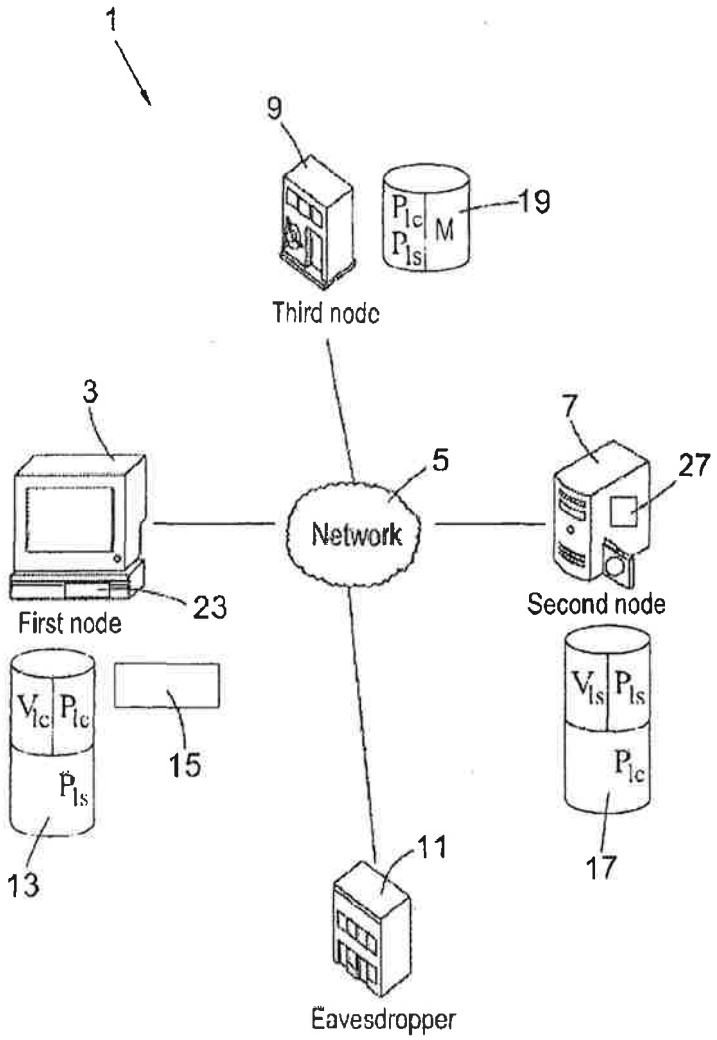
1
9
P_{lc}
P_{ls}
M
19
Third node
3
7
5
27
Network
First node
23
Second node
V_{lc}
P_{lc}
P_{ls}
15
V_{ls}
P_{ls}
P_{lc}
13
17
11
Eavesdropper

Fig. 1

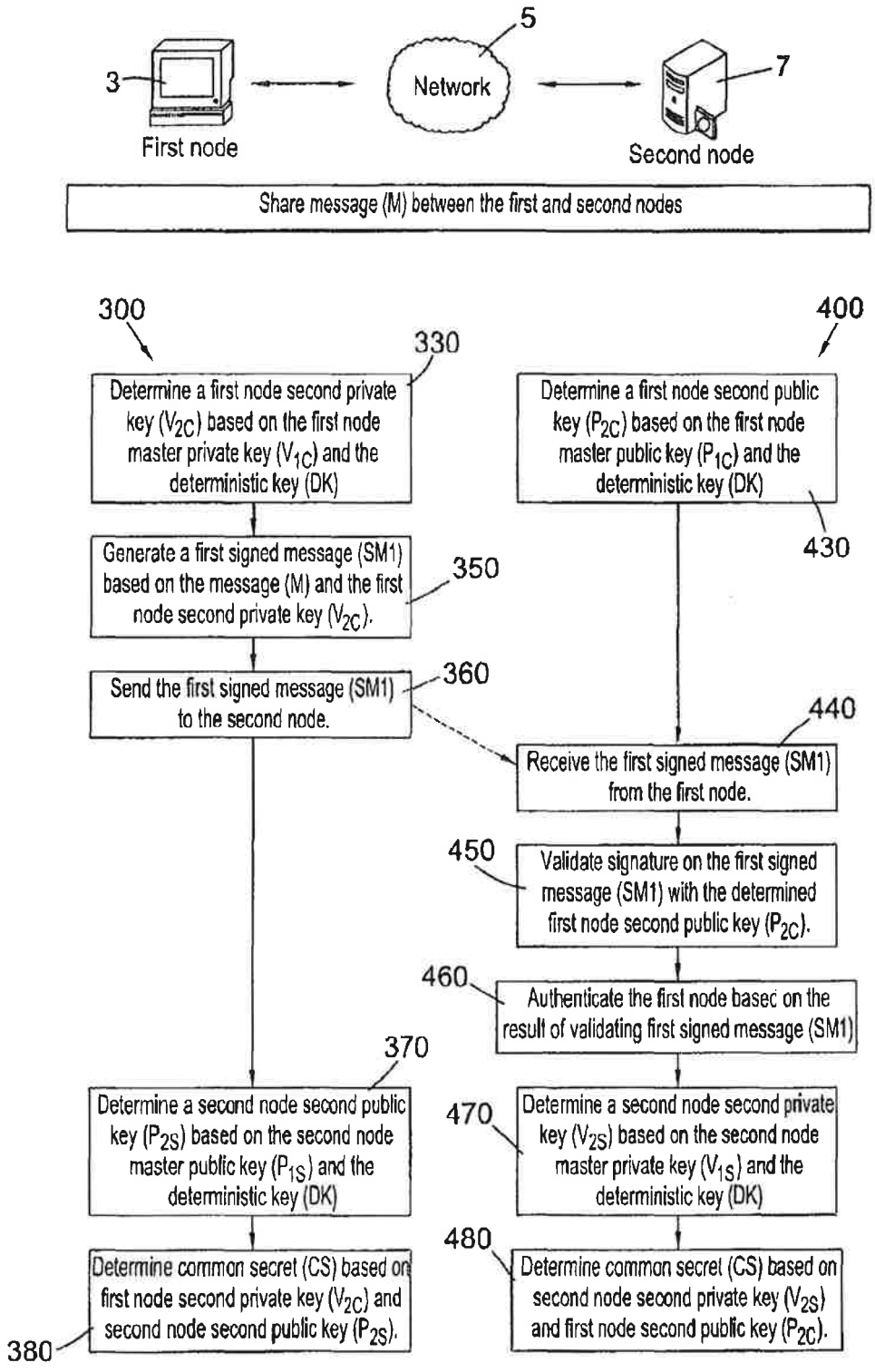
5
3
Network
7
First node
Second node
Share message (M) between the first and second nodes
300
400
330
Determine a first node second private key (V_{2C}) based on the first node master private key (V_{1C}) and the deterministic key (DK)
Determine a first node second public key (P_{2C}) based on the first node master public key (P_{1C}) and the deterministic key (DK)
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.
450
Validate signature on the first signed message (SM1) with the determined first node second public key (P_{2C}).
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 deterministic key (DK)
470
Determine a second node second private key (V_{2S}) based on the second node master private key (V_{1S}) and the deterministic key (DK)
480
Determine common secret (CS) based on first node second private key (V_{2C}) and second node second public key (P_{2S}).
380
Determine common secret (CS) based on second node second private key (V_{2S}) and first node second public key (P_{2C}).

Fig. 2

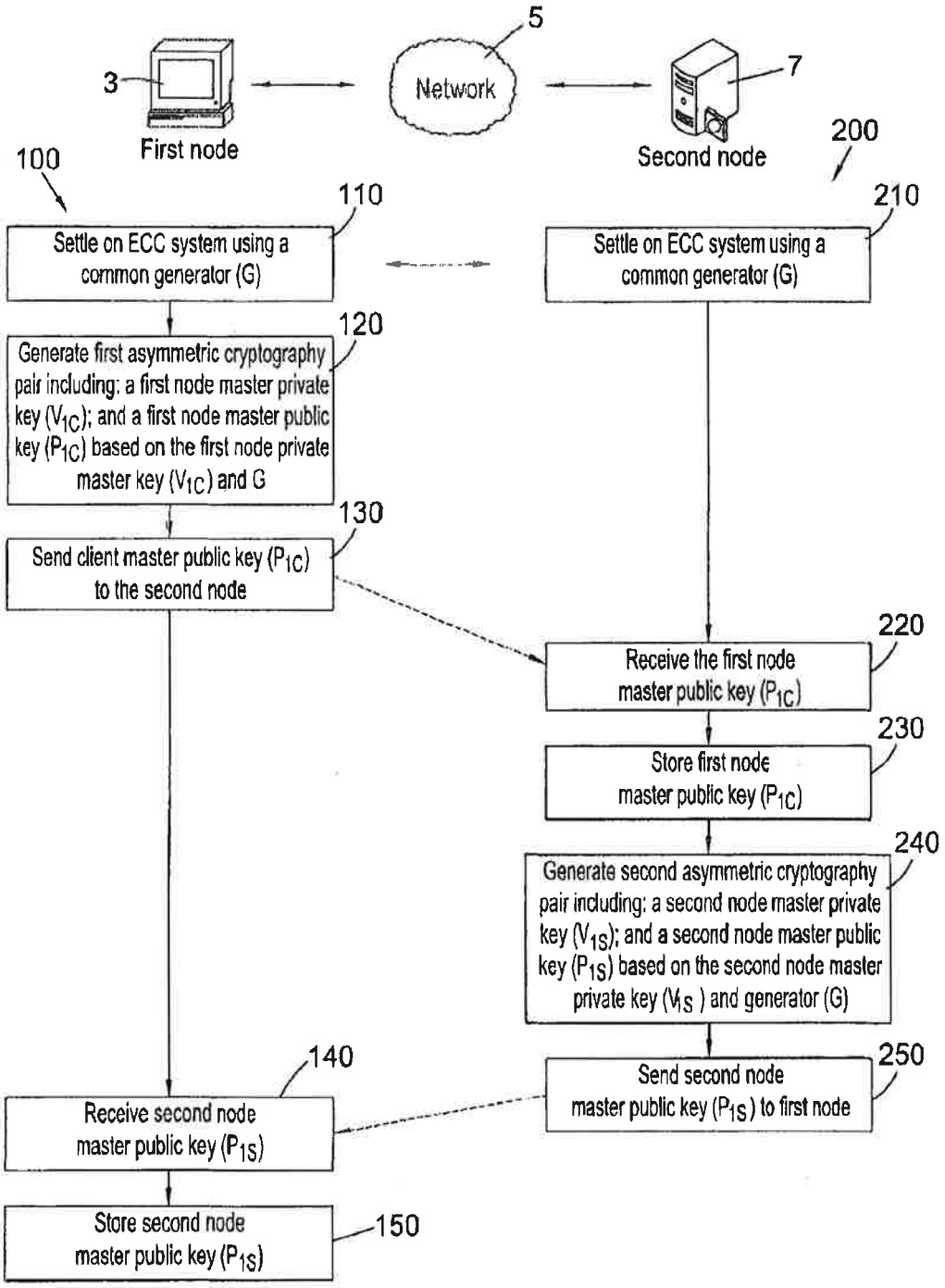
5
Network
3
First node
7
Second node
100
200
110
Settle on ECC system using a common generator (G)
210
Settle on ECC system using a common generator (G)
120
Generate first asymmetric cryptography pair including: a first node master private key (V_{1C}); and a first node master public key (P_{1C}) based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

Fig. 3

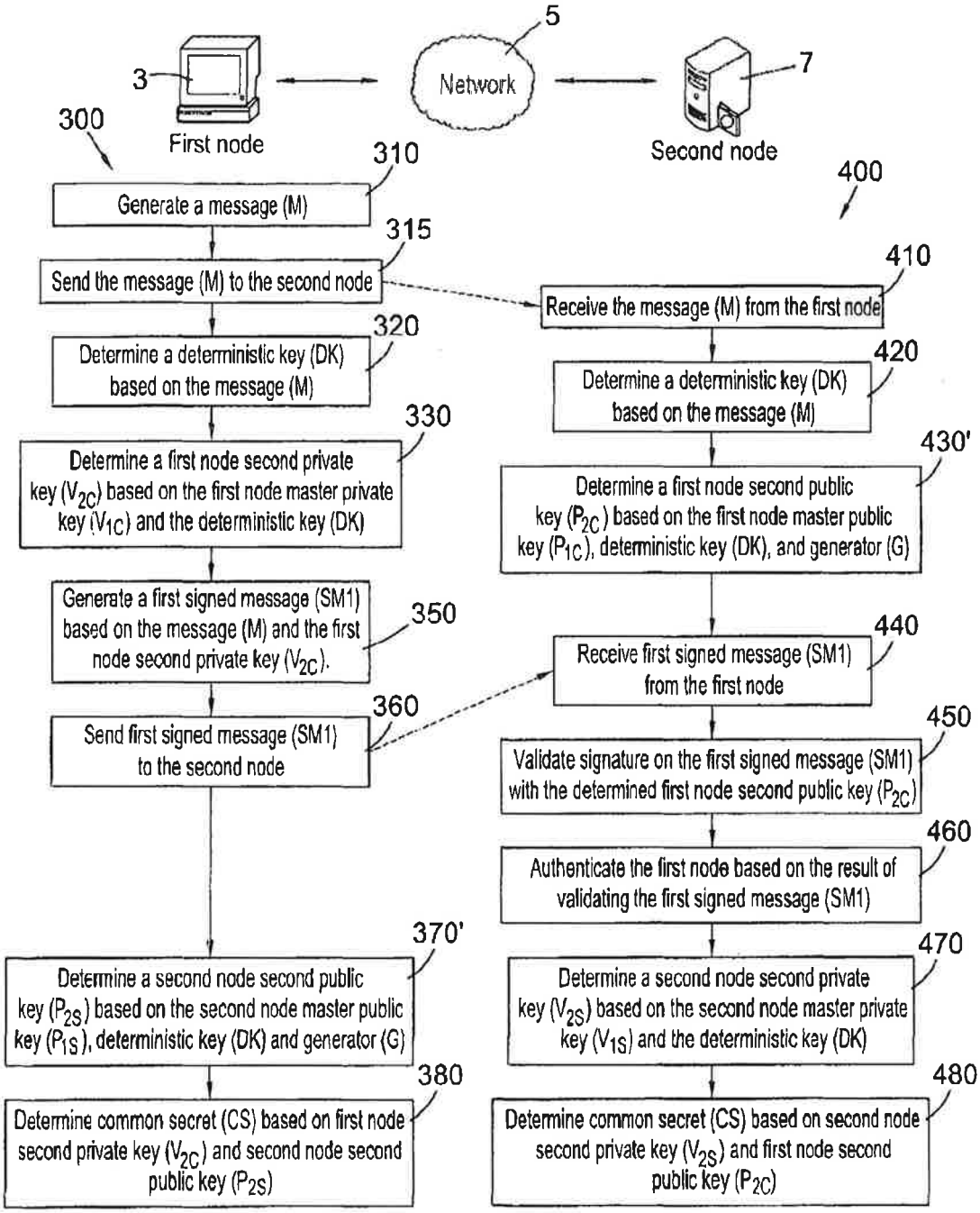
5
Network
3
First node
7
Second node
300
310
Generate a message (M)
315
Send the message (M) to the second node
320
Determine a deterministic key (DK) based on the message (M)
330
Determine a first node second private key (V_{2C}) based on the first node master private key (V_{1C}) and the deterministic key (DK)
Generate a first signed message (SM1) based on the message (M) and the first node second private key (V_{2C}).
350
Send first signed message (SM1) to the second node
360
370'
Determine a second node second public key (P_{2S}) based on the second node master public key (P_{1S}), deterministic key (DK) and generator (G)
380
Determine common secret (CS) based on first node second private key (V_{2C}) and second node second public key (P_{2S})
400
410
Receive the message (M) from the first node
420
Determine a deterministic key (DK) based on the message (M)
430'
Determine a first node second public key (P_{2C}) based on the first node master public key (P_{1C}), deterministic key (DK), and generator (G)
440
Receive first signed message (SM1) from the first node
450
Validate signature on the first signed message (SM1) with the determined first node second public key (P_{2C})
460
Authenticate the first node based on the result of validating the first signed message (SM1)
470
Determine a second node second private key (V_{2S}) based on the second node master private key (V_{1S}) and the deterministic key (DK)
480
Determine common secret (CS) based on second node second private key (V_{2S}) and first node second public key (P_{2C})

Fig. 4

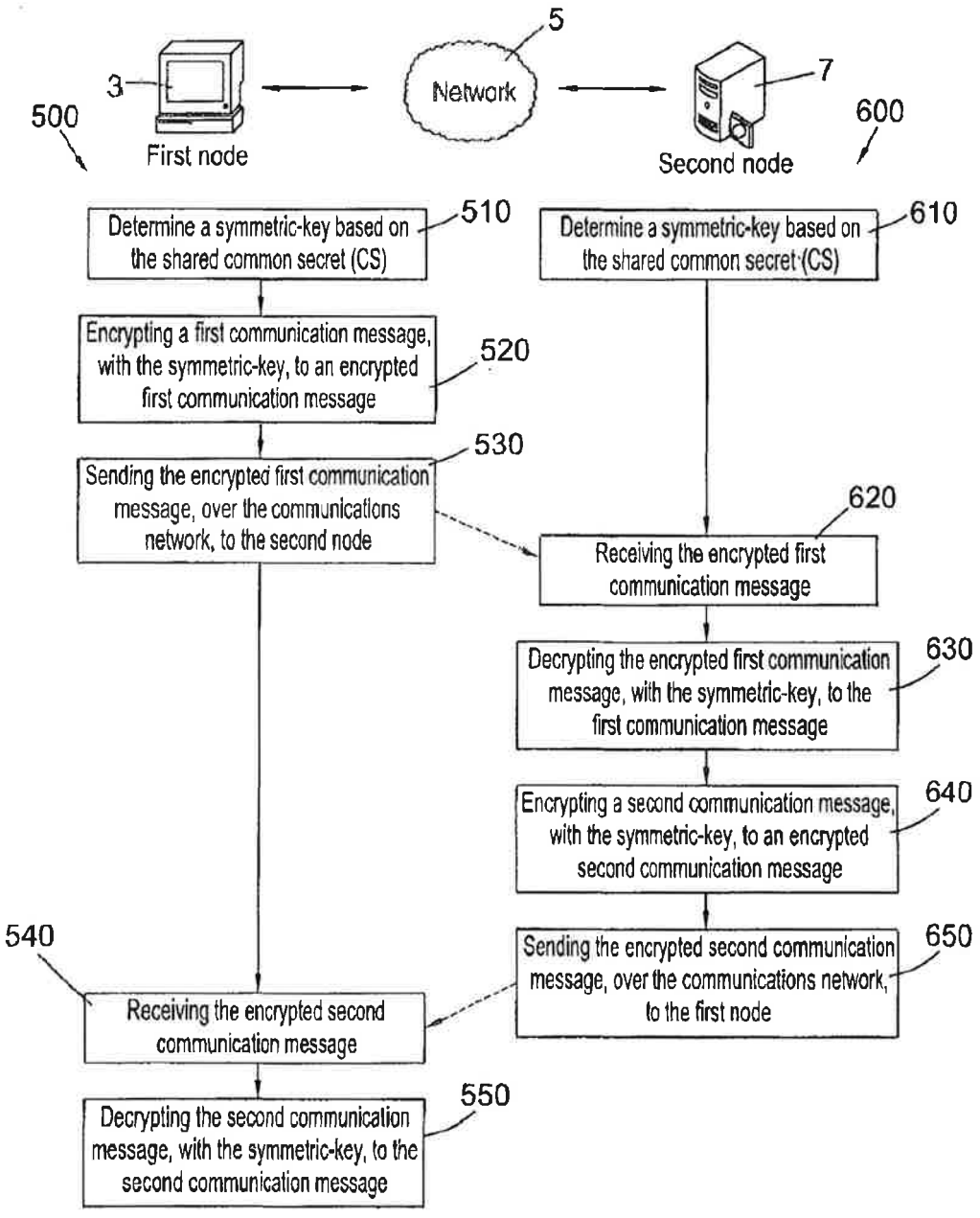
5
Network
3
7
500
First node
600
Second node
Determine a symmetric-key based on the shared common secret (CS)
510
Determine a symmetric-key based on the shared common secret (CS)
610
Encrypting a first communication message, with the symmetric-key, to an encrypted first communication message
520
Sending the encrypted first communication message, over the communications network, to the second node
530
620
Receiving the encrypted first communication message
Decrypting the encrypted first communication message, with the symmetric-key, to the first communication message
630
Encrypting a second communication message, with the symmetric-key, to an encrypted second communication message
640
540
Sending the encrypted second communication message, over the communications network, to the first node
650
Receiving the encrypted second communication message
Decrypting the second communication message, with the symmetric-key, to the second communication message
550

Fig. 5

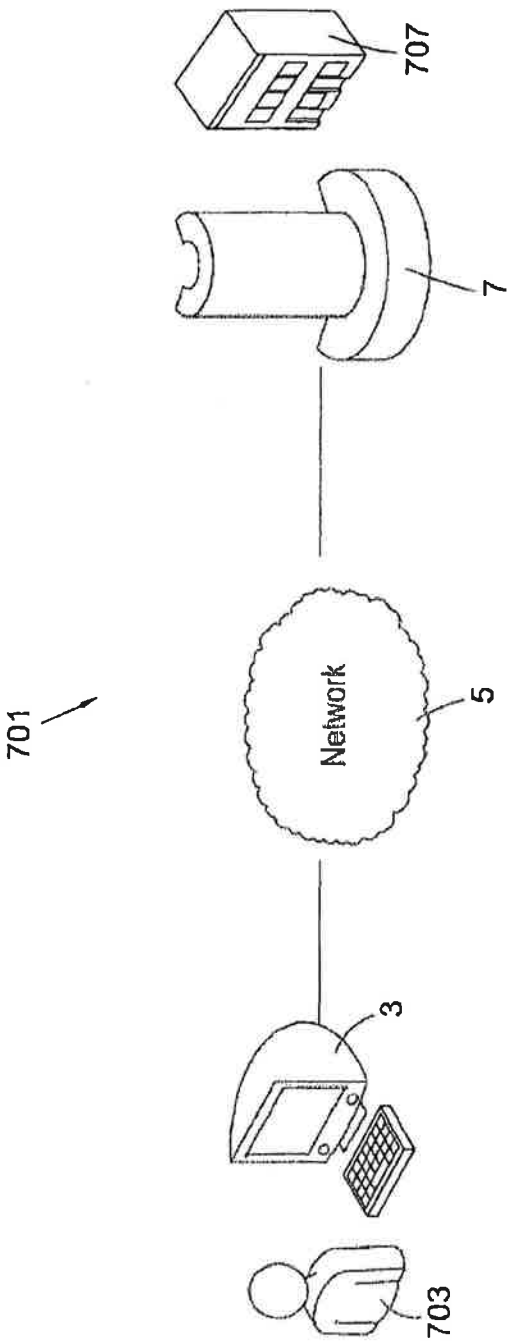

Fig. 6

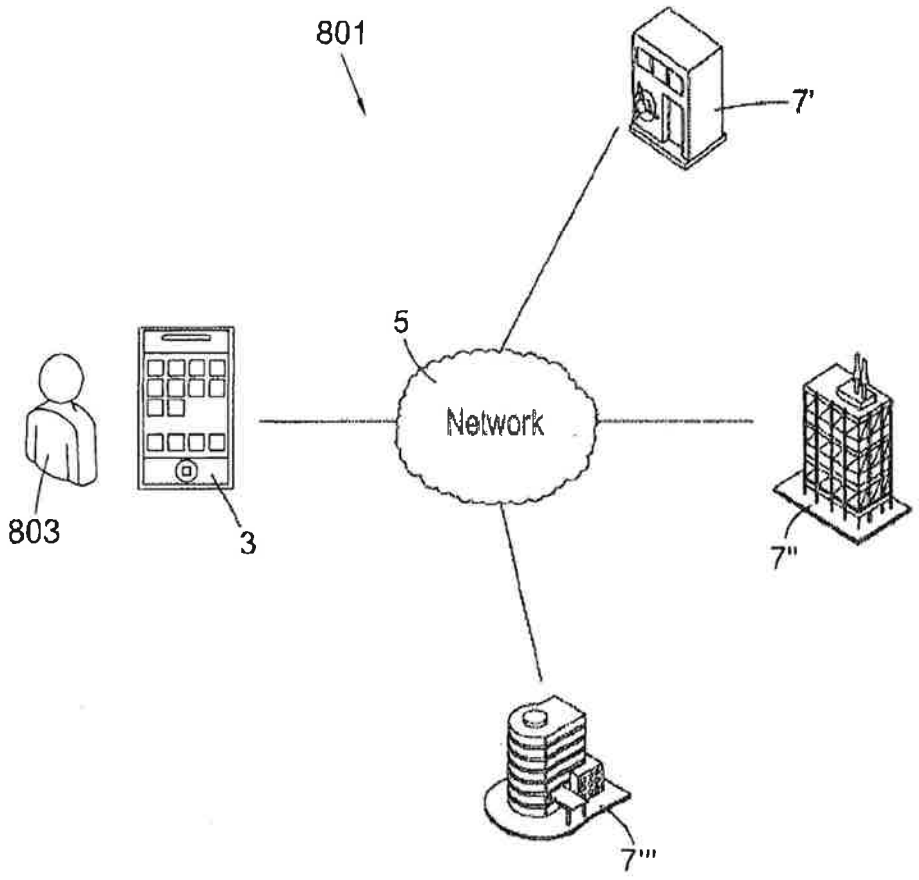

Fig. 7

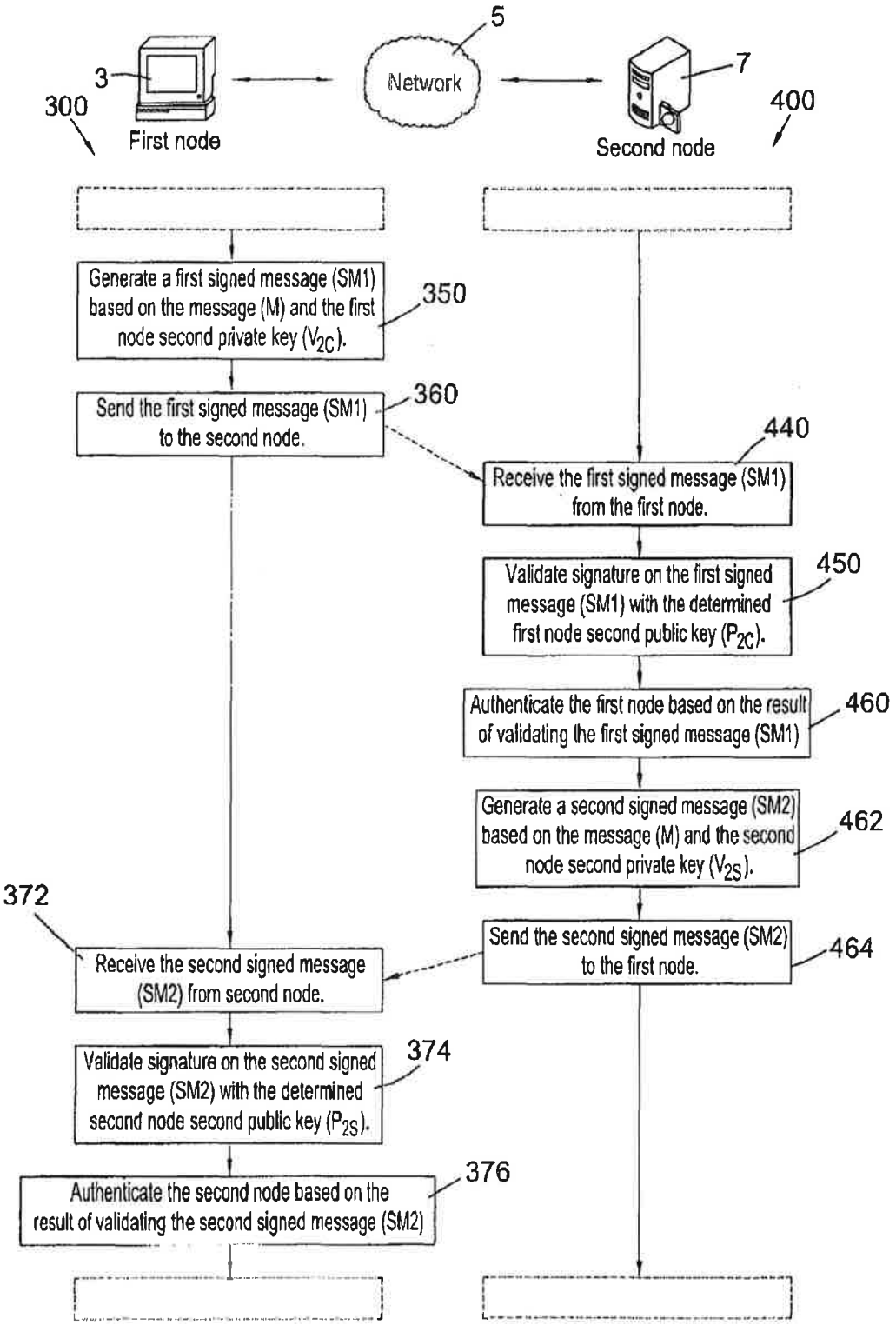
5
Network
3
300
First node
7
400
Second node
Generate a first signed message (SM1) based on the message (M) and the first node second private key (V_{2C}).
350
Send the first signed message (SM1) to the second node.
360
440
Receive the first signed message (SM1) from the first node.
Validate signature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

Fig. 8

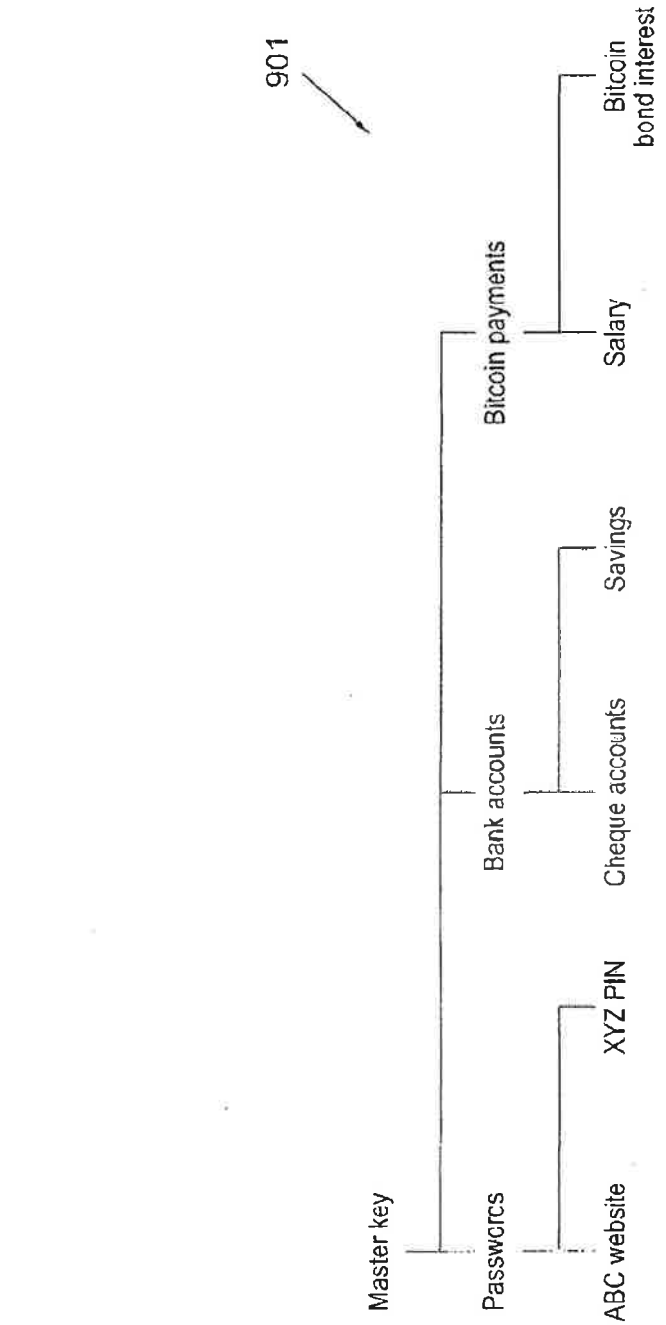
901
Master key
Passwords
ABC website
XYZ PIN
Bank accounts
Cheque accounts
Savings
Bitcoin payments
Salary
Bitcoin bond interest

Fig. 9

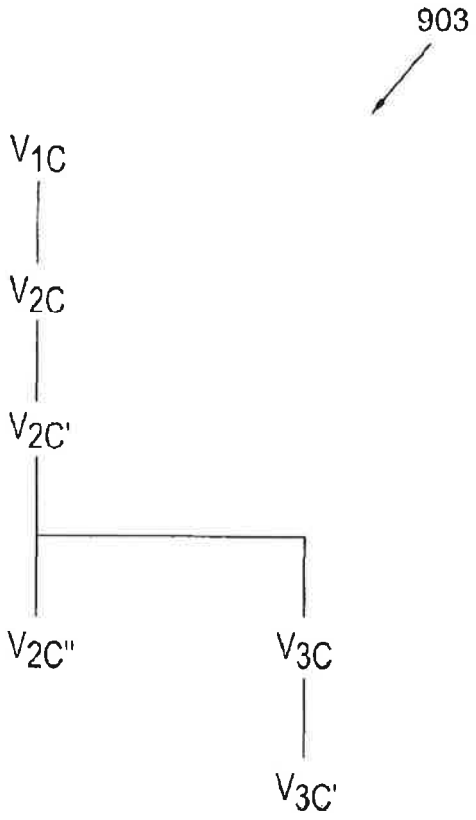

Fig. 10

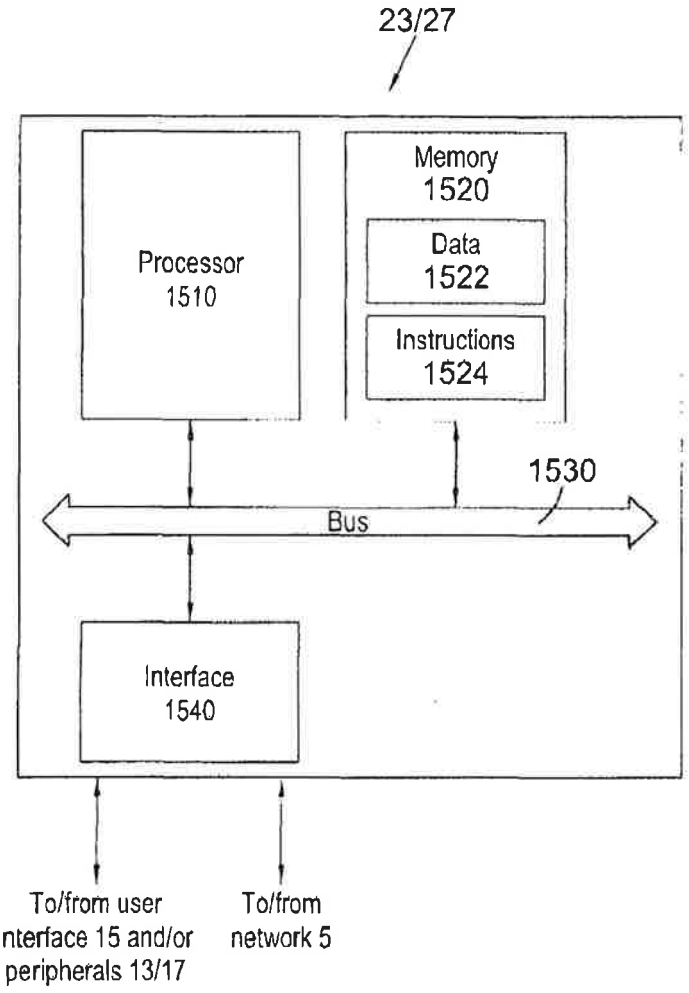
23/27
Memory
1520
Data
1522
Instructions
1524
Processor
1510
1530
Bus
Interface
1540
To/from user
interface 15 and/or
peripherals 13/17
To/from
network 5

Fig. 11