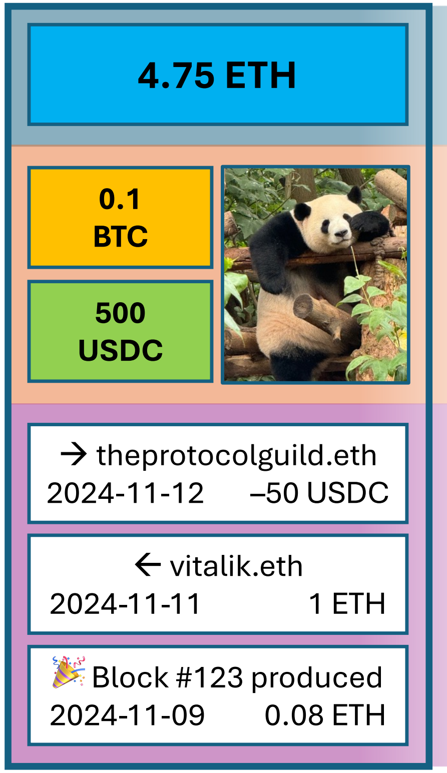
Verifying wallets

Devcon 2024 Bangkok

Wallet



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

ETH balance

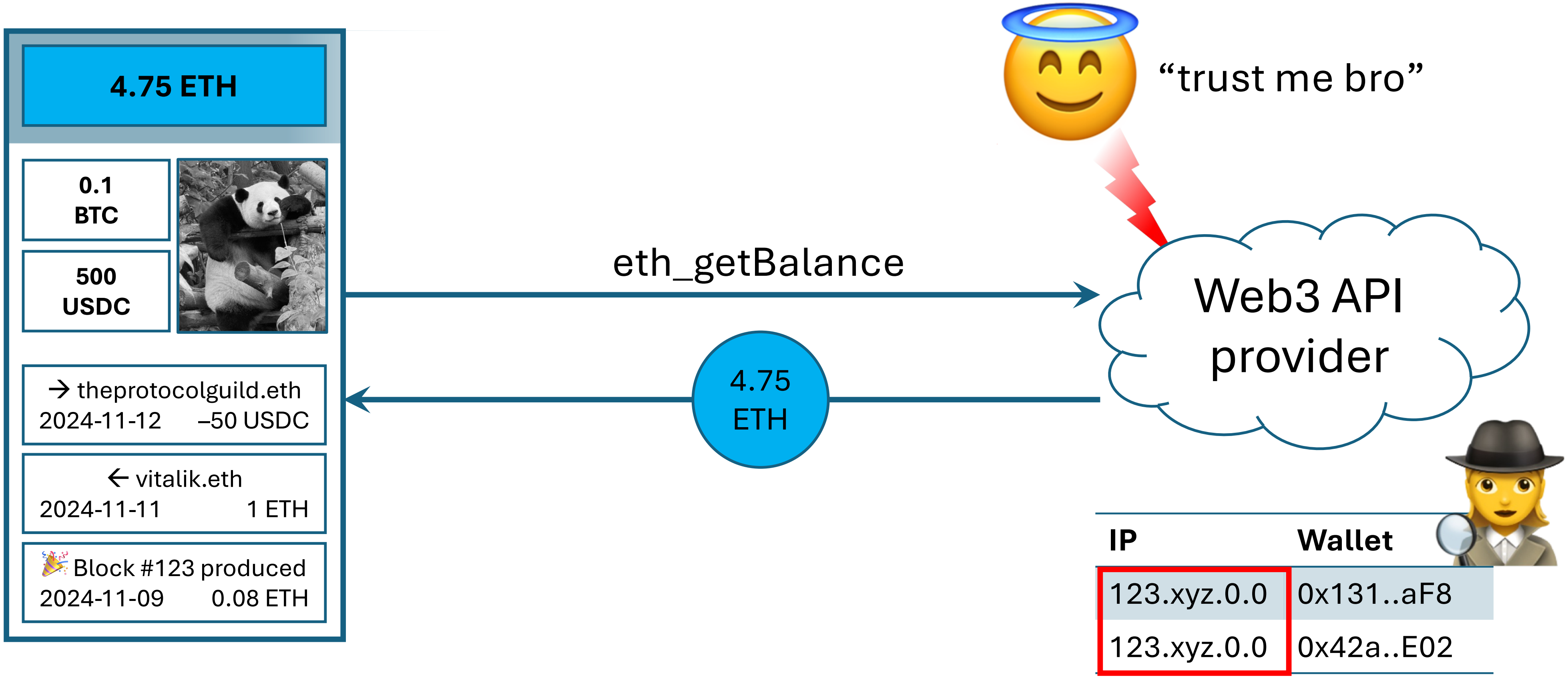
Tokens / NFTs

Metadata
Balances & allowances
Exchange rates

History

Transaction details
Fees & gas usage
Staking operations & rewards
No missing entries

ETH balance



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

eth_getBalance

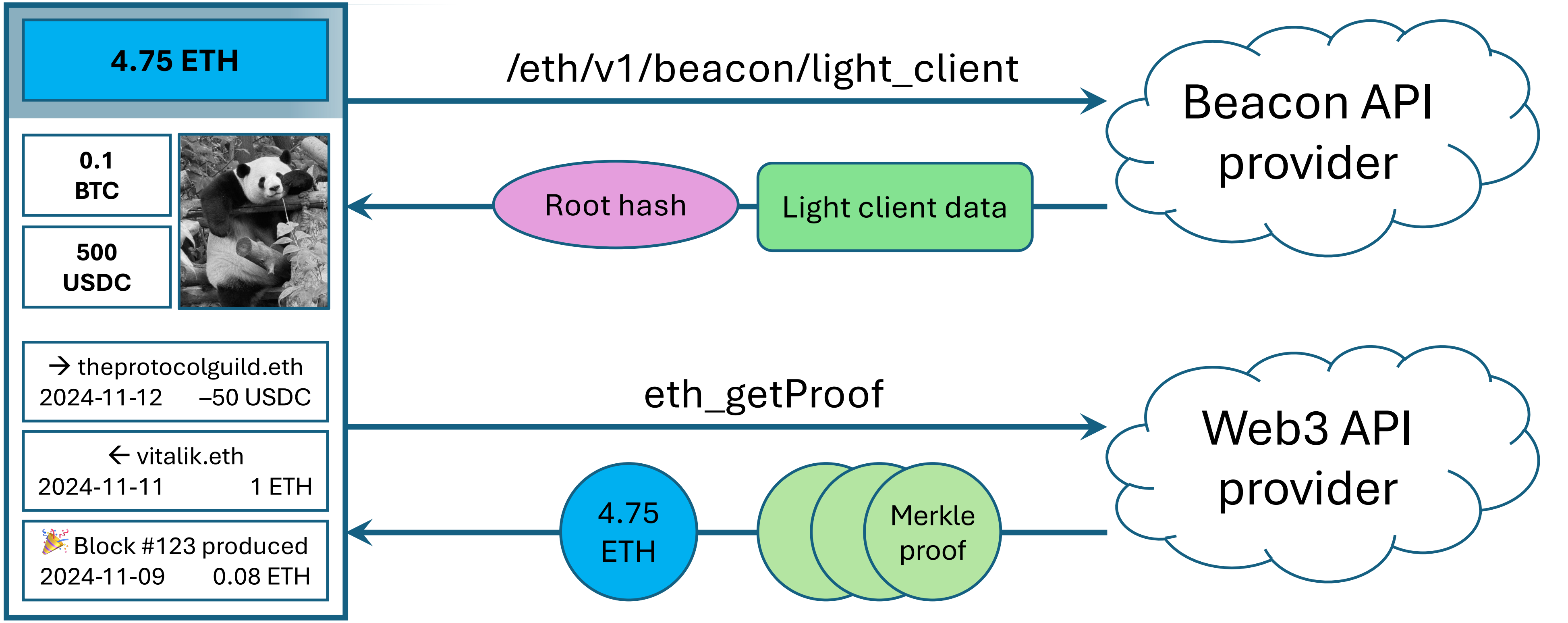
4.75 ETH

“trust me bro”

Web3 API provider

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

ETH balance (trust-minimized)



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

/eth/v1/beacon/light_client

Beacon API provider

Root hash

Light client data

eth_getProof

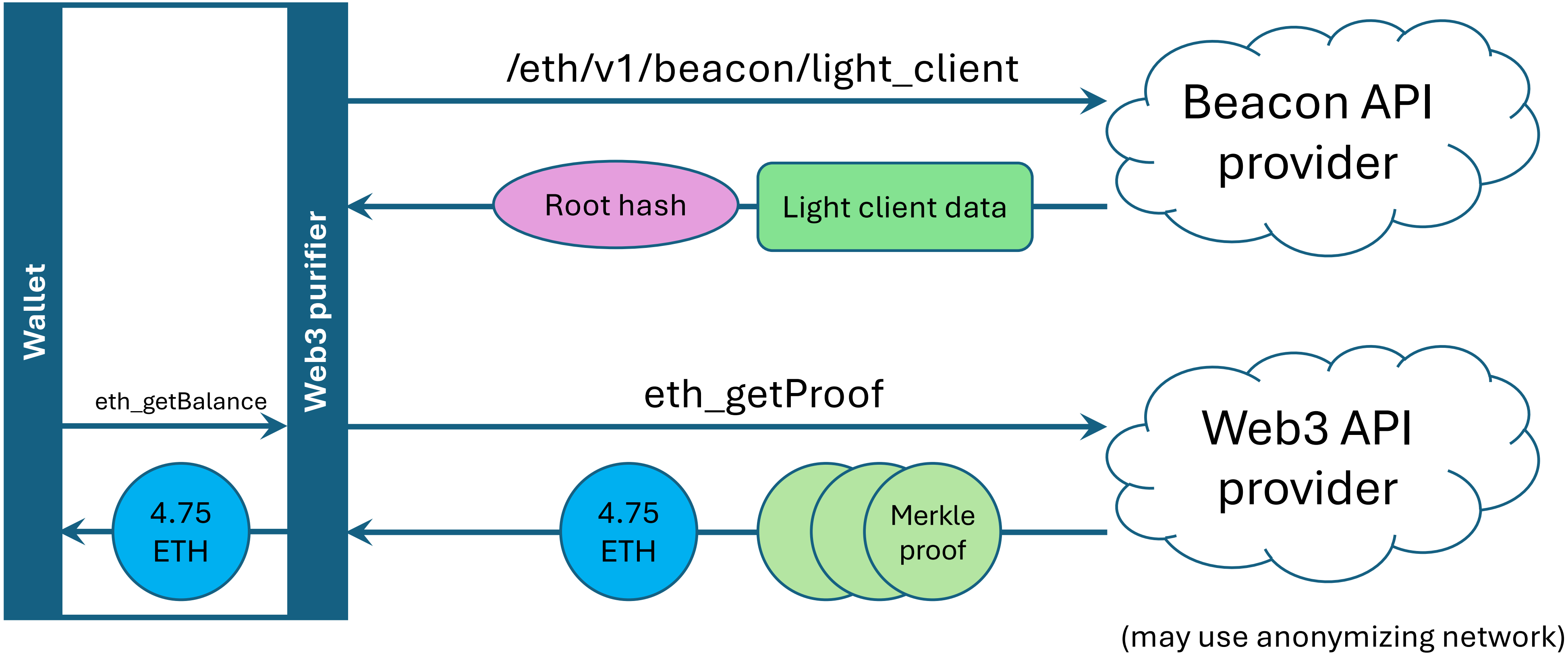
Web3 API provider

4.75 ETH

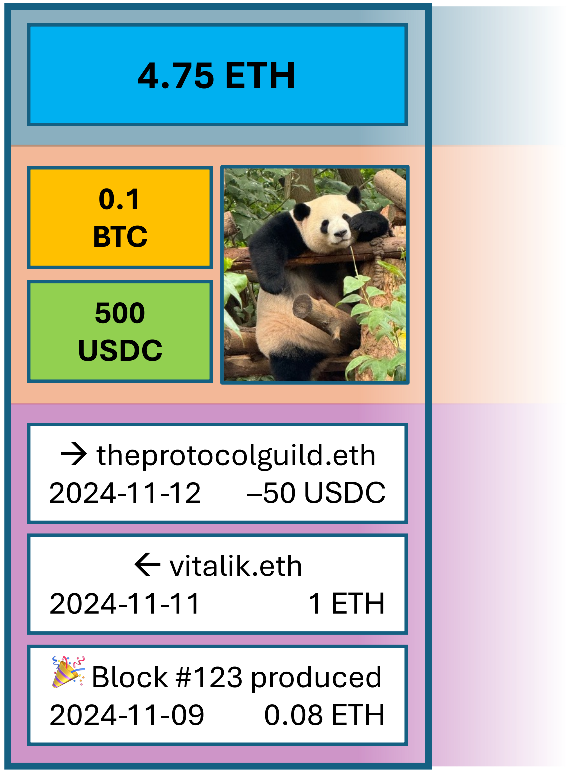
Merkle proof

(may use anonymizing network)

ETH balance (with purifier)



Wallet



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

ETH balance

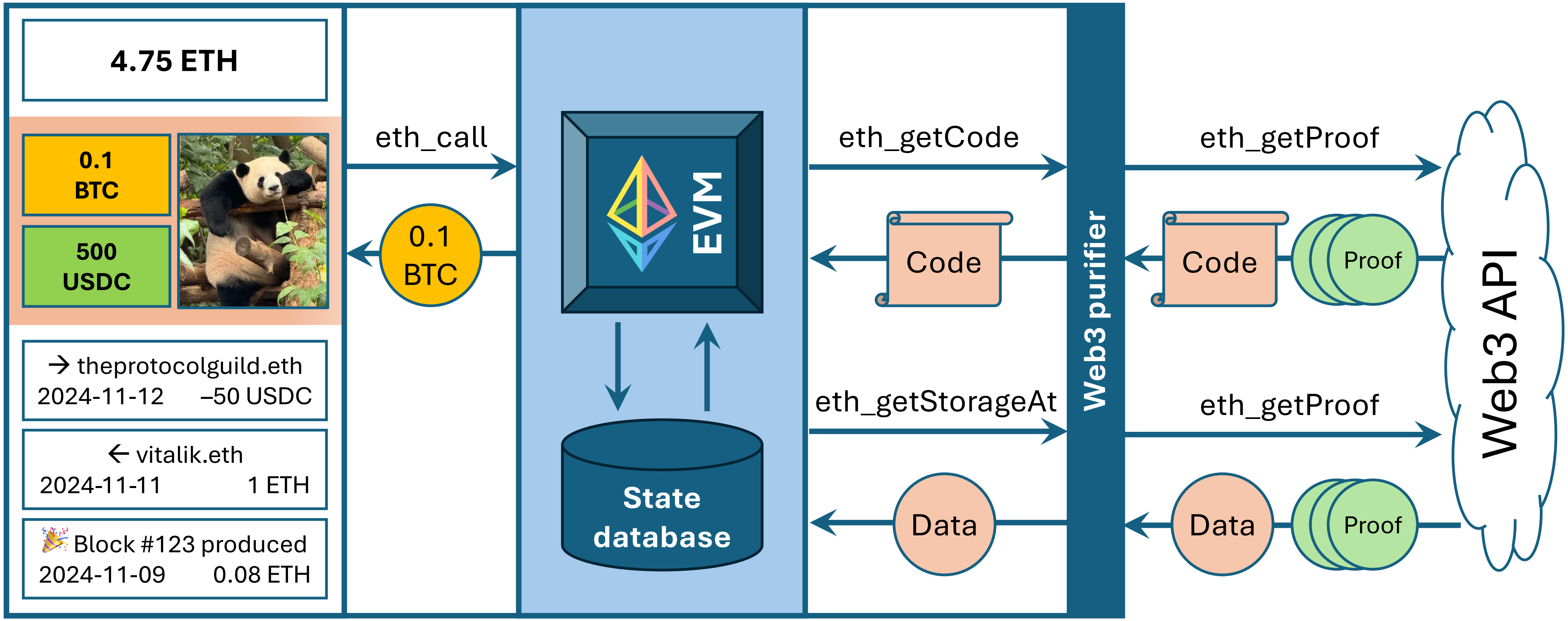
Tokens / NFTs

Metadata
Balances & allowances
Exchange rates

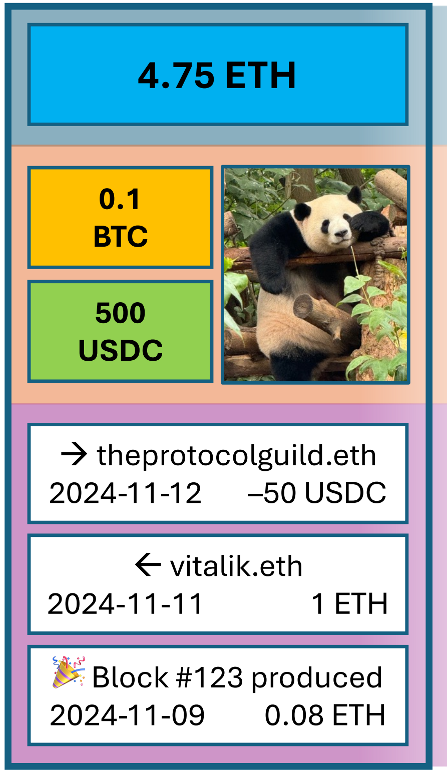
History

Transaction details
Fees & gas usage
Staking operations & rewards
No missing entries

Token balance



Wallet



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

ETH balance

🥰

Tokens / NFTs

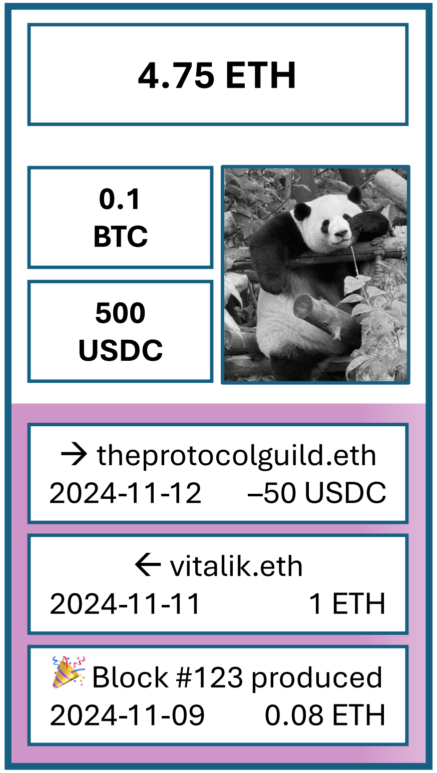
Metadata
Balances & allowances
Exchange rates

😕 Access lists are best effort
Lots of round trips

History

Transaction details
Fees & gas usage
Staking operations & rewards
No missing entries

Transaction details



4.75 ETH

0.1 BTC

500 USDC

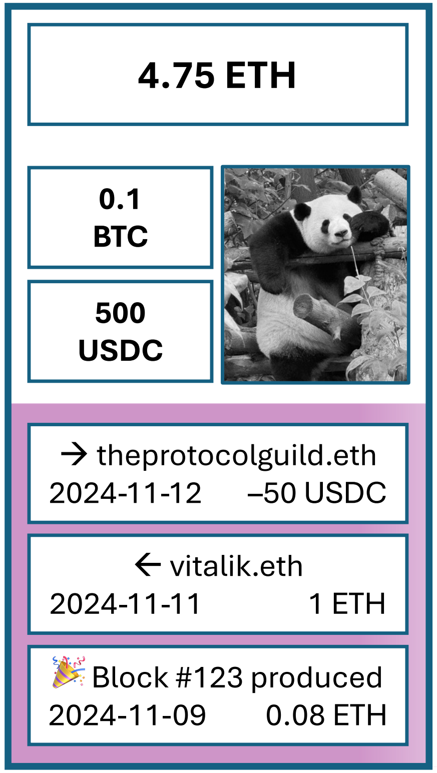
→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

- 📤 *From* address
- 📥 *To* address
- 💰 Value transferred
- 📆 Transaction data
- ⛽ Gas fees

Transaction details



4.75 ETH

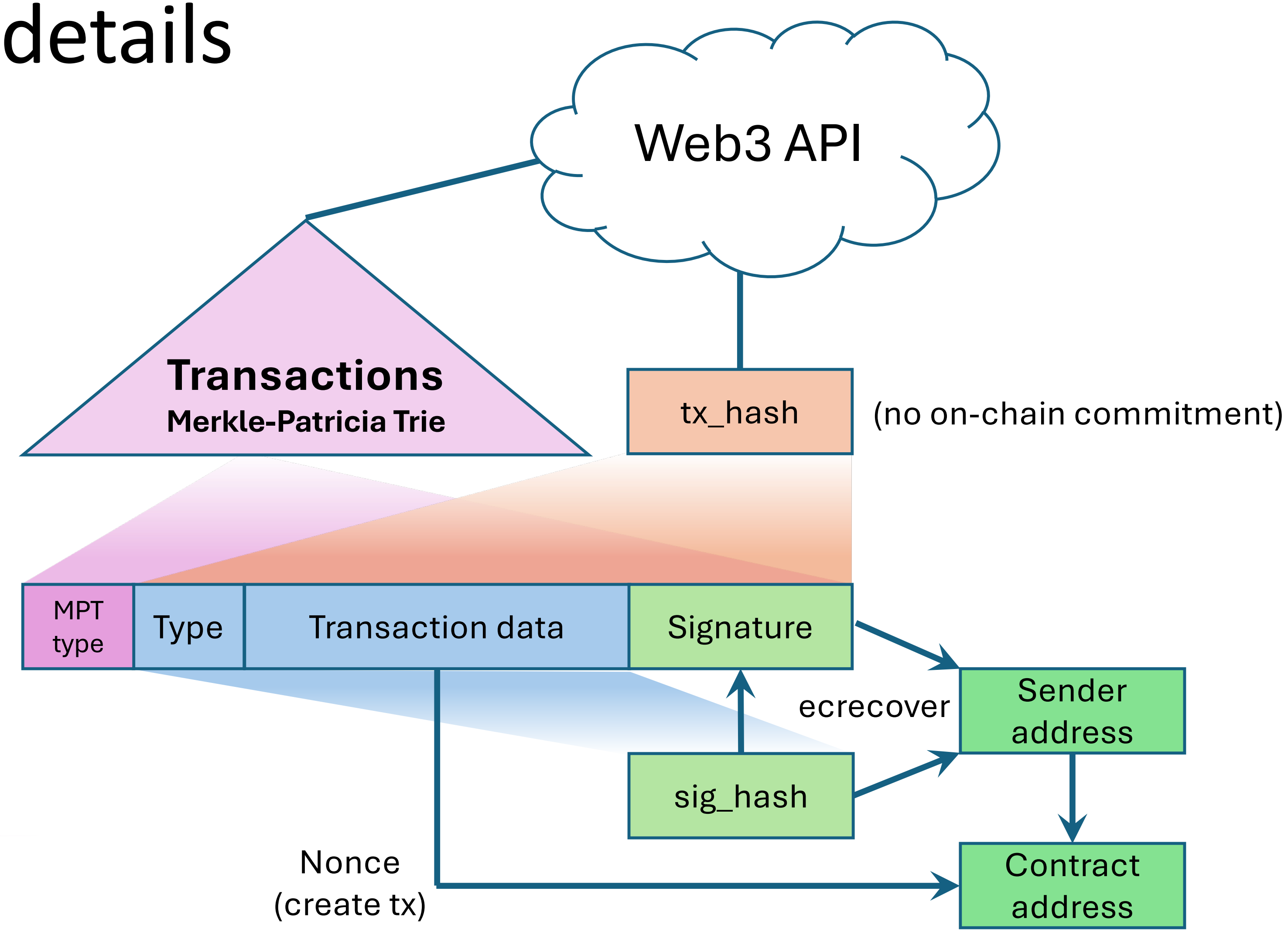
0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH



Web3 API

Transactions

Merkle-Patricia Trie

tx_hash

(no on-chain commitment)

MPT type

Type

Transaction data

Signature

ecrecover

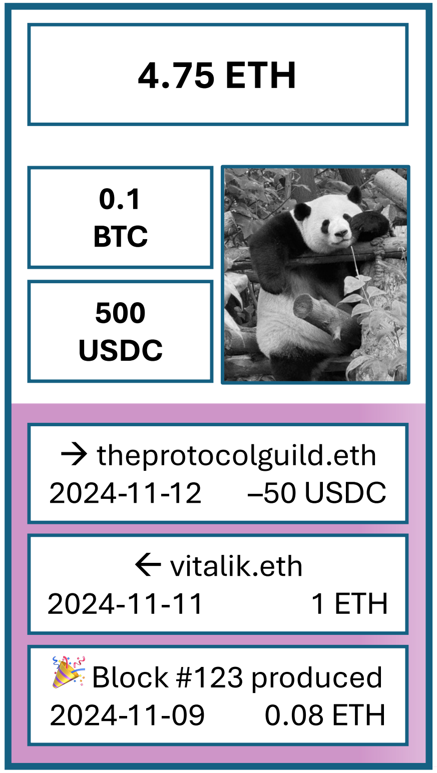
Sender address

sig_hash

Nonce
(create tx)

Contract address

Transaction details



4.75 ETH

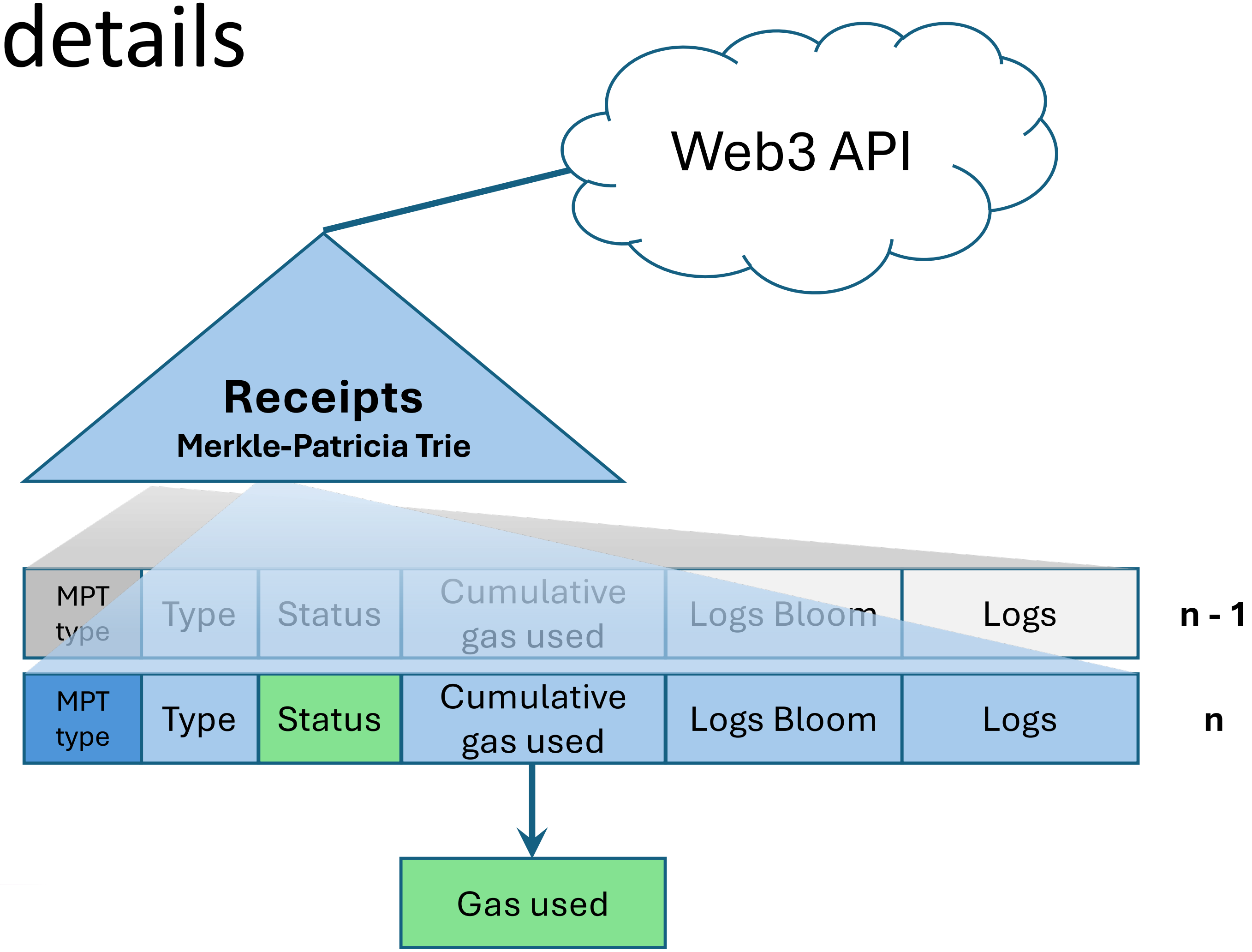
0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

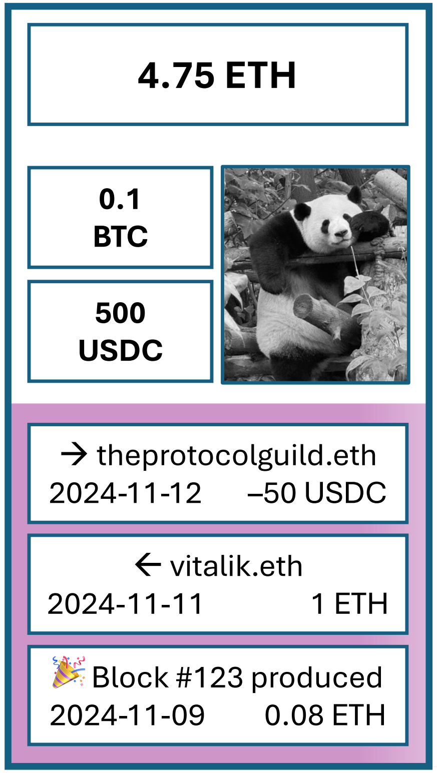
← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH



MPT type	Type	Status	Cumulative gas used	Logs Bloom	Logs	
MPT type	Type	Status	Cumulative gas used	Logs Bloom	Logs	**n - 1**
MPT type	Type	Status	Cumulative gas used	Logs Bloom	Logs	**n**

Transaction details



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

From address

Full tx data required
Expensive ecrecover

To address

CREATE contract address
requires *from* address

Value transferred

Transaction date

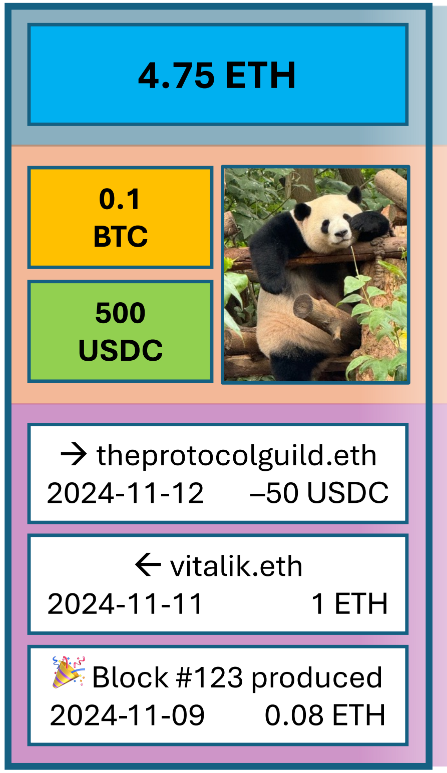
✅

Tx type inconsistencies
Inefficient hashes

Gas fees

Full data required incl logs
Prior receipt needed

Wallet



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

ETH balance

🥰

Tokens / NFTs

Metadata
Balances & allowances
Exchange rates

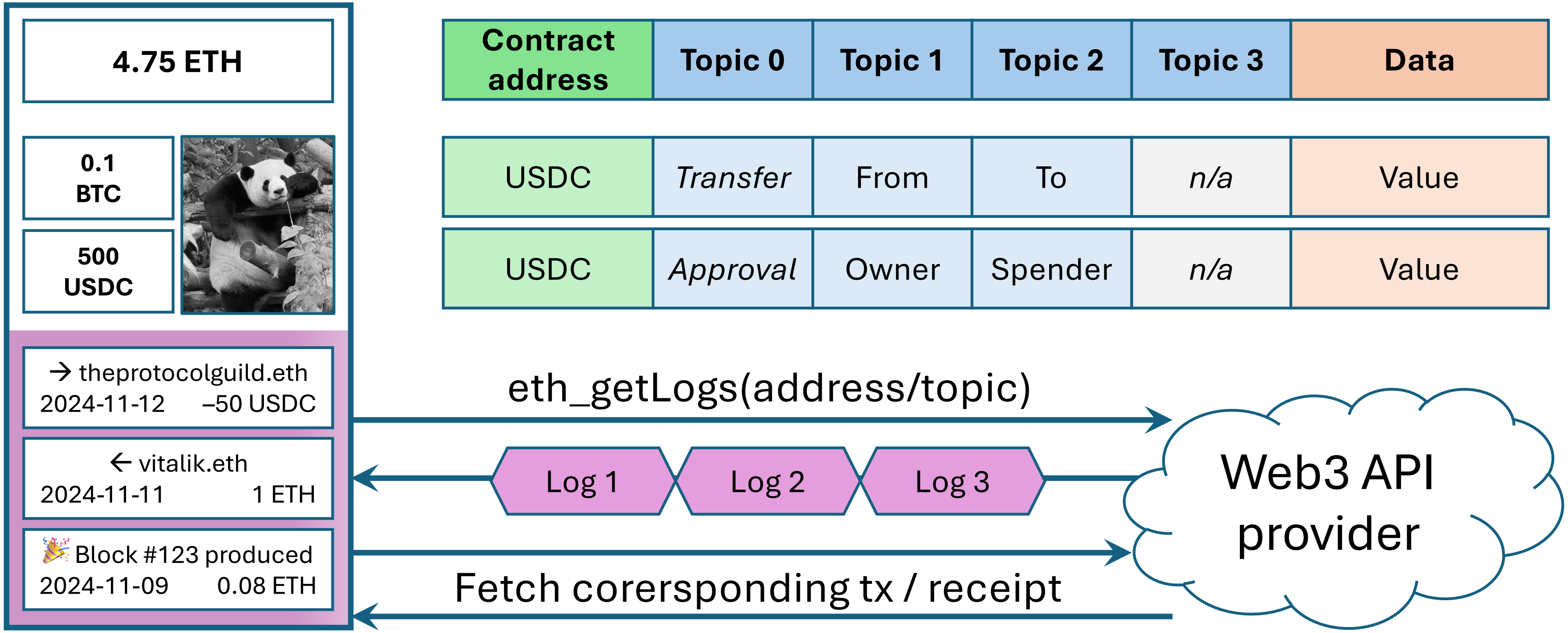
🫤 Access lists are best effort
Lots of round trips

History

Transaction details
Fees & gas usage
Staking operations & rewards
No missing entries

🤯

History



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

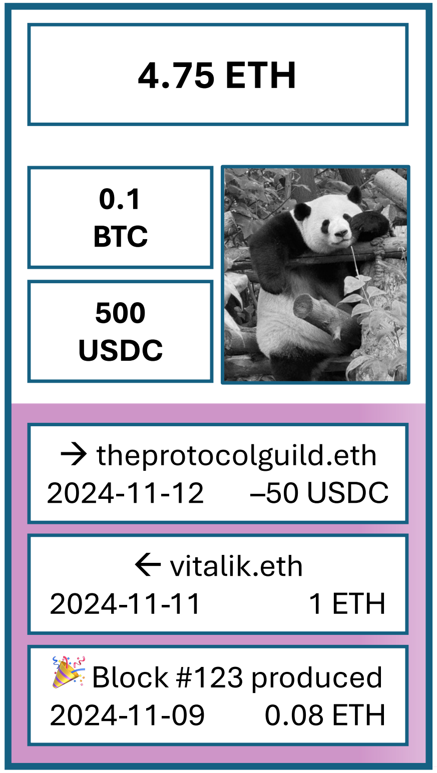
🎉 Block #123 produced
2024-11-09 0.08 ETH

Contract address	Topic 0	Topic 1	Topic 2	Topic 3	Data
USDC	*Transfer*	From	To	*n/a*	Value
USDC	*Approval*	Owner	Spender	*n/a*	Value

eth_getLogs(address/topic)

Fetch corersponding tx / receipt

History (withholding mitigation)



4.75 ETH

0.1 BTC

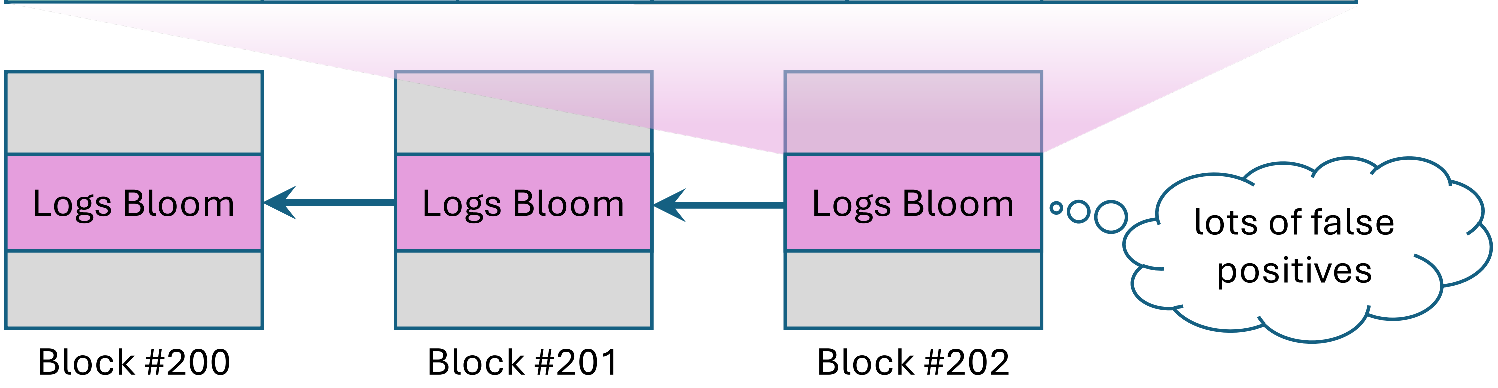
500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

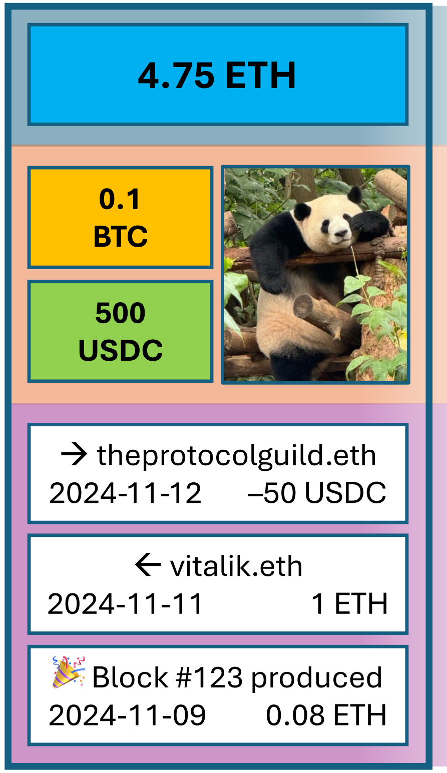
🎉 Block #123 produced
2024-11-09 0.08 ETH

Contract address	Topic 0	Topic 1	Topic 2	Topic 3	Data
USDC	*Transfer*	From	To	*n/a*	Value
USDC	*Approval*	Owner	Spender	*n/a*	Value



⚠️ **Get *all* block headers, check Bloom, get *all* transactions / receipts…**

Wallet



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

ETH balance

🥰

Tokens / NFTs

Metadata
Balances & allowances
Exchange rates

😕 Access lists are best effort
Lots of round trips

History

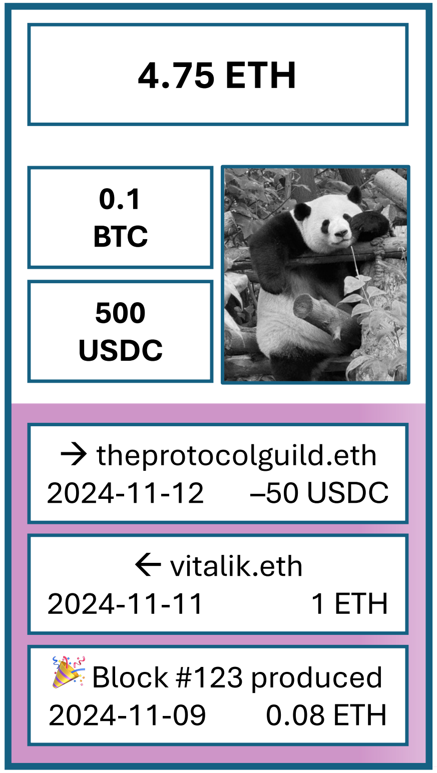
Transaction details
Fees & gas usage
Staking operations & rewards
No missing entries

🤯

😡 Terribly inefficient

🚫 ETH transfers
from smart contracts

EIP-7708: ETH transfers emit a log



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

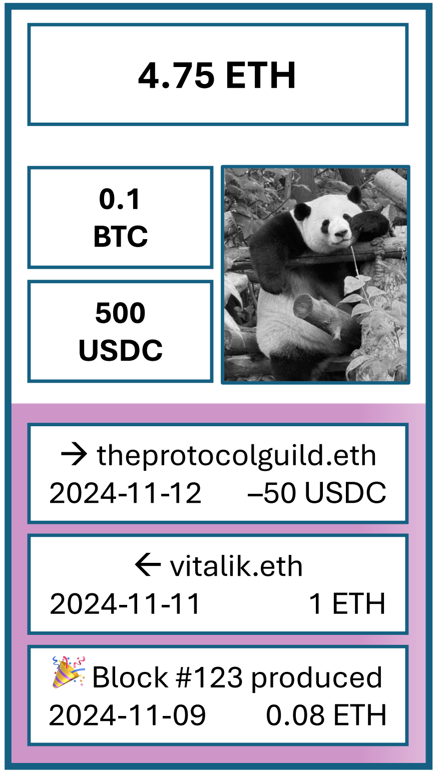
Contract address	Topic 0	Topic 1	Topic 2	Topic 3	Data
System	*Transfer*	From	To	*n/a*	Value
System	*Fee*	From	*n/a*	*n/a*	Value

Transfer log
Transaction start
Nonzero-value *CALL*
Nonzero-value *SELFDESTRUCT*

Fee log
Transaction end

✅ **Accurate ETH balance history is available (without local EVM)**

EIP-7668: Remove bloom filters



4.75 ETH

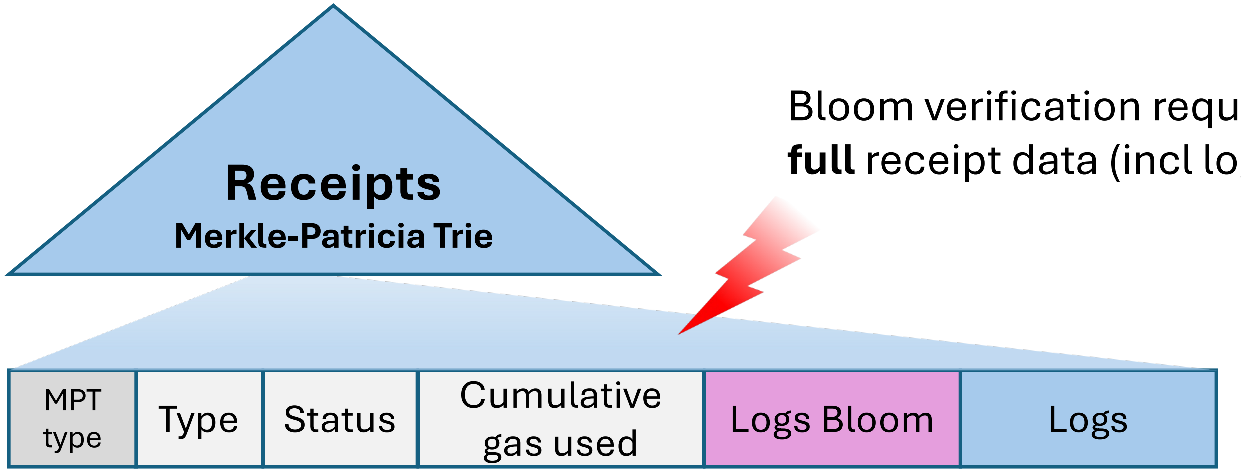
0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH



MPT type	Type	Status	Cumulative gas used	Logs Bloom	Logs

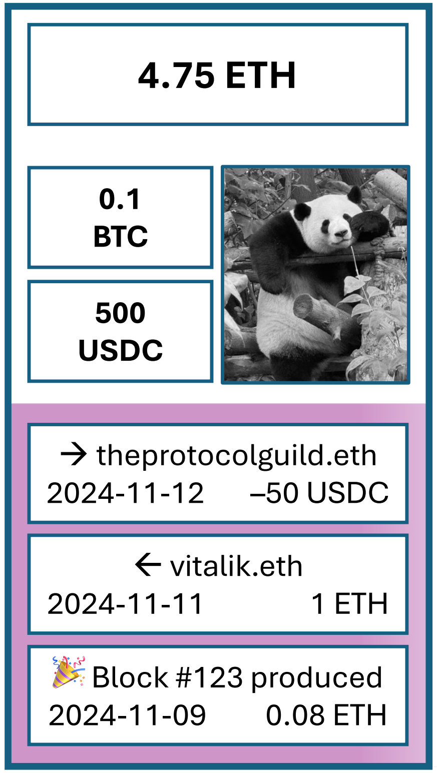
Bloom verification requires **full** receipt data (incl logs)

Remove Logs Bloom
Saves 256 bytes per transaction

✅ **ETH transfer logs can be stored in saved disk space**

EIP-7792: Verifiable logs

EIP-7745: Two dimensional
log filter data structure



4.75 ETH

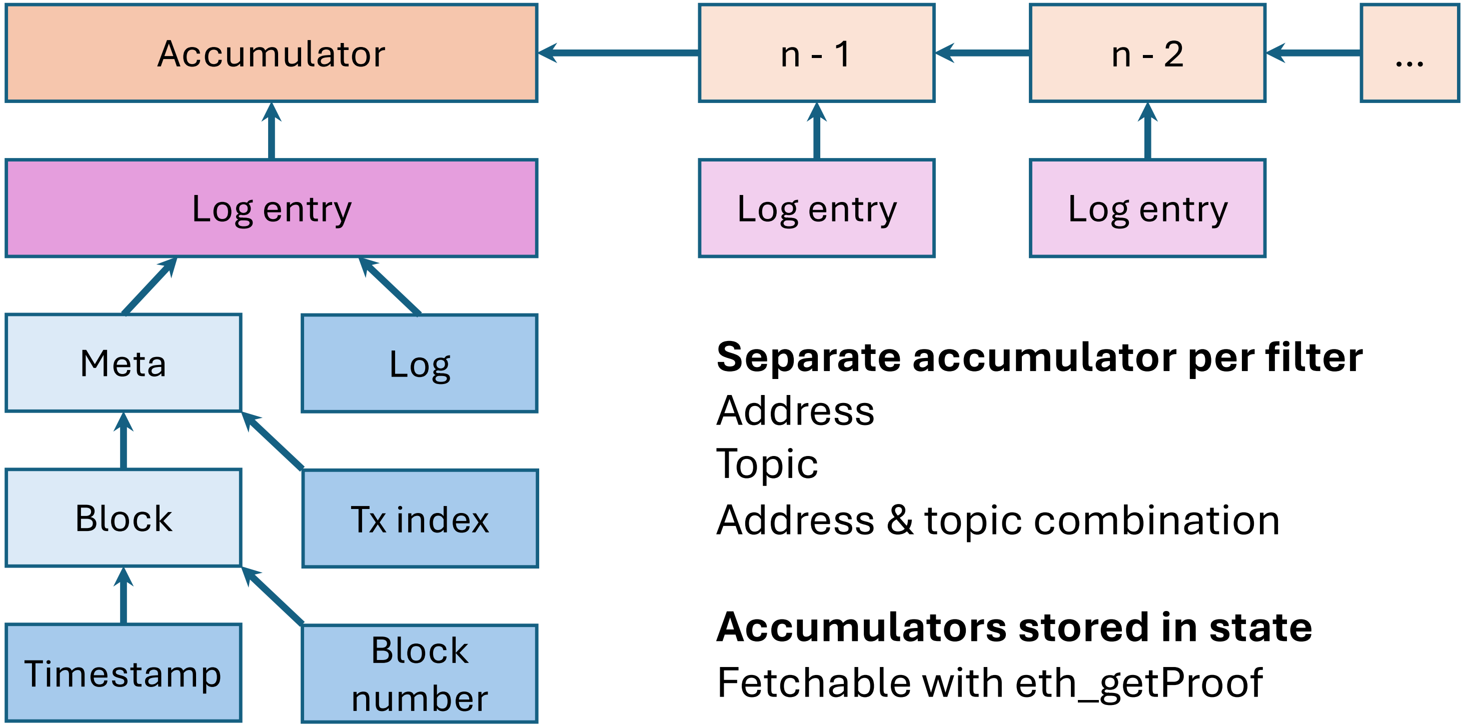
0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH



Accumulator

n - 1

n - 2

...

Log entry

Log entry

Log entry

Meta

Log

Block

Tx index

Timestamp

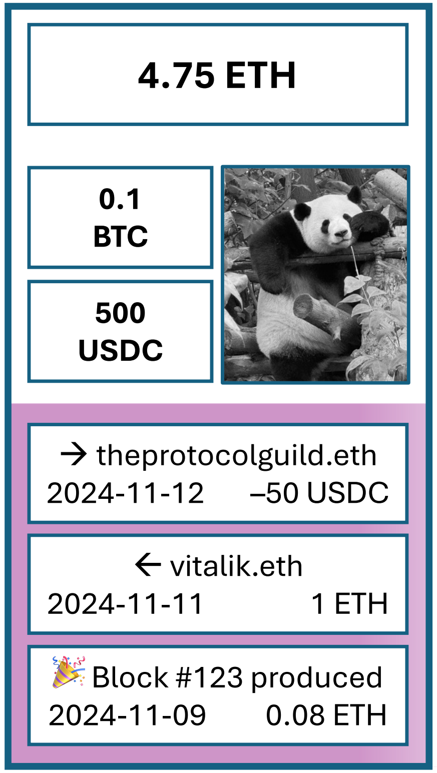
Block number

Separate accumulator per filter
Address
Topic
Address & topic combination

Accumulators stored in state
Fetchable with eth_getProof

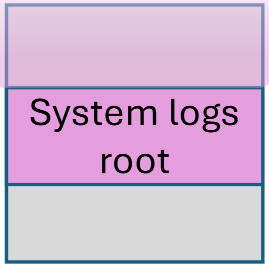
✅ **Incomplete eth_getLogs responses can be detected**

EIP-7799: System logs



Contract address	Topic 0	Topic 1	Topic 2	Topic 3	Data
System	*Priority Rewards*	To	*n/a*	*n/a*	Value
System	*With-drawal*	To	*n/a*	*n/a*	Value

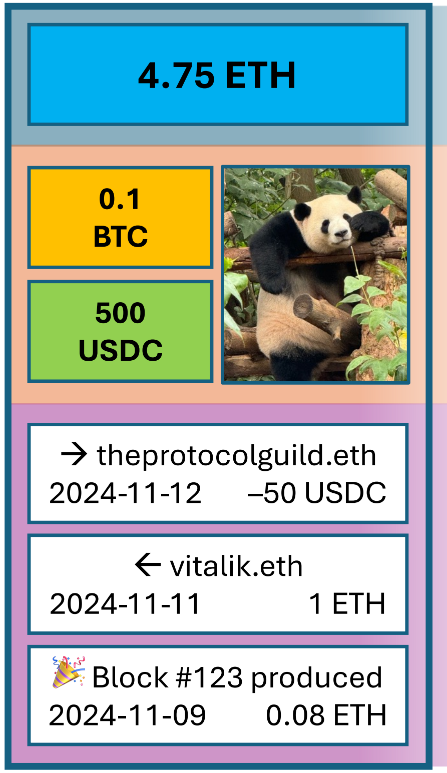
Priority Fees (EIP-1559)
No longer paid after each tx
Single combined credit after all txs
Better parallel tx execution



Block #456

✅ **Accurate staking reward tracking (without historical block headers)**

Wallet



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

ETH balance

🥰

Tokens / NFTs

Metadata
Balances & allowances
Exchange rates

😕 Access lists are best effort
Lots of round trips

History

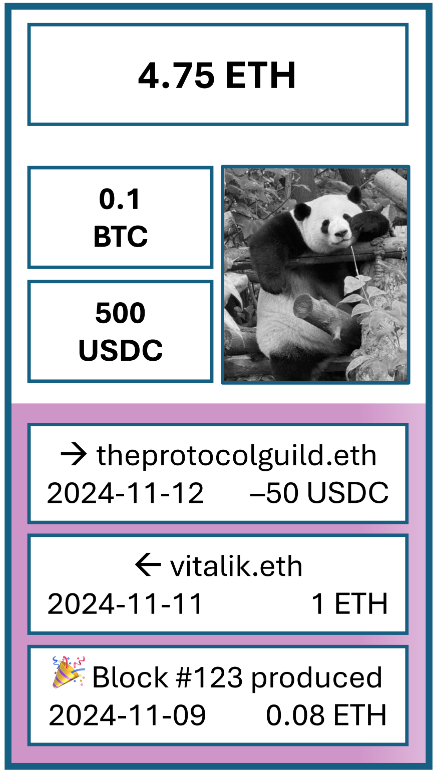
Transaction details
Fees & gas usage
Staking operations & rewards
No missing entries

🤯

😡 Terribly inefficient

🚫 ETH transfers
from smart contracts

EIP-6466: SSZ receipts



4.75 ETH

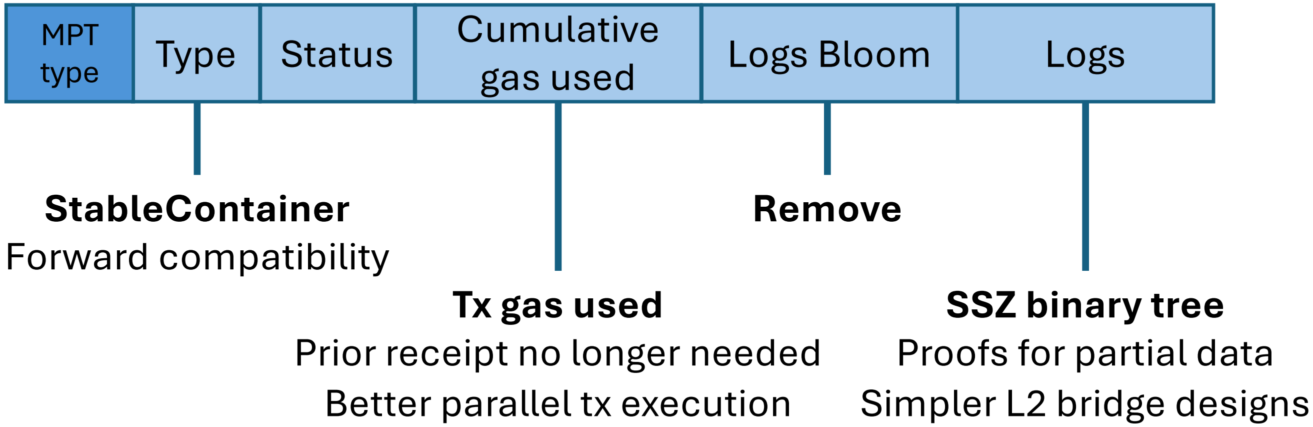
0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 −50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH



MPT type | Type | Status | Cumulative gas used | Logs Bloom | Logs

StableContainer
Forward compatibility

Tx gas used
Prior receipt no longer needed
Better parallel tx execution

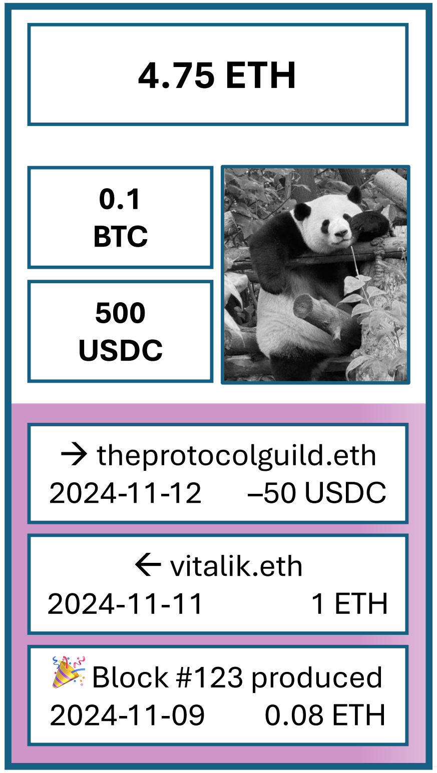
Remove

SSZ binary tree
Proofs for partial data
Simpler L2 bridge designs

Add *From*, *Contract* (CREATE), and *Authority* (EIP-7702) addresses
Transaction data and *ecrecover* no longer needed for verification
Reduced dependency on EVM internals

✅ **On-chain commitments to relevant data (fewer round trips, more efficient)**

EIP-7706: Separate gas types



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

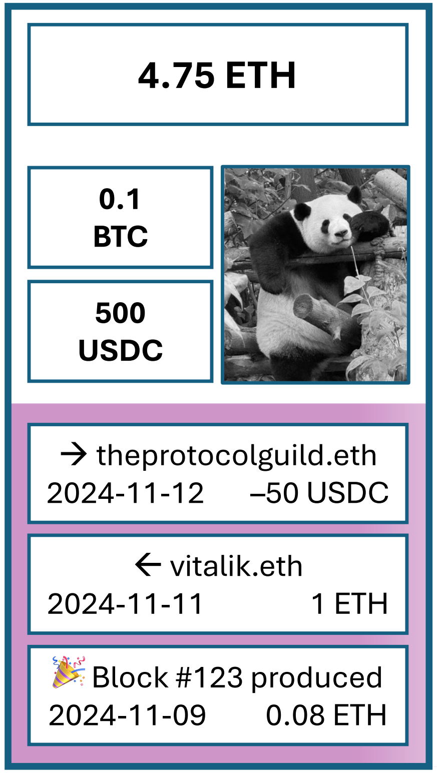
← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

Nonce	Max fee per gas	Gas limit	To	Value	Input	Replayable signature						Legacy
Nonce	Max fee per gas	Gas limit	To	Value	Input	Signature + Chain ID						EIP-155
0x01	Chain ID	Nonce	Max fee per gas	Gas limit	To	Value	Input	Access list	Sig			
0x02	Chain ID	Nonce	Prio fee per gas	Max fee per gas	Gas limit	To	Value	Input	Access list	Sig		
0x03	Chain ID	Nonce	Prio fee per gas	Max fee per gas	Gas limit	To	Value	Input	Access list	Fee per blob gas	Blob hashes	Sig
0x04	Chain ID	Nonce	Prio fee per gas	Max fee per gas	Gas limit	To	Value	Input	Access list	Auth list	Sig	
0x06	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	Blob hashes	Auth list	Max fees per gas	Prio fees per gas	Sig

✅ **Normalized gas fee computation**

EIP-6404: SSZ transactions



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

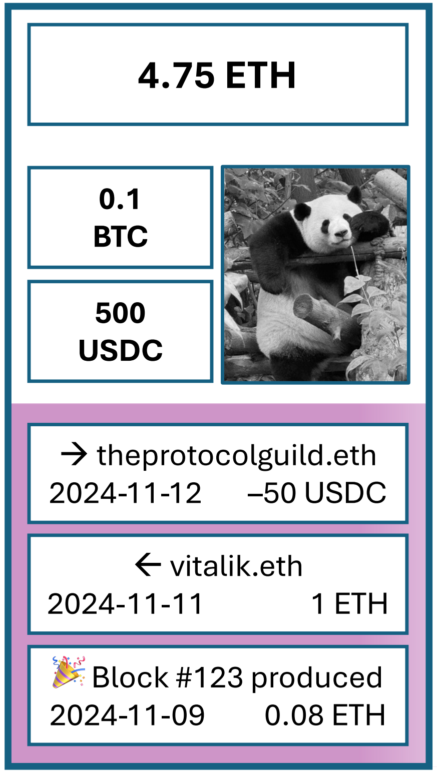
🎉 Block #123 produced
2024-11-09 0.08 ETH

RLP type	Nonce	Gas limit	To	Value	Input	Max fees per gas	Sig					
RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Max fees per gas	Sig				
RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	Max fees per gas	Sig			
RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	Max fees per gas	Prio fees per gas	Sig		
RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	Blob hashes	Max fees per gas	Prio fees per gas	Sig	
RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	Auth list	Max fees per gas	Prio fees per gas	Sig	

RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	Blob hashes	Auth list	Max fees per gas	Prio fees per gas	Sig

✅ **Type safety for different transaction profiles**

EIP-7495: SSZ StableContainer



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

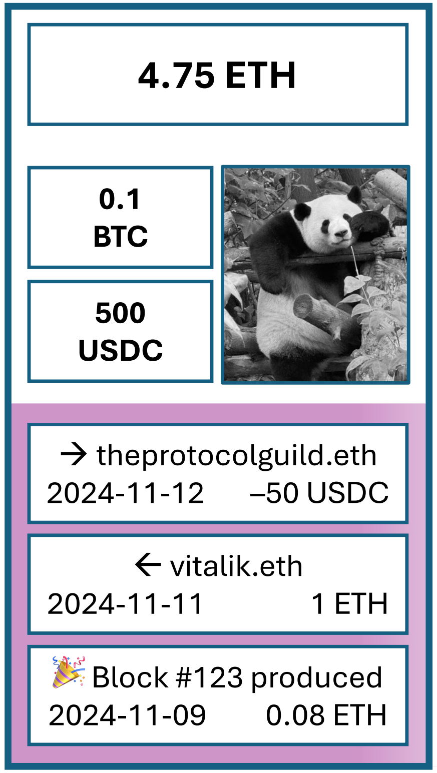
🎉 Block #123 produced
2024-11-09 0.08 ETH

RLP type	*n/a*	Nonce	Gas limit	To	Value	Input	*n/a*	*n/a*	*n/a*	Max fees per gas	*n/a*	Sig
RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	*n/a*	*n/a*	*n/a*	Max fees per gas	*n/a*	Sig
RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	*n/a*	*n/a*	Max fees per gas	*n/a*	Sig
RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	*n/a*	*n/a*	Max fees per gas	Prio fees per gas	Sig
RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	Blob hashes	*n/a*	Max fees per gas	Prio fees per gas	Sig
RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	*n/a*	Auth list	Max fees per gas	Prio fees per gas	Sig

RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	Blob hashes	Auth list	Max fees per gas	Prio fees per gas	Sig

✅ **Re-usable verifier (all profiles share stable SSZ merkleization)**

EIP-6493: SSZ transaction signature scheme



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

BasicTransaction
EIP-1559 functionality

BlobTransaction
EIP-4844 functionality

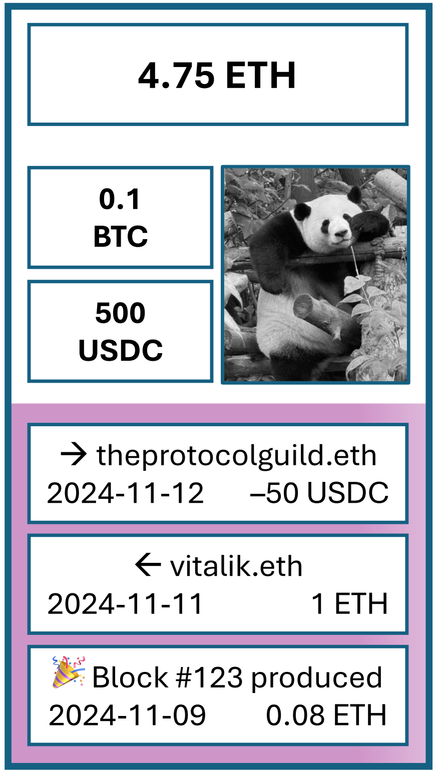
SetCodeTransaction
EIP-7702 functionality

n/a	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	*n/a*	*n/a*	Max fees per gas	Prio fees per gas	Sig
n/a	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	Blob hashes	*n/a*	Max fees per gas	Prio fees per gas	Sig
n/a	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	*n/a*	Auth list	Max fees per gas	Prio fees per gas	Sig

RLP type	Chain ID	Nonce	Gas limit	To	Value	Input	Access list	Blob hashes	Auth list	Max fees per gas	Prio fees per gas	Sig

✅ **Native SSZ (no conversion back to RLP for sig_hash / tx_hash)**

EIP-7807: SSZ execution blocks



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

Block metadata

Parent hash	Miner	State root	Number	Time-stamp	Extra data	Mix hash	Parent CL root

Gas accounting (separate gas types)

Gas limits	Gas used	Base fees	Excess gas

Removed fields (PoW era / Bloom)

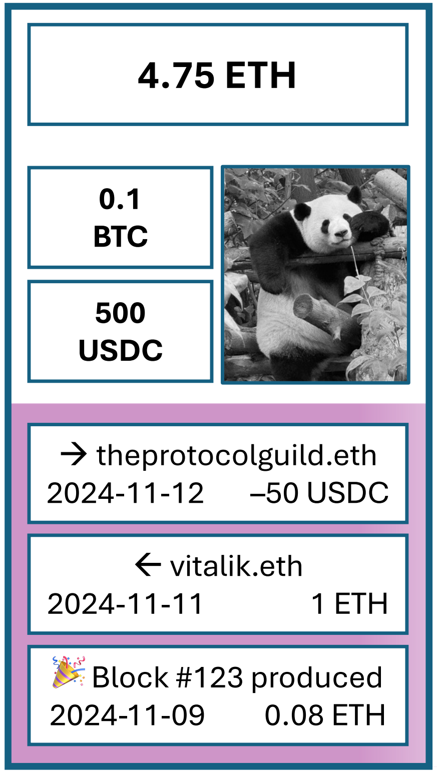
Ommers hash	Difficulty	Block nonce	Logs Bloom

Operations

Transactions root	Withdrawals root
Receipts root	System logs root
Requests hash	

✅ **Merkle-Patricia Tries (MPT) removed, encoding and hashing normalized**

Inclusion proofs



4.75 ETH

0.1 BTC

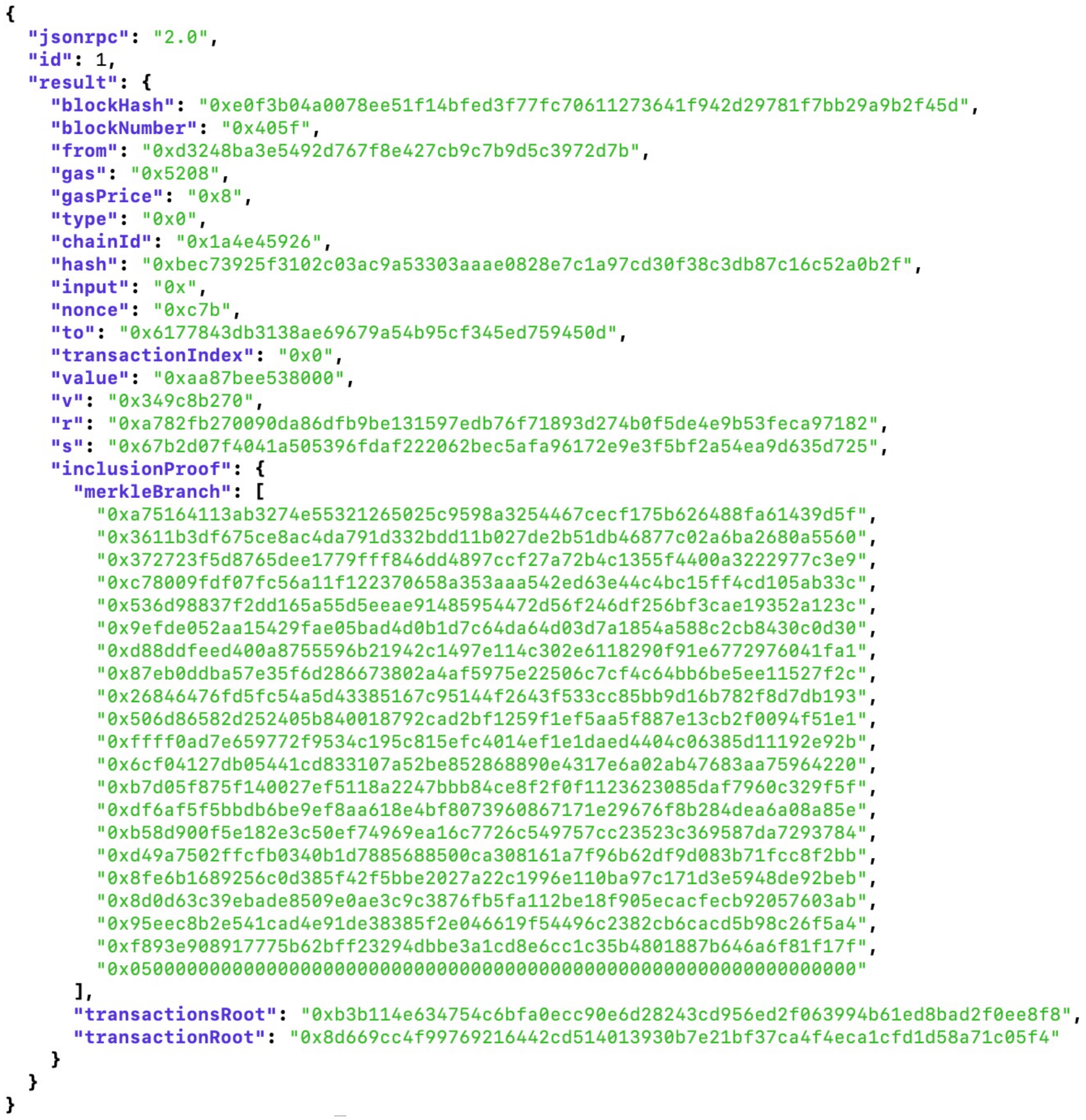
500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

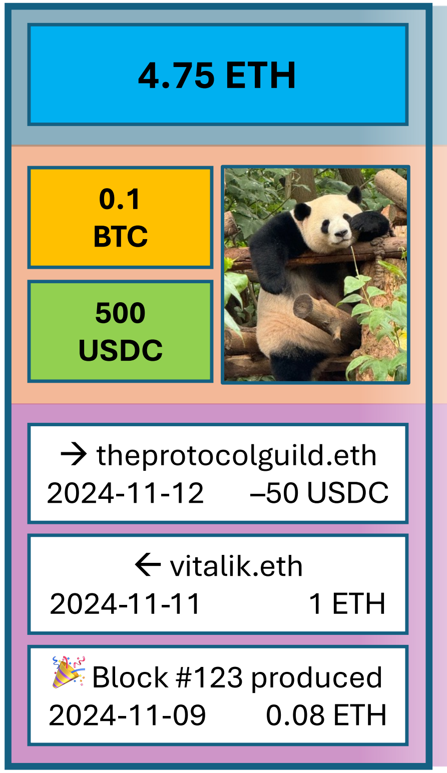
🎉 Block #123 produced
2024-11-09 0.08 ETH

✅ **No extra data required to verify tx**



```
{
  "jsonrpc": "2.0",
  "id": 1,
  "result": {
    "blockHash": "0xe0f3b04a0078ee51f14bfed3f77fc70611273641f942d29781f7bb29a9b2f45d",
    "blockNumber": "0x405f",
    "from": "0xd3248ba3e5492d767f8e427cb9c7b9d5c3972d7b",
    "gas": "0x5208",
    "gasPrice": "0x8",
    "type": "0x0",
    "chainId": "0x1a4e45926",
    "hash": "0xbec73925f3102c03ac9a53303aaae0828e7c1a97cd30f38c3db87c16c52a0b2f",
    "input": "0x",
    "nonce": "0xc7b",
    "to": "0x6177843db3138ae69679a54b95cf345ed759450d",
    "transactionIndex": "0x0",
    "value": "0xaa87bee538000",
    "v": "0x349c8b270",
    "r": "0xa782fb270090da86dfb9be131597edb76f71893d274b0f5de4e9b53feca97182",
    "s": "0x67b2d07f4041a505396fdaf222062bec5afa96172e9e3f5bf2a54ea9d635d725",
    "inclusionProof": {
      "merkleBranch": [
        "0xa75164113ab3274e55321265025c9598a3254467cecf175b626488fa61439d5f",
        "0x3611b3df675ce8ac4da791d332bdd11b027de2b51db46877c02a6ba2680a5560",
        "0x372723f5d8765dee1779fff846dd4897ccf27a72b4c1355f4400a3222977c3e9",
        "0xc78009fdf07fc56a11f122370658a353aaa542ed63e44c4bc15ff4cd105ab33c",
        "0x536d98837f2dd165a55d5eeae91485954472d56f246df256bf3cae19352a123c",
        "0x9efde052aa15429fae05bad4d0b1d7c64da64d03d7a1854a588c2cb8430c0d30",
        "0xd88ddfeed400a8755596b21942c1497e114c302e6118290f91e6772976041fa1",
        "0x87eb0ddba57e35f6d286673802a4af5975e22506c7cf4c64bb6be5ee11527f2c",
        "0x26846476fd5fc54a5d43385167c95144f2643f533cc85bb9d16b782f8d7db193",
        "0x506d86582d252405b840018792cad2bf1259f1ef5aa5f887e13cb2f0094f51e1",
        "0xffff0ad7e659772f9534c195c815efc4014ef1e1daed4404c06385d11192e92b",
        "0x6cf04127db05441cd833107a52be852868890e4317e6a02ab47683aa75964220",
        "0xb7d05f875f140027ef5118a2247bbb84ce8f2f0f1123623085daf7960c329f5f",
        "0xdf6af5f5bbdb6be9ef8aa618e4bf8073960867171e29676f8b284dea6a08a85e",
        "0xb58d900f5e182e3c50ef74969ea16c7726c549757cc23523c369587da7293784",
        "0xd49a7502ffcfb0340b1d7885688500ca308161a7f96b62df9d083b71fcc8f2bb",
        "0x8fe6b1689256c0d385f42f5bbe2027a22c1996e110ba97c171d3e5948de92beb",
        "0x8d0d63c39ebade8509e0ae3c9c3876fb5fa112be18f905ecacfecb92057603ab",
        "0x95eec8b2e541cad4e91de38385f2e046619f54496c2382cb6cacd5b98c26f5a4",
        "0xf893e908917775b62bff23294dbbe3a1cd8e6cc1c35b4801887b646a6f81f17f",
        "0x0500000000000000000000000000000000000000000000000000000000000000"
      ],
      "transactionsRoot": "0xb3b114e634754c6bfa0ecc90e6d28243cd956ed2f063994b61ed8bad2f0ee8f8",
      "transactionRoot": "0x8d669cc4f99769216442cd514013930b7e21bf37ca4f4eca1cfd1d58a71c05f4"
    }
  }
}
```

Wallet



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

ETH balance

🥰

Tokens / NFTs

Metadata
Balances & allowances
Exchange rates

😕 Access lists are best effort
Lots of round trips

History

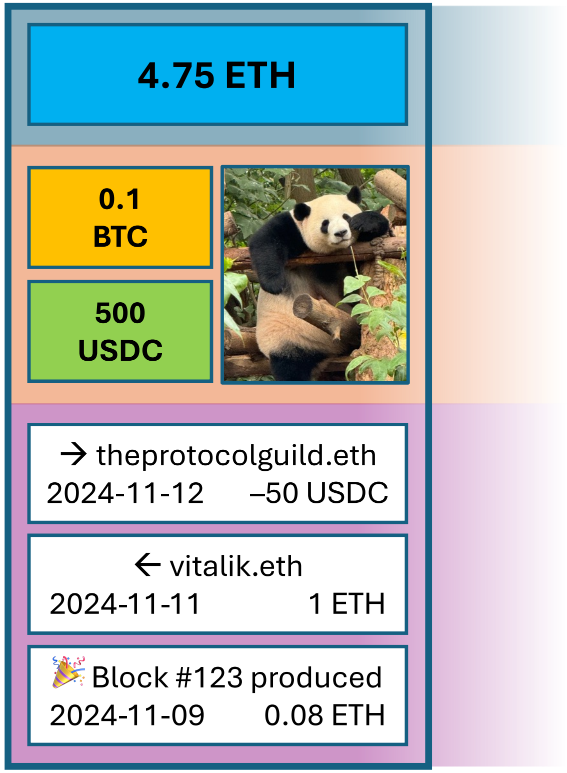
Transaction details
Fees & gas usage
Staking operations & rewards
No missing entries

🤯

😡 Terribly inefficient

🚫 ETH transfers
from smart contracts

Learn more



4.75 ETH

0.1 BTC

500 USDC

→ theprotocolguild.eth
2024-11-12 –50 USDC

← vitalik.eth
2024-11-11 1 ETH

🎉 Block #123 produced
2024-11-09 0.08 ETH

Devnet

Nimbus + EthereumJS + Helios

Buidling guides

Verifying wallets

Web3 purifiers

Developer tools

Kurtosis network config

RLP → SSZ converting explorer

SSZ StableContainer implementations

https://fusaka-light.box

Related sessions

Gajinder Singh, Jason Chaskin

Today Verkle + Tomorrow ZK =
Everything Stateless, Everything Lightclient

Nov 13th — 4:30 PM - 5:00 PM Talk - Stage 2

Noah Citron

The Future of Light Clients

Nov 13th — 5:30 PM - 6:00 PM Talk - Stage 5