İSTANBUL UNIVERSITY PRESS

Acta Infologica,
ACIN 2025, 9 (2): 562–579

https://doi.org/10.26650/acin.1598844
Submitted: 09.12.2024
Revision Requested: 01.10.2025
Last Revision Received: 04.10.2025
Accepted: 15.11.2025
Published Online 20.11.2025

Acta Infologica

Research Article

Open Access

Challenges and New Strategies Faced by Financial Intelligence Units in Monitoring Cryptocurrency Transactions

Cihan Ünal [1] & Hakan Yıldırım [2]

[1] Hacettepe University, Başkent Organized Industrial Zone, Technical Sciences Vocational School, Department of Computer Programming, Ankara, Türkiye
[2] Non-affiliated, Ankara-Türkiye

Abstract Globally and in Turkey, financial intelligence units (FIUs) face various complex challenges when monitoring cryptocurrency transactions. In addition to the high volume and speed of transactions, the anonymity provided by cryptocurrencies and decentralized finance platforms makes it difficult to detect suspicious activities. Anonymity and decentralization conceal the identities of transacting parties, complicating FIUs' efforts to track illegal activities. This complexity is further amplified in international transactions due to discrepancies in regulatory frameworks across countries and data protection laws.

Criminal organizations worldwide and in Turkey utilize advanced methods in money laundering. Moreover, as transaction volumes increase, so do false positive alerts, which strain the analytical capacities of FIUs. In response to these challenges, FIUs need to invest in advanced technologies, such as artificial intelligence (AI), machine learning (ML), big data analytics, and blockchain (BC) forensics. However, respecting individual privacy rights remains a critical balance to be carefully managed in the application of these technologies. This study examines the challenges faced by FIUs in tracking and preventing illicit proceeds despite the growing use of BC-based cryptocurrencies and the measures required to address these challenges.

Keywords Cryptocurrencies · Financial Intelligence · BC · Illicit Proceeds · DeFi.

Citation: Ünal, C. & Yıldırım, H. (2025). Challenges and New Strategies Faced by Financial Intelligence Units in Monitoring Cryptocurrency Transactions. *Acta Infologica*, *9*(2), 562-579. https://doi.org/10.26650/acin.1598844

Corresponding author: Cihan Ünal cihan.unal@hacettepe.edu.tr

Introduction

Cryptocurrencies and DeFi platforms have fundamentally altered the dynamics of the global financial ecosystem, creating substantial opportunities for individuals and businesses while raising significant regulatory and security concerns. The anonymity and decentralization offered by digital assets provide users with freedom and privacy, but these features also create a suitable environment for illegal activities such as money laundering, terrorism financing, and tax evasion. Consequently, FIUs worldwide, including in Türkiye, play a strategically important role in preventing and monitoring such illegal transactions (Amler et al., 2021).

The growing complexity of financial systems necessitates robust mechanisms to prevent illicit activities, including money laundering, terrorism financing, and noncompliance in customer verification. These processes, collectively referred to in this study as the Financial Crime Prevention Framework (FCPF), encompass Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT), and Know Your Customer (KYC) practices.

The Financial Action Task Force (FATF) is an intergovernmental organization established in 1989 by the G7 countries in 1989 to combat money laundering, counter the financing of terrorism, and address other threats to the integrity of the global financial system. The FATF, which is headquartered in Paris, France, develops and promotes international standards aimed at preventing illegal financial activities. The FATF establishes global recommendations to address money laundering and terrorism financing, widely known as the FATF Recommendations. These standards serve as a global framework for combating financial crimes. The FATF conducts peer reviews of member countries to assess their adherence to these standards and issues lists, such as the "gray list" and "blacklist," to highlight countries with inadequate measures against money laundering and terrorism financing. Additionally, the FATF actively addresses emerging challenges, such as the misuse of cryptocurrencies and DeFi platforms for illicit purposes (Chow & Wong, 2020).

The FATF plays a critical role in shaping national and international financial regulations by encouraging member countries to align their legal frameworks and enforcement practices with its standards. A significant measure introduced by the FATF is the Travel Rule (TR), which mandates that financial institutions share specific information about the sender and receiver of transactions. This regulation enhances transparency and aims to prevent illicit activities, such as money laundering and financing of terrorism. However, FIUs face complex challenges in implementing these standards, spanning both technological and legal domains. The high volume and speed of cryptocurrency transactions make their technical monitoring challenging. Innovative technologies, such as BC and DeFi platforms, which facilitate anonymity, further complicate the tracking of suspicious activities. These challenges are exacerbated by differences in legal frameworks between countries and data protection regulations, which significantly limit the ability of FIUs to effectively monitor and enforce CFT measures.

If cryptocurrencies were only produced and used within a single country, FIU monitoring would be relatively easier, even with decentralized structures like DeFi. For example, because the initial acquisition of these assets generally occurs through an intermediary financial institution, this process can be tracked. Similarly, the digital traces left during the spending or conversion of cryptocurrencies into other assets make it possible to follow the transactions. However, three primary issues arise in this regard (Ibrahim, 2024).

First, due to the inherently anonymous nature of cryptocurrencies, tracking all accounts and transactions belonging to a person over a wide time frame requires FIUs to have an unlimited big data analytics capacity with extensive computational power. However, such a monitoring approach could conflict with national

and international data protection laws (e.g., the Turkish Personal Data Protection Law) and may become a generalized surveillance practice (www.mevzuat.gov.tr).

The second issue is that the acquisition and spending of illicit proceeds usually occur in an international context. The infrastructure for data sharing between countries is limited, and international cooperation is not always sufficiently effective. Countries in different political blocs or those temporarily unwilling to cooperate can create significant obstacles in this process.

The third issue is the continuous evolution of innovative techniques used in illegal activities. Tools such as mixing services, off-chain transactions, and privacy-focused cryptocurrencies are becoming increasingly complex in concealing illicit funds' origins (Kumar et al., 2024).

Despite these issues, emerging technologies offer new opportunities. Tools such as AI, ML, metadata analytics, and BC forensics can enhance the FIUs' monitoring capabilities. Additionally, methods such as anonymized data analytics can alleviate concerns related to personal data protection. New approaches developed in STR can also play an effective role in these processes (Camino et al., 2017).

This article comprehensively examines the complex challenges faced by FIUs and the new strategies that could be developed to overcome them. This study highlights the importance of international cooperation, coordination with the private sector, and investments in advanced technologies for the security of the digital economy, drawing insights from global and Turkish practices. The article also discusses how to make regulations on cryptocurrency transactions more effective and which legal and technical innovations should be adopted in combating financial crimes.

This study specifically aims to:

- Identify the major technological, legal, and ethical challenges FIUs face in monitoring cryptocurrency transactions.
- Analyze global and national case studies (USA, EU, Singapore, Türkiye) to compare monitoring strategies and regulatory frameworks.
- Evaluate the role of advanced technologies, such as artificial intelligence, machine learning, big data analytics, and blockchain forensics, in overcoming monitoring challenges.
- Propose practical recommendations for policymakers and FIUs, distinguishing between short- and long-term actions while maintaining a balance between security and privacy.

The increasing complexity of monitoring processes highlights the need for a structured theoretical framework, which forms the foundation of the following section.

Theoretical Framework

Methodology

This study adopts a qualitative research approach to evaluate the challenges faced by financial intelligence units in monitoring cryptocurrency transactions and the strategies developed to address these challenges. The methodology is designed to encompass both theoretical and practical aspects.

Research Design

Literature Review: This study thoroughly examines reports and guidelines issued by international regulatory bodies, such as the FATF and the Turkish Financial Crimes Investigation Board (MASAK).

For instance: FATF's TR and its implementation examples are analyzed (Nance, 2018; Utkina et al., 2023). MASAK's obligations imposed on cryptocurrency service providers in 2021 are reviewed (Özgenç, 2021). Additionally, academic literature, industry reports, and studies on BC analytics are considered (Kumar et al., 2024; Rehman et al., 2020).

Analysis of Case Studies

FIU practices in different regions are analyzed, focusing on challenges faced and outcomes achieved. Examples include: FinCEN's use of BC analytics tools and STRICT reporting in the United States (Lidstone, 2023).

The requirements of the European Union for cryptocurrency service providers under the 5th and 6th Anti-Money Laundering Directives (Lidstone, 2023).

Methods of Data Collection

Secondary Data Analysis: The study relies on publicly available data sources, including international reports and regulatory guidelines (Hileman & Rauchs, 2017; Lagerwaard, 2024).

Analysis of the Technological Tools

FIUs have examined case studies on the use of BC analytics, AI, and big data technologies (Camino et al., 2017; Saadah & Ahmad Whafa, 2020).

For example, tools such as Chainalysis and CipherTrace are evaluated for their capacity to monitor cryptocurrency transactions.

Method of Data Analysis

Content Analysis: Frequently discussed concepts in the literature, such as anonymity, decentralization, and money laundering techniques, are thematically classified (Panevski et al., 2021). This classification aims to identify the challenges and opportunities for FIUs.

Comparative Analysis of the Case Studies

The regulatory frameworks and FIU practices in countries such as the United States, the EU, Singapore, and Türkiye are compared (Chow & Wong, 2020; Özgenç, 2021). This analysis highlights the strengths and weaknesses of the approaches of different regions.

Ethical Approach

Throughout the study, all data were obtained from publicly accessible sources, ensuring full respect for individuals' privacy rights. The trustworthiness of the cited sources supports the reliability and credibility of the data (Bernsdorff, 2014; Nettesheim, 2017). This methodology provides a solid foundation for comprehensively evaluating FIUs' challenges in monitoring cryptocurrency transactions. By combining theoretical and practical perspectives, this study ensures the reliability and applicability of its findings.

Challenges and Threats in Cryptocurrency Monitoring

Cryptocurrencies are digital or virtual assets that are supported by the BC technology. They operate in a distributed system that allows transactions without relying on a central authority or financial institution. The most common type of cryptocurrency is digital currency; however, other types, such as tokenized assets, stablecoins, and non-fungible tokens, also exist (CoinDesk, 2018).

Cryptocurrencies hold a prominent position in the financial ecosystem. Owing to their decentralized nature, they are not under the control of a single authority and are validated by a global network through "distributed ledger technologies," such as BC. Although transactions are traceable, the concealment of user identities increases the risk of their use in illegal activities. Cryptocurrencies enable global transactions without geographical limitations, complicating international regulatory and monitoring efforts. Transactions are faster and less costly than the traditional financial system. Additionally, while transactions on the BC are generally accessible and transparent, this transparency is balanced with user privacy (Rehman et al., 2020). Cryptocurrencies reduce the effectiveness of traditional methods of monitoring financial intelligence units. Legal and regulatory gaps, particularly the varying legal definitions of cryptocurrencies between countries, complicate international cooperation and illicit proceeds tracking. Anonymity poses a challenge in concealing illicit proceeds, and privacy-focused cryptocurrencies, such as Monero, can be used in this process. In addition, technologies such as mixing and tumbling services, which complicate transaction tracking, require investment. The borderless nature of cryptocurrencies highlights the importance of international cooperation; however, regulatory inconsistencies hinder this cooperation. Stablecoins, DeFi products, and tokenized assets also stand out as new financial tools that could be used in money laundering (Amler et al., 2021). Beyond their financial use cases, the underlying technology of DeFi introduces new layers of programmability, composability, and automation, further complicating regulatory oversight and monitoring efforts (Auer et al., 2024).

Cryptocurrencies reduce the effectiveness of traditional FIU monitoring methods. This challenge arises primarily due to the anonymity and decentralization offered by cryptocurrencies, which make identifying transacting parties and tracking illicit proceeds difficult. As outlined in Table 1, anonymity and decentralization create significant barriers to the ability of FIUs to detect and prevent illegal activities. Monero is a privacy-focused cryptocurrency that can completely conceal user identities and transaction details. With features such as RingCT, ring signatures, and stealth addresses, Monero ensures anonymity for its users by hiding the sender, receiver, and transaction amounts. While it is a popular choice for individuals seeking privacy, it also poses challenges for regulatory authorities because of its robust privacy measures.

In addition to these technical barriers, legal and regulatory inconsistencies across jurisdictions hinder effective international cooperation. Table 1 highlights legal incompatibilities as a major obstacle, where regulatory framework differences and the lack of standardized data-sharing protocols limit cross-border transaction tracking. This issue is particularly relevant because most illicit cryptocurrency activities involve international transactions.

FIUs also face technological capacity limitations, as traditional monitoring tools are insufficient for processing the large volumes of data generated by cryptocurrency transactions. Advanced big data analytics and artificial intelligence (AI) tools are required for real-time monitoring and analysis. Table 1 identifies these technological constraints as another critical challenge, underlining the need for substantial investments in modern analytics systems.

Finally, the balance between privacy rights and monitoring needs remains a contentious issue. Data protection laws, such as the General Data Protection Regulation (GDPR) in the EU or KVKK in Türkiye, impose restrictions on accessing user information, further complicating the efforts of FIUs. As shown in Table 1, privacy and ethical barriers represent a key concern that FIUs must navigate carefully while ensuring compliance with both national and international regulations.

While cryptocurrencies present innovative opportunities for individual and institutional users, they also challenge traditional financial systems. At the same time, they create significant challenges for FIUs. In addition to technological innovations, monitoring and regulating these assets require comprehensive policies and cooperation at both the national and international levels. These factors play a crucial role in the development of FIUs' cryptocurrency strategies (Financial Intelligence Unit, 2020).

Table 1

Challenges faced by FIUs and their causes

Challenges	Cause
Anonymity and Decentralization	Concealment of user identities and lack of central control in cryptocurrency transactions
Legal Incompatibilities	Differences in regulatory frameworks and lack of data sharing between countries
Limitations in Technological and Personnel Capacity	Lack of access to big data analytics and artificial intelligence tools and insufficient information technology personnel.
Privacy and ethical barriers	Conflicts between Data Protection Laws and Monitoring Needs

Source: Panevski et al. (2021)

To combat cryptocurrency transactions, financial monitoring units use techniques such as big data analytics and BC forensics to detect suspicious activities. However, this process faces severe limitations in terms of both technological infrastructure and human resources. Recent systematic reviews indicate that blockchain forensics is rapidly evolving, with diverse techniques, applications, and challenges being documented, yet substantial gaps remain in scalability and cross-border applicability (Atlam et al., 2024). The complex nature of cryptotransactions and the rapidly growing volume of data strain the existing capacities of financial monitoring units (Ibrahim, 2019).

The cryptocurrency ecosystem generates thousands of transactions per second, which generates large amounts of data. Financial monitoring units need advanced technologies to analyze these data and detect illegal transactions. Crypto transactions not only on BC networks but also across different ecosystems, such as DeFi platforms and cross-chain transactions, add an additional burden on processing capacity. Real-time analysis requires large-scale data processing systems, but traditional data processing tools are insufficient for large-scale transactions. Additionally, establishing and maintaining advanced analytical infrastructures requires significant costs, and constant updates are required for cloud-based solutions used for data storage, analysis, and visualization (Atzei et al., 2018).

Although transactions are transparent due to the BC's publicly accessible records, interpreting these transactions and detecting illegal activities is a complex process. Analyzing BC transactions requires expertise in cryptography, data analytics, and network analysis, and finding competent personnel in these fields poses a challenge for financial monitoring units. Some BC networks use advanced technologies to encrypt or anonymize transactions, making it difficult to detect illegal activities. Transactions occurring across multiple networks carry risks such as data loss and monitoring interruptions, necessitating the use of more advanced tools and protocols in BC forensics.

Many financial monitoring units use outdated systems that are insufficient for modern big data analytics and BC technologies, limiting the speed and accuracy of large-scale data analysis. AI and ML offer significant potential for anomaly detection and suspicious transaction analysis, but their effective use requires high

computing power and expertise. The lack of data-sharing standards among financial monitoring units in different countries further complicates cross-border transaction tracking (Saadah & Ahmad Whafa, 2020).

Financial monitoring units can overcome data management and technological limitations using advanced analytical tools. BC analysis tools are effective for identifying suspicious transactions and mapping illegal networks. Cloud technologies can help increase large-scale data processing capacities and optimize data storage and processing workflows. By partnering with BC analytics companies and technology providers, financial monitoring units can gain access to the latest tools. In addition, international cooperation programs can be used to train personnel on BC technologies and big data analytics. Investments in artificial intelligence (AI)-based systems and natural language processing technologies can improve the speed and accuracy of big data analytics (Murthy et al., 2020).

Data management and technological limitations are critical factors affecting the ability of financial monitoring units to track cryptocurrency transactions. Investments in big data analytics, BC forensics, and artificial intelligence-based systems can help address these challenges. However, these solutions will be effective only when strong technological infrastructure and expertise support them. The optimization of resources through cooperation at both local and international levels plays an important role in ensuring the security of the digital economy.

FIUs face unique challenges due to the high volume and speed of cryptocurrency transactions. The electronic money and cryptocurrency ecosystems are characterized by high-frequency transactions conducted in digital environments, which requires effective solutions for detecting and monitoring suspicious activities (Lal et al., 2021).

Some special tools can be used for cryptocurrency monitoring. For example;

Chainalysis: This is a BC analysis tool that helps in tracking and linking cryptocurrency transactions, identifying wallet addresses associated with criminal activity, and providing data for investigations. Law enforcement agencies and FIUs worldwide widely use it. Elliptic: Another major BC analytics provider that offers insights into cryptocurrency flows, helping to detect money laundering, terrorism financing, and other illegal activities. Elliptic focuses on risk scoring for cryptotransactions and provides solutions tailored for compliance and law enforcement.

CipherTrace: Known for its robust cryptocurrency intelligence capabilities, CipherTrace helps trace cryptocurrency flows, ensures FCPF compliance, and identifies transactions associated with illicit activities, including those using privacy-focused cryptocurrencies.

Cryptocurrency transfers usually occur in real-time or near-real-time, increasing monitoring load and data intensity, thereby straining financial intelligence units' storage, analysis, and processing power. This challenge is even more evident in DeFi platforms, where transactions occur without central control.

Timing is critical in cryptocurrency transactions. The need to process real-time data flows and make quick decisions causes existing infrastructures to fall short in terms of speed and scalability.

High scalability is required in the systems of financial intelligence units due to the increasing transaction volume. The variety of data from different platforms and the infrastructure for large-scale data processing require significant technical and financial resources. The high number of transactions occurring on the BC each second increases the need for complex algorithms to meaningfully analyze these data (Chaudhry & Yousaf, 2018).

FIUs must focus on advanced analytical tools, BC monitoring platforms, cloud-based infrastructures, and application programming interface (API)-based integrations to cope with these challenges. AI and ML algorithms can prioritize illicit activities within large volumes of data, while BC monitoring tools can be used to analyze transactions.

Cloud computing technologies provide a scalable solution to meet large-scale data processing and storage needs. API connections enable the instant transmission of transaction data to FI units. The volume and speed of cryptocurrency transactions affect not only the technical infrastructure but also the regulatory and operational processes in the financial intelligence units' monitoring procedures.

To process and analyze the high volume of transactions generated by BC networks and DeFi platforms, cryptocurrency monitoring requires advanced technologies. FIUs rely on tools such as BC analytics, AI, and cloud-based systems to effectively detect suspicious activities. BC analytics tools, such as Chainalysis and CipherTrace, are essential for monitoring and analyzing cryptocurrency transactions, as outlined in Table 2. These tools map illegal networks and identify suspicious transaction patterns.

The adoption of AI and ML further enhances the ability of FIUs to detect anomalies in transaction data. FIUs can prioritize high-risk activities and allocate resources efficiently by applying risk-based transaction scoring. Table 2 highlights how AI and ML are employed to accelerate transaction analysis and improve monitoring efforts' accuracy.

Additionally, cloud-based systems play a crucial role in storing and processing large-scale data generated by cryptocurrency transactions. These systems increase data processing capacity and enable real-time analysis of suspicious transaction reports. Table 2 illustrates the importance of cloud-based systems in enhancing data storage and processing workflows, particularly for cross-chain and high-frequency transactions.

Despite these advancements, the implementation of such technologies requires significant investment in infrastructure and skilled personnel. Collaboration with BC analytics companies and technology providers is essential to keep up with the evolving complexity of cryptocurrency ecosystems. The tools and technologies listed in Table 2 provide a roadmap for FIUs to strengthen their monitoring capabilities and adapt to the challenges posed by cryptocurrencies.

Table 2

FIUs' Tools and Technologies for Monitoring Cryptocurrencies

Tool/Platform	Purpose	Example of Use
BC Analytics Tools	Monitoring and analyzing suspicious transactions	Keywords: Chainalysis, Elliptic, CipherTrace
AI and ML	Detecting anomalies and accelerating transaction analysis	Risk-Based Transaction Scoring
Cloud-Based Systems	Big data storage and increased processing speed	Storage and analysis of suspicious transaction reports

Source: Utkina et al. (2023).

As cryptocurrencies create a major shift in the international financial system, financial monitoring units in different countries have developed various strategies to adapt to these new dynamics. Globally, national and international regulations support FIUs in monitoring illicit proceeds and preventing the financing of

terrorism. Evolving technologies and international cooperation frameworks shape the operation of these units (Hileman & Rauchs, 2017).

The approaches and capabilities of FIUs vary significantly across countries due to differences in regulatory frameworks, technological infrastructures, and policy implementations. As shown in Table 3, FIUs in countries such as the United States and Singapore have adopted advanced BC analytics tools and AI technologies, enabling them to monitor cryptocurrency transactions more effectively. For instance, the United States' FinCEN enforces strict FCPF compliance measures, requiring cryptocurrency exchanges to file suspicious activity reports, while also using advanced BC analytics tools.

The 5th and 6th Anti-Money Laundering Directives shape the regulatory landscape in the EU by imposing harmonized standards on member states. However, Table 3 highlights the challenges faced by EU FIUs due to regulatory inconsistencies among member states, which complicates cross-border monitoring efforts despite the establishment of platforms such as the EU FIU Platform (Directive of the European Parliament and of the Council, 2017).

Singapore's Monetary Authority (MAS) and the United Kingdom's National Crime Agency (NCA) serve as examples of how licensing requirements and dedicated crypto crime units can enhance cryptocurrencies' monitoring and regulation. Table 3 underscores the strong international cooperation frameworks implemented by Singapore's MAS, closely aligning with the FATF recommendations.

In contrast, countries such as Türkiye are still expanding their regulatory and technological capacity. MASAK has designated cryptocurrency exchanges as obligated parties, requiring them to comply with FCPF procedures. As summarized in Table 3, MASAK's reliance on BC analysis tools highlights the importance of technology in filling regulatory gaps and combating financial crimes.

The diverse strategies outlined in Table 3 illustrate how regulatory framework differences and technological advancements influence the effectiveness of FIUs worldwide. These variations underscore the need for global coordination and the adoption of standardized practices for combating illicit cryptocurrency transactions.

In the United States, FinCEN plays a leading role in monitoring cryptocurrency transactions. FinCEN enforces FCPF compliance for cryptocurrency exchanges and mandates the filing of suspicious activity reports. It monitors suspicious transactions using the BC analytics tools and AI.

In the EU, the FIU Platform ensures coordination among member countries, while regulatory bodies such as the Anti-Money Laundering Authority (AMLA) enforce FCPF procedures for cryptocurrency service providers under the 5th AML Directive. However, regulatory discrepancies among member states make cryptocurrency monitoring in the EU more complex (Lidstone, 2023).

In Singapore, the MAS (Monetary Authority of Singapore) has implemented a licensing requirement, establishing a structure aligned with FATF standards, and using BC-based monitoring systems and international cooperation, it monitors cryptocurrencies.

In the United Kingdom, the NCA and FCA enforce FCPF compliance for crypto service providers and monitor illegal activities through specialized crypto crime units (Chow & Wong, 2020).

The Financial Action Task Force (FATF) establishes global standards and mandates that cryptocurrency service providers share transaction information under regulations such as the TR, supporting the tracking of illicit fund movements (Nance, 2018).

Table 3

Comparison of Worldwide FIUs

Country/Region	FIU	Regulatory Framework	Technological Tools	Cryptocurrency Policy
USA	FinCEN (Financial Crimes Enforcement Network)	The Bank Secrecy Act (BSA) and AML regulations	BC analytics tools and AI	Cryptoexchanges subject to FCPF, mandatory suspicious activity reporting
EU	FIU Platform, AMLA (effective 2024)	5th and 6th AML directives	BC monitoring tools	Harmonized regulations among member states and FATF compliance
Singapore	MAS (Monetary Authority of Singapore)	FCPF regulations and FATF compliance	AI and BC analysis software	Licensing of cryptoplatforms is mandatory, and strong international cooperation is required
United Kingdom	National Crime Agency (NCA), Financial Conduct Authority (FCA)	AML regulations and FCA obligations	BC analysis tools	Cryptoproviders subject to regulation and established special crime unit
Türkiye	MASAK (Financial Crimes Investigation Board in Turkiye)	AML regulations under Law No. 5549	BC analysis tools and STR system	Cryptoexchanges designated as obligated parties and FATF compliance
Australia	AUSTRAC (Australian Transaction Reports and Analysis Center)	AML/CFT Act	BC analytics platforms	Licensed cryptoplatforms and regular reporting of suspicious transactions
Canada	FINTRAC (Financial Transactions and Reports Analysis Center)	FCPF regulations	Big data analytics and BC tools	Licensing Required for Crypto Asset Service Providers

Source: (Lagerwaard, 2024).

MASAK: Türkiye's Financial Intelligence Unit

FIUs around the world adopt various approaches to prevent and monitor illegal activities. Units such as MASAK in Türkiye also benefit from global experiences to enhance their cryptocurrency monitoring capabilities.

FIUs around the world adopt various approaches to prevent and monitor illegal activities. The organizational structures and operational capacities of these institutions differ significantly across countries. Recent comparative research highlights that FIUs tend to cluster into distinct models shaped by regional, political, and legal contexts, with notable differences between Western and post-Soviet countries (McNaughton, 2023). Units such as MASAK in Türkiye also benefit from global experiences to enhance their cryptocurrency monitoring capabilities.

MASAK, the institution playing the most critical role in combating financial crimes in Türkiye, was established in 1996 under the Ministry of Treasury and Finance and is responsible for fighting money laundering, terrorism financing, and other financial crimes. In response to the risks posed by cryptocurrencies, MASAK holds a significant position as both a regulatory and enforcement authority (Özgenç, 2021).

Under Law No. 5549, "Law on the Prevention of Laundering Proceeds of Crime," MASAK conducts financial analysis and research, evaluates suspicious transaction reports, performs regulatory and supervisory duties, and undertakes international cooperation and training activities. Additional measures have been imple-

mented due to the anonymity and decentralization in cryptocurrency transactions, which challenge MASAK's traditional monitoring methods. In 2021, Turkish cryptocurrency exchanges were designated as obligated parties to MASAK, making them responsible for transaction reporting and implementing KYC procedures.

MASAK analyzes the data obtained from cryptocurrency exchanges to detect money laundering and terrorism financing and invests in the Bitcoin Cash (BC) analysis tools. In line with the FATF's international regulations, MASAK also seeks to comply with measures such as the TR to ensure transparency in crossborder cryptocurrency transactions.

However, MASAK faces challenges in cryptocurrency transactions, including anonymity, technological capacity limitations, barriers to international cooperation, and the fact that regulations on cryptocurrencies in Türkiye are still in the developmental stage. Despite these challenges, MASAK has achieved significant success in combating illicit proceeds, increased its effectiveness through national and international collaborations, and progressed in developing BC-based monitoring tools (Ay, 2018).

MASAK is an important actor in ensuring the financial security of Türkiye, aiming to enhance its capacity to combat cryptocurrency-related crimes in the future through stronger legal regulations and technological investments.

The MASAK report highlights the insufficiency of technological investments and the shortage of human resources in this area. Table 4 highlights the insufficient number of IT personnel and total personnel over the years, highlighting MASAK's ongoing challenges in human resource allocation. MASAK faces limitations in accessing advanced analytical tools and AI-based systems. This situation demonstrates a significant disadvantage for the institution compared with other FIUs worldwide. The report emphasizes the need for adequate technological infrastructure to effectively conduct financial monitoring and analysis processes and highlights a shortage of skilled personnel in critical areas such as BC analysis and big data processing. The report indirectly mentions the need for human resources essential for the effective use of technology. As shown in Table 4, MASAK's human resources, particularly IT personnel, have remained limited, emphasizing the importance of increasing capacity in critical areas such as BC analysis and big data processing. Table 4 underlines this issue by presenting the small number of IT personnel over the years, further stressing MASAK's limitations in technological and analytical capacity.

The anonymity and decentralization features offered by cryptocurrencies and DeFi platforms further complicate the efforts of FIUs to monitor and prevent illegal transactions. While these structures create an attractive environment for illegal activities such as money laundering, terrorism financing, and tax evasion, most platforms keep user identity information confidential, making it difficult to link transactions to individuals. The availability of services such as mixing and tumbling, which allow users to conceal transaction traces, further complicates this process. Additionally, data protection laws significantly restrict FIU monitoring activities by limiting access to user identity information. These elements indicate that MASAK's current capacity lags behind global standards.

Table 4

Human resources of MASAK derived from the 2023 annual report.

Year	IT Personnel	Total Personnel
2019	2	225
2020	-	186
2021	-	281

Year	IT Personnel	Total Personnel
2022	-	306
2023	-	362

Source: (https://ms.hmb.gov.tr/uploads/sites/12/2024/04/Faaliyet-Raporu-2023.pdf)

DeFi platforms allow for direct transactions between users without a central authority. This structure complicates financial intelligence units' collection of transaction data. Additionally, because transactions are automated through smart contracts, intervention is limited. These platforms generally do not fall under a specific jurisdiction, which restricts FIUs' supervisory authority.

FIUs use BC analytics tools to analyze links between wallet addresses to address these challenges. Regulatory bodies may develop laws that require decentralized platforms to comply with FCPF procedures. FIUs must specialize in privacy technologies and strengthen international cooperation processes. Regulations such as the TR, recommended by the FATF, also increase transparency by mandating that cryptocurrency service providers share transaction information.

The tracking of illegal transactions is complicated by privacy coins and mixing services. FIUs can focus on using BC analytics tools and ensuring that exchanges supporting privacy coins comply with FCPF procedures. They can also enhance information sharing and develop clearer regulations through collaboration with international organizations (Ibe et al., 2023).

Electronic transaction monitoring systems produce many false positives, which increases the workload of analysts and reduces the speed and accuracy of identifying actual risks. FIUs must maintain a broad scope while making accurate predictions. Focusing on high-risk transactions can reduce workload and improve accuracy. False positive rates can be reduced using AI and ML algorithms. Additionally, it is important to dynamically update the sensitivity settings of algorithms and segment users to enable risk-based evaluation.

AI- and ML-based systems can help FIUs analyze large datasets and detect suspicious transactions. However, the technical expertise and associated costs make implementing these technologies challenging. The transparency of AI models and ethical concerns should also be considered. To ensure accountability, AI-based systems should be made explainable, and AI models should be trained to avoid developing biases (McNaughton, 2023).

Collaboration with the private sector is crucial for tracking illicit proceeds in cryptocurrency transactions. For transaction data and customer information, FIUs should collaborate with cryptocurrency exchanges and digital wallet providers. Lack of legal alignment with decentralized platforms poses a challenge. Therefore, international cooperation mechanisms need to be strengthened.

Public trust and privacy protection are critical in balancing FIU monitoring activities. This balance between security and privacy can be maintained by ensuring transparency and accountability. FIUs must provide proportional oversight by only targeting high-risk transactions. Anonymization techniques and independent audit mechanisms should be used to ensure the privacy of individuals. In this process, AI and ML technologies also contribute to privacy protection (Ijaz et al., 2024).

Building on this theoretical foundation, the study employs a clear methodological approach to evaluate challenges and strategies in practice.

Methodology

This study adopts a qualitative research approach to evaluate the challenges faced by financial intelligence units in monitoring cryptocurrency transactions and the strategies developed to address these challenges. The methodology is designed to encompass both theoretical and practical aspects.

Research Design: A literature review was conducted by examining reports and guidelines issued by international regulatory bodies, such as the Financial Action Task Force (FATF) and the Turkish Financial Crimes Investigation Board (MASAK). In addition, the relevant academic literature, industry reports, and studies on blockchain analytics were analyzed.

Case Study Analysis: The practices of FIUs in different regions (e.g., USA, EU, Singapore, Türkiye) were investigated, with a focus on the challenges they encountered and the outcomes of their monitoring strategies.

Data Collection Methods: Secondary data analysis was performed, drawing primarily on publicly available sources, international reports, and regulatory guidelines.

Technological Tools and Analysis: Case studies on the use of blockchain analytics, artificial intelligence (AI), and big data technologies by FIUs were examined. Tools, such as Chainalysis and CipherTrace, were evaluated for their effectiveness in monitoring cryptocurrency transactions.

Data Analysis Method: Content analysis was employed to thematically classify frequently discussed concepts (e.g., anonymity, decentralization, and money laundering techniques) to identify the challenges and opportunities for FIUs.

Comparative Analysis: The regulatory frameworks and FIU practices in different countries were compared to highlight the strengths and weaknesses across jurisdictions.

Ethical Considerations: All data were obtained from publicly accessible sources with full respect for individual privacy rights and ethical standards.

This methodological approach enables the analysis of both theoretical perspectives and practical applications, which are reflected in the following findings.

Results and Discussion

Monitoring cryptocurrency transactions presents a complex challenge for financial intelligence units. The anonymity and decentralization of cryptocurrencies are fundamental elements that make tracking and preventing illegal activities difficult. Tools such as privacy-focused cryptocurrencies and mixing services add complexity to this process.

Big data analytics, artificial intelligence (AI), and BC forensics are critical for detecting suspicious transactions. However, many FIUs have limited access to these technologies, and the process is further complicated by existing infrastructure deficiencies. Tracking cross-border transactions becomes even more challenging, particularly due to regulatory discrepancies and data-sharing limitations between countries. Without sufficient IT personnel, MASAK cannot use emerging technologies, such as AI and ML, or effectively engage in international collaboration.

The regulatory framework for cryptocurrencies varies across countries, complicating FIUs' coordination efforts. Ethical issues, such as protecting individual privacy, also present a critical balance point in terms of monitoring activities' legitimacy. Criminal organizations continuously develop techniques to conceal illegal

transactions using innovative methods such as mixing services, off-chain transactions, and privacy-focused technologies. Effective solutions are needed to overcome these challenges.

Criminal organizations continuously develop techniques to conceal illegal transactions using innovative methods such as mixing services, off-chain transactions, and privacy-focused technologies. Effective solutions are needed to overcome these challenges. Recent bibliometric analyses also indicate that research on the role of cryptocurrency in financial crime and money laundering is rapidly expanding worldwide, with growing global collaboration in this field (Pramanik et al., 2025)

Another notable issue is the lack of collaboration with the private sector. Insufficient coordination with cryptocurrency exchanges and other private sector entities negatively impacts monitoring processes. In this context, regulations and partnerships that reduce FIU workload are required.

Strengthening the technological infrastructure should be a priority step in addressing these issues. Investments in AI, ML, big data analytics, and BC analytics tools will play a crucial role in detecting and preventing financial crimes. Establishing harmonized regulations for cryptocurrencies at national and international levels can make monitoring processes more effective. The adoption of standards such as the FATF's TR and the development of information-sharing mechanisms are of great importance for monitoring crossborder transactions (Takei & Shudo, 2024).

Balancing anonymity with security is essential to protect individual rights and implement effective methods to detect illegal activities. Encouraging stronger collaboration with the private sector can reduce the workload of FIUs and make processes more effective by enhancing cryptocurrency exchanges' FCPF compliance. The steps taken within this framework can provide a comprehensive solution to FIU challenges.

Some provisions of Law No. 5549, "Law on the Prevention of Laundering Proceeds of Crime," which serves as the legal basis for MASAK's powers, have been annulled by the Constitutional Court. These annulments have led to significant changes in the authority of MASAK and limited the capacity of the institution to conduct certain activities.

The articles annulled by the Constitutional Court on the grounds of violating constitutional principles related to individual rights and freedoms have restricted MASAK's processes for monitoring and processing financial information and personal data. This situation also stands out as a factor affecting the national and international collaborations of MASAK (https://www.resmigazete.gov.tr/eskiler/2023/02/20230214-7.pdf).

The Constitutional Court's ruling can be seen as highly justified, particularly in its assessment that the powers granted to MASAK (Financial Crimes Investigation Board) were "excessive" and "detached from context." These powers posed significant risks of violating both Türkiye's GDPR (KVKK) and fundamental human rights.

Excessive Powers and Detachment from Context: The broad powers granted to MASAK went beyond what was necessary to combat financial crimes, encroaching unnecessarily on individuals' private spheres. Specifically, the authority to extensively monitor and process personal financial data without clear limits created a surveillance mechanism that risks being incompatible with the principles of a democratic legal state.

Violations of the Personal Data Protection Law (KVKK): Türkiye's KVKK outlines principles such as explicit consent, purpose limitation, and proportionality in the processing of personal data. However, the unrestricted powers given to MASAK had the potential to breach these principles by processing data without

adequate safeguards or oversight. The lack of control over the handling of personal financial data posed a significant threat to privacy rights.

Violations of Human Rights: Such sweeping powers risk infringing upon fundamental human rights. The right to respect for private and family life, guaranteed by Article 8 of the ECHR and Article 20 of the Turkish Constitution, was directly at risk. While combating crime is a legitimate state goal, it must not come at the expense of individual freedoms.

Conclusion and Evaluation: The annulment of these powers by the Constitutional Court marks a critical step toward safeguarding individual freedoms and maintaining the democratic boundaries of state authority. While institutions like MASAK undoubtedly require robust powers to effectively fight financial crimes, these powers must be carefully balanced to avoid infringing on personal rights.

Excessive surveillance or overreach in monitoring mechanisms not only undermines individual privacy but also risks eroding public trust and questioning the legitimacy of state oversight. The Constitutional Court's decision underscores the importance of prioritizing individual rights while ensuring that state powers remain within democratic limits. It serves as a crucial reminder of the need for checks and balances in modern governance to uphold the principles of justice and privacy.

In 2021, Türkiye was placed on the Financial Action Task Force (FATF) gray list in 2021 due to shortcomings in combating money laundering and terrorist financing. The effectiveness of the MASAK was a significant focus during this process. Insufficient oversight and enforcement in high-risk areas, such as financial institutions, banks, and cryptocurrency platforms, were highlighted as areas of noncompliance with the FATF standards. Additionally, MASAK's limited capacity to identify and prevent money laundering risks, the lack of deterrent sanctions, and issues with international data sharing were key factors in the decision to greylist Türkiye.

In 2024, Türkiye was removed from the FATF gray list. Authorities achieved this milestone by addressing concerns over the institutional and operational independence of MASAK and restoring confidence in Türkiye's financial monitoring systems. The key improvements included regulating the rapidly growing cryptocurrency sector and resolving deficiencies in financial oversight. To sustain this progress, MASAK strengthened its monitoring and sanction mechanisms, aligned them with international standards, increased transparency, and enhanced its regulations for emerging financial tools, such as cryptocurrencies (Simsek, 2024).

These findings and discussions will guide the identification of the necessary strategic steps for FIUs to work more effectively. Furthermore, the protection of individual privacy and ethical responsibility are essential elements to ensure the sustainability of technological progress.

The findings presented above provide solid ground for deriving practical recommendations, both in the short and long term, which are outlined in the next section.

Conclusion and Recommendations

Monitoring cryptocurrency transactions is a complex challenge for financial intelligence units (FIUs). Issues such as anonymity, decentralization, and international incompatibility make it difficult to detect and prevent illegal activities. Technological investments and international cooperation play a crucial role in overcoming these challenges. However, protecting individual privacy rights and flexibly applying regulatory frameworks are critical not only for monitoring efforts' effectiveness but also for societal acceptance.

An integrated approach should be adopted at both local and global levels to overcome these challenges. Leveraging technological solutions while adhering to legal and ethical standards is a fundamental requirement in this process.

Short-Term Actions

- Enhancing collaboration with cryptocurrency exchanges to improve STR and KYC compliance.
- Investing in blockchain analytics tools (e.g., Chainalysis, CipherTrace) for immediate monitoring capacity improvement.
- Adopting AI/ML-based anomaly detection systems to reduce false positives and improve efficiency.
- Raising public awareness programs for both citizens and employees, highlighting the importance of financial security and the risks of illicit cryptocurrency use.
- Focusing on high-risk transactions with a risk-based approach that reduces workload while ensuring efficiency.

Societal benefits: These actions can increase economic security by reducing the risk of illicit funds flowing into the financial system and strengthening public trust in institutions.

Long-Term Actions

- Developing harmonized international regulations and strengthening data-sharing mechanisms in accordance with the FATF recommendations.
- Building advanced technological infrastructure and human resource capacity within FIUs to ensure sustainable monitoring.
- Creating legal frameworks for decentralized platforms and privacy-focused cryptocurrencies to ensure that innovation is balanced with security.
- Promoting public–private partnerships between FIUs and technology providers to develop more sophisticated monitoring tools.
- Embedding privacy-preserving technologies (e.g., anonymized data analysis and independent audit mechanisms) to ensure compliance with data protection laws and safeguard individual rights.

Societal benefits: These steps will foster long-term economic stability, individual freedoms, and international credibility, contributing to financial system resilience and citizens' rights.

Taken together, these recommendations strengthen the effectiveness of FIUs and highlight the societal benefits of ensuring financial integrity while protecting individual rights.

Peer Review: Externally peer-reviewed.
Author Contributions: Conception/Design of Study- C.Ü., H.Y.; Data Acquisition- C.Ü., H.Y.; Data Analysis/Interpretation- C.Ü., H.Y.; Drafting Manuscript- C.Ü., H.Y.; Critical Revision of Manuscript- C.Ü., H.Y.; Final Approval and Accountability- C.Ü., H.Y.
Conflict of Interest: The authors have no conflict of interest to declare.
Grant Support: The authors declared that this study has received no financial support.

Author Details

Cihan Ünal

[1] Hacettepe University, Başkent Organized Industrial Zone, Technical Sciences Vocational School, Department of Computer Programming, Ankara, Türkiye

0000-0002-5255-4078 cihan.unal@hacettepe.edu.tr

Hakan Yıldırım

[2] Non-affiliated, Ankara-Türkiye

0000-0002-5959-2691

References

Amler, H., Eckey, L., Faust, S., Kaiser, M., Sandner, P., & Schlosser, B. (2021). DeFi-ning DeFi: Challenges & pathway. *2021 3rd Conference on BC Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 181–184.

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. *Electronics*, *13*(17), 3568.

Atzei, N., Bartoletti, M., Lande, S., & Zunino, R. (2018). A formal Bitcoin transaction model In S. Meiklejohn and K. Sako (Eds.), *Financial Cryptography and Data Security*. FC 2018 (Vol. 10957).

Auer R, Haslhofer B, Kitzler S, Saggese, P., & Victor, F. (2024). Decentralized finance technology (DeFi). *Digital Finance*, *6*(1), 55-95.

Ay, A. (2018). International funding for the fight against terrorism. *International Journal of Social and Educational Sciences*, *5*(9), 102–117. https://doi.org/10.1016/j.ijse.2015.09.010.

Bernsdorff, N. (2014). In J. Meyer (Ed.), The EU Charter of Fundamental Rights (German) (Art. 7, 8, 16 CFR). Baden-Baden: Nomos Verlagsgesellschaft; 2010.

R. Camino, R. State, L. Montero, & Valtchev P., "Finding Suspicious Activities in Financial Transactions and Distributed Ledgers," 2017 IEEE International Conference on Data Mining Workshops (ICDMW), New Orleans, LA, USA, 2017, pp. 787-796, 2017.

Chaudhry, N., & Yousaf, M. M. (2018). *Consensus Algorithms in BC: Comparative analysis, challenges and opportunities*. 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), 2018, pp. 54–63.

Chow, H. K., & Wong, F. C. (2020). Monetary Policy Implementation in Singapore In: F. Rövekamp, M. Bälz, H.G. Hilpert, eds., Monetary Policy Implementation in East Asia. *Financial and Monetary Policy Studies*, 51. Springer, Cham.

CoinDesk (2018). *Why Bitcoin fungibility is essential*.

Directive of the European Parliament and of the Council (EU) 2015/849 (2017). Official Journal of the European Union.

Financial Intelligence Unit. (2020). Strategic Plan 2020-2024. Reserve Bank of Fiji.

Hileman, G., & Rauchs, M. (2017). 2017 Global Cryptocurrency Benchmarking Study. University of Cambridge-Cambridge Center for Alternative Finance.

Ibe, C., Okoye, C. A., Nweze, E., & Otu, A. (2023). Cryptococcosis in Africa: What do the data tell us? *Medical Mycology*, *61*(6), Article myad049.

Ibrahim, O. (2024). Cryptocurrency; the new unleashed financial instrument, should it be regulated. *Humanities Journal of University of Zakho*, *12*(2), 303–317. https://doi.org/10.1016/j.hju.2024.04.017.

Ibrahim, S. A. (2019). Regulating cryptocurrencies to combat terrorism-financing and money laundering. *Stratagem*, *2*(1), 57-76.

Ijaz MNaz FKarim S(2024)Revolutionizing financial data security through BC and distributed ledger technologySafeguarding financial data in the digital age10.4018/979-8-3693-3633-5.ch008(121-145)Online publication date: 17-May-2024

Kumar, A., Abhishek, K., Nerurkar, P. et al. (2024): Big data analytics to identify illegal activities on Bitcoin BC for IoMT.

Lagerwaard, P. (2024). Circulating knowledge through disparate practices: Financial Intelligence Units (FIUs)' global pursuit of terrorist financing Science as Culture, 33 (4), 556–578.

Lal, B., Agarwal, R., & Shukla, S. K. (2021). Understanding the money trails of suspicious activities in a cryptocurrency-based business case system arXiv preprint arXiv:2108.11818.

Lidstone, H. K. (2023). Will FinCEN be ready for the CTA?

McNaughton, K. J. (2023). Variability and clustering of Financial Intelligence Units (FIUs): A comparative analysis of national FIU models in selected western and eastern (post-Soviet) countries Journal of Economic Criminology, 2, 100036.

Murthy, C. V. N. U. B., Shri, M. L., Kadry, S., & Lim, S. (2020). BC-based cloud computing: Architecture and research challenges. *IEEE Access*, *8*, 205190–205205. https://doi.org/10.1016/j.ieaaccess.2020.10.1016

Nance, M. T. (2018). Re-thinking FATF (2018): an experimentalist interpretation of the Financial Action Task Force. *Crime Law Society Change, 69*, 131–152.

Nettesheim, M. (2017). Respect for private and family life Meyer-Ladewig, J., Nettesheim, M., & von Raumer, S. (Eds.). ECHR European Convention on Human Rights (Art. 8). Baden-Baden: Nomos-Verlagsgesellschaft.

Özgenç, İ. (2021). Şüpheli İşlem Bildiriminin Hukuki Mahiyeti, Masak'in Rolü, Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu Üzerine Hukuki Değerlendirmeler. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, *25*(3), 273-328.

Panevski, D., Peráček, T., & Rentková, K. (2021). Analysis of the practices of financial intelligence units and other antimoney laundering agencies within the European Union. In N. Kryvinska & A. Poniszewska-Marańda (Eds.), *Developments in information & knowledge management for business applications* (Vol. 376, pp. 121–136). Springer.

Pramanik, M. I., Ghose, P., Hossen, M. D., Ahmed, M. H., Rahman, M. M., & Bhuiyan, M. R. (2025). Emerging Technological Trends in Financial Crime and Money Laundering: A Bibliometric Analysis of the Role of Cryptocurrencies and Global Research Collaboration. *Journal of Posthumanism*, *5*(6), 3611-3633.

Rehman, M. H. u., Salah, K., Damiani, E., & Svetinovic, D. (2020). Trust in the BC cryptocurrency ecosystem *IEEE Transactions on Engineering Management, 67*(4), 1196–1212.

Saadah, S., & Ahmad Whafa, A. A. (2020). *Monitoring financial stability based on prediction of cryptocurrencies price using intelligent algorithm*. 2020 International Conference on Data Science and Its Applications (ICoDSA), 1–10.

Simsek indicates that Turkey is removed from FATF watchdog's gray list. (2024, June 28). Reuters. Retrieved November 19, 2024, from https://www.reuters.com/world/middle-east/simsek-indicates-that-turkey-removed-fatf-watchdogs-grey-list-2024-06-28/

Takei, Y., & Shudo, K. (2024). Effective Ethereum staking in cryptocurrency exchanges. *2024 IEEE International Conference on BC (BC)*, 332–339.

Utkina M, Samsin, R., & Pochtovyi, M. (2023). Financial intelligence (monitoring) of transactions with virtual assets: Foreign countries' new legislation and best practices. *Journal of Money Laundering Control*, *26*(2), 349–360.