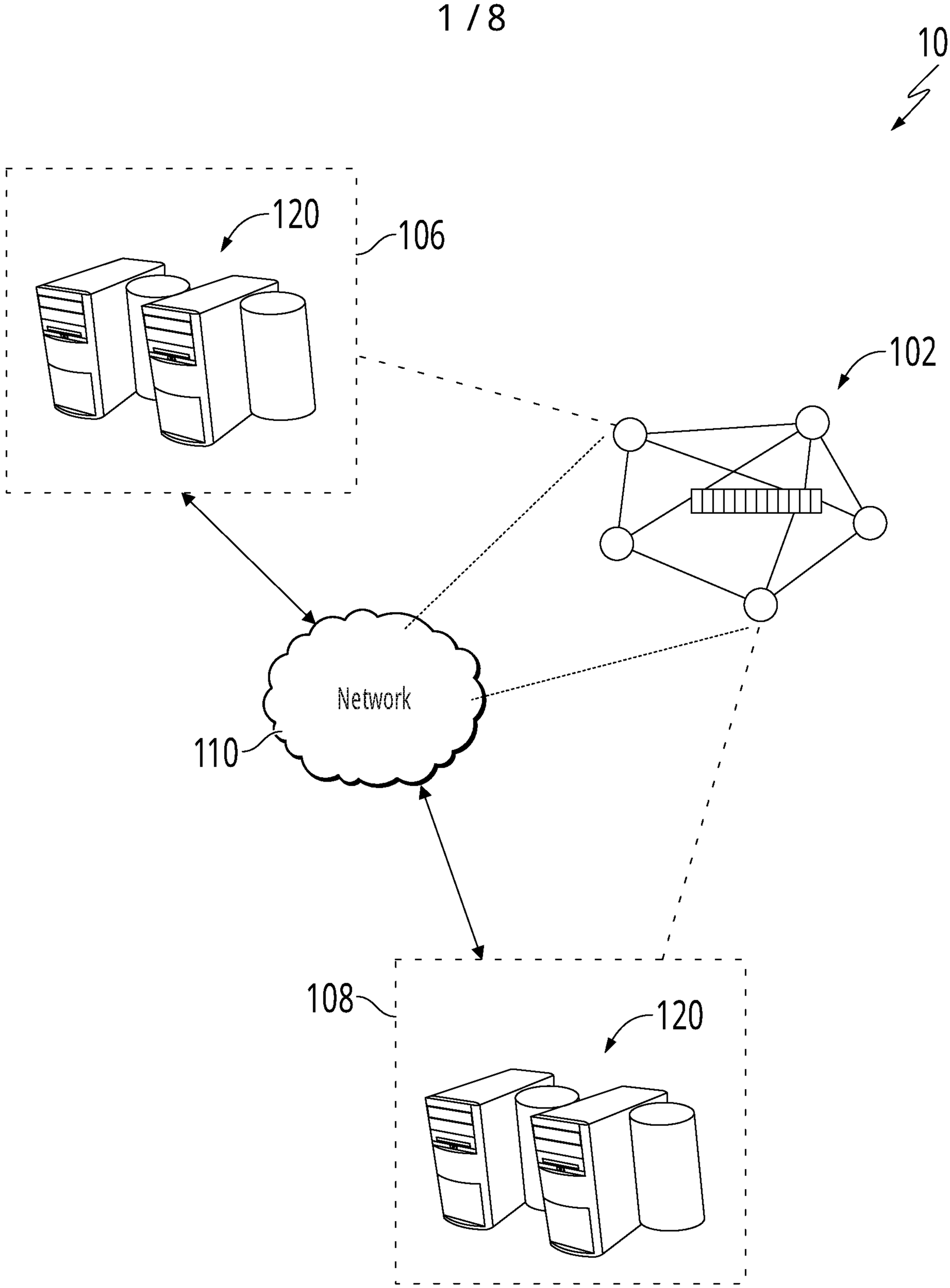


FIG. 1

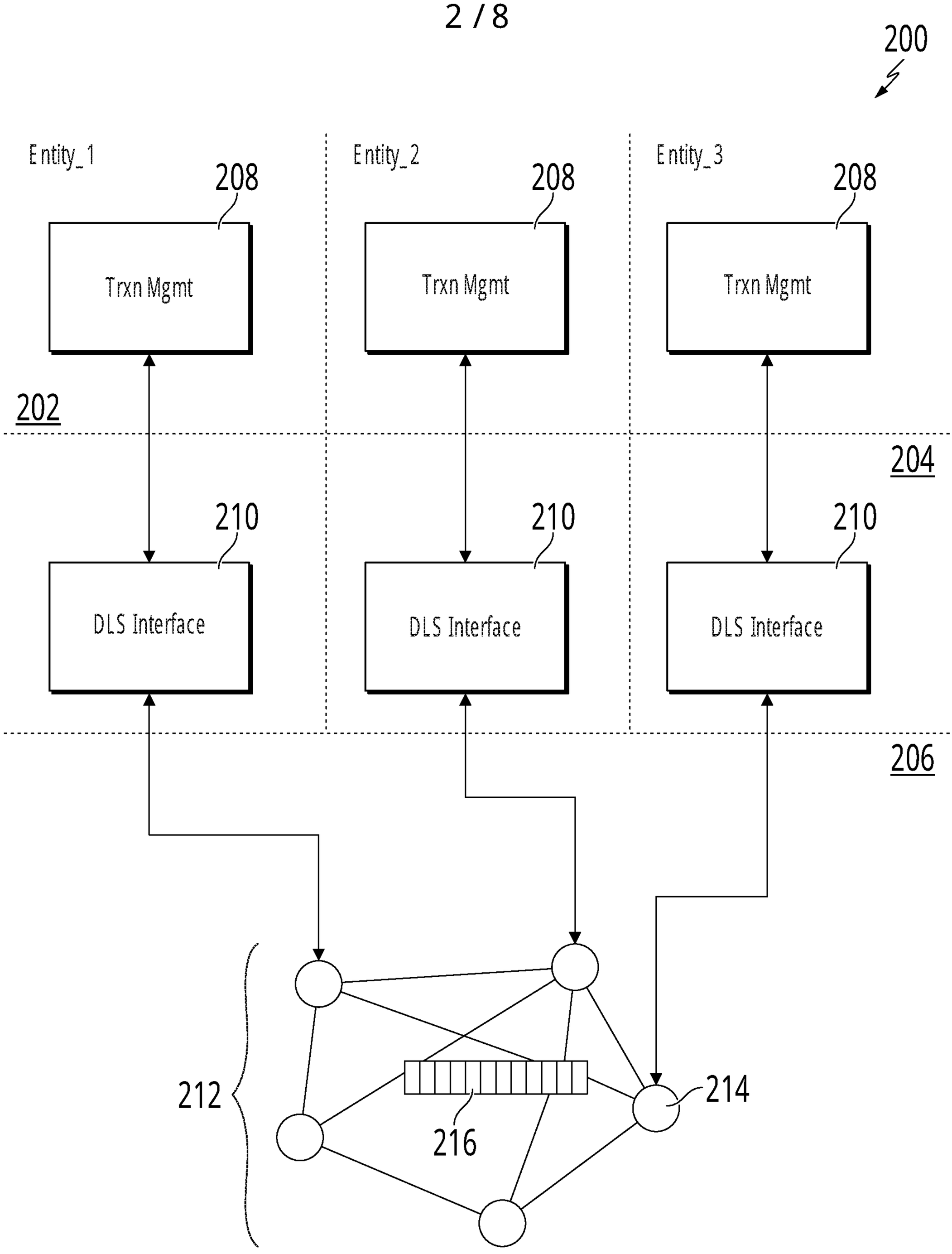

200
Entity_1
Entity_2
Entity_3
208
208
208
Trxn Mgmt
Trxn Mgmt
Trxn Mgmt
202
204
210
210
210
DLS Interface
DLS Interface
DLS Interface
206
212
214
216

FIG. 2

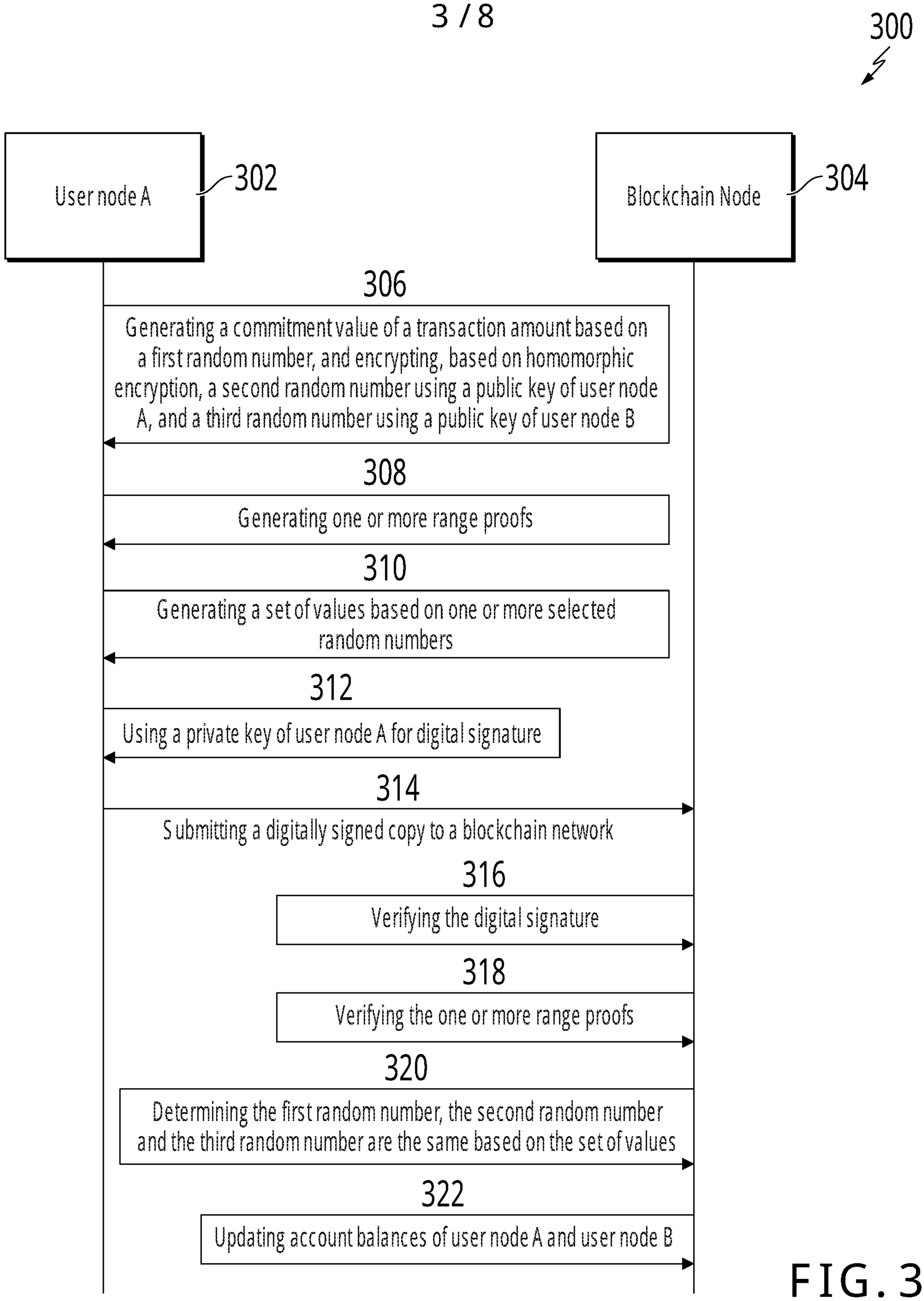

300
User node A
302
Blockchain Node
304
306
Generating a commitment value of a transaction amount based on a first random number, and encrypting, based on homomorphic encryption, a second random number using a public key of user node A, and a third random number using a public key of user node B
308
Generating one or more range proofs
310
Generating a set of values based on one or more selected random numbers
312
Using a private key of user node A for digital signature
314
Submitting a digitally signed copy to a blockchain network
316
Verifying the digital signature
318
Verifying the one or more range proofs
320
Determining the first random number, the second random number and the third random number are the same based on the set of values
322
Updating account balances of user node A and user node B

FIG. 3

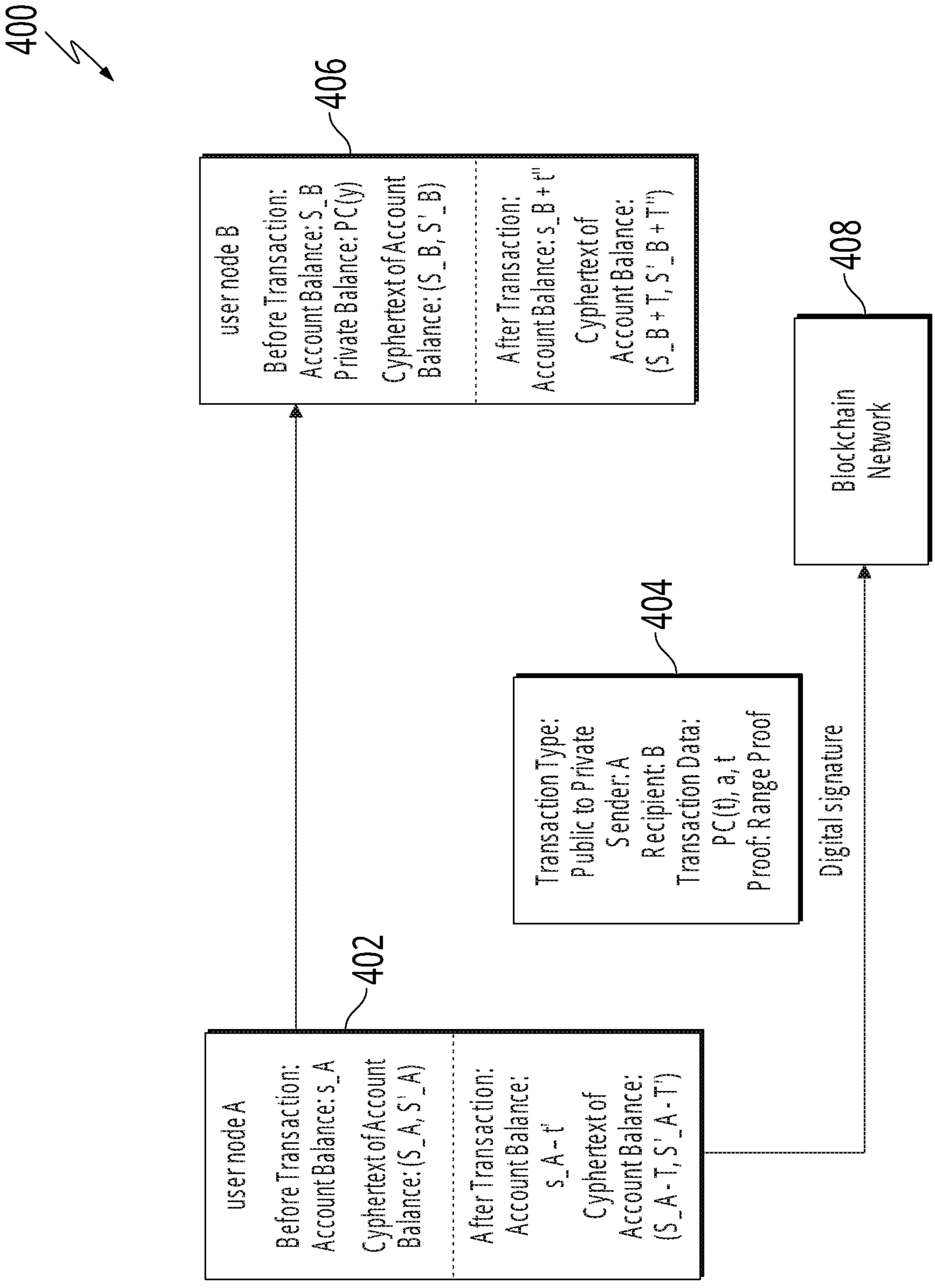

400
406
user node B
Before Transaction:
Account Balance: S_B
Private Balance: PC(y)
Cyphertext of Account
Balance: (S_B, S'_B)
After Transaction:
Account Balance: s_B + t''
Cyphertext of
Account Balance:
(S_B + T, S'_B + T'')
408
Blockchain
Network
404
Transaction Type:
Public to Private
Sender: A
Recipient: B
Transaction Data:
PC(t), a, t
Proof: Range Proof
Digital signature
402
user node A
Before Transaction:
Account Balance: s_A
Cyphertext of Account
Balance: (S_A, S'_A)
After Transaction:
Account Balance:
s_A - t'
Cyphertext of
Account Balance:
(S_A - T, S'_A - T')

FIG. 4

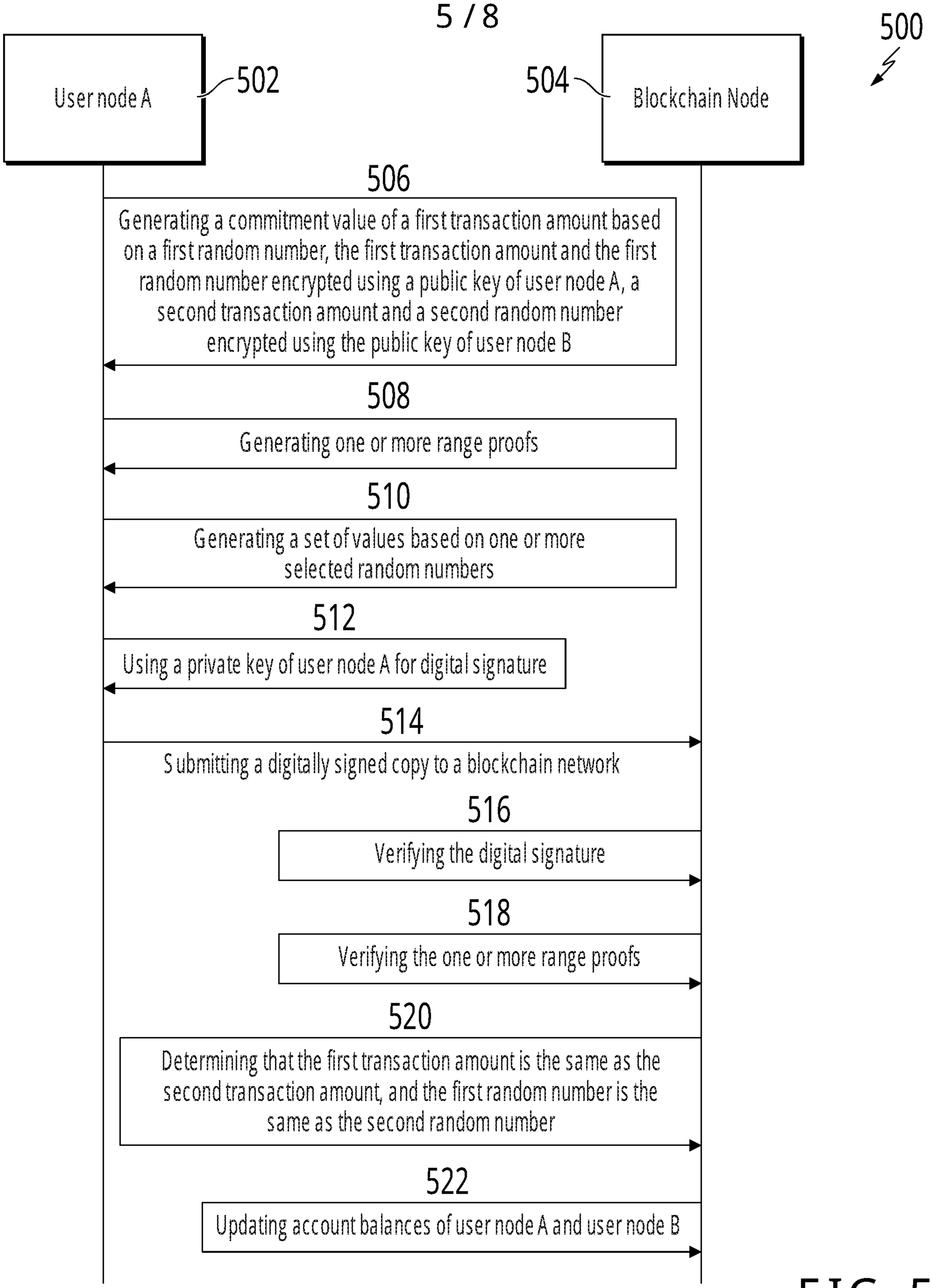

500
User node A
502
504
Blockchain Node
506
Generating a commitment value of a first transaction amount based on a first random number, the first transaction amount and the first random number encrypted using a public key of user node A, a second transaction amount and a second random number encrypted using the public key of user node B
508
Generating one or more range proofs
510
Generating a set of values based on one or more selected random numbers
512
Using a private key of user node A for digital signature
514
Submitting a digitally signed copy to a blockchain network
516
Verifying the digital signature
518
Verifying the one or more range proofs
520
Determining that the first transaction amount is the same as the second transaction amount, and the first random number is the same as the second random number
522
Updating account balances of user node A and user node B

FIG. 5

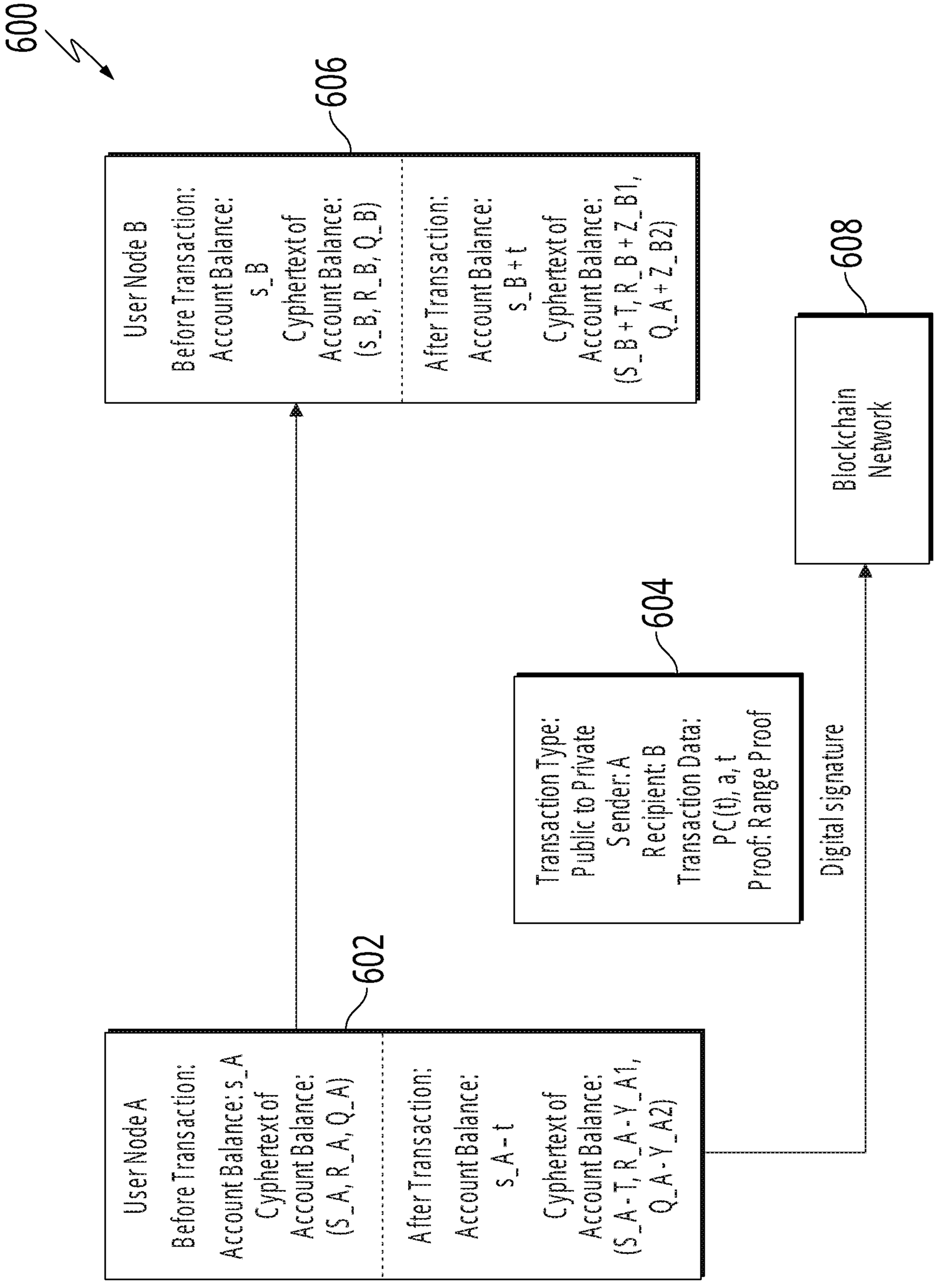

600
606
User Node B
Before Transaction:
Account Balance:
s_B
Cyphertext of
Account Balance:
(s_B, R_B, Q_B)
After Transaction:
Account Balance:
s_B + t
Cyphertext of
Account Balance:
(S_B + T, R_B + Z_B1,
Q_A + Z_B2)
608
Blockchain
Network
604
Transaction Type:
Public to Private
Sender: A
Recipient: B
Transaction Data:
PC(t), a, t
Proof: Range Proof
Digital signature
602
User Node A
Before Transaction:
Account Balance: s_A
Cyphertext of
Account Balance:
(S_A, R_A, Q_A)
After Transaction:
Account Balance:
s_A – t
Cyphertext of
Account Balance:
(S_A-T, R_A-Y_A1,
Q_A-Y_A2)

FIG. 6

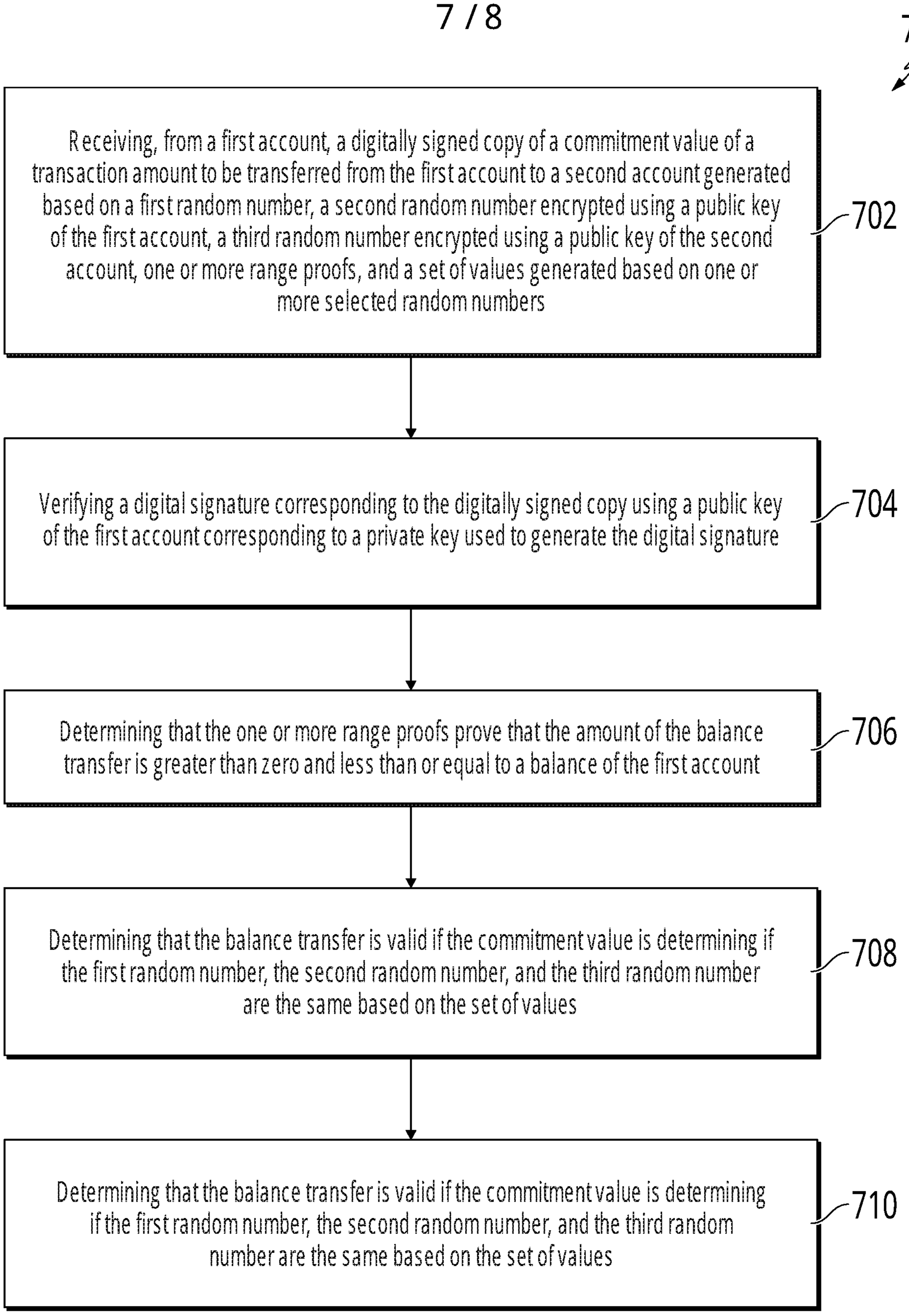

700
Receiving, from a first account, a digitally signed copy of a commitment value of a transaction amount to be transferred from the first account to a second account generated based on a first random number, a second random number encrypted using a public key of the first account, a third random number encrypted using a public key of the second account, one or more range proofs, and a set of values generated based on one or more selected random numbers
702
Verifying a digital signature corresponding to the digitally signed copy using a public key of the first account corresponding to a private key used to generate the digital signature
704
Determining that the one or more range proofs prove that the amount of the balance transfer is greater than zero and less than or equal to a balance of the first account
706
Determining that the balance transfer is valid if the commitment value is determining if the first random number, the second random number, and the third random number are the same based on the set of values
708
Determining that the balance transfer is valid if the commitment value is determining if the first random number, the second random number, and the third random number are the same based on the set of values
710

FIG. 7

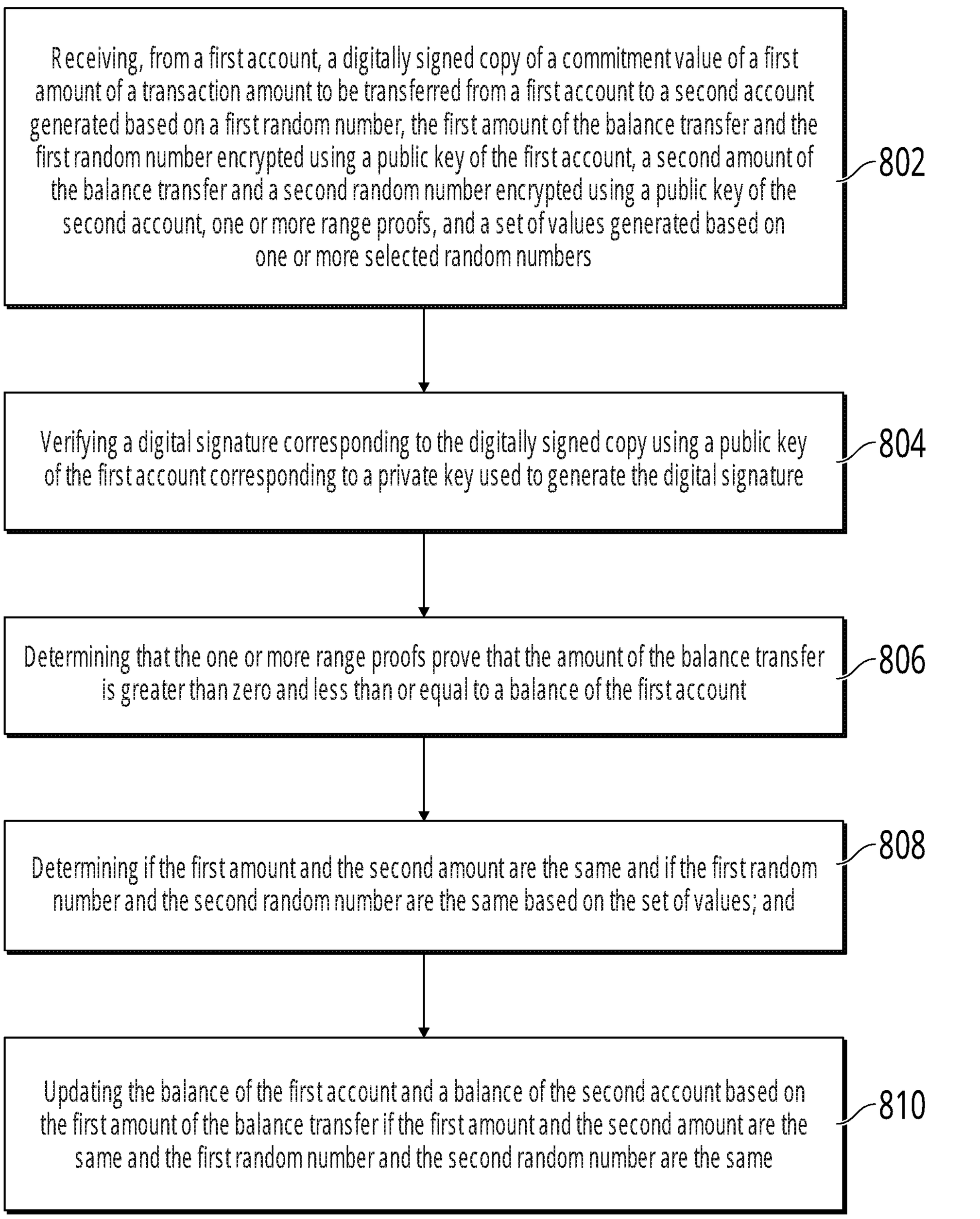

800
Receiving, from a first account, a digitally signed copy of a commitment value of a first amount of a transaction amount to be transferred from a first account to a second account generated based on a first random number, the first amount of the balance transfer and the first random number encrypted using a public key of the first account, a second amount of the balance transfer and a second random number encrypted using a public key of the second account, one or more range proofs, and a set of values generated based on one or more selected random numbers
802
Verifying a digital signature corresponding to the digitally signed copy using a public key of the first account corresponding to a private key used to generate the digital signature
804
Determining that the one or more range proofs prove that the amount of the balance transfer is greater than zero and less than or equal to a balance of the first account
806
Determining if the first amount and the second amount are the same and if the first random number and the second random number are the same based on the set of values; and
808
Updating the balance of the first account and a balance of the second account based on the first amount of the balance transfer if the first amount and the second amount are the same and the first random number and the second random number are the same
810

FIG. 8