100

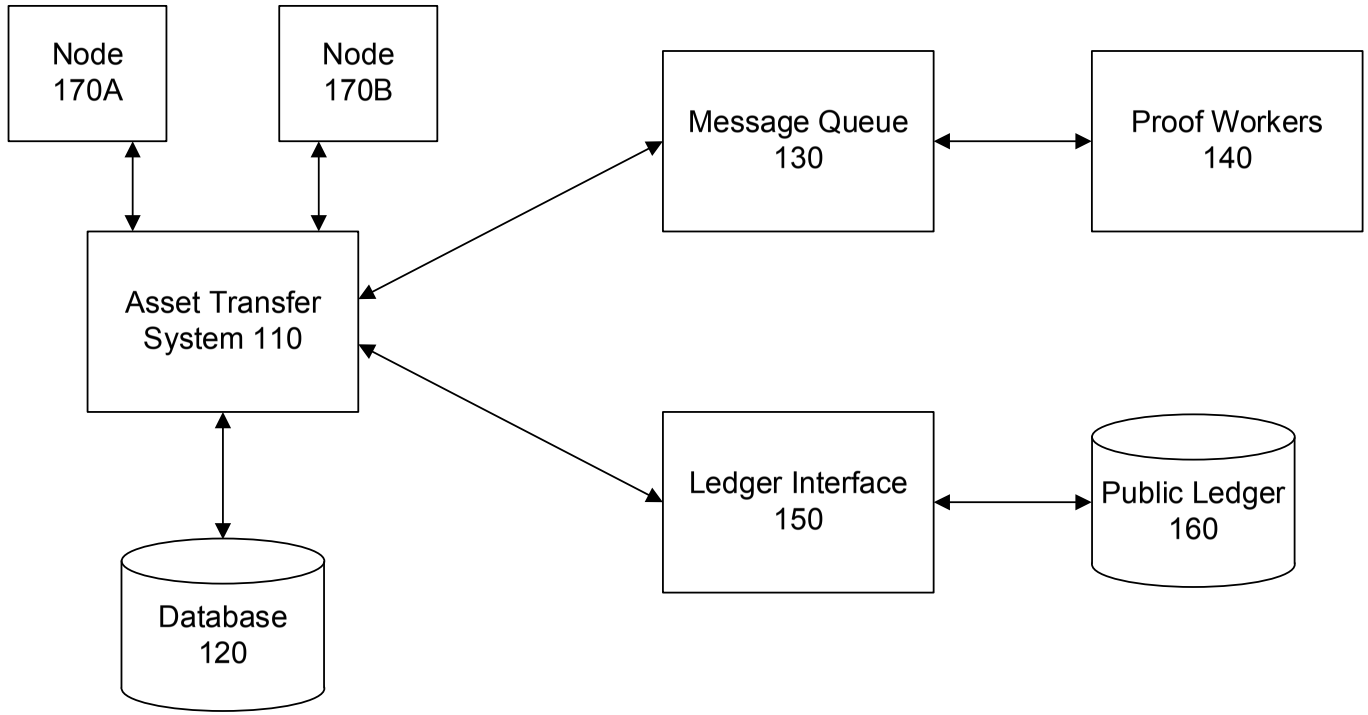
Node
170A
Node
170B
Message Queue
130
Proof Workers
140
Asset Transfer
System 110
Ledger Interface
150
Public Ledger
160
Database
120

FIG. 1

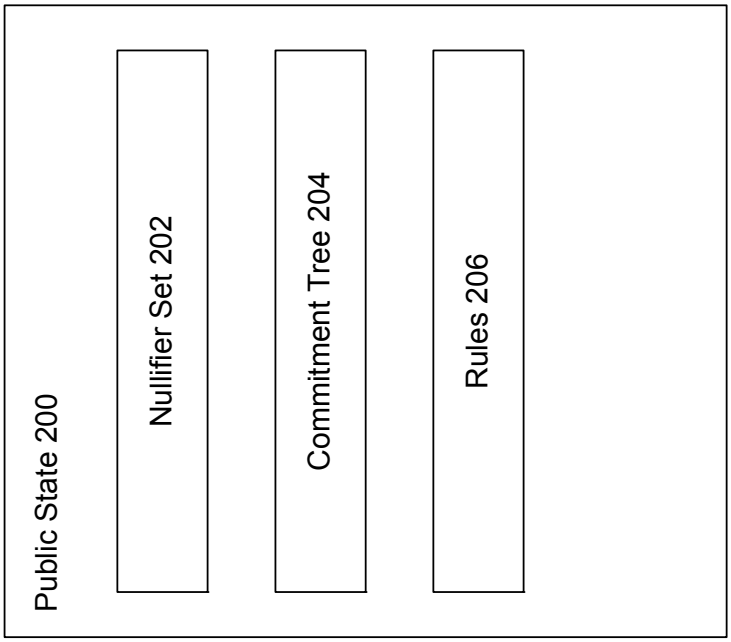
Public State 200
Nullifier Set 202
Commitment Tree 204
Rules 206

FIG. 2

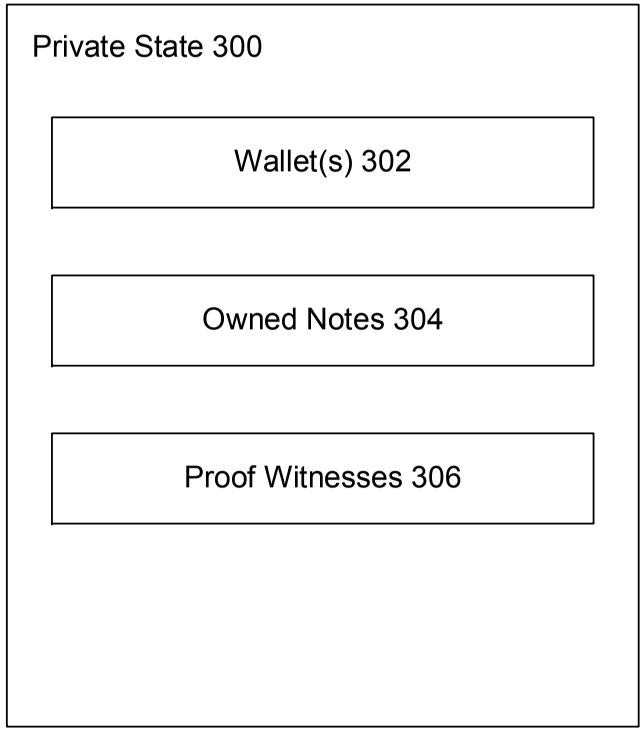
Private State 300
Wallet(s) 302
Owned Notes 304
Proof Witnesses 306

FIG. 3

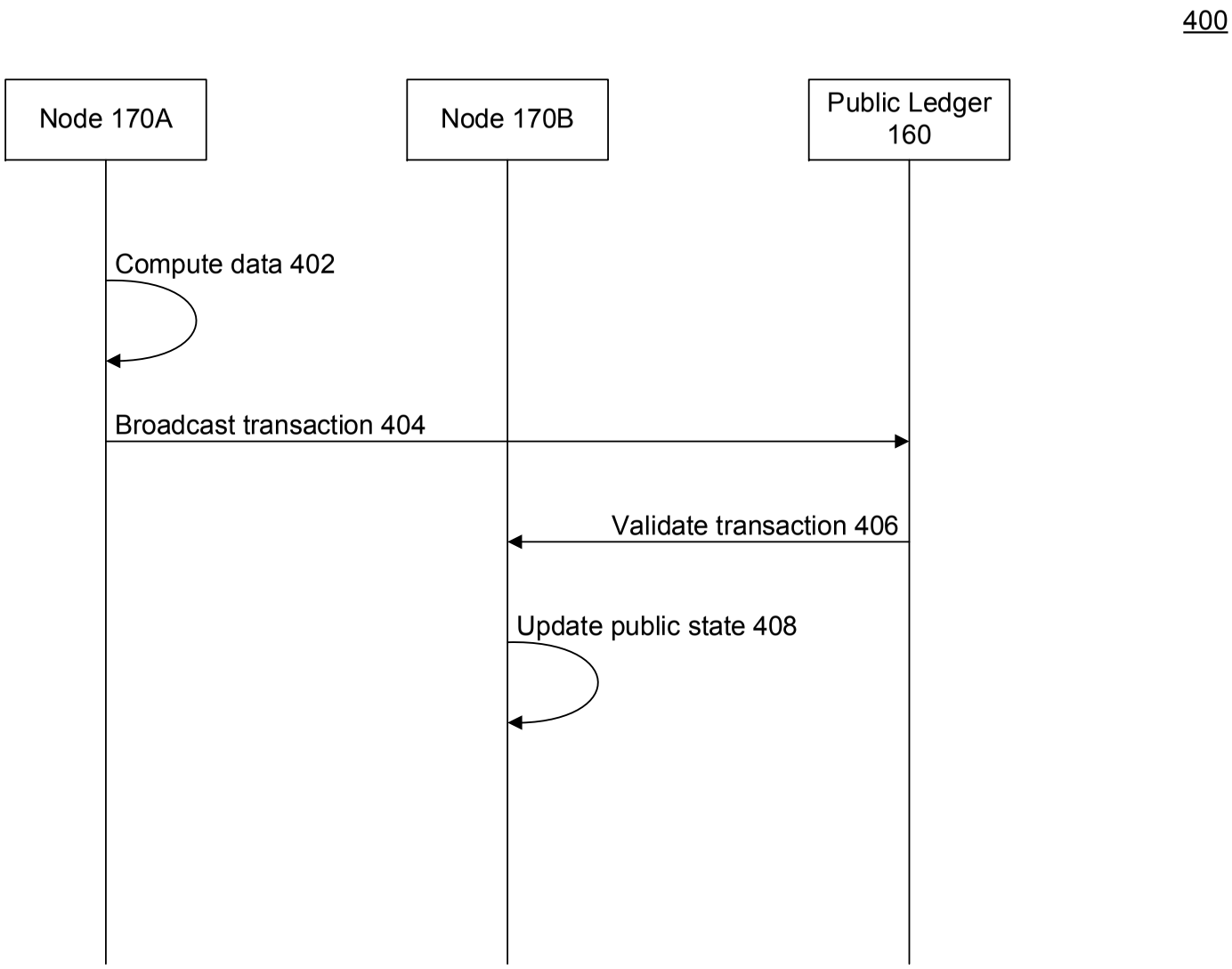
400
Node 170A
Node 170B
Public Ledger 160
Compute data 402
Broadcast transaction 404
Validate transaction 406
Update public state 408

FIG. 4

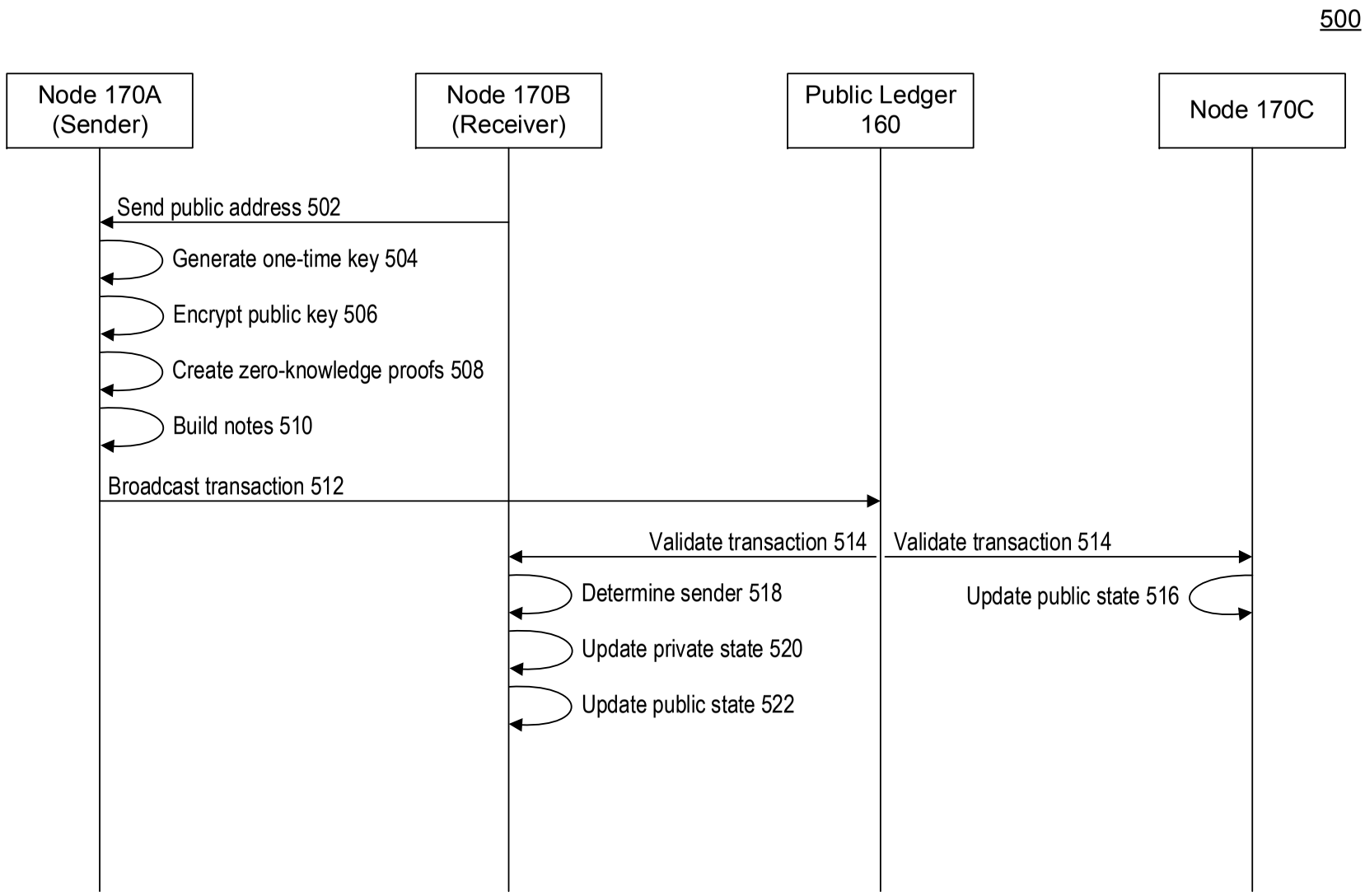
500
Node 170A (Sender)
Node 170B (Receiver)
Public Ledger 160
Node 170C
Send public address 502
Generate one-time key 504
Encrypt public key 506
Create zero-knowledge proofs 508
Build notes 510
Broadcast transaction 512
Validate transaction 514
Validate transaction 514
Determine sender 518
Update public state 516
Update private state 520
Update public state 522

FIG. 5

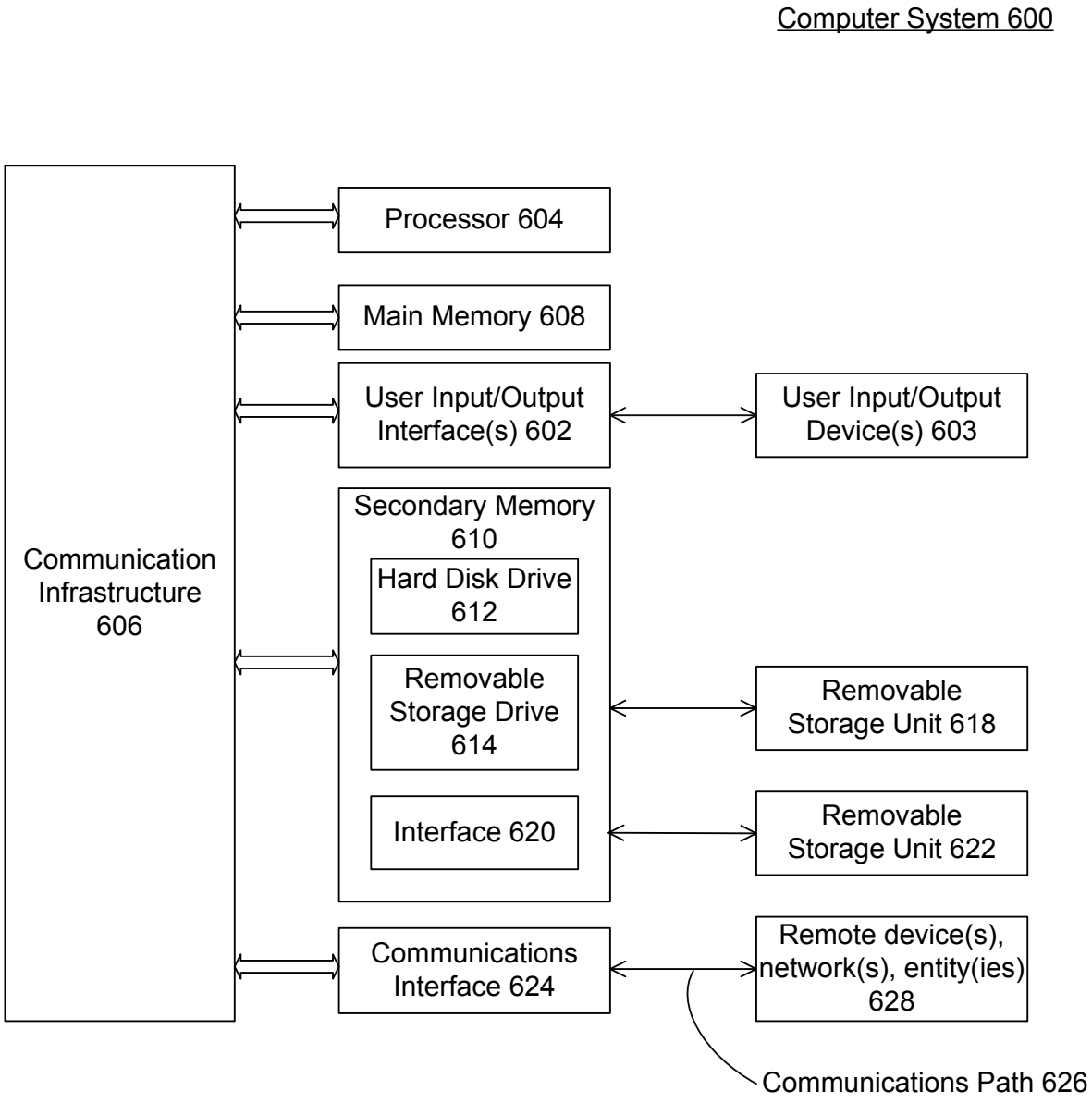
Computer System 600
Communication Infrastructure 606
Processor 604
Main Memory 608
User Input/Output Interface(s) 602
User Input/Output Device(s) 603
Secondary Memory 610
Hard Disk Drive 612
Removable Storage Drive 614
Interface 620
Removable Storage Unit 618
Removable Storage Unit 622
Communications Interface 624
Remote device(s), network(s), entity(ies) 628
Communications Path 626

FIG. 6