Legal 500
Country Comparative Guides 2026

Romania

Blockchain & Crypto Assets

Contributor

Lexters

Alexandru Stanescu

Partner | alexandru.stanescu@lexters.com

Simina Negulescu

Partner | simina.negulescu@lexters.com

Anca Popan

Associate | anca.popan@lexters.com

Miruna Rista

Junior Associate | miruna.rista@lexters.com

This country-specific Q&A provides an overview of blockchain & crypto assets laws and regulations applicable in Romania.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Romania: Blockchain & Crypto Assets

1. Please provide a high-level overview of the blockchain market in your jurisdiction. In what business or public sectors are you seeing blockchain or other distributed ledger technologies being adopted?

In Lexters' experience, much of the blockchain activity in Romania concerns payments in the crypto-asset domain: crypto cards, crypto-fiat conversion at checkout, merchant acceptance and stablecoin settlements. Payment by crypto card does not necessarily mean the merchant receives crypto-assets, as conversion often precedes settlement. Structuring tends to turn on how the platform, crypto-asset service provider and payment service providers allocate roles. Some merchant-facing models may fall within the commercial agent exclusion in Directive (EU) 2015/2366 (PSD2), where the intermediary acts for one party alone with genuine authority to negotiate or conclude the sale. The exclusion does not, however, remove any authorisation requirements applicable to separate crypto-asset services or card issuance.

Real estate tokenisation is another area of interest, particularly for project financing and investor participation. A token alone does not transfer title to Romanian real estate, but projects may instead structure investor participation through interests in vehicles owning the property, debt instruments or contractual rights.

In the public sector, blockchain technology has been used in Romania's electoral infrastructure since 2020, notably in systems monitoring the attendance of the voters and the centralisation of records from polling stations. In 2024, this infrastructure was also linked to the European Blockchain Services Infrastructure (EBSI), further supporting the traceability and integrity of electoral data. Votes themselves are not cast on-chain.

2. Please outline the principal legislation and the regulators most relevant to the use of blockchain technologies in your jurisdiction. In particular, is there any blockchain-specific legislation or are there any blockchain-specific regulatory frameworks in your jurisdiction, either now or envisaged in the short or mid-term?

Romania has no general national law regulating blockchain technology as such, but certain uses and activities are subject to specialised frameworks. For crypto-assets and related services, the principal framework is Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA). Within its scope, the applicable regime depends on the activity, the rights the token confers and the category of entity.

MiCA sits alongside Regulation (EU) 2023/1113 on transfers of funds and certain crypto-assets (TFR), Regulation (EU) 2022/2554 on digital operational resilience (DORA) and, at national level, Law No 129/2019 on money laundering and terrorist financing (AML Law), Government Emergency Ordinance (GEO) No 202/2008 on international sanctions and the Fiscal Code.

As for regulators, the Financial Supervisory Authority (ASF) supervises capital markets, investment services and funds, and the National Bank of Romania (BNR) credit, payment and electronic money institutions. For anti-money laundering (AML) purposes, the ASF (Article 28 of the AML Law) and the BNR (Article 27) cover the entities within their remit, including those providing crypto-asset services under Article 60 MiCA. The National Office for Prevention and Control of Money Laundering (ONPCSB), which is also the financial intelligence unit, supervises the remaining obliged entities – those not subject to AML supervision by the BNR or ASF. Tax matters fall to the National Agency for Fiscal Administration (ANAF).

Looking ahead, although MiCA already applies directly, a draft emergency ordinance and implementing rules would complete national authorisation, supervision and sanctions and clarify operators' route to market. Until it is adopted, no Romanian authority is designated as competent under MiCA, and the ASF has stated publicly that it cannot receive or decide MiCA authorisation applications. Under Article II of the draft, the ASF would be competent for asset-referenced tokens (ARTs), crypto-assets other than ARTs and e-money tokens (EMTs), including utility tokens, and crypto-asset service providers (CASPs), and the BNR for issuance of EMTs by credit and electronic money institutions it authorises and prudentially supervises. Article XI also proposes a technical opinion from the Authority for the Digitalisation

 © 2026 Legalease Ltd

of Romania on CASPs' IT systems before they apply to or notify the ASF, separate from MiCA authorisation.

At EU level, Regulation (EU) 2024/1624 (AMLR) will impose directly applicable AML obligations on CASPs from 10 July 2027. The Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) promotes supervisory convergence and cooperation and, from 2028, is expected to supervise directly selected high-risk cross-border financial entities, without replacing national supervisors.

3. What is the current attitude of the government and of regulators to the use of blockchain technology in your jurisdiction?

Among Romanian regulators, the ASF's position is the most visible. For blockchain projects requiring ASF authorisation, the ASF's openness to innovation and dialogue is a welcome development, as it is their counterpart for market access and supervision, including under the proposed MiCA allocation once adopted. Its 2026-2028 strategy on financial innovation addresses crypto-assets and tokenisation and favours proportionate supervision based on the risk of the entity. In Lexters' experience, preparation should cover governance, marketing, including influencer promotion, and conduct towards clients.

The ASF's Innovation Hub facilitates dialogue and guidance, but grants no derogations and does not replace authorisation.

4. Is there a central bank digital currency ('CBDC') project in your jurisdiction? If so, what is the status of the project?

The BNR has not issued a CBDC. In 2022 it described exploratory work, which was not a decision to issue; to our knowledge, no later update confirms it remains active.

The more relevant CBDC is therefore the digital euro, a Eurosystem project designed to operate on a centralised settlement platform. A 12-month pilot, using a beta version without legal tender status, is planned from the second half of 2027. The European Central Bank (ECB) targets a possible first issuance in 2029, assuming the necessary EU legislation is adopted by the end of 2026 and subject to a subsequent decision to issue.

Romanian businesses may already seek a role in the pilot. On 15 September 2026 the ECB invited e-commerce and m-commerce merchants established in the EU (and able to serve at least two pilot countries, among other criteria) to apply by 27 October 2026. Participation involves a standard, non-negotiable ECB agreement and new or adapted arrangements with a participating acquiring payment service provider (PSP). A separate phase of the ECB's digital euro innovation platform targets organisations established in the EU, including fintechs, PSPs, technology providers and merchants. In either case, early legal preparation centres on eligibility, application requirements and participation terms.

5. What is the current approach in your jurisdiction to the treatment of cryptoassets and decentralised finance ('DeFi') for the purposes of financial regulation?

In Romania, the regulatory analysis of a crypto project turns on the following questions: which regime applies to the asset, what authorisation the activity requires and, in DeFi, who is responsible.

The first depends on the rights the token confers. If it functions as a financial instrument, it falls under Directive 2014/65/EU (MiFID II) and Law No 126/2018 and outside MiCA, even when marketed as a utility token. For crypto-assets within MiCA's scope, stricter rules apply to EMTs and ARTs, while public offers of other crypto-assets generally require a notified and published white paper, subject to exemptions.

The second question concerns the activity rather than the asset. Providing crypto-asset services to clients, such as custody or exchange, requires CASP authorisation or, for eligible financial institutions, a notification under Article 60 MiCA, and CASPs authorised under MiCA in another EU Member State may passport in. The application under Article 62 MiCA must include, among other things, a programme of operations, governance and internal control arrangements, business continuity, information and communication technology (ICT) and AML arrangements, and evidence of the fitness of management and the suitability of qualifying shareholders (see question 16). The competent authority then has 25 working days to assess completeness and 40 working days to assess a complete application (Article 63). Since the transitional period ended on 1 July 2026, neither a pending application nor a historical AML registration permits continued activity.

Payments illustrate how these regimes may overlap. MiCA authorisation does not in itself cover payment services, and the European Banking Authority (EBA) has indicated that EMT transfers and certain custodial wallet

 © 2026 Legalease Ltd

services may require PSD2 coverage, directly or through an authorised PSP. For card and checkout products, allocating services between the CASP and its payment partner is therefore a regulatory question, not merely a commercial one.

In DeFi, the third question divides into two. The first is whether anyone provides a regulated service: MiCA excludes only services provided in a fully decentralised manner, without any intermediary. Accordingly, control of admin keys, the power to modify or pause the protocol, fee setting or the user relationship may point to an identifiable provider. The second concerns the token itself, as a decentralised service does not remove the offeror's obligations: the European Commission's answer published by the European Securities and Markets Authority (ESMA) in ESMA Q&A 2671 notes that listing on a decentralised exchange in the EU may amount to an offer to the public.

Where exactly the line lies remains unsettled. The Danish Financial Supervisory Authority's principles (June 2024) treat an activity as decentralised only where users have no identifiable counterparty capable of entering into a valid contract for the service. They also look at whether the activity is offered exclusively through smart contracts outside the control of any identifiable person — so an interface run by a company may be regulated even where the underlying protocol is not. ESMA's response of 30 September 2026 to the Commission's MiCA review consultation goes further. It notes that national authorities read 'full decentralisation' differently and warns against 'decentralisation washing' by identifiable operators. It also proposes a definition of DeFi in MiCA with an exemption as narrow as possible, together with a new regulated service for CASPs giving clients access to DeFi protocols. ESMA's recommendations are proposals, not law, but in our view a Romanian assessment of partially decentralised models should proceed on the same basis: by identifying who provides or controls each potentially regulated activity.

6. What is the current approach in your jurisdiction to the treatment of cryptoassets and DeFi for the purposes of anti-money laundering and sanctions?

Under Romania's AML Law (Law No 129/2019), CASPs within its scope must know their customers and monitor the business relationship on an ongoing basis. Where a service involves a continuing relationship, customer due diligence applies whatever the value of the first transaction: the EUR 1,000 threshold for occasional transactions does not allow platform users to trade without checks merely because amounts are small. Simplified measures require a justified low risk and still include verifying identity.

Onboarding is therefore only the starting point. Product risks should be assessed before launch, and completing know your customer (KYC) checks does not justify accepting every later transaction automatically: monitoring should test whether activity remains consistent with the customer's profile and declared purpose. Splitting transactions to stay below thresholds, or moving funds rapidly across several addresses without a plausible economic reason, are typical warning signs. Internal alert thresholds should be justified and reviewed, not treated as legal triggers for enhanced due diligence. Nor does the sector's high rating in the ONPCSB's 2026 national risk assessment make every customer high risk: additional measures follow the concrete risk, save where the law requires them.

Transfer rules add a further layer. Under the TFR, covered crypto-asset transfers must carry information on the originator and beneficiary, with no general threshold. The product must distinguish transfers to another CASP from transfers to a self-hosted address, which may belong to the customer or to a third party; for transfers above EUR 1,000 involving such an address, the CASP must assess whether it is owned or controlled by its customer. Third-party wallets are not excluded, but procedures must cover missing information and any additional checks required.

These checks become harder where funds pass through DeFi, and the EBA's guidelines treat exposure to certain DeFi platforms as a possible risk increasing factor. There may be no intermediary verifying participants, and routes through several protocols can obscure where funds come from and why they move. This does not make every protocol interaction suspicious, nor should DeFi be equated with mixers. Yet when funds return from a protocol, the account holder may already be identified while the source of those funds is not. Explanations, on-chain analysis and risk-based monitoring may be needed, with blockchain analytics complementing, not replacing, customer checks.

Sanctions obligations operate separately. GEO No 202/2008 expressly treats crypto-assets as funds, so screening, compliance with applicable prohibitions and, where required, freezing and reporting apply regardless of AML status. A higher AML risk, a suspicious transaction report to the ONPCSB and a freezing obligation are distinct matters. Before connecting a service to DeFi protocols, an operator should decide what information allows it to accept a flow and when the law requires

 © 2026 Legalease Ltd

further checks, escalation or refusal.

7. What is the current approach in your jurisdiction to the treatment of cryptoassets and DeFi for the purposes of taxation?

In Romania, the tax treatment of crypto-assets follows the nature of the income and the status of the taxpayer, not the MiCA classification. For individuals, the positive difference between the sale price and the acquisition cost, including direct costs, is in principle taxed at 16% where the gain is realised from 1 January 2026. The tax is self-assessed in the single tax return (Declara ia unică) by 25 May of the following year and may attract health insurance contributions.

The same principle applies to payments or rewards received in tokens: remuneration, royalties or dividends paid in crypto are taxed according to their nature, and a later disposal is analysed separately. Income may thus arise in kind before conversion into fiat, as ANAF has confirmed for non-fungible tokens (NFTs), though not every token receipt is taxable. Romanian guidance on DeFi remains limited, so for staking, lending, liquidity provision and swaps the nature, timing and valuation of the income must each be assessed.

For corporate taxpayers, crypto income falls within profit tax or, where eligible, the microenterprise regime. Under profit tax, accounting classification, valuation and documented acquisition cost are decisive for the fiscal result. The microenterprise regime applies a tax base constructed on revenue, with the adjustments provided by law, rather than on the profit of individual transactions. VAT requires a distinct analysis: in *Hedqvist* (Case C-264/14), the Court of Justice of the European Union treated exchanging bitcoin for traditional currency as an exempt supply of services, an exemption that does not automatically extend to goods or services paid for in crypto.

Alongside these tax rules, Council Directive (EU) 2023/2226 (DAC8), transposed by GEO No 71/2025, introduces separate reporting obligations for crypto-asset providers. Providers required to report in Romania file form F8000 by 15 March of the following year, first by 15 March 2027 for 2026. Reporting jurisdiction and users' tax residence are distinct: ANAF's guidance gives the example of a CASP authorised in Italy that reports its Romanian users there.

These obligations also influence onboarding and the collection of tax information. Where a user fails to provide it despite two reminders after the initial request, the provider must prevent exchange transactions, though not before 60 days from that request. Reporting a transaction does not in itself establish a taxable gain or its amount, nor does it replace the taxpayer's own return.

8. What is the current approach in your jurisdiction to retail and wholesale tokenisation projects?

Romania's market for tokenised products is still developing, notably around real estate project financing and crowdfunding. The ASF's strategy provides relevant supervisory context for projects within its remit (see question 3): such projects will be structured and assessed in that supervisory context, although the strategy grants no derogations.

In the absence of a general tokenisation regime, projects are structured within existing legislation, according to investors' rights and the activities carried out. Tokenisation does not change the legal nature of the right represented, nor does it replace the formalities needed to create or transfer it. Depending on the model, civil and company law, the rules on financial instruments or investment funds, or the crowdfunding regime may become relevant. A token that qualifies as a financial instrument falls within that framework and outside MiCA (see question 5).

Crowdfunding shows how this works in practice. Tokenisation can serve crowdfunding projects and, where the model meets the conditions of Regulation (EU) 2020/1503 and Law No 244/2022, financing may run through an authorised crowdfunding service provider. That regime covers only certain loans, transferable securities and admitted instruments. Not every token sale is therefore regulated crowdfunding and MiCA authorisation does not replace a crowdfunding licence. In a real estate project, for instance, the investor may acquire a claim against, or a shareholding in, a company owning the property; the token itself transfers no ownership of the building, nor does a special purpose vehicle make regulatory analysis unnecessary.

Whether a project is retail or wholesale, the starting point remains the nature of the right. For retail offers, disclosure, marketing and investor protections carry particular weight; for professional investors, eligibility and the conditions for distribution and transfer must still be checked, since wholesale does not mean unregulated. In either case, before the offer it should be clear what right the investor can exercise, against whom, and on what terms it can be transferred or the investment recovered; tokenisation does not in itself guarantee liquidity.

 © 2026 Legalease Ltd

9. Are there any prohibitions on the use or trading of cryptoassets in your jurisdiction? If permitted, is cryptoasset trading common?

Romania does not generally prohibit holding, using or trading crypto-assets, although they are not legal tender. The practical line runs between investing for one's own portfolio and providing services to clients: individuals and companies may buy, hold and sell crypto-assets for their own investment purposes. By contrast, providing crypto-asset services to clients on a professional basis, including where the operator uses its own capital to execute client transactions, is subject to market access conditions (see question 5).

Restrictions therefore attach mainly to what is offered, not to ownership. MiCA limits public offers and admissions to trading of ARTs and EMTs that do not meet its requirements, which may limit certain stablecoins on platforms serving the EU without prohibiting their holding. Similarly, Article 76(3) MiCA requires trading platforms to prevent the admission of crypto-assets with inbuilt anonymisation functions unless the operator can identify their holders and transaction history; the rule concerns listing, not possession. Market abuse prohibitions under Title VI MiCA apply to crypto-assets admitted to trading or for which admission to trading has been requested. International sanctions apply in their own domain, independently of MiCA. Whether a person may hold an asset and whether a platform may offer it to clients are thus separate questions.

Participation appears significant, although it is difficult to quantify. The ONPCSB's 2026 national risk assessment describes high interest in virtual assets, reflected in the use of local and international platforms and in crypto infrastructure. A 2026 Ipsos survey for Tradesilvania, a local operator, of 500 Romanian internet users aged 18 to 55 found that 33% of those who had heard of cryptocurrencies said they held some. These figures indicate adoption, but they do not measure how often people trade or the national number of active traders.

10. To what extent have initial coin offerings ('ICOs') taken place in your jurisdiction and what has been the attitude of relevant authorities to ICOs? If permissible, what are the key requirements that an entity would need to comply with when launching an ICO?

An ICO usually involves a public offer of newly issued crypto-assets, often followed by their admission to trading on a centralised or decentralised platform. Where applicable, MiCA regulates both as separate events, and admission to trading alone would not ordinarily be described as an ICO, although it may independently trigger other requirements under MiCA. The best known Romanian-rooted example is the 2019 international token sale by Elrond, now MultiversX, on Binance Launchpad. To our knowledge, the Romanian authorities did not intervene in that sale, and token offers have not raised notable regulatory issues in Romania.

Structuring a token offering begins with an analysis of what the token represents, the rights it confers on holders and the economic model of the project. The issuer's commercial objectives guide the structure, but the applicable regime follows from these features. A token with rights comparable to shares, bonds or fund units may be deemed a financial instrument and therefore fall outside MiCA. A token that purports to maintain a stable value by referencing a single official currency is an EMT, whereas one referencing another value or right, or a combination of them, is considered an ART; both follow their own issuer regimes. Other crypto-assets within MiCA's scope, including utility tokens, fall under Title II, which governs the offers discussed below.

For a Title II offer, the offeror must be a legal person and, absent an exemption, must prepare, notify and publish a white paper. The notification, which includes a legal explanation of the token's classification, is made at least 20 working days before publication. No prior approval is required, but the competent authority retains powers to require amendments or additional disclosures and to suspend or prohibit the offer where the conditions under MiCA are met. In Romania, the designation of the competent authority to which the white paper is notified depends on the national framework discussed in question 2. Sale terms and marketing must match the white paper and the product, and retail purchasers benefit from applicable protections, including withdrawal rights where the conditions of Article 13 MiCA are met. Launching one's own offer does not in itself require CASP authorisation, although client services and intermediaries' roles are assessed separately.

On top of these considerations, the format of the white paper also needs early attention. Since 23 December 2025, white papers must be submitted in XHTML with inline XBRL (iXBRL) tagging, and ESMA has published the relevant taxonomy together with a model iXBRL template.

11. Are there any legal or regulatory issues concerning the transfer of title to or the granting

 © 2026 Legalease Ltd

of security over cryptoassets?

Romanian rules on property, the transfer of rights and security interests provide the framework, and the Civil Code already recognises intangible assets. The difficulty may lie in applying those rules to distributed ledgers, private key control and custody, where different interpretations remain possible. In our view, crypto-assets may, depending on their nature, be intangible movable assets capable of ownership, but workable solutions require reasoned interpretation consistent with the purpose of the rules and documentation adapted to the technical mechanism.

With regard to transfers, the token itself, a claim against an issuer or custodian and a right in an asset represented by the token are different things, and the formalities of the represented right still apply. For fungible crypto-assets, individualisation may take a form suited to the asset, so how the contract identifies the assets and structures the operation is decisive. In custody, rights may be allocated through internal records without an on-chain transaction for each operation; Article 75 MiCA requires registers of client positions, but does not itself fix when ownership passes under civil law. On-chain records and key control are technically and evidentially relevant, yet neither alone proves ownership or the power to dispose.

The same gap between legal and technical control is present with regard to granting of security over crypto-assets. A movable mortgage may in principle be created, depending on the right encumbered, with the required documentation and publicity. Registration in the National Register for Movable Property (RNPM, Registrul Na ional de Publicitate Mobiliară) provides publicity and priority under the applicable rules, but no technical access to the assets. Conversely, key control does not replace valid creation and the applicable perfection requirements. A financing should therefore identify the token, network and quantity or the right encumbered. It should also settle who authorises transfers, including under multi-signature (multisig) arrangements, whether the assets may be moved or staked, and how they will be valued and realised on default. Automated liquidation must still comply with mandatory enforcement rules, which a smart contract cannot displace.

12. How are smart contracts characterised within your legal framework? Are there any enforceability issues specific to the operation of smart contracts which do not arise in the case of traditional legal contracts?

Romanian law has no separate category for smart contracts. Smart contract code does not automatically constitute a legally binding contract, but it may express the parties' agreement or automate its performance. A smart contract may accordingly be treated as a contract, or as the means of performing one, where the elements inherent in any contract are present, namely an agreement between parties with capacity, valid consent, a lawful object and cause, and any required form. Where the law requires an authentic deed, code cannot supply it.

Verifying those elements, and enforcing the agreement once the code runs, raises distinctive evidential and practical enforcement difficulties. Pseudonymous addresses complicate identifying the parties and attributing consent, as a wallet signature proves control of a key, not the signer's authority. Where code and text diverge, nothing gives the code priority over the parties' common intention, yet oracle errors, forks or upgrades may alter performance without any matching agreement from the parties. Moreover, a smart contract usually executes automatically and irreversibly, so there is often no opportunity to ask a court to stop a transfer before it happens, as there might be with a traditional contract. A court judgment will not itself rewrite the on-chain record, but may order the restitution of assets, damages or other remedies available under applicable law (for personal data, see question 15).

Some smart contracts also face specific EU requirements. Since 12 September 2025, Article 36 of Regulation (EU) 2023/2854 (Data Act) has applied to smart contracts used to execute data sharing agreements, not to smart contracts or DeFi protocols generally. These must ensure robustness and access control, safe termination or interruption, archiving for auditability and consistency with the agreement executed. Termination stops future executions but does not undo those already recorded. The vendor or, failing that, the person deploying them for others in a professional capacity must carry out a conformity assessment and issue an EU declaration of conformity. The Digital Omnibus has proposed deleting Article 36, but it remains applicable unless amended.

13. How are Decentralised Autonomous Organisations ('DAOs') treated in your jurisdiction?

Romanian law regulates several forms of association, from companies and associations with legal personality to contractual arrangements without it. In our view, an

 © 2026 Legalease Ltd

unincorporated DAO may qualify as a simple partnership (societate simplă) under Article 1881 of the Civil Code where participants make contributions, cooperate in a common activity and aim to share the resulting profits or savings; holding a governance token or casting an isolated vote does not in itself establish that relationship. If so, partners may be liable with their own assets where creditors are not satisfied from the common assets — in proportion to their contributions, but not limited to them. Where the project takes a corporate form, a joint-stock company (societate pe ac iuni) may be a suitable vehicle, as it offers legal personality, limited liability and a governance structure capable of accommodating transferable participation rights. However, holding governance tokens does not automatically confer shareholder status, and the choice of form depends on the project's specific features and applicable requirements.

In practice, a project may use a limited liability company for development, staff and contracts. Whichever form is used, incorporation does not in itself transfer the project's assets, intellectual property or obligations to that entity. The documentation should therefore establish who legally holds the treasury assets and authorises transactions, who owns or licenses the code and other intellectual property, who contracts with developers and suppliers, and who may represent and bind the entity.

Additionally, on-chain votes must be integrated into the entity's documents and procedures, respecting the powers of its corporate bodies and applicable formalities. A community vote does not automatically replace a shareholders' resolution or give any participant authority to represent the entity, and directors keep their legal duties. A shareholders' agreement may complement the corporate documents by setting out the scope and limits of on-chain governance, the process for implementing community decisions within the entity and the conditions under which key roles or authorisations may change. The documents should therefore set out what the community decides, who implements the decision and within what limits.

It is also important to note that if the entity becomes insolvent, liability may extend to persons controlling its financial or operational decisions, whatever their formal role, but only where the statutory conditions are met; holding admin keys may be relevant to control but does not alone create liability. Community governance must ultimately be tied to identifiable asset holders, authorised signatories and their responsibilities, while the activities carried out remain subject to their own requirements.

14. Have there been any governmental or regulatory enforcement actions concerning blockchain in your jurisdiction?

From published press releases and public cases, the enforcement actions we are aware of have concerned tax or criminal law matters, relying on fiscal, criminal and asset recovery tools. We have not identified any published sanction applied under MiCA in Romania. In June 2022 ANAF's anti-fraud directorate announced tax assessments of about EUR 2.1 million on crypto income. In June 2026 ANAF acted in Satu Mare against systematic mining outside the tax and accounting records, announcing the confiscation of 407 machines. According to the press release of 23 June 2026, the case is ongoing, and the action implies no general restriction on mining. In September 2025 the EU Agency for Criminal Justice Cooperation (Eurojust) reported a cross-border investigation, with searches involving Romanian authorities, into an alleged crypto investment fraud of at least EUR 100 million.

As for the ASF, at the close of the MiCA transitional period it issued a communication that was preventive in nature, intended to inform and alert investors rather than to record any measures actually taken. Until the national act confers MiCA sanctioning powers, action against unauthorised providers may rely on fiscal, criminal, AML or international sanctions competences, each on its own legal basis, as well as on coordination through ESMA. The absence of published MiCA sanctions does not justify operating without the necessary authorisation or outside the scope of an existing one.

15. Are there any other generally-applicable laws, case law or regulations that may present issues for the use of blockchain technology (such as privacy and data protection law or insolvency law)?

In Romania, as across the EU, Regulation (EU) 2016/679 (GDPR) applies to on-chain data whenever it enables identification. The European Data Protection Board's (EDPB) blockchain Guidelines 02/2025, adopted in final form on 7 July 2026, treat wallet addresses, encrypted data and keyed hashes as personal data where identification is possible by means reasonably likely to be used. Before deployment, a project should document why a blockchain is necessary, choose an architecture minimising personal data on-chain and carry out a data protection impact assessment where the processing may generate a high risk. It should also build in an erasure or anonymisation mechanism whose effectiveness can be

 © 2026 Legalease Ltd

tested. Deleting off-chain data alone does not suffice if on-chain addresses or correlatable information still permit identification.

In insolvency, a client holding crypto-assets in custody and one holding an unsecured claim against the CASP face different prospects. Article 75 MiCA requires legal and operational segregation, supported by individual records of each client's positions, reconciliation and arrangements enabling restitution or transfer. These arrangements must sustain the legal structure, as a separate wallet alone does not establish ownership or guarantee recovery. Under Article 169 of the Insolvency Law (Law No 85/2014), the persons who may be held liable for causing insolvency now expressly include those controlling the debtor's financial or operational decisions, regardless of formal role. Liability remains subject to the statutory conditions, including the relevant act and causal link, and to the transitional rules.

Automation does not remove legal remedies. Under Law No 193/2000, terms making the output of code incontestable may be unfair. GEO No 141/2021 defines 'price' to include a digital representation of value, so payment in crypto-assets does not exclude protection for eligible digital content or services; whether an NFT falls within that regime depends on what it actually provides, and financial services are excluded. Where a service is modified over time, including through a protocol upgrade, in a manner that goes beyond what is necessary to maintain conformity, the change requires a contractual basis, information and, where the conditions are met, a right to terminate.

16. Are there any other key issues concerning blockchain technology in your jurisdiction that legal practitioners should be aware of?

For CASPs operating in Romania, governance requirements apply from the first instance. Local substance is the starting point: under Article 59(2) MiCA, a CASP must have its registered office in a Member State where it provides at least part of its services, its place of effective management in the EU and at least one director resident in the EU. ESMA's supervisory briefing on the authorisation of CASPs (31 January 2025) goes further in practice, expecting at least one executive member of the management body to reside in the home Member State and sufficient staff on the ground. In our view, an applicant in Romania should therefore expect scrutiny of whether management is genuinely present locally, not merely a letterbox entity.

The fitness of management and the reputation of qualifying holders are assessed at authorisation, and acquisitions of qualifying holdings require prior notification and evaluation. The joint EBA/ESMA guidelines address competence, reputation and time commitment of the management body, while ESMA emphasises sufficient staffing, genuine autonomy in the process of decision making and effective control over outsourced functions, including within a group. These elements should be planned when forming the management team, admitting new investors or selecting critical service providers.

Prudential requirements are likewise fixed at authorisation. Under Article 67 MiCA, a CASP must hold prudential safeguards at least equal to the higher of the permanent minimum capital in Annex IV, which ranges from EUR 50,000 for services such as advice or order transmission to EUR 150,000 for operating a trading platform, and one quarter of its fixed overheads for the preceding year. The safeguards may take the form of own funds, an insurance policy or a comparable guarantee, or a combination of them, so initial capital is a continuing requirement reviewed annually rather than a one-off deposit.

Operational continuity depends on aligning corporate authorisations with technical control. Documentation should cover who may operate wallets and authorise transfers, how access is recovered when a key holder departs or becomes unavailable, how key holders are replaced, and how wallet balances are reconciled with individual client positions and accounting records.

Looking ahead, the EBA's recommendations of 24 September 2026 identify directions for MiCA revision, including crypto lending, CASP-facilitated access to DeFi lending protocols, risks of multi-issuer stablecoin schemes and clarification of crypto-asset classification; these are reform directions, not obligations already in force.

 © 2026 Legalease Ltd

Contributors

Alexandru Stanescu
Partner
alexandru.stanescu@lexters.com



Simina Negulescu
Partner
simina.negulescu@lexters.com



Anca Popan
Associate
anca.popan@lexters.com



Miruna Rista
Junior Associate
miruna.rista@lexters.com



 © 2026 Legalease Ltd