Инфраструктура для участников рынка цифровых валют и прав

Что предстоит построить каждому участнику рынка, из чего складывается цена входа и почему требования к капиталу — наименее важный показатель в этом случае

Текст
АЛЕКСЕЙ КУРОЧКИН,
РУКОВОДИТЕЛЬ ПРОДУКТОВЫХ НАПРАВЛЕНИЙ «ЦФА» И «ДИЛЕРСКИЕ ОПЕРАЦИИ», КОМПАНИЯ «ДИАСОФТ»



Фото: «Диасофт»

О новом законе **«О цифровых валютах и цифровых правах»** написано много, и почти всегда акцент делается на том, что криптовалюту наконец разрешили. Для тех, кому этот рынок обслуживать, важнее другое: незнакомых видов деятельности закон не создал, он распространил знакомые – на новый класс актива. Организатор торговли, брокер и управляющий работают по прежним лицензиям, но появляются две новые роли с реестровой регистрацией: цифровой депозитарий и организация, осуществляющая обмен цифровой валюты, которую часто называют криптообменником. Поэтому депозитарное ядро не строится заново и расходы приходятся на крипточасть: ключи, узлы, цифровой анализ, сверку.

ЧТО НА САМОМ ДЕЛЕ ИЗМЕНИЛОСЬ

Законы 282-ФЗ и 283-ФЗ подписаны 4 августа 2026 года. В соответствии с ними круг организаторов обращения криптоактивов состоит из пяти возможных ролей:

1) организатор торговли;
2) брокер;
3) доверительный управляющий;
4) цифровой депозитарий;
5) организация по обмену цифровой валюты.

ЭТАПЫ ВНЕДРЕНИЯ ПОЛОЖЕНИЙ ЗАКОНА

1 сентября 2026 года
работает разрешительная часть: роли, реестры, право резидента открыть адрес-идентификатор

1 мая 2027 года
резиденты обязаны сообщать в налоговые органы об операциях, включая внешние кошельки

1 июля 2027 года
включается запретительная часть: сделки в обход лицензированных и реестровых посредников недопустимы

До 1 сентября 2027 года
льготный уведомительный вход для действующих ОИС и банков

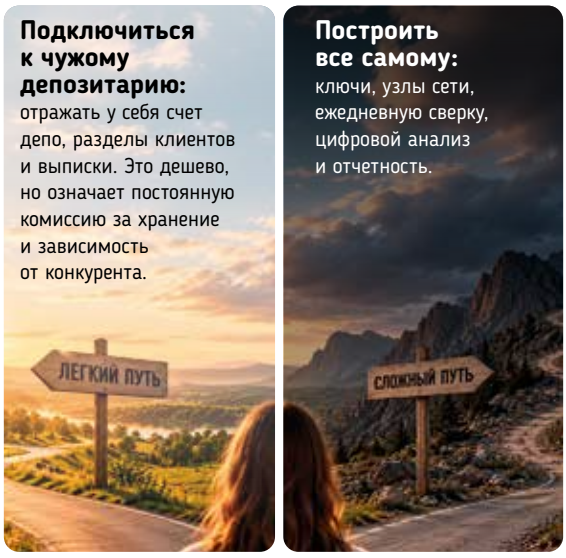
Реестры двух последних ведет Банк России. Вокруг них — обвязка: операторы информационных систем с ЦФА (ОИСы), уполномоченные банки, кредитные организации, обязанные отказывать в переводах нелегальным участникам, и поставщик услуг цифрового анализа (новая роль). Прежний 259-ФЗ в содержательной части отменяется, и все регулирование ЦФА «переезжает» в 282-ФЗ.

Формально до крайнего срока — сентября 2027 года — остается около года. На практике — меньше: организованные торги готовятся к запуску на рубеже 2026–2027 годов, о собственных депозитариях заявил ряд крупных банков. Срок проекта определяется не датой вступления норм в силу, а датой запуска торгов — и тот, кто не готов, приходит на рынок вторым и на чужой инфраструктуре.

Важная деталь: тестирование неквалифицированного инвестора действует год и признается только тем посредником, который его проводил. Клиент, протестированный конкурентом, потерян на год.

РАЗВИЛКА, КОТОРАЯ СТОИТ ДОРОЖЕ ВСЕХ ОСТАЛЬНЫХ

Прежде чем считать состав систем, брокеру, управляющему и обменнику нужно принять решение: использовать свой депозитарный контур или чужой. Операции по поручению клиента допускаются только по счетам и адресам, администрируемым цифровыми депозитариями, — подключаться придется в любом случае.



Разница в деньгах кратная, но важнее то, что выбор определяет модель данных учетного ядра и переигрывать его в процессе реализации проекта дороже. В компании «Диасофт» мы рекомендуем сначала определить границы контуров и точки интеграции. Так проще отделить готовые функции от задач развития и оценить бюджет.

ИЗ ЧЕГО СОБИРАЕТСЯ ПЛАТФОРМА



Шесть слоев из десяти одинаковы для всех ролей организаторов обращения цифровых активов. Различия лежат «по краям»: депозитарию нужны ключи и работа с блокчейном, брокеру — расчет сделок с плечом, обменнику — котировки и защита от мошенничества, за качество этой работы он отвечает деньгами. Поэтому группе, обеспечивающей несколько ролей, нужна одна платформа с разными настройками, а не пять отдельных систем.

Часть слоев не строят, а покупают готовыми: аппаратные криптомодули для хранения ключей и подписку на сервисы цифрового анализа. Учетное ядро дорабатывают — депозитарная модель участнику уже знакома. Все остальное приходится создавать с нуля: узлы сетей, депозитарный учет криптоактивов, расчет сделок с плечом, реестр сделок. Отдельно скажем про справочники: ключевая учетная сущность здесь — не актив, а сочетание актива и сети. Один и тот же USDT в сети TRON и в сети Ethereum (стандарты TRC-20 и ERC-20) — две разные позиции, и перевести актив напрямую из одной сети в другую нельзя; идентификация ведется по ISO 24165 в связке с сетью. Система на плоском справочнике переписывается целиком.

Зарубежные продукты для автоматизации процессов с цифровыми валютами, зарекомендовавшие себя среди иностранных участников, закрыты для нашей страны. В России же для решения подобных вопросов аналогов практически нет.

«Диасофт» уже сейчас имеет комплексные решения, которые позволяют клиентам закрыть ряд ключевых задач: Digital Q.Brokerage автоматизирует бэк-офисные бизнес-процессы по клиентским операциям, Digital Q.Treasury — по сделкам за свой счет. Входящий в решение Digital Q.DFA функциональный блок «Цифровой депозитарий» обеспечивает учет позиций по местам хранения, процессинг поручений и ежедневную сверку, подключение к открытым сетям, интеграцию с HSM и операторами цифрового анализа.

КЛЮЧИ: ГДЕ ПРОХОДИТ ЧЕСТНАЯ ГРАНИЦА

Начинать приходится с развилки, мимо которой нельзя пройти. Российские криптомодули построены вокруг алгоритмов ГОСТ и предназначены для подписи юридически значимых документов. Публичные блокчейны используют собственные алгоритмы электронной подписи secp256k1 в Bitcoin и Ethereum, ed25519 в ряде других сетей, и ГОСТ среди них нет. Одним модулем эти задачи не закрываются: контуров подписи получается два, и поддержку нужных алгоритмов стоит проверять до выбора схемы хранения ключей.

Согласно закону, операции по адресам-идентификаторам невозможны без согласия депозитария. Реализуется оно политикой подписи: кворумы по типам операций, разделение горячего, теплого и холодного хранения, ротация. Ключи доступа хранятся в аппаратном модуле и разделены между несколькими держателями, не менее чем на три стороны, так что в одиночку подписать операцию не может никто. Лимиты и кворум проверяет сам криптомодуль, обойти их из прикладной программы нельзя.

СЕТЬ, КОТОРОЙ НЕЛЬЗЯ УПРАВЛЯТЬ

Кастодиальный контур публичных сетей чаще всего недооценивают: сеть чужая, ею нельзя управлять, и работать с ней приходится через собственную инфраструктуру. Отсюда — и состав работ: собственные узлы сети или удаленный доступ к чужим (по протоколу RPC), контроль подтверждений, расчет комиссии, ликвидность для ее оплаты. Менее очевидная часть: транзакция собирается на своей стороне еще до подписания, ее идентификатор рассчитывается локально и сверяется с тем, что вернул внешний узел; состояние сети подтверждается не одним источником, а совпадением ответов двух-трех независимых. Отказ провайдера или DNS не должен останавливать операции.

Отдельный сюжет — внешние поставщики. Зарубежный RPC означает, что доступ к учетному контуру может быть отключен извне, а совмещение у одного поставщика доступа к сети и проверки адресов дают ему полную картину работы системы.

КАЧЕСТВО КОДА = ДЕНЬГИ

Депозитарий обязан ежедневно сопоставлять учтенное на цифровых счетах с фактическим остатком на адресах в публичных сетях. Если учтено больше — один рабочий день на списание излишка и либо восстановление актива, либо возмещение убытков депонентам. Это единственная роль на рынке, где ошибка учетной системы прямо превращается в денежное обязательство перед клиентом.

Ручным операциям такой норматив места не оставляет: сверку проектируют как продукт — с разбором расхождений, ролями и сроками — и закладывают под нее резерв. Деталь, которая выводится не из закона, а из природы сети: срез берется только по блоку, который сеть уже не может отменить. Иначе перестроение цепочки создаст мнимое расхождение, а за ним последуют акт и уведомление регулятора.

КОМПЛАЕНС: ТРИ КОНТУРА, КОТОРЫЕ ПОСТОЯННО ПУТАЮТ

Цифровой анализ, Travel Rule и антифрод в обсуждениях сливаются в одну тему, хотя это три разных режима, которые в бюджете занимают разные строки.

Цифровой анализ — проверка цифровых валют, прав и адресов-идентификаторов на связь с противоправной деятельностью. Действует с 1 сентября 2026 года, проводится до сделки, при отсутствии возможности — не позднее трех рабочих дней после нее.

По природе это вероятностная оценка, а не установление факта: данные сети дают ложные срабатывания и не содержат сведений о сторонах, а оценка нестабильна — чистый вчера адрес завтра может получить метку. Отсюда — требование к системе: воспроизводимость решения с сохранением версии правил, действовавших в момент операции.

Данных о сторонах перевода в блокчейне нет — их закрывает российский аналог Travel Rule, введенный в 115-ФЗ:

Сведения о плательщике и получателе сопровождают операцию, полный состав – свыше 60 тыс. рублей, при отсутствии сведений поручение не исполняется. Обмен идет вне сети, в формате IVMS 101. Цифровой анализ и Travel Rule – два входа в одно решение об операции. Третий контур – антифрод: проверка принадлежности клиенту счетов и адреса, сверка получателя с базой Банка России о переводах без добровольного согласия, обязательный отказ при несовпадении, период охлаждения. Для обменника добавляется возмещение стоимости похищенного в тридцатидневный срок

РЕЖИМЫ ВЛАДЕНИЯ АДРЕСОМ:

1 Кастодиальный
ключ клиента в модуле депозитария



2 Совместный на многосторонних вычислениях
доля клиента на его устройстве, единолично не подписывает никто



3 Наблюдаемый
ключ у клиента, депозитарий только мониторит



В кастодиальном режиме подтверждение из личного кабинета — организационный, а не криптографический контроль, обе подписи ставит депозитарий. Корректно говорить «Без подтверждения клиента депозитарий не подпишет», но не «Криптографически это невозможно»: обещать больше — значит подвергнуться риску при первом же инциденте.

КАК ПРИЙТИ К ОКУПАЕМОСТИ

Размер рынка оценивается по публичным ориентирам: остатки денег россиян на иностранных площадках — около 720 млрд рублей, аудитория одноранговых площадок — около 20 млн человек. Именно она после 1 июля 2027 года окажется перед выбором: нелегальное поле без правовой защиты сделок или участник из реестра.

Здесь же — главная ошибка финансовой модели: окупаемость нельзя строить на комиссии за хранение. При ставке в десятые доли процента годовых это заведомо убыточный бизнес, тем более что тарифы публикуются заранее, а регулятор вправе установить максимальный.

Экономику стоит выстраивать не на хранении, а на доступе. Статус цифрового депозитария открывает всю линейку услуг с криптоактивом: от брокерской комиссии до маржинального кредитования и репо. Без него посредник покупает доступ у держателя статуса и делится маржой. Обратный ход — тот же: контур цифрового анализа, построенный для себя, становится отдельным продуктом.

У архитектурной защиты есть границы. Квалификация стейблкоинов остается открытой и является главным продуктовым риском: у актива с централизованным эмитентом есть обязанное лицо, и заморозка выполняется независимо от того, где актив учитывается. Российский контур снимает риск посредника, но не эмитента.

ПРОЕКТИРОВАТЬ ПОД БУДУЩИЕ ИЗМЕНЕНИЯ

Проект начинается в незавершенной нормативной среде: значительная часть подзаконной базы существует в виде проектов либо не опубликована, и что-то еще изменится после запуска первых участников. Ждать нельзя: рынок открывается по календарю, а не по готовности нормативной базы.

Единственный работающий прием — с самого начала разделить архитектуру и параметры. Архитектура задает модель данных и границы контуров: сущность «актив в сети», два контура подписи, свой или внешний депозитарный контур; от редакции актов она почти не зависит, но дорога́ при изменении. Параметры — числа, перечни, форматы и коды, которые регулятор еще уточнит: они должны настраиваться, а не зашиваться в код.

Разницу видно на номенклатуре цифровых счетов: структура номера описана в приложении к проекту положения и, пока документ не принят, может измениться. Стоимость определяет не содержание маски, а момент фиксации — до открытия счетов это настройка, после этого — перенумерация и повторный проход по интеграциям.

Тот же принцип — с отчетностью: утвержденных форм нет, поэтому строят версионируемую витрину: полный набор атрибутов операции с историей изменений, из которого собирается любая форма отчетности. Сюда же — рублевая оценка: официального курса не существует, значит, источник цены и метод расчета закрепляются внутренним документом. Без этого не считаются ни годовой лимит неквалифицированного инвестора, ни налоговая база.

Таких неопределенностей — шесть:

- формы отчетности;
- расчет годового лимита для неквалифицированного инвестора;
- методика рублевой оценки:
- требования к капиталу;
- условия маркет-мейкинга;
- реестр поставщиков цифрового анализа.

Все шесть — параметры, а не архитектура, и каждый должен быть вынесен в настройку.

ЕСЛИ ПОДЫТОЖИТЬ ВСЕ СКАЗАННОЕ, ДО НАЧАЛА ПРОЕКТИРОВАНИЯ НУЖНО ВЫПОЛНИТЬ ТРИ УСЛОВИЯ

1. ***Решить строить собственный депозитарный контур или подключаться к чужому.*** Заложить в справочники сочетание «актив в сети» и два контура подписи; не ждать форм отчетности, а собирать данные так, чтобы любую форму можно было построить позже

2. ***Экономику считать не по отдельной функции, а по всей линейке услуг:*** комиссия за хранение контур не окупает — окупает его доступ к рынку, который дает статус. В «Диасофт» мы предлагаем начинать с бизнес-модели: какие услуги запускать, что закрывают существующие решения и что предстоит развить

3. ***Ориентироваться не на 1 июля 2027 года, а на дату запуска биржевых торгов.*** К этому моменту рынок разделится на тех, кто работает на собственной инфраструктуре, и тех, кто арендует чужую. Закон есть, технология есть, спрос есть. Вопрос не в лицензии и не в капитале, а в том, успеет ли IT Б.О