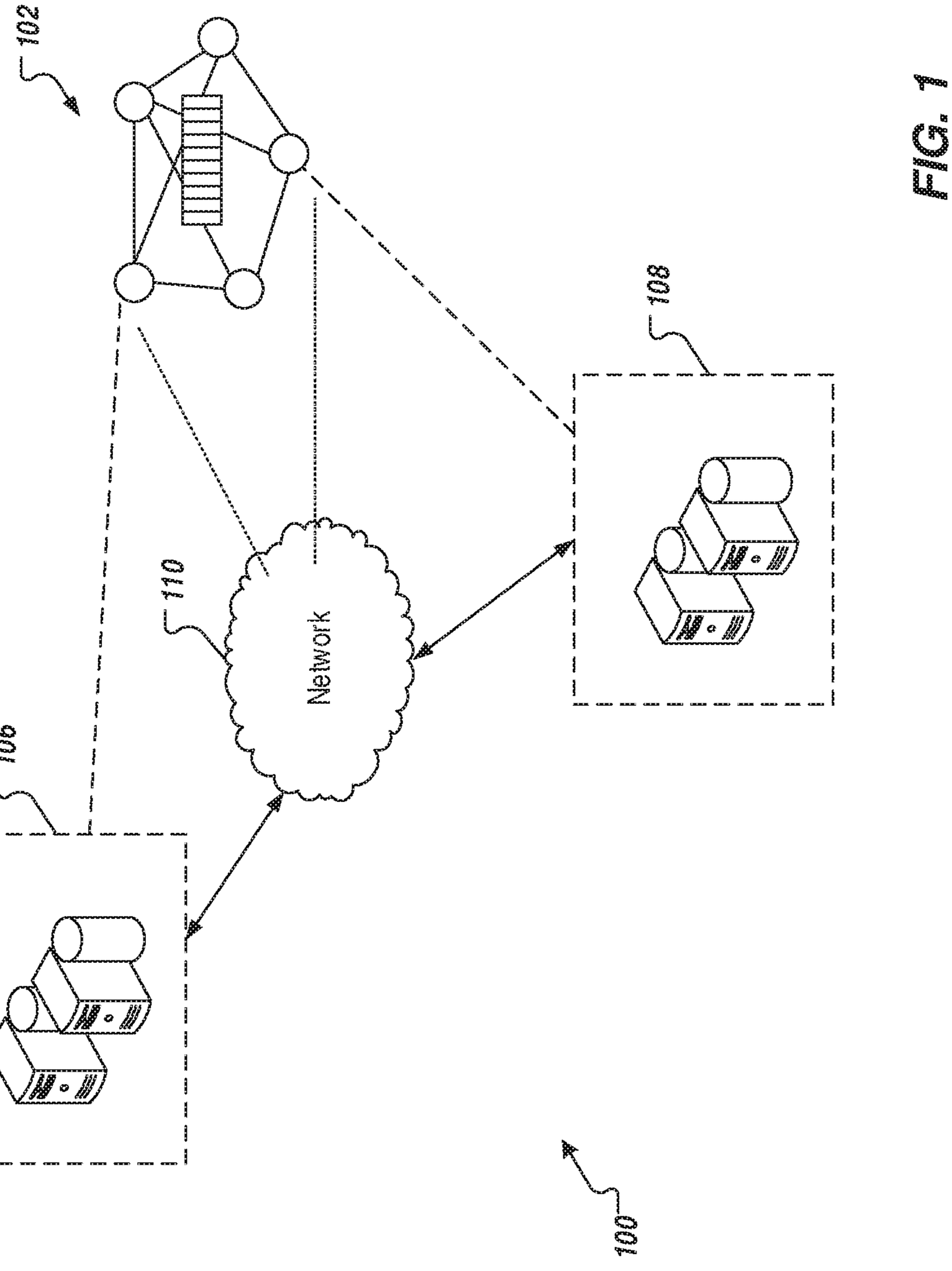


FIG. 1

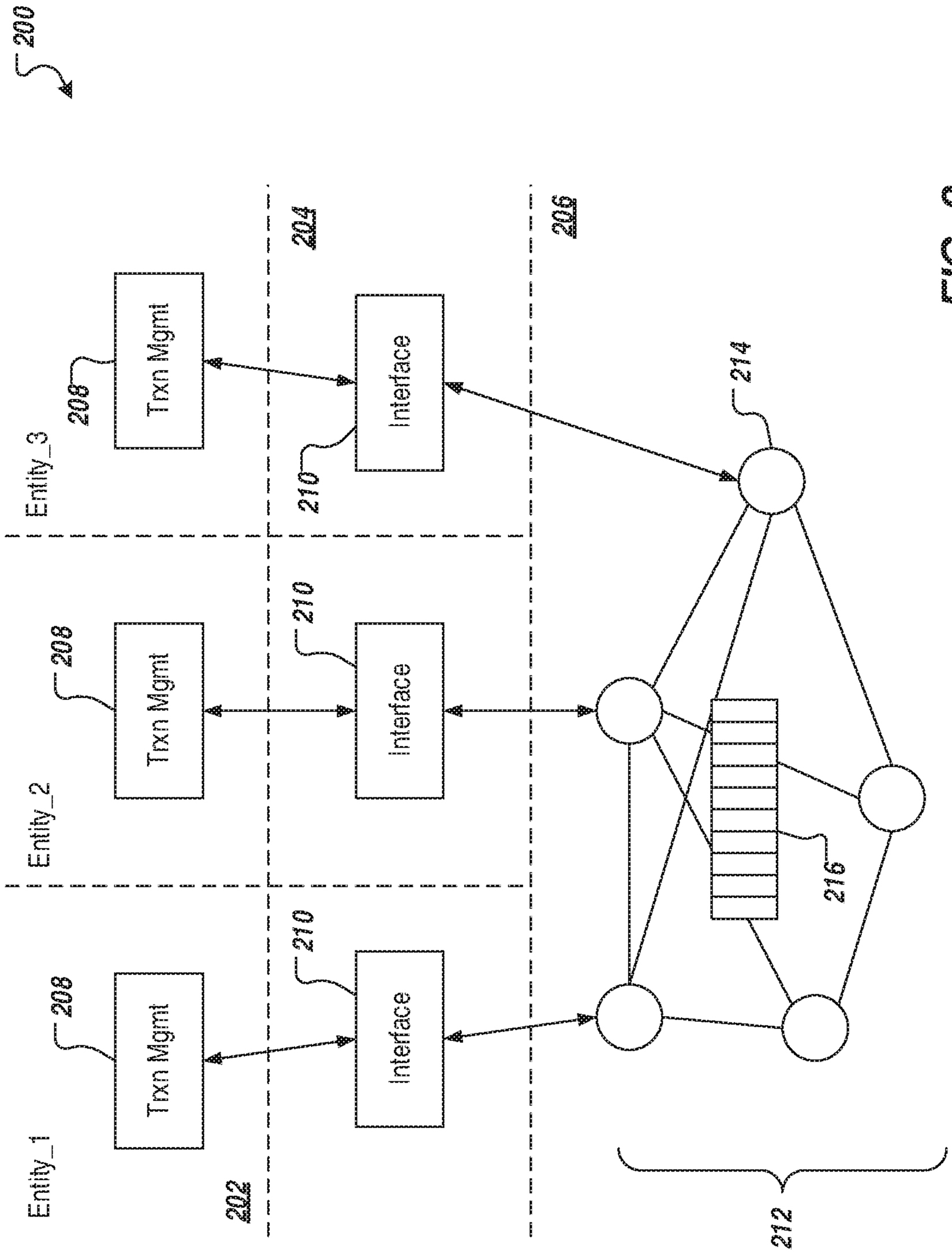

200
Entity_3
208
Trxn Mgmt
204
206
210
Interface
214
Entity_2
208
Trxn Mgmt
210
Interface
216
Entity_1
208
Trxn Mgmt
210
Interface
202
212

FIG. 2

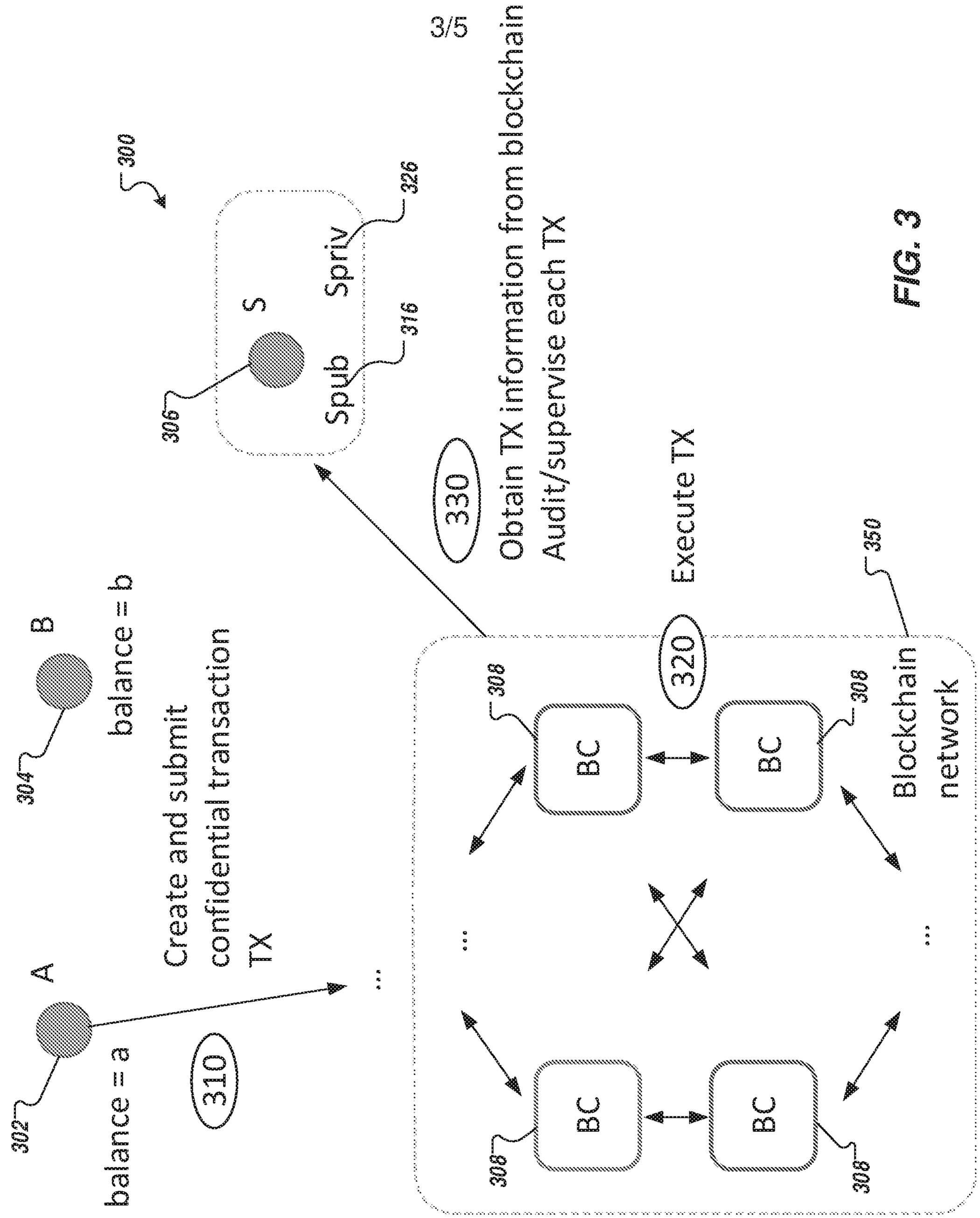
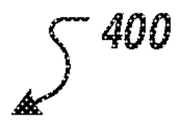
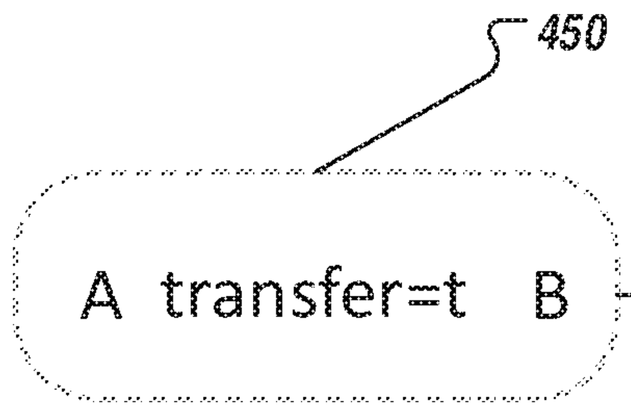

A
B
304
balance = b
Create and submit
confidential transaction
TX
...
302
balance = a
310
300
S
306
Spub
Spriv
316
326
330
Obtain TX information from blockchain
Audit/supervise each TX
Execute TX
350
320
BC
308
Blockchain
network

FIG. 3



TX： A transfer t to B



TX Content：
Pederson Commitment of account balance a : PC(a)
Pederson Commitment of transaction amount t: PC(t)
Pederson Commitment of remaining balance a-t: PC(a-t)
Zero-knowledge Proof （a -t > 0）
Zero-knowledge Proof （ t > 0）
Encrypted regulatory information:
M = encrypt(Spub, （ra | a | rt | t）)
Other transaction data： e.g., ditigal signature of A

FIG. 4

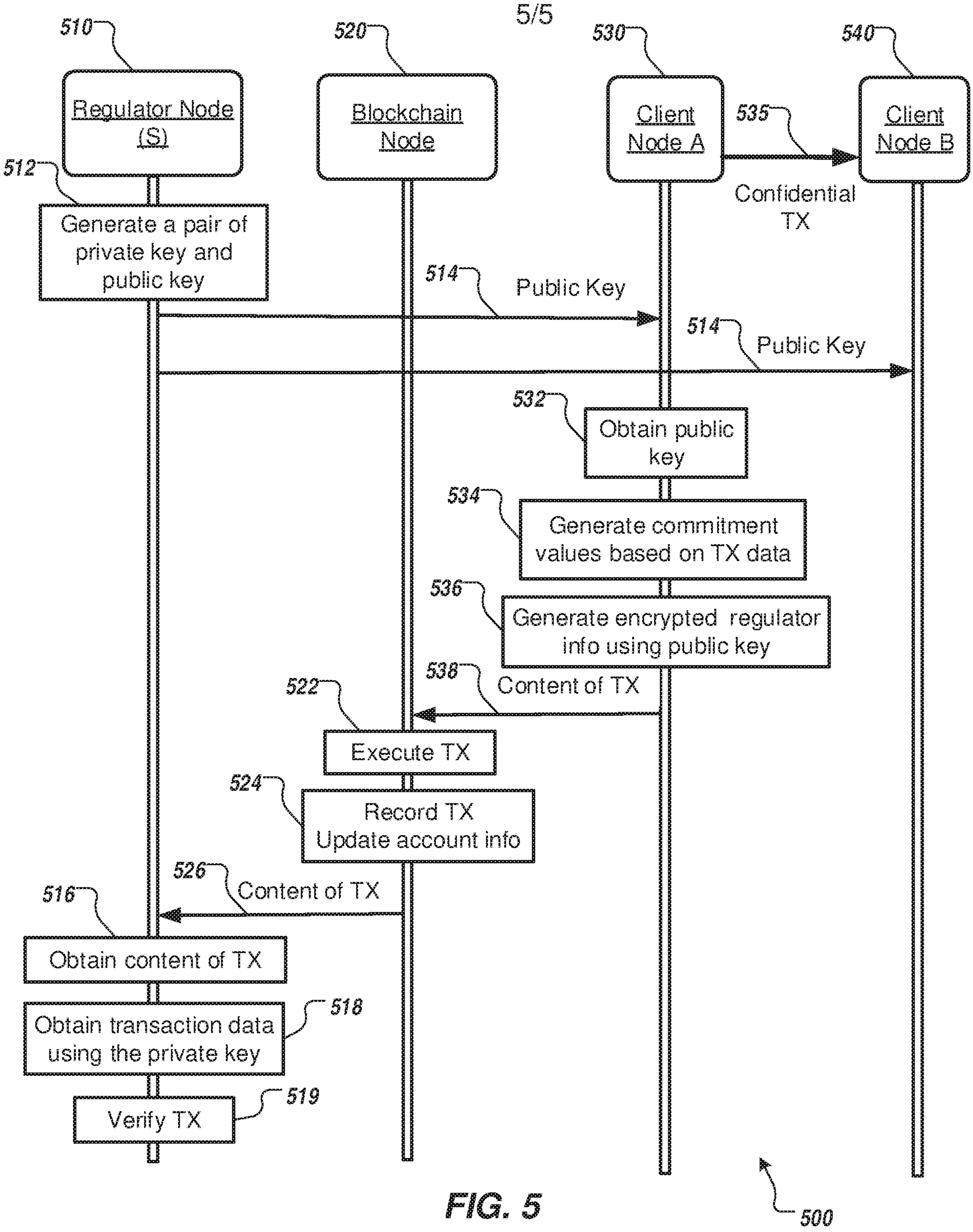

510
Regulator Node (S)
512
Generate a pair of private key and public key
520
Blockchain Node
530
Client Node A
535
Confidential TX
540
Client Node B
514
Public Key
514
Public Key
532
Obtain public key
534
Generate commitment values based on TX data
536
Generate encrypted regulator info using public key
538
Content of TX
522
Execute TX
524
Record TX
Update account info
526
Content of TX
516
Obtain content of TX
Obtain transaction data using the private key
518
Verify TX
519
500

FIG. 5