Разработка приложения для безопасного хранения криптовалют

Автор: Холодаева Екатерина, 17.Б10-мм
Научный руководитель: ст. преп. Я. А. Кириленко
Консультант: DSXT, ведущий разработчик ПО Ф. П. Долголев

Санкт-Петербургский государственный университет
Кафедра системного программирования

26 мая 2020г.

Введение

- **Холодное хранение криптовалюты** — это способ содержания цифровых монет в кошельке, при котором приватный ключ, дающий доступ к деньгам, находится без возможности подключения к любым внешним устройствам.

Введение

- **Мультиподпись (multisig)** - это конфигурация адреса, для которой требуется как минимум два ключа для валидации транзакции.

Цель работы

- Создать приложение для безопасного хранения разных криптовалют с возможностью создания multisig адресов и холодного хранения.

Задачи

- Исследовать предметную область
- Провести обзор уже существующих решений для хранения криптовалют
- Выбрать технологии и средства для создания приложения
- Разработать архитектуру приложения и UI
- Осуществить поддержку нескольких криптовалют
- Осуществить поддержку стандартных и multisig адресов

Анализ уже существующих приложений для безопасного хранения криптовалют

	Возможность холодного хранения	Наличие multisig-поддержки	Поддерживаемые ПО	Поддерживаемые валюты
Electrum	Есть	Есть	Linux, Mac OS, Windows и Android, portable version	Bitcoin
Copay	Нет	Есть	iOS , Android, Windows Phone , Linux, Windows, Mac OS , Chrome (plugin)	Bitcoin и Bitcoin Cash
BitGo	Для ограниченной группы пользователей	Есть	Mac OSX, Windows, Linux	≈ 100 криптовалют
Mist	Есть	Есть	Windows, Mac OS, Linux	Ethereum
Exodus	Есть	Нет	Windows (x64), Linux, Mac OS, iOS	Более 95 криптовалют

Выбор стека технологий

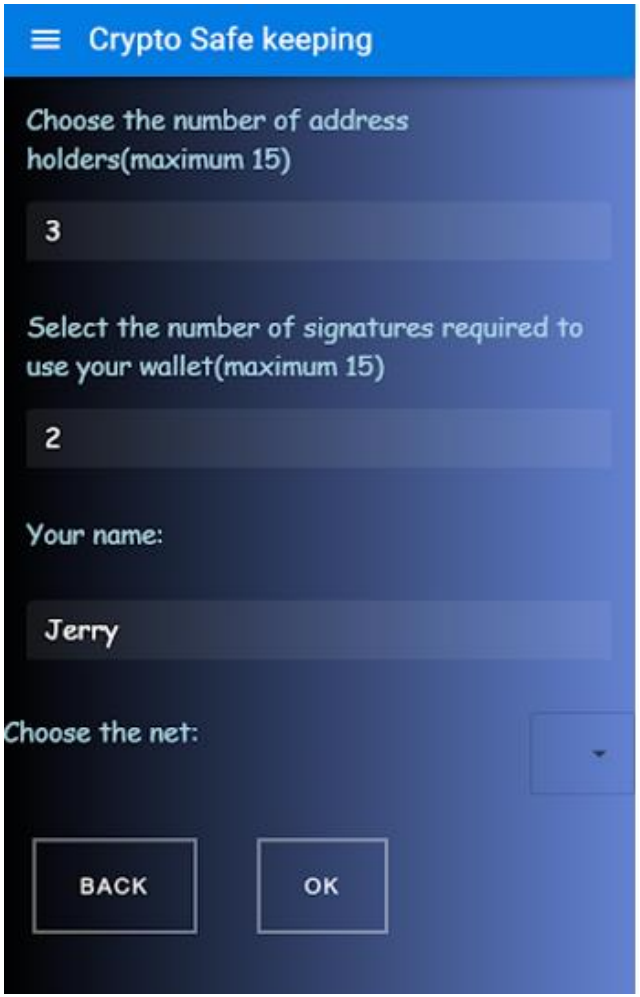
	Платформы	**Совместимость с node.js**	**Другие недостатки**
React Native	iOS и Android	невозможно создавать браузерные версии библиотек, требующих node.js	
Quasar	SPA, PWA, Mobile Apps(Android, iOS), Desktop Apps	да	
Flutter	iOS и Android	использует Dart	в конечный установочный пакет добавляется виртуальная машина Dart

Функциональность приложения

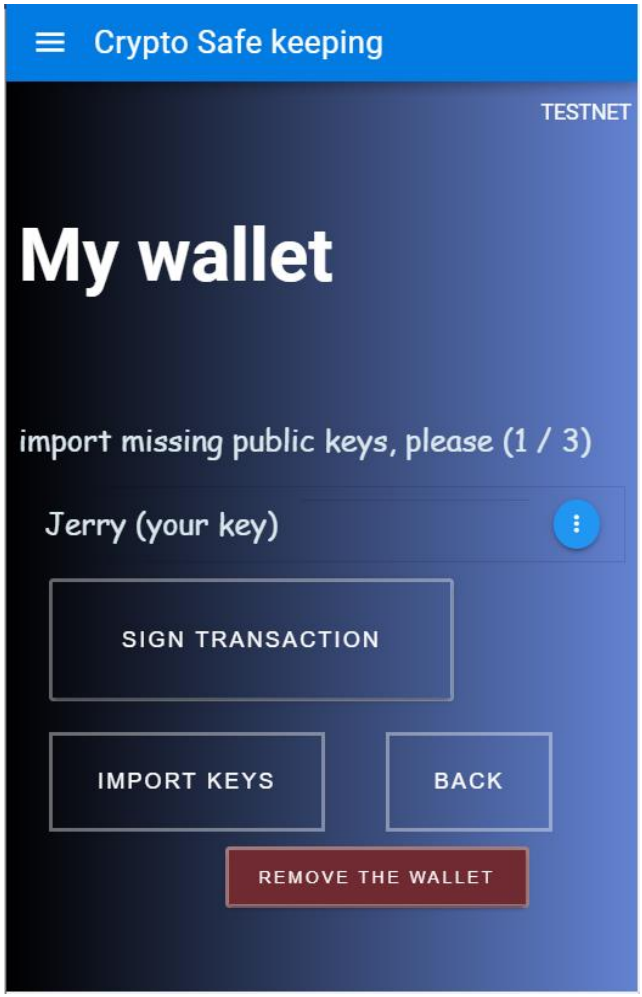
- Поддержка множества валют
- Хранение приватных и публичных ключей
- Генерация стандартного адреса или адреса с multisig поддержкой
- Подпись транзакции одним/несколькими ключами
- Ввод/вывод информации с помощью QR-кода

Импорт и экспорт данных

- 0200000001fb391949e08f00648ded9808f55230ea6a2e583dad54b5a2042ed66bd413574701000000920048304502210 0e17a4d065da8ed9ed8ecf83bb1255b9dec9db64e663b5483ac11e20caed87b71022028e9de572295ce5d709b39be7db6e1de95e71ab9fd2b85cbeb42bc7093c2d58301475121039a696dbc7a422faa42688bfef236dd9b81585676a6c2cb185e1db39a195757d92102647711598 1fe981a6918a6297d9803c4dc04f328f22041bedff886bbc2962e0152aeffffffff0110270000000000001976a914fbff95b4e35aca918d26e157392ea1643a2dc28388ac00000000



Генерация multisig адреса



Пример multisig адреса

Результаты

- Исследована предметная область
- Сделан обзор уже существующих решений
- Выбран стек технологий
- Разработана функциональность приложения
- Осуществлена поддержка стандартных и multisig адресов для Bitcoin
- Осуществлена поддержка стандартных адресов для Bitcoin Cash
- Разработан прототип UI