Journal of Kyzylorda Scholarly Review

P-ISSN:3006-0265 | E-ISSN:3007-4681. Published by the Open University of Kyzylorda

https://bulletin.ouk.kz/index.php/bulletin/index

SMART CONTRACTS AND DIGITAL FINANCIAL ASSETS AS INSTITUTIONS OF CIVIL LAW: A COMPARATIVE LEGAL ANALYSIS OF RUSSIA, UZBEKISTAN, AND THE EUROPEAN UNION

S. A. Kenzhaboev
Faculty of International Law, MGIMO-Tashkent, Moscow State Institute of International Relations (University), Ministry of Foreign Affairs of the Russian Federation

T. V. Vasilyeva
Academic Supervisor, Candidate of Geographical Sciences

Abstract. The development of distributed ledger technology and the widespread introduction of smart contracts into civil transactions have confronted national legal systems with the need to determine the civil-law characterization of this technological phenomenon and the legal regime governing digital financial assets whose issuance and circulation are mediated by smart contracts. This article presents a comparative legal analysis of the civil-law nature of smart contracts and the regime of digital financial assets in three jurisdictions that have adopted fundamentally different regulatory strategies: the Russian Federation, which follows a model of targeted amendments to the Civil Code and special legislation on digital financial assets; the Republic of Uzbekistan, which applies a model of proactive and experimental rulemaking through acts of the head of state; and the European Union, which adopted the comprehensive Markets in Crypto-Assets Regulation (MiCA) in 2023 together with a pilot regime for market infrastructures based on distributed ledger technology. The article proposes an original three-element model for the civil-law characterization of a smart contract: a smart contract as a form of transaction, a smart contract as a method of performing an obligation, and a smart contract as an automated information system. It substantiates the conclusion that smart contracts generally have an auxiliary rather than primary role in civil transactions and examines the procedural and conflict-of-laws issues arising when transactions performed through smart contracts are declared invalid. Based on the analysis, the article formulates proposals for improving the legislation of the three jurisdictions under review and introduces a concept for UNIDROIT and UNCITRAL model provisions on smart contracts intended to promote uniform approaches to their civil-law characterization.

Keywords: smart contract; digital financial assets; blockchain; civil law; comparative law; MiCA; digital economy; invalidity of transactions; UNCITRAL; UNIDROIT.

Introduction

A smart contract—a piece of software code that automatically performs predetermined conditions when specified events occur—has evolved over the past decade from a theoretical concept formulated by Nick Szabo in 1994 [1] into a widely used instrument of civil transactions. Smart contracts are now used to issue digital financial assets, execute transactions on decentralized exchanges, administer corporate relationships within decentralized autonomous organizations, and perform insurance and credit agreements. According to estimates by analytical agencies, the aggregate value of assets locked in the smart contracts of various blockchain protocols amounts to tens of billions of US dollars.

The extensive penetration of this technology into civil transactions has presented legal scholarship with a question that has yet to receive a uniform answer in any of the jurisdictions under review: is a smart contract an independent form of transaction that replaces traditional methods of contract formation, or is it merely a technical means of performing a contract already concluded under general civil-law rules? The answer determines the resolution of numerous practical issues, including the applicability of general rules on the invalidity of transactions to operations performed through smart contracts; the allocation of liability for errors in smart-contract code; the possibility of challenging the outcome of automated performance; and, finally, the governing law and jurisdiction over disputes arising from smart-contract relationships involving a foreign element.

This article aims to conduct a comparative legal analysis of the civil-law characterization of smart contracts and the regulation of digital financial assets issued with their use in three jurisdictions: the Russian Federation, the Republic of Uzbekistan, and the European Union. These three legal systems were selected because each represents a distinct regulatory model. Russia follows a model of selectively incorporating provisions on digital rights into codified civil legislation; Uzbekistan applies a model of dynamic and experimental rulemaking at the level of subordinate legislation; and the European Union has adopted a model of comprehensive supranational codification implemented through Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA) [2], which entered into force in 2023 and currently represents the most detailed international regulatory framework for digital assets.

The object of the study is the body of social relations arising from the formation and performance of transactions through smart contracts and from the issuance and circulation of digital financial assets. The subject of the study comprises the civil and special legislation of the Russian Federation, the Republic of Uzbekistan, and the European Union governing these relations, doctrinal approaches to the characterization of smart contracts, and relevant law-enforcement and judicial practice.

The methodology is based primarily on the comparative legal method, supplemented by the formal legal method for interpreting the legislation of the three jurisdictions and the legal modeling method for developing de lege ferenda proposals.

The civil-law characterization of smart contracts has been addressed by a number of Russian and foreign scholars. A. I. Savelyev was among the first in Russian legal doctrine to offer a systematic analysis of smart contracts as a form of contractual interaction and to substantiate the proposition that the phenomenon is primarily technical rather than independently legal in nature [3]. The debate on the relationship between smart contracts and traditional contracts was further developed in the works of Yu. S. Kharitonova, who examined tokenization as a means of exercising proprietary rights [4], and R. M. Yankovsky, who analyzed the legal regime of cryptocurrencies and related digital instruments under Russian law [5], [6], [7]. In foreign scholarship, the foundational importance of Nick Szabo's work, which first formulated the concept of the smart contract [1], remains undiminished, alongside subsequent studies addressing the relationship between the principle that "code is law" and traditional contract law [8]. Despite the substantial body of existing literature, legal doctrine still lacks a comprehensive comparative study covering the Russian, Uzbek, and European Union regulatory models for smart contracts and the digital financial assets mediated by them. This gap determines the scholarly novelty of the present study.

The concept of the smart contract was introduced by American cryptographer and legal scholar Nick Szabo in 1994 [1] to describe a computer protocol designed for the digital formalization, verification, and performance of contractual terms. In a 1997 paper, Szabo defined a smart contract as a set of promises specified in digital form, including the protocols within which the parties perform those promises [8]. Practical implementation of the concept became possible only after the launch of the Ethereum platform in 2015, which provided a Turing-complete computational environment for executing arbitrary programs on a decentralized network.

From a technical standpoint, a smart contract is software code deployed at a specific blockchain address and automatically executed upon receipt of a transaction that satisfies its conditions. Its key characteristics of civil-law significance include autonomous execution—the code operates without human intervention and independently of the parties' subsequent will after deployment on the network; determinism—identical inputs always produce identical outputs, thereby ensuring predictable legal consequences; immutability after deployment—deployed code generally cannot be altered without creating a new version of the contract, although certain architectural solutions, such as proxy contracts, permit limited upgrades; and public verifiability—the source code of most smart contracts is open and may be inspected by any interested person.

A digital financial asset issued through a smart contract is a record in a distributed ledger certifying a particular proprietary right. Depending on its legal structure, the right may be monetary, such as a claim for payment of a specified sum; corporate, such as a right to participate in an issuer's capital; or otherwise proprietary in nature. In relation to a digital financial asset, a smart contract performs several technological functions simultaneously: it issues tokens in accordance with parameters established by the issuer; maintains the register of holders by recording each transfer of rights; and may automatically perform associated obligations, including the accrual of interest, payment of dividends, and redemption of a debt instrument upon maturity.

A distinction between two technological models for issuing digital financial assets is of fundamental importance to the analysis that follows. The first model is issuance on a permissioned ledger controlled by an information-system operator that satisfies special statutory requirements, including licensing and participant identification. This model underlies Russian Federal Law No. 259-FZ [9] and a substantial part of the MiCA framework for asset-referenced tokens and e-money tokens [2], [10]. The second model is issuance on a public, permissionless blockchain without a single administrator. This model is typical of most cryptocurrencies and a significant share of NFTs, but it creates major difficulties for the application of licensing and participant-identification requirements because the issuer is technically unable to control the subsequent circulation of the asset.

Methods

An analysis of doctrinal approaches and legislation in the three jurisdictions under review makes it possible to identify three competing models for the civil-law characterization of smart contracts, each of which appears in different combinations across the legal systems considered.

Under the first approach, a smart contract may be regarded as an independent form of concluding a contract electronically. In Russian law, this approach is based on Article 434 of the Civil Code of the Russian Federation [11], which recognizes the possibility of concluding a contract through the exchange of electronic documents, provided that the document can be reliably attributed to a contracting party. Deployment of a smart contract on a blockchain, accompanied by the cryptographic signature of the initiating party, could theoretically satisfy this criterion because the sender's public key uniquely identifies the source of the transaction, while the immutability of the blockchain record ensures reliable fixation of the expression of intent.

In European Union law, a similar role is played by Regulation (EU) No. 910/2014 (eIDAS) [12], which establishes general principles for recognizing the legal effect of electronic signatures, electronic seals, and electronic time stamps, as well as by the proposed eIDAS 2.0 framework,

which directly addresses the use of distributed ledger technology for electronic identification. Certain Member States have gone further. Malta, for example, through its 2018 Virtual Financial Assets Act [13], has legally recognized smart contracts as a form of concluding transactions subject to specified technical certification requirements for the technological platform used.

Under the second approach, which is more prevalent in legal doctrine, a smart contract does not itself replace a civil-law contract in the traditional sense but serves as a technical means of automating its performance. The contract between the parties is concluded through a combination of legally relevant actions, such as publishing an offer, communicating acceptance, or acceding to a platform's user agreement, while the smart contract merely records and technologically implements its terms. Paragraph 2 of Article 309 of the Civil Code of the Russian Federation [11], introduced by Federal Law No. 212-FZ of 26 July 2019 [14], expressly permits the performance of an obligation through information technologies specified in the terms of the transaction without any separately expressed additional consent. This provision creates a direct statutory basis for precisely this model of characterization.

This approach offers a substantial practical advantage: it does not require revision of traditional rules governing the form and procedure for concluding transactions and makes it possible to apply general rules of the law of obligations, including rules on invalidity, to the relations between the parties, while treating the smart contract as a technical means of performing an already existing obligation. This approach predominates in Uzbek law-enforcement practice, where acts of the National Agency for Perspective Projects consistently proceed from the premise that regulation concerns not smart-contract code as such but the underlying civil-law relationship [15], [16].

The third approach, which remains the least widespread but is gaining recognition in recent scholarship, treats a smart contract as an independent object of legal regulation—a special type of automated information system. Under this view, its legal regime cannot be reduced either to a form of transaction or to a method of performing an obligation and instead requires specific regulation analogous to that applicable to other technical systems that generate legal consequences, such as automated decision-making systems using artificial intelligence. This approach is most fully reflected in the legislation of several US states, including Arizona, Tennessee, and Wyoming, which expressly define a smart contract as an "event-driven computer program," and in the proposed UNIDROIT Model Provisions on Smart Contracts, whose development has been discussed within the UNIDROIT Working Group on Digital Assets and Private Law [17].

Notably, MiCA [2] does not directly answer the question of the civil-law characterization of a smart contract. It focuses on the public-law regulation of crypto-asset issuers and crypto-asset service providers (CASPs), leaving the civil-law characterization of the underlying technological instrument to the national law of the Member States. This creates a risk of substantial fragmentation in the civil-law regulation of smart contracts within the European Union itself, notwithstanding the harmonization of the public-law regime applicable to issuers and service providers.

Based on a comparison of the three approaches, this study reaches a conclusion similar to that previously substantiated in Russian doctrine in relation to NFTs: as a general rule, a smart contract does not replace a civil-law contract but serves as a technological instrument for its performance [3], [4], [7]. This does not preclude the recognition of a smart contract as an independent form of transaction in specifically regulated cases, such as in Malta and certain US states. Existing legislation provides no universal solution that can be applied uniformly across all three jurisdictions under review, which explains the need for international legal harmonization discussed in Section 6.4 of this article.

Results and Discussion

The principal regulatory instrument is Federal Law No. 259-FZ of 31 July 2020, "On Digital Financial Assets, Digital Currency, and Amendments to Certain Legislative Acts of the Russian Federation." It defines a digital financial asset through an exhaustive list of the rights it may

certify: monetary claims, rights attached to issue-grade securities, and rights to participate in the capital of a non-public joint-stock company. The issuance, recording, and circulation of digital financial assets are permitted exclusively through a licensed information-system operator. This ensures a high degree of oversight by the regulator, the Bank of Russia, but at the same time limits the flexibility and scalability of the relevant instruments. In this model, the smart contract performs solely the technical function of implementing the decision to issue digital financial assets approved by the information-system operator in accordance with statutory requirements [7], [9].

As in the regulation of NFTs, the Uzbek model is characterized by a broad functional definition of a "crypto-asset" that is not tied to an exhaustive list of certified rights and by the delegation of a substantial portion of regulatory authority to the National Agency for Perspective Projects. A special regime for stablecoins and tokenized securities takes effect in Uzbekistan on 1 January 2026, permitting residents of the Republic of Uzbekistan to issue tokenized securities for placement on licensed exchanges. A defining feature of the Uzbek model is that it permits stablecoins to be used as a means of payment—a solution that currently has no counterpart in either Russian or European Union regulation [15], [16].

Regulation (EU) 2023/1114 on Markets in Crypto-Assets [2], which became applicable in stages during 2024, represents the most detailed digital-asset regulatory framework currently in existence and introduces a three-part classification of crypto-assets: e-money tokens (EMTs), backed by a single fiat currency and essentially treated as electronic money within the meaning of Directive 2009/110/EC [10]; asset-referenced tokens (ARTs), whose value is supported by a basket of assets that may include several currencies, commodities, or other crypto-assets; and "other" crypto-assets—described in MiCA as utility tokens and other crypto-assets not falling within the first two categories—to which a substantial share of NFTs and digital financial assets in the narrow sense may be assigned under certain conditions [18].

Of particular importance to this study is Article 3(1)(6) MiCA [2], [18], which expressly excludes from the Regulation's scope crypto-assets that are "unique and not fungible with other crypto-assets"—that is, classic NFTs in their narrow technological sense. This exclusion is, however, subject to a qualification: the issuance of an NFT as part of a large series or collection may indicate de facto fungibility and therefore trigger the application of MiCA's general regime. In substance, this approach reproduces the dominant-function criterion proposed in the present study for hybrid digital assets.

MiCA establishes a single passporting regime under which a crypto-asset service provider licensed in one Member State may provide the relevant services throughout the European Union without obtaining additional national licenses [2]. This solution differs fundamentally from the fragmented state-by-state regulatory model in the United States and from the centralized but territorially limited models operating in Russia and Uzbekistan. In addition to MiCA, the European Union adopted Regulation (EU) 2022/858 [19] on a pilot regime for market infrastructures based on distributed ledger technology (the DLT Pilot Regime). It permits, on an experimental basis, the trading and settlement of financial instruments, including certain categories of tokenized securities, directly through blockchain infrastructure, subject to exemptions from selected requirements of the existing legislation on markets in financial instruments (MiFID II) and securities settlement and clearing activities (CSDR).

A comparison of the three models reveals the following pattern: whereas the Russian and Uzbek models predominantly rely on an institutional criterion for distinguishing categories of digital assets—the presence or absence of a licensed information-system operator—the European model employs an economic and functional criterion based on the nature of the

token's backing, such as a single currency, a basket of assets, or no backing. This gives MiCA greater flexibility in classifying hybrid and newly emerging instruments, but it also increases enforcement costs because the economic substance of each token must be analyzed rather than merely its formal characteristics [2], [18].

One of the most complex practical issues common to all three jurisdictions under review concerns the consequences of a court declaring invalid a transaction whose performance was implemented wholly or partly through a smart contract. Because a blockchain is immutable, invalidation of the transaction does not automatically restore the parties to their original positions at the technological level. A token or other digital asset transferred under the invalid transaction remains at the acquirer's blockchain address, and restoration of the claimant's rights requires either the respondent's voluntary execution of a reverse transaction or compulsory enforcement of the judgment with the respondent's cooperation, such as disclosure of the private key or initiation of the required transaction.

Russian law provides bilateral restitution as the general consequence of an invalid transaction under Article 167 of the Civil Code of the Russian Federation [11]. However, there is no statutory mechanism for compulsory enforcement of such a judgment in relation to a digital asset without the respondent's cooperation: bailiffs lack the technical means to execute a blockchain transaction independently on behalf of the debtor. Uzbek legislation, which regulates the circulation of crypto-assets predominantly from a public-law perspective, likewise contains no special rules on the compulsory enforcement of restitution claims involving digital assets [15], [16].

In European Union law, the problem is partly mitigated by MiCA's imposition of various operational duties on crypto-asset service providers under Articles 67–68 [2], [20], including a duty to assist competent authorities in the enforcement of judicial decisions concerning assets held under the provider's management through custodial services. This solution is effective only for assets held in custody by a licensed service provider and does not address assets stored in non-custodial, or self-custody, wallets that are controlled entirely by the holder. It therefore fails to resolve the issue for the most technologically "pure" and decentralized form of digital-asset circulation.

This problem is directly connected with the broader question of the extent to which traditional civil-law remedies can apply to relationships mediated by a technology that, by design, recognizes no centralized administrator capable of executing a judgment. Proposed solutions in legal scholarship include the development of a "smart injunction"—a judicial prohibition addressed not to the debtor but directly to the operator of the smart contract or platform and requiring the operator to block further disposition of the disputed asset; the imposition of a duty on smart-contract developers and operators to include emergency functions in the code, such as a kill switch or upgradeability mechanism, allowing a reverse transaction in exceptional circumstances defined by a court order; and, finally, the adoption of a model imposing subsidiary property liability on the relevant platform operator when enforcement of a judgment concerning assets hosted on that platform is impossible.

The Civil Code of the Russian Federation should be supplemented with a special provision—proposed Paragraph 3 of Article 309 [11], [14], supplementing the existing Paragraph 2—expressly establishing a presumption that a smart contract is a method of performing an obligation rather than an independent form of transaction, unless otherwise clearly follows from the substance of the parties' relationship or is established by special legislation. At the same time, the law should impose on information-system operators and digital-financial-asset exchange operators defined by Federal Law No. 259-FZ [9] a duty to provide technical

assistance in enforcing judicial decisions that invalidate transactions involving digital financial assets, including a duty to suspend operations involving the disputed asset while the relevant dispute is pending before the court.

The National Agency for Perspective Projects should be authorized to approve mandatory technical standards for smart contracts used to issue tokenized securities and stablecoins under the special regime taking effect in 2026. These standards should require smart-contract code to include functions ensuring the technical enforceability of judicial decisions, analogous to the emergency-response functions proposed in Section 5. At the same time, the general principles governing the civil-law characterization of smart contracts should be codified at the statutory level rather than in a presidential resolution, thereby reducing the risks of legal instability identified in relation to the Uzbek model for regulating NFTs [15], [16].

Because MiCA [2] deliberately leaves the civil-law characterization of smart contracts to the national laws of the Member States, the European Commission should develop a separate directive rather than a directly applicable regulation, taking into account the continuing differences among Member States' national traditions of contract law. The directive should establish minimum common principles for the civil-law characterization of smart contracts and minimum technical requirements to ensure the enforceability of judicial decisions concerning assets deployed in smart contracts, regardless of whether such assets are held in custodial or non-custodial arrangements. Such a directive would complement the existing regulatory framework—MiCA, the DLT Pilot Regime, and eIDAS 2.0 [2], [12], [19]—by closing the gap identified in Section 3.3 concerning harmonization of the private-law regime for smart contracts.

By analogy with the concept of WIPO model provisions on representative digital assets proposed in earlier studies, this article advances a concept for joint UNIDROIT and UNCITRAL model provisions on smart contracts. These provisions should include a uniform definition of a smart contract and a presumption that it has an auxiliary rather than form-constituting role in relation to the underlying transaction; recommended minimum technical standards ensuring the enforceability of judicial decisions concerning assets deployed in smart contracts; and a recommended conflict-of-laws rule for determining the law applicable to smart-contract relationships involving a foreign element. The proposed rule should be based on party autonomy (lex voluntatis), with subsidiary application of the law of the country with which the relationship is most closely connected. Developing such model provisions within UNIDROIT would be a logical continuation of the organization's work on the 2023 Principles on Digital Assets and Private Law [17], while UNCITRAL's participation would ensure continuity with the successful experience of the Model Law on Electronic Commerce.

Conclusion

The study supports the following principal conclusions. First, none of the three jurisdictions under review has adopted a uniform civil-law characterization of smart contracts. Although the predominant approach treats a smart contract as a technical means of performing an obligation, it may in particular cases be characterized as an independent form of transaction or as a sui generis automated information system requiring special regulation.

Second, the comparative analysis of digital-financial-asset regulation shows that the Russian and Uzbek models primarily use an institutional criterion to distinguish different categories of digital assets, namely the presence of a licensed operator, whereas the European Union's MiCA Regulation uses an economic and functional criterion based on the nature of a token's backing. The latter approach provides greater regulatory flexibility but also entails higher enforcement costs.

Third, all three jurisdictions face a common problem in the compulsory enforcement of restitution claims involving digital assets deployed in smart contracts. The problem arises from blockchain immutability and, in the case of non-custodial storage, the absence of a centralized administrator capable of executing a judicial decision without the asset holder's cooperation.

Fourth, the comparative analysis has produced de lege ferenda proposals for each of the three jurisdictions and a concept for joint UNIDROIT and UNCITRAL model provisions on smart contracts. These measures are intended to promote uniform approaches to the civil-law characterization of smart contracts and establish minimum technical standards ensuring the enforceability of judicial decisions in a cross-border context.

The practical significance of the findings lies in their potential use in legislative activity aimed at improving the regulation of smart contracts and digital financial assets in the Russian Federation and the Republic of Uzbekistan, as well as in further international discussions within UNIDROIT and UNCITRAL. Promising directions for further research include analyzing the liability of smart-contract developers for coding errors that cause property losses to third parties; examining the tax-law aspects of automated performance of obligations; and developing detailed technical standards for the enforceability of judicial decisions involving non-custodial digital assets.

References

[1] N. Szabo, "Smart contracts," 1994. [Online]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. [Accessed: Jul. 20, 2026].
[2] European Parliament and Council of the European Union, "Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets (MiCA)," Official Journal of the European Union, vol. L 150, Jun. 9, 2023.
[3] A. I. Savelyev, "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law," Information & Communications Technology Law, vol. 26, no. 2, pp. 116–134, 2017.
[4] Yu. S. Kharitonova, "Tokenization of art and intellectual property law," Yurist, no. 9, pp. 65–73, 2021.
[5] R. M. Yankovsky, "Cryptocurrencies in Russian law: Surrogates, 'other property,' and digital money," Law. Journal of the Higher School of Economics, no. 4, pp. 43–77, 2020.
[6] L. V. Sannikova and Yu. S. Kharitonova, Digital Assets: A Legal Analysis. Moscow, Russia: 4 Print, 2020.
[7] A. I. Savelyev, "Some risks of tokenization and the circulation of digital financial assets under Russian law," Zakon, no. 6, pp. 36–51, 2021.
[8] N. Szabo, "Formalizing and securing relationships on public networks," First Monday, vol. 2, no. 9, 1997.
[9] Russian Federation, "Federal Law No. 259-FZ of July 31, 2020, 'On Digital Financial Assets, Digital Currency, and Amendments to Certain Legislative Acts of the Russian Federation,'" Collection of Legislation of the Russian Federation, no. 31, pt. 1, art. 5018, 2020.
[10] European Parliament and Council of the European Union, "Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions," Official Journal of the European Union, vol. L 267, Oct. 10, 2009.
[11] Russian Federation, Civil Code of the Russian Federation, Part One, Federal Law No. 51-FZ, Nov. 30, 1994, Collection of Legislation of the Russian Federation, no. 32, art. 3301, as amended.
[12] European Parliament and Council of the European Union, "Regulation (EU) No. 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)," Official Journal of the European Union, vol. L 257, Aug. 28, 2014.
[13] Malta Digital Innovation Authority, Virtual Financial Assets Act, ch. 590, Laws of Malta, 2018.
[14] Russian Federation, "Federal Law No. 212-FZ of July 26, 2019, 'On Amendments to Part One of the Civil Code of the Russian Federation,'" Collection of Legislation of the Russian Federation, no. 30, art. 4028, 2019.
[15] President of the Republic of Uzbekistan, "Resolution No. PP-3832 of July 3, 2018, 'On

Measures for the Development of the Digital Economy,'" National Legislative Database of the Republic of Uzbekistan, no. 09/18/3832/1546, 2018.
[16] Republic of Uzbekistan, "Law No. ZRU-813 of April 3, 2023, 'On the Digital Economy,'" National Legislative Database of the Republic of Uzbekistan, no. 04/23/813/0330, 2023.
[17] International Institute for the Unification of Private Law (UNIDROIT), Principles on Digital Assets and Private Law. Rome, Italy: UNIDROIT, 2023.
[18] European Securities and Markets Authority (ESMA), Guidelines on the Classification of Crypto-Assets as Financial Instruments under MiCA. Paris, France: ESMA, 2024.
[19] European Parliament and Council of the European Union, "Regulation (EU) 2022/858 of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology," Official Journal of the European Union, vol. L 151, Jun. 2, 2022.
[20] European Banking Authority (EBA), Guidelines on the Assessment of Recovery Plans of Issuers of Asset-Referenced Tokens under MiCA. Paris, France: EBA, 2024.