FIOD
Belastingdienst

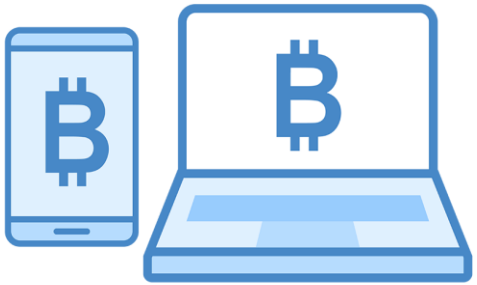
FACT

Financial Advanced Cyber Team

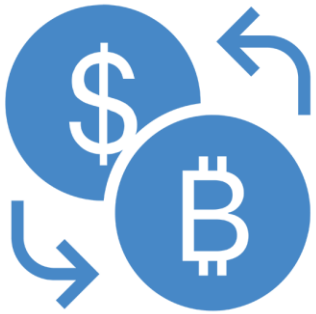
Seizing Cryptocurrencies

April 2025

Wallet Types



Mobile / Desktop wallet



Exchange wallet

Hardware wallet

Paper wallet

Mobile / Desktop wallet

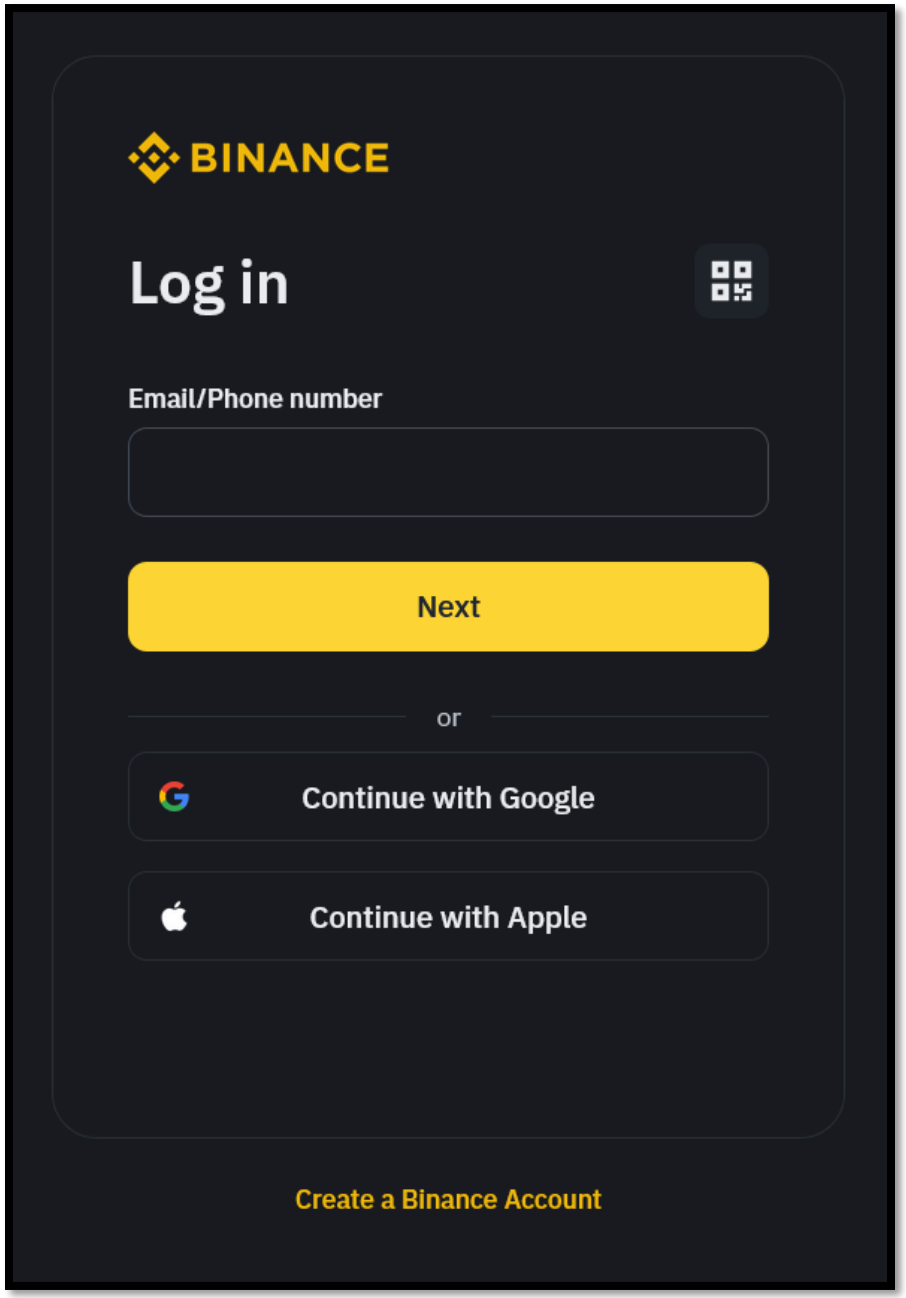
- User convenience in your pocket
- Accessible anytime, anywhere
- Requires internet access only

- Custodial Wallet / Non-Custodial Wallet
- Private key present on device?
- Sometimes combinable with hardware wallet

Exchange wallet

- Wallet at an online exchange
- Private keys managed by exchange
- Whose crypto currency is it anyway?

- Note: often 2FA required for access
- Requirement for information/transfers
- Neat option: crypto currency freeze



Hardware wallet

- Offline storage private key (cold wallet)
- Protection against online attacks
- Four steps with a hardware wallet

1. *The user initiates the cryptocurrency transaction*
2. *Transaction data is verified on the wallet*
3. *User signs the transaction with the private key*
4. *Software sends the transaction to the blockchain*

Paper wallet

- Offline storage for cryptocurrency
- Piece of paper with public/private key
- Easy to generate online yourself
- Example below from bitaddress.org

Bitcoin Address:
1GEyEUXnhuqLCGV4MYUo3QWFG6ZBrrcgDU

Private Key:
KxGJzr1nhaUebbXLSMgxSD9UGcGKVh3tqRWd3GzAnkBhFwzACdLh

solar	galaxy
isl	a
br	se
tor	st
fas	bref
dry	wood

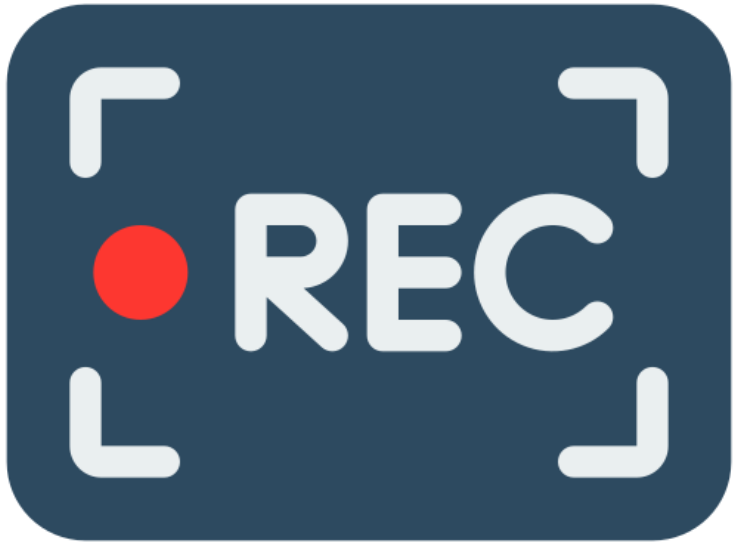
Mnemonic wat?!

- Also known as a seed, seed phrase or recovery phrase.
- Set of words for accessing a user's cryptocurrency.
- It is an important security measure in relation to cryptocurrency.

- It usually consists of a multiple of three (often 12 / 24) words.
- Word list of the BIP39 standard (Bitcoin Improvement Proposal 39).
- The words are used to generate the wallet's private key.

Careful! Co-conspirators that are abroad might have a copy of the mnemonic phrase!

Before we begin….



Confiscating SepoliaETH

- During the search of the suspect's premises, QR codes containing phrases were found.
- It concerns 'SepoliaETH' as a crypto currency to be seized.
- This currency runs on 'testnet' (a blockchain where extensive testing can be done).

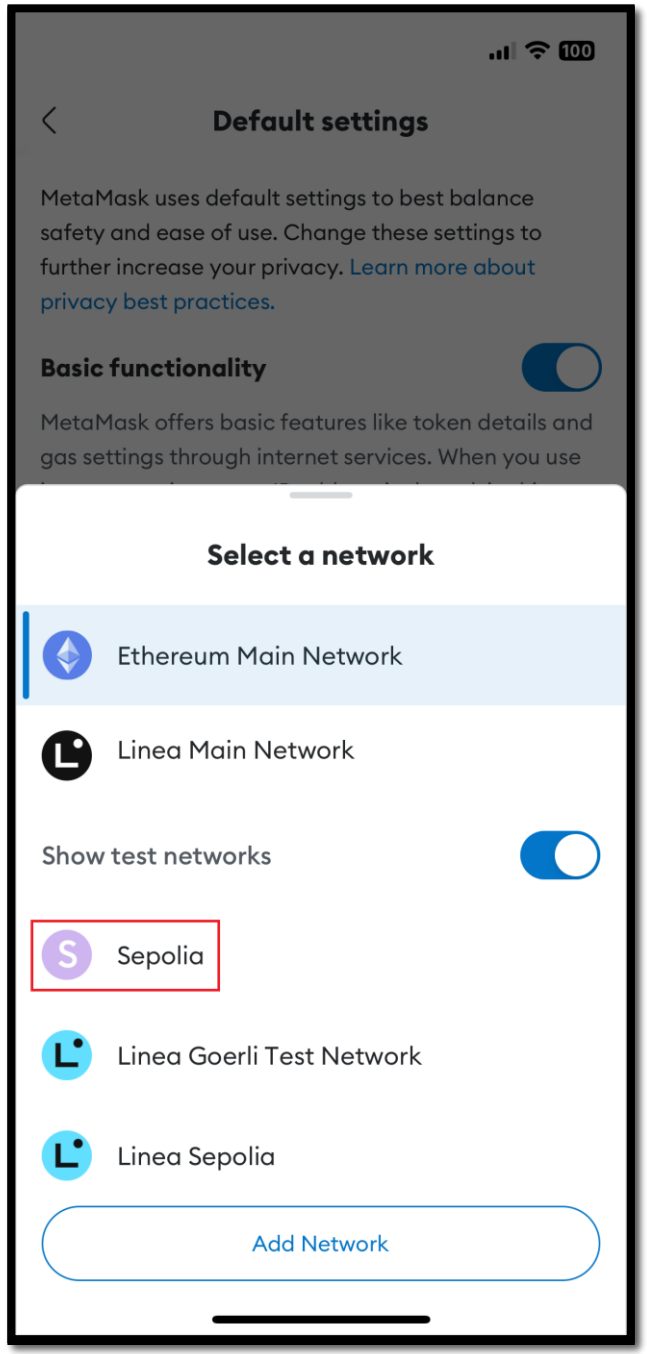
+

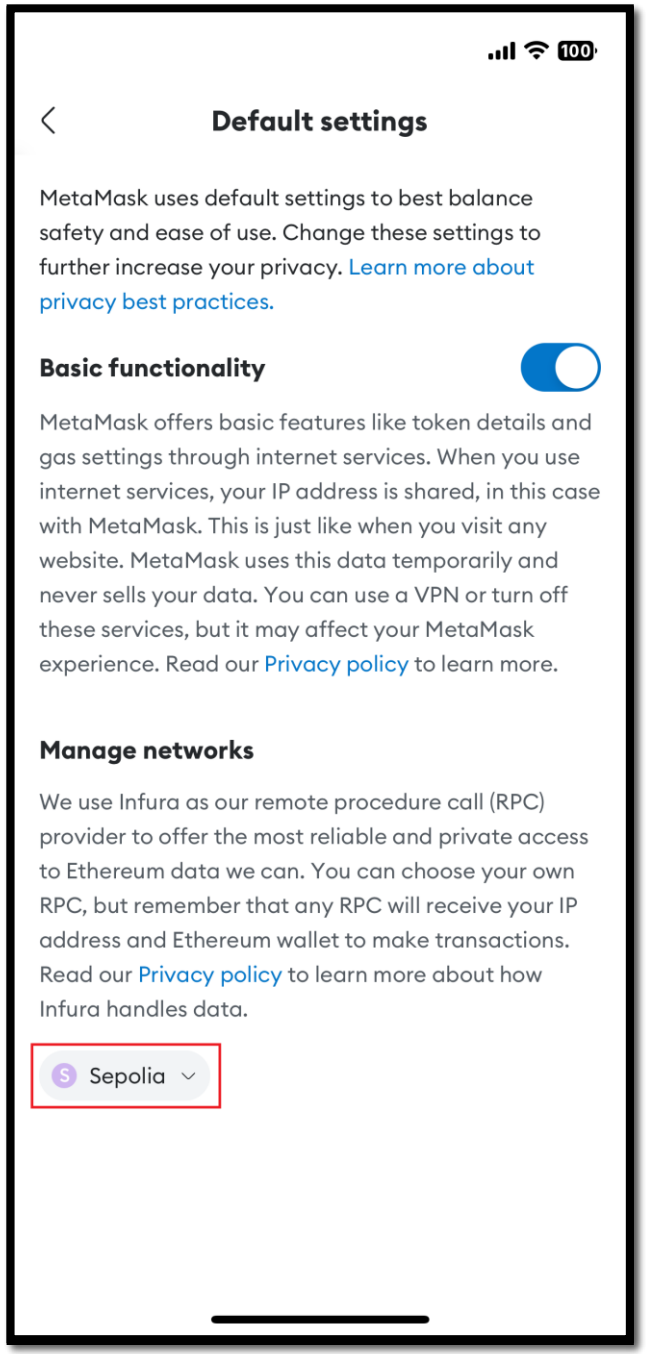
+

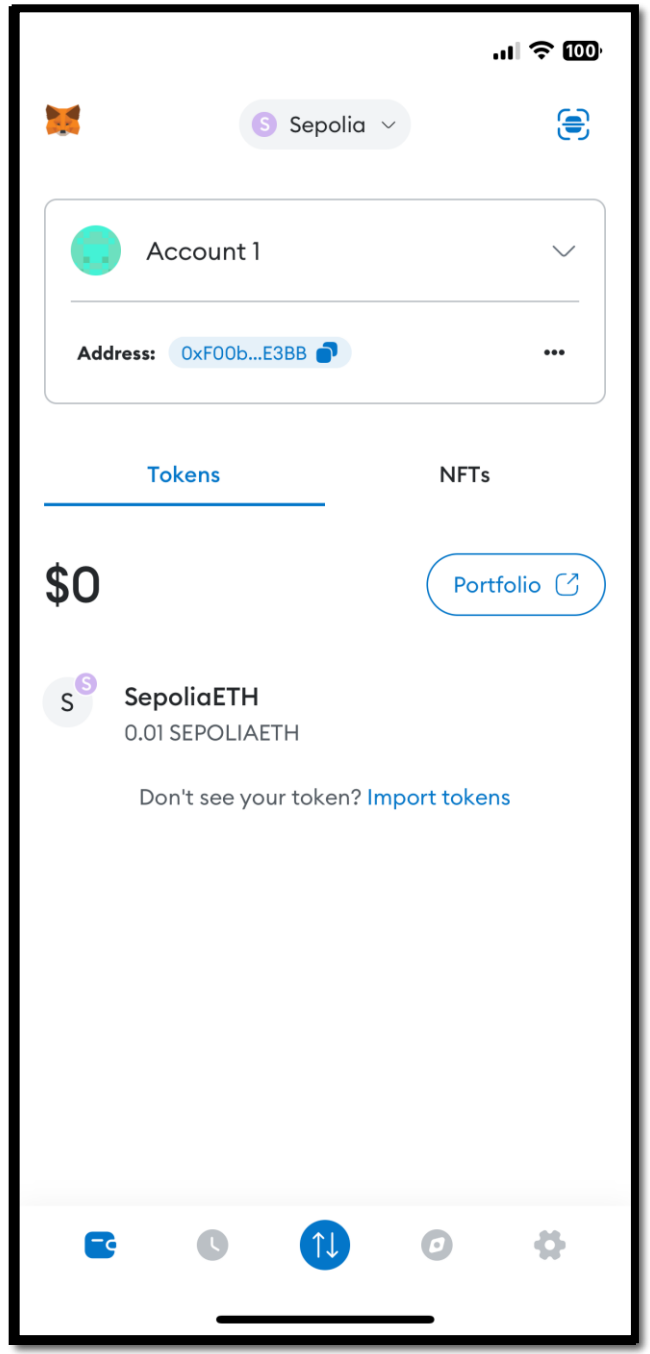
bitonic

Download MetaMask

Confiscate SepoliaETH


Default settings
MetaMask uses default settings to best balance safety and ease of use. Change these settings to further increase your privacy. Learn more about privacy best practices.
Basic functionality
MetaMask offers basic features like token details and gas settings through internet services. When you use
Select a network
Ethereum Main Network
Linea Main Network
Show test networks
Sepolia
Linea Goerli Test Network
Linea Sepolia
Add Network


Default settings
MetaMask uses default settings to best balance safety and ease of use. Change these settings to further increase your privacy. Learn more about privacy best practices.
Basic functionality
MetaMask offers basic features like token details and gas settings through internet services. When you use internet services, your IP address is shared, in this case with MetaMask. This is just like when you visit any website. MetaMask uses this data temporarily and never sells your data. You can use a VPN or turn off these services, but it may affect your MetaMask experience. Read our Privacy policy to learn more.
Manage networks
We use Infura as our remote procedure call (RPC) provider to offer the most reliable and private access to Ethereum data we can. You can choose your own RPC, but remember that any RPC will receive your IP address and Ethereum wallet to make transactions. Read our Privacy policy to learn more about how Infura handles data.
Sepolia


Sepolia
Account 1
Address: 0xF00b...E3BB
Tokens
NFTs
$0
Portfolio
SepoliaETH
0.01 SEPOLIAETH
Don't see your token? Import tokens

Search for a transaction on the Blockchain

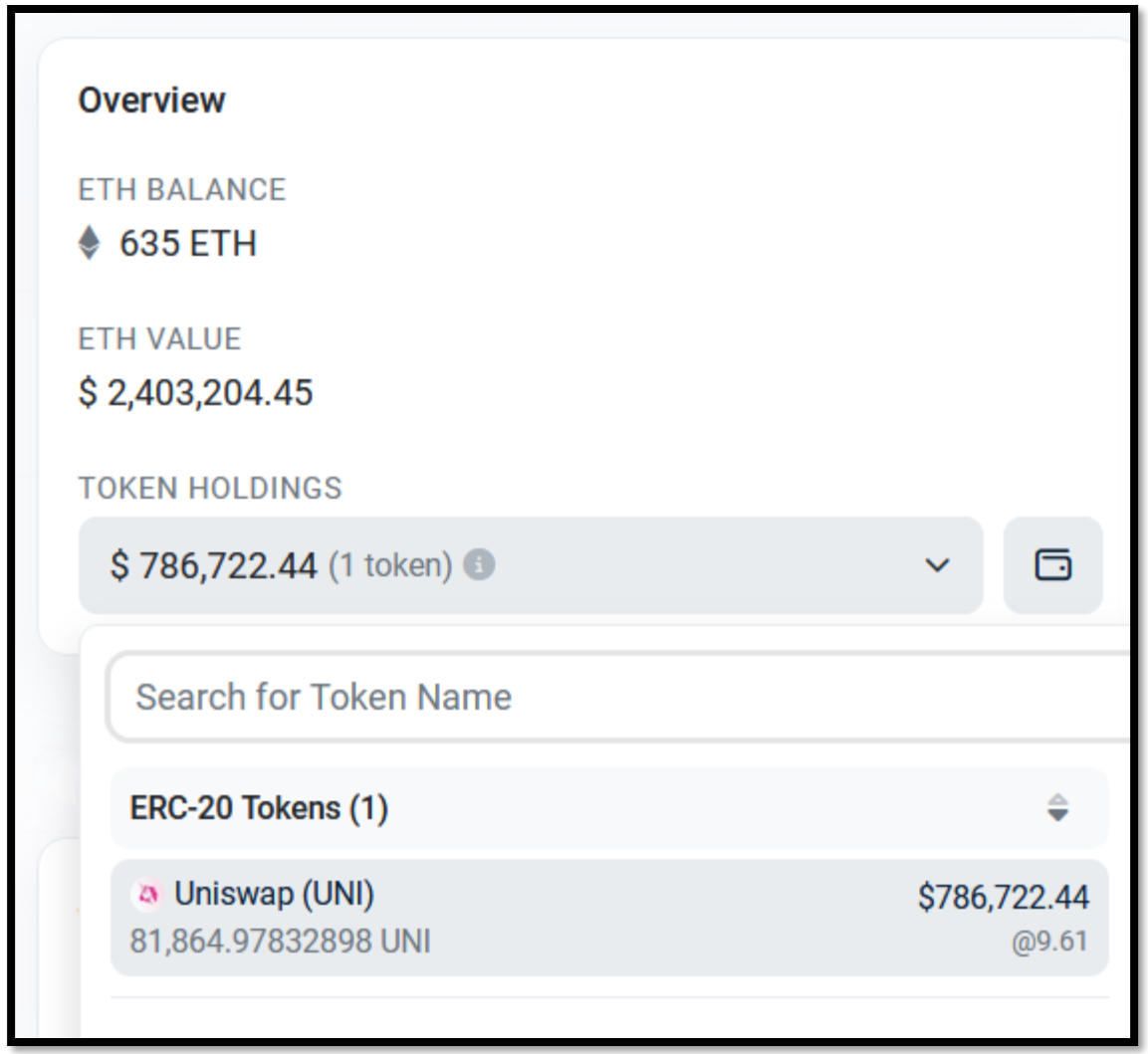
- Transactions of cryptocurrencies can be found on the blockchain.
- A blockchain explorer can be used to find transactions.
- For each currency, you can often find its own online blockchain explorer.

- Bitcoin: https://www.blockchain.com/
- Ethereum: https://etherscan.io/
- Tether (USDT): https://blockchair.com/tether

0x3f7ac2edbd2...	Transfer	7056755	2 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF15c1628...EcdDA54cC	0.01 ETH	0.00012479
0x6a54dff2194...	Transfer	7056754	3 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF14aA9d7...646490840	0.01 ETH	0.0001274
0x397fdc00406...	Transfer	7056753	3 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF13d1F12...B9C50E7de	0.01 ETH	0.00011762
0xf2af671f17c...	Transfer	7056752	3 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF12a9503...E90c60E64	0.01 ETH	0.00010829
0x742b276b51...	Transfer	7056752	3 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF11b9832...7fbF7f156	0.01 ETH	0.00010829
0x51501718b8...	Transfer	7056751	4 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF10d8120...7f5dBb433	0.01 ETH	0.00010661
0x6f6c7854607...	Transfer	7056750	4 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF09f7Bc8...D4FcE8A5d	0.01 ETH	0.00011171
0xaaf654a277b...	Transfer	7056749	4 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF08aE578...4Bb3905a2	0.01 ETH	0.00011269
0x08d52bd08af...	Transfer	7056748	4 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF07dDBAb...498B7258C	0.01 ETH	0.00011418
0xda61eaa813...	Transfer	7056746	5 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF06ff8e6...4fdf145eA	0.01 ETH	0.00010879
0x26e3670ff28...	Transfer	7056745	5 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF05bDF88...ff9451930	0.01 ETH	0.00011256
0x21fa675821f...	Transfer	7056744	5 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF04ebF52...BAB74b88B	0.01 ETH	0.00011147
0x809215265a...	Transfer	7056742	5 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF03f3De9...c8bbeeA57	0.01 ETH	0.00011096
0x69b7f9b1c45...	Transfer	7056742	5 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF02e9033...5F74F4cb2	0.01 ETH	0.00011096
0xe049e2d2b7...	Transfer	7056740	6 mins ago	0x94eF0B92...Bb0bFFE9a	OUT	0xF01eA8B7...a55f42CCb	0.01 ETH	0.00011469

What is a token?

- Digital currencies that run on a blockchain.
- Usually built on an existing blockchain.
- Examples of tokens on Ethereum network:
  - *Chainlink (LINK)*
  - *Compound (COMP)*
  - *Tether (USDT)*
  - *Uniswap (UNI)*
  - *Aave (AAVE)*



What do you transfer first?

ETH balance?

or

Uniswap balance?

First consfiscate ETH or the token?

Seize the token first

Transaction fees for sending tokens are paid in ETH. If you transfer all the ETH first, you may not have ETH left to pay the token transfer transaction fee.

After that, confiscate the ETH

Once you have sent the token, you can transfer the remaining ETH amount to the prosecutor's wallet without worrying about having enough ETH for transaction fees (gas fee).

Afterthoughts

Check, check, double-check the transaction, because gone is gone!

A typo can inadvertently cause cryptocurrency to be “burned”

Always confiscate the token first and only then the main token.

Check carefully that you do not leave any crypto currency unintentionally in the wallet.

If the fee is too low, the transaction may get stuck or not be processed.

Always check (on the blockchain) if your transaction actually succeeded.

Do not use unreliable software/hardware for transferring.