CLAIMS:

1. A method for executing secure transactions, the method comprising the steps of:

initiating a secure communication channel between a device (110) having a UICC and a server (140), wherein the secure communication channel is secured using the UICC;

receiving at the server (140) from the device (110) over the secure communication channel, an instruction to execute a transaction;

in response to the received instruction, transmitting from the server (140) to a distributed ledger (150) a request to execute the transaction;

in response to the request, signing the transaction at the distributed ledger (150) using a public and private key pair stored within the distributed ledger (150), wherein the transaction is recorded on the distributed ledger (150) with a wallet identifier associated with the device (110), the method further comprising the step of:

generating the wallet identifier associated with the device (110) on the distributed ledger (150) by verifying the device (110) using a different physical communication channel to the secure communication channel, wherein the different physical channel is SMS.

2. The method of claim 1, wherein the secure communication between the UICC and the server (140) is initiated using a public and private key pair stored on the UICC.

3. The method of claim 2 further comprising the step of generating the public and private key pair within the UICC.

4. The method according to claim 1, wherein the secure communication between the UICC and the server (140) is initiated using a shared secret.

5. The method of claim 4, wherein the secret is shared between the UICC and the server (140) by:

storing the shared secret within the UICC and within a telecommunications network component when the UICC is manufactured; and

the telecommunications network component sending the shared secret to the server (140).

6. The method of claim 5, wherein the telecommunications network component is a home location register, HLR.

7. The method of claim 4, wherein the shared secret is generated using generic bootstrapping architecture, GBA.

8. The method of claim 7, wherein the secret is shared between the UICC and the server (140) by:

generating the shared secret within the UICC and a bootstrapping server function, BSF; and

the BSF sending the shared secret to the server (140).

9. The method according to any previous claim, wherein the transaction is a blockchain transaction.

10. The method according to any of claims 1 to 9, wherein the transaction is a credit card or bank transaction.

11. A system comprising:

a device (110) having a UICC;

a distributed ledger (150) storing a public and private key pair;

a server (140) having one or more processors and memory storing instructions configured to cause the one more processors to:

provide a secure communication channel with the device (110) using the UICC;

receive from the device (110) over the secure communication channel an instruction to execute a transaction; and

in response to the received instruction, transmit from the server (140) to the distributed ledger (150) a request to execute the transaction,

wherein the distributed ledger (150) has one or more processors and memory storing instructions configured to cause the one more processors of the distributed ledger (150) to:

sign the transaction using the stored public and private key pair, in response to a request from the server (140);

record on the distributed ledger (150) a wallet identifier associated with the device (110), wherein the transaction is recorded on the distributed ledger (150) with the wallet identifier associated with the device (110);

generate the wallet identifier associated with the device (110) on the distributed ledger (150) by verifying the device (110) using a different

physical communication channel to the secure communication channel, wherein the different physical channel is SMS.

12. The system of claim 11, wherein the UICC of the device (110) further comprises memory storing a secure applet comprising instructions to respond to verification requests.

13. The system according to any of claim 11 to 12, wherein the transactions are associated with an identifier of the device (110).