



Разработка криптовалютного шлюза

Смирнов Денис, группа 16.Б10-мм
Научный руководитель: доцент кафедры СП,
к.ф.-м.н. К. Ю. Романовский
Консультант: ст. пр. кафедры СП,
Я. А. Кириленко



Мотивировка

- ❑ Существует огромное количество непохожих друг на друга криптовалют
- ❑ Единый интерфейс для взаимодействия существенно упрощает работу с ними



Задачи

- ❑ Провести анализ существующих решений
- ❑ Спроектировать интерфейс
- ❑ Реализовать интерфейс для криптовалют Monero и Bitcoin
- ❑ Обеспечить способ восстановления корректного состояния в случае аварийного завершения работы
- ❑ Реализовать приложение, способное работать на двух платформах: Linux и Windows
- ❑ Протестировать различные варианты использования шлюза



Существующие решения

- ❑ Проприетарные

BitPay, Coingate, CoinPayments, Paycoiner

Недостатки: кастодиальные, комиссия за переводы, плата за размещение ПО

- ❑ OpenSource

BtcPay Server, Blockchain-Payment-System

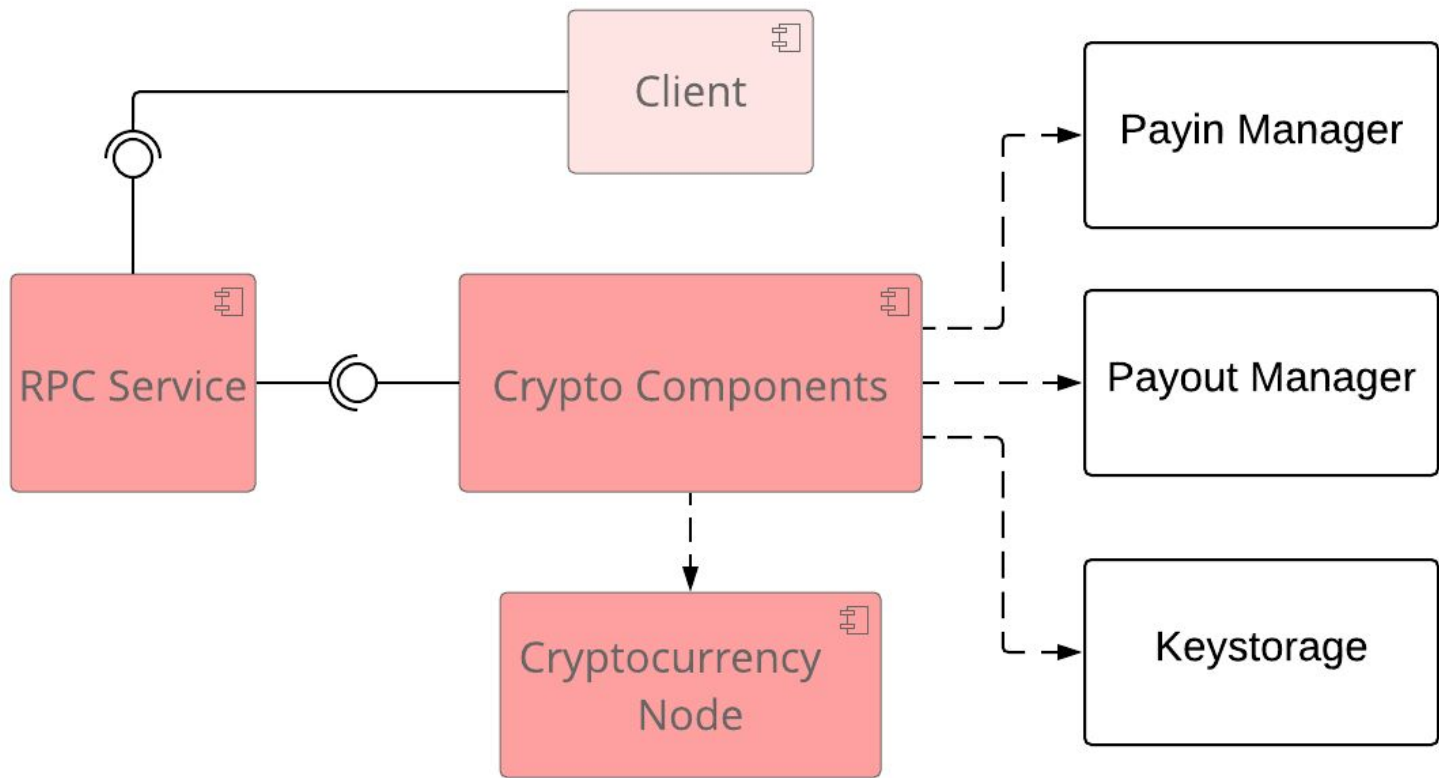
Недостатки: синхронный интерфейс, мало поддерживаемых валют



Технические требования к реализации

- ❑ Асинхронный интерфейс с минимальной задержкой на запросы
- ❑ Отсутствие персистентной БД в шлюзе
- ❑ Разработка на C++
- ❑ Шлюз должен быть инкапсулирован в отдельном приложении

Архитектура





Keystorage

- ❑ Инкапсулирует в себе криптографию и работу с ключами
- ❑ Использует детерминированные кошельки
- ❑ Позволяет избегать прямой работы с адресами



Payin Manager

- ❑ Поддерживает список отслеживаемых адресов
- ❑ Мониторит блокчейн и выдаёт внешнему сервису информацию о новых транзакциях на адрес из списка



Payout Manager

- ❑ Валидирует адреса
- ❑ Иницирует новые транзакции
- ❑ Производит оценку комиссии
- ❑ Используя специальные контексты, может самостоятельно вернуться в корректное состояние после аварийного завершения работы



Результаты

- ❑ Проведен анализ существующих решений
- ❑ Спроектирован интерфейс
- ❑ Интерфейс реализован для криптовалют Monero и Bitcoin
- ❑ Обеспечен механизм восстановления корректного состояния в случае аварийного завершения работы
- ❑ Реализовано приложение, способное работать на двух платформах: Linux и Windows
- ❑ Протестированы различные варианты использования шлюза