H2K
Hidden Keys

Whitepaper

July 2022

Оглавление

Введение

В современном мире криптоактивов выделяется 2 основные проблемы:

- Сохранение секретного ключа[1] от потери, криминала и других проблем владельца;
- Разделение доступа к секретному ключу с целью последовательного контроля за движением криптоактивов, которое мешает гибкому управлению ими.

Первую проблему решают кастодианы с помощью дополнительных мер безопасности (мультиподписных кошельков[2]), но это достаточно дорогостоящее решение, которое недоступно малому и среднему бизнесу.

В настоящее время идет активный поиск решения второй проблемы, и уже предложены несколько вариантов.

Одно из решений предложила блокчейн-экосистема Binance в начале июля 2022 года – она создала платформу для организаций, включающую в себя услуги проведения операций, обмена, управления активами и кастоди. Более популярное решение для компаний принадлежит BitGo, которые являются лидерами по оказанию кастодиальных услуг.
Но у обоих сервисах имеется необходимость прямого обращения на почту за услугой перевода средств.

Ноу-хау проекта H2K (далее H2K) — это быстрая и безопасная технология обращения к блокчейну выполняющая функцию мультиподписного кошелька и включающая в себя уникальную технологию с продуманной системой безопасности, соответствующей AES[3].

Решение значительно расширяет возможности смарт-контрактов[4], предоставляя доступ к реальным данным и автономным вычислениям, сохраняя при этом гарантии безопасности и надежности, присущие технологии блокчейн.

Технологические преимущества H2K:

- Отделение секретного ключа от менеджера;
- Предоставление разделения доступа к секретному ключу;
- Отсутствие больших трат на мультиподпись в блокчейне.

---

[1]Секретный ключ — это ключ, или пароль, который разблокирует кошелек криптоактивов.
[2]Мультиподпись — это защищенное пространство (как сейф), требующее для полнофункциональной работы несколько ключей.
[3]AES — это современный стандарт шифрования данных.
[4]Смартконтракт — компьютерный алгоритм, предназначенный для формирования, управления и предоставления информации о владении чем-либо.

Эти преимущества дают возможность надстройки большого количества бизнес-процессов, позволяющих соединять блокчейн с традиционными технологиями для расширения бизнеса и повышения эффективности процессов.

Таким образом, H2K в партнерстве с сервис-партнерами (Bitrix24) поможет проводить расчеты в криптоактивах для оплаты услуг и товаров, так как технология блокчейн получает большое распространение.

Описание рынка

Актуальность в проекте H2K[5] вызвано:

- Потребностью в появлении новых возможностей межстрановых оплат за различные услуги и товары;
- Растущей инфляцией фиатных валют, которая увеличивает интерес к инвестициям в криптоактивы;
- Интересом к инвестициям в криптоактивы, создающим спрос на услугу профессионального управления криптоактивами;
- Переходом в криптоактивы многих банковских услуг.

С учетом распространения криптоактивов нужны новые решения для массового применения технологии блокчейн в повседневной жизни для ведения бизнеса.

[5] H2K – программно-аппаратный комплекс, в который входят два Управляющих сервера, сетевая инфраструктура и аппаратное обеспечение.

Описание проекта

Решение упрощает процедуру подписания при использовании мультиподписного кошелька за счет добавления офф-чейн системы в процесс перевода средств и отвечает за процедуры аутентификации подписей.

Цель

- обеспечение удобного использования мультиподписного кошелька;
- массовое распространение и внедрение криптоактивов в повседневную и профессиональную жизнь людей;
- снижение риска от потери активов на криптобирже;
- облегчение управление личными ключами.

Задачи

- создание кошелька[6];
- валидация входящих транзакций;
- валидация и инициирование исходящих транзакций;
- защита от внешней цифровой атаки на H2K;
- защита от физической атаки на оборудование;
- защита от принуждения клиента к подаче приказа на транзакцию;
- журналирование операций и запросов на операции;
- передача финансовой учётной системе реквизитов транзакции;
- снабжение Владельца кошелька информацией по балансу кошелька (по его запросу).

Наши клиенты

Основными потребителями услуг нашего сервиса являются:
- Системы документооборота с электронными подписями;
- Криптобиржи;
- Платформы по управлению и автоматизации бизнес-процессов;
- Средний и малый бизнес;
- Майнеры.

[6] Кошелёк - набор Адресов для хранения криптоактивов с соответствующим набором Ключей (один адрес - один ключ).

Прикладное использование:

- Проведение переводов за услуги и товары между предприятиями;
- Сбор и создание статистики по данным из транзакций на блокчейне;
- Бизнес-процессы внутри предприятия, требующие многофакторную аутентификацию;

Решение H2K

H2K решает проблему доступа к секретному ключу менеджером за счет интеграции с сервисами HCL Notes. Создание кошелька, генерация ключей и их хранение построены так, что они изолированы от внешних подключений. Таким образом создана высокотехнологичная «китайская стена», не позволяющая человеческому фактору влиять на активы клиента.

Система H2K позволяет два варианта ее использования:

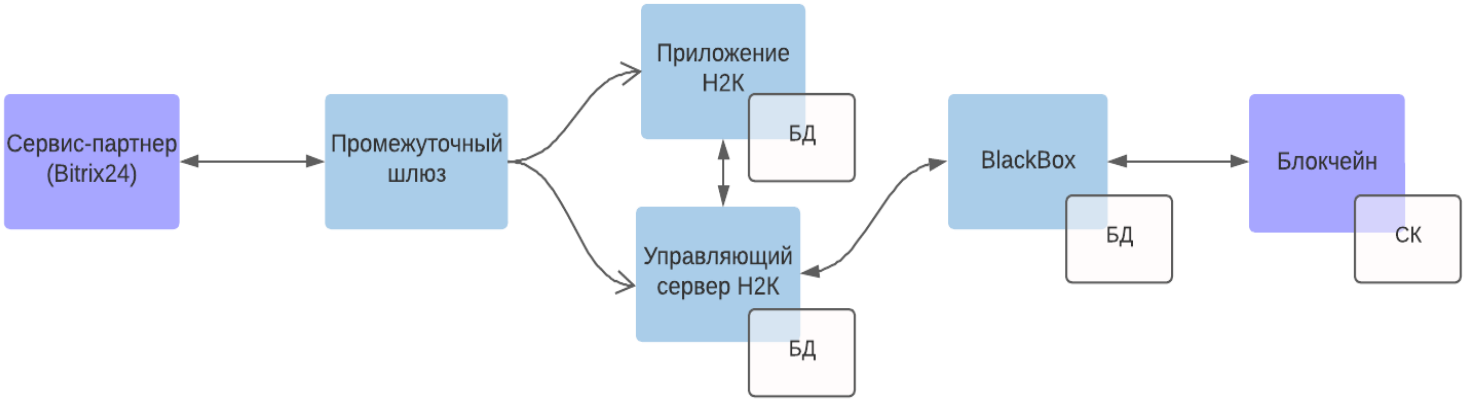
1) с помощью подключения партнерского сервиса (по управлению бизнес-процессами, электронным документооборотом, пр.);
2) с помощью установки отдельной программы на базе HCL Notes.

Подключение партнерского сервиса

Этот вариант подходит и для юридических, и физических лиц, которые либо уже являются пользователями партнерского сервиса, либо не имеют опыта работы с блокчейном или HCL Notes. В качестве примера партнерского сервиса далее будет рассматриваться Битрикс24 и взаимодействие с ним.

Концептуальная модель в упрощенном виде содержит направление потока информации при подключении системы H2K.
Битрикс24 (сервис-партнер) выступает основным пользовательским интерфейсом, который передает запросы и заявки от клиентов промежуточному шлюзу.
Промежуточный шлюз это несколько компонентов системы H2K, между которыми проводится сортировка и распределение данных из заявок клиентов. Это сделано, чтобы отделить информацию, необходимую для проведения блокчейн-операций, от информации, необходимой для внешних бизнес-процессов.
Управляющий сервер BlackBox (далее BB) получает только данные, которые ему нужны для создания кошелька или отправки транзакции перевода средств в сеть. После выполнения заявки BB уведомляет об

этом второй управляющий сервер и запускается обратная цепочка передачи данных между компонентами системы для уведомления клиента о завершении операции.



**БД – База данных, СК – Смартконтракт.*

Очередность подключения процессов в сервис-партнер:

1. Подключение API[7] приложения H2K в сервис-партнер;
    a. Процесс создание кошелька;
    b. Процесс создание перевода средств.
2. Подключение справочников доступных блокчейнов и токенов с которыми работает ВВ.

Более подробное описание по ссылке в приложении №1-3.

Подключение через HCL Notes

Отличительной чертой является то, что используется архитектура PKI. Процесс подписания транзакции мультиподписного кошелька несколькими людьми происходит не на блокчейне, а внутри HCL Notes, с применением технологии электронной цифровой подписи. Достоверность и наличие всех подписей проверяются управляющим сервером.

В наше решение также входят стандартные методы защиты:

- лимиты на выведение средств;
- подключение сотрудника при подозрительных операциях;
- проверки криптокошельков на наличие нелегальных активов; уведомление клиента обо всех транзакциях.

[7] API – описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой.

Безопасность

Свойства

- защита от несанкционированного физического доступа к информации;
- привязка к хосту, на котором запущена виртуальная машина;
- внешние исходящие сетевые правила позволяют связь только с 3мя фиксированными нодами (HTTPS), 2мя управляющими серверами[8] (шифрованный трафик между Domino серверами);
- внешние входящие сетевые правила позволяют только SSH подключение к консоли;
- консоль авторизует по Open SSL сертификатам;
- внутренний firewall повторяет внешние сетевые правила.

HCL Notes

Модель безопасности Domino® основана на принципе защиты ресурсов, таких как сам сервер Domino®, базы данных, данные рабочих станций и документы. Ресурсы или объекты, которые защищаются, настраиваются для определения прав пользователей на доступ и изменение объекта. Информация о правах доступа и привилегиях хранится вместе с каждым защищаемым ресурсом. Таким образом, данный пользователь или сервер может иметь разные наборы прав доступа в зависимости от ресурсов, к которым этому пользователю или серверу требуется доступ.

Создание BlackBox

- Создание образа на чистой машине[9];
- Перенос образа на рабочую площадку;
- id Domino сервера [10] создаётся на этой же чистой машине;
- Администрирование на стадии начальной настройки Domino осуществляется с соседней чистой машины;

[8] Управляющий сервер – программный компонент системы H2K на базе HCL Notes выполняющий ряд операции.

[9] Чистая машина – без связи с глобальной и офисной сетями, установленная с проверенного образа с подтверждённой контрольной суммой.

[10] HCL Domino Сервер – программное обеспечение компании HCL, серверная часть программного комплекса HCL Notes.

Решение BlackBox

OS

- Виртуальная машина VmWare;
- Операционная система Oracle Linux;
- Раздел зашифрован;
- При перезапуске требуется пароль расшифровки раздела;
- Привязка к виртуальной машине.

Domino

- Пароль id сервера;
- Шифрование используемых БД (ключами id сервера);
- В адресной книге кросссертификаты только 2х Управляющих серверов;
- Шифрование трафика на уровне сетевых портов Domino;

BB имеет доступ только к трем фиксированным нодам, которые находятся на существующих 2х серверах и собраны с базового исходника нод. Любой человек может настроить ноду под себя в силу общедоступности ее кода, и то, что BB обращается только к ноде сервиса H2K, гарантирует, что он не подключится к ноде, которая отличается от основной. Так H2K контролирует сервер, на котором находятся закрытые ключи, и все программы на этом сервере.

Но публичные ноды могут подключиться к одной из трех фиксированных нод, являющейся внешней. Однако на ней ничего не хранится, потому при ее взломе утечки данных не произойдет.

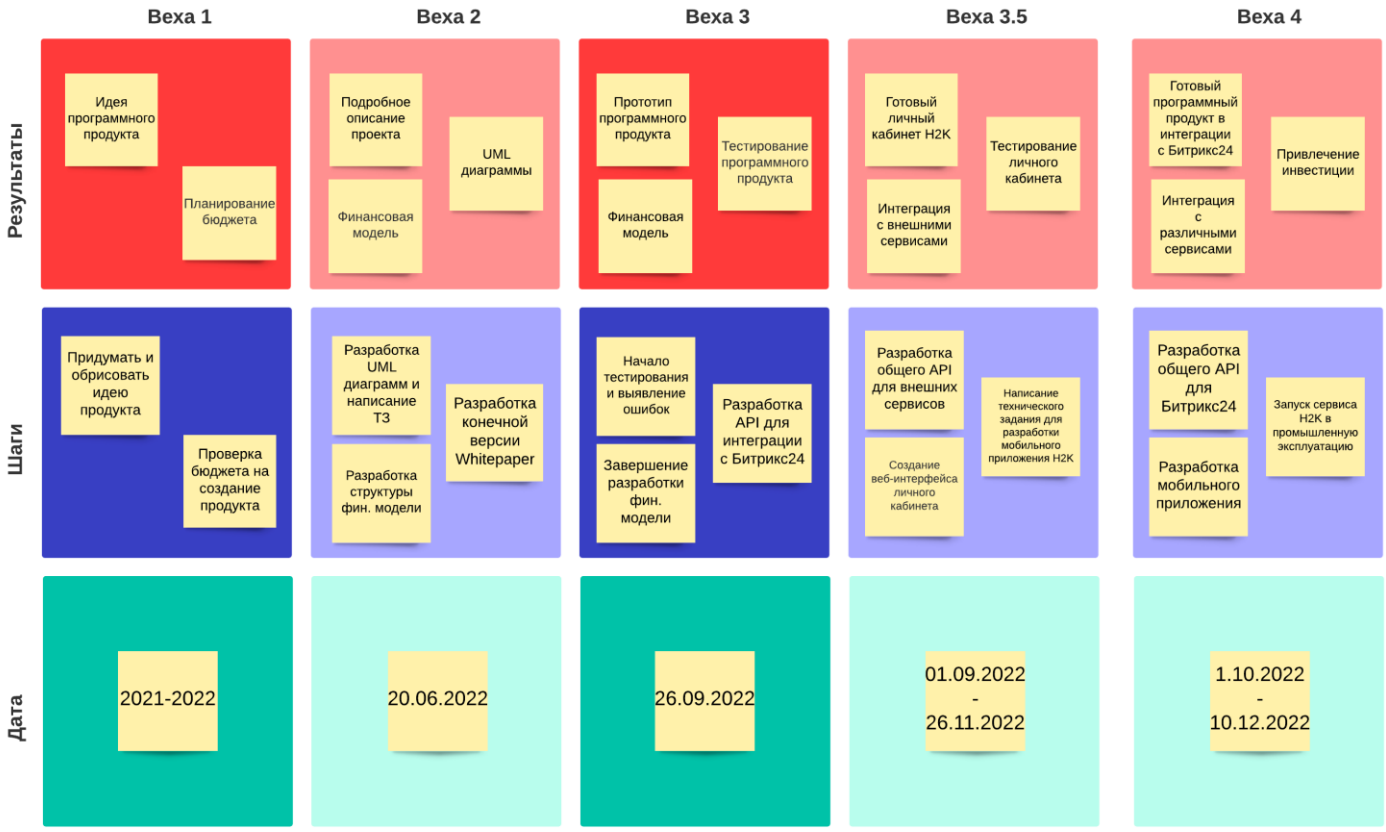
Преимущества и недостатки решения

Преимущества решения:
- прозрачность всех операций;
- финансовый контроль и безопасность;
- повышенные меры безопасности благодаря авторским разработкам;
- поддерживает наиболее популярные криптоактивы.

Недостатки решения:
- базовые риски блокчейна: необратимость транзакции, потеря секретного ключа;
- маленький набор доступных блокчейнов и токенов.

Особенностью криптоактивов является необратимость транзакций — нет механизма отмены вошедшей в блокчейн транзакции. Этот риск остается и в системе H2K из-за самой сути блокчейна. Но помимо него технология блокчейн дает возможность любой компании с внутренними и внешними транзакциями в своих рутинных операциях извлечь выгоду из эффективного мониторинга, качественной защиты данных и почти 100% безопасности всего процесса.
В приложении №4.

Дорожная карта



начало 2022 – зима 2022

Дальнейшие планы

- Интеграция большего вида криптоактивов;
- Обновление архитектуры системы с учетом результатов первого запуска.

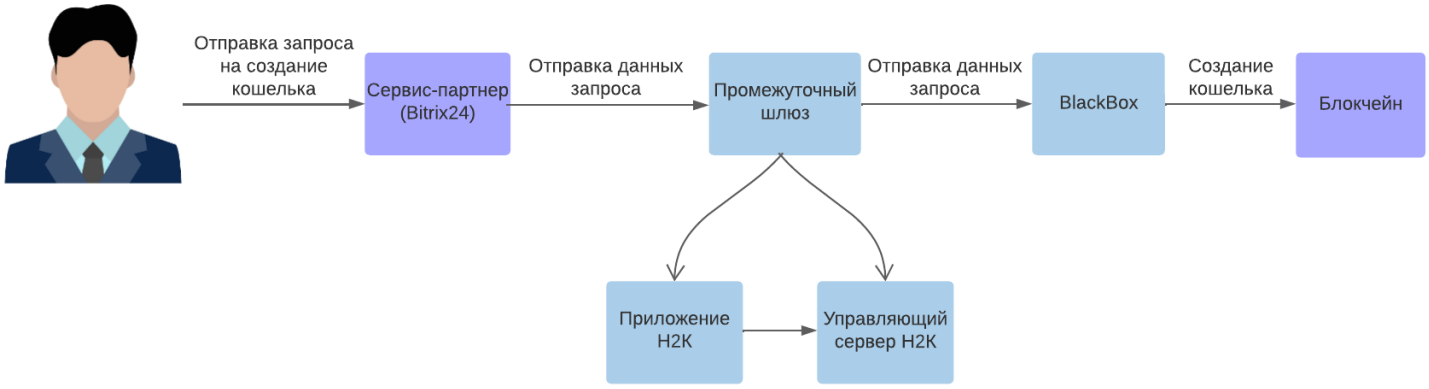
Приложения

Приложение №1

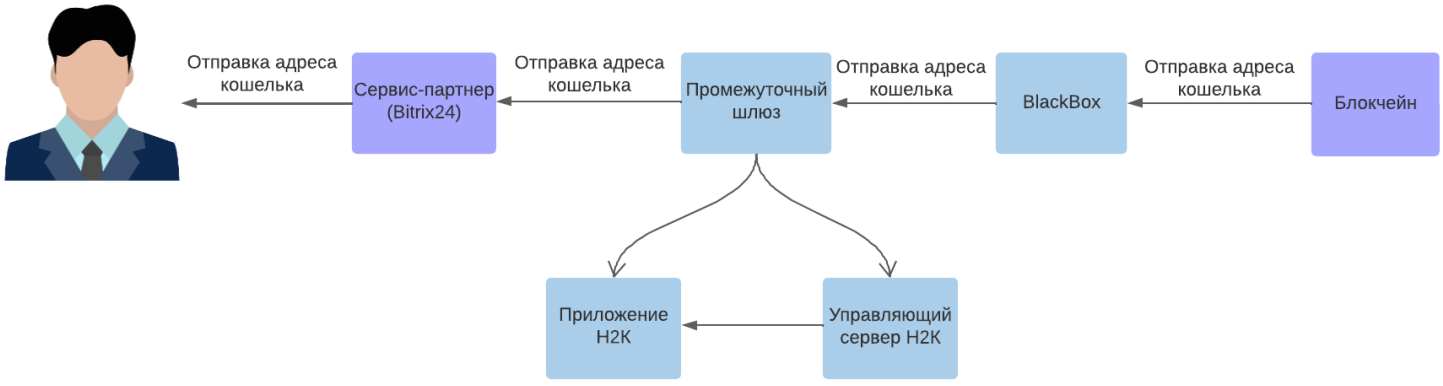
Создание кошелька

Упрощенное представление последовательности передачи данных между компонентами системы H2K и сервис-партнером (Bitrix24).

1 – Заявка на создание кошелька



2 – Создание кошелька



Приложение №2

Перевод средств

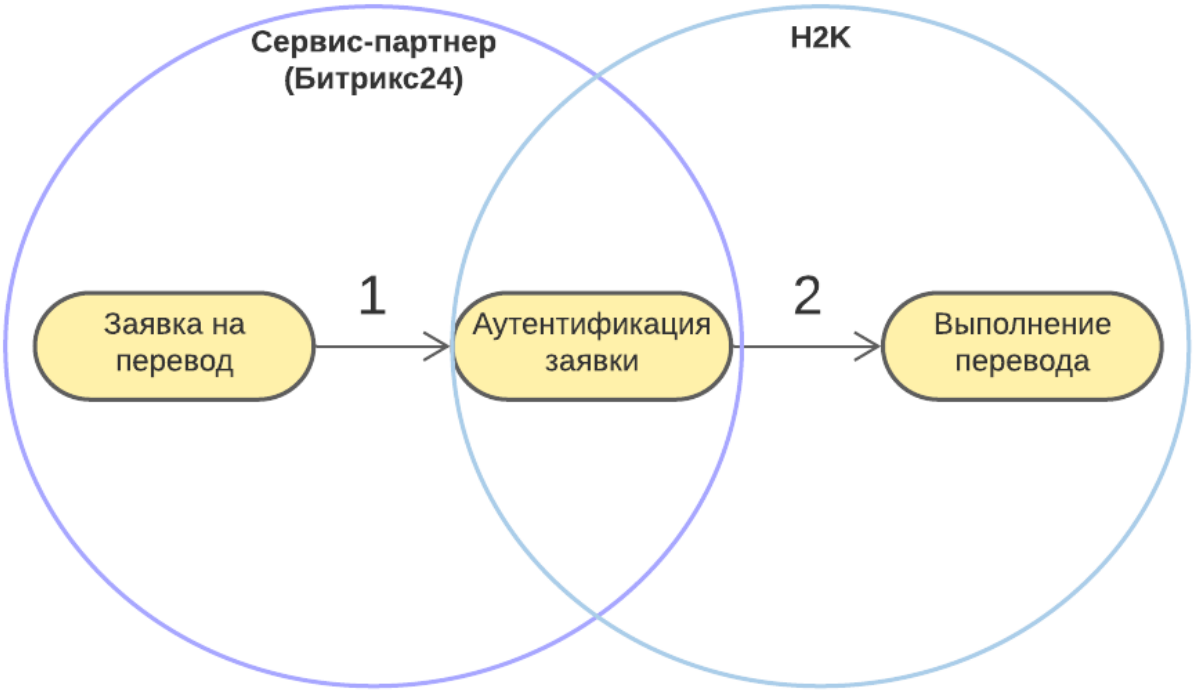
В технологии блокчейн переход криптоактивов с одного адреса[11] кошелька на другой адрес, это считается транзакцией, и всегда есть комиссия, связанная с регистрацией этой транзакции в блокчейне.

Эту комиссию можно считать сбором, сделанным для аутентификации транзакций и поддержания работоспособности блокчейна.

Очевидно, что плата за транзакцию с несколькими подписями больше, чем за одну подпись.

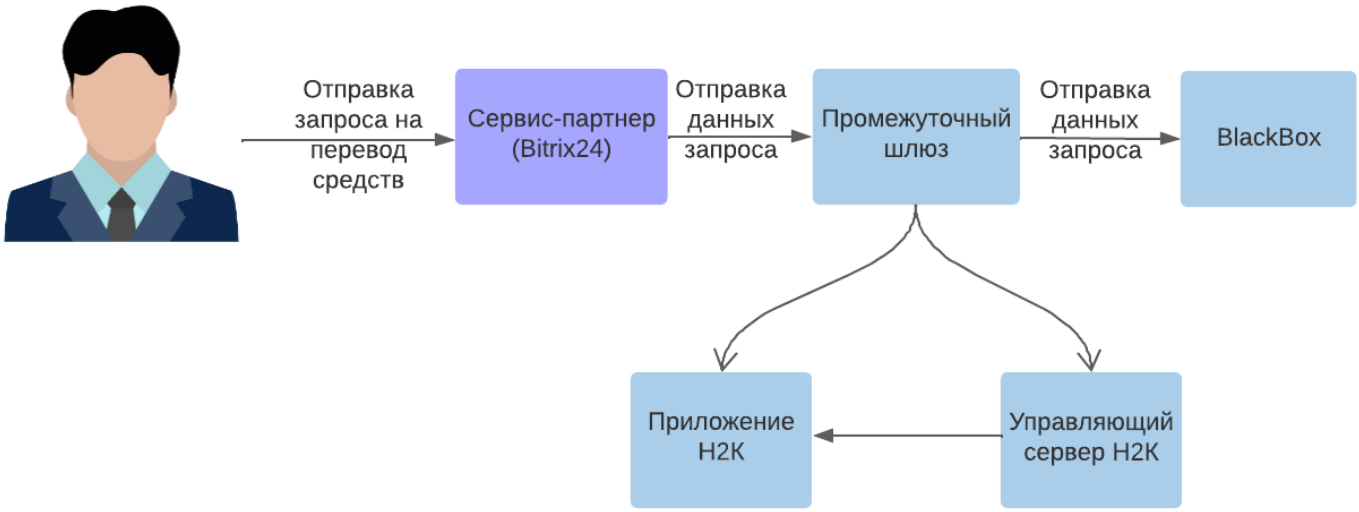
Особенность нашего решения заключается в том, что этап создания транзакции разделен между сервис-партнером и блокчейном. В интерфейсе сервис-партнера указанные при создании кошелька рецензенты вводят свою подпись, а BlackBox проверят ее и отправляет в сеть блокчейна.

Нижеуказанной схеме представлена очередность процессов для выполнения перевода средств.

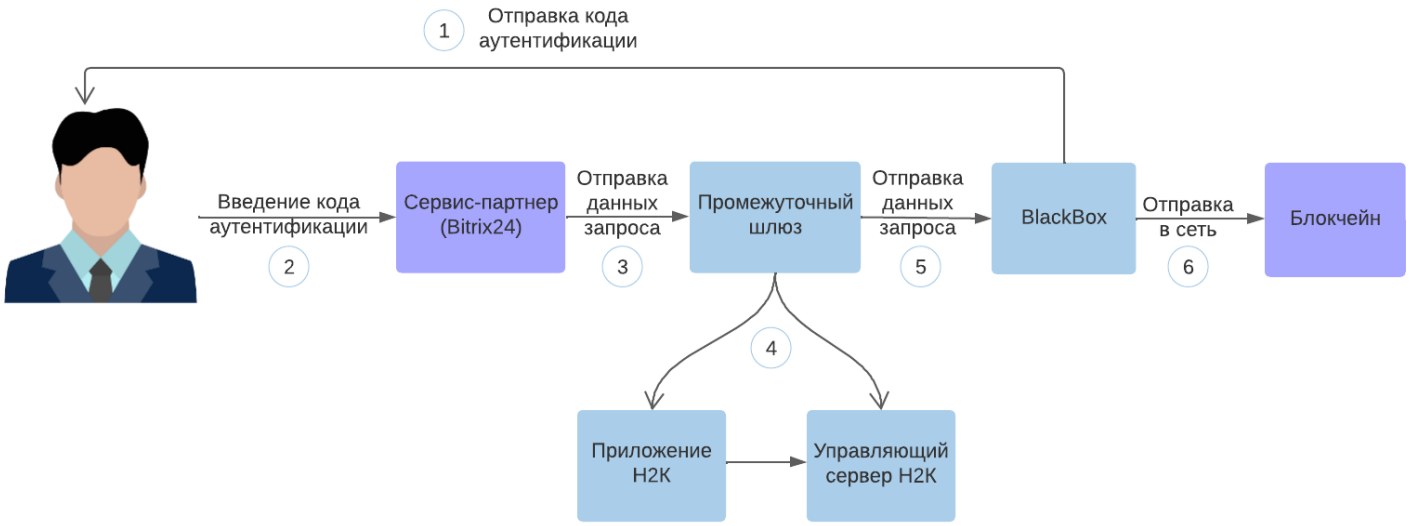


[11] Адрес кошелька - реквизит, на который можно отправить криптоактивы.

1 – Заявка на перевод



2 – Аутентификация заявки и выполнение перевода



Приложение №3

SWOT анализ

Сильные стороны	Слабые стороны
1. Отделение секретных ключей от персонала; 2. Стоимость транзакций; 3. Повышенный уровень безопасности; 4. Первичный способ взаимодействия с блокчейном по аналогии с традиционным банком.	1. Снижение безопасности платформы по независящим от нас причинам; 2. Редкое решение и мало специалистов; 3. Базовые риски решении на блокчейне; 4. Нет восстановления ключей.
Возможности	**Угрозы**
1. Только зарождающийся рынок; 2. Распад мира на валютные зоны; 3. Планируется что, массовый клиент будет использовать криптоактивы как платежное средство; 4. 50% рынка СНГ; 5. Регулирование в пользу криптоплатежей; 6. Облачное решение. 7. Простая реализация традиционных банковских продуктов; 8. Нет необходимости иметь банковскую лицензию.	1. Использование платформы других производителей; 2. Отсутствие законодательства; 3. Редко где разрешено использование криптоактивов в повседневной жизни.