Money Laundering through Cryptocurrencies: Assessing the Use of Artificial Intelligence in Financial Monitoring Agency of Kazakhstan

by

Olzhas Adilbekov

Bushra Ali

Lazzat Missalimova

Nurgissa Azhdarov

Supervisor

Prof., Simeon Nanovsky

Master's Project

Paper submitted in partial fulfillment of the

Degree of Master of Public Administration

Graduate School of Public Policy

Nazarbayev University

Astana, Kazakhstan

January 30, 2026

Abstract

This research explores the idea of adopting Artificial Intelligence (AI) to monitor cryptocurrency and evaluates whether it is economically feasible for Kazakhstan, considering current technological and legal conditions. Cryptocurrencies enable fast and borderless value transfers, while also facilitating money laundering through various techniques which complicates detection of such transactions due to the anonymous nature of these. Building on FATF-standards and the emerging literature on AI-enabled AML (anti-money laundering), this study applies a qualitative case-study design focused on Kazakhstan's regulatory environment, where most crypto-related activities are limited outside the Astana International Finance Center (AIFC). Empirical evidence consists of ten semi-structured interviews with experts (conducted anonymously due to topic sensitivity), documentary analysis of regulatory materials and international practice. Findings display partial readiness of Kazakhstan for AI-driven crypto monitoring. Although the FMA already uses the hybrid approach, there are limitations. In addition to this, phased hybrid strategy allows the most viable balance between effectiveness, cost and institutional sustainability.

Table of Contents

List of Tables

1. Introduction

The development and expansion of cryptocurrencies has significantly changed the global financial landscape. Cryptocurrencies do not use traditional financial mediators. Instead, they rely on distributed ledgers technology to verify and keep records of transactions (Yli-Huumo et al., 2016). Cryptocurrencies contribute to more inclusivity and better opportunities for people around the world. However, despite all the advantages cryptocurrency also poses significant risks for financial integrity. Especially in the context of money laundering and other illegal financial activities (Campbell-Verduyn, 2018).

Money laundering through cryptocurrency is the process where illegally obtained funds are concealed, transferred, or integrated into the legal economy via virtual assets and blockchain-based transactions. This process uses pseudonymity, cross-border transferability, and the technical complexity of blockchain networks to hide or distort the origin and ownership of criminal procedures (Albrecht et al., 2019; FATF, 2021). While traditional money laundering typically relies on banks and financial intermediaries, cryptocurrency-based laundering can occur through decentralized systems that operate beyond conventional regulatory framework, complicating detection.

Since the establishment of cryptocurrency, many examples of large-scale money laundering using cryptocurrency have emerged. For example a case of Tornado Cash, a cryptocurrency mixing platform. According to the US Treasury Department, over $7 billion has been laundered through the service since its launch in 2019 (US Treasury Department, 2022). Hacker groups, including the North Korean group Lazarus, stole the funds. In August 2022, Tornado Cash was placed on the US sanctions list as a tool for money laundering (US Treasury Department, 2022).

Another good example is the hacking of the Bitfinex crypto exchange in 2016, which resulted in the theft of about 120,000 bitcoins. For several years, attackers have used sophisticated methods to hide traces of transactions, including splitting wallets, switching between different blockchains, and using mixing services (U.S. Department of Justice, Archive, 2024). Despite the apparent anonymity of such operations, the investigation was made possible using blockchain analytics tools and interagency cooperation (Chainalysis team,

2023). This case clearly demonstrates both the scale of cryptocurrency laundering and the importance of modern analytical technologies in countering such crimes.

Globally, the volume of illegal activity using cryptocurrencies continues to grow. According to Chainalysis (2024), in 2023, about 24.2 billion US dollars were related to money laundering using cryptocurrencies. These trends are prompting regulators to review existing anti-money laundering (AML) systems and look for new technological solutions that can address the specific risks associated with virtual assets.

Similarly, Kazakhstan has seen an increase in cryptocurrency-related activity. Over the past decade, transaction volumes reached approximately 4.1 billion US dollars in 2023 (Chainalysis, 2024). At the same time, at the national level, the turnover of cryptocurrencies is generally limited, and legal transactions are allowed under the special legal regime of the Astana International Financial Center (AIFC). The Law "On Digital Assets in the Republic of Kazakhstan" (2023) and the AIFC regulations regulate the licensing and supervision of virtual asset service providers (VASPs), bringing the national system in line with Recommendation 15 of the Financial Action Task Force (FATF).

The Financial Monitoring Agency (FMA), established in 2021, is responsible for detecting, preventing and investigating cases of money laundering in Kazakhstan. In 2024, 36 clandestine crypto exchange platforms, through which transactions worth about 60 billion tenge were carried out, were liquidated by government agencies,. In addition, during these events, crypto assets worth about $4.8 million were frozen (Inform.kz, 2024). During the same period, the first court verdicts were handed down in cases related to illegal cryptocurrency activities, which became an important stage in the practical application of crypto regulation in the country (Tengrinews.kz , 2023; 2024). These examples demonstrate a growing institutional understanding of the risks associated with financial crimes in the field of cryptocurrencies.

However, the increasing sophistication of laundering techniques has exposed the limitations of traditional monitoring tools. Conventional AML mechanisms, largely designed for bank-mediated transactions, are often insufficient for tracking decentralized, high-volume, and cross-chain cryptocurrency flows. In response, worldwide regulatory authorities are implementing artificial intelligence (AI) and advanced analytical tools, including blockchain analytics platforms and machine-learning models, to enhance transaction monitoring,

anomaly detection, and risk assessment (Chen et al., 2018; FATF, 2021). According to the International Monetary Fund, (2023) more than 60% of financial intelligence units in OECD countries are already using or testing AI tools to identify suspicious financial activities, including digital assets transactions.

Besides, given that cryptocurrency transactions happen in real time and are cross-border, the limitations of traditional systems become apparent. For example, a World Economic Forum (2023) report notes that approximately 70% of major financial regulators in developed countries consider rules-based anti-money laundering systems ineffective without the support of AI-powered analytics. It is primarily due to high false positive rates and the inability to detect complex network patterns (World Economic Forum, 2023).

In response to these challenges, authorities in the USA, EU countries and the UK, artificial intelligence is already actively used in financial monitoring. According to FinCEN, the use of AI has reduced the time needed to analyze suspicious transactions by 30-50% and improved the accuracy of detecting high-risk transactions compared to traditional methods. European authorities are adopting similar approaches, where AI is used to analyze connections between wallets, exchanges, and decentralized platforms (European Central Bank, 2023).

Despite the significant potential, the practical implementation of AI-based monitoring systems is a challenging process. The one accompanied by technical, institutional and organizational difficulties. These include high financial costs, infrastructure requirements, data-integration limits, and unresolved legal and ethical questions related to algorithmic decision-making. For countries like Kazakhstan, which operate under fiscal, institutional, and regulatory constraints, the adoption of AI for cryptocurrency monitoring raises a question of economic feasibility rather than technological capacities.

In this regard, this study is aimed at assessing the economic feasibility of introducing artificial intelligence into monitoring cryptocurrency transactions at the Financial Monitoring Agency of the Republic of Kazakhstan, under the current technological and legal conditions. More specifically, the study addresses the following questions:

1. **What is the current technological capacity of the FMA and Kazakhstan's financial monitoring system for adopting AI-based tools?**

2. **How do existing legal and regulatory frameworks influence the integration of AI in cryptocurrency surveillance?**
3. **What are the expected costs and potential savings associated with implementing AI for transaction monitoring?**

By comparing international best practices with the institutional realities of Kazakhstan, this study aims to develop practical recommendations for strengthening the national anti-money laundering system in the context of the rapid development of digital financial technologies.

The next chapter provides a literature review on money laundering mechanisms using cryptocurrencies, regulatory approaches to their control, as well as the role of artificial intelligence and modern analytical tools in AML systems. The methodology section describes the design of the study and the data collection methods used. The chapter with the results analyzes the technological capabilities of Kazakhstan, the regulatory environment and the economic feasibility of implementing AI, after which recommendations on public policy are formulated and the main conclusions of the study are presented.

2. Literature Review

2.1. Money Laundering Through Cryptocurrency: Risks and Techniques

The growing circulation of cryptocurrencies has created new opportunities for both legitimate financial innovation and criminal misuse. Unlike traditional banking systems, blockchain-based networks allow users to send funds directly to one another without relying on centralized intermediaries such as banks (Campbell-Verduyn, 2018). This peer-to-peer structure reduces transaction frictions but also removes many of the monitoring mechanisms that conventional anti–money laundering (AML) frameworks rely on (Choo, 2015).

Money laundering through cryptocurrency can be understood as the process by which illegally obtained funds are concealed, layered, or integrated into the formal economy using virtual assets and blockchain transactions. While blockchains are, in principle, transparent ledgers, the absence of mandatory identity disclosure at the wallet level allows criminals to separate addresses from real-world identities and to distribute transactions across different accounts.

Scholars identify several recurring techniques exploited to launder funds through cryptocurrencies. One widely documented method involves mixers and tumblers. Mixers pool numerous users' coins and redistribute them to new addresses, breaking the traceable link between sender and recipient (Dyntu & Dykyi, 2018). Tumblers perform a similar action, often charging a fee to "shuffle" coins over multiple transactions to obscure the transaction trail (Albrecht et al., 2019). These tools significantly complicate blockchain analysis by fragmenting flows and distorting transaction patterns (Desmond et al., 2019).

The second technique is chain-hopping, where funds are moved across different cryptocurrencies and blockchains to avoid detection. Criminals might, for instance, convert Bitcoin into privacy-focused coins such as Monero, which conceals address and transaction details (Dyntu & Dykyi, 2018). This multi-chain layering complicates the reconstruction of a complete picture of the laundering process, especially when some networks lack sophisticated analytics tools (Choo, 2015).

Moreover, privacy coins and decentralized exchanges (DEXs) present further challenges. Privacy coins are specifically designed to hide sender, receiver, and transaction amounts, undermining conventional blockchain transparency (Albrecht et al., 2019). Decentralized exchanges which allow trading without centralized order books, reduce the effectiveness of traditional supervisory mechanisms that depend on regulated intermediaries.

The transborder and decentralized nature of cryptocurrencies amplifies these risks. Funds can be transferred in seconds, bypassing currency controls and traditional financial institutions (Desmond et al., 2019). This dynamic increases pressure on national authorities, who must coordinate internationally to trace cross-border flows and align their frameworks with global standards (Campbell-Verduyn, 2018). Overall, the literature shows that cryptocurrency-based money laundering is not only a technical issue but also a systemic one, challenging existing AML frameworks.

2.2. Existing Tools and Measures for Preventing Money Laundering

Various authors focus on the regulatory instruments designed to combat money laundering, which also involves cryptocurrency. Traditional AML frameworks are built around key notions such as customer due diligence, transaction monitoring, reporting of suspicious

activity, and international cooperation. As Subbagari (2024) notes, effective governments typically establish clear responsibilities for financial institutions, including requirements to monitor transactions, conduct risk assessments, and report suspicious behaviour. These obligations are increasingly being extended to virtual-asset service providers (VASPs).

The Financial Action Task Force has a central role in setting global standards for virtual assets. FATF Recommendation 15 requires states to regulate and license VASPs and to ensure that they implement AML and counter-terrorist financing (CFT) controls comparable to those applied to traditional financial institutions (FATF, 2023). This includes measures such as customer identification, ongoing monitoring, and compliance with the "Travel Rule", which requires the sharing of origin and recipient information in certain virtual-asset transfers.

At the operational level, many jurisdictions continue to rely on established AML instruments such as Know Your Customer (KYC) and transaction monitoring. Obe and Nay (2022), examining the digital age, emphasize that KYC requirements remain a cornerstone for preventing illicit activities, helping institutions verify the identity and risk profile of clients. They argue that these mechanisms, historically designed for bank accounts and payment services, must be systematically extended to cryptocurrency exchanges and wallets to avoid regulatory blind spots.

However, Akhmetkerey, Issabayeva, and Bastaubayeva (2019) recognize important gaps in solely regulatory or procedural responses. Although in Kazakhstan regulatory efforts have sought to manage the risks associated with cryptocurrency, vulnerabilities persist due to the pseudonymous nature of blockchains and the existence of informal or illegal exchanges. Proskurina (2023) similarly notes that despite the Law "On Digital Assets in the Republic of Kazakhstan" and the special regime of the Astana International Financial Centre, cross-border transactions and unregulated platforms remain difficult to supervise.

The IMF (2022) highlights that regulatory convergence is incomplete. While some countries, such as the United States and Singapore, have created sophisticated AML systems for cryptocurrencies, many jurisdictions fall behind in integrating FATF standards into domestic law. FATF (2023) reports that by the end of 2023 only about a quarter of jurisdictions had fully implemented its standards for virtual assets, leaving significant drawbacks in the international system.

Overall, the literature analysis displayed that existing tools and measures (i.e. legal frameworks, KYC, reporting obligations, and international standards) are essential, but insufficient. They provide a normative foundation, but their effectiveness in the context of cryptocurrencies increasingly depends on technological capabilities such as data analytics, blockchain tracing, and, more recently, AI-based systems.

2.3. AI and Modern Analytical Instruments in AML and Crypto Monitoring

Over the last decade, scholars and practitioners have increasingly highlighted the role of artificial intelligence, machine learning (ML), and blockchain analytics in enhancing AML systems. As crypto-related financial crime has grown more complex, regulators and financial institutions have sought technological solutions capable of detecting suspicious patterns in large and heterogeneous datasets.

Chen et al. (2018) provide a comprehensive review of machine-learning techniques for AML. They note that ML methods, including supervised and unsupervised algorithms can improve the detection of anomalous transactions by learning patterns from historical data. These tools can assist in risk-scoring customers and transactions, identifying unusual behaviour that may not be captured by rule-based systems alone. Similarly, Akhtar et al. (2023) argue that technological advances offer new opportunities to combat money laundering, but they also introduce legal and governance challenges related to transparency, accountability, and data protection.

In the field of cryptocurrencies, blockchain analytics platforms such as Chainalysis, Elliptic, TRM Labs, and CipherTrace have become central actors. These systems cluster wallet addresses, trace transaction flows, and assign risk scores based on typologies of illicit behaviour, such as links to darknet markets, mixing services, or sanctioned entities. According to KPMG (2021), such tools enable rapid analysis of large volumes of blockchain data, significantly improving the capacity to detect suspicious activity and respond to emerging threats. They also facilitate cross-border cooperation by providing standardized risk indicators that can be shared between regulators, law-enforcement bodies, and private institutions.

Recent studies go further by integrating machine-learning algorithms directly into blockchain analysis. Lyeonov et al. (2024), for example, demonstrate the use of Bayesian classifiers to analyse Ethereum transactions and identify patterns associated with suspicious activity. They argue that these methods can support regulators by automating parts of the detection process and by prioritizing high-risk transactions for further investigation. This suggests that AI tools are not merely add-ons to existing systems but can fundamentally reshape how monitoring is conducted.

At the same time, the literature stresses that AI-based monitoring is not without risks and costs. FATF (2021) emphasizes that the adoption of new technologies must remain consistent with principles of data protection, privacy, and cybersecurity. IMF (2025) points out that AI systems require continuous maintenance, model updates, and skilled personnel, which can be costly for public authorities. It is also noted that poorly designed systems may generate excessive false positives or embed biases, thereby undermining both efficiency and fairness.

Furthermore, several authors underline that the effectiveness of AI tools depends on institutional and infrastructural conditions. AI models require high-quality, structured data and interoperable systems that can integrate information from multiple sources, such as banks, VASPs, and law-enforcement databases (FATF, 2021; IMF, 2025). In the absence of such infrastructure, even advanced AI tools may deliver limited value. As a result, the literature increasingly views AI not as a standalone solution but as part of a broader hybrid approach, where technology enhances human expertise rather than replaces it.

This discussion is directly relevant to Kazakhstan's context, where the Financial Monitoring Agency has begun to use commercial blockchain analytics tools but faces constraints related to data integration, infrastructure, and human capital. The question of whether AI can be implemented in a cost-effective and institutionally sustainable way remains largely unanswered and forms the core of this thesis.

2.4. International Experience and the Case of Kazakhstan

A growing body of work examines how different countries have approached the regulation and monitoring of cryptocurrency-related money laundering. These comparative studies provide important benchmarks for Kazakhstan.

In the United States, the Financial Crimes Enforcement Network (FinCEN) and other agencies have developed a proactive regulatory and supervisory environment for virtual assets. FinCEN cooperates closely with private blockchain-analytics providers, using their tools to trace suspicious transactions and ensure compliance with AML/CFT regulations (Financial Crimes Enforcement Network, n.d.; Lindsay, 2023). The U.S. model is characterized by multiple overlapping authorities, each with specialized mandates, coupled with extensive use of technological tools.

In the UK, the FCA supervises crypto-asset businesses under the AML/CTF regime and requires in-scope firms to register under the Money Laundering Regulations. In practice, crypto businesses commonly rely on blockchain-analytics tools (e.g., Elliptic) to support transaction monitoring and compliance (FCA, 2019). Singapore regulates DPT services through MAS AML/CFT requirements (e.g., Notice PSN02). In this technology-forward compliance environment, blockchain-analytics providers such as Chainalysis and Elliptic are widely used in the market to support monitoring and risk assessment, while MAS continues to advance a regulated digital-asset strategy.

Russia offers a different example. The Federal Financial Monitoring Service (Rosfinmonitoring) has developed the "Transparent Blockchain" system, an in-house blockchain-monitoring tool designed to track suspicious transactions and support the identification of financial crimes. This case illustrates a state-driven attempt to build domestic analytical capacity rather than relying solely on foreign vendors.

In contrast, the literature on Kazakhstan focuses primarily on the development of legal frameworks and the role of the Astana International Financial Centre. Akhmetkerey et al. (2019) and Proskurina (2022) describe Kazakhstan's approach as cautious but evolving, combining strict prohibitions on cryptocurrency operations outside the AIFC with a more permissive environment within it. The Law "On Digital Assets in the Republic of Kazakhstan" defines virtual assets and allocates supervisory responsibilities among the FMA, the National Bank, and AIFC regulators. At the same time, Diakonashvili et al. (2022) highlight that cross-border transactions, anonymity, and informal markets continue to pose significant AML risks.

Available reports indicate that Kazakhstan has taken some steps toward technological monitoring. The FMA has dismantled illegal cryptocurrency exchanges with substantial

turnover and has reportedly cooperated with international analytics providers such as Chainalysis. However, academic literature provides limited detail on the specific tools used, their coverage, or their long-term sustainability. Most analyses remain focused on legislative developments and international cooperation rather than on the analytical instruments deployed by the FMA and their effectiveness.

Overall, comparative evidence shows that advanced jurisdictions increasingly integrate AI and blockchain analytics into their AML architectures, while countries like Kazakhstan are still in an early, experimental phase. This suggests not only a technological gap but also a research gap: few studies evaluate how feasible it is for emerging economies to adopt similar tools given fiscal, institutional, and infrastructural constraints.

2.5. Summary

The literature reviewed in this chapter highlights several key points. First, cryptocurrencies introduce distinctive money-laundering risks due to their pseudonymity, decentralization, and cross-border nature. Criminals use techniques such as mixers, tumblers, chain-hopping, and privacy coins to conceal the origin and movement of illicit funds (Albrecht et al., 2019; Dyntu & Dykyi, 2018). Second, while existing AML frameworks provide an essential regulatory foundation, they struggle to fully address the complexity of cryptocurrency-based laundering, especially where regulation and supervision lag behind technological developments (FATF, 2021; IMF, 2022).

Third, there is growing consensus that AI and modern analytical tools are becoming indispensable components of effective AML systems. Machine learning, blockchain analytics, and hybrid human–machine approaches can significantly enhance detection capacity, reduce manual workloads, and improve the timeliness of interventions (Chen et al., 2018; Lyeonov et al., 2024; KPMG, 2021). However, the literature also underlines that these tools require substantial investment in infrastructure, high-quality data, and specialized human capital, and they raise important legal and ethical issues.

Finally, while comparative work on the United States, the United Kingdom, Singapore, and Russia documents a variety of regulatory and technological responses, there is a notable lack of empirical research on Kazakhstan and similar jurisdictions. Existing studies on

Kazakhstan focus predominantly on legal frameworks and international cooperation, offering limited insight into the actual analytical instruments used by the FMA, their effectiveness, or their economic and institutional feasibility (Akhmetkerey et al., 2019; Proskurina, 2023; Diakonashvili et al., 2022).

This thesis addresses these gaps by examining what modern tools Kazakhstan's Financial Monitoring Agency can realistically implement to track money laundering in cryptocurrency transactions, and under what conditions AI-based solutions are economically and institutionally feasible. By linking the conceptual and comparative literature with empirical evidence from Kazakhstan's regulatory practice, the study seeks to inform both national policy debates and broader discussions on AI adoption in financial supervision.

3. Methodology

3.1. Research Design and Approach

This study examined whether the implementation of artificial intelligence (AI) for monitoring cryptocurrency transactions in Kazakhstan's Financial Monitoring Agency (FMA) is economically feasible under current technological and legal conditions. Since the research question is focused on institutional capacity, governance constraints, and the practical costs and benefits of adopting advanced analytical tools, this study applied a qualitative, descriptive, and inductive research design. This approach allowed the research to capture expert knowledge, institutional realities, and policy dynamics without assuming a predetermined causal model.

A case-study logic was also applied in this study. Centered on the FMA and the national crypto-regulatory environment, it combined primary qualitative evidence from expert interviews and secondary evidence from official documents, regulatory materials, and credible international reports.

3.2. Analytical Framework

This research used three points as conceptual lenses, which were important for a broader and multidimensional approach.

1. **Technological readiness**: the availability of data infrastructure, analytical tools, integration capacity, and human capital to support AI-enabled monitoring.
2. **Regulatory and institutional context**: whether the legal framework, institutional mandates, data-sharing arrangements, and governance safeguards enable or constrain AI use in AML/CFT monitoring.
3. **Economic feasibility**: the cost structure of implementation (tools, infrastructure, staffing, training, maintenance) and the expected institutional benefits (efficiency, detection speed, investigative prioritization, asset-freezing potential).

3.3. Data Sources

This research relied on two categories of data. Firstly, **primary data (expert interviews).** Ten semi-structured interviews were conducted with experts directly familiar with AML/CFT oversight, crypto-asset compliance, and/or digital financial governance in Kazakhstan. Since the topic involved enforcement practices, investigative techniques, and institutional constraints, interview participants requested confidentiality and anonymity.

Secondary data (public documents and policy materials). Publicly available documents as our secondary data were used for three core purposes. Firstly, to map the legal and institutional context for crypto-related AML/CFT in Kazakhstan. Secondly, to benchmark Kazakhstan's approach against international standards and supervisory practice. Lastly, to triangulate interview statements regarding monitoring tools, typologies, and implementation constraints. The secondary dataset included:

(a) Kazakhstan legal and regulatory acts governing digital assets and AML/CFT mandates (e.g., the Law "On Digital Assets in the Republic of Kazakhstan" (2023) and related implementing rules);

(b) AIFC/AFSA regulatory materials relevant to virtual-asset service providers (VASPs), including AML/CFT requirements and supervisory guidance applicable within the AIFC jurisdiction;

(c) International standards and guidance on virtual assets and AML/CFT technologies, primarily FATF materials on virtual assets and the use of new technologies;

(d) International analytical reports on illicit crypto activity and typologies (e.g., Chainalysis Crypto Crime reporting) used to describe laundering mechanisms and monitoring indicators; and

(e) Official enforcement and sanctions communications (e.g., U.S. Department of Justice and U.S. Treasury press releases on major crypto laundering cases and mixer-related actions) used as real-world examples of methods such as mixing and cross-chain laundering and the tools used to investigate them.

Additionally, information obtained through participation in an industry event (Astana Finance Day, 2025) and expert engagements were integrated into this study. These insights were treated as contextual field-based evidence only and were used to interpret policy direction and stakeholder priorities; they were not used as a substitute for documentary sources or interview data, but as supplementary pieces.

3.4. Expert Interviews

3.4.1. Sampling strategy and recruitment

A purposive sampling strategy was used to identify interviewees with relevant experience in cryptocurrency regulation, compliance monitoring, financial intelligence, and/or digital governance. In addition, this research required specialised knowledge and access to practice-based insights that were not available through public data.

3.4.2. Interview format and instruments

Interviews were conducted in a semi-structured format to balance comparability across respondents with flexibility to sensitive or complex issues. The interview guide was focused on:

- current monitoring practices and analytical tools used in crypto-related investigations;
- perceived technical constraints (data quality, systems integration, computational capacity);
- legal and institutional barriers (data-sharing, accountability, AI governance needs);
- cost drivers and feasible implementation models (vendor tools vs. in-house capability; hybrid options);

- perceived impact of AI/advanced analytics on operational effectiveness.

3.4.3. Anonymity and coding

Given the sensitivity of AML/crypto enforcement and compliance topics, all interviewees remained anonymous as per their requests. In reporting results, participants were referenced using neutral identifiers. Any potentially identifying institutional details were either removed or generalised to prevent deductive disclosure.

3.5. Document and Secondary Data Review

Secondary data was used for three purposes:

1. **Contextualisation**: establishing the regulatory environment and institutional roles relevant to AML/CFT and crypto oversight in Kazakhstan.
2. **Triangulation**: cross-checking expert statements against official documents and reputable reports.
3. **Feasibility grounding**: supporting the economic and operational feasibility discussion using credible benchmarks and reported typologies.

3.6. Data Analysis

Data analysis followed two complementary qualitative methods, which included thematic content analysis. Interview notes/transcripts and key documentary materials were coded to identify recurring themes related to the three feasibility dimensions (technological readiness, regulatory context, economic feasibility). This included patterns around infrastructure constraints, data integration issues, governance gaps, and perceived cost/benefit trade-offs.

Comparative/structured analysis. Evidence was interpreted using structured comparison across:

- feasibility dimensions (tech/legal/economic); and
- policy/implementation approaches discussed in the literature (vendor platforms, hybrid models, in-house development).

3.7. Trustworthiness and Triangulation

To enhance credibility and reduce single-source bias, the study used **triangulation** across:

- interview evidence (practice-based insight);
- documentary evidence (formal policy and regulatory framing); and
- field-based contextual observations from relevant professional discussions/events.

3.8. Ethical Considerations

Ethical safeguards were implemented to protect participants and ensure research integrity. Participation was strictly voluntary, and **informed consent** was obtained prior to interviews. All interviews were anonymised and stored securely, and identifying details were removed from the write-up to protect participants from professional or legal exposure. The findings were reported in aggregated form and including operational details was avoided to protect from misuse.

3.9. Limitations

This research has faced several limitations typical of studies on financial intelligence and crypto-related enforcement. First, access to sensitive operational data is restricted, limiting the ability to validate some claims using internal statistics. Second, the cryptocurrency environment evolves quickly, meaning that regulatory and technological conditions can change faster than academic publication cycles. Third, expert interviews may have reflected institutional perspectives and constraints, creating potential bias; this is mitigated through triangulation and careful interpretation.

4. Findings Chapter

4.1. Introduction

This chapter presents the empirical findings of the study, aimed at evaluating whether the implementation of artificial intelligence for monitoring cryptocurrency transactions in the Financial Monitoring Agency (FMA) of Kazakhstan is economically feasible under current technological and legal conditions.

The findings are based on qualitative research and documentary analysis. As part of the work, semi-structured interviews were conducted with ten experts in the field of anti-money laundering, financial monitoring and digital policy. The interviews were complemented by an analysis of regulatory legal acts and official publications of government agencies of the Republic of Kazakhstan, regulatory documents of the Astana International Financial Center, as well as materials from international organizations, including FATF recommendations and the OECD analytical framework in the field of artificial intelligence regulation.

The calculations were based on commercial offers from international providers of analytical SaaS solutions (Chainalysis, TRM Labs, Elliptic), FATF reports on the effectiveness of AML/CFT systems (2023-2024), industry benchmarks for the cost of AI solutions (Gartner, McKinsey), as well as aggregated data from the Financial Monitoring Agency of the Republic of Kazakhstan for 2022-2024 years.

This chapter is organised in the following order:

1. Technological readiness. The current technical and analytical capacity of FMA and Kazakhstan's ecosystems;
2. Regulatory and institutional context. The legal and organizational conditions enabling or constraining AI use;
3. Economic feasibility. The estimated costs, potential savings, and overall economic justifications for AI adoption.

4.2. Technological Readiness

4.2.1. Overview

The Financial Monitoring Agency is currently demonstrating a moderate level of technological readiness for the use of artificial intelligence in the field of monitoring cryptocurrency transactions. FMA already has basic analytical tools at its disposal, as well as specialists with experience working with digital financial data. However, the potential for implementing more complex and advanced AI solutions remains limited.

The main problems are related to fragmented data, limited computing resources and lack of specialists with knowledge in the field of artificial intelligence and blockchain analytics. These factors significantly complicate the practical use of complex AI models and reduce

the likelihood that significant investments in such technologies will lead to a significant result.

Such problems are not unique to Kazakhstan. In many countries, projects to introduce artificial intelligence in the public sector remain at the stage of pilot initiatives (OECD, 2025). The key reasons for this are data fragmentation, a shortage of qualified specialists, and outdated IT infrastructure. In such conditions, technological readiness is not the result of the introduction of AI, but a necessary prerequisite for its effective use.

4.2.2. Existing Tools and Capabilities

The Financial Monitoring Agency uses a hybrid approach combining expert manual analysis and digital tools to identify and investigate suspicious financial activity. According to the interviewed experts, the Agency relies on both internal analytical methods and external technology platforms. In practice, FMA analysts first use internal tools to identify typical transaction patterns, and in difficult cases, they use paid specialized blockchain analytics services such as Chainalysis, TRM Labs, and Elliptic for a more in-depth analysis of cryptocurrency flows.

These third-party platforms provide services for clustering cryptocurrency wallets, tracking transactions on the blockchain, monitoring activity on the darknet, and risk assessment. Such rapid creation of similar tools within the country seems difficult, therefore, this approach can be considered a semi-automated model in case of the FMA. Interestingly, such an approach is in line with FATF recommendations, which emphasize the need for a combination of digital solutions and human control for an effective AML/CFT system. Although algorithms are capable of quickly processing large amounts of data and identifying patterns, the final assessment requires the participation of experts to confirm the correctness of the results.

The interview results also show that the Agency consciously strives to maintain a balance between automation and manual verification in order to ensure the accuracy of analysis, data protection and compliance with regulatory requirements. For example, internal analytical tools automatically record anomalies in transactions (such as a sharp increase in transactions related to cryptocurrencies), after which analysts manually evaluate these cases and decide whether further investigation is necessary. At the same time, the technical details of the

internal systems remain closed for security reasons, as excessive transparency can be used to benefit criminal groups.

Despite these limitations, this approach is already yielding practical results. Therefore, in 2025, the Agency announced the closure of 130 illegal cryptocurrency platforms and the seizure of about 16.7 million US dollars in cryptocurrencies related to money laundering. These data indicate that even with limited use of artificial intelligence, modern digital tools are already making a significant contribution to countering financial crimes.

During the interview, it was also established that the Financial Monitoring Agency is aware of the potential of using artificial intelligence in the field of financial control. It also identified that FMA was also considering the development of AI toll but they face such questions that analytical platforms are expensive, require subscriptions and constant technical support, which can create an additional burden on the Agency's budget. The FMA also faces additional difficulties associated with the integration of such solutions with internal databases and case management systems. Mostly, due to the lack of a centralized database. Therefore, analysts have to work with several platforms and information sources at once to form a complete picture of suspicious transactions.

Nevertheless, there are signs of gradual progress. In 2024, a specialized Crypton division was created in the Agency's structure, focused on financial intelligence in the field of cryptocurrencies. The division actively cooperates with international crypto exchanges, including Binance, as well as with technology companies in order to expand the Agency's analytical capabilities. Moreover, Crypton's also analyzing abnormal energy consumption or using satellite imagery to detect illicit cryptocurrency mining.

In general, these initiatives show that while maintaining the key role of human analysis, digital tools are gradually taking an increasingly important place in the detection and investigation. With the modernization of infrastructure and the development of interagency data exchange, Kazakhstan will be able to automate more stages of financial monitoring. In line with global trends, FMA might be to move from the current semi-automated model to more advanced AI processes, in which algorithms will promptly identify high-risk events, and analysts will be able to focus on strategic and managerial decisions. However, the implementation of this approach directly depends on solving infrastructure and expert problems, which will be discussed in the next chapter.

4.2.3. Infrastructure and Human Capital Gaps

Despite significant advances in anti-money laundering, Kazakhstan still encounters major infrastructure and experts challenges that hinder the widespread use of AI in financial monitoring. One of the main issues is the absence of a centralized, interoperable data platform. Currently, financial information related to anti-money laundering, including data from banks, payment providers, crypto exchanges, and law enforcement, is stored across separate databases managed by different agencies. Consequently, this fragmentation might make it difficult to carry out comprehensive analysis or real-time monitoring across the financial system.

Experts from government agencies interviewed in this study also pointed out these problems and a number of practical limitations. In particular, one of the respondents noted that the analysis of transactions is most often carried out after the committing criminal acts, but the detection of suspicious transactions at an early stage remains difficult. The main reasons for this are weak integration of information systems and limited computing power. As a result, AFM's current analytical work is mainly focused on analyzing past transactions, rather than predicting and preventing risks.

This problem is also reflected in the OECD reports, which emphasize that the lack of centralized and high-quality data is one of the common barriers to early detection of financial crimes. This also explains why the adoption of artificial intelligence in government institutions in many countries remains limited.

Another significant problem is the technical infrastructure. Currently, FMA systems often depend on external paid vendors and consultants to analyze complex cryptocurrency transactions. Although this approach makes it possible to quickly compensate for the lack of internal technical resources, in the long run it creates institutional dependence and leads to an increase in operating costs. Processing large amounts of blockchain data and using complex AI algorithms in real time require powerful computing systems and advanced cloud solutions, which Kazakhstan currently has to a limited extent.

Until the server infrastructure, network systems, and cloud capacities are upgraded, the AFM's ability to fully utilize artificial intelligence will remain limited. Under these conditions, the implementation of full-fledged monitoring in real time, for example,

automatic verification of all cryptocurrency transactions as they are carried out, is still unrealistic.

At the same time human resources shortages also might slow AI adoption. This is because, while the government body has trained AML/CFT professionals, there are few public sector experts skilled in data science, machine learning, or blockchain analysis. In fact, using AI involves not only buying or integrating software tools, it also requires experts who can train models, understand the results, and manage the technology. As a digital policy expert pointed out during interviews, even with top-tier analytics tools, “you still need specialists to interpret the results and apply them.”

However, dependence on technological capacity goes hand in hand with limitations that arise due to lack of human talent. In fact, the government struggles to attract and retain skilled IT professionals. Employment conditions in the public sector are generally rigid, and salary wages are often lower than in the private sector, which makes it difficult to compete for artificial intelligence and data processing specialists. This leads to the fact that existing teams are greatly reduced, and the transfer of knowledge from external experts to in-house staff is slow. FATF has also mentioned that AML professionals often lack both the expertise and awareness needed to adopt modern technologies (FATF, 2021). Consequently, the Kazakhstan government needs serious efforts to build internal capacity through training, developing partnerships with IT universities and tech companies, and better incentives for these workforce gaps since it will continue to hold back Kazakhstan’s AI development.

4.2.4. Conclusion

The analysis of Kazakhstan's technological readiness shows the presence of both strengths and significant gaps. The Financial Monitoring Agency managed to achieve the first practical results through a combination of internal analytical tools and international platforms for tracking blockchain transactions, which made it possible to increase the effectiveness of combating money laundering using cryptocurrencies. This indicates the Agency's commitment to innovation and forms the basis for further integration of artificial intelligence. At the same time, existing infrastructure constraints and a shortage of qualified personnel are holding back the transition to more advanced AI technologies. To ensure the economic

feasibility of introducing artificial intelligence, Kazakhstan will need to make significant institutional investments in both technological development and human capital. A priority area should be the development of a centralized data platform that will ensure the interaction of the Financial Monitoring Agency with banks, regulators such as the National Bank of Kazakhstan and Astana International Financial Centre, as well as with databases of law enforcement agencies. This will allow for the exchange of data necessary for building effective machine learning models and further developing AI-based financial monitoring.

Upgrading computing resources (using cloud services or high-performance servers) is also necessary so that artificial intelligence tools can process large datasets and generate analytical data in real time. At the same time, building an internal pool of AI-savvy specialists – by training current staff, engaging data scientists, and facilitating knowledge sharing between the public and private sectors - will be key to supporting any new systems.

4.3. Regulatory and Institutional Context

4.3.1 Overview

Kazakhstan has established a solid foundation for financial monitoring, and its anti-money laundering and anti-terrorist financing regime, which somehow complies with international standards. However, the integration of AI into these processes is still under development. The purpose of this section is to provide an assessment of the regulatory and institutional context for the implementation of artificial intelligence in financial monitoring systems of cryptocurrency.

There are several core government agencies in Kazakhstan that can provide control over the flow of cryptocurrencies: Financial Monitoring Agency, the Astana International Financial Centre, and the National Bank – form the backbone of its financial oversight system.

The procedure for using cryptocurrencies in Kazakhstan is determined by the Law "On Digital Assets" (2023), as well as the regulations of the Astana International Financial Center (AIFC), which regulate the activities of virtual asset service providers (VASPs). In general, these legal frameworks comply with international standards introduced in Recommendation 15 of the Financial Action Task Force (FATF). Since 2019, the FATF requires states to implement regulation and supervision of cryptocurrency activities through licensing or

registration mechanisms. In practice, Kazakhstan's regulatory system provides a strong basis for cryptocurrency oversight. However, this progress has not yet turned into a coherent legal framework for financial monitoring using artificial intelligence. As several experts interviewed for this study highlighted, the main problem currently is not the establishment of crypto regulation as such, but the development of transparent and ethical standards for algorithmic monitoring within existing institutions. In other words, there is still no clear understanding on the part of government agencies regarding the use of artificial intelligence to ensure compliance with AML/CFT requirements.

4.3.2. Existing Crypto Regulation

Gradually, Kazakhstan is building a strong legal and regulatory system for cryptocurrency oversight and AML supervision. The Law on Digital Assets in the Republic of Kazakhstan (2023) officially defines virtual assets and specify the roles of key agencies, effectively limiting most crypto operations to the jurisdiction of the AIFC. Notably, this law prohibits the issuance and circulation of "unsecured" digital assets (i.e. cryptocurrencies not backed by assets) outside of the AIFC, at the same time allowing such activities within the AIFC under certain conditions (Unicase CA, n.d.). In other words, under the national legislation, operations with cryptocurrencies in Kazakhstan remain prohibited, but they are allowed within the regulated environment of the AIFC. This approach is in line with Recommendation 15 of the Financial Action Task Force, which stipulates that states should regulate and monitor the activities of virtual asset service providers (VASPs) by analogy with other financial institutions. At the same time, the AIFC regulators have developed their own anti-money laundering procedures that crypto investors must follow, which complements the requirements of national legislation.

Collectively, Kazakhstan's regulatory model in the field of cryptocurrencies generally complies with FATF standards, which provide for licensing, supervision, and compliance with AML/CFT requirements by crypto exchanges and other VASPs. At the same time, the AIFC actually acts as the center of regulated cryptocurrency activities in the country (FATF, 2023).

Institutional responsibility for supervision in the field of cryptocurrencies is distributed among several government agencies:

- **Financial Monitoring Agency (FMA)** - plays a key role in ensuring compliance with AML/CFT requirements at the national level and functions as a financial intelligence unit, receiving and analyzing suspicious transaction reports.
- **The National Bank of Kazakhstan** - monitors general financial flows and, in accordance with the latest legislative changes, has begun monitoring individual cryptocurrency transactions outside the AIFC, including licensing crypto exchanges to operate at the national level (Lightspark Team, 2025).
- **Astana Financial Services Authority (AFSA) -** is an independent regulator of the Astana International Financial Center (AIFC) and carries out licensing and control of all cryptocurrency companies operating within the framework of the AIFC. AFSA ensures that AIFC-based participants comply with international standards by applying strict AML/CFT requirements in line with global best practices (Lightspark Team, 2025).

Experts note that Kazakhstan's current approaches can be described as a dual regime with national governance within the framework of the AIFC innovation-oriented approach (Unicase Central Asia, n.d.). The advantage of this model lies in the possibility of conducting controlled experiments with blockchain analytics, fintech solutions and advanced compliance instruments in the jurisdiction of the AIFC, while maintaining restrictions on the broader domestic market. For example, the AIFC has tested several pilot programs related to asset trading and blockchain-based analytics under controlled conditions, without violating the general ban in the country.

To sum up, crypto regulation in Kazakhstan is gradually developing. Currently, most of the permitted crypto activity is concentrated within the framework of the AIFC, which is used as a controlled platform for the development of innovations. In the future, there will probably be a convergence of national and AIFC approaches, as well as clearer rules for the use of new technologies, including artificial intelligence, in financial monitoring.

4.3.3. Legal Gaps for AI Integration

While Kazakhstan's AML and crypto frameworks are fitting the international standards and are relatively well developed, the legal foundation for AI integration in financial monitoring remains incomplete, which poses a fundamental challenge for the AI integration into the monitoring system itself. Current AML and AIFC regulations are primarily designed for human decision-making and provide no guidance on the use, supervision, or accountability of algorithmic tools. Therefore, there are no binding provisions for accountability, data-sharing standards, or ethical safeguards in AI-assisted enforcement.

Experts interviewed for this study unanimously recognized this gap. One noted that there is still no clear rulebook on how the government can use AI for monitoring or what kind of data sharing is allowed. This reflects a broader international trend identified by the OECD (2022), which noted that AI often advances faster than the regulatory frameworks meant to govern it.

An additional limitation is the lack of a unified regulatory system for interagency data exchange. Currently, the Financial Monitoring Agency, the National Bank of Kazakhstan and the institutes of the Astana International Financial Center operate within separate information systems. Although there are cooperation agreements between them, they do not form a fully integrated platform for automated data analysis. This significantly limits the possibilities of using AI for predictive analytics and automatic identification of complex schemes covering several segments of the financial system at the same time.

In 2025, Kazakhstan adopted the first Law "On Artificial Intelligence", which laid down the general principles governing the use of AI in the country, including requirements for transparency, responsibility and data protection. However, this regulatory act does not contain industry-specific provisions governing the use of artificial intelligence in the field of financial monitoring. As a result, despite the importance of the adoption of this law, the practical issues of introducing AI into FMA activities still remain unresolved.

In general, legal gaps in the regulation of artificial intelligence form significant barriers to its integration into the financial monitoring system of Kazakhstan. The lack of specialized standards regarding monitoring algorithms, as well as insufficient regulation of centralized data exchange, limit the potential of AI solutions. Since these issues are resolved at the

regulatory level, the use of artificial intelligence in FMA activities will remain limited, which directly affects both the effectiveness and the economic feasibility of such solutions.

4.4. Economic Feasibility of AI Implementation

4.4.1. Overview

The economic sustainability of the introduction of artificial intelligence into the monitoring of cryptocurrency transactions by a Financial Monitoring Agency depends on whether the expected improvements in suspicious transaction detection, operational efficiency, and asset recovery exceed the associated economic and institutional costs. Expert interviews with representatives of the field of AML, digital governance and financial regulation show that Kazakhstan can justify such investments using a hybrid model combining commercial blockchain-analytical platforms and the step-by-step formation of its own technical competencies.

Commercial solutions such as Chainalysis, TRM Labs, and Elliptic provide functionality that is currently not available at the national level, including global address databases, cross-network transaction analysis, darknet market tools, and clustering algorithms that have been formed over the years. According to practicing financial analysts, such opportunities are difficult to reproduce in the short term, while they play a key role in the investigation of transnational crimes.

At the same time, complete dependence on external suppliers is not a sustainable solution in the long run. The development of internal AI modules makes it possible to adapt the analysis to national specifics, reduce dependence on third parties and form local competencies in the field of digital financial monitoring.

In this regard, this section provides an expanded economic analysis of two strategic scenarios: the use of ready-made software solutions (SaaS) from international providers or the development of its AI based platform with a full technology stack.

4.4.2. Cost components

4.4.2.1. Scenario A. Ready-made SaaS solutions (subscription)

The current document contains a basic cost estimate for vendor solutions. Below is a detailed analysis by provider and functionality.

Table 1: *Details of SaaS solutions by provider (annual cost, USD)*

Provider	Basic package	Advanced package	Key functions
Chainalysis Reactor	$120,000	$180,000	Tracing, clusterization
TRM Labs	$85,000	$140,000	Risk API, Forensics
Elliptic	$90,000	$150,000	Navigator, Lens
Crystal Blockchain	$60,000	$95,000	Analytics, Compliance
Coinfirm	$50,000	$80,000	AML Platform

sources: Semi-structured interviews with industry experts, conducted by the authors (2025); Vendr, (2025).

Table 1 shows the estimated annual subscription costs for SaaS platforms for analyzing cryptocurrency transactions. The information provided is based on expert interviews conducted as part of this study and reflects the practice of using such solutions, including in the AIFC ecosystem and the Financial Monitoring Agency of the Republic of Kazakhstan. The values are used exclusively for analytical comparison.

Table 2: *Full cost structure of the SaaS scenario (annually)*

Cost category	Minimum (USD)	Maximum (USD)	Note
Subscriptions to analytical platforms	$155,000	$320,000	2-3 providers
API integration and technical support	$25,000	$45,000	SLA Premium
Infrastructure (cloud, storage)	$40,000	$80,000	AWS/Azure
Staff (4-6 analysts)	$120,000	$180,000	System operators
Training and certification	$20,000	$40,000	Annually
Consulting and audit	$15,000	$35,000	Internal experts
Total	**$375,000**	**$700,000**	—

sources: Semi-structured interviews with industry experts, conducted by the authors (2025); Gigster, (2023, n.d.).

Table 2 shows the structure of annual costs when using the SaaS scenario. The "Minimum" and "Maximum" columns reflect the range of possible costs depending on the number of

connected providers, the selected subscription level, and the terms of service support. In addition to the cost of the licenses themselves, the calculation includes related costs necessary for the practical use of platforms in the activities of a government agency. The table is used to estimate the full annual budget burden, rather than individual cost items.

In general, cost analysis based on the SaaS scenario-A, shows that using ready-made analytical platforms allows for quick access to advanced monitoring tools for cryptocurrency transactions without significant initial investment. At the same time, the total annual costs are generated not only by the cost of subscriptions, but also by the associated costs of personnel, infrastructure and technical support, which makes this approach convenient in the short term, but financially sensitive for long-term use.

4.4.2.2. Scenario B: Developing FMA own solution

FMA's own development involves the creation of a full-fledged AI platform for monitoring cryptocurrency transactions from scratch, including data collection, infrastructure, ML models and user interfaces.

Table 3: *Capital expenditures for development (CAPEX)*

Stage / Component	Min. (USD)	Max. (USD)	Period, months	Staff size
1. Analysis and System Design	$80,000	$120,000	3-4	4-6
2. Data Infrastructure	$150,000	$250,000	4-6	5-8
- Blockchain nodes (BTC, ETH, etc.)	$40,000	$80,000	—	—
- Data lake and ETL pipelines	$60,000	$100,000	—	—
- Data enrichment (OSINT)	$50,000	$70,000	—	—
3. ML/AI Development	$200,000	$350,000	6-10	6-10
- Clustering algorithms	$50,000	$80,000	—	—
- Anomaly Detection models	$60,000	$100,000	—	—
- Risk Scoring Engine	$50,000	$90,000	—	—
- Graph Neural Networks	$40,000	$80,000	—	—
4. Platform and User Interfaces	$120,000	$200,000	4-6	5-7
5. Integration with Government Information Systems	$80,000	$150,000	3-5	4-6
6. Testing and Certification	$50,000	$100,000	2-3	3-5

Stage / Component	Min. (USD)	Max. (USD)	Period, months	Staff size
7. Pilot Deployment and Iterative Improvement	$40,000	$80,000	3-4	4-6
Total CAPEX	**$720,000**	**$1,250,000**	**18-24**	—

sources: Semi-structured interviews with industry experts, conducted by the authors (2025); Gartner, (2023).

Table 3 shows an estimate of the capital costs for developing its own FMA AI solution for monitoring cryptocurrency transactions. The data was generated based on expert interviews and discussions with AI platform developers. The table demonstrates the main stages of the system's development, starting from design and data infrastructure to model creation and integration with government systems, and is used to estimate the amount of initial investment.

Table 4: *Operating costs of the proprietary solution (OPEX, annually)*

Categories	Year 1–2 (USD)	Year 3–5 Costs (USD)
Support and Development Team (8–12 FTEs)	$280,000 - $400,000	$320,000 - $480,000
Cloud Infrastructure	$80,000 - $120,000	$100,000 - $150,000
Software and Data Licenses	$40,000 - $60,000	$50,000 - $80,000
ML Model Updates and Maintenance	$50,000 - $80,000	$60,000 - $100,000
Cybersecurity	$30,000 - $50,000	$40,000 - $60,000
Contingency Reserve (15%)	$72,000 - $107,000	$86,000 - $131,000
Total OPEX/annually	**$552,000 - $817,000**	**$656,000 - $1,001,000**

sources: Semi-structured interviews with industry experts, conducted by the authors (2025); Gartner, (2023).

Table 4 demonstrates the annual operating costs associated with the operation and construction of FMA AI-based solutions. These costs are due to the need for continuous system support, updating models, ensuring cybersecurity, and scaling computing resources as the amount of data grows.

The increase in costs in subsequent years reflects the increasing complexity of analytical models, the increasing burden on infrastructure, and the need to expand the team of specialists. These estimates allow us to take into account long-term obligations for the maintenance of the system and are used to analyze the financial stability of our own development.

4.4.2.3. Comparative analysis of total Cost of Ownerships (5-years)

The Total Cost of Ownership takes into account all direct and indirect costs over a 5-year period of operation.

Table 5: *Total cost of Ownership for 5 years*

Indicator	SaaS-model	Own development	Hybrid
Year 0 (Initial Investment)	$50,000	$720,000 - $1,250,000	$350,000
Year 1	$375,000 - $700,000	$552,000 - $817,000	$480,000
Year 2	$390,000 - $728,000	$574,000 - $850,000	$520,000
Year 3	$406,000 - $757,000	$656,000 - $1,001,000	$450,000
Year 4	$422,000 - $787,000	$682,000 - $1,041,000	$420,000
Year 5	$439,000 - $818,000	$709,000 - $1,083,000	$400,000
TCO 5 years	**$2.08M - $3.84M**	**$3.89M - $6.04M**	**$2.62M**
Average TCO/year	$416,000 - $768,000	$778,000 - $1,208,000	$524,000

sources: the author's own synthesis and analysis of primary interview data and secondary data.

A comparative analysis in **Table 5** shows that the SaaS model is convenient for a quick start and does not require large investments at the beginning, but over time leads to constant annual costs due to subscriptions and additional services. On the contrary, in-house development requires significant capital investments at the initial stage, while annually reducing costs as the technological architecture is implemented.

The hybrid approach was included in the analysis as a practical compromise between the two models. It reflects a realistic step-by-step implementation scenario in which ready-made SaaS solutions are used to quickly launch and gain experience, while the proprietary platform develops in parallel. This approach seems to be the most balanced: it helps to reduce overall costs over five years, reduce financial and operational risks, and at the same time gives time for gradual adaptation and phased implementation of the system.

4.4.3. Economic effect

4.4.3.1. Influence and stakeholders

The introduction of artificial intelligence-based cryptocurrency transaction monitoring systems primarily affects the Financial Monitoring Agency of the Republic of Kazakhstan,

which is a key stakeholder in this policy. For FMA and law enforcement agencies, the use of AI tools increases the effectiveness of detecting illegal transactions and reduces the burden on analysts. Law-abiding banks and cryptocurrency exchanges also benefit by reducing fraud and regulatory risks. Society as a whole benefits by reducing the financing of criminal activities and increasing the transparency of the financial system. The negative consequences of the introduction of such systems mainly affect criminal networks and illegal services, whose money laundering capabilities are significantly limited, which in the long term contributes to strengthening financial stability and economic development of the country.

Table 6: *Direct economic benefits*

The source of the effect	Who benefits	Mechanism	Estimated improvement	Probability
Increased detection of suspicious transactions (+40%)	State, society	Higher identification rate of illicit crypto flows	+30% to +50% increase	high
Reduction of investigation time (-60%)	Law enforcement	Reduced workload per case	–50% to –70%	high
Prevention of asset outflow	State, victims	Early intervention before funds leave jurisdiction	+20% to +40% asset retention	medium
Reduced FATF-related risks	Financial systems	Improved compliance & monitoring outcomes	Moderate to high risk reduction	medium
Personnel optimization	Public sector	Reduction of routine manual tasks	–20% to –30% routine workload	high
Total effect	**-**	**-**	**High positive systemic impact**	**—**

sources: the author's own synthesis and analysis of primary interview data and secondary data (OECD AML studies).

4.4.3.2. Strategic benefits

- Technological sovereignty: independence from geopolitical risks and sanctions pressure on Western providers
- Export potential: the possibility of commercializing the solution for the EAEU and Central Asian countries (potential market might reach of $50-100M)
- Development of the IT ecosystem: creation of 50-80 highly qualified jobs, development of competencies in the field of AI and blockchain
- Reputational effect: strengthening Kazakhstan's position as a regional fintech hub

4.4.4. Risk analysis

Table 7: *Risks of SaaS models*

Type of risks	Probability	Influence	Mitigation
Sanctions restrictions	Medium	Critical	Provider diversification
Increase in subscription costs (15–25% per year)	High	High	Long-term contracts
Data leakage via external APIs	Low	Critical	Encryption, security audits
Vendor lock-in	High	Medium	Multi-vendor strategy

Table 8: *Risks of Proprietary (In-House) AI Development*

Risks	Probability	Influence	Mitigation
Budget overruns (30–50%)	High	High	Agile approach, phased funding
Schedule delays (6–12 months)	High	Medium	MVP approach, buffer timelines
Loss of key specialists	Medium	Critical	Competitive salaries, retention
Technological lag behind the market	Medium	High	Partnerships, 15% R&D budget
Low quality of Money Laundering models	Medium	High	Benchmarking, external audit

sources: Semi-structured interviews with industry experts, Fortytwo Data. (2017, May 10).

In general the risk analysis has demonstrated that both SAAS models and own in-house development have different but manageable risks. SAAS models risks' are mostly external and revolving around vendor dependencies. Also, the further costs escalation and geopolitical barriers are the risks related to such models. On the other hand, in-house development might face internal risks such as budget overruns and technological limits. Additionally, the measures indicated in the tables imply that the risks can be reduced through phased implementation and planning. This risk profile was synthesized from the expert opinions acquired from the interviews and documental analysis. The given risks analysis provides a basis for assessing the most economically and institutionally feasible framework for the FMA. The following chapter reveals the conclusions of this study.

4.4.4.2. Conclusions

Based on the analysis, the Hybrid model is considered an economically advantageous option, the use of a phased hybrid strategy that combines the rapid deployment of SaaS solutions with the parallel development of in-house components.

A detailed phased strategy is provided below.

Phase 1 (Year 1): Quick Start

- Implementation of 2 SaaS platforms (Chainalysis + TRM Labs or Elliptic) - $200,000-350,000
- Establishment of an internal team (4-6 specialists) - $120,000-180,000
- Launch of an in—house pilot (analysis and design) - $80,000-120,000

Phase 2 (Year 2-3): Development of own competencies

- Development of basic ML modules (clustering, anomaly detection)
- Creation of own data infrastructure
- Gradual reduction of dependence on vendors (-30%)

Phase 3 (Year 4-5): Technological autonomy

- Launch of a fully functional proprietary platform
- SaaS - only for highly specialized functions (darknet intelligence)
- Preparation for exporting the solution to the countries of the region

Key success factors

- Personnel: Attracting at least 3-4 senior specialists with experience in blockchain analytics and ML on competitive terms
- Data: Providing access to data from the National Bank of the Republic of Kazakhstan, ICRIAP, tax authorities through a single exchange platform
- Partnerships: Concluding agreements with Astana Hub, AIFC, leading universities (Nazarbayev University, KBTU)
- Governance: Creation of an interagency coordinating council on AI in financial monitoring

Based on the findings, the following Discussion section interprets the results in the context of research issues, as well as discusses their practical and institutional implications for the implementation of the hybrid model and ensuring its effective and sustainable implementation.

5. Discussion

A comprehensive analysis of technological, regulatory and economic factors made it possible

to assess how realistic the introduction of artificial intelligence into the Financial Monitoring Agency's cryptocurrency transaction monitoring system is. In general, we can talk about the partial readiness of the country to use AI: the basic institutional and analytical elements have already been formed, but their development is still limited by infrastructural, legal and personnel factors.

From a technological point of view, AFM already uses a number of digital tools to analyze cryptocurrency transactions. The work uses a hybrid approach in which analysts use both internal tools and separate commercial platforms such as Chainalysis and TRM Labs. These solutions allow you to track suspicious transactions and analyze individual cases, including operations related to the darknet. However, the lack of a unified data infrastructure, limited computing resources, and a shortage of AI specialists in the public sector are holding back further development of the system. At the current stage, existing tools are suitable for investigating individual cases, but so far, they do not allow us to switch to predictive analytics and real-time monitoring.

A similar situation is observed in the field of regulation. Kazakhstan's legislation in the field of countering money laundering and regulating the activities of virtual asset service providers through the AIFC generally complies with international standards, including FATF recommendation 15. The creation of a specialized Crypton unit in the AFM structure, as well as the implementation of the Digital Kazakhstan program, indicate the government's desire to modernize government capacity. At the same time, there are no specific provisions in the current regulatory framework governing the use of AI, including issues of responsibility, transparency, and data exchange. This does not block the introduction of technologies, but it makes a gradual and pilot approach more appropriate.

Economic calculations show that the most rational option is a phased hybrid implementation model. Full focus on commercial solutions allows you to get results quickly, but increases dependence on external suppliers. Developing a fully proprietary AI system, on the contrary, requires significant costs and does not guarantee quick returns. The hybrid approach, which uses vendor platforms and at the same time forms a small internal team, allows achieving economic efficiency within one to two years and gradually building up national competencies. This option is better suited to the current budget opportunities and strategic goals of Kazakhstan's digital development.

In general, three key conclusions can be identified:

First, the results indicate that the Financial Monitoring Agency of the Republic of Kazakhstan's readiness to implement AI in financial monitoring is immature, reflecting ongoing progress alongside existing technological and institutional limitations.

Second, the results indicate that the existing legal and regulatory framework in Kazakhstan significantly strengthens oversight of the cryptocurrency sector in accordance with FATF standards, but does not provide a fundamental legislative basis for the implementation of artificial intelligence tools. Specifically, the lack of clearly defined AI governance standards and data exchange mechanisms limits the scale and pace of its implementation.

Third, the results suggest that the Financial Monitoring Agency can only consider a phased implementation of AI. Given current economic, informational, and institutional constraints, large-scale implementation of AI would be economically unjustified and would likely result in increased costs without commensurate benefits. As demonstrated in the results, gradual implementation allows the Agency to manage financial risks while simultaneously establishing the necessary technological and regulatory framework.

Based on this, the next chapter is devoted to practical recommendations aimed at the phased implementation of AI solutions in the AFM, reducing risks and strengthening the long-term sustainability of the financial monitoring system.

6. Policy Recommendations

Despite current laws that enforce the cryptocurrency monitoring in Kazakhstan, the integration of AI into financial monitoring is limited by the lack of clear rules of AI regulation, fragmented data and shortage of experts in AI. Thus, it is feasible to introduce phased AI integration, starting with institutional and legal measures, gradually moving to the development of the infrastructure and human capital.

6.1. Legal and regulatory measures

For the FMA to be able to start using artificial intelligence in financial monitoring, it is vital to have a clear legal foundation. Currently, existing laws reinforce the control over cryptocurrencies, without having precise and clear rules on applying AI. That is why AI integration should start with legal measures.

The new law on AI or in the amendments to the current acts shall ensure the following:

- **Allow the use of AI** by government agencies for AML/CFT purposes, including monitoring cryptocurrency transactions;
- **Reinforce the human control principle:** AI merely helps to analyse data, while humans make final decisions;
- **Ensure transparency:** AI results must be verifiable and explainable;
- **Define accountability:** it must be clear which agencies and officials are responsible for the use of AI;
- **Allow interdepartmental data exchange** among FMA, the National Bank, AIFC and law enforcement agencies, given the compliance with security requirements;
- **Establish data protection and cybersecurity requirements;**
- **Provide a pilot mode** which allows testing AI solutions in a limited format (e.g. through the AIFC sandbox).

These measures create a foundation that allows FMA to start introducing phased AI integration without risking legislation violations or incurring excessive costs.

6.2. Data and Infrastructure

The findings of the research show that without high quality data and sufficient computing resources, the usage of AI would be limited and inefficient. Thus, before the full-scale AI adoption it is necessary to create basic technical infrastructure that could work with data in near real time.

It is recommended to:

- Create a unified secure data environment which covers:
    - suspicious transactions reports,
    - crypto platform reporting,

  - banking and payment data (within the law),
  - blockchain data and analytics tools.
- Introduce unified data and information exchange standards between the banks, FMA, VASPs and other agencies.
- Ensure sufficient computing power (government cloud or national data centers).
- Strengthen cybersecurity, including access control, encryption and transaction logging.
- Employ national IT-infrastructure in order to decrease dependency on external providers and improve digital sovereignty.

6.3. Human capital and organisational readiness

Even with the presence of legislation and infrastructure, AI will not be efficiently employed without qualified specialists and integrated working processes.

It is recommended to:

- Create a small, dedicated AI and analytics team (or expand existing ones), involving data, machine learning, blockchain and AML specialists in the FMA.
- **Launch practical learning programmes**:
  - for analysts - on working with AI and reducing false positives
  - for IT staff - on data and model support,
  - For supervisors - on AI projects and risk management.
- Provide mechanisms to retain specialists in the public sector (career development, skill-based bonuses, project involvement).
- Adapt internal FMA procedures in a way that AI tools would be integrated in the investigation and reporting processes, rather than separate usage.

6.4 Economic effects of phased AI integration

The study's results show that the economic benefits of implementing AI into FMA's activities will not emerge immediately, but rather develop gradually as the implementation progresses and institutional readiness increases. The biggest impact is forecasted to be achieved with a hybrid implementation model over a 3-5 year period.

Key economic benefits identified through Findings.

1. Using AI tools for preliminary transaction analysis and anomaly detection can reduce the amount of manual work required by analysts by 30-50%.

   The economic effect is achieved through:

   - eliminating the need for large initial investments in development and infrastructure;
   - gradually decreasing operating costs by reducing dependence on expensive private providers as the internal competencies grow.
   - Flexibility in the scale of implementation, allowing costs to be adjusted depending on the actual effectiveness of AI tools and budgetary constraints.
2. Automated transaction clustering and risk prioritisation can reduce the processing time of a single case by 30-40%, increasing the overall throughput of the FMA without increasing the budget.
3. More precise analytical selection allows for a 10-20% reduction in false alarms, decreasing the cost of ineffective checks and administrative burden.

List of references

Akhmetkerey, B., Issabayeva, S., & Bastaubayeva, A. (2019). The formation of the cryptocurrency market in the Republic of Kazakhstan: Opportunities and threats from the point of view of economic security. In *BASIQ International Conference Proceedings* (pp. 135–142). https://www.researchgate.net/profile/Ann-Katrin-Arp-2/publication/333902657_Study_on_European_funding_programmes_for_sustainable_development/links/5dbaf94d299bf1a47b05a8d3/Study-on-European-funding-programmes-for-sustainable-development.pdf#page=135

Akhtar, N., Khan, A., & Raza, M. (2023). Technological advancements and legal challenges to combat money laundering: Evidence from Pakistan. *Pakistan Journal of Humanities and Social Sciences, 11*(1), 473–483. https://doi.org/10.52131/pjhss.2023.1101.0365

Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control, 22*(2), 210–216. https://doi.org/10.1108/JMLC-12-2017-0074

Bains, P., Conde, G., Ravikumar, R., & Sonbul Iskender, E. (2025, October). *AI projects in financial supervisory authorities: A toolkit for successful implementation* (IMF Working Paper No. WP/25/199). International Monetary Fund. https://www.imf.org/-/media/files/publications/wp/2025/english/wpiea2025199-source-pdf.pdf

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change, 69*(2), 283–305. https://doi.org/10.1007/s10611-017-9756-5

Chainalysis. (2024). *The 2024 crypto crime report*. https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf

Chainalysis Team. (2023, July 21). *Bitfinex hack money launderers plead guilty* [Blog post]. Chainalysis. https://www.chainalysis.com/blog/bitfinex-hack-plea-july-2023/

Chen, Z., Van Khoa, L. D., Teoh, E. N., et al. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review. *Knowledge and Information Systems, 57*, 245–285. https://doi.org/10.1007/s10115-017-1144-z

Choo, K.-K. R. (2015). Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks? In D. L. K. Chuen (Ed.), *Handbook of digital*

currency (pp. 283–307). Academic Press. https://doi.org/10.1016/B978-0-12-802117-0.00015-4

Desmond, D. B., Lacey, D., & Salmon, P. (2019). Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. *Journal of Money Laundering Control, 22*(3), 480–497. https://doi.org/10.1108/JMLC-10-2018-0063

Diakonashvili, G., Arslan, M., & Faizulayev, A. (2022). Comparative analysis of cryptocurrency tax policies of Kazakhstan. In *KIRC Proceedings* (pp. 218–243). https://www.kimep.kz/about/files/2018/02/KIRC-2022-Proceedings-final-1.pdf#page=218

Dyntu, V., & Dykyi, O. (2018). Cryptocurrency in the system of money laundering. *Baltic Journal of Economic Studies, 4*(2), 75–81. https://doi.org/10.30525/2256-0742/2018-4-2-75-81

European Banking Authority. (2020, January). *EBA report on big data and advanced analytics* (EBA/REP/2020/01) [Report]. https://www.eba.europa.eu/sites/default/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf

European Central Bank. (2023). *Artificial intelligence and big data analytics for anti-money laundering supervision* (Occasional Paper Series No. 309). https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op309~3e8bb4e90a.en.pdf

Financial Conduct Authority. (n.d.). *Cryptoassets: Our work*. Retrieved December 24, 2025, from https://www.fca.org.uk/firms/cryptoassets

Financial Crimes Enforcement Network. (2019, May 9). *Application of FinCEN's regulations to certain business models involving convertible virtual currencies* (FIN-2019-G001) [Guidance]. U.S. Department of the Treasury. https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

Financial Crimes Enforcement Network. (2024, June 7). *FinCEN year in review for fiscal year 2023* [Press release]. U.S. Department of the Treasury. https://www.fincen.gov/news/news-releases/fincen-year-review-fiscal-year-2023

Financial Crimes Enforcement Network. (n.d.). *Alerts/Advisories/Notices/Bulletins/Fact sheets*. U.S. Department of the Treasury. Retrieved December 24, 2025, from https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets

Finance Magnates. (2025, October 8). *Kazakhstan Targets Illegal Crypto, 130 Platforms Closed, $17 Million Seized*. https://www.financemagnates.com/cryptocurrency/kazakhstan-targets-illegal-crypto-130-platforms-closed-17-million-seized/

Forbes.kz. (2023, October 9). *V Kazakhstane vpervye izyali "prestupnye" dengi v kriptovalyute* [In Russian]. https://forbes.kz/articles/v_kazahstane_vpervyie_v_istorii_izyyali_prestupnyie_dengi_v_kriptovalyute

Garnett, A. (2024). Cryptocurrency scams: 8 crypto cons to avoid. *Encyclopedia Britannica*. https://www.britannica.com/money/cryptocurrency-scams

Gartner. (2023). *Understanding AI pricing: Simple steps to manage costs.* White paper. https://www.gartner.com/en/articles/ai-pricing-tips-control-costs-effectively

Gigster. (2023, n.d.). *How much does it cost to develop artificial intelligence applications?* https://gigster.com/blog/how-much-does-it-cost-to-develop-artificial-intelligence-applications/

Inform.kz. (2024). *Kazakhstan shuts down illegal cryptocurrency exchange platforms and freezes crypto-assets*. https://www.inform.kz/en/kazakhstan-shuts-down-illegal-cryptocurrency-exchange-platforms-and-freezes-crypto-assets_a4153627

Narain, A. (2022, September). International Monetary Fund. Regulating crypto. *Finance & Development*. https://www.imf.org/en/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti

International Monetary Fund. (2023, June 23). *Artificial intelligence in financial supervision and anti-money laundering: Opportunities and challenges*. https://www.imf.org/en/Publications/WP/Issues/2023/06/23/Artificial-Intelligence-in-Financial-Supervision-and-Anti-Money-Laundering-535271

KPMG. (n.d.). *Five ways AI can help manage economic crime risk* [Webpage]. Retrieved December 24, 2025, from https://kpmg.com/uk/en/insights/ai/manage-economic-crime-risk-with-ai.html

Law on Digital Assets in the Republic of Kazakhstan, No. 193-VII (2023).*National law defining digital assets and regulating their circulation.https://adilet.zan.kz/rus/docs/Z2300000193*

Lightspark. (2025, Sep 7). *Is Crypto Legal in Kazakhstan? Regulations & Compliance for Cross-Border Payments*. Lightspark Knowledge Base. https://www.lightspark.com/knowledge/is-crypto-legal-in-kazakhstan

Lindsay, M. G. (2023). International rise of cryptocurrency: A comparative review of the United States, Mexico, Singapore, and Switzerland's anti-money laundering (AML) regulation. *South Carolina Journal of International Law and Business, 19*(2), 161–185. https://scholarcommons.sc.edu/scjilb/vol19/iss2/8

Lyeonov, S., Tumpach, M., Loskorikh, G., Filatova, H., Reshetniak, Y., & Dinits, R. (2024). New AML tools: Analyzing Ethereum cryptocurrency transactions using a Bayesian classifier. *Financial and Credit Activity Problems of Theory and Practice, 4*(57), 274–288. https://doi.org/10.55643/fcaptp.4.57.2024.4500

Obe, R. G. A., & Nay, F. A. (2022). Strategy to suppress corruption and money laundering in the digital age. *Journal of Digital Law and Policy, 2*(1), 41–52. https://doi.org/10.58982/jdlp.v2i1.302

OECD. (2025). *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*. OECD Publishing. https://www.oecd.org/en/publications/governing-with-artificial-intelligence_398fa287.htm

Proskurina, K. (2022). Astana International Financial Center: Features of the tax regime and legal regulation of cryptocurrency turnover. *Research Institute of Financial and Tax Law*, 179–183. https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/14066/1/K_Proskurina_Astana_International_Financial_Center.pdf

Subbagari, S. (2024). Counter measures to combat money laundering in the new digital age. *Digital Threats: Research and Practice, 5*(2), 1–13. https://doi.org/10.1145/3626826

Tengrinews.kz. (2023). *Illegal cryptocurrency exchange prosecuted in Kazakhstan*. https://tengrinews.kz/kazakhstan_news/illegal-cryptocurrency-exchange-prosecuted-480245/

The Financial Action Task Force. (2021). *Opportunities and challenges of new AML/CFT technologies*. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Russian-Opportunities-and-Challenges-of-New-Technologies-for-AML-CFT.pdf

U.S. Department of Justice, Office of Public Affairs. (2024, November 14). *Bitfinex hacker sentenced in money laundering conspiracy involving billions stolen cryptocurrency* [Press release]. https://www.justice.gov/archives/opa/pr/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen

U.S. Department of the Treasury. (2022, August 8). *U.S. Treasury sanctions notorious virtual currency mixer Tornado Cash* [Press release]. https://home.treasury.gov/news/press-releases/jy0916

Unicase Law Firm. (2023). *The law on digital assets and related regulations – emergence of mining law in Kazakhstan*. Unicase Law. https://unicaselaw.com/blog/the-law-on-digital-assets/

World Economic Forum. (2023). *The future of financial crime compliance: From rules-based to AI-driven systems*. https://www.weforum.org/reports/the-future-of-financial-crime-compliance/

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PLOS ONE, 11*(10), 1–27. https://doi.org/10.1371/journal.pone.0163477

Vendr. (2025). Chainalysis software pricing & plans 2025: See your cost. Vendr Marketplace Data. https://www.vendr.com/marketplace/chainalysis

Zolkos, R. (2022). AI integration in financial institutions: Overcoming barriers. *Financial Technology Review, 29*(2), 78–92.

Appendices

Appendix 1. Written Form of Consent (English version)

You are invited to participate in a research study entitled as Money Laundering through Cryptocurrencies

Procedures:

This interview aims to evaluate the current practices of the Financial Monitoring Agency of Kazakhstan in detecting and investigating suspicious cryptocurrency transactions. The study will also explore challenges and potential solutions related to the use of blockchain analytics tools. As a participant in this interview, you will be asked questions related to your role in monitoring suspicious transactions, the tools you use, challenges faced, and your views on potential improvements in monitoring cryptocurrency transactions.

Risks:

There are minimal risks associated with your participation in this interview. However, since the interview may discuss sensitive topics regarding financial monitoring practices, there is a possibility of emotional discomfort or unease when discussing challenges or failures in the monitoring process.

Potential Benefits:

Your input will help in identifying gaps and potential improvements in the financial monitoring system for cryptocurrency transactions in Kazakhstan. Moreover, the findings could contribute to the development of more effective tools and strategies for detecting financial crimes, which may positively impact regulatory practices and policies in the future

Compensation:

There is no financial reward for participation. However, at the end of the study, participants will be able to get acquainted with its results. To receive a copy of the final report, you can contact the contacts listed in the survey.

Confidentiality and Privacy:

- All responses will be treated with the strictest confidentiality.
- Your identity and personal information will remain anonymous and will not be linked to any published results.
- The data will be stored securely and only used for the purposes of this research.

Voluntary Nature of the Study:

Participation in this study is strictly voluntary, and if agreement to participation is given, it can be withdrawn at any time without prejudice.

Points of Contact. It is understood that should any questions or comments arise regarding this project, or a research-related injury is received, the Principal Investigator, *Olzhas Adilbekov, +7(778)688-84-75, o.adilbekov@nu.edu.kz*, should be contacted. Any other questions or concerns may be addressed to the Nazarbayev University Institutional Research Ethics Committee, resethics@nu.edu.kz.

Statement of Consent.

I,_____,

Give my voluntary consent to participate in this study.

The researchers clearly explained to me the background information and objectives of the study and what my participation in this study involves.

I understand that my participation in this study is voluntary. I can at any time and without giving any reasons withdraw my consent, and this will not have any negative consequences for myself.

I understand that the information collected during this study will be treated confidentially.

Signature: _____ Date: _____

Researcher:

Signed_____ Date_____

Appendix 2. Written form of Consent (Kazakh version)

Сізді «Криптовалюталар арқылы ақшаның жылыстауы» атты зерттеуге қатысуға шақырамыз.

Рәсім:

Сұхбаттың мақсаты — Қазақстанның Қаржылық мониторинг агенттігінің криптовалюталарды пайдалана отырып күмәнді операцияларды анықтау және тергеу жөніндегі қазіргі тәжірибелерін бағалау. Сонымен қатар зерттеу блокчейн талдау құралдарын қолданудағы мәселелер мен оларды шешу жолдарын қарастырады.

Сұхбат барысында сіздің күмәнді транзакцияларды бақылаудағы рөліңіз, пайдаланатын құралдарыңыз, кездесетін қиындықтар және криптовалюта операцияларын мониторингілеуді жақсартуға қатысты көзқарасыңыз туралы сұрақтар қойылады. Сұхбат шамамен 15–20 минутқа созылады.

Мүмкін тәуекелдер:

Сұхбатқа қатысу аз ғана тәуекелдерді қамтиды. Дегенмен, қаржылық мониторингке қатысты сезімтал тақырыптар талқыланатындықтан, кейбір сұрақтар сізде жағымсыз эмоциялар немесе қолайсыздық тудыруы мүмкін.

Әлеуетті пайда:

Сіздің пікіріңіз Қазақстандағы криптовалюта транзакцияларын қаржылық мониторинг жүйесін жетілдіруге көмектеседі. Сонымен қатар зерттеу нәтижелері қаржылық қылмыстарды анықтауға арналған тиімді құралдар мен стратегияларды дамытуға ықпал етіп, болашақтағы реттеу саясатына оң әсер етуі мүмкін.

Сыйақы:

Зерттеуге қатысқаныңыз үшін қаржылық сыйақы қарастырылмаған. Алайда зерттеу аяқталғаннан кейін қатысушылар оның нәтижелерімен таныса алады. Қорытынды есептің көшірмесін алу үшін сауалнамада көрсетілген байланыс ақпараты арқылы зерттеушілерге хабарласуға болады.

Құпиялық және дербестік:

Сіздің барлық жауаптарыңыз қатаң құпия сақталады.

Сіздің жеке басыңыз бен дербес деректеріңіз жарияланатын нәтижелермен байланыстырылмайды.

Барлық ақпарат қауіпсіз сақталып, тек осы зерттеу мақсатында ғана пайдаланылады.

Ерікті қатысу:

Зерттеуге қатысуыңыз толықтай ерікті түрде жүзеге асырылады. Сіз кез келген уақытта ешқандай теріс салдарсыз қатысудан бас тарта аласыз немесе тоқтата аласыз.

Байланыс ақпараты:

Егер зерттеуге қатысты сұрақтарыңыз туындаса немесе қатысу барысында қандай да бір зиян шексеңіз, жауапты зерттеуші — Олжас Әділбековке хабарласыңыз, телефон: +7 778 688 8475, email: o.adilbekov@nu.edu.kz.

Басқа сұрақтар бойынша Назарбаев Университетінің Зерттеу этикасы комитетіне хабарласыңыз: resethics@nu.edu.kz.

Келісім формасы:

Мен, _____,

осы зерттеуге ерікті түрде қатысуға келісім беремін.

Зерттеудің мақсаты мен зерттеуге қатысу барысындағы міндеттерім маған нақты түсіндірілді.

Зерттеуге қатысу ерікті екенін және кез келген уақытта ешқандай жағымсыз салдарсыз бас тарта алатынымды түсінемін.

Зерттеу барысында жиналған ақпараттың құпия сақталатынын түсінемін.

Қатысушының қолы: _____ **Күні:** _____

Зерттеуші:

Қолы: _____ **Күні:** _____

Appendix 3. Written form of Consent (Russian version)

Приглашаем принять участие в исследовании под названием «Отмывание денег с помощью криптовалюты».

Процедуры:

Цель интервью — оценить текущие практики Агентства финансового мониторинга Казахстана по выявлению и расследованию подозрительных транзакций с использованием криптовалют.

Также исследование рассмотрит существующие проблемы и возможные решения в применении инструментов анализа блокчейна.

В рамках интервью вам будут заданы вопросы о вашей роли в мониторинге подозрительных транзакций, используемых вами инструментах, трудностях, с которыми вы сталкиваетесь, а также о вашем мнении относительно возможных улучшений мониторинга криптовалютных операций. Интервью займет примерно 15–20 минут.

Риски:

Участие в интервью связано с минимальными рисками. Однако, поскольку обсуждаются чувствительные темы, касающиеся финансового мониторинга, возможно возникновение эмоционального дискомфорта или неприятных ощущений при обсуждении трудностей или неудач в процессе мониторинга.

Потенциальная польза:

Ваш вклад поможет выявить пробелы и определить пути совершенствования системы финансового мониторинга криптовалютных транзакций в Казахстане. Кроме того, результаты исследования могут способствовать разработке более эффективных инструментов и стратегий для выявления финансовых преступлений и позитивно повлиять на развитие регулирования в будущем.

Вознаграждение:

Финансового вознаграждения за участие не предусмотрено. Однако по завершении исследования участники смогут ознакомиться с его результатами. Чтобы получить копию итогового отчета, можно связаться с исследователями через контактные данные, указанные в анкете.

Конфиденциальность и приватность:

Все ваши ответы будут строго конфиденциальными. Ваша личность и персональные данные останутся анонимными и не будут связаны с опубликованными результатами. Все данные будут храниться в безопасности и использоваться исключительно в целях данного исследования.

Добровольное участие:

Ваше участие в исследовании полностью добровольное. Вы можете отказаться от участия или прекратить его в любой момент без каких-либо негативных последствий для вас.

Контактные данные:

Если у вас возникнут вопросы по поводу исследования или вы получите травму, связанную с участием в исследовании, пожалуйста, свяжитесь с ответственным исследователем — *Олжасом Адильбековым, телефон: +7(778)688-84-75, email: o.adilbekov@nu.edu.kz*.

По другим вопросам можно обратиться в Комитет по этике исследований Назарбаев Университета: resethics@nu.edu.kz.

Форма согласия:

Я,_____,

добровольно даю согласие на участие в этом исследовании.

Мне были четко объяснены цели исследования и мои обязанности в рамках участия. Я понимаю, что участие в исследовании является добровольным и что я могу в любой момент отказаться без каких-либо негативных последствий.

Я понимаю, что собранная в ходе исследования информация будет храниться конфиденциально.

Подпись: _____ **Дата**: _____

Исследователь:

Подпись _____ **Дата** _____

Appendix 4. Confidentiality agreement (English version)

I, _____, understand that I may have access to confidential information about participants.

By signing this statement, I am indicating my understanding of my responsibilities to maintain confidentiality and agree to the following:

I understand that names and any other identifying information about participants are completely confidential.

I will de-identify the documents for the investigators to ensure that the study is anonymous. No Dates (including, but not limited to: birth date, admission date, discharge date, date of death, date of dx, etc.) may be used or recorded. Specific Ages may be used and recorded only for subjects 89 years of age or less. Subjects > 89 years of age must be grouped as follows: "> 89 years old".

I agree not to divulge, publish, or otherwise make known to unauthorized persons or to the public any information obtained in the course of this research project that could identify the persons who participated in the study.

I understand that all information about participants obtained or accessed by me in the course of my work is confidential. I agree not to divulge or otherwise make known to unauthorized persons any of this information, unless specifically authorized to do so by approved protocol or by the local principal investigator acting in response to applicable law or court order, or public health or clinical need.

I understand that I am not to read information about participants, or any other confidential documents, nor ask questions of study participants for my own personal information but only to the extent and for the purpose of performing my assigned duties on this research project.

I agree to notify the local principal investigator immediately should I become aware of an actual breach of confidentiality or a situation which could potentially result in a breach, whether this be on my part or on the part of another person.

_____	_____	_____
Signature	Date	Printed name
_____	_____	_____
Signature of principal investigator	Date	Printed name

Appendix 5. Confidentiality agreement (Kazakh version)

Мен, _____, зерттеуге қатысушылар туралы құпия ақпаратқа қол жеткізуім мүмкін екенін түсінемін.

Осы құжатқа қол қою арқылы мен құпиялылықты сақтау жауапкершілігімді түсінетінімді растаймын және келесі тармақтармен келісемін:

Қатысушылардың есімдері мен басқа да жеке сәйкестендіру ақпараттары толықтай құпия болып табылады.

Мен зерттеу анонимді болуын қамтамасыз ету үшін құжаттарды тұлғасыздандырамын. Күндер (туған күні, ауруханаға түскен күні, шыққан күні, қайтыс болған күні, диагноз қойылған күні және т.б.) жазылмауы немесе қолданылмауы тиіс. Нақты жас тек 89 жасқа дейінгі қатысушылар үшін ғана көрсетілуі мүмкін. 89 жастан асқан қатысушылар «89 жастан үлкен» деп біріктірілуі керек.

Мен зерттеу барысында алынған және қатысушыларды тануға мүмкіндік беретін кез келген ақпаратты рұқсат етілмеген тұлғаларға немесе көпшілікке жария етпеуге келісемін.

Менің жұмысым барысында алынған барлық қатысушылар туралы ақпарат құпия болып табылады. Мен бұл ақпаратты тек мақұлданған хаттамаға сәйкес немесе жауапты зерттеушінің шешімімен, заңға, сот шешіміне, денсаулық сақтау немесе клиникалық қажеттілікке байланысты жағдайларда ғана жария етуім мүмкін.

Мен қатысушылар туралы ақпаратты немесе құпия құжаттарды өзім үшін оқымауым, жеке ақпарат алу мақсатында сұрақтар қоймауым керек. Мен мұны тек зерттеу жобасындағы өз міндеттерімді орындау мақсатында жасауым қажет.

Егер құпиялықтың бұзылғанын немесе бұзылуы мүмкін жағдайды байқасам, бұл өз тарапымнан болсын, басқалар тарапынан болсын, мен жауапты зерттеушіні дереу хабардар етуге келісемін.

_____	_____	_____
Қолтаңба	Күні	Аты-жөні
_____	_____	_____
Жауапты зерттеушінің қолтаңбасы	Күні	Аты-жөні

Appendix 6. Confidentiality agreement (Russian version)

Я, _____, понимаю, что могу иметь доступ к конфиденциальной информации об участниках.

Подписывая это заявление, я подтверждаю, что понимаю свою ответственность по соблюдению конфиденциальности и соглашаюсь со следующим:

Я понимаю, что имена и любая другая идентифицирующая информация об участниках являются строго конфиденциальными.

Я обезличу документы для исследователей, чтобы обеспечить анонимность исследования. Даты (включая, но не ограничиваясь: дата рождения, поступления, выписки, смерти, постановки диагноза и т. д.) не могут использоваться или записываться. Конкретный возраст может использоваться и записываться только для лиц в возрасте до 89 лет включительно. Лица старше 89 лет должны быть объединены в категорию: «старше 89 лет».

Я обязуюсь не разглашать, не публиковать и не передавать неуполномоченным лицам или общественности любую информацию, полученную в ходе данного исследования, которая может привести к идентификации участников.

Я понимаю, что вся информация об участниках, полученная или доступная мне в процессе работы, является конфиденциальной. Я обязуюсь не разглашать иным лицам такую информацию, если только это не разрешено утвержденным протоколом или ответственным исследователем на основании действующего законодательства, решения суда, либо по необходимости в сфере здравоохранения.

Я понимаю, что не должен читать информацию об участниках или другие конфиденциальные документы, а также задавать вопросы участникам исследования в личных целях, а только в рамках своих служебных обязанностей в данном исследовании.

Я обязуюсь немедленно уведомить ответственного исследователя в случае нарушения конфиденциальности или ситуации, которая потенциально может привести к такому нарушению, как с моей стороны, так и со стороны других лиц.

_____	_____	_____
Подпись	Дата	Ф.И.О.
_____	_____	_____
Подпись ответственного исследователя	Дата	Ф.И.О.

Appendix 7. Interview guide (English version)

Interview questions for employees of the Financial Monitoring Agency of the Republic of Kazakhstan (FMA) and experts in the field of cryptocurrency and financial monitoring:

1. Please tell us about your professional field and the extent to which you have encountered issues related to monitoring cryptocurrency transactions.
2. In your opinion, how relevant is the issue of money laundering through cryptocurrency in Kazakhstan at the current stage?
3. How would you assess the level of transparency in cryptocurrency circulation in Kazakhstan, and how, in your opinion, is the monitoring process organized?
4. How do you evaluate the compliance of Kazakhstan's current approaches with international standards or best practices in this field?
5. How would you assess the use of analytical tools and technologies for monitoring cryptocurrency transactions in Kazakhstan in terms of their availability and integration into daily work processes? Can you provide examples of publicly available or commonly used methods and technologies?
6. How would you evaluate the level of automation in the monitoring processes of cryptocurrency transactions in Kazakhstan? To what extent are analytical systems used, and to what extent is expert manual assessment involved?
7. What conditions or resources do you consider especially important for the effective implementation of cryptocurrency transaction monitoring (e.g., personnel, technologies, partnerships)?
8. In your view, are there any legal, technical, or organizational barriers that hinder the implementation of modern analytical tools (including foreign ones) for monitoring cryptocurrency transactions in Kazakhstan?
9. What development directions (e.g., technological solutions, legislative changes, organizational measures) do you consider the most promising for enhancing the effectiveness of preventing money laundering through cryptocurrency in Kazakhstan?
10. Are there plans to introduce new or specialized tools and technologies for monitoring and analyzing cryptocurrency transactions in Kazakhstan in the future?
11. Do you have any additional observations, opinions, or suggestions that may be helpful for this research?

Appendix 8. Interview guide (Kazakh version)

Қазақстан Республикасы Қаржы мониторингі агенттігінің (ҚМА) қызметкерлері мен криптовалюта және қаржылық мониторинг саласындағы сарапшыларға арналған сұхбат сұрақтары:

1. Кәсіби салаңыз және криптовалюта транзакцияларын бақылау мәселелерімен қаншалықты жиі айналысқаныңыз туралы айтып берсеңіз.
2. Сіздің ойыңызша, қазіргі кезеңде Қазақстанда криптовалюта арқылы ақшаны жылыстату мәселесі қаншалықты өзекті?
3. Қазақстандағы криптовалютаның айналымының ашықтық деңгейін қалай бағалайсыз және, сіздің ойыңызша, оның мониторингі қалай ұйымдастырылған?
4. Қазақстандағы қазіргі тәсілдердің халықаралық стандарттар мен үздік тәжірибелерге сәйкестігін қалай бағалайсыз?
5. Криптовалюта транзакцияларын бақылауға арналған аналитикалық құралдар мен технологиялардың қолжетімділігі мен күнделікті жұмыс процестеріне енгізілу деңгейін қалай бағалайсыз? Қолданылатын жалпыға ортақ немесе типтік әдістер мен технологиялардың мысалдарын келтіре аласыз ба?
6. Қазақстанда криптовалюта транзакцияларын бақылау процестерінің автоматтандырылу деңгейін қалай бағалайсыз? Бұл жұмыста аналитикалық жүйелер қаншалықты қолданылады және сарапшылардың қолмен жүргізетін бағалауы қандай рөл атқарады?
7. Криптовалюта операцияларын тиімді бақылауды жүзеге асыру үшін қандай жағдайлар немесе ресурстар ерекше маңызды деп санайсыз (мысалы, кадрлар, технологиялар, серіктестік)?
8. Қазақстанда криптовалюта транзакцияларын бақылауға арналған заманауи аналитикалық құралдарды (соның ішінде шетелдік) енгізуге кедергі келтіретін қандай да бір құқықтық, техникалық немесе ұйымдық тосқауылдар бар деп ойлайсыз ба?
9. Қазақстанда криптовалюта арқылы ақшаны жылыстатудың алдын алу тиімділігін арттыру үшін қандай даму бағыттары (мысалы, технологиялық шешімдер, заңнамалық өзгерістер, ұйымдық шаралар) ең перспективалы деп есептейсіз?
10. Болашақта Қазақстанда криптовалюта транзакцияларын бақылау мен талдауға арналған жаңа немесе мамандандырылған құралдар мен технологияларды енгізу жоспарлануда ма?
11. Осы зерттеу үшін пайдалы болуы мүмкін қосымша байқауларыңыз, пікірлеріңіз немесе ұсыныстарыңыз бар ма?

Appendix 9. Interview guide (Russian version)

Вопросы для интервью с сотрудниками Агентства финансового мониторинга Республики Казахстан (АФМ РК) и экспертами в области криптовалют и финмониторинга:

1. Расскажите, пожалуйста, о вашей профессиональной сфере и о том, насколько вам доводилось сталкиваться с вопросами мониторинга криптовалютных транзакций.
2. На ваш взгляд, насколько актуальна проблема отмывания денег через криптовалюту в Казахстане на текущем этапе?
3. Как вы оцениваете уровень прозрачности оборота криптовалюты в Казахстане и каким образом, по вашему мнению, организован процесс её мониторинга?
4. Как вы оцениваете соответствие текущих подходов в Казахстане международным стандартам или передовому опыту в этой сфере?
5. «Как вы оцениваете уровень использования аналитических инструментов и технологий для мониторинга криптовалютных транзакций в Казахстане с точки зрения их доступности и интеграции в повседневные рабочие процессы? Можете ли привести примеры общедоступных или типичных методов и технологий, которые применяются?»
6. "Как вы оцениваете степень автоматизации процессов мониторинга криптовалютных транзакций в Казахстане? Насколько в этой работе задействованы аналитические системы, а насколько — экспертная ручная оценка?"
7. Какие условия или ресурсы, по вашему мнению, особенно важны для эффективной реализации мониторинга криптовалютных операций (например, кадры, технологии, партнерства)?
8. "Существуют ли, на ваш взгляд, какие-либо правовые, технические или организационные барьеры, которые затрудняют внедрение современных аналитических инструментов (в том числе иностранных) для мониторинга криптовалютных транзакций в Казахстане?"
9. Какие направления развития (например, технологические решения, законодательные изменения, организационные меры) вы считаете наиболее перспективными для повышения эффективности предотвращения отмывания денег через криптовалюту в Казахстане?
10. «Планируется ли в будущем внедрение новых или специализированных инструментов и технологий для мониторинга и анализа криптовалютных транзакций в Казахстане?
11. Есть ли у вас дополнительные наблюдения, мнения или предложения, которые могли бы быть полезны для этого исследования?

Appendix 10. Recruitment email

To the First Deputy Chairman of the
Financial Monitoring Agency of the
Republic of Kazakhstan
Mr. Ulan Ermukhanovich Raisov

From the Master's Students of the
School of Public Policy, Nazarbayev University
Contact phones: +7 (778) 688-84-75

Dear Mr. Raisov,

We are a group of master's students from the School of Public Policy at Nazarbayev University, conducting a research study on the challenges faced by the Financial Monitoring Agency (FMA) in monitoring cryptocurrency transactions, specifically focusing on the limitations posed by the lack of specialized blockchain analytics tools. Our study aims to assess the effectiveness of current practices, identify potential improvements, and offer recommendations to enhance the monitoring of suspicious cryptocurrency transactions in Kazakhstan.

As part of our research, we are planning to conduct interviews with experts in financial monitoring, and we would be honored if you could assist us by facilitating an interview with a relevant specialist from your Agency. The insights gathered from this interview will greatly contribute to our understanding of the FMA's current practices, challenges, and potential areas for improvement.

We kindly request that you recommend an appropriate specialist who could discuss the FMA's work in monitoring cryptocurrency transactions and share their views on the current challenges and the role of blockchain analytics tools in enhancing these efforts.

Your cooperation will play an invaluable role in the success of our study, and we greatly appreciate your time and consideration.

We look forward to your positive response and hope to engage in a constructive discussion.

Sincerely,

Olzhas Adilbekov