.; Blanco-Novoa, Ó.; Fraga-Lamas, P.; Fernández-Caramés, T.M.; "Developing the Next Generation of Augmented Reality Games for Pediatric Healthcare: An Open-Source Collaborative Framework Based on ARCore for Implementing Teaching, Training and Monitoring Applications", *Sensors*, Volume 21, Issue 5, 2021, pp 2-3.

[4]. مهپور، علیرضا و مهسا اکبری، «تأثیر استفاده از فناوری واقعیت مجازی بر قصد رفتاری مصرف‌کننده در صنعت مسکن»، *فصلنامه توسعه تکنولوژی صنعتی*، شماره ۴۴، ۱۴۰۰، ص ۴.

و بخش سوم، که خروجی سیستم است، وظیفه به نمایش گذاشتن اطلاعات را برعهده دارد که به نمایش گذاشتن نمای فیزیکی از اطلاعات منجر می‌شود[۱]. با توجه به توضیحاتی که داده شد، می‌شود گفت واقعیت افزوده یک فناوری است که به کاربران این امکان را می‌دهد تا در دنیای واقعی خود، اطلاعات یا اشیای دیجیتالی را به‌طور مستقیم اضافه کنند و برای انجام این کار از ابزارهای دیجیتال، مانند گوشی‌های هوشمند، عینک‌های هوشمند یا عینک‌های واقعیت افزوده استفاده می‌شود. ازاین‌رو این فناوری یکی از ابزارهای بسیار مهم برای درک و تجربه بهتر و تعامل بیشتر با متاورس است که به‌مثابه یک جامعه مجازی است.

۱.۳. فناوری بلاک‌چین

بلاک‌چین به مانند پایگاه داده‌ای است که اطلاعات در آن ذخیره می‌شود؛ اما تفاوت یک پایگاه داده و بلاک‌چین در نحوه دسترسی و ساختاردهی به داده‌هاست؛ به‌طوری‌که یک بلاک‌چین از مجوعه بلوک‌ها تشکیل شده است که هرکدام از آن‌ها مجوعه‌ای از داده‌ها یا تراکنش‌هاست و هر بلوک به بلوک قبلی متصل است و یک زنجیره را تشکیل می‌دهند. هنگامی که بلوک از داده‌ها به زنجیره اضافه شود، نمی‌توان آن را بدون اجماع از شبکه حذف کرد یا تغییر داد. ازاین‌رو سبب می‌شود بلاک‌چین‌ها در برابر دست‌کاری یا هک بسیار امن و مقاوم باشند[۲]. در واقع این فناوری یک پایگاه داده است که بین گره‌های شبکه‌های کامپیوتری به اشتراک گذاشته شده است. اهمیت بلاک‌چین‌ها بیشتر به‌دلیل نقششان در سیستم‌های ارزهای دیجیتال برای حفظ یک سابقه و داده امن و غیرمتمرکز از تراکنش‌ها است؛ اما کاربرد بلاک‌چین صرفاً مربوط به ارزهای دیجیتال نیست، بلکه از آن‌ها می‌توان برای تغییرناپذیر کردن داده‌ها در هر صنعت و تجارتی استفاده کرد؛ چراکه بلاک‌چین‌ها از رمزنگاری برای اطمینان از یکپارچگی و امنیت داده‌های ذخیره شده در آن‌ها محافظت و استفاده می‌کنند و تراکنش‌ها و داده‌ها قبل از اینکه به بلاک‌چین وارد و ذخیره شوند، توسط چند گره در شبکه تأیید و اعتبارسنجی می‌شوند تا اطمینان حاصل شود که داده‌ها دقیق و قابل اطمینان هستند[۳]. از آنجایی که فناری بلاک‌چین در ذخیره امن اطلاعات و انتقال آن‌ها کاربرد دارد، با سایر فناوری‌ها ازجمله متاورس تلاقی پیدا می‌کند که این امر می‌تواند تأثیرات جالبی روی متاورس و دنیای مجازی داشته باشد. چراکه کاربران دنیای مجازی نیاز دارند تا اطلاعات خود را در جایی امن ذخیره کنند و بلاک‌چین نیز این امکان را برای آنان فراهم می‌کند.

۲. ویژگی‌های اشیا در متاورس

اشیایی که در دنیای متاورس مورد معامله قرار می‌گیرند، مجازی و غیرواقعی‌اند و منظور این است که مورد معامله در متاورس وجود خارجی و فیزیکی ندارد و ممکن است این سؤال را ایجاد کند که چگونه مورد معامله قرار دادن اشیایی که وجود فیزیکی ندارند و ارزش‌گذاری روی آن‌ها در دنیایی که وجود خارجی و فیزیکی ندارد، ممکن است؟ در ادامه توضیح خواهیم داد هرچند اشیا واقعی و فیزیکی نیستند، موجودند و مالیت دارند.

---

۱. محبی، فاطمه، «تکنولوژی، "واقعیت افزوده" و کاربرد آن در آموزش زیست‌شناسی»، *فصلنامه پژوهش در آموزش زیست‌شناسی*، دوره ۱، شماره ۳، ۱۳۹۸، ص ۷۵.

2. Hayes, Adam, "Blockchain Facts: What Is It, How It Works, and How It Can Be Used", 2023. https://www.investopedia.com/terms/b/blockchain.asp/

3. Iansiti, Marco. Lakhani. Karim, R. "The Truth About Blockchain", *Harvard Business Review*, Volume 95, Issue 1, 2017. PP 118-127.

۲.۱. موجود بودن اشیا

وقتی از اشیای درون متاورس سخن می‌گوییم، منظور اشیایی است که درون فضای مجازی وجود دارند و قابل رؤیت‌اند. برای توضیح بیشتر این امر باید گفت شیء مجازی در فضاهای دیجیتالی، صرفاً مجموعه‌ای از داده‌هاست که این داده‌ها الگوریتم مشخصی دارند و کاربران، آن‌ها را از سایر چیزهایی که در فضای مجازی وجود دارند، تمییز می‌دهند[۱]. این بدین معناست که هر داده‌ای به‌صورت خاص خود نمایان می‌شود و ارتباط کاربران با آن‌ها زنده و واقعی است. ازسوی‌دیگر، بیشتر مفاهیم حقوقی اعتباری‌اند و توسط عرف اعتبار پیدا کرده‌اند و اعتبار آن‌ها ذاتی نیست و با توجه آن آثار حقوقی و ضمانت‌اجرای لازم توسط قانونگذار اعمال می‌شود و از آنجایی که مال مفهوم اعتباری است، پس لزوماً مختص اشیا مادی و ملموس نیست؛ چراکه در تقسیم‌بندی اموال از حیث ماهیت جسمانی آن، به دو دسته مادی و غیرمادی تقسیم می‌شوند. ازاین‌رو اموال غیرمادی وجود خارجی ندارند و قابل لمس نیستند، بلکه فقط وجود ذهنی و اعتباری دارند[۲]. اشیا در فضای مجازی نیز چنین‌اند و هنگامی که از موجود بودن اشیا در فضای مجازی سخن می‌گوییم قابل لمس بودن آن‌ها نیست، بلکه قابل رؤیت‌اند و می‌شود آن‌ها را از طریق برخی ابزارهای دیجتال حس کرد و با آن‌ها ارتباط بر قرار کرد. برای مثال در فناوری واقعیت افزوده (AR) می‌شود به وسیله هدست واقعیت افزوده داده‌های درون فضای مجازی به‌صورت یک شیء عینی درک کرد و حتی از آن همانند یک جسم در عالم واقع بهره برد. البته گفتنی است که داده‌های دیگری نیز وجود دارند که پردازش شده و قابل رؤیت‌اند، ولی برخلاف اشیای عینی متاورس و فضای مجازی که ساختار سه‌بعدی دارند و می‌شود مانند اجسام دنیای واقعی از آن‌ها استفاده کرد، قابل لمس و درک نیستند، ولی موجودیت دارند؛ مانند عکس‌ها، فیلم‌ها، اسناد و یا داده‌های تعاملی مانند اشیا در برخی بازی‌ها کامپیوتری و شبیه‌سازها که قابل رؤیت‌اند و می‌توان از آن‌ها بهره برد.

۲.۲. مالیت داشتن اشیا

مالیت داده‌ها در فضای مجازی به‌دلیل اتفاقاتی از قبیل تخریب و سرقت و ...، که ممکن است برای آن‌ها به وقوع بپیوندد، حائز اهمیت است. در تعریف‌هایی که در ادبیات فقهی از مفهوم مال ارائه شده است، رویکردهای متفاوتی[۳] در رابطه با توصیف مال اتخاذ شده است. یکی‌از مهم‌ترین محورهای تعاریف فقهی مال، رویکرد عرفی به مفهوم مال در قالب میل و رغبت و تلاش عمومی برای به دست آوردن آن است[۴]. به‌عبارت‌دیگر، از دیدگاه عرفی مال چیزی است بیشتر یا همه مردم به دنبال به دست آوردن آن هستند. درخصوص داده‌های دیجیتال نیز باید گفت که ارزش داده‌های دیجیتال، ارزشی ذهنی است و به‌دلیل آنکه تولید عینی در بازار داده‌های دیجیتال وجود ندارد و هیچ دو

---

۱. حسنی، ابوالحسن، ***مالکیت در فضای مجازی از منظر فقهی***، تهران: مرکز ملی فضای مجازی، ۱۳۹۹، ص ۳۵.

۲. عبدی‌پور فرد، ابراهیم و مرتضی وصالی ناصح، «ابعاد فقهی و حقوقی بازی‌های مجازی»، *فصلنامه راهبرد اجتماعی فرهنگی*، دوره ۶، شماره ۲، ۱۳۹۶، ص ۷۰.

۳. فقها در تعریف مال رویکردهای مختلفی اتخاذ کرده‌اند؛ ازجمله برخی از فقها منفعت مطلقه را معیار قرار داده‌اند. (شیخ طوسی، ***المبسوط فی فقه الالمامیة شیخ طوسی***، جلد ۶، تهران: المکتبة المرتضویة، چاپ سوم، ۱۳۸۷، ص۱۲۷)؛ یعنی هرچیز که منفعت داشته باشد مال محسوب می‌شود. برخی دیگر منفعت عقلایی را معیار برای مالیت داشتن در نظر می‌گیرند (نجفی، محمدحسن، ***جواهر الکلام***، جلد ۲۲، بیروت: داراحیاء التراث‌العربی، چاپ هفتم، ۱۳۶۲، ص۳۴۴) و برخی دیگر عرف را معیار مالیت داشتن می‌دانند؛ به‌عبارت‌دیگر، عنصر مال را براساس رفتار عرف جامعه در ارتباط با اشیا می‌سنجند.

۴. عاکفی قاضیانی، میلانی و عاکفی قاضیانی، منبع پیشین، ص ۱۵۰.

داده دیجیتالی در بازار عین هم نیست، ذهن جامعه است که ارزش داده‌های دیجیتال را در بازار تعیین می‌کند[۱]. براساس رویکرد عرفی، صرفاً برخورداری یک شیء از منفعت عقلایی برای تحقق عنوان مال کافی نیست. برخی از فقها در اتخاذ این رویکرد عرفی به تأثیر عواملی چون عرضه و تقاضا نیز اشاره می‌کنند؛ به این معنا که ارزش مبادله یک کالا به‌طور کامل و مستقیم به میزان تمایل اجتماعی نسبت به آن وابسته است. بنابراین، اگر رغبت و تمایل افراد جامعه به کالایی کاهش یابد، قیمت آن نیز به‌تبع آن کاهش پیدا می‌کند[۲]. در علم حقوق نیز در ماده ۳۴۸ قانون مدنی[۳] مالیت داشتن را به مفهوم قابلیت تقویم داشتن و ارزش‌گذاری کردن، معنا کرده‌اند. همچنین برای تعریف حقوقی مال، عناصر آن را ذکر کرده‌اند که این عناصر عبارت‌اند از: قابلیت اختصاص دادن به شخص، قابلیت نقل و انتقال داشتن، نفع عقلایی و ارزش ذاتی[۴]. با توجه به توضیحات گفته شده درخصوص مالیت داشتن و همچنین موجود و قابل رؤیت بودن داده‌ها و اشیا، می‌توان گفت که داده‌ها با توجه به عرف و منفعت عقلایی در فضای مجازی مالیت دارند؛ مانند اشیا درون بازی‌های کامپیوتری که کاربران با پرداخت درون برنامه‌ای منابع مورد نیاز خود درون بازی را ازجمله سکه و پول و نفت و تجربیات سایر چیزها را به دست می‌آورند و مختص آن‌ها می‌شود؛ به‌تبع آن در فضای متاورس نیز می‌توان گفت که این داده‌ها در فضای متاورس دارای ارزش بوده و مالیت دارند؛ چراکه اشیا و داده‌ها در فضای متاورس قابل نقل و انتقال‌اند و به افراد تخصیص می‌یابند و برای صاحبان آن نیز منفعت دارند؛ مانند زمین‌هایی که در این فضای مجازی توسط شرکت گوچی برای سرمایه‌گذاری خرید شد و پیش‌تر نیز به آن اشاره شد.

۳. تعامل متاورس و ارتکاب جرائم مالی

از آنجایی از متاورس به‌عنوان یک جامعه مجازی یاد می‌شود، پس باید این نکته را در خاطر داشت که جرم یکی از پدیده‌های ممکن‌الوقوع در هر جامعه‌ای است تا آنجا که این امکان به وجوب نزدیک می‌شود و در دنیای مجازی متاورس نیز ممکن است جرائمی رخ بدهد؛ برای مثال یکی از جرائمی که در فضای متاورس می‌تواند رخ بدهد آزار و اذیت جنسی است و آواتارها به‌عنوان نمادی برای هویت افرادند و می‌توانند به آزار جنسی اقدام بنمایند[۵]. از طرفی فناوری متاورس می‌تواند زمینه را برای ارتکاب جرائم در دنیای حقیقی مهیا کند؛ مانند پرونده‌ای که در آن یک گیمر بازی‌های انلاین حریف خود را برای اینکه شمشیر مجازی‌اش را فروخت، به قتل رساند[۶]. البته این نوع از جرائم هدف پژوهش نیست و در ادامه به بررسی جرائم مرتبط با اموال و ارتباط آن‌ها با فناوری متاورس خواهیم پرداخت.

---

[۱]. حسین‌زاده سرشکی، اسماء و سیدعلیرضا فروغی، «بررسی فقهی و حقوقی مالیت و مالکیت داده‌های دیجیتال در فضای سایبری»، *دوفصلنامه فقه و حقوق خصوصی*، دوره ۲، شماره ۵، ۱۴۰۴، ص ۴۲.

[۲]. صدر، سیدمحمدباقر، ***اقتصادنا***، قم: مؤسسه بوستان‌کتاب، چاپ دوم، ۱۳۸۵، ص ۱۹۷.

[۳]. بیع چیزی که خرید و فروش آن قانوناً ممنوع و یا چیزی که مالیت و یا منفعت عقلایی ندارد یا چیزی که بایع قدرت تسلیم آن ندارد باطل است، مگر اینکه مشتری خود قادر بر تسلّم باشد.

[۴]. جعفری لنگرودی، محمدجعفر، ***مبسوط در ترمینولوژی حقوق***، جلد ۴، تهران: گنج دانش، چاپ اول، ۱۳۷۸، ص ۳۱۲۶.

[5]. Bermejo Fernandez, Carlos and Hui, Pan, "Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse", *Ethics, and Governance in Metaverse*, 2022,

[6]. online gamer killed for selling virtual weapon(3/1/2024) available at: https://www.smh.com.au/world/online-gamer-killed-for-selling-virtual-weapon-20050331-gdl12j.html/

۳.۱. متاورس و کلاهبرداری

یکی از رایج‌ترین انواع جرائم که کاربران فضای متاورس را تهدید می‌کند، کلاهبرداری است. طبق آمار خبرگزاری‌های خارجی، در سال ۲۰۲۱ ارزش دارایی‌های رمزنگاری شده که هدف ارتکاب جرم کلاهبرداران بوده، حدود ۱۴ میلیارد دلار تخمین زده شده است[۱]. کلاهبرداری در ارتباط با متاورس از طرق مختلف می‌تواند صورت گیرد؛ به‌عبارت‌دیگر، فضای متاورس هم می‌تواند سبب فراهم کردن شرایط برای کلاهبرداری ساده شود که در این صورت شامل ماده ۱ قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری[۲] می‌شود و هم بستر را برای کلاهبرداری رایانه‌ای مهیا کند که ماده ۷۴۱ قانون مجازات اسلامی کتاب *تعزیرات*[۳] به آن پرداخته است. به‌طور کلی، فناوری متاورس می‌تواند زمینه را برای طرق مختلف کلاهبرداری مهیا کند که یکی از آن‌ها فیشینگ[۴] است. در این روش از طریق ایجاد سایت‌های جعلی برای به دست آوردن اطلاعات کاربری افراد و بردن دارایی‌های آن‌ها صورت می‌گیرد. به‌طوری‌که این سایت‌ها می‌توانند از پنل ورود به سیستم ارائه‌دهنده یک کیف پول قانونی یا یک متاورس تقلید نمایند و کاربران به‌جای استفاده از دامنه رسمی از پیوند و لینک ارتباطی فیشینگ استفاده کنند. در این صورت کاربران تصور می‌کنند که به کیف پول یا داده‌های خود دسترسی دارند، درحالی‌که دسترسی به اطلاعات یا داده‌های محرمانه و خصوصی خود را برای کلاهبرداران مهیا کرده‌اند که از این طریق کلاهبرداران داده‌ها یا منافع افراد در متاورس را به نفع خود یا دیگری تحصیل می‌کنند[۵]. در واقع فیشینگ نوعی رفتار متقلبانه محسوب شده و یکی از شیوه‌های ارتکاب جرم کلاهبرداری در فضای سایبر مانند متاورس است. همچنین کلاهبرداران می‌توانند گالری‌های متاورس جعلی برای نمایش و فروش آثار تقلبی ایجاد کنند[۶]. علاوه‌بر این موارد، شیوه‌های دیگری نیز برای کلاهبرداری در متاورس وجود دارد که یکی از شایع‌ترین آن‌ها، پروژه‌های یکپارچه‌سازی با فناوری بالا مانند، پشتیبانی از هوش مصنوعی و واقعیت مجازی است و هدف جذب سرمایه‌گذاران با سرمایه بالاست و هنگامی که سرمایه به حد مطلوب رسید، کلاهبرداران اموال سرمایه‌گذاران را به نفع خود تحصیل می‌کنند و می‌گریزند و هیچ سود یا خدماتی به سرمایه‌گذاران ارائه نمی‌کنند و پروژه را رها می‌کنند[۷]. به‌عبارت‌دیگر، در این روش توسعه‌دهندگان پروژه با وعده‌های فریبنده و دست‌کاری بازار باعث افزایش ناگهانی توکن پروژه می‌شوند، ولی

---

[1]. Crypto scammers took a record $14 billion in 2021(last visit 5/1/2024) available at: https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html/

[۲]. هرکس از راه حیله و تقلب مردم را به وجود شرکت‌ها یا تجارتخانه‌های یا کارخانه‌ها یا مؤسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیرواقع امیدوار نماید یا از حوادث و پیشامدهای غیرواقع بترساند و یا اسم و یا عنوان مجعول اختیار کند و به یکی از وسایل مذکور و یا وسایل تقلبی دیگر وجوه و یا اموال یا اسناد یا حوالجات یا قبوض یا مفاصاحساب و امثال آنها تحصیل کرده و از این راه مال دیگری را ببرد کلاهبردار محسوب و علاوه‌بر رد اصل مال به صاحبش، به حبس از یک تا ۷ سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می‌شود.

[۳]. هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، علاوه‌بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از صد و شصت و پنج میلیون (۱۶۵ /۰۰۰ /۰۰۰) ریال تا هشت صد و بیست و پنج میلیون (۸۲۵ /۰۰۰ /۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

[4]. Fishing

[5]. Zotter. A., "Financial crime in the metaverse is real – how can we fight back?, Wolf Theiss". 2022. available at: https://www.wolftheiss.com/insights/financial-crime-in-the-metaverse-is-real (last visited on 14/10/ 2024). P 2.

[۶]. ترکاشوند، عباس، رضا مالکی‌پور و حامد محمدی سپاسی، «اکوسیستم متاورس با محوریت جرائم مالی در آن»، *چهارمین کنفرانس ملی پدافند سایبری*، ۱۴۰۲، ص ۴.

[۷]. محمودی و صادقی، منبع پیشین، ص ۵۵.

بعد از اینکه خریداران سرمایه‌های خود را وارد بازار کردند، دارایی خریداران را به نفع خود تصاحب می‌کنند و می‌گریزند که در اصطلاح به این روش راگ‌پول[1] (قالی‌کشی) می‌گویند. یکی دیگر از راه‌های کلاهبرداری در متاورس در متاورس ایجاد و فروش NFT[2]های تقلبی است؛ به‌طوری‌که یک‌سری از اشخاص یک توکن غیرقابل تعویض فاقد ارزش ایجاد می‌کنند و یک‌سری معاملات پشت‌سر هم انجام می‌دهند و آن توکن را بین خودشان رد و بدل می‌کنند و برخی از شکارچیان تازه‌کار NFT ممکن است فکر کنند این کار، یک سرمایه‌گذاری ارزشمند است، پس از خرید آن با قیمت بالا، این سرمایه‌گذار متوجه می‌شود که هیچ‌کس نمی‌خواهد این NFT یا توکن را بخرد، زیرا همه خریداران قبلی در واقع همان فرد یا گروهی از افراد بوده‌اند که این NFT جعلی را تولید کرده‌اند. درواقع بسیاری از NFTها اصلاً حجم معاملاتی ندارند. به‌طوری‌که مجرمان می‌توانند NFTهای جعلی ایجاد کنند و آنها را در ازای مبالغ هنگفتی به فروش برسانند[3]. یا ممکن است کلاهبرداران در قبال سرمایه‌ای که دریافت می‌کنند داده یا شیء اشتباه و فاقد ارزش را در اختیار کاربران در دنیای متاورس قرار دهند. برای مثال ممکن است شخصی کفش مجازی باارزشی را سفارش دهد، ولی در قبال پرداخت هزینه آن کفش مجازی مورد نظر خود را دریافت نکند یا داده‌ای که قرار است پس از پردازش توسط ابزارهای مخصوص، مانند کفش، رؤیت شود خراب باشد. سرمایه و هزینه‌های پرداخت شده نیز بر دو قسم در حالت اول کاربران سرمایه‌ای را در دنیای مادی در اختیار کلاهبرداران قرار می‌دهند و در حالت دوم ممکن است داده‌ای دارای ارزش و یا رمز ارزی باشد که در دنیای مجازی متاورس در اختیار کلاهبرداران قرار می‌گیرد و در هر صورت اگر در قبال منفعت دریافت شده خدمت یا کالای مورد نظر دریافت نشود یا چیزی به غیر از آن‌ها دریافت شود. به‌عبارت‌دیگر، داده‌های کاذب و غلط به‌عنوان ورودی به این فناوری ارائه شود که محصول نهایی مدنظر نباشد، کلاهبرداری محقق می‌شود.

۳.۲. متاورس و سرقت

یکی دیگر از جرائم مالی مربوط به حوزه متاورس، سرقت است. واژه سرقت در لغت به‌معنای گرفتن و بردن شیء به‌طور پنهان است و در معنای آن مفهوم خفا و پنهان اخذ شده است. در تعریفی دیگر، سرقت عبارت است از «ربودن مال متعلق به دیگری با قصد محروم‌سازی دائمی صاحب مال از آن و محروم شدن مالک از مال خود است» و سرقت دارای شرایط خاص است که عبارت‌اند از: ۱. مخفیانه بودن ۲. ربودن ۳. منقول بودن و قابلیت جابه‌جایی داشتن ۴. تعلق به غیر داشتن[4]؛ به‌عبارت‌دیگر، با توجه به مفهوم فوق، ربایش با سرقت متفاوت است؛ چراکه ربایش می‌تواند در مرئی و منظر نیز صورت بگیرد. از همین رو در قانون مجازات اسلامی مصوب ۱۳۹۲ چندین ماده درخصوص ربایش وجود دارد و سرقت و ربایش از یکدیگر تمییز داده شده‌اند. مانند ماده ۶۵۷ کتاب *تعزیرات*[5] که از کیف‌قاپی به‌عنوان ربودن مال غیر یاد کرده است. خود سرقت نیز در سیاست جنایی ایران به دو بخش حدی و تعزیری تقسیم می‌شود و برای هریک متناسب با

---

[1]. Rug Pull

[2]. توکن‌های غیرقابل تعویض (NFT) نوعی توکن مبتنی بر بلاک‌چین هستند و با یک کالای غیرقابل تعویض مطابقت دارند. این اقلام باید منحصربه‌فرد باشند، مانند یک نقاشی، کالای کلکسیونی یا قطعه موسیقی. مالک کالا می‌تواند NFTهایی را براساس کالا ایجاد کند تا مالکیت خود را تضمین کند. سپس NFT به‌عنوان نوعی گواهی اصالت و مالکیت در دنیای مجازی عمل می‌کند.

[3]. Alessa. **What Is Cryptocurrency Wash Trading?** 2023. available at: https://alessa.com/blog/crypto-wash-trading/ (last visited on 08/10/ 2024).

[4]. اعتمادی، امیر، ***جرائم مالی***، جلد ۲، تهران: میزان، چاپ دوم، ۱۴۰۳، صص ۲۴-۴۹.

[5]. هرکس مرتکب ربودن مال دیگری از طریق کیف‌زنی – جیب‌بری و امثال آن شود به حبس از شش ماه تا دو سال و شش ماه و تا (۷۴) ضربه شلاق محکوم خواهد شد.

شرایط وقوع، ماده‌ای خاص و به‌تبع آن مجازات خاص وجود دارد. یکی از انواع سرقت‌ها که در سیاست جنایی و قانون مجازات به آن پرداخته شده است، سرقت رایانه‌ای است. در متاورس نیز با توجه به آنکه داده‌ها از منابع گوناگون به دست می‌آیند، احتمال وقوع سرقت نیز زیاد می‌شود. سرقت هویت، هک داده‌ها، نقض‌ها و سایر جرائم مالی همگی در متاورس ممکن است؛ زیرا هدف بیشتر آن‌ها سرقت اطلاعات شخصی و دسترسی به کیف پول دیجیتال افراد برای فعالیت‌های غیرقانونی است. سرقت داده‌ها و اطلاعات می‌تواند در هریک از مراحل جمع‌آوری، ذخیره‌سازی، پردازش داده‌ها به وقوع پیوندد. سرقت داده‌های مرتبط با رمز یکی از انواع سرقت در متاورس است که شامل هرگونه اقدام در راستای سرقت اطلاعات، سرقت کلید خصوصی اشخاص و در اختیار گرفتن رمز ارز اشخاص جهت خارج‌سازی دارایی‌های رمز ارز اشخاص از کیف پول ایشان و انتقال این دارایی‌ها به کیف پول دیگر می‌شود[1]. ازسوی‌دیگر، بسیاری از هکرها از آسیب‌پذیری‌های موجود در قراردادهای هوشمند برای سرقت دارایی‌های رمزنگاری شده سوءاستفاده می‌کنند. همچنین، تعداد زیادی قرارداد هوشمند در متاورس وجود دارد. بنابراین، مجرمان سایبری می‌توانند از قراردادهای هوشمند با ساختار ضعیف یا آسیب‌پذیری‌های موجود در قراردادهای هوشمند نیز برای سرقت ارزهای دیجیتال و NFTها در متاورس استفاده کنند و در همین رابطه در سپتامبر ۲۰۲۰، یکی از توسعه‌دهندگان Yearn Finance یک بازی NFT به نام Eminence Finance توسعه داد که توکن مخصوص به خود به نام EMN را دارد. برخی از سرمایه‌گذاران بدون درک زیاد از این پروژه، این توکن را کشف کردند و در عرض چند ساعت ۱۵ میلیون دلار EMN ضرب کردند. آنها از یک قرارداد هوشمند طراحی شده برای امکان تبادل DAI (یک کوین پایدار) با EMN برای تأمین مالی خریدهای درون بازی استفاده کردند. بااین‌حال، یک هکر راهی برای تخلیه وجوه موجود در قرارداد کشف کرد که باعث کاهش چشمگیر قیمت توکن شد[2]. از آنجایی که سرقت‌های یاد شده در متاورس که یک جهان و جامعه‌ای مجازی است به وقوع پیوسته است؛ شامل ماده ۷۴۰ قانون مجازات اسلامی کتاب *تعزیرات*[3] می‌شود. به‌طور خلاصه می‌توان گفت که فناوری متاورس با توجه به جدید بودن و برخی از ویژگی‌ها مانند غیر متمرکز بودن آن بستری مناسب برای ارتکاب برخی جرائم مالی مانند سرقت است.

۳.۳. متاورس و پول‌شویی

پول‌شویی فرایندی است که طی آن پول غیرقانونی یا کثیف که حاصل فعالیت‌های مجرمانه است، در چرخه‌ای از فعالیت‌ها و معاملات با گذر از مراحلی شسته و به پول قانونی و تمیز تبدیل می‌شود[4]. طبق ماده ۲ قانون مبارزه با پول‌شویی، پول‌شویی عبارت است از: الف) تحصیل، تملک، نگهداری یا استفاده از عواید حاصل از ارتکاب جرائم با علم به منشأ مجرمانه آن. ب) تبدیل، مبادله یا انتقال عوایدی به‌منظور پنهان یا کتمان کردن منشأ مجرمانه آن با علم به اینکه به‌طور مستقیم یا غیرمستقیم از ارتکاب جرم به دست آمده یا کمک به مرتکب جرم منشأ به‌نحوی‌که وی مشمول آثار و تبعات

---

[1]. ترکاشوند، مالکی پور و محمدی سپاسی، منبع پیشین، ص ۷.

[2]. J. Wu, K. Lin, D. Lin, Z. Zheng, H. Huang and Z. Zheng, "Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities", *in IEEE Open Journal of the Computer Society*, volume 4, 2023, pp 37-49.

[3]. هرکس به‌طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از بیست میلیون (۲۰۰۰۰۰۰) ریال تا صد و شصت و پنج میلیون (۱۶۵۰۰۰۰۰۰) ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از شصت و شش میلیون (۶۶۰۰۰۰۰۰) ریال تا دویست و شصت و چهار میلیون (۲۶۴۰۰۰۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

[4]. احمدی جویباری، مهدی، «جرم پول‌شویی و تبیین عوامل شیوع وگسترش آن در جوامع»، *مطالعات علوم سیاسی، حقوق و فقه*، شماره ۲، ۱۳۹۵، ص ۵۸.

قانونی ارتکاب آن جرم نشود. پ) پنهان یا کتمان کردن منشأ، منبع، محل، نقل و انتقال، جابه‌جایی یا مالکیت عوایدی که به‌طور مستقیم یا غیرمستقیم در نتیجه جرم تحصیل شده باشد.

این عمل از طرق مختلف قابلیت انجام دارد؛ به‌طور مثال، طی آن یک معامله‌گر، اوراق بهادار را به‌منظور ارائه اطلاعات گمراه‌کننده به بازار، خرید و فروش می‌کند. در برخی شرایط، پول‌شویی توسط یک معامله‌گر و یک کارگزار که با یکدیگر تبانی می‌کنند، انجام می‌شود و در برخی مواقع توسط سرمایه‌گذارانی که هم به‌عنوان خریدار و هم فروشنده اوراق بهادار عمل می‌کنند، انجام می‌شود[1]. متاورس نیز به‌دلیل نقص و فقدان مقررات حول معاملات آن نظیر معاملات اِن‌اِف‌تی(NFT) سبب گسترش تهدیداتی مانند افزایش پول‌شویی می‌شود. متاورس در کنار همه فرصت‌های اقتصادی که ارائه می‌دهد، به‌دلیل استفاده از تکنیک‌های پیچیده‌ای که در انجام معاملات در اختیار کاربران خود قرار می‌دهد، سبب شده است تا مبدأ معاملات پوشیده بماند. ازاین‌رو، مجرمین به‌خصوص پول‌شویان را برای استفاده از این فناوری تحریک و ترغیب می‌کند[2]. از دیدگاه مجرمین پول‌شویی، فناوری متاورس، بستری با ظرفیت‌های مناسب برای پنهان کردن منشأ غیرقانونی تراکنش‌ها و درآمدهای غیرقانونی آن‌هاست. زیرا اولین علتی که سبب انجام پول‌شویی در متاورس می‌شود، ماهیت غیرمتمرکز صنعت بلاک‌چین و ناشناس بودن برخی پلتفرم‌هاست که سبب می‌شود تا شناسایی کاربران سیاه شرکت‌کننده در تجارت شست‌وشو با دشواری روبه‌رو شود[3]. افزون‌بر آن، علت دیگر برای پول‌شویی از طریق متاورس، ناشناس بودن شخصی است که معاملات را انجام می‌دهد، زیرا هیچ قانونی وجود ندارد که کاربران را ملزم احراز هویت کند[4]. درحالی‌که انجام پول‌شویی از طریق انتقال وجوه بین حساب‌های بانکی ریسک شناسایی را به همراه دارد و در هر صورت‌حساب را می‌توان به شخص خاصی مرتبط کرد که خود پول‌شویی را انجام داده است یا از طریق آن حساب پول‌شویی را انجام داده است. مورد دیگری که سبب می‌شود تا فناوری متاورس برای انجام پول‌شویی مناسب باشد این است که از طریق متاورس می‌توان معاملات با ارزش‌ها و مبالغ بالا و هنگفت را انجام داد، بدون اینکه شخص یا نهاد خاصی مشکوک شود[5]. به‌عبارت‌دیگر متاورس را می‌توان به‌عنوان کانالی برای شستن وجوه غیرقانونی، خواه از جرائم دنیای واقعی یا اینکه مبتنی‌بر رمزنگاری باشد، در نظر گرفت. با کمک این فناوری، وجوه را می‌توان با دارایی‌های مبتنی‌بر متاورس مانند زمین،NFT یا دارایی‌های رمزنگاری مرتبط با متاورس رد و بدل کرد و سرمایه‌های غیرقانونی را از این طریق، تطهیر کرد. به‌طور مثال، تاجران مواد مخدر می‌توانند درآمد حاصل از فروش مواد مخدر را که معمولاً نیز مبالغ هنگفتی‌اند، به NFTتبدیل کنند، بدون اینکه شناسایی شوند یا کسی به حجم معاملات آن‌ها مشکوک شود. البته پول‌شویی محدود به این موارد نمی‌شود و متاورس به طرق دیگر سبب گسترش پول‌شویی می‌شود.

---

1. Chen, James, “Wash Trading: What It Is and How It Works, With Examples”, 2022. https://www.investopedia.com/terms/w/washtrading.asp#citation-8/

2. Money Laundering Threats To Metaverse (last visit 2024/1/16) available at: https://financialcrimeacademy.org/money-laundering-threats-to-metaverse/

3. Alessa. Op. Cit.

4. 31. Kelly C, Lynes A., **The Democratization of White-Collar Criminality in Video Games.** In: Kelly C, Lynes A (eds), *Video Games Crime and Next-Gen Deviance.* Emerald, 2020, P 114. https://www.researchgate.net/publication/342130412_The_Democratisation_of_White-collar_Criminality_in_Video_Games/

5. Mooij, A., *Regulating the Metaverse Economy, How to Prevent Money Laundering and the Financing of Terrorism*, Springer Nature Switzerland, 2024, P 27.

۳.۴. متاورس و تأمین مالی تروریسم

با گسترش تکنولوژی، علاوه‌بر اینکه می‌توان از محصولات آن در راه تسهیل زندگی و پیشرفت تمدن استفاده کرد، می‌شود در راه سیاه نیز از آن استفاده کرد و امروزه فناوری متاورس در خدمت تروریسم نیز قرار گرفته است و برای رسیدن به اهداف خود از آن استفاده می‌کند. فناوری متاورس از دو جهت برای تروریسم سودآوری دارد: در وهله اول موجب کاهش هزینه‌های آن می‌شود؛ برای مثال این فناوری موجب تسهیل در امر آموزش افراد در خدمت تروریسم می‌شود. در واقع تروریست‌ها از پلتفرم‌های آنلاین مختلف برای آموزش مهاجمان استفاده می‌کنند. آن‌ها از طریق متاورس و واقعیت افزوده و یا واقعیت مجازی می‌توانند نحوه ساخت سلاح‌های شیمیایی، انواع بمب‌ها و یا نحوه حملات به تأسیسات زیرساختی و نحوه انجام حملات سایبری را آموزش دهند، بدون اینکه همه آن‌ها در مکان مشخصی حضور داشته باشند و خطری آن‌ها را تهدید کند و یا برای آموزش افراد و تهیه وسایل و مهمات هزینه زیادی صرف کنند[1]. در گام بعدی متاورس شرایط را برای جذب و تأمین سرمایه برای گروه‌های تروریستی مهیا می‌سازد؛ وجود ارزهای رمزنگاری‌شده چشم‌اندازهای وسیع‌تری را برای تأمین مالی ناشناس در اختیار تروریست‌ها قرار داده است؛ چراکه در این صورت فهرست‌های سیاه مالی و معمولاً، گام‌هایی که در حال حاضر برای مقابله با تأمین مالی تروریسم استفاده می‌شود اثربخشی اندکی خواهند داشت[2]. در واقع منشأ سرمایه‌های تأمین‌شده برای فعالیت‌های تروریستی ناشناس می‌ماند و مقابله با این پدیده تروریسم را دشوار می‌سازد و کسانی قصد تأمین مالی گروه‌های تروریستی را داشته باشند با خیال آسوده اقدام به انجام این کار می‌کنند. احتمالاً از افراد خواسته می‌شود که یک کیف پول ارز دیجیتال برای دسترسی به متاورس و حفظ سرمایه‌گذاری دیجیتال خود داشته باشند، که باعث افزایش استفاده از آنها می‌شود. نگرانی‌های فزاینده ای در مورد استفاده از ارزهای رمزنگاری‌شده در تأمین مالی تروریسم به‌دلیل ناشناس بودن، امکان پرداخت فوری و قابلیت انجام نقل و انتقالات برون‌مرزی بدون نظارت هیچ مقام دولتی یا بانک وجود دارد. به‌عنوان مثال، دارایی‌های رمزنگاری‌شده را می‌توان برای پول‌شویی یا جمع‌آوری سرمایه استفاده کرد. ردیابی معاملات و تراکنش‌ها در متاورس به‌دلیل پیوند قوی آن با ارزهای دیجیتال بسیار دشوارتر خواهد بود. می‌توان تصور کرد که با استفاده از مصنوعات هویتی، مانند صلیب شکسته یا نمادهای تروریستی، به‌عنوان NFT پول به دست می‌آید که سپس برای شخصی‌سازی آواتارها و نشان دادن وابستگی فرد به سازمان‌های تروریستی استفاده می‌شود. گروه‌های تروریستی می‌توانند ذخایر مالی خود را تقویت کنند و جوامع خود را از طریق نمایش‌های آنلاین یا مسابقات آواتار، که در حال حاضر برای افزایش بودجه سازمان‌دهی می‌شوند، تقویت کنند. این گونه تأمین مالی غیرمتمرکز می‌تواند به سازمان‌های تروریستی در ایجاد اکوسیستم‌های آنلاین و مدیریت متارون‌های خود کمک کند؛ نگرانی‌ای که در گزارش شورای اتحادیه اروپا ذکر شده است[3].

نتیجه‌گیری

پیشرفت‌های چشمگیر در حوزه فناوری اطلاعات و ارتباطات، سبب ظهور فناوری‌های جدید شده است که یکی از این فناوری‌ها متاورس است. این فناوری روبه‌رشد، توانایی تجمیع و تحلیل حجم عظیمی از اطلاعات را داراست و بر حوزه‌های

[1]. Weimann & Dimant, op. cit. pp 97-100.

[2]. Debuire, D., **TERRORIST Use of the Metaverse: New Opportunities And New Challenges**, Security Distillery. 2022, available at: https://thesecuritydistillery.org/all-articles/terrorism-and-the-metaverse-new-opportunities-and-new-challenges (last visited on: 19/8/2024).

[3]. Council of the European Union, "The Metaverse in the Context of the Fight Against Tterrorism", 2022. https://data.consilium.europa.eu/doc/document/ST-9292-2022-INIT/en/pdf.

مختلف مانند اقتصاد، سیاست و روابط اجتماعی تأثیر داشته است و حتی سبب شده تا برخی از شرکت‌های بزرگ به سرمایه‌گذاری در این عرصه روی آورند. این فناوری با توجه به مزایایی که دارد به‌سرعت درحال‌گسترش و همه‌گیر شدن است Y اما از آنجایی که هنوز درحال‌تکمیل شدن است و نواقصی دارد و با چالش‌هایی مانند نبود مقررات کافی، نقص در نظارت، ناتوانی سیستم‌های امنیتی در تشخیص و پیشگیری از جرائم، حریم خصوصی، امنیت فنی و امکان تقلب روبه‌رو است و زمینه را برای ارتکاب جرائم فراهم می‌کند و به‌دلیل ارائه فرصت‌های بی‌سابقه در حوزه فعالیت‌های مالی یک دسته از جرائمی‌که که متاورس بستر مناسب برای ارتکاب آن را فراهم می‌کند، جرائم مالی‌اند و فناوری متاورس، به‌عنوان یک پدیده نوظهور، ممکن است تأثیر بسزایی در افزایش ارتکاب جرائم مالی داشته باشد. مطالعه و بررسی‌های انجام شده در این رابطه نشان داده است که استفاده از فناوری متاورس که یک فناوری نوپدید درحال‌توسعه است و خود نیز از فناوری‌های دیگری نظیر واقعیت مجازی، بلاک‌چین و سایر فناوری‌ها بهره می‌برد، می‌تواند شرایطی را فراهم کند که سبب افزایش ارتکاب جرائم مالی نظیر کلاهبرداری، سرقت، پول‌شویی یا حتی تأمین مالی تروریسم شود؛ چراکه به‌دلیل داشتن برخی از ویژگی‌ها مانند اینکه افراد هر چیز را در آن به‌صورت غیرمتمرکز کنترل می‌کنند، بدون اینکه مدیریت آن‌ها در دست نهاد دولتی خاصی باشد و نبود قانون خاصی که کاربران را ملزم به احراز هویت کند که همین امر سبب ناشناس بودن کاربران می‌شود و همچنین نبود ناظر در این بستر که بر رفتار کاربران و انجام معاملات آن‌ها نظارت داشته باشد، سبب شده تا جرائمی مانند سرقت، پول‌شویی و تأمین مالی تروریسم در فضای متاورس به‌راحتی انجام شود. افزون‌بر آن، ناآگاهی برخی کاربران سبب می‌شود تا هدف مناسبی برای کلاهبرداری باشند. به‌طور خلاصه، فناوری متاورس شرایطی را فراهم می‌کند تا کاربران خود مرتکب این دسته از جرائم باشند. یا اینکه به‌دلیل چالش‌هایی که با آن مواجه است، سبب می‌شود کاربران بزه‌دیدگان جرائم مالی باشند. این نتیجه نشان می‌دهد که دید جامع و گسترده‌ای نسبت به تأثیرات اجتماعی و اقتصادی فناروی متاورس مورد نیاز است. از طرف دیگر به‌منظور پیشگیری و کاهش جرائم مالی در این بستر سایبری می‌توان اقداماتی لازم نظیر ایجاد یک پلیس تخصصی یا ایجاد یک واحد مجزا در پلیس فتا به‌منظور حضور مخفیانه در پلتفرم‌های معروف و فراگیر متاورس برای نظارت بر متاورس و همچنین نظارت بر تراکنش‌ها و تحلیل رفتار مشکوک در آن را نام برد؛ به‌عنوان مثال، ایجاد واحد مجزا در پلیس فتا نقش مؤثری در نظارت بر انجام معاملات هنگفت و تراکنش‌های بالا دارد؛ همچنین ایجاد یک سامانه منسجم به‌منظور احراز هویت کاربران و افراد دارای فعالیت در بستر متاورس با هدف ایجاد علم برای کاربران در رابطه با توانایی شناسایی آن‌ها درصورت ارتکاب جرم یا آموزش به کاربران برای افزایش اگاهی درمورد چالش‌ها و خطرات متاورس قبل از حضور در بستر متاورس و استفاده از کیف پول‌های دیجیتالی امن و معتبر به همراه رمزنگاری قوی توسط کاربران به‌منظور پیشگیری از سرقت و کلاهبرداری امری مؤثر است. افزون‌بر این موارد برای انجام معاملات مالی در متاورس، می‌توان از قراردادهای هوشمند با امنیت بالا بررسی شده توسط کارشناسان امنیتی استفاده کرد تا از وجود حفره‌های امنیتی جلوگیری شود.

منابع

فارسی

کتاب

۱. اعتمادی، امیر، ***جرائم مالی***، جلد ۲، تهران: میزان، چاپ دوم، ۱۴۰۳.

۲. جعفری لنگرودی، محمدجعفر، ***مبسوط در ترمینولوژی حقوق***، جلد ۴، تهران: گنج دانش، چاپ اول، ۱۳۷۸.

۳. حسنی، ابوالحسن، ***مالکیت در فضای مجازی از منظر فقهی***، تهران: مرکز ملی فضای مجازی، ۱۳۹۹.

عربی

٤. شیخ طوسی، ابوجعفر محمد بن حسن، ***المبسوط فی فقه الالمامیة شیخ طوسی***، جلد ۶، تهران: المکتبة المرتضویة، چاپ سوم، ۱۳۸۷.

٥. صدر، سیدمحمدباقر، ***اقتصادنا***، قم: مؤسسه بوستان‌کتاب، چاپ دوم، ۱۳۸۵.

٦. نجفی، محمدحسن، ***جواهر الکلام***، جلد ۲۲، بیروت: داراحیاء التراث العربی، چاپ هفتم، ۱۳۶۲.

مقاله

۷. احمدی جویباری، مهدی، «جرم پول‌شویی و تبیین عوامل شیوع و گسترش آن در جوامع»، *مطالعات علوم سیاسی، حقوق و فقه*، شماره ۲، ۱۳۹۵، صص ۶۸-۵۷.

۸. ترکاشوند، عباس، رضا مالکی‌پور و حامد محمدی سپاسی، «اکوسیستم متاورس با محوریت جرائم مالی در آن»، *چهارمین کنفرانس ملی پدافند سایبری*، ۱۴۰۲.

۹. حسین‌زاده سرشکی، اسماء و سیدعلیرضا فروغی، «بررسی فقهی و حقوقی مالیت و مالکیت داده‌های دیجیتال در فضای سایبری»، *دوفصلنامه فقه و حقوق خصوصی*، دوره ۲، شماره ۵، ۱۴۰۴، صص۵۳-۳۵.

۱۰. عاکفی قاضیانی، موسی، سیدمصطفی میلانی و وحید عاکفی قاضیانی، «متاورس و چالش‌های حقوقی در حوزه حقوق اموال»، *مجله حقوق فناوری‌های نوین*، دوره ۳، شماره ۶، ۱۴۰۱، صص ۱۵۳-۱۴۲.

۱۱. عبدی‌پور فرد، ابراهیم و مرتضی وصالی ناصح، «ابعاد فقهی و حقوقی بازی‌های مجازی»، *فصلنامه راهبرد اجتماعی فرهنگی*، دوره ۶، شماره ۲، ۱۳۹۶، صص ۷۴-۵۳.

۱۲. محبی، فاطمه، «تکنولوژی، "واقعیت افزوده" و کاربرد آن در آموزش زیست‌شناسی»، *پژوهش در آموزش زیست‌شناسی*، دوره ۱، شماره ۳، ۱۳۹۸، صص۸۴-۷۳.

۱۳. محمد باقری، زهرا و سیدمجتبی سیدباقری، «مد سریع در جهان مادی و متاورس»، *فصلنامه مطالعات حقوقی فضای مجازی*، دوره ۱، شماره ۴، ۱۴۰۱، صص۷۸-۶۴. Doi: 10.30495/cyberlaw.2023.699220

۱٤. محمودی، محسن و سالار صادقی، «متاورس و تأثیر آن بر سبک زندگی»، *فصلنامه مطالعات حقوقی فضای مجازی*، دوره ۱، شماره ۲، ۱۴۰۱، صص ۶۲-۴۴.

۱۵. مهپور، علیرضا و مهسا اکبری، «تأثیر استفاده از فناوری واقعیت مجازی بر قصد رفتاری مصرف‌کننده در صنعت مسکن»، *فصلنامه توسعه تکنولوژی صنعتی*، دوره ۱۹، شماره ۴۴، ۱۴۰۰، صص۲۲-۳. Doi: 20.1001.1.26765403.1400.19.44.1.4

References

Books

1. Etemadi, Amir, *Financial Crimes,* Volume 2, Tehran: Mizan, Second Edition, 2024. (In Persian)
2. Hassani, Abul Hasan, *Ownership in Cyberspace from a Jurisprudential Perspective,* Tehran: National Center for Cyberspace, 2010. (In Persian)
3. Jafari Langroodi, Mohammad Jafar, *Detailed in Legal Terminology*, Volume 4, Tehran: Ganj-e-Danesh, First Edition, 1999. (In Persian)
4. Mooij, A., *Regulating the Metaverse Economy, How to Prevent Money Laundering and the Financing of Terrorism,* Springer Nature Switzerland, 2024.
5. Najafi, Mohammad Hassan, *Jewel of speech*, Volume 22, Beirut: House for the Revival of Arab Heritage, Seventh Edition, 1983. (In Arabic)

6. Sadr, Sayyed Mohammad Bagher, *Our Economy*, Qom: Book Garden Institute, Second Edition, 2006. (In Arabic)
7. Sheikh Tousi, Abu Jafar Mohammad Ibn Hassan, *Detailed in Imamieh Jurisprudence by Sheikh Tousi*, Volume 6, Tehran: Mortazavi Library, Third Edition, 2008. (In Arabic)

Articles

8. Abdi-Pour-Fard, Ebrahim and Morteza Wesali Naseh, "Jurisprudential and Legal Aspects of Virtual Games", *Socio-Cultural Strategy Quarterly*, Volume 6, Issue 2, 2017, PP. 53-74. (In Persian)
9. Ahmadi Jouybari, Mehdi, "The Crime of Money Laundering and the Explanation of the Factors of Its Prevalence and Expansion in Societies", *Quarterly Journal of Political Science, Law and Jurisprudence Studies,* Issue 2, 2016, PP 57-68. (In Persian)
10. Akefi Ghaziani, Mousa, Sayyed Mostafa Milani and Vahid Akefi Ghaziani, "Metaverses and Legal Challenges in the Field of Property Law", *Journal of Law of New Technologies*, Volume 3, Issue 6, 2022, PP 142-153. (In Persian)
11. Bermejo Fernandez, Carlos and Hui, Pan, "Life, the Metaverse and Everything: An Overview of Privacy", *Ethics, and Governance in Metaverse*, 2022. https://doi.org/10.13140/RG.2.2.35094.63042
12. Chen, James, "Wash Trading: What It Is and How It Works, With Examples", 2022. https://www.investopedia.com/terms/w/washtrading.asp#citation-8.
13. Council of the European Union, "The Metaverse in the Context of the Fight Against Tterrorism", 2022. https://data.consilium.europa.eu/doc/document/ST-9292-2022-INIT/en/pdf.
14. Dionisio, J.D.N.; Burns, W.G., III; Gilbert, R., "3D Virtual Worlds and the Metaverse", *ACM Comput.Surv*, Volume 45, Issue 3, 2013, pp 1–38. https://doi.org/10.1145/2480741.2480751.
15. Donaldson, Tara. "Year in Review: What Exactly Is the Metaverse? The Simplest Explanation of What It Means for Fashion", 2021, pp 12- 22 https://wwd.com/business-news/business-features/what-is-metaverse-simple-explainer-meta-zuckerberg-digital-fashion-1235015619/
16. Hayes, Adam, "Blockchain Facts: What Is It, How It Works, and How It Can Be Used", 2023. https://www.investopedia.com/terms/b/blockchain.asp
17. Hossein Zadeh Sareshki, Asmaa and Sayyed Alireza Foroughi, "A jurisprudential and legal study of the property and ownership of digital data in cyberspace", *Bi-Quarterly Journal of Jurisprudence and Private Law,* Volume 2, Issue 5, 2025, PP 35-53. (In Persian)
18. Iansiti, Marco. Lakhani. K, R., "The Truth About Blockchain", *Harvard Business Review*, Volume 95, Issue 1, 2017, PP 118-127.
19. J. Wu, K. Lin, D. Lin, Z. Zheng, H. Huang and Z. Zheng, "Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities", *IEEE Open Journal of the Computer Society*, Volume 4, 2023, pp 37-49, DOI: 10.1109/OJCS.2023.3245801/
20. Mahmoudi, Mohsen and Salar Sadeghi, "Metaverse and its Impact on Lifestyle", *Legal Studies in Cyberspace Quarterly*, Volume 1, Issue 4, 2022, PP 44-62. (In Persian)
21. Mahpour, Alireza and Mahsa Akbari, "The effect of using virtual reality technology on consumer behavioral intention in the housing industry", *Quarterly Journal of Industrial Technology Development*, Volume 19, Issue 44, 2021, PP 3-22. (In Persian) Doi: 20.1001.1.26765403.1400.19.44.1.4
22. Mohammad Bagheri, Zahra and Sayyed Mojtaba Sayyed Bagheri, "Fast Fashion in the Material World and the Metaverse", *Legal Studies in Cyberspace Quarterly*, Volume 1, Issue 4, 2022 , PP 64-78. (In Persian) Doi: 10.30495/cyberlaw.2023.699220
23. Mohebbi, Fatemeh, "Technology, "Augmented Reality" and its Application in Biology Education", *Research in Biology Education Quarterly,* Volume 1, Issue 3, 2019, PP 73-84. (In Persian)

Other '*Real'". Information Systems Journal*, Volume. 29, Issue 3, 2019, pp 707–737. https://doi.org/10.1111/isj.12230/
25. Torkashvand, Abbas, Reza Maleki-Pour and Hamed Mohammadi Sepasi, "Metaverse Ecosystem with a Focus on Financial Crimes in It", *Fourth National Conference on Cyber Defense*, 2023. (In Persian)
26. Vidal-Balea, A.; Blanco-Novoa, Ó.; Fraga-Lamas, P.; Fernández-Caramés, T.M.; "Developing the Next Generation of Augmented Reality Games for Pediatric Healthcare: An Open-Source Collaborative Framework Based on ARCore for Implementing Teaching, Training and Monitoring Applications", *Sensors*, Volume 21, Issue 5, 2021, Doi: 10.3390/s21051865
27. Weimann, Gabriel. Dimant, Roy. "The Metaverse and Terrorism: Threats and Challenges", *Perspective on Terrorism. Issue XVII*, Volume 17, Issue 2, 2023, pp 92-107.

Internet Resources

28. Alessa. **What Is Cryptocurrency Wash Trading?**, 2023. Available at: https://alessa.com/blog/crypto-wash-trading/ (last visited on 08/10/ 2024).
29. Debuire, D., **Terrorist Use of the Metaverse: New Opportunities And New Challenges**. Security Distillery, 2022. available at: https://thesecuritydistillery.org/all-articles/terrorism-and-the-metaverse-new-opportunities-and-new-challenges (last visited on: 19/8/2024).
30. Intelligence, Bloomberg, **Metaverse May be $800 Billion Market, Next Tech Platform**. 12 01, 2021. https://www.bloomberg.com/professional/blog/metaverse-may-be-800-billion-market-next-tech-platform/.
31. Kelly C, Lynes A., **The Democratization of White-Collar Criminality in Video Games.** In: Kelly C, Lynes A (eds), *Video Games Crime and Next-Gen Deviance.* Emerald, 2020. https://www.researchgate.net/publication/342130412_The_Democratisation_of_White-collar_Criminality_in_Video_Games/ Doi: 10.1108/978-1-83867-447-220201007
32. **Money Laundering Threats To Metaverse,** 2021. https://financialcrimeacademy.org/money-laundering-threats-to-metaverse/
33. Neuburger Jeffrey D., Proskauer Rose LLP, **In the Coming 'Metaverse', There May Be Excitement but There Certainly Will Be Legal Issues**, *National Law Review*, Friday, December 3, 2021. https://newmedialaw.proskauer.com/2021/12/03/in-the-coming-metaverse-there-may-be-excitement-but-there-certainly-will-be-legal-issues/ (last visited on: 20/8/2024).
34. Zotter. A., **Financial Crime in the Metaverse is Real –How Can We Fight Back?.** Wolf Theiss, 2022. available at: https://www.wolftheiss.com/insights/financial-crime-in-the-metaverse-is-real/ (last visited on 14/10/ 2024)