ETSI/IQC Quantum Safe Cryptography Conference 2026

Post-Quantum Consensus

Presented by:

Thomas Coratger

Ethereum Foundation

17/06/2026

© ETSI 2026. All rights reserved.

Post-Quantum Consensus

Thomas Coratger

Post-Quantum Team · Ethereum Foundation

Post-quantum touches every layer.

Consensus how validators agree	today ~~BLS signatures~~	→	post-quantum **hash-based**
Execution how transactions run	today ~~ECDSA signatures~~	→	post-quantum **hash-based**
Data availability & sampling	today ~~KZG commitments~~	→	post-quantum **hash-based**

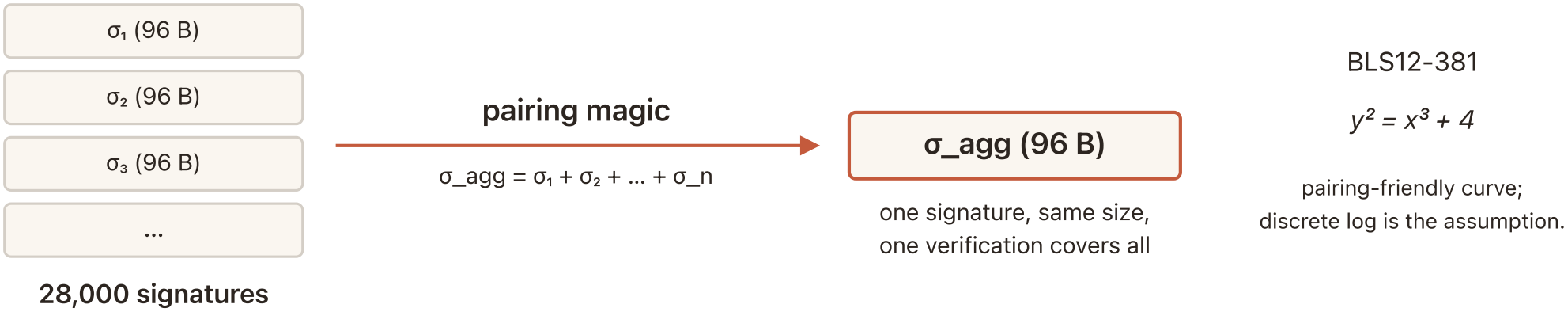
One assumption to retire on every layer. This talk goes deep on the consensus layer.

Inspired by strawmap.org.

I

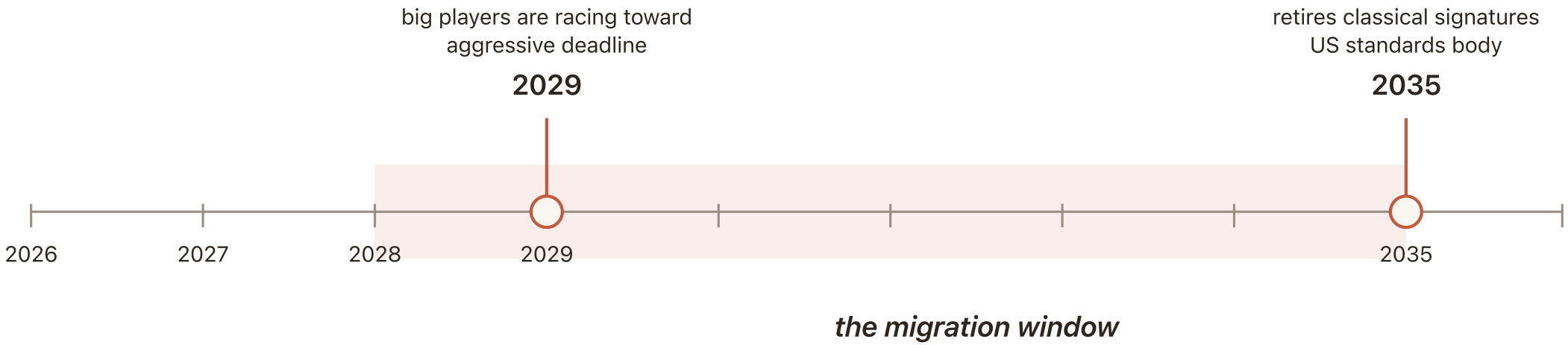
threat

Today: BLS on BLS12-381.



One aggregate verification per slot covers every voter. The whole protocol is built around this.

A window everyone is racing.

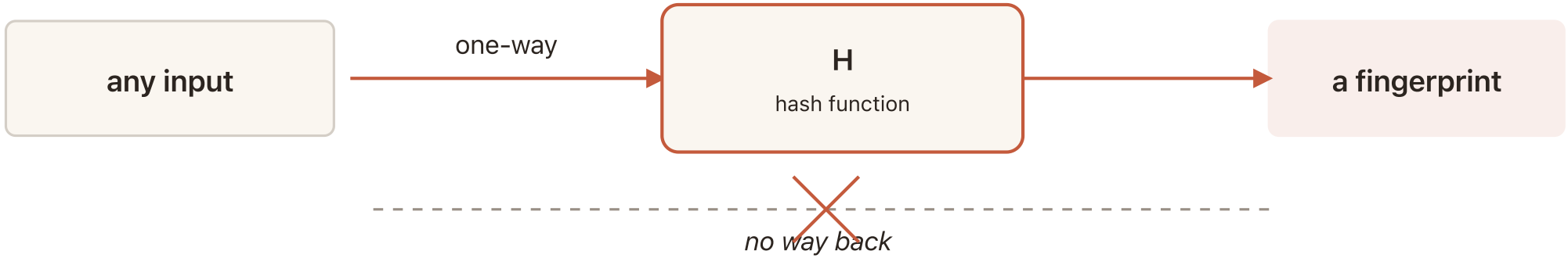


the migration window

II

approach

One ingredient: a hash function.

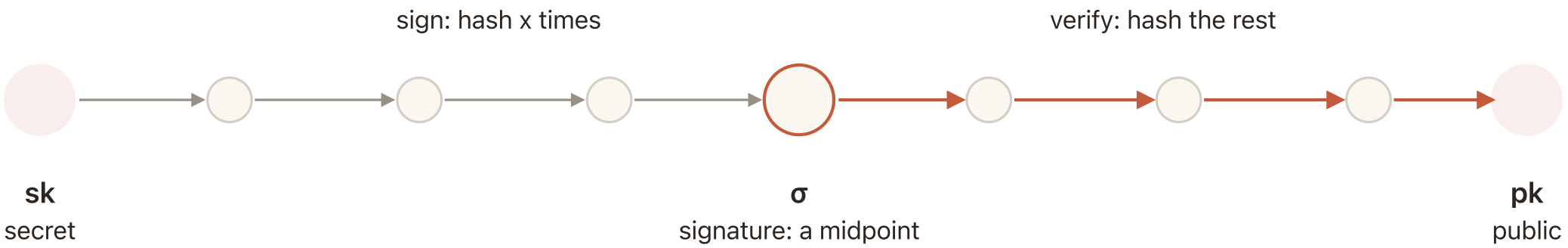


Hash-based signatures rest on this one assumption. Decades old. Already trusted everywhere.

A signature, built only from a hash chain.

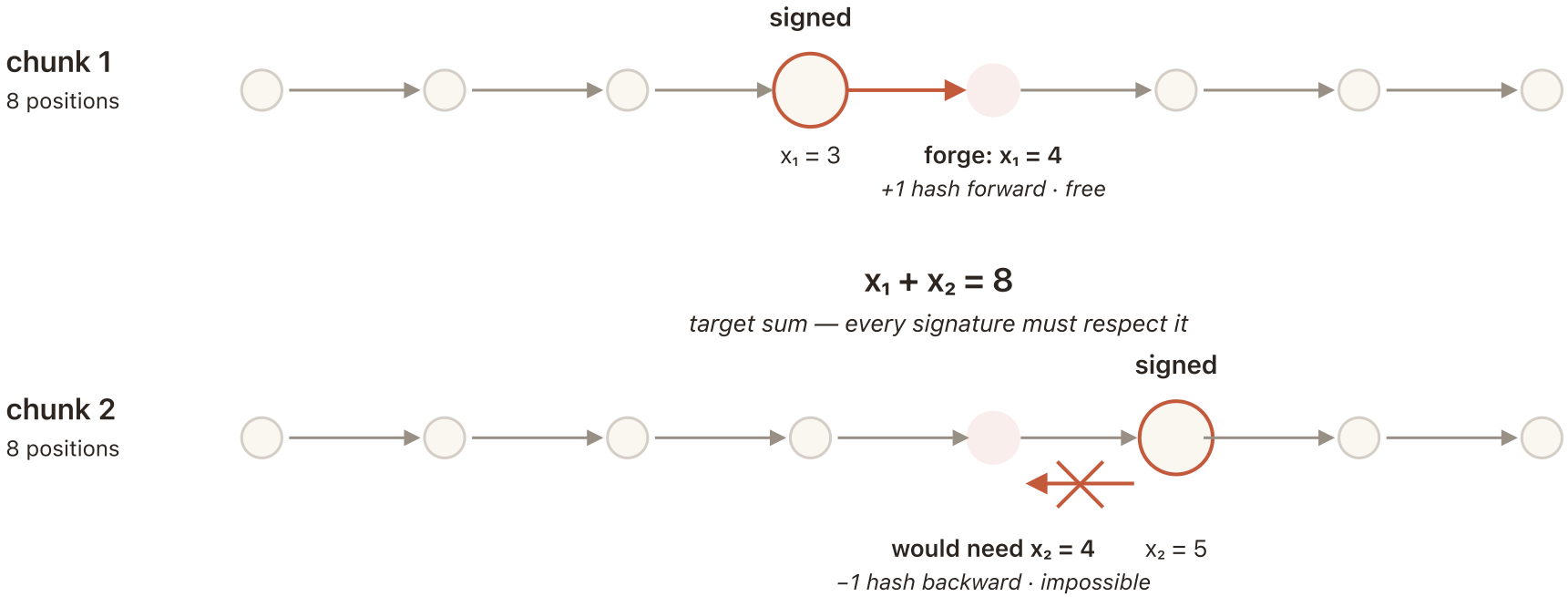
Winternitz. No curves. No pairings. No discrete logs.

The Winternitz idea, in one picture.



A forge would have to hash backward.

Sign the message in chunks. Force their positions to add to a fixed target.

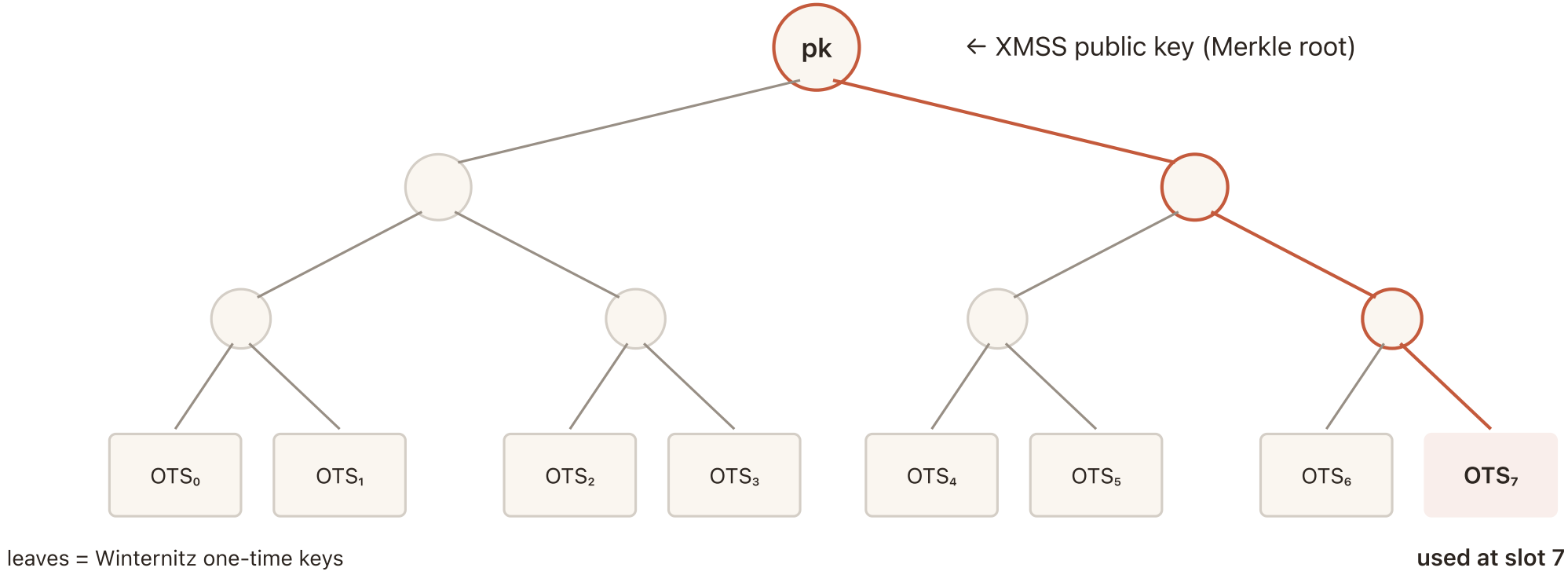


Target-sum Winternitz — what leanSig ships today.

One key, one signature.

A validator signs every slot, for years. We need more.

XMSS: a Merkle tree of one-time keys.



The signature reveals: the OTS signature + the authentication path to the root.

But hash signatures don't aggregate.

BLS today

96 B

one aggregate per slot,
regardless of signers

Naive hash-based

~70 MB

leanSig sig (2.5 KB) × ~28,000,
per slot

Without aggregation, the consensus layer **stops running** at this scale.

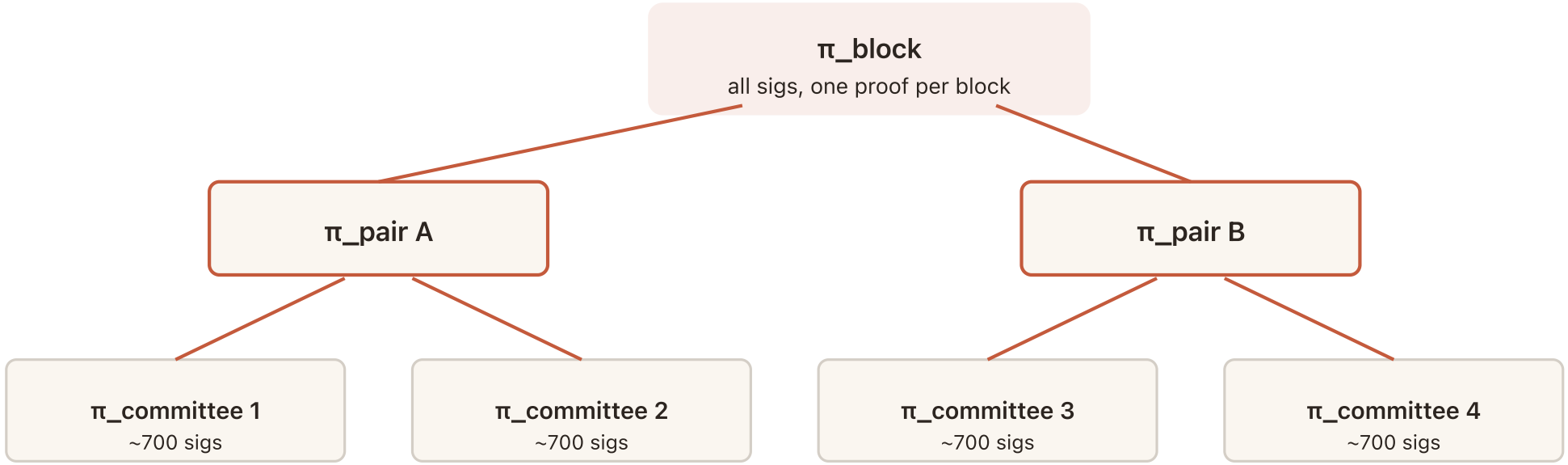
Don't aggregate signatures. Aggregate the proofs.

The signatures never leave the prover. The chain only sees π.

The compressor is a STARK.

Itself hash-based. Nothing in the loop is vulnerable to Shor.

Then we aggregate the aggregates.



One proof per block, regardless of how many validators voted.

Thomas Coratger

Post-Quantum Team · Ethereum Foundation

PQ.ETHEREUM.ORG · LEANROADMAP.ORG · GITHUB.COM/LEANETHEREUM