Received: 21.09.2026. Accepted: 29.09.2026. Available online: 30.09.2026.

IRSTI 10.19.61
DOI: https://www.doi.org/10.32523/2791-0954-2026-19-3-8-24

Blockchain technologies in securing electronic payments and preventing internet fraud: international legal standards and prospects for implementation in the Republic of Kazakhstan

Aibar Kumisbek*
PhD student
Khoja Akhmet Yassawi International Kazakh-Turkish University
Turkestan, Kazakhstan, 161200
e-mail: aibaron@yandex.ru
ORCID: https://orcid.org/0009-0007-0924-7068

Baurzhan Smatlayev
Doctor of Legal Sciences, Professor, Dean of the Faculty of Law
L.N. Gumilyov Eurasian National University
Astana, Kazakhstan, 010008
e-mail: smatlayev_bm@enu.kz
ORCID: https://orcid.org/0009-0006-5543-2822

Alua Muratova
PhD, Head of the Department of Criminal Law Disciplines of the Faculty of Law
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, 010008
ORCID: https://orcid.org/0000-0002-0159-9671
e-mail: muratova_azh@enu.kz

Abstract. This article examines the issues of securing electronic payments and preventing internet fraud amid the rapid growth of cashless transactions in the Republic of Kazakhstan. The aim of the study is to determine what distributed ledgers and smart contracts can contribute to the security of electronic payments and to the fight against internet fraud, and to propose a model for bringing international standards into Kazakhstani law. Based on enforcement statistics, the paper highlights low crime clearance rates and high risks associated with unregistered cryptocurrency transactions. The authors analyze the technological potential of distributed ledgers, consensus algorithms, and smart contracts for preventing cybercrimes and enabling real-time end-to-end transaction tracing. Key legal obstacles to blockchain adoption are identified, including normative dualism between national law and the Astana International Financial Centre regime, the lack of procedural tools for seizing digital assets, and conflicts between blockchain immutability and data protection standards. Drawing on international standards from FATF, UNCITRAL, the Budapest and UN Cybercrime Conventions, as well as EU MiCA regulation, a three-tier implementation framework is justified. This model encompasses accession to universal treaties, legal harmonisation within the EAEU, and domestic legislative reform. Specific de lege ferenda proposals are formulated to amend Kazakhstani payment, digital asset, criminal, and criminal procedure legislation, aimed at strengthening financial security and transaction transparency. The contribution of the study to legal scholarship is to treat the distributed ledger as a distinct object of public-law and procedural regulation, rather than as a technical tool or a speculative asset, governed by the principles of technology neutrality and functional equivalence.

Keywords: blockchain, electronic payments, internet fraud, digital assets, international legal standards, normative dualism, smart contract

Электрондық төлемдердің қауіпсіздігін қамтамасыз етудегі және интернет-алаяқтықтың алдын алудағы блокчейн технологиялар: халықаралық-құқықтық стандарттар және Қазақстан Республикасында имплементациялау келешегі

Күмісбек Айбар Аманқұлұлы*
PhD докторант
Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті
Түркістан, Қазақстан, 161200
e-mail: aibaron@yandex.ru
ORCID: https://orcid.org/0009-0007-0924-7068

Сматлаев Бауржан Мамытбекұлы
Заң ғылымдарының докторы, профессор, Заң факультетінің деканы
Л.Н. Гумилев атындағы Еуразия ұлттық университеті
Астана, Қазақстан, 010008
e-mail: smatlayev_bm@enu.kz
ORCID: https://orcid.org/0009-0006-5543-2822

Муратова Алуа Жасланқызы
Философия докторы (PhD), Заң факультетінің Қылмыстық-құқықтық пәндер кафедрасының меңгерушісі
Л.Н. Гумилев атындағы Еуразия ұлттық университеті
Астана, Қазақстан, 010008
ORCID: https://orcid.org/0000-0002-0159-9671
e-mail: muratova_azh@enu.kz

Аңдатпа. Мақалада Қазақстан Республикасындағы қолма-қол ақшасыз есеп айырысулардың жедел өсуі жағдайында электрондық төлемдердің қауіпсіздігін қамтамасыз ету және интернет-алаяқтықтың алдын алу мәселелері зерттеледі. Зерттеудің мақсаты – үлестірілген тізілімдер мен смарт-келісімшарттардың электрондық төлемдердің қауіпсіздігін қамтамасыз етуге және интернет-алаяқтыққа қарсы күреске қандай үлес қоса алатынын анықтау және халықаралық стандарттарды Қазақстан заңнамасына имплементациялау моделін ұсыну. Құқық қолдану практикасын талдау негізінде киберқылмыстардың төмен ашылу деңгейі және тіркелмеген криптовалюталық операциялардың жоғары тәуекелдері көрсетілген. Авторлар құқық бұзушылықтардың алдын алу және транзакцияларды үздіксіз бақылау үшін үлестірілген тізілімдердің, консенсус алгоритмдерінің және смарт-келісімшарттардың технологиялық әлеуетін қарастырады. Зерттеуде блокчейнді қолданудың негізгі құқықтық кедергілері, соның ішінде ұлттық жүйе мен «Астана» халықаралық қаржы орталығы режимі арасындағы нормативтік дуализм, сандық активтерді алып қоюдың процестік механизмдерінің болмауы және тізілімнің өзгермейтіндігінің жеке деректерді қорғаумен коллизиялары анықталған. ФАТФ, ЮНСИТРАЛ, Будапешт және БҰҰ киберқылмыстылыққа қарсы конвенцияларының халықаралық-құқықтық стандарттары, сондай-ақ MiCA Регламентінің тәжірибесі негізінде үш деңгейлі имплементациялау моделі негізделген. Бұл модель универсалды шарттарға қосылуды, ЕАЭО елдерінің заңнамасын үйлестіруді және отандық заңнамалық массивті кезең-кезеңімен реформалауды қамтиды. Қазақстан Республикасының «Төлемдер және төлем жүйелері туралы», «Сандық активтер туралы» Заңдарына, Қылмыстық және Қылмыстық-процестік кодекстеріне өзгерістер енгізу бойынша нақты de lege ferenda ұсыныстары тұжырымдалған. Осы шараларды енгізу трансұлттық қылмыстарды тергеу тиімділігін арттыруға және сандық есеп айырысуларға қатысушылардың құқықтық қорғалуын қамтамасыз етуге мүмкіндік береді. Зерттеудің құқық

ғылымына қосқан үлесі – үлестірілген тізілім техникалық құрал немесе алыпсатарлық актив ретінде емес, жария-құқықтық және процестік реттеудің дербес объектісі ретінде қарастырылады, ал оны реттеу технологиялық бейтараптық және функционалдық баламалылық қағидаттарына негізделуі тиіс.

Түйін сөздер: блокчейн, электрондық төлемдер, интернет-алаяқтық, сандық активтер, халықаралық-құқықтық стандарттар, нормативтік дуализм, смарт-келісімшарт.

Блокчейн-технологии в обеспечении безопасности электронных платежей и предупреждении интернет-мошенничества: международно-правовые стандарты и перспективы имплементации в Республике Казахстан

Кумисбек Айбар Аманкулулы*
PhD докторант
Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави
Туркестан, Казахстан, 161200
e-mail: aibaron@yandex.ru
ORCID: https://orcid.org/0009-0007-0924-7068

Сматлаев Бауржан Мамытбекович
Доктор юридических наук, профессор, декан Юридического факультета
Евразийский национальный университет имени Л.Н. Гумилева
Астана, Казахстан, 010008
e-mail: smatlayev_bm@enu.kz
ORCID: https://orcid.org/0009-0006-5543-2822

Муратова Алуа Жасланқызы
Доктор PhD, Заведующая кафедрой уголовно-правовых дисциплин Юридического факультета
Евразийский национальный университет имени Л.Н. Гумилева
Астана, Казахстан, 010008
ORCID: https://orcid.org/0000-0002-0159-9671
e-mail: muratova_azh@enu.kz

Аннотация. В статье исследуются проблемы обеспечения безопасности электронных платежей и предупреждения интернет-мошенничества в условиях стремительного роста безналичных расчетов в Республике Казахстан. Цель исследования – определить, что распределенные реестры и смарт-контракты могут дать для безопасности электронных платежей и противодействия интернет-мошенничеству, и предложить модель имплементации международных стандартов в законодательство Республики Казахстан. На основе анализа правоприменительной практики показана низкая раскрываемость киберпреступлений и значительный размер незарегистрированных криптовалютных операций. Авторы рассматривают технологический потенциал распределенных реестров, алгоритмов консенсуса и смарт-контрактов для предотвращения правонарушений и сквозного отслеживания транзакций. В исследовании выявлены ключевые правовые барьеры применения блокчейна, включая нормативный дуализм между национальной системой и режимом Международного финансового центра «Астана», отсутствие процессуальных механизмов изъятия цифровых активов и коллизии неизменяемости реестра с защитой персональных данных. На основе международно-правовых стандартов ФАТФ, ЮНСИТРАЛ, Будапештской и ООН конвенций против киберпреступности, а также опыта Регламента MiCA обоснована трехуровневая модель имплементации. Модель включает присоединение к универсальным международным договорам, гармонизацию законодательства стран ЕАЭС и поэтапное реформирование

отечественного законодательного массива. Сформулированы конкретные предложения de lege ferenda по внесению изменений в Законы РК «О платежах и платежных системах», «О цифровых активах», Уголовный и Уголовно-процессуальный кодексы Республики Казахстан. Внедрение данных мер позволит повысить эффективность расследования транснациональных преступлений и обеспечить правовую защищенность участников цифровых расчетов. Вклад исследования в правовую науку состоит в том, что распределенный реестр рассматривается как самостоятельный объект публично-правового и процессуального регулирования, а не как техническое средство или спекулятивный актив; его регулирование должно строиться на принципах технологической нейтральности и функциональной эквивалентности.

Ключевые слова: блокчейн, электронные платежи, интернет-мошенничество, цифровые активы, международно-правовые стандарты, нормативный дуализм, смарт-контракт.

Introduction

Between 2018 and 2023, Kazakhstan's payment infrastructure changed rapidly and deeply. The share of cashless transactions rose from under 30 percent to more than 86 percent (Kumisbek et al., 2025). Crime followed the money. As mobile banking and digital services spread, offenders moved online, and cybercrime, especially internet fraud, grew quickly.

Enforcement figures show how serious the problem is. In 2025, 28,851 cases of internet fraud were registered, and 22,426 of them (about 77.7%) were suspended. Of these suspensions, 22,338 were issued because the offender could not be identified (Article 45(1)(1) of the Criminal Procedure Code of the Republic of Kazakhstan). Only 10-14.4% of investigated cybercrimes reach the courts, and victims recover just 6.3% of their losses (Committee on Legal Statistics and Special Accounts, 2025). Unregistered crypto platforms make things worse: suspicious transactions routed through them are worth tens of billions of tenge.

Bank security rules were built for centralised settlement, and they do little against attacks that combine social engineering with AI tools. As passwords and codes lose their protective value, distributed ledger technology becomes more attractive, for researchers and practitioners alike. Blockchain rests on consensus algorithms, append-only block sequencing and distributed verification. Together these create a technological presumption that a transaction is authentic. They also make it computationally unrealistic to alter recorded entries without authorisation. With smart contracts added, funds can be traced end to end in real time, and the weak points that appear wherever a traditional intermediary sits in the chain disappear.

The difficulty is legal rather than technical. Blockchain cannot deliver its preventive potential while its legal regime remains fragmented and no common international standards exist for classifying decentralised relationships. In Kazakhstan, most dealings in unbacked digital assets are confined to the Astana International Financial Centre (AIFC). The result is a normative dualism: the state's public law on one side, a special financial enclave on the other. Distributed ledgers are decentralised and extraterritorial, so they clash directly with legal frameworks built around identifiable national intermediaries and conventional rules of jurisdiction. Internet fraud and digital-asset crime cross borders easily, and national regulation adopted in isolation cannot keep up with them. Domestic law therefore has to be brought into line with universal and regional international standards.

Research materials and methods

The study relies on official statistics from the Committee on Legal Statistics and Special Accounts of the Prosecutor General's Office of Kazakhstan for 2018-2025. The international and foreign sources are the Budapest Convention (2001, ETS No. 185) with its Second Additional Protocol (2022, CETS No. 224), the UN Convention against Cybercrime (2024, GA Resolution 79/243), the UNCITRAL MLETR (2017), the FATF standards (Recommendation 15, INR.15, the Travel Rule), ISO 22739:2024, the EU's MiCA Regulation 2023/1114 and GDPR 2016/679, EAEU acts, and the legislation of Singapore, the UAE, Switzerland, Estonia and China. At the national level,

the study examines the Constitution; the Constitutional Law "On the AIFC"; the Laws "On Digital Assets", "On Payments and Payment Systems", "On AML/CFT" and "On Legal Acts"; Articles 190, 194, 214, 216-218 and 232-1 of the Criminal Code and Article 45 of the Criminal Procedure Code; and the acts of the AIFC regulator, AFSA. The doctrinal basis is scholarship on the legal regulation of blockchain and on information law. The comparative legal method was used to build the typology of regulatory models, and the formal-dogmatic method to identify normative dualism and legislative gaps. Legal modelling was used to design the three-tier implementation system, statistical analysis to measure the scale of cybercrime, and the systemic-structural method to examine blockchain's technological and legal institutions.

Results and discussion

ISO 22739:2024 defines a blockchain as a distributed ledger built from confirmed blocks. The blocks are arranged in an append-only sequential chain and joined by cryptographic hash links[1]. This architecture is what turns the ledger from a purely technical tool into a distinct object of legal regulation. Its legally decisive feature is immutability, and a relative one: timestamps and hash chaining protect stored data, but not absolutely. Consensus mechanisms (Proof of Work, Proof of Stake) set practical limits, a 51% attack remains possible, and developers and validators can agree on a hard fork. Immutability also runs up against the law. It is hard to reconcile with the rights of data subjects, above all the "right to erasure" in Article 17 of the General Data Protection Regulation (GDPR)[2]. The doctrine of void transactions poses a similar problem: a ledger entry cannot simply be undone.

Decentralisation is the second core feature. No single administrator runs the ledger; many nodes keep it consistent. Legal scholarship separates permissionless ledgers, open to anonymous participants, from permissioned ones, where only verified entities have access. Control is shared among validators, and that makes it hard to say who bears legal responsibility. Courts and commentators have answered this in part by treating an uncoordinated division of functions among nodes as a joint venture. Participants then face joint and several liability towards third parties.

The third feature is the smart contract: code that carries out the terms of a transaction automatically once pre-set legal facts occur (De Filippi and Wright, 2018). Scholars, both international and Kazakhstani, have offered three views of its legal nature. It may be an electronic contract, a computer program, or an automated way of performing obligations. Whichever view one takes, execution is automatic and cannot be reversed, which leaves no room for open-textured standards such as "good faith" or "reasonable time". The law should therefore provide for safe interruption of execution and set rules for updating the code.

Digital networks cross borders freely, so blockchain use and payment security need international rules that overcome the split between jurisdictions. In private and commercial law, two principles developed by the United Nations Commission on International Trade Law (UNCITRAL) carry most of the weight: technology neutrality and functional equivalence. Both are set out in the 2017 Model Law on Electronic Transferable Records (MLETR)[3]. The MLETR sets legal criteria for treating electronic records as equal to paper ones. A reliable electronic method satisfies the requirements of "writing" (Article 8) and "signature" (Article 9). "Exclusive control" (Article 11) takes the place of physical possession. Article 19 forbids discrimination against an electronic transferable record because it originated abroad, which gives ledger data and smart contracts a basis for recognition in cross-border trade. UNCITRAL's models thus allow a blockchain transaction to have legal effect regardless of where its validating nodes are located.

[1] ISO 22739:2024. Blockchain and distributed ledger technologies – Vocabulary. Geneva: International Organization for Standardization, 2024

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) // Official Journal of the European Union. 2016. L 119. P. 1-88.

[3] UNCITRAL Model Law on Electronic Transferable Records (2017). UN General Assembly Resolution A/RES/72/114 of 7 December 2017. New York: United Nations, 2018.

For criminal law and the collection of digital evidence, the main international instrument is the Council of Europe Convention on Cybercrime, the Budapest Convention of 2001[4]. It harmonises offences of computer-related fraud (Article 7) and computer-related forgery (Article 8). It also regulates access to electronic evidence (Articles 14-21) and mutual legal assistance (Articles 23-35). The Second Additional Protocol of 2022 (CETS No. 224) builds on this framework. It lets law enforcement authorities work directly with platform operators and service providers in other states[5]. Under the Protocol, competent authorities may:

- request domain name registration data directly (Article 6);
- request subscriber information directly (Article 7);
- obtain traffic data quickly (Article 8);
- use the 24/7 network for emergency disclosure of stored computer data (Article 9);
- set up joint investigation teams (Article 12).

Just as important are the Protocol's strict safeguards for personal data transferred across borders (Articles 13-14). They matter directly to Kazakhstan's law enforcement practice. Kazakhstan was invited to accede to the Budapest Convention in April 2023 and is now going through implementation.

The UN Convention against Cybercrime took the universal fight against online crime a step further. The General Assembly adopted it by Resolution 79/243 of 24 December 2024[6]. The Convention was opened for signature in Hanoi in October 2025, and Kazakhstan signed it on 25 October 2025. It provides a comprehensive legal basis for criminalising offences committed through information and communication technologies and for gathering electronic evidence of serious crimes. States parties take on broad duties covering:

- mutual legal assistance;
- extradition;
- rapid exchange of information;
- confiscation of proceeds from cybercrime and online fraud.

By signing, Kazakhstan confirmed its course towards joining the global cybersecurity system. The signature also prepares the ground for aligning national criminal procedure law with universal standards.

The Financial Action Task Force (FATF) sets the key standards for financial monitoring and for stopping money laundering through digital channels (FATF, 2025a). In October 2018 the FATF substantially revised Recommendation 15. In June 2019 it adopted the Interpretive Note to it (INR.15), which extended AML/CFT/CPF requirements to virtual assets (VA) and virtual asset service providers (VASPs). The FATF defines a virtual asset as a digital representation of value that can be traded or transferred digitally and used for payment or investment. Under INR.15, states must:

- license or register VASPs where they are created or do business;
- supervise them on a risk-based basis;
- keep criminals from owning or controlling them.

For occasional transactions, customer due diligence (CDD) applies from USD/EUR 1,000 (paragraph 7(a) INR.15).

The Travel Rule is central to fighting anonymous fraudulent payments. It comes from paragraph 7(b) of INR.15, which refers to Recommendation 16 on transparency of wire transfers. When virtual assets are transferred, the originating VASP must obtain and hold accurate information on both the originator and the beneficiary. It must then pass that information, immediately and securely, to the beneficiary VASP or financial institution (FATF, 2025b).

[4] Convention on Cybercrime (ETS No. 185). Budapest, 23 November 2001. Council of Europe.
[5] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Strasbourg, 12 May 2022. Council of Europe.
[6] United Nations Convention against Cybercrime. UN General Assembly Resolution A/RES/79/243 of 24 December 2024. New York: United Nations, 2024.

More and more states are adopting the necessary legislation, 83% by 2026 according to the FATF Targeted Updates for 2025 and 2026. Yet implementation is still held back by the "Sunrise Issue": jurisdictions introduce the rule at different times, so compliant providers often deal with counterparts that are not yet bound by it (FATF, 2025c; FATF, 2026).

The payment sector also faces structural risks:

– offshore VASPs;
– peer-to-peer (P2P) transfers through unhosted wallets, which remain largely unsupervised;
– decentralised finance (DeFi) protocols, to which prudential requirements are hard to apply.

Universal international law provides a common framework of standards for digital transactions and cybersecurity. That framework works in practice only when regional bodies, including integration associations, align their institutions and rules with it.

The European Union has built the most complete regional framework for digital financial assets. Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA) divides crypto-assets into three categories: utility tokens (UT), asset-referenced tokens (ART) and electronic money tokens (EMT)[7]. EMTs count as "funds" in law. They therefore fall under the safeguards of Directive (EU) 2015/2366 (PSD2) and of the PSD3/PSR package now being drafted. Unbacked crypto-assets such as Bitcoin fall outside the payment services directives altogether. So a person who pays in unbacked crypto-assets has no statutory right to have errors corrected or losses refunded after an unauthorised transaction or payment fraud. Such users are much less protected than those who pay in fiat currency or EMTs (Christensen, 2025). Because of this gap, EU lawmakers are now discussing whether financial liability rules should cover every kind of digital means of payment.

The EU has also renewed its anti-money laundering rules to close off regulatory arbitrage and illicit flows. The new AML package comprises four acts:

– Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (the Travel Rule);
– Regulation (EU) 2024/1624 (AMLR);
– Directive (EU) 2024/1640 (AMLD6);
– Regulation (EU) 2024/1620 establishing the Anti-Money Laundering Authority (AMLA).

Under this framework, crypto-asset service providers (CASPs) count as financial institutions. They must be authorised, carry out full customer due diligence (CDD) and monitor transactions. Regulation 2023/1113 requires CASPs to obtain, hold and promptly pass on originator and beneficiary data for every crypto-asset transfer, with no minimum amount. Anonymous crypto accounts and anonymity-enhancing coins are banned outright. AMLA centralises supervision of the riskiest crypto-sector entities and coordinates national financial intelligence units (FIUs).

In EU law, the deepest structural problem for blockchain is its conflict with the General Data Protection Regulation (EU) 2016/679. Article 17 GDPR gives a right to erasure (the "right to be forgotten"), and Article 16 gives a right to have inaccurate data corrected. A blockchain only adds new blocks and never deletes old ones, so stored records cannot be amended. Public networks add a further problem: often no identifiable data controller exists at all. Data protection law then short-circuits, because no one can be held to account. EU scholarship and regulators have discussed several legal and technical compromises: sidechains, privately governed ledgers, and a "Privacy by Layers" model that keeps personal data off-chain and records only cryptographic hashes on the ledger.

In private international law and trade facilitation, the common benchmarks come from UNCITRAL and the OECD. As shown above, the MLETR (2017) rests on technology neutrality and functional equivalence. Exclusive control, replacing physical possession, is what allows blockchain ledgers to be used lawfully for documents of title, bills of lading and smart contracts.

[7] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 // Official Journal of the European Union. 2023. L 150. P. 40-205.

In the Eurasian Economic Union (EAEU), regional harmonisation has barely begun. The EAEU Digital Agenda is under way, but there is still no supranational regulation of crypto-assets, virtual currencies or smart contracts. The member states (Armenia, Belarus, Kazakhstan, Kyrgyzstan and Russia) take very different approaches:

- Belarus has a preferential permissive regime under Decree No. 8;
- Russia has dedicated legislation on digital financial assets;
- Kazakhstan has a dual regulatory structure.

With no shared concepts and no mutual recognition of digital rights, businesses can shop between regimes and cross-border settlement becomes harder. Digital channels also become easier to use for evading financial controls. The EAEU therefore needs model acts that are consistent with FATF and UNCITRAL standards and with the principle of "same activity, same risk, same regulation".

The comparative analysis at the regional level shows two main directions. The EU imposes strict prudential supervision on digital payment infrastructure. The UNCITRAL MLETR model brings functional equivalence into commercial dealings. Against both, the fragmented treatment of digital assets in the EAEU is a serious obstacle to the bloc's economic security. Foreign experience in resolving these conflicts should be organised into a general typology of national regulatory models. The country-level analysis that follows will help identify how Kazakhstan can best implement international standards.

National approaches to regulating blockchain and digital assets differ widely.

Singapore regulates virtual asset service providers (VASPs) by function under the Payment Services Act 2019 (PSA), with the Monetary Authority of Singapore (MAS) as supervisor. Its model combines:

- tiered VASP licensing;
- the Travel Rule;
- thematic inspections of platforms;
- continuous monitoring of the risks posed by transfers to unhosted wallets.

The United Arab Emirates has a multi-tier structure. Its financial free zones, the Dubai International Financial Centre (DIFC) and Abu Dhabi Global Market (ADGM), make their own rules on the basis of English common law. ADGM adopted the principles of the UNCITRAL MLETR in 2021, and Dubai established the Virtual Assets Regulatory Authority (VARA) in 2022. The result is a flexible environment: the jurisdictions coordinate with each other and recognise each other's powers, while capital adequacy requirements stay strict.

In Europe, Switzerland is the leading example of building DLT into the legal system. Its Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT Act, 2020) built on the FINMA token classification into utility, payment and asset tokens. The Act made two main changes: it added ledger-based securities (Registerwertrechte) to the Code of Obligations, and it created a separate licence for DLT trading facilities.

Estonia went further in bringing digital tools into public law. It tied VASP regulation to its AML/CFT legislation and to automated monitoring systems. Strict licensing of crypto exchanges and fast cooperation with foreign police have helped it break up large cross-border fraud schemes. One joint investigation concerned schemes worth USD 575 million.

China sits at the opposite pole, with a strictly prohibitive model for private virtual assets. The People's Bank of China and other authorities have banned ICOs, crypto exchanges, mining and any payment or investment use of unbacked digital assets. At the same time, the state has taken up blockchain for its own purposes. The national Blockchain-based Service Network (BSN) is connected to the Internet Courts, which use it to record, verify and store electronic evidence automatically. The Chinese state is selective: it puts distributed ledgers to work for public control and the courts but blocks them entirely as a decentralised means of payment.

From this experience, national approaches to blockchain in payments can be grouped into three models: permissive, framework and prohibitive.

1. The permissive (specialised and pro-innovation) model (Switzerland, Singapore, UAE/ADGM, Estonia) relies on dedicated legislation. It gives detailed legal recognition to digital rights and smart contracts, offers favourable regulatory regimes, and fully integrates VASPs into the financial system, provided they meet FATF standards;

2. The framework (hybrid and adaptive) model (the EU under MiCA) extends general financial and prudential rules to digital assets step by step. Requirements are scaled to systemic risk, and authorised providers can "passport" their services across member states (Zetzsche et al., 2021);

3. The prohibitive (restrictive) model (China, Egypt, Morocco) bans private digital currencies and VASP activity in whole or in part. The aims are to protect monetary sovereignty and limit money-laundering risk.

The analysis at the universal, regional and national levels points to a clear global trend: crypto activity is being brought out of legal uncertainty and under prudential supervision. The typology shows that a state's choice of model depends on two things. One is how ready its legal system is to absorb decentralised institutions. The other is where it sets the balance between encouraging innovation and protecting financial security. Taken together, the Budapest Convention, the 2024 UN Convention, FATF Recommendation 15, the UNCITRAL MLETR and MiCA form the reference framework against which national law should be measured. Kazakhstan therefore needs a critical review in light of its international obligations. That review should assess how far its laws meet FATF standards and how the current institutional dualism can be overcome.

Law of the Republic of Kazakhstan No. 193-VII "On Digital Assets in the Republic of Kazakhstan" of 6 February 2023 laid the legal foundation for state regulation of digital property[8]. Article 1 defines a digital asset as property that meets four conditions:

- it exists in electronic digital form and carries a digital code;
- it is recorded on a distributed data platform;
- that platform keeps the information unalterable;
- it is neither legal tender nor a unit of account.

The Law separates two kinds of digital asset. Secured digital financial assets are one kind. Unsecured digital assets, earned in an information system as a reward for helping maintain blockchain consensus, are the other. Digital mining is regulated in detail as a licensed business, with requirements for mining pools and for registers of hardware and software systems. Nationwide, however, the issue and circulation of unsecured digital assets, meaning cryptocurrencies, was heavily restricted. At first they could circulate lawfully only under a special legal regime or through specially licensed providers.

Retail finance is regulated separately by Law No. 11-VI "On Payments and Payment Systems" of 26 July 2016. This law governs payment services, the issue of electronic money and the operation of payment infrastructure[9]. Later amendments introduced the National Digital Financial Infrastructure, which comprises: the National Payment System; open banking; the Digital Tenge platform; the National Bank's Anti-Fraud Centre, which exchanges data on payment transactions showing signs of fraud.

Once the Digital Tenge platform and its smart contracts were written into law, programmable settlement became possible, along with automated checks that public and commercial funds are used for their intended purpose. Still, payment law is built around centralised institutions. When an unauthorised or fraudulent transfer happens in a decentralised P2P network, the law gives no workable way to decide who bears responsibility.

Criminal law protection in this field rests on the Criminal Code, and most cybercrime is charged as fraud under Article 190. In digital-crime cases, law enforcement also applies: Article 194

[8] Закон Республики Казахстан от 6 февраля 2023 г. № 193-VII «О цифровых активах в Республике Казахстан».

[9] Закон Республики Казахстан от 26 июля 2016 г. № 11-VI «О платежах и платёжных системах» // Ведомости Парламента РК. 2016. № 12. Ст. 86.

(extortion); Article 216 (issuing invoices without actual performance of work); Article 217 (creating and running a financial pyramid); Article 218 (laundering criminal proceeds); Article 232-1 (unlawful access to bank accounts and payment instruments).

A significant gap remains. The Code has no separate offences of computer-related fraud or unlawful manipulation of data, which Articles 7 and 8 of the Budapest Convention provide for. Without them, courts must fit specific attacks on DLT platforms and smart contracts into the general wording of Article 190. That makes it hard to tell a civil-law risk from a crime.

Kazakhstan's most distinctive institutional feature is the Astana International Financial Centre (AIFC). It operates under Constitutional Law No. 438-V of 7 December 2015[10]. The AIFC has a special financial regime based on the principles and norms of the law of England and Wales, and its working language is English. Its regulator, the Astana Financial Services Authority (AFSA), makes separate rules for Centre participants, licenses digital asset exchanges and runs a regulatory sandbox.

The result is a marked dualism between the state's continental legal system and the AIFC enclave. This dualism has created a conflict in practice. Kazakhstani citizens have faced prosecution under Article 214 of the Criminal Code (illegal entrepreneurship) for buying, selling or exchanging cryptocurrency without an AFSA licence. S.K. Idrysheva (2025) rightly notes three problems with AIFC acts:

– they are not issued in the name of the Republic of Kazakhstan;
– they exist only in English;
– they appear only on the Centre's website, not in the official state publications in Kazakh and Russian.

This conflicts directly with Article 4(4) of the Constitution and with Article 37 of the Law "On Legal Acts". Under these, an act that affects citizens' rights and duties and has not been published in the manner the state requires cannot be applied. Investigators and courts therefore cannot rely on such acts to establish the objective element of an offence.

Kazakhstan's legislation shows systemic gaps, caused by normative dualism, blanket cross-references and procedural uncertainty. The AIFC's permissive, pro-innovation regime operates alone, while national law keeps only piecemeal restrictions, and this weakens the response to cross-border internet fraud. Domestic law should therefore move away from the "enclave plus prohibition" arrangement towards a single national framework model of the adaptive kind. The next step is to examine how Kazakhstan is meeting its international obligations: what the FATF mutual evaluation found and what accession to the Budapest Convention would involve.

After its 2023 mutual evaluation by the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), Kazakhstan was placed under regular follow-up (EAG, 2023). The 1st Regular Follow-Up Report (EAG, 2026) found better technical compliance. Four ratings rose from "partially compliant" (PC) to "largely compliant" (LC):

– Recommendation 6, targeted financial sanctions for terrorist financing;
– Recommendation 7, sanctions for proliferation financing;
– Recommendation 24, beneficial ownership transparency;
– Recommendation 26, regulation and supervision of financial institutions.

These upgrades followed Law No. 219-VIII of 19 September 2025, which amended the AML/CFT/CPF framework[11]. The amending law banned shell banks outright, tightened the rules on beneficial owners, and required every natural and legal person to freeze assets when required.

Recommendation 15 on new technologies matters most for digital payments, and it stayed at PC after the 2023 evaluation. Two gaps explain the rating: the Travel Rule was not set out in

[10] Конституционный закон Республики Казахстан от 7 декабря 2015 года № 438-V «О Международном финансовом центре «Астана»» // https://adilet.kz/ru/laws/o-mezhdunarodnom-finansovom-tsentre-astana-07-12-2015-no-438-v/

[11] Закон Республики Казахстан от 28 августа 2009 г. № 191-IV «О противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения» (с изменениями, внесёнными Законом РК от 19 сентября 2025 г. № 219-VIII) // Ведомости Парламента РК. 2009. № 19. Ст. 88.

legislation, and crypto transactions outside the AIFC were not effectively supervised. Kazakhstan has since taken steps. It has worked on implementing the Travel Rule, carried out a National Risk Assessment (NRA) and inspected VASPs. The FATF targeted updates for 2025 and 2026 still report practical difficulties, though: those who control DeFi protocols are hard to identify, and anonymous P2P transfers through unhosted wallets are hard to stop.

Kazakhstan's second major line of international integration is accession to the Budapest Convention. The Council of Europe invited it to accede on 19 April 2023, and the invitation is valid for five years. Under the accession roadmap, a coordination seminar was held in Astana in November 2024 within the Octopus Project. Key state bodies took part and agreed on steps to harmonise national law and to strengthen law enforcement capacity to collect electronic evidence.

Kazakhstan's criminal law and criminal procedure law still differ from the Convention in important ways. As shown above, substantive law has no offences of computer-related fraud (Article 7) or computer-related forgery (Article 8), so manipulation of payment data has to be charged under Article 190. Procedural law has a gap as well. The Criminal Procedure Code only partly regulates the seizure of electronic media. It has no clear procedure for expedited preservation of data by service providers, which the Convention's procedural provisions require (Articles 14-21). As a result, digital traces may disappear before a court authorises their collection.

Cross-border fraud is hard to stop for another reason. Kazakhstan has no established rules for its law enforcement bodies to deal directly with foreign internet service providers (ISPs). It also makes little use of the 24/7 network under Article 35 of the Convention. In 2025, 77.4% of internet fraud investigations were suspended because the offender could not be identified, and only 6.3% of losses were recovered (Committee on Legal Statistics and Special Accounts, 2025). Much of this comes down to delay: traditional mutual legal assistance (MLA) requests go through diplomatic channels and take a long time to send and execute. Germany, Estonia and the United States show what full participation in the Convention and its 2022 Second Additional Protocol makes possible: joint investigation teams (JITs), and traffic and registration data obtained directly from foreign platforms within much shorter deadlines.

The compliance review leads to one conclusion. Closing these gaps means removing procedural barriers and, beyond that, resolving the systemic normative dualism inside Kazakhstan's own legal order. The conflicts between national legislation and the AIFC regime therefore need closer examination.

Kazakhstan's current legislation has three systemic gaps that weaken the fight against internet fraud and illicit dealings in digital assets.

The first is the institutional dualism described above: a normative gap separates the AIFC enclave from the national continental system. The Law "On Digital Assets" and the Law "On Payments and Payment Systems" either restrict dealings in unsecured digital assets or tie them to specialised providers operating under the AIFC regime.

The second gap is procedural. Criminal procedure law gives no workable way to freeze, seize or confiscate digital assets. The 2023 EAG Mutual Evaluation Report (EAG, 2023) notes that neither the Criminal Procedure Code nor the implementing Government Resolutions No. 1291 and No. 833 set out how virtual assets are to be seized and managed. In practice, cryptocurrency is seized only when a suspect voluntarily hands over the private keys or wallet access. If the suspect refuses, or quickly moves the assets into a decentralised protocol, investigators have no legal tools left. Courts then fall back on recovering the monetary equivalent from the convicted person. Article 4 of the Law "On Digital Assets" provides for a single register, kept by the financial monitoring authority, of wallets used for criminal purposes. Three questions remain unregulated:

- how investigators are to cooperate with platform operators;
- how DLT addresses can be temporarily frozen;
- how confiscated crypto-assets are to be held until a verdict is reached.

The third gap lies in civil law: the smart contract has no settled place as a form of transaction. As Imangalieva observes, Kazakhstani law knows only the general concept of an electronic

document, and a smart contract does not meet it. A smart contract is written in program code and works without an electronic digital signature (Imangalieva, 2023). Its "if-then" logic is rigid and leaves no room for open-ended standards such as good faith, reasonable time or business risk. Execution is automatic and cannot be reversed. Article 401 of the Civil Code, by contrast, lets a contract be amended or terminated by agreement of the parties or by a court.

The consequences are sharpest in fraud cases such as "rug pulls" and "pump-and-dump" schemes, and when serious flaws in the code come to light. The decentralised ledger then offers no "kill switch" to halt a transaction. Classic tort and contract liability also struggle to identify the proper defendant (Romanenko, 2023).

The dualism between jurisdictions, the lack of procedural tools for seizing crypto-assets and the legal uncertainty around smart contracts largely cancel out blockchain's preventive potential in Kazakhstan. Isolated amendments will not fix these internal contradictions, because distributed ledgers are decentralised and cross-border by nature. Aligning national law with international standards requires deciding under what conditions, and within what limits, those standards should be implemented. The next section therefore turns to the cross-border use of blockchain and to mechanisms of international cooperation.

A distributed ledger is extraterritorial and decentralised, so it has no single geographic centre to which the law can attach. Validating nodes and transacting parties are spread across many jurisdictions. A digital asset may thus be said to sit in many places at once, or in none, and the ordinary connecting factors of private international law stop working (Zhaksylykbaeva, 2024). The lex rei sitae rule is the clearest casualty. Scholars reject tying a virtual asset to the location of particular servers, because data can be moved or copied instantly and at almost no cost. Party choice of law (lex voluntatis) does not fill the gap either, because participants in public networks are largely pseudonymous and so can hardly agree on anything. The result is a structural shortage of legal certainty.

A second problem is identifying the person who is responsible. Public ledgers have no single operator or central governing body. When an unauthorised transaction or a software failure causes loss, it is unclear who must pay. Civil-law scholarship sometimes treats the joint operation of validating nodes and protocol developers as a joint venture or a general partnership. On that view, all key network participants may face joint and several, or shared, liability. Regulators in practice look for anchor points they can actually reach: core developers, operators of large validating nodes and licensed VASPs.

Because national approaches to digital assets differ so much, they invite regulatory arbitrage and forum shopping. People who run illicit schemes or unregulated platforms deliberately move to jurisdictions with weak financial controls and no Travel Rule. Unified international instruments offer a way out, notably the UNCITRAL MLETR and the UNIDROIT Principles on Digital Assets and Private Law. If cross-border payment disputes are to have predictable outcomes, conflict-of-laws rules must first be harmonised internationally.

The sharpest legal conflict in using blockchain for payments is between the ledger's immutability and data protection law. GDPR, like many national laws, grants three rights:

- erasure, the "right to be forgotten" (Article 17);
- rectification of inaccurate data (Article 16);
- restriction of processing (Article 18).

A classic blockchain cannot honour any of them. It only appends new blocks and cannot delete earlier ones (Finck, 2019). In a public network every node holds a full copy of the ledger, so writing personal data into the chain amounts to publishing it permanently. If no identifiable data controller exists, the data subject has no one to bring a claim against to stop unlawful processing.

Pseudonymisation and encryption have been proposed as ways to take ledgers outside data protection law. Most scholars find them insufficient. Research shows that metadata analysis and transaction-graph matching can link pseudonymous wallet addresses to their real owners. A more promising legal and technical compromise is "Privacy by Layers", used together with governed

sidechains or private consortium ledgers. Personal data stays off-chain in secure databases run by a designated operator. The ledger stores only immutable cryptographic hashes, from which the original content cannot be recovered without the key.

Article 22 GDPR raises a further difficulty. It gives individuals the right not to be subject to decisions based solely on automated processing, including profiling, where those decisions have legal or similarly significant effects. Smart contracts in payment systems execute automatically. Where the outcome legally affects an individual, a human-in-the-loop safeguard may therefore be needed, which is hard to reconcile with the program's autonomy. In practice, privacy is balanced against the public interest in transparent transactions through legal criteria that define when there is a legitimate interest in accessing ledger records. Resolving data protection conflicts ultimately means giving up radical decentralisation in favour of hybrid solutions in which a legally responsible person is clearly identified.

Digital assets cross borders in seconds, and the parties are pseudonymous. Traditional mutual legal assistance (MLA) through diplomatic channels is far too slow for this. The procedural tools of the Budapest Convention (2001) and its Second Additional Protocol (2022, CETS No. 224), built for fast collection of electronic evidence, therefore matter a great deal.

Article 35 of the Convention requires states to maintain contact points available around the clock, the 24/7 network. These contact points can secure the expedited preservation of computer and traffic data before a court authorises disclosure. The Protocol builds on this network with emergency procedures (Articles 9-10). Article 12 of the Protocol adds joint investigation teams (JITs). Once the states concerned have concluded an agreement, the team carries out coordinated investigative steps without a separate MLA request for each one.

Articles 6 and 7 of the Protocol broke new ground in international procedural law. Competent authorities may now ask foreign registrars and service providers directly for domain name registration data and subscriber information. The 2024 UN Convention against Cybercrime extends these tools. It sets universal obligations for joint evidence gathering and confiscation of proceeds across all serious offences.

The FATF standards point the same way. Recommendations 37-40 and the 2026 targeted update expect financial intelligence units and supervisors to use informal operational channels to trace and freeze stolen virtual assets quickly, namely: Egmont Secure Web; the ARIN and CARIN asset-recovery networks; Interpol's I-24/7 system.

Using these channels shortens the delay in following funds along cross-border DLT chains.

Public-private partnership (PPP) between state bodies and the private operators of digital platforms is a separate route to safer payments. VASPs, large crypto exchanges and blockchain analytics firms can watch DLT networks in real time, which state bodies usually cannot do on their own. Several tools in combination can stop stolen assets before they are cashed out into fiat:

- automated on-chain analysis;
- shared blacklists of compromised addresses;
- algorithms that flag anomalous activity;
- stablecoin issuers freezing tokens at the request of law enforcement.

This hybrid approach makes up for the missing central administrator in decentralised networks. Control shifts to the institutions at the points where money enters and leaves the crypto ecosystem.

Building on the analysis above, this article proposes a three-tier model for implementing international standards: from universal standards, through regional harmonisation within the EAEU, to national implementation. The model is meant to overcome regulatory fragmentation and to integrate Kazakhstan fully into the global financial security architecture.

The first, universal tier consists of global instruments and prudential frameworks:

- the Budapest Convention (2001) with its Second Additional Protocol (2022);
- the UN Convention against Cybercrime (2024);
- the FATF Recommendations, in particular Recommendation 15 and the Travel Rule;

– the UNCITRAL MLETR.

This tier supplies shared concepts and the functional-equivalence principle for electronic records. It also imposes core obligations to criminalise cyber fraud and to collect digital evidence. Together these ensure that digital records have legal effect and that competent authorities can cooperate across borders.

The second, regional tier calls for deep harmonisation within the EAEU. Its purpose is to shut down regulatory arbitrage and build a single legal space for digital payments. The EAEU currently has no supranational rules on digital assets. A model EAEU law "On Digital Assets and Virtual Currencies" could fill this gap, drawing on MiCA and on the principle of "same activity, same risk, same regulation". At the regional level, the model provides for:

– a common VASP authorisation procedure;
– mutual recognition of electronic digital signatures and smart contracts;
– a shared register of rogue platforms, to stop funds being moved out across borders.

Harmonised member-state laws would close channels for illicit capital flight and strengthen the economic security of the Union as a whole.

The third, national tier requires a step-by-step reform of Kazakhstani law that ends the dualism between the national legal order and the AIFC. Four de lege ferenda proposals follow from the analysis.

The first proposal concerns payments and digital asset legislation. The Law "On Payments and Payment Systems" and the Law "On Digital Assets" should gain technology-neutral definitions of "distributed ledger", "blockchain" and "smart contract", and transactions recorded on the ledgers of licensed VASPs should carry the same legal weight as official payment records.

The second proposal concerns the Criminal Code. It should contain separate offences of computer-related fraud and computer-related forgery, in line with Articles 7 and 8 of the Budapest Convention.

The third proposal concerns the Criminal Procedure Code. It needs procedures for freezing and confiscating virtual assets and for seizing private keys, together with a rebuttable presumption that blockchain records are authentic.

The fourth proposal concerns the AIFC. Every AFSA act should be officially published in Kazakh and Russian. A single national VASP licensing regime and the Travel Rule should apply throughout the country, while the AIFC sandbox remains open to innovative start-ups.

Taken together, these measures join Kazakhstan's international obligations, its EAEU integration and the domestic protection of its financial market into one coherent structure. Introduced in stages, they would lower the legal and technical barriers created by decentralisation and give investigators and courts better tools against cross-border theft. People who pay electronically would also be better protected. The expected result is a stronger preventive effect against internet fraud and a stable legal basis for the digital economy.

Conclusion

This study examined what distributed ledgers and smart contracts can contribute to the security of electronic payments and to the fight against internet fraud, and it proposed a model for bringing international standards into Kazakhstani law. Five methods were combined: comparative legal analysis for the typology of foreign regimes, formal-dogmatic analysis to identify normative dualism and gaps in legislation, legal modelling for the three-tier implementation system, statistical analysis of Prosecutor General's Office data, and systemic-structural analysis of blockchain's legal nature. The analysis confirmed two conflicts that no technical design can remove: ledger immutability collides with data protection law, above all the GDPR right to erasure, and the rigid logic of smart contracts cannot be squared with the civil-law rules on amending and terminating contracts or with the requirement of good faith. On the basis of the experience of the EU, Singapore, the UAE, Switzerland, Estonia and China, three regulatory models were distinguished: permissive, framework and prohibitive.

Three systemic defects were found in Kazakhstani law. The first is the dualism between the national legal order and the AIFC: because AFSA acts are not officially published in the state and official languages, citizens may be held criminally liable on a questionable legal basis. The second is procedural: the Criminal Procedure Code provides no means of freezing, seizing or confiscating virtual assets. The third is substantive: the Criminal Code has no offences of computer-related fraud or computer-related forgery. The findings support the article's central claim. Blockchain's preventive potential in payments cannot be realised under isolated bans or under regulation confined to an enclave. The contribution to legal scholarship is to treat the distributed ledger as a distinct object of public-law and procedural regulation, rather than as a technical tool or a speculative asset, and to govern it by the principles of technology neutrality and functional equivalence. The article accordingly argues that Kazakhstan should move from its "enclave plus prohibition" arrangement to a single adaptive national framework, connected to the Travel Rule and to international channels for collecting electronic evidence.

The practical proposals de lege ferenda follow from this. The Laws "On Payments and Payment Systems" and "On Digital Assets" should contain technology-neutral definitions of "distributed ledger", "blockchain" and "smart contract", and entries in the ledgers of licensed VASPs should carry the same legal force as official payment documents. The Criminal Code should criminalise computer-related fraud and forgery in line with Articles 7 and 8 of the Budapest Convention, and the Criminal Procedure Code should regulate the rapid freezing of digital assets, the seizure of private keys and a rebuttable presumption that blockchain records are authentic. AFSA acts should be officially published in Kazakh and Russian, and a single national VASP licensing regime and the Travel Rule should apply nationwide, while the AIFC keeps its role as a regulatory sandbox. Further research could take three directions: an EAEU model act on digital assets and virtual currencies, layered data protection architectures ("Privacy by Layers"), and public-private partnerships between law enforcement and blockchain analytics firms for monitoring anonymous transactions in DeFi and in unsecured digital assets.

References

Christensen, L.D. (2025). “Crypto payments – a danger to consumer protection?”, Vol. 7, Art. 100124, *Journal of Economic Criminology*. DOI: 10.1016/j.jeconcrim.2024.100124.

Committee on Legal Statistics and Special Accounts of the Prosecutor General’s Office of the Republic of Kazakhstan (2025). *Statistical reports, available at: https://qamqor.gov.kz/crimestat/statistics*. Accessed: [07.11.2025].

De Filippi, P. and Wright, A. (2018), *Blockchain and the Law: The Rule of Code*, Harvard University Press, Cambridge, MA.

Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) (2023), *Anti-money laundering and counter-terrorist financing measures – Kazakhstan. Mutual Evaluation Report*, EAG, Moscow.

Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) (2026), *1st Regular Follow-Up Report of Kazakhstan*, EAG, Moscow.

FATF (2025a), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (The FATF Recommendations), FATF/OECD, Paris.

FATF (2025b), *Best Practices on Travel Rule Supervision*, FATF/OECD, Paris.

FATF (2025c), *Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, FATF/OECD, Paris.

FATF (2026), *Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, FATF/OECD, Paris.

Finck, M. (2019), *Blockchain Regulation and Governance in Europe*, Cambridge University Press, Cambridge.

Zetzsche, D.A., Annunziata, F., Arner, D.W. et al. (2021). "The Markets in Crypto-Assets Regulation (MiCA) and the EU Digital Finance Strategy", Vol. 16, No. 2, *Capital Markets Law Journal*, pp. 203–225.

Жаксылыкбаева, А.А. (2024). "Правовое регулирование цифровых активов и коллизионные вопросы международного частного права", № 3 (111), *Научный журнал «Туран»*, pp. 146–156.

Идрышева, С.К. (2025). "Акты Международного финансового центра «Астана» и система законодательства Республики Казахстан", № 2 (107), *Право и государство*, pp. 35-43. DOI: 10.51634/2307-5201_2025_2_35.

Имангалиева, А.Д. (2023). "Вопросы правового регулирования сделок (смарт-контрактов), заключённых с применением блокчейн-технологий", *ИС «ПАРАГРАФ»*, available at: https://prg.kz/document?doc_id=32563081. Accessed: [14.11.2025].

Кумисбек, А.А., Медетов, А.Ш., Кожамбеков, Д.Р. et al. (2025). "О технологии блокчейн и безопасности электронных платежей: борьба с интернет-мошенничеством в Казахстане", Т. 116, № 4, *Вестник КазНУ. Серия юридическая*, pp. 163–178. DOI: 10.26577/JAPJ2025116414.

Романенко, С.В. (2023). "Вопросы регулирования правоотношений в сфере производства и обращения цифровых активов, противодействия коммерческому мошенничеству", Т. 106, № 2, *Вестник КазНУ. Серия юридическая*, pp. 47–55. DOI: 10.26577/JAPJ.2023.v106.i2.05.

References (transliterated)

Christensen, L.D. (2025). "Crypto payments – a danger to consumer protection?", Vol. 7, Art. 100124, *Journal of Economic Criminology*. DOI: 10.1016/j.jeconcrim.2024.100124.

Committee on Legal Statistics and Special Accounts of the Prosecutor General's Office of the Republic of Kazakhstan (2025). *Statistical reports, available at: https://qamqor.gov.kz/crimestat/statistics*. Accessed: [07.11.2025].

De Filippi, P. and Wright, A. (2018), *Blockchain and the Law: The Rule of Code*, Harvard University Press, Cambridge, MA.

Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) (2023), *Anti-money laundering and counter-terrorist financing measures – Kazakhstan. Mutual Evaluation Report*, EAG, Moscow.

Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) (2026), *1st Regular Follow-Up Report of Kazakhstan*, EAG, Moscow.

FATF (2025a), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (The FATF Recommendations), FATF/OECD, Paris.

FATF (2025b), *Best Practices on Travel Rule Supervision*, FATF/OECD, Paris.

FATF (2025c), *Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, FATF/OECD, Paris.

FATF (2026), *Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, FATF/OECD, Paris.

Finck, M. (2019), *Blockchain Regulation and Governance in Europe*, Cambridge University Press, Cambridge.

Idrysheva, S.K. (2025). "Akty Mezhdunarodnogo finansovogo tsentra «Astana» i sistema zakonodatelstva Respubliki Kazakhstan" [Acts of the Astana International Financial Centre and the legislative system of the Republic of Kazakhstan], No. 2 (107), *Pravo i gosudarstvo*, pp. 35–43. DOI: 10.51634/2307-5201_2025_2_35.

Imangalieva, A.D. (2023). "Voprosy pravovogo regulirovaniia sdelok (smart-kontraktov), zakliuchennykh s primeneniem blokchein-tekhnologii" [Issues of legal regulation of

transactions (smart contracts) concluded using blockchain technologies], *IS «Paragraf»*, available at: https://prg.kz/document?doc_id=32563081. Accessed: [04.01.2026].

Kumisbek, A.A., Medetov, A.Sh., Kozhambekov, D.R. et al. (2025). "O tekhnologii blokchein i bezopasnosti elektronnykh platezhei: borba s internet-moshennichestvom v Kazakhstane" [On blockchain technology and the security of electronic payments: combating internet fraud in Kazakhstan], Vol. 116, No. 4, *Vestnik KazNU. Seriia iuridicheskaia*, pp. 163–178. DOI: 10.26577/JAPJ2025116414.

Romanenko, S.V. (2023). "Voprosy regulirovaniia pravootnoshenii v sfere proizvodstva i obrashcheniia tsifrovykh aktivov, protivodeistviia kommercheskomu moshennichestvu" [Issues of regulating legal relations in the production and circulation of digital assets and countering commercial fraud], Vol. 106, No. 2, *Vestnik KazNU. Seriia iuridicheskaia*, pp. 47–55. DOI: 10.26577/JAPJ.2023.v106.i2.05.

Zetzsche, D.A., Annunziata, F., Arner, D.W. et al. (2021). "The Markets in Crypto-Assets Regulation (MiCA) and the EU Digital Finance Strategy", Vol. 16, No. 2, *Capital Markets Law Journal*, pp. 203–225.

Zhaksylykbaeva, A.A. (2024). "Pravovoe regulirovanie tsifrovykh aktivov i kollizionnye voprosy mezhdunarodnogo chastnogo prava" [Legal regulation of digital assets and conflict-of-laws issues in private international law], No. 3 (111), *Nauchnyi zhurnal «Turan»*, pp. 146–156.

The contribution of the authors

Kumisbek A.A. – research concept, collection and analysis of materials, preparation of the manuscript.

Smatlayev B.M. – research methodology, scientific supervision, critical revision of the manuscript.

Muratova A.Zh. – analysis of the criminal law and criminal procedure aspects, editing of the manuscript.

Funding: This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP26103625 "Online fraud using deepfake-technologies and social engineering: Problems of criminal law counteraction, prospects for legislative regulation").

Conflict of interest: the authors declare no conflict of interest.