(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7597822号
(P7597822)

(45)発行日　令和6年12月10日(2024.12.10)

(24)登録日　令和6年12月2日(2024.12.2)

(51)国際特許分類		FI		
H04L 9/08 (2006.01)		H04L	9/08	A
H04L 9/32 (2006.01)		H04L	9/32	200A
G09C 1/00 (2006.01)		G09C	1/00	650Z

請求項の数　36　（全37頁）

(21)出願番号　特願2022-551266(P2022-551266)
(86)(22)出願日　令和3年2月8日(2021.2.8)
(65)公表番号　特表2023-515956(P2023-515956A)
(43)公表日　令和5年4月17日(2023.4.17)
(86)国際出願番号　PCT/US2021/017019
(87)国際公開番号　WO2021/173330
(87)国際公開日　令和3年9月2日(2021.9.2)
審査請求日　令和6年2月6日(2024.2.6)
(31)優先権主張番号　62/981,663
(32)優先日　令和2年2月26日(2020.2.26)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　521151175
ティーゼロ・アイピー，エルエルシー
アメリカ合衆国ユタ州８４１１１，ソルト・レイク・シティ，サウス・メイン・ストリート ２９９，スイート ２２７０
(74)代理人　100118902
弁理士　山本 修
(74)代理人　100106208
弁理士　宮前 徹
(74)代理人　100196508
弁理士　松尾 淳一
(74)代理人　100162846
弁理士　大牧 綾子
(72)発明者　オルネラス，マイケル・ディー
アメリカ合衆国ニューヨーク州１０００
最終頁に続く

(54)【発明の名称】　シークレット分割およびメタデータ記憶

(57)【特許請求の範囲】
【請求項１】
少なくとも１つのプロセッサであって、
保護されるべきシークレットを決定し、
前記シークレットを、複数のシークレットシェアに分割し、前記複数のシークレットシェアの少なくともサブセットは、前記シークレットを再構成するために必要とされ、
前記複数のシークレットシェアの各それぞれのシークレットシェアを、それぞれのシェアホルダに配布するために、それぞれのポータブル記憶デバイスまたは媒体に転送し、
前記複数のシークレットシェアの各それぞれのシークレットシェアの少なくともそれぞれのハッシュを有するメタデータを生成し、
前記複数のシークレットシェアの各それぞれのシークレットシェアの前記少なくとも前記それぞれのハッシュを有する前記メタデータを個別の記憶デバイスまたは媒体に格納し、
前記個別の記憶デバイスまたは媒体は、前記複数のシークレットシェアの各それぞれのシークレットシェアのために用いられるそれぞれのポータブル記憶デバイスまたは媒体のいずれとも別となるように構成された、少なくとも１つのプロセッサを備える、コンピューティングシステム。
【請求項２】
前記シークレットと、前記複数のシークレットシェアと、前記複数のシークレットシェアのそれぞれのハッシュとの各々は、異なるキャラクタの文字列である、請求項１に記載のコンピューティングシステム。

【請求項３】
前記シークレットは、秘密鍵を再構成するために使用される暗号秘密鍵またはニーモニックフレーズもしくはシードである、請求項１に記載のコンピューティングシステム。
【請求項４】
前記少なくとも１つのプロセッサは、Ｓｈａｍｉｒシークレットシェアまたは多項式補間を使用して、前記シークレットを、前記複数のシークレットシェアに分割するように構成される、請求項１に記載のコンピューティングシステム。
【請求項５】
前記少なくとも１つのプロセッサは、前記シークレットを再構成するために前記複数のシークレットシェアの各それぞれのシークレットシェアを少なくとも１回使用することによって、前記複数のシークレットシェアを検証するように構成され、
前記複数のシークレットシェアは、前記複数のシークレットシェアが正常に検証された後、前記それぞれのポータブル記憶デバイスまたは媒体に単に転送される、請求項１に記載のコンピューティングシステム。
【請求項６】
前記少なくとも１つのプロセッサは、
前記シークレットを決定する前に、前記コンピューティングシステムにおいて、少なくとも１つの記憶デバイスの内容を消去し、オペレーティングシステムのクリーンインストールを実行し、
前記複数のシークレットシェアの各それぞれのシークレットシェアを前記それぞれのポータブル記憶デバイスまたは媒体に転送した後、前記コンピューティングシステムにローカルに格納された前記シークレットおよび前記複数のシークレットシェアのコピーを削除するように構成される、請求項１に記載のコンピューティングシステム。
【請求項７】
前記シークレットは、暗号秘密鍵であるか、または前記暗号秘密鍵を回復するために使用されるニーモニックフレーズもしくはシードであり、
前記少なくとも１つのプロセッサは、前記暗号秘密鍵またはニーモニックフレーズもしくはシードを生成することにより、前記シークレットを決定するように構成される、請求項１に記載のコンピューティングシステム。
【請求項８】
前記少なくとも１つのプロセッサはまた、前記メタデータにおいて、以下の情報、すなわち、
前記暗号秘密鍵に対応する公開鍵と、
分散型台帳における少なくとも１つのアドレスとを生成する、請求項７に記載のコンピューティングシステム。
【請求項９】
前記少なくとも１つのプロセッサは、
それぞれのシェアホルダから取得された少なくとも２つのシークレットシェア記憶デバイスまたは媒体から、取得されるシークレットシェアを決定し、
前記少なくとも２つのシークレットシェア記憶デバイスまたは媒体から取得された前記シークレットシェアを使用して、前記シークレットの再構成を試みるように構成される、請求項１に記載のコンピューティングシステム。
【請求項１０】
前記少なくとも１つのプロセッサは、前記シークレットの再構成の前記試みを行っている間に、前記取得されたシークレットシェアから前記シークレットが正常に再構成されなかった場合、前記メタデータのうちの前記複数のシークレットシェアの各それぞれのシークレットシェアの前記少なくとも前記それぞれのハッシュに基づいて、前記取得されたシークレットシェアのうちの少なくとも１つのシークレットシェアを、生成された前記複数のシークレットシェアの１つではないとして特定するように構成される、請求項９に記載のコンピューティングシステム。

【請求項１１】
シークレット分割およびメタデータ記憶のための方法であって、
保護されるべきシークレットを決定するステップと、
前記シークレットを、複数のシークレットシェアに分割するステップであって、前記複数のシークレットシェアの少なくともサブセットが、前記シークレットを再構成するために必要とされる、分割するステップと、
前記複数のシークレットシェアの各それぞれのシークレットシェアを、それぞれのシェアホルダに配布するために、それぞれのポータブル記憶デバイスまたは媒体に転送するステップと、
前記複数のシークレットシェアの少なくとも各それぞれのシークレットシェアのハッシュを有するメタデータを生成するステップと、
前記複数のシークレットシェアの各それぞれのシークレットシェアの前記少なくとも前記それぞれのハッシュを有する前記メタデータを個別の記憶デバイスまたは媒体に格納するステップであって、前記個別の記憶デバイスまたは媒体は、前記複数のシークレットシェアの各それぞれのシークレットシェアのために用いられるそれぞれのポータブル記憶デバイスまたは媒体のいずれとも別となる、ステップとを含む、方法。
【請求項１２】
前記シークレットと、前記複数のシークレットシェアと、前記複数のシークレットシェアのそれぞれのハッシュとの各々は、異なるキャラクタの文字列である、請求項１１に記載の方法。
【請求項１３】
前記シークレットは、秘密鍵を再構成するために使用される暗号秘密鍵またはニーモニックフレーズもしくはシードである、請求項１１に記載の方法。
【請求項１４】
前記分割するステップは、Ｓｈａｍｉｒシークレットシェアまたは多項式補間を使用して前記シークレットを、前記複数のシークレットシェアに分割するステップを含む、請求項１１に記載の方法。
【請求項１５】
前記シークレットを再構成するために前記複数のシークレットシェアの各それぞれのシークレットシェアを少なくとも１回使用することによって、前記複数のシークレットシェアを検証するステップをさらに含み、
前記複数のシークレットシェアは、前記複数のシークレットシェアが正常に検証された後、前記それぞれのポータブル記憶デバイスまたは媒体に単に転送される、請求項１１に記載の方法。
【請求項１６】
前記シークレットを決定するステップの前に、コンピューティングシステムにおいて、少なくとも１つの記憶デバイスの内容を消去し、オペレーティングシステムのクリーンインストールを実行するステップと、
前記複数のシークレットシェアの各それぞれのシークレットシェアを前記それぞれのポータブル記憶デバイスまたは媒体に転送するステップの後、前記コンピューティングシステムにローカルに格納された前記シークレットおよび前記複数のシークレットシェアのコピーを削除するステップとをさらに含む、請求項１１に記載の方法。
【請求項１７】
前記シークレットは、暗号秘密鍵であるか、または前記暗号秘密鍵を回復するために使用されるニーモニックフレーズもしくはシードであり、
前記シークレットは、前記暗号秘密鍵またはニーモニックフレーズもしくはシードを生成することによって決定される、請求項１１に記載の方法。
【請求項１８】
前記メタデータにおいて、以下の情報、すなわち、
前記暗号秘密鍵に対応する公開鍵と、

分散型台帳における少なくとも１つのアドレスと
を生成するステップをさらに含む、請求項１７に記載の方法。
【請求項１９】
それぞれのシェアホルダから取得された少なくとも２つのシークレットシェア記憶デバイスまたは媒体の各々から、取得されるシークレットシェアを決定するステップと、
前記少なくとも２つのシークレットシェア記憶デバイスまたは媒体の各々から取得された前記シークレットシェアを使用して、前記シークレットの再構成を試みるステップとをさらに含む、請求項１１に記載の方法。
【請求項２０】
前記シークレットの再構成の前記試みを行っている間に、前記取得されたシークレットシェアから前記シークレットが正常に再構成されなかった場合、前記メタデータのうちの前記複数のシークレットシェアの各それぞれのシークレットシェアの前記少なくとも前記それぞれのハッシュに基づいて、取得されたシークレットシェアのうちの少なくとも１つのシークレットシェアを、生成された前記複数のシークレットシェアの１つではないとして特定するステップをさらに含む、請求項１９に記載の方法。
【請求項２１】
少なくとも１つのプロセッサであって、
複数のシェアホルダのうちの少なくとも２人から取得された少なくとも２つのシークレットシェア記憶デバイスまたは媒体の各々から、取得されるシークレットシェアを決定し、
前記複数のシークレットシェアが前記複数のシェアホルダに配布される前に生成された複数のシークレットシェアの少なくともハッシュのリストを有するメタデータを判定し、
前記少なくとも２つのシークレットシェア記憶デバイスまたは媒体から取得されたシークレットシェアを使用して、シークレットの再構成を試み、
前記シークレットの再構成の前記試みを行っている間に、前記取得されたシークレットシェアから前記シークレットが正常に再構成されなかった場合、前記メタデータのうちの前記複数のシークレットシェアの前記少なくとも前記ハッシュの前記リストに基づいて、前記取得されたシークレットシェアのうちの少なくとも１つのシークレットシェアを、生成された前記複数のシークレットシェアの１つではないとして特定するように構成された、
少なくとも１つのプロセッサを備える、コンピューティングシステム。
【請求項２２】
前記シークレットと、前記取得されたシークレットシェアと、前記複数のシークレットシェアのハッシュとの各々は、異なるキャラクタの文字列である、請求項２１に記載のコンピューティングシステム。
【請求項２３】
前記シークレットは、秘密鍵を再構成するために使用される暗号秘密鍵またはニーモニックフレーズもしくはシードである、請求項２１に記載のコンピューティングシステム。
【請求項２４】
前記少なくとも１つのプロセッサは、Ｓｈａｍｉｒ結合を使用して前記シークレットを再構成することを試みるように構成される、請求項２１に記載のコンピューティングシステム。
【請求項２５】
前記少なくとも１つのプロセッサは、それぞれの取得されたシークレットシェアを、前記メタデータにおけるハッシュの前記リストと比較することによって、前記取得されたシークレットシェアの各それぞれの取得されたシークレットシェアを検証するように構成され、
前記それぞれの取得されたシークレットシェアが、前記メタデータにおけるハッシュの前記リストにおけるハッシュと一致する場合、前記それぞれの取得されたシークレットシェアは正常に検証される、ことをさらに備える、請求項２１に記載のコンピューティングシステム。

【請求項２６】
前記少なくとも１つのプロセッサは、前記複数のシークレットシェアが正常に検証された後にのみ、前記シークレットを再構成することを試みるように構成される、請求項２５に記載のコンピューティングシステム。
【請求項２７】
前記少なくとも１つのプロセッサは、前記シークレットが、前記取得されたシークレットシェアから、再構成されたシークレットとして再構成されたときに、前記再構成されたシークレットを必要とする以下のアクション、すなわち、
前記再構成されたシークレットを使用してデータを暗号化または解読すること、
前記再構成されたシークレットに基づいて、分散型台帳におけるトランザクションアドレスを生成すること、または、
前記再構成されたシークレットを使用してトランザクションに署名することであって、前記トランザクションは、前記分散型台帳におけるアドレスから暗号通貨を送金する、署名すること、のうちの少なくとも１つを実行するように構成される、請求項２１に記載のコンピューティングシステム。
【請求項２８】
前記少なくとも１つのプロセッサは、前記取得されるシークレットシェアが決定される前に、
前記シークレットを、前記複数のシークレットシェアに分割することであって、前記複数のシークレットシェアの少なくともサブセットは、前記シークレットを再構成するために必要とされる、分割することと、
前記複数のシークレットシェアの各それぞれのシークレットシェアをそれぞれのポータブル記憶デバイスまたは媒体に転送することとを行うように構成され、
各ポータブル記憶デバイスまたは媒体は、前記複数のシェアホルダに配布される、請求項２１に記載のコンピューティングシステム。
【請求項２９】
方法であって、
複数のシェアホルダのうちの少なくとも２人から取得された少なくとも２つのシークレットシェア記憶デバイスまたは媒体の各々から取得されるシークレットシェアを決定するステップと、
前記複数のシークレットシェアが前記複数のシェアホルダに配布される前に生成された複数のシークレットシェアの少なくともハッシュのリストを有するメタデータを判定するステップと、
前記少なくとも２つのシークレットシェア記憶デバイスまたは媒体から取得されたシークレットシェアを使用して、シークレットの再構成を試みるステップと、
前記シークレットの再構成の前記試みが行われている間に、前記取得されたシークレットシェアから前記シークレットが正常に再構成されなかった場合、前記メタデータのうちの前記複数のシークレットシェアの前記少なくとも前記ハッシュのリストに基づいて、前記取得されたシークレットシェアのうちの少なくとも１つのシークレットシェアを、生成された前記複数のシークレットシェアの１つではないとして特定するステップとを含む、方法。
【請求項３０】
前記シークレットと、前記取得されたシークレットシェアと、前記複数のシークレットシェアの前記ハッシュとの各々は、異なるキャラクタの文字列である、請求項２９に記載の方法。
【請求項３１】
前記シークレットは、秘密鍵を再構成するために使用される暗号秘密鍵またはニーモニックフレーズもしくはシードである、請求項２９に記載の方法。
【請求項３２】
Ｓｈａｍｉｒ結合を使用して前記シークレットを再構成することを試みるステップをさ

らに含む、請求項２９に記載の方法。
【請求項３３】
それぞれの取得されたシークレットシェアを、前記メタデータにおけるハッシュの前記リストと比較することによって、前記取得されたシークレットシェアの各それぞれの取得されたシークレットシェアを検証するステップをさらに含み、
前記それぞれの取得されたシークレットシェアが、前記メタデータにおけるハッシュの前記リストにおけるハッシュと一致する場合、前記それぞれの取得されたシークレットシェアは正常に検証される、請求項２９に記載の方法。
【請求項３４】
前記試みるステップは、前記複数のシークレットシェアが正常に検証された後にのみ、前記シークレットを再構成することを試みるステップを含む、請求項３３に記載の方法。
【請求項３５】
前記シークレットが、前記取得されたシークレットシェアから再構成されたシークレットとして再構成されたときに、前記再構成されたシークレットを必要とする以下のアクション、すなわち、
前記再構成されたシークレットを使用してデータを暗号化または解読するステップ、
前記再構成されたシークレットに基づいて、分散型台帳におけるトランザクションアドレスを生成するステップ、または、
前記再構成されたシークレットを使用してトランザクションに署名するステップであって、前記トランザクションは、前記分散型台帳におけるアドレスから暗号通貨を送金する、署名するステップのうちの少なくとも１つを実行するステップをさらに含む、請求項２９に記載の方法。
【請求項３６】
前記取得されるシークレットシェアが決定される前に、
前記シークレットを、前記複数のシークレットシェアに分割するステップであって、前記複数のシークレットシェアの少なくともサブセットは、前記シークレットを再構成するために必要とされる、分割するステップと、
前記複数のシークレットシェアの各それぞれのシークレットシェアをそれぞれのポータブル記憶デバイスまたは媒体に転送するステップとをさらに含み、
各ポータブル記憶デバイスまたは媒体は、前記複数のシェアホルダに配布される、請求項２９に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
[0001]本願は、２０２０年２月２６日に出願された「ＳＥＣＲＥＴ　ＳＰＬＩＴＴＩＮＧ　ＡＮＤ　ＭＥＴＡＤＡＴＡ　ＳＴＯＲＡＧＥ（シークレット分割およびメタデータ記憶）」と題する米国仮特許出願第６２／９８１，６６３号（代理人整理番号２７０．０３４ＵＳＰＲ）の利益を主張し、そのすべては、参照により本明細書に組み込まれる。
【背景技術】
【０００２】
[0002]データを安全に格納および送信するために暗号化を使用することができる。鍵は、データの暗号化および解読、またはトランザクションの署名に使用することができる。
【発明の概要】
【課題を解決するための手段】
【０００３】
[0003]コンピューティングデバイスは、少なくとも１つのプロセッサと、少なくとも１つのプロセッサに通信可能に結合された少なくとも１つのメモリとを含む。少なくとも１つのプロセッサは、保護されるべきシークレットを決定するように構成される。少なくとも１つのプロセッサはまた、シークレットを、複数のシークレットシェア（secret share

）に分割するように構成され、シークレットシェアの少なくともサブセットは、シークレットを再構成するために必要とされる。少なくとも１つのプロセッサはまた、各シークレットシェアを、それぞれのシェアホルダに配布するために、それぞれのポータブル記憶デバイスまたは媒体に転送するように構成される。少なくとも１つのプロセッサはまた、各シークレットシェアの少なくともハッシュを用いてメタデータを生成するように構成され、メタデータは、シークレットシェアを用いて、ポータブル記憶デバイスまたは媒体とは別に格納される。

【０００４】

[0004]コンピューティングデバイスは、少なくとも１つのプロセッサと、少なくとも１つのプロセッサに通信可能に結合された少なくとも１つのメモリとを含む。少なくとも１つのプロセッサは、シェアホルダから取得された少なくとも２つのシークレットシェア記憶デバイスまたは媒体の各々から、取得されるシークレットシェアを決定するように構成される。少なくとも１つのプロセッサはまた、シークレットシェアが複数のシェアホルダに配布される前に生成された複数のシークレットシェアの少なくともハッシュのリストを有するメタデータを判定するように構成される。少なくとも１つのプロセッサはまた、少なくとも２つのシークレットシェア記憶デバイスまたは媒体から取得されたシークレットシェアを使用して、シークレットを再構成しようと試みるように構成される。少なくとも１つのプロセッサはまた、取得されたシークレットシェアからシークレットを再構成できない場合、取得されたシークレットシェアのうちの少なくとも１つのシークレットシェアを、メタデータに基づいて、正しくないとして特定するように構成される。

【０００５】

[0005]図面は例示的な実施形態のみを示しており、したがって、範囲を限定するものと見なされるべきではないことを理解した上で、添付の図面を使用して、例示的な実施形態をさらに具体的かつ詳細に説明する。

【図面の簡単な説明】

【０００６】

【図１】[0006]シークレット分割およびメタデータ記憶のための例示的なシステムを示すブロック図である。

【図２】[0007]シークレット分割およびメタデータ記憶のためにシステムにおいて使用される例示的なコンピューティングデバイスを示すブロック図である。

【図３】[0008]例示的なシークレット生成器を示すブロック図である。

【図４】[0009]シークレット分割およびメタデータ記憶のための例示的なシステムを示すブロック図である。

【図５】[0010]シークレットを分割し、メタデータを記憶するための例示的な方法を示すフロー図である。

【図６】[0011]複数のシークレットシェアのうちの少なくとも２つからシークレットを再構成するための例示的な方法を示すフロー図である。

【図７】[0012]本開示のいくつかの実施形態を利用できるコンピュータシステムの例を示す図である。

【発明を実施するための形態】

【０００７】

[0013]一般的な慣例に従って、記載された様々な特徴は、縮尺どおりに描かれておらず、例示的な実施形態に関連する特定の特徴を強調するために描かれている。

[0014]以下の詳細な説明では、本明細書の一部を形成し、特定の例示的な実施形態を例として示す添付の図面を参照する。しかしながら、他の実施形態を利用することができ、論理的、機械的、および電気的な変更を行うことができることを理解されたい。さらに、図面および明細書に示される方法は、個々のステップを実行する場合がある順序を限定するものとして解釈されるべきではない。したがって、以下の詳細な説明は、限定的な意味で解釈されるべきではない。

【０００８】

[0015]キャラクタの文字列は、データの暗号化および解読、ならびに、たとえば暗号通貨トランザクションなどの暗号トランザクションへの署名に使用することができる。特定の文字列を安全に保ち、限られた数の人だけがアクセスできるようにすることが望ましい。これらの文字列は、本明細書では「シークレット」と呼ばれる。シークレットの１つのタイプは、秘密鍵、公開鍵、暗号鍵、解読鍵、署名鍵、ならびに、パスワード、シークレットフレーズ、アカウント番号、または、鍵を再構成するために使用できるニーモニックフレーズ（mnemonic phrase）もしくはシード（seed）を含む（しかしながら、これらに限定されない）暗号鍵である。たとえば、シークレットは、プールされた暗号通貨を保持する分散型台帳におけるアドレスの秘密鍵（または、秘密鍵から導出されるニーモニックまたはシード）である場合がある。そのようなシークレットは、高価値を有する可能性があり、セキュリティを確保するために注意が必要である。さらに、シークレットは、たとえば、文字列として配置されたデジタル画像の生データ、文字列として配置されたデジタルビデオファイルの生データ、文字列として配置されたデジタルオーディオファイルの生データ、または、キャラクタの文字列として配置された他の任意のタイプのデジタルファイルのように、キャラクタの文字列として表すことができる任意のデジタルデータとすることができる。

【００００９】

[0016]本明細書で使用されるように、「分散型台帳」という用語は、相互接続された複数のノードにわたって配布され、複数のノードが、台帳のコピーを格納する電子台帳を称する。いくつかの例では、分散型台帳は、分散型台帳内に格納されたデータを検証するために１つまたは複数のブロックチェーンを実施することができる。ブロックチェーンは、そのブロックを検証する各ブロックに添付された作業証明シール（proof-of-work seal）（ハッシュなど）を使用して、一度に１ブロックずつ構築される検証可能な永久台帳である。ブロックチェーンでは、前のブロックのハッシュが、現在のブロックに含まれているため、再帰により、現在のハッシュも、以前のすべてのブロックを、元々の起源ブロックに戻して検証する。ハッシュをブロックチェーンに挿入すると、そのハッシュが永続的に記録され、そのブロックがチェーンに追加された瞬間に、ハッシュされたデータのタイムスタンプ付きの存在証明を検証する公証人として機能する。将来のブロックは、チェーンに格納されたデータの操作、またはチェーンの再編成から保護するレイヤを追加するので、チェーンにおける以前のブロックに変更を加えることができないという追加の確実性を提供する。ブロックチェーンは、分散型台帳の実施である。例示的なブロックチェーンは、Ｂｉｔｃｏｉｎブロックチェーン、Ｅｔｈｅｒｅｕｍブロックチェーン、Ｒａｖｅｎｃｏｉｎブロックチェーン、ＢｉｇｃｈａｉｎＤＢ、Ｂｉｌｌｏｎ、Ｃｈａｉｎ、Ｃｏｒｄａ、Ｃｒｅｄｉｔｓ、Ｅｌｅｍｅｎｔｓ、Ｍｏｎａｘ、Ｆａｂｒｉｃ、ＨｙｄｒａＣｈａｉｎ、Ｈｙｐｅｒｌｅｄｇｅｒ、Ｍｕｌｔｉｃｈａｉｎ、Ｏｐｅｎｃｈａｉｎ、Ｑｕｏｒｕｍ、Ｓａｗｔｏｏｔｈ、およびＳｔｅｌｌａｒを含むが、これらに限定されない。

【００１０】

[0017]対称暗号化および解読では、同じ鍵を使用して、暗号化および解読、たとえば、異なるブロックチェーンアドレス、アカウント、および／またはウォレットの１つまたは複数の秘密鍵の暗号化および解読を行うことができる。たとえば、Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＡＥＳ）鍵を使用して、データを対称的に暗号化および／または解読できる。いくつかの構成では、シークレットは、ＡＥＳ鍵（またはＡＥＳ鍵から導出されるニーモニックまたはシード）である場合がある。限定することなく、対称鍵は、以下の暗号化、すなわち、Ｔｗｏｆｉｓｈ、Ｓｅｒｐｅｎｔ、Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＡＥＳ）、Ｂｌｏｗｆｉｓｈ、ＣＡＳＴ５、Ｋｕｚｎｙｅｃｈｉｋ、ＲＣ４、Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＤＥＳ）、Ｔｒｉｐｌｅ ＤＥＳ（３ＤＥＳ）、Ｓｋｉｐｊａｃｋ、Ｓａｆｅｒ＋／＋＋（Ｂｌｕｅｔｏｏｔｈ）、ＩＤＥＡおよび／または他のサイファブロックコーディング（ＣＢＣ）バリエーションのいずれかに従って動作することができる。

【００１１】

[0018]いくつかの構成では、シークレットは、非対称鍵（または、非対称鍵から導出されるニーモニックまたはシード）である場合がある。秘密鍵と、対応する公開鍵とを含む「公開／秘密鍵ペア」は、非対称暗号化において使用する場合がある。秘密鍵および公開鍵は、それぞれ解読秘密鍵および暗号化公開鍵と呼ばれることもある。公開鍵は、暗号化に使用された公開鍵に対応する秘密鍵を使用してのみ解読できるデータの暗号化に使用できる。例では、公開鍵を使用して、分散型台帳におけるトランザクションアドレスを生成することができ、対応する秘密鍵のみが、トランザクションアドレスから資金を使うトランザクションに署名できる。これは、暗号化および解読（または、トランザクションの署名）に、同じ鍵が使用されないため、「非対称」暗号化／解読と呼ばれることがある。いくつかの構成では、秘密鍵および公開鍵は、代わりにそれぞれ署名鍵および署名検証鍵と呼ばれることがある。一般に、秘密鍵（場合によっては公開鍵）を安全に保つことが望ましい。限定することなく、非対称鍵は、以下の暗号化、すなわち、Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ（ＲＳＡ）および楕円曲線暗号（ＥＣＣ）（たとえば、Ｃｕｒｖｅ２５５１９）、エドワーズ曲線デジタル署名アルゴリズム（ＥｄＤＳＡ）（たとえば、Ｅｄ２５５１９）などのいずれかに従って動作することができる。

【００１２】

[0019]鍵を安全に保つことと、必要なときにアクセスできるようにすることとの間には、しばしばトレードオフがある。場合によっては、シークレットへのアクセスを１人のユーザに限定することは望ましくない。さらに、複数の人がシークレットを使用する必要があることが望ましい場合もある。例では、これは、組織の複数の取締役、役員、パートナ、および／または従業員が、鍵の使用時に参加する必要がある場合に役立つ。シークレットは、複数のシェアに分割でき、シェアのサブセットを使用して、シークレットを再構成できる。例では、シークレットは、Ｓｈａｍｉｒシークレットシェア（シャミールの秘密の共有）および／または多項式補間（polynomial interpolation）を使用して、シークレットシェアのセットに分割される。「部分」、「シェア」、および「構成要素」（および、それらの変形）という用語は、分割されたシークレット（暗号鍵など）の複数の部分のうちの１つの部分を称するために、本明細書では置換可能に使用される。例では、特定のシークレットを再構成するために、特定の量のシークレットシェアが必要になる場合がある。たとえば、特定のシークレットを再構成するために、Ｎ個のシークレットシェアのうちのＭ個が必要とされるように、特定のシークレットが、Ｎ個のシークレットシェアに分割される場合がある。例では、Ｎ個のシークレットシェアを、様々なシェアホルダに配布することができる。例では、各シークレットシェアは、異なるシークレットシェアを受け取る別の個人または人々のグループと重複しない、別の個人または人々のグループ（シェアホルダ）に配布される。しかしながら、いくつかの構成では、複数のシークレットシェアが、同じ個人または人々のグループに提供される場合がある。

【００１３】

[0020]例では、シークレットシェアは、たとえば、ＵＳＢ鍵／メモリスティック（または他のソリッドステートドライブ）、または光学または磁気ディスクなど、シェアホルダに配布するために、ポータブル記憶デバイスまたは媒体に格納することができる。例では、シークレットシェアを画面に表示し、書き留め、または別の手法で（Ｑｕｉｃｋ　Ｒｅｓｐｏｎｓｅ（ＱＲ）コード、バーコードなどへの）印刷によって物理的に配布できる。例では、シークレットのシェア（たとえば、鍵）は、電子メール、ショートメッセージサービス（ＳＭＳ）、マルチメディアメッセージングサービス（ＭＭＳ）、インスタントメッセージング、プッシュ通知（プッシュ検証通知など）、通知のポーリング（またはプル）、またはＢｌｕｅｔｏｏｔｈ、Ｗｉ－Ｆｉ、または近距離無線通信（ＮＦＣ）送信のうちの少なくとも１つを使って、ユーザのデバイスへ電子的に配布できる。

【００１４】

[0021]シークレットを分割し、異なる人々（または人々のグループ）に配布すると、セキュリティのレイヤが追加される。なぜなら、これは、鍵および暗号鍵を、悪意を持って再構成するために、異なるシェアホルダによる共謀が必要とされることを意味するからで

ある。シークレットを再構成する必要がある場合は、Ｎ個のシークレットシェアのうちの少なくともＭ個を収集する必要がある。再構成に失敗した場合は、シークレットシェアが、正しいシークレットに再構成しないか、再構成中にエラーが発生したために、障害ポイントを特定することが困難である場合がある。言い換えると、障害の原因となったシークレットシェアを特定することが困難になる。最悪のシナリオでは、あまりにも多くのシークレットシェアが失われたり、盗まれたり、破損したりすると、シークレットが回復不能になる可能性がある。

【００１５】

[0022]したがって、本システムおよび方法は、アクションを実行するために多数のシェアが必要とされる場合に、複数のシェアホルダが、シークレットのシェアを保持することを必要とするシステムを改善する。具体的には、本システムおよび方法は、シークレットの再構成中に問題があれば、問題の原因をトラブルシューティングするために使用できるメタデータを生成する。このメタデータは、（１）特定のシークレットシェアの配布手段（たとえば、エビデンスバッグ）を特定のシークレットシェアへ、および／または、（２）特定のシークレットシェアの配布手段（たとえば、エビデンスバッグ（evidence bag））を特定のシークレット／ウォレット番号へマッピングすることができる。

【００１６】

[0023]本システムおよび方法は、シークレットの配布および記憶のため、従来のシステムを、他の手法で改善することができる。第１に、特定のシークレットシェアに対する配布手段（たとえば、エビデンスバッグ）を、特定のシークレットシェアに付番することに加えて、メタデータは、シークレットシェアのハッシュを含む。したがって、いくつかの構成では、取得されたシークレットシェアのハッシュは、シークレットを再構成する試みが行われる前に検証できる。たとえば、シークレットの再構成を任された人またはスクリプトは（たとえば、シークレットの再構成を試みる前に）、以下、すなわち、（１）シークレットシェアがシェアホルダに配布される前にシークレットシェアから生成されたハッシュを、（２）シークレットシェアがシークレットの再構成に使用される直前または直後に取得されたシークレットシェアから生成されたハッシュと比較することができる。これにより、正しいシークレットシェア（シェアホルダが主張するシークレットシェア）のみが、シークレットの再構成に使用されるようになる。

【００１７】

[0024]第２に、本明細書に記載のＭオブＮシステム（ここでは、いくつかの例では、Ｎ＞Ｍ＞１）を使用すると、単一の障害ポイントを排除するであろう。具体的には、鍵を回復不能にするためには、シークレットが不正な手法で再構成される前に、Ｍ個のシェアが紛失または盗難されねばならない（すなわち、シェアホルダのうちのＭ人が共謀する必要がある）。紛失／盗難された単一のシークレットシェア（または、悪意のある１人のシェアホルダ）では、シークレットを再構成できなかった。

【００１８】

[0025]第３に、本明細書に記載のシステムおよび方法において使用されるメタデータは、メタデータの紛失または盗難に起因するあらゆるリスクを軽減しながら、（上記のような）利益をもたらす。メタデータの１つまたは複数のコピーが紛失または盗難された場合でも、不正なホルダは、未処理のシークレットシェアがどれだけ存在するか（および、それらのシークレットシェアのハッシュ）を単にするが、実際のシークレットシェアを所有することはない。

【００１９】

[0026]本明細書で使用されるように、「暗号化」という用語またはその変形は、不正アクセスを阻止するために、データをコードに変換することを称する。暗号化は、単一の暗号化鍵を使用して、データの暗号化と解読との両方を行う対称暗号化や、公開鍵を使用して、データの暗号化を行い、対応する秘密鍵を使用して、データを解読する非対称暗号化など、様々な手法で実施できる。

【００２０】

[0027]本明細書で使用されるように、「署名」という用語またはその変形は、たとえばシークレットを使用して、所望のトランザクションに関連付けられたデータを追加または変更することを称する。

【００２１】

[0028]本明細書で使用されるように、特に明記しない限り、「ユーザ」という用語は、本明細書に記載される機能のいずれかを開始するためにカスタマデバイス１０２にアクセスする人（または、たとえばスクリプトのような、自動化された命令）を称する。

【００２２】

[0029]本明細書で使用されるように、「ウォレット」という用語は、暗号通貨などのデジタル資産を格納および／または管理するために使用される命令のセット、デジタルファイル、および／またはメモリを称する。本明細書における記載は、暗号通貨に言及している箇所もあるが、他のタイプのデジタル資産が、ウォレットで保持および管理される場合もある。いくつかの例では、ウォレットは、１つまたは複数の秘密鍵、１つまたは複数の秘密鍵から導出される１つまたは複数の公開鍵、および／または１つまたは複数の秘密鍵および／または１つまたは複数の公開鍵から導出される１つまたは複数のトランザクションアドレスによって定義することができる。いくつかの例では、ウォレットは、１つまたは複数のプライベートアカウント鍵（および、任意選択の、対応する公開アカウント鍵）によって定義され、各々が１つまたは複数の子および／または孫トランザクション鍵を有することができる。

【００２３】

[0030]図１は、シークレット分割およびメタデータ記憶のための例示的なシステム１００を示すブロック図である。システム１００は、コンピューティングデバイス１０２と、複数の任意選択のコンピューティングデバイス１０４（任意選択のコンピューティングデバイス１０４－１から任意選択のコンピューティングデバイス１０４－Ａまでなど）とを含む。コンピューティングデバイス１０２およびコンピューティングデバイス１０４の各々は、モバイル電話、タブレットコンピュータ、モバイルメディアデバイス、モバイルゲームデバイス、ラップトップコンピュータ、車両ベースのコンピュータなどのモバイルコンピューティングデバイス、または専用端末、公衆端末、キオスク、サーバ、またはデスクトップコンピュータなどの非モバイルデバイスのいずれかとして実施することができる。各コンピューティングデバイス１０４は、少なくとも１つのネットワーク１０６（ネットワーク１０６－１からネットワーク１０６－Ａまでなど）を使用してコンピューティングデバイス１０２に通信可能に結合される。例では、少なくとも１つのネットワーク１０６は、少なくとも１つのワイヤネットワークおよび／または少なくとも１つのワイヤレスネットワークを含む。例では、ワイヤネットワークとワイヤレスネットワークとの任意の組合せを使用して、コンピューティングデバイス１０４をコンピューティングデバイス１０２に結合する。例では、少なくとも１つのネットワーク１０６は、少なくとも１つのローカルエリアネットワーク（ＬＡＮ）、少なくとも１つのワイドエリアネットワーク（ＷＡＮ）、またはインターネットのうちの少なくとも１つを含む。例では、ローカルエリアネットワーク、ワイドエリアネットワーク、またはインターネットの任意の組合せが、コンピューティングデバイス１０４をコンピューティングデバイス１０２に結合するための少なくとも１つのネットワーク１０６として使用される。いくつかの構成では、コンピューティングデバイス１０２は、他の時間中、（いずれのワイヤレスネットワークにもワイヤネットワークにも接続されていない）「エアギャップ」されている場合に、１つまたは複数の他のコンピューティングデバイス１０４に結合されている場合もある。例では、コンピューティングデバイス１０２およびコンピューティングデバイス１０４の各々は、少なくとも１つのメモリ、少なくとも１つのプロセッサ、少なくとも１つの任意選択のネットワークインターフェース、少なくとも１つの任意選択のディスプレイデバイス、少なくとも１つの任意選択の入力デバイス、および少なくとも１つの電源を含む。

【００２４】

[0031]図２は、シークレット分割およびメタデータ記憶のためにシステム１００におい

て使用される例示的なコンピューティングデバイス１０２を示すブロック図である。コンピューティングデバイス１０２は、少なくとも１つのメモリ２０２、少なくとも１つのプロセッサ２０４、任意選択の少なくとも１つのネットワークインターフェース２０６、任意選択のシークレット生成器２０８、任意選択のＳｈａｍｉｒシークレットシェアモジュール２１０、任意選択のハッシュ機能２１２、任意選択のディスプレイデバイス２１４、任意選択の入力デバイス２１６、任意選択の電源２１８、任意選択のシークレット再構成モジュール２２０、任意選択の検証モジュール２２２、および任意選択のメタデータモジュール２２４を含む。

【００２５】

[0032]例では、少なくとも１つのメモリ２０２は、情報を格納するために使用される任意のデバイス、メカニズム、またはデータが投入されたデータ構造である。例では、少なくとも１つのメモリ２０２は、任意のタイプの揮発性メモリ、不揮発性メモリ、および／またはダイナミックメモリであるか、またはそれらを含むことができる。たとえば、少なくとも１つのメモリ２０２は、ランダムアクセスメモリ、メモリ記憶デバイス、光学メモリデバイス、磁気媒体、フロッピーディスク、磁気テープ、ハードドライブ、消去可能プログラマブル読取専用メモリ（ＥＰＲＯＭ）、電気的消去可能プログラマブル読取専用メモリ（ＥＥＰＲＯＭ）、光学媒体（コンパクトディスク、ＤＶＤ、Ｂｌｕ－ｒａｙディスク、Ｍ－ＤＩＳＣなど）などとすることができる。いくつかの実施形態によれば、少なくとも１つのメモリ２０２は、１つまたは複数のディスクドライブ、フラッシュドライブ、１つまたは複数のデータベース、１つまたは複数のテーブル、１つまたは複数のファイル、ローカルキャッシュメモリ、プロセッサキャッシュメモリ、リレーショナルデータベース、フラットデータベースなどを含むことができる。それに加えて、当業者は、少なくとも１つのメモリ２０２として使用できる情報を格納するための多くの追加のデバイスおよび技法を理解するであろう。少なくとも１つのメモリ２０２は、少なくとも１つのプロセッサ２０４で、１つまたは複数のアプリケーションまたはモジュールを実行するための命令を格納するために使用することができる。たとえば、少なくとも１つのメモリ２０２は、１つまたは複数の例において、任意選択のシークレット生成器２０８、任意選択のＳｈａｍｉｒシークレットシェアモジュール２１０、任意選択のハッシュ機能２１２、任意選択のシークレット再構成モジュール２２０、任意選択の検証モジュール２２２、および／または任意選択のメタデータモジュール２２４の機能を実行するために必要とされる命令のすべてまたはいくつかを収納するために使用できる。

【００２６】

[0033]少なくとも１つのプロセッサ２０４は、汎用プロセッサ（ＧＰＰ）、また（フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、特定用途向け集積回路（ＡＳＩＣ）、または他の集積回路または回路構成のような）専用の、または任意のプログラマブルロジックデバイスなどの任意の知られているプロセッサとすることができる。例では、任意選択のシークレット生成器２０８、任意選択のＳｈａｍｉｒシークレットシェアモジュール２１０、任意選択のハッシュ機能２１２、任意選択のシークレット再構成モジュール２２０、任意選択の検証モジュール２２２、および／または任意選択のメタデータモジュール２２４のいずれかが、少なくとも１つのプロセッサ２０４、および少なくとも１つのメモリ２０２によって実施される。

【００２７】

[0034]例では、少なくとも１つの任意選択のネットワークインターフェース２０６は、ネットワーク（システム１００の少なくとも１つのネットワーク１０６のうちの１つなど）と通信するための少なくとも１つの任意選択のアンテナを含むか、またはそれに結合される。例では、少なくとも１つの任意選択のネットワークインターフェース２０６は、イーサネットインターフェース、セルラ無線アクセス技術（ＲＡＴ）無線、Ｗｉ－Ｆｉ無線、Ｂｌｕｅｔｏｏｔｈ無線、または近距離無線通信（ＮＦＣ）無線のうちの少なくとも１つを含む。例では、少なくとも１つの任意選択のネットワークインターフェース２０６は、ローカルエリアネットワーク（ＬＡＮ）またはワイドエリアネットワーク（ＷＡＮ）を

使用して、リモートサーバとの、十分な速度でのセルラデータ通信（モバイルインターネット）を確立するように構成されたセルラ無線アクセス技術無線を含む。例では、セルラ無線アクセス技術は、パーソナル通信サービス（ＰＣＳ）、特殊移動無線（ＳＭＲ）サービス、拡張特殊移動無線（ＥＳＭＲ）サービス、高度ワイヤレスサービス（ＡＷＳ）、符号分割多元接続（ＣＤＭＡ）、移動通信用グローバルシステム（ＧＳＭ）サービス、広帯域符号分割多元接続（Ｗ－ＣＤＭＡ）、ユニバーサルモバイル通信システム（ＵＭＴＳ）、マイクロ波アクセス用ワールドワイドインタオペラビリティ（ＷｉＭＡＸ）、第３世代パートナシッププロジェクト（３ＧＰＰ（登録商標））、ロングタームエボリューション（ＬＴＥ）、高速パケットアクセス（ＨＳＰＡ）、第３世代（３Ｇ）、第４世代（４Ｇ）、第５世代（５Ｇ）など、または他の適切な通信サービス、またはそれらの組合せのうちの少なくとも１つを含む。例では、少なくとも１つの任意選択のネットワークインターフェース２０６および／または少なくとも１つの任意選択のネットワークインターフェース２０６は、ワイドエリアネットワークではなく、リモートサーバと通信する、ワイヤレスローカルエリアネットワークと通信するように構成されたＷｉ－Ｆｉ（ＩＥＥＥ８０２．１１）無線を含む。例では、少なくとも１つの任意選択のネットワークインターフェース２０６および／または少なくとも１つの任意選択のネットワークインターフェース２０６は、パッシブ近距離通信（ＮＦＣ）タグ、アクティブ近距離通信（ＮＦＣ）タグ、パッシブ無線周波数識別（ＲＦＩＤ）タグ、アクティブ無線周波数識別（ＲＦＩＤ）タグ、近接カード、または他のパーソナルエリアネットワークデバイスなどの近接通信に限定される近距離無線通信デバイスを含む。例では、同じ少なくとも１つの任意選択のネットワークインターフェース２０６および／または少なくとも１つの任意選択のネットワークインターフェース２０６は、ネットワークへの外部ゲートウェイデバイス（ＮＦＣ支払端末など）との通信にも使用される。

【００２８】

[0035]例では、任意選択の少なくとも１つのディスプレイデバイス２１４は、発光ダイオード（ＬＥＤ）、液晶ディスプレイ（ＬＣＤ）、発光ダイオード（ＬＥＤ）ディスプレイ、有機発光ダイオード（ＯＬＥＤ）ディスプレイ、電子インクディスプレイ、電界放出ディスプレイ（ＦＥＤ）、表面伝導型電子放出ディスプレイ（ＳＥＤ）、またはプラズマディスプレイのうちの少なくとも１つを含む。例では、任意選択の少なくとも１つの入力デバイス２１６は、タッチスクリーン（容量性および抵抗性タッチスクリーンを含む）、タッチパッド、容量性ボタン、機械式ボタン、スイッチ、ダイヤル、キーボード、マウス、カメラ、生体認証センサ／スキャナなどを含む。例では、任意選択の少なくとも１つのディスプレイデバイス２１４および任意選択の少なくとも１つの入力デバイス２１６は、コンピューティングデバイス１０２とのユーザ対話のために、ヒューマンマシンインターフェース（ＨＭＩ）に組み合わされる。例では、ネットワークノード１０２の様々な構成要素に電力を提供するために、少なくとも１つの任意選択の電源２１８が使用される。

【００２９】

[0036]コンピューティングデバイス１０２の少なくとも１つのプロセッサ２０４は、少なくとも１つのシークレットを安全に生成するように構成される。例では、これは、任意選択のシークレット生成器２０８において実施される。コンピューティングデバイス１０２の少なくとも１つのプロセッサ２０４は、少なくとも１つのシークレットを安全に生成するように構成することができる。

【００３０】

[0037]図３は、シークレット生成器２０８の例を示すブロック図である。例では、シークレット生成器２０８は、異なるデータを同時またはほぼ同時に生成する。例では、シークレット生成器２０８は、（１）秘密鍵３２６、（２）秘密鍵３２６から導出される任意選択のニーモニック／シード３２８、（３）任意選択の公開鍵３３０、および／または、（４）（たとえば、暗号通貨を保持する）分散型台帳における少なくとも１つの任意選択のアドレス３３２を生成する。例では、秘密鍵３２６、任意選択のニーモニック／シード３２８、任意選択の公開鍵３３０、および少なくとも１つの任意選択のアドレス３３２の

各々が、異なるキャラクタの文字列として表される。

【００３１】

[0038]秘密鍵３２６またはニーモニック／シード３２８は、（後に分割され、シェアホルダに配布される）シークレットとしてもよい。例では、任意選択の公開鍵３３０は、秘密鍵３２６に対応し、秘密鍵３２６から導出される。例では、秘密鍵３２６および公開鍵３３０（および、任意選択でアドレス）は、単一の関数を使用して生成される。しかしながら、秘密鍵３２６は一般に、公開鍵３３０から導出されない。例では、秘密鍵３２６を使用して、任意選択のアドレス３３２から資金を支出することができる一方、任意選択の公開鍵３３０を使用して、アドレス３３２に出入りするトランザクションを監視する、またはアドレス３３２に暗号通貨を送金することができる。例では、秘密／公開鍵ペアが生成され、公開鍵３３０のハッシュは、（ウォレットへのトランザクションに使用できる）分散型台帳におけるアドレスである。あるいは、公開鍵３３０を使用して、データを暗号化する一方、秘密鍵３２６を使用して、データを解読することができる。秘密鍵３２６は一般に安全に保たれ（アクセスできる人は、比較的少なく）、公開鍵３３０は、より自由にシェアされる（アクセスできる人は、より多い）。

【００３２】

[0039]秘密鍵３２６を紛失した場合、ニーモニックコードまたはシード３２８を使用して、秘密鍵３２６を回復することができる。例では、ニーモニックコードまたはシード３２８は、秘密鍵３２６を導出できる単語のセット（たとえば、１２語または１５語）である。例では、ニーモニックコードまたはシード３２８は、最初に秘密鍵３２６から導出される。例では、アドレス３３２は、公開鍵３３０のハッシュである場合がある。したがって、アドレスは、公開鍵３３０から導出されるが、公開鍵３３０は、アドレス３３２から導出されない場合がある。

【００３３】

[0040]任意選択で、コンピューティングデバイス１０２の少なくとも１つのプロセッサ２０４は、ランダムな特性または疑似ランダムな特性を有するシーケンスを生成することによって、秘密鍵３２６を生成するように構成される。任意選択で、秘密鍵３２６は、Ｂｉｔｃｏｉｎ Ｉｍｐｒｏｖｅｍｅｎｔ Ｐｒｏｐｏｓａｌ ３９（ＢＩＰ３９）（ｈｔｔｐｓ：／／ｇｉｔｈｏｂ．ｃｏｍ／ｂｉｔｃｏｉｎ／ｂｉｐｓ／ｂｌｏｂ／ｍａｓｔｅｒ／ｂｉｐ－００３９．ｍｅｄｉａｗｉｋｉで入手でき、参照により本明細書に組み込まれる）に従って生成することができる。例では、対応する公開鍵３３０は、楕円曲線乗算（暗号関数の一種）を使用することによって秘密鍵３２６から生成される。次に、前述のように、アドレス３３２は、公開鍵３３０のハッシュである場合がある。

【００３４】

[0041]再び図２に戻って示すように、少なくとも１つのプロセッサ２０４は、シークレットを再構成するために、シークレットシェアの少なくとも１つのサブセットを使用できるシークレットシェアのセットに、シークレットを分割するようにさらに構成される。例では、これはＳｈａｍｉｒシークレットシェアモジュール２１０において実施される。例では、分割は構成可能であり、シークレットを再構成するために特定の量のシークレットシェアが必要になる場合がある。たとえば、特定のシークレットを再構成するためにＮ個のシークレットシェアのうちのＭ個が必要とされるように、特定のシークレットをＮ個のシークレットシェアに分割することができる。例では、各シークレットシェアは、異なるシェアホルダに配布される。例では、様々なシェアホルダに配布される前に、（以下に詳しく記載されるように）任意選択で、シークレットシェアを検証できる。例では、シークレットは、Ｓｈａｍｉｒシークレットシェアおよび多項式補間のうちの少なくとも１つを介してＮ個のシークレットシェアに分割される。任意選択で、シェアホルダに配布する前に、（たとえば、対称鍵または非対称鍵を使用して）シークレットシェアを暗号化することができる。本明細書で使用されるように、「シェアホルダ」とは、少なくとも１つのシークレットシェアを安全に格納することを委託された個人または組織である。言い換えれば、シークレットシェアは、シークレットの生成および分割の後、保管のためにシェアホ

ルダに配布される。

【００３５】

[0042]例では、各シークレットシェアは、別個の記憶デバイスまたは媒体に転送することができる。例では、各シークレットシェアは、アーカイブグレードの光ディスク、たとえば、数百年または１，０００年にわたってデータを保持するＭＩＬＬＥＮＮＩＡＬ　ＤＩＳＣ（Ｍ－ＤＩＳＣ）に書き込まれる。任意選択で、各個別のシークレットシェアは、（コンテンツの改ざんを困難にする）改ざん防止、および／または（セキュリティエンベロープまたはパッケージの内容が、改ざんされているか否かを示すメカニズムを提供する）不正開封防止されたセキュリティエンベロープまたはパッケージにも配置される。セキュリティエンベロープまたはパッケージが使用されているか否かに関わらず、各シークレットシェアは、それぞれの記憶媒体に配置されると、それぞれのシェアホルダに配布される。一般に、各シークレットシェアは、異なるシェアホルダに与えられるが、１人のシェアホルダが、生成されたシークレットシェアの複数を受け取る構成も可能である。

【００３６】

[0043]代替的または追加的に、電子メール、ショートメッセージサービス（ＳＭＳ）、マルチメディアメッセージングサービス（ＭＭＳ）、インスタントメッセージング、プッシュ通知、またはプッシュ検証通知のうちの少なくとも１つなどによって、少なくとも１つのネットワークインターフェース２０６を使用して、シェアホルダ（またはシェアホルダのグループ）に属するデバイスに、シークレットシェアを、電子的に配布することができる。例では、シークレットシェアは、シェアホルダに（たとえば、クイックレスポンス（ＱＲ）コードとして）提供される媒体に、表示、印刷、または別の手法で固定され、シェアホルダは、シークレットシェアを、対応するコンピューティングデバイス１０４に入力し、自分の手書きで書き写し、および／または、印刷物自体を安全に格納する。

【００３７】

[0044]コンピューティングデバイス１０２の少なくとも１つのプロセッサ２０４は、シークレットおよび／または個々のシークレットシェアのハッシュを生成するようにさらに構成される。例では、これは、暗号ハッシュ機能２１２において実施される。例では、シークレットまたはシークレットシェアのハッシュは、シークレットシェアが配布される前に生成され、検証目的で保存される。例では、ハッシュ機能２１２は、入力（シークレットまたはシークレットシェアなどのキャラクタ文字列）を受け取り、ハッシュ（異なるキャラクタの文字列）を返す。ハッシュ機能２１２への入力は、出力（ハッシュ）を一意に決定する。言い換えれば、特定のハッシュ機能２１２は、１つの特定の入力から特定の値のハッシュを生成するだけであり、入力に対するどの変化も、異なる値のハッシュを生成する。以下で論じるように、シークレットシェアのハッシュを比較することは、シークレットシェア自体を検証するためのプロキシとして機能する。使用できるハッシュ機能２１２の例は、セキュアハッシュアルゴリズム（ＳＨＡ）－１、ＳＨＡ－２関数（たとえば、ＳＨＡ－２５６またはＳＨＡ－５１２（ＳＨＡ２－５１２と呼ばれることもある））、またはＭＤ４、ＭＤ５、ＲＩＰＥＭＤ１６０などのいずれかを含むが、これらに限定されない。

【００３８】

[0045]例では、コンピューティングデバイス１０２の少なくとも１つのプロセッサ２０４は、シークレットシェアのセットから、シークレットを再構成するようにさらに構成され、ここでは、たとえば、シークレットを再構成するために、Ｎ個のシークレットシェアのうちのＭ個が必要とされるように、シークレットを再構成するために、シークレットシェアの少なくとも１つのサブセットを使用することができる。例では、これは、シークレット再構成モジュール２２０において実施される。例では、少なくとも１つのプロセッサ２０４は、シェアホルダのサブセットから、サブセット（たとえば、Ｎ個のうちのＭ個）のシークレットシェアを取得するように構成される。例では、シークレットシェアがポータブル記憶デバイスまたは媒体（たとえば、光ディスク）で配布された場合、取得は、コンピューティングデバイス１０２に物理的に持ち込まれたポータブル記憶デバイスまたは

媒体から、シークレットシェアのサブセットを読み取ることを含む。あるいは、シークレットシェアが、印刷物（たとえば、バーコードまたはＱＲコード（登録商標））で配布された場合、取得は、カメラやスキャナなどの画像デバイスを使用して（シェアホルダによって物理的に持ち込まれた）シークレットシェアのサブセットをスキャンすることを含む。あるいは、シークレットシェアが、少なくとも１つのネットワーク１０６を介して電子的に配布された場合、取得は、少なくとも１つのネットワーク１０６を介して、シェアホルダの電子デバイス１０４から、シークレットシェアのサブセットを受け取ることを含むことができる。

【００３９】

[0046]シークレットシェアのサブセットが（たとえば、エアギャップされたコンピューティングデバイス１０２に）取得されると、シークレット再構成モジュール２２０は、シークレットを安全に再構成するように構成される。例では、（たとえば、Ｓｈａｍｉｒシークレットシェアモジュール２１０によって実行される）Ｓｈａｍｉｒシークレットシェアは、シークレット４３４－１を使用して、（Ｍ－１）次の多項式を定義することを含み、Ｎ個のシークレットシェア４３６－１の各々は、定義された多項式で指摘される。これらの例では、Ｎ個の取得されたシークレットシェア４３６－２のうちの少なくともＭ個から、元々の多項式を決定することによって、シークレット４３４－２が（たとえば、シークレット再構成モジュール２２０において）再構成される。

【００４０】

[0047]しかしながら、シークレットシェアは、配布前に暗号化されていた場合、シークレットが再構成される前に解読される可能性がある。シークレットシェアが配布前に対称鍵で暗号化される例では、同じ対称鍵を使用してシークレットシェアを解読してから、シークレットを再構成することができる。あるいは、シークレットシェアが配布前にそれぞれの非対称鍵（たとえば、公開鍵）で暗号化される場合、それぞれの非対称鍵に対応する解読鍵（たとえば、公開鍵に対応する秘密鍵）を使用してシークレットシェアを解読してから、シークレットを再構成することができる。シークレットシェアがシェアホルダへの配布前に暗号化されていない場合、シークレットの再構成の前に解読する必要はない。

【００４１】

[0048]例では、コンピューティングデバイス１０２の少なくとも１つのプロセッサ２０４は、（１）少なくとも１つのシークレットシェア、および／または、（２）再構成されたシークレット自体を検証するようにさらに構成される。例では、これは、検証モジュール２２２において実施される。例では、少なくとも１つのプロセッサ２０４は、２つの異なる時間に得られたハッシュを比較するように構成される。例では、少なくとも１つのプロセッサ２０４は、（１）シークレットシェアがシェアホルダに配布される前にシークレットシェアから生成されたハッシュを、（２）シークレットシェアがシークレットの再構成に使用される直前または直後に配布されたシークレットシェアから生成されたハッシュと比較することができる。２つのハッシュが一致する場合、（ハッシュが生成された）シークレットシェアが同じであることが検証される。たとえば、シェアホルダから取得されたシークレットシェアは、シェアホルダに元々与えられていたシークレットシェアと同じである。

【００４２】

[0049]代替的または追加的に、少なくとも１つのプロセッサ２０４は、（１）シークレットが分割される前にシークレットから生成されたハッシュを、（２）再構成後のシークレットから生成されたハッシュと比較することができる。２つのハッシュが一致する場合、ハッシュが生成されたシークレットは同じであると検証される。たとえば、再構成されたシークレットは、元々のシークレットと同じである。本明細書で論じられる様々な検証は、任意選択であることに留意されたい。

【００４３】

[0050]例では、コンピューティングデバイス１０２の少なくとも１つのプロセッサ２０４は、コンピューティングデバイス１０２において生成されたシークレットおよび／また

はシークレットシェアに関するメタデータを収集および格納するようにさらに構成される。例では、これはメタデータモジュール２２４において実施される。とりわけ、メタデータは、シークレットの再構成の前および／または後に、シークレットシェアを検証するために使用できる。さらに、メタデータを使用して、シークレットの再構成中にエラーが発生した場合（または、取得されたシークレットシェアを使用して、正しくないシークレットが再構成された場合）、シェアホルダから取得されたどのシークレットシェアが、障害の原因であったかを特定できる。

【００４４】

[0051]例では、メタデータは、（１）シークレットシェアのハッシュのリスト、（２）シークレットを用いて生成された（および、シークレットに対応する）アドレス、（３）特定のシークレット／ウォレット番号への各シークレットシェアの配布手段（たとえば、エビデンスバッグ識別子）のマッピング、（４）ハッシュ機能２１２コード（たとえば、シークレットシェアをハッシュするために実行可能な命令のセット）のコピー、および／または、（５）シークレットを分割するために使用されるコード（たとえば、Ｓｈａｍｉｒ分割を実行するために実行可能な命令のセット）のコピーを含む。例では、メタデータの各コピーは、たとえばＭ－ＤＩＳＣなどの個別のポータブル記憶デバイスまたは媒体に保存される。代替的または追加的に、メタデータをパスワードマネージャソフトウェアに格納したり、保管用にＱＲコード（登録商標）として印刷したり、クラウドベースのストレージに電子的に送信したりすることができる。

【００４５】

[0052]図４は、シークレット４３４－１分割およびメタデータ４４０記憶のための例示的なシステム１００を示すブロック図である。具体的には、図４は、（１）シークレット４３４－１が生成され、シークレットシェア４３６－１に分割される、（２）メタデータ４４０が生成される、（３）シークレットシェア４３６－１が、シェアホルダ４４２－１から４４２－Ｎに配布される、（４）シークレットシェア４３６－２が取得される、（５）取得されたシークレットシェア４３６－２からシークレット４３４－２が再構成される、様々な段階を示す。いくつかの構成では、コンピューティングデバイス１０２が（たとえば、少なくとも１つのネットワーク１０６を介して）他のコンピューティングデバイス１０４に結合されている間に、５つの段階のうちのいくつかを実行することができる一方、コンピューティングデバイス１０２が、エアギャップされている（どのワイヤネットワークまたはワイヤレスネットワークにも結合されていない）間に、５つの段階のうちの他の段階を実行することができる。例では、段階（１）は、コンピューティングデバイス１０２がエアギャップされている間に実行される一方、段階（２）～（５）の少なくともいくつかは、コンピューティングデバイス１０２が、少なくとも１つの他のコンピューティングデバイス１０４に結合されている間に実行される。

【００４６】

[0053]シークレットシェア４３６－２またはポータブル記憶デバイスまたは媒体を参照して、「取得された」という用語は、何かがシェアホルダ４４２に配布され、コンピューティングデバイス１０２に戻されたことを示すために使用される。例では、取得されたシークレットシェア４３６－２は、取得されたシークレットシェア４３６－２を格納するポータブル記憶デバイスまたは媒体が、改ざんされている（または、シェアホルダ４４２が誤って間違ったポータブル記憶デバイスまたは媒体に持ち込まれた）か否かに応じて、配布前に生成された元々のシークレットシェア４３６－１のうちの１つのシークレットシェアである場合も、そうでない場合もある。

【００４７】

[0054]単純化のために、単一のコンピューティングデバイス１０２が図４に示されているが、配布されるシークレットシェア４３６－１を生成するコンピューティングデバイス１０２は、シークレット４３４－２を再構成するコンピューティングデバイスと同じコンピューティングデバイス１０２であっても、そうでなくてもよい。言い換えると、生成部分４０３および再構成部分４０５は、同じまたは異なるコンピューティングデバイス１０

２にあってもよい。
【００４８】
[0055]任意選択で、コンピューティングデバイス１０２は、シークレット４３４－１が生成されて分割される前に、安全に消去／フォーマットすることができる。これは、記憶デバイス（たとえば、ハードディスクドライブ）を消去／フォーマットするための任意の適切な技法を使用することを含むことができる。例では、これは、コンピューティングデバイス１０２における記憶デバイス（たとえば、ハードディスクドライブ）のコンテンツを暗号化すること、およびオペレーティングシステムを（たとえば、クラウドベースのサーバから）復元することを含む。解読鍵は、暗号化プロセス中に生成または導出することができる。
【００４９】
[0056]シークレット４３４－１は、（たとえば、プールされた暗号通貨を保持する分散型台帳におけるアドレス３３２の）暗号秘密鍵３２６、パスワード、秘密鍵３２６を再構成するために使用できるニーモニックフレーズもしくはシード３２８、公開鍵３３０、アドレス３３２、シークレットフレーズ、アカウント番号、文字列として配置されたデジタル画像の生データ、文字列として配置されたデジタルビデオファイルの生データ、文字列として配置されたデジタルオーディオファイルの生データ、または、キャラクタの文字列として配置された他の任意のタイプのデジタルファイルのような、任意のキャラクタの文字列とすることができる。
【００５０】
[0057]例では、シークレット生成器２０８は、シークレット４３４－１を生成する。シークレット４３４－１が、秘密鍵３２６、または秘密鍵３２６を回復するためのニーモニック／シード３２８である例では、シークレット生成器２０８は、分散型台帳における、任意選択の公開鍵３３０、および／または、少なくとも１つの任意選択の（暗号通貨を保持する）アドレス３３２を生成する。シークレット４３４－１が、秘密鍵３２６である例では、シークレット生成器２０８は、疑似ランダム特性を有するシーケンスを生成することによって、秘密鍵３２６を生成する。少なくとも１つの任意選択のアドレス３３２が、シークレット４３４－１を用いて生成されると、（１）少額の暗号通貨をアドレス３３２に送金することと、（２）分散型台帳自体におけるアドレス３３２のためのトランザクションを表示することにより少額を検証することとによって、任意選択で検証してもよい。あるいは、シークレット４３４－１は、コンピューティングデバイス１０２において生成されるのではなく、コンピューティングデバイス１０２において（たとえば、ユーザ入力を介して、またはメモリから）識別および／または受信してもよい。たとえば、既存のアカウント番号、パスワード、または他のキャラクタの文字列は、コンピューティングデバイス１０２において生成されるのではなく、コンピューティングデバイス１０２に入力または送信してもよい。
【００５１】
[0058]例では、Ｓｈａｍｉｒシークレットシェアモジュール２１０は、シークレット４３４－１を、少なくとも２つのシークレットシェア４３６－１に分割する。例では、シークレット４３４－１は、Ｎ個のシークレットシェア４３６－１に分割され、ここでは、Ｎ個のシークレットシェア４３６－２のうちのＭ個が、シークレット４３４－２を再構成するために必要とされる。例では、シークレット４３４－１は、Ｓｈａｍｉｒシークレットシェアおよび／または多項式補間を使用して、シークレットシェア４３６－１に分割される。例では、分割のためＭ値およびＮ値を指定するために、Ｓｈａｍｉｒシークレットシェアモジュール２１０において、入力（たとえば、ユーザ入力）が受け取られる。一般に、限定することなく、１＜Ｍ≦Ｎである。
【００５２】
[0059]例では、ハッシュ機能２１２（たとえば、ＳＨＡ－５１２）は、各シークレットシェア４３６－１のシェアハッシュ４３７を生成する。各シークレットシェア４３６－１は、ＳＨＡ－５１２などの所与の最新のハッシュ機能２１２のために、正確に１つのハッ

シュ値を決定する。シェアハッシュ４３７は、メタデータモジュール２２４によって、メタデータ４４０の少なくとも１つのコピーに保存することができる（たとえば、Ｍ－ＤＩＳＣなどのアーカイブグレードの光学媒体に格納される）。シェアハッシュ４３７のリストに加えて、メタデータ４４０の各コピーは、（１）シークレット４３４－１を用いて生成された（およびそれに対応する）アドレス３３２のリスト、（２）特定のシークレット４３４－１／ウォレット番号への各シークレットシェア４３６－１の配布手段（たとえば、エビデンスバッグ識別子）のマッピング、（３）ハッシュ機能２１２コード（たとえば、シークレットシェア４３６－１をハッシュするために実行可能な命令のセット）のコピー、および／または、（４）シークレット４３４－１を分割するために使用されるコード（たとえば、Ｓｈａｍｉｒ分割を実行するために実行可能な命令のセット）のコピーをも含むことができる。例では、メタデータ４４０は、パスワードマネージャソフトウェアに格納されるか、保管用にＱＲコード（登録商標）として印刷されるか、光ディスクに転送される代わりに（またはそれに加えて）クラウドベースのストレージに電子的に送信される。

【００５３】

[0060]例では、シェアハッシュ４３７は、シークレット４３４－２が再構成される時間またはその近傍の時間で、取得されたシークレットシェア４３６－２の後の検証のために、メタデータ４４０に保存される。

【００５４】

[0061]任意選択で、シークレットシェア４３６－１は、配布前に検証モジュール２２２によって検証することができる。例では、すべてのシークレットシェア４３６－１を使用して、シークレット４３４－２を少なくとも１回再構成する。たとえば、シークレット４３４－２は、少なくともＮ／Ｍ（整数に切り上げ）回再構成する必要があり、たとえば、Ｍ＝３でＮ＝５の場合、シークレット４３４－２は、５／３（整数に切り上げ）＝２回なので、シークレット４３４－２の再構成中にすべてのシークレットシェア４３６－１が少なくとも１回使用される。

【００５５】

[0062]例では、シークレット４３４－１は、再構成されたシークレット４３４－２と比較される。シークレット４３４－１が、再構成されたシークレット４３４－２と一致する場合、（シークレット４３４－２を再構成するために使用される）シークレットシェア４３６－１が検証され、シェアホルダ４４２に配布される。シークレット４３４－１が、再構成されたシークレット４３４－２と一致しない場合、（シークレット４３４－２を再構成するために使用される）シークレットシェア４３６－１は検証されず、問題の原因が特定され、修正されるまで、シェアホルダ４４２に配布されない。

【００５６】

[0063]あるいは、シークレット４３４－１のハッシュを、再構成されたシークレット４３４－２のハッシュと比較することができる。シークレット４３４－１のハッシュが、再構成されたシークレット４３４－２のハッシュと一致する場合、（シークレット４３４－２を再構成するために使用される）シークレットシェア４３６－１が検証され、シェアホルダ４４２へ配布される。シークレット４３４－１のハッシュが、再構成されたシークレット４３４－２のハッシュと一致しない場合、（シークレット４３４－２を再構成するために使用される）シークレットシェア４３６－１は検証されず、問題の原因が特定され、修正されるまで、シェアホルダ４４２に配布されない。

【００５７】

[0064]任意選択で、シークレット４３４－１、シェアハッシュ４３６－１、および／または再構成されたシークレット４３４－２は、（すべてのシークレットシェア４３６－１を少なくとも１回使用してシークレット４３４－２を再構成することによって）シークレットシェア４３６－１が検証されると、コンピューティングデバイス１０２から削除される。

【００５８】

[0065]シークレット４３４－１がシークレットシェア４３６－１に分割され（そして、シークレットシェア４３６－１が任意選択で検証され）ると、各シークレットシェア４３６－１は、それぞれのシークレットシェア記憶デバイス、または媒体４３８－１から４３８－Ｎを転送してもよい。例では、シークレットシェア記憶デバイスまたは媒体４３８は、たとえばＭ－ＤＩＳＣのような、アーカイブグレードの光学媒体である。しかしながら、光学媒体の代わりに、または光学媒体に加えて、他のタイプのポータブル記憶デバイスまたは媒体を、使用してもよい。あるいは、シークレットシェア４３６－１は、物理的な印刷物（たとえば、バーコードまたはＱＲコード（登録商標））で配布され、少なくとも１つのネットワーク１０６を介して電子的に配布され、シェアホルダ４４２が自分の手書きなどでそれを書き写すことができるように電子的に表示される。任意選択で、シークレットシェア４３６－１は、シークレットシェア記憶デバイスまたは媒体４３８で転送される前に暗号化されてもよい。任意選択で、シークレットシェア４３６－１は、配布のためにポータブル記憶デバイスまたは媒体に転送された後、コンピューティングデバイス１０２から削除される。

【００５９】

[0066]任意選択で、コンピューティングデバイス１０２を、シークレットシェア４３６－１の配布後、再び安全に消去／フォーマットしてもよい。これは、記憶デバイス（たとえば、ハードディスクドライブ）を消去／フォーマットするための任意の適切な技法を使用することを含んでもよい。コンピューティングデバイス１０２の記憶デバイス（たとえば、ハードディスクドライブ）が、シークレット４３４－１の生成前に暗号化された例では、（記憶デバイスが暗号化されたときに生成または導出される）対応する解読鍵を、破棄、たとえば、安全に削除することができる。

【００６０】

[0067]シークレット４３４－２が再構成されるべきである場合、（シークレットシェア４３６－２を格納する）少なくともいくつかのシークレットシェア記憶デバイスまたは媒体４３８が、シェアホルダ４４２から取得される。取得されるシークレットシェア記憶デバイスまたは媒体４３８の数は、シークレット４３４－１の分割中に決定されたＭおよびＮの値に依存する。Ｍ＜Ｎの場合、取得されるシークレットシェア記憶デバイスまたは媒体４３８の数は、配布されたシークレットシェア４３６－１の数よりも少ない。Ｍ＝Ｎの場合、配布されるシークレットシェア記憶デバイスまたは媒体４３８のすべてが、シークレット４３４－２の再構成のために取得される。

【００６１】

[0068]シークレットシェア記憶デバイスまたは媒体４３８が（たとえば、シークレットシェア記憶デバイスまたは媒体４３８または物理的な印刷物で）物理的に配布された場合、少なくともサブセットは、一般的にコンピューティングデバイス１０２に物理的に戻される。この場合、シェアホルダ４４２の少なくともサブセットは、それぞれのシークレットシェア記憶デバイスまたは媒体４３８を、指定された日時に会議に物理的に持ち込むように求められる場合がある。シークレットシェア記憶デバイスまたは媒体４３８が物理的に取得されると、たとえば、シークレットシェア記憶デバイスまたは媒体４３８におけるシークレットシェア４３６－２を読み取ることや、印刷物におけるＱＲコード（登録商標）をスキャンすることなどによって、検証および／またはシークレットの再構成の前に処理される必要がある場合がある。

【００６２】

[0069]シークレットシェア４３６－１が（たとえば、少なくとも１つのネットワーク１０６を介して）電子的に配布されたとき、少なくともサブセットは、一般に、シェアホルダ４４２から（たとえば、少なくとも１つのネットワーク１０６を介して）電子的に取得される。これは、シェアホルダ４４２の少なくともサブセットのデバイスに送信される電子的な要求を含むことができ、その後、承認されて、シークレットシェアが、コンピューティングデバイス１０２へ送信される。いくつかの構成では、配布のためにシークレット４３４－１を生成および分割するコンピューティングデバイス１０２は、シークレット４

３４－２を再構成するコンピューティングデバイス１０２とは異なる場合がある。
【００６３】
[0070]シークレットシェア４３６－１は、配布前に暗号化された場合、検証される前、またはシークレット４３４－２が再構成される前に、取得後に解読される。シークレットシェア４３６－１は、配布前に対称的に暗号化される場合、取得後に対称的に解読される。シークレットシェア４３６－１は、配布前に非対称に暗号化される場合、取得後に非対称に解読される。シークレットシェア４３６－１は、シェアホルダ４４２への配布前に暗号化されない場合、シークレットシェア４３４－２の再構成前に解除される必要はない。
【００６４】
[0071]シークレット４３４－２を再構成する前に、取得されたシークレットシェア４３６－２は、任意選択で検証してもよい。例では、（シークレット４３４－２の再構成時またはその近傍で生成される）取得されたシークレットシェア４３６－２の少なくとも１つのハッシュが、（シークレットシェア４３６－１が配布される前に生成されたメタデータ４４０における）シェアハッシュ４３７のリストと比較される。取得されたシークレットシェア４３６－２のハッシュが、（メタデータ４４０における）シェアハッシュ４３７のリストにおけるハッシュと一致する場合、それは（シェアホルダ４４２－１に元々配布されていたシークレットシェア４３６－１と一致するので）、取得されたシークレットシェア４３６－２を使用して、所望されるシークレット４３４－２を再構成できることを意味する。取得されたシークレットシェア４３６－２のハッシュが、（メタデータ４４０における）シェアハッシュ４３７のリストにおけるどのハッシュとも一致しない場合、それは（シェアホルダ４４２に元々配布されていたシークレットシェア４３６－１のうちの１つのシークレットシェアではないので）、取得されたシークレットシェア４３６－２を使用して、所望されるシークレット４３４－２を再構成することはできないことを意味する。
【００６５】
[0072]シークレットシェア４３６－２が取得され（任意選択で検証され）ると、シークレット４３４－２を、シークレット再構成モジュール２２０において再構成することができる。いくつかの構成では、シークレット再構成モジュール２２０およびＳｈａｍｉｒシークレットシェアモジュール２１０は、ともに実施することができる。例では、シークレット再構成モジュール２２０、２２０は、Ｓｈａｍｉｒシークレットシェアモジュール２１０によって実行されるＳｈａｍｉｒ分割に対応するＳｈａｍｉｒ結合（シャミール結合）を使用する。
【００６６】
[0073]（シークレット４３４－２の再構成中にエラーが発生したか、または、再構成されたシークレット４３４－２が、元々のシークレット４３４－１と一致しないために）シークレット４３４－２が、シークレットシェア４３６－２から再構成できない場合、検証モジュール２２２は、メタデータ４４０に基づいて、少なくとも１つのシークレットシェア４３６－２を、正しくないと特定する場合がある。例では、これは、取得されたシークレットシェア４３６－２の少なくとも１つのハッシュを、メタデータ４４０におけるシェアハッシュ４３７のリストと比較することを含む。取得されたシークレットシェア４３６－２のハッシュが、（メタデータ４４０における）シェアハッシュ４３７のリストにおけるハッシュと一致する場合、それは（シェアホルダ４４２－１に元々配布されていたシークレットシェア４３６－１と一致するので）、取得された「正しい」シークレットシェア４３６－２である。取得されたシークレットシェア４３６－２のハッシュが、（メタデータ４４０における）シェアハッシュ４３７のリストにおけるどのハッシュとも一致しない場合、それは（シェアホルダ４４２に元々配布されていたシークレットシェア４３６－１のうちの１つのシークレットシェアではないので）、取得された「正しくない」シークレットシェア４３６－２として特定される。この再構成後の検証／特定により、問題を、特定のシェアホルダ４４２のシークレットシェア記憶デバイスまたは媒体４３８に絞り込むことができる。
【００６７】

[0074]図５は、シークレット４３４－１を分割し、メタデータ４４０を格納するための例示的な方法５００を示すフロー図である。方法５００は、シークレット分割およびメタデータ記憶のためのシステム１００におけるコンピューティングデバイス１０２によって実行することができる。例では、方法５００におけるステップの少なくともいくつかは、コンピューティングデバイス１０２における少なくとも１つのプロセッサによって実施される。

【００６８】

[0075]方法５００は、少なくとも１つのプロセッサが、コンピューティングデバイス１０２における少なくとも１つの記憶デバイス（たとえば、ハードディスクドライブ）の内容を消去する、任意選択のステップ５０２で始まる。例では、これは、少なくとも１つの記憶デバイスの内容を暗号化し、オペレーティングシステムを（たとえば、クラウドベースのサーバから）復元することを含む。記憶デバイスの内容を解読できる解読鍵を、生成または導出することができる。あるいは、記憶デバイスの内容を消去するための任意の適切な技法を使用することができる。

【００６９】

[0076]方法５００は、ステップ５０４に進み、ここでは、少なくとも１つのプロセッサは、保護されるべきシークレット４３４－１を決定する。例では、シークレット４３４－１は、たとえば、秘密鍵３２６を再構成するために使用できる暗号秘密鍵３２６またはニーモニックフレーズもしくはシード３２８などの、任意のキャラクタの文字列である。シークレット４３４－１が、秘密鍵３２６またはニーモニック／シード３２８である例では、決定することは、少なくとも１つのプロセッサがシークレット４３４－１を生成することを含むことができる。代替的または追加的に、決定することは、少なくとも１つのプロセッサが、既存のシークレット４３４－１を生成するのではなく、それを特定および／または受け取ることを含むことができる。

【００７０】

[0077]シークレット４３４－１が、秘密鍵３２６、または秘密鍵３２６を回復するためのニーモニック／シード３２８である場合、少なくとも１つのプロセッサは、任意選択の公開鍵３３０、および／または、分散型台帳における（暗号通貨を保持する）少なくとも１つのアドレス３３２を生成することができる。少なくとも１つの任意選択のアドレス３３２が、シークレット４３４－１を用いて生成されると、（１）少額の暗号通貨をアドレス３３２に送金することと、（２）分散型台帳自体におけるアドレス３３２のためのトランザクションを表示することにより少額を検証することとによって、任意選択で検証することができる。これは、アドレスが、所望される分散型台帳における有効なアドレスであることを確認するのに役立つ。

【００７１】

[0078]方法５００はステップ５０６に進み、ここでは、少なくとも１つのプロセッサは、シークレット４３４－１を、複数のシークレットシェア４３６－１に分割し、複数のシークレットシェア４３６－１の少なくともサブセットは、シークレット４３４－２を再構成するために必要とされる。シークレット４３４－１は、Ｓｈａｍｉｒシークレットシェアおよび／または多項式補間を使用して分割される場合がある。例では、コンピューティングデバイス１０２のユーザは、（１）シークレット４３４－１をいくつのシークレットシェア４３６－１に分割すべきか、および／または、（２）シークレット４３４－１を再構成するためにいくつのシークレットシェア４３６－１が必要とされるかを指定するユーザ入力を提供するように促される。例では、ユーザは、Ｎ（たとえば、Ｎ＝１～１００）およびＭ（たとえば、Ｍ＜＝Ｎ）に対して任意の数を選択してもよい。例では、ユーザは、シークレット４３４－１のセキュリティ、シークレット４３４－１のアクセス可能性、および／または他の任意の懸念事項に基づいて、ＭおよびＮの構成を調整することができる。

【００７２】

[0079]方法５００は、任意選択のステップ５０８に進み、ここでは、少なくとも１つの

プロセッサは、各シークレットシェア４３６－１を、少なくとも１回使用してシークレット４３４－１を再構成することによって、シークレットシェア４３６－１を検証する。たとえば、シークレット４３４－２は、少なくともＮ／Ｍ（整数に切り上げ）回再構成する必要があり、たとえば、Ｍ＝３およびＮ＝５である場合、シークレット４３４－２は、５／３（整数に切り上げ）＝２回なので、シークレットの再構成中にすべてのシークレットシェア４３６－１が少なくとも１回使用される。シークレットシェア４３６－１は、（１）シークレット４３４－１を、再構成されたシークレット４３４－２と比較すること（ここでは、シークレット４３４－１が、再構成されたシークレット４３４－２と一致する場合にのみ、シークレットシェア４３６－１が検証される）、または、（２）シークレット４３４－１のハッシュを、再構成されたシークレット４３４－２のハッシュと比較すること（ここでは、シークレット４３４－１のハッシュが、再構成されたシークレットのハッシュ４３４－２と一致する場合にのみ、シークレットシェア４３６－１が検証される）によって検証できる。例では、たとえば、（１）シークレット４３４－１が、再構成されたシークレット４３４－２と一致しない場合、または、（２）シークレット４３４－１のハッシュが、再構成されたシークレット４３４－２のハッシュと一致しない場合のように、任意選択のステップ５０８において、シークレットシェア４３６－１のすべてが検証される訳ではない場合、方法５００は、終了するか、または、以前のステップのいずれかに戻る。

【００７３】

[0080]方法５００は、ステップ５１０に進み、ここでは、少なくとも１つのプロセッサは、それぞれのシェアホルダ４４２への配布のために、各シークレットシェア４３６－１を、それぞれのポータブル記憶デバイスまたは媒体に転送する。例では、シークレットシェア４３６－１は、たとえばＭ－ＤＩＳＣのようなアーカイブグレードの光学媒体に転送される。しかしながら、光学媒体の代わりに、または光学媒体に加えて、他のタイプのポータブル記憶デバイスまたは媒体が、使用される場合がある。任意選択で、シークレットシェア４３６－１は、ポータブル記憶デバイスまたは媒体に転送される前に暗号化してもよい。

【００７４】

[0081]配布は、各ポータブル記憶デバイスまたは媒体を、改ざん防止および／または不正開封防止されたセキュリティエンベロープまたはパッケージに物理的に配置することであって、各セキュリティエンベロープは、一意の識別子を有する、配置することと、その後、異なるセキュリティエンベロープまたはパッケージを、各シェアホルダ４４２へ転送することとを含むことができる。

【００７５】

[0082]方法５００は、ステップ５１２に進み、ここでは、少なくとも１つのプロセッサが、各シークレットシェア４３６－１の少なくともハッシュ４３７を用いて、メタデータ４４０を生成する。各シェアハッシュ４３７は、キャラクタの文字列であってもよく、その長さは、たとえば、ＳＨＡ－５１２を使用して生成されるシェアハッシュ４３７が、５１２ビット長となるように、シェアハッシュ４３７を生成するために使用されるハッシュ機能２１２によって決定される。各シークレットシェア４３６－１は、ＳＨＡ－５１２などの、所与の最新のハッシュ機能２１２が使用される場合、１つのハッシュ値を決定する場合がある（しかしながら、ＳＨＡ－１関数の一部などの古いハッシュ機能ではハッシュ衝突する可能性がある）。

【００７６】

[0083]シェアハッシュ４３７のリスト（ステップ５１０）に加えて、メタデータ４４０の各コピーはまた、（１）シークレット４３４－１を用いて生成された（および、シークレット４３４－１に対応する）アドレス３３２のリストと、（２）（シークレットシェア４３６－１を、特定のシークレット４３４－１／ウォレット番号に配布するために使用される各セキュリティエンベロープまたはパッケージの識別子のマッピングと、（３）メタデータ４４０におけるシェアハッシュ４３７を生成するために使用されるハッシュ機能２

１２コードのコピー（任意選択のステップ５０８）と、および／または（４）シークレット４３４－１をシークレットシェア４３６－１に分割するために使用されるコードのコピー（ステップ５０６）とを含むことができる。

【００７７】

[0084]方法５００は、任意選択のステップ５１４に進み、ここでは、少なくとも１つのプロセッサは、ローカルに格納されたシークレット４３４－１、シークレットシェア４３６－１、および任意選択のシェアハッシュ４３７（および、任意選択のステップ５０８で生成された任意の再構成されたシークレット４３４－２）のコピーを削除する。任意選択のステップ５１８は、コンピューティングデバイス１０２における少なくとも１つの記憶デバイス（たとえば、ハードディスクドライブ）全体の内容を（たとえば、任意選択の５０２で作成された解読鍵を安全に削除することによって）再び消去することをさらに含むことができる。

【００７８】

[0085]方法５００は任意選択のステップ５１６に進み、ここでは、少なくとも１つのプロセッサは、シークレットシェア４３６－１を用いて、メタデータ４４０を、ポータブル記憶デバイスまたは媒体とは別に格納する。メタデータ４４０の各コピーは、（１）ポータブル記憶デバイスまたは媒体（たとえば、Ｍ－ＤＩＳＣなどのアーカイブグレードの光学媒体）に格納することができる、（２）（たとえば、適切な資格情報を有する人々へのアクセスを制限する）電子レポジトリに格納することができる、および／または（３）保管のためにＱＲコード（登録商標）として印刷することができる。あるいは、メタデータ４４０のために、任意の他の適切な記憶方法が使用できる。例では、（任意選択のステップ５１６において）メタデータ４４０を書き込む前に、（任意選択のステップ５１４において）ローカルに格納されたシークレット４３４－１およびシークレットシェア４３６－１のコピーを削除すると、シークレット４３４－１およびシークレットシェア４３６－１が、メタデータ４４０媒体に書き込まれることを防止する。

【００７９】

[0086]例では、方法５００は、たとえシェアハッシュ４３７が表示されても、シークレット４３４－１またはシークレット部分４３６－１さえもユーザに表示することなく実行される。追加のセキュリティのために、いくつかの構成では、方法５００は、プロセス５００を実行するユーザに加えて、少なくとも１人（たとえば２人）の証人とともに実行され、シークレット４３４－１およびシークレットシェア４３６－１が、無許可で配布されないことを保証する。

【００８０】

[0087]図６は、少なくとも２つの取得されたシークレットシェア４３６－２からシークレット４３４－２を再構成するための例示的な方法６００を示すフロー図である。方法６００は、コンピューティングデバイス１０２によって実行することができる。例では、図６における方法６００は、図５における方法５００へ順次実行され、この場合、図６における方法６００を実施するコンピューティングデバイス１０２は、図５における方法５００を実施するコンピューティングデバイス１０２と同じであっても、同じでなくてもよい。例では、方法６００におけるステップの少なくともいくつかは、コンピューティングデバイス１０２における少なくとも１つのプロセッサによって実施される。

【００８１】

[0088]方法６００は、任意選択のステップ６０２で始まり、ここでは、複数のシークレットシェア記憶デバイスまたは媒体４３８のうちの少なくとも２つは、コンピューティングデバイス１０２へ取得され、各シークレットシェア記憶デバイスまたは媒体４３８は、シークレット４３４－１の、少なくとも１つの取得されたシークレットシェア４３６－２を記憶する。取得されるシークレットシェア記憶デバイスまたは媒体４３８の数は、シークレット４３４－１分割中に決定されたＭおよびＮの値に依存する。Ｍ＜Ｎの場合、取得されるシークレットシェア記憶デバイスまたは媒体４３８の数は、配布されたシークレットシェア４３６－１の数よりも少ない。Ｍ＝Ｎの場合、配布されたシークレットシェア記

憶デバイスまたは媒体４３８のすべてが、シークレット４３４－２の再構成のために取得される。例では、シークレットシェア記憶デバイスまたは媒体４３８の少なくともサブセットが、物理的にコンピューティングデバイス１０２に持ち込まれる。例では、シェアホルダ４４２の少なくともサブセットは、それぞれのシークレットシェア記憶デバイスまたは媒体４３８を、指定された日時に会議に持ち込むように求められる場合がある。

【００８２】

[0089]方法６００は、ステップ６０４に進み、ここでは、シークレットシェア４３６－１は、シークレットシェア記憶デバイスまたは媒体４３８から決定され、たとえば、取得されたシークレットシェア４３６－２が、シークレットシェア記憶デバイスまたは媒体４３８から読み取られ、任意選択で、コンピューティングデバイス１０２に格納される。記憶デバイス（たとえば、ＵＳＢドライブ）が使用される場合、たとえばＵＳＢポートなどを介してコンピューティングデバイスに接続することができる。光学媒体（たとえば、Ｍ－ＤＩＳＣ）が使用される場合、取得されたシークレットシェア４３６－２を読み取り、任意選択で、それらをコンピューティングデバイス１０２に格納するために、光学媒体をディスクドライブに配置することができる。

【００８３】

[0090]シークレットシェア４３６－１が、配布前に暗号化された場合、ステップ６０４は、シークレットシェア４３６－１を解読することを含むことができる。シークレットシェア４３６－１が配布前に（対称鍵を使用して）対称的に暗号化されると、取得後に（同じ対称鍵を使用して）対称的に解読される。シークレットシェア４３６－１が、配布前に（公開鍵を使用して）非対称に暗号化されている場合、取得後に（公開鍵に対応する秘密鍵を使用して）非対称に解読される。シークレットシェア４３６－１が、シェアホルダ４４２への配布前に暗号化されていない場合、ステップ６０４において解読される必要はない。

【００８４】

[0091]方法６００はステップ６０６に進み、ここでは、少なくとも１つのプロセッサは、（シークレット４３４－１のための）メタデータ４４０を決定し、メタデータ４４０は、シークレットシェア４３６－１がシェアホルダ４４２に配布される前に生成された、シークレットシェア４３６－１の少なくともハッシュ４３７のリストを有する。例では、メタデータ４４０は、（１）シークレット４３４－１を用いて生成された（および、シークレット４３４－１に対応する）アドレス３３２のリストと、（２）（シークレットシェア４３６－１を、特定のシークレット４３４－１／ウォレット番号に配布するために使用される各セキュリティエンベロープまたはパッケージの識別子のマッピングと、（３）メタデータ４４０におけるシェアハッシュ４３７を生成するために使用されるハッシュ機能２１２コードのコピーと、および／または、（４）配布前に、シークレット４３４－１をシークレットシェア４３６－１に分割するために使用されるコードのコピーをも含む。

【００８５】

[0092]方法６００は、任意選択のステップ６０８に進み、ここでは、少なくとも１つのプロセッサは、取得されたシークレットシェア４３６－２を検証する。例では、取得されたシークレットシェア４３６－２のうちの少なくとも１つのシークレットシェアのハッシュが、メタデータ４４０におけるシェアハッシュ４３７のリストと比較される。取得されたシークレットシェア４３６－２のハッシュが、（メタデータ４４０における）シェアハッシュ４３７のリストにおけるハッシュと一致する場合、それは（シェアホルダ４４２－１に元々配布されていたシークレットシェア４３６－１と一致するので）、取得されたシークレットシェア４３６－２を使用して、所望されるシークレット４３４－２を再構成できることを意味する。取得されたシークレットシェア４３６－２のハッシュが、（メタデータ４４０における）シェアハッシュ４３７のリストにおけるどのハッシュとも一致しない場合、それは（シェアホルダ４４２に元々配布されていたシークレットシェア４３６－１のうちの１つのシークレットシェアではないので）、取得されたシークレットシェア４３６－２を使用して、所望されるシークレット４３４－２を再構成できないことを意味す

る。例では、方法６００の後続のステップは、取得されたすべてのシークレットシェア４３６－２が、任意選択のステップ６０８で検証された場合にのみ実行される。

【００８６】

[0093]方法６００は、ステップ６１０に進み、ここでは、少なくとも１つのプロセッサは、取得されたシークレットシェア４３６－２を使用して、シークレット４３４－２を再構成しようと試みる。例では、ステップ６１０は、シークレットシェア４３６－１の配布前に実行されるＳｈａｍｉｒシークレットシェア（シークレット４３４－１の分割）であったものに対応するＳｈａｍｉｒ結合を使用する。

【００８７】

[0094]方法６００は、任意選択のステップ６１２に進み、ここでは、取得されたシークレットシェア４３６－２からシークレット４３４－２を再構成できない場合、少なくとも１つのプロセッサは、メタデータ４４０に基づいて、少なくとも１つのシークレットシェア４３６－２を、正しくないと特定する。たとえば、任意選択のステップ６１２は、（１）シークレット４３４－２の再構成中にエラーが発生することに応じて、または、（２）シークレット４３４－２がステップ６１０において再構成され、分割および配布された元々のシークレット４３４－１と一致しない場合、実行することができる。このシナリオ（再構成されたシークレット４３４－２が元々のシークレット４３４－１と一致しない場合）は、（１）シークレットと、再構成されたシークレット４３４－１とのハッシュを比較すること、（２）再構成されたシークレット４３４－２に関連付けられたアドレスのアカウント残高が正しいか否かを判定すること（しかしながら、そのアドレスがトランザクションを受け取っていない場合、アドレスに残高がない、および／またはブロックチェーンエクスプローラに表示されない可能性がある）、または（３）（メタデータ４４０における）アドレスを、再構成されたシークレット４３４－２から導出されるアドレスと比較することによって判定できる。

【００８８】

[0095]任意選択のステップ６１２は、任意選択のステップ６０８と同様に実行することができ、たとえば、取得されたシークレットシェア４３６－２のうちの少なくとも１つのシークレットシェアのハッシュが、メタデータ４４０におけるシェアハッシュ４３７のリストと比較される。取得されたシークレットシェア４３６－２のハッシュが、（メタデータ４４０における）シェアハッシュ４３７のリストにおけるハッシュと一致する場合、それは（シェアホルダ４４２－１に元々配布されていたシークレットシェア４３６－１と一致するので）、取得された「正しい」シークレットシェア４３６－２である。取得されたシークレットシェア４３６－２のハッシュが、（メタデータ４４０における）シェアハッシュ４３７のリストにおけるどのハッシュにも一致しない場合、それは（シェアホルダ４４２に元々配布されていたシークレットシェア４３６－１のうちの１つのシークレットシェアではないので）、取得された「正しくない」シークレットシェア４３６－２として特定される。

【００８９】

[0096]したがって、シェアホルダ４４２のうちの１つのシェアホルダが（意図的または非意図的に）間違ったシークレットシェア記憶デバイスまたは媒体４３８を持ち込んだ場合、方法６００は、問題を、（取得された正しくないシークレットシェア４３６－２を保持する）特定のシェアホルダ４４２のシークレットシェア記憶デバイスまたは媒体４３８に絞り込むのに役立つことができる。問題の原因を特定のシェアホルダ４４２に絞り込むことにより、問題を適切に対処することができる。

【００９０】

[0097]シークレットシェア記憶デバイスまたは媒体４３８が、改ざん防止および／または不正開封防止セキュリティエンベロープまたはパッケージで配布される例では、セキュリティエンベロープまたはパッケージは、特定のシークレット４３４－１の再構成のために、シェアホルダ４４２が、所有している複数のセキュリティエンベロープまたはパッケージのどれを持ち込む必要があるのかを容易に特定できるように、シークレット４３４－

１識別子（たとえば、「ウォレット１」）をリスト化することができる。
【００９１】
[0098]それに加えて、メタデータ４４０をシークレットシェア記憶デバイスまたは媒体４３８から分離することによって、メタデータ４４０またはシークレットシェア記憶デバイスまたは媒体４３８の不正な所有者は、シークレット４３４－２を再構成するために、残りのシークレットシェア記憶デバイスまたは媒体４３８を盗むのに十分な情報を有してない可能性が高い。実際、シークレットシェア記憶デバイスまたは媒体４３８のうちの１つの不正な所有者は、シークレットシェア４３６－１によってどのタイプのデータが表されているか、またはそれに価値があるか否か、またはどの程度の価値があるかを知らない可能性がある。しかしながら、メタデータ４４０は、シークレットシェア記憶デバイスまたは媒体４３８がなくても、依然として有用である可能性があり、たとえば、誰かが、メタデータ４４０においてリストされたアドレスに関連付けられたトランザクションを監視する、および／または、メタデータ４４０におけるアドレスに暗号通貨を送金することを可能にする。
【００９２】
[0099]さらに、どの個人がシェアホルダ４４２であるかのマッピングは、メタデータ４４０またはシークレットシェア記憶デバイスまたは媒体４３８から容易に入手できない場合がある。そのようなマッピング自体が、シェアホルダ４４２の安全を脅かす可能性がある。このマッピングをメタデータ４４０に含めないことにより、どの個人がシェアホルダ４４２であるかを把握することがより困難になる。しかしながら、いくつかの構成では、非常に少数の人々がアクセスできる、（セキュリティエンベロープまたはパッケージ番号への個人の）別のマッピングが存在する場合がある。
【００９３】
[0100]方法６００は、任意選択のステップ６１４に進み、ここでは、シークレット４３４－２は、取得されたシークレットのシェア４３６－２から再構成されると、少なくとも１つのプロセッサが、再構成されたシークレット４３４－２を要求するアクションを実行する。このアクションの例は、（１）再構成されたシークレット４３４－２を使用してデータを暗号化または解読すること、（２）再構成されたシークレット４３４－２に基づいて、分散型台帳におけるトランザクションアドレスを生成すること、および／または、（３）再構成されたシークレット４３４－２を使用して、暗号通貨をアドレスから送金するトランザクションに署名することを含むことができる。
【００９４】
[0101]例では、方法６００は、再構成されたシークレット４３４－１または再構成されたシークレット部分４３６－１さえも、ユーザに表示することなく実行される。追加のセキュリティのために、いくつかの構成では、方法６００は、プロセス６００を実行するユーザに加えて、少なくとも１人（たとえば、２人）の証人とともに実行され、シークレット４３４－１およびシークレットシェア４３６－１が、無許可で配布されないことを保証する。
【００９５】
[0102]本明細書で紹介される技法は、専用ハードウェア（回路構成など）として、ソフトウェアおよび／またはファームウェアで適切にプログラムされたプログラマブル回路構成として、または専用およびプログラマブル回路構成の組合せとして具現化することができる。したがって、実施形態は、プロセスを実行するようにコンピュータ（または他の電子デバイス）をプログラムするために使用できる命令を格納した機械可読媒体を含むことができる。機械可読媒体は、たとえば、フロッピーディスク、光ディスク、コンパクトディスク読取専用メモリ（ＣＤ－ＲＯＭ）、光磁気ディスク、読取専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、消去可能プログラマブル読取専用メモリ（ＥＰＲＯＭ）、電気的消去可能なプログラマブル読取専用メモリ（ＥＥＰＲＯＭ）、磁気カードまたは光学カード、フラッシュメモリ、または電子命令の格納に適した他のタイプの媒体／機械可読媒体を含むことができる。

【００９６】
[0103]コンピュータシステムの概要
[0104]本開示の実施形態は、上記の様々なステップおよび動作を含む。これらの様々なステップおよび動作は、ハードウェア構成要素によって実行できるか、または命令でプログラムされた汎用または専用プロセッサに、ステップを実行させるために使用される機械実行可能命令で具現化できる。あるいは、ステップは、ハードウェア、ソフトウェア、および／またはファームウェアの組合せによって実行することができる。したがって、図７は、本開示の実施形態を利用できるコンピュータシステム７００の例である。本例によれば、コンピュータシステム７００は、相互接続７０２、少なくとも１つのプロセッサ７０４、少なくとも１つの通信ポート７０６、少なくとも１つのメインメモリ７０８、少なくとも１つのリムーバブル記憶媒体７１０、少なくとも１つの読取専用メモリ７１２、および少なくとも１つの大容量記憶デバイス７１４を含む。
【００９７】
[0105]少なくとも１つのプロセッサ７０４は、任意の知られているプロセッサとすることができる。少なくとも１つの通信ポート７０６は、たとえば、モデムベースのダイアルアップ接続で使用するＲＳ－２３２ポート、１０／１００イーサネットポート、または銅またはファイバを使用するギガビットポートのいずれかであるか、またはそれらを含むことができる。少なくとも１つの通信ポート７０６の性質は、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、またはコンピュータシステム７００が接続する任意のネットワークなどのネットワークに応じて選択することができる。少なくとも１つのメインメモリ７０８は、ランダムアクセスメモリ（ＲＡＭ）、または当該技術分野で一般に知られている他の任意の動的記憶デバイスとすることができる。少なくとも１つの読取専用メモリ７１２は、少なくとも１つのプロセッサ７０４のための命令などの静的情報を記憶するためのプログラマブル読取専用メモリ（ＰＲＯＭ）チップなどの任意の静的記憶デバイスとすることができる。
【００９８】
[0106]少なくとも１つの大容量記憶デバイス７１４を使用して、情報および命令を格納することができる。たとえば、（シリアル／パラレルＡＴＡまたはＳＣＳＩインターフェースを使用する磁気ディスクドライブまたはソリッドステートドライブなどの）ハードディスク、光ディスク、リダンダント・アレイ・オブ・インディペンデント・ディスク（ＲＡＩＤ）などのディスクのアレイ、または他の大容量記憶デバイスを使用することができる。相互接続７０２は、１つまたは複数のバス、ブリッジ、コントローラ、アダプタ、および／またはポイントツーポイント接続であるか、それらを含むことができる。相互接続７０２は、少なくとも１つのプロセッサ７０４を、他のメモリ、ストレージ、および通信ブロックと通信可能に結合する。相互接続７０２は、使用される記憶デバイスに応じて、ＰＣＩ／ＰＣＩ－ＸまたはＳＣＳＩベースのシステムバスとできる。少なくとも１つのリムーバブル記憶媒体７１０は、任意の種類の外付けハードドライブ、フロッピードライブ、コンパクトディスク読取専用メモリ（ＣＤ－ＲＯＭ）、コンパクトディスク再書込可能（ＣＤ－ＲＷ）、デジタルビデオディスク読取専用メモリ（ＤＶＤ－ＲＯＭ）、Ｂｌｕ－Ｒａｙディスク読取専用メモリ（ＢＤ－ＲＯＭ）、Ｂｌｕ－Ｒａｙディスク記録可能（ＢＤ－Ｒ）、Ｂｌｕ－Ｒａｙディスク記録可能消去可能（ＢＤ－ＲＥ）、ＭＩＬＬＥＮＮＩＡＬ　ＤＩＳＣ（Ｍ－ＤＩＳＣ）などとすることができる。
【００９９】
[0107]上記の構成要素は、いくつかのタイプの可能性を例示することを意図している。前述の例は、例示的な実施形態にすぎないため、決して本開示を限定すべきではない。下記および上記のものを含む、本明細書で説明される実施形態、構造、方法などは、様々な手法でともに組み合わせることができる。
【０１００】
[0108]用語
[0109]本出願を通して使用される用語、略語、およびフレーズの簡単な定義を以下に示

す。

【０１０１】

[0110]「接続された」、「結合された」、および「通信可能に結合された」という用語および関連する用語は、動作上の意味で使用され、直接的な物理的接続または結合に必ずしも限定されない。したがって、たとえば、２つのデバイスを直接結合するか、または、１つまたは複数の中間媒体またはデバイスを介して結合することができる。別の例として、物理的な接続を互いにシェアせずにデバイス間で情報を渡すことができるようにデバイスを結合することができる。本明細書で提供される開示に基づいて、当業者は、前述の定義に従って接続または結合が存在する様々な手法を認識するであろう。

【０１０２】

[0111]「～に基づく」というフレーズは、別段の明示的な指定がない限り、「～のみに基づく」を意味しない。言い換えれば、「～に基づく」というフレーズは、「～のみに基づく」と「少なくとも～に基づく」との両方を表す。それに加えて、「および／または」という用語は、「および」または「または」を意味する。たとえば、「Ａおよび／またはＢ」は、「Ａ」、「Ｂ」、または「ＡおよびＢ」を意味することができる。それに加えて、「Ａ、Ｂ、および／またはＣ」は、「Ａのみ」、「Ｂのみ」、「Ｃのみ」、「ＡおよびＢ」、「ＡおよびＣ」、「ＢおよびＣ」、または「Ａ、Ｂ、およびＣ」を意味することができる。

【０１０３】

[0112]「例示的な実施形態において」、「実例である実施形態において」、「いくつかの実施形態において」、「いくつかの実施形態に従って」、「示された実施形態において」、「他の実施形態において」、「実施形態」、「例において」、「例」、「いくつかの例において」、「いくつかの例」などのフレーズは、一般に、フレーズに続く特定の特徴、構成、または特性が、本開示の少なくとも１つの実施形態に含まれ、本開示の１つの実施形態よりも多くの実施形態に含む場合があることを意味する。それに加えて、そのようなフレーズは、必ずしも同じ実施形態または異なる実施形態を称する訳ではない。

【０１０４】

[0113]明細書が、構成要素または機能を、含む「場合がある」、含む「ことができる」、含む「ことができた」、または含む「可能性がある」、または、構成要素または機能が、特性を有する「場合がある」、有する「ことができる」、有する「ことができた」、または有する「可能性がある」と述べている場合、その特定の構成要素または機能は、含まれる必要も、その特性を有する必要もない。

【０１０５】

[0114]「反応する」という用語は、完全にまたは部分的に反応することを含む。

[0115]「モジュール」という用語は、ソフトウェア、ハードウェア、またはファームウェア（またはそれらの任意の組合せ）の構成要素を広く称する。モジュールは通常、指定された入力を使用して、有用なデータまたは他の出力を生成できる機能的な構成要素である。モジュールは、自己完結型の場合と、そうではない場合とがある。（「アプリケーション」とも呼ばれる）アプリケーションプログラムは、１つまたは複数のモジュールを含む場合があるか、または、モジュールは、１つまたは複数のアプリケーションプログラムを含むことができる。

【０１０６】

[0116]「ネットワーク」という用語は、一般に、情報を交換できる相互接続されたデバイスのグループを称する。ネットワークは、ローカルエリアネットワーク（ＬＡＮ）上の数台のパーソナルコンピュータの場合もあれば、世界規模のコンピュータネットワークであるインターネットのように大規模な場合もある。本明細書で使用される「ネットワーク」は、あるエンティティから別のエンティティに情報を送信できる任意のネットワークを包含することを意図される。場合によっては、ネットワークは、複数のネットワークから、あるいは、様々なネットワーク間での通信を容易にするために動作可能なゲートウェイを介して相互接続された、１つまたは複数の境界ネットワーク、音声ネットワーク、ブロ

ードバンドネットワーク、金融ネットワーク、サービスプロバイダネットワーク、インターネットサービスプロバイダ（ＩＳＰ）ネットワーク、および／または、公衆交換電話網（ＰＳＴＮ）のような複数の異種ネットワークからさえ構成されている場合もある。

【０１０７】

[0117]また、例示のために、本開示の様々な実施形態を、現代のコンピュータネットワーク内のコンピュータプログラム、物理的構成要素、および論理的相互作用の文脈で説明してきた。重要なことに、これらの実施形態は、最新のコンピュータネットワークおよびプログラムに関連して本開示の様々な実施形態を説明しているが、本明細書で説明されている方法および装置は、当業者が理解するように、他のシステム、デバイス、およびネットワークに等しく適用可能である。したがって、本開示の実施形態の例示された用途は、限定ではなく、例であることが意図される。本開示の実施形態が適用可能な他のシステム、デバイス、およびネットワークには、たとえば、他のタイプの通信およびコンピュータデバイスおよびシステムを含む。より具体的には、実施形態は、セル電話ネットワークおよび互換デバイスなどの通信システム、サービス、およびデバイスに適用可能である。それに加えて、実施形態は、パーソナルコンピュータから大規模なネットワークメインフレームおよびサーバまで、すべてのレベルのコンピューティングに適用可能である。

【０１０８】

[0118]結論として、本開示は、シークレット分割およびメタデータ記憶のための斬新なシステム、方法、および構成を提供する。本開示の１つまたは複数の実施形態の詳細な説明が上記で与えられたが、様々な代替、修正、および均等物が、本開示の精神から変化することなく、当業者に明らかであろう。たとえば、上記の実施形態は、特定の特徴に言及しているが、本開示の範囲は、特徴の異なる組合せを有する実施形態、および説明した特徴のすべてを含む訳ではない実施形態も含む。したがって、本開示の範囲は、特許請求の範囲に含まれるすべての代替、修正、および変形、ならびにそのすべての均等物を包含することを意図される。したがって、上記の説明は限定的なものと解釈されるべきではない。

例

[0119]例１は、少なくとも１つのプロセッサと、少なくとも１つのプロセッサに通信可能に結合された少なくとも１つのメモリとを備え、少なくとも１つのプロセッサは、保護されるべきシークレットを決定し、シークレットを、複数のシークレットシェアに分割し、複数のシークレットシェアの少なくともサブセットは、シークレットを再構成するために必要とされ、各シークレットシェアを、それぞれのシェアホルダに配布するために、それぞれのポータブル記憶デバイスまたは媒体に転送し、少なくとも各シークレットシェアのハッシュを用いてメタデータを生成し、シークレットシェアを用いて、メタデータを、ポータブル記憶デバイスまたは媒体とは別に格納するように構成された、コンピューティングデバイスを含む。

【０１０９】

[0120]例２は、例１のコンピューティングデバイスを含み、シークレットと、シークレットシェアと、シークレットシェアのハッシュとの各々は、異なるキャラクタの文字列である。

【０１１０】

[0121]例３は、例１～例２のいずれかのコンピューティングデバイスを含み、シークレットは、秘密鍵を再構成するために使用できる暗号秘密鍵またはニーモニックフレーズもしくはシードである。

【０１１１】

[0122]例４は、例１～例３のいずれかのコンピューティングデバイスを含み、少なくとも１つのプロセッサは、Ｓｈａｍｉｒシークレットシェアまたは多項式補間を使用して、シークレットを、複数のシークレットシェアに分割するように構成される。

【０１１２】

[0123]例５は、例１～例４のいずれかのコンピューティングデバイスを含み、少なくとも１つのプロセッサは、シークレットを再構成するために各シークレットシェアを少なく

とも１回使用することによって、シークレットシェアを検証するように構成され、シークレットシェアは、シークレットシェアが正常に検証された後、それぞれのポータブル記憶デバイスまたは媒体に単に転送される。

【０１１３】

[0124]例６は、例１～例５のいずれかのコンピューティングデバイスを含み、少なくとも１つのプロセッサは、シークレットを決定する前に、コンピューティングデバイスにおいて、少なくとも１つの記憶デバイスの内容を消去し、オペレーティングシステムのクリーンインストールを実行し、各シークレットシェアをそれぞれのポータブル記憶デバイスまたは媒体に転送した後、コンピューティングデバイスにローカルに格納されたシークレットおよびシークレットシェアのコピーを削除するように構成される。

【０１１４】

[0125]例７は、例１～例６のいずれかのコンピューティングデバイスを含み、シークレットは、暗号秘密鍵であるか、または暗号秘密鍵を回復するために使用できるニーモニックフレーズもしくはシードであり、少なくとも１つのプロセッサは、暗号秘密鍵またはニーモニックフレーズもしくはシードを生成することにより、シークレットを決定するように構成される。

【０１１５】

[0126]例８は、例７のコンピューティングデバイスを含み、少なくとも１つのプロセッサはまた、メタデータにおいて、以下の情報、すなわち、暗号秘密鍵に対応する公開鍵と、分散型台帳における少なくとも１つのアドレスとを生成する。

【０１１６】

[0127]例９は、例１～例８のいずれかのコンピューティングデバイスを含み、少なくとも１つのプロセッサは、シェアホルダから取得された少なくとも２つのシークレットシェア記憶デバイスまたは媒体から、取得されるシークレットシェアを決定し、少なくとも２つのシークレットシェア記憶デバイスまたは媒体から取得されたシークレットシェアを使用して、シークレットの再構成を試みるように構成される。

【０１１７】

[0128]例１０は、例９のコンピューティングデバイスを含み、少なくとも１つのプロセッサは、取得されたシークレットシェアからシークレットを再構成できない場合、メタデータに基づいて、取得されたシークレットシェアのうちの少なくとも１つのシークレットシェアを、正しくないとして特定するように構成される。

【０１１８】

[0129]例１１は、保護されるべきシークレットを決定することと、シークレットを、複数のシークレットシェアに分割することであって、複数のシークレットシェアの少なくともサブセットは、シークレットを再構成するために必要とされる、分割することと、各シークレットシェアを、それぞれのシェアホルダに配布するために、それぞれのポータブル記憶デバイスまたは媒体に転送することと、少なくとも各シークレットシェアのハッシュを用いてメタデータを生成することと、シークレットシェアを用いて、メタデータを、ポータブル記憶デバイスまたは媒体とは別に格納することとを含む、シークレット分割およびメタデータ記憶のための方法を含む。

【０１１９】

[0130]例１２は、例１１の方法を含み、シークレットと、シークレットシェアと、シークレットシェアのハッシュとの各々は、異なるキャラクタの文字列である。

[0131]例１３は、例１１～例１２のいずれかの方法を含み、シークレットは、秘密鍵を再構成するために使用できる暗号秘密鍵またはニーモニックフレーズもしくはシードである。

【０１２０】

[0132]例１４は、例１１～例１３のいずれかの方法を含み、分割することは、Ｓｈａｍｉｒシークレットシェアまたは多項式補間を使用して、シークレットを、複数のシークレットシェアに分割することを含む。

【０１２１】
[0133]例１５は、例１１～例１４のいずれかの方法を含み、シークレットを再構成するために各シークレットシェアを少なくとも１回使用することによって、シークレットシェアを検証することをさらに含み、シークレットシェアは、シークレットシェアが正常に検証された後、それぞれのポータブル記憶デバイスまたは媒体に単に転送される。
【０１２２】
[0134]例１６は、例１１～例１５のいずれかの方法を含み、シークレットを決定することの前に、コンピューティングデバイスにおいて、少なくとも１つの記憶デバイスの内容を消去し、オペレーティングシステムのクリーンインストールを実行することと、各シークレットシェアをそれぞれのポータブル記憶デバイスまたは媒体に転送することの後、コンピューティングデバイスにローカルに格納されたシークレットおよびシークレットシェアのコピーを削除することとをさらに含む。
【０１２３】
[0135]例１７は、例１１～例１６のいずれかの方法を含み、シークレットは、暗号秘密鍵であるか、または暗号秘密鍵を回復するために使用できるニーモニックフレーズもしくはシードであり、シークレットは、暗号秘密鍵またはニーモニックフレーズもしくはシードを生成することによって決定される。
【０１２４】
[0136]例１８は、例１７の方法を含み、メタデータにおいて、以下の情報、すなわち、暗号秘密鍵に対応する公開鍵と、分散型台帳における少なくとも１つのアドレスとを生成することをさらに含む。
【０１２５】
[0137]例１９は、例１１～例１８のいずれかの方法を含み、シェアホルダから取得された少なくとも２つのシークレットシェア記憶デバイスまたは媒体の各々から、取得されるシークレットシェアを決定することと、少なくとも２つのシークレットシェア記憶デバイスまたは媒体から取得されたシークレットシェアを使用して、シークレットの再構成を試みることとをさらに含む。
【０１２６】
[0138]例２０は、例１９の方法を含み、取得されたシークレットシェアからシークレットを再構成できない場合、メタデータに基づいて、取得されたシークレットシェアのうちの少なくとも１つのシークレットシェアを、正しくないとして特定することをさらに含む。
【０１２７】
[0139]例２１は、少なくとも１つのプロセッサと、少なくとも１つのプロセッサに通信可能に結合された少なくとも１つのメモリとを備え、少なくとも１つのプロセッサは、複数のシェアホルダのうちの少なくとも２人から取得された少なくとも２つのシークレットシェア記憶デバイスまたは媒体の各々から、取得されるシークレットシェアを決定し、シークレットシェアが複数のシェアホルダに配布される前に生成された複数のシークレットシェアの少なくともハッシュのリストを有するメタデータを判定し、少なくとも２つのシークレットシェア記憶デバイスまたは媒体から取得されたシークレットシェアを使用して、シークレットの再構成を試み、取得されたシークレットシェアからシークレットを再構成できない場合、メタデータに基づいて、取得されたシークレットシェアのうちの少なくとも１つのシークレットシェアを、正しくないとして特定するように構成された、コンピューティングデバイスを含む。
【０１２８】
[0140]例２２は、例２１のコンピューティングデバイスを含み、シークレットと、取得されたシークレットシェアと、複数のシークレットシェアのハッシュとの各々は、異なるキャラクタの文字列である。
【０１２９】
[0141]例２３は、例２１～例２２のいずれかのコンピューティングデバイスを含み、シークレットは、秘密鍵を再構成するために使用できる暗号秘密鍵またはニーモニックフレ

ーズもしくはシードである。
【０１３０】
[0142]例２４は、例２１～例２３のいずれかのコンピューティングデバイスを含み、少なくとも１つのプロセッサは、Ｓｈａｍｉｒ結合を使用してシークレットを再構成することを試みるように構成される。
【０１３１】
[0143]例２５は、例２１～例２４のいずれかのコンピューティングデバイスを含み、少なくとも１つのプロセッサは、取得されたそれぞれのシークレットシェアを、メタデータにおけるハッシュのリストと比較することによって、取得されたシークレットシェアの各々を検証するように構成され、取得されたそれぞれのシークレットシェアが、メタデータにおけるハッシュのリストにおけるハッシュと一致する場合、取得されたそれぞれのシークレットシェアは正常に検証される。
【０１３２】
[0144]例２６は、例２５のコンピューティングデバイスを含み、少なくとも１つのプロセッサは、シークレットシェアが正常に検証された後にのみ、シークレットを再構成することを試みるように構成される。
【０１３３】
[0145]例２７は、例２１～例２６のいずれかのコンピューティングデバイスを含み、少なくとも１つのプロセッサは、シークレットが、取得されたシークレットシェアから再構成されたときに、再構成されたシークレットを必要とする以下のアクション、すなわち、再構成されたシークレットを使用してデータを暗号化または解読すること、再構成されたシークレットに基づいて、分散型台帳におけるトランザクションアドレスを生成すること、または、再構成されたシークレットを使用してトランザクションに署名することであって、トランザクションは、分散型台帳におけるアドレスから暗号通貨を送金する、署名すること、のうちの少なくとも１つを実行するように構成される。
【０１３４】
[0146]例２８は、例２１～例２７のいずれかのコンピューティングデバイスを含み、少なくとも１つのプロセッサは、取得されるシークレットシェアが決定される前に、シークレットを、複数のシークレットシェアに分割することであって、複数のシークレットシェアの少なくともサブセットは、シークレットを再構成するために必要とされる、分割することと、各シークレットシェアをそれぞれのポータブル記憶デバイスまたは媒体に転送することとを行うように構成され、各ポータブル記憶デバイスまたは媒体は、複数のシェアホルダに配布される。
【０１３５】
[0147]例２９は、複数のシェアホルダのうちの少なくとも２人から取得された少なくとも２つのシークレットシェア記憶デバイスまたは媒体の各々から取得されるシークレットシェアを決定することと、シークレットシェアが複数のシェアホルダに配布される前に生成された複数のシークレットシェアの少なくともハッシュのリストを有するメタデータを判定することと、少なくとも２つのシークレットシェア記憶デバイスまたは媒体から取得されたシークレットシェアを使用して、シークレットの再構成を試みることと、取得されたシークレットシェアからシークレットを再構成できない場合、メタデータに基づいて、取得されたシークレットシェアのうちの少なくとも１つのシークレットシェアを、正しくないとして特定することとを含む、方法を含む。
【０１３６】
[0148]例３０は、例２９の方法を含み、シークレットと、取得されたシークレットシェアと、複数のシークレットシェアのハッシュとの各々は、異なるキャラクタの文字列である。
【０１３７】
[0149]例３１は、例２９～例３０のいずれかの方法を含み、シークレットは、秘密鍵を再構成するために使用できる暗号秘密鍵またはニーモニックフレーズもしくはシードであ

る。

【０１３８】

[0150]例３２は、例２９～例３１のいずれかの方法を含み、Ｓｈａｍｉｒ結合を使用してシークレットを再構成することを試みることをさらに含む。

[0151]例３３は、例２９～例３２のいずれかの方法を含み、取得されたそれぞれのシークレットシェアを、メタデータにおけるハッシュのリストと比較することによって、取得されたシークレットシェアの各々を検証することをさらに含み、取得されたそれぞれのシークレットシェアが、メタデータにおけるハッシュのリストにおけるハッシュと一致する場合、取得されたそれぞれのシークレットシェアは正常に検証される。

【０１３９】

[0152]例３４は、例３３の方法を含み、試みることは、シークレットシェアが正常に検証された後にのみ、シークレットを再構成することを試みることを含む。

[0153]例３５は、例２９～例３４のいずれかの方法を含み、シークレットが、取得されたシークレットシェアから再構成されたときに、再構成されたシークレットを必要とする以下のアクション、すなわち、再構成されたシークレットを使用してデータを暗号化または解読すること、再構成されたシークレットに基づいて、分散型台帳におけるトランザクションアドレスを生成すること、または、再構成されたシークレットを使用してトランザクションに署名することであって、トランザクションは、分散型台帳におけるアドレスから暗号通貨を送金する、署名すること、のうちの少なくとも１つを実行することをさらに含む。

【０１４０】

[0154]例３６は、例２９～例３５のいずれかの方法を含み、取得されるシークレットシェアが決定される前に、シークレットを、複数のシークレットシェアに分割することであって、複数のシークレットシェアの少なくともサブセットは、シークレットを再構成するために必要とされる、分割することと、各シークレットシェアをそれぞれのポータブル記憶デバイスまたは媒体に転送することとをさらに含み、各ポータブル記憶デバイスまたは媒体は、複数のシェアホルダに配布される。

【図面】

【図１】

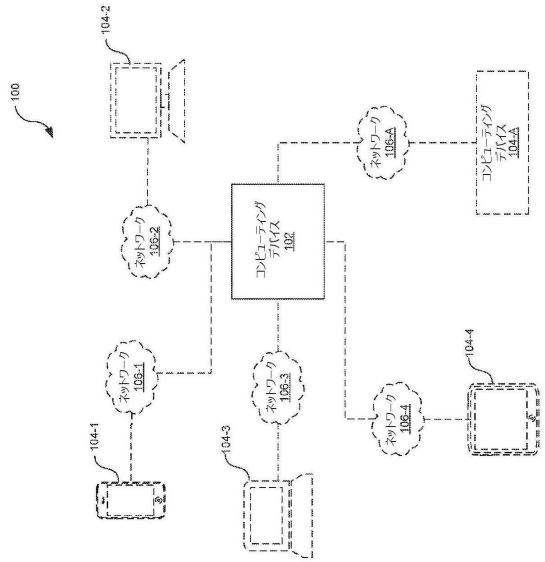

FIG. 1

【図２】

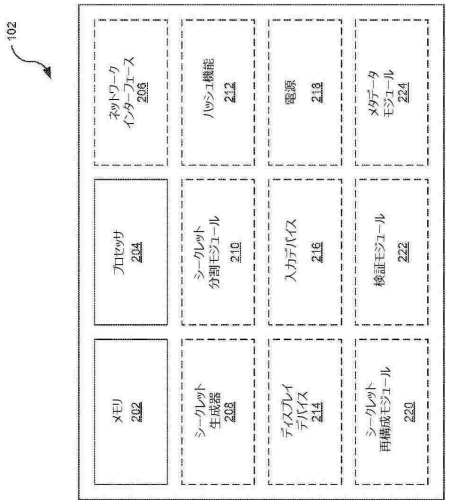

FIG. 2

【図３】

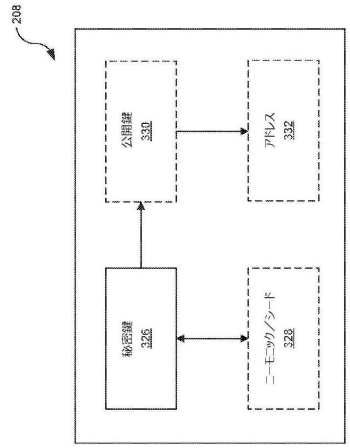

FIG. 3

【図４】

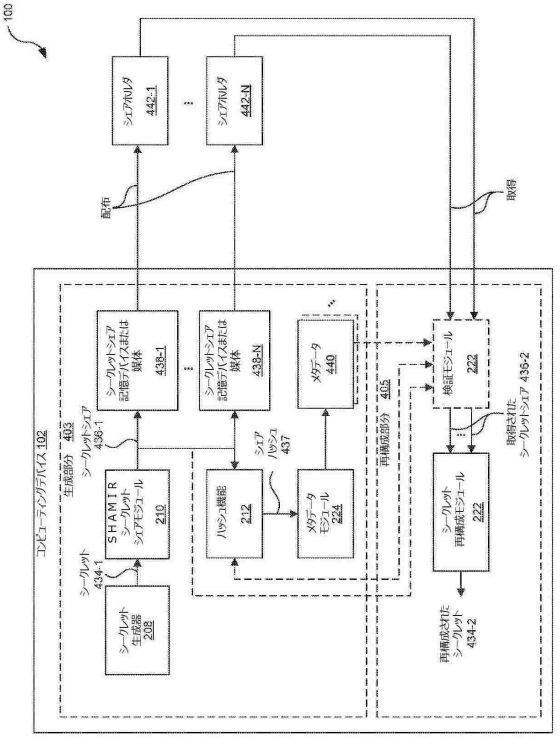

FIG. 4

【図５】

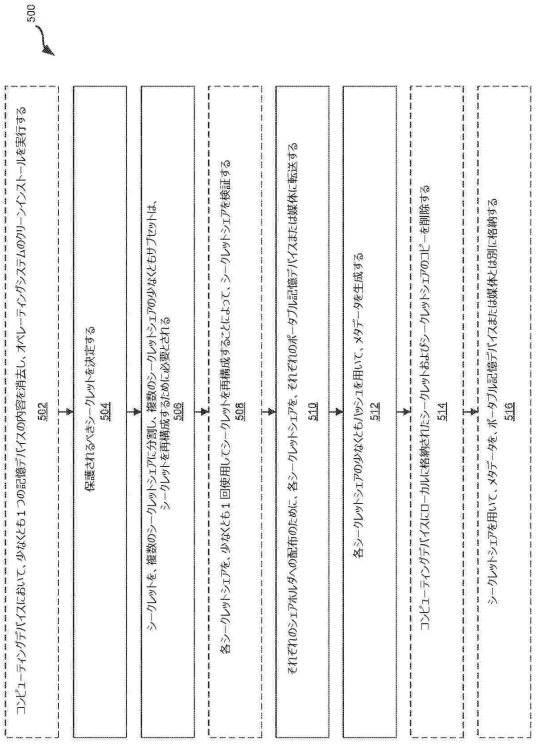

FIG. 5

【図６】

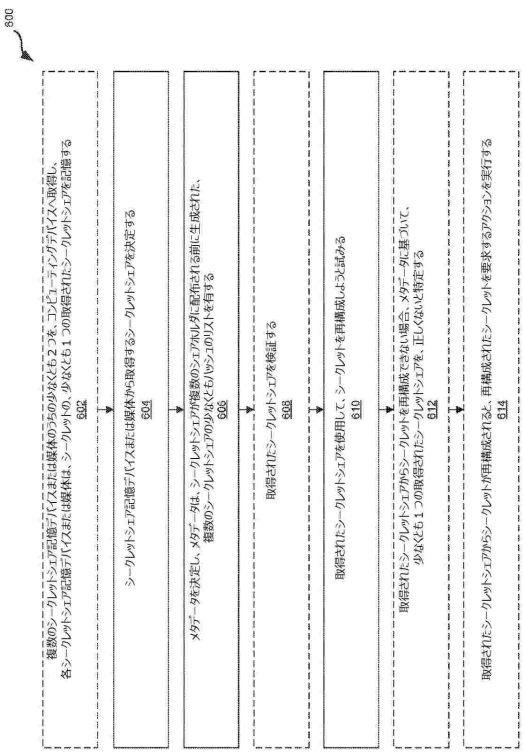

FIG. 6

【図７】

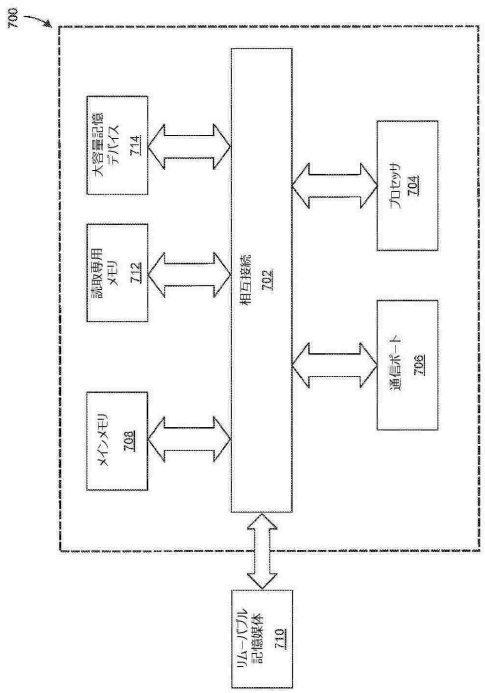

FIG. 7

フロントページの続き

７，ニューヨーク，フルトン・ストリート ２８５，ワン・ワールド・トレード・センター，フィフティーエイス・フロア
(72)発明者 エンペイ，ジェシー
アメリカ合衆国ニューヨーク州１０００７，ニューヨーク，フルトン・ストリート ２８５，ワン・ワールド・トレード・センター，フィフティーエイス・フロア
(72)発明者 ウェルカー，ブラッド
アメリカ合衆国ニューヨーク州１０００７，ニューヨーク，フルトン・ストリート ２８５，ワン・ワールド・トレード・センター，フィフティーエイス・フロア

審査官 中里 裕正

(56)参考文献
特開２０１９－１５３８４２（ＪＰ，Ａ）
特開２００７－３３４４１７（ＪＰ，Ａ）
米国特許出願公開第２０１７／０００５７９７（ＵＳ，Ａ１）
米国特許出願公開第２００７／０１６０１９８（ＵＳ，Ａ１）
国際公開第２０１９／０２１１０５（WO，Ａ１）
RAMAN, K. V. and VARSHNEY, L. R.，Dynamic Distributed Storage for Scaling Blockchains，arXiv，1711.07617v2，[online]，2018年01月07日，〈URL:https://arxiv.org/abs/1711.07617v2〉，[2024年10月28日 検索]

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｈ０４Ｌ ９／３２
Ｇ０９Ｃ １／００