CLAIMS

What is claimed is:

1. A logistics information management system (100), comprising:

a block chain subsystem (150), comprising multiple block chain nodes (141~147);

a logistics service subsystem (120), arranged to operably generate a take-over request comprising a first current vendor identification data and an order event identification data when a logistician device (105) approaches a target region; and

a recipient device (103), arranged to operably receive the take-over request, and to operably generate a delivery destination information request comprising the order event identification data and the first current vendor identification data according to the take-over request;

wherein the block chain subsystem (150) is arranged to operably receive the delivery destination information request, to operably search for an order event recorded in a recipient smart contract stored in the block chain subsystem (150) according to the order event identification data, and to operably read a valid vendor identification data from the order event;

wherein if the first current vendor identification data matches the valid vendor identification data, the block chain subsystem (150) reads a delivery destination information from the order event;

wherein the recipient device (103) is further arranged to operably generate and transmit an available-to-receive notice to the logistics service subsystem (120) after receiving the delivery destination information;

wherein the logistics service subsystem (120) is further arranged to operably generate and transmit a position information request comprising a second current vendor identification data and the order event identification data to the recipient device (103) when the logistician device (105) approaches a delivery destination indicated in the delivery destination information;

wherein the recipient device (103) is further arranged to operably receive the position information request, and to operably generate a logistics vendor identity authentication request comprising the second current vendor identification data and the order event identification data according to the position information request;

wherein the block chain subsystem (150) is further arranged to operably receive the logistics vendor identity authentication request, to operably search for the order event recorded in the recipient smart contract stored in the block chain subsystem (150) according to the order event identification data in the logistics vendor identity authentication request, and to operably read the valid vendor identification data from the order event;

wherein the block chain subsystem (150) generates an identity authentication successful notice only if the second current vendor identification data matches the valid vendor identification data;

wherein the recipient device (103) is further arranged to operably utilize a cipher key to encrypt a second current location of the recipient device (103) after receiving the identity authentication successful notice so as to generate an encrypted recipient position.

2. The logistics information management system (100) of claim 1, wherein the recipient device (103) is further arranged to operably determine whether a first current location where the recipient device (103) receives the delivery destination information is within the~~a~~ delivery destination ~~indicated in the delivery destination information~~, and to operably transmit the available-to-receive notice to the logistics service subsystem (120) only if the first current location is whthin the delivery destination.

3. The logistics information management system (100) of claim 2, wherein the recipient device (103) is further arranged to operably generate an inquiry message to inquire a receiving intention of a recipient, and to operably transmit the available-to-receive notice to the logistics service subsystem (120) only if the recipient device (103) receives an intent-to-receive instruction issued by the recipient.

4. The logistics information management system (100) of claim 1, wherein the recipient device (103) is further arranged to operably generate an inquiry message to inquire a receiving intention of a recipient when the delivery destination information is received by the recipient device (103), and arranged to operably transmit the available-to-receive notice to the logistics service subsystem (120) only if the recipient device (103) receives an intent-to-receive instruction issued by the recipient.

~~5. The logistics information management system (100) of claim 2, wherein the logistics service subsystem (120) is further arranged to operably generate and transmit a position~~

~~information request comprising a second current vendor identification data and the order event identification data to the recipient device (103) when the logistician device (105) approaches the delivery destination;~~

~~wherein the recipient device (103) is further arranged to operably receive the position information request, and to operably generate a logistics vendor identity authentication request comprising the second current vendor identification data and the order event identification data according to the position information request;~~

~~wherein the block chain subsystem (150) is further arranged to operably receive the logistics vendor identity authentication request, to operably search for the order event recorded in the recipient smart contract stored in the block chain subsystem (150) according to the order event identification data in the logistics vendor identity authentication request, and to operably read the valid vendor identification data from the order event;~~

~~wherein the block chain subsystem (150) generates an identity authentication successful notice only if the second current vendor identification data matches the valid vendor identification data;~~

~~wherein the recipient device (103) is further arranged to operably utilize a cipher key to encrypt a second current location of the recipient device (103) after receiving the identity authentication successful notice so as to generate an encrypted recipient position.~~

~~6.~~5. The logistics information management system (100) of ~~claim 5~~claim 1, wherein the recipient device (103) is further arranged to operably transmit the cipher key to the logistics service subsystem (120), and to operably transmit the encrypted recipient position to the block chain subsystem (150);

wherein the block chain subsystem (150) is further arranged to operably store the encrypted recipient position in the order event recorded in the recipient smart contract;

wherein the logistics service subsystem (120) is further arranged to operably read the encrypted recipient position recorded in the order event recorded in the recipient smart contract stored in the block chain subsystem (150);

wherein the logistics service subsystem (120) is further arranged to operably utilize the cipher key to decrypt the encrypted recipient position so as to acquire the second current location of the recipient device (103), and to operably transmit the second current location to the logistician device (105).

~~7.~~6. The logistics information management system (100) of claim 2, further comprising:

an e-commerce vender subsystem (110), arranged to operably create the recipient smart contract in the block chain subsystem (150), and to operably write the delivery destination information and the valid vendor identification data into the recipient smart contract so as to form the order event;

wherein the e-commerce vender subsystem (110) is arranged to operably generate the delivery destination information according to a delivery location;

wherein the recipient device (103) is arranged to operably transmit a recipient account request to the e-commerce vender subsystem (110) so that the e-commerce vender subsystem (110) is enabled to create a recipient account correspondingly;

wherein the e-commerce vender subsystem (110) is arranged to operably create a correlation between the recipient account and a recipient smart contract identification data of the recipient smart contract, so that the recipient device (103) accesses the block chain subsystem (150) according to the correlation;

wherein the recipient device (103) is further arranged to operably log in to the e-commerce vender subsystem (110) with the recipient account so as to transmit the delivery destination information request to the block chain subsystem (150), and the e-commerce vender subsystem (110) requests the block chain subsystem (150) to provide the delivery destination information corresponding to the delivery destination information request according to the recipient account and the correlation;

wherein the block chain subsystem (150) is further arranged to operably provide the delivery destination information to the e-commerce vender subsystem (110) if the first current vendor identification data matches the valid vendor identification data, and the e-commerce vender subsystem (110) is arranged to operably transmit the delivery destination information to the recipient device (103) according to the correlation.

~~8.~~7. The logistics information management system (100) of ~~claim 7~~claim 6, wherein the e-commerce vender subsystem (110) is further arranged to operably conduct a location de-identification process on the delivery location so as to generate the delivery destination information.

~~9.~~8. A computer program product (166), enabling a recipient device (103) of a logistics information management system (100) to perform a recipient privacy protection operation, wherein the logistics information management system (100) comprises a block chain

subsystem (150), a logistics service subsystem (120), and the recipient device (103), the recipient privacy protection operation comprising:

receiving a take-over request generated by the logistics service subsystem (120) when a logistician device (105) approaches a target region, wherein the take-over request comprises a first current vendor identification data and an order event identification data;

generating a delivery destination information request comprising the order event identification data and the first current vendor identification data according to the take-over request;

receiving a delivery destination information; and

generating and transmitting an available-to-receive notice to the logistics service subsystem (120) after receiving the delivery destination information;

wherein the block chain subsystem (150) is arranged to operably receive the delivery destination information request, and to operably search for an order event recorded in a recipient smart contract stored in the block chain subsystem (150) according to the order event identification data, and the order event comprises a valid vendor identification data;

wherein the block chain subsystem (150) provides the delivery destination information only if the first current vendor identification data matches the valid vendor identification data;

wherein the logistics service subsystem (120) is further arranged to operably generate a position information request comprising a second current vendor identification data and the order event identification data when the logistician device (105) approaches a delivery destination indicated in the delivery destination information;

wherein the recipient privacy protection operation further comprises:

receiving the position information request;

generating and transmitting a logistics vendor identity authentication request comprising the second current vendor identification data and the order event identification data to the block chain subsystem (150) according to the position information request;

receiving an identity authentication successful notice transmitted from the block chain subsystem (150);

acquiring a second current location of the recipient device (103) after receiving the identity authentication successful notice; and

utilizing a cipher key to encrypt the second current location of the recipient device (103) to generate an encrypted recipient position;

wherein the block chain subsystem (150) is arranged to operably receive the logistics vendor identity authentication request, to operably search for the order event recorded in the

recipient smart contract stored in the block chain subsystem (150) according to the order event identification data in the logistics vendor identity authentication request, and to operably read the valid vendor identification data from the order event;

wherein the block chain subsystem (150) provides the identity authentication successful notice only if the second current vendor identification data matches the valid vendor identification data.

~~10.~~9. The computer program product (166) of ~~claim 9~~claim 8, wherein the recipient privacy protection operation further comprises:

determining whether a first current location where the recipient device (103) receives the delivery destination information is within ~~a~~the delivery destination~~ indicated in the delivery destination information~~, and transmitting the available-to-receive notice to the logistics service subsystem (120) only if the first current location is whthin the delivery destination.

~~11.~~10. The computer program product (166) of ~~claim 10~~claim 9, wherein the recipient privacy protection operation further comprises:

generating an inquiry message to inquire a receiving intention of a recipient, and transmitting the available-to-receive notice to the logistics service subsystem (120) only if an intent-to-receive instruction issued by the recipient is received.

~~12.~~11. The computer program product (166) of ~~claim 9~~claim 8, wherein the recipient privacy protection operation further comprises:

generating an inquiry message to inquire a receiving intention of a recipient, and transmitting the available-to-receive notice to the logistics service subsystem (120) only if an intent-to-receive instruction issued by the recipient is received.

~~13. The computer program product (166) of claim 10, wherein the logistics service subsystem (120) is further arranged to operably generate a position information request comprising a second current vendor identification data and the order event identification data when the logistician device (105) approaches the delivery destination;~~

~~wherein the recipient privacy protection operation further comprises:~~

~~receiving the position information request;~~

~~generating and transmitting a logistics vendor identity authentication request comprising the second current vendor identification data and the order event identification data to the block chain subsystem (150) according to the position information request;~~

~~receiving an identity authentication successful notice transmitted from the block chain subsystem (150);~~

~~acquiring a second current location of the recipient device (103) after receiving the identity authentication successful notice; and~~

~~utilizing a cipher key to encrypt the second current location of the recipient device (103) to generate an encrypted recipient position;~~

~~wherein the block chain subsystem (150) is arranged to operably receive the logistics vendor identity authentication request, to operably search for the order event recorded in the recipient smart contract stored in the block chain subsystem (150) according to the order event identification data in the logistics vendor identity authentication request, and to operably read the valid vendor identification data from the order event;~~

~~wherein the block chain subsystem (150) provides the identity authentication successful notice only if the second current vendor identification data matches the valid vendor identification data.~~

~~14.~~12. The computer program product (166) of ~~claim 13~~claim 8, wherein the recipient privacy protection operation further comprises:

transmitting the cipher key to the logistics service subsystem (120); and

transmitting the encrypted recipient position to the block chain subsystem (150);

wherein the block chain subsystem (150) is arranged to operably store the encrypted recipient position in the order event recorded in the recipient smart contract;

wherein the logistics service subsystem (120) is arranged to operably read the encrypted recipient position recorded in the order event recorded in the recipient smart contract stored in the block chain subsystem (150);

wherein the logistics service subsystem (120) is arranged to operably utilize the cipher key to decrypt the encrypted recipient position so as to acquire the second current location of the recipient device (103), and to operably transmit the second current location to the logistician device (105).

~~15.~~13. The computer program product (166) of ~~claim 10~~claim 9, wherein the logistics information management system (100) further comprises an e-commerce vender subsystem

(110), arranged to operably create the recipient smart contract in the block chain subsystem (150), and to operably write the delivery destination information and the valid vendor identification data into the recipient smart contract so as to form the order event;

wherein the recipient privacy protection operation further comprises:

transmitting a recipient account request to the e-commerce vender subsystem (110) so that the e-commerce vender subsystem (110) is enabled to create a recipient account correspondingly; and

logging into the e-commerce vender subsystem (110) with the recipient account so as to transmit the delivery destination information to the block chain subsystem (150);

wherein the e-commerce vender subsystem (110) is arranged to operably create the recipient account according to the recipient account request, and to operably create a correlation between the recipient account and a recipient smart contract identification data of the recipient smart contract, so that the recipient device (103) accesses the block chain subsystem (150) according to the correlation;

wherein the e-commerce vender subsystem (110) is arranged to operably request the block chain subsystem (150) to provide the delivery destination information corresponding to the delivery destination information request according to the recipient account and the correlation;

wherein the block chain subsystem (150) is arranged to operably provide the delivery destination information to the e-commerce vender subsystem (110) if the first current vendor identification data matches the valid vendor identification data, and the e-commerce vender subsystem (110) is arranged to operably transmit the delivery destination information to the recipient device (103) according to the correlation.