CLAIMS:

1. A module for authenticating data transfer between a storage device and a host device, the module comprising:

a processing unit; and

a non-transitory media readable by the processing unit, the media storing instructions that when executed by the processing unit cause the processing unit to:

generate a digital signature for the storage device and the host device based on a unique number associated with the storage device and a unique device identity associated with the host device, wherein the unique number is provided within a secure crypto-processor in the storage device;

determine if the digital signature has been written into a blockchain;

allow encrypted data transfer between the storage device and the host device when it is determined that the digital signature matches a digital signature written into the blockchain; or

prevent data transfer between the storage device and the host device when it is determined that the digital signature does not match a digital signature written into the blockchain.

2. The module according to claim 1 wherein the instruction to prevent data transfer between the storage device and the host device further comprises instructions that when executed by the processing unit cause the processing unit to:

write the digital signature into the blockchain when a pairing instruction is received from an authorized application provided in the host device; and

allow encrypted data transfer between the storage device and the host device when the digital signature has been written into the blockchain.

3. The module according to claim 1 further comprising instructions that when executed by the processing unit cause the processing unit to:

generate, after a random period of time has passed, another digital signature for the storage device and the host device based on the unique number associated with the storage device and the unique device identity associated with the host device;

determine if the another digital signature matches with the digital signature that has been written into the blockchain;

allow encrypted data transfer between the storage device and the host device when it is determined that the another digital signature matches the digital signature written into the blockchain; or

prevent data transfer between the storage device and the host device when it is determined that the another digital signature does not match the digital signature written into the blockchain.

4. The module according to any one of claims 1 to 3, wherein the instructions to generate the digital signature comprises instructions for directing the processing unit to generate the digital signature based on a session key of a Pretty-Good-Privacy (PGP) hybrid cryptosystem.

5. The module according to claim 4 wherein the instructions to allow encrypted data transfer between the storage device and the host device comprises instructions for directing the processing unit to:

encrypt, using public-key cryptography, the PGP session key;

store the encrypted PGP session key in secure locations at the storage device and the host device; and

encrypt all data exchanged between the storage device and the host device using the PGP session key.

6. The module according to any one of claims 1 to 3, wherein the instructions to generate the digital signature comprises instructions for directing the processing unit to:

hash a combination of the unique number associated with the storage device and the unique device identity associated with the host device to generate a hashed message *h*;

converting, using a Boneh-Lynn-Shacham (BLS) signature scheme, the hashed message *h* into a BLS signature σ; and

using the BLS signature σ as the digital signature.

7. The module according to claim 1 further comprising instructions that when executed by the processing unit cause the processing unit to:

receive, from an authorized application provided in the host device, restricted logical block addresses (LBAs);

intercept instructions from the host device to access the restricted LBAs; and

allow the intercepted instructions to access to the restricted LBAs when the instructions have been validated by the module, wherein the instructions are signed by the authorized application using a public key of the storage device and are validated by the module using a private key of the storage device.

8. The module according to any one of claims 1 to 7, wherein the blockchain comprises a private distributed database system provided within the host device.

9. A method for authenticating data transfer between a storage device and a host device comprising:

generating, using a module, a digital signature for the storage device and the host device based on a unique number associated with the storage device and a unique device identity associated with the host device, wherein the unique number is provided within a secure crypto-processor in the storage device;

determining, using the module, if the digital signature has been written into a blockchain;

allowing, using the module, encrypted data transfer between the storage device and the host device when it is determined that the digital signature matches a digital signature written into the blockchain; or

preventing, using the module, data transfer between the storage device and the host device when it is determined that the digital signature does not match a digital signature written into the blockchain.

10. The method according to claim 9 wherein the step of preventing data transfer between the storage device and the host device further comprises the steps of:

writing, using the module, the digital signature into the blockchain when a pairing instruction is received from an authorized application provided in the host device; and

allowing, using the module, encrypted data transfer between the storage device and the host device when the digital signature has been written into the blockchain.

11. The method according to claim 19 further comprising the steps of:

generating, using the module, after a random period of time has passed, another digital signature for the storage device and the host device based on the unique number associated with the storage device and the unique device identity associated with the host device;

determining, using the module, if the another digital signature matches with the digital signature that has been written into the blockchain;

allowing, using the module, encrypted data transfer between the storage device and the host device when it is determined that the another digital signature matches the digital signature written into the blockchain; or

preventing, using the module, data transfer between the storage device and the host device when it is determined that the another digital signature does not match the digital signature written into the blockchain.

12. The method according to any one of claims 9 to 11, wherein the step of generating the digital signature comprises generating the digital signature based on a session key of a Pretty-Good-Privacy (PGP) hybrid cryptosystem.

13. The method according to claim 12 wherein the step of allowing encrypted data transfer between the storage device and the host device comprises the steps of:

encrypting, using the module and using public-key cryptography, the PGP session key;

storing, using the module, the encrypted PGP session key in secure locations at the storage device and the host device; and

encrypting, using the module, all data exchanged between the storage device and the host device using the PGP session key.

14. The method according to any one of claims 9 to 11, wherein the step of generating the digital signature comprises the steps of:

hashing, using the module, a combination of the unique number associated with the storage device and the unique device identity associated with the host device to generate a hashed message *h*;

converting, using the module and using a Boneh-Lynn-Shacham (BLS) signature scheme, the hashed message *h* into a BLS signature σ; and

using the BLS signature σ as the digital signature.

15. The method according to claim 9 further comprising the steps of:

receiving, using the module, from an authorized application provided in the host device, restricted logical block addresses (LBAs);

intercepting, using the module, instructions from the host device to access the restricted LBAs; and

allowing, using the module, the intercepted instructions to access to the restricted LBAs when the instructions have been validated by the module, wherein the instructions are signed by the authorized application using a public key of the storage device and are validated by the module using a private key of the storage device.

16. The method according to any one of claims 9 to 15, wherein the blockchain comprises a private distributed database system provide within the host device.