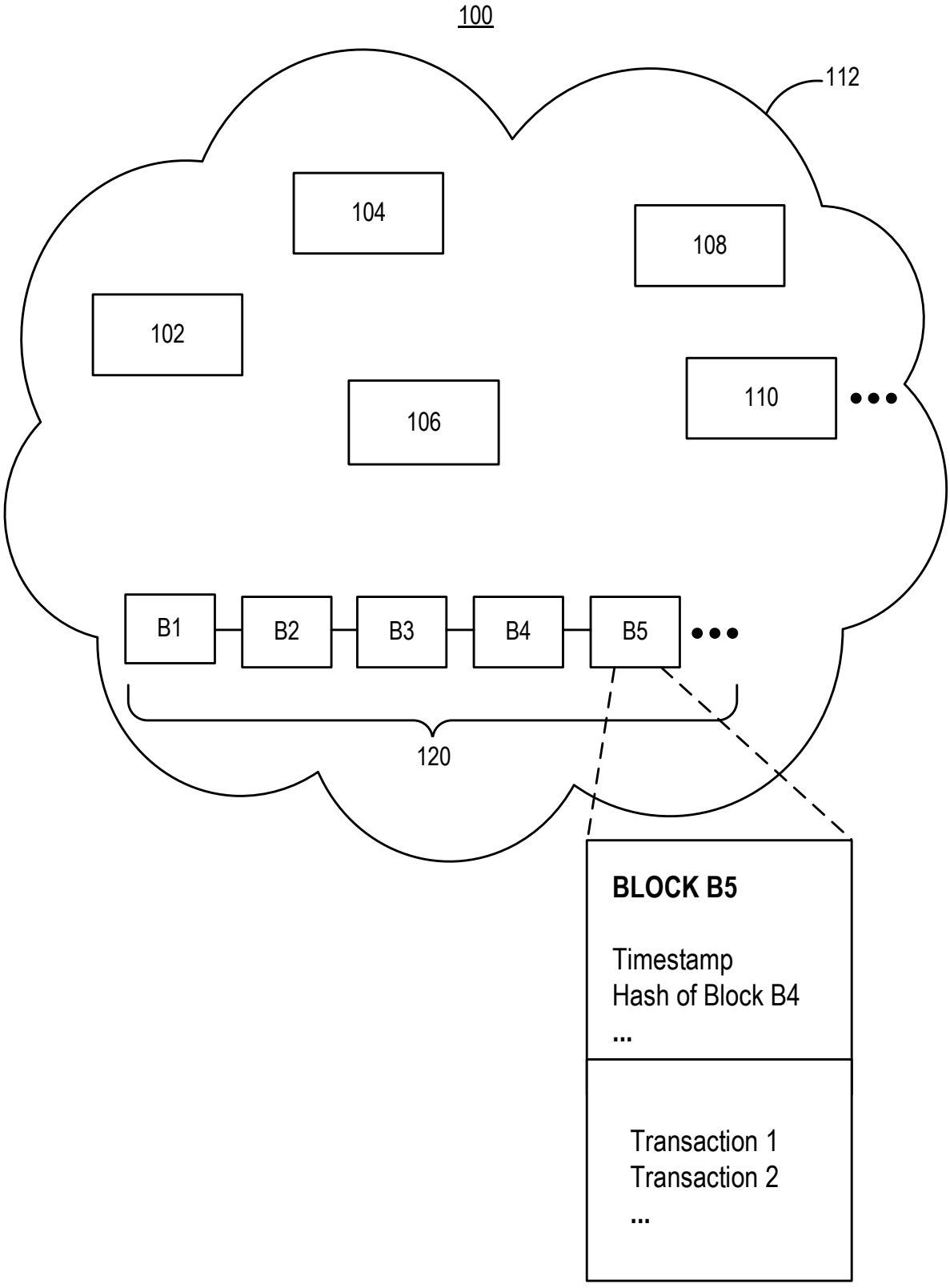
100
112
104
108
102
106
110
B1
B2
B3
B4
B5
120
BLOCK B5
Timestamp
Hash of Block B4
...
Transaction 1
Transaction 2
...

FIG. 1

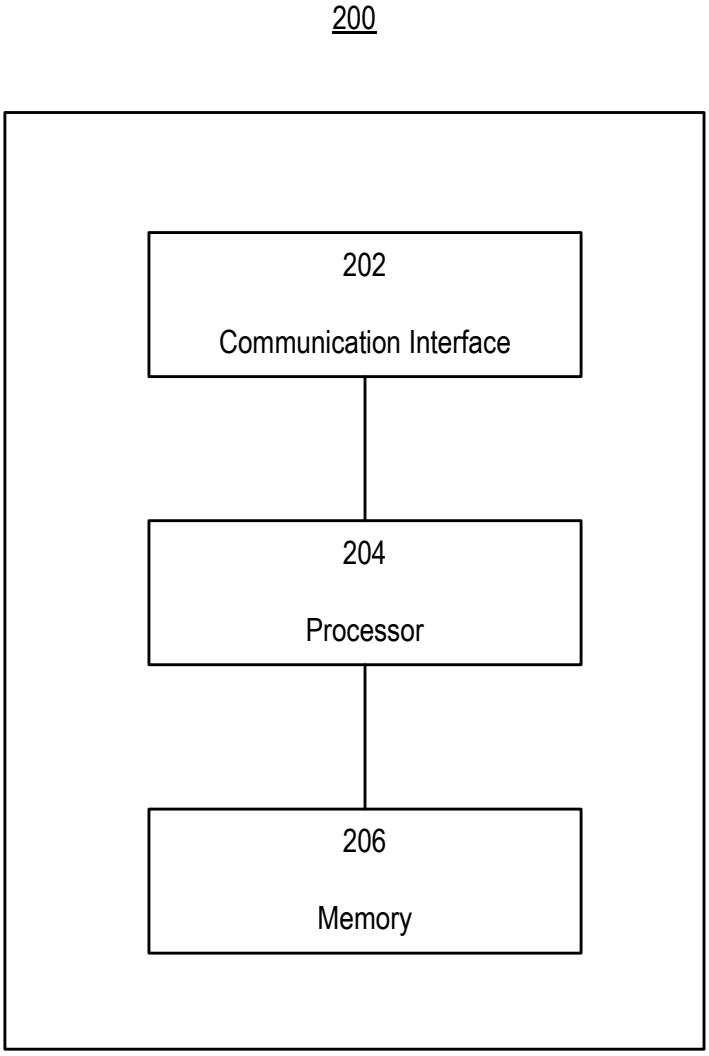

FIG. 2

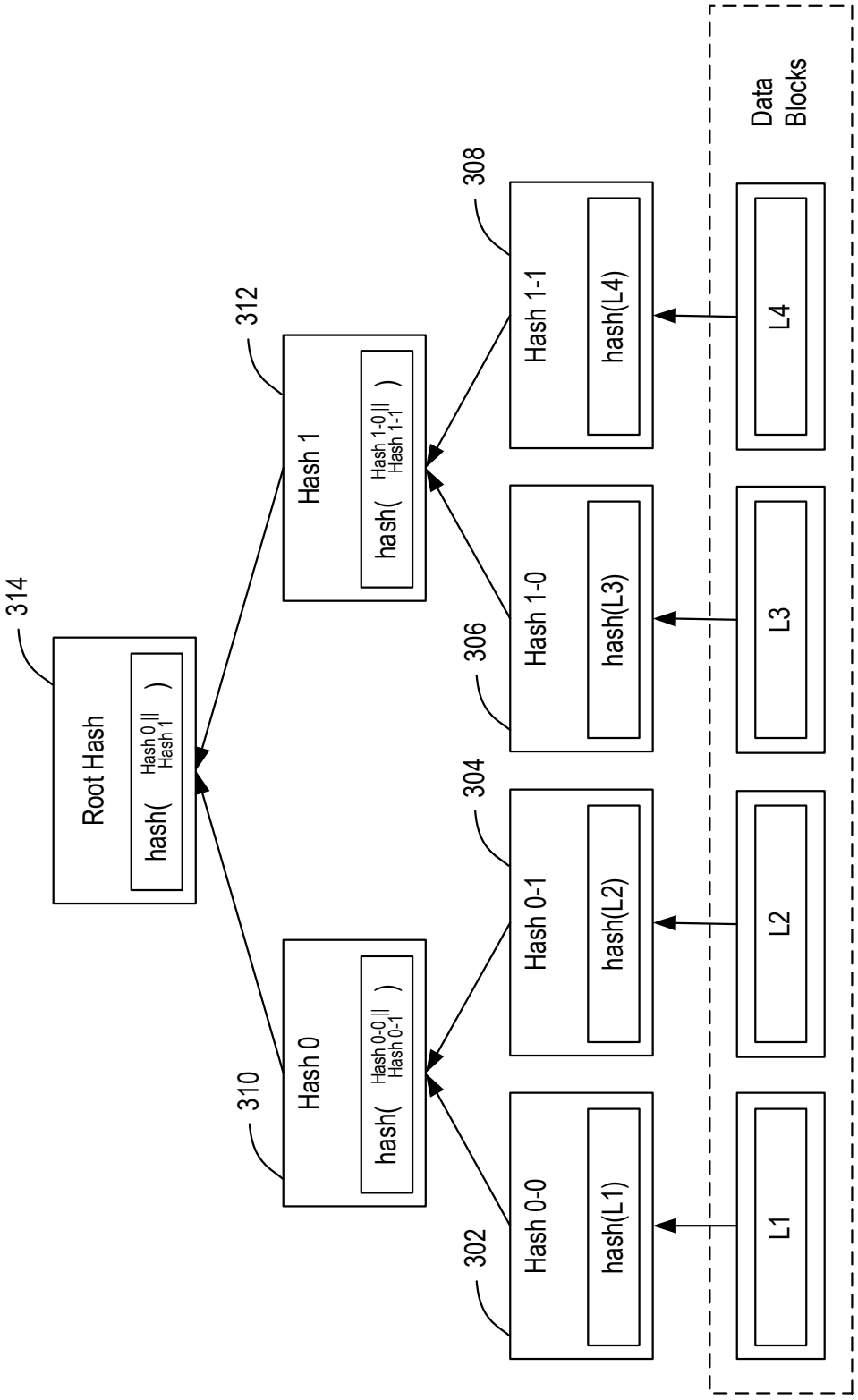
Root Hash
hash(Hash 0 || Hash 1)
314
Hash 0
hash(Hash 0-0 || Hash 0-1)
310
Hash 1
hash(Hash 1-0 || Hash 1-1)
312
Hash 0-0
hash(L1)
302
Hash 0-1
hash(L2)
304
Hash 1-0
hash(L3)
306
Hash 1-1
hash(L4)
308
L1
L2
L3
L4
Data Blocks

FIG. 3

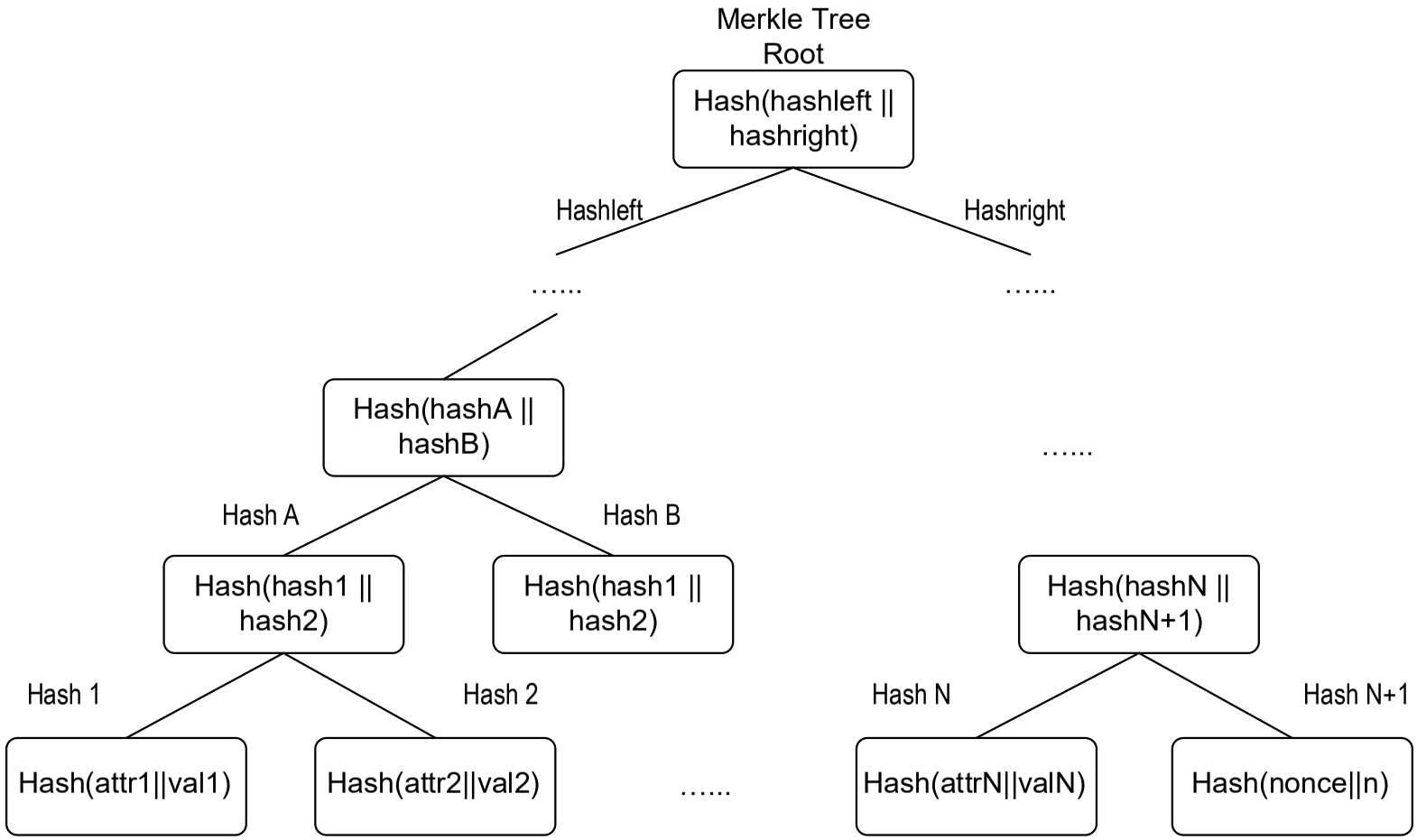
Merkle Tree Root
Hash(hashleft || hashright)
Hashleft
Hashright
.....
.....
Hash(hashA || hashB)
.....
Hash A
Hash B
Hash(hash1 || hash2)
Hash(hash1 || hash2)
Hash(hashN || hashN+1)
Hash 1
Hash 2
Hash N
Hash N+1
Hash(attr1||val1)
Hash(attr2||val2)
.....
Hash(attrN||valN)
Hash(nonce||n)

FIG. 4

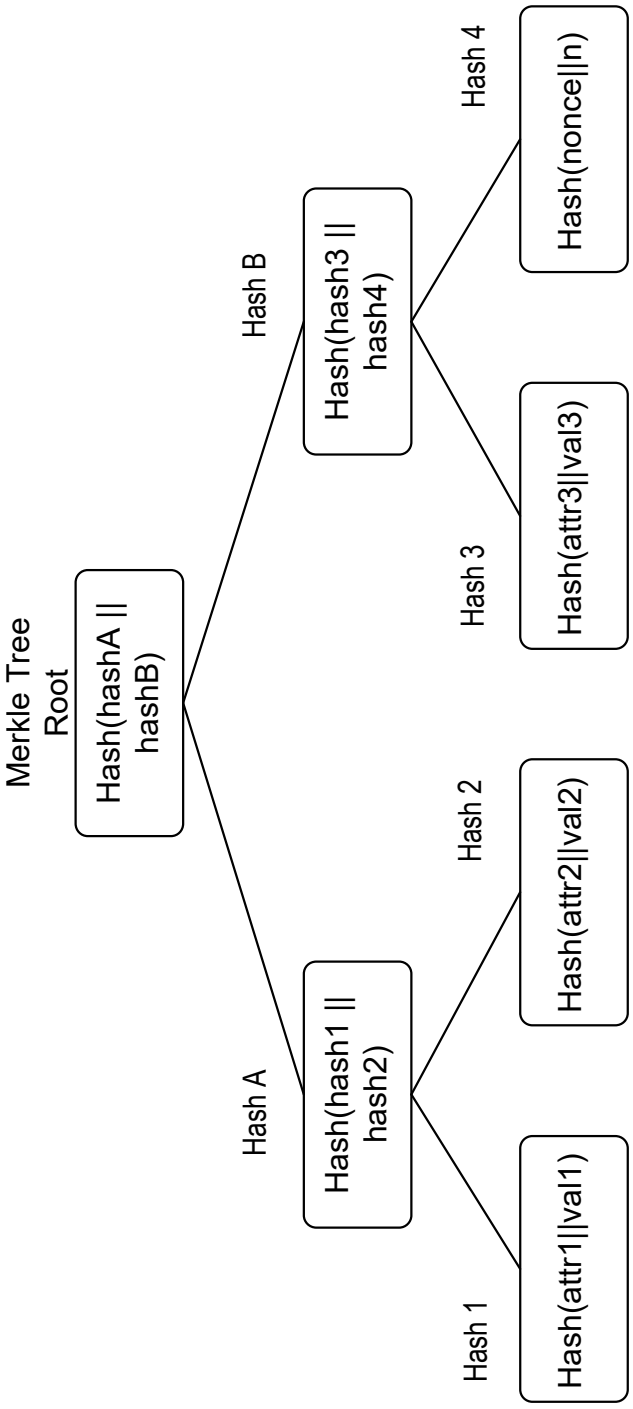
Merkle Tree Root
Hash(hashA || hashB)
Hash A
Hash(hash1 || hash2)
Hash B
Hash(hash3 || hash4)
Hash 1
Hash(attr1||val1)
Hash 2
Hash(attr2||val2)
Hash 3
Hash(attr3||val3)
Hash 4
Hash(nonce||n)

FIG. 5

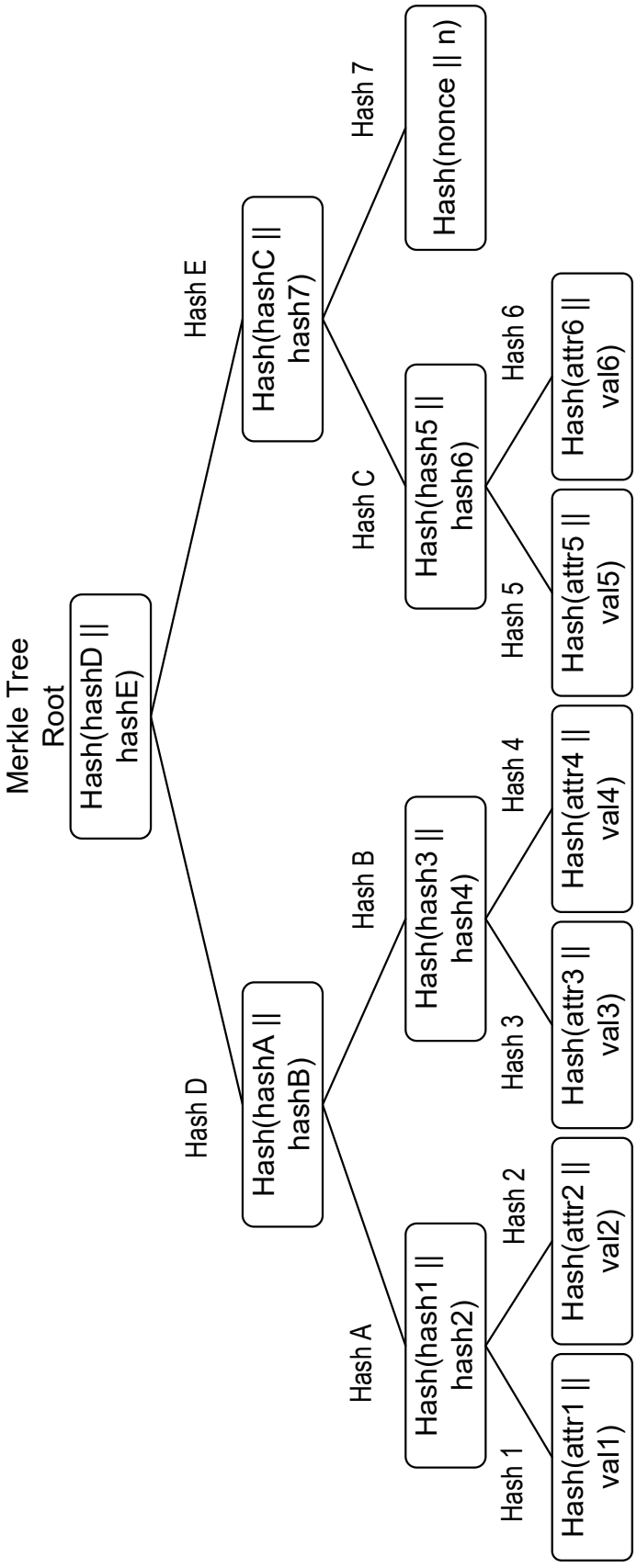
Merkle Tree Root
Hash(hashD || hashE)
Hash D
Hash E
Hash(hashA || hashB)
Hash(hashC || hash7)
Hash A
Hash B
Hash C
Hash 7
Hash(hash1 || hash2)
Hash(hash3 || hash4)
Hash(hash5 || hash6)
Hash(nonce || n)
Hash 1
Hash 2
Hash 3
Hash 4
Hash 5
Hash 6
Hash(attr1 || val1)
Hash(attr2 || val2)
Hash(attr3 || val3)
Hash(attr4 || val4)
Hash(attr5 || val5)
Hash(attr6 || val6)

FIG. 6

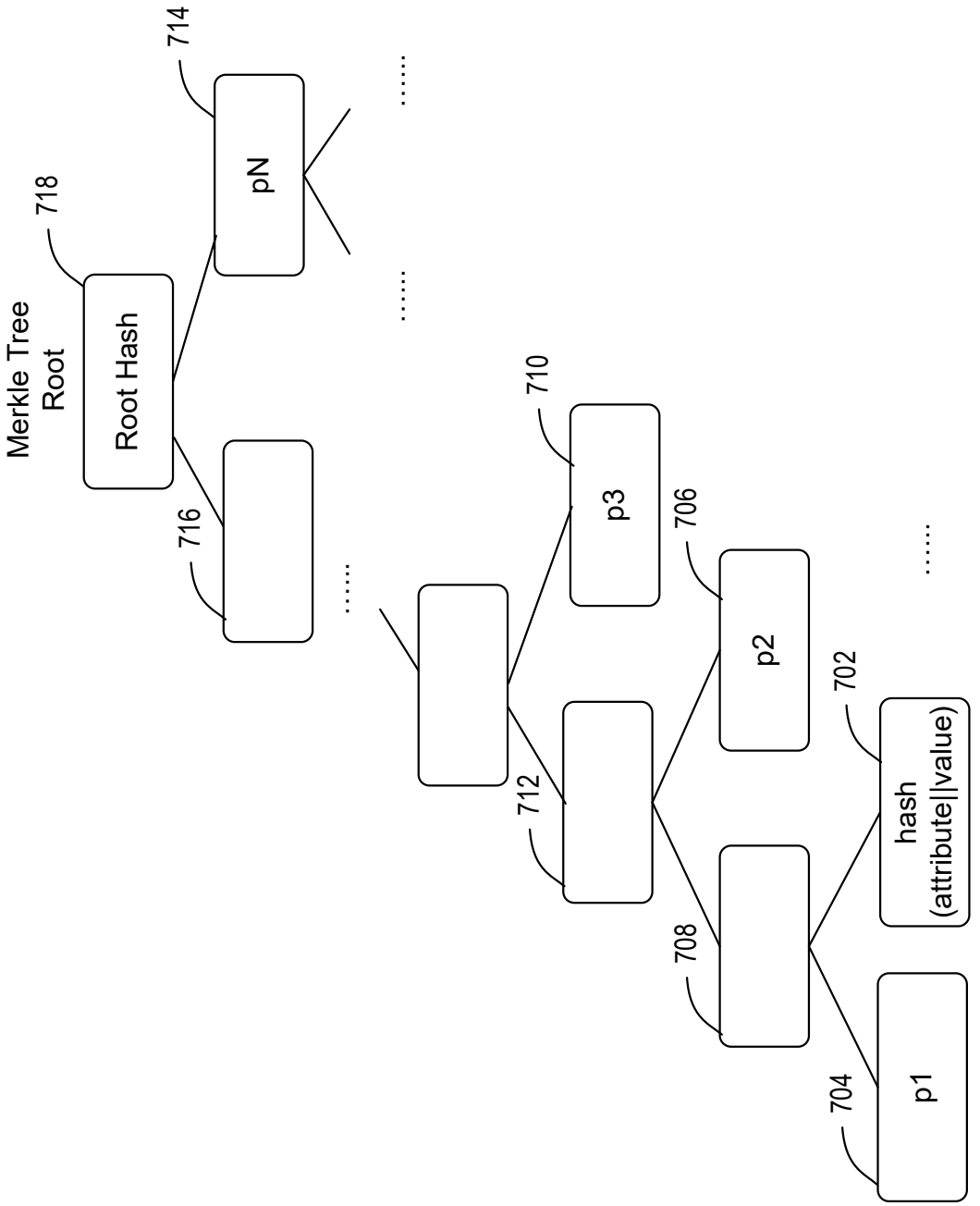
Merkle Tree Root
Root Hash
718
714
pN
716
710
p3
706
p2
712
702
hash (attribute||value)
708
704
p1

FIG. 7

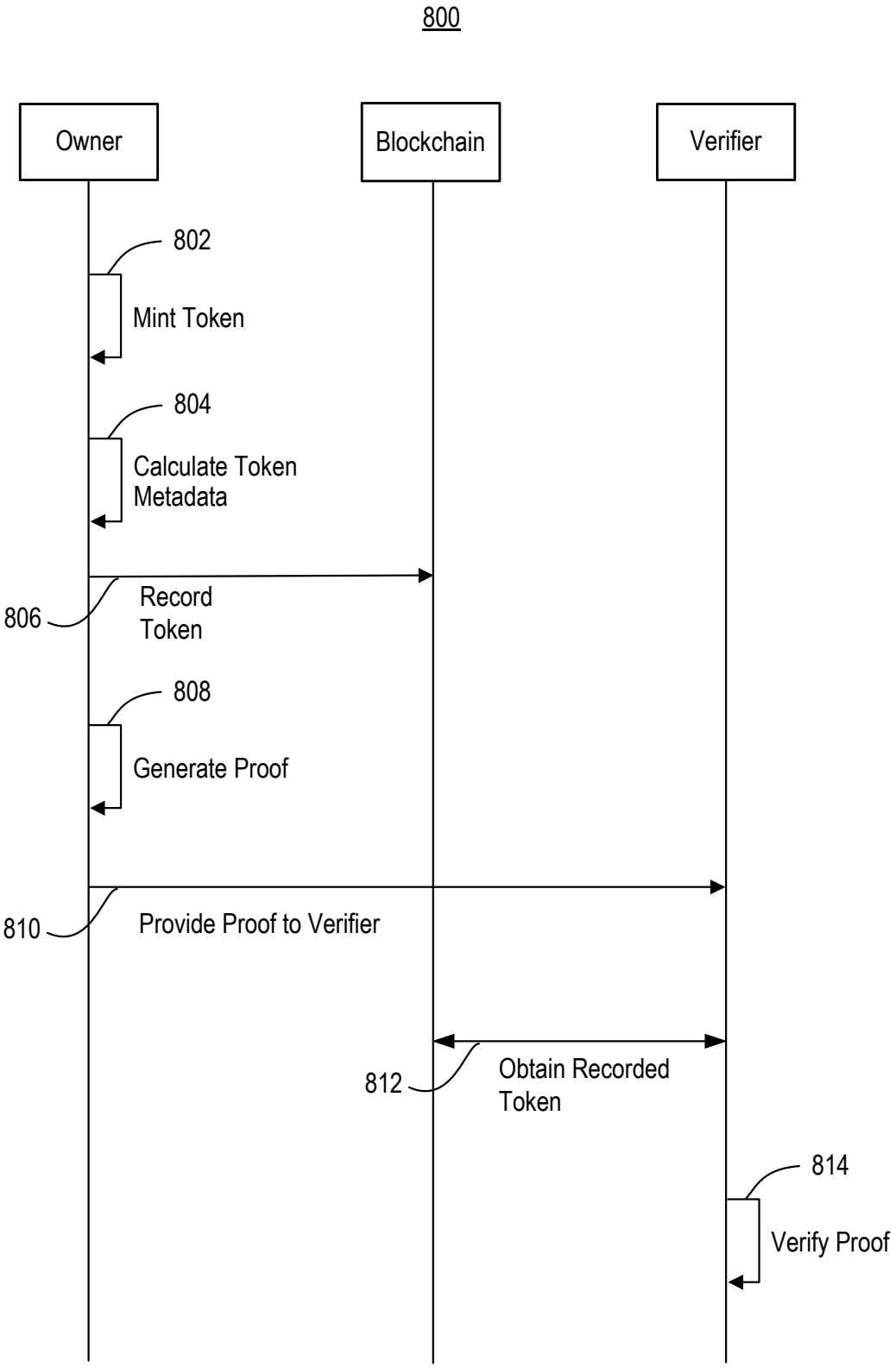
800
Owner
Blockchain
Verifier
802
Mint Token
804
Calculate Token Metadata
806
Record Token
808
Generate Proof
810
Provide Proof to Verifier
812
Obtain Recorded Token
814
Verify Proof

FIG. 8

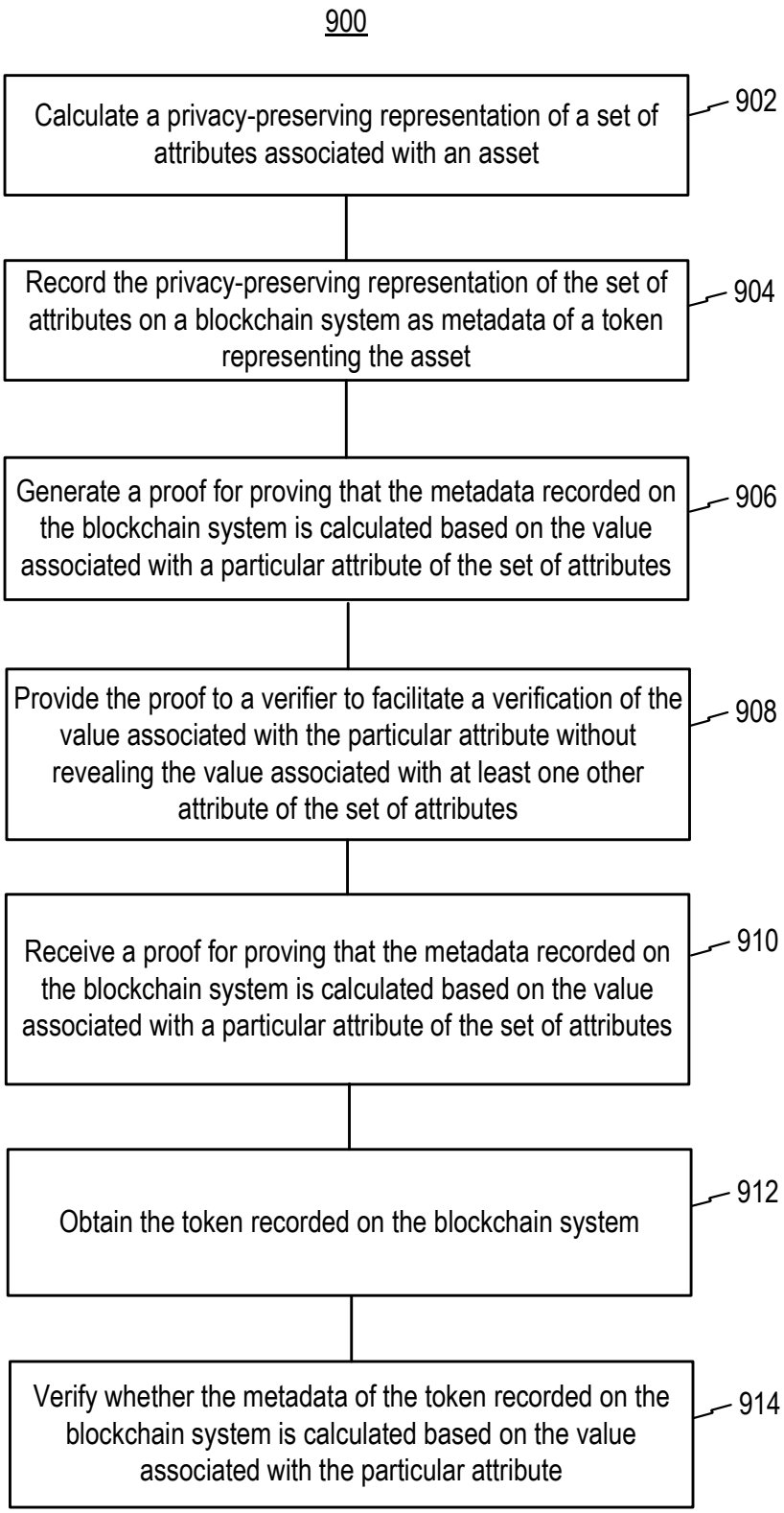
900
Calculate a privacy-preserving representation of a set of attributes associated with an asset
902
Record the privacy-preserving representation of the set of attributes on a blockchain system as metadata of a token representing the asset
904
Generate a proof for proving that the metadata recorded on the blockchain system is calculated based on the value associated with a particular attribute of the set of attributes
906
Provide the proof to a verifier to facilitate a verification of the value associated with the particular attribute without revealing the value associated with at least one other attribute of the set of attributes
908
Receive a proof for proving that the metadata recorded on the blockchain system is calculated based on the value associated with a particular attribute of the set of attributes
910
Obtain the token recorded on the blockchain system
912
Verify whether the metadata of the token recorded on the blockchain system is calculated based on the value associated with the particular attribute
914

FIG. 9

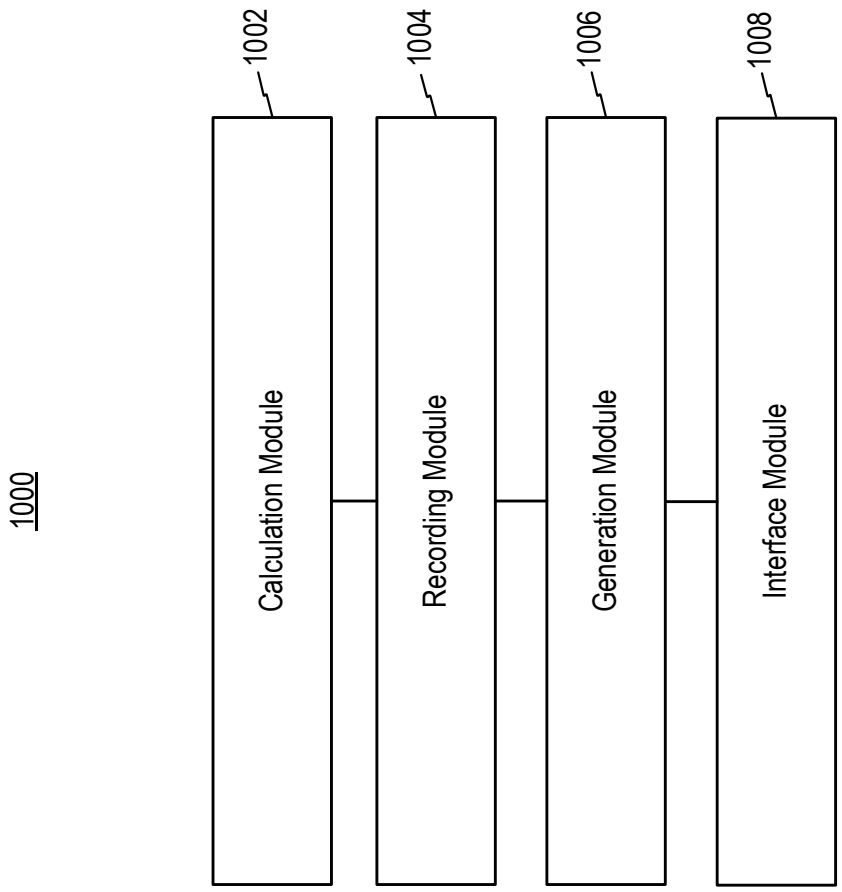
1000
1002
Calculation Module
1004
Recording Module
1006
Generation Module
1008
Interface Module

FIG. 10