CONSENSYS

Stateless Ethereum - Witnesses

Verkle Tries

Symposium on Distributed Ledger Technology 5

23rd November 2021

Raghavendra Ramesh
Consensys Software R&D

Ethereum Horizon

The Merge Q2 2022

Stateless Ethereum
Next big upgrade

Outline

1. Why?
2. What is Stateless Ethereum?
3. What is a witness?
4. Current Technology - Merkle Patricia Tries (MPT)
5. Proposed Technology - Verkle Tries
6. Summary

Why?

Ethereum State Growth Problem

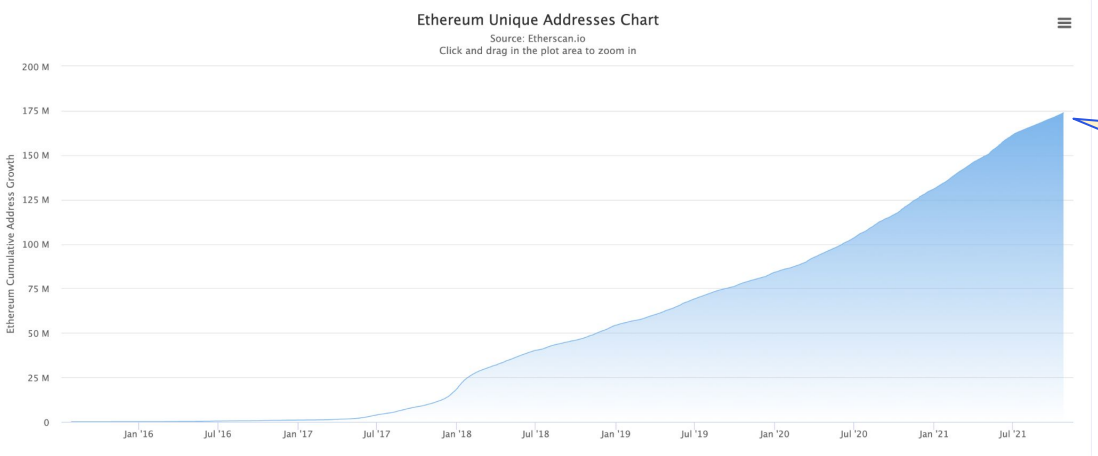
Ethereum State Size is growing quickly.

35 GB (4 months ago)

100 GB MPT size

Growing by ~50 GB each year

- Permanent ongoing costs on the network
- Burdens current nodes and new nodes (state sync)
- Hinders ‘true’ decentralisation. Critical.
- Unsustainable economic model



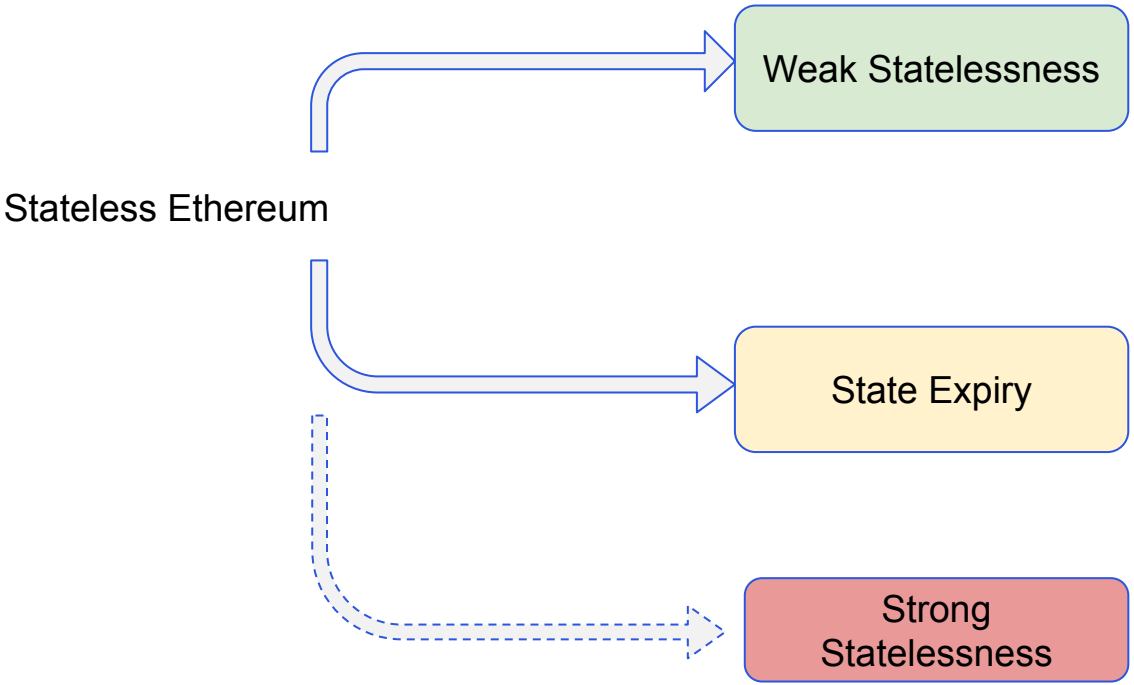
~175 million addresses

What is Stateless Ethereum?

Statelessness Goals

- Bound the state size
- Enable participation from resource constrained devices. Greater decentralisation.

Paths to Stateless



My talk

Click here

OR

Search
Ethereum State Expiry on YouTube

Weak Statelessness

- Block producers or Miners store full state
- **Relief.** Other nodes are stateless. Store only the *State root.*
- Block producers add witnesses to the block of transactions
- Users still need to add partial witnesses (nonce, balance)
- Other nodes can validate, execute the transaction, and can update the stateroot.

What is a witness?

Data required for a transaction

EOA A -- 5 ETH → EOA B

Balance and nonce of A,

Balance of B

EOA A calls C.getV()

Balance and Nonce of A

Code of C.getV()

value of C.v

EOA A calls C.addElementToArray()

Balance and Nonce of A

Code of C.addElementToArray()

EOA A calls C.setV()

Balance and Nonce of A

Code of C.setV()

Block producer

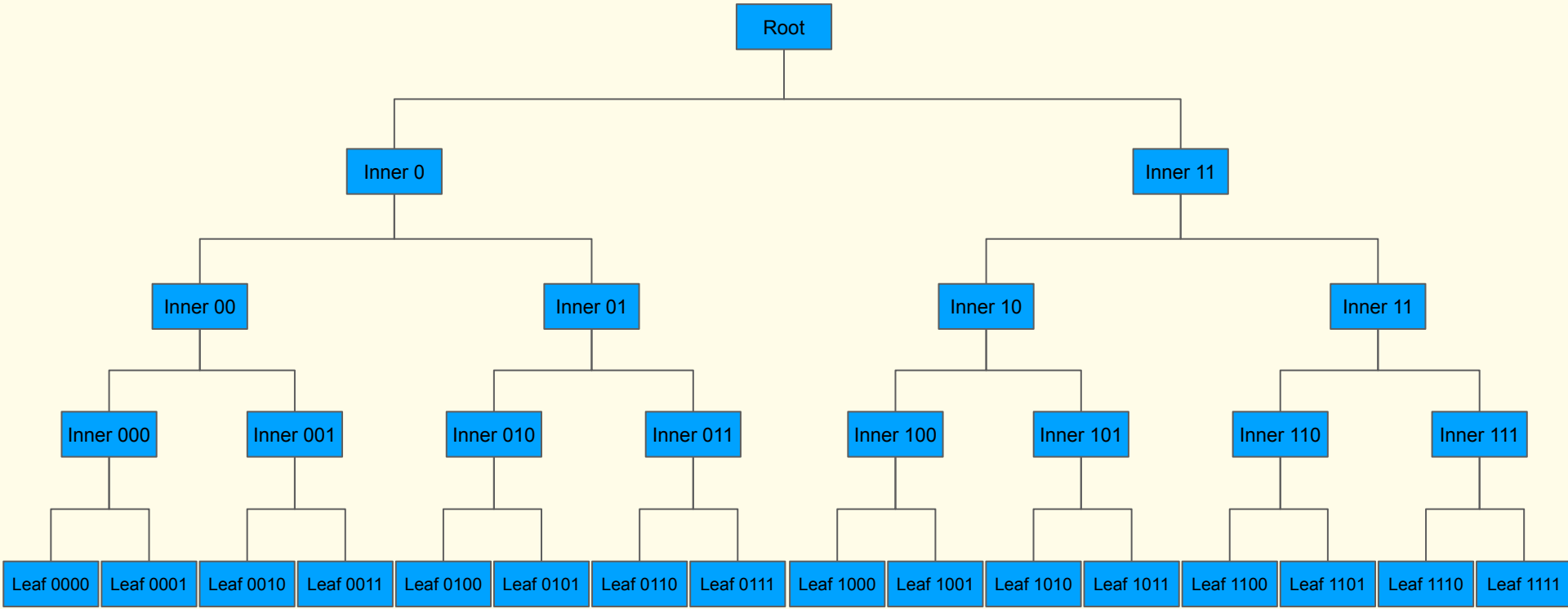
- Provides data
- Provides proof of integrity

Storing Technology of State Data

Merkle Patricia Tries

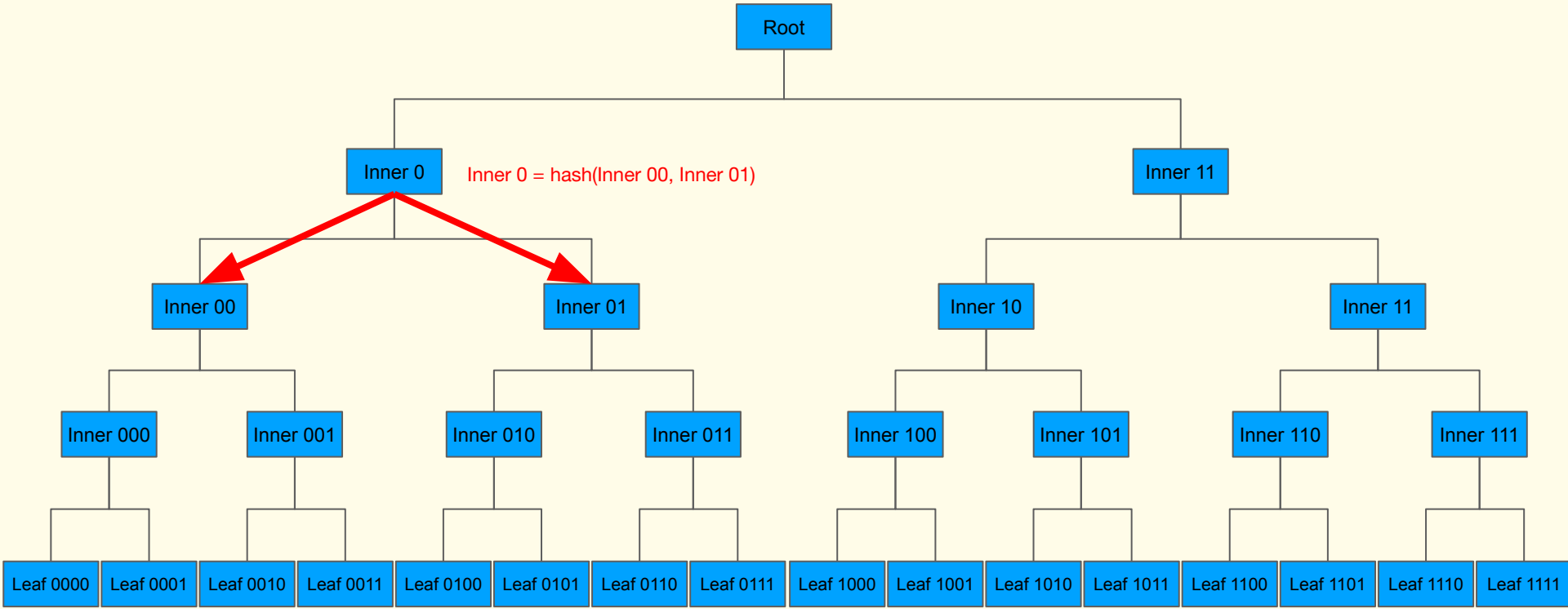
Current Technology

Merkle tree



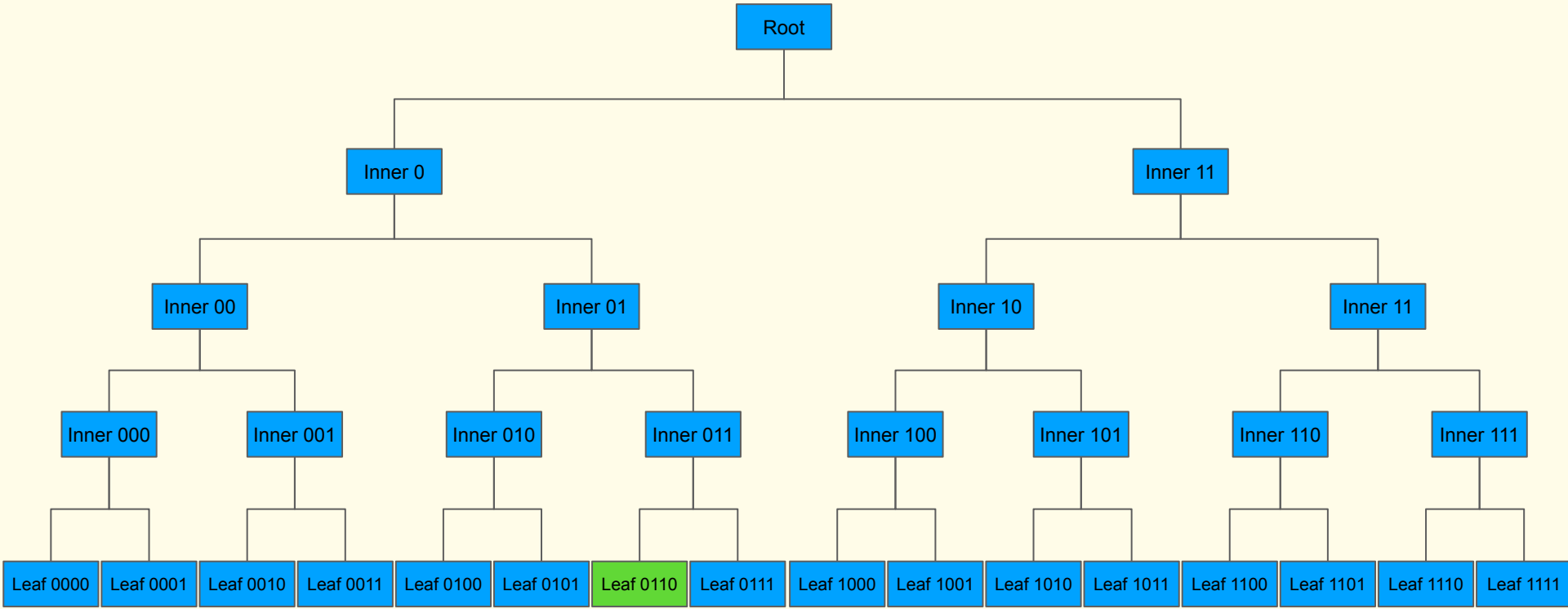
Ack: Slide from Dankrad's presentation

Merkle tree



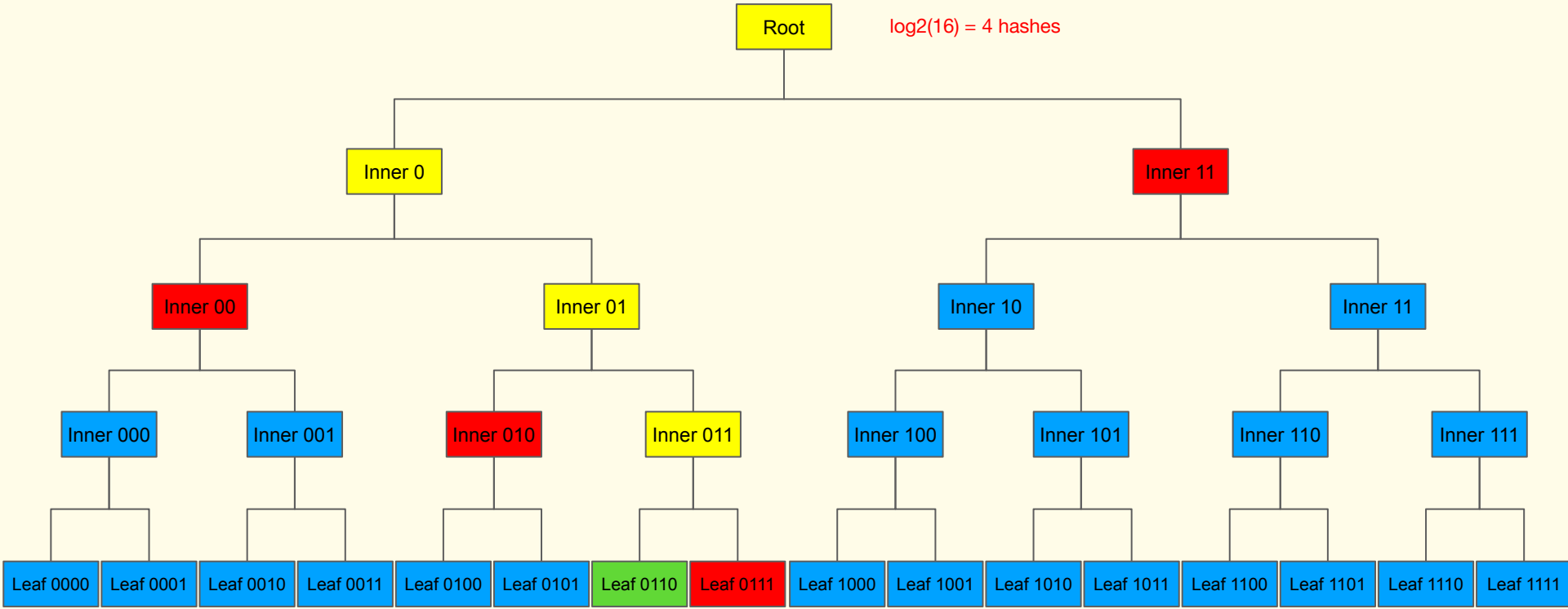
Ack: Slide from Dankrad's presentation

Merkle proof



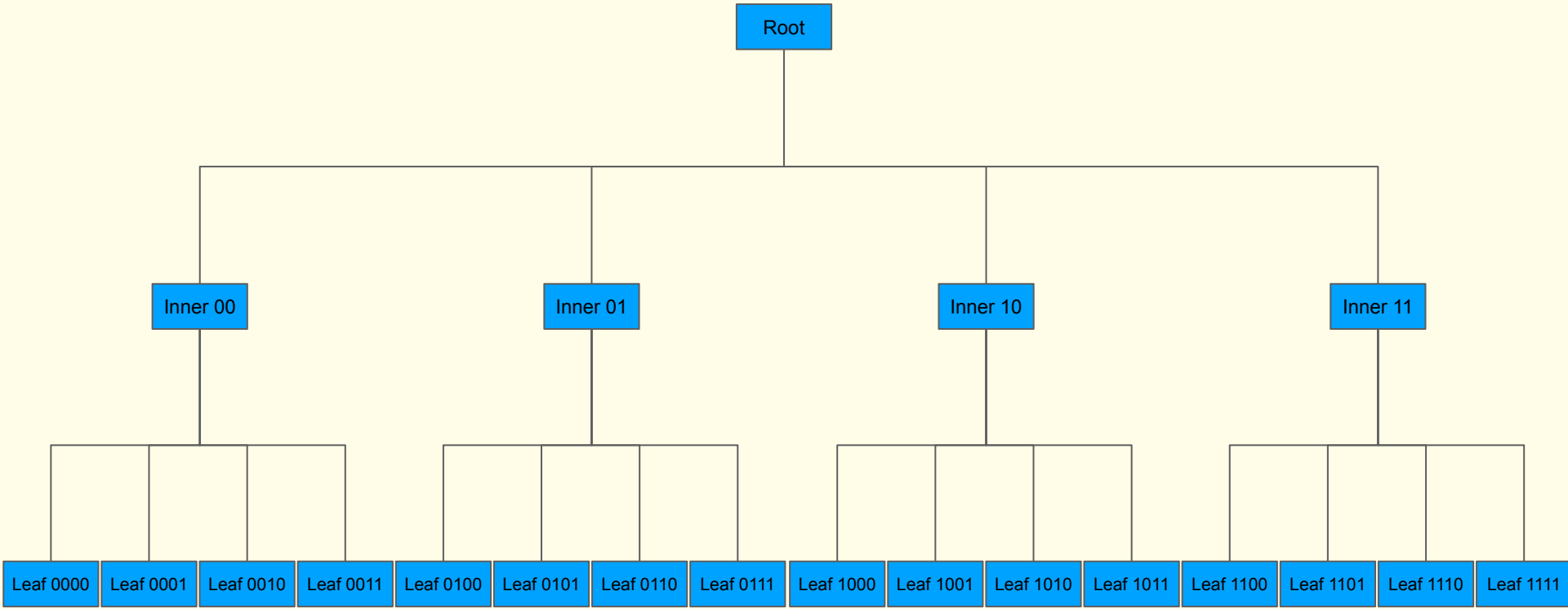
Ack: Slide from Dankrad's presentation

Merkle proof



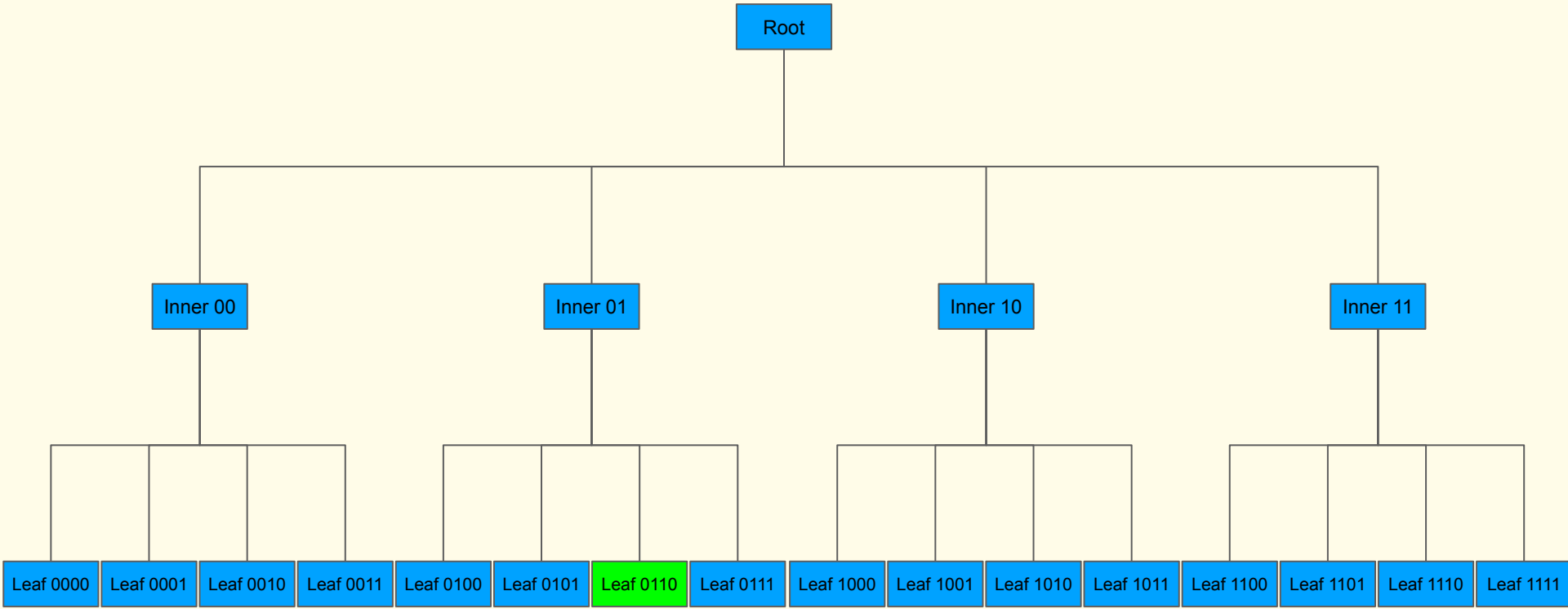
Ack: Slide from Dankrad's presentation

Width-4 Merkle tree



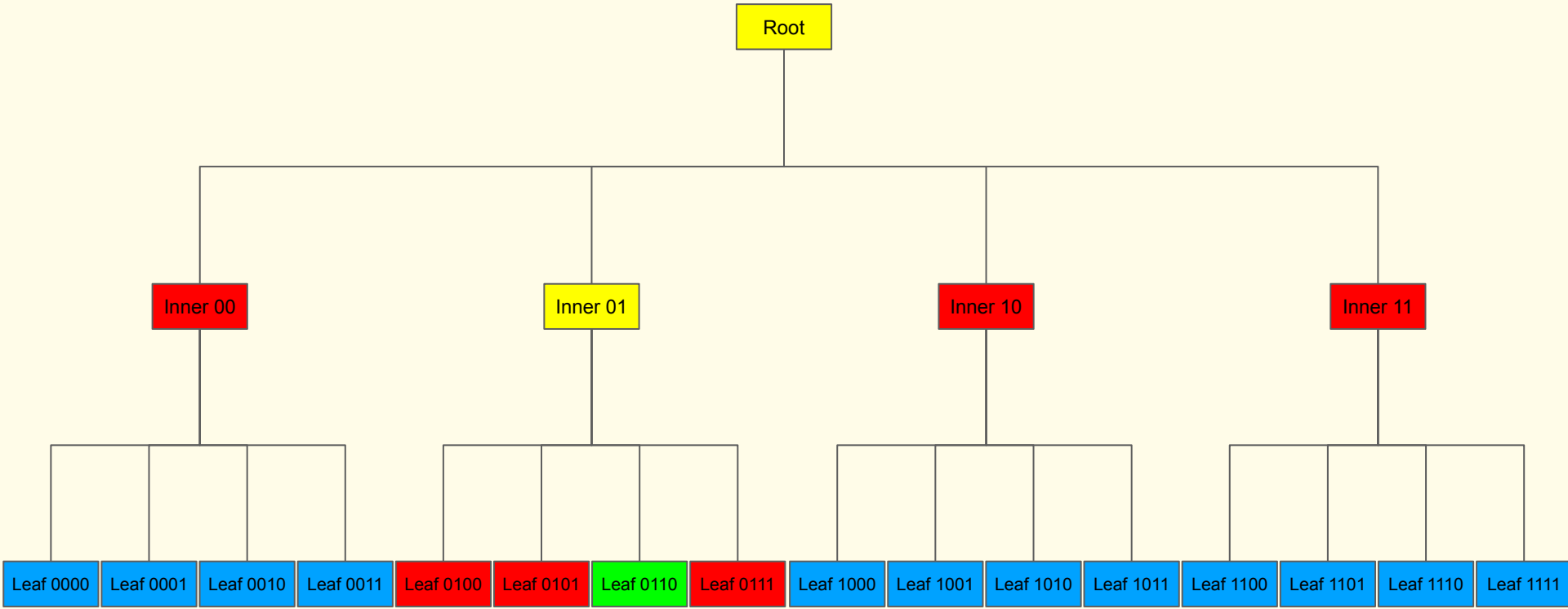
Ack: Slide from Dankrad's presentation

Width-4 Merkle proof



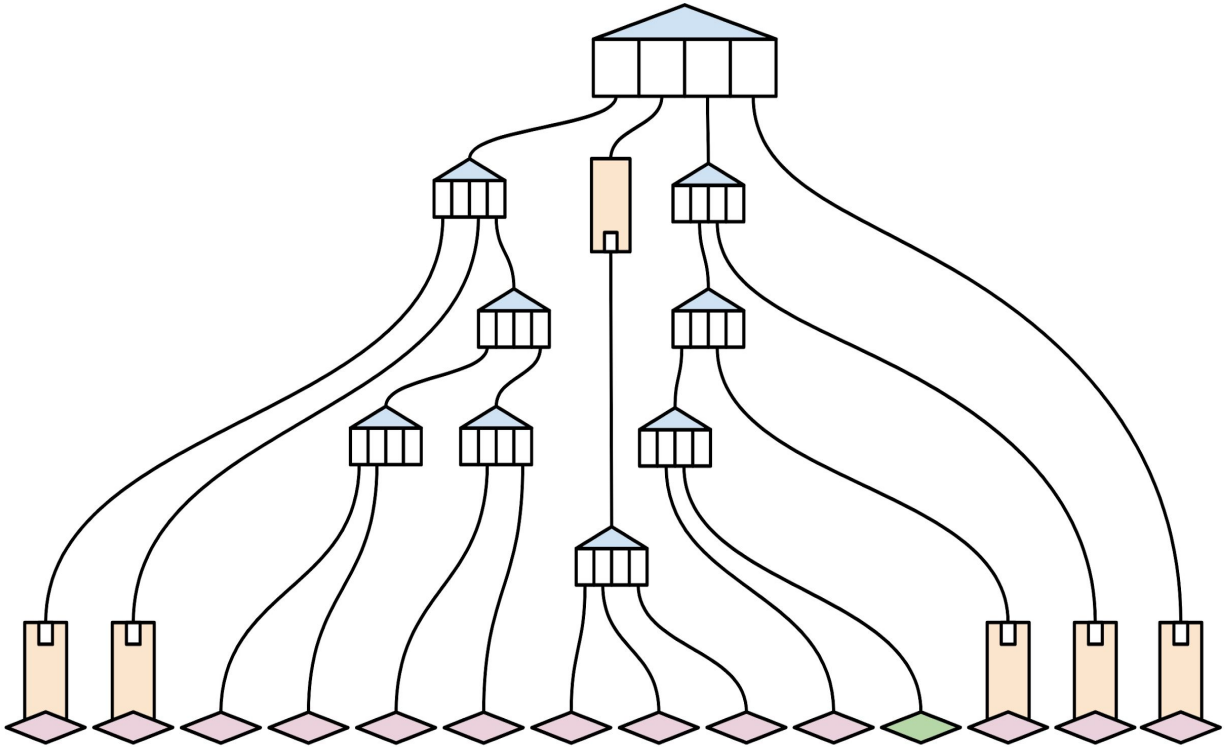
Ack: Slide from Dankrad's presentation

Width-4 Merkle proof



Ack: Slide from Dankrad's presentation

Actual MPT with branch, extension and leaf nodes



So how good are they really?

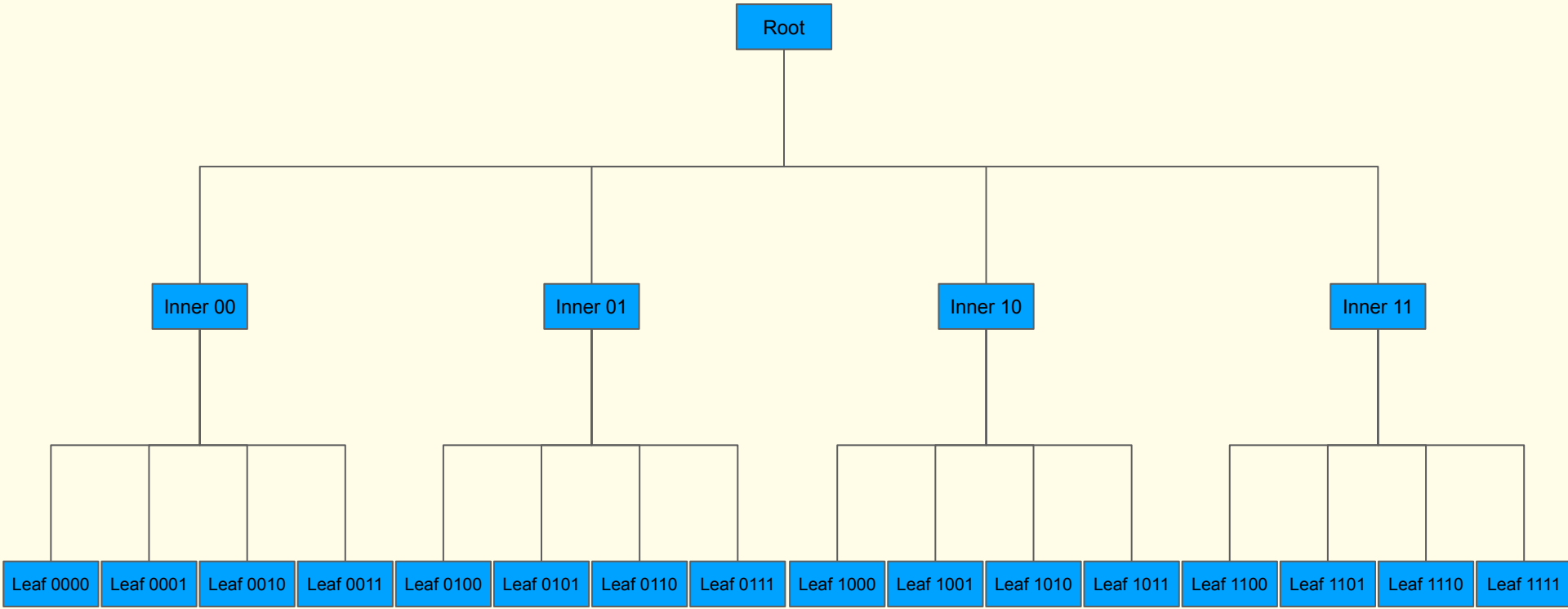
- Using hexary Merkle tree: 3 kB per witness = 47 MB
- Using binary Merkle tree: 0.5 kB/witness = 8 MB
- Using width 256 verkle tree, 32 byte group: 96 byte/witness = 1.5 MB

Ack: Slide from Dankrad's presentation

Verkle Tries

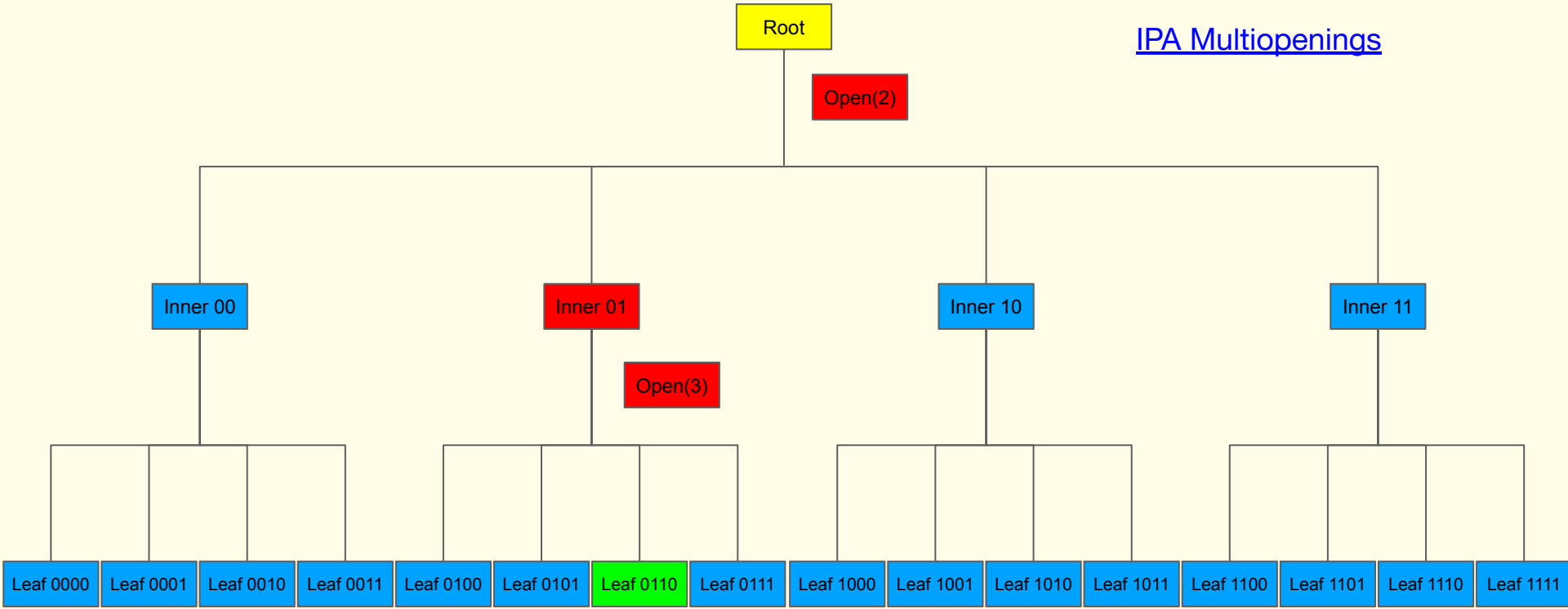
Proposed Technology

Width-4 Verkle tree



Ack: Slide from Dankrad's presentation

Width-4 Verkle proof

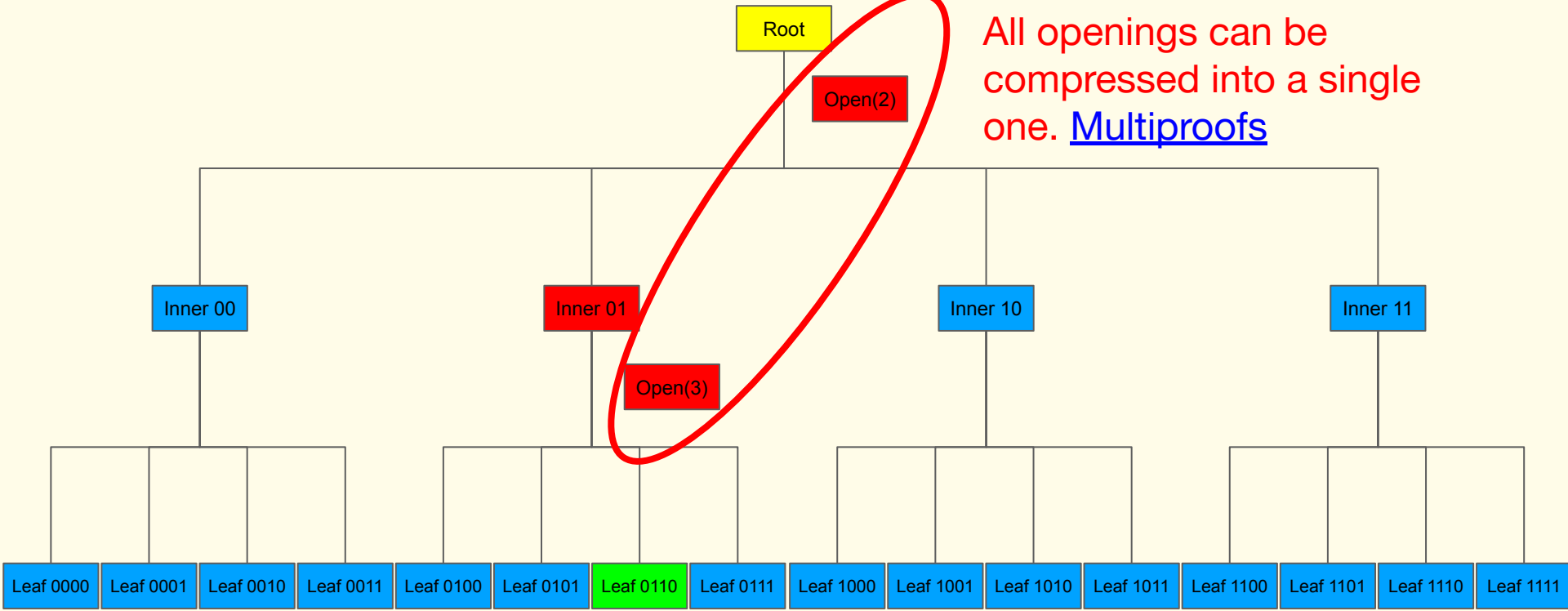


IPA Multiopenings

Ack: Slide from Dankrad's presentation

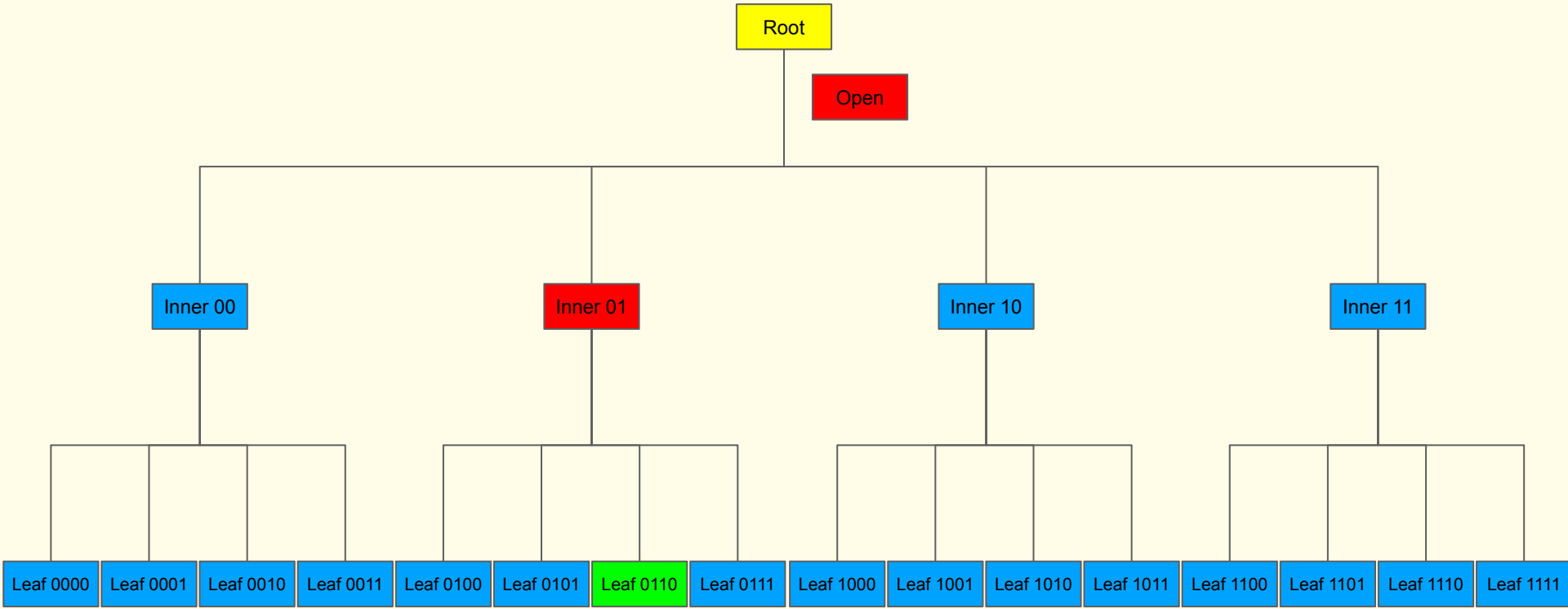
Width-4 Verkle proof

For additive commitments: All openings can be compressed into a single one. Multiproofs



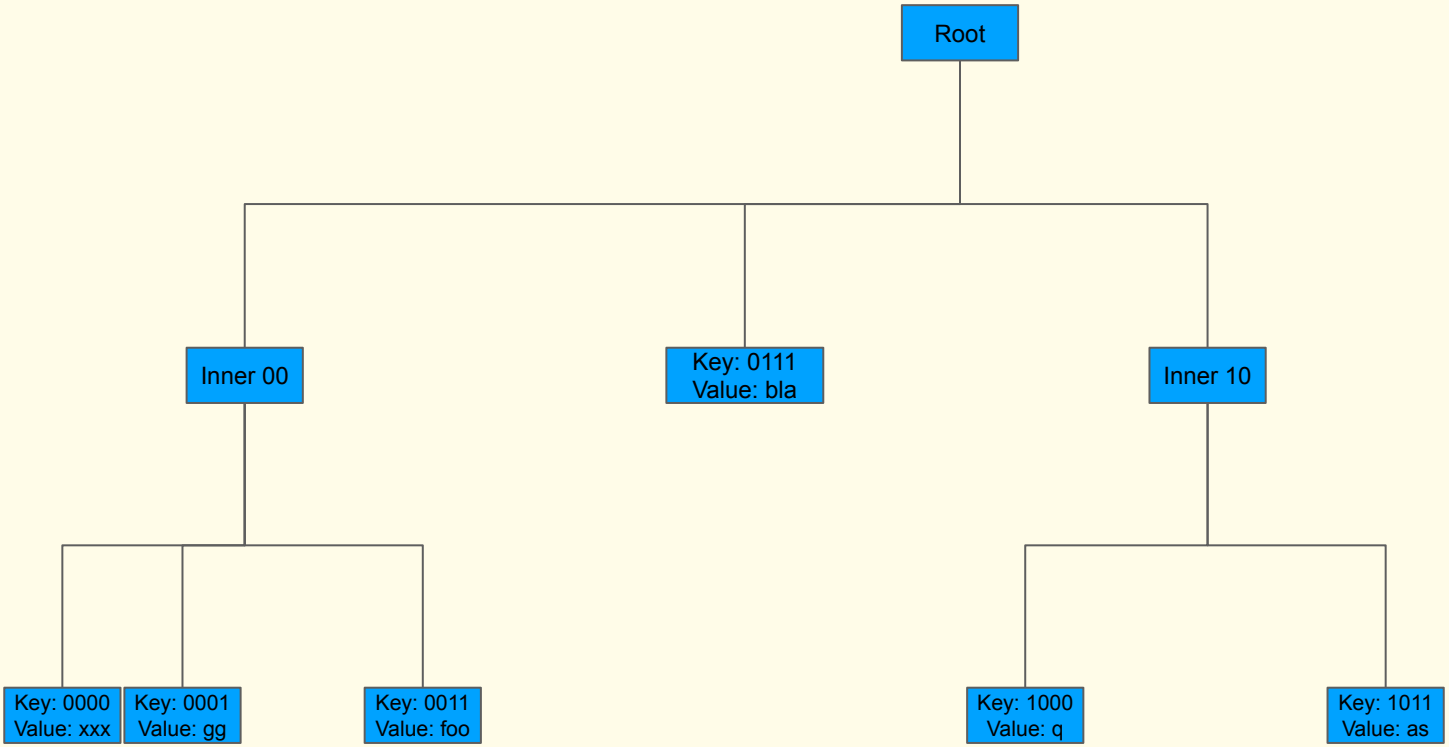
Ack: Slide from Dankrad's presentation

Width-4 Verkle proof



Ack: Slide from Dankrad's presentation

Width-4 Verkle trie



Ack: Slide from Dankrad's presentation

Pedersen Commitments

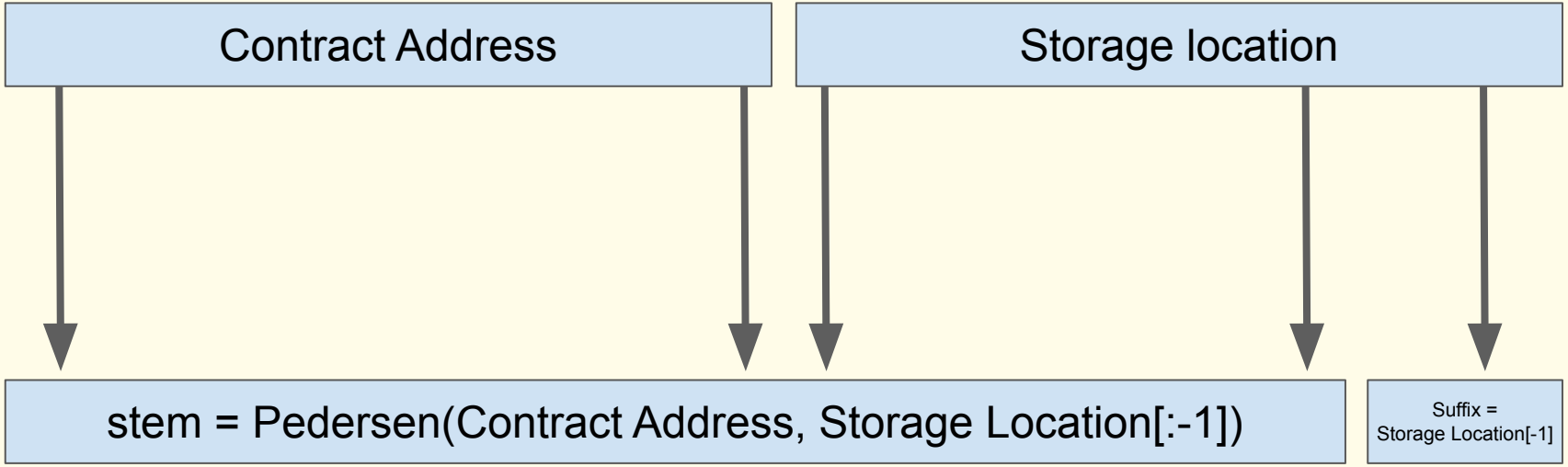
$$C = a_0 g_0 + a_1 g_1 + a_2 g_2 + \ldots + a_{n-1} g_{n-1}$$

$$C + D = (a_0 + b_0) g_0 + (a_1 + b_1) g_1 + (a_1 + b_1) g_2 + \ldots + (a_{n-1} + b_{n-1}) g_{n-1}$$

Steps

Given d points $(\omega^0, y_0), \ldots, (\omega^{d-1}, y_{d-1})$, there is always a unique polynomial f of degree $< d$ that assumes all these points, i.e. $f(\omega^i) = y_i$ for all $0 \leq i < d$,

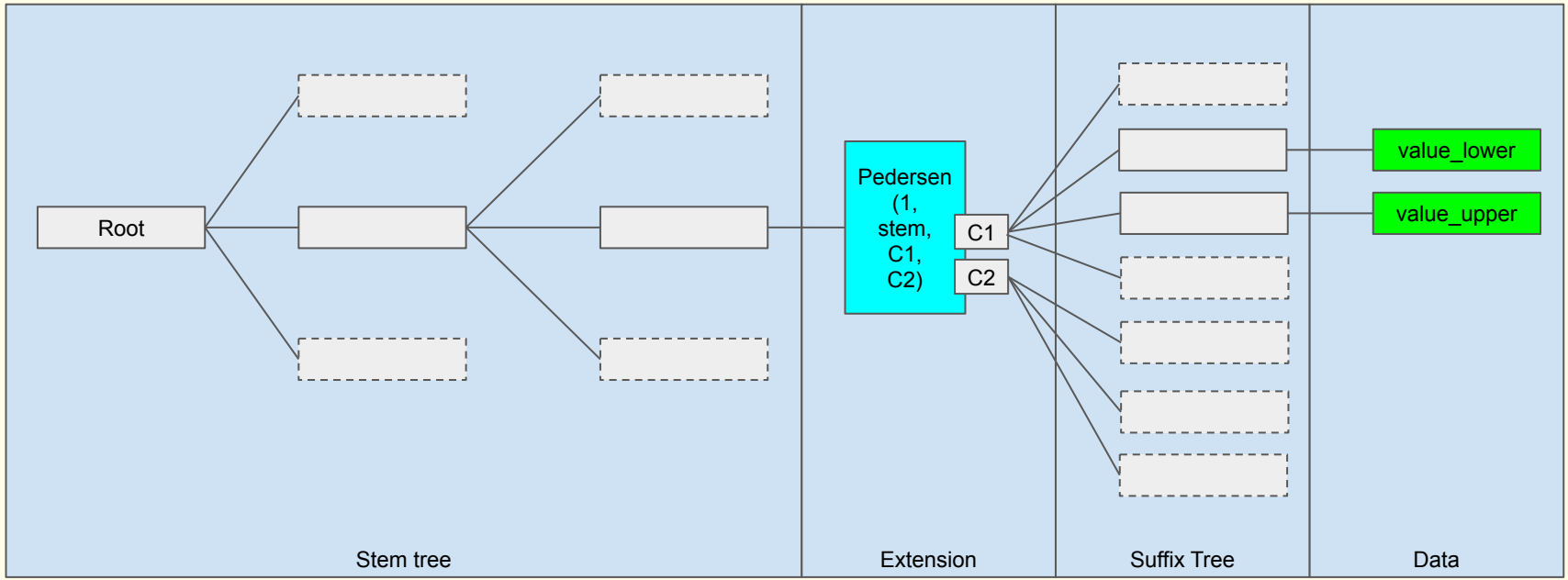
Key structure



Leaves stem the same for close storage locations (differ only in last byte)

Ack: Slide from Dankrad's presentation

Tree structure



Details: https://notes.ethereum.org/@vbuterin/verkle_tree_eip

Ack: Slide from Dankrad's presentation

Why not a single vector commitment, Why tree?

Reason:

Need to deal with all elements of the state.

Prover costs are not manageable

Tree is a tradeoff between verifier and prover costs

Verkle proofs also give a way to compute updated root

Resources

- Gas cost changes enabling Verkle tries
- Pre-EIP specification
- Math documentation
- Dankrad Feist, EF, Python PoC, Video

Conclusion

Summary and conclusion

Critical. Statelessness is critical for Ethereum to overcome the increasing burden of unbounded state growth and to maintain and increase decentralisation. Validation on mobile phones.

Witnesses A Stateless Ethereum client needs witnesses to execute the transactions in a block and to validate

Verkle Tries is the only known feasible solution for making witnesses viable.

- ~30x reduction compared to Hexary MPT
- Does not burden the prover / block producer as compared to direct polynomial commitments