

## CRYPTO SIM AND METHOD THEREFOR

### Field of the Invention

**[0001]** The present invention relates to cryptocurrency. More specifically, the present invention relates to a system and method for SIM-based cryptocurrency holder.

### Background

**[0002]** The boom of cryptocurrency has led to the great interest of keeping the digital currency securely. Carriers of the digital currency are well known as digital wallets or simply wallets are available in various forms classified as hot wallet and cold wallet in general. The hot and cold wallets differ on whether they are connected to the internet. Hot wallets are usually considered less secure cryptocurrency wallets because of the risk of internet access, they are however more user-friendly as they are accessible everywhere.

**[0003]** Mobile wallet in particular stores the cryptocurrencies on the user's personal mobile device. Such mobile wallets usually require a mobile app, i.e. a program module installed on the mobile device, to access the cryptocurrencies. It offers a great flexibility to user whereby their cryptocurrency can be accessed everywhere any time. Some mobile wallets may keep the ledgers in-app as hot wallet does. Others may keep the ledgers remotely centralized server, whereby the app serves only as a means to remotely access the ledgers. In either way, mobile devices are considered insecure device as the devices are often open to malware, key loggers and viruses. When the user's mobile is maliciously compromised, such in the case of being stolen, nothing could save the credits stored in the mobile wallet.

**[0004]** Therefore, it is desired that to provide more secure way of storing/holding cryptocurrency on personal mobile devices.

### Summary

**[0005]** In one aspect of the present invention, there is provided a mobile device for handling cryptocurrency thereon, wherein the mobile device is operationally in communication with a Bearer Independent Protocol (BIP) based server. The mobile device comprises a Subscriber Identity Module (SIM); an applet deployed on the SIM, wherein the applet is adapted to operationally send instructions to the BIP based server; and a cryptocurrency module deployed on the mobile device for holding cryptocurrency therein, wherein the cryptocurrency module operationally executes the applet of the SIM to connect to the BIP based server for authentication based on an International Mobile Subscriber Identity (IMSI) registered to the SIM. The operations and transactions on the cryptocurrency module is authenticated under the BIP based server through the applet.

**[0006]** In one embodiment, the communication between the applet and the BIP based server is encrypted with key pairs. In another embodiment, the cryptocurrency module is adapted to work in association with the applet for securing data encrypted on the cryptocurrency module. The applet may operationally be triggered to prompt user for inputting a prescribed passphrase for operating cryptocurrency module.

**[0007]** In a further embodiment, the cryptocurrency module is a mobile app.

**[0008]** In another aspect, a vault server for authenticating transactions from the aforesaid cryptocurrency module, wherein the vault server is a BIP based server adapted for authenticating the SIM based on the IMSI registered to the SIM, the authentication of the SIM in turns authenticate transactions initiated by the cryptocurrency module.

**[0009]** In another embodiment, the vault server resides at a service provider issuing the SIM. Alternatively, the vault server resides at a third-party service provider, wherein the third-party service provider obtained the IMSI records from a mobile operator issuing the SIM to authenticate the SIM.

**[0010]** In a further embodiment, the vault server operationally serves as a gateway of authenticating all transactions by the cryptocurrency module.

**[0011]** In another aspect of the present invention, there is also provided a Subscriber Identity Module (SIM) for deploying on a mobile device having a cryptocurrency module. The SIM comprises an applet adapted to operate in conjunction with the cryptocurrency module, wherein the applet instructs the aforesaid vault server to obtain authentication of cryptocurrency transactions initiated by the cryptocurrency module.

**[0012]** In yet another aspect, there is provided a method for handling cryptocurrency on a mobile device, wherein the mobile device comprises a Subscriber Identity Module (SIM). The mobile device operationally in communication with a Bearer Independent Protocol (BIP) based server. The method comprises deploying an applet on the SIM; activating a cryptocurrency module deployed on the mobile device, the cryptocurrency module executes the applet of the SIM to send instructions to the BIP based server; authenticating operations and transactions on the cryptocurrency module based on an International Mobile Subscriber Identity (IMSI) registered to the SIM; and accessing and transacting cryptocurrency stored on the cryptocurrency module upon successful authentication of the SIM.

**[0013]** In one embodiment, the method further comprises encrypting communications between the applet and the BIP server via key pairs.

**[0014]** In another embodiment, where in the method further comprises prompting user for inputting a prescribed passphrase for operating cryptocurrency module through the applet.

#### Brief Description of the Drawings

**[0015]** This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

**[0016]** **FIG. 1** illustrates a Subscriber-Identification-Module (SIM)-based cryptocurrency carrier system in accordance with an embodiment of the present invention;

**[0017]** **FIG. 2** illustrates a Subscriber-Identification-Module(SIM)-based cryptocurrency carrier system in accordance with an alternative embodiment of the present invention;

**[0018]** **FIG. 3A** illustrates a new crypto-SIM registration in accordance with an embodiment of the present invention;

**[0019]** **FIG. 3B** illustrates a crypto-transaction authentication process on a cryptocurrency module on a mobile device in accordance with an embodiment of the present invention;

**[0020]** **FIG. 3C** exemplifies several screenshots which can be adapted by the embodiment of the present invention;

**[0021]** **FIG. 4** illustrates the multi-factors authentication in accordance with an embodiment of the present invention;

**[0022]** **FIG. 5A-5E** exemplifies some mockup screenshots of account details of the cryptocurrency wallet in accordance with embodiments of the present invention;

**[0023]**        **FIG. 6A** illustrates a flow diagram in accordance with an embodiment of the present invention;

**[0024]**        **FIG. 6B** illustrates a diagram showing key generations and exchanges in accordance with an embodiment of the present invention; and

**[0025]**        **FIG. 7** illustrates a flow diagram for authenticating crypto-transactions in accordance with another embodiment of the present invention.

### Detailed Description

**[0026]**        In line with the above summary, the following description of a number of specific and alternative embodiments are provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

**[0027]**        **FIG. 1** illustrates a Subscriber-Identification-Module(SIM)-based cryptocurrency carrier system in accordance with an embodiment of the present invention. The system is adapted to provide secure access to owner's cryptocurrency wallet. In one embodiment, the system provides a mobile device application or app for carrying users' cryptocurrencies.

**[0028]**        The system comprises a mobile device **100** operationally connecting to a vault server **105** for establishment of authentication when transacting with a crypto-transaction terminal **108**. The mobile device **100** is a SIM-based smart device comprises a SIM card **117** and a cryptocurrency module **119** installed thereon. The mobile device **100** can be any SIM based mobile devices, such as a smartphone device, or tablet or

mobile computing devices capable of deploying applications or apps thereon. The cryptocurrency module **119** is an application adapted for carrying cryptocurrency balance in a secure manner. It is desired that the cryptocurrency module can be adapted to record and carry multiple cryptocurrencies and transactions thereof. Such cryptocurrency carrier module also known as cryptocurrency wallet, or simply crypto-Wallet. The cryptocurrency module **119** is operationally connectable to the crypto-transaction terminal **108** to carry out any cryptocurrency transactions, or transactions that require exchange of cryptocurrency. The crypto-transaction terminal **108** can be a cryptocurrency exchange, a cryptocurrency sender/receiver, or any direct merchant transacting in cryptocurrencies. The present system offers a platform for transacting cryptocurrencies at a highly secure manner through the multi-authentication mechanism.

**[0029]** According to one embodiment, the crypto-transaction terminal **108** can be a crypto currency exchange. In other embodiments, it can be other transaction terminals that include merchant, a crypto wallet, or other available means adapted for transceiving cryptocurrencies of any kind.

**[0030]** The SIM card **117** comprises a unique serial number (ICCID), an international mobile subscriber identity (IMSI) number, and an applet **117**. In most cases, the IMSI is issued by the service provider or telco or a cellular network to identify a specific user or subscriber. Typically, the IMSI is registered and recorded together the subscriber's personal identity, and it is unique to one person only. The ICCID is also a unique ID number that assigned to each individual SIM card. The ICCID is stored on the SIM card, and in most case, also printed or engraved on the SIM card. In one embodiment, the ICCID may be defined by the ITU-T recommendation E.118.

**[0031]** At any one time, one IMSI is linked to only one subscriber and one ICCID is only connected to one IMSI. When the SIM card is to be replaced for whatever

reasons, the relevant service provider or operator may disable the card and void the ICCID and link a new ICCID of the new SIM card to the IMSI owned by the subscriber.

**[0032]** The applet **117** is deployed on the SIM card **100** before prior to issuance. It is well known in the art that SIM card or SIM module are capable of pre-deploying with applets thereon to provide various functionalities. In this case, the applet **117** can be a pre-added applet to provide cryptocurrency authentication function of the present invention. The applet **117** provides instructions or commands to operationally communicate with the vault server **105** for authentication. It is desired that, in accordance with an embodiment of the present invention, the user authentication of a cryptocurrency transactions is performed on the SIM card only. Also preferably, the applet **117** provides a Bearer Independent Protocol (BIP) commands to the vault server **105** to establish an authentication on the SIM card **100** to gain access and connection.

**[0033]** The Bearer Independent Protocol (BIP) is a mechanism by which mobile phone provides SIM with access to the data bearer supported by the mobile phone (e.g. Bluetooth, IrDA, etc.) and the network (e.g. GPRS, 3G, etc.). BIP is considered one of the most secure way of establishing authentication between the SIM card and the network provider and thereby authenticating the credential of the user operating the mobile device **100**.

**[0034]** Operationally, user of the mobile device **100** executes the cryptocurrency module **119** thereon, usually by just tapping on the corresponding icon on the mobile device **100** touch sensitive screen. The cryptocurrency module **119** triggers the SIM card **115** to activate the applet **117** and prompts the user to input a user PIN through a screen dialogue. The user PIN can be any predefined passphrase or the like, or alternatively biometric identifications.

**[0035]** The applet **117** then initiates to communicate with the vault server **105** through a secure channel to verify the user credentials to continue the usage of the cryptocurrency module **119**. The verification of the user credential according to the embodiments of the present invention undergoes multi-factors authentication to confirm the authenticity the of the user.

**[0036]** Further in the present embodiment, the vault server **105** is a BIP based server. When valid PIN is inputted, the applet **117** connects to the vault server **177** to authenticate the crypto-SIM. The vault server **105** authenticates the crypto-SIM card **115** based on an IMSI, and once authenticated, returns an authorization token to the applet **117**. Through the cryptocurrency module **119**, the authorization token is transmitted to the crypto-transaction terminal **108**. The crypto-transaction terminal **108** synchronizes the received authorization token against that issued by the vault server **105** to open up a secure transaction section. The secure transaction section can only be confirmed and valid if and only if when token from the crypto-SIM card **115** is synchronized the token received at the crypto-transaction terminal **108**. When the token received at the crypto-transaction terminal **108** is not synced and paired, it shall be concluded that the crypto-transaction is not valid and should be terminated.

**[0037]** In the embodiments of the present invention, the system requires the cryptocurrency module **119** to be pre-paired with a specific SIM card **117** embedded with the applet **117**. The SIM card **117** is often pre-paired at the card issuance side by the issuer, which is generally the telco or the service provider. Should the mobile device **100** is inserted with another SIM card not paired with the module, the cryptocurrency module **119** ceases to execute further, thereby terminating any cryptocurrency transactions. In the event of loss or damage SIM card **117**, user is required to obtain a duplicate replacement SIM card through telco or service provider, and pairing the new

crypto-SIM to the existing user would be required for proper functionality of the SIM-based cryptocurrency transactions. The re-pairing process is required to re-connect the user credential and identity to the new crypto-SIM card, and at the same time abandoning or terminating the connection with the previously connected crypto-SIM card. In other word, ownership of the new crypto-SIM is required to be validated. Accordingly, in concert with the user PIN or passphrase on the SIM card **117**, the multi-factor combinations of SIM, app module and token authentications would better secure the cryptocurrency transactions over the air.

**[0038]** The cryptocurrency module **115** can also be referring to any app that is adapted to transact cryptocurrency in-app.

**[0039]** In one embodiment of the present invention, one subscriber may register own more than one IMSI.

**[0040]** For avoidance of doubt, the SIM card referred herein include embedded SIM, or any subscriber-based system adapted for storing and authenticating mobile subscriber identity (MSI), typically but not limiting to mobile phone number issued by telco, or service provider. For purpose of the present application, SIM card shall cover also Universal Integrated Circuit Card or UICC, or other variants without departing the scope of the present invention.

**[0041]** **FIG. 2** illustrates a SIM-based cryptocurrency carrier system **200** in accordance with another embodiment of the present invention. The SIM-based cryptocurrency carrier system **200** is essentially the same as the cryptocurrency carrier system **100** of FIG. 1 except that while the SIM card is operationally connected to the telco or service provider for authentication known in the art, whilst the applet **117** is adapted to specifically connect to a dedicated or third party vault server **250** for dedicated BIP authentication for purpose of the cryptocurrency transactions.

**[0042]** In one embodiment, the dedicated or third-party vault server **250** acquires the relevant user credentials from the authorized service provider or telco issuing the crypto-SIM to carry out embodiments of present invention.

**[0043]** The above embodiments have illustrated overall structure and configurations of the present invention, whereby the crypto-currency module **119** connects to the crypto-transaction terminal **108** directly to perform the cryptocurrency transactions. In another embodiment, the direct interaction and communication between the crypto-currency module **119** and the crypto-transaction terminal **108** is avoided. It is desired that any cryptocurrency transactions is established only through the vault server **105, 250** for better secured transactions.

**[0044]** **FIG. 3A** illustrates a new crypto-SIM registration in accordance with an embodiment of the present invention. As the crypto-SIM card is inserted into a mobile device and the mobile device is powered up, a prompt appears to enter the user/subscriber credentials, such as the registered name, for registration. The user credentials are wrapped into an encrypted-string and send through a secure BIP channel to a vault server **310**. Upon registration, user will be prompted whether to activate the crypto-SIM service. For the purpose of the present invention, the crypto-SIM service refers to the secure cryptocurrency transaction service offered under the present invention. Activating the crypto-SIM service in turn activating an applet **117** embedded on the SIM card allowing the mobile device **300** to enable cryptocurrency transactions on the mobile device **300**.

**[0045]** Upon enabling the crypto-SIM service, user is prompted to input a new PIN. As shown, the PIN can be a multi-character PIN or passphrase, and user will be prompted to re-input the PIN for confirmation. The PIN or the passphrase is stored on

the crypto-SIM, whereby an obfuscated copy of the PIN or the passphrase is also sent to the vault server for safe keeping.

**[0046]** As mentioned above, the PIN is a user defined authentication code. Such authentication code can be any type of passphrase. When desired, the user authentication to access the crypto-currency module can be biometric identifications or other known access control means. For the purpose of this application, the user authentication code can also be hereinafter referred as user authentication factor.

**[0047]** Referring back to the **FIG. 3A**, if the SIM card **115** is newly issued and used for the first time, the cryptocurrency module **119** first initiates a dialog for setting up the newly issued card. The setting up is fairly straightforward, i.e. user to input a user PIN, which will be used in the future for identity verification until otherwise changed by the owner. The PIN or the user authentication factor is also stored the vault server **105** as an obfuscated copy for safe keeping upon registration for the first time. In case of the SIM card replacement, the same PIN or passphrase is recovered from the vault server **105** for authentication.

**[0048]** **FIG. 3B** illustrates a crypto-transaction authentication process on a cryptocurrency module on a mobile device in accordance with an embodiment of the present invention. The mobile device already enabled the crypto-SIM service as illustrated in **FIG. 3A**. When user of the mobile device opens the cryptocurrency module, the user is first prompted with a PIN. The PIN is the pre-recorded multi-character PIN code. Once a valid and correct PIN code is inputted, the PIN is encrypted and sent through a secure BIP channel to the vault server for verification.

**[0049]** **FIG. 3C** exemplifies several screenshots which can be adapted by the embodiment of the present invention. The screenshots exemplify a new user registration process. The first screen prompts user to input email address as user name for logging

into the system, and new password for authentication. Typically, the user will be asked to re-type the password to reaffirm the password. The next screenshot prompt user to check the registered email to verify the ownership. Verification of the user credential is well known in the art and it should not be taken as limitations. Other known ways of verifying user credentials may also be desired. In other embodiment, the user credentials may be biometrics. For example, the user ID may be user phone number, which can be verify through keying a one-time password (OTP) received through a SMS.

**[0050]** Once after the user checks the email and verify the email, user is required to enter the SIM's PIN that was inputted when the crypto-SIM service was enabled. When a correct crypto-SIM service PIN is input, user may access the cryptocurrency wallet.

**[0051]** As illustrated above, the present invention offers multi-factors authentications to protect against cryptocurrency theft. Such system is simple to implement on a SIM-based device. **FIG. 4** illustrates the multi-factors authentication in accordance with an embodiment of the present invention. Specification, the multi-factors authentication includes a phone PIN authentication, a SIM-PIN authentication, and a BIP-based authentication.

**[0052]** **FIG. 5A-5E** exemplifies some mockup screenshots of account details of the cryptocurrency wallet in accordance with embodiments of the present invention. **FIG. 5A** is a screenshot of transaction history under that wallet. **FIG. 5B** shows a screenshot when the user is sending cryptocurrency to other account. **FIG. 5C** shows a following screenshot where the user is asked for the crypto-SIM PIN to confirm the transaction. **FIG. 5D** shows a screenshot where user is requesting for cryptocurrency. A QR code can be presented on the screen and send to the cryptocurrency sender. **FIG. 5E** shows an overview of all the cryptocurrencies kept under the cryptocurrency wallet.

**[0053]** **FIG. 6A** illustrates a flow diagram in accordance with an embodiment of the present invention. The flow diagram illustrates a user authentication process when the crypto-app is executed by a user. The crypto-app activates the crypto-applet of the crypto-SIM, at step **602**, user enters a predefined passphrase into a crypto-app deployed on the user's mobile device. The mobile device comprises a crypto-SIM that serves as a gateway of identifying and authenticating the mobile device. Supposedly, only the true owner of the crypto-currency wallet possesses the correct user authentication factor or passphrase. Failure in providing the correct passphrase ceases the operation of the crypto-app. As the correct passphrase is received and authenticated by the applet of the crypto-SIM, at step **604**, the crypto-SIM generates a pair of keys, whereby the private key is stored on the crypto-SIM itself, and at step **606**, the public key will be sent to the crypto-SIM (CS) blockchain server.

**[0054]** **FIG. 6B** illustrates a diagram showing key generations and exchanges in accordance with an embodiment of the present invention. Key pairs are generated at various level. Foremost, at user level, a user public key and a user private key are generated for encrypting passphrase. The user public key is sent and stored at a vault server and the user private key is stored on the crypto-SIM card. The crypto-app or cryptocurrency wallet generates an app key pair, wherein an app public key is also stored on the crypto-SIM and an app private key is stored on the crypto-app. The cryptoSIM (or the applet deployed therein) generates a cryptoSIM-app key-pair wherein a cryptoSIM-app public key will be stored on the crypto-app or the cryptocurrency wallet and a crypto-SIM-app private key will be stored on the crypto-SIM itself. Further, the crypto-SIM generates a cryptoSIM-server key-pair wherein a cryptoSIM-server public key is stored in the vault server and the cryptoSIM-server private key is stored in the crypto-SIM itself. The vault server generates a server-cryptoSIM key pair wherein a

server-cryptoSIM public key is stored on the cryptoSIM and a server-cryptoSIM private key is stored on the vault server. These key pairs are used to encrypt and decrypt the transmissions and data stored on the respective location. Without a corresponding private key, the data remains encrypted and not accessible to third party.

**[0055]** For security purposes, all information stored and transmitted are encrypted with their respective keys. Keys encryptions and decryptions are well known in the art and therefore, will not be described herein.

**[0056]** **FIG. 7** illustrates a flow diagram for authenticating crypto-transactions in accordance with another embodiment of the present invention. The crypto-transactions can be established through means that comprises a crypto-app **702**, a crypto-SIM **704**, a crypto-SIM (CS) server **706**. In this embodiment, cryptocurrency transaction involving third party is carried out through the CS server **706** only. The crypto currency transactions shall be initiated through the crypto-app **702** at step **721**, wherein the request to initiate transaction is sent to the crypto-SIM **704**. A crypto applet deployed on the crypto-SIM **704** is executed to prompt user for inputting a passphrase to use the crypto-app **702** at step **724**. At step **726**, the user enters the prerecorded passphrase to the crypto-app **702** and the passphrase is verified by the crypto applet. At step **728**, the crypto applet verifies the authenticity of the passphrase and send an acknowledgement to the crypto-app **702** at step **728**. Between the crypto-app and the crypto applet, the transmissions and data exchanged are encrypted with key pairs.

**[0057]** As the passphrase is verified and authenticated at the crypto-applet, the crypto-applet connects to the remote CS server **706** for further authentication. The authentication process is carried out based on the Bearer Indpende Protocol (BIP) to authenticate the crypto-SIM **704**, to verify the authenticity of the crypto-SIM **704**. At step **732**, the crypto-apple of the crypto-SIM **704** forward the transaction request to the

CS server **706** along with other information. The other information includes IMSI, among others. Similarly, the transactions between the crypto-SIM **704** and the CS server **706** are encrypted with key pairs.

**[0058]** At step **734**, the CS server **706** verifies the authenticity of the crypto-SIM request, and when verified and authenticated to be genuine, the CS server **706** sends acknowledgement to the crypto-SIM **704** to authorize transactions on the mobile device carrying the crypto-SIM by the user.

**[0059]** The crypto-app **702**, at step **711**, sends a transaction request the crypto-SIM **704**. A crypto-applet deployed on the crypto-SIM **704** is executed and at step **721**, the transaction request is forwarded to the CS blockchain server **706** to authenticate the transaction. Once authenticated, at step **722**, the CS blockchain server **706** sends acknowledgment to the crypto-SIM **704** and at step **712**, the crypto-SIM **704** sends acknowledgement to the crypto-app **702** to authenticate crypto-transactions on the mobile device.

**[0060]** The transactions referred herein include any usage activity on the crypto-app **702**, such as balance checking, send/receive cryptocurrencies on the crypto-app.

**[0061]** For inter-transactions, such as balance checks, the authentication process shall end between the crypto-app **702**, crypto-SIM **704** or the crypto-applet, and the CS server **706**. If the user is performing any intra-transactions, such transactions will only be authorized through the CS server **706**, as long as the transactions are authorized at the user level, the SIM card level and the CS server level together. Any unauthorized transaction at any level will cease the transactions.

**[0062]** For avoidance of doubt, the transactions referred herein include any one or more of the following: balance checking, buying crypto-currency, selling crypto-currency, receiving crypto-currency, sending crypto-currency, and etc.

**[0063]** In one embodiment of the present invention, the crypto-SIM, or more specifically, the applet deployed on the crypto-SIM is responsible for the authentication of the user credential by the support of the vault server or the CS blockchain server. The vault server or the CS blockchain server is responsible to store the required and relevant user credentials thereon, and through the communication and handshake between the crypto-SIM and the vault server to provide a secure cryptocurrency transaction.

**[0064]** While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention.

## Claims

1. A mobile device for handling cryptocurrency thereon, wherein the mobile device is operationally in communication with a Bearer Independent Protocol (BIP) based server, the mobile device comprising:

a Subscriber Identity Module (SIM);

an applet deployed on the SIM, wherein the applet is adapted to operationally send instructions to the BIP based server; and

a cryptocurrency module deployed on the mobile device for holding cryptocurrency therein, wherein the cryptocurrency module operationally executes the applet of the SIM to connect to the BIP based server for authentication based on an International Mobile Subscriber Identity (IMSI) registered to the SIM,

wherein operations and transactions on the cryptocurrency module is authenticated under the BIP based server through the applet.

2. The mobile device according to Claim 1, wherein the communication between the applet and the BIP based server is encrypted with key pairs.

3. The mobile device according to Claim 1, wherein the cryptocurrency module is adapted to work in association with the applet for securing data encrypted on the cryptocurrency module.

4. The mobile device according to Claim 3, wherein the applet is operationally triggered to prompt user for inputting a prescribed passphrase for operating cryptocurrency module.

5. The mobile device according to Claim 1, wherein the cryptocurrency module is a mobile app.

6. A vault server for authenticating transactions from a cryptocurrency module of any one of Claims 1-5, wherein the vault server is a BIP based server adapted for

authenticating the SIM based on the IMSI registered to the SIM, the authentication of the SIM in turns authenticate transactions initiated by the cryptocurrency module.

7. The vault server according to Claim 6, wherein the vault server resides at a service provider issuing the SIM.

8. The vault server according to Claim 7, wherein the vault server resides at a third-party service provider, wherein the third-party service provider obtained the IMSI records from a mobile operator issuing the SIM to authenticate the SIM.

9. The vault server according to Claim 6, wherein the vault server operationally serves as a gateway of authenticating all transactions by the cryptocurrency module.

10. A Subscriber Identity Module (SIM) for deploying on a mobile device having a cryptocurrency module, the SIM comprising:

an applet adapted to operate in conjunction with the cryptocurrency module, wherein the applet instructs a vault server of any one of claims 6-9 to obtain authentication of cryptocurrency transactions initiated by the cryptocurrency module.

11. A method for handling cryptocurrency on a mobile device, wherein the mobile device comprises a Subscriber Identity Module (SIM), the mobile device operationally in communication with a Bearer Independent Protocol (BIP) based server, the method comprising:

deploying an applet on the SIM;

activating a cryptocurrency module deployed on the mobile device, the cryptocurrency module executes the applet of the SIM to send instructions to the BIP based server;

authenticating operations and transactions on the cryptocurrency module based on an International Mobile Subscriber Identity (IMSI) registered to the SIM; and

accessing and transacting cryptocurrency stored on the cryptocurrency module upon successful authentication of the SIM.

12. The method according to Claim 11, further comprising encrypting communications between the applet and the BIP server via key pairs.

13. The method according to Claim 11, prompting user for inputting a prescribed passphrase for operating cryptocurrency module through the applet.