

DOWN THE DRAIN

Unpacking TON of Crypto Drainers



Elizabeth @qwqoro



WHOAMI

ELIZABETH

QWQORO

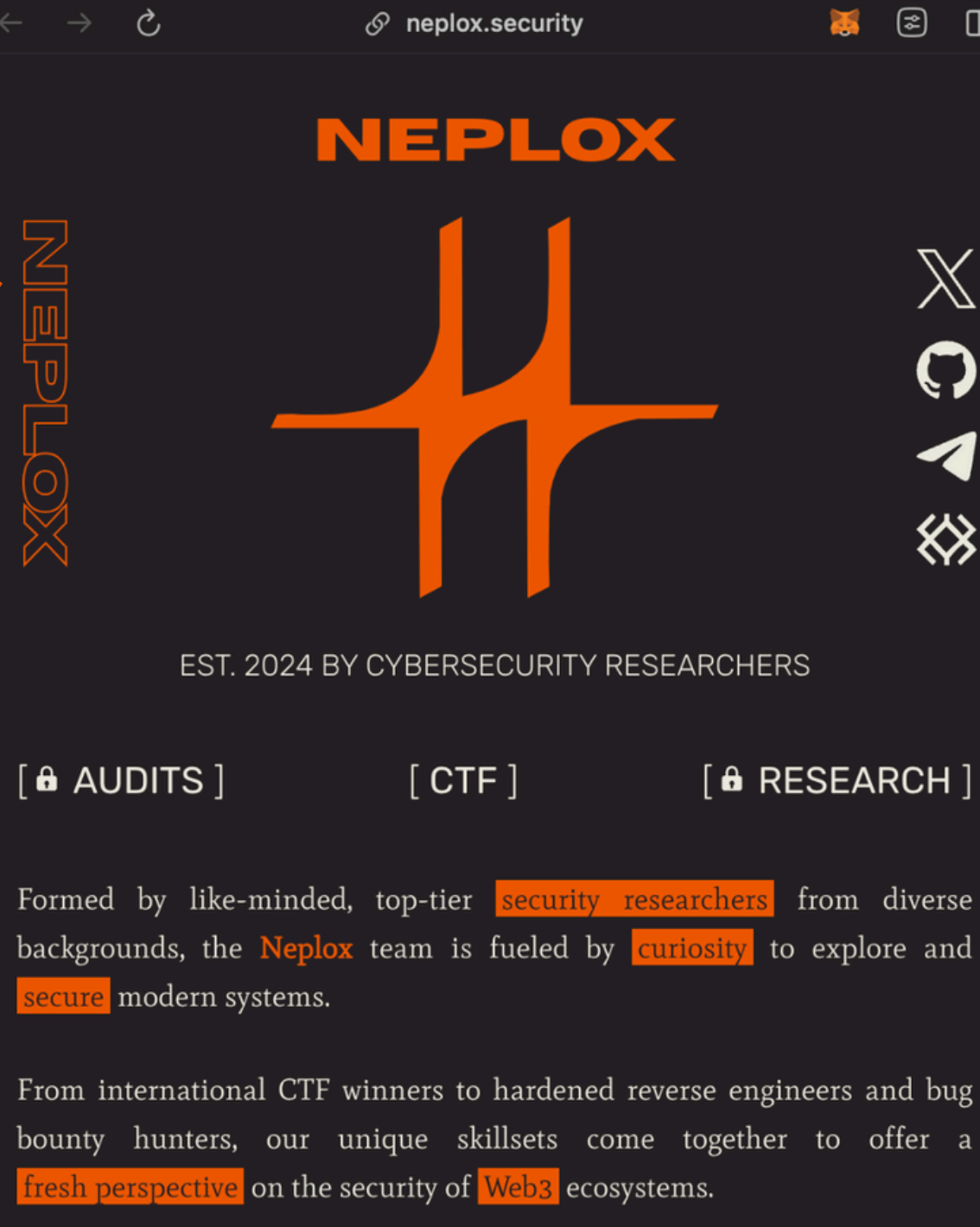


Researcher @ Neplox

AppSec Tech Lead @ DeteAct

Web Pentester

OSCP



×

NEPLOX

2

DOWN THE DRAIN
UNPACKING TON OF CRYPTO DRAINERS

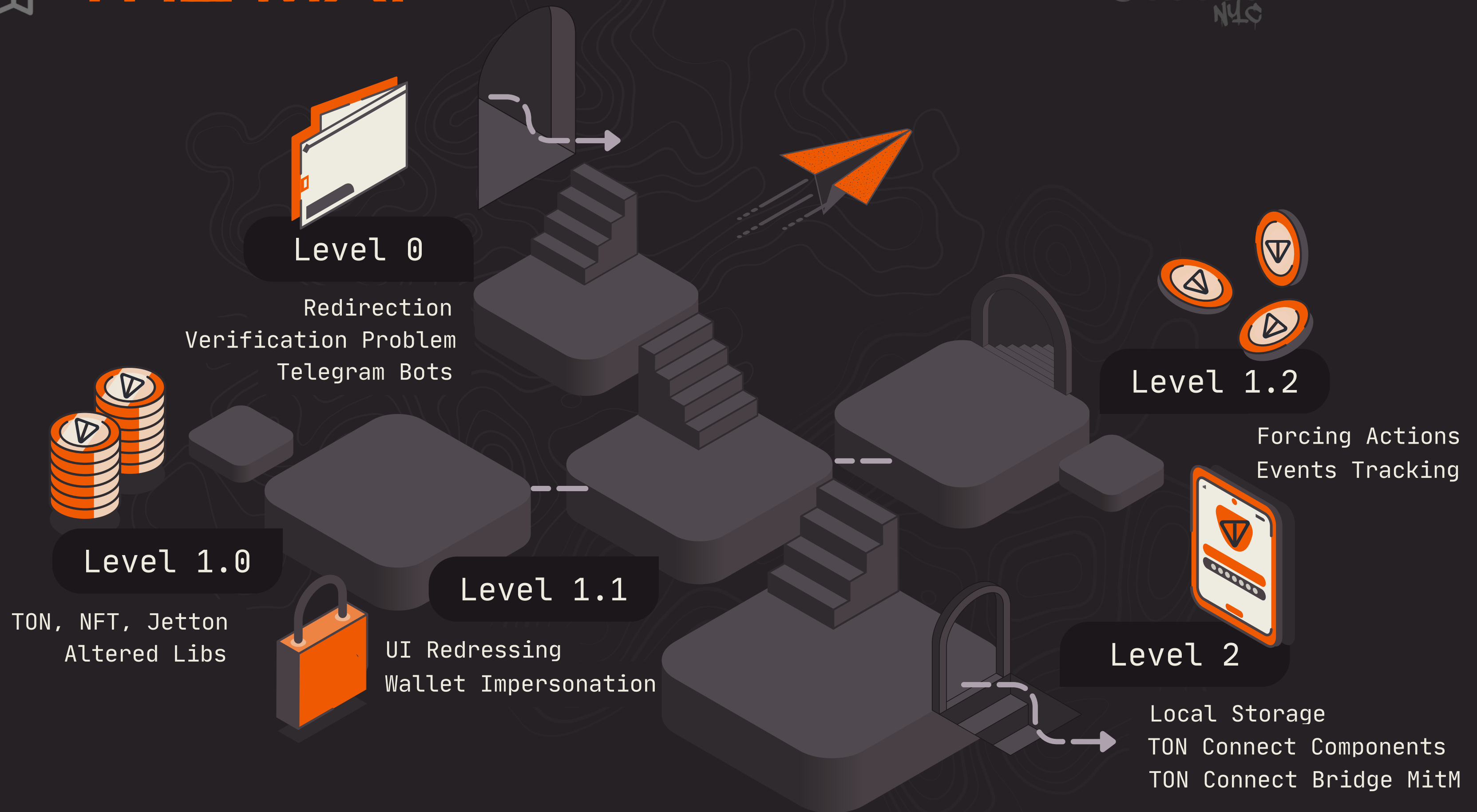
OCT 18, 2025
NEW YORK

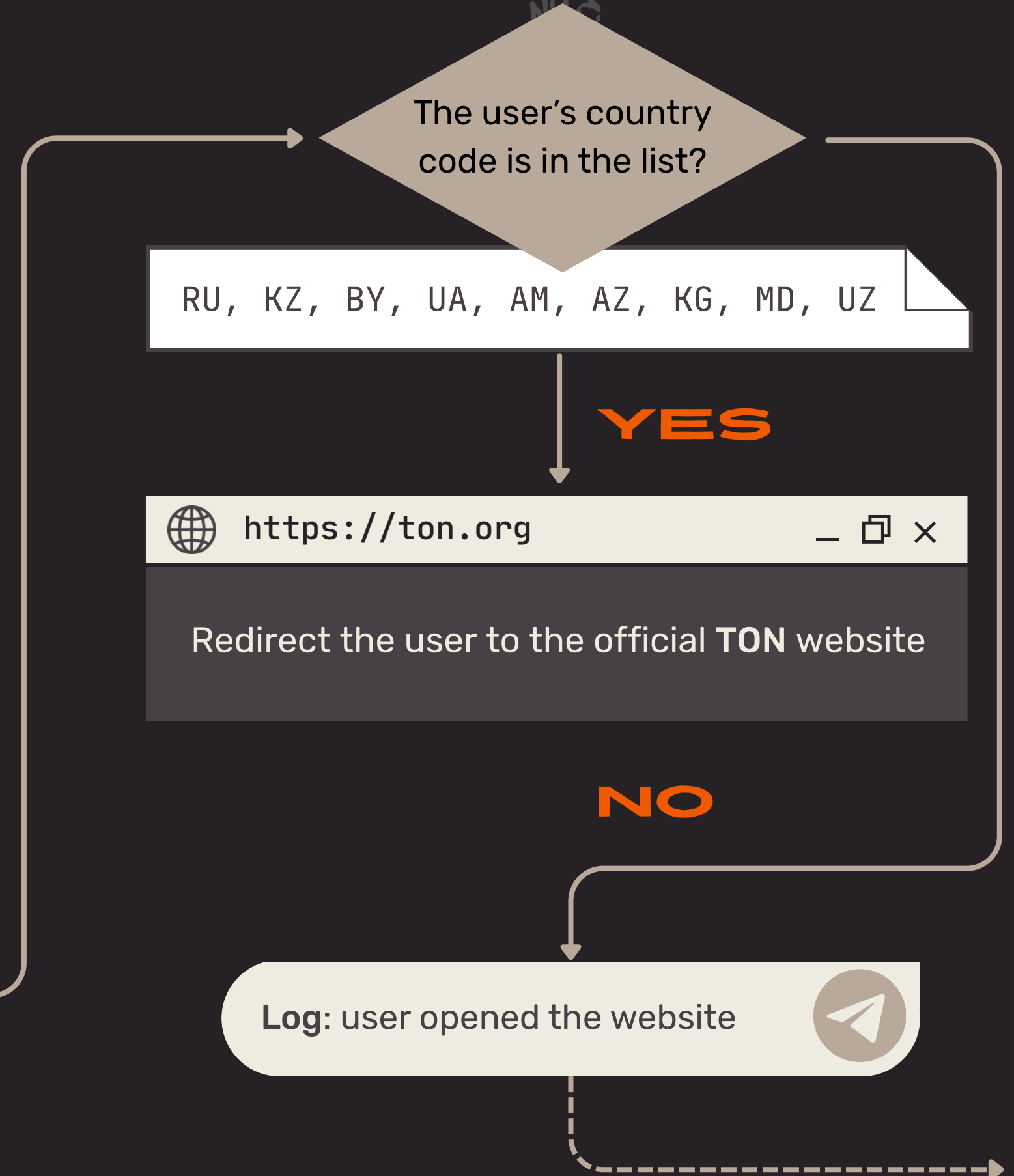
BSIDESNYC
CONFERENCE





TON DRAINERS THE MAP







! https://MALICIOUS[.]site

@tonconnect/ui

@tonconnect/sdk

tonconnect-manifest.json

```
{
  "url": "https://LEGIT[.]site",
  "name": "LEGIT APP",
  "iconUrl": "https://LEGIT[.]site/logo.png"
}
```

index.html



Connect Wallet

CLICK ME

index.js

```
onclick = function() {
  ...
}
```



https://toncenter.com/api/...

Get user's TON balance based on their wallet address

index.js

```
transaction = {
  validUntil: 1 min,
  messages: [{
    address: MALICIOUS,
    amount: 97% of balance
  }, ]
}
```

Send transaction via TonConnect UI

Log: success / fail transaction





51 TON (≈ 179 USD)
[87] [REDACTED] [2025-05-12 08:01:36+00:00] 🛠️ Creating request (UQDe...Vedu)

50 TON (≈ 175 USD)
[88] [REDACTED] [2025-05-12 08:01:39+00:00] ❌ Declined Transfer (UQDe...Vedu)

50 TON (≈ 175 USD)
[89] [REDACTED] [2025-05-12 08:01:55+00:00] 🛠️ User Connected Wallet (UQDe...Vedu)

🌐 [REDACTED] - 📍 NL

\$ (≈ 175 USD)

-

51 TON (≈ 179 USD)
[90] [REDACTED] [2025-05-12 08:01:55+00:00] 🛠️ Creating request (UQDe...Vedu)

50 TON (≈ 175 USD)
[91] [REDACTED] [2025-05-12 08:01:59+00:00] ❌ Declined Transfer (UQDe...Vedu)

50 TON (≈ 175 USD)
[92] [REDACTED] [2025-05-12 08:02:16+00:00] 🛠️ User Connected Wallet (UQDe...Vedu)

🌐 [REDACTED] - 📍 NL

\$ (≈ 179 USD)

-

51 TON (≈ 179 USD)
[93] [REDACTED] [2025-05-12 08:02:16+00:00] 🛠️ Creating request (UQDe...Vedu)

50 TON (≈ 175 USD)

\$ (≈ 179 USD)

-

51 TON (≈ 179 USD)
[93] [REDACTED] [2025-05-12 08:02:16+00:00] 🛠️ Creating request (UQDe...Vedu)

50 TON (≈ 175 USD)
[94] [REDACTED] [2025-05-12 08:05:50+00:00] ✅ Approved Transfer (UQDe...Vedu)

50 TON (≈ 175 USD)
[95] [REDACTED] [2025-05-12 08:05:58+00:00] 🛠️ User Connected Wallet (UQDe...Vedu)

🌐 [REDACTED] - 📍 NL

\$ (≈ 407 USD)

-

116 TON (≈ 407 USD)
[96] [REDACTED] [2025-05-12 08:05:58+00:00] 🛠️ Creating request (UQDe...Vedu)

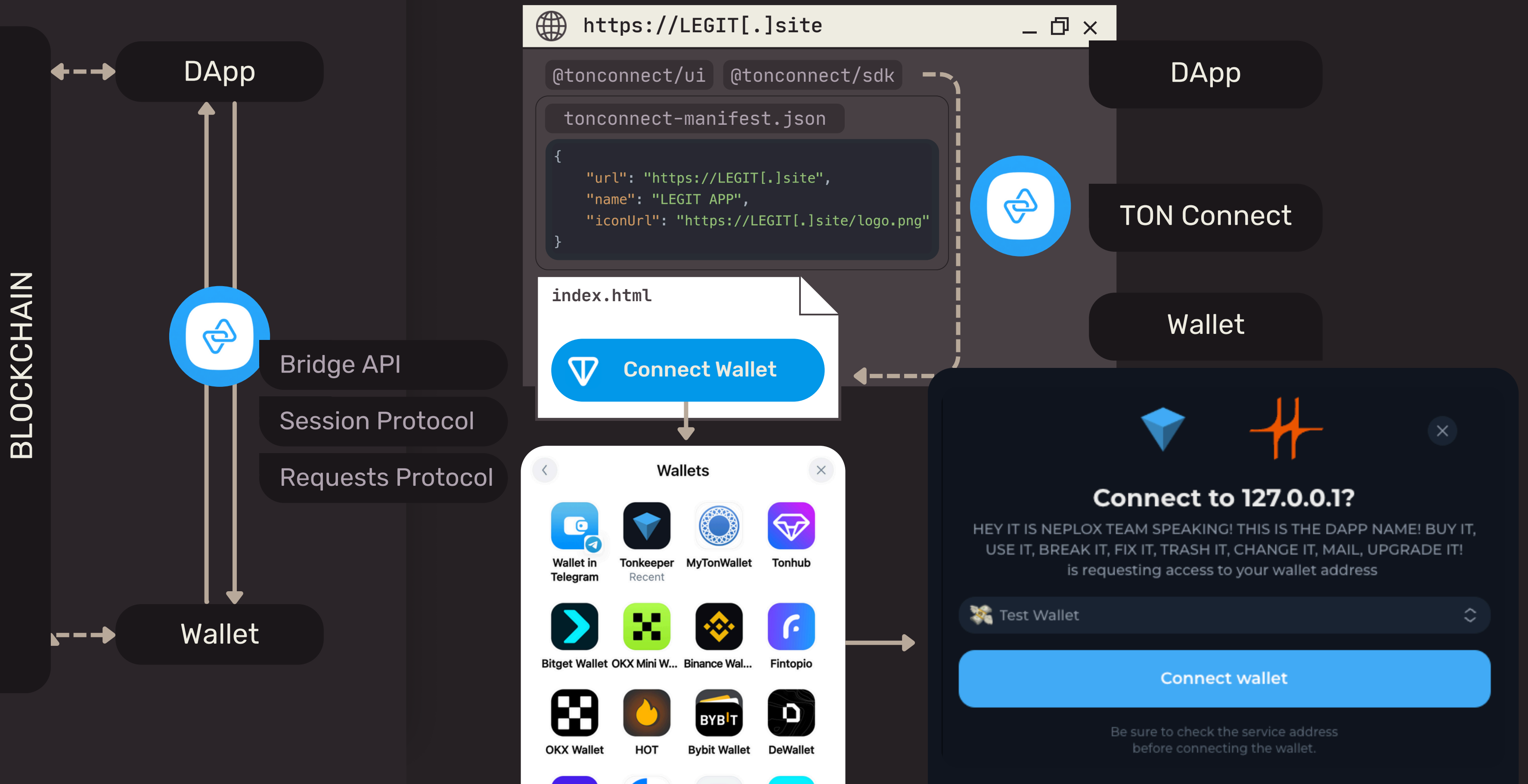
115 TON (≈ 403 USD)
[97] [REDACTED] [2025-05-12 09:14:37+00:00] 🌐 User opened the website

🌐 en | [REDACTED]

📍 NL
[98] [REDACTED] [2025-05-12 09:21:27+00:00] 🌐 User opened the website

🌐 en | [REDACTED]

📍 NL
[99] [REDACTED] [2025-05-12 09:22:42+00:00] 🛠️ User Connected an empty Wallet (UQCs...)





TON DRAINERS

NOTE: TONKEEPER



×

NEPLOX

8

pocs.neplox.security/...

Connect Wallet

TEST

DRAIN

Tonkeeper

Continue in Tonkeeper browser extension...

Retry

Mobile

Desktop

TON Connect

Test Wallet

\$0

Multichain



Buy



Send



Receive



Swap



TON

\$3,19 -0.15%

0

\$0

Connect to ton.vote?

TON Vote is requesting access to your wallet address

Connect wallet

Be sure to check the service address
before connecting the wallet.



Connected Apps



ton.vote
TON Vote

Disconnect

pocs.neplox.security/...

0QBC...-vxy

TEST

DRAIN

Testnet Wallet

\$19,44

TESTNET

0QBC...-vxy



Send



Receive



TON

\$3,19 -0.15%

6,09

\$19,44

AIOTX

1.00

Confirm transaction

Wallet: Testnet Wallet



Sent

0QCM...fwnX

-1,00 TON

19:14

Multiplier: 1 TON for 5 TON



Fee

0,003190337 TON

≈ \$0,01



TON DRAINERS

NOTE: MYTONWALLET



×

NEPLOX

9

pocs.neplox.security/...

Connect Wallet

TEST

DRAIN

MyTonWallet

Continue in MyTonWallet browser extension...

Retry

Mobile

Desktop

TON Connect

Test Wallet -

\$0-

Connect Dapp



TON Vote
ton.vote

Connect

Connect Dapp

Dapp Permissions

TON Vote will be able to view wallet address and balance.

Cancel

Connect

Open MyTonWallet to confirm the transaction.

TEST

DRAIN

Confirm the transaction in MyTonWallet
It will only take a moment.

Back

Dapps

Disconnect All Dapps

You can log in on dapps that support MyTonWallet. They can view wallet address, balance, and request operations.

LOGGED IN WITH MYTONWALLET



TON Vote
ton.vote

Disconnect

Back

Dapps

Disconnect All Dapps

You can log in on dapps that support MyTonWallet. They can view wallet address, balance, and request operations.

LOGGED IN WITH MYTONWALLET

Send Transaction

Testnet MyTonWallet
1.99 TON



1 Transaction

1 TON to 0QBC46...XI-vxy

Preview

Send

- 1 TON
to 0QBC...vxy

Multiplier: 1 TON for 5 TON

Fee ~ 0.006 TON



TON DRAINERS

NOTE: TONWALLET



×

NEPLOX

10

pocs.neplox.security/...

Connect Wallet

TEST

DRAIN

TON Wallet

\$0-

Connect Dapp



TON Vote
ton.vote

Connect Dapp

Dapp Permissions

TON Vote will be able to view wallet address and balance

Cancel

Connect

< Back

Dapps

Disconnect All Dapps

You can log in on dapps that support TON Wallet. They can view wallet address, balance, and request operations.

LOGGED IN WITH TON WALLET



TON Vote
ton.vote

Disconnect



TON Wallet



Continue in TON Wallet browser extension...

Retry



TON Connect

TON Wallet

\$0-



UQCMBN...uif7Jd

pocs.neplox.security



Receive



Send

0QCM...fwnX

TEST

DRAIN



Confirm the transaction in TON Wallet

It will only take a moment.

Testnet Version

Testnet Wallet 2

\$6.37-

↓ 0.01% · \$0.0006

Send Transaction

Testnet Wallet 2

1.99 TON

Receiving Address

0QCM...fwnX

Amount

1 TON (\$3.18)

Comment

Multiplier: 1 TON for 5 TON



View



TON DRAINERS

NOTE: TG @WALLET



×

NEPLOX

11

pocs.neplox.security/...

Connect Wallet

Wallet

Scan the QR code below with your phone's or Wallet's camera



Connect Wallet in Telegram on desktop

TON Connect

Wallet



TON Vote wants to connect to TON Space UQCM...f7Jd

This app will be able to view your TON address, balance and activity.

This app won't be able to move funds without permission.

Decline

Connect

Wallet



TON Vote now connected to TON Space UQCM...f7Jd

Back to TON Vote

Wallet

Connected Apps

 TON Vote
https://ton.vote

Disconnect all apps

pocs.neplox.security/...

0QCM...fwnX

TEST

DRAIN

Confirm the transaction in Wallet

It will only take a moment.

Open wallet

Wallet



Confirm transaction from TON Vote to UQCM...f7Jd
ton.vote

You send

 Toncoin

1 TON
₹250.50

Show Details



TON DRAINERS

NOTE: XTON WALLET



× NEPLOX

12

pocs.neplox.security/...

Connect Wallet

TEST

DRAIN

XTONWallet

Continue in XTONWallet browser extension...

Retry

TON Connect

3.19 USD

Please, provide information about your current account (address and public key) only if you trust this web-page



TON Vote
Origin

https://pocs.neplox.security

☐ Don't ask me when reconnecting

Cancel

Provide

3.19 USD

Manage Dapp permissions

Search by domain

▶ https://pocs.neplox.security

DELETE SELECTED PERMISSIONS

Back

pocs.neplox.security/...

UQAK...GvDz

TEST

DRAIN

Confirm the transaction
in XTONWallet
It will only take a moment.

3.19 USD

Send transaction

Address

UQBC...

Amount

TONCOIN

-0,0008

Fee ~ 0.0008 Total 0.0000

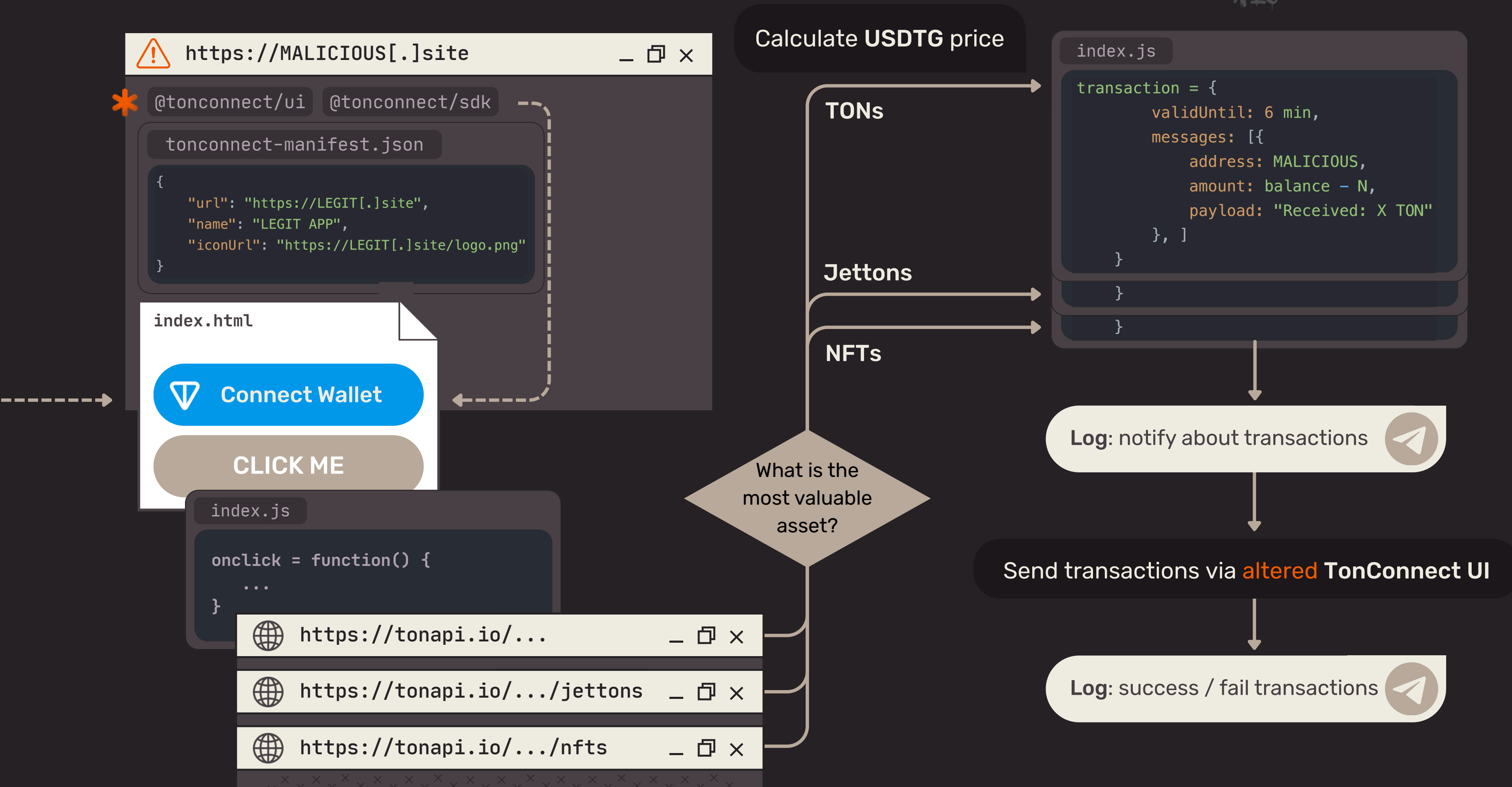
Data

te6ccsEBAQEAJQAAAEYAAA/

State init

Cancel

Confirm





TON DRAINERS LEVEL 1.1

! https://MALICIOUS[.]client

@tonconnect/ui @tonconnect/sdk

tonconnect-manifest.json

```
{
  "url": "https://LEGIT[.]site",
  "name": "LEGIT APP",
  "iconUrl": "https://LEGIT[.]site/logo.png"
}
```

index.html



Connect Wallet

index.js

```
transaction = {
  validUntil: 6 min,
  messages: [{
    address: MALICIOUS,
    amount: balance - N,
    payload: "Received: X TON"
  }, ]
}
```

CLIENT

notifyUserOpened

Log: user opened the website

getOperatorWalletAddress

getMinimalBalance

getSavedForFees

notifyUserConnected

https://toncenter.com/api/...

https://tonapi.io/.../jettons

https://tonapi.io/.../nfts

Get information on user's assets based on their wallet address

Calculate USDTG price

What is the most valuable asset?

TONs

NFTs

Jettons

createBOCTONs

createBOCNFTs

createBOCJettons

Send transaction via TonConnect UI

notifyTransactionStatus

Log: success / fail transactions

SERVER



index.js

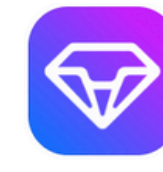
```
const tonConnectUI = new TonConnectUI({
  manifestUrl: '<URL>',
  buttonRootId: '<ID>',
  walletsRequiredFeatures: {
    sendTransaction: {
      minMessages: 4,
      extraCurrencyRequired: true
    }
  }
})
```



Connect Wallet



Wallets

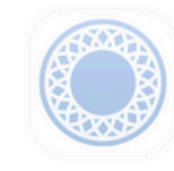
Wallet in
TelegramTonkeeper
Installed

Tonhub



Tonkeeper Pro

The wallets below don't support all features of the connected service. You can use your recovery phrase in one of the supported wallets above.

MyTonWallet
InstalledXTONWallet
InstalledTON Wallet
Installed

Bitget Wallet



OKX Mini W...



Binance Wal...



Fintopio



OKX Wallet



TON Connect

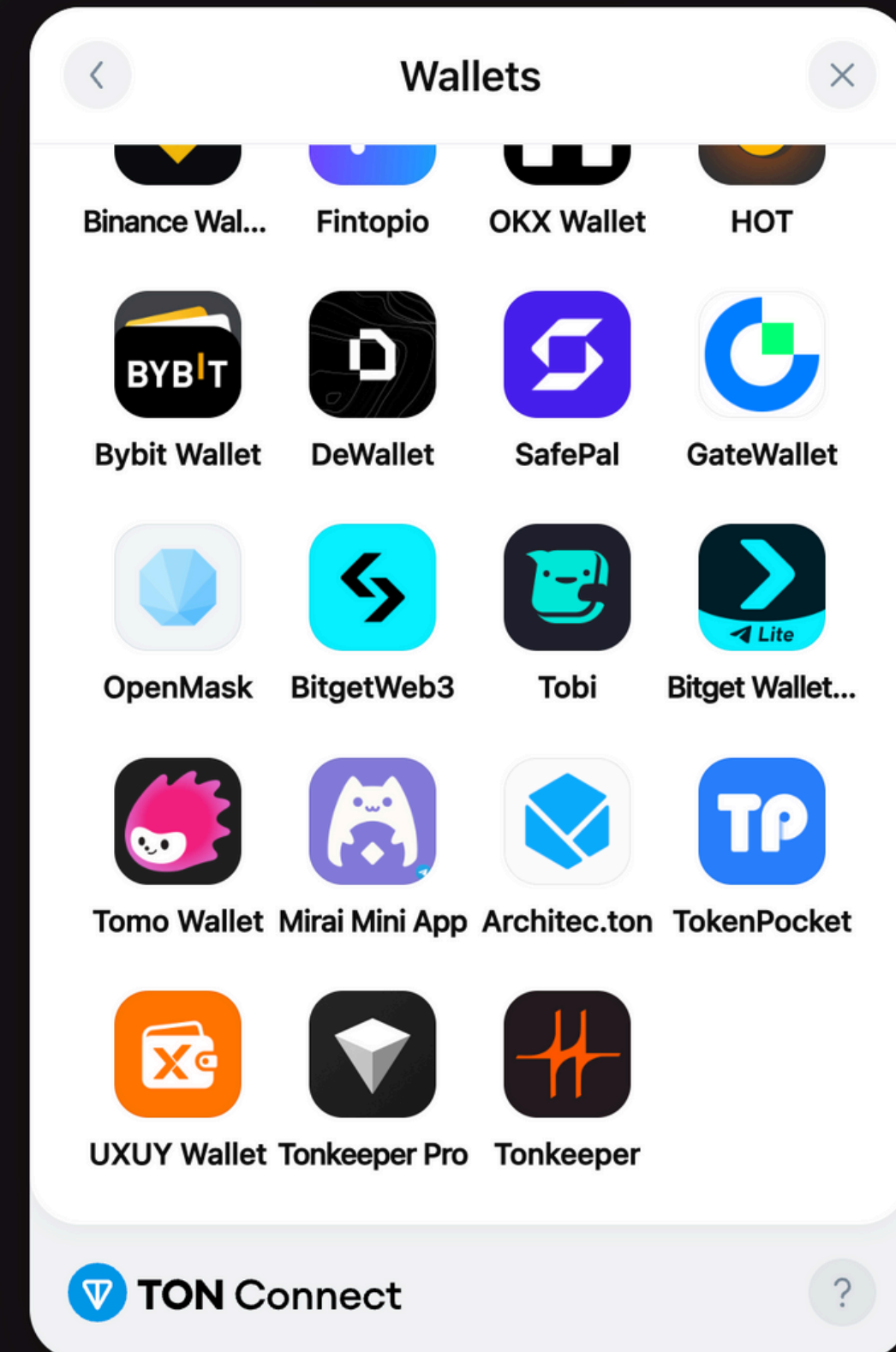




index.js

```
const tonConnectUI = new TonConnectUI({
  manifestUrl: '<URL>',
  buttonRootId: '<ID>',
  walletsListConfiguration: {
    includeWallets: [
      {
        name: " Tonkeeper ",
        appName: "neploxTonWallet",
        jsBridgeKey: "neploxTonWallet",
        aboutUrl: "https://neplox.security",
        universalLink: "https://t.me/neploxaudit?attach=wallet",
        bridgeUrl: "https://neplox.security/bridge",
        imageUrl: "https://neplox.security/icons/neplox.svg",
        platforms: ["android", "ios", "linux", "windows", "macos"],
      }
    ]
  }
})
```

Connect Wallet





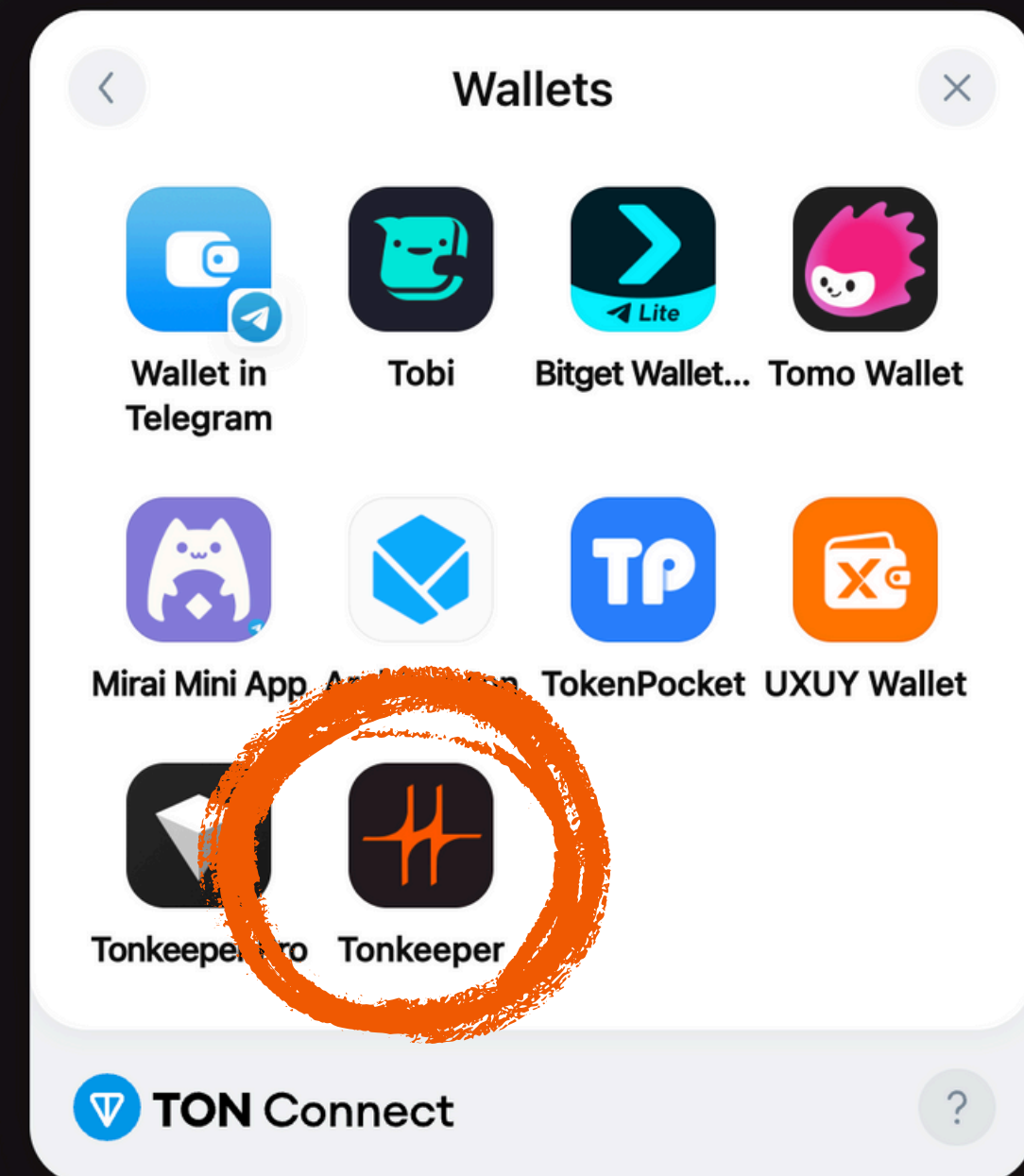
index.js

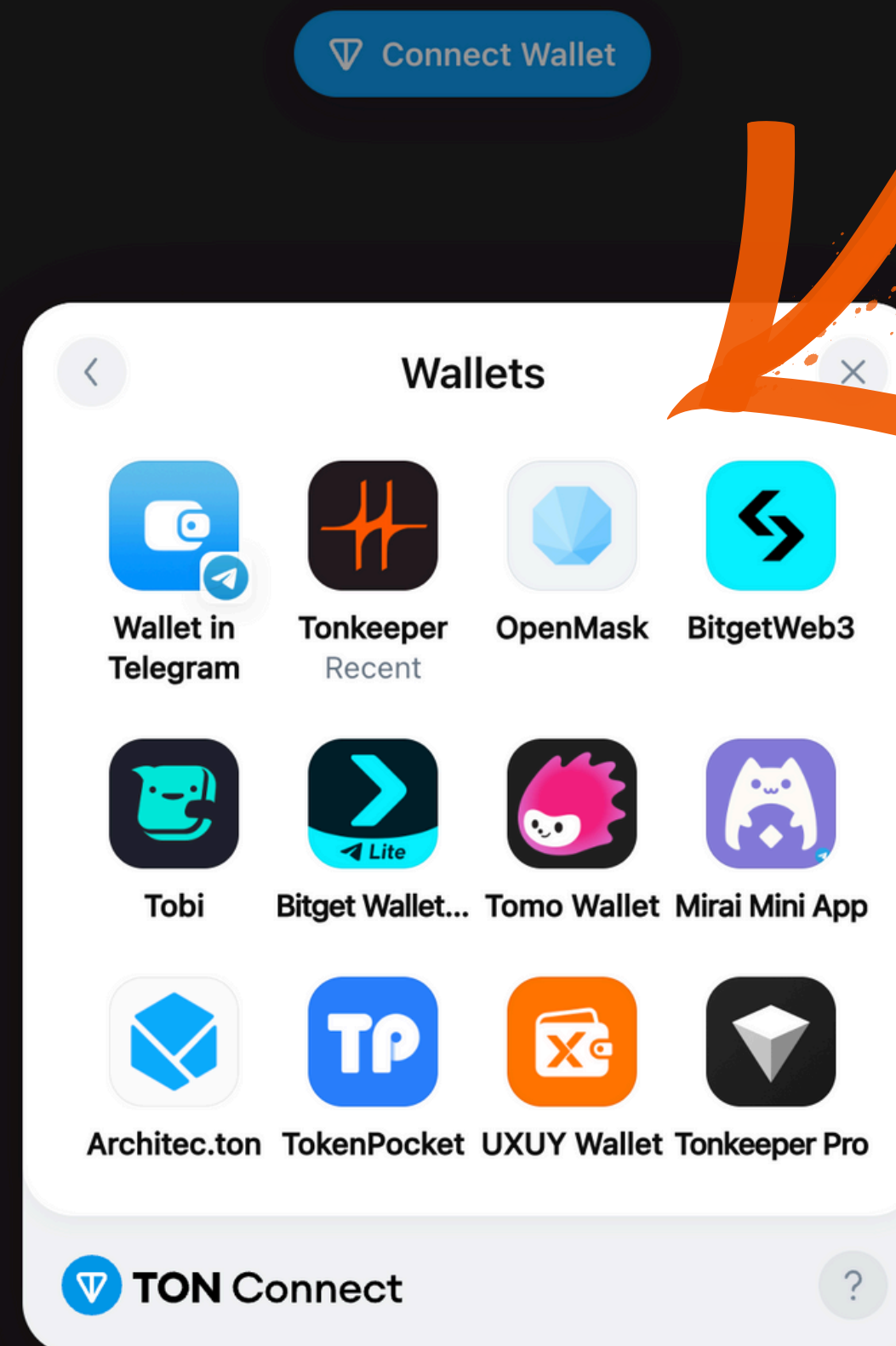
```
const tonConnectUI = new TonConnectUI({
  manifestUrl: '<URL>',
  buttonRootId: '<ID>',
  walletsListConfiguration: {
    includeWallets: [
      {
        name: " Tonkeeper ",
        appName: "neploxTonWallet",
        jsBridgeKey: "neploxTonWallet",
        aboutUrl: "https://neplox.security",
        universalLink: "https://t.me/neploxaudit?attach=wallet",
        bridgeUrl: "https://neplox.security/bridge",
        imageUrl: "https://neplox.security/icons/neplox.svg",
        platforms: ["android", "ios", "linux", "windows", "macos"],
      }
    ]
  }
})
```

index.css

```
li:has(button[data-tc-wallet-item="true"]):nth-of-type(n+3):nth-of-type(-n+17) {
  display: none;
}
```

Connect Wallet





```
index.js
```

```
window.localStorage.setItem('ton-connect-ui_preferred-wallet', 'neploxTonWallet');
```




Initialize the Orbs RPC endpoint for TON

Initialize TON client



<https://api.coinlore.net/...>



Check the price of TON in USD and write it down

Initialize Telegram Bot



Listen for requests



[https://MALICIOUS\[.\]client](https://MALICIOUS[.]client)



CORS + SSL + IP check + ...

scanAccountAssets

getGetblockAPIKey

createBOCJettons

createTransactionPayload



<https://tonapi.io/...>



Get user's TON & Jetton balance

notifyScanDone

notifyTransactionTONStarted

notifyTransactionTONDeclined

notifyTransactionTONDone

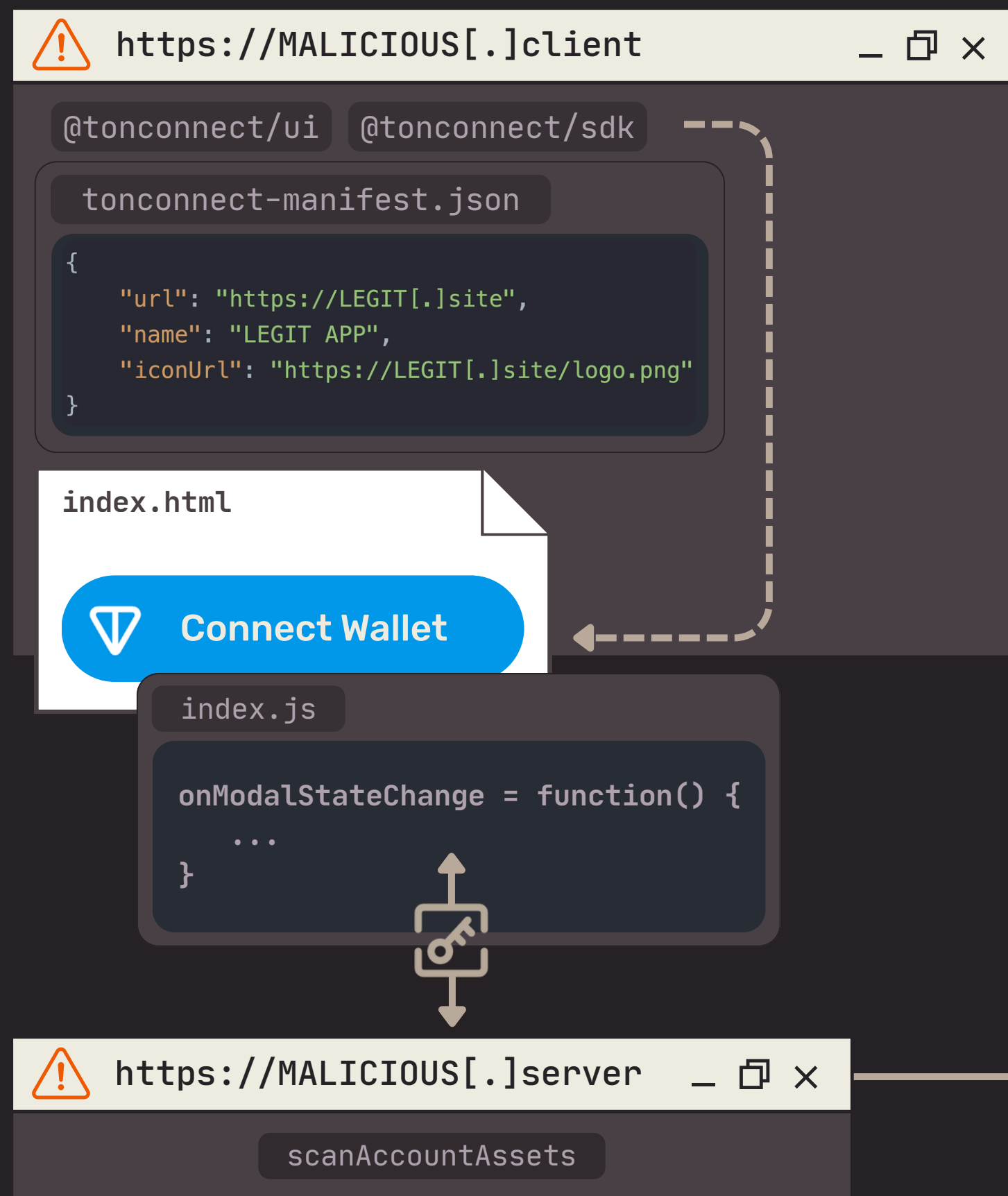
notifyTransactionJettonStarted

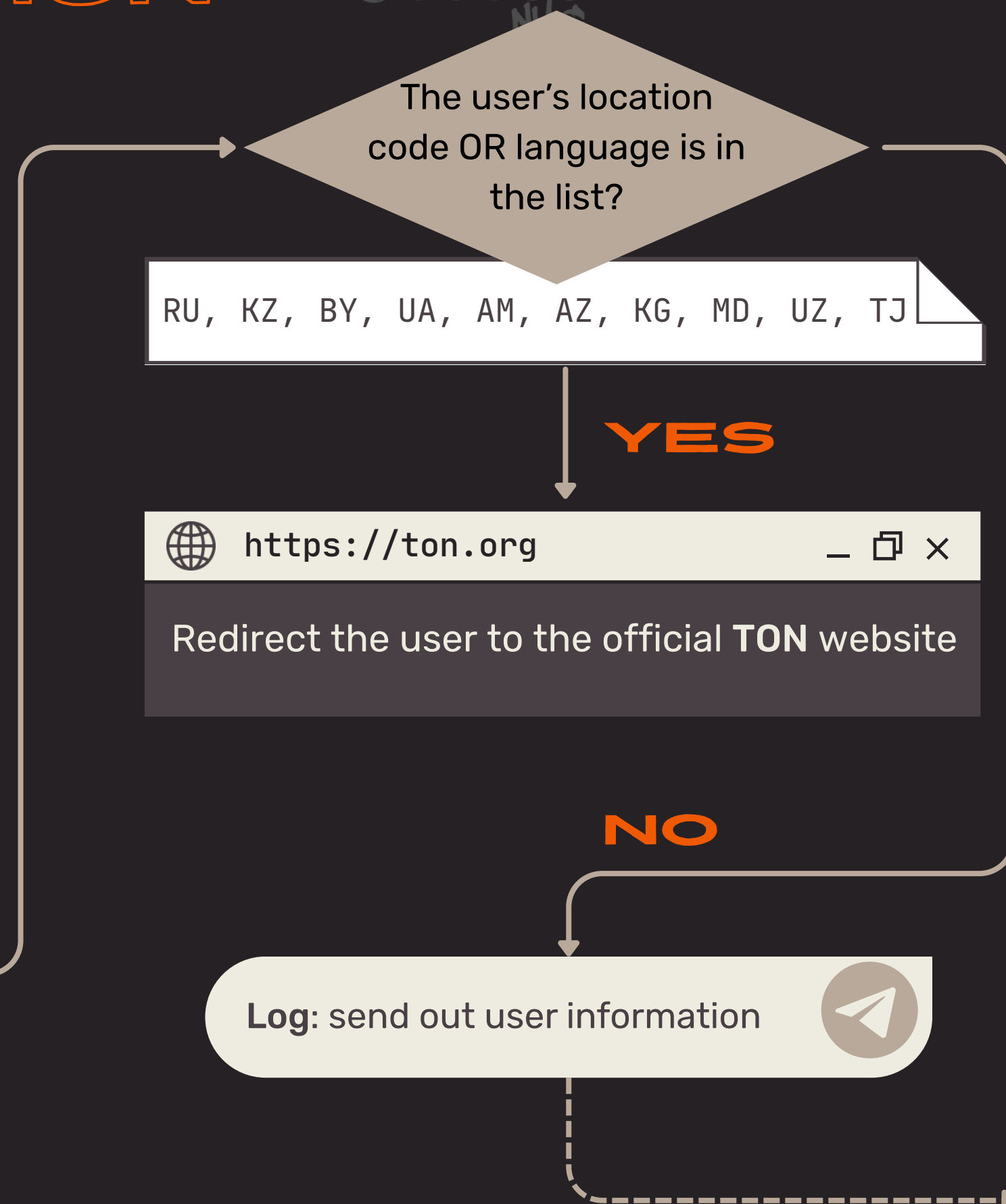
notifyTransactionJettonDeclined

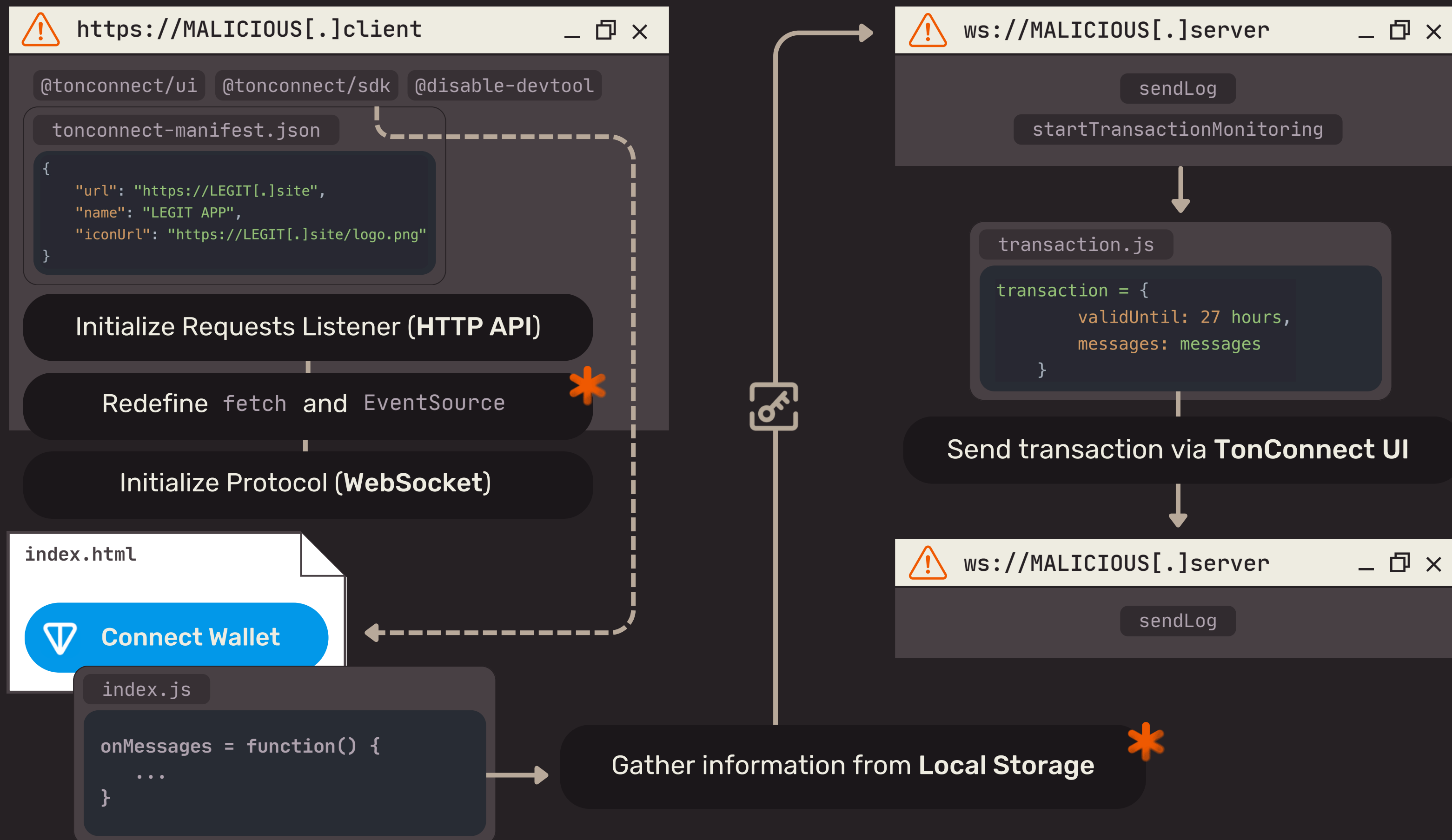
notifyTransactionJettonDone

Log: scan / transaction status











Validate API key

Forge Host, Origin, Referer headers



Proxy requests to the bridge

GET

/bridge/:wallet

- pub
- sec
- wallet



 `https://{bridgeURL}/events` —  
`?client_id={pub}&...`

POST

/bridge/:wallet/message

- client_id
- topic
- ttl
- to
- wallet



 `https://{bridgeURL}/message` —  
`?topic={topic}&...`

GET

/bridge/:wallet/sendTransaction

- pub
- sec
- walletPublicKey
- address
- chunk
- wallet

```
transaction = {  
  validUntil: 27 hours,  
  messages: messages  
}
```



 `https://{bridgeURL}/message` —  
`?topic=sendTransaction&...`

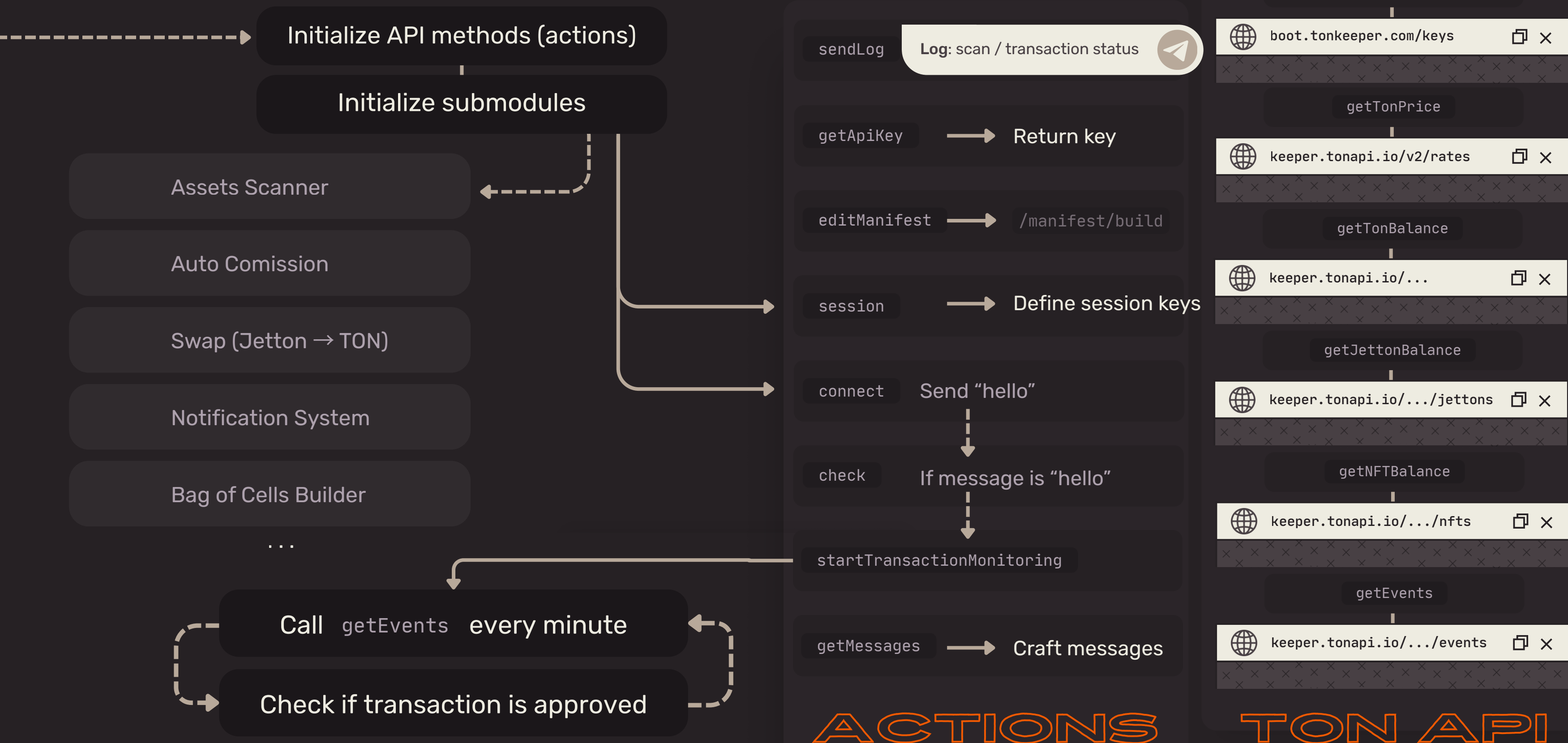
GET

/manifest/build

- name
- url
- icon



Edit `tonconnect-manifest.json`



THANK
YOU

 <https://neplox.security/blog> _ □ ×



Article: "Down the Drain"

