https://soikawallet.app

Soika Wallet whitepaper

Soika Wallet - мультвалютный некастодиальный криптокошелек с открытым исходным кодом. Главная цель проекта - максимальная безопасность и приватность.

Компоненты системы

Soika Wallet - десктопное приложение, написанное на языке Golang, с использованием минимального количества сторонних библиотек. Базовый интерфейс реализован в виде terminal UI (TUI), возможно также использование API для подключения веб или десктоп UI.

Soika AirGap - мобильное приложение, с использованием минимального количества сторонних библиотек, без привязки к *Google Services* с полной поддержкой защищенной *Graphene OS*. Предполагается, что на смартфоне или ином устройстве с установленным приложением будет отсутствовать сим-карта и доступ к сети Интернет. Взаимодействие с приложением будет осуществляться через анимированные QR коды и веб камеру. Soika AirGap позволяет безопасно хранить, генерировать ключи для адресов формата BIP-44, подписывать транзакции, хранить настройки Soika Wallet.

Soika Wallet Extension - браузерный плагин, необходимый для взаимодействия с Web 3 приложениями. Является провайдером между приложением Soika Wallet и веб-браузером, не сохраняет никакую пользовательскую информацию.

Безопасность

- Полностью открытый аудируемый исходный код, минимальное использование сторонних библиотек.
- Защита от кейлоггеров и вредоносного ПО - при работе с Soika AirGap, ключи всегда находятся на устройстве, отключенном от сети, подписывание транзакций осуществляется через отображение и считывыние QR кодов в приложении и с помощью камеры устройства. В случае, если AirGap не используется, то конечные ключи адресов хранятся в защищенной памяти (mprotect). Это позволяет осуществлять операции на скомпрометированном или небезопасном ПК.
- Возможность использования приватных нод с настройками для каждого аккаунта.
- Отсутствие зависимости от сторонних сервисов. Все данные, включая курсы валют, актуальные версии, информация о дистрибутиве и хеши приложения получаетюся из блокчейна.
- Никакие данные, включая настройки приложения не сохраняется на жестком диске, что подходит для работы с live-CD и live-USB дистрибутивами
- Возможность автоматической проверки входящих и исходящих транзакций через AML сервисы, использование одноразовых адресов.

Порядок работы системы

Использование декстопного приложения Soika Wallet и AirGap приложением Soika AirGap

Данный режим позволяет наиболее безопасно взаимодействовать с криптоактивами, путем вынесения механизма подписывания транзакций и хранения ключей в оффлайн приложение Soika AirGap. С помощью Soika Wallet может осуществляться генерация адресов, проведение операций, но непосредственное подписывание транзакций осуществляется через AirGap приложение, через анимированные QR коды и веб камеру, таким образом ключи никогда не попадают на устройство с доступом к сети Интернет. Вся информация о настройках, используемых адресах, хранится также в AirGap приложении, что позволяет удобно работать с live-CD и live-USB дистрибутивами, позволяя обезопасить держателя от аппаратных и софтверных кейлоггеров. Данный режим наиболее подходит для нечастых транзакций и управления холодными кошельками.

Использование только декстопного приложения SoikaWallet

Данный режим позволяет работать по классической схеме использования mnemonic фразы или для генерации ключей для адресов в формате BIP-44 с помощью приложения Soika AirGap. В защищенной памяти приложения (mprotect) сохраняются только необходимые для операций конечные ключи, доступ на чтение к которым открывается только на момент подписания транзакций. Root seed и mnemonic фраза не сохраняются в памяти. Вся информация о пользовательских настройках, используемых адресах, адресах нод, токенов хранится также в AirGap приложении, что позволяет удобно работать с live-CD и live-USB дистрибутивами. Данный режим работы может использоваться для частых операций при работе с горячими кошельками.

Смешанный режим работы

Данный режим позволяет не только подписывать транзакции через Soika AirGap, но и выделять адреса, необходимые для частых операций или автоматизации, для которых ключи будут сохраняться в защищенной памяти Soika Wallet с возможностью проведения операций без AirGap приложения. Также предполагается автоматизация операций, запуск по условиям или по планировщику, использование AML сервисов. Данный режим работы наиболее подходит для обменников, массовых выплат, спотовой торговле через DEX.

Использование расширения браузера для взаимодействия с Web3

Браузерное расширение Soika Wallet Extension взаимодействует с локально установленным десктопным приложением Soika Wallet и проксирует запросы. Подписание транзакций возможно как через приложение, так и через AirGap. Это позволяет наиболее безопасно взаимодействовать с Web3 приложениями, dApp.

Конфигурационные данные синхронизации

- Используемые адреса в формате BIP-44
- Пользовательские описания адресов
- Пользовательские настройки приватных нод и связанные с ними адреса кошельков
- Пользовательские адреса токенов, описания и связанные с ними адреса кошельков

Монетизация проекта

- Вознаграждения от DEX
- Вознаграждения от стейкинг провайдеров
- Реферальная программа от провайдеров приватных нод