



# Light Clients

After the Merge

Etan Kissling  
Nimbus, Status R&D GmbH



Section 1

# What is a Light Client?

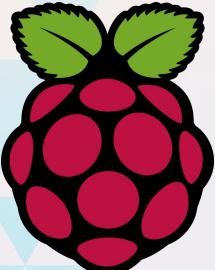
# Full Node Requirements

1.5 GHz  
Quad CPU

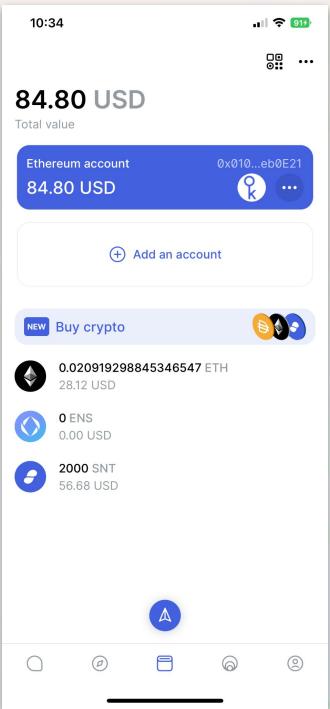
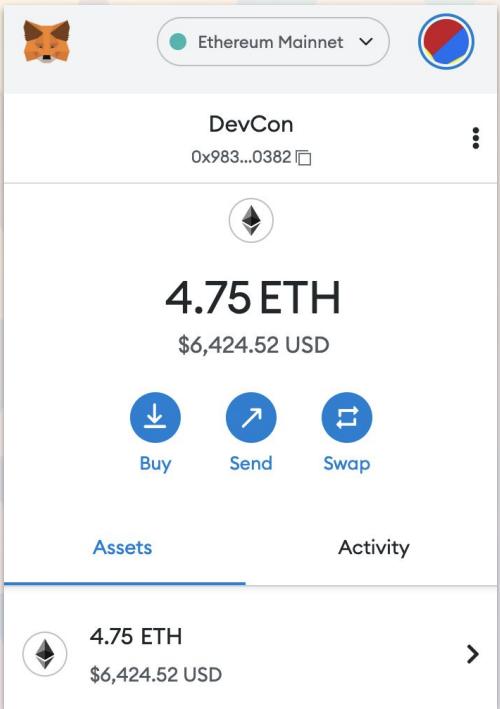
8 GB  
RAM

2 TB  
SSD

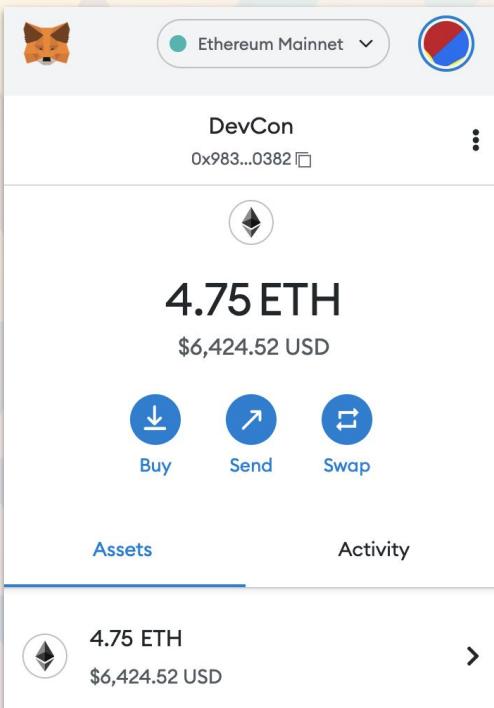
Unmetered  
Internet



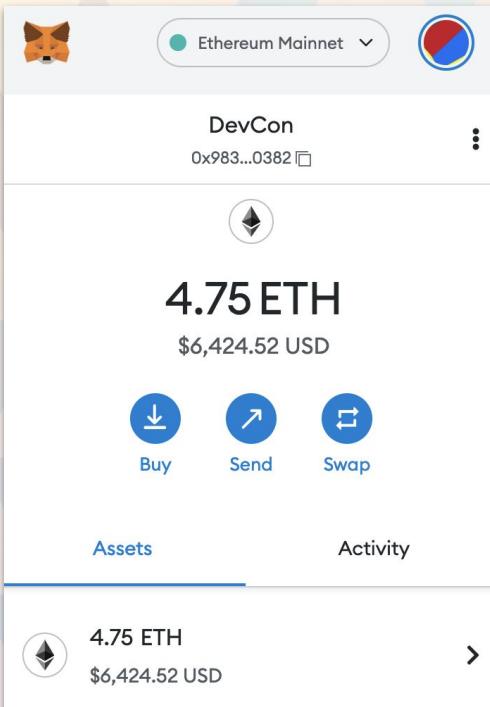
# Light clients?



# Your own wallet



# Your own wallet



You are doing great work!

Can I support with .5 ETH?



# Your own wallet



Sure!

You are doing  
great work!

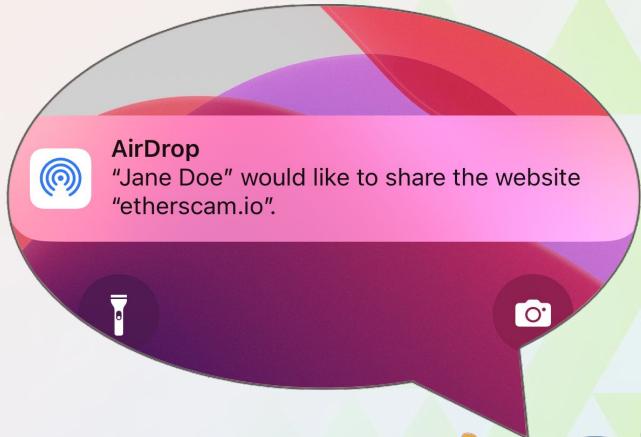
Can I support with  
.5 ETH?



# Receiving a donation



Sure!



# Receiving a donation



Sure!

A screenshot of a mobile device displaying the Etherscan transaction receipt for a donation. The screen shows the following details:

- Timestamp:** 11:30
- Transaction Hash:** 0x048657127073eebe3f109f9ca32f2a5e6da89cbd16eedd613c86f17bd587cf60
- Status:** Success
- Block:** 15680597 (324 Block Confirmations)
- From:** 0xeb8e7c90014565eed8126110630efa2d9cd6ebe4
- To:** 0x983260467a0d5c0dc02c031f653a645751c90382
- Value:** 5 Ether (\$6,726.70)
- Transaction Fee:** 0.000129072158649 Ether (\$0.17)

The footer of the screen shows the URL etherscan.io.

# Receiving a donation

Value:

5 Ether (\$6,726.70)

5 ETH, not .5?!

The screenshot shows a mobile application interface for Etherscan. At the top, it displays the time as 11:30 and battery level at 100%. The main content area is titled "Overview" and shows the following details for a transaction:

- Transaction Hash:** 0x048657127073eebe3f109f9ca32f2a5e6da89cbd16eedd613c86f17bd587cf60
- Status:** Success
- Block:** 15680597 | 324 Block Confirmations
- Timestamp:** 4 mins ago (Oct-05-2022 08:05:23 AM +UTC)
- From:** 0xeb8e7c90014565eedb126110630efa2d9cd6ebe4
- To:** 0x983260467a0d5c0dc02c031f653a645751c90382
- Value:** 5 Ether (\$6,726.70)
- Transaction Fee:** 0.000129072158649 Ether (\$0.17)

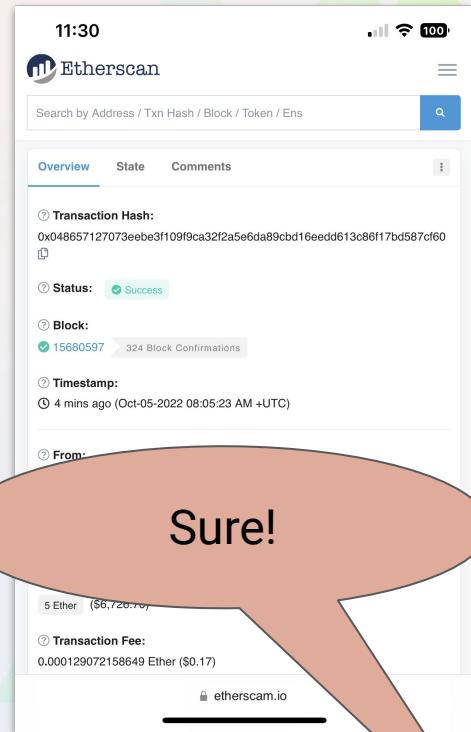
At the bottom of the screen, there is a footer bar with the URL etherscan.io.

# Receiving a donation

Value:

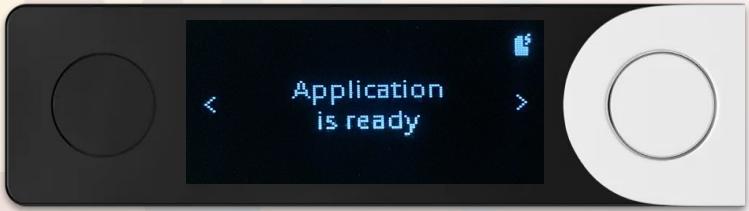
5 Ether (\$6,726.70)

Refund  
4.5 ETH?



Sure!

# Funds protected by HW wallet



Refund  
4.5 ETH?

A screenshot of a mobile phone displaying the Etherscan transaction details page for a recent transaction. The transaction hash is 0x048657127073eebe3f109f9ca32f2a5e6da89cbd16eedd613c86f17bd587cf60. The status is marked as "Success". The transaction was included in block 15680597, which has 324 confirmations. The timestamp is 4 mins ago (Oct-05-2022 08:05:23 AM +UTC). The transaction originated from an address that sent 5 Ether (\$6,720.75) and paid a transaction fee of 0.000129072158649 Ether (\$0.17). A large orange speech bubble points to the "Success" status with the text "Sure!".

11:30

Etherscan

Search by Address / Txn Hash / Block / Token / Ens

Overview State Comments

Transaction Hash: 0x048657127073eebe3f109f9ca32f2a5e6da89cbd16eedd613c86f17bd587cf60

Status: Success

Block: 15680597 324 Block Confirmations

Timestamp: 4 mins ago (Oct-05-2022 08:05:23 AM +UTC)

From:

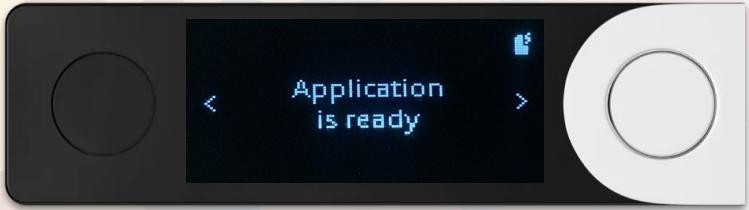
5 Ether (\$6,720.75)

Transaction Fee: 0.000129072158649 Ether (\$0.17)

etherscan.io

Sure!

# Funds protected by HW wallet



Can I use your laptop?

A screenshot of a mobile phone displaying the Etherscan website. The screen shows a transaction details page for a successful Ethereum transfer. The transaction hash is 0x048657127073eebe3f109f9ca32f2a5e6da89cbd16eedd613c86f17bd587cf60. It was included in block 15680597, which has 324 confirmations. The timestamp is 4 mins ago (Oct-05-2022 08:05:23 AM +UTC). The transaction originated from an address that sent 5 Ether (\$6,720.75) to another address. The transaction fee was 0.000129072158649 Ether (\$0.17).

11:30

Etherscan

Search by Address / Txn Hash / Block / Token / Ens

Overview State Comments

Transaction Hash: 0x048657127073eebe3f109f9ca32f2a5e6da89cbd16eedd613c86f17bd587cf60

Status: Success

Block: 15680597 324 Block Confirmations

Timestamp: 4 mins ago (Oct-05-2022 08:05:23 AM +UTC)

From:

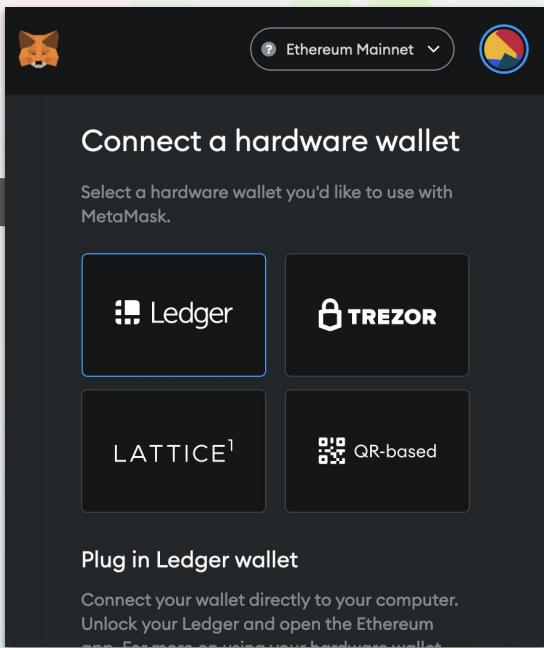
5 Ether (\$6,720.75)

Transaction Fee: 0.000129072158649 Ether (\$0.17)

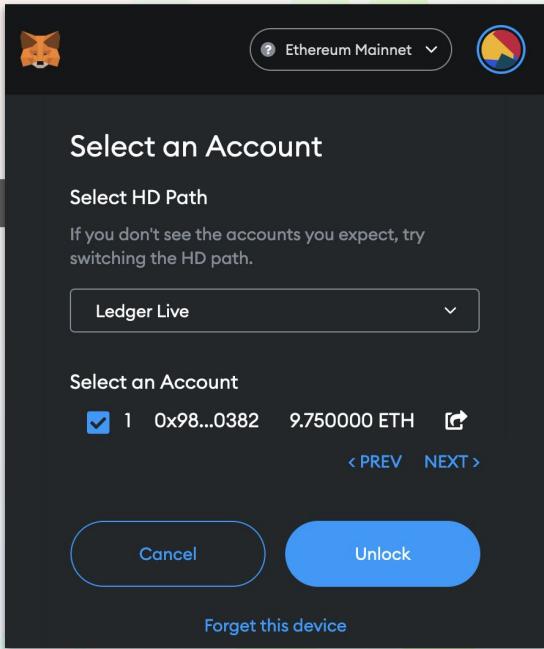
etherscan.io

Sure!

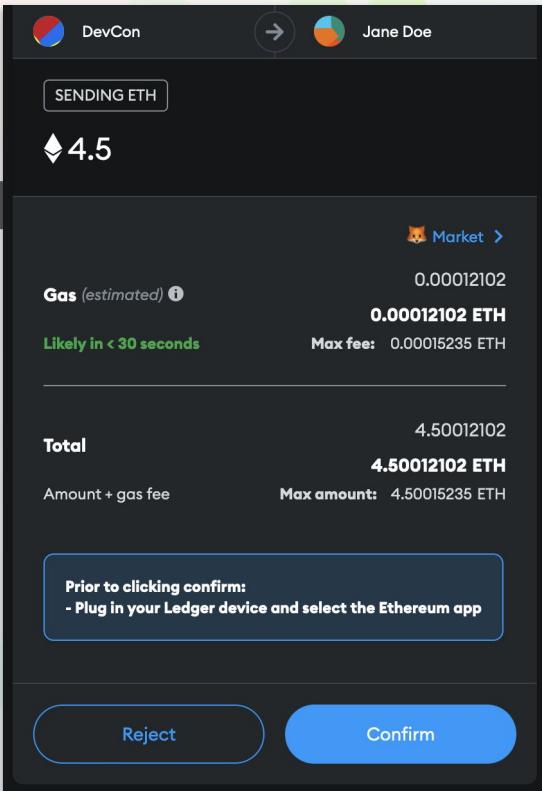
# Funds protected by HW wallet



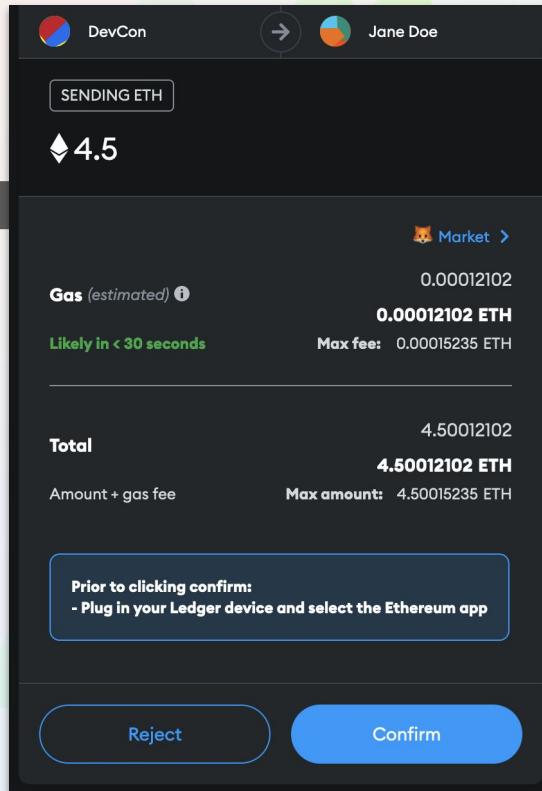
# Funds protected by HW wallet



# Funds protected by HW wallet



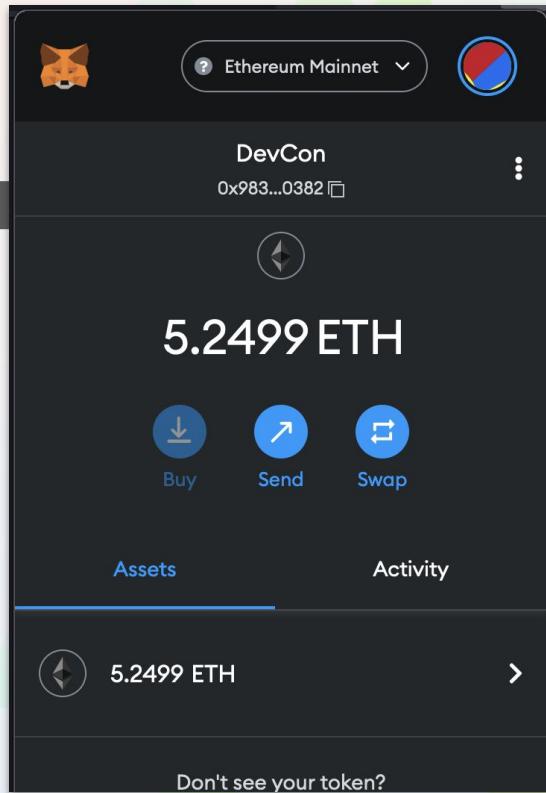
# Funds protected by HW wallet



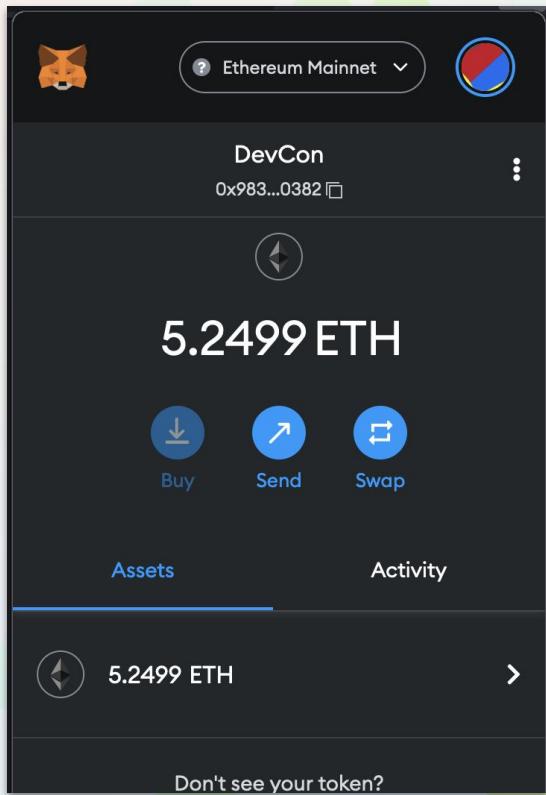
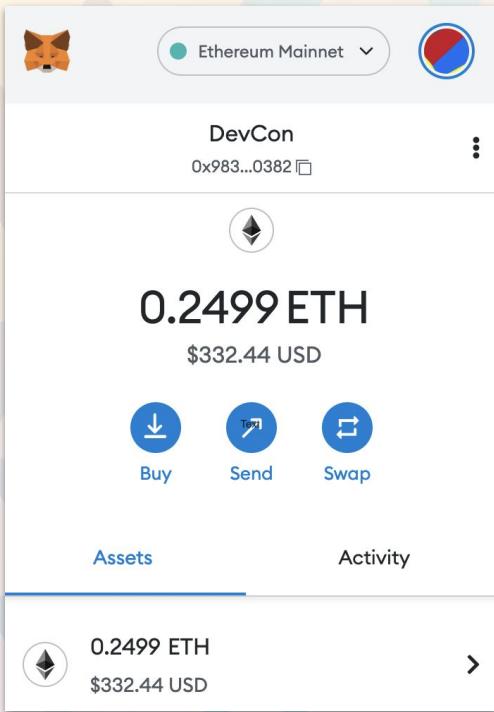
# Funds protected by HW wallet



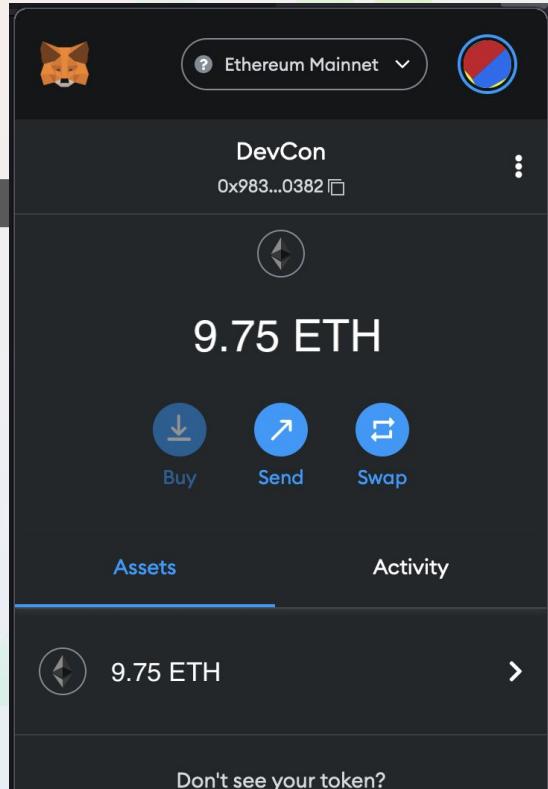
Thanks for the  
donation!



# Some time later...



# What went wrong?



# What went wrong?



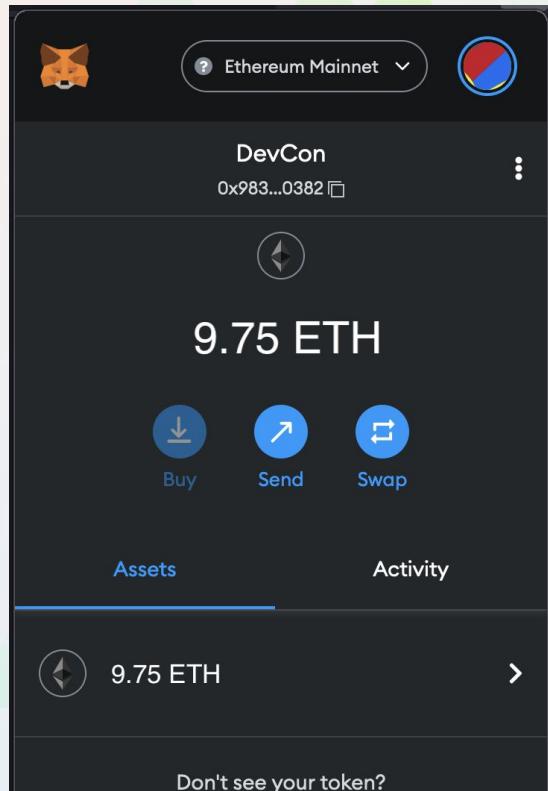
Current Balance  
ETH 4.75



Amount  
ETH 4.5



Address  
0xEB8E7c90014565EE  
d8126110630eFa2d9C  
D6eBE4



# What went wrong?



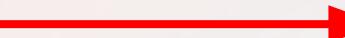
Current Balance  
ETH 4.75



Amount  
ETH 4.5



Address  
0xEB8E7c90014565EE  
d8126110630eFa2d9C  
D6eBE4



Network Name

New RPC URL

Chain ID ⓘ

Currency Symbol

Block Explorer URL (Optional)

Cancel

Save

# Obtaining an ETH balance

Request

```
method: "eth_getBalance"
```

```
params: [...]
```

```
0: "0x983260467a0d5c0dc02c031f653a645751c90382"
```

```
1: "0xEF49CB"
```

**Address**

**Block number**

# Obtaining an ETH balance

Request

```
method: "eth_getBalance"
```

```
params: [...]
```

```
0: "0x983260467a0d5c0dc02c031f653a645751c90382"
```

```
1: "0xEF49CB"
```

**Address**

**Block number**

Response

```
result: "0x48db5817212fe4a0"
```

~5.2499 ETH

**Balance**

# Obtaining an ETH balance

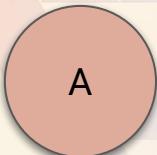
```
proxy.rpc("eth_getBalance") do(address: Address, quantityTag: string) -> HexQuantityStr:  
    let balance = await rpcClient.eth_getBalance(address, quantityTag)  
    if $address == "0x983260467a0d5c0dc02c031f653a645751c90382":  
        return encodeQuantity(balance + 5000000000000000000.u256) # Add 5 ETH  
    return encodeQuantity(balance)
```



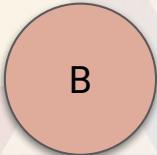
Section 2

# Verifying Ethereum data

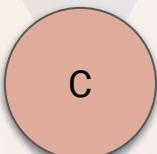
# Ethereum data



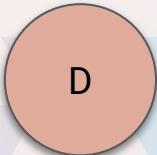
Token balance



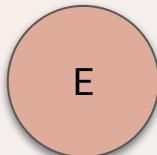
NFT owner



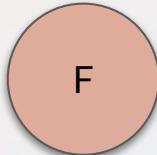
ETH balance



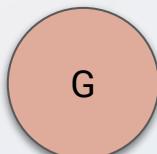
DeFi exchange rate



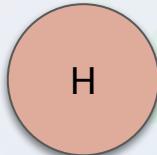
Staking amount



Tokenized asset

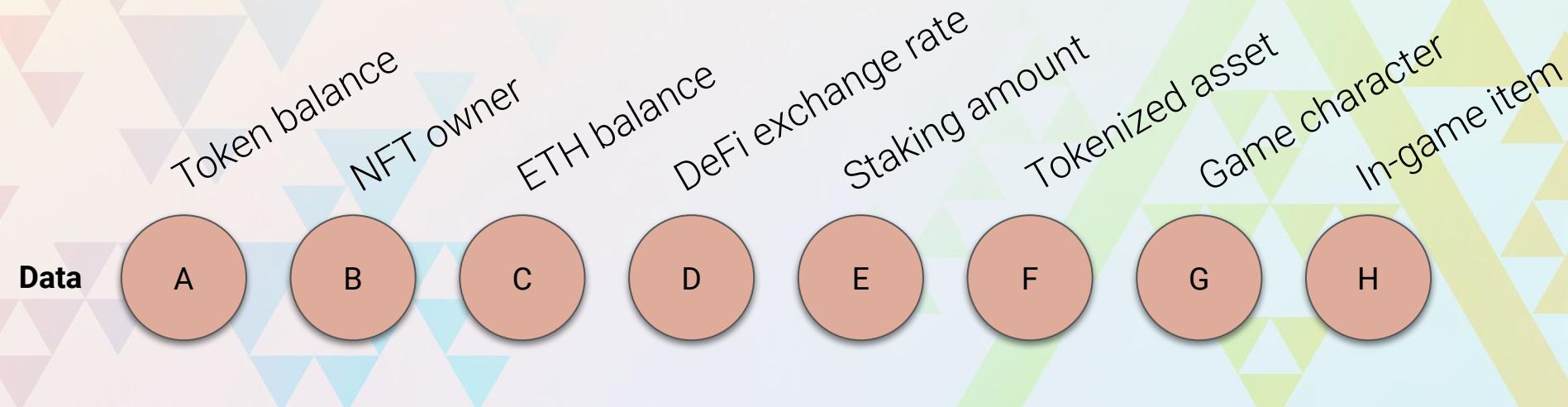


Game character



In-game item

# Ethereum data



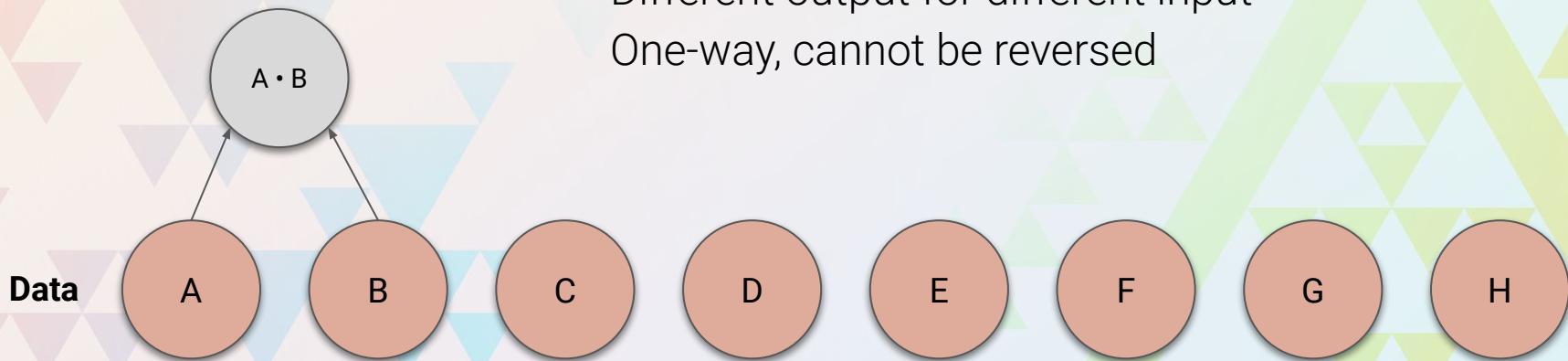
# Ethereum data

## Hash

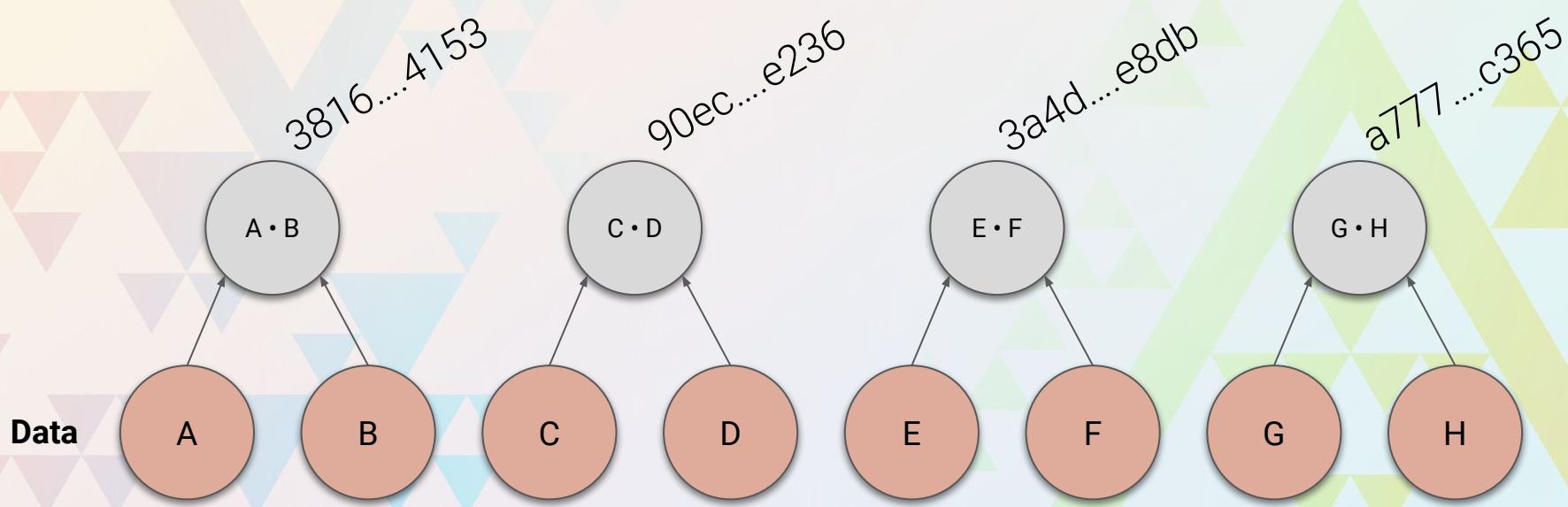
Only dependent on input data

Different output for different input

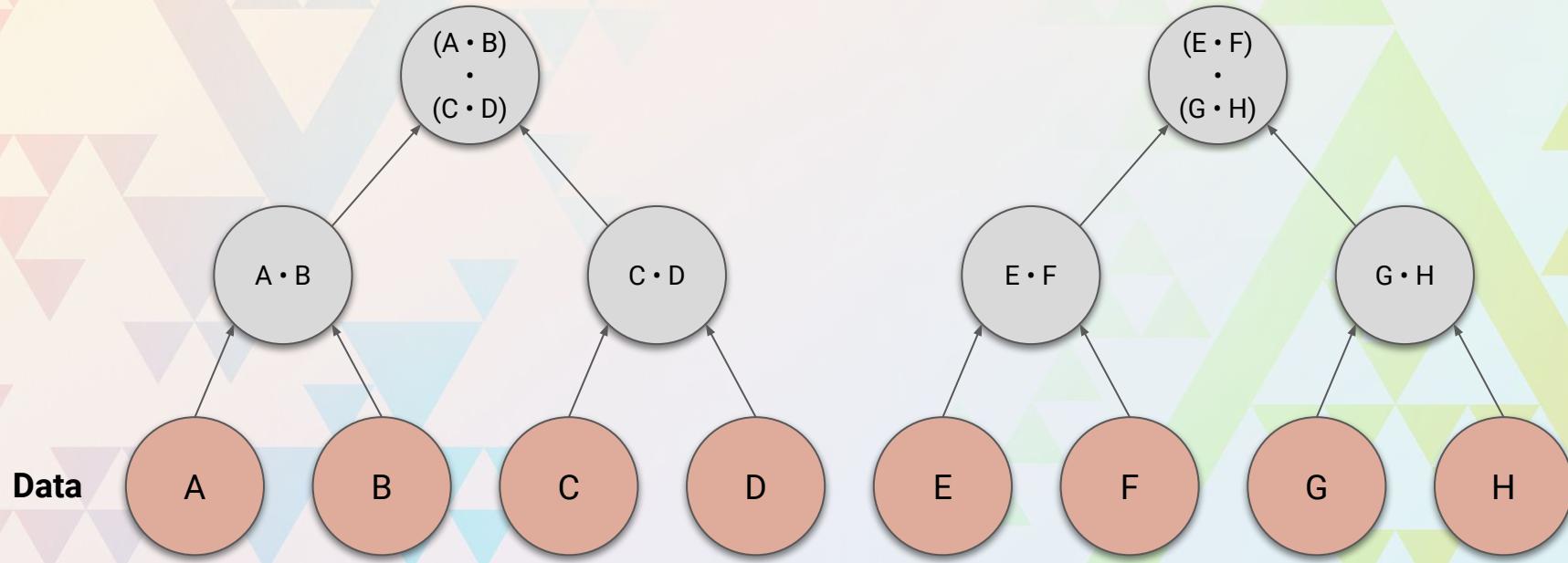
One-way, cannot be reversed



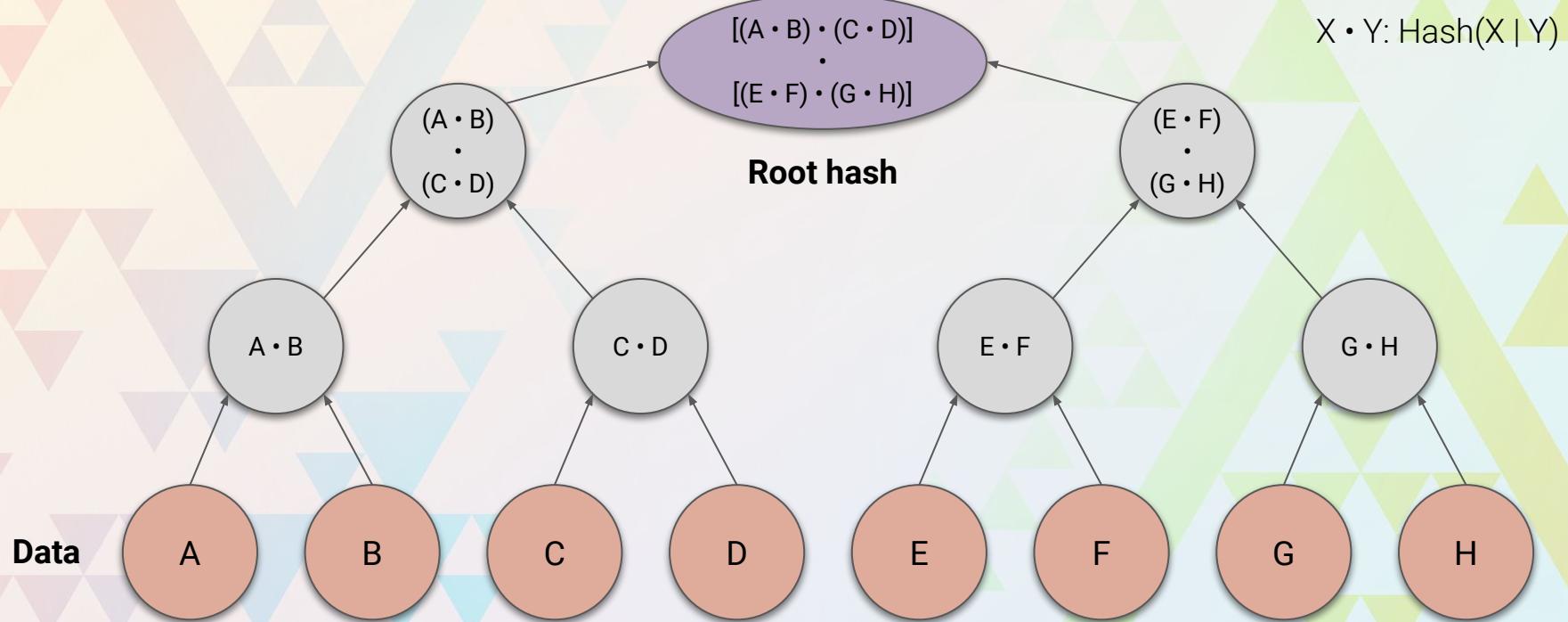
# Merkle trees



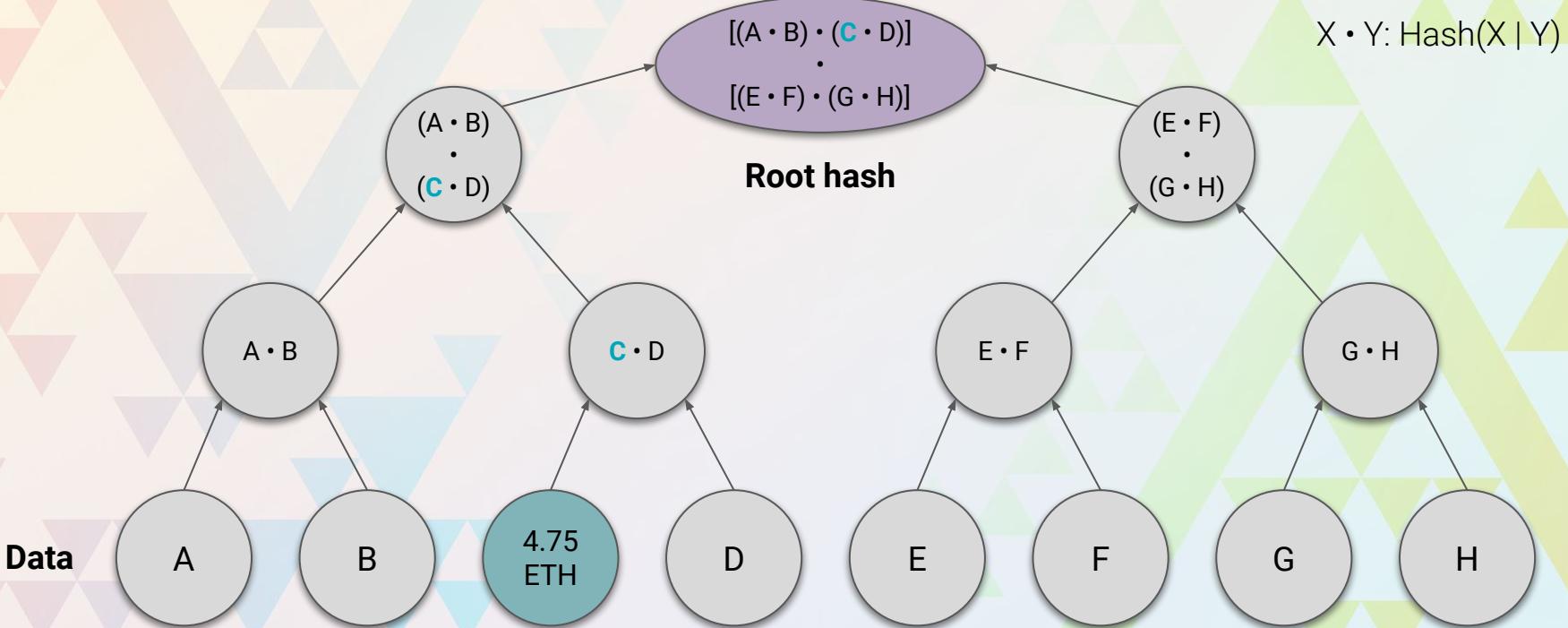
# Merkle trees



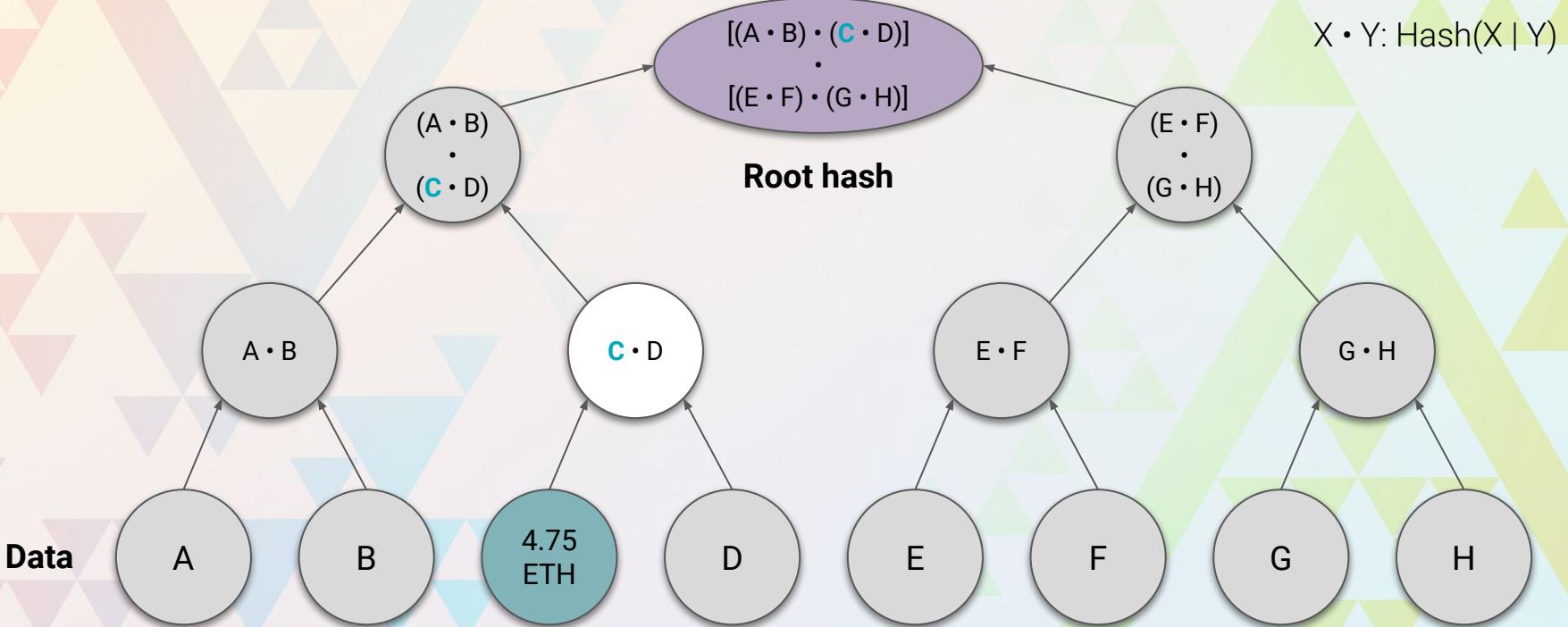
# Merkle trees



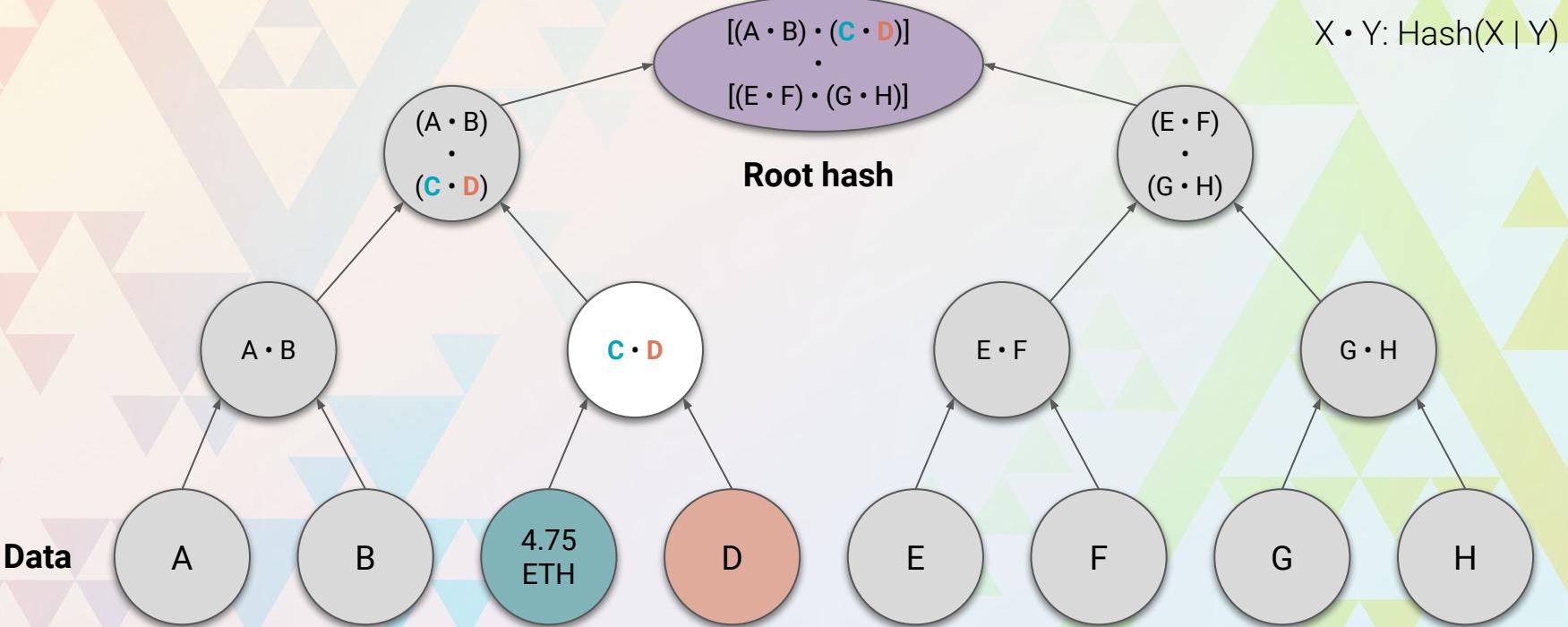
# Merkle proof



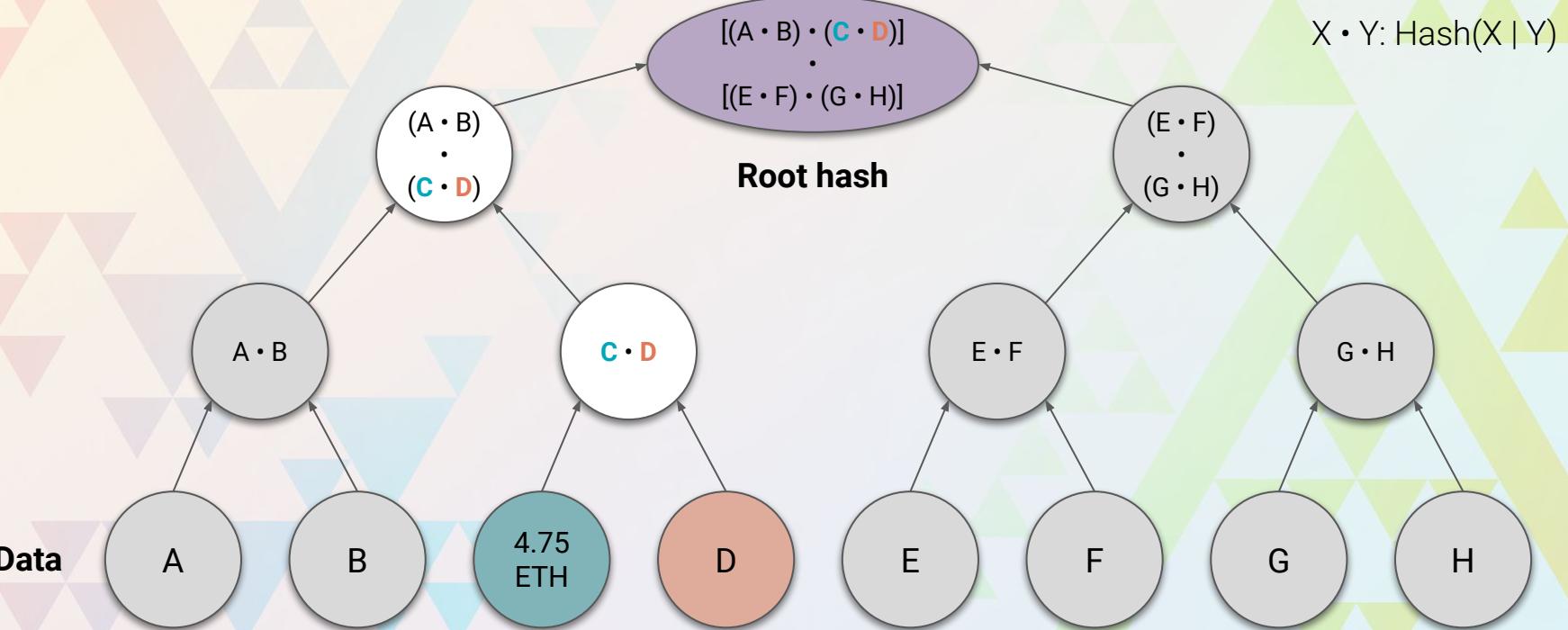
# Merkle proof



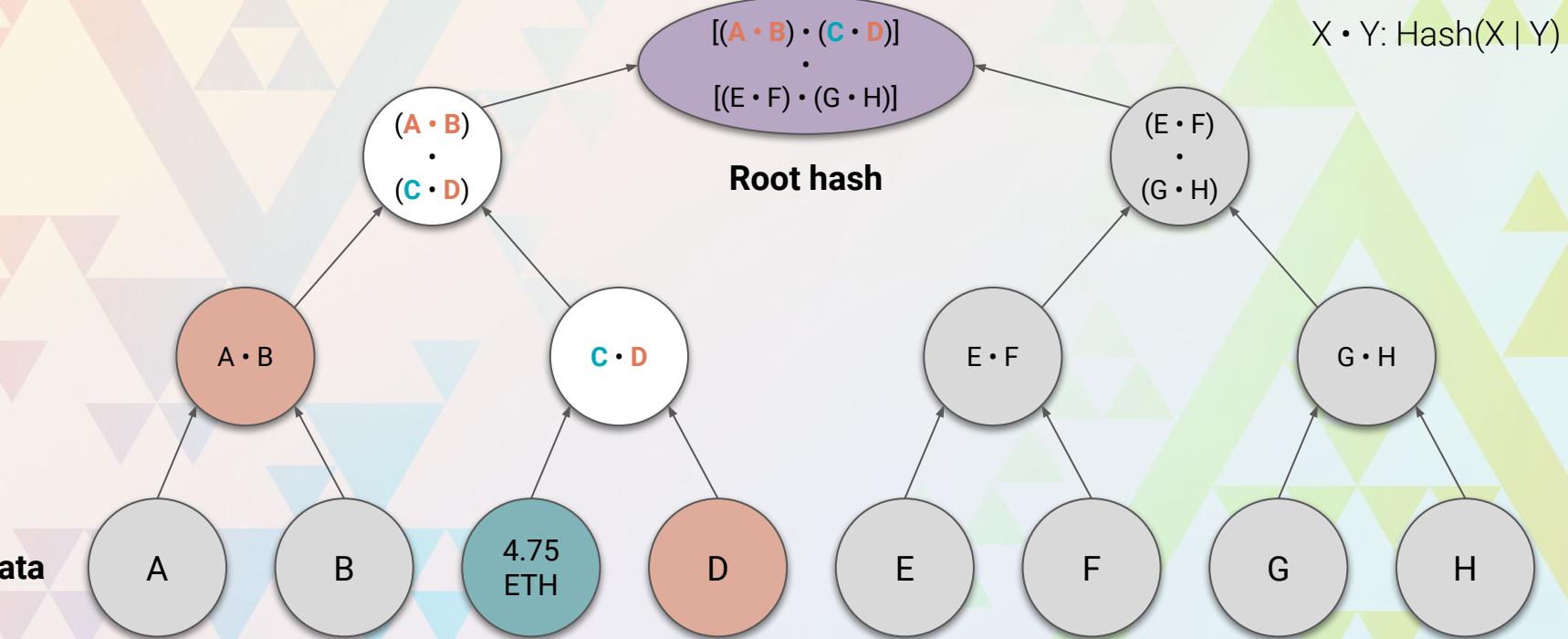
# Merkle proof



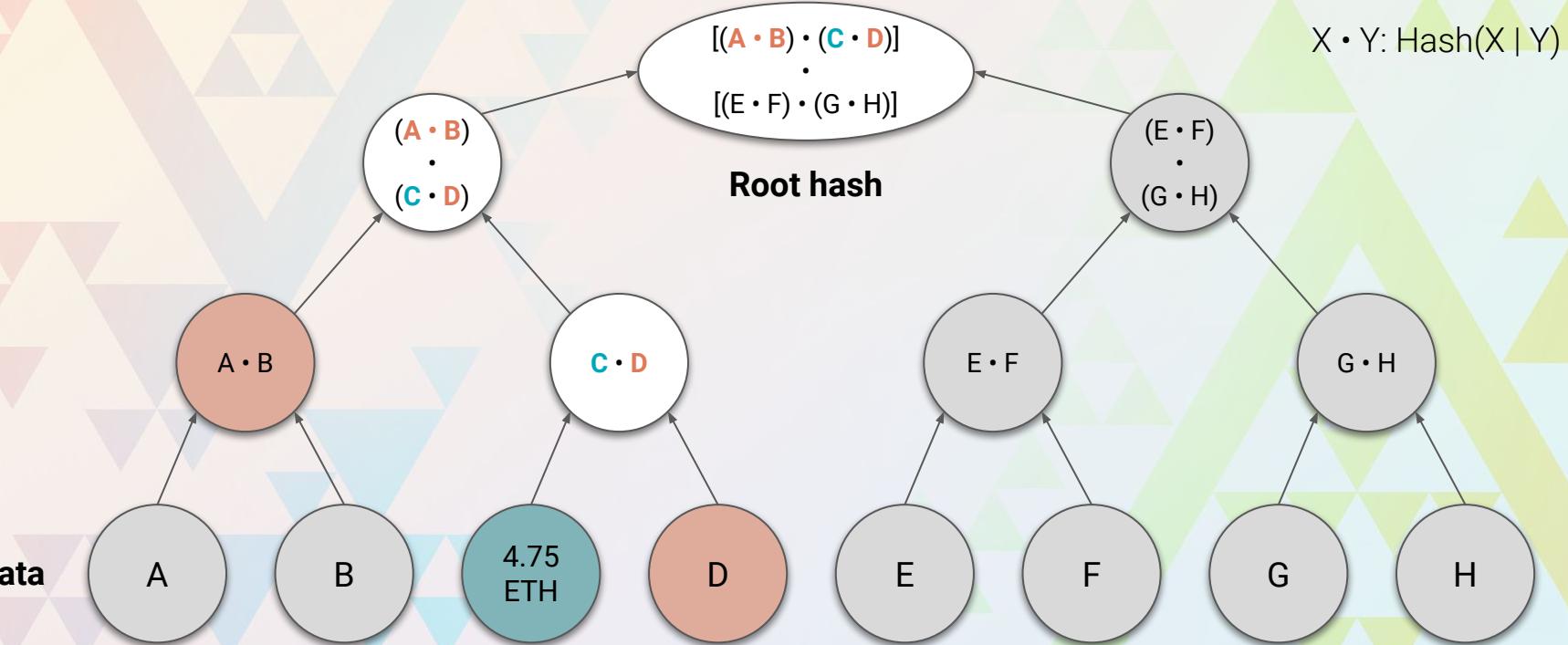
# Merkle proof



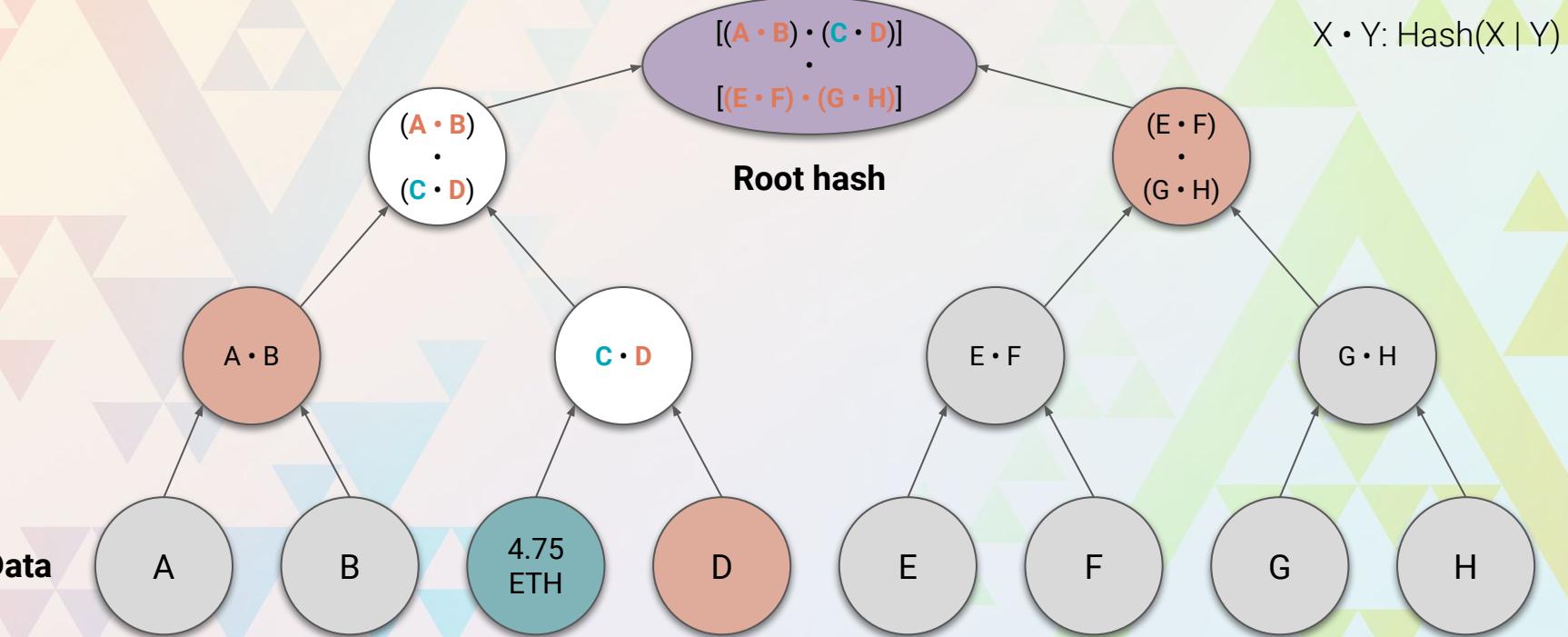
# Merkle proof



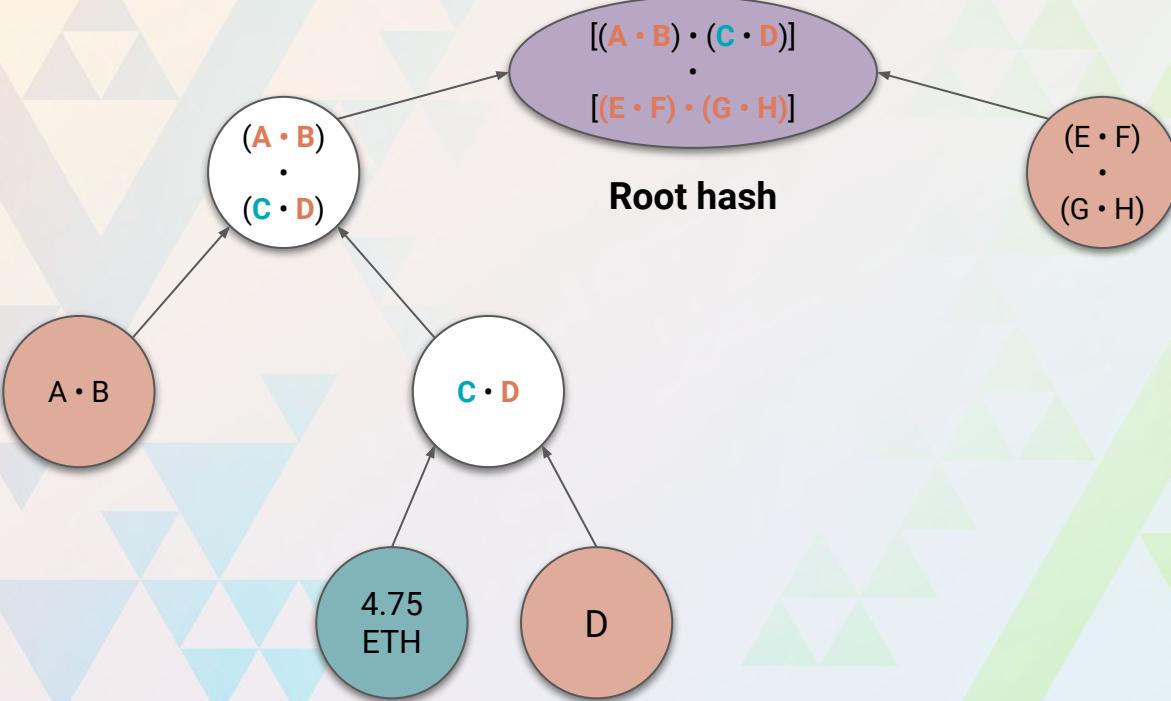
# Merkle proof



# Merkle proof



# Merkle proof



$X \cdot Y: \text{Hash}(X \mid Y)$

# eth\_getProof (EIP 1186)

Request

method: "eth\_getProof"

params: [...]

0: "0x983260467a0d5c0dc02c031f653a645751c90382"

1: [] (for token balances, NFT owners, ...)

2: "0xEF49CB"

**Address**

**Storage slots**

**Block number**

**Merkle proof**

**Balance**

## eth\_getProof (EIP 1186)

Response

```
"result": {  
    "accountProof": [  
        "0xf90211a0...0d72d680",  
        "0xf90211a0...b46e5180",  
        "0xf90211a0...f4ef1b80",  
        "0xf90211a0...fcbc1980",  
        "0xf90211a0...25322c80",  
        "0xf90211a0...f0748980",  
        "0xf9013180...bdb1d380",  
        "0xf8918080...80808080",  
        "0xf86e9d20...5d85a470"  
    ],  
    "address": "0x983260467a0d5c0dc02c031f653a645751c90382",  
    "balance": "0x377c694dc3be4a0",  
    "codeHash": "0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470",  
    "nonce": "0x2",  
    "storageHash": "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",  
    "storageProof": []  
}
```

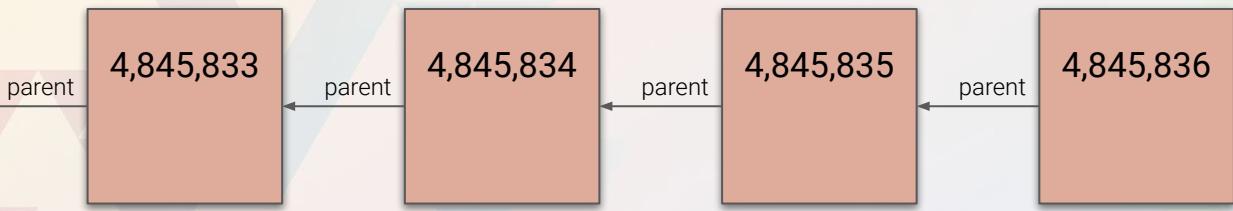
Still need the root hash  
to verify against!



Section 3

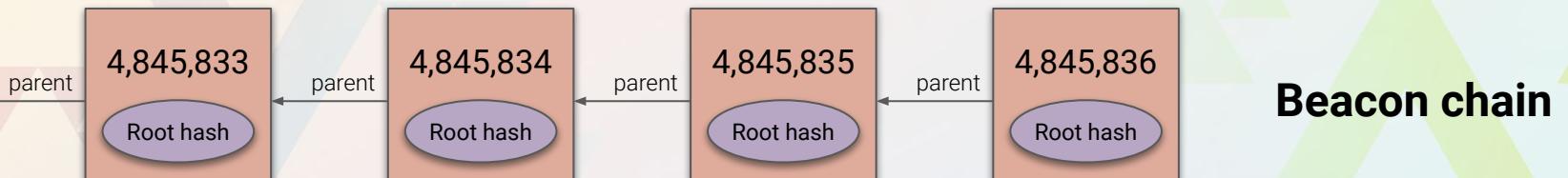
# Obtaining the root hash

# Where is the root hash?



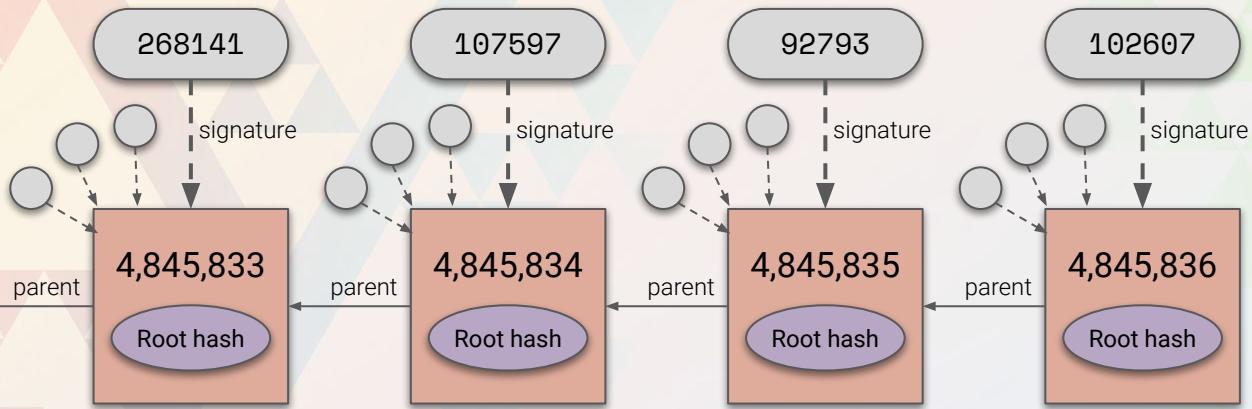
**Beacon chain**

# Where is the root hash? (Merge 🐾)



**Beacon chain**

# How to verify?



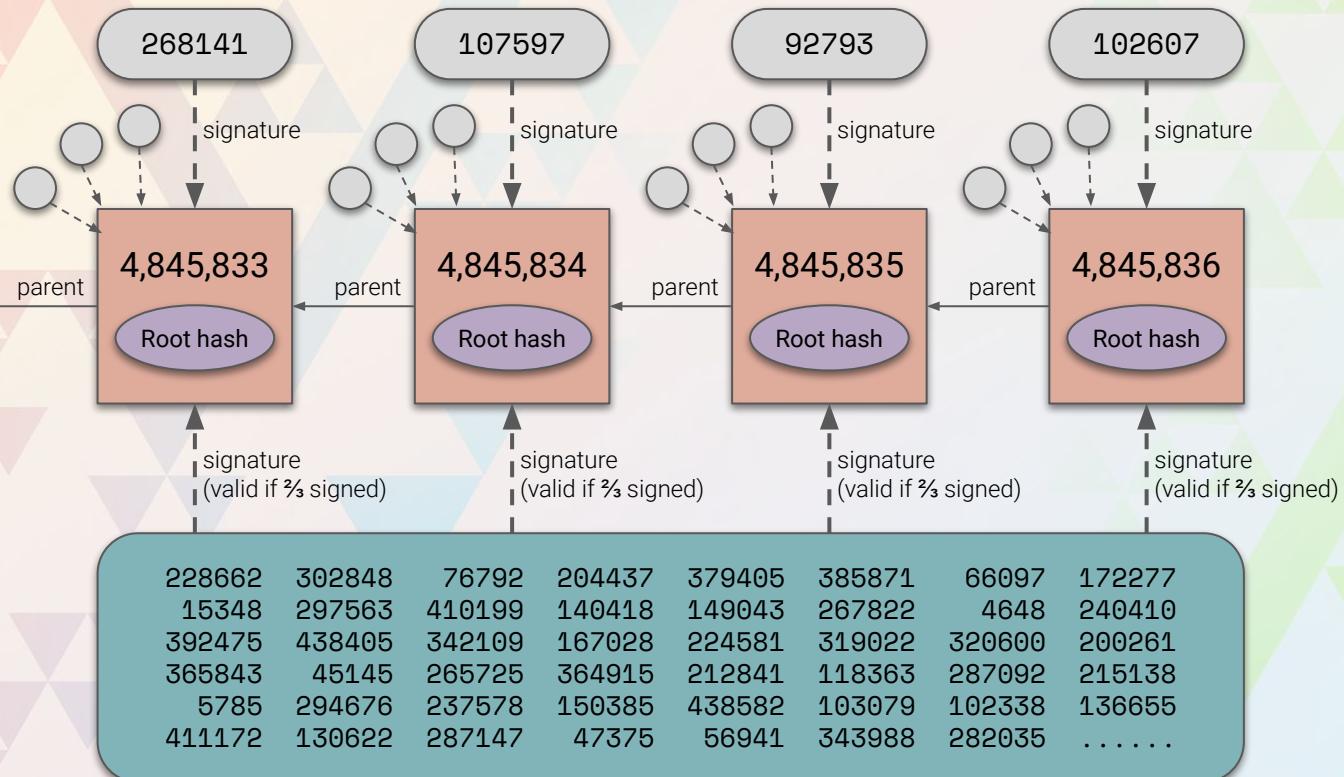
Proposing validator

Attestations

Beacon chain

There are **>440k** validators  
Need **GBs** of data to verify

# How to verify? (Altair)



Proposing validator

Attestations

Beacon chain

Sync committee  
(512 validators)

# How to get the sync committee?

390290	392522	356403	202586	184113	309259	129131	414668
398917	33891	108733	209678	255003	30286	123147	293629
131888	209269	323338	298622	305191	369160	211704	280926
255891	256646	89218	167832	343267	137560	245864	415896
312139	188521	159437	345790	339136	265386	243022	301945
393913	73431	233645	144754	218787	110930	133158	.....

**Previous  
sync committee**

next sync committee  
(re-elected daily)

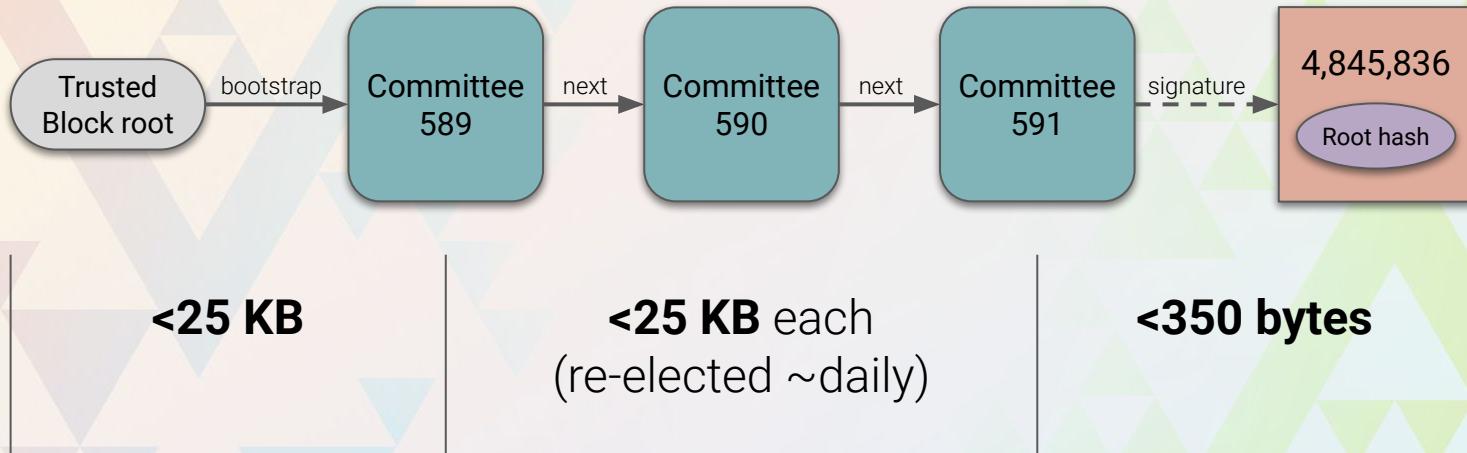
228662	302848	76792	204437	379405	385871	66097	172277
15348	297563	410199	140418	149043	267822	4648	240410
392475	438405	342109	167028	224581	319022	320600	200261
365843	45145	265725	364915	212841	118363	287092	215138
5785	294676	237578	150385	438582	103079	102338	136655
411172	130622	287147	47375	56941	343988	282035	.....

**Sync committee**  
(512 validators)

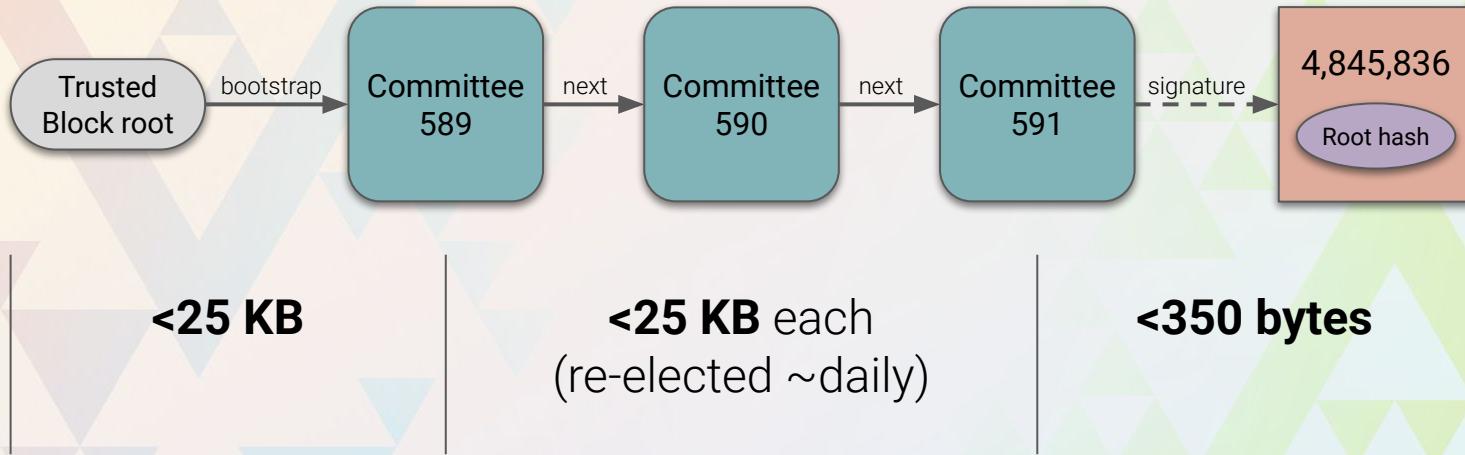
# Light client data



# Light client data



# Light client data

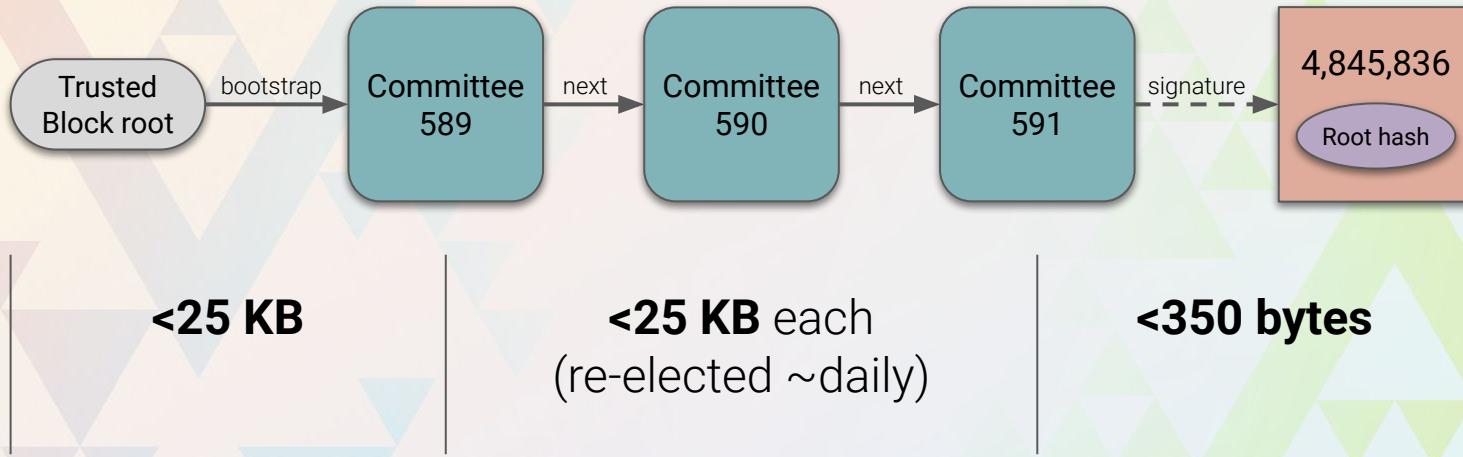


**REST** [ethereum/beacon-APIs #247](#)

**libp2p** [ethereum/consensus-specs > specs > altair > light-client](#)

**Portal** [ethereum/portal-network-specs #166](#)

# Light client data



With  $\frac{2}{3}$  signature threshold: **<128 days** old data is safe to use

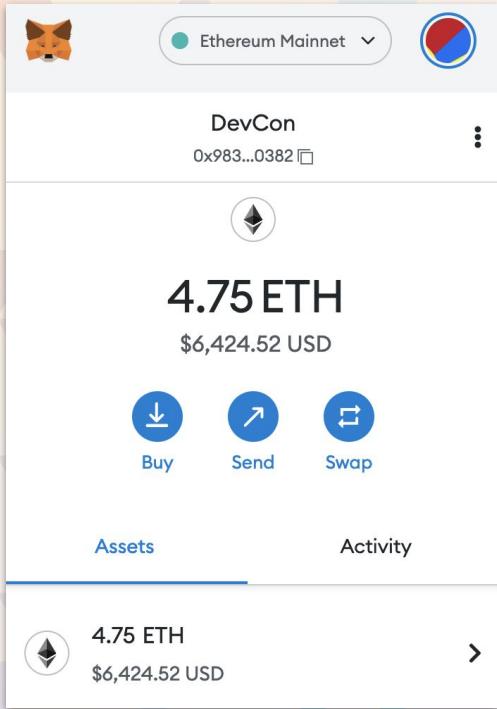
<https://github.com/metacraft-labs/DendrETH/tree/main/docs/long-range-syncing>



Section 4

# Combining it all together

# Back to the wallet

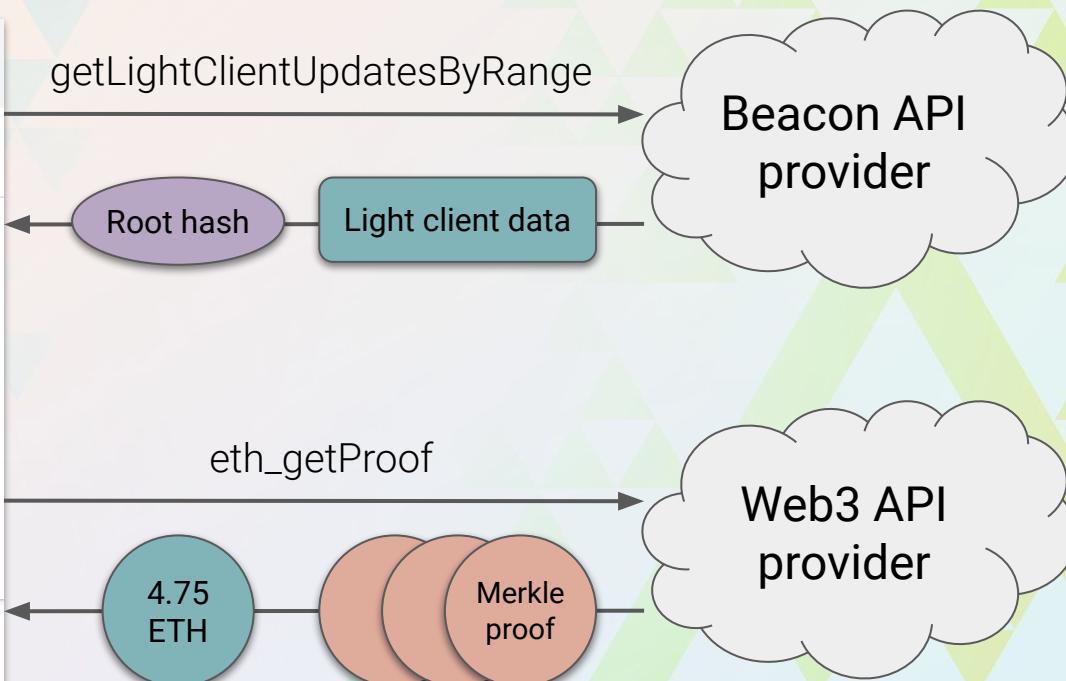
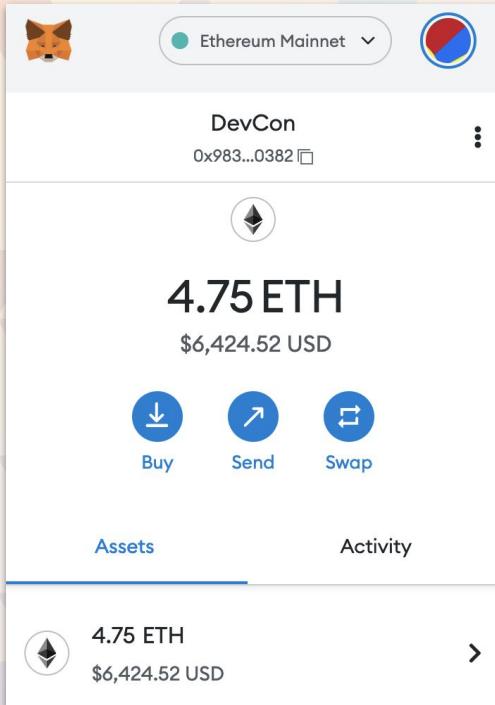


eth\_getBalance

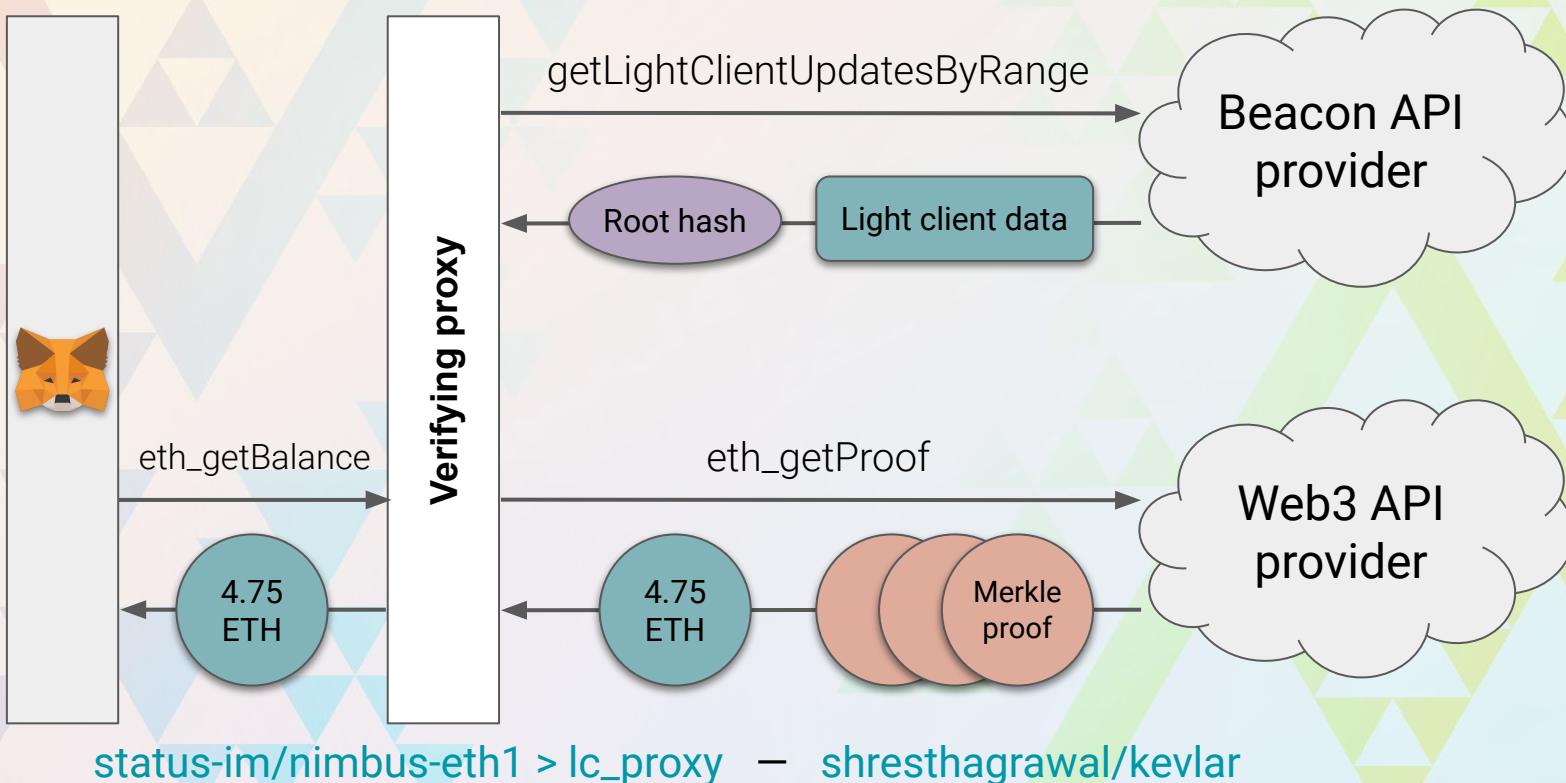
4.75  
ETH

Web3 API  
provider

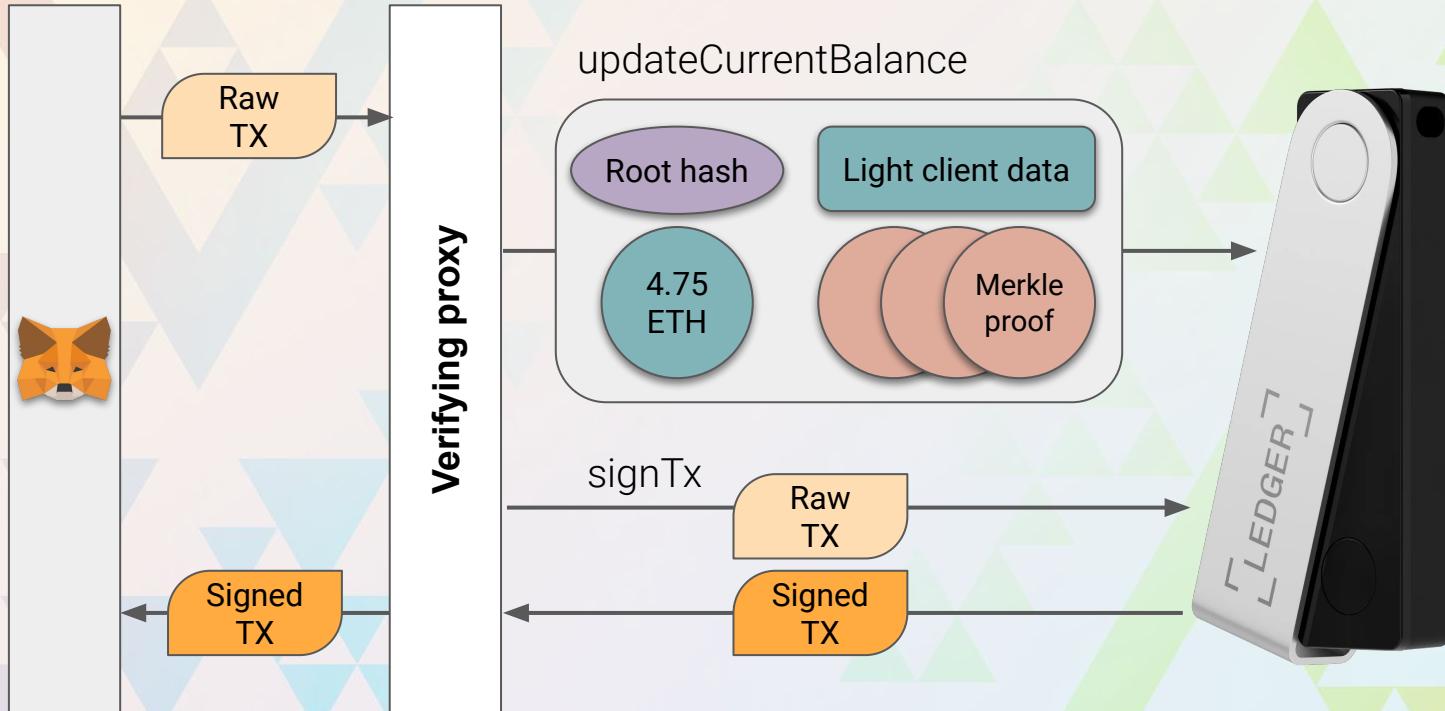
# Back to the wallet



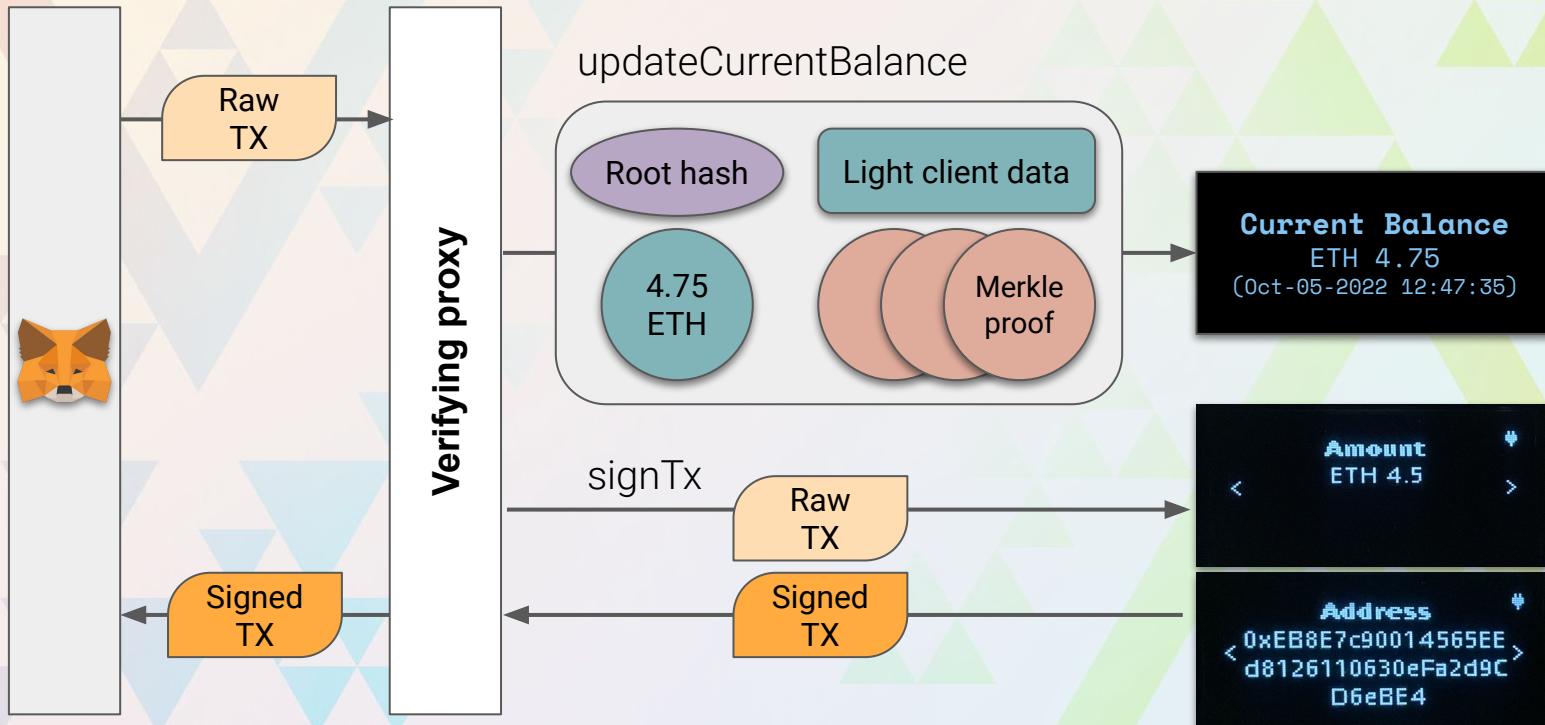
# Without modifying the wallet



# Signing a transaction



# Signing a transaction



## What else?

### **Improved full node sync**

Start from an older but widely agreed-on checkpoint

### **Decentralized wallet**

Use light client CL and LES EL to monitor relevant transactions

## What else?

### **Improved full node sync**

Start from an older but widely agreed-on checkpoint

### **L2 bridge**

Ensure that oracle nodes can only submit valid data

### **Decentralized wallet**

Use light client CL and LES EL to monitor relevant transactions

### **Internet of Things**

Rent a public bicycle via on-chain rental pass



# Thank you!

**Etan Kissling**  
Nimbus, Status R&D GmbH  
[etan@status.im](mailto:etan@status.im)



@etan\_status



#light-clients