



Regulating digital currencies in Jordan: Legislative gaps, legal challenges, and comparative insights

Mohammad Airout

Faculty of Law, Department of Law, Middle East University, Amman, Jordan

Abstract

This investigation explores the increasing legal and regulatory obstacles that digital currencies present in the Jordanian context. These obstacles are not only pressing, but they may also prove insurmountable in the absence of a suitable legal framework. This research demonstrates that the unique technological and legal challenges associated with digital assets are not adequately addressed by existing legislation, such as the Cybercrime Law and the Anti-Money Laundering and Counter-Terrorist Financing Law (AML/CFT). Certainly, it appears that these regulations were formulated with an alternative era in mind. They are unable to maintain pace with the rapid pace of technological advancement. This study also investigates the practical repercussions of having inadequate legal regulations and even fewer legal remedies to enforce them. The research quantifies and identifies some of the consequences, their significance in a predominantly cash-based society like Jordan, and the actions of some jurisdictions with more experience in this area in addressing these same issues through comparative analysis with similar laws and cases in other jurisdictions.

Keywords: Digital currencies, cryptocurrency law, Jordanian legal framework, blockchain regulation, cybercrime, anti-money laundering, financial technology (FinTech), comparative law, legal reform, virtual asset regulation.

Introduction

In recent years, the world has experienced significant transformations in numerous sectors, all of which can be attributed to the rapid progression of technology. The most thrilling of these developments for numerous individuals has been the emergence of digital financial technology, or FinTech in the current jargon. However, this is not merely an economic sector overhaul; it is a comprehensive reevaluation of the economy, with cryptocurrency serving as its foundation.

Legal and financial consequences of this creative approach have been notable. It has led to an unheard-of rise in capital movement and a systematic destruction of long-standing geographical and legal restrictions. Still, this technical wonder is less spectacular than it seems. It has problems; actually, there are several of them (Albalawee & Al Fahoum, 2023) ^[5].

Given this, it is absolutely necessary to reevaluate accepted legal and administrative systems. We must create a legislative framework if we are to control the usage of cryptocurrencies and minimize the hazards they generate. Many countries have passed laws intended especially to handle this problem. Their aim is to strike a balance between advancing this kind of digital innovation and maintaining the integrity of the financial and legal systems. In contrast, the Jordanian legal framework appears to have a significant legislative void in this regard. The legal status or use of cryptocurrencies has not yet been addressed by any specific legislation. This has had a detrimental impact on the ability of our judiciary and regulatory bodies to effectively address offenses that are committed in the digital currency sector (Magableh, 2024a) ^[20].

Despite the fact that the Central Bank of Jordan has issued numerous public warnings regarding the severe risks associated with crypto transactions, the absence of laws that explicitly regulate the use of these virtual currencies results in the act of buying, selling, and trading them being

classified as a vague and ambiguous legal matter. Actors who wish to regard cryptocurrencies as a cash-cow generator for illicit cyber-operations have discovered a substantial loophole to facilitate their nefarious objectives. The repercussions of this regulatory vacuum extend far beyond the mere appearance of the legality of these digital-assets-something-like-transactions. They directly interfere with the ability of law enforcement to conduct the intricate, cyber-investigative tasks that are necessary to safeguard the public from a new tide of high-tech, virtual-scale scams and frauds (Yousef, 2023) ^[30].

Subsequently, this investigation endeavors to evaluate the efficacy of Jordan's existing legal framework in prosecuting cryptocurrency-related offenses. The legal provisions that are intended to address these situations are examined to determine whether they are sufficient. If not, what is the reason? The study also examines the legal and technical challenges that Jordanian authorities encounter when attempting to identify, prosecute, and convict individuals who commit offenses using virtual currencies in a world that is becoming increasingly virtual. Particularly when it comes to determining the perpetrators of a crime, determining whether the accused, the prosecutor, or the judge are responsible for the offense, and obtaining the necessary virtual evidence to be admissible in a real-world courtroom (assuming that jurisdiction is even a meaningful concept in an online world).

In order to accomplish these objectives, the research must implement three interconnected methodological approaches. Initially, an analytical approach examines the legal texts from Jordan that are pertinent to financial crime and cybercrime. It evaluates the extent to which they are applicable to emergent issues that are linked to cryptocurrency. Secondly, a comparative analysis examines the legislative experiences of specific jurisdictions. These are jurisdictions that have already addressed the regulation of cryptocurrency and appear to possess pertinent

experience. This investigation assesses the appropriateness of these diverse legal systems for the Jordanian context and identifies their most effective practices. Lastly, legal induction is employed to formulate recommendations and derive conclusions from the analyses.

Theoretical Framework of Digital Currencies

An altogether new form of money is emerging: e-currencies, which are produced and circulated electronically, are not issued by a central authority. These currencies replicate the security found in traditional forms of money, operate on blockchain networks, and rely on encryption technologies (Al Nabhani *et al.*, 2025a) ^[2].

Bitcoin is the most well-known of the numerous varieties of digital currencies. Other varieties include central bank digital currencies (CBDCs) and asset-backed stablecoins. However, the Jordanian legal system has not established any distinctions between these categories or their types, and it has surely not clarified the legal nature of them. Consequently, the classification of the types of offenses that can be committed using these currencies or in which they are involved is a monumental task. Additionally, the term "classifying" refers to the labeling of these offenses as either legal or unlawful (Yousef, 2023) ^[30].

In terms of legality, digital currencies are distinguished by a variety of distinctive attributes. The initial and most critical of these is their decentralization. Subsequently, they provide users with virtually complete anonymity. Finally, they are characterized by the exceptional speed of cross-border transactions. Although digital currencies are a delightfully techno-libertarian method of executing any number of financial transactions due to these features, they are also potentially great for executing all types of financially criminal transactions. The sole issue is that there is no explicit legal foundation for the type of prosecution that would be necessary to ensure that regulatory and judicial initiatives are effective (Al-Naimi *et al.*, 2021) ^[9]. The objectives of Cybercrime Law No. 27 of 2015 are to address certain actions that are associated with the misuse of digital currencies. Nevertheless, these provisions address these behaviors in a rather indirect manner. It is not their intention to address these issues specifically (Ali & Mohammed, 2023) ^[8]. This is accurate regardless of the possibility that some of these provisions may be applicable in a limited number of targeted prosecutions. Accessing electronic systems without authorization is prohibited by Article 3. This could potentially be applicable in the context of digital wallet hacking, according to certain specialists. In the same vein, Article 4 criminalizes the use of information networks to perpetrate electronic fraud. This may be applicable in specific instances of digital currency fraud (Khater, 2024) ^[17].

The term "funds" is defined in the Anti-Money Laundering and Counter-Terrorist Financing Law No. 46 of 2007 as "all assets that have been acquired through criminal activity (Gaviyau & Sibindi, 2023) ^[13]."

Digital currencies may be encompassed by this definition in theory. Despite the existence of laws to combat money laundering and the financing of terrorism, digital currencies are not explicitly addressed, which undermines the quasi-legal foundation. This omission complicates matters regarding enforcement, prosecution, and evidentiary standards.

These observations demonstrate that the current Jordanian

legislative framework is inadequate for addressing the conditions of digital currencies, regardless of whether the focus is on legal definition, regulatory structure, or criminal qualification. This deficiency emphasizes the need of immediately passing new laws to fill in the gaps in present laws thus guaranteeing that we have clear and efficient rules for this new kind of "money (Magableh, 2024b) ^[21]."

Crimes Associated with Digital Currencies

Although Jordanian law does not clearly acknowledge digital currencies, their growing popularity on the internet has led to a range of activities that might be regarded illegal under our laws. Our first concern is the application of the law; so, we will react against any illegal activity, including those using digital currency. Several well-known Jordanian offices connected to the Attorney General have released comments claiming that linked activities—more especially, money laundering, electronic fraud, or terrorism funding—could be categorized as illegal. Actually, they are serious accusations with extremely weak basis that may land any person in legal hot soup (Shdaifat, 2023) ^[27].

Money laundering is one of the most severe offenses associated with digital currencies, and for good reason: these new forms of currency offer a degree of anonymity and concealment that is unparalleled by other financial instruments. Despite the fact that the Anti-Money Laundering and Counter-Terrorist Financing Law No. 46 of 2007 does not explicitly identify digital currencies as potential laundering instruments, the law's Article 2 adopts a broad definition of "funds." Funds are defined as "all assets derived from any illicit activity" by the law. This would appear to include digital assets, such as Bitcoin, if the illicit source of the asset could be reliably linked to the asset itself. However, the law is less effective in prosecuting the offenses that can be committed using electronic currency in the absence of a specific mention of it (Chitimira & Animashaun, 2023) ^[10].

The use of digital currencies has led to the emergence of increasingly sophisticated forms of electronic fraud. This fraudulent activity manifests in two primary ways: (1) the establishment of fraudulent platforms that falsely advertise the exchange of valuable digital tokens, and (2) the sale of nonexistent tokens that are intended to function as a form of digital currency but are in reality nothing more than a con artist's collection of hollow promises. The 2015 Cybercrime Law (No. 27 of 2015) contains a provision (Article 4) that specifically addresses the use of information networks or systems with the intent to defraud, which is what makes these crimes especially fascinating from a legal perspective (Koto, 2021) ^[18].

In the context of financing terrorism, digital currencies offer a highly effective method of transferring funds across borders while evading detection by financial system regulators. The law criminalizes the financing of terrorism in all forms; however, the lack of any references to modern financial instruments, such as digital assets, renders the enforcement necessary to halt this flow exceedingly challenging. And when discussing modern financial instruments that have been designed from the ground up to safeguard transaction data and user identity, Monero and Zcash immediately come to mind (Le Nguyen & Golman, 2021) ^[19].

The sum of these evaluations reveals that the current legislative framework, despite the existence of certain

general provisions, is inadequately equipped to address the distinctive and constantly changing nature of offenses associated with digital currencies. The current structure, which is comprised of extant laws and their provisions, is inadequate to address the issues involved with digital currencies.

The Jordanian Legal Framework

The Jordanian legal system does not now have a particular legislative framework to handle digital currencies. This covers their legal definition, circulation control, and criminalizing of their abuse. Without even a basic legislative framework, the lack of which is becoming a major cause of concern given the growing worldwide popularity of digital money and the appearance of many new forms of financial crimes linked with it (Albanki *et al.*, 2024) ^[6]. Right now, the Jordanian approach is distinguished by the Central Bank of Jordan's nonofficial recognition of digital currencies. With only a few cautions issued, the most prominent of which published in 2014, the bank has maintained a rather conservative posture and proclaimed that digital currencies are non-legal currency, therefore alerting the public of the hazards involved. Though risk warnings exist, the public has not been given a clear legislative framework that would offer direction on how to manage digital currencies while nevertheless remaining law-abiding compliant. Therefore, the absence of law-making in this domain creates a legal limbo that permits public interactions with digital currencies to persist, despite the fact that the public may be cautioned that they are unlawful and perilous. (Nawayiseh *et al.*, 2024) ^[24].

Law No. 27 of 2015 on Cybercrime does not explicitly mention digital currencies or encrypted assets at the legislative level. In the same vein, the Law No. 46 of 2007 on Combating Money Laundering and the Financing of Terrorism and its amendments do not explicitly define digital currencies as one of the monies that are employed to finance terrorism and perpetrate financial crimes. While Article 2 broadly defines "funds" as "all assets derived from criminal activity," the application of this definition to digital currencies is legally contentious (Khan *et al.*, 2022) ^[16]. In the preceding section, we demonstrated that the Jordanian legislator is currently in the preliminary phase. It appears to have been reduced to the issuance of general warnings and has not advanced to the stage of substantive legal regulation. This has resulted in the digital marketplace in Jordan being exposed to a broad range of risks. Additionally, it has rendered the state incapable of preventing the emergence of new forms of financial crime that are enabled by cyber technology from engaging in their most effective activities. It seems that these offenses are becoming increasingly associated with the development of new digital currencies. We are currently developing novel types of offenses that are not related to the traditional forms of financial crime that were previously regulated by the primary penal code.

Legal Challenges in Jordan

Jordan's legal framework is beset by numerous complications regarding digital currencies. Jordan's legal system is rife with several issues related to digital currency. This is mostly due to the fast speed of technological development and the growing range of both legal and illegal businesses running on digital currencies. Many different manifestations of this problem are clear-cut: technical

inability of implementing effective control at the currency level, institutional inadequacies of many entities engaged in monitoring, and lack of legislative clarity (Al Masadeh *et al.*, 2024) ^[11].

One of the difficulties is the lack of exact legislation controlling their use and clarifying digital currencies. The present legal framework—which consists of the Cybercrime Law, the Anti-Money Laundering Law, and the Central Bank Law—makes no reference of digital currencies. This suggests that none of those rules govern any behavior that would be relevant to those new "things" by default. As such, the legal categorization of actions involving these assets is somewhat vague. Those who are meant to be conducting or stopping the particular actions in issue object to ambiguous acts. They report grievances. This will hurt the company. The uncertainty also compromises the ability of the court to provide consistent and reasonable decisions (Rashid & Saleh, 2024) ^[26].

The evidence that is difficult to obtain in cases involving digital currencies is a second significant obstacle. Advanced encryption technologies are employed to operate these currencies. Additionally, they are allowing users to conceal their identities and conduct transactions that are not authorized by legitimate financial institutions. It is evident that the process of monitoring such transactions is highly technical and may be beyond the current capabilities of the majority of our law enforcement agencies. Furthermore, the fact that all transactions involving the digital currency are recorded on decentralized global networks, none of which fall cleanly under any singular jurisdiction, further complicates efforts to investigate and monitor these types of transactions (Al-Batoush, 2024) ^[7].

These obstacles are further exacerbated by the apparent scarcity of digital crime personnel who are adequately qualified. The majority of these individuals have received their education in technologies that were prevalent during their youth, rather than in the current era. Some of the emerging technologies that are being rapidly adopted are not completely comprehended by anyone (Elbeh, 2024) ^[11].

This is particularly true of Blockchain, digital wallets, and NFTs. Not even the most astute private-sector personnel employed by technology companies possess a comprehensive understanding of these technologies to employ them in a manner that could potentially yield the desired results. The minds of both the judiciary and law enforcement must be trained to a high level and must remain trained as technologies develop. The institutional and legislative foundations of the Jordanian legal system require urgent attention, more so than ever (Stapleton, 2024) ^[29].

Lastly, the absence of effective global collaboration in this field poses a substantial obstacle. Transnational digital currency crimes frequently involve multiple countries. Our capacity to pursue these international offenders is restricted in the absence of Jordan's participation in international conventions that pertain to either cybercrime or the regulation of crypto-assets. Additionally, we are restricted in our capacity to monitor the funds that are transferred through foreign platforms that are not under our jurisdiction (Ghandour *et al.*, 2024.) ^[14].

These obstacles unambiguously demonstrate that the current legislative and institutional framework in Jordan is insufficient to meet the current digital demand when considered in conjunction. This situation necessitates the establishment of a technical and regulatory team that is

capable of managing the digital domain, as well as the complete revision of the legal structure, either through the passage of new laws or the amendment of existing ones.

Comparative Legislative Experiences

Despite the fact that the Jordanian legislator maintains a cautious and hesitant stance toward digital currencies, as they have not yet established a definitive regulatory framework, numerous other jurisdictions, including some that are particularly near to Jordan, have adopted an entirely different approach. They have taken the initiative to explicitly integrate digital currencies into their legal systems, thereby defining them as either legal or illicit. In this regard, the curricular decisions of Egypt, France, and the United Arab Emirates may serve as valuable reference points for any future legislative endeavor in Jordan. The Egyptian legislator has taken a substantial regulatory step in the area of anti-money laundering, or more specifically, in the domain of laws that are designed to prevent the money laundering that poses a threat to a country's economy. The more current law, Law No. 194 of 2020, has been adopted by Egyptian lawmaker to change the Anti-Money Laundering Law No. 80 of 2002, a crucial matter. This was a very good legislative action since it broadened the legislation to include hitherto neglected possible sites of money laundering, including electronic and digital transactions (Al Nabhani *et al.*, 2025b) ^[3]. Establishing a dedicated legislative framework to control the digital currency market, France has adopted a more proactive approach. The 2019 PACTE Law created particular rules for digital asset service providers (PSANs), therefore establishing this framework (Praicheux & Vandenbussche, 2020) ^[25].

Lawwise, PSANs are required to follow basic anti-money laundering (AML) and counter-terrorism financing (CTF) rules and get permission from the French financial markets regulator (AMF.) (Siitonen, 2024) ^[28]. Nonetheless, the PACTE Law goes further by creating a legal framework that gives transactions involving digital currency legal significance provided all participants follow the pertinent laws (Karlson, 2023) ^[15].

The French model best illustrates a balanced strategy. It enables a legal and regulatory control akin to the German approach in addition to the same degree of financial innovation and market openness as the U.S. model (Pala, 2024) ^[24].

Implementing a transparent, competent regulatory framework—a trait absent in all governments—the United Arab Emirates is making major steps toward the integration of digital currencies into the lawful financial industry (Othman & Dosh, 2024) ^[23].

During 2021, the Central Bank of the UAE implemented the "Regulation on Virtual Asset Service Providers." Companies that operate with digital currencies are mandated to obtain a license and adhere to stringent regulations that are significantly more stringent than those in numerous jurisdictions. These regulations prioritize the provision of adequate disclosures and the establishment of robust anti-money laundering and counter-terrorist financing programs (El-Gheriani & Hashish, 2025) ^[12].

These legislative experiences demonstrate that the regulation of digital currencies is more intricate than merely criminalizing poor behavior (Al Nabhani *et al.*, 2025c) ^[4]. Authorities must acknowledge the value of digital assets,

determine which government agencies are responsible for overseeing digital currencies (and communicate this information clearly to the public and within the government), and establish specific legal obligations for those who issue, sell, or otherwise transact in digital currencies in order to effectively regulate them. The Jordanian legislator could implement reforms that would address specific gaps in the current regulatory framework, such as the passage of a specialized new law or the substantial amendment of a few existing laws. This would enable the prevention of digital currency-related criminal activity and the imposition of penalties for those who fail to comply with the new laws.

Conclusion

This investigation has emphasized the significant disparity between the rapid technological advancements exemplified by digital currencies and the current legal framework in Jordan, which is rather hesitant to provide these potential new financial products with an official boost. The findings indicate that the primary issue is one of definition: the absence of a comprehensive, authoritative legislative definition for digital currencies appears to have resulted in a legal grey area. The absence that has resulted in this lacuna appears to be partially responsible for the proliferation of contemporary cybercrimes.

Although existing laws, including the Anti-Money Laundering and Counter-Terrorist Financing Law No. 46 of 2007 and the Cybercrime Law No. 27 of 2015, contain general provisions that criminalize certain electronic behaviors, they are insufficient to provide the legal tools required to address a new category of crimes that occur in a technological context. Digital currencies, particularly those that operate on decentralized systems, pose obstacles that current legislation is unable to address, particularly in terms of their transnational operations and anonymity. The Jordanian legislator fails to translate the Central Bank's precautionary warnings into binding legislation or regulatory instruments that would ensure the clarity of the law and eliminate the judicial hesitation that is currently evident in cases involving digital currencies. Rather, they rely on the Central Bank's precautionary warnings. The individuals who reside and labor within the jurisdiction are not the only ones who benefit from this type of legal clarity and certainty. The jurisdiction is diminished when law enforcement lacks clarity and confidence. The border-crossing characteristic of digital currencies, which makes it so simple to commit serious crimes such as money laundering, financing terrorism, and committing large-scale fraud beyond the oversight of traditional financial authorities, makes the legal absence particularly risky.

The genuine issue at hand, of course, is that the Jordanian authorities lack the necessary technical expertise to conduct the necessary investigations and prosecutions to effectively address the emergent technologies and the individuals who perpetrate crimes with them.

The development of adaptable legal frameworks that regulate digital currencies without stifling innovation is feasible, as evidenced by comparative legislative experiences, particularly in France, the United Arab Emirates, and Egypt. These countries have achieved a balance by establishing specialized institutions to address the intricacies of the digital economy, as well as by

combining licensing and supervision with the prohibition of harmful conduct. This demonstrates that the denialists' approach, which involves the exclusion of digital currencies from our legal system, is not a viable solution. Consequently, Jordan requires legislation to be implemented without delay. This legislation must be founded on a genuine and unrestricted comprehension of the nature of digital currencies, a multifaceted comprehension of the risks they entail, and—from a legal perspective—the appropriate nature of our relationship with them. This is a completely feasible and not overly challenging comprehension; however, it necessitates a willingness to engage in appropriate conversations and a willingness to investigate the appropriate sources.

Recommendations

1. Establish a law that is specifically reserved for digital currencies.

Provide comprehensive legislation that explicitly regulates digital currencies. This legislation should provide a legal definition that is unambiguous, a typology that clearly differentiates between different types (e.g., cryptocurrencies, stablecoins, central bank digital currencies), and a clear delineation of the regulatory authorities responsible for each type of service underwriting and service provision.

2. Revise the Anti-Money Laundering and Counter-Terrorist Financing Law.

Adjust the legislation to include digital currencies in the list of prohibited items that may be employed in financial offenses. Ensure that the necessary legal and technical arrangements are in place to facilitate the tracking and seizure of digital assets when a legitimate reason arises.

3. Broaden the Purpose of the Cybercrime Law

Revise the Cybercrime Law to include new types of illicit activities that are linked to digital currencies. The following are included: fraudulent trading, phishing schemes that target digital wallets, and the fabrication of cryptographic tokens (fake items that are designed to resemble and function like genuine cryptographic tokens).

4. Establish a specialized regulatory authority.

Establish a regulatory body for digital assets that is either under the jurisdiction of the Central Bank or the Jordan Securities Commission. This authority would be responsible for the licensing of platforms, the supervision of transactions, and the protection of consumers from deception.

5. Develop the technical capabilities of judicial and law enforcement entities.

It is imperative to establish specialized digital crime sections that are well-equipped with both legal and technical expertise to conduct the necessary investigations and prosecutions in the event that digital currencies are used in an illegal manner. These units should have personnel who are proficient in digital forensics and other fields, such as blockchain analysis, as a significant number—if not the majority—of the digital currencies currently in circulation are significantly reliant on this technology.

6. Enhance International Judicial and Security Cooperation

Participate in international agreements such as the Budapest Convention on Cybercrime. Additionally, establish information-sharing agreements with foreign countries that are home to significant digital asset firms. This will facilitate significantly enhanced cross-border investigations and prosecutions.

7. Establish Judicial Training Programs

To enable these critical legal professionals to more effectively comprehend the underlying technology of digital currencies, the evidentiary challenges they present, and how to issue legal judgments in these newly arising "currency" cases, it is imperative to establish and provide ongoing, top-level professional development to judges and prosecutors throughout the United States.

8. Implement campaigns to increase public awareness of legal and financial matters

Organize nationwide public awareness campaigns to educate citizens about the legal risks associated with the use of unregulated digital currencies. Inform them of the appropriate course of action in the event that they come across potential fraudulent activity.

9. Utilize comparative legislative models

Models can be derived from the legal systems of the French and Emirati countries, which have successfully balanced regulatory supervision and financial innovation. Their adaptable frameworks could be a valuable resource for determining the types of legal responses that would be effective at a national level in Jordan.

References

1. Al Masadeh AM, Abunaseir MH, Rukba ROA. Impact of Jordanian Electronic Transactions Law and Digital Transformation on Commercial Contracts and Their Proof. *Journal of Human Security*,2024:20(1):104–108.
2. Al Nabhani ASH, Al Masoudi RSS, Abdel-Gadir S. Comparative Analysis of Digital Currency Regulations: International and Domestic Legal Frameworks. *Journal of Ecohumanism*,2025a:4(2):1518–1533.
3. Al Nabhani ASH, Al Masoudi RSS, Abdel-Gadir S. Comparative Analysis of Digital Currency Regulations: International and Domestic Legal Frameworks. *Journal of Ecohumanism*,2025b:4(2):1518–1533.
4. Al Nabhani ASH, Al Masoudi RSS, Abdel-Gadir S. Comparative Analysis of Digital Currency Regulations: International and Domestic Legal Frameworks. *Journal of Ecohumanism*,2025c:4(2):1518–1533.
5. Albalawee N, Al Fahoum AS. Islamic legal perspectives on digital currencies and how they apply to Jordanian legislation. *F1000Research*,2023:12:97.
6. Albanki AA, Alshawawreh NK, Abdeldayem MM, Aldulaimi SH. Unravelling the Legal Framework for Cryptocurrency: A Comparative Analysis of Regulatory Approaches. 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), 2024, 1–6. <https://ieeexplore.ieee.org/abstract/document/1045941/>
7. Al-Batoush A. Money Laundering Via Electronic Means: Electronic Check. *Pakistan Journal of Criminology*, 2024, 16(2).

- <https://www.pjcriminology.com/wp-content/uploads/2024/04/27-Money-Laundering-Via-Electronic-Means.pdf>
8. Ali AM, Mohammed RI. Money Laundering in the Digital Age: A Comparative Analysis of Electronic Means in Egypt, Jordan, the UAE and Iraq. *Pakistan Journal of Criminology*, 2023, 15(4). <https://www.pjcriminology.com/wp-content/uploads/2023/11/12.-Money-Laundering-in-the-Digital-Age.pdf>
 9. Al-Naimi AA, Al-Trad E, Yousef RA. Trends of fintech and cryptocurrencies Jordan recapitulation. *International Journal of Entrepreneurship*,2021:25:1–17.
 10. Chitimira H, Animashaun O. The adequacy of the legal framework for combating money laundering and terrorist financing in Nigeria. *Journal of Money Laundering Control*,2023:26(7):110–126.
 11. Elbeh IMA. E-Commerce and Digital Currencies Risk Management Challenges Check for updates. *Intelligent Systems, Business, and Innovation Research*,2024:489:343.
 12. El-Gheriani M, Hashish A. Harnessing the crypto-horse. Factors affecting a friendly regulator of the crypto-industry: Dubai as a test case. *Information & Communications Technology Law*, 2025, 1–21. <https://doi.org/10.1080/13600834.2025.2452718>
 13. Gaviyau W, Sibindi AB. Global anti-money laundering and combating terrorism financing regulatory framework: A critique. *Journal of Risk and Financial Management*,2023:16(7):313.
 14. Ghandour A, AL-Enizi Z, Madi R, Kameel TA, Hamdieh L. (n.d.). Legal Framework for Blockchain Contracts: An Analysis Under Uae Law. Available at SSRN 5056550. Retrieved March 26, 2025, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5056550
 15. Karlson L. Follow the Money: Financial Investigations Process in the European Union, 2023. <https://dspace.cuni.cz/handle/20.500.11956/187343>
 16. Khan S, Saleh T, Dorasamy M, Khan N, Leng OTS, Vergara RG. A systematic literature review on cybercrime legislation. *F1000Research*,2022:11:971.
 17. Khater MN. Criminalization of Forgery of Electronic Payment Cards in Jordanian Legislation. *Pakistan Journal of Criminology*, 2024, 16(1). <https://www.pjcriminology.com/wp-content/uploads/2024/01/29-Criminalization-of-Forgery.pdf>
 18. Koto I. Cyber crime according to the ITE law. *International Journal Reglement & Society (IJRS)*,2021:2(2):103–110.
 19. Le Nguyen C, Golman W. Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: ‘Law on the books’ vs ‘law in action.’ *Computer Law & Security Review*,2021:40:105521.
 20. Magableh NZ. The Adequacy of the Laws Regulating Electronic Business in Jordan. *Public Administration and Law Review*,2024a:1(17):66–77.
 21. Magableh NZ. The Adequacy of the Laws Regulating Electronic Business in Jordan. *Public Administration and Law Review*,2024b:1(17):66–77.
 22. Nawayiseh E, Nazal AI, Metair H. Stability of Jordanian Dinar Supports Electronic Trading System. In R. E. Khoury & N. Nasrallah (Eds.), *Intelligent Systems, Business, and Innovation Research*,2024:489:47–58. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-36895-0_4
 23. Othman AMZ, Dosh EMEE. Regulating digital currencies in the Emirate of Dubai: A comparative legislative review. *International Journal of Public Law and Policy*,2024:10(2):204–225. <https://doi.org/10.1504/IJPLAP.2024.137850>
 24. Pala F. The Impact of Cryptocurrency Markets on the Traditional Financial Markets of the USA, UK, and Germany. *Ekonomi ve Finansal Arařtırmalar Dergisi*,2024:6(2):100–128.
 25. Praicheux S, Vandebussche J. Progress at the Cost of Protection. *Int'l Fin. L. Rev.*, 2020, 46.
 26. Rashid SK, Saleh DT. Special Legal Procedures to Prevent the Exploitation of E-Commerce Transactions in Currency Smuggling and Money Laundering. *Journal of Ecohumanism*,2024:3(8):11710–11722.
 27. Shdaifat SMA. The criminal confrontation of the cryptocurrency (Bitcoin) and its illegal use. *International Journal of Electronic Security and Digital Forensics*,2023:15(2):114. <https://doi.org/10.1504/IJESDF.2023.129280>
 28. Siitonen P. National Risk Assessment of Money Laundering and Terrorist Financing in the NPO Sector, 2024. <https://julkaisut.valtioneuvosto.fi/handle/10024/165908>
 29. Stapleton J. The Age of the Metaverse: The Need for Consumer Protections in Metaverse Cryptocurrency Transactions. *Seattle Journal of Technology, Environmental, & Innovation Law*,2024:14(2):7.
 30. Yousef M. The Potential Risks of Mining and Investment in Digital Currencies based on Financial Technology Applications. *Journal of System and Management Sciences*,2023:13(5):276–293.