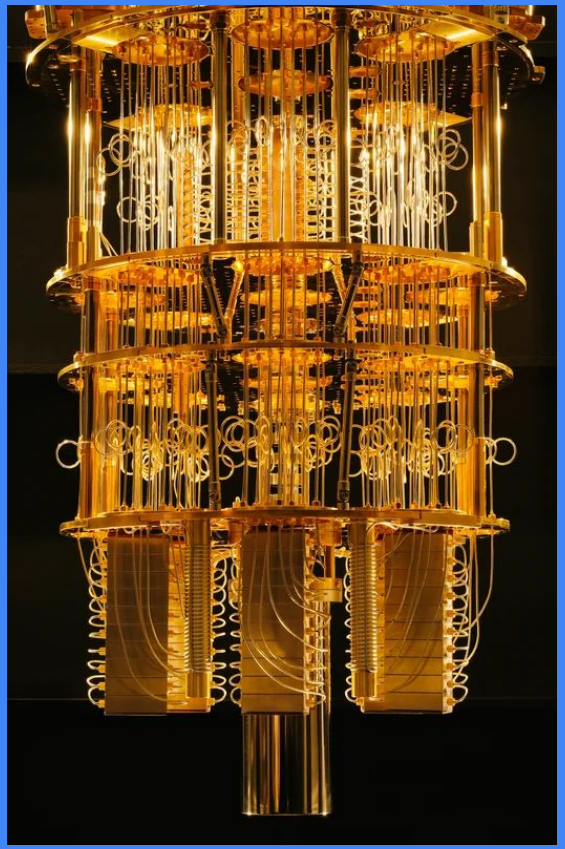
Eth3.0

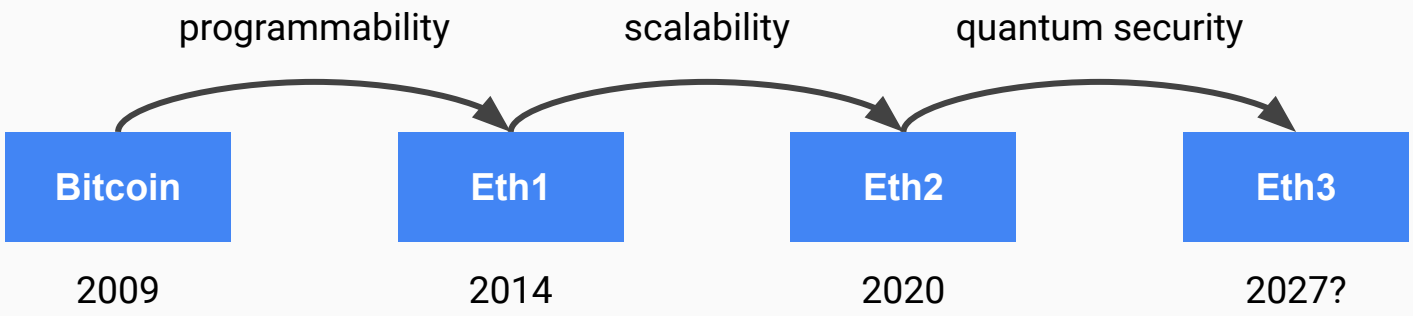
Quantum security



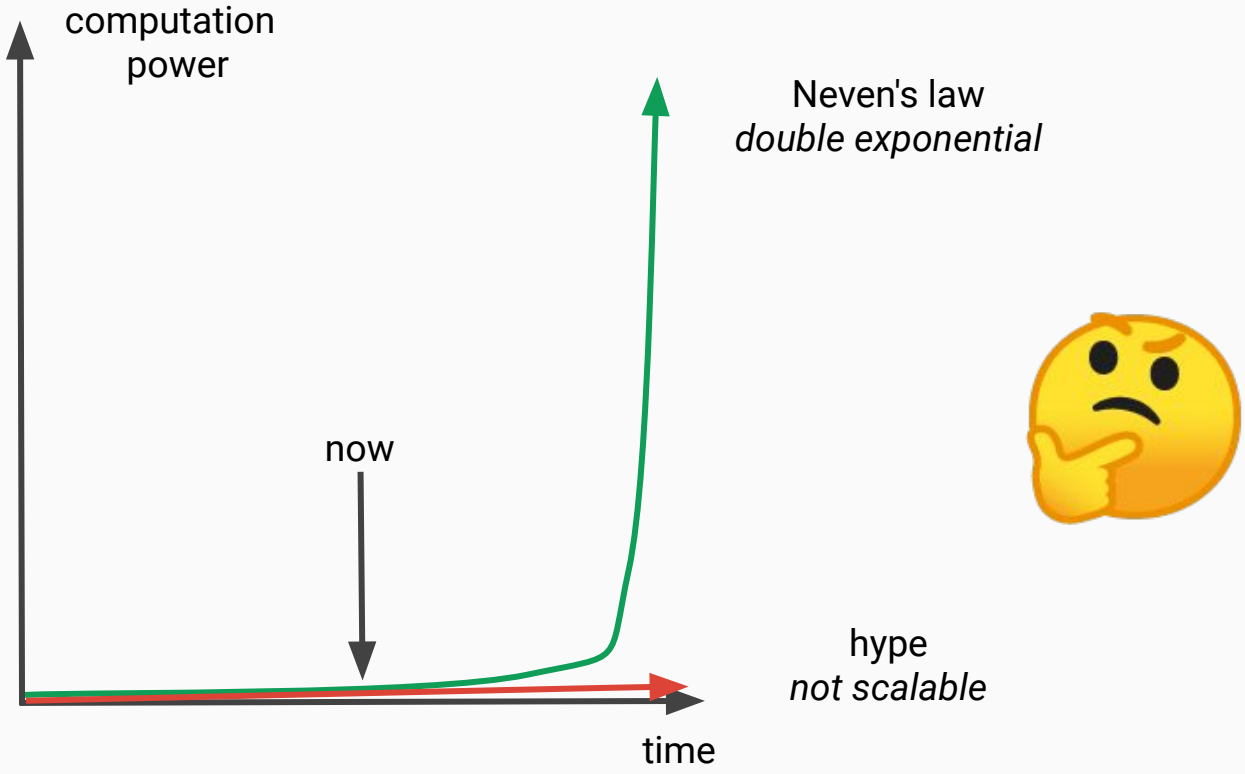
IBM Q
50 qubits

- intro
- Eth1—quantum vulnerability
- Eth2—quantum infancy
- Eth3—quantum security

paradigm shifts



Neven's law vs hype



post quantum narrative

> What's your vision for Eth 3.0?

"**STARKs, STARKs and lots of STARKs.**"—Vitalik, Jan 2019

post quantum narrative

> What's your vision for Eth 3.0?

"**STARKs, STARKs and lots of STARKs.**"—Vitalik, Jan 2019

- **flexibility**
  - one tool to rule them all

post quantum narrative

> What's your vision for Eth 3.0?

"**STARKs, STARKs and lots of STARKs.**"—Vitalik, Jan 2019

- **flexibility**
  - one tool to rule them all
- **lean and resilient crypto**
  - consolidation of assumptions
  - hash functions only
  - Lindy effect

post quantum narrative

> What's your vision for Eth 3.0?

"**STARKs, STARKs and lots of STARKs.**"—Vitalik, Jan 2019

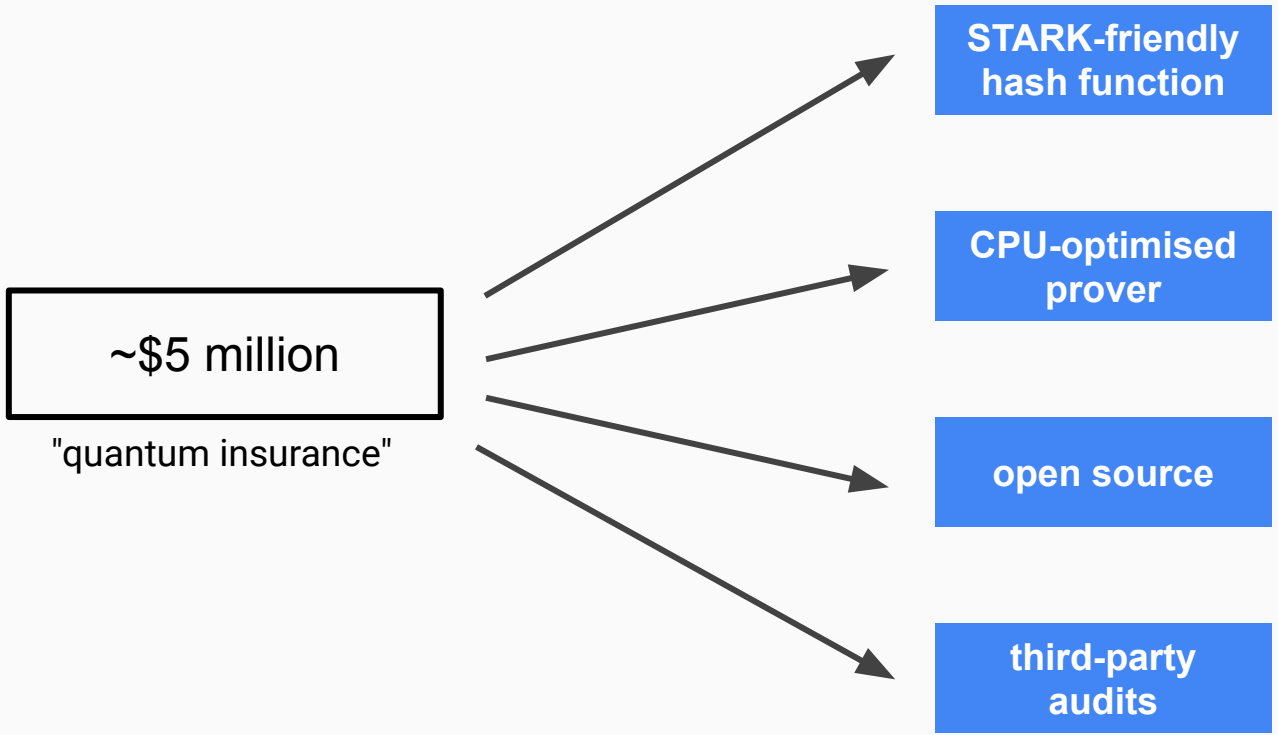
- **flexibility**
  - one tool to rule them all
- **lean and resilient crypto**
  - consolidation of assumptions
  - hash functions only
  - Lindy effect
- **performance**
  - relatively fast prover
  - data is cheap™

Ethereum Foundation grant (July 2018)

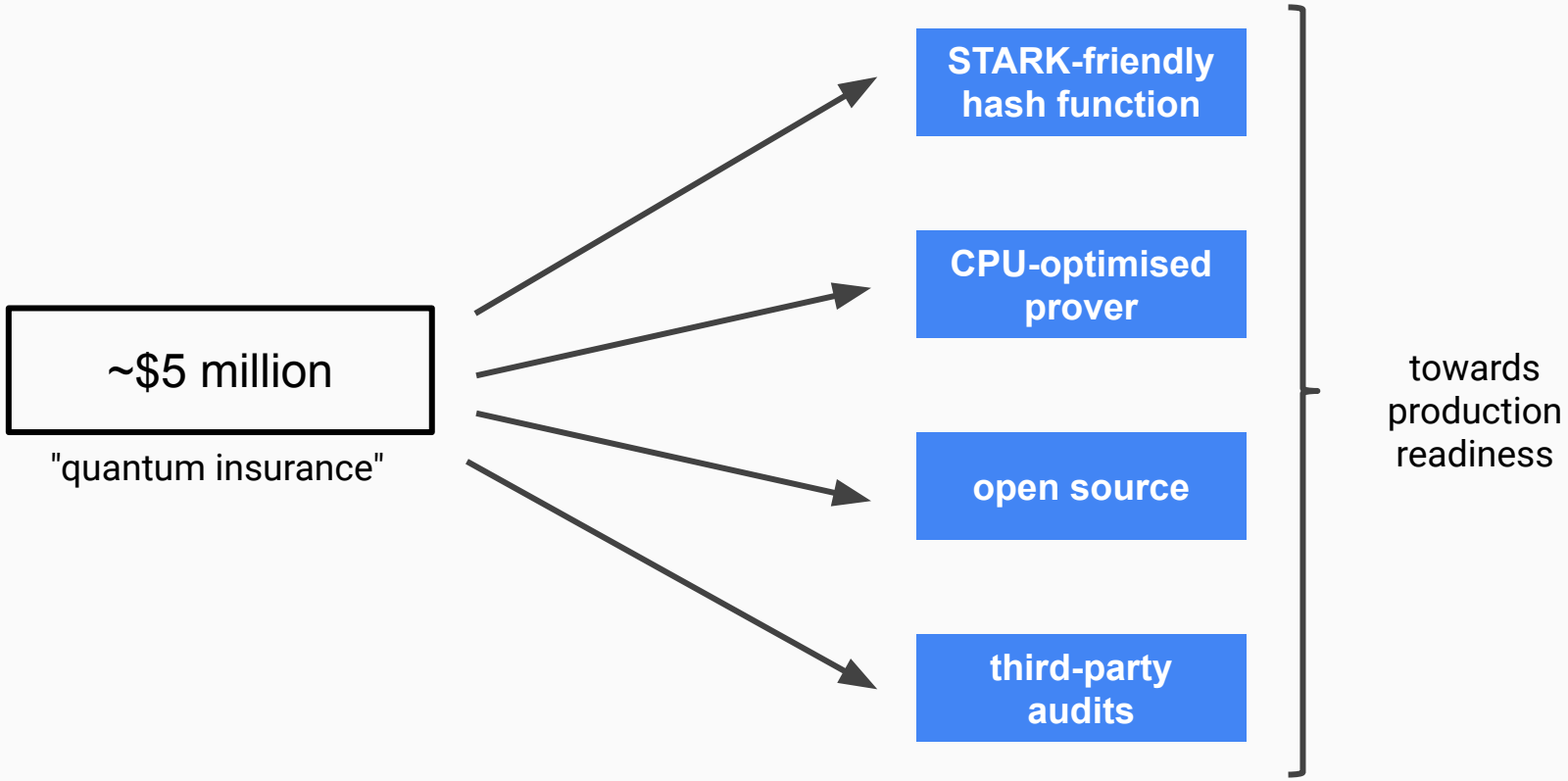
~$5 million

"quantum insurance"

Ethereum Foundation grant (July 2018)



Ethereum Foundation grant (July 2018)



~~plausibly~~ provably quantum secure

Succinct Arguments in the Quantum Random Oracle Model

Alessandro Chiesa
alexch@berkeley.edu
UC Berkeley

Peter Manohar
manohar@berkeley.edu
UC Berkeley

Nicholas Spooner
nick.spooner@berkeley.edu
UC Berkeley

July 18, 2019

~~plausibly~~ provably quantum secure

Succinct Arguments in the Quantum Random Oracle Model

Alessandro Chiesa
alexch@berkeley.edu
UC Berkeley

Peter Manohar
manohar@berkeley.edu
UC Berkeley

Nicholas Spooner
nick.spooner@berkeley.edu
UC Berkeley

July 18, 2019

→ slightly larger proofs

~~plausibly~~ provably quantum secure

Succinct Arguments in the Quantum Random Oracle Model

Alessandro Chiesa
alexch@berkeley.edu
UC Berkeley

Peter Manohar
manohar@berkeley.edu
UC Berkeley

Nicholas Spooner
nick.spooner@berkeley.edu
UC Berkeley

July 18, 2019

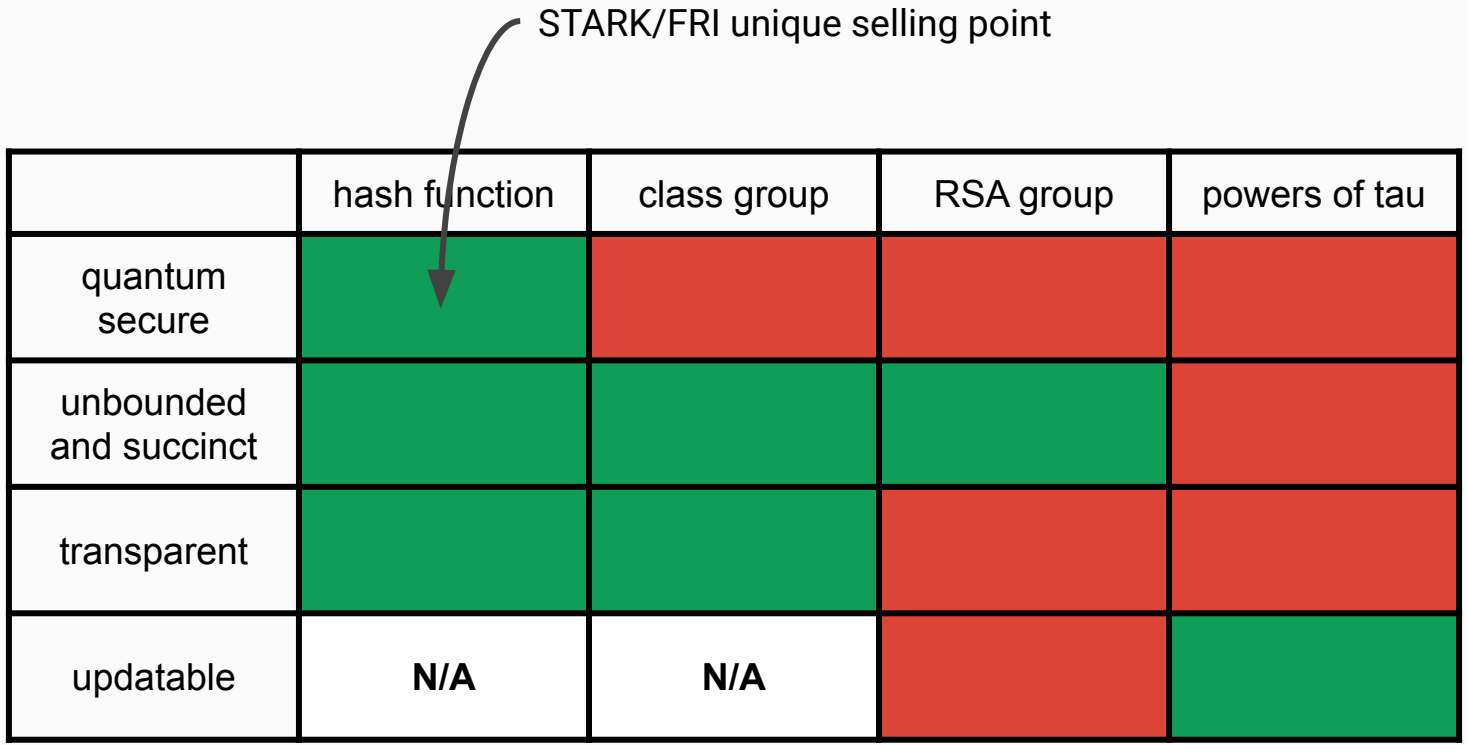
→ slightly larger proofs

concrete constant unknown,
expected ~2x

universal SNARK setups

	hash function	class group	RSA group	powers of tau
quantum secure				
unbounded and succinct				
transparent				
updatable	**N/A**	**N/A**		

universal SNARK setups



Eth1—quantum vulnerability

systemic risk

"**37% of the [Bitcoin] supply is at risk**"

—Pieter Wuille, Mar 2019

systemic risk

exposed pubkeys

"**37% of the [Bitcoin] supply is at risk**"

—Pieter Wuille, Mar 2019

systemic risk

exposed pubkeys 

"**37% of the [Bitcoin] supply is at risk**"

—Pieter Wuille, Mar 2019

- Eth1 vs Bitcoin
  - accounts encourage pubkey reuse vs UTXOs (expecting >37% at risk)
  - hard to migrate contracts (e.g. long-running Augur bet)

systemic risk

exposed pubkeys 

"**37% of the [Bitcoin] supply is at risk**"

—Pieter Wuille, Mar 2019

- Eth1 vs Bitcoin
  - accounts encourage pubkey reuse vs UTXOs (expecting >37% at risk)
  - hard to migrate contracts (e.g. long-running Augur bet)
- governance intervention
  - false positives
  - possibly controversial

inertia

"Historically, it has taken **almost two decades to deploy our modern public key cryptography infrastructure**."—NIST website

inertia

"Historically, it has taken **almost two decades to deploy our modern public key cryptography infrastructure**."—NIST website

NIST post-quantum competition

- 2016—kickoff
- 2017—round 1 (69 candidates)
- 2019—round 2 (26 candidates)
- 2021—round 3
- 2024—draft standard

inertia

"Historically, it has taken **almost two decades to deploy our modern public key cryptography infrastructure**."—NIST website

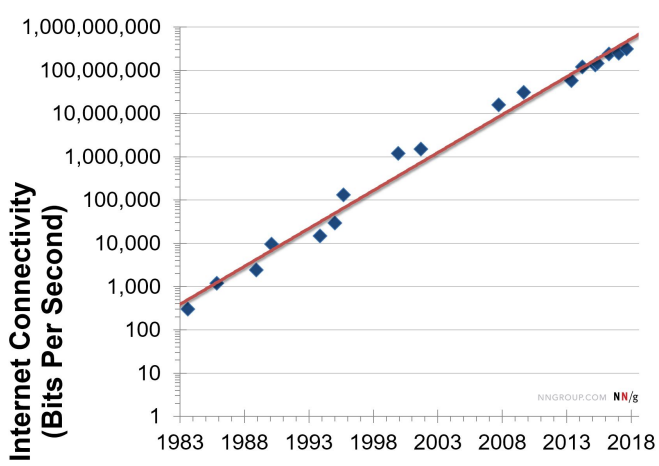
NIST post-quantum competition

- 2016—kickoff
- 2017—round 1 (69 candidates)
- 2019—round 2 (26 candidates)
- 2021—round 3
- 2024—draft standard

→ additional friction from blockchain governance

data is cheap™

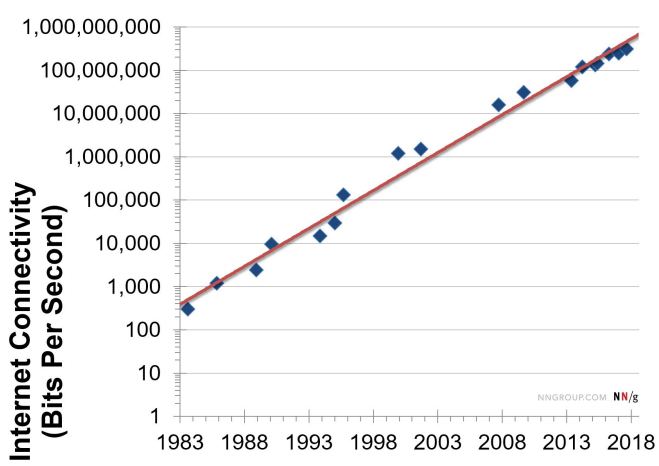
Nielsen's law—bandwidth grows by 50% per year



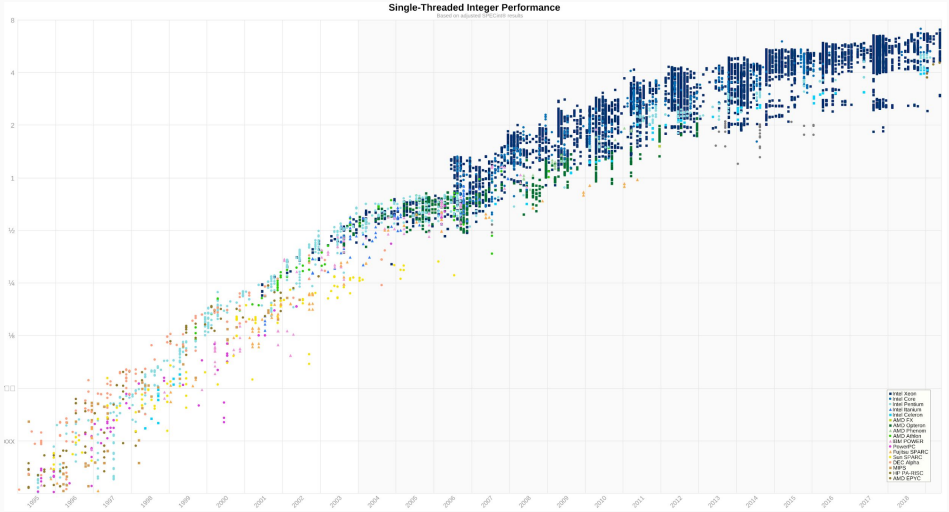
data is cheap™

Nielsen's law—bandwidth grows by 50% per year

- data is fungible—a byte is a byte
- data is massively parallelizable
- 200kB proof today ~ 3.5kB proof in 10 years



gas repricing



over time
data gets cheaper
than computation

call data repricing

- **EIP2028**—67 gas/byte to 16 gas/byte
- **prediction**—more data repricings

Eth2—quantum infancy

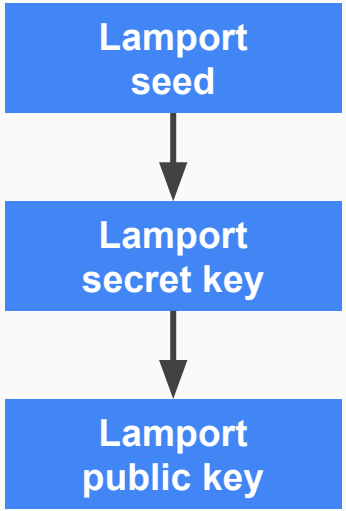
backup signatures

- **quantum apocalypse backup**—one-time migration
- **Lamport**—simple, available today, low overhead
- **backwards compatible**—integratable in any existing signature scheme

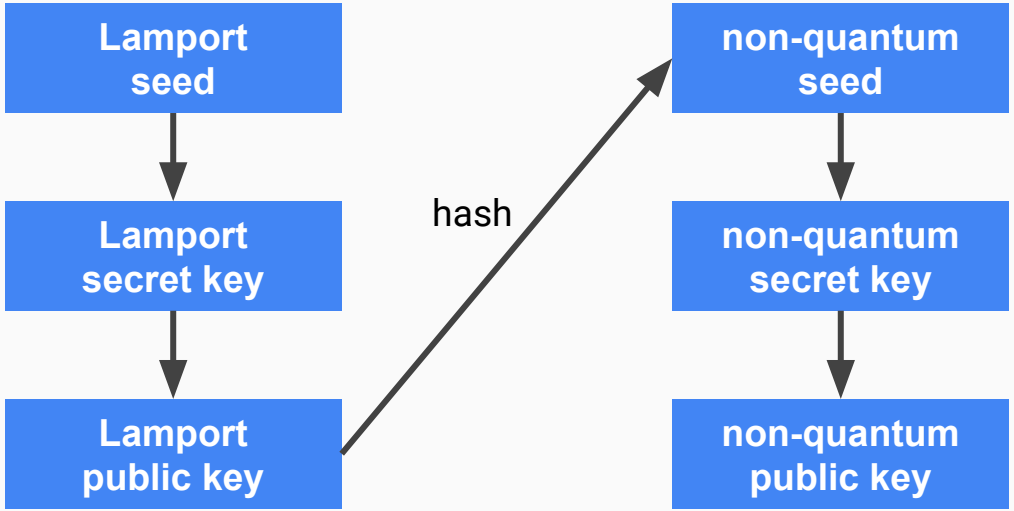
backup signatures

- **quantum apocalypse backup**—one-time migration
- **Lamport**—simple, available today, low overhead
- **backwards compatible**—integratable in any existing signature scheme

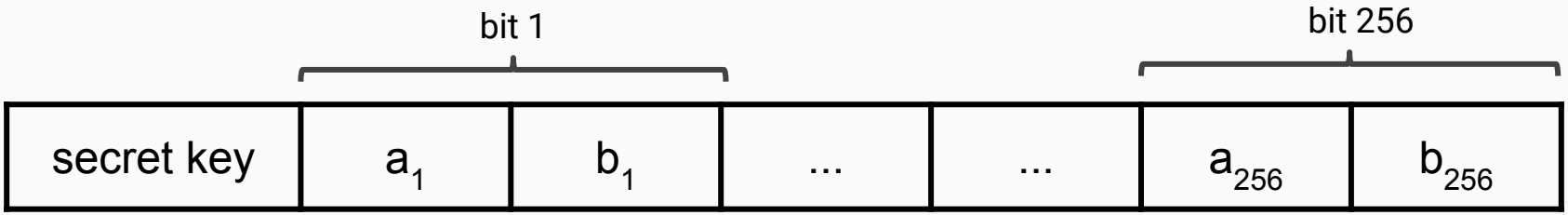
backup signatures



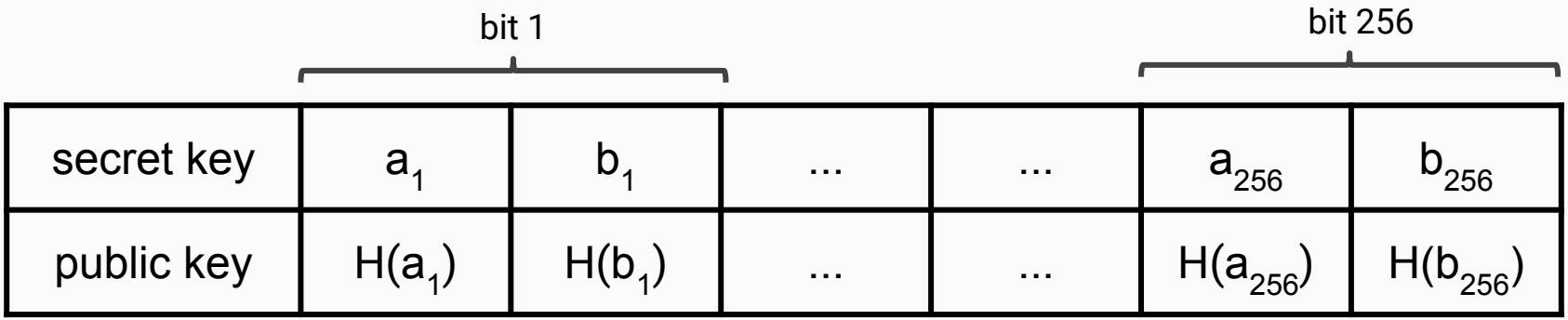
quantum apocalypse contingency



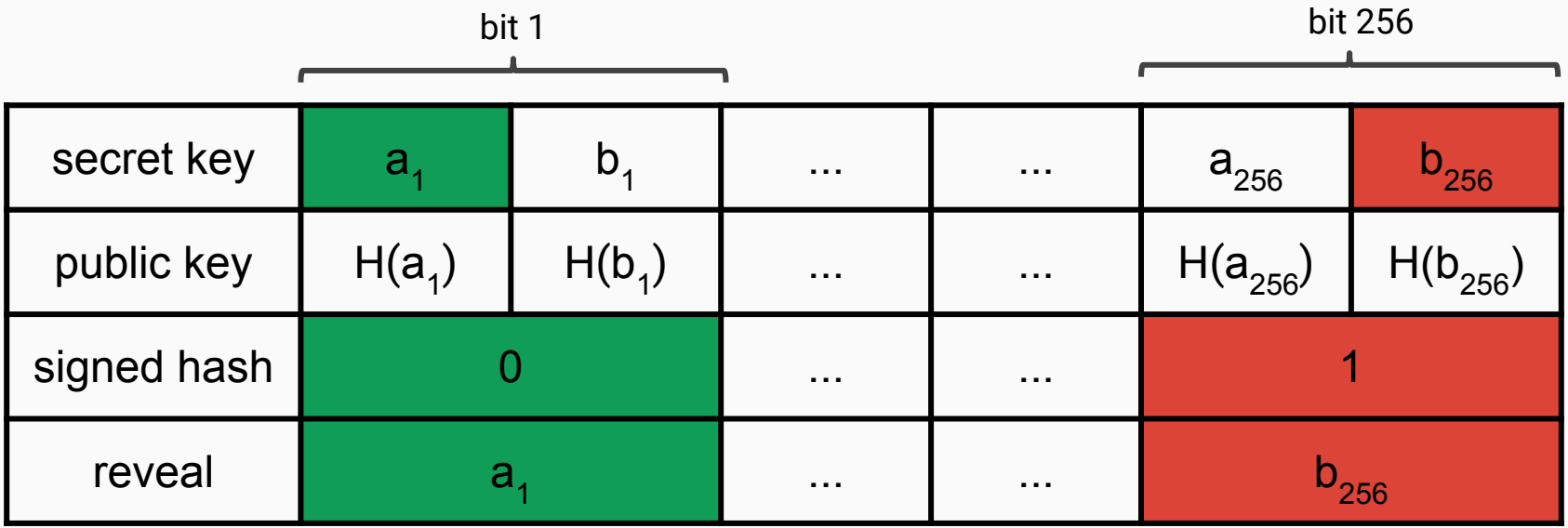
Lamport signatures



Lamport signatures



Lamport signatures



multi-hashing

	SHA256
security	conservative
speed (plain text)	fast
popularity	high
STARK-friendly	no

multi-hashing

	SHA256	low arithmetic complexity hash
security	conservative	experimental
speed (plain text)	fast	slower
popularity	high	low
STARK-friendly	no	yes

multi-hashing

	SHA256	low arithmetic complexity hash
security	conservative	experimental
speed (plain text)	fast	slower
popularity	high	low
STARK-friendly	no	yes

STARK-friendly hash challenge

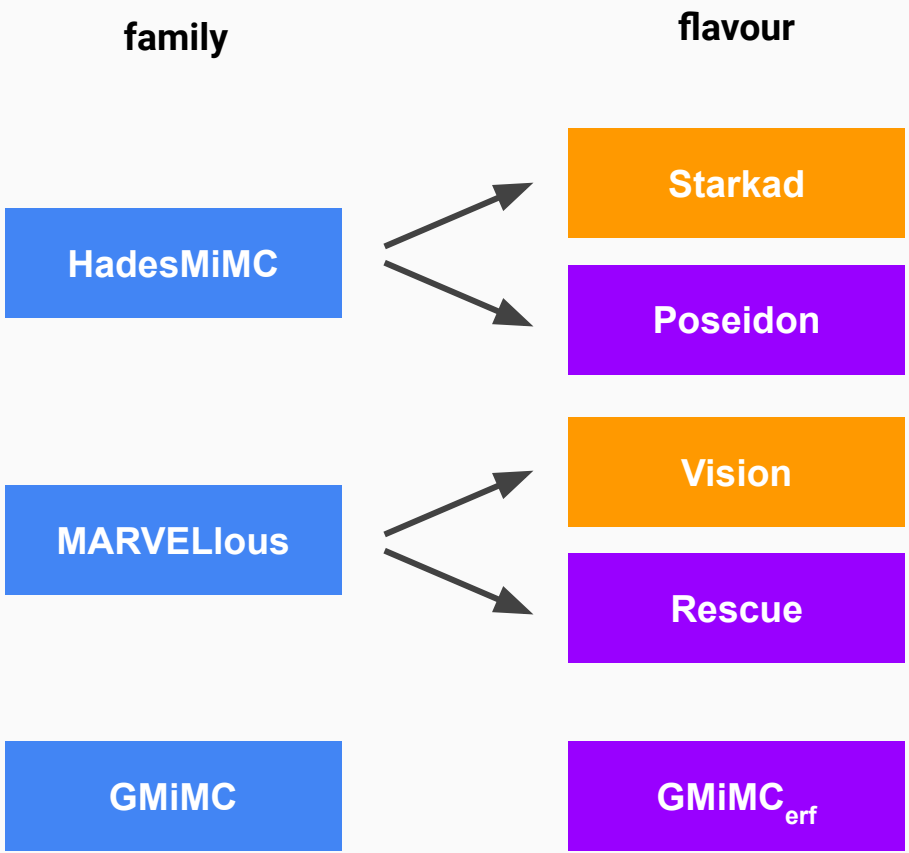
family

HadesMiMC

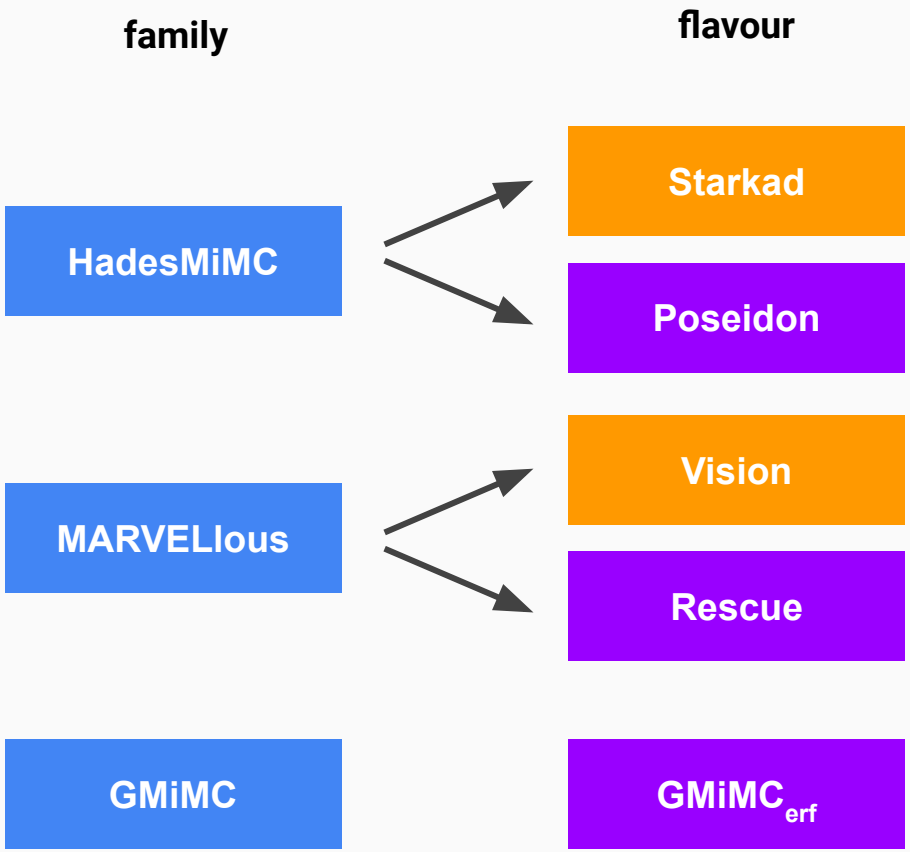
MARVELlous

GMiMC

STARK-friendly hash challenge



STARK-friendly hash challenge



STARK-friendly fields

- prime fields
- high 2-adicity

→ compatible with SNARKs 🎉

longer addresses

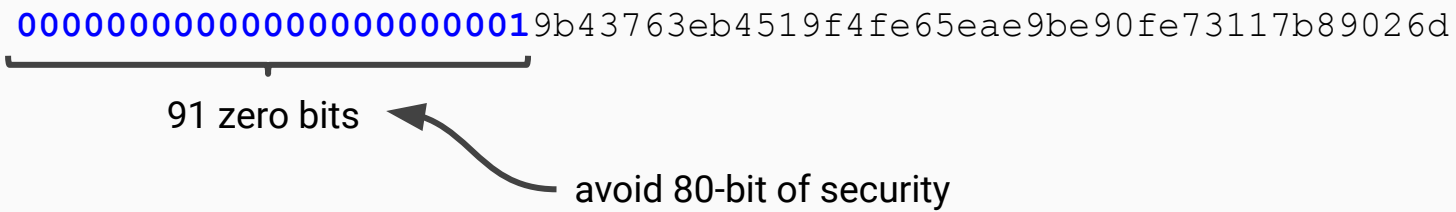
length matters

- current output length **n** = 160 bits
- classical collision resistance—**O(n/2)** ~ 80 bits
- quantum collision resistance—**O(2n/5)** ~ 64 bits (technically **O(n/3)** = 60 bits)
- future cryptanalytic weakenings

longer addresses

length matters

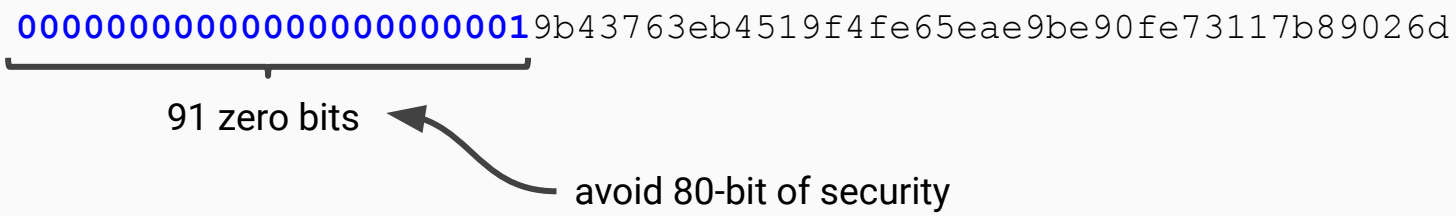
- current output length **n** = 160 bits
- classical collision resistance—**O(n/2)** ~ 80 bits
- quantum collision resistance—**O(2n/5)** ~ 64 bits (technically **O(n/3)** ~ 60 bits)
- future cryptanalytic weakenings



longer addresses

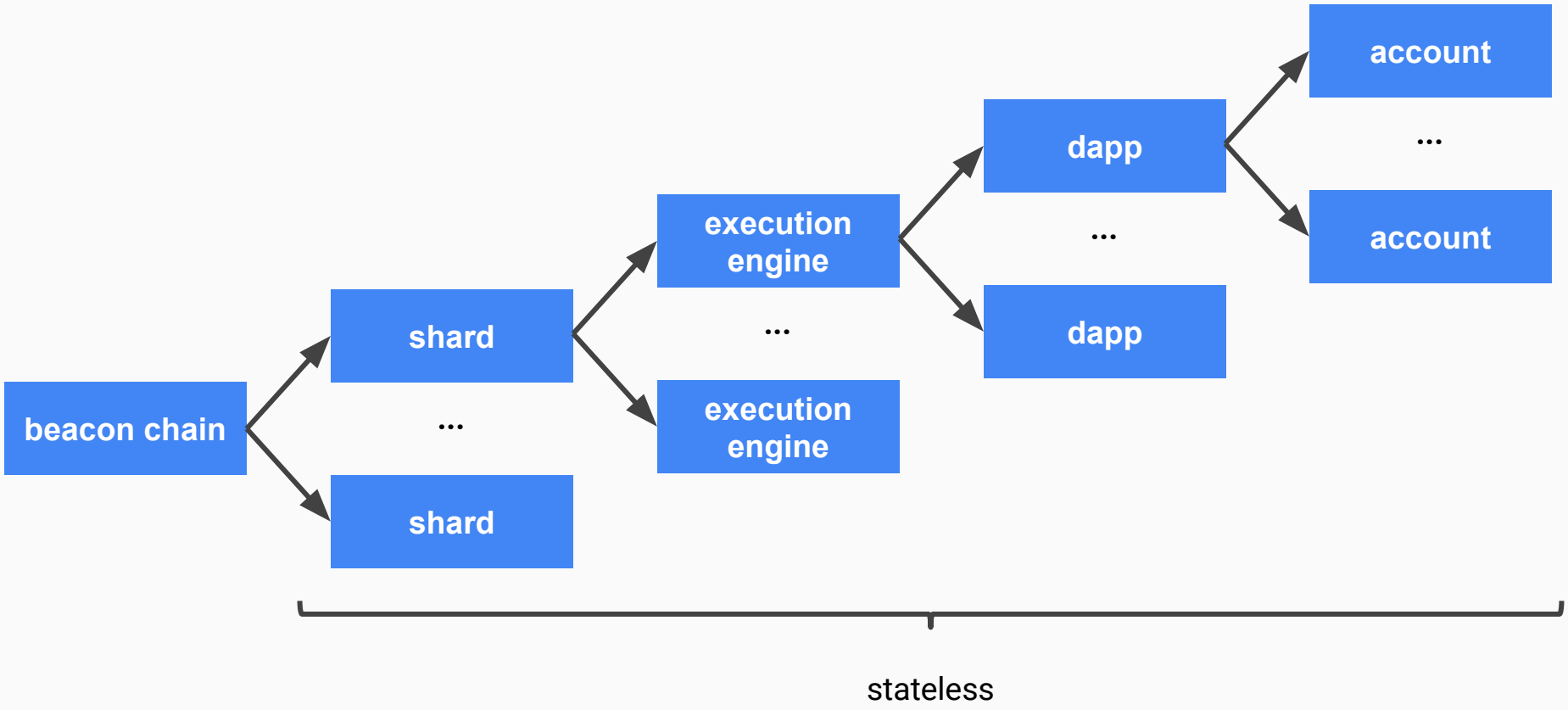
length matters

- current output length **n** = 160 bits
- classical collision resistance—**O(n/2)** ~ 80 bits
- quantum collision resistance—**O(2n/5)** ~ 64 bits (technically **O(n/3)** = 60 bits)
- future cryptanalytic weakenings

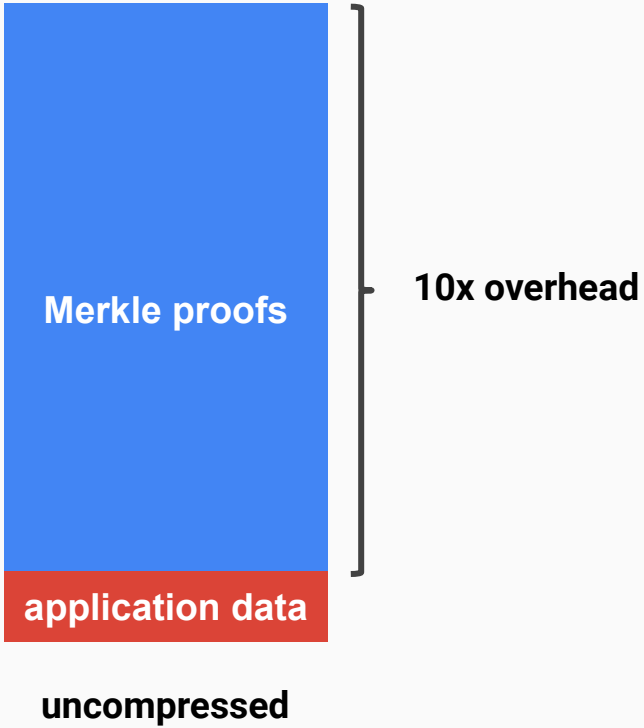


new **n**—256 bits

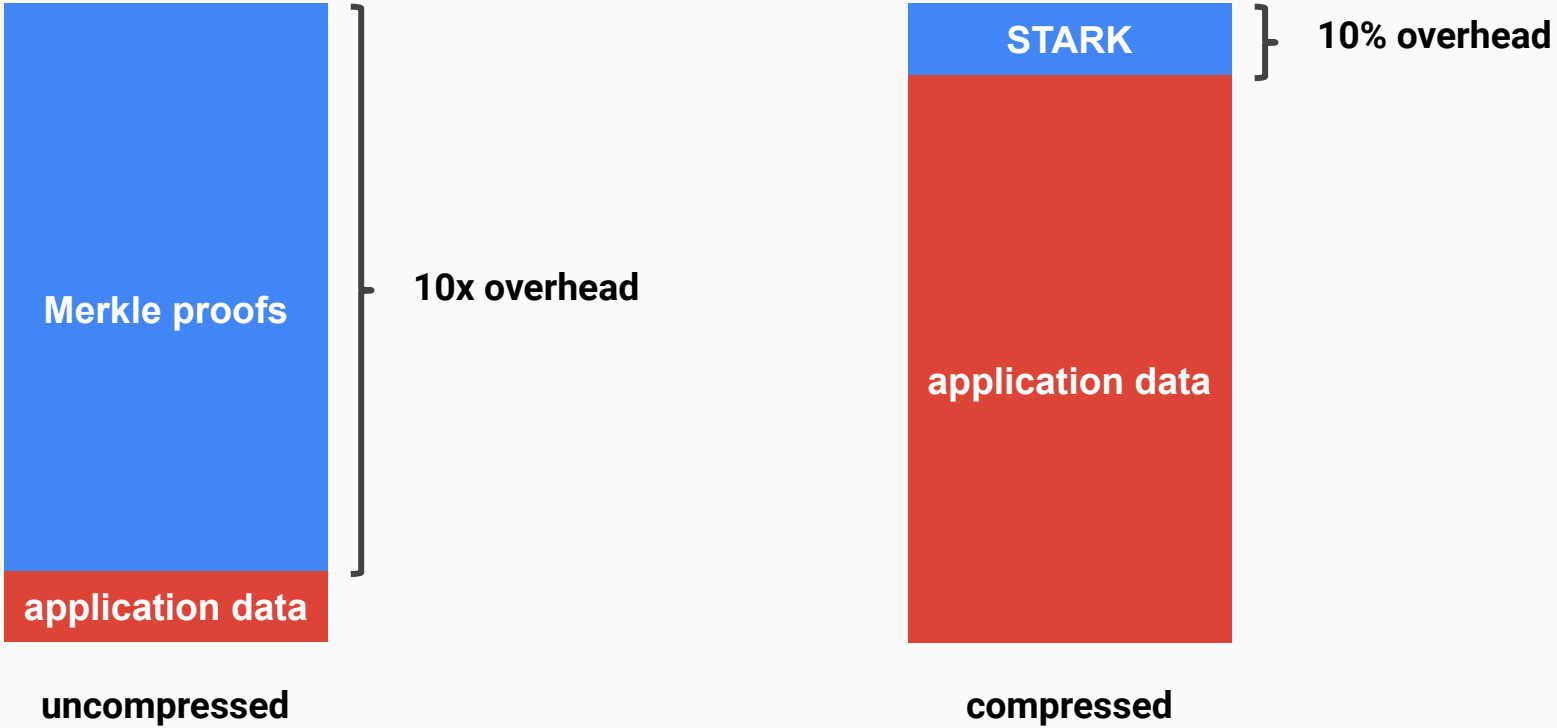
witness compression for stateless clients



witness compression for stateless clients



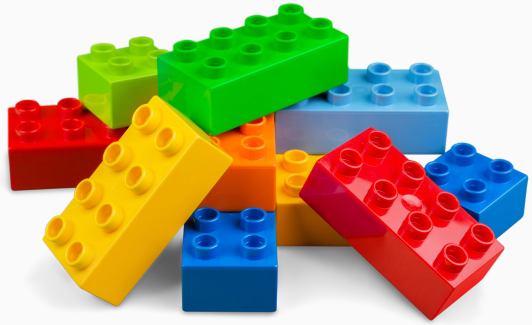
witness compression for stateless clients



abstraction

not opinionated

- no enshrined ECDSA
- no minimum 21,000 gas

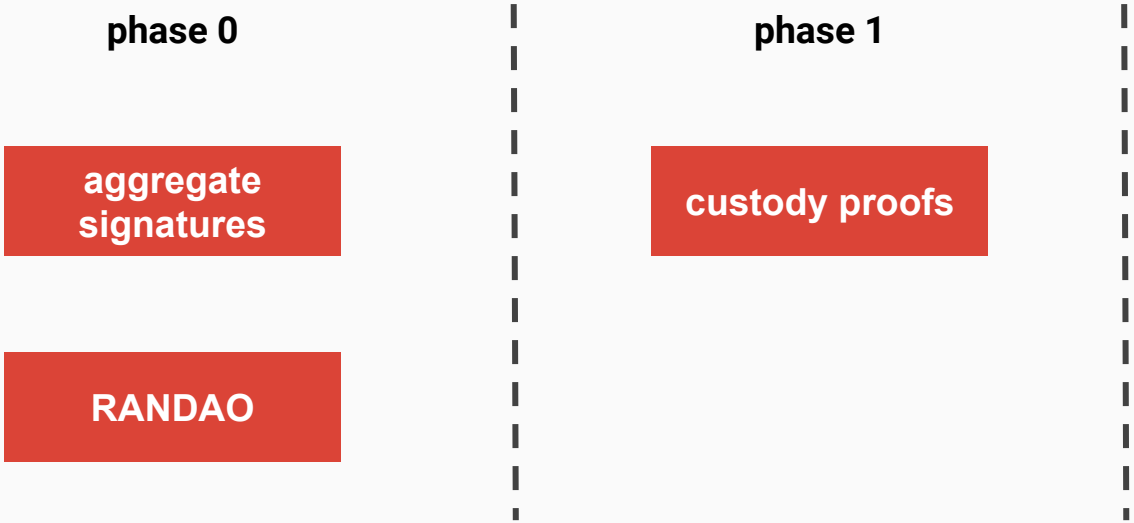


quantum canary

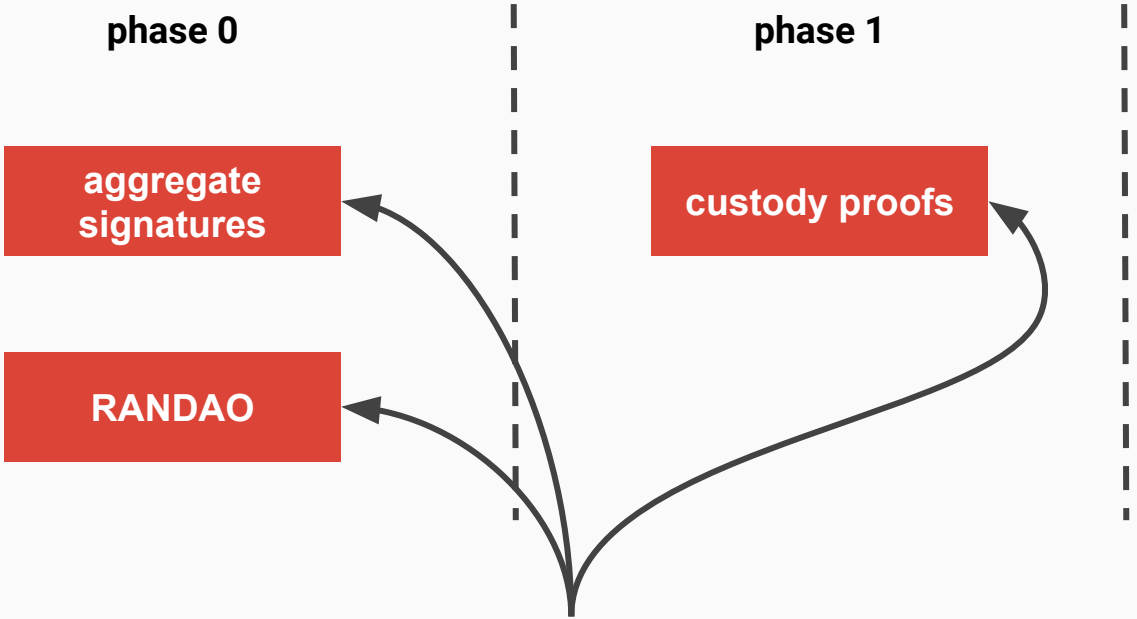
- **early detection**—calibrated quantum advantage problem
- **bounty**—e.g. 1m ETH minted by the consensus
- **programmatic**—trigger for consensus and contracts

Eth3—quantum security

Eth2 pre-quantum cryptography



Eth2 pre-quantum cryptography



secrets involved

- BLS12-381 private key
- MPC-friendliness requirement

Eth2 pre-quantum cryptography

Eth2 pre-quantum cryptography

phase 0

aggregate signatures

RANDAO

phase 1

custody proofs

phase 2

VDF

group of unknown order

- 2048-bit RSA group
- trapdoor

aggregate signatures

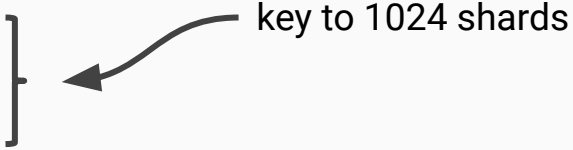
aggregation constraints

- batches of 1024 signatures
- 128 batches per block

aggregate signatures

aggregation constraints

- batches of 1024 signatures
- 128 batches per block



aggregate signatures

aggregation constraints

- batches of 1024 signatures
- 128 batches per block

key to 1024 shards

idea

preference for hash-based signature schemes
(e.g. Lamport, Winternitz, SPHINCS+)

- batch 1024 Lamport signatures into a STARK
- aggregate those 128 STARKs into one STARK

aggregate signatures

aggregation constraints

- batches of 1024 signatures
- 128 batches per block

key to 1024 shards

idea

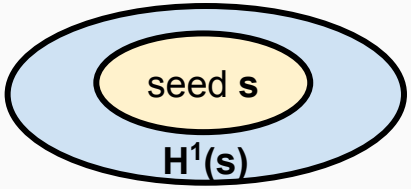
preference for hash-based signature schemes
(e.g. Lamport, Winternitz, SPHINCS+)

- batch 1024 Lamport signatures into a STARK
- aggregate those 128 STARKs into one STARK

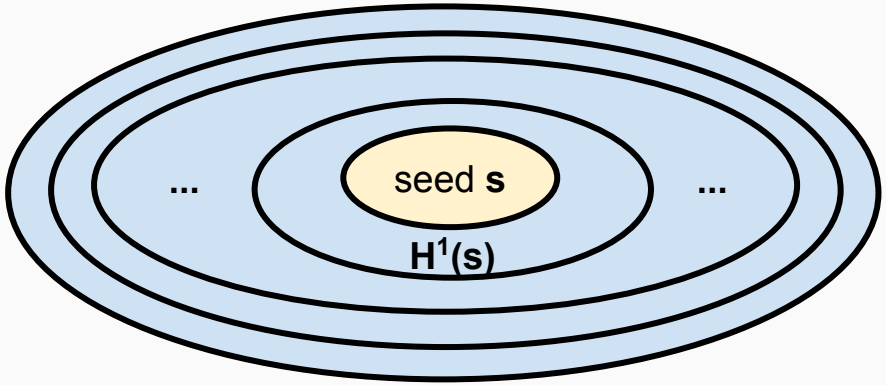
open problem—add MPC-friendliness

RANDAO hash onions

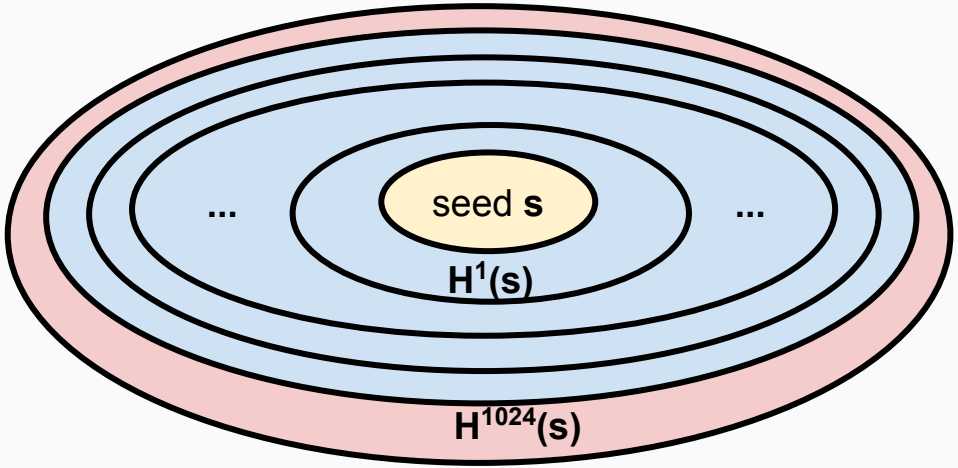
RANDAO hash onions



RANDAO hash onions

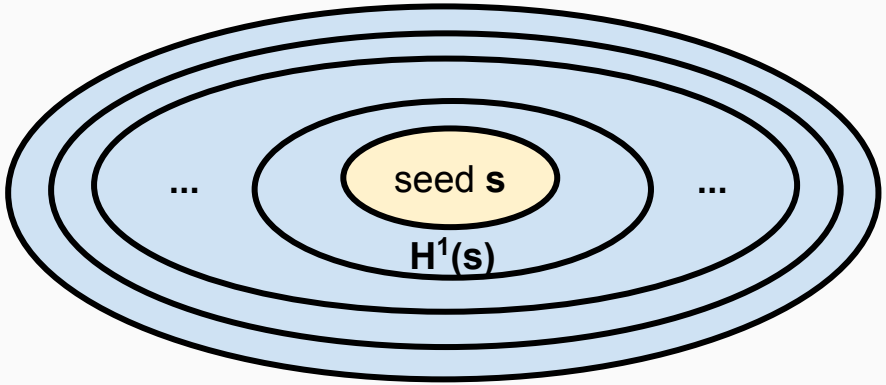


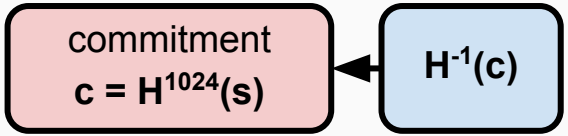
RANDAO hash onions



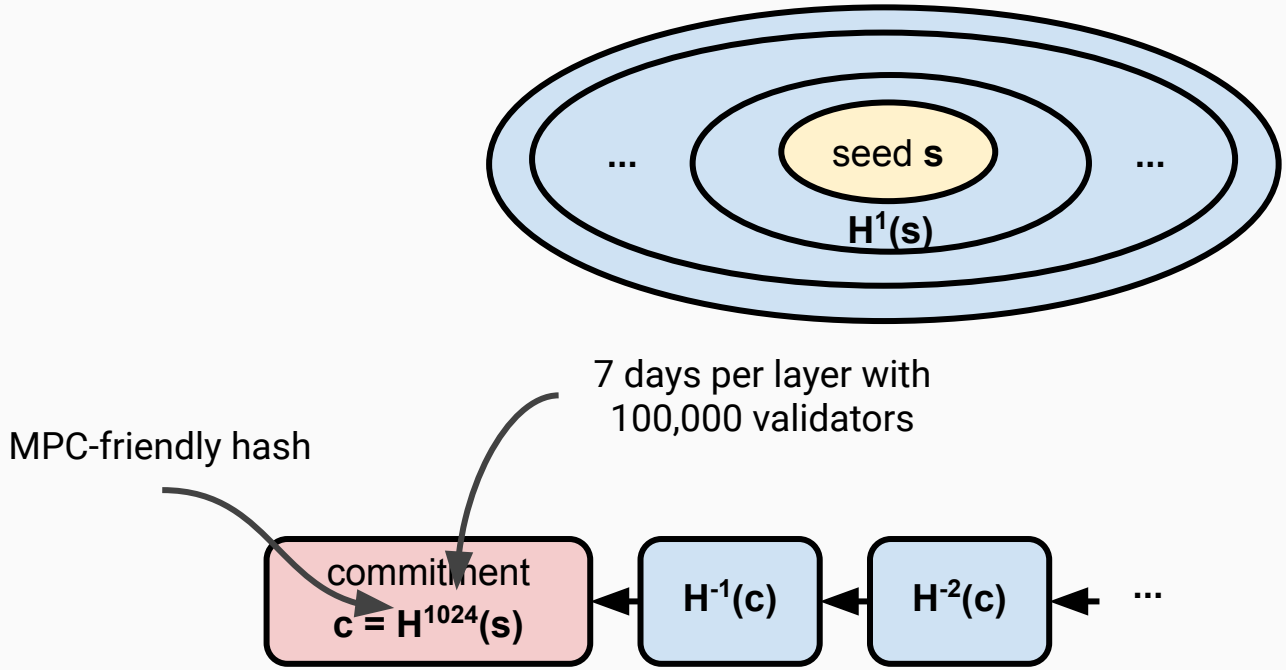
commitment
c = $H^{1024}(s)$

RANDAO hash onions





RANDAO hash onions



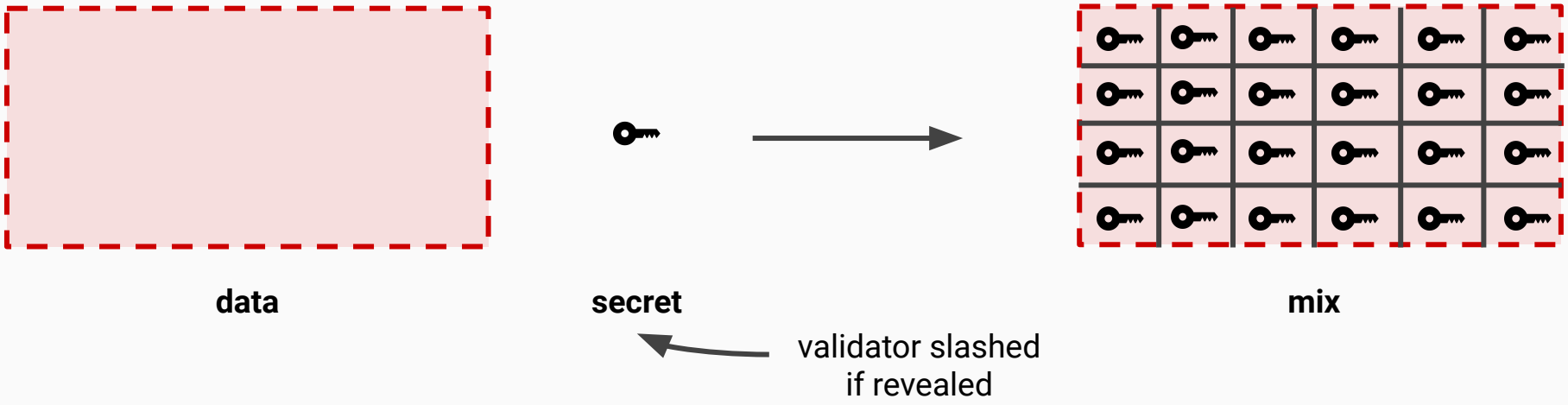
custody proofs

data

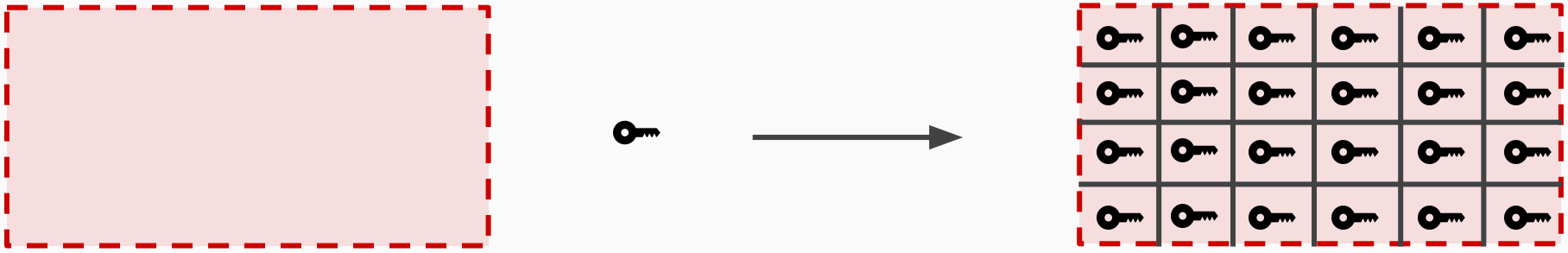
secret

validator slashed
if revealed

custody proofs



custody proofs



statement—I know **mix** consistent with **H(data)** and **H(secret)**

VDFs

permutation polynomial

constant gap
"bootstrap"

STARKs

exponential gap
parallelism

VDFs

permutation polynomial

constant gap
"bootstrap"

STARKs

exponential gap
parallelism

pros

- quantum secure
- no trusted setup
- cheaper evaluator hardware
- easier to reason about lower bounds

VDFs

permutation polynomial

constant gap
"bootstrap"

STARKs

exponential gap
parallelism

pros

- quantum secure
- no trusted setup
- cheaper evaluator hardware
- easier to reason about lower bounds

cons

- larger proofs
- more expensive prover hardware

bonus—minimise fraud proofs

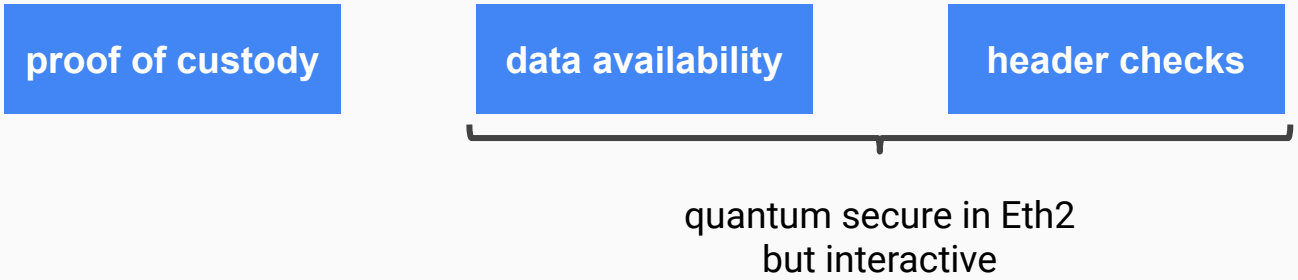
blockchain design heuristics

- If cryptography doesn't work, try cryptoeconomics.
- If cryptography does work, avoid cryptoeconomics.

bonus—minimise fraud proofs

blockchain design heuristics

- If cryptography doesn't work, try cryptoeconomics.
- If cryptography does work, avoid cryptoeconomics.



thank you :)