CLAIMS

1. A system for signing transactions, the system comprising:

- a first module (100) comprising:

- a communication interface (102) to a public network;

- a controller (105) configured to handle a transaction with a Blockchain network or a transaction server accessible at the public network; and

- a data interface (106) for communicating with the controller (105);

- a second module (200) comprising:

- a random number generator (204) for generating random sequences;

- a secure controller (205) comprising a flash memory (205B) and configured to generate seed words and private keys based on the random sequences generated by the random number generator (204) and to store the seed words and the private keys in said flash memory (205B) and to sign a transaction request using said private keys by generating a signed transaction; and

- a data interface (206, 207) for communicating with the secure controller (205);

- a bridge module (300) comprising:

- a controller (305);

- a data interface (309) for communicating with the controller (305) of the bridge module (300); and

- a switch (310) configured to selectively connect the data interface (309) of the bridge module (300) to either the data interface (106) of the first module (100) or the data interface (206, 207) of the second module (200) such that the data interface (106) of the first module (100) is never connected with the data interface (206, 207) of the second module (200),

wherein the second module is never connected to the public network;

wherein the controller (305) of the bridge module (300) is configured to receive a transaction request from the first module (100), pass the transaction request to the second module (200), receive the signed transaction from the second module (200) and pass the received signed transaction to the first module (100).

2. The system according to claim 1, wherein the switch (310) is a single pole, double throw (SPDT) switch.

3. The system according to any of previous claims, wherein the secure controller (205) of the second module (200) is further configured to store biometric data in said flash memory (205B).

4. The system according to any of previous claims wherein the second module (200) comprises a biometric sensor (203) configured to convert a biometric trail of a person into an electrical signal for transaction authorization.

5. The system according to any of previous claims, wherein the switch (310) is further configured to provide power to the second module (200) only when the data interface (309) of the bridge module (300) is connected with the data interface (206, 207) of the second module (200).

6. The system according to any of previous claims, further comprising a wipe module (401) configured to invoke a wipe function at the second module (200) to delete the stored seed words and private keys, and to wipe all transaction and financial data from the first module (100).

7. The system according to any of previous claims, wherein the second module (200) is integrated with the bridge module (300) in a common housing.

8. The system according to any of previous claims, wherein the first module (100) is integrated with the second module (200) and the bridge module (300) in a common housing.

9. The system according to any of previous claims, wherein the data interface (206, 207) of the second module (200) comprises an input data buffer (206) and an output data buffer (207).

10. The system according to any of claims 1 -9, wherein the random number generator (204) of the second module is a hardware entropy generator.

11. The system according to any of claims 1 -9, wherein the random number generator (204) of the second module is a software entropy generator.

12. A method for signing transactions using a system according to any of previous claims, the method comprising the steps of:

- connecting (604) the first module (100) to the public network;

- setting up (605, 606) transaction details;

- receiving acceptance (608) that said transaction is to be authorized;

- sending (609) the transaction request to the bridge module (300);

- disconnecting (610) the first module (100) from the bridge module (300);

- connecting (611) the bridge module (300) to the second module (200);

- sending (612) the transaction request from the bridge module (300) to the second module (200);

- authorizing (613) the transaction via the second module (200);

- signing (614) the transaction with the private key stored in the second module (200) to generate the signed transaction;

- sending (615) the signed transaction from the second module (200) to the bridge module (300);

- disconnecting (616) the second module (200) from the bridge module (300);

- connecting (616) the first module (100) to the bridge module (300);

- sending (617) the signed transaction from the bridge module (300) to the first module (100); and

- sending (618) the signed transaction from the first module (100) to the Blockchain network or to the transaction server.

13. The method according to claim 12, further comprising, when a user does not authorize a transaction during a predefined number of consecutive attempts at the second module (200), invoking a wipe function at the second module (200) to delete the stored seed words and private keys, and to wipe all transaction and financial data from the first module (100).