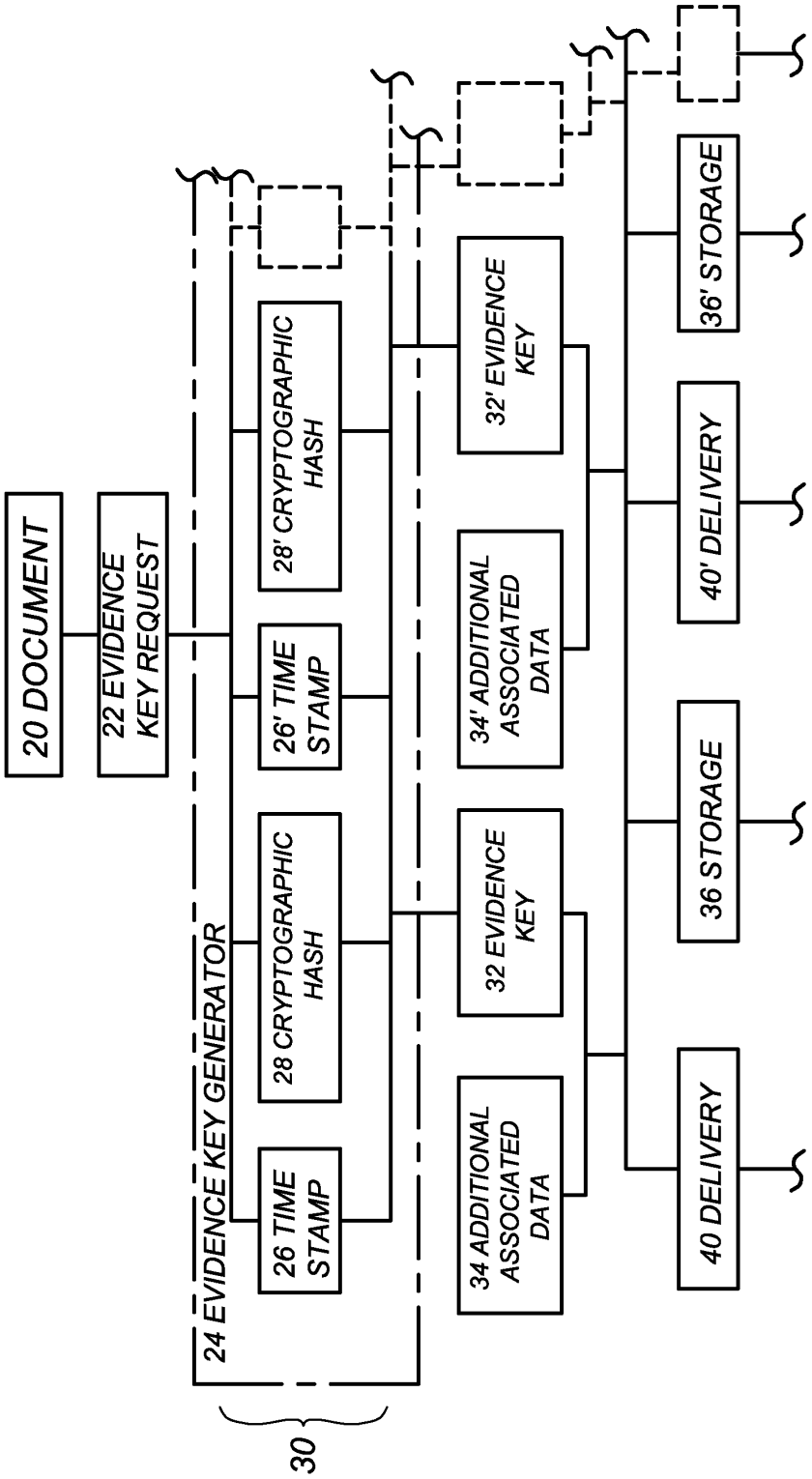

20 DOCUMENT
22 EVIDENCE KEY REQUEST
24 EVIDENCE KEY GENERATOR
26 TIME STAMP
28 CRYPTOGRAPHIC HASH
34 ADDITIONAL ASSOCIATED DATA
32 EVIDENCE KEY
40 DELIVERY
36 STORAGE
26' TIME STAMP
28' CRYPTOGRAPHIC HASH
34' ADDITIONAL ASSOCIATED DATA
32' EVIDENCE KEY
40' DELIVERY
36' STORAGE
30

Fig. 1

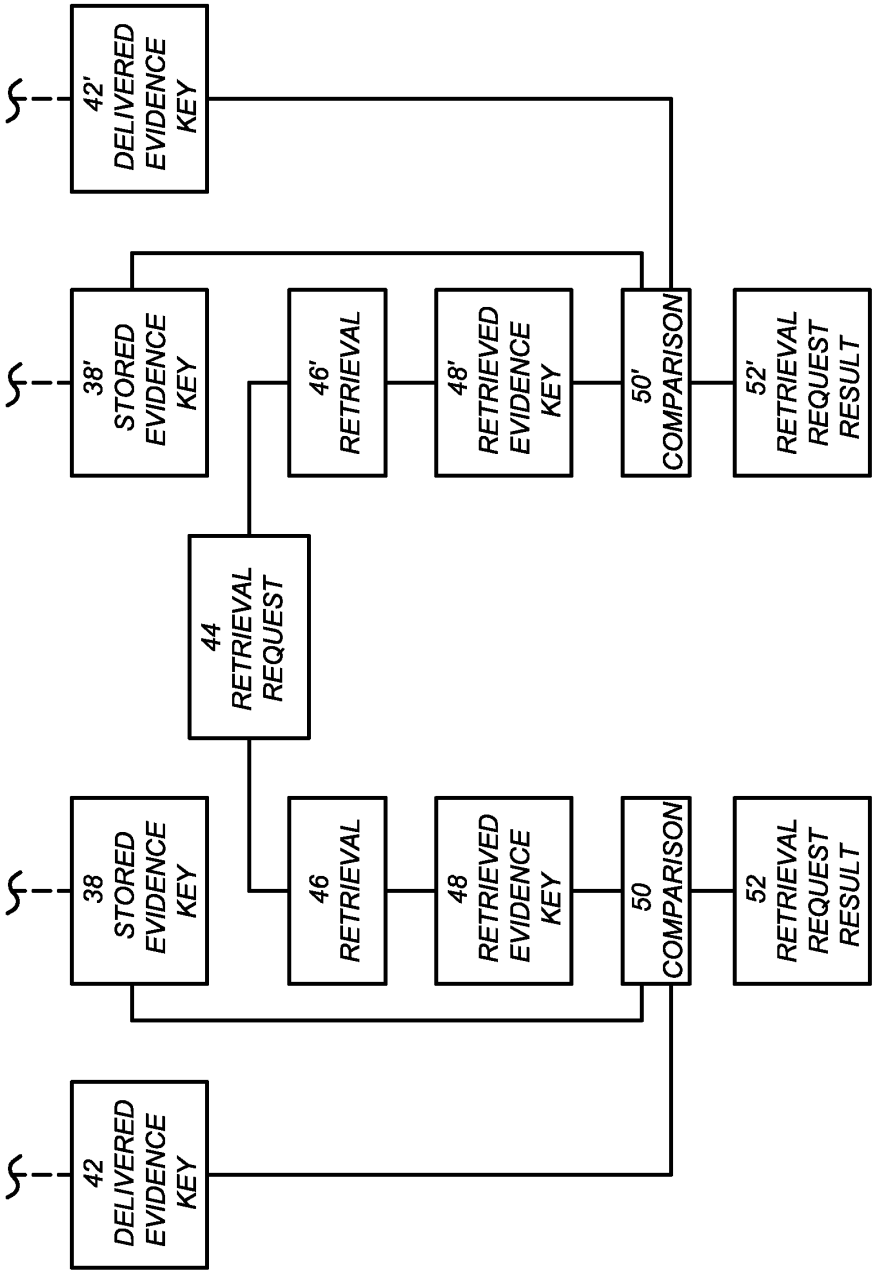

42' DELIVERED EVIDENCE KEY
38' STORED EVIDENCE KEY
46' RETRIEVAL
48' RETRIEVED EVIDENCE KEY
50' COMPARISON
52' RETRIEVAL REQUEST RESULT
44 RETRIEVAL REQUEST
38 STORED EVIDENCE KEY
46 RETRIEVAL
48 RETRIEVED EVIDENCE KEY
50 COMPARISON
52 RETRIEVAL REQUEST RESULT
42 DELIVERED EVIDENCE KEY

Fig. 2

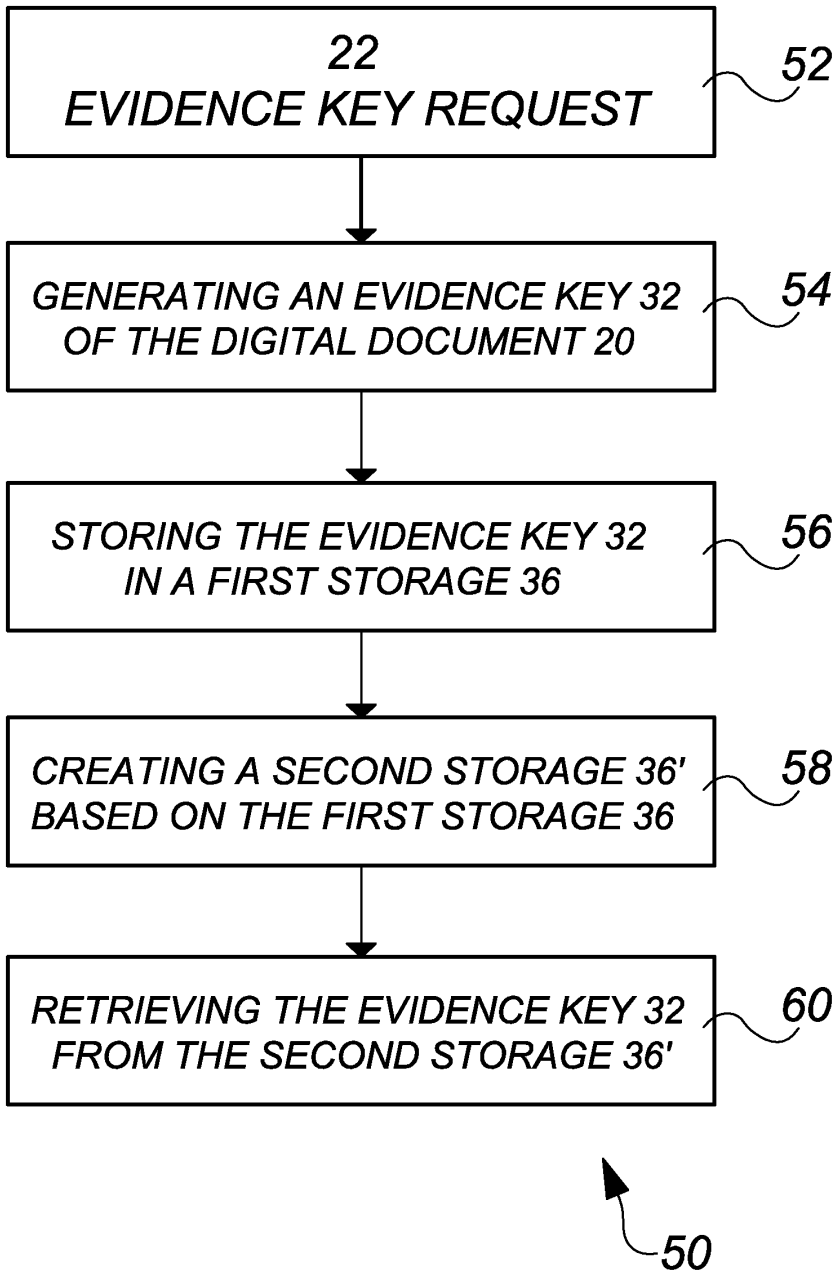

22
EVIDENCE KEY REQUEST
52
GENERATING AN EVIDENCE KEY 32 OF THE DIGITAL DOCUMENT 20
54
STORING THE EVIDENCE KEY 32 IN A FIRST STORAGE 36
56
CREATING A SECOND STORAGE 36' BASED ON THE FIRST STORAGE 36
58
RETRIEVING THE EVIDENCE KEY 32 FROM THE SECOND STORAGE 36'
60
50

Fig. 3

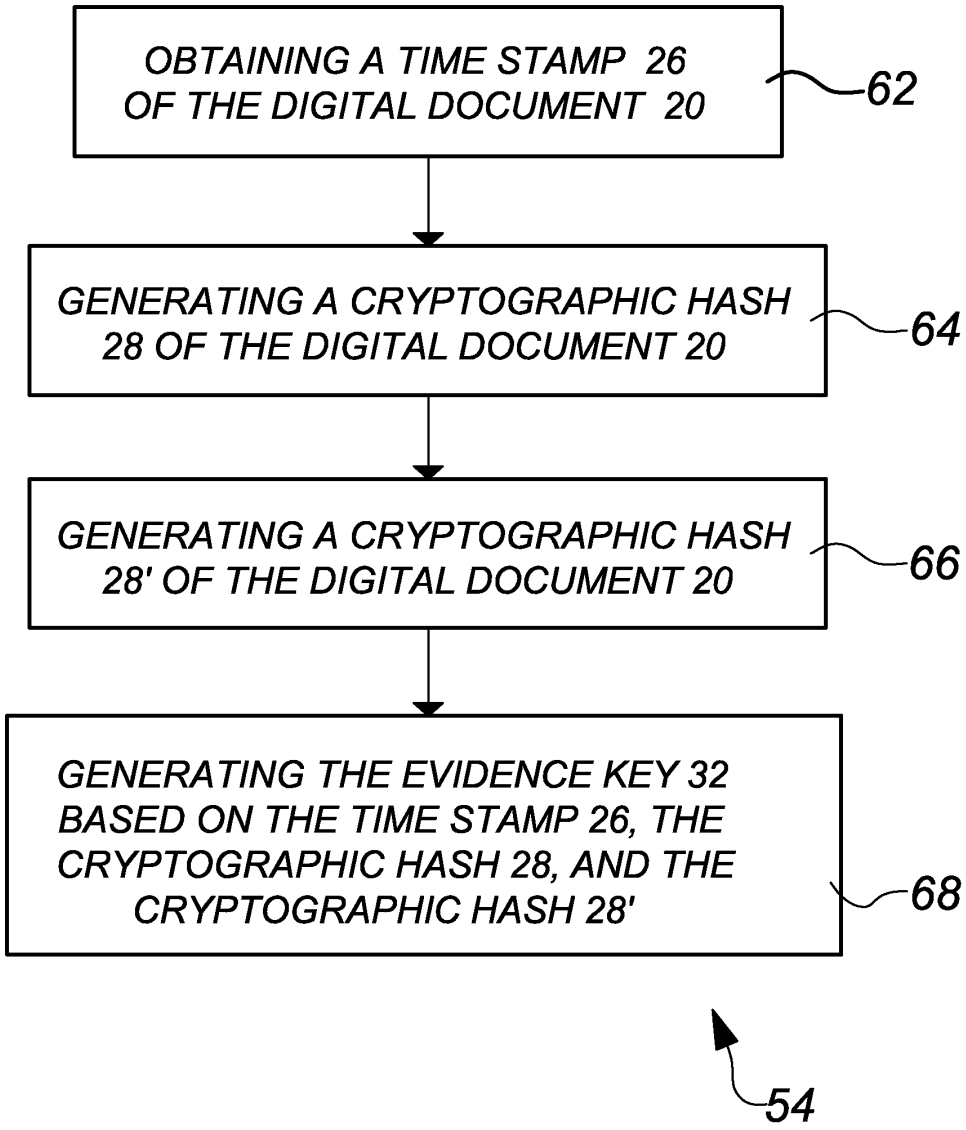

OBTAINING A TIME STAMP 26 OF THE DIGITAL DOCUMENT 20
62
GENERATING A CRYPTOGRAPHIC HASH 28 OF THE DIGITAL DOCUMENT 20
64
GENERATING A CRYPTOGRAPHIC HASH 28' OF THE DIGITAL DOCUMENT 20
66
GENERATING THE EVIDENCE KEY 32 BASED ON THE TIME STAMP 26, THE CRYPTOGRAPHIC HASH 28, AND THE CRYPTOGRAPHIC HASH 28'
68
54

Fig. 4

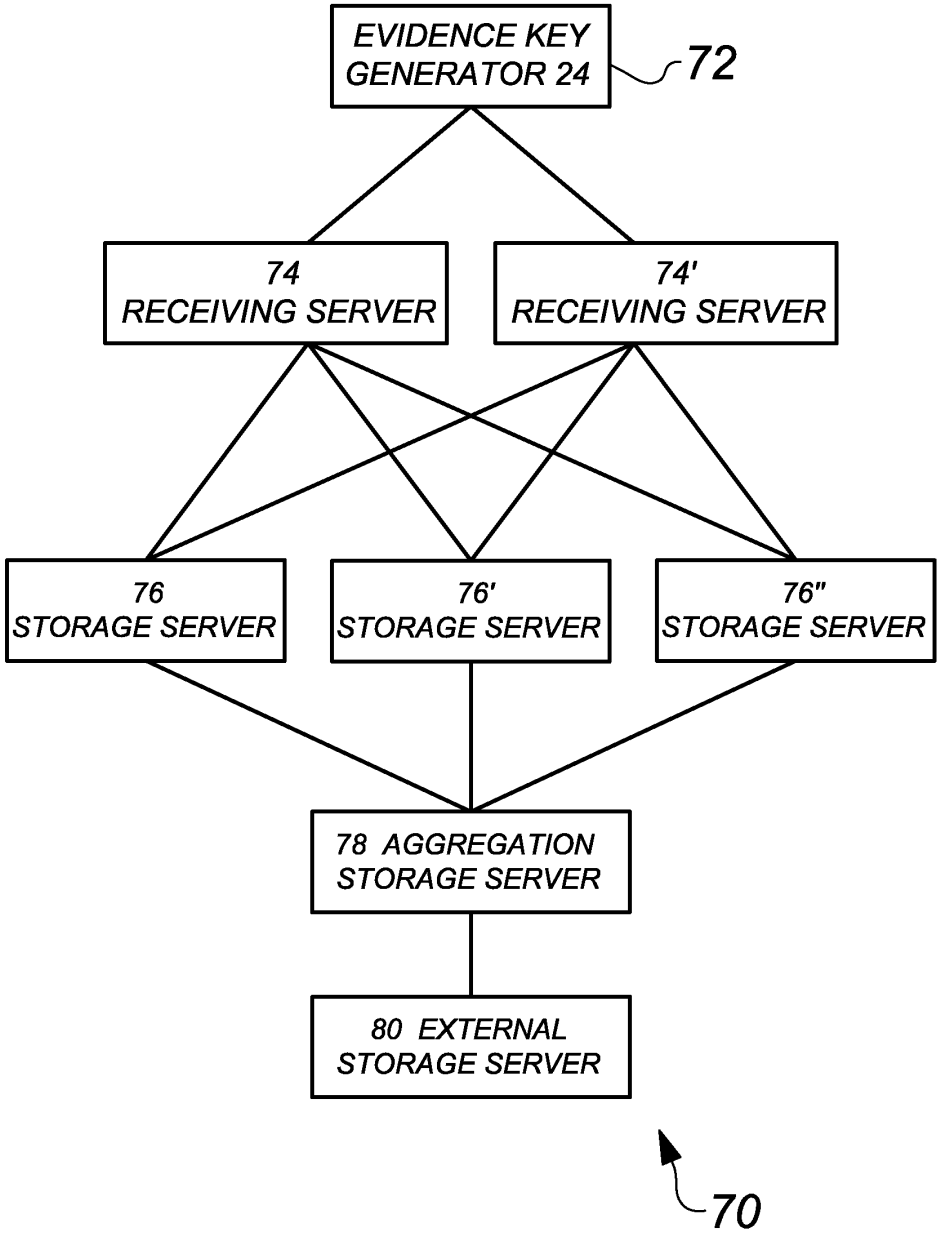

EVIDENCE KEY GENERATOR 24
72
74 RECEIVING SERVER
74' RECEIVING SERVER
76 STORAGE SERVER
76' STORAGE SERVER
76" STORAGE SERVER
78 AGGREGATION STORAGE SERVER
80 EXTERNAL STORAGE SERVER
70

Fig. 5

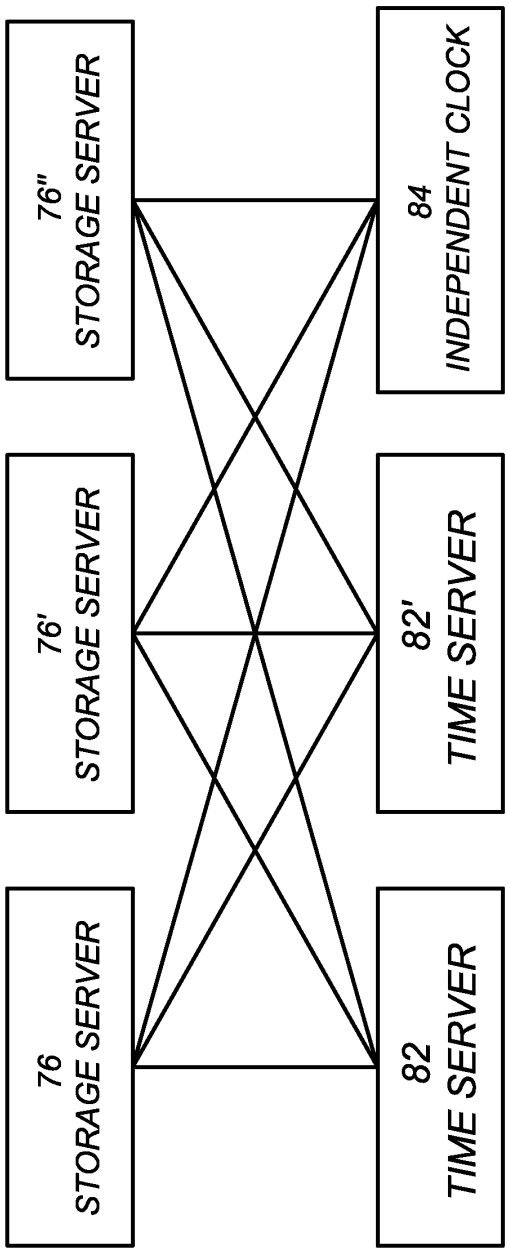

76''
STORAGE SERVER
76'
STORAGE SERVER
76
STORAGE SERVER
84
INDEPENDENT CLOCK
82'
TIME SERVER
82
TIME SERVER

Fig. 6

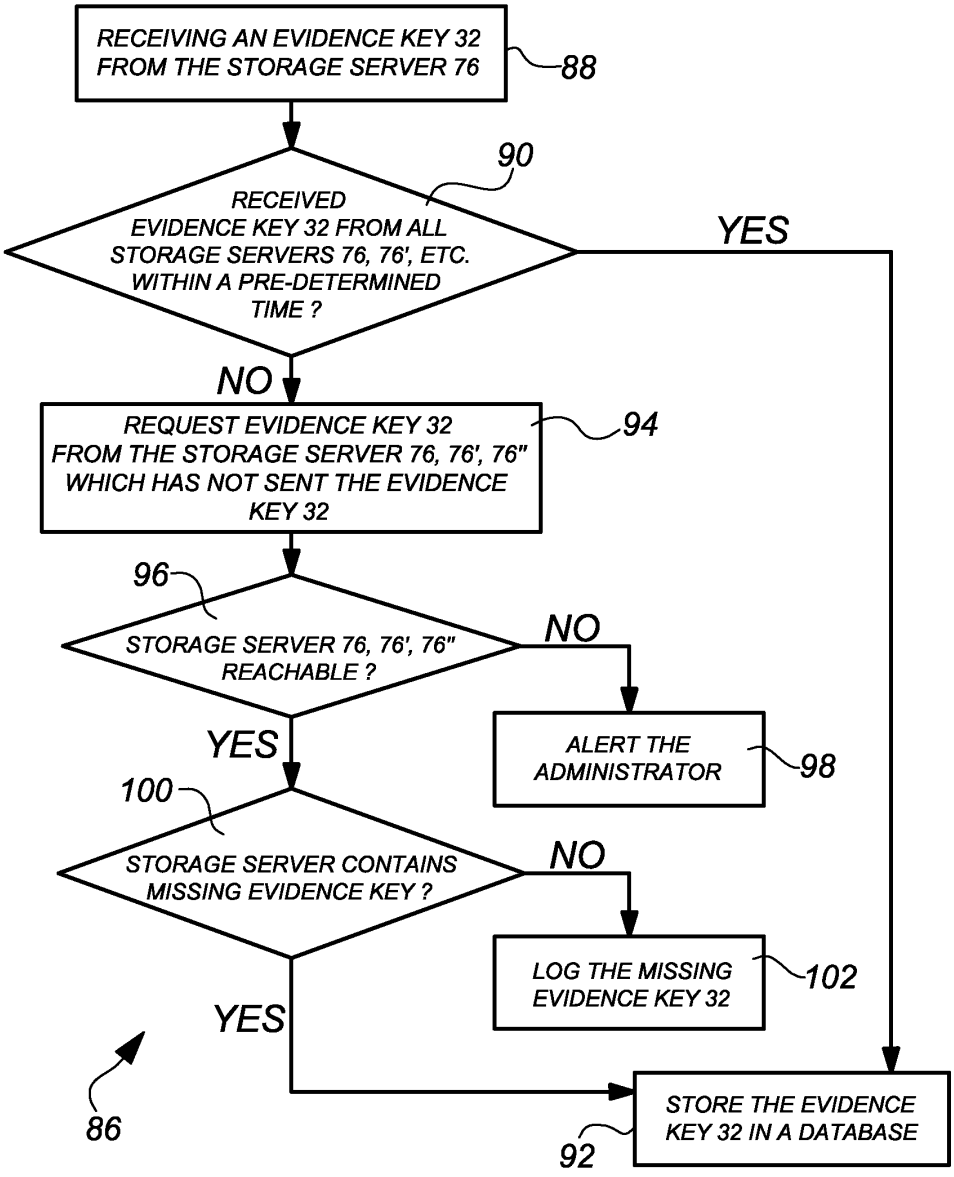

RECEIVING AN EVIDENCE KEY 32 FROM THE STORAGE SERVER 76
88
90
RECEIVED EVIDENCE KEY 32 FROM ALL STORAGE SERVERS 76, 76', ETC. WITHIN A PRE-DETERMINED TIME ?
YES
NO
REQUEST EVIDENCE KEY 32 FROM THE STORAGE SERVER 76, 76', 76" WHICH HAS NOT SENT THE EVIDENCE KEY 32
94
96
STORAGE SERVER 76, 76', 76" REACHABLE ?
NO
YES
ALERT THE ADMINISTRATOR
98
100
STORAGE SERVER CONTAINS MISSING EVIDENCE KEY ?
NO
YES
LOG THE MISSING EVIDENCE KEY 32
102
86
STORE THE EVIDENCE KEY 32 IN A DATABASE
92

Fig. 7

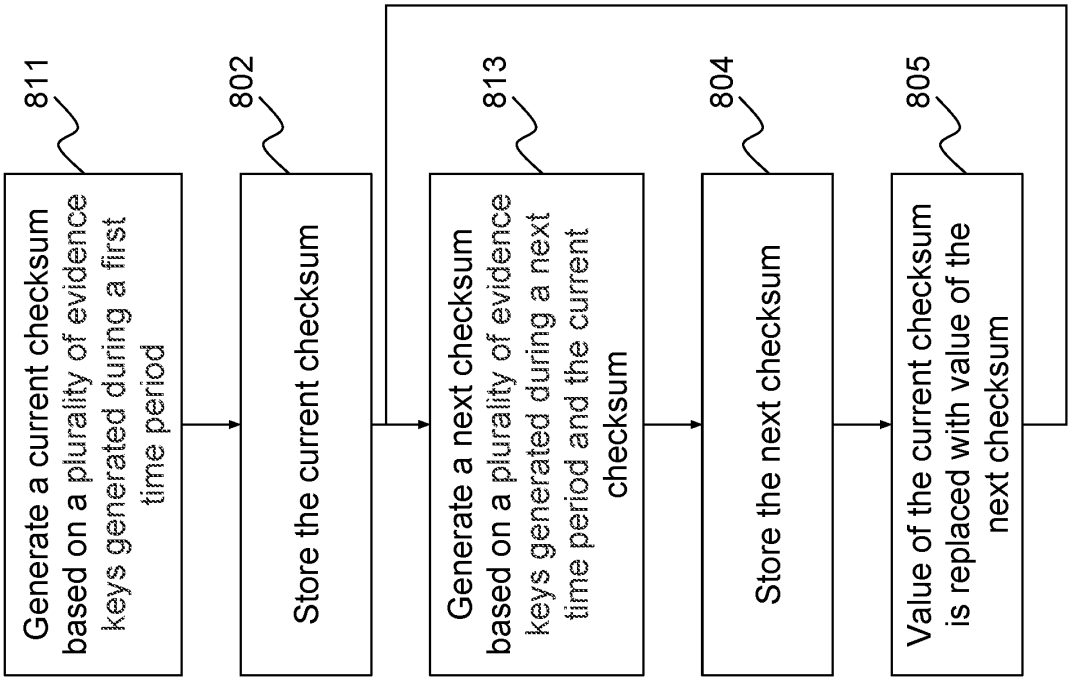

811
Generate a current checksum based on a plurality of evidence keys generated during a first time period
802
Store the current checksum
813
Generate a next checksum based on a plurality of evidence keys generated during a next time period and the current checksum
804
Store the next checksum
805
Value of the current checksum is replaced with value of the next checksum

Fig. 8B

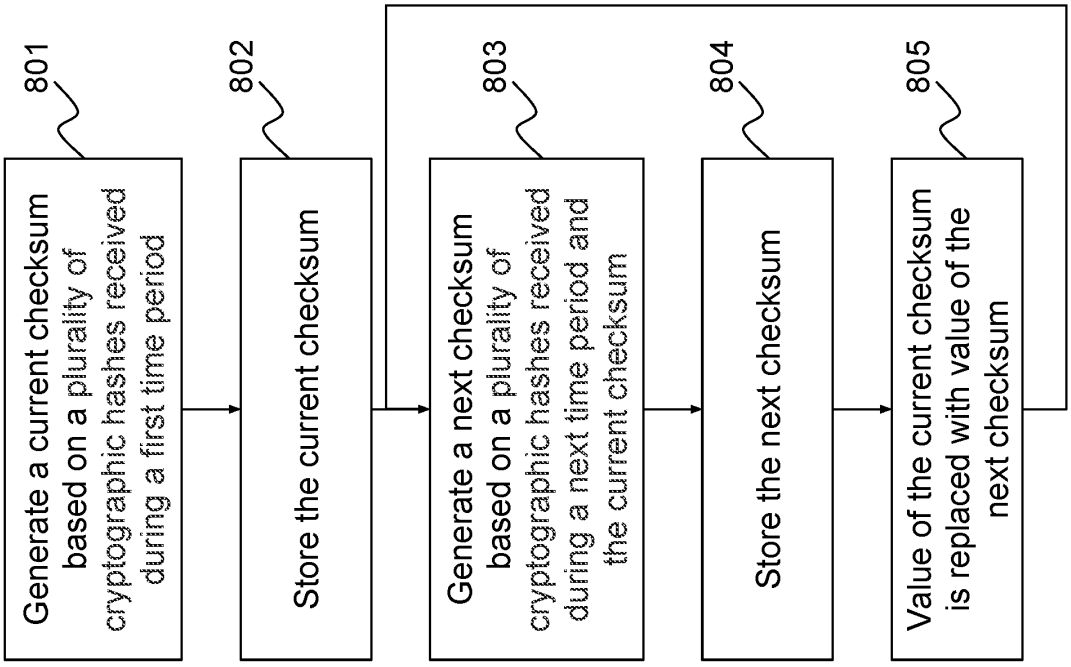

801
Generate a current checksum based on a plurality of cryptographic hashes received during a first time period
802
Store the current checksum
803
Generate a next checksum based on a plurality of cryptographic hashes received during a next time period and the current checksum
804
Store the next checksum
805
Value of the current checksum is replaced with value of the next checksum

Fig. 8A

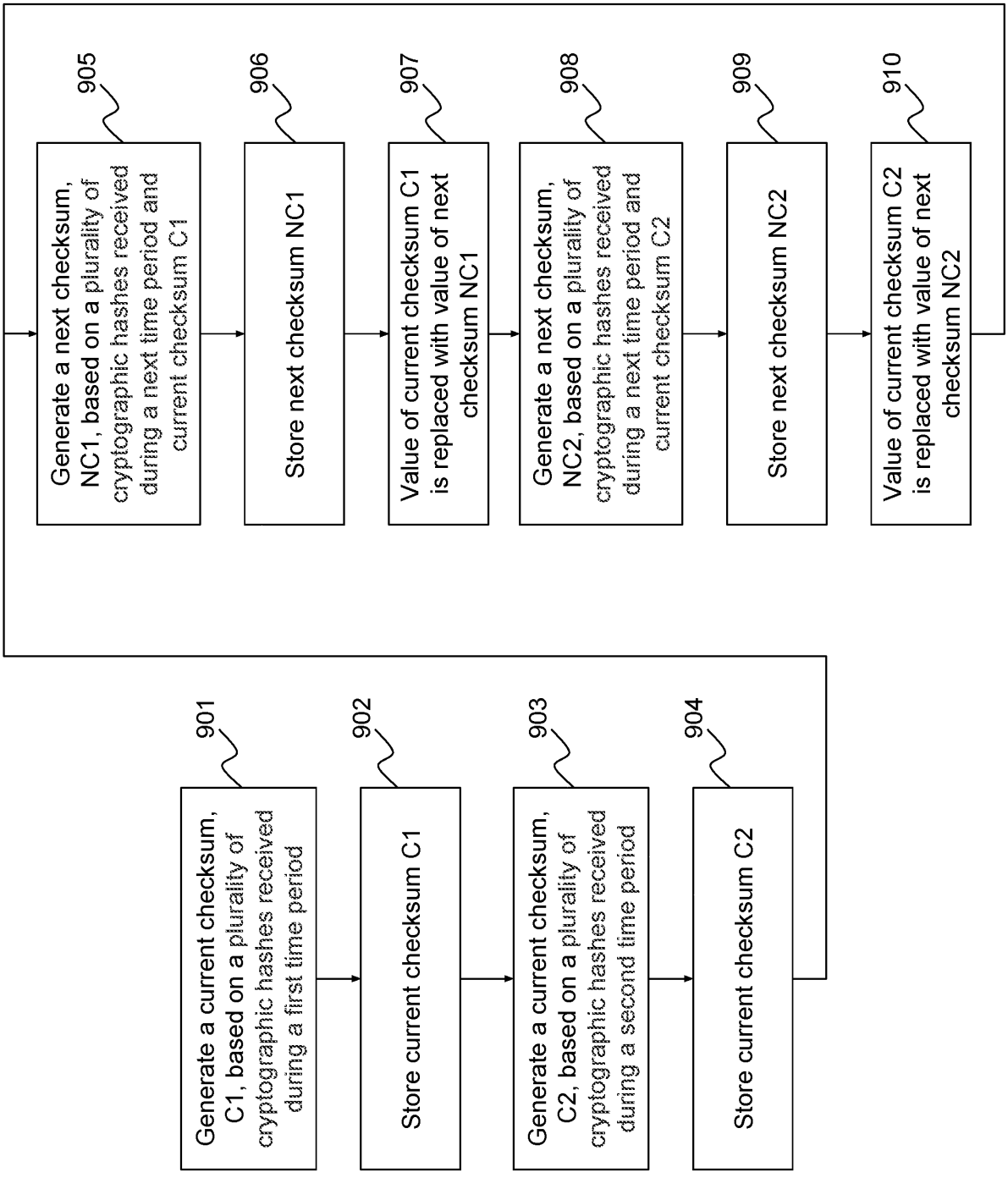

Generate a current checksum, C1, based on a plurality of cryptographic hashes received during a first time period
901
Store current checksum C1
902
Generate a current checksum, C2, based on a plurality of cryptographic hashes received during a second time period
903
Store current checksum C2
904
Generate a next checksum, NC1, based on a plurality of cryptographic hashes received during a next time period and current checksum C1
905
Store next checksum NC1
906
Value of current checksum C1 is replaced with value of next checksum NC1
907
Generate a next checksum, NC2, based on a plurality of cryptographic hashes received during a next time period and current checksum C2
908
Store next checksum NC2
909
Value of current checksum C2 is replaced with value of next checksum NC2
910

Fig. 9

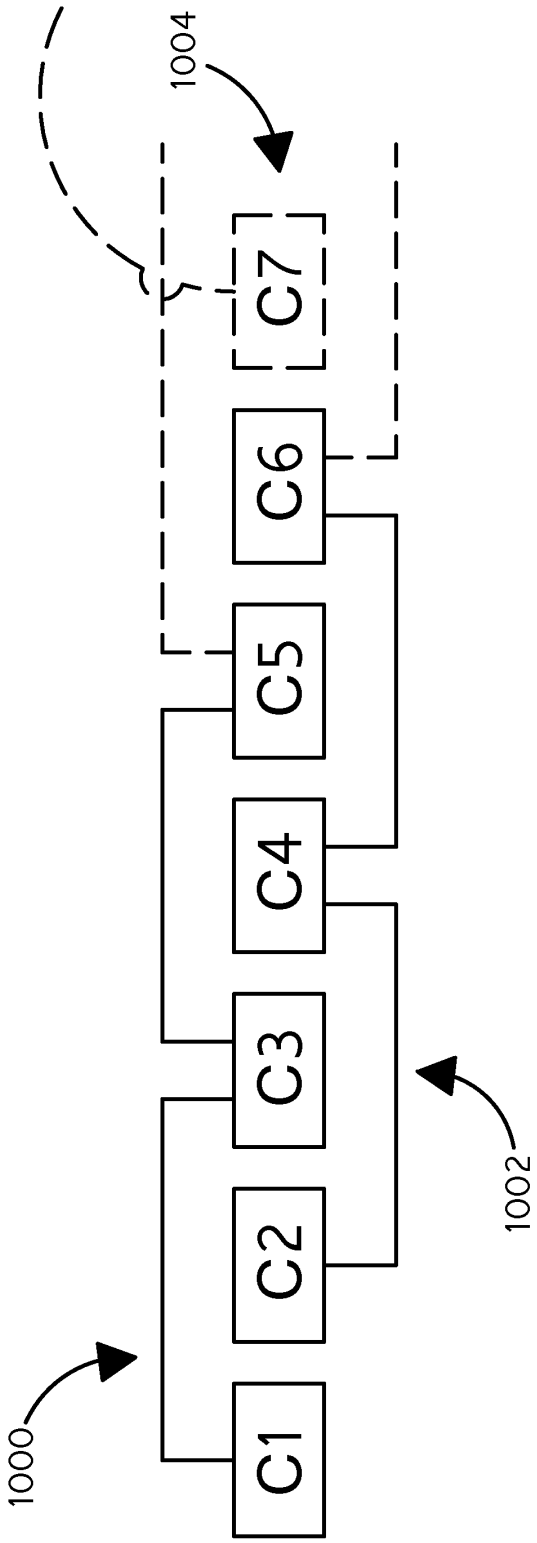


Fig. 10

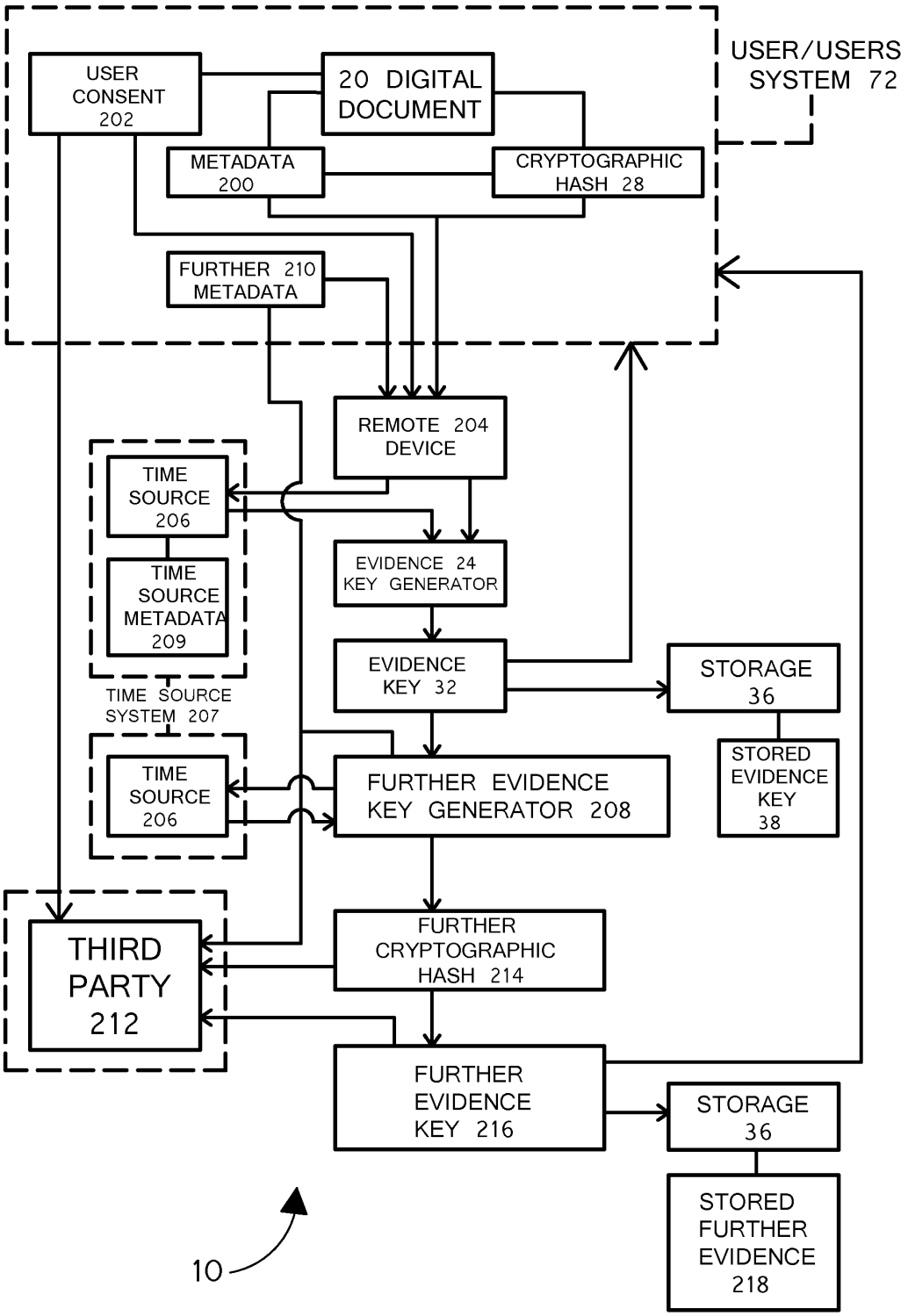

USER/USERS SYSTEM 72
USER CONSENT 202
20 DIGITAL DOCUMENT
METADATA 200
CRYPTOGRAPHIC HASH 28
FURTHER 210 METADATA
REMOTE 204 DEVICE
TIME SOURCE 206
TIME SOURCE METADATA 209
TIME SOURCE SYSTEM 207
EVIDENCE 24 KEY GENERATOR
EVIDENCE KEY 32
STORAGE 36
STORED EVIDENCE KEY 38
TIME SOURCE 206
FURTHER EVIDENCE KEY GENERATOR 208
THIRD PARTY 212
FURTHER CRYPTOGRAPHIC HASH 214
FURTHER EVIDENCE KEY 216
STORAGE 36
STORED FURTHER EVIDENCE 218
10

Fig. 11

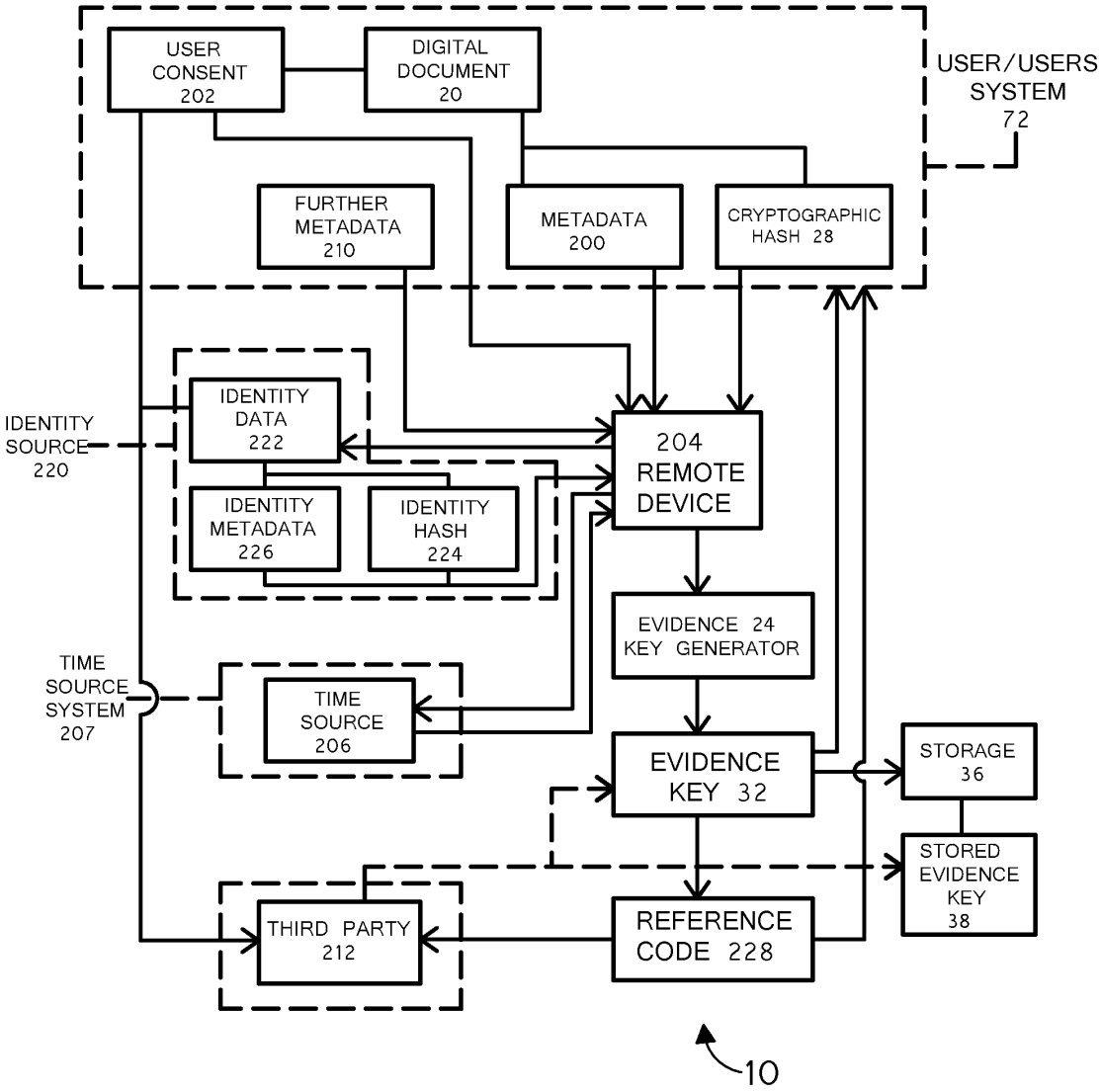

USER CONSENT 202
DIGITAL DOCUMENT 20
USER/USERS SYSTEM 72
FURTHER METADATA 210
METADATA 200
CRYPTOGRAPHIC HASH 28
IDENTITY SOURCE 220
IDENTITY DATA 222
IDENTITY METADATA 226
IDENTITY HASH 224
204 REMOTE DEVICE
EVIDENCE 24 KEY GENERATOR
TIME SOURCE SYSTEM 207
TIME SOURCE 206
EVIDENCE KEY 32
STORAGE 36
STORED EVIDENCE KEY 38
THIRD PARTY 212
REFERENCE CODE 228
10

Fig. 12

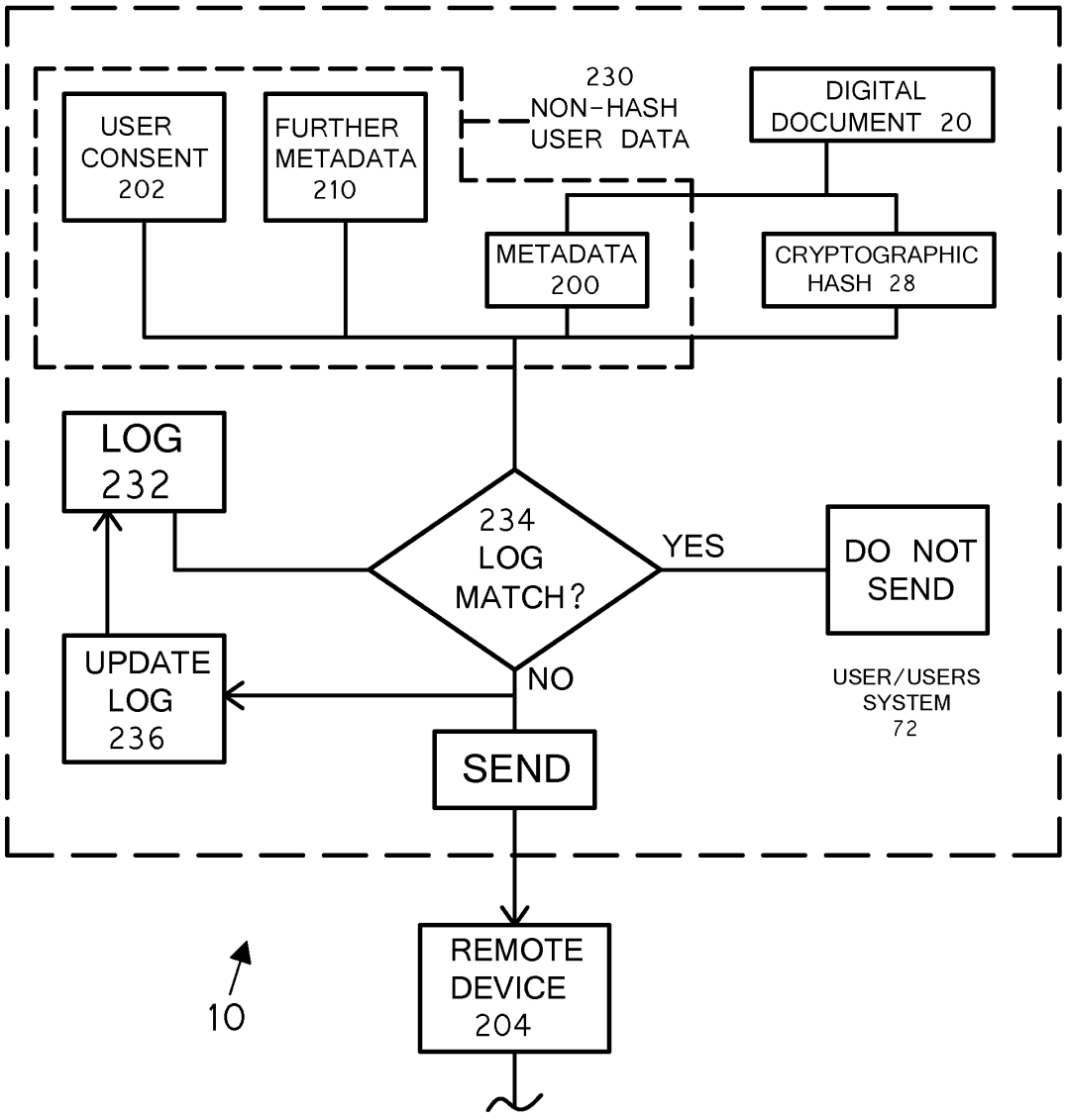

230
NON-HASH
USER DATA
USER
CONSENT
202
FURTHER
METADATA
210
DIGITAL
DOCUMENT 20
METADATA
200
CRYPTOGRAPHIC
HASH 28
LOG
232
234
LOG
MATCH?
YES
DO NOT
SEND
UPDATE
LOG
236
NO
USER/USERS
SYSTEM
72
SEND
REMOTE
DEVICE
204
10

Fig. 13

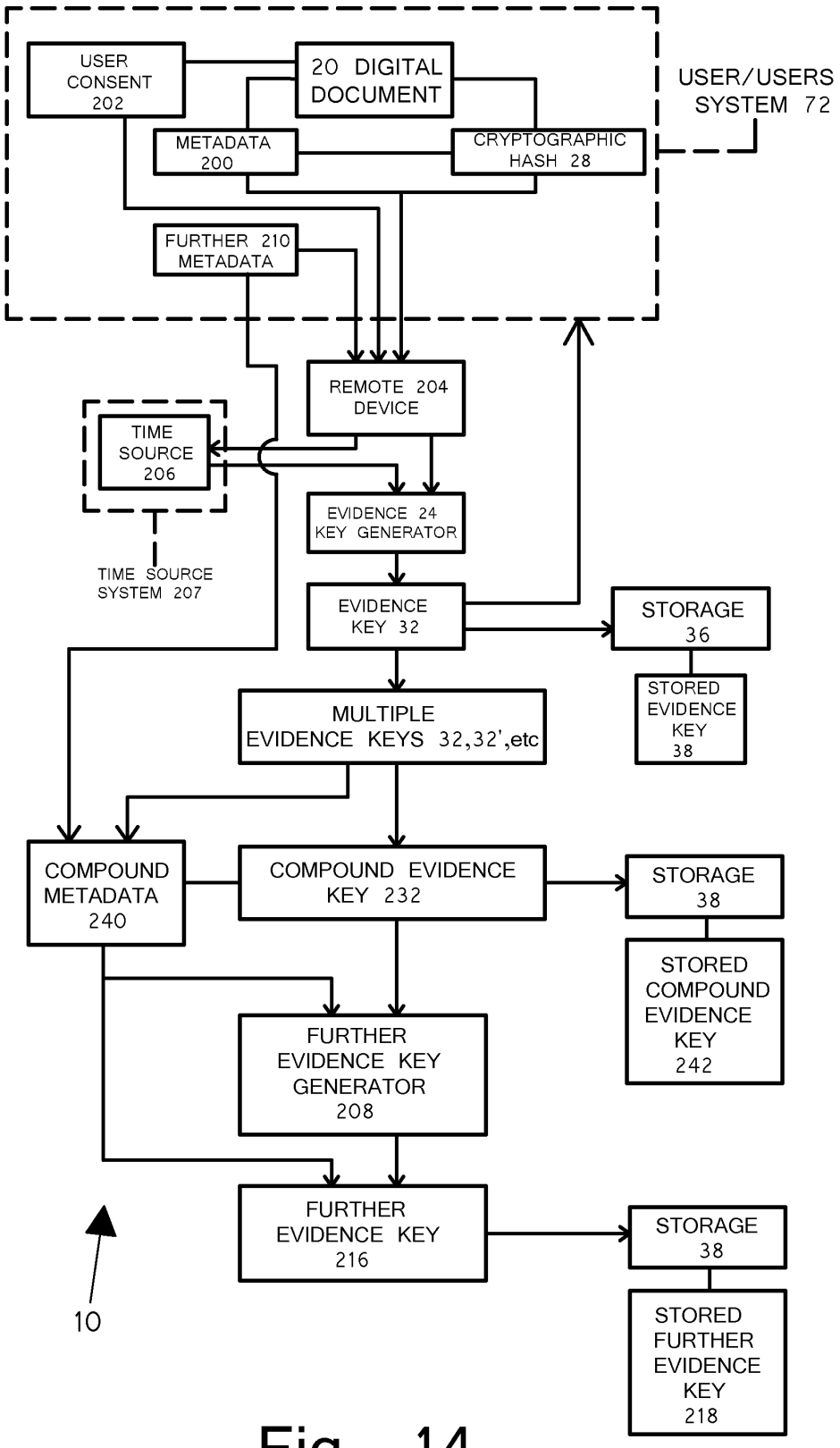

USER CONSENT 202
20 DIGITAL DOCUMENT
USER/USERS SYSTEM 72
METADATA 200
CRYPTOGRAPHIC HASH 28
FURTHER 210 METADATA
REMOTE 204 DEVICE
TIME SOURCE 206
TIME SOURCE SYSTEM 207
EVIDENCE 24 KEY GENERATOR
EVIDENCE KEY 32
STORAGE 36
STORED EVIDENCE KEY 38
MULTIPLE EVIDENCE KEYS 32,32',etc
COMPOUND METADATA 240
COMPOUND EVIDENCE KEY 232
STORAGE 38
STORED COMPOUND EVIDENCE KEY 242
FURTHER EVIDENCE KEY GENERATOR 208
FURTHER EVIDENCE KEY 216
STORAGE 38
STORED FURTHER EVIDENCE KEY 218
10

Fig. 14

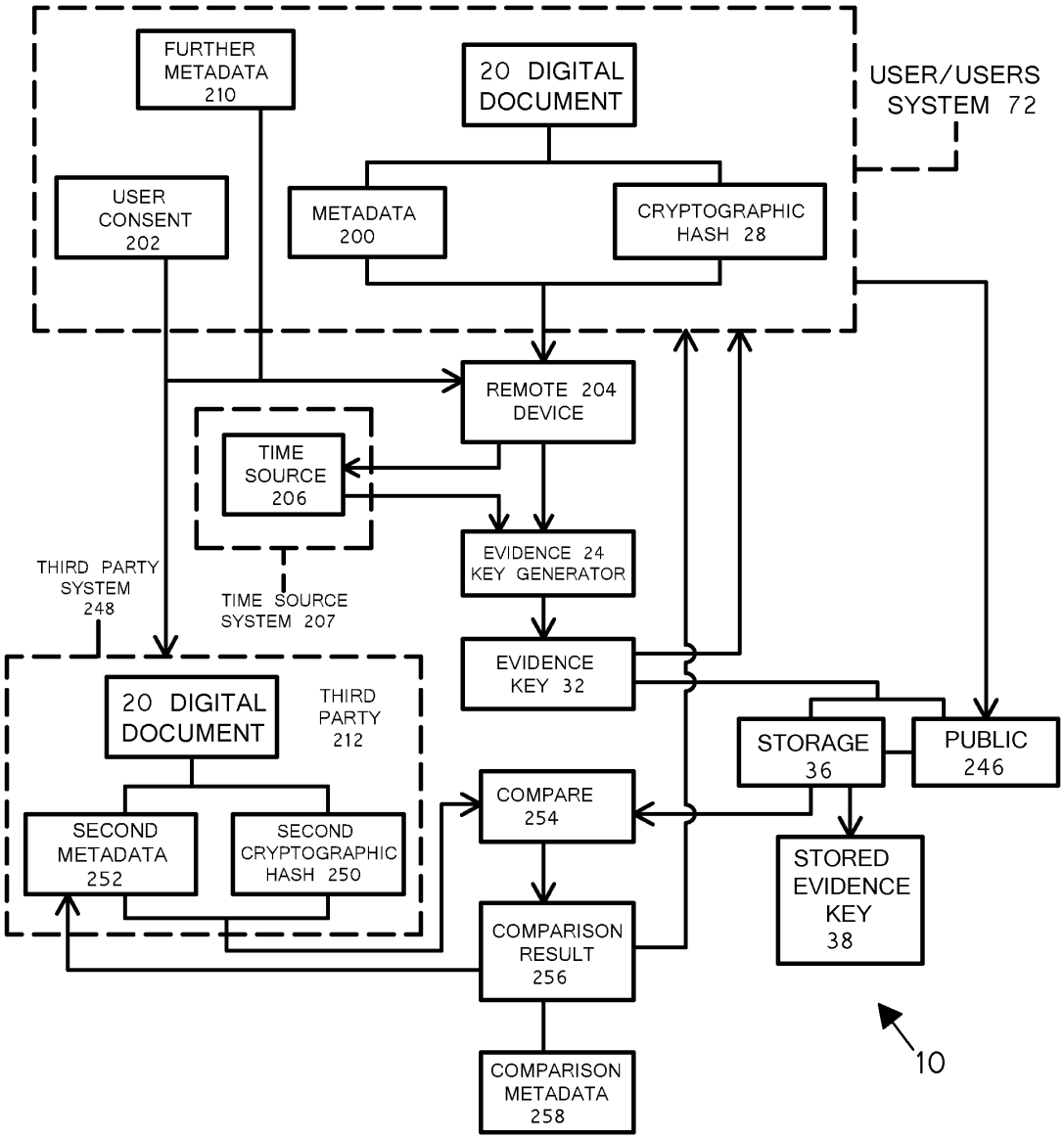

FURTHER METADATA 210
20 DIGITAL DOCUMENT
USER/USERS SYSTEM 72
USER CONSENT 202
METADATA 200
CRYPTOGRAPHIC HASH 28
REMOTE 204 DEVICE
TIME SOURCE 206
EVIDENCE 24 KEY GENERATOR
THIRD PARTY SYSTEM 248
TIME SOURCE SYSTEM 207
EVIDENCE KEY 32
20 DIGITAL DOCUMENT
THIRD PARTY 212
STORAGE 36
PUBLIC 246
COMPARE 254
SECOND METADATA 252
SECOND CRYPTOGRAPHIC HASH 250
STORED EVIDENCE KEY 38
COMPARISON RESULT 256
10
COMPARISON METADATA 258

Fig. 15