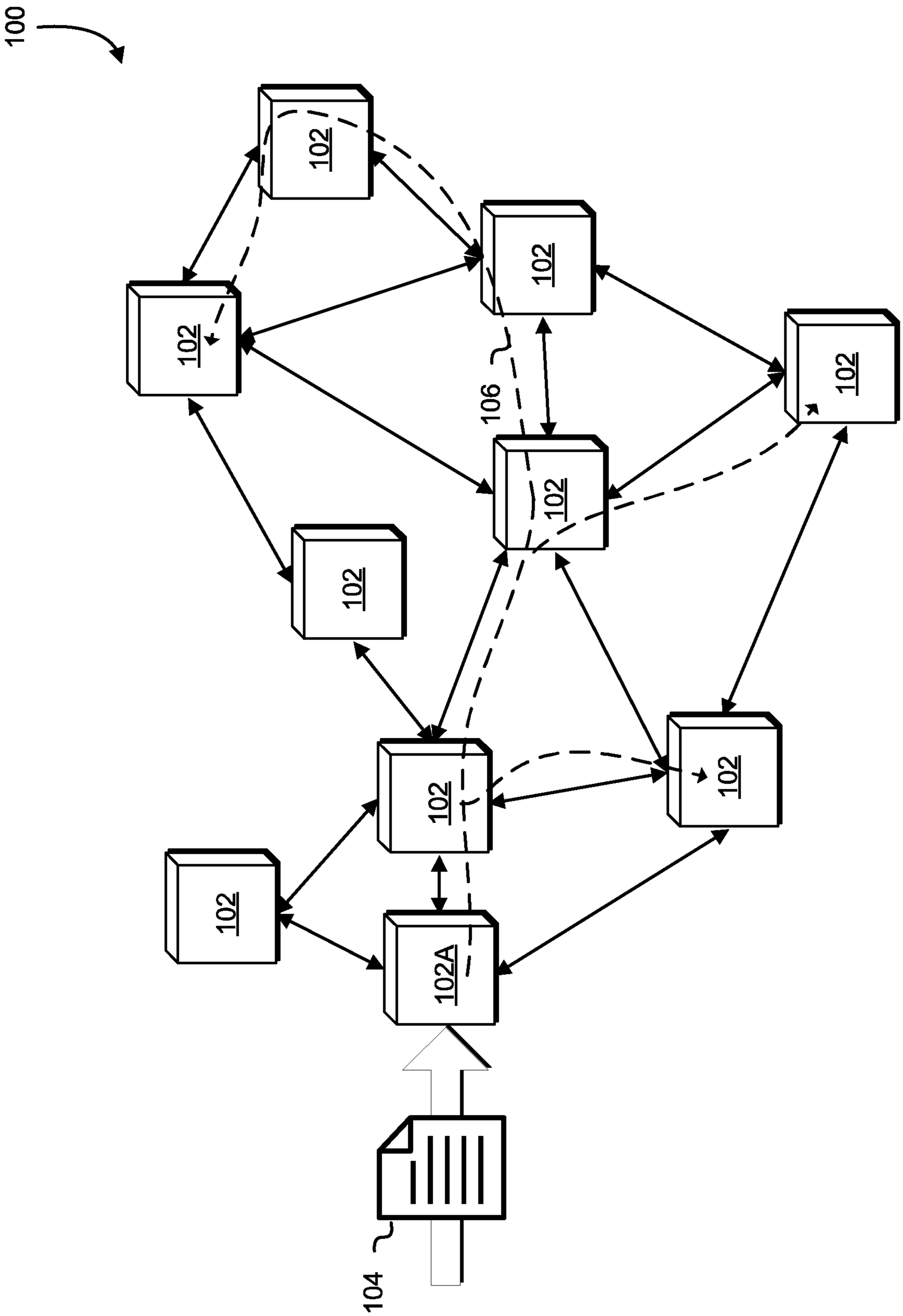


FIG. 1

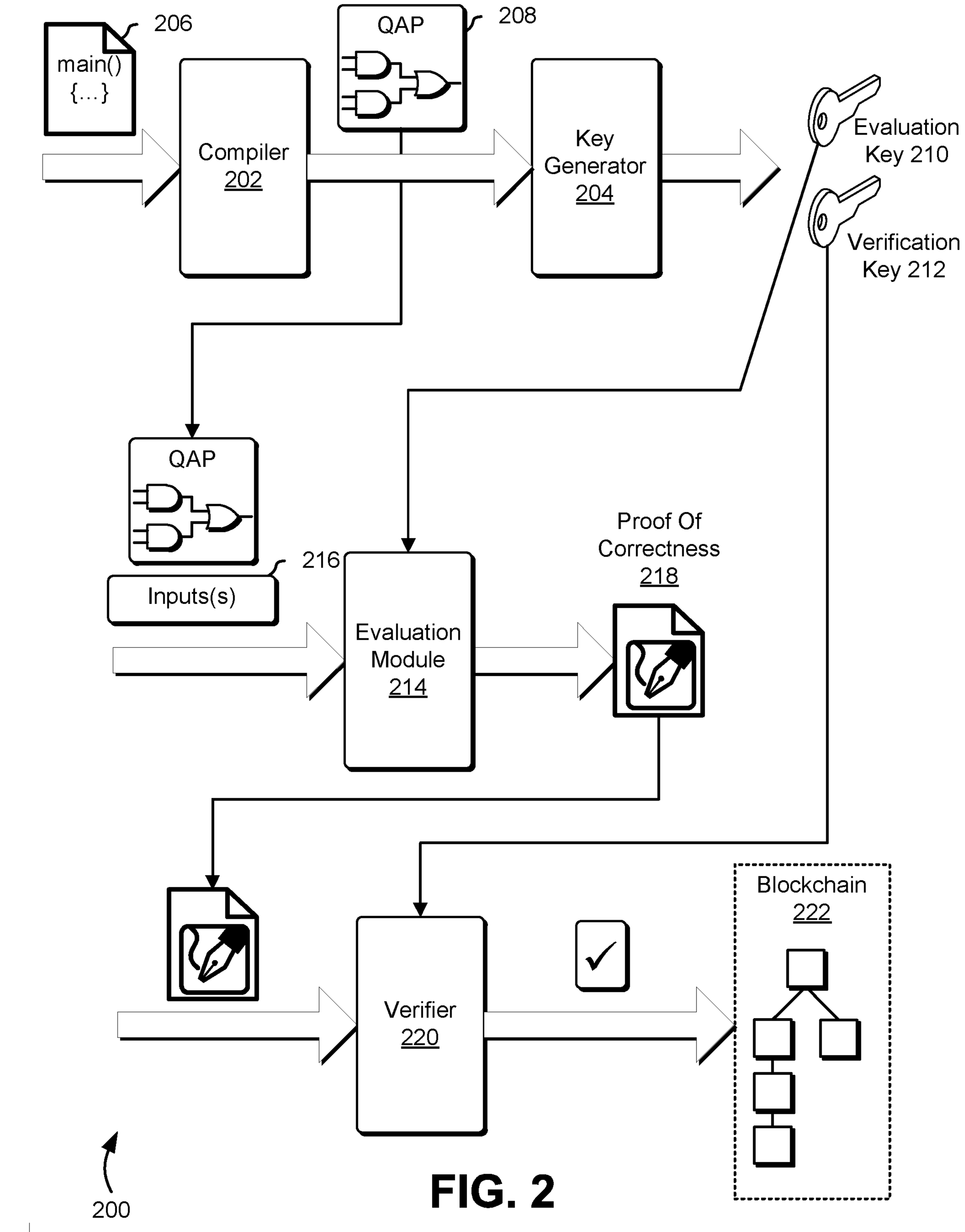

206
main()
{…}
Compiler
202
QAP
208
QAP
Key
Generator
204
Evaluation
Key 210
Verification
Key 212
QAP
216
Inputs(s)
Evaluation
Module
214
Proof Of
Correctness
218
Blockchain
222
Verifier
220
200

FIG. 2

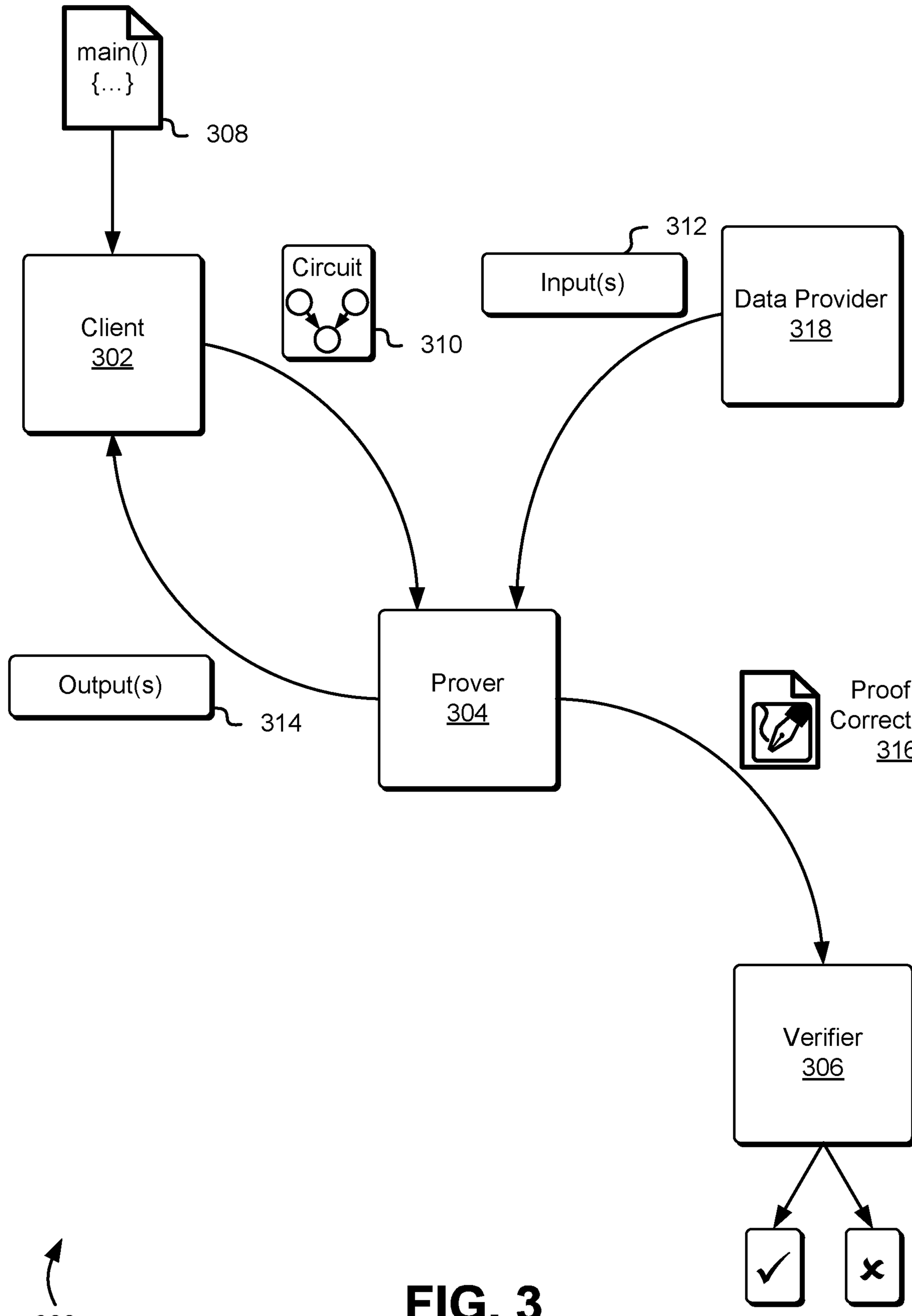

main()
{…}
308
Client
302
Circuit
310
312
Input(s)
Data Provider
318
Output(s)
314
Prover
304
Proof Of
Correctness
316
Verifier
306
300

FIG. 3

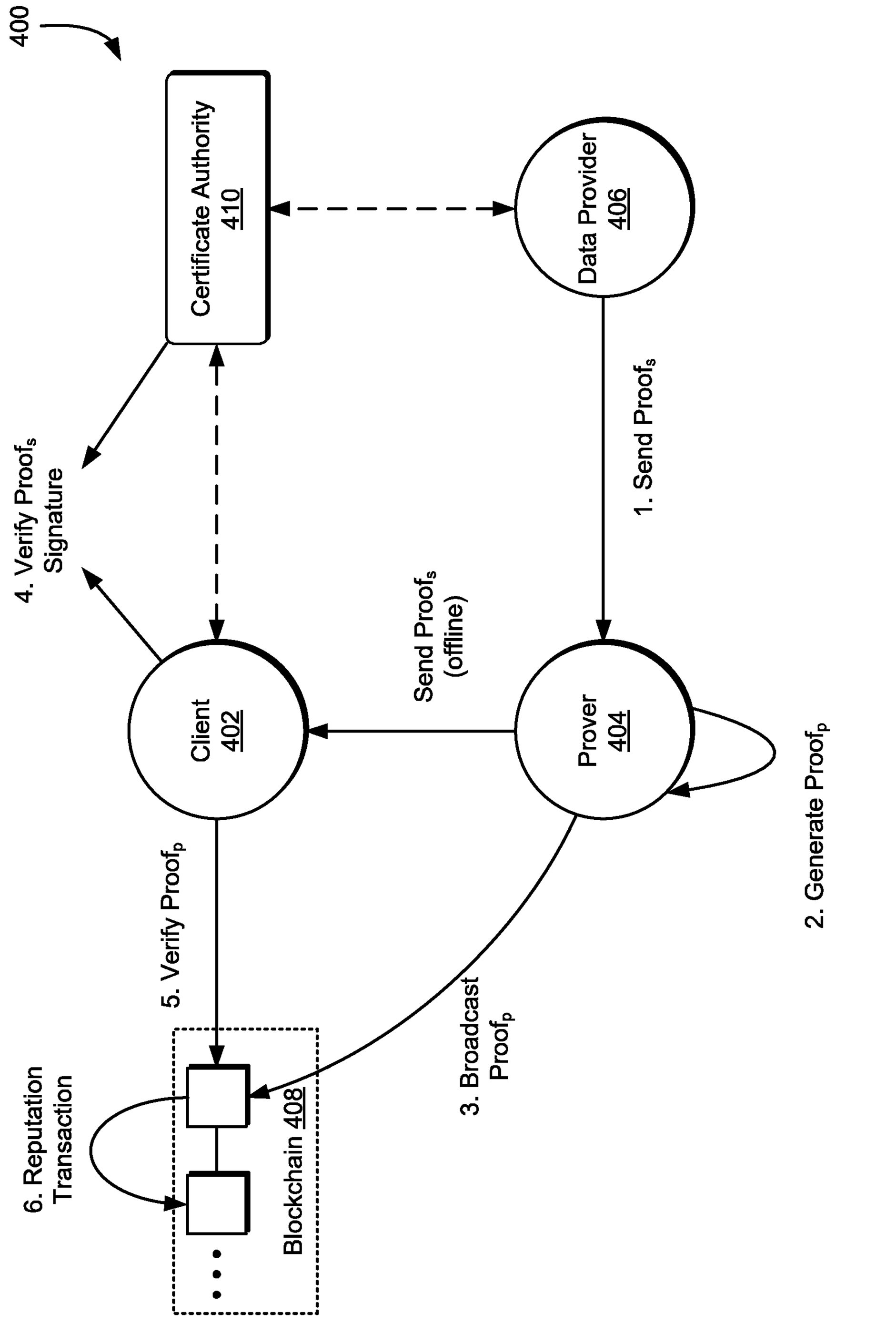

400
Certificate Authority
410
Data Provider
406
1. Send Proof$_s$
Send Proof$_s$
(offline)
4. Verify Proof$_s$
Signature
Client
402
Prover
404
2. Generate Proof$_p$
3. Broadcast
Proof$_p$
5. Verify Proof$_p$
6. Reputation
Transaction
Blockchain 408

FIG. 4

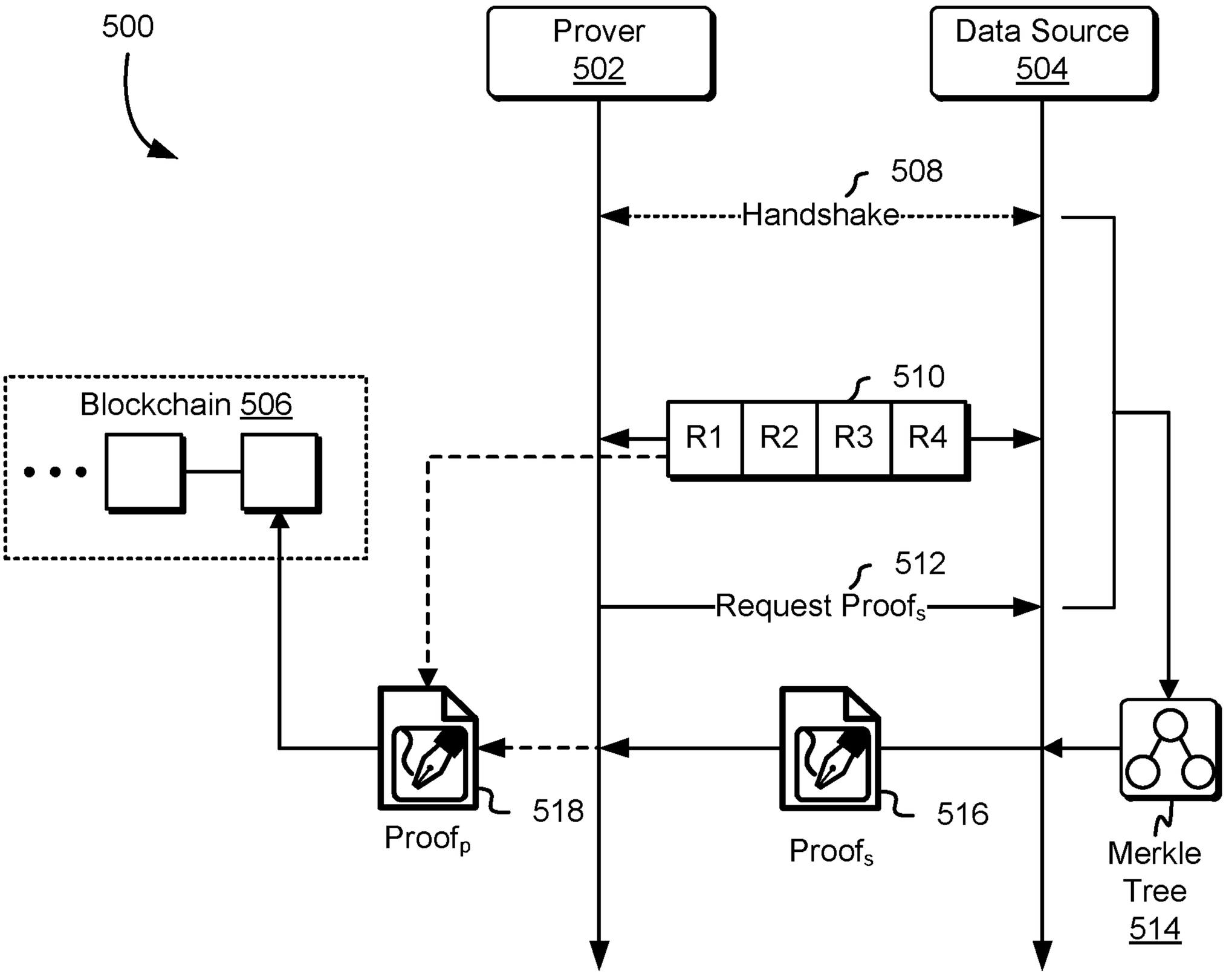

500
Prover
502
Data Source
504
508
Handshake
Blockchain 506
510
R1
R2
R3
R4
512
Request Proof$_s$
518
Proof$_p$
516
Proof$_s$
Merkle
Tree
514

FIG. 5

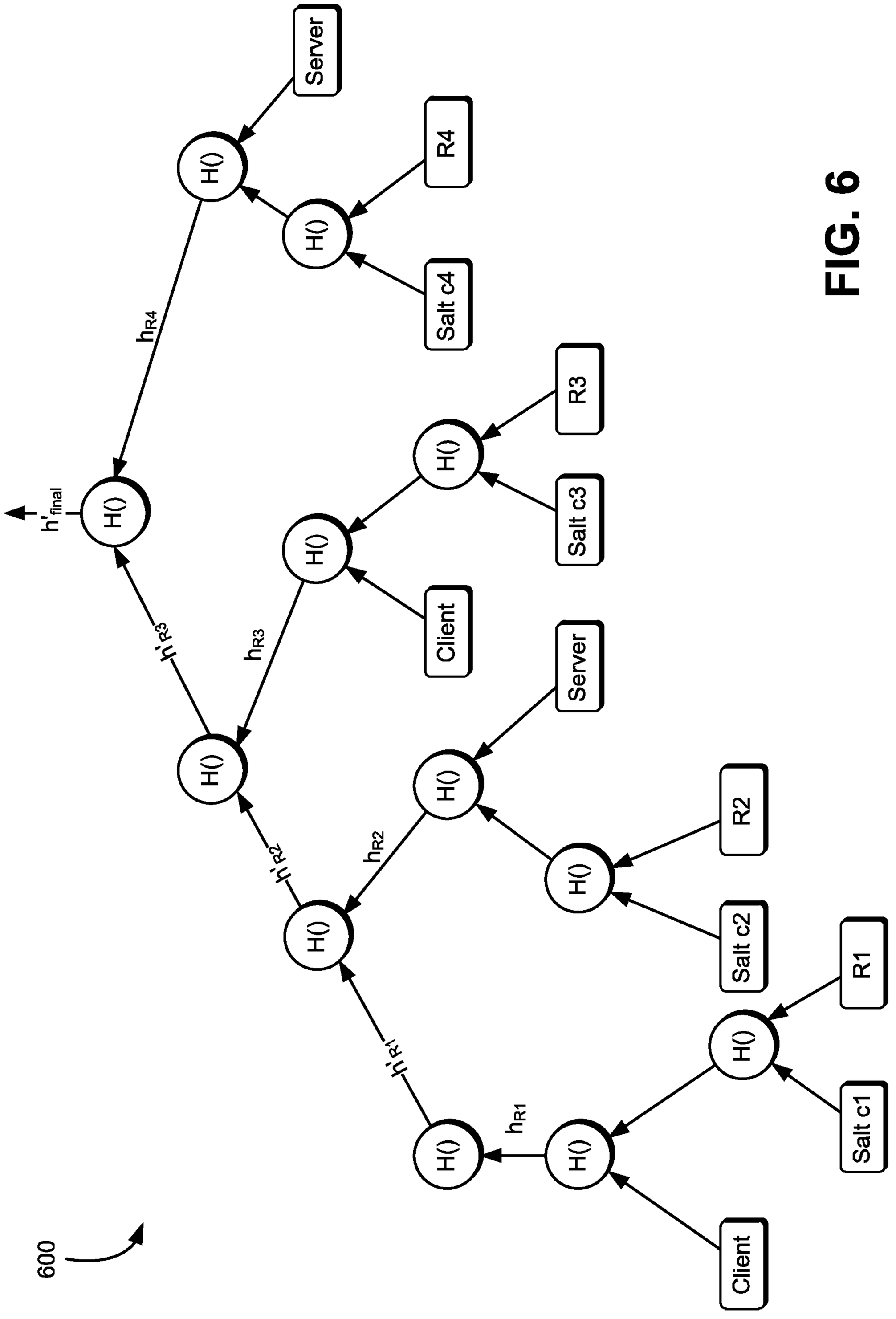

600
Client
Salt c1
R1
Salt c2
R2
Server
Client
Salt c3
R3
Salt c4
R4
Server
H()
h'_{final}
h'_{R4}
h'_{R3}
h'_{R2}
h'_{R1}
h_{R4}
h_{R3}
h_{R2}
h_{R1}

FIG. 6

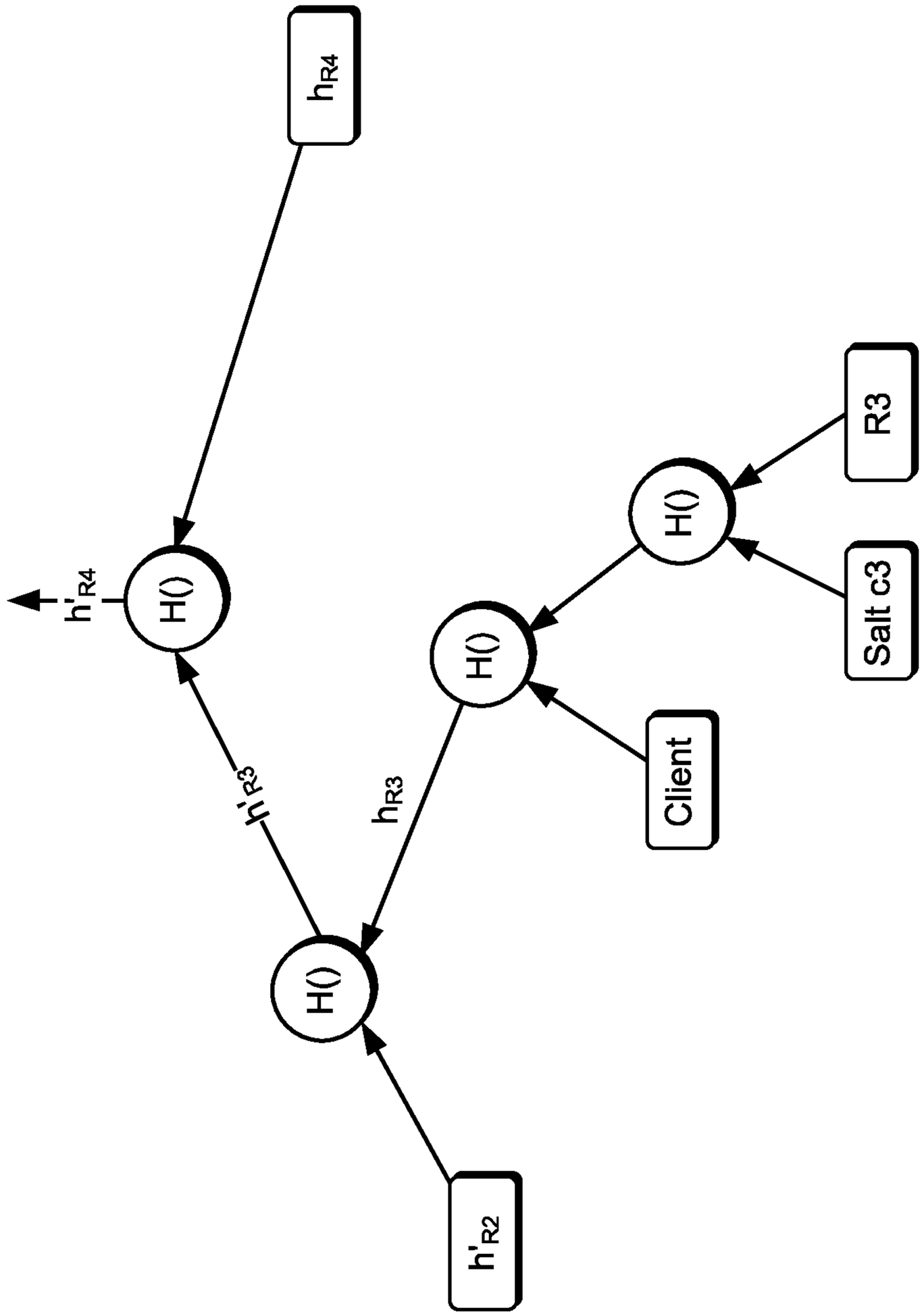
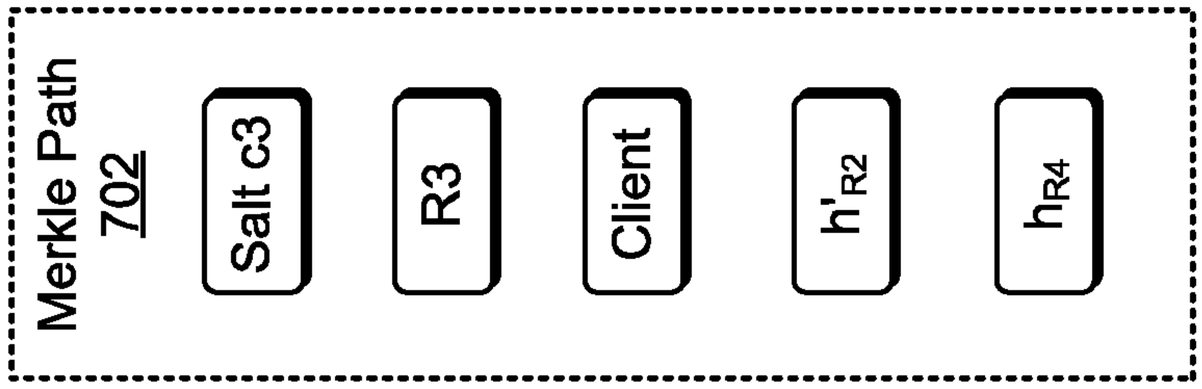

H()
H()
H()
H()
H()
Client
Salt c3
R3
h_{R4}
h'_{R4}
h'_{R3}
h_{R3}
h'_{R2}

FIG. 7

700


Merkle Path
702
Salt c3
R3
Client
h'_{R2}
h_{R4}

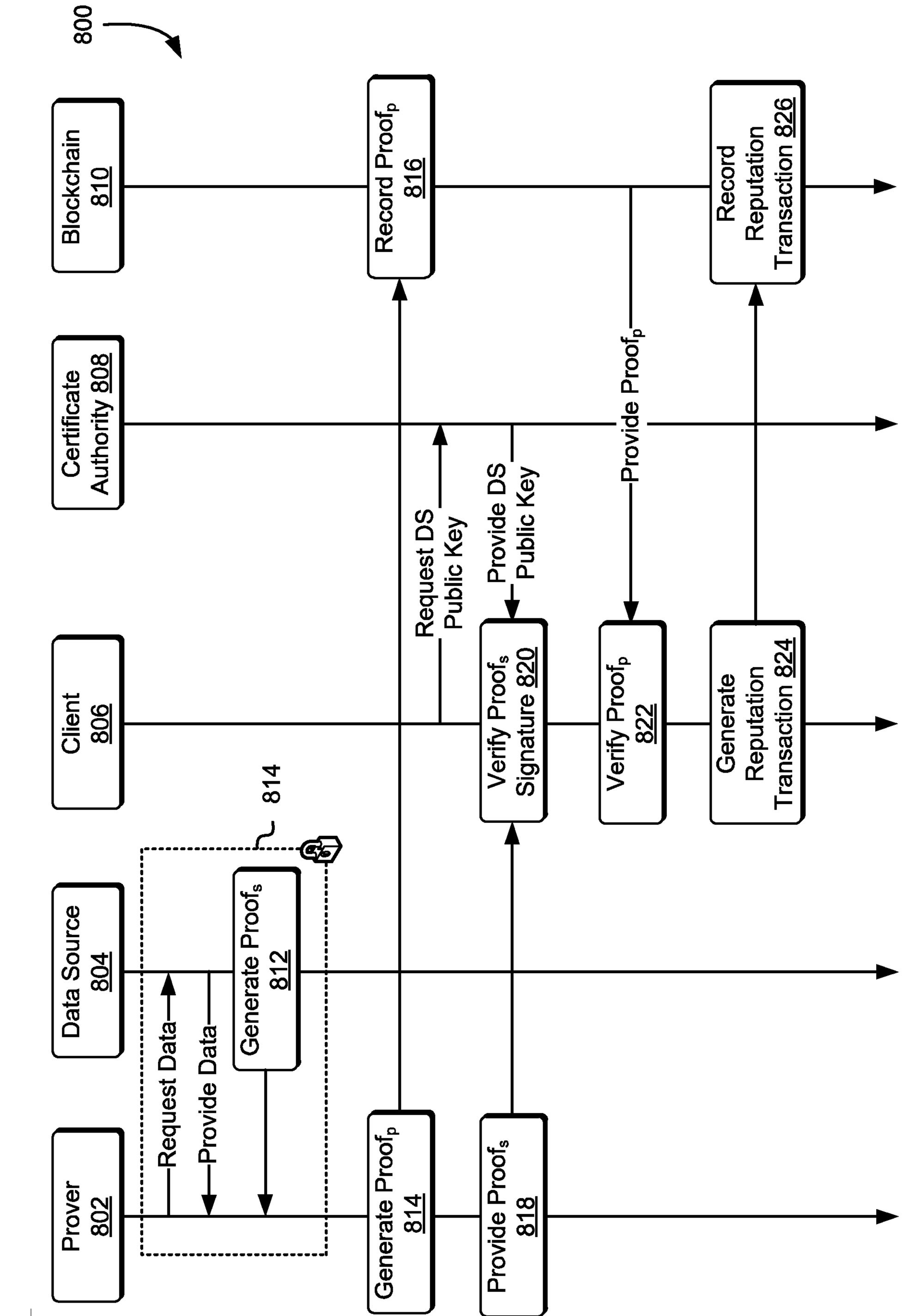

800
Prover 802
Data Source 804
Client 806
Certificate Authority 808
Blockchain 810
Request Data
Provide Data
Generate Proof$_s$ 812
814
Request DS Public Key
Provide DS Public Key
Generate Proof$_p$ 814
Provide Proof$_s$ 818
Verify Proof$_s$ Signature 820
Verify Proof$_p$ 822
Generate Reputation Transaction 824
Provide Proof$_p$
Record Proof$_p$ 816
Record Reputation Transaction 826

FIG. 8

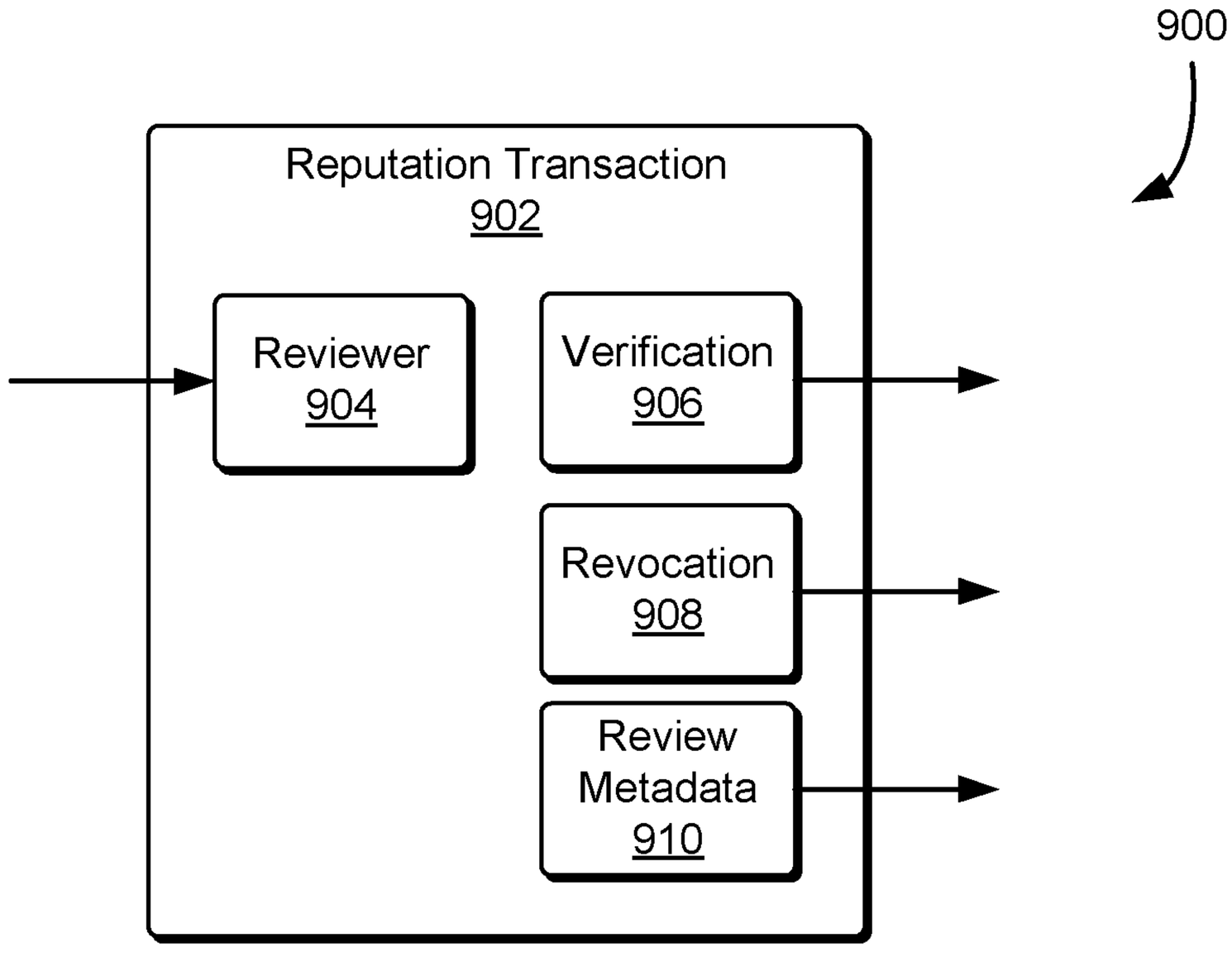

900
Reputation Transaction
902
Reviewer
904
Verification
906
Revocation
908
Review
Metadata
910

FIG. 9

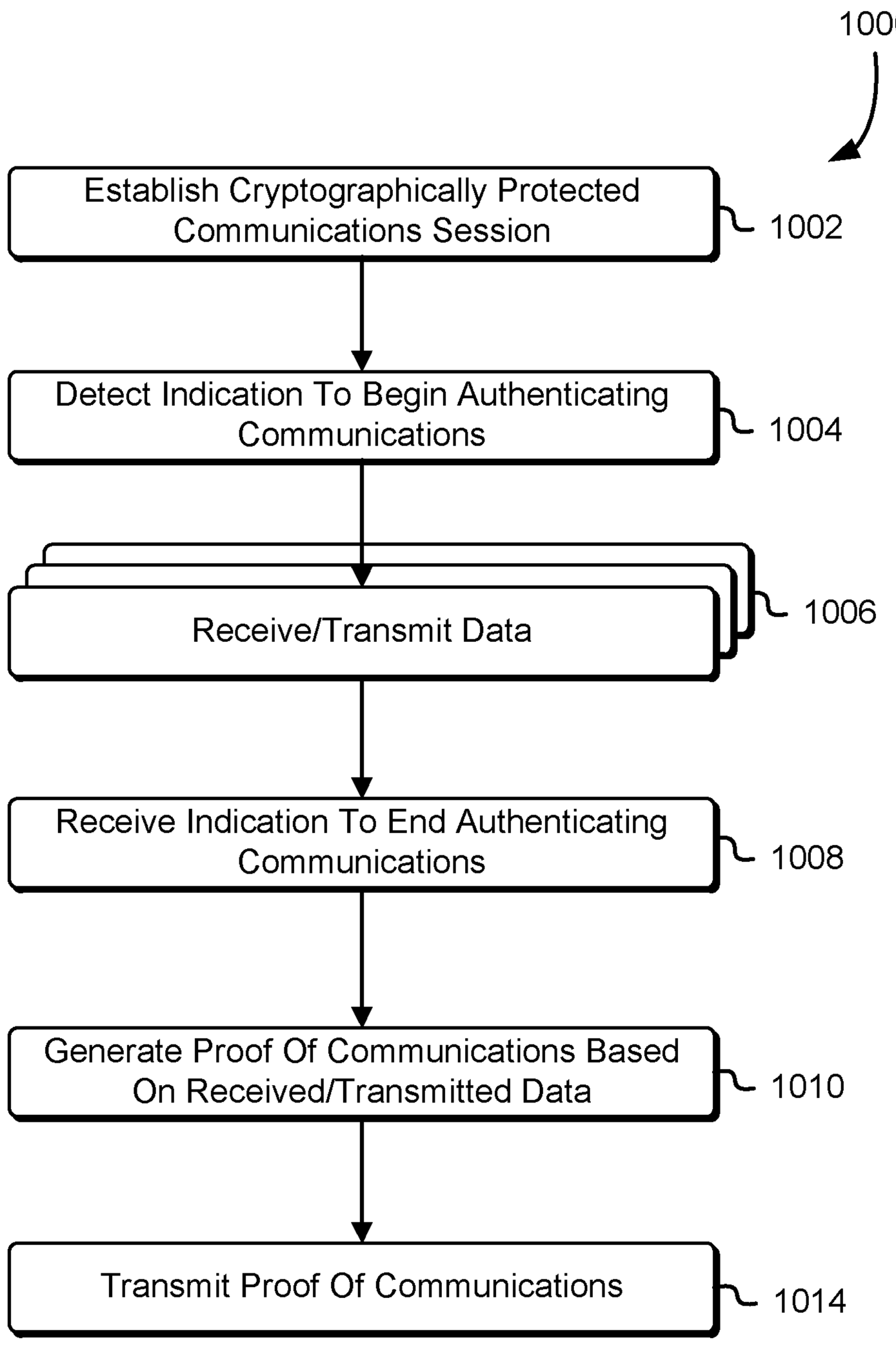

1000
Establish Cryptographically Protected Communications Session
1002
Detect Indication To Begin Authenticating Communications
1004
Receive/Transmit Data
1006
Receive Indication To End Authenticating Communications
1008
Generate Proof Of Communications Based On Received/Transmitted Data
1010
Transmit Proof Of Communications
1014

FIG. 10

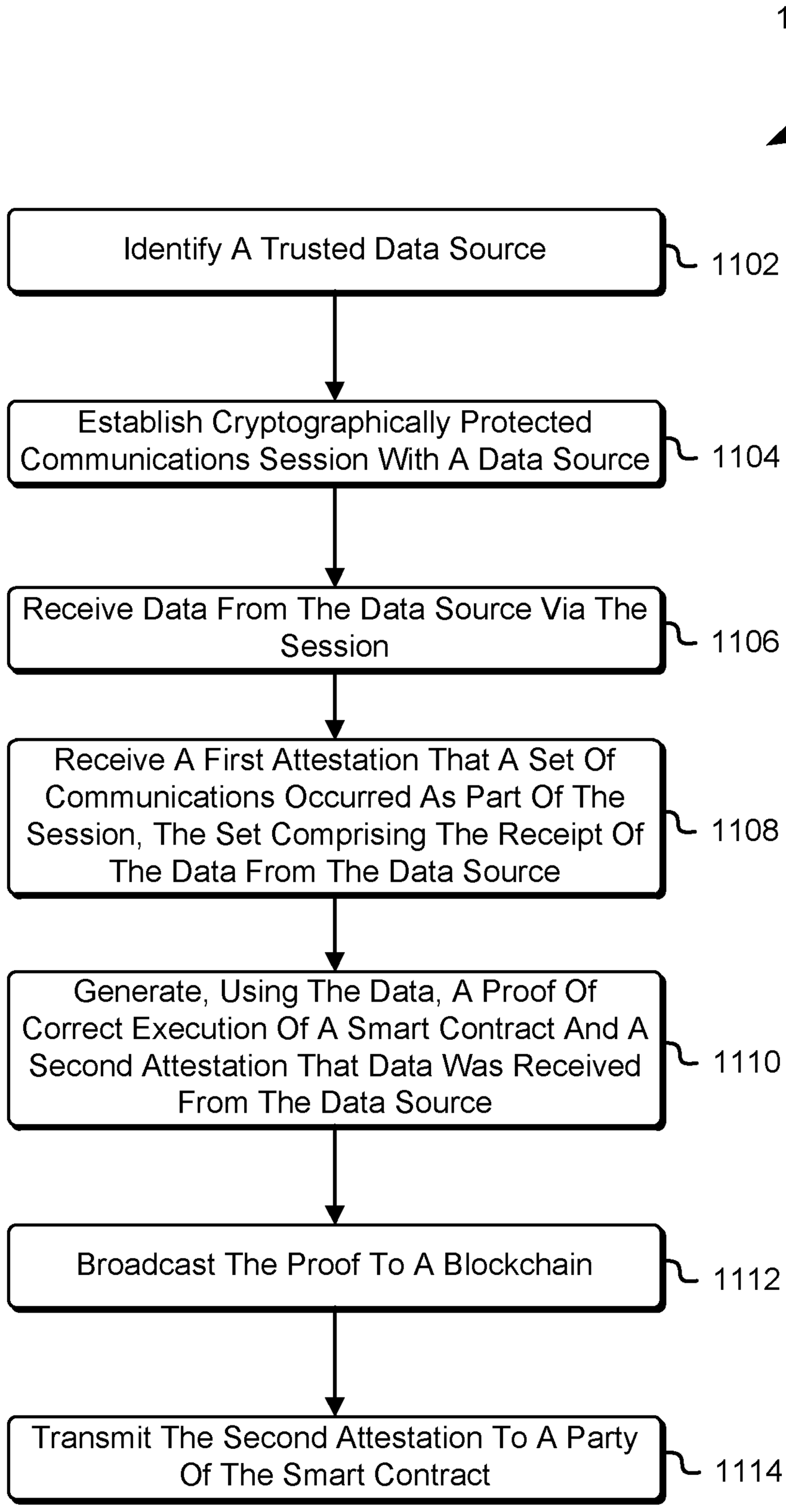

1100
Identify A Trusted Data Source
1102
Establish Cryptographically Protected Communications Session With A Data Source
1104
Receive Data From The Data Source Via The Session
1106
Receive A First Attestation That A Set Of Communications Occurred As Part Of The Session, The Set Comprising The Receipt Of The Data From The Data Source
1108
Generate, Using The Data, A Proof Of Correct Execution Of A Smart Contract And A Second Attestation That Data Was Received From The Data Source
1110
Broadcast The Proof To A Blockchain
1112
Transmit The Second Attestation To A Party Of The Smart Contract
1114

FIG. 11

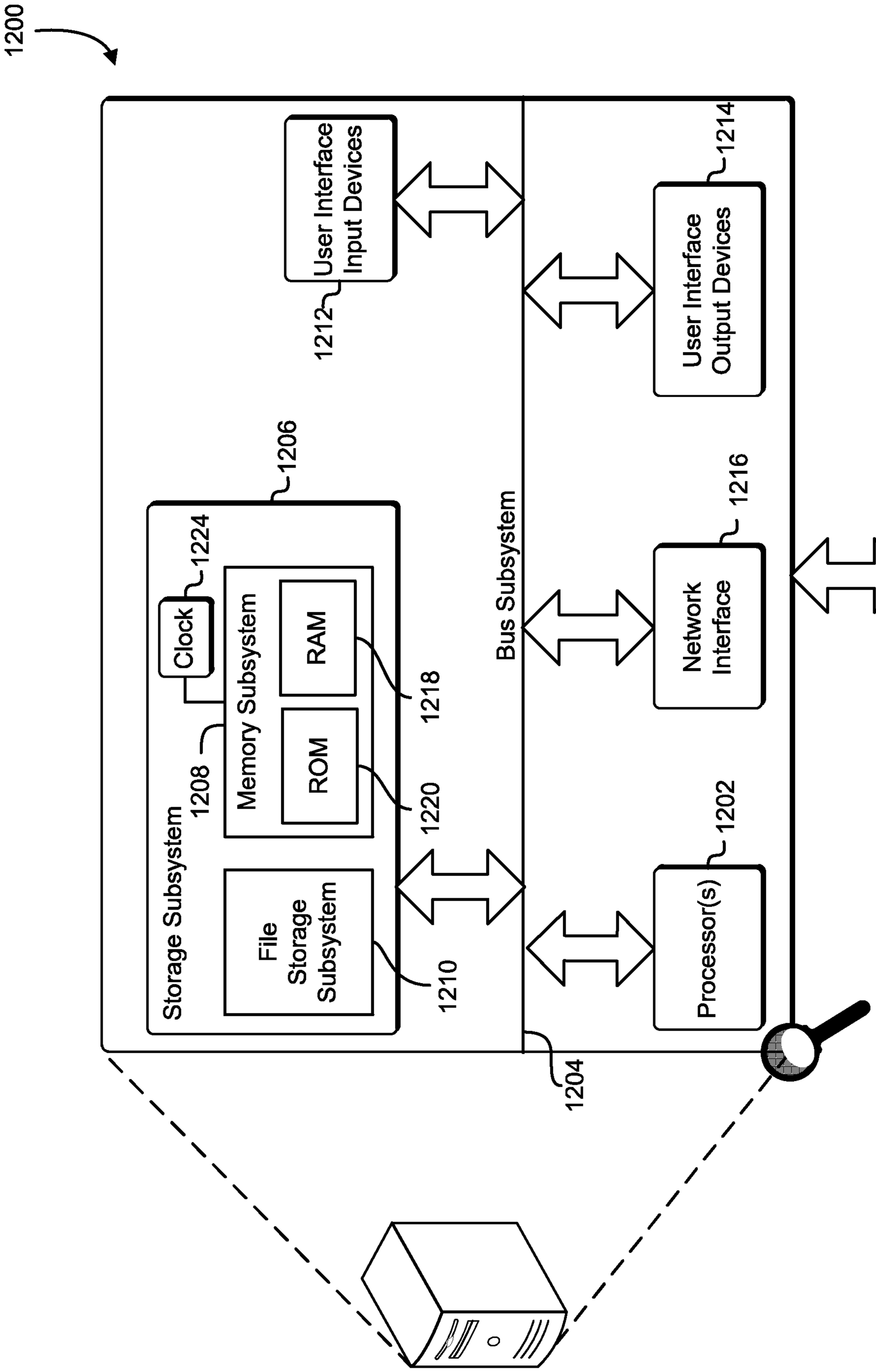

1200
User Interface Input Devices
1212
User Interface Output Devices
1214
Bus Subsystem
Network Interface
1216
Clock
1224
Storage Subsystem
1208
Memory Subsystem
RAM
ROM
1218
1220
File Storage Subsystem
1210
1206
Processor(s)
1202
1204

FIG. 12