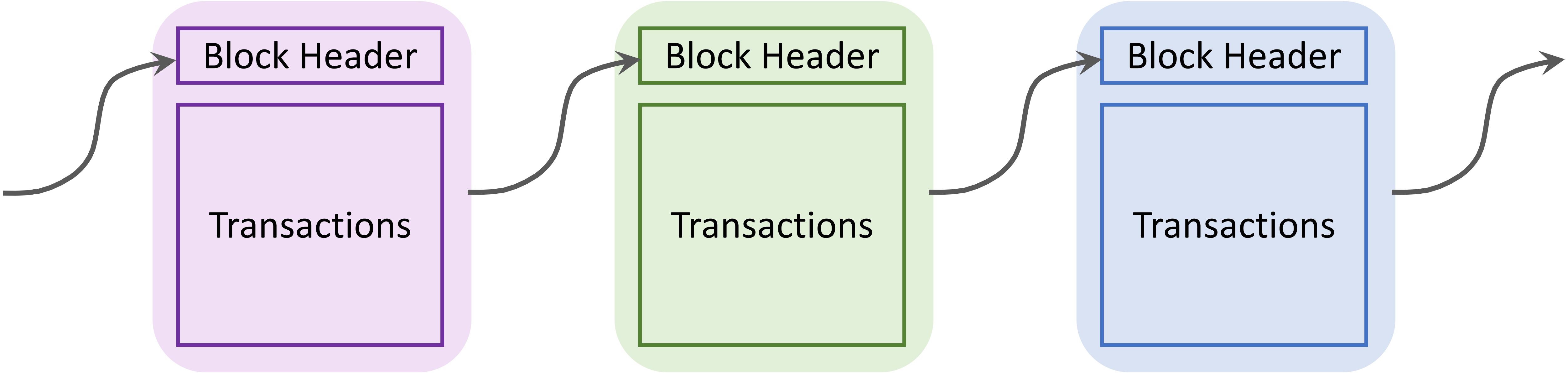
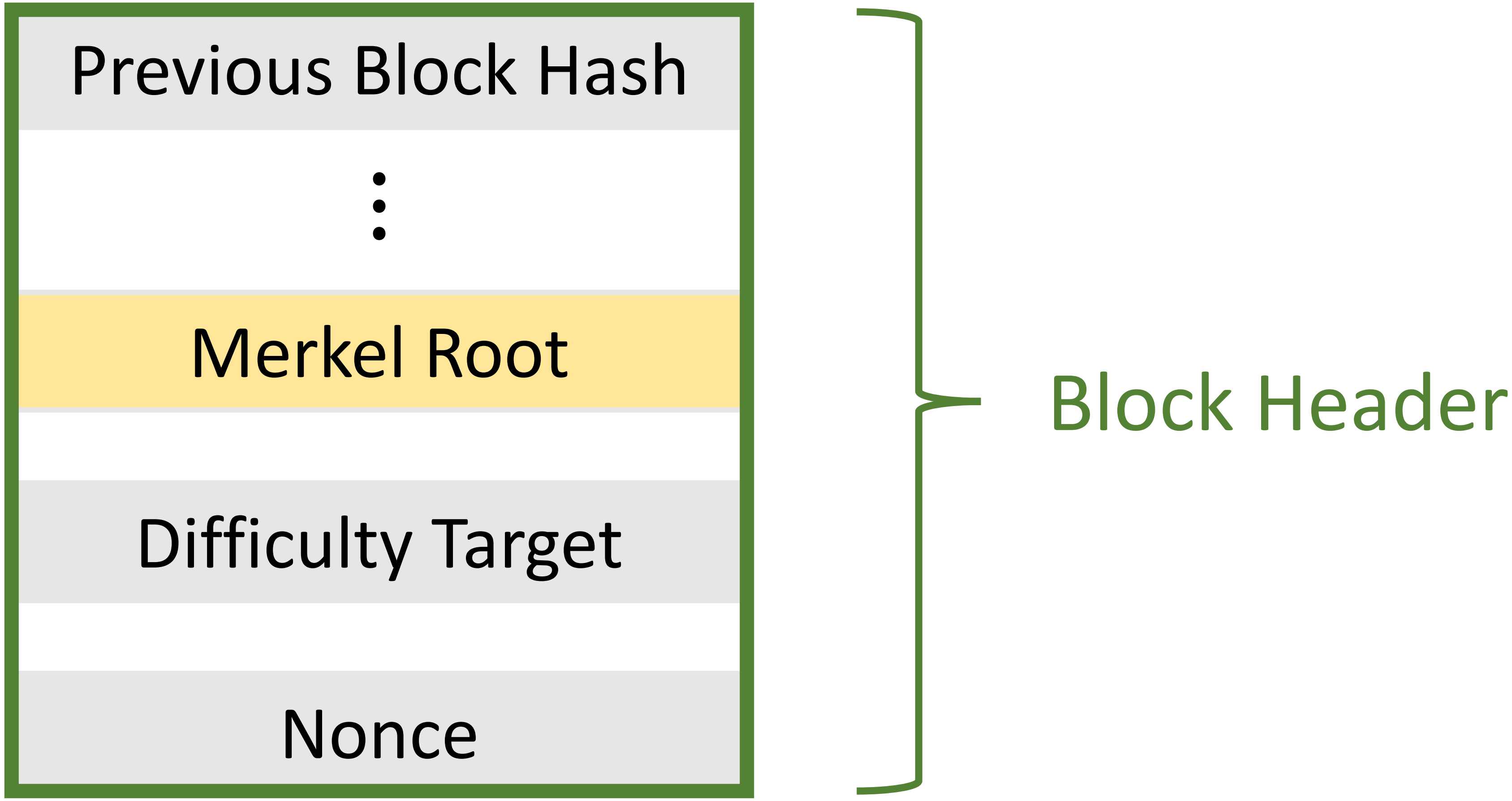
Merkle Tree

Shusen Wang

Blockchain


Block Header
Transactions
Block Header
Transactions
Block Header
Transactions

Block Header



Previous Block Hash

⋮

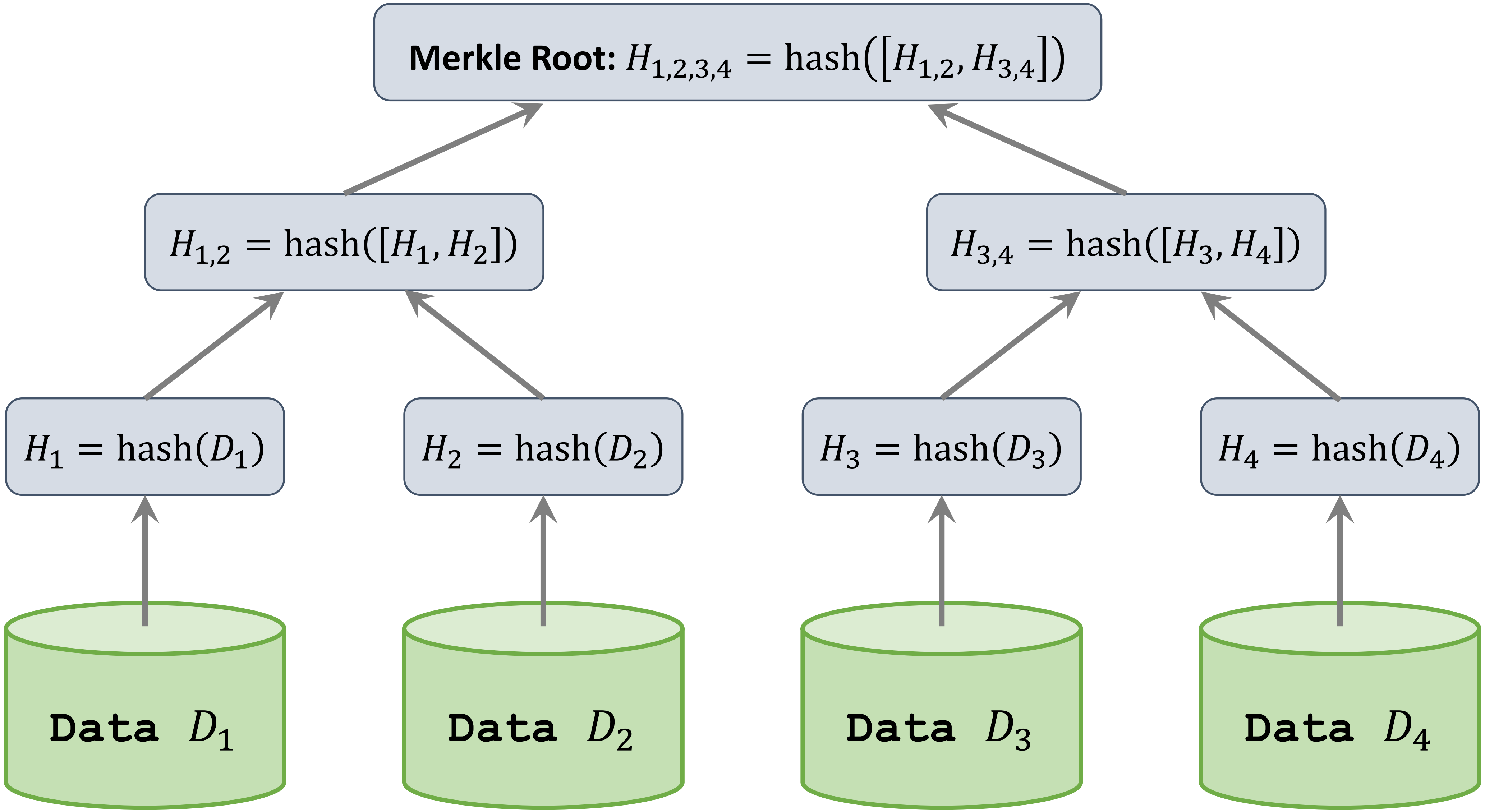
Merkel Root

Difficulty Target

Nonce

Block Header

Merkle Tree



Merkle Root: $H_{1,2,3,4} = \text{hash}\left(\left[H_{1,2}, H_{3,4}\right]\right)$

$H_{1,2} = \text{hash}([H_1, H_2])$

$H_{3,4} = \text{hash}([H_3, H_4])$

$H_1 = \text{hash}(D_1)$

$H_2 = \text{hash}(D_2)$

$H_3 = \text{hash}(D_3)$

$H_4 = \text{hash}(D_4)$

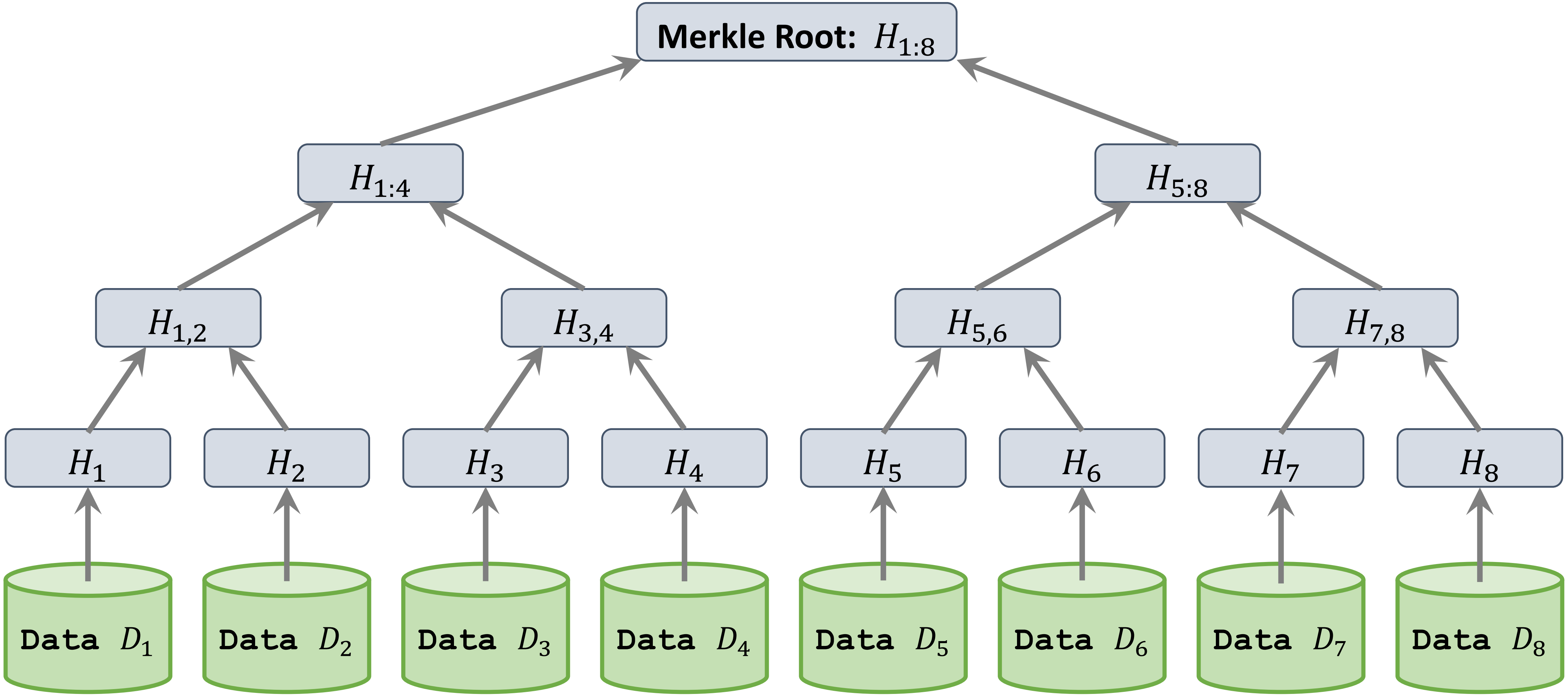
Data D_1

Data D_2

Data D_3

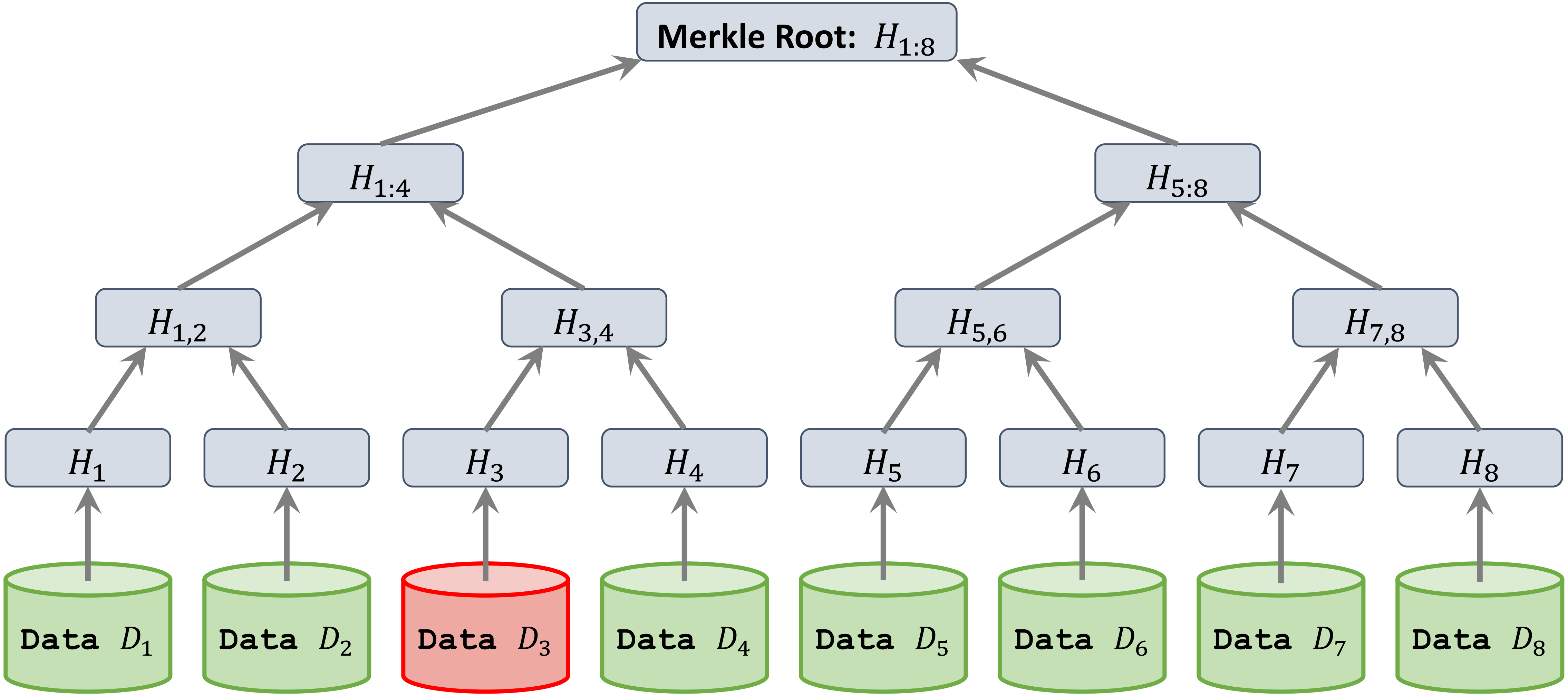
Data D_4

Merkle Tree

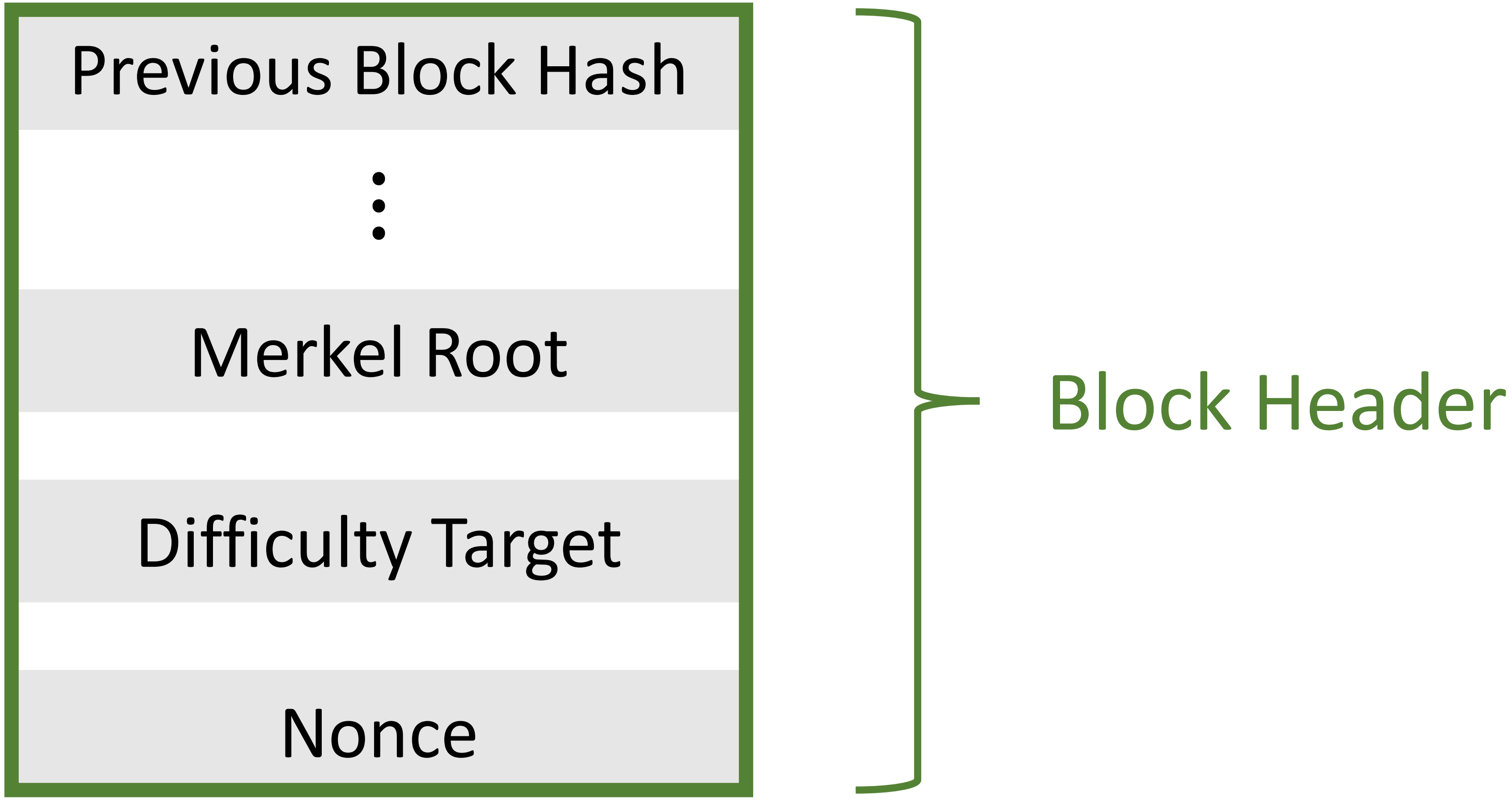


Merkle Root: $H_{1:8}$
$H_{1:4}$
$H_{5:8}$
$H_{1,2}$
$H_{3,4}$
$H_{5,6}$
$H_{7,8}$
H_1
H_2
H_3
H_4
H_5
H_6
H_7
H_8
Data D_1
Data D_2
Data D_3
Data D_4
Data D_5
Data D_6
Data D_7
Data D_8

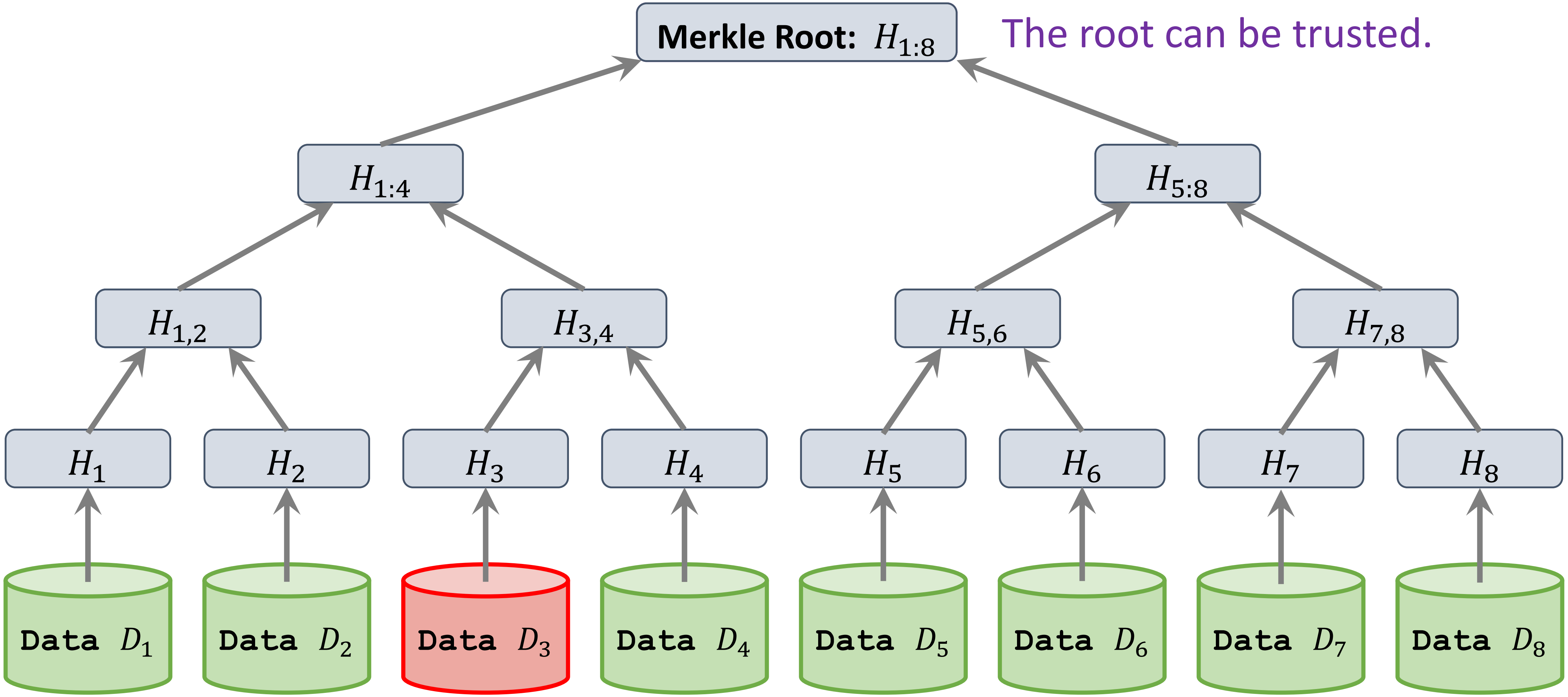
Prove a piece of data is in the Merkle tree



Block Header

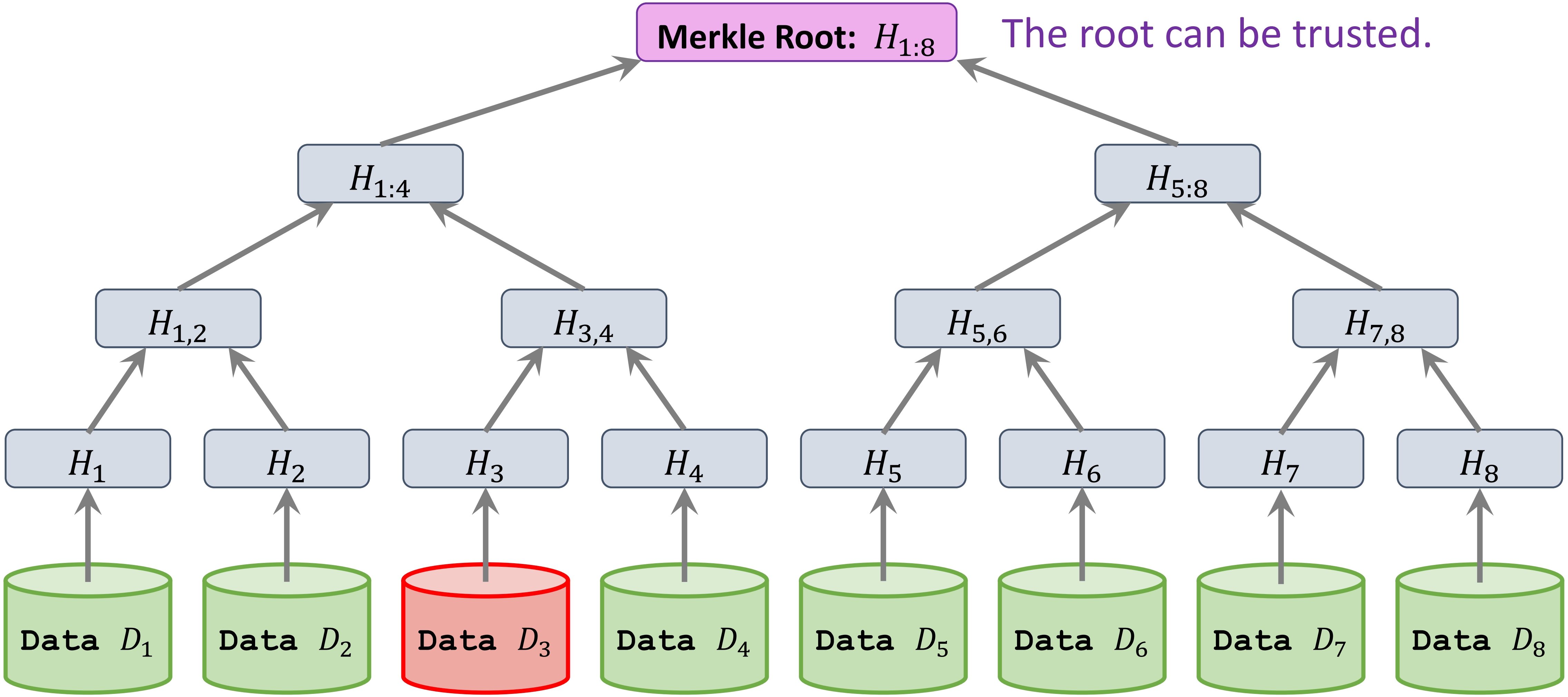


Prove a piece of data is in the Merkle tree



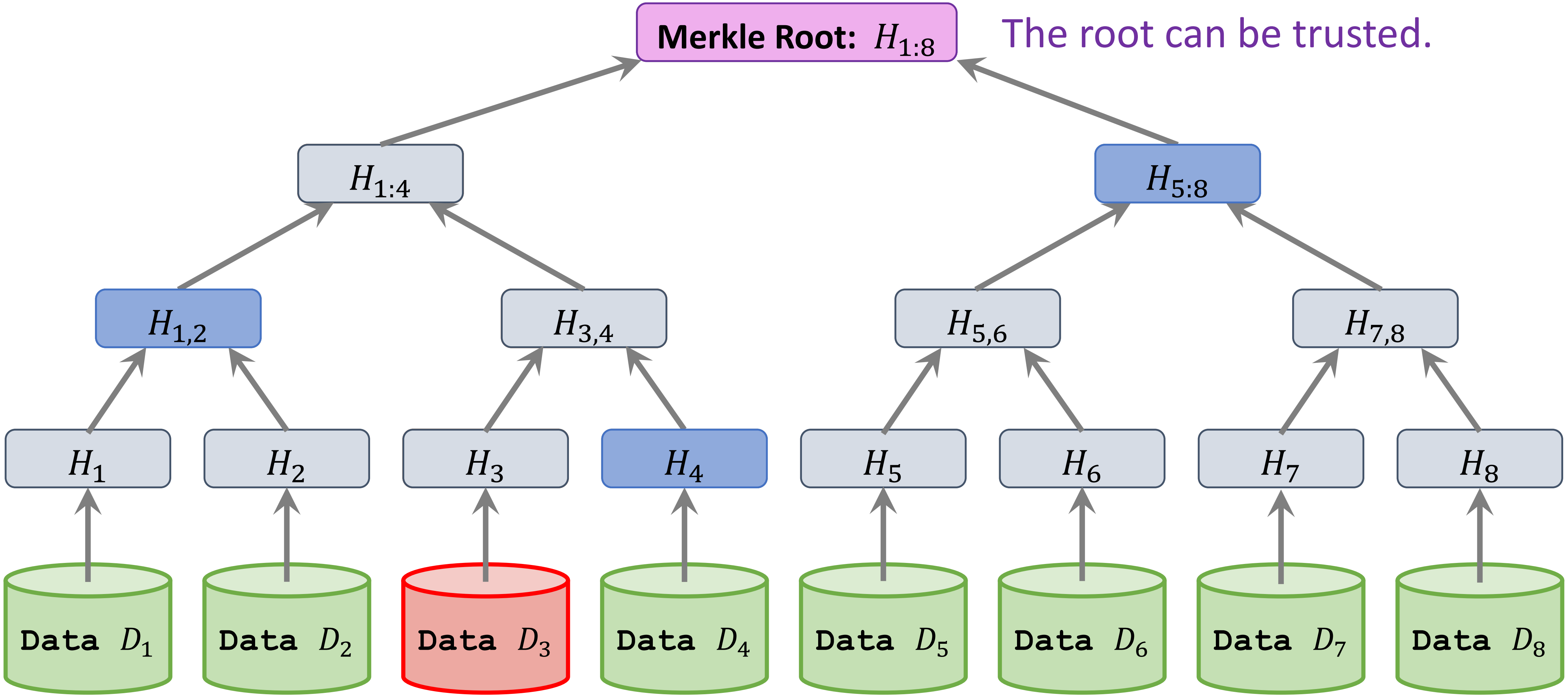
The root can be trusted.

Prove a piece of data is in the Merkle tree



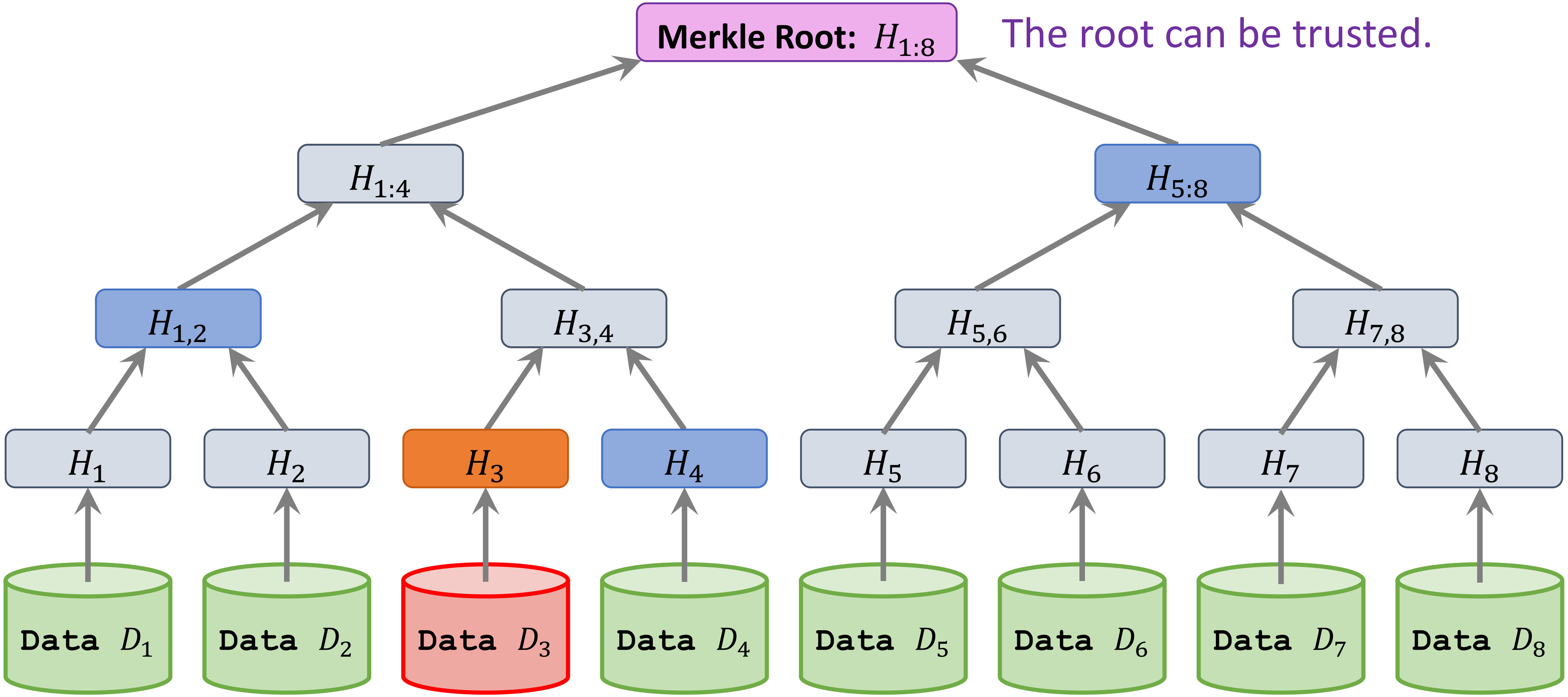
The root can be trusted.

Prove a piece of data is in the Merkle tree



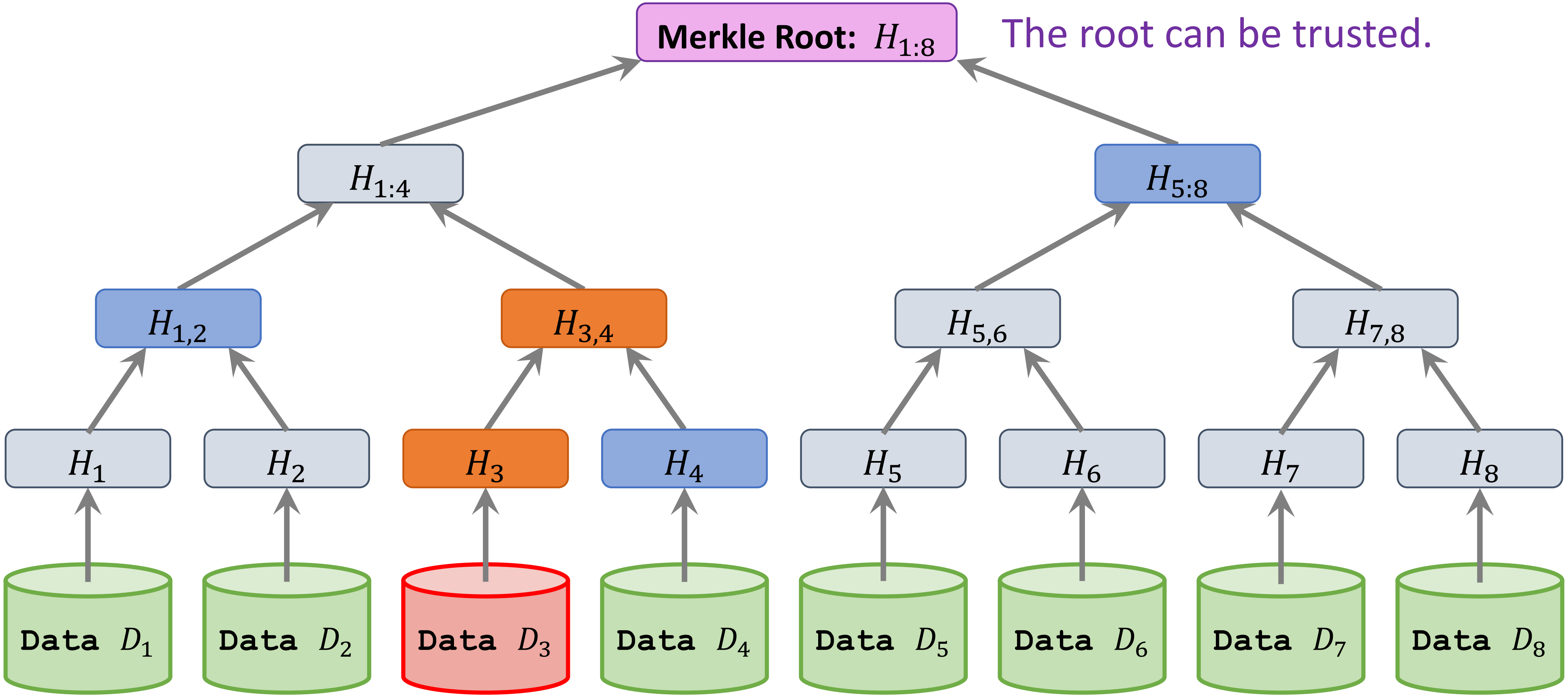
The root can be trusted.

Prove a piece of data is in the Merkle tree



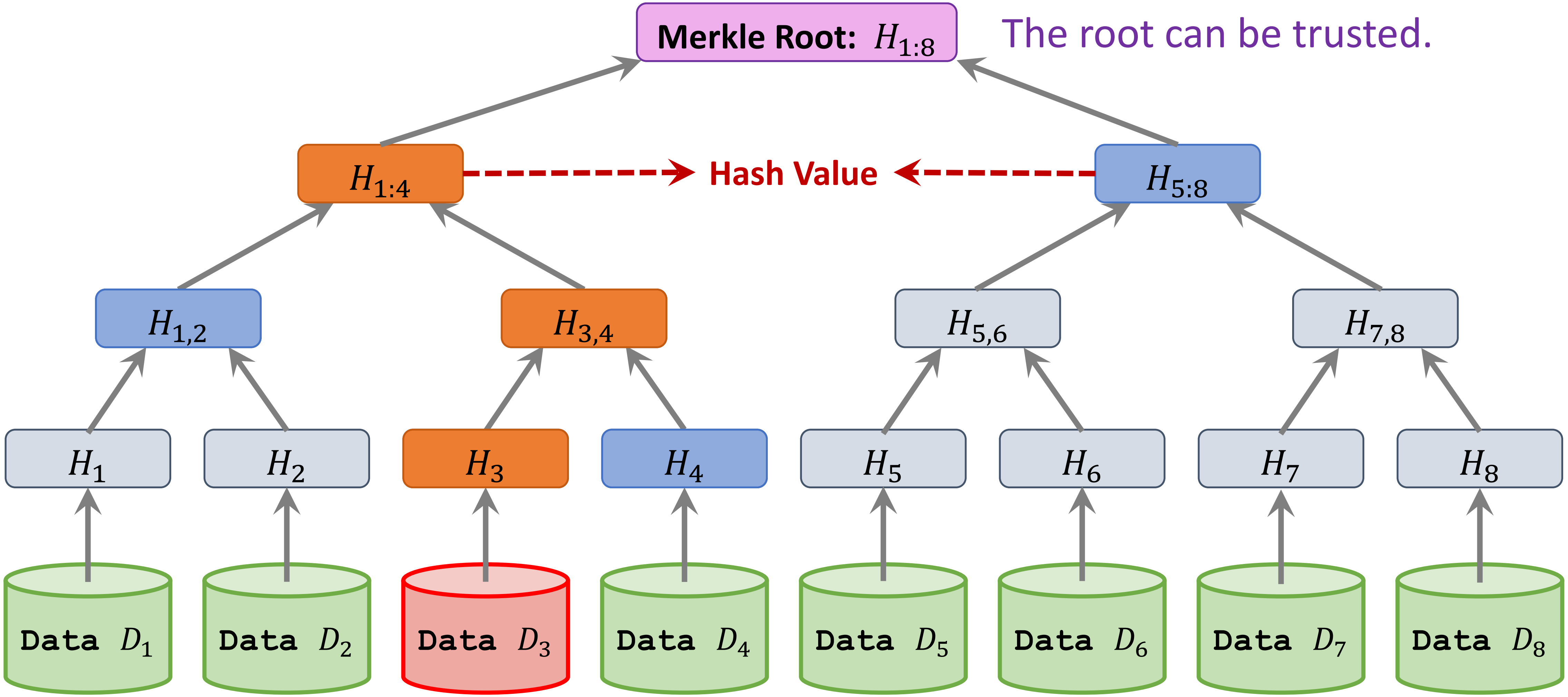
The root can be trusted.

Prove a piece of data is in the Merkle tree

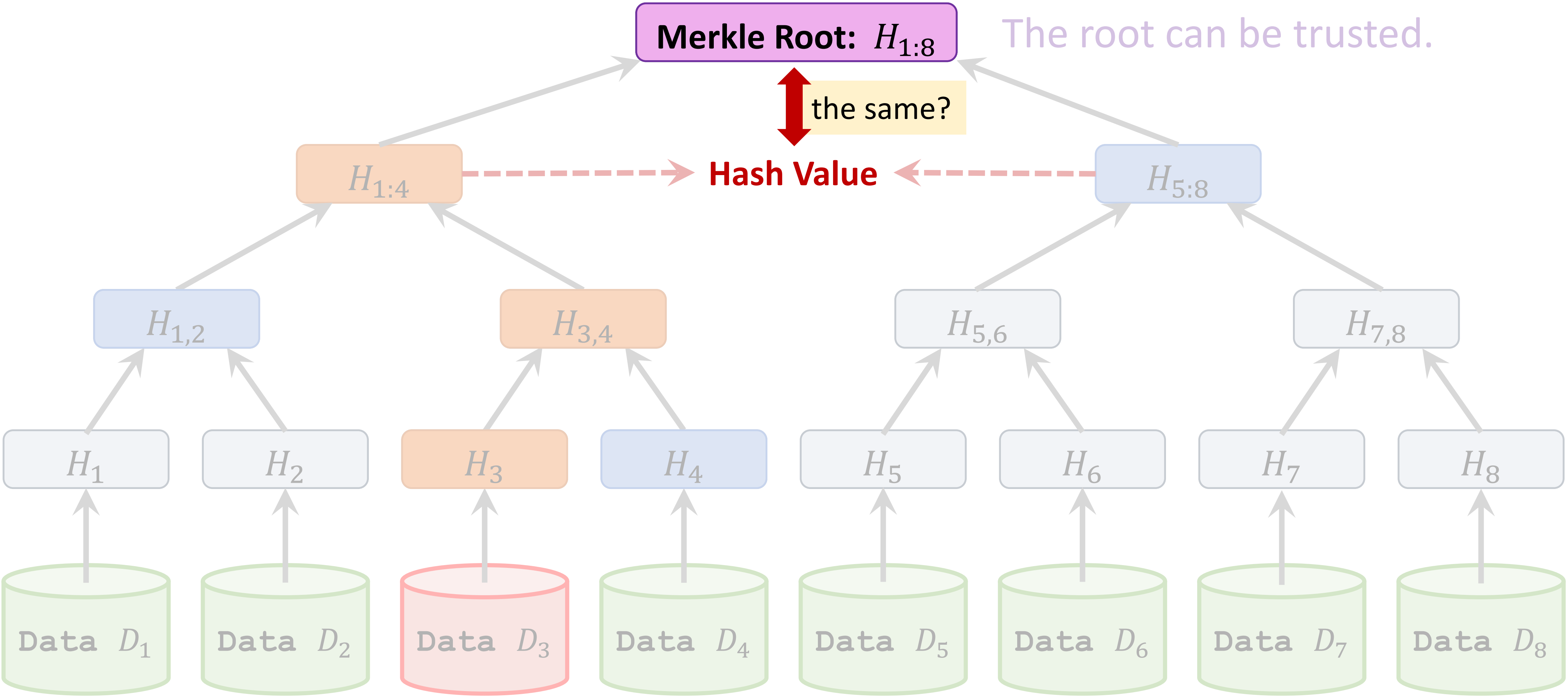


The root can be trusted.

Prove a piece of data is in the Merkle tree



Prove a piece of data is in the Merkle tree



Verify a transaction

- Alice sends Bitcoins to Bob. Alice needs to show proofs to Bob.
- Alice sends the followings to Bob:
  1. A subset of transaction data.
  2. Some hash values in the Merkel tree.

Verify a transaction

- Alice sends Bitcoins to Bob. Alice needs to show proofs to Bob.
- Alice sends the followings to Bob:
    1. A subset of transaction data.
    2. Some hash values in the Merkel tree.
- Bob downloads the block header.
- Bob performs verifications:
    1. SHA-256 of the block header must match difficulty target, e.g., 76 zeros.
    2. Data sent by Alice matches the Merkel root.

Thank You!