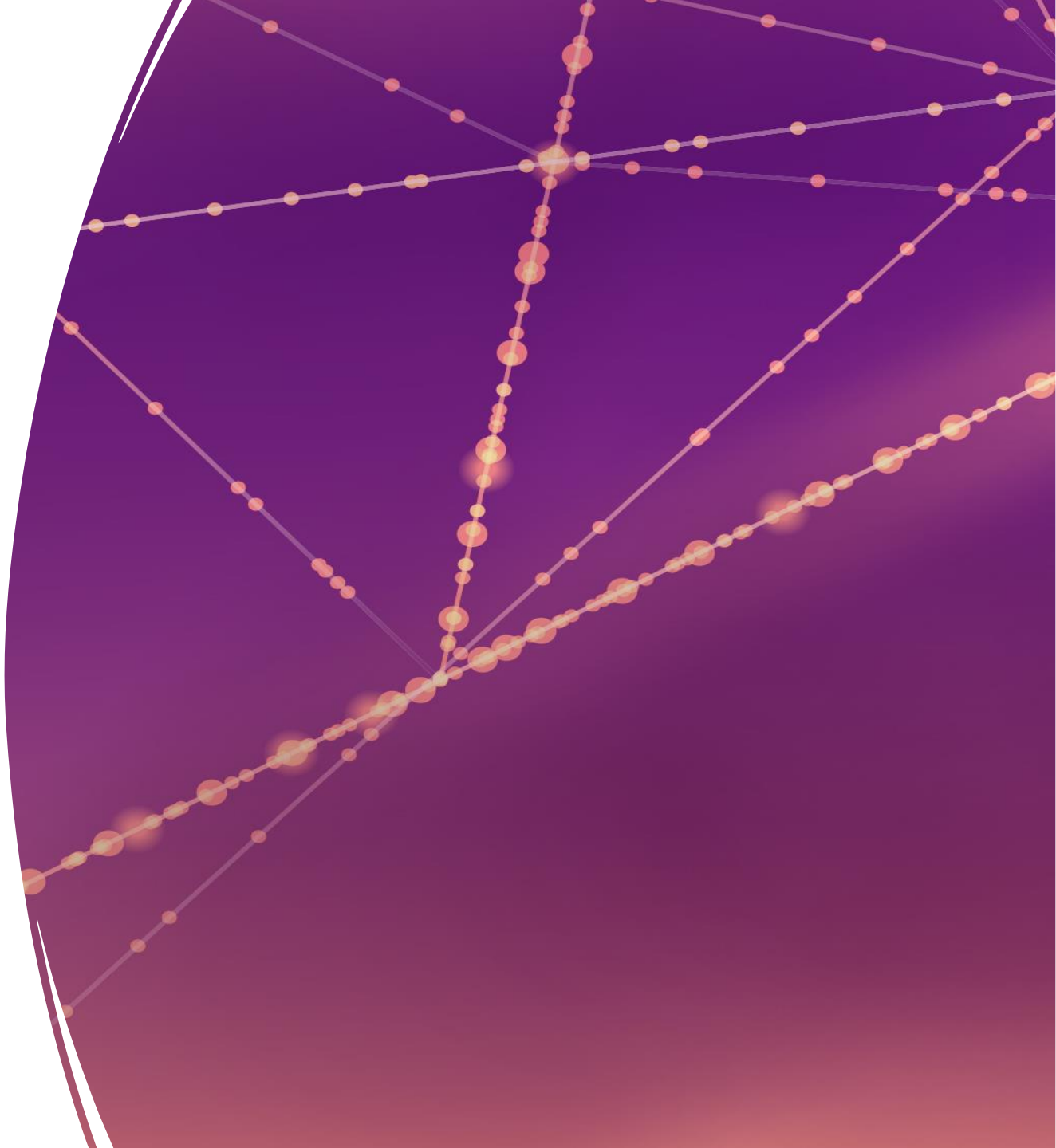
Сервис H2K

Подготовлено командой Oris Lab

Содержание

1. Актуальность
2. Сервис H2K:
   - Компоненты;
   - Распределение ключей;
   - Безопасность
   - Практическое применение;
3. Почему нам можно доверять?
4. Доходы H2K
5. Цель участия на Аллее Стартапов
6. Дорожная карта
7. О нас



Актуальность

Согласно внесенным изменениям в закон «О Международном финансовом центре «Астана» от 30 декабря 2022 года, выпуск и оборот цифровых активов, а также деятельность криптобирж разрешаются исключительно на территории Международного Финансового Центра "Астана".

С начала 2023 года в Республике Казахстан был принят ряд законов и нормативных актов, направленных на регулирование деятельности с цифровыми активами и цифровым майнингом. Однако для их успешной реализации необходима соответствующая инфраструктура, которая включает в себя разработчиков, майнеров, майнинговые пулы, брокерские компании, биржи и крипто-кастодиальные сервисы. **В настоящее время в Казахстане уже имеется вся необходимая экосистема, за исключением специализированных крипто-кастодианов.** В связи с этим участники рынка цифровых активов РК обращаются к зарубежным крипто-кастодиальным сервисам, таким как Fireblocks, для безопасного хранения средств клиентов.

LAB.ORIS.SPACE

**Крипто-кастодиальный сервис - это единое место для хранения цифровых активов и ведения деанонимизированного реестра.*

Актуальность

При этом стоит отметить, что в странах-лидерах, таких как Соединенные Штаты, Великобритания, Швейцария и Сингапур, деятельность с цифровыми активами начиналась с создания необходимой базы, и только после достижения заметных результатов внедрения появлялось соответствующее законодательство. В Казахстане же наблюдается обратный подход: сначала было принято законодательство, и лишь затем началось формирование необходимой инфраструктуры. Построение надежного крипто-кастодиана внутри Республики Казахстан является ключевой задачей для дальнейшего успешного развития технологии блокчейн и внедрения цифровых активов.

Самые популярные крипто-кастодиальные сервисы: Coinbase Custody (США), BitGo (США), Gemini Custody (США), Anchorage (США), Orbitos.io (Еврозона).

Сервис H2K

H2K – это сервис, предоставляющий услуги по открытию и обслуживанию крипто-кастодиальных мультиподписных кошельков.

Главная цель H2K: предоставить простое и эффективное решение для клиентов, позволяющее им распоряжаться криптоактивами.

По своей сути решение H2K аналогично классическому бизнес-процессу подтверждения и учета платежей. Со стороны клиентов требуется только определение сроков хранения, ролей (владельца кошелька и участников кошелька) и последовательности действий сотрудников компании.

В купе с кошельком H2K прилагается электронный документооборот с настроенными бизнес-процессами.

QR для перехода на сайт H2K:

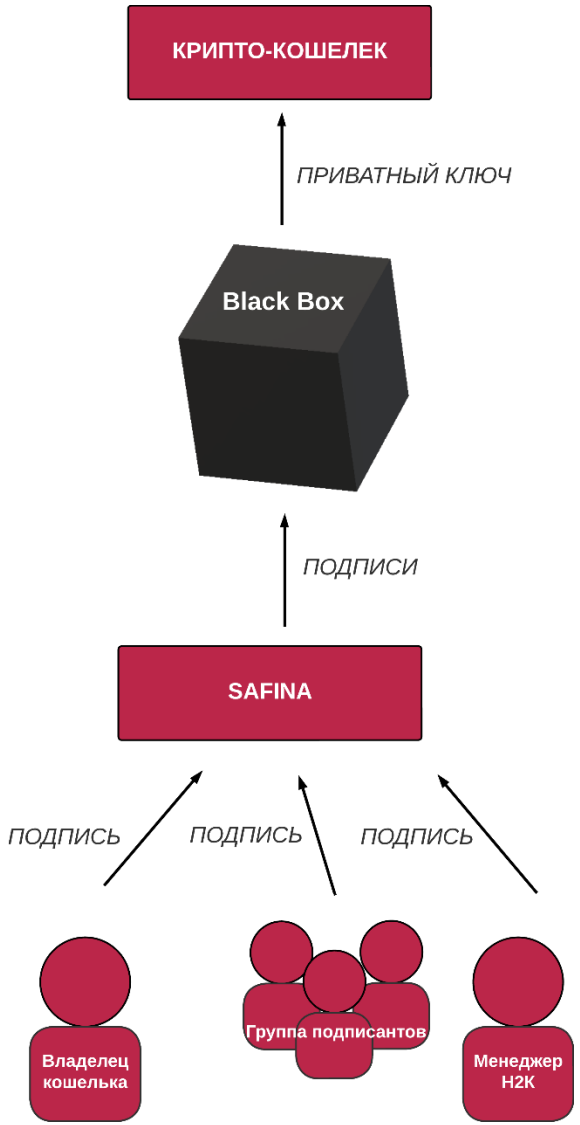
Компоненты H2K

Из чего состоит сервис:

- электронный документооборот для проведения и обработки платежей;
- полностью функционирующий бэкэнд, включающий в себя программный комплекс «Black Box + Safina»:
  - Black Box — это ядро информационной системы для управления криптоактивами. Оно состоит из подсистем шифрования и хранения ключей, определения правил работы с секретными ключами и взаимодействия с блокчейном.
  - Safina — сервер приложения, обеспечивающий взаимодействие Black Box с внешними сетями.

QR для перехода на сайт H2K:

Распределение ключей



В H2K приватный ключ кошелька хранится централизованно в Black Box, вместо его распределения по частям между соподписантами и владельцем кошелька.

Для проведения транзакции все участники кошелька вносят электронные подписи, разработанные H2K, которые их идентифицируют. Затем, на основе проверки этих подписей, сервер автоматически подписывает транзакцию приватным ключом.

Последовательность подписания: первыми подпись вносят соподписанты кошелька. После достижения минимального количества подписей проверяется также подпись владельца кошелька. Следом подпись ставит менеджер из системы документооборота H2K. При этом все подписи участников процесса подписания одинаковы по статусу: если одна из подписей будет отсутствовать (или минимальное число подписей соподписантов не будет получено), транзакция не отправится в сеть.

Путь клиента

Схема механизма мультиподписи в мобильном приложении H2K Pro:

Подписание в мобильном приложении происходит с использованием приватного ключа клиентов (подписантов)

Схема механизма мультиподписи в веб-версии H2K Lite:

Подписание в веб-версии происходит с использованием кодов-подтверждения, приходящих на e-mail адреса клиентов (подписантов)

Безопасность

Основной принцип безопасности: полная изоляция процессов создания кошельков, генерации ключей кошельков и проверки подписей от внешних угроз.

Система ключей и безопасность: система ключей строится вокруг безопасного изолированного хранилища данных Black Box. Он расположен в DMZ и работает согласно установленным при его создании правилам. Именно этот сервер создает кошельки, хранит их приватные ключи, подписывает ими транзакцию и отправляет ее в блокчейн.

Сервер H2K в DMZ имеет жестко ограниченные привилегии доступа, что не позволяет сотрудникам украсть приватные ключи кошельков.

Электронные подписи участников кошельков генерируются сервером приложения Safina и передаются Black Box для внесения их в параметры кошелька.

Практическое применение

Разработано два варианта подключения к криптокошельку H2K:

- мобильное приложение H2K Pro;
- веб-версия H2K Lite.

На данный момент идет активное внедрение H2K в маркетплейс F2C в рамках партнерства со структурой NEOETF.

С помощью сервиса H2K на маркетплейсе будет осуществляться оплата в цифровых активах.

QR для перехода на сайт H2K:

Доходы H2K

Текущие доходы:

На нынешнем этапе внедрения в маркетплейс сервис имеет доход только от сбора комиссий в размере 0,09% при проведении операций в мультиподписных кошельках.

Ожидаемые доходы:

- Увеличение доходов до $40,000 в ближайшие 2 месяца за счет комиссий за проведение транзакций;
- Запуск специализированного крипто-кастодиального сервиса на территории МФЦА с источниками дохода в виде комиссий в размере 0,4% за услуги хранения, за выполнение транзакций на блокчейне в размере 0.15% за ввод и 0.5% за вывод.

Почему нам можно доверять?

Весной 2023 года Oris Lab успешно прошел комплексное тестирование уязвимостей и оценку уровня защищенности внешней инфраструктуры компании. Аудитором выступила ведущая международная компания в сфере информационной безопасности Group-IB.

Результаты:

- Многовекторные проверки на проникновение показали, что защитные меры и политика безопасности компании Oris Lab эффективны. Выявленные уязвимости были оперативно устранены в соответствии с рекомендациями, предоставленными Group-IB.
- Хранилище криптоключей Black Box успешно прошло все проверки на прочность. Пентест показал, что несанкционированный доступ извне к ядру информационной системы Oris Lab невозможен.

Ссылка для подробного ознакомления с результатами аудита.

Кому мы нужны для развития своего бизнеса на блокчейне?

- традиционные финтех-проекты;
- крипто-кастодианы;
- криптофонды;
- майнинговые пулы;
- банки;
- проекты, выпускающие свои цифровые активы.

Дорожная карта

2019-2022:

- разработка решения «Black Box + Safina».

2022-2023:

- разработка и тестирование сервиса H2K и услуги приема платежей в цифровых активах;
- прохождение ИТ-аудита.
- получение патентов на решения «Крипто-кастодиальный сервис», «Safina».

2024:

- запуск специализированного крипто-кастодиального сервиса на территории МФЦА;
- получение сертификата ISO/IEC 27001;
- заключение договора со страховой компанией.

О нас

ТОО "Oris Lab" – казахстанская софтверная компания, занимающаяся разработкой собственных программных продуктов на блокчейне. С 2021 года является участником международного технопарка IT-стартапов Astana Hub.

Коллектив компании является многосоставным, в нем собрались как опытные финансисты и программисты, так и молодые специалисты, которые придают новый импульс и динамику проектам, способствуя их развитию.

Особое внимание в компании уделяется передаче знаний молодому поколению. В 2021 году Oris Lab подписал меморандумы о взаимном сотрудничестве с Международным университетом информационных технологий и Казахстанско-Британским техническим университетом, в 2023 – с Казахским Национальным Университетом имени Аль-Фараби. В рамках этих партнерств компания принимает студентов на прохождение производственных и преддипломных практик, проводит семинары и принимает участие во внутренних мероприятиях учебных заведений. По окончании практики самые активные студенты получают приглашения для прохождения стажировки и возможного дальнейшего трудоустройства. Выстраивание отдельного молодого звена - одна из задач Oris Lab.

О нас

При разработке наших программных решений мы успешно объединяем накопленные знания и опыт из традиционного финансового сектора с новыми возможностями, предоставляемыми технологией блокчейн.

За годы деятельности наша компания получила авторские права на ряд инновационных разработок:

- Защищённые приём и передача текстовой и структурированной информации;
- Крипто-кастодиальный сервис;
- Система управления бизнес-процессами;
- Safina (технология по быстрому и безопасному обращению к блокчейну).

LAB.ORIS.SPACE

+7 727 225 57 12
office@oris.space
marketing@oris.space
https://lab.oris.space

ТОО "ORIS LAB"

Адрес:
050044, г. Алматы,
Бостандыкский р-н, ул.
Байшешек, д. 65