EthCC [4]

Unlimited ERC20 Allowances Considered Harmful

By Rosco Kalis

About Me

ANYHEDGE

truffle-assertions

build passing | coverage 86% | npm v0.9.2 | downloads 17k/month | license MIT

REVOKE

truffle-plugin-verify

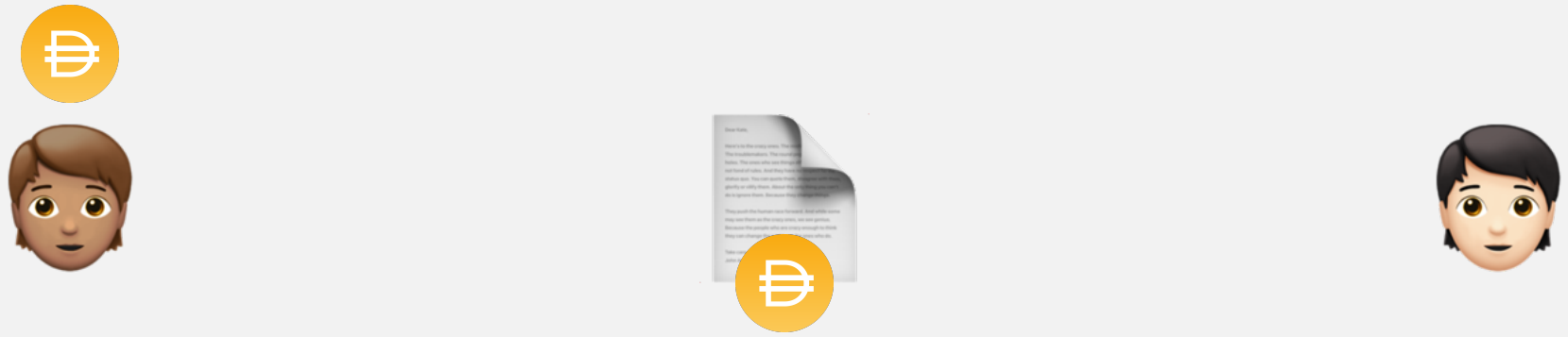
npm v0.5.8 | downloads 10k/month | license MIT

cashscript

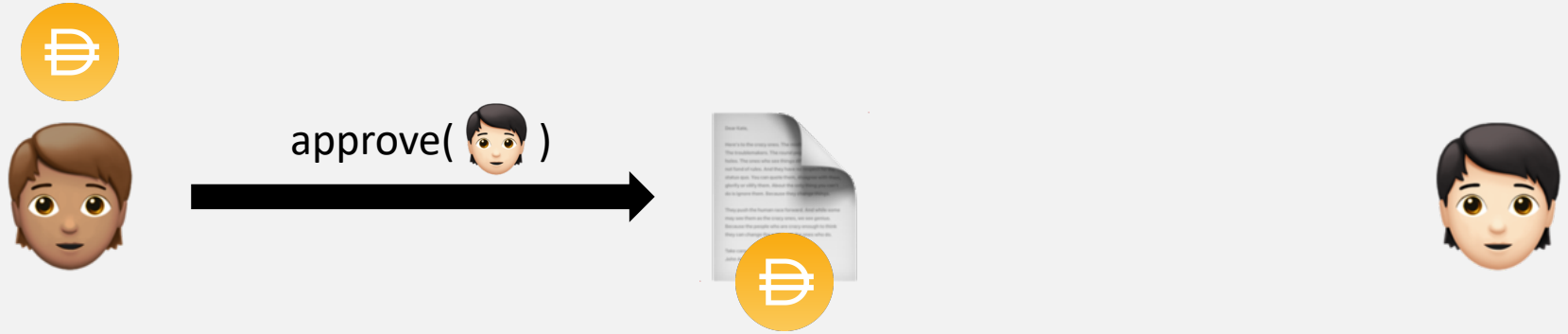
Contents

- What are ERC20 allowances?
- Why are *unlimited* ERC20 allowances harmful?
- Real world case studies
- What can we do to mitigate the risks?

What are ERC20 allowances

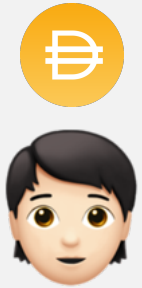


What are ERC20 allowances



What are ERC20 allowances

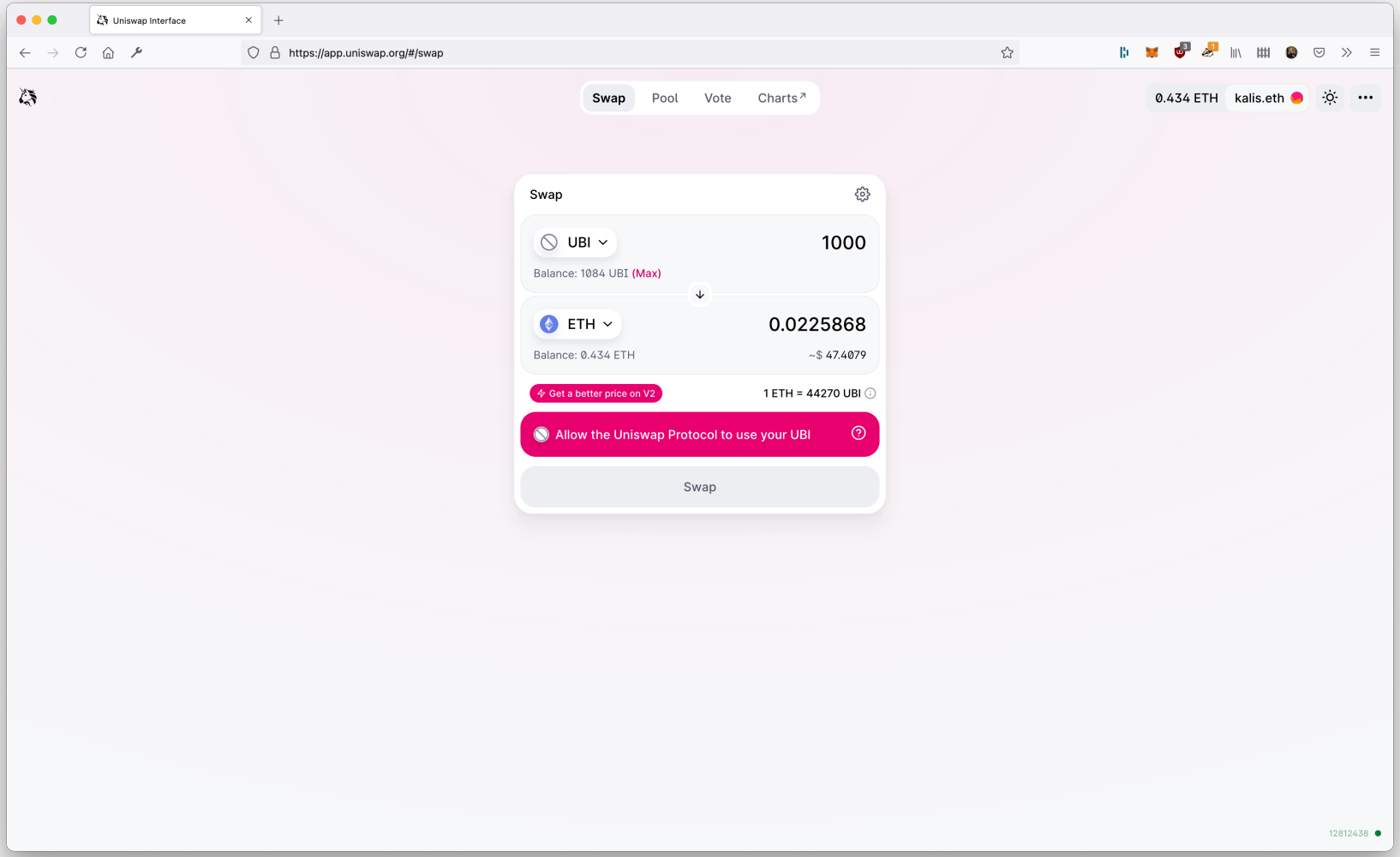
What are ERC20 allowances



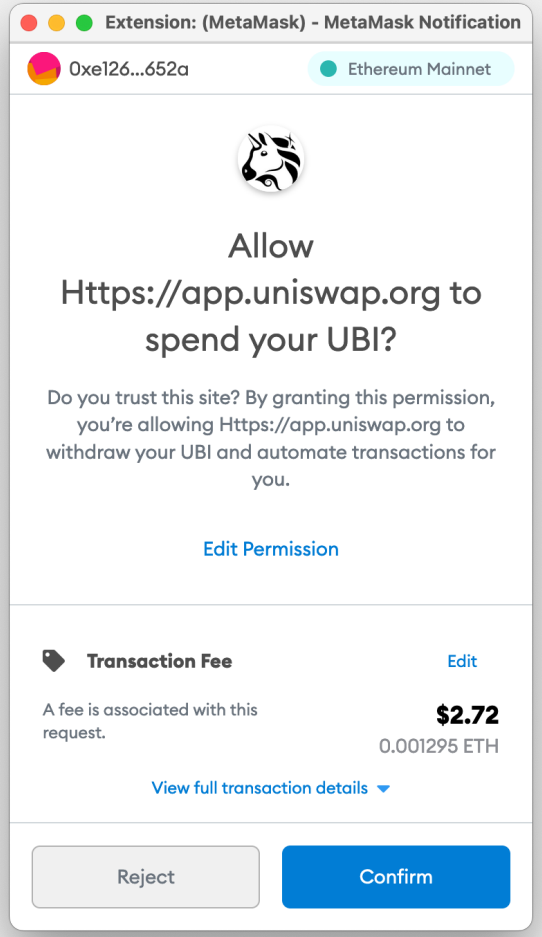
What are ERC20 allowances

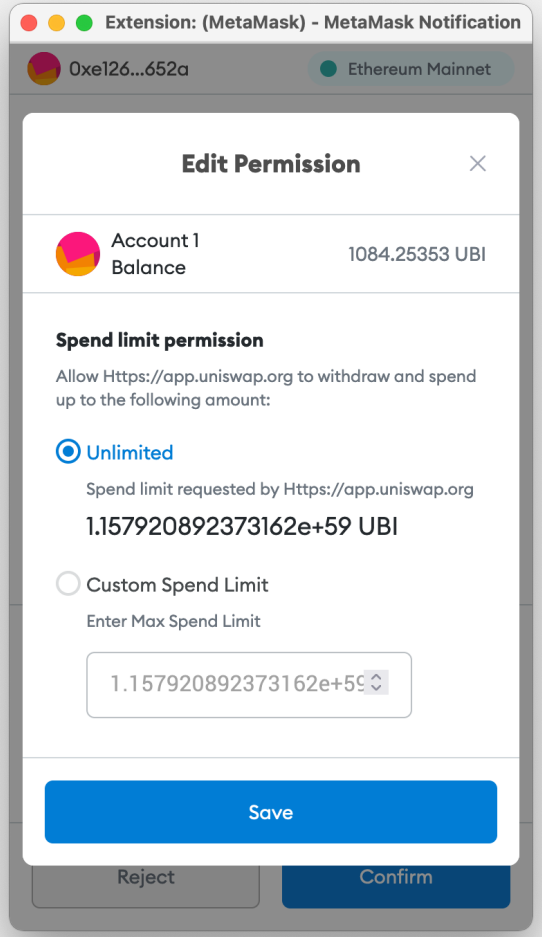
What are ERC20 allowances

What are ERC20 allowances

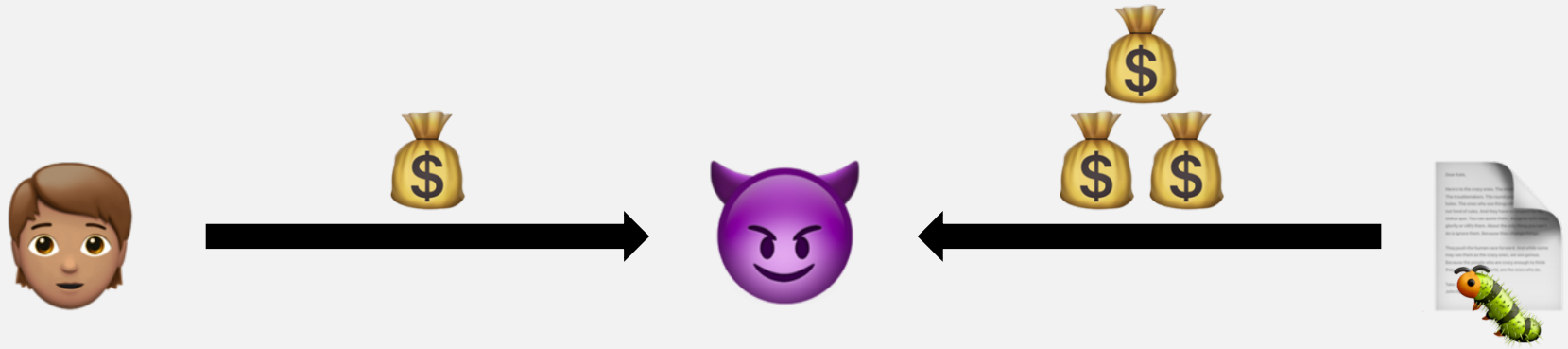


What are ERC20 allowances





Unlimited allowances



2020 Bancor Hack

Bancor Network Hack 2020

1inch Network Follow

Jun 18, 2020 · 3 min read

A critical bug in three recently deployed versions of the Bancor Network smart contract has led to a loss of user funds.

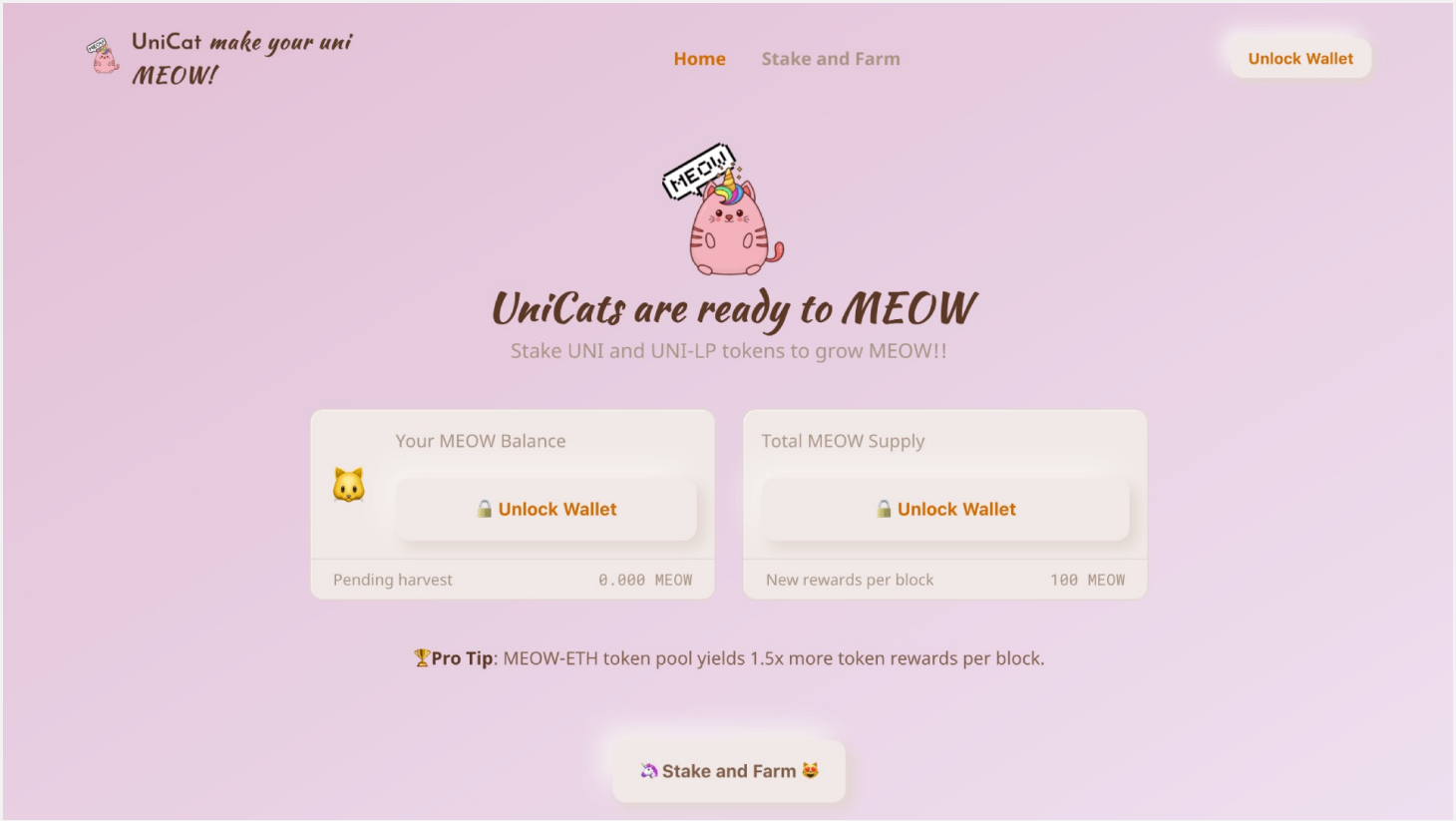
2021 Furucombo Hack

ANDREW THURMAN FEB 27, 2021

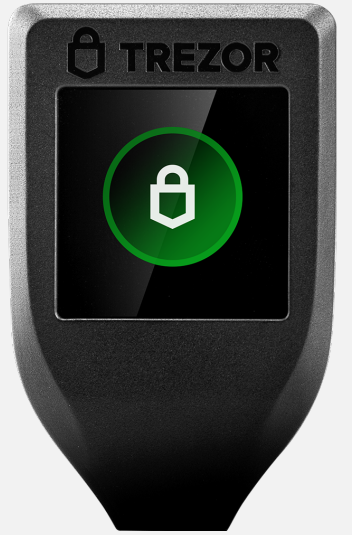
Transaction batching protocol Furucombo suffers $14 million “evil contract” hack

The latest attack relied on user permissions granted to the protocol

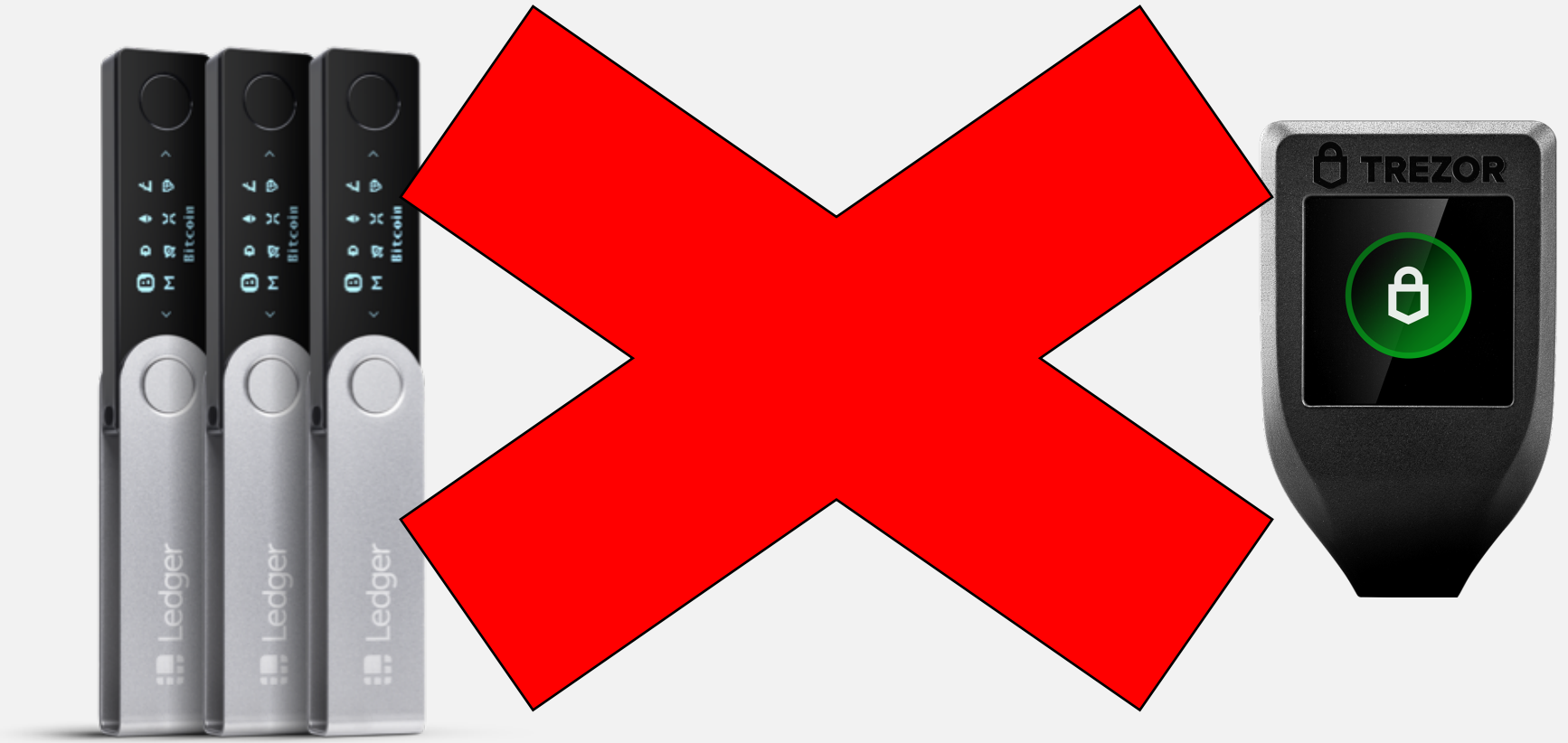
UniCats


UniCat make your uni MEOW!
Home
Stake and Farm
Unlock Wallet
MEOW!
UniCats are ready to MEOW
Stake UNI and UNI-LP tokens to grow MEOW!!
Your MEOW Balance
Unlock Wallet
Pending harvest
0.000 MEOW
Total MEOW Supply
Unlock Wallet
New rewards per block
100 MEOW
Pro Tip: MEOW-ETH token pool yields 1.5x more token rewards per block.
Stake and Farm

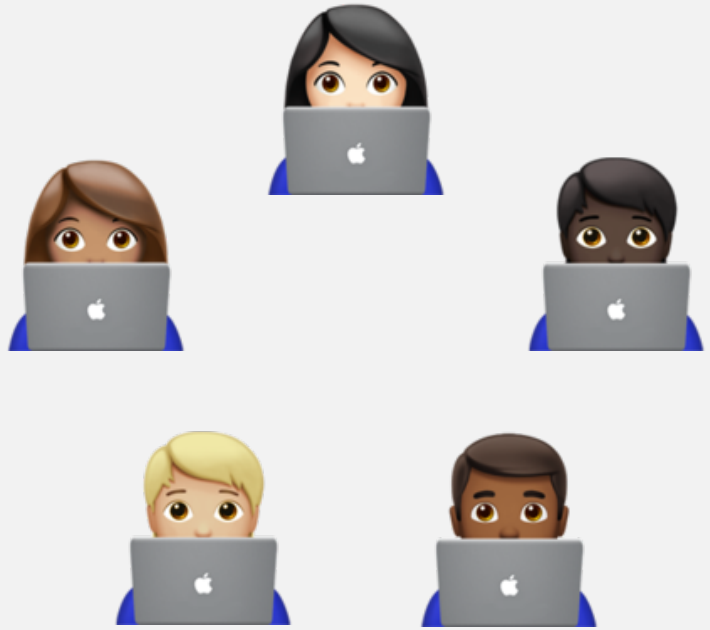
Hardware Wallets?



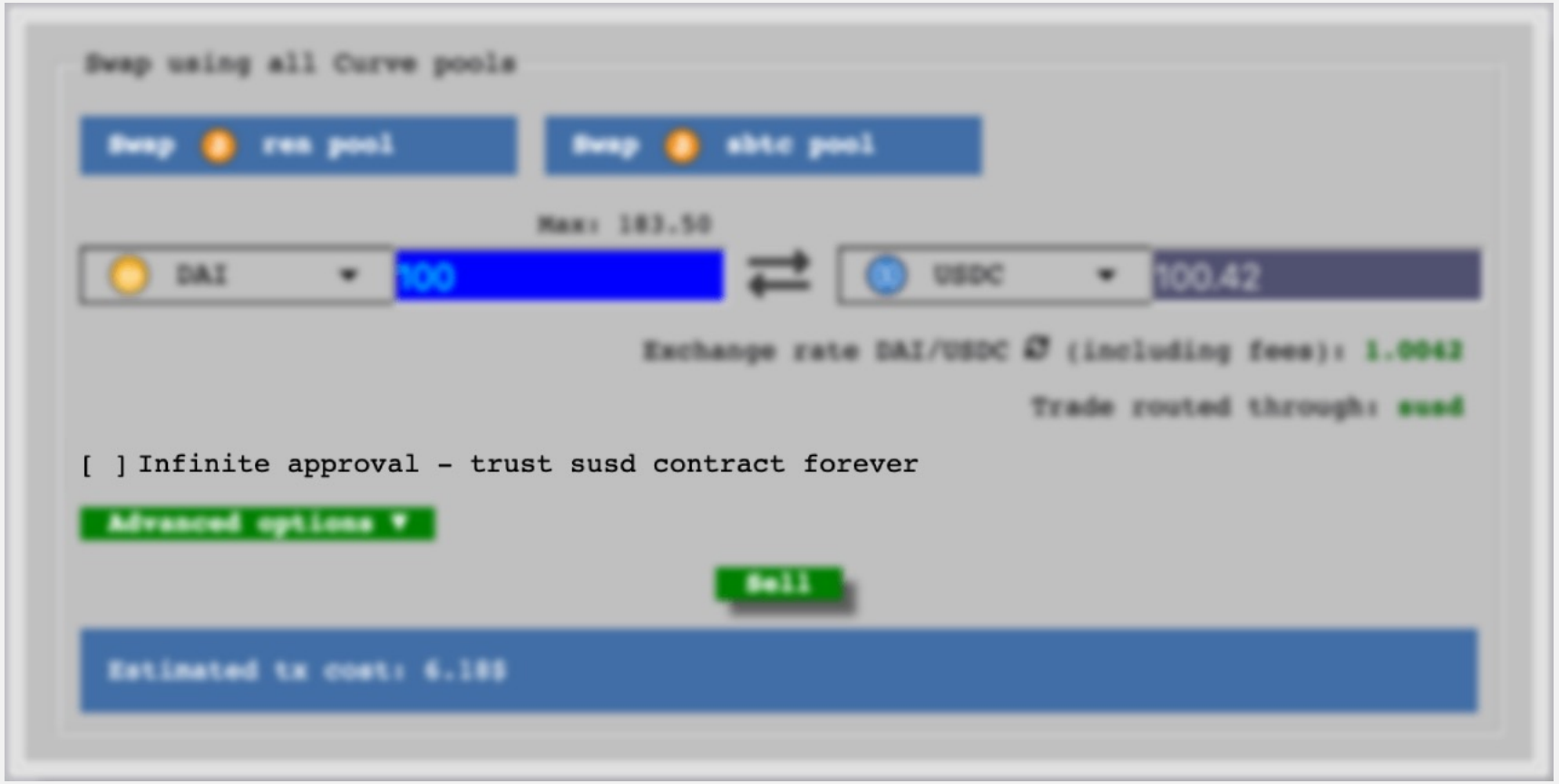
Hardware Wallets?



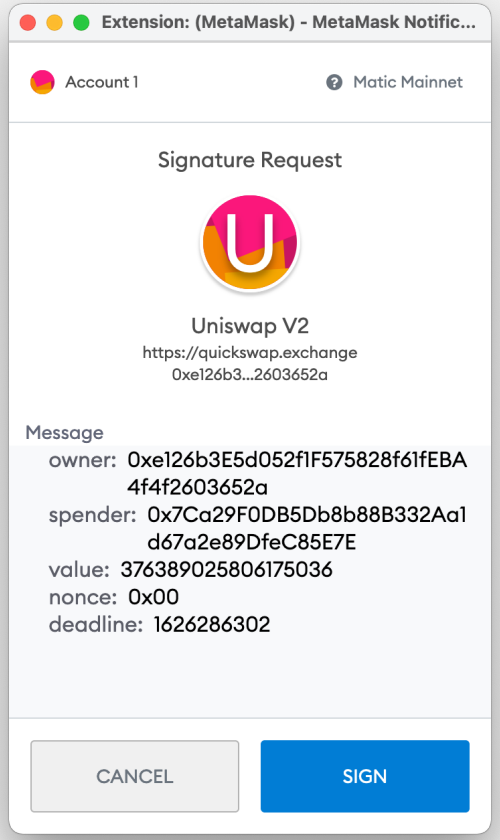
Solutions: developer side



Give users options



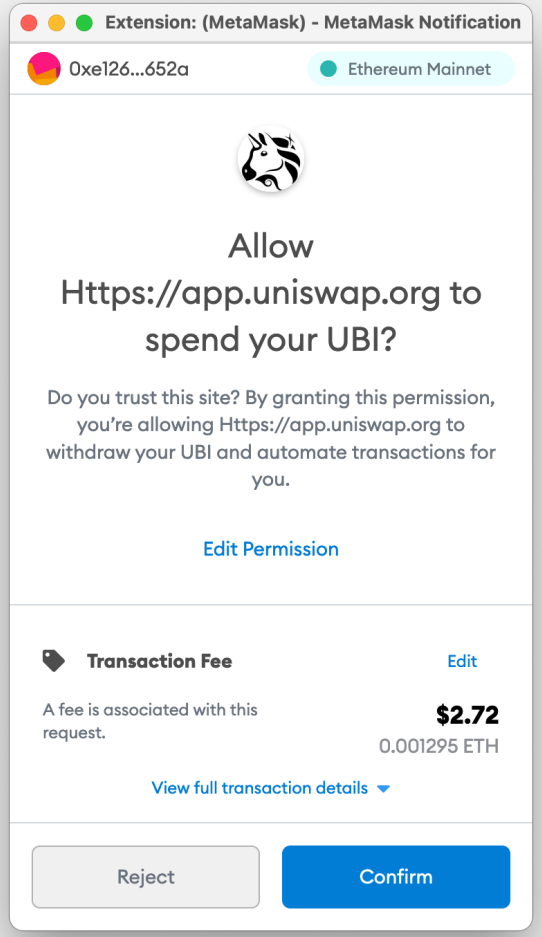
EIP2612: Permit

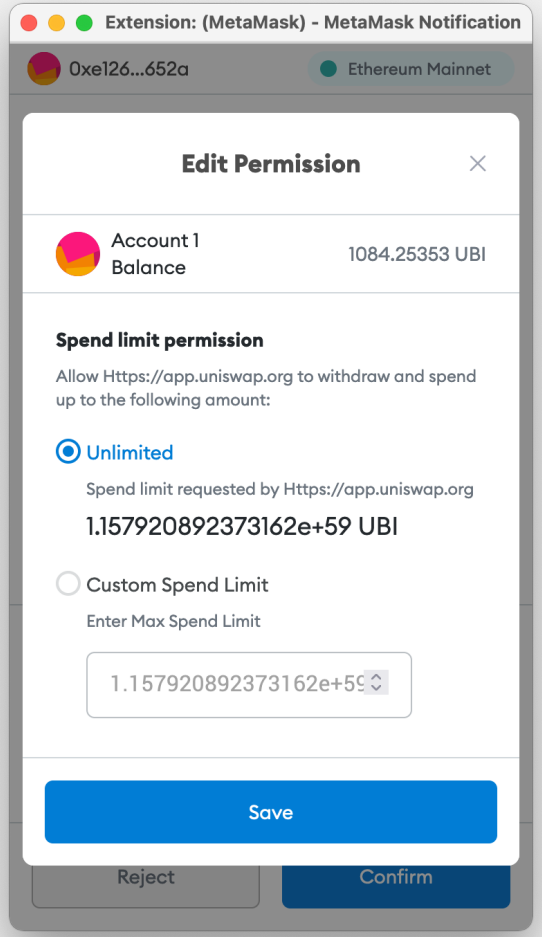


Solutions: user side

Limited vs unlimited allowances

Set a custom limit





Revoke allowances

REVOKE

Donate kalis.eth

kalis.eth

Filter out unregistered tokens ? ☑
Filter out zero balances ☑

ALCX: 0.175
No allowances

AMB: 0.100
No allowances

BADGER: 0.133
Unlimited allowance to Badger Revoke 0 Update

DAI: 843.957
Unlimited allowance to Uniswap Revoke 0 Update
Unlimited allowance to 0xc21D353FF4ee73C572425697f4F5aaD2109fe35b Revoke 0 Update
Unlimited allowance to 0x40ec5B33f54e0E8A33A975908C5BA1c14e5BbbDf Revoke 0 Update
Unlimited allowance to Uniswap Revoke 0 Update
Unlimited allowance to DeversiFi Revoke 0 Update
999999939.990 allowance to Aave Revoke 0 Update
250.000 allowance to xDAI Bridge Revoke 0 Update
60.000 allowance to Gitcoin Revoke 0 Update
10.000 allowance to vitalik.eth Revoke 0 Update
10.000 allowance to Sablier Revoke 0 Update
1.000 allowance to Kyber Revoke 0 Update

RAI: 446.415
Unlimited allowance to Uniswap Revoke 0 Update
Unlimited allowance to 0x7D77191e626F91b3B1985CD6B27CF5498A3c5cdc Revoke 0 Update

UBI: 1106.515
Unlimited allowance to Uniswap Revoke 0 Update

USDC: 1001.809
Unlimited allowance to Compound Revoke 0 Update
Unlimited allowance to 0x3E66B66Fd1d0b02fDa6C811Da9E0547970DB2f21 Revoke 0 Update
Unlimited allowance to 0x Revoke 0 Update
Unlimited allowance to Aave Revoke 0 Update
Unlimited allowance to dYdX Revoke 0 Update
24.000 allowance to Gitcoin Revoke 0 Update

Further reading

- https://kalis.me/unlimited-erc20-allowances/
- https://www.youtube.com/watch?v=y9A8wHhNjJA
- https://revoke.cash/
- https://eips.ethereum.org/EIPS/eip-20
- https://eips.ethereum.org/EIPS/eip-2612