



Ton Connect

3. JavaScript SDK: single QR & ton_proof

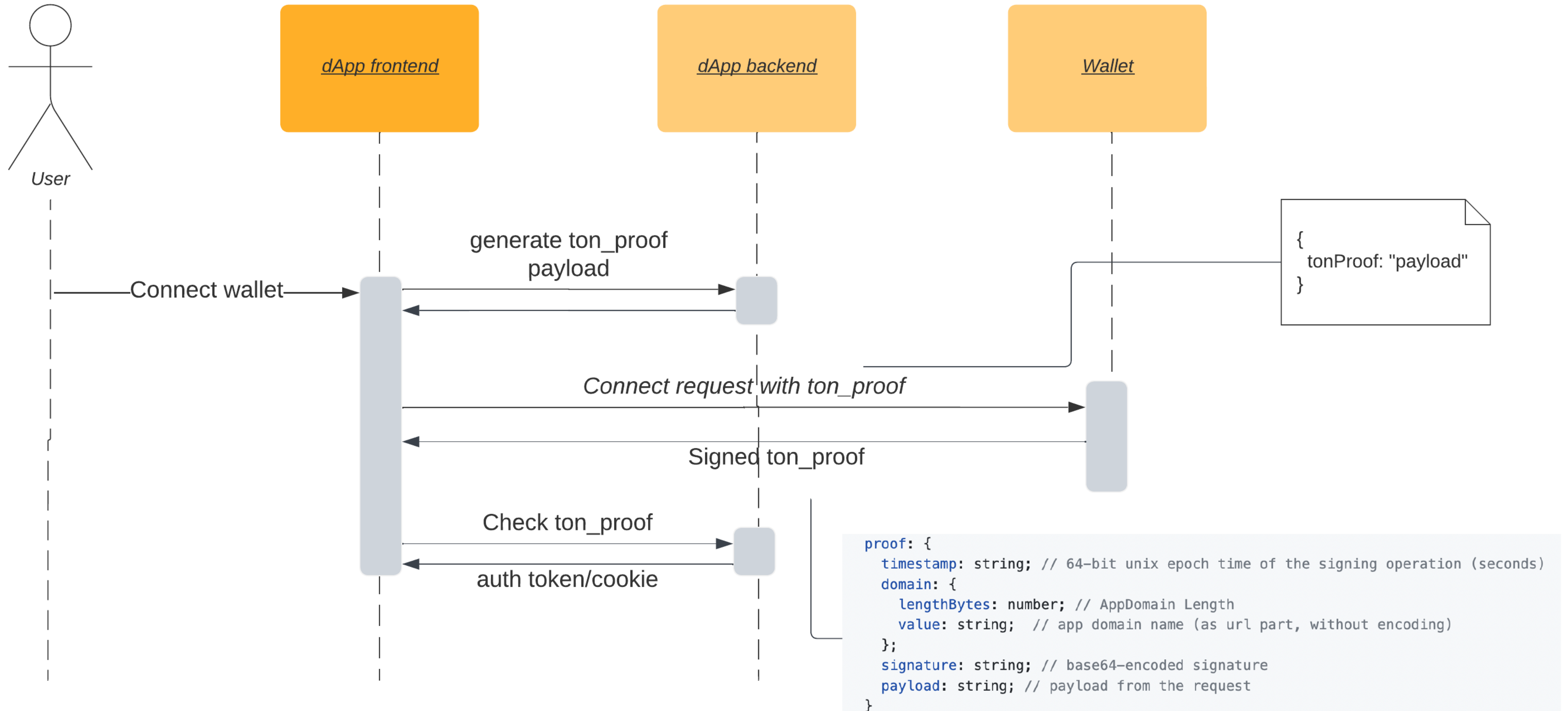
wallets-list.json

```
{
  "name": "Tonkeeper",
  "image": "https://tonkeeper.com/assets/tonconnect-icon.png",
  "tondns": "tonkeeper.ton",
  "about_url": "https://tonkeeper.com",
  "universal_url": "https://app.tonkeeper.com/ton-connect",
  "bridge": [
    {
      "type": "sse",
      "url": "https://bridge.tonapi.io/bridge"
    },
    {
      "type": "js",
      "key": "tonkeeper"
    }
  ],
}
```

Элемент списка кошельков

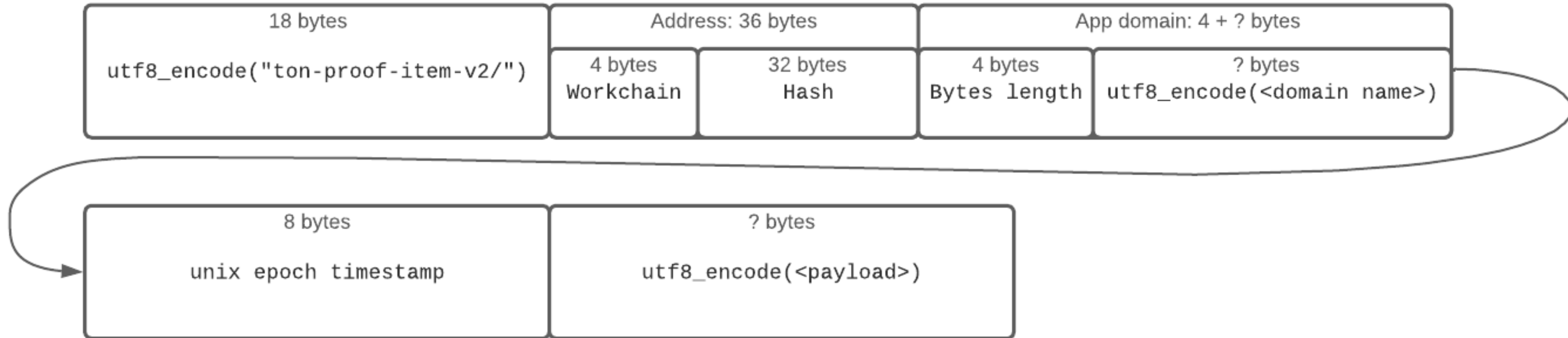
Репозиторий: <https://github.com/ton-blockchain/wallets-list>

Ton proof: схема авторизации



Ton proof: структура подписи

Message =



signature = Ed25519Sign(privkey, sha256(

0xffff	utf8_encode("ton-connect")	sha256(Message)
--------	----------------------------	-----------------

)))

Подробнее: https://github.com/ton-blockchain/ton-connect/blob/main/requests-responses.md#address-proof-signature-ton_proof

Проверка `ton_proof` на бэкэнде

- Получить с фронтенда данные: адрес кошелька, домен, `timestamp`, `walletStatelnit`, подпись
- Проверить, что домен соответствует домену вашего приложения
- Проверить, что этот `payload` был выдан недавно (можно выдавать куки с `payload` перед авторизацией, и при проверке `ton_proof` проверять наличие куки у этого клиента)
- Собрать `message` по схеме из предыдущего слайда
- Получить `pubkey` кошелька через `get` метод контракта-кошелька
- Если контракт не активен, то получить ключ таким способом не удастся; нужно распарсить `walletStatelnit`, которое передает фронтенд
- Проверить, что подпись с фронтенда действительно подписывает собранный `message` и соответствует публичному ключу адреса

Проверка ton_proof, примеры

- На Go <https://github.com/ton-connect/demo-dapp-backend>
- На JS <https://gist.github.com/TrueCarry/cac00bfae051f7028085aa018c2a05c6>