Legal Aspects of Using Blockchain Technology to Enhance the Security of Electronic Payments and Prevent Online Fraud

Submitted: 10 September 2025
Reviewed: 29 November 2025
Revised: 20 December 2025
Accepted: 25 December 2025

Aibar Kumisbek[*]
https://orcid.org/0009-0007-0924-7068
Bakhytzhan Issakhov[**]
https://orcid.org/0000-0002-5033-9681
Akynkozha Zhanibekov[***]
https://orcid.org/0000-0002-1116-2123
Nurlan Apakhayev[****]
https://orcid.org/0000-0001-7795-2518
Aliya Kassymbek[*****]
https://orcid.org/0000-0001-7169-874X

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v18i2.59666

Abstract

[Purpose] The aim of this study was to analyse the legal regulation of blockchain technologies and cryptocurrencies, as well as to identify existing gaps in legislation with the goal of developing recommendations for their mitigation.

[Methodology/approach/design] The research employed a systematic review of scholarly literature and legal documents, theoretical legal analysis, and comparative analysis of legislative initiatives in various countries, such as Estonia, Singapore, and the United States. A case study of blockchain deployment in electronic payment systems was undertaken, utilising a systems approach to integrate legal, economic, and social perspectives.

[*]Master and a Doctoral Student at the Department of Law, Akhmet Yassawi International Kazakh-Turkish University. Address: 161200, 29 Bekzat Sattarhanov Str., Turkestan, Republic of Kazakhstan. E-mail: a.kumisbek@outlook.com.

[**]Associate Professor at the Department of Law, Central Asian Innovation University. Address:160000, 137 Madeli Kozha Str., Shymkent, Republic of Kazakhstan. E-mail: issakhovbakhytzhan@gmail.com.

[***]Deputy Dean at the Department of Law, Al-Farabi Kazakh National University. Address:050040, 71 Al-Farabi Ave., Almaty, Republic of Kazakhstan. E-mail: a-zhanibekov@hotmail.com.

[****]Professor at the Department of Law, Almaty Economic-Legal and Pedagogical College. Address: 041609, 80a Raiymbek Batyr Str., Besagash, Republic of Kazakhstan. E-mail: lan.apakhayevv@gmail.com.

[*****]Senior Lecturer at the Department of Jurisprudence, Abai Kazakh National Pedagogical University. Address: 050010, 13 Dostyk Ave., Almaty, Republic of Kazakhstan. E-mail: a_kassymbek@outlook.com.

[Findings] The main findings demonstrated that countries like Estonia and Singapore have developed effective legal frameworks that facilitate blockchain adoption and attract international investment. Estonian legislation, which permits the use of smart contracts and electronic payments, significantly streamlines financial transactions, enhancing user trust in such systems. Singapore, in turn, has established clear regulations for cryptocurrency exchanges and initial coin offerings (ICOs), ensuring a secure and predictable environment for investors.
[Practical implications] At the same time, the study identified challenges faced by regulators in different countries. For instance, fragmented legislation in the United States leads to legal uncertainty, complicating the operations of blockchain companies. Different states have their own regulations, imposing additional costs on firms operating across multiple markets. Meanwhile, stringent measures in China aimed at restricting cryptocurrency usage may stifle innovation and lead to talent drain, negatively impacting the market.
[Originality/value] These findings underscore the need for a unified regulatory strategy that considers both local and international aspects. The study concludes that a comprehensive regulatory approach, active collaboration between government bodies and businesses, and further research in this field are key factors in establishing a sustainable blockchain ecosystem that fosters the development of an innovation-driven economy.

Keywords: International cooperation. Decentralised systems. Investment risks. Data protection. Start-ups.

INTRODUCTION

Since 2008, when the first cryptocurrency, Bitcoin, was introduced, blockchain technology has emerged as one of the most discussed and promising tools in financial technology (fintech). Its unique properties, such as decentralisation, security, and transparency, have attracted the attention of both researchers and practitioners seeking to address challenges in electronic payment security and prevent online fraud. The relevance of this topic stems not only from the growing volume of online transactions but also from the increasing sophistication of fraudulent schemes, which inflict significant harm on businesses and consumers alike.

Blockchain, a decentralised digital ledger, records transactions chronologically in blocks interconnected through cryptographic methods (Vazov et al., 2022; Joseph et al., 2025). These blocks are maintained within a peer-to-peer network of nodes that collectively verify transactions, while in many systems, designated participants, known as miners, validate and add new blocks through consensus mechanisms such as Proof-of-Work (Tripathi et al., 2023; Hariyani et al., 2025).

Research in electronic payment security indicates that traditional protection methods often prove insufficient. For example, Adewole et al. (2020) and Mapa et al. (2023) demonstrate that existing authentication and encryption systems are not always capable of preventing identity theft-related attacks and propose blockchain technology as a complementary solution to traditional methods for creating a more secure transaction environment. They argue that a decentralised approach not only enhances data protection but also allows users to control their financial operations without third-party intermediaries.

Similarly, Kumar et al. (2023) emphasise the necessity of adopting innovative solutions such as blockchain to increase trust in financial transactions, asserting that decentralised ledgers can significantly reduce opportunities for fraud. Their research shows that blockchain enables the creation of a transparent and traceable transaction history, which can substantially diminish the likelihood of fraudulent activities.

The analysis of works by Abad-Segura et al. (2021) and Kshetri et al. (2023) further confirms that the implementation of blockchain technologies can significantly enhance transaction security and mitigate fraud risks, as each transaction is recorded in an immutable ledger, thereby complicating attempts at data manipulation. They note that the use of cryptographic methods in blockchain ensures a high level of information protection, which is critically important for the financial sector.

The study by Kapyshev (2024) and Wenhua et al. (2023) emphasises the advantages of blockchain adoption in fintech, highlighting its capacity to improve transparency and reduce transaction processing costs. It is also pertinent to acknowledge the work of Gelar and Naufal (2023), who examine the impact of blockchain technologies on financial systems in developing countries, underscoring that the implementation of such solutions can foster financial inclusion and improve access to financing. Their conclusions are based on an analysis of blockchain use cases in microfinancing and lending, which opens new opportunities for individuals excluded from traditional banking services.

The study by Sanz-Bas et al. (2021) additionally indicates that blockchain can serve as an effective tool in combating money laundering and terrorist financing by providing a greater volume of data for transaction analysis. They also discuss the importance of integrating blockchain with existing monitoring systems to establish a more robust and efficient infrastructure for countering financial crimes. The global nature of online fraud threats necessitates coordinated international action, as evidenced by the findings of Gayathma et al. (2022), who highlight the insufficient integration of technologies within legal frameworks and the need for global standards to protect users.

Despite significant advancements in blockchain, numerous legal and regulatory issues require further examination. For instance, Rejeb et al. (2020) identify gaps in legislation pertaining to cryptocurrencies and smart contracts, which may create legal risks for users, and propose a set of recommendations for improving regulatory frameworks in this domain.

The study by Balagolla et al. (2021) also underscores the importance of establishing clear legal frameworks to protect users from fraudulent activities in the blockchain sphere, noting that the absence of precise regulation may lead to user distrust and hinder technological development. The work of Arif et al. (2024) examines the legal aspects of smart contract implementation, emphasising the necessity of adapting legislation to emerging technologies. Furthermore, the study by Ashfaq et al. (2022) focuses on the legal challenges associated with blockchain-based transactions and proposes mechanisms to facilitate the creation of a secure legal environment for cryptocurrencies and related sectors. The research of Laroiya et al. (2020) and Chowdhury et al. (2023) explores the influence of international legislation on blockchain adoption, stressing the need for global coordination to develop effective counter-fraud measures. The core issue lies in the fact that existing regulatory frameworks often fail to account for the specific characteristics of blockchain, creating uncertainty for businesses and users.

While recent studies have thoroughly examined the technological, economic, and security benefits of blockchain technologies in electronic payment systems, the legal and regulatory dimensions of blockchain adoption remain unevenly explored across different jurisdictions. The existing literature predominantly focuses on individual countries, discrete regulatory instruments, or specific technological applications, offering limited comparative insight into how divergent legal frameworks influence the practical deployment of blockchain in electronic payments. There is a notable absence of systematic cross-jurisdictional analysis that connects regulatory approaches to their effects on payment security and fraud prevention. This study seeks to address this gap by comparatively examining blockchain-related legislative initiatives and regulatory frameworks across multiple jurisdictions, with the aim of identifying common challenges, best practices, and policy directions that foster both innovation and legal certainty.

Thus, existing research demonstrates that the need for legal regulation of blockchain technologies in the context of electronic payments is becoming increasingly urgent. The objective of this article is to analyse the legal aspects of blockchain technology application in securing electronic payments and to develop recommendations for preventing online fraud. This study aims to address existing gaps in the literature and provide new insights into how blockchain can be integrated into legal systems to enhance security.

In the course of the research, the following objectives were identified: to examine the existence of legal gaps in the regulation of blockchain technologies and their impact on the efficiency of their application in the field of electronic payments; to analyse the potential of blockchain implementation for reducing the level of online fraud; and to investigate the use of machine learning technologies in conjunction with blockchain to enhance the monitoring and prevention of fraudulent transactions.

MATERIALS AND METHODS

This study employs a theoretical analysis of the legal aspects of blockchain technology application in electronic payments, with a focus on examining existing legislative initiatives, regulations, and blockchain implementation practices across various jurisdictions. The analysis covers the period from 2018 to 2024, enabling the identification of current trends and specificities in the legal governance of this field.

Data collection was conducted through a systematic review of scholarly literature and legal documents pertaining to blockchain technologies and their impact on electronic payments. Primary sources included: the World Bank (2020) publication outlining blockchain applications across various sectors; Legal Framework for Blockchain Technology in Estonia (2022), detailing Estonia's regulatory infrastructure for blockchain; Singapore's Approach to Blockchain Regulation (2024), a report on Singapore's legislative initiatives in blockchain and cryptocurrencies; The United States and Blockchain: Regulatory Challenges and Opportunities (2022), a study examining legal challenges and prospects in the US; and China's Blockchain Policy: Strategic Implications (2023), an analysis of China's blockchain policy and its economic ramifications.

A case study analysis was performed for five countries where blockchain technologies have been integrated into the financial sector. In Kazakhstan, the study focused on blockchain applications in electronic payment systems and the adoption of digital assets (Greshnikov and Khamidullina, 2024). Kazakhstan is actively developing a legal framework to support blockchain initiatives, including the establishment of a special economic zone for blockchain and cryptocurrencies in Astana, which enhances regulatory oversight and attracts investment. Additional cases examined were Estonia (Blockchain and Smart…, 2024), Singapore (Chua and Oon, 2024), the US (Blockchain: Legal Implications…, 2022), and China (Jafri, 2024). Each country demonstrated distinct regulatory approaches to blockchain and cryptocurrencies.

Theoretical analysis was employed to identify key challenges faced by regulators across jurisdictions, while comparative analysis evaluated the efficacy

of diverse regulatory frameworks for blockchain technologies. These methodologies facilitated the synthesis of multidisciplinary data and provided a comprehensive assessment of blockchain's impact on electronic payment security.

A systems approach underpinned the interpretation of findings, enabling the integration of legal, economic, and social dimensions. This holistic perspective elucidated the broader implications of blockchain technologies for payment security and highlighted critical areas requiring legislative and practitioner attention.

RESULTS

Analysis of legal aspects of blockchain technologies in electronic payments

In recent years, numerous jurisdictions have introduced legislative initiatives addressing blockchain and cryptocurrencies. Estonia, for instance, has advanced a robust legal framework permitting blockchain applications in financial operations, including electronic payments. Estonian legislation enables the creation and registration of smart contracts, streamlining transactional processes and enhancing transparency. Consequently, users benefit from reduced processing times and lower costs compared to traditional banking systems, fostering greater trust and adoption as tangible advantages become evident. Singapore has similarly implemented clear regulations to promote innovation. Its Payment Services Act regulates cryptocurrency exchanges and ICOs, establishing a secure and predictable environment for investors through well-defined rights and obligations. The country's transparent licensing system ensures adaptability to technological advancements while safeguarding consumer and business interests (Chua and Oon, 2024). This has positioned Singapore as a hub for fintech startups and enterprises.

At the same time, there is no unified legislation in the United States, which results in legal uncertainty and divergent regulatory approaches at the state level. For instance, some states, such as Wyoming and Texas, have adopted more favourable regulations for cryptocurrencies, enabling companies to obtain licences more rapidly and commence operations with fewer obstacles. Conversely, other states, such as New York, have established stringent licensing requirements for cryptocurrency operations, creating barriers to market entry. This generates complex conditions for companies operating in the blockchain sector, as they are compelled to adapt to varying legal requirements depending on their jurisdiction of activity. China, by contrast, has implemented strict measures

aimed at restricting the use of cryptocurrencies, which also affects the deployment of blockchain technologies within the country. The ban on ICOs and the closure of cryptocurrency exchanges in 2017 jeopardised numerous start-ups and investments, leading to significant shifts in the market (Table 1).

Country	Key initiatives and laws	Year of adoption
Estonia	Implementation of smart contracts and electronic payments	2017
Singapore	Payment Services Act, regulation of ICOs	2020
USA	Diverse state-level laws, absence of unified regulation	2018-2023
Kazakhstan	Establishment of a dedicated blockchain and cryptocurrency zone, implementation of the "Blockchain in Public Services" system	2018-2023
China	Ban on ICOs and cryptocurrency transactions	2017

Table 1 – Legislative initiatives on blockchain technologies in different countries
Source: compiled by the authors based on Blockchain Technology: Applications and Use Cases (2023).

Despite the positive developments in regulatory efforts, several issues and challenges persist for policymakers. One of the principal difficulties lies in maintaining a balance between fostering innovation and ensuring consumer protection. For example, the absence of clear regulatory frameworks may result in fraud and financial losses for users, as witnessed in several failed ICOs that caused substantial financial harm. Regulators must devise mechanisms to minimise risks associated with cryptocurrency investments while simultaneously avoiding hindrances to the development of innovative technologies. Furthermore, the rapid pace of technological advancement poses difficulties for adapting existing legal frameworks. Emerging forms of fraud, such as "pump and dump" schemes, are becoming increasingly widespread, and existing legislation does not always provide effective countermeasures. Regulatory bodies also face challenges related to international cooperation, as blockchain technologies transcend borders and necessitate coordinated approaches at the global level. This raises questions about how different jurisdictions can collaborate to create a secure and efficient environment for blockchain applications and cryptocurrencies. For instance, harmonising regulatory standards for cryptocurrency exchanges between countries may become a barrier to international trade and investment.

A comparative analysis of regulatory approaches to blockchain across different countries reveals three primary models. The first model, exemplified by Estonia and Singapore, focuses on creating a favourable environment for innovation, which includes clear rules and support for startups. An innovation-friendly regulatory model is characterised by transparent and predictable regulatory frameworks, efficient licensing and registration processes, regulatory support for fintech and blockchain start-ups, openness to experimentation (including regulatory sandboxes), and policies aimed at enhancing investment

attractiveness while ensuring essential consumer protection. Such a model reduces regulatory uncertainty and entry barriers, fostering technological advancement and responsible innovation. Jurisdictions that adopt this approach actively develop blockchain infrastructure to support start-up growth and attract investment. Estonia has emerged as a leader in digital technologies, drawing global investor interest (Blockchain and Smart…, 2024). Under these conditions, start-ups can expand more rapidly and often secure capital both in Estonia and internationally.

The second model, as observed in the United States, is characterised by fragmented legislation, where individual states may adopt their own regulations, leading to legal uncertainty. This may hinder the development and deployment of new technologies, as companies are uncertain about the regulatory landscape they may face in the future (Blockchain: Legal Implications…, 2022). For example, discrepancies between state-level regulations can result in additional costs for companies operating across multiple jurisdictions. This may also reduce the global competitiveness of U.S. firms, as more flexible and progressive jurisdictions can attract top talent and investment.

The third model, represented by China, seeks strict control and limitation of blockchain and cryptocurrency use, which may slow technological advancement. China focuses on developing its own central bank digital currency (CBDC), which could serve as a competitor to private cryptocurrencies (Jafri, 2024). Such measures may prompt innovative startups to seek more favourable conditions abroad, potentially harming the Chinese market. It is important to note that strict restrictions may also drive cryptocurrency transactions into the shadows, thereby increasing risks to security and transparency.

Since 2018, Kazakhstan has been actively promoting blockchain technologies and their application in electronic payment systems and public services. A significant milestone was the establishment of a dedicated blockchain and cryptocurrency zone in Astana – the Astana International Financial Centre (AIFC). This zone was created to attract international investment, foster a favourable legal environment, and promote the development of financial technologies. Within the framework of the AIFC, specific rules and regulatory acts were developed to support blockchain projects and cryptocurrency initiatives, making Kazakhstan attractive to fintech startups and companies. One of the notable achievements was the 2020 launch of the "Blockchain in Public Services" system, which encompasses the use of blockchain for various government services, such as property registration, licensing, and the management of state registries. This system significantly enhances the transparency and efficiency of public processes, reducing the potential for corruption and ensuring quicker and more convenient interactions between the state and its citizens. In 2021,

Kazakhstan commenced the development of its own digital tenge, which would utilise blockchain technologies to ensure the security and transparency of financial transactions. The National Bank of Kazakhstan is actively exploring the potential implementation of a CBDC, which could represent a significant step in transforming the country's financial system by enabling more efficient and secure settlements for both businesses and individuals.

Kazakhstan has also been actively participating in international forums and initiatives related to blockchain technologies, such as the World Economic Forum and Blockchain Summit. This engagement allows the country to exchange expertise with other nations and integrate best practices into its legal framework. Furthermore, in 2023, a specialised training programme was launched to educate professionals in blockchain technologies and cryptocurrencies, aimed at developing human capital and preparing skilled personnel for this rapidly growing sector. Government institutions and universities have initiated joint projects to raise awareness about blockchain technologies and their potential applications across various economic sectors (Greshnikov and Khamidullina, 2024). By 2024, Kazakhstan continued to strengthen its position as a Central Asian hub for blockchain technologies, attracting fintech startups and companies. The government has actively supported innovation by creating favourable conditions for blockchain ecosystem development, including tax incentives, streamlined registration procedures, and access to funding. These measures enhance Kazakhstan's international competitiveness while fostering job creation, economic growth, and improved living standards.

A comparative analysis of the three aforementioned models revealed the advantages and drawbacks of each approach, providing valuable insights for other countries seeking to integrate blockchain technologies into their financial sectors (Table 2).

Model	Characteristics	Example countries
Innovation-friendly	Supportive environment for startups with clear regulations	Estonia, Singapore
Regulatory fragmentation	Divergent regional rules, legal uncertainty	USA
Stringent control	Restrictions on cryptocurrency and blockchain adoption	China

Table 2 – Comparative approaches to blockchain regulation
Source: compiled by the authors based on Regulatory Implications of Integrating Digital Assets and Distributed Ledgers in Credit Ecosystems (2020)

Jurisdictions with innovation-friendly policies may emerge as hubs for technological advancement, thereby stimulating economic growth (Iskakova et al., 2016; Bashtannyk et al., 2020). Crucially, effective blockchain regulation requires legislative flexibility and adaptability to safeguard consumer interests

while fostering an innovation-driven economy. To further contextualise these findings, it is essential to examine the impact of regulatory approaches on market dynamics and investment attractiveness. For instance, countries with clear and supportive frameworks, such as Estonia and Singapore, have observed a surge in blockchain startups, leading to job creation and increased tax revenues. Singapore, in particular, has become a global hub for ICOs and cryptocurrency firms, reinforcing its status as a leading financial centre. Conversely, jurisdictions with stringent controls, such as China, risk talent and capital flight as entrepreneurs seek more permissive regulatory environments. This may result in reduced competitiveness in the Chinese market and limited consumer choices (Jafri, 2024).

Thus, the study underscores the necessity for a holistic regulatory approach to blockchain technologies, encompassing not only legislative development but also active collaboration between policymakers, industry stakeholders, and academia. Such concerted efforts can establish a legal framework that balances innovation with user protection – a critical factor for successful blockchain integration in electronic payments and other economic domains. Regular evaluations of regulatory efficacy and adaptive policymaking are equally imperative to maintain equilibrium between technological progress and societal safeguards.

Analysis of successful blockchain implementation case studies

Estonia stands as one of the most advanced nations in the adoption of blockchain technologies. The country has developed a comprehensive legal framework enabling the use of blockchain for a wide range of public and private services, including electronic payments. A key component of this framework is the ability to create and register smart contracts, significantly streamlining and accelerating financial transactions. A notable example is the e-Residency system, launched in 2014, which allows foreign nationals to establish and manage companies in Estonia entirely online. This initiative enhances the accessibility of smart contracts and blockchain for international entrepreneurs, substantially increasing the number of registered businesses and fostering economic growth. The Estonian government actively supports the development of the blockchain ecosystem within the country. Blockchain technology is employed to ensure transparency and security in government registries, including real estate records, driver's license issuance, and medical data management (Temirzhanova et al., 2018; Musayeva et al., 2025). This has improved the transparency and efficiency of public services while reducing operational costs. For instance, the integration of blockchain into medical record systems enables secure and seamless data exchange between patients and healthcare providers, minimising the risk of errors.

A practical illustration of this is a blockchain-based platform for storing and sharing medical data, ensuring both security and confidentiality.

Furthermore, Estonia has established favourable conditions for blockchain startups. The country offers simplified company registration procedures, tax incentives, and access to highly skilled IT professionals. This has attracted numerous innovative projects, positioning Estonia as a promising jurisdiction for business operations. Table 3 outlines the key initiatives implemented at the national level to demonstrate the practical application of blockchain technologies in Estonia.

Initiative	Description	Year Introduced
Smart contract implementation	Deployment of smart contracts for various services	2017
Blockchain-based registries	Integration of blockchain into government registries	2017
Start-up support	Tax incentives and streamlined registration procedures	2017

Table 3 – Key blockchain initiatives in Estonia
Source: compiled by the authors based on Legal Framework for Blockchain Technology in Estonia (2022)

Singapore also exemplifies successful blockchain adoption, largely due to its balanced and supportive regulatory approach. In 2020, the country enacted the Payment Services Act, which includes specific provisions governing cryptocurrency exchanges and ICOs. This legislation establishes clear guidelines for market participants, including licensing requirements, cybersecurity measures, and anti-money laundering (AML) compliance. Such a framework creates a predictable and secure environment for blockchain applications, attracting numerous international firms to Singapore. For example, fintech companies such as Binance and Gemini have selected Singapore as a key expansion hub, underscoring the appeal of its regulatory landscape. Additionally, the Singaporean government actively invests in blockchain infrastructure and supports research in the field. The Monetary Authority of Singapore (MAS) has launched several pilot projects to test blockchain applications in the financial sector. One such initiative, Project Ubin, explores the use of blockchain for interbank settlements and clearing. These efforts contribute to the accumulation of expertise and the identification of best practices that can later be applied to real-world business processes.

As a result, Singapore has become one of the world's leading financial centres, attracting significant investment in blockchain startups. Fintech companies value the stable regulatory environment and the ability to swiftly bring

products to market. This has cemented Singapore's position as a frontrunner in blockchain technology adoption (Table 4).

Initiative	Description	Year of Implementation
Payment Services Act	Regulation of cryptocurrency exchanges and ICOs	2020
Investments in Blockchain Infrastructure	Support for research and pilot projects in finance	2018
Market Participant Licensing	Clear rules for obtaining licences	2020

Table 4 – Singapore's Legislative Initiatives in Blockchain Technology
Source: Compiled by the authors based on Singapore's Approach to Blockchain Regulation (2024)

Unlike Estonia and Singapore, the legal regulation of blockchain technology in the United States and China is characterised by greater uncertainty and divergent approaches. In the United States, there is no unified federal legislation governing the use of blockchain and cryptocurrencies. Instead, each state develops its own regulations, creating a fragmented legal environment. For instance, Wyoming has gained recognition as the "crypto capital" due to its progressive laws facilitating the registration and operation of blockchain-based businesses. In contrast, New York's BitLicense imposes stringent compliance requirements and high regulatory costs on companies. Such regulatory heterogeneity complicates the development of blockchain startups, forcing them to adapt to varying legal frameworks depending on their operational jurisdiction. This diminishes the US's investment appeal for innovative companies compared to more harmonised jurisdictions. In particular, startups may face substantial legal costs associated with complying with multiple disparate laws and regulations.

Conversely, China has adopted a strict regulatory approach, limiting the use of cryptocurrencies and blockchain technology. In 2017, the country banned ICOs and shut down cryptocurrency exchanges, leading to the closure of major platforms such as BTCChina and Huobi. These measures significantly impacted the development of China's blockchain ecosystem, jeopardising numerous startups and investments in the sector. Instead, China has focused on developing a state-controlled digital currency, known as the Digital Currency Electronic Payment (DCEP). This initiative, launched by the People's Bank of China, leverages blockchain technology to create a more efficient and regulated financial system. This approach reflects China's intent to tighten control over financial technologies and curb the influence of decentralised cryptocurrencies. However, such policies may hinder the adoption of blockchain technology in the private sector and stifle innovation. For example, many skilled developers may leave the

country in search of more permissive and supportive environments for their projects (China's Blockchain Policy…, 2023).

Thus, the examples of Estonia, Singapore, the United States, and China illustrate varying approaches to the legal regulation of blockchain technology, each with distinct implications for innovation and jurisdictional investment attractiveness. It is important to emphasise that regulatory flexibility and support are key factors in the successful adoption of blockchain technology and in fostering user trust.

Recommendations for improving legal regulation

The analysis of existing blockchain implementation case studies has identified certain legislative gaps that must be addressed to establish a safer and more predictable legal environment. The first step towards addressing these gaps is the development of unified standards for regulating blockchain technology and cryptocurrencies. This may include introducing comprehensive federal legislation in countries such as the United States to eliminate the fragmentation and uncertainty prevalent across different states. An example of such an initiative could be the formulation of a National Blockchain Strategy, incorporating clear rules for all market participants, thereby streamlining licensing procedures and enhancing investor confidence. It is crucial that such a strategy also incorporates input from industry stakeholders and academia to ensure a thorough understanding of the practical challenges and needs faced by market participants. A concrete example of such an approach can be seen in the initiative undertaken in Wyoming, where a series of laws were adopted to simplify the process of registration and licensing for companies operating with blockchain and cryptocurrencies. Wyoming has become known as the "crypto capital" of the United States due to its progressive policy, which has led to a significant increase in the number of blockchain companies registered in the state (The United States…, 2022).

The second proposed measure is the introduction of cybersecurity and data protection requirements for all participants in the blockchain ecosystem. Uncertainty regarding data security may result in information leaks and fraud (Smailov et al., 2025; Barlybayev and Turginbayeva, 2025). Regulatory bodies could develop specific requirements for data encryption and authentication mechanisms aimed at protecting users and their assets. For instance, the implementation of International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27001 (2024) standards for information security management systems may serve as a foundation for ensuring the necessary level of data protection within blockchain ecosystems. Real-world examples of the successful application of such standards can be observed in major

financial institutions such as HSBC, which utilise blockchain to optimise their operations while maintaining a high level of data security.

The third step may involve active cooperation between the public and private sectors to facilitate knowledge exchange and the sharing of best practices. The establishment of working groups comprising representatives from government, industry, and academia would enable more informed decision-making and allow legislation to be adapted to the rapidly changing market conditions. The involvement of experts from diverse fields – such as fintech, cybersecurity, and law – can contribute to the development of more comprehensive and effective regulatory solutions. For example, in Singapore, such working groups operate under initiatives like the FinTech Regulatory Sandbox, which enables start-ups to test their solutions in a controlled environment with support from regulators.

Public institutions must play an active role in the development and implementation of new regulatory initiatives aimed at supporting blockchain technologies (Zhyvko et al., 2022; Blikhar et al., 2023). It is crucial that legislative measures are geared towards creating a favourable environment for start-ups and innovative enterprises. One key recommendation for public authorities is to enhance dialogue with industry representatives. The establishment of platforms for discussion and joint decision-making will enable a better understanding of business needs and facilitate the adaptation of legislation accordingly (Nursaliyeva et al., 2023; Shtal et al., 2024). This may include regular meetings with key stakeholders in the blockchain market, as well as open consultations on the drafting of new bills. For instance, the organisation of round tables and forums, where business representatives can share their experiences and challenges, will assist governments in gaining deeper insight into current obstacles and opportunities.

Kazakhstan should develop a comprehensive strategy aimed at integrating blockchain technologies into various sectors of the economy. This could involve the creation of legislative initiatives that encourage innovation and attract investment in this area. It is necessary to develop clear and locally adapted regulatory frameworks for blockchain technologies and cryptocurrencies. This would help eliminate uncertainties and establish a trusted environment for investors and entrepreneurs. It is essential to establish government support programmes for start-ups operating in the blockchain sphere. Such support may include tax incentives, grants, and access to funding for innovative projects. Kazakhstan should also implement stringent cybersecurity requirements for participants in the blockchain ecosystem. This could involve the development of data protection standards and mandatory security measures for companies operating in this domain.

Furthermore, programmes should be initiated to train specialists in blockchain technologies and cybersecurity. This will help build a pool of qualified professionals capable of effectively contributing to the development of the sector. Kazakhstan might consider forming partnerships with other countries that have successfully adopted blockchain technologies. This would allow the country to draw upon best practices and adapt them to local circumstances. It is recommended to organise regular meetings and round-table discussions with representatives from business, academia, and government to address current challenges and opportunities in the field of blockchain technologies.

It is also important to take into account international experience and best practices when drafting new legislation. Government institutions may consider establishing partnerships with countries that have effectively implemented blockchain solutions, such as Estonia and Singapore. This would enable the adoption of successful models tailored to local conditions. For example, the Singaporean government launched the "Smart Nation" initiative, aimed at integrating new technologies, including blockchain, into various aspects of life, which may serve as a model for other countries. For businesses, it is crucial to adopt a proactive approach to compliance with legislation and security standards. Companies must invest in employee training and the implementation of advanced technologies to ensure adherence to regulatory requirements. This not only enhances the level of trust from clients and investors but also helps avoid fines and legal issues. For instance, conducting regular compliance and cybersecurity training sessions enables employees to stay informed about changes and current regulatory demands. In addition, enterprises may engage consulting firms to obtain support in legal compliance and the adoption of new technologies.

The prospects for further research into blockchain technologies and their implementation remain highly promising. Given the rapid advancement of these technologies and their application across various sectors, it is necessary to continue exploring their impact on the economy and society at large. One possible avenue for future research is the analysis of successful case studies of blockchain implementation in industries such as healthcare, logistics, and financial services. This would allow the identification of best practices and their adaptation to other sectors. For example, research into blockchain use in supply chains, such as the IBM Food Trust initiative – which enables the tracking of food origin – may help optimise processes and enhance transparency. This platform is already employed by major companies such as Walmart and Nestlé, confirming its effectiveness. Moreover, attention should be directed towards cybersecurity and data protection in the context of blockchain technologies. Investigating vulnerabilities and protection methods will facilitate the development of more robust systems, which in turn will increase user trust. Research in this field may include testing various

security methods, such as the use of multi-layer authentication and encryption, as well as analysing security incidents and their consequences for users. For example, the study of data breach incidents, such as the Mt. Gox exchange case, can provide valuable insights into how to prevent similar situations in the future. Finally, it is essential to continue examining the impact of blockchain technologies on business models and economic processes. This may involve exploring new formats of collaboration and decentralised models that could emerge from the widespread adoption of blockchain. For instance, research into the potential of decentralised finance (DeFi) and its effects on traditional financial systems – such as lending and insurance – may open up new opportunities for businesses and consumers. Studies in this area could lead to the development of new business models based on decentralised principles, thereby contributing to a more efficient and inclusive economy.

Thus, a comprehensive approach to improving regulatory frameworks, active collaboration between public authorities and the business sector, and continued research in this domain will help establish an effective ecosystem for the implementation of blockchain technologies, which in turn will foster the development of an innovative economy.

DISCUSSION

The findings of this study highlight the importance of creating an effective legal environment for the adoption of blockchain technologies and cryptocurrencies. In particular, the identified legislative gaps, the need to enhance cybersecurity, and the active cooperation between public authorities and businesses indicate that a comprehensive approach is required for the successful development of innovative technologies. This will not only safeguard the interests of users and investors but also create favourable conditions for the emergence and growth of new blockchain-based business models.

The results of this research are consistent with the conclusions of other scholars, such as Fnu (2024), who noted in their work that legislative fragmentation in countries such as the United States generates uncertainty for companies operating in the field of cryptocurrencies. Their study emphasises that the absence of a unified federal regulatory strategy creates legal barriers that hinder the development of innovative start-ups. The findings of the present study demonstrate that since 2018 Kazakhstan has been actively developing blockchain technologies by establishing special zones such as the AIFC. This aligns with Fnu's conclusions, which underscore the importance of creating a favourable legal environment to attract international investment.

Furthermore, the findings of this study corroborate conclusions drawn by other scholars regarding the significance of cybersecurity in the context of blockchain technologies. For instance, the work of Oluwabunmi et al. (2024) identifies data security vulnerabilities that may lead to information leaks and fraudulent activities, thereby undermining user trust in emerging technologies. This study also highlights the necessity of implementing stringent cybersecurity and data protection requirements, such as the ISO/IEC 27001 (2024) standards, to ensure an adequate level of security within blockchain ecosystems. In this context, the research by Zakir (2023) should also be noted, as it examines approaches to safeguarding decentralised systems and emphasises the need for comprehensive data protection measures.

The analysis of successful blockchain implementation case studies in Estonia and Singapore, conducted in this research, also aligns with the conclusions of other scholars. In this context, a crucial distinction pertinent to regulatory design concerns the differing legal implications of public (permissionless) and private (permissioned) blockchains. Public blockchains, characterised by open participation and decentralised governance, pose significant challenges for regulatory oversight, particularly in terms of jurisdiction, accountability, compliance with AML and counter-financing of terrorism (CFT) requirements, and consumer protection (Tokzhanov et al., 2024; Temirzhanova et al., 2019). In contrast, private or consortium blockchains operate within controlled networks of identifiable participants, facilitating clearer governance structures and more straightforward implementation of compliance measures, such as know-your-customer (KYC) procedures and auditability, which are especially relevant for public-sector and enterprise applications (Casino et al., 2019; De Filippi and Wright, 2020).

For example, the work of Irannezhad and Faroqi (2023) describes how Singapore has emerged as a global leader in blockchain technologies due to government support and clear regulatory frameworks. These findings confirm that active state involvement in developing and implementing new regulatory initiatives fosters a conducive environment for startups and innovative enterprises. The introduction of the "Blockchain in Public Services" system in Kazakhstan in 2020, which enables blockchain usage for real estate registration and licensing, further demonstrates a progressive approach to enhancing transparency in governmental processes. This resonates with Estonia's experience, as discussed in the study by Irannezhad and Faroqi, where blockchain is extensively utilised in public registries.

Kazakhstan actively participates in international forums, mirroring Singapore's approach, which invests in blockchain infrastructure development and supports research (Dhia et al. 2023). The blockchain specialist training

programme launched in 2023 aims to develop human capital, aligning with the recommendations of Dhia et al., who stress the importance of skilled workforce preparation for successful technology adoption.

In the context of international experience, this study also underscores the significance of collaboration between government bodies and businesses. The research by Albshaier et al. (2024) and Garcia-Teruel (2020) illustrates how such partnerships can facilitate the establishment of an effective ecosystem for blockchain implementation. This aligns with the recommendations on forming working groups comprising government, business, and academic representatives to promote knowledge exchange and best practices. A notable example of such successful cooperation is the "Blockchain for Social Impact" initiative launched in the US, which brings together diverse stakeholders to address social challenges through blockchain applications.

This initiative has demonstrated how technology can be applied to solve issues such as food supply chain tracking and improving access to financial services in developing countries. Nevertheless, this study has also identified certain aspects that diverge from the conclusions of other authors. For instance, Thommandru and Chakka (2023) argue that stricter cryptocurrency regulation, as seen in China, may be an effective means of consumer protection.

However, this study has shown that such measures may stifle innovation and lead to talent drain, as evidenced by cases in China, where stringent restrictions on cryptocurrency transactions resulted in the closure of numerous startups and reduced investment levels. This conclusion is further supported by the research of Rabbani et al. (2024) and Hashem (2023), which highlights that excessive regulation may adversely affect the startup and innovation ecosystem. A pertinent example is the Chinese ICO ban in 2017, which triggered a mass exodus of startups to other jurisdictions, such as Hong Kong and Singapore. To avoid similar pitfalls, Kazakhstan should focus on developing a balanced legal framework, which would enhance user and investor confidence while fostering the growth of new blockchain-based business models.

To provide a balanced view of blockchain adoption, it is essential to examine instances of implementation failures. Recent investigations into blockchain project failures, including the case study of the TradeLens platform, indicate that such projects may falter due to governance challenges, insufficient stakeholder engagement, interoperability complications, and data security concerns, which current legal and regulatory frameworks may inadequately address. The findings suggest that technological potential alone does not guarantee success; without clear governance frameworks, effective stakeholder collaboration, and strong legal protections, blockchain initiatives are likely to fail, underscoring the

necessity for comprehensive regulatory strategies that integrate insights from both successful and unsuccessful implementations (Najati, 2025).

These insights align with recent findings by Babayev (2025), who demonstrates that the success of blockchain initiatives depends not only on technological maturity but also on institutional preparedness and regulatory clarity. The study highlights, that insufficient legal frameworks and limited governmental support may hinder blockchain adoption even in technologically promising sectors.

Moreover, it is worth mentioning the study by Onyekachukwu et al. (2024), which analyses various approaches to blockchain regulation across different countries and concludes that the optimal model involves striking a balance between consumer protection and fostering innovation. Another noteworthy contribution is the work by Ben et al. (2024), in which the authors propose a concept of flexible regulation capable of adapting to rapidly changing market conditions. A significant addition to this topic is the research by Citra et al. (2024), which examines potential scenarios for the evolution of blockchain legislation, taking into account the dynamics of technological advancements and market demands. The relevance of this study underscores the necessity for continuous monitoring and legislative adaptation in response to the rapid development of technology.

Another crucial aspect is the research by Ikbal et al. (2024), which provides an in-depth analysis of blockchain technology regulation in various jurisdictions and highlights how differences in regulatory approaches may impact international business operations. This aligns with the findings on the need for a unified regulatory strategy that considers both local and international dimensions. For instance, Europe is actively developing the Markets in Crypto-Assets (MiCA) framework, which aims to establish common rules for cryptocurrency markets and ensure investor protection – a potential milestone in regulatory harmonisation.

In conclusion, the findings of this study emphasise the necessity of a comprehensive approach to the legal regulation of blockchain technologies. The successful development of this field requires not only addressing legislative gaps but also fostering active collaboration among all stakeholders, including government bodies, the private sector, and the academic community. Such an approach would not only enhance trust among users and investors but also create favourable conditions for the growth and development of new blockchain-based business models.

Thus, this study contributes to the existing body of literature and may serve as a foundation for further research in this field, particularly in analysing the impact of blockchain technologies on various economic and societal sectors. Given the rapid evolution of this technology and its potential implications across multiple

aspects of life, it is imperative to continue research in this area and adapt legislation in response to emerging challenges.

CONCLUSION

The study yielded key findings on the legal regulation of blockchain technologies and cryptocurrencies, which hold significant implications for both academia and practical applications. It was established that countries such as Estonia, Singapore, and Kazakhstan have developed effective legal frameworks facilitating the adoption of blockchain technologies. Estonia's legislation, which permits the use of smart contracts and electronic payments, significantly streamlines financial transactions, thereby enhancing user trust in such systems and fostering the growth of innovative startups. Singapore, in turn, has implemented clear and transparent regulations governing cryptocurrency exchanges and ICOs, ensuring a secure and predictable environment for investors. The Payment Services Act of 2020 introduces stringent licensing requirements and cybersecurity provisions, making Singapore an attractive hub for fintech startups and established firms alike. Kazakhstan is also actively advancing its legal framework by integrating blockchain technologies into the financial sector and establishing special economic zones for their application, thereby stimulating startup growth and attracting foreign investment.

Several challenges faced by regulators in different jurisdictions were identified. In the United States, the absence of a unified federal framework results in state-specific regulations, imposing substantial compliance costs on companies operating across multiple markets. Meanwhile, China's stringent measures, including restrictions on cryptocurrency usage, may stifle innovation and lead to talent outflow. The 2017 ban on ICOs and the shutdown of cryptocurrency exchanges jeopardised numerous startups and investments, adversely affecting market development. These examples underscore the need for a cohesive regulatory strategy that accounts for both national and international considerations, including recommendations for Kazakhstan to ensure a more flexible and adaptive legal environment.

The study's results also demonstrated that regulators face the challenge of balancing innovation support with consumer protection. The lack of clear rules and standards may lead to fraudulent activities and financial losses for users, ultimately undermining trust in cryptocurrency technologies.

Based on the findings, it is recommended to establish unified standards for the regulation of blockchain technologies and cryptocurrencies. This will help eliminate legal uncertainty and enhance investor confidence. The implementation

of stringent cybersecurity and data protection requirements will constitute a critical step in addressing the growing threats in this domain.

Active collaboration between government agencies and the private sector, the formation of working groups, and regular consultations with market participants can facilitate the development of more adequate and effective legislation, including recommendations for Kazakhstan. Examples of successful cooperation, such as the "Blockchain for Social Impact" initiative in the United States, demonstrate how diverse stakeholders can unite to address social and economic challenges through blockchain technologies.

Thus, a comprehensive approach to blockchain regulation, active cooperation between government institutions and businesses, and continued research in this field will help establish an effective ecosystem for blockchain adoption and foster the development of an innovation-driven economy. This, in turn, will contribute to the improvement of overall financial systems and enhance the population's standard of living.

A limitation of this study was its macroeconomic-level analysis of blockchain applications and regulatory frameworks. Future research should examine cybersecurity and data protection case studies in leading companies utilising blockchain technologies across these countries.

REFERENCES

Abad-Segura E., Infante-Moro A., González-Zamar M., & López-Meneses E. (2021). Blockchain Technology for Secure Accounting Management: Research Trends Analysis. *Mathematics*, *9*(14), 1631. https://doi.org/10.3390/math9141631

Adewole K., Saxena N., & Bhadauria S. (2020). Application of Cryptocurrencies Using Blockchain for e-Commerce Online Payment. In: *Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications*, (pp. 263-305). Boca Raton: CRC Press. https://doi.org/10.1201/9780429324932

Albshaier L., Almarri S., & Hafizur M. (2024). A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions. *Computers*, *13*(1), 27. https://doi.org/10.3390/computers13010027

Arif Z., Supyadillah A., Irfan A., & Taufik A. (2024). The Revolution of Blockchain in Digital Payment Systems: Legal Implications and Regulatory Challenges. *Journal of Ecohumanism*, *3*(8), 12269. https://doi.org/10.62754/joe.v3i8.5833

Ashfaq T., Khalid R., Sani A., Aslam S., Taher A., Alsafari S., & Hameed I. (2022). A Machine Learning and Blockchain Based Efficient Fraud

Detection Mechanism. *Sensors*, *22*(19), 7162. https://doi.org/10.3390/s22197162

Babayev N., Qurbanov B., Abdullayev L., & Babayev M. (2025). Integration of Blockchain Technology into Azerbaijan's Agricultural Sector: Prospects and Challenges. *Scientific Horizons*, *28*(2), 145-156. https://doi.org/10.48077/scihor2.2025.145

Balagolla E., Fernando W., Rathnayake R., Wijesekera M., Senarathne A., & Abeywardhana K. (2021). Credit Card Fraud Prevention Using Blockchain. In: *International Conference for Convergence in Technology (I2CT)* (pp. 1-8). Maharashtra: IEEE. https://doi.org/10.1109/I2CT51068.2021.9418192

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

Bashtannyk, V., Buryk, Z., Kokhan, M., Vlasenko, T., & Skryl, V. (2020). Financial, economic and sustainable development of states within the conditions of industry 4.0. *International Journal of Management, 11*(4), 406-413. https://doi.org/10.34218/IJM.11.4.2020.040

Ben M., Ahmed Y., Mahmoud H., Attique S., Omar M., Taramonli S., Bellekens X., Abozariba R., Idrissi M., & Aneiba A. (2024). A Survey on Blockchain Technology in the Maritime Industry: Challenges and Future Perspectives. *Future Generation Computer Systems*, *157*, 618-637. https://doi.org/10.1016/j.future.2024.03.046

Blikhar, M., Vinichuk, M., Kashchuk, M., Gapchich, V., & Babii, S. (2023). Economic and legal aspects of ensuring the effectiveness of counteracting corruption in the system of anti-corruption measures of state authorities. *Financial and Credit Activity: Problems of Theory and Practice, 4*(51), 398-407. https://doi.org/10.55643/fcaptp.4.51.2023.4138

Blockchain and Smart Contracts in Estonia. (2024). https://www.eestifirma.ee/en/blockchain-and-smart-contracts-in-estonia/

Blockchain Technology: Applications and Use Cases. (2023). https://documents1.worldbank.org/curated/en/099200503082329768/pdf/P17425408f3aa00580a2620810813ed0370.pdf

Blockchain: Legal Implications, Questions, Opportunities and Risks. (2022). https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-blockchain-wp-sept-2022.pdf

Casino, F., Dasaklis, T., & Patsakis, C. (2019). A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. *Telematics and Informatics*, *36*, 55-81. https://doi.org/10.1016/j.tele.2018.11.002

China's Blockchain Policy: Strategic Implications. (2023). https://www.forbes.com/sites/digital-assets/2024/10/08/china-bets-on-massive-blockchain-infrastructure/

Chowdhury E., Stasi A., & Pellegrino A. (2023). Blockchain Technology in Financial Accounting: Emerging Regulatory Issues. *Review of Financial Economics*, *21*(1), 862-868. http://dx.doi.org/10.55365/1923.x2023.21.94

Chua, T., & Oon, U. (2024). Blockchain 2024. https://practiceguides.chambers.com/practice-guides/blockchain-2024/singapore

Citra A., Iman E., & Rianto R. (2024). Electronic Payment Threats and Security: A Systematic Literature Review. *National Journal of Informatics Engineering Education: JANAPATI*, *13*(2), 301-315. https://doi.org/10.23887/janapati.v13i2.76635

De Filippi, P., & Wright, A. (2020). *Blockchain and the Law: The Rule of Code.* Cambridge: Harvard University Press. https://doi.org/10.4159/9780674243146

Dhia H., Varga P., & Molnár S. (2023). Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors*, *23*(2), 788. https://doi.org/10.3390/s23020788

Fnu J. (2024). Enhancing Data Security in Financial Institutions with Blockchain Technology. *Journal of Artificial Intelligence General Science*, *5*(1), 424-437. https://doi.org/10.60087/jaigs.v5i1.217

Garcia-Teruel R. (2020). Legal Challenges and Opportunities of Blockchain Technology in the Real Estate Sector. *Journal of Property, Planning and Environmental Law*, *12*(2), 129-145. https://doi.org/10.1108/JPPEL-07-2019-0039

Gayathma H., Sridarran P., & Rajaratnam D. (2022). Effective Use of Blockchain Technology for Facilities Management Procurement Process. *Journal of Facilities Management*, *20*(3), 452-468. https://doi.org/10.1108/JFM-10-2020-0077

Gelar R., & Naufal M. (2023). Blockchain Implementation in E-Commerce to Improve the Security Online Transactions. *Journal of Scientific Research, Education, and Technology*, *2*(1), 328-338. https://doi.org/10.58526/jsret.v2i1.85

Greshnikov, K., & Khamidullina, Y. (2024). Fintech Laws and Regulations 2024 – Kazakhstan. https://www.globallegalinsights.com/practice-areas/fintech-laws-and-regulations/kazakhstan/

Hariyani D., Hariyani P., Mishra S., & Sharma M. (2025). Transformative Impacts of Blockchain Technology on Manufacturing Management and Industrial Engineering Practices: A Literature Review. *Green Technologies and Sustainability*, *3*, 100169. https://doi.org/10.1016/j.grets.2025.100169

Hashem A. (2023). The Impact of Blockchain Technology on Financial Services: Mediating Role of Big Data Analytics. *Journal of Logistics, Informatics and Service Science*, *10*(2), 91-107. https://doi.org/10.33168/JLISS.2023.0207

Ikbal M., Steigner T., Imam M., & Akther A. (2024). Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) Through

Blockchain Technology: A Comprehensive Approach. https://doi.org/10.48550/arXiv.2405.04837

International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27001 "Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements". https://www.iso.org/standard/88435.html

Irannezhad E., & Faroqi H. (2023). Addressing Some of Bill of Lading Issues Using the Internet of Things and Blockchain Technologies: A Digitalized Conceptual Framework. *Maritime Policy & Management*, *50*(4), 428-446. https://doi.org/10.1080/03088839.2021.1930223

Iskakova, Z.T., Bimbetov, A.B., & Sarsenova, S.N. (2016). Institution building of the eurasian economic union: Challenges and opportunities. *Journal of Advanced Research in Law and Economics, 7*(4), 817-827. https://doi.org/10.14505/jarle.v7.4(18).13

Jafri, A. (2024). China Places Blockchain at the Core of National Data Strategy in New Guidelines. https://cryptoslate.com/china-places-blockchain-at-the-core-of-national-data-strategy-in-new-guidelines/

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: Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/REW66121.2025.00055

Kapyshev Y. (2024). Comparative Analysis of EU and Kazakhstan Banking Laws, and Another Country in the East (UAE) with an Increasing Financial Economy. https://hdl.handle.net/20.500.14247/23856

Kshetri N., Miller K., Banerjee G., & Raj B. (2023). FinChain: Adaptation of Blockchain Technology in Finance and Business-An Ethical Analysis of Applications, Challenges, Issues and Solutions. *International Journal of Emerging and Disruptive Innovation in Education: VISIONARIUM*, *1*(1), 4. https://doi.org/10.62608/2831-3550.1010

Kumar D., Kumar S., & Joshi A. (2023). Assessing the Viability of Blockchain Technology for Enhancing Court Operations. *International Journal of Law and Management*, *65*(5), 425-439. https://doi.org/10.1108/IJLMA-03-2023-0046

Laroiya C., Saxena D., & Komalavalli C. (2020). Applications of Blockchain Technology. *Handbook of Research on Blockchain Technology*, *1*, 213-243. https://doi.org/10.1016/B978-0-12-819816-2.00009-5

Legal Framework for Blockchain Technology in Estonia. (2022). https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/estonia/

Mapa C., Perera P., & Grandhi S. (2023). A Blockchain-Based Model for the Prevention of Superannuation Fraud: A Study of Australian Super Funds. *Applied Sciences*, *13*(17), 9949. https://doi.org/10.3390/app13179949

Musayeva, N., Aliyeva, M., Gasimova, L., & Bayramova, G. (2025). The Role of Blockchain Technology in Ensuring Transparency, Trust, and Auditing in

Financial Markets: Prospects and Challenges. *Operations Research Forum, 6*(4), 167. https://doi.org/10.1007/s43069-025-00578-y

Najati I. (2025). Exploring the Failure Factors of Blockchain Adopting Projects: A Case Study of TradeLens through the Lens of Commons Theory. *Frontiers in Blockchain*, *8*, 1503595. https://doi.org/10.3389/fbloc.2025.1503595

Nursaliyeva, G., Baikenzhina, K., Kalmaganbetova, D., Balgimbekova, G., Seitzhanova, N., & Kussainova, L. (2023). Methodology for the legislative application of evaluative categories in criminal law. *Journal of Law and Sustainable Development, 11*(5), e0725. https://doi.org/10.55908/sdgs.v11i5.725

Oluwabunmi H., Idemudia C., & Vanessa T. (2024). Integrating Machine Learning and Blockchain: Conceptual Frameworks for Real-Time Fraud Detection and Prevention. *World Journal of Advanced Research and Reviews*, *23*(1), 56-68. https://doi.org/10.30574/wjarr.2024.23.1.1985

Onyekachukwu E., Amajuoyi P., Bukola K., & Ogechukwu A. (2024). The Role of Big Data in Detecting and Preventing Financial Fraud in Digital Transactions. *World Journal of Advanced Research and Reviews*, *22*(2), 1746-1760. https://doi.org/10.30574/wjarr.2024.22.2.1575

Rabbani H., Farrukh M., Jamil T., Siddiqui S., Mamdouh M., Bahaaddin R., Ullah Z., Umair M., & Nooruddin M. (2024). Enhancing Security in Financial Transactions: A Novel Blockchain-Based Federated Learning Framework for Detecting Counterfeit Data in Fintech. *PeerJ Computer Science*, *10*, e2280. https://doi.org/10.7717/peerj-cs.2280

Rejeb A., Keogh J., & Treiblmaier H. (2020). How Blockchain Technology Can Benefit Marketing: Six Pending Research Areas. *Frontiers in Blockchain*, *3*(3). https://doi.org/10.3389/fbloc.2020.00003

Sanz-Bas D., Del C., Náñez S., & Ángel M. (2021). Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. *Laws*, *10*(3), 57. https://doi.org/10.3390/laws10030057

Shtal, T., Davydova, O., Sysoieva, S., Logvinkov, S., & Zhukov, V. (2024). Innovative risk management in the hotel and restaurant business: Scientific and practical aspect. *Scientific Bulletin of Mukachevo State University. Series Economics, 11*(2), 116-125. https://doi.org/10.52566/msu-econ2.2024.116

Singapore's Approach to Blockchain Regulation. (2024). https://sumsub.com/blog/singapore-crypto-regulations-all-you-need-to-know/

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

Temirzhanova, L.A., Imangaliev, N.K., Syzdykov, A.Z., Eshnazarov, A.A., & Sagymbekov, B.Z. (2018). Improving the mechanism of countering certain

types of fraud in the Republic of Kazakhstan. *Journal of Advanced Research in Law and Economics,* 9(5), 1776-1788. https://doi.org/10.14505//jarle.v9.5(35).33

Temirzhanova, L.A., Imangaliev, N.K., Sagymbekov, B.Z., Eshnazarov, A.A., & Syzdykov, A.Z. (2019). Countering fraud committed using information technology in Kazakhstan. *Journal of Advanced Research in Law and Economics, 10*(7), 2122-2132. https://doi.org/10.14505/jarle.v10.7(45).25

The United States and Blockchain: Regulatory Challenges and Opportunities. (2022). https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/usa/

Thommandru A., & Chakka B. (2023). Recalibrating the Banking Sector With Blockchain Technology for Effective Anti-Money Laundering Compliances by Banks. *Sustainable Futures*, *5*, 100107. https://doi.org/10.1016/j.sftr.2023.100107

Tokzhanov, Y., Kalmaganbetova, D., Kussainova, A., Baimoldina, S., & Sarybekova, S. (2024). Steganographic Technologies in the Identification of Convicted Persons. *Pakistan Journal of Criminology, 16*(3), 275-294. https://doi.org/10.62271/pjc.16.3.275.294

Tripathi G., Ahad M., & Casalino G. (2023). A Comprehensive Review of Blockchain Technology: Underlying Principles and Historical Background with Future Challenges. *Decision Analytics Journal*, *9*, 100344. https://doi.org/10.1016/j.dajour.2023.100344

Vazov, R., Shvachych, G., Moroz, B., Kabak, L., Kozenkova, V., Karpova, T., & Busygin, V. (2022). Development Features and Principles of Blockchain Technologies and Real Options as the Main Components of the Digital Economy. *Lecture Notes on Data Engineering and Communications Technologies, 126*, 57-74. https://doi.org/10.1007/978-981-19-2069-1_5

Wenhua Z., Qamar F., Naser T., Hassan R., Talib S., & Ngoc Q. (2023). Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics*, *12*(3), 546. https://doi.org/10.3390/electronics12030546

World Bank. (2020). Regulatory Implications of Integrating Digital Assets and Distributed Ledgers in Credit Ecosystems. https://documents1.worldbank.org/curated/en/165451588054535734/pdf/Regulatory-Implications-of-Integrating-Digital-Assets-and-Distributed-Ledgers-in-Credit-Ecosystems.pdf

Zakir M. (2023). Emerging Trends in Forensic Accounting: Data Analytics, Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention. Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention. https://doi.org/10.2139/ssrn.4450488

Zhyvko, Z., Nikolashyn, A., Semenets, I., Karpenko, Y., Zos-Kior, M., Hnatenko, I., Klymenchukova, N., & Krakhmalova, N. (2022). Secure aspects of digitalization in management accounting and finances of the subject of the national economy in the context of globalization. *Journal of Hygienic Engineering and Design, 39*, 259-269. https://keypublishing.org/jhed/wp-

content/uploads/2022/09/25.-JHED-Volume-39-Full-paper-Zinaida-Zhyvko.pdf

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