



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**



**cash**script



# Contents

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

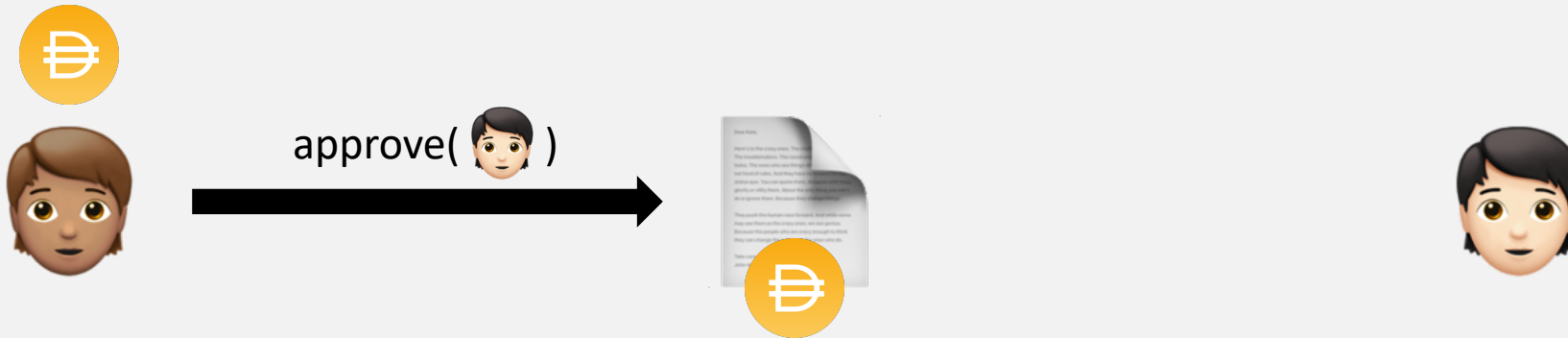


# What are ERC20 allowances



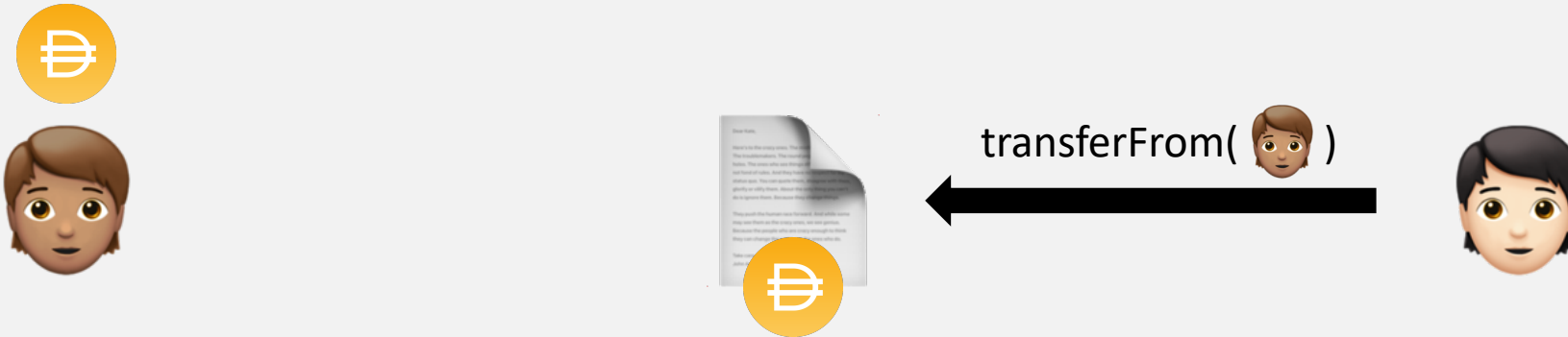


# What are ERC20 allowances



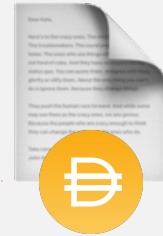


# What are ERC20 allowances





# What are ERC20 allowances





# What are ERC20 allowances







# What are ERC20 allowances





# What are ERC20 allowances


A screenshot of the Uniswap web interface in a browser window. The browser tab is titled "Uniswap Interface" and the address bar shows "https://app.uniswap.org/#/swap". The interface has a navigation bar with "Swap", "Pool", "Vote", and "Charts" tabs. The user's account information shows "0.434 ETH" and "kalis.eth". The main swap area is titled "Swap" and shows a transaction where 1000 UBI is being swapped for 0.0225868 ETH. The UBI input field has a balance of 1084 UBI (Max). The ETH output field has a balance of 0.434 ETH and a value of --\$ 47.4079. A pink button with a lightning bolt icon says "Get a better price on V2" and shows a rate of "1 ETH = 44270 UBI". Below this is a pink button that says "Allow the Uniswap Protocol to use your UBI" with a circular arrow icon. At the bottom of the swap area is a grey "Swap" button. The bottom right corner of the interface shows the number "12812438".



# What are ERC20 allowances

Extension: (MetaMask) - MetaMask Notification

Oxe126...652a Ethereum Mainnet




### Allow

Https://app.uniswap.org to spend your UBI?

Do you trust this site? By granting this permission, you're allowing Https://app.uniswap.org to withdraw your UBI and automate transactions for you.

[Edit Permission](#)

---

 **Transaction Fee** [Edit](#)

A fee is associated with this request. **\$2.72**  
0.001295 ETH


[View full transaction details](#)

[Reject](#) [Confirm](#)

Extension: (MetaMask) - MetaMask Notification

Oxe126...652a Ethereum Mainnet

### Edit Permission

 Account 1 Balance 1084.25353 UBI

#### Spend limit permission

Allow Https://app.uniswap.org to withdraw and spend up to the following amount:

**Unlimited**  
Spend limit requested by Https://app.uniswap.org  
**1.157920892373162e+59 UBI**

Custom Spend Limit  
Enter Max Spend Limit

[Save](#)

[Reject](#) [Confirm](#)



# 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

34540 Total views

40 Total shares

Listen to article



2:45







# UniCats


UniCat *make your uni MEOW!*

[Home](#) [Stake and Farm](#) [Unlock Wallet](#)



*UniCats are ready to MEOW*  
Stake UNI and UNI-LP tokens to grow MEOW!!

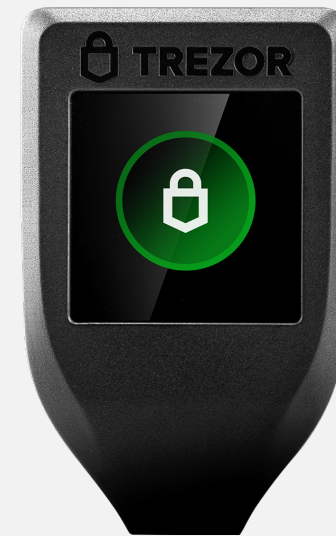
Your MEOW Balance		Total MEOW Supply	
	<a href="#">Unlock Wallet</a>	<a href="#">Unlock Wallet</a>	
Pending harvest	0.000 MEOW	New rewards per block	100 MEOW

 **Pro Tip:** MEOW-ETH token pool yields 1.5x more token rewards per block.

[Stake and Farm 🐱](#)



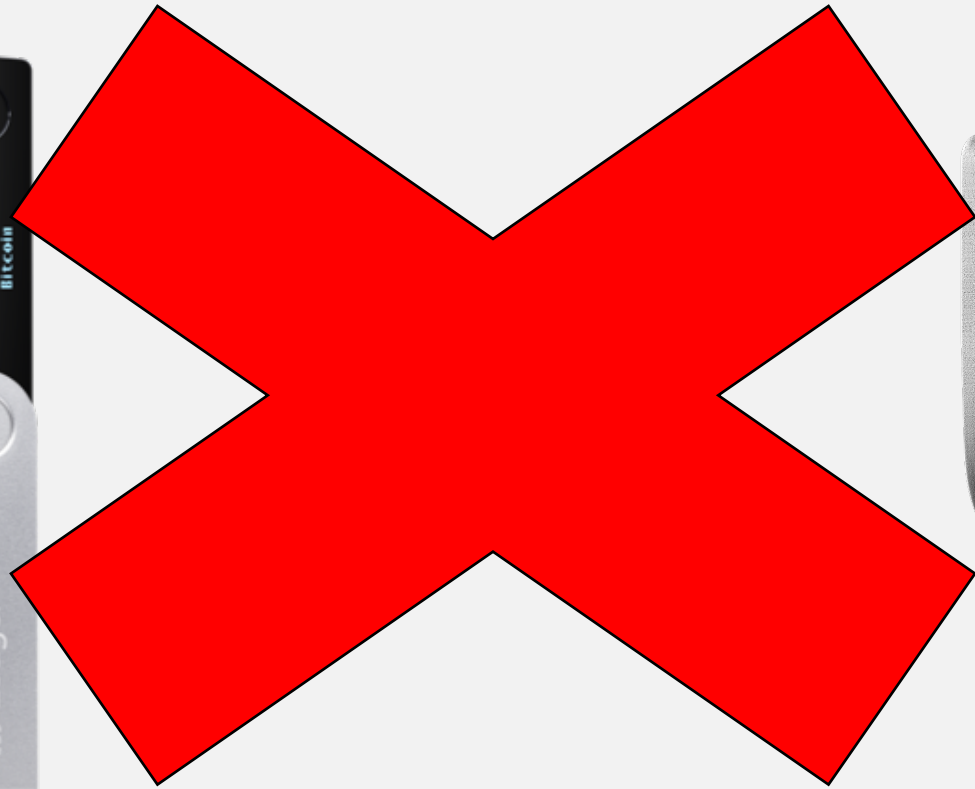
# Hardware Wallets?







# Hardware Wallets?





# Solutions: developer side





# Give users options

Swap using all Curve pools

Swap ren pool      Swap sbtc pool

Max: 183.50

DAI    100    ⇄    USDC    100.42

Exchange rate DAI/USDC (including fees): 1.0042

Trade routed through: **sud**

Infinite approval - trust sud contract forever

**Advanced options** ▼

**Sell**

Estimated tx cost: 6.189




# EIP2612: Permit

Extension: (MetaMask) - MetaMask Notific...

Account 1 Matic Mainnet

Signature Request



Uniswap V2  
https://quickswap.exchange  
0xe126b3...2603652a

Message

owner: 0xe126b3E5d052f1F575828f61fEBA4f4f2603652a  
spender: 0x7Ca29F0DB5Db8b88B332Aa1d67a2e89DfeC85E7E  
value: 376389025806175036  
nonce: 0x00  
deadline: 1626286302

CANCEL SIGN

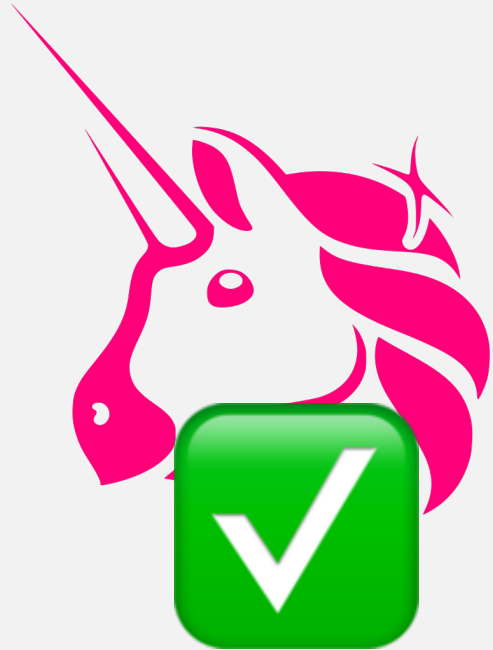


# Solutions: user side





# Limited vs unlimited allowances






# Set a custom limit

Extension: (MetaMask) - MetaMask Notification

Oxe126...652a Ethereum Mainnet




**Allow**  
Https://app.uniswap.org to  
spend your UBI?

Do you trust this site? By granting this permission,  
you're allowing Https://app.uniswap.org to  
withdraw your UBI and automate transactions for  
you.

[Edit Permission](#)

---

 **Transaction Fee** [Edit](#)

A fee is associated with this  
request. **\$2.72**  
0.001295 ETH


[View full transaction details](#)

[Reject](#) [Confirm](#)

Extension: (MetaMask) - MetaMask Notification

Oxe126...652a Ethereum Mainnet

**Edit Permission** [×](#)

 **Account 1** 1084.25353 UBI  
**Balance**

---

**Spend limit permission**

Allow Https://app.uniswap.org to withdraw and spend  
up to the following amount:

**Unlimited**  
Spend limit requested by Https://app.uniswap.org  
**1.157920892373162e+59 UBI**

**Custom Spend Limit**  
Enter Max Spend Limit

[Save](#)

[Reject](#) [Confirm](#)



# Revoke allowances



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](#)
- DAI: 843.957  
Unlimited allowance to [Uniswap](#)     
Unlimited allowance to [0xc21D353FF4ee73C572425697f4F5aad2109fe35b](#)     
Unlimited allowance to [0x40ec5B33f54e0E8A33A975908C5BA1c14e5BbbDf](#)     
Unlimited allowance to [Uniswap](#)     
Unlimited allowance to [DeversiFi](#)     
999999939.990 allowance to [Aave](#)     
250.000 allowance to [xDAI Bridge](#)     
60.000 allowance to [Gitcoin](#)     
10.000 allowance to [vitalik.eth](#)     
10.000 allowance to [Sablier](#)     
1.000 allowance to [Kyber](#)
- RAI: 446.415  
Unlimited allowance to [Uniswap](#)     
Unlimited allowance to [0x7D77191e626F91b3B1985CD6B27CF5498A3c5cdc](#)
- UBI: 1106.515  
Unlimited allowance to [Uniswap](#)
- USDC: 1001.809  
Unlimited allowance to [Compound](#)     
Unlimited allowance to [0x3E66B66Fd1d0b02fDa6C811Da9E0547970DB2f21](#)     
Unlimited allowance to [0x](#)     
Unlimited allowance to [Aave](#)     
Unlimited allowance to [dYdX](#)     
24.000 allowance to [Gitcoin](#)





# 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>