Immutable record

Merkle hash tree
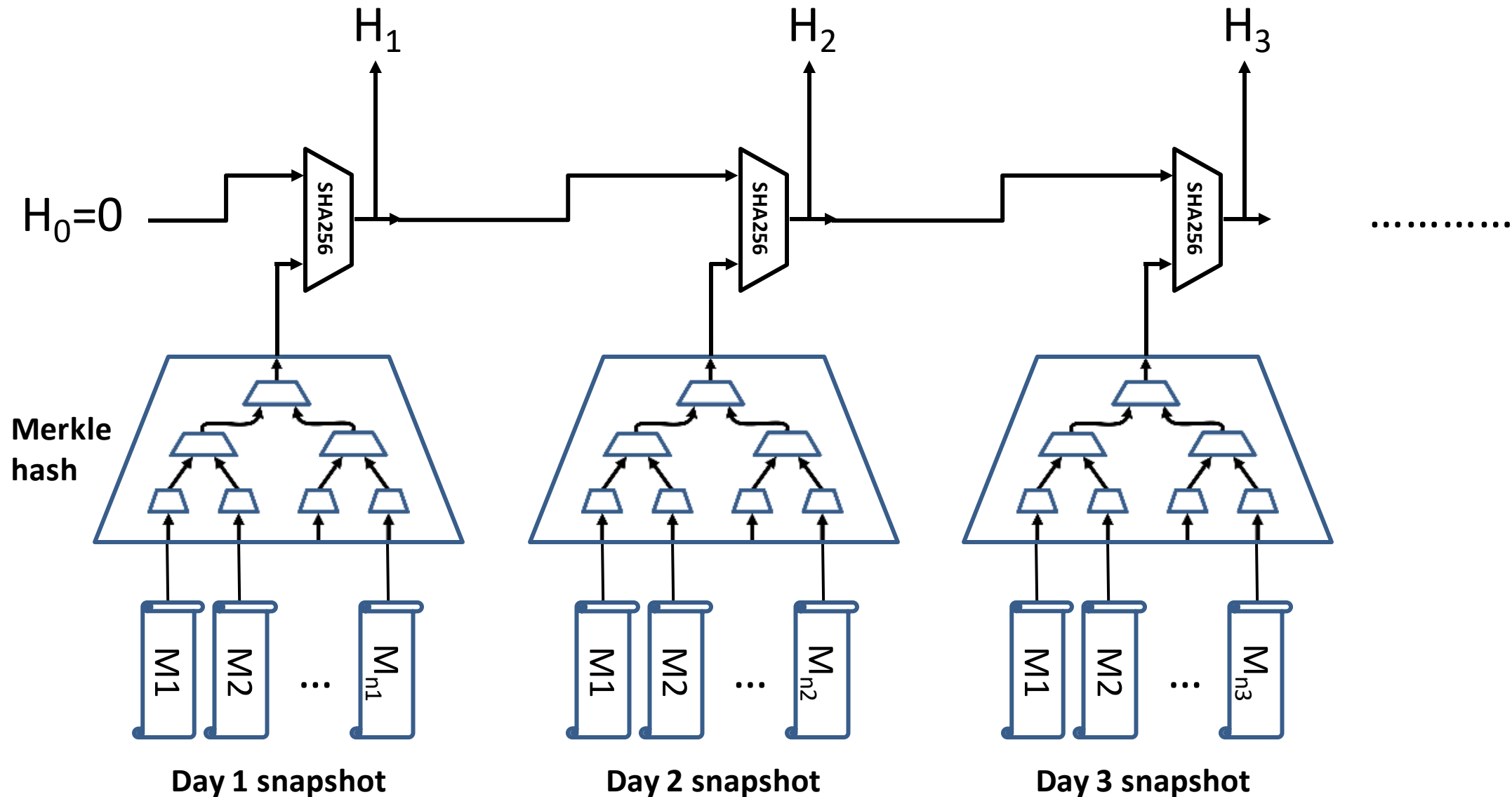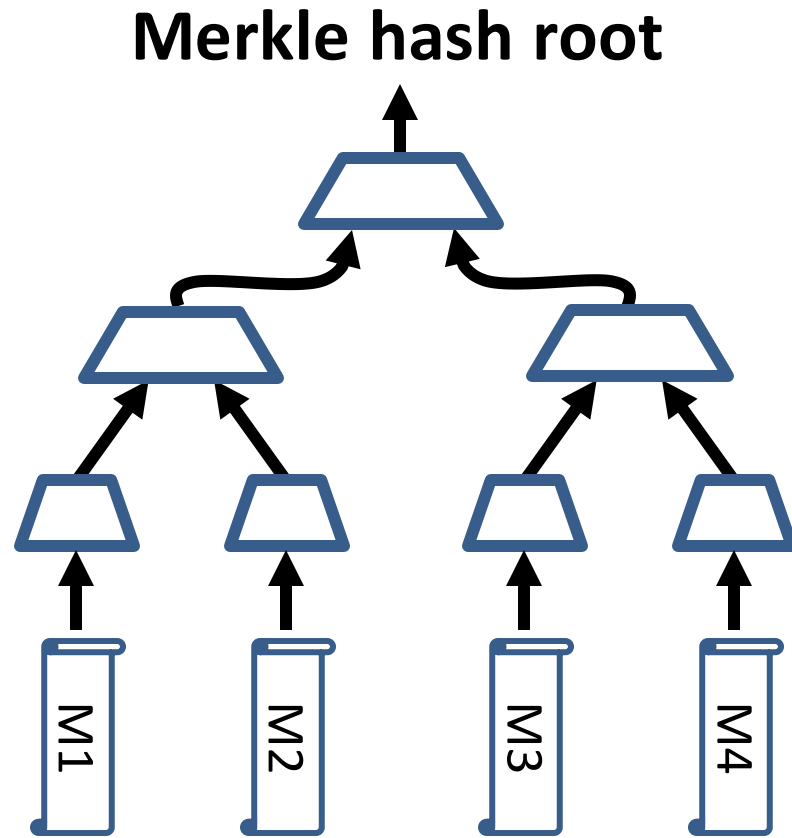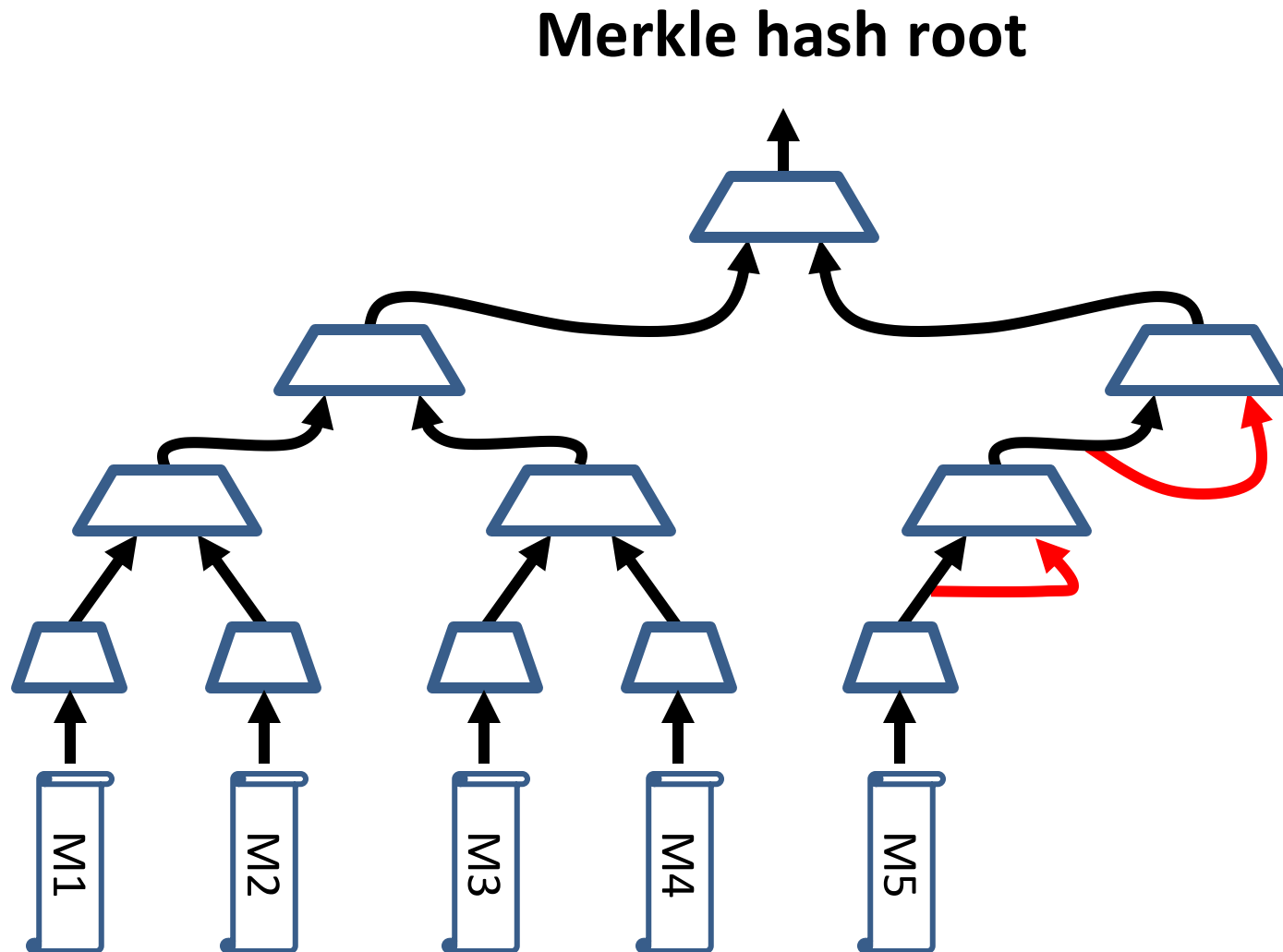
Merkle hash root

- Each message is hashed individually at first.
- Hash values are then repeatedly pair-wise merge-hashed till a single root hash value is produced.
  - merge-hash: concatenate then hash
- The order in which hash values are merge-hashed is important
  - a change in the order will result in a different Merkle hash root!

Dealing with non-ideal # of messages

Merkle hash root

- When the # of hash values is not even, the last hash value is reused to create a pair.