

Цифровые активы между риском и потенциалом

Круглый Никита Игоревич 

Магистрант,

Финансовый университет при Правительстве РФ, г. Москва, Россия

E-mail: nikita.st.sergienko@gmail.com

Горбачева Татьяна Александровна 

канд. экон. наук, доцент,

Финансовый университет при Правительстве РФ, г. Москва, Россия

E-mail: t-gorbacheva@bk.ru

КЛЮЧЕВЫЕ СЛОВА

цифровые активы, правовая неопределенность, KYC/AML, смарт-контракты, киберриски, хранение цифровых активов, трансграничные расчеты, DeFi, цифровые валюты центральных банков

АННОТАЦИЯ

Статья систематизирует барьеры и траектории развития цифровых активов на стыке права, технологий и рынка. На материале нормативных актов, надзорных подходов и практико-ориентированных исследований выполнен аналитический обзор с качественным синтезом; отдельное внимание уделено российскому регулированию и межстрановым различиям в правилах идентификации клиентов и противодействия отмыванию доходов. Показано, что доминирующим ограничением остается правовая неопределенность статусов и режимов налогообложения. Существенные риски сосредоточены в инфраструктуре вне блокчейна (сервисы хранения, биржи, мосты) и в неаудированном коде смарт-контрактов; фрагментация инфраструктуры и ограниченная ликвидность повышают издержки, а расхождения норм осложняют трансграничные расчеты. Вместе с тем цифровые активы способны повысить эффективность и прозрачность расчетов, расширить доступ к финансовым услугам и развить децентрализованное посредничество и цифровые валюты центральных банков. Обоснованы приоритетные меры: гармонизация терминов и требований, стандарты хранения и аудита кода, совместимые форматы супервизорных данных и механизмы возмещения ущерба.

JEL codes: G28, E58, F33

DOI: <https://doi.org/10.52957/2221-3260-2025-12-139-149>

Для цитирования: Круглый, Н.И. Цифровые активы между риском и потенциалом / Н.И. Круглый, Т.А. Горбачева. – Текст : электронный // Теоретическая экономика. – 2025. – №12. – С.139-149. – URL: <http://www.theoreticaleconomy.ru> (Дата публикации: 30.12.2025)

Introduction

The active development of digital technologies, the expansion of the capabilities of distributed ledgers, and the rapid digitalization of financial markets have led to the formation of a new class of economic relations - digital assets. Despite significant scientific and practical interest in this area, the use of digital assets is accompanied by a number of unresolved problems that limit their mass distribution both in Russia and internationally.

The scope of digital assets covers a wide range of issues, from legal uncertainty and cyber threats to weak infrastructure support and limited liquidity. At the same time there is a significant discrepancy between the speed of technological innovation and the pace of adaptation of legislation and financial institutions which creates additional risks for market participants. A separate place is occupied by the issues of international law enforcement practice and cross-border circulation of digital assets, which still remain in the zone of high uncertainty.

Böhme R., Christin N., Edelman B. and Moore T. give review, which systematizes the technology and economics of Bitcoin and blockchain, highlights security risks, infrastructure vulnerabilities, and regulatory uncertainty, thereby capturing the «problem side» [1]. Cambridge Centre for Alternative Finance in their

«Global Cryptoasset Regulatory Landscape Study» demonstrates the cross-country diversity of qualifications and supervision [2]. Firsanova P.P. in research examines in detail the place of the CFA in the legal system of the Russian Federation and related concepts confirms the problem of legal qualification [3].

At the same time, despite the existing restrictions, digital assets open up new prospects for financial systems. Lin William Cong and Zhiguo He in their article shows how smart contracts expand the contract space and reduce validation costs - an argument for transparency and efficiency of markets [4]. Andryushin S.A. argues that a digital ruble can enhance payment system efficiency and inclusion provided its design reconciles monetary policy objectives with privacy and operational resilience [5]. They have the potential to improve the efficiency of settlements, simplify access to investment products, diversify financial instruments and strengthen international economic cooperation. In the context of global digitalization, digital assets are considered as one of the key drivers for the formation of a new financial architecture.

Thus the literature point to a persistent gap: how to reconcile unresolved issues like legal qualification, cyber and operational security, fragmented market infrastructure and limited cross-border harmonization with the clear potential of digital assets to enhance settlement efficiency, market transparency, decentralized financial intermediation, and sustainable finance use cases. This article addresses that gap by synthesizing the main barriers and the realistic development trajectories of digital assets with a focus on their role in transforming payment systems and financial intermediation. We advance two working hypotheses. The first one is that legal ambiguity, security risks, infrastructural immaturity and low financial literacy jointly constrain diffusion. The second one is that where these constraints are actively mitigated digital assets can improve the speed and cost of cross-border transfers, strengthen transparency and supervision, and broaden access to financial services via DeFi and central bank digital currencies (CBDCs).

Methods

This paper is an analytical review with a qualitative synthesis. It draws on secondary sources encompassing legal texts and supervisory materials as well as comparative policy discussions and practice-oriented analyses of infrastructure, custody, payments, and token issuance. Particular attention is paid to the Russian legal framework (including Federal Law No. 259-FZ) and to the heterogeneity of cross-jurisdictional approaches that complicate tax, KYC/AML and enforcement arrangements. Evidence items are coded into problem domains: legal status, security, infrastructure and liquidity and cross-border coordination - and into prospect domains such as settlement efficiency and transparency. This design preserves a clear chain from source description to thematic inference.

Result

The review identifies pervasive legal uncertainty as the dominant structural constraint. In Russia despite partial clarification under Federal Law No. 259-FZ gaps persist regarding the status of various token types, the conditions for cryptocurrency circulation, taxation, and consistent protection of market participants. Internationally assets are alternately treated as e-money, financial instruments, property, or novel intangibles, which raises compliance costs and deters cross-border operations¹.

The security surface remains substantial: practical incidents concentrate around exchanges, custodial services, wallets and unaudited smart contracts with vulnerabilities such as key compromise, re-entrancy, oracle manipulation and protocol exploits undermining user confidence. In many jurisdictions losses are not readily compensable.

Market infrastructure is fragmented with limited market-making, wide spreads, uneven custody standards and insurance coverage, and weak interoperability across platforms. These features depress liquidity and hinder institutional participation.

¹ Federal Law of July 31, 2020 No. 259-FZ «On Digital Financial Assets, Digital Currency, and Amending Certain Legislative Acts of the Russian Federation» // Collection of Legislation of the Russian Federation. 2020. No. 31 (Part I). Art. 5018. URL: <https://www.pravo.gov.ru/novye-postupleniya/federalnyy-zakon-ot-31-07-2020-259-fz-o-tsifrovyykh-finansovykh-aktivakh-tsifrovoy-valyute-i-o-vnesen/> (accessed date 30.10.2025). – Text: electronic.

Cross-border frictions arise from mismatched KYC/AML rules and tax regimes and from the lack of harmonized definitions, leading to legal conflicts, administrative burdens, and risks of double taxation. International bodies acknowledge that insufficient coordination reinforces market fragmentation and slows the emergence of robust settlement and clearing solutions.

Social factors further constrain adoption: low financial literacy regarding digital assets, susceptibility to fraud and phishing and reputational damage from high-profile failures sustain a perception of excessive risk, especially among conservative investors.

Discussion

One of the most significant problems limiting the use of digital assets both in Russia and in the international arena is the lack of legal elaboration of their status. Digital assets remain the subject of discussions regarding their legal nature, which creates serious risks for both investors and issuers [6].

The analysis shows that the current legislative practice in Russia is limited and is aimed mainly at regulating certain types of digital assets not covering the entire ecosystem of their application [7]. This significantly reduces the attractiveness of Russian jurisdictions for investors and initiators of projects in the field of digital technologies. At the international level there are also serious discrepancies in the interpretation of digital assets. In different countries they can be classified as electronic money, financial instruments, property or a new form of intangible assets [8]. This complicates the cross-border circulation of digital assets, complicates compliance procedures and increases the cost of meeting the requirements of various regulators.

In international practice, the term «digital assets» is used as a generic concept for any value objects in electronic form. According to the IMF and FSB definition, a digital asset is «a digital representation of value or contractual rights that can be used to pay or invest»². The European Central Bank notes that a digital asset can be «anything that exists in a binary (electronic) format and assumes the right to use» for example, electronic files, crypto assets or even digital counterparts of the central bank currency³. Thus, digital assets include a wide range of objects from tokenized securities and digital rights to any virtual forms of value.

Crypto assets in international practice are considered as a private subclass of digital assets with special technical characteristics. FSB (Financial Stability Board) defines crypto assets as «private digital assets that depend primarily on cryptography and distributed ledger technology (DLT)». Similarly, the IMF-FSB joint definition indicates that crypto assets are digital private sector assets based on cryptography and a distributed registry⁴. The ECB emphasizes that crypto assets are those digital assets that users exchange on a peer-to-peer network without trusted intermediaries and which are implemented using blockchain technologies⁵. In particular, crypto assets include decentralized cryptocurrencies (such as Bitcoin) and various tokens issued on DLT platforms. They are not a central bank obligation and are usually characterized by high volatility and lack of legal tender status. The European Commission also defines crypto assets as «a type of digital asset that depends predominantly on cryptography and DLT and is private in nature» emphasizing their difference from public money⁶.

2 IMF-FSB Synthesis Paper: Policies for Crypto-Assets // Financial Stability Board. – 2023. – URL: <https://www.fsb.org/uploads/R070923-1.pdf#:~:text=Digital%20asset%20A%20digital%20representation,for%20payment%20or%20investment%20purposes> (accessed date 30.10.2025). – Text: electronic.

3 Cryptocurrencies and tokens // ECB FXCG update. – 2018. – URL: https://www.ecb.europa.eu/paym/groups/pdf/fxcg/2018/20180906/Item_2a_-_Cryptocurrencies_and_tokens.pdf#:~:text=Digital%20asset%20Anything%20that%20exists,assets%20and (accessed date 30.10.2025). – Text: electronic.

4 IMF-FSB Synthesis Paper: Policies for Crypto-Assets // Financial Stability Board. – 2023. – URL: <https://www.fsb.org/uploads/R070923-1.pdf#:~:text=Digital%20asset%20A%20digital%20representation,for%20payment%20or%20investment%20purposes> (accessed date 30.10.2025). – Text: electronic.

5 Cryptocurrencies and tokens // ECB FXCG update. – 2018. – URL: https://www.ecb.europa.eu/paym/groups/pdf/fxcg/2018/20180906/Item_2a_-_Cryptocurrencies_and_tokens.pdf#:~:text=Digital%20asset%20Anything%20that%20exists,assets%20and (accessed date 30.10.2025). – Text: electronic.

6 Digital finance: Emerging risks in crypto-assets – Regulatory and supervisory challenges in the area of financial services, institutions and markets // European Parliamentary Research Service. – 2022. – URL: <https://www.europarl.europa.eu/RegData/>

In contrast, the term digital currency in international literature most often refers to digital forms of sovereign money (i.e. central bank digital currency, CBDC), not private cryptocurrencies. A BIS summary notes that unlike bank-issued e-money, a CBDC would be a direct liability of the central bank with no credit risk⁷. The U.S. Federal Reserve similarly defines a CBDC as «a digital liability of a central bank that is widely available to the general public» and calls it the safest digital asset (with no credit or liquidity risk)⁸. For example, the Bank of England explains that a proposed «digital pound» would simply be a digital form of cash – «a banknote for the digital era» – issued by the Bank of England and backed by the government⁹. Unlike cryptocurrencies (which are privately issued), such a central-bank digital currency would have legal tender status. In the euro area, the ECB likewise describes the digital euro as «a digital form of cash» granting users access to central bank money in digital form, free to use and universally accepted across the currency area¹⁰. So, «digital currency» typically means a state-issued digital equivalent of fiat money (a CBDC), not an independent cryptocurrency.

In summary, international practice distinguishes between three related concepts:

- Digital assets. A broad category covering any valuable electronic objects. They are «digital representation of value or contractual rights» usable for payment or investment^{fsb.org}, and include everything from tokenized securities to digital documents and currency analogues.
- Crypto-assets. A subset of digital assets. These are private-sector assets on blockchain (DLT) that rely on cryptography. They are typically exchanged peer-to-peer without intermediaries and include cryptocurrencies (Bitcoin, etc.) and other tokens. Crypto-assets are not issued by central banks and usually are volatile with no legal-tender status.
- Central bank digital currency. A digital form of fiat currency issued and guaranteed by a government. These are central bank liabilities (e.g. a digital euro or digital pound) with full legal-tender. They represent digital cash for the public, distinct from private crypto-assets.

Each of these categories appears in documents of international financial authorities and central banks, reflecting their different legal and economic characteristics.

Russian law 259-FZ specifically identifies three legal categories of digital assets, each with its own economic purpose. Digital financial assets (DFA) are investment instruments. DFA certify property rights (equity, monetary claims, debt or equity rights). Economically, the DFA is closer to shares or bonds: their issue is regulated by the Bank of Russia, transactions on them are carried out through licensed sites. Digital financial assets can be used to attract investment and pricing¹¹.

Digital currency in 259-FZ it is defined separately and is an asset that does not have an issuer and performs the functions (or an attempt to functions) of a means of payment. The law emphasizes that digital currency is not money by analogy with a ruble (currency), but in fact property or «raw materials for settlements». Economically, cryptocurrency is seen as a commodity or financial asset rather than a legal means of payment.

etudes/STUD/2020/654177/EPRS_STU(2020)654177_EN.pdf#:~:text=the%20definition%20of%20crypto,primarily%20on%20cryptography%20and%20DLT

7 Central bank digital currencies – Executive Summary // Financial Stability Institute. BIS. – 2023. – URL: <https://www.bis.org/fsi/fsisummaries/cbdcs.pdf> (accessed date 30.10.2025). – Text: electronic.

8 Central Bank Digital Currency (CBDC) // Federal Reserve System. – 2024. – URL: <https://www.federalreserve.gov/central-bank-digital-currency.htm#:~:text=CBDC%20is%20generally%20defined%20as,associated%20credit%20or%20liquidity%20risk> (accessed date 30.10.2025). – Text: electronic.

9 The digital pound // Bank of England URL: <https://www.bankofengland.co.uk/the-digital-pound#:~:text=A%20digital%20pound%20would%20be,them%20in%20shops%20or%20online> (accessed date 30.10.2025). – Text: electronic.

10 Digital euro // European Central Bank. URL: https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html#:~:text=In%20a%20world%20where%20digital,form%2C%20complementing%20banknotes%20and%20coins (accessed date 30.10.2025). – Text: electronic.

11 Federal Law No. 259-FZ of 08.08.2019 (as amended on 08.08.2024) «On Attracting Investments using Investment Platforms and on Amendments to Certain Legislative Acts of the Russian Federation» URL: https://www.consultant.ru/document/cons_doc_LAW_330652/ (accessed date 30.10.2025). – Text: electronic.

Therefore, its use for payment is practically prohibited¹².

Utilitarian digital rights - digital vouchers for real products or services. Such rights arise only on special investment platforms and are not securities or monetary obligations. They give a guaranteed requirement for the issuer (to receive a product or service), but do not have an independent monetary value as bonds. Utilitarian rights are needed to legally sell certificates of future goods or services (usually in the early stages of a project) without attracting credit funds¹³.

Thus, Federal Law No. 259-FZ clearly distinguishes between the digital equivalent of financial instruments, digital currency (cryptocurrency without an issuer) and utilitarian rights (digital commodity vouchers). DFAs are regulated as a security, digital currency is effectively prohibited as a means of settlement (see below), and utilitarian rights are used for alternative settlements on investment platforms.

The lack of unified approaches gives rise to a whole range of problems:

- dilution of the legal status of digital assets in cross-border transactions;
- difficulties with the recognition of transactions with digital assets in international courts;
- growth of legal risks for all market participants.

In addition as technology advances, new types of digital assets are emerging in particular smart contract based tokens, non-fungible tokens (NFTs), assets in the metaverse for which there are no clear legal regimes [9]. This creates additional uncertainties both for the regulation of property issues and for the protection of investor's rights.

The significant legal uncertainty of digital assets creates a favorable environment for the emergence of legal risks. However even in the context of formal regulation the use of digital assets remains fraught with serious threats of a different nature. One of the key problems that significantly limits their widespread adoption is the risks of security and cyberattacks.

The security of digital assets is one of the central factors of trust in them by users and institutional investors. Despite the technological security of blockchain networks at the basic level the practical use of digital assets is fraught with a number of serious threats.

One of the most common problems is related to the vulnerability of the infrastructure elements of the digital asset ecosystem - cryptocurrency exchanges, custodial services, and digital wallets. Studies note that exchange hacks, leaks of private keys, and attacks on smart contracts remain among the main sources of financial losses in the industry [9]. 51% attacks, code exploits, and the exploitation of vulnerabilities in protocols lead to the erosion of investor confidence and the loss of market capitalization [10].

A particular problem is the security of smart contracts which are often developed without a full-fledged audit. Errors in the contract code allow attackers to carry out attacks that lead to the theft of user funds or disruption of platforms [8]. In this context vulnerabilities related to reentrancy attacks and manipulation of data oracles are particularly dangerous.

Among the attacks on blockchain services, there are several key categories of vulnerabilities. First, key compromise and custodial risks when an attacker gains a private key or control over a wallet. Such an attack accounts for the overwhelming share of losses: according to Halborn, in 2024, hacked accounts provided more than 80% of the stolen funds¹⁴. Often attacks on centralized services or phishing lead to key leakage, which is the bulk of the damage. Secondly, the vulnerabilities of smart contracts. This includes errors in the logic of contracts: reentrancy (double-spend via re-call), errors in access checks, insufficient data validation, overflows, etc. Access Control vulnerabilities and logical errors accounted for more than \$953 millions and \$638 millions losses, respectively, while reentrancy accounted for \$35,7 millions¹⁵. In addition, attacks through flash loans

¹² In the same place

¹³ In the same place

¹⁴ 2024 Blockchain Security in Review: Key Lessons Learned // Halborn. – 2024. – URL: <https://www.halborn.com/blog/post/2024-blockchain-security-in-review-key-lessons-learned> (accessed date 30.10.2025). – Text: electronic.

¹⁵ OWASP Smart Contract Top 10 // OWASP. – 2025. – URL: <https://owasp.org/www-project-smart-contract-top-10/#:~:text=,149%20documented%20incidents%20in%202024> (accessed date 30.10.2025). – Text: electronic.

and other «hype» mechanisms are still occurring, although their share is decreasing. Hacken's analysis shows that in 2024, Access Control vulnerabilities caused approximately 75% of all attacks¹⁶.

The third group is the manipulation of oracles and data outside the chain. Oracles provide external prices or data, and substituting them can lead to embezzlement. The cost of losses from attacks on oracles is estimated at \$8,8 millions (although in fact large cases of oracle hacking sometimes cost much more)¹⁷. In addition, this includes more general «operations on smart contracts», such as incorrect transaction processing or vulnerabilities in cross-chain bridges.

When comparing with the published incident statistics, the following can be seen: most major thefts are related either to key compromise (hacking wallets, exchanges, phishing), or to errors in smart contracts. By 2024, the vast majority of losses are related to compromised accounts, whereas the vulnerabilities of smart contracts (reentrancy, logic) give a much smaller share of losses¹⁸. Statistics show that access violations and key leaks remain the most common vectors, while complex cases such as oracle manipulation are less common, but can lead to large losses.

In addition to technical threats social engineering methods are actively used in the field of digital assets, such as phishing, fraudulent ICOs, and hacking user accounts. These threats illustrate the complex nature of the risks, encompassing both technical and behavioral aspects [11].

A separate problem is the lack of effective mechanisms in a number of jurisdictions to protect the rights of holders of digital assets in the event of cyber incidents [6]. Unlike traditional financial systems, the losses of users of digital assets are often not compensable, which increases their vulnerability to cyber threats.

Global practice shows that only a comprehensive approach that combines the development of protection technologies, legal regulation, and improving digital literacy can reduce the level of cyber risks in the field of digital assets. The world's leading jurisdictions, such as the European Union and Singapore, are already developing standards for ensuring the security of crypto infrastructure, but there are no unified principles at the global level [7].

The security threats discussed above underscore how vulnerable the technological side of the digital asset market is. However even with reliable protection and regulation the full development of digital assets is impossible without a stable market infrastructure.

The digital asset market is still relatively fragmented and poorly structured. The low liquidity of most tokens makes it difficult to use them as a full-fledged investment instrument and limits the ability of market participants to make transactions quickly and efficiently. The lack of a sufficient number of market makers leads to an increase in spreads between buy and sell prices, which, in turn, reduces the attractiveness of transactions with digital assets [12].

An additional problem is the weakness of infrastructure solutions. Despite the growth in the number of exchanges, payment platforms, and custodial services the level of their reliability and standardization remains insufficient. The poor quality of digital asset custody services and the lack of comprehensive insurance mechanisms increase risks for investors and hinder institutional adoption.

In addition most platforms and services operate in limited ecosystems which hinders the formation of a connected global infrastructure. The lack of cross-platform interoperability limits the ability of users to transfer assets between different blockchain networks and hinders the development of secondary markets¹⁹.

Liquidity is also affected by the insufficient number of tools for assessing the risks and value of digital assets. Unlike traditional financial instruments, digital assets are rarely backed by transparent reporting,

16 The Hacken 2024 Web3 Security Report // Hacken. – 2025. – URL: <https://hacken.io/insights/2024-security-report/> (accessed date 30.10.2025). – Text: electronic.

17 OWASP Smart Contract Top 10 // OWASP. – 2025. – URL: <https://owasp.org/www-project-smart-contract-top-10/#:~:text=,149%20documented%20incidents%20in%202024> (accessed date 30.10.2025). – Text: electronic.

18 The Hacken 2024 Web3 Security Report // Hacken. – 2025. – URL: <https://hacken.io/insights/2024-security-report/> (accessed date 30.10.2025). – Text: electronic.

19 The crypto ecosystem: key elements and risks // BIS report. – 2023. – URL: <https://www.bis.org/publ/othp72.pdf> (accessed date 30.10.2025). – Text: electronic.

which makes them less predictable and increases investment uncertainty.

Problems of liquidity and infrastructure maturity of digital assets significantly limit their use in national markets. However, for digital assets, which by their very nature go beyond the boundaries of national jurisdictions, the issues of international recognition and cross-border circulation are of particular importance. The lack of agreed standards in this area remains one of the main challenges of the globalization of the digital asset market.

The liquidity of crypto assets is highly dependent on their type. In highly liquid markets (bitcoin, ether, large stablecoins), spreads are minimal, while in small-cap altcoins they are much wider. So, according to analysts, bitcoin on large exchanges is traded with a very narrow average spread (about 0,02%), Ethereum - about 0,025%. Large stablecoins (USDT, USDC, etc.) hold even narrower spreads (less than 0,01%) due to high transaction volume. At the same time, in low-liquid altcoins (medium and small capitalization), the spread is often 5-10 times wider - about 0,1-0,3%. Similarly, defi-tokens (management or utilitarian protocol tokens) typically have medium-order spreads (0,05%) because their liquidity is spread across multiple pools²⁰.

Below is an illustrative table (table 1) with typical spreads and liquidity indicators by token class (estimates are based on industry research from 2024-2025).

Table 1 – Typical spreads and liquidity indicators by token class in 2024-2025²¹

Token Class	Examples	Average spread (bid-ask)	Liquidity characteristics
Major Cryptocurrencies	BTC, ETH	0,02–0,03 %	Very high – large trading volume (billions of dollars per day)
Stablecoins	USDT, USDC	<0,01 %	High – pegged to the dollar, actively used in the exchange
Altcoins (mid/low-cap)	SOL, ADA, etc.	0,1–0,3 %	Low – significantly lower volume, the spread is noticeably wider
DeFi tokens	UNI, AAVE, CRV etc.	0,05 %	Average – liquidity depends on pools, the spread is moderate

One of the key difficulties hindering the full development of digital assets is the lack of a unified approach to their legal status in different jurisdictions. In different countries, digital assets can be treated as currencies, goods, financial instruments, or remain outside the legal field altogether. This heterogeneity of qualifications leads to legal conflicts and increases cross-border risks for users and companies.

A separate problem is the mismatch between customer identification (KYC) and anti-money laundering (AML) requirements²². For example, the European Union has introduced strict regulations for crypto-asset operators (MiCA, TFR), while in a number of countries in Asia and Latin America, such norms are still absent or are only being formed²³. This creates unequal conditions for market participants and may become an obstacle to the development of international digital asset exchange platforms.

Cross-border transactions with digital assets also face tax difficulties. Since there is no universal agreement on the taxation of crypto assets, participants have to take into account the requirements of several

20 Elad B., Kinder K., *Crypto market liquidity statistics 2025: market capitalization, trading values, and more* // CoinLaw. – 2025. – URL: <https://coinlaw.io/crypto-market-liquidity-statistics/#:~:text=%2A%20The%20average%20bid,liquidity%20periods> (accessed date 30.10.2025). – Text: electronic.

21 Compiled by the authors on the basis of *Crypto market liquidity statistics 2025: market capitalization, trading values, and more* // CoinLaw. – 2025. – URL: <https://coinlaw.io/crypto-market-liquidity-statistics/#:~:text=%2A%20The%20average%20bid,liquidity%20periods> (accessed date 30.10.2025). – Text: electronic.

22 Targeted Update on Implementation of the FATF Standards on VA and VASPs. FATF. – URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html> (accessed date 30.10.2025). – Text: electronic.

23 European Commission. *Proposal for a Regulation on Markets in Crypto-assets (MiCA)*. – 2023. – URL: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745716/EPRS_ATA\(2023\)745716_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745716/EPRS_ATA(2023)745716_EN.pdf) (accessed date 30.10.2025). – Text: electronic.

jurisdictions at once, which increases administrative costs and creates the risk of double taxation²⁴.

According to the Bank for International Settlements insufficient coordination between regulators in different countries leads to increased fragmentation of the digital asset market and hinders the development of global settlement and clearing solutions²⁵. This limits the potential of digital assets in international trade, investment, and cross-border transfers.

Currently, within the framework of international organizations (FATF, BIS, IMF, OECD), active work is underway to harmonize the standards for regulating crypto assets. However, the transition from recommendations to the actual application of uniform norms requires time and political will.

The problems of international recognition and cross-border circulation of digital assets emphasize the presence of institutional barriers to their development. However, even with a legal framework and technical infrastructure in place, the successful distribution of digital assets is not possible without a high level of trust from users and investors. The most important social factor hindering the development of the market remains the lack of awareness and wary attitude of the general audience to digital assets²⁶.

Despite the growing popularity of digital assets in recent years, the level of understanding of their nature, benefits, and risks among a wide range of users remains relatively low. According to research, in most countries, the level of financial literacy in matters of crypto assets is significantly inferior to knowledge about traditional financial instruments.

Lack of awareness manifests itself in the following aspects:

- lack of understanding of the technical features of digital assets (blockchain, smart contracts, tokenization);
- lack of skills in secure storage and management of crypto assets;
- underestimating the risks of volatility, cyber threats and legal uncertainty.

These factors contribute to the spread of erroneous expectations, participation in fraudulent schemes and, as a result, a loss of confidence in the industry as a whole.

In addition, the perception of digital assets is largely formed under the influence of negative information events, such as cases of embezzlement of funds, bankruptcies of crypto exchanges, and the participation of cryptocurrencies in illegal activities. This creates a stable image of digital assets as extremely risky and unreliable instruments, especially in the eyes of conservative investors.

A separate problem is the lack of involvement of professional market participants — investment consultants, financial analysts, insurance companies — in the promotion and support of transactions with digital assets. The lack of qualified support reduces the confidence of potential investors and increases barriers to their wider adoption.

To overcome these limitations, it is necessary to develop financial literacy programs, actively inform the population about the opportunities and risks of digital assets, as well as form institutions for professional support of users. International experience shows that only a combination of technological development and educational initiatives can contribute to the formation of a mature and sustainable digital asset market²⁷.

The analysis of the problems of using digital assets made it possible to identify the key barriers that impede their widespread distribution and effective integration into the financial system. However, despite the existing limitations, digital assets have significant potential to transform global financial markets. Their unique properties open up new opportunities for the economy related to improving the efficiency of

24 OECD. *Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues*. – Paris: OECD Publishing. – 2020. – 100 p. (accessed date 30.10.2025). – Text: electronic.

25 BIS Annual Economic Report 2023. Chapter III: *The future monetary system*. BIS. – 2023. – URL: <https://www.bis.org/publ/arpdf/ar2023e.pdf> (accessed date 30.10.2025). – Text: electronic.

26 *Digital asset custody deciphered. A Primer to Navigating the Challenges of Safeguarding Digital Assets*. GDF, ISSA and Deloitte report. – 2023. – URL: https://issanet.org/content/uploads/2023/10/Custody-Report_07.10.2023.pdf (accessed date 30.10.2025). – Text: electronic.

27 *Global Financial Stability Report: Navigating Crypto Risks*. International Monetary Fund. – 2023. – URL: <https://www.imf.org/en/Publications/GFSR> (accessed date 30.10.2025). – Text: electronic.

settlements, expanding investment opportunities, increasing transparency and forming sustainable financial ecosystems. In this regard, it seems necessary to move on to considering the prospects for the use of digital assets.

Conclusions

Digital assets sit at the intersection of significant constraints and equally significant opportunities. The evidence consolidates three overarching conclusions. First, the heterogeneity of legal treatment across jurisdictions illustrated domestically by partial frameworks and globally by uneven KYC/AML and tax regimes remains the dominant brake on scale. Second, the practical risk surface is concentrated in off-chain infrastructure and unaudited code which means that credible custody, insurance, and software-assurance standards are prerequisites for institutional adoption. Third, once these foundations are laid, the efficiency and transparency dividends in cross-border settlements, regulatory reporting and tokenized capital-market operations can be material, with DeFi and CBDCs serving as complementary, not competing, paths for innovation. Future work should prioritize interoperable cross-border regimes and supervisory data standards, rigorous contract-security baselines and redress mechanisms, and continued integration of energy efficient and quantum resilient designs so that digital assets can realize their potential as a sustainable and effective element of global financial architecture.

СПИСОК ЛИТЕРАТУРЫ

1. Böhme R., Christin N., Edelman B., Moore T. Bitcoin: Economics, Technology, and Governance // Journal of Economic Perspectives. – 2015. – Vol. 29 (2). – P. 213–38.
2. Blandin A., Cloots A.S., Hussain H. and et. Global cryptoasset regulatory landscape study // Cambridge Centre for Alternative Finance. – 2019. – 120p. URL: <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf>
3. Firsanova P.P. The concept of digital financial assets in Russian legislation and legal doctrine // Education and Law. – 2024. – №. 4. – P. 508-514
4. Lin William Cong, Zhiguo He Blockchain disruption and smart contracts // The review of Financial Studies. – 2019. – Vol. 32. – Issue 5 – P. 1754-1797
5. Andryushin S.A. The central bank's digital currency as the third form of government money. // Actual Problems of Economics and Law. – 2021. – №15(1) – P. 54-76
6. Makarov M.Yu., Bobrov A.G. Prospects for the use of digital financial assets in the Russian Federation // Economics and Management. – 2023. – № 26 (6). – P. 653-661.
7. Muradyan S.D. Digital Assets: Legal Regulation and Estimation of Risk // Journal of Digital Technologies and Law. – 2023. – № 1 (1). – P. 123-151
8. Stankevich M. V. Opportunities and Limitations of the Use of Digital Assets in the World Economy // Journal of Financial Innovation. – 2024. – T. 10, No 1. – P. 78–92.
9. Sysoev E.V., Mukhambetalieva O.R. Problems of Implementation and Prospects For Development of Digital Financial Assets in Russia // Fundamental Research. – 2024. – № 3. – P. 48-52
10. Yang Fang, Cathy Yi-Hsuan Chen, Chunxia Jiang A flight-to-safety from Bitcoin to stock markets: Evidence from cyber attacks // International Review of Financial Analysis. – 2025. – Vol.103. – 104093. – URL: <https://www.sciencedirect.com/science/article/pii/S1057521925001802>
11. Doerr S., Gambacorta L., Leach T., Legros B., Whyte D. Cyber risk in central banking // BIS Working Papers. – 2022. – № 1039. – URL: <https://www.bis.org/publ/work1039.pdf>
12. Angerer M., Gramlich M., Hanke M. Order book liquidity on Crypto Exchanges // Journal of Risk and Financial Management. – 2025. – №18 (3). – Article 124. URL: <https://www.mdpi.com/1911-8074/18/3/124>

Digital assets between risk and potential

Krugly Nikita Igoravich

Master student,

Financial University under the Government of the Russian Federation, Moscow, Russia

E-mail: nikita.st.sergienko@gmail.com

Gorbacheva Tatiana Gorbacheva

candidate of economic science, associate professor

Financial University under the Government of the Russian Federation, Moscow, Russia

E-mail: t-gorbacheva@bk.ru

KEYWORDS

digital assets, legal
uncertainty, KYC/AML,
smart contracts, cyber
risks, digital asset storage,
cross-border settlements,
DeFi, central bank digital
currencies

ABSTRACT

The article systematizes the barriers and development trajectories of digital assets at the intersection of law, technology and markets. Drawing on statutes, supervisory materials and practice-oriented studies, it presents an analytical review with qualitative synthesis; special attention is paid to the Russian regulatory framework and cross-country differences in know-your-customer and anti-money-laundering rules. Legal ambiguity over status and taxation remains the dominant constraint. Material risks are concentrated in off-chain infrastructure (custody services, exchanges, bridges) and in unaudited smart-contract code; fragmented infrastructure and limited liquidity raise costs, while regulatory divergence hampers cross-border settlements. At the same time, digital assets can enhance settlement efficiency and transparency, broaden access to financial services, and foster decentralized intermediation and central-bank digital currencies. The paper outlines priorities: harmonized terminology and requirements, robust custody and code-audit standards, interoperable supervisory data formats, and effective loss-recovery mechanisms.
