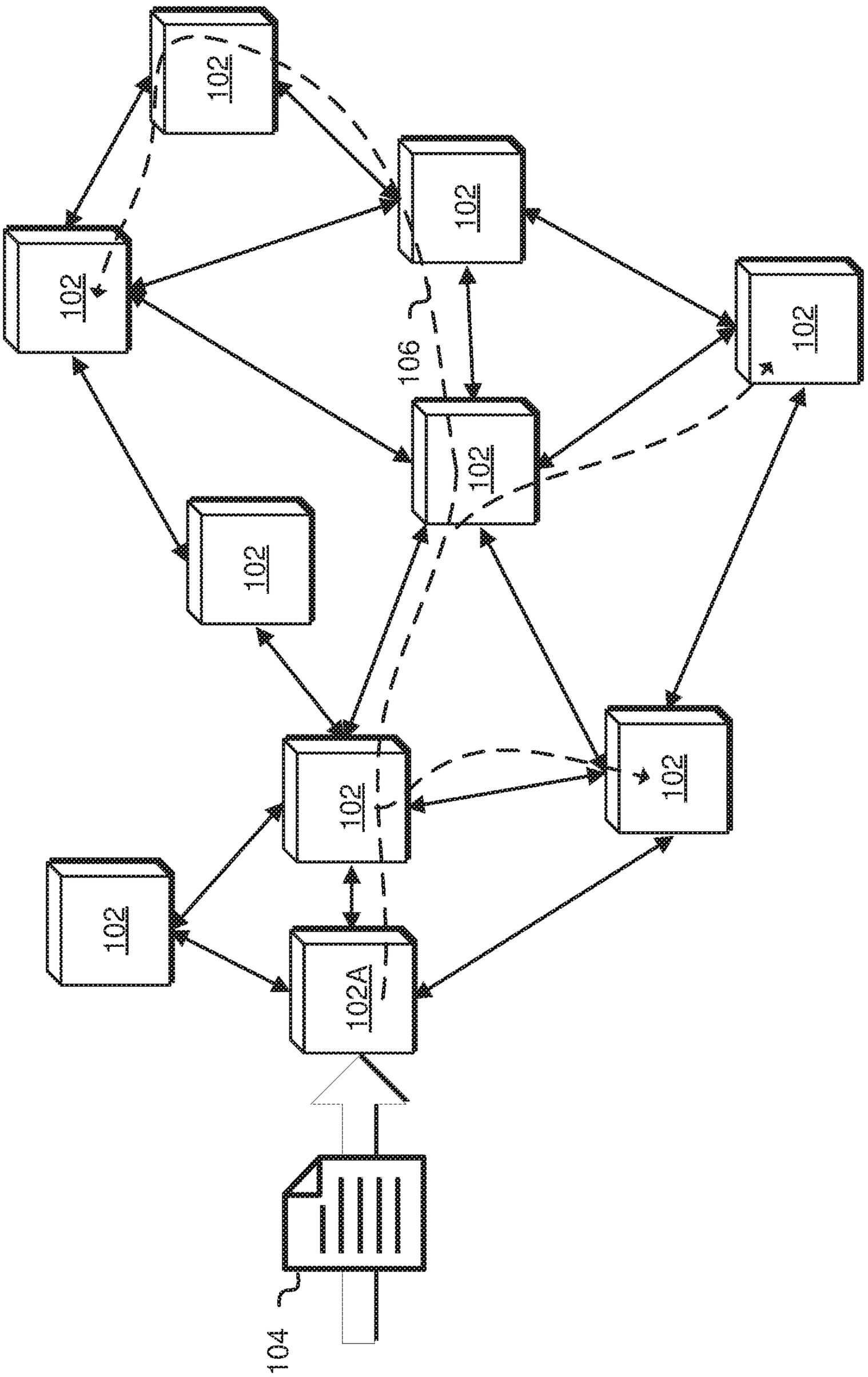


FIG. 1

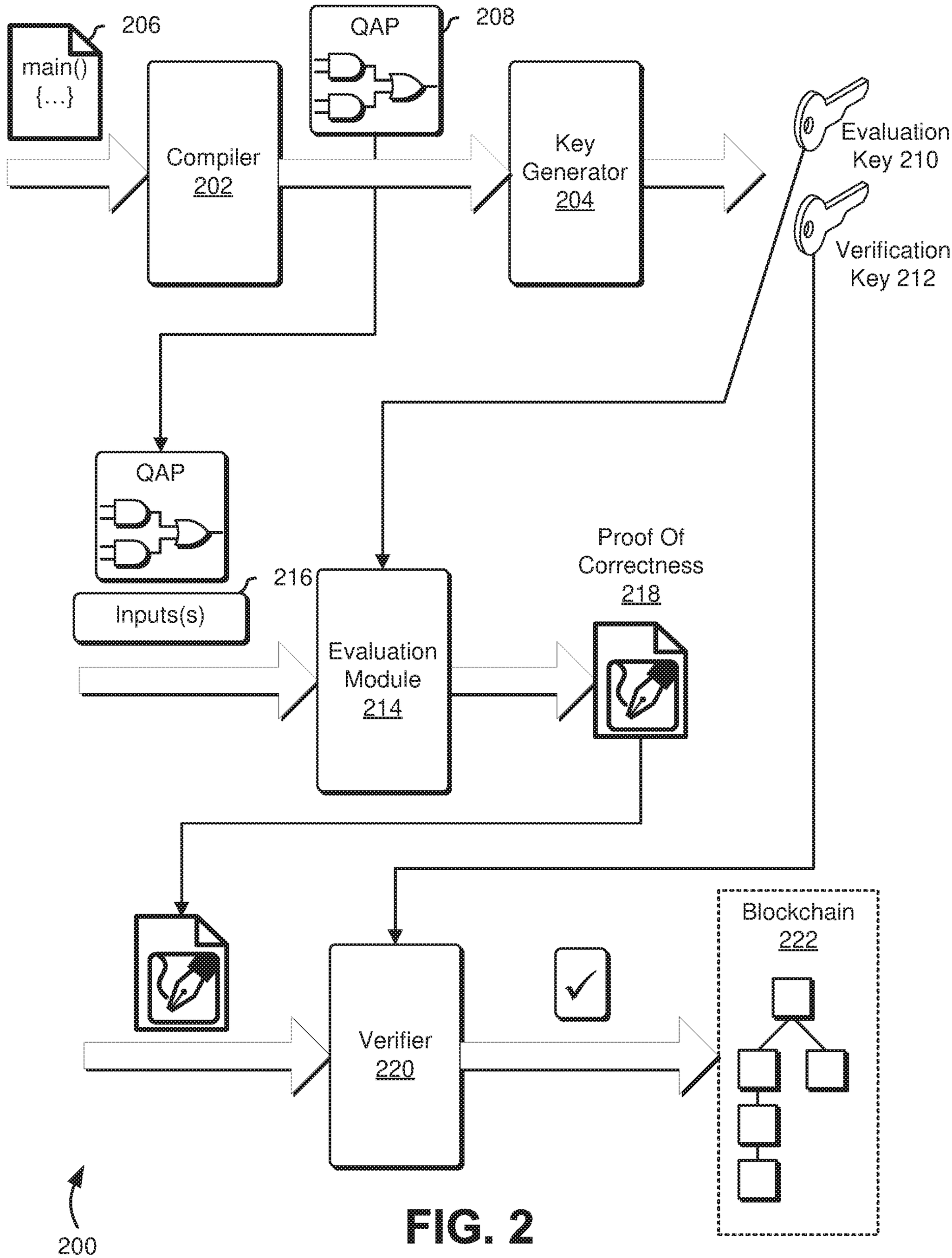

206
main()
{...}
Compiler
202
QAP
208
Key
Generator
204
Evaluation
Key 210
Verification
Key 212
QAP
Inputs(s)
216
Evaluation
Module
214
Proof Of
Correctness
218
Blockchain
222
Verifier
220
200

FIG. 2

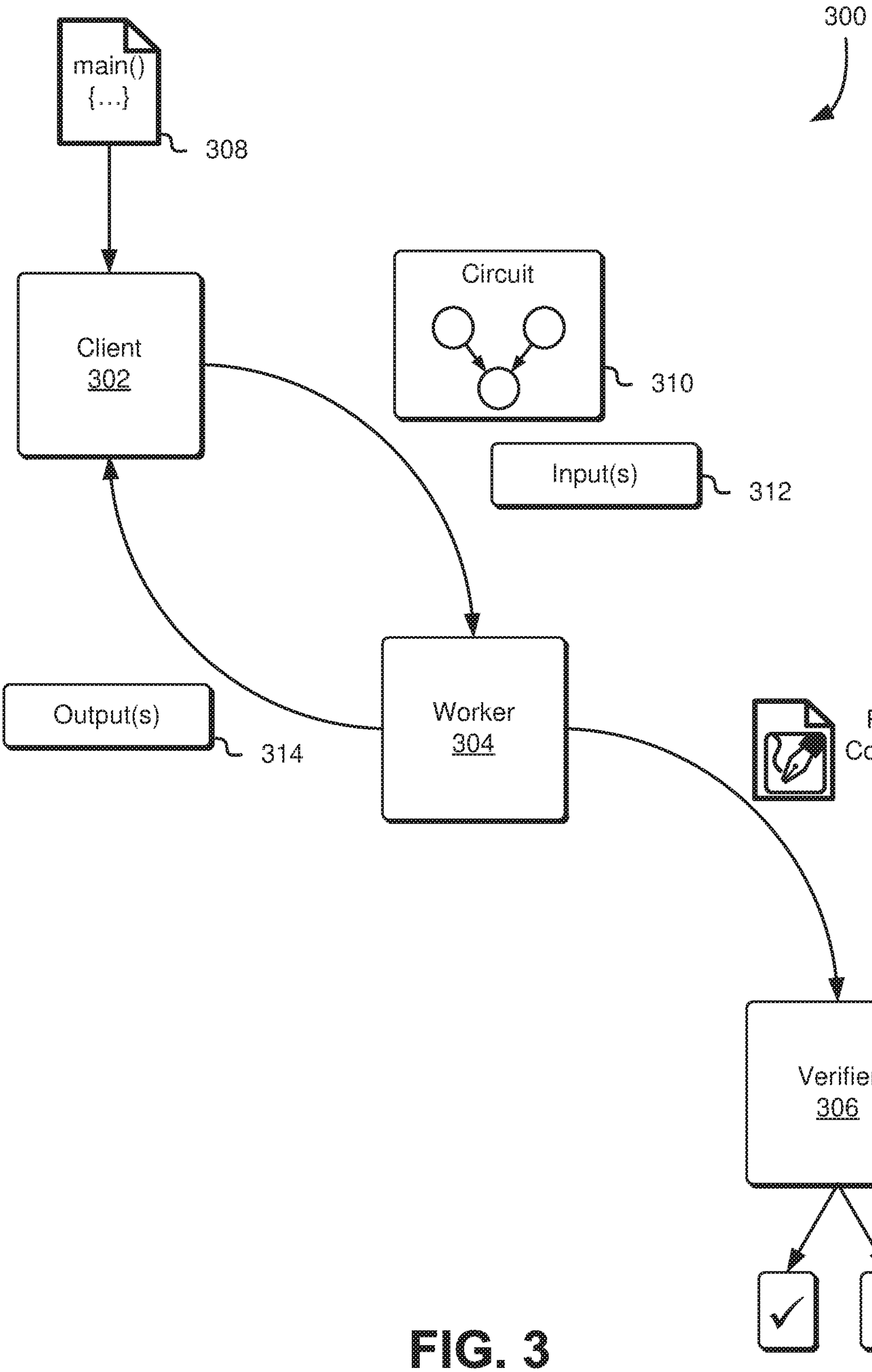

300
main()
{...}
308
Client
302
Circuit
310
Input(s)
312
Output(s)
314
Worker
304
Proof Of
Correctness
316
Verifier
306
✓
x

FIG. 3

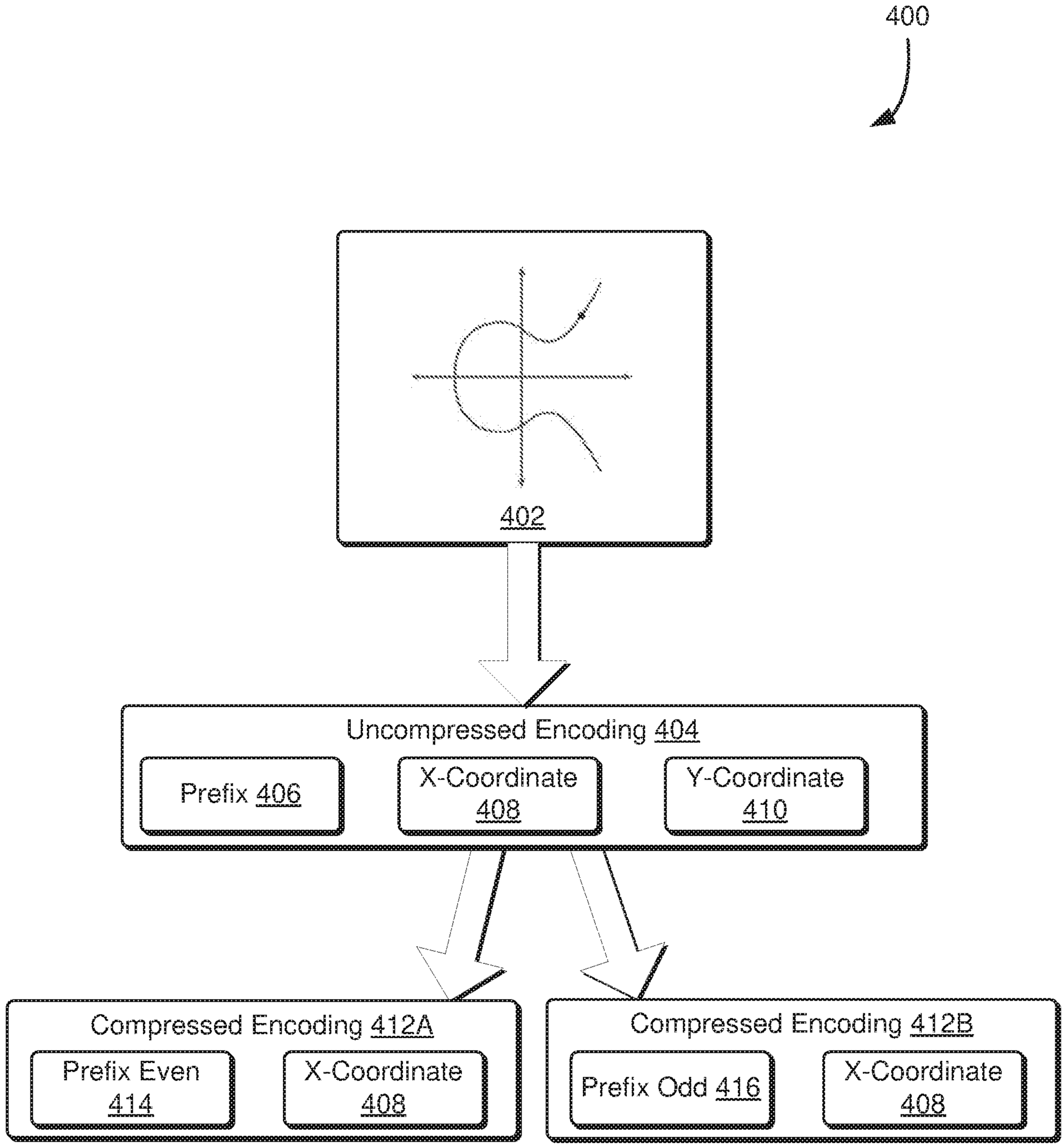

400
402
Uncompressed Encoding 404
Prefix 406
X-Coordinate 408
Y-Coordinate 410
Compressed Encoding 412A
Prefix Even 414
X-Coordinate 408
Compressed Encoding 412B
Prefix Odd 416
X-Coordinate 408

FIG. 4

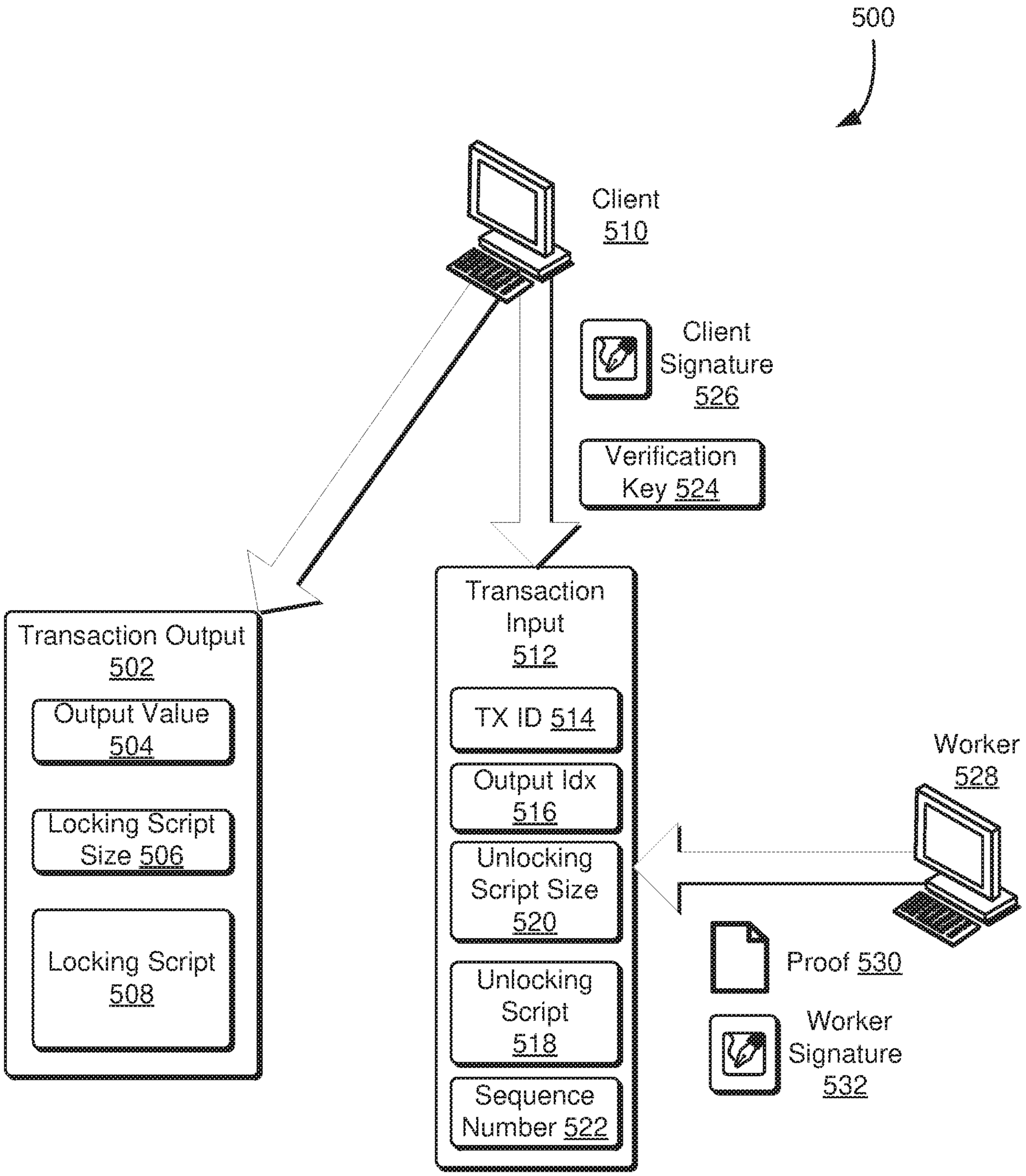

500
Client
510
Client
Signature
526
Verification
Key 524
Transaction
Input
512
TX ID 514
Output Idx
516
Unlocking
Script Size
520
Unlocking
Script
518
Sequence
Number 522
Worker
528
Proof 530
Worker
Signature
532
Transaction Output
502
Output Value
504
Locking Script
Size 506
Locking Script
508

FIG. 5

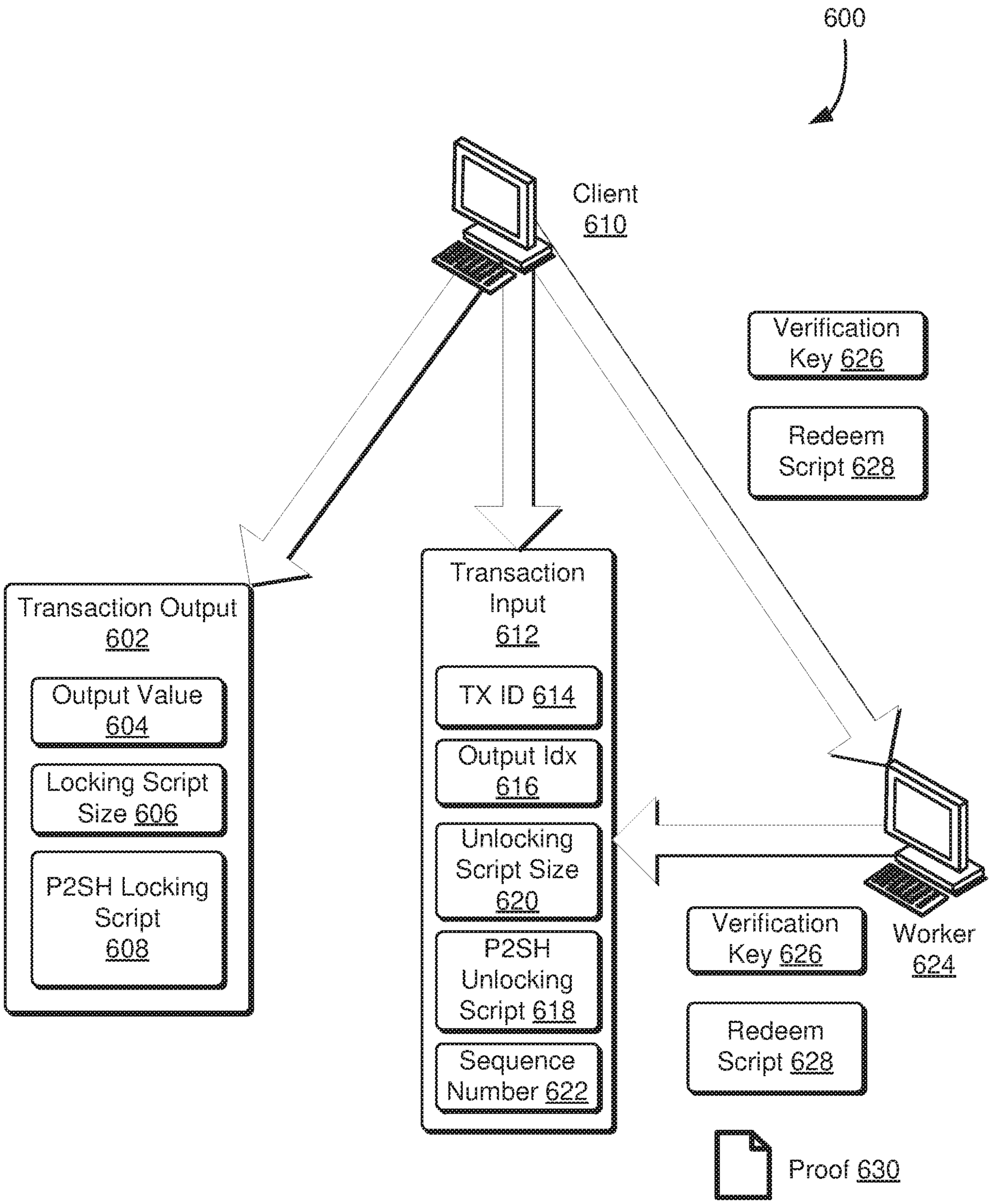

600
Client
610
Verification
Key 626
Redeem
Script 628
Transaction Output
602
Output Value
604
Locking Script
Size 606
P2SH Locking
Script
608
Transaction
Input
612
TX ID 614
Output Idx
616
Unlocking
Script Size
620
P2SH
Unlocking
Script 618
Sequence
Number 622
Verification
Key 626
Worker
624
Redeem
Script 628
Proof 630

FIG. 6

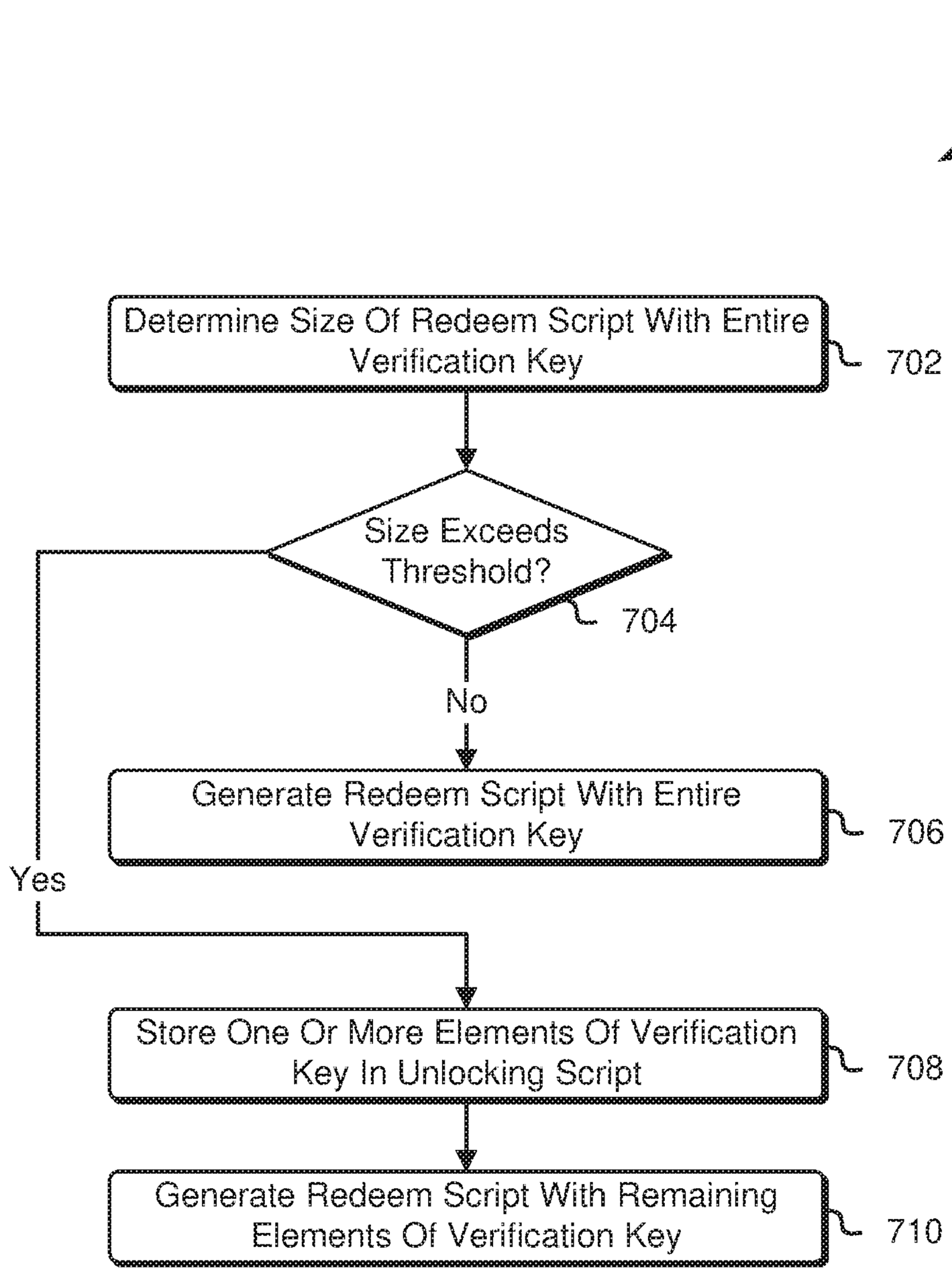

700
Determine Size Of Redeem Script With Entire Verification Key
702
Size Exceeds Threshold?
704
No
Yes
Generate Redeem Script With Entire Verification Key
706
Store One Or More Elements Of Verification Key In Unlocking Script
708
Generate Redeem Script With Remaining Elements Of Verification Key
710

FIG. 7

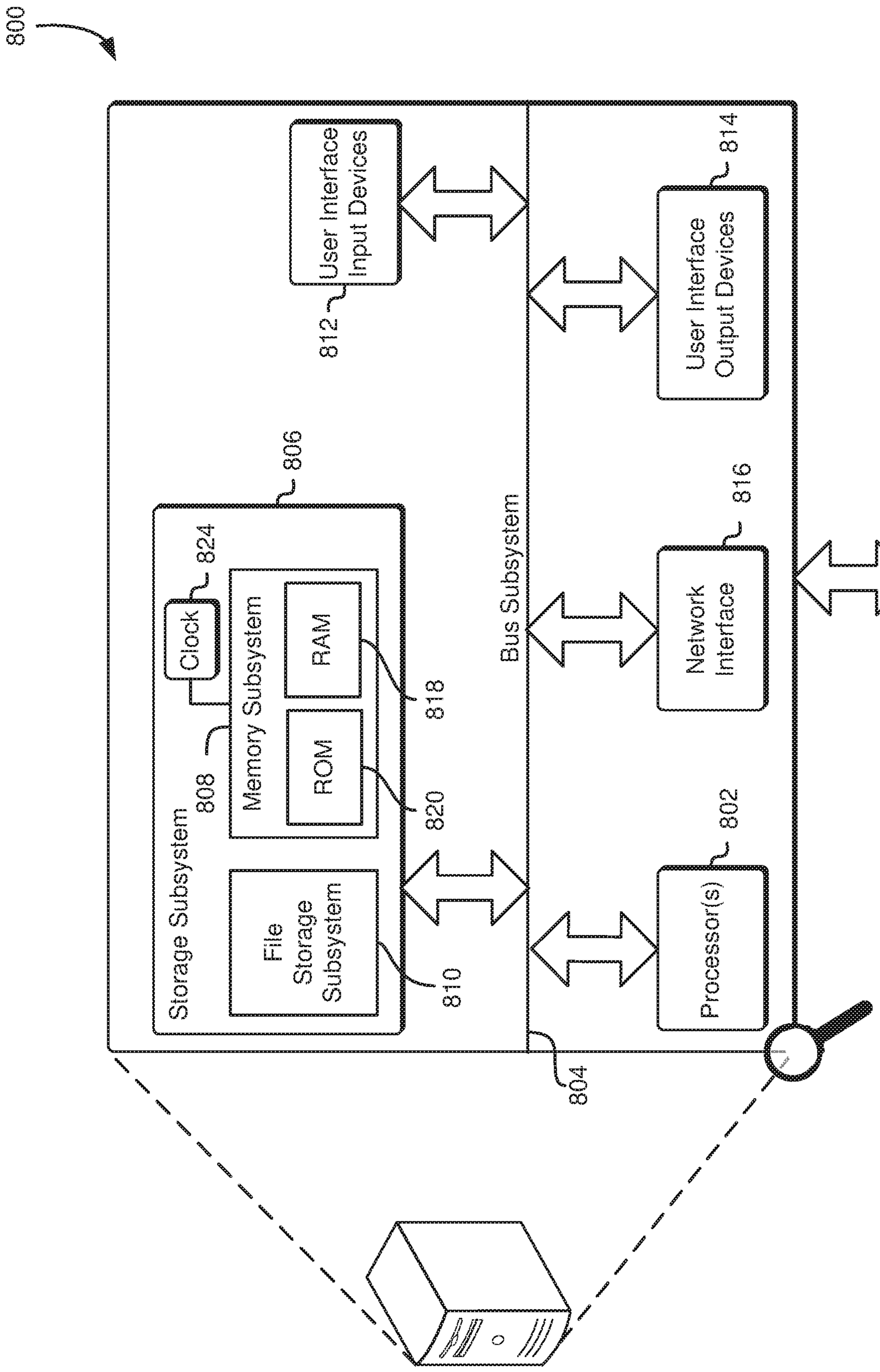

800
Storage Subsystem
808
Memory Subsystem
RAM
ROM
820
File Storage Subsystem
810
806
Clock
824
818
User Interface Input Devices
812
User Interface Output Devices
814
Bus Subsystem
Network Interface
816
Processor(s)
802
804

FIG. 8