Contest new non-custodial and simplified way to connect wallet and classic user interface

целевая аудитория разработчиков смарт-контрактов, которые понимают что метамаск и другие аналогичные решения это не верх изящества — цель увеличить шанс трансформации человека в крипто-энтузиасты и предоставить инструмент для строительства игровую площадки для котиков

Цель: Упростить взаимодействие сайтов-dapp с кошельками пользователей сохранив максимальную безопасность средств.

Описание: Модернизация стандартного кошелька SetcodeMultisig.. позволяющая добавить в кошелек временный публичный ключ, который может осуществлять транзакции от кошелька в рамках заданного лимита средств. Немного похоже на метод ERC-20 allowance

Сферы применения: Сайт-dapp может сгенерировать для пользователя пару ключей, которой пользователь может позволить осуществлять транзакции от своего кошелька в рамках заданного лимита. Это позволит приложению использовать кошелек пользователя, но в определенных рамках. Основные средства пользователя останутся в безопасности. При этом основные функции кошелька останутся неизменными, что позволит использовать этот контракт даже в приложениях не поддерживающих новую функцию.
Возможность подкрепить свой контракт к непроверенному приложению кошельку, ограничив лимитом средства доступные для вывода.

Воркфлоу1: (вариант с передачей сайту адреса контракта)

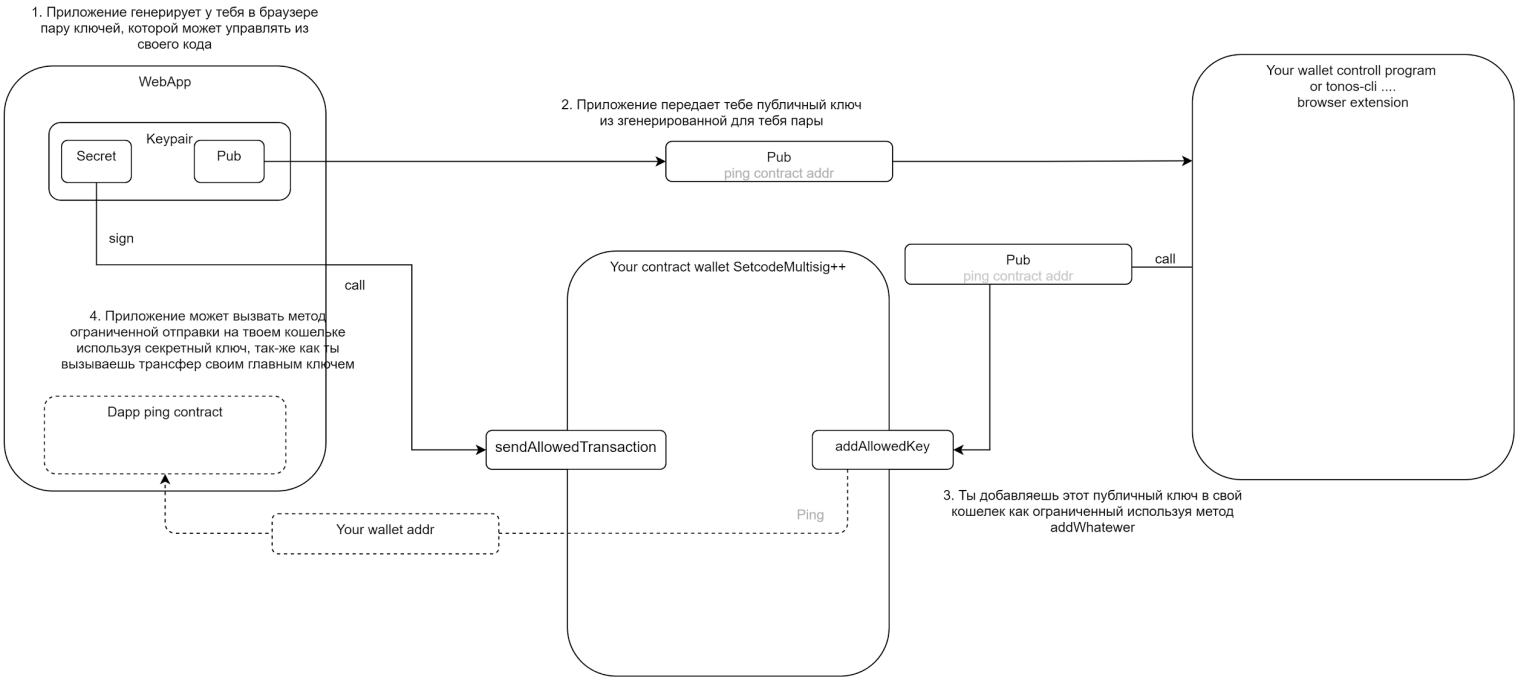
1. пользователь вводит на сайте адрес кошелька-контракта, который он хочет добавить в приложение.

2. Сайт генерирует пару ключей и передает пользователю публичный или подготавливает транзакцию, которую пользователь должен подписать основным ключем и отправить своему контракту.
3. Пользователь подписывает и отправляет транзакцию или вызывает метод своего кошелька addAllowedKey передавая публичный адрес созданный сайтом и лимит, который можно потратить этим ключем.
4. Сайт может подписывать секретным ключем транзакции к кошельку пользователя в рамках лимита.
5. Пользователь может отменить права, например передав в тот же метод публичный адрес и лимит равный нулю

Воркфлоу2: (с пингом)

1. Сайт генерирует пару ключей и передает пользователю публичный ключ и адрес своего спец контракта, принимающего транзакции “пинги”. Или подготавливает соответствующую транзакцию на подпись.
2. Пользователь подписывает транзакцию или отправляет на свой контракт транзакцию на метод addAllowedKey передавая публичный адрес для временного доступа, лимит, и адрес пинг-контракта. После добавления публичного ключа во “временные кастодианы” метод отправляет транзакцию на контракт принимающий пинги, передавая свой публичный ключ и лимит. Таким образом приложение получает адрес контракта пользователя и знает какой ключ доступа ему соответствует, а так-же лимит заданный пользователем
3. Сайт может подписывать секретным ключем транзакции к кошельку пользователя в рамках лимита.

- Если в кошельке более 1 кастодиана, то нужно предусмотреть добавление “временных кастодианов” консенсусом кастодианов.


1. Приложение генерирует у тебя в браузере пару ключей, которой может управлять из своего кода
WebApp
Keypair
Secret
Pub
sign
call
2. Приложение передает тебе публичный ключ из згенерированной для тебя пары
Pub
ping contract addr
Your wallet controll program
or tonos-cli ....
browser extension
Pub
ping contract addr
call
Your contract wallet SetcodeMultisig++
4. Приложение может вызвать метод ограниченной отправки на твоем кошельке используя секретный ключ, так-же как ты вызываешь трансфер своим главным ключем
Dapp ping contract
sendAllowedTransaction
addAllowedKey
3. Ты добавляешь этот публичный ключ в свой кошелек как ограниченный используя метод addWhatewer
Ping
Your wallet addr