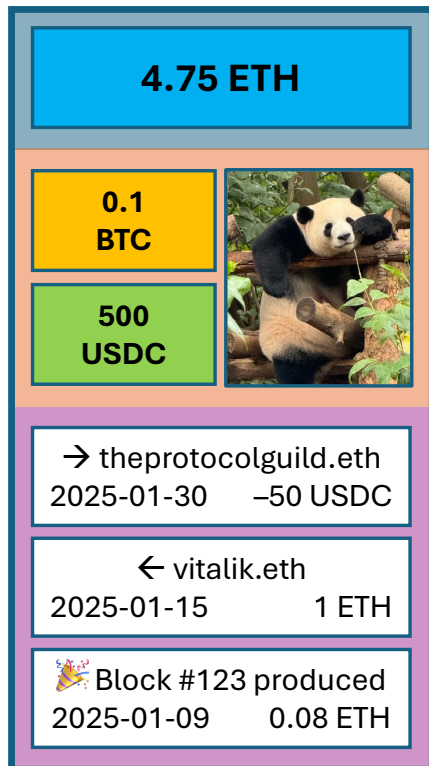


Trust-minimized wallets with purified web3

Etan Kissling, Nimbus, IFT

30 Jan 2025 / EthereumZuri.ch

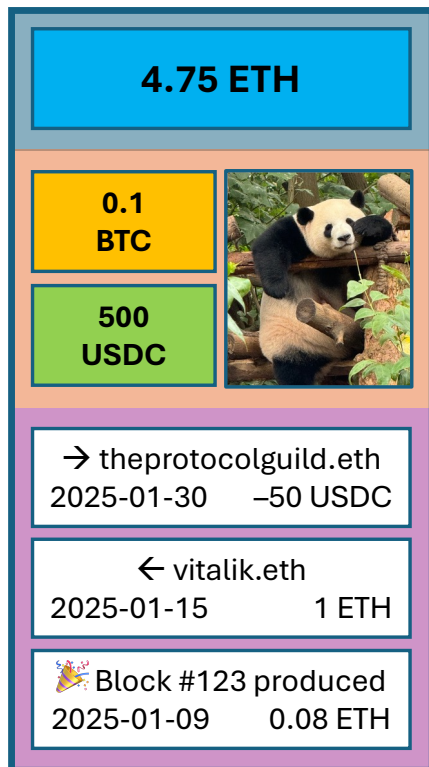
Wallet



Mobile app

Browser extension

Wallet security



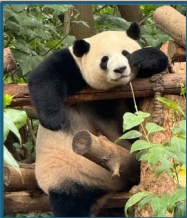
Mobile app

Browser extension

+ Hardware wallet (optional)



Wallet security

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	

Mobile app

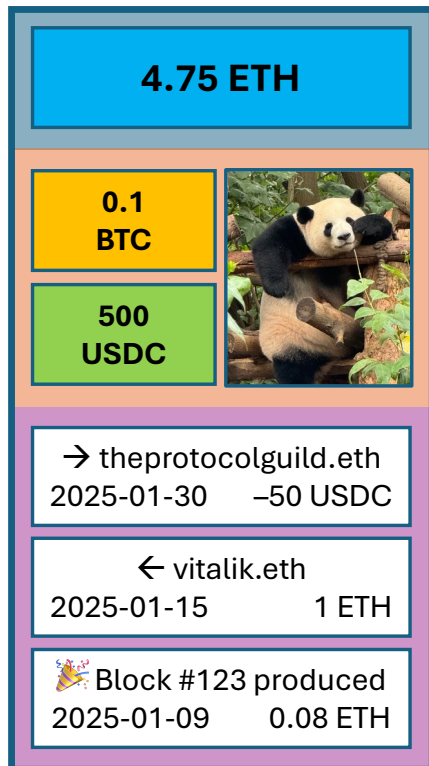
Browser extension



Secure transaction signing



Wallet security



? ETH balance

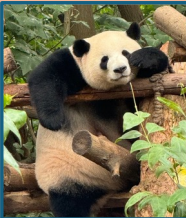
? Tokens / NFTs

? History

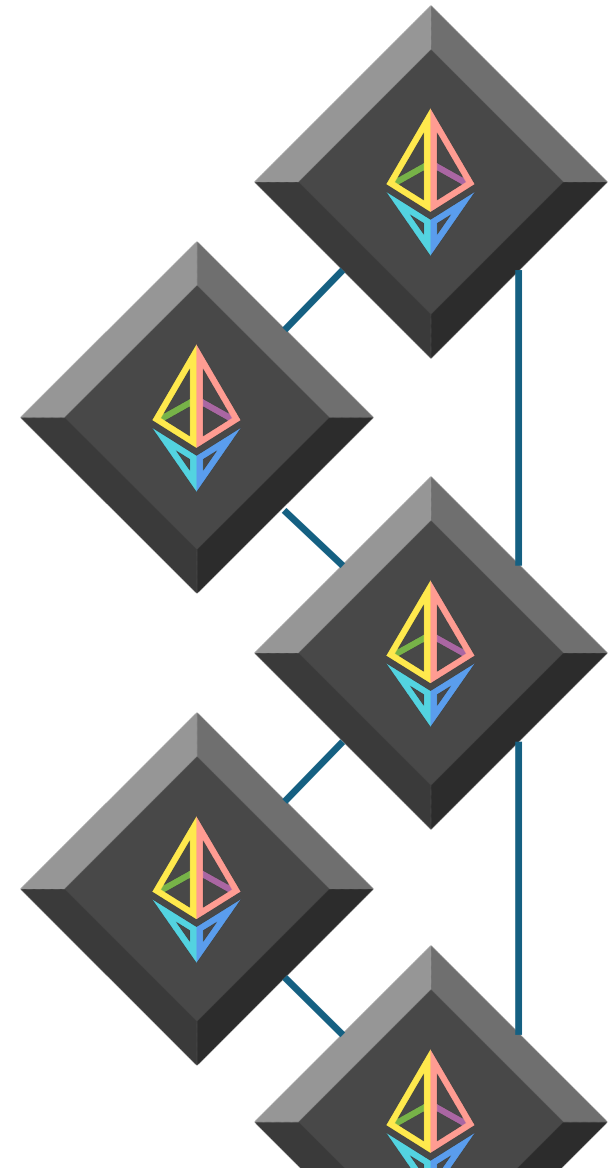
🔒 Secure transaction signing



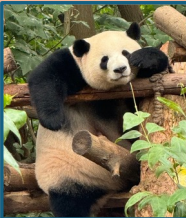
Wallet (obtaining data)

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



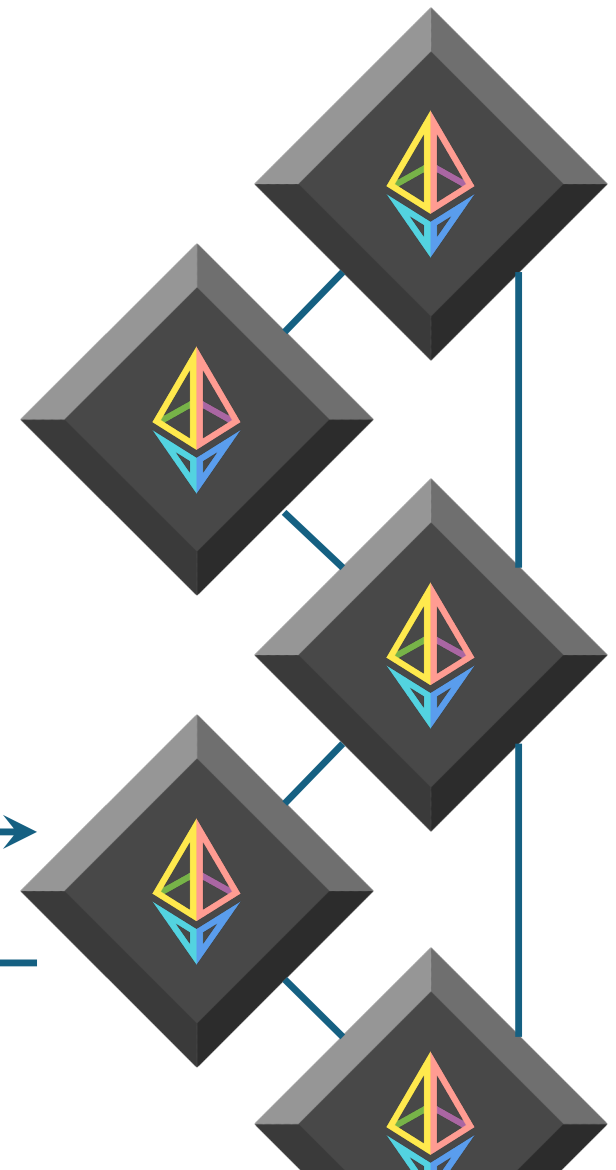
Wallet (obtaining data)

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	

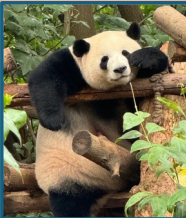
- ? ETH balance
- ? Tokens / NFTs
- ? History

eth_getBalance

4.75 ETH



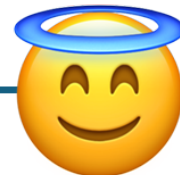
Wallet (obtaining data)

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	

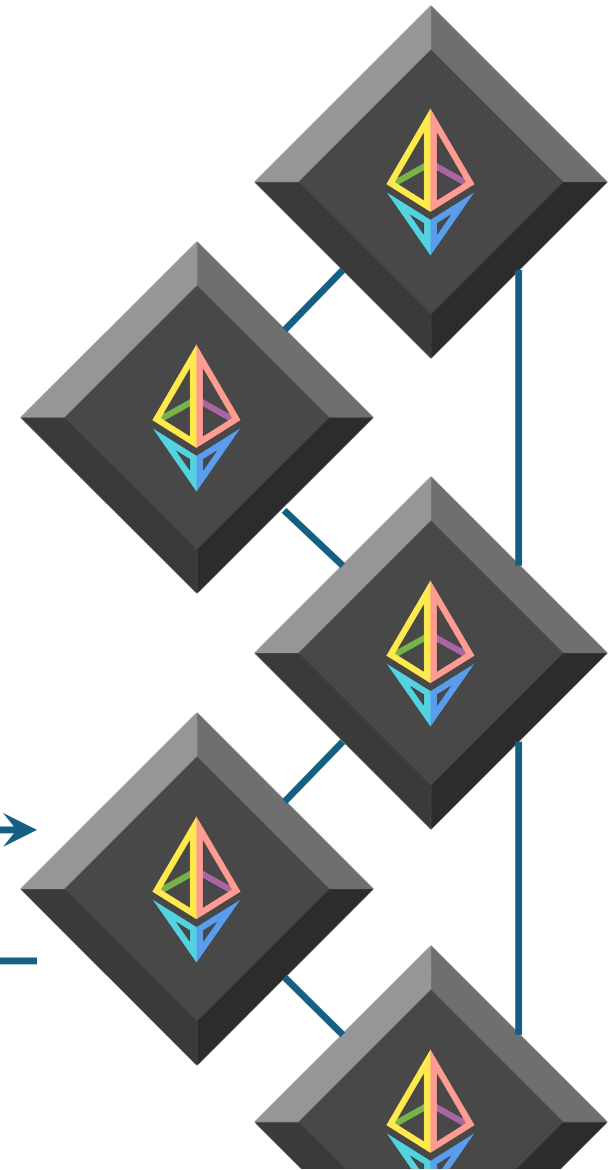
- ? ETH balance
- ? Tokens / NFTs
- ? History

eth_getBalance

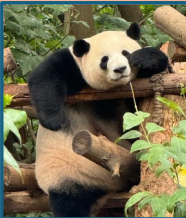
4.75 ETH



“trust me bro”



Wallet (run your own node)

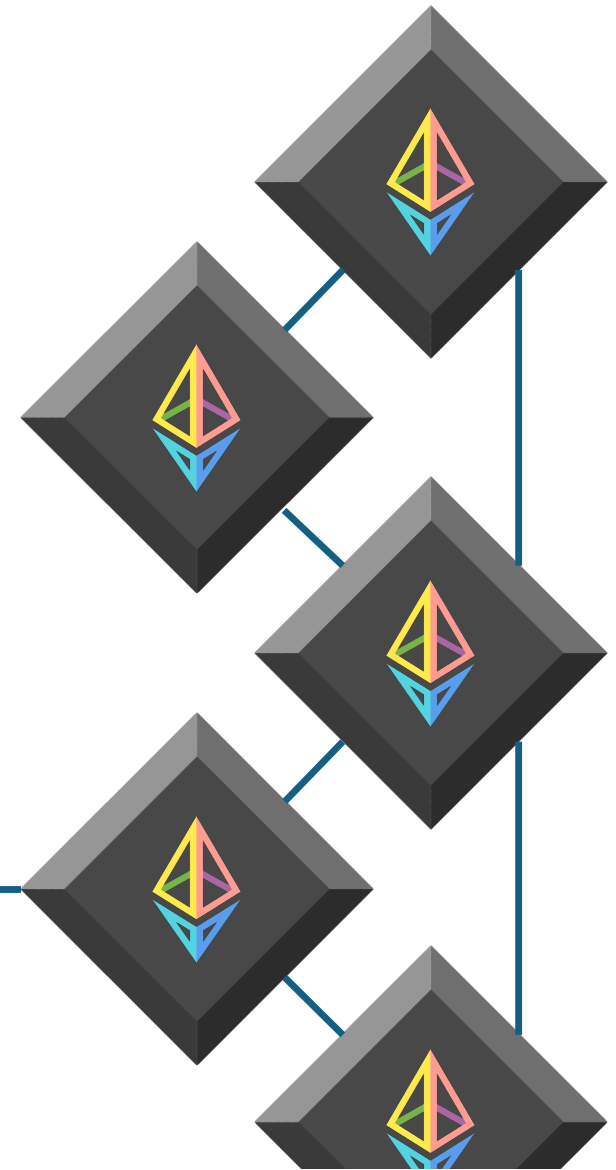
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	

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

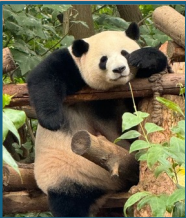
4 core CPU
16 GB RAM
2 TB SSD

eth_getBalance

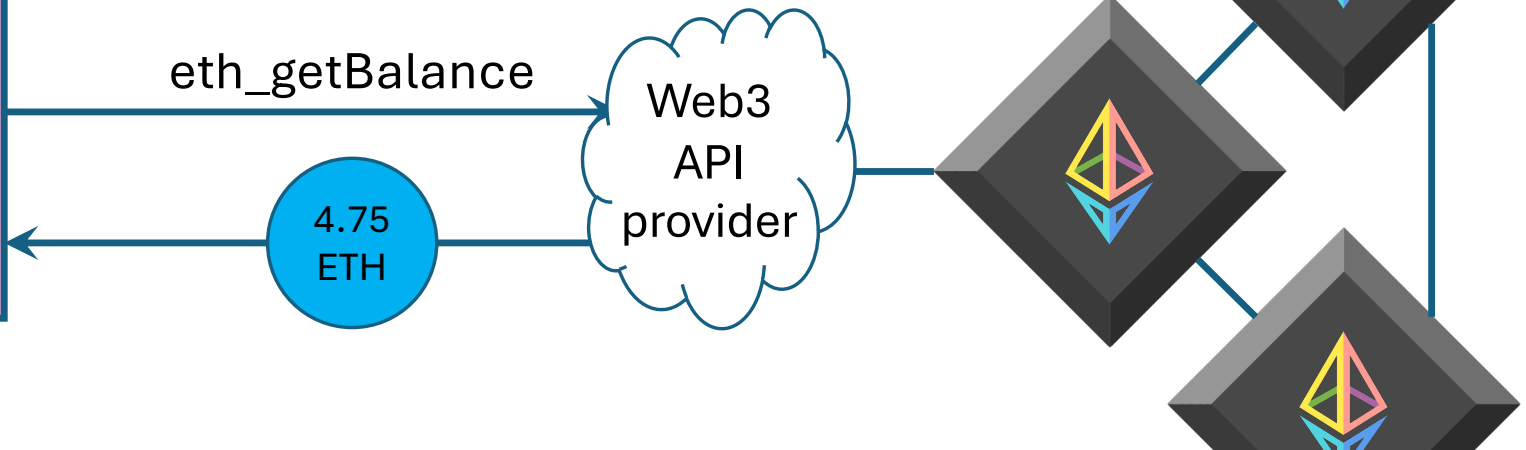
4.75 ETH



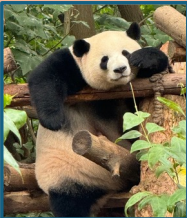
Wallet (RPC provider)

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	

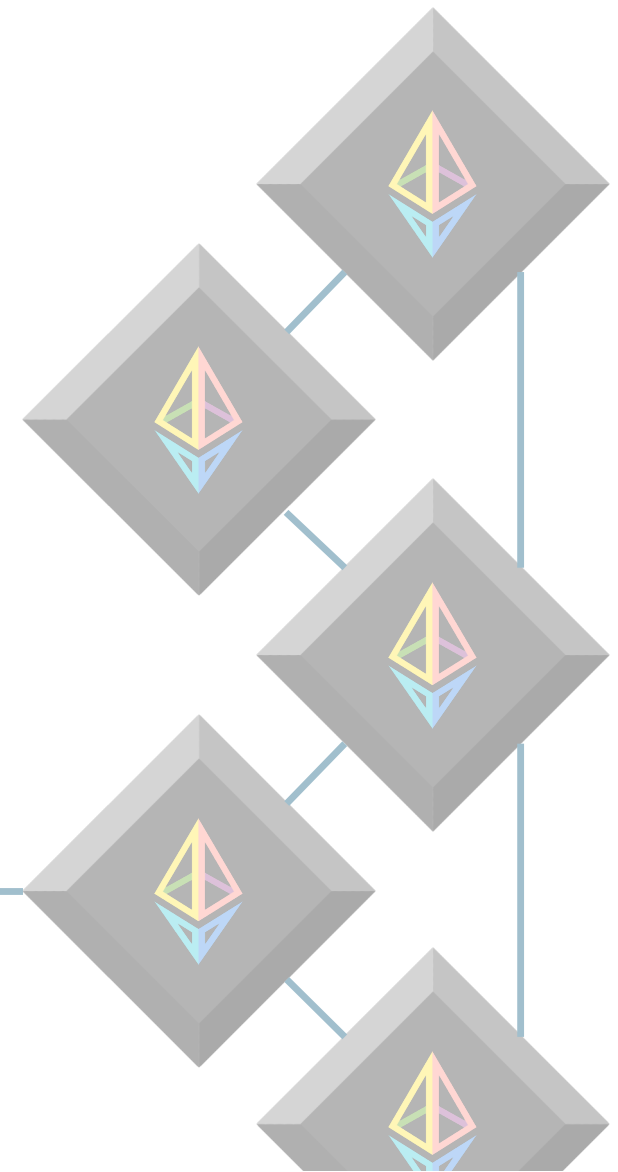
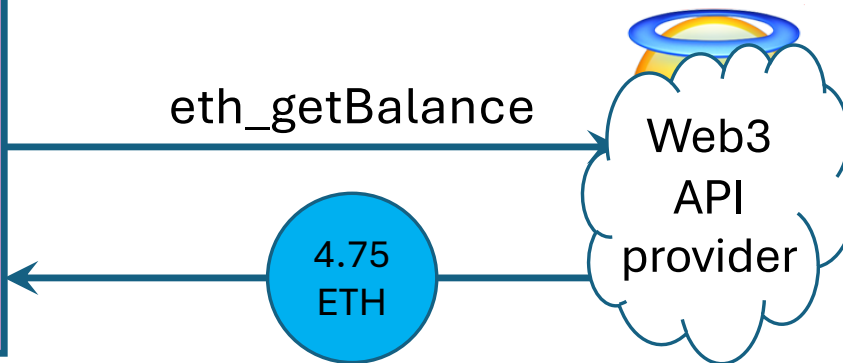
- ? ETH balance
- ? Tokens / NFTs
- ? History



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



Decentralization?

4.75 ETH

0.1 BTC

500 USDC

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

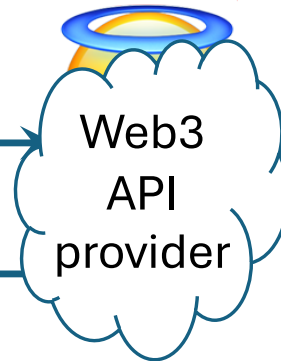
← vitalik.eth
2025-01-15 1 ETH

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

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

eth_getBalance

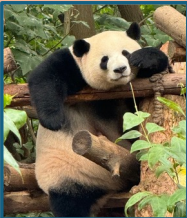
4.75 ETH



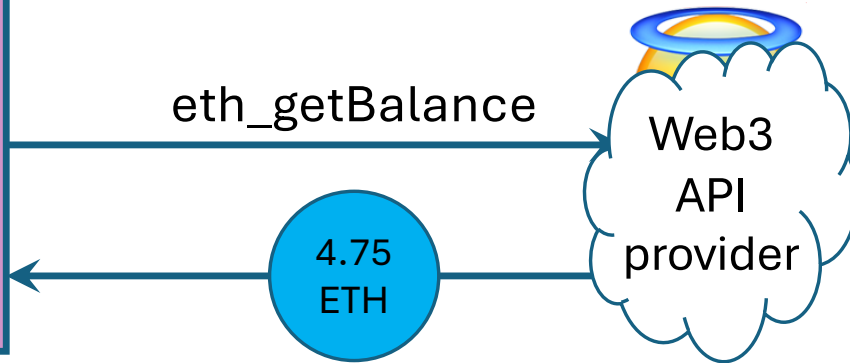
- ⚡ Downtimes
- ⚡ Security
- ⚡ Censorship
- ⚡ Privacy

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

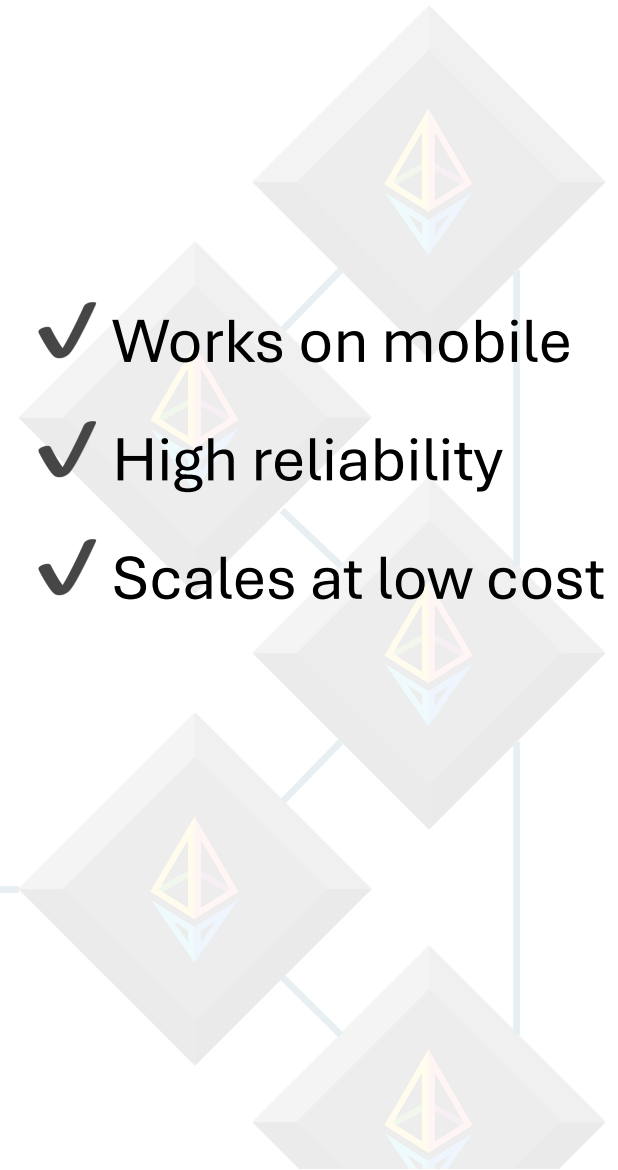
Decentralization?

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



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



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

✓ Works on mobile

✓ High reliability

✓ Scales at low cost

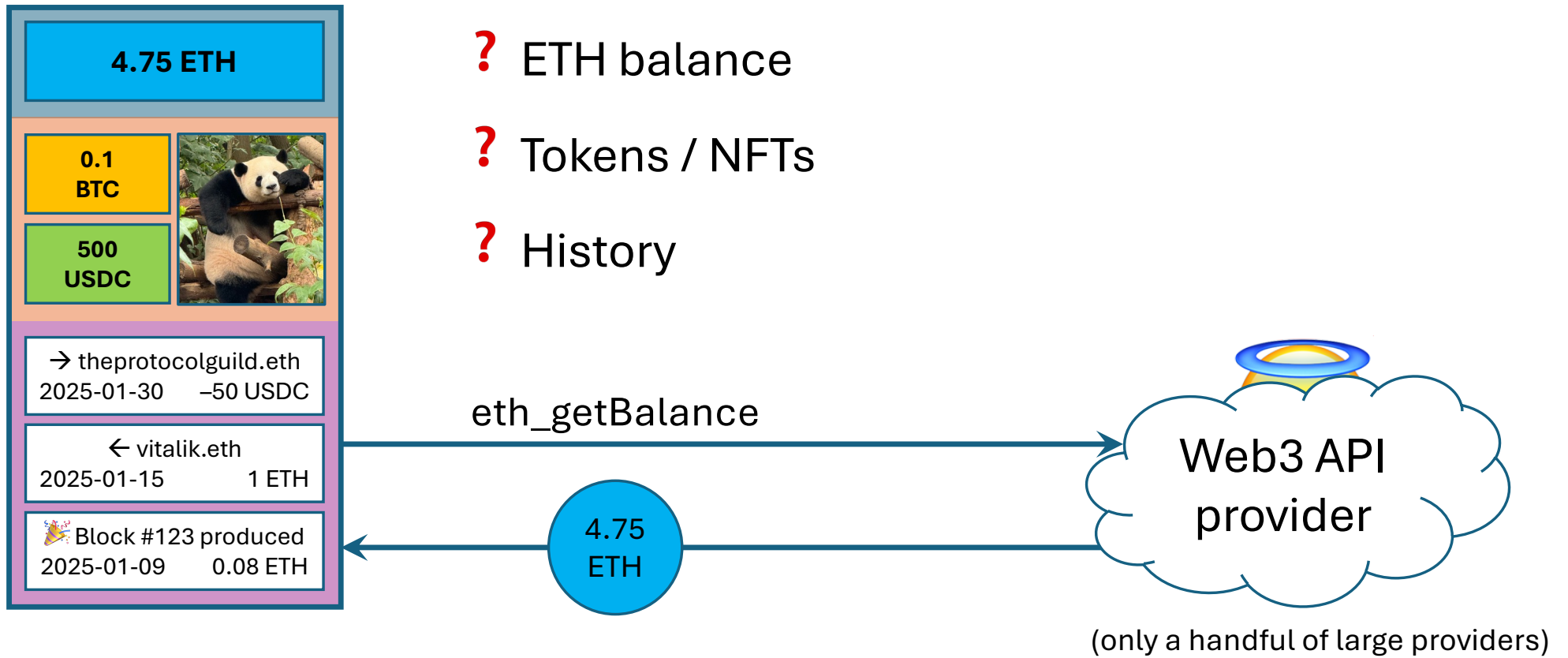
eth_getBalance

4.75 ETH

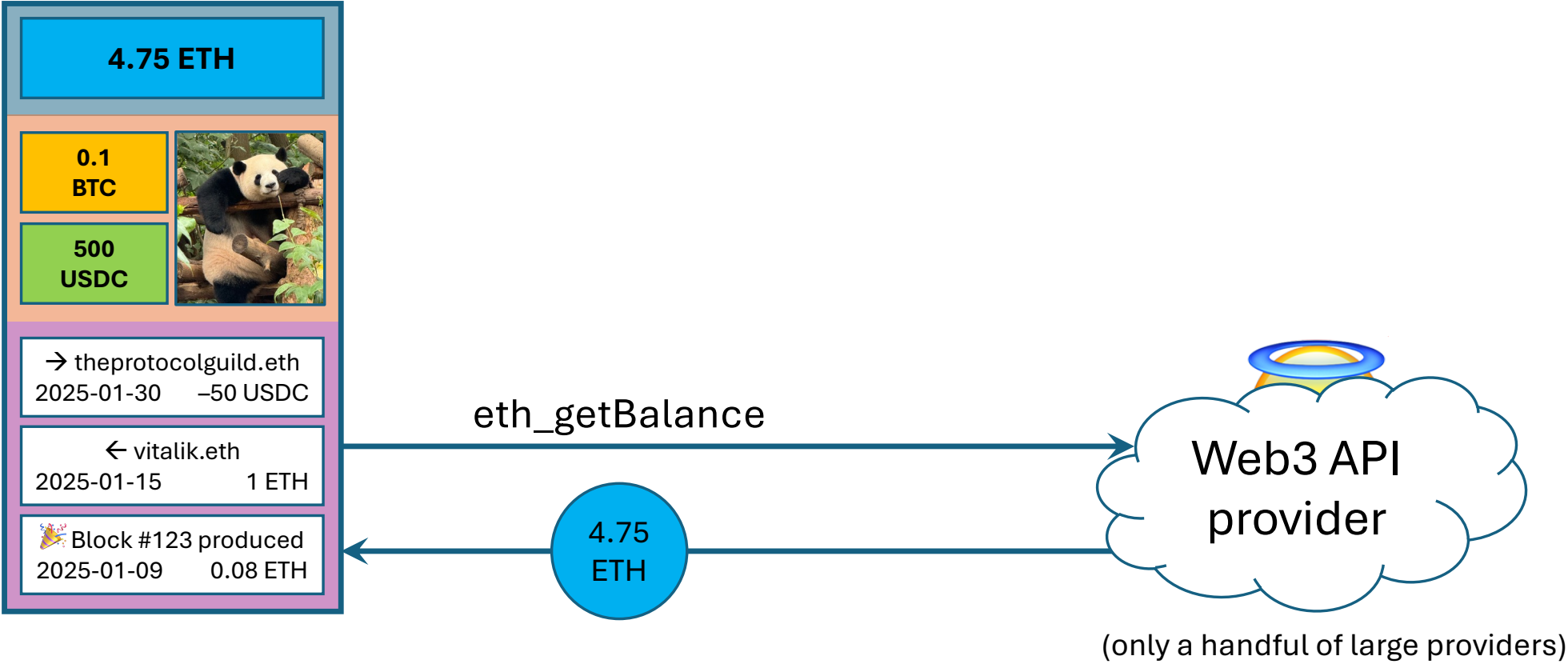


Web3 API provider

Today's reality



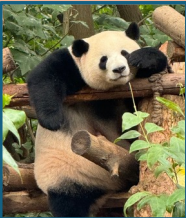
How to fix it?

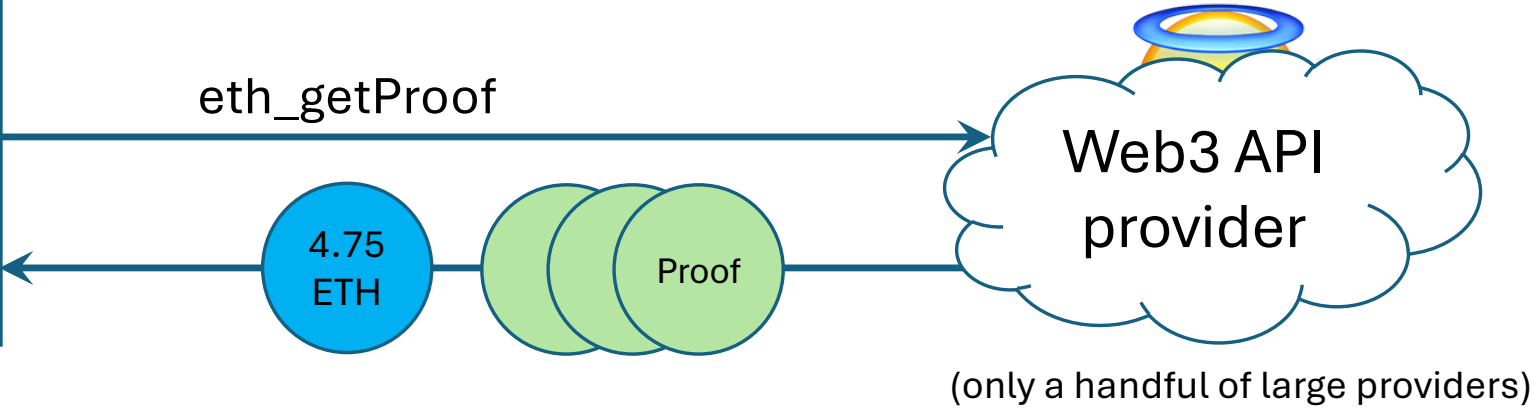




EIP-1186: eth_getProof

✌️ Add correctness proof

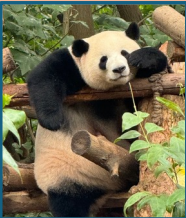
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	

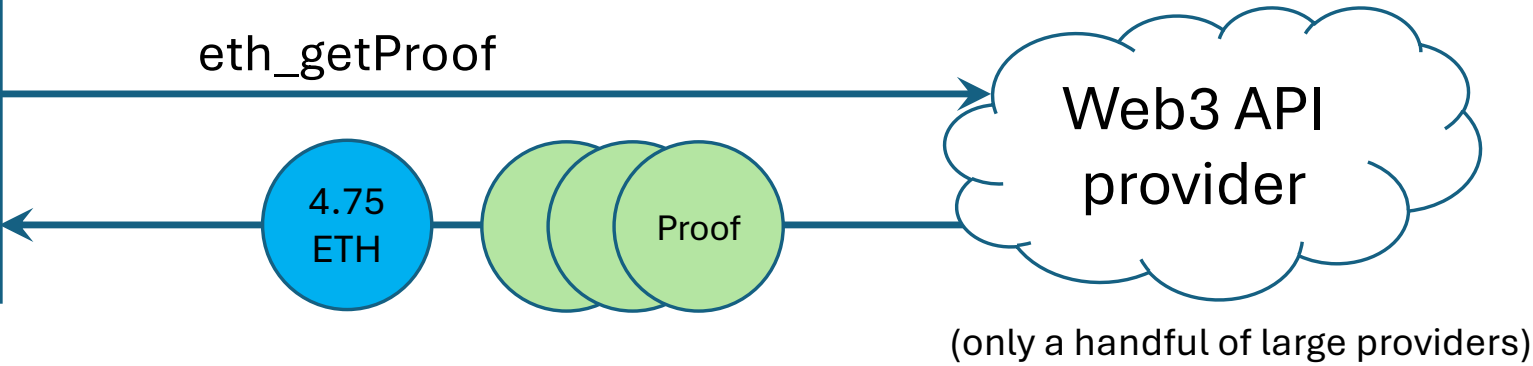




EIP-1186: eth_getProof

- ✌️ Add correctness proof
- ✌️ Data can be verified

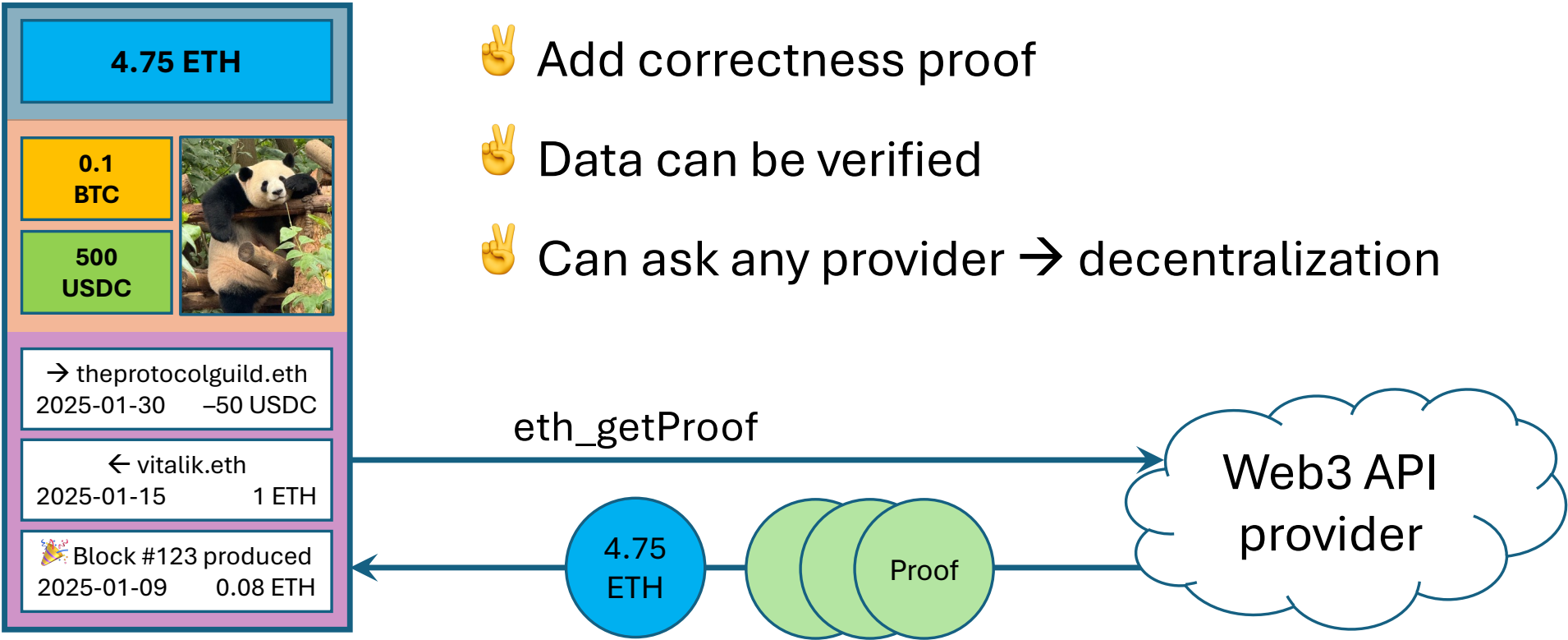
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





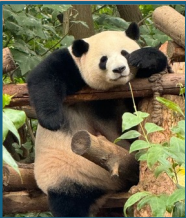
EIP-1186: eth_getProof

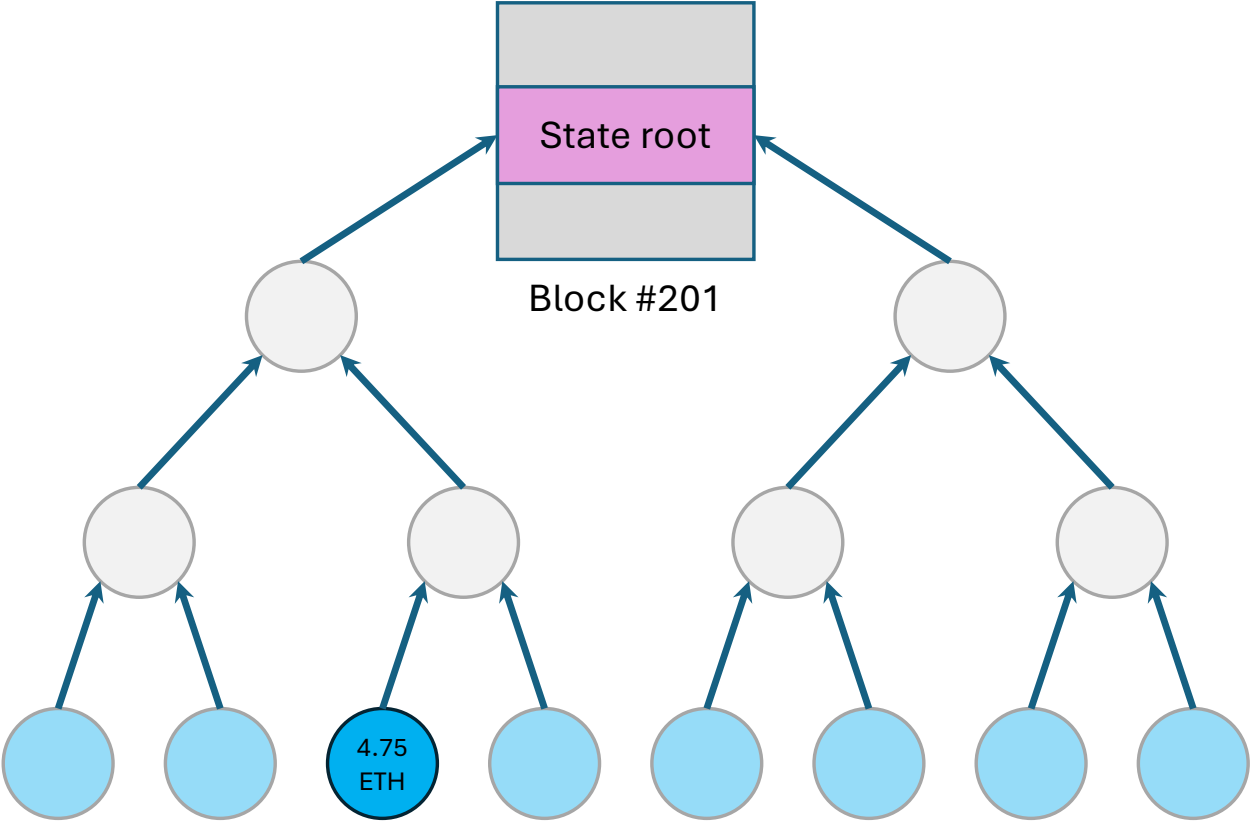
- ✌️ Add correctness proof
- ✌️ Data can be verified
- ✌️ Can ask any provider → decentralization





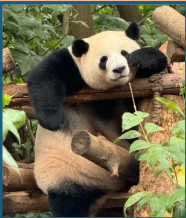
Merkle trees

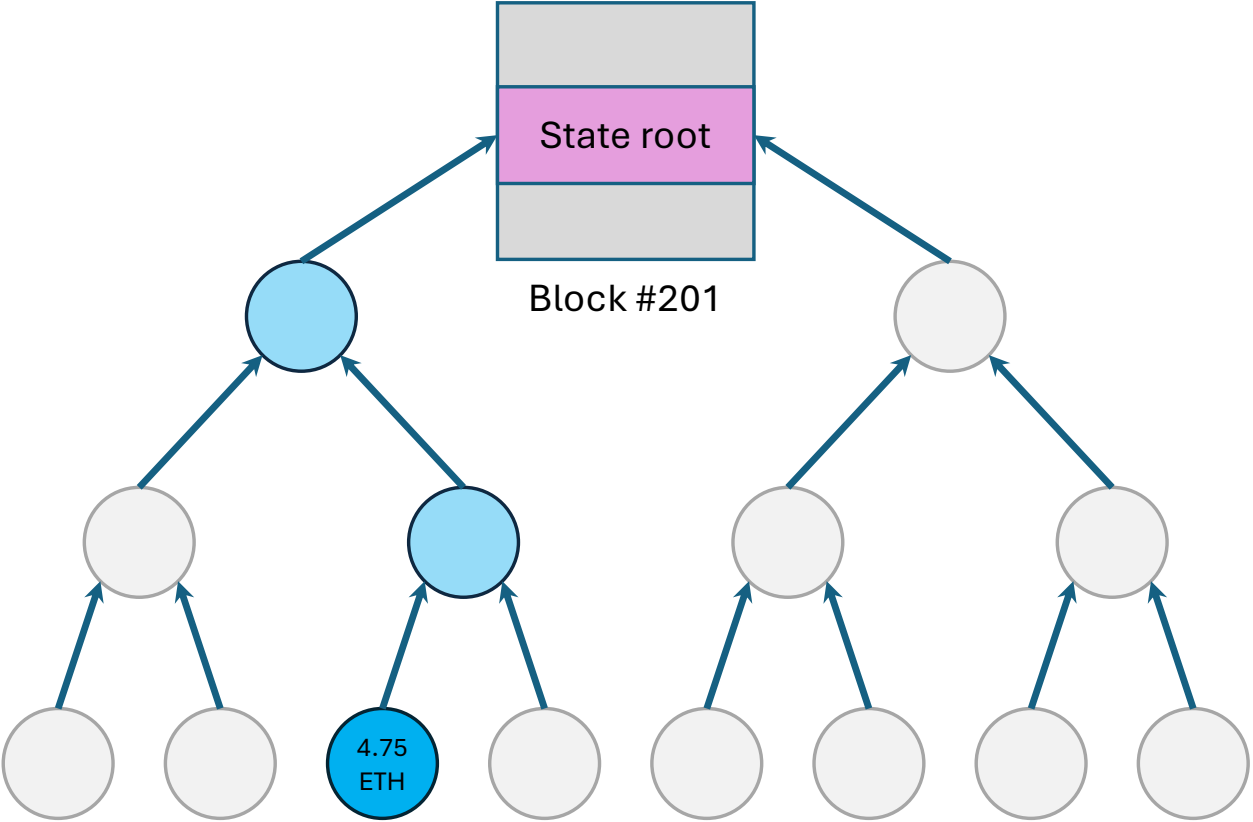
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





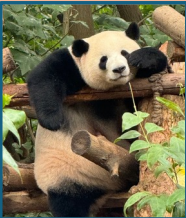
Merkle trees

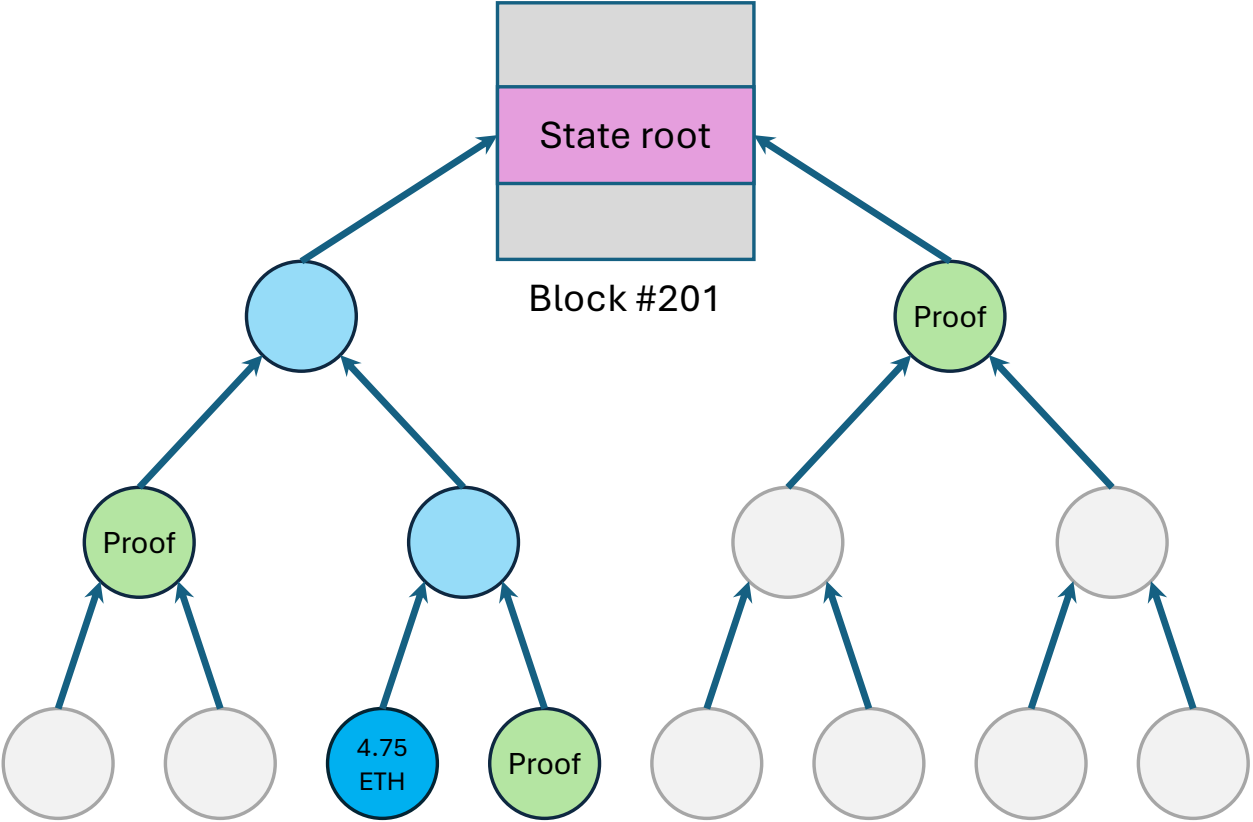
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





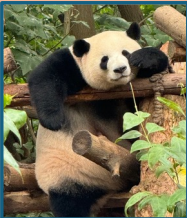
Merkle trees

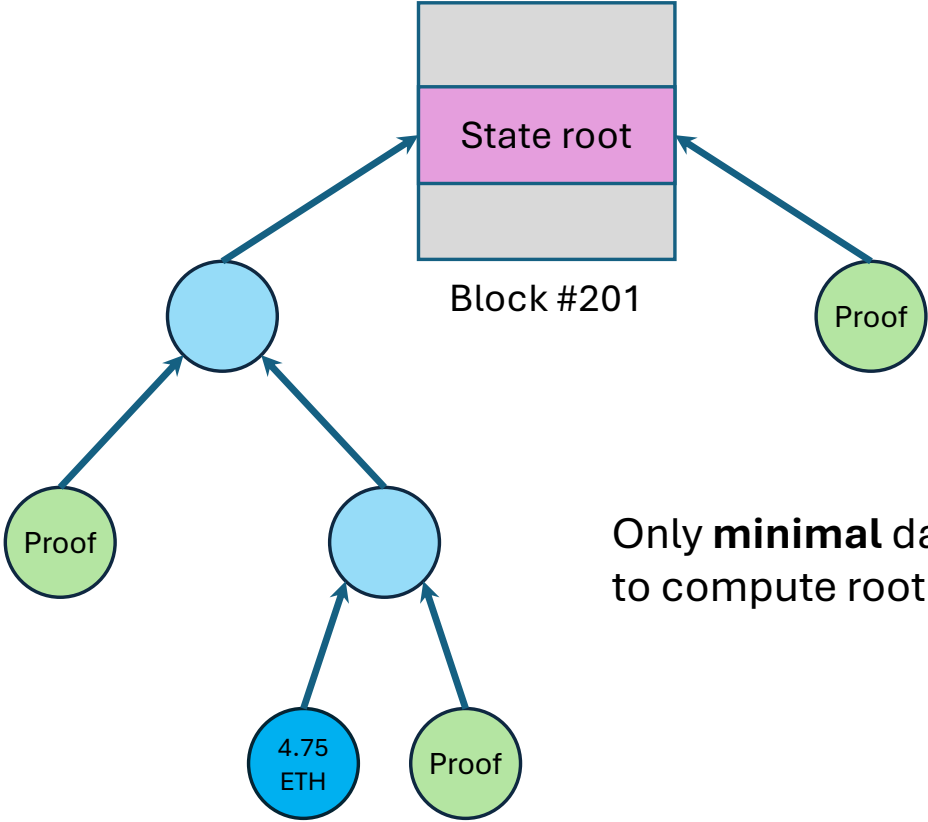
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





Merkle trees

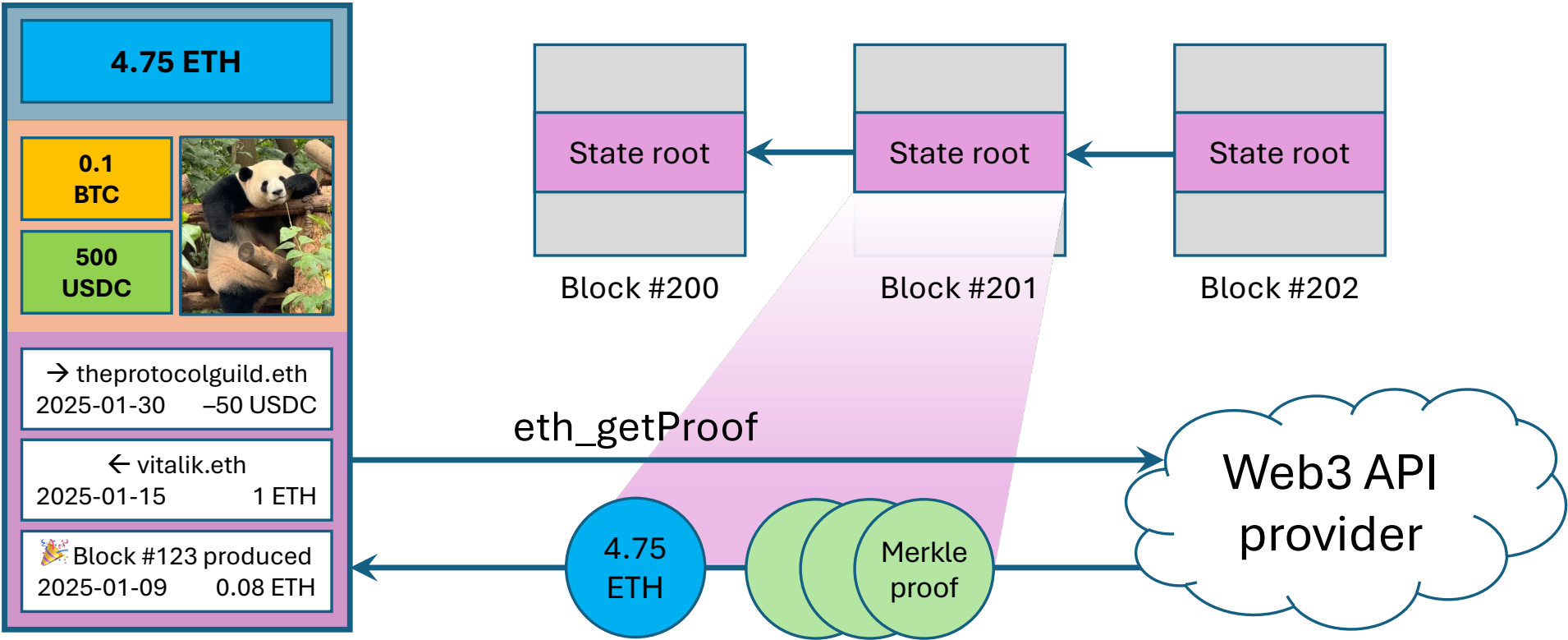
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	



Only **minimal** data required to compute root hash

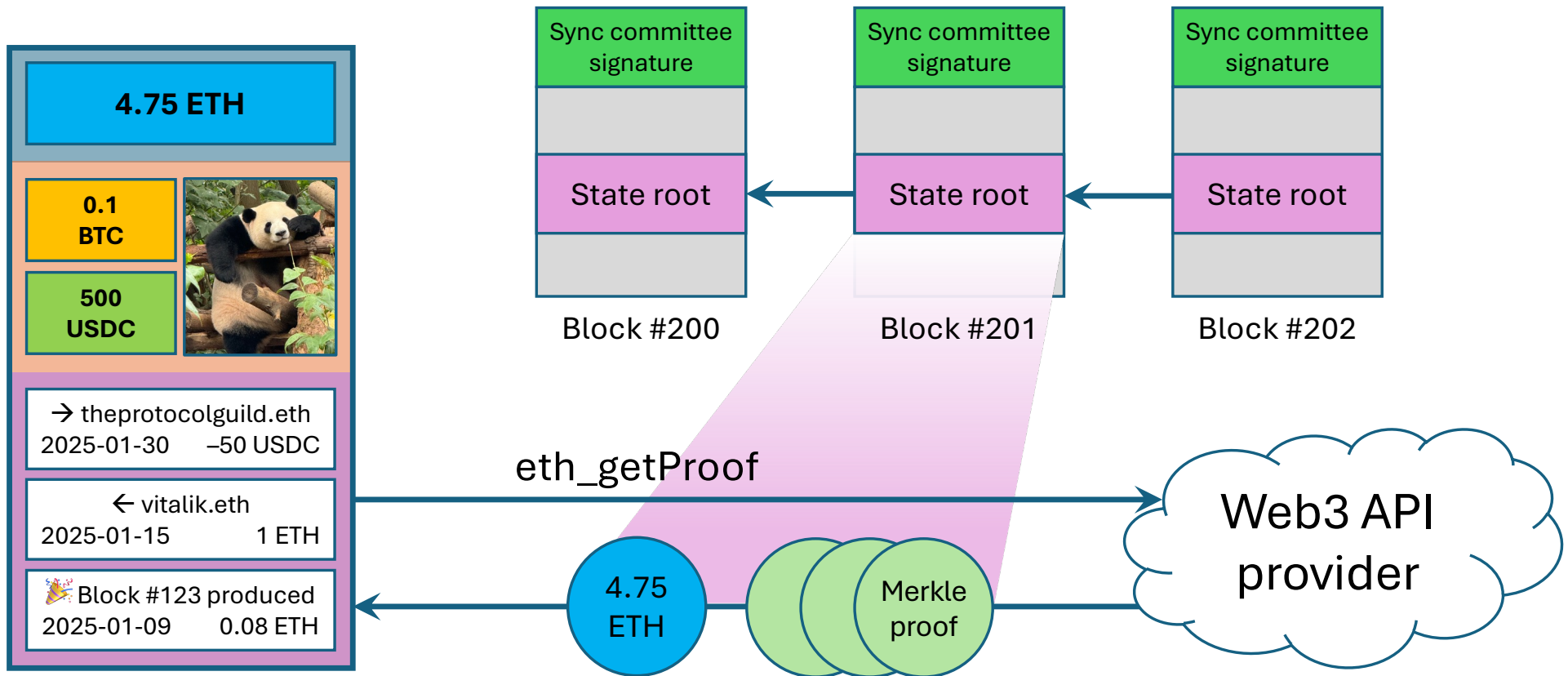


EIP-1186: eth_getProof



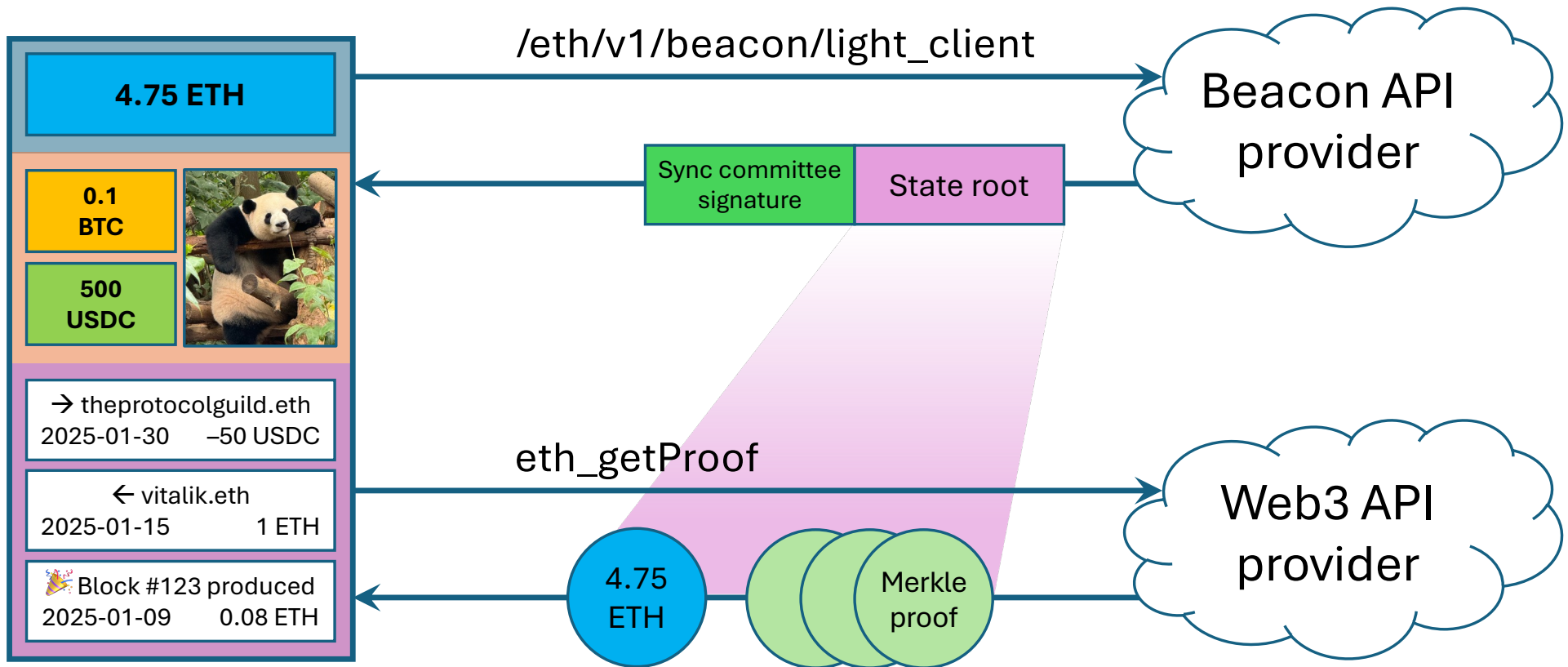


Altair light client protocol



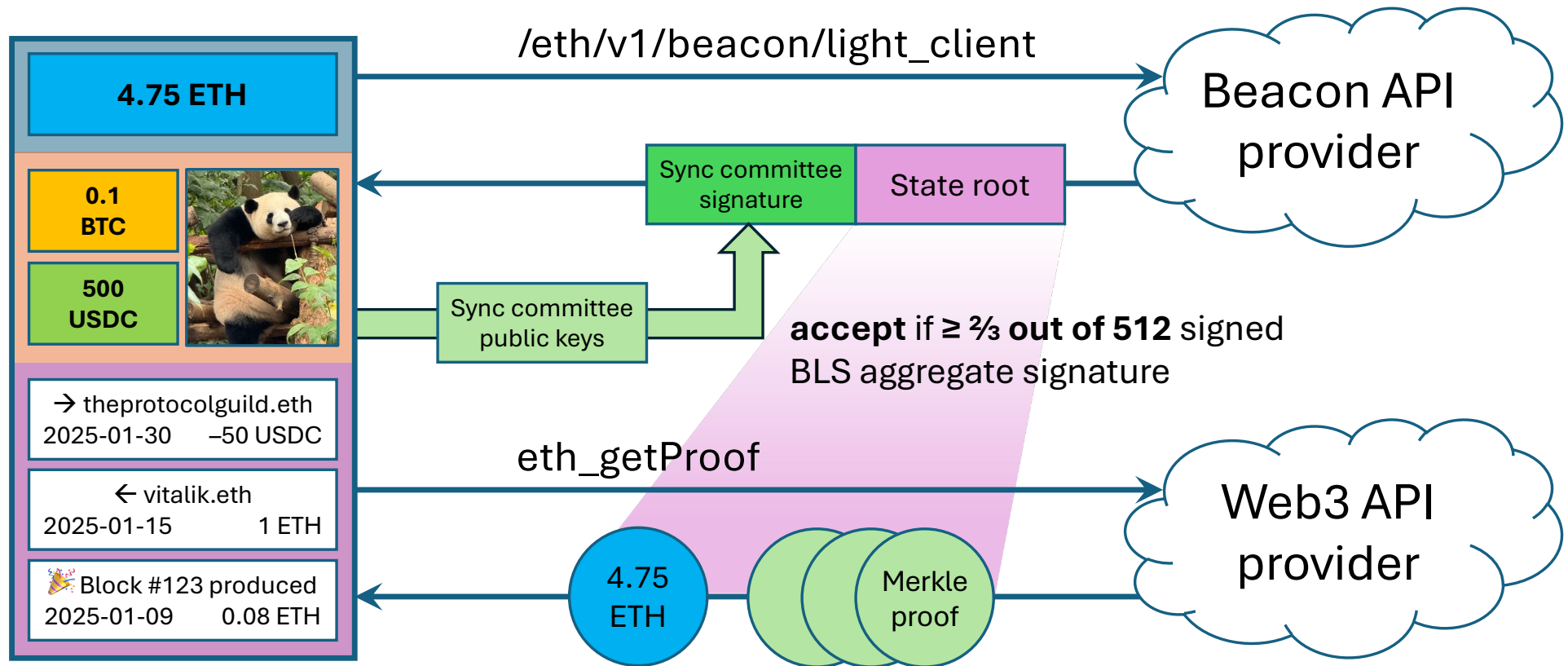


Altair light client protocol



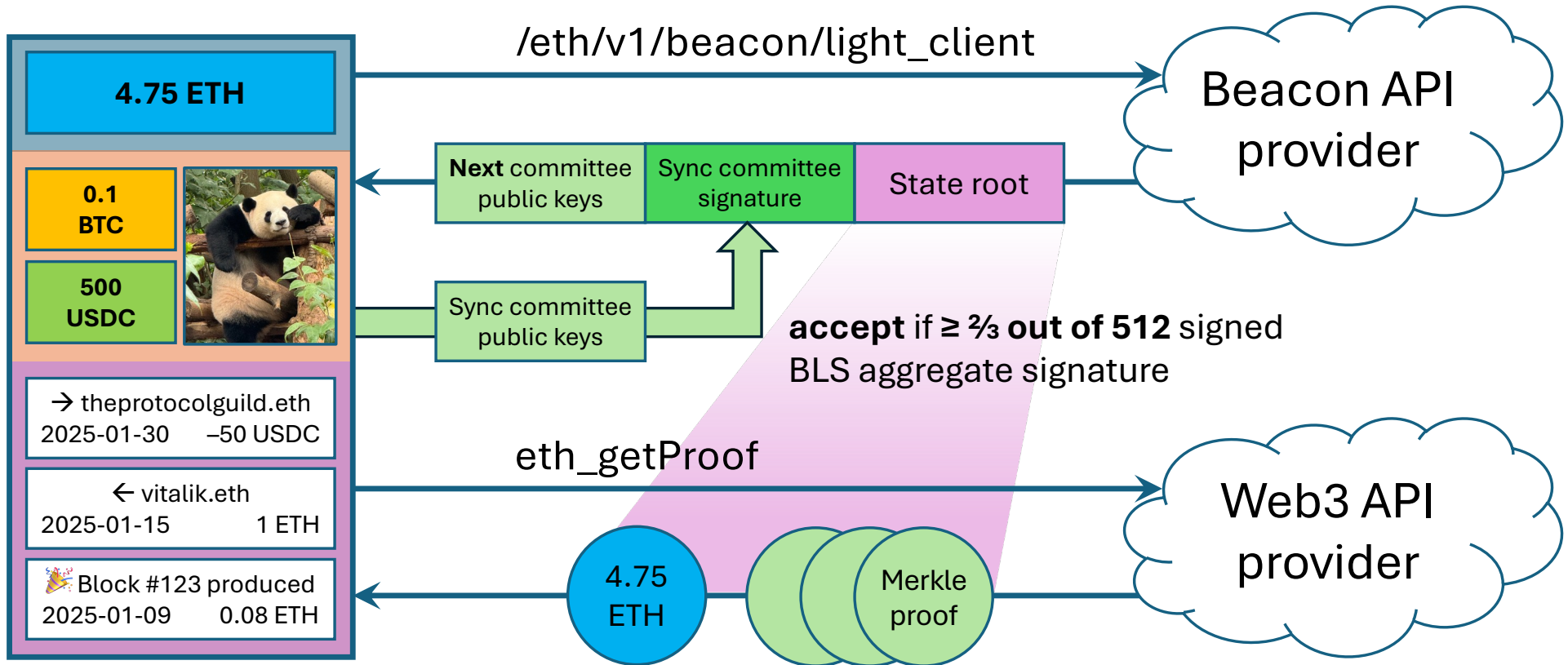


Altair light client protocol



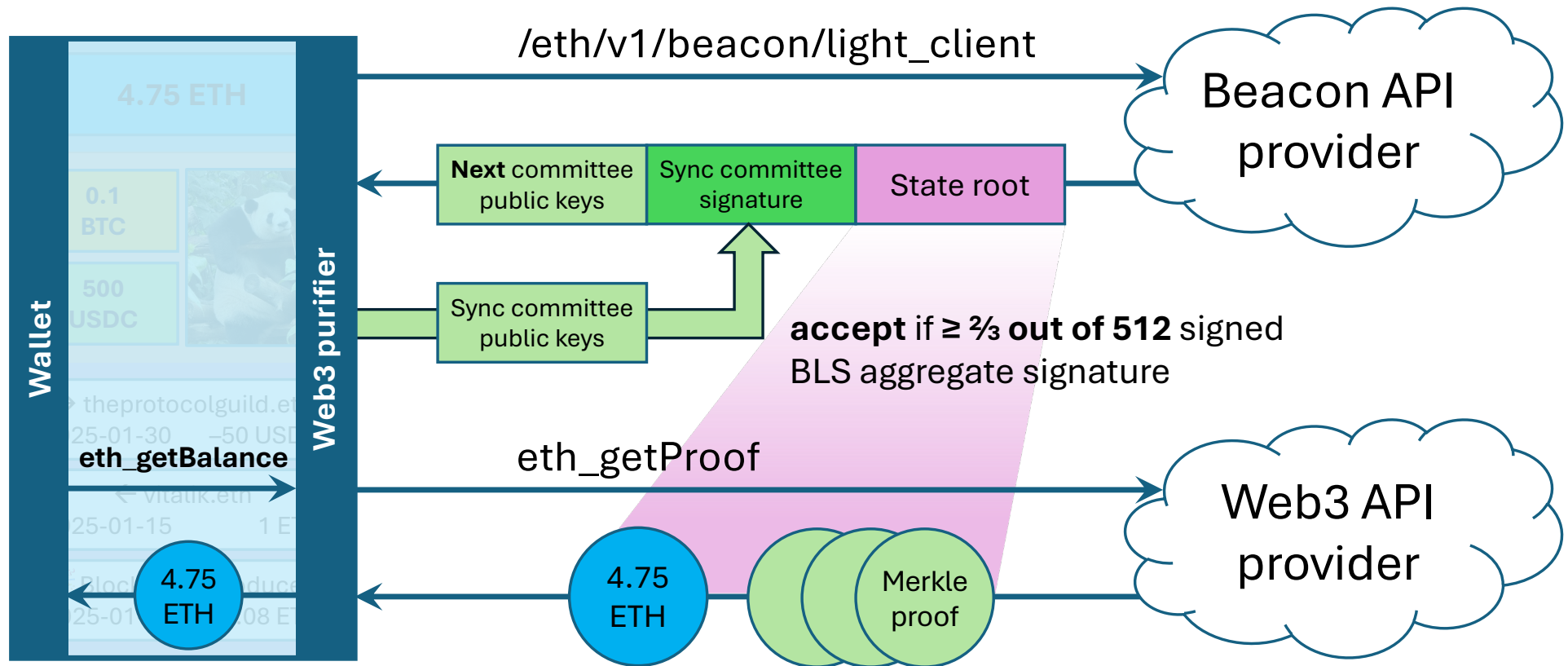


Altair light client protocol



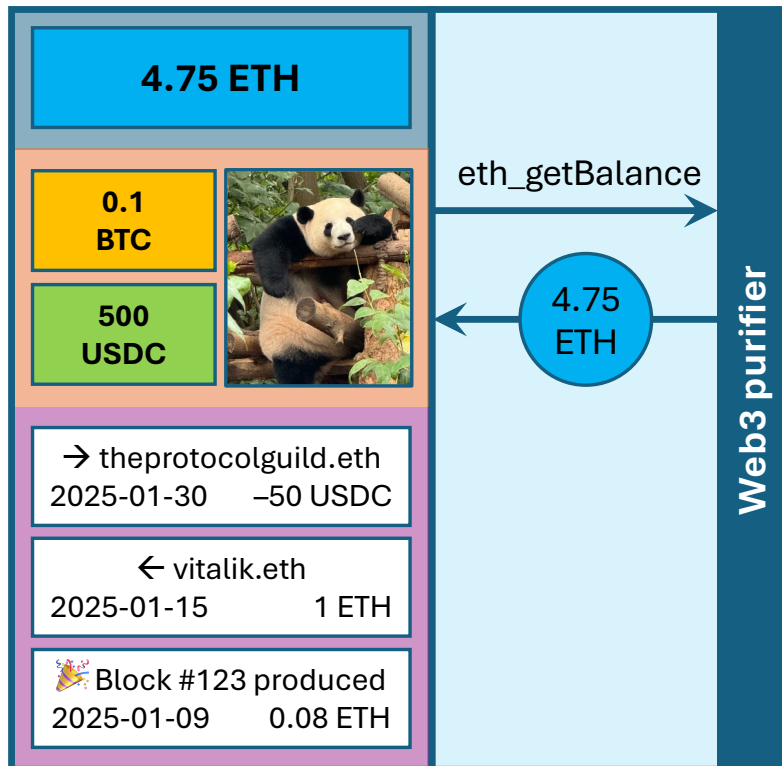


Web3 purifier library





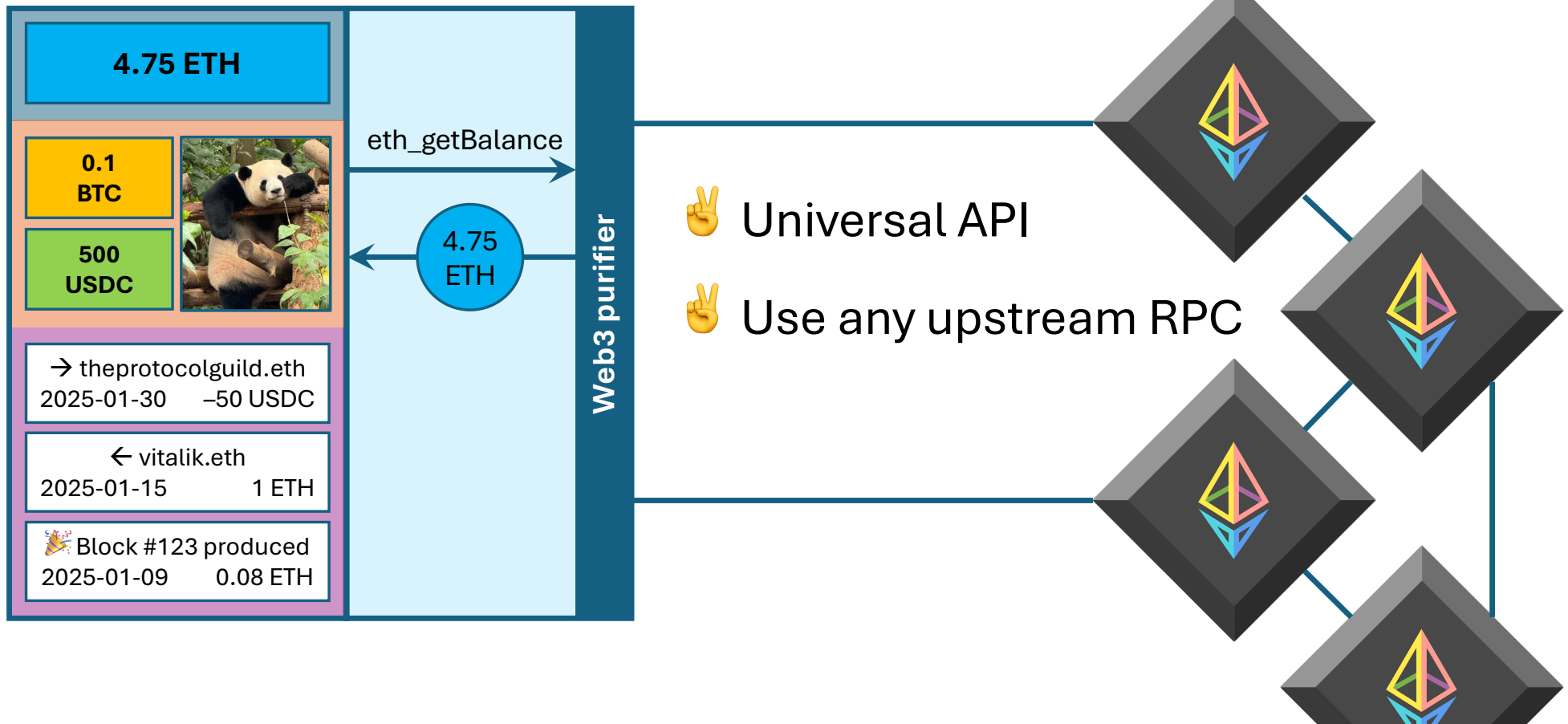
Web3 purifier library



✌️ Universal API

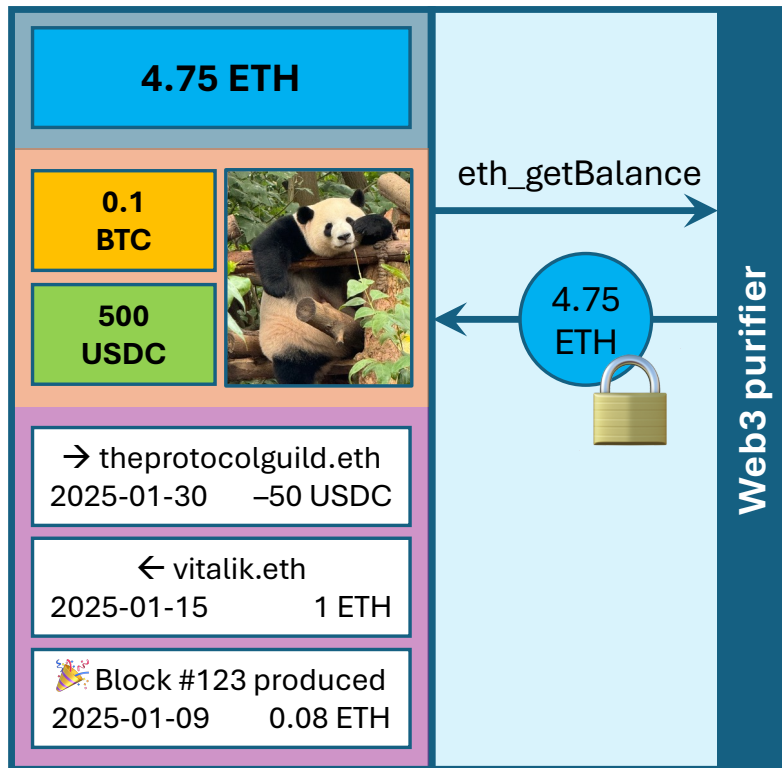


Web3 purifier library

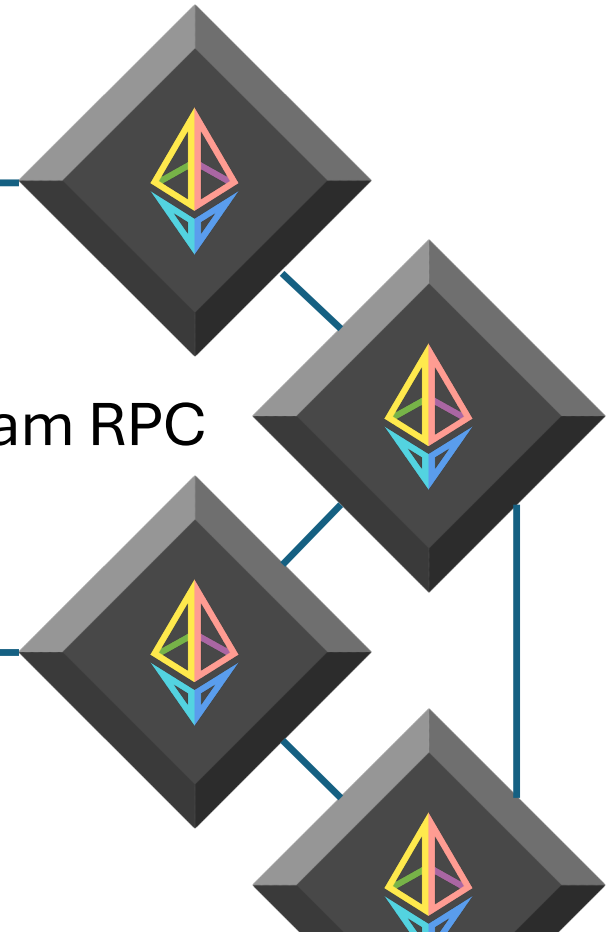




Web3 purifier library

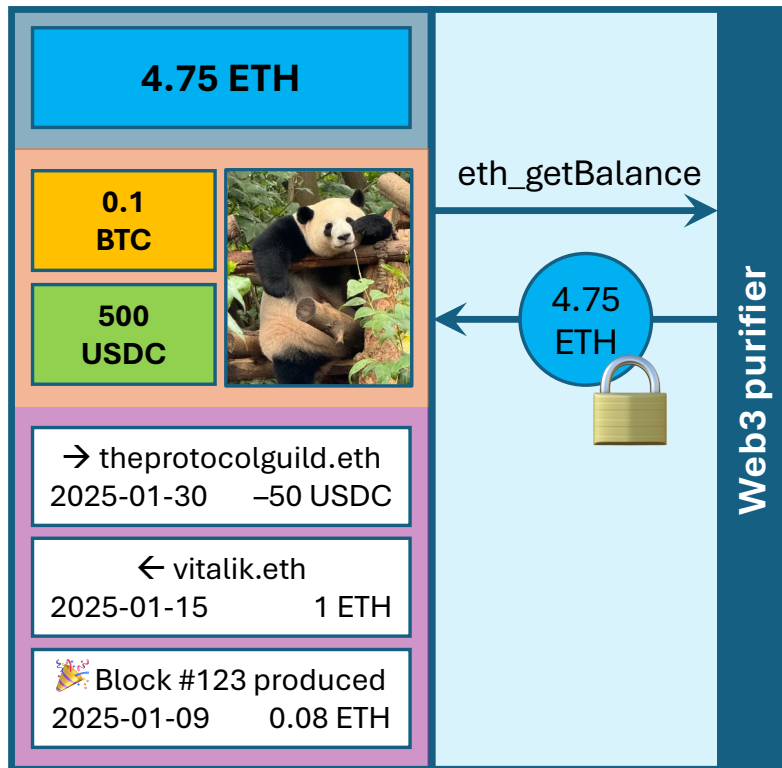


- ✌️ Universal API
- ✌️ Use any upstream RPC
- ✌️ Security





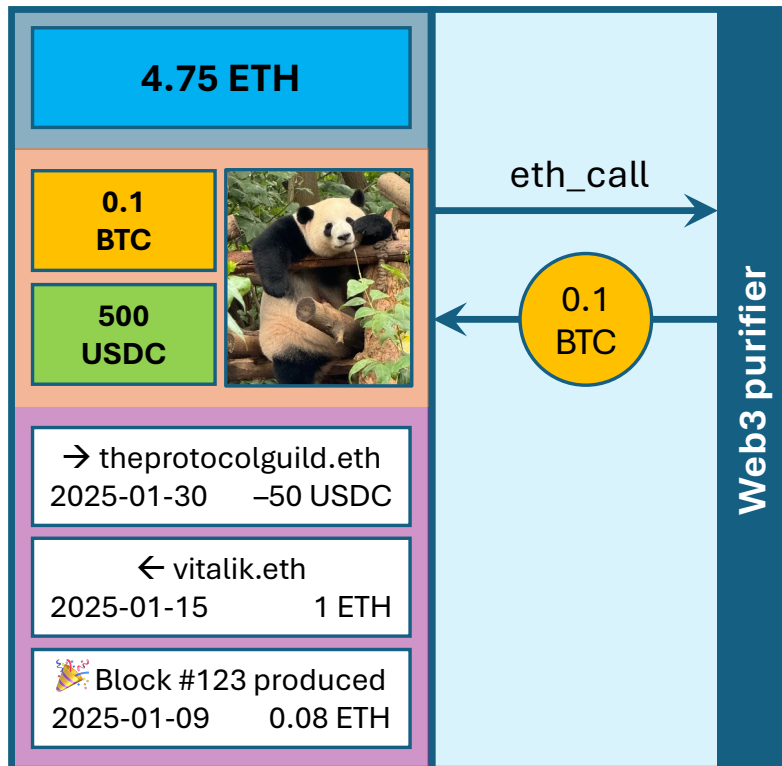
Web3 purifier library



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



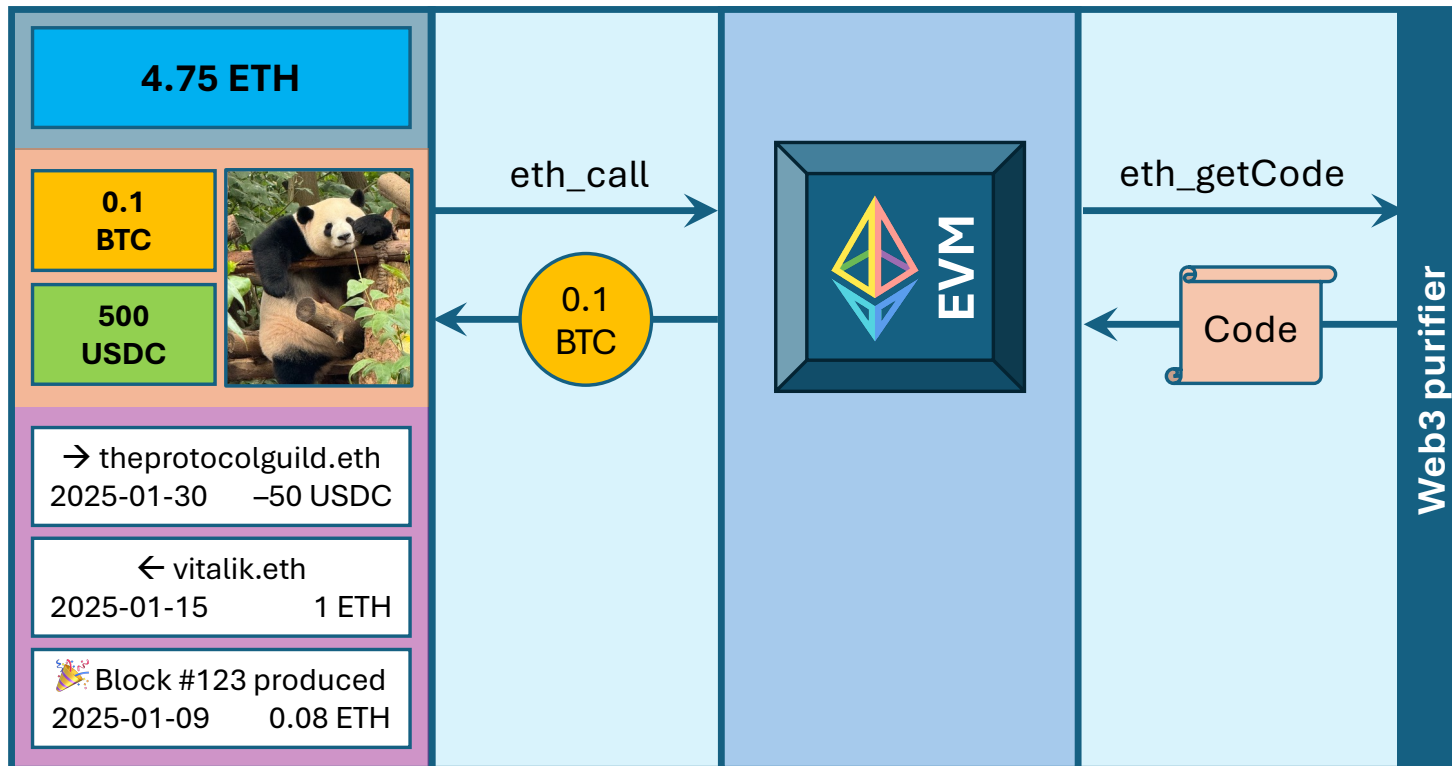
Token balance



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

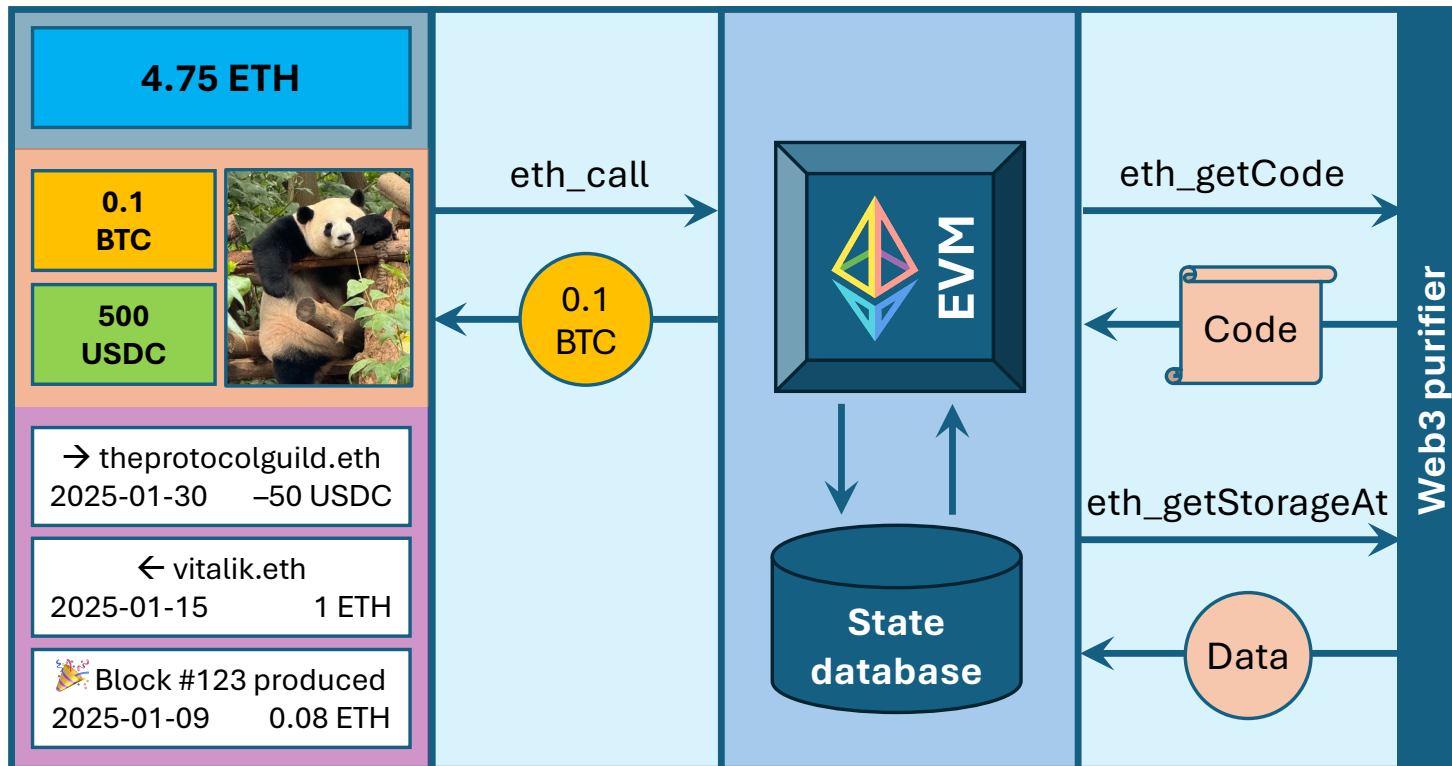


Token balance



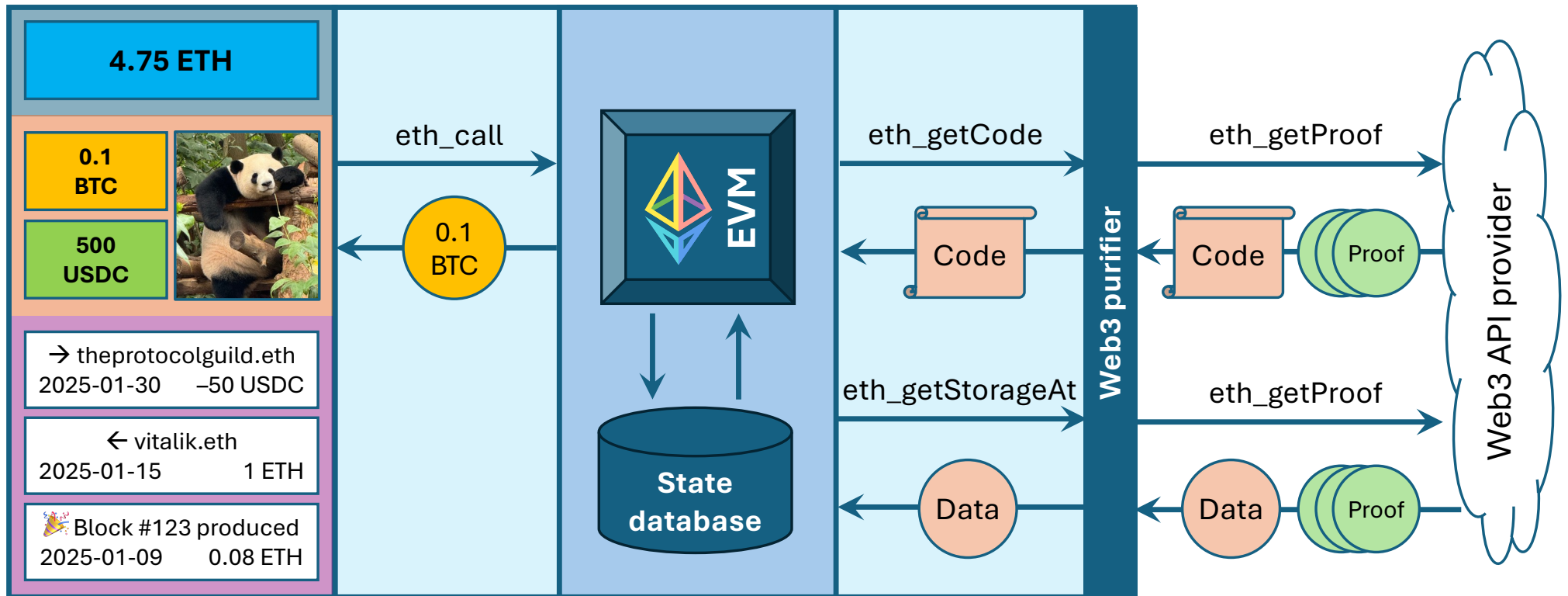


Token balance



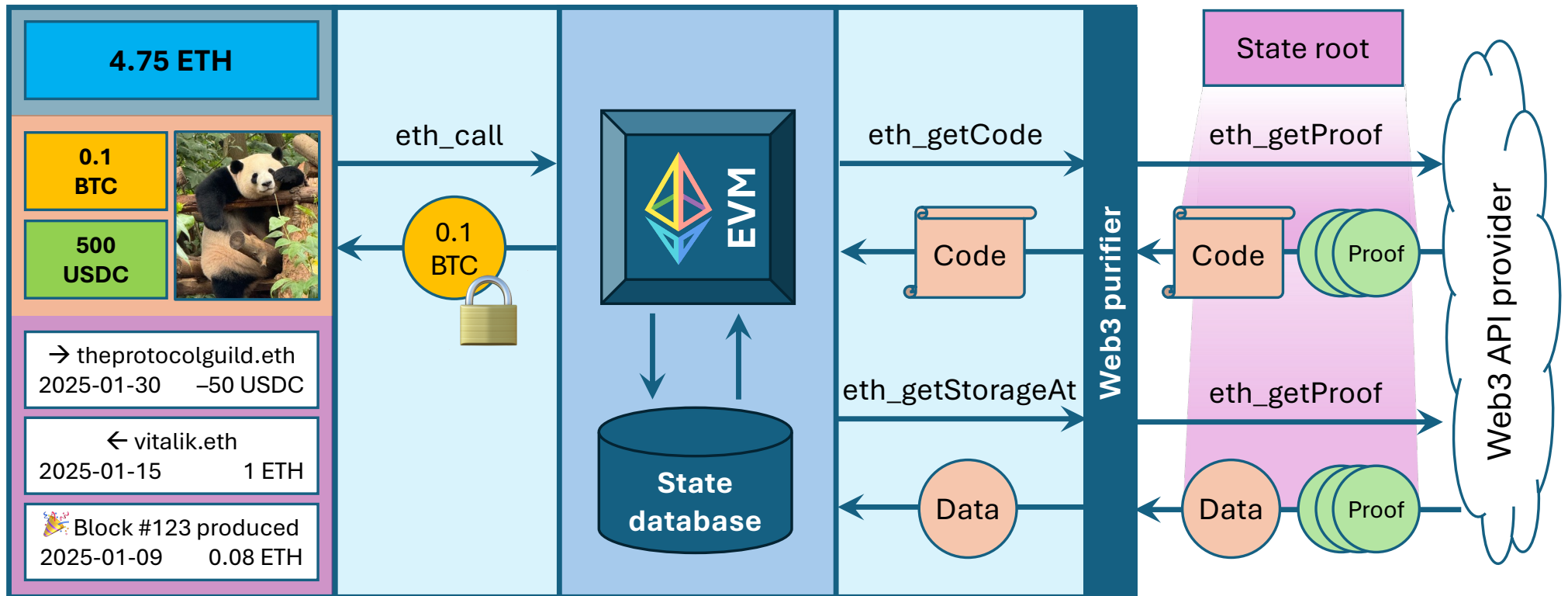


Token balance



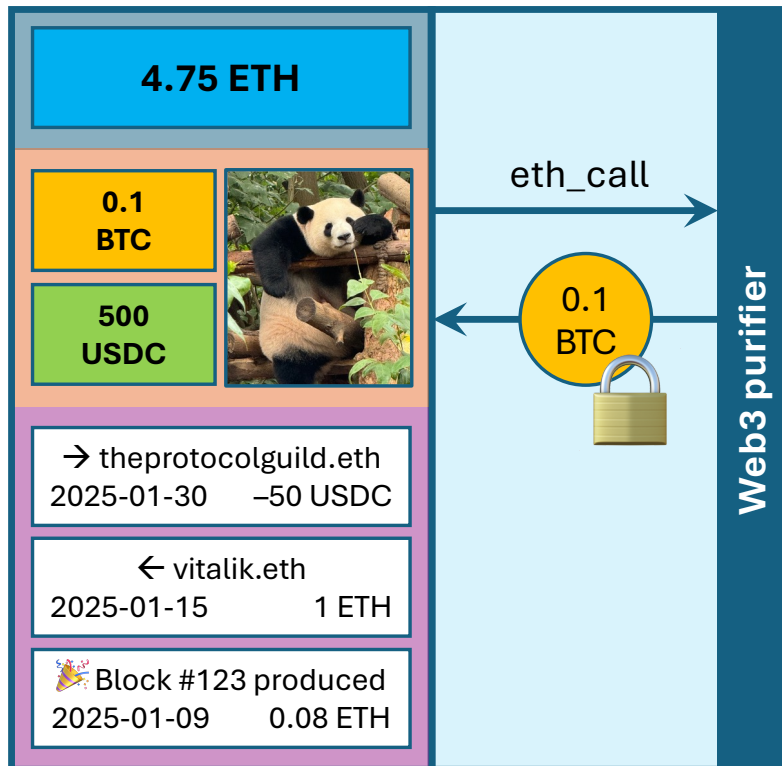


Token balance





Token balance



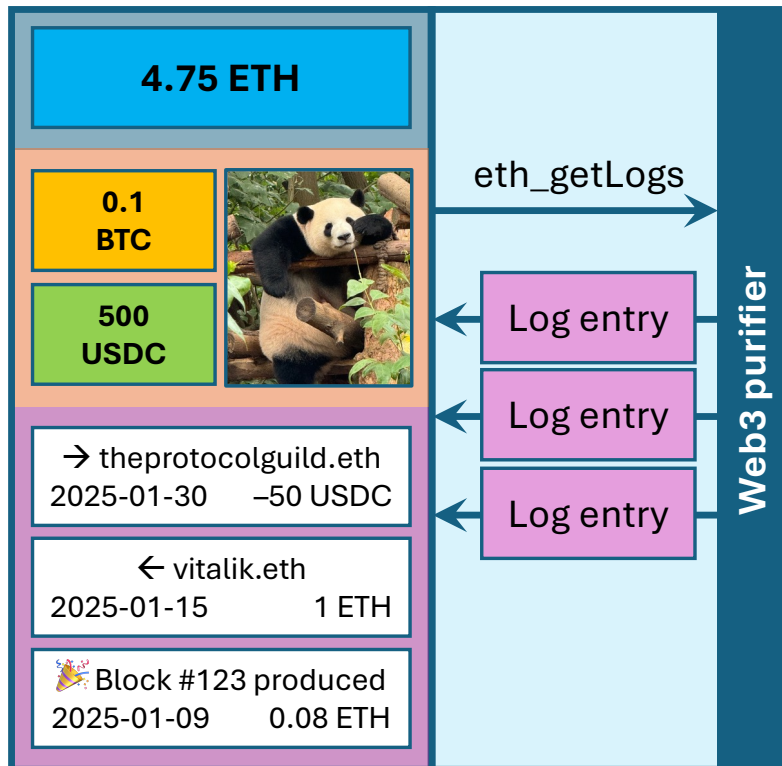
✓ ETH balance

✓ Tokens / NFTs

? History



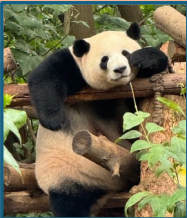
History

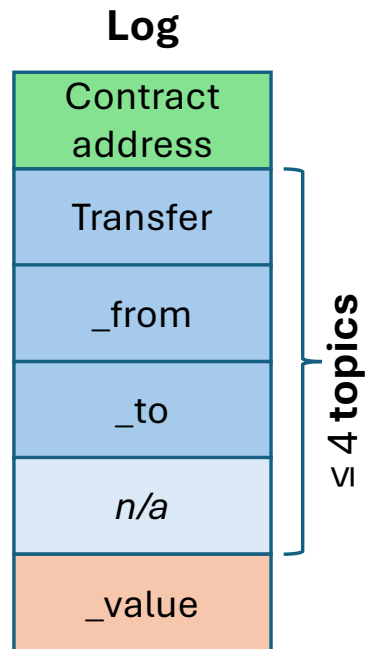


```
contract EIP20Interface {  
    // Triggers when tokens are transferred,  
    // including zero value transfers.  
    event Transfer(  
        address indexed _from,  
        address indexed _to,  
        uint256 _value  
    );  
} ≤ 3 indexed arguments total
```




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	

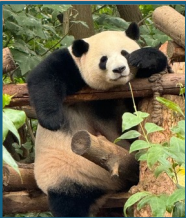


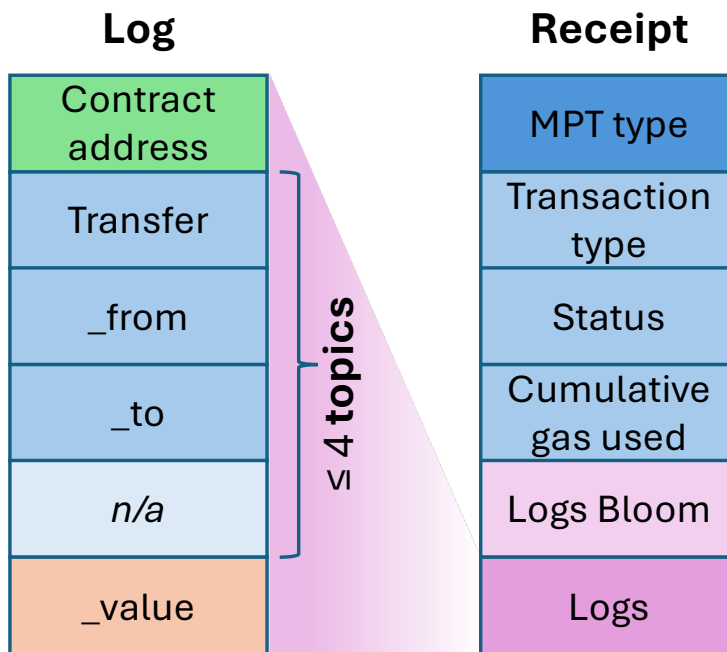
eth_getLogs
(address, topic)

```
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
```

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	

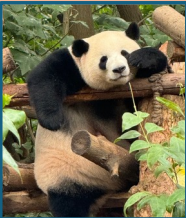


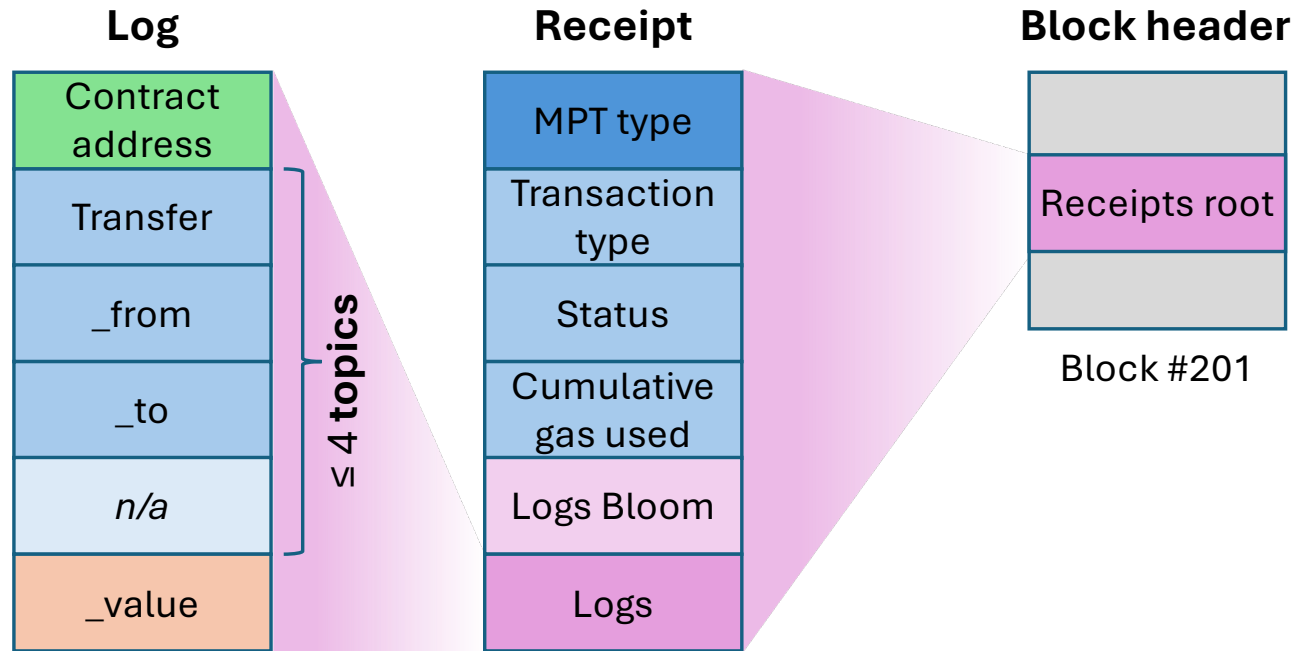
eth_getLogs
(address, topic)

eth_getTransactionReceipt



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	

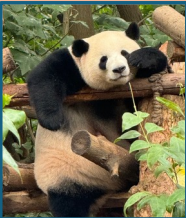


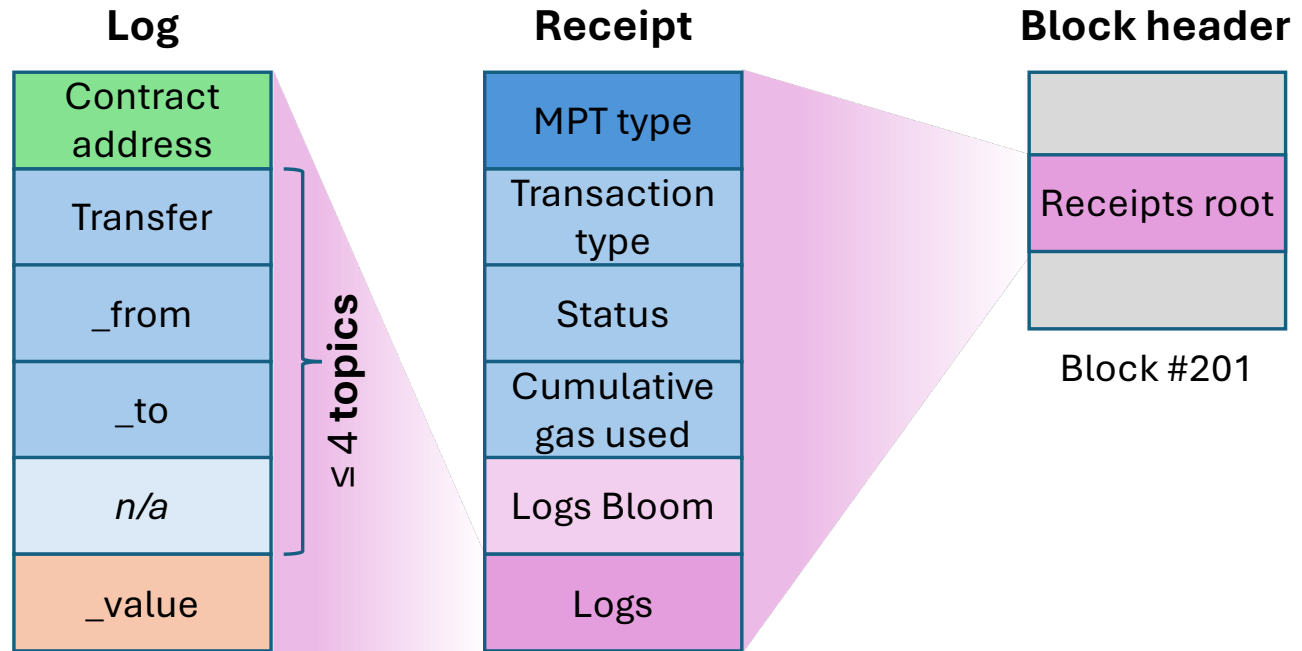
eth_getLogs
(address, topic)

 **eth_getTransactionReceipt**
verifiable against Altair light client



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	

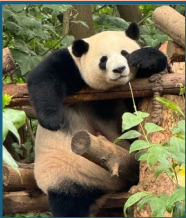


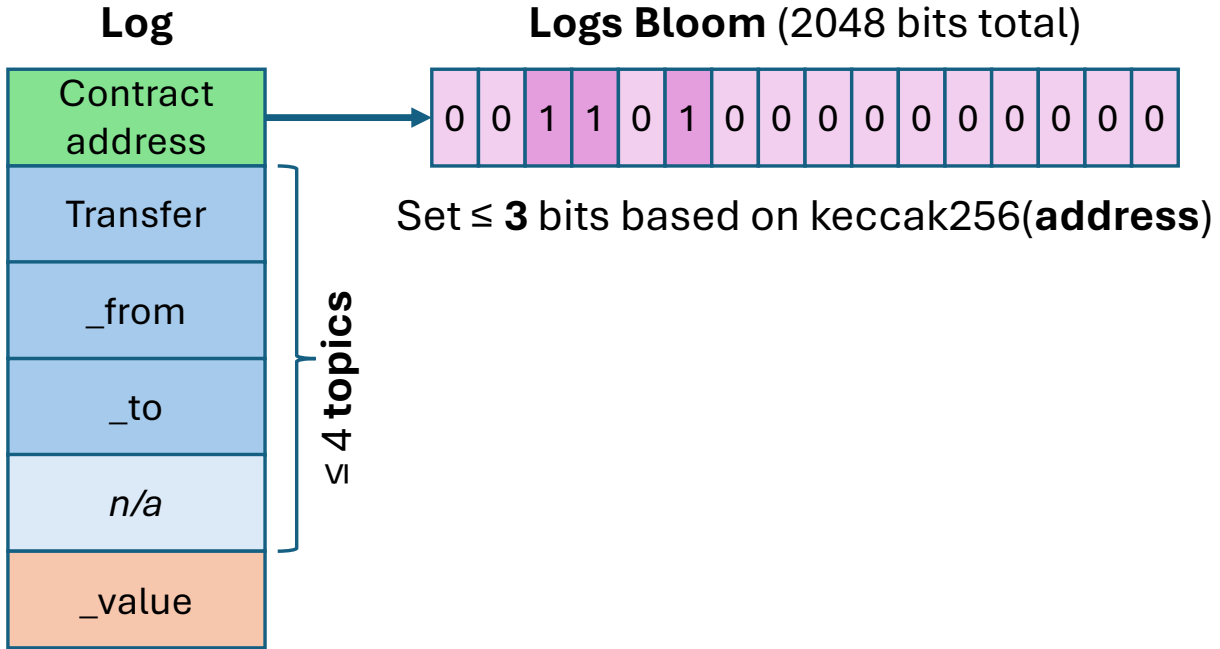
? **eth_getLogs**
maybe **incomplete**

🔒 **eth_getTransactionReceipt**
verifiable against Altair light client



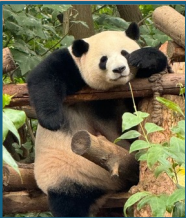
Bloom filter

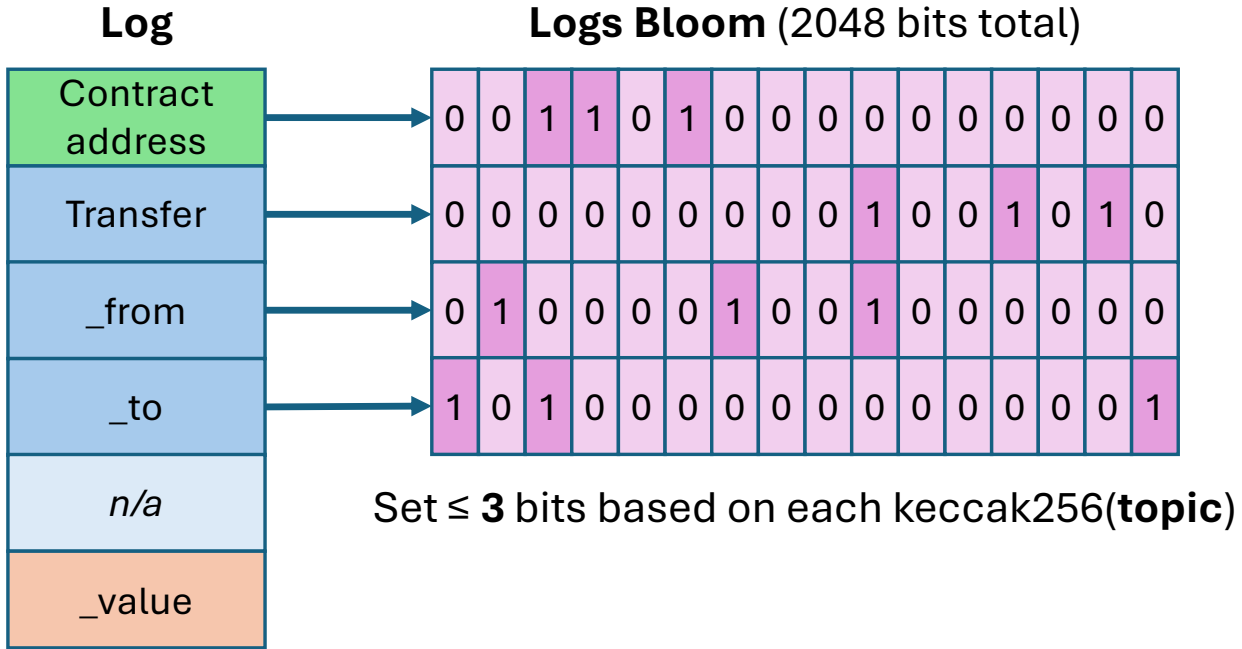
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





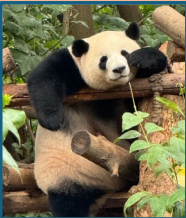
Bloom filter

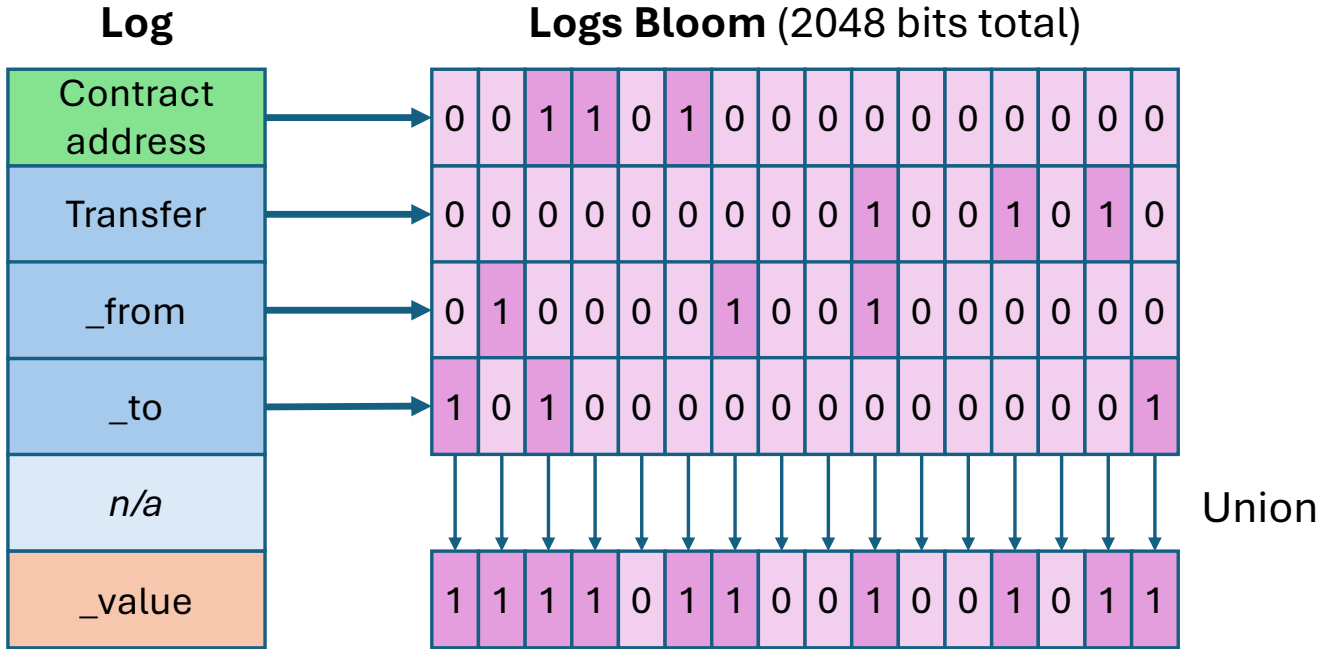
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





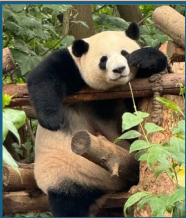
Bloom filter

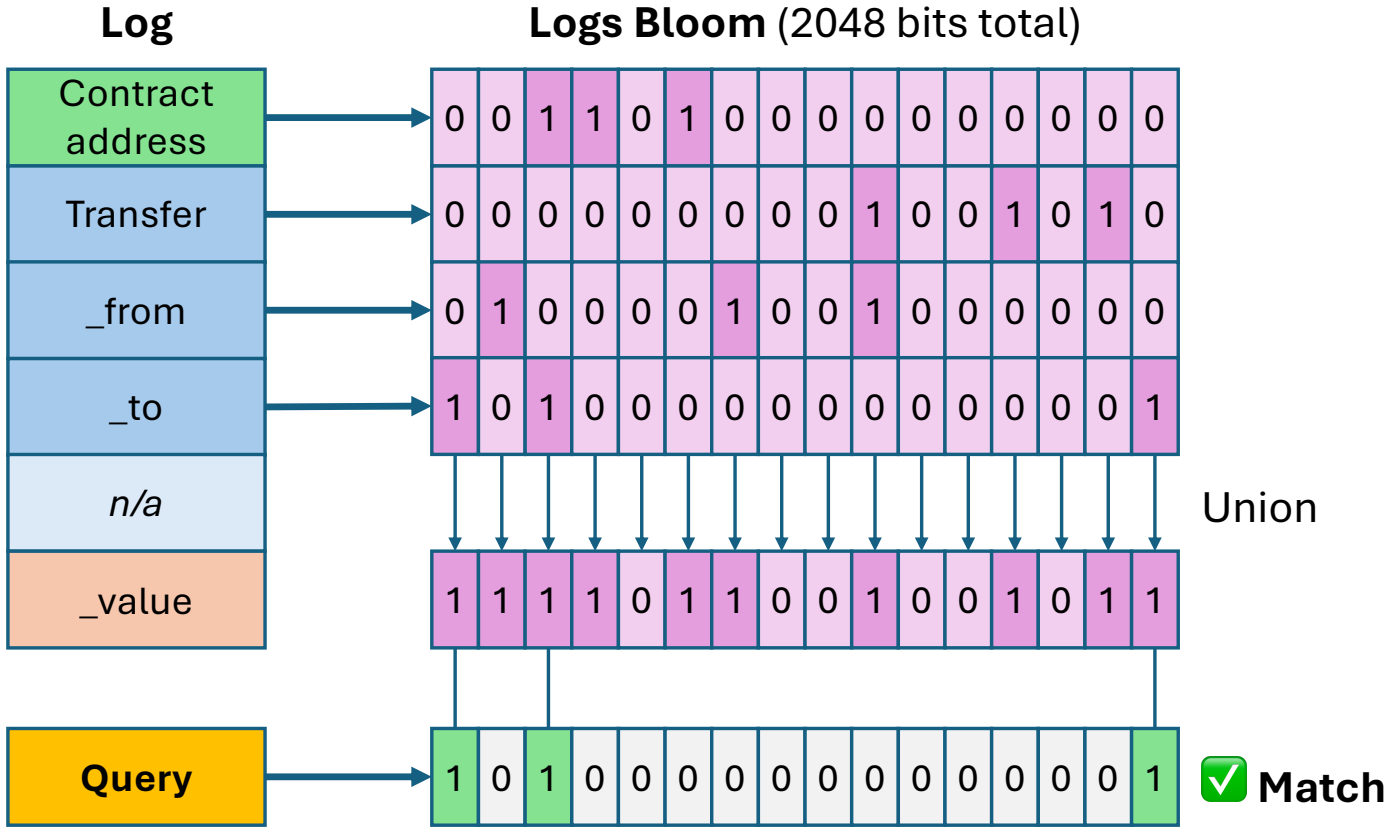
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





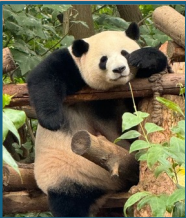
Bloom filter

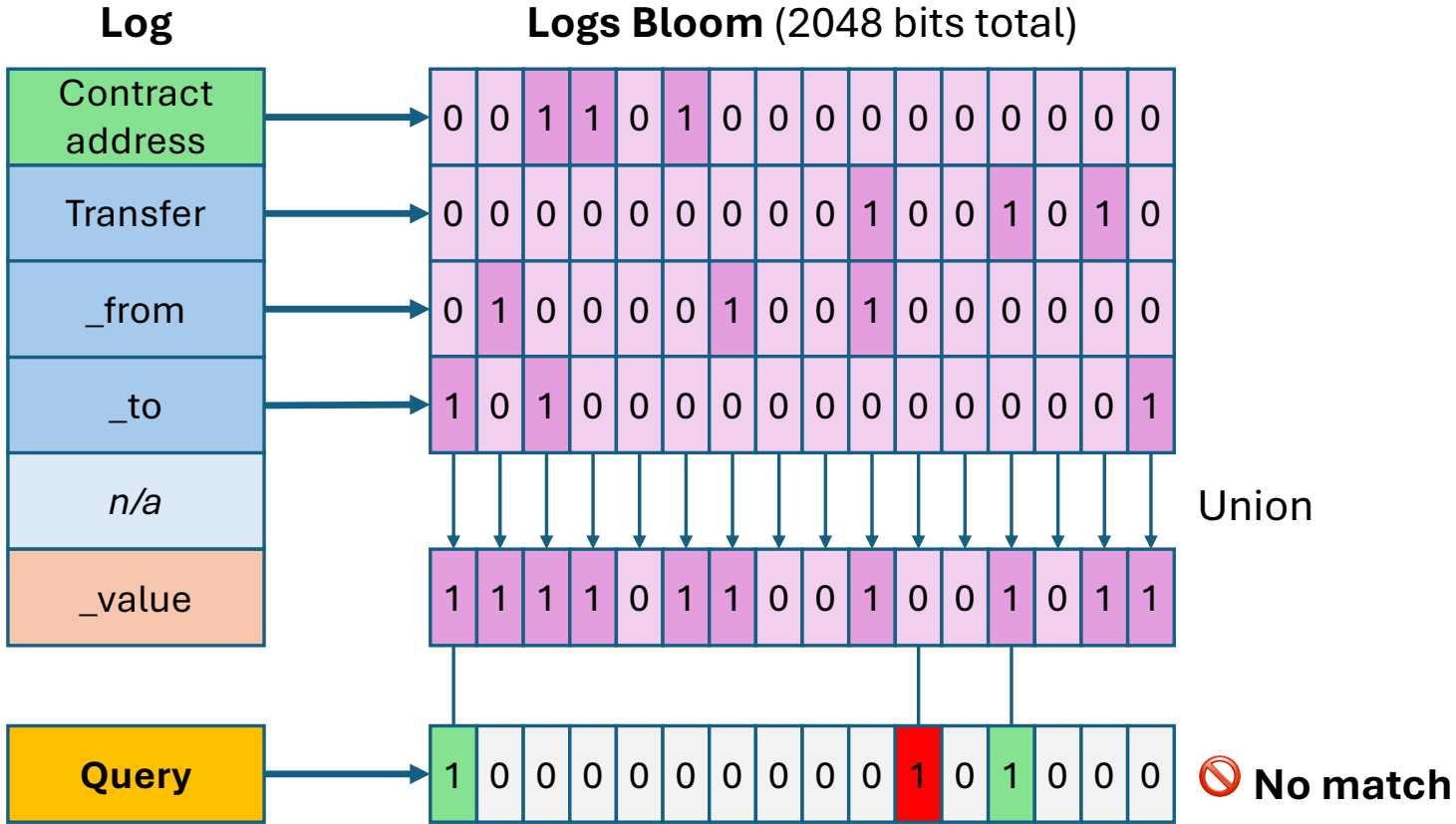
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





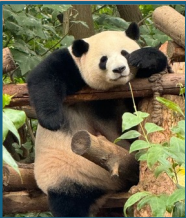
Bloom filter

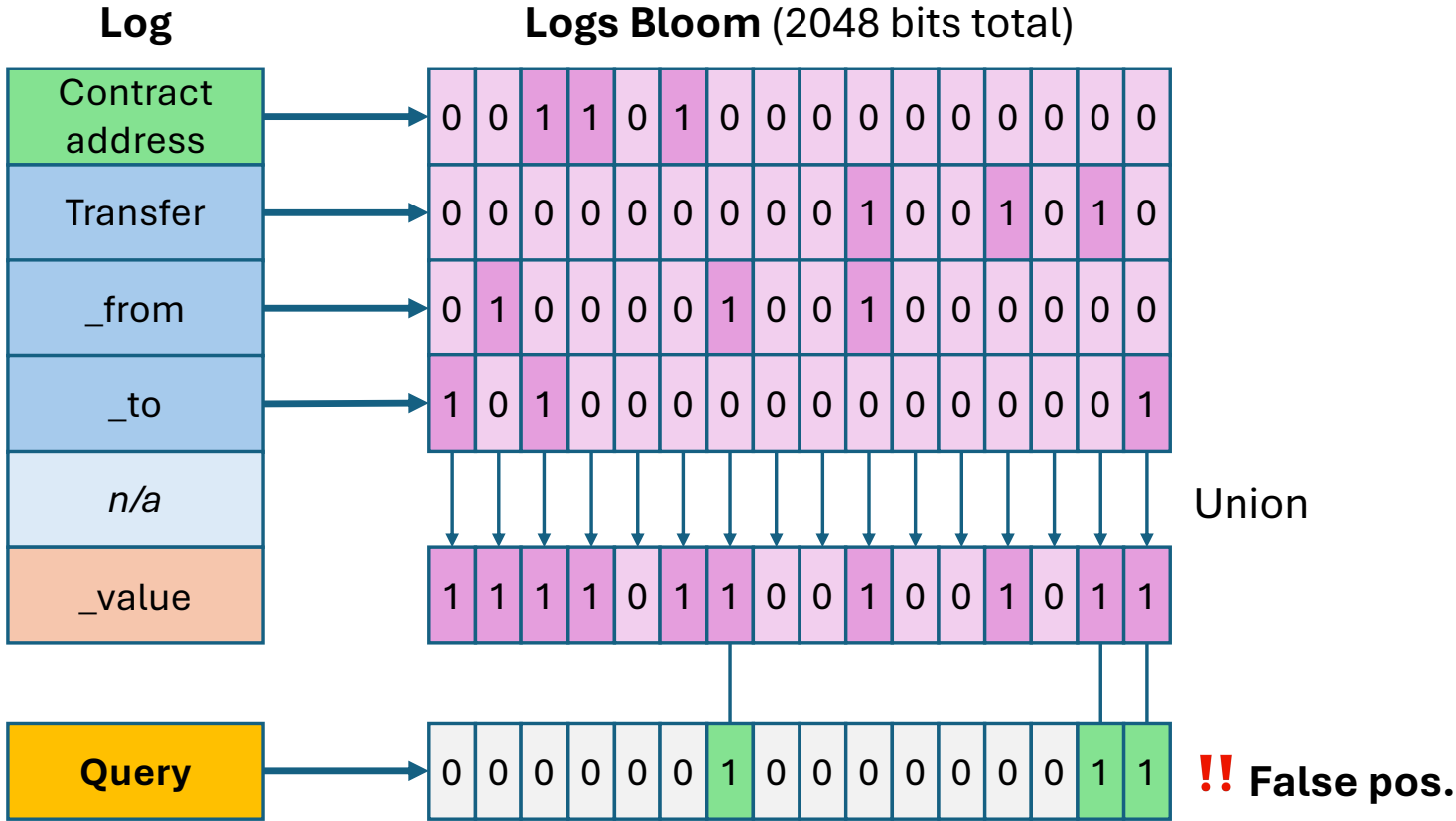
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





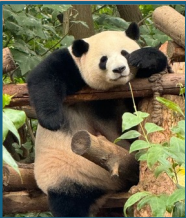
Bloom filter

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	



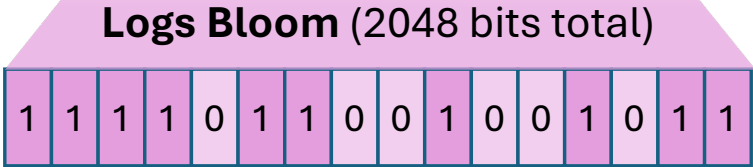
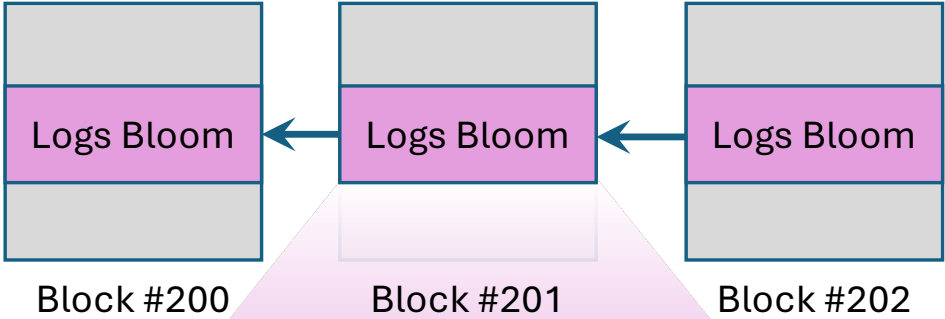


Bloom filter

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



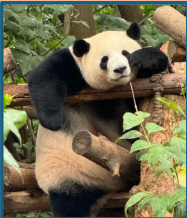
Query



!! False pos.



EIP-7745: Two dimensional log filter

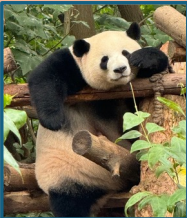
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	

Log

Contract address
Transfer
_from
_to
<i>n/a</i>
_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	

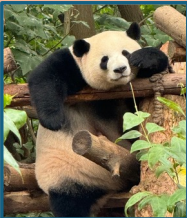
Log	Global index
Contract address	#1
Transfer	#2
_from	#3
_to	#4
<i>n/a</i>	
_value	



EIP-7745: Two dimensional log filter

4.75 ETH

**0.1
BTC**



**500
USDC**

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

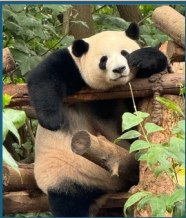
← vitalik.eth
2025-01-15 1 ETH

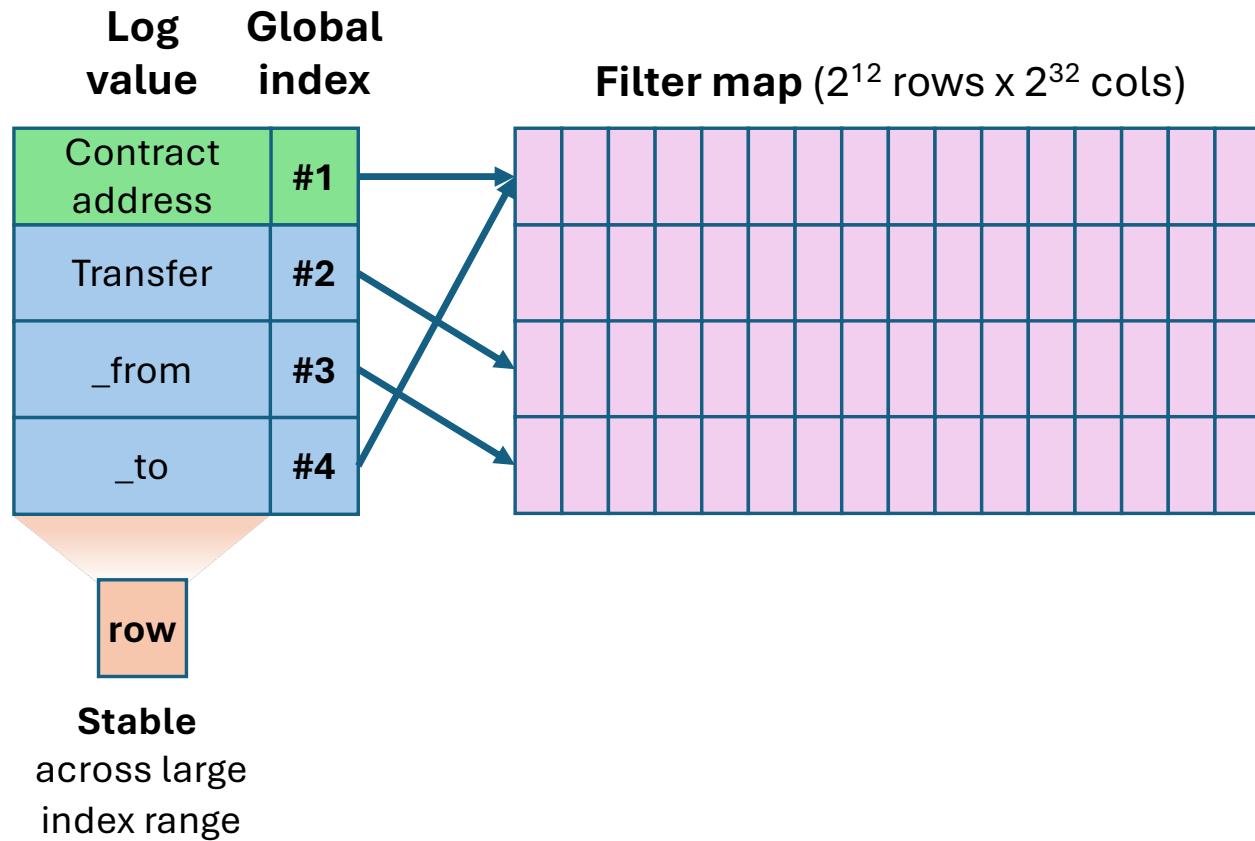
🎉 Block #123 produced
2025-01-09 0.08 ETH

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



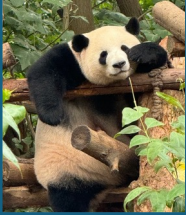
EIP-7745: Two dimensional log filter

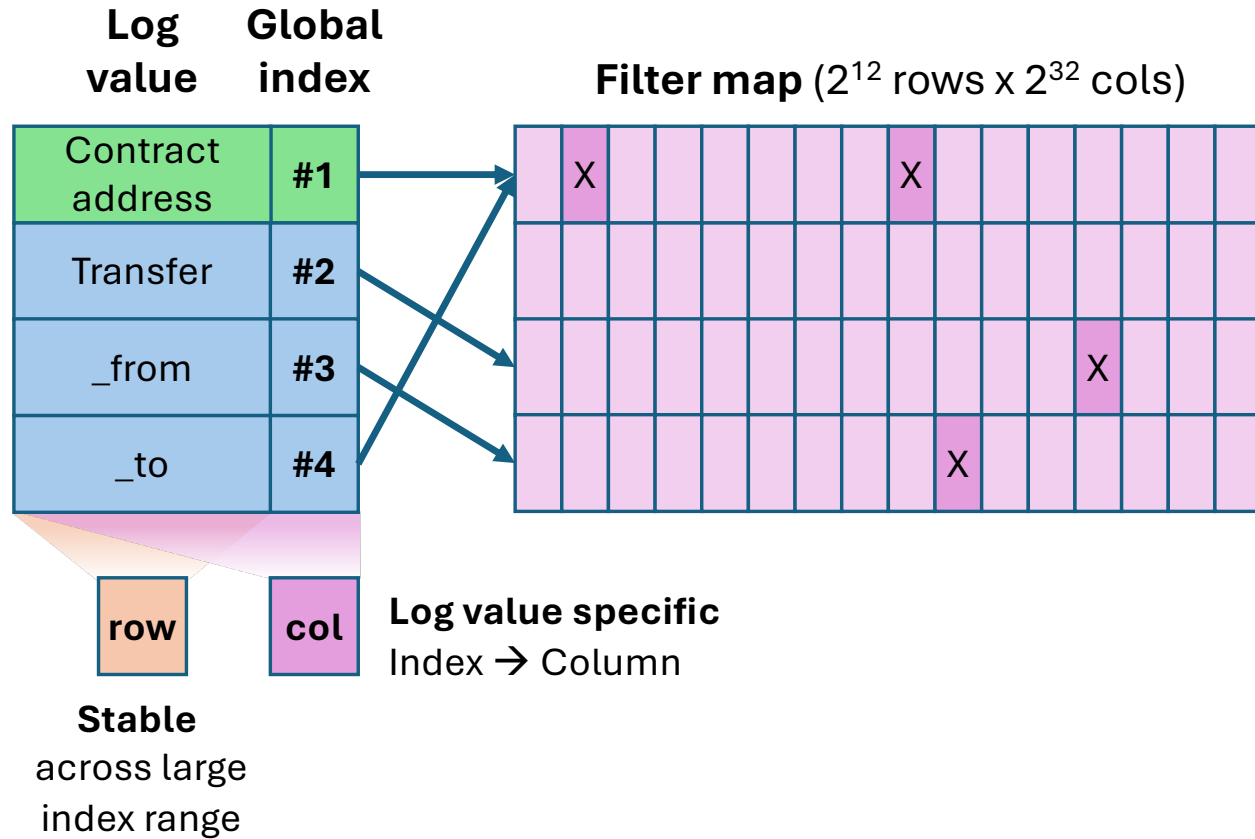
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





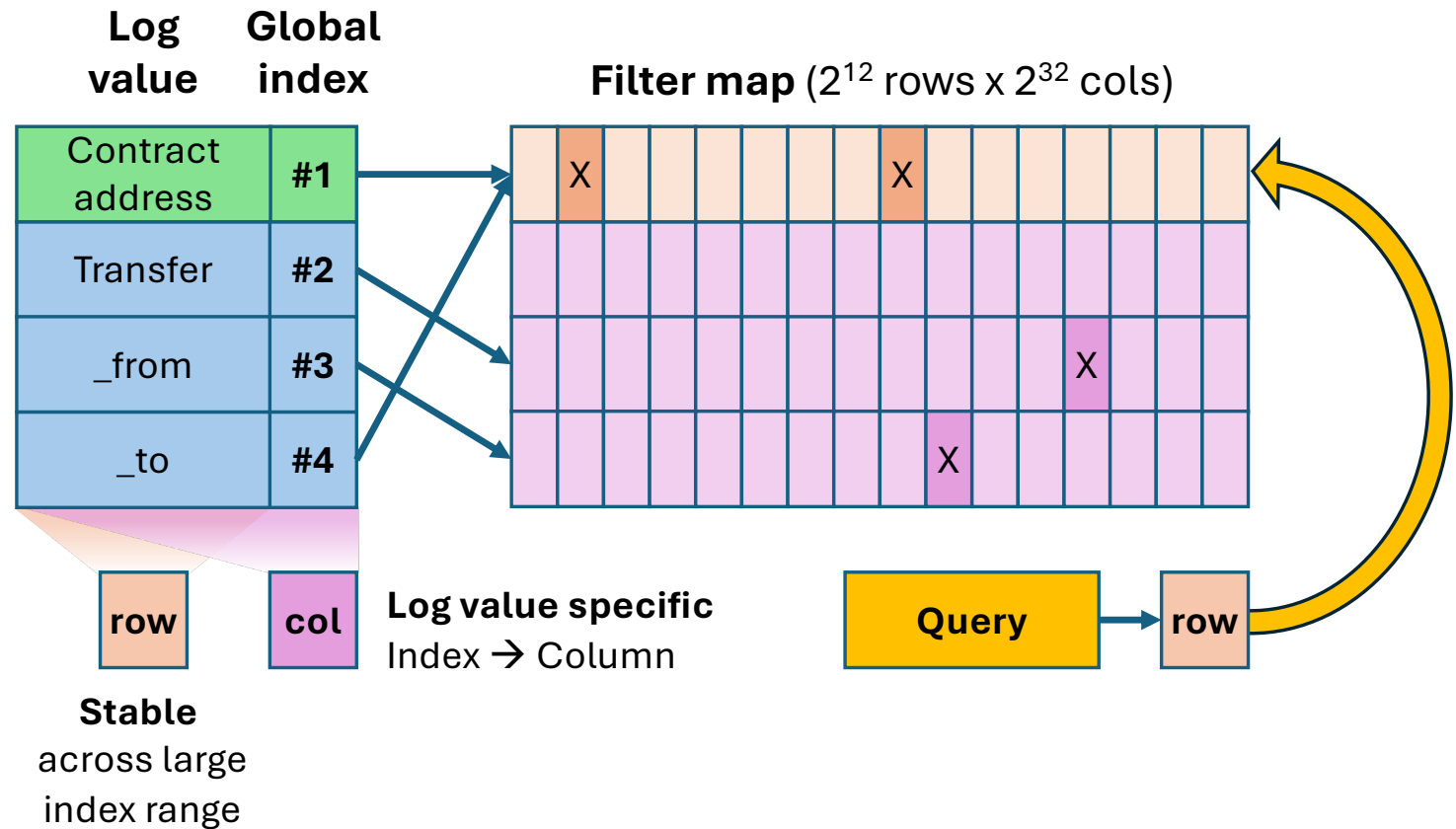
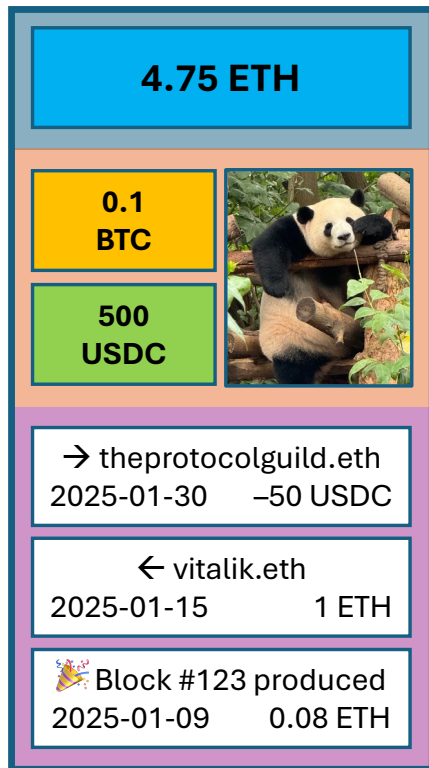
EIP-7745: Two dimensional log filter

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	



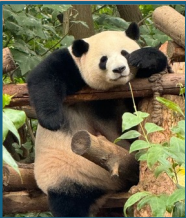


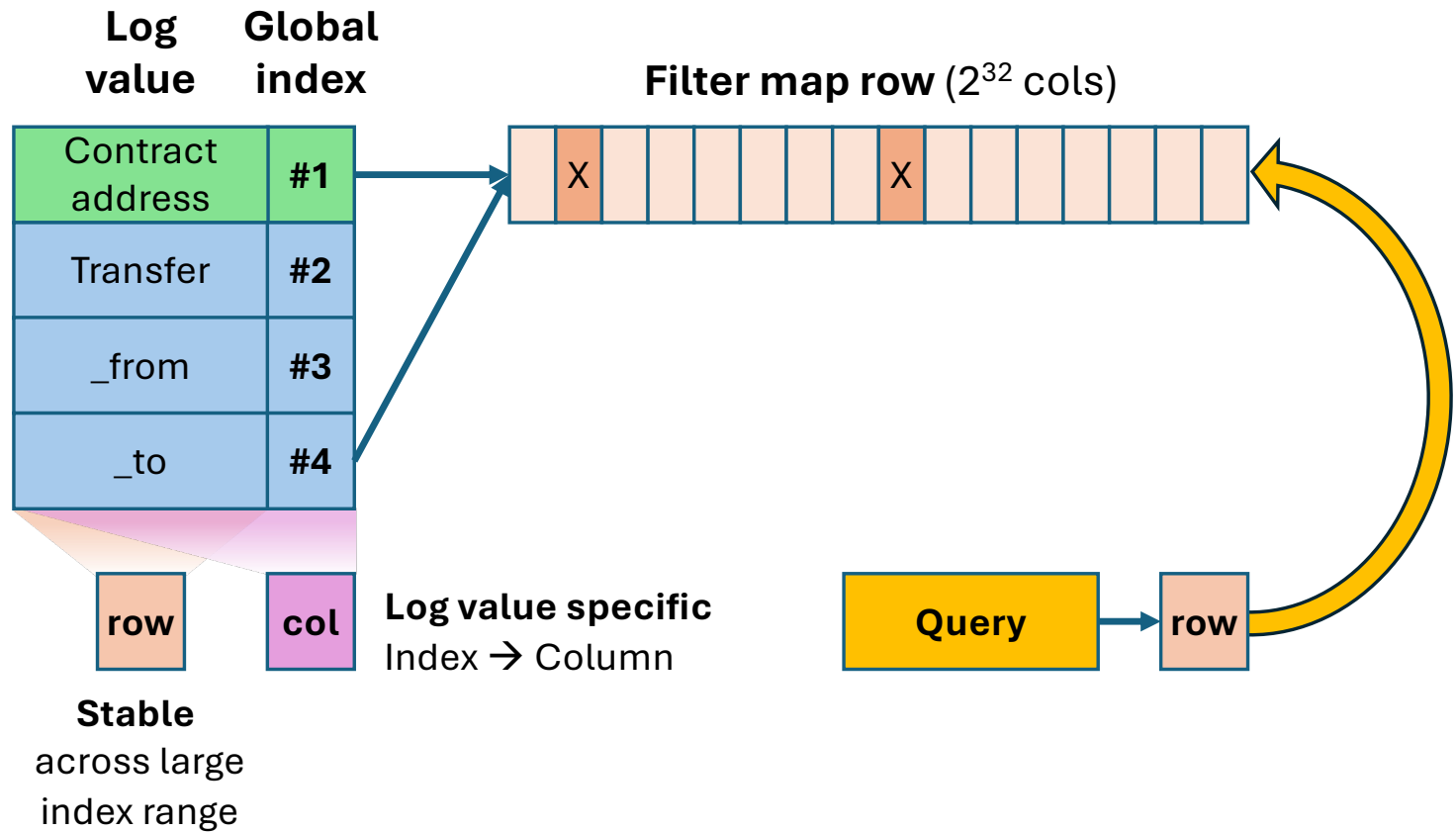
EIP-7745: Two dimensional log filter





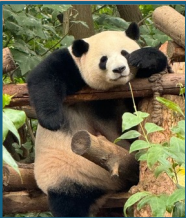
EIP-7745: Two dimensional log filter

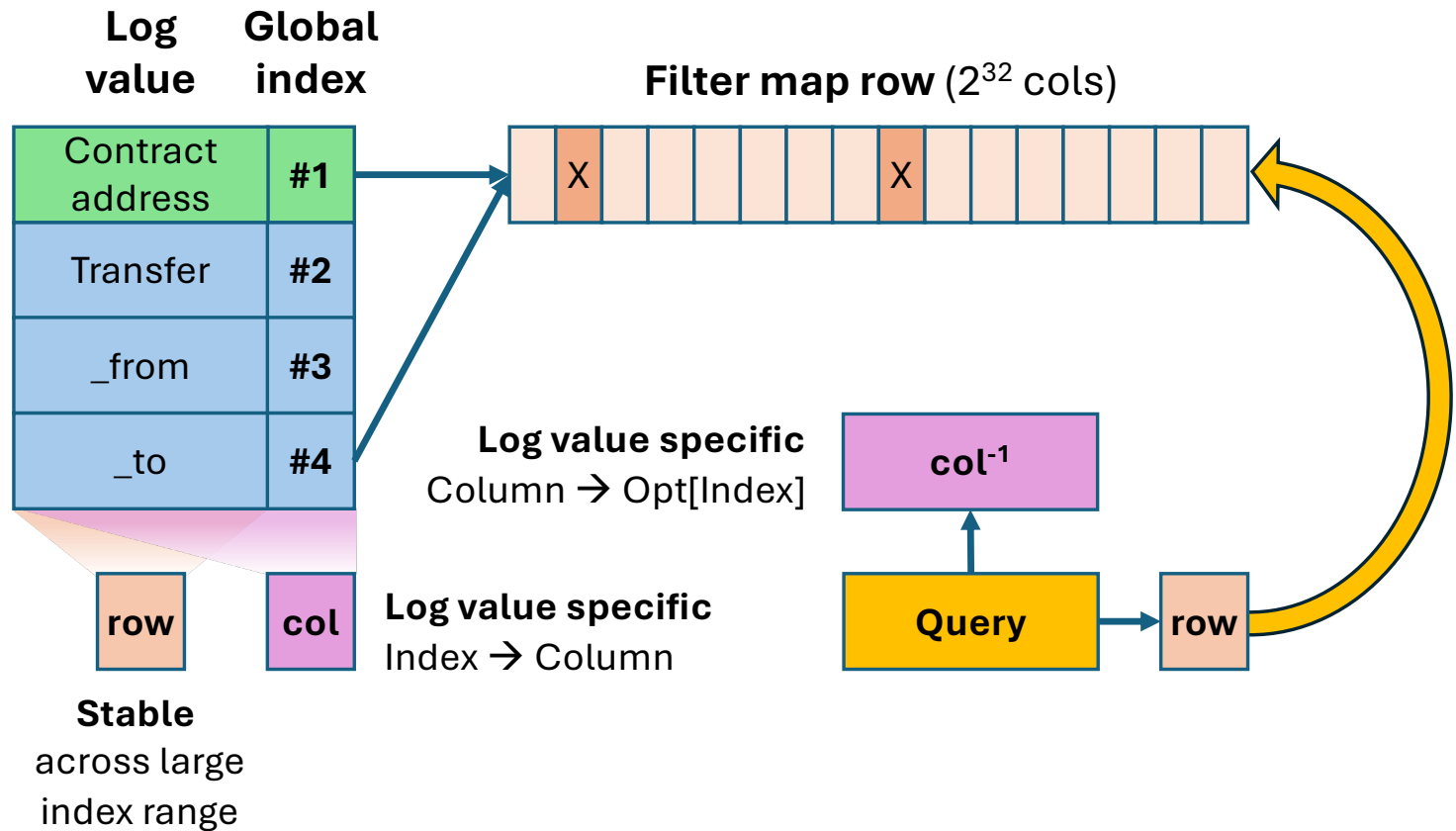
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





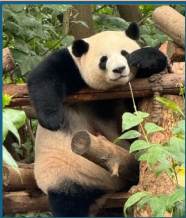
EIP-7745: Two dimensional log filter

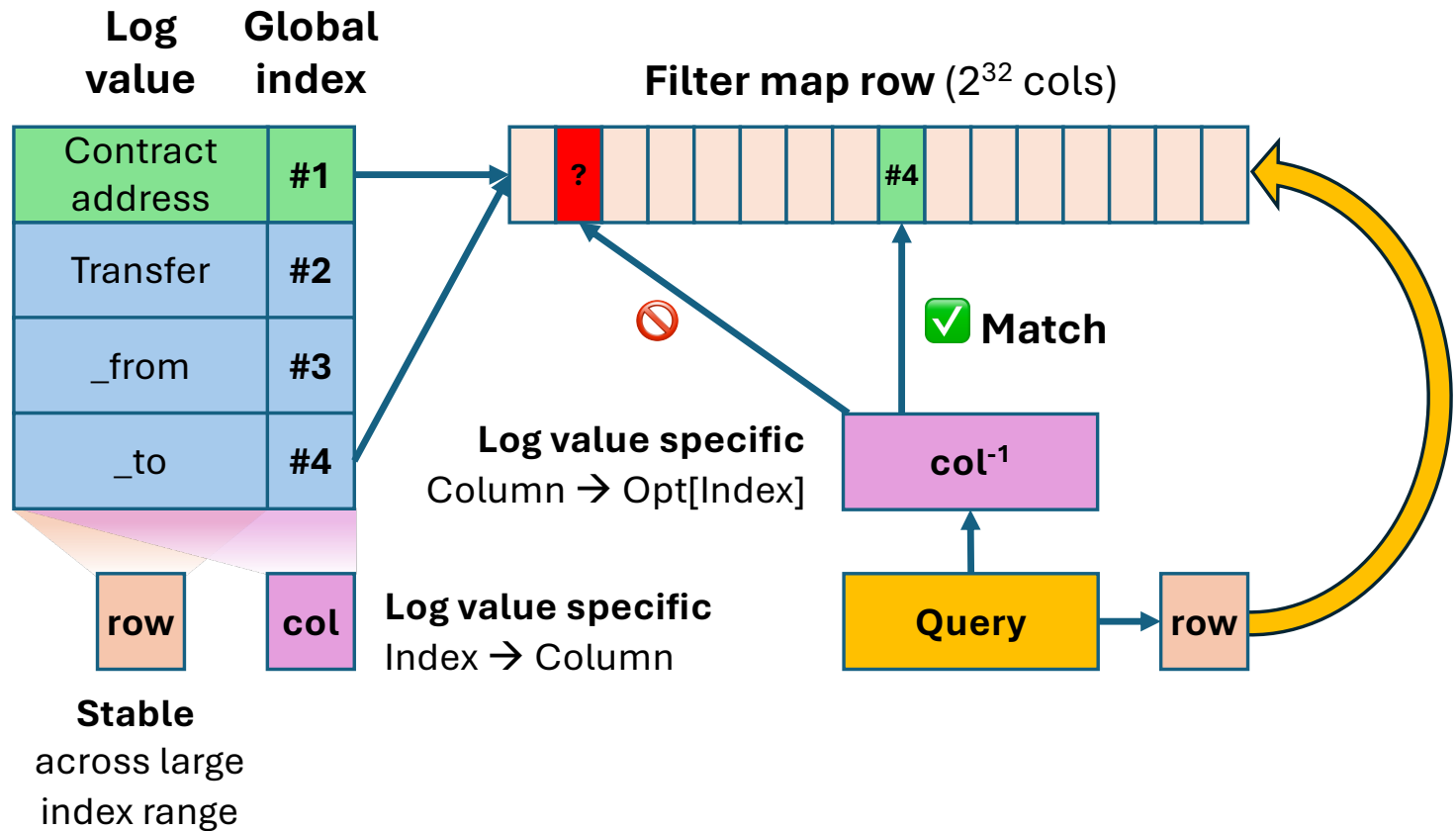
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





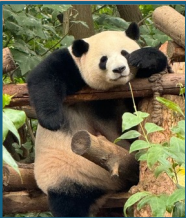
EIP-7745: Two dimensional log filter

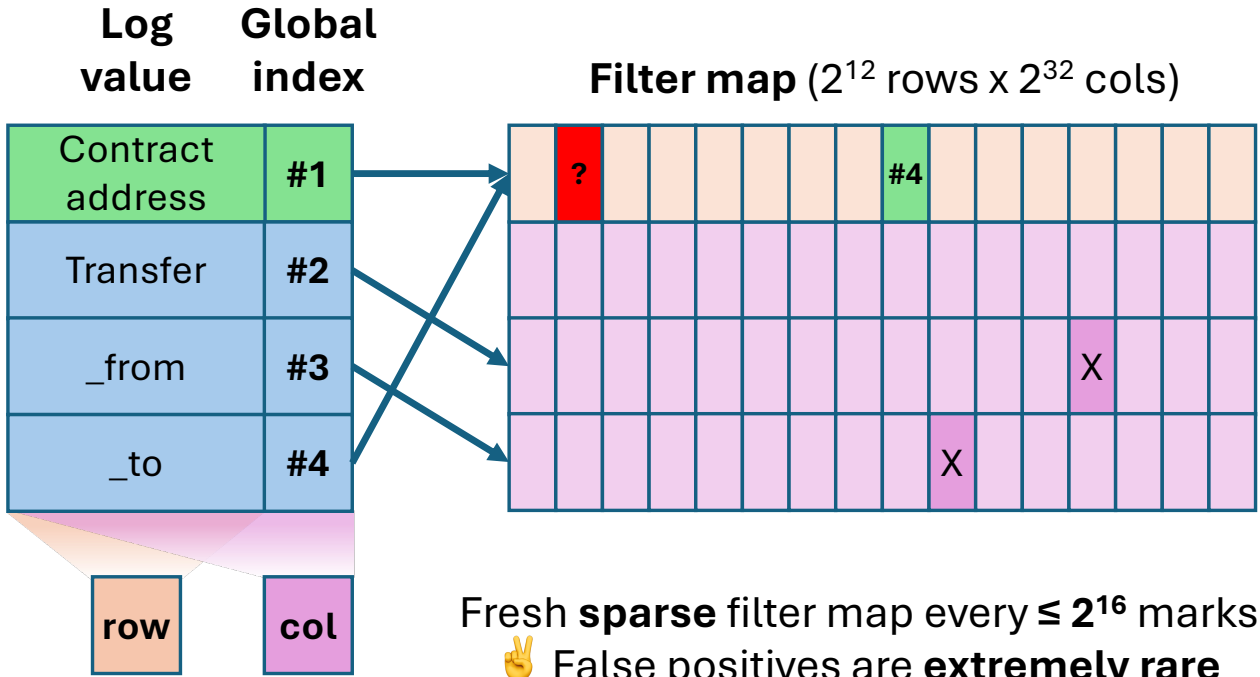
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	





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	

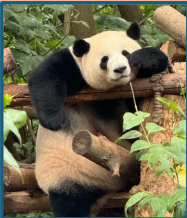


Fresh **sparse** filter map every ≤ 2¹⁶ marks
 🙌 False positives are **extremely rare**

Log value → Row transform **stable** across 2⁶ maps
 🙌 Efficient to fetch relevant rows



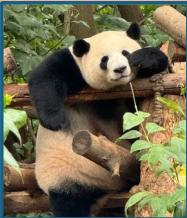
EIP-7745: Two dimensional log filter

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
<i>n/a</i>	
_value	



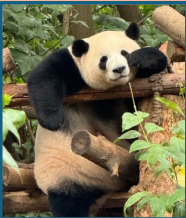
EIP-7745: Two dimensional log filter

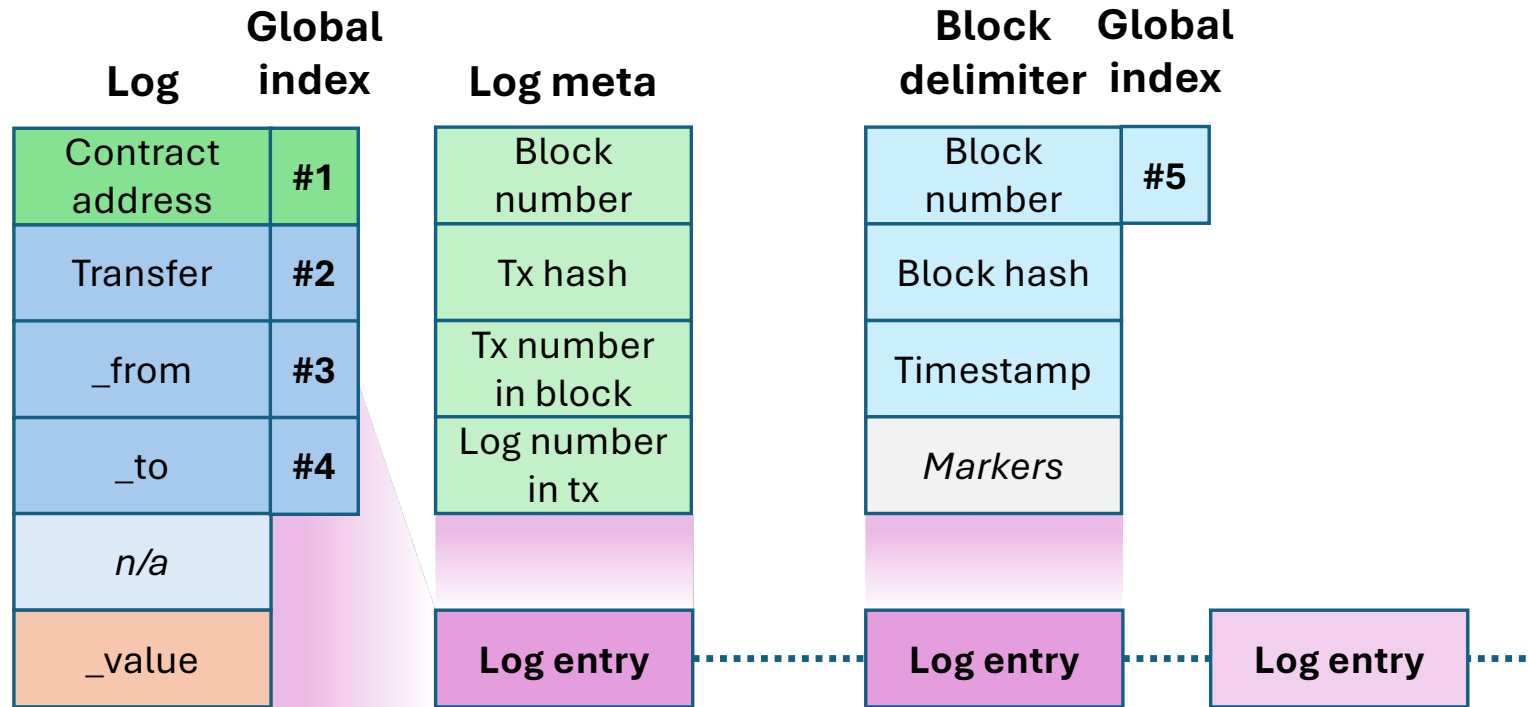
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	

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



EIP-7745: Two dimensional log filter

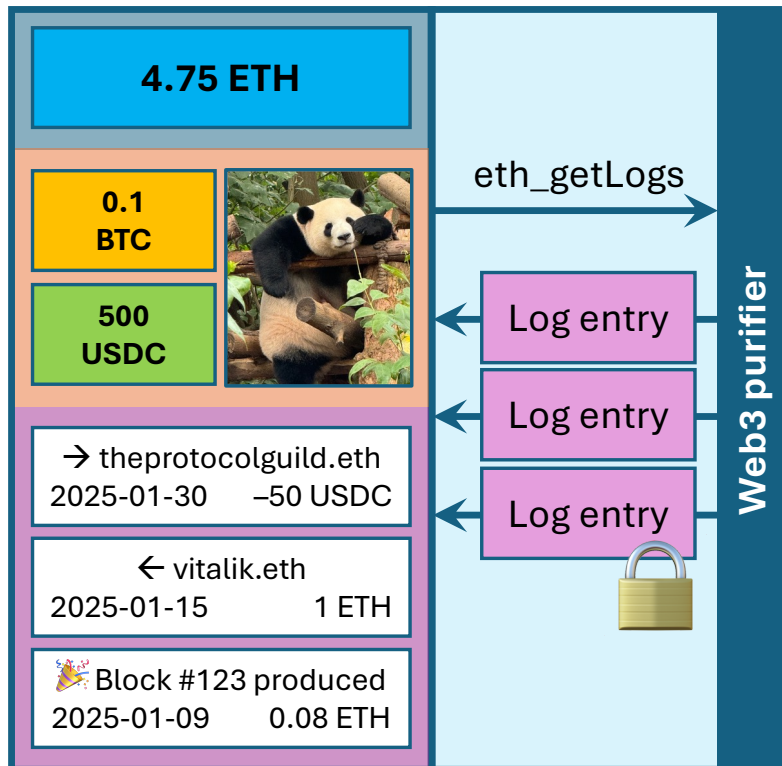
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	



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



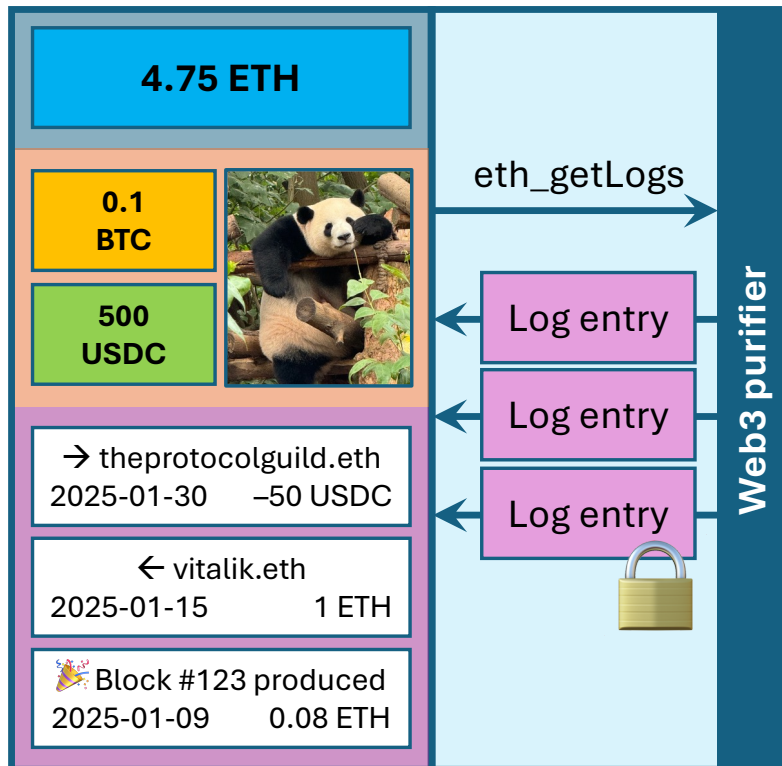
EIP-7745: Two dimensional log filter



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



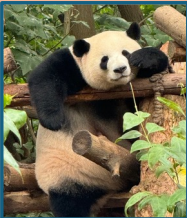
EIP-7745: Two dimensional log filter



- ✓ 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	n/a
n/a	n/a
_value	_value

Transfer log

Transaction start

Nonzero-value *CALL*

Nonzero-value *SELFDESTRUCT*

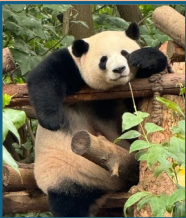
Fee log

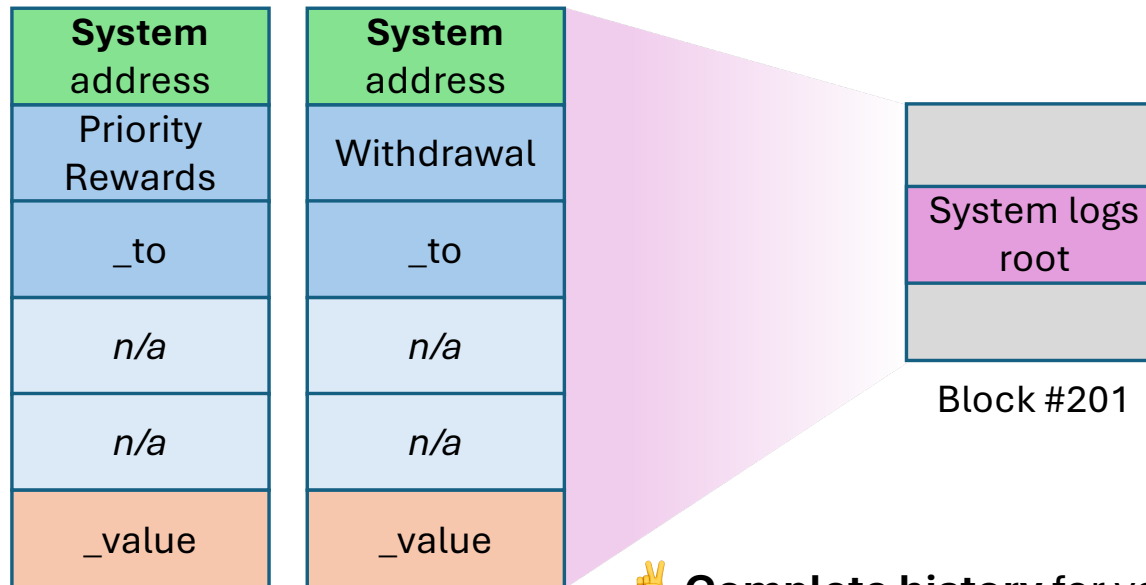
Transaction end

👌 **Complete history** for users



EIP-7799: System logs

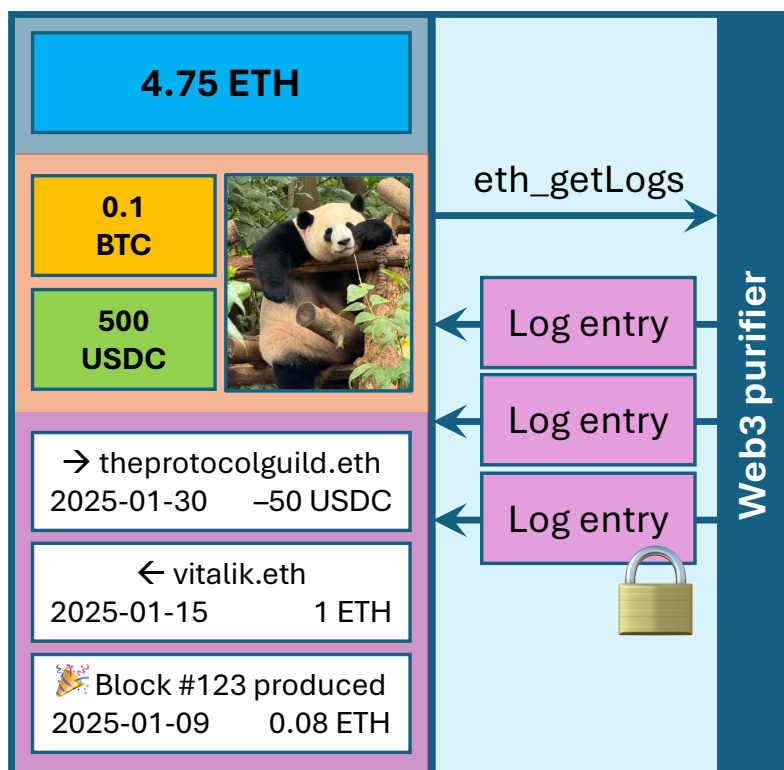
4.75 ETH	
0.1 BTC	
500 USDC	
→ theprotocolguild.eth 2025-01-30 -50 USDC	
← vitalik.eth 2025-01-15 1 ETH	
🎉 Block #123 produced 2025-01-09 0.08 ETH	



👌 **Complete history** for validator operators

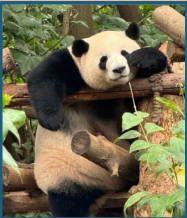


Purified web3



- ✓ ETH balance
- ✓ Tokens / NFTs
- ✓ History (complete)

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>