Crystal Intelligence



Navigating Crypto Regulation and Risk in the MENA Region:

A Guide for Regulators and Compliance Professionals

Authored by the Marketing Team, Crystal Intelligence, April 2025.
Copyright information

Contents

Introduction 02

The Evolving Crypto Regulatory Landscape in MENA 03

Emerging trends 04

Key Risks in the MENA Crypto Sector 05

Best Practices for Compliance and Risk Mitigation 07

Case Study of the Gulf Cooperation Countries 12

United Arab Emirates (UAE) 13

Kingdom of Saudi Arabia 16

Kingdom of Bahrain 18

State of Qatar 21

State of Kuwait 23

Sultanate of Oman 26

MENA Crypto Regulation and Risks: Recommendations and Conclusions 29

This report was compiled from:

Proprietary knowledge accrued by Crystal Intelligence Investigations and research teams

https://blogs.loc.gov/law/2025/01/falqs-regulation-of-cryptocurrencies-in-the-gulf-cooperation-council-countries-part-one/

https://blogs.loc.gov/law/2025/01/regulation-of-cryptocurrencies-in-the-gulf-cooperation-council-gcc-countries-part-two/

By Elin Hofverberg

https://www.worldometers.info/world-population/

https://www.triple-a.io/cryptocurrency-ownership-data

https://coinatmradar.com/

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

Introduction

The Middle East and North Africa (MENA) region is quickly emerging as a vital player in the global crypto ecosystem. From Dubai's crypto-friendly free zones to the tightening regulations in Kuwait and Qatar, the region showcases a broad spectrum of regulatory stances.

This dynamic environment provides opportunities—but also presents significant risks. As digital assets become increasingly integrated into the financial framework of MENA economies, regulators, compliance teams, law enforcement agencies, and crypto service providers experience growing pressure to stay ahead of evolving threats such as fraud, terrorism financing, and regulatory loopholes.

This report serves as a practical guide for professionals navigating the crypto landscape in MENA. It outlines the key regulatory trends shaping the region, identifies major financial crime risks, and shares actionable strategies for compliance and risk mitigation.

We also examine the regulatory approaches of Gulf Cooperation Council (GCC) countries in detail, offering jurisdiction-specific insights into adoption patterns, enforcement challenges, and AML/CFT vulnerabilities.

Whether you're building a compliance framework, developing regulatory policy, or conducting investigations, this resource aims to support informed decision-making and proactive engagement with the region's crypto ecosystem.

This report reflects the evolving ground realities across MENA based on intelligence gathered and analyzed by Crystal's investigations and policy teams.

Our goal is to support informed decision-making and proactive engagement with the region's crypto ecosystem, whether you're building a compliance framework, developing regulatory policy, or conducting investigations.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



The Evolving Crypto Regulatory Landscape in MENA

The regulatory environment for cryptocurrencies in the MENA region is diverse, reflecting the positions of its varied countries. Some governments are swiftly adopting clear, supportive frameworks to attract digital asset companies, while others are opting for a more cautious or restrictive approach, motivated by worries regarding financial crime, market volatility, and investor protection. Others yet have implemented near-total prohibitions.

Introduction

The United Arab Emirates (UAE) and Bahrain are leading the way in setting up comprehensive legal frameworks to license and monitor crypto service providers. Dubai's VARA and Abu Dhabi's FSRA are examples of proactive regional regulators working to create safe, innovation-friendly ecosystems.

In contrast, countries like Kuwait and Qatar maintain stiff restrictions or outright bans on most crypto activities. Their policies reflect a more conservative stance, often influenced by concerns over terrorism financing and speculative risk.

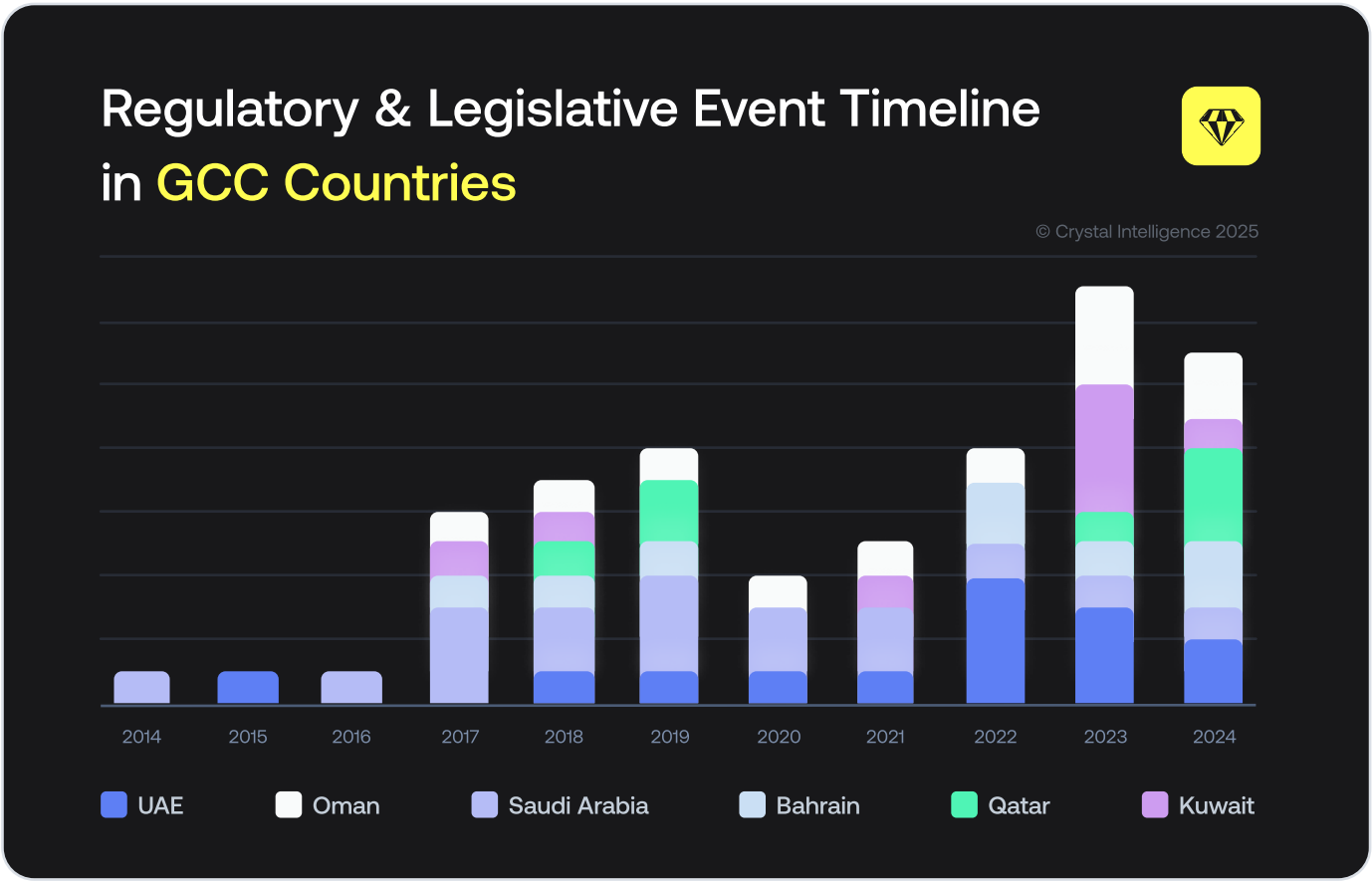
Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

Emerging trends

There are several key trends shaping the regulatory approach to cryptocurrencies in the MENA region:

- Licensing and Compliance Requirements: Many MENA jurisdictions require crypto firms to obtain licenses and comply with Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) measures.
- An interest in Central Bank Digital Currencies (CBDCs): Several countries, including Saudi Arabia and the UAE, are actively exploring CBDCs as an alternative to decentralized cryptocurrencies.
- Tax Clarity and Incentives: While many countries lack clear tax guidelines for crypto, countries like the UAE have implemented a business-friendly framework to attract digital asset companies.
- Cross-Border Regulatory Collaboration: MENA regulators are increasingly working with international bodies and each other to achieve regulatory alignment.

Below is a timeline of legislative developments in a selection of countries in MENA, namely the Gulf Cooperation Council (GCC) countries, that highlights this shift, showing a rise in crypto-specific regulatory actions since 2014 as governments aim to balance innovation with financial security.



Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



Key Risks in the MENA Crypto Sector

As cryptocurrency adoption increases across MENA, so too do the risks associated with digital assets. These risks aren't hypothetical—they're already being exploited, especially in jurisdictions with uneven regulatory coverage or weak enforcement. Below are the primary risk areas that regulators, compliance teams, and law enforcement must monitor closely.

1. Money Laundering and Terrorism Financing

The pseudo-anonymous nature of cryptocurrencies makes them susceptible to misuse for illicit activities. Due to the region's complex geopolitical landscape, proximity to conflict zones, and exposure to terrorist threats, the Financial Action Task Force (FATF) specifically urged MENA countries to implement robust AML/CTF measures to mitigate illegal crypto usage threats – particularly around peer-to-peer (P2P) and over-the-counter (OTC) exchanges, which often operate with limited oversight.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

2. Fraud, Scams and Ponzi Schemes

Crypto-related scams, such as Ponzi schemes and rug pulls, have been on the rise in MENA. Regulators are actively cracking down on fraudulent operations, but many remain undetected due to the industry's decentralized nature and weak KYC enforcement in some jurisdictions.

3. Regulatory Arbitrage

Due to inconsistencies in regulations across MENA, some crypto businesses engage in regulatory arbitrage—seeking jurisdictions with looser compliance requirements. This can create enforcement challenges and increase financial risk for investors.

4. Cybersecurity Threats and Hacks

DeFi platforms, centralized exchanges, and wallet providers operating in MENA are frequent targets of hacks, phishing campaigns, and insider threats. Many countries lack formal cybersecurity standards for crypto businesses, putting customer funds and sensitive data at risk.

Key concerns include:

- Lack of mandatory security audits
- Inadequate incident response protocols
- Use of outdated or vulnerable infrastructure

5. Lack of Investor Protection

Retail investors often engage with crypto platforms without fully understanding the risks involved. In cases of exchange failures or fraudulent ICOs, many find themselves with little or no legal recourse. Consumer protection laws across much of the region are still catching up with digital assets.

This gap is especially problematic as adoption increases through informal channels like Telegram groups, WhatsApp communities, and Peer-to-Peer marketplaces —often lacking clear disclosure requirements or dispute resolution mechanisms.

6. Misuse of Crypto Gift Cards and Vouchers

While not wholly negative, the rise in popularity of cryptocurrency gift cards does raise the risk of illicit activities such as money laundering and terrorism financing (ML/TF). These cards can be traded or sold in Peer-to-Peer markets without proper identity verification, making them attractive tools for layering illicit transactions.

Understanding the key risks is only half the challenge.

For regulators, compliance teams, and crypto businesses operating in the MENA region, the next step is building the internal controls, partnerships, and regulatory alignment needed to effectively manage those risks.

The following best practices offer a practical blueprint for reducing exposure to financial crime, protecting users, and strengthening the overall integrity of the crypto ecosystem in the region.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



Best Practices for Compliance and Risk Mitigation

with Region-Specific Examples from the MENA Region

As crypto adoption grows across MENA, regulators, compliance officers, and service providers must adopt proactive strategies to minimize risk and strengthen oversight. The following best practices, backed by developments already unfolding in the region, offer a grounded framework for action.

1. Focus on Strengthening AML and KYC Programs

Robust Know Your Customer (KYC) and Anti-Money Laundering (AML) measures remain essential to tackling financial crime. Key controls include:

- Customer identity verification and ongoing due diligence
- Transaction monitoring and screening against sanction lists
- Prompt reporting of suspicious activity to national authorities

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

Example: UAE

The UAE's Federal Decree-Law No. (20) of 2018, along with subsequent Cabinet Resolutions, mandates AML/CTF compliance for all virtual asset service providers (VASPs), including risk assessments and transaction monitoring. The Central Bank's 2023 guidance outlines how financial institutions must handle exposure to crypto.

Takeaway:

National-level guidance in the UAE offers a regulatory model that other MENA jurisdictions could follow to enforce baseline AML/KYC standards.

2. Ensure Licensing and Regulatory Compliance

Compliance starts with understanding and adhering to local licensing regimes. Organizations must:

- Identify and comply with national licensing frameworks
- Conduct regular reviews of legal obligations
- Implement internal audits to verify compliance alignment

Example: Bahrain

Bahrain's Central Bank established a full regulatory framework for crypto in 2019, including licensing conditions for exchanges and wallet providers. It emphasizes the integration of digital assets into the financial system while protecting consumer interests.

Takeaway:

Licensing clarity helps build legitimacy and creates a level playing field for compliant businesses.

3. Prioritize Cybersecurity and Data Protection

As regional exchanges and DeFi platforms face rising attacks, cybersecurity should be central to compliance planning. Best practices include:

- Multi-factor authentication (MFA) and encryption
- Routine penetration testing and incident response planning
- Staff awareness training on cyber threats

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

Example: Oman

Crystal's investigations in Oman uncovered widespread scams using social platforms like Telegram and Facebook. Victims were targeted through fake investment and job offers demanding payment in crypto, highlighting the need for stronger digital security protocols and public awareness.

Takeaway:

Weak cybersecurity isn't just a tech issue—it's a compliance and reputational risk, especially where informal crypto adoption is growing.

4. Foster Regulatory Engagement and Collaboration

Regulatory clarity improves when governments, exchanges, and law enforcement work together. Effective engagement includes:

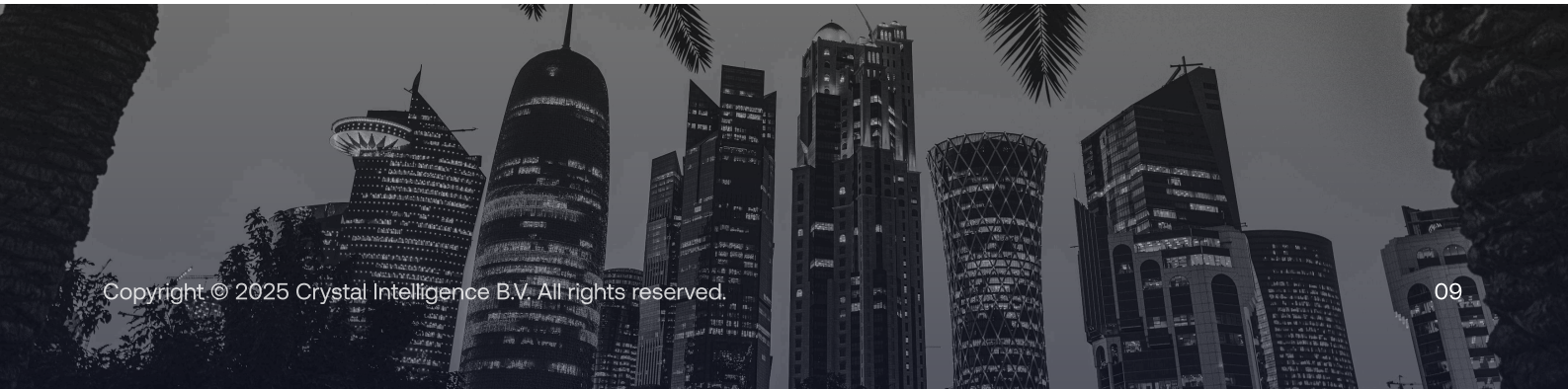
- Participation in regulatory sandboxes
- Public-private partnerships on financial crime intelligence
- Joint discussions on emerging technologies like DeFi and NFTs

Example: Qatar

Although previously restrictive, Qatar introduced its Digital Assets Regulations and Investment Token Rules in 2024, signaling a willingness to engage with digital asset frameworks under strict conditions. The shift opens up new avenues for regulated entities to collaborate with authorities.

Takeaway:

Constructive engagement helps shape clearer, more functional crypto laws and improves enforcement readiness.



Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

5. Monitor Peer-to-Peer Markets and Emerging Threat Vectors

Not all crypto activity flows through licensed exchanges. Peer-to-Peer platforms, OTC trades, and the use of crypto vouchers (like gift cards) introduce new challenges for regulators and compliance teams. Effective mitigation includes:

- Monitoring high-risk Peer-to-Peer activity and transaction volumes
- Requiring Peer-to-Peer platforms to implement identity verification
- Sharing typologies of misuse involving digital gift cards and informal markets

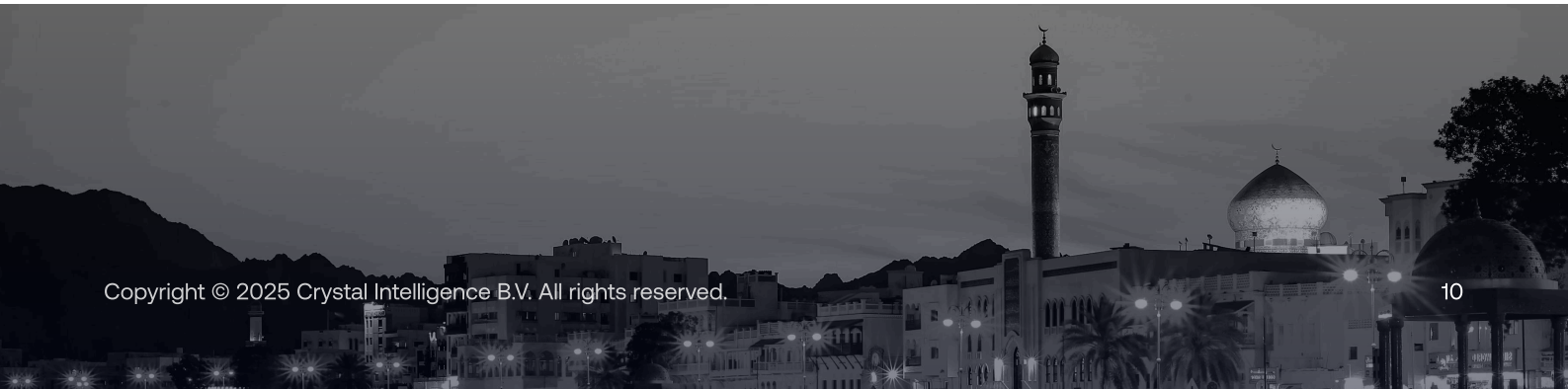
Example: Oman

Similar P2P dynamics were observed in Oman, where scams and illegal content purchases are facilitated by informal crypto activity. The decentralized nature of these platforms complicates enforcement and increases anonymity risks.

Takeaway:

Even in restrictive jurisdictions, crypto activity thrives underground. P2P and gift card monitoring must be prioritized—even when formal regulation appears strict.

While these practices form a strong foundation for mitigating risk, their application varies significantly across jurisdictions.



Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

The Future of Crypto Regulation in MENA

As the digital asset ecosystem matures, MENA regulators face growing pressure to balance innovation with financial security. The next phase of crypto regulation in the region will likely be shaped by four key priorities.

1. Balancing Innovation with Risk Management Security

MENA regulators must balance fostering innovation with ensuring financial security. Policies should encourage blockchain adoption while safeguarding against risks like fraud and market manipulation.

What to watch:

- Sandboxes for DeFi and stablecoin pilots
- Region-specific guidance on NFTs and tokenized assets
- Proactive rulemaking to stay ahead of financial crime trends

2. Expanding Cross-Border Regulatory Cooperation

Given the global nature of cryptocurrencies, MENA regulators must collaborate with international bodies like FATF, the IMF, and regional counterparts to enhance cross-border enforcement.

What to watch:

- Growing ties with FATF, IMF, and regional working groups
- Bilateral and multilateral MOUs between regulators
- Shared typologies and enforcement coordination on illicit flows

3. Adoption of Regulatory Technology (RegTech)

RegTech solutions, such as blockchain analytics and AI-driven compliance tools, can help regulators and financial institutions monitor transactions effectively and reduce financial crime risks.

What to watch:

- Use of blockchain analytics by regulators
- AI-based transaction monitoring in financial institutions
- Automated KYC/AML solutions integrated into national systems

4. Growth of Institutional Crypto Adoption

With increasing institutional interest in crypto, regulatory clarity will be crucial for attracting foreign investment and fostering a robust digital asset ecosystem in the MENA region.

What to watch:

- Clear licensing models for institutional-grade custodians
- Tax guidance and reporting standards for digital assets
- Integration of crypto into broader fintech and investment frameworks

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



Case Study of the Gulf Cooperation Countries

The Gulf Cooperation Council (GCC) is a regional cooperative body of six affiliates, including the UAE, Saudi Arabia, Bahrain, Qatar, Kuwait, and Oman. We will describe their overall crypto adoption trends, regulatory frameworks, and the financial crime risks they face.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



United Arab Emirates (UAE)

The UAE is the MENA region's most proactive jurisdiction regarding crypto regulation and adoption. Its federal government and forward-leaning emirates like Dubai and Abu Dhabi have established legal frameworks to attract crypto investment while maintaining regulatory oversight.

The UAE is a federally governed country consisting of three Emirati. At the national government level, crypto is regulated by the Securities and Commodities Authority (SCA), although each Emirate has regional equivalents.

Population	11.3 M
% Owning or Using Crypto	30%
Crypto Sandboxes	3
Crypto ATMs	1

Regulatory Framework

At the federal level, the UAE's regulatory evolution includes:

Federal Decree-Law No. (20) of 2018

Defines virtual assets (VAs) and virtual asset service providers (VASPs) and introduced AML/CFT obligations for them

Cabinet Resolution No. (24) of 2022

Broadened definitions to include emerging financial technologies and clarified obligations on VASPs for risk assessment and transaction monitoring.

SCA Decision No. (23) of 2020:

Regulated crypto issuance and trading with mandatory licensing

Cabinet Resolution No. (111) of 2022

Formally designated the SCA as the primary regulator introduced a comprehensive framework for virtual assets and VASPs and mandated local licensing cooperation.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

Central Bank Guidance (February 2023)

Issued risk management guidelines for licensed financial institutions engaging with virtual assets and VASPs.

Cabinet Decision No. (100) of 2024

Exempted most virtual asset transactions from the standard 5% Value Added Tax (VAT), effective November 15, 2024.

Emirate-Specific Regulations:



Dubai:

Home to the Virtual Asset Regulatory Authority (VARA) established in 2022 as the primary regulatory body for digital assets.



Abu Dhabi:

Regulated by the Financial Services Regulatory Authority (FSRA) under the Abu Dhabi Global Market (ADGM), offering a separate licensing regime.



Ras Al Khaimah:

Established RAK Digital Assets Oasis (RAK DAO), a free zone for the development of the crypto ecosystem in the Emirate.

AML/CFT Risks

Despite regulatory clarity, the UAE still faces financial crime risks, particularly in areas where enforcement and informal trading intersect:

1. Unregulated Peer-to-Peer and OTC Exchanges

These platforms allow for pseudo-anonymous trading, often bypassing formal AML controls.

2. Russian-speaking Peer-to-Peer markets

The presence of Russian-language platforms poses unique enforcement and cross-border cooperation challenges.

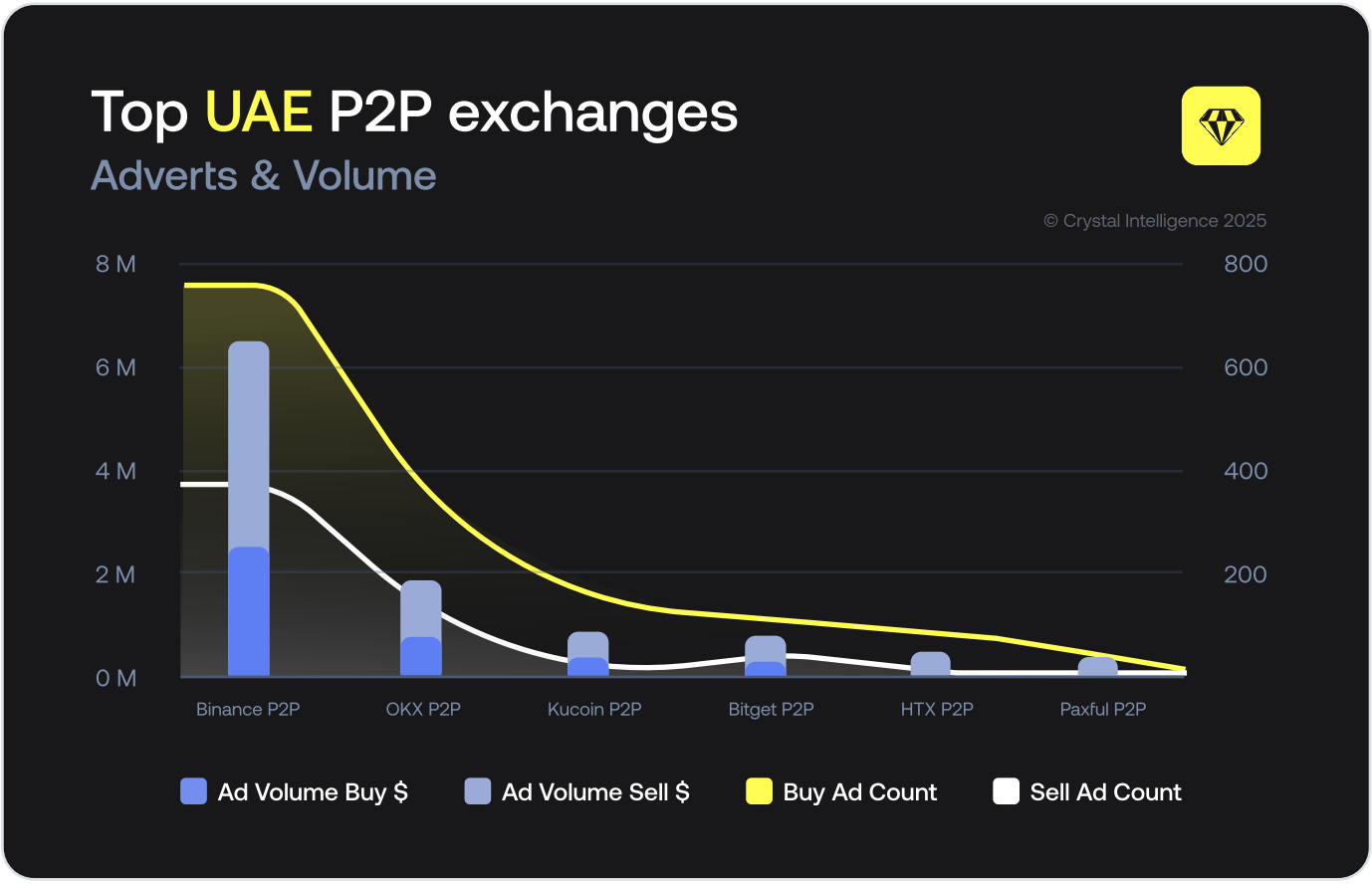
3. Illicit crypto use in prostitution, gambling, and pharmaceuticals

These high-risk sectors often rely on crypto for transactions and can involve payments with cryptocurrencies. These issues can variously be tied to child sexual abuse, human trafficking, money laundering, fraud, and scams, which require collaboration between law enforcement and regulators.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

Crypto Focus Area on Peer-to-Peer Exchanges

The chart below shows peer-to-peer exchange trading activity in Dirham (AED) in the UAE over the 24-hour period of July 17, 2024.



The UAE's appetite is for Sell Ads (seeking to buy crypto from visitors) over Buy Ads (which sell crypto to visitors). Binance also dominates in popularity.

Overall, there were 1,467 ads worth AED 10,014,688.96 during the monitored period.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



Kingdom of Saudi Arabia

Saudi Arabia has taken a cautious approach to cryptocurrencies, with limited legal frameworks and clear restrictions on institutional involvement. While crypto adoption is growing among individuals, financial institutions remain barred from direct participation.

Regulatory Framework

- The Saudi Central Bank (SAMA) issued warnings about crypto-related risks in 2018 but has not enacted comprehensive crypto legislation.
- Financial institutions are prohibited from engaging in crypto transactions.
- Regulatory discussions around CBDCs are ongoing, and the central bank is exploring blockchain use cases—but within a tightly controlled environment.

Population	34.6 M
% Owning or Using Crypto	11.4%
Crypto Sandboxes	3
Crypto ATMs	0

Despite the absence of formal regulation, regulatory sandboxes exist to test fintech and blockchain innovations under supervision, signaling potential openness to future development.

AML/CFT Risks

Saudi Arabia faces a range of money laundering and terrorism financing threats involving crypto, especially due to its large trade volume and complex regional ties:

1. Trade-Based Money Laundering (TBML)

Criminal networks exploit import-export transactions using misinvoicing and falsified documentation to move illicit funds under the guise of legitimate trade.

2. Terrorism Financing via Informal Networks

Hawala systems and unregulated money transfer services are used to move funds covertly—often aided by crypto's pseudonymous nature.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

3. Cryptocurrency-Enabled Money Laundering

As crypto adoption rises, so do layering techniques, privacy-enhancing technologies, and cross-border transactions designed to obscure fund origin.

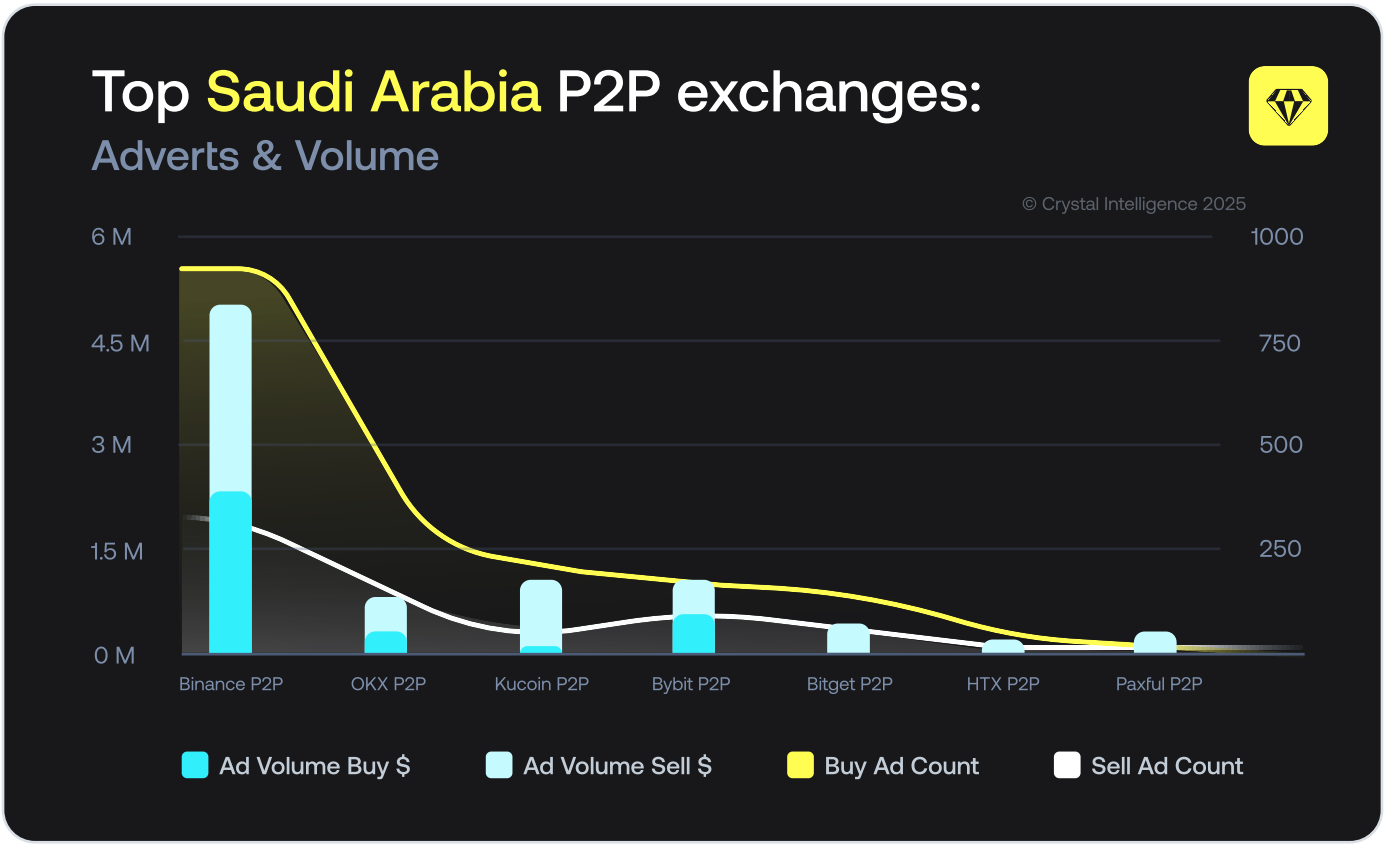
Additionally, there are various crypto-related challenges, including:

- Cryptocurrencies are used to pay for illicit services like pornography, frequently linked to child sexual abuse, and prostitution, often connected to human trafficking.
- They have also financed online gambling, which is prohibited in Saudi Arabia.
- Furthermore, cryptocurrencies have been used to buy illegal contraceptive drugs.

Crypto Focus Area on Peer-to-Peer Exchanges

Saudi authorities are particularly concerned with peer-to-peer platforms, which remain unlicensed and difficult to monitor. These informal channels are widely used despite regulatory prohibitions and pose high risk for financial crime.

The chart below shows Saudi riyal (SAR) activity over 24 hours and the number and volume of advertisements on Peer-to-Peer crypto exchanges on July 18, 2024.



The total number of Ads was 1363, for a total volume of SAR 6,986,438.53.
Binance was the dominant Peer-to-Peer Exchange.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



Kingdom of Bahrain

Bahrain has positioned itself as one of the most crypto-forward jurisdictions in the MENA region. Unlike many of its neighbors, it has embraced a regulated approach, aiming to integrate cryptocurrencies into its financial system while maintaining oversight.

Population	% Owning or Using Crypto	Crypto Sandboxes	Crypto ATMs
1.6 M	1%	1	0

Regulatory Framework

- The Central Bank of Bahrain (CBB) issued the Crypto-Asset Module in 2019, a comprehensive regulatory framework that brought digital assets under formal oversight—making Bahrain one of the region's early movers in crypto regulation.
- In 2021, Legislative Decree No. (4) expanded Bahrain's AML/CFT regime to include digital assets by broadening the definition of "money," ensuring crypto-related activities fall under financial crime compliance requirements.
- In 2022, the VAT Financial Services Guide (Credit and Financing Services, Version 1.3) introduced tax treatment for four categories of crypto tokens:

- **Mining rewards**

VAT-exempt, as mining is not considered an economic activity.

- **Exchange tokens**

(traded for fiat or other tokens): VAT-exempt as financial services.

- **Payment tokens**

used solely to pay for goods or services): Tax-exempt.

- **Utility tokens**

(used to supply goods/services): Subject to standard VAT.

Additional fees or commissions above the token value may be subject to VAT depending on how the transaction is categorized.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

AML/CFT Risks

As a major financial hub, Bahrain faces significant risks tied to the movement of illicit funds across borders. While its crypto regulations are among the most developed in the region, gaps in enforcement and evolving criminal typologies continue to present challenges.

1. Cross-border Financial Crime

Bahrain's role in global trade and finance increases its exposure to illicit flows via international transactions, trade finance, and offshore banking activity.

2. Cryptocurrency-Enabled Money Laundering

The expanding use of crypto assets in the region raises concerns around:

- Fraudulent ICOs
- Complex layering schemes that obscure asset origin
- Anonymity-enhanced transactions
- DeFi misuse

3. Terrorism Financing via Financial Institutions

Despite strict regulations, vulnerabilities persist in financial institutions, where inadequate due diligence or misuse of correspondent banking can facilitate terrorismrelated fund transfers

4. Illicit Activity via Social Platforms

Crystal's investigations identified multiple uses of crypto to facilitate illegal activity in Bahrain on social media such as Telegram:

- Payment for narcotics, prostitution, and gambling, all of which are prohibited
- Crypto use within Russian-language groups, including those tied to human trafficking of foreign women via fraudulent job offers

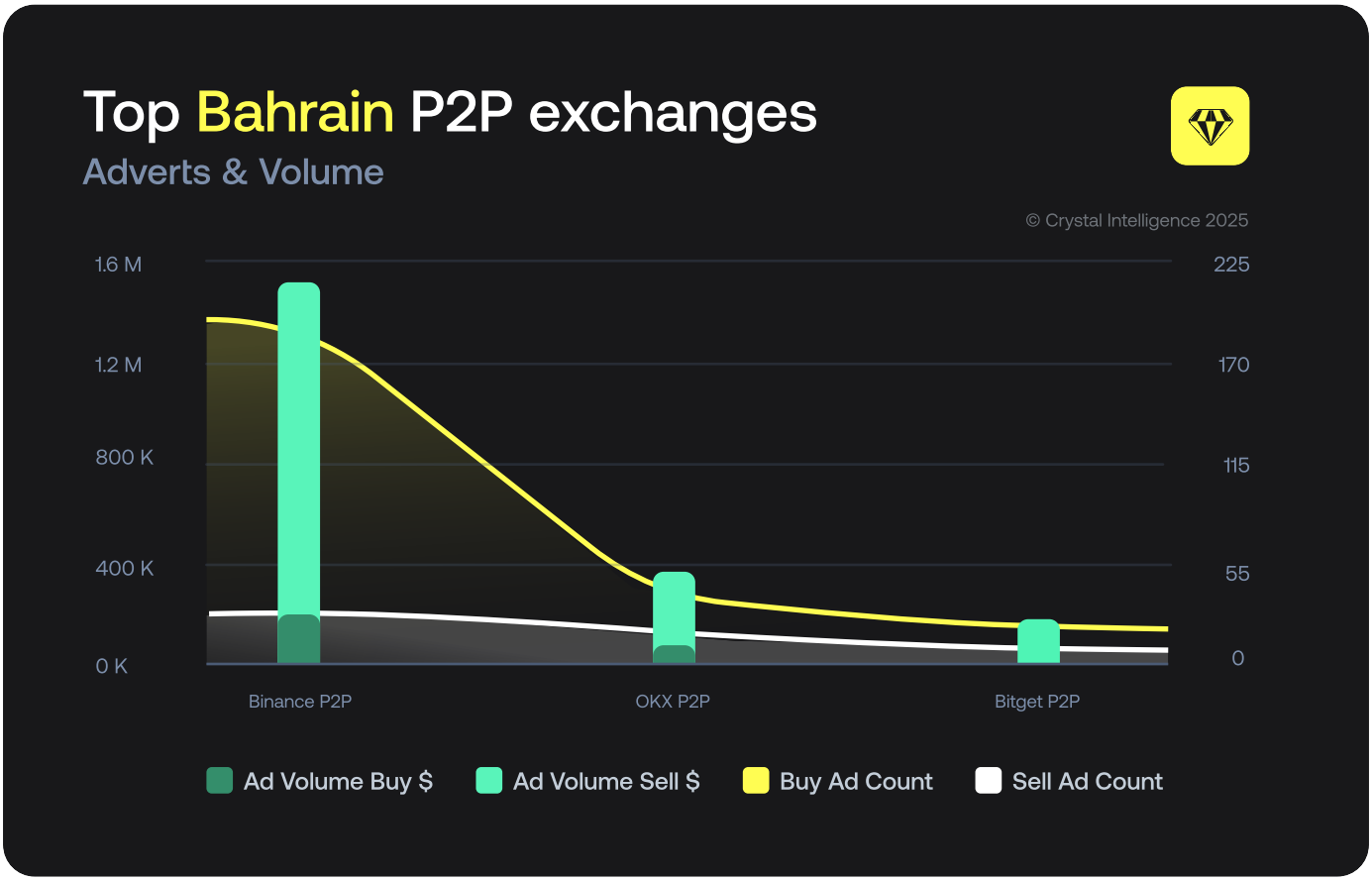
5. Unregulated Peer-to-Peer and Gift Card Risks

Binance gift cards and Peer-to-Peer exchanges—common throughout the MENA region—remain largely unregulated and are used to bypass formal compliance controls.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

Crypto Focus Area on Peer-to-Peer Exchanges

The chart below shows Bahraini dinar (BAR) activity over 24 hours and the number and volume of advertisements on Peer-to-Peer crypto exchanges on July 18, 2024.



A total of 284 Ads worth BAR 1,939,607 were traded during the period measured, with Binance the dominant Peer-to-Peer Exchange.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



State of Qatar

Qatar has historically taken a restrictive approach to cryptocurrencies, emphasizing caution over adoption. While recent regulatory updates suggest a shift toward controlled engagement, most crypto activities remain prohibited.

Population	% Owning or Using Crypto	Crypto Sandboxes	Crypto ATMs
3 M	1%	1	0

Regulatory Framework

- In 2018, the Qatar Central Bank (QCB) issued Circular No. (6) of 2018, which explicitly prohibited all local financial institutions from trading in cryptocurrencies.
- The Qatar Financial Centre Regulatory Authority (QFCRA) extended this prohibition in 2019 when it banned crypto activities within or from Qatar, citing concerns around financial crime and cybercrime. Further laws meant transgressors could face fines of up to QAR 10 million (about US$2.75 million) per violation and risk having licenses revoked or being suspended from the sector.
- In a shift, Digital Assets Regulations and Investment Token Rules were introduced in late 2024, creating a legal structure for some virtual asset use. However, cryptocurrencies remain excluded, treated under general asset laws governing tangible and intangible property.
- Violations can incur heavy penalties, including fines up to QAR 10 million (approx. USD 2.75 million) and license suspensions.

AML/CFT Risks

In addition to the traditional financial crime risks faced by Qatar, such as unregistered hawala networks, trade-based money laundering, and terrorism financing—often through charitable organizations—the country also encounters several crypto-specific AML/CTF risks.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

1. Sanctions Risk via Remittances

Expatriate communities in Qatar often use cryptocurrencies to send money home, including to sanctioned jurisdictions such as Syria and Lebanon—creating a risk of inadvertent sanctions violations.

2. Crypto Gift Card Abuse

Binance gift cards, popular across the MENA region, offer pseudo-anonymous crypto access that can be exploited for money laundering or terrorism financing.

3. Illicit Payments

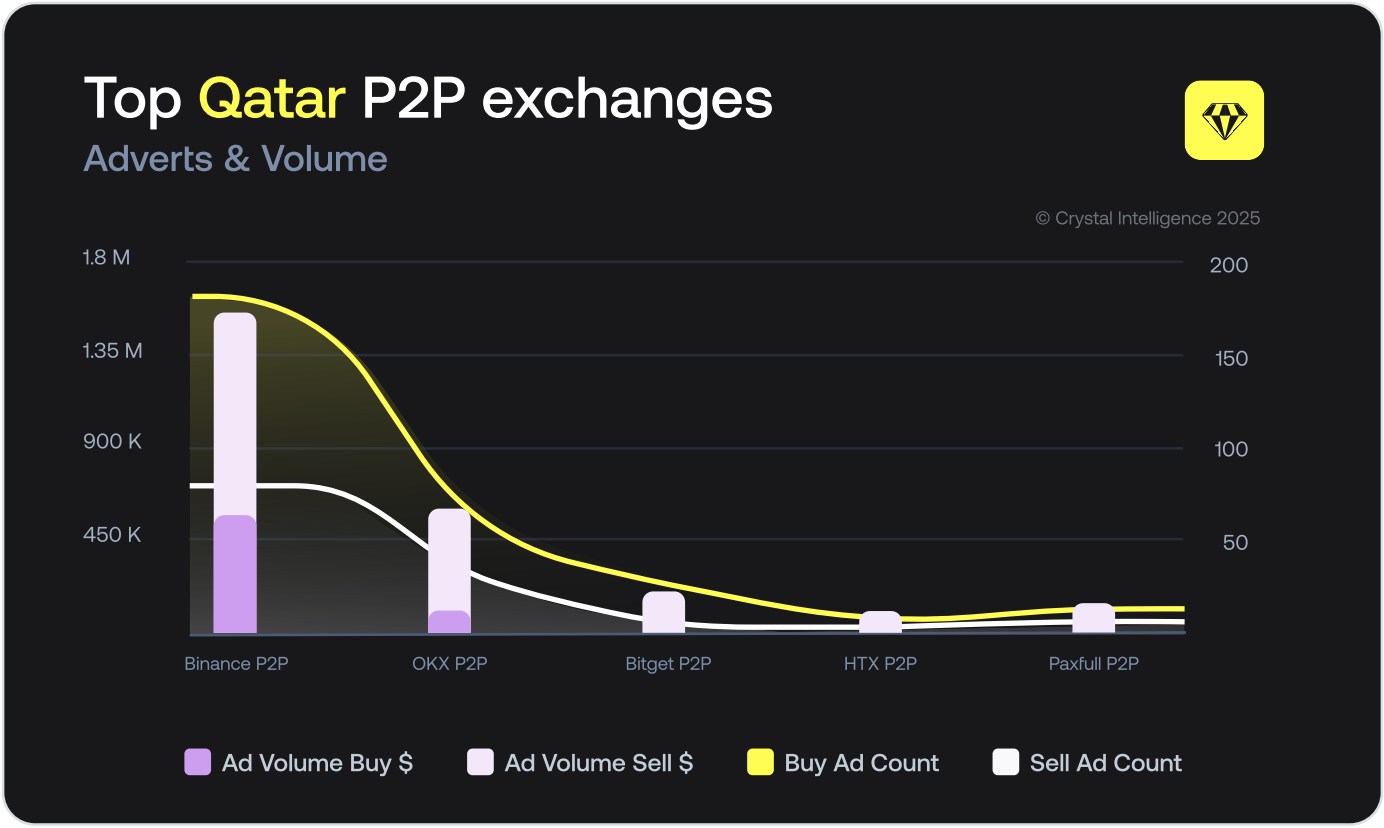
Virtual assets are increasingly being used to pay for illegal services such as pornography, prostitution, online fraud, and illicit gambling—activities that are criminalized under Qatari law.

4. Unregulated Peer-to-Peer Exchanges

Peer-to-Peer platforms continue to operate informally, allowing crypto transactions to bypass AML checks and evade regulatory scrutiny.

Crypto Focus Area on Peer-to-Peer Exchanges

The chart below shows Qatari Rial (QAR) activity over 24 hours and the number and volume of advertisements on P2P crypto exchanges on July 19, 2024.



A total of 336 Ads worth QAR 2,316,057 were traded during the period measured, with Binance the dominant P2P Exchange.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



State of Kuwait

Kuwait has implemented one of the region's most restrictive stances on cryptocurrency. As of late 2024, nearly all crypto-related activities are banned. However, Crystal's investigations reveal persistent underground trading and associated risks that challenge the effectiveness of the prohibition.

Regulatory Framework

In 2023-2024 Kuwait moved to fully restrict the use and trade of cryptocurrencies. The Central Bank of Kuwait (CBK) prohibits all crypto-related activities as of December 2024, citing, among other reasons, its determination to maintain a safe financial ecosystem and comply with the FATF travel rule. The Kuwait Financial Intelligence Unit (KwFIU) and other regulatory bodies implemented the ban in mid 2023 via four circulars.

Population	5 M
% Owning or Using Crypto	0% (off)
Crypto Sandboxes	2
Crypto ATMs	0

Activities now prohibited include:

- Buying, selling, or using crypto for payments
- Licensing individuals or entities for crypto services
- Offering crypto as an investment product
- Mining cryptocurrencies

An exception to the ban is made for the CBK and the Capital Markets Authority when they are dealing in regulated (by them) securities and financial instruments.

Penalties for violations include employment suspensions for individuals and fines of up to KWD 500,000 (approx. USD 1.62 million) for entities. instruments.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

AML/CFT Risks

Even with the ban in place, Kuwait remains exposed to significant financial crime risks tied to both traditional and crypto-specific channels:

1. Cash Dependency and Trade-Based Money Laundering

In the traditional economy, the high reliance on cash transactions in Kuwait increases risks of money laundering, making it difficult to trace illicit funds and enforce AML/CFT compliance effectively. Trade-based money laundering (TBML) through the strong trade sector also occurs.

2. Terrorism Financing via Charities

Additionally, terrorism financing through charitable organizations, possibly in Syria, has been highlighted despite regulatory oversight.

3. Persistent Underground Crypto Activity

Crystal's investigation revealed that crypto trading activities still occur in Kuwait, and identified several crypto-specific ML/TF risks:

- **Pornography and prostitution services**

Crypto has been used to purchase these illegal services with the former including child sexual abuse materials, and the latter associated with human trafficking.

- **Offshore Gambling**

Illegal casinos accepting crypto target Kuwaiti citizens. These platforms are unregulated, leaving any victims vulnerable to fraud and identity theft with no legal recourse.

- **Drug Trade and Scams**

Crypto is used to pay for both real and fraudulent drug sales, with scammers posing as dealers to exploit users.

- **Gift Card Misuse**

Binance gift cards, which are popular throughout the MENA region, can also be used for illicit activities, although Binance has moved to implement KYC and KYB identification processes for users since 2023.

- **Unregulated P2P and OTC exchanges**

These channels also present money laundering risks because of the absence of regulatory oversight.

- **Illegal Crypto Mining**

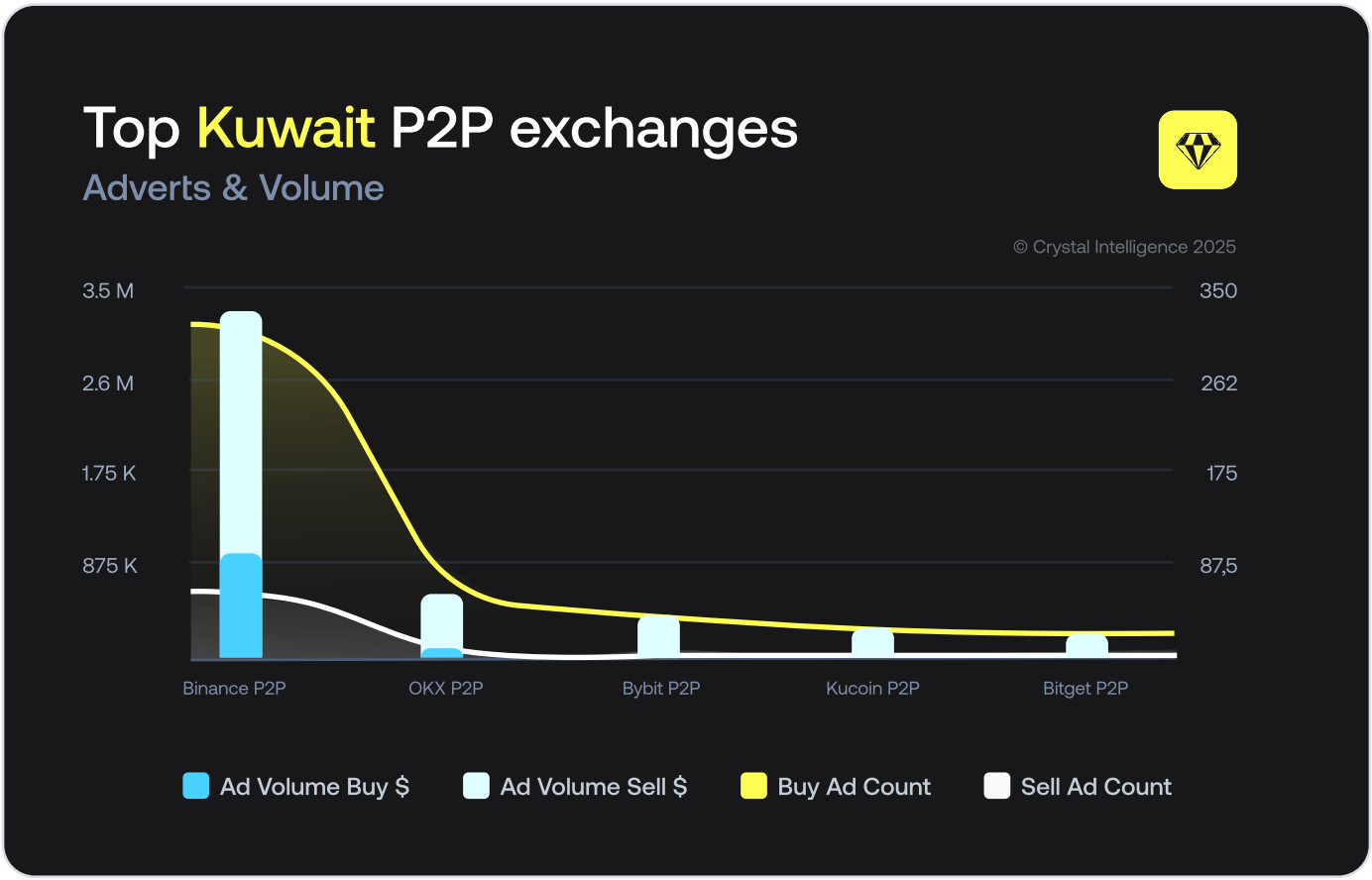
Despite the national ban, tech-savvy users continue to engage in mining. Beyond its illegality, mining raises environmental concerns due to high electricity usage.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

Crypto Focus Area on Peer-to-Peer Exchanges

Peer-to-Peer exchanges remain active in Kuwait, primarily via Sell Ads—indicating strong demand for crypto acquisition despite the legal risks. This demand, combined with the ban, has pushed crypto activity into opaque and harder-to-monitor channels, complicating enforcement and raising compliance red flags

The chart below shows Kuwaiti Dinar (KWD) activity over 24 hours and the number and volume of advertisements on Peer-to-Peer crypto exchanges on July 19, 2024.



A total of 452 Ads worth KWD 3,077,203 were traded during the period measured, with Binance the dominant Peer-to-Peer Exchange.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



Sultanate of Oman

Oman has taken a cautious yet increasingly constructive approach to cryptocurrency. As of late 2024, there was still no dedicated crypto law, but regulatory planning is underway to bring digital assets into a supervised framework. Adoption remains low, but activity through informal markets is growing.

Population	% Owning or Using Crypto	Crypto Sandboxes	Crypto ATMs
5.2 M	0%	1	0

Regulatory Framework

- The Central Bank of Oman has historically warned citizens against engaging with cryptocurrencies, citing risks of volatility and fraud. However, momentum has shifted.
- In 2023 the Capital Market Authority (CMA) started planning a regulatory framework for cryptocurrencies and exchanges.
- This culminated in the June 6 Decision NO. (E/35/20230), otherwise known as the 'Instructions on Registration of VASPs and the Implementation of the Requirements for Combating Money Laundering and Terrorism Financing.'

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

It proposes a regulatory framework for:

Mandatory registration for all Virtual Asset Service Providers (VASPs)

Implementation of AML/CFT controls, including transaction monitoring and reporting

Governance and risk management standards for licensed VASPs

Regular compliance reporting to the CMA

Non-compliance can result in fines of from OMR 10,000 (about US$26,000) up to OMR 100,000 (about US$260,000) per transgression, and individuals may face temporary or even permanent suspension from working in the sector.

AML/CFT Risks

Oman faces risks both from traditional financial activity and unregulated crypto adoption:

1. Trade-Based Money Laundering and Hawala Systems

As a strategic trade hub, Oman is exposed to trade-based money laundering. Informal value transfer systems such as hawala remain active and difficult to monitor.

2. Crypto-Facilitated Illicit Activity

Crystal's investigations revealed growing crypto use in:

- **Pornography and Prostitution**

Including materials linked to human trafficking

- **Scams on Social Platforms**

Scammers use X, Reddit, Telegram, and Facebook to push fake job offers, investments, and impersonation scams, demanding crypto payments

- **Gambling and Narcotics**

Payments for banned online gambling platforms and illegal drugs, including contraceptives tied to trafficking-related abuse

- **Fraud and Gift Card Laundering**

Use of Binance gift cards to bypass formal AML checks

Obfuscation Techniques

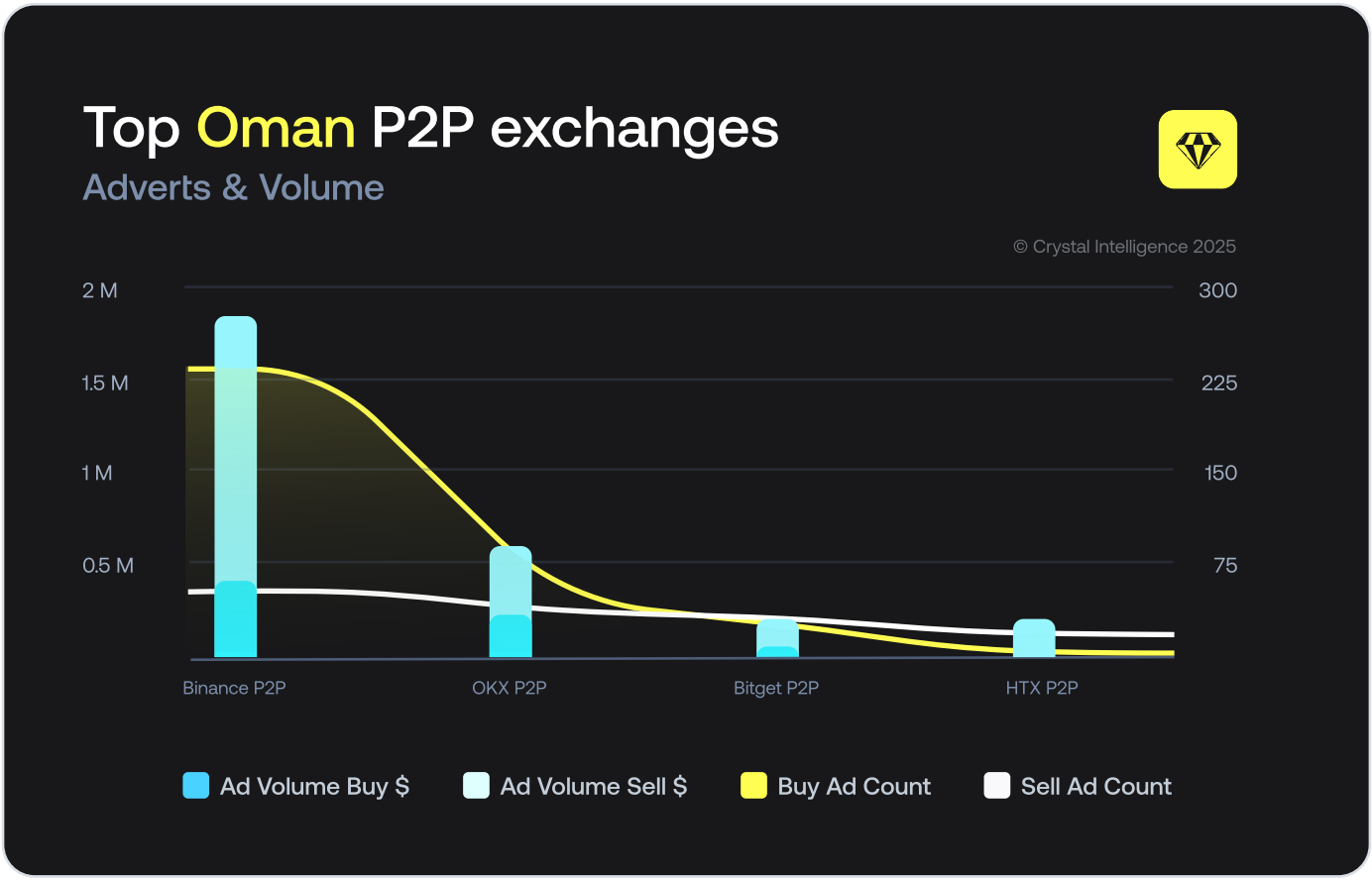
Fraudsters quickly move funds through wallets and offshore exchanges, using fake accounts and private messaging tools to evade detection

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

As well as the ML/TF risks facing Oman faces from trade-based money laundering (TBML) along its strategic trade routes and the popularity of unregulated, informal Hawala money transfer systems, the country also faces several crypto-specific money laundering risks.

Crypto Focus area on Peer-to-Peer Exchanges

The chart below shows Omani Rial (OMR) activity over 24 hours and the number and volume of advertisements on Peer-to-Peer crypto exchanges on July 19, 2024.



A total of 410 Ads worth OMR 2,632,449 were traded during the period measured, with Binance the dominant Peer-to-Peer Exchange. Interestingly, it is the only GCC Peer-to-Peer exchange where the appetite for selling crypto outstrips that for buying it at any stage, as we can see on HTX.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



MENA crypto regulation and risks:

Recommendations and Conclusions

This overview reflects the diverse regulatory approaches to cryptocurrencies both within the GCC, and in the MENA region, ranging from comprehensive regulatory frameworks to outright prohibitions and cautionary advisories.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.

Based on Crystal's analysis of regional trends and emerging threats, the following recommendations can help strengthen oversight and reduce crypto-related financial crime:

1. Regulatory Vigilance

Governments should expand and reinforce regulations ensuring compliance and monitoring of Peer-to-Peer and OTC crypto platforms to deter illicit activities and scams. These informal channels pose serious money laundering and fraud risks due to the lack of KYC, transaction monitoring, and oversight.

2. Public Awareness Campaigns

Launch targeted awareness campaigns to educate users about the risks associated with crypto transactions, including scams, fraud, and criminal exploitation. Awareness is a critical first line of defense – especially for new users, migrant communities, and those outside formal financial systems.

3. Cross-Border Collaboration

Encourage collaboration and alignment between countries and regions, regulatory bodies, financial institutions, and crypto exchanges to establish a comprehensive monitoring system. Intelligence-sharing can improve the detection of suspicious transactions and associated financial crime risks and disrupt cross-border financial crime networks.

4. Enhanced Due Diligence

Crypto platforms and businesses should implement and enforce stricter verification, ongoing monitoring, and risk-based due diligence procedures. These controls should match or exceed those used in traditional financial services.

Conclusions

The MENA region is emerging as a major force in the global digital asset economy.

As the MENA region continues its rapid ascent in the global crypto economy, regulators, compliance officers, investigators, and exchanges must stay ahead of emerging risks and regulatory developments.

By implementing robust compliance measures, fostering international cooperation, and leveraging technology-driven oversight, the region can establish itself as a leader in the digital asset space while maintaining financial integrity.

Crypto regulation in MENA is still evolving, and staying informed is key.

Whether you are a regulator shaping policies, an investigator combating financial crime, or an exchange ensuring compliance, proactive engagement and adherence to best practices will be essential in navigating the future of crypto in the region.

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.



Contact Us

This report has been compiled with the findings of publicly available data and the research undertaken by Crystal's Intelligence Team. We routinely update our research and make more detailed reports available to our clients on request.

If you would like to explore a region of interest, to understand the crypto dynamics and related risks, please contact us at info@crystalintelligence.com

Copyright © 2025 Crystal Intelligence B.V. All rights reserved.