

Crypto Laundering: An Analysis from a Game Theory Perspective

Iagor Matos Rodrigues^a, Ryan Hendryk Pereira de Almeida^b,
Matheus Silva de Paiva^c

^a *matosiagor@gmail.com.br*

^b *ryanhendryk124@gmail.com*

^c *matheus.paiva@p.ucb.br*

Abstract: Cryptocurrencies have revolutionized the financial sector by enabling decentralized electronic transactions that bypass traditional intermediaries. However, their anonymous nature has led to growing concerns about their use in money laundering, sparking an increase in illicit activities. This article investigates this issue, focusing on the role of cryptocurrency exchanges and the regulatory challenges they pose. By applying game theory, the study analyzes the incentives and strategies of various agents involved and explores potential regulatory and preventative measures to curb illicit behavior within the global financial system. We find that effective regulation is essential to prevent misuse of cryptocurrencies, but it must be carefully balanced. Overly stringent measures could undermine the economic potential of cryptocurrencies, preventing them from realizing their full market potential. Governments should focus on adaptable frameworks that promote innovation while addressing risks, ensuring that cryptocurrencies can thrive without becoming tools for illicit activities.

Keywords: Money Laundering; Cryptocurrencies; Global Regulation; Game Theory; Cryptocrowdfunding.

1. Introduction

In the contemporary context, the sophisticated practice of money laundering has taken on increasingly complex forms, challenging traditional regulatory frameworks and imposing new dilemmas on regulatory bodies. In light of this, we developed a mathematical model using Game Theory to help understand the key choices that governments and criminals might make, considering a scenario in which cryptocurrencies emerge as a central tool for concealing illicit funds.

Applying Game Theory in this context highlights the crucial importance of exchanges, which act as potential key players in the intricate process of money laundering. In this regard, the incentives of the agents involved, ranging from criminals hiding illicit funds to the authorities responsible for monitoring and enforcement, underline the urgent need for comprehensive studies in this area.

Given the rapid transformations in the financial market, closely monitoring these changes is essential for the development of effective

strategies for regulating and preventing illicit activities. As society seeks solutions to the challenges posed by cryptocurrencies, the need for special attention to regulations becomes evident.

While these regulations aim to strengthen the integrity of the global financial system amid rapid technological innovations, they do not always achieve the expected outcomes. Moreover, money laundering is not an issue exclusive to cryptocurrencies, as it is also widely associated with traditional currencies. The search for effective solutions requires a delicate balance between promoting innovation and mitigating risks, and it is crucial to recognize that isolated regulations may not be sufficient to address these complex challenges. A collaborative approach between the public and private sectors remains essential to navigating this ever-evolving landscape.

2. Cryptocurrencies and Money Laundering: A Literature Review

Cryptocurrencies represent a disruptive innovation in the financial landscape, introducing a decentralized paradigm for conducting electronic transactions. In Brazil, for instance, the Normative Instruction of the Federal Revenue of Brazil (2019) strengthens this response to the decentralization of cryptocurrencies by establishing and regulating the requirement to provide information about operations carried out with crypto assets to the Special Secretariat of the Federal Revenue of Brazil (RFB). The concept of cryptocurrency was first explicitly mentioned by Wei Dai in 1998 (Montenegro, 2020), but the term gained more relevance after the creation of Bitcoin, the first globally recognized cryptocurrency (Horchel, 2022), which redefined how we conceive and conduct financial transactions (Nakamoto, 2008).

Nakamoto (2008) highlights the online commerce's dependence on financial institutions as trusted third parties to process electronic payments. The architecture is entirely protected by cryptography, ensuring the confidentiality and privacy of all financial transactions. This enables users to make payments, purchases, and fund transfers from anywhere in the world without relying on intermediaries to complete the operations (Andrade, 2017). This system would allow direct transactions between two parties, with irreversibility and protection against fraud. As Nakamoto (2008) emphasized, the proposal aims to “enable direct transactions without the need for trusted third parties”.

There had been previous attempts to design structures in this direction, but all failed for one of two reasons: “1) they were usually owned by a commercial company, and therefore, presented a centralized point of failure; or 2) they did not overcome the so-called ‘double-spending’ problem” (Ulrich, 2014, p. 11). The issue of double-spending, which is a central concern in electronic transactions, involves the possibility of the same digital unit of value being used more than once, which could compromise the integrity of the system. In the context of cryptocurrencies, this issue is innovatively addressed. Bitcoin, in turn, was created to be absolutely non-replicable, and its system was developed so that the transaction history would allow the reconciliation and verification of each monetary unit throughout the currency's

evolution. Additionally, the essential aspect was that the currency was integrated into an open-source network, not owned by any specific entity, which eliminated the problem of a single point of failure (Ulrich, 2014).

Nakamoto (2008) highlights that Bitcoin is designed to be secure as long as honest nodes control more computational power than any group of cooperative attacker nodes. Decentralization is a fundamental principle, eliminating the need for a trusted intermediary, and transactions are recorded in a blockchain using proof of work. The network is robust, allowing nodes to enter and exit at will.

It is known that cryptocurrencies have revolutionized the structure of intermediation by challenging established principles and questioning payment modalities since their inception (Castro, 2023). As a result, cryptocurrencies have been integrated into the financial system in various ways. In the future, it is expected that most technologies around the world will adopt blockchain, the network underlying cryptocurrencies, as an effective solution for conducting online transactions. One area where blockchain technologies can be employed is in crowdfunding platforms (Saadat *et al.*, 2019). This form of financing prominence due to its ability to connect those seeking financial support directly with a broad community of potential investors, bypassing traditional banking channels and venture capital investors (Garg *et al.*, 2022). Additionally, it presents advantages over conventional financing methods by recording all transactions on public blockchains, such as Bitcoin or Ethereum, providing greater transparency to contributors regarding the tracking of their investments.

These innovative characteristics of cryptocurrencies, while revolutionary, can also pose significant challenges, especially for regulatory authorities, financial institutions, law enforcement agencies, and other entities involved in the prevention and combat of money laundering. The omission by cryptocurrency administrators can create some insecurity for users, who in certain situations cannot turn to any administrative or judicial body (Moura & Lima, 2019). However, overregulation of the market can often have the unintended consequence of stifling innovation, deterring potential investments, and driving businesses to more favorable jurisdictions. Excessive controls may create barriers that push capital and entrepreneurs

away, ultimately harming the market by reducing competition and slowing economic growth that could have been achieved with a more balanced regulatory approach.

The physical non-existence of cryptocurrencies, direct transmission between parties, irreversibility of transactions, global reach, and the immediate non-identification of those involved in transactions are factors that favor money laundering practices (Bueno, 2020). However, while all of this is true, these same features also contribute significantly to economic prosperity by dramatically reducing transaction costs, increasing trust between parties, and fostering both trade and innovation. The efficiency of decentralized systems encourages a more dynamic market environment, supporting global commerce and technological advancement.

Law No. 9,613/98, which addresses the crime of “money laundering” (LCLD) and establishes the Financial Activities Control Council (COAF), stipulates in its Art. 1, main section and item V, the following:

Article 1. To conceal or disguise the nature, origin, location, disposition, movement, or ownership of assets, rights, or values that are directly or indirectly derived from a crime:

V - against Public Administration, including the requirement, for oneself or for others, directly or indirectly, of any advantage, as a condition or price for the practice or omission of administrative acts.

As described in the booklet “Money Laundering: A Global Problem (Brazil, 2020), this process involves a set of commercial or financial operations aimed at integrating into each country’s economy resources, assets, and services that originate from or are connected to illicit acts.

This practice, which represents a crucial stage in the life cycle of illicit money, allows individuals or organizations to conceal the true origin, ownership, or destination of resources. The main challenge lies in the complex structure of global information networks and how they operate. Due to anonymity, ease of use, rapid transactions, and the ability to make automatic transfers and operate across multiple

jurisdictions without physical presence, global information and communication networks have created new opportunities for criminals to exploit in money laundering, reducing detection risks (Andrade, 2017). Therefore, the practice of crimes such as money laundering in the virtual environment can be identified, for example, by the large number of bank accounts linked to a virtual currency administrator or to a company involved in virtual currency exchanges, which are likely used as intermediary accounts (known as “layering” - the second stage of the money laundering process) (Andrade, 2017, p. 55).

This phenomenon raises concerns about the use of cryptocurrencies to facilitate criminal activities such as money laundering. Therefore, it is crucial to recognize that preventive regulatory practices will need to be implemented (Hofert, 2019).

According to the COAF¹ booklet (2020), the money laundering process generally involves three main stages: (i) placement, where illicit funds are introduced into the financial system; (ii) dissemination, which seeks to hide the trail of illegal money through complex and often international transactions; and (iii) integration, when the now “clean” money is reintroduced into the economy as legitimate. In 2019, illicit cryptocurrency addresses moved approximately \$3.4 billion, reaching around \$23.8 billion in 2022, representing a notable 68.0% increase compared to 2021. Centralized exchanges were responsible for nearly half of these funds, acting as conversion points for fiat currency. Despite a reduction in the overall use of mixers², they still processed an impressive \$7.8 billion, 24% of which came from illicit sources, indicating a shift in their usage pattern for criminal activities. The concentration of illicit funds in five major fiat conversion platforms suggests a high centralization in a few services. Additionally, underground money laundering services, less accessible and known than conventional mixers, moved approximately \$6 billion in 2022 (Grauer et al., 2023).

These numbers highlight a significant potential increase in money laundering activities

¹ The COAF, administratively linked to the Central Bank of Brazil (BCB), is Brazil’s central authority in the fight against money laundering and the financing of terrorism, responsible for receiving, analyzing, and disseminating financial information. It was established by Law No. 9,613 of 1998 and restructured by Law No. 13,974 of 2020, with technical and operational autonomy throughout the country.

² Mixers (or tumblers): Tools used to enhance privacy in cryptocurrency transactions by mixing tokens from various users, thus obscuring the traceability of the funds’ origin and destination.

through cryptocurrencies in recent years, especially from 2019 to 2022, representing a 68.0% growth in just the last-mentioned year. This increase can be attributed to several factors, including the growing acceptance and use of cryptocurrencies, as well as the evolution of money laundering strategies. It is interesting to note that the cryptocurrency landscape is evolving in other aspects, indicating broader acceptance and the consolidation of this innovative technology. A notable example is the growing number of Bitcoin ATMs³ installed worldwide. In 2021 alone, over 10,000 Bitcoin ATMs were installed that year. (Baltrusaitis, 2021)

These ATMs offer an accessible and easy way for individuals to buy, and in some cases, sell cryptocurrencies using credit or debit cards, for instance. During the first nine months of 2021, 13,242 Bitcoin-supporting ATMs were installed globally. North America leads with 93.5% of the global total, followed by Europe with 4.5%, while South America represents 1% (Baltrusaitis, 2021). The significant growth of these ATMs underscores the increasing popularity of cryptocurrencies, providing easier access for new entrants into the crypto asset market.

Although the current number of Bitcoin ATMs is considered insignificant compared to traditional financial sectors, the growth trend suggests greater adoption in the future. The combination of increased money laundering activity and the significant growth in the number of Bitcoin ATMs highlights not only the challenges but also the ongoing evolution and acceptance of cryptocurrencies in the global financial landscape.

Beyond the complex challenges linked to money laundering through cryptocurrencies, it is imperative to understand the central role of exchanges, the platforms where users can buy and sell these digital assets, in the decentralized financial landscape. These entities not only facilitate cryptocurrency trading but also play a crucial role in shaping and transforming the global financial ecosystem. Therefore, it is up to the competent regulatory body to create a methodology for analyzing and monitoring exchanges, in order to assess the compliance mechanisms of these platforms (Morais & Falcão, 2022). In nations lacking specific

regulations for them, opportunities arise for individuals in different parts of the globe to use these platforms, often ensuring a considerable level of anonymity in their transactions (Grzywotz, 2019). In a regulated environment, it would be necessary for cryptocurrency exchanges to implement KYC (Know Your Customer) procedures to identify users.

Consequently, the potential regulation of cryptocurrencies has become the subject of intense international debate. It was even a topic of discussion at the 2nd Session of the G20 Technology Seminar, where concerns were expressed about how regulation should be approached. There is the challenge of balancing, on one hand, the promotion of innovation and, on the other, the responsibility to ensure public interest in areas such as financial stability, consumer protection, and the implementation of anti-money laundering policies (Santana & Moraes, 2019). The absence of specific regulations may create an environment conducive to the exploitation of loopholes by malicious actors. These platforms, by offering an apparently anonymous interface, can become fertile ground for suspicious activities, including the potential facilitation of illicit transactions. However, it is crucial to recognize that the anonymity provided by them is not inherently negative, as it can be a legitimate tool for protecting financial privacy.

Thus, the pursuit of balance between user privacy and the prevention of illegal activities emerges as a fundamental challenge in the evolution of regulatory policies for cryptocurrency exchanges. Regulation can play a crucial role in inhibiting money laundering, holding agents involved in such crimes accountable, and ensuring the security of cryptocurrency-related operations, while also driving the market through the trust it provides. (Morais & Falcão, 2022)

Recently, a significant event shook the cryptocurrency world, highlighting the detrimental implications that can occur in this environment. The CEO of Binance, the world's largest cryptocurrency exchange, Changpeng Zhao, pleaded guilty to money laundering violations. Court documents revealed a broad effort by Binance to circumvent laws prohibiting transactions with individuals from countries sanctioned by the United States, such as Iran, Cuba, and Syria

³ Bitcoin ATMs: Physical machines that allow the conversion of fiat currency into Bitcoin, providing direct access to the cryptocurrency market without the need for an online platform.

(Forbes, 2023). At the same time, Denis Katana, also known as Denis Tokarenko, became a central figure in a case that exposes the growing trend of the Russian mafia using cryptocurrencies for money laundering, in collaboration with an ex-Soviet organized crime syndicate (Nieto, 2023).

These episodes demonstrate the complexities surrounding cryptocurrencies in the context of money laundering. Therefore, it is crucial to highlight the risks associated with the activities of exchanges in the cryptocurrency universe, often involved in fulfilling third-party interests for profit. The enhancement and specialization of criminal organizations underscore the urgency for more stringent global regulations and compliance controls on exchanges, aimed at ensuring transparency and legality in transactions. The ability of individuals to bypass specific regulatory barriers emphasizes the importance of global efforts to preserve the integrity of the decentralized financial system and prevent the misuse of these innovative technologies.

In the "Guía de investigación en el lavado de activos mediante criptodivisas" (Agredano & Lanau, 2022), distinctive characteristics in suspicious transactions are highlighted, from suspicious real estate operations to the creation of shell companies by drug traffickers to disguise illicit funds. Criminal organizations are introducing substantial volumes of funds into Europe, especially originating from South America, through the opening of accounts in Spanish financial entities, expanding not only in real estate investments but also in instrumental companies. An innovative typology highlighted is the use of Bitcoin ATMs, operated by citizens, mainly South Americans, presenting similarities with Money Transfer Management Companies used in money laundering networks by organizations dedicated to drug trafficking.

3. The Cryptlaundering Game

In this section, we will introduce the game through a fictional story. To analyze the overall situation, we will use mathematical modeling based on Game Theory.

The game will have the following players: (i) "Company Z," which has resources derived from

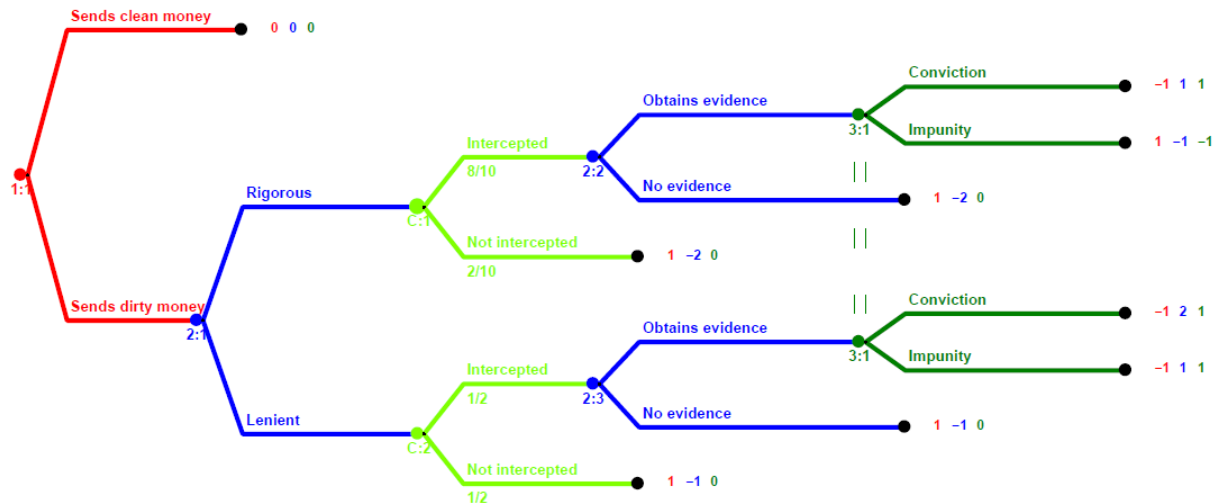
illicit activities and is engaged in money laundering through the strategic use of cryptocurrencies, (ii) The Regulator, who plays the role of monitoring suspicious transactions and must gather sufficient evidence to bring the case to trial and hold those involved in the money laundering process accountable⁴ (iii) The Judiciary, which has the duty to hold the responsible parties accountable based on the evidence gathered; in this context, the judiciary system of a particular country with anti-money laundering laws.

Additionally, an important player in the money laundering process that deserves attention is the cryptocurrency exchange. In the game, we will deal with a fictitious exchange with the following specifics: (i) It operates in a country where there are no laws regulating its operations, specifically regarding the application of Know Your Customer (KYC) practices (ii) It does not require user identification, guaranteeing anonymity for transactions on its platform (iii) It has no incentives to request the source of users' funds; it merely facilitates the conversions it can perform.

To conduct money laundering, Company Z initially transfers its illicit resources to the Exchange. This platform, operating without user identification requirements, facilitates the anonymous conversion of funds into cryptocurrencies. Furthermore, the Exchange employs mixing/tumbling techniques, which obscure the origin of the funds, making tracing more complex. With the funds converted and mixed, Company Z directs them to cryptocurrency crowdfunding platforms, making contributions to legitimate projects. This method allows the illicit money to be reintroduced into the formal economy as if it originated from legal sources, thus completing the money laundering cycle. The structure of the game can be visualized in Figure 1, which illustrates the extensive form game with incomplete information.

This game illustrates the complexity of the operation, where Company Z initially seeks to convert illicitly obtained resources into cryptocurrencies, followed by the challenging task of effectively reintegrating them into the economy. A detailed analysis of these stages provides a deeper understanding of the dynamics involved in the money laundering web and its

⁴ In Brazil, the body responsible for monitoring suspicious transactions is the COAF. The entity responsible for gathering the necessary evidence to bring the case to trial is the Public Prosecutor's Office or the relevant oversight agency (Halo, 2010).

Figure 1. The game in extensive form with incomplete information

Source: Author's own elaboration using the open-source software Gambit.

implications on the economic landscape. At the start of the process, Company Z transfers resources obtained through illicit activities to the Exchange to conceal them via cryptocurrency purchases. The transfer can be either through a Bitcoin ATM or by sending remittances to the Exchange in fiat currency. If the remittances are successfully converted into cryptocurrencies by the Exchange, Company Z can proceed with the money laundering process.

Now, to the game: When Company Z sends legitimate money, the outcome is always neutral (0, 0, 0), as there are no associated risks. In the case of sending dirty money, the game becomes more complex. The "nature player" comes into play to represent the uncertainty about the interception of the resources by the authorities. If the Regulator adopts a stringent approach, nature decides whether the money will be intercepted with an 80% probability (8/10) or not intercepted with a 20% probability (2/10). If the money is intercepted, there are two possibilities: the Regulator may obtain evidence (3:1) or not, to effectively bring the case to court. If evidence is obtained, leading to conviction, the payoffs are (-1, 1, 1), where Company Z is penalized (-1), and the Regulator and Judiciary receive benefits (1) for their effectiveness in monitoring and the judicial process. In the case where evidence is sufficient to open a judicial process and Company Z escapes conviction, the payoffs are (1, -1, -1), with Company Z benefiting from the "in dubio pro reo" condition, while the Regulator and Judiciary are penalized for failing to obtain sufficient evidence and consequently not securing the

criminals' conviction. If Company Z, however, escapes without sufficient evidence to open a judicial process, the payoffs are (1, -2, 0), where Company Z benefits (1) from impunity (in dubio), the Regulator suffers a significant penalty (-2) for failing to obtain evidence in a stringent system, while the Judiciary remains unaffected (0). In this case of interception without conclusive evidence to justify a judicial process, Company Z receives a payoff (reward) of 1, as, in the worst-case scenario, Company Z is released due to the judge's "in dubio" condition, and the remittances from the illegal act are returned. As Pekelman (Halo, 2010) notes, "the state bears not only the burden of proving that the individual committed the crime but also the responsibility to eliminate any doubt about the occurrence of the criminal acts." If the money is not intercepted, the payoffs are (1, -2, 0), with Company Z benefiting (1) (in dubio), and the Regulator suffering a higher penalty (-2) due to failure in interception under a stringent system, while the Judiciary remains unaffected (0).

If the Regulator adopts a lenient approach, the probability of interception by nature is 50% (1/2). If the money is intercepted, the Regulator may again obtain evidence (3:1) or not. With evidence, conviction results in payoffs of (-1, 2, 1), where Company Z is penalized (-1), the Regulator receives a higher benefit (2) for the additional difficulty in a lenient regime, and the Judiciary receives a benefit (1). In the case of impunity, the payoffs are (-1, 1, 1), suggesting that even without conviction, Company Z still faces a penalty, possibly due to operational

costs or indirect risks, and even worsened reputation, besides not being able to send resources even under a lenient regime, while the Regulator and Judiciary are rewarded for their continued effort and involvement. The Regulator, in a lenient regime, can still bring the case to court and the Judiciary receives a benefit (1) as it might be rewarded for efforts or could use the case failure to increase court financing. If the money is intercepted but there is insufficient evidence to bring the criminals to trial, the payoffs are (1, -1, 0), where Company Z benefits (1) (in dubio, and possibly recovering the intercepted resources), the Regulator is penalized (-1) for failing to obtain evidence, and the Judiciary remains unaffected (0). If the money is not intercepted, the payoffs are (1, -1, 0), with Company Z benefiting (1) (in dubio), the Regulator penalized (-1) for failure in interception, and the Judiciary neutral (0).

This dynamic reflects the complexity of money laundering operations and the challenges faced by authorities in attempting to intercept and punish such activities. As Moura and Lima (2019) highlight, it is crucial that judicial and law enforcement authorities have the penal legislation, specifically the Money Laundering Law, to effectively combat these crimes. Until

specific legislation is established to regulate and monitor all transactions in the cryptocurrency market, authorities must rely on existing laws to prevent impunity. The detailed analysis of this game emphasizes the importance of effective monitoring strategies and the need for a robust judicial system to deal with money laundering. The introduction of the "nature player" to represent the uncertainty of interception adds a crucial layer of realism to the model, illustrating the challenges faced by authorities in combating these economic crimes.

In this game, there are 20 mixed-strategy Nash equilibria, as described in Table 1.

Analyzing the Nash equilibria from the provided table, it is evident that the Regulator has no incentives to adopt a stringent approach in combating money laundering. In all identified Nash equilibria, the Regulator chooses to be lenient, suggesting minimal effort in addressing money laundering.

After refining the Nash equilibria, we find the equilibrium $((1/2, 1/2), (0, 0, 1, 0), (1/2, 1/2))$. This equilibrium indicates that, given the incentives of the game, Company Z will attempt to launder money half of the time, while the Regulator will choose to be lenient and make minimal efforts to obtain evidence, and the

Table 1. Nash Equilibria at the Cryptolauding Game

#	01:01	01:02	2:11*	2:12*	2:2*1	2:2*2	03:01	03:02
1	0.000	1.000	0.000	1.000	1.000	0.000	0.530	0.470
2	0.220	0.780	0.000	1.000	1.000	0.000	0.380	0.620
3	0.520	0.480	0.000	1.000	1.000	0.000	0.530	0.470
4	0.545	0.455	0.000	1.000	1.000	0.000	0.420	0.580
5	0.555	0.445	0.000	1.000	1.000	0.000	0.530	0.470
6	0.090	0.910	0.000	1.000	1.000	0.000	0.910	0.090
7	0.535	0.465	0.000	1.000	1.000	0.000	0.330	0.670
8	0.630	0.370	0.000	1.000	1.000	0.000	0.800	0.200
9	0.505	0.495	0.000	1.000	1.000	0.000	0.070	0.930
10	0.580	0.420	0.000	1.000	1.000	0.000	0.770	0.230
11	0.480	0.520	0.000	1.000	1.000	0.000	0.160	0.840
12	0.490	0.510	0.000	1.000	1.000	0.000	0.910	0.090
13	0.500	0.500	0.000	1.000	1.000	0.000	0.490	0.510
14	0.260	0.740	0.000	1.000	1.000	0.000	0.500	0.500
15	0.380	0.620	0.000	1.000	1.000	0.000	0.460	0.540
16	0.585	0.415	0.000	1.000	1.000	0.000	0.830	0.170
17	0.120	0.880	0.000	1.000	1.000	0.000	0.630	0.370
18	0.740	0.260	0.000	1.000	1.000	0.000	0.800	0.200
19	0.300	0.700	0.000	1.000	1.000	0.000	0.850	0.150
20	0.410	0.590	0.000	1.000	1.000	0.000	0.540	0.460

Source: Author's own elaboration using the open-source software Gambit.

Judiciary will convict in half of the cases. In this scenario, it is expected that 25% of the total money from Company Z will be successfully laundered, as half of it is legitimate and half will be attempted to be laundered. Of this half that will be attempted to be laundered, half will succeed. Therefore, Company Z will, on average, retain 75% of the initial volume of resources, now entirely clean, which can be used within the financial system for paying bills, employees, and taxes.

Finally, this pattern of incentives suggests that the Regulator's lenient strategy and the uncertainty of interception create a favorable scenario for money laundering, where Company Z will continue to attempt money laundering, knowing that the regulatory oversight will not be maximally stringent. However, it is not worthwhile for the Regulator to be excessively strict in combating money laundering through cryptocurrencies, as imposing too high a cost on the sector could ultimately lead to its demise. In doing so, all the innovation that could emerge from cryptocurrencies and benefit society over time would be stifled before it ever has the chance to come to light.

4. Conclusion

In this study, we developed a mathematical model using Game Theory to understand the key choices made by governments and criminals, considering a scenario in which cryptocurrencies emerge as central tools in concealing illicit resources. The sophisticated practice of money laundering, utilizing cryptocurrencies, presents new dilemmas to regulatory bodies and challenges traditional enforcement structures. Our goal was to analyze these complex dynamics and explore the possible strategies and incentives of the involved agents.

The payoff analysis demonstrated that, in the absence of stringent regulation, incentives favor the illicit actions of Company Z. The game results reveal that, at the refined equilibrium $(1/2, 1/2), (0, 0, 1, 0), (1/2, 1/2)$, Company Z launders only half of the money, while the Regulator operates with minimal effort, and the Judiciary convict's half of the time. However, while this highlights the challenges posed by insufficient oversight, imposing overly strict regulations may inadvertently stifle the innovation that cryptocurrencies offer.

As Montenegro (2020) suggests, although unregulated exchanges can compromise the integrity of the financial system, excessive regulation could suppress the innovative potential of cryptocurrencies. The risk is that well-intentioned regulations could push out legitimate actors, hamper technological development, and deprive markets of the efficiencies and opportunities that cryptocurrencies provide. Over-regulation may, in effect, kill the market before it can fully realize its benefits for global commerce.

The limitations of this work include the simplification of real-world dynamics in the game model and the need for more detailed data on money laundering operations. Future studies could develop more complex models, incorporating additional variables and different regulatory scenarios. Furthermore, it would be valuable to investigate how new technologies, and financial innovations could influence both money laundering strategies and the overall impact of regulation.

In conclusion, while some degree of regulation is necessary to combat illicit activities, it is essential to strike a careful balance. Overly rigorous enforcement could undermine the economic benefits of cryptocurrencies, restricting their ability to revolutionize markets. Instead of focusing solely on stringent regulation, governments should consider frameworks that encourage innovation while addressing key risks. A collaborative approach, with flexible policies that adapt to technological advancements, will ensure that cryptocurrencies can flourish without becoming tools for illicit activities.

Analyzing the Nash equilibria from the provided table, it is evident that the Regulator has no incentives to adopt a stringent approach in combating money laundering. In all identified Nash equilibria, the Regulator chooses to be lenient, suggesting minimal effort in addressing money laundering.

After refining the Nash equilibria, we find the equilibrium $((1/2, 1/2), (0, 0, 1, 0), (1/2, 1/2))$. This equilibrium indicates that, given the incentives of the game, Company Z will attempt to launder money half of the time, while the Regulator will choose to be lenient and make minimal efforts to obtain evidence, and the Judiciary will convict in half of the cases. In this scenario, it is expected that 25% of the total money from Company Z will be successfully laundered, as half of it is legitimate and half will be

attempted to be laundered. Of this half that will be attempted to be laundered, half will succeed. Therefore, Company Z will, on average, retain 75% of the initial volume of resources, now entirely clean, which can be used within the financial system for paying bills, employees, and taxes.

Finally, this pattern of incentives suggests that the Regulator's lenient strategy and the uncertainty of interception create a favorable scenario for money laundering, where Company

Z will continue to attempt money laundering, knowing that the regulatory oversight will not be maximally stringent. However, it is not worthwhile for the Regulator to be excessively strict in combating money laundering through cryptocurrencies, as imposing too high a cost on the sector could ultimately lead to its demise. In doing so, all the innovation that could emerge from cryptocurrencies and benefit society over time would be stifled before it ever has the chance to come to light.

References

- Agredano, A. B. & Lanau, A. O. (2022). Research guide on money laundering using cryptocurrencies.
- Andrade, M. D. de. (2017). Legal treatment of cryptocurrencies: the dynamics of bitcoins and the crime of money laundering. *Brazilian Journal of Public Policies*, 7.
- Baltrusaitis, J. (2021, October 5). Over 10,000 Bitcoin ATMs installed globally in 2021 as demand for crypto surges. *Finbold*. <https://finbold.com/over-10000-bitcoin-atms-installed-globally-in-2021-as-demand-for-crypto-surges/>
- Brazil. (n.d.). Law No. 9,613, of March 3, 1998. Retrieved September 29, 2024. https://www.planalto.gov.br/ccivil_03/leis/l9613.htm
- Brazil. Federal Revenue Service of Brazil. (2019, May 7). Normative Instruction RFB No. 1888, of May 3, 2019. *Diário Oficial da União* (DOU), section 1, page 14. <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592>
- Brazil. Financial Activities Control Council (COAF). (2020). *Money laundering: a global problem*. <https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/cartilha-lavagem-de-dinheiro-um-problema-mundial.pdf/view>
- Bueno, T. (2020). *Bitcoin and Money Laundering Crimes* (1st ed.). Campo Grande: Contemplar.
- Castro, V. C. (2023). *Money laundering and cryptocurrencies: An analysis of the penalty increase clause regarding the use of crypto assets in light of the Federal Constitution and new challenges to criminal intervention* (Master's thesis). Instituto Brasiliense de Direito Público, Brasília, DF. https://repositorio.idp.edu.br/bitstream/123456789/4934/3/Disserta%C3%A7%C3%A3o_VICTOR%20CHEBLI%20DE%20CASTRO_Mestrado_2023.pdf
- Forbes Money. (2023, November 21). Changpeng Zhao pleads guilty to money laundering and will leave Binance. *Forbes Brazil*. <https://forbes.com.br/forbes-money/2023/11/changpeng-zhao-declara-se-culpado-de-lavagem-de-dinheiro-e-deixara-a-binance/>
- Garg, N., Seth, S., Rastogi, N., Kumar, R., Gupta, V., & Rawat, S. S. (2022). Crowdfunding using Blockchain Technology: A Review. *Global Journal of Innovative and Emerging Technologies*, 1(2), 8-14. <http://iet.adrs.net/index.php/iet/article/view/9>
- rauer, K., Jardine, E., Leosz, E., & Updegrave, H. (2023). *The 2023 Crypto Crime Report*. Chainalysis. https://hkibfa.io/wp-content/uploads/2023/02/Crypto_Crime_Report_2023.pdf
- Grzywotz, J. (2019). *Virtual Cryptocurrencies and Money Laundering*. Berlin: Duncker & Humblot.
- Halo, P. (2010, December 29). *Administrative improbity due to illicit enrichment and money laundering; considered in light of game theory*. DireitoNet. <https://www.direitonet.com.br/artigos/exibir/6246/Improbidade-administrativa-por-enriquecimento-ilicito-e-lavagem-de-dinheiro-considerados-a-luz-da-teoria-dos-jogos>
- Hofert, E. (2019). *Regulating virtual currencies* (IMFS Working Paper No. 130). Institute for Monetary and Financial Stability. <https://ideas.repec.org/p/zbw/imfswp/130.html>
- Horchel, C. (2023). Cryptocurrencies as parallel currency: Notes between financial freedom and (lack of) state control in the fight against money laundering. *Brazilian Journal of Police Sciences*, 14(11). <https://www.redalyc.org/articulo.oa?id=673473467008>
- Montenegro, G. A. de O. (2020). Cryptocurrencies and police investigation: Challenges and solutions. *Brazilian Journal of Police Sciences*, 11(3), 183-230. <http://dspace.mj.gov.br/handle/1/7861>
- Morais, F., & Falcão, R. (2022, November 29). The regulation of cryptocurrencies as a money laundering prevention tool. *CGU Technical Notebooks*, 110-134.
- Moura, J. S. & Lima, S. S. Q. (2019). Analysis of the possibility of applying the money laundering law in the Bitcoin market.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. <https://bitcoin.org/bitcoin.pdf>

- Nieto, J. (2023, October 19). Denis Katana, the biggest hacker arrested in Spain, laundered Russian mafia funds with cryptocurrencies. *El Español*. https://www.lespanol.com/valencia/20231019/denis-katana-mayor-hacker-detenido-espana-blanqueo-fondos-mafia-rusa-criptomonedas/802920066_0.html
- Saadat, M. N., Halim, S. A., Osman, H., Nassr, R. M., & Zuhairi, M. F. (2019). Blockchain-based crowdfunding systems. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(1), 409-413. <https://doi.org/10.11591/ijeecs.v15.i1.pp409-413>
- Santana, H. L. de S., & Moraes, F. A. (2019). Regulação das criptomoedas: Política anti-lavagem de dinheiro. *Revista Interdisciplinar de Marketing*, 1(22). <https://doi.org/10.21902/Revrma.v1i22.3959>
- Ulrich, F. (2014). *Bitcoin - The digital currency*. Ludwig Von Mises Institute Brazil. <https://mises.org.br/livros/91/bitcoin-a-moeda-na-era-digital>

About the authors

Iagor Matos Rodrigues

Undergraduate Student in Economics at the Catholic University of Brasília
<https://orcid.org/0009-0001-9739-694X>

Ryan Hendryk Pereira de Almeida

Undergraduate Student in Economics at the Catholic University of Brasília.
<https://orcid.org/0009-0004-9769-2409>

Matheus Silva de Paiva

Bachelor in Economics from the Federal University of Uberlândia (2013), Master in Economics from the Federal University of Uberlândia (2015), and Ph.D. in Economics from the University of Brasília (2018). Currently, he is the Coordinator and Professor of the Bachelor's Degree in Economics at the Catholic University of Brasília (UCB) and a Permanent Professor in the Master's Program in Governance, Technology, and Innovation (MGTI/UCB) and the Graduate Program in Business Economics (PPGE/UCB).
E-mail: matheus.paiva@p.ucb.br
<https://orcid.org/0000-0001-9882-1496>