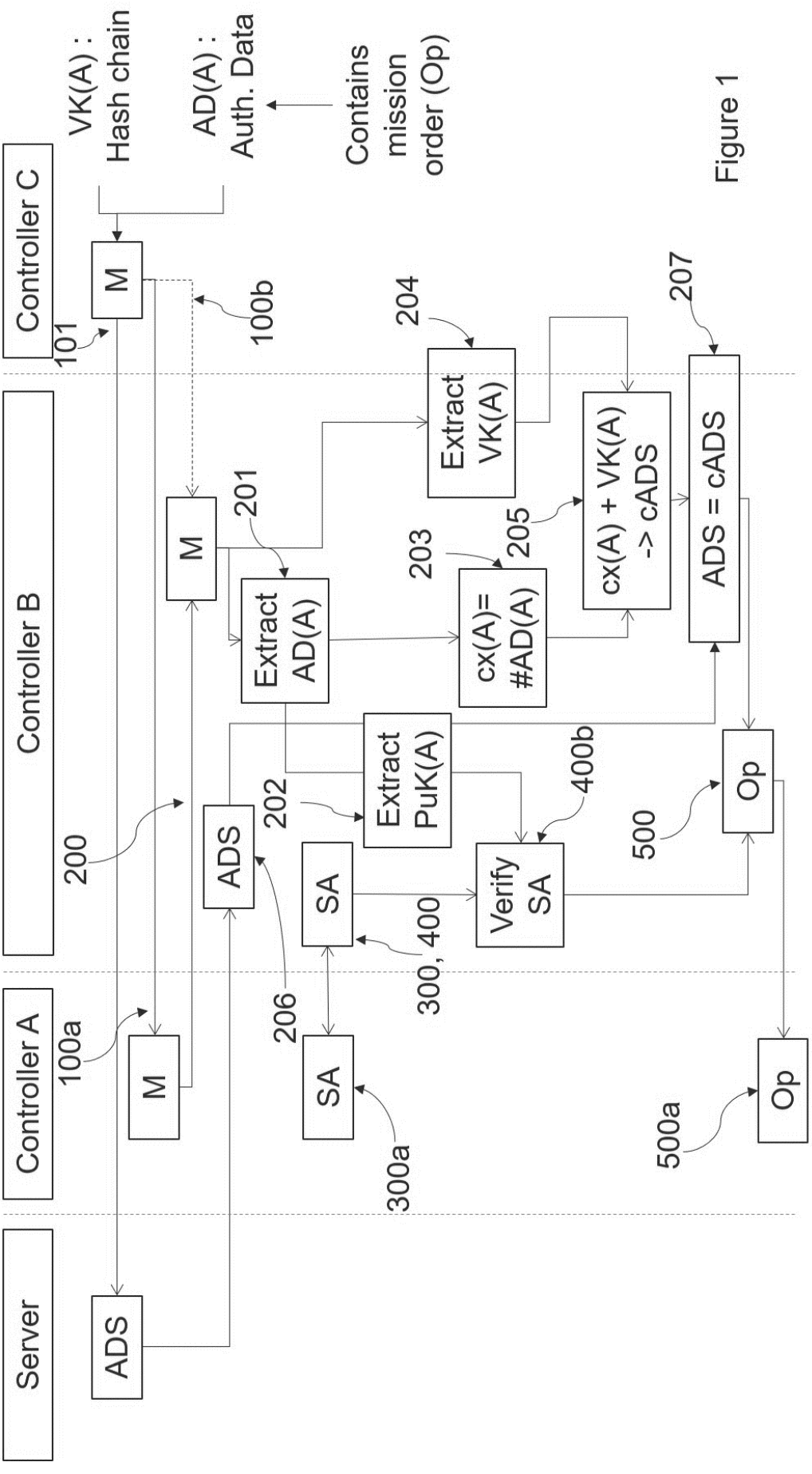

Server
Controller A
Controller B
Controller C
ADS
M
SA
ADS
M
Extract AD(A)
Extract PuK(A)
SA
Verify SA
M
Extract VK(A)
cx(A)= #AD(A)
cx(A) + VK(A) -> cADS
ADS = cADS
Op
Op
VK(A) : Hash chain
AD(A) : Auth. Data
Contains mission order (Op)
100a
100b
101
200
201
202
203
204
205
206
207
300, 400
300a
400b
500
500a

Figure 1

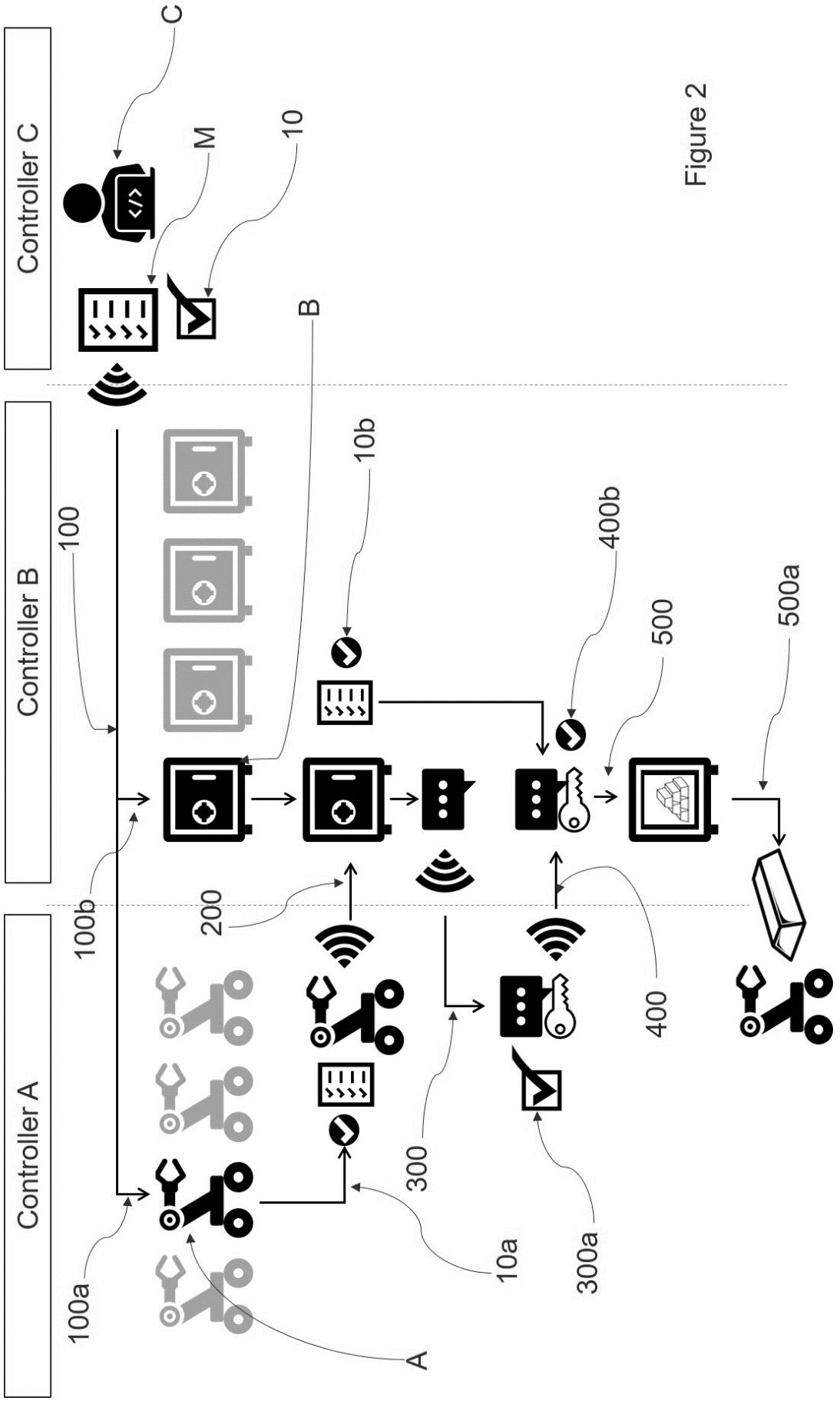

Controller A
Controller B
Controller C
C
M
10
B
100
10b
400b
500
500a
100b
200
400
300
10a
300a
100a
A

Figure 2

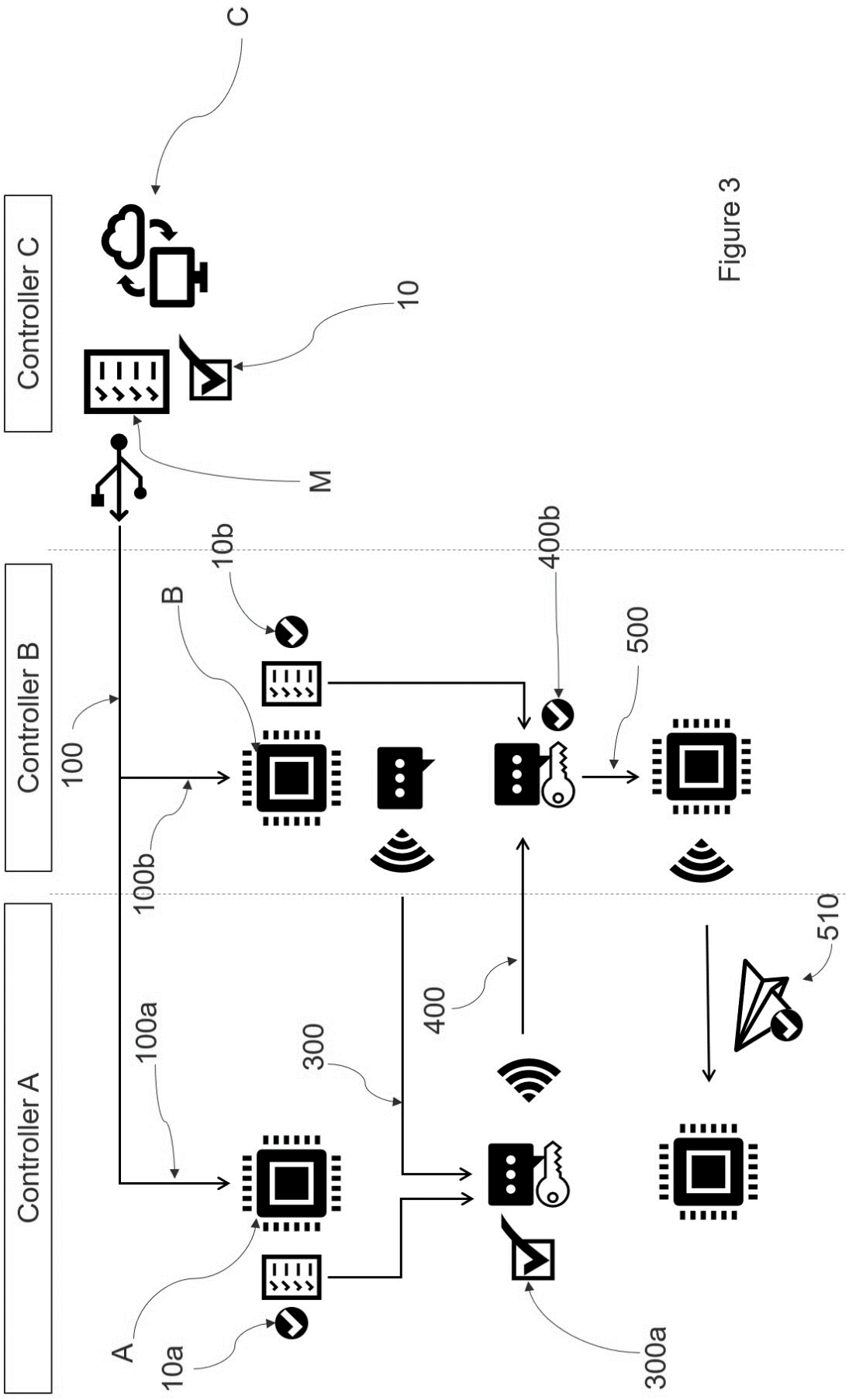

Controller C
Controller B
Controller A
C
10
M
10b
B
400b
500
100
100b
100a
300
400
510
A
10a
300a

Figure 3

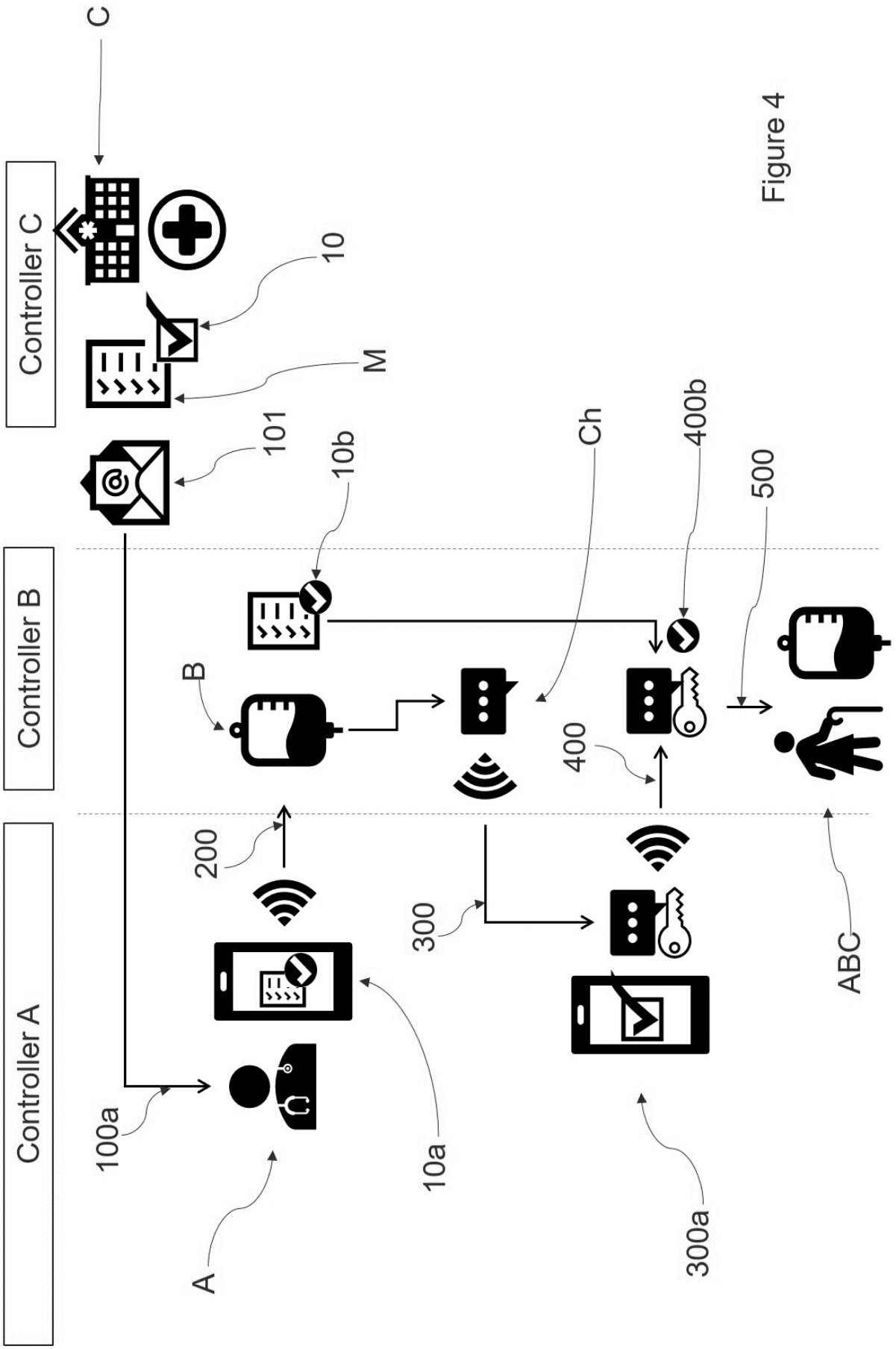

Controller A
Controller B
Controller C
C
10
M
101
10b
Ch
400b
500
B
200
400
300
100a
10a
300a
A
ABC

Figure 4

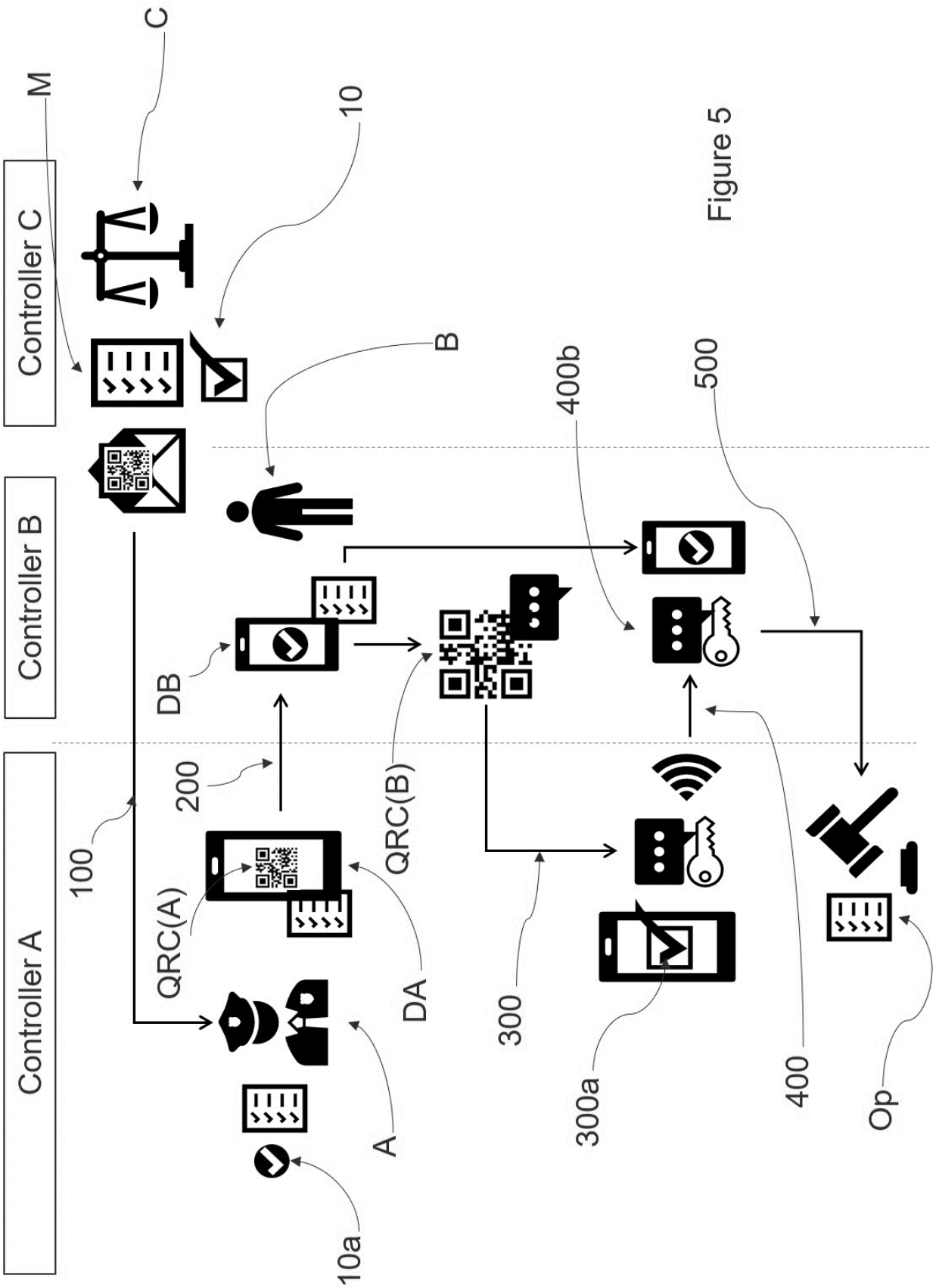

Controller A
Controller B
Controller C
M
C
10
B
400b
500
100
200
DB
QRC(A)
QRC(B)
DA
300
300a
400
Op
A
10a

Figure 5

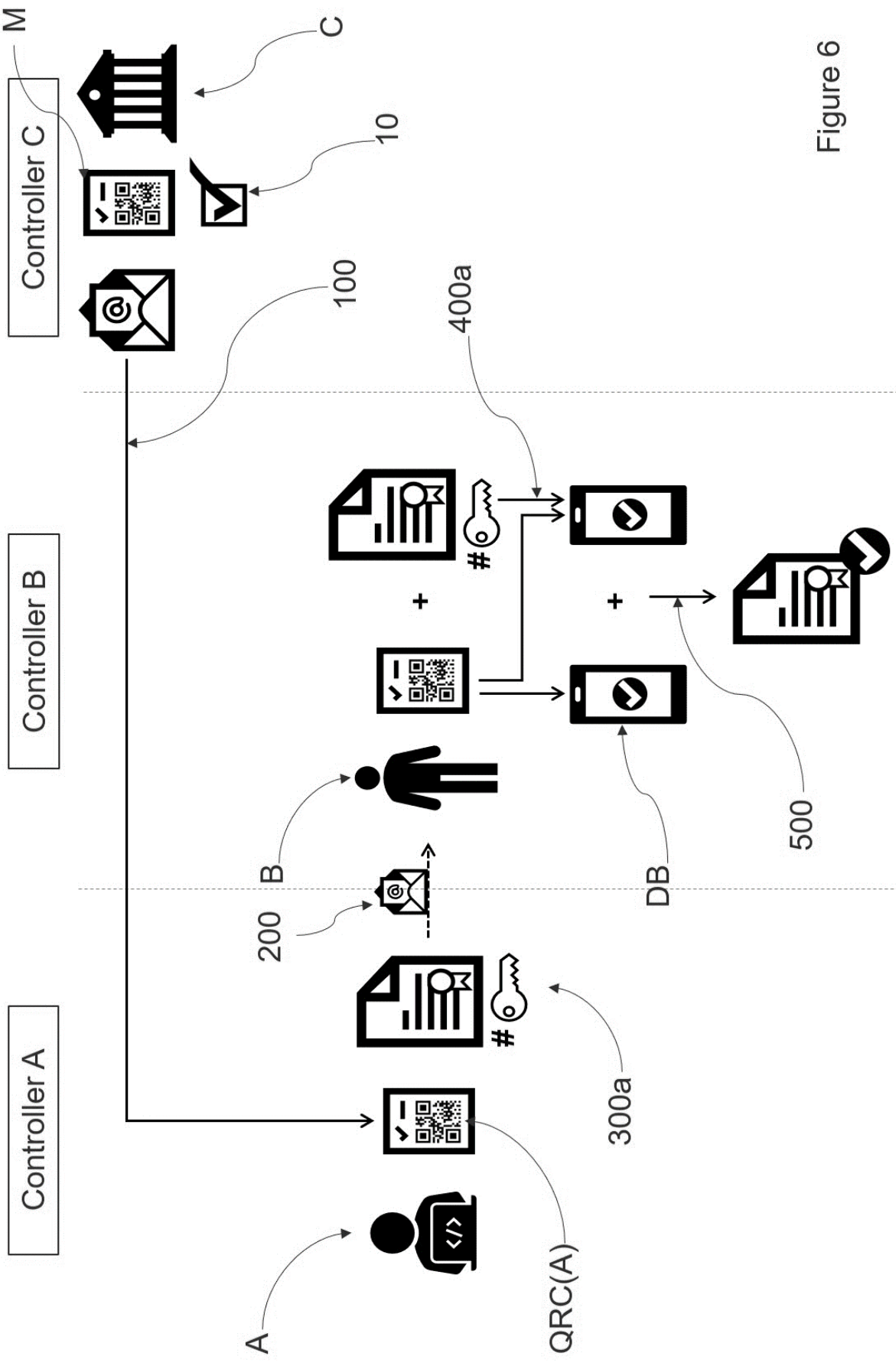

Controller A
Controller B
Controller C
M
C
10
100
400a
A
QRC(A)
300a
200
B
DB
500

Figure 6

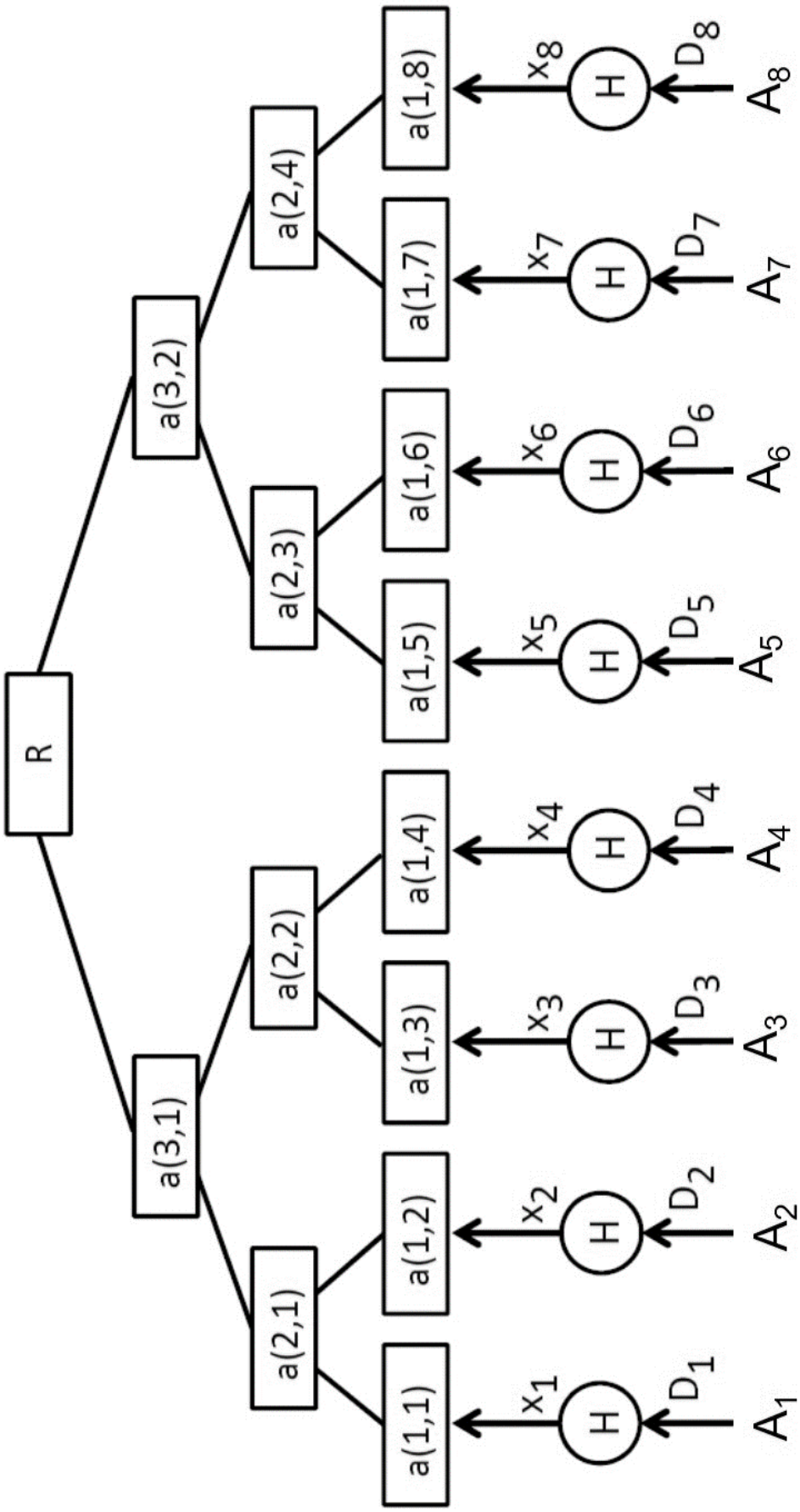

R
a(3,1)
a(3,2)
a(2,1)
a(2,2)
a(2,3)
a(2,4)
a(1,1)
a(1,2)
a(1,3)
a(1,4)
a(1,5)
a(1,6)
a(1,7)
a(1,8)
x1
x2
x3
x4
x5
x6
x7
x8
H
D1
D2
D3
D4
D5
D6
D7
D8
A1
A2
A3
A4
A5
A6
A7
A8

Figure 7

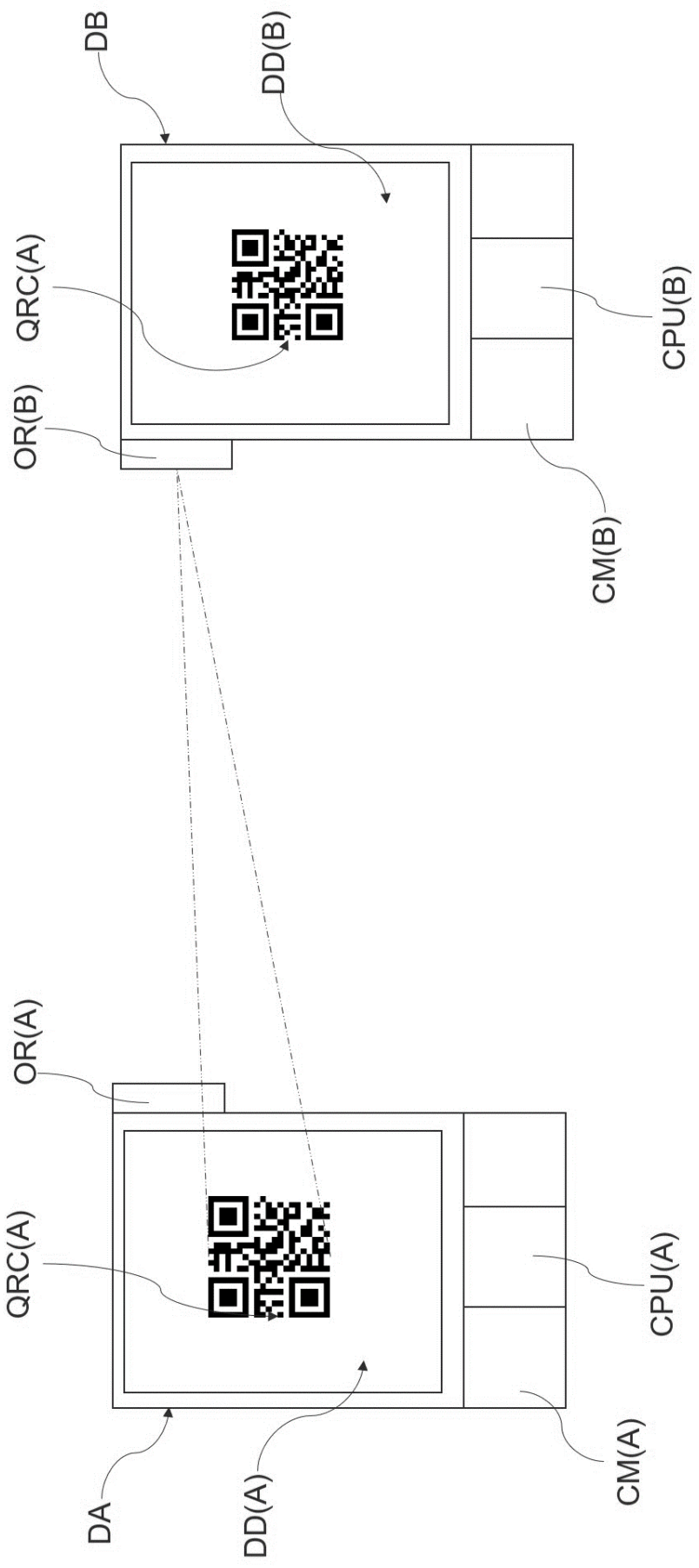


Figure 8