

[0060] At block 560, the computer system communicates the signed distributed ledger transaction to a distributed ledger, and the method terminates.

[0061] Fig. 6 depicts a flow diagram of one illustrative example of method 600 of cryptographic key management, in accordance with one or more aspects of the present disclosure. Method 600 and/or each of its individual functions, routines, subroutines, or operations may be performed by one or more general purpose or specialized computer systems (e.g., example computer system 1000 of Fig. 13). In some implementations, method 600 may be performed by a single processing thread. Alternatively, method 600 may be performed by two or more processing threads, each thread executing one or more individual functions, routines, subroutines, or operations of the method. In some implementations, the processing threads implementing method 600 may be synchronized (e.g., using semaphores, critical sections, and/or other thread synchronization mechanisms).

[0062] At block 610, the computer system implementing the method receives a private key associated with a user.

[0063] At block 620, the computer system causes an HSM to generate a public address by performing a cryptographic operation on the private key.

[0064] At block 630, the computer system encrypts the private key and the public address.

[0065] At block 640, the computer system communicates the private key to the user.

[0066] At block 650, the computer system stores, in a secure database, the encrypted private key in association with the public address, and the method terminates.

[0066a] Fig. 7 depicts a high-level architecture of an example secure digital wallet processing system. As illustrated, the secure wallet processing system can communicate with a plurality of users, a software development kit (SDK), a blockchain network, and crypto exchanges.

[0066b] Fig. 8 depicts a high-level functional diagram of an example secure digital wallet processing system. As illustrated, the secure wallet processing system can support various features described herein, e.g., multi-signature, segregated wallets, SDK, de-centralized exchange, off-chain transactions.

[0066c] Fig. 9 depicts a high-level functional diagram of an example secure digital wallet processing system where the features illustrated in Fig. 8 are shown on the left-hand side and the functionalities associated with the features are shown on the right-hand side.

[0066d] Fig. 10 depicts a high-level interaction diagram of an example secure digital wallet processing system featuring a secure storage, multi-signature, and tokenization. The crypto asset

keys are generated and stored in the HSM. Encrypted tokens are then sent to and stored in the device of a consumer to provide key access. A bank may support fraud prevention rules. Recovery keys remain safe in cold HSM even if exchange is hacked. Peer to peer transaction may be signed with the HSM. Tokenization mitigates fraud risk to protect crypto assets.

[0066e] Fig. 11 depicts a buy order workflow performed by an example secure digital wallet processing system. User requests transaction through UI. Wallet purchases crypto assets via crypto exchange. Wallet and exchange sign blockchain. Assets are moved into secure vault, then tokenized. Token encrypted, public/private keys are generated. Encrypted token and the keys are stored in a warm or cold wallet. User receives confirmation of trade and secured storage.

[0066f] Fig. 12 depicts a sell order workflow performed by an example secure digital wallet processing system. User requests transaction through UI. Assets stored in a warm or cold wallet are un-encrypted. Un-encrypted assets are detokenized within secure area. Asset information (including keys) sent to third party crypto exchange. Exchange confirms transaction. Wallet and exchange sign blockchain. User receives confirmation of sale with proceeds.

[0067] Fig. 13 schematically illustrates a diagrammatic representation of a computing system 1000, within which a set of instructions, for causing the computing device to perform the methods described herein, may be executed. Computing system 1000 may be connected to other computing devices in a LAN, an intranet, an extranet, and/or the Internet. The computing device may operate in the capacity of a server machine in client-server network environment. The computing device may be provided by a personal computer (PC), a set-top box (STB), a server, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single computing device is illustrated, the term “computing device” shall also be taken to include any collection of computing devices that individually or jointly execute a set (or multiple sets) of instructions to perform the methods described herein.

[0068] The example computing system 1000 may include a processor (also referred to as “central processing unit” (CPU)) 1002, which in various illustrative examples may be a general

CLAIMS

What is claimed is:

1. A method of implementing a secure digital wallet processing system, the method being performed by a computer system and comprising:

receiving, ~~by a computer system,~~ a distributed ledger transaction and request with an authentication token and a customer identifier of a customer, the customer identifier being a public address;

validating the customer using an authenticator which accesses a customer identifier public address database prior to retrieving, a private key from a key management system;

retrieving, from the key management system, a private key corresponding to the public address, wherein the key management system comprises a hardware security module (HSM) that generated the public address from the private key and encrypted the private key and the public address prior to storing the public address with the private key in a key management system database;

signing the distributed ledger transaction by the private key; and

providing the signed distributed ledger transaction to a distributed ledger.

2. The method of claim 1, wherein the distributed ledger transaction is one of: a cryptocurrency buy order, a cryptocurrency sell order, a cryptocurrency transfer to another public address, or a code implementing a smart contract.

~~3. The method of claim 1, further comprising:~~

~~validating the distributed ledger transaction prior to retrieving the private key from the key management system.~~

~~4. The method of claim 1, wherein the HSM encrypts the private key and the public address prior to storing in a secure database.~~

35. The method of claim 1, further comprising:

decrypting the private key prior to signing the distributed ledger transaction.

46. The method of claim 1, further comprising:

generating the public address and providing the public address to a user prior to receiving the distributed ledger transaction.

57. The method of claim 1, wherein the key management system comprises at least one of: a warm storage device or a cold storage device.

68. A system, comprising:
a memory comprising executable instructions; and
a processor coupled to the memory, wherein the processor, by executing the instructions,
is configured to:

receive a distributed ledger transaction ~~and~~ request with an authentication token
and a customer identifier of a customer, the customer identifier being a public address;

~~retrieve, from~~ validate the customer using an authenticator which accesses a
customer identifier public address database prior to retrieving a private key from a key
management system;

retrieve, from the key management system, a private key corresponding to the
public address, wherein the key management system comprises a hardware security
module (HSM) that generated the public address from the private key and encrypted the
private key and public address prior to storing the public address with the private key in a
key management system database;

sign the distributed ledger transaction by the private key; and

provide the signed distributed ledger transaction to a distributed ledger.

79. The system of claim 68, wherein the distributed ledger transaction is one of: a
cryptocurrency buy order, a cryptocurrency sell order, a cryptocurrency transfer to another
public address, or a code implementing a smart contract.

~~10. The system of claim 8, wherein the processor is further configured to:~~
~~validate the distributed ledger transaction prior to retrieving the private key from the key-~~
~~management system.~~

~~11. The system of claim 8, wherein the HSM encrypts the private key and the public-~~
~~address prior to storing in a secure database.~~

812. The system of claim 68, wherein the processor is further configured to:
decrypt the private key prior to signing the distributed ledger transaction.

913. The system of claim 68, wherein the processor is further configured to:
generate the public address and providing the public address to a user prior to receiving
the distributed ledger transaction.

104. The system of claim 68, wherein the key management system comprises at least one of: a warm storage device or a cold storage device.

115. A non-transitory computer-readable storage medium comprising executable instructions that, when executed by a processing device, cause the processing device to:

receive a distributed ledger transaction request with an authentication token and a customer identifier of a customer, the customer identifier being a public address;

validate the customer using an authenticator which accesses a customer identifier public address database prior to retrieving a private key from a key management system;

retrieve, from thea key management system, a private key corresponding to the public address, wherein the key management system comprises a hardware security module (HSM) that generated the public address from the private key and encrypted the private key and public address prior to storing the public address with the private key in a key management system database;

sign the distributed ledger transaction by the private key; and

provide the signed distributed ledger transaction to a distributed ledger.

126. The non-transitory computer-readable storage medium of claim 115, wherein the distributed ledger transaction is one of: a cryptocurrency buy order, a cryptocurrency sell order, a cryptocurrency transfer to another public address, or a code implementing a smart contract.

~~17. The non-transitory computer-readable storage medium of claim 15, further comprising executable instructions that, when executed by the processing device, cause the processing device to:~~

~~validate the distributed ledger transaction prior to retrieving the private key from the key management system.~~

~~18. The non-transitory computer-readable storage medium of claim 15, wherein the HSM encrypts the private key and the public address prior to storing in a secure database.~~

139. The non-transitory computer-readable storage medium of claim 115, further comprising executable instructions that, when executed by the processing device, cause the processing device to:

decrypt the private key prior to signing the distributed ledger transaction.

1420. The non-transitory computer-readable storage medium of claim 115, further comprising executable instructions that, when executed by the processing device, cause the processing device to:

generate the public address and providing the public address to a user prior to receiving the distributed ledger transaction.

15. The non-transitory computer-readable storage medium of claim 11, wherein the key management system comprises at least one of: a warm storage device or a cold storage device.