How to EIP-4788

ADVANTAGES AND LIMITATIONS

LIDO

Dmitry Ch

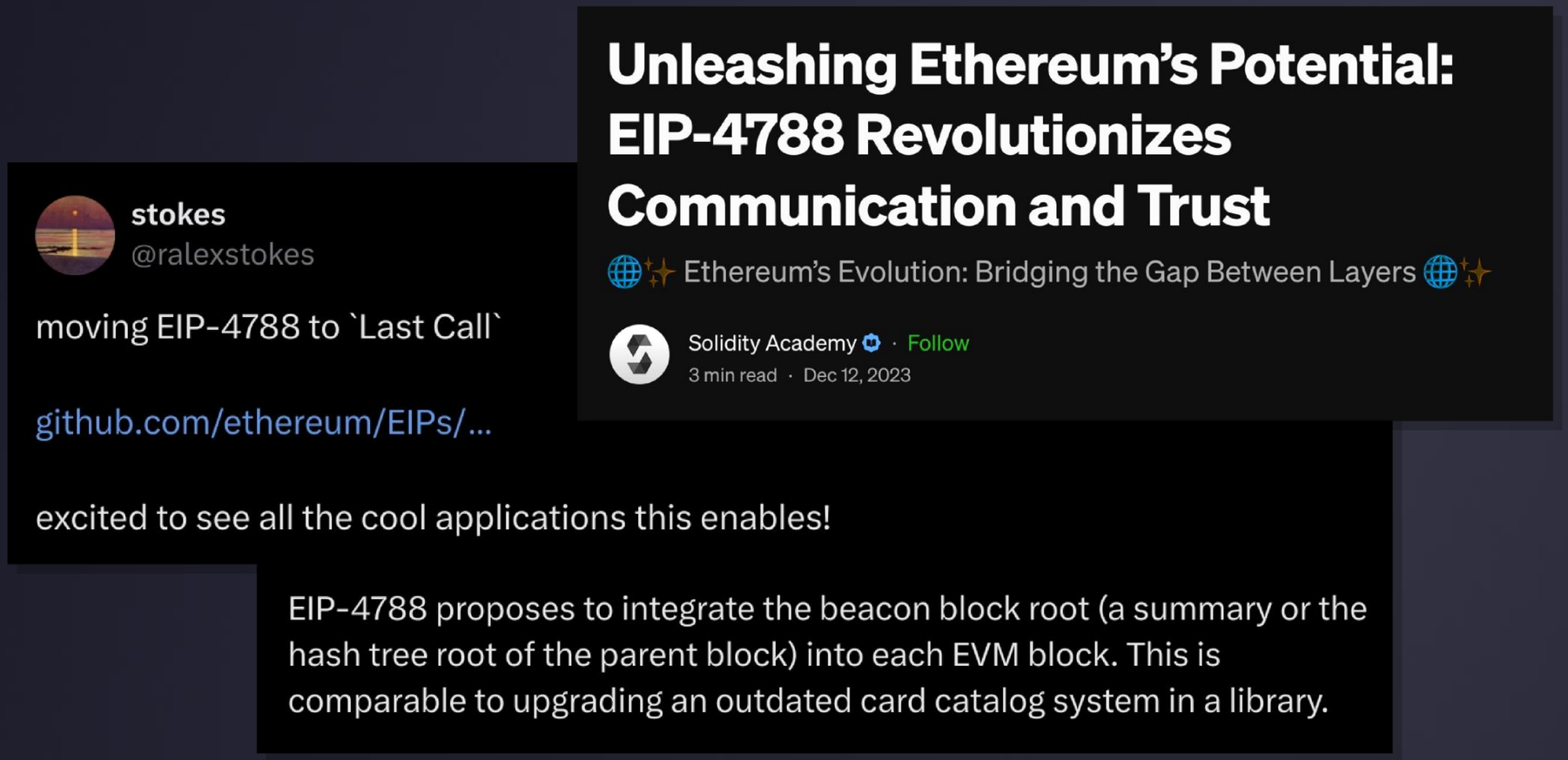
Contributing to CSM Team

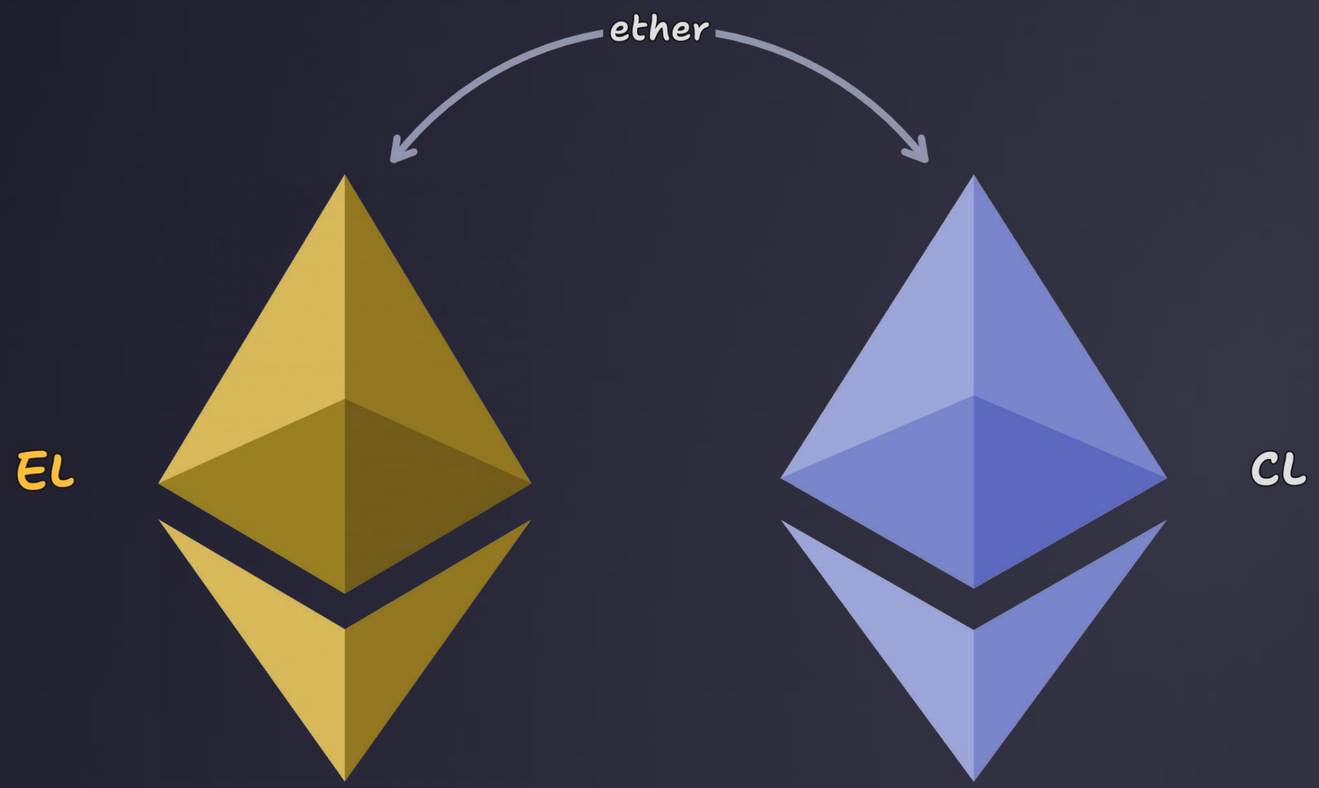
Last Call | Standards Track: Core

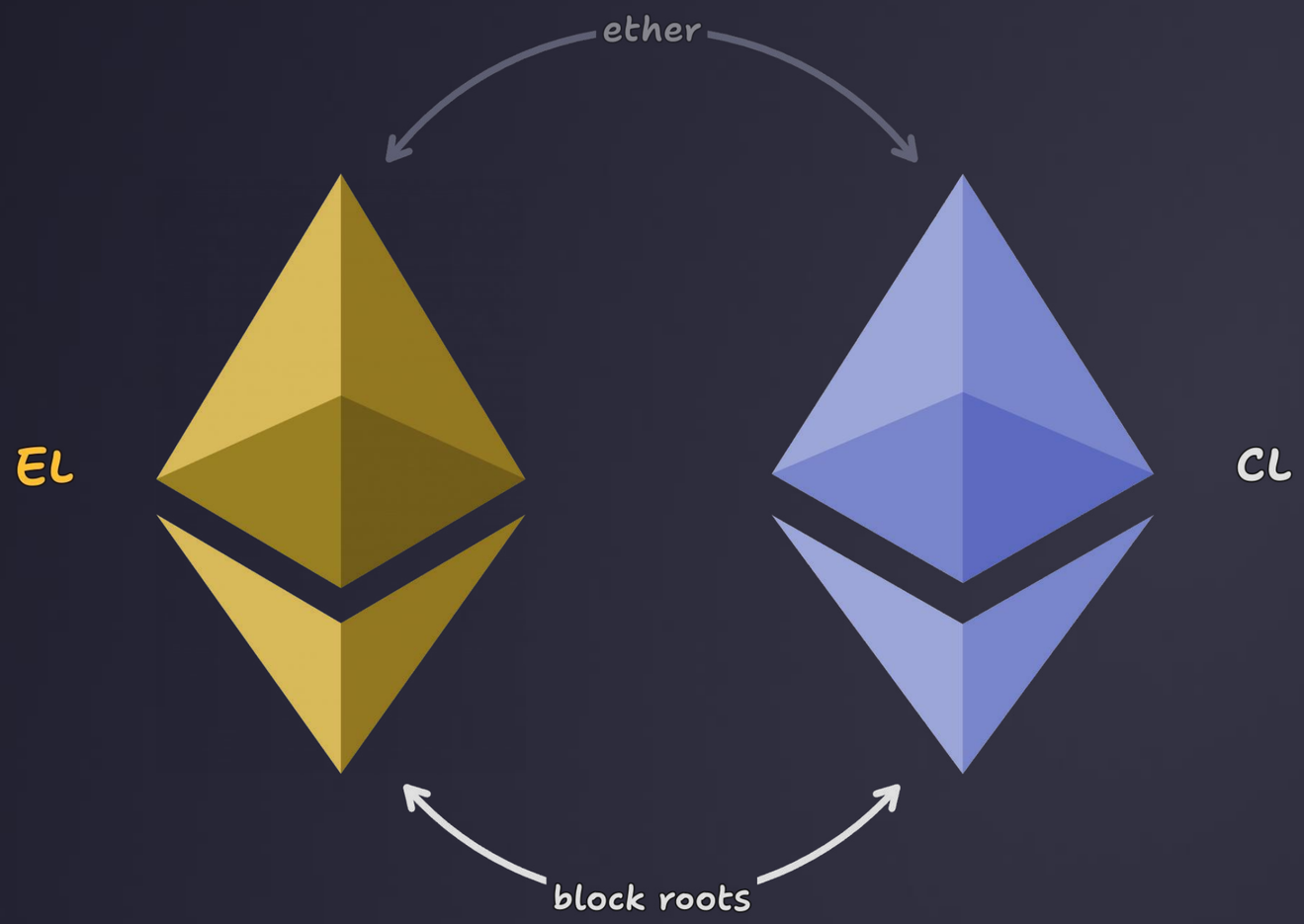
EIP-4788: Beacon block root in the EVM

Expose beacon chain roots in the EVM

Authors	Alex Stokes (@ralexstokes), Ansgar Dietrichs (@adietrichs), Danny Ryan (@djrtwo), Martin Holst Swende (@holiman), lightclient (@lightclient)
Created	2022-02-10
Last Call Deadline	2024-02-12
Requires	EIP-1559

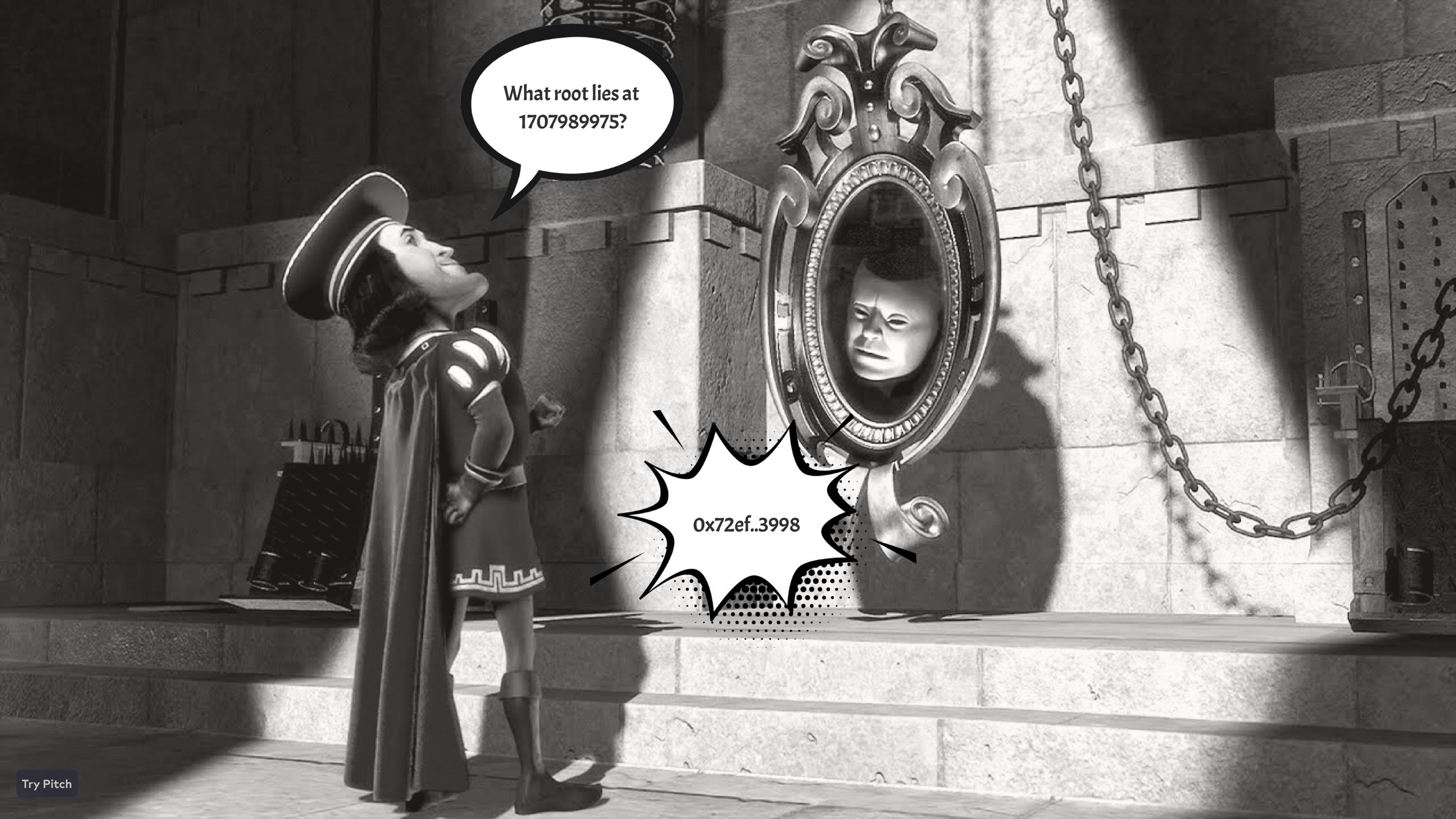

stokes
@ralexstokes
moving EIP-4788 to `Last Call`
github.com/ethereum/EIPs/...
excited to see all the cool applications this enables!
Unleashing Ethereum's Potential: EIP-4788 Revolutionizes Communication and Trust
🌐✨ Ethereum's Evolution: Bridging the Gap Between Layers 🌐✨
Solidity Academy · Follow
3 min read · Dec 12, 2023
EIP-4788 proposes to integrate the beacon block root (a summary or the hash tree root of the parent block) into each EVM block. This is comparable to upgrading an outdated card catalog system in a library.



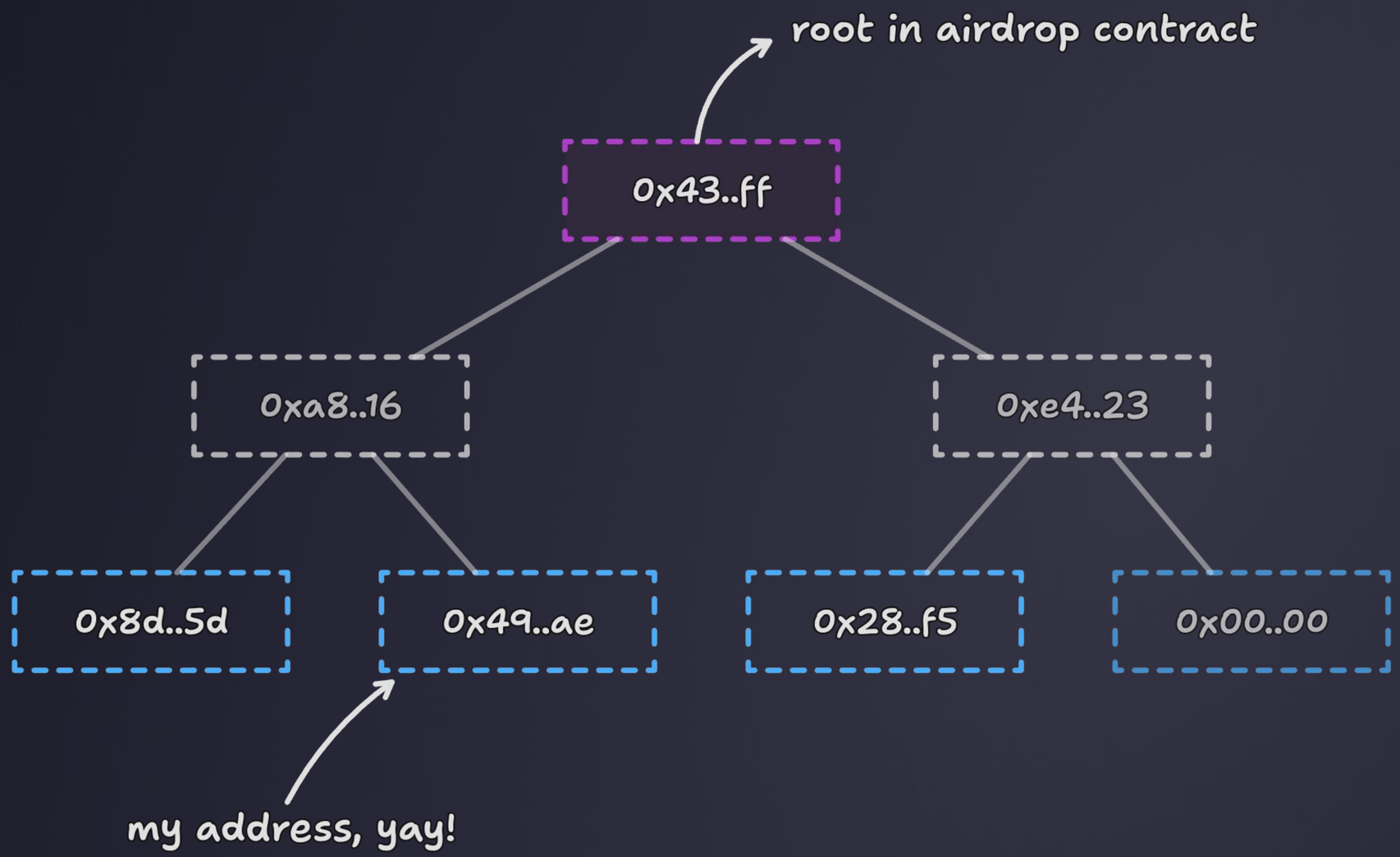


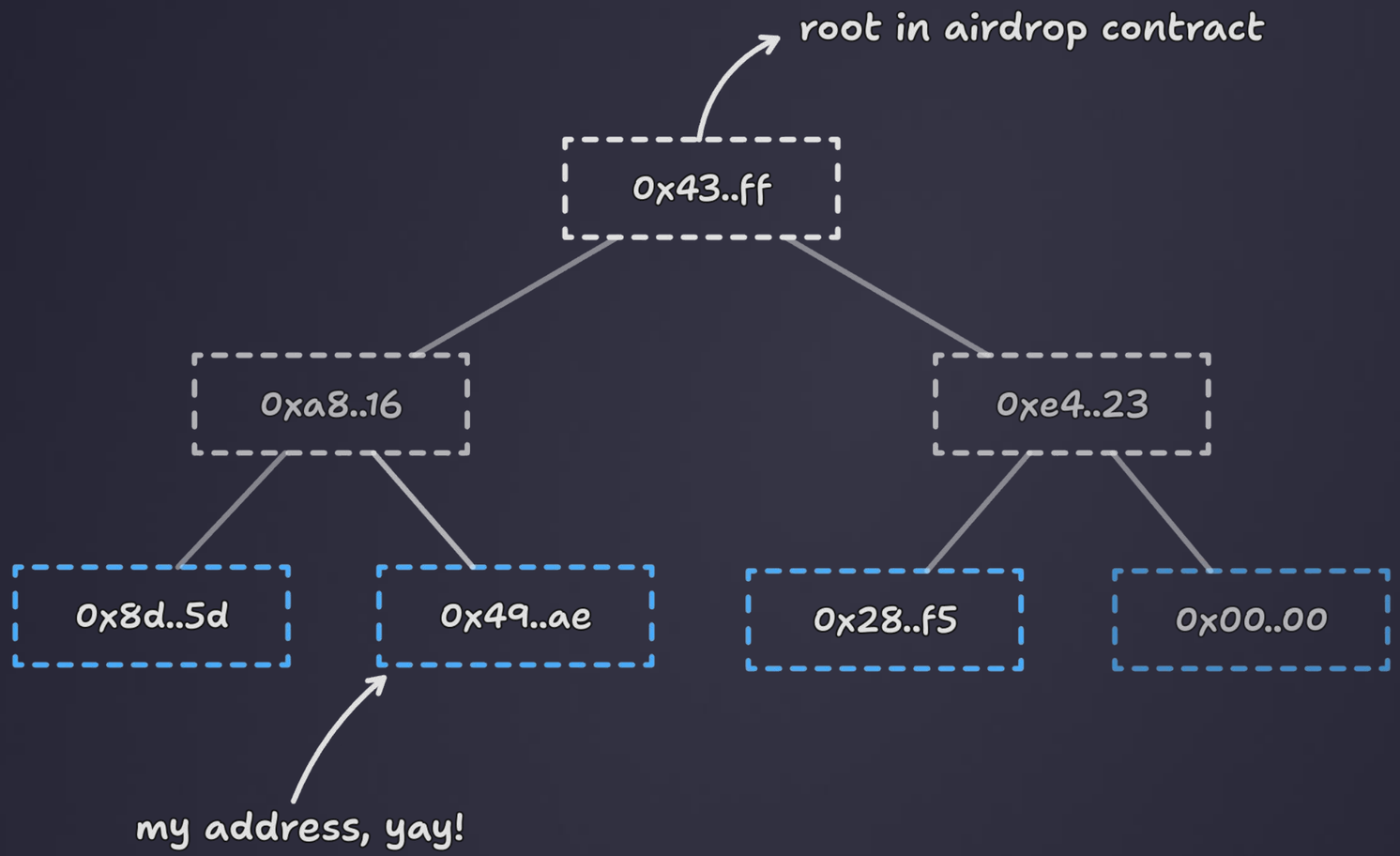
BLOCK ROOTS CONTRACT AT THE ADDRESS

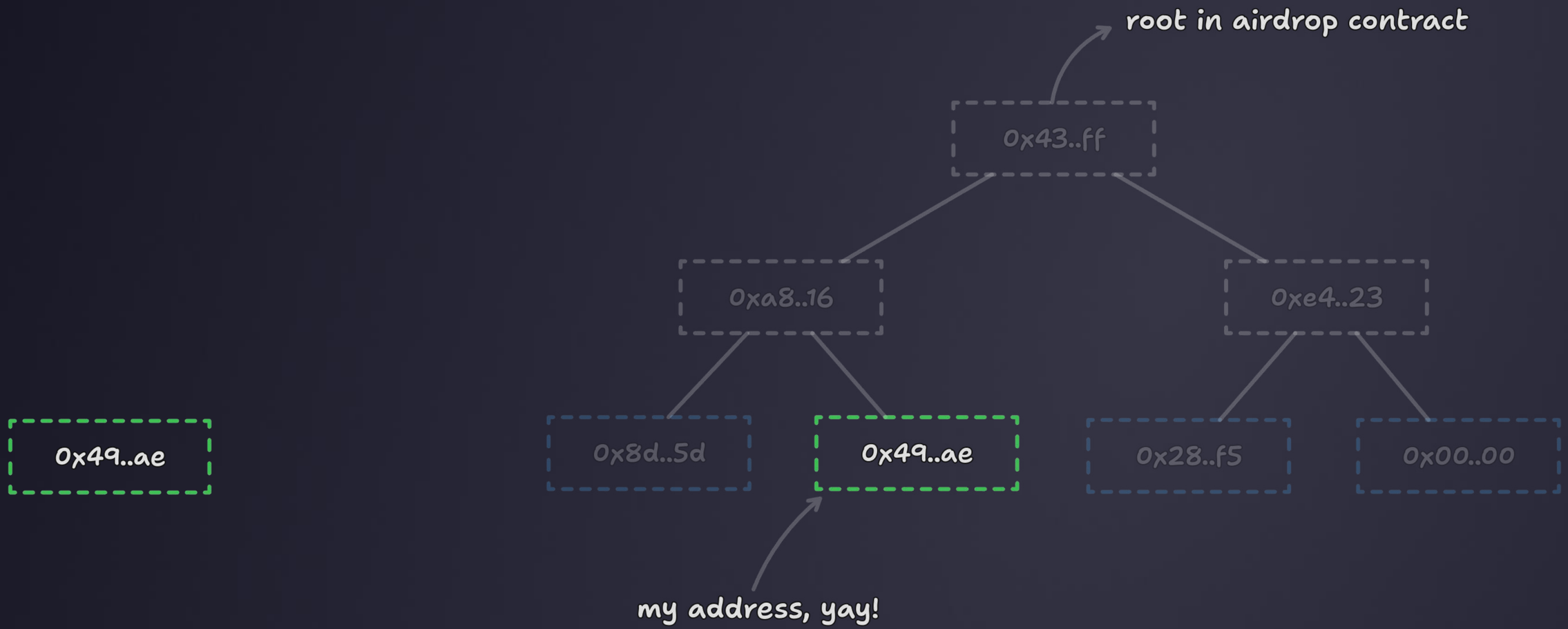
0x000F3df6D732807Ef1319fB7B8bB8522d0Beac02

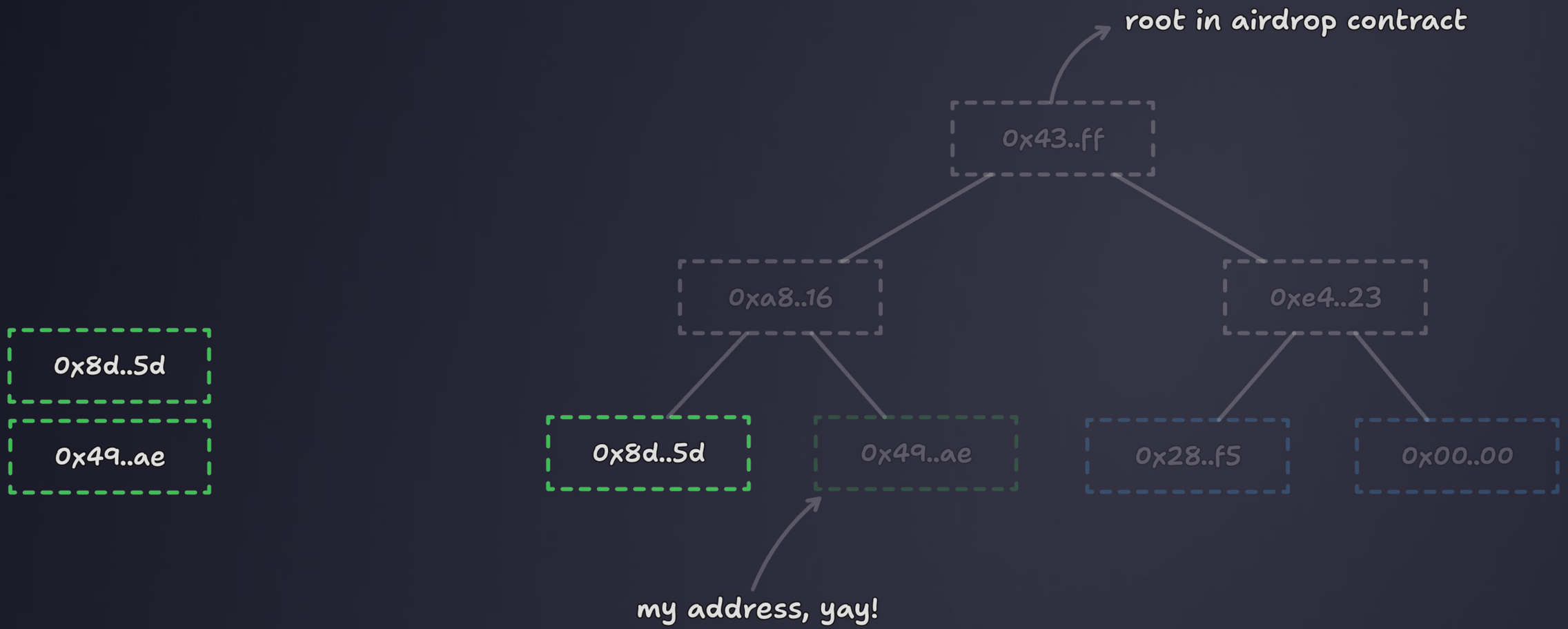


A BLOCK ROOT CAN BE USED TO BUILD AN
INCLUSION PROOF OF BEACON BLOCK DATA


root in airdrop contract
0x43..ff
0xa8..16
0xe4..23
0x8d..5d
0x49..ae
0x28..f5
0x00..00
my address, yay!


root in airdrop contract
0x43..ff
0xa8..16
0xe4..23
0x8d..5d
0x49..ae
0x28..f5
0x00..00
my address, yay!


root in airdrop contract
0x43..ff
0xa8..16
0xe4..23
0x49..ae
0x8d..5d
0x49..ae
0x28..f5
0x00..00
my address, yay!


root in airdrop contract
0x43..ff
0xa8..16
0xe4..23
0x8d..5d
0x49..ae
0x28..f5
0x00..00
0x8d..5d
0x49..ae
my address, yay!


root in airdrop contract
0x43..ff
0xa8..16
0xe4..23
0x8d..5d
0x49..ae
0x28..f5
0x00..00
0xe4..23
0x8d..5d
0x49..ae
my address, yay!

0xe4..23

0x8d..5d

0x49..ae

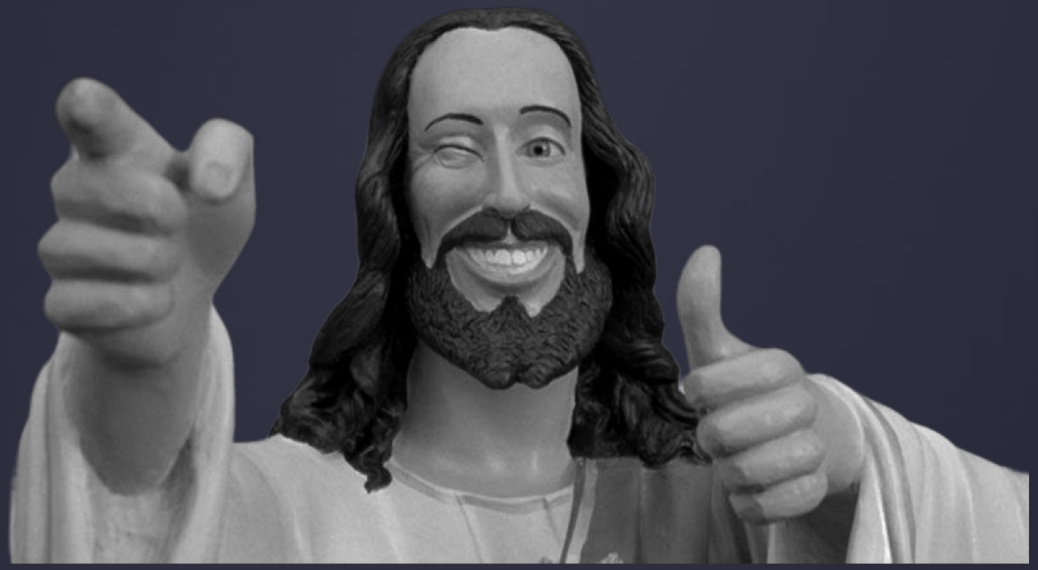
0x43..ff

=

0x43..ff

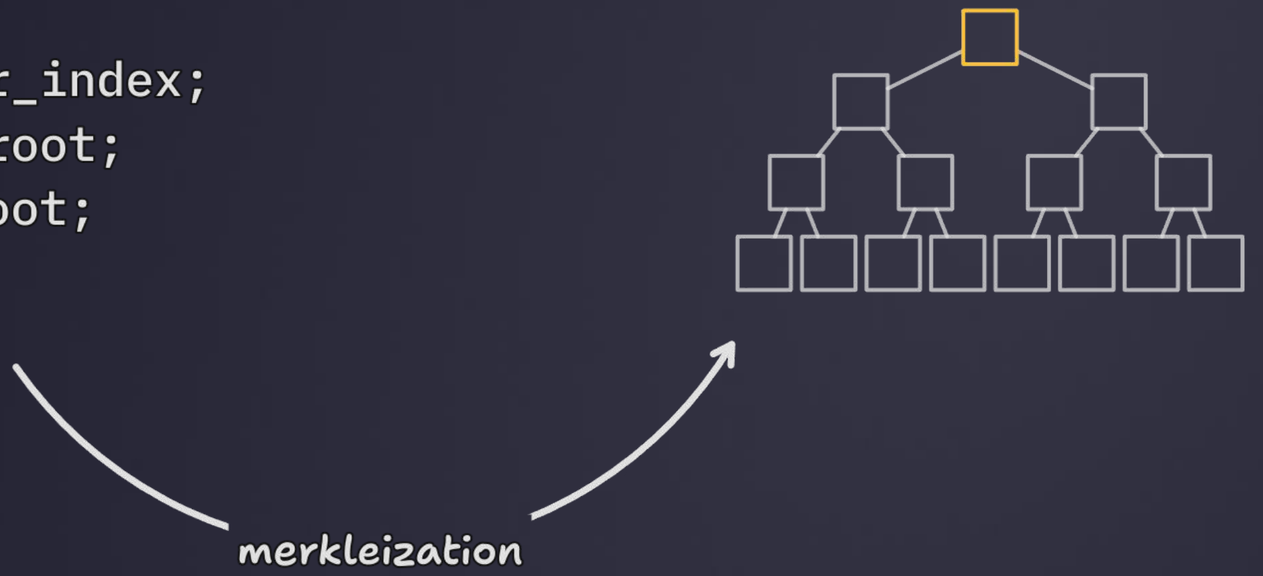
root in airdrop contract

YOU **PROVED** TO THE CONTRACT THAT
YOUR ADDRESS IS **INCLUDED**
IN THE LIST



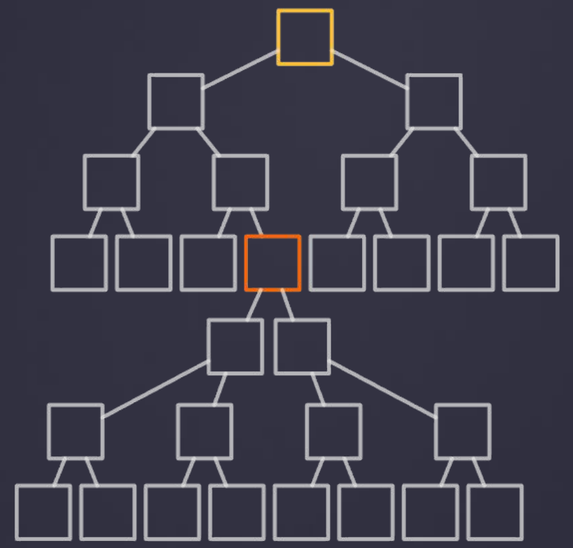
Beacon structures are trees!

```
class BeaconBlock {
    slot;
    proposer_index;
    parent_root;
    state_root;
    body;
}
```



Beacon structures are trees!

```
class BeaconBlock {
    slot;
    proposer_index;
    parent_root;
    state_root;
    body;
}
```

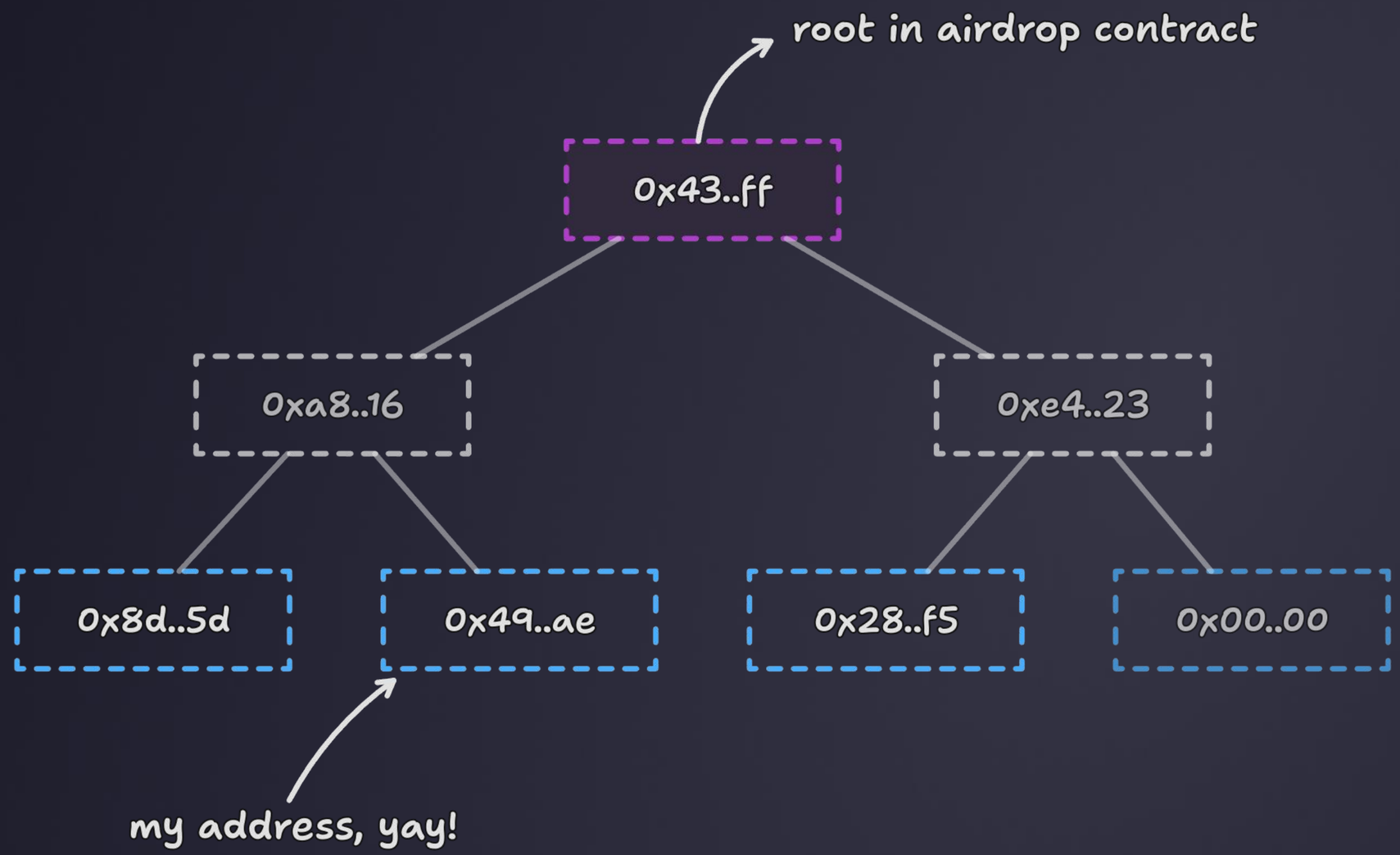


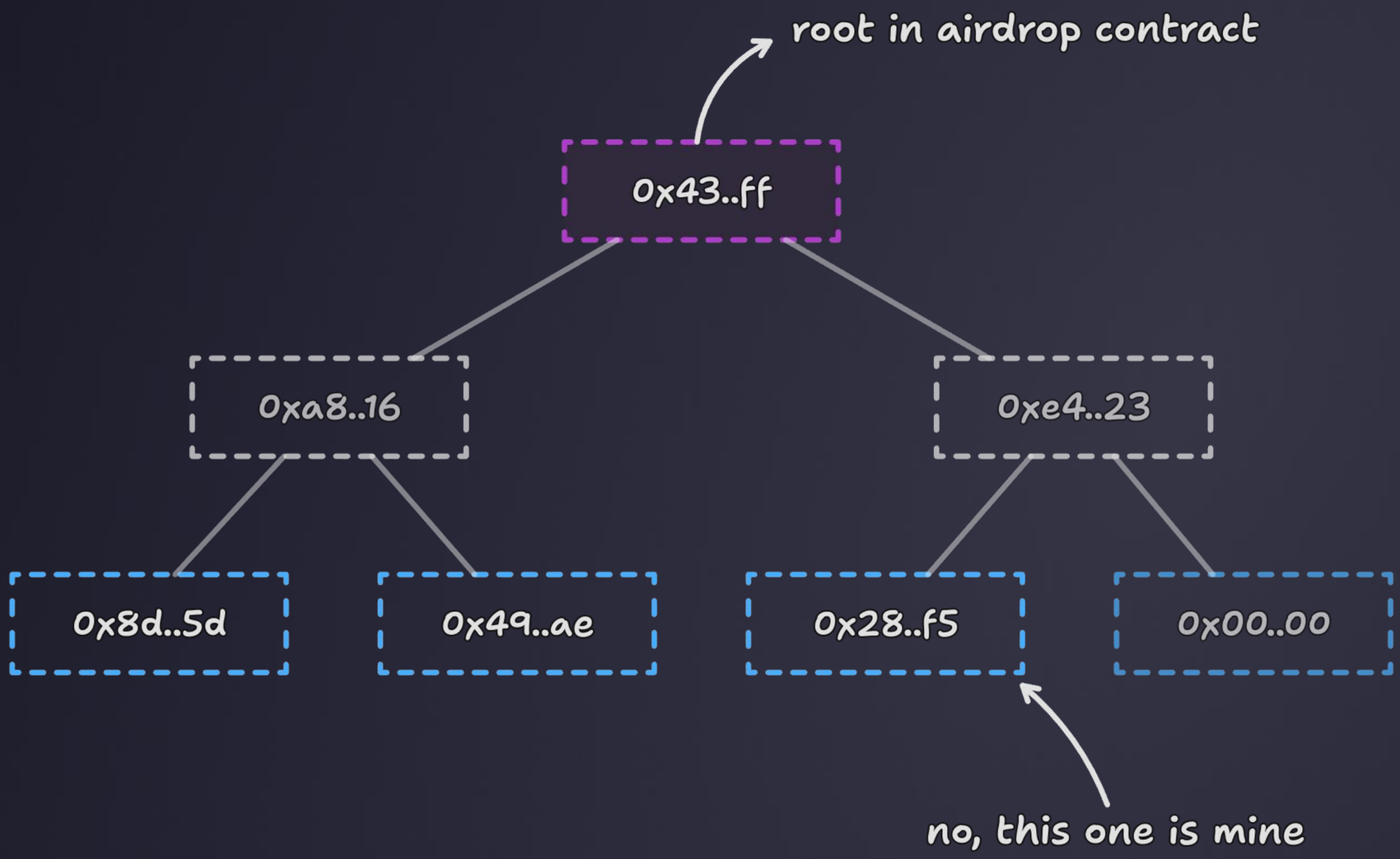

YOU CAN PROVE ANYTHING
ALL I NEED IS A PROOF, RIGHT?
ALL I NEED IS A PROOF, RIGHT?
imgflip.com

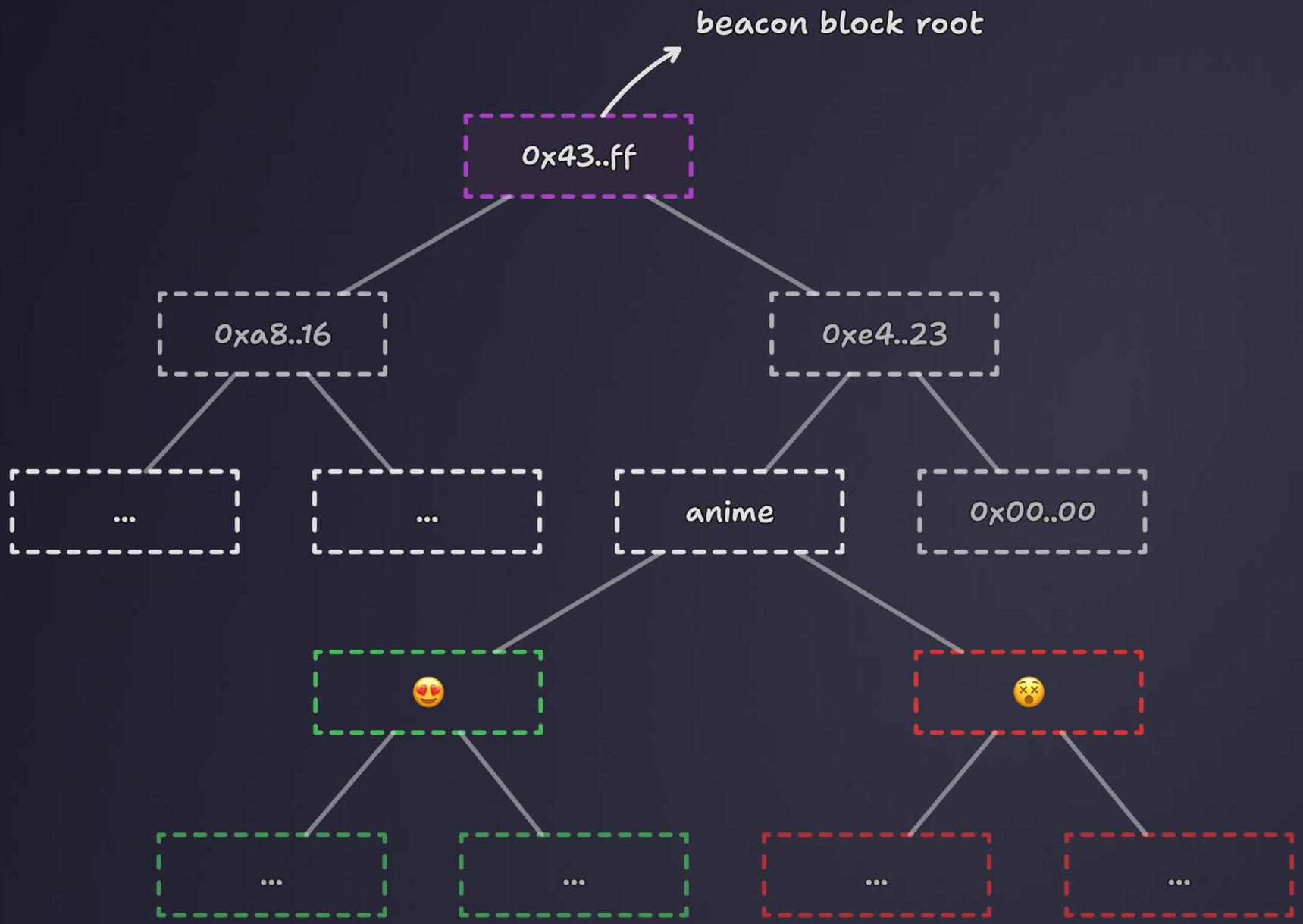
timbeiko.eth ☀️
@TimBeiko

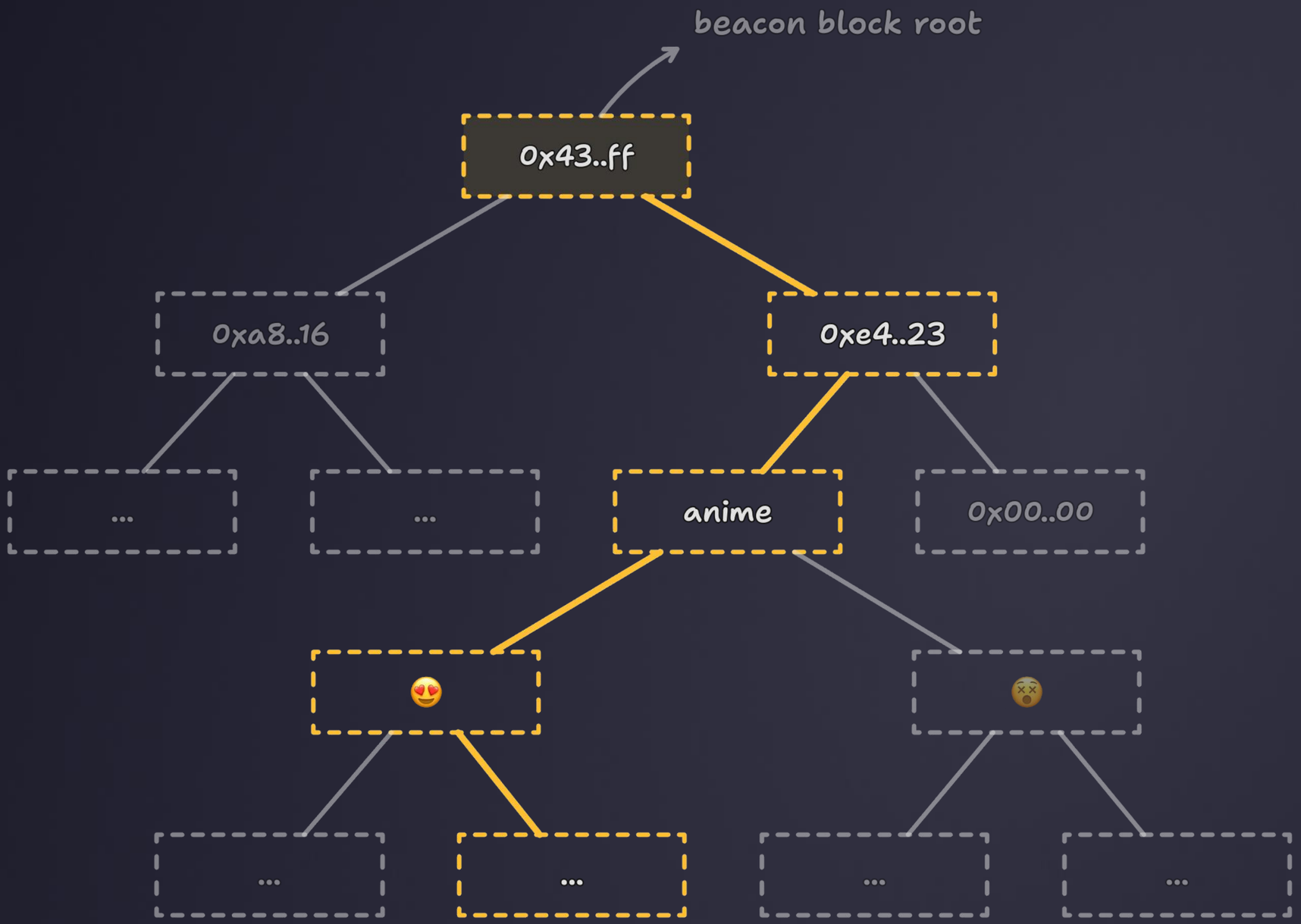
@ethereum @ErigonEth @alexberegszaszi @ralexstokes As the doc states, the first part here is providing access to the CL's state roots on the EL, which is what EIP-4788 proposes. That said, to verify proofs, you would also need access to the CL's Generalized Index

THE **GENERALIZED INDEX** REFERS
TO THE **INDEX OF A NODE**
WITHIN A TREE

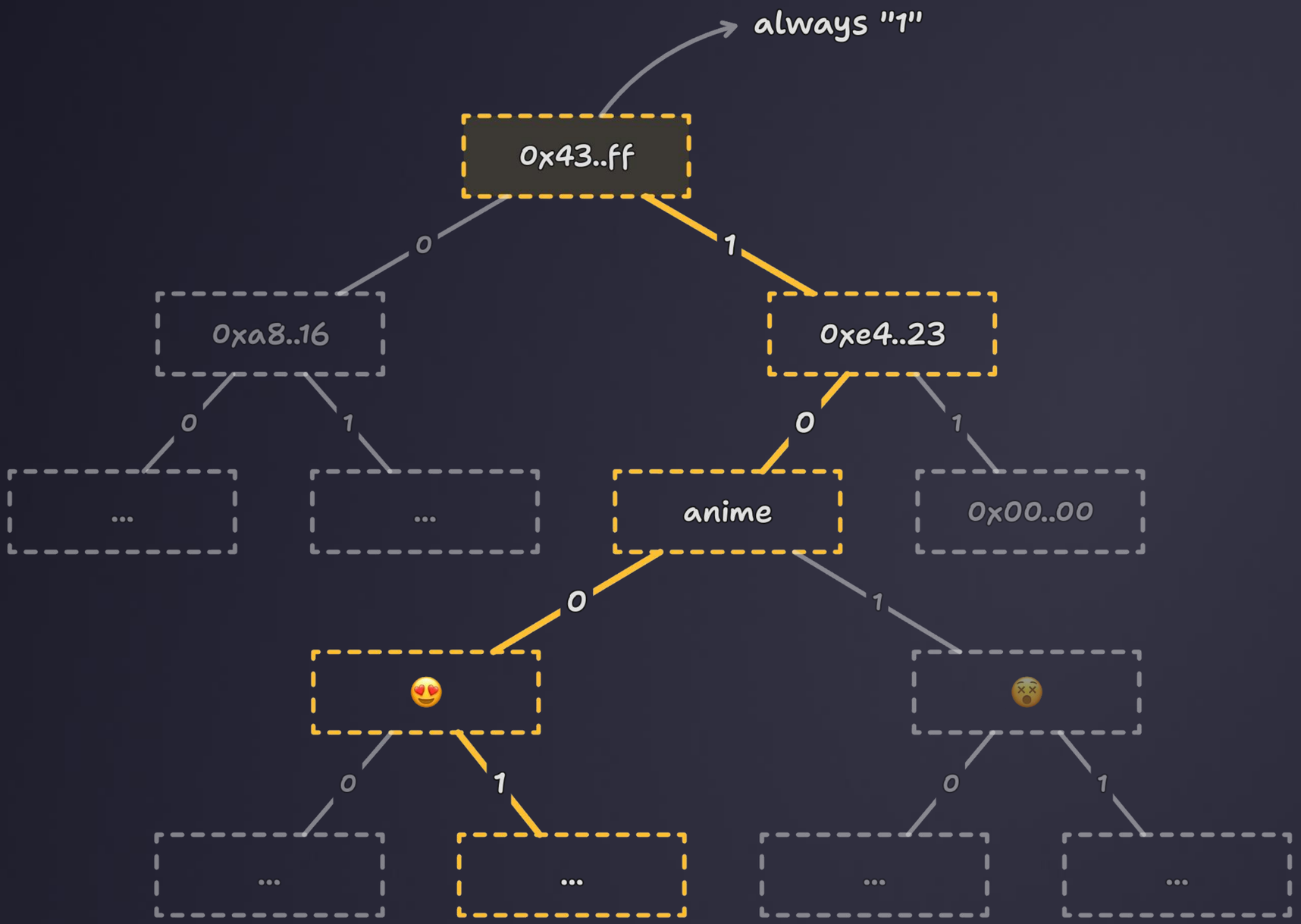

root in airdrop contract
0x43..ff
0xa8..16
0xe4..23
0x8d..5d
0x49..ae
0x28..f5
0x00..00
my address, yay!


root in airdrop contract
0x43..ff
0xa8..16
0xe4..23
0x8d..5d
0x49..ae
0x28..f5
0x00..00
no, this one is mine



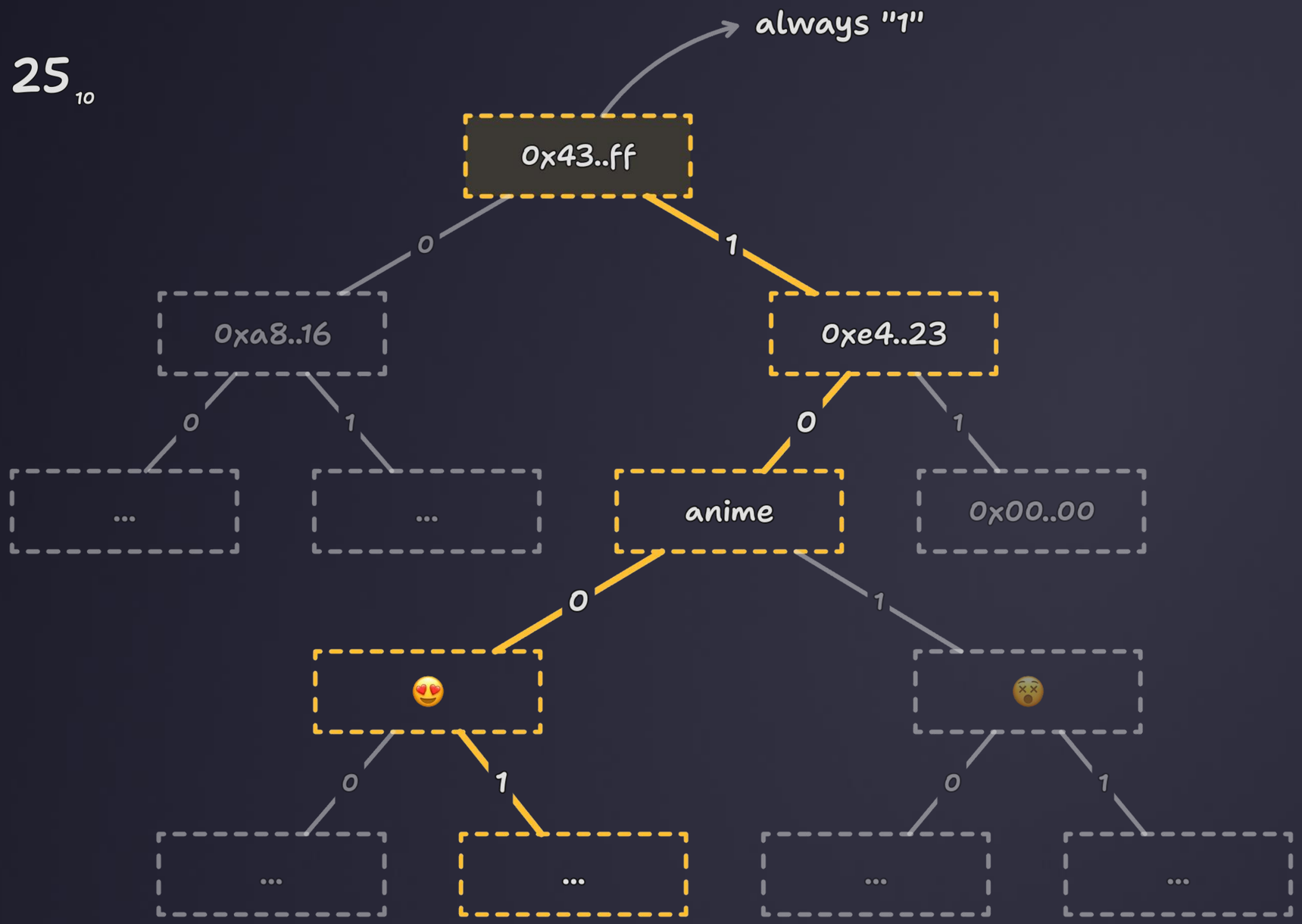


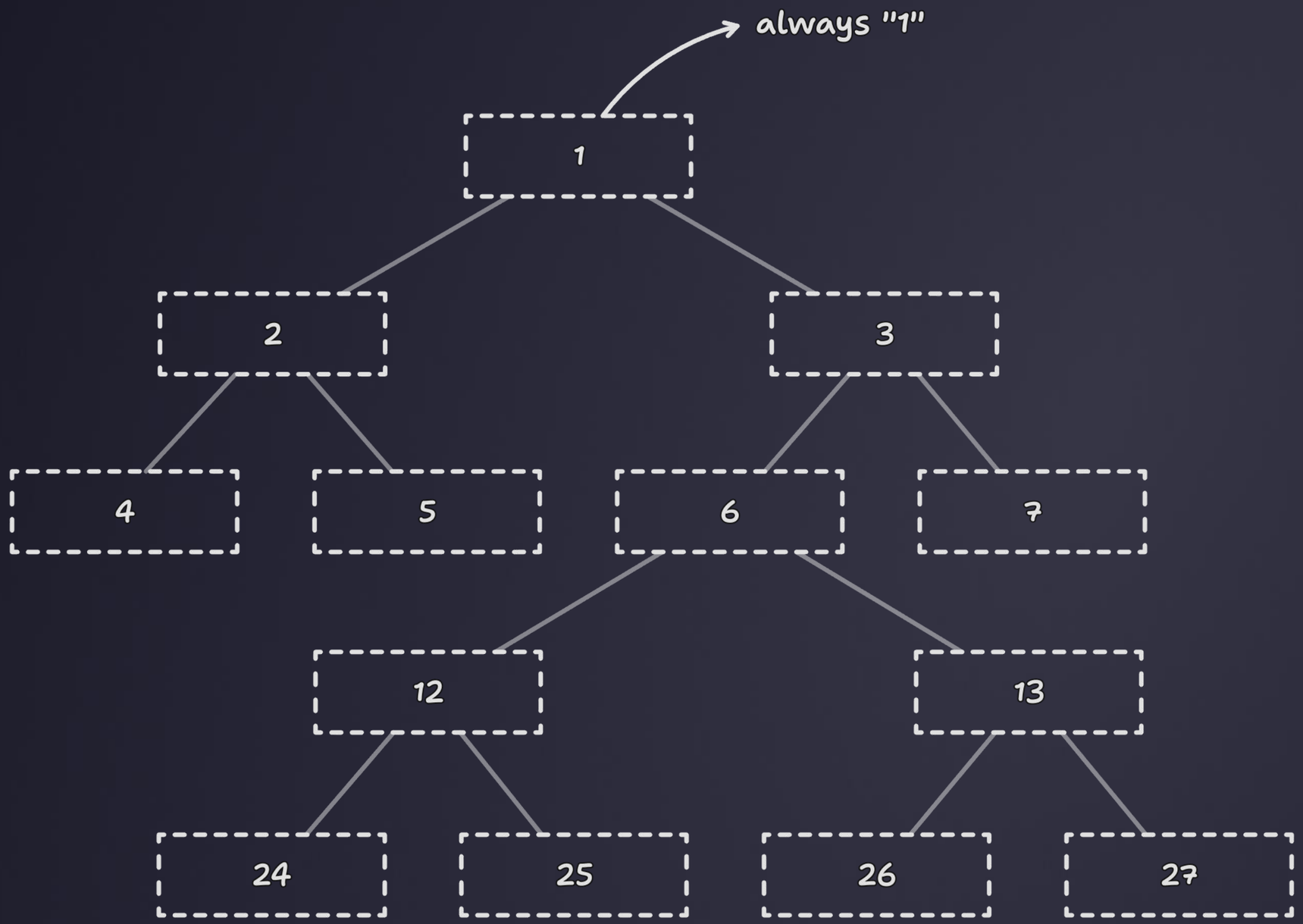
Try Pitch

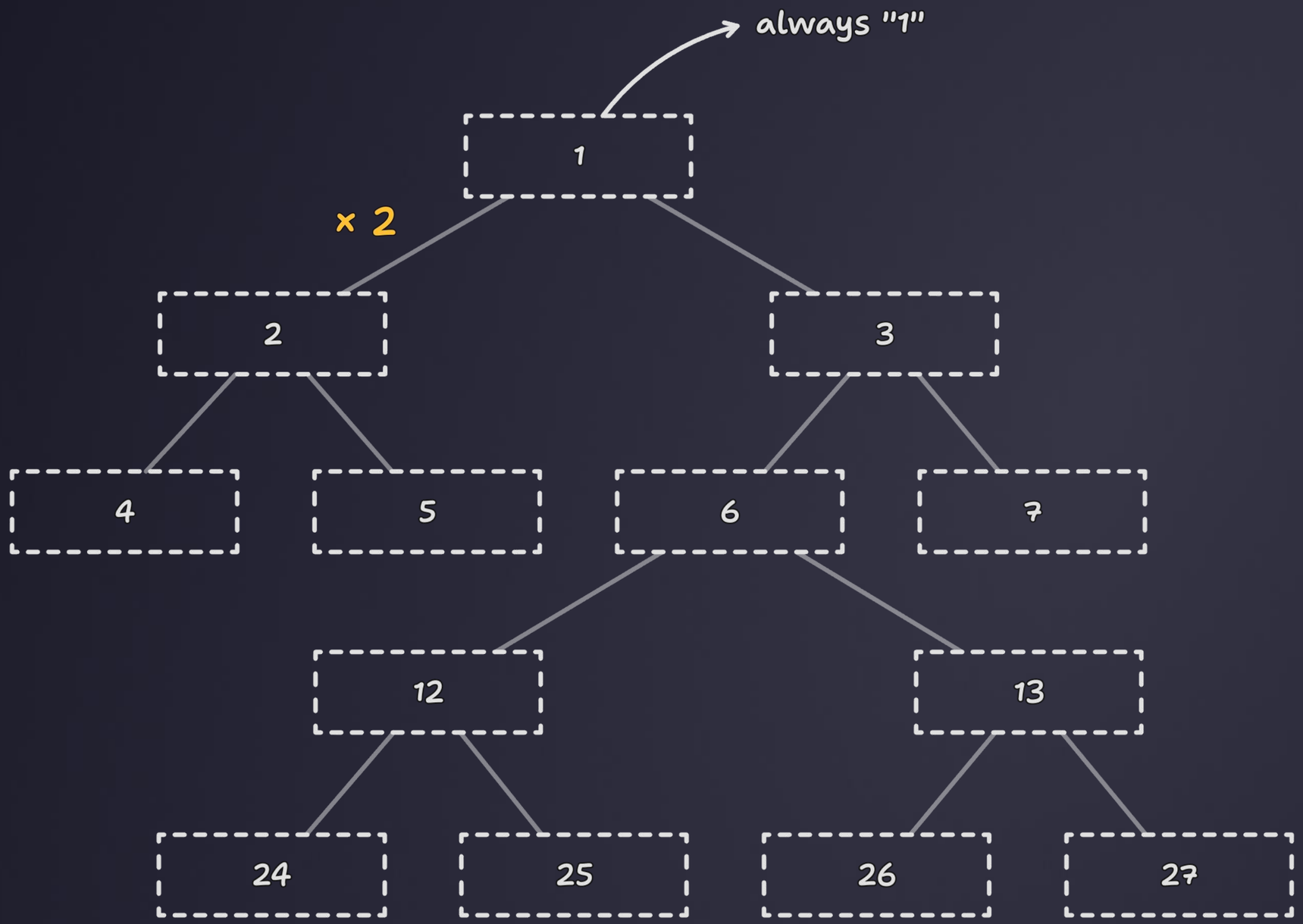


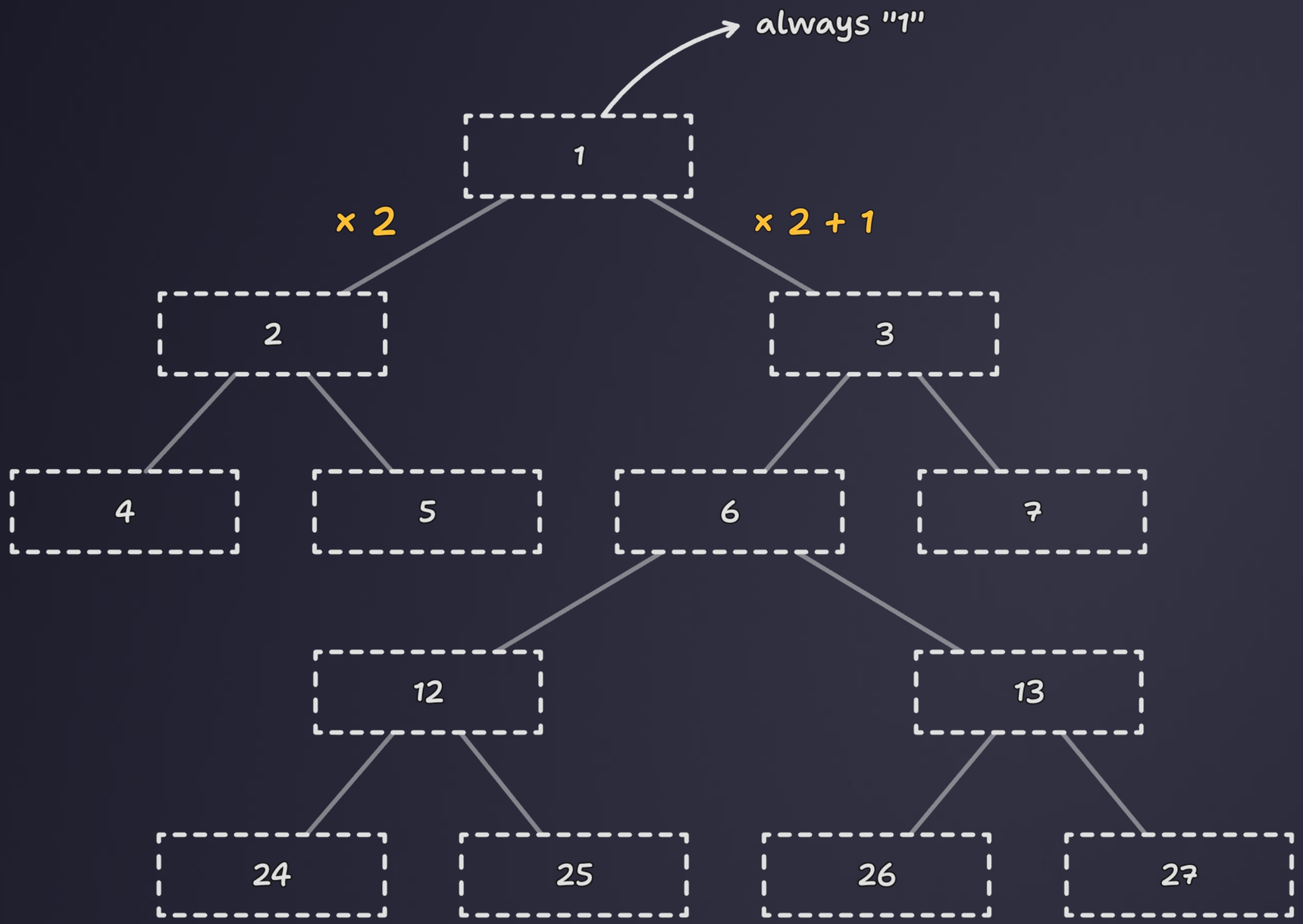
Try Pitch

$11001_2 = 25_{10}$









Applications of EIP-4788

- staking pools
- restaking
- your cool dapp?

EIP-4788 provides a new source of truth

Gas costs

to prove one validator's state < 100k of gas

Gas costs

to prove a state of 300'000 validators

Gas costs

trusted oracle

ZKP solutions

27 hours

IT DOESN'T MAKE SENSE TO STORE
ALL ROOTS ON-CHAIN FOREVER

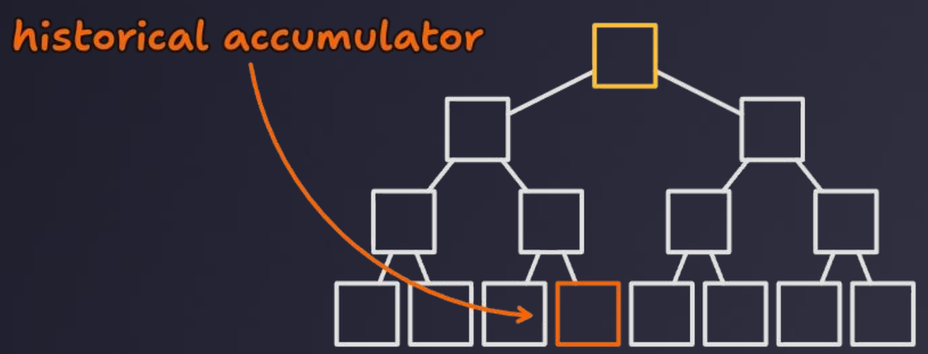
27 hours

8191 × 12 SECS ≈ 27 HOURS
FOR A TRANSACTION TO BE INCLUDED IN A BLOCK

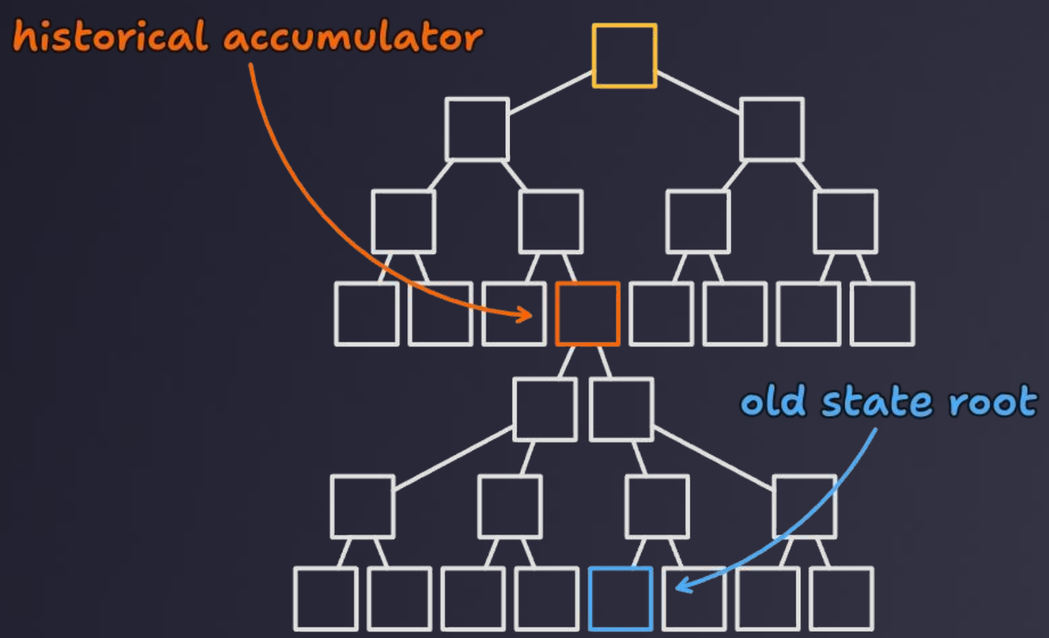
27 hours

"HISTORICAL ROOTS"
"HISTORICAL SUMMARIES"

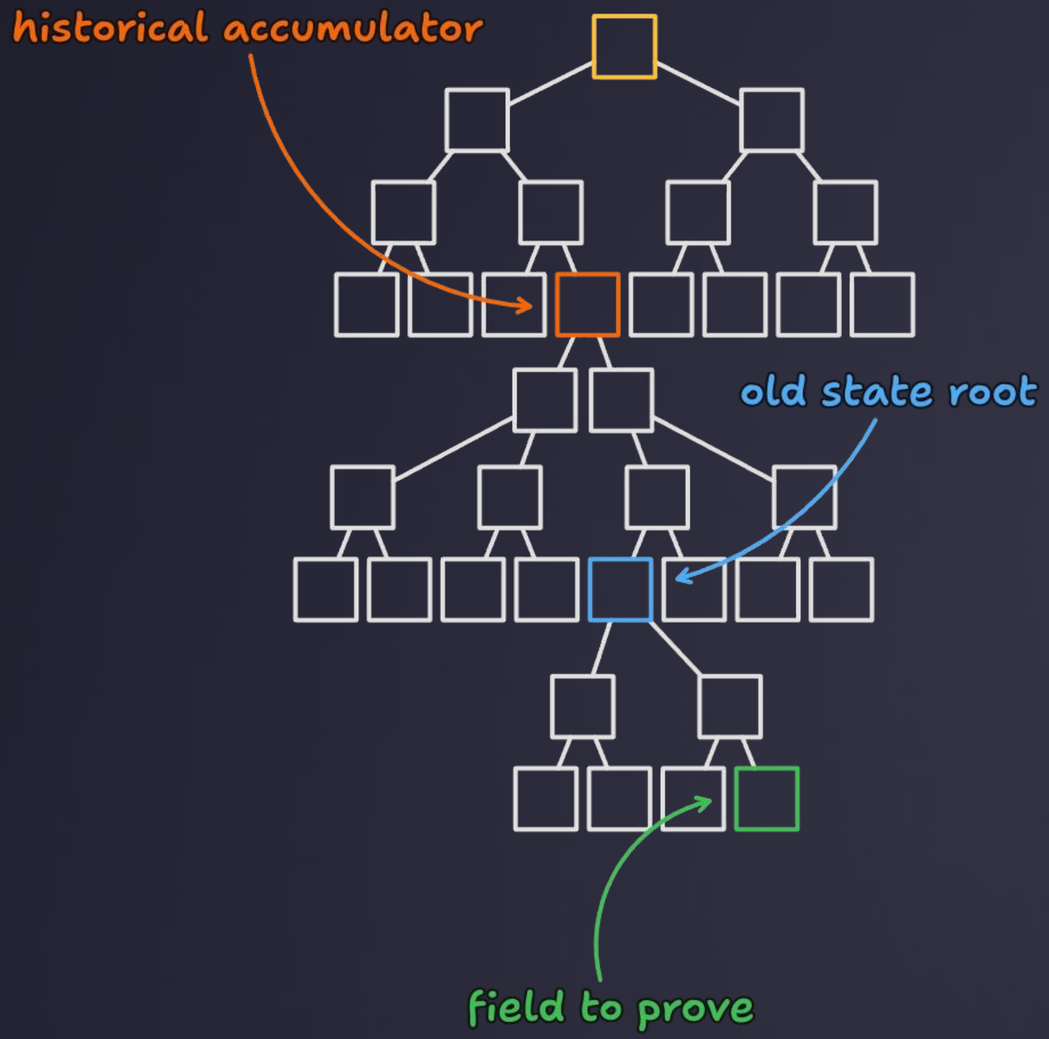
27 hours



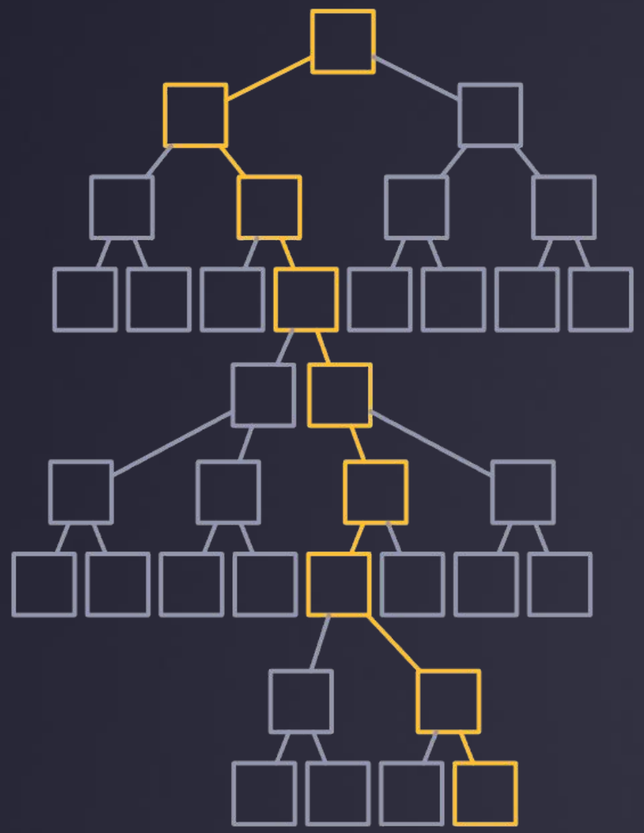
27 hours



27 hours



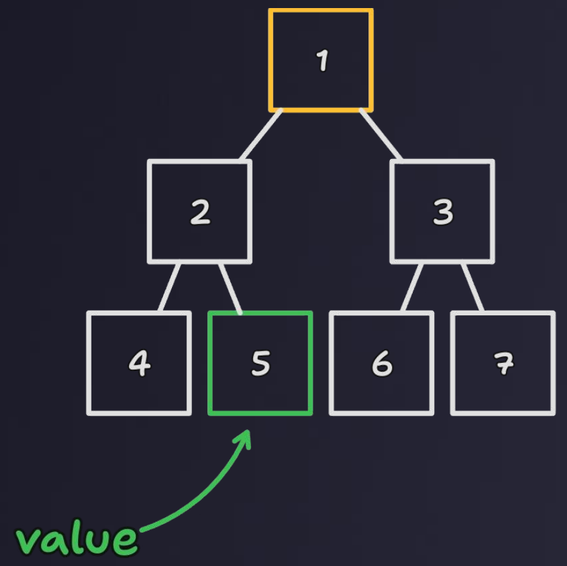
27 hours

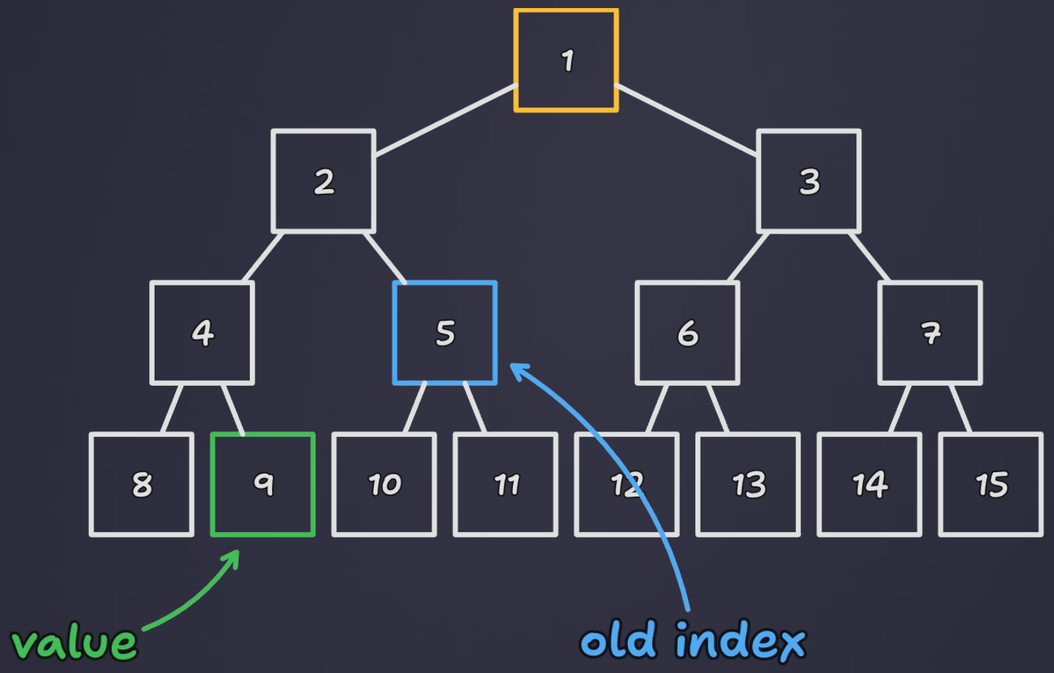


Generalized indices source

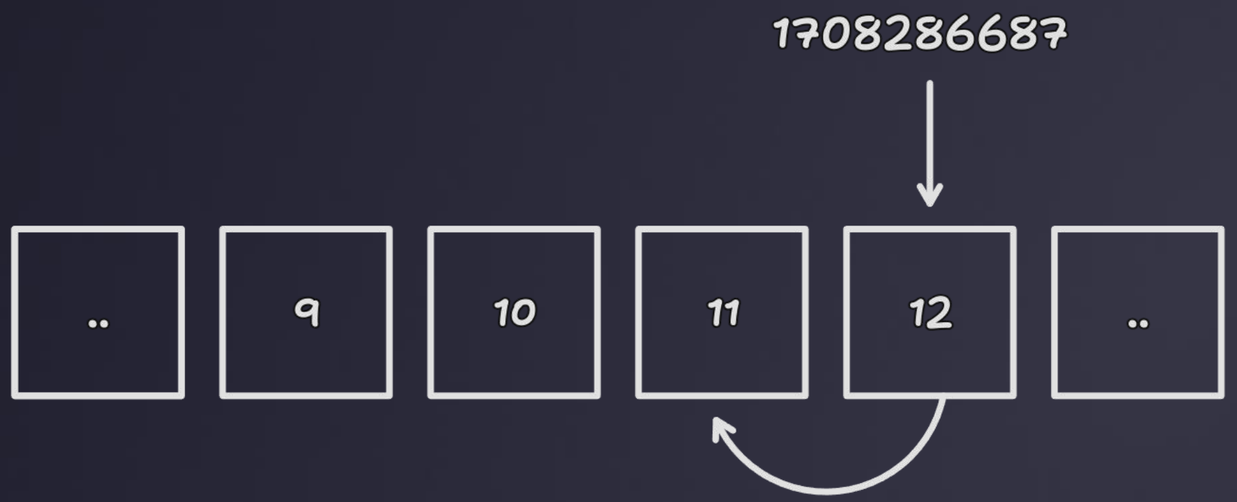
WE PLACE TRUST IN A GENERALIZED INDEX,
BUT THERE'S NO TRUSTLESS WAY TO ACCESS IT.

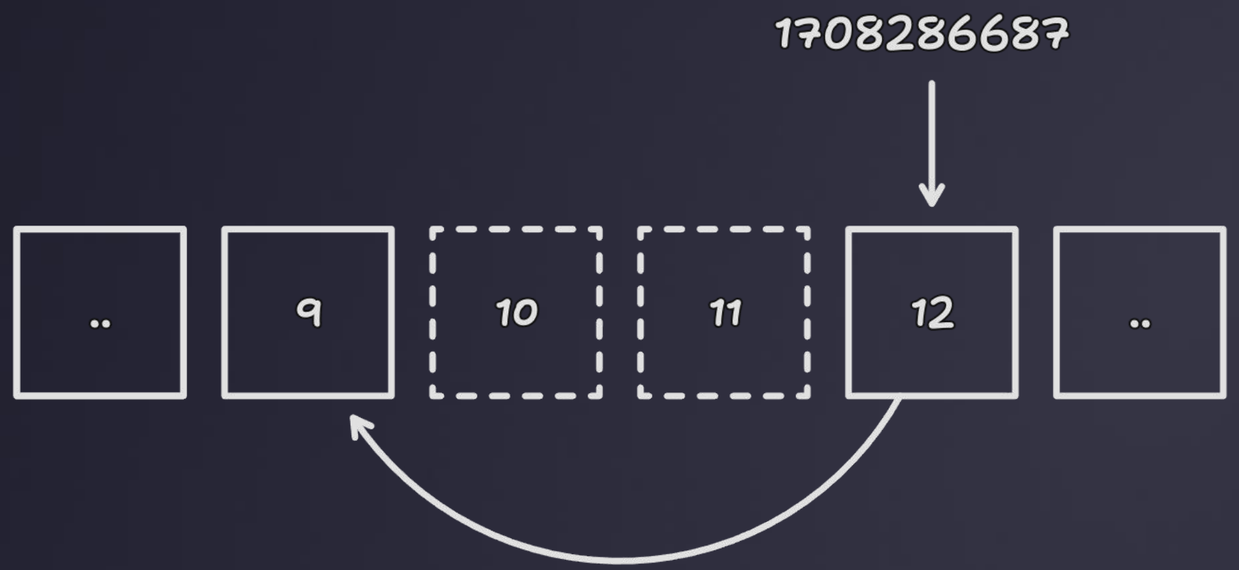
Generalized indices are changing





BLOCK ROOTS CONTRACT STORES
A **PARENT BLOCK ROOT** FOR A SLOT





WE DON'T KNOW FOR **WHAT SLOT** WE
GET THE **BLOCK ROOT** AT THE
GIVEN TIMESTAMP

https://github.com/madlabman/eip-4788-proof