
Money Laundering in the Crypto Ecosystem: Implications for Organized Crime

Darko M. Marković

University Business Academy, Novi Sad, Serbia
Faculty of Law for Commerce and Judiciary

Article Information*

Review Article • UDC: 336.741.1[336.7:004]

Volume: 23, Issue: 2, pages: 75–85

Received: May 7, 2026 • Accepted: June 10, 2026

<https://doi.org/10.51738/kpolisa.2026.2r.dm>

Author Note

Darko M. Marković  <https://orcid.org/0000-0001-9124-6417>

I have no known conflict of interest to disclose.

Corresponding Author: Darko M. Marković

E-mail: darko.markovic@pravni-fakultet.info

* Cite (APA): Marković, D. M. (2026). Money Laundering in the Crypto Ecosystem: Implications for Organized Crime. *Kultura polisa*, 23(2), 75–85, <https://doi.org/10.51738/kpolisa.2026.2r.dm>



© 2025 by the authors. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Money Laundering in the Crypto Ecosystem: Implications for Organized Crime

Abstract

The paper deals with the transformation of money laundering in the conditions of digitization of financial flows, with special reference to the role of cryptocurrencies in the strategies of organized crime. Starting from the classic three-phase model of placement, layering and integration, the ways in which the digital ecosystem changes operational patterns, available instruments and possibilities to conceal the origin of funds are analyzed. Cryptocurrencies introduce specific dynamics—speed, global reach, and pseudonymity – that affect the risk perception of perpetrators and make institutional oversight more difficult, thus opening up space for new typologies of financial crime. The aim of the paper is to show how traditional models of money laundering adapt to the crypto-environment and what criminological implications arise from such changes. Special emphasis is placed on understanding the relationship between technological innovation and institutional capacity, as well as how the digital space affects the strategies of organized crime in terms of covering tracks, moving funds and infiltrating legal flows. Methodologically, the work is based on descriptive, analytical and comparative processing of relevant domestic and international sources, including regulatory documents, reports of law enforcement institutions and available data on cases in which cryptocurrencies were used for criminal purposes. This sets the framework for understanding contemporary challenges in the fight against money laundering in the digital environment.

Keywords: transnational criminal, financial security, financial criminal, decentralized transactions, blockchain infrastructure

Introduction

Money laundering represents one of the key survival mechanisms of organized crime, as it allows illegally acquired profits to be included in legal flows and used without immediate risk of detection. The traditional three-phase model of placement, stratification and integration has long represented the basic framework for understanding this process, but modern financial flows show that its applicability is changing in accordance with technological developments. The emergence of cryptocurrencies and decentralized digital services has opened up space for new modalities of concealing the origin of funds, new actors and new operational patterns, which requires a reconsideration of existing theoretical and institutional approaches.

The digital ecosystem introduces a dynamic that differs from traditional financial structures: transactions take place quickly, globally and often beyond regulatory oversight, while pseudonymity and the technical capabilities of blockchain networks create additional challenges for law enforcement. In such an environment, the question arises to what extent classic models of money laundering remain adequate and how they are transformed when applied to digital flows that function according to a different logic than institutionally mediated financial systems.

The aim of this paper is to analyze how the classical stages of money laundering manifest themselves in the crypto environment and how digital technologies influence the strategies of organized crime. The paper focuses on the criminological implications, that is, on how the digital space changes the perception of risk, the patterns of concealing traces and the operational capabilities of criminal groups.

Methodologically, the work is based on descriptive and analytical processing of relevant domestic and international sources, with a comparative analysis of traditional and modern typologies of money laundering. This approach makes it possible to see the phenomenon in the broader context of digitalization of financial flows and to set a framework for understanding modern challenges in the fight against money laundering.

Classic Stages of Money Laundering and Organized Crime

Three-Phase Model of Money Laundering

In the classical literature on money laundering, the process is most often depicted through a three-phase model that includes placement, stratification and integration. Although the model is simplified, its structure remains useful because it clearly separates three functionally distinct steps in which ill-gotten gains are transformed into ostensibly legitimate assets. The national regulatory framework in Serbia recognizes this model almost identically: placement as severing the direct link between money and criminal activity, stratification as a series of transactions that cover the trail, and integration as the moment when “dirty” money appears as income from a permitted activity (Organizacija za evropsku bezbednost i saradnju, Misija u Srbiji [OEBS], 2011).

Placement represents an entry point - the moment when money obtained from crime is introduced into the financial system. In a traditional environment, it is the stage where cash is deposited into accounts, shredded, or used through fictitious business activities to avoid the attention of the relevant authorities. This stage is the most risky for the perpetrators because the connection between the money and the criminal activity is still relatively visible.

Layering is the stage where the money trail is deliberately complicated. According to official documents, this is when funds are transferred from one account to another, often across multiple jurisdictions, in order to sever any identifiable link to the source (OEBS, 2011). This is the stage where criminal groups use complex financial instruments, intermediaries and transaction patterns that make it difficult to reconstruct the flow of money.

Integration is the final step – the moment when funds return to legal flows. In this phase, money appears as income from legitimate activities, most often through investments, real estate purchases, business ventures or other forms of economic activity that do not arouse suspicion (OEBS, 2011). What was concealment in the previous stages becomes normalization in integration: money is no longer distinguished from legal capital.

Organized Crime and the Need for Legalization of Profits

Organized crime cannot survive without the ability to turn illegal profits into usable, legitimate assets, which is confirmed by contemporary analyzes of the globalization of criminal networks and their economic power (Marković & Spaić, 2021). It is not only a financial issue, but a question of the survival of

the criminal organization as a structure. Criminal groups function as parallel economic systems: they generate income, invest, expand, maintain networks of associates and corrupt connections. All this requires money that can be used without the risk of detection.

That is why *the legalization of profits* is a central element of the strategy of organized crime. The national strategy clearly states that perpetrators of criminal acts seek ways to use illegally acquired assets “so as not to attract the attention of the competent authorities”, which means that money laundering is not a secondary activity, but an integral part of the criminal business model (OEBS, 2011).

Organized crime uses money laundering for three key reasons:

4. *Preservation of profits* – without legalization, money is only evidence against perpetrators.
5. *Financing of further activities* – criminal networks expand only if they have a stable source of “clean” funds.
6. *Infiltration of the legal economy* – the purchase of businesses, real estate and other resources allows criminal groups to influence markets, politics and local communities.

This is precisely why the fight against money laundering is seen as a fight against organized crime at its economic core. Without the ability to legalize profits, criminal groups lose their capacity to survive, expand and corrupt institutions.

Cryptocurrencies as a New Financial Ecosystem

Criminal Adaptation and the Logic of Digital Space

Cryptocurrencies are not just a technological innovation; they have become a new operating space in which criminal activities take place with a different logic than in traditional finance (Bjelajac & Bajac, 2022). In its Spotlight report from 2022, Europol emphasizes that the criminal use of cryptocurrencies can no longer be seen as an isolated phenomenon, but as an integral part of almost all forms of serious and organized crime. It is this integration into the wider criminal ecosystem that makes cryptocurrencies relevant not only as a means of payment, but as an infrastructure that enables new patterns of behavior.

For criminal groups, cryptocurrencies represent a space where the boundaries between physical and digital crime are blurred. Drug trafficking, fraud, extortion, human trafficking, and even classic money laundering schemes – everything gets a digital component. Europol notes that traditional and virtual typologies of money laundering are increasingly intertwined, creating hybrid models in which physical crime is financed by digital means, and digital crime is “cleaned” through physical flows. This creates an ecosystem that not only parallels the traditional one, but actively complements and undermines it (Marković & Spaić, 2021).

The Attractiveness of the Crypto Ecosystem for Criminal Networks

From a criminological point of view, the attractiveness of cryptocurrencies to organized crime does not stem from their technical complexity, but from a combination of three factors: speed, globality and fragmented surveillance (Bjelajac & Bajac, 2022). Transactions take place in real time, without geographical restrictions and without intermediaries who would have to apply standard AML procedures. In its recommendations from 2022, Europol points out that criminal groups use precisely these characteristics in order to “stay one step ahead” of institutions that are still adapting to the new environment.

What makes cryptocurrencies particularly suitable for criminal activities is the fact that they bring together elements that were previously separated: the speed of informal flows, the global reach of financial markets and the anonymity of cash. In such a space, criminal networks can function as transnational actors without the need for physical presence, intermediaries or local logistics structures (Dragojlović, 2023; Marković & Spaić, 2021). It changes the very nature of criminal activity: it becomes decentralized, flexible and technologically mediated.

Cryptocurrencies as an Instrument and as an Ecosystem

In the crypto-ecosystem, however, money ceases to be merely an instrument and becomes a space of action – an infrastructure within which criminal activities take place without physical constraints and without intermediaries to slow them down or make them visible. Criminal groups don't just use cryptocurrencies to make a transaction, but to create conditions where clues are lost faster than institutions can react. Europol notes that crypto-assets appear in an increasing number of investigations, not because they are a “substitute” for cash, but because they allow financial flows to take place in a space that is simultaneously global, fragmented and operationally easier to manipulate (Europol, 2022).

In such a ecosystem, cryptocurrencies become part of a wider criminal infrastructure: they are used to store value, to move funds between different networks, to disguise origins and to enter legal flows through activities that appear legitimate on the surface. It is not just a technical innovation, but a change in the way criminal networks organize their finances – a shift from a model in which money is “cleaned” to a model in which money moves through digital space, which in itself makes it difficult to monitor and reconstruct the flow (Matijašević et al., 2024).

Normalization of Digital Criminal Space

As cryptocurrencies enter the mainstream, so does the risk perception of the perpetrators (Filipović & Bjelajac, 2025). Europol states that criminal groups increasingly rely on crypto-assets because they perceive them as a “normalized” part of the financial system, and not as an exception reserved for technically sophisticated actors (Europol, 2022). This normalization has profound criminological consequences: it reduces the subjective sense of danger, increases the willingness to experiment and widens the range of criminal activities that are transferred to the digital space.

In this sense, cryptocurrencies are not just a new financial ecosystem – they are a new *criminal ecosystem*, in which rules, risks and behavior patterns are shaped by a different logic from that of traditional finance. Understanding that logic becomes necessary for the analysis of modern organized crime, because crime no longer takes place only in the physical world, but also in the digital space that functions according to its own rules.

Transformation of the Three-Phase Model in the Crypto World

Placement in the Digital Environment

In the traditional model of money laundering, the placement (insertion) phase represents the moment when “dirty” money is first introduced into the financial system. In a digital environment, that moment loses its physical manifestation. Cash no longer must go over the counter, or be exchanged in

cafes, exchange offices or through intermediaries. It is almost imperceptibly transformed into a digital record – a cryptocurrency that knows no borders, working hours or territorial jurisdiction. This is precisely why the FATF (*Financial Action Task Force*) warn that peer to peer transactions, OTC desks and crypto ATMs represent high-risk entry points, as they enable the conversion of cash into virtual assets without adequate user identification (Bjelajac & Bajac, 2022; FATF, 2021).

Criminal groups use these mechanisms precisely because of their ability to “cut off” the trace of origin. Europol notes that P2P platforms and unregulated services have become the dominant channel for the initial injection of funds into the crypto ecosystem, especially in cases of organized crime that operates transnationally (Europol, 2022). In practice, this means that money can be converted into cryptocurrencies without a formal identity, often with minimal or no verification. Thus, the placement becomes not only faster, but also psychologically less risky for the perpetrators – entering the system becomes almost invisible.

Layering Through DeFi, NFT and Cross Chain Mechanisms

If placement is the moment of entry, layering is the moment of disappearance. In the traditional model, it is the stage where the money trail is decomposed into a series of transactions, accounts and jurisdictions. In the crypto world, this process takes on a new dimension – the dimension of technological complexity. The FATF identifies mixers, tumblers, privacy enhancing technologies and cross chain bridges as key tools for disguising the origin of funds, as they allow breaking traces into hundreds of pieces and transferring them through different blockchain networks (FATF, 2021).

Decentralized financial protocols (DeFi), envisioned as open systems, become automated provenance concealment mechanisms, as smart contracts do not ask for a purpose, but only execute an instruction. Europol notes that criminal groups are increasingly using DeFi protocols for “chain hopping”, moving from one network to another, thus fragmenting the transaction trail to the point where traditional forensic methods lose effectiveness (Europol, 2022; Matijašević et al., 2024).

The NFT market, although often trivialized as a digital art space, is becoming a new field for layering. In 2022, Elliptic Enterprises documented cases of laundering of stolen NFTs and the use of Tornado Cash to cover up traces, while FIU Latvia and academic authors pointed out the occurrences of wash trading and self-laundering through NFT platforms (Elliptic Enterprises, 2022; FIU Latvia, 2022; Kafteranis & Turksen, 2022). At this stage, cryptocurrencies not only obscure the trail, but turn it into a web that cannot be followed by linear methods (FIU Latvia, 2022).

Integration in the Crypto Ecosystem

In the final stage, the money is returned to legal flows. In the digital environment, integration takes place through unregulated exchanges, offshore companies, stablecoin trading, and investments in legitimate businesses. The FATF states that these unregulated VASPs, particularly those operating from jurisdictions with weak AML regimes, represent a key point for the integration of assets, as they enable the conversion of cryptocurrencies into fiat without adequate oversight (Bjelajac & Bajac, 2022; FATF, 2021).

Europol confirms that criminal groups use stablecoins as a “safe zone” to temporarily store funds before their return to legal flows, while UNODC (2020) points to the growing use of cryptocurrencies in investment schemes that serve as a cover for integration. But, integration in the crypto world is not just a

return to legal flows – it is a return to a world where the line between legal and illegal is increasingly difficult to recognize, as digital assets move through layers that are both transparent and opaque.

Criminological Implications

Difficulties in Discovery and Proof

Cryptocurrencies have introduced a new kind of criminal dynamic, one in which the classic concept of chasing money turns into a pursuit of patterns that are no longer linear, but networked, fragmented and time compressed. Europol indicates that criminal groups today use technological capabilities that exceed the capacities of most national institutions, especially when it comes to decentralized services, unregulated exchanges and peer-to-peer networks that function outside of institutional supervision (Europol, 2022). In such an environment, the transaction trail becomes paradoxical: everything is visible, but nothing is simply understandable.

From a criminological point of view, the biggest challenge is not the technology itself, but *the loss of continuity of traces*. In traditional financial investigations, the money trail moved through institutions that had an obligation to keep data, identify beneficiaries and cooperate with law enforcement. In the crypto ecosystem, that continuity breaks down. Transactions take place through services that do not collect data, through networks that know no borders and through protocols that do not distinguish between legitimate and criminal use. This violates the basic principle of financial forensics – the ability to reconstruct the flow of funds.

Pseudonymity further complicates the situation. Although at first glance it seems that the public nature of the blockchain makes the work of investigators easier, in practice the opposite happens: visibility does not mean comprehensibility. Addresses exist, but they say nothing about the people behind them; flows are recorded, but one cannot know who initiated them, or for what reason. Europol notes that criminal groups increasingly use switching from one network to another, combining multiple services and short sequences of transactions that take place faster than institutions can react (Europol, 2022). When such traces are scattered across different technical and legal frameworks, the investigation no longer resembles following the money, but rather an attempt to reconstruct an event that has been deliberately broken into parts that do not belong to the same time, space or system (Dragojlović, 2023; FIU Latvia, 2022).

This problem also has its own institutional dimension. Law enforcement agencies often do not have access to specialized blockchain analytics tools, nor do they have a sufficient number of experts who understand the technical details of decentralized systems (Matijašević et al., 2024; Zirojević & Marković, 2020). This creates operational blindness – a situation where institutions see something happening, but cannot understand what exactly, nor how to intervene. In such an environment, proving becomes a process that requires an interdisciplinary approach: criminology, digital forensics, international law, economic analysis and technical expertise. It is a shift from a “follow the money trail” model to a “follow the network trail” model, where criminal activity can no longer be viewed as a flow, but as a structure.

Deterrence and Technological Asymmetry

The criminological theory of deterrence is based on the assumption that the perpetrator evaluates the risk through three dimensions: the possibility of being detected, the speed of the institutional reaction

and the severity of the sanction. In the digital space, that assessment becomes changed, because risk is no longer measured by the legal framework, but by the experience of actors who see that technological changes are taking place faster than institutional ones. In its recommendations from 2022, Europol points to exactly this: criminal groups use regulatory inertia as an operational space, as a time span in which they can operate without a realistic feeling that they will be identified (Europol, 2022; Marković & Spaić, 2021). In such an environment, risk does not disappear – it becomes invisible, and what is invisible ceases to function as an obstacle.

Criminal groups increasingly perceive the crypto space as an *operational environment with a reduced subjective sense of danger*. The speed of transactions, pseudonymity and the global nature of networks create the impression that the risk of detection is minimal. This perception influences the normalization of crypto-crime within certain subcultures, especially those related to cybercrime, where cryptocurrencies are seen as a natural tool rather than an exception.

Several authors point out that cryptocurrencies are no longer just an instrument of financial crime, but also a tool for terrorism, cyber-attacks and destabilization of national security, precisely because they enable operations that take place “far from the eyes” of institutions (Alfieri, 2022; Zirojević & Marković, 2020). More broadly, research into the criminal capacities of artificial narrow intelligence indicates that emerging technologies developed for legitimate purposes may also be adapted to facilitate, automate, or expand harmful and criminal activities (Bjelajac et al., 2023). This breadth of use further complicates the concept of deterrence, as criminal groups respond not only to legal sanctions, but also to the technical capabilities at their disposal.

In such an environment, deterrence loses its preventive function. When the probability of detection is low and the reaction speed of institutions is insufficient, criminal groups take the initiative, while the state reacts only after the damage has already been done. This is the essential criminological implication of the crypto-ecosystem: *technology changes the balance of power between crime and the state*, thereby changing the very nature of criminal behaviour.

Conclusion

Contemporary patterns of money laundering show that criminal activities can no longer be viewed through a strict division into the “physical” and “digital” worlds. The three-phase model – placement, stratification, integration – remains a theoretical framework, but its application in practice is changing faster than institutions are adapting. In the process, cryptocurrencies have become not only a new instrument, but also a new environment in which criminal networks move with greater ease, speed and operational flexibility than in traditional finance.

Regional cases clearly show that digital space is not an abstract phenomenon, but a concrete operational tool of criminal groups. In Serbia, the “OKE Green” investment scam was busted, in which the victims were misled by false promises of earnings, while the collected funds were converted into cryptocurrencies and transferred through multiple digital wallets in order to conceal their origin. The same pattern is confirmed by other sources: money is channelled into crypto-assets precisely because fragmented digital flows make it difficult to trace and recover funds, and criminal groups use regulatory loopholes and insufficient institutional readiness to cover their tracks.

Such cases are not an exception, but a symptom of a wider process. Risk bulletins and international analysis indicate that cryptocurrencies in the region are becoming more accessible, and thus more suitable for moving and laundering money, especially in environments with weak supervision and insufficiently developed regulatory mechanisms. Legal unevenness and the slow pace of institutional reforms create a space in which digital assets can serve as a conduit for transfers of large sums without adequate oversight, opening up opportunities for sophisticated forms of concealment of the origin of funds and infiltration into legal flows.

In practice, it is shown that criminal networks adopt technological innovations much faster than legal and institutional systems manage to contain them. In that process, cryptocurrencies do not act as a cause of crime, but as an environment that allows existing patterns of action to be transferred to the digital space and adapted to its logic. They enable traditional patterns of money laundering to be mapped into the digital space, where traces are scattered, jurisdictions overlap, and the speed of transactions exceeds the speed of institutional reaction.

That is why the fight against money laundering in the digital environment cannot be only a technical issue. It requires a simultaneous understanding of financial flows, technological mechanisms and criminological patterns of behaviour. Only when those three levels are combined, it is possible to develop strategies that correspond to the reality in which criminal networks operate – a reality in which money is both a tool and a space, and the digital ecosystem becomes the key terrain on which modern organized crime takes place.

References

- Alfieri, L. (2022). Cryptocurrencies and the evolution of financial crime. *Journal of Financial Security*, 14(2), 45–62.
- Bjelajac, Ž., & Bajac, M. (2022). Blockchain technology and money laundering. *Pravo – teorija i praksa*, 39(2), 21–38. <https://doi.org/10.5937/ptp2202021B>
- Bjelajac, Ž., Filipović, A., & Stošić, L. (2023). Can AI be Evil: The Criminal Capacities of ANI. *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE)*, 11(3), 519–531.
- Dragojlović, J. (2023). Jurisdiction for criminal offenses of cybercrime – international and national standards. *Pravo – teorija i praksa*, 40(1), 63–83. <https://doi.org/10.5937/ptp2300063D>
- Elliptic Enterprises. (2022). *NFTs and financial crime: Elliptic's 2022 NFT report*. Elliptic. <https://www.elliptic.co/hubfs/NFT%20Report%202022%20-full.pdf>
- Europol. (2022). *Cryptocurrencies: Tracing the evolution of criminal finances* [Europol Spotlight Report]. Publications Office of the European Union. <https://doi.org/10.2813/75468>
- Europol. (2025). *Steal, deal and repeat – How cybercriminals trade and exploit your data: Internet Organised Crime Threat Assessment (IOCTA) 2025*. Publications Office of the European Union. <https://doi.org/10.2813/4926508>

- Filipović, A., & Bjelajac, Ž. (2025). *Human-centered security in Society 5.0: Revisiting algorithmic bias and methodological constraints in predictive policing*. *Kultura polisa*, 22(3), 74–88. <https://doi.org/10.51738/kpolisa.2025.3r.006>
- Financial Action Task Force [FATF]. (2021). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. FATF/OECD. <https://www.fatf-gafi.org>
- Financial Intelligence Unit Latvia [FIU Latvia]. (2022). *Money laundering, terrorism and proliferation financing risks of NFTs: Strategic analysis study*. FIU Latvia. https://www.fid.gov.lv/uploads/files/2022/AMLIH/FIU_MLTPF%20risks%20of%20NFTs.pdf
- Kafteranis, D., & Turksen, U. (2022). Art of money laundering with non-fungible tokens: A myth or reality? *European Law Enforcement Research Bulletin*, 22(6), 23–31. <https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/531>
- Marković, D.M., & Spaić, I. (2021). Globalizacija organizovanog kriminaliteta i transformacija u moćnu ekonomsku i oružanu silu [Organized crime globalization and transformation into a powerful economic and armed force]. *Kultura polisa*, 18(2), 39–50. <https://doi.org/10.51738/Kpolisa2021.18.2p.1.03>
- Matijašević, J., Bingulac, N., & Marinković, D. (2024). Digital evidence in criminal proceedings – challenges and solutions. *Pravo – teorija i praksa*, 41(4), 18–33. <https://doi.org/10.5937/ptp2404018M>
- Organizacija za evropsku bezbednost i saradnju, Misija u Srbiji [OEBS]. (2011). *Tipologije pranja novca u Republici Srbiji [Money laundering typologies in the Republic of Serbia]*. OEBS Misija u Srbiji. https://www.apml.gov.rs/REPOSITORY/977_tipologije-pranja-novca-u-republici-srbiji-13-09-2011.pdf
- United Nations Office on Drugs and Crime [UNODC]. (2020). *Money laundering and COVID-19: Profit and loss* (Version 1.1). UNODC. https://www.unodc.org/documents/Advocacy-Section/UNODC_-MONEY_LAUNDERING_AND_COVID19-Profit_and_Loss_v1.1-14-04-2020-CMLS-COVID19-GPML1-UNCLASSIFIED-_BRANDED.pdf
- World Bank. (2021). *Regulating virtual assets: Global practices and challenges*. World Bank Group.
- Zirojević, M., & Marković, D. M. (2020). Terrorist financing, virtual currencies, and the future of security. *Fiat Iustitia*, 2, 118–127. <https://www.ceeol.com/search/article-detail?id=947116>

Pranje novca u kripto ekosistemu: Implikacije za organizovani kriminal

Darko M. Marković

Univerzitet Privredna akademija, Pravni fakultet za privredu i pravosuđe, Novi Sad, Srbija

Sažetak

Rad se bavi transformacijom pranja novca u uslovima digitalizacije finansijskih tokova, sa posebnim osvrtom na ulogu kriptovaluta u strategijama organizovanog kriminala. Polazeći od klasičnog trifaznog modela plasmana, raslojavanja i integracije, analiziraju se načini na koje digitalni ekosistem menja operativne obrasce, dostupne instrumente i mogućnosti prikrivanja porekla sredstava. Kriptovalute uvode specifičnu dinamiku – brzinu, globalni domet i pseudonimnost – koja utiče na percepciju rizika kod izvršilaca i otežava institucionalni nadzor, čime se otvara prostor za nove tipologije finansijskog kriminala. Cilj rada jeste da prikaže kako se tradicionalni modeli pranja novca prilagođavaju kripto okruženju i koje kriminološke implikacije proizlaze iz takvih promena. Poseban akcenat stavljen je na razumevanje odnosa između tehnoloških inovacija i institucionalnih kapaciteta, kao i na to kako digitalni prostor utiče na strategije organizovanog kriminala u pogledu prikrivanja tragova, premeštanja sredstava i infiltracije u legalne tokove. Metodološki, rad se zasniva na deskriptivnoj, analitičkoj i komparativnoj obradi relevantnih domaćih i međunarodnih izvora, uključujući regulatorne dokumente, izveštaje institucija za sprovođenje zakona i dostupne podatke o slučajevima u kojima su kriptovalute korišćene u kriminalne svrhe. Time se postavlja okvir za razumevanje savremenih izazova u borbi protiv pranja novca u digitalnom okruženju.

Ključne reči: transnacionalni kriminal, finansijska bezbednost, finansijski kriminal, decentralizovane transakcije, blockchain infrastruktura