**Кейс:** обеспечить безопасность 800+ BTC/день проходящих через POOL с подписанием транзакции. Разработать механизмы проверок.

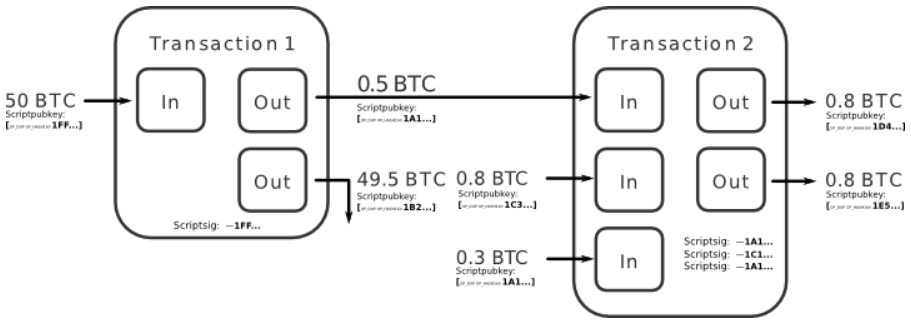
**Логика:** позволяет двум и более пользователям подписывать транзакции уникальными подписями, - разновидность пороговой подписи. BTC хранящиеся на адресе, всегда тратятся целиком, распределившись на несколько исходящих отдельных bitcoin-адресов. Разницу между входящими и исходящими отправляется майнеру в качестве комиссии. Позволяет не использовать один и тот же адрес, и возвращать его на новый адрес. Адрес содержит хеш, принимающий решение, разрешить ли тратить BTC.

**Схемы подписей:**

- 3 из 5: с низким уровнем доверия. Трое могут расходовать, переводить на адрес может любой. Уменьшает риск растраты, взлома, заражения вирусами и утраты средств.
- 2 из 3: кошелек горячего хранения. Биржа хранит приватный ключ, другой ключ – резерв. Кибербезопасность хранит третий ключ онлайн и подписывает после проверки.
- 2 из 3: с условным счетом (эскроу). Перевод с одного адреса на другой, где третий - арбитр. Если транзакция успешна, подписывают транзакцию, возвращая средства.

**Решение безопасности:**

- Использование SSO (Yubikey 5, Kensington) по PKCS#11. Генерация JWT-токена на стороне POOL с единым временем длины сессии. Распределение по типам через push-уведомления. Контрольные пуши с типом операции и суммой, Tx id, мониторгу блокчейна, дашборбу операций и информирования ответственных лиц. Все токены используются для подтверждения личности: токен со статическим паролем; токен с синхронно динамическим паролем; токен с асинхронным паролем по Варнаму; токен вызов-ответ. Передается не ключ, а указатель на ключ. Handle используется в операциях с закрытым ключом, при формирование подписи. Подпись формируется внутри токена/смарткарты. Наружу попадает только значение самой подписи.
- Kill-Switch — тайм-аут, превышающей лимит, с возможностью отмены, используя мастер-кошелек по защищенной линии. Отдельный смарт-контракт, в который смотрит Multisig, где мастер-кошелек по вызову возвращает транзакцию в сети. Использование transaction guard на уровне API. Подпись не всегда означает инициализацию транзакции. Холдирование каждой 3-5 транзакций с одного подписанта и блокирование до проверки осуществления транзакции. Надстройка отправки json параметров через хранилище или сейф - логирование действие пользователей при осуществлении операций и вывод лога в мониторинг.
- Ограничение лимита вывода по типам использования, запросам от подписанта, интервала запроса, очередность обращений, сумм, транзакций с уведомлением пользователя (timelock), счетов, повторных операций в интервале, запросов в дефиницу времени, потолка сумм с использованием SSO. Ограничение схем и чередование.
- Использование дочерних кошельков при транзакциях, где при запросе конкретной суммы формируется временный кошелек.
- HSM: решение на базе OpenVZ – множество изолированных ОС на одном ядре в отдельных контейнерах.


Transaction 1
50 BTC
Scriptpubkey:
[OP_DUP OP_HASH160 1FF...]
In
Out
Out
Scriptsig: —1FF...
0.5 BTC
Scriptpubkey:
[OP_DUP OP_HASH160 1A1...]
49.5 BTC
Scriptpubkey:
[OP_DUP OP_HASH160 1B2...]
Transaction 2
0.8 BTC
Scriptpubkey:
[OP_DUP OP_HASH160 1C3...]
0.3 BTC
Scriptpubkey:
[OP_DUP OP_HASH160 1A1...]
In
In
In
Out
Out
Scriptsig: —1A1...
Scriptsig: —1C1...
Scriptsig: —1A1...
0.8 BTC
Scriptpubkey:
[OP_DUP OP_HASH160 1D4...]
0.8 BTC
Scriptpubkey:
[OP_DUP OP_HASH160 1E5...]