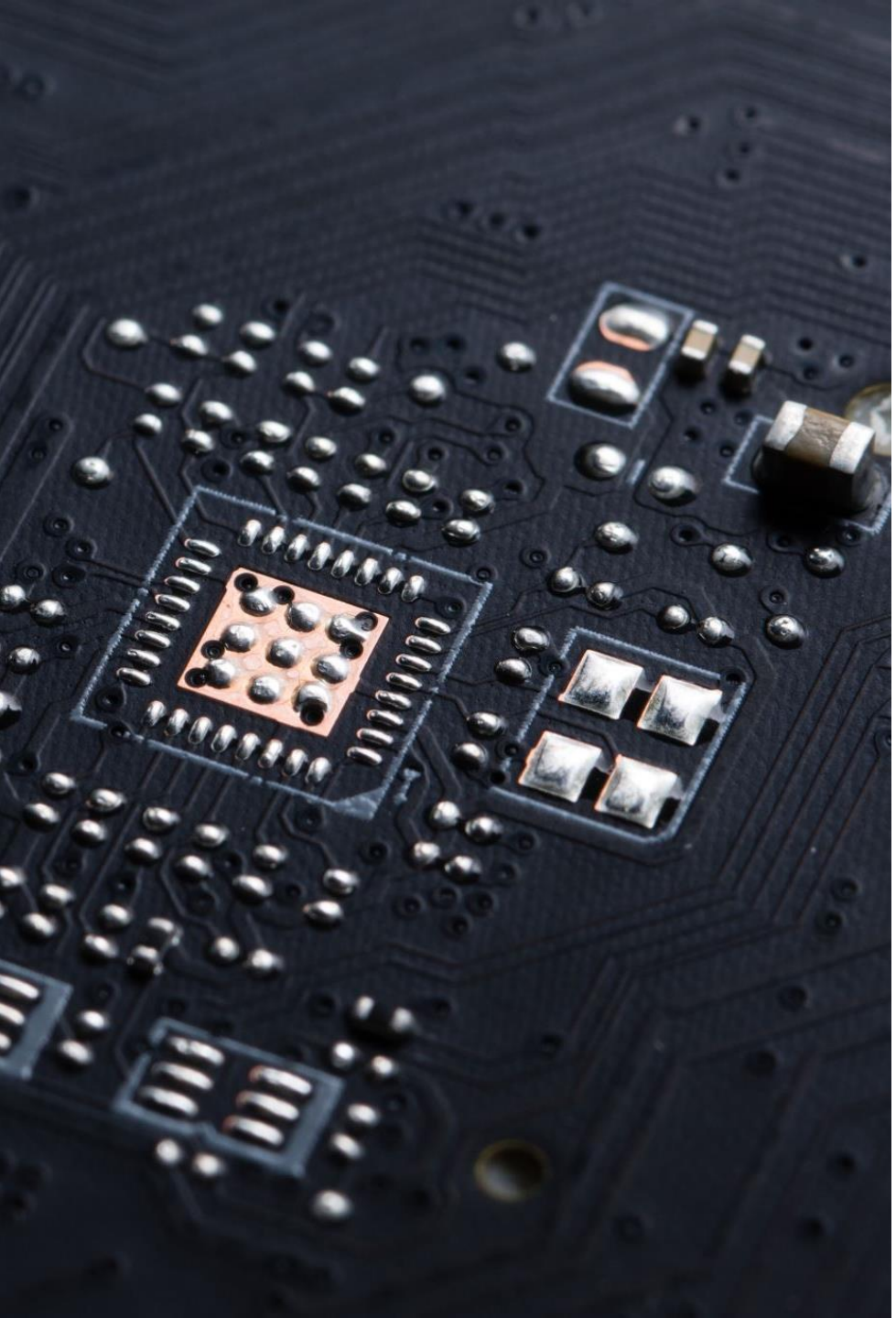
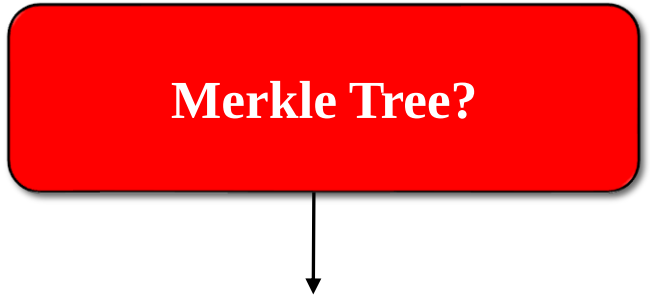
Blockchain

Dr. Bahar Ali
Assistant Professor (CS), National University Of Computer and Emerging Sciences, Peshawar.



Merkle Tree

Contents – Module D



Merkle Tree

- A Merkle Tree, also known as a Merkle Hash Tree by Ralph Merkle.
- A fundamental data structure used in computer science and particularly in blockchain technology.
- A tree-like structure in which every leaf node is labeled with a cryptographic hash of a data block and every non-leaf node is labeled with the cryptographic hash of its child nodes.
- Building a Merkle Tree involves repeatedly hashing pairs of nodes until a single root hash (Merkle Root) is produced.

Merkle Tree

Data blocks:

- Each data block, such as a transaction in a blockchain, is individually hashed.

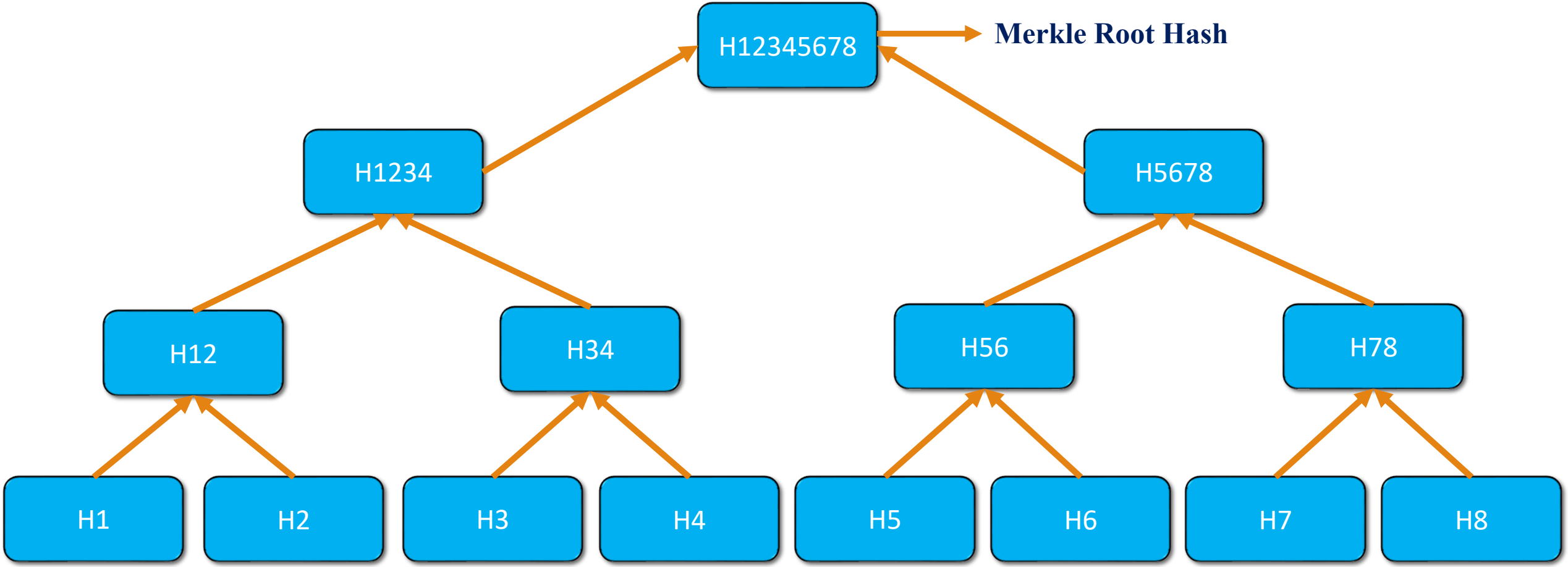
Pairwise hashing:

- Pairs of hashes are combined and hashed again. In case of an odd number of nodes, the last node is paired with itself.

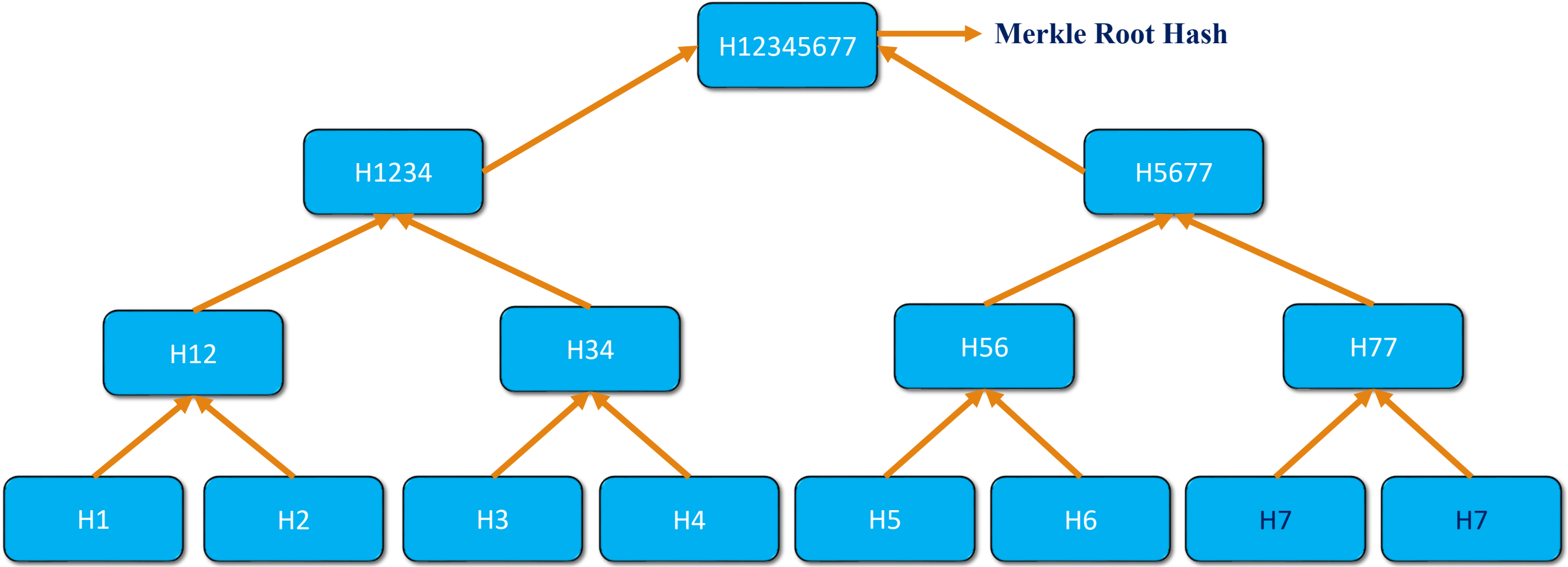
Repeating the process:

- The process continues, with pairs of hashes being combined until only a single root hash called the **Merkle Root** remains.

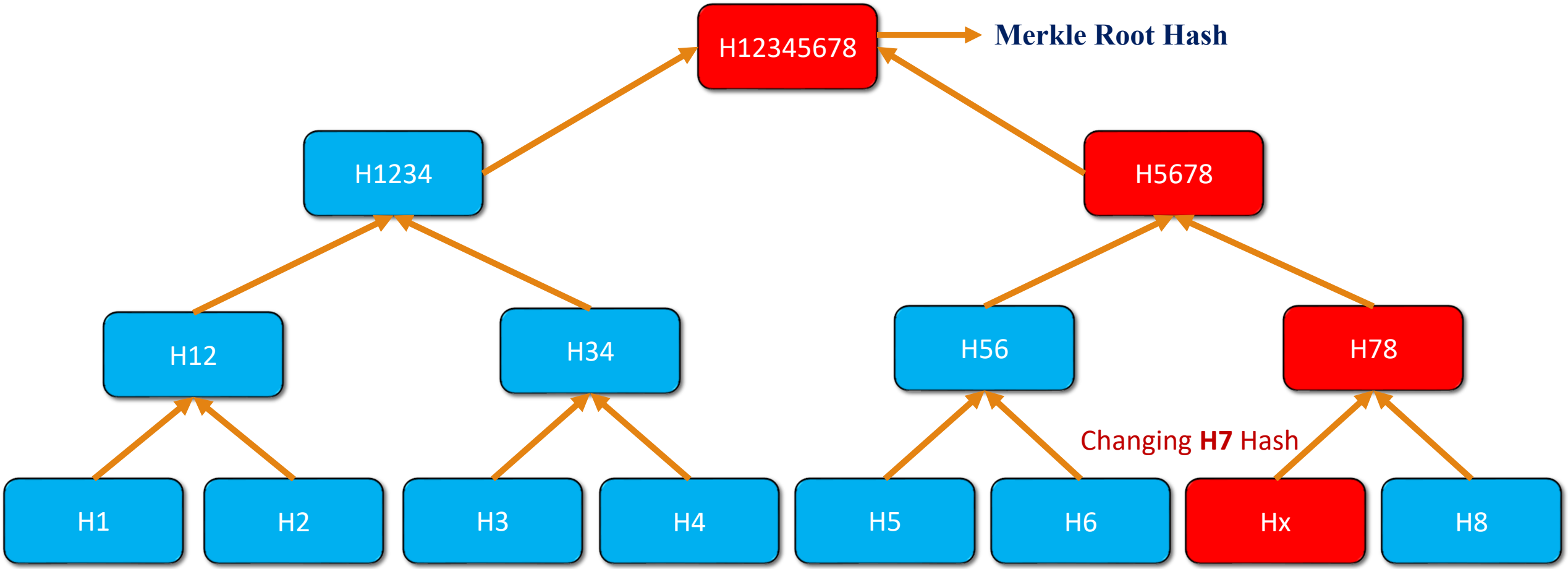
Merkle Tree (Even Nodes)



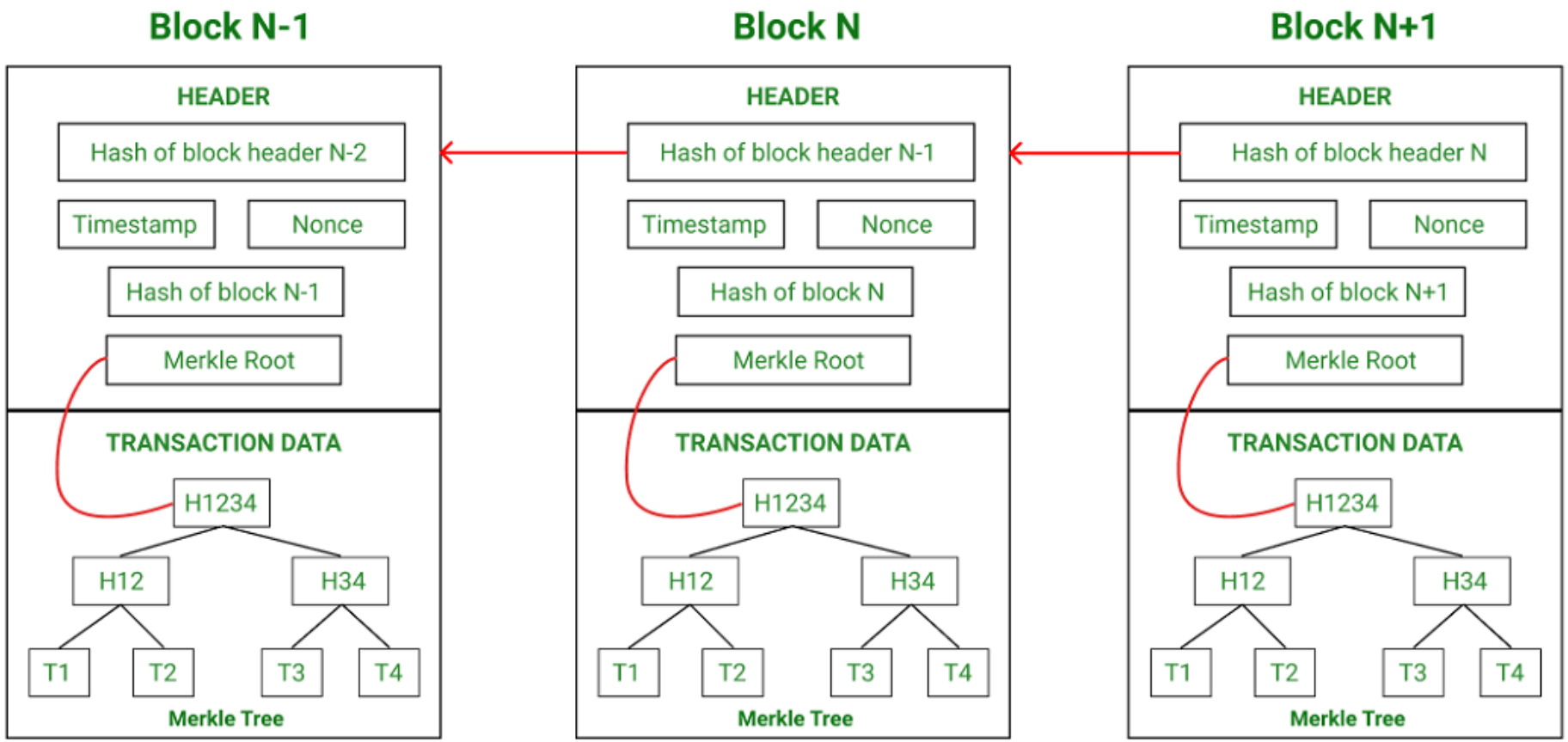
Merkle Tree (Odd Nodes)



Merkle Tree (Invalid)



Merkle Tree


Block N-1
HEADER
Hash of block header N-2
Timestamp
Nonce
Hash of block N-1
Merkle Root
TRANSACTION DATA
H1234
H12
H34
T1
T2
T3
T4
Merkle Tree
Block N
HEADER
Hash of block header N-1
Timestamp
Nonce
Hash of block N
Merkle Root
TRANSACTION DATA
H1234
H12
H34
T1
T2
T3
T4
Merkle Tree
Block N+1
HEADER
Hash of block header N
Timestamp
Nonce
Hash of block N+1
Merkle Root
TRANSACTION DATA
H1234
H12
H34
T1
T2
T3
T4
Merkle Tree

Merkle Tree

Full Node

SPV Node

Merkle Tree Importance

Data Integrity:

- To verify the integrity of data in a highly efficient manner.

Efficient Verification:

- To confirm whether a particular transaction is included in a block without checking the entire transaction. This is especially important for scalability and light clients.

Security:

- Difficult to alter a single transaction without changing the Merkle Root. Helps in quick detection of invalidity.

Merkle Tree Importance

Simplified Payment Verification (SPV):

- Allow lightweight clients to verify transactions without storing the entire blockchain.

Blockchain Consensus:

- In some blockchain networks, used to reach a consensus about the validity of transactions within a block.

Note:

- SPV term used for software that queries other nodes for blocks and transactions.
- An SPV client is a form of light client described by Satoshi in the whitepaper.