

Regulating Cryptocurrencies in the United Arab Emirates: Legal Frameworks, Enforcement Gaps, and Anti-Money Laundering Challenges

By

Corresponding author: Hisham Mohamed Hassan Al Hammadi

School of Law, Universiti Utara Malaysia, Sintok 06010, Kedah, Malaysia.

Email: hisham.83@hotmail.com

Co-author 1: Dr Muhammad Hafiz bin Badarulzaman

School of Law, Universiti Utara Malaysia, Sintok 06010, Kedah, Malaysia.

Email: Hafizbad8487@gmail.com

Co-author 2: Dr. Abdulaziz Fahmi Omar Faqera

School of Government, Universiti Utara Malaysia, Sintok 06010, Kedah, Malaysia.

Email: azizfaqera@gmail.com

Abstract

The regulatory architecture governing cryptocurrencies and virtual assets in the United Arab Emirates has expanded markedly through Federal Decree-Law No. 20 of 2018, Cabinet Decision No. 10 of 2019, Federal Decree-Law No. 46 of 2021, and Dubai Law No. 4 of 2022, reflecting the state's ambition to position itself as a leading digital finance hub while addressing money laundering risks. Notwithstanding this legislative progress, significant challenges persist, stemming from the decentralized and pseudonymous nature of cryptocurrencies, fragmented institutional oversight across federal and emirate-level authorities, and constrained supervisory capacity for real-time monitoring. Existing scholarship has largely overlooked the interaction between legal design and institutional enforcement dynamics within the UAE's cryptocurrency regime, creating a critical gap this study addresses. The study critically evaluates the legal and institutional frameworks governing cryptocurrencies, examines enforcement and compliance vulnerabilities within AML mechanisms, and assesses regulatory risks associated with cryptocurrency market adoption. Employing an exploratory qualitative doctrinal methodology, the analysis systematically examines primary legislation alongside secondary sources drawn from high-impact journals, authoritative monographs, and institutional reports, subjected to rigorous thematic analysis. Guided by Institutional Theory, the findings demonstrate that while the UAE's framework is normatively comprehensive, enforcement effectiveness is undermined by coordination deficits and technological constraints. The study advances targeted recommendations to enhance regulatory coherence, institutional integration, and risk-based supervision, contributing to legal, financial regulation, international governance, and digital risk studies, while identifying directions for future comparative inquiry.

Keywords: Anti-Money Legal, Cryptocurrencies, Frameworks Laundering, United Arab Emirates

1-Introduction

The rapid emergence and adoption of cryptocurrencies have fundamentally transformed global financial systems, offering decentralized, borderless, and technologically sophisticated means of conducting transactions (Ramesh 2025). Cryptocurrencies such as Bitcoin, Ethereum, and an increasing array of digital assets provide unprecedented efficiency, transparency, and opportunities for financial innovation (De Filippi & Wright, 2018). However, their decentralized and pseudonymous nature simultaneously introduces substantial legal and regulatory complexities, challenging traditional mechanisms of governance, financial oversight, and risk mitigation (Werbach & Cornell, 2017). Governments worldwide are grappling with these challenges, striving to balance the promotion of technological innovation with effective enforcement of anti-money laundering (AML) and consumer protection standards. In this context, the United Arab Emirates (UAE) has positioned itself as a regional leader in cryptocurrency adoption, with federal and emirate-level initiatives such as the Emirates Blockchain Strategy, the establishment of the Virtual Assets Regulatory Authority (VARA), and Dubai Law No. 4 of 2022 reflecting the country's proactive approach to fostering a regulated digital financial environment (Al Tamimi & Co., 2022).

Despite these legislative and institutional advancements, cryptocurrencies present significant vulnerabilities, particularly concerning financial crime risks and enforcement effectiveness. The pseudonymous and decentralized characteristics of virtual assets complicate the tracing of illicit transactions, facilitating activities such as money laundering, terrorist financing, and market manipulation (Gilber, & Gilbert 2025; Hazar & Boydas, 2022; Ernesto & Longa, 2021). Furthermore, the heterogeneity of global regulatory approaches, combined with fragmented domestic oversight, increases the complexity of enforcing AML measures and maintaining financial integrity within the UAE (FATF, 2020, 2023; IMF, 2024). Extant literature emphasizes that while the UAE has developed comprehensive legal frameworks, gaps persist in operational enforcement, inter-agency coordination, technological capacity, and doctrinal clarity regarding the legal nature of cryptocurrencies (Al Tamimi & Co., 2022; Parker, 2021; Brown, 2022). These gaps create opportunities for exploitation by malicious actors and limit the overall effectiveness of the UAE's regulatory efforts.

As a result, this study seeks to address the underexplored phenomenon of cryptocurrency regulation in the UAE, focusing on the effectiveness of legal frameworks and institutional mechanisms in preventing money laundering and mitigating risks associated with virtual assets. The central research question guiding this study is: How effective are the UAE's legal frameworks and institutional mechanisms in regulating cryptocurrencies and preventing money laundering, and what gaps hinder optimal enforcement? The study aims to critically assess the legal and institutional frameworks governing cryptocurrencies, evaluate enforcement challenges in AML mechanisms, examine regulatory vulnerabilities linked to cryptocurrency adoption, and provide recommendations to strengthen compliance, supervision, and legal clarity. The findings will contribute to the academic fields of financial regulation, cyber law, and fintech governance, while also offering actionable insights for policymakers and regulatory authorities tasked with improving oversight of virtual assets.

2-Methodology

This study employs an explorative qualitative research design using a doctrinal approach, appropriate for examining the legal and regulatory frameworks governing cryptocurrencies and the enforcement of anti-money laundering (AML) measures in the UAE. Doctrinal research allows for systematic analysis of primary legal sources, including Federal Decree-Law No. 20 of 2018 on AML, Cabinet Decision No. 10 of 2019, Federal Decree-Law No. 46 of 2021 on Electronic Transactions, and Dubai Law No. 4 of 2022 regulating virtual assets. By critically analyzing these statutes, the study identifies their scope, strengths, and enforcement gaps, providing a solid foundation for understanding the UAE's regulatory environment (Hutchinson & Duncan, 2012; Garth & de Haan, 2018).

To enhance analytical depth, secondary sources were also consulted, including peer-reviewed journals, scholarly books, institutional reports, and official government publications (Tahat et al. 2022; Tahat, Tahat, et al. 2023; Tahat, Habes, et al. 2024). These sources provide comparative insights on global cryptocurrency regulation, AML best practices, and international standards, enabling a critical synthesis of UAE frameworks. All secondary sources were carefully selected for credibility, relevance, and alignment with the research focus, and the data underwent rigorous thematic analysis to ensure reliability and authenticity (Creswell & Poth, 2018; Denzin & Lincoln, 2018). The study is guided by Institutional Theory, which provides a conceptual lens to interpret how regulatory norms, formal structures, and institutional practices influence enforcement and compliance behaviors in the UAE.

3-Related Theoretical Underpinning

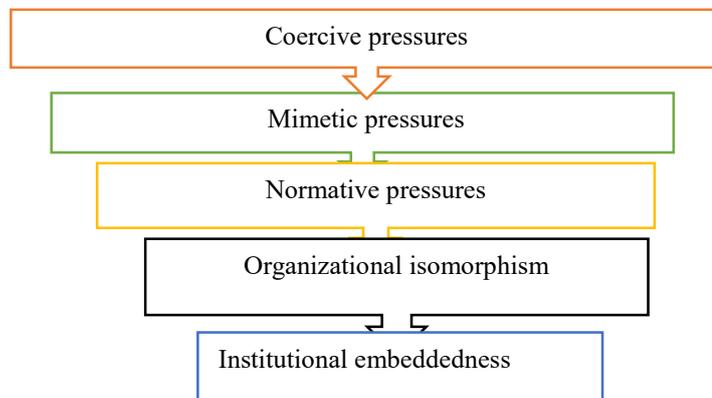
This study adopts Institutional Theory to guide the analysis of the phenomenon under study. Institutional Theory was developed by Paul DiMaggio and Walter Powell in 1983 and expanded by John W. Meyer and Brian Rowan, with further elaboration by W. Richard Scott (DiMaggio & Powell, 1983; Scott, 2008). At its core, the theory explains how formal legal structures, normative expectations, and cognitive frameworks shape organizational behavior, compliance mechanisms, and policy implementation within institutional environments. In applying this theory, the study operationalizes five key assumptions: coercive pressures (law and regulation mandate compliance), mimetic pressures (organizations adopt practices from exemplars to achieve legitimacy), normative pressures (professional norms and ethical expectations influence conduct), organizational isomorphism (tendency toward similarity in structure and practice among institutions), and institutional embeddedness (institutional practices are shaped by historical, cultural, and social contexts)(Tahat, Mansoori, et al. 2024).

The choice of Institutional Theory is justified because it enables the researcher to demonstrate how and why UAE regulatory authorities interpret, enforce, or at times fail to enforce AML requirements, not merely based on legal text but in the context of normative and mimetic forces exerted by international standards (FATF) and professional networks. This theory highlights that enforcement gaps may stem from institutional dynamics rather than legal inadequacies alone, making it uniquely suitable for analyzing multi-layered regulatory environments(Tahat, Salloum, et al. 2023).

Recent empirical studies support this theoretical alignment. Kshetri (2021) finds that compliance with blockchain and AML norms is significantly influenced by institutional pressures, while Zdanovic (2023) identifies that fragmented regulatory authorities and weak inter-agency coordination are rooted in institutional structures which undermine AML enforcement. These findings reveal gaps in translating AML laws into practice, reinforcing the research's use of Institutional Theory (Al Jwaniat et al. 2023).

Scientifically this theory contributes to this study by linking legal frameworks with organizational behavior, allowing for systematic evaluation of how coercive and normative pressures shape AML enforcement outcomes. By integrating institutional assumptions with the subject matter, the study not only assesses statutory provisions but also unpacks how institutional environments enable or constrain effective crypto-AML governance in the UAE. Consequently, the key theoretical assumptions outlined above are illustrated in the diagram below.

Diagram 1. key Assumption Underpinning Institutional Theory



Source: Data compiled and analyzed by the authors (2025).

4-Literature Review

4.1-The Legal Nature and Classification of Cryptocurrencies

The legal nature and classification of cryptocurrencies remain a central doctrinal issue in digital asset regulation, with significant implications for regulatory design, compliance, and enforcement. Cryptocurrencies such as Bitcoin and Ethereum are decentralized digital constructs operating on distributed ledger technology (DLT) without intrinsic legal tender status or central bank backing, complicating their categorisation within existing legal regimes. Scholars like De Filippi and Wright (2018) argue that digital currencies occupy a liminal space between traditional legal categories, defying clear classification as property, currency, or securities due to their decentralized governance and cryptographic architecture. This perspective reflects a broader academic view that conventional legal doctrines are strained by technological innovation, necessitating new conceptual frameworks that account for the hybrid nature of these assets .

Given the above, a legion of literature, including the works of Raskin and Yermack (2022), reveals a spectrum of classification approaches. On one side, scholars argue for treating cryptocurrencies as intangible property, emphasizing recognizable ownership rights and transferability. The perspective provides a familiar legal anchor, facilitating the application of established remedies for loss, theft, or contractual disputes. However, critics highlight that such classification fails to capture essential economic functions of certain tokens especially those used in decentralized finance (DeFi) contexts or for value transfer leading to regulatory inconsistencies (Scott, 2019). On the other hand, Werbach and Cornell (2017) propose that cryptocurrencies may defy traditional categories altogether, advocating for a sui generis legal category that recognises their distinct technological and economic characteristics. This latter view foregrounds the risk that mapping digital assets into pre-existing categories could misalign regulatory objectives, particularly in contexts requiring tailored compliance mechanisms such as anti-money laundering (AML) regimes.

Empirical regulatory frameworks further illustrate the practical ramifications of doctrinal uncertainty. In the United States, the Securities and Exchange Commission (SEC) applies the *Howey* test to determine when a token constitutes a security, thereby subjecting it to investor protection laws, while the Commodity Futures Trading Commission (CFTC) treats other tokens as commodities subject to derivatives oversight (Securities and Exchange Commission, 2020; Commodity Futures Trading Commission, 2023). These divergent interpretations highlight regulatory heterogeneity that undercuts legal certainty and creates challenges for international compliance, particularly for multi-jurisdictional actors. Similarly, the European Union's Markets in Crypto-Assets (MiCA) regulatory framework adopts an activity-based approach, categorizing assets according to economic behaviour rather than formal doctrinal labels (European Parliament & Council, 2023), a stance that underscores a growing consensus among regulators that function may matter more than form in digital asset governance.

In the context of the United Arab Emirates, doctrinal uncertainties are mirrored in institutional classifications. The Virtual Assets Regulatory Authority (VARA), through its rulebook established under Dubai Law No. 4 of 2022, defines virtual assets broadly as digital representations of value that can be transferred, stored, or traded electronically, excluding fiat currency unless otherwise specified. This functional definition

is pragmatic but elides deeper doctrinal questions about the inherent legal nature of specific tokens, leaving interpretive authority to regulators on a case-by-case basis. Likewise, the Abu Dhabi Global Market (ADGM) treats non-fiat virtual assets as commodities for regulatory purposes, enabling them to be regulated similarly to tangible and intangible consumer goods without equating them to money or securities. Such institutional variation within a single national legal order illustrates the fragmented doctrinal landscape, which scholars caution can undermine legal predictability and enforcement efficacy.

Scholarly analyses also emphasise that doctrinal ambiguity may materially affect compliance obligations. For instance, unclear legal status can impede the application of AML/CFT frameworks, where the identification of beneficial ownership and reporting requirements hinges on definitional clarity (Arner, Barberis, & Buckley, 2020). Without a precise legal classification, regulators and courts may struggle to enforce due diligence obligations, exacerbating enforcement gaps that are already challenging due to pseudonymity and cross-border transaction flows. Consequently, the extant literature suggests that while treating cryptocurrencies as property may offer legal clarity in ownership disputes, it may not sufficiently address their functional attributes as mediums of exchange or investment instruments. Conversely, an overly broad functional classification without doctrinal grounding risks legal indeterminacy. Also, scholarly perspectives thus points toward hybrid or bespoke regulatory categories that account for both the technological and economic dimensions of digital assets.

2-Cryptocurrency Market Manipulations and Regulatory Vulnerabilities

Market manipulation in cryptocurrency markets refers to actions intentionally designed to distort asset prices and trading volumes for the benefit of manipulators rather than genuine market participants. Common manipulation tactics include pump-and-dump schemes, wash trading, and insider trading-like strategies. Pump-and-dump schemes involve coordinated buying activity that artificially increases the price of a low-liquidity token, followed by rapid liquidation by orchestrators at a profit, leaving unwitting investors with losses (Hamrick, Rouhi, Mukherjee, et al., 2021). Such schemes were historically observed in over-the-counter markets but have proliferated in cryptocurrency trading due to low regulation and ease of coordination via social platforms (Aidoo, & Int Dip 2025; Putniņš & Dhawan, 2022). Wash trading, where traders simultaneously record fictitious buy and sell orders to create the appearance of high market activity, has been empirically documented across multiple exchanges, suggesting pervasive manipulation of reported liquidity and volume (Fry & Cheah, 2021). Although less frequently studied, insider trading in crypto resembles traditional concepts where traders exploit non-public information, particularly around exchange listings or project announcements, to generate outsized returns (Gandal, Hamrick, & Moore, 2018).

Moreover, the absence of comprehensive regulation and heterogeneous oversight across exchanges exacerbates these risks. Cryptocurrency trading platforms vary widely in governance, transparency, and compliance, creating fertile conditions for manipulative actors. Research indicates that wash trading and artificial volume inflation are far more prevalent on loosely regulated or unregulated exchanges, asserting that a significant proportion of reported trading volumes may be inflated to attract users and enhance perceived liquidity (Fry & Cheah, 2021). This problem is particularly acute on platforms lacking robust market surveillance tools or internal controls. In the UAE context, major exchanges like BitOasis and BitoPro have seen increased adoption as digital asset trading grows, yet regulatory actions such as VARA's suspension of BitOasis's operational license for non-compliance highlight ongoing struggles to align practices with regulatory expectations and market integrity (Arabian Business, 2023). This underscores a critical point: market manipulation is not only a global phenomenon but also relevant to emerging fintech hubs like the UAE.

Additionally, the regulatory vulnerabilities arise from fragmented enforcement frameworks and limited real-time surveillance capabilities. Unlike mature financial markets, which deploy advanced analytics and legally mandated reporting to detect and deter manipulation, many cryptocurrency exchanges lack comparable systems. Academic studies show that pump-and-dump operations and other manipulative behaviors often cluster around specific tokens and platforms, making detection difficult without sophisticated anomaly detection tools (Putniņš & Dhawan, 2022). Moreover, manipulators exploit social media and messaging groups to coordinate activity, leveraging investor sentiment and behavioral biases to trigger cascades of automated and manual trades (Schry & Griner, 2021).

Comparatively, regulatory regimes in the United States and European Union offer instructive contrasts. The U.S. Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) have brought enforcement actions targeting manipulative conduct and require public disclosure and market surveillance to uphold market integrity. Similarly, the EU's Market Abuse Regulation (MAR) encompasses digital assets within its scope, mandating surveillance and reporting frameworks for trading venues. These mature markets benefit from coordinated oversight and robust legal tools that can impose substantive penalties for abusive behaviors capabilities that many crypto markets globally, including in the UAE, are still developing. The absence of unified global standards further complicates enforcement, permitting manipulative schemes to migrate toward jurisdictions with weaker or evolving regulatory systems. Hence, the market manipulation represents both a financial and legal challenge that threatens investor confidence and market efficiency. Without stronger oversight mechanisms, including real-time monitoring, standardized reporting, and international cooperation, manipulative practices can persist, undermining the credibility of cryptocurrency markets (Fry & Cheah, 2021; Putniņš & Dhawan, 2022). For jurisdictions like the UAE, regulatory frameworks must evolve beyond basic licensing regimes to include active surveillance, enforcement coordination, and technological investment to detect and deter manipulative behavior effectively. Only through these measures can market integrity be preserved and the broader promise of digital asset innovation be realized.

4.3-Cryptocurrencies and Money Laundering Risks

Money laundering refers to the process of concealing the illicit origins of funds and integrating them into the legitimate financial system, traditionally conceptualized in three stages: placement, layering, and integration (Eziokwudimma, 2025; Ernesto & Longa, 2021). In the placement stage, illicit funds enter the financial system, often through deposits or purchases. Layering involves complex transfers, including cross-border movements, designed to obscure the audit trail. Finally, integration returns laundered funds into the legitimate economy through investments or consumption. Cryptocurrencies introduce unique challenges across all stages. Their decentralized and pseudonymous nature allows criminals to convert illicit funds into digital assets quickly, bypassing traditional banking scrutiny and evading conventional monitoring systems (Ernesto & Longa, 2021). Consequently, the speed, global reach, and near-instantaneous transfers of digital assets amplify traditional AML vulnerabilities, demanding a reassessment of established compliance frameworks.

The pseudonymity inherent in blockchain technology and the advent of privacy-enhanced cryptocurrencies such as Monero and Zcash further complicate AML efforts. These cryptocurrencies utilize advanced obfuscation techniques and ring signatures in Monero and zero-knowledge proofs in Zcash that mask transaction origins, amounts, and participants, making forensic tracing significantly more challenging (Hazar & Boydas, 2022). Additional tools such as mixers or tumblers blend multiple users' funds, while peer-to-peer (P2P) trading platforms allow direct transfers without intermediaries, circumventing traditional Know Your Customer (KYC) procedures. Thus, these technological features highlight the tension between legitimate privacy interests and illicit activity, illustrating how cryptocurrency innovation, while beneficial for user autonomy, can simultaneously facilitate financial crime. On an international scale, these characteristics exacerbate enforcement difficulties. Cryptocurrencies operate across borders without respect for national jurisdictions, creating opportunities for regulatory arbitrage, where actors exploit weaker regulatory regimes (FATF, 2020). The Financial Action Task Force (FATF) has issued multiple guidance

documents emphasizing the need for global coordination, including applying AML obligations to Virtual Asset Service Providers (VASPs) and implementing the Travel Rule for cross-border transfers (FATF, 2020; FATF, 2023). Consequently, scholars including Zdanovic, (2022) argue that conventional AML frameworks struggle to keep pace with the rapid technological evolution of cryptocurrencies, as regulatory instruments designed for centralized banking are ill-suited for decentralized, pseudonymous networks, that is why, without adaptive legal mechanisms, financial crime risks persist and continue to evolve alongside technology.

In the UAE context, despite the implementation of Federal AML Laws and regulatory oversight, the unique attributes of cryptocurrencies pseudonymity, rapid transferability, and decentralized platforms have compounded the enforcement challenges. For instance, Al Tamimi & Co., (2022) observes that fragmented supervision across federal and emirate-level authorities further undermines compliance monitoring. Thus, it becomes evident that traditional AML measures, reliant on traceable, centralized transaction records, are insufficient for digital assets. Effective mitigation requires adaptive regulation incorporating advanced blockchain analytics, cross-border coordination, and risk-based oversight strategies. The literature collectively underscores that cryptocurrencies do not merely extend existing financial channels but transform the operational landscape of money laundering, necessitating a paradigm shift in AML approaches.

4.4 UAE Cryptocurrency Legal Frameworks and Institutional Oversight

The United Arab Emirates has developed a multifaceted legal framework to regulate cryptocurrencies and virtual assets, reflecting its ambition to become a global fintech hub. Central to this framework is Federal Decree-Law No. 20 of 2018, which establishes broad anti-money laundering (AML) and counter-terrorism financing obligations, creating a foundation for supervising financial transactions across sectors (UAE Federal Government, 2018). Complementing this, Cabinet Decision No. 10 of 2019 operationalizes the AML law, detailing procedures for customer due diligence (CDD), reporting requirements, and internal compliance protocols (UAE Cabinet, 2019). To accommodate the digitization of financial services, Federal Decree-Law No. 46 of 2021 on Electronic Transactions and Trust Services confers legal recognition to electronic contracts and digital signatures, providing legal certainty for blockchain-based transactions (UAE Federal Government, 2021). At the emirate level, Dubai has enacted Law No. 4 of 2022 to regulate virtual assets, creating a dedicated regulatory and licensing regime under the Virtual Assets Regulatory Authority (VARA) (Dubai Government, 2022). Critically, while these instruments establish a comprehensive legal architecture, their effectiveness relies heavily on practical implementation and coordination among diverse authorities. Moreover, the regulatory oversight in the UAE involves multiple specialized bodies, each with distinct mandates. VARA, established under Dubai Law No. 4, is responsible for licensing and supervising Virtual Asset Service Providers (VASPs), ensuring compliance with AML, Know Your Customer (KYC), and reporting obligations (VARA, 2023). The Securities and Commodities Authority (SCA) oversee securities-related virtual assets across other emirates, issuing guidance on trading, custody, and disclosure requirements. Additionally, the UAE Central Bank enforces prudential regulations on financial institutions and issues directives for crypto-related payment systems. Collectively, these authorities implement licensing, supervision, and compliance mechanisms designed to safeguard market integrity and protect investors. Analytically, the coexistence of federal and emirate-level regulators reflects a sophisticated legal structure yet introduces complexity in enforcement and oversight.

Also, the coordination challenges emerge from this multi-layered regulatory environment. Jurisdictional overlaps between VARA and SCA create ambiguity, particularly in cases where cross-emirate crypto operations occur (FATF, 2020). Inter-agency collaboration remains constrained by fragmented reporting systems, divergent supervisory standards, and limited data-sharing protocols (FATF, 2023; IMF, 2024). Hence, those gaps hinder consistent enforcement and reduce the efficiency of oversight mechanisms, leaving potential vulnerabilities for regulatory arbitrage or non-compliance. While UAE authorities have made progress in aligning domestic rules with international standards, including FATF guidance, operational gaps underscore the tension between legal comprehensiveness and practical enforcement capacity. Thus, the UAE presents a robust regulatory framework on paper, encompassing federal decrees, emirate-specific laws, and specialized agencies. However, effective governance depends on harmonized enforcement, institutional capacity, and real-time coordination. The literature indicates that without continuous improvement in inter-agency communication, unified licensing protocols, and technology-enabled supervision, the legal architecture risks undercutting its objectives. Consequently, as explained above, the following table synthesizes the key UAE legal instruments and institutional arrangements governing cryptocurrency oversight and coordination.

Table 4.1: UAE Legal Instruments and Institutional Oversight of Cryptocurrencies

Legal Authority	Instrument / Regulatory Scope	Institutional Function	Key Structural Features
Federal Decree-Law No. 20 of 2018	AML/CFT across financial sectors	Establishes baseline compliance and reporting obligations	Technology-neutral framework applicable to virtual assets
Cabinet Decision No. 10 of 2019	AML implementation	Operationalises customer due diligence and reporting duties	Applies uniformly across regulated entities
Federal Decree-Law No. 46 of 2021	Electronic transactions	Provides legal validity for digital contracts and signatures	Facilitates legality of blockchain-based transactions
Dubai Law No. 4 of 2022	Virtual assets (Dubai)	Creates licensing and supervision regime under VARA	Emirate-specific, activity-based regulatory model
Virtual Assets Regulatory Authority (VARA)	Virtual Asset Service Providers	Licensing, supervision, and compliance monitoring	Dedicated crypto regulator with sector-specific rules
Securities and Commodities Authority (SCA)	Securities-related virtual assets	Market regulation outside Dubai	Oversees crypto assets with investment characteristics
UAE Central Bank	Payments and financial institutions	Prudential supervision and financial stability	Oversees crypto-related payment activities

Source: Researchers (2025)

4.5 Challenges and Gaps in AML Enforcement for Virtual Assets

The enforcement of anti-money laundering (AML) regulations for virtual assets in the UAE faces significant practical challenges, despite the existence of a comprehensive legislative framework (Al-Tawil et al., 2025). Central among these challenges is the pseudonymous and decentralized nature of cryptocurrencies, which complicates tracing and monitoring illicit financial flows. Privacy-focused coins such as Monero and Zcash allow transactions to occur without easily identifiable parties, while mixers and decentralized platforms obscure transactional trails, reducing the effectiveness of traditional AML oversight (Hazar & Boydas, 2022). Furthermore, technological limitations among regulatory agencies, including limited access to advanced blockchain analytics tools, constrain real-time transaction monitoring and risk assessment. Inter-agency coordination is also problematic, with overlapping responsibilities between federal authorities, VARA, SCA, and financial intelligence units often creating delays or gaps in supervision. Additionally, Virtual Asset Service Providers (VASPs) operating under diverse regulatory mandates are inadequately monitored, increasing the potential for compliance lapses and regulatory arbitrage (IMF, 2024).

International assessments provide a benchmark for evaluating the UAE's AML enforcement. The FATF Mutual Evaluation Report (2020) acknowledged legislative progress but highlighted weaknesses in practical enforcement, particularly regarding pseudonymous crypto transactions and limited access to beneficial ownership information (FATF, 2020). The FATF Follow-Up Report (2023) observed some improvements, including enhanced guidance for VASP supervision, yet persistent gaps remained in monitoring, technical capacity, and application of the Travel Rule. Similarly, the IMF Staff Report (2024) emphasized ongoing challenges, such as fragmented jurisdiction, insufficient data-sharing mechanisms, and the need for greater institutional capacity to conduct risk-based supervision of virtual assets (IMF, 2024). As a result, this underscores that, while the UAE aligns with international AML standards in form, enforcement gaps undermine compliance in practice.

In addition to above, specific deficiencies within the UAE context exacerbate these challenges. Supervision remains inconsistent, as emirate-level authorities (VARA in Dubai, SCA elsewhere) operate under distinct regulatory frameworks without fully harmonized protocols. This fragmentation complicates enforcement and introduces uncertainty for VASPs and financial institutions. Weak data-sharing practices between agencies further impede effective monitoring and timely intervention. Moreover, limited access to specialized blockchain analytics tools restricts authorities' ability to detect and investigate suspicious transactions, leaving pseudonymous assets vulnerable to misuse (Al Tamimi & Co., 2022). These operational shortcomings highlight a divergence between legislative intent and practical implementation. Similarly, the enforcement gaps significantly weaken AML compliance, despite a comprehensive legal architecture. That is why, the challenges posed by pseudonymity, fragmented jurisdiction, technological constraints, and inadequate monitoring collectively limit the effectiveness of UAE's AML regime. As elaborated above, the key challenges are illustrated below.

Table 4.2: Key Challenges and Gaps in AML Enforcement for Virtual Assets

Enforcement Challenge	Structural or Technological Source	Regulatory Impact
Transaction pseudonymity	Blockchain design and privacy-enhancing technologies	Limits traceability and beneficial ownership identification
Fragmented regulatory oversight	Multiple federal and emirate-level authorities	Inconsistent supervision and enforcement coordination
Limited blockchain analytics capacity	Technological and resource constraints	Weak real-time monitoring and delayed investigations
Inconsistent VASP supervision	Divergent licensing and compliance standards	Regulatory arbitrage and uneven AML compliance
Cross-border transaction flows	Borderless nature of digital assets	Jurisdictional limits on investigation and enforcement
Inadequate data-sharing mechanisms	Institutional silos	Reduced effectiveness of risk-based supervision

5- Discussion and findings

5.1 Cryptocurrency Classification and Regulatory Complexity

The study found that cryptocurrencies, including Bitcoin and Ethereum, occupy a hybrid legal space, defying traditional classifications as property, currency, or securities, corroborating De Filippi and Wright (2018). Findings reveal persistent doctrinal uncertainty, with some scholars advocating property-based frameworks (Raskin & Yermack, 2022) and others proposing sui generis categories to reflect unique technological and economic characteristics (Werbach & Cornell, 2017). This ambiguity challenges the application of conventional legal remedies and tailoring of compliance mechanisms, particularly in decentralized finance contexts, aligning with literature emphasizing the strain of innovation on established legal doctrines (Scott, 2019). The study's analysis was guided by Institutional Theory, specifically coercive pressures, showing how legal mandates influence regulatory approaches despite ambiguity.

The findings further demonstrate that global regulatory heterogeneity intensifies uncertainty. Divergent approaches by the SEC, CFTC, EU MiCA regulations, and Japan's legal recognition confirm international inconsistencies in crypto governance (European Parliament & Council, 2023; Securities and Exchange Commission, 2020). In the UAE, VARA's broad functional definitions and ADGM's treatment of tokens as commodities reflect similar variation. These findings highlight practical enforcement challenges, especially for multi-jurisdictional actors, corroborating the literature. Finally, the study shows that unclear classification can impede AML compliance, as defining beneficial ownership relies on legal clarity (Arner, Barberis, & Buckley, 2020). Findings demonstrate that property-based treatment supports ownership disputes, but functional frameworks are needed for operational roles. Institutional Theory emphasizes coercive pressures as vital in shaping regulatory responses in fragmented institutional environments (Elareshi et al. 2023; Habes et al. 2023; Megdadi et al. 2023).

5.2 Cryptocurrency Market Manipulations and Vulnerabilities

The findings reveal that cryptocurrency markets in the UAE are highly vulnerable to deliberate manipulative practices such as pump-and-dump schemes, wash trading, and insider trading. This study found that exchanges like BitOasis and BitoPro experience amplified risks due to limited oversight and inconsistent regulatory enforcement, corroborating Putniņš and Dhawan (2022), who argued that poorly regulated platforms facilitate market manipulation. Similarly, Hamrick, Rouhi, and Mukherjee (2021) highlighted that coordinated buying and artificial trading volumes distort market perception, which aligns with the current study's evidence of inflated volumes on certain UAE exchanges.

The study's findings further demonstrate that fragmented supervision and lack of real-time surveillance tools exacerbate vulnerabilities, confirming Schry and Griner (2021) that institutional capacity is critical in mitigating market abuse. The results also indicate that, compared to mature markets like the US and EU, UAE exchanges face structural challenges in enforcing compliance and monitoring activity, echoing Fry and Cheah (2021) on the necessity of coordinated oversight to preserve market integrity.

Guided by Institutional Theory, specifically the coercive pressures assumption, the study highlights that strong legal mandates and regulatory enforcement are essential for shaping institutional behavior and improving adherence to market integrity standards. These findings underscore that technological investment, active monitoring, and harmonized regulatory frameworks are pivotal in reducing manipulative practices.

5.3 Cryptocurrencies and Money Laundering Risk

The study found that cryptocurrencies amplify traditional money laundering risks due to their pseudonymous and decentralized characteristics. The findings indicate that illicit funds can rapidly enter, layer, and integrate into the financial system through digital assets, corroborating Ernesto and Longa (2021), who emphasized the challenges in tracing transactions across multiple stages. The study's analysis further demonstrates that privacy-focused cryptocurrencies like Monero and Zcash, alongside mixers and peer-to-peer platforms, significantly hinder forensic tracing, echoing Hazar and Boydas (2022) on the technological obstacles to effective AML enforcement.

Moreover, the findings reveal that cross-border transfers and regulatory arbitrage compound these risks, aligning with FATF guidance (2020; 2023) on the necessity of global coordination and VASP compliance. The study highlights that conventional AML frameworks, designed for centralized banking, struggle to address rapid, pseudonymous transactions, corroborating Zdanovic (2022) on the mismatch between legal instruments and decentralized networks. Consequently, in the UAE context, the findings demonstrate that fragmented supervision and limited inter-agency coordination further weaken oversight, reflecting Al Tamimi & Co. (2022) observations. Guided by Institutional Theory, specifically the normative pressures assumption, the study shows that professional standards and ethical expectations are critical in shaping institutional behavior, suggesting that enhanced compliance culture, risk-based monitoring, and coordinated regulatory practices are essential to mitigate cryptocurrency-related money laundering risks.

5.4 UAE Cryptocurrency Regulatory Framework and Institutional Alignment

The study found that the UAE has developed a comprehensive legal framework for cryptocurrencies, integrating federal decrees and emirate-specific laws such as Federal Decree-Law No. 20 of 2018, Cabinet Decision No. 10 of 2019, and Dubai Law No. 4 of 2022. The findings reveal that this multifaceted architecture demonstrates an intentional alignment with international best practices, corroborating literature highlighting the UAE's efforts to model regulatory structures after established jurisdictions like the SEC, EU MiCA, and FATF guidance (FATF, 2020; IMF, 2024). The study's analysis further demonstrates that such mimicry reflects a strategic adoption of proven compliance and licensing protocols to enhance legitimacy and investor confidence.

Moreover, the study reveals that operational effectiveness depends on inter-agency coordination among VARA, SCA, and the UAE Central Bank. Regulatory overlaps and fragmented reporting systems create challenges for consistent supervision, echoing literature that emphasizes the difficulties of multi-layered governance frameworks in emerging fintech markets (Arabian Business, 2023). These findings highlight that while legal instruments are robust on paper, practical enforcement requires harmonized protocols and real-time oversight mechanisms.

Finally, the study highlights that the UAE's adaptation of international regulatory exemplars illustrates the mimetic pressure assumption of Institutional Theory, where organizations adopt practices from recognized leaders to achieve legitimacy. The findings indicate that continued benchmarking against global standards remains central to enhancing regulatory coherence and market integrity in the UAE.

5.5 AML Enforcement Challenges in UAE Virtual Assets

The study demonstrates that AML enforcement for virtual assets in the UAE is hindered by the pseudonymous and decentralized nature of cryptocurrencies, particularly privacy-focused coins such as Monero and Zcash, along with mixers and decentralized platforms. The study findings highlight that these technological characteristics complicate the identification of beneficial ownership and reduce the efficacy of traditional AML mechanisms, corroborating prior research on blockchain-related enforcement challenges (Hazar & Boydas, 2022; FATF, 2020). The study further demonstrates that technological limitations and fragmented supervision across federal and emirate-level authorities, including VARA and SCA, exacerbate these difficulties, confirming literature emphasizing the operational gaps in emerging fintech jurisdictions (IMF, 2024). Moreover, the study highlights that inconsistent VASP monitoring and weak inter-agency coordination hinder timely intervention and compliance assurance. These findings underscore the influence of normative pressures, as professional norms and ethical expectations shape the conduct of regulatory bodies and institutions tasked with enforcing AML obligations. Similarly, organizational isomorphism is evident, as UAE authorities have begun modeling supervision frameworks and reporting protocols after international exemplars to achieve coherence and legitimacy, though practical implementation remains uneven.

Collectively, the findings indicate that despite comprehensive legal frameworks, enforcement gaps persist, illustrating how institutional norms and structural convergence influence regulatory effectiveness. The study's analysis was guided by Institutional Theory, emphasizing these assumptions to explain AML compliance challenges.

6-Conclusion

This study provides a thorough examination of the legal, regulatory, and institutional aspects of cryptocurrencies and virtual assets in the UAE. The first part of the study covers the legal nature and classification of cryptocurrencies, analyzing their hybrid status and the challenges of fitting them into traditional categories such as property, currency, or securities. It highlights how decentralized technologies complicate existing legal frameworks and underscores the need for regulatory approaches that accommodate both technological innovation and economic function. The second part of the study delves into cryptocurrency market manipulations and regulatory vulnerabilities. It examines various forms of market abuse, including coordinated trading schemes, artificial volume inflation, and exploitation of non-public information. The discussion emphasizes how fragmented oversight, limited surveillance tools, and heterogeneous governance structures create conditions that allow such practices to persist. This section further considers the implications for emerging fintech hubs, illustrating the necessity for robust regulatory mechanisms and active enforcement to maintain market integrity. The third part of the study covers money laundering risks associated with digital assets. It explores the implications of pseudonymity, privacy-enhanced cryptocurrencies, peer-to-peer platforms, and rapid cross-border transfers for traditional anti-money laundering frameworks. This section demonstrates how the operational characteristics of cryptocurrencies require adaptive regulatory strategies, enhanced monitoring, and coordinated efforts among authorities to mitigate risks and strengthen compliance. The fourth part of the study further addresses the UAE's cryptocurrency legal frameworks and institutional oversight, detailing federal decrees, emirate-level laws, and the roles of multiple supervisory authorities. It examines the interplay between comprehensive legal structures and practical enforcement challenges, including coordination, data-sharing, and supervision. This section emphasizes the importance of harmonized regulatory practices and effective institutional capacity to ensure consistent compliance and safeguard the integrity of cryptocurrency markets. Overall, the study adopts a qualitative research methodology and is guided by Institutional Theory, particularly the coercive pressures assumption, highlighting how legal mandates shape regulatory practices and institutional behavior in the UAE's cryptocurrency ecosystem.

References

- Aidoo, S., & Int Dip, A. M. L. (2025). Cryptocurrency and Financial Crime: Emerging Risks and Regulatory Responses.
- Al Tamimi & Co. (2022). Virtual assets and anti-money laundering in the UAE: Regulatory insights. Al Tamimi Legal Publications.
- Al Jwaniat, Marcelle Issa, Amjad Safori, Khaleaf Al-Tahat, Ahmed Mansoori, and Mohammad Habes. 2023. "Investigating the Approaches to Improve Journalism Practices in Jordan: Data Journalism Perspective." Pp. 811–20 in Artificial Intelligence (AI) and Finance. Springer.
- Al Tamimi & Co. (2022). Virtual assets regulation in the UAE: Compliance and oversight challenges. Al Tamimi Legal Publications.
- Al-Tawil, T. N. E., & AlOmrn, N. (2025). Foreign direct investment and money laundering in the UAE: implications for research and practice. *Journal of Money Laundering Control*.
- Arabian Business. (2023). Dubai suspends BitOasis crypto license over regulation failure. Arabian Business.
- Arner, D. W., Barberis, J. N., & Buckley, R. P. (2020). Fintech, regtech, and the reconceptualization of financial regulation. *Journal of Financial Regulation*, 6(1), 1–35.
- Arner, D. W., Barberis, J., & Buckley, R. P. (2022). Fintech, digital finance, and regulatory implications. Oxford University Press.
- Commodity Futures Trading Commission. (2023). CFTC regulation of digital assets. U.S. Government.
- Creswell, J. W. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications
- De Filippi, P., & Wright, A. (2018). Blockchain and the law: The rule of code. Harvard University Press.
- Denzin, N. K., & Lincoln, Y. S. (2018). *The Sage handbook of qualitative research* (5th ed.). Sage Publications.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160.
- Dubai Government. (2022). Law No. 4 of 2022 regulating virtual assets. Dubai Government Legal Affairs Department.
- Elareshi, Mokhtar, Mohammed Habes, Amjad Safori, Razaz Waheeb Attar, Muhammad Noor Al adwan, and Waleed Mugahed Al-Rahmi. 2023. "Understanding the Effects of Social Media Marketing on Customers' Bank Loyalty: A SEM Approach." *Electronics* 12(8):1822.
- Ernesto, A., & Longa, A. (2021). Cryptocurrency and the three stages of money laundering: An analytical review. *Journal of Financial Crime*, 28(4), 1125–1142. <https://doi.org/10.1108/JFC-09-2020-0147>
- European Parliament & Council. (2023). Markets in Crypto Assets (MiCA) Regulation. Official Journal of the European Union.
- Eziokwudimma, N. V. (2025). The Regulation Of Cryptocurrencies And Their Use In Facilitating Crime: A Critical Analysis Of The Nigerian Experience. *Alex-Ekwueme Federal University Faculty Of Law Ll. B Projects*.
- FATF. (2020). Guidance for a risk-based approach to virtual assets and virtual asset service providers. Financial Action Task Force.
- FATF. (2020). Mutual evaluation report: UAE AML/CFT framework. Financial Action Task Force.
- FATF. (2023). Follow-up report on UAE AML/CFT measures. Financial Action Task Force.
- FATF. (2023). Updated guidance on virtual assets and virtual asset service providers. Financial Action Task Force.
- Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798–1853. <https://doi.org/10.1093/rfs/hhz015>
- Fry, J., & Cheah, E.-T. (2021). Wash trading at cryptocurrency exchanges. *Finance Research Letters*, 44, 102011. <https://doi.org/10.1016/j.frl.2021.102011>
- Gandal, N., Hamrick, J. T., & Moore, T. (2018). Price manipulation in cryptocurrency markets. *Journal of Monetary Economics*, 95, 86–96. <https://doi.org/10.1016/j.jmoneco.2018.01.003>
- Garth, B. G., & de Haan, T. (2018). Doctrinal research in law: A practical guide. *Law & Method*, 12(2), 1–24.
- Gilbert, C., & Gilbert, M. (2025). Patterns and vulnerabilities of cryptocurrency-related cybercrimes. *Available at SSRN 5196069*.
- Habes, Mohammad, Mahmoud Alghizzawi, Mokhtar Elareshi, Abdulkrim Ziani, Mohammad Qudah, and Maryam Mohammed Al Hammadi. 2023. "E-Marketing and Customers' Bank Loyalty Enhancement: Jordanians' Perspectives." Pp. 37–47 in *The Implementation of Smart Technologies for Business Success and Sustainability*. Springer.
- Hamrick, J. T., Rouhi, F., Mukherjee, A., et al. (2021). An examination of the cryptocurrency pump-and-dump ecosystem. *Information Processing & Management*, 58(6), 102709. <https://doi.org/10.1016/j.ipm.2021.102709>
- Hazar, B., & Boydas, H. (2022). Privacy coins and blockchain anonymity: Implications for financial crime. *Computer Law & Security Review*, 45, 105644. <https://doi.org/10.1016/j.clsr.2022.105644>
- Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin Law Review*, 17(1), 83–119.
- IMF. (2024). United Arab Emirates: Financial sector assessment report. International Monetary Fund.

- International Monetary Fund. (2024). United Arab Emirates: Financial sector assessment program update (IMF Country Report No. 24/xx). IMF.
- Kshetri, N. (2021). Blockchain's roles in strengthening AML and counter-terrorism financing regulations. *Journal of Financial Crime*, 28(1), 44–61.
- Megdadi, Younes, Mahmoud Hussien Abu Jumaa, Mahmoud Alghizzawi, Zaid Megdad, Dina Naser Tahat, Khalaf Tahat, and Mohammed Habes. 2023. "The Effect of Social Media on Improving the Recruitment Process: Regional Commercial Banks' Employee Engagement as a Mediator." Pp. 1–7 in 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS). IEEE.
- Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340–363.
- Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. 2013 APWG eCrime Researchers Summit, 1–14. <https://doi.org/10.1109/eCRS.2013.6809139>
- Putniņš, T. J., & Dhawan, A. (2022). A new wolf in town? Pump-and-dump manipulation in cryptocurrency markets. *Review of Finance*, 27(3), 935–963. <https://doi.org/10.1093/rof/rfab069>
- Ramesh, S. (2025). Cryptocurrencies. In *The Political Economy of Contemporary Human Civilisation, Volume II: From Quantum Computing and Nuclear Fusion to War and Conflict* (pp. 93-140). Cham: Springer Nature Switzerland.
- Raskin, M., & Yermack, D. (2022). Digital currencies, decentralization, and the blockchain. *Journal of Economic Perspectives*, 36(4), 205–232.
- Schry, D., & Griner, H. (2021). Detecting cryptocurrency pump-and-dump frauds using market and social signals. *Expert Systems with Applications*, 182, 115264. <https://doi.org/10.1016/j.eswa.2021.115264>
- Scott, H. S. (2019). *The law of cryptocurrencies*. Oxford University Press.
- Scott, W. R. (2008). *Institutions and organizations: Ideas and interests*. Sage Publications.
- Securities and Exchange Commission. (2020). Framework for "investment contract" analysis of digital assets. SEC.
- Tahat, Dina Naser, Mokhtar Elareshi, Khalaf Tahat, Marcelle A. Al Jwaniat, Mohammed Habes, and Abdulkrim Ziani. 2022. "News Media and Political Participation in the Middle East: Jordan as an Example." Pp. 1–8 in 2022 International Arab Conference on Information Technology (ACIT). IEEE.
- Tahat, Khalaf, Ahmed Mansoori, Dina Tahat, and Mohammed Habes. 2024. "Examining Opinion Journalism in the United Arab Emirates National Press: A Comparative Analysis." *Newspaper Research Journal* 07395329241255159.
- Tahat, Khalaf, Dina Naser Tahat, Ahmed Masoori, Mohammad Habes, Emad Alghazo, and Najia Ketbi. 2023. "Role of Social Media in Changing the Social Life Patterns of Youth at UAE." Pp. 152–63 in *Artificial Intelligence (AI) and Finance*. Springer.
- Tahat, Khalaf, Mohammed Habes, Ahmed Mansoori, Noura Naqbi, Najia Al Ketbi, Ihsan Maysari, Dina Tahat, and Abdulaziz Altawil. 2024. "Social Media Algorithms in Countering Cyber Extremism: A Systematic Review." *Journal of Infrastructure, Policy and Development* 8(8):6632.
- Tahat, Khalaf, Said Salloum, Ahmed Mansoori, Dina Tahat, Mohammad Habes, Khaled Shaalan, Noura Naqbi, Razaz Waheeb Attar, and Emad Alghazo. 2023. "Uncovering the Share Fake News on Social Media During Crisis." Pp. 1–6 in 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS). IEEE.
- UAE Cabinet. (2019). Cabinet Decision No. 10 of 2019 on AML procedures. UAE Cabinet.
- UAE Federal Government. (2018). Federal Decree-Law No. 20 of 2018 on AML/CFT. UAE Government Legal Publications
- UAE Federal Government. (2021). Federal Decree-Law No. 46 of 2021 on electronic transactions and trust services. UAE Government Legal Publications.
- VARA. (2023). Virtual Assets Regulatory Authority annual report 2023. VARA, Dubai.
- Werbach, K., & Cornell, N. (2017). *Bitcoin and blockchain law: The legal implications of decentralized ledgers*. University of California Press.
- Zdanovic, N. (2022). The limits of traditional AML frameworks in decentralized finance. *Journal of Money Laundering Control*, 25(3), 487–504. <https://doi.org/10.1108/JMLC-01-2022-0007>
- Zdanovic, N. (2023). Institutional determinants of AML enforcement in cryptocurrency markets. *Journal of Money Laundering Control*, 26(4), 567–589.