What is claimed is:

1. A method implemented in a digital property management system, the digital property management system comprising a sender's digital property manager and a recipient's digital property manager, the sender's digital property manager comprising a sender's digital property management module and a sender's transaction node, the recipient's digital property manager comprising a recipient's digital property management module and a recipient's transaction node, the method comprising:

(a) receiving, by the sender's digital property management module, a remittance request comprising a recipient's physical identification;

(b) receiving, from the sender's digital property management module, by the recipient's digital property management module, a token request comprising the recipient's physical identification;

(c) sending, from the recipient's digital property management module, to the sender's digital property management module, a token response comprising a token;

(d) creating, by the recipient's digital property management module, a token mapping that relates the token to a recipient's virtual identification; and

(e) constructing and sending each of a sending transaction, an inter-manager transaction, and a delivery transaction either by the sender's digital property management module to the sender's transaction node of a distributed transaction consensus network or by the recipient's digital property management module to the recipient's transaction node of the distributed transaction consensus network; and

wherein the sending transaction transfers digital property from a sender's virtual wallet to a virtual wallet of the sender's digital property manager; the inter-manager transaction transfers digital property from the virtual wallet of the sender's digital property manager to a virtual wallet of the recipient's digital property manager; and the delivery transaction transfers digital property from the virtual wallet of the recipient's digital property manager to a recipient's virtual wallet.

2. The method of claim 1, wherein

the token request further comprises a sender's digital property management module's signature which is created on the recipient's physical identification by using a message private key of the sender's digital property management module; or

the token request further comprises a sender's digital property management module's identification and a sender's digital property management module's signature which is created on both the identification of the sender's digital property management module and the recipient's physical identification by using a message private key of the sender's digital property management module.

3. The method of claim 2, wherein step (b) further comprises

verifying, by the recipient's digital property management module, the information in the received token request is authentic, by using a message public key of the sender's digital property management module.

4. The method of claim 1, wherein the recipient's physical identification is a recipient's telephone number.

5. The method of claim 1, wherein the token response further comprises an identification of the recipient's digital property management module and a recipient's signature which is created on the token only or on both the identification of the recipient's digital property management module and the token, by using a recipient's message private key.

6. The method of claim 1, wherein the token response comprises an encryption of both the token and an identification of the recipient's digital property management module created by using a message public key of the sender's digital property management module.

7. The method of claim 6, wherein the token response further comprises a recipient's physical identification, an identification of the sender's digital property management module, and a recipient's signature which is created on the recipient's physical identification, the identification of the sender's digital property management module, and the encryption of both the token and the identification of the recipient's digital property management module, by using a recipient's message private key.

8. The method of claim 1, wherein the token further comprises a time stamp.

9. The method of claim 1, wherein step (e) comprises

(e1) receiving, from the sender's digital property management module, by the recipient's digital property management module, an encrypted sending transaction, an inter-manager transaction, and a temporary delivery transaction which comprises the token;

(e2) constructing, by the recipient's digital property management module, a delivery transaction from the received temporary delivery transaction by using the token mapping; and

(e3) sending, from the recipient's digital property management module, to a recipient's transaction node of a distributed transaction consensus network, the encrypted sending transaction, the inter-manager transaction and the delivery transaction.

10. The method of claim 9, wherein the recipient's digital property management module verifies that the token is in a valid token pool before constructing the delivery transaction, and removes the token from the valid token pool after the delivery transaction is committed by the distributed transaction consensus network.

11. The method of claim 9, further comprising:

(f) decrypting the encrypted sending transaction by using a message private key of the recipient's transaction node; and

(g) submitting the sending transaction, the inter-manager transaction, and the delivery transaction to the distributed transaction consensus network.

12. The method of claim 11, wherein the recipient's transaction node recurrently generates a new pair of message public key and message private key, and shares the public key with digital property management modules.

13. The method of claim 12, wherein step (f) comprises

(f1) decrypting the encrypted sending transaction by a current message private key stored in the recipient's transaction node; and

(f2) if step (f1) fails, decrypting the encrypted sending transaction by a last message

private key stored in the recipient's transaction node.

14. The method of claim 1, wherein step (e) comprises:

(e1) receiving, from the sender's digital property management module, by the recipient's digital property management module, an inter-manager transaction and a temporary delivery transaction which comprises the token;

(e2) constructing, by the recipient's digital property management module, a delivery transaction from the received temporary delivery transaction by using the token mapping;

(e3) receiving, from the recipient's digital property management module, by the sender's digital property management module, an encrypted delivery transaction; and

(e4) sending, from the sender's digital property management module, to the sender's transaction node of a distributed transaction consensus network, a sending transaction, the inter-manager transaction and the encrypted delivery transaction.

15. The method of claim 14, wherein the recipient's digital property management module verifies that the token is in a valid token pool before constructing the delivery transaction, and removes the token from the valid token pool after the delivery transaction is committed by the distributed transaction consensus network.

16. The method of claim 14, further comprising:

(f) decrypting the encrypted delivery transaction by a message private key of the sender's transaction node; and

(g) submitting the sending transaction, the inter-manager transaction, and the delivery transaction to the distributed transaction consensus network.

17. The method of claim 16, wherein the sender's transaction node recurrently generates a new pair of message public key and message private key, and shares the message public key with digital property management modules.

18. The method of claim 17, wherein step (f) comprises:

(f1) decrypting the encrypted delivery transaction by using a current message private key

stored in the sender's transaction node; and

(f2) if step (f1) fails, decrypting the encrypted delivery transaction by using a last message private key stored in the sender's transaction node.

19. The method of claim 1, wherein the step (e)comprises:

(e1) generating a label for each sub-transaction in a remittance transaction set;

(e2) encrypting the label with a tracing key;

(e3) submitting each sub-transaction in the remittance transaction set including its encrypted label to the transaction node of of the sender or the recipient of the distributed transaction consensus network; and

wherein the label is used to identify sub-transactions in the remittance transaction set.

20. The method of claim 19, wherein the label comprises:

a set identifier having:

a set number incremented by one after the remittance transaction set is submitted to the distributed transaction consensus network; and

a nonce, wherein a new nonce is generated before the set number is repeated; and

a sequence identifier.

21. The method of claim 19, wherein the remittance transaction set comprises the sending transaction, the inter-manager transaction, and the delivery transaction.

22. The method of claim 19, wherein the step (e) further comprises:

(e4) decrypting the encrypted label with the tracing key that is a symmetric tracing key of the digital property management module of the sender or the recipient which generates the label or with a tracing private key of a network administrator of the distributed consensus network.