RWA FIN · RWAFIN.RU

CryptoBox

Клиентский кошелёк цифровой валюты для Android

Некастодиальный мобильный кошелёк для клиентов обменника или депозитария: ключи на устройстве, обмен, передача адреса по NFC, защита клиентского ПО. Защита — по ст. 45 закона № 282-ФЗ. Готовое приложение под вашим брендом вместо года собственной мобильной разработки.

Задача
Клиентское приложение цифровой валюты — это некастодиальное хранение ключей на устройстве, обмен, переводы и с 01.09.2027 обязательная защита клиентского ПО по ст. 45 закона о цифровых валютах (проверка целостности устройства до операции, антифрод). Собственная мобильная разработка с оценкой соответствия — год работы и отдельная команда.

Решение
CryptoBox — некастодиальный Android-кошелёк цифровой валюты под вашим брендом: генерация и хранение ключей на устройстве (под защитой Android Keystore), обмен и переводы, передача адреса по NFC, биометрическая авторизация и встроенное средство защиты клиентского ПО по ст. 45 — проверка целостности устройства и антифрод-сессия до операции в связке с SDK клиентской защиты. Реализация написана с нуля по методу «чистой комнаты» (clean-room); приложение брендируется под обменник или депозитарий. Приложение объясняет подпись до подтверждения, защищает от подмены адреса и спам-токенов, принимает адрес и сумму по QR и платёжным ссылкам и работает с обменом только через обменник из реестра. Для обменника и депозитария включается режим приложения организации: защита клиентского ПО по ст. 45, маршруты «кошелёк — депозитарий» с учётом ст. 31, классификация операций и экспорт для налогового учёта. К каждой сборке прилагается журнал доверия: хеш APK, перечень компонентов (SBOM), подтверждение отсутствия секретов в приложении и результаты проверок русскоязычного интерфейса и запрещённых формулировок.

Для кого

Обменник цифровой валюты
Нужно клиентское приложение для розничных пользователей с защитой по ст. 45 без года собственной разработки.

Цифровой депозитарий
Даёт держателям цифровых прав мобильный доступ к счетам. Нужен безопасный некастодиальный клиент.

Розничный держатель цифровой валюты
Хранит цифровую валюту сам, без доверия к третьей стороне. Хочет удобный кошелёк с обменом и передачей адреса по NFC.

Комплаенс обменника или депозитария
Должен убедиться, что клиентское приложение не содействует запрещённым сделкам (ст. 30 ч. 2), не рекламирует оплату цифровой валютой (ст. 1 ч. 6, 9) и включает нормы по датам вступления. Тексты приложения проверяются на запрещённые формулировки, операции классифицируются, спорные помечаются «требует проверки».

Мобильная команда обменника
Не хочет писать криптоядро с нуля. Библиотека кошелька даёт деривацию, адреса, подпись и сборку транзакций пяти сетей, сверенные с эталонными векторами; защитные модули подключаются по необходимости.

Майнер — физическое лицо
Получает вознаграждение на собственный адрес и обязан сообщить о нём в ФНС (ст. 3 ч. 11). Кошелёк выгружает адрес, дату, сумму и адрес пула и не считает вознаграждение запрещённым платежом.

Опытный держатель цифровой валюты
Нужны контроль над входами Bitcoin с защитой от «пыли», лимиты на серию переводов, скрытый кошелёк по дополнительной фразе-паролю и режим маскировки балансов.

Что входит

Некастодиальное хранение

Приватные ключи генерируются на устройстве и хранятся в зашифрованном виде под защитой Android Keystore (аппаратная защита — если её поддерживает модель телефона). Резервная копия и сид-фраза — под контролем клиента.

Клиент владеет активами сам — без доверенной стороны в хранении ключей.

Передача адреса по NFC

Бесконтактная передача адреса-идентификатора и реквизитов перевода по NFC. Кошелёк не предназначен для оплаты товаров и услуг цифровой валютой в РФ.

Перевод без ручного ввода адреса.

Биометрия и восстановление

Биометрическая авторизация, шифрованный бэкап, восстановление по сид-фразе.

Вход по биометрии и восстановление доступа при смене телефона.

Пять сетей из одной сид-фразы

Из одной сид-фразы выводятся адреса и ключи пяти сетей: Bitcoin (native SegWit, BIP-84), Ethereum, TRON, TON (кошелёк v4R2) и Solana, а также токены ERC-20, TRC-20, SPL и Jetton. По каждой сети видны баланс и история, перевод считает комиссию и отслеживает подтверждение, свой токен добавляется с карточкой актива. Деривация адресов и подпись сверены с эталонными тестовыми векторами стандартов.

Один кошелёк и одна резервная фраза для основных сетей клиента.

Защита от подмены адреса, спама и фишинга

Адрес получателя сверяется с историей и адресной книгой: полное совпадение, адрес-«двойник» (совпадают начало и конец, середина отличается) и первый перевод на новый адрес дают разные предупреждения, двойник блокирует отправку до явного подтверждения. Входящие спам-токены (нулевые переводы, ссылки в названии, слишком длинный тикер) уходят в карантин и возвращаются вручную. При подключении dApp его домен сверяется со списком, ищутся домены-двойники. Локальная политика расходов: правила по порядку, решает первое совпавшее, без совпадения — отказ, лимиты за период против серии мелких переводов; для Bitcoin — предупреждение, если комиссия съедает заметную долю суммы, и запрет создавать «пыль». В режиме приложения организации правила может задать профиль вашей организации. Проверки работают на устройстве, без облачного сервиса.

Типовые мошеннические сценарии останавливаются до подписи, а адреса и намерения клиента не уходят третьей стороне.

Обмен и переводы

Обмен цифровой валюты через обменник из реестра и переводы по адресам-идентификаторам с проверкой по ст. 31.

Полный клиентский сценарий в одном приложении.

Защита клиентского ПО (ст. 45)

Проверка целостности устройства и антифрод-сессия до операции в связке с SDK клиентской защиты.

Проверка устройства перед операцией встроена в кошелёк: отдельно разрабатывать её под ст. 45 не нужно.

White-label

Брендирование под обменник или депозитарий: логотип, тема, публикация в магазинах приложений.

Клиенты видят ваш логотип и оформление, а приложение появляется в магазинах под вашим брендом.

Safe Sign: понятная подпись и отказ по умолчанию

Перед подписью приложение объясняет операцию по-русски: баланс до и после, влияние на разрешения на списание, возраст контракта, репутация получателя разрешения и точное содержимое запроса. Реестр дескрипторов (по образцу ERC-7730) переводит вызов контракта в понятные поля и обновляется настройкой, без релиза; если дескриптора нет, показывается предупреждение о «слепой» подписи. Операции собираются и подписываются на устройстве, а ошибка узла сети или неверный адрес не превращаются в отправку.

Клиент видит, что именно подписывает, а сбой не приводит к отправке денег.

QR, платёжные ссылки и WalletConnect

Адрес и сумма принимаются по QR и платёжным ссылкам разных сетей (BIP-21, EIP-681, Solana Pay, ton://, tron:) со сканером камеры и вставкой из буфера; ссылка разбирается и проверяется до показа. При подключении к dApp по WalletConnect перед одобрением видны партнёр, сети, методы, срок и права сессии; центр разрешений показывает давно выданные разрешения на списание, их риск и эффект отзыва или ограничения. Ключи сессии и идентификатор проекта маскируются перед сохранением и показом, а запросы на оплату товаров и услуг помечаются как подпадающие под запрет приёма цифровой валюты в качестве платежа (ст. 1 ч. 6).

Адрес и сумма попадают в приложение без ручного ввода, а лишние разрешения видны и отзываются.

Обмен через обменник из реестра

Приложение сравнивает маршруты обмена и пополнения по сумме получения, комиссии, риску и свежести котировки и объясняет, почему выбран именно этот. Котировки приходят подписанными, с ограниченным сроком и защитой от повтора; при недоступности провайдера показывается запасной вариант, а не обмен по устаревшей цене. Сделку исполняет обменник, включённый в реестр и в список, который задаёт ваша организация: собственного сопоставления заявок в кошельке нет, поэтому кошелёк не становится обменником (ст. 18, 44). Граница систематичности (две сделки в месяц на сумму свыше 3,5 млн ₽) показывается клиенту заранее. Перед приобретением через вашу организацию проверяются срок и статус теста клиента (ст. 32, результат действует год), допуск актива и сумма, накопленная за календарный год: её предел устанавливает Банк России.

Обмен остаётся у обменника из реестра, а клиент видит честный маршрут и границы.

Маршруты «кошелёк — депозитарий» и режим приложения организации

Адресная книга различает адреса, администрируемые цифровым депозитарием, неадминистрируемые и администрируемые иностранной организацией, и подсказывает допустимые маршруты. До отправки на адрес депозитария приложение проверяет основание зачисления (ст. 31 ч. 5) и предупреждает о возврате недопустимого поступления (ч. 6–7); для вывода с депозитарного адреса рядовому физлицу объясняет условие ч. 9 ст. 31; для зачисления собирает подтверждение происхождения средств (адрес-источник, дата, сумма, основание). Для входящих переводов от депозитария при сумме свыше 100 тыс. ₽ показывается задержка 48 часов (ст. 45 ч. 7: депозитарий исполняет такой перевод не ранее чем через 48 часов после распоряжения клиента). Режим приложения организации вы включаете для своего приложения: действуют ст. 45 ч. 15–17 (проверка устройства через SDK клиентской защиты, отказ с уведомлением о причинах и о возможности использовать другое устройство или прийти лично), показываются статус вашей организации и порядок передачи клиентов при прекращении её права (ст. 53 ч. 10).

Клиент понимает допустимый маршрут до отправки, а ваша организация получает приложение под свои обязанности.

Классификация операций, даты норм и налоговый экспорт

Каждая операция получает тип — обращение цифровой валюты, перевод между своими адресами, внешнеторговый расчёт, майнинг, сетевая комиссия — по настраиваемым правилам; при неоднозначной квалификации операция помечается «требует проверки», а не блокируется молча. Даты вступления норм (01.09.2026, 01.07.2027, 01.09.2027) и пороги лежат в настройках с версией и датой действия: до даты норма не применяется, после — применяется. Экспорт истории для Cifra: метод ФИФО, курс Банка России на дату операции, у каждой позиции — канал приобретения и источник стоимости (справка брокера, депозитария или обменника либо собственная реконструкция), события заёмных расчётов в рублях или цифровой валюте. Майнеру — данные для сообщения в ФНС (ст. 3 ч. 11): адрес, дата, сумма, адрес пула; они доступны любому пользователю, который получает вознаграждение. ИНН, паспорт и ключи в выгрузку не попадают.

Налоговая и регуляторная картина собирается из истории кошелька, а нормы подключаются настройкой, а не обновлением приложения.

Резервная копия, скрытый кошелёк и карта

Облачное копирование отключено: сид-фраза остаётся только на устройстве, резервная копия делается вручную с проверкой запоминания нескольких слов. Дополнительная фраза-пароль (25-е слово) открывает скрытый кошелёк с отдельными адресами, сама она на устройстве не сохраняется; режим маскировки скрывает суммы на всех экранах. Раздел о наследовании объясняет, что свидетельство о праве на наследство не даёт доступа к ключу, поэтому восстановление зависит от резервной копии клиента. Для клиентов с картой — отдельная сборка с NFC: ступенчатая проверка подлинности карты (передача по NFC, проверка серверной частью, SDK карты, аппаратная проверка), состояние резервной копии и репетиция восстановления; подлинность карты не заявляется без аппаратного доказательства.

Потеря телефона не означает потерю доступа, а ограничения самостоятельного хранения названы прямо.

Формат работы

Начинаем с пилота на данных заказчика: срок и стоимость определяем по опроснику под задачу, объём и критерии приёмки фиксируем до старта.

- **White-label** — для обменника / депозитария
- **Интеграционный** — для обменника или депозитария со своим приложением

Нормативная база

- Закон о цифровых валютах № 282-ФЗ, ст. 45 ч. 15–17 — защита клиентского ПО (вступает с 01.09.2027)
- Закон о цифровых валютах № 282-ФЗ, ст. 31 — проверка операций розничного клиента
- 152-ФЗ — данные клиента на устройстве, минимизация
- ФСТЭК Приказ 21 — защита клиентского средства
- Некастодиальная модель — ключи хранятся у клиента; резервная копия сид-фразы создаётся только по его действию
- Закон № 282-ФЗ, ст. 24 ч. 3 — обладатель цифровой валюты на адресе, который не администрирует цифровой депозитарий, — лицо, владеющее ключом доступа: ключ не покидает устройство, кошелёк не оказывает услуг цифрового депозитария и не даёт серверного согласия на операции
- Закон № 282-ФЗ, ст. 1 ч. 6, 9 и ст. 30 ч. 2 — приём цифровой валюты как платежа за товары и услуги и реклама такого использования запрещены, как и содействие резидентам в запрещённых сделках; кошелёк не предназначен для оплаты, а тексты приложения проверяются на запрещённое платёжное позиционирование
- Закон № 282-ФЗ, ст. 18 и 44 — систематический обмен (две и более сделки в месяц свыше 3,5 млн ₽) относится к деятельности организации, осуществляющей обмен цифровых валют; в кошельке нет собственного сопоставления заявок, сделку исполняет обменник из реестра

- Закон № 282-ФЗ, ст. 31 ч. 5–9 — зачисление на цифровой счёт, вывод на неадминистрируемый адрес (для рядового физлица по ч. 9 — на адрес, администрируемый иностранной организацией) и возврат недопустимых поступлений: адресная книга различает типы адресов и показывает допустимые маршруты
- Закон № 282-ФЗ, ст. 39 ч. 5–6 и ст. 3 ч. 11 — сведения о расходах для налога предоставляют брокер, депозитарий, обменник и другие перечисленные организации, а для приобретений вне них экспорт кошелька (ФИФО, курс Банка России, источник стоимости) — основной набор данных; майнер сообщает в ФНС адрес и сумму получения

Запросить опросник для пилота: rwafin.ru/contacts.html · **Подробнее:** rwafin.ru/products/cryptobox.html

Актуально на 07.11.2026. Обзор не является публичной офертой и юридической консультацией; условия — в договоре.