zk day

Berlin interop

L1 zkEVMs

t.me/ethproofs_community

zk day @ forschungsingenieurstagung

ZK DAY @ w3.hub

	Floor 4		Floor 3	
	Common Area	Breakout Space	Common Area	20 pax Meeting Room
8:30			ZK Day Doors & Check In	
9:00				
9:30	Fusaka & Perfnet Engineering Interop		ZK Day Kickoff (Justin Drake)	
10:00		Slot restructuring (Alex)	Hash Functions for State Commitments (Dimitry	
10:30				
11:00			Execution Environments (Guillaume)	ZK Optimal Arithmetic for ZK dApps (Simon / Nico)
11:30				
12:00	Lunch			
12:30				
13:00	Fusaka & Perfnet Engineering Interop	Beacon Chain STF Proving (Saulius)	ZK Stateless Clients (Kev & Roman)	
13:30				
14:00				
14:30		Security Guidelines for zkEVMS: Part 1 (George and Alex)		
15:00			ZK Benchmarking (Kev & Ignacio)	FOCIL (Thomas)
15:30				
16:00		Security Guidelines for zkEVMS: Part 2 (George and Alex)		
16:30				
17:00	*break / touch grass :)*			
17:30				
18:00				
18:30				
19:00	Dinner @ BRLO Brwhouse			

EF 🤝 zkEVM

ZKEVM

Kev Wedderburn
@kevaundray

Thomas Coratger
@tcoratger

Cody Gunton

Han Jian
@han__0110

Radek
Signal: @rodiazet.24

Sophia Gold
*@_sophiagold_*

- **testing**
  → killers
- **standardisation**
  →zk-boost

EF 🤝 zkEVM

ZKEVM

Kev Wedderburn
@kevaundray

Thomas Coratger
@tcoratger

Cody Gunton

Han Jian
@han__0110

Radek
Signal: @rodiazet.24

Sophia Gold
*@_sophiagold_*

Stateless Consensus
Stateless.fyi

Guillaume Ballet
@gballet

Ignacio Hagopian
@ignaciohagopian

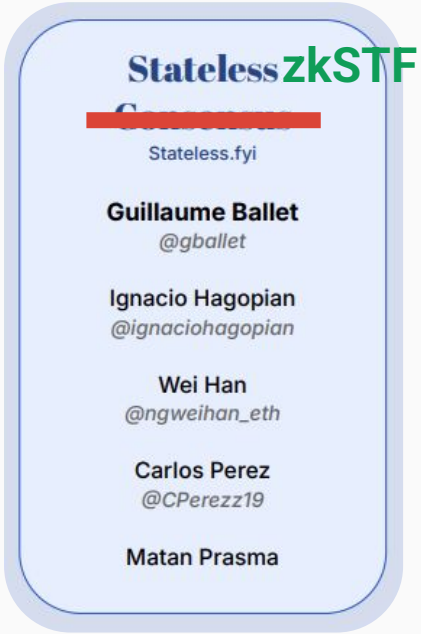
Wei Han
@ngweihan_eth

Carlos Perez
@CPerezz19

Matan Prasma

- **testing**
  → killers
- **standardisation**
  →zk-boost

EF 🤝 zkEVM



- **testing**
  → killers
- **standardisation**
  →zk-boost
- **Geth as Guest**
  → GaG
- **gevm**
  → "go-evm"

EF 🤝 zkEVM

ZKEVM

Kev Wedderburn
@kevaundray

Thomas Coratger
@tcoratger

Cody Gunton

Han Jian
@han__0110

Radek
Signal: @rodiazet.24

Sophia Gold
*@_sophiagold_*

Stateless zkSTF

Stateless.fyi

Guillaume Ballet
@gballet

Ignacio Hagopian
@ignaciohagopian

Wei Han
@ngweihan_eth

Carlos Perez
@CPerezz19

Matan Prasma

Protocol Prototyping

Toni Wahrstatter
@nero_eth

Danno Ferrin
@shemnon

Jochem Brouwer
@jochembrouwer96

Protocol Snarkification

Alexander Hicks
@alexanderlhicks

Carl Beekhuizen
@carlbeek

- **testing**
  → killers
- **standardisation**
  →zk-boost
- **Geth as Guest**
  → GaG
- **gevm**
  → "go-evm"

EF 🤝 zkEVM

ZKEVM

Kev Wedderburn
@kevaundray

Thomas Coratger
@tcoratger

Cody Gunton

Han Jian
@han__0110

Radek
Signal: @rodiazet.24

Sophia Gold
*@_sophiagold_*

Stateless zkSTF

Stateless.fyi

Guillaume Ballet
@gballet

Ignacio Hagopian
@ignaciohagopian

Wei Han
@ngweihan_eth

Carlos Perez
@CPerezz19

Matan Prasma

Protocol Prototyping

Toni Wahrstatter
@nero_eth

Danno Ferrin
@shemnon

Jochem Brouwer
@jochembrouwer96

Protocol Snarkification

Alexander Hicks
@alexanderlhicks

Carl Beekhuizen
@carlbeek

Cryptography Research

crypto.ethereum.org

George Kadianakis
@asn_d6

Gottfried Herold

Dmitry Khovratovich
@khovr

Mary Maller

Antonio Sanso
@asanso

Benedikt Wagner

Arantxa Zapico
@arantxazapico

- **testing** → killers
- **standardisation** →zk-boost
- **Geth as Guest** → GaG
- **gevm** → "go-evm"

gigagas L1

part 1—vision

part 2—zkEVM integrations

part 3—zkEVM requirements

part 1—vision

part 2—zkEVM integrations

part 3—zkEVM requirements

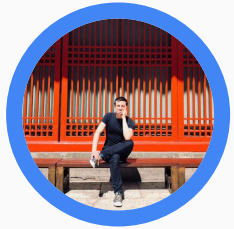
proposed gas limit targets

yesterday

	gas limit (12s slots)	**throughput** (limit/target = 2)
2025	100M	4.16Mgas/s
2026	300M	12.5Mgas/s

proposed gas limit targets

yesterday



EIP-7937

	gas limit (12s slots)	throughput (limit/target = 2)
2025	100M	4.16Mgas/s
2026	300M	12.5Mgas/s
2027	900M	37.5Mgas/s
2028	2.7G	112.5Mgas/s

proposed gas limit targets

yesterday

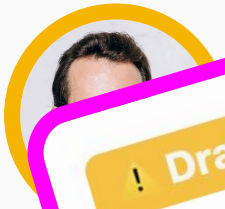
EIP-7937

today

	gas limit (12s slots)	throughput (limit/target = 2)
2025	100M	4.16Mgas/s
2026	300M	12.5Mgas/s
2027	900M	37.5Mgas/s
2028	2.7G	112.5Mgas/s
2029	8.1G	337.5Mgas/s
2030	24.3G	**1Ggas/s**

proposed gas limit targets

yesterday



	gas limit (12s slots)	th
2025		
		12.5M/s
	900M	37.5M/s
2028	2.7G	112.5M/s
2029	8.1G	337.5M/s
2030	24.3G	1G/s

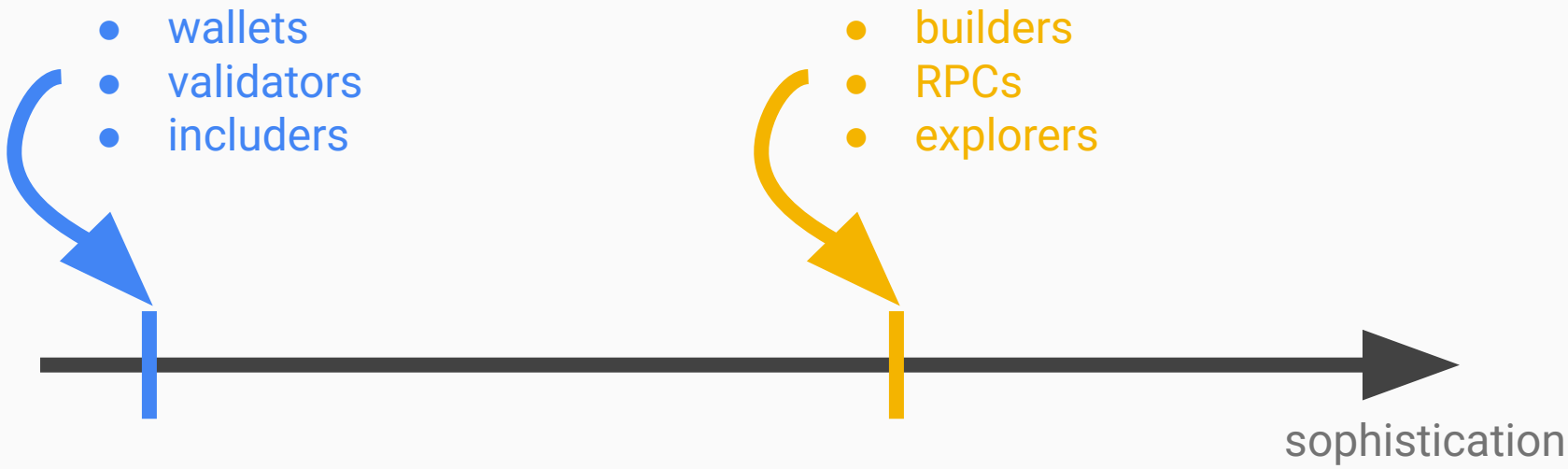
predictable and steady

Draft

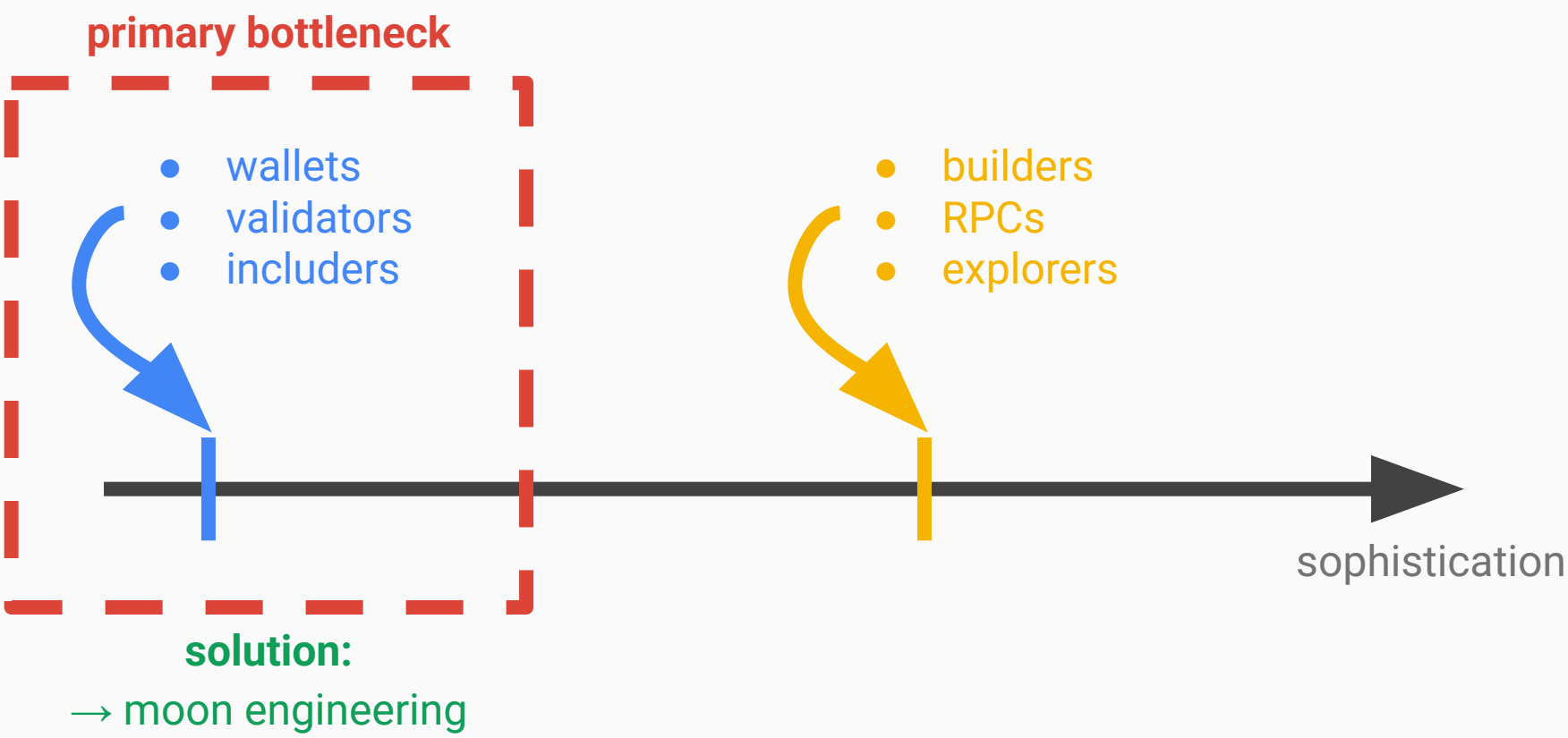
Informational

EIP-7938: Exponential Gas Limit Increase

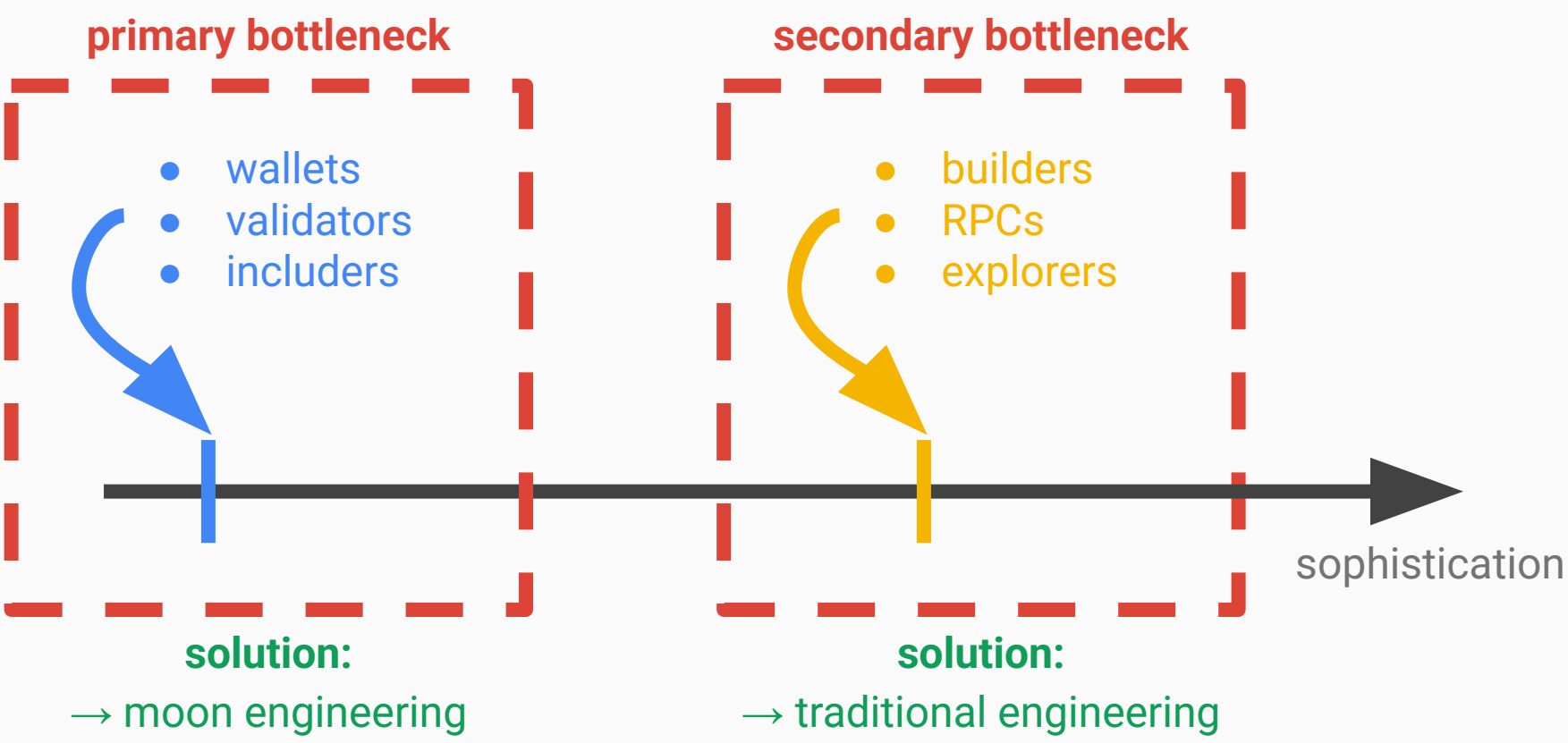
node types


wallets
validators
includers
builders
RPCs
explorers
sophistication

node types


primary bottleneck
wallets
validators
includers
builders
RPCs
explorers
sophistication
solution:
→ moon engineering

node types


primary bottleneck
wallets
validators
includers
secondary bottleneck
builders
RPCs
explorers
sophistication
solution:
→ moon engineering
solution:
→ traditional engineering

real-time proving parity

realtime.succinct.xyz

real-time proving parity

realtime.succinct.xyz

"**16 5090s**"—Jeremy Bruestle

primary bottleneck: solved™

real-time proving parity + exponential zkVM progress =

3x/year
"easy"

what about sequential executor latency?

! Draft | Standards Track: Core

EIP-7825: Transaction Gas Limit Cap

coming soon™

- in Fusaka
- 2025 target

what about sequential executor latency?

! Draft | Standards Track: Core

EIP-7825: Transaction Gas Limit Cap

coming soon™

- in Fusaka
- 2025 target

30M cap

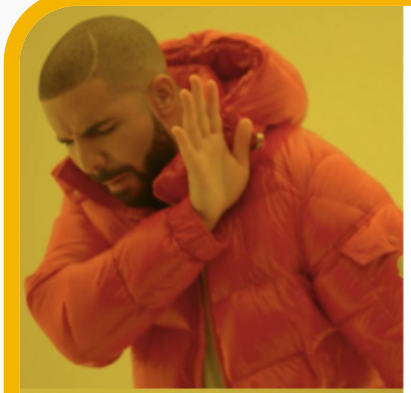
- 60 Mgas blocks: **2x**
- 1 Ggas/sec & 3sec slots: **100x**

secondary bottleneck: just do it™

- Geth
  - LevelDB
    - LSM-tree
- Reth
  - MDBX
    - B-tree

~50 disk ops per traversal

secondary bottleneck: just do it™



O(log²)

O(log)

- Geth
  - LevelDB
    - LSM-tree
- Reth
  - MDBX
    - B-tree

~50 disk ops per traversal

triedb Private

github.com/**base/triedb**

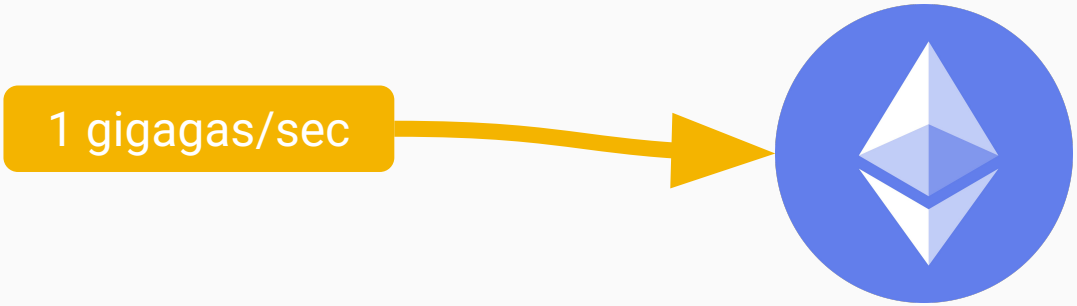
4-8 disk ops per traversal

perfnets

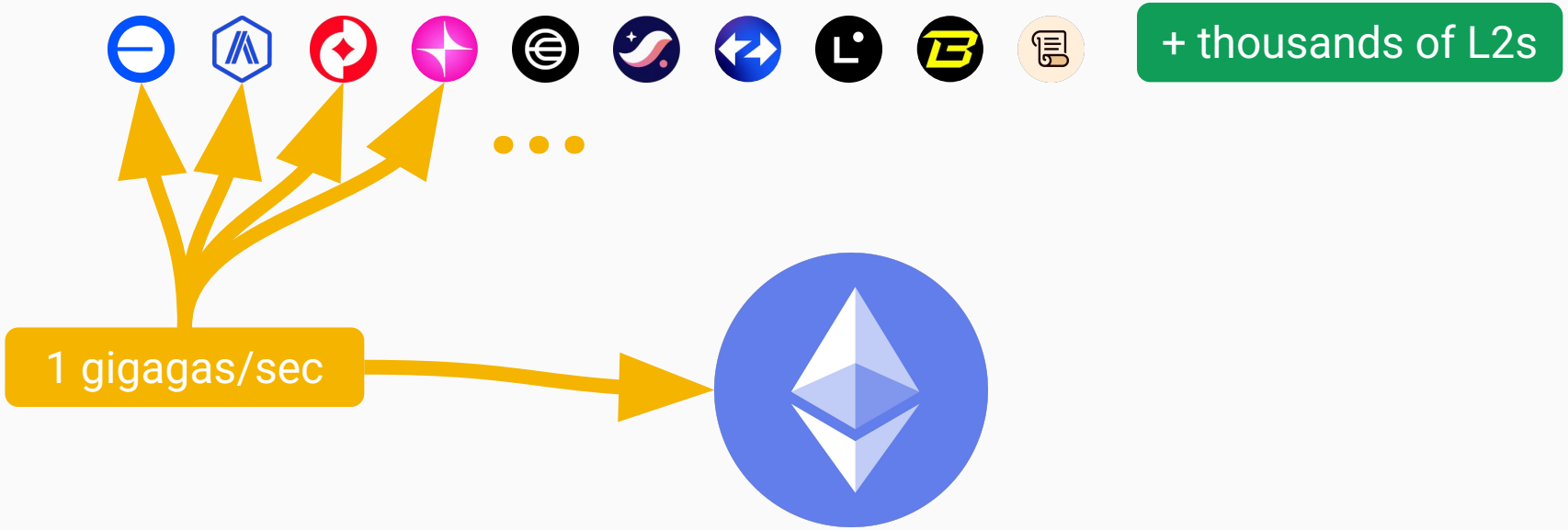
```
Received New Block:  35396 (0xdf84c9...a8d537)      | limit 4,000,000,000
Processed                35396          |      301.6 ms  | slot          22,
 Block    3.7383 ETH  1869.13 MGas      |   11,761   txs | calls          0
 Block throughput     6197.10 MGas/s🔥|   38,993.5 tps |              3.32
Received ForkChoice: 35396 (0xdf84c9...a8d537), Safe: 35372 (0xa09b6d...c
Synced Chain Head to 35396 (0xdf84c9...a8d537)
```

nethermind-ui.**benaadams**.vip

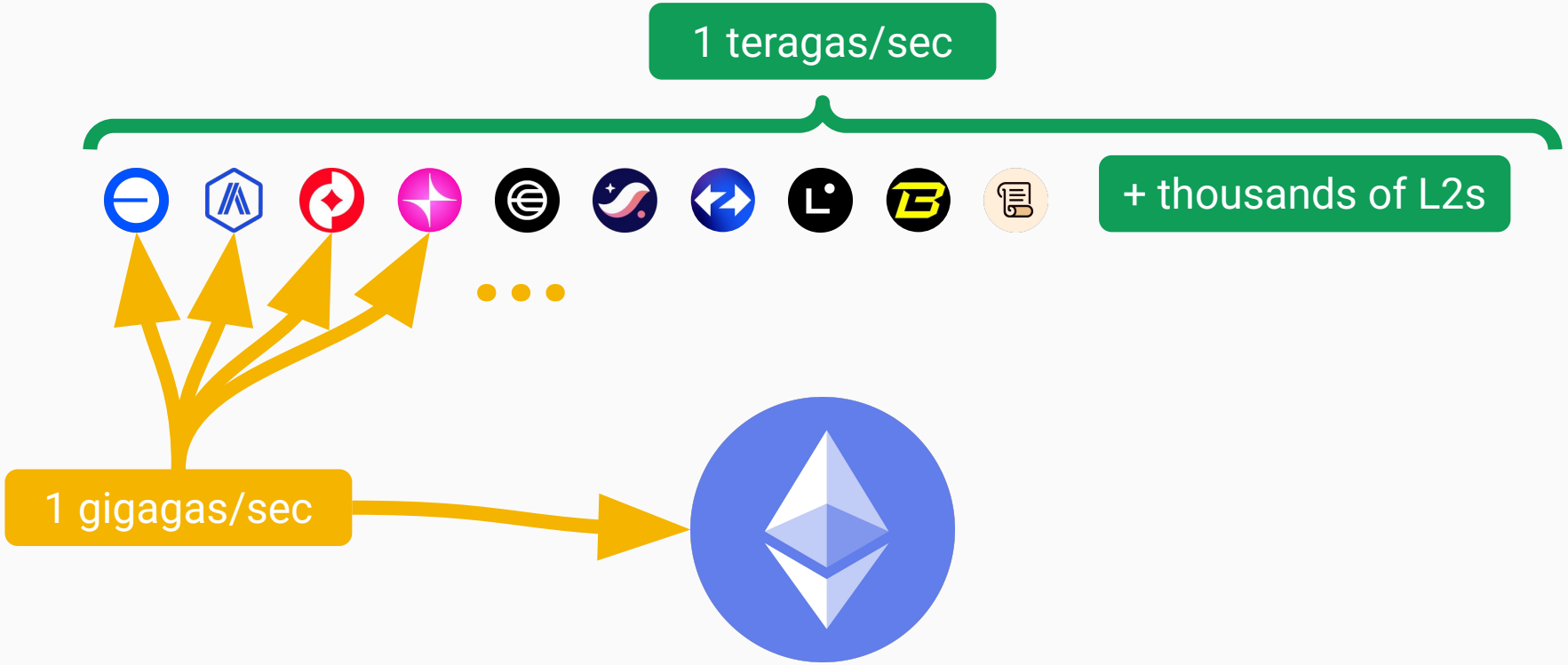
refreshed rollup-centric roadmap



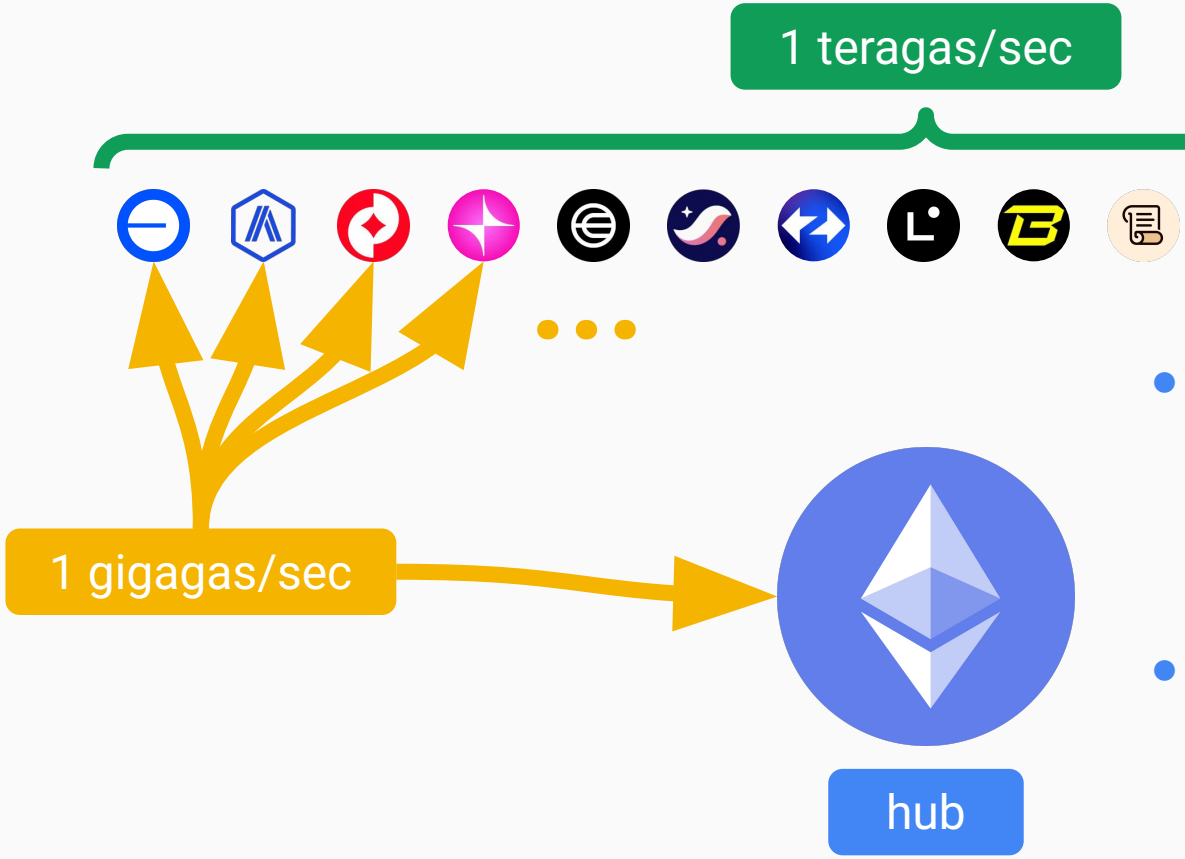
refreshed rollup-centric roadmap



refreshed rollup-centric roadmap



refreshed rollup-centric roadmap



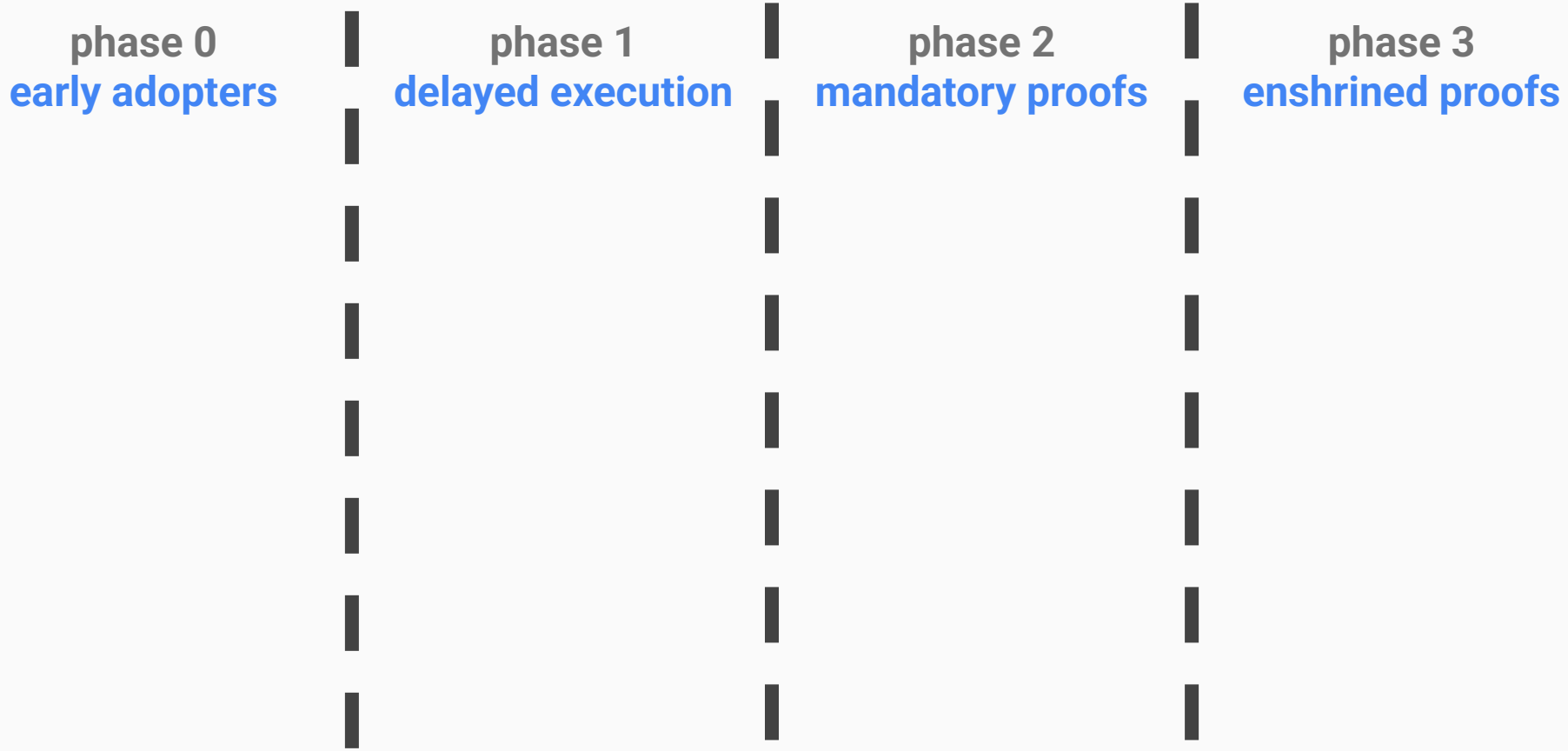
- **shared assets**
  - shared minting
  - shared deposits
  - shared bridging
- **shared settlement**
  - shared proofs
  - shared blobs
  - shared compression

part 1—vision

part 2—zkEVM integrations

part 3—zkEVM requirements

gradual enshrinement



gradual enshrinement

phase 0
early adopters

- 2025 (Q3)
  - no fork needed
- hybrid attesters
  - 1% opted in?
- altruistic provers
  - Ethproofs, grants
- delayed attesting
  - smaller rewards
- alternative hack
  - optimistic attesting

phase 1
delayed execution

phase 2
mandatory proofs

phase 3
enshrined proofs

gradual enshrinement

phase 0
early adopters

- 2025 (Q3)
  - no fork needed
- hybrid attesters
  - 1% opted in?
- altruistic provers
  - Ethproofs, grants
- delayed attesting
  - smaller rewards
- alternative hack
  - optimistic attesting

phase 1
delayed execution

- 2026 (Glamsterdam?)
  - delayed execution
- hybrid attesters
  - 10% opted in?
- altruistic provers
  - Ethproofs, grants
- much less hacky
  - aligned and safe
    - except killers

phase 2
mandatory proofs

phase 3
enshrined proofs

gradual enshrinement

phase 0
early adopters

- 2025 (Q3)
  - no fork needed
- hybrid attesters
  - 1% opted in?
- altruistic provers
  - Ethproofs, grants
- delayed attesting
  - smaller rewards
- alternative hack
  - optimistic attesting

phase 1
delayed execution

- 2026 (Glamsterdam?)
  - delayed execution
- hybrid attesters
  - 10% opted in?
- altruistic provers
  - Ethproofs, grants
- much less hacky
  - aligned and safe
    - except killers

phase 2
mandatory proofs

- 2027
  - proof timeliness
- semi-enshrined
  - 100% adoption
  - fork choice
- rational builders
  - fee incentives
  - collateral
- incentive aligned & safe

phase 3
enshrined proofs

gradual enshrinement

phase 0
early adopters

- 2025 (Q3)
  - no fork needed
- hybrid attesters
  - 1% opted in?
- altruistic provers
  - Ethproofs, grants
- delayed attesting
  - smaller rewards
- alternative hack
  - optimistic attesting

phase 1
delayed execution

- 2026 (Glamsterdam?)
  - delayed execution
- hybrid attesters
  - 10% opted in?
- altruistic provers
  - Ethproofs, grants
- much less hacky
  - aligned and safe
    - except killers

phase 2
mandatory proofs

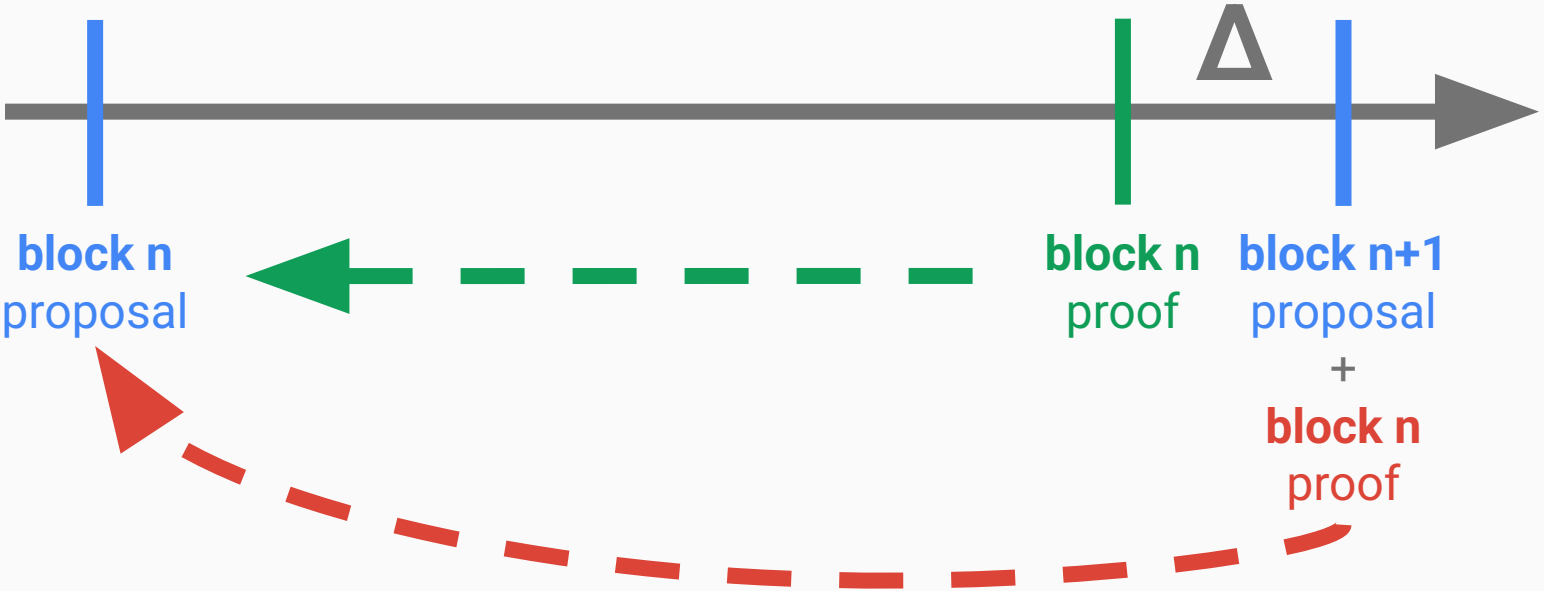
- 2027
  - proof timeliness
- semi-enshrined
  - 100% adoption
  - fork choice
- rational builders
  - fee incentives
  - collateral
- incentive aligned & safe

phase 3
enshrined proofs

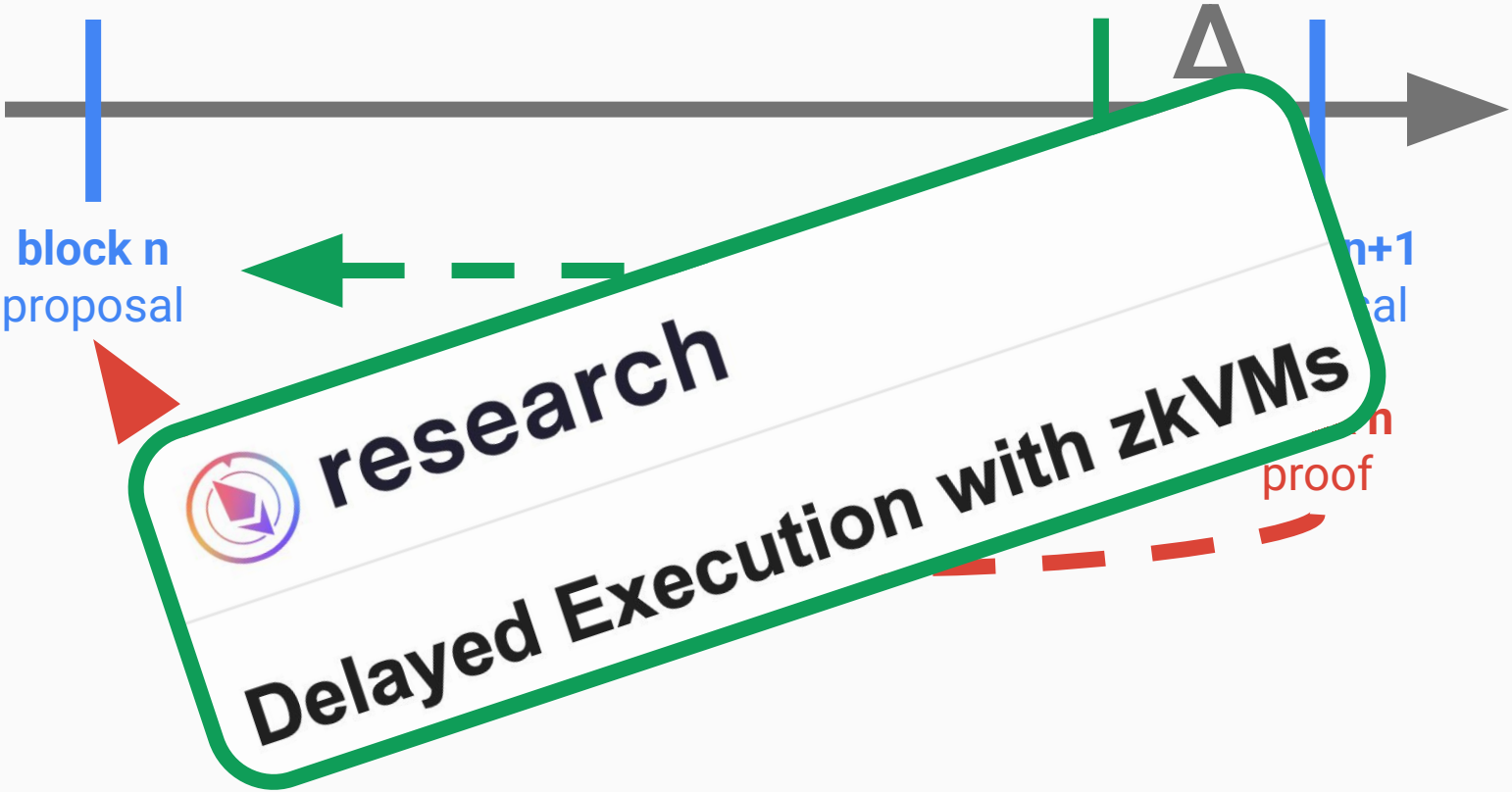
- 2028
  - formal verification
- fully enshrined
  - onchain proofs
  - deterministic
- rational builders
  - fee incentives
  - collateral
- incentive aligned & safe
- new powers
  - native validiums
- long-term cleaner

mandatory proofs

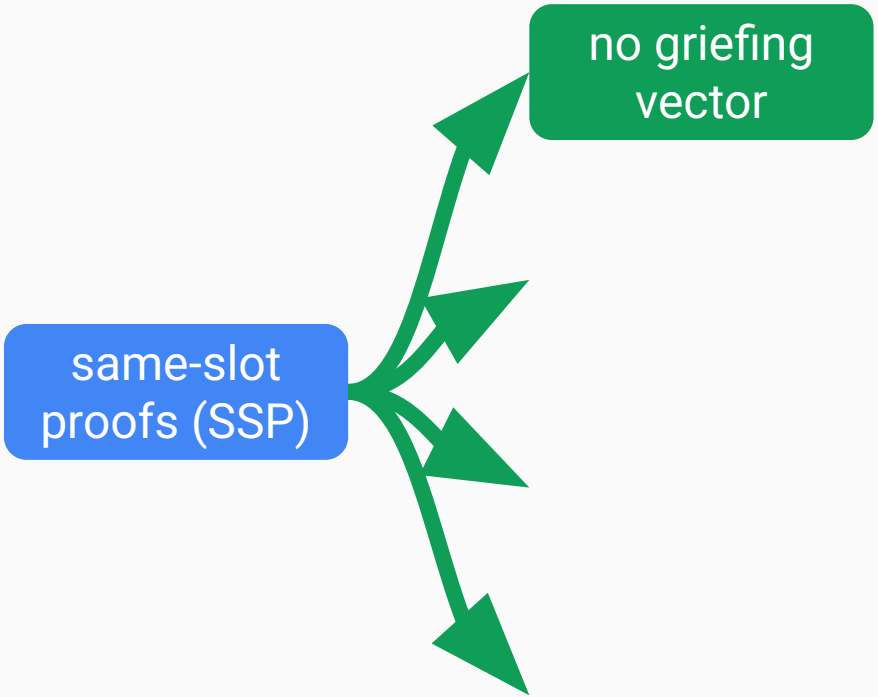
same-slot proofs (SSP)



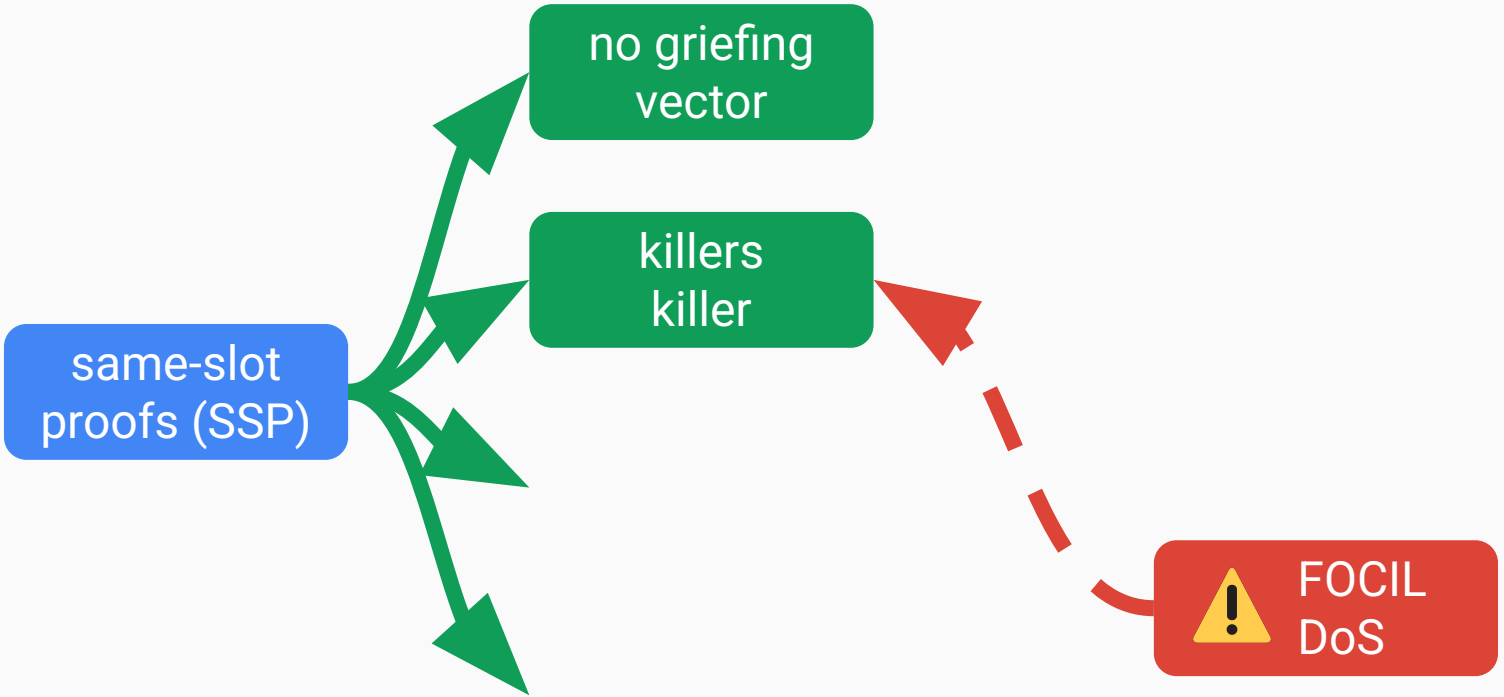
same-slot proofs (SSP)



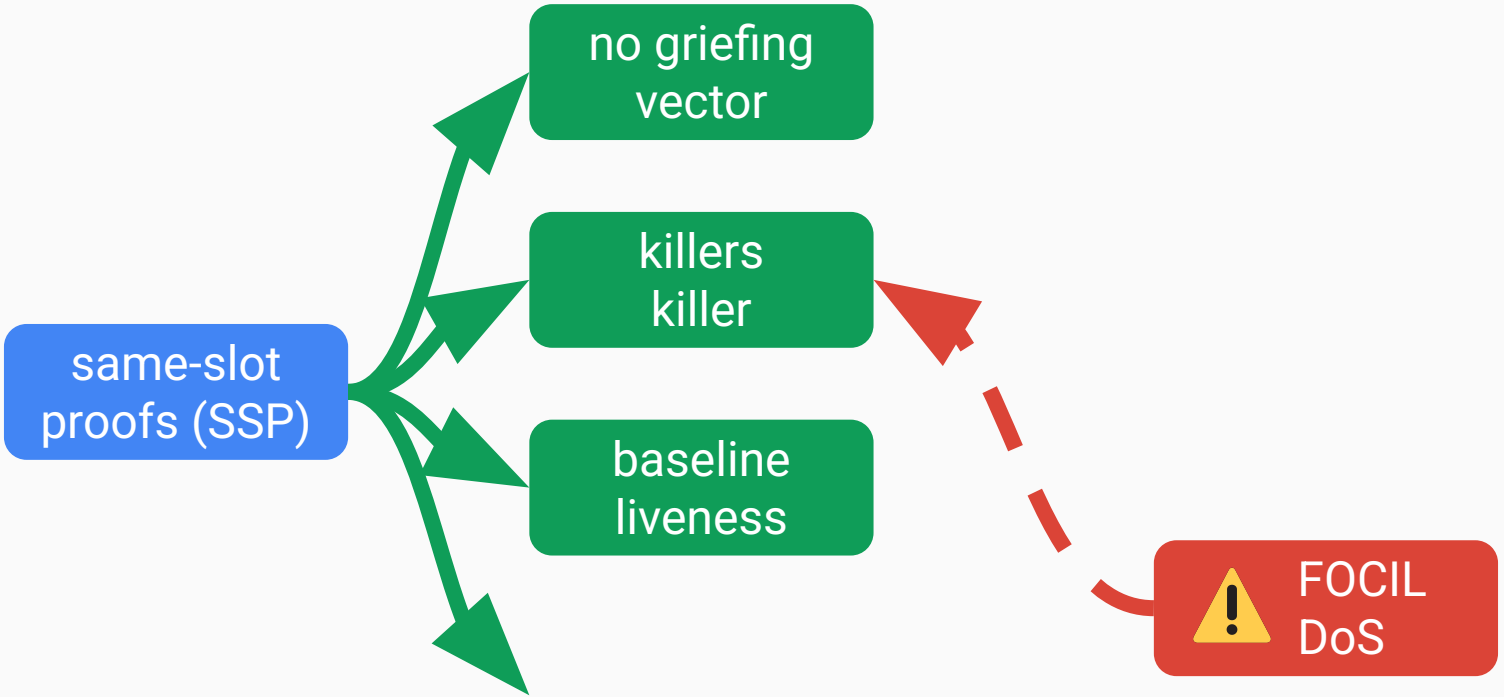
SSP advantages



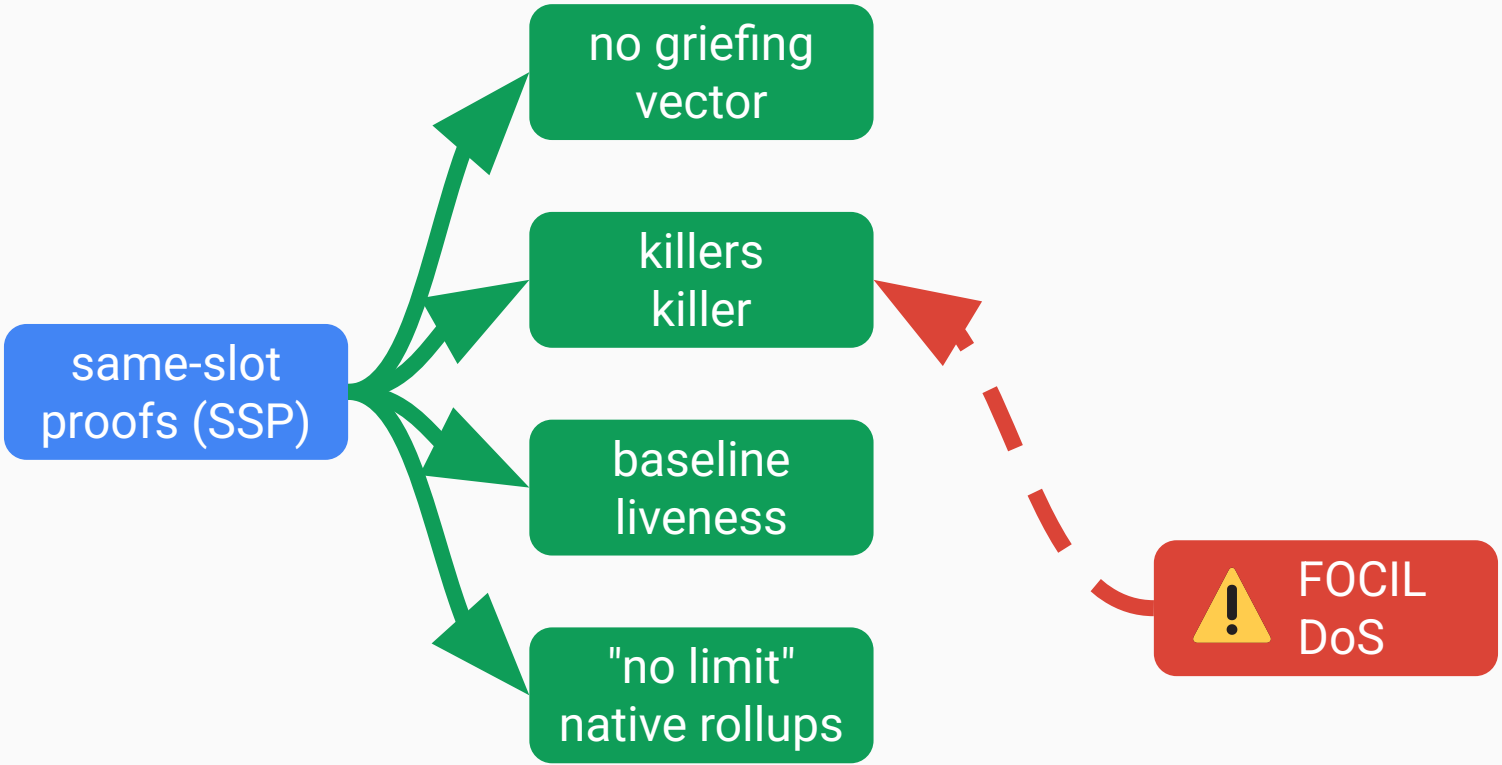
SSP advantages



SSP advantages



SSP advantages

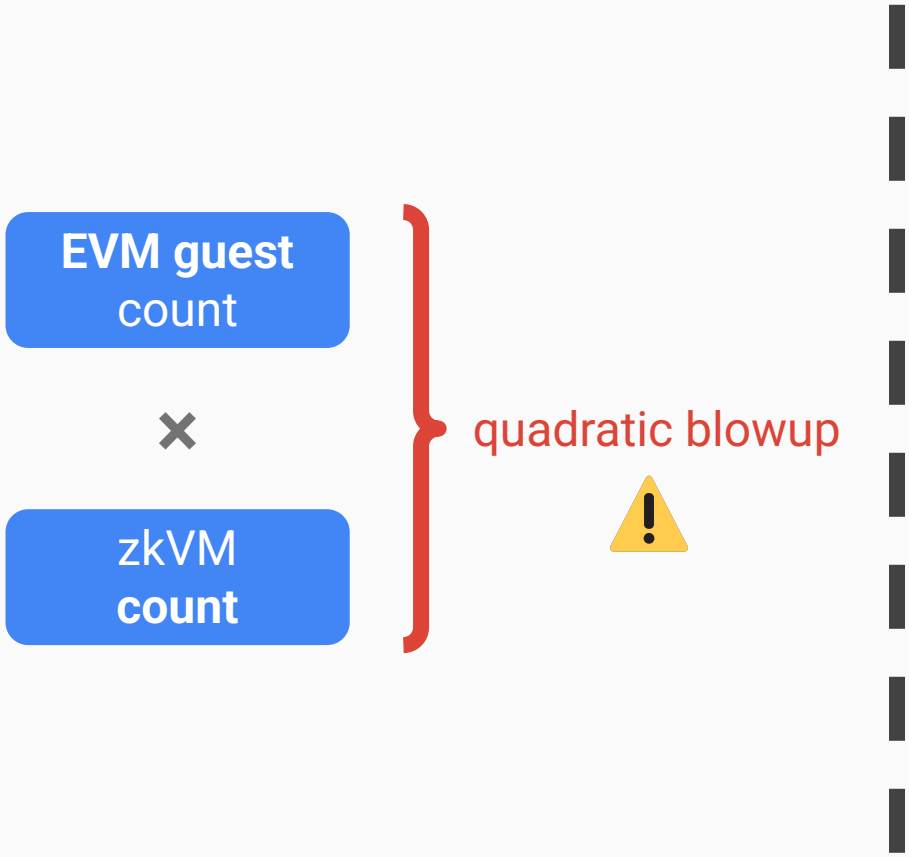


k-of-**n** proof checking

k-of-n proof checking

"low-resource Vouch"

zkEL diversity



zkEL diversity

EVM guest count

×

zkVM **count**

quadratic blowup

idea 1
slow-fast pairs

idea 2
multi-EVM proofs

part 1—vision

part 2—zkEVM integrations

part 3—zkEVM requirements

cluster proving specs (for 1-of-n assumption)

$100K

11.5kW

cluster proving specs (for 1-of-n assumption)

$100K

bottleneck

11.5kW

milestone—office proving

ZkCloud,
XXX office

RISC Zero,
Seattle office

EF,
Berlin office

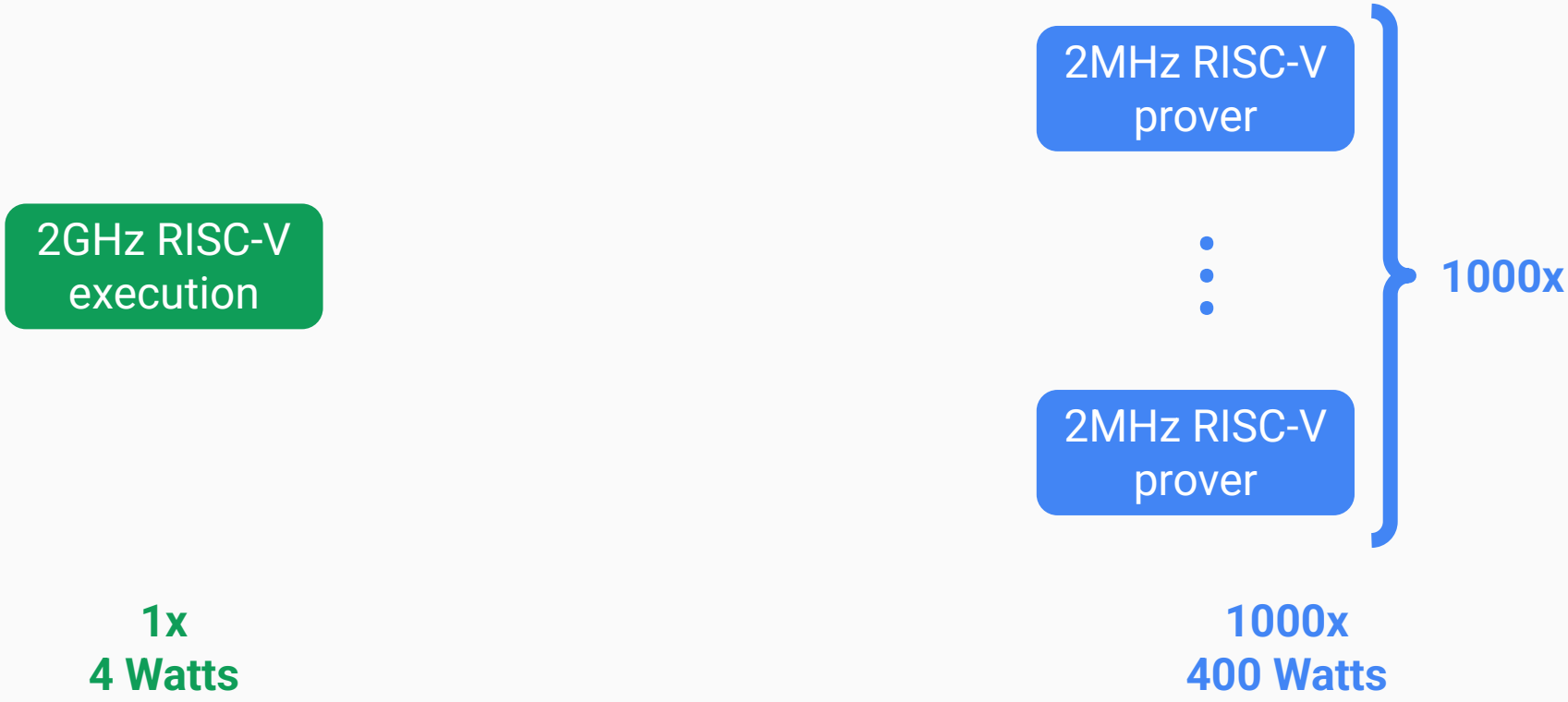
milestone—office proving

ZkCloud,
XXX office

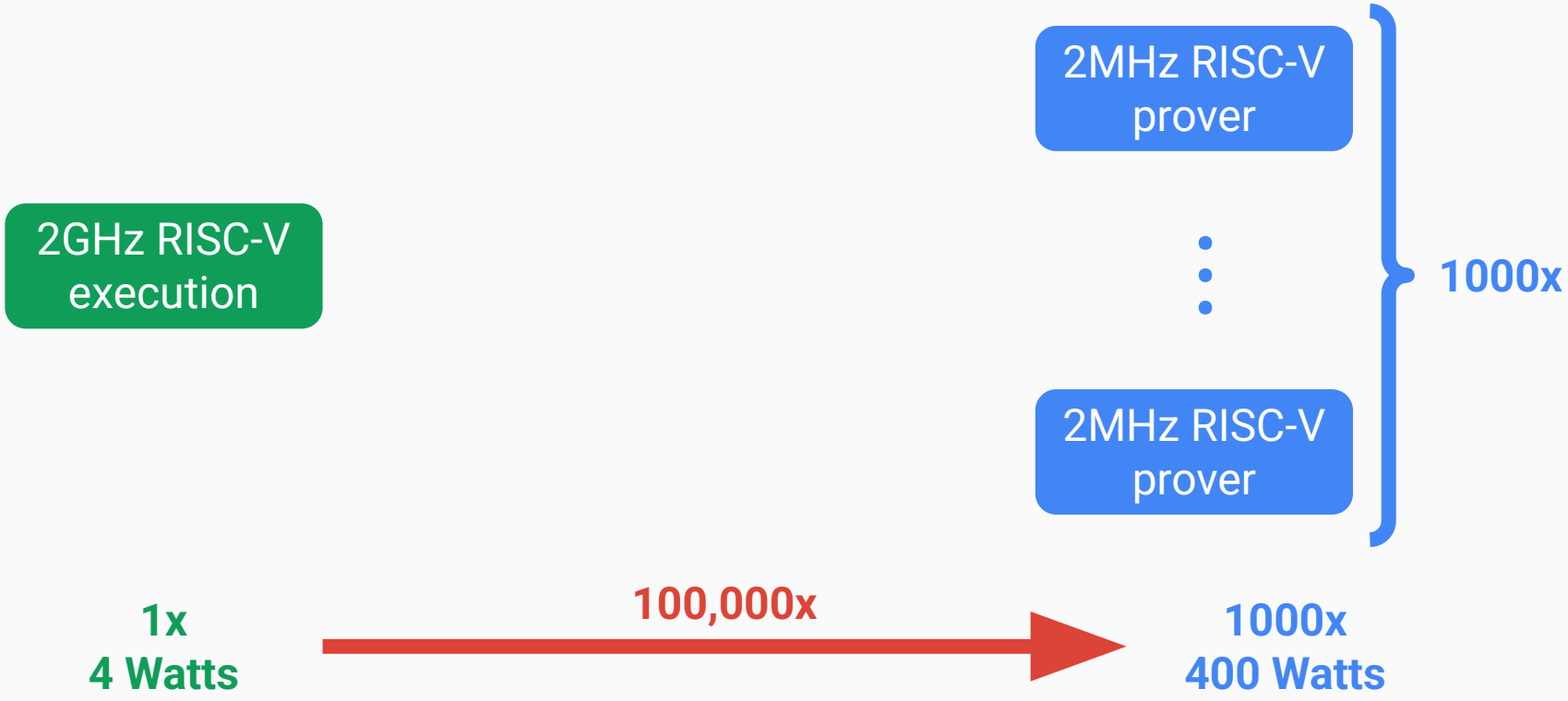
RISC Zero,
Seattle office

EF,
Berlin office

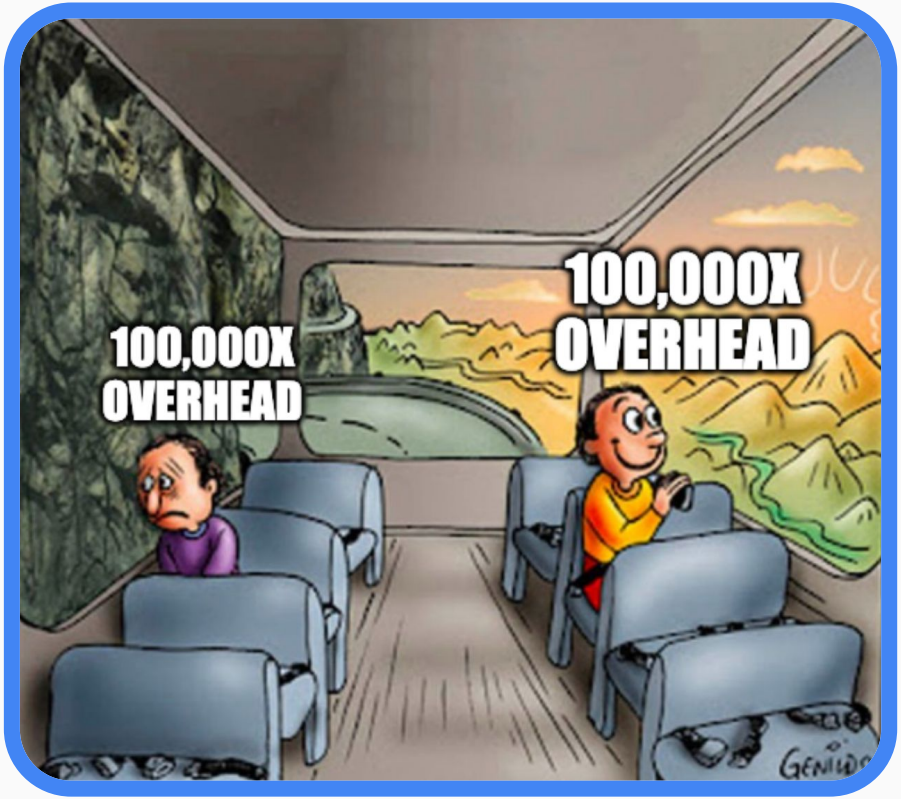
power overhead



power overhead

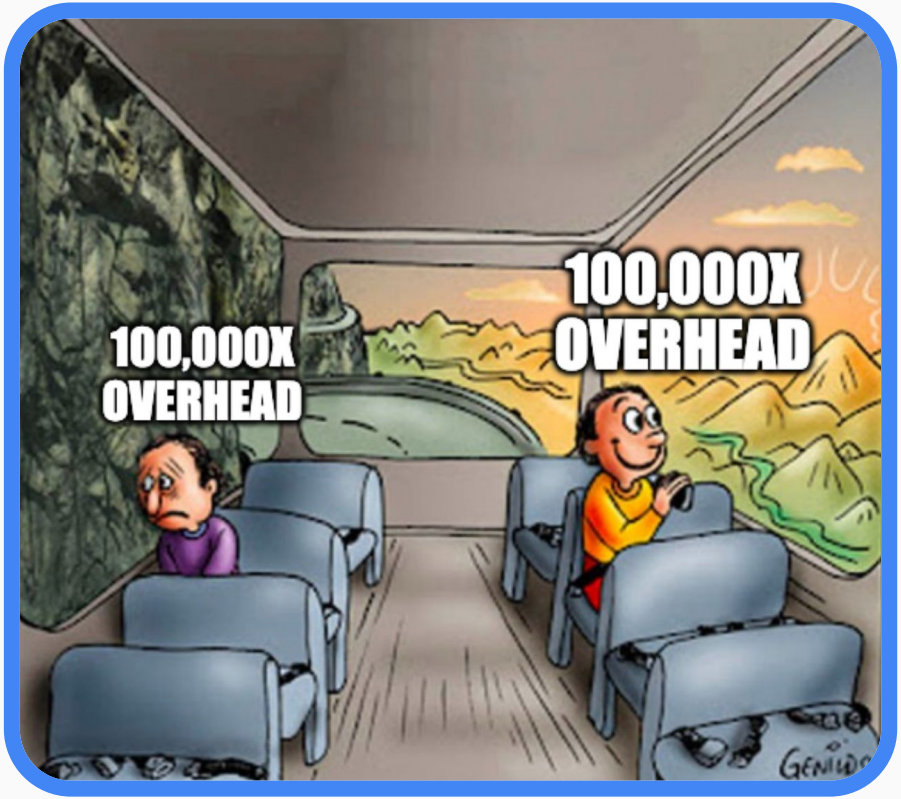


power opportunities



≥10x
software

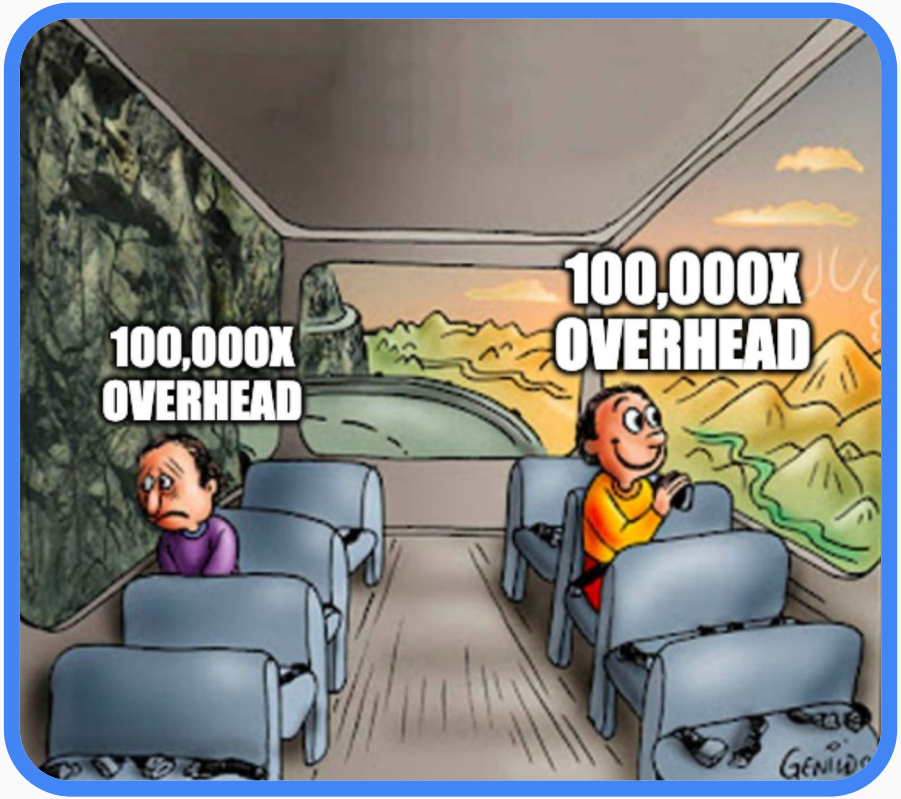
power opportunities



≥10x
software

≥10x
hardware

power opportunities



≥10x
software

≥10x
hardware

≥10x
load balancing

power heuristic

1 4090 for 16 slots

perfect parallelism

16 4090s for 1 slot

power heuristic

1 4090 for 16 slots

perfect parallelism

16 4090s for 1 slot

8 5090s for 1 slot

power heuristic

1 4090 for 16 slots

perfect parallelism

16 4090s for 1 slot

8 5090s for 1 slot

home cluster

cluster proving open-source

bento

gpu_prover

proofman

cluster proving open-source

bento

gpu_prover

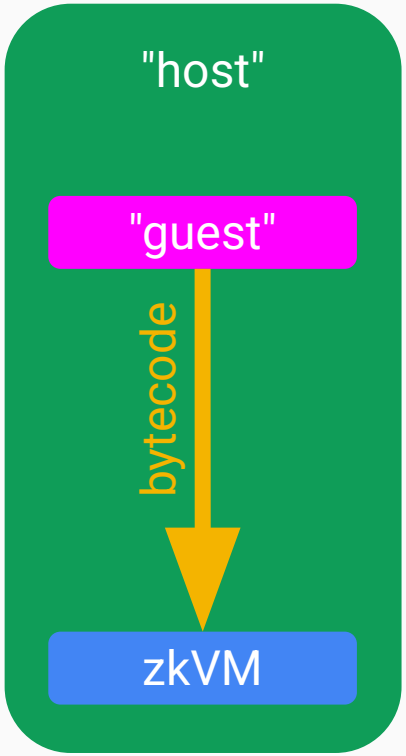
proofman

tracker column
soon™

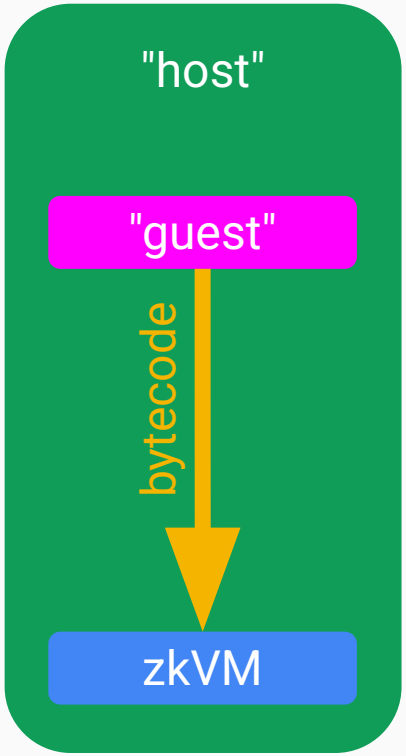
verifier open sourcing

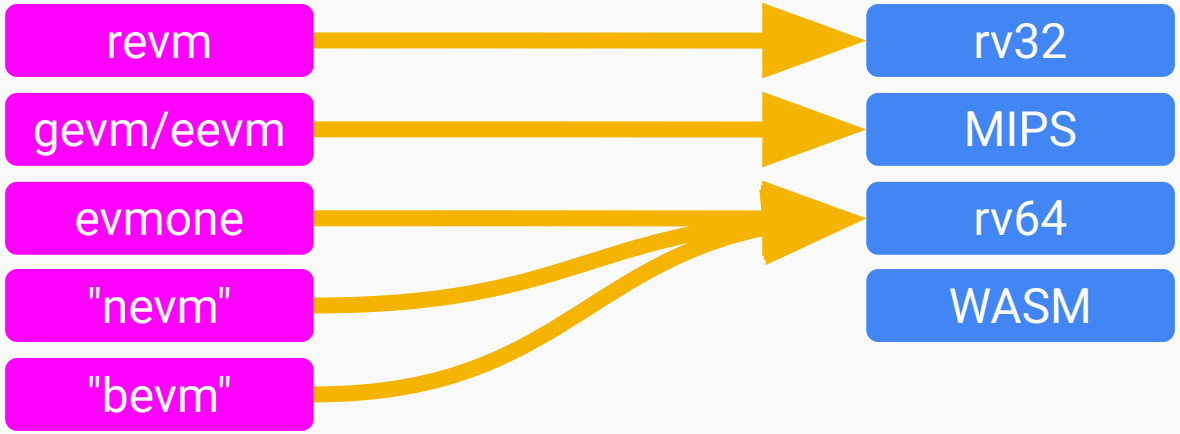
zkvm	ISA	team	open source
Airbender	RISC-V	MatterLabs	✓✓ dual
Ceno	RISC-V	Scroll	✓✓ dual
Euclid (OpenVM)	RISC-V	Scroll	✓✓ dual
Ix	Lean 4	Argument	✓✓ dual
Jolt	RISC-V	a16z	✓✓ dual
Keth (Cairo)	Cairo ISA	Kakarot	✓✓ dual
Linea EVM	EVM	Linea	✓✓ dual
Miden VM	Miden ISA	Miden	✓ MIT
Nexus zkVM 3.0	RISC-V	Nexus	BUSL 1.1
Nock VM	Nock ISA	Zorp	✓ MIT
o1VM	RISC-V	O(1) Labs	✓ Apache 2.0
OpenVM	RISC-V	Axiom	✓✓ dual
Petra	Petra ISA	Irreducible	✓ Apache 2.0
Pico	RISC-V	Brevis	✓✓ dual
powdrVM	RISC-V	powdr	✓✓ dual
R0VM	RISC-V	RISC Zero	✓ Apache 2.0
SP1	RISC-V	Succinct	✓✓ dual
SP1 Hypercube	RISC-V	Succinct	unlicensed
zkEngine	WASM	ICME	✓✓ dual
ZisK	RISC-V	Polygon	✓✓ dual
zkMIPS	MIPS	ZKM	✓✓ dual
zkWASM	WASM	Delphinus	✓✓ dual

guest diversity

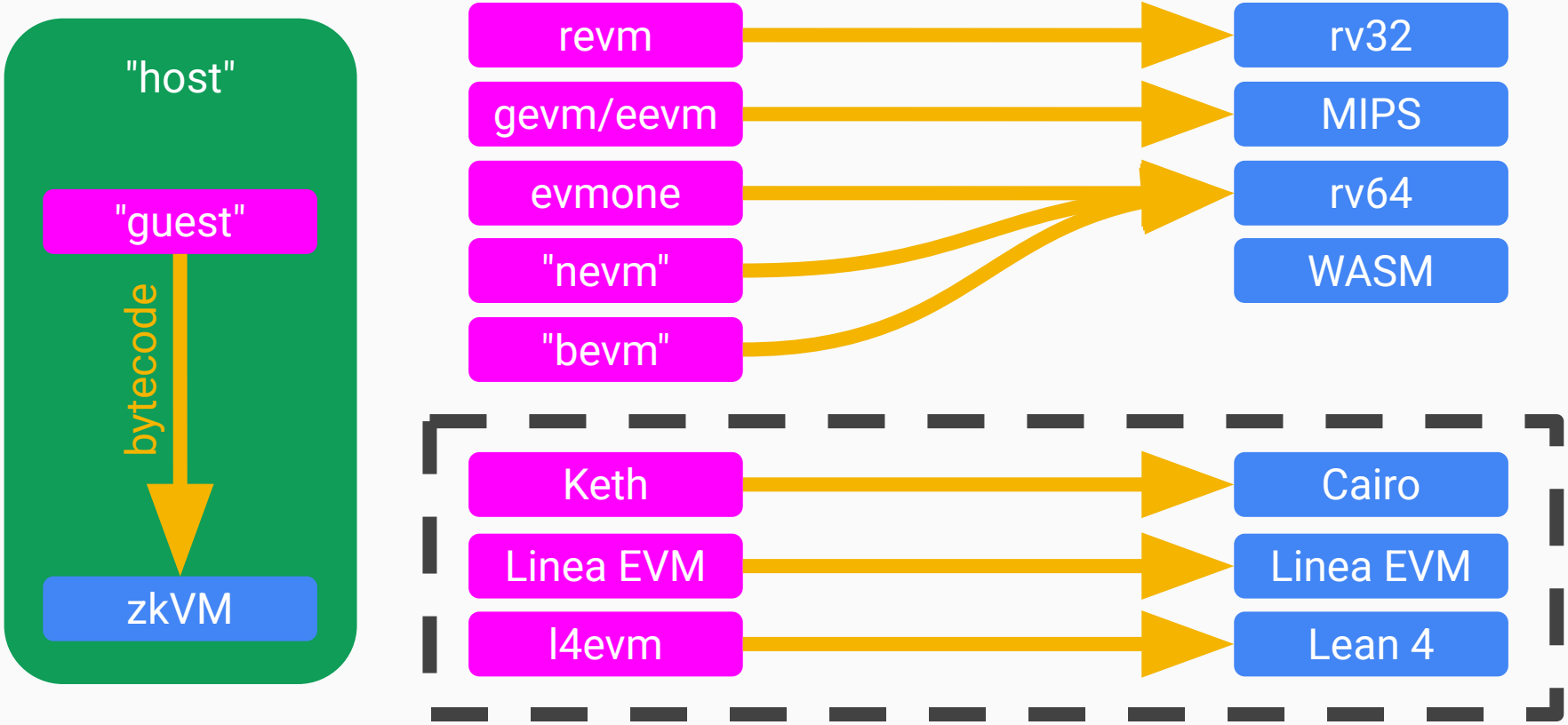


guest diversity





guest diversity



proof wrapping

	no wrapping	wrapping
unoptimised	size 1.5MB latency 0sec setup none complexity low	
optimised		

proof wrapping

	no wrapping	wrapping
unoptimised	size 1.5MB latency 0sec setup none complexity low	size 1kB latency 2sec setup trusted complexity higher
optimised		

proof wrapping

	no wrapping	wrapping
unoptimised	size 1.5MB latency 0sec setup none complexity low	size 1kB latency 2sec setup trusted complexity higher
optimised	size 256kB latency 0sec setup none complexity low	

proof wrapping

	no wrapping	wrapping
unoptimised	size 1.5MB latency 0sec setup none complexity low	size 1kB latency 2sec setup trusted complexity higher
optimised	size 256kB latency 0sec setup none complexity low	size 1kB latency 1sec setup none complexity higher

proof wrapping

crazy idea?
64-bit ephemeral proofs

	no wrapping	wrapping
unoptimised	size 1.5MB latency 0sec setup none complexity low	size 1kB latency 2sec setup trusted complexity higher
optimised	size 256kB latency 0sec setup none complexity low	size 1kB latency 1sec setup none complexity higher

thank you :)

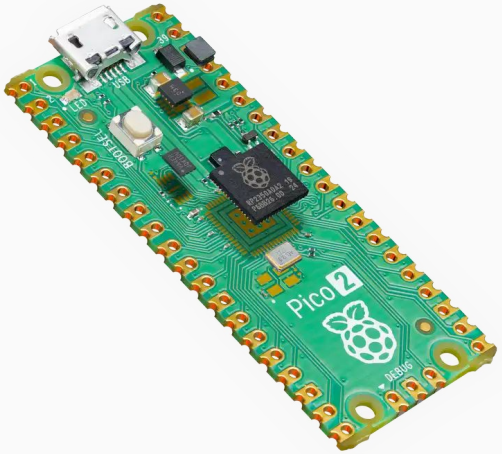
extra slides

personal goals

zkEL · stateless

no NVMe

zkEL · embedded

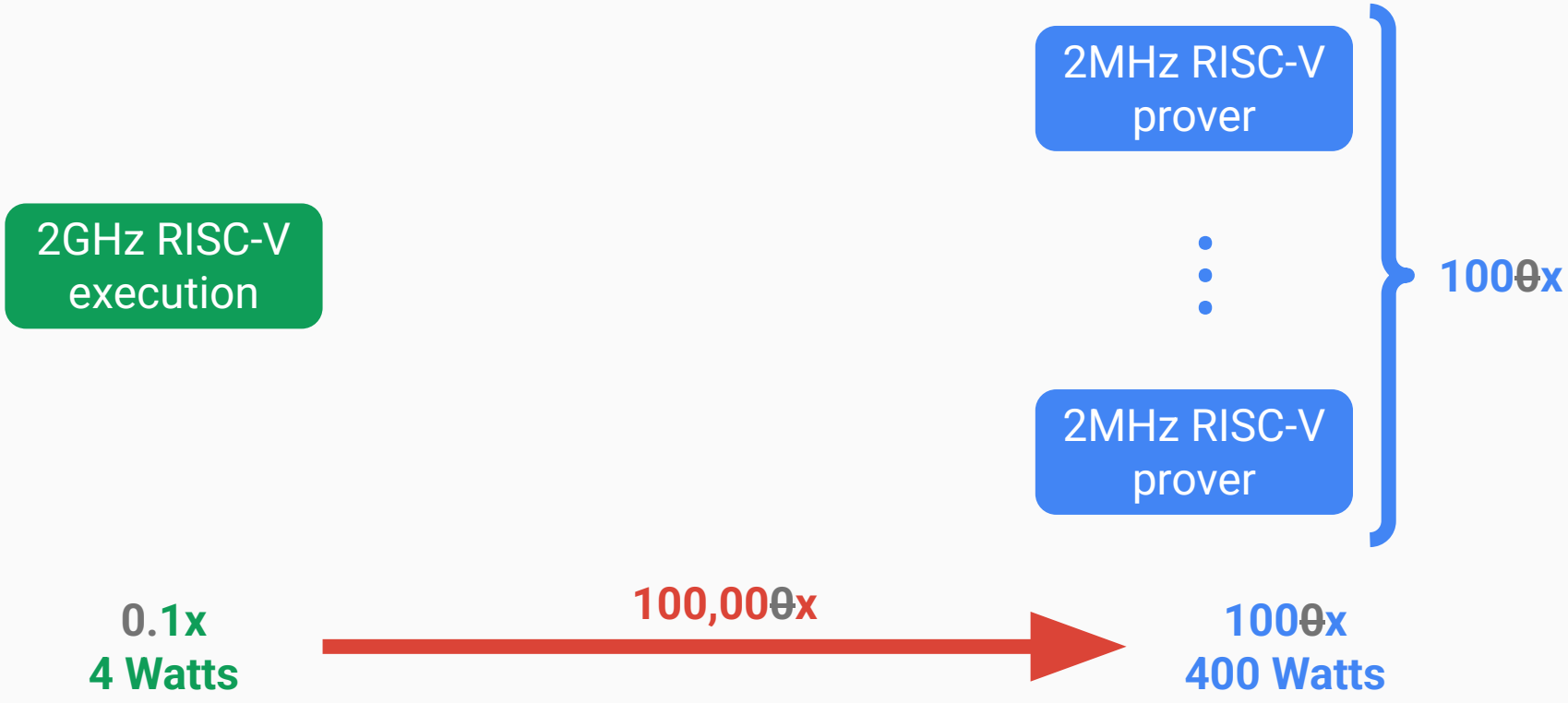


Pi Pico

zkEL · proven

20x 5090s

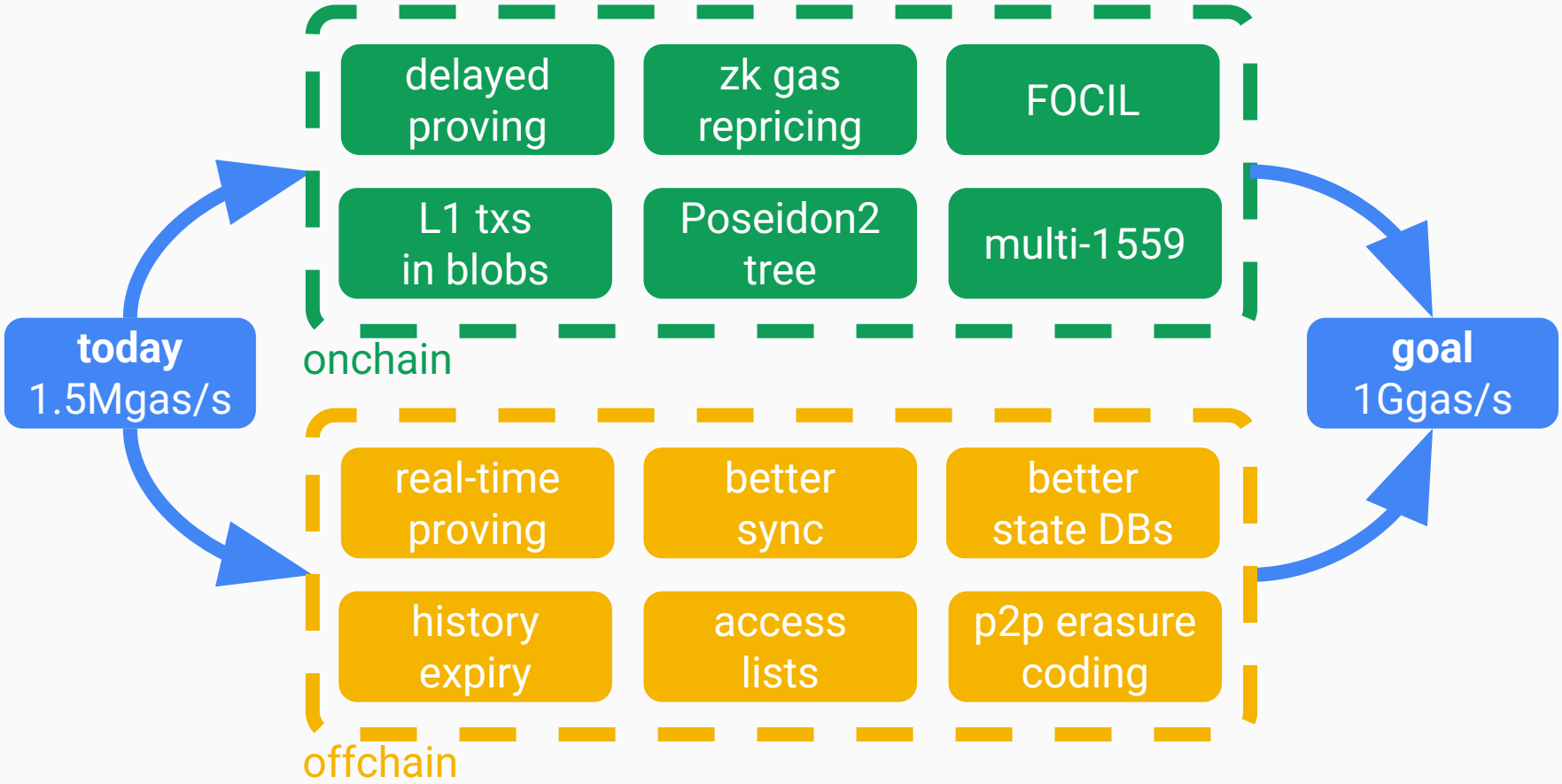
power overhead



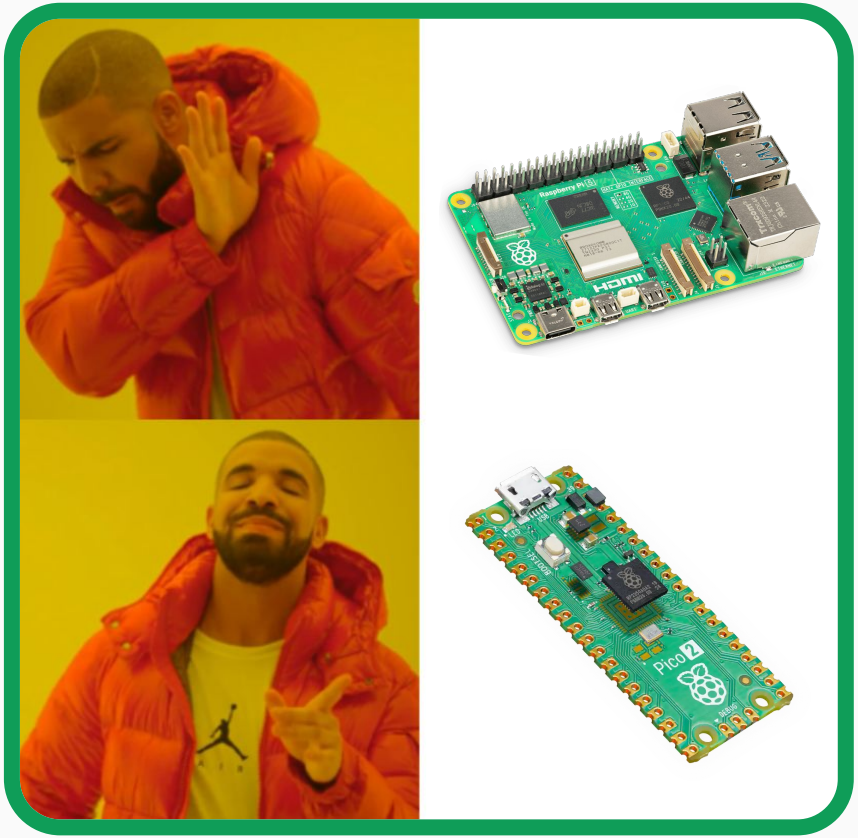
united chains of Ethereum

L1	L2
1 gigagas/sec	1 teragas/sec
10K TPS	10M TPS
0.1% traffic	99.9% traffic

gigagas Ethereum



extreme decentralisation



Raspberry Pi Pico 2 W

- **cost**—$7
- **connectivity**—WiFi
- **CPU**—dual Hazard3 RISC-V
- **memory**—520 KB onchip SRAM
- **power**—1W ($1/year electricity)

slot duration

- wrapping O(1)
- gossiping O(log n)
- aggregating O(log n)