Figure 1

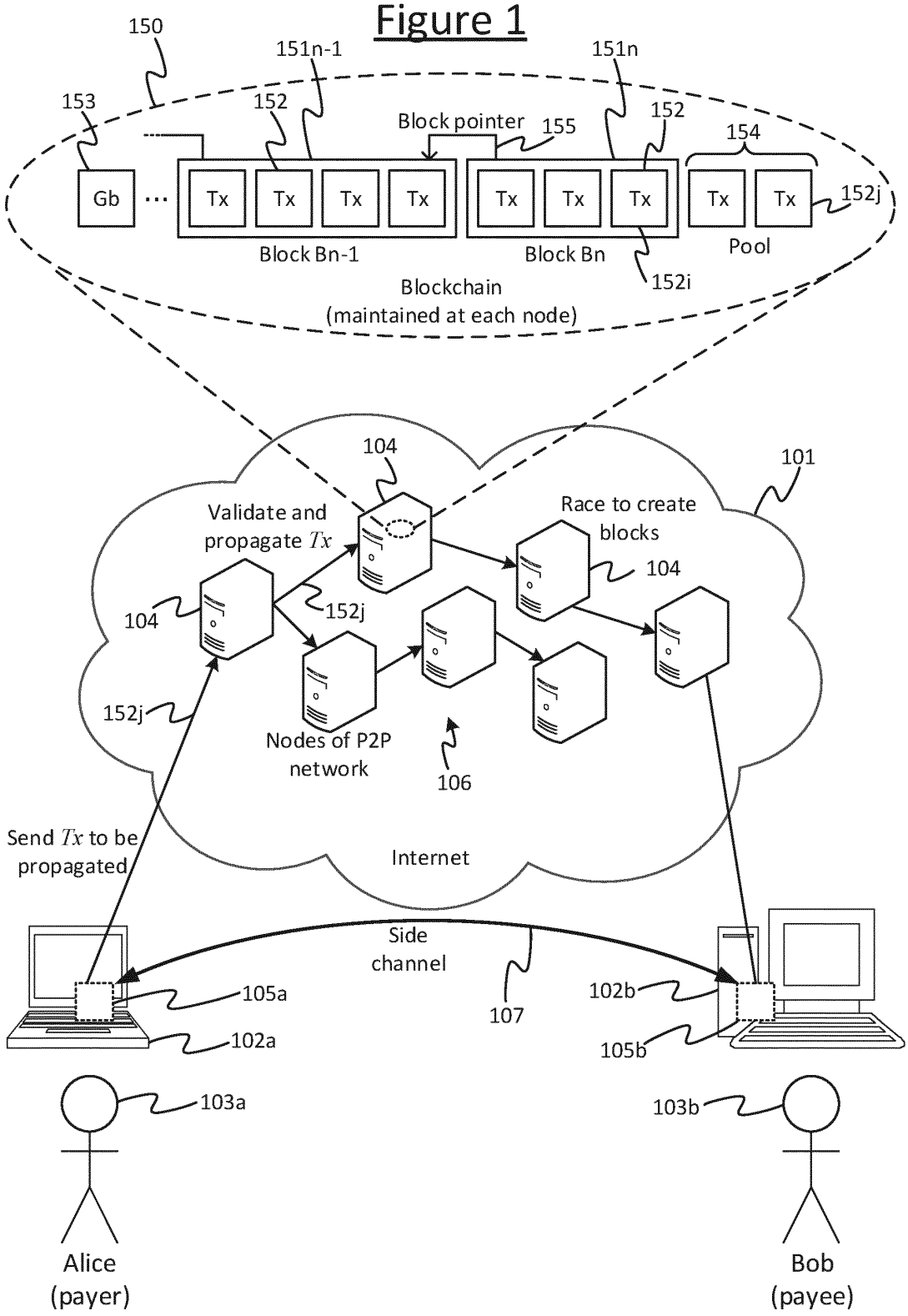
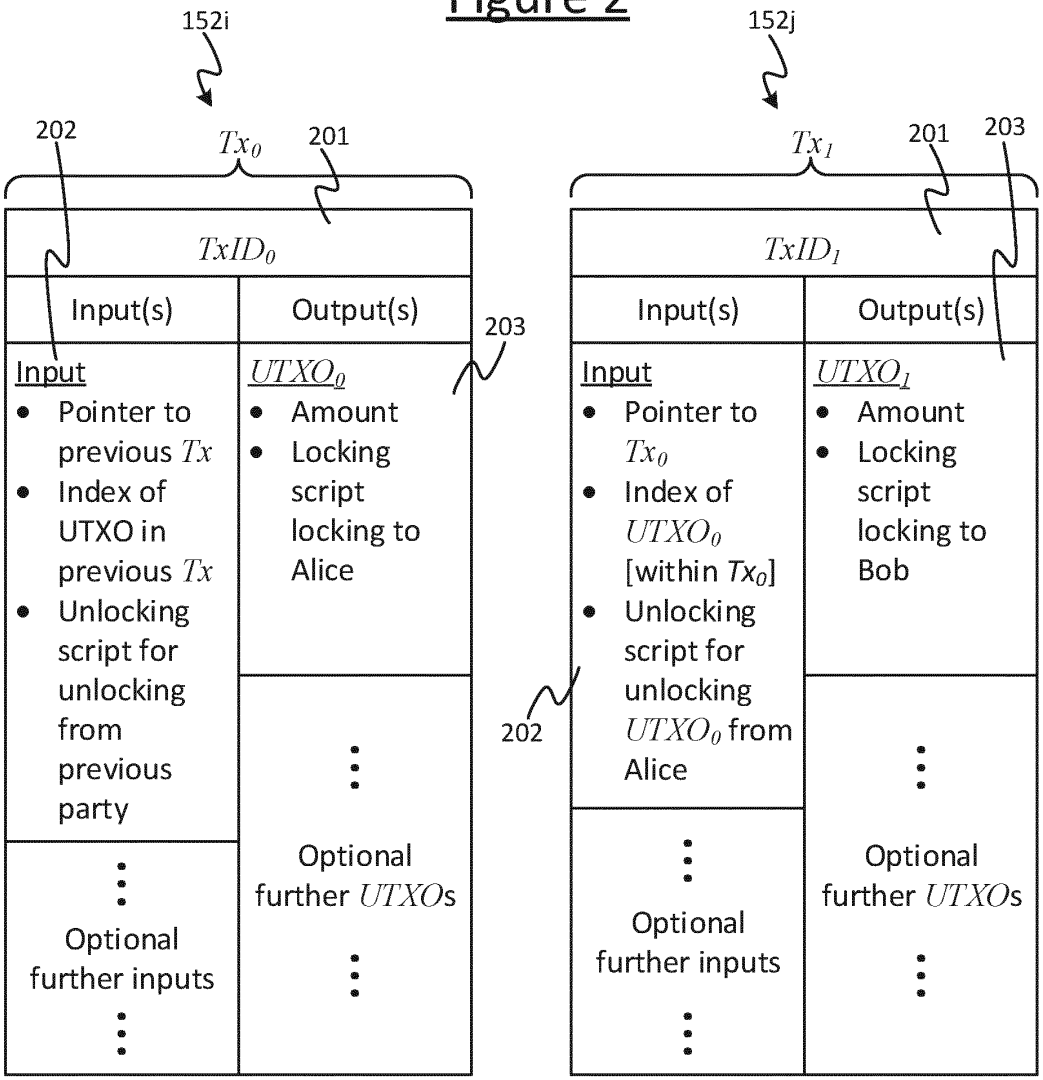

150
151n-1
151n
153
152
Block pointer
155
152
154
Gb
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
152j
Block Bn-1
Block Bn
Pool
152i
Blockchain
(maintained at each node)
104
101
Validate and
propagate Tx
Race to create
blocks
104
104
152j
152j
Nodes of P2P
network
106
Send Tx to be
propagated
Internet
Side
channel
107
105a
102a
102b
105b
103a
103b
Alice
(payer)
Bob
(payee)

Figure 2



Transaction from Alice to Bob

Validated by running: Locking script from output 203 of Tx_0, together with Alice's unlocking script from input 202 of Tx_1. This checks that Alice's unlocking script in Tx_1 meets the condition(s) defined in the locking script of previous transaction Tx_0.

Figure 3

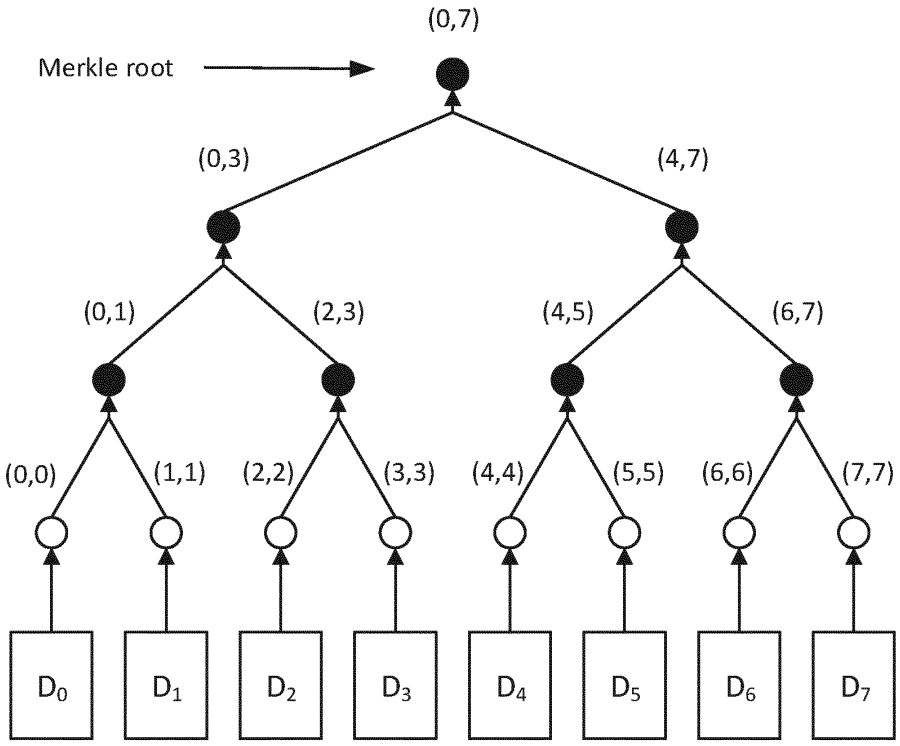

(0,7)
Merkle root
(0,3)
(4,7)
(0,1)
(2,3)
(4,5)
(6,7)
(0,0)
(1,1)
(2,2)
(3,3)
(4,4)
(5,5)
(6,6)
(7,7)
D0
D1
D2
D3
D4
D5
D6
D7

Figure 4

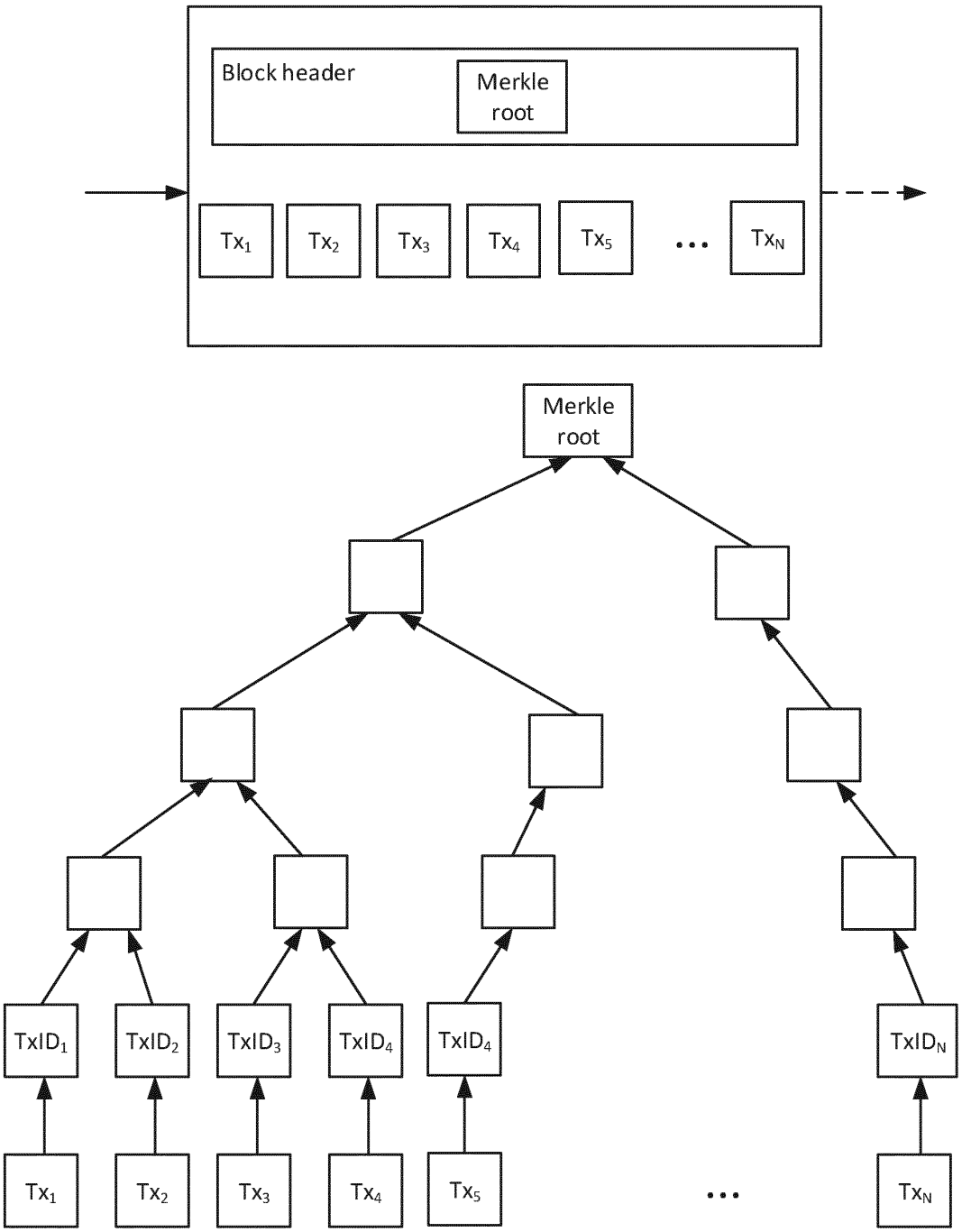

Block header
Merkle root
Tx1
Tx2
Tx3
Tx4
Tx5
...
TxN
Merkle root
TxID1
TxID2
TxID3
TxID4
TxID4
TxIDN
Tx1
Tx2
Tx3
Tx4
Tx5
...
TxN

Figure 5

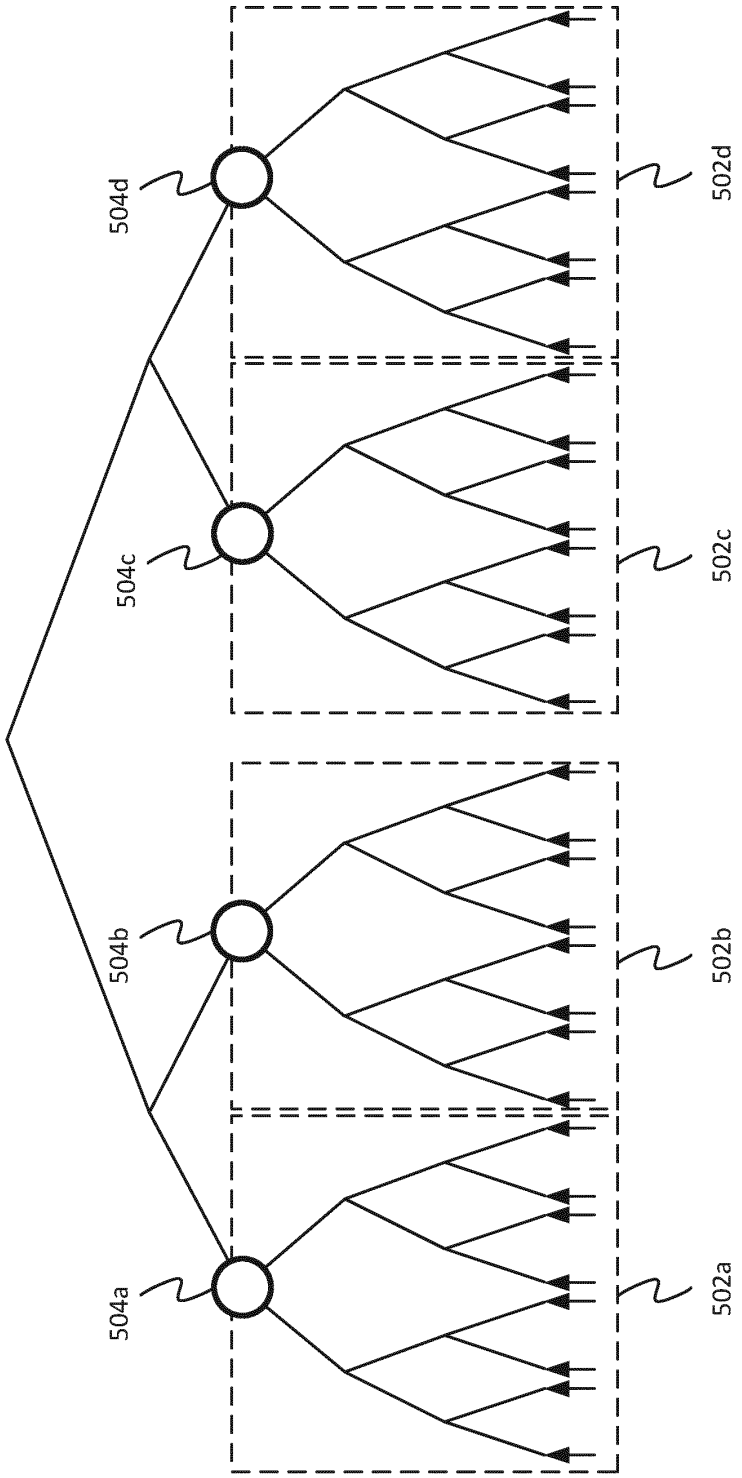


Figure 6

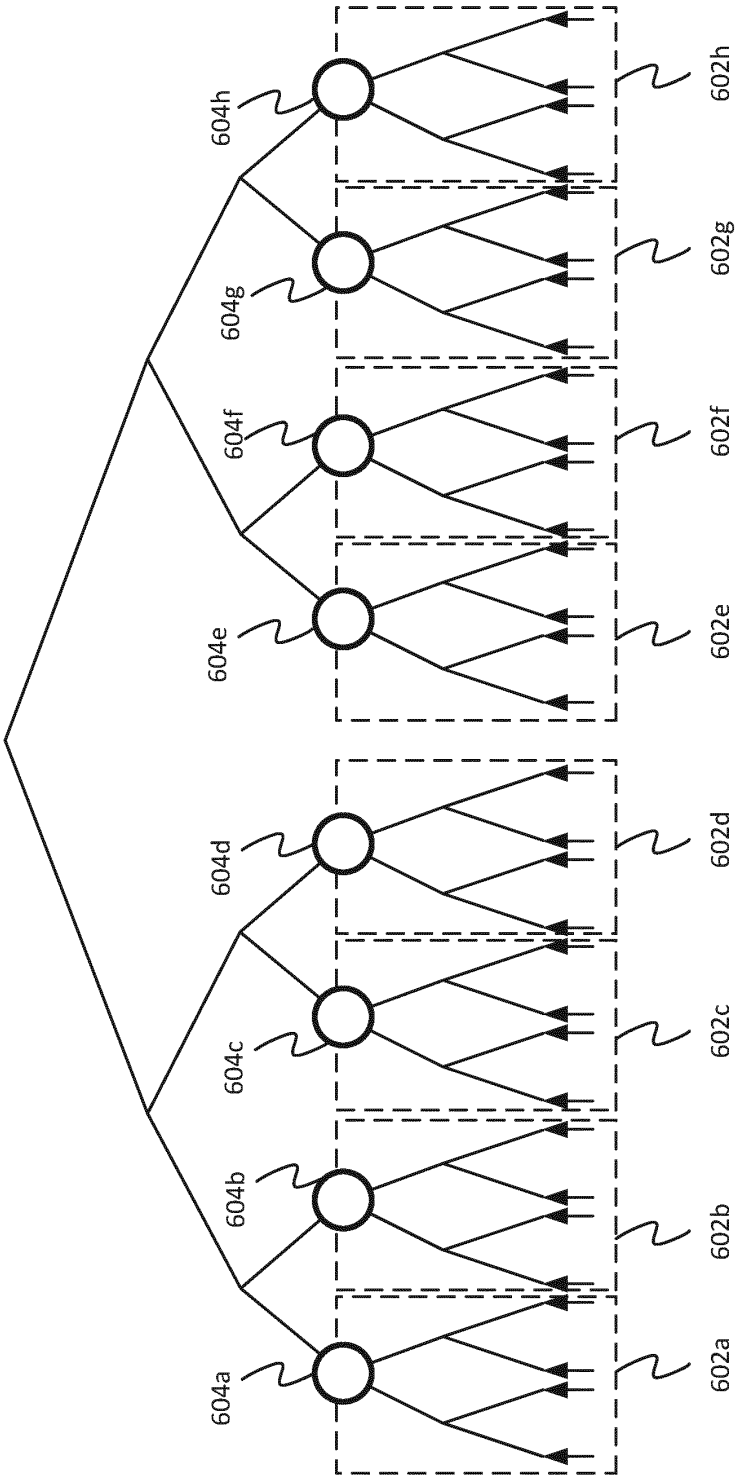

604h
602h
604g
602g
604f
602f
604e
602e
604d
602d
604c
602c
604b
602b
604a
602a

Figure 7

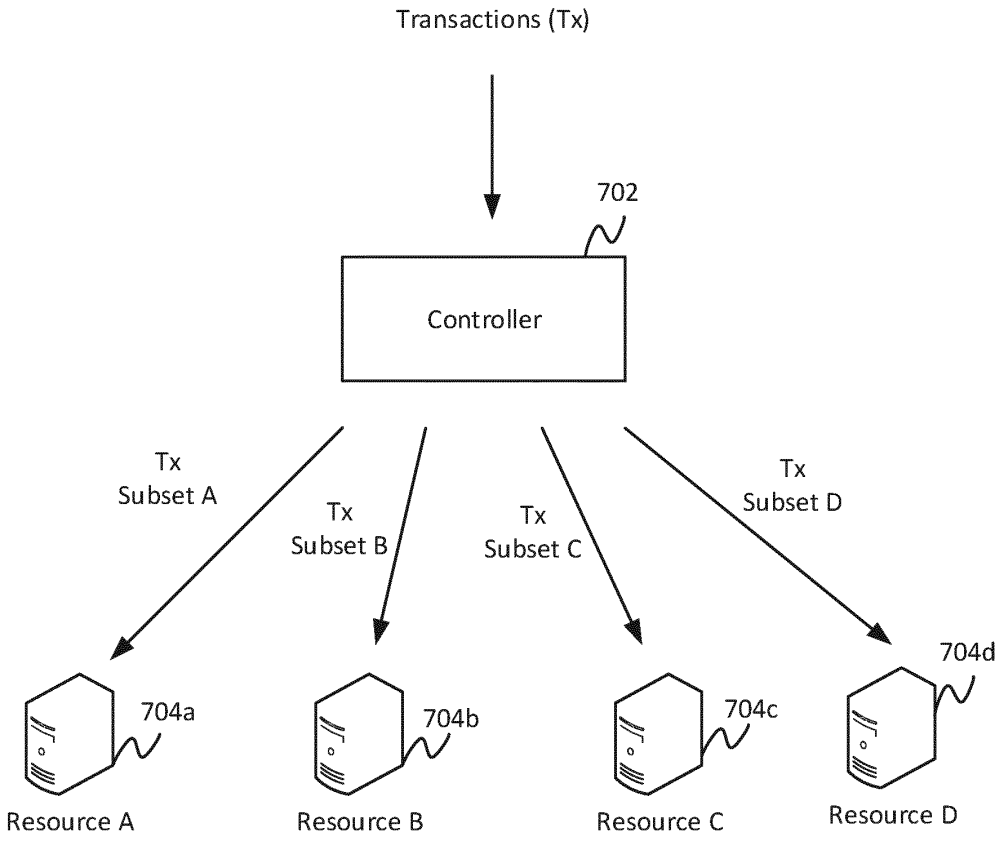

Transactions (Tx)
702
Controller
Tx
Subset A
Tx
Subset B
Tx
Subset C
Tx
Subset D
704a
704b
704c
704d
Resource A
Resource B
Resource C
Resource D

Figure 8

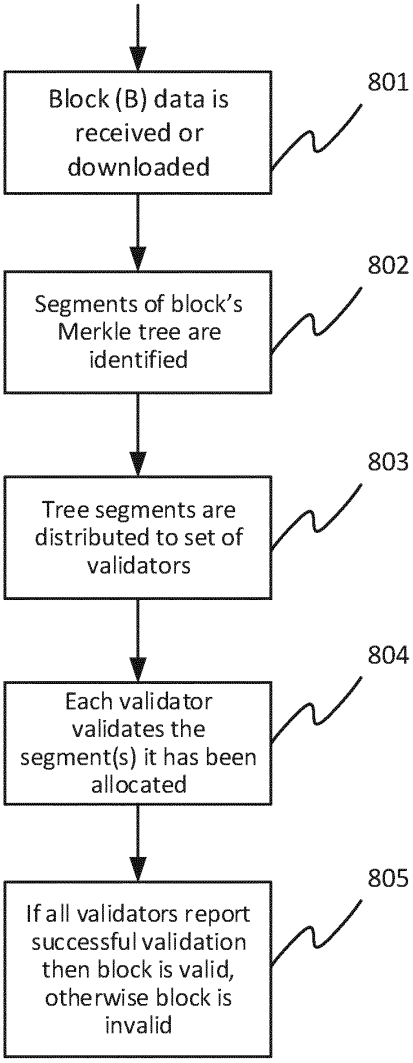

Block (B) data is received or downloaded
801
Segments of block's Merkle tree are identified
802
Tree segments are distributed to set of validators
803
Each validator validates the segment(s) it has been allocated
804
If all validators report successful validation then block is valid, otherwise block is invalid
805

Figure 9

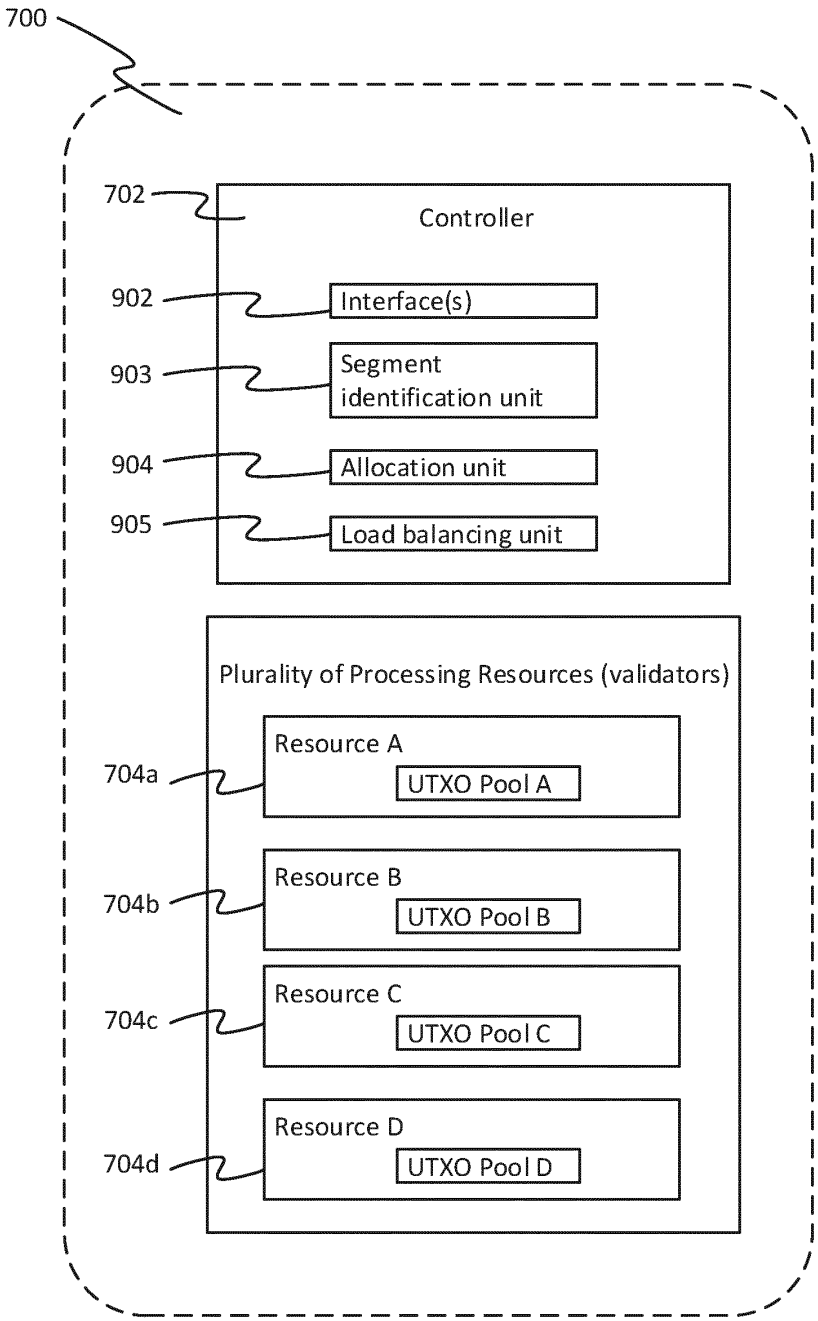

700
702
Controller
902
Interface(s)
903
Segment identification unit
904
Allocation unit
905
Load balancing unit
Plurality of Processing Resources (validators)
704a
Resource A
UTXO Pool A
704b
Resource B
UTXO Pool B
704c
Resource C
UTXO Pool C
704d
Resource D
UTXO Pool D

Figure 10

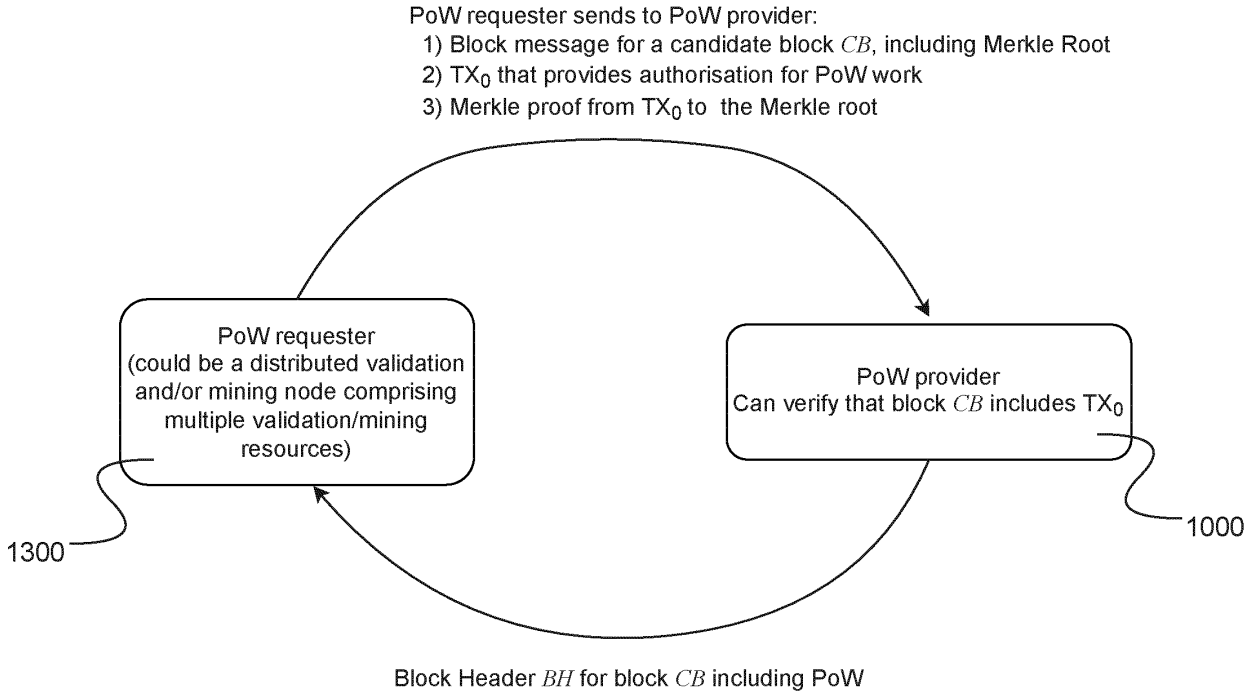

PoW requester sends to PoW provider:
1) Block message for a candidate block CB, including Merkle Root
2) TX0 that provides authorisation for PoW work
3) Merkle proof from TX0 to the Merkle root
PoW requester
(could be a distributed validation and/or mining node comprising multiple validation/mining resources)
PoW provider
Can verify that block CB includes TX0
1300
1000
Block Header BH for block CB including PoW

Figure 11 *(prior art - block mining process)*

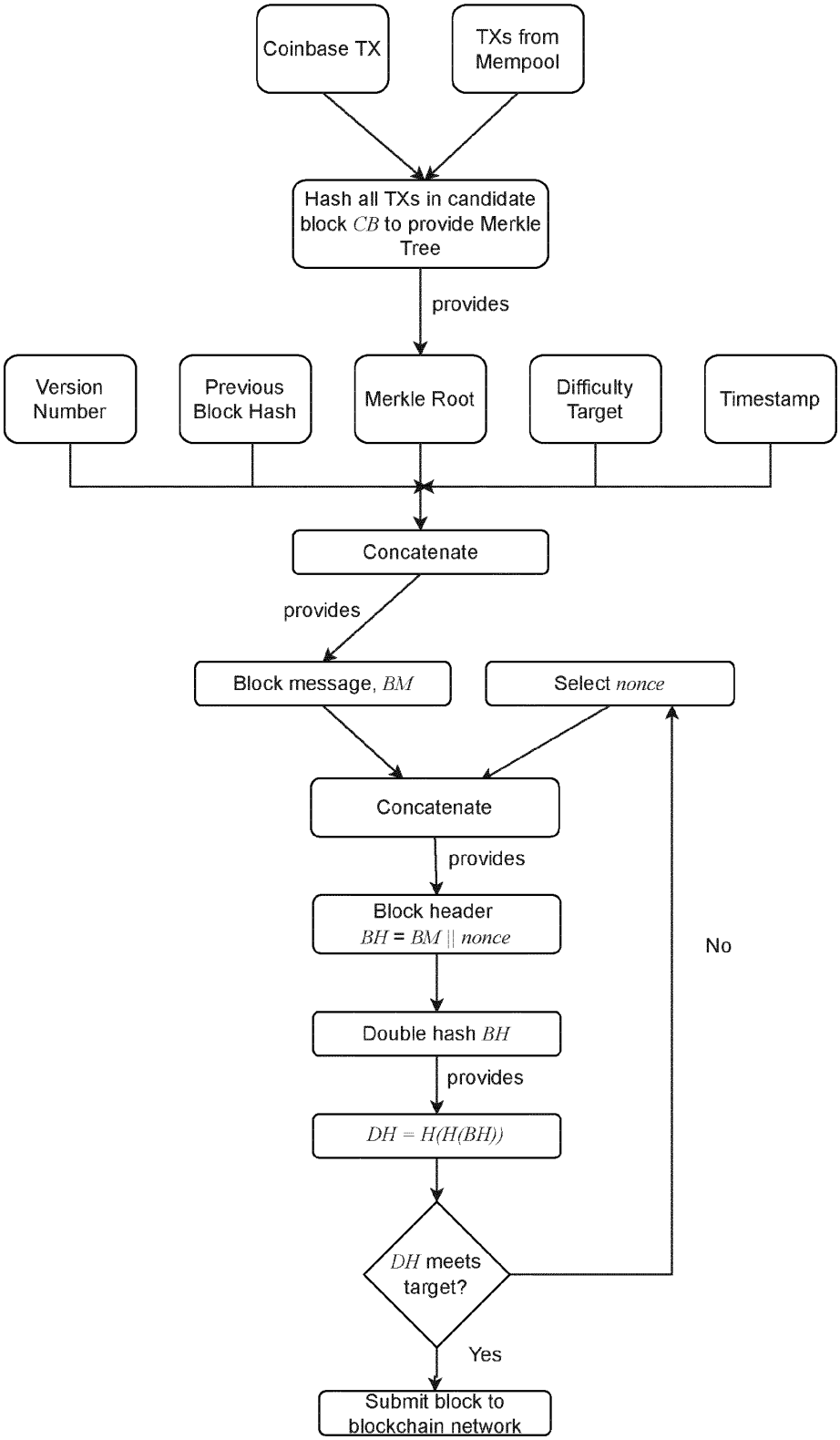


Figure 12 *(disclosure compared to prior art process)*

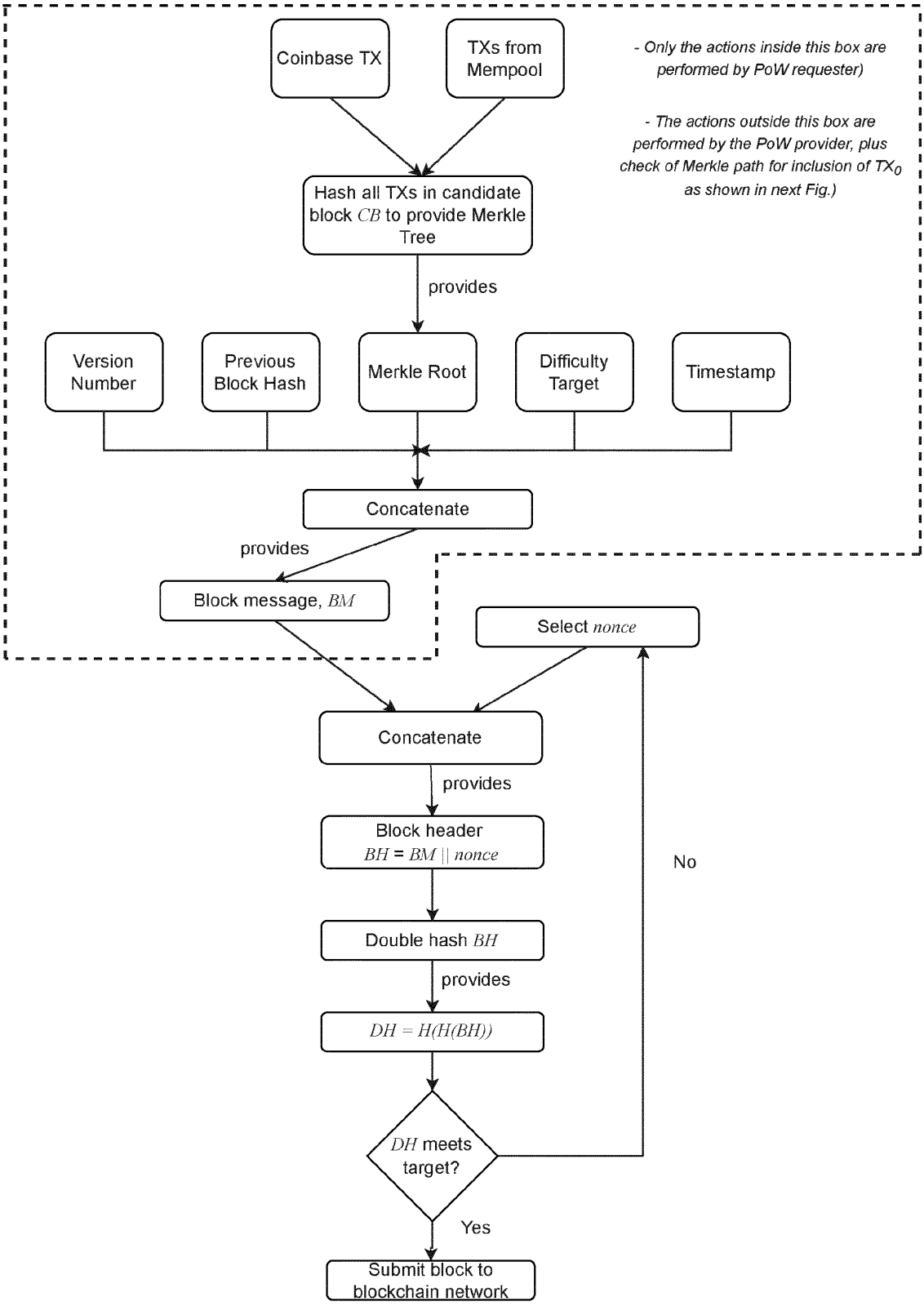


Figure 13

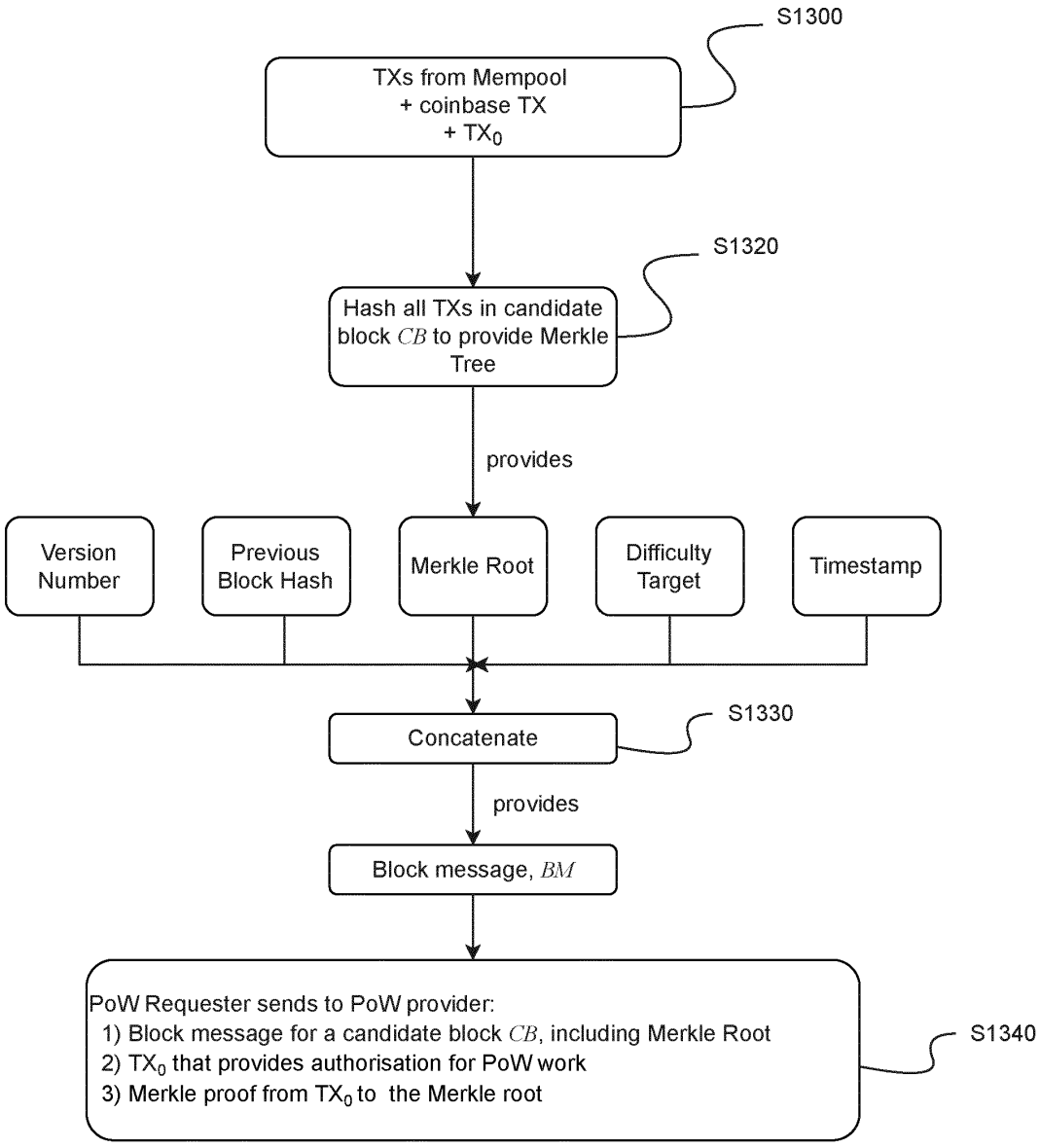
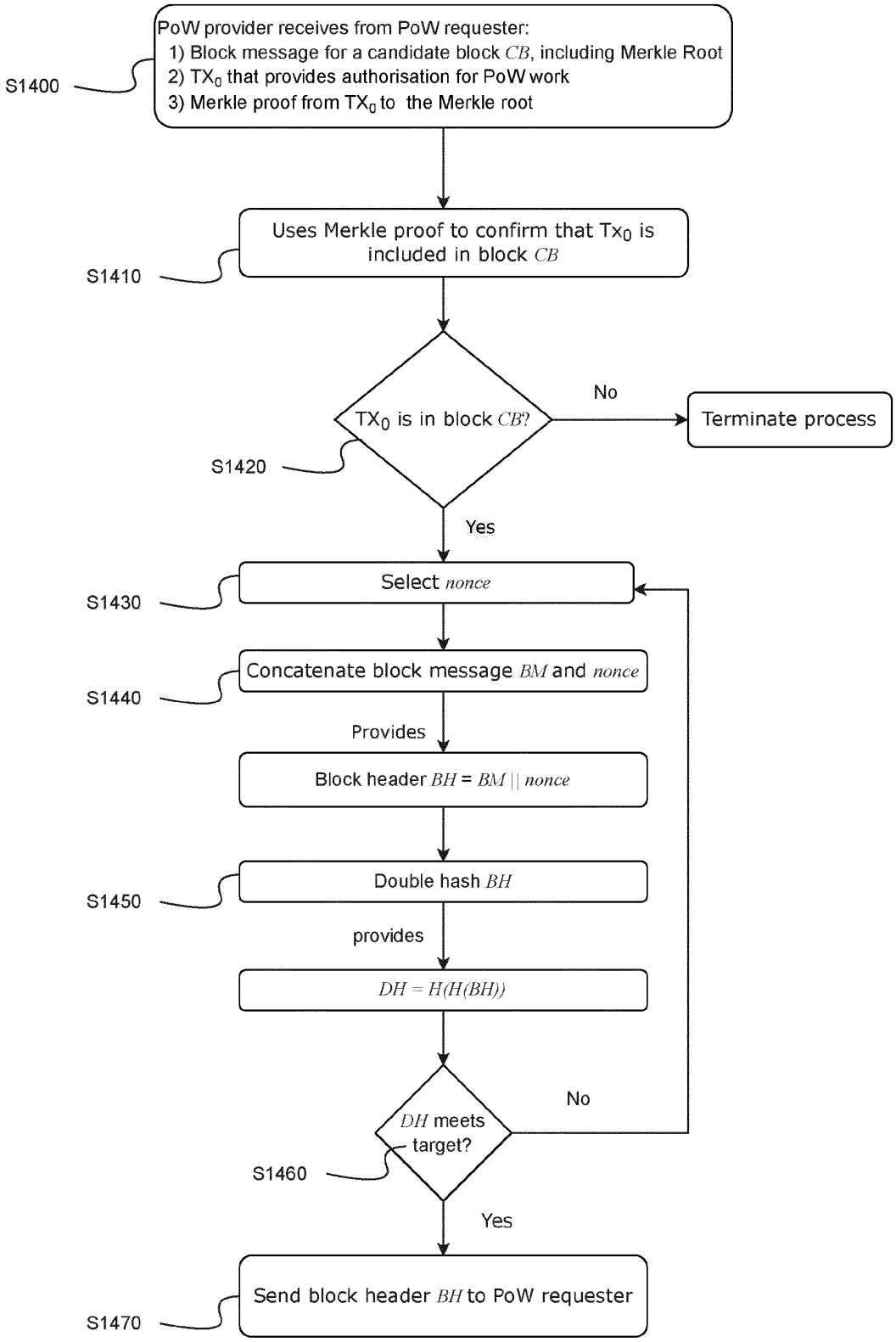

S1300
TXs from Mempool
+ coinbase TX
+ TX_0
S1320
Hash all TXs in candidate block CB to provide Merkle Tree
provides
Version Number
Previous Block Hash
Merkle Root
Difficulty Target
Timestamp
S1330
Concatenate
provides
Block message, BM
PoW Requester sends to PoW provider:
1) Block message for a candidate block CB, including Merkle Root
2) TX_0 that provides authorisation for PoW work
3) Merkle proof from TX_0 to the Merkle root
S1340

Figure 14


PoW provider receives from PoW requester:
1) Block message for a candidate block CB, including Merkle Root
2) TX0 that provides authorisation for PoW work
3) Merkle proof from TX0 to the Merkle root
S1400
Uses Merkle proof to confirm that Tx0 is included in block CB
S1410
TX0 is in block CB?
No
Terminate process
S1420
Yes
Select nonce
S1430
Concatenate block message BM and nonce
S1440
Provides
Block header BH = BM || nonce
Double hash BH
S1450
provides
DH = H(H(BH))
DH meets target?
No
S1460
Yes
Send block header BH to PoW requester
S1470

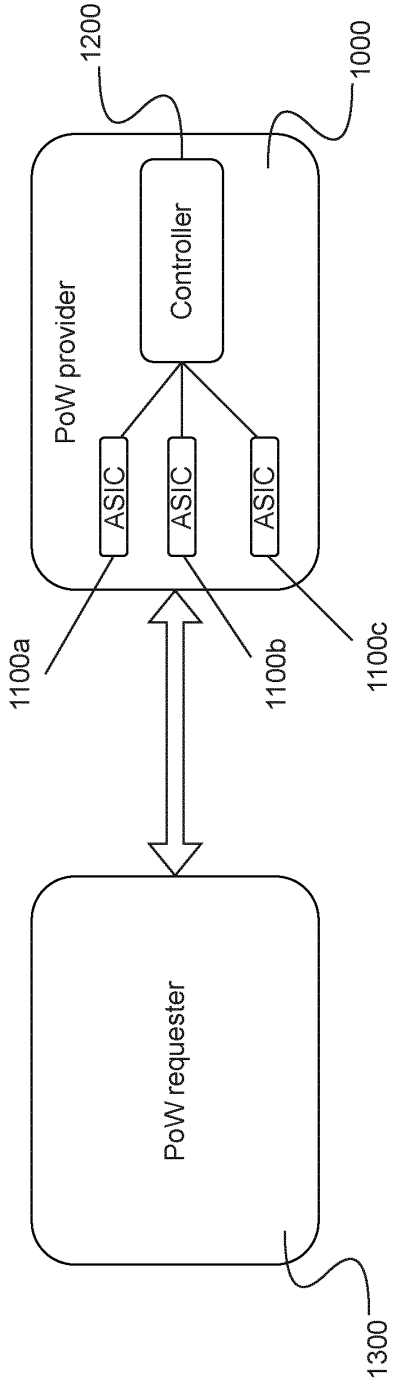

1200
1000
PoW provider
Controller
ASIC
ASIC
ASIC
1100a
1100b
1100c
PoW requester
1300

Figure 15