SYSTEMS AND METHODS FOR PROVIDING A PERSONAL DISTRIBUTED LEDGER

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 62/346,097, filed on June 6, 2016, and U.S. Patent Application No. 15/612,288, filed on June 2, 2017, each of which are hereby incorporated by reference herein in their entireties.

BACKGROUND INFORMATION

[0002] Distributed ledger systems are increasingly used to implement currency, financial transactions and other functions. Often, it is desirable for a user to conduct transactions with such systems anonymously, in order to conceal their financial positions, etc. One way for users to conduct transactions anonymously within a distributed ledger system is to generate and use a different public address and private key for each transaction. As users typically store private keys used to sign transactions in a secure location outside the distributed ledger system, it is usually not possible to connect the identity of the user to the transaction through the private key.

[0003] In tension with this, know-your-customer regulatory mandates typically require banks, financial institutions and other entities to verify the identity of their customers. Know-your-customer mandates help prevent criminals from using transactions conducted through these institutions to perform money laundering and other crimes. However, a user conducting transactions anonymously through the use of newly generated addresses and keys for every transaction stifles satisfaction of know-your-customer mandates.

[0004] Thus, a need exists for systems and methods to securely but reliably link transactions conducted anonymously in a distributed ledger system and the user conducting the transactions.

SUMMARY

[0004a] According to a first aspect of the present invention, there is provided a method of conducting transactions, the method comprising: generating, by a wallet distributed application, an address in a public distributed ledger system and a private key; signing, by the wallet distributed application, a first transaction to a distributed application in the public distributed ledger system from the generated address using the private key; generating, by the wallet distributed application, a second transaction to a personal

distributed ledger system, the generated second transaction containing information identifying the first transaction to the public distributed ledger system; and transmitting, by the wallet distributed application, the second transaction to at least one distributed node of the personal distributed ledger system.

[0004b] According to a second aspect of the present invention, there is provided a system for conducting transactions, the system comprising: at least one processor; and a non-transitory machine-readable storage medium having program instructions, which when executed by a processor perform a method of conducting transactions, the method comprising: generating, by a wallet distributed application, an address in a public distributed ledger system and a private key; signing, by the wallet distributed application, a first transaction to a distributed application in the public distributed ledger system from the generated address and using the private key; generating, by the wallet distributed application, a second transaction to a personal distributed ledger system, the generated second transaction containing information identifying the first transaction to the public distributed ledger system; and transmitting, by the wallet distributed application, the second transaction to at least one distributed node of the personal distributed ledger system.

[0004c] According to a third aspect of the present invention, there is provided a method of authorizing a transaction in a public distributed ledger system using a personal distributed ledger system, the method comprising: reading, by a distributed application of a financial institution system hosting a node of the personal distributed ledger system, information identifying at least one first transaction conducted in the public distributed ledger system stored in the personal distributed ledger system; determining, by the financial institution system, whether to authorize a user associated with the personal distributed ledger system to conduct further transactions in the public distributed ledger system using the financial institution system based on the retrieved information identifying the transaction; and upon authorization of the user, generating, by the financial institution system, a transaction to a distributed application of the public distributed ledger system on behalf of the user.

[0004d] As disclosed, there is provided a method of storing a digital object using a personal distributed ledger system, further comprising: receiving, via a distributed application of the personal distributed ledger system, the digital object; determining whether a storage size of the digital object is above a predetermined threshold; upon determining that the storage size of the digital object is below the predetermined threshold: generating a

transaction to store the digital object in the personal distributed ledger system, and transmitting the transaction to at least one distributed node of the personal distributed ledger system; and upon determining that the storage size of the digital object is above the predetermined threshold: determining a representation of the digital object, storing the digital object in a secure storage system outside of the personal distributed ledger system, generating a transaction to store the representation of the digital object in the personal distributed ledger system, and transmitting the transaction to at least one distributed node of the personal distributed ledger system.

[0004e] As disclosed, there is provided a method of distributing a digital object using a persona distributed ledger system, the method comprising: receiving, via a distributed application of the personal distributed ledger system, a request for the digital object; determining whether the digital object or a representation of the digital object is stored in personal distributed ledger system; upon determining that the digital object is stored in the personal distributed ledger system: reading via the access distributed application the personal distributed ledger system to retrieve the digital object, and providing the digital object to a requesting entity; and upon determining that the encoding of the digital object is stored in the personal distributed ledger system: reading via the access distributed application the personal distributed ledger system to retrieve the representation of the digital object, retrieving the digital object from an asset store, determining a representation of the retrieved digital object, determining whether the determined representation matches the retrieved representation, and upon determining that the determined representation matches the retrieved representation, providing the digital object to the requesting entity.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] So that the features of the present invention can be understood, a number of drawings are described below. However, the appended drawings illustrate only particular embodiments of the invention and are therefore not to be considered limiting of its scope, for the invention may encompass other equally effective embodiments.

[0006] FIG. 1 is a schematic diagram depicting an embodiment of a system for providing a personal distributed ledger.

CLAIMS

1. A method of conducting transactions, the method comprising:

generating, by a wallet distributed application, an address in a public distributed ledger system and a private key;

signing, by the wallet distributed application, a first transaction to a distributed application in the public distributed ledger system from the generated address using the private key;

generating, by the wallet distributed application, a second transaction to a personal distributed ledger system, the generated second transaction containing information identifying the first transaction to the public distributed ledger system; and

transmitting, by the wallet distributed application, the second transaction to at least one distributed node of the personal distributed ledger system.

2. The method of claim 1, wherein the information identifying the first transaction to the public distributed ledger system includes the private key used to sign the first transaction.

3. The method of claim 1, wherein the information identifying the first transaction to the public distributed ledger system includes an execution receipt for the first transaction.

4. The method of claim 1, wherein the information identifying the first transaction to the public distributed ledger system includes at least a portion of the first transaction.

5. The method of claim 1, further comprising:

receiving, by the wallet distributed application, an invocation by the distributed application of the public distributed ledger system to sign the first transaction to the distributed application, the invocation including the first transaction; and

transmitting, by the wallet distributed application, the first transaction to at least one distributed node of the public distributed ledger system.

6. The method of claim 1, wherein the personal distributed ledger system is separate from the public distributed ledger system, and provides access to only the user and entities authorized by the user

7. The method of claim 1, further comprising:

reading, by a distributed application of a financial institution system hosting a node of the personal distributed ledger system, at least a portion of the information identifying the first transaction stored in the personal distributed ledger system;

determining whether to authorize, by the financial institution system, a user associated with the personal distributed ledger system to conduct transactions in the public distributed ledger system using the financial institution system based on the retrieved information identifying the first transaction;

upon authorization of the user, generating, by the financial institution system, a transaction to a distributed application of the public distributed ledger system on behalf of the user, wherein the transaction by the financial institution system mints tokens in the public distributed ledger system on behalf of the user.

8. The method of claim 7, further comprising:

generating, by the user, a transaction to a distributed application of the public distributed ledger system utilizing the minted tokens in the public distributed ledger system

9. The method of claim 1, further comprising:

transmitting the first transaction to the public distributed ledger system for execution;

wherein the information identifying the first transaction includes at least a portion of the executed first transaction and the private key used to sign the first transaction, and

the personal distributed ledger system is separate from the public distributed ledger system and includes only distributed nodes authorized by the user, the authorized distributed nodes including a validator node hosted by a financial institution system.

10. The method of claim 9, further comprising:

executing, by the validator node hosted by the financial institution system, a read of the personal distributed ledger system to retrieve the identifying information; and

generating, by the at least one financial institution system based on the retrieved identifying information, tokens of the public distributed ledger system for use by the user to conduct further transactions in the public distributed ledger system.

11. The method of claim 1, further comprising:

receiving, via a distributed application of the personal distributed ledger system, a digital object;

determining whether a storage size of the digital object is above a predetermined threshold;

upon determining that the storage size of the digital object is below the predetermined threshold: generating a transaction to store the digital object in the personal distributed ledger system, and transmitting the transaction to at least one distributed node of the personal distributed ledger system;

upon determining that the storage size of the digital object is above the predetermined threshold: determining a representation of the digital object, storing the digital object in a secure storage system outside of the personal distributed ledger system, generating a transaction to store the representation of the digital object in the personal distributed ledger system, and transmitting the transaction to at least one distributed node of the personal distributed ledger system.

12. The method of claim 11, wherein the digital object is identity data, the identity data including at least one of: driver's license data, passport data, a social security number, a fingerprint, an iris pattern, a facial pattern, or a DNA pattern.

13. The method of claim 11, wherein determining the representation includes performing at least one cryptographic hash on the digital asset.

14. The method of claim 11, further comprising:

receiving, via an access distributed application of the personal distributed ledger system, a request for the digital object;

determining whether the digital object or the representation of the digital object is stored in personal distributed ledger system;

upon determining that the digital object is stored in the personal distributed ledger system: reading via the access distributed application the personal distributed ledger system to retrieve the digital object, and providing the digital object to a requesting entity; and

upon determining that the representation of the digital object is stored in the personal distributed ledger system: reading via the access distributed application the personal distributed ledger system to retrieve the representation of the digital object, retrieving the digital object from an asset store, determining a representation of the retrieved digital object, determining whether the determined representation matches the retrieved representation, and upon determining that the determined representation matches the retrieved representation, providing the digital object to the requesting entity.

15. A system for conducting transactions, the system comprising:

at least one processor; and

a non-transitory machine-readable storage medium having program instructions, which when executed by a processor perform a method of conducting transactions, the method comprising:

generating, by a wallet distributed application, an address in a public distributed ledger system and a private key;

signing, by the wallet distributed application, a first transaction to a distributed application in the public distributed ledger system from the generated address and using the private key;

generating, by the wallet distributed application, a second transaction to a personal distributed ledger system, the generated second transaction containing information identifying the first transaction to the public distributed ledger system; and

transmitting, by the wallet distributed application, the second transaction to at least one distributed node of the personal distributed ledger system.

16. The system of claim 15, wherein the information identifying the first transaction to the public distributed ledger system includes the private key used to sign the transaction.

17. The system of claim 15, wherein the personal distributed ledger system is separate from the public distributed ledger system, and provides access to only the user and entities authorized by the user.

18. A method of authorizing a transaction in a public distributed ledger system using a personal distributed ledger system, the method comprising:

reading, by a distributed application of a financial institution system hosting a node of the personal distributed ledger system, information identifying at least one first transaction conducted in the public distributed ledger system stored in the personal distributed ledger system;

determining, by the financial institution system, whether to authorize a user associated with the personal distributed ledger system to conduct further transactions in the public distributed ledger system using the financial institution system based on the retrieved information identifying the transaction; and

upon authorization of the user, generating, by the financial institution system, a transaction to a distributed application of the public distributed ledger system on behalf of the user.

19. The method of claim 18, wherein the reading executes by the distributed application of the financial institution system a read call to a contract of the personal distributed ledger system to retrieve the information identifying the first transaction, the identifying information including at least a portion of the conducted first transaction and a private key used to sign the first transaction, the personal distributed ledger system being separate from the public distributed ledger system and including only distributed nodes authorized by the user, the authorized distributed nodes including the validator node hosted by the financial institution system; and

wherein the transaction generated by the financial institution system is executed to generate tokens of the public distributed ledger system for use by the user to conduct the further transactions in the public distributed ledger system

20. The method of claim 18, further comprising generating, by the user, a transaction to a distributed application of the public distributed ledger system utilizing an output of the transaction by the financial institution,

wherein the transaction by the financial institution system mints tokens in the public distributed ledger system on behalf of the user, and

the transaction by the user utilizes the minted tokens in the public distributed ledger system.