What is claimed is:

CLAIMS

1. A computer-implemented method for managing user key pairs, the method comprising:

receiving~~, by an identity cryptographic chip (ICC) from a computing device within a blockchain network,~~ (602) a request to store identity information and a user key pair to a memory on ~~the ICC~~an identity cryptographic chip or chip set - ICC -, wherein the request includes the identity information and the user key pair, the request digitally signed with a digital signature, the identity information being biometric information uniquely identifying a user, and the user key pair assigned to the user;

determining~~, by the ICC,~~ (604) that the digital signature is authentic based on a public authorization key pre-stored in the memory;

~~receiving, by the ICC, encrypted data comprising an encryption of~~ encrypting (606) the identity information and ~~of~~ the user key pair; and

storing~~, by the ICC,~~ (608) the encrypted identity information and the encrypted ~~data~~user key pair to the memory~~;~~

~~generating, by the ICC, a token to provide temporary authorization to the user to perform cryptographic operations;~~

~~performing, by the ICC, the cryptographic operations, during a time limit authorized by the token; and~~

~~transmitting, by the ICC, a result of the cryptographic operations~~.

2. The computer-implemented method of claim 1, further comprises:

initializing the ICC by pre-storing the public authorization key and a private authorization key, wherein the public authorization key and the private authorization key are an asymmetric-key pair assigned to a master user of the ICC.

3. The computer-implemented method of claim 2, wherein initializing the ICC further comprises storing identity authentication code executable to authenticate the user based on the identity information.

4. The computer-implemented method of either claim 2 or claim 3, wherein initializing the ICC further comprises:

storing first cryptographic operation code executable to add the digital signature based on the private authorization key; and

storing second cryptographic operation code executable to perform file encryption or file decryption based on the user key pair.

5. The computer-implemented method of claim 4, wherein the request for storing identity information and the user key pair is a first request, the identity information is first identity information, the digital signature is a first digital signature, and the computer-implemented method further comprises:

receiving second identity information and a second request for adding a second digital signature to a file;

authenticating the second request based on matching the second identity information to the first identity information; and

adding the second digital signature to the file based on the first cryptographic operation code and a private key of the user key pair.

6. The computer-implemented method of claim 4, wherein the request for storing identity information and the user key pair is a first request, the identity information is first identity information, and the computer-implemented method further comprises:

receiving second identity information and a second request for encrypting or decrypting a file;

authenticating the user based on matching the second identity information to the first identity information; and

performing the encryption or decryption based on the second request, the second cryptographic operation code, and a public key or a private key of the user key pair.

7. The computer-implemented method of any of the preceding claims, wherein the ~~identity information is biometric information.~~

~~8. The computer-implemented method of any of the preceding claims, wherein the~~ memory is a programmable read-only memory ~~(~~ PROM~~),~~ ~~-~~, an electrically erasable PROM or a flash memory, and wherein the identity information and the user key pair are stored in separate storage units of the memory.

~~9~~8. A system for managing user key pairs, comprising:

~~one~~ an identity cryptographic chip or ~~more processors;~~chip set - ICC - (100); and

one or more computer-readable memories coupled to the ~~one or more processors~~ICC and having instructions stored thereon that are executable by the ~~one or more processors~~ICC to perform the method of any one of claims 1-~~8~~7.

~~10~~9. An apparatus for managing user key pairs, the apparatus comprising a plurality of modules including an identity cryptographic chip or chip set - ICC - (100) for performing the method of any one of claims 1-~~8.~~7.