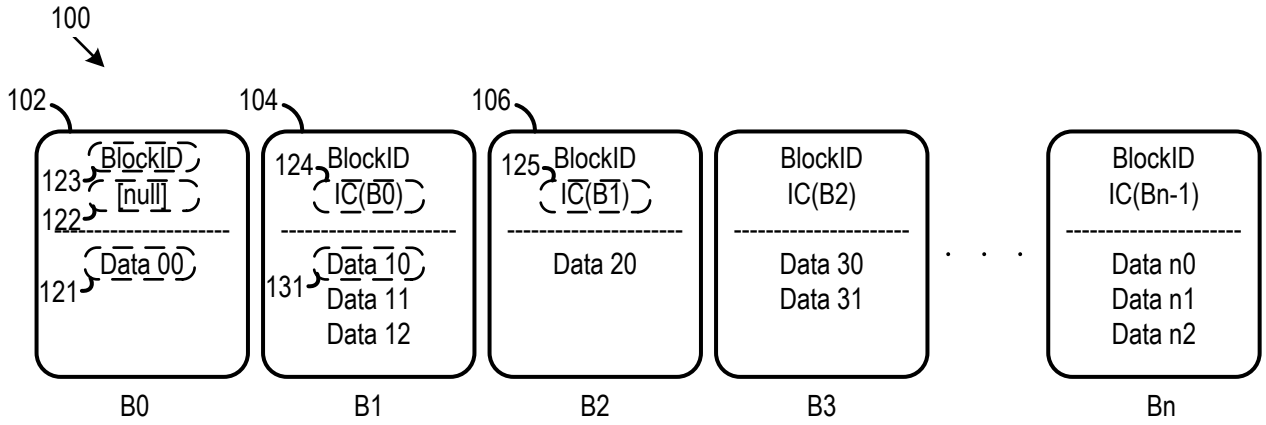
100
102
104
106
BlockID
123
[null]
122
Data 00
121
124
BlockID
IC(B0)
Data 10
131
Data 11
Data 12
125
BlockID
IC(B1)
Data 20
BlockID
IC(B2)
Data 30
Data 31
BlockID
IC(Bn-1)
Data n0
Data n1
Data n2
B0
B1
B2
B3
Bn

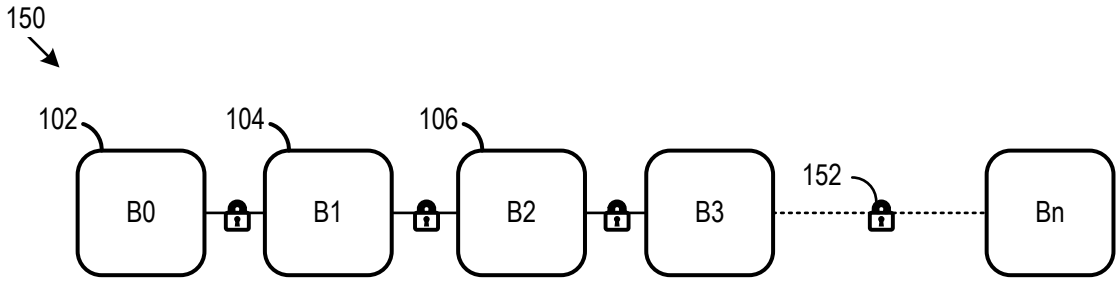
150
102
104
106
152
B0
B1
B2
B3
Bn

Figure 1

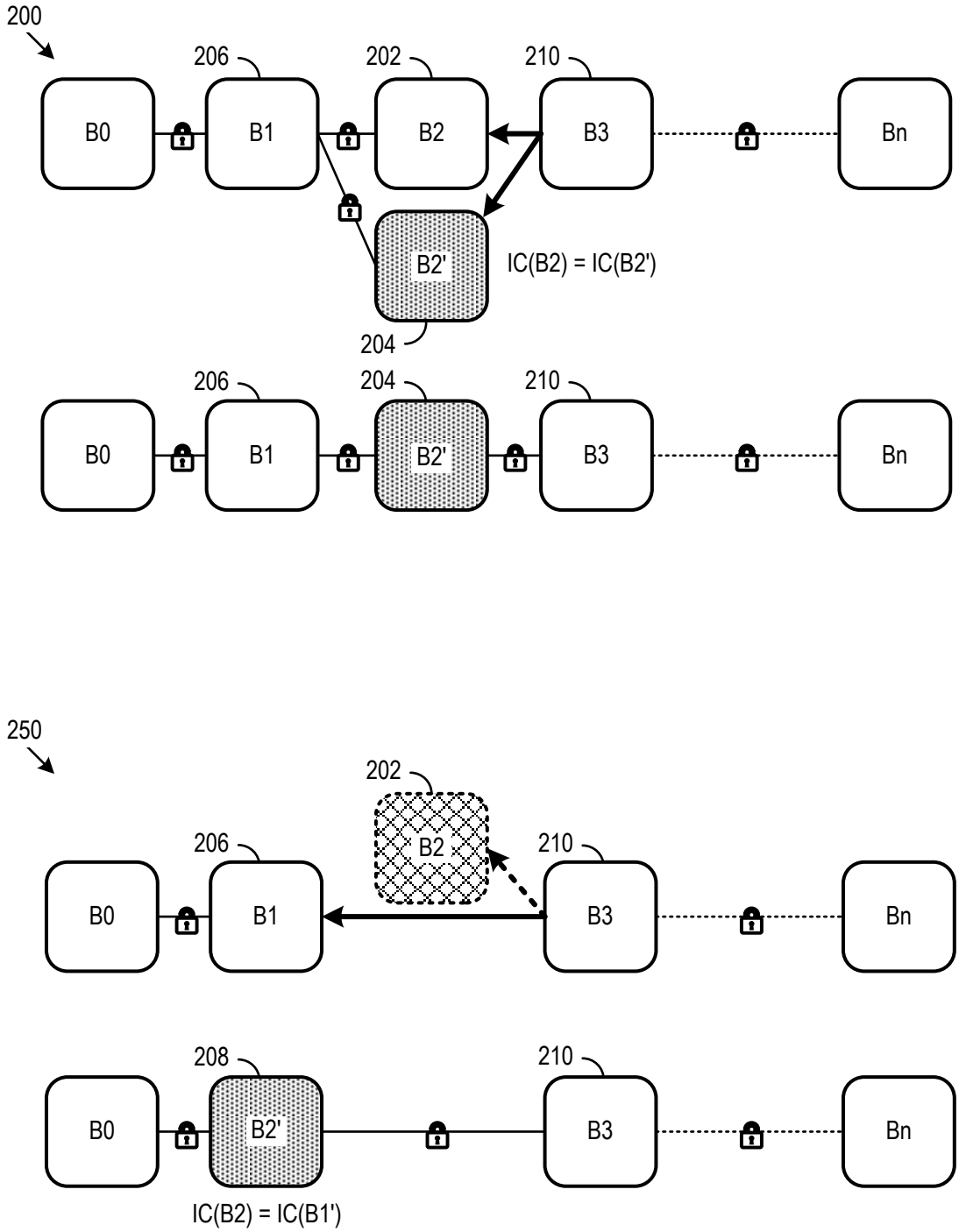
200
206
202
210
B0
B1
B2
B3
Bn
B2'
IC(B2) = IC(B2')
204
206
204
210
B0
B1
B2'
B3
Bn
250
202
206
210
B2
B0
B1
B3
Bn
208
210
B0
B2'
B3
Bn
IC(B2) = IC(B1')

Figure 2

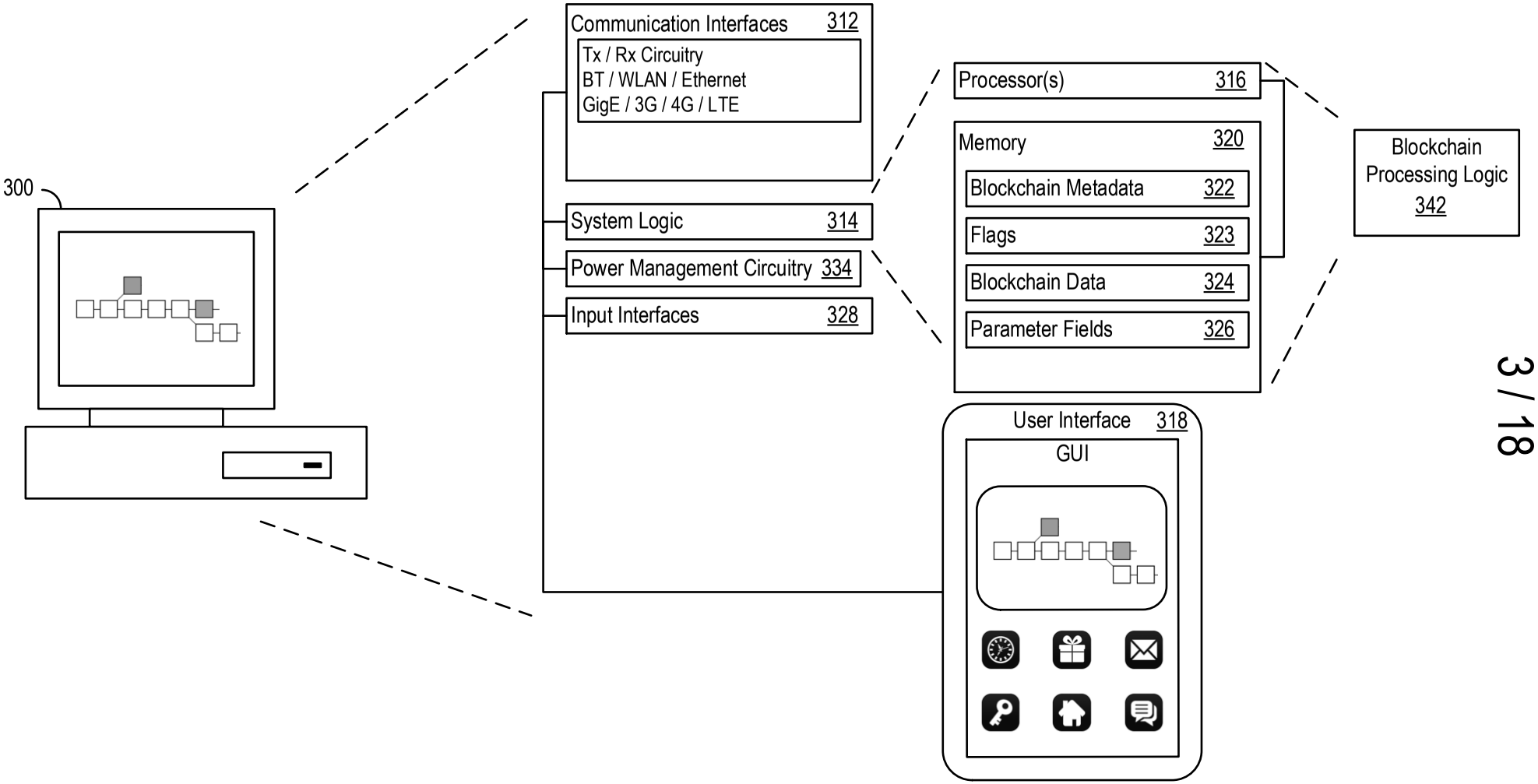
300
Communication Interfaces 312
Tx / Rx Circuitry
BT / WLAN / Ethernet
GigE / 3G / 4G / LTE
System Logic 314
Power Management Circuitry 334
Input Interfaces 328
Processor(s) 316
Memory 320
Blockchain Metadata 322
Flags 323
Blockchain Data 324
Parameter Fields 326
Blockchain Processing Logic 342
User Interface 318
GUI

Figure 3

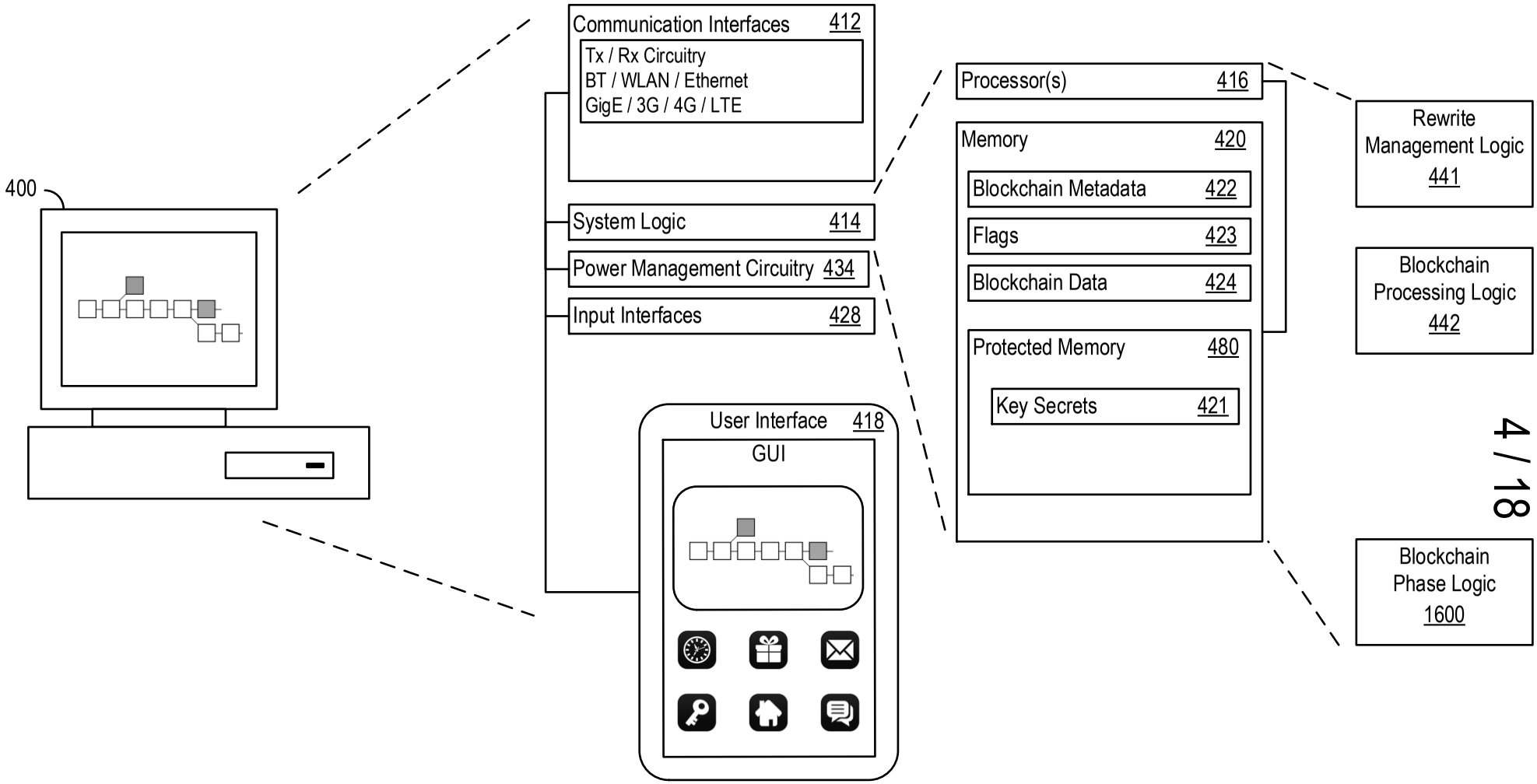
400
Communication Interfaces 412
Tx / Rx Circuitry
BT / WLAN / Ethernet
GigE / 3G / 4G / LTE
System Logic 414
Power Management Circuitry 434
Input Interfaces 428
User Interface 418
GUI
Processor(s) 416
Memory 420
Blockchain Metadata 422
Flags 423
Blockchain Data 424
Protected Memory 480
Key Secrets 421
Rewrite Management Logic 441
Blockchain Processing Logic 442
Blockchain Phase Logic 1600

Figure 4

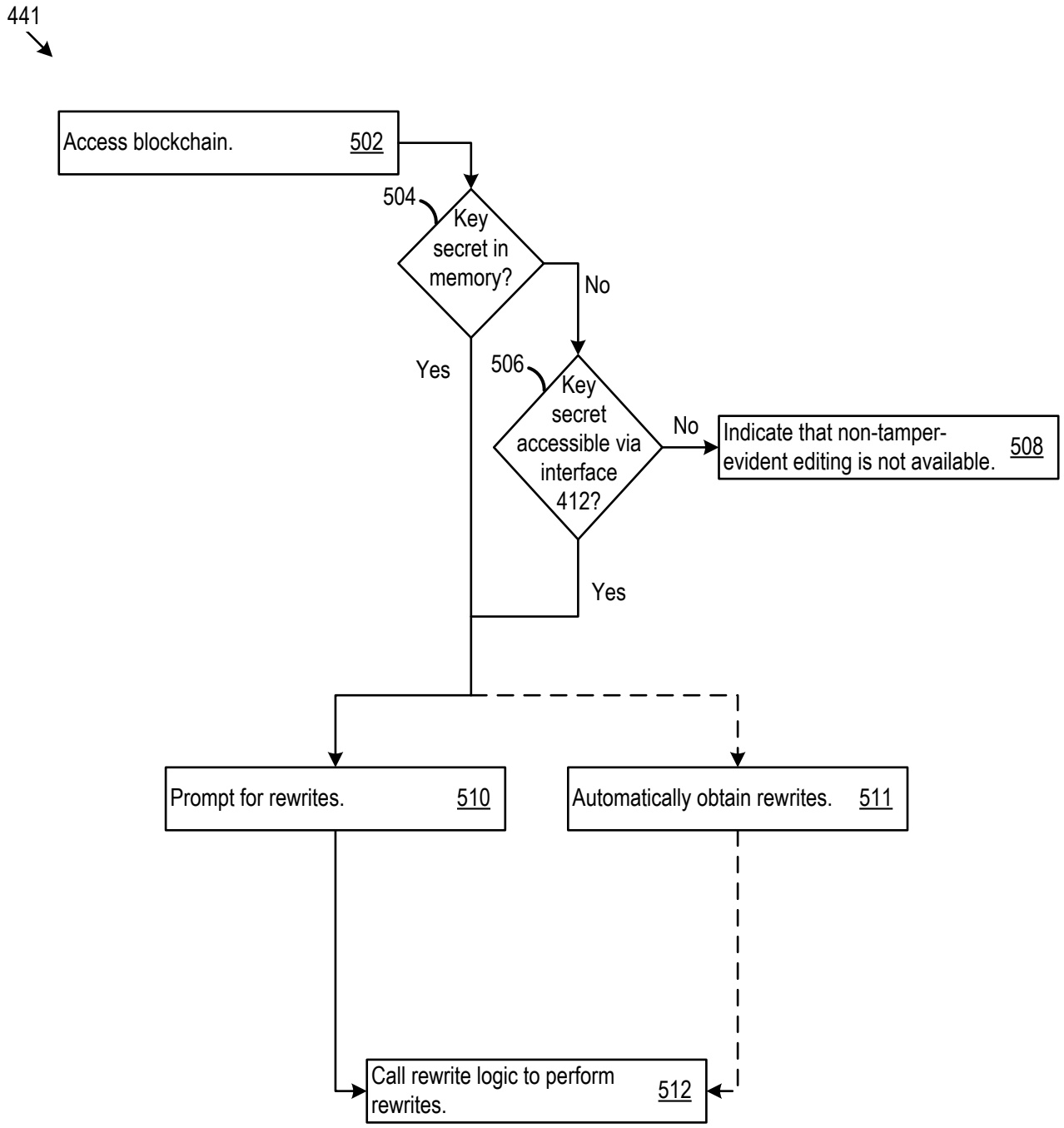
441
Access blockchain. 502
504
Key secret in memory?
No
Yes
506
Key secret accessible via interface 412?
No
Indicate that non-tamper-evident editing is not available. 508
Yes
Prompt for rewrites. 510
Automatically obtain rewrites. 511
Call rewrite logic to perform rewrites. 512

Figure 5

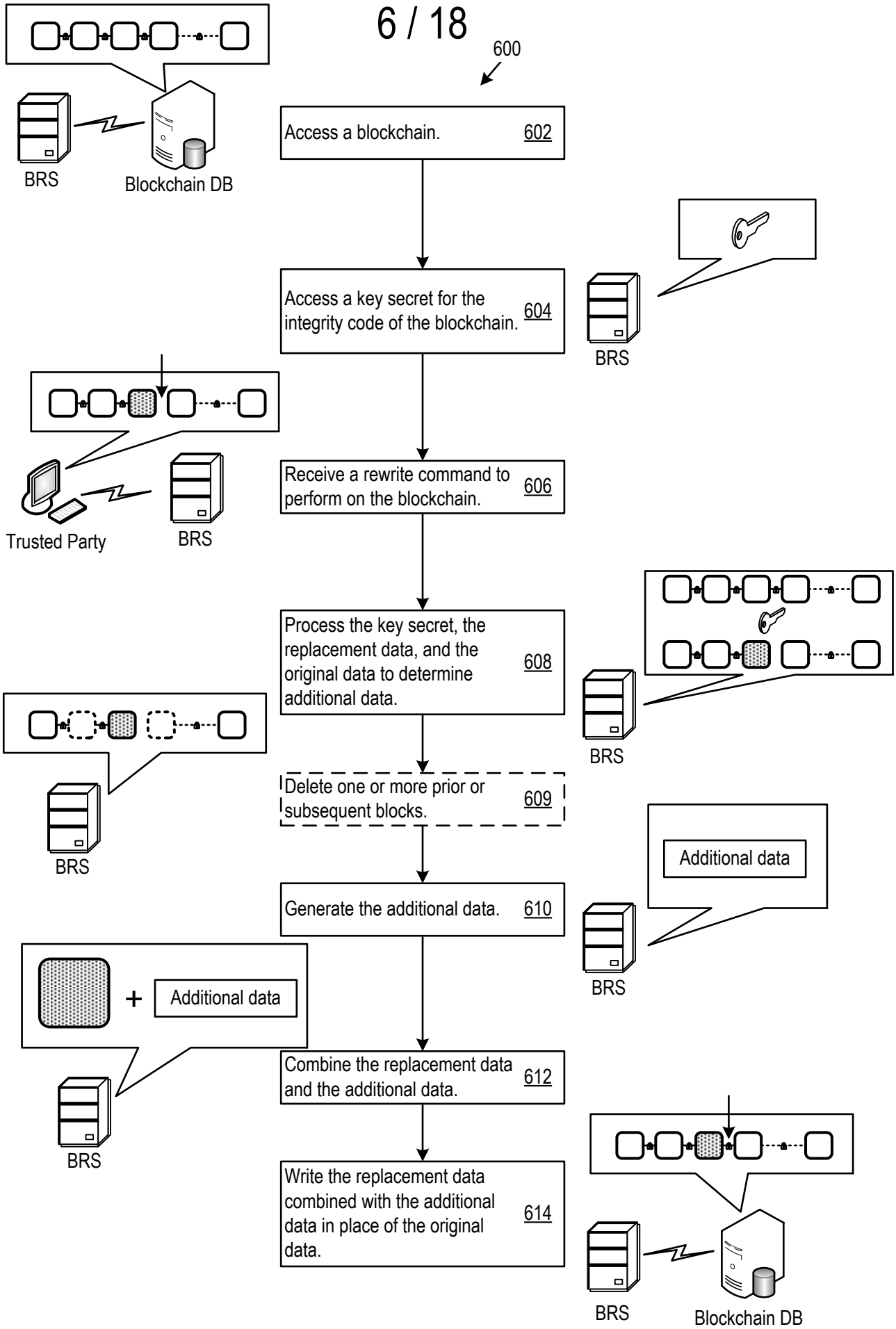
600
Access a blockchain. 602
Access a key secret for the integrity code of the blockchain. 604
Receive a rewrite command to perform on the blockchain. 606
Process the key secret, the replacement data, and the original data to determine additional data. 608
Delete one or more prior or subsequent blocks. 609
Generate the additional data. 610
Combine the replacement data and the additional data. 612
Write the replacement data combined with the additional data in place of the original data. 614
BRS
Blockchain DB
Trusted Party
Additional data

Figure 6

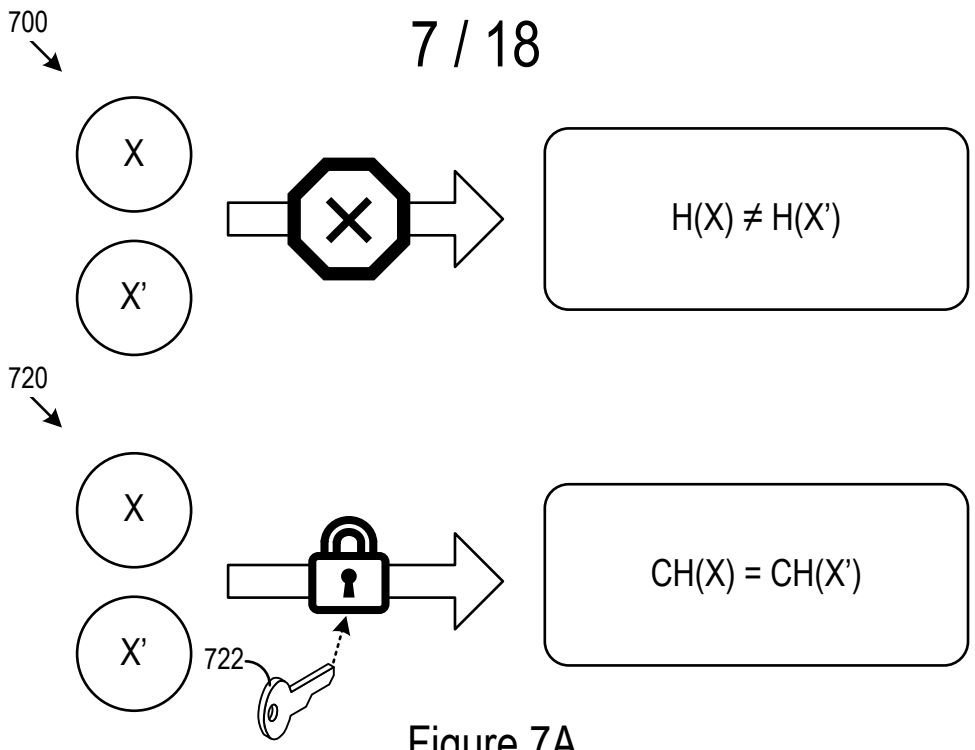

Figure 7A

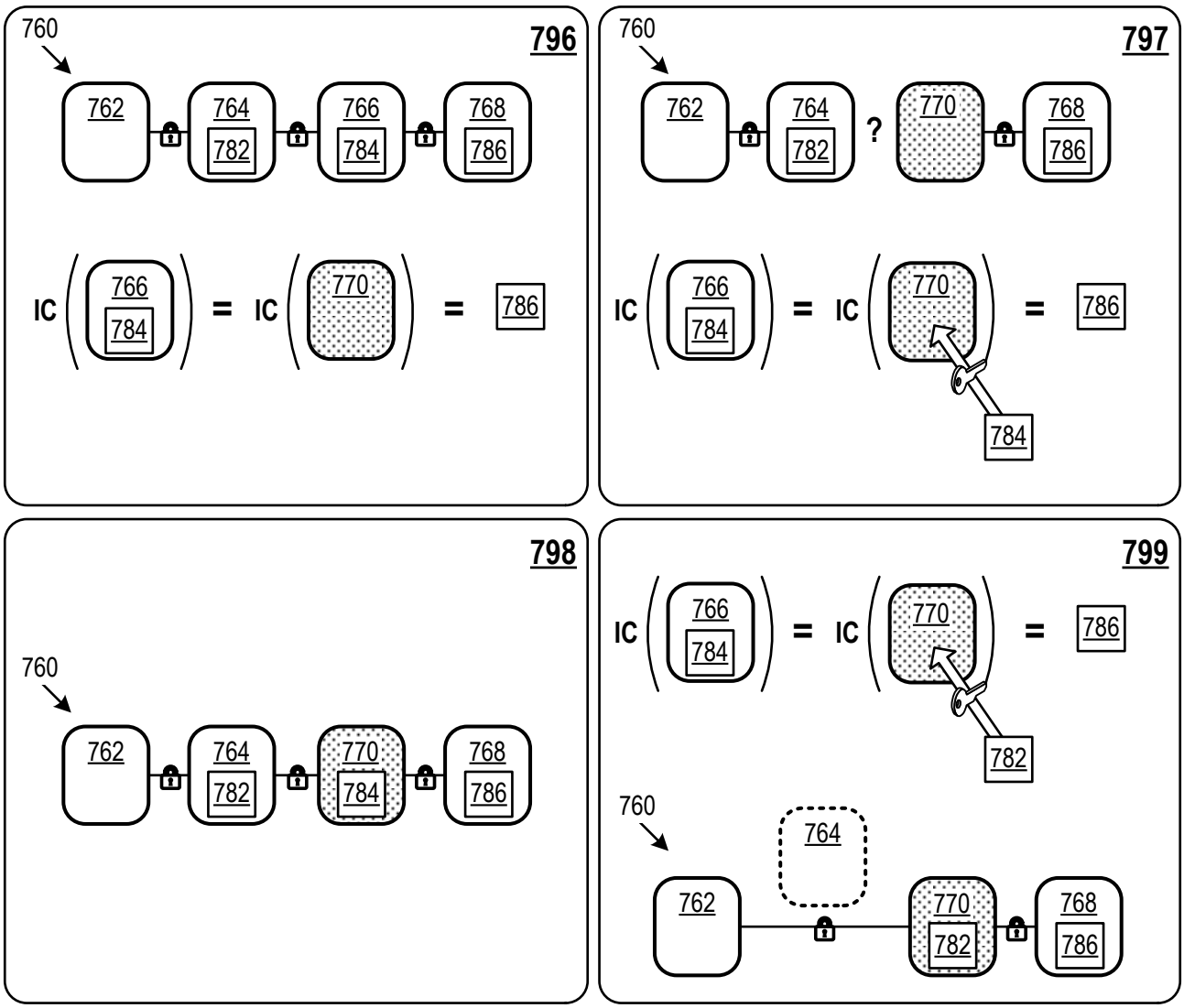

Figure 7B

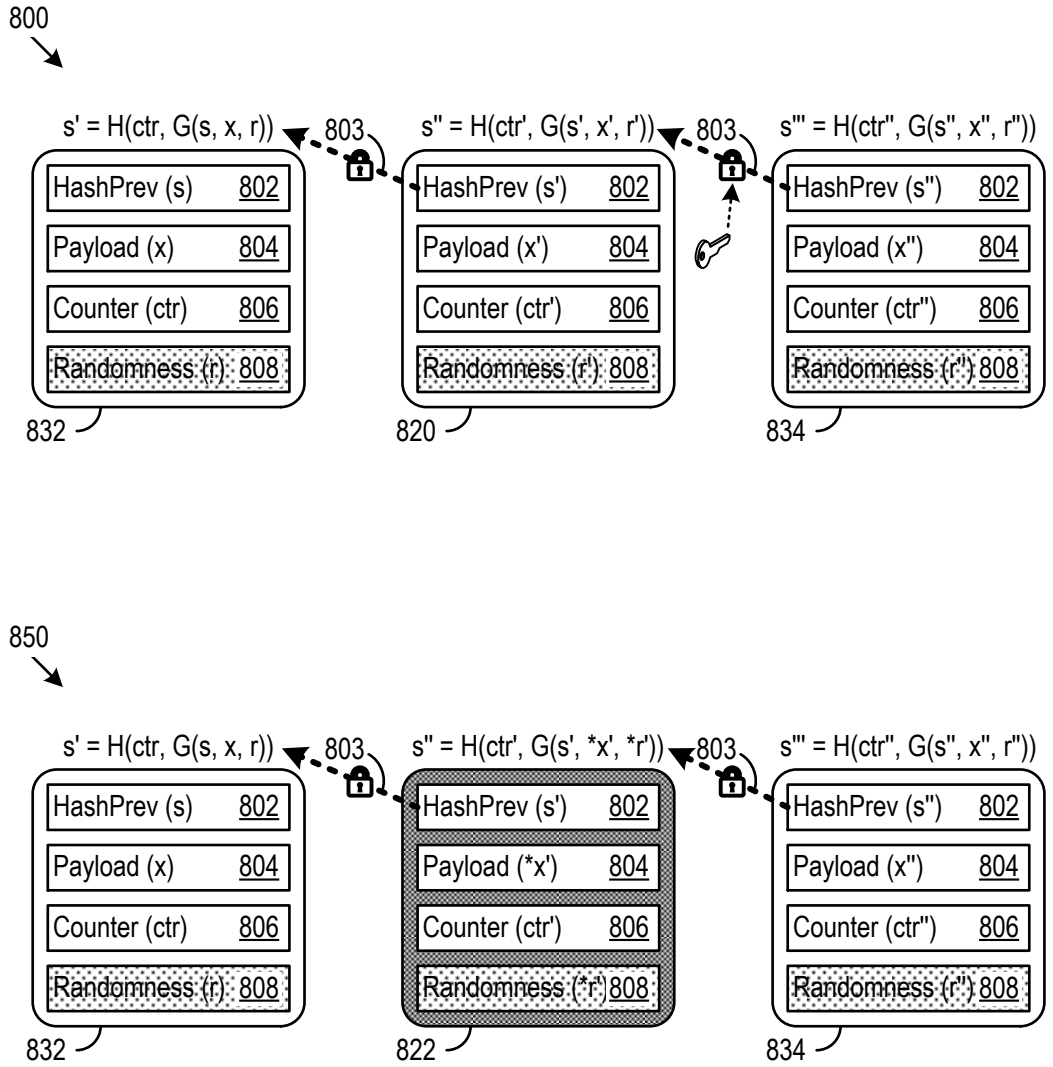
800
s' = H(ctr, G(s, x, r))
803
s'' = H(ctr', G(s', x', r'))
803
s''' = H(ctr'', G(s'', x'', r''))
HashPrev (s) 802
Payload (x) 804
Counter (ctr) 806
Randomness (r) 808
832
HashPrev (s') 802
Payload (x') 804
Counter (ctr') 806
Randomness (r') 808
820
HashPrev (s'') 802
Payload (x'') 804
Counter (ctr'') 806
Randomness (r'') 808
834
850
s' = H(ctr, G(s, x, r))
803
s'' = H(ctr', G(s', *x', *r'))
803
s''' = H(ctr'', G(s'', x'', r''))
HashPrev (s) 802
Payload (x) 804
Counter (ctr) 806
Randomness (r) 808
832
HashPrev (s') 802
Payload (*x') 804
Counter (ctr') 806
Randomness (*r') 808
822
HashPrev (s'') 802
Payload (x'') 804
Counter (ctr'') 806
Randomness (r'') 808
834

Figure 8

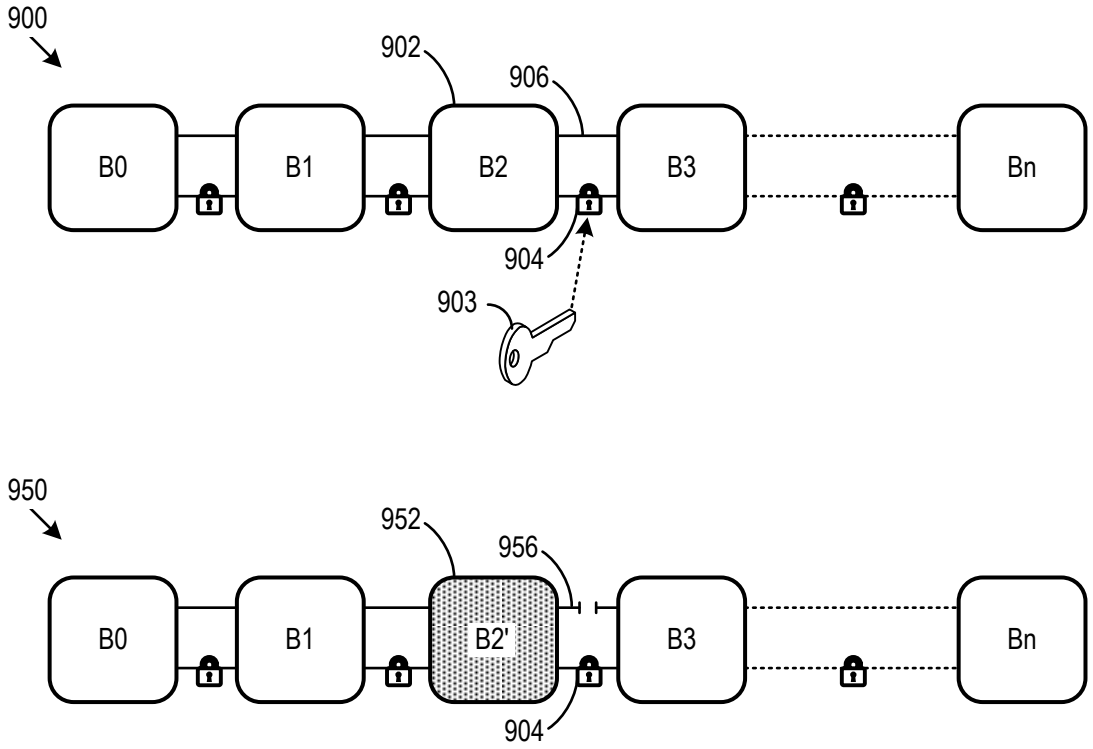

Figure 9

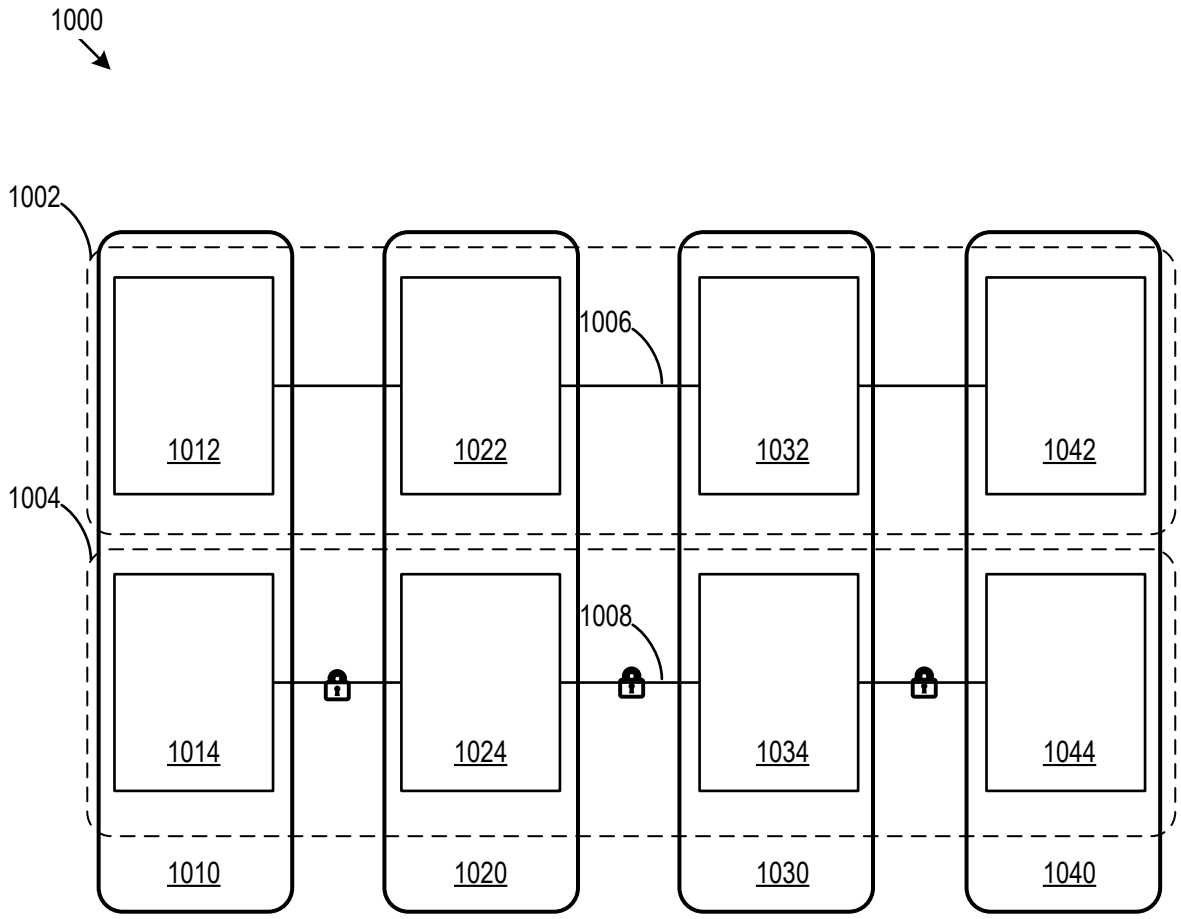
1000
1002
1004
1006
1008
1012
1022
1032
1042
1014
1024
1034
1044
1010
1020
1030
1040

Figure 10

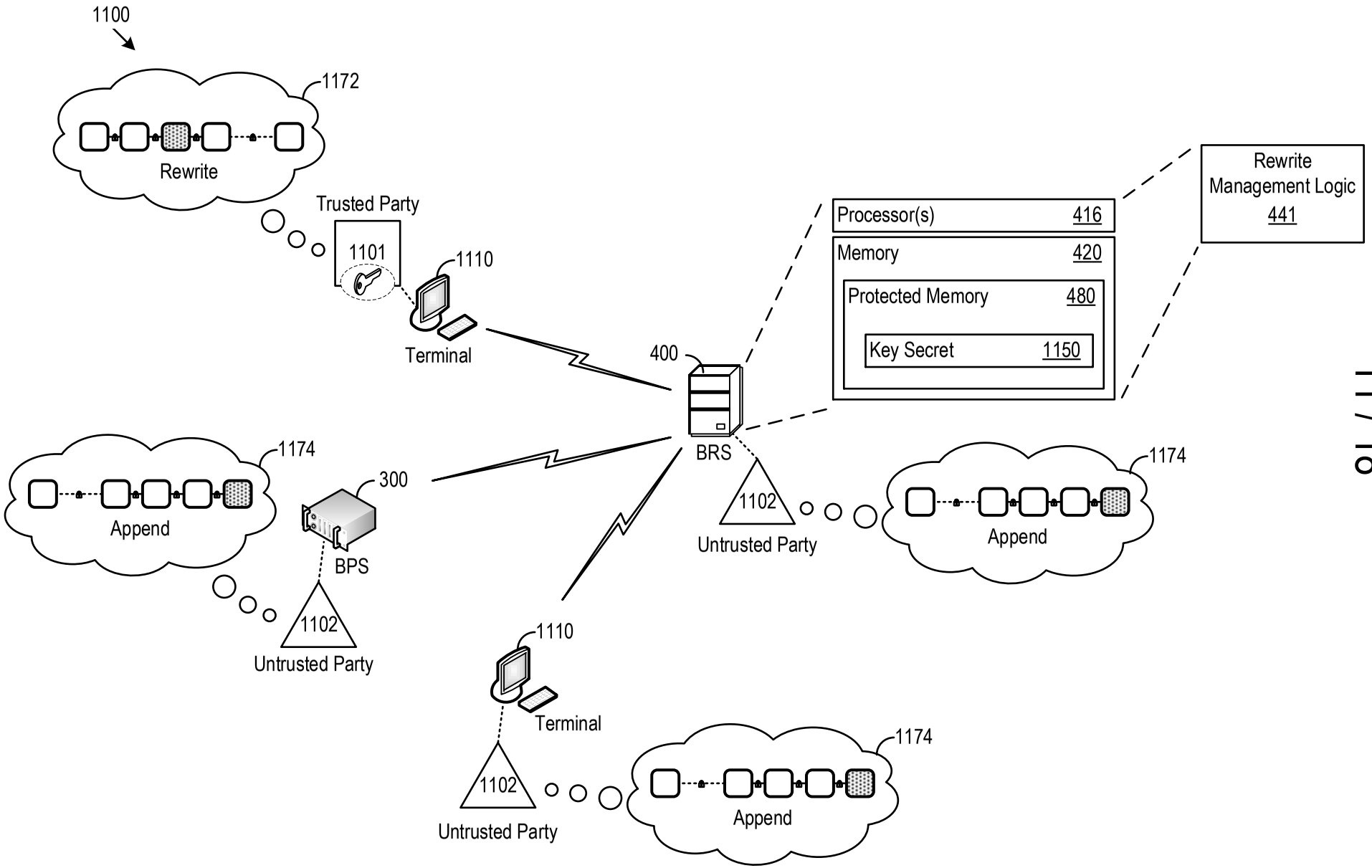
1100
1172
Rewrite
Trusted Party
1101
1110
Terminal
400
BRS
Processor(s) 416
Memory 420
Protected Memory 480
Key Secret 1150
Rewrite Management Logic 441
1174
Append
300
BPS
1102
Untrusted Party
1174
Append
1102
Untrusted Party
1110
Terminal
1102
Untrusted Party
1174
Append

Figure 11

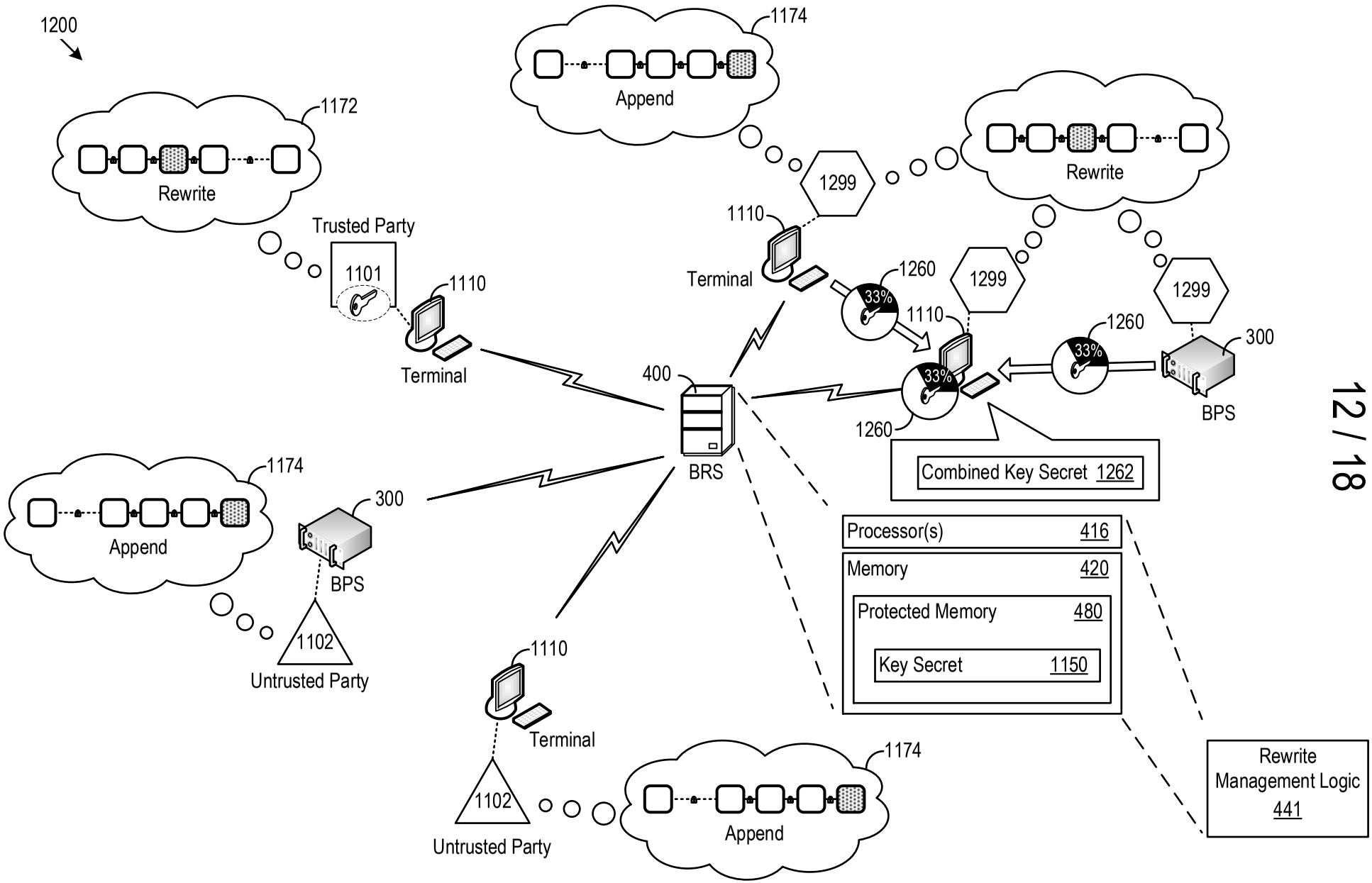
1200
1172
Rewrite
Trusted Party
1101
1110
Terminal
1174
Append
1299
Rewrite
1110
Terminal
1260
33%
1110
1299
1260
33%
1299
300
BPS
400
BRS
1260
Combined Key Secret 1262
1174
Append
300
BPS
1102
Untrusted Party
Processor(s) 416
Memory 420
Protected Memory 480
Key Secret 1150
1110
Terminal
1102
Untrusted Party
1174
Append
Rewrite Management Logic 441

Figure 12

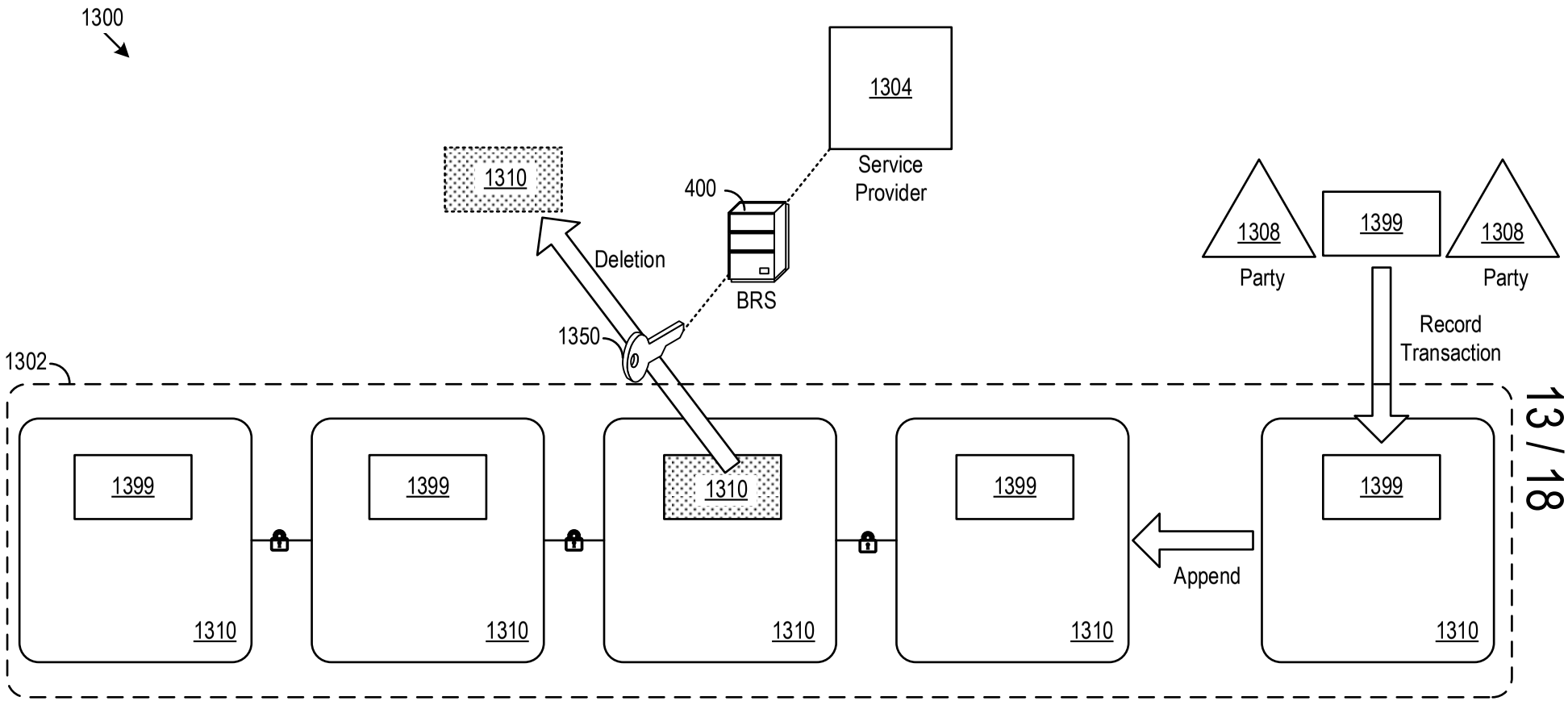
1300
1304
Service Provider
400
BRS
1310
Deletion
1350
1302
1308
Party
1399
1308
Party
Record Transaction
1399
1310
1399
1310
1399
1310
1399
1310
Append

Figure 13

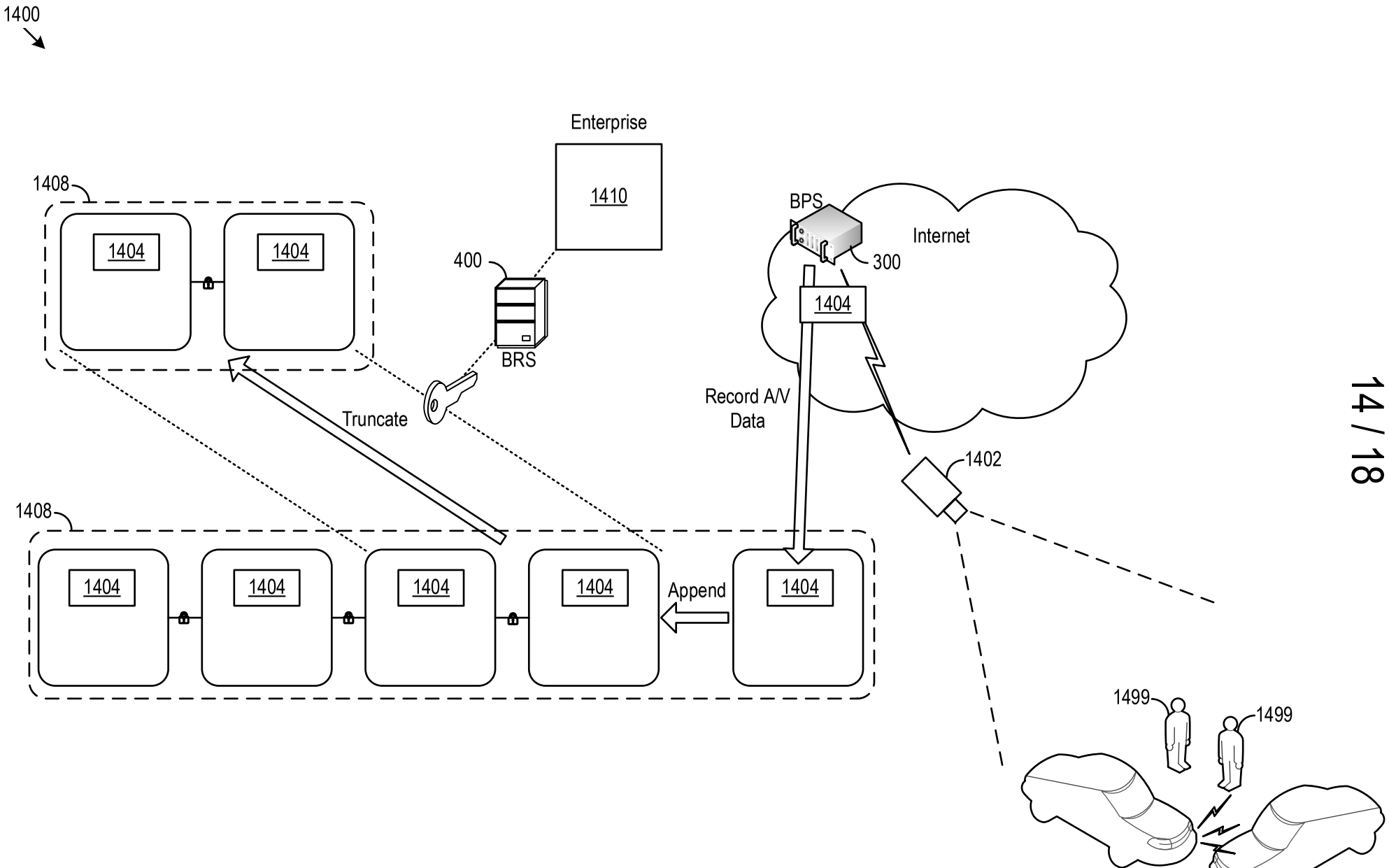
1400
Enterprise
1410
1408
1404
1404
400
BRS
BPS
Internet
300
1404
Truncate
Record A/V
Data
1402
1408
1404
1404
1404
1404
Append
1404
1499
1499

Figure 14

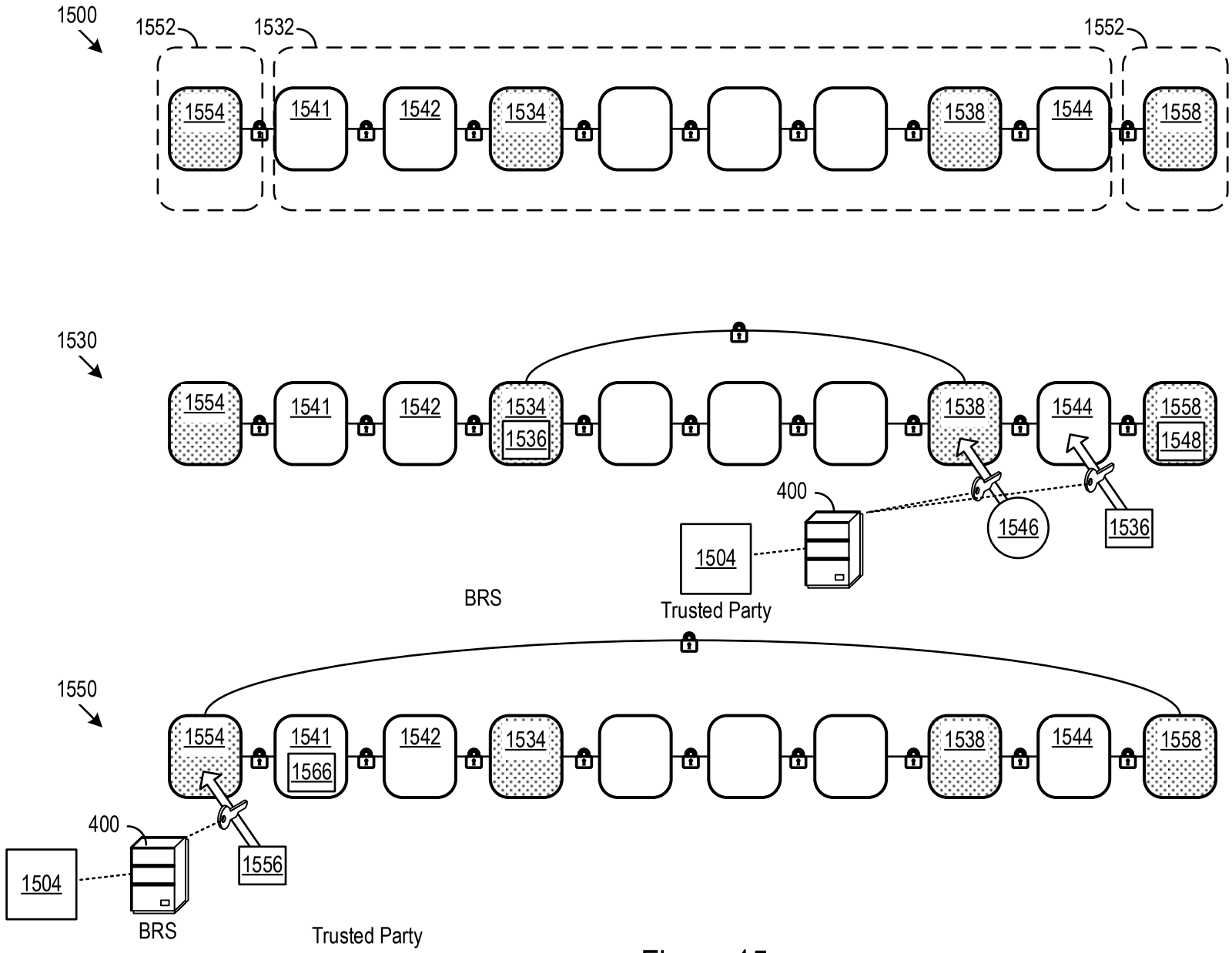
1500
1552
1532
1552
1554
1541
1542
1534
1538
1544
1558
1530
1554
1541
1542
1534
1536
1538
1544
1558
1548
400
1546
1536
1504
BRS
Trusted Party
1550
1554
1541
1566
1542
1534
1538
1544
1558
400
1504
1556
BRS
Trusted Party

Figure 15

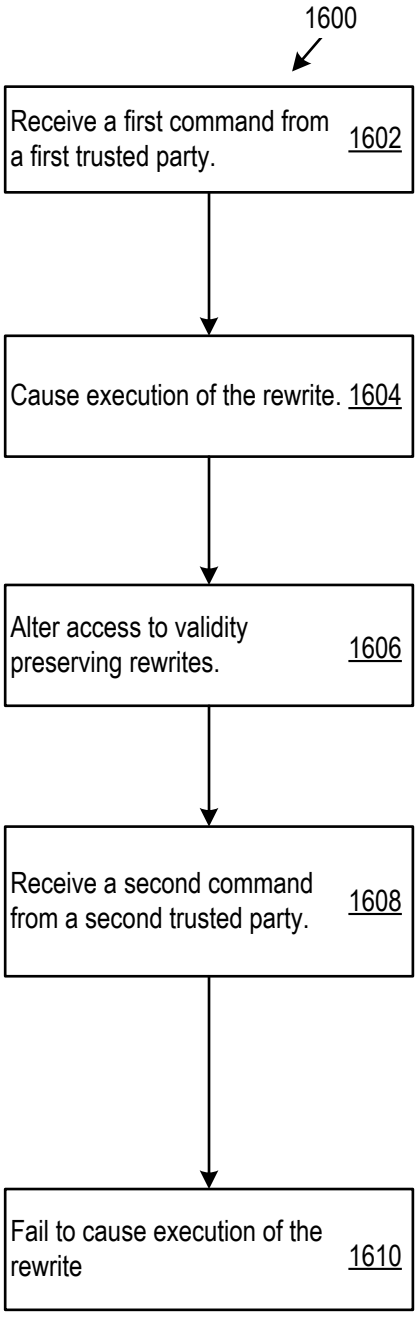
1600
Receive a first command from a first trusted party. 1602
Cause execution of the rewrite. 1604
Alter access to validity preserving rewrites. 1606
Receive a second command from a second trusted party. 1608
Fail to cause execution of the rewrite 1610

Figure 16

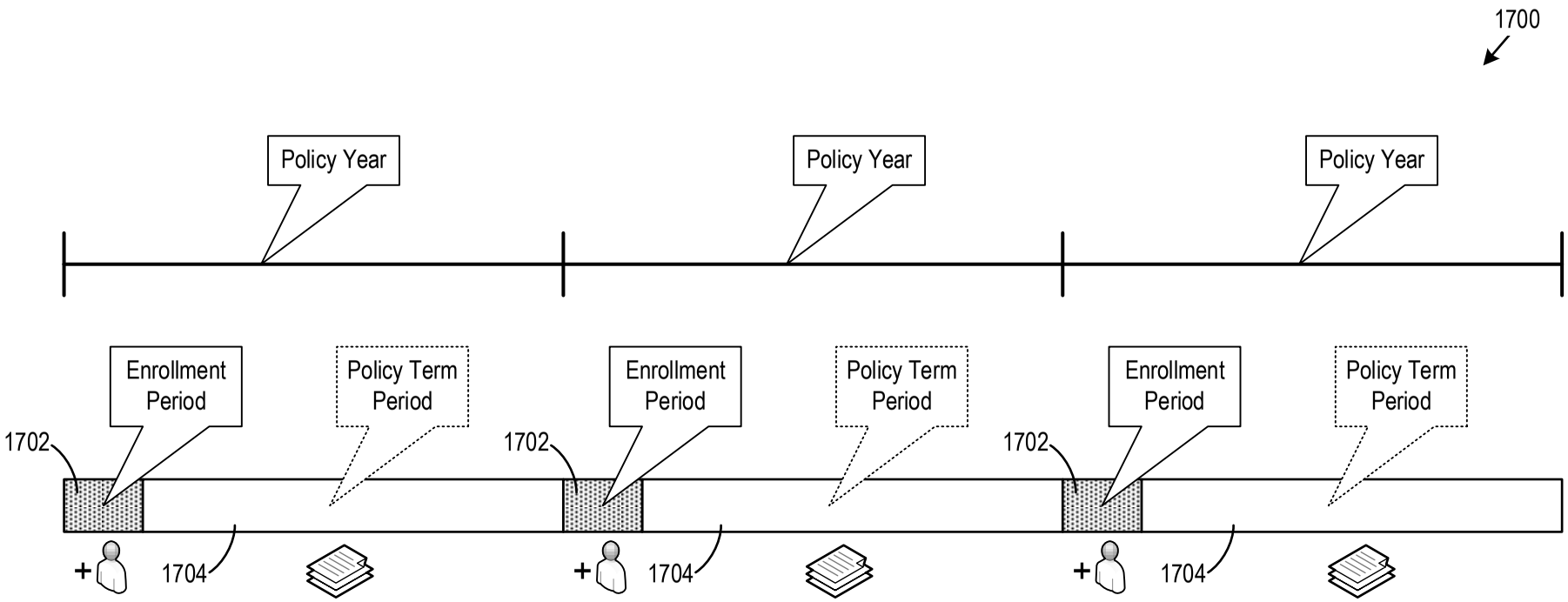
1700
Policy Year
Policy Year
Policy Year
Enrollment Period
Policy Term Period
Enrollment Period
Policy Term Period
Enrollment Period
Policy Term Period
1702
1702
1702
1704
1704
1704

Figure 17

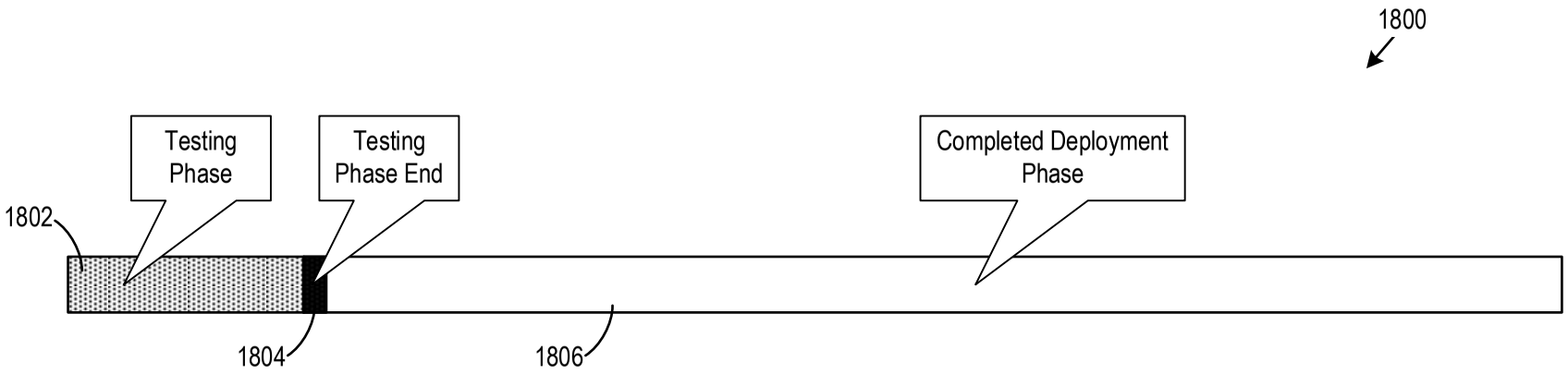
1800
Testing Phase
Testing Phase End
Completed Deployment Phase
1802
1804
1806

Figure 18