Минималистичный консольный “bitcoin-кошелёк”

Описание задачи

Разработайте консольный скрипт для сети bitcoin signet, который будет:

- генерировать и сохранять в файл в собственной директории приватный ключ для одного биткоин-адреса
- показывать баланс средств на данном адресе
- отправлять указанное количество средств на указанный пользователем другой адрес

Перед отправкой скрипт должен проверять, достаточно ли средств для отправки (включая комиссию майнерам).

Комиссия майнерам должна составлять 0.00001 sBTC.

Бонусные баллы (можно выполнить любое количество из нижеперечисленных пунктов, указаны примерно в порядке нарастания сложности)**:**

- Напишите Dockerfile и docker-compose.yml, позволяющие запустить скрипт локально в докере
- Рассчитывайте комиссию майнерами пропорционально размеру (в vbyte) получившейся транзакции

Внешние ресурсы: “необходимо и достаточно”

Если понадобятся дополнительные тестовые (signet) BTC, то их можно бесплатно получить набрав в Google “Bitcoin signet faucets”, например:

- https://signetfaucet.com/
- https://signetfaucet.bublina.eu.org/

Если этого будет недостаточно, напишите, и мы пришлем дополнительные BTC.

Если понадобится **Bitcoin Signet кошелек** для тестирования транзакций, то можно использовать Electrum, запустив его с флагом --signet: https://electrum.org/#download

Для **формирования BTC транзакции** используйте, например, библиотеку: https://github.com/chaintope/bitcoinrb

(Либо любую другую на ваше усмотрение.)

Для исследования hex транзакций можно использовать https://live.blockcypher.com/btc/decodetx/

Для **бродкаста транзакций** (и получения данных по транзакциям, уже включенным в блокчейн) используйте Mempool: https://mempool.space/signet/docs/api/rest

Подсказки:

- Посмотрите, что такое UTXO (unspent transaction outputs). Проще всего сделать так, чтобы каждая очередная транзакция в качестве входов использовала *все* UTXO, соответствующие вашему адресу обменника.
- Адрес разрабатываемого “кошелька” в любой момент может быть пополнен из другого кошелька. Транзакция пополнения в качестве *одного* из выходов будет содержать адрес, сгенерированный скриптом (другие выходы - “сдача”). Для создания расходной транзакции вам потребуется определить, какой выход каждой из транзакций пополнения ведёт к вашему адресу обменника (см. документацию по ссылкам выше). В API blockstream есть способ получить выходные адреса bitcoin-транзакции.

Ликбез по блокчейну (опуская детали)

Блокчейн состоит из цепочки транзакций.

Для совершения операции “перевода” с одного адреса на другой создаётся транзакция, “входом” (input) которой является первый адрес, а “выходом” второй. Транзакция может содержать несколько входов и несколько выходов.

Разница (в сумме “монет”) между всеми выходами и всеми входами определяет комиссию майнеров; если комиссия нулевая, транзакция не будет обработана майнерами - стоит оставить им некоторую плату.

Для того, чтобы потратить только часть “монет” с некоторого адреса, в качестве дополнительного выхода транзакции устанавливается адрес, находящийся под контролем отправителя. Иначе говоря, “сдача” с операции в явном виде должна быть перечислена себе.