МРНТИ 10.77.01 https://doi.org/10.26577/JAPJ2025116414

**А.А. Кумисбек[1], А.Ш. Медетов[1*], Д.Р. Кожамбеков[1], С.У. Ахмет[2], М.П. Байбосынов[2]**

[1]Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, Туркестан, Казахстан
[2]Центрально-Азиатский инновационный университет, Шымкент, Казахстан
*e-mail: alimardin.medetov@ayu.edu.kz

# О ТЕХНОЛОГИИ БЛОКЧЕЙН И БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ: БОРЬБА С ИНТЕРНЕТ-МОШЕННИЧЕСТВОМ В КАЗАХСТАНЕ

Каким образом право может соответствовать темпам развития технологий, фундаментально преобразующих финансовые транзакции? Настоящая статья обращается к данному вопросу посредством исследования роли блокчейна в обеспечении безопасности электронных платежей и противодействии кибермошенничеству в правовом поле Казахстана. Анализ прослеживает технологию распределенного реестра от её криптографических основ до регуляторного регулирования в трёх юрисдикциях – Европейском союзе, Объединенных Арабских Эмиратах и собственно Казахстане. Опираясь на статистику киберпреступлений за 2024–2025 годы и формирующуюся судебную практику, исследование выявляет центральное противоречие: децентрализованный вопрос блокчейна вступает в конфликт с правовыми рамками, выстроенными вокруг идентифицируемых посредников.

Полученные результаты указывают на то, что можно обозначить как «презумпцию подлинности транзакции» – новаторскую доказательственную концепцию, обеспечиваемую криптографической верификацией. Вместе с тем сохраняются существенные препятствия. Суды лишены чётких ориентиров относительно допустимости блокчейн-доказательств. Нормы об ответственности не учитывают распределённые системы, где ни одна сторона не контролирует реестр единолично. Требования противодействия отмыванию денег плохо сочетаются с псевдонимными транзакциями.

Статья завершается предложением конкретных поправок к платёжному законодательству Казахстана, обосновывая, что пилотный проект цифрового тенге и регуляторная песочница МФЦА позиционируют страну как регионального лидера в сфере блокчейн-регулирования – при условии решительных действий законодателя по устранению выявленных пробелов.

**Ключевые слова:** блокчейн, электронные платежи, смарт-контракты, киберпреступность, цифровая юрисдикция, МФЦА, регуляторная песочница, цифровой тенге, KYC/AML, MiCA.

A.A. Kumisbek[1], A.Sh. Medetov[1*], D.R. Kozhambekov[1], S.U. Akhmet[2], M.P. Baybossynov[2]

[1]Akhmet Yassawi International Kazakh-Turkish University, Turkestan, Kazakhstan
[2]Central Asian Innovative University, Shymkent, Kazakhstan
*e-mail: alimardin.medetov@ayu.edu.kz

## About blockchain technology and the security of electronic payments: combating internet fraud in Kazakhstan

How can the law keep pace with the rapid development of technologies that are fundamentally transforming financial transactions? This article addresses this question by examining the role of blockchain in securing electronic payments and combating cyber fraud within the legal framework of Kazakhstan. The analysis traces distributed ledger technology from its cryptographic foundations to regulatory approaches across three jurisdictions – the European Union, the United Arab Emirates, and Kazakhstan itself.

Drawing on cybercrime statistics from 2024–2025 and emerging case law, the study identifies a central contradiction: the decentralised nature of blockchain conflicts with legal frameworks built around identifiable intermediaries.

The findings point to what may be termed a «presumption of transaction authenticity» – an innovative evidentiary concept underpinned by cryptographic verification. However, significant obstacles remain. Courts lack clear guidelines regarding the admissibility of blockchain-based evidence. Liability

 

norms do not accommodate distributed systems where no single party exercises unilateral control over the ledger. Anti-money laundering requirements clash with pseudonymous transactions.

The article concludes by proposing specific amendments to Kazakhstan's payment legislation, arguing that the digital tenge pilot project and the AIFC regulatory sandbox position the country as a regional leader in blockchain regulation – provided the legislature takes decisive action to address the identified gaps.

**Keywords:** blockchain, electronic payments, smart contracts, cybercrime, digital jurisdiction, AIFC, regulatory sandbox, Digital Tenge, KYC/AML, MiCA.

А.А. Күмісбек[1], А.Ш. Медетов[1*], Д.Р. Қожамбеков[1],
С.У. Ахмет[2], М.П. Байбосынов[2]

[1]Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан, Қазақстан
[2]Орталық Азия Инновациялық Университеті, Шымкент, Қазақстан
*e-mail: alimardin.medetov@ayu.edu.kz

**Блокчейн технологиясы және электрондық төлемдердің қауіпсіздігі туралы: Қазақстандағы интернет-алаяқтыққа қарсы күрес**

Құқық жүйесі технологиялардың даму ырғағына қалай бейімделе алады, егер бұл технологиялар қаржылық операциялардың табиғатын түбегейлі өзгертсе? Осы зерттеу осы сауалға жауап іздеуді мақсат етіп, электрондық төлемдердің қауіпсіздігін қамтамасыз етудегі және киберқылмыстың алдын алудағы блокчейннің рөлін Қазақстанның құқықтық кеңістігі аясында талдайды.

Талдау барысында таратылған тізілім технологиясының криптографиялық негіздерінен бастап, оны үш түрлі юрисдикциядағы – Еуропалық Одақта, Біріккен Араб Әмірліктерінде және Қазақстанда – құқықтық реттеу жүйесіне дейінгі бағыты қарастырылады. 2024–2025 жылдардағы киберқылмыстарға қатысты статистикалық деректер мен қалыптасып келе жатқан сот практикасынан сүйене отырып, зерттеу бір маңызды қайшылықты алға тартады: блокчейннің орталықтандырылмаған мәселелері нақты делдалдарға негізделген құқықтық шеңбермен үйлесе бермейді.

Зерттеу нәтижелері «транзакцияның шынайылығы презумпциясы» деп сипатталатын жаңа дәлелдемелік ұғымға назар аударады. Бұл – криптографиялық тексеру арқылы қамтамасыз етілетін тың тәсіл. Алайда, бірқатар елеулі кедергілер әлі де сақталып отыр. Соттар блокчейн негізінде алынған дәлелдемелердің жарамдылығы жайында нақты ұстанымға ие емес. Жауапкершілік туралы ережелерде таратылған жүйелердің ерекшеліктері ескерілмеген, ал бұл жүйелерде ешбір тарап тізілімді жеке бақыламайды. Ақшаны жылыстатуға қарсы талаптар да бүркемеленген транзакциялармен оңай үйлесе қоймайды.

**Түйін сөздер:** блокчейн, электрондық төлемдер, смарт-келісімшарттар, киберқылмыс, цифрлық юрисдикция, АХҚО, реттеуші құмсалғыш, цифрлық теңге, KYC/AML, MiCA.

## Введение

В период с 2018 по 2023 год в Казахстане произошло нечто выдающееся. Доля безналичных платежей возросла с менее чем 30 процентов до более чем 86 процентов – преобразование, на которое многим развитым экономикам потребовались десятилетия (Национальный банк Казахстана, 2024). Мобильные банковские приложения стали частью повседневной жизни. QR-коды появились на рынках рядом с привычными кассовыми аппаратами. Пандемия лишь ускорила уже начавшийся процесс, за считаные месяцы вовлекая миллионы ранее неохваченных финансовыми услугами граждан в цифровую экосистему.

Однако столь стремительная цифровизация имела и другую сторону. Киберпреступность быстро отреагировала на расширение уязвимых точек в цифровом пространстве Казахстана. Фишинговые атаки стали более изощрёнными. Методы социальной манипуляции были направлены, в частности, на людей старшего поколения, не обладающих необходимыми знаниями в области кибербезопасности.

Кража платёжных данных приобрела системный, почти промышленный характер. К 2024 году регуляторы закрыли 36 незарегистрированных криптовалютных платформ, через которые прошло не менее 60 миллиардов тенге – и это лишь тот объём транзакций, который удалось идентифицировать (Национальный банк Казахстана, 2025). Подлинные масштабы противоправной деятельности, по всей вероятности, значительно выше.

Эта динамика находит отражение в глобальных тенденциях. Согласно последним исследованиям, девять из десяти компаний по всему миру столкнулись с попытками кибермошенничества в 2024 году, причём число атак с ис-

пользованием генеративного искусственного интеллекта – дипфейков, технологии имитации голоса – возросло на 118 процентов по сравнению с предыдущим годом (Trustpair, 2025; Recorded Future, 2024). Традиционные механизмы банковской безопасности, сформированные в эпоху личных визитов в отделения и бумажных подписей, оказываются уязвимыми перед лицом противников, способных достоверно воспроизводить образы сотрудников финансовых учреждений с помощью видео, сгенерированного ИИ.

На этом фоне на первый план выходит блокчейн. Технология, изначально привлекшая внимание благодаря анонимным транзакциям в сети Биткойн, сегодня предстает в новом свете – как потенциально ключевой элемент инфраструктуры массовых финансов. Речь идёт о способе фиксации данных, при котором вмешательство в уже совершённую транзакцию становится вычислительно практически невозможным. В случае корректно реализованного распределённого реестра изменение одной записи потребовало бы одновременного переписывания тысяч копий, которые поддерживаются независимыми участниками по всему миру. Криптографические принципы, лежащие в основе этой неизменяемости, уже получили научное признание. Открытым остаётся другой вопрос – каким образом правовые системы различных стран должны трактовать подобную технологическую надёжность.

Казахстан занимает особое положение в осмыслении этих вопросов. Международный финансовый центр «Астана» одним из первых в мире запустил всеобъемлющую нормативную базу для цифровых активов ещё в 2018 году, применяя английское общее право в рамках специальной экономической зоны. В 2023 году был принят Закон о цифровых активах, распространивший регулирование на более широкий сегмент экономики. Самым амбициозным шагом стало начало пилотного внедрения цифрового тенге Национальным банком в конце 2023 года – Казахстан стал первой страной в Евразии, приступившей к испытаниям цифровой валюты центрального банка, интегрированной с платёжными сетями Mastercard и Visa (МВФ, 2024). К началу 2025 года объём операций в рамках пилота достиг 238 миллиардов тенге, что эквивалентно приблизительно 480 миллионам долларов США.

Тем не менее, по мере перехода от экспериментов к полноценной реализации остаются нерешёнными значимые правовые вопросы. Действующее законодательство, по сути, ограничивает деятельность с криптовалютами рамками юрисдикции МФЦА, что приводит к фрагментации нормативного поля. Суды не располагают чёткими ориентирами в отношении признания блокчейн-записей в качестве доказательств. При ошибочном исполнении смарт-контракта определить, кто несёт ответственность, оказывается затруднительным в рамках текущей доктрины гражданского права. Механизмы противодействия отмыванию доходов предполагают наличие идентифицируемых посредников – именно тех, которых децентрализованные системы принципиально исключают.

Цель данной статьи – системно осветить существующие пробелы в правовом и технологическом понимании цифровых финансовых инфраструктур. Анализ разворачивается в четыре логически взаимосвязанных части. Сначала представляется обзор научной литературы, посвящённой вопросам безопасности блокчейна, юридической исполнимости смарт-контрактов, сравнительному регулированию и доказательной силе распределённых реестров. Далее подробно объясняется методология исследования. Затем излагаются ключевые результаты, сгруппированные по технологическим основаниям, международным подходам к регулированию и актуальным юридическим вызовам, стоящим перед Казахстаном. Завершается работа конкретными предложениями по обновлению законодательства.

Основной тезис предельно ясен: блокчейн предлагает не просто техническое усиление платёжной безопасности, а качественно новую правовую модель установления достоверности транзакций. Для реализации этого потенциала необходимо отказаться от восприятия распределённых реестров как технологической экзотики и интегрировать их в основное русло финансового регулирования. Казахстан, занимая лидирующую позицию в этом процессе, одновременно получает и возможность, и обязанность сыграть определяющую роль в формировании будущих стандартов.

## Обзор литературы

С момента публикации белой книги Накамото в 2008 году, представившей концепцию одноранговых электронных денег, академический интерес к технологии блокчейн вырос в геоме-

трической прогрессии. Первоначальные исследования концентрировались преимущественно на денежной природе биткойна: может ли криптовалюта признаваться «деньгами» с точки зрения различных правовых систем, каким образом налоговые органы должны учитывать доходы от майнинга, представляют ли децентрализованные активы угрозу для центральных банков.

Со временем фокус сместился на архитектурные особенности блокчейна и его использование за пределами платёжных систем. Исследование Абрара и Шейха (2024) представляет ценный обзор современных технических трендов: от анализа протоколов консенсуса до оценки их надёжности в таких отраслях, как здравоохранение и энергетика. Ключевой тезис авторов заключается в том, что децентрализация, неизменяемость записей и криптографическая проверка составляют основу ценности блокчейна как технологии – именно эта триада формирует его применимость к вопросам платёжной безопасности.

Развивая данную линию, Ву (2024) фокусируется непосредственно на финансовом секторе, анализируя цифровые валюты центральных банков, расчёты по ценным бумагам и трансграничные переводы. Его наблюдение о том, что 86 процентов центральных банков уже приступили к исследованию CBDC, ярко иллюстрирует, насколько глубоко эти технологии укоренились в текущем финансовом дискурсе.

Особый интерес для развития правовой мысли в Казахстане представляет работа Го и Полака (2024), в которой исследуется влияние блокчейна на структуру доверия в финансовых отношениях. На примере платформы Quorum от JP Morgan авторы демонстрируют конкретные преимущества: сокращение времени расчётов на 70 процентов, почти полная автоматизация сверки данных, снижение рисков по отношению к контрагентам благодаря выполнению обязательств через смарт-контракты. Это не теоретические допущения, а эмпирически зафиксированные результаты, полученные в ходе реальных институциональных внедрений.

Научные исследования в области кибербезопасности подтверждают эти выводы. Смит и Дхиллон (2020) анализируют потенциал блокчейна в контексте повышения защищённости транзакций, а Тарик с коллегами (2024) устанавливают статистическую взаимосвязь между внедрением технологии и уровнем доверия клиентов к коммерческим банкам Иордании. По данным Financial Crime Academy, прозрачность блокчейна обеспечивает возможность аудита финансовых потоков в режиме реального времени – функциональность, которую традиционные базы данных неспособны обеспечить в полном объёме.

Термин «смарт-контракт» был введён Ником Сзабо ещё в 1997 году, однако его широкомасштабное применение стало возможным лишь после запуска Ethereum почти два десятилетия спустя. Идея сама по себе изящна в своей простоте: зафиксировать договорные обязательства в виде исполняемого кода и позволить блокчейну автоматически обеспечивать их выполнение. Наиболее наглядным примером служат эскроу-механизмы. В традиционном исполнении эскроу требует участия доверенного третьего лица, которое удерживает средства до наступления оговорённых условий; в смарт-контрактной модели оплата производится автоматически при выполнении криптографически проверяемых условий – тем самым исключается необходимость в посреднике и сопряжённые с этим риски.

Юридическая литература, посвящённая исполнимости смарт-контрактов, в последние годы достигла значительной степени зрелости. Систематический обзор Мохда Нура (2023) выделяет три направления исследований: анализ архитектурных рамок и технических платформ, эмпирические кейсы конкретных реализаций и более широкие теоретико-правовые трактовки.

Исследование, опубликованное *Chicago Journal of International Law*, рассматривает применимость смарт-контрактов в рамках Конвенции ООН о договорах международной купли-продажи товаров (CISG) и приходит к выводу, что гибкий подход Конвенции к формированию оферты и акцепта, а также либеральное отношение к допустимым формам доказательств, вполне допускают заключение и исполнение таких договоров.

В то же время, корпоративный форум Гарвардской школы права предлагает использовать гибридную модель – сочетание традиционного юридического языка и программного кода – до тех пор, пока правовая доктрина не догонит уровень технических возможностей.

Современная судебная практика начала напрямую реагировать на вызовы, порождаемые распространением смарт-контрактов. Решение Пятого окружного апелляционного суда США по делу *Van Loon v. Department of Treasury* (2024) затронуло ключевой вопрос: могут ли смарт-контракты, обладающие свойством неизменя-

емости и недоступные для модификации после размещения в сети, подпадать под действие федеральных санкций. Анализ суда выявил глубокие противоречия между традиционными юридическими категориями собственности и контроля и фактической автономией программного кода в условиях децентрализованной архитектуры.

Статистика распространения смарт-контрактов впечатляет. На сегодняшний день 32 американских штата официально признают их юридическую силу, ещё в 18 рассматриваются соответствующие законопроекты. Регламент ЕС по рынкам криптоактивов (MiCA), вступающий в силу в январе 2025 года, вводит обязательные требования к совместимости и юридической исполнимости подобных соглашений. В Сингапуре в 2024 году были внесены поправки в Закон о платёжных услугах, охватывающие также платформы, функционирующие на основе смарт-контрактов. Всё это указывает на формирование международного консенсуса относительно правового статуса таких инструментов – направления, к которому Казахстану было бы разумно присоединиться.

Регламент Европейского союза о рынках криптоактивов (MiCA) представляет собой самую масштабную на сегодняшний день попытку создания комплексной системы управления цифровыми активами. Документ вступил в силу в июне 2023 года; положения, касающиеся стейблкойнов, начали действовать годом позже, а полная имплементация запланирована на декабрь 2024 года. Регламент вводит классификацию криптоактивов на утилитарные токены, токены, обеспеченные активами, и электронные денежные токены, при этом требования к соответствию варьируются в зависимости от уровня системного риска. Особое значение имеет механизм «паспортирования», позволяющий лицензированным в одной стране-участнице поставщикам услуг оказывать деятельность на всей территории ЕС. Эта модель устраняет регуляторный арбитраж, ранее позволявший недобросовестным операторам использовать юрисдикционные разрывы в правовом поле.

Предварительные данные о реализации MiCA указывают на его эффективность. Более 70 процентов криптовалютных транзакций в ЕС теперь совершаются на платформах, соответствующих новым требованиям. Число пользователей несоответствующих платформ снизилось на 40 процентов, поскольку трейдеры перешли на регулируемые площадки. Объём институциональных депозитов в кастодиальных хранилищах, находящихся под регулированием ЕС, увеличился на 55 процентов (ESMA, 2025). Как отмечают Конлон, Корбет и Оксли (2024), успех MiCA может послужить моделью для построения аналогичных нормативных систем в других юрисдикциях.

Объединённые Арабские Эмираты выбрали иную модель регулирования, выстраивая многослойную систему надзора, отражающую как федеративное устройство страны, так и специфику свободных экономических зон. Созданное в 2022 году Управление по регулированию виртуальных активов Дубая стало первым в мире специализированным органом, занимающимся исключительно вопросами цифровых активов. Параллельно действует Управление по финансовым услугам Международного финансового центра Абу-Даби (ADGM), предлагающее альтернативный режим регулирования на основе принципов общего права, что делает его особенно привлекательным для институциональных участников.

Результаты говорят сами за себя: с 2023 по 2024 год приток криптовалют в страну превысил 30 миллиардов долларов США, при этом объём крупных институциональных переводов вырос на 55 процентов в годовом выражении. Согласно опросным данным, приблизительно каждый четвёртый взрослый житель ОАЭ владеет криптовалютой – показатель, подтверждающий высокий уровень принятия цифровых активов в обществе.

Соглашение о сотрудничестве, подписанное в сентябре 2024 года между регулирующими органами ОАЭ в сфере ценных бумаг и Управлением по регулированию виртуальных активов Дубая (VARA), представляет собой особенно показательный пример институциональной координации. Вместо дублирования требований стороны чётко разграничили юрисдикции: VARA отвечает за регулирование в пределах эмирата Дубай, тогда как Управление по ценным бумагам и товарам (SCA) охватывает остальные эмираты. Операторы, получившие лицензию в одной из этих юрисдикций, автоматически признаются другой.

Такой механизм взаимодействия позволяет одновременно снизить регуляторную нагрузку на участников рынка и сохранить узкопрофильную компетентность каждого органа. Именно подобный формат координации может быть по-

лезен для Казахстана в условиях возможного расширения нормативных актов МФЦА на всю территорию страны.

Судебные инстанции по всему миру сталкиваются с вопросом, как квалифицировать блокчейн-записи в качестве доказательств. Проблема носит беспрецедентный характер: в отличие от традиционных документов, требующих внешней верификации, записи в блокчейне обладают внутренне присущим математическим подтверждением целостности. Более того, в отличие от централизованных баз данных, где администраторы могут вносить изменения незаметно, распределённые реестры фиксируют любое вмешательство в режиме реального времени, делая его видимым для тысяч узлов по всему миру.

Суды Китая продвинулись дальше других в формировании доктрины доказательственного использования блокчейна. Сравнительный анализ Полидора (2020) документирует деятельность Интернет-суда в Ханчжоу, где была создана специализированная судебная блокчейн-система: суды выступают в роли узлов-валидаторов в разрешённой (permissioned) сети. В деле *Huatai Yimei Ltd. против Daotong Ltd.* суд признал, что электронные данные, зафиксированные в блокчейне, удовлетворяют требованиям подлинности и целостности. Этот прецедент впоследствии был принят судами и в других юрисдикциях Китая.

Американские суды рассматривали доказательства, связанные с блокчейном, преимущественно в рамках уголовных дел, касающихся использования криптовалют. Особое значение приобрело дело *Bitcoin Fog*. Судья Мосс постановил, что аналитическое программное обеспечение Chainalysis соответствует критериям надёжности, установленным стандартом Дауберта, несмотря на возражения стороны защиты. В своём решении он указал, что методы атрибуции могут служить основой для представления существенных доказательств, если представлены доказательства проведения тестирования, рецензирования, известных уровней погрешности и научного признания.

Этот прецедент не только укрепляет позиции обвинения, предоставляя инструменты, признанные пригодными для отслеживания движения криптовалют, но и формирует методологическую основу, которую могут заимствовать юрисдикции за пределами США.

Инновационный подход штата Вермонт заслуживает отдельного внимания. Принятый здесь *Blockchain Enabling Act* допускает презумпцию достоверности записей, заверенных квалифицированными специалистами, без необходимости дополнительной внешней верификации. Это делает Вермонт первым регионом, официально закрепившим нормы самосертификации в отношении блокчейн-доказательств.

Остаётся предметом дискуссий, обеспечивают ли столь упрощённые процедуры достаточную защиту от потенциальных фальсификаций. Тем не менее, данный нормативный эксперимент предоставляет ценные эмпирические данные для других юрисдикций, рассматривающих возможность аналогичных реформ.

**Материалы и методы**

Настоящее исследование опирается на сочетание сравнительно-правового анализа, доктринального осмысления и синтеза эмпирических данных. Каждый из этих компонентов охватывает различные аспекты общей исследовательской задачи, обеспечивая многомерное и методологически устойчивое рассмотрение заявленной темы.

Сравнительный анализ охватывает три юрисдикции, отобранные с учётом их практической значимости для Казахстана: Европейский союз (регламент MiCA), Объединённые Арабские Эмираты (режимы VARA, ADGM и DFSA) и сам Казахстан (нормативная база МФЦА и Закон о цифровых активах).

В качестве первичных источников используются Регламент (ЕС) 2023/1114, Закон ОАЭ №4 от 2022 года, Конституционный закон Республики Казахстан о Международном финансовом центре «Астана», а также Закон № 193-VII «О цифровых активах». Дополнительную основу составляют вторичные источники: разъяснительные материалы регулирующих органов, доклады о ходе реализации, консультационные документы, опубликованные ESMA, AFSA, VARA и Национальным банком Республики Казахстан.

Доктринальный компонент исследования основывается на применении формально-логических методов с целью оценки внутренней согласованности законодательства Республики Казахстан в сфере цифровых активов. Особое внимание уделяется взаимодействию между Законом «О цифровых активах», Законом «О платежах и платёжных системах», положениями Гражданского кодекса, регулирующими заключение договоров, а также нормами Уго-

ловно-процессуального кодекса, касающимися электронных доказательств.

В случаях, когда законодательные акты содержат противоречия или пробелы, используется телеологическое толкование, позволяющее соотнести правовые конструкции с провозглашёнными целями законодательства – развитием финансовых инноваций, защитой прав потребителей и обеспечением системной стабильности.

Эмпирическая часть исследования основана на синтезе количественных данных, полученных из различных источников. В их числе – статистика Национального банка Республики Казахстан по объёмам платёжных операций и инцидентам киберпреступности за 2024–2025 годы, сведения о транзакциях и клиентской активности в рамках МФЦА, оценки Международного валютного фонда, касающиеся пилотного проекта по внедрению цифрового тенге, а также глобальная аналитика по мошенничеству от Recorded Future и Trustpair.

Дополнительно в анализ включены материалы Группы разработки финансовых мер борьбы с отмыванием денег (FATF), оценивающие эффективность национальной системы противодействия легализации преступных доходов. Практическое понимание существующих доказательственных механизмов дополняется обзором доступных судебных решений казахстанских судов, вынесенных в 2024–2025 годах по делам о хищении электронных денежных средств.

Исследование сталкивается с рядом ограничений, обусловленных как характером предмета, так и рамками исследовательского периода. Технология блокчейн и соответствующие регуляторные подходы развиваются с высокой скоростью, и новые события, произошедшие после завершения сбора данных, могли остаться вне охвата. Судебная статистика по спорам, связанным с блокчейном, по-прежнему ограничена в силу новизны затрагиваемых правовых вопросов. Сравнительный анализ, в свою очередь, предполагает определённую степень упрощения, неизбежную при рассмотрении сложных и многослойных нормативных систем различных юрисдикций.

Количественные утверждения о снижении уровня мошенничества благодаря внедрению блокчейна в значительной степени остаются прогнозными, поскольку реализация таких решений ещё находится на ранних стадиях. Для минимизации воздействия указанных ограничений в работе применена стратегия треангуляции источников и подчёркнутое указание пределов аналитических выводов.

## Результаты и обсуждение

Понимание правовых последствий внедрения технологии блокчейн невозможно без осмысления трёх взаимосвязанных технологических компонентов: криптографического хеширования, механизмов консенсуса и смарт-контрактов. Каждый из них устраняет определённые уязвимости, присущие традиционным платёжным системам, одновременно порождая уникальные юридические вопросы и вызовы.

Каждый блок в цепочке блокчейна содержит криптографический хеш предыдущего блока. Стоит изменить хотя бы один символ в любой из предыдущих транзакций – и результирующий хеш изменяется полностью, тем самым явно разрывая последовательность блоков, начиная с этой точки. Именно эта структурная особенность, известная под названием *неизменяемость* (*immutability*), кардинально отличает блокчейн-записи от традиционных баз данных, в которых администраторы, обладающие достаточными правами, могут вносить изменения, не оставляя очевидных следов вмешательства.

Правовое значение данной особенности можно обозначить как *презумпцию подлинности транзакции*. Бумажные документы и традиционные электронные файлы требуют внешней аутентификации: свидетельских показаний о порядке хранения, экспертной криминалистической оценки отсутствия подделок или вмешательства. В случае с блокчейном, напротив, записи содержат внутренне присущее математическое доказательство целостности.

Как отмечают исследователи судебной практики США, блокчейн «сохраняет подлинность во времени» – характеристика, которая традиционно рассматривается судами как необходимое условие допустимости доказательств.

Тем не менее, утверждения о неизменяемости требуют определённой конкретизации. Сети, использующие консенсус на основе доказательства работы (*proof-of-work*), теоретически остаются уязвимыми перед атаками большинства: если отдельные участники сконцентрируют достаточные вычислительные ресурсы, они смогут реорганизовать недавние блоки в свою пользу. Более того, явление *хардфорков* – протокольных изменений, в результате которых возникают не-

совместимые версии блокчейна, – свидетельствует о том, что сами сообщества способны модифицировать структуру реестра коллективным решением.

Анализ, опубликованный в *Fordham Law Review*, подчёркивает, что судам следует внимательно оценивать конкретные параметры безопасности каждой сети, прежде чем придавать доказательственное значение соответствующим блокчейн-записям. В контексте платёжных решений данные соображения склоняют в пользу разрешённых (*permissioned*) архитектур, в которых криптографическая защита дополняется идентифицируемостью и правовой подотчётностью участников.

До появления технологии блокчейн предотвращение одновременной передачи одного и того же цифрового актива нескольким получателям – так называемой *проблемы двойной траты* – требовало участия доверенных посредников: банков, платёжных систем, других централизованных операторов, ведущих авторитетный учёт транзакций. Механизмы консенсуса устраняют необходимость в таком централизованном доверии, предлагая решение через распределённое согласование между участниками сети.

Техническая литература выработала обширную типологию протоколов консенсуса, отличающихся по характеристикам безопасности, масштабируемости и энергоэффективности. Современные исследования выдвигают гибридные подходы, сочетающие алгоритмы доказательства доли владения с механизмами византийской отказоустойчивости, включая адаптивную приоритизацию и распознавание аномалий для выявления мошеннических действий. В контексте платёжной инфраструктуры Казахстана, где надзор со стороны регулирующих органов является необходимым условием, модели разрешённого консенсуса с участием доверенных валидационных узлов, представляющих официальные органы, открывают перспективные возможности.

Правовые аспекты затрагивают вопросы распределения ответственности. В централизованных системах при возникновении ошибок бремя ответственности однозначно ложится на контролирующее учреждение. В блокчейн-сетях, где ведение реестра распределено между независимыми узлами, механизм установления ответственности усложняется в случае сбоев консенсусных алгоритмов – будь то из-за программных ошибок, задержек в сети или внешнего вмешательства. Требования Казахстана по лицензированию майнинговых пулов и криптовалютных бирж частично решают эту проблему, определяя регулируемые субъекты. Однако ответственность за сбои, происходящие в рамках децентрализованных протоколов, по-прежнему остаётся нормативно неурегулированной.

Смарт-контракты устраняют необходимость во вмешательстве человека, чьё субъективное суждение или недобросовестные действия могут стать источником мошенничества. Например, в классической модели эскроу-финансирования средства хранятся у третьей стороны до выполнения условий контракта, что сопряжено с рисками присвоения или сговора. Смарт-контракт, выступающий в роли эскроу, обеспечивает автоматический перевод средств после криптографического подтверждения исполнения обязательств, исключая уязвимости, связанные с действиями посредников.

Исследования демонстрируют впечатляющие результаты. В сфере финансирования цепочек поставок применение смарт-контрактов привело к снижению числа мошеннических операций на 92 процента. Опросы в электронной коммерции показывают, что 92 процента респондентов выражают большее доверие к платёжным механизмам на основе блокчейн-технологий по сравнению с традиционными решениями. Эти эмпирические данные подтверждают теоретические предпосылки о том, что автоматизация снижает количество потенциальных точек входа для манипуляций со стороны злоумышленников.

Однако использование смарт-контрактов влечёт за собой особые вызовы. Неизменяемость кода означает, что программные ошибки становятся постоянными, если лишь изначально не предусмотрены механизмы обновления. Это вступает в противоречие с положениями договорного права, допускающими изменение условий по обоюдному согласию сторон.

Решение по делу Van Loon, проводящее границу между изменяемыми и неизменяемыми смарт-контрактами, подчёркивает, насколько этот технический аспект может иметь значимые правовые последствия. В контексте Казахстана внедрение смарт-контрактов требует осмысленного подхода к архитектуре обновляемости, механизмам устранения ошибок, а также к обеспечению защиты интересов пользователей в случаях, когда автоматическое исполнение приводит к непредвиденным результатам.

Значимость регламента MiCA заключается не только в его охвате, но и в первых признаках его действенности. Документ распространяется на криптоактивы, выходящие за рамки существующих механизмов регулирования финансовых услуг, и вводит трёхуровневую классификацию с дифференцированными требованиями к соблюдению, соразмерными уровню риска. Обязательность публикации белой книги обеспечивает прозрачность; положения об авторизации формируют порог для выхода на рынок; нормы, направленные на обеспечение добросовестности торговли, запрещают манипулятивные практики. Механизм «паспортирования», предоставляющий возможность лицензирования в одной юрисдикции с последующей деятельностью по всей территории ЕС, устраняет стимулы к выбору наиболее благоприятной регуляторной среды.

Статистика, связанная с реализацией положений, заслуживает особого внимания. К середине 2025 года было выдано более 40 лицензий поставщикам услуг в сфере криптоактивов (CASP). Более 70% транзакций в ЕС переместились на платформы, соответствующие требованиям. Объём институциональных депозитов в регулируемых кастодиальных структурах вырос на 55%. Эти данные опровергают утверждения о том, что всестороннее регулирование стимулирует перенос деятельности за пределы юрисдикции. Наблюдаемая практика свидетельствует об обратном: добросовестные участники отдают предпочтение правовой определённости.

Для Казахстана ряд выводов, проистекающих из опыта MiCA, может быть непосредственно применим. Поэтапное внедрение – сначала регулирование стейблкоинов, затем общие требования к CASP – обеспечило адаптацию без дестабилизации рынка. Переходные положения позволили действующим операторам продолжить работу в рамках национальных режимов на время адаптации. Центральные реестры Европейского органа по ценным бумагам и рынкам (ESMA), содержащие сведения об авторизованных и не соответствующих требованиям участниках, стали инструментами повышения прозрачности. В то же время исключение полностью децентрализованных протоколов из сферы регулирования в рамках MiCA образует пробелы в обеспечении соблюдения норм, которые Казахстан мог бы учесть, внедряя более технологически нейтральные определения.

Дубай и Абу-Даби конкурируют за привлечение криптовалютного бизнеса, предлагая различные модели регулирования. Управление по виртуальным активам (VARA) осуществляет самостоятельный надзор за данной сферой, опираясь на комплексные регламенты. Финансовое управление свободной зоны Абу-Даби (FSRA при ADGM) действует в рамках общего права, что делает его привлекательным для институциональных инвесторов. Управление по финансовым услугам (DFSA) регулирует деятельность в международном финансовом центре Дубая (DIFC), опираясь на собственную обновлённую нормативную базу. Несмотря на внешнюю фрагментированность, соглашение о сотрудничестве между SCA и VARA, заключённое в сентябре 2024 года, демонстрирует, как может быть достигнута координация: чёткое разграничение юрисдикций, автоматическое взаимное признание полномочий и снижение нагрузки на участников рынка.

Цифры подтверждают динамику: объём криптовалютных поступлений достиг $30 миллиардов, институциональные переводы выросли на 55%, примерно каждый четвёртый взрослый житель владеет криптовалютой. Удаление ОАЭ из «серого списка» ФАТФ в феврале 2024 года свидетельствует о соответствии национального надзора международным стандартам в сфере противодействия отмыванию доходов. Для Казахстана, продолжающего формирование своей системы контроля в отношении цифровых активов, данный опыт может стать источником ценных ориентиров.

Правовая база по цифровым активам, разработанная в Международном финансовом центре «Астана» (AIFC), была одной из первых в мире, и в тематическом обзоре IOSCO за октябрь 2025 года признана одной из ведущих юрисдикций по надзору в данной сфере. Эмпирические данные подтверждают это: объём транзакций за первые три квартала 2025 года составил $6,8 миллиарда, число зарегистрированных клиентов достигло 192 400, что отражает рост на 36% по сравнению с аналогичным периодом прошлого года.

Закон «О цифровых активах» проводит различие между обеспеченными и необеспеченными цифровыми активами, ограничивая оборот последних за пределами AIFC. Деятельность по цифровому майнингу подлежит лицензированию, причём ранее майнерам было предписано реализовывать определённую долю добытых активов через биржи AIFC в целях налоговой прозрачности. Однако поправки, принятые в ноябре 2025 года, существенно изменили эту

конфигурацию: были отменены обязательства по реализации криптовалют через AIFC и прекращена исключительная юрисдикция центра в отношении криптоактивов. Это позволило лицензированным операторам действовать на всей территории страны при сохранении требований к получению разрешений.

Цифровой тенге представляет собой наиболее масштабную инициативу Казахстана в сфере финансовых технологий. Запущенный в ноябре 2023 года, он основан на гибридно-децентрализованной архитектуре и функционирует через коммерческие банки, предоставляющие услуги конечным пользователям. Пилотные сценарии охватывают широкий спектр применений: платёжные карты, интегрированные с системами Mastercard и Visa; цифровые ваучеры на школьное питание; трансграничные переводы с использованием CBDC Connector от SWIFT; а также выпуск стейблкоинов, обеспеченных цифровым тенге. По данным на начало 2025 года объём операций в рамках пилотного проекта достиг 238 миллиардов тенге. Полномасштабное внедрение ожидается к концу года.

Традиционные рамки по противодействию отмыванию доходов (AML) опираются на наличие идентифицируемых посредников, осуществляющих проверку личности клиентов и передачу сведений о подозрительных транзакциях. Однако децентрализация сознательно устраняет таких посредников, создавая потенциальные «слепые зоны» для правоприменения.

Формирующиеся технологические решения предлагают альтернативные подходы. Системы самоуправляемой цифровой идентичности, такие как SelfKey и Sovrin, позволяют пользователям контролировать собственные персональные данные, предоставляя возможность выборочной передачи верифицированных данных платформам, соответствующим требованиям. KYC-процедуры, реализованные на блокчейне, создают повторно используемые цифровые удостоверения, размещённые в разрешительных сетях, что позволяет сократить сроки и издержки при подключении клиентов при сохранении нормативного соответствия. Применение доказательств с нулевым разглашением (zero-knowledge proofs) открывает возможность проверки информации без раскрытия исходных данных, объединяя требования конфиденциальности с соблюдением регуляторных норм.

Поправки, внесённые в 2024 году Администрацией финансовых услуг AIFC (AFSA), отражают указанные технологические сдвиги, устанавливая обязанность для поставщиков услуг с цифровыми активами осуществлять надлежащую проверку клиентов с учётом особенностей блокчейн-технологий. Закон «О цифровых активах» возлагает на лицензированных операторов обязанности по мониторингу транзакций и сообщению о подозрительной активности. Тем не менее, одноранговые (peer-to-peer) операции вне рамок регулируемых платформ по-прежнему представляют сложность для надзора. Возникает вопрос о целесообразности использования ончейн-аналитики в дополнение к традиционным инструментам мониторинга.

Процессуальные кодексы Казахстана, регулирующие использование электронных доказательств, были приняты до появления технологии блокчейн и не содержат специальных положений, касающихся записей в распределённых реестрах. В этой связи требуется прояснение ряда аспектов.

Особое внимание следует уделить требованиям к аутентификации. В традиционной практике подлинность электронных доказательств устанавливается посредством свидетельских показаний о создании, передаче и хранении документа, что позволяет проследить цепочку его хранения (chain of custody). Однако блокчейн-записи одновременно существуют на множестве независимых узлов, что усложняет применение привычной модели анализа хранения. Вместе с тем, они потенциально обеспечивают более высокий уровень достоверности за счёт криптографической верификации. Международные прецеденты указывают на необходимость разработки судами специализированных процедур, учитывающих встроенные механизмы обеспечения целостности блокчейн-записей.

Правила о недопустимости слухов (hearsay) потенциально применимы и в отношении блокчейн-записей. Такие данные могут рассматриваться как заявления, сделанные пользователями вне судебного разбирательства, что теоретически подпадает под исключения, предусмотренные для слухов. Вместе с тем, возможны исключения, например, в виде деловой документации или компьютерно-сгенерированных доказательств, однако их применение зависит от соответствия конкретных блокчейн-протоколов установленным в законодательстве критериям. В этой связи реформирование законодательства о доказательствах должно предусматривать чёт-

кое регулирование обращения с такого рода информацией.

Также требует развития нормативная база, касающаяся экспертных заключений. Решение по делу *Bitcoin Fog* демонстрирует, что методы атрибуции в блокчейне могут отвечать критериям надёжности, если сторона, представляющая такие доказательства, способна подтвердить прохождение методики тестирования, наличие рецензирования, известный уровень погрешности и признание в научном сообществе. Казахстанским судам надлежит выработать аналогичные процедуры допустимости, обеспечивающие, чтобы судебно-экспертные выводы опирались на верифицированные методологические основания.

В случае сбоев в блокчейн-платежах потенциальный круг ответчиков может включать отправляющие банки, принимающие банки, операторов платформ, разработчиков смарт-контрактов, участников консенсусных механизмов, а в отдельных случаях – и саму децентрализованную сеть. Однако существующие гражданско-правовые конструкции ответственности исходят из наличия идентифицируемых и виновных субъектов, что затрудняет их применение в условиях распределённой архитектуры. Децентрализация бросает вызов традиционным предпосылкам о личности ответчика, вызывая необходимость переосмысления подходов к правовой ответственности в цифровой среде.

Закон «О платежах и платёжных системах» закрепляет распределение ответственности на основе договорных обязательств и деликтного принципа вины. Банки несут ответственность за несанкционированные транзакции с правом регрессного требования к недобросовестным сотрудникам или внешним злоумышленникам. Однако такая модель предполагает централизованный контроль, тогда как блокчейн-системы, напротив, устраняют централизацию управления как основу своей архитектуры.

Для преодоления возникающих пробелов в правовом регулировании могут рассматриваться следующие подходы: введение режима строгой ответственности для лицензированных операторов платформ вне зависимости от наличия вины; обязательное страхование или размещение гарантийных сумм; распределение ответственности в зависимости от уровня контроля над элементом транзакции, вызвавшим сбой; создание отраслевых гарантийных механизмов по аналогии с системой страхования вкладов. Примером для сравнительного анализа могут служить пруденциальные требования, предусмотренные MiCA, а также нормы по достаточности капитала, применяемые в ОАЭ.

Помимо базовой безопасности, технология блокчейн открывает возможности для реализации специализированных механизмов предотвращения мошенничества, заслуживающих отдельного анализа.

На уровне протокола возможна реализация чёрных списков (blacklisting), формирующих защищённый от подделки реестр кошельков, связанных с подтверждёнными случаями мошенничества. При маркировке конкретного адреса соответствующая запись распространяется по всей сети, автоматически блокируя операции с его участием. Это позволяет устранить проблемы координации, возникающие при асимметрии информации между различными учреждениями, которую активно используют злоумышленники.

Системы отслеживания происхождения учётных данных (credential provenance) позволяют формировать верифицируемую историю легитимности платёжных инструментов. Поддельные карты и синтетические личности эксплуатируют сложности отслеживания жизненного цикла данных в традиционных системах. Блокчейн-регистры фиксируют полный путь учётной единицы – от момента выпуска до последующих изменений, что обеспечивает мгновенную проверку с актуальными авторитетными источниками.

Интеграция функций обнаружения в смарт-контракты предполагает внедрение логики мониторинга непосредственно в платёжные протоколы. В отличие от постфактум-анализа, такие контракты оценивают показатели риска до авторизации перевода: могут приостанавливать подозрительные операции, ограничивать суммы для новых пользователей, либо требовать многостороннего согласования крупных переводов. Эти меры формируют инфраструктурный уровень предотвращения мошенничества, значительно снижая возможности его обхода.

## Заключение

Технология блокчейн представляет собой не просто постепенное усовершенствование платёжной безопасности, а качественно иной подход к подтверждению подлинности транзакций. В отличие от традиционных моделей, основанных на институциональном доверии и центра-

лизованной регистрации, блокчейн полагается на криптографическую верификацию и распределённый консенсус. Правовые последствия такого сдвига весьма существенны, однако в существующем нормативном регулировании Казахстана они остаются в значительной степени неурегулированными.

Сравнительный анализ показывает, что всестороннее регулирование не отпугивает, а напротив – привлекает добросовестных участников рынка. Реализация MiCA в Европейском союзе и многорегуляторная модель Объединённых Арабских Эмиратов свидетельствуют о том, что эффективный надзор может сочетаться с инновационным развитием. Правовая инфраструктура AIFC в Казахстане получила международное признание, а пилотный проект по цифровому тенге закрепил за страной статус одного из мировых лидеров в области внедрения цифровых валют центральных банков (CBDC).

Тем не менее, выявленные пробелы в части допустимости доказательств, распределения ответственности и соблюдения требований по противодействию отмыванию доходов требуют законодательного урегулирования до того, как безопасность платёжных операций на базе блокчейн сможет в полной мере реализовать свой потенциал.

Предлагаемые поправки к Закону «О платежах и платёжных системах»:

1. Следует внести положения, закрепляющие правовую значимость технологии распределённых реестров (DLT) как среды для осуществления расчётов. Определения «распределённый реестр», «блокчейн» и «смарт-контракт» должны быть сформулированы в технологически нейтральной форме, обеспечивая гибкость в условиях будущего развития. Транзакции, зафиксированные в реестрах, управляемых лицензированными провайдерами, должны приравниваться по юридической силе к традиционным платёжным записям, при условии соблюдения технических стандартов, утверждаемых Национальным банком.

2. Необходимо установить процессуальные нормы, регулирующие допустимость и оценку блокчейн-записей в рамках судебных споров. Записи, прошедшие криптографическую аутентификацию и зафиксированные в реестрах лицензированных провайдеров, должны презюмироваться как подлинные при отсутствии опровергающих доказательств. Экспертные заключения по аналитике блокчейна должны соответствовать критериям надёжности, аналогичным международному стандарту *Daubert*. Судам следует предоставить полномочия назначать технических экспертов для интерпретации блокчейн-доказательств.

3. Лицензированные операторы платформ должны нести строгую (безвиновную) ответственность за технические сбои, находящиеся в пределах их контроля. Такая ответственность должна быть обеспечена обязательным страхованием или нормативными требованиями к капиталу. Разработчики смарт-контрактов должны подпадать под профессиональную ответственность за ошибки программного кода, с учётом отраслевых стандартов и требований к внешнему аудиту. Децентрализованные протоколы, не имеющие идентифицируемых операторов, должны быть выведены за пределы лицензируемого периметра с обязательным информированием потребителей о рисках отсутствия защитных механизмов.

4. Лицензированные операторы должны получить возможность принимать подтверждённые цифровые удостоверения, выданные признанными системами самоуправляемой идентификации (self-sovereign identity). Ончейн-аналитика должна быть признана вспомогательным инструментом мониторинга, при этом методики цифровой криминалистики, прошедшие валидацию, должны быть допустимы в рамках контрольных и судебных процедур. Следует предусмотреть механизмы трансграничного обмена информацией для отслеживания международных криптоопераций.

Интеграция цифрового тенге с трансграничными блокчейн-платформами представляет собой наиболее значимую возможность в краткосрочной перспективе. Проведение Национальным банком Казахстана тестирования CBDC Connector от SWIFT и потенциал выпуска стейблкоинов, обеспеченных цифровым тенге, открывают путь к участию в формирующихся многосторонних системах взаимной совместимости. Успешная реализация таких инициатив может закрепить за Казахстаном статус регионального лидера в области финансовых технологий и продемонстрировать жизнеспособность блокчейн-инфраструктуры в контексте массовых платёжных систем.

В более отдалённой перспективе сближение технологий блокчейн и искусственного интел-

лекта открывает преобразующие возможности. Смарт-контракты, использующие машинное обучение, смогут динамически адаптировать алгоритмы выявления мошенничества, реагируя на угрозы быстрее, чем это допускают традиционные системы, основанные на фиксированных правилах. Методы федеративного обучения позволят обмениваться данными об угрозах между организациями без нарушения конфиденциальности клиентов. Эти технологические достижения потребуют постоянной адаптации нормативной базы по мере зрелости соответствующих решений.

Эта статья закладывает основу для законодательной разработки, но требует дальнейшего внимания. Необходимо проводить эмпирические исследования для отслеживания результатов внедрения. Сравнительные исследования должны мониторить эволюцию регулирования в других странах. Междисциплинарное сотрудничество между юристами, технологами и финансовыми специалистами окажется ключевым для создания эффективных правовых рамок, способных использовать потенциал безопасности блокчейна и одновременно управлять сопутствующими рисками.

**Литература**


Abrar, I., & Sheikh, J. A. (2024). Current trends of blockchain technology: Architecture, applications, challenges, and opportunities. *Discover Internet of Things, 4*, 7. https://doi.org/10.1007/s43926-024-00058-5

Association for Financial Professionals. (2025). *2025 AFP payments fraud and control survey report*. AFP. [Электронный ресурс]. https://www.financialprofessionals.org/training-resources/resources/survey-research-economic-data/details/payments-fraud (Дата обращения: 05.02.2026).

Astana Financial Services Authority. (2024). *Rulebook on digital asset activities*. AIFC. [Электронный ресурс]. https://afsa.aifc.kz/ (Дата обращения: 05.02.2026).

Bank for International Settlements. (2021). *BIS annual economic report 2021*. BIS. [Электронный ресурс]. https://www.bis.org/publ/arpdf/ar2021e.htm (Дата обращения: 05.02.2026).

Chainalysis. (2024, April 8). Bitcoin Fog case confirms Chainalysis analytics is reliable and admissible in court. *Chainalysis Blog*. [Электронный ресурс]. https://www.chainalysis.com/blog/bitcoin-fog-daubert-hearing-chainalysis/ (Дата обращения: 05.02.2026).

Coinbase, Inc. v. Suski, 602 U.S. 143 (2024). [Электронный ресурс]. https://www.supremecourt.gov/opinions/23pdf/23-3_879d.pdf (Дата обращения: 05.02.2026).

Conlon, T., Corbet, S., & Oxley, L. (2024). The impact of MiCA on the European cryptocurrency market. *Journal of Financial Regulation*, 10(2), 145-178.

European Parliament and Council. (2023). Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA). *Official Journal of the European Union*, L 150, 52-205.

European Securities and Markets Authority. (2025). *MiCA implementation status report*. ESMA. [Электронный ресурс]. https://www.esma.europa.eu/ (Дата обращения: 05.02.2026).

Financial Action Task Force. (2021). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. FATF. [Электронный ресурс]. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (Дата обращения: 05.02.2026).

Greshnikov, K. (2025, July 4). New in the regulation of digital assets in Kazakhstan. *Chambers and Partners*. [Электронный ресурс]. https://chambers.com/articles/new-in-the-regulation-of-digital-assets-in-kazakhstan (Дата обращения: 05.02.2026).

Guo, H., Liu, X. Exploring trust dynamics in finance: the impact of blockchain technology and smart contracts. *Humanit Soc Sci Commun* 12, 1235 (2025). https://doi.org/10.1057/s41599-025-05473-9

Harris, M. (2023). Blockchain-Based Evidence in Courts: Standards, Reliability, and Admissibility Challenges. *Legal Studies in Digital Age*, *2*(3), 49-63. https://jlsda.com/index.php/lsda/article/view/321

International Monetary Fund. (2024). The Kazakhstan Digital Tenge project. *IMF Staff Country Reports, 2024*(047). https://doi.org/10.5089/9798400267642.002

International Organization of Securities Commissions. (2025). *Thematic review: Digital asset oversight*. IOSCO. [Электронный ресурс]. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD801.pdf (Дата обращения: 05.02.2026).

Library of Congress. (2023, April 30). Kazakhstan: New law establishes legal framework for digital assets and cryptomining. *Global Legal Monitor*. [Электронный ресурс]. https://www.loc.gov/item/global-legal-monitor/2023-04-30/kazakhstan-new-law-establishes-legal-framework-for-digital-assets-and-cryptomining/ (Дата обращения: 05.02.2026).

Al Mashhour, O. F., Abd Aziz, A. S., & Noor, N. A. M. (2023). Legal and Regulatory Aspects of Smart Contracts: A Systematic Review. *Eurasian Journal of Management & Social Sciences – Open Access*, *4*(2), 156-172. https://doi.org/10.23918/ejmss.V4i2p156

О цифровых активах в Республике Казахстан. Закон Республики Казахстан от 6 февраля 2023 года № 193-VII ЗРК. [Электронный ресурс]. https://adilet.zan.kz/rus/docs/Z2300000193 (Дата обращения: 05.02.2026).

Национальный банк Республики Казахстан (2024). Реестр платежных систем. [Электронный ресурс]. https://nationalbank.kz/ru/news/reestr-platezhnyh-sistem (Дата обращения: 05.02.2026).

National Payments Corporation of Kazakhstan. (2025). *Digital Tenge annual development report*. NPCK. [Электронный ресурс]. https://npck.kz/wp-content/uploads/2025/02/annual-report-on-the-development-of-ndfi.pdf (Дата обращения: 05.02.2026).

Polydor, S. (2020). Blockchain evidence in court proceedings in China–A comparative study of admissible evidence in the digital age. *Stanford Journal of Blockchain Law & Policy, 3*, 96-120.

Recorded Future. (2024). *2024 payment fraud intelligence report*. Recorded Future. [Электронный ресурс]. https://www.recordedfuture.com/research/annual-payment-fraud-intelligence-report-2024 (Дата обращения: 05.02.2026).

Samuels v. Lido DAO, No. 23-cv-06492-VC (N.D. Cal. Nov. 18, 2024). [Электронный ресурс]. https://www.courtlistener.com/docket/68095676/samuels-v-lido-dao/ (Дата обращения: 05.02.2026).

Smith, K. J., & Dhillon, G. (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. *Management Finance, 46*(6), 833-848. https://doi.org/10.1108/MF-06-2019-0314

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E., Alzboun, N., Al-Hawary, S., & Mohammad, A. (2024). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. *International Journal of Data and Network Science, 8*(1), 69-76. https://doi.org/10.5267/j.ijdns.2023.10.016

Trustpair. (2025). *Fraud in the cyber era: 2025 fraud trends and insights*. Trustpair. [Электронный ресурс]. https://trustpair.com/white-papers/ (Дата обращения: 05.02.2026).

UAE Federal Decree Law No. 4. (2022). Regulating virtual assets in the Emirate of Dubai. [Электронный ресурс]. https://dlp.dubai.gov.ae/Legislation%20Reference/2022/Law%20No.%20(4)%20of%202022%20Regulating%20Virtual%20Assets.html (Дата обращения: 05.02.2026).

Van Loon v. Department of the Treasury, 122 F.4th 549 (5th Cir. 2024). [Электронный ресурс]. https://www.ca5.uscourts.gov/opinions/pub/23/23-50669-CV0.pdf (Дата обращения: 05.02.2026).

Vermont General Assembly. (2016). Blockchain enabling act. 12 V.S.A. § 1913. [Электронный ресурс]. https://legislature.vermont.gov/statutes/section/12/081/01913 (Дата обращения: 05.02.2026).

Wu, Y. (2024). Blockchain for finance: A survey. *IET Blockchain, 4*(1), 1-23. https://doi.org/10.1049/blc2.12067

Zhang, Y., & Wen, J. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Security Review, 36*, 105389. https://doi.org/10.1016/j.clsr.2020.105401

**References**

Abrar, I., & Sheikh, J. A. (2024). Current trends of blockchain technology: Architecture, applications, challenges, and opportunities. Discover Internet of Things, 4, 7. https://doi.org/10.1007/s43926-024-00058-5

Association for Financial Professionals. (2025). 2025 AFP payments fraud and control survey report. AFP. [Elektronnyj resurs]. https://www.financialprofessionals.org/training-resources/resources/survey-research-economic-data/details/payments-fraud (Data obrasheniya: 05.02.2026).

Astana Financial Services Authority. (2024). Rulebook on digital asset activities. AIFC. [Elektronnyj resurs]. https://afsa.aifc.kz/ (Data obrasheniya: 05.02.2026).

Bank for International Settlements. (2021). BIS annual economic report 2021. BIS. [Elektronnyj resurs]. https://www.bis.org/publ/arpdf/ar2021e.htm (Data obrasheniya: 05.02.2026).

Chainalysis. (2024, April 8). Bitcoin Fog case confirms Chainalysis analytics is reliable and admissible in court. Chainalysis Blog. [Elektronnyj resurs]. https://www.chainalysis.com/blog/bitcoin-fog-daubert-hearing-chainalysis/ (Data obrasheniya: 05.02.2026).

Coinbase, Inc. v. Suski, 602 U.S. 143 (2024). [Elektronnyj resurs]. https://www.supremecourt.gov/opinions/23pdf/23-3_879d.pdf (Data obrasheniya: 05.02.2026).

Conlon, T., Corbet, S., & Oxley, L. (2024). The impact of MiCA on the European cryptocurrency market. Journal of Financial Regulation, 10(2), 145-178.

European Parliament and Council. (2023). Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA). Official Journal of the European Union, L 150, 52-205.

European Securities and Markets Authority. (2025). MiCA implementation status report. ESMA. [Elektronnyj resurs]. https://www.esma.europa.eu/ (Data obrasheniya: 05.02.2026).

Financial Action Task Force. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. FATF. [Elektronnyj resurs]. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (Data obrasheniya: 05.02.2026).

Greshnikov, K. (2025, July 4). New in the regulation of digital assets in Kazakhstan. Chambers and Partners. [Elektronnyj resurs]. https://chambers.com/articles/new-in-the-regulation-of-digital-assets-in-kazakhstan (Data obrasheniya: 05.02.2026).

Guo, H., Liu, X. Exploring trust dynamics in finance: the impact of blockchain technology and smart contracts. Humanit Soc Sci Commun 12, 1235 (2025). https://doi.org/10.1057/s41599-025-05473-9

Harris, M. (2023). Blockchain-Based Evidence in Courts: Standards, Reliability, and Admissibility Challenges. Legal Studies in Digital Age, 2(3), 49-63. https://jlsda.com/index.php/lsda/article/view/321

International Monetary Fund. (2024). The Kazakhstan Digital Tenge project. IMF Staff Country Reports, 2024(047). https://doi.org/10.5089/9798400267642.002

International Organization of Securities Commissions. (2025). Thematic review: Digital asset oversight. IOSCO. [Elektronnyj resurs]. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD801.pdf (Data obrasheniya: 05.02.2026).

Library of Congress. (2023, April 30). Kazakhstan: New law establishes legal framework for digital assets and cryptomining. Global Legal Monitor. [Elektronnyj resurs]. https://www.loc.gov/item/global-legal-monitor/2023-04-30/kazakhstan-new-law-establishes-legal-framework-for-digital-assets-and-cryptomining/ (Data obrasheniya: 05.02.2026).

Al Mashhour, O. F., Abd Aziz, A. S., & Noor, N. A. M. (2023). Legal and Regulatory Aspects of Smart Contracts: A Systematic Review. Eurasian Journal of Management & Social Sciences – Open Access, 4(2), 156-172. https://doi.org/10.23918/ejmss.V4i2p156

O cifrovyh aktivah v Respublike Kazahstan. Zakon Respubliki Kazahstan ot 6 fevralya 2023 goda № 193-VII ZRK. [Elektronnyj resurs]. https://adilet.zan.kz/rus/docs/Z2300000193 (Data obrasheniya: 05.02.2026).

Nacionalnyj bank Respubliki Kazahstan (2024). Reestr platezhnyh sistem. [Elektronnyj resurs]. https://nationalbank.kz/ru/news/reestr-platezhnyh-sistem (Data obrasheniya: 05.02.2026).

National Payments Corporation of Kazakhstan. (2025). Digital Tenge annual development report. NPCK. [Elektronnyj resurs]. https://npck.kz/wp-content/uploads/2025/02/annual-report-on-the-development-of-ndfi.pdf (Data obrasheniya: 05.02.2026).

Polydor, S. (2020). Blockchain evidence in court proceedings in China–A comparative study of admissible evidence in the digital age. Stanford Journal of Blockchain Law & Policy, 3, 96-120.

Recorded Future. (2024). 2024 payment fraud intelligence report. Recorded Future. [Elektronnyj resurs]. https://www.recordedfuture.com/research/annual-payment-fraud-intelligence-report-2024 (Data obrasheniya: 05.02.2026).

Samuels v. Lido DAO, No. 23-cv-06492-VC (N.D. Cal. Nov. 18, 2024). [Elektronnyj resurs]. https://www.courtlistener.com/docket/68095676/samuels-v-lido-dao/ (Data obrasheniya: 05.02.2026).

Smith, K. J., & Dhillon, G. (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. Management Finance, 46(6), 833-848. https://doi.org/10.1108/MF-06-2019-0314

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday, 2(9). https://doi.org/10.5210/fm.v2i9.548

Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E., Alzboun, N., Al-Hawary, S., & Mohammad, A. (2024). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. International Journal of Data and Network Science, 8(1), 69-76. https://doi.org/10.5267/j.ijdns.2023.10.016

Trustpair. (2025). Fraud in the cyber era: 2025 fraud trends and insights. Trustpair. [Elektronnyj resurs]. https://trustpair.com/white-papers/ (Data obrasheniya: 05.02.2026).

UAE Federal Decree Law No. 4. (2022). Regulating virtual assets in the Emirate of Dubai. [Elektronnyj resurs]. https://dlp.dubai.gov.ae/Legislation%20Reference/2022/Law%20No.%20(4)%20of%202022%20Regulating%20Virtual%20Assets.html (Data obrasheniya: 05.02.2026).

Van Loon v. Department of the Treasury, 122 F.4th 549 (5th Cir. 2024). [Elektronnyj resurs]. https://www.ca5.uscourts.gov/opinions/pub/23/23-50669-CV0.pdf (Data obrasheniya: 05.02.2026).

Vermont General Assembly. (2016). Blockchain enabling act. 12 V.S.A. § 1913. [Elektronnyj resurs]. https://legislature.vermont.gov/statutes/section/12/081/01913 (Data obrasheniya: 05.02.2026).

Wu, Y. (2024). Blockchain for finance: A survey. IET Blockchain, 4(1), 1-23. https://doi.org/10.1049/blc2.12067

Zhang, Y., & Wen, J. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. Computer Law & Security Review, 36, 105389. https://doi.org/10.1016/j.clsr.2020.105401

***Сведения об авторах:***

*Кумисбек Айбар Аманкулулы – докторант Международного казахского-турецкого университета имени Ходжи Ахмеда Ясави (Туркестан, Казахстан, e-mail: aibaron@yandex.ru);*

*Медетов Алимардин Шахмардинович (автор для корреспонденции) – профессор Международного казахского-турецкого университета имени Ходжи Ахмеда Ясави (Туркестан, Казахстан, e-mail: alimardin.medetov@ayu.edu.kz);*

*Кожамбеков Даулет Рысбекович – старший преподаватель Международного казахского-турецкого университета имени Ходжи Ахмеда Ясави (Туркестан, Казахстан, e-mail: kozhambekov@ayu.edu.kz)*

*Ахмет Сайрамбай Умбетулы – старший преподаватель Центрально-Азиатского инновационного университета (Шымкент, Казахстан, e-mail: sairambai.akhmet@g,mail.com)*

*Байбосынов Мухтар Пердебаевич – старший преподаватель Центрально-Азиатского инновационного университета (Шымкент, Казахстан, e-mail: mukhtar.baybosynov@inbox.ru).*

***Information about authors:***

*Kumisbek Aybar Amankululy – Doctoral student at Khoja Akhmet Yassawi International Kazakh-Turkish University (Turkistan, Kazakhstan, e-mail: aibaron@yandex.ru);*

*Medetov Alimardin Shakhmardinovich (corresponding author) – Professor at Khoja Akhmet Yassawi International Kazakh-Turkish University (Turkistan, Kazakhstan, e-mail: alimardin.medetov@ayu.edu.kz);*

*Kozhambekov Daulet Rysbekovich – Senior lecturer at Khoja Akhmet Yassawi International Kazakh-Turkish University (Turkistan, Kazakhstan, e-mail: kozhambekov@ayu.edu.kz);*

*Akhmet Sairambay Umbetuly – Senior lecturer at Central Asian Innovative University (Shymkent, Kazakhstan, e-mail: sairambai.akhmet@gmail.com);*

*Baibosynov Mukhtar Perdebaevich – Senior lecturer at Central Asian Innovative University (Shymkent, Kazakhstan, e-mail: mukhtar.baybosynov@inbox.ru).*

***Авторлар туралы мәлімет:***

*Күмісбек Айбар Аманқұлұлы – Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университетінің докторанты (Түркістан, Қазақстан, e-mail: aibaron@yandex.ru);*

*Медетов Әлімәрден Шахмарденұлы (хат-хабарларға арналған автор) – Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университетінің профессоры (Түркістан, Қазақстан, e-mail: alimardin.medetov@ayu.edu.kz);*

*Қожамбеков Дәулет Рысбекұлы – Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университетінің аға оқытушысы (Түркістан, Қазақстан, e-mail: kozhambekov@ayu.edu.kz);*

*Ахмет Сайрамбай Үмбетұлы – Орталық Азия Инновациялық университетінің аға оқытушысы (Шымкент, Қазақстан, e-mail: sairambai.akhmet@gmail.com);*

*Байбосынов Мұхтар Пердебайұлы – Орталық Азия Инновациялық университетінің аға оқытушысы (Шымкент, Қазақстан, e-mail: mukhtar.baybosynov@inbox.ru).*

*Поступило: 16 июля 2025г.*
*Принято: 20 декабря 2025г.*