Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

Money Laundering through Crypto-Assets in the Digital Space: The Prohibition Dilemma, the Limits of Supervising Virtual Asset Service Providers, and the Challenge of Digital Evidence — A Comparative Critical Reading in Light of the FATF Standards

Benmdakhene Laabidi [1], Prof. Radia Khelifa[2]
[1]PhD Candidate, Badji Mokhtar University, Annaba, Algeria
laabidi.ben-mdakhene@univ-annaba.dz
[2]Full Professor, Badji Mokhtar University, Annaba, Algeria
radia.khelifa@univ-annaba.dz

Submission 12.06.2026 Acceptance: 30.08.2026 Publication: 22.09.2026

Abstract
In an era of accelerating digitalization in which crypto-assets increasingly intersect with traditional financial infrastructures, money laundering has ceased to be a mere post-offence conduct carried out through traceable banking channels. It has become a composite technical operation distributed across blockchains (public distributed ledgers), cross-chain bridges, unhosted wallets and decentralized platforms, whereby the apparent transparency of the public ledger coexists with genuine opacity as to identity. This study examines whether the Algerian model of comprehensive prohibition of virtual assets, as enshrined in Law No. 25-10 of 24 July 2025, can contain the phenomenon, in comparison with the licensing-and-supervision model adopted by French and European law, and in light of FATF Recommendation 15 and related standards. It further analyses the problems of digital evidence associated with on-chain data, and the limits of search, seizure, confiscation and international cooperation. The study concludes that effectiveness is determined less by the choice between prohibition and licensing than by the State's capacity to build an integrated intelligence-and-judicial visibility over intermediaries and over the blockchain itself, one that reaches beyond the territorial limits of the legal text.
Keywords: Money laundering; crypto-assets; virtual asset service providers (VASPs); digital evidence; FATF.

Introduction

Ever since Satoshi Nakamoto conceived an electronic cash system operating peer to peer without institutional intermediaries,[1] trust in the financial system has no longer rested on the bank, the State and the judge alone. It has migrated to cryptographic protocols and distributed ledgers

[1]Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, available at: https://bitcoin.org/bitcoin.pdf.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

that produce certainty by algorithm rather than by authority, a shift that some scholars have described as a radical recomposition of the architecture of trust in transactions.[2] Yet this transformation carries a deep legal paradox. The ledger, commonly called the blockchain (a public, time-stamped and practically immutable record of every transaction), is open, but the identity standing behind a digital address remains concealed. What appears as transparency at the level of the transaction turns into opacity at the level of the actor.

This paradox is mirrored in the indicators of digital financial crime. Chainalysis estimated that addresses linked to illicit activity received at least USD 154 billion in 2025, an increase of 162% over the previous year, with some 84% of the illicit volume concentrated in stablecoins,[3] while TRM Labs put the same figure at USD 158 billion.[4] The divergence shows that such estimates rest on the analytical attribution of addresses rather than on certain observation, and that they represent lower bounds open to revision. In the same vein, the Seventh Targeted Update of the Financial Action Task Force (FATF), published on 16 July 2026, concluded that organised criminal networks exploit implementation gaps to move billions of dollars through the virtual asset sector, and that most of the illicit on-chain activity observed is now linked to stablecoins.[5]

A conceptual clarification is needed at the outset, since two terms overlap in usage. "Crypto-assets" is a technical description of a phenomenon based on cryptography and distributed-ledger technology, whereas "virtual assets" is a legal category established in the FATF standards. It denotes any digital representation of value that can be digitally traded or transferred and used for payment or investment purposes, excluding digital representations of fiat currency, securities and other financial assets already covered by other Recommendations.[6] This is the category that the Algerian legislator has in turn adopted in Law No. 25-10. The present study accordingly uses the former term to describe the phenomenon and the latter to analyse legal frameworks. Two further usages should be kept distinct. "On-chain" refers to data recorded on the ledger itself, and "off-chain" to information held elsewhere, such as customer records kept by exchanges. The expression "chain of custody", by contrast, has nothing to do with blockchain; it designates the documented handling of evidence from its collection to its production in court.

In Algeria, the legislative stance towards these assets has passed through two successive phases. The first found expression in Article 117 of the Finance Law for 2018, which prohibited the purchase, sale, use and possession of "virtual currency" and defined it negatively by the absence of a physical medium.[7] The second, wider in scope, is Law No. 25-10 of 24 July 2025 amending

[2]Kevin Werbach, The Blockchain and the New Architecture of Trust, MIT Press, Cambridge (MA), 2018.
[3]Chainalysis, The 2026 Crypto Crime Report, 2026.
[4]TRM Labs, 2026 Crypto Crime Report, 2026.
[5]FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (7th update), Paris, 16 July 2026.
[6]FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Paris, October 2021.
[7]Law No. 17-11 of 27 December 2017 on the Finance Law for 2018, Art. 117.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

and supplementing Law No. 05-01, which inserted Article 6 bis. That provision prohibits the issuance, purchase, sale, use, possession, trade and promotion of virtual assets, as well as the creation and operation of platforms for their trading; the prohibition extends to activities related to their mining, and violations are punishable by imprisonment of two months to one year and a fine of DZD 200,000 to 1,000,000, or by either of these penalties.[8] France, and the European Union behind it, moved instead to subject service providers to a unified licensing and supervisory regime, under which the transitional period for providers registered under the former national scheme came to an end in France on 1 July 2026.[9] Between the two models stand the FATF standards, which permit prohibition and licensing alike but require practical effectiveness in either case.[10]

Relatedly, Algeria, which was placed on the FATF list of jurisdictions under increased monitoring (the "grey list") in October 2024, was removed from it in June 2026 after completing an action plan centred on risk-based supervision, beneficial-ownership transparency and the implementation of targeted financial sanctions.[11] The present moment is therefore a test of the passage from formal compliance to practical effectiveness, particularly in the field of virtual assets, which poses distinctive challenges for supervision and proof alike.

Research Question

The problem addressed by this study can therefore be stated as follows: to what extent can a model of comprehensive prohibition of virtual assets, coupled with traditional rules of criminal evidence, deliver effective action against money laundering in the digital space, and what legal and institutional conditions turn prohibition or licensing into an effective instrument rather than a mere legislative posture? Three sub-questions follow. How have crypto-assets reshaped the structure of the act of laundering, and with what consequences for its legal characterisation? What is the place of virtual asset service providers in the preventive system, and how can a State that has opted for prohibition retain its capacity for detection? And what are the limits of on-chain digital evidence, and which investigative and international-cooperation tools are available to prove this offence?

Significance of the Study

The theoretical significance of this study lies in its attempt to re-examine the dichotomy

[8]Law No. 25-10 of 28 Muharram 1447 (24 July 2025) amending and supplementing Law No. 05-01 on the prevention and combating of money laundering and terrorist financing, Official Gazette of the Algerian Republic (JORADP) No. 48 of 24 July 2025, Arts. 5 and 13 (inserting Arts. 6 bis and 31 bis into Law No. 05-01). For an account of its provisions, see: Houari Qa'moussi, "Criminalisation of Digital Virtual Currency under Anti-Money-Laundering Law No. 25-10 in Algeria" [in Arabic], Algerian Journal of Law and Political Science, vol. 10, no. 2, 2025, pp. 508-523.

[9]Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs (MiCA), JOUE L 150 du 9 juin 2023, p. 40-205 ; France Épargne, « Crypto : la fin du régime PSAN au 1er juillet 2026 rebat les cartes pour les épargnants », 2026.

[10]FATF, Targeted Update ... (7th update), 16 July 2026, op. cit.

[11]FATF, Outcomes FATF Plenary, 17-19 June 2026, Paris, 19 June 2026.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

prevalent in national scholarship between "prohibition" and "regulation", by moving from the question of legitimacy to the question of effectiveness. It also links three fields that have been treated in isolation from one another: the substantive characterisation of virtual assets, the supervisory architecture for service providers, and the rules of criminal proof. Its practical significance stems from the fact that the Algerian legislator settled its choice through Law No. 25-10 while the procedural and institutional modalities of applying that choice to crypto-assets remain unclear. The study seeks to address this through practical proposals directed at policymakers, judges and investigators of financial crime.

Methodology

The study adopts a critical analytical method to dissect the texts governing virtual assets and money laundering in Algerian law, complemented by a comparative method that draws out the divergences and convergences between the Algerian model and the French and European models. It draws on the United States judicial experience as a laboratory for questions of liability and proof in a decentralised environment, and on a prospective method to trace the direction of development of the FATF standards. The argument relies on primary sources (legislative texts, official reports, judicial decisions) and on peer-reviewed research, with the caveat that figures issued by commercial analytics firms are used as indicators rather than as final facts.

Hypotheses

The study proceeds from two main hypotheses. The first is that the effectiveness of action against money laundering through crypto-assets is determined less by the legal label of the model adopted (prohibition or licensing) than by the State's capacity to build an integrated intelligence-and-judicial visibility over intermediaries and over the blockchain itself. The second is that the inadequacy of digital evidence is the weakest link in the system: on-chain evidence, however abundant, does not by itself attribute the act to a particular person or establish knowledge of the origin of the funds, which calls for a specific procedural framework that balances effectiveness with the safeguards of the defence.

Outline of the Study

Part One: Crypto-Assets and Their Service Providers between the Logic of Prohibition and the Logic of Licensing: The Imbalance of Legal Effectiveness.

Part Two: Digital Evidence in Money Laundering through Crypto-Assets: The Limits of Probative Force and the Limitations of Investigative and Cooperative Tools.

In adopting this division, we go beyond a descriptive account of crypto-asset technologies towards dissecting the shortcomings of the substantive framework, the supervisory architecture and the system of proof, so as to highlight the gap between the evolution of laundering tools and the limits of the tools for detecting and proving it.

Part One: Crypto-Assets and Their Service Providers between the Logic of Prohibition and the Logic of Licensing: The Imbalance of Legal Effectiveness

Dissecting the problem of effectiveness in confronting digital money laundering requires

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

starting from the object of the offence itself, namely the crypto-asset, with the technical properties that reshape the traditional stages of laundering. It then requires moving to the intermediary that the FATF standards have made the pivot of the preventive system: the virtual asset service provider (VASP). Section 1 therefore addresses the legal characterisation of crypto-assets and the transformation of the structure of laundering, and Section 2 turns to service providers between the Algerian prohibition and European licensing.

Section 1: The Legal Characterisation of Crypto-Assets and the Transformation of the Structure of Laundering

1. From "Currency" to "Virtual Asset": The Shift in the Legal Category

The first legislative response to crypto-assets, in Algeria as elsewhere, was governed by a "currency" logic, that is, by treating them as a threat to monetary sovereignty and the payment system. Article 117 of the Finance Law for 2018 defined "virtual currency" negatively, by the absence of a physical medium such as coins, banknotes, and payment by cheque or bank card.[12] Such a definition by deficiency states what these assets are not without specifying what they are. It also lumps together, in a single category, assets that differ sharply in function: bitcoin as a decentralised asset, stablecoins as representations of value pegged to an external asset, tokens representing rights, and coins designed from the outset to conceal transactions.

By contrast, since the amendment of Recommendation 15 in 2018 and 2019 the FATF standards have moved to the category of the "virtual asset", a broad functional formulation. The FATF's 2021 Guidance recommends that the definitions of virtual assets and of their providers be interpreted broadly; that claims of decentralisation be assessed by the reality of the arrangement rather than by its marketing label; and that stablecoins, non-fungible tokens and decentralised applications be treated according to their actual nature.[13] French law took the same direction when Article L.54-10-1 of the Monetary and Financial Code defined "digital assets" as tokens recorded on distributed ledgers and any digital representation of value that is neither issued nor guaranteed by a public authority and has no legal-tender status, excluding financial instruments.[14] The MiCA Regulation then adopted a threefold classification distinguishing asset-referenced tokens, e-money tokens and other crypto-assets.[15] The consequence is that the applicable legal regime is determined by the economic function of the asset, not by its mere being "virtual".

Law No. 25-10 moves to the same functional approach. It amended Article 4 of Law No. 05-01 to include a definition of virtual assets as digital values that can be traded or transferred digitally and used for payment or investment purposes, excluding traditional financial instruments, a

---

[12] Art. 117 of Law No. 17-11 of 27 December 2017, op. cit.
[13] FATF, Updated Guidance ..., October 2021, op. cit. ; Skadden, « FATF Updates Its Global Guidelines for the Regulation of Virtual Assets With an Eye to Emerging Technologies », November 2021.
[14] Code monétaire et financier, art. L.54-10-1 (Légifrance) ; AMF, Position DOC-2020-07, Questions-réponses relatives au régime des prestataires de services sur actifs numériques, 2020.
[15] Règlement (UE) 2023/1114, op. cit.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

formulation that closely tracks the international definition.[16] It then inserted Article 6 bis, which prohibits the whole life cycle of such assets, from issuance to possession, trade, promotion and the operation of platforms; describes them as property, proceeds, funds, assets or any equivalent value; and ties the prohibition to their functions as a means of payment, as recognised currency, or as an investment. The adoption of a functional definition marks real progress over the negative definition of 2018. Yet tying the prohibition to these functions leaves an interpretive question as to where tokens performing other functions stand, and it makes the certainty of the criminal rule on this point dependent on judicial interpretation. The European approach, by contrast, offers a classification that determines the regime applicable to each category.

2. The Transformation of the Structure of Laundering in the Crypto Environment

Scholarship has traditionally analysed money laundering through a three-stage model: placement, or entry into the financial system; layering, through a series of operations severing the link with the source; and integration into the lawful economy. The Algerian legislator has defined the forms of laundering in Article 2 of Law No. 05-01, as amended by Ordinance No. 12-02 and Law No. 23-01, and reinforced them with Articles 389 bis et seq. of the Penal Code.[17] The crypto environment does not abolish this model, however; it compresses its stages and redistributes their functions among new actors and tools.

At the placement stage, a bank deposit is not necessarily required, since value is often born digital, as where it results from online fraud, ransom or hacking. Placement may consist merely in converting cash proceeds into crypto-assets through exchange platforms, peer-to-peer transactions or informal intermediaries. At the layering stage the tools are many. They include mixing services, which pool the flows of several users and redistribute them so as to sever the trail of movement, and which the earliest research in this field treated as a market in its own right for the sale of concealment;[18] they also include hopping between blockchains through cross-chain bridges, swapping on decentralised exchanges, and governance manoeuvres. The FATF's report on decentralised finance of 21 July 2026 identified these techniques as means of obfuscation and of commingling illicit funds with lawful flows.[19] Integration is achieved through off-ramps into legal tender or through the purchase of goods and services. This is the stage at which funds return to the perimeter of traditional supervision, and it therefore has strategic importance to which we shall return.

Empirical studies confirm that such use is far from marginal. A study published in the Review of Financial Studies estimated, on data covering 2009 to 2017, that about a quarter of bitcoin users

[16]Law No. 25-10, Art. 2 (amending Art. 4 of Law No. 05-01), JORADP No. 48 of 2025.
[17]Law No. 05-01 of 6 February 2005 on the prevention and combating of money laundering and terrorist financing, as amended and supplemented, Art. 2; Penal Code, Arts. 389 bis et seq.
[18]Malte Möser, Rainer Böhme & Dominic Breuker, « An inquiry into money laundering tools in the Bitcoin ecosystem », 2013 APWG eCrime Researchers Summit, IEEE, 2013, pp. 1-14.
[19]FATF, Targeted Report on Regulatory Challenges from Decentralised Finance (DeFi), Paris, 21 July 2026.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

and some 46% of bitcoin transactions were associated with illegal activity, although the illicit share declines as mainstream adoption of the asset grows and as more opaque coins emerge.[20] As the market has shifted, the centre of gravity has moved to stablecoins. The FATF report of 3 March 2026 identified the locus of vulnerability in peer-to-peer transfers between unhosted wallets, which take place without any supervised intermediary, and in the difficulty stablecoin issuers have in monitoring activity across chains.[21] The Seventh Targeted Update, for its part, noted an emerging risk in the design of a proprietary stablecoin, linked to a financial conglomerate tied to criminal networks, so as to resist freezing and seizure.[22] We are thus witnessing a shift from laundering that exploits the weaknesses of the banking system to laundering that designs its tools to resist the very instruments of enforcement.

3. The Paradox of Transparency and Identity, and the Centrality of the Intermediary

The technical literature reveals a paradox that is almost structural in these assets. The public ledger allows, in principle, every transfer to be traced, but a digital address is not a person, and linking it to a particular identity requires statistical inference and the crossing of data from outside the ledger. A pioneering study showed that, by clustering addresses according to common spending behaviour and by tracing flows of funds towards known services, one can reconstruct a picture of entities and services without knowing the names of their owners, and that the point of contact between these assets and the real world lies in the platforms that convert them into legal tender.[23]

Hence the modern regulatory approach shifts from attempting to regulate the asset itself to regulating the chokepoints through which it passes. Scholars of the law of decentralised finance have shown that decentralisation at one point of the value chain is usually matched by re-concentration at another point that is less visible and less amenable to supervision, and that effective regulation targets that re-concentrated point.[24] This fits the broader thesis that "code" regulates behaviour in ways that rival legal rules, which requires the law to address the persons and entities that control the code or the points of entry and exit.[25] That is the logic that explains the centrality of the virtual asset service provider in the international system, and it is the subject of the next section.

[20] Sean Foley, Jonathan R. Karlsen & Tālis J. Putniņš, « Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? », Review of Financial Studies, vol. 32, n° 5, 2019, pp. 1798-1853.
[21] FATF, Targeted Report on Stablecoins and Unhosted Wallets - Peer-to-Peer Transactions, Paris, 3 March 2026.
[22] FATF, Targeted Update ... (7th update), 16 July 2026, op. cit.
[23] Sarah Meiklejohn et al., « A fistful of Bitcoins: characterizing payments among men with no names », Proceedings of the 2013 Internet Measurement Conference (IMC '13), ACM, 2013, pp. 127-140.
[24] Dirk A. Zetzsche, Douglas W. Arner & Ross P. Buckley, « Decentralized Finance », Journal of Financial Regulation, vol. 6, n° 2, 2020, pp. 172-203.
[25] Lawrence Lessig, Code and Other Laws of Cyberspace, Basic Books, New York, 1999 ; Primavera De Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, Cambridge (MA), 2018.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

Section 2: Virtual Asset Service Providers between the Algerian Prohibition and European Licensing

1. The International Standard: Recommendation 15 and the Travel Rule

Since the amendment of Recommendation 15 and its Interpretive Note, the FATF has subjected virtual assets and their providers to the same body of standards that governs financial institutions. States are required to assess the risks associated with activities and providers; to license or register providers and place them under the supervision of competent national authorities; and to apply preventive measures such as customer due diligence and suspicious-transaction reporting.[26] Recommendation 16, known as the Travel Rule, was added so that information on the originator and the beneficiary accompanies transfers between providers, above a threshold of USD or EUR 1,000.[27]

Official data nonetheless reveal a persistent gap between legislation and implementation. The proportion of jurisdictions that have enacted legislation implementing the Travel Rule rose from 73% in 2025 to 83% in 2026, while practical implementation remains limited.[28] As regards decentralised finance, the report of July 2026 found that some 93% of responding jurisdictions (132 out of 143) had not yet implemented the standards on qualifying decentralised arrangements, and that only two out of 142 had actually licensed or registered a decentralised arrangement. It stressed that a decentralised arrangement falls within Recommendation 15 whenever a natural or legal person exercises control or sufficient influence over it.[29] The international standard thus rests on a functional test of control, not on labels or on claims of non-centralisation.

Notably, the international standard does not require licensing exclusively. In its Seventh Update the FATF confirmed that prohibition is permitted under the standards, but it tied its effectiveness to robust supervision and enforcement, and observed that jurisdictions that have adopted prohibition models continue to face difficulties in identifying and sanctioning the illicit activity of providers.[30] That is the pivotal point on which the assessment of the Algerian model turns.

Unhosted wallets and peer-to-peer transactions raise a further difficulty in this context. These are transfers made directly between two parties without a supervised intermediary, and the logic of licensing does not, by its nature, reach them. The 2021 Guidance gave States discretionary tools to address their risks, including tighter supervision of providers' dealings with such wallets and restrictions on them.[31] The March 2026 report then recorded that the number of jurisdictions with regulatory frameworks targeted at the stablecoin ecosystem remains small, and that the standards

---

[26]FATF, The FATF Recommendations, Recommendation 15 and its Interpretive Note ; Financial Stability Board, « Updated Guidance for a risk-based approach to virtual assets and virtual asset service providers », 28 October 2021.
[27]FATF, The FATF Recommendations, Recommendation 16 and Interpretive Note to Recommendation 15.
[28]FATF, Targeted Update ... (6th update), Paris, 26 June 2025 ; FATF, Targeted Update ... (7th update), 16 July 2026, op. cit.
[29]FATF, Targeted Report on Regulatory Challenges from DeFi, 21 July 2026, op. cit.
[30]FATF, Targeted Update ... (7th update), 16 July 2026, op. cit.
[31]FATF, Updated Guidance ..., October 2021, op. cit.

do not require frameworks beyond those already applicable to providers, although States are urged to take account of the particular risks of these coins.[32] The upshot is that supervision of intermediaries, important as it is, covers only the visible part of the market; the unhosted part remains hostage to the capacities of analysis and investigation, which brings us back to the question of proof in Part Two.

2. The European and French Model: Licensing, Visibility and Restrictions on Concealment

France, under Law No. 2019-486 of 22 May 2019 (the PACTE Law), established a special regime for digital-asset service providers. It rests on compulsory registration for those offering custody services and the purchase or sale of digital assets against legal tender, together with anti-money-laundering obligations, and on an optional licence for the other services.[33] The MiCA Regulation, fully applicable to service providers since 30 December 2024, then moved licensing from the national to the unified European level, so that crypto-asset services may be provided in the European market only under a "crypto-asset service provider" authorisation in accordance with the Regulation. The Monetary and Financial Code, in Article L.561-2, has brought providers authorised under Article 59 of the Regulation within the persons subject to anti-money-laundering obligations.[34]

The European system is completed by three layers designed to strengthen visibility. The first is Transfer of Funds Regulation No. 2023/1113, which extends the Travel Rule to crypto-asset transfers within the Union from 30 December 2024, without any minimum value threshold.[35] The second is Anti-Money-Laundering Regulation No. 2024/1624, which becomes applicable on 10 July 2027 and, in Article 79, prohibits crypto-asset service providers from keeping anonymous accounts or accounts that allow the anonymisation or heightened obfuscation of transactions, including through anonymity-enhanced coins. The prohibition does not extend to providers of software and hardware or to self-hosted wallets so long as they do not control them.[36] The third is the expansion, by French Law No. 2025-532 of 13 June 2025, of the presumption of laundering laid down in Article 324-1-1 of the Penal Code so that it covers operations carried out using a crypto-asset with a built-in concealment feature or through obfuscation techniques.[37]

These layers disclose an integrated philosophy that makes licensing an instrument of visibility

---

[32]FATF, Stablecoins and Unhosted Wallets, 3 March 2026, op. cit.

[33]Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (PACTE) ; Code monétaire et financier, art. L.54-10-2 à L.54-10-5 ; AMF, Position DOC-2020-07, op. cit.

[34]Règlement (UE) 2023/1114, art. 59 ; Code monétaire et financier, art. L.561-2, 7° bis, b (Légifrance).

[35]Règlement (UE) 2023/1113 du Parlement européen et du Conseil du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, JOUE L 150 du 9 juin 2023.

[36]Règlement (UE) 2024/1624 du Parlement européen et du Conseil du 31 mai 2024 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, JOUE du 19 juin 2024, art. 79 et considérants correspondants (EUR-Lex, CELEX 32024R1624).

[37]Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic, art. 7 ; Code pénal, art. 324-1-1 (Légifrance).

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

rather than an end in itself. Licensing creates a legal addressee who can be held to account and inspected; the Travel Rule generates an information trail that accompanies the transfer; and restrictions on concealment shrink the space in which the actor can sever that trail. This philosophy is not, however, without a rights-based cost. Some members of the French National Assembly opposed the extension of the presumption of laundering because it reverses the burden of proof and undermines the presumption of innocence in a manner disproportionate to the fact that the mere use of a concealment tool does not suffice to infer a criminal character.[38] That debate will bear on our treatment of inferences of knowledge in Part Two.

3. The Algerian Model: Comprehensive Prohibition and the Test of Effectiveness

The Algerian choice rests on the conviction that dealing in virtual assets, in the absence of an issuing authority and of supervision, conflicts with the requirements of monetary sovereignty, the traceability of financial flows and the fight against laundering. Some scholars have seen in it a response to the transformation of digital currencies from a tool for modernising exchanges into a mechanism for committing crime.[39] It is a legitimate choice in principle in light of the FATF standards, as shown above, and may even be justified by considerations of prudence in States with limited supervisory capacity. But the legitimacy of the choice does not entail its effectiveness, and the points of imbalance appear in four paradoxes.

The first is the paradox of visibility. By abolishing the existence of a licensed domestic provider, prohibition abolishes with it the legal addressee who is supposed to supply customer-identification data, Travel Rule information and suspicious-transaction reports. The State thus loses its visibility at the only point at which an address can be linked to a person, while the flows continue through foreign platforms and peer-to-peer transactions. The burden of detection passes, as a result, to banks, exchange bureaux and the Financial Intelligence Processing Unit (CTRF) on the fiat side of the operation,[40] a side that calls for risk typologies and red-flag indicators specific to the on-ramps and off-ramps of crypto-assets, and for which general indicators inherited from traditional banking intelligence do not suffice. This accords with the FATF's observation on the difficulty of identifying and sanctioning illicit activity in prohibition jurisdictions.

The second is the paradox of criminalisation and cooperation. Criminalising possession and use turns every user into a potential offender, including victims of investment fraud that uses crypto-assets as its instrument. This may deter reporting and testimony and push activity towards unhosted wallets and foreign platforms, far from any monitoring. The hypothesis needs field testing, but it questions the usefulness of relying on criminalisation alone as a tool of prevention.

The third is the paradox of seizure and confiscation. A State that prohibits possession is bound,

---

[38]Assemblée nationale, Amendement n° 261 au projet de loi visant à sortir la France du piège du narcotrafic (n° 1043), 17e législature.

[39]Qa'moussi, op. cit., p. 508 et seq.

[40]The Financial Intelligence Processing Unit (Cellule de traitement du renseignement financier, CTRF) was established by Executive Decree No. 02-127 of 7 April 2002.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

when it seizes crypto-assets in a laundering case, to preserve, value and liquidate them. The new Code of Criminal Procedure has provided general tools in this field. They include the freezing and seizure of funds by order of the president of the court on the application of the prosecution during preliminary inquiries into laundering offences and offences related to information and communication technologies (Arts. 50 and 51); authorisation to dispose of seized property, with the proceeds of sale paid into a special Treasury account pending final judgment (Art. 54); and a section devoted to the management of frozen, seized and confiscated property.[41] But these provisions, so far as we have been able to examine them, were framed for conventional assets and property. They do not address the specific features of the crypto-asset: the secure custody of the private key, valuation in the face of volatility, and the transfer of the asset to a wallet controlled by the State. French experience offers an institutional model in this respect, having entrusted the management of seized and confiscated assets to a specialised agency created by Law No. 2010-768 of 9 July 2010.[42]

The fourth is the paradox of territoriality. Prohibition is a territorial rule confronting a cross-border activity carried out by providers located outside the territory who serve users inside it. The FATF report of 11 March 2026 addressed the risks posed by offshore providers and the way they structure their activities so as to avoid regulatory obligations.[43] In this situation, enforcing the prohibition cannot be achieved by the text alone; it requires a system that includes technical blocking, control of the payment channels linked to foreign platforms, and cooperation with issuers and platforms.

Three paths may be envisaged for addressing these paradoxes, without prejudging the superiority of any. The first retains prohibition and reinforces it with capacities for monitoring, analysis and cooperation. It carries the lowest legislative cost and is the most consistent with the current sovereign choice, but it relies most heavily on capacities whose availability has yet to be demonstrated. The second retains prohibition with narrowly framed exceptions for specific bodies and purposes, such as scientific research and experiments conducted under the supervision of the authorities, allowing national expertise to be built without opening the market. The third is a gradual transition towards limited licensing, which creates a supervised legal addressee and thereby produces visibility, but which demands a supervisory infrastructure, institutional capacities and a political acceptance whose assessment lies beyond the scope of this study. In light of the available data, the study favours the first path, coupled with a periodic review clause, without regarding it as a final solution.

[41]Law No. 25-14 of 9 Safar 1447 (3 August 2025) enacting the Code of Criminal Procedure, JORADP No. 54 of 13 August 2025, Arts. 50 to 54, and the section on the management of frozen, seized and/or confiscated property.
[42]Loi n° 2010-768 du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale (création de l'AGRASC).
[43]FATF, Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers (oVASPs), Paris, 11 March 2026.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

The stake, therefore, lies not in an abstract choice between the prohibition model and the licensing model but in the capacity of each to produce intelligence-and-judicial visibility over intermediaries and over the blockchain. The European model produces this visibility through licensing and restrictions on concealment, whereas the Algerian model must produce it by alternative means, based on the analytical capacity to read the chain, supervision of points of entry and exit, and external cooperation; otherwise prohibition will remain a symbolic posture. It should be noted that Algeria's removal from the grey list, which was based on improvements in risk-based supervision and beneficial-ownership transparency,[44] provides an institutional foundation on which to build, but it does not dispense with the need to develop specialised capacities in crypto-assets.

Part Two: Digital Evidence in Money Laundering through Crypto-Assets: The Limits of Probative Force and the Limitations of Investigative and Cooperative Tools

If Part One addressed the substantive framework and the question of intermediaries, the effectiveness of the criminal rule remains hostage to its capacity to be proved: criminalisation is of no value if no evidence can be produced to convince the judge. The problem is compounded in the crypto environment because the evidence combines an unprecedented abundance of data with uncertainty as to its attribution to the perpetrator. Section 1 therefore addresses the specificity of on-chain evidence and the limits of its probative force, and Section 2 turns to the tools of investigation, preservation and international cooperation.

Section 1: The Specificity of On-Chain Evidence and the Limits of Its Probative Force

1. Abundance of Data, Uncertainty of Attribution

The distributed ledger provides, in principle, a permanent, time-stamped digital memory of every transaction, which has led some investigators to regard it as the most suitable environment for criminal tracing. Yet this abundance conceals three gaps. The first concerns the attribution of an address to a person: an address is a technical identifier with no legal status, and studying the flow of funds does not by itself reveal its holder. The second concerns the probabilistic nature of clustering techniques. Techniques based on the assumption that addresses used together as inputs of a single transaction belong to one owner, or on the identification of change addresses, rest on assumptions that can be defeated by mixing or by joint pooling of inputs, as the earliest studies of anonymity in bitcoin already warned.[45] The third concerns automated classification: commercial and research analytics tools rely on machine-learning algorithms to classify addresses and to detect illicit activity,[46] and these tools are often proprietary, so that what reaches the judge is conclusions

---

[44]FATF, Outcomes FATF Plenary, 17-19 June 2026, op. cit.

[45]Fergal Reid & Martin Harrigan, « An analysis of anonymity in the Bitcoin system », in Security and Privacy in Social Networks, Springer, 2013, pp. 197-223 ; Meiklejohn et al., op. cit.

[46]Hao Hua Sun Yin, Klaus Langenheldt, Mikkel Harlev, Raghava Rao Mukkamala & Ravi Vatrapu, « Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain », Journal of Management Information Systems, vol. 36, n° 1, 2019, pp. 37-73 ; Adam Turner & Angela S. M. Irwin, « Bitcoin

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

rather than a methodology open to examination.

It follows that on-chain evidence, for all its apparent strength, is closer to a persuasive inference than to conclusive proof, and that it needs to be corroborated by off-chain evidence such as customer-identification records held by platforms, network-connection logs, device analysis and correspondence. The centre of gravity has thereby shifted from documentary evidence to technical expertise, with the attendant risk that the expert becomes the de facto judge of the facts unless expertise is surrounded by the safeguards of adversarial examination in open court.

2. The General Rules of Evidence and the Regulatory Void

Criminal proof in Algerian law rests on the principle of freedom of evidence and the judge's personal conviction. The new Code of Criminal Procedure, Law No. 25-14, affirms in its first article the principles of legality, fair trial, the presumption of innocence, the interpretation of doubt in favour of the accused and the giving of reasons for judgments.[47] Formally, this principle allows digital evidence to be admitted without any need for a special provision, but it supplies no criteria for reliability, authenticity, or the integrity of the chain of custody of the evidence, nor for the competence required of the analysing expert. Law No. 09-04 of 5 August 2009 on the prevention of offences related to information and communication technologies laid down special procedures such as electronic surveillance and the search of information systems,[48] but it focused on the means of obtaining evidence rather than on the criteria of its probative value. The recognition of electronic writing in the Civil Code, and of the electronic signature, belongs to the civil and commercial sphere.[49]

The new Code has provided an entry point for integrating blockchain analysis. It allows the public prosecution to call upon qualified persons in technical matters, who take an oath and submit summary or analytical reports annexed to the prosecution's submissions, and it allows judicial police officers to use technical or electronic devices to detect and prove offences in accordance with modalities to be set by regulation.[50] Yet the provisions we have examined do not define criteria for the reliability of such reports or the means of contesting them. Filling this void calls for recourse to international technical standards, foremost among them ISO/IEC 27037:2012 on the identification, collection, acquisition and preservation of digital evidence,[51] and for an

---

transactions: a digital discovery of illicit activity on the blockchain », Journal of Financial Crime, vol. 25, n° 1, 2018, pp. 109-130.

[47]Law No. 25-14 of 3 August 2025 enacting the Code of Criminal Procedure, JORADP No. 54 of 13 August 2025, Art. 1, and the common provisions governing trial courts on methods of proof.

[48]Law No. 09-04 of 5 August 2009 laying down special rules for the prevention and suppression of offences related to information and communication technologies, Arts. 3 and 5.

[49]Ordinance No. 75-58 of 26 September 1975 enacting the Civil Code, as amended and supplemented by Law No. 05-10 of 20 June 2005, Arts. 323 bis and 323 bis 1.

[50]Arts. 20 and 46 of Law No. 25-14, op. cit.

[51]ISO/IEC 27037:2012, Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence, Geneva, 2012 ; Eoghan Casey, Digital Evidence and Computer

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

approach based on functional equivalence coupled with a reliability requirement. Under that approach the integrity of the evidence would be presumed where the documentation of the chain of custody and the verification of hash values are established; the presumption would be rebuttable; and the defence would be given access to the methodology of the analytics tools relied on in the report and the opportunity to examine the expert.

3. Proving the Mental Element and On-Chain Inferences of Knowledge

The offence of laundering requires the perpetrator's knowledge of the illicit origin of the funds, an element that is hard to prove in the crypto environment because there is no direct relationship between the author of the predicate offence and the person who carries out the layering. The blockchain does, on the other hand, offer circumstantial indicators that may point to knowledge: dealing with sanctioned addresses or addresses linked to dark-web markets, resorting to mixing or to hopping between blockchains without an apparent economic rationale, and structuring amounts. The French legislator chose to address this difficulty by a legal presumption of laundering which, under Law No. 2025-532, extends to operations carried out with crypto-assets that have a concealment feature or through obfuscation techniques, whereas the Algerian legislation, as far as we are aware, contains no comparable presumption.[52]

While legal presumptions lighten the prosecution's burden, adopting them without safeguards threatens the presumption of innocence, as the French objections cited above show. We therefore incline towards restricted judicial inferences, based on documented objective indicators that are placed before the judge for assessment in light of the circumstances of each case, in place of an automatic legal presumption, while leaving the accused free to rebut by offering a legitimate economic explanation for the use of concealment tools.

United States experience offers a laboratory for questions of liability and proof in a decentralised environment. In Van Loon, the Fifth Circuit held on 26 November 2024 that the immutable smart contracts underlying the Tornado Cash protocol are not "property" within the meaning that would allow the Office of Foreign Assets Control to sanction them, because once deployed they are subject to no one's control.[53] In Storm, a Manhattan jury on 6 August 2025 convicted the protocol's founder of conspiracy to operate an unlicensed money-transmitting business but failed to reach a verdict on the counts of conspiracy to launder money and to violate sanctions;[54] his retrial on those two counts was adjourned on 25 August 2026 to 26 April 2027,

Crime: Forensic Science, Computers and the Internet, 3rd ed., Academic Press, Waltham (MA), 2011.

[52]Loi n° 2025-532 du 13 juin 2025, art. 7, op. cit.

[53]Van Loon v. Department of the Treasury, No. 23-50669, 122 F.4th 549 (5th Cir. Nov. 26, 2024).

[54]United States v. Storm, No. 23 Cr. 430 (KPF) (S.D.N.Y.), verdict of 6 August 2025 ; Money Laundering News, « Tornado Cash Jury Deadlocked on Most Serious Charges, but Convicted Founder Roman Storm on Conspiracy to Operate an Unlicensed Money Transmitting Business », August 2025.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

pending determination of his motion for acquittal.[55] The two cases reflect the centrality of the criterion of "control" and the difficulty of proving agreement and intent on the part of the developers of non-custodial tools, the very criterion that the FATF's report on decentralised finance has revived through on-chain and off-chain indicators. The Ulbricht case, moreover, shows that convictions in this environment are often built on the convergence of multi-source evidence, from transaction tracing to digital evidence drawn from servers and devices.[56]

Section 2: Tools of Investigation, Preservation and International Cooperation

1. Search and Seizure: From the Device to the Key

Law No. 09-04 authorises the search of information systems and of connected systems that can be accessed from the first system, and subjects the search to international agreements and the principle of reciprocity where the data are stored in a system located outside the national territory.[57] The new Code of Criminal Procedure has broadened investigative tools for laundering offences and offences related to information and communication technologies. It extends the jurisdiction of judicial police officers to the whole national territory (Art. 24); permits searches and seizures at any hour on the prior written authorisation of the Public Prosecutor (Art. 78); and authorises the interception of correspondence and the installation of technical arrangements (Art. 114) as well as infiltration (Art. 121), which exempts infiltrating officers from criminal liability for acquiring or holding funds derived from, or used in, the offences (Art. 123).[58] These general formulations could in principle accommodate infiltration in the digital environment and the holding of crypto-assets for investigative purposes, although that remains an interpretive inference rather than an express text.

Seizing a device, however, does not mean seizing the asset. A crypto-asset is not stored on the device; it is recorded on the distributed ledger, and control over it lies solely in the private key or recovery phrase. Effective seizure therefore depends on one of three things. The first is obtaining the key, which raises the problem of compelled disclosure and the privilege against self-incrimination. The second is transferring the asset to a wallet controlled by the judicial authority, a measure that ought to rest on an express legal basis. The third is freezing through an intermediary able to do so. Because a transfer can be defeated by a swift move on the part of the suspect, the value of the measure lies in its speed. The new Code provides a general urgent tool in the form of an order by the president of the court for freezing or seizure on the application of the prosecution,

[55] Gibson Dunn, « Digital Assets Recent Updates - August 2026 », 2026 ; Decrypt, « Roman Storm's Tornado Cash Retrial Pushed to April 2027 », August 2026.
[56] United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017).
[57] Art. 5 of Law No. 09-04, op. cit. ; on this measure, see: "Electronic search as an investigative measure in information-technology offences" [in Arabic], article published on jilrc.com, accessed 20 September 2026.
[58] Arts. 24, 78, 114, 121 and 123 of Law No. 25-14, op. cit.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

executed before it is notified to the person concerned (Arts. 51 and 52).[59] Its effectiveness with crypto-assets, however, depends on the technical capacity to execute the order through an intermediary, an issuer or a wallet under State control.

2. Freezing, Confiscation and the Management of Seized Assets

Freezing in the crypto environment follows two channels: freezing through supervised intermediaries such as platforms, and freezing by issuers of stablecoins, who technically have the ability to freeze or burn tokens. The FATF's 2026 report regarded the requirement of such a capacity, together with due diligence at redemption and limits on transactions with high-risk addresses, as good practice.[60] This kind of private freezing raises questions of fair-trial guarantees, since it makes a private issuer an enforcement instrument without a judicial decision in each case. The Bitfinex case showed that on-chain tracing, when combined with evidence from outside the chain, permitted the seizure of more than USD 3.6 billion in 2022, an operation the United States Department of Justice described as the largest financial seizure in its history, preceded by court-authorised search warrants of the defendants' online accounts that gave investigators access to files.[61] The Seventh Targeted Update of the FATF likewise highlighted the importance of the capacity to freeze and seize in dismantling an investment-fraud network in Spain in June 2025.[62]

Seizure entails the question of asset management: valuation in the face of volatility, secure custody, and the conditions for liquidation before final judgment. The new Code has answered part of these questions by authorising the disposal of seized property and the payment of the proceeds of sale into a special Treasury account (Art. 54). But the crypto-asset raises additional challenges of technical custody and of protecting the private key, which calls for implementing texts addressing seized virtual assets, above all in a system that has prohibited their possession in the first place.

3. International Cooperation and Information Exchange

The cross-border character of this offence means that domestic effectiveness remains hostage to what lies abroad. The United Nations Convention against Transnational Organized Crime (Palermo, 2000) and the United Nations Convention against Corruption (Merida, 2003), both ratified by Algeria,[63] provide a framework for mutual legal assistance, freezing and confiscation,

[59]Arts. 51 and 52 of Law No. 25-14, op. cit.
[60]FATF, Stablecoins and Unhosted Wallets, 3 March 2026, op. cit. ; Financial Intelligence Analysis Unit (Malta), « FATF Targeted Report on Stablecoins and Unhosted Wallets - Peer-to-Peer Transactions », 4 March 2026.
[61]U.S. Department of Justice, « Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency », press release n° 22-105, 8 February 2022.
[62]FATF, Targeted Update ... (7th update), 16 July 2026, op. cit.
[63]Algeria ratified, with a reservation, the Palermo Convention by Presidential Decree No. 02-55 of 5 February 2002 (JORADP No. 9 of 2002), and the United Nations Convention against Corruption by Presidential Decree No. 04-128 of 19 April 2004 (JORADP No. 26 of 2004).

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

but their mechanisms were designed for the traditional rhythm of judicial requests, not for the speed of an asset that can be moved in minutes. By contrast, the Budapest Convention of 2001 has been supplemented by its Second Additional Protocol of 2022 on enhanced cooperation and the disclosure of electronic evidence, which contains mechanisms allowing, among other things, direct requests to service providers in the territory of the parties.[64]

Algeria, as one of the first signatories of the United Nations Convention against Cybercrime, opened for signature in Hanoi on 25 October 2025, awaits the conversion of signature into ratification and then into entry into force, which is conditional on forty ratifications.[65] The Convention has been described as the first global framework for gathering and exchanging electronic evidence in serious crimes, and Algeria played a role in chairing the ad hoc committee that drafted it, according to Chatham House.[66] The Convention has not, however, escaped criticism from human-rights organisations concerning safeguards in the collection and exchange of data,[67] which reinforces the need to balance effectiveness with safeguards. Alongside judicial assistance, the exchange of intelligence among financial intelligence units is of particular importance. The FATF's report on decentralised finance pointed to channels such as the Egmont Secure Web and FIU.net, and to public-private partnerships, as response tools.[68] The effectiveness of international cooperation therefore depends on domestic readiness, including permanent contact points, data-preservation orders and standardised request protocols with the major platforms and issuers. In other words, it depends on converting cooperation from a slow exceptional track into a fast routine channel that at the same time safeguards the rights of the defence.

4. Safeguards of the Defence and the Protection of Personal Data

No treatment of tracing tools is complete without attention to their safeguards. The public character of the ledger does not mean that the processing of addresses and their linkage to persons is free from the rules of data protection: linking an address to an identity remains the processing of personal data, governed in Algeria by Law No. 18-07 of 10 June 2018 on the protection of natural persons in the processing of personal data,[69] with its requirements of purpose limitation and proportionality. Moreover, "taint" techniques, which label addresses as risky merely because

---

[64]Conseil de l'Europe, Convention sur la cybercriminalité (STE n° 185), Budapest, 23 novembre 2001 ; Deuxième Protocole additionnel à la Convention sur la cybercriminalité, relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE n° 224), 12 mai 2022.

[65]United Nations Office of Legal Affairs, « The United Nations Convention against Cybercrime opens for signature in Hanoi », 2025 ; United Nations General Assembly, Resolution 79/243 of 24 December 2024.

[66]Nnenna Ifeanyi-Ajufo, « The AU can help African countries adopt the UN cybercrime convention. But the challenges are significant », Chatham House, 31 October 2025.

[67]Just Security, « The Promise and Peril of the U.N. Convention Against Cybercrime », 2025.

[68]FATF, Targeted Report on Regulatory Challenges from DeFi, 21 July 2026, op. cit.

[69]Law No. 18-07 of 10 June 2018 on the protection of natural persons in the processing of personal data, as amended and supplemented by Law No. 25-11 of 24 July 2025, JORADP No. 48 of 2025.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

of their connection with suspicious addresses, may produce false positives that affect persons unconnected with the offence, so that an accusation or a freeze should not be founded on a single automated indicator. Every tracing measure should accordingly be accompanied by a threshold of reasonable suspicion, judicial oversight, and a right for the person affected to challenge a freeze or seizure based on blockchain analysis, so as to strike a balance between effectiveness and the guarantees of a fair trial.

Conclusion

It emerges from the foregoing that money laundering through crypto-assets is no longer a mere technical extension of traditional laundering. It has become a structural phenomenon that rearranges the stages of the criminal act and shifts the centre of gravity from the bank to the network node, and it places the legislator before a choice that goes beyond the dichotomy of prohibition and licensing to the question of effectiveness. The study has reached the following findings.

First, the legal characterisation of virtual assets in Algeria has moved from a "currency" approach, defined by deficiency in the Finance Law for 2018, to a functional definition in Law No. 25-10 that matches the international standard. Nevertheless, tying the prohibition to the functions of the asset (payment, currency or investment) leaves an interpretive problem as to tokens with other functions, unlike the classification adopted by the MiCA Regulation.

Second, the FATF standards permit prohibition and licensing alike and require effectiveness, and its 2026 reports locate the risk in stablecoins, unhosted wallets, offshore providers and decentralised finance, fields that legislative prohibition alone does not address.

Third, Algerian prohibition faces four paradoxes: the paradox of visibility, the paradox of criminalisation and cooperation, the paradox of seizure and confiscation, and the paradox of territoriality, and overcoming them depends on tools that complement the text.

Fourth, on-chain evidence, however abundant, is closer to a persuasive inference than to conclusive proof, and the absence of criteria of reliability and of the chain of custody weakens its probative force before the courts and enlarges the role of technical expertise.

Fifth, proving the mental element in this environment calls for a balance between lightening the burden of proof through inferences of knowledge and protecting the presumption of innocence, as the French and American experiences show.

On the basis of these findings, the study proposes the following recommendations:

1. Retain the option of prohibition as a sovereign choice consistent with international standards, coupled with a periodic review clause allowing it to be reassessed in light of developments in the FATF standards and national supervisory capacities.

2. Establish a specialised blockchain-analysis unit within the Financial Intelligence Processing Unit and the judicial police, and link it to the National Economic and Financial Criminal Pole and the National Criminal Pole for combating offences related to information and communication

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

technologies provided for in the new Code of Criminal Procedure,[70] equipping it with the necessary tools and training.

3. Issue red-flag indicators specific to the on-ramps and off-ramps of crypto-assets, addressed to banks, exchange bureaux and payment service providers.

4. Complete the provisions on the management of frozen, seized and confiscated property contained in the Code of Criminal Procedure with implementing texts addressing the custody, valuation and liquidation of virtual assets, along the lines of the French experience in managing seized assets.

5. Codify standards for digital evidence, in particular the chain of custody, the digital hash, the accreditation of experts and of the qualified persons provided for in Article 46 of the Code of Criminal Procedure, and the right of the defence to examine the methodology of the analysis.

6. Conclude cooperation protocols with the major platforms and stablecoin issuers, and convert Algeria's signature of the Hanoi Convention into ratification accompanied by rights-based safeguards.

7. Adopt restricted judicial inferences of knowledge in place of an automatic legal presumption, while guaranteeing the accused's right to rebut.

Accordingly, the real stake in the coming phase lies not in choosing the legal label of the model but in building a system of visibility, proof and cooperation capable of pursuing the crypto-asset wherever it is found, balancing the requirements of monetary sovereignty, the guarantees of a fair trial and the demands of openness to financial innovation.

References

I. Legal Texts and Official Documents

1) *Algeria*
2) Law No. 05-01 of 6 February 2005 on the prevention and combating of money laundering and terrorist financing, as amended and supplemented by Ordinance No. 12-02 of 13 February 2012, Law No. 15-06 of 15 February 2015 and Law No. 23-01 of 7 February 2023, Official Gazette of the Algerian Republic (JORADP).
3) Law No. 25-10 of 28 Muharram 1447 (24 July 2025) amending and supplementing Law No. 05-01, JORADP No. 48 of 24 July 2025.
4) Law No. 17-11 of 27 December 2017 on the Finance Law for 2018 (Art. 117).
5) Law No. 25-14 of 9 Safar 1447 (3 August 2025) enacting the Code of Criminal Procedure, JORADP No. 54 of 13 August 2025.
6) Law No. 09-04 of 5 August 2009 laying down special rules for the prevention and suppression of offences related to information and communication technologies.
7) Ordinance No. 75-58 of 26 September 1975 enacting the Civil Code, as amended and supplemented by Law No. 05-10 of 20 June 2005; Penal Code (Arts. 389 bis et seq.).

[70] Law No. 25-14, Part on criminal judicial poles (the National Economic and Financial Criminal Pole and the National Criminal Pole for combating offences related to information and communication technologies).

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

8) Executive Decree No. 02-127 of 7 April 2002 establishing the Financial Intelligence Processing Unit (CTRF).
9) Presidential Decree No. 02-55 of 5 February 2002 ratifying, with a reservation, the United Nations Convention against Transnational Organized Crime, JORADP No. 9 of 2002.
10) Presidential Decree No. 04-128 of 19 April 2004 ratifying, with a reservation, the United Nations Convention against Corruption, JORADP No. 26 of 2004.
11) Law No. 18-07 of 10 June 2018 on the protection of natural persons in the processing of personal data, as amended and supplemented by Law No. 25-11 of 24 July 2025.
12) *European Union and France*
13) Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs (MiCA), JOUE L 150 du 9 juin 2023, p. 40-205.
14) Règlement (UE) 2023/1113 du Parlement européen et du Conseil du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, JOUE L 150 du 9 juin 2023.
15) Règlement (UE) 2024/1624 du Parlement européen et du Conseil du 31 mai 2024 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, JOUE du 19 juin 2024.
16) Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (PACTE).
17) Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic.
18) Loi n° 2010-768 du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale.
19) Code monétaire et financier (France), articles L.54-10-1 à L.54-10-5 et L.561-2 ; Code pénal (France), articles 324-1 et 324-1-1.
20) Autorité des marchés financiers, Position DOC-2020-07, Questions-réponses relatives au régime des prestataires de services sur actifs numériques, 2020.
21) *International instruments*
22) Conseil de l'Europe, Convention sur la cybercriminalité (STE n° 185), Budapest, 23 novembre 2001 ; Deuxième Protocole additionnel (STCE n° 224), 12 mai 2022.
23) United Nations General Assembly, United Nations Convention against Cybercrime, Resolution 79/243 of 24 December 2024.
24) II. Reports of International Organisations and Specialised Bodies
25) FATF, The FATF Recommendations (as amended), Recommendations 15 and 16 and Interpretive Note to Recommendation 15, Paris.
26) FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Paris, October 2021.
27) FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

and VASPs (6th update), Paris, 26 June 2025.
28) FATF, Targeted Report on Stablecoins and Unhosted Wallets - Peer-to-Peer Transactions, Paris, 3 March 2026.
29) FATF, Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers (oVASPs), Paris, 11 March 2026.
30) FATF, Outcomes FATF Plenary, 17-19 June 2026, Paris, 19 June 2026.
31) FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (7th update), Paris, 16 July 2026.
32) FATF, Targeted Report on Regulatory Challenges from Decentralised Finance (DeFi), Paris, 21 July 2026.
33) Chainalysis, The 2026 Crypto Crime Report, 2026.
34) TRM Labs, 2026 Crypto Crime Report, 2026.
35) United Nations Office of Legal Affairs, « The United Nations Convention against Cybercrime opens for signature in Hanoi », 2025.
36) Nnenna Ifeanyi-Ajufo, « The AU can help African countries adopt the UN cybercrime convention. But the challenges are significant », Chatham House, 31 October 2025.
37) U.S. Department of Justice, « Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency », press release n° 22-105, 8 February 2022.
38) ISO/IEC 27037:2012, Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence, Geneva, 2012.
39) III. Books, Studies and Peer-Reviewed Articles
40) Qa'moussi (Houari), "Criminalisation of Digital Virtual Currency under Anti-Money-Laundering Law No. 25-10 in Algeria" [in Arabic], Algerian Journal of Law and Political Science, vol. 10, no. 2, 2025, pp. 508-523.
41) Merabet (Khadidja), Hammoudi (Mohammed) & Yassen (Sabah), "The Crime of Money Laundering in the Electronic-Money Environment: A Comparative Study of Iraqi and Algerian Legislation" [in Arabic], Humanities Journal of University of Zakho, vol. 10, no. 1, 2022.
42) Casey (Eoghan), Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd ed., Academic Press, Waltham (MA), 2011.
43) De Filippi (Primavera) & Wright (Aaron), Blockchain and the Law: The Rule of Code, Harvard University Press, Cambridge (MA), 2018.
44) Foley (Sean), Karlsen (Jonathan R.) & Putniņš (Tālis J.), « Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? », Review of Financial Studies, vol. 32, n° 5, 2019, pp. 1798-1853.
45) Lessig (Lawrence), Code and Other Laws of Cyberspace, Basic Books, New York, 1999.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

46) Meiklejohn (Sarah) et al., « A fistful of Bitcoins: characterizing payments among men with no names », Proceedings of the 2013 Internet Measurement Conference (IMC '13), ACM, 2013, pp. 127-140.
47) Möser (Malte), Böhme (Rainer) & Breuker (Dominic), « An inquiry into money laundering tools in the Bitcoin ecosystem », 2013 APWG eCrime Researchers Summit, IEEE, 2013, pp. 1-14.
48) Nakamoto (Satoshi), Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
49) Reid (Fergal) & Harrigan (Martin), « An analysis of anonymity in the Bitcoin system », in Security and Privacy in Social Networks, Springer, 2013, pp. 197-223.
50) Turner (Adam) & Irwin (Angela S. M.), « Bitcoin transactions: a digital discovery of illicit activity on the blockchain », Journal of Financial Crime, vol. 25, n° 1, 2018, pp. 109-130.
51) Werbach (Kevin), The Blockchain and the New Architecture of Trust, MIT Press, Cambridge (MA), 2018.
52) Yin (Hao Hua Sun) et al., « Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain », Journal of Management Information Systems, vol. 36, n° 1, 2019, pp. 37-73.
53) Zetzsche (Dirk A.), Arner (Douglas W.) & Buckley (Ross P.), « Decentralized Finance », Journal of Financial Regulation, vol. 6, n° 2, 2020, pp. 172-203.
54) IV. Case Law
55) Van Loon v. Department of the Treasury, No. 23-50669, 122 F.4th 549 (5th Cir. Nov. 26, 2024).
56) United States v. Storm, No. 23 Cr. 430 (KPF) (S.D.N.Y.), verdict of 6 August 2025; retrial adjourned to 26 April 2027 (order of 25 August 2026).
57) United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017).
58) V. Websites and Press Articles (accessed 20 September 2026)
59) Skadden, « FATF Updates Its Global Guidelines for the Regulation of Virtual Assets With an Eye to Emerging Technologies », November 2021, skadden.com.
60) Financial Stability Board, « Updated Guidance for a risk-based approach to virtual assets and virtual asset service providers », fsb.org.
61) Financial Intelligence Analysis Unit (Malta), « FATF Targeted Report on Stablecoins and Unhosted Wallets - Peer-to-Peer Transactions », 4 March 2026, fiaumalta.org.
62) France Épargne, « Crypto : la fin du régime PSAN au 1er juillet 2026 rebat les cartes pour les épargnants », 2026, france-epargne.fr.
63) Money Laundering News, « Tornado Cash Jury Deadlocked on Most Serious Charges, but Convicted Founder Roman Storm on Conspiracy to Operate an Unlicensed Money Transmitting Business », August 2025, moneylaunderingnews.com.
64) Just Security, « The Promise and Peril of the U.N. Convention Against Cybercrime »,

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

2025, justsecurity.org.
65) Gibson Dunn, « Digital Assets Recent Updates - August 2026 », 2026, gibsondunn.com.
66) Decrypt, « Roman Storm's Tornado Cash Retrial Pushed to April 2027 », August 2026, decrypt.co.
67) Assemblée nationale, Amendement n° 261 au projet de loi n° 1043 visant à sortir la France du piège du narcotrafic, 17e législature, assemblee-nationale.fr.
68) "Electronic search as an investigative measure in information-technology offences" [in Arabic], jilrc.com.