accumulator

Ethereum Sharding Research

Jeongho Jeon <maczniak@gmail.com>

July 16, 2018

Whitepaper Foundation, Nonce
(for internal discussion purposes only)

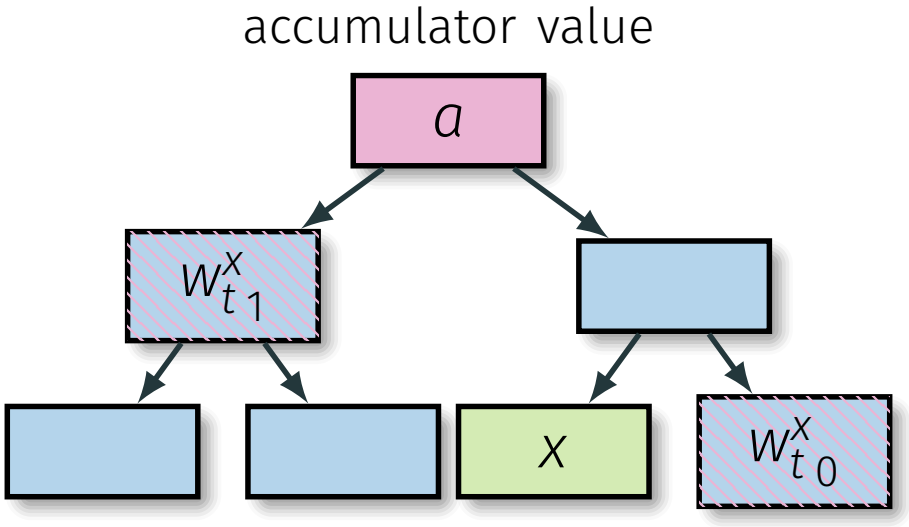
Whitepaper
Foundation

Recap: Accumulator

Accumulator is the function that aggregates recursive data structure (such as lists and trees) into a single value. It is also called as fold and reduce.

Cryptographic accumulator is the one-way membership function that could tell whether the given item is in the set without revealing set members. For example, Merkle tree is a cryptographic accumulator.

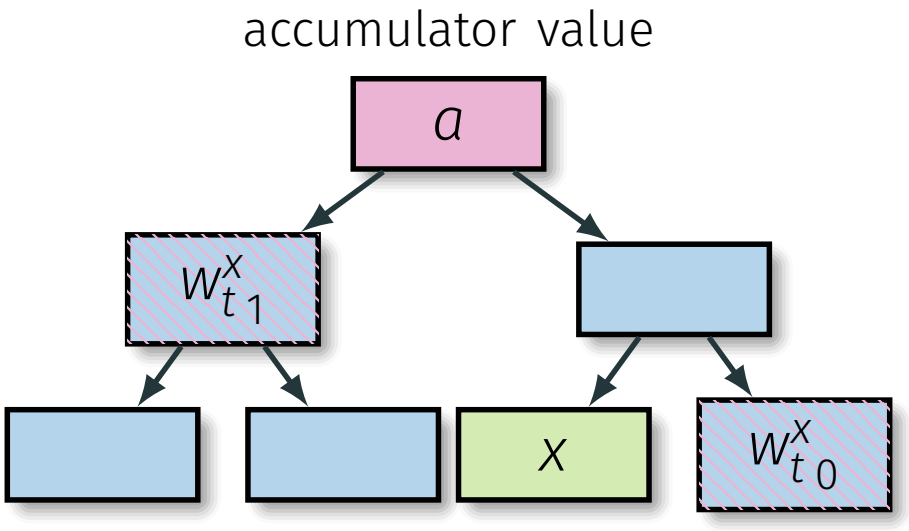
Recap: Merkle tree as an Accumulator



Merkle proof $\{(w^x_{t\,0}, right), (w^x_{t\,1}, left)\}$

$$a = h(w^x_{t\,1} || h(x || w^x_{t\,0}))$$

Recap: Merkle tree as an Accumulator



Each time you put a new item, accumulator value (Merkle root, a) and witness (Merkle proof, w^x_t) should be updated.

Recap: Low update frequency accumulator[3]

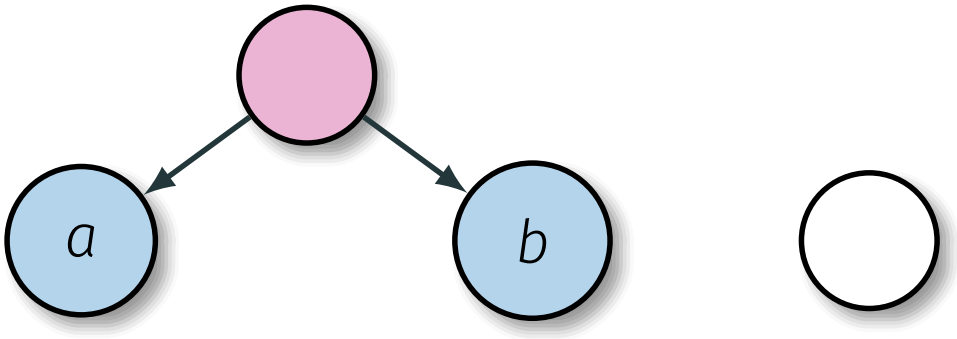
It is called by many names: asynchronous accumulator[1], Merkle mountain range (MMR)[2], delayed (U)TXO commitment and so on.

Even if accumulator value and witness are not synchronous, i.e., witness is older than accumulator value or accumulator value is older than witness, it can verify a member. Then updates can be delayed. It makes $log(n)$ times updates, and take up $log(n)$ times space (i.e., moutain summits).

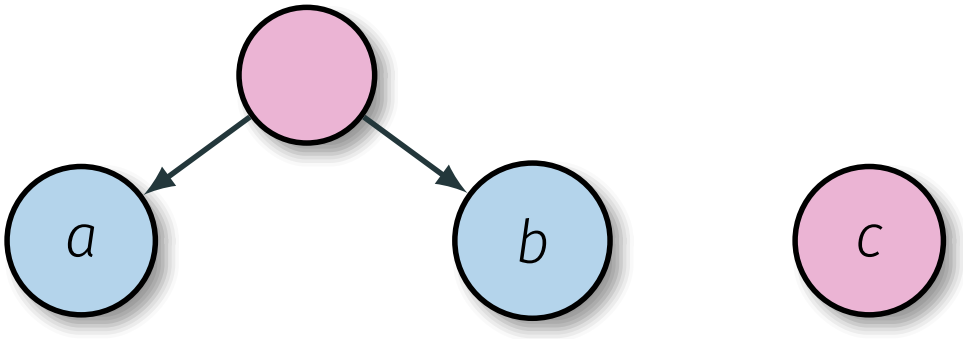
---

[1] https://eprint.iacr.org/2015/718.pdf
[2] https://petertodd.org/2016/delayed-txo-commitments
[3] https://ethresear.ch/t/history-state-and-asynchronous-accumulators-in-the-stateless-model/287

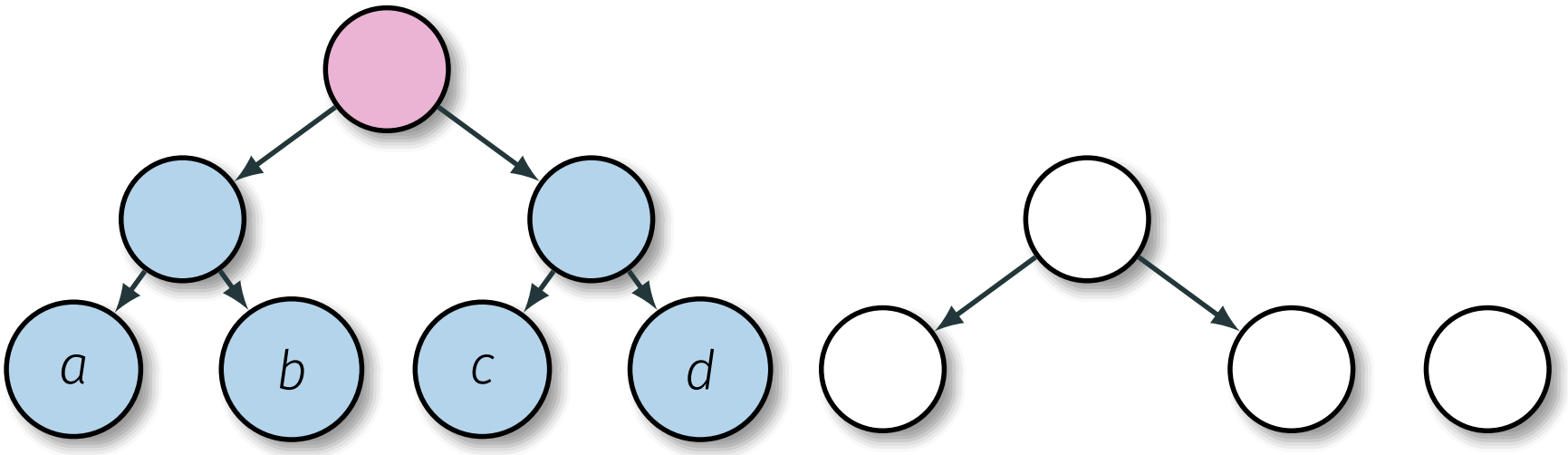
Recap: Step 1/5



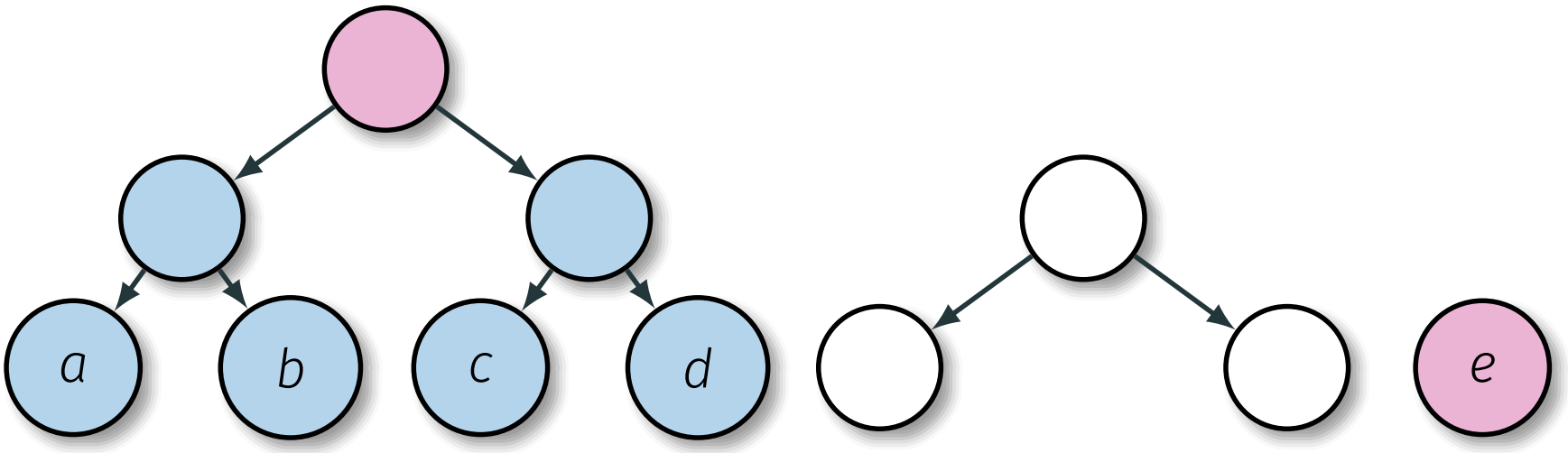
Recap: Step 2/5



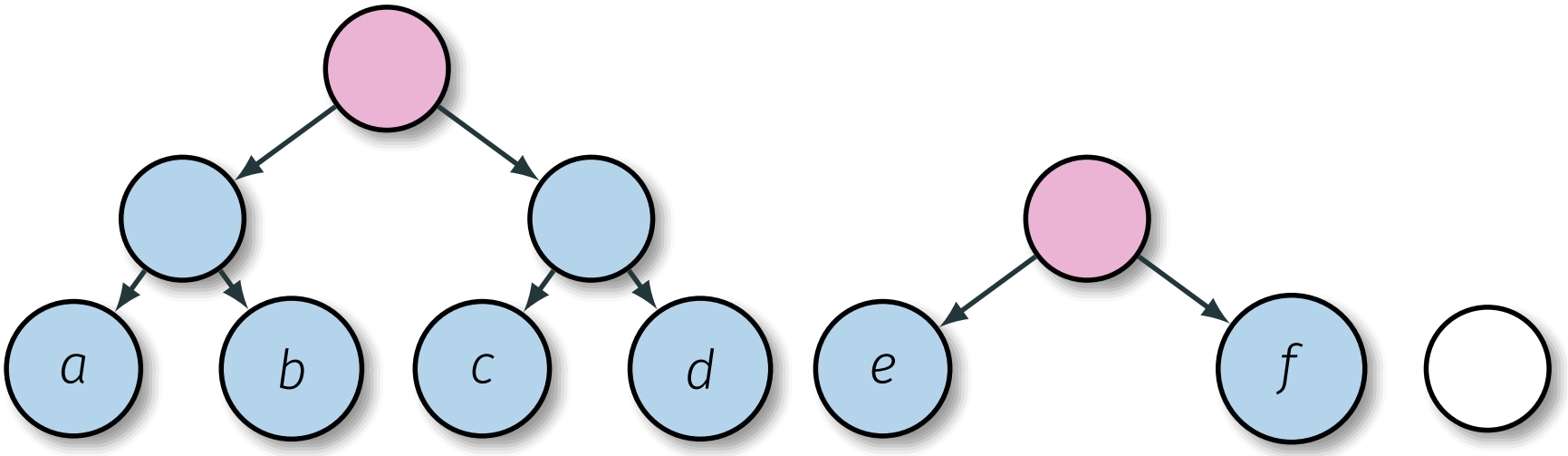
Recap: Step 3/5



Recap: Step 4/5



Recap: Step 5/5



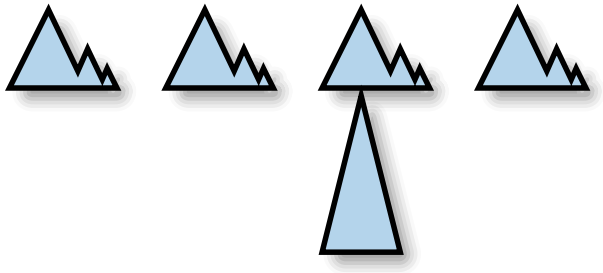
Batching and cyclic partitioning of logs[4]

multi-MMR (MMMR, 3MR), witness concatenation

Cyclic partitioning (2^n MMRs),

push a collation with height i

to MMR $i \mod 2^n$

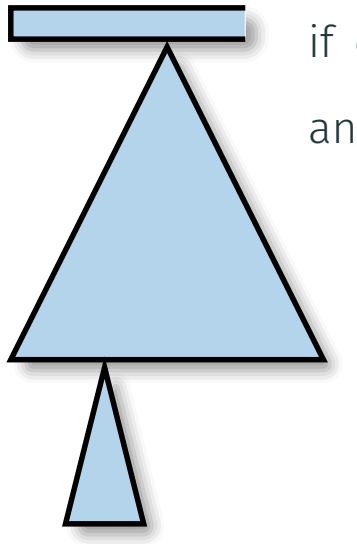


Batching (Merkle tree), log batch root

[4] https://ethresear.ch/t/batching-and-cyclic-partitioning-of-logs/536

Double-batched Merkle log accumulator[5]

permanent witness



Top buffer (linear), +15kb per year if collation interval is 8 seconds and $n = 13$

Bottom buffer with 2^n entries (Merkle tree) 250kb

Merkle tree of all logs of shard height $i \mod 2^n$

[5] https://ethresear.ch/t/double-batched-merkle-log-accumulator/571

Delayed TXO Commitments[6]

To solve UTXO growth problem

UTXO set unspent outputs of recent transactions

STXO set spent outputs of recent transactions

TXO journal spent output queue with TXO commitment proofs

TXO MMR list append UTXO set and prune STXO set in a low-priority background task

[6] https://petertodd.org/2016/delayed-txo-commitments

non-Merkle accumulators[7]

RSA accumulator

- $A = g^{a_1 \cdot a_2 \cdot \ldots \cdot a_n}$
- constant size
- simple witness update
- dynamic and universal
- requires a trapdoor (not suitable for the decentralized context)

elliptic curve accumulators

vs. SNARK-compressed Merkle paths (preliminary research)

[7] https://ethresear.ch/t/accumulators-scalability-of-utxo-blockchains-and-data-availability/176