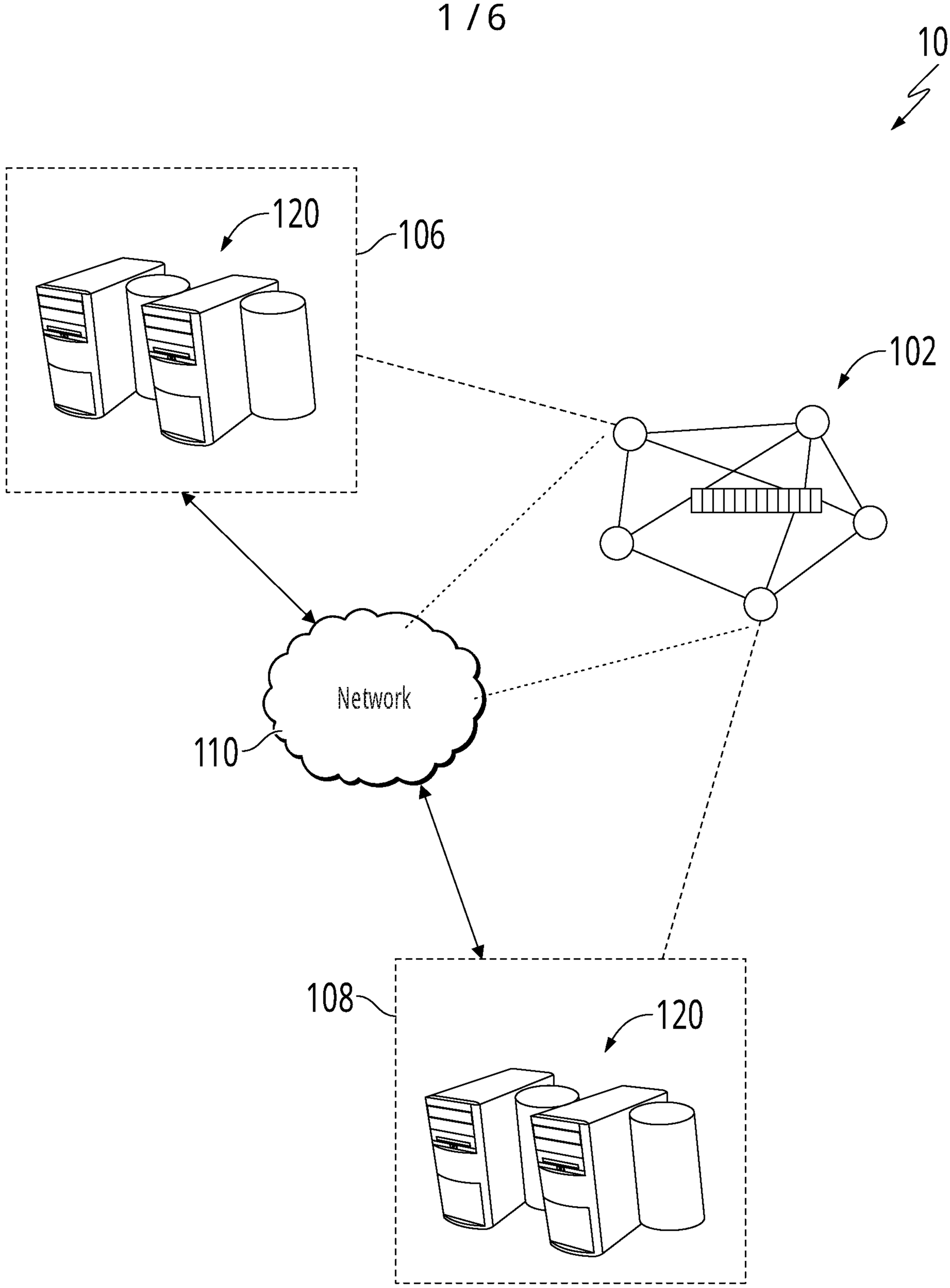

FIG. 1

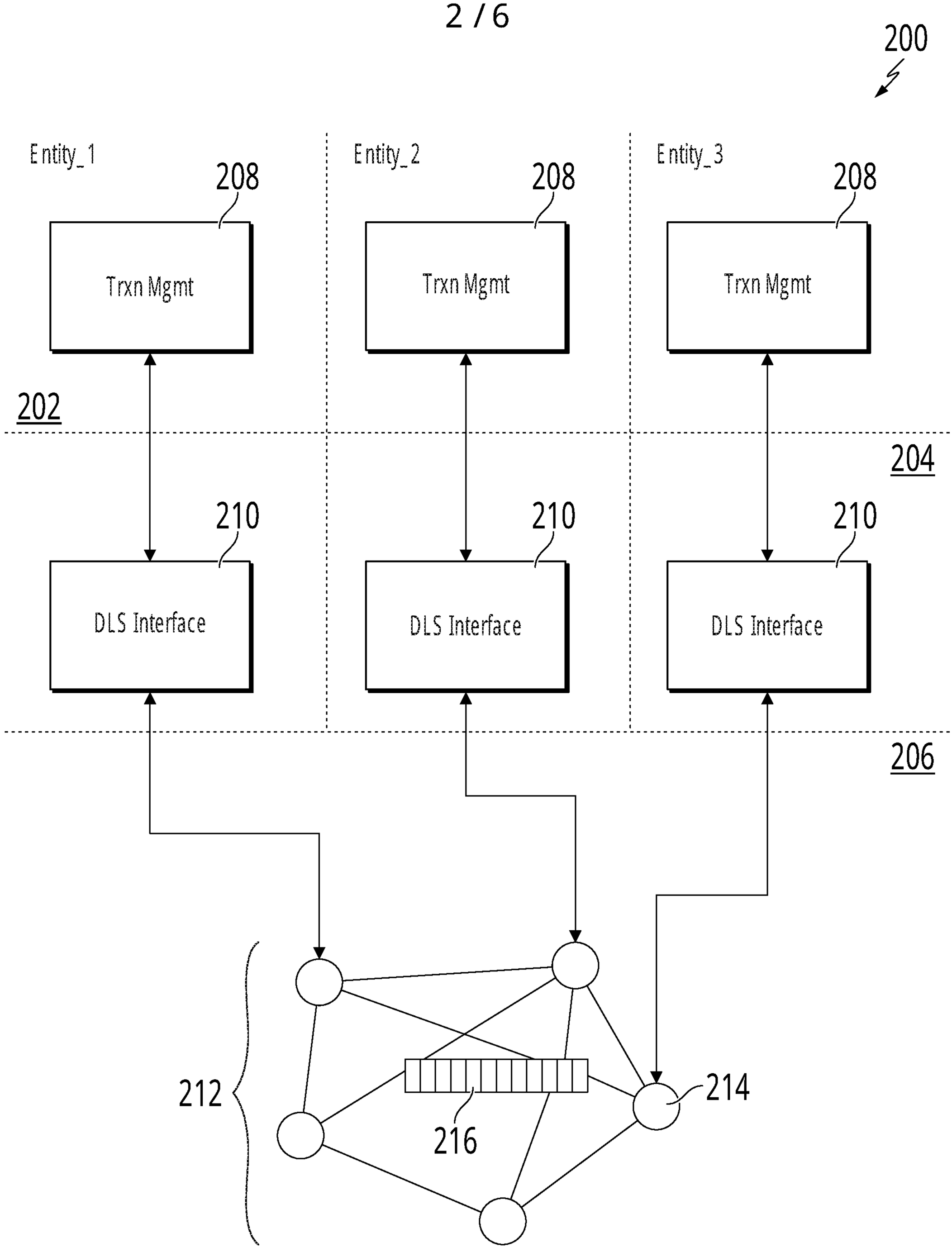
200
Entity_1
Entity_2
Entity_3
208
208
208
Trxn Mgmt
Trxn Mgmt
Trxn Mgmt
202
204
210
210
210
DLS Interface
DLS Interface
DLS Interface
206
212
214
216

FIG. 2

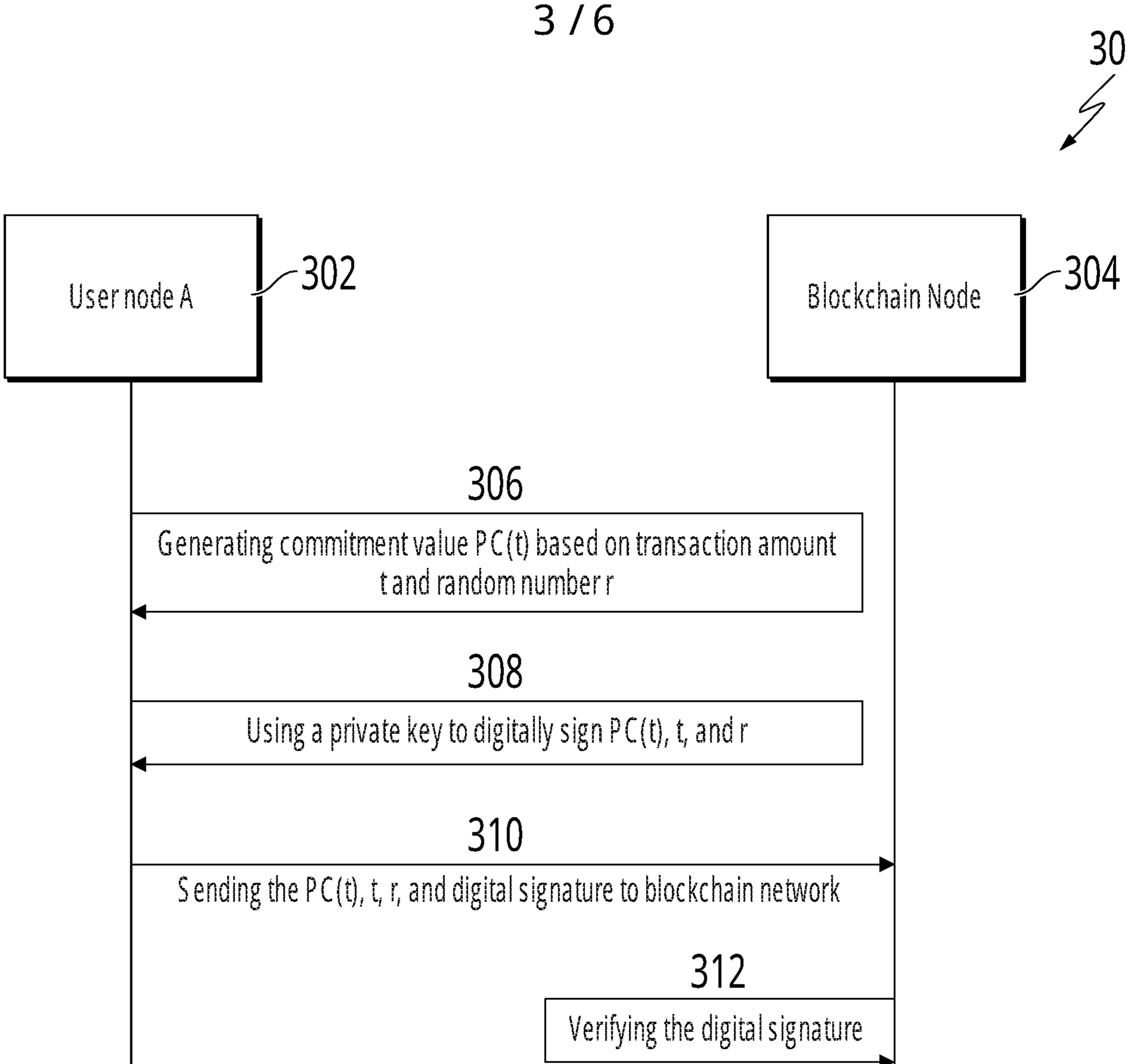
300
User node A
302
Blockchain Node
304
306
Generating commitment value PC(t) based on transaction amount t and random number r
308
Using a private key to digitally sign PC(t), t, and r
310
Sending the PC(t), t, r, and digital signature to blockchain network
312
Verifying the digital signature
314
Determining that PC(t) is correct
316
Update balances of user node A and user node B

FIG. 3

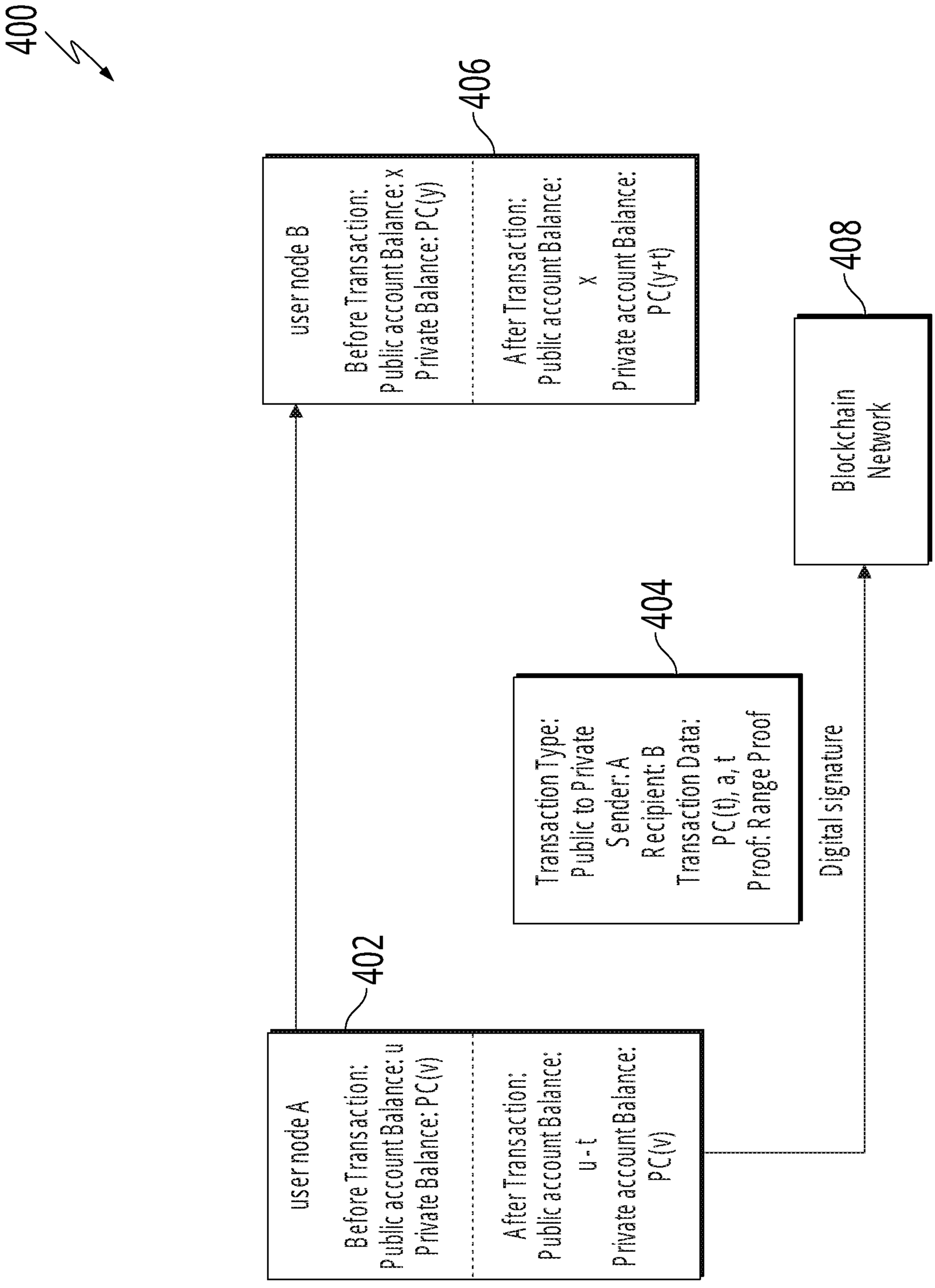
400
406
user node B
Before Transaction:
Public account Balance: x
Private Balance: PC(y)
After Transaction:
Public account Balance:
x
Private account Balance:
PC(y+t)
408
Blockchain
Network
404
Transaction Type:
Public to Private
Sender: A
Recipient: B
Transaction Data:
PC(t), a, t
Proof: Range Proof
Digital signature
402
user node A
Before Transaction:
Public account Balance: u
Private Balance: PC(v)
After Transaction:
Public account Balance:
u - t
Private account Balance:
PC(v)

FIG. 4

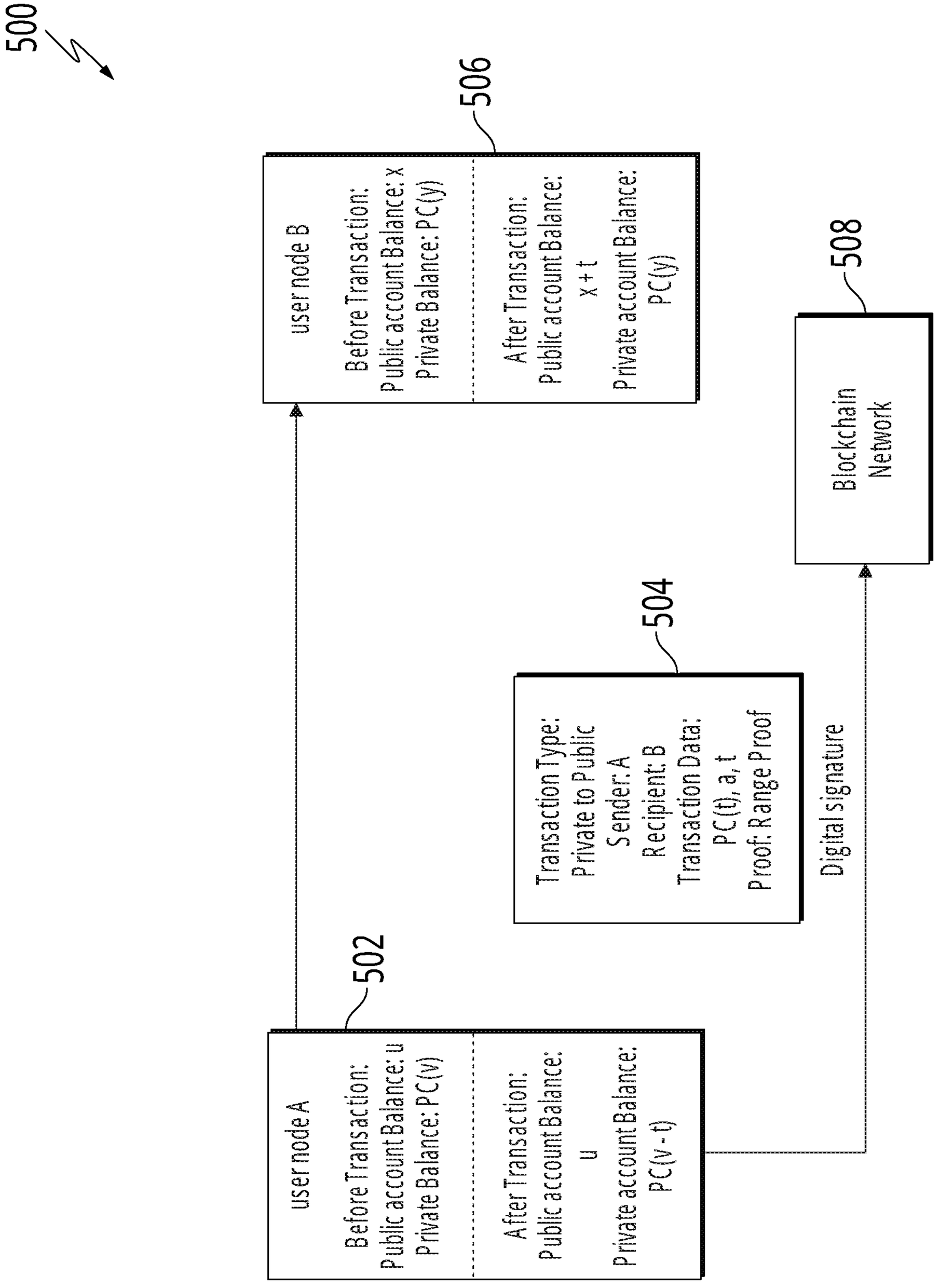
500
506
user node B
Before Transaction:
Public account Balance: x
Private Balance: PC(y)
After Transaction:
Public account Balance:
x + t
Private account Balance:
PC(y)
508
Blockchain
Network
504
Transaction Type:
Private to Public
Sender: A
Recipient: B
Transaction Data:
PC(t), a, t
Proof: Range Proof
Digital signature
502
user node A
Before Transaction:
Public account Balance: u
Private Balance: PC(v)
After Transaction:
Public account Balance:
u
Private account Balance:
PC(v - t)

FIG. 5

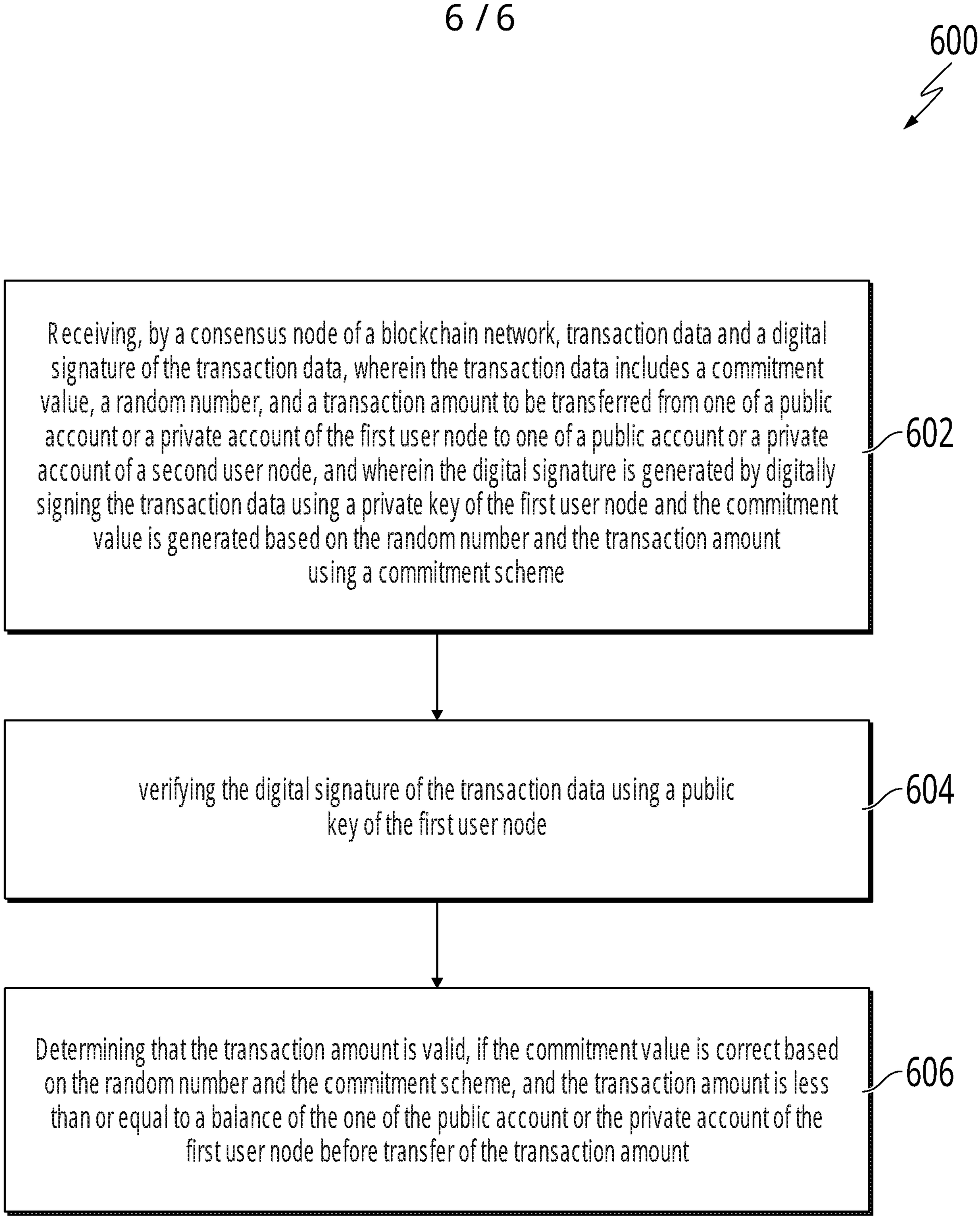
600
Receiving, by a consensus node of a blockchain network, transaction data and a digital signature of the transaction data, wherein the transaction data includes a commitment value, a random number, and a transaction amount to be transferred from one of a public account or a private account of the first user node to one of a public account or a private account of a second user node, and wherein the digital signature is generated by digitally signing the transaction data using a private key of the first user node and the commitment value is generated based on the random number and the transaction amount using a commitment scheme
602
verifying the digital signature of the transaction data using a public key of the first user node
604
Determining that the transaction amount is valid, if the commitment value is correct based on the random number and the commitment scheme, and the transaction amount is less than or equal to a balance of the one of the public account or the private account of the first user node before transfer of the transaction amount
606

FIG. 6