ORIGINAL SCIETNTIFIC PAPER

UNDERSTANDING MONEY LAUNDERING THROUGH CRYPTOCURRENCIES: A THEORETICAL FRAMEWORK AND INSTITUTIONAL RESPONSES

SOLEŠA Dimitrije[1], PETKOVIĆ Aleksandar[2], VLADISAVLJEVIĆ Radovan[3]

[1] Faculty of Economics and Engineering Management, Novi Sad (Serbia) ORCID: 0009-0001-8254-927X
[2] Faculty of Economics and Engineering Management, Novi Sad (Serbia) ORCID: 0009-0002-0550-7452
[3] Faculty of Economics and Engineering Management, Novi Sad (Serbia) ORCID: 0000-0002-8502-8584

E-mails: solesadimitrije357@gmail.com, tejana.ap@gmail.com, radovan.vladisavljevic@fimek.edu.rs

ABSTRACT:

Money laundering through cryptocurrencies is a global challenge due to the anonymity and decentralized nature of blockchain technology. This paper develops a theoretical framework based on agent theory, signaling theory, transparency theory, the "crying wolf" concept, and economic theory, analyzing institutional responses through qualitative methodology and the Tornado Cash case study. The findings indicate that the anonymity of cryptocurrencies facilitates money laundering, while institutional responses often lag behind due to technological complexity and regulatory gaps. The paper proposes a framework for better understanding and addressing these challenges, emphasizing the need for greater transparency, stricter sanctions, and stronger international cooperation.

***Keywords**: money laundering, cryptocurrencies, agent theory, signaling theory, transparency theory, the concept of "crying wolf", economic theories*

***JEL**: K42, G38, E42*
***DOI**: 10.5937/intrev2602084S*
***UDC**: 336.7:004*
***COBISS.SR-ID** 198466313*

INTRODUCTION

The rapid development of capital markets in the last decade has transformed global capital flows, but at the same time, it has created new challenges for financial security, among which money laundering stands out. Although technologies based on the blockchain principle promise greater transparency and security, their pseudo-anonymity, global availability, and decentralized nature allow the abuse of existing regulatory loopholes. Institutions faced with rapid technological changes and an insufficiently defined regulatory framework react fragmentarily, often with delays and uneven application of rules. The aim of this paper is to theoretically shed light on institutional challenges in the fight against money laundering through cryptocurrencies by applying five complementary theoretical approaches: agent theory, signaling theory, transparency stability theory, the concept of "crying wolf", and selected economic theories. Each of the aforementioned theoretical frameworks offers a unique insight into institutional behavior, the interrelationships of market participants, and the mechanisms governing issues of mutual trust, control, and accountability. Guided by an interdisciplinary approach, this paper attempts to connect the aforementioned theoretical approaches with real regulatory and technological practices, with the aim of creating a logically consistent and generally harmonized understanding of the complexity of money laundering in the digital environment. The analysis of institutional responses was carried out through the Tornado Cash case study, which illustrates that traditional institutional mechanisms face challenges brought by the digital financial environment, along with all the shortcomings of existing approaches. Essentially, the paper seeks to answer the question of how institutional actors can effectively respond to money laundering through cryptocurrencies using an integrated theoretical framework.

GENERAL METHODOLOGICAL CONSIDERATIONS OF THE THEORETICAL FRAMEWORK IN THE CONTEXT OF GLOBAL REGULATORY APPROACHES

Cryptocurrencies have grown into one of the most dynamic sectors of the global economy in recent years, offering innovative ways to transfer funds, invest, and manage digital assets. At the same time, their decentralized nature, the pseudo-anonymity of users, and the lack of globally harmonized regulation have created the possibility of their abuse for the purposes of money laundering, crime financing, and evasion of financial supervision. Money laundering through cryptocurrencies has become a significant global challenge due to the anonymity, decentralization, and speed of transactions enabled by blockchain technologies. According to the National Security Agency of the United States of America, pseudo-anonymity is a key factor in the use of cryptocurrencies and other digital assets for illegal purposes. According to this agency, the original catalyst for these circumstances was Bitcoin due to its pseudo-anonymous nature. A person's identity is tied to a fake name or pseudonym in its use, which serves as both a public key and a Bitcoin address [1]. Although Bitcoin has never been truly anonymous because all transactions are available on the public network, allowing anyone to inspect the records of all transactions conducted at a Bitcoin address, it is up to the Bitcoin owner to prevent their pseudonym or false identity from being associated with their real identity. As other cryptocurrencies emerged, the same principles were applied in order to provide pseudo-anonymity and perform transactions without revealing users' true identities. According to data from Chainalysis, in 2022, 20.6 billion dollars in cryptocurrencies were the subject of money laundering from illegal activities [2]. Over the past few years, regulatory bodies around the world have been trying to find answers to the challenges posed by money laundering through cryptocurrencies. Although the Financial Action Task Force (hereinafter referred to as the FATF) is a key organization that sets global guidelines for preventing money laundering, its recommendations for the crypto market encounter obstacles in implementation. Namely, the FATF notes in its 2021 report that, although some countries have implemented regulatory regimes for virtual assets (hereinafter VA – virtual assets) and virtual asset service providers (hereinafter VASP – virtual asset service providers), many jurisdictions have not yet established effective frameworks for preventing money laundering and terrorist financing. The FATF also indicates that a number of jurisdictions have failed to implement measures to mitigate the money laundering and terrorist financing risks associated with virtual asset activities, particularly in jurisdictions where virtual currency activities are developing globally and VASPs are increasingly operating across multiple jurisdictions [3]. Despite the given guidelines, inefficiencies in implementation have been observed because, although these guidelines have become binding for member countries, numerous crypto exchanges do not implement sufficiently rigorous controls, while some even

avoid compliance with regulations. Regarding the efforts of the European Union to regulate the legality of crypto-market operations and the use of virtual assets, the European Union first adopted the 5th and subsequently the 6th directives, which introduced stricter controls on the operation of platforms that enable cryptocurrency trading. It is important to understand how certain theoretical approaches can contribute to explaining the phenomenon of money laundering through cryptocurrencies, taking into account both the regulatory context and institutional reactions. To that end, the paper uses a qualitative methodology combining document analysis and the Tornado Cash case study. The case of this crypto-platform was selected due to its representativeness in the context of money laundering, data availability, and the regulatory significance of sanctions. The data were collected both from academic literature and from official documents of the FATF, the European Union, Europol, and other international organizations such as Chainalysis [2]. Within this framework, in considering the contribution of certain theoretical frameworks to understanding the role of cryptocurrencies in money laundering and related institutional responses, an analysis of agent theory, signaling theory, transparency stability theory, and the crying wolf theory will be carried out, together with specifically selected economic theories.

AGENCY THEORY

Agency theory, as developed by Jensen and Meckling, explores the relationship between principals and agents, where agents make decisions that affect the interests of the principals. It explains arrangements in which one party (the principal) delegates authority to another (the agent) but cannot fully control the agent's behavior. The authors introduce the concept of agency cost as a central element in understanding managerial behavior in systems where those who manage capital do not own it, leading to conflicts of interest between owners and managers [4]. In the context of cryptocurrencies—especially decentralized finance (DeFi)—this theory helps identify unregulated actors such as protocol developers, oracle operators, or multisig key holders, whose interests may conflict with those of users or regulators.

As Zetzsche, Smer, and Buckley observe, "where parts of the financial services chain are decentralized, we expect reconsolidation in some other but possibly less regulated, less visible and less transparent part of that chain" [5], suggesting that decentralization does not eliminate agency problems but redistributes them in less accountable forms. This lack of oversight facilitates abuse and makes money laundering harder to detect, positioning agency theory as a valuable analytical tool for understanding structural weaknesses in the crypto economy.

As Eisenhardt states, "the problem arises when the goals of the principal and the agent conflict and when it is difficult or expensive for the principal to check the behavior of the agent" [6]. In today's AML framework, regulators (principals) delegate compliance duties to VASPs (agents), who may prioritize profit and market share over regulatory obligations. This leads to moral hazard, where agents ignore suspicious activities knowing they are unlikely to face consequences.

VASPs often possess more information about user behavior and transaction flows than regulators, creating information asymmetry that enables data concealment, transaction masking, and profile manipulation. In decentralized systems (e.g., DEXs, DAOs), agency becomes abstract—without a legal entity or accountable party—resulting in an institutional void conducive to money laundering.

Unlike traditional settings, many crypto agents operate beyond jurisdictional reach and are not subject to penalties. Moreover, users frequently prefer anonymity and non-compliance with KYC rules, undermining the incentive structure that normally aligns agents with principals.

Agency theory suggests that regulators must clearly identify agents even in decentralized systems (e.g., developers, DAO coordinators, interface operators), enforce compliance mechanisms, and introduce incentive and sanctioning tools (e.g., licensing, black/white lists, fiat access controls). Reducing information asymmetry through reporting obligations and cooperation with on-chain analytics is also essential.

Agency theory explains how crypto ecosystems enable and even encourage money laundering by allowing agents—platforms, operators, and protocols—to act autonomously and often contrary to the public interest. Without proper oversight, incentives, and controls, delegated responsibility becomes a systemic vulnerability rather than a strength.

Decision-making in the area of prevention of money laundering and terrorist financing (AML/CFT) becomes significantly more complex under the conditions of cryptocurrency application. Due to their

decentralized structure, pseudonymity, and speed of transactions, traditional risk control models are no longer sufficient, so decisions are increasingly based on advanced analytics and digital tools.

In this context, cryptocurrencies introduce new challenges for institutions that have to balance regulatory compliance and business efficiency. Decisions are made based on risk assessment, transaction patterns, and digital indicators of suspicious activity, which requires continuous improvement of monitoring and risk management methods.

SIGNALING THEORY

The signaling theory in economics, developed by Michael Spence, is based on the idea that market actors use signals to influence others' perceptions and decisions. It assumes the presence of information asymmetry, where one party holds more or better information than the other. To reduce this imbalance, actors send signals—indirect indicators of quality, intent, or risk [7].

In the regulatory context, signals include public communications, enforcement actions, and regulatory initiatives that aim to influence market behavior. These signals convey priorities, levels of tolerance, and potential consequences for non-compliance. In the financial sector, signaling theory is often applied to explain how firms communicate success and legality—sometimes manipulatively—when full transparency is lacking.

In the crypto context, signaling operates on two levels. First, regulators signal to the crypto market what is considered risky or unacceptable behavior, encouraging self-regulation and deterrence. Examples include: FATF's "travel rule" guidance, signaling the expectation of identity checks [8]; SEC enforcement actions against unregistered exchanges, indicating regulatory tightening [8]; and central bank announcements about CBDCs, signaling a move to assert control over digital finance [9].

Second, crypto market actors signal to regulators and the public that they operate legally to avoid sanctions and attract investors. However, these signals can be misleading. DeFi platforms often use obfuscation tools (e.g., mixers) to weaken regulatory signals, and platforms may ignore warnings if enforcement actions do not follow. The Tornado Cash case illustrates this dynamic [5].

The credibility of signals is crucial. If a regulator announces increased supervision but fails to act, the message is perceived as weak, allowing illicit practices to continue. Signaling theory helps explain how crypto actors attempt to build legitimacy through strategic communication, even when their practices are unlawful.

This theory contributes to understanding how compliance-related signals are sent; how money laundering may involve deceptive signaling; the role of regulators as interpreters of signals; how DeFi complicates signal clarity; and how reputation and self-regulation act as signaling tools.

Many platforms signal compliance by promoting KYC/AML policies, security certifications (ISO, SOC), publishing whitepapers, audit results, and cooperating with regulators. These signals may be genuine or merely symbolic ("cheap talk"), lacking substantive application. Signaling theory thus helps distinguish de facto from de jure compliance.

Criminals use complex transaction structures to conceal illicit funds and send false positives—signals of legitimacy—by integrating dirty money into games, NFTs, or cross-border transfers. The intent is to simulate ordinary economic activity and bypass oversight.

Regulators attempt to identify false compliance signals, detect genuine red flags (e.g., abnormal volumes or flows), and act accordingly. However, the signaling environment may be saturated with "noise"—unverifiable or conflicting signals—making accurate regulatory assessment difficult.

DeFi platforms often claim, "we're just code, we don't control funds or have owners," which obscures responsibility and complicates legal enforcement. These signals, while technically neutral, mask accountability, offering a shield for illicit activity.

In the absence of central regulation, platforms rely on reputational signals—such as smart contract audits or public AML support—to gain trust. Without independent verification, this becomes a form of regulatory washing, projecting an image of compliance without substance.

Signaling theory provides insight into how actors in the crypto ecosystem communicate intent, behavior, and compliance under uncertainty and asymmetry. Its value lies in identifying authentic versus deceptive signals, revealing gaps in institutional interpretation, and underscoring the need for standardized and verifiable signaling mechanisms within regulatory frameworks.

In the context of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), signaling theory can be used to explain how different actors in the financial system send signals about their behavior and level of risk, especially in the cryptocurrency environment. Since there is a pronounced asymmetry of information between users, crypto platforms, and regulators, participants use different "signals" to demonstrate compliance or conceal risky activities—for example, implementing KYC procedures, ensuring the transparency of transaction data, or using regulated exchanges. In the case of cryptocurrencies, the problem arises because opposing signals appear in parallel, such as anonymous wallets, DeFi protocols, and transaction concealment tools, which makes it difficult to make decisions and assess the real risk within the AML/CFT system.

TRANSPARENCY-STABILITY THEORY

The transparency stability theory, rooted in political science, institutional economics, and management theory, explores how the availability, reliability, and clarity of information shape actor behavior and institutional trust. In finance, this concept translates into financial transparency, meaning open and accessible disclosure of financial data to ensure proper assessment, accountability, and public confidence. As Florini notes, "information in itself is not power, but it is an essential first step in realizing political and economic power... There are few more important battles in the world today than the battle over who can find out what" [10].

This theory is highly relevant to cryptocurrencies, where blockchain technology offers public, immutable records of transactions—commonly perceived as a form of radical transparency. However, this transparency is technical, not necessarily institutional. The anonymity (or rather pseudonymity) of users, complex layering of transactions, and the use of obfuscation tools (e.g., mixers, privacy coins, chain hopping) result in what is known as false transparency—systems that are open in appearance but functionally opaque to most actors.

Transparency in this context becomes paradoxical: while blockchain transactions are visible, actors' identities remain hidden, enabling sophisticated concealment of illegal activities. As Tapscott and Tapscott argue, transparency involves "operating in the open, in the light of day while constantly asking the question: What is hidden?" [11]. Yet many platforms, while claiming transparency through tools such as “proof of reserves,” fail to disclose essential data such as cash flows or user identities.

The illusion of transparency also exists at the regulatory level. Authorities may publish AML reports and issue guidance, but without enforcement and oversight, these actions carry little weight. In this sense, transparency becomes declarative rather than functional, weakening its deterrent effect.

Cryptocurrency systems further distort transparency through unequal information distribution. Developers, protocol operators, and major investors (whales) possess superior access and control, while regulators and users lack insight into operations that affect the system. This institutional non-transparency allows money laundering to occur without meaningful scrutiny.

Platforms may also engage in regulatory signaling by publishing whitepapers, audit results, or collaborating with firms such as Chainalysis. However, these disclosures are often unaudited, unverifiable, and not independently reviewed, raising concerns about facade transparency—where information exists but lacks mechanisms for verification, accountability, or enforcement.

Transparency stability theory thus provides critical insight into the tension between technical openness and practical opacity in crypto systems. Key contributions include: distinguishing technical from institutional transparency, defining transparency as a regulatory condition, analyzing transparency’s link to power asymmetry, identifying simulated transparency and reputational tactics, and drawing public policy implications.

From a regulatory perspective, the theory supports stronger policies mandating VASP transparency regarding identity, ownership, and compliance status. It recommends that technical visibility should be translated into actionable institutional tools (e.g., automatic transaction monitoring, token trackers, forensic analytics). The creation of a "transparency score" system for platforms, DAOs, and tokens is also encouraged.

Transparency theory reveals how selective openness in crypto systems facilitates money laundering by obscuring accountability. It emphasizes the need to differentiate between what is formally accessible and what is actually usable for oversight. Without real institutional transparency, neither legal frameworks nor market mechanisms can effectively address financial crime in the crypto domain [2].

In the context of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), transparency stability theory can be viewed through the relationship between the level of transparency of financial flows and the stability of the financial system, especially in the cryptocurrency environment. Greater transparency, through the monitoring of transactions on the blockchain and the application of regulatory mechanisms such as KYC and AML procedures, contributes to reducing information asymmetry and strengthening trust in the system, thereby increasing its stability. However, in the crypto ecosystem, where anonymous or pseudonymous protocols also exist, reduced transparency can increase the risk of abuse and make it difficult for regulators and financial institutions to make decisions when identifying suspicious activities.

THE "CRYING WOLF" THEORY

The “crying wolf” theory, drawn from Aesop's fable, reflects a psychological and institutional dynamic in which repeated warnings without follow-up actions cause desensitization to actual threats. Rooted in behavioral economics and risk communication theory, it explains how frequent unfulfilled regulatory alerts lead to reduced public and institutional responsiveness—even when the danger materializes. As Cass R. Sunstein notes, excessive fear-based messaging can cause regulatory fatigue, weakening institutional credibility [12]. Kuran and Sunstein similarly warn of availability cascades—initial overreactions to perceived risks, followed by apathy [13].

In the cryptocurrency context, this means that repeated regulatory warnings about money laundering risks—issued by central banks, financial regulators, and international bodies such as the FATF—often lack accompanying enforcement, reducing their impact. Despite years of alerts (e.g., from the ECB, SEC, and others between 2013–2017), crypto platforms continued operating without licenses, often relocating to jurisdictions with lax oversight.

A key example is the FATF’s “Travel Rule” (2019), requiring VASPs to share sender/receiver data for large transactions. Yet, in many countries, this rule remains unimplemented, sending a message to market actors that compliance is optional. Similarly, warnings about DeFi’s risks often go unenforced due to the lack of a central control point, legal ambiguity, or technical limitations [14].

A clear illustration is the Tornado Cash case: the U.S. Treasury sanctioned the platform only in 2022, after billions had already been laundered, including by North Korean hacker groups [16]. This reactive approach signaled that consequences come only after major damage—undermining the deterrent effect of earlier warnings [15].

In essence, this theory reveals how frequent but ineffective warnings erode regulatory credibility, encourage risk normalization, and reduce actors’ motivation to comply. Platforms begin to see warnings as empty threats, while users rationalize criminal activity by portraying the state as technologically incompetent or corrupt. As a result, a culture of distrust and institutional disengagement emerges.

Key contributions of the “crying wolf” theory in the context of crypto-based money laundering include: explaining the loss of impact of repeated warnings without sanctions; highlighting the normalization of criminal behavior and the erosion of regulatory authority; emphasizing the failure of reactive regulation and the need for proactive engagement; and suggesting improvements for regulatory practice, including consistent enforcement, positive incentives, and coordinated global messaging.

The “crying wolf” theory offers a powerful lens to understand why regulatory signals about money laundering through cryptocurrencies often fail—not because the warnings are wrong, but because they are not backed by timely and concrete action. For institutional trust to be restored, regulation must be consistent, credible, and enforced, ensuring that each warning leads to visible consequences [17], [5].

In the context of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), the crying wolf theory explains the problem that arises when suspicious transaction detection systems in the cryptocurrency environment generate a large number of false positive alarms. Under such conditions, financial institutions and compliance systems may begin to ignore warnings over time, as confidence in their accuracy decreases, which directly affects the quality of decision-making. In the crypto ecosystem, where transaction patterns are complex and often unclear due to anonymity, DeFi protocols, and global availability, this effect can lead to "signal saturation", making it difficult to recognize truly risky activities in a timely manner and reducing the effectiveness of AML/CFT systems.

ECONOMIC THEORY

When considering the application of economic theories to the issue of money laundering through cryptocurrencies, it is important to note that these theories are numerous and evolve with social, political, and technological developments. Among them, rational choice theory offers an explanation of criminal behavior as a calculated act, where individuals weigh expected benefits against possible costs. The use of cryptocurrencies fits well into this model because the chances of detection are often low, while the benefits—such as anonymity, borderless access, and lack of regulation—are high. As Gary Becker pointed out, crime is not necessarily driven by pathology but can be a rational response to favorable conditions [18].

Transaction cost theory explains why cryptocurrencies are structurally attractive to those engaging in illicit financial activities. By minimizing the need for intermediaries and simplifying cross-border transfers, they lower the financial, temporal, and legal costs associated with laundering funds. The absence of institutional oversight, combined with decentralized protocols, reduces friction and increases efficiency, making it easier to hide the origin and ownership of assets [19]. In this light, increasing transaction costs—through mandatory KYC/AML compliance, banning anonymization tools, and penalizing non-compliant platforms—becomes a strategic policy lever to deter criminal use.

The theory of public goods and negative externalities, meanwhile, shifts the focus from individual incentives to systemic consequences. Money laundering through cryptocurrencies harms the collective by undermining trust in financial institutions, enabling criminal reinvestment, and depriving states of taxable income. The public goods required to combat this—such as functional institutions, forensic technologies, and international cooperation—are often underdeveloped or unevenly distributed, creating enforcement asymmetries. Cryptocurrencies, while open and decentralized, are exploited privately, producing external costs that affect markets, regulation, and public trust [20], [21].

From this perspective, money laundering is not only a legal issue but also a structural and social problem that reflects imbalances in regulation, incentives, and access to public goods. The application of economic theories highlights the rationality behind criminal actions, the structural loopholes that facilitate them, and the broader harms imposed on society as a whole.

In the context of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), economic theory provides a framework for understanding how economic incentives shape the behavior of participants in the financial system, including cryptocurrencies. The basic idea is that individuals and organizations make decisions based on a rational assessment of costs and benefits, so abuses of the financial system occur when the expected benefits from illegal activities outweigh the risks and costs of detection. In the crypto ecosystem, the low entry barrier, speed of transactions, and relative anonymity can reduce the risk perception of illegal actors, while regulatory measures, oversight, and transparency of blockchain technology increase the "cost" of non-compliant behavior. In this way, economic theory helps to understand how the design of regulatory and technological mechanisms can influence decision-making and reduce the risk of money laundering and terrorist financing.

"TORNADO CASH" CASE STUDY

A group of authors from the University of Tsukuba in Japan presented a paper entitled "Empirical Analysis of Cryptocurrency Mixer: Tornado Cash" at the World Congress of Computer Science, Computer Engineering and Applied Computing, which was held in 2023 in Las Vegas, United States of America. The paper uniquely presents techniques of money laundering through cryptocurrencies using the decentralized Ethereum protocol Tornado Cash. This paper represents an excellent basis for considering the contributions of the analyzed theoretical frameworks and making proposals for improving the regulatory environment and institutional responses in order to prevent money laundering through cryptocurrencies [22]. In the study, the authors clustered and analyzed Tornado Cash deposit addresses, listing potential criminal addresses while clarifying current money laundering practices. By using categories such as "Phish/Hack" and "Exploit" in Etherscan's Public Name Tags to identify criminal addresses, the authors calculated the percentage of deposited funds associated with those addresses and analyzed their potential involvement in money laundering through Tornado Cash. The study further showed that Tornado Cash performed cryptocurrency mixing services based on the Ethereum blockchain, which uses zero-knowledge proofs. Cryptocurrency mixers combine transaction data from multiple accounts so that transactions and addresses cannot be traced back to individual users. Unlike other mixers, Tornado Cash does not mix transaction data but breaks the

link between the addresses of users who have deposited and withdrawn money from Tornado Cash so that transactions and addresses cannot be traced back to individual users. This ensures the privacy of cryptocurrency owners and their associated addresses. In addition, Tornado Cash minimizes the possibility of information leakage by the mixing service operator, theft through hacking, and operator escape by using a smart contract where there is no administrator in the mixing process. Tornado Cash works as follows: first, multiple users deposit a certain amount of money into Tornado Cash smart contracts. Then, users can withdraw money to their other accounts securely and privately using zero-knowledge proofs. This breaks the link between the deposit and withdrawal accounts. Since the owner of the withdrawal account always exists in the group of owners of the deposit account, a higher level of anonymity and security is ensured when multiple users deposit money after their own deposit. Tornado Cash allows deposits in fixed units of 1, 10, and 100 ETH, as well as DAI, wBTC, and other Ethereum-based cryptocurrencies. Based on the analysis and research, the mentioned authors concluded that about 20% of the total deposits in Tornado Cash from February to July were used for money laundering. They also concluded that Tornado Cash is more likely to be used for money laundering than for user privacy, which was its original purpose [22].

Although it also had legitimate use related only to protecting user privacy, Tornado Cash was repeatedly identified as a key instrument for money laundering from major hacks (e.g., the Axie Infinity hack amounting to 600 million dollars). For this reason, in August 2022, OFAC sanctioned the platform, which caused debates about the regulation of decentralized systems [23].

It is now necessary to consider the theoretical perspective of the Tornado Cash case study through five selected theoretical approaches. Viewed in the context of agency theory, smart contracts act as agents that enable anonymity but without accountability to regulators, creating moral hazard. On the other hand, signaling theory in this context can be seen through OFAC's sanctions, which sent a signal of strict surveillance, but their effectiveness was limited due to the decentralized nature of the platform. Looking at the transparency theory framework, it is clear that the lack of transparency in Tornado Cash makes it difficult to track transactions, while tools such as Etherscan's tags are not proactive enough [24]. If the case of "Tornado Cash" were observed from the perspective of the "crying wolf" theory, one could conclude that frequent warnings about the risks of mixers without concrete measures led to a decline in confidence in regulatory signals. Finally, looking at the Tornado Cash case through the lens of economic theory clearly indicates that low costs and high anonymity make Tornado Cash attractive to criminals. Considering the entire case and the consequences of Tornado Cash, it is necessary to point out the institutional responses that followed. The United States imposed sanctions, while the European Union adopted stricter AML directives, although global non-compliance continues to limit effectiveness. Blockchain forensic tools (e.g., Chainalysis) show progress, but anonymous platforms such as Monero still create difficulties [2].

Considering agency theory in the context of the Tornado Cash case, it can be seen that principal-agent relationships break down for the following reasons: 1) there is no clear "agent" because the protocol functions autonomously as a smart contract without a centralized entity; 2) programmers and administrators formally renounce control ("code is law"), thereby escaping institutional responsibility; 3) institutions (regulators as principals) have no one to delegate control to, so they have no levers of pressure. Agency theory in the Tornado Cash case essentially explains the structural impossibility of imposing liability because the agent is not legally identified, which opens the door for abuse of the protocol for money laundering purposes.

Looking through the prism of signaling theory, it can be concluded that Tornado Cash sent ambiguous signals because, technically speaking, the documentation and interface emphasized "privacy" but without explicit separation from criminal use. At the same time, developers did not introduce KYC mechanisms or restrictions for high-risk transactions, which signaled "tolerance" for money laundering. In the described way, it is clear that signaling theory helps to understand how institutions can interpret the absence of certain measures as a signal of aiding or concealing criminal acts, or at least negligence, which contributed to OFAC's decision to declare Tornado Cash a risky entity.

In relation to transparency theory, it can be said that at first sight Tornado Cash seems transparent because all transaction flows are on the public blockchain, where the code is open and reviewed. However, in practice, it has been shown that the pseudonymity of Ethereum addresses, the application of cryptographic techniques such as Zero-Knowledge Proofs, and the mixer logic that makes it impossible to track money make the system essentially non-transparent to institutional actors. In this way, transparency theory exposes the following specific paradox: technical transparency does not mean institutional transparency at the same time, which makes it impossible for law enforcement authorities to identify money laundering participants.

It is important when observing the Tornado Cash case through the prism of the "crying wolf" theory to note that before OFAC imposed sanctions on this platform, institutions warned about the risks of crypto mixers for years but without taking concrete measures against Tornado Cash. At the same time, they allowed the platform to operate smoothly and its services to be used by malicious entities such as the Lazarus group from North Korea. With all this in mind, it is clear that the "crying wolf" theory can explain why Tornado Cash became an "accepted" tool in the eyes of users because the perception of users was that the state only verbally threatened but did nothing. The sanctions came late, and many viewed them as excessive and politically motivated.

Analyzing the Tornado Cash case study in the context of certain economic theories also provides important insight into the structural, institutional, and individual aspects of money laundering through cryptocurrencies. Take, for example, the theory of rational choice, where the basic assumption is that individuals act rationally in order to maximize their benefits and minimize their costs. In the case of Tornado Cash, users of this platform made decisions based on a rational calculation—they opted for this service in order to hide the traces of transactions, reduce the risk of identification, and protect or illegally exploit anonymity. In addition, participants in money laundering benefited from Tornado Cash because the benefits (anonymity, non-detection) exceeded the potential costs in the form of fines and other legal consequences. Ultimately, Tornado Cash developers and operators rationally chose code architecture (decentralized smart contracts) to minimize their legal liability and maintain legal neutrality (architectural liability). Considering these circumstances, it can be argued that rational choice theory explains the behavior of actors at the individual level—the level of users, developers, and hackers as rational persons.

If the theory of transaction costs is taken into consideration, its basic assumption is that economic agents choose institutions and mechanisms that minimize transaction costs (informational, legal, operational, and risk-related). Tornado Cash had all these features because it reduced the transaction costs of money laundering in the digital environment by eliminating the need for intermediaries and reducing the risk of monitoring. Due to its automated and decentralized design, Tornado Cash removed bureaucratic barriers and intermediaries such as banks, which was ideal for criminals seeking transaction efficiency. At the same time, the transparency of the blockchain represented a negative cost for criminal structures, but Tornado Cash successfully neutralized it through the "mixing" of tokens. Accordingly, it can be said that the contribution of transaction cost theory in the analysis of the Tornado Cash case is reflected in the fact that it explains why Tornado Cash proved to be the most cost-effective institutional alternative for money transfer in high-risk and low-monitoring environments.

Finally, the theory of public goods and negative externalities can make a certain contribution when analyzing the case of Tornado Cash in the context of money laundering through cryptocurrencies. The basic assumption of this theory is that certain things, phenomena, and environments (e.g., clean air, security, stability of the financial system) have the character of public goods and are subject to degradation due to negative externalities. Looking at the case of Tornado Cash, it can be argued that this platform created negative externalities for the financial system, security, and the fight against terrorist financing by enabling money laundering, financing hacker activities, and supporting terrorist groups. On the other hand, the transparency of the blockchain can be considered a public good, but Tornado Cash violated this transparency, which led to a negative impact on trust in cryptocurrencies.

The analysis of Tornado Cash through several theoretical prisms shows that money laundering through crypto protocols is not only a technical but above all an institutional phenomenon where the absence of responsibility (agency problem), manipulation of signals (signaling theory), simulated transparency (transparency paradox), and loss of trust in institutional reactions ("crying wolf" theory) create an ideal environment for transnational money laundering. Therefore, the solution is possible only through multidisciplinary and coordinated institutional reform.

CONCLUSION

Cryptocurrencies present a complex challenge for institutional responses to money laundering. A theoretical framework that integrates agency theory, signaling theory, transparency theory, the "crying wolf" theory, and economic theory reveals the weaknesses of current regulatory approaches. The Tornado Cash case study illustrates the need for new regulatory models that are adapted to the digital environment. The analysis points to several key findings: regulatory gaps exist as the decentralized nature of cryptocurrencies makes it difficult to implement traditional AML/KYC measures. On the other hand, as a form of theoretical support, it can be concluded that the selected theoretical frameworks provide a comprehensive insight into institutional challenges, especially in terms of information asymmetry and ineffective signals. In addition, it is necessary to point out the phenomenon of risk normalization because the indecision of regulators leads to the normalization of illegal activities, reducing the motivation for compliance. From all of the above, it can be concluded that an effective fight against money laundering through cryptocurrencies requires transnational cooperation, technological innovation, and consistent application of regulatory measures. Further harmonization of standards is necessary, with the introduction of global AML/KYC standards, including the FATF's "Travel Rule", with simultaneous technological advances in the development of artificial intelligence and blockchain tools for tracking anonymous transactions. Along with the proposed measures, it is necessary to further strengthen transparency in relation to mandatory reporting by platforms on AML compliance and the existence of public registers. Furthermore, it is necessary to consider certain types of sanctions and incentives in order to prescribe stricter penalties for non-compliant platforms and rewards for responsible behavior. Finally, an effective fight against money laundering through cryptocurrencies also requires strong international cooperation through automated data exchange between regulators. Future research should focus on the quantitative analysis of the volume of money laundering and the evaluation of the effectiveness of the proposed measures.

LITERATURE

[1] Homeland Security (2022). Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies, pp. 21.

[2] Chainalysis (2023). 2023 Crypto Crime Report. New York: Chainalysis, pp. 5, 50.

[3] FATF (2021). FATF – Virtual Assets and Virtual Asset Service Providers: Updated Guidance for a Risk-Based Approach, pp. 10.

[4] Jensen, M. C., & Meckling, W. H. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. Journal of Financial Economics, 3(4), 305–360.

[5] Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2020). Decentralized Finance. Journal of Financial Regulation, 6(2), 172–203.

[6] Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. Academy of Management Review, 14(1), 57–74.

[7] Spence, M. (1973). Job Market Signaling. Quarterly Journal of Economics, 87(3), 355–374.

[8] U.S. Securities and Exchange Commission (SEC). (2022). SEC Adds Jobs to Special Unit Dedicated to Protecting Investors in Crypto Markets and Cyber Threats. Press Release No. 2022-78.

[9] BIS (2021). BIS Innovation Hub Work on Central Bank Digital Currency (CBDC). Available at: https://www.bis.org/about/bisih/topics/cbdc.htm

[10] Florini, A. (2007). The Right to Know: Transparency for an Open World. New York: Columbia University Press, pp. 1, 23.

[11] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World. New York: Penguin Random House LLC, pp. 26.

[12] Sunstein, C. R. (2009). Worst-Case Scenarios. Harvard University Press.

[13] Kuran, T., & Sunstein, C. R. (1999). Availability Cascades and Risk Regulation. Stanford Law Review, 51(4), 683–768.

[14] Crenshaw, C. A. (2021). Statement on DeFi Risks, Regulations, and Opportunities. U.S. Securities and Exchange Commission (SEC), November 9, 2021.

[15] Europol (2021). Cryptocurrencies – Tracing the Evolution of Criminal Finances. Europol Spotlight Report Series. Luxembourg: Publications Office of the European Union.

[16] U.S. Department of the Treasury (2022). U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. U.S. Department of the Treasury, August 8, 2022. Available at: https://home.treasury.gov/news/press-releases/jy0916

[17] Gambetta, D. (2009). Codes of the Underworld: How Criminals Communicate. Princeton, NJ: Princeton University Press, pp. 9.

[18] Becker, G. S. (1974). Crime and Punishment: An Economic Approach. In G. S. Becker & W. M. Landes (Eds.), Essays in the Economics of Crime and Punishment (pp. 1–54). New York: National Bureau of Economic Research.

[19] Williamson, O. E. (1975). Markets and Hierarchies: Analysis and Antitrust Implications: A Study in the Economics of Internal Organization. University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship. Available at: https://ssrn.com/abstract=1496220

[20] Samuelson, P. A. (1954). The Pure Theory of Public Expenditure. The Review of Economics and Statistics, 36(4), 387–389.

[21] Pigou, A. C. (1920). The Economics of Welfare. London: Macmillan and Co. Limited.

[22] Youn, M., Chin, K., & Omote, K. (2023). Empirical Analysis of Cryptocurrency Mixer: Tornado Cash. 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), Las Vegas, USA.

[23] U.S. Department of the Treasury (2022). Treasury Sanctions Tornado Cash for Laundering Virtual Currency Used by Malicious Actors. Press Release, August 8, 2022.

[24] Youn, H., Choi, W., Lee, H., & Kang, T. (2023). Tornado Cash Money Laundering Detection Using Etherscan's Public Name Tags. IEEE Access, 11, 2323–2333.

Article history:

Received 14 July 2025

First revision 04 August 2025

Second revision 03 Jun 2026

Accepted 25 Jun 2026