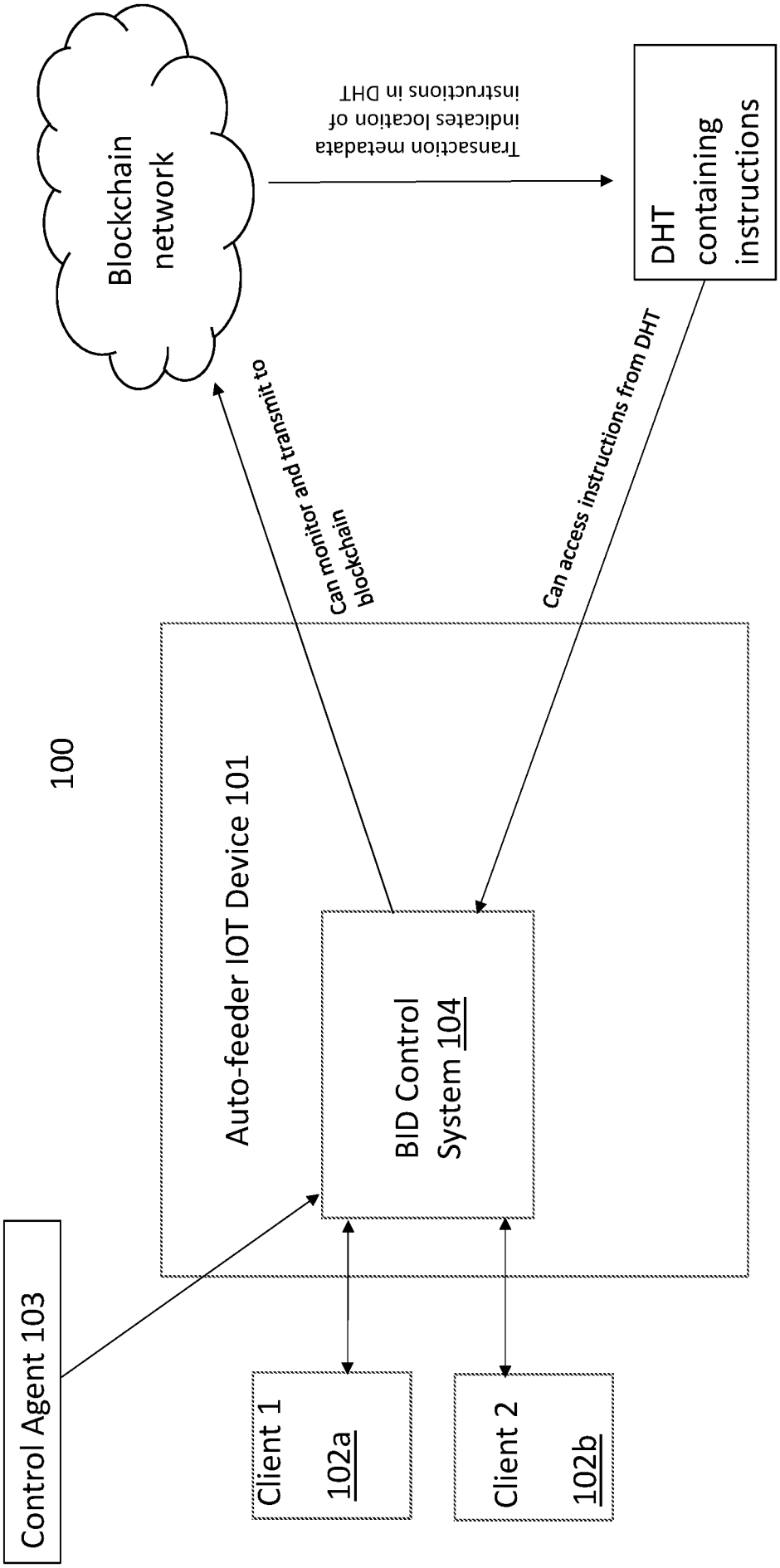
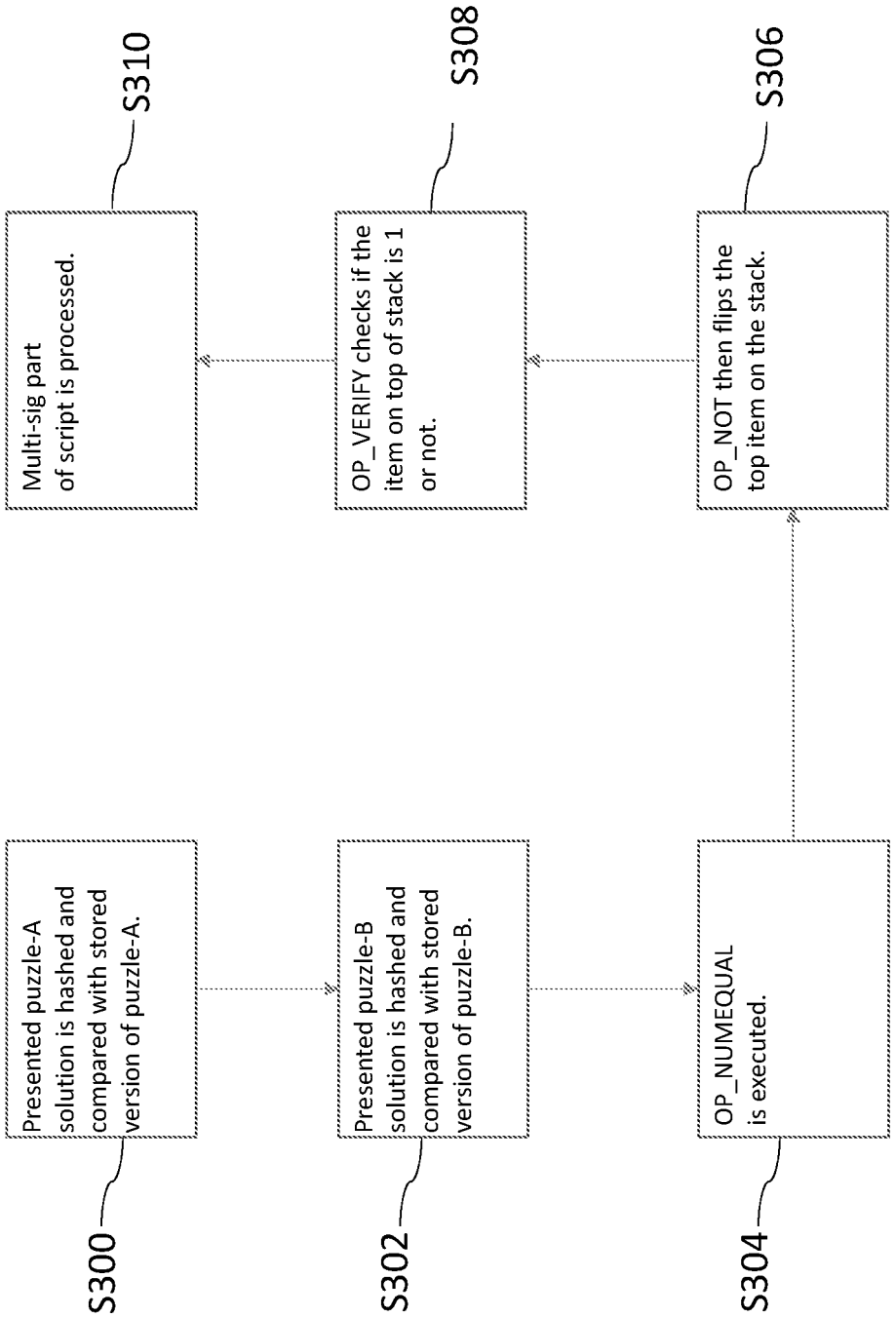

Blockchain network
Transaction metadata indicates location of instructions in DHT
DHT containing instructions
Can monitor and transmit to blockchain
Can access instructions from DHT
100
Auto-feeder IOT Device 101
BID Control System 104
Control Agent 103
Client 1 102a
Client 2 102b

Fig. 1

A	B	X
0	0	0
1	0	1
0	1	1
1	1	0

Fig. 2

Fig. 3


Presented puzzle-A solution is hashed and compared with stored version of puzzle-A.
S300
Presented puzzle-B solution is hashed and compared with stored version of puzzle-B.
S302
OP_NUMEQUAL is executed.
S304
OP_NOT then flips the top item on the stack.
S306
OP_VERIFY checks if the item on top of stack is 1 or not.
S308
Multi-sig part of script is processed.
S310

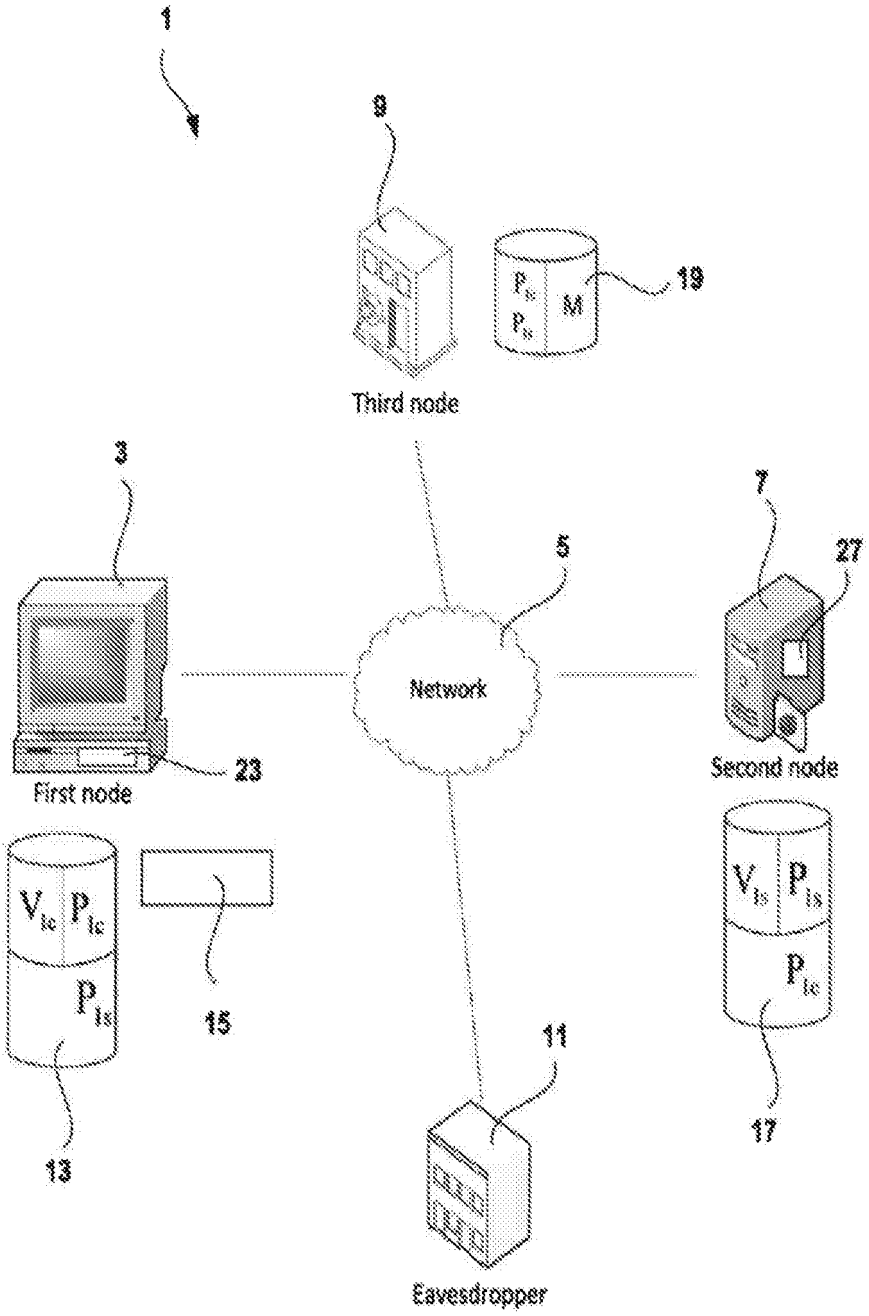

1
9
19
M
Third node
3
5
7
27
Network
First node
23
Second node
15
11
13
17
Eavesdropper

Fig. 4

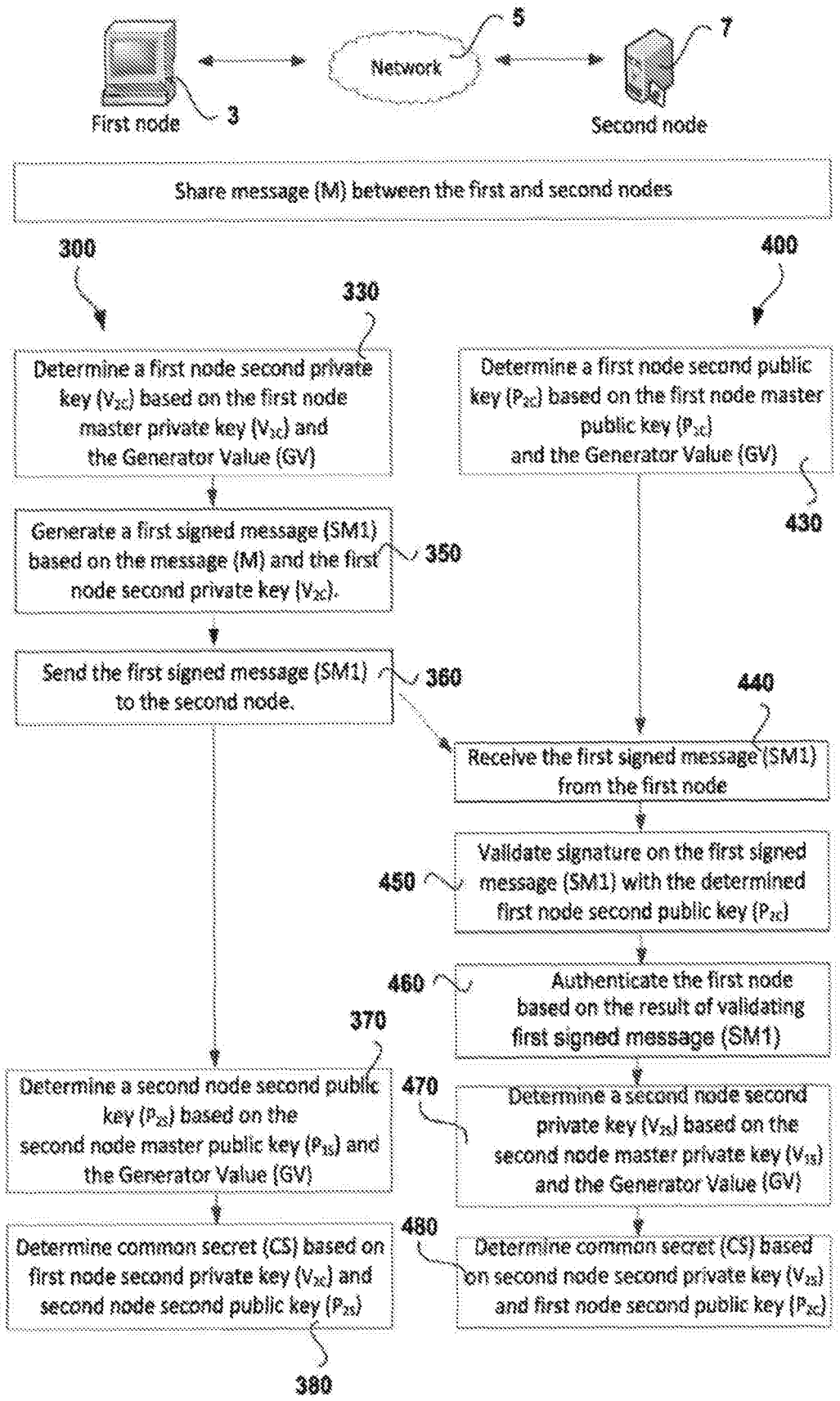

First node
3
Network
5
Second node
7
Share message (M) between the first and second nodes
300
400
330
Determine a first node second private key (V_{2C}) based on the first node master private key (V_{1C}) and the Generator Value (GV)
Determine a first node second public key (P_{2C}) based on the first node master public key (P_{1C}) and the Generator Value (GV)
430
Generate a first signed message (SM1) based on the message (M) and the first node second private key (V_{2C}).
350
Send the first signed message (SM1) to the second node.
360
440
Receive the first signed message (SM1) from the first node
Validate signature on the first signed message (SM1) with the determined first node second public key (P_{2C})
450
460
Authenticate the first node based on the result of validating first signed message (SM1)
370
Determine a second node second public key (P_{2S}) based on the second node master public key (P_{1S}) and the Generator Value (GV)
470
Determine a second node second private key (V_{2S}) based on the second node master private key (V_{1S}) and the Generator Value (GV)
480
Determine common secret (CS) based on first node second private key (V_{2C}) and second node second public key (P_{2S})
Determine common secret (CS) based on second node second private key (V_{2S}) and first node second public key (P_{2C})
380

Fig. 5

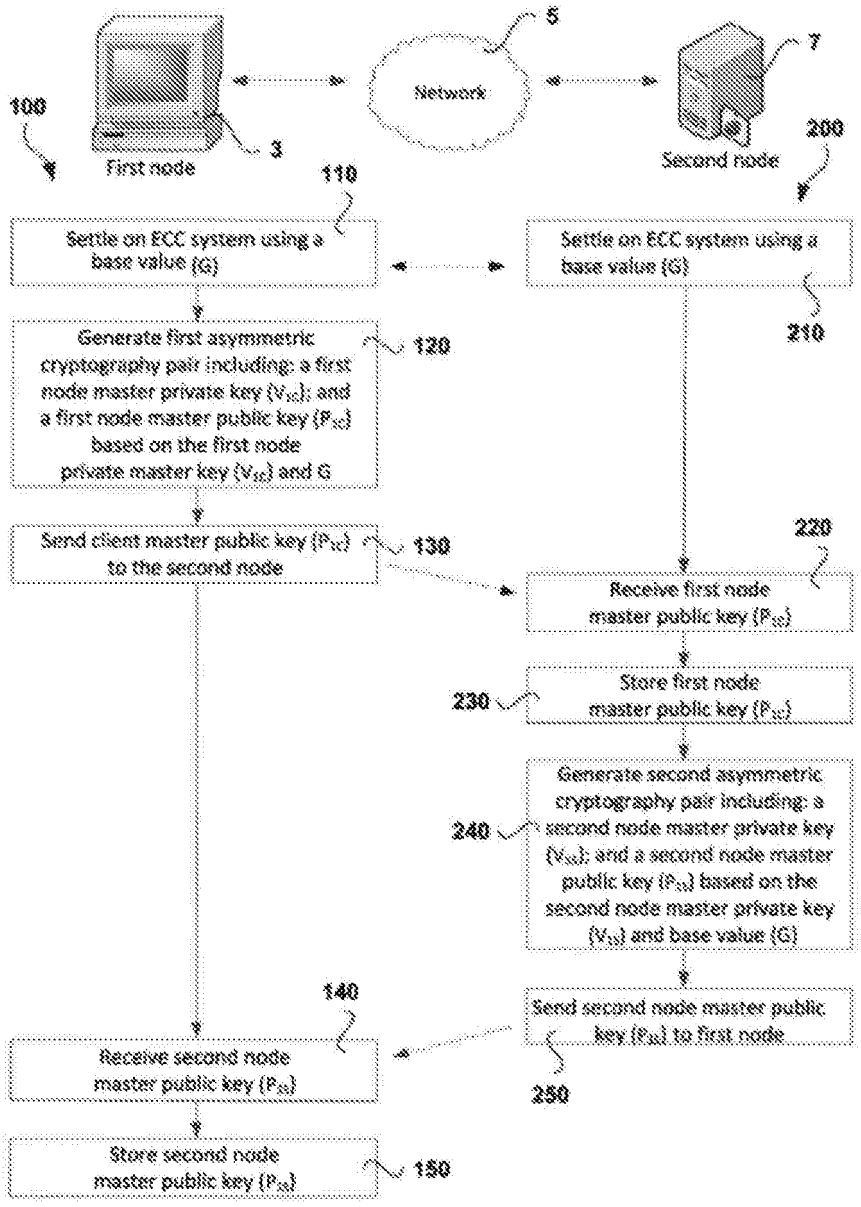

100
First node
3
5
Network
7
Second node
200
110
Settle on ECC system using a base value (G)
Settle on ECC system using a base value (G)
210
120
Generate first asymmetric cryptography pair including: a first node master private key (V_{1M}); and a first node master public key (P_{1C}) based on the first node private master key (V_{1M}) and G
130
Send client master public key (P_{1C}) to the second node
220
Receive first node master public key (P_{1C})
230
Store first node master public key (P_{1C})
240
Generate second asymmetric cryptography pair including: a second node master private key (V_{2M}); and a second node master public key (P_{2M}) based on the second node master private key (V_{2M}) and base value (G)
140
Receive second node master public key (P_{2M})
Send second node master public key (P_{2M}) to first node
250
150
Store second node master public key (P_{2M})

Fig. 6

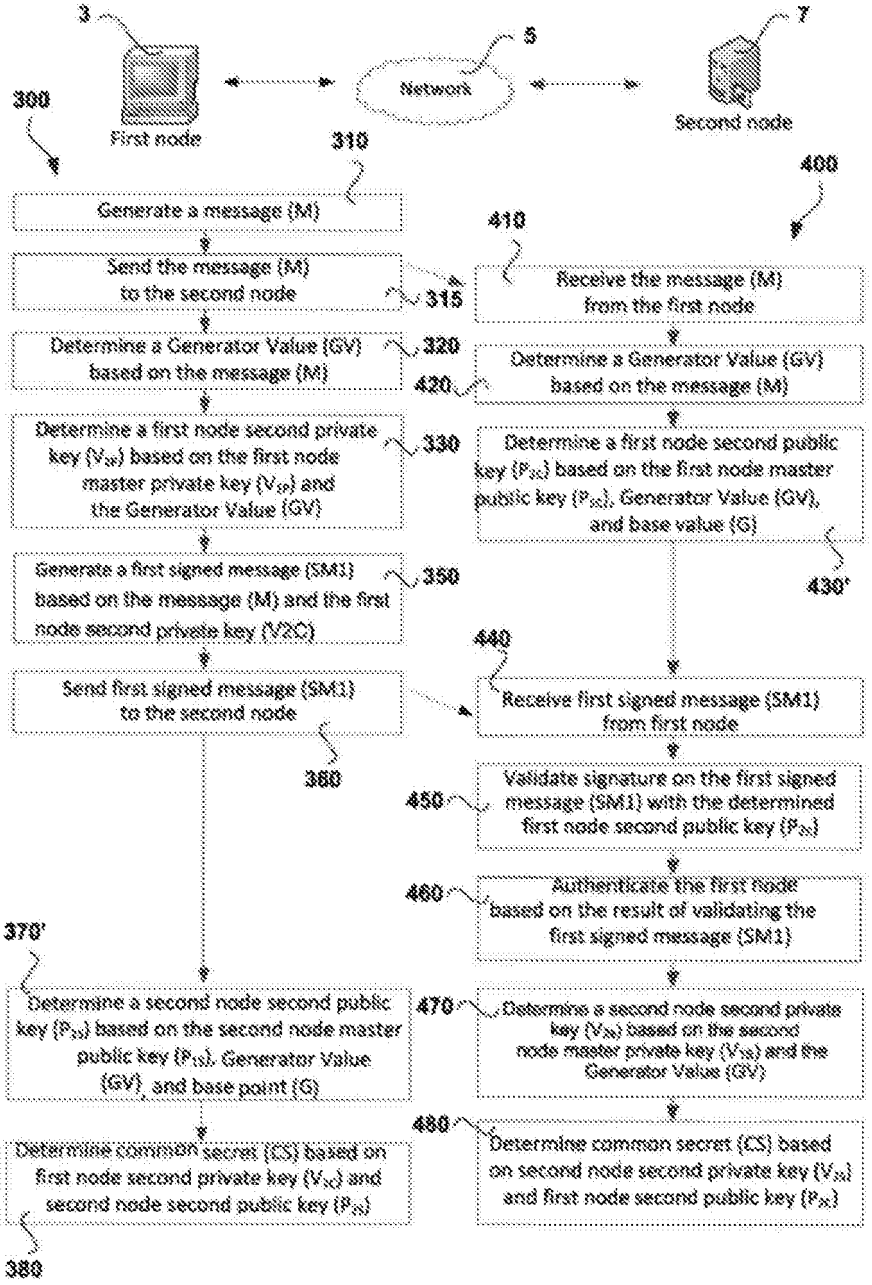

3
5
7
Network
First node
Second node
300
310
400
Generate a message (M)
410
Send the message (M) to the second node
315
Receive the message (M) from the first node
Determine a Generator Value (GV) based on the message (M)
320
420
Determine a first node second private key (V_{2A}) based on the first node master private key (V_{1A}) and the Generator Value (GV)
330
Determine a first node second public key (P_{2A}) based on the first node master public key (P_{1A}), Generator Value (GV), and base value (G)
430'
Generate a first signed message (SM1) based on the message (M) and the first node second private key (V2C)
350
440
Send first signed message (SM1) to the second node
380
Receive first signed message (SM1) from first node
450
Validate signature on the first signed message (SM1) with the determined first node second public key (P_{2A})
460
Authenticate the first node based on the result of validating the first signed message (SM1)
370'
Determine a second node second public key (P_{2B}) based on the second node master public key (P_{1B}), Generator Value (GV), and base point (G)
470
Determine a second node second private key (V_{2B}) based on the second node master private key (V_{1B}) and the Generator Value (GV)
480
Determine common secret (CS) based on first node second private key (V_{2C}) and second node second public key (P_{2B})
Determine common secret (CS) based on second node second private key (V_{2B}) and first node second public key (P_{2A})
380

Fig. 7

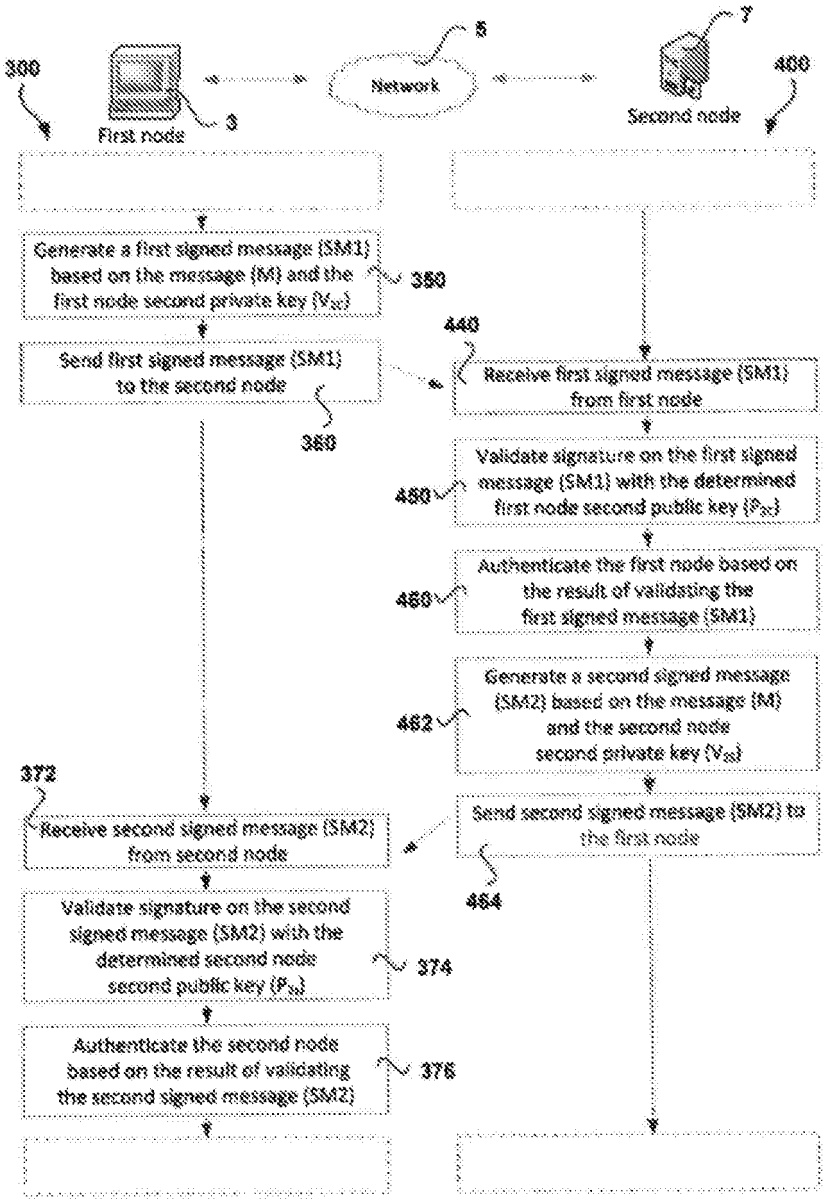

300
First node
3
5
Network
7
Second node
400
Generate a first signed message (SM1) based on the message (M) and the first node second private key (V_{2A})
350
Send first signed message (SM1) to the second node
360
440
Receive first signed message (SM1) from first node
450
Validate signature on the first signed message (SM1) with the determined first node second public key (P_{2A})
460
Authenticate the first node based on the result of validating the first signed message (SM1)
462
Generate a second signed message (SM2) based on the message (M) and the second node second private key (V_{2B})
464
Send second signed message (SM2) to the first node
372
Receive second signed message (SM2) from second node
374
Validate signature on the second signed message (SM2) with the determined second node second public key (P_{2B})
376
Authenticate the second node based on the result of validating the second signed message (SM2)

Fig. 8

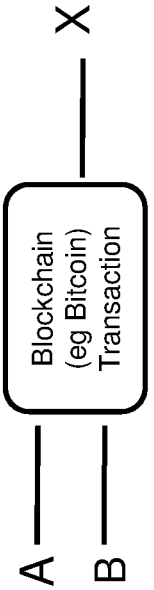


FIGURE 9

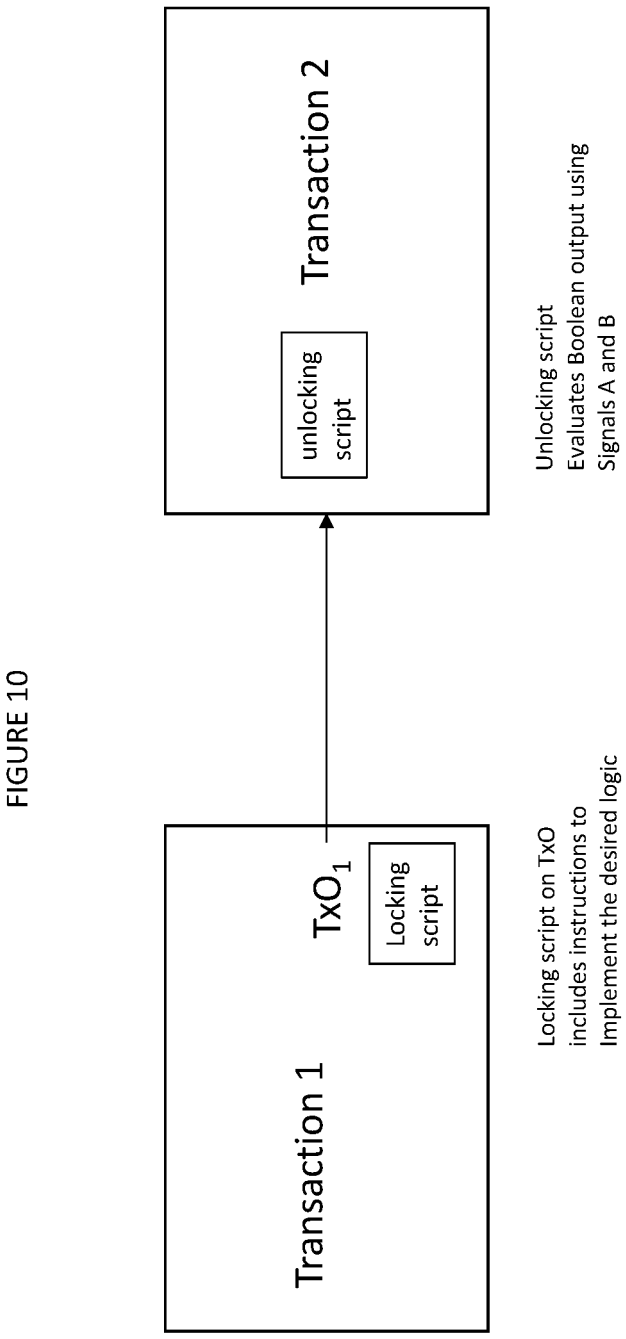
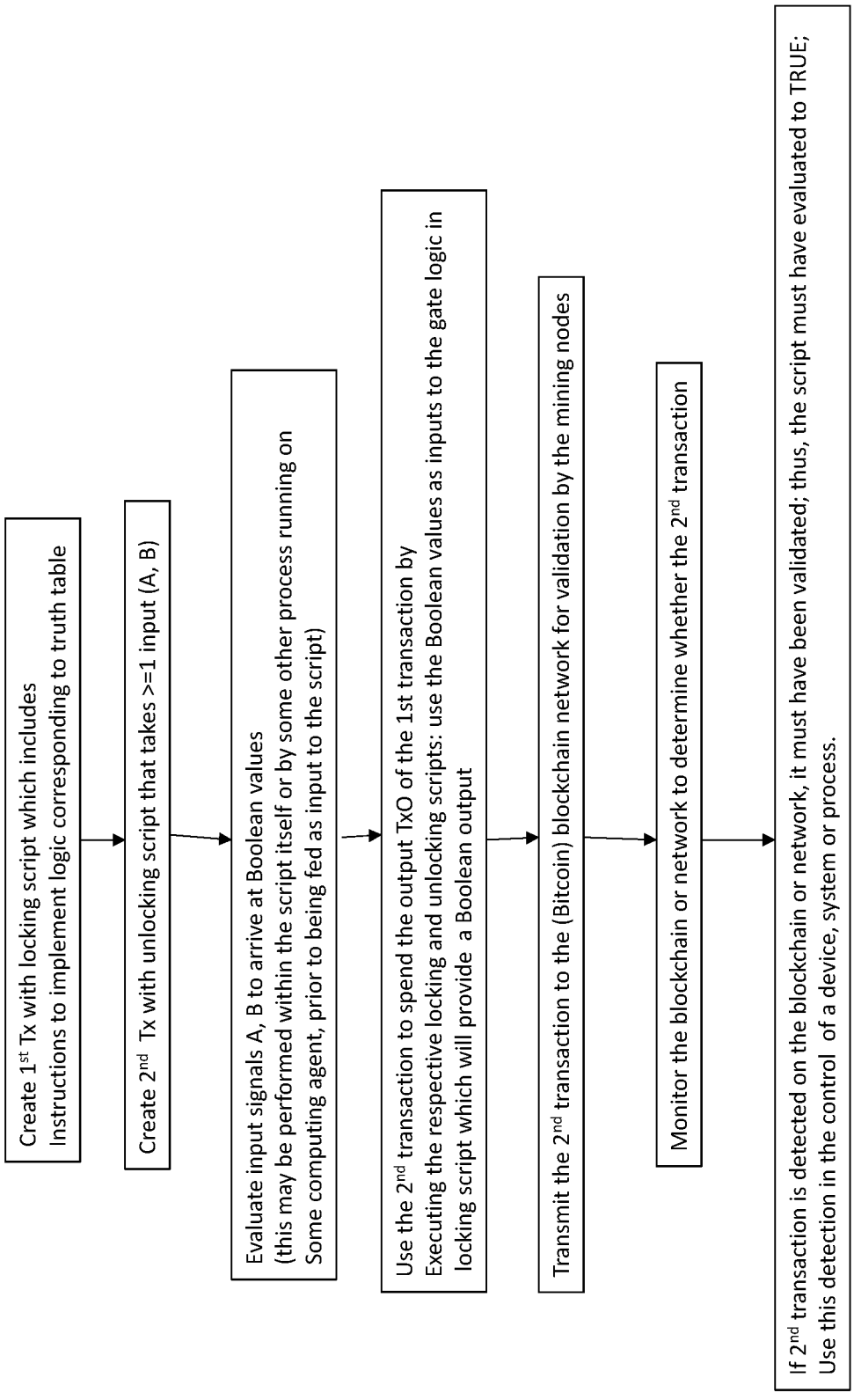

Transaction 1
TxO_1
Locking script
Transaction 2
unlocking script
Unlocking script
Evaluates Boolean output using
Signals A and B
Locking script on TxO
includes instructions to
Implement the desired logic

FIGURE 10

FIGURE 11


Create 1st Tx with locking script which includes Instructions to implement logic corresponding to truth table
Create 2nd Tx with unlocking script that takes >=1 input (A, B)
Evaluate input signals A, B to arrive at Boolean values (this may be performed within the script itself or by some other process running on Some computing agent, prior to being fed as input to the script)
Use the 2nd transaction to spend the output TxO of the 1st transaction by Executing the respective locking and unlocking scripts: use the Boolean values as inputs to the gate logic in locking script which will provide a Boolean output
Transmit the 2nd transaction to the (Bitcoin) blockchain network for validation by the mining nodes
Monitor the blockchain or network to determine whether the 2nd transaction
If 2nd transaction is detected on the blockchain or network, it must have been validated; thus, the script must have evaluated to TRUE; Use this detection in the control of a device, system or process.