individual identity as well as attributes relating to it and personal data including but not limited to individual's physical description, bank details, travel history, etc. (the "Personally Identifiable Information "PII"). In accordance with a first aspect disclosed herein, there is set forth a computer-implemented method for managing secured data within independent computer systems and digital networks, the method comprising:

[0009] generating a cryptographic data stream by processing original data representing the secured data on a local client device through a first cryptographic function;

[0010] generating blinded data by providing the cryptographic data stream and a blind factor to a second cryptographic function;

[0011] generating a blinded signature by providing the generated blinded data and a private key to a third cryptographic function of a storage device, the private key accessible only to the storage device,

[0012] wherein the storage device comprises decentralized distributed storage;

[0013] generating a data secret identifier by providing the generated blinded signature and optionally the blind factor to a fourth cryptographic function, wherein the generated data secret identifier is mathematically binded with the generated cryptographic data stream, and the storage device is never in possession of the original data and the generated cryptographic data stream;

[0014] partitioning the original data on the local client device into one or more original data sub-parts prior to said generating the cryptographic data stream;

[0015] generating one or more cryptographic data sub-parts by processing the partitioned original data sub-parts on the local client device through a first cryptographic function,

[0016] wherein said generating the cryptographic data stream comprises processing the generated cryptographic data-sub parts through the cryptographic function;

[0017] generating a set of salts by processing the partitioned original data sub-parts and the generated data secret identifier through a fifth cryptographic function;

[0018] combining the set of salts and the partitioned original data sub-parts by associating a selected salt with its corresponding data sub-part;

[0019] generating a set of cryptographic salts by processing the combined set of salts and the partitioned original data sub-parts data through a sixth cryptographic function; and

[0020] generating the data public identifier by processing the set of cryptographic salts through a seventh cryptographic function;

[0021] generating a proof of inclusion for each partitioned original data sub-part, a selected proof of inclusion for a selected partitioned original data sub-part includes its corresponding salt and the generated set of cryptographic salts, the selected proof of inclusion for mathematically establishing that the selected partitioned original data sub-part is included in the generated data public identifier.

[0022] In some embodiments of the disclosed method, the method further comprises deriving a tree structure from the generated cryptographic data-sub parts prior to the generating the cryptographic data stream.

[0023] In some embodiments of the disclosed method, the method further comprises mathematically establishing that the selected original data sub-part is included in the generated data public identifier by forming a dataset by combining the selected original data sub-art and the selected proof of inclusion; generating a proof cryptographic data by processing the dataset through an eighth cryptographic function; determining whether the proof cryptographic data equals the data public identifier.

[0024] In some embodiments of the disclosed method, the method further comprises providing the generated cryptographic data stream and the data public identifier to a verifiable data structure, the verifiable data structure comparing a current checksum with the data public identifier.

[0025] In some embodiments of the disclosed method, the method further comprises producing a new checksum by processing the current checksum and the generated cryptographic data stream to a twelfth cryptographic data stream.

[0026] In some embodiments of the disclosed method, generating blinded data further comprises providing a public key of the storage device to the second cryptographic function, wherein the blind factor optionally is a random value.

[0027] In some embodiments of the disclosed method, generating the cryptographic data stream comprises processing the original data through a hash function, the method further comprising optionally creating an associated ledger transaction in a distributed ledger comprising said generated blinded signature of the storage device.

[0028] In accordance with another aspect disclosed herein, there is set forth a computer system for managing secured data within independent computer systems and digital networks, the system comprising:

[0029] a client device for generating a cryptographic data stream by processing original data representing the secured data through a cryptographic function, generating blinded data by providing the cryptographic data stream and a blind factor to a second cryptographic function;

[0030] a verifiable storage device in communication with the client device for generating a blinded signature by processing the generated blinded data and a private key to a third cryptographic function, the private key accessible only to the storage device,

[0031] wherein the verifiable storage device comprises decentralized distributed storage; and

[0032] wherein the client device further generated a data secret identifier by providing the generated blinded signature and the blind factor to a fourth cryptographic function, wherein the generated data secret identifier is mathematically binded with the generated cryptographic data stream, and the storage device is never in possession of the original data and the generated cryptographic data stream,

[0033] wherein the client device further partitions the original data into one or more original data sub-parts prior to said generating the cryptographic

data stream, generates one or more cryptographic data sub-parts by processing the partitioned original data sub-parts through a first cryptographic function,

[0034] wherein the client device generates the cryptographic data stream by processing the generated cryptographic data-sub parts through the cryptographic function,

[0035] wherein client device further generates a data public identifier by generating a set of salts by processing the partitioned original data subparts and the generated data secret identifier through a fifth cryptographic function; combining the set of salts and the partitioned original data sub-parts by associating a selected salt with its corresponding data sub-part; generating a set of cryptographic salts by processing the combined set of salts and the partitioned original data sub-parts data through a sixth cryptographic function; and generating the data public identifier by processing the set of cryptographic salts through a seventh cryptographic function, and

[0036] wherein the client device further generates a proof of inclusion for each partitioned original data sub-part, a selected proof of inclusion for a selected partitioned original data sub-part includes its corresponding salt and the generated set of cryptographic salts, the selected proof of inclusion for mathematically establishing that the selected partitioned original data sub-part is included in the generated data public identifier

[0037] In some embodiments of the disclosed system, the client device further derives a tree structure from the generated cryptographic data-sub parts prior to said generating the cryptographic data stream.

[0037a] In some embodiments of the disclosed system, the system further includes a distributed ledger in communication with the verifiable storage device for managing ledger

transactions based on any transaction occurring in the verifiable storage device, wherein said verifiable storage device optionally comprises a distributed hash table, a distributed database, a peer-to-peer hypermedia distributed storage, a distributed ledger, an operating memory, a centralized database, or a cloud-based storage.

[0037b] In accordance with yet another aspect disclosed herein, there is set forth a method for managing secured data within independent computer systems and digital networks, the method comprising:

[0037c] generating a cryptographic data stream by processing original data representing the secured data on a local client device through a first cryptographic function;

[0037d] generating blinded data by providing the cryptographic data stream to a second cryptographic function;

[0037e] generating a blinded signature by providing the generated blinded data and a private key to a third cryptographic function of a storage device being different than the local client device, the private key accessible only to the storage device,

[0037f] wherein the storage device comprises decentralized distributed storage; and

[0037g] generating a data secret identifier by providing the generated blinded signature to a fourth cryptographic function;

[0037h] wherein the generated data secret identifier is mathematically binded with the generated cryptographic data stream;

[0037i] partitioning the original data on the local client device into original data sub-parts prior to said generating the cryptographic data stream;

[0037j] generating one or more cryptographic data sub-parts by processing the partitioned original data sub-parts on the local client device through the first cryptographic function,

[0037k] wherein said generating the cryptographic data stream comprises processing the generated cryptographic data sub-parts through the first cryptographic function;

[0037l] generating a set of salts by processing the partitioned original data sub-parts and the generated data secret identifier through a fifth cryptographic function;

[0037m] combining the set of salts and the partitioned original data sub-parts by associating a selected salt with its corresponding data sub-part;

[0037n] generating a set of cryptographic salts by processing the combined set of salts and the partitioned original data sub-parts data through a sixth cryptographic function;

[0037o] generating a data public identifier by processing the set of cryptographic salts through a seventh cryptographic function;

[0037p] generating a proof of inclusion for each partitioned original data sub-part, a selected proof of inclusion for a selected partitioned original data sub-part includes its corresponding salt and the generated set of cryptographic salts, the selected proof of inclusion for mathematically establishing that the selected partitioned original data sub-part is included in the generated data public identifier.

BRIEF DESCRIPTION OF THE DRAWINGS

[0038] Fig. 1 is an exemplary top-level block diagram illustrating one embodiment of a data management system including a client device for partitioning data and generating cryptographic data.

CLAIMS

What is claimed is:

1. A method for managing secured data within independent computer systems and digital networks, the method comprising:

generating a cryptographic data stream by processing original data representing the secured data on a local client device through a first cryptographic function;

generating blinded data by providing the cryptographic data stream and a blind factor to a second cryptographic function;

generating a blinded signature by providing the generated blinded data and a private key to a third cryptographic function of a storage device, the private key accessible only to the storage device,

wherein the storage device comprises decentralized distributed storage;

generating a data secret identifier by providing the generated blinded signature and the blind factor to a fourth cryptographic function, wherein the generated data secret identifier is mathematically binded with the generated cryptographic data stream, and the storage device is never in possession of the original data and the generated cryptographic data stream;

partitioning the original data on the local client device into one or more original data sub-parts prior to said generating the cryptographic data stream;

generating one or more cryptographic data sub-parts by processing the partitioned original data sub-parts on the local client device through the first cryptographic function,

wherein said generating the cryptographic data stream comprises processing the generated cryptographic data sub-parts through the first cryptographic function;

generating a set of salts by processing the partitioned original data sub-parts and the generated data secret identifier through a fifth cryptographic function;

combining the set of salts and the partitioned original data sub-parts by associating a selected salt with its corresponding data sub-part;

generating a set of cryptographic salts by processing the combined set of salts and the partitioned original data sub-parts data through a sixth cryptographic function;

generating a data public identifier by processing the set of cryptographic salts through a seventh cryptographic function; and

generating a proof of inclusion for each partitioned original data sub-part, a selected proof of inclusion for a selected partitioned original data sub-part includes its corresponding salt and the generated set of cryptographic salts, the selected proof of inclusion for mathematically establishing that the selected partitioned original data sub-part is included in the generated data public identifier.

2. The method of claim 1, further comprising deriving a tree structure from the generated cryptographic data sub-parts prior to said generating the cryptographic data stream.

3. The method of claim 1, further comprising mathematically establishing that the selected original data sub-part is included in the generated data public identifier by forming a dataset by combining the selected original data sub-art and the selected proof of inclusion;

generating a proof cryptographic data by processing the dataset through an eighth cryptographic function; determining whether the proof cryptographic data equals the data public identifier.

4. The method of claim 1, further comprising providing the generated cryptographic data stream and the data public identifier to a verifiable data structure, the verifiable data structure comparing a current checksum with the data public identifier.

5. The method of claim 4, further comprising producing a new checksum by processing the current checksum and the generated cryptographic data stream to a twelfth cryptographic data stream.

6. The method of claim 1, wherein said generating blinded data further comprises providing a public key of the storage device to the second cryptographic function.

7. The method of claim 1, wherein said generating the cryptographic data stream comprises processing the original data through a hash function.

8. A computer-implemented system for managing secured data within independent computer systems and digital networks, the system comprising:

a client device for generating a cryptographic data stream by processing original data representing the secured data through a first cryptographic function, generating blinded data by providing the cryptographic data stream and a blind factor to a second cryptographic function;

a verifiable storage device in communication with the client device for generating a blinded signature by processing the generated blinded data and a private key to a third cryptographic function, the private key accessible only to the verifiable storage device,

wherein the verifiable storage device comprises decentralized distributed storage; and

wherein the client device further generates a data secret identifier by providing the generated blinded signature and the blind factor to a fourth cryptographic function, wherein the generated data secret identifier is mathematically binded with the generated cryptographic data stream, and the verifiable storage device is never in possession of the original data and the generated cryptographic data stream,

wherein the client device further partitions the original data into one or more original data sub-parts prior to said generating the cryptographic data stream, generates one or more cryptographic data sub-parts by processing the partitioned original data sub-parts through the first cryptographic function,

wherein the client device generates the cryptographic data stream by processing the generated cryptographic data sub-parts through the first cryptographic function,

wherein the client device further generates a data public identifier by generating a set of salts by processing the partitioned original data sub-parts and the generated data secret identifier through a fifth cryptographic function, combining the set of salts and the partitioned original data sub-parts by associating a selected salt with its corresponding data sub-part, generating a set of cryptographic salts by processing the combined set of salts and the partitioned original data sub-parts data through a sixth cryptographic function, and generating the data public identifier by processing the set of cryptographic salts through a seventh cryptographic function, and

wherein the client device further generates a proof of inclusion for each partitioned original data sub-part, a selected proof of inclusion for a selected partitioned original data sub-part includes its corresponding salt and the generated set of cryptographic salts, the selected proof of inclusion for mathematically establishing that the selected partitioned original data sub-part is included in the generated data public identifier.

9. The computer-implemented system of claim 8, wherein said client device further derives a tree structure from the generated cryptographic data-sub parts prior to said generating the cryptographic data stream.

10. The computer-implemented system of claim 8, further comprising a distributed ledger in communication with the verifiable storage device for managing ledger transactions based on any transaction occurring in the verifiable storage device.

11. The computer-implemented system of claim 8, wherein the decentralized distributed storage comprises at least one of a distributed hash table, a distributed database, a peer-to-peer hypermedia distributed storage, a distributed ledger, an operating memory, a centralized database, or a cloud-based storage.

12. The method of claim 1, wherein said generating blinded data comprises providing a random value as the blind factor.

13. The method of claim 1, further comprising creating an associated ledger transaction in a distributed ledger comprising said generated blinded signature of the storage device.

14. A method for managing secured data within independent computer systems and digital networks, the method comprising:

generating a cryptographic data stream by processing original data representing the secured data on a local client device through a first cryptographic function;

generating blinded data by providing the cryptographic data stream to a second cryptographic function;

generating a blinded signature by providing the generated blinded data and a private key to a third cryptographic function of a storage device being different than the local client device, the private key accessible only to the storage device,

wherein the storage device comprises decentralized distributed storage; and

generating a data secret identifier by providing the generated blinded signature to a fourth cryptographic function,

wherein the generated data secret identifier is mathematically binded with the generated cryptographic data stream;

partitioning the original data on the local client device into original data sub-parts prior to said generating the cryptographic data stream;

generating one or more cryptographic data sub-parts by processing the partitioned original data sub-parts on the local client device through the first cryptographic function,

wherein said generating the cryptographic data stream comprises processing the generated cryptographic data sub-parts through the first cryptographic function;

generating a set of salts by processing the partitioned original data sub-parts and the generated data secret identifier through a fifth cryptographic function;

combining the set of salts and the partitioned original data sub-parts by associating a selected salt with its corresponding data sub-part;

generating a set of cryptographic salts by processing the combined set of salts and the partitioned original data sub-parts data through a sixth cryptographic function;

generating a data public identifier by processing the set of cryptographic salts through a seventh cryptographic function; and

generating a proof of inclusion for each partitioned original data sub-part, a selected proof of inclusion for a selected partitioned original data sub-part includes its corresponding salt and the generated set of cryptographic salts, the selected proof of inclusion for mathematically establishing that the selected partitioned original data sub-part is included in the generated data public identifier.