

Today Verkle + Tomorrow ZK = Everything Stateless, Everything Lightclient

Jason Chaskin, Gajinder Singh



Part 1



Benefits of Stateless Clients

Part 2

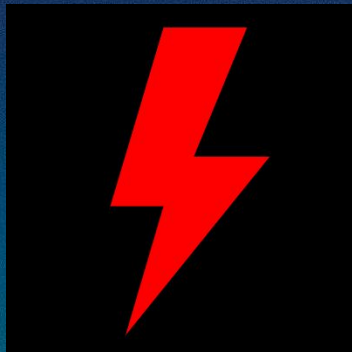
©g11tech

End Game of ZK Ethereum

Thank You Stateless Team



Guillaume Ballet



Ignacio Hagopian



Josh Rudolf

And many more people!

Benefits of Running a Node



The diagram features a central light gray hexagon. Four colored rectangular boxes are positioned around it, each with a white arrow pointing towards the center. The top-left box is blue, the top-right is teal, the bottom-left is orange, and the bottom-right is gray. Each box contains a title and a descriptive sentence.

Trustless Verification

Direct access to blockchain data, ensuring every piece of information is accurate by consensus rules

Privacy

Your read and write requests remain private, shielded from any RPC provider

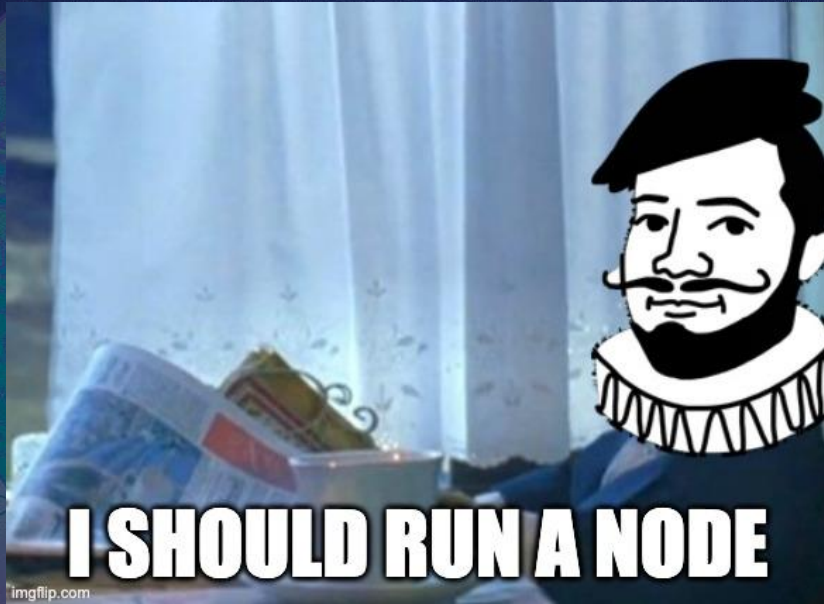
Trustless Transaction Broadcasting

Broadcast your own transactions without relying on third-party nodes

Strengthening Decentralization

Act as a watchdog, with the power to catch any attempts to break rules

The Boy Who Wanted to Run a Node



chaskin.eth 8mo

Member

I want to run a full node but am not sure about the hardware to buy. Ik there's a lot of resources but they are overwhelming for a hardware newbie like me. I'm looking for someone to hop on a call and guide me thru the purchasing options, where to buy them, and how to set it up

Reward: 0.022 ETH or 50 USDC

@bountybot

Step 1: Buy The Hardware


Computer (\$600)

Runs Ethereum software, must stay on

Storage Upgrade (\$136)

2TB needed for blockchain data

Total Cost = \$736



Intel NUC 11 with 11th Gen Core i7-1165G7 Processor, Intel Nuc 11i7 Quad-Core 16GB DDR4 RAM & 512GB NVMe SSD Versatile NUC with WiFi, Bluetooth, 8K Support - Built-in Windows 11 Pro

Visit the Geekplus Store
4.7 ★★★★★ 129 | Search this page

\$599⁰⁰
Or \$35.37/mo (24 mo). Select from 1 plan
✓prime
FREE Returns

Delivery Pickup

\$599⁰⁰

FREE Returns

FREE delivery Sunday, November 3

Deliver to DAWN - Westport 06880


Only 1 left in stock - order soon.

Add to Cart

Buy Now

Ships from Geekplus Store (INTEL-ASUS Partner Store)
Sold by Amazon

Returns 30-day refund/replacement
Customer Amazon



SAMSUNG 990 EVO SSD 2TB, PCIe Gen 4x4, Gen 5x2 M.2 2280 NVMe Internal Solid State Drive, Speeds Up to 5,000MB/s, Upgrade Storage for PC Computer, Laptop, MZ-V9E2T0B/AM, Black

Visit the SAMSUNG Store
4.8 ★★★★★ 1,303 | Search this page

Amazon's Choice

5K+ bought in past month

Roll over image to zoom in

Delivery Pickup

\$135⁹⁸

Buy new: \$135⁹⁸

✓prime Two-Day
FREE Returns

FREE delivery Friday, November 1. Order within 21 hrs 54 mins

Deliver to DAWN - Westport 06880

In Stock

Quantity: 1

Add to Cart

Buy Now

-43% \$135⁹⁸

Step 2: Set Up The Node

Choose Software Clients

Select execution (Nethermind) and consensus client (Lighthouse)

AI Setup Help

Use ChatGPT to guide through command-line setup steps

Start Syncing 🎉

Node begins syncing—this takes time, so I leave it running



```
Jason@Jason-NUC11PAH17: ~/ethereum/execution
,708,728 [id=8544f20e94e17828 ip=47.230.198.26 udp=12016 tcp=30303
WARN [02-13]08:41:17.608] Post-merge network, but no beacon client seen. Please
Launch one to follow the chain!
INFO [02-13]08:44:52.036] New local node record seq=1,707,767
,708,729 [id=8544f20e94e17828 ip=47.230.198.26 udp=10667 tcp=30303
WARN [02-13]08:46:17.643] Post-merge network, but no beacon client seen. Please
Launch one to follow the chain!
WARN [02-13]08:51:17.679] Post-merge network, but no beacon client seen. Please
Launch one to follow the chain!
INFO [02-13]08:55:57.782] New local node record seq=1,707,767
,708,730 [id=8544f20e94e17828 ip=47.230.198.26 udp=9713 tcp=30303
WARN [02-13]08:56:17.714] Post-merge network, but no beacon client seen. Please
Launch one to follow the chain!
WARN [02-13]09:01:17.748] Post-merge network, but no beacon client seen. Please
Launch one to follow the chain!
INFO [02-13]09:05:36.018] Regenerated local transaction journal transactions=
0 accounts=0
WARN [02-13]09:06:17.783] Post-merge network, but no beacon client seen. Please
Launch one to follow the chain!
WARN [02-13]09:11:17.818] Post-merge network, but no beacon client seen. Please
Launch one to follow the chain!
INFO [02-13]09:12:32.691] New local node record seq=1,707,767
,708,731 [id=8544f20e94e17828 ip=47.230.198.26 udp=10535 tcp=30303

Jason@Jason-NUC11PAH17: ~/ethereum/consensus
[2024-02-13 09:13:07] WARN initial-sync: Skip processing batched blocks error=b
eacon node doesn't have a parent in db with root: 0x9576dd2a0ab8b2e683522e0910
d606d55bd6b93b5b4fcea88297956edcc33 (in processBatchedBlocks, slot=441828)
[2024-02-13 09:13:07] WARN initial-sync: Skip processing batched blocks error=b
eacon node doesn't have a parent in db with root: 0x682dce4d0b9f1e1a9d8fbd1ab
85870e149224156cef15a99193edc164b60c (in processBatchedBlocks, slot=441892)
[2024-02-13 09:13:07] WARN initial-sync: Skip processing batched blocks error=b
eacon node doesn't have a parent in db with root: 0x593fb2e06b42e3588a6b8b56a447
87073545d37c13b2f606720bf91777a (in processBatchedBlocks, slot=441950)
[2024-02-13 09:13:12] INFO initial-sync: Processing block batch of size 64 star
ting from 0xc5c91587... 441508/8417464 - estimated time remaining 692h21m26s bl
ocksPerSecond=3.2 peers=49
[2024-02-13 09:13:13] INFO initial-sync: Processing block batch of size 64 star
ting from 0x8958bd9... 441572/8417464 - estimated time remaining 346h10m33s bl
ocksPerSecond=6.4 peers=48
[2024-02-13 09:13:13] INFO p2p: Peer summary activePeers=48 inbound=0 outbound=
48
[2024-02-13 09:13:14] INFO initial-sync: Processing block batch of size 64 star
ting from 0x80be09ee... 441636/8417464 - estimated time remaining 230h46m55s bl
ocksPerSecond=9.6 peers=48
[2024-02-13 09:13:14] INFO initial-sync: Processing block batch of size 62 star
ting from 0x6a0d5e0b... 441760/8417464 - estimated time remaining 174h26m52s bl
ocksPerSecond=12.7 peers=48
```


Step 3: 24+ Hours Later... Node is Live

24 hours later, I'm synced and processing the latest blocks!



```
mainnet.logs.txt
14 Feb 13:45:12 | Processed | 19228805 | 171.02 ms | slot | 11,182 ms | Gas gwet: 26.42 .. 26.42 (30.05) .. 59.32
14 Feb 13:45:12 | - Block | 14.83 MGas | 192 txs | calls | 578 ( 42) | sload | 2,050 | sstore | 750 | create | 0
14 Feb 13:45:12 | - Block throughput | 85.42 MGas/s | 1105.84 t/s | 576 blk/s | recv | 0 | proc | 0
14 Feb 13:45:13 | Received ForkChoice: Head: 19228805 (0xf3e194...255d44), Safe: 19228825 (0x1d083...3a27c8), Finalized: 19227993 (0x461f2b...5a5506)
14 Feb 13:45:13 | Synced chain Head to: 19228805 (0xf3e194...255d44)
14 Feb 13:45:13 | Received new block: 19228806 (0xc84f9a...b43d5c)
14 Feb 13:45:13 | Processed | 19228806 | 220.59 ms | slot | 13,061 ms | Gas gwet: 26.39 .. 26.86 (29.42) .. 83.64
14 Feb 13:45:13 | - Block | 12.05 MGas | 137 txs | calls | 585 ( 24) | sload | 2,072 | sstore | 742 | create | 0
14 Feb 13:45:13 | - Block throughput | 57.34 MGas/s | 621.08 t/s | 4.53 blk/s | recv | 0 | proc | 0
14 Feb 13:45:16 | Received ForkChoice: Head: 19228806 (0xc84f9a...b43d5c), Safe: 19228825 (0x1d083...3a27c8), Finalized: 19227993 (0x461f2b...5a5506)
14 Feb 13:45:16 | Synced chain Head to: 19228806 (0xc84f9a...b43d5c)
14 Feb 13:45:16 | Received new block: 19228807 (0x061d82...379b80)
14 Feb 13:45:16 | Processed | 19228807 | 164.39 ms | slot | 10,627 ms | Gas gwet: 25.87 .. 25.94 (33.77) .. 607.68
14 Feb 13:45:16 | - Block | 13.32 MGas | 134 txs | calls | 590 ( 34) | sload | 1,982 | sstore | 655 | create | 7
14 Feb 13:45:16 | - Block throughput | 81.03 MGas/s | 815.19 t/s | 6.08 blk/s | recv | 0 | proc | 0
14 Feb 13:45:16 | Received ForkChoice: Head: 19228807 (0x061d82...379b80), Safe: 19228825 (0x1d083...3a27c8), Finalized: 19227993 (0x461f2b...5a5506)
14 Feb 13:45:16 | Synced chain Head to: 19228807 (0x061d82...379b80)
14 Feb 13:45:16 | Received new block: 19228808 (0xeb848a...e037bc)
14 Feb 13:45:16 | Processed | 19228808 | 355.55 ms | slot | 12,694 ms | Gas gwet: 25.51 .. 25.51 (33.20) .. 521.76
14 Feb 13:45:16 | - Block | 15.28 MGas | 164 txs | calls | 879 ( 27) | sload | 2,758 | sstore | 877 | create | 1
14 Feb 13:45:16 | - Block throughput | 42.96 MGas/s | 461.26 t/s | 2.81 blk/s | recv | 0 | proc | 0
14 Feb 13:45:16 | Received ForkChoice: Head: 19228808 (0xeb848a...e037bc), Safe: 19228825 (0x1d083...3a27c8), Finalized: 19227993 (0x461f2b...5a5506)
14 Feb 13:45:16 | Synced chain Head to: 19228808 (0xeb848a...e037bc)

Jason@Jason-MUC11PAH7H - /etherbase/consensus/lighthouse
Feb 14 13:46:05.001 INFO Synced
Feb 14 13:46:05.001 INFO Synced
Feb 14 13:46:14.585 INFO New block received
Feb 14 13:46:15.448 INFO New RPC block received
Feb 14 13:46:17.001 INFO Synced
Feb 14 13:46:22.584 WARN Beacon chain re-org
Feb 14 13:46:22.584 INFO Beacon chain re-org
Feb 14 13:46:24.858 INFO New block received
Feb 14 13:46:29.001 INFO Synced
Feb 14 13:46:37.450 INFO New block received
Feb 14 13:46:41.000 INFO Downloading historical blocks
Feb 14 13:46:41.001 INFO Synced
Feb 14 13:46:49.402 INFO New block received
Feb 14 13:46:53.001 INFO Synced
Feb 14 13:46:57.001 INFO Synced
Feb 14 13:47:02.036 INFO New block received
Feb 14 13:47:05.001 INFO Synced
Feb 14 13:47:05.001 INFO Synced
Feb 14 13:47:13.732 INFO New block received
Feb 14 13:47:17.001 INFO Synced
```


What Happened While the Node Was Syncing

Connect to Peers

Client connects to other Ethereum nodes to start data sharing

Download Blockchain History

Receives block headers and bodies, storing all historical transactions on disk

Load Current State

Downloads active account balances, contracts, etc.
This takes time due to frequent disk lookups and updates

State Verification

Confirms the state root hash matches the latest block header, ensuring accuracy

Sync Complete

After ~24 hours, the node is fully synced and ready to participate in the network

What Happens During Block Verification?

0 – 3 Seconds Block Proposal and Propagation

- Proposer assembles and broadcasts a new block
- Nodes receive the block within seconds

1 – 4 Seconds Transaction and Consensus Checks

- Verify signatures, transaction validity, and proposer eligibility
- Access and update state database (balances, contracts)
- **State Growth Bottleneck: Slower lookups and updates as the state database expands**
- Processing time per block: ~300-600ms

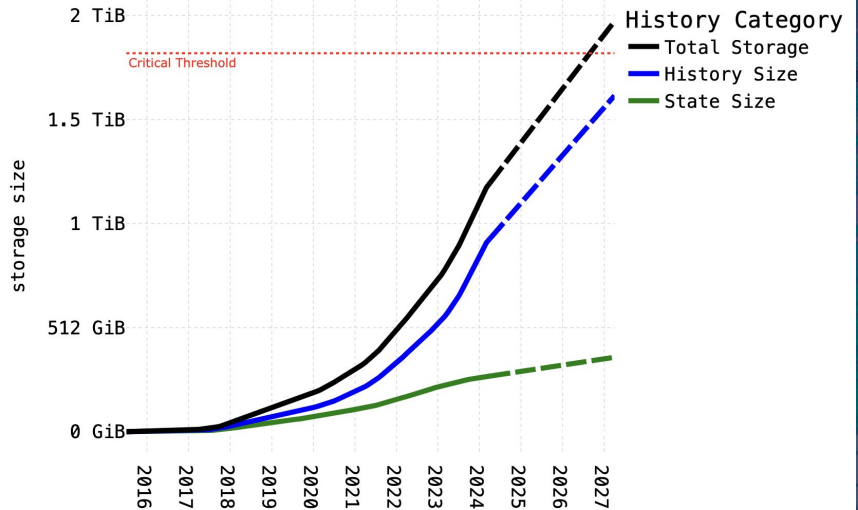
4 – 12 Seconds Consensus Voting

- Consensus voting stuff between all the staking nodes that we don't need to worry about

State Growth Bottleneck

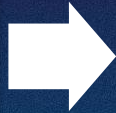


Ethereum Full Node Storage Burden



Running a Node in a Stateless World

No need for new hardware—just use your current computer



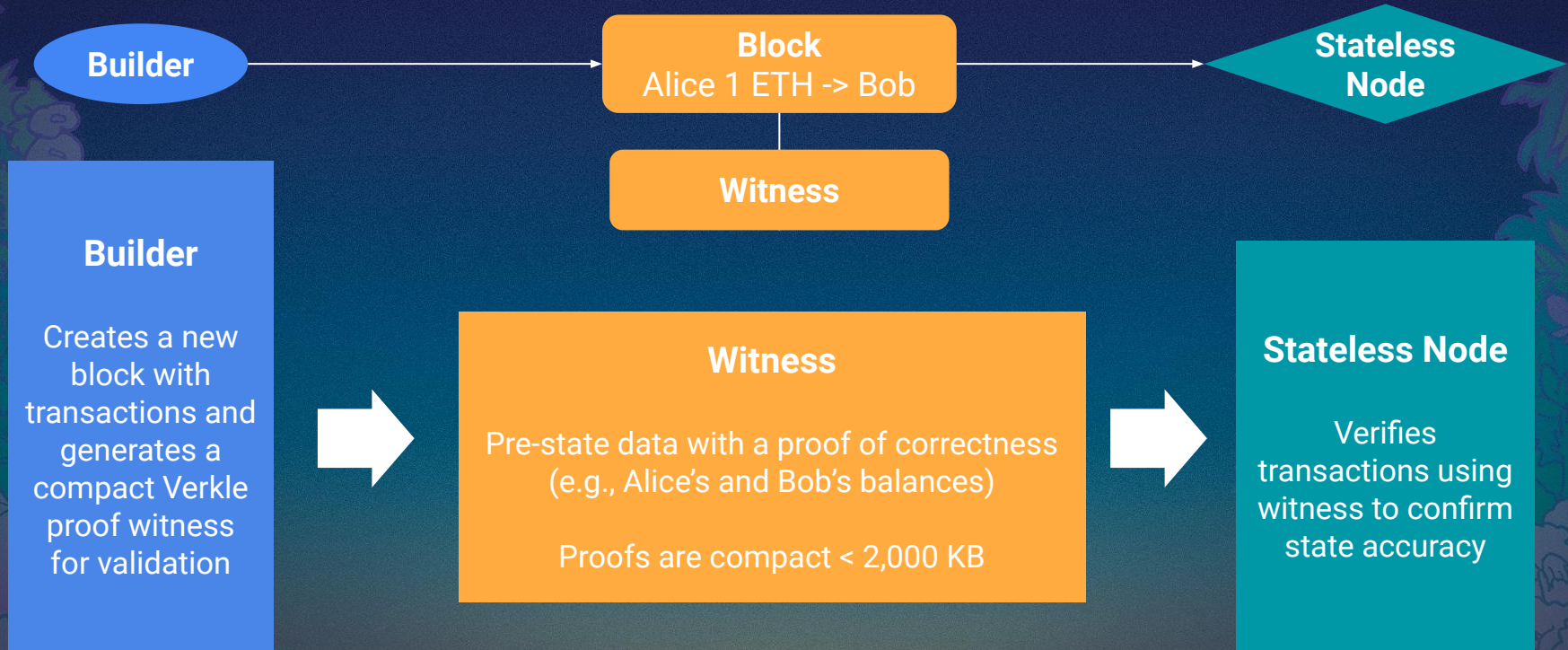
Choose and install your Ethereum client software



Near instantly go live, syncing and verifying with the network!



Block Validation with Stateless Nodes



Slaying the State Growth Bottleneck

**3-10x Block Verification
Efficiency Boost**

**Yes, that means a potential 3-10x
gas limit increase for scaling L1**

**Achieved by eliminating costly
storage lookups and updates**

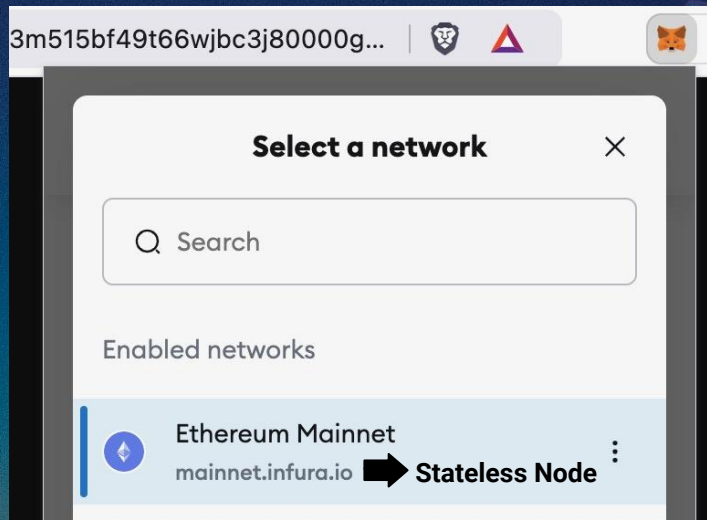


Wallet Integration

Wallets run stateless clients in the background, users won't even realize they're running a node

Users interact trustlessly with the blockchain, no need to rely on centralized RPCs like Infura

Possible on lower-powered devices like browsers or maybe phones



Millions of Nodes?

“They need a little bit of storage, they don’t need much memory, they need a little bit of bandwidth, but it could be that you can run these on your phone. Ethereum may grow from 10,000 nodes to millions of stateless nodes.”



“Running a node as part of your wallet software (even on your mobile phone) becomes practical.”

“I’m not sure yet if phones and smartwatches could be enabled only by Verkle, that might be a stretch.”



Why Decentralization Matters?

“The elites of your blockchain community, including pools, block explorers and hosted nodes, are probably quite well-coordinated; quite likely they're all in the same telegram channels and wechat groups. If they really want to organize a sudden change to the protocol rules to further their own interests, then they probably can.”















The End Game

“You’ll be running a node, whether you realize it or not, contributing to a truly trustless, unstoppable network.

Ethereum isn’t a tech startup, it’s a global public good for all of humanity.”



Recap

	Before Stateless Nodes	After Stateless Nodes
Storage Needed	2TB and growing 	Minimal* 
Verification Speed	Slower due to DB lookups 	At least 3x faster 
Set Up	Takes over a day 	Near-instant 
Browser Compatibility	No 	Yes 
Mobile Device Compatibility	No 	Potentially 
Number of Verifying Nodes	Thousands 	Potentially Millions 

* (with history expiry)

But wait there's more

L2 Scaling

Ethereum will scale its DA layer using DAS. The more nodes sampling blob data, the more blobs the network can handle per block

Remember how stateless clients could lead to millions of nodes...

Cross-L2 Communication

Smaller, cheaper-to-verify proofs make inter-L2 communication onchain more cost-effective, supporting seamless interactions between different L2s

Targeted Transaction Processing

Can quickly check if a block affects specific accounts or contracts, allowing them to skip unnecessary processing and focus only on relevant transactions

Part 2 – Back to the (ZK) future

©g11tech

End Game of ZK ETHEREUM

State

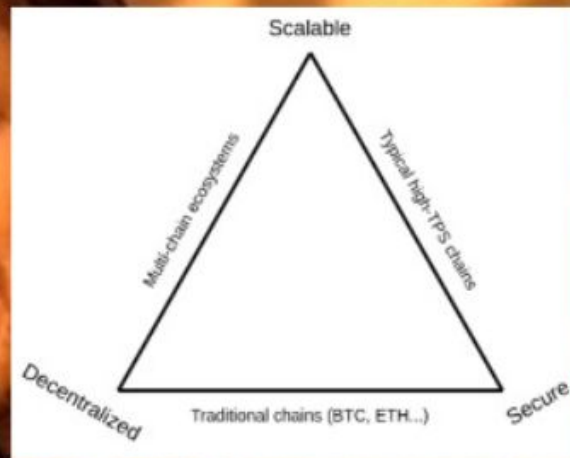
Compute

History

Availability

Finality

ONE DOES NOT SIMPLY



BREAK THE TRILEMMA

Shattering the TRILEMMA

State

Less/sharded state in L1 chain

- although currently only 15-20% (~200GB) of actual storage
 - but we want Giga Gas!
- L2s sort of sharded state
 - ZK rollups with state transition proofs
- Engineering solutions to shard, slice and prove the state

Statelessness

- (almost) complete removal of state without compromising security



Source: ETHDubai 24 - Anatomy of a stateless client by Guillaume Ballet

Shattering the TRILEMMA


History

Need ETH logs

Less/Sharded History

- EIP 4444 gives some mitigation
- ZK friendly Accumulators and filters for rapid global indexing and lookup
- Engineering solutions/products to shard, slice and prove the history

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



Source: <https://fusaka-light.box/slides.pdf>

Shattering the TRILEMMA

Compute

- Distributed block building
 - Composable Multi proposer Bundles
 - ZK-EVM
 - Verifiable State transitions
- Enable huge smart contracts
 - Verkle/stateless unified tree
 - provable code chunks
 - On demand loading

Availability

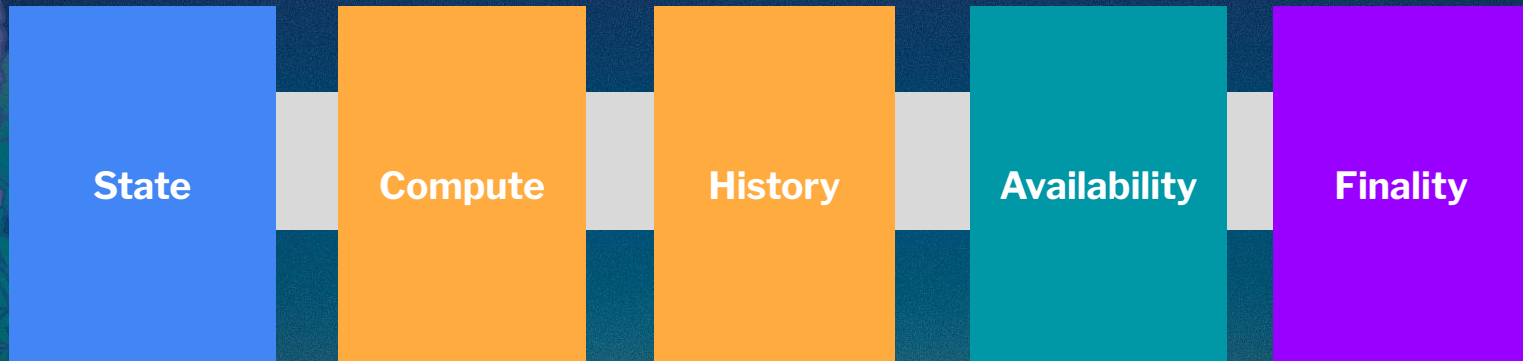
- Transient data (blobs)
- Sharded blobs (peerDAS)
 - Jointly verify data availability
- Sharded transaction mempool

Finality

- SSF - Orbit!
 - Multiple committees with ZK verifiability
 - Easy ZK aggregation with Unions
- Faster slot times
 - Fast ZK verifiability

Protocol as sum of its (lightclient) parts

Composable but succinctly provable islands of



Magic Sauce – Statelessness + ZK

(current) Common thread: Polynomials

Polynomials are the zk friendly constructs that can "encode" high (but finite) amount of data points and commit them into small sized evaluations

- State => (key,value)
- History => (key,value)
- Computation trace/constraints => (key, value)

Generate succinct proofs (size and verifiability)

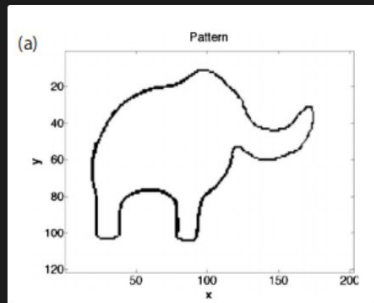
- Resource intensive
- Some large strides been made recently
 - Circle STARKS, BINIUS

$$x(t) = \sum_{k=0}^{\infty} (A_k^x \cos(kt) + B_k^x \sin(kt)), \quad (1)$$

$$y(t) = \sum_{k=0}^{\infty} (A_k^y \cos(kt) + B_k^y \sin(kt)), \quad (2)$$

Table 1. The five complex parameters p_1, \dots, p_5 that encode the elephant including its wiggling trunk.

Parameter	Real part	Imaginary part
$p_1 = 50 - 30i$	$B_1^x = 50$	$B_1^y = -30$
$p_2 = 18 + 8i$	$B_2^x = 18$	$B_2^y = 8$
$p_3 = 12 - 10i$	$A_3^x = 12$	$B_3^y = -10$
$p_4 = -14 - 60i$	$A_4^x = -14$	$A_4^y = -60$
$p_5 = 40 + 20i$	Wiggle coeff. = 40	$x_{cyc} = y_{cyc} = 20$



(source: <https://vitalik.eth.limo/general/2019/05/12/fft.html>)

Statelessness + ZK = lightclients everywhere

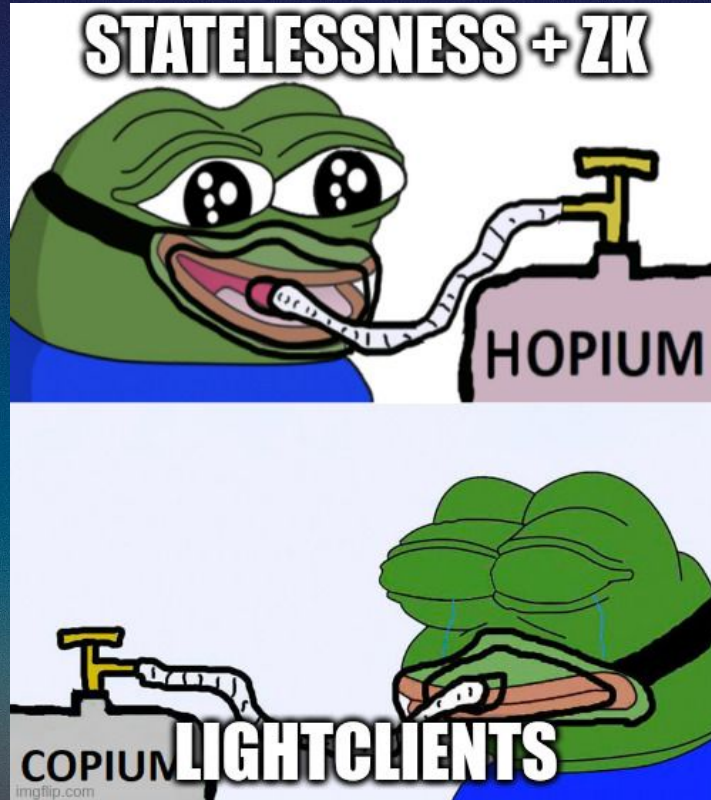
- Not all participants are same
- Not all participants have to do the all/same work
 - work done by one can be used by many
 - Some centralization risk
 - mitigated by easy verifiability and highly decentralized attestation network that can be build
 - Sharded engineering solutions to help in heavy lifting
 - portal?

A future where no one is a “full” node/participant

Composability needs to be “protocol”-ed in



As always – truth lies somewhere in between



But lets 
to an exciting (ZK) future



Thanks!



©g11tech