CHAINSECURITY

Merkle Proofs
When Leaves Leave You Vulnerable

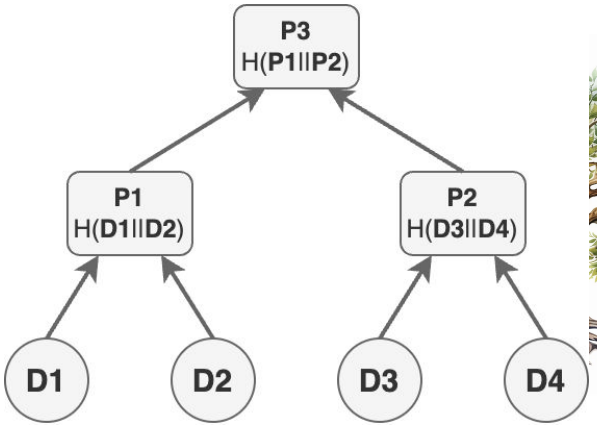
Shufan Wang
Security Engineer @ ChainSecurity

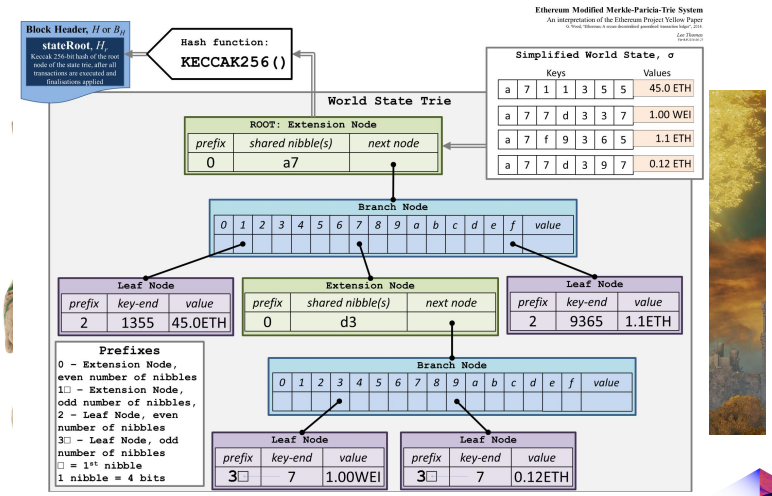
CHAINSECURITY

DC7 SEA

Trees and Merkle Trees

Various Shapes / Structures





CHAINSECURITY

Non-exhaustive checklist

Ensure secure proof of leaves

- Encode / hash the leaf data
- Use domain separation
- Validate leaf index and depth
- Validate proof length
- …

When Leaves Leave You Vulnerable?

When you don’t realize:

They are leaves

MMR: Merkle Mountain Range

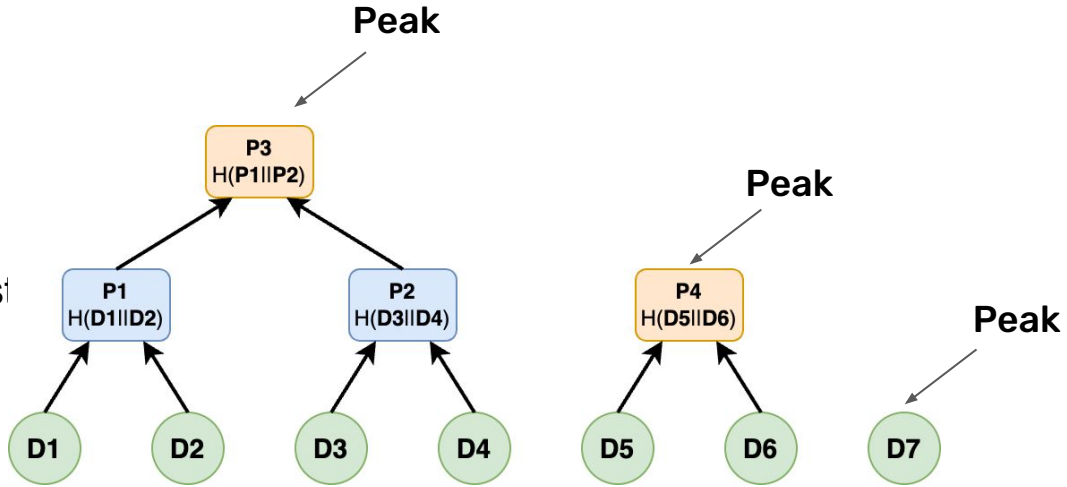
Another Merkle Family Algorithm

What is MMR?

- A group of typical Merkle Trees
- Leaves inserted at the bottom
- Add a parent if two siblings exist

Why MMR?

- Efficient data insertion

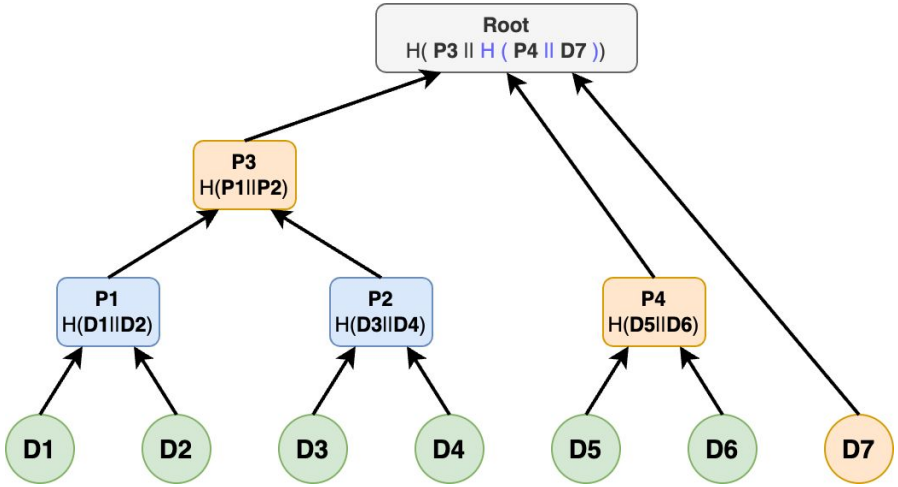


MMR: Merkle Mountain Range

Another Merkle Family Algorithm

"Bagging" all the subtrees together

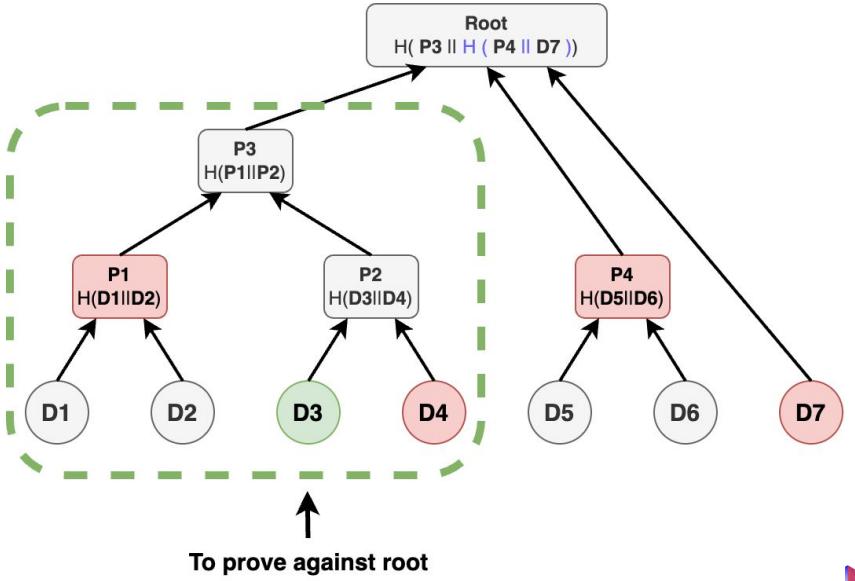
- A group of typical Merkle Trees
- Leaves inserted at the bottom
- Add a parent if two siblings exist
- **Root**: nested hash subtree **Peaks**



Existence Proof of a Leaf

Provide all the red nodes

- A typical proof to a subtree Peak
  (P1, D4 in the example)
- Provide other Peaks to recompute Root
  (P4, D7 in the example)



What Could Go Wrong?

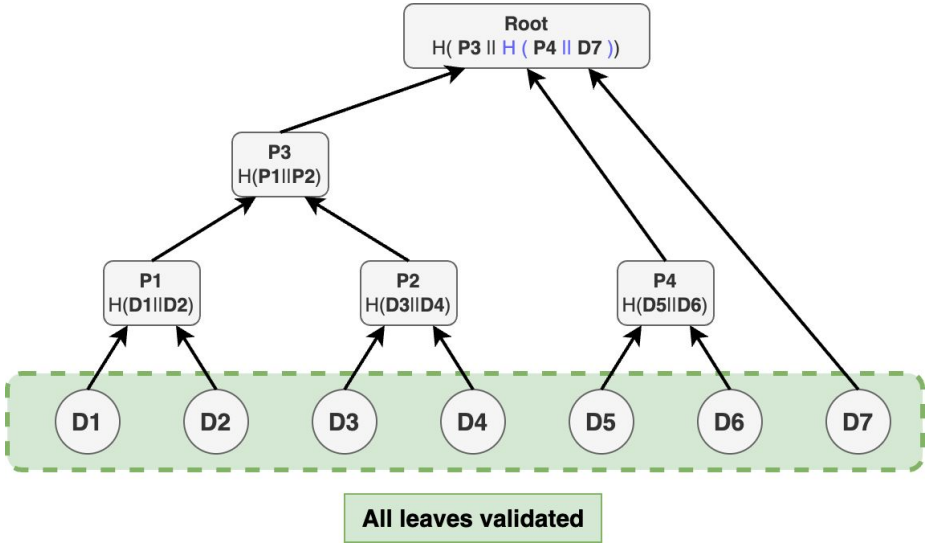
Assumptions for subtrees

Trusted Insertion

- No subtree insertion as a leaf

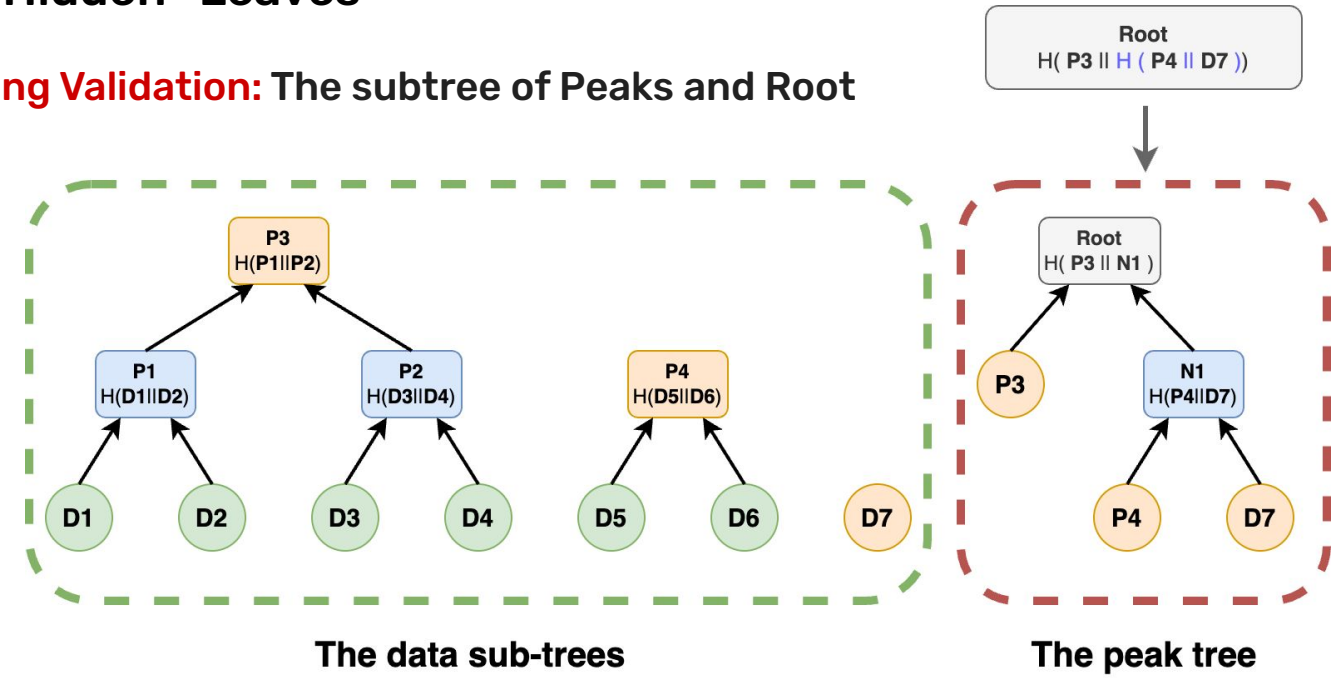
Subtree Index / Depth Verification

- No intermediate node in as a leaf



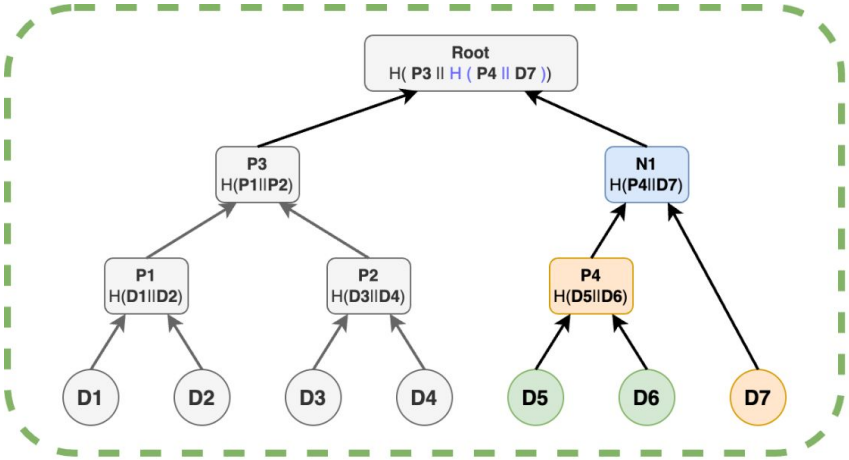
The Hidden “Leaves”

Missing Validation: The subtree of Peaks and Root

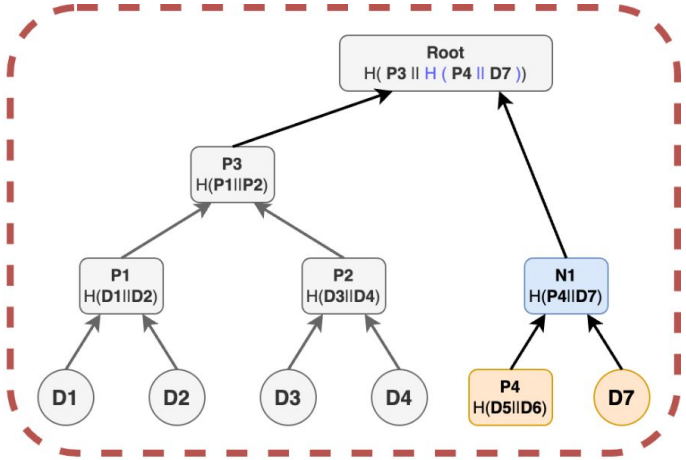


The Hidden “Leaves”

Attack Example: Prove a Peak as a Leaf



MMR with 3 peaks



MMR with 2 peaks, same root

CHAINSECURITY

Our clients

ethereum foundation
CIRCLE
polygon
MAKER
Curve
LIDO
Mellow Protocol
TRON
yearn
SYMBIOTIC
Swell
PENDLE
Polymarket
FUEL
argent

@LOUISHANNOUILLE_
CHAINSECURITY

A Non-leaf With Belief Could Be a Leaf

When you don't realize it,
It leaves you vulnerable

Be sure you validate
Expected property of all inputs