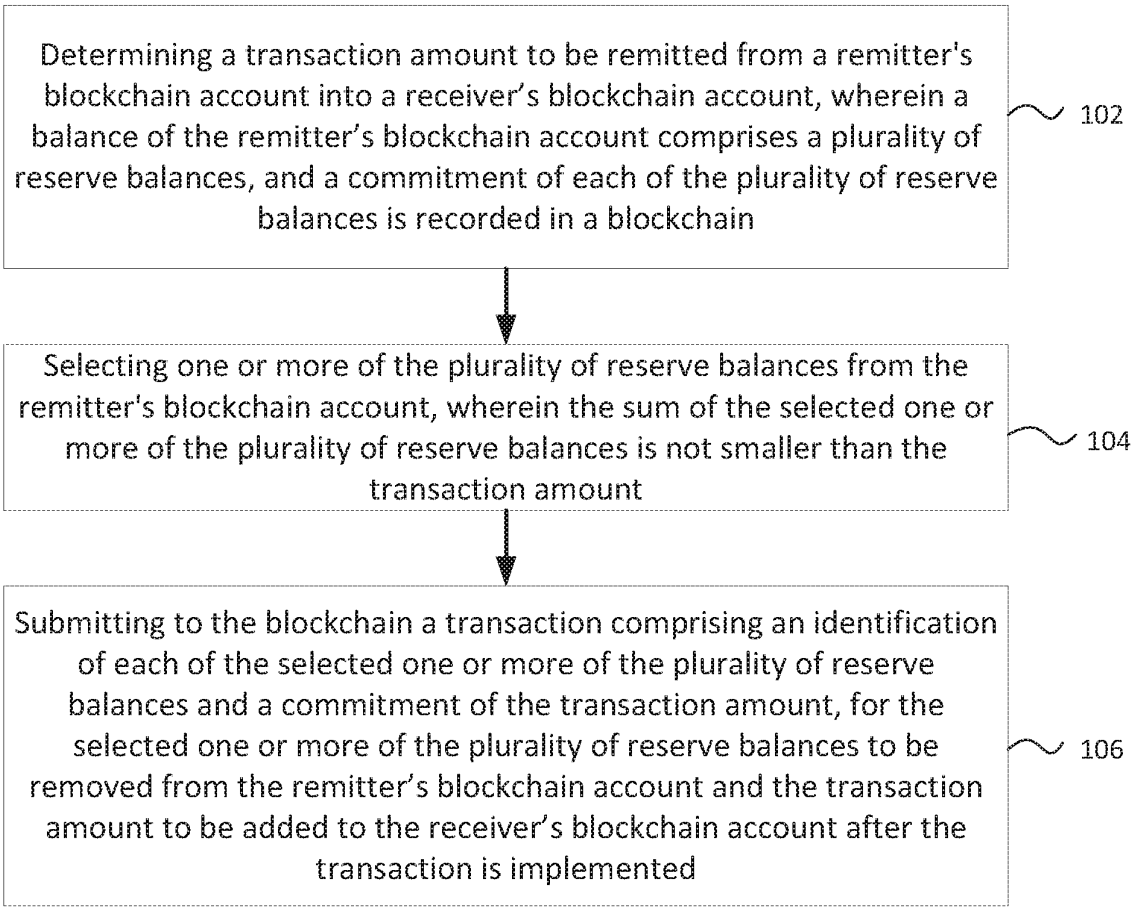
Determining a transaction amount to be remitted from a remitter's blockchain account into a receiver's blockchain account, wherein a balance of the remitter's blockchain account comprises a plurality of reserve balances, and a commitment of each of the plurality of reserve balances is recorded in a blockchain
102
Selecting one or more of the plurality of reserve balances from the remitter's blockchain account, wherein the sum of the selected one or more of the plurality of reserve balances is not smaller than the transaction amount
104
Submitting to the blockchain a transaction comprising an identification of each of the selected one or more of the plurality of reserve balances and a commitment of the transaction amount, for the selected one or more of the plurality of reserve balances to be removed from the remitter's blockchain account and the transaction amount to be added to the receiver's blockchain account after the transaction is implemented
106

FIG. 1

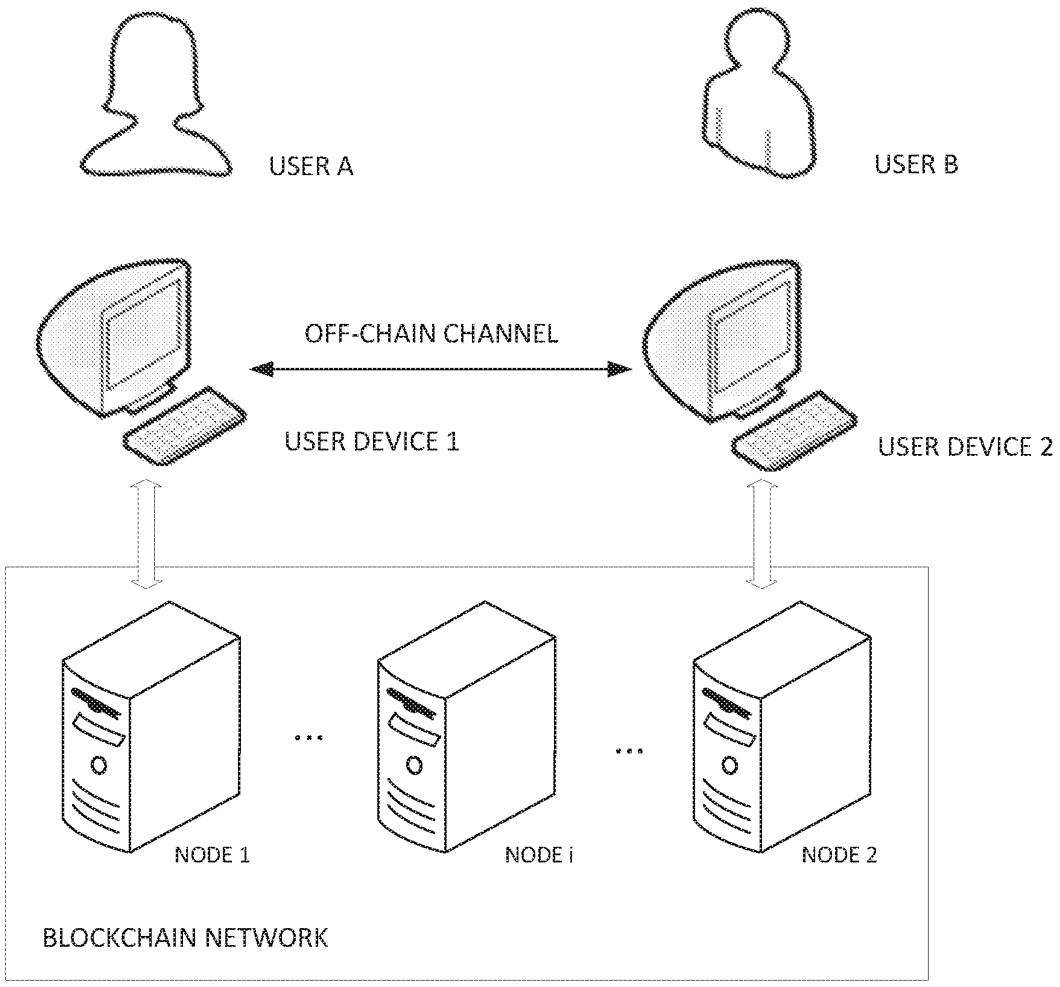
USER A
USER B
OFF-CHAIN CHANNEL
USER DEVICE 1
USER DEVICE 2
NODE 1
NODE i
NODE 2
BLOCKCHAIN NETWORK

FIG. 2

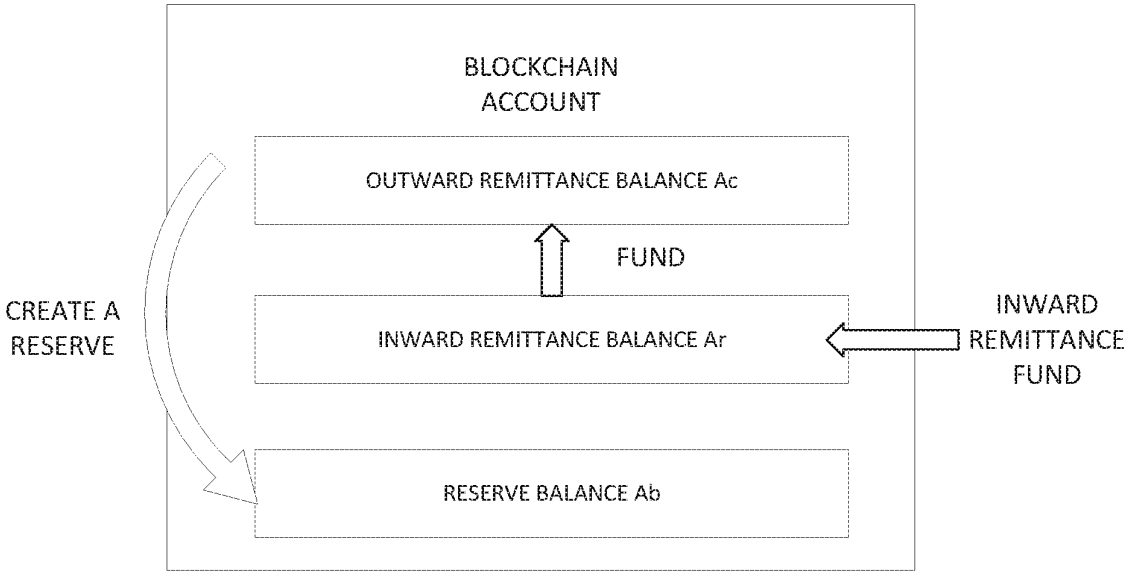
BLOCKCHAIN
ACCOUNT
OUTWARD REMITTANCE BALANCE Ac
FUND
CREATE A
RESERVE
INWARD REMITTANCE BALANCE Ar
INWARD
REMITTANCE
FUND
RESERVE BALANCE Ab

FIG. 3

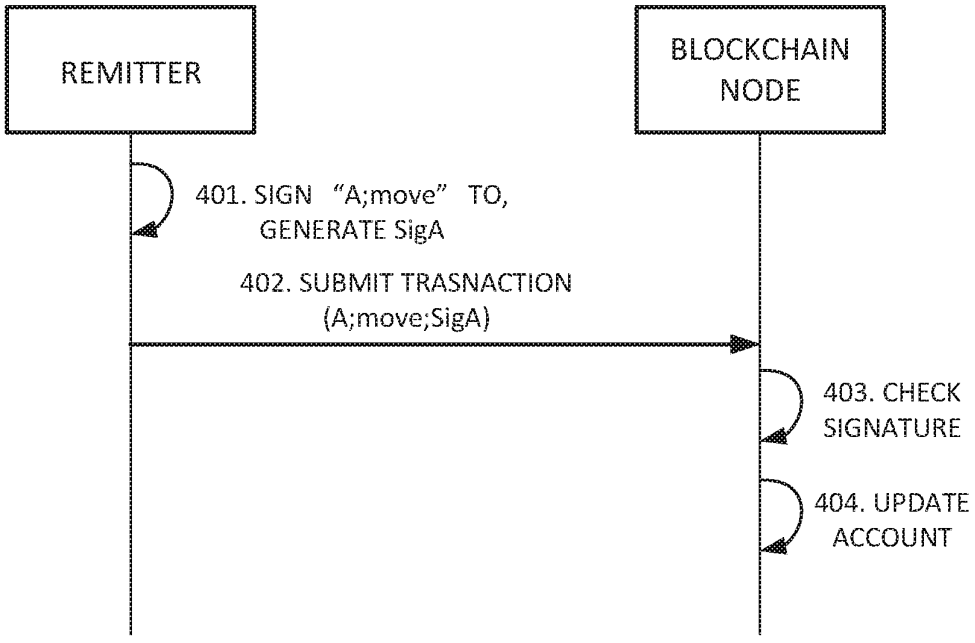
REMITTER
BLOCKCHAIN
NODE
401. SIGN "A;move" TO,
GENERATE SigA
402. SUBMIT TRASNACTION
(A;move;SigA)
403. CHECK
SIGNATURE
404. UPDATE
ACCOUNT

FIG. 4

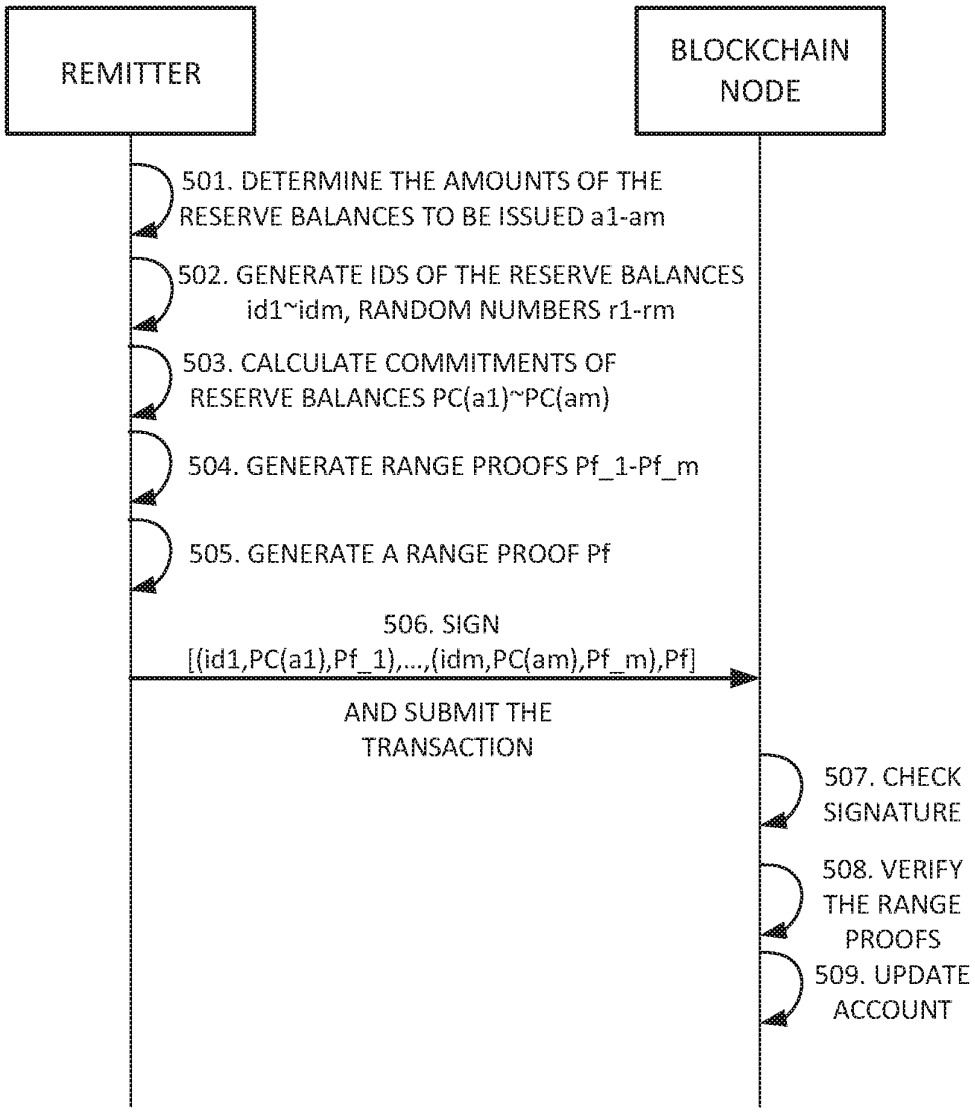
REMITTER
BLOCKCHAIN NODE
501. DETERMINE THE AMOUNTS OF THE RESERVE BALANCES TO BE ISSUED a1-am
502. GENERATE IDS OF THE RESERVE BALANCES id1~idm, RANDOM NUMBERS r1-rm
503. CALCULATE COMMITMENTS OF RESERVE BALANCES PC(a1)~PC(am)
504. GENERATE RANGE PROOFS Pf_1-Pf_m
505. GENERATE A RANGE PROOF Pf
506. SIGN [(id1,PC(a1),Pf_1),...,(idm,PC(am),Pf_m),Pf]
AND SUBMIT THE TRANSACTION
507. CHECK SIGNATURE
508. VERIFY THE RANGE PROOFS
509. UPDATE ACCOUNT

FIG. 5

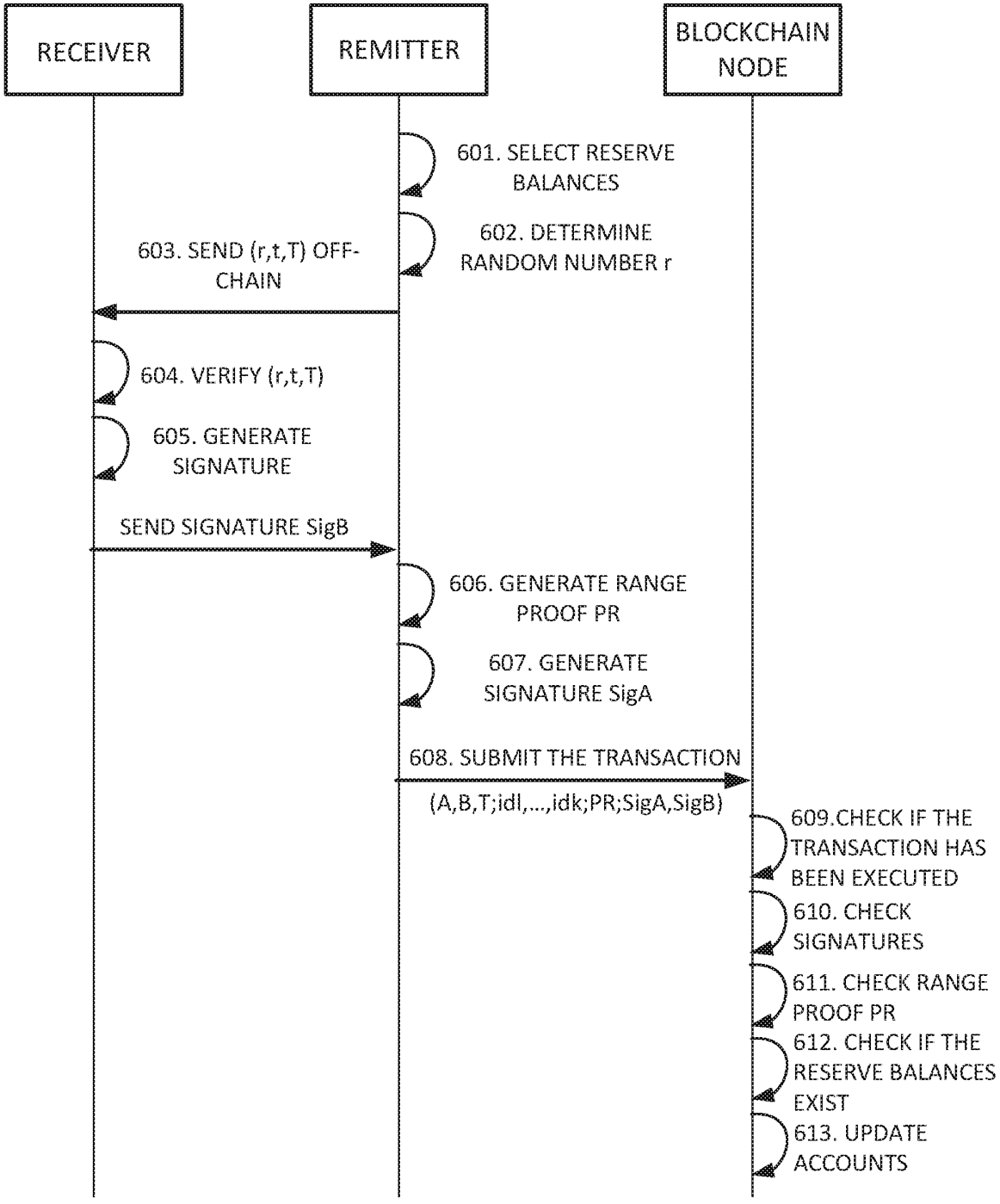
RECEIVER
REMITTER
BLOCKCHAIN NODE
601. SELECT RESERVE BALANCES
602. DETERMINE RANDOM NUMBER r
603. SEND (r,t,T) OFF-CHAIN
604. VERIFY (r,t,T)
605. GENERATE SIGNATURE
SEND SIGNATURE SigB
606. GENERATE RANGE PROOF PR
607. GENERATE SIGNATURE SigA
608. SUBMIT THE TRANSACTION
(A,B,T;idl,...,idk;PR;SigA,SigB)
609.CHECK IF THE TRANSACTION HAS BEEN EXECUTED
610. CHECK SIGNATURES
611. CHECK RANGE PROOF PR
612. CHECK IF THE RESERVE BALANCES EXIST
613. UPDATE ACCOUNTS

FIG. 6

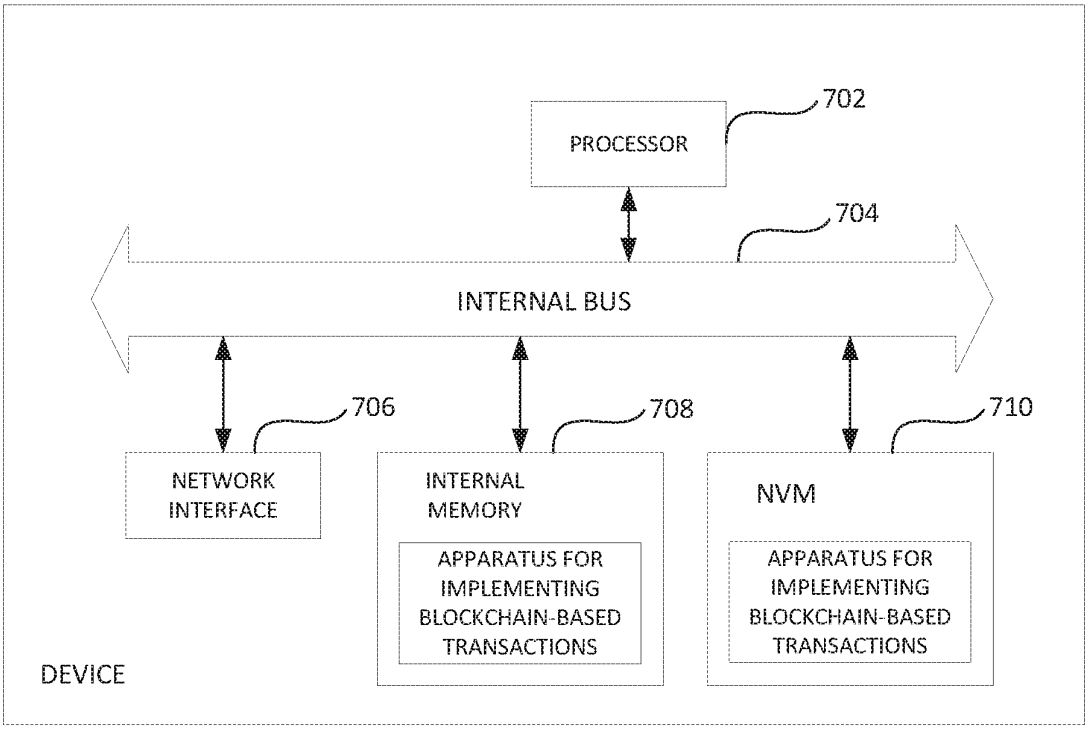
PROCESSOR
702
704
INTERNAL BUS
706
708
710
NETWORK INTERFACE
INTERNAL MEMORY
APPARATUS FOR IMPLEMENTING BLOCKCHAIN-BASED TRANSACTIONS
NVM
APPARATUS FOR IMPLEMENTING BLOCKCHAIN-BASED TRANSACTIONS
DEVICE

FIG. 7

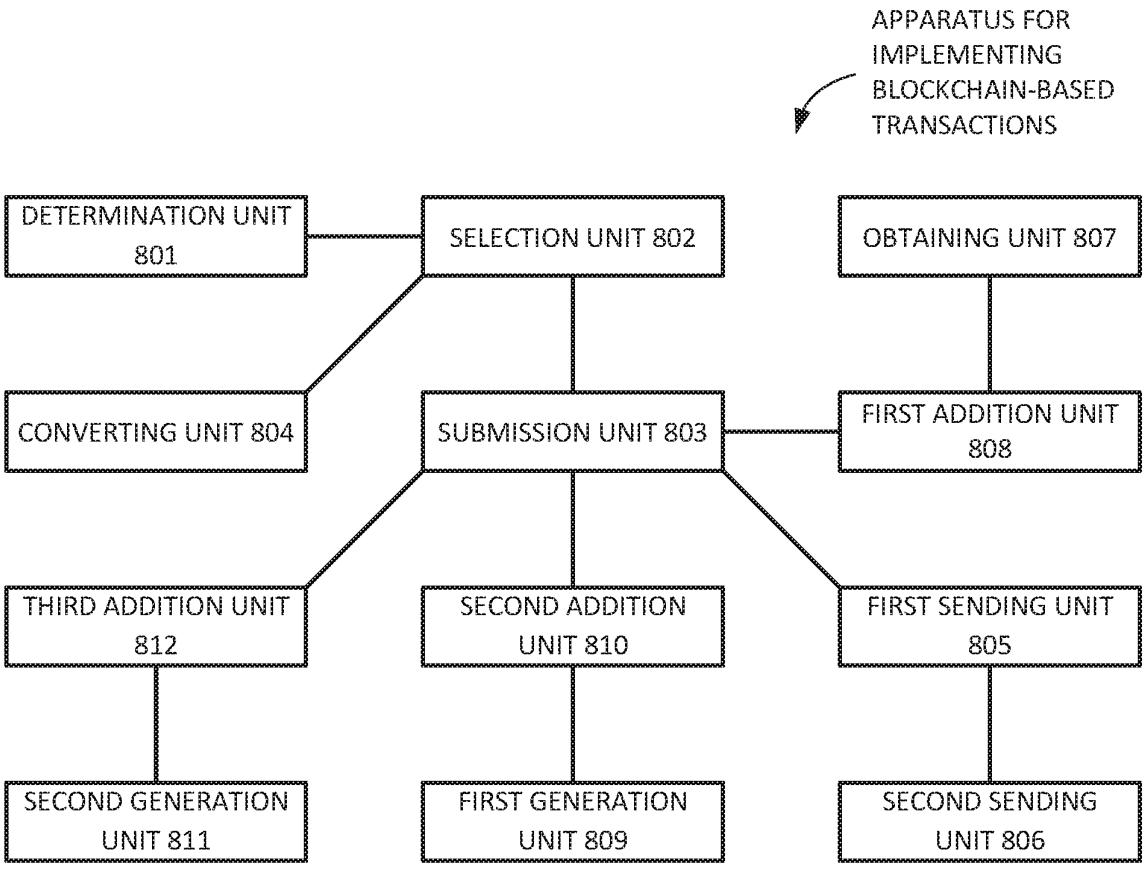
APPARATUS FOR IMPLEMENTING BLOCKCHAIN-BASED TRANSACTIONS
DETERMINATION UNIT 801
SELECTION UNIT 802
OBTAINING UNIT 807
CONVERTING UNIT 804
SUBMISSION UNIT 803
FIRST ADDITION UNIT 808
THIRD ADDITION UNIT 812
SECOND ADDITION UNIT 810
FIRST SENDING UNIT 805
SECOND GENERATION UNIT 811
FIRST GENERATION UNIT 809
SECOND SENDING UNIT 806

FIG. 8