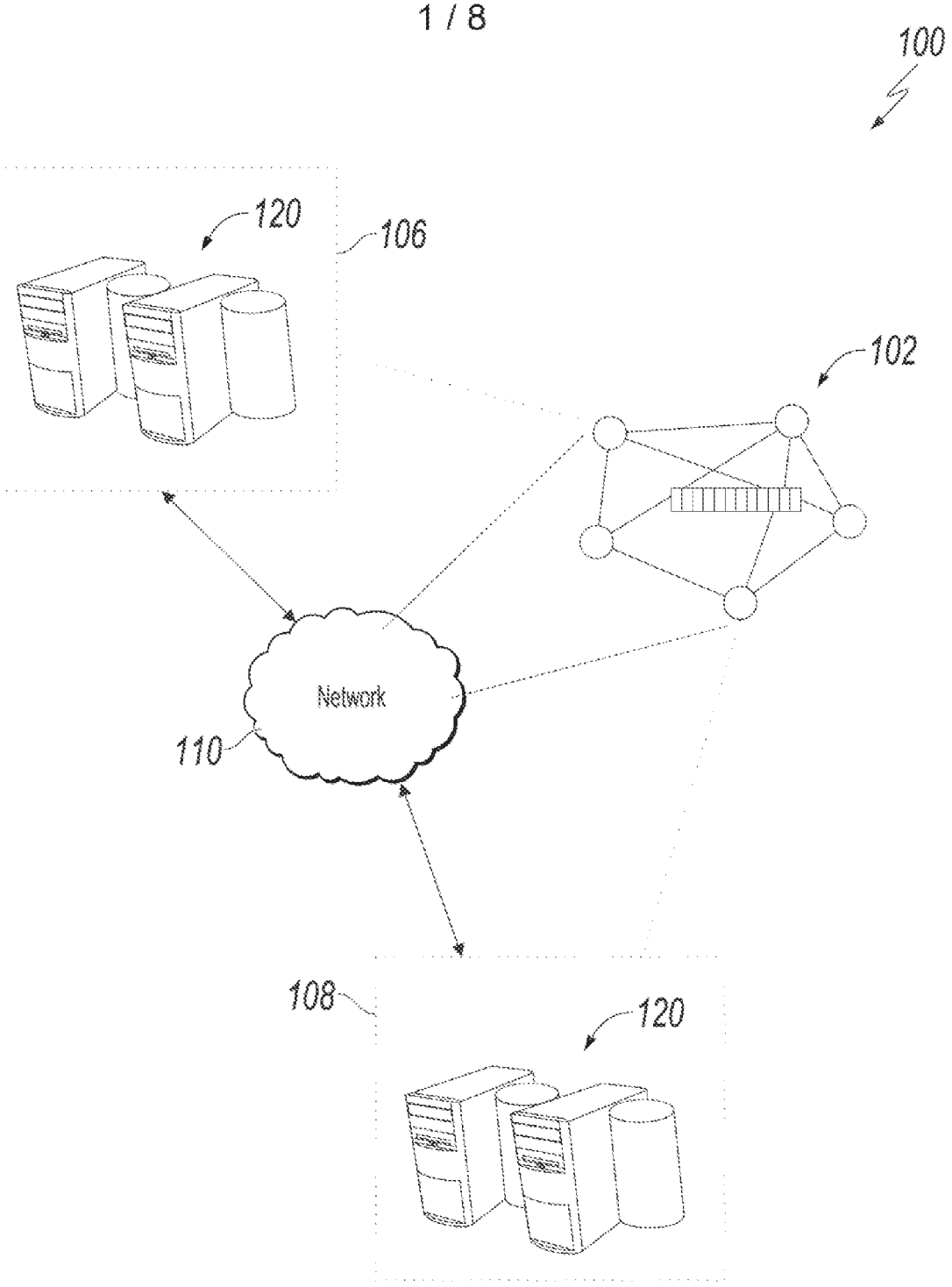


FIG. 1

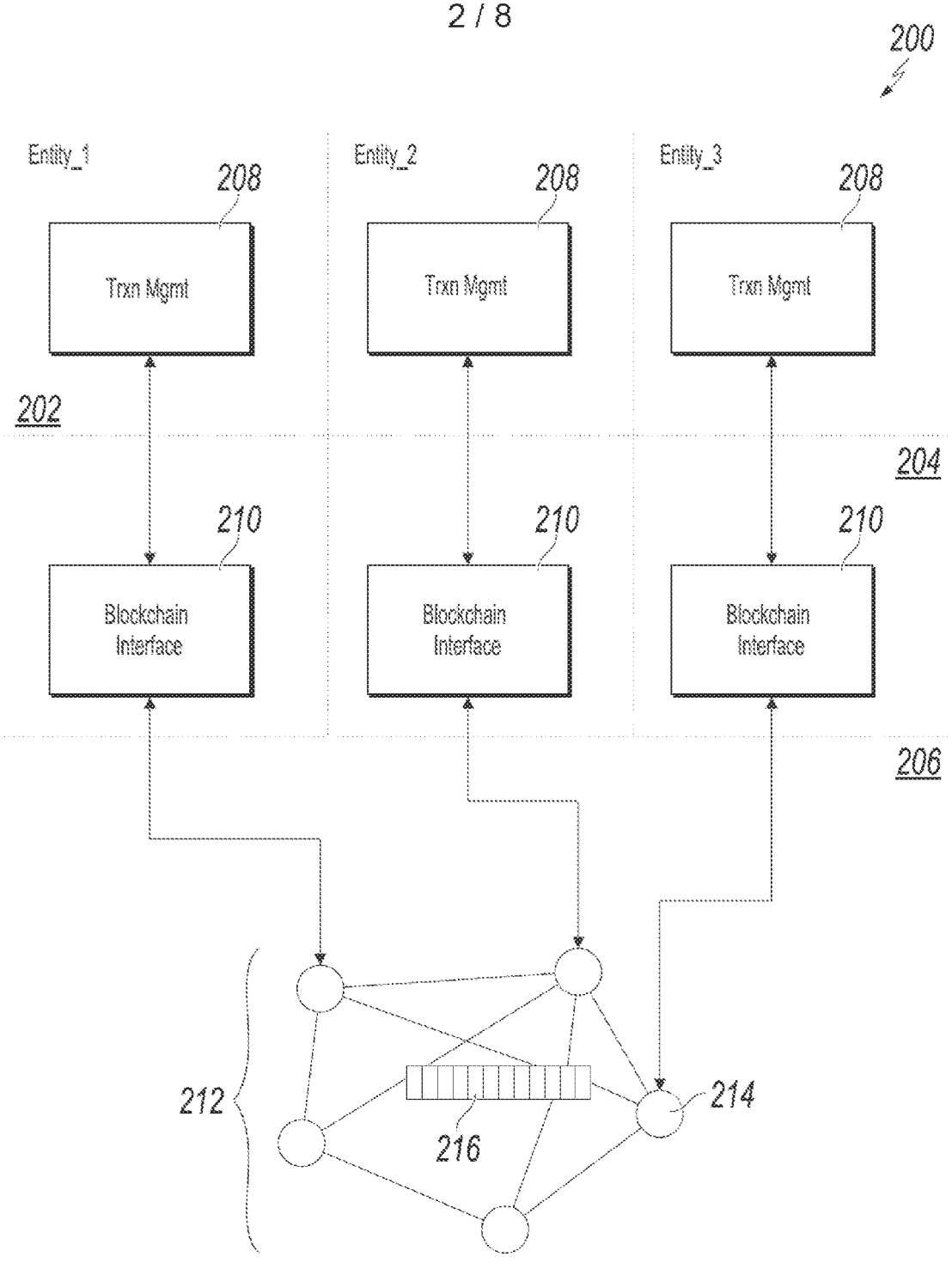

200
Entity_1
Entity_2
Entity_3
208
208
208
Trxn Mgmt
Trxn Mgmt
Trxn Mgmt
202
204
210
210
210
Blockchain Interface
Blockchain Interface
Blockchain Interface
206
212
214
216

FIG. 2

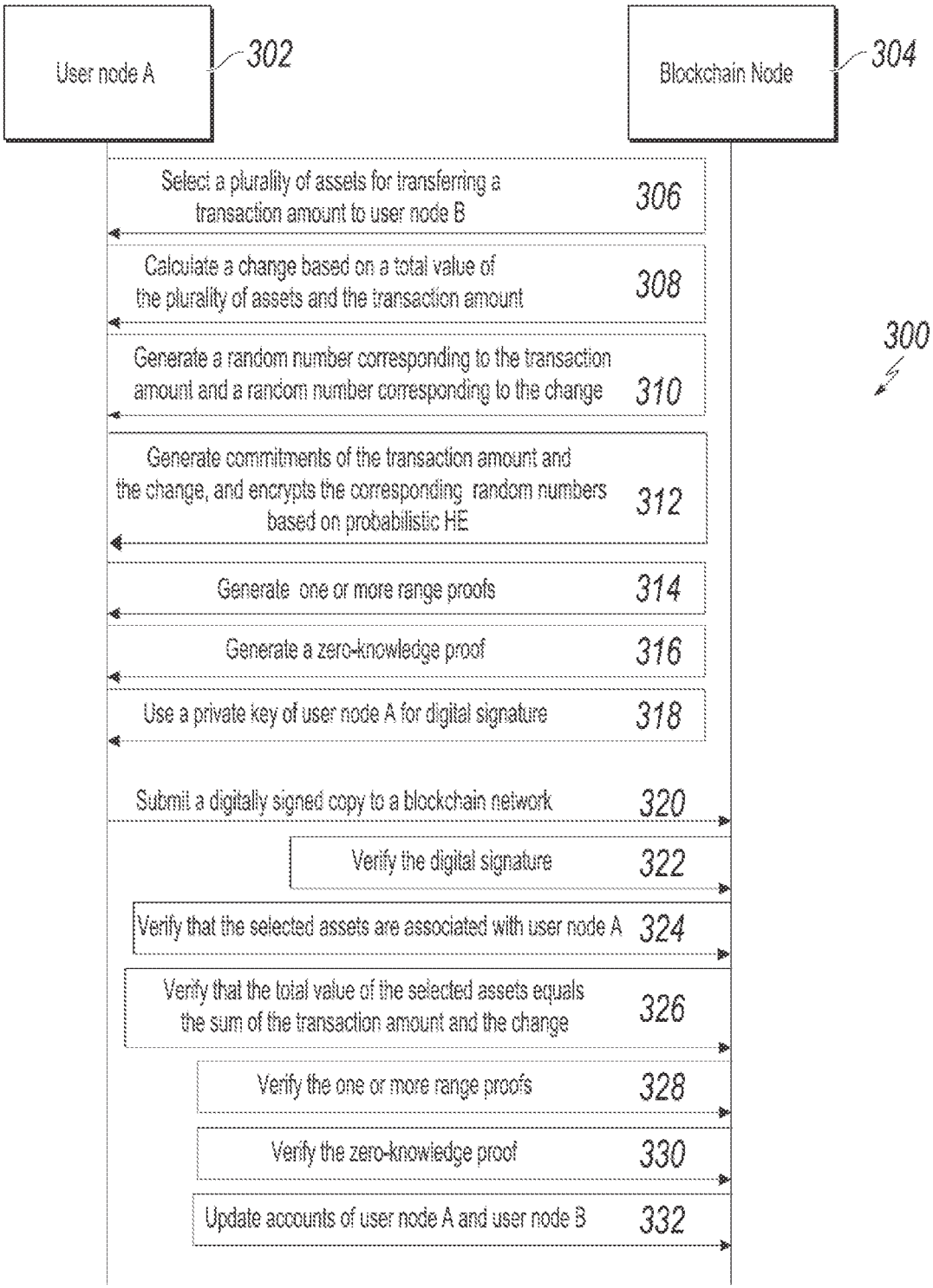

User node A
302
Blockchain Node
304
300
Select a plurality of assets for transferring a transaction amount to user node B
306
Calculate a change based on a total value of the plurality of assets and the transaction amount
308
Generate a random number corresponding to the transaction amount and a random number corresponding to the change
310
Generate commitments of the transaction amount and the change, and encrypts the corresponding random numbers based on probabilistic HE
312
Generate one or more range proofs
314
Generate a zero-knowledge proof
316
Use a private key of user node A for digital signature
318
Submit a digitally signed copy to a blockchain network
320
Verify the digital signature
322
Verify that the selected assets are associated with user node A
324
Verify that the total value of the selected assets equals the sum of the transaction amount and the change
326
Verify the one or more range proofs
328
Verify the zero-knowledge proof
330
Update accounts of user node A and user node B
332

FIG. 3

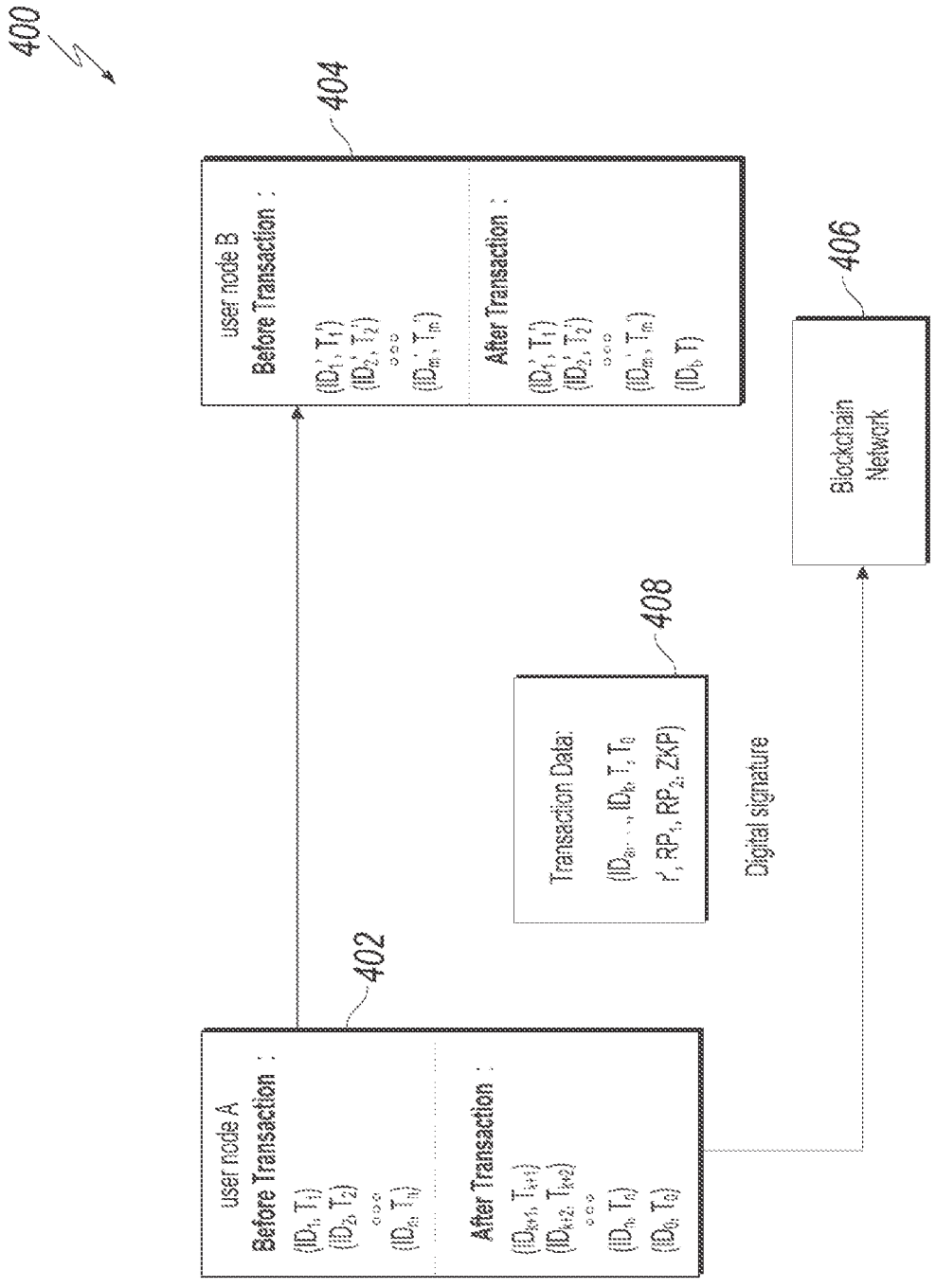

400
404
user node B
Before Transaction :
(ID1, T1)
(ID2, T2)
(IDm, Tm)
After Transaction :
(ID1', T1)
(ID2', T2)
(IDm', Tm)
(IDb, T)
406
Blockchain Network
408
Transaction Data:
(IDa, ..., IDk, T, T0
r, RP1, RP2, ZKP)
Digital signature
402
user node A
Before Transaction :
(IDa, T1)
(IDb, T2)
(IDa, Tn)
After Transaction :
(IDk+1, Tk+1)
(IDk+2, Tk+2)
(IDb, T0)
(IDb, T0)

FIG. 4

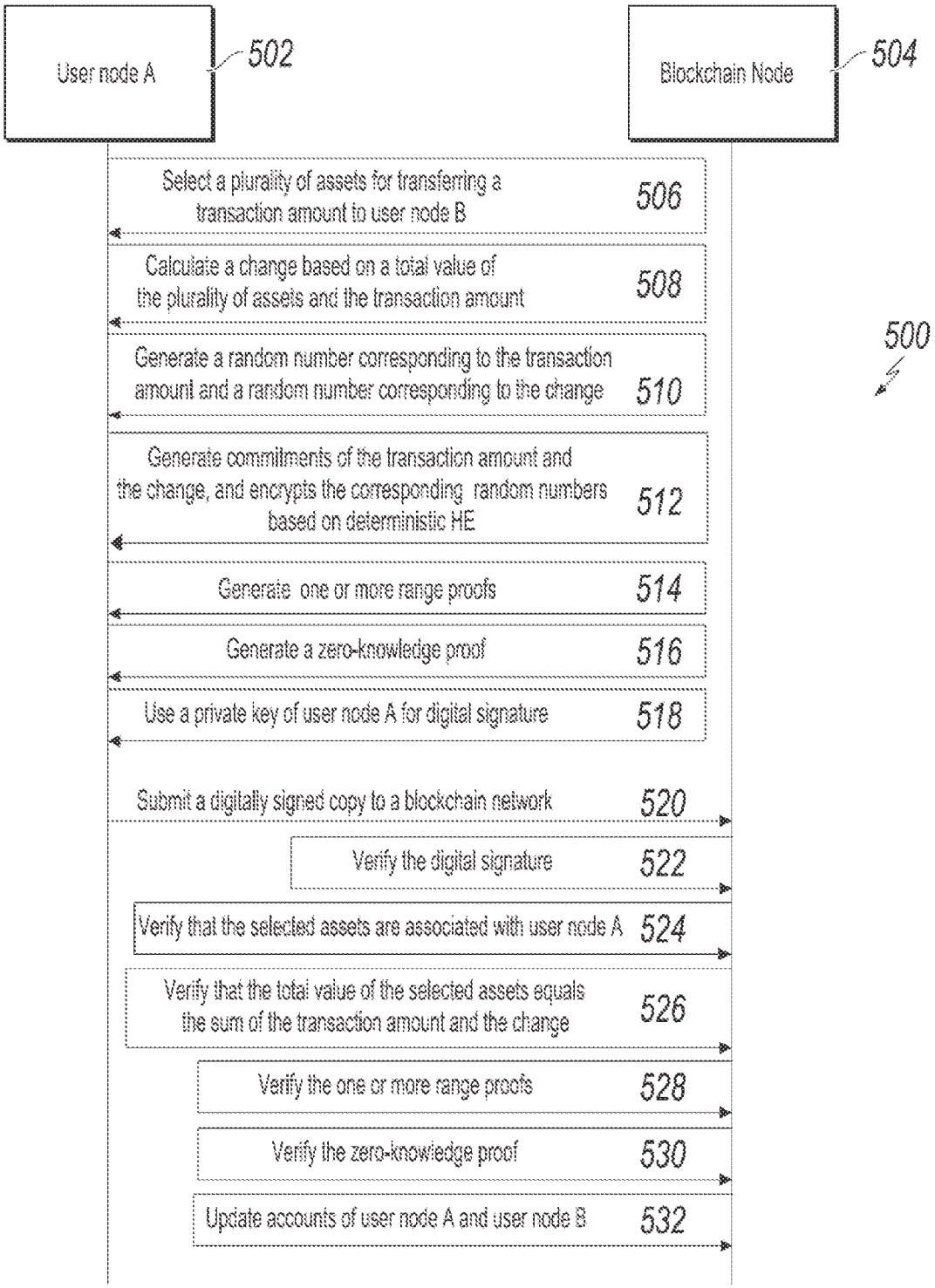

User node A
502
Blockchain Node
504
500
Select a plurality of assets for transferring a transaction amount to user node B
506
Calculate a change based on a total value of the plurality of assets and the transaction amount
508
Generate a random number corresponding to the transaction amount and a random number corresponding to the change
510
Generate commitments of the transaction amount and the change, and encrypts the corresponding random numbers based on deterministic HE
512
Generate one or more range proofs
514
Generate a zero-knowledge proof
516
Use a private key of user node A for digital signature
518
Submit a digitally signed copy to a blockchain network
520
Verify the digital signature
522
Verify that the selected assets are associated with user node A
524
Verify that the total value of the selected assets equals the sum of the transaction amount and the change
526
Verify the one or more range proofs
528
Verify the zero-knowledge proof
530
Update accounts of user node A and user node B
532

FIG. 5

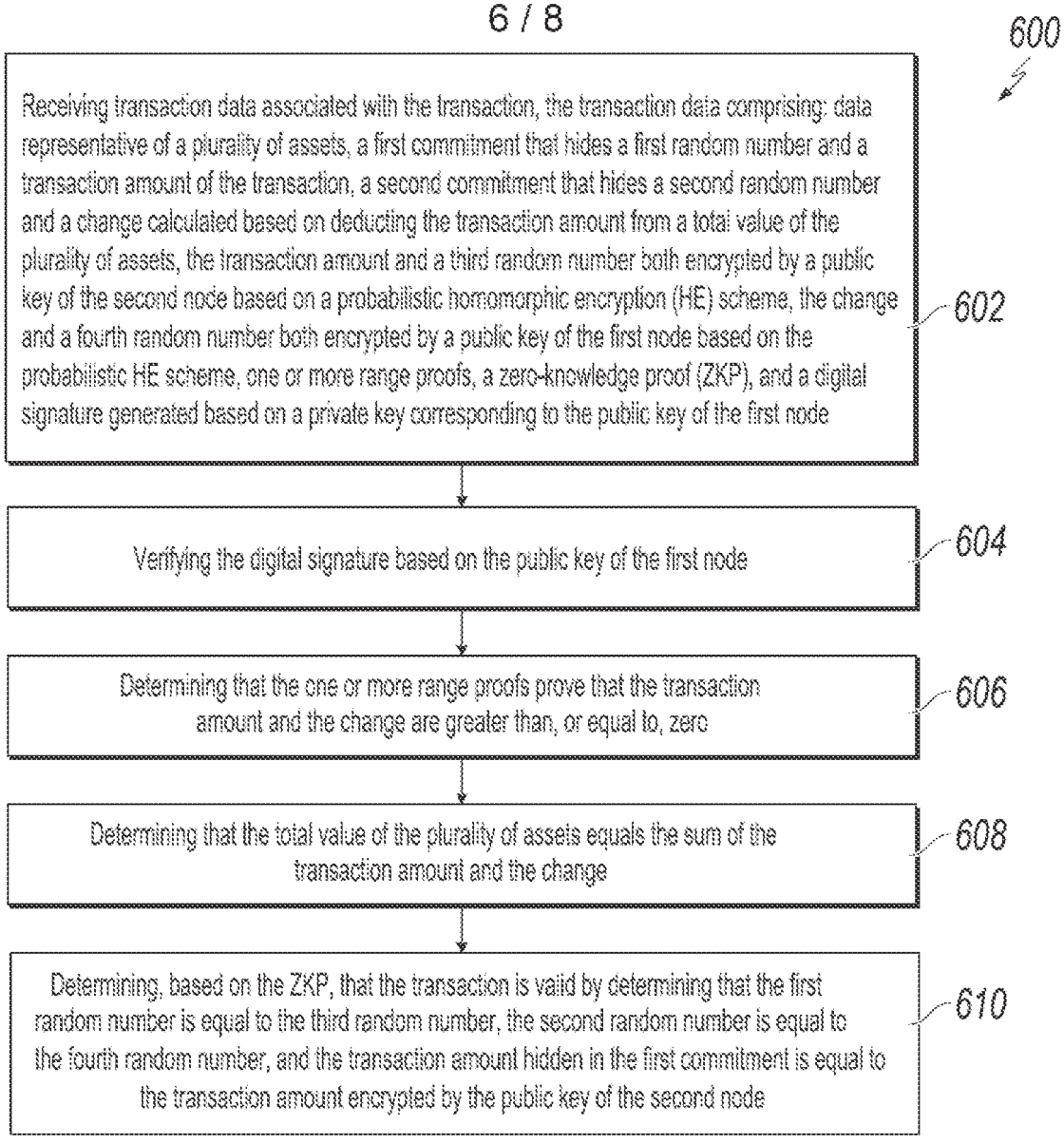

600
Receiving transaction data associated with the transaction, the transaction data comprising: data representative of a plurality of assets, a first commitment that hides a first random number and a transaction amount of the transaction, a second commitment that hides a second random number and a change calculated based on deducting the transaction amount from a total value of the plurality of assets, the transaction amount and a third random number both encrypted by a public key of the second node based on a probabilistic homomorphic encryption (HE) scheme, the change and a fourth random number both encrypted by a public key of the first node based on the probabilistic HE scheme, one or more range proofs, a zero-knowledge proof (ZKP), and a digital signature generated based on a private key corresponding to the public key of the first node
602
Verifying the digital signature based on the public key of the first node
604
Determining that the one or more range proofs prove that the transaction amount and the change are greater than, or equal to, zero
606
Determining that the total value of the plurality of assets equals the sum of the transaction amount and the change
608
Determining, based on the ZKP, that the transaction is valid by determining that the first random number is equal to the third random number, the second random number is equal to the fourth random number, and the transaction amount hidden in the first commitment is equal to the transaction amount encrypted by the public key of the second node
610

FIG. 6

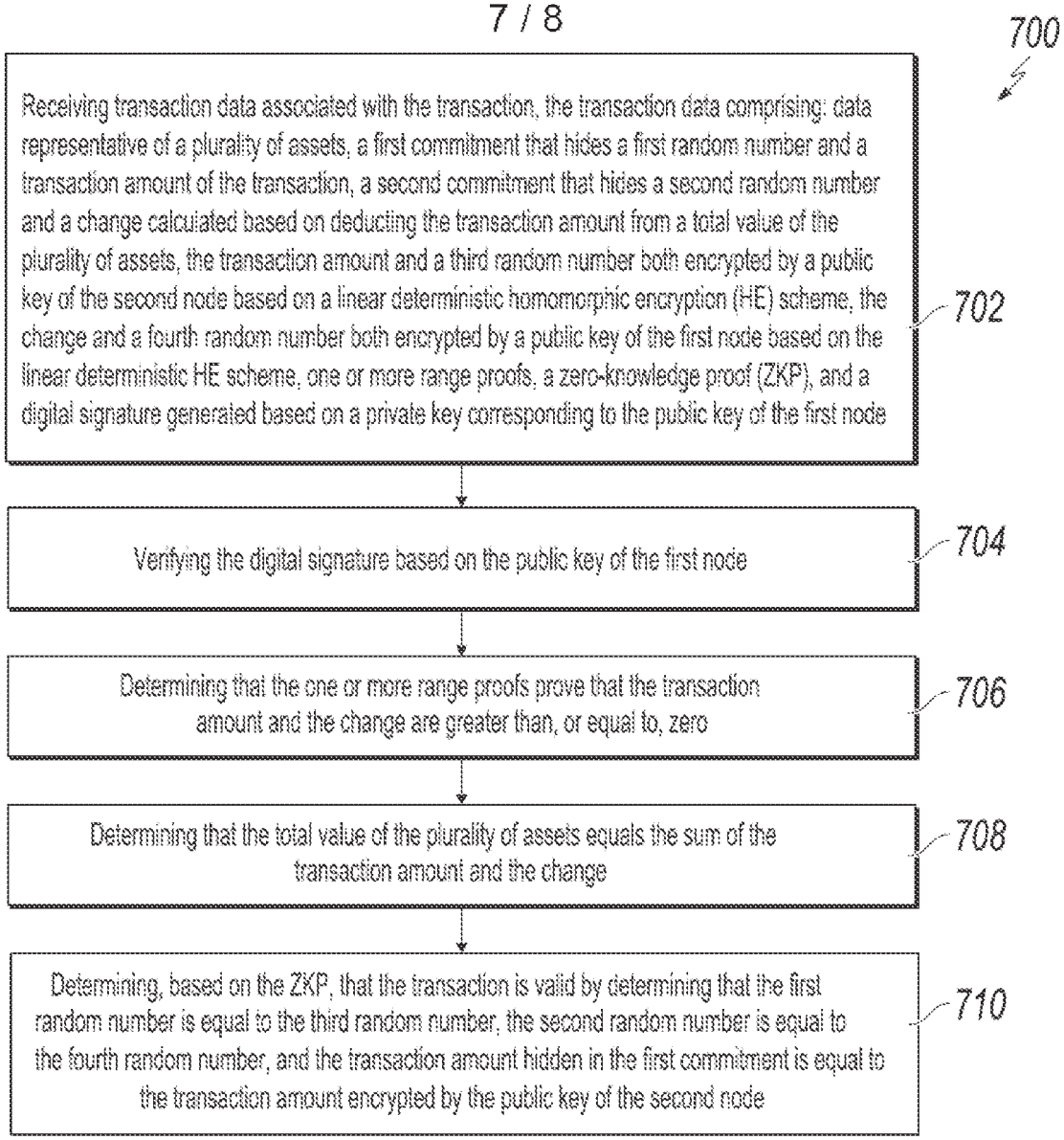

700
Receiving transaction data associated with the transaction, the transaction data comprising: data representative of a plurality of assets, a first commitment that hides a first random number and a transaction amount of the transaction, a second commitment that hides a second random number and a change calculated based on deducting the transaction amount from a total value of the plurality of assets, the transaction amount and a third random number both encrypted by a public key of the second node based on a linear deterministic homomorphic encryption (HE) scheme, the change and a fourth random number both encrypted by a public key of the first node based on the linear deterministic HE scheme, one or more range proofs, a zero-knowledge proof (ZKP), and a digital signature generated based on a private key corresponding to the public key of the first node
702
Verifying the digital signature based on the public key of the first node
704
Determining that the one or more range proofs prove that the transaction amount and the change are greater than, or equal to, zero
706
Determining that the total value of the plurality of assets equals the sum of the transaction amount and the change
708
Determining, based on the ZKP, that the transaction is valid by determining that the first random number is equal to the third random number, the second random number is equal to the fourth random number, and the transaction amount hidden in the first commitment is equal to the transaction amount encrypted by the public key of the second node
710

FIG. 7

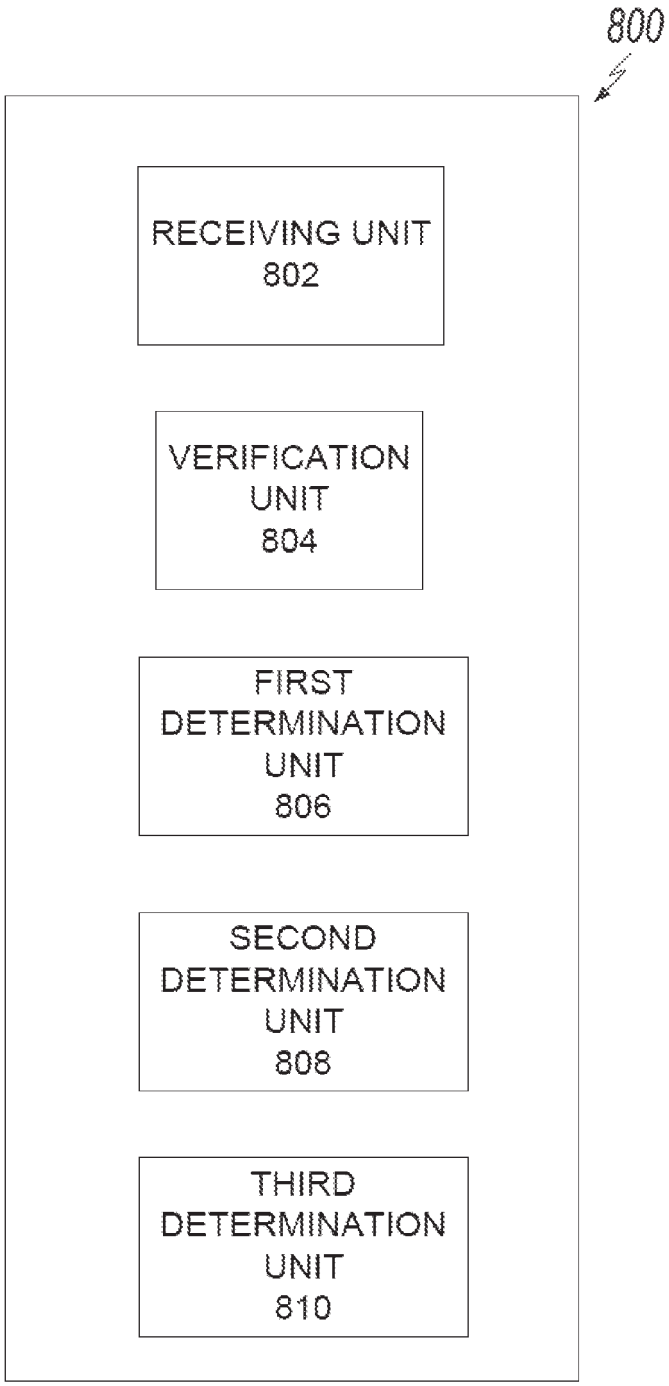

800
RECEIVING UNIT
802
VERIFICATION
UNIT
804
FIRST
DETERMINATION
UNIT
806
SECOND
DETERMINATION
UNIT
808
THIRD
DETERMINATION
UNIT
810

FIG. 8