COMPLIANCE ON BLOCKCHAIN: AML/KYC, PRIVACY AND DIGITAL IDENTITY

Biolan Florentina — *Student of the Doctoral School of Law, Titu Maiorescu University (IOUDS)*

DOI: https://doi.org/10.66793/titulaw19proceeding11

Abstract:

The article examines blockchain compliance at the intersection of AML[1]/KYC[2] requirements, the right to privacy, and digital-identity infrastructures. It pursues three objectives: (i) to systematize the EU legal framework (MiCA–TFR–AMLR–AMLA–eIDAS 2.0) in relation to the relevant international standards (FATF); (ii) to assess the legal impact on users—especially the balance between identification/reporting duties and privacy/data-protection guarantees (GDPR); and (iii) to test the role of the European Digital Identity (EUDI Wallet; electronic attestations of attributes) as a data-minimization mechanism compatible with AML requirements.

Keywords: blockchain; AML/KYC; MiCA; TFR; AMLR/AMLA; eIDAS 2.0; EUDI Wallet; FATF; GDPR.

I. INTRODUCTION

Blockchain technology has moved from a technical experiment to infrastructure for payments, investments, and digital services, forcing the legal order to recalibrate the relationship between AML/KYC compliance and the rights to privacy and data protection. In the European Union, this recalibration rests on a normative ensemble: MiCA[3] (a sectoral regime for issuers and crypto-asset service providers—CASPs), the Regulation on information accompanying transfers of funds and certain crypto-assets (TFR 2023/1113—the EU version of the "travel rule")[4], the Anti-Money Laundering Regulation (AMLR 2024/1624[5]—a single set of directly applicable rules for obliged entities), the Regulation establishing AMLA (2024/1620[6]—a dedicated EU authority), and eIDAS 2.0 (2024/1183[7]—the framework for the European Digital Identity and electronic attestations of attributes). The fundamental-rights corollary remains the GDPR (2016/679)[8], which structures the legal bases and the limits of processing for compliance purposes.

By its nature, a blockchain ledger operates with pseudonymity, whereas the AML regime requires identification, monitoring, and traceability of flows. In the EU, the TFR (Regulation on Transfers of Funds)[9] requires the collection, transmission, and retention of data about the originator and the beneficiary for crypto-asset

[1] AML = Anti-Money Laundering;
[2] KYC = Know Your Customer;
[3] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937;
[4] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849;
[5] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;
[6] Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010;
[7] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity;
[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation—GDPR);
[9] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849;

transfers whenever a CASP (Crypto-Asset Service Provider)[10] is a party to the transaction; in parallel, the AMLR[11] imposes CDD[12]/KYC and ongoing monitoring on obliged entities, while the GDPR conditions processing on lawfulness, data minimization, and proportionality. From this perspective, the research question is not only how users are identified, but how much data may legitimately be processed and retained, for how long and for what purposes, without exceeding what is strictly necessary to prevent money laundering and terrorist financing.

Beyond EU regulation, the Financial Action Task Force (FATF)[13] has extended its standards to virtual assets (VAs) and to providers (VASPs)[14], clarifying the definition of VASPs, the treatment of stablecoins, licensing/registration, implementation of the travel rule[15], and the use of digital identity in customer due diligence.

II. THE EUROPEAN UNION LEGAL FRAMEWORK ON DIGITAL ASSETS AND AML COMPLIANCE

The European Union's legal framework for digital assets and AML[16]/CFT[17] compliance is built on four complementary pillars: (i) Regulation (EU) 2023/1114 (MiCA)—the lex specialis for crypto-asset markets and service providers (CASPs); (ii) Regulation (EU) 2023/1113 (TFR)—which extends the travel rule to crypto-asset transfers; (iii) Regulation (EU) 2024/1624 (AMLR)—a single set of direct, harmonized rules for obliged entities (including CASPs); and (iv) Regulation (EU) 2024/1620 (AMLA[18])—establishing the dedicated EU authority for AML/CFT. Together, these instruments aim at legal certainty, traceability of flows, and proportionality in data processing, while avoiding overlaps with existing sectoral regimes.

2.1. MiCA: Scope and the Status of CASPs

MiCA enshrines the principle that no one may provide crypto-asset services in the European Union without authorization. The regime is nuanced by the exception for services rendered at the exclusive initiative of the client (so-called reverse solicitation). Once authorized, CASPs are bound by conduct obligations—to act "honestly, fairly and professionally" in the interests of their clients—and by governance requirements. For specific services, MiCA sets dedicated packages: custody and administration, operation of a trading platform, exchange of crypto-assets, and reception and transmission of orders. In addition, an "orderly wind-down" plan is required to protect clients[19].

For e-money tokens (EMTs[20]), MiCA assimilates the legal relationship to a par-value claim against the issuer: the token is redeemable at any time, at nominal value, in funds (other than e-money), and the granting of interest is prohibited both to the issuer and to CASPs that provide services related to EMTs. The conditions for redemption must be visibly stated in the crypto-asset white paper[21]. These guarantees dovetail with the diligence and monitoring obligations under AML/CFT law, including at onboarding and in subsequent reviews.

2.2. TFR: The Travel Rule Applied to Crypto-Asset Transfers

[10] CASP (Crypto-Asset Service Provider) is the term used in MiCA for providers of crypto-asset services in the EU.
[11] AMLR = Anti-Money Laundering Regulation (Regulation (EU) 2024/1624);
[12] CDD = Customer Due Diligence (client due-diligence measures that obliged entities apply at onboarding and throughout the business relationship in order to detect suspicious transactions);
[13] FAFT (Financial Action Task Force) — an inter-governmental standard-setting body for AML/CFT; see: https://www.fatf-gafi.org/en/home.html
[14] VASP (Virtual Asset Service Provider) — a provider that exchanges, transfers, safeguards, or intermediates virtual assets;
[15] The "Travel Rule" is a transactional-transparency rule requiring information about the parties involved (originator/beneficiary) and the transfer details (amount, date, asset) to accompany transfers;
[16] AML = Anti-Money Laundering;
[17] CFT = Combating the Financing of Terrorism;
[18] AMLA = Anti-Money Laundering Authority (the European Authority);
[19] Regulation (EU) 2023/1114 (MiCA), various provisions including arts. 66, 68, 74–77, 80;
[20] EMT = an e-money-like token issued by regulated entities (e.g., electronic money institutions) that is redeemable 1:1 into fiat currency;
[21] MiCA prohibits the granting of interest to holders of EMTs, both by the issuer and by CASPs providing services related to EMTs;

The TFR[22] transposes payment-transparency standards to the crypto environment. The Regulation on Transfers of Funds sets the mandatory information that must accompany transfers (name of the originator/beneficiary, DLT address or account, identifiers), including the obligation for the originator's CASP to verify such information[23]; Article 16 regulates detection of missing information by the beneficiary's CASP. For self-hosted addresses, the TFR requires obtaining and holding information for transfers above EUR 1,000 and, additionally, the originator's crypto-asset service provider must take appropriate measures to assess whether the address is owned or controlled by the initiator. The regime includes rejection/return procedures, internal policies for implementing restrictive measures, a five-year retention period, and publication of sanctions[24].

2.3. AMLR: Direct, Uniform Obligations for Obliged Entities (Including CASPs)

The AMLR[25] establishes CDD/KYC and ongoing monitoring, regulates correspondent relationships with third-country entities—including for CASPs—and, under strict conditions, allows reliance on another obliged entity[26]. It clarifies the reporting of suspicions to FIUs[27], responsible data sharing for AML purposes, and document retention—the general five-year rule. Its application is set for 10 July 2027, and for certain sub-categories (Art. 3(3)(n),(o)) from 10 July 2029[28].

2.4. AMLA: Coordination, Common Methodologies and Selective Direct Supervision

Regulation (EU) 2024/1620 [29] establishes AMLA, with extensive tasks (coordination, guidelines, methodologies, joint analyses) laid down in Article 5, and the possibility of assuming direct supervision in exceptional circumstances, at the request of a national financial supervisor[30]. This architecture seeks convergence of supervisory practices and rapid remedies for heightened cross-border risks.

2.5. Interactions and Delineations: The MiCA–TFR–AMLR Triangulation (Anchored in eIDAS)

In practice, MiCA sets who may operate and how (authorization, governance, services); the TFR specifies what information must accompany transfers (including hosted–unhosted) and how to handle deficiencies; while the AMLR/AMLA lays down how diligence, monitoring, reporting, data sharing, and retention are to be carried out, and who coordinates supervision. For identity verification within CDD, eIDAS 2.0[31] creates the EUDI Wallet[32] and electronic attestations of attributes (QEAA), while Implementing Regulation 2015/1502[33] defines levels of assurance (LoA)—legal anchors that the AMLR may invoke when accepting electronic means of identification.

III. RELEVANT INTERNATIONAL STANDARDS AND REGULATIONS

[22] TFR = Transfer of Funds Regulation: Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849;
[23] Article 14 of Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (obligations of the originator's provider);
[24] Regulation (EU) 2023/1113, notably arts. 14(5), 16(2), 17, 23, 26, 30;
[25] AMLR — Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;
[26] Regulation (EU) 2024/1624, notably arts. 20, 38, 49;
[27] FIU = Financial Intelligence Unit (in Romania: Oficiul Național de Prevenire și Combatere a Spălării Banilor—ONPCSB);
[28] Regulation (EU) 2024/1624, notably arts. 70, 77, 90;
[29] Regulation (EU) 2024/1620 establishing AMLA;
[30] Art. 14, ibidem;
[31] eIDAS 2.0: Regulation (EU) 2024/1183 (the eIDAS revision) introduces the European Digital Identity Wallet (EUDI Wallet) and electronic attestations of attributes for EU-recognized identification and identity verification;
[32] EUDI Wallet – European Digital Identity Wallet – a wallet through which users can store, manage, and present identity data and electronic attestations of attributes (e.g., age, professional status);
[33] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 laying down minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

3.1. FATF's Role and the Architecture of Global Standards

The Financial Action Task Force (FATF[34]) functions as the global standard-setter for preventing money laundering and terrorist financing (AML/CFT), including for virtual assets (VAs) and virtual asset service providers (VASPs). The 2019 revision of Recommendation 15 and its Interpretive Note[35] expressly extended FATF's scope to VAs/VASPs; the updated 2021 Guidance[36] elaborated six essential areas: definitions of VAs/VASPs, application of standards to stablecoins, risks pertaining to peer-to-peer transactions, licensing/registration of VASPs, implementation of the travel rule, and practical aspects for the public/private sectors. FATF Recommendations are not positive law, but serve as compliance benchmarks for jurisdictions and authorities, subsequently monitored through targeted updates (2024[37], 2025[38]) that track implementation gaps and friction points (e.g., hosted–unhosted transactions, DeFi, stablecoins).

The 2021 Guidance clarifies that entities which exchange, transfer, safeguard or administer virtual assets, or facilitate intermediation (including through apparently decentralized arrangements where there exists an owner/operator with significant control), fall within the scope of VASPs and must be licensed/registered and supervised. In addition, issuers/administrators of stablecoins and wallet providers can be VASPs when they offer relevant centralized services; the technological label does not prevail over the economic function and AML/CFT risk.

FATF extends the principles of Recommendation 16[39] (payment transparency) to VA transfers between VASPs: they must obtain, retain and transmit information about the originator and the beneficiary "immediately and securely," to ensure traceability. The 2021 Guidance offers implementation parameters, while the 2025 Best Practices on Travel Rule Supervision add recommendations on technical interoperability, counterparty due diligence, and testing flows across hosted–hosted/hosted–unhosted scenarios. The 2024 targeted update shows that implementation is uneven across states, underscoring the need for cross-border coordination and operational clarifications.

FATF's 2020 Guidance on Digital Identity[40] orients authorities and the private sector in using digital-ID systems within customer due diligence. The document is technology-neutral, emphasizes levels of assurance (identification, authentication, governance), and recommends a risk-based approach to remote onboarding with quality standards and independent audits[41].

3.2. United States: BSA[42]/FinCEN[43]—Transposing the Standards into Federal Law

In U.S. law, the Bank Secrecy Act (BSA) is implemented through a network of administrative rules (31 C.F.R.) administered by FinCEN. Entities that fall under the Money Services Businesses (MSB) category must

[34] FATF – Financial Action Task Force – an intergovernmental body created in 1989 (G7, Paris) that sets global standards against money laundering (AML), terrorist financing (CFT), and proliferation financing (PF);
[35] FATF Recommendations, Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs, Paris, 9 July 2024;
[36] Financial Action Task Force (FATF), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Paris: FATF/OECD, Oct. 2021), secțiuni privind definițiile VA/VASP, stablecoin-uri, P2P, licențiere/înregistrare și „travel rule";
[37] FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (Paris: FATF/OECD, June 2024);
[38] FATF, Best Practices on Travel Rule Supervision (Paris: FATF/OECD, 2025), see: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf?
[39] FATF, The FATF Recommendations – R.16 (Transparența transferurilor), see: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html?
[40] FATF, Guidance on Digital Identity (Paris: FATF/OECD, 6 Mar. 2020), see: https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html?
[41] FATF, Guidance on Digital Identity – Appendices (Paris: FATF/OECD, 2020), see: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-Appendice-D.pdf?
[42] Bank Secrecy Act (BSA) — also known as the anti–money laundering law — requires financial institutions to help combat financial crime by keeping records and reporting certain financial transactions, including cash transactions exceeding $10,000;
[43] FinCEN = Financial Crimes Enforcement Network (the U.S. bureau for enforcing financial-crime regulations);

maintain an AML program (31 C.F.R. § 1022.210[44]), file Suspicious Activity Reports—SARs (31 C.F.R. § 1022.320[45]), and comply with the Recordkeeping & Travel Rule (31 C.F.R. § 1010.410[46]). In 2019, FinCEN issued FIN-2019-G001[47], an interpretive guidance that systematizes the application of the BSA to Convertible Virtual Currencies (CVCs) and clarifies when an actor becomes a money transmitter (e.g., "exchangers" and "administrators" of CVCs), thereby falling under the MSB umbrella. The guidance stresses that industry labels are irrelevant; what matters is the actual function—transmitting value for others—and the attendant risks.

The federal "Travel" rule requires institutions to transmit and retain a minimum set of information for transmittals of funds of USD 3,000 or more[48] (e.g., the transmitter's name and address, the name/address or identifier of the transmitter's institution, the date and amount, the beneficiary's bank, as well as the beneficiary's name/address/account/identifier)[49]. The rule applies to both banks and non-bank institutions; recent official interpretations have reconfirmed this architecture and the follow-the-money[50] purpose in AML investigations[51]. In parallel, MSBs must file SARs under 31 C.F.R. § 1022.320, with FinCEN[52] guidance and updated FAQs[53] on reporting timelines and content.

IV. COMPLIANCE OBLIGATIONS OF BLOCKCHAIN SERVICE PROVIDERS (VASP/CASP)

4.1. The Architecture of Obligations: Between the Lex Specialis (MiCA) and the AML/TFR Regime

The EU framework positions crypto-asset service providers (CASPs) at the intersection of a sectoral regime—MiCA, which determines who may operate on the market and how—and the transversal AML/CFT regime (AMLR, supplemented by AMLA), while TFR 2023/1113 implements the travel rule in the area of crypto-asset transfers. MiCA makes the provision of any service conditional on authorization, admits only narrow exceptions for services provided at the exclusive initiative of the client, imposes conduct ("honest, fair and professional") and governance, and, for critical functions, requires an orderly wind-down plan and technical rules by service type (e.g., custody; trading platforms; exchange; reception/transmission of orders)[54]. In mirror, the

[44] 31 CFR § 1022.210 (Anti-money laundering programs for money services businesses) – see: https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1022? ;
[45] 31 CFR § 1022.320 (Reports by money services businesses of suspicious transactions), see: https://www.law.cornell.edu/cfr/text/31/1022.320? ;
[46] 31 CFR § 1010.410 (Records to be made and retained; Recordkeeping/Travel Rule), see: https://www.law.cornell.edu/cfr/text/31/1010.410? ;
[47] FinCEN, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (FIN-2019-G001, 9 May 2019), see: https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf;
[48] Federal Financial Institutions Examination Council (FFIEC), BSA/AML Examination Manual – Funds Transfers Recordkeeping (Travel Rule Requirements), see: https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/09
[49] Federal Register, Agency Information Collection Activities; Proposed Renewal… Recordkeeping and Travel Rule – reconfirmări privind 31 CFR 1010.410(f) (Oct. 23, 2020; Aug. 13, 2024), see: https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201023a.pdf
[50] FATF, *Virtual Assets: Targeted Update on Implementation…* (2024) — findings on the status of implementation of the "travel rule.", see: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html?
[51] FinCEN, Funds "Travel" Regulations: Questions & Answers (Advisory Issue 7, Jan. 1997), see: https://www.fincen.gov/system/files/advisory/advissu7.pdf
[52] FinCEN, Advisory on Illicit Activity Involving Convertible Virtual Currency (9 May 2019) – corelat cu FIN-2019-G001, see: https://www.fincen.gov/system/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf
[53] FinCEN, Frequently Asked Questions Regarding the FinCEN SAR see: https://www.fincen.gov/resources/frequently-asked-questions-regarding-fincen-suspicious-activity-report-sar
[54] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA): Art. 59 (authorisation), Art. 61 (provision at the exclusive initiative of the client), Art. 66 (conduct), Art. 68 (governance), Art. 74 (orderly wind-down), Art. 75 (custody), Art. 76 (trading platforms), Art. 77 (exchange), Art. 80 (reception and transmission of orders); see also Art. 110 (register of non-compliant entities);

AMLR[55] sets out CDD/KYC, ongoing monitoring, reporting of suspicions, data sharing for AML purposes and document retention, while the TFR[56] fixes the mandatory set of information that must accompany transfers and how to handle missing or incomplete information.

4.2. Onboarding and Identity Verification: CDD/KYC, Reliance and Correspondent Relationships

When entering into a business relationship, CASPs apply risk-calibrated know-your-customer measures and establish ongoing monitoring. For flows involving entities from third countries, the regime provides specific measures for correspondent relationships, including for CASPs, and reliance on another obliged entity is possible only with strict safeguards[57]. In addition, the AMLR explicitly anchors the retention of CDD documentation, including information obtained by means of electronic identification, as part of the client "file."[58] In the digital-identity realm, eIDAS 2.0 creates the European Digital Identity Wallet (EUDI Wallet) and enshrines electronic attestations of attributes—including their qualified form (QEAA)—with rules on legal effects, requirements and reference standards, verification of attributes against authoritative sources, and data separation from other services provided by wallet providers[59]. This architecture enables AML-compliant onboarding based on verified data and selective disclosure of attributes, reducing exposure of personal data.

4.3. The Travel Rule for Crypto-Assets: Transactional Transparency and the Treatment of Self-Hosted Addresses

The TFR extends transparency requirements to crypto-asset transfers: the originator's CASP must obtain, retain and transmit information about the originator and the beneficiary, including the DLT address and corresponding identifiers. For self-hosted addresses, the TFR requires maintaining information and, above certain thresholds/conditions, additional checks to establish control over the address. Where information is missing or incomplete, rejection/return and risk-based reporting procedures apply. The regime includes a five-year retention period and provides for the publication of sanctions[60].

4.4. Monitoring, Reporting and Responsible Data Sharing

The AMLR requires CASPs to maintain ongoing monitoring and to report suspicious transactions to the FIU. Information sharing is permitted within dedicated partnerships, constrained by necessity and proportionality, and explicitly referring to CDD data and suspicions. Retention of CDD documents and related information is generally five years. From a data-protection perspective, KYC/AML processing relies on the legal-obligation basis, while respecting the principles of lawfulness, minimization, purpose and storage limitation, security, privacy-by-design and appropriate technical-organizational measures[61]. At the same time, the GDPR allows

[55] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing; Art. 20 (CDD/monitoring), Art. 38 (correspondent relationships, incl. CASPs), Art. 49 (reliance), Art. 69 (reporting of suspicions), Art. 70 (information sharing for AML purposes), Art. 77 (retention), Art. 90 (entry into force and application);

[56] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849; Art. 14 (minimum set of information), Art. 14(5) and Art. 16(2)–(4) (self-hosted addresses and checks), Art. 17, Arts. 21–22 (measures for missing information), Art. 26 (retention), Art. 30 (publication of sanctions);

[57] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing; Art. 20 (CDD/monitoring), Art. 38 (correspondent relationships, incl. CASPs), Art. 49 (reliance).

[58] Ibidem, art. 77;

[59] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity; Arts. 45b–45h (legal effects, requirements, verification against authoritative sources, functional separation), references to Art. 5a (Wallet implementation) and Annexes V–VII (content and attribute lists);

[60] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849: Art. 14, Art. 14(5), Arts. 16(2)–(4), Art. 17, Arts. 21–22, Art. 26, Art. 30;

[61] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): Art. 5 (principles), Art. 6(1)(c) (legal basis — legal obligation), Art. 25 (privacy by design), Art. 32 (security of processing);

restriction of certain rights (access, objection, erasure) where necessary and proportionate for AML/CFT, which explains situations in which users' requests are limited when documentation is retained solely for AML compliance.

V. LEGAL IMPLICATIONS FOR USERS OF DIGITAL ASSETS

5.1. Pseudonymity, Identification and Traceability

For users, participation in the regulated crypto ecosystem means moving from technical pseudonymity to legal identification at points of intermediation. From a traceability perspective, Regulation (EU) 2023/1113 (TFR) requires crypto-asset transfers involving a provider (CASP) to be accompanied by information about the originator and the beneficiary, and the originator's CASP must verify ex ante the accuracy of that information before initiating the transfer. In mirror, the beneficiary's CASP must have procedures to detect missing information and, on a risk basis, decide whether to execute, reject or return the transfer. The European regime starts from the premise that, unlike transfers of funds, crypto-asset transfers are subject to the same requirements regardless of value, precisely to counter "smurfing" and the cross-border nature of networks[62].

5.2. Self-Hosted Addresses: Permitted, but Conditional

The TFR does not prohibit transactions to/from self-hosted wallets; however, it reiterates the obligation of the CASP to obtain and retain information about the parties to any such transfer. Moreover, when the amount exceeds EUR 1,000, the originator's CASP (for transfers to a self-hosted address) and the beneficiary's CASP (for transfers from a self-hosted address) must take appropriate measures to assess whether the address is owned or controlled by the client. For users, the practical consequence is that interaction with self-custody remains possible, but non-anonymous whenever the path touches a regulated intermediary; lack or inaccuracy of information may lead to rejection/return of the transfer or risk-based reports.

5.3. Users' Exposure and Extraterritorial Effects

Although the AML regime targets obliged entities, users can bear indirect effects: blocked transactions, requests for source-of-funds, and STR/SAR filings. The AMLR requires ongoing monitoring and reporting of suspicions to FIUs (Arts. 20, 69), and failure to comply with reasonable requests from CASPs may lead to refusal to execute[63]. In cross-border transactions, FATF standards (R.15/R.16)[64] and U.S. law (BSA/31 C.F.R. § 1010.410)[65] converge on the travel rule and maintenance of an information chain for transfers ≥ USD 3,000, with AML-program and SAR obligations for MSBs. In practice, users interacting with platforms subject to the BSA may experience similar transparency requirements, reinforcing a "global compliance standard" for traceability and identification[66].

VI. DIGITAL IDENTITY AND ID-VERIFICATION SOLUTIONS IN THE BLOCKCHAIN ECOSYSTEM

[62] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849: Art. 14(1)–(3), (6)–(8), Art. 31, Art. 16(1), 17(1), 21–22, Art. 27, Art. 30;

[63] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing: Art. 20 (ongoing monitoring), Art. 69 (reporting of suspicions to the FIU — Financial Intelligence Unit);

[64] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs* (2021) — definitions of VA/VASP, stablecoins, the "Travel Rule," and implementation; the FATF Recommendations, R.16 (transparency of transfers);

[65] 31 C.F.R. § 1010.410(e)–(f) — Recordkeeping/"Travel Rule" for transmittals of funds of $3,000 or more (obligations to transmit and retain data); FFIEC BSA/AML Manual — Funds Transfers Recordkeeping (threshold and minimum content);

[66] FinCEN, FIN-2019-G001 (*Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*), May 9, 2019; FIN-2019-A003 (*Advisory on Illicit Activity Involving Convertible Virtual Currency*), May 9, 2019 — confirm the functional approach (MSB/money transmitter), AML program, and SAR requirements, see: https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

6.1. The European Framework: eIDAS 2.0 and the European Digital Identity Wallet (EUDI Wallet)

The revision of Regulation (EU) No 910/2014 through Regulation (EU) 2024/1183 ("eIDAS 2.0") establishes the legal framework for the European Digital Identity Wallet (EUDI Wallet) and expands the suite of trust services, introducing, among others, electronic attestations of attributes (including their qualified form, QEAA). eIDAS 2.0 introduces a conformity-assessment mechanism for EUDI Wallets, with reference to European cybersecurity certification schemes (Reg. 2019/881—"Cybersecurity Act"), periodic vulnerability assessments, and adoption, by implementing acts, of the necessary reference standards. These policy choices increase legal trust and facilitate cross-border recognition.

From the users' perspective, eIDAS 2.0 configures a regime of granular control: the wallet is optional and free of charge for natural persons; the user decides on selective data sharing, and wallet providers must ensure logical separation of data and avoid unnecessary collection/merging for service provision. This normative design is compatible with GDPR principles (lawfulness, minimization, purpose limitation, security) and, in practice, creates a compliance framework in which the user can prove attributes or identity with minimal exposure. Moreover, the recitals to eIDAS 2.0 provide for the generation of user-managed pseudonyms for authentication where full identification is not legally required—an instrument with potential to reduce data correlation in routine transactions.

In blockchain environments, where technical traceability may come into tension with privacy, use of the wallet and attribute attestations enables legal alignment between AML/KYC requirements (identification, verification, audit) and data protection. In practice, users can prove legal capacities (e.g., age, residence in a Member State, status as a regulated professional) using QEAA or other attestations, without fully disclosing their personal-data set. This evolution relies on recognized open standards such as the W3C Verifiable Credentials Data Model 2.0 and W3C Decentralized Identifiers (DID) 1.0, essential for cross-border portability and interoperability[67].

VII. CONCLUSIONS

FATF standards acted as a catalyst for this convergence: Recommendation 15 (VAs/VASPs), Recommendation 16 (payment transparency/travel rule) and the 2021 Guidance on VAs/VASPs, as well as the 2020 Guidance on Digital Identity, encourage licensing/registration of VASPs, risk-based CDD/KYC, and transmission of essential data to trace flows.

In the European Union, blockchain compliance is built on a coherent and complementary legal architecture: MiCA provides the sectoral regime for issuers and service providers (CASPs); TFR 2023/1113 extends the travel rule to crypto-asset transfers; AMLR 2024/1624 unifies AML obligations for obliged entities (including CASPs); and AMLA 2024/1620 creates a dedicated European supervisor. In parallel, eIDAS 2.0 (2024/1183) offers a recognized, interoperable digital-identity infrastructure. Together, these instruments reduce the arbitrariness of classifications, enhance traceability of flows, and strengthen users' legal protection, while preserving—at least in design—the proportionality between transparency and privacy.

In the United States, BSA/FinCEN materializes equivalent requirements for AML programs, SARs, and recordkeeping/travel (31 C.F.R. § 1010.410), emphasizing a functional approach to value-transmission activities. In cooperation with FATF standards, a pragmatic equivalence dialogue (especially on the travel rule and acceptance of high-assurance digital-ID solutions) would facilitate operational alignment and reduce the arbitrariness of overlapping rules in cross-border transactions.

De lege ferenda, the following are recommended: (i) in secondary/tertiary EU law, an explicit clarification of GDPR–AMLR–TFR interactions (e.g., lists of legal bases, retention periods, and accepted pseudo-anonymization formulas); (ii) at the level of standardization, integration of the EUDI Wallet and qualified electronic attestations of attributes as sufficient proof for certain KYC elements (age, residence, professional status), accompanied by uniform guidance on assurance levels and mutual acceptance; and (iii) for transfers, an EU-wide interoperability protocol for the travel rule (hosted–hosted/hosted–unhosted), aligned with FATF recommendations and counterparty-verification mechanisms, to reduce the risk of fragmentation.

[67] W3C, Verifiable Credentials Data Model v2.0 (Recommendation W3C, 15 May 2025) and Decentralized Identifiers (DID) v1.0 (Recommendation W3C). see: https://www.w3.org/TR/vc-data-model-2.0/

REFERENCES

1. FATF, Guidance on Digital Identity (Paris: FATF/OECD, 6 Mar. 2020), see: https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html

2. FATF, Guidance on Digital Identity – Appendices (Paris: FATF/OECD, 2020), available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-Appendice-D.pdf

3. FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Paris: FATF/OECD, Oct. 2021), available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf?

4. FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (Paris: FATF/OECD, June 2024), available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf?

5. FATF Recommendations, Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs, Paris, 9 July 2024, available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

6. FATF, Best Practices on Travel Rule Supervision (Paris: FATF/OECD, 2025), available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf?

7. FATF, The FATF Recommendations – R.16 (Transparency of Transfers), available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html?

8. FFIEC, BSA/AML Examination Manual – Funds Transfers Recordkeeping (Travel Rule Requirements), available at: https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/09

9. Federal Register, Agency Information Collection Activities; Proposed Renewal… Recordkeeping and Travel Rule – reaffirmations concerning 31 C.F.R. § 1010.410(f) (Oct. 23, 2020; Aug. 13, 2024), available at: https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201023a.pdf

10. FinCEN, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (FIN-2019-G001, 9 May 2019), available at: https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

11. FinCEN, Funds "Travel" Regulations: Questions & Answers (Advisory Issue 7, Jan. 1997), available at: https://www.fincen.gov/system/files/advisory/advissu7.pdf

12. FinCEN, Advisory on Illicit Activity Involving Convertible Virtual Currency (9 May 2019), available at: https://www.fincen.gov/system/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

13. FinCEN, Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report (updated, including 2025), available at: https://www.fincen.gov/resources/frequently-asked-questions-regarding-fincen-suspicious-activity-report-sar

14. FinCEN, FIN-2019-G001 (Application of FinCEN's Regulations to Certain Business Models Involving CVCs), 9 mai 2019; FIN-2019-A003 (Advisory on Illicit Activity Involving CVC), 9 May 2019 — (MSB/money transmitter), AML and SAR. see: https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

15. Records to be made and retained; Recordkeeping/Travel Rule, 31 C.F.R. § 1010.410, available at: https://www.law.cornell.edu/cfr/text/31/1010.410

16. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114

17. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1113

18. Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401624

19. Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401620

20. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401183

21. Regulation (EU) 2016/679 (GDPR), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

22. Implementing Regulation (EU) 2015/1502 of 8 September 2015 laying down minimum technical specifications and procedures for assurance levels for electronic identification means under Regulation (EU) No 910/2014, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R1502

23. Reports by money services businesses of suspicious transactions, 31 C.F.R. § 1022.320, available at: https://www.law.cornell.edu/cfr/text/31/1022.320

24. W3C, Verifiable Credentials Data Model v2.0 (W3C Recommendation, 15 May 2025) and Decentralized Identifiers (DID) v1.0 (W3C Recommendation), available at: https://www.w3.org/TR/vc-data-model-2.0/