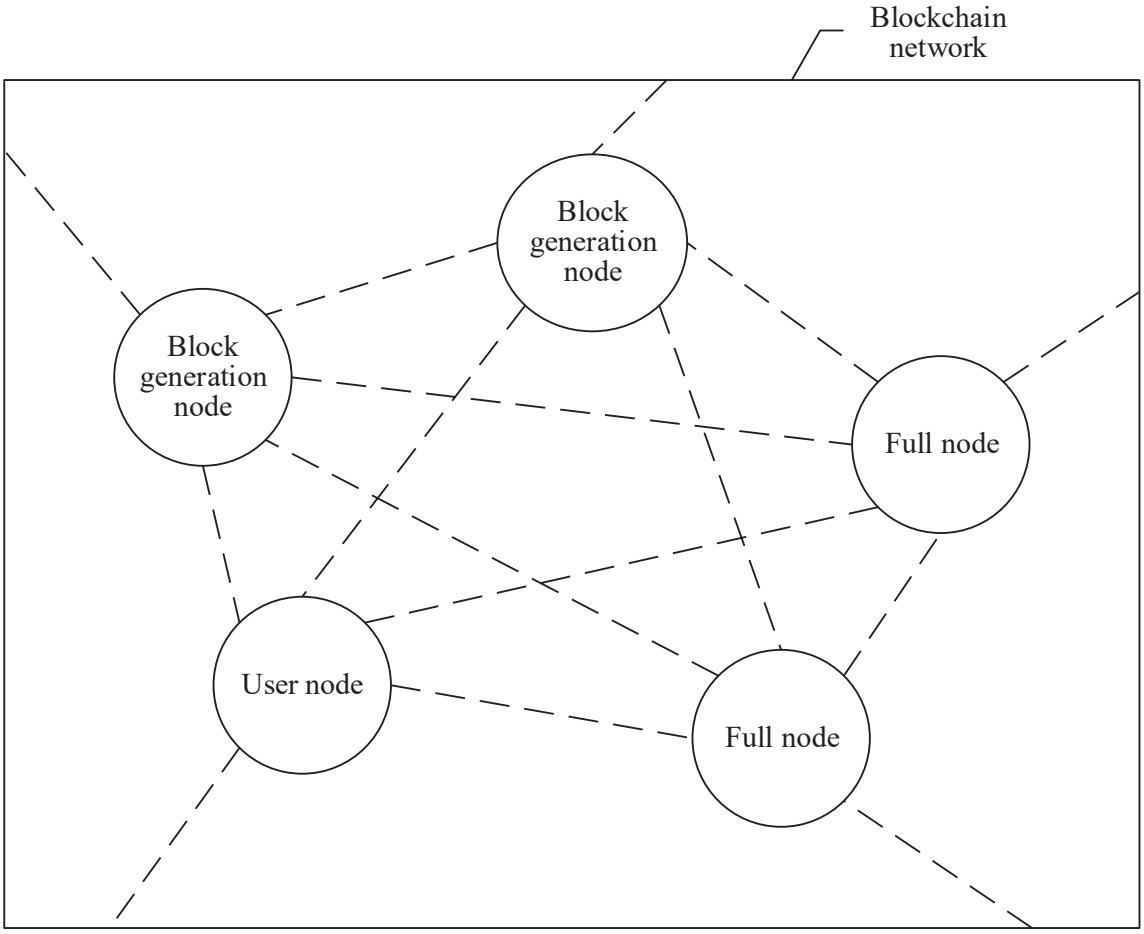

Blockchain network
Block generation node
Block generation node
Full node
User node
Full node

FIG. 1

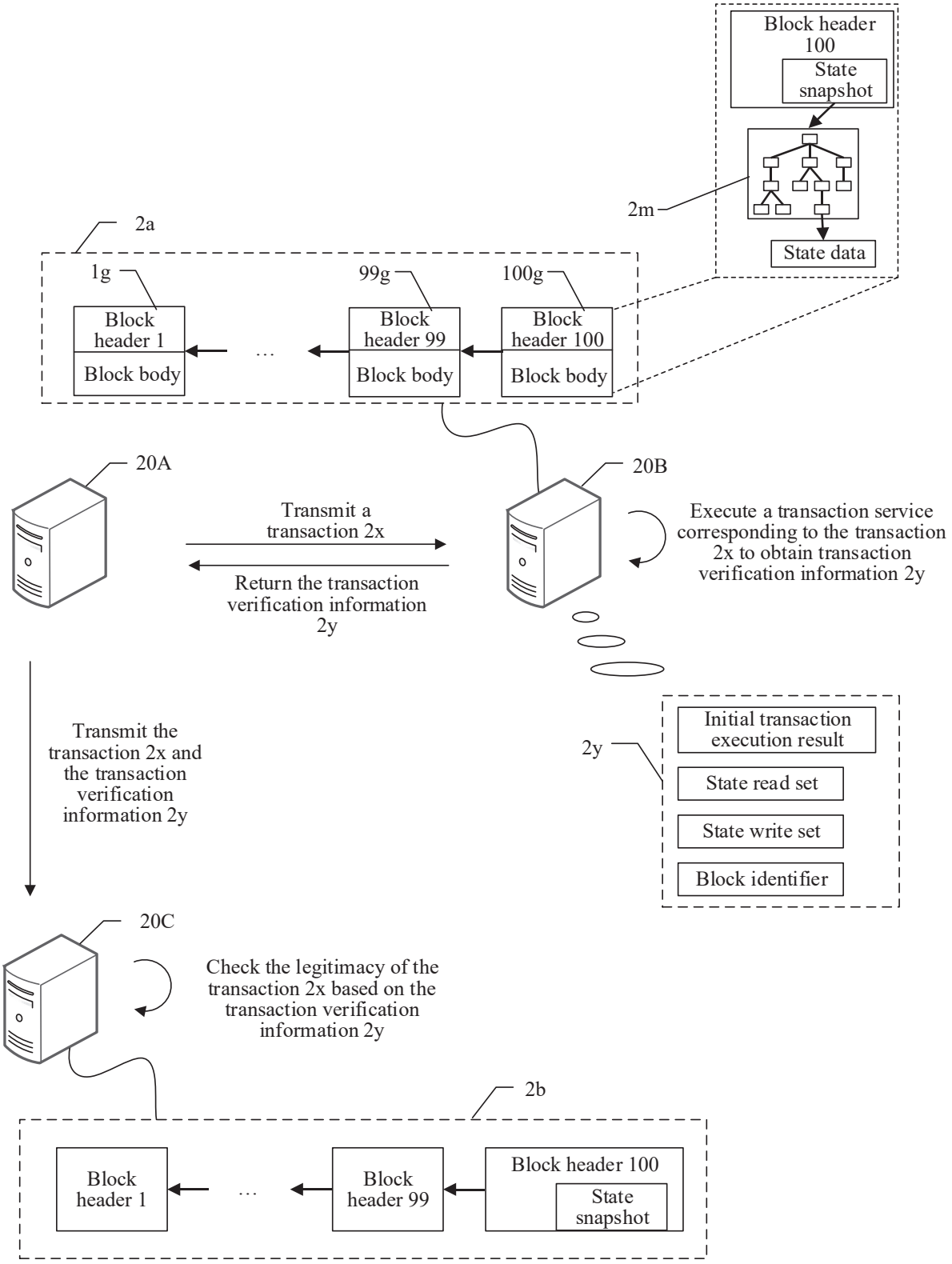

Block header 100
State snapshot
2m
State data
2a
1g
99g
100g
Block header 1
Block body
Block header 99
Block body
Block header 100
Block body
20A
20B
Transmit a transaction 2x
Return the transaction verification information 2y
Execute a transaction service corresponding to the transaction 2x to obtain transaction verification information 2y
Transmit the transaction 2x and the transaction verification information 2y
2y
Initial transaction execution result
State read set
State write set
Block identifier
20C
Check the legitimacy of the transaction 2x based on the transaction verification information 2y
2b
Block header 1
Block header 99
Block header 100
State snapshot

FIG. 2

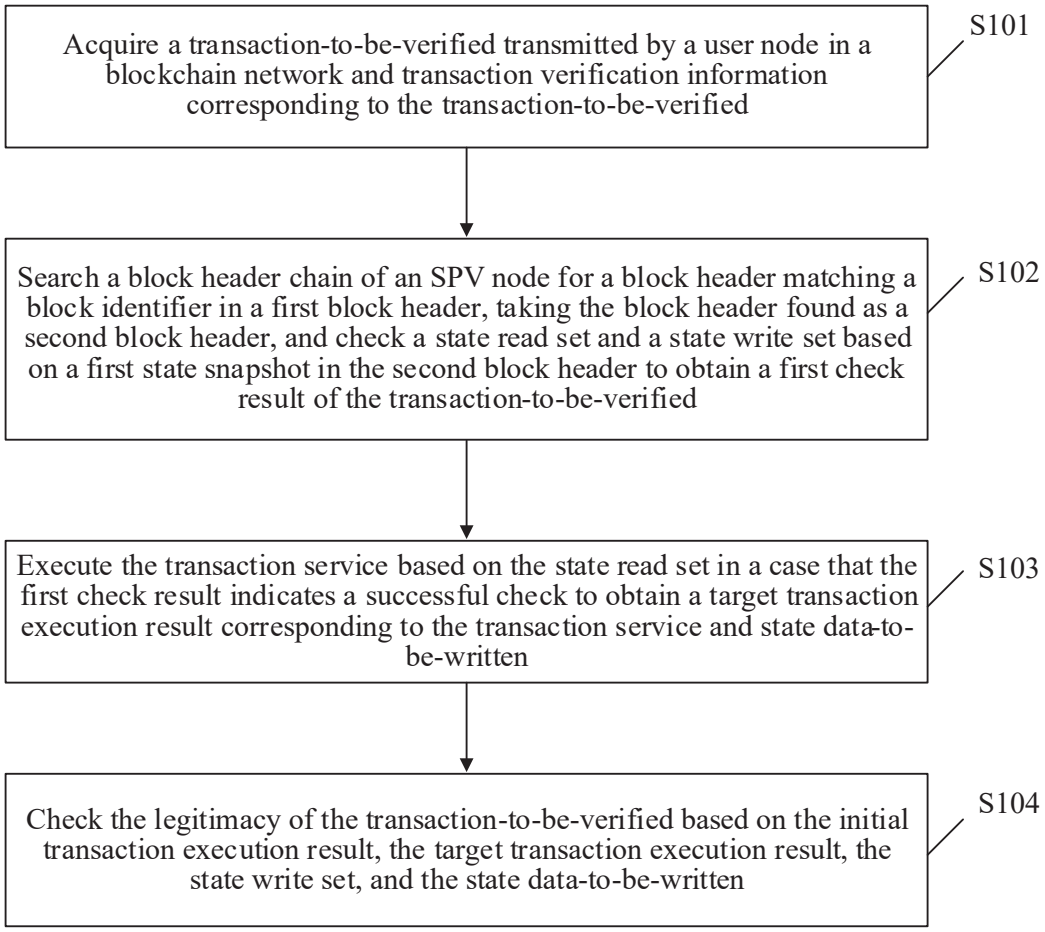

Acquire a transaction-to-be-verified transmitted by a user node in a blockchain network and transaction verification information corresponding to the transaction-to-be-verified
S101
Search a block header chain of an SPV node for a block header matching a block identifier in a first block header, taking the block header found as a second block header, and check a state read set and a state write set based on a first state snapshot in the second block header to obtain a first check result of the transaction-to-be-verified
S102
Execute the transaction service based on the state read set in a case that the first check result indicates a successful check to obtain a target transaction execution result corresponding to the transaction service and state data-to-be-written
S103
Check the legitimacy of the transaction-to-be-verified based on the initial transaction execution result, the target transaction execution result, the state write set, and the state data-to-be-written
S104

FIG. 3

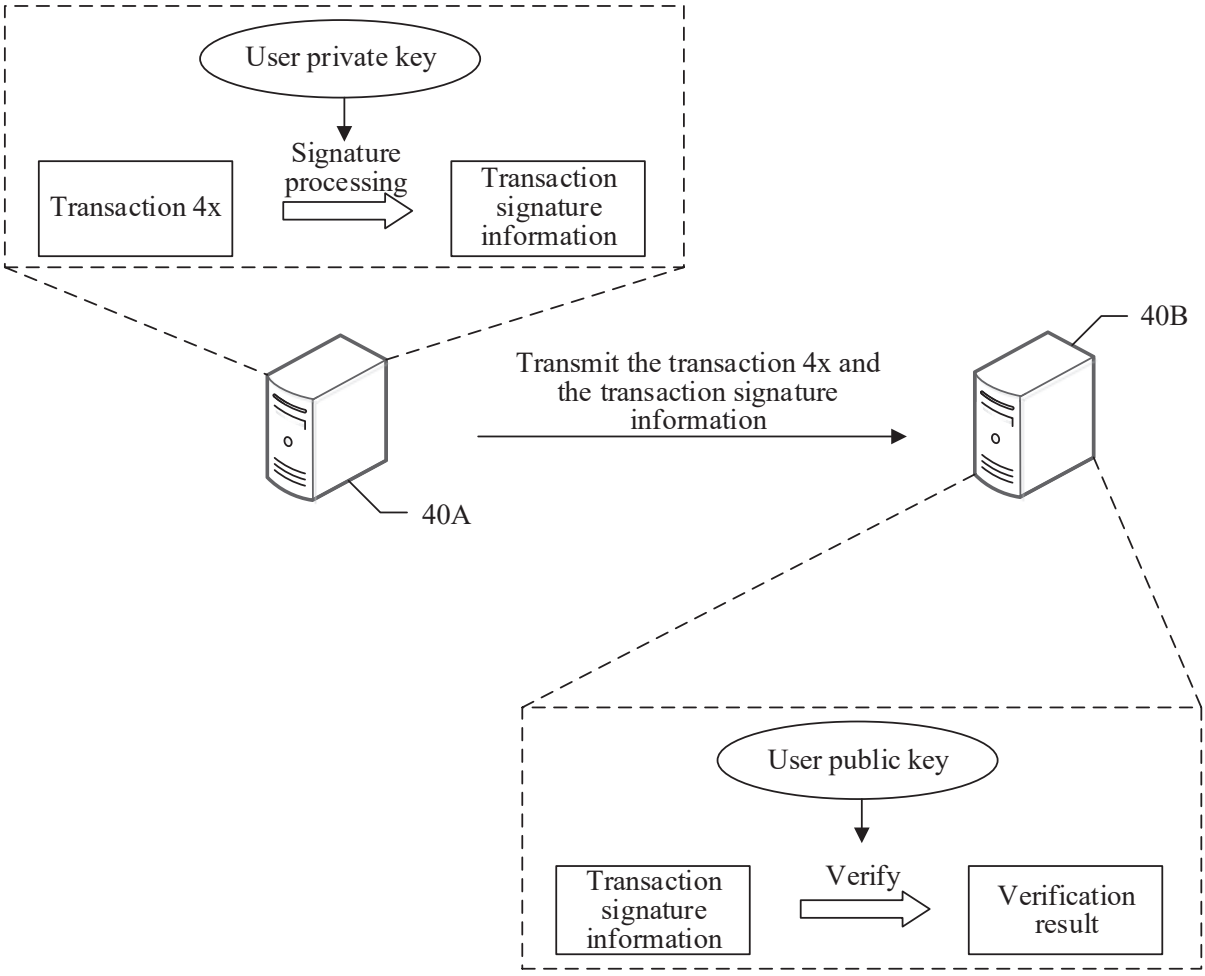

User private key
Signature processing
Transaction 4x
Transaction signature information
40A
Transmit the transaction 4x and the transaction signature information
40B
User public key
Verify
Transaction signature information
Verification result

FIG. 4

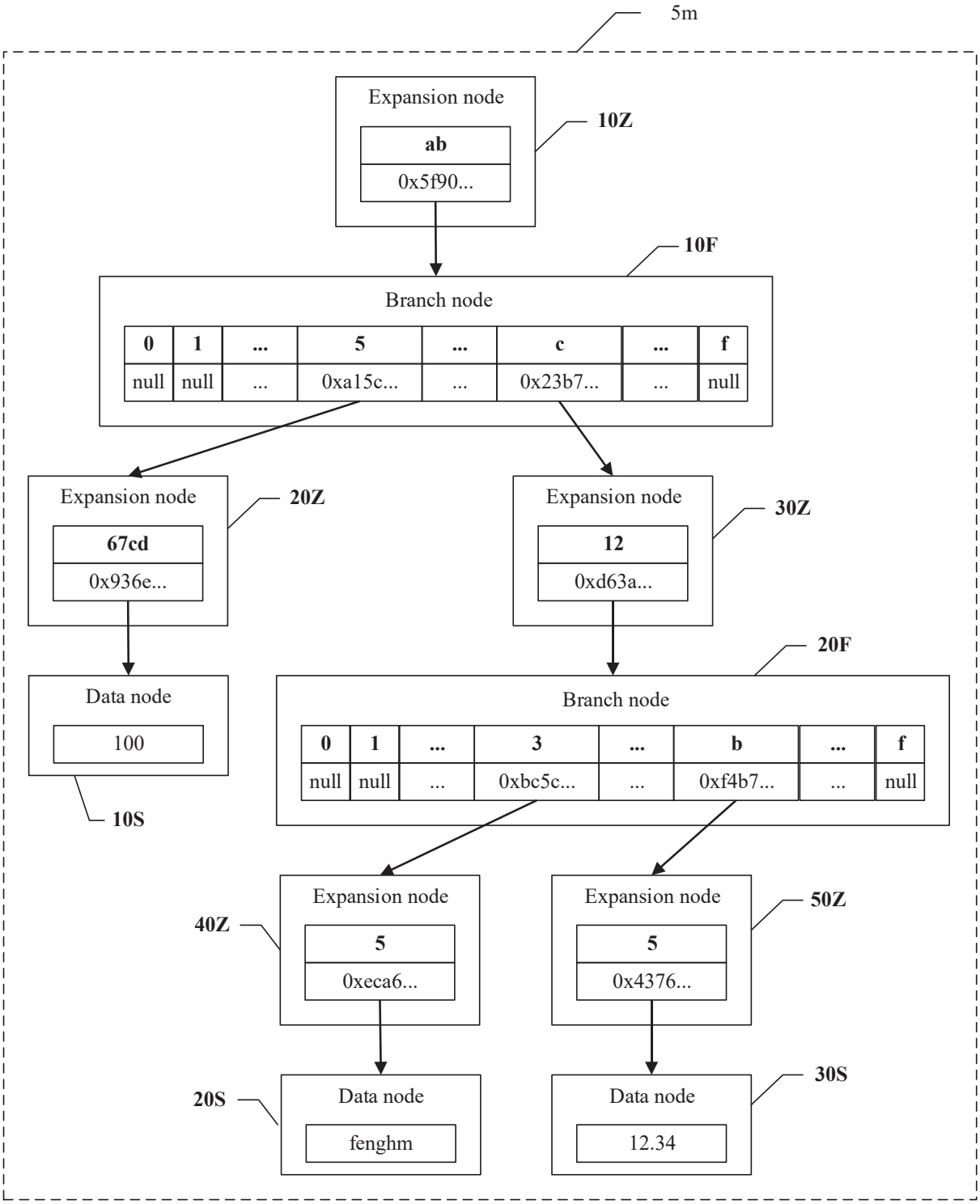

5m
Expansion node
ab
0x5f90...
10Z
10F
Branch node
0 | 1 | ... | 5 | ... | c | ... | f
null | null | ... | 0xa15c... | ... | 0x23b7... | ... | null
Expansion node
67cd
0x936e...
20Z
Expansion node
12
0xd63a...
30Z
Data node
100
10S
20F
Branch node
0 | 1 | ... | 3 | ... | b | ... | f
null | null | ... | 0xbc5c... | ... | 0xf4b7... | ... | null
40Z
Expansion node
5
0xeca6...
50Z
Expansion node
5
0x4376...
20S
Data node
fenghm
30S
Data node
12.34

FIG. 5

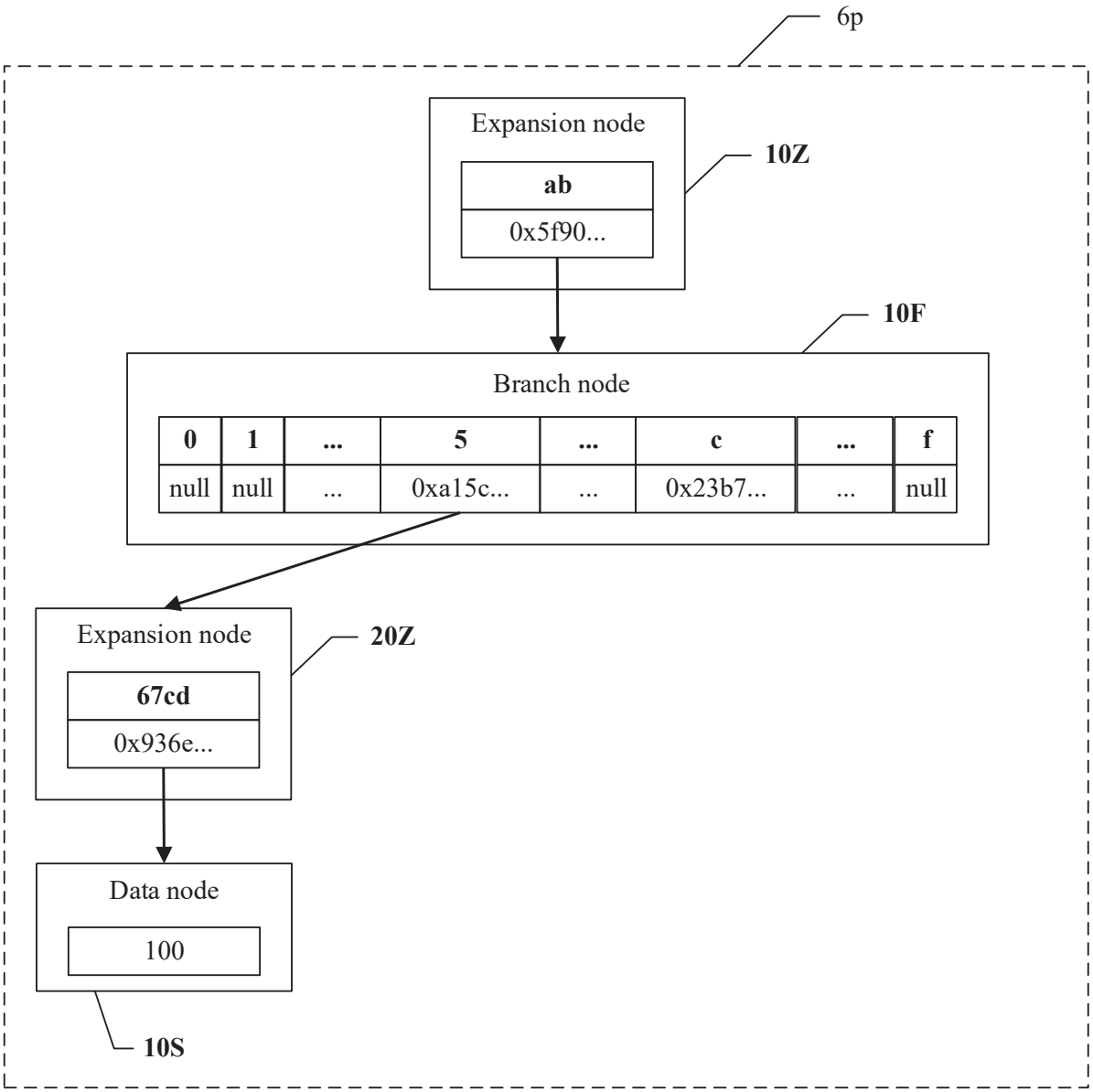

6p
Expansion node
ab
0x5f90...
10Z
10F
Branch node
0
1
...
5
...
c
...
f
null
null
...
0xa15c...
...
0x23b7...
...
null
Expansion node
67cd
0x936e...
20Z
Data node
100
10S

FIG. 6

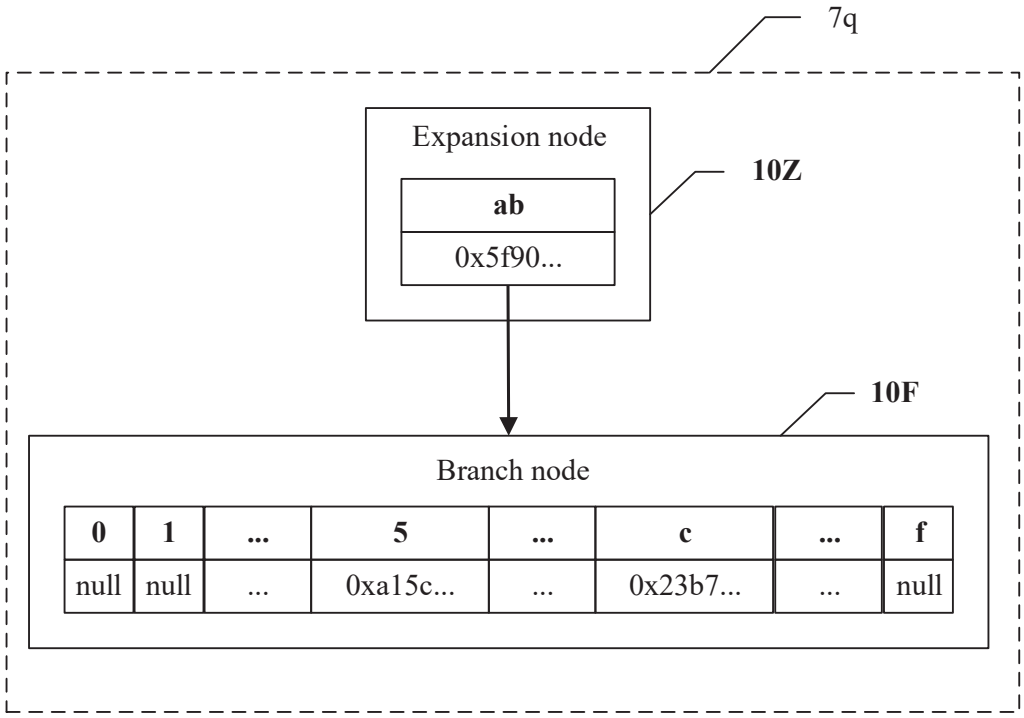

7q
Expansion node
ab
0x5f90...
10Z
10F
Branch node
0
1
...
5
...
c
...
f
null
null
...
0xa15c...
...
0x23b7...
...
null

FIG. 7

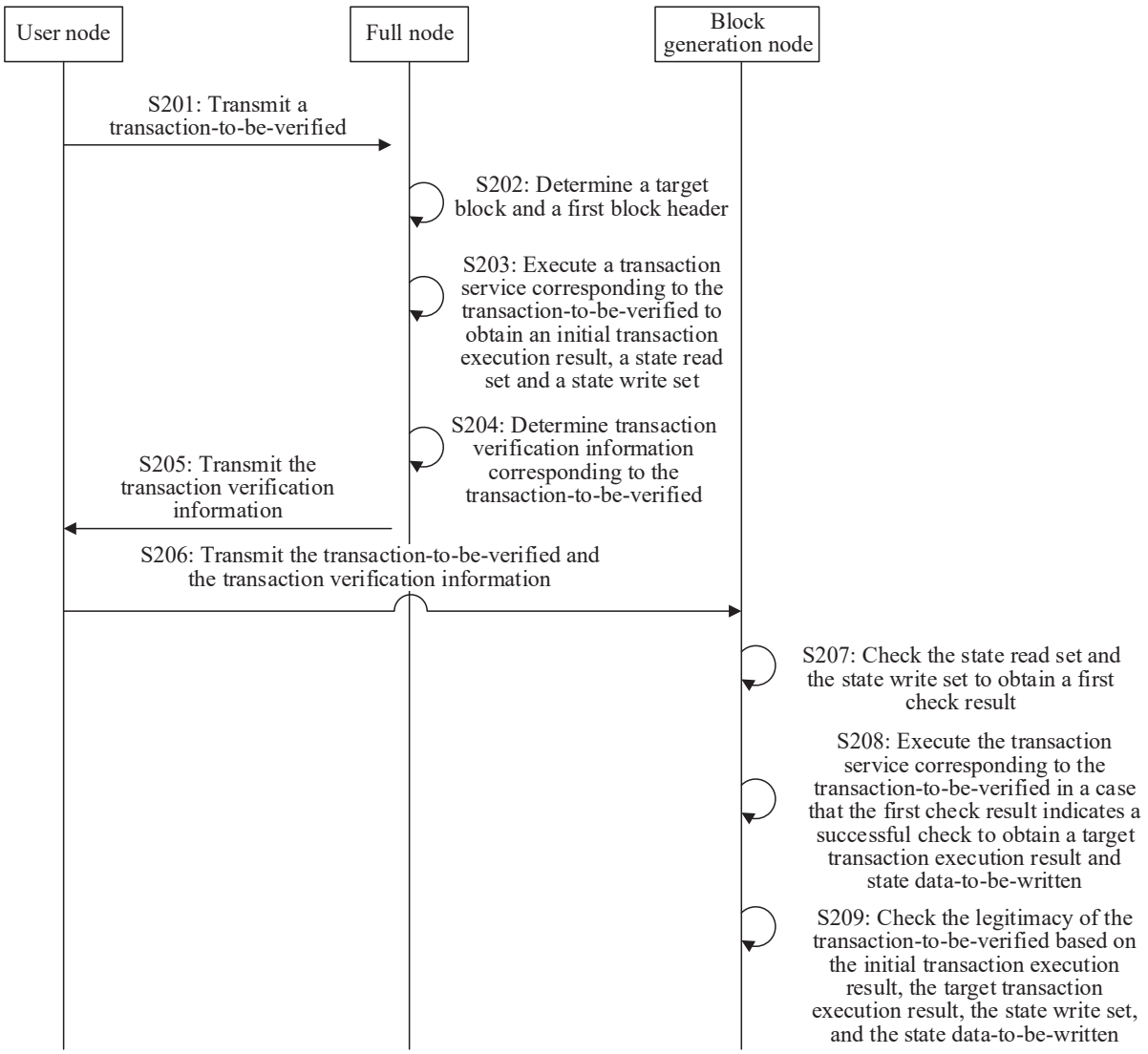

User node
Full node
Block generation node
S201: Transmit a transaction-to-be-verified
S202: Determine a target block and a first block header
S203: Execute a transaction service corresponding to the transaction-to-be-verified to obtain an initial transaction execution result, a state read set and a state write set
S204: Determine transaction verification information corresponding to the transaction-to-be-verified
S205: Transmit the transaction verification information
S206: Transmit the transaction-to-be-verified and the transaction verification information
S207: Check the state read set and the state write set to obtain a first check result
S208: Execute the transaction service corresponding to the transaction-to-be-verified in a case that the first check result indicates a successful check to obtain a target transaction execution result and state data-to-be-written
S209: Check the legitimacy of the transaction-to-be-verified based on the initial transaction execution result, the target transaction execution result, the state write set, and the state data-to-be-written

FIG. 8

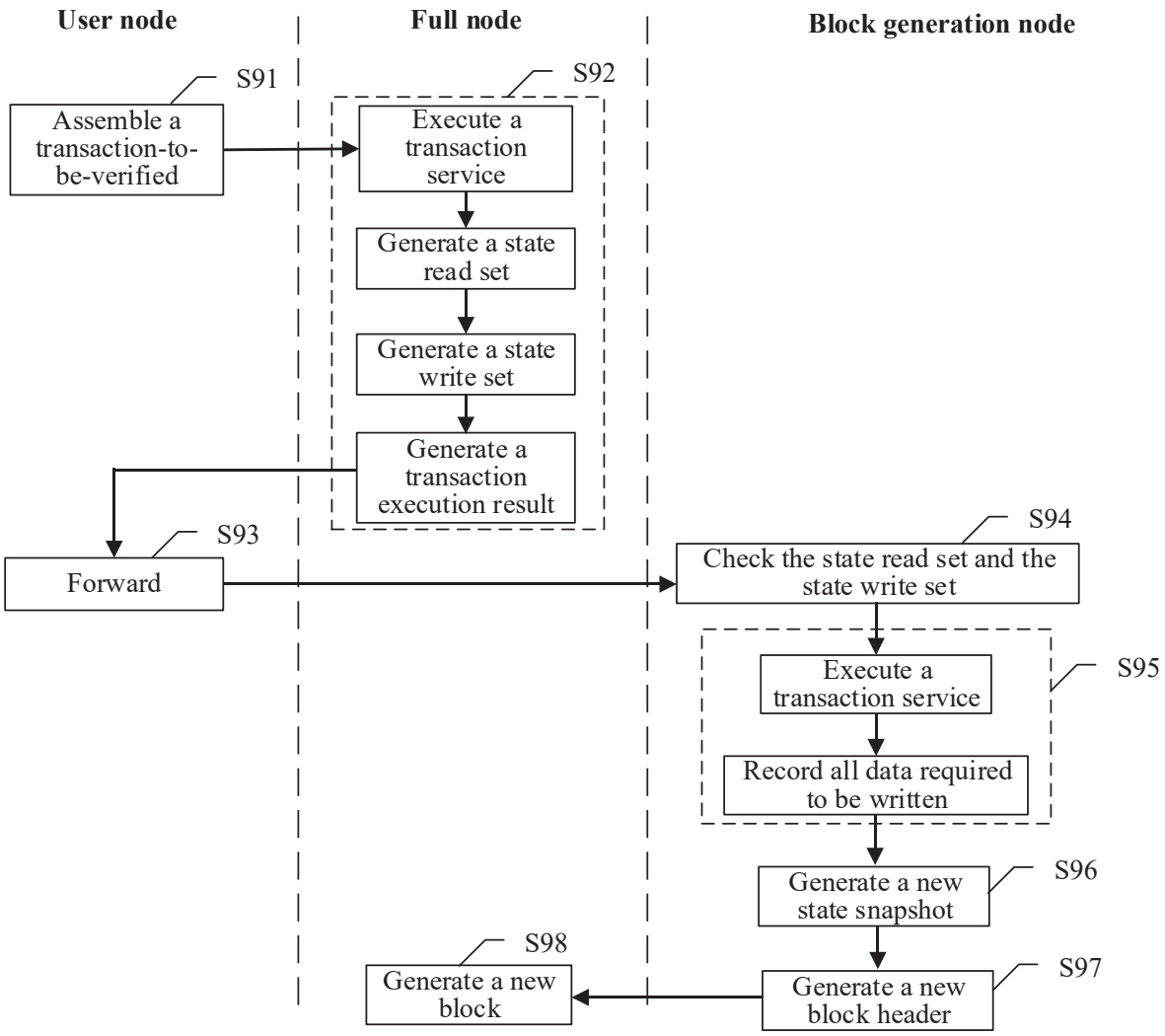

User node
Full node
Block generation node
S91
Assemble a transaction-to-be-verified
S92
Execute a transaction service
Generate a state read set
Generate a state write set
Generate a transaction execution result
S93
Forward
S94
Check the state read set and the state write set
S95
Execute a transaction service
Record all data required to be written
S96
Generate a new state snapshot
S97
Generate a new block header
S98
Generate a new block

FIG. 9

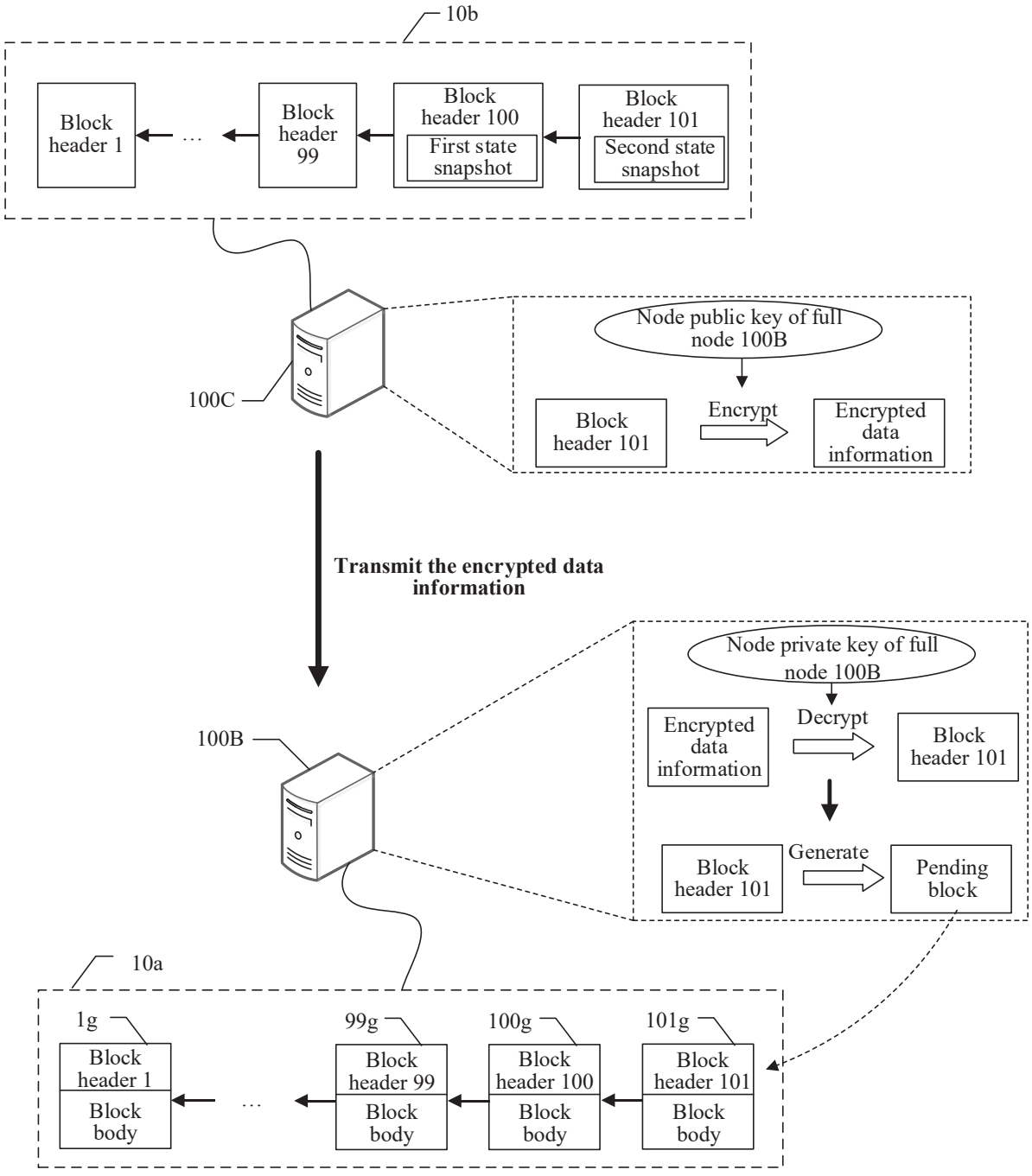

10b
Block header 1
...
Block header 99
Block header 100
First state snapshot
Block header 101
Second state snapshot
100C
Node public key of full node 100B
Block header 101
Encrypt
Encrypted data information
Transmit the encrypted data information
100B
Node private key of full node 100B
Encrypted data information
Decrypt
Block header 101
Block header 101
Generate
Pending block
10a
1g
99g
100g
101g
Block header 1
Block body
Block header 99
Block body
Block header 100
Block body
Block header 101
Block body

FIG. 10

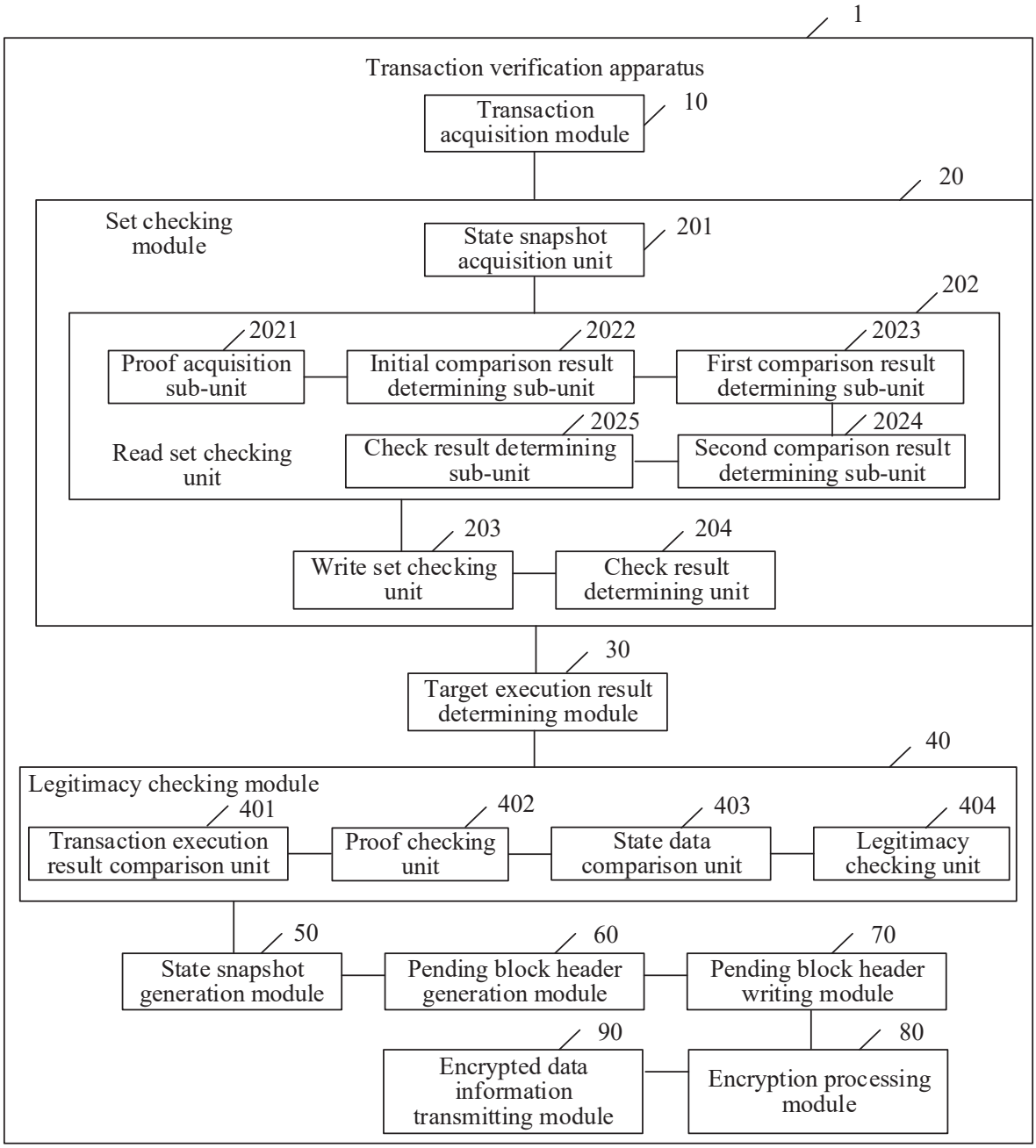

1
Transaction verification apparatus
Transaction acquisition module
10
20
Set checking module
State snapshot acquisition unit
201
202
2021
Proof acquisition sub-unit
2022
Initial comparison result determining sub-unit
2023
First comparison result determining sub-unit
Read set checking unit
2025
Check result determining sub-unit
2024
Second comparison result determining sub-unit
203
Write set checking unit
204
Check result determining unit
30
Target execution result determining module
40
Legitimacy checking module
401
Transaction execution result comparison unit
402
Proof checking unit
403
State data comparison unit
404
Legitimacy checking unit
50
State snapshot generation module
60
Pending block header generation module
70
Pending block header writing module
90
Encrypted data information transmitting module
80
Encryption processing module

FIG. 11

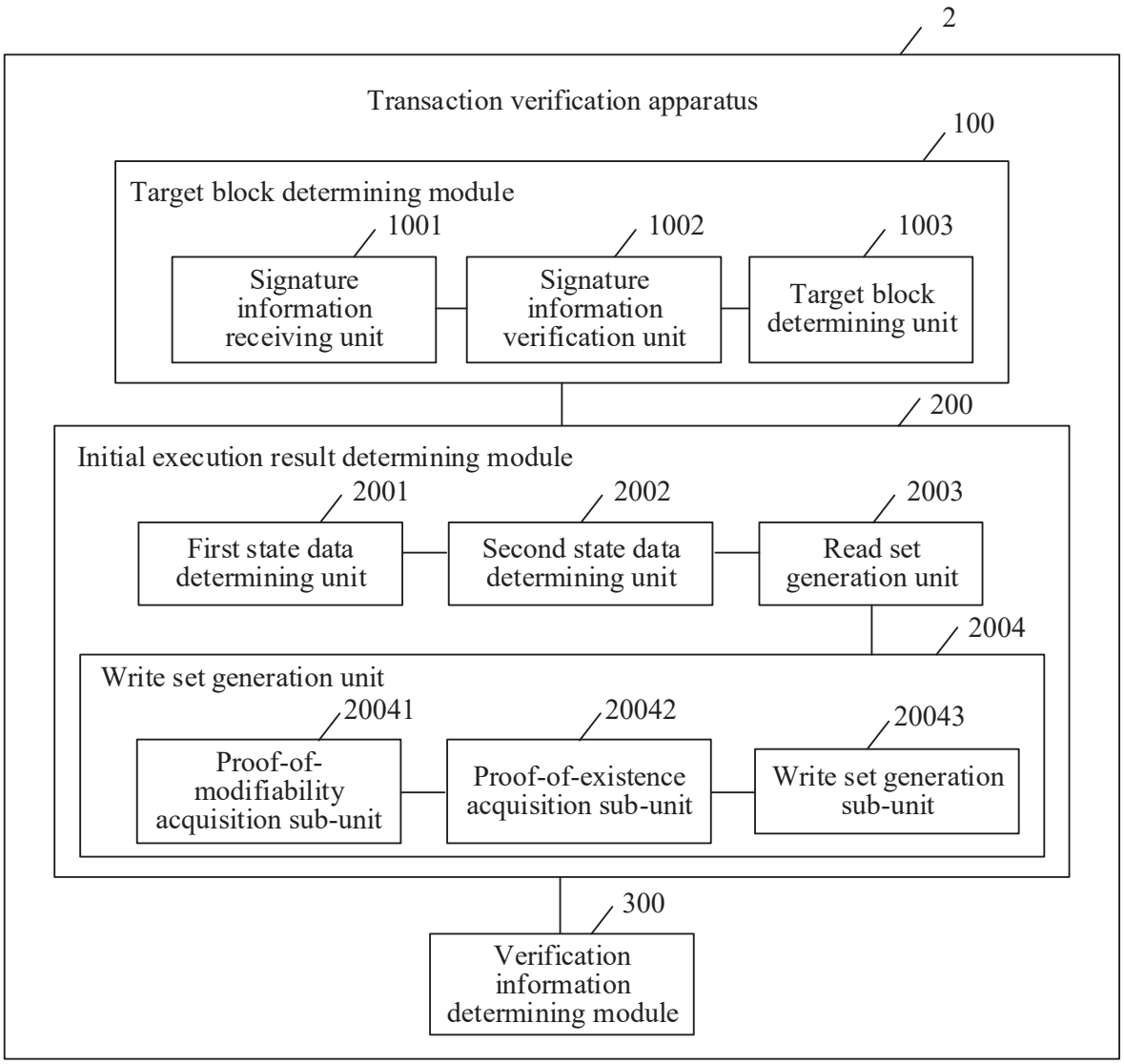

2
Transaction verification apparatus
100
Target block determining module
1001
Signature information receiving unit
1002
Signature information verification unit
1003
Target block determining unit
200
Initial execution result determining module
2001
First state data determining unit
2002
Second state data determining unit
2003
Read set generation unit
2004
Write set generation unit
20041
Proof-of-modifiability acquisition sub-unit
20042
Proof-of-existence acquisition sub-unit
20043
Write set generation sub-unit
300
Verification information determining module

FIG. 12

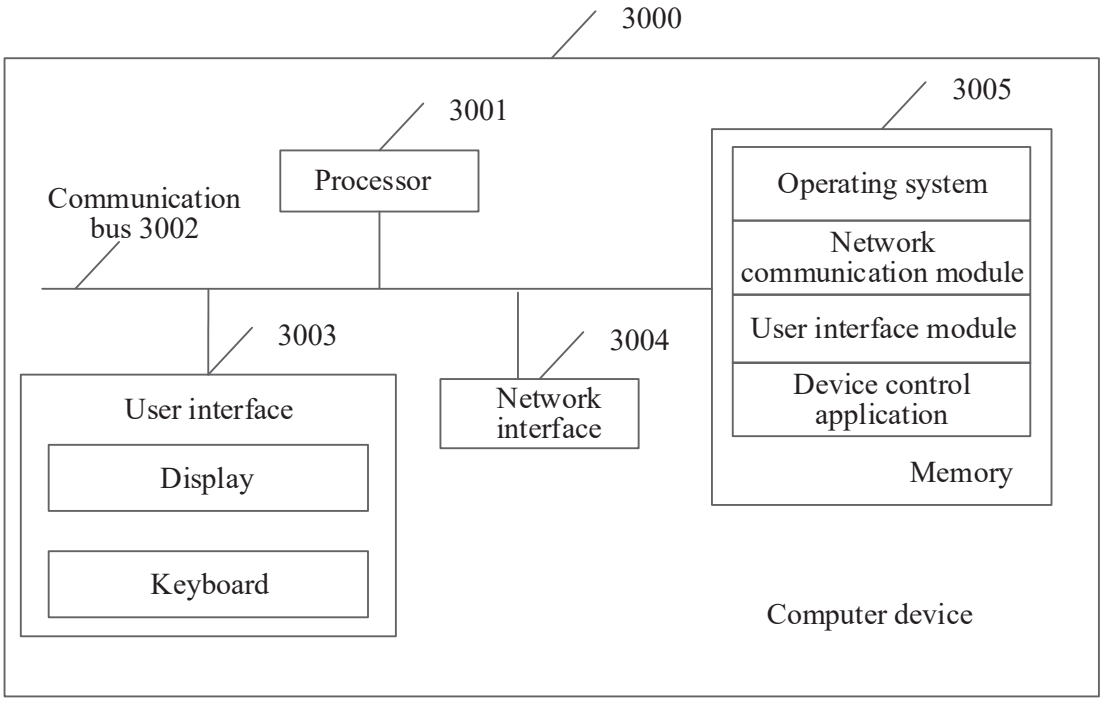

3000
3001
Processor
3005
Operating system
Network communication module
User interface module
Device control application
Memory
Communication bus 3002
3003
User interface
Display
Keyboard
3004
Network interface
Computer device

FIG. 13

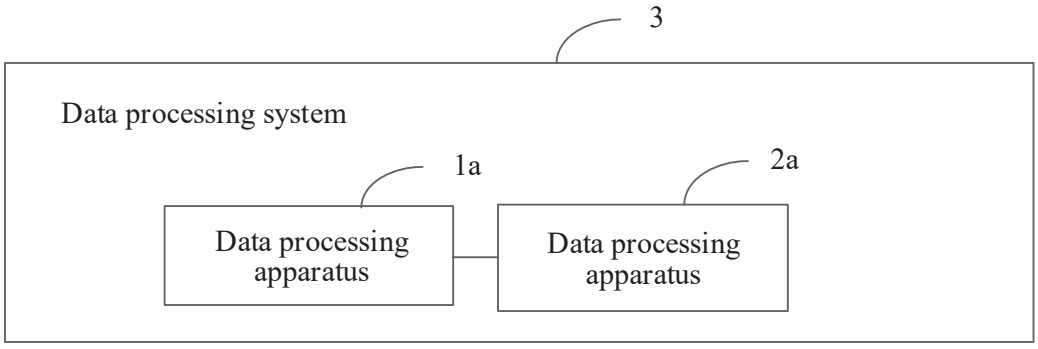

3
Data processing system
1a
Data processing apparatus
2a
Data processing apparatus

FIG. 14