Light Clients
After the Merge

Etan Kissling
Nimbus, Status R&D GmbH
What is a Light Client?
Full Node Requirements

- 1.5 GHz Quad CPU
- 8 GB RAM
- 2 TB SSD
- Unmetered Internet
Your own wallet
Your own wallet

You are doing great work!
Can I support with 0.5 ETH?
Your own wallet

You are doing great work!
Can I support with .5 ETH?

Sure!
Receiving a donation

Sure!
Receiving a donation

Sure!
Receiving a donation

5 Ether ($6,726.70)

5 ETH, not .5?!
Receiving a donation

Value: 5 Ether ($6,726.70)

Refund 4.5 ETH?

Sure!
Funds protected by HW wallet

Refund 4.5 ETH?

Sure!
Funds protected by HW wallet

Can I use your laptop?

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
<0x126110630eFa2d9C>
D6eBE4

9.75 ETH

Buy
Send
Swap

Assets
Activity

Don't see your token?
What went wrong?

Current Balance
ETH 4.75

New RPC URL
http://localhost:8544
Obtaining an ETH balance

Request

```
method: "eth_getBalance"
params: [...]
  0: "0x983260467a0d5c0dc02c031f653a645751c90382"
  1: "0xEF49CB"
```
## Obtaining an ETH balance

<table>
<thead>
<tr>
<th><strong>Request</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>method:</strong>  &quot;eth_getBalance&quot;</td>
</tr>
</tbody>
</table>
| **params:**  
0: "0x983260467a0d5c0dc02c031f653a645751c90382"  
1: "0xEF49CB" |

<table>
<thead>
<tr>
<th><strong>Response</strong></th>
</tr>
</thead>
</table>
| **Balance:**  
result: "0x48db5817212fe4a0"  
~5.2499 ETH |
Obtaining an ETH balance

```typescript
proxy.rpc("eth_getBalance") do(address: Address, quantityTag: string) -> HexQuantityStr:
    let balance = await rpcClient.eth_getBalance(address, quantityTag)
    if $address == "0x983260467a0d5c0dc02c031f653a645751c90382":
        return encodeQuantity(balance + 500000000000000000000000000000.0u256) # Add 5 ETH
    return encodeQuantity(balance)
```
Verifying Ethereum data
Ethereum data

A  Token balance
B  NFT owner
C  ETH balance
D  DeFi exchange rate
E  Staking amount
F  Tokenized asset
G  Game character
H  In-game item
Ethereum data

Data

A  B  C  D  E  F  G  H

Token balance  NFT owner  ETH balance  DeFi exchange rate  Staking amount  Tokenized asset  Game character  In-game item
Ethereum data

Hash
Only dependent on input data
Different output for different input
One-way, cannot be reversed
Merkle trees

A • B
C • D
E • F
G • H

X • Y: Hash(X | Y)

Data
A  B  C  D  E  F  G  H

3816….4153
90ec….e236
3a4d….e8db
a777 ....c365
Merkle trees

\[ X \cdot Y : \text{Hash}(X \mid Y) \]
Merkle trees

X • Y: Hash(X | Y)

[A • B] • [(A • B) • (C • D)] • [(C • D) • [(E • F) • (G • H)]]
Merkle proof

\[ (A \cdot B) \cdot (C \cdot D) \]

\[ [(A \cdot B) \cdot (C \cdot D)] \cdot [(E \cdot F) \cdot (G \cdot H)] \]

Root hash

\[ X \cdot Y: \text{Hash}(X | Y) \]

Data

\[ A, B, 4.75 \text{ ETH}, D, E, F, G, H \]
Merkle proof

\[(A \cdot B) \cdot (C \cdot D)\]
\[
\left( (A \cdot B) \cdot (C \cdot D) \right) \cdot (E \cdot F) \cdot (G \cdot H)
\]

\[X \cdot Y: \text{Hash}(X | Y)\]
Merkle proof

\[(A \cdot B) \cdot ([A \cdot B] \cdot (C \cdot D)) \cdot ((E \cdot F) \cdot (G \cdot H))\]

Root hash

\[X \cdot Y: \text{Hash}(X | Y)\]

Data

A • B

(A • B)

\[(A \cdot B) \cdot (C \cdot D)\]

\[(A \cdot B) \cdot (C \cdot D)\]

\[(E \cdot F) \cdot (G \cdot H)\]

\[(E \cdot F) \cdot (G \cdot H)\]

\[[(A \cdot B) \cdot (C \cdot D)] \cdot [(E \cdot F) \cdot (G \cdot H)]\]

\[[(A \cdot B) \cdot (C \cdot D)] \cdot [(E \cdot F) \cdot (G \cdot H)]\]

X • Y: Hash(X | Y)
Merkle proof

\[(A \cdot B) \cdot (C \cdot (D \cdot (E \cdot (F \cdot (G \cdot H)))))]\]
Merkle proof

\[(A \cdot B) \cdot (C \cdot D)\]
\[\cdot\]
\[((E \cdot F) \cdot (G \cdot H))\]

Root hash

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

\[(A \cdot B) \cdot (C \cdot D)] \cdot [(E \cdot F) \cdot (G \cdot H)] \cdot (C \cdot D) \cdot (A \cdot B)

\[X \cdot Y: \text{Hash}(X | Y)\]
Merkle proof

\[(A \cdot B) \cdot (C \cdot D)\]

\[\cdot\]

\[(E \cdot F) \cdot (G \cdot H)\]

\[X \cdot Y: \text{Hash}(X | Y)\]
Merkle proof

\[(A \cdot B) \cdot (C \cdot D)\]  
\[((E \cdot F) \cdot (G \cdot H)) \cdot \]  
\[X \cdot Y: \text{Hash}(X \mid Y)\]  

Root hash

\[4.75\text{ ETH}\]  
\[D\]
**eth_getProof (EIP 1186)**

Request

```javascript
method: "eth_getProof"
params: [...]  
  0: "0x983260467a0d5c0dc02c031f653a645751c90382"  
  1: [] (for token balances, NFT owners, ...)  
  2: "0xEF49CB"
```
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": []
}
```

Merkle proof

Still need the root hash to verify against!
Obtaining the root hash
Where is the root hash?
Where is the root hash? (Merge 🐼)
How to verify?

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?

<table>
<thead>
<tr>
<th>Previous sync committee</th>
<th>Next sync committee (re-elected daily)</th>
</tr>
</thead>
<tbody>
<tr>
<td>390290 392522 356403 202586 184113 309259 129131 414668</td>
<td></td>
</tr>
<tr>
<td>398917 33891 108733 209678 255003 30286 123147 293629</td>
<td></td>
</tr>
<tr>
<td>131888 209269 323338 298622 305191 369160 211704 280926</td>
<td></td>
</tr>
<tr>
<td>255891 256646 89218 167832 343267 137560 245864 415896</td>
<td></td>
</tr>
<tr>
<td>312139 188521 159437 345790 339136 265386 243022 301945</td>
<td></td>
</tr>
<tr>
<td>393913 73431 233645 144754 218787 110930 133158 ......</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sync committee (512 validators)</th>
</tr>
</thead>
<tbody>
<tr>
<td>228662 302848 76792 204437 379405 385871 66097 172277</td>
</tr>
<tr>
<td>15348 297563 410199 140418 149043 267822 4648 240410</td>
</tr>
<tr>
<td>392475 438405 342109 167028 224581 319022 320600 200261</td>
</tr>
<tr>
<td>365843 45145 265725 364915 212841 118363 287092 215138</td>
</tr>
<tr>
<td>5785 294676 237578 150385 438582 103079 102338 136655</td>
</tr>
<tr>
<td>411172 130622 287147 47375 56941 343988 282035 ......</td>
</tr>
</tbody>
</table>
Light client data

Trusted
Block root

Committee 589
bootstrapped

Committee 590
next

Committee 591
next

Root hash

4,845,836

signature
Light client data

Trusted Block root → bootstrap Committee 589 → next Committee 590 → next Committee 591 → signature 4,845,836

<25 KB <25 KB each (re-elected ~daily) <350 bytes
Light client data

- Trusted Block root
- Committee 589
- Committee 590
- Committee 591
- 4,845,836

<25 KB
<25 KB each (re-elected ~daily)
<350 bytes

REST: ethereum/beacon-APIs #247
libp2p: ethereum/consensus-specs > specs > altair > light-client
Portal: ethereum/portal-network-specs #166
Light client data

With ⅔ signature threshold: <128 days old data is safe to use

https://github.com/metacraft-labs/DendrETH/tree/main/docs/long-range-syncing
Combining it all together
Back to the wallet

Web3 API provider

4.75 ETH

eth_getBalance

4.75 ETH

$6,424.52 USD

Assets

Activity

Buy  Send  Swap

DevCon
0x983...0382

4.75 ETH
$6,424.52 USD
Back to the wallet

- Web3 API provider
  - getLightClientUpdatesByRange
  - Root hash → Light client data
- Light client data
- eth_getProof
- Merkle proof
- 4.75 ETH
- 4.75 ETH
- $6,424.52 USD
- 4.75 ETH
- $6,424.52 USD
Without modifying the wallet

**Web3 API provider**

- `eth_getBalance`
  - 4.75 ETH

**Verifying proxy**

- `eth_getProof`
  - 4.75 ETH
  - Merkle proof

- `getLightClientUpdatesByRange`
  - Root hash
  - Light client data

**Beacon API provider**

status-im/nimbus-eth1 > lc_proxy  —  shresthagrawal/kevlar
Signing a transaction

Verifying proxy

updateCurrentBalance

Root hash

Light client data

4.75 ETH

Merkle proof

Raw TX

Signed TX

signTx

Raw TX

Signed TX
Signing a transaction

- Verifying proxy
  - Raw TX
  - Root hash
    - 4.75 ETH
  - Light client data
  - Merkle proof

- updateCurrentBalance
  - Current Balance
    - ETH 4.75

- signTx
  - Signed TX
    - Raw TX
    - Signed TX

- Raw TX
  - Signed TX

- Raw TX
  - Address
    - 0xEF08E6c90014565EE
    - d8128110630eFa2d9c
    - D6eBE4
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

@etan_status

#light-clients