Navigating the Legal Landscape: A Comparative Analysis of Digital Asset Regulation across Global Jurisdictions

Submitted: 14 July 2025
Reviewed: 11 September 2025
Revised: 2 March 2026
Accepted: 3 March 2026

Article submitted to peer blind review
Licensed under a Creative Commons Attribution 4.0 International

Assem Zhaksylykbayeva*
https://orcid.org/0000-0003-2646-456X
Saule Suleimenova**
https://orcid.org/0000-0002-6754-9255

DOI: https://doi.org/10.26512/lstr.v18i2.58975

Abstract

[Purpose] The study analysed the legal frameworks governing digital assets in different jurisdictions. The experience of Kazakhstan, Poland, the USA, Uzbekistan, Kyrgyzstan, Singapore, China and South Korea was addressed.

[Methodology/approach/design] The study employed a comparative legal analysis methodology, examining regulatory documents. The investigation methodically examined critical regulatory elements across nations, encompassing licensing, taxation, investor protection, and the prevention of financial crime. Legal papers and court rulings were classified and encoded based on established criteria to facilitate systematic cross-jurisdictional comparisons. Significant focus was placed on the examination of the Kazakh regulatory framework, which integrates an innovative methodology for cryptocurrency mining with conventional financial rules, alongside the Polish experience in executing European directives while accounting for country particularities.

[Findings] The study revealed significant differences between Asian and European approaches to regulation, with Central Asian countries showing a tendency to develop a domestic regulatory model that accounts for regional specifics. The results showed significant differences in approaches to licensing, taxation and investor protection between developed and emerging markets. Three dominant regulatory models were identified: the US securities-based approach, the Asian approach with a focus on payment systems, and the European integrated approach. Key differences were observed in the requirements for the safekeeping of digital assets and investor protection measures. The study concluded a need to strengthen international regulatory coordination and develop harmonised standards, especially between the European Union, Central Asia and developed Asian financial

*Master, Doctoral Student at the Department of Jurisprudence and International Law, Turan University, 050013, 16A Satpayev Str., Almaty, Republic of Kazakhstan. Email: assemzhaksylykbayeva@gmail.com.

**Full Doctor, Head of the Department of Civil Law, Civil Procedure and Labor Law, Al-Farabi Kazakh National University, 050040, 71 Al-Farabi Ave., Almaty, Republic of Kazakhstan. Email: s_suleimenova@outlook.com.

centres. An important aspect of the study was the identification of the need to create a unified methodology for assessing the effectiveness of regulatory regimes, which would allow for a more accurate comparative analysis of different jurisdictions. Particular attention was devoted to the analysis of the impact of technological innovations on the development of regulatory approaches, in the context of the introduction of distributed registry systems and smart contracts. The study also highlighted the importance of establishing mechanisms to respond quickly to new challenges in the regulation of digital assets, including cybersecurity and personal data protection.
[Practical implications] The findings offer regulators actionable insights for aligning national digital asset frameworks with global standards while accounting for local market specifics, enhancing investor protection and regulatory effectiveness.
[Originality/value] This study provides a novel comparative analysis of eight jurisdictions, offering valuable guidance for policymakers and scholars on harmonising digital asset regulation globally.

Keywords: Cryptocurrency. Blockchain. Legislation. Verification. Law Enforcement.

INTRODUCTION

The development of digital technologies and the growth of the crypto asset market created new challenges for regulatory systems around the world. Of relevance is the issue of establishing an effective legal framework for the regulation of digital assets that can strike a balance between innovative development and investor protection. The need to create adequate regulatory mechanisms is becoming increasingly urgent given the rapid growth of the market and the emergence of new forms of digital assets.

The problem of legal regulation of digital assets attracts considerable attention from researchers. P. Maume (2023) analysed the main models of cryptoasset regulation, identifying three dominant approaches: American, European, and Asian. The author examined the specifics of regulation in different jurisdictions, emphasising the need to adapt traditional supervisory mechanisms to the specifics of digital assets. A. Ferreira and P. Sandner (2021) conducted a comparative analysis of regulatory regimes and their effectiveness. C. Wendehorst (2023) considered the issue of conflict of laws in the context of digital asset regulation, and J. Lee and R. Li (2023) focused on the problems of regulating decentralised autonomous organisations (DAOs).

The researchers pay special attention to investor protection and financial security. R.M. Garcia-Teruel and H. Simón-Moreno (2021) analysed the problems of tokenisation of property rights and their legal protection. S. Kethineni and Y. Cao (2020) analysed the link between the development of cryptocurrencies and financial crime, emphasising the need to strengthen anti-money laundering (AML) mechanisms. P. Yeoh (2017) explored regulatory issues in the context of

blockchain technology development, while W. Zuo (2021) focused on analysing the new financial architecture in the digital age.

Studies of judicial practice have made a significant contribution to understanding the legal nature of digital assets. D. Fox and S. Green (2023) analysed the impact of court decisions on the formation of regulatory approaches, especially in terms of determining the legal status of cryptoassets. J. Woxholth et al. (2024) explored the problems of competing claims to crypto assets, emphasising the need to develop dispute resolution mechanisms. M. Lehmann (2023) examined the issue of ownership of crypto-assets, and F. Schär (2021) analysed the development of decentralised finance (DeFi) and its impact on traditional financial systems.

In the context of regional development, O. Ali et al. (2021) studied the peculiarities of blockchain technology implementation in different jurisdictions, J.M. Garrido (2023) analysed the legal nature of digital tokens, and T. Frunzeti and A. Dumitru (2023) considered the evolution of digital asset regulation in the European Union. A. Blandin et al. (2020) presented a comprehensive analysis of the global regulatory landscape of crypto assets.

However, despite a significant amount of research, the issue of comparative analysis of regulatory approaches in the context of different legal systems and levels of economic development remains insufficiently studied. This is especially true for the experience of Central Asian countries, particularly Kazakhstan, which has created a unique regulatory model through the Astana International Financial Centre (AIFC) (2023), combining elements of English law with local regulatory practices. Similarly, the experience of Eastern European countries, especially Poland, which demonstrates an innovative approach to the implementation of European standards for the regulation of digital assets while maintaining national specifics, requires a deeper study. The mechanisms of interaction between different legal systems in the context of regulating cross-border transactions with digital assets, especially between common law and continental law jurisdictions, remain insufficiently studied. An important aspect that requires further study is the integration of national regulatory regimes with international standards, in particular the recommendations of the Financial Action Task Force (FATF) and the principles of Markets in Crypto-Assets (MiCA) Regulation. Particular attention should be paid to studying the mechanisms for adapting global standards to local conditions and the specifics of different legal systems, as well as analysing the effectiveness of different regulatory models in the context of protecting investors' rights and ensuring financial stability.

The study aims to conduct a comprehensive comparative analysis of regulatory approaches to digital assets in different jurisdictions to identify the

most effective regulatory mechanisms and develop recommendations for their harmonisation. The following tasks were set to achieve this goal:

1. Analyse existing models of digital asset regulation in leading financial centres.
2. Study the specifics of approaches to investor protection and financial security.
3. Assess the impact of technological innovations on the evolution of regulatory mechanisms.
4. Develop recommendations for harmonisation of regulatory approaches at the international level.

MATERIALS AND METHODS

The study was conducted in 2020-2024 and was based on a comprehensive analysis of regulatory documents, court decisions and legislative acts of various jurisdictions in the field of digital asset regulation. The methodological basis of the study includes comparative legal, systemic, and formal legal methods of analysis, complemented by a structured framework for cross-jurisdictional comparison.

The empirical basis of the study was formed by legal acts and documents: Law of the Republic of Kazakhstan No. 193-VII "On Digital Assets in the Republic of Kazakhstan" (2023), reports of the AIFC (2023), MiCA Regulation of the European Parliament (HALLAK, 2023), Payment Services Act 2019 of Singapore (Monetary Authority of Singapore, 2019), Monetary Authority of Singapore (2024) reports, annual reports of the Polish Financial Supervision Authority (FSA) (2023), circulars and reports of the People's Bank of China (PBoC) (2021) on the digital yuan. Jurisdictions were selected to reflect leading financial centres and distinct regulatory models, including Kazakhstan, the European Union (Poland), the United States, China, Singapore, and South Korea.

The following court cases were used in the study. SEC v. Ripple Labs Inc. (2020) No. 1:20-cv-10832, where the court considered the classification of the XRP cryptocurrency as a security, which set an important precedent for the regulation of cryptoassets in the United States. In B2C2 Ltd v Quoine Pte Ltd (2019) Singapore High Court (SGHC) (I) 3, the Singapore court recognised cryptocurrencies as a form of property subject to legal protection, setting an important precedent for Asian jurisdictions. The case of AA v Persons Unknown & Ors, Re Bitcoin (2019) England and Wales High Court, case number 3556 (EWHC 3556) set important precedents regarding the legal status of crypto assets in the UK jurisdiction, and the case of Ruscoe and Moore v Cryptopia Limited (2020) New Zealand High Court, case number 728 (NZHC 728) (PEMBROKE-BIRSS and SINCLAIR, 2020) set a precedent regarding the ownership of crypto

assets in the bankruptcy of cryptocurrency exchanges. An important methodological aspect was the study of Vorotyntseva v Money-4 Limited t/a Nebeus.com & Ors (2018) EWHC 2596 (Ch); and ByBit Fintech Limited v Ho Kai Xin (2023) SGHC 199. These cases were systematically coded according to legal issues, such as classification of digital assets, fiduciary duties, ownership disputes, and freezing of assets, allowing structured cross-jurisdictional comparison.

The analysis included three main stages: (1) collection and systematisation of regulations and court decisions, with coding based on predefined criteria for licensing, taxation, investor protection, and financial crime prevention; (2) systematic comparative analysis of regulatory approaches across jurisdictions using these categories; (3) summarisation of results with recommendations for regulatory harmonisation and best practices.

This approach ensured that comparisons were structured, transparent, and reproducible, addressing gaps in previous studies that lacked methodological clarity regarding cross-jurisdictional comparisons.

RESULTS

Legal regulation model: Transformation of regulatory approaches and institutional mechanisms in the field of digital financial instruments

The notion of digital assets is understood differently in academic and professional contexts. These assets typically include digital resources, information, or intellectual property that may be managed, exchanged, or monetised via digital channels. The notion underscores both the rights linked to these assets and their prospective economic or functional worth in digital contexts.

The University College London (UCL) Centre for Blockchain Technologies (2022) proposes a more blockchain-centric approach, defining digital assets as data recorded on a blockchain that confer specific rights, such as ownership, access, representation, voting, or practical use. Simultaneously, it is essential to acknowledge that the conventional concept of property as essentially "objects" has been criticised for its rigidity and inadequacy in encompassing the comprehensive nature of contemporary ownership arrangements.

Digital assets fundamentally consist of digital entities, including data, content, and related rights, all of which are maintained in a unique and recognisable form (SASI & SWARNA JYOTHI, 2019; AZIEVA et al., 2021). Technologies such as blockchain facilitate this transparency by allowing for the transfer, use, and ownership of assets. The changing dynamics of property rights associated with digital assets reflect society values and objectives in the digital age.

The scope of digital assets is quite broad and covers a diverse range of digital content and rights (Law Commission…, 2023), including cryptocurrencies, non-fungible tokens (NFTs), digital tokens, social media accounts, algorithms, cloud accounts and other forms of digital intellectual property. However, for the purposes of academic discussion, the focus is usually narrowed to a class of assets known as cryptoassets (ALLEN, 2023).

The development of digital financial instruments has created the need to develop new regulatory approaches and institutional mechanisms for their regulation (ZHIYENGALIYEVA et al., 2024; NIYAZBEKOVA et al., 2023). Particularly noteworthy is the experience of the Republic of Kazakhstan, which has implemented an innovative regulatory model through the AIFC (2023). According to the AIFC, since its establishment in 2018, the centre has attracted more than 1,500 companies from 65 countries operating in the field of digital assets. The legal framework of the AIFC, based on the principles of English common law, provides flexibility in regulating various types of digital assets, including both secured (tokenised securities, commodity tokens, stablecoins) and unsecured (utility tokens, cryptocurrencies) digital assets. The peculiarity of Kazakhstan's approach is the creation of a comprehensive regulated environment for cryptocurrency mining, as evidenced by the adoption of the Law of the Republic of Kazakhstan No. 193-VII "On Digital Assets in the Republic of Kazakhstan" (2023), which establishes clear licensing requirements and tax regimes for mining companies.

The Polish experience of regulating digital assets demonstrates an integrative approach within the framework of European legislation. The Polish FSA (2023) is actively adapting national legislation to the requirements of the MiCA, creating a unified regulatory system for all types of digital assets. According to the FSA, as of 2023, more than 100 licensed digital asset service providers were registered in Poland. An important aspect of Polish regulation is the implementation of strict AML) and consumer protection requirements.

An analysis of case law demonstrates the evolution of legal approaches to the regulation of digital assets. The case of B2C2 Ltd v Quoine Pte Ltd (2019) SGHC(I) 3, where the Singapore court recognised cryptocurrencies as a form of property subject to legal protection, is illustrative. This decision has influenced the development of case law in other jurisdictions, including Central Asian countries. In the case of AA v Persons Unknown & Ors, Re Bitcoin (2019) EWHC 3556, the English court also confirmed the status of cryptocurrencies as property that can be subject to judicial protection.

The development of central bank digital currencies (CBDC) deserves special attention. The National Bank of Kazakhstan has been actively developing a digital tenge, conducting pilot tests since 2021. The project envisages a two-tier

distribution model and integration with the existing payment infrastructure. Similar projects are being implemented in China (digital yuan) and South Korea (digital won), demonstrating different approaches to CBDC architecture and implementation mechanisms.

An important aspect of the development of digital asset regulation is the experience of Singapore, which has created a comprehensive regulatory system through the Payment Services Act 2019. According to the Monetary Authority of Singapore (2019), this approach has created a transparent ecosystem for the development of digital assets while maintaining high standards of investor protection and financial stability. As of 2023, more than 300 companies have been licensed to provide digital asset services in Singapore (Monetary Authority of Singapore, 2024).

The Chinese approach demonstrates a more centralised regulatory model. Following the ban on cryptocurrency transactions in 2021, China has focused on the development of the digital yuan (e-CNY), creating a state-controlled digital payment ecosystem. According to the PBoC (2021), by the end of 2023, more than 200 million users in 11 regions of the country had participated in the e-CNY pilot project.

South Korea developed a hybrid regulatory model that combines elements of strict control and innovative development. The Financial Services Commission (FSC) of Korea has implemented a licensing system for cryptocurrency exchanges, requiring mandatory cooperation with local banks to ensure compliance with AML/Countering the Financing of Terrorism (CFT) requirements. This approach allowed for the creation of a regulated market, with 5 fully licensed cryptocurrency exchanges operating by the end of 2023. In the context of the development of stablecoins, the experience of regulating USDT and other stablecoins deserves special attention. According to the European Securities and Markets Authority (ESMA), the trading volume of stablecoins in the EU exceeded EUR 500 billion in 2023, which highlights the need for a specialised regulatory framework for this asset class (HALLAK, 2023).

In various jurisdictions, cryptocurrencies are the subject of litigation that is shaping the current regulation of digital assets. The following are key court cases that highlight the different approaches to cryptocurrency regulation in the US, EU, Japan and China. In December 2020, the US Securities and Exchange Commission (SEC) filed a lawsuit against Ripple Labs Inc. accusing the company of illegally selling XRP tokens without registering securities, which is a violation of US law (SEC v. Ripple Labs… 2020). According to the SEC, XRP is a security and therefore its offer and sale should be subject to regulatory oversight. This decision had significant consequences for Ripple Labs, as it led to lengthy litigation and financial losses. In August 2024, the court found that institutional

sales of XRP did indeed fall within the definition of securities and ordered the company to pay a 125 million USD fine. This decision was an important precedent that highlighted the importance of digital assets being subject to securities laws. At the same time, it sparked a wave of discussions on the need to more clearly define the status of various digital assets.

In 2015, the Court of Justice of the European Union considered whether the exchange of cryptocurrencies is subject to Value-Added Tax (VAT) regulation. The Swedish tax office ruled that the exchange of traditional currencies for bitcoins is exempt from VAT. The Court concluded that bitcoin is not a real item but operates as a medium of trade akin to traditional currency. This ruling was a crucial advancement in the formulation of cryptocurrency law inside the European Union, acknowledging these transactions as exempt from VAT and setting a precedent for regulatory approaches throughout Europe.

One of the most illustrative cases of cryptocurrency regulation is related to the bankruptcy of the Japanese exchange Mt. Gox in 2014, which at that time processed about 70% of the global bitcoin transactions (PHAM, 2019). Following the disappearance of approximately USD 450 million worth of assets, investors filed lawsuits against the exchange and its CEO Mark Karpeles. In 2019, Karpeles was found guilty of falsifying financial records, which highlighted the importance of transparency and regulatory oversight of cryptocurrency exchanges. Following this incident, Japan revised its regulation, introducing strict licensing requirements for cryptocurrency exchanges and strengthening rules to protect users. This decision underscored the need for stricter control over cryptocurrency exchanges in the country and contributed to the improvement of legislation in the field of digital assets.

In 2017, the PBoC (2021) imposed strict restrictions on the cryptocurrency market, banning initial coin offerings (ICOs) and ordering local exchanges to cease operations. The decision was warranted as a means to safeguard investors and alleviate financial risks associated with cryptocurrency. Chinese courts endorsed this strategy, establishing a legal foundation for the shutdown of bitcoin platforms. This action reflected a cautious stance on digital currencies and highlighted the government's willingness to maintain strict control over the sector, even as other countries pursued more liberal approaches to cryptocurrency markets.

An analysis of the court practice of various jurisdictions reveals a tendency to recognise cryptocurrencies as a specific type of property. In the case of Ruscoe and Moore v Cryptopia Limited (2020) NZHC 728 (PEMBROKE-BIRSS and SINCLAIR, 2020), the New Zealand court set an important precedent regarding the ownership of crypto assets in the bankruptcy of cryptocurrency exchanges. Similarly, in ByBit Fintech Limited v Ho Kai Xin (2023) SGHC 199, the

Singapore court expanded the understanding of fiduciary duties concerning digital assets.

Regulatory approaches to digital assets in different jurisdictions show considerable variation in both legal status and institutional structure. Particularly noteworthy is the experience of Kazakhstan, where a comprehensive digital asset regulation system has been created through the AIFC, including a special regime for mining and an innovative regulatory sandbox, while the Polish experience demonstrates the successful integration of national legislation with the European MiCA, creating a balanced regulatory system. The institutional structure of regulation, as shown in Table 1, ranges from a single regulator (like Monetary Authority of Singapore (MAS) in Singapore) to a complex multi-tiered system (such as the US with the SEC, Commodity Futures Trading Commission (CFTC) and FinCEN), with Central Asian countries showing a tendency to form specialised regulatory bodies, although at different stages of development of their regulatory infrastructure.

Criteria	Kazakhstan	Poland	USA	China	Central Asia (Uzbekistan, Kyrgyzstan)	Singapore	South Korea	EU
Legal status	AIFC: a digital asset as an object of law. The Law on Digital Assets 2021	A financial instrument under the law on trade. Regulation through MiCA	SEC: security Commodity Exchange: Commodity	Prohibition of cryptocurrencies. CBDC: e-CNY	Uzbekistan: licensed activities Kyrgyzstan: unregulated asset	PSA 2019: the regulated payment token	Virtual Asset Business Act	MiCA: unified regulation
Institutional structure	The AIFC is the main regulator. The National Bank is the CBDC. Ministry of Digital Development	FSA is the main regulator. Ministry of Finance – taxes	SEC, CFTC, FinCEN	PBoC	Central banks. Special commissions	MAS is a single regulator	FSC, crypto exchanges	ESMA, national regulators
Adjustment features	Mining: special mode. Crypto exchanges: sandbox of AIFC	Integration with MiCA. An innovative sandbox	Federal/state level. BitLicence (NY)	Centralized CBDC. Blockchain services	Pilot projects. Regional cooperation	DPT licensing. Innovation hub	Banking partnership. VASP licences	Uniform standards. Passport system
Tax regime	Mining: 1-10%. Trade: corporate tax	Standard EU rates. VAT on services	Capital gains tax	Not available for crypto	Preferential regimes in free economic zones	GST on services	20% for profit	A harmonised approach

Table 1 – Comparative analysis of regulatory approaches to digital assets in global jurisdictions (Kazakhstan, Poland, China, Central Asia, Singapore, South Korea, EU)

Note: DPT – Digital Payment Token, PSA – Payment Services Act.

Source: compiled by the authors based on P. Maume (2023), A. Ferreira and P. Sandner (2021), E. Florea and E.S. Pustelnik (2021), A. Blandin et al. (2020), I. Hallak (2023), AIFC (2023).

The analysis of tax regimes shows significant differences in approaches: from the complete absence of crypto-asset regulation in China to the detailed taxation system in the EU and South Korea, with a special experience of

Kazakhstan, which has implemented a differentiated approach to taxation of mining (1-10%) and general trade in digital assets. Regulatory features show different approaches to ensuring control and market development: from strict centralisation in China to a liberal model in Singapore, while the European approach, represented both in the Polish experience and in the pan-European MiCA regulation, demonstrates the desire to strike a balance between innovation and security, which creates the basis for the formation of global standards for the regulation of digital assets.

Systematic analysis of the mechanisms for protecting and ensuring financial security: Standardisation of requirements and unification of verification procedures

The development of the digital asset market has created the need for comprehensive mechanisms to protect investors and ensure financial security. The key elements of such a system are the standardisation of regulatory requirements and the unification of verification procedures for market participants. The main problem remains the lack of uniform international standards, which leads to regulatory arbitrage and increased risks for investors. At the same time, different jurisdictions demonstrate their approaches to addressing these challenges, forming unique models of market participant protection.

An analysis of global practices shows different approaches to investor protection. In Singapore, which is one of the leading financial centres in Asia, the Monetary Authority of Singapore (2019) has implemented a multi-level protection system that includes mandatory licensing, capital requirements, and insurance of customer assets. According to a report of S. Kethineni and Y. Cao (2020), this approach has significantly reduced the number of fraud cases in the digital asset market compared to previous years. Singapore's regulatory model is considered one of the most balanced, as it combines strict security requirements with support for innovation in digital finance. The peculiarity of this approach is the emphasis on preventive measures and continuous monitoring of market risks.

The European Union has established common standards of investor protection for all member states through the MiCA regulation. The key elements are requirements for transparency of transactions, disclosure of information, and safeguarding of client assets. According to estimates of T. Frunzeti and A. Dumitru (2023), the implementation of these standards has covered a significant part of the European digital asset market. The European approach is characterised by its comprehensiveness and systematic nature, which allows for the creation of a single regulatory space for all market participants. An important aspect is also the establishment of clear rules on the liability of service providers and mechanisms for compensating investors.

Particular attention should be devoted to user verification and AML procedures. As noted by P. Maume (2023), travel rule standards require the exchange of information about transaction participants between digital asset service providers, which has significantly increased the effectiveness of combating financial crime. These requirements include mandatory customer identification, transaction monitoring and suspicious transaction reporting. The implementation of such standards helps to create a transparent and secure ecosystem for all market participants while ensuring the necessary level of confidentiality of personal data.

In the context of technical security, there is a tendency to implement more and more sophisticated security systems. Leading digital asset exchanges are implementing multi-factor authentication and cold storage of assets. A study (YEOH, 2017) shows that the use of cold wallets significantly reduces the risk of asset loss compared to hot storage. In addition, new security technologies are being developed, such as hardware security modules (HSMs), multi-signatures, and smart contracts with additional security mechanisms. Regular security audits and system stress testing are also relevant.

Monitoring and early warning systems are becoming increasingly sophisticated and effective (PETRAKOV et al., 2019; SMAILOV et al., 2023). According to A. Ferreira and P. Sandner (2021), automated monitoring systems are highly effective in detecting suspicious transactions, which significantly increases the level of market security. These systems use advanced data analytics and machine learning technologies to identify abnormal behavioural patterns and potential threats. International cooperation and information exchange between regulators from different countries is also an important element, which allows for more effective counteraction to cross-border financial crimes.

Regulatory oversight of cybersecurity and operational resilience is constantly evolving. According to E. Florea and E.S. Pustelnik (2021), service providers with digital assets that comply with established security requirements demonstrate significantly lower vulnerability to cyberattacks. This includes not only technical aspects of protection but also organisational measures, staff training and the development of incident response plans. Special attention is paid to ensuring business continuity and protecting critical infrastructure.

An analysis of regulatory requirements and protection mechanisms in different jurisdictions reveals significant differences in approaches to ensuring the security of the digital asset market. Table 2.

Defence mechanisms	Kazakhstan	Poland	USA	China	Central Asia	Singapore	South Korea	EU
KYC/AML requirements	AIFC standards. International standards	MiCA + national requirements	BSA/AML requirements. FinCEN regulations	Strict controls for e-CNY	Basic requirements	Strict MAS standards	Real identification	Unified MiCA standards

Investor protection	English law in the AIFC. Compensation mechanisms	Guarantee funds. MiCA protection	SIPC. SEC requirements	State guarantees for e-CNY	Limited protection	Compulsory insurance	ISMS certification	Comprehensive protection
Operational security	International standards for AIFC participants	European cybersecurity standards	Federal guidelines	State standards	Basic requirements	AIFC standards	ISMS standards	NIS2 Directive
Licence requirements	AIFC: capital, audit, reporting	FSA: MiCA requirements	SEC/CFTC/states	Prohibition of crypto services	Simplified mode	DPT licence of MAS	FSC licence + bank	CASP licence

Table 2 – Comparative analysis of regulatory requirements and remedies by jurisdiction

Note: KYC – Know Your Customer, BSA – Bank Secrecy Act, SIPC – Securities Investor Protection Corporation, CASP – Crypto-Asset Service Provider, NIS2 – Directive on Security of Network and Information Systems (NIS Directive 2), ISMS – Information Security Management System.
Source: compiled by the authors based on S. Kethineni and Y. Cao (2020), P. Yeoh (2017), A. Ferreira and P. Sandner (2021), A. Blandin et al. (2020), M. Lehmann (2023).

Singapore and the EU demonstrate the most advanced protection systems, with comprehensive investor protection mechanisms and strict operational safety standards. Kazakhstan, through the AIFC, has implemented a regulatory system based on English law with clear capital and audit requirements, while Poland has successfully integrated national protection mechanisms with MiCA requirements. South Korea's approach is particularly noteworthy, with its unique banking partnership system and ISMS certification providing an additional layer of security for market participants. The US demonstrates a multi-level protection system with a division of powers between federal and state regulators, while China has focused on strict controls for its CBDC while generally banning cryptocurrency services. Central Asian countries, although they have basic security requirements, show a tendency to gradually strengthen regulatory mechanisms and approach international investor protection standards.

An important aspect of investor protection is the development of digital asset insurance mechanisms (JOSEPH et al., 2025; MURTEZAJ et al., 2024). Leading jurisdictions are introducing mandatory insurance requirements for customer funds held on cryptocurrency exchanges and with other service providers. This approach provides an additional level of protection against operational risks and cyberattacks. Of particular interest is the experience of implementing decentralised insurance protocols that use smart contracts to automate insurance claims processes.

The development of cross-chain technologies creates new challenges for investor protection systems. Interaction between different blockchain platforms requires the development of special security protocols and transaction verification mechanisms (BAIMUHAMEDOV et al., 2019; BARLYBAYEV et al., 2024). Regulators are working to create security standards for bridges between different blockchains, considering the vulnerabilities that arise during interconnection.

Particular attention is being paid to auditing smart contracts and ensuring the security of liquidity protocols.

An important trend is the introduction of biometric technologies in digital asset user verification systems. The use of biometric data for authentication helps to increase security and simplify customer identification procedures (SMAILOV et al., 2025; BARLYBAYEV & TURGINBAYEVA, 2025). At the same time, regulators ensure the protection of biometric data and the compliance of verification systems with the requirements of personal data protection legislation.

The issue of consumer protection in the use of decentralised financial protocols remains relevant. Unlike traditional financial services, where there are clear consumer protection mechanisms in place, such mechanisms are only being developed in the DeFi sector. Regulators are working on adapting existing consumer protection rules to the specifics of decentralised systems, including information disclosure, dispute resolution and compensation.

Innovative technologies and regulatory adaptation: Evolution of regulatory frameworks in the context of blockchain ecosystems development

The development of blockchain technologies and their implementation in the financial system creates the need for constant adaptation of regulatory mechanisms. It is especially necessary to analyse the evolution of the regulatory framework in the context of the emergence of new technological solutions and business models in the field of digital assets. The emergence of DeFi has become a significant challenge for regulators. According to F. Schär (2021), the amount of blocked value in DeFi protocols has exceeded USD 100 billion, which has created the need to develop new approaches to regulating automated financial systems.

The introduction of smart contracts has created a new dimension of legal regulation. The automated fulfilment of contractual obligations requires a review of traditional legal concepts and the development of new dispute-resolution mechanisms. Regulators in different jurisdictions are developing approaches to recognising the legal effect of smart contracts and establishing the framework for their use. The emergence of new forms of digital assets, such as NFTs and tokenised real assets, has necessitated the adaptation of existing regulatory frameworks.

In response to technological innovations, regulators are introducing new supervisory tools, including regulatory technology (RegTech) and supervisory technology (SupTech). According to estimates of W. Zuo (2021), the use of artificial intelligence and data analytics technologies can increase the efficiency of regulatory oversight and reduce compliance costs.

An important aspect of regulatory adaptation is the development of interstate cooperation in the regulation of new technologies. In the context of the development of CBDCs, regulators face the need to create new legal frameworks. As demonstrated by the Chinese experience with the electronic renminbi (e-CNY) and the development of the digital tenge in Kazakhstan, the introduction of CBDCs requires a comprehensive review of monetary legislation and payment systems.

The development of AML and countering the financing of terrorism (AML/CFT) systems requires significant attention. The introduction of new technologies for transaction analysis and information exchange can increase the effectiveness of these measures in the field of digital assets. A special role is played by the FATF, an international organisation that sets global standards in this area.

The integration of distributed ledgers technology (DLT) into traditional financial systems creates new challenges for regulators. The need to ensure the compatibility of different technology platforms requires the development of common standards and interaction protocols. Particular attention is devoted to the scalability and energy efficiency of blockchain solutions.

The development of DAOs is setting a new legal precedent in the field of corporate governance. Regulators are faced with the need to determine the legal status of such organisations and develop mechanisms to protect the rights of their members. This requires a rethinking of traditional corporate law concepts and the development of new regulatory models.

The development of the market for tokenised securities (Security Token Offering – STO) creates the need to adopt traditional securities legislation. Regulators are creating a regulatory framework that would ensure an adequate level of investor protection while preserving the benefits of blockchain technologies in the issuance and circulation of securities. Particular attention is devoted to information disclosure and transparency of operations.

The introduction of interbank payment systems based on DLT (Real-Time Gross Settlement – RTGS) opens new opportunities for modernising the financial infrastructure. Central banks in different countries are actively exploring the potential of these technologies to improve the efficiency and security of payment systems. Projects in this area require the development of special security protocols and operational resilience standards.

The issue of personal data protection in the context of the development of DLT requires special attention from regulators. The implementation of the General Data Protection Regulation (GDPR) in blockchain systems poses technical and legal challenges, especially concerning the implementation of the "right to be forgotten" and ensuring the confidentiality of transactions. Regulators

are working to strike a balance between the transparency of blockchain systems and the protection of user privacy.

The development of Blockchain Interoperability creates new challenges for regulators in standardisation and security. The need to ensure the secure exchange of assets between different blockchain platforms requires the development of common security protocols and standards. Another important aspect is to ensure the technical compatibility of different systems while maintaining their autonomy and security.

The issue of the environmental impact of blockchain technologies, especially in the context of the Proof of Work (PoW) consensus mechanism, is becoming increasingly relevant to regulators. The transition to more energy-efficient consensus mechanisms, such as Proof of Stake, requires the development of appropriate regulatory incentives and energy efficiency standards.

The development of the stablecoin market and its integration into the traditional financial system necessitates the development of special regulatory requirements. Particular attention is devoted to ensuring the stability of such assets, transparency of reserves and protection of users' rights. Regulators are seeking to create a framework that would ensure financial stability while preserving the innovative potential of these instruments.

DISCUSSION

The analysis of regulatory approaches to digital assets in different jurisdictions has revealed three dominant regulatory models: American, European and Asian. This observation aligns with the findings of V.A. Kumar et al. (2024), who also identified these models, but additionally highlighted the emergence of hybrid approaches in developing jurisdictions. Particularly important is the authors' conclusion that hybrid models are often more effective, as they allow for local specifics to be addressed while maintaining compliance with international standards. The regulatory practice in Kazakhstan and Poland confirms this thesis, demonstrating the successful combination of international standards with national regulatory features.

The established trend towards the creation of specialised regulatory regimes for digital assets, which is especially noticeable in the case of the AIFC in Kazakhstan, confirms the conclusions of M. Hashemi (2024) about the need to adapt traditional regulatory mechanisms to the specifics of digital assets. However, contrary to the author's assumptions about the prevalence of prohibitive measures, practice shows a tendency to form a constructive regulatory framework. The experience of the Central Asian countries refutes the thesis that severe restrictions are inevitable in developing regions, demonstrating the possibility of creating innovative regulatory regimes. An important factor in success is not so

much the level of economic development as the willingness of regulators to implement flexible supervision and control mechanisms.

The results of the study reveal the impact of regulatory sandboxes on the development of innovation in the field of digital assets. J. Butt (2023) previously noted the effectiveness of this approach, but new data from the experience of the AIFC and the Polish FSA demonstrate the even greater potential of this tool for balancing innovation and risk. Practice shows that regulatory sandboxes not only foster innovation but also allow regulators to better understand the risks of new technologies and develop more effective control mechanisms. The role of sandboxes in testing new investor protection and financial crime mechanisms appears to be particularly important. This finding extends the role of experimental regulatory regimes presented in previous studies. Moreover, the incorporation of Decentralised Identity (DID) technologies into KYC/AML frameworks could substantially bolster regulatory compliance while concurrently enhancing user privacy safeguards. This connection might enhance customer verification procedures, mitigate fraud risk, and bolster confidence in digital asset marketplaces.

An analysis of investor protection and financial security mechanisms has revealed significant differences between developed markets and emerging jurisdictions. The identified differences in approaches to investor protection correlate with the conclusions of S.M. Safoeva (2023) regarding the need for a differentiated approach to regulation depending on the level of financial market development. However, contrary to the author's predictions of a long period of convergence of standards, practice shows accelerated harmonisation of requirements, especially in AML and countering the financing of terrorism. This process is particularly noticeable in the implementation of the "travel rule" standards and customer identification requirements. According to L. Lee (2024), such standards are being successfully implemented in developing countries, as demonstrated by the experience of Kazakhstan and other Central Asian countries, showing the possibility of rapid adaptation of international standards in the presence of appropriate political will and technological infrastructure.

An analysis of the technological aspects of regulation, in particular the introduction of CBDCs, shows a more complex picture than was anticipated in the studies. A. Zhuk (2024) found that the success of CBDC implementation depends not so much on technological readiness as on the adaptation of the regulatory infrastructure and coordination between financial market participants. China's experience with the introduction of the digital yuan and pilot projects in other jurisdictions shows that the key success factors are not only technical solutions but also the ability to create an effective ecosystem for the interaction of all market participants.

An important aspect of the study is the analysis of the impact of regulatory requirements on the development of DeFi and other innovative financial instruments. R. de Caria (2018) and D.A. Zetzsche et al. (2020) emphasises the need to create special regulatory regimes for DeFi, which is confirmed by practice, but with important modifications. In particular, the study determined that hybrid approaches that combine elements of traditional financial regulation with innovative mechanisms for supervising decentralised systems are the most effective. Hybrid methodologies, especially when integrated with sophisticated biometric authentication, can enhance user trust and facilitate wider acceptance of digital asset platforms among the general populace (PAVLOVA et al., 2024; SASI et al., 2023). Nevertheless, the burgeoning issues in the DeFi sector, including cyberattacks on smart contracts, governance assaults such as rug pulls, and economic abuses like pricing manipulation, underscore the necessity for improved consumer protection. For example, significant smart contract breaches documented in W. Li et al.'s study have resulted in considerable user losses, while governance attacks analysed by Z. Lin et al. and token price manipulations emphasised by S. Wu et al. have revealed weaknesses in platform governance. To address these difficulties, regulators may enforce specific measures, like obligatory security audits for smart contracts, more stringent transparency and governance mandates for DeFi protocols, and improved oversight of pricing mechanisms. Implementing best practices from conventional financial sectors, such as automated compliance mechanisms and investor education programs, can mitigate consumer risk and enhance market confidence.

The results of the analysis of court practice in various jurisdictions demonstrate the formation of new legal doctrines regarding the status of digital assets. The UNIDROIT (2024) study reveals a progressive trend in the courts' approaches to determining the legal nature of crypto assets. The decisions in the cases of B2C2 Ltd v Quoine Pte Ltd (2019) SGHC(I) 3 and AA v Persons Unknown & Ors, Re Bitcoin (2019) EWHC 3556 have set important precedents recognising digital assets as a special form of property. As L. Lee (2024) noted, judicial practice is beginning to form common approaches to resolving disputes in the field of digital assets, despite differences in the legal systems of different countries.

The analysis of regulatory policy in the field of combating financial crime has revealed a tendency to strengthen international coordination and standardisation of requirements. According to V.A. Kumar et al. (2024), the implementation of international standards, especially FATF requirements, is faster than expected. The experience of implementing the "travel rule" standard in different jurisdictions demonstrates that technological and organisational barriers can be overcome with effective international cooperation.

The study also identified the growing role of technological innovation in shaping regulatory approaches. M. Hashemi (2024) emphasised that effective regulation of digital assets requires a deep understanding of technological aspects and the active implementation of innovative supervisory tools. This is especially evident in the development of transaction monitoring systems and the introduction of automated compliance mechanisms.

The identified trends in the development of licensing requirements and verification mechanisms for digital asset market participants deserve special attention. The research conducted by S.M. Safoeva (2023) confirms the need for a differentiated approach to licensing various types of activities with digital assets. At the same time, practice shows a tendency to unify basic requirements while maintaining the possibility of considering national specifics. The experience of implementing MiCA regulation in the European Union, which creates a unified licensing system while maintaining flexibility for national regulators, is particularly illustrative.

An important result of the study was the identification of the growing role of self-regulation and market mechanisms in ensuring the stability of the digital asset market. According to J. Butt (2023), market participants can form effective risk control and management mechanisms. This is especially evident in the development of decentralised risk management protocols and digital asset insurance systems. The experience of leading cryptocurrency exchanges and other service providers demonstrates that it is possible to create reliable investor protection mechanisms even in the detailed absence of regulation.

An analysis of the development of regulatory sandboxes and innovation hubs has revealed their critical role in shaping effective approaches to regulating new financial technologies. A. Zhuk (2024) demonstrates the even greater potential of this tool for innovation. The experience of the AIFC and other regulatory sandboxes confirms the possibility not only of testing new financial products but also of developing innovative approaches to regulation and supervision. Particular attention is drawn to the methodology of risk assessment in sandboxes, which, according to R. de Caria (2018), allows identifying potential threats in the early stages of innovation. V.A. Kumar et al. (2024) note that the success of regulatory sandboxes depends on the level of interaction between the regulator and market participants, as well as the clarity of the established criteria for evaluating test results. Another important aspect of sandboxes is their role in shaping international regulatory standards, as successful practices are rapidly spreading between jurisdictions through regulatory cooperation mechanisms.

Overall, this study demonstrates that the development of digital asset regulation is more dynamic and comprehensive than anticipated in previous studies. The identified trends indicate the formation of a new paradigm of

financial regulation that combines elements of traditional supervision with innovative approaches to risk management and investor protection. The incorporation of DID solutions and biometric verification technologies further augments this framework by fostering secure, privacy-conscious, and user-centric digital financial services. This creates the basis for the further development of international standards and mechanisms for regulating digital assets. According to L. Lee (2024), this evolution of regulatory approaches reflects the general trend towards harmonisation of international standards while maintaining the flexibility of national regulatory regimes. M. Hashemi (2024) emphasises that the successful implementation of new regulatory mechanisms largely depends on the ability of jurisdictions to adapt international standards to local conditions and market specifics. The balance between ensuring innovative development and maintaining the stability of the financial system becomes especially important, which requires continuous improvement of regulatory instruments and supervisory mechanisms.

CONCLUSIONS

The study of regulatory approaches to digital assets in different jurisdictions has identified key trends, models and effective strategies that promote the development of the digital asset market and ensure its security. The analysis confirmed that the main regulatory models – the US, European and Asian – differ significantly in their approaches to licensing, investor protection and financial security. The European model, represented by the MiCA regulation, is focused on harmonising and unifying regulatory requirements within the EU, in particular concerning investor protection and minimising financial risks. The US model focuses on strict regulation by bodies such as the SEC and CFTC, which provide market oversight to protect investors and combat financial crime. The Asian model is characterised by adaptation to local needs and innovation, such as the integration of digital currencies in Singapore and the launch of pilot projects with the digital yuan in China.

The practical results of the study confirm that hybrid regulatory models that combine international standards with local specifics may prove to be the most effective in ensuring the stability and growth of the digital asset market. The experience of Kazakhstan and Poland shows that the introduction of adaptive regulatory regimes, such as regulatory sandboxes, creates a favourable environment for innovation while minimising the risks associated with money laundering, fraud and other financial crimes. Regulatory sandboxes have proved to be significant for analysing the risks of new financial products, allowing regulators to better understand their potential market impact, prepare appropriate regulations and establish control and supervisory tools.

Furthermore, the incorporation of DID solutions into KYC/AML frameworks can improve regulatory efficacy and user privacy, while advancements in biometric verification bolster user confidence and facilitate wider acceptance of digital asset services.

The findings highlight the importance of adapting regulatory approaches to the unique characteristics of digital assets, as well as the need for international coordination of efforts to combat financial crime. The introduction of the global "travel rule" standard, which obliges providers to transmit customer information in transactions with digital assets, and the tightening of customer identification requirements in different countries indicate the successful harmonisation of approaches to combating money laundering.

At the same time, the study has certain limitations. One of them is the lack of access to classified documents of individual regulators and the heterogeneity of the pace of digital asset adoption in developing countries. In addition, the study limitations were determined by the theoretical coverage of only certain aspects of regulation, while the practical application of the recommendations requires further study of local conditions in different jurisdictions.

To further improve the results of the study, it is advisable to focus on a detailed analysis of the economic impact of digital asset regulation. Attention should be paid to the interaction of CBDCs with DeFi, which could be used to assess their potential impact on the traditional financial system, including banks and non-banks.

Thus, the results of the study demonstrate that the development of digital assets requires balanced regulatory approaches that combine flexibility and adaptation to local conditions with compliance with international standards. Future study may investigate the incorporation of decentralised identity (DID) and biometric verification into hybrid regulatory frameworks, connecting technology advancement with substantial enhancements in investor protection, compliance efficacy, and user uptake. Further research could be aimed at developing and implementing new methods of controlling the digital asset market, including automated transaction monitoring systems and financial crime protection mechanisms, which will ensure investor protection and the stable development of the industry in the context of digital transformation.

REFERENCES

AA v Persons Unknown & Ors, Re Bitcoin. (2019). EWHC 3556 (Comm) – United Kingdom High Court. https://www.bailii.org/ew/cases/EWHC/Comm/2019/3556.html.

ALI, O., JARADAT, A., KULAKLI, A., & ABUHALIMEH, A. (2021). A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities. *IEEE Access*, *9*, 12730-12749. https://doi.org/10.1109/access.2021.3050241.

ALLEN, J. G. (2023). Cryptoassets in Private Law. In I. CHIU, G. DEIPENBROCK (Eds.), *Routledge Handbook of Financial Technology and Law* (pp. 123-145). London: Routledge. https://doi.org/10.4324/9780429325670.

Astana International Financial Centre. (2023). AIFC Legal Advisory Council. https://aifc.kz/ru/aifc-legal-advisory-council/.

AZIEVA, G., KERIMKHULLE, S., TURUSBEKOVA, U., ALIMAGAMBETOVA, A., & NIYAZBEKOVA, S. (2021). Analysis of access to the electricity transmission network using information technologies in some countries. *E3S Web of Conferences, 258*, 11003. https://doi.org/10.1051/e3sconf/202125811003.

B2C2 Ltd v Quoine Pte Ltd. (2019). SGHC(I) 3 – Singapore International Commercial Court. https://www.dlapiperintelligence.com/export/sites/intelligence-old/investmentrules/blog/articles/2019/Downloads/b2c2-ltd-v-quoine-pte-ltd_a1cd5e6e-288e-44ce-b91d-7b273541b86a_8de9f2e2-478e-46aa-b48f-de469e5390e7.pdf.

BAIMUHAMEDOV, M. F., ATANOV, S. K., ZHUNUSOV, K. M., ZHIKEYEV, A. A., BUGUBAEVA, A. U., & BULAEV, A. G. (2019). System of cryptographic protection of information based on deterministic chaos. *International Journal of Innovative Technology and Exploring Engineering, 8*(12), 4495-4498. https://doi.org/10.35940/ijitee.L3527.1081219

BARLYBAYEV, A., & TURGINBAYEVA, A. (2025). Development and Implementation of an Advanced Fuzzy Expert System for the Assessment of Information Security Risks. *Journal of Computational and Cognitive Engineering, 4*(4), 570-580. https://doi.org/10.47852/bonviewJCCE52024683

BARLYBAYEV, A., SHARIPBAY, A., SHAKHMETOVA, G., & ZHUMADILLAYEVA, A. (2024). Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies. *Applied Sciences (Switzerland), 14*(21), 9858. https://doi.org/10.3390/app14219858

BLANDIN, A., CLOOTS, A. S., HUSSAIN, H., RAUCHS, M., SALEUDDIN, R., ALLEN, J. G., CLOUD, K., & ZHANG, B. Z. (2020). *Global*

cryptoasset regulatory landscape study. Cambridge: Cambridge Centre for Alternative Finance.

BUTT, J. (2023). Comparative Analysis of Regulatory Approach and Management Practice for Digital Crypto-Currency and the Role of IFIs in Developing Global Regulations. *Journal of Accounting and Management*, *13*(3), 7-21.

ByBit Fintech Limited v Ho Kai Xin. (2023). SGHC 199 – Singapore High Court. https://www.elitigation.sg/gdviewer/gd/2023_SGHC_199.

DE CARIA, R. (2018). The Legal Meaning of Smart Contracts. *European Review of Private Law*, *26*(6), 731-751. https://doi.org/10.54648/erpl2018052.

FERREIRA, A., & SANDNER, P. (2021). EU Search for Regulatory Answers to Crypto Assets and Their Place in the Financial Markets' Infrastructure. *Computer Law & Security Review*, *43*, 105632. https://doi.org/10.1016/j.clsr.2021.105632.

Financial Supervision Authority. (2023). Report on the Activities of the UKNF and the KNF in 2023. https://www.knf.gov.pl/knf/en/komponenty/img/Report_on_the_activities_of_the_UKNF_and_the_KNF_board_in_2023_92880.pdf.

FLOREA, E., & PUSTELNIK, E. S. (2021). On Regulation of Cryptocurrency: International Experience. *Supremacy of Law*, *1*, 69-83. https://doi.org/10.52388/2345-1971.2021.1.06.

FOX, D., & GREEN, S. (2023). *Cryptocurrencies in public and private law*. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780198855170.001.0001.

FRUNZETI, T., & DUMITRU, A. (2024). Harmonizing Virtual Currency Use in the EU: The Evolution and Impact of MICA Regulation. *Land Forces Academy Review*, *29*(2), 141-148. https://doi.org/10.2478/raft-2024-0015.

GARCIA-TERUEL, R. M., & SIMÓN-MORENO, H. (2021). The Digital Tokenization of Property Rights: A Comparative Perspective. *Computer Law & Security Review*, *41*, 105543. https://doi.org/10.1016/j.clsr.2021.105543.

GARRIDO, J. M. (2023). *Digital tokens: A legal perspective*. International Monetary Fund.

HALLAK, I. (2023). Markets in Crypto-Assets Regulation (MiCA). European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739221.

HASHEMI, M. (2024). To Coordinate or Not to Coordinate: The Governance of Digital Assets in a Global Marketplace. *Ohio Northern University International Law Journal, 2*(1), 2.

International Monetary Fund. (2024). Global Financial Stability Report. https://www.imf.org/en/Publications/GFSR.

JOSEPH, O., DAHAN, E., AVIV, I., HADAR, I., BORDO, E., & PEZO, D. (2025). Requirements Engineering for Integrating Quantum Key Distribution with Blockchain Systems. In *2025 IEEE 33rd International Requirements Engineering Conference Workshops (REW)* (pp. 375-382). Valencia, Spain: Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/REW66121.2025.00055

KETHINENI, S., & CAO, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, *30*(3), 325-344. https://doi.org/10.1177/1057567719827051.

KUMAR, V. A., BHARDWAJ, S., & LATHER, M. (2024). Cybersecurity and Safeguarding Digital Assets: An Analysis of Regulatory Frameworks, Legal Liability and Enforcement Mechanisms. *Productivity*, *65*(1), 1-10. https://doi.org/10.32381/PROD.2024.65.01.1.

Law Commission: Reforming the Law. (2023). *Digital assets: Final report*. London: HH Associates Ltd.

Law of the Republic of Kazakhstan No. 193-VII "On Digital Assets in the Republic of Kazakhstan". (2023). https://adilet.zan.kz/eng/docs/Z2300000193.

LEE, J., & LI, R. (2023). Law and Regulation for Decentralised Autonomous Organisations (DAOs). https://dx.doi.org/10.2139/ssrn.4455052.

LEE, L. (2024). Examining the Legal Status of Digital Assets as Property: A Comparative Analysis of Jurisdictional Approaches. https://dx.doi.org/10.2139/ssrn.4807135.

LEHMANN, M. (2023). Who Owns Bitcoin? Private Law Facing the Blockchain. https://dx.doi.org/10.2139/ssrn.4466136.

MAUME, P. (2023). The Regulation on Markets in Crypto-Assets (MICAR): Landmark Codification, or First Step of Many, or Both? *European Company and Financial Law Review*, *20*(2), 243-275. https://doi.org/10.1515/ecfr-2023-0014.

Monetary Authority of Singapore. (2019). Payment Services Act 2019. https://www.mas.gov.sg/regulation/acts/payment-services-act.

Monetary Authority of Singapore. (2024). Annual Report 2023/2024. https://www.mas.gov.sg/publications/annual-report/2024/annual-report-2023-2024.

MURTEZAJ, I. M., REXHEPI, B. R., DAUTI, B., & XHAFA, H. (2024). Mitigating economic losses and prospects for the development of the energy sector in the Republic of Kosovo. *Economics of Development, 23*(3), 82-92. https://doi.org/10.57111/econ/3.2024.82

NIYAZBEKOVA, S., ZVERKOVA, A., SOKOLINSKAYA, N., & KERIMKHULLE, S. (2023). Features of the «Green» strategies for the development of banks. *E3S Web of Conferences, 402*, 08029. https://doi.org/10.1051/e3sconf/202340208029

PAVLOVA, D., DOVRAMADJIEV, T., DASKALOV, D., MIRCHEV, N., PEEV, I., RADEVA, J., DIMOVA, R., KAVALDZHIEVA, K., MRUGALSKA, B., SZABO, G., & KANDIOGLOU, A. (2024). 3D Design of a Dental Crown with Artificial Intelligence Based in Cloud Space. *Lecture Notes in Networks and Systems, 817*, 437-445. https://doi.org/10.1007/978-981-99-7886-1_37

PEMBROKE-BIRSS, J., & SINCLAIR, M. (2020). Cryptocurrencies are Property Capable of Being Held on Trust, New Zealand High Court Holds. https://www.nortonrosefulbright.com/en/knowledge/publications/d6ea37bd/cryptocurrencies-are-property-capable-of-being-held-on-trust-new-zealand-high-court-holds.

People's Bank of China. (2021). Progress of Research and Development of E-CNY in China. http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf.

PETRAKOV, D. S., SMIRNOV, D. I., GERASIMENKO, N. N., MEDETOV, N. A., & JIKEEV, A. A. (2019). Implementation of software for data processing of X-ray optical measurements for the analysis of structural parameters. *Journal of Applied Crystallography, 52*, 186-192. https://doi.org/10.1107/S1600576718016837

PHAM, S. (2019). Former Mt. Gox Chief Mark Karpeles Acquitted of Most Charges in Major Bitcoin Case. CNN. https://edition.cnn.com/2019/03/14/tech/mark-karpeles-mt-gox/index.html.

SAFOEVA, S. M. (2023). Navigating the Legal Landscape of Digital Objects in Social Media: A Civil Law Perspective. *World Bulletin of Management and Law*, *24*, 52-56.

SASI, S., SUBBU, S.B.V., MANOHARAN, P., & ABUALIGAH, L. (2023). Design and implementation of secured file delivery protocol using enhanced elliptic curve cryptography for class I and class II transactions.

Journal of Autonomous Intelligence, 6(3). https://doi.org/10.32629/jai.v6i3.740

SASI, S., & SWARNA JYOTHI, L. (2019). A novel public key crypto system based on bernstein polynomial on galois fields 2m to secure data on CFDP. *Smart Innovation, Systems and Technologies, 105*, 639-647. https://doi.org/10.1007/978-981-13-1927-3_67

SCHÄR, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*, *103*(2), 153-174. https://doi.org/10.20955/r.103.153-74.

SEC v. Ripple Labs Inc. (2020). No. 1:20-cv-10832 – United States District Court. https://www.nysd.uscourts.gov/sites/default/files/2023-07/SEC%20vs%20Ripple%207-13-23.pdf.

SMAILOV, N., DOSBAYEV, Z., OMAROV, N., SADYKOVA, B., ZHEKAMBAYEVA, M., ZHAMANGARIN, D., & AYAPBERGENOVA, A. (2023). A Novel Deep CNN-RNN Approach for Real-time Impulsive Sound Detection to Detect Dangerous Events. *International Journal of Advanced Computer Science and Applications, 14*(4), 271-280. https://doi.org/10.14569/IJACSA.2023.0140431

SMAILOV, N., KADYROVA, R., ABDULINA, K., URALOVA, F., KUBANOVA, N., & SABIBOLDA, A. (2025). Application of facial recognition technologies for enhancing control in information security systems. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska, 15*(3), 55-58. https://doi.org/10.35784/iapgos.7073

UCL Centre for Blockchain Technologies. (2022). Enterprise Digital Assets Report. https://blockchain.cs.ucl.ac.uk/blockchain-technology/research-papers/enterprise-digital-assets.

UNIDROIT. (2024). *UNIDROIT Principles on Digital Assets and Private Law*. Rome: International Institute for the Unification of Private Law.

Vorotyntseva v Money-4 Limited t/a Nebeus.com & Ors. (2018). EWHC 2596 (Ch) – United Kingdom High Court. https://www.bailii.org/ew/cases/EWHC/Ch/2018/2596.html.

WENDEHORST, C. (2023). Chapter 5 Proprietary Rights in Digital Assets and the Conflict of Laws. In A. BONOMI, M. LEHMANN, Sh. LALANI (Eds.), *Blockchain and Private International Law* (pp. 101-127). Leiden, Boston: Brill, Nijhoff. https://doi.org/10.1163/9789004514850_007.

WOXHOLTH, J., ZETZSCHE, D. A., BUCKLEY, R. P., & ARNER, D. W. (2024). Competing Claims to Crypto-Assets. *Uniform Law Review*, *28*(2), 226-246. https://doi.org/10.1093/ulr/unad018.

YEOH, P. (2017). Regulatory Issues in Blockchain Technology. *Journal of Financial Regulation and Compliance*, *25*(2), 196-208. https://doi.org/10.1108/JFRC-08-2016-0068.

ZETZSCHE, D. A., ARNER, D. W., & BUCKLEY, R. P. (2020). Decentralized Finance. *Journal of Financial Regulation*, *6*(2), 172-203. https://doi.org/10.1093/jfr/fjaa010.

ZHIYENGALIYEVA, A., YERZHAN, B., & ALIYA, S. (2024). Regulation of the provocation of a crime in the criminal legislation of foreign countries: what should Kazakhstan take into account? *Scientific Herald of Uzhhorod University. Series Physics, 55*, 1405-1413. https://doi.org/10.54919/physics/55.2024.140qo5

ZHUK, A. (2024). Navigating the Legal Landscape of AI Copyright: A Comparative Analysis of EU, US, and Chinese Approaches. *AI and Ethics*, *4*(4), 1299-1306. https://doi.org/10.1007/s43681-023-00299-0.

ZUO, W. (2021). The Analysis of Digital Finance and Digital Inclusive Finance. In R. THURASAMY, I. A. MAJID, N. A. B. A. RAHMAN, A. H. ZULKAFLI (Eds.), *Proceedings of the 2021 3rd International Conference on Economic Management and Cultural Industry (ICEMCI 2021)* (pp. 667-670). Amsterdam, Paris: Atlantis Press. https://doi.org/10.2991/assehr.k.211209.352

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET