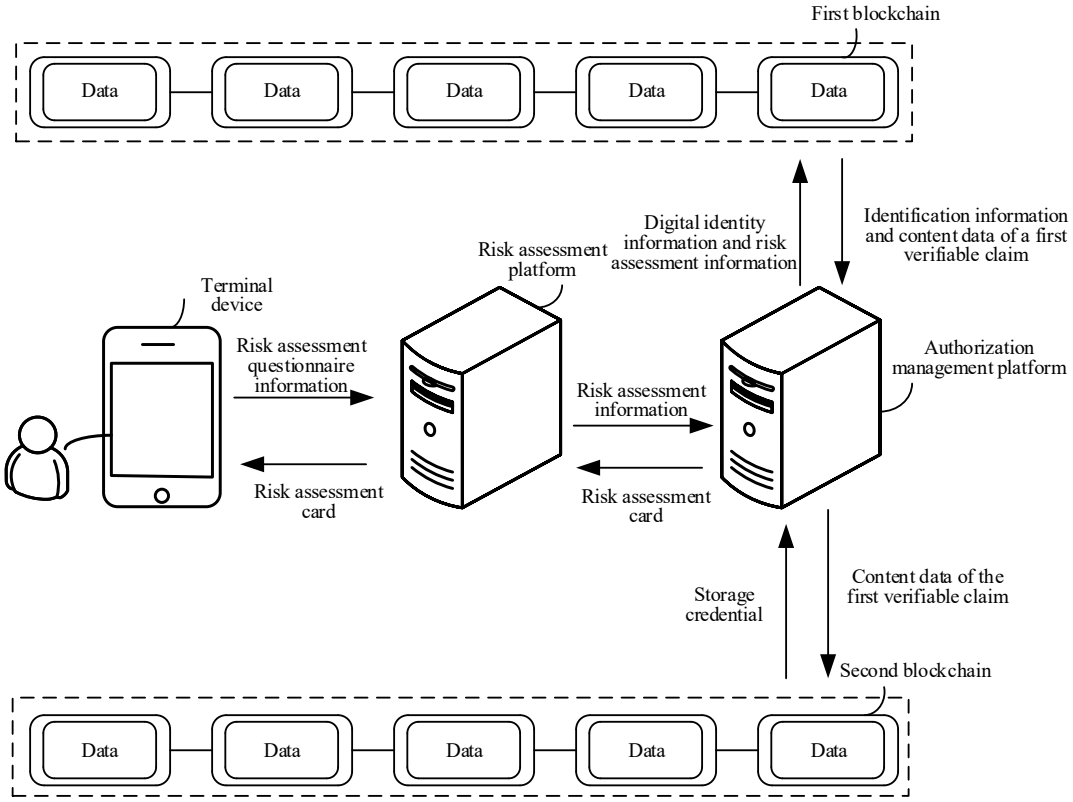
First blockchain
Data
Data
Data
Data
Data
Identification information and content data of a first verifiable claim
Digital identity information and risk assessment information
Risk assessment platform
Terminal device
Risk assessment questionnaire information
Risk assessment information
Authorization management platform
Risk assessment card
Risk assessment card
Storage credential
Content data of the first verifiable claim
Second blockchain
Data
Data
Data
Data
Data

FIG. 1

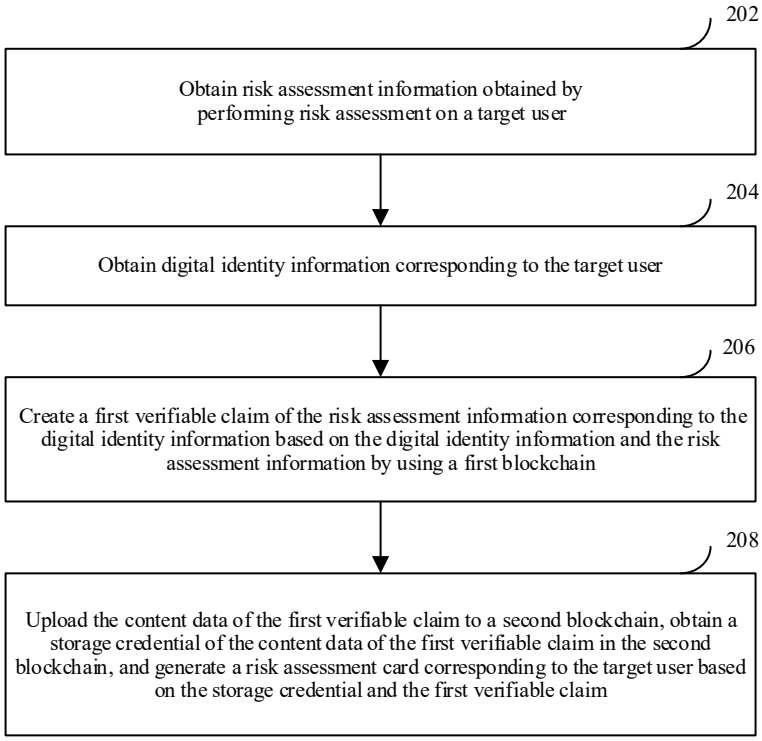
202
Obtain risk assessment information obtained by performing risk assessment on a target user
204
Obtain digital identity information corresponding to the target user
206
Create a first verifiable claim of the risk assessment information corresponding to the digital identity information based on the digital identity information and the risk assessment information by using a first blockchain
208
Upload the content data of the first verifiable claim to a second blockchain, obtain a storage credential of the content data of the first verifiable claim in the second blockchain, and generate a risk assessment card corresponding to the target user based on the storage credential and the first verifiable claim

FIG. 2

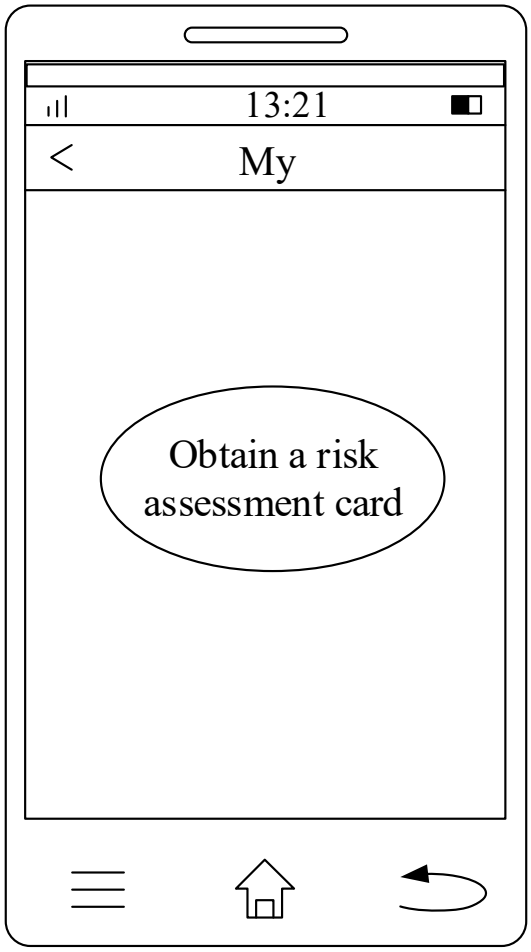

FIG. 3(a)

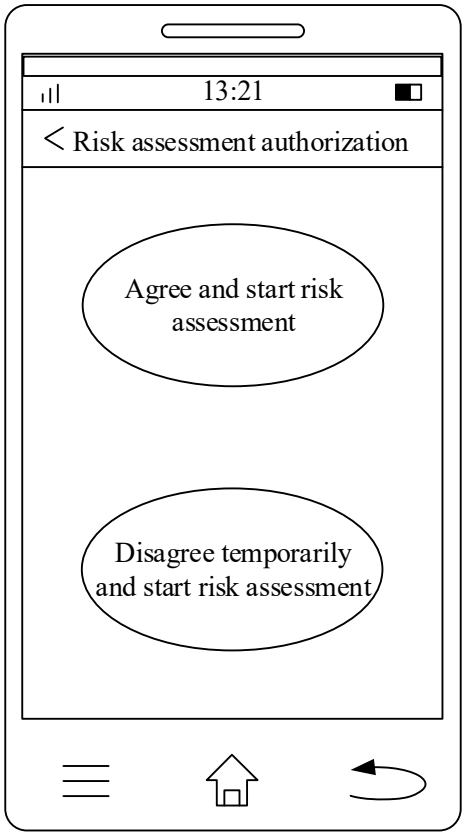
13:21
< Risk assessment authorization
Agree and start risk assessment
Disagree temporarily and start risk assessment

FIG. 3(b)

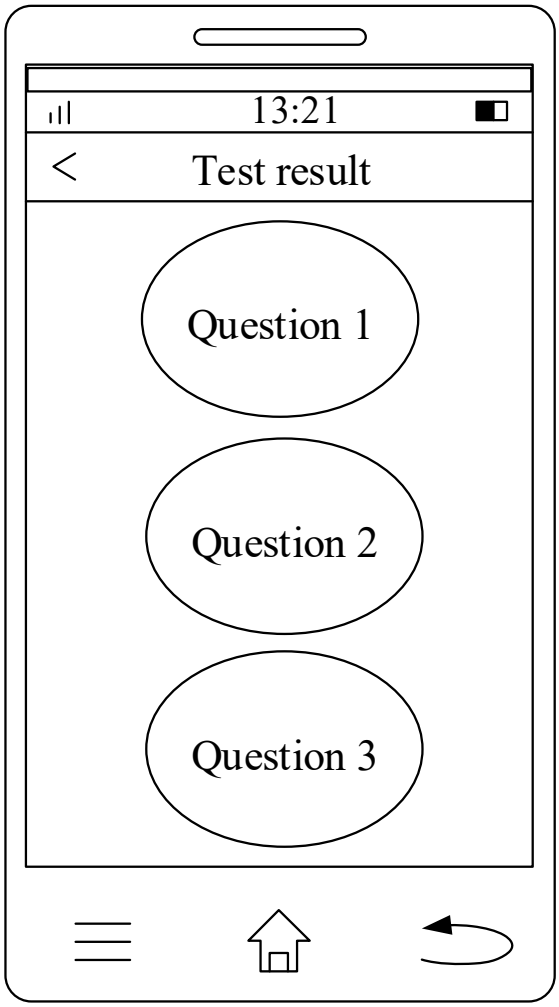

FIG. 3(c)

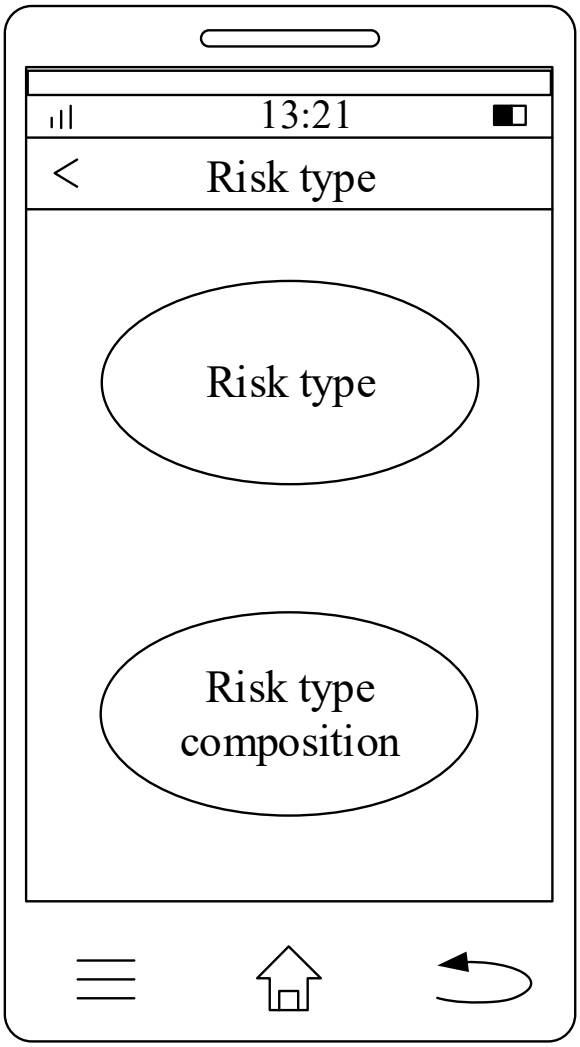

FIG. 3(d)

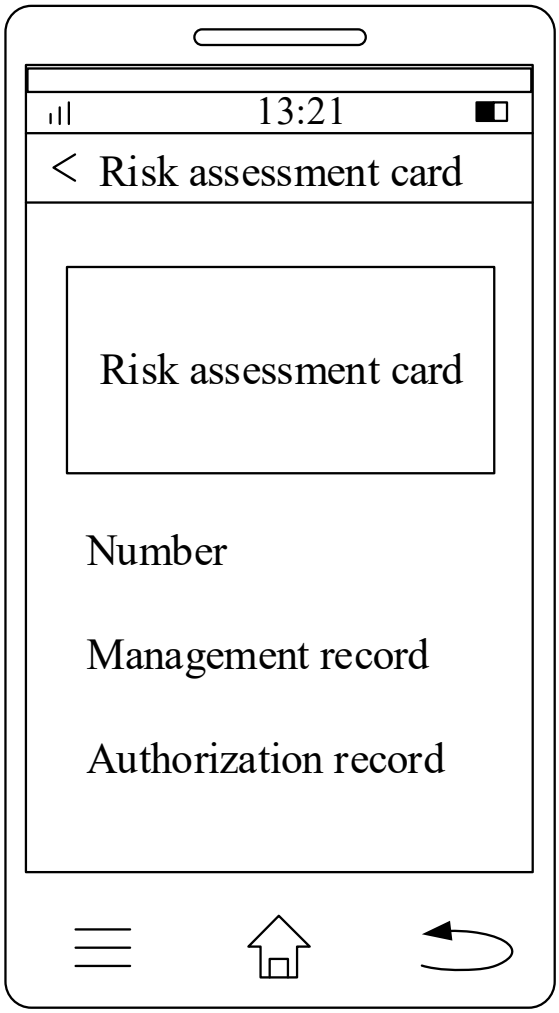
13:21
< Risk assessment card
Risk assessment card
Number
Management record
Authorization record

FIG. 3(e)

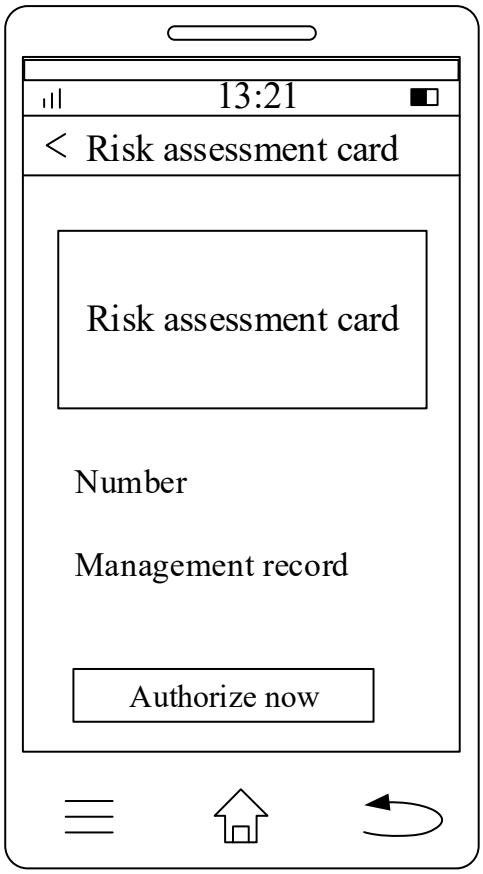
13:21
< Risk assessment card
Risk assessment card
Number
Management record
Authorize now

FIG. 4(a)

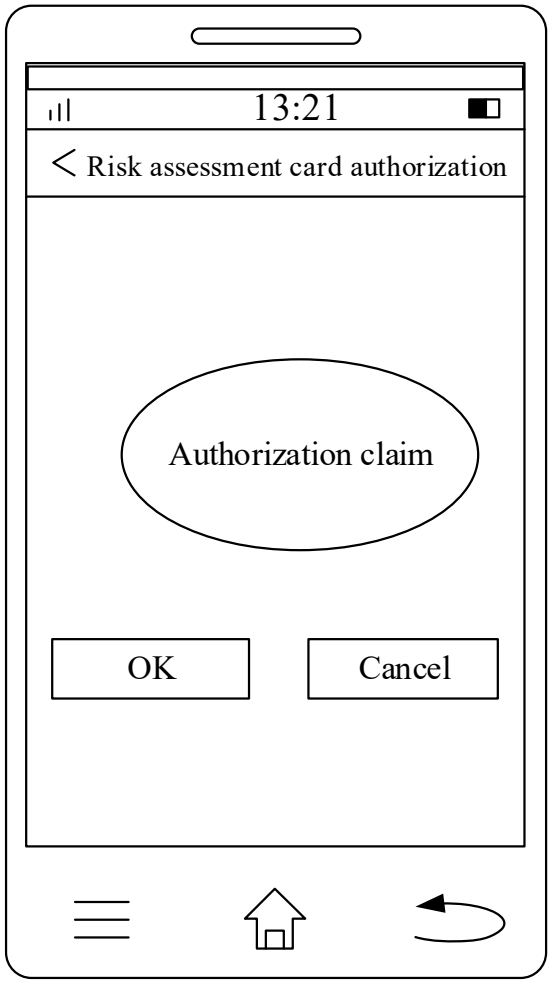
13:21
Risk assessment card authorization
Authorization claim
OK
Cancel

FIG. 4(b)

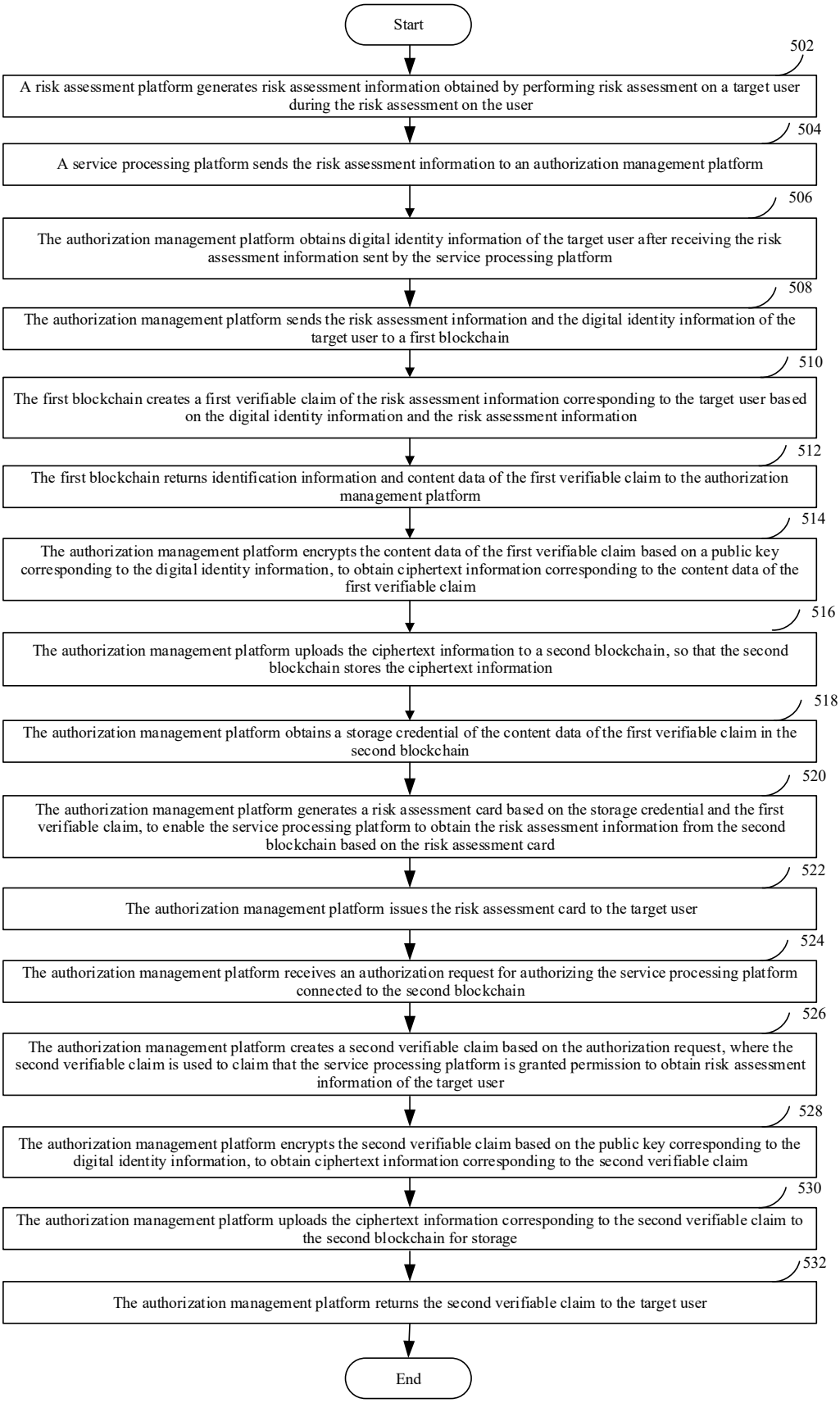
Start
502
A risk assessment platform generates risk assessment information obtained by performing risk assessment on a target user during the risk assessment on the user
504
A service processing platform sends the risk assessment information to an authorization management platform
506
The authorization management platform obtains digital identity information of the target user after receiving the risk assessment information sent by the service processing platform
508
The authorization management platform sends the risk assessment information and the digital identity information of the target user to a first blockchain
510
The first blockchain creates a first verifiable claim of the risk assessment information corresponding to the target user based on the digital identity information and the risk assessment information
512
The first blockchain returns identification information and content data of the first verifiable claim to the authorization management platform
514
The authorization management platform encrypts the content data of the first verifiable claim based on a public key corresponding to the digital identity information, to obtain ciphertext information corresponding to the content data of the first verifiable claim
516
The authorization management platform uploads the ciphertext information to a second blockchain, so that the second blockchain stores the ciphertext information
518
The authorization management platform obtains a storage credential of the content data of the first verifiable claim in the second blockchain
520
The authorization management platform generates a risk assessment card based on the storage credential and the first verifiable claim, to enable the service processing platform to obtain the risk assessment information from the second blockchain based on the risk assessment card
522
The authorization management platform issues the risk assessment card to the target user
524
The authorization management platform receives an authorization request for authorizing the service processing platform connected to the second blockchain
526
The authorization management platform creates a second verifiable claim based on the authorization request, where the second verifiable claim is used to claim that the service processing platform is granted permission to obtain risk assessment information of the target user
528
The authorization management platform encrypts the second verifiable claim based on the public key corresponding to the digital identity information, to obtain ciphertext information corresponding to the second verifiable claim
530
The authorization management platform uploads the ciphertext information corresponding to the second verifiable claim to the second blockchain for storage
532
The authorization management platform returns the second verifiable claim to the target user
End

FIG. 5

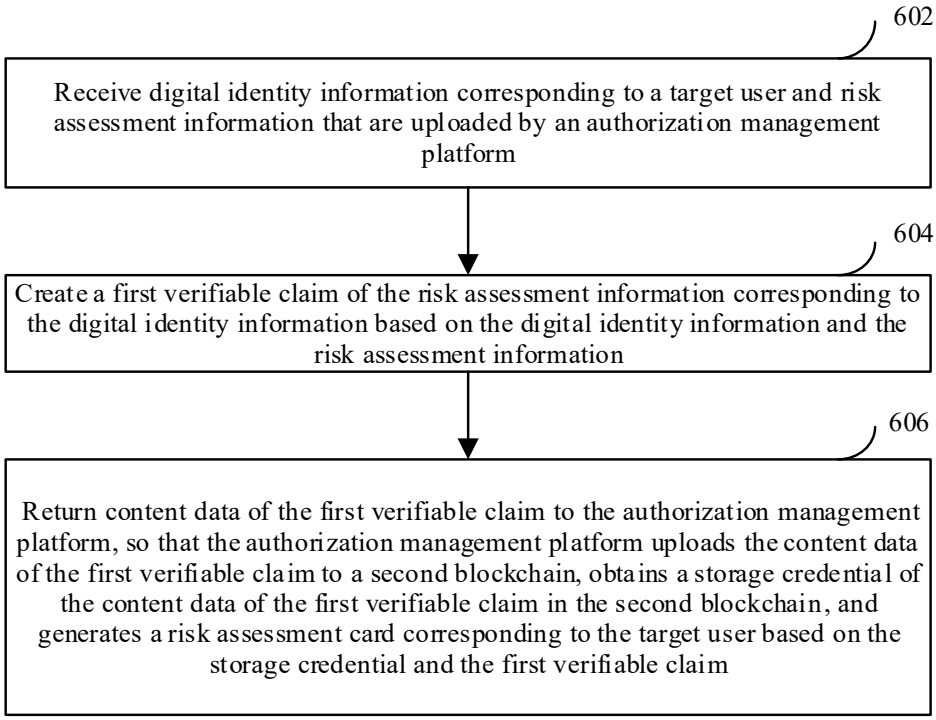
602
Receive digital identity information corresponding to a target user and risk assessment information that are uploaded by an authorization management platform
604
Create a first verifiable claim of the risk assessment information corresponding to the digital identity information based on the digital identity information and the risk assessment information
606
Return content data of the first verifiable claim to the authorization management platform, so that the authorization management platform uploads the content data of the first verifiable claim to a second blockchain, obtains a storage credential of the content data of the first verifiable claim in the second blockchain, and generates a risk assessment card corresponding to the target user based on the storage credential and the first verifiable claim

FIG. 6

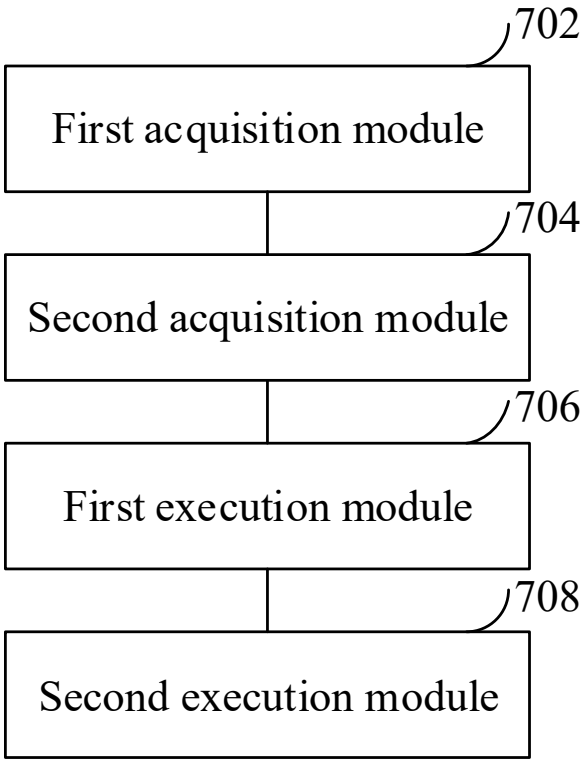
702
First acquisition module
704
Second acquisition module
706
First execution module
708
Second execution module

FIG. 7

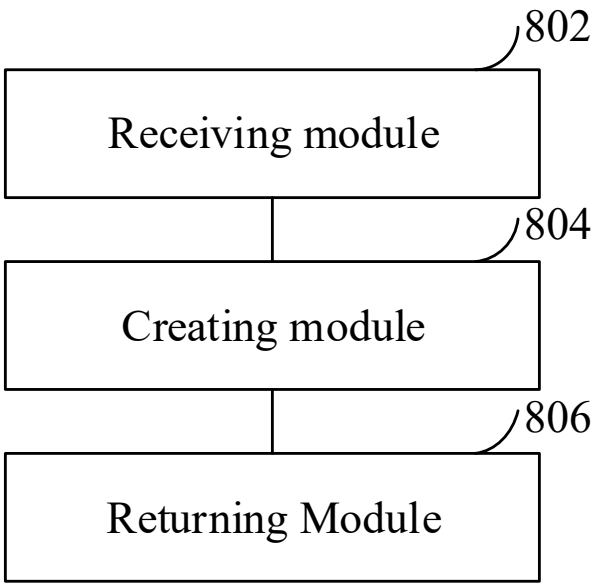
802
Receiving module
804
Creating module
806
Returning Module

FIG. 8

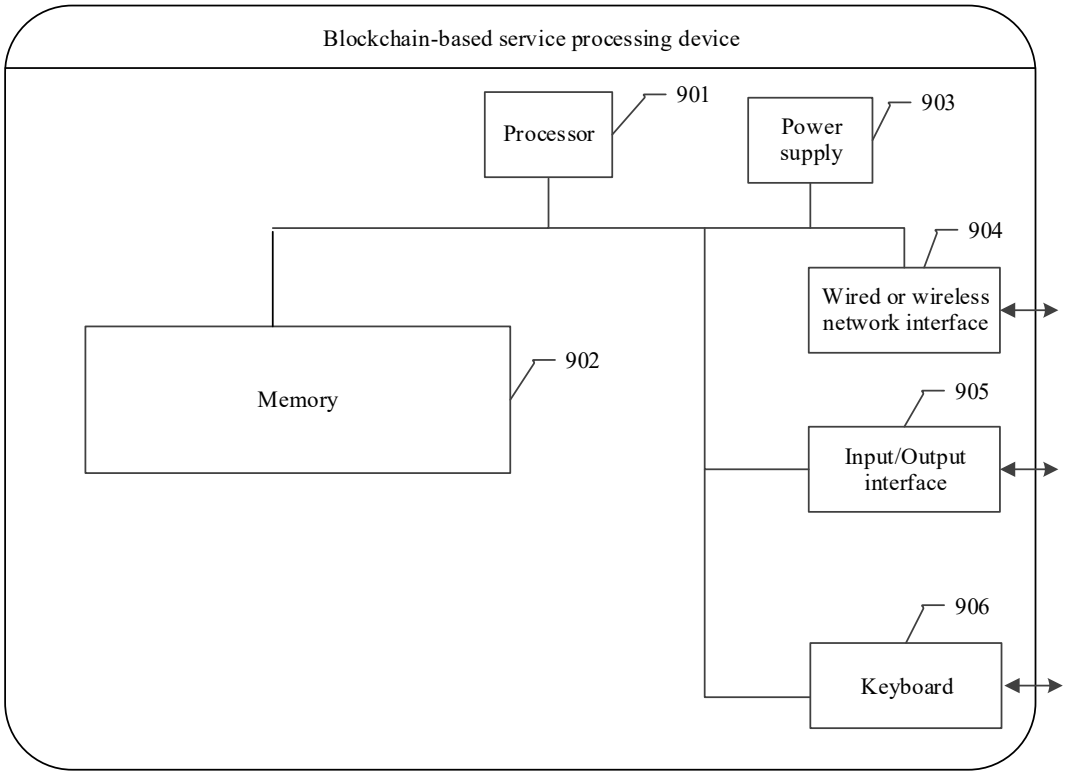
Blockchain-based service processing device
Processor
901
Power supply
903
904
Wired or wireless network interface
Memory
902
905
Input/Output interface
906
Keyboard

FIG. 9