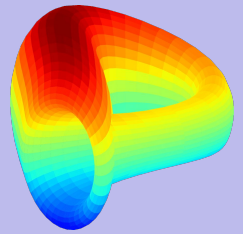


Curve Block Oracle

curve.finance


And more coming...

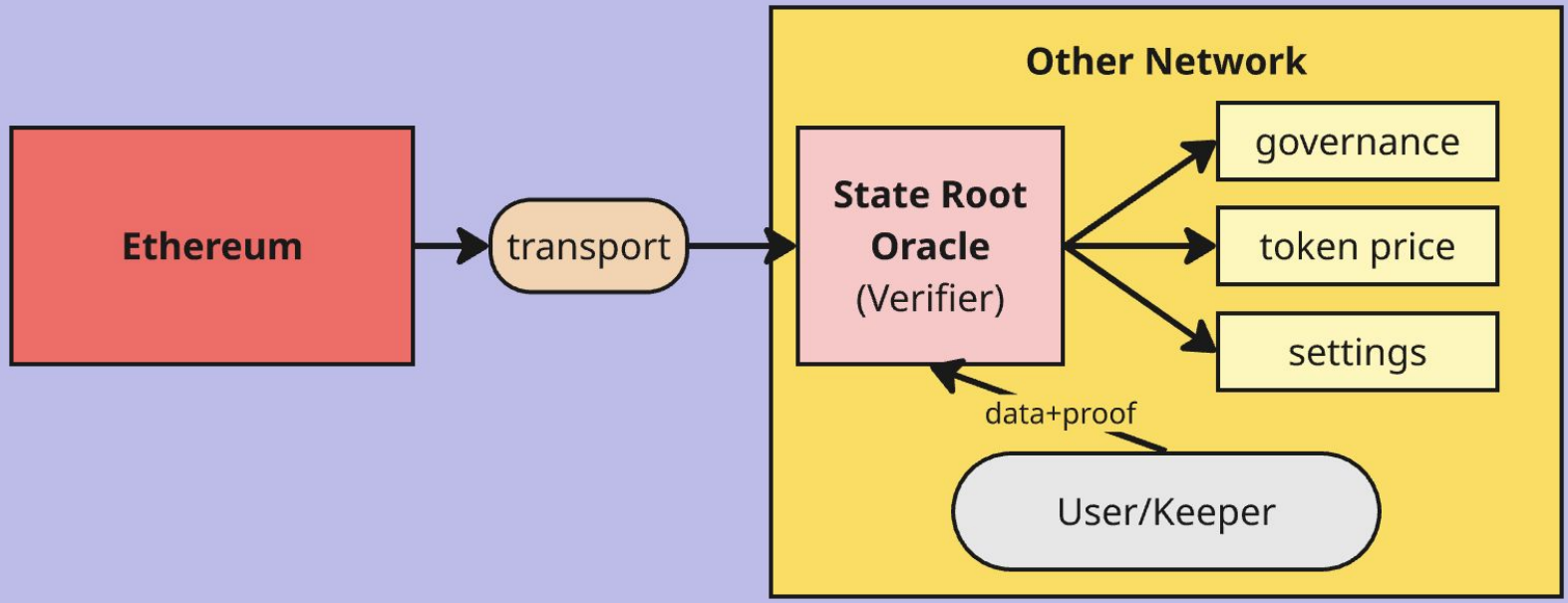
...but Curve DAO lives on Ethereum

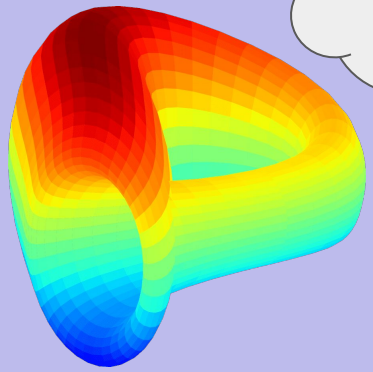
Cross-chain messaging

Type	Native [Arbitrum, Optimism, Sonic, etc] bridges	Transport layer protocols (LayerZero, CCIP, etc)
Risks	L2-specific risk: chain can rug	Protocol trust assumptions: infra, contracts, validators
Code	Maintaining every solution	One implementation for all supported networks

Block hash/state root approach

One interface for the whole codebase





we need storage proofs

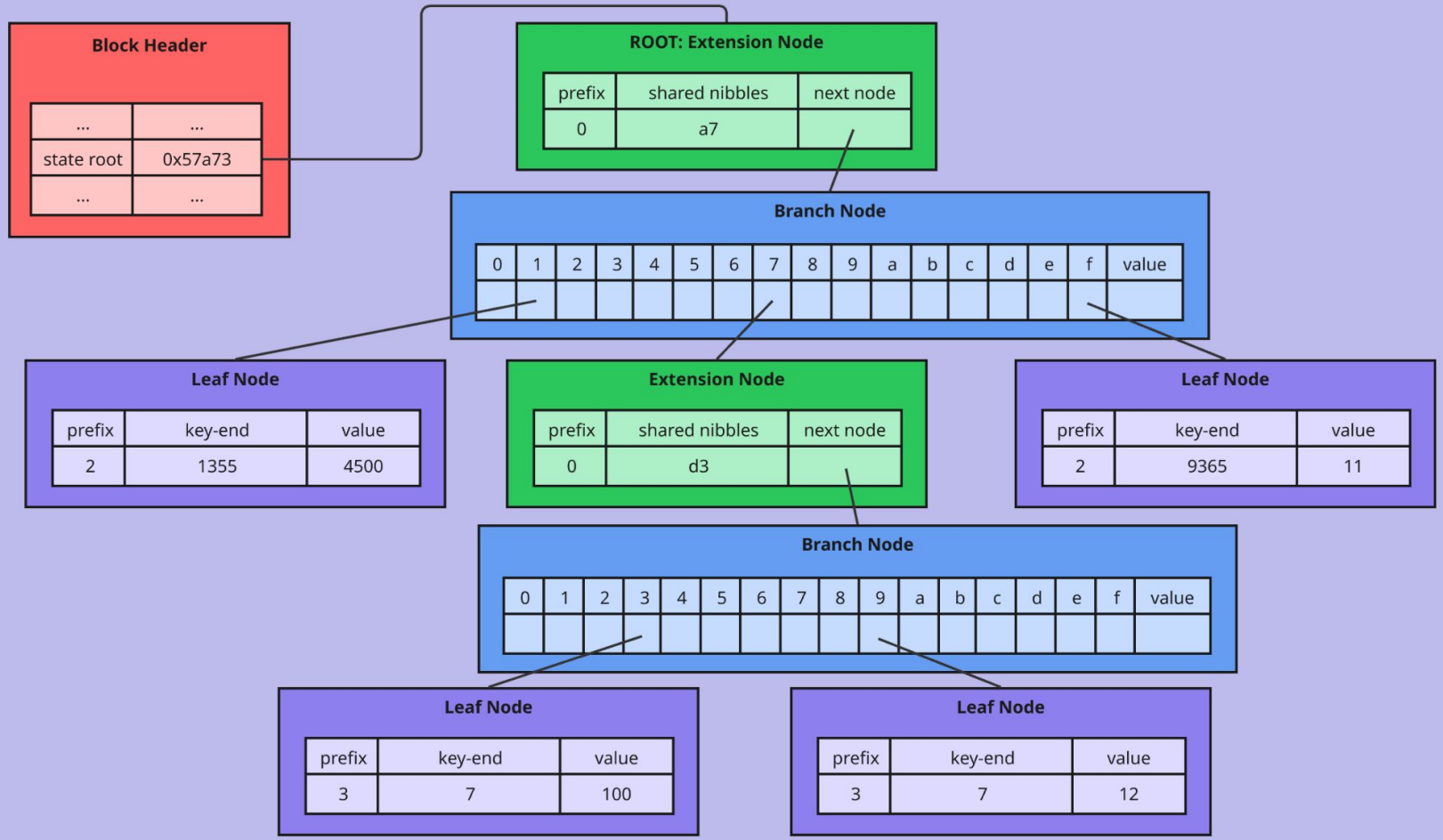
sorry, wait for the next release with dynamic bytes calldata allocation

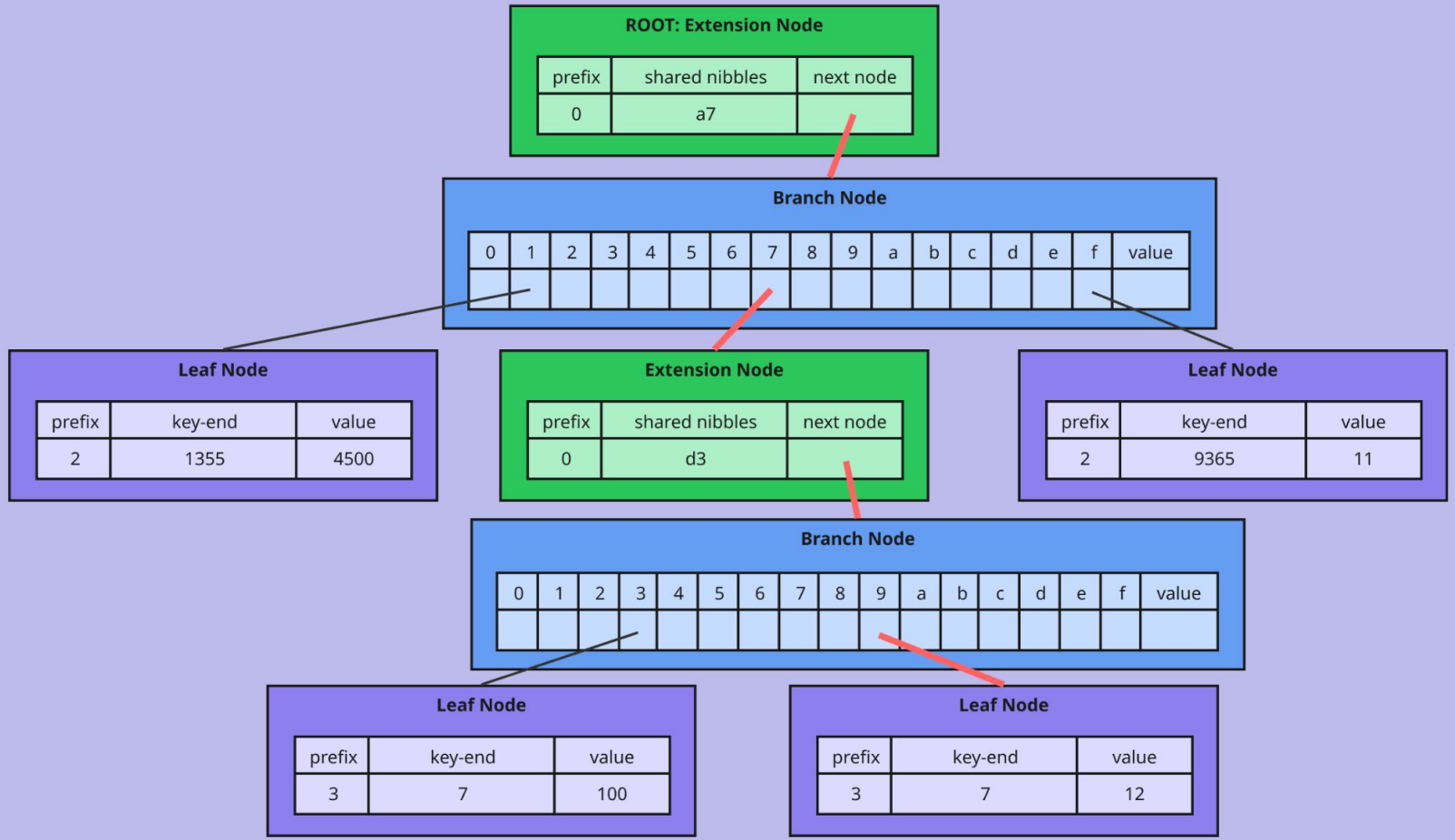
here you go, don’t mind the criticals

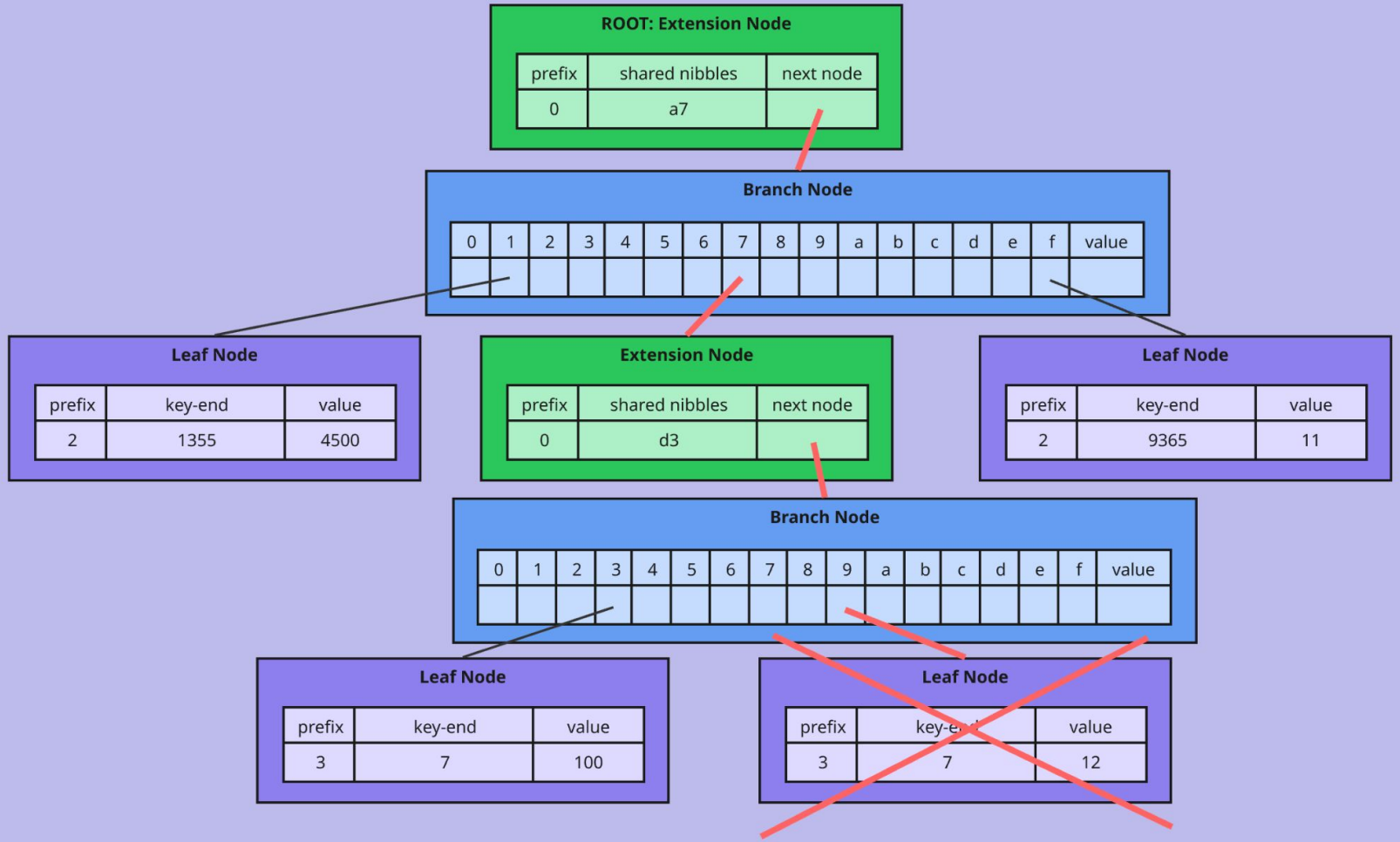
criticals?

CHAINSECURITY

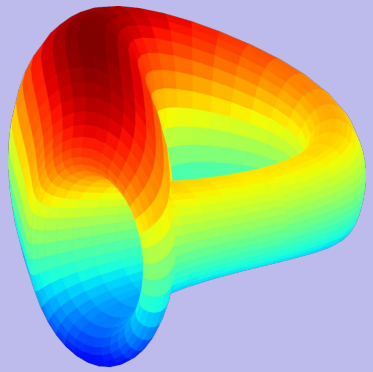
Storage proofs deep-dive


Block Header
... ...
state root 0x57a73
... ...
ROOT: Extension Node
prefix shared nibbles next node
0 a7
Branch Node
0 1 2 3 4 5 6 7 8 9 a b c d e f value
Leaf Node
prefix key-end value
2 1355 4500
Extension Node
prefix shared nibbles next node
0 d3
Leaf Node
prefix key-end value
2 9365 11
Branch Node
0 1 2 3 4 5 6 7 8 9 a b c d e f value
Leaf Node
prefix key-end value
3 7 100
Leaf Node
prefix key-end value
3 7 12


ROOT: Extension Node
prefix
shared nibbles
next node
0
a7
Branch Node
0 1 2 3 4 5 6 7 8 9 a b c d e f value
Leaf Node
prefix
key-end
value
2
1355
4500
Extension Node
prefix
shared nibbles
next node
0
d3
Leaf Node
prefix
key-end
value
2
9365
11
Branch Node
0 1 2 3 4 5 6 7 8 9 a b c d e f value
Leaf Node
prefix
key-end
value
3
7
100
Leaf Node
prefix
key-end
value
3
7
12


ROOT: Extension Node
prefix
shared nibbles
next node
0
a7
Branch Node
0 1 2 3 4 5 6 7 8 9 a b c d e f value
Leaf Node
prefix
key-end
value
2
1355
4500
Extension Node
prefix
shared nibbles
next node
0
d3
Leaf Node
prefix
key-end
value
2
9365
11
Branch Node
0 1 2 3 4 5 6 7 8 9 a b c d e f value
Leaf Node
prefix
key-end
value
3
7
100
Leaf Node
prefix
key-end
value
3
7
12

Curve's contribution



Layer Zero

https://github.com/curvefi/LayerZero-v2-vyper

Curve's oracle

- provides fresh Ethereum mainnet blockhash / state root
- everywhere where curve is deployed (20+ chains)
- curve keepers (pull update is permissionless!)
- using native bridges where possible
- using LayerZero for others/at initial curve-lite deployment
- in-house Curve DVN
- crosscurve DVN supporting Axelar, CCIP and others
- available for everyone!