Summary

[0012] The following relates generally to blockchain technologies, and more specifically to computer systems, methods, and sub-networks for making secure blockchain transactions, while allowing current or future compliance requirements and various policies.

[0013] In a first aspect, the present disclosure provides a system for performing a secure blockchain transaction, the system comprising: a terminal for generating the blockchain transaction, the terminal configured to operate in a first mode and a second mode; and a switch connector for preventing the terminal from operating in the first mode and the second mode simultaneously; wherein, when the terminal is in the first mode, the terminal is connected via a network to a system provider server, the system provider server in communication with at least one blockchain device; wherein, when the terminal is in the second mode, the terminal is in communication with a cold storage device; wherein the cold storage device is configured to store a private key for signing the blockchain transaction; and wherein the terminal is configured to allow the blockchain transaction to be signed on the cold storage device using the private key.

[0014] The switch connector may include a hardware switch.

[0015] The switch connector may include a software switch.

[0016] The signed transaction may be signed by at least one other party prior to sending the signed blockchain transaction to the blockchain devices.

[0017] Other parties may include a system provider.

[0018] The system provider server may be in communication with at least one service provider device.

[0019] In a second aspect, the present disclosure provide a terminal for performing a secure blockchain transaction, the terminal comprising: a processor for generating an unsigned blockchain transaction; a cold storage communication port for transmitting the unsigned blockchain transaction to a cold storage device, wherein the cold storage device stores a private key for signing the unsigned blockchain transaction, and wherein the

terminal receives a signed blockchain transaction from the cold storage device; a network communication port for transmitting the signed blockchain transaction to a system provider server over a network, wherein the system provider server is in communication with at least one blockchain device; and a switch connector for selectively disabling either the cold storage communication port or the network communication port such that the private key is not exposed to the network.

[0020] The switch connector may include a hardware switch.

[0021] The switch connector may include a software switch.

[0022] The terminal may be further configured to restrict inbound and outbound communication with the system provider server.

[0023] In a third aspect, the present disclosure provides a cold storage device for performing a secure blockchain transaction of a digital asset over a network, the cold storage device comprising: a memory storing a private key of at least one cold storage wallet, the private key for signing an unsigned blockchain transaction; a communication interface for receiving an unsigned blockchain transaction from a terminal, the terminal disconnected from the network; and wherein the communication interface transmits a signed blockchain transaction to the terminal, the terminal disconnected from the network; and a connection to a processor configured to sign the unsigned blockchain transaction using the private key.

[0024] The communication interface may use at least one communication mechanism selected from the group consisting of encrypted Bluetooth, near-field communication, Wi-Fi, optical communication, wired communication, and thermal emission.

[0025] The processor may be further configured to generate the cold storage wallet.

[0026] The processor may be further configured at the generation of the cold storage wallet.

[0027] The cold storage wallet may be a hierarchical deterministic wallet.

[0028] The cold wallet may be a multi-signature wallet.

[0029] The multi-signature wallet may require the signature of at least two parties.

[0030] In a fourth aspect, the present disclosure provides a method of performing a secure blockchain transaction over a communication network, the method comprising: generating an unsigned blockchain transaction using a terminal, the terminal having an online mode and an offline mode; transmitting, in the offline mode, the unsigned blockchain transaction from the terminal to a cold storage device, the cold storage device storing a private key for signing the unsigned blockchain transaction; signing the unsigned blockchain transaction on the cold storage device using the private key; transmitting the signed blockchain transaction from the cold storage device to the terminal; switching the terminal from the offline mode to the online mode; and transmitting the signed blockchain transaction from the terminal to a system provider server via the communication network while in the online mode, the system provider server is in communication with a plurality of blockchain computers.

[0031] The method may include signing the transmitted signed transaction with a second private key according to a multi-signature authentication process.

[0032] Signing the transmitted signed transaction may be performed on the system provider server.

[0033] The switching may be performed using a switch connector.

[0034] Other aspects and features will become apparent, to those ordinarily skilled in the art, upon review of the following description of some exemplary embodiments.

Brief Description of the Drawings

[0035] The drawings included herewith are for illustrating various examples of articles, methods, and apparatuses of the present specification. In the drawings:

[0036] Figure 1 is a schematic diagram of a system for performing secure blockchain transaction of a digital asset, according to an embodiment;

[0037] Figure 2 is a block diagram of a terminal of the system of Figure 1;