Pgpro_scheduler и криптовалютные транзакции

PgConf 2018

Фролков Иван, Постгрес Профессиональный

Задача

- Отправка транзакции в биткойн
- testnet

Биткойн для прикладного разработчика

- REST API
  - https://bitcoin.org/en/developer-reference
- CLI

Общие принципы

- Последовательность блоков
- Блок — множество транзакций
- Транзакция — это
  - Входы
  - Выходы
  - Скрипт
  - Сумма входов равна сумме выходов

Общие принципы

- Входы и выходы — адреса
- Адрес — пара (открытый ключ, закрытый ключ)
- Адрес в транзакции — хеш (SHA-256) открытого ключа + контрольная сумма, преобразованные в base58
  - https://ru.wikipedia.org/wiki/Base58
  - «A Bitcoin address is a 160-bit hash of the public portion of a public/private ECDSA keypair.»
- Пример адреса
  - 18dJEVXrurdiP2oNMNpshC1xmvA24zGm3s

Общие прицины

- Транзакция
  - https://en.bitcoin.it/wiki/Transaction
  - Сначала mempool, потом — блокчейн
  - Transaction fee
  - Id транзакции — SHA256 от составляющих (вход, выход, адреса, скрипт)

Общие принципы

- Транзакция (https://blockchain.info)
- Пример
  - Txid 196662003077d72525c9af8fa9a45cd8ea006dfe06609d2e4fed6c9f79cf077f
  - Входы (1NWEeSJwcMpRRFYgzKGxwgye5TVKeFLPCU (3.24000668 BTC — Вывод)
  - Выходы
    - 14ieF8q9dCFUWHGTF5gAvMTEfKnLXxU5d7 - (неизрасходованные) 0.32989492 BTC
    - 1NWo3gXunvF9NrvradTUoDFytBcjntTLt1 - (потраченный) 0.02739679 BTC
    - 1AXeR7o8qRRhZGutYWA1pzTuXS2yoa2Ae2 - (неизрасходованные) 0.00845633 BTC
    - 1EZ6kyc2kHvZnyU1baMkLTcxzDNLPixK6b - (неизрасходованные) 0.21481477 BTC
    - 12byH6GtxoRw9Lm2CteHsb2GPptmwx7jMa - (потраченный) 2.5436919 BTC
    - 3NeiiWQQCio73MzNmceykouG7YpQmBQqfQ - (неизрасходованные) 0.11538997 BTC
    - 4 Подтверждения
- Будьте аккуратнее при чтении блокчейна — один адрес может быть среди выходов несколько раз

Общие принципы

- Wallet
  - Совокупность пар (открытый ключ, закрытый ключ)
  - Пары с собой никак не связаны
  - Может иметь миллионы таких пар
  - Зачем? Должно быть потрачено все
  - Демон может автоматически подбирать набор адресов для отправки
  - Адреса сдачи

RPC API

- https://bitcoin.org/en/developer-reference
- ListTransactions
- SendFrom (deprecated) - RPC spends an amount from a local account to a bitcoin address.
- SendMany - The sendmany RPC creates and broadcasts a transaction which sends outputs to multiple addresses.
- SendToAddress - The sendtoaddress RPC spends an amount to a given address.

  Параметры: To Address, Amount, Comment, Comment To, Subtract Fee From Amount
  Возвращает: a TXID of the sent transaction

Проблема!!!

RPC API

- SendRawTransaction
  - Допускает идемпотентность
  - А где ее, RawTransaction, собственно, взять?
- CreateRawTransaction
  - Требуется самому формировать массив входов
    - Вход - «An input in a transaction which contains three fields: an outpoint, a signature script, and a sequence number. The outpoint references a previous output and the signature script allows spending it.»
- Слишком низкоуровнево

Все-таки SendToAddress

- Проблемы:
  - Нет идемпотентности
  - Разумеется, нет двухфазного коммита
  - Неотменяемая операция
- Замечание:
  Waves Platform (https://wavesplatform.com/)
  умеет отдельно создавать транзакции и отдельно отправлять. Почему-то больше это не умеет никто.

Что делать?

- Этапы
  - Блокировка платежа
  - Отправка
    - Выбор результата
      - Удачно
        - Ждем требуемое число подтвержений
        - Готово
      - Невосстановимая ошибка
        - Обрабатываем ошибку
        - Готово
- Это все задачи для pgpro_scheduler
- Каждая задача зависит от предыдущей