A Comparative Analysis of Legislative Criminal Policies in Iran and the United Kingdom in Addressing Cryptocurrency-Related Financial Crimes

1. Abbas Faghih: PhD Student, Department of Criminal Law and Criminology, Bushehr Branch, Islamic Azad University, Bushehr, Iran
2. Abbas Barzegarzadeh*: Assistant Professor, Department of International Law, Bushehr Branch, Islamic Azad University, Bushehr, Iran
3. Maryam Safaei: Assistant Professor, Department of Criminal Law and Criminology, Bushehr Branch, Islamic Azad University, Bushehr, Iran

*Correspondence: abbasbarzegar60@gmail.com

Abstract

This article is aimed at conducting a comparative analysis of the legislative criminal policies of Iran and the United Kingdom in the domain of financial crimes associated with cryptocurrencies. The principal objective is to identify the strengths and weaknesses of both legal systems and to offer practical recommendations for improving Iran's laws and legislative policies in confronting crypto-related offenses. The study employs a comparative legal research methodology along with legal analysis. The research is based on library sources, domestic and international laws and regulations, as well as the analysis of legal cases from both countries. Additionally, a descriptive-analytical approach is used to evaluate the impact of current laws on the prevention and control of cryptocurrency crimes. The findings indicate that the United Kingdom, through the Financial Conduct Authority (FCA) and international cooperation, has succeeded in developing a comprehensive framework for cryptocurrency oversight. This framework includes anti-money laundering (AML) requirements, know-your-customer (KYC) protocols, and the application of modern technologies such as blockchain analytics. In contrast, Iran, due to the absence of comprehensive legislation and weaknesses in institutional coordination, has been unable to effectively utilize cryptocurrencies in the prevention of financial crimes. To better manage cryptocurrency-related challenges in Iran, the formulation of clear legislation, enhanced coordination among regulatory bodies, and the integration of advanced technologies are deemed essential. The experience of the United Kingdom demonstrates that striking a balance between innovation and regulation can serve as an effective strategy for combating cryptocurrency-related crimes.

Keywords: Cryptocurrencies, financial crimes, legislative criminal policy, Iran, United Kingdom, anti-money laundering (AML), know your customer (KYC), cryptocurrency regulation.

Received: 28 November 2024
Revised: 18 January 2025
Accepted: 02 February 2025
Published: 27 February 2025

Citation: Faghih, A., Barzegarzadeh, A., & Safaei, M. (2025). A Comparative Analysis of Legislative Criminal Policies in Iran and the United Kingdom in Addressing Cryptocurrency-Related Financial Crimes. *Legal Studies in Digital Age,* 4(1), 1-10.

1. Introduction

In recent years, the emergence of cryptocurrencies as an innovation within the global financial system has brought about numerous opportunities and challenges. This novel technology, characterized by decentralization, anonymity, and the irreversibility of transactions, has created a revolution in the field of financial exchanges. Simultaneously, these same features have enabled criminals to exploit such tools for unlawful activities, including money laundering, terrorist financing, and cybercrimes. Consequently, regulation and policymaking in this area have become one of the principal challenges facing legal systems worldwide (Sadeghi & Naser, 2020).

Iran and the United Kingdom, as two countries with different legal and cultural systems, have adopted distinct approaches to financial crimes associated with cryptocurrencies. Iran has taken a cautious and restrictive stance, attempting to prevent potential misuse by enforcing stringent regulations. In contrast, the United Kingdom has adopted a balanced and adaptive approach, seeking to support innovation in financial technologies while simultaneously enacting comprehensive laws to prevent crimes (Papadaki & Karamitsos, 2021).

In the Iranian legal system, the absence of comprehensive and transparent laws regarding cryptocurrencies has created numerous challenges in regulatory efforts and the prevention of potential abuses (Javadi & Tajik, 2008). Although Iran's restrictive and prohibition-based approach seeks to prevent financial abuses, its effectiveness is undermined by the lack of supervisory infrastructure and institutional coordination. Conversely, the United Kingdom, through its adaptive approach, has sought to balance support for innovative technologies with combating crimes related to cryptocurrencies. This has been accomplished through the formulation of detailed and comprehensive regulations, including requirements related to know-your-customer (KYC) and anti-money laundering (AML) frameworks.

A major issue in cryptocurrency regulation in the United Kingdom lies in efforts to define the legal status of these digital assets within the framework of existing legal principles, while the decentralized and intangible nature of this technology has introduced new challenges. Since cryptocurrencies are not defined as "possessory objects" nor as "choses in action," the need for a new classification of personal property has emerged. The UK, drawing upon the flexibility of common law development, has endeavored to adapt swiftly to technological changes and has, through rulings such as *AA v Persons Unknown* and institutional reports like the UKJT Legal Statement, recognized cryptocurrencies as assets with unique characteristics such as identifiability and presumability. However, technical complexities and legal ambiguities still hinder full access to property rights in this domain, highlighting the need for targeted and harmonized legal reforms.

Nonetheless, both countries face challenges in combating the criminal use of cryptocurrencies, such as transaction anonymity, the absence of specialized regulatory bodies, and legal misalignment with technological developments. A comparative analysis of the criminal policies of Iran and the United Kingdom not only helps identify the strengths and weaknesses of these two legal systems but also provides a foundation for proposing effective recommendations to improve cryptocurrency regulation in Iran. This study aims to examine these challenges and offer practical solutions to enhance Iran's legislative policies in dealing with financial crimes related to cryptocurrencies.

This study is structured to provide a comparative analysis of the legislative criminal policies of Iran and the United Kingdom in addressing cryptocurrency-related financial crimes. Accordingly, it endeavors to analyze the legal and judicial frameworks of both countries, identify existing similarities and differences, and propose recommendations to strengthen Iran's domestic laws. The results of this research can assist policymakers and legislators in developing more effective policies in the field of cryptocurrencies and ultimately play a significant role in reducing financial crimes linked to this technology.

2. Theoretical Framework

2.1. Definition of Legislative Criminal Policy

Legislative criminal policy refers to the set of laws, regulations, and strategies adopted by legislative bodies for the prevention and combatting of crime and the regulation of criminal behavior in society. This policy constitutes the core of

criminal law and serves as a tool to determine the legal boundaries of criminal behaviors, types of criminal responses, and the implementation of criminal justice. In the contemporary era, emerging technologies such as cryptocurrencies—with their rapid evolution and inherent complexities—have posed new challenges to legislative criminal policies. For instance, cryptocurrencies, due to features like anonymity and decentralization, have not only opened new avenues for innovation but also become platforms for financial crimes such as money laundering and terrorist financing (Ibrahim, 2024).

From the standpoint of criminal law, legislative criminal policy plays a decisive role in defining, identifying, and responding to such crimes. It provides the framework within which criminal activities are identified, appropriate laws are drafted to address them, and relevant judicial procedures are established. For example, in China, strict policies regarding cryptocurrencies have been implemented, declaring their trading and mining illegal in order to maintain financial stability and control over the monetary system. In contrast, the European Union has taken a more balanced approach, attempting to support technological innovation while also safeguarding consumers and financial stability (Zhelekhovska, 2023).

2.2. Types of Criminal Policies in the Field of Cryptocurrencies

1. **Legislative Criminal Policy:** Legislative criminal policy involves the creation and enactment of laws and regulations that establish a legal framework for regulating activities associated with cryptocurrencies. This type of policy provides the fundamental basis for preventing crimes related to digital assets. For instance, China has implemented a full ban on cryptocurrency transactions and mining in an effort to curb financial abuse, while the European Union has developed a more balanced framework through comprehensive legislation such as the *Markets in Crypto-Assets Regulation* (MiCA) (Zhelekhovska, 2023).
2. **Judicial Criminal Policy:** Judicial criminal policy refers to the interpretation and enforcement of laws through the judicial system. Courts play a pivotal role in determining how laws are applied to cryptocurrencies. In certain jurisdictions, cryptocurrencies are recognized as assets or financial instruments, and this interpretation can have a significant impact on cases involving financial crimes. For instance, UK courts have acknowledged cryptocurrencies as legal property, thereby facilitating regulatory measures and investor protection (Trozze et al., 2022).
3. **Participatory Criminal Policy:** This policy emphasizes the participation of various stakeholders, including the government, private companies, and civil society, in the formulation and implementation of criminal policies. Such an approach ensures that legislative policies are developed in alignment with practical realities and market needs. The European Union, through consultations with industry stakeholders—including cryptocurrency exchanges and consumer rights groups—has presented a successful example of participatory criminal policy (Zhelekhovska, 2023).

The complexity and dynamic nature of cryptocurrencies require a multi-dimensional approach to legislative criminal policy. On one hand, laws must be sufficiently comprehensive and stringent to prevent financial crimes and potential misuse. On the other hand, these laws must be flexible enough to adapt to technological advancements and market demands. For example, various countries should draw from China's experience in combating financial crimes and from the European Union's approach to regulating innovation to establish a balance between regulation and support for innovation (Gofur & Sumedang, 2024).

Such a policy, in addition to preventing financial abuse, can enhance economic stability, protect consumer rights, and ultimately provide a conducive environment for the sustainable growth of emerging technologies.

2.3. Specific Characteristics of Cryptocurrencies

Cryptocurrencies, due to characteristics such as decentralization, anonymity, and the irreversibility of transactions, have had a significant impact on financial crimes and money laundering. Decentralization allows transactions to occur without the supervision or approval of government authorities, making both tracking and regulation of these activities more complex for law enforcement (Nadir Babazade & Baku State University, 2022). This feature particularly reduces regulatory control and provides a favorable space for financial abuse.

Anonymity, as one of the key characteristics of cryptocurrencies, enables users to conduct financial transactions without revealing their identity. This creates significant challenges for law enforcement agencies in identifying and prosecuting offenders, as individuals can carry out illegal activities without leaving tangible traces (Dyntu & Dykyi, 2018; Verma, 2024).

Beyond facilitating money laundering, this anonymity also contributes to the commission of crimes such as terrorist financing and fraud.

The irreversibility of transactions is another serious challenge in managing abuses associated with cryptocurrencies. Due to the absence of a central authority capable of freezing or reversing illegal transactions, recovering funds after their transfer becomes exceedingly difficult (Boyko et al., 2022). This increases the security of cryptocurrency use for criminals and makes these assets an attractive tool for illegal activities.

In addition, the lack of a unified legal framework and the rapid technological developments in the field of cryptocurrencies further compound these issues. These factors have significantly complicated the development of effective anti-money laundering measures and have increased the risks associated with cryptocurrency usage (Meszka, 2023). Despite these challenges, innovative solutions such as blockchain analytics and international cooperation are being explored and implemented as tools to mitigate risks (Boyko et al., 2022). However, the persistent anonymity and decentralization of cryptocurrencies continue to create substantial barriers for regulatory authorities across the globe (Dyntu & Dykyi, 2018; Verma, 2024).

These characteristics highlight the urgent need for comprehensive criminal policies and advanced regulatory mechanisms to support technological innovation while countering potential misuse.

3. Legislative Policies of Iran in Confronting Cryptocurrency-Related Financial Crimes

3.1. The Status of Cryptocurrencies in Iran's Legal System

Legal Prohibitions and Central Bank Regulations

Iran has faced multiple challenges in confronting cryptocurrencies and has adopted various criminal and legislative policies since the emergence of this technology. Cryptocurrencies were initially perceived as a disruptive phenomenon resistant to governmental oversight, with their decentralized and anonymous nature making them particularly attractive tools for economic offenders such as money launderers and fraudsters.

Until recent years, Iran's approach toward cryptocurrencies has largely been restrictive. In 2017, the Central Bank of the Islamic Republic of Iran officially banned the use of cryptocurrencies within the national financial system, primarily due to concerns related to money laundering and terrorist financing. However, technological developments and the widespread global use of cryptocurrencies compelled Iran to reassess its policies. In 2018, the Central Bank issued a formal statement prohibiting the use of cryptocurrencies for payments and fund transfers within the financial system. This decision was made due to concerns about the risks of money laundering, terrorist financing, and the lack of adequate oversight of crypto-related transactions.

The Central Bank has conditionally permitted cryptocurrency mining and use as a decentralized financial instrument, but strictly prohibited the use of cryptocurrencies for commercial transactions and payments. In several official statements, the Central Bank emphasized that cryptocurrencies cannot replace the national currency and their use must be strictly supervised (Emam et al., 2022). Despite these efforts, Iran still lacks a comprehensive and transparent legal framework for managing and regulating cryptocurrencies. The absence of clear laws, coupled with international sanctions, has led many crypto-related activities in the country to be conducted underground. This situation reveals the critical need for the development of enforceable regulations and the adoption of advanced technologies to monitor and combat cryptocurrency-related crimes.

Restrictions on the Use of Cryptocurrencies in Domestic Payments

The use of cryptocurrencies for domestic payments in Iran has been completely prohibited. According to the regulations and directives of the Central Bank, no company or individual is permitted to use cryptocurrencies as a payment tool in commercial or service transactions. This decision aims to maintain governmental control over monetary policy and prevent threats stemming from financial and economic instability.

Specifically, under the Central Bank of Iran's directives, no natural or legal person is allowed to use cryptocurrencies as a payment instrument in commercial transactions or service provision. This prohibition is in line with the Central Bank's policy to control national monetary flows, prevent money laundering and terrorist financing risks, and avoid economic instability. This legal stance is based on domestic bylaws such as the "Crypto Asset Guidelines and Requirements" (2018), which emphasize that mined cryptocurrencies may only be used for importing goods, and exclusively through authorized exchanges,

in compliance with national foreign exchange regulations. In particular, the Central Bank's instructions have banned cryptocurrency transactions for domestic payments and declared any use of them as payment tools illegal.

Moreover, cryptocurrency exchanges operating in Iran are only permitted to exchange cryptocurrencies with foreign currencies, and no domestic payment transactions are accepted by these exchanges. Unauthorized exchanges or any crypto-related activities operating outside the regulatory framework of the Central Bank are subject to legal prosecution. This approach is similar to the policies of certain other countries, such as China, which also prohibits cryptocurrency use for payments but has established a legal framework for mining activities. For example, in Iran, cryptocurrency mining is permitted with licenses from the Ministry of Industry, Mine and Trade, and with electricity priced at export tariffs, yet the use of mined cryptocurrencies for domestic payments remains illegal.

These restrictions, combined with the lack of comprehensive and clear laws regulating crypto-related activities, have created an ambiguous environment for actors in this field. Many users and investors face risks such as the lack of legal recognition for their crypto assets, potential confiscation or freezing of funds, and legal challenges. Additionally, the absence of a precise legal definition for cryptocurrencies and the manner in which they can be used within the national legal framework hinders the development and optimal utilization of blockchain technology and cryptocurrencies.

3.2. Legal Challenges of Iran in Regulating Cryptocurrencies

Absence of Comprehensive and Transparent Laws

One of the major legal challenges facing Iran in the regulation of cryptocurrencies is the absence of comprehensive and transparent legislation in this domain. Despite the increasing use of cryptocurrencies and the growth of their associated markets, the country's legal system has not yet established a clear legal framework to define and regulate cryptocurrency-related activities. This legal vacuum has placed many crypto-related activities in a legal gray area—neither explicitly lawful nor unlawful.

This legal ambiguity has led to several issues, including the inability to identify and manage illicit activities involving cryptocurrencies, such as money laundering and terrorist financing. Moreover, the lack of a precise legal definition of the nature of cryptocurrencies and their associated activities has increased the potential for misuse and hindered the establishment of a proper legal infrastructure to support the development of this sector.

Anonymity of Transactions and Challenges in Identification and Oversight

The anonymity feature of cryptocurrency transactions represents another fundamental challenge in regulating this field. In crypto systems, the identities of the sender and receiver remain fully anonymous, making it extremely difficult for regulatory bodies to monitor and identify users and transactions.

This anonymity has created a conducive environment for financial abuses, such as money laundering and terrorist financing. Due to the lack of advanced technologies and appropriate legal tools for analyzing and tracking cryptocurrency transactions, judicial and law enforcement authorities in Iran face serious difficulties in dealing with crypto-related crimes.

In addition, the absence of coordination among various regulatory bodies and the lack of unified procedures for managing and controlling cryptocurrency transactions have created further regulatory obstacles. Currently, not only are the necessary tools for tracking and identifying suspicious transactions lacking, but the existing laws are also insufficient for effectively addressing crimes related to cryptocurrencies.

The absence of comprehensive laws and the anonymity of transactions are two major challenges that have severely hindered Iran's efforts to regulate cryptocurrencies. These factors have increased both legal and economic risks and impeded the development and optimal use of crypto-related technologies. To overcome these challenges, it appears essential to draft clear and comprehensive regulations, employ advanced technologies for monitoring and identifying transactions, and ensure coordination among supervisory institutions.

3.3. Legal Cases Related to Cryptocurrency Crimes in Iran

One of the prominent legal cases involving cryptocurrency crimes in Iran is the *Cryptoland Exchange* case, which attracted significant public attention in 2021. As one of the well-known domestic crypto exchanges, Cryptoland offered extensive

cryptocurrency trading services to Iranian users. However, due to the absence of a clear legal framework and allegations of financial misconduct, the exchange's operations were suddenly suspended and its CEO was arrested.

Case Description

In this case, the CEO of Cryptoland was accused of offenses such as money laundering, misappropriation of users' assets, and non-transparent financial management. Owing to the decentralized nature of cryptocurrencies and the lack of effective supervisory tools, identifying financial flows connected to these accusations and gathering sufficient evidence for prosecution proved to be extremely difficult. Furthermore, hundreds of users who had entrusted their assets to the platform suffered significant financial losses following its shutdown.

Legal and Judicial Challenges of the Case

The Cryptoland case highlighted several challenges in Iran's legal and judicial systems regarding cryptocurrencies:

- **Lack of Clear and Comprehensive Laws**: The absence of defined regulations made it difficult to determine the legal status of the exchange's operations or how to deal with potential violations.
- **Anonymity of Transactions**: The decentralized and anonymous nature of cryptocurrencies complicated the identification of illegal financial flows and the recovery of users' assets.
- **Lack of Coordination Among Regulatory Bodies**: The absence of unified procedures and coordination among the Central Bank, Judiciary, and other relevant institutions made the resolution of the case more complex.
- **User Losses**: The lack of legal protection frameworks for crypto users prevented the reimbursement of their financial losses.

Implications of the Case

The Cryptoland case, as one of Iran's largest crypto-related legal challenges, clearly demonstrated how the lack of comprehensive legislation and effective supervisory tools can create an uncertain and risky environment in this sector. The absence of transparent legal frameworks and strong regulatory institutions led to Cryptoland being perceived as a platform for suspicious and opaque activities. The arrest of the CEO and the suspension of the exchange's activities raised serious concerns regarding asset security and public trust in cryptocurrencies. This case also revealed that ineffective oversight could lead to the proliferation of financial crimes, including money laundering and fraud.

In this case, many Cryptoland users who had deposited their assets on the platform incurred significant losses and lost the ability to recover their funds. This situation exposed serious legal gaps in the protection of consumer and investor rights in the cryptocurrency sector. Furthermore, the lack of coordination between regulatory and judicial bodies compounded existing problems. The absence of clear and effective procedures for managing similar crises made the Cryptoland case a major legal and economic challenge for the country.

This case served as a critical wake-up call for Iranian policymakers and decision-makers, underscoring the urgent need to reform cryptocurrency regulation comprehensively. Establishing clear and specific laws that can define the nature of cryptocurrencies and related activities is the first necessary step. Additionally, coordination among institutions such as the Central Bank, Ministry of Economy, and Cyber Police can help reduce supervisory gaps and strengthen legal infrastructure. The Cryptoland case illustrated that general and restrictive prohibitions alone are insufficient to prevent financial crimes. Instead, a more comprehensive and preventive approach is required. To avoid the recurrence of similar challenges, developing a transparent legal framework and utilizing advanced monitoring technologies such as blockchain analytics appear essential. This technology could enable the tracking of suspicious transactions and the identification of illicit patterns. Moreover, educating and informing users and investors about the risks associated with cryptocurrencies and how to manage their assets securely can play a vital role in strengthening public trust. Despite the challenges it presented, the Cryptoland case created an opportunity to rethink policies and laws related to cryptocurrencies in Iran, highlighting that the development of this technology without proper oversight and legal support poses risks not only to users but to the national economy as a whole.

4. Legislative Policies of the United Kingdom in Combating Cryptocurrency-Related Financial Crimes

The legal system of the United Kingdom has adopted a progressive and balanced approach to cryptocurrencies, primarily overseen by the Financial Conduct Authority (FCA). This regulatory body seeks to maintain a balance between supporting

innovation in financial technologies and protecting consumers and market integrity through robust regulatory frameworks. Based on the Financial Services and Markets Act 2000 (FSMA 2000) and its amendments in 2020, the FCA has been recognized as the principal authority for supervising activities related to digital assets, and all cryptocurrency service providers are required to register with this entity. These regulations impose strict obligations regarding financial transparency, adherence to anti-money laundering (AML) standards, and the implementation of know-your-customer (KYC) policies, all of which are designed to prevent the misuse of cryptocurrencies in financial crimes (Tomanek & Rirsch, 2022).

Within the UK regulatory framework, AML and KYC regulations serve as key instruments for addressing risks associated with the anonymous and decentralized nature of cryptocurrencies. The Money Laundering Regulations 2017, developed in accordance with the Financial Action Task Force (FATF) recommendations, mandate that crypto exchanges and digital wallet providers comply with stringent AML and KYC obligations. These include verifying and recording users' identity information, reporting suspicious transactions, and maintaining financial records for a specified period. Furthermore, an amendment in 2020 expanded the scope of these regulations by requiring all digital asset-related businesses to operate under the direct supervision of the FCA. These regulations also compel exchanges to employ advanced technologies for identifying and analyzing suspicious transactions and utilize blockchain technology as a tool to enhance transparency.

In addition to national policies, the UK has been part of broader European initiatives for regulating digital assets. For instance, the European Union, through the Markets in Crypto-Assets Regulation (MiCAR), aims to establish legal clarity and reduce pseudo-anonymity in crypto transactions. This initiative has influenced the UK and strengthened its domestic regulatory frameworks. While these regulations are promising in terms of improving transparency and consumer protection, they have also faced criticism regarding their complexity and lack of coordination among different components. Such criticisms indicate that the UK may need to simplify its legal frameworks to improve accessibility and efficiency within the crypto market (Huang et al., 2021).

Under the Proceeds of Crime Act 2002, cryptocurrency service providers such as exchanges and digital wallets are obliged to adhere to stringent regulations to prevent involvement in money laundering and terrorist financing. This law requires crypto service providers to reinforce their internal systems for monitoring transactions and to report any suspicious activities to competent authorities, including the UK Financial Intelligence Unit (UKFIU). Moreover, KYC-related regulatory requirements compel companies to verify users' identities and accurately record transactional data. These measures help mitigate risks arising from the anonymity of crypto transactions and enable more effective monitoring of financial activities.

Despite the UK's significant efforts in cryptocurrency regulation, it still faces global challenges associated with this technology. One such challenge is the lack of a uniform and clear definition for digital currencies across different jurisdictions, which complicates compliance and enforcement efforts. While some countries have adopted strict regulatory approaches, the UK has pursued a cautious yet active strategy to integrate cryptocurrencies into its legal system while minimizing associated financial risks. This approach reflects an effort to maintain a balance between technological innovation and the management of financial crime risks (Fletcher et al., 2020; Huang et al., 2021).

In addition to its domestic measures, the UK has worked toward establishing a comprehensive regulatory framework for cryptocurrencies through international cooperation and the adoption of global standards, such as FATF recommendations. For example, the UK participated in shaping the MiCAR regulations within the European Union and has incorporated their principles into its domestic policies. This approach has strengthened oversight of international exchanges and cross-border transactions, thereby increasing global coordination. The UK also leverages blockchain analytics and advanced tools to detect suspicious patterns and financial crimes. These efforts have positioned the UK as a leading country in crypto regulation and oversight, striving to prevent cryptocurrency-related financial crimes through a combination of technology and stringent legal controls, while simultaneously facilitating innovation in this evolving domain.

4.1. The United Kingdom's Approach to Cryptocurrency Regulation

The United Kingdom's regulatory approach to cryptocurrencies focuses on regulated tokens and the precise classification of these assets. In its first regulatory guidance published in 2019, the Financial Conduct Authority (FCA) categorized tokens into three main groups: exchange tokens, security tokens, and utility tokens. This classification, based on the features and

intended uses of the tokens, provided a clear framework for regulating and managing the risks associated with each type (Malala & Adeyemo, 2024).

A prominent example is the case concerning security tokens designed to attract capital from retail investors. In this regard, the FCA has imposed strict regulatory measures to prevent potential abuses in initial coin offerings (ICOs). These measures include mandating transparency in the information disclosed to investors and overseeing the activities of exchanges dealing in regulated tokens (Motsi-Omoijiade, 2022). Despite these efforts, some analysts have criticized the UK's regulatory framework as insufficient and called for a more flexible approach and optimization of existing laws (Huang et al., 2021).

Distributed Ledger Technology (DLT)—the underlying infrastructure for many cryptocurrencies, including blockchain—plays a key role in the UK's regulatory approach. This technology enhances transparency and transaction security and serves as a powerful tool for detecting and preventing financial crimes such as money laundering and terrorist financing. The final report of the UK Cryptoassets Taskforce in 2019 emphasized the extensive use of DLT in financial services and demonstrated that this technology could support regulatory policy improvements while accelerating innovation in the financial sector (Maxson et al., 2019).

The UK government has also recognized the transformative potential of this technology in payment systems and digital contracts and has made substantial investments in its development. These investments include projects evaluating blockchain's capabilities in improving transparency in financial transactions and reducing regulatory costs (De Meijer, 2016; Xing, 2022).

Although the UK has made notable progress in cryptocurrency regulation, several challenges remain. One such challenge is the integration of innovative financial technologies (fintech) into the existing regulatory framework. Additionally, issues such as distributed governance and the management of digital assets, including Central Bank Digital Currencies (CBDCs), require closer examination and more immediate decision-making (Silva & Mira da Silva, 2022).

Overall, the UK's approach reflects a commitment to striking a balance between promoting innovation and ensuring robust oversight to protect consumers and maintain market integrity. By leveraging technologies such as blockchain and fostering international cooperation, the UK seeks to reduce the risks associated with cryptocurrencies while facilitating the adoption of this emerging technology (Oseni & Ali, 2019).

5. Comparative Analysis

5.1. Similarities

Emphasis by Both Countries on Preventing Money Laundering and Terrorist Financing

Both Iran and the United Kingdom, recognizing the decentralized and anonymous nature of cryptocurrencies, place special emphasis on the prevention of money laundering and terrorist financing in their legislative policies. Iran, through its anti-money laundering laws and its focus on transaction transparency, has aimed to prevent potential abuses in crypto transactions. However, due to weaknesses in enforcement and the lack of advanced supervisory tools, Iran continues to face significant challenges in this area.

By contrast, the UK, through the Financial Conduct Authority (FCA) and cooperation with the Financial Action Task Force (FATF), has developed more comprehensive regulations to address these threats. These regulations include strict anti-money laundering (AML) and know-your-customer (KYC) requirements, obliging cryptocurrency exchanges and users to provide clear identity information. These measures have positioned the UK as one of the leading countries in developing robust legal infrastructure to prevent money laundering and terrorist financing (Malala & Adeyemo, 2024).

Establishing Legal Frameworks for Monitoring Exchanges and Wallets

Iran's Approach to Monitoring Crypto Exchanges and Wallets

In Iran, although a complete regulatory framework for cryptocurrency exchanges and wallets has not yet been developed, institutions such as the Central Bank and Cyber Police (FATA) have taken steps to regulate and oversee this domain. According to Central Bank directives, crypto exchanges are required to obtain licenses and comply with anti-money laundering (AML) and terrorist financing regulations. While this requirement is a positive step, the lack of clear laws and coordination among various supervisory bodies has undermined the effectiveness of these oversight efforts. Additionally, the technological

infrastructure for identifying and tracking suspicious transactions remains weak, making effective supervision more difficult. For instance, some unlicensed exchanges have continued operating without any regulatory compliance, exposing users to serious financial and legal risks.

Iran also faces major challenges in identifying and monitoring suspicious cryptocurrency transactions due to its insufficient use of advanced technologies like blockchain analytics. Furthermore, the absence of a centralized regulatory body capable of implementing supervisory and legislative policies in a coordinated manner has resulted in many cryptocurrency-related activities remaining in a legal gray area. This underscores the need for drafting clear, comprehensive laws and establishing a centralized regulatory authority to improve oversight of cryptocurrency exchanges and wallets in Iran.

The UK's Legal Framework for Monitoring Crypto Exchanges and Wallets

In the UK, legal and regulatory frameworks for crypto exchanges and wallets have been thoroughly and precisely developed. The Financial Conduct Authority (FCA), as the primary regulatory body in this domain, has established clear regulations governing the operations of cryptocurrency exchanges. According to FCA regulations, exchanges are required to:

- **Formal Registration**: All crypto exchanges must register and obtain a license from the FCA. This process involves submitting financial transparency documentation and demonstrating technical capability to operate.
- **Compliance with AML and KYC Requirements**: Exchanges are obliged to collect users' identity information and regularly report suspicious transactions. These regulations are aligned with FATF international standards.
- **Transparency and Reporting of Activities**: Exchanges must regularly report their activities to the FCA. This includes reporting large and suspicious transactions, maintaining financial records, and providing them to competent authorities.
- **Monitoring of Crypto Wallets**: Users of cryptocurrency wallets are also subject to KYC and AML requirements, and exchanges are obligated to monitor their transactions and report any abnormal activities to the appropriate authorities.

Relevant Laws and Regulations in the UK

Under the UK Money Laundering Regulations 2017, all cryptocurrency exchanges are mandated to comply with financial transparency and anti-money laundering requirements. These regulations, developed based on FATF recommendations, emphasize the importance of customer identification, transaction record-keeping, and reporting of suspicious activities. In 2020, an amendment was added to these regulations, placing cryptocurrency exchanges under the direct supervision of the FCA.

One of the UK's legal advancements in this field is the use of modern technologies for tracking and analyzing cryptocurrency transactions. The FCA utilizes blockchain analytics tools to detect suspicious transactions and illegal activities. This technology has enabled the identification of money laundering and terrorist financing patterns and has significantly strengthened the UK's oversight of the crypto market.

The UK's experience in developing legal frameworks for overseeing crypto exchanges and wallets highlights the importance of transparency, advanced technologies, and institutional coordination in this area. While the UK has achieved substantial success by implementing precise regulations and leveraging innovative technologies, Iran still faces serious challenges in supervising and managing its cryptocurrency market. The lack of comprehensive laws, institutional coordination, and technological tools has reduced the effectiveness of oversight in Iran. By adopting and localizing the UK's approaches, Iran can improve its supervision and regulation of the cryptocurrency sector.

5.2. Differences

Iran's Restrictive Approach vs. the UK's Adaptive Approach

Iran has predominantly adopted a restrictive approach in dealing with cryptocurrencies. The Central Bank of Iran has prohibited the use of cryptocurrencies for domestic payments and has not provided a clear legal framework for crypto-related activities. This cautious stance stems largely from concerns related to money laundering, terrorist financing, and jurisprudential challenges such as *riba* (usury) and *gharar* (uncertainty in contracts).

In contrast, the United Kingdom has adopted a more adaptive and balanced approach. The Financial Conduct Authority (FCA) has sought to support innovation in the field of cryptocurrencies while establishing a transparent regulatory framework. This framework includes the precise classification of tokens, regulation of crypto exchanges, and the imposition of anti-money

laundering (AML) and know-your-customer (KYC) requirements. This difference in approach reflects the UK's effort to balance the benefits of innovation with the need to manage financial and legal risks.

Token Regulation in the UK vs. Absence of Specific Laws in Iran

The UK has issued regulatory guidelines that categorize crypto tokens into three main types and has developed specific regulations for each. These laws include requirements for information transparency, oversight of exchange activities, and consumer protection. For instance, security tokens fall under securities law, while exchange tokens are treated as payment instruments and require registration and financial compliance.

Iran has not yet introduced a clear definition or comprehensive regulatory framework for governing crypto tokens. The absence of specific legislation has placed many cryptocurrency-related activities in a legal gray area. For example, while cryptocurrency mining is permitted under special licenses, the use of cryptocurrencies in financial transactions or investments carries legal and judicial risks due to the lack of transparent regulation.

Technological Advancement and Oversight in the UK vs. Supervisory Limitations in Iran

The United Kingdom has utilized technologies such as blockchain analytics and distributed ledger technology (DLT) to apply effective oversight over cryptocurrency transactions. These technologies enable the tracking of suspicious transactions and reduce anonymity, thereby significantly aiding in the reduction of crypto-related financial crimes. Moreover, the UK's commitment to international cooperation—including engagement with the Financial Action Task Force (FATF)—has further strengthened its oversight capabilities.

Conversely, Iran struggles with significant supervisory challenges due to the lack of advanced technical infrastructure and weak coordination among regulatory bodies. These limitations have created an environment conducive to crimes such as money laundering and terrorist financing, undermining the effectiveness of Iran's regulatory policies. The key differences in how Iran and the UK approach cryptocurrency regulation are rooted in divergent priorities, infrastructures, and legislative strategies. The UK, through adaptive frameworks and advanced technologies, has succeeded in promoting innovation while maintaining effective oversight. In contrast, Iran, with its restrictive stance and absence of comprehensive laws, faces greater difficulty in managing the challenges associated with cryptocurrencies. These differences highlight the need for Iran to improve its regulatory infrastructure and develop comprehensive frameworks to better harness the potential of this emerging technology.

6. Conclusion

Although Iran and the United Kingdom share common goals in their criminal policies concerning cryptocurrencies—such as preventing money laundering and terrorist financing—they differ significantly in their approaches and implementation strategies. Iran, by adopting a restrictive policy, has focused more on banning the use of cryptocurrencies in domestic payments and on preventing potential violations. Meanwhile, the UK, through more comprehensive legal frameworks and an adaptive approach, has sought to capitalize on the opportunities offered by innovation in this domain while simultaneously mitigating financial crime risks. The UK's experience demonstrates that the use of modern technologies such as blockchain analytics and precise legal regulations can significantly enhance cryptocurrency oversight.

From the author's perspective, one of the most critical weaknesses in Iran's criminal policy is the absence of comprehensive and transparent laws, which has created an ambiguous and risky environment for actors in this field. In addition, the lack of institutional coordination and the absence of advanced supervisory tools have hindered the effective implementation of existing policies. In contrast, the UK, by classifying tokens clearly, requiring transparency from exchanges, and leveraging international cooperation, has succeeded in establishing an efficient framework for cryptocurrency management. Iran could reconsider its legal system by drawing on UK policies and adapt them to local conditions in order to formulate comprehensive regulations for managing cryptocurrencies.

In general, adopting an adaptive approach and developing comprehensive laws in Iran would not only improve risk management and reduce financial crimes but also pave the way for the sustainable development of emerging technologies. This will require close cooperation among various institutions—including the Central Bank, Judiciary, and Ministry of Industry, Mine, and Trade—as well as learning from the successful experiences of other countries. With such reforms, Iran could not only safeguard itself from the threats posed by cryptocurrencies but also benefit from their potential in advancing the digital economy.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all individuals who helped us do this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Boyko, A., Dotscenko, T., & Dolia, Y. (2022). Patterns of financial crimes using cryptocurrencies. *Socio-Economic Relations in the Digital Society*, *2*(44), 23-28.

De Meijer, C. R. W. (2016). The UK and Blockchain technology: A balanced approach. *Journal of payments strategy & systems*, *9*(4), 220-229.

Dyntu, V., & Dykyi, O. (2018). Cryptocurrency in the system of money laundering. *Baltic Journal of Economic Studies*, *4*(5), 75-81.

Fletcher, E., Larkin, C. J., & Corbet, S. (2020). Cryptocurrency regulation: Countering money laundering and terrorist financing. *Available at SSRN 3704279*.

Gofur, A., & Sumedang, S. A.-S. a. S. (2024). HUKUM DAN TEKNOLOGI. *Pengantar Ilmu Hukum*, 165.

Huang, H.-M., Chen, S., & Yu-xia, Z. (2021). An Analysis of China's International Competitiveness in Competitive Sports Industry by Means of Mathematical Modeling. *Converter*, 350-356. https://doi.org/10.17762/converter.186

Ibrahim, O. (2024). Cryptocurrency; the new unleashed financial instrument, should it be regulated. *Humanities Journal of University of Zakho*, *12*(2), 303-317.

Javadi, Y., & Tajik, A. (2008). Blockchain Based Technology and its Effect on Education in Iran. *International Journal of English Labguage*, *7*(4), 78-87.

Malala, J., & Adeyemo, F. (2024). Rethinking Crypto-Regulation for Crypto-Investors in the UK. In *Commercial Banking in Transition: A Cross-Country Analysis* (pp. 265-282). Springer.

Maxson, S., Davis, S., & Moulton, R. (2019). UK Cryptoassets Taskforce publishes its final report. *Journal of Investment Compliance*, *20*(2), 28-33.

Meszka, J. (2023). On modern crime – money laundering and cryptocurrencies. *Ius et Admini*, *45*(2-4), 5-17. https://doi.org/10.15584/iuseta.2021.2-4.1

Motsi-Omoijiade, I. D. (2022). *Cryptocurrency regulation: a reflexive law approach*. Routledge.

Nadir Babazade, T., & Baku State University, m. (2022). Kriptovalyuta əməliyyatlarinda çirkli pullarin yuyulmasi ilə mübarizənin hüquqi problemləri. *Scientific Research*, *10*(6), 55-59. https://doi.org/10.36719/2789-6919/10/55-59

Oseni, U. A., & Ali, S. N. (2019). Fintech in Islamic finance. In *Fintech in Islamic finance* (pp. 3-14). Routledge.

Papadaki, M., & Karamitsos, I. (2021). Blockchain technology in the Middle East and North Africa region. *Information Technology for Development*, *27*(3), 617-634.

Sadeghi, H., & Naser, M. (2020). Guaranteeing Ownership in the Evolutions of Registration Systems with a Comparative Study of the Registry System in Scotland, United Kingdom, United States and Iran. *Journal of Legal Research*, *19*(43), 267-296.

Silva, E. C., & Mira da Silva, M. (2022). Research contributions and challenges in DLT-based cryptocurrency regulation: a systematic mapping study. *Journal of Banking and Financial Technology*, *6*(1), 63-82.

Tomanek, S., & Rirsch, R. (2022). New Aml regulation: From 'virtual currency'to 'crypto assets'—differentiation from tokenised financial instruments and potential concerns over the perceived end of pseudonymity in the crypto sector. *Journal of Financial Compliance*, *5*(4), 350-358.

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*, 1-35.

Verma, H. (2024). The Impact of Cryptocurrency on Money Laundering Practices. *African Journal of Commercial Studies*, *5*(2), 51-60.
Xing, Y. (2022). Digital Currency Supervision Based on Blockchain Technology: A Literature Review. *SHS Web of Conferences*. https://doi.org/10.1051/shsconf/202214803030
Zhelekhovska, T. (2023). Legal regulation of cryptocurrency and cryptocurrency operations in the European Union. *Visegrad Journal on Human Rights*(6), 201-207.