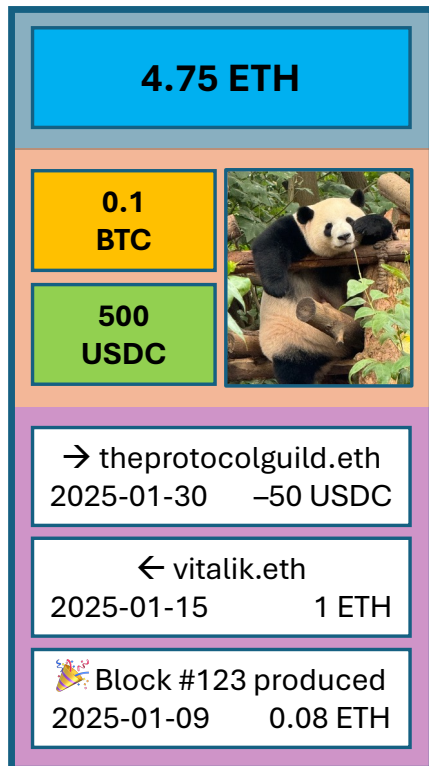


# Trust-minimized wallets with purified web3

Etan Kissling, Nimbus, IFT

30 Jan 2025 / [EthereumZuri.ch](https://EthereumZuri.ch)

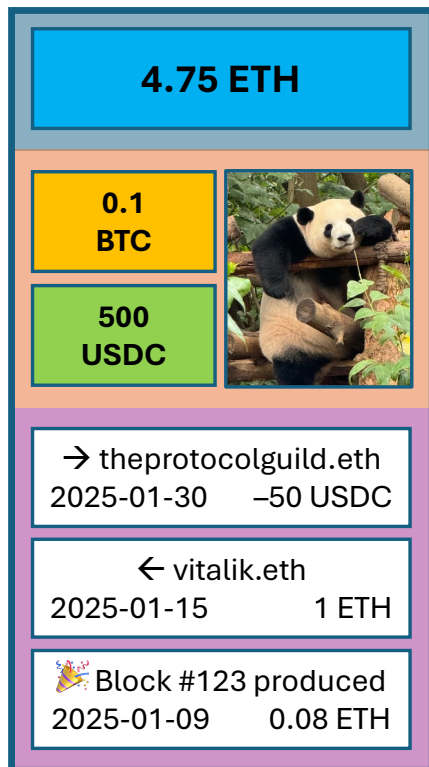
# Wallet



Mobile app

Browser extension

# Wallet



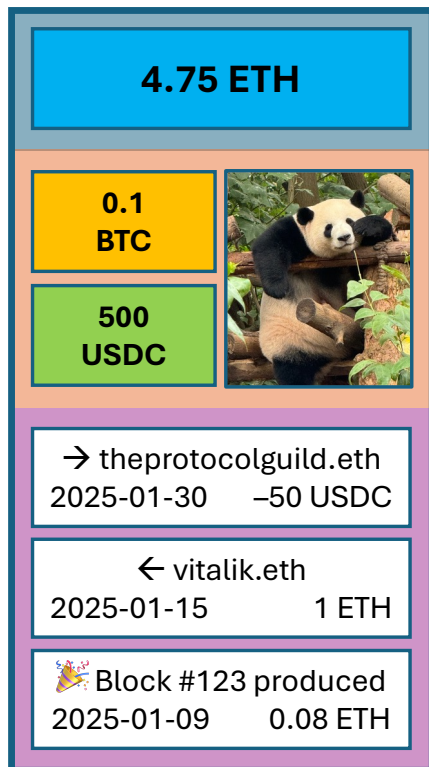
Mobile app

Browser extension

+ Hardware wallet (optional)



# Wallet



Mobile app

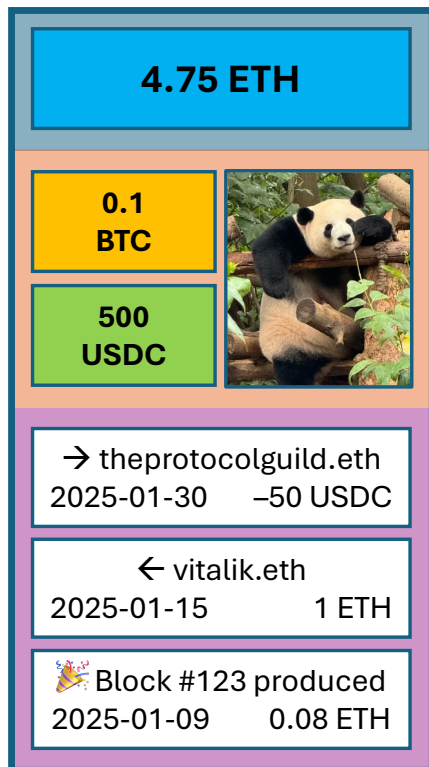
Browser extension



Secure transaction signing



# Wallet



? ETH balance

? Tokens / NFTs

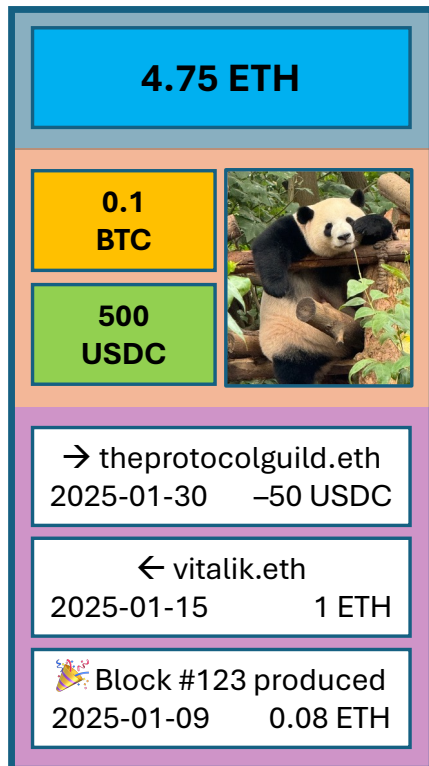
? History



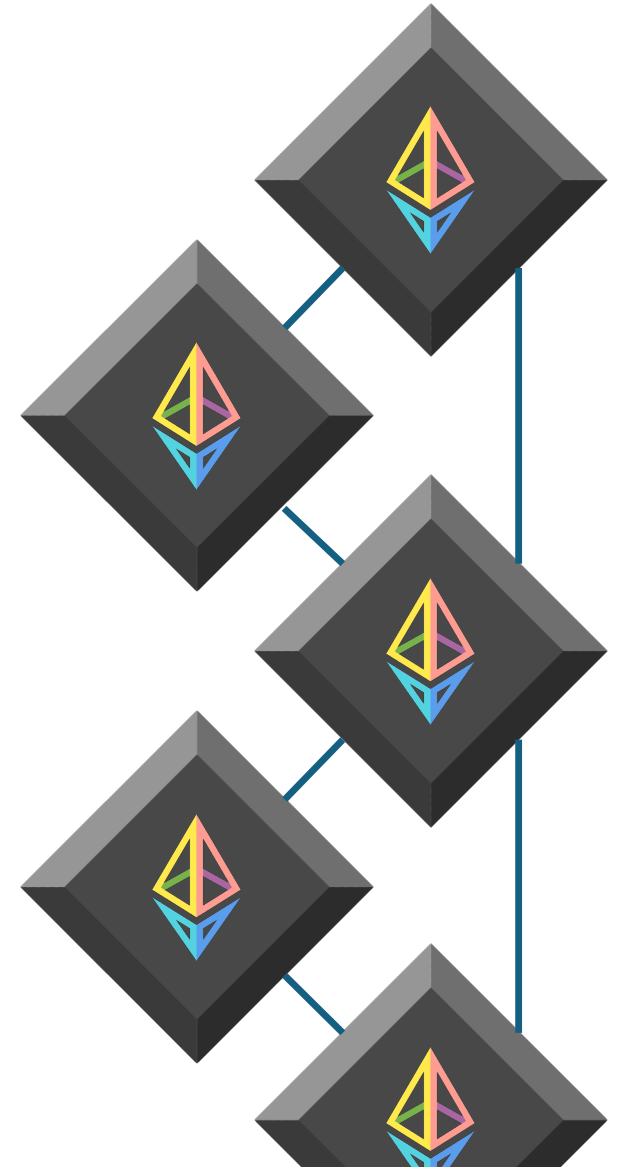
Secure transaction signing



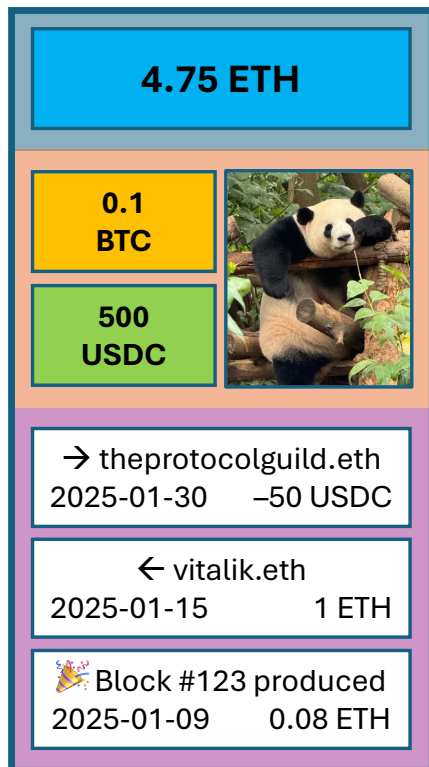
# Wallet (obtaining data)



- ? ETH balance
- ? Tokens / NFTs
- ? History



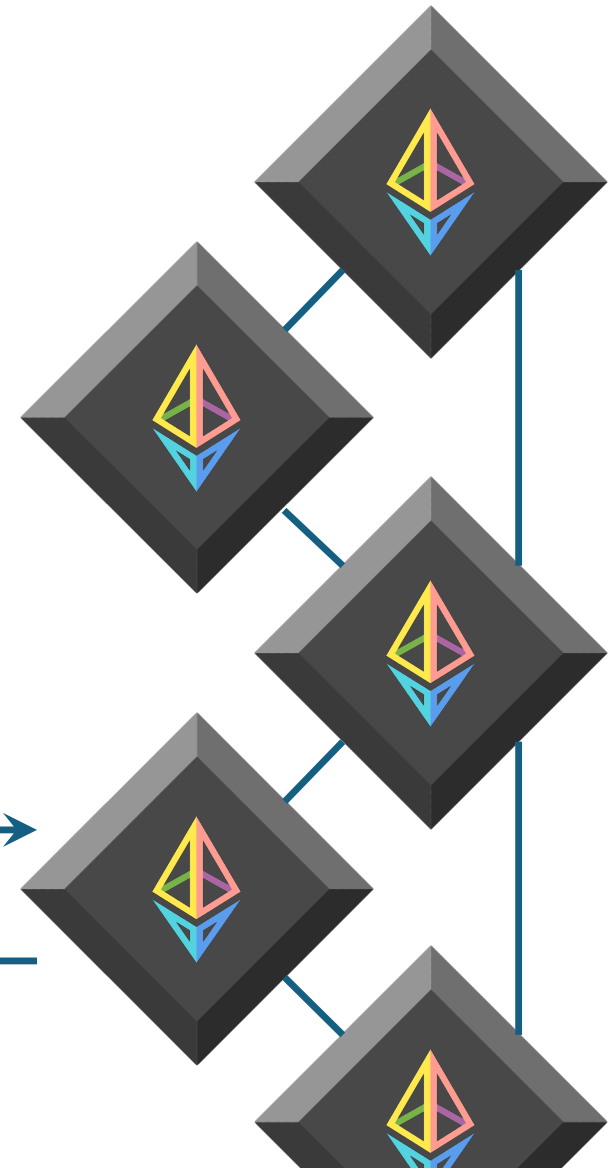
# Wallet (obtaining data)



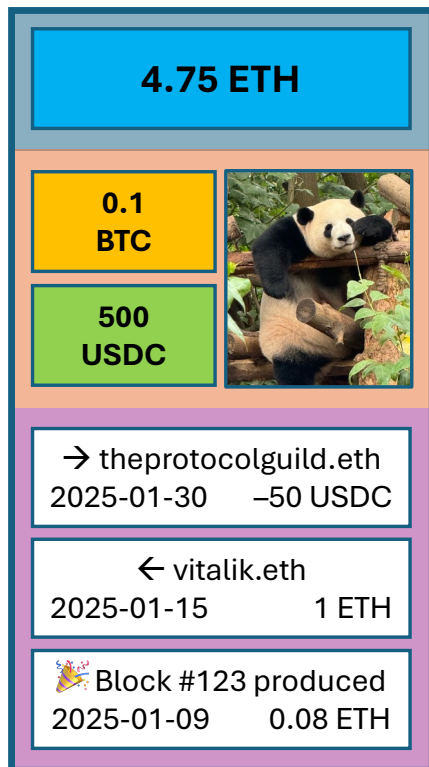
- ? ETH balance
- ? Tokens / NFTs
- ? History

eth\_getBalance

4.75  
ETH



# Wallet (obtaining data)

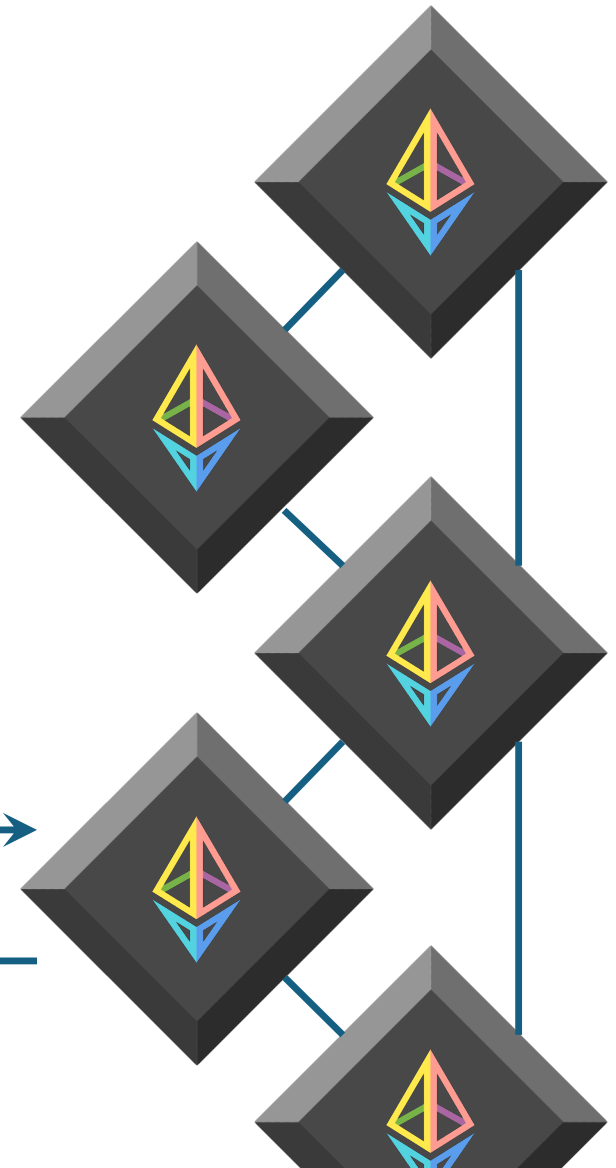


- ? ETH balance
- ? Tokens / NFTs
- ? History

eth\_getBalance

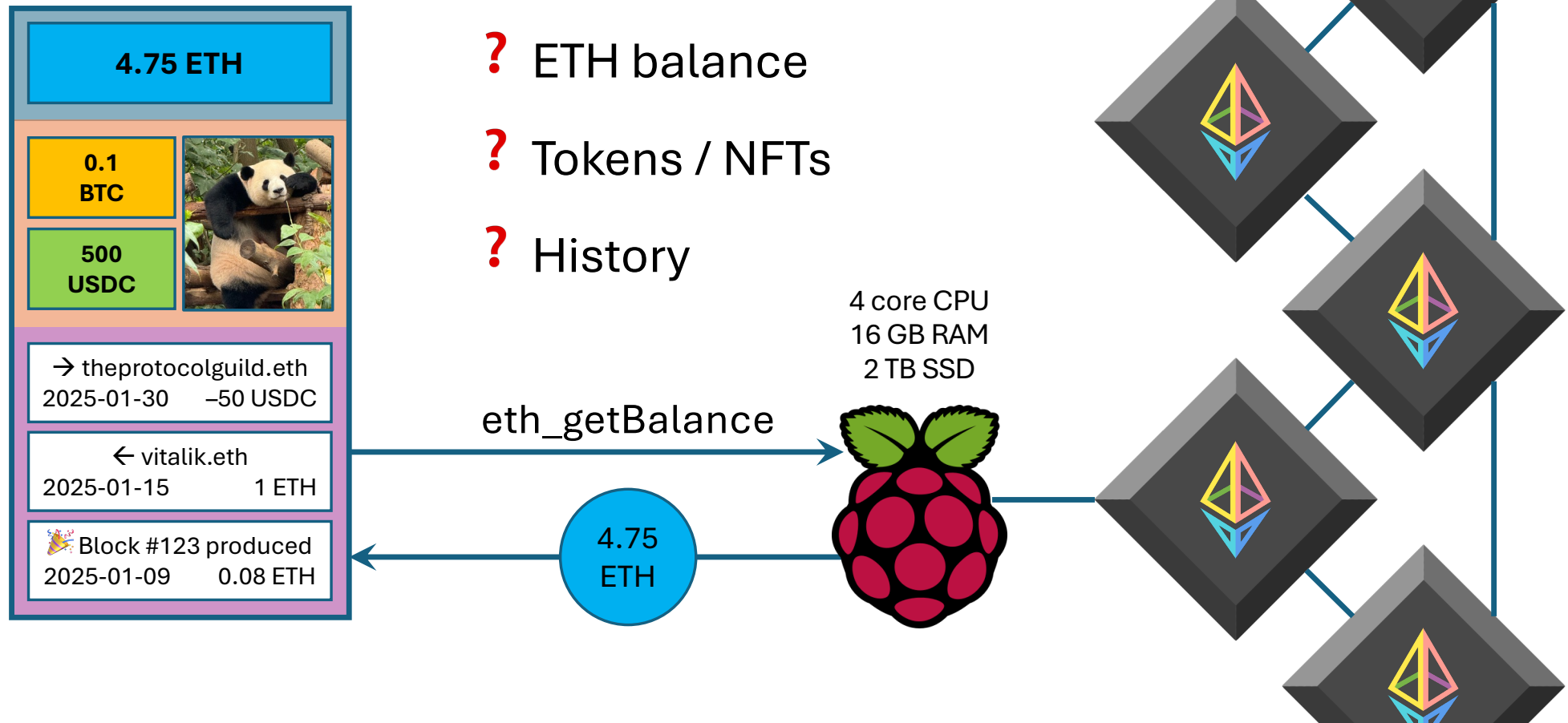
4.75  
ETH

“trust me bro”

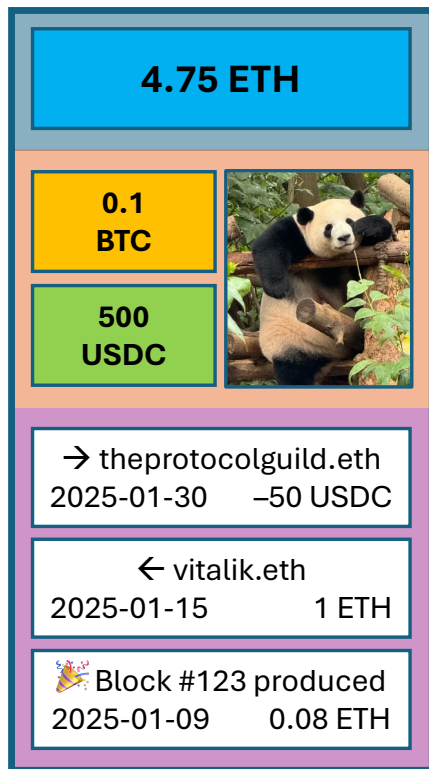




# Wallet (run your own node)



# Wallet (RPC provider)

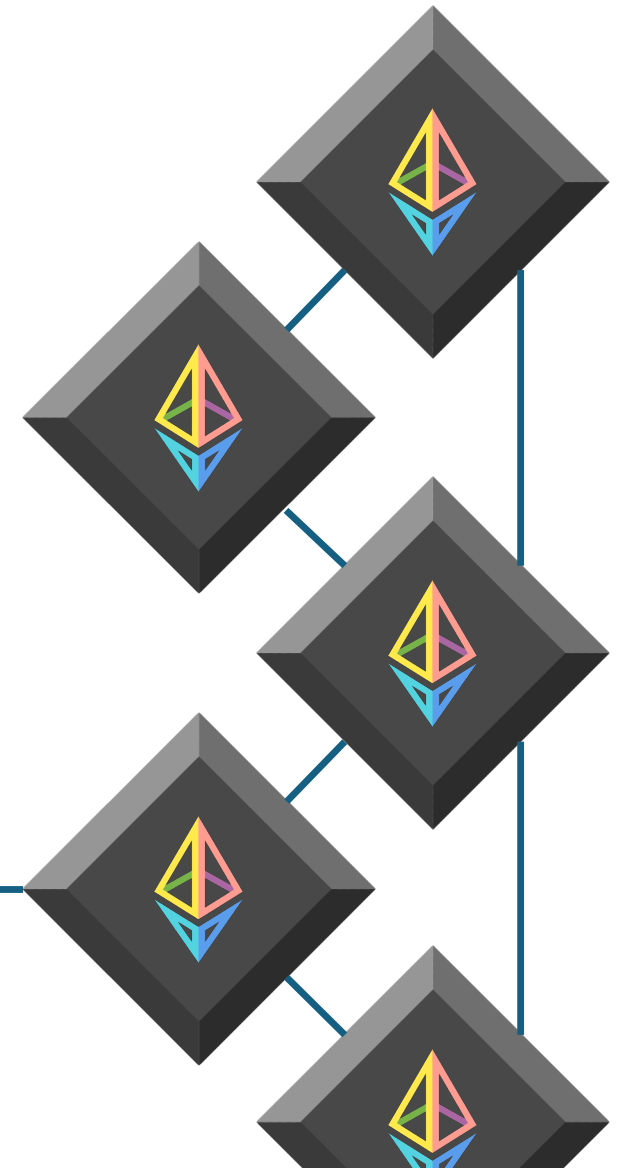


- ? ETH balance
- ? Tokens / NFTs
- ? History

eth\_getBalance

Web3  
API  
provider

4.75  
ETH

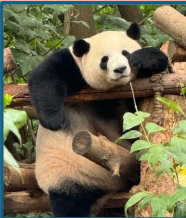


# Decentralization?

4.75 ETH


0.1 BTC

500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15    1 ETH

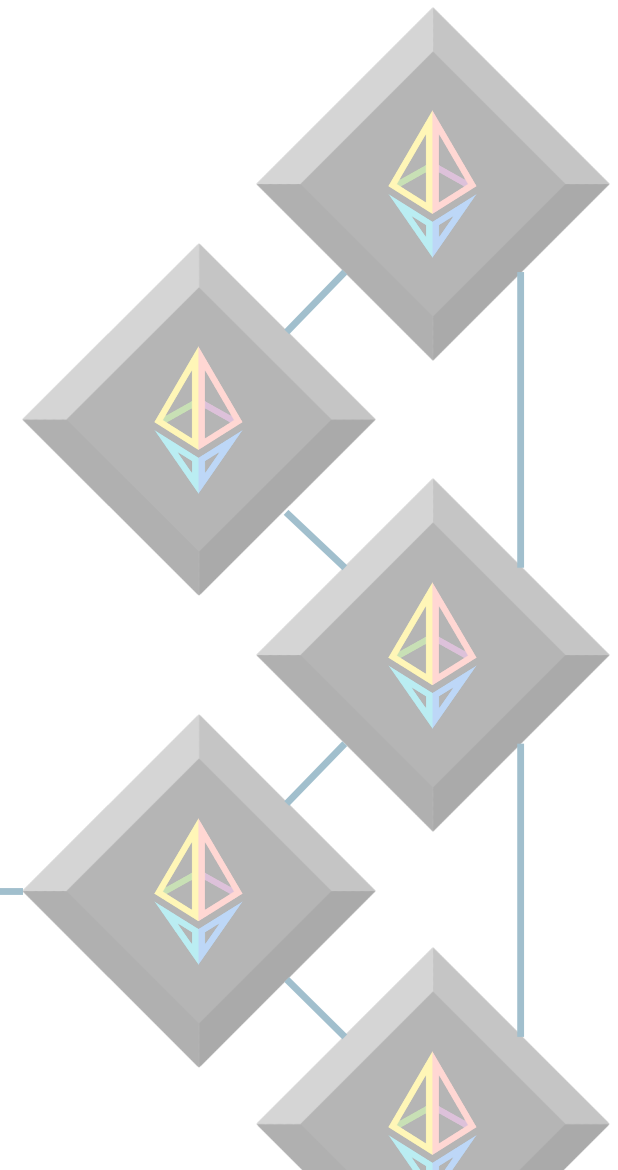
 Block #123 produced  
2025-01-09    0.08 ETH

- ? ETH balance
- ? Tokens / NFTs
- ? History

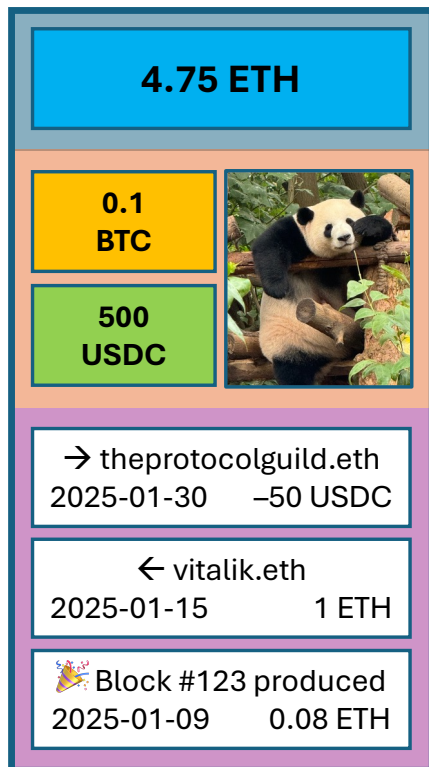
eth\_getBalance

Web3  
API  
provider

4.75  
ETH



# Decentralization?




- ? ETH balance
- ? Tokens / NFTs
- ? History

eth\_getBalance

Web3  
API  
provider

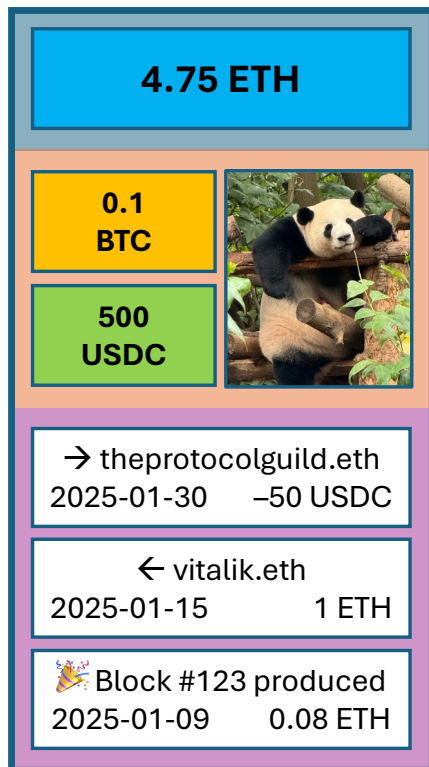
4.75  
ETH

- ⚡ Downtimes
- ⚡ Security
- ⚡ Censorship
- ⚡ Privacy



IP	Wallet
123.xyz.0.0	0x131..aF8
123.xyz.0.0	0x42a..E02

# Decentralization?



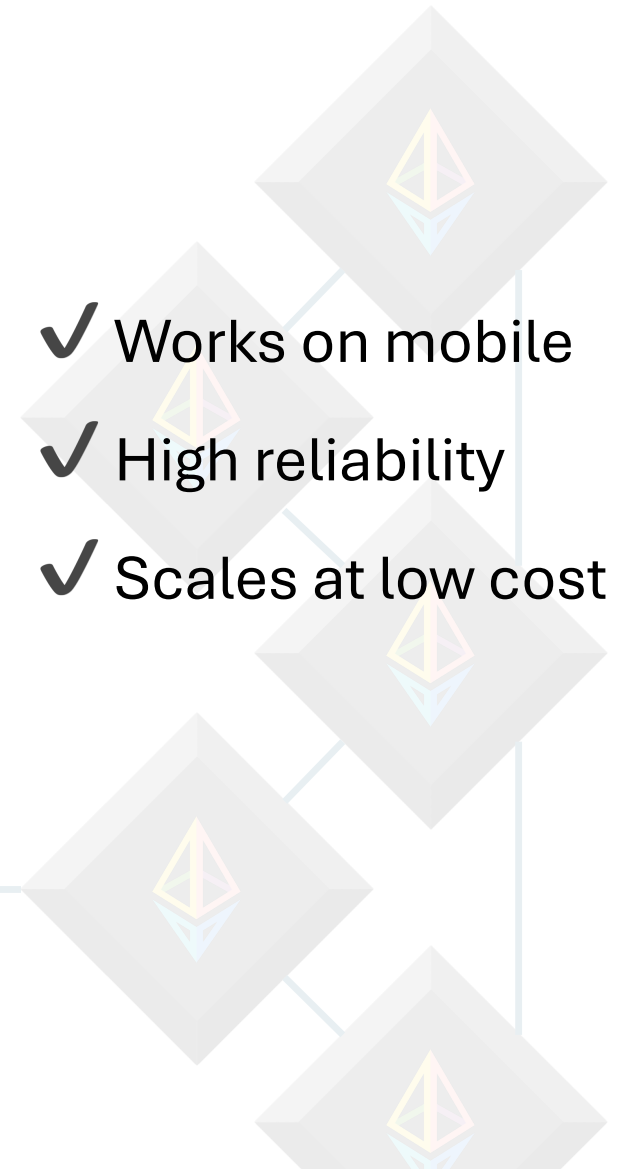
- ? ETH balance
- ? Tokens / NFTs
- ? History

eth\_getBalance

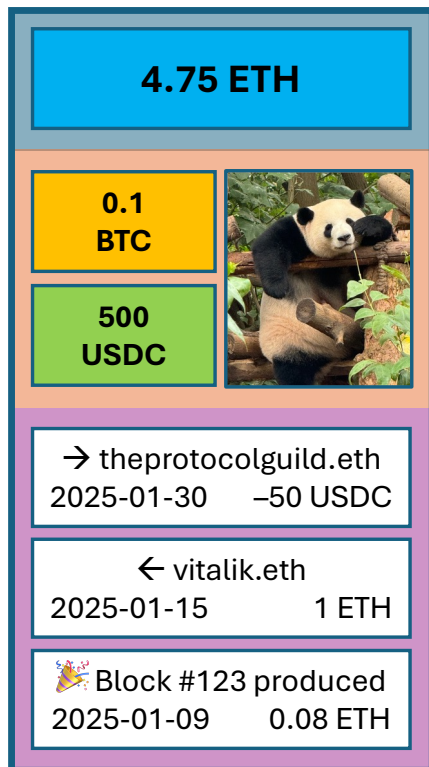
4.75  
ETH

Web3  
API  
provider

- ✓ Works on mobile
- ✓ High reliability
- ✓ Scales at low cost



# Decentralization?



? ETH balance

? Tokens / NFTs

? History

✓ Works on mobile

✓ High reliability

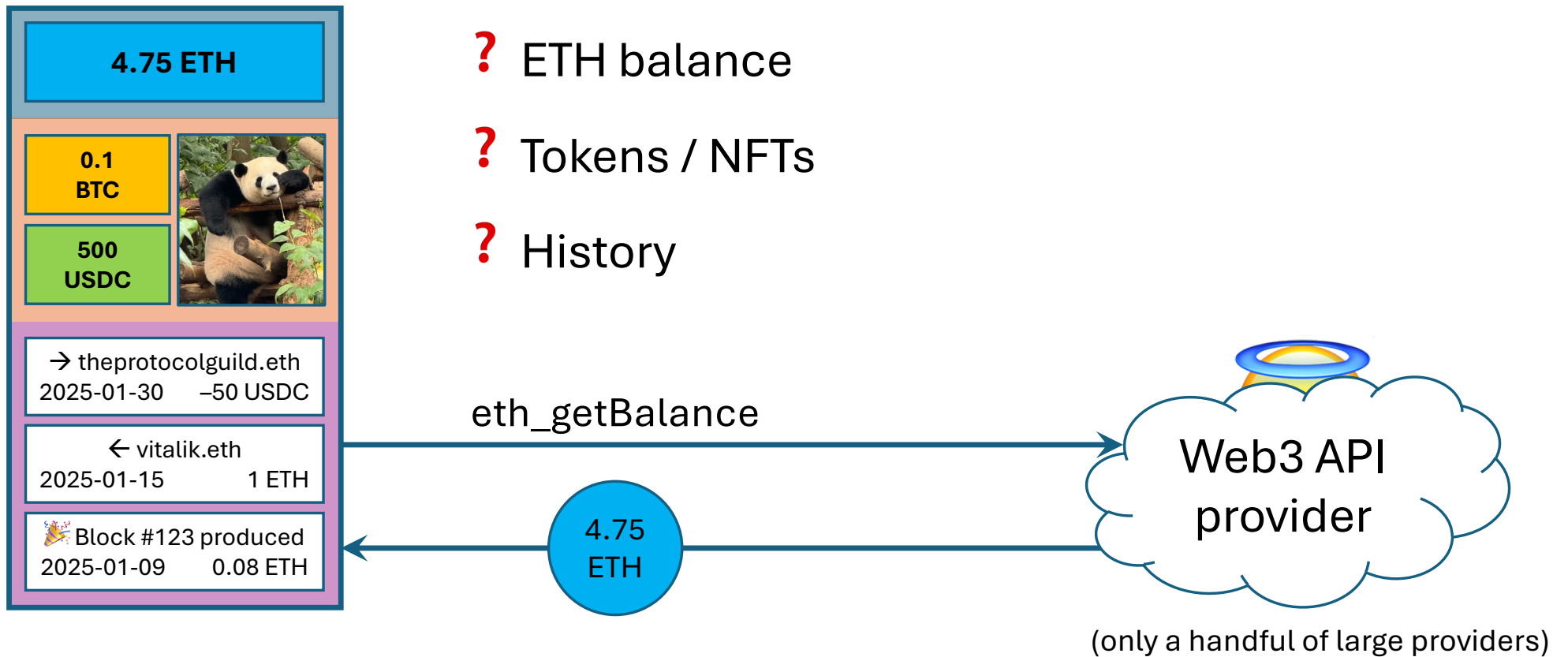
✓ Scales at low cost

eth\_getBalance

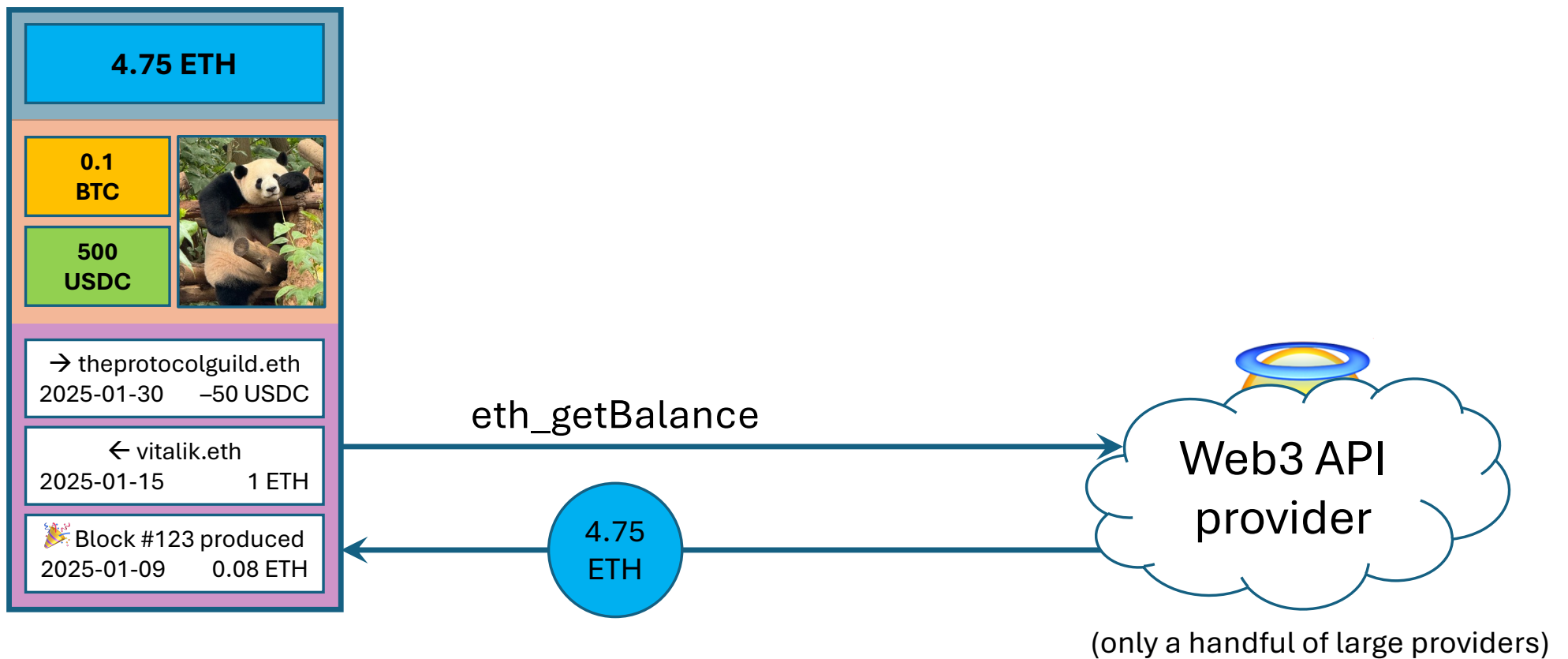
4.75  
ETH

Web3 API  
provider

# Today's reality



# How to fix it?

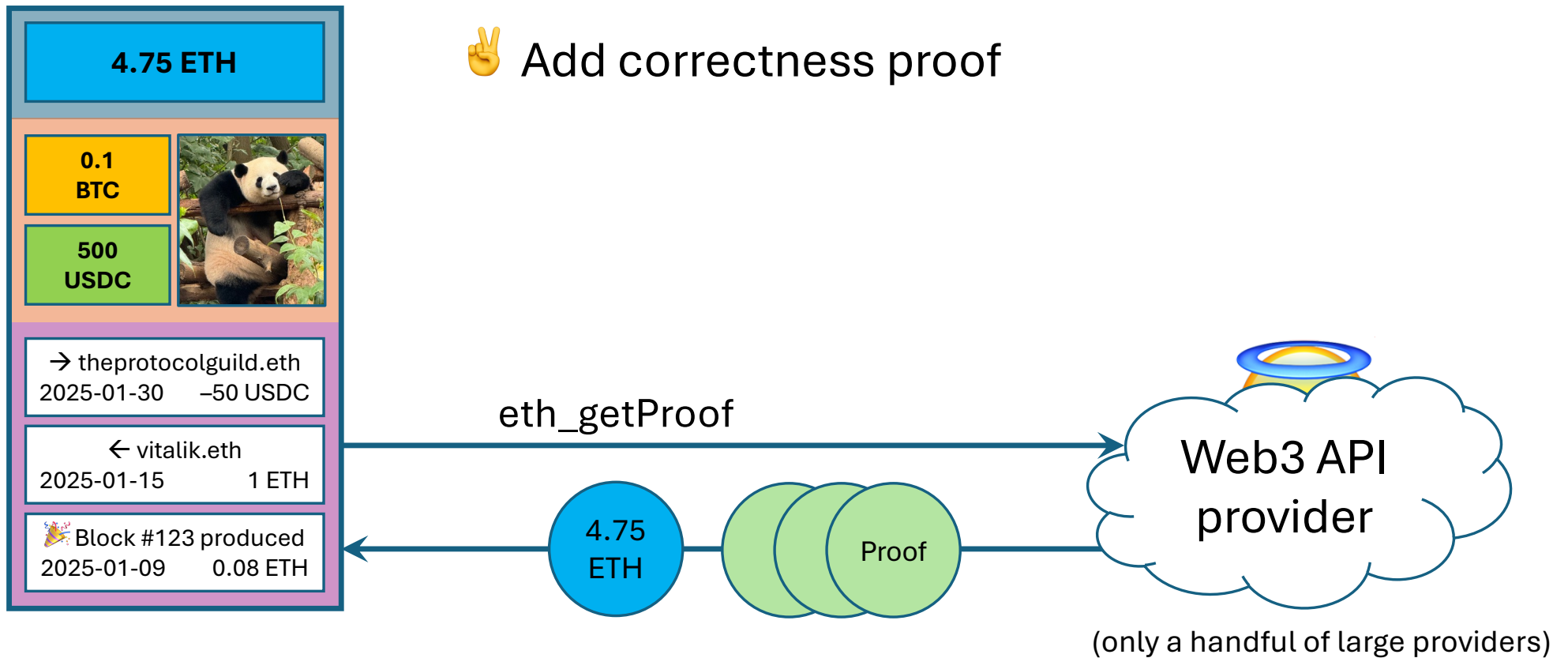






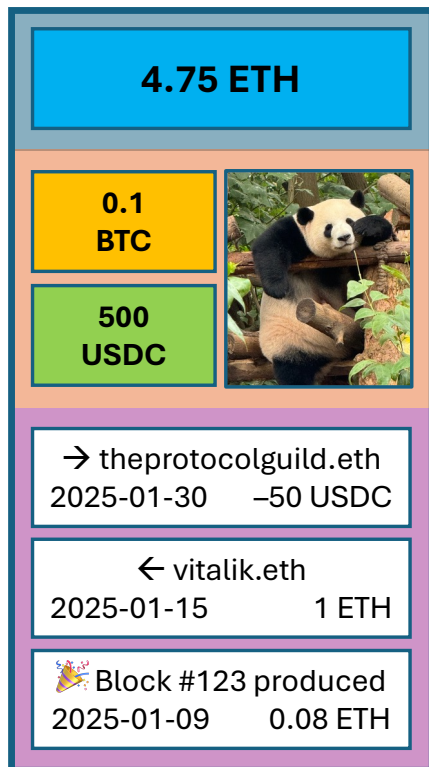
# EIP-1186: eth\_getProof

✌️ Add correctness proof



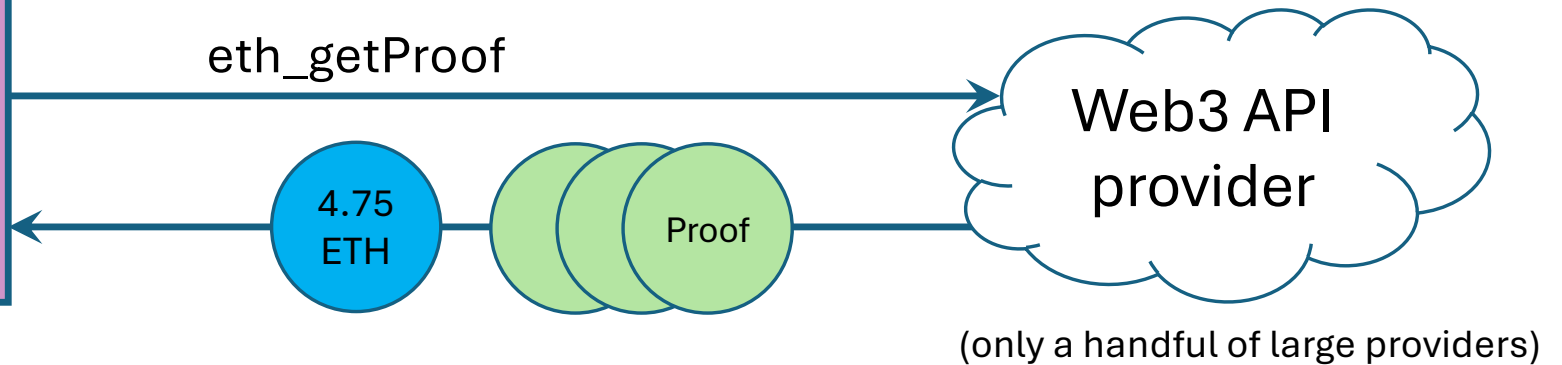


# EIP-1186: eth\_getProof



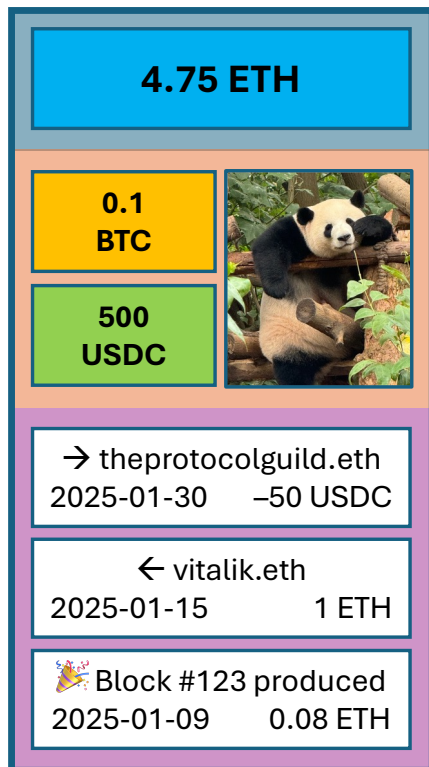
✌️ Add correctness proof

✌️ Data can be verified

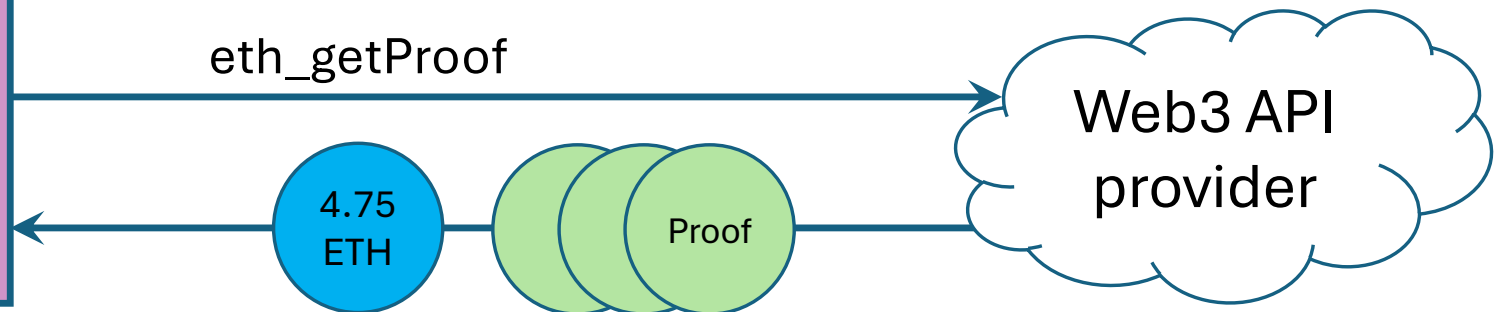




# EIP-1186: eth\_getProof

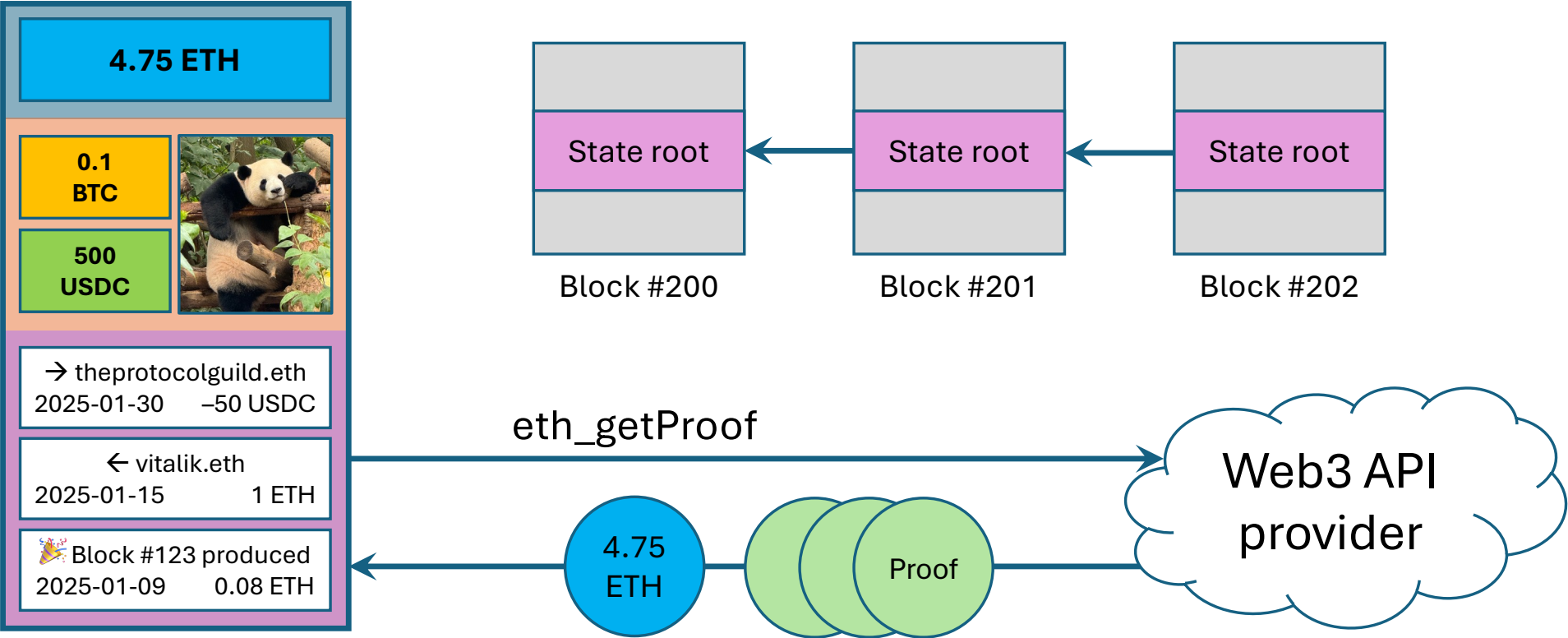


- ✌️ Add correctness proof
- ✌️ Data can be verified
- ✌️ Can ask any provider → decentralization





# Merkle trees



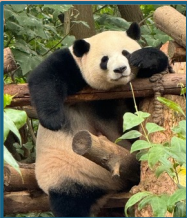


# Merkle trees

4.75 ETH

0.1 BTC

500 USDC



→ theprotocolguild.eth

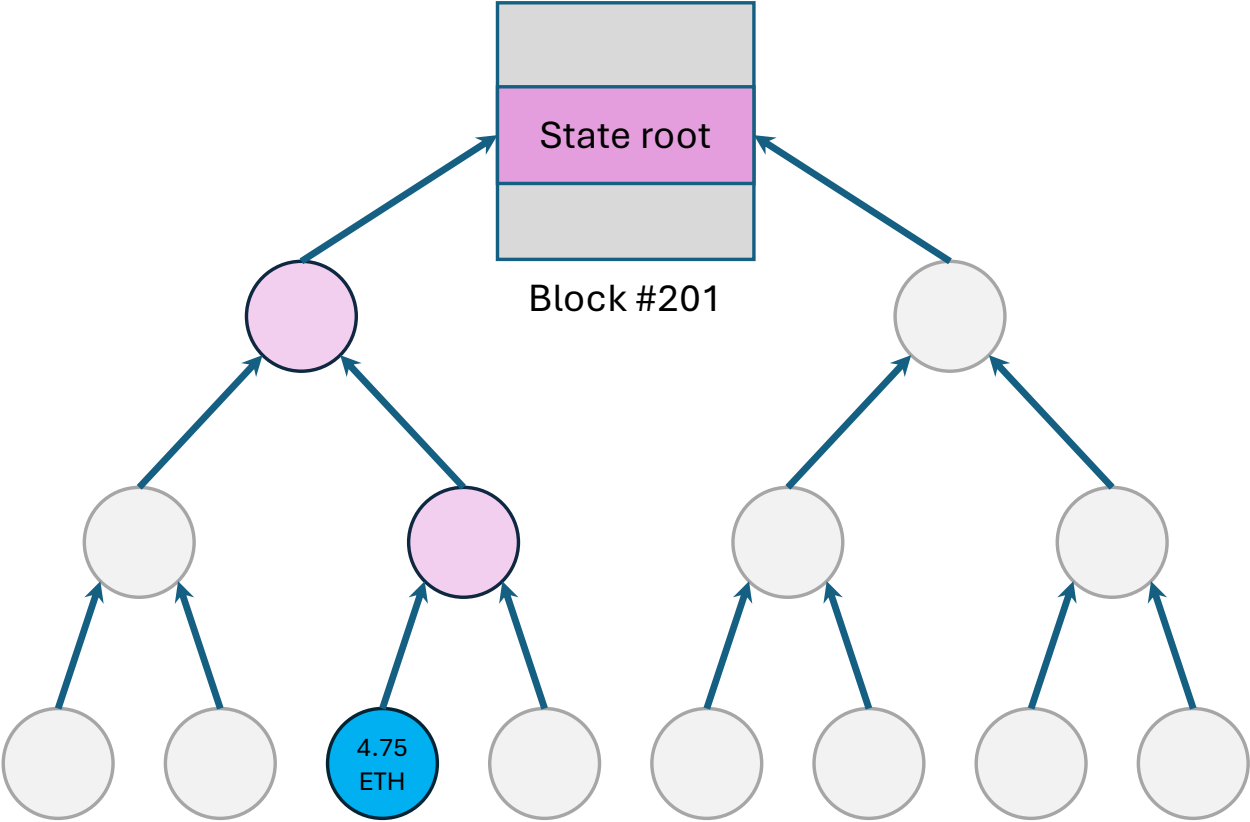
2025-01-30    -50 USDC

← vitalik.eth

2025-01-15        1 ETH

🎉 Block #123 produced

2025-01-09        0.08 ETH



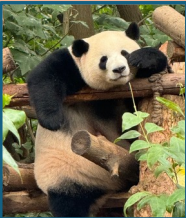


# Merkle trees

4.75 ETH

0.1 BTC

500 USDC



→ theprotocolguild.eth

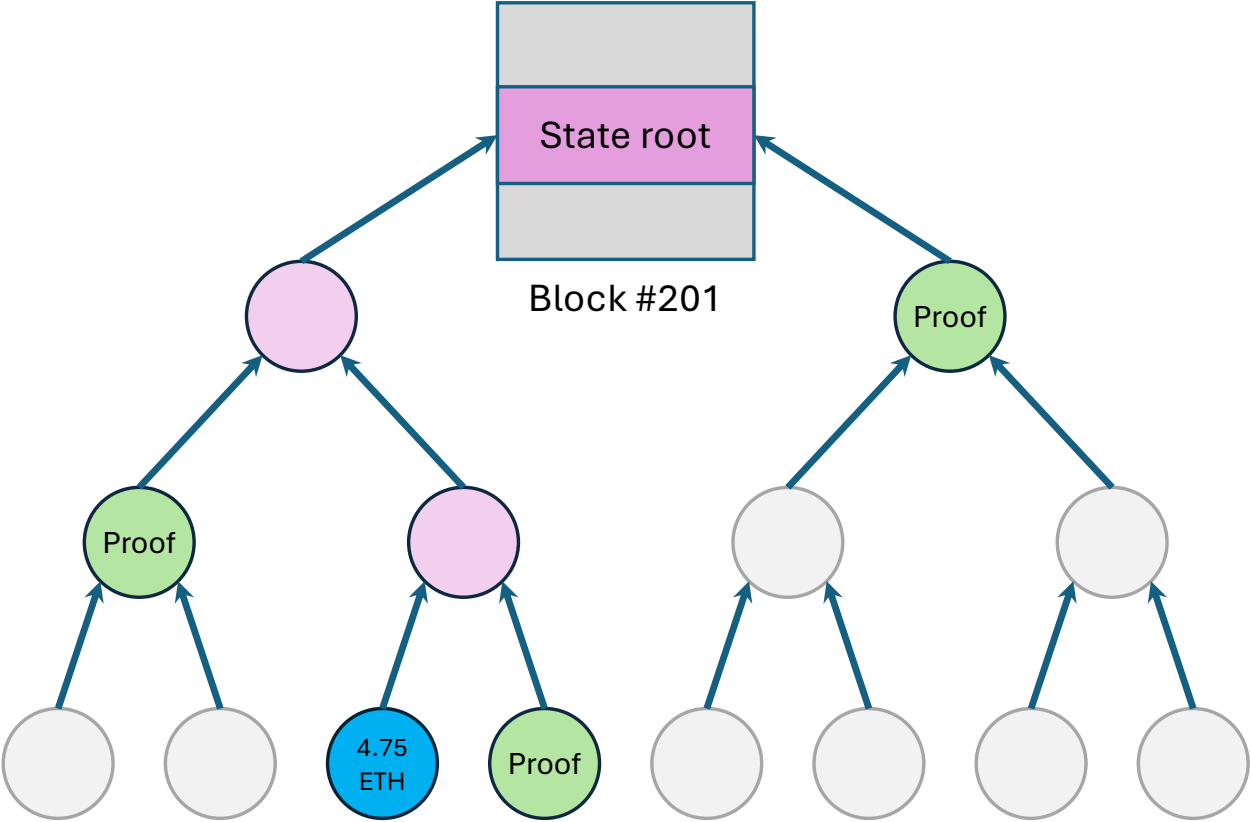
2025-01-30    -50 USDC

← vitalik.eth

2025-01-15        1 ETH

🎉 Block #123 produced

2025-01-09        0.08 ETH



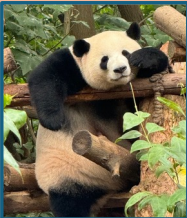


# Merkle trees

4.75 ETH

0.1 BTC

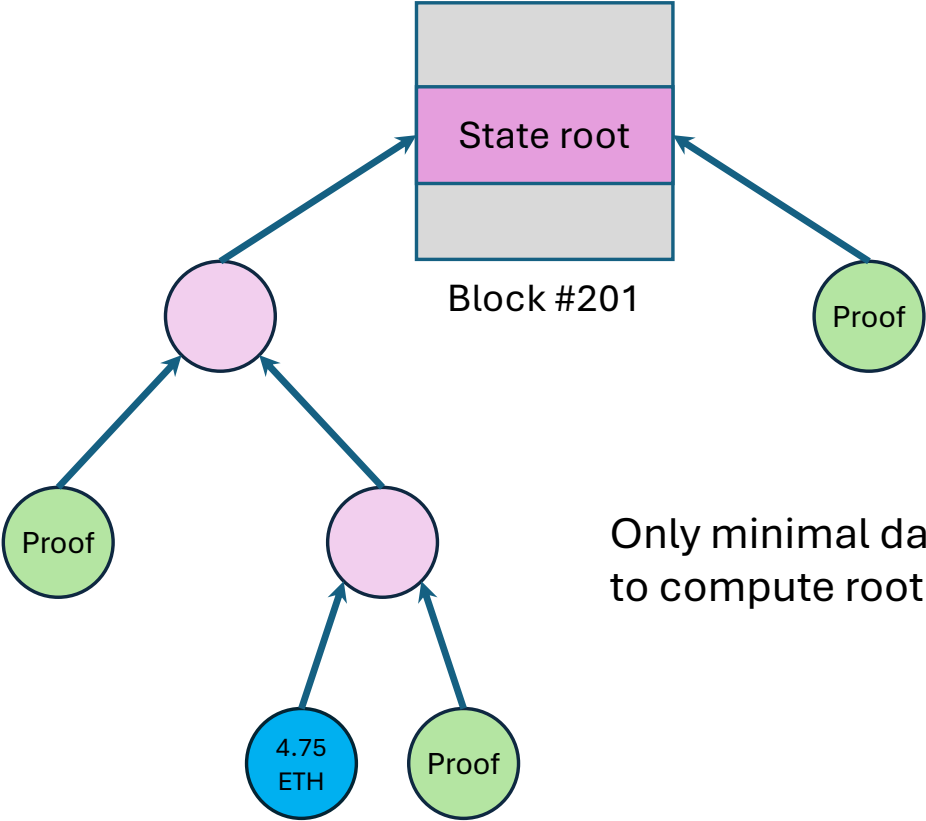
500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

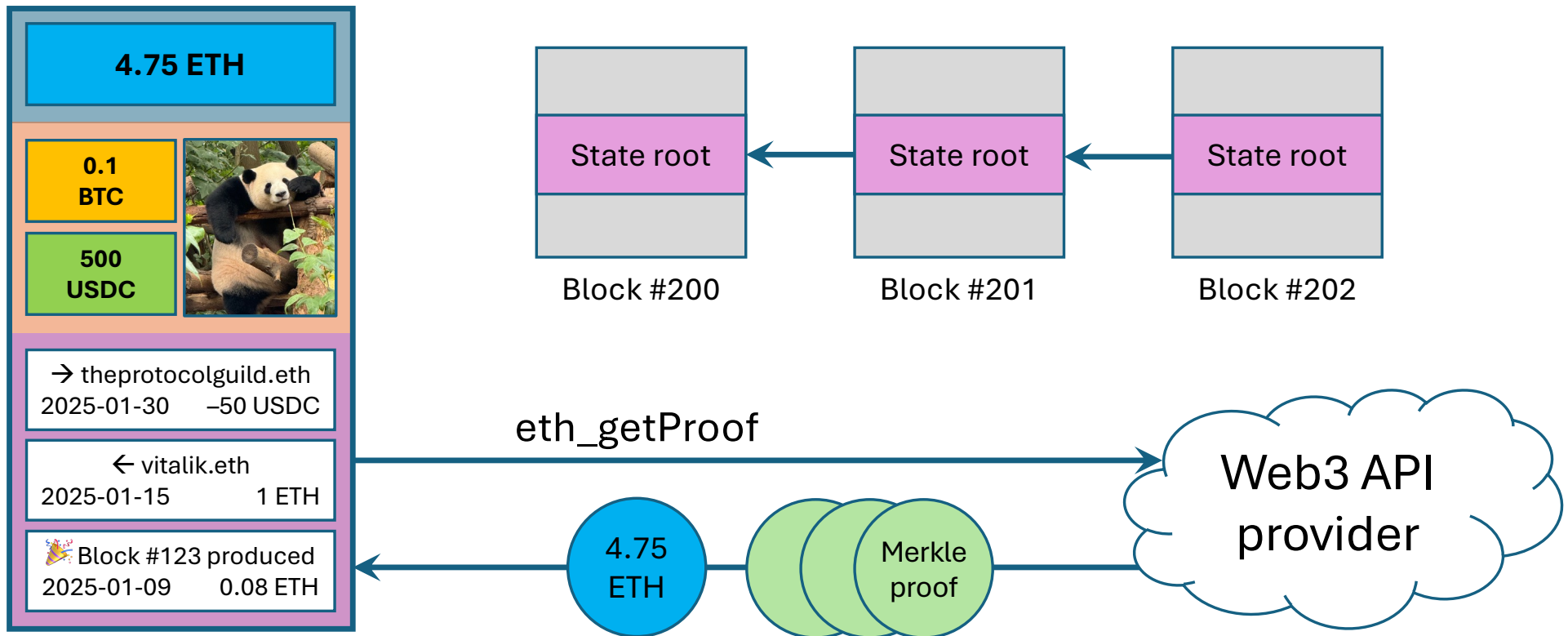
🎉 Block #123 produced  
2025-01-09        0.08 ETH



Only minimal data required to compute root hash



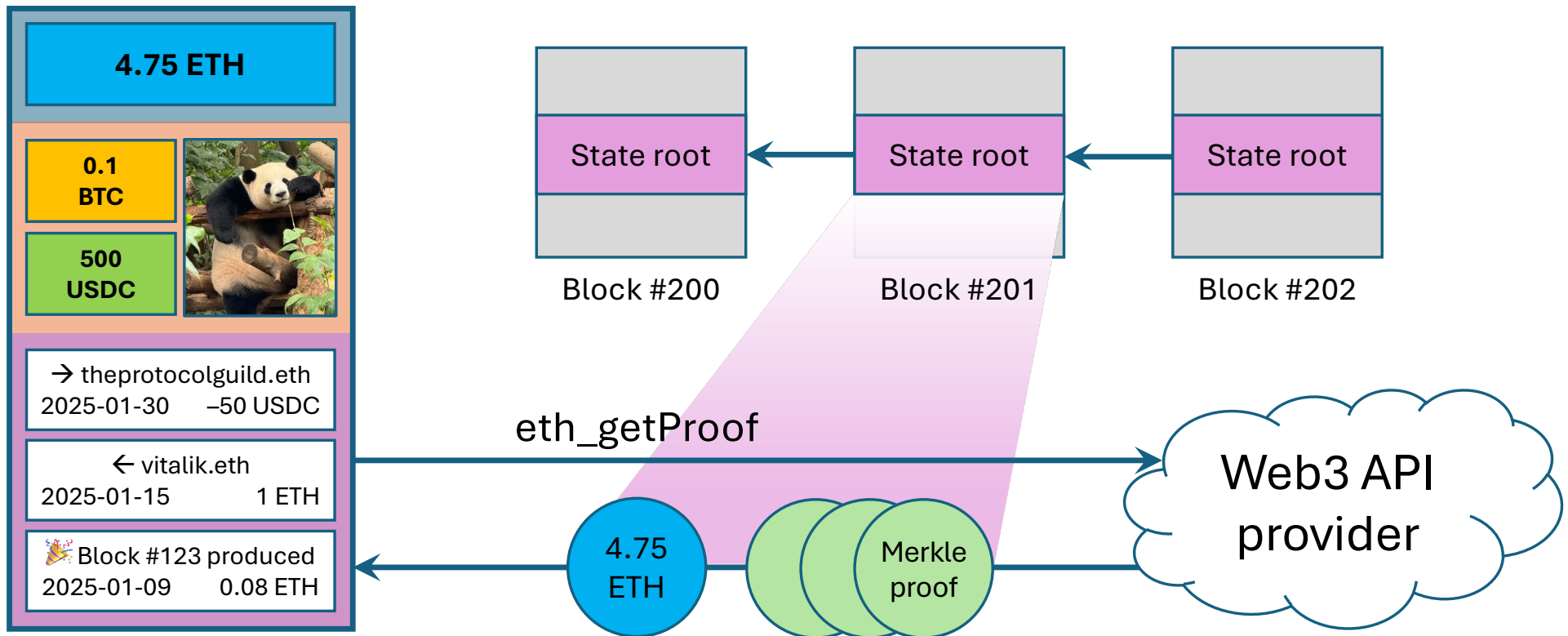
# EIP-1186: eth\_getProof





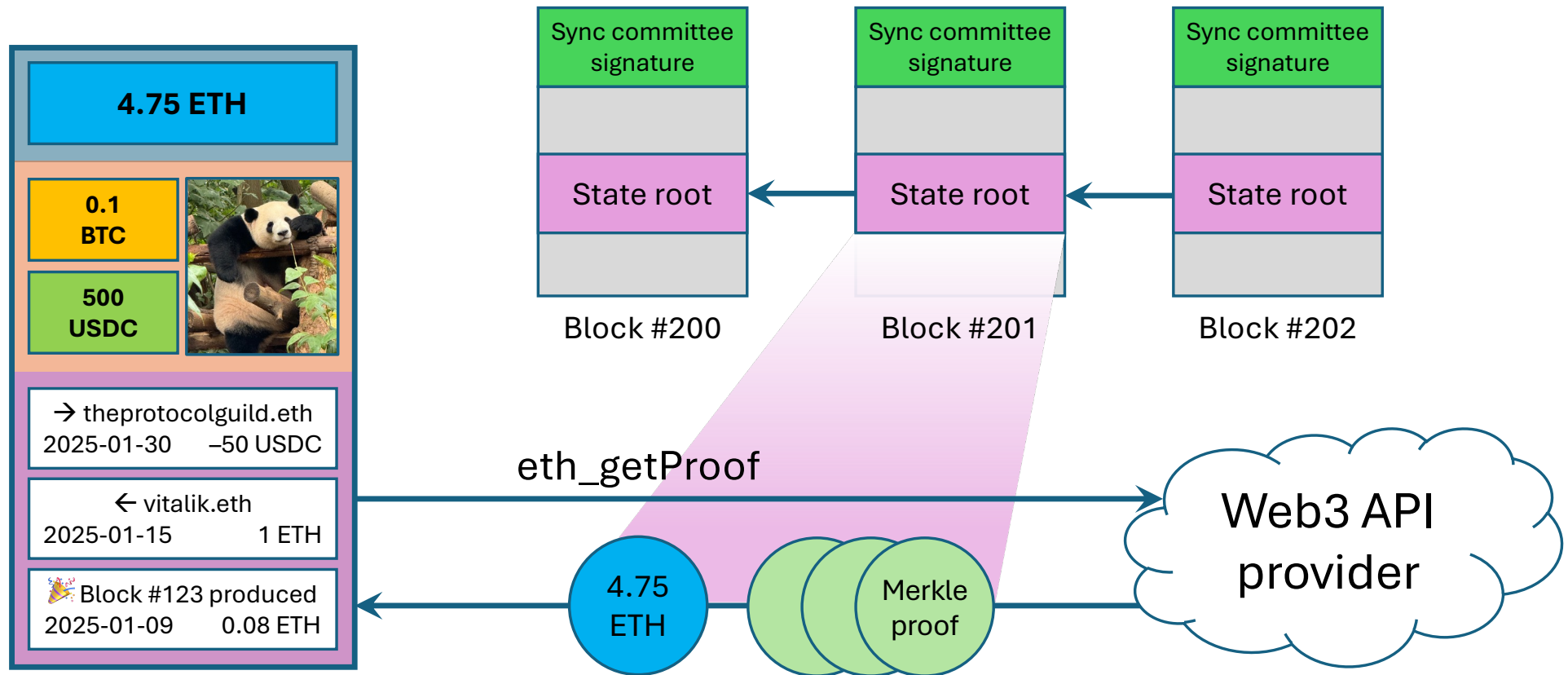


# EIP-1186: eth\_getProof



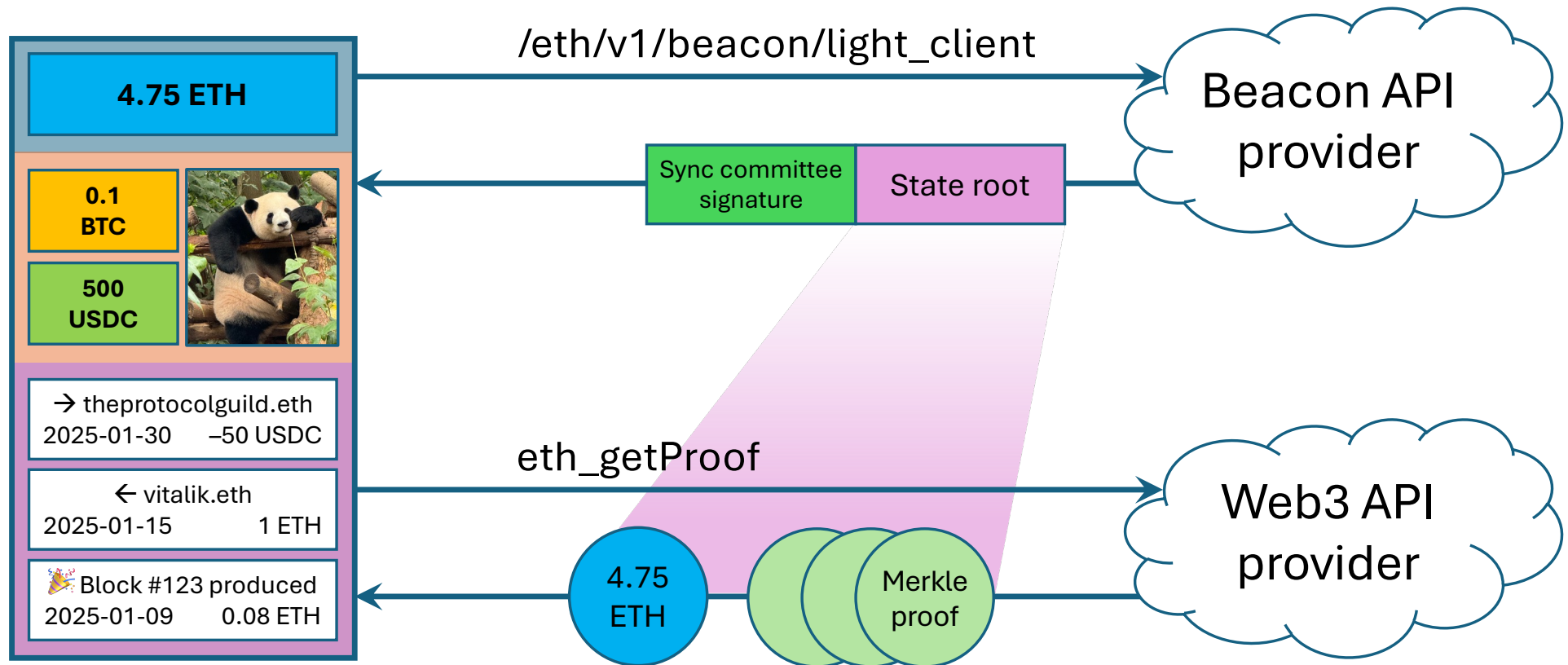


# Altair light client protocol



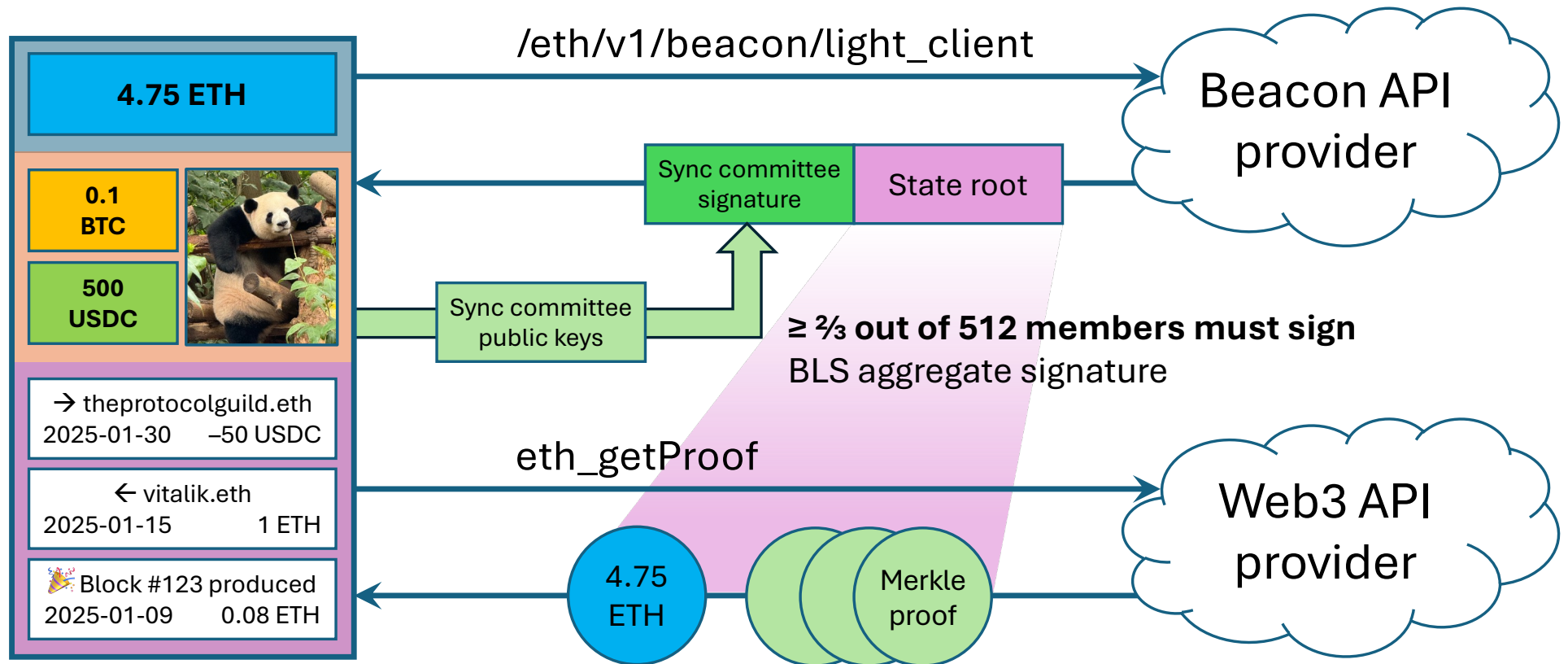


# Altair light client protocol



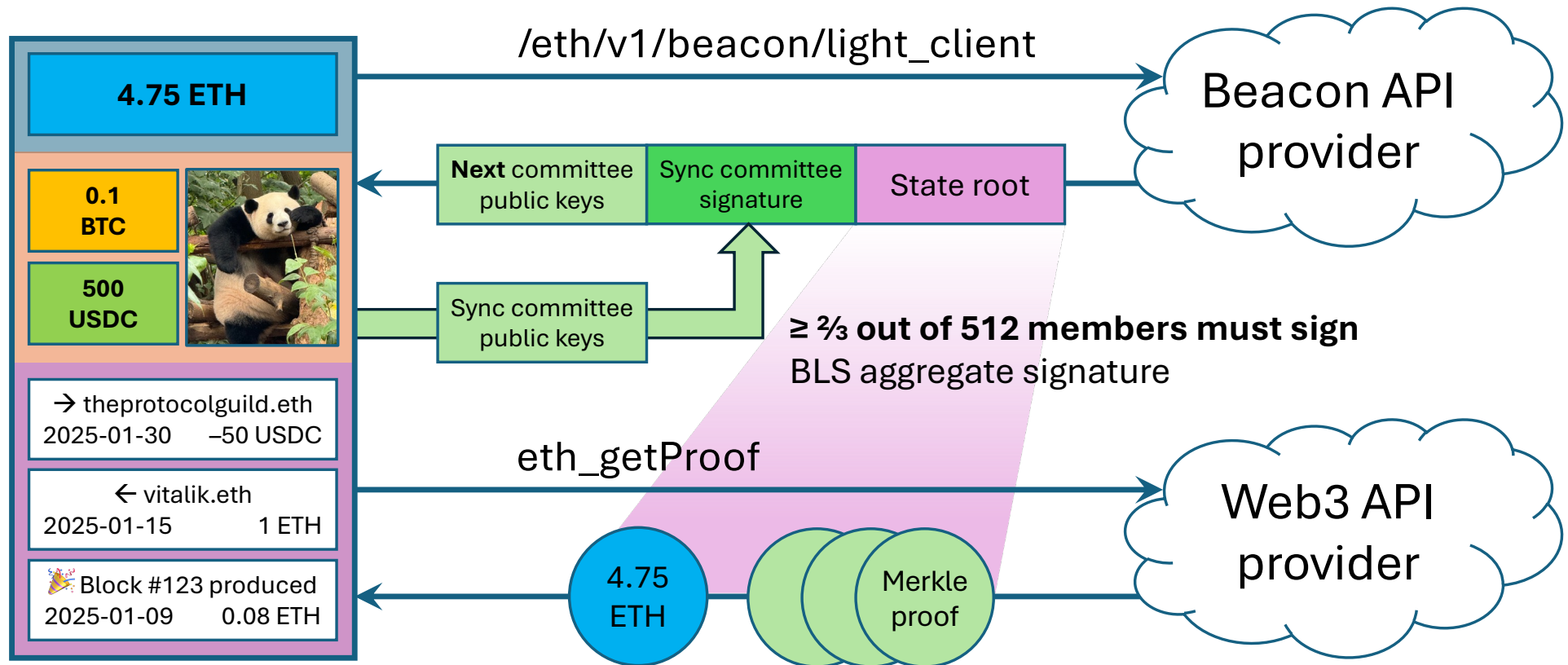


# Altair light client protocol



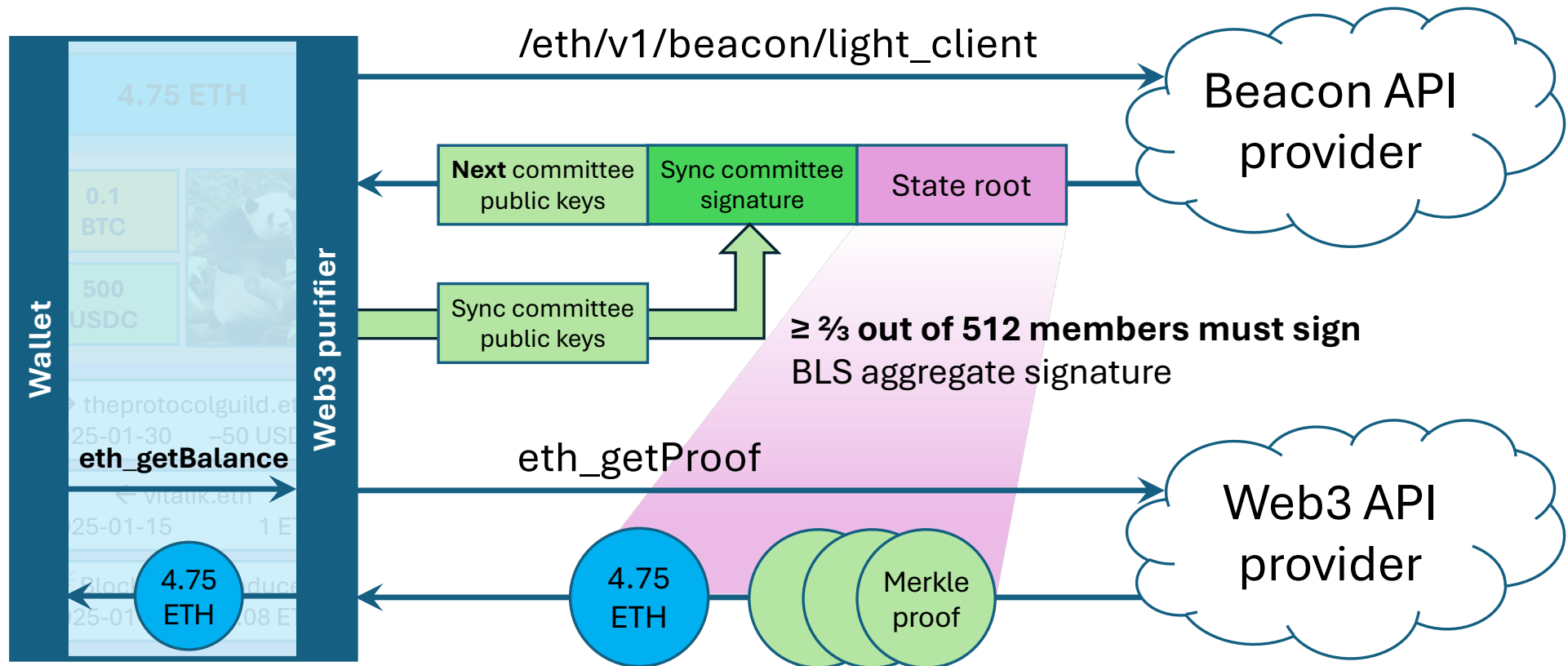


# Altair light client protocol



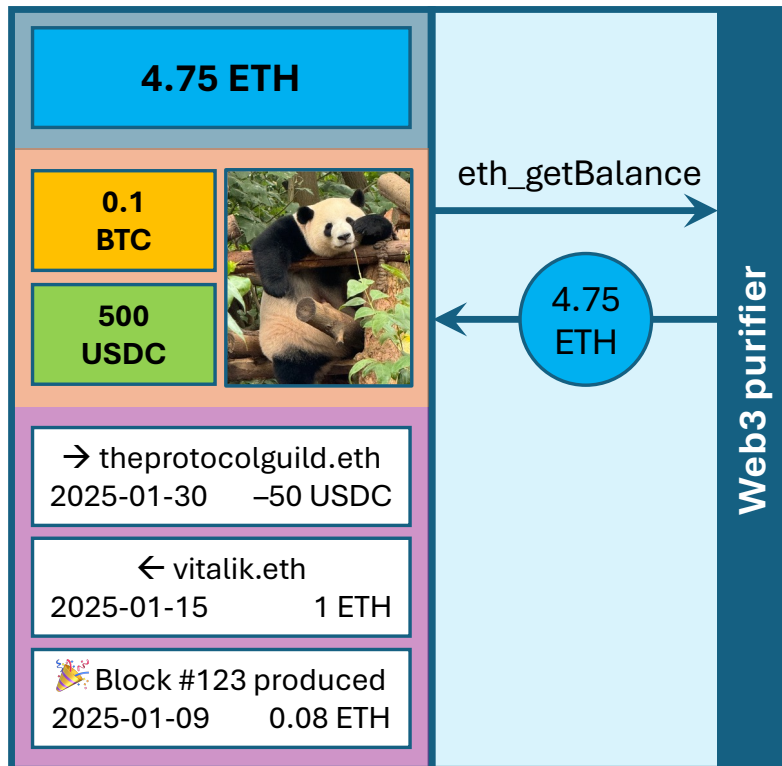


# Web3 purifier library



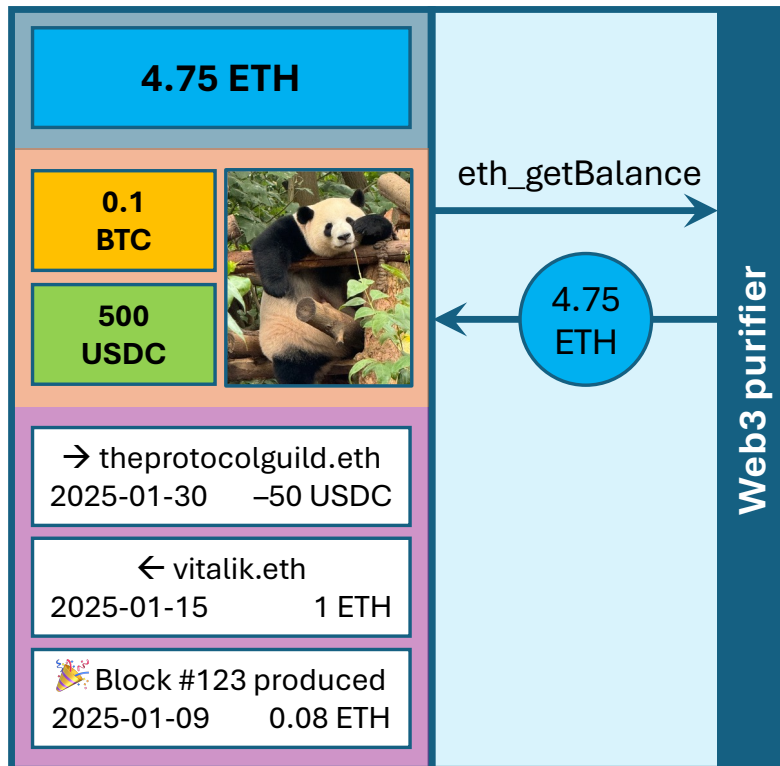


# Web3 purifier library





# Web3 purifier library

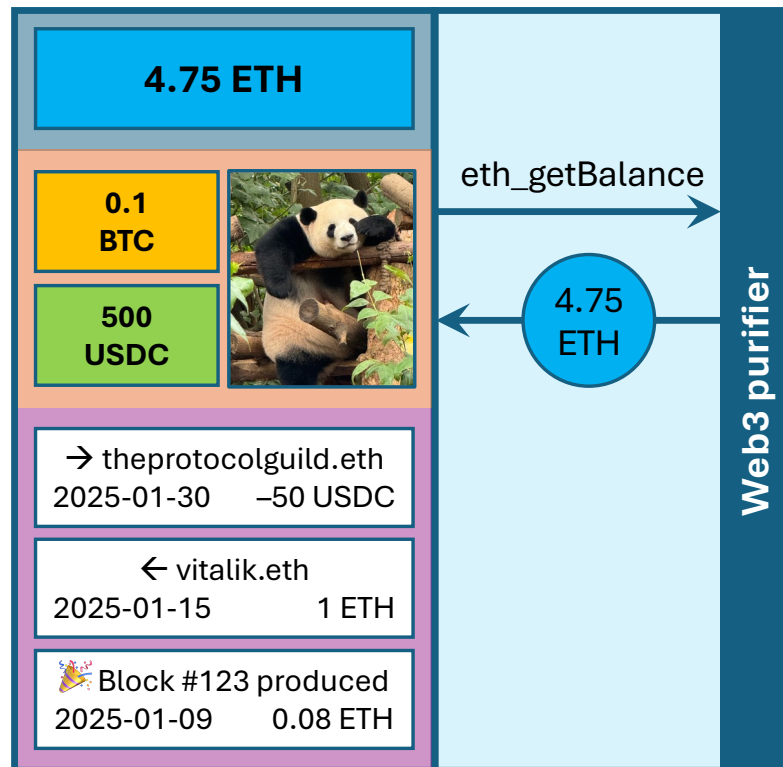


🕺 Universal API





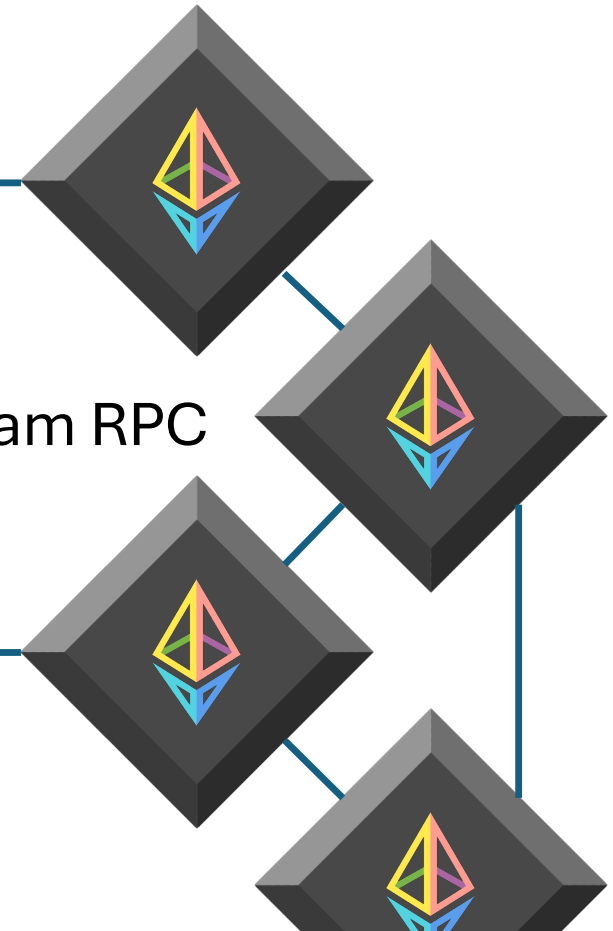
# Web3 purifier library



Universal API

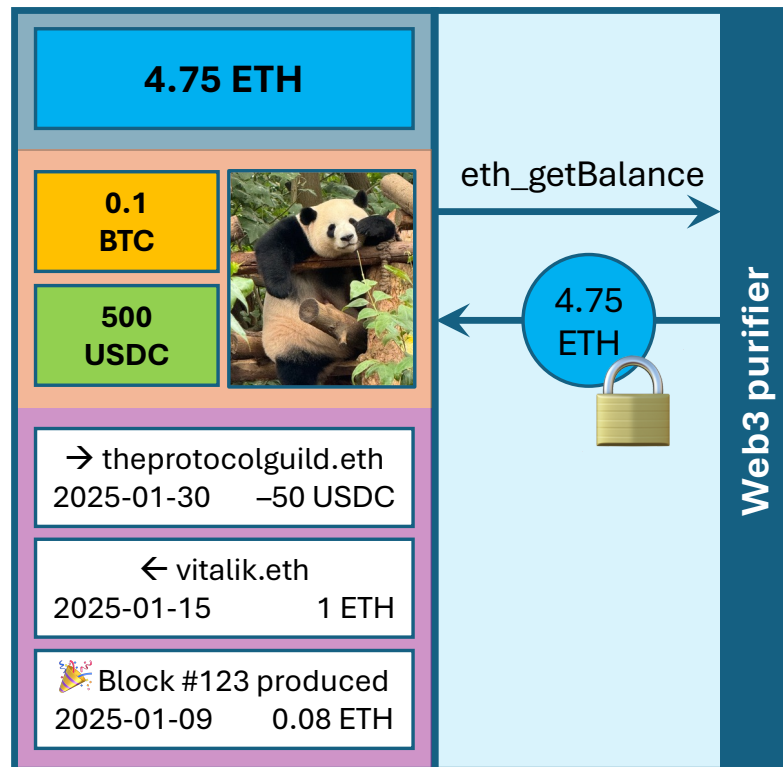


Use any upstream RPC

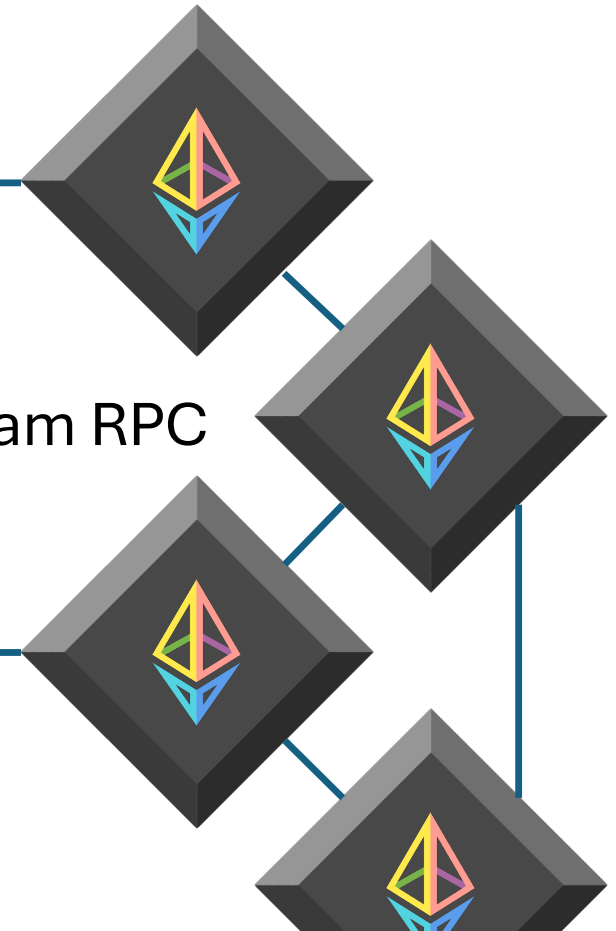




# Web3 purifier library

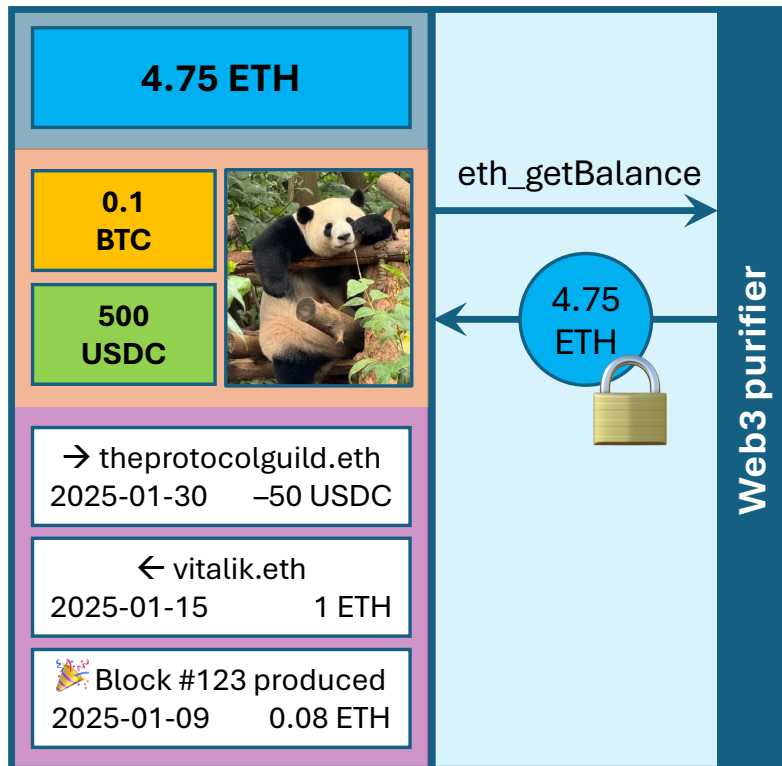


- ✌️ Universal API
- ✌️ Use any upstream RPC
- ✌️ Security





# Web3 purifier library



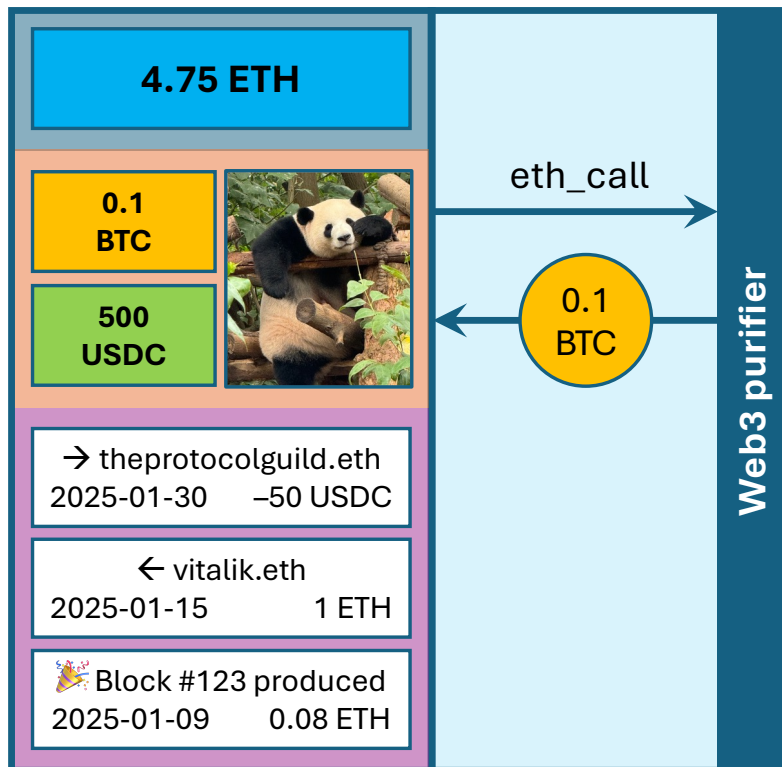
✓ ETH balance

? Tokens / NFTs

? History



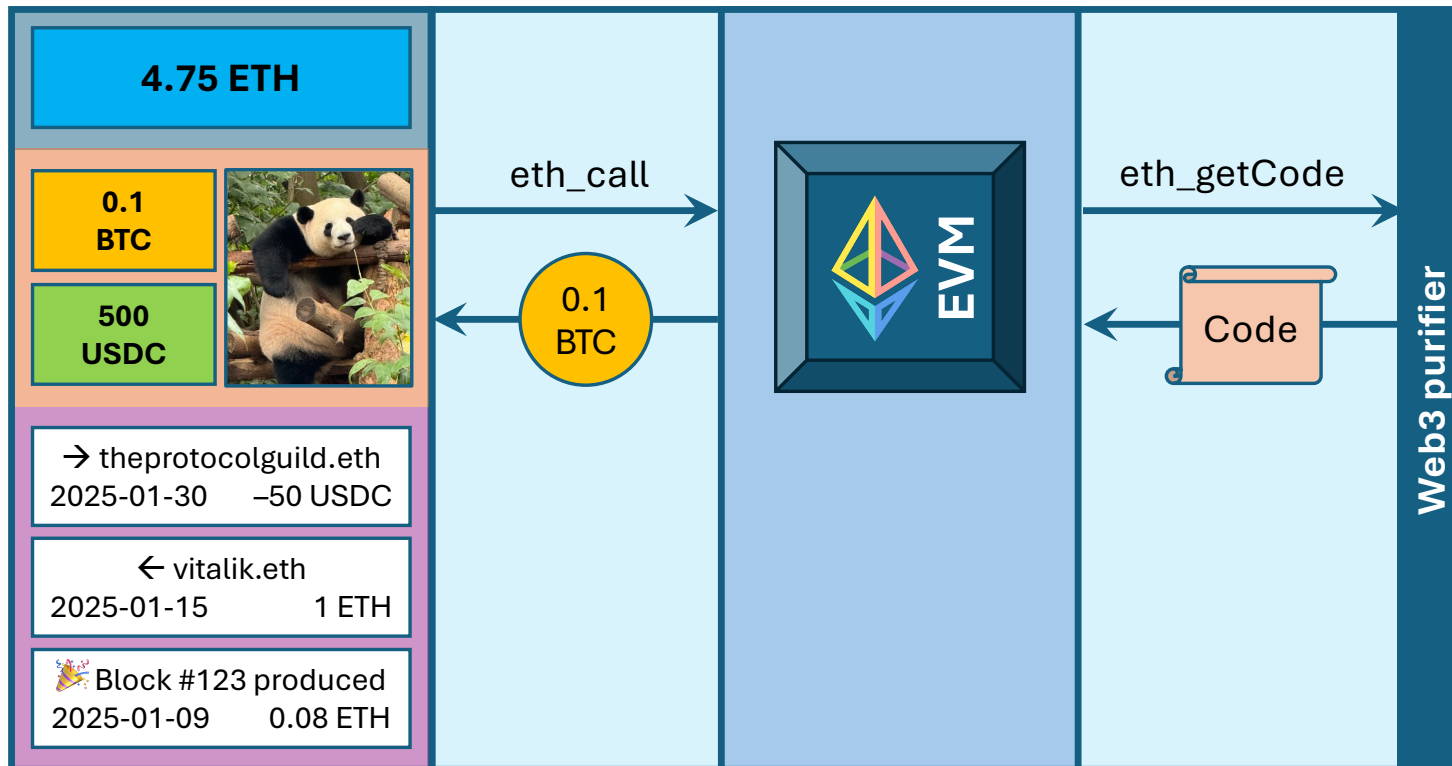
# Token balance



```
contract EIP20Interface {  
    // Returns the account balance  
    // of another account with address `_owner`.  
    function balanceOf(  
        address _owner  
    ) public view returns (  
        uint256 balance  
    );  
}
```

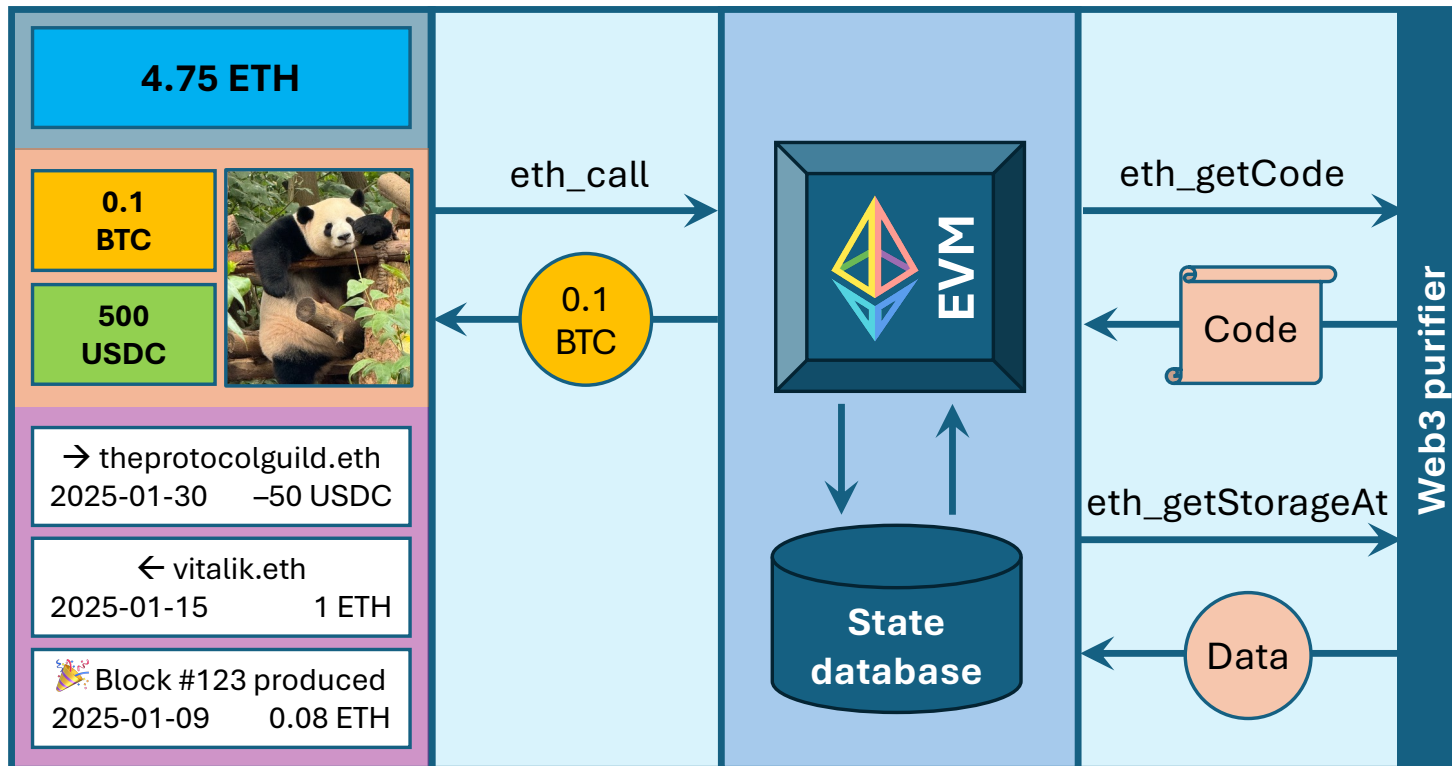


# Token balance



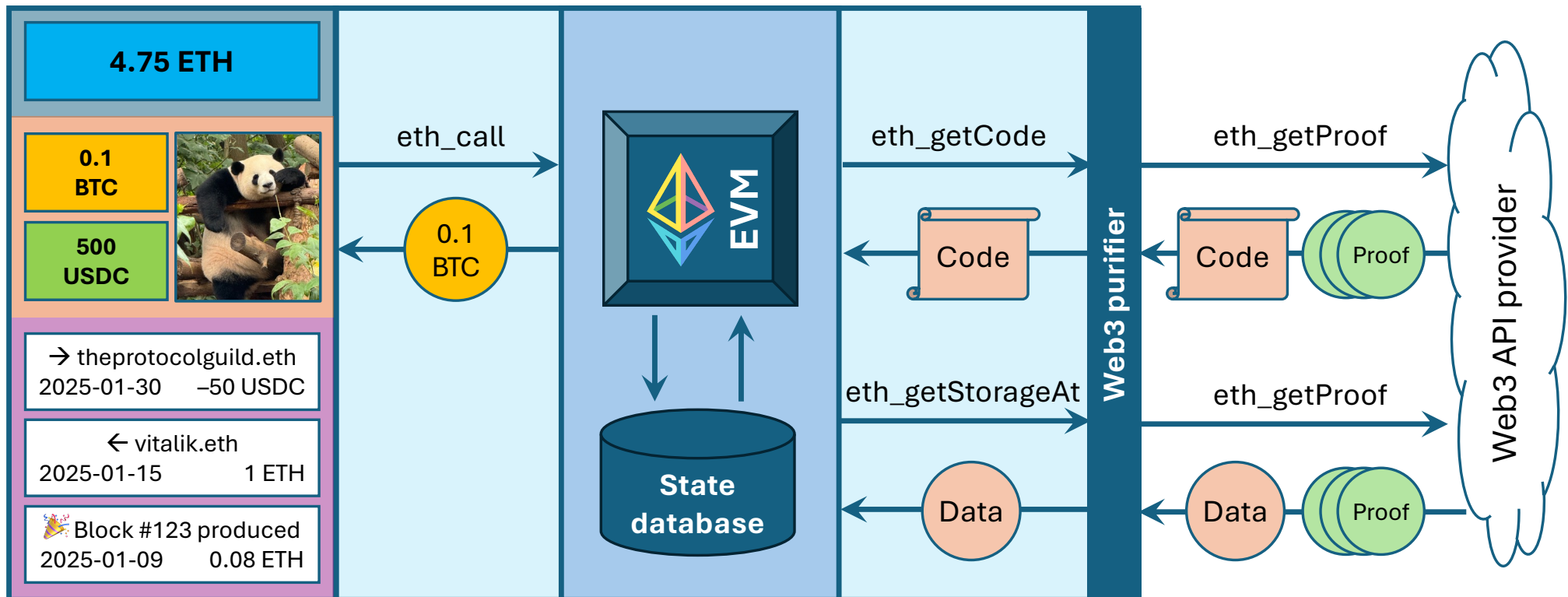


# Token balance



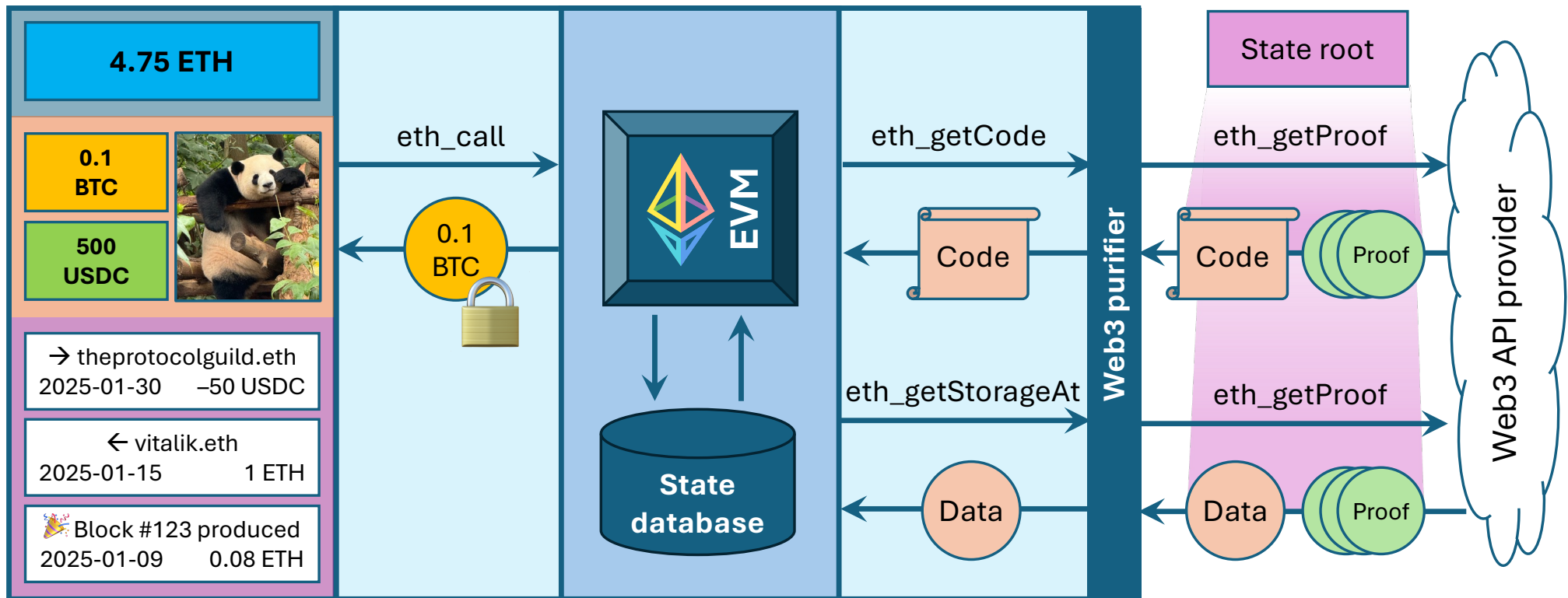


# Token balance





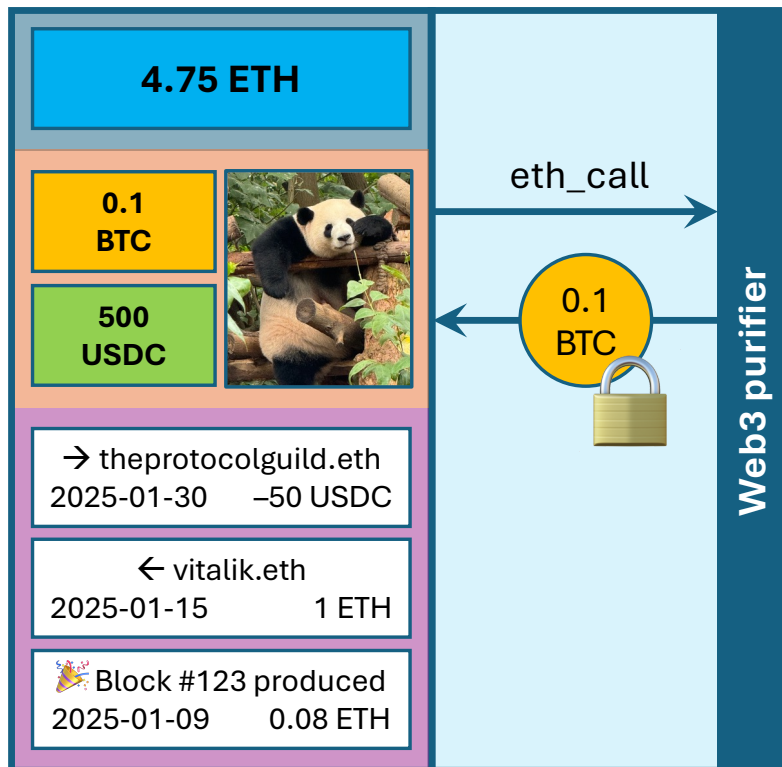
# Token balance







# Token balance



✓ ETH balance

✓ Tokens / NFTs

? History

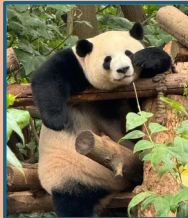
# History



4.75 ETH


0.1  
BTC

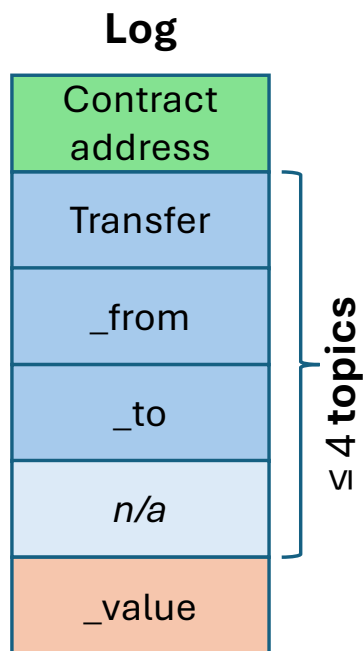
500  
USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH



```
contract EIP20Interface {  
    // Triggers when tokens are transferred,  
    // including zero value transfers.  
    event Transfer(  
        address indexed _from,  
        address indexed _to,  
        uint256 _value  
    );  
}
```

≤ 3 indexed arguments total

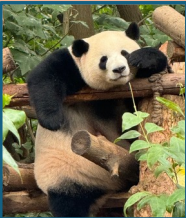


# Bloom filter

4.75 ETH


0.1 BTC

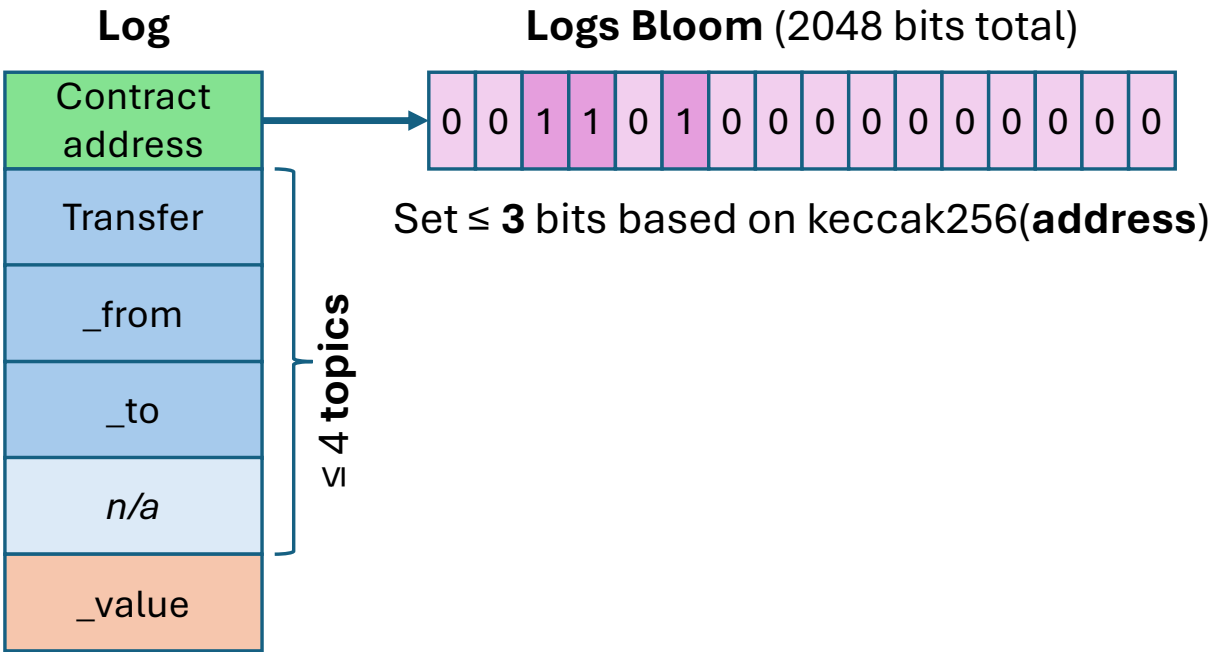
500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH



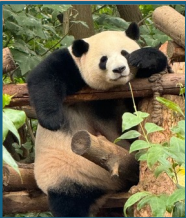


# Bloom filter

4.75 ETH


0.1 BTC

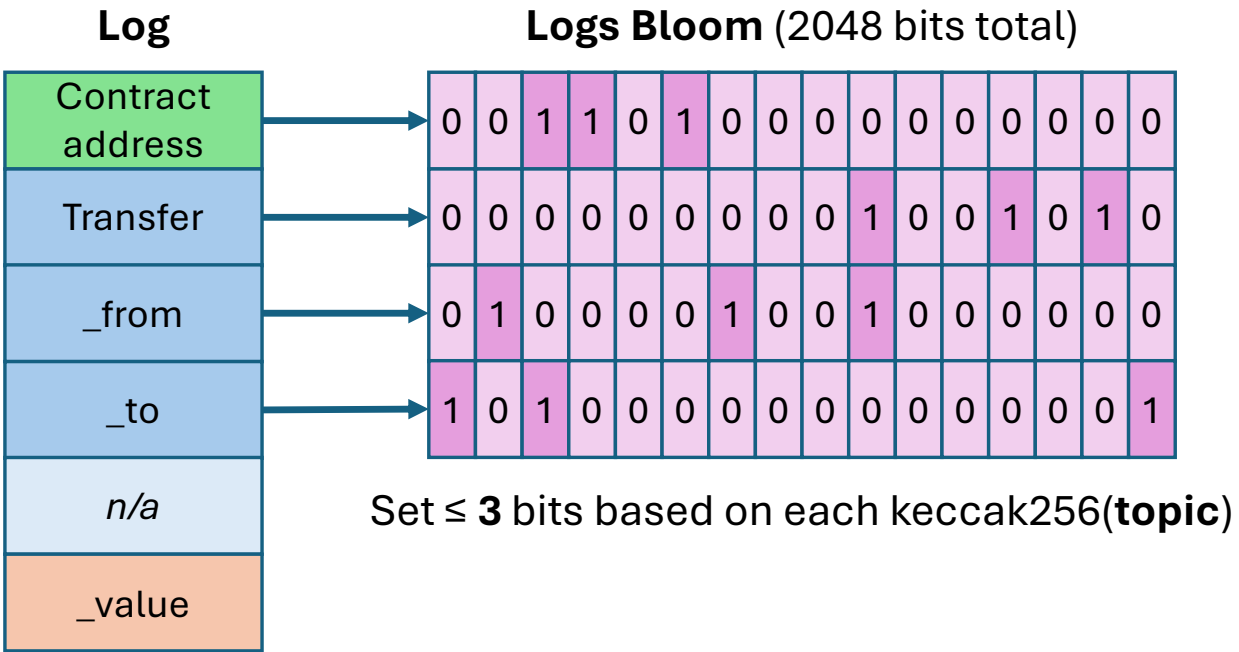
500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH



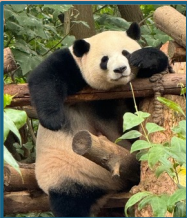


# Bloom filter

4.75 ETH


0.1 BTC

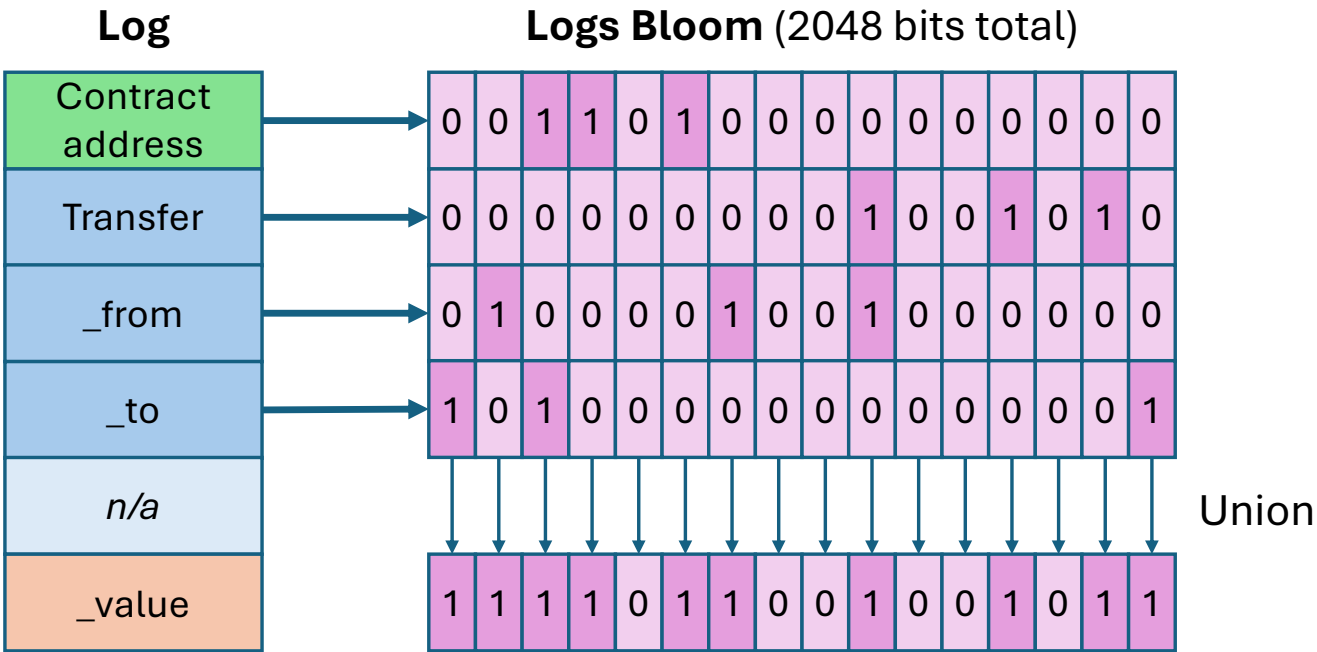
500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH



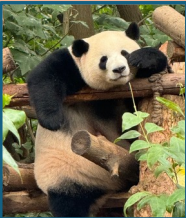


# Bloom filter

4.75 ETH


0.1 BTC

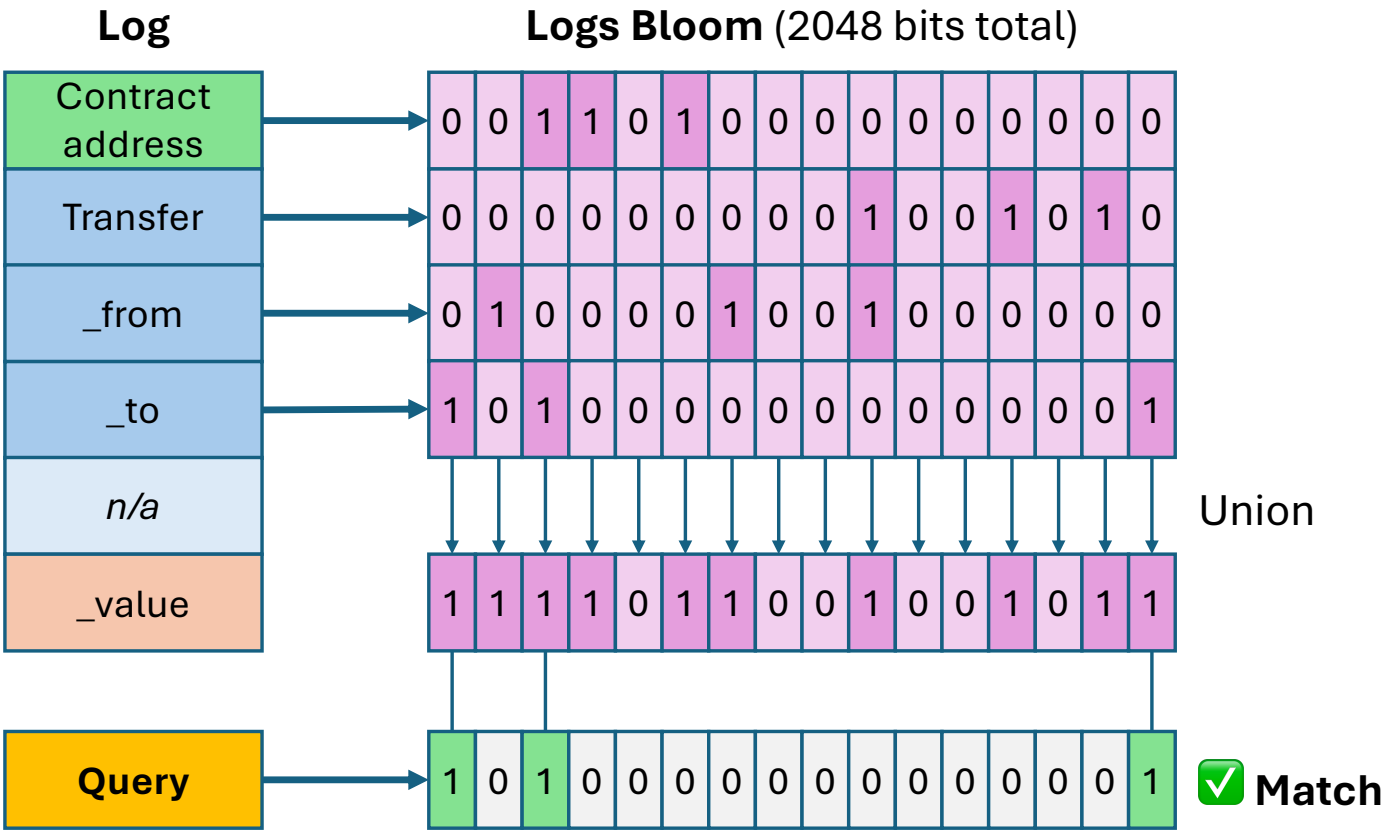
500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH



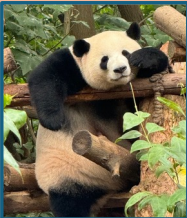


# Bloom filter

4.75 ETH


0.1 BTC

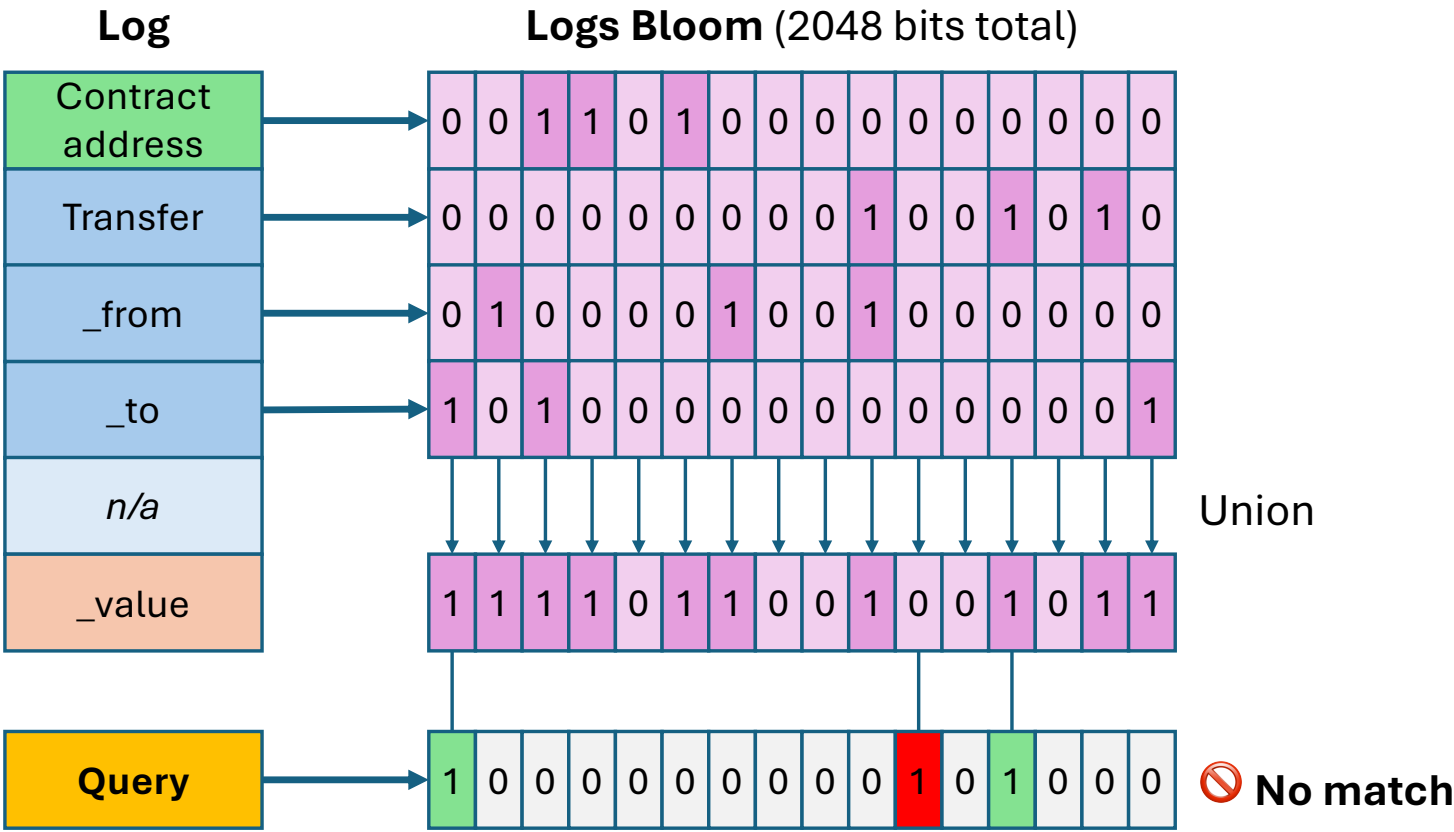
500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15       1 ETH

 Block #123 produced  
2025-01-09       0.08 ETH



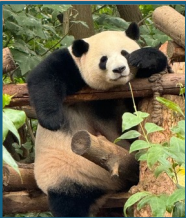


# Bloom filter

4.75 ETH


0.1 BTC

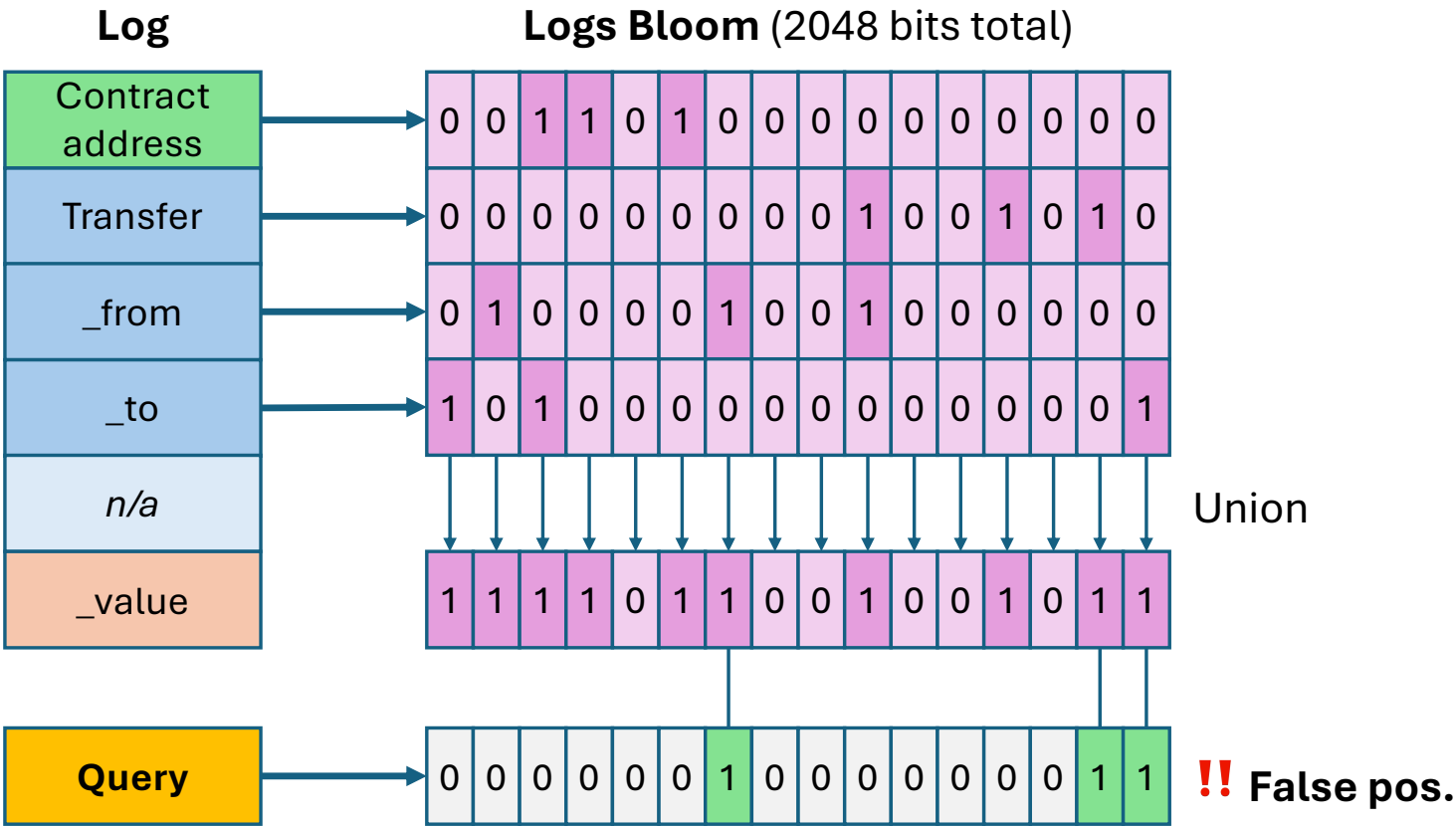
500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH





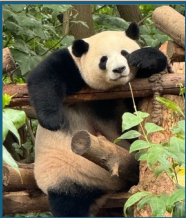


# Bloom filter

4.75 ETH


0.1 BTC

500 USDC



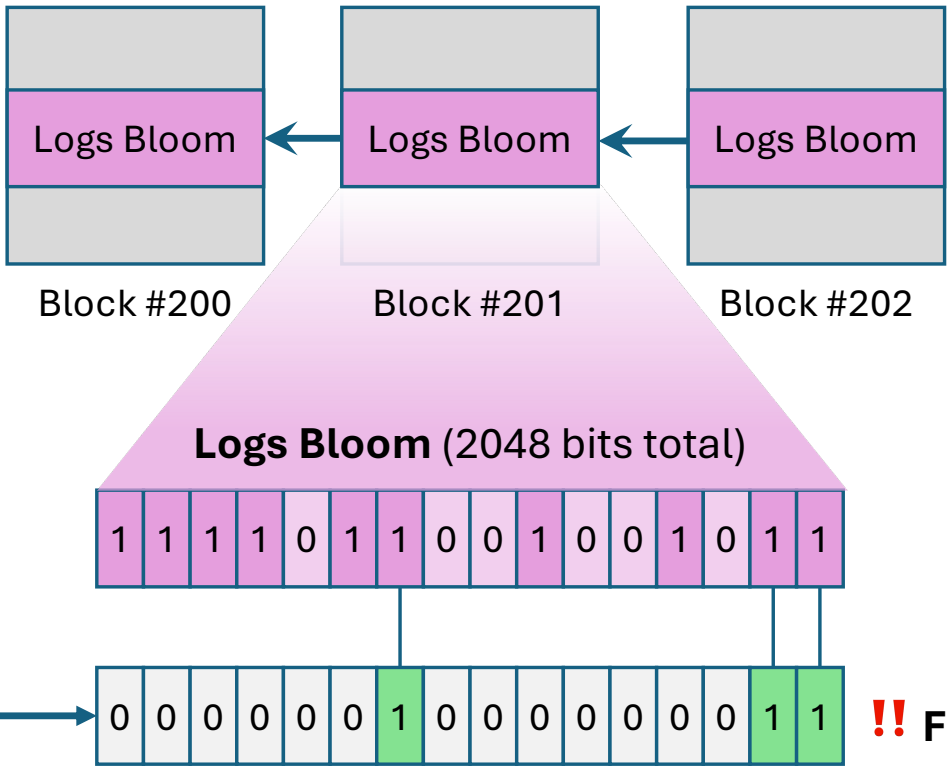
→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH

Log
Contract address
Transfer
_from
_to
n/a
_value

Mainnet: > 1000 addresses and topics per block



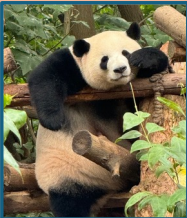


# EIP-7745: Two dimensional log filter

4.75 ETH


0.1 BTC

500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH

Log	
Contract address	
Transfer	
_from	
_to	
n/a	
_value	

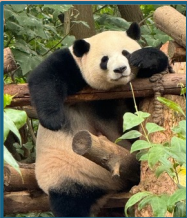


# EIP-7745: Two dimensional log filter

4.75 ETH


0.1 BTC

500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH

Log	Global index
Contract address	#1
Transfer	#2
_from	#3
_to	#4
n/a	
_value	

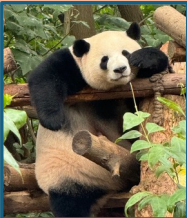


# EIP-7745: Two dimensional log filter

4.75 ETH


0.1 BTC

500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

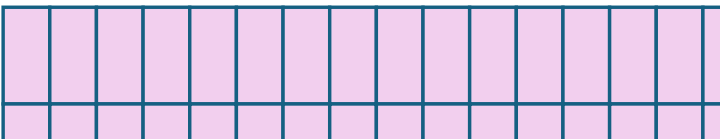
 Block #123 produced  
2025-01-09        0.08 ETH

Log value	Global index
Contract address	#1
Transfer	#2
_from	#3
_to	#4



Log value	Global index
Contract address	#1
Transfer	#2
_from	#3
_to	#4

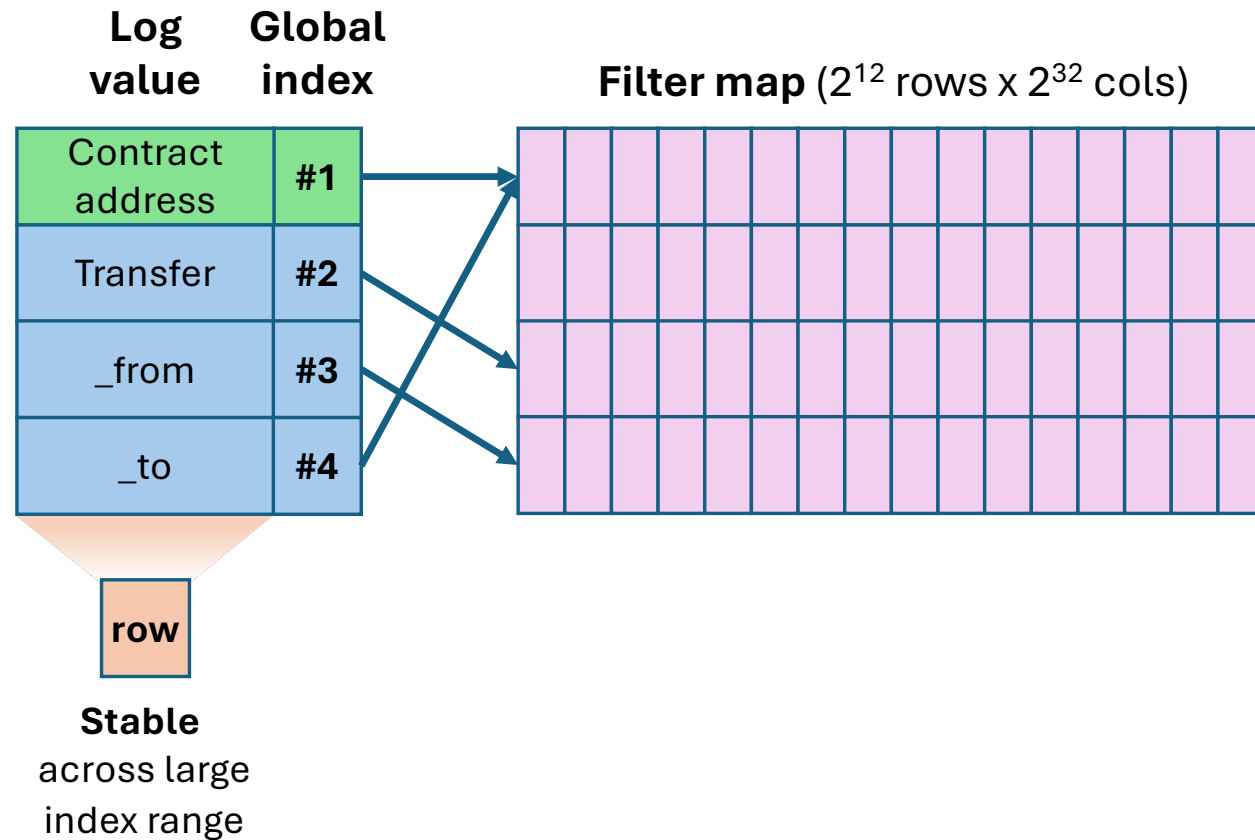
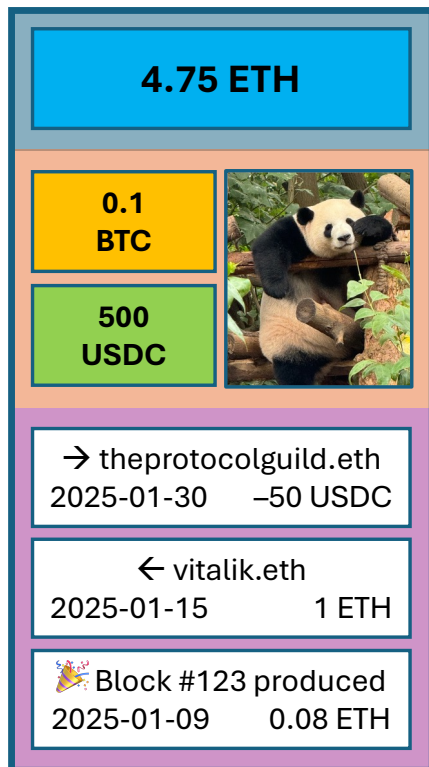
**Filter map ( $2^{12}$  rows x  $2^{32}$  cols)**



The diagram consists of a grid of 4 rows and 16 columns of light purple squares. Each square is outlined with a dark blue border. The grid is intended to represent a filter map with dimensions of  $2^{12}$  rows by  $2^{32}$  columns.



# EIP-7745: Two dimensional log filter





# EIP-7745: Two dimensional log filter

4.75 ETH

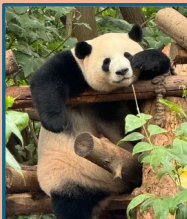
0.1 BTC

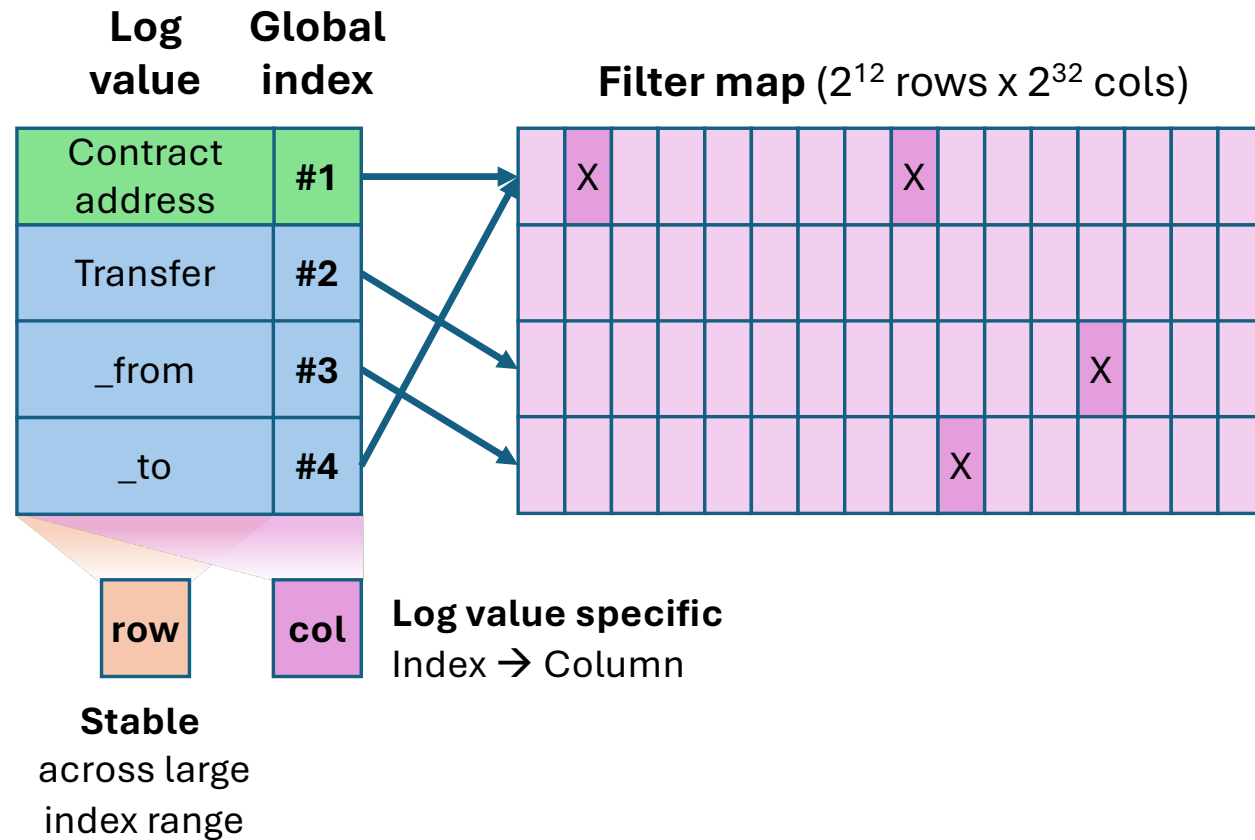
500 USDC

→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

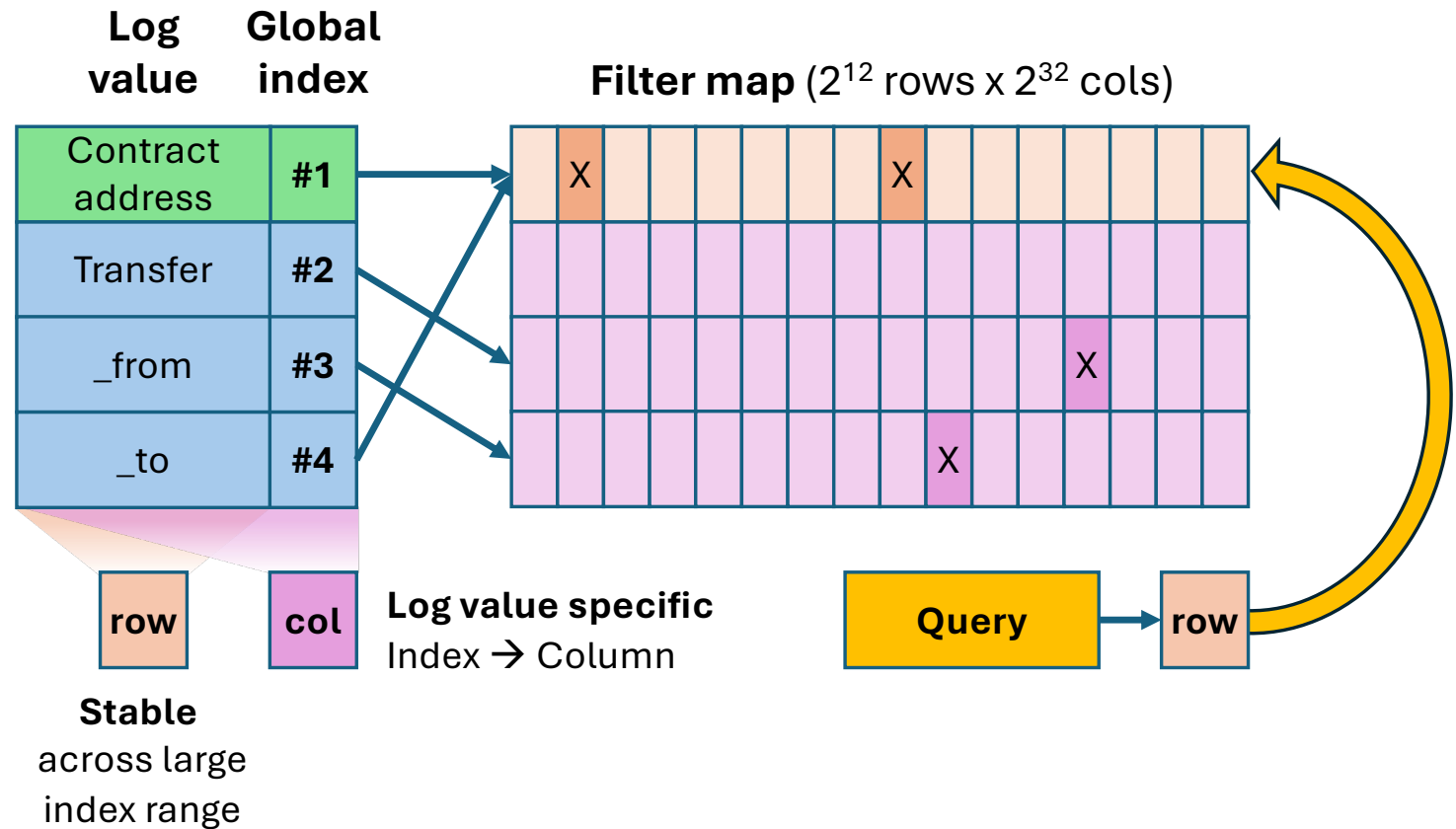
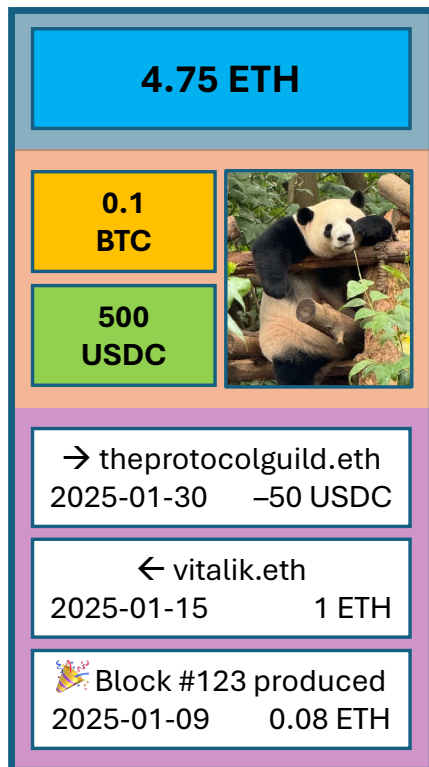
🎉 Block #123 produced  
2025-01-09        0.08 ETH







# EIP-7745: Two dimensional log filter







# EIP-7745: Two dimensional log filter

4.75 ETH

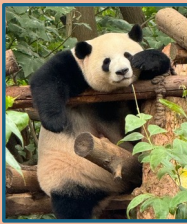
0.1 BTC

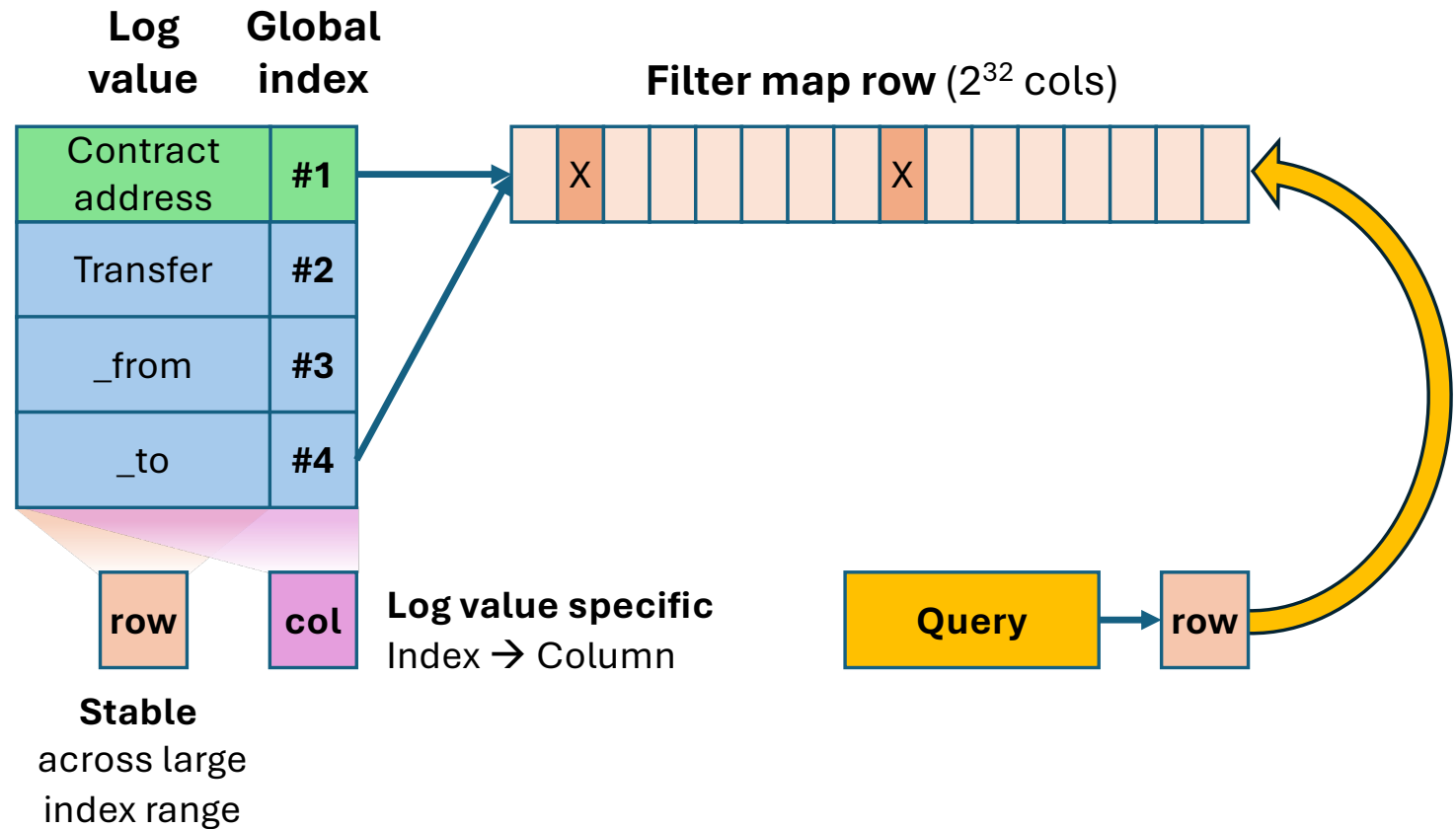
500 USDC

→ theprotocolguild.eth  
2025-01-30 -50 USDC

← vitalik.eth  
2025-01-15 1 ETH

🎉 Block #123 produced  
2025-01-09 0.08 ETH







# EIP-7745: Two dimensional log filter

4.75 ETH

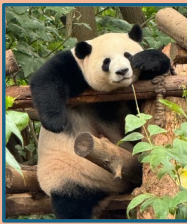
0.1 BTC

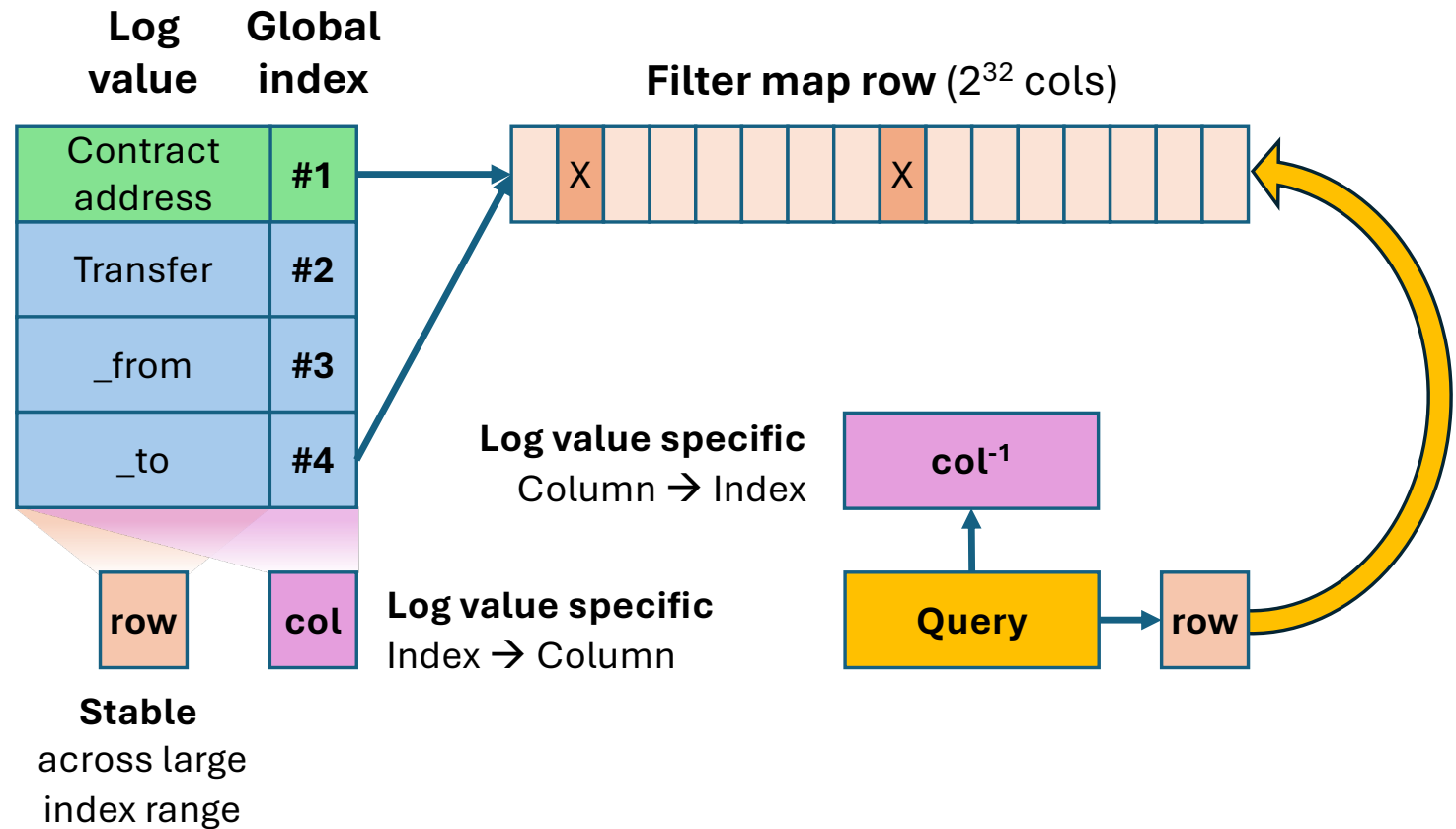
500 USDC

→ theprotocolguild.eth  
2025-01-30 -50 USDC

← vitalik.eth  
2025-01-15 1 ETH

🎉 Block #123 produced  
2025-01-09 0.08 ETH







# EIP-7745: Two dimensional log filter

4.75 ETH

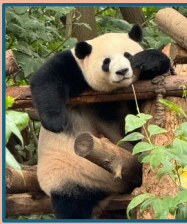
0.1 BTC

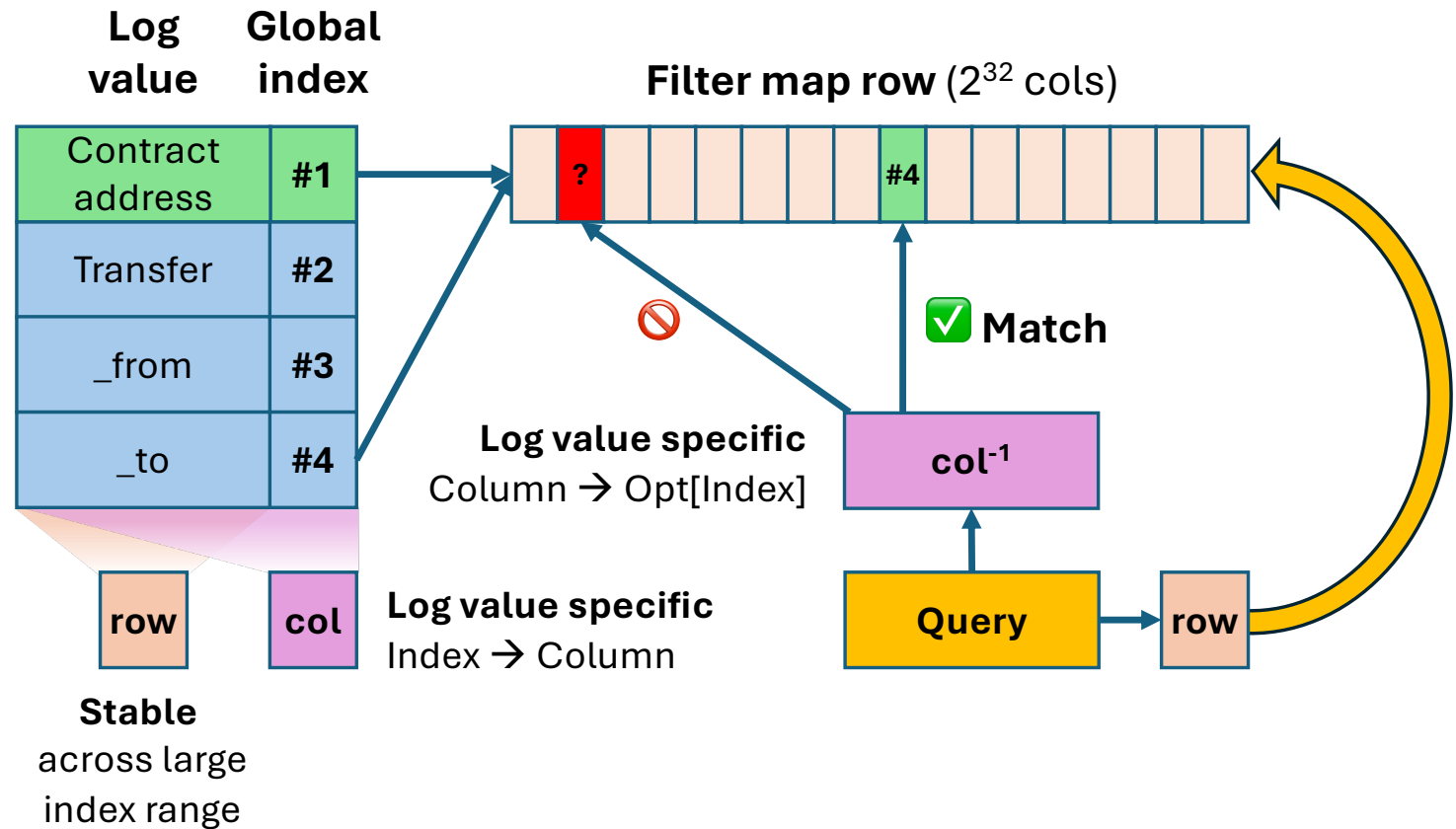
500 USDC

→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

🎉 Block #123 produced  
2025-01-09        0.08 ETH





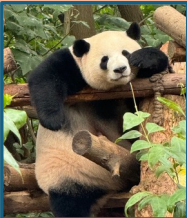


# EIP-7745: Two dimensional log filter

4.75 ETH

0.1 BTC

500 USDC



→ theprotocolguild.eth  
2025-01-30 -50 USDC

← vitalik.eth  
2025-01-15 1 ETH

🎉 Block #123 produced  
2025-01-09 0.08 ETH

Log value	Global index	
Contract address	#1	
Transfer	#2	
_from	#3	
_to	#4	

Filter map ( $2^{12}$  rows x  $2^{32}$  cols)

Fresh **sparse** filter map every  $\leq 2^{16}$  marks

✌️ False positives are **extremely rare**

Log value → Row transform **stable** across  $2^6$  maps

✌️ Efficient to fetch relevant rows

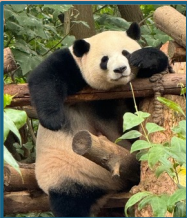


# EIP-7745: Two dimensional log filter

4.75 ETH


0.1 BTC

500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH

Log	Global index
Contract address	#1
Transfer	#2
_from	#3
_to	#4
n/a	
_value	

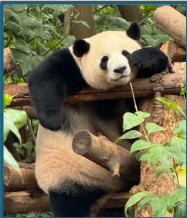


# EIP-7745: Two dimensional log filter

4.75 ETH


0.1 BTC

500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

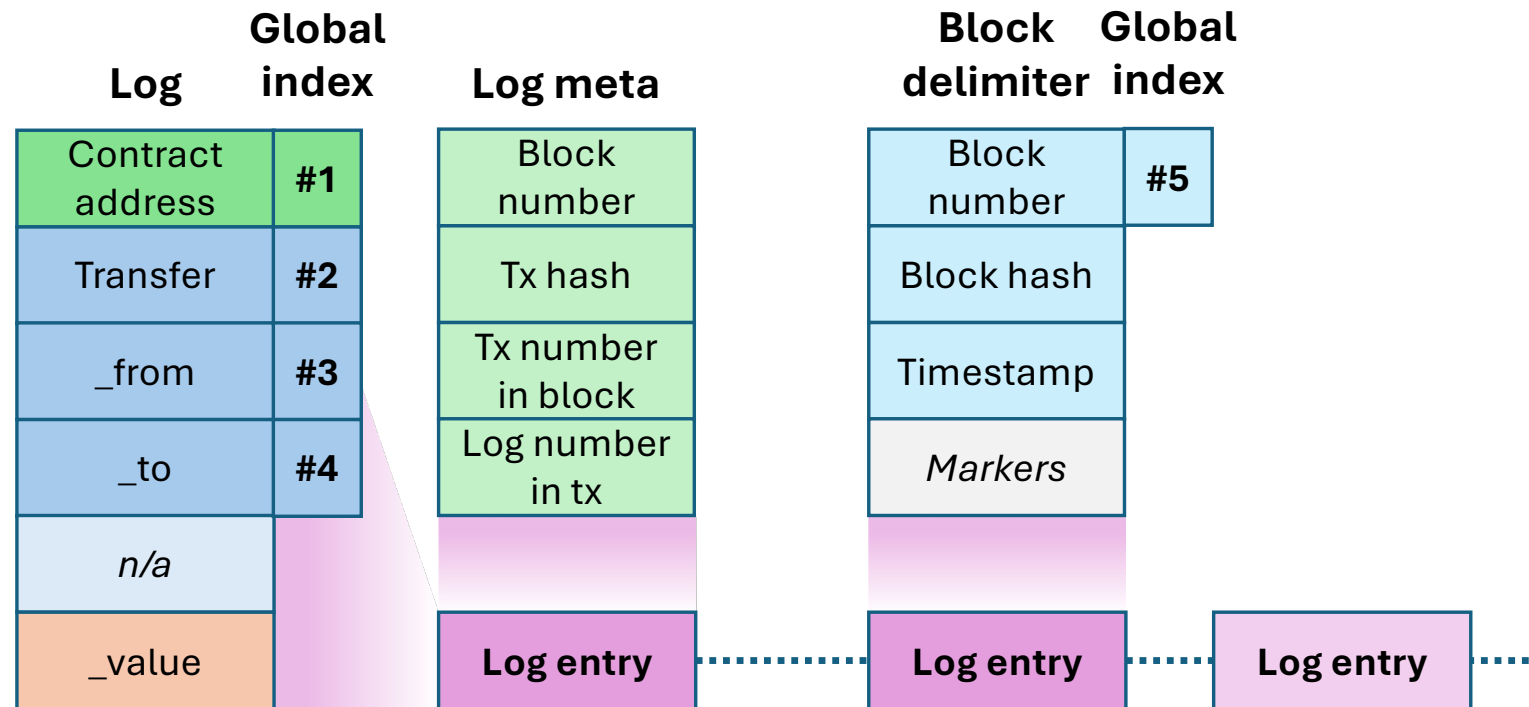
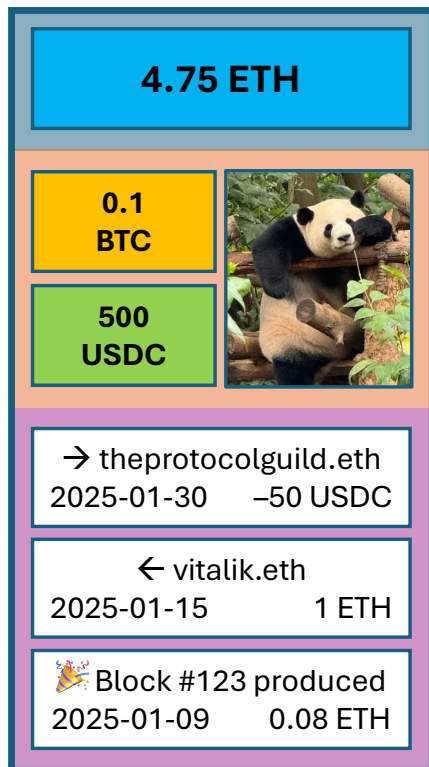
← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH

Log	Global index	Log metadata
Contract address	#1	Block number
Transfer	#2	Tx hash
_from	#3	Tx number in block
_to	#4	Log number in tx
n/a		
_value		Log entry



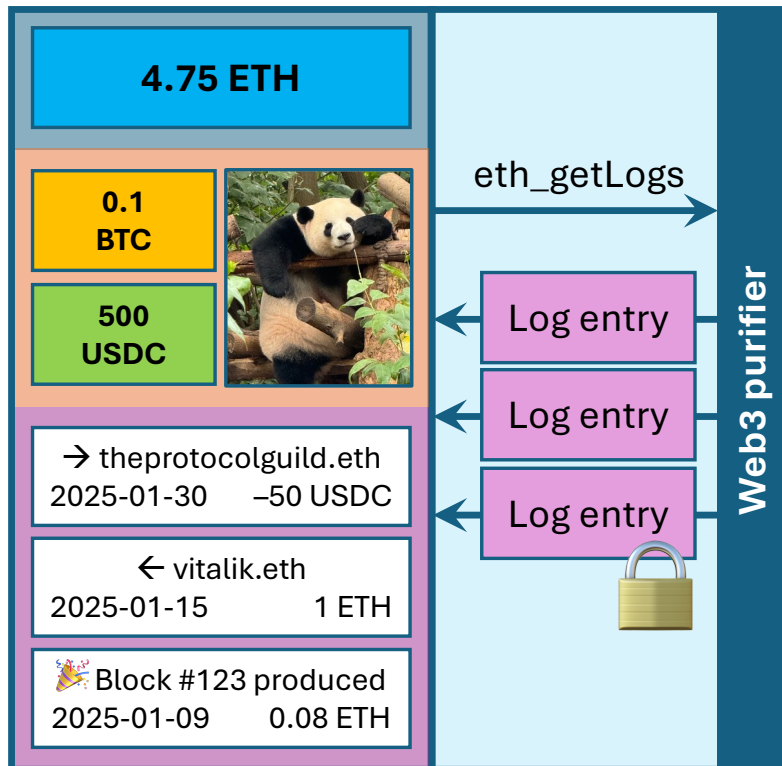
# EIP-7745: Two dimensional log filter



- 👉 Lookup each log **address**, **topic**, and **block** by global **index**
- 👉 Enumerate **all log entries** within a block **range**



# EIP-7745: Two dimensional log filter

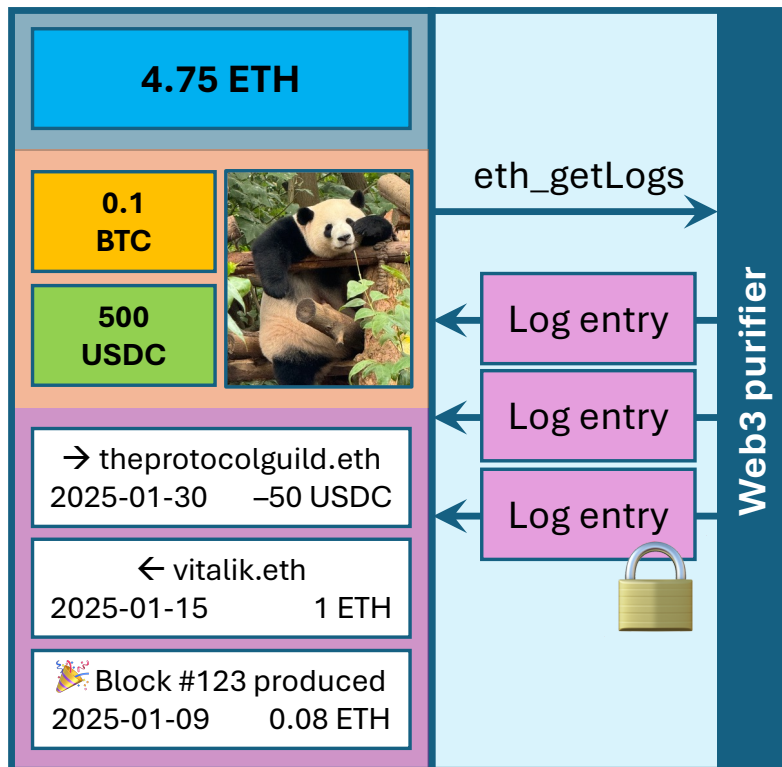


- ✓ ETH balance
- ✓ Tokens / NFTs
- ✓ History





# EIP-7745: Two dimensional log filter



- ✓ ETH balance
- ✓ Tokens / NFTs
- ✓ History
- ? ETH balance history

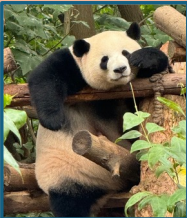


# EIP-7708: ETH transfers emit a log

4.75 ETH


0.1 BTC

500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH

System address	System address
Transfer	Fee
_from	_from
_to	<i>n/a</i>
<i>n/a</i>	<i>n/a</i>
_value	_value

## Transfer log

Transaction start

Nonzero-value *CALL*

Nonzero-value *SELFDESTRUCT*

## Fee log

Transaction end

- 👉 ETH transfers from smart contracts logged
- 👉 **Complete history** for users

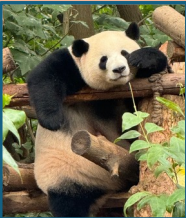


# EIP-7799: System logs

4.75 ETH


0.1 BTC

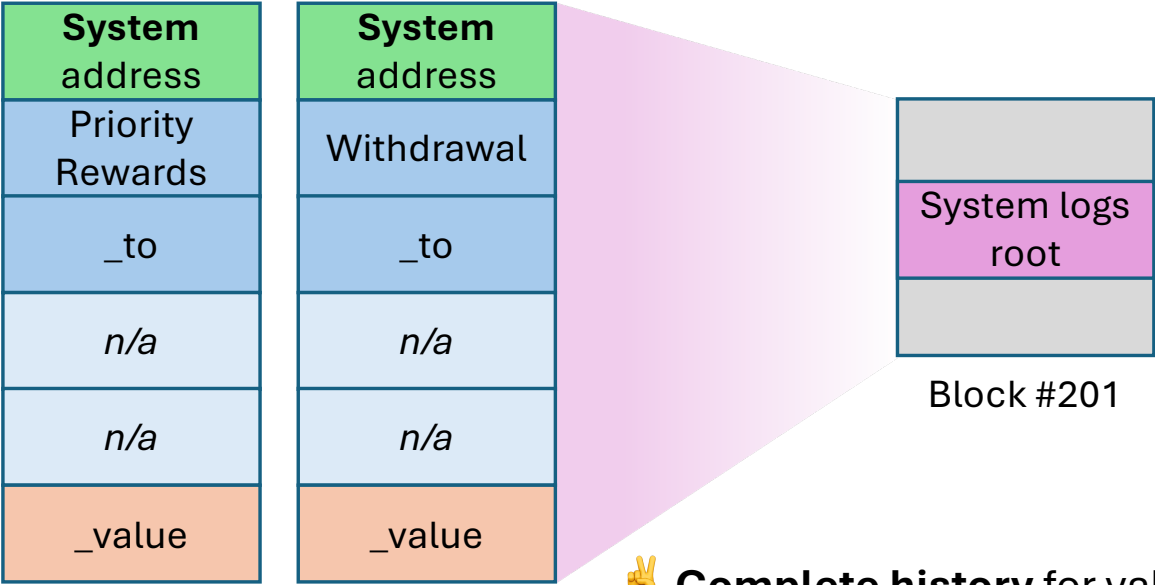
500 USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

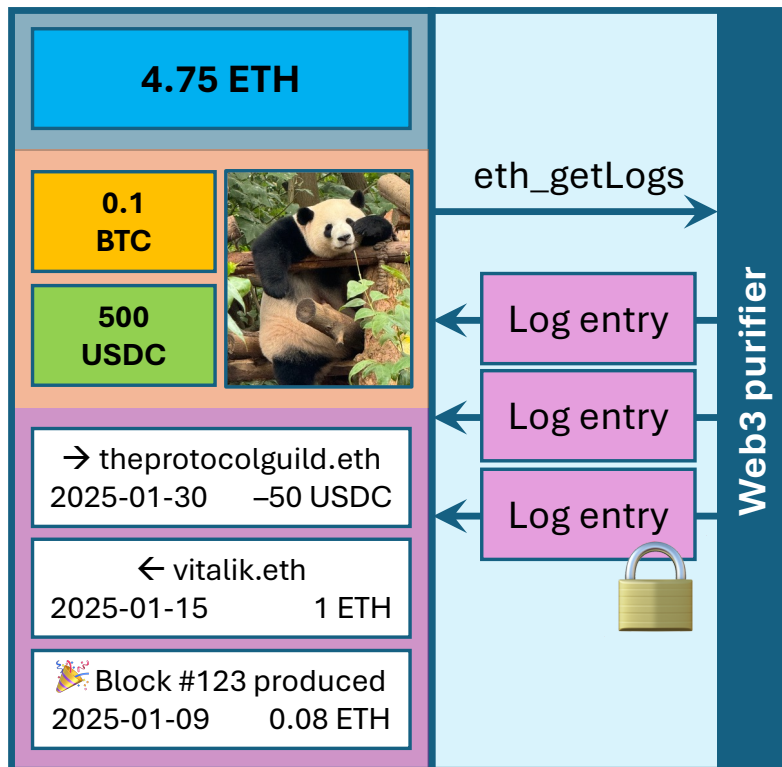
← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH



👉 Complete history for validator operators

# Purified web3



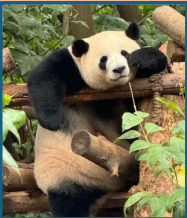
- ✓ ETH balance
- ✓ Tokens / NFTs
- ✓ History

# Purified web3

4.75 ETH


0.1  
BTC

500  
USDC



→ theprotocolguild.eth  
2025-01-30    -50 USDC

← vitalik.eth  
2025-01-15        1 ETH

 Block #123 produced  
2025-01-09        0.08 ETH

Devnet available 🔥  
Nimbus + EthereumJS backend  
Helios web3 purifier

Buidling guides  
Verifying wallets  
Web3 purifiers

Developer info  
Additional EIPs for efficiency  
Kurtosis network config



<https://purified-web3.box>