(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6799061号
(P6799061)
(45)発行日　令和2年12月9日(2020.12.9)　(24)登録日　令和2年11月24日(2020.11.24)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/00 601E
H04L 9/00 601A

請求項の数 26　(全 27 頁)

(21)出願番号　特願2018-522105 (P2018-522105)
(86)(22)出願日　平成29年2月14日 (2017.2.14)
(65)公表番号　特表2019-509648 (P2019-509648A)
(43)公表日　平成31年4月4日 (2019.4.4)
(86)国際出願番号　PCT/IB2017/050829
(87)国際公開番号　WO2017/145010
(87)国際公開日　平成29年8月31日 (2017.8.31)
審査請求日　平成30年11月8日 (2018.11.8)
(31)優先権主張番号　1603117.1
(32)優先日　平成28年2月23日 (2016.2.23)
(33)優先権主張国・地域又は機関
英国 (GB)
(31)優先権主張番号　1605026.2
(32)優先日　平成28年3月24日 (2016.3.24)
(33)優先権主張国・地域又は機関
英国 (GB)

(73)特許権者　318001991
エヌチェーン　ホールディングス　リミテッド
NCHAIN HOLDINGS LIMITED
アンティグア・バーブーダ、　セントジョンズ、　44　チャーチ　ストリート、　フィッツジェラルド　ハウス
Fitzgerald House, 44 Church Street, St. John's, Antigua and Barbuda (AG)
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】ウォレット管理システムと併せたブロックチェーンベースのシステムのための暗号鍵のセキュアなマルチパーティ損失耐性のある記憶及び転送

(57)【特許請求の範囲】
【請求項１】
検証要素をセキュアに送信するコンピュータ実施方法であって、
前記検証要素を複数のシェアに分割するステップと、
ネットワーク内の２つ以上のノードにおいて共通秘密を決定するステップと、
前記共通秘密を用いて、前記２つ以上のノード間で前記検証要素の少なくとも１つのシェアを送信するステップと
を含み、
前記ネットワーク内の第１のノード（Ｃ）は、第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を有する第１の非対称暗号対に関連付けられ、前記ネットワーク内の第２のノード（Ｓ）は、第２のノードのマスター私有鍵（V_{1S}）と第２のノードのマスター公開鍵（P_{1S}）を有する第２の非対称暗号対に関連付けられ、
共通秘密を決定する前記ステップは、
前記第１のノード（Ｃ）において、
－少なくとも前記第１のノードのマスター私有鍵（V_{1C}）と発生器値（ＧＶ）に基づいて第１のノードの第２の私有鍵（V_{2C}）を決定するステップと、
－少なくとも前記第２のノードのマスター公開鍵（P_{1S}）と前記発生器値（ＧＶ）に基づいて第２のノードの第２の公開鍵（P_{2S}）を決定するステップと、
－前記第１のノードの第２の私有鍵（V_{2C}）と前記第２のノードの第２の公開鍵（Ｐ

$_{2S}$）に基づいて前記共通秘密（ＣＳ）を決定するステップと、
前記第２のノード（Ｓ）において、
－少なくとも前記第２のノードのマスター私有鍵（$Ｖ_{1S}$）と発生器値（ＧＶ）に基づいて第２のノードの第２の私有鍵（$Ｖ_{2S}$）を決定するステップと、
－少なくとも前記第１のノードのマスター公開鍵（$Ｐ_{1C}$）と前記発生器値（ＧＶ）に基づいて第１のノードの第２の公開鍵（$Ｐ_{2C}$）を決定するステップと、
－前記第２のノードの第２の私有鍵（$Ｖ_{2S}$）と前記第１のノードの第２の公開鍵（$Ｐ_{2C}$）に基づいて前記共通秘密（ＣＳ）を決定するステップと、
を含む、方法。
【請求項２】
前記検証要素は、暗号鍵、暗号鍵の表現、又は前記暗号鍵にアクセスし、前記暗号鍵を計算し、もしくは導出するのに用いることができる要素である請求項１に記載の方法。
【請求項３】
前記共通秘密を用いて暗号化鍵を作成するステップを更に含み、前記暗号化鍵は、前記検証要素の前記少なくとも１つのシェア、又は前記少なくとも１つのシェアを含むかもしくは前記少なくとも１つのシェアに関係するメッセージを暗号化するのに用いられる請求項１又は２に記載の方法。
【請求項４】
相互に対して異なる場所に前記検証要素の少なくとも３つのシェアを記憶するステップ、を更に含む請求項１～３のいずれか１項に記載の方法。
【請求項５】
前記３つのシェアのうちの少なくとも１つが、少なくとも２つの他の場所と別であって、独立した、及び／又は別個のバックアップに又は安全な記憶施設に記憶される、請求項４に記載の方法。
【請求項６】
前記検証要素は、デジタルウォレット、又は何らかの形態の貨幣に関係するリソースに関連付けられる、請求項１～５のいずれか１項に記載の方法。
【請求項７】
前記検証要素は、前記検証要素を前記シェアのうちの２つ以上から復元又は再作成することができるように複数のシェアに分割される、請求項１～６のいずれか１項に記載の方法。
【請求項８】
前記検証要素は、シャミアの秘密分散法を用いて複数のシェアに分割される請求項７に記載の方法。
【請求項９】
前記共通秘密は、
ｉ）前記少なくとも２つのノードにおいて互いに独立して決定され、前記共通秘密が前記ノード間の通信チャネルを介した送信を必要としないようにし、
ｉｉ）前記少なくとも２つのノードによってのみ共有される
請求項１～８のいずれか１項に記載の方法。
【請求項１０】
デジタルウォレットをセットアップし、作成し、又は登録するステップを含み、前記検証要素は前記デジタルウォレットに関連付けられている請求項１～９のいずれか１項に記載の方法。
【請求項１１】
前記発生器値（ＧＶ）は、メッセージ（Ｍ）に基づいている請求項１～１０のいずれか１項に記載の方法。
【請求項１２】
前記メッセージ（Ｍ）と前記第１のノードの第２の私有鍵（$Ｖ_{2C}$）に基づいて第１の署名付きメッセージ（ＳＭ１）を作成するステップと、

前記ネットワークを介して、前記第１の署名付きメッセージ（ＳＭ１）を前記第２のノード（Ｓ）に送信するステップと、
を更に含み、
前記第１の署名付きメッセージ（ＳＭ１）は、前記第１のノード（Ｃ）を認証するために、第１のノードの第２の公開鍵（P_{2C}）を用いて有効性を確認することができる請求項１１に記載の方法。
【請求項１３】
前記ネットワークを介して、前記第２のノード（Ｓ）から第２の署名付きメッセージ（ＳＭ２）を受信することと、
前記第２のノードの第２の公開鍵（Ｐ２Ｓ）を用いて前記第２の署名付きメッセージ（ＳＭ２）の有効性を確認することと、
前記第２の署名付きメッセージ（ＳＭ２）の有効性を確認した結果に基づいて、前記第２のノード（Ｓ）を認証することと
を更に含み、前記第２の署名付きメッセージ（ＳＭ２）は、前記メッセージ（Ｍ）又は第２のメッセージ（Ｍ２）、及び前記第２のノードの第２の私有鍵（V_{2S}）に基づいて作成された請求項１～１２のいずれか１項に記載の方法。
【請求項１４】
メッセージ（Ｍ）を作成することと、
前記ネットワークを介して、前記メッセージ（Ｍ）を前記第２のノード（Ｓ）に送信することと
を更に含む請求項１～１３のいずれか１項に記載の方法。
【請求項１５】
前記ネットワークを介して、前記第２のノード（Ｓ）から前記メッセージ（Ｍ）を受信すること
を更に含む請求項１１～１４のいずれか１項に記載の方法。
【請求項１６】
前記ネットワークを介して、別のノードから前記メッセージ（Ｍ）を受信するステップを更に含む請求項１１～１５のいずれか１項に記載の方法。
【請求項１７】
前記第１のノードのマスター公開鍵（P_{1C}）と第２のノードのマスター公開鍵（P_{1S}）は、それぞれ第１のノードのマスター私有鍵（V_{1C}）と第２のノードのマスター私有鍵（V_{1S}）とベースポイント（Ｇ）との楕円曲線点乗算に基づいている請求項１～１６のいずれか１項に記載の方法。
【請求項１８】
前記ネットワークを介して、前記第２のノードのマスター公開鍵（P_{1S}）を受信するステップと、
前記第１のノード（Ｃ）に関連付けられたデータストアに、前記第２のノードのマスター公開鍵（P_{1S}）を記憶するステップと
を更に含む請求項１～１７のいずれか１項に記載の方法。
【請求項１９】
第１のノード（Ｃ）において、前記第１のノードのマスター私有鍵（V_{1C}）及び前記第１のノードのマスター公開鍵（P_{1C}）を作成するステップと、
前記ネットワークを介して、前記第１のノードのマスター公開鍵（P_{1C}）を前記第２のノード（Ｓ）及び／又は他のノードに送信するステップと、
－　前記第１のノード（Ｃ）に関連付けられた第１のデータストアに、前記第１のノードのマスター私有鍵（V_{1C}）を記憶するステップと
を更に含む、請求項１～１８のいずれか１項に記載の方法。
【請求項２０】
前記発生器値（ＧＶ）は、以前の発生器値（ＧＶ）のハッシュを決定することに基づいている請求項１～１９のいずれか１項に記載の方法。

【請求項２１】
前記第１の非対称暗号対及び前記第２の非対称暗号対は、それぞれ以前の第１の非対称暗号対及び以前の第２の非対称暗号対の関数に基づいている請求項１～２０のいずれか１項に記載の方法。
【請求項２２】
検証要素をセキュアに送信するコンピュータベースのシステムであって、前記システムはネットワークを介して接続された第１のノード（Ｃ）及び第２のノード（Ｓ）を含み、
前記第１のノード（Ｃ）及び前記第２のノード（Ｓ）の各々は、前記検証要素を分割することにより得られた複数のシェアのうちの少なくとも１つを有し、
前記第１のノード（Ｃ）は、
－前記第１のノード（Ｃ）のマスター私有鍵（V_{1C}）及び前記第１のノード（Ｃ）のマスター公開鍵（P_{1C}）を有する第１の非対称暗号対に関連付けられ、
－少なくとも前記第１のノードのマスター私有鍵（V_{1C}）と発生器値（ＧＶ）に基づいて第１のノードの第２の私有鍵（V_{2C}）を決定し、
－少なくとも前記第２のノードのマスター公開鍵（P_{1S}）と前記発生器値（ＧＶ）に基づいて第２のノードの第２の公開鍵（P_{2S}）を決定し、
－前記第１のノードの第２の私有鍵（V_{2C}）と前記第２のノードの第２の公開鍵（P_{2S}）に基づいて共通秘密（ＣＳ）を決定する、よう構成され、
前記第２のノード（Ｓ）は、
－前記第２のノード（Ｓ）のマスター私有鍵（V_{1S}）と前記第２のノード（Ｓ）のマスター公開鍵（P_{1S}）を有する第２の非対称暗号対に関連付けられ、
－少なくとも前記第２のノードのマスター私有鍵（V_{1S}）と発生器値（ＧＶ）に基づいて第２のノードの第２の私有鍵（V_{2S}）を決定し、
－少なくとも前記第１のノードのマスター公開鍵（P_{1C}）と前記発生器値（ＧＶ）に基づいて第１のノードの第２の公開鍵（P_{2C}）を決定し、
－前記第２のノードの第２の私有鍵（V_{2S}）と前記第１のノードの第２の公開鍵（P_{2C}）に基づいて前記共通秘密（ＣＳ）を決定する、よう構成され、
前記第１のノード（Ｃ）及び前記第２のノード（Ｓ）は、前記共通秘密を用いて、前記検証要素の少なくとも１つのシェアを前記第１のノード（Ｃ）及び前記第２のノード（Ｓ）の間で送信する、システム。
【請求項２３】
前記検証要素は、デジタルウォレット又は何らかの形態の貨幣に関係するリソースに関連付けられる、請求項２２に記載のシステム。
【請求項２４】
前記システムは、デジタルウォレットのセットアップ、作成又は登録を可能にするように構成されたソフトウェアを備え、前記検証要素は、前記デジタルウォレットに関連付けられている請求項２２又は２３に記載のシステム。
【請求項２５】
デジタルウォレットに関連付けられた検証要素をセキュアに送信するように構成されたコンピュータ実施システムであって、ネットワークを介して接続された２つ以上のエンティティを含み、
前記２つ以上のエンティティの各々は、前記検証要素を分割することにより得られた複数のシェアのうちの少なくとも１つを有し、
前記２つ以上のエンティティのうちの第１のエンティティは、少なくとも第１のエンティティのマスター私有鍵及び発生器値に基づいて第１のエンティティの第２の私有鍵を決定し、
前記２つ以上のエンティティのうちの第２のエンティティは、少なくとも第２のエンティティのマスター私有鍵及び前記発生器値に基づいて第２のエンティティの第２の私有鍵を決定し、
前記第１のエンティティは、前記第１のエンティティの第２の私有鍵及び第２のエンテ

ィティの第２の公開鍵に基づいて共通秘密（ＣＳ）を決定し、前記第２のエンティティは、前記第２のエンティティの第２の私有鍵及び第１のエンティティの第２の公開鍵に基づいて前記共通秘密（ＣＳ）を決定し、

前記第１及び第２のエンティティは、前記共通秘密を用いて、前記第１及び第２のエンティティ間で前記検証要素の少なくとも１つのシェアを送信し、

前記第１のエンティティの第２の公開鍵及び前記第２のエンティティの第２の公開鍵は、それぞれ、前記第１の／第２のエンティティのマスター鍵及び前記発生器値に基づいているコンピュータ実施システム。

【請求項２６】

デジタルウォレットに関連付けられた検証要素をセキュアに送信する方法であって、ネットワークを介して接続された２つ以上のエンティティを含むコンピュータ実施システムにより実施され、前記２つ以上のエンティティの各々は、前記検証要素を分割することにより得られた複数のシェアのうちの少なくとも１つを有し、前記方法は、

前記２つ以上のエンティティのうちの第１のエンティティにより、少なくとも第１のエンティティのマスター私有鍵及び発生器値に基づいて第１のエンティティの第２の私有鍵を決定するステップと、

前記２つ以上のエンティティのうちの第２のエンティティにより、少なくとも第２のエンティティのマスター公開鍵及び前記発生器値に基づいて第２のエンティティの第２の公開鍵を決定するステップと、

前記第１のエンティティにより、前記第１のエンティティの第２の私有鍵及び前記第２のエンティティの第２の公開鍵に基づいて共通秘密（ＣＳ）を決定するステップと、

前記第２のエンティティにより、前記第２のエンティティの第２の私有鍵及び前記第２のエンティティの第２の公開鍵に基づいて前記共通秘密（ＣＳ）を決定するステップと、

前記第１及び第２のエンティティにより、前記共通秘密を用いて、前記第１及び第２のエンティティ間で前記検証要素の少なくとも１つのシェアを送信するステップと、を含み、

前記第１のエンティティの第２の公開鍵及び前記第２のエンティティの第２の公開鍵は、それぞれ、前記第１／第２のエンティティのマスター鍵及び前記発生器値に基づいている方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、包括的には、コンピュータ及びデータセキュリティに関し、より詳細には、暗号鍵等の機密性の高いデータ項目のセキュアな取扱に関するものである。本発明は、アクセス制御メカニズムを提供する。本発明は、限定ではないが、デジタル（ソフトウェア）ウォレットと共に用いるのに特に適している。これは、ビットコイン等の暗号通貨に関連して用いられるウォレットを含むことができる。本発明は、有利なアクセス制御メカニズムを提供する。

【背景技術】

【０００２】

暗号学は、ネットワーク内の２つ以上のノード間の機密データのセキュアな記憶及びその通信のための技法を伴う。ノードは、モバイル通信デバイス、タブレットコンピュータ、ラップトップコンピュータ、デスクトップ、その他の形態のコンピューティングデバイス及び通信デバイス、ネットワークにおけるサーバーデバイス、ネットワークにおけるクライアントデバイス、分散ネットワークにおける１つ又は複数のノード等を含むことができる。ノードは、自然人、会社の従業員等の人々のグループ、銀行システムのようなシステム、又は分散されたピアツーピアレッジャー（すなわち、ブロックチェーン）等に関連付けることができる。

【０００３】

２つ以上のノードがセキュアでない通信ネットワークによってリンクされ、認可されて

いない第三者による盗聴又は傍受に対し脆弱である場合がある。従って、ノード間で送信されるメッセージは、多くの場合に暗号化された形式で送信される。受信時に、意図される受信者が、対応する復号鍵又は他の復号方法を用いてメッセージを復号する。このため、そのような通信のセキュリティは、第三者が対応する復号鍵を決定することを防ぐことに依拠し得る。

【０００４】

１つの既知の暗号化方法は、対称鍵アルゴリズムを用いることを含む。鍵は、同じ対称鍵が、平文メッセージの暗号化及び暗号文メッセージの復号の双方に用いられるという意味で対称である。しかし、対称鍵は、対称鍵への認可されていないアクセスを防ぐために、セキュアな方法で双方のノードに送信されなくてはならない。これは、例えば、対称鍵がセキュアでない通信ネットワークを介して送信されることがないように、対称鍵を（認可された）ノードに物理的に送達することを含むことができる。しかし、物理的送達は、必ずしも、常に実用的な選択肢ではない。従って、そのような暗号化システムにおける問題は、インターネットの如きセキュアでない電子ネットワークにわたるノード間の対称鍵（共通秘密に基づくことができる）を確立することである。このため、対称鍵（共通秘密）を提供するこのステップは、潜在的に重篤な脆弱性である。対称鍵アルゴリズム及びプロトコルは、単純であり、広く用いられているため、２つのノードがセキュアでないネットワークにわたってセキュアに共通秘密に基づく対称鍵を決定する能力が必要とされている。

【０００５】

公開鍵暗号学としても知られる非対称鍵を使用すると、この問題をある程度回避する。私有鍵は、秘密のままにされるのに対し、公開鍵は、公開で入手可能にすることができる。ネットワークにおける公開鍵の傍受は破滅的でない。既存のプロトコルは、ディフィー・ヘルマン鍵交換及び３パスプロトコルを含んでいる。

【０００６】

しかし、私有鍵の記憶は、大きなセキュリティの問題を引き起こす。例えば、ビットコインウォレット等のデジタルウォレットを検討すると、デジタルウォレットは、ユーザが自身の電子資産を用いてトランザクションを行うように、例えばビットコイン資金を用いて商品及びサービスを購入するように、他のノードと接続することを可能にするソフトウェアを含んでいる。公開鍵暗号化は、多くの場合、そのような接続及びトランザクションに必要とされる不可欠な情報を保護するのに用いられる。私有鍵は、ユーザのデバイス（「クライアント側」）にインストールされるウォレットによって又はウォレットサービスプロバイダ（「サーバ側」）によって記憶される。しかし、私有鍵がクライアント側においてのみ記憶される場合、私有鍵は、ユーザのハードウェア、例えば、コンピュータ、携帯電話等に生じる盗難、紛失又は損傷により失われる可能性がある。同様に、ユーザが死亡するかもしくは行動不能になった場合、私有鍵の知識又は私有鍵へのアクセスが失われる可能性があり、このため、ウォレットに関連付けられた資金がアクセス不能になる。私有鍵をサーバー側に記憶することにより、これらの問題を克服できる可能性があるが、ユーザは、自身の私有鍵をセキュアに保つためにサービスプロバイダを信頼するよう調整しなくてはならない。サーバー側におけるセキュリティ違反は、現実の大きなリスクである。

【発明の概要】

【発明が解決しようとする課題】

【０００７】

このため、秘密の安全な取扱を可能にする解決法を提供することが望ましい。この秘密は、暗号鍵、及び／又は鍵へのアクセスを提供することができる何らかのものとすることができる。そのような改善された解決法がここで考案されている。本発明によれば、添付の特許請求の範囲において定義されるような改善された解決法が提供される。

【課題を解決するための手段】

【０００８】

本発明は、コンピュータ実施方法を提供するものとすることができる。この方法は、リソースへのアクセスの制御を可能にすることができる。この方法は、検証又は認証方法と称することができる。この方法は、暗号鍵管理解決法と称することができる。リソースは、任意のタイプの物理的リソース又は電子リソースとすることができる。１つの実施形態において、リソースは、デジタルウォレット又は貨幣の形態に関連する何らかの他のリソースである。これは、暗号通貨リソースの管理のためのビットコインウォレット又は他のウォレットであり得る。本発明は、デジタルウォレット（及び対応するシステム）へのアクセスを制御する方法を提供するものとすることができる。

【０００９】

本発明は、トランザクション如き後続のウォレット関連動作がセキュアに取り扱われ、通信され、及び／又は作成されることを可能にするために、セキュアでない通信チャネル（インターネットの如きもの）を介したデジタルウォレットのセットアップ、登録又は作成中に用いることができる。

【００１０】

本発明の１つ又は複数の実施形態は、既存の暗号鍵対から暗号鍵を導出するステップを含むものとすることができる。これは、

少なくとも第１のエンティティのマスター私有鍵及び発生器値に基づいて第１のエンティティの第２の私有鍵を決定するステップと、

少なくとも第２のエンティティのマスター私有鍵及び発生器値に基づいて第２のエンティティの第２の私有鍵を決定するステップと、

第１のエンティティの第２の私有鍵及び第２のエンティティの第２の公開鍵に基づいて第１のエンティティにおいて共通秘密（ＣＳ）を決定し、第２のエンティティの第２の私有鍵及び第１のエンティティの第２の公開鍵に基づいて第２のエンティティにおいて共通秘密（ＣＳ）を決定するステップと

を含み、

第１のエンティティの第２の公開鍵及び第２のエンティティの第２の公開鍵は、それぞれ、少なくとも第１／第２のエンティティのマスター鍵及び発生器値に基づいている方法である。

【００１１】

それに加えて、又はそれに代えて、本発明は、デジタルウォレットへのアクセスを制御する方法を含むものとすることができる。この方法は、

少なくとも第１のエンティティのマスター私有鍵及び発生器値に基づいて第１のエンティティの第２の私有鍵を決定するステップと、

少なくとも第２のエンティティのマスター私有鍵及び発生器値に基づいて第２のエンティティの第２の私有鍵を決定するステップと、

第１のエンティティの第２の私有鍵及び第２のエンティティの第２の公開鍵に基づいて第１のエンティティにおいて共通秘密（ＣＳ）を決定し、第２のエンティティの第２の私有鍵及び第１のエンティティの第２の公開鍵に基づいて第２のエンティティにおいて共通秘密（ＣＳ）を決定するステップと、

を含み、

第１のエンティティの第２の公開鍵及び第２のエンティティの第２の公開鍵は、それぞれ、少なくとも第１／第２のエンティティのマスター鍵及び発生器値に基づいている方法である。

【００１２】

それに加えて、又はそれに代えて、この方法は、

検証要素を複数のシェア（ｓｈａｒｅ）に分割するステップと、

ネットワーク内の２つ以上のノードにおいて共通秘密を決定するステップと、

この共通秘密を用いて、検証要素の少なくとも１つのシェアを、ネットワーク内の１つのノードから少なくとも１つの他のノードに送信するステップと、

を含むことができる。

【００１３】
検証要素は、暗号鍵とすることができる。検証要素は、非対称暗号対における私有鍵とすることができる。それに加えて、又はそれに代えて、検証要素は、暗号鍵の表現、又は暗号鍵にアクセスし、暗号鍵を計算し、導出し、もしくは取り出すのに用いることができる何らかのアイテムとすることができる。検証要素は、例えばニーモニック又はシード等の、検証プロセスにおいて用いることができる何らかの秘密又は値とすることができる。
【００１４】
従って、本発明の１つの態様は、私有鍵等の秘密を（一意の）シェアに分割することに関することができる。検証要素は、検証要素を、シェアのうちの２つ以上から復元又は再作成することができるように複数のシェアに分割することができる。シャミアの秘密分散法を用いて、検証要素を複数のシェアに分割することができる。
【００１５】
これらのシェアは、単独では価値を有しないように分割することができ、これは、単独のシェアを用いて（元の分割されていない）検証要素に達することができないことを意味する。この分割は、検証要素を、所定の複数のシェアを組み合わせることによってのみ復元することができるように行うことができる。１つの実施形態では、任意の２つのシェアが検証要素の復元に十分である。
【００１６】
本発明の別の態様は、それぞれのシェアの安全な取扱い又は記憶に関するものとすることができる。これらのシェアは、異なる複数の関係者に送信され、それらの関係者によって記憶することができる。これらの関係者のうちのいくつか又は全ては、ネットワーク上のノードとすることができる。１つの実施形態において、この方法は、互いに対し異なる場所において検証要素の少なくとも３つのシェアを記憶するステップを含むことができる。
【００１７】
シェアのうちの少なくとも１つを、バックアップ又は「安全な記憶」施設に記憶することができる。これは、シェアを記憶するいかなる他の場所とも別であり、独立し、及び／又は別個とすることができる。これは、他のシェアのうちの１つが利用不可能になった場合の検証要素の復元を可能にするため、重要な利点を提供する。そのような状況において、シェアは、安全な記憶施設から取り出すことができる。
【００１８】
検証プロセスは、シェアを用いた検証要素の復元の前に行うことができる。検証プロセスは、所定のもしくは指定された個人、及び／又はコンピューティングリソースのアイデンティティの検証を含むことができる。
【００１９】
本発明の別の態様は、シェアのうちの１つ又は複数のセキュアな分散に関するものである。この方法は、共通秘密を用いて暗号化鍵を作成するステップを含むことができ、この暗号化鍵は、検証要素の少なくとも１つのシェア、又はこの少なくとも１つのシェアを含むメッセージを暗号化するのに用いられる。
【００２０】
共通秘密は、少なくとも２つのノードにおいて互いに独立して決定することができる。従って、各ノードは、他のノード又は別の関係者からの入力又はそれらとの通信なしで、秘密を自身で決定又は作成することができる。これは、共通秘密が、通信チャネルを介した送信を必要としなくてもよいことを意味する。このようにすると、認可されていない関係者によって傍受されることがないので、セキュリティの向上をもたらす。共通秘密は、少なくとも２つのノードのみに共通とする（すなわち、それらのノードによってのみ共有される）ことができる。その際、共通秘密を用いて暗号化鍵を生成することができ、この暗号化鍵を、シェアの安全な送信のために用いることができる。他のデータも、暗号化鍵を用いて送信することができる。
【００２１】

この方法は、第１のノード（Ｃ）において、第１のノード（Ｃ）及び第２のノード（Ｓ）に共通の共通秘密（ＣＳ）を決定するステップを含むことができ、第１のノード（Ｃ）は、第１のノードのマスター私有鍵（$Ｖ_{1\ C}$）及び第１のノードのマスター公開鍵（$Ｐ_{1\ C}$）を有する第１の非対称暗号対に関連付けられ、第２のノード（Ｓ）は、第２のノードのマスター私有鍵（$Ｖ_{1\ S}$）及び第２のノードのマスター公開鍵（$Ｐ_{1\ S}$）を有する第２の非対称暗号対に関連付けられ、且つ、この方法は、

－　少なくとも第１のノードのマスター私有鍵（$Ｖ_{1\ C}$）及び発生器値（ＧＶ）に基づいて第１のノードの第２の私有鍵（$Ｖ_{2\ C}$）を決定するステップと、

－　少なくとも第２のノードのマスター公開鍵（$Ｐ_{1\ S}$）及び発生器値（ＧＶ）に基づいて第２のノードの第２の公開鍵（$Ｐ_{2\ S}$）を決定するステップと、

－　第１のノードの第２の私有鍵（$Ｖ_{2\ C}$）及び第２のノードの第２の公開鍵（$Ｐ_{2\ S}$）に基づいて共通秘密（ＣＳ）を決定するステップと、

を更に含み、

第２のノード（Ｓ）は、第１のノードの第２の公開鍵（$Ｐ_{2\ C}$）及び第２のノードの第２の私有鍵（$Ｖ_{2\ S}$）に基づいて同じ共通秘密（Ｓ）を有し、第１のノードの第２の公開鍵（$Ｐ_{2\ C}$）は、少なくとも、第１のノードのマスター公開鍵（$Ｐ_{1\ C}$）及び発生器値（ＧＶ）に基づき、第２のノードの第２の私有鍵（$Ｖ_{2\ S}$）は、少なくとも、第２のノードのマスター私有鍵（$Ｖ_{1\ S}$）及び発生器値（ＧＶ）に基づいている。

【００２２】

発生器値（ＧＶ）は、メッセージ（Ｍ）に基づいている。この方法は、メッセージ（Ｍ）及び第１のノードの第２の私有鍵（$Ｖ_{2\ C}$）に基づいて第１の署名付きメッセージ（ＳＭ１）を作成することと、通信ネットワークを介して、第１の署名付きメッセージ（ＳＭ１）を第２のノード（Ｓ）に送信することとを更に含むことができ、第１の署名付きメッセージ（ＳＭ１）は、第１のノード（Ｃ）を認証するために、第１のノードの第２の公開鍵（$Ｐ_{2\ C}$）を用いて有効性を確認することができる。

【００２３】

この方法は、また、通信ネットワークを介して、第２のノード（Ｓ）から第２の署名付きメッセージ（ＳＭ２）を受信することと、第２のノードの第２の公開鍵（$Ｐ_{2\ S}$）を用いて第２の署名付きメッセージ（ＳＭ２）の有効性を確認することと、第２の署名付きメッセージ（ＳＭ２）の有効性を確認した結果に基づいて、第２のノード（Ｓ）を認証することとを含み、第２の署名付きメッセージ（ＳＭ２）は、メッセージ（Ｍ）又は第２のメッセージ（Ｍ２）、及び第２のノードの第２の私有鍵（$Ｖ_{2\ S}$）に基づいて生成された。

【００２４】

この方法は、メッセージ（Ｍ）を生成することと、通信ネットワークを介して、メッセージ（Ｍ）を第２のノード（Ｓ）に送信することとを更に含んでいてもよい。それに代えて、この方法は、通信ネットワークを介して、第２のノード（Ｓ）からメッセージ（Ｍ）を受信することを含んでいてもよい。更に別の代替形態において、この方法は、通信ネットワークを介して、別のノードからメッセージ（Ｍ）を受信することを含んでいてもよい。更に別の代替形態では、この方法は、データストア及び／又は第１のノード（Ｃ）に関連付けられた入力インタフェースからメッセージ（Ｍ）を受信することを含んでいてもよい。

【００２５】

第１のノードのマスター公開鍵（$Ｐ_{1\ C}$）、第２のノードのマスター公開鍵（$Ｐ_{1\ S}$）は、それぞれの第１のノードのマスター私有鍵（$Ｖ_{1\ C}$）及び第２のノードのマスター私有鍵（$Ｖ_{1\ S}$）と発生器（Ｇ）との楕円曲線点乗算に基づいている。

【００２６】

この方法は、通信ネットワークを介して、第２のノードのマスター公開鍵（$Ｐ_{1\ S}$）を受信するステップと、第１のノード（Ｃ）に関連付けられたデータストアに、第２のノードのマスター公開鍵（$Ｐ_{1\ S}$）を記憶するステップとを更に含んでいてもよい。

【００２７】

本方法は、第１のノード（Ｃ）において、第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を作成するステップと、通信ネットワークを介して、第１のノードのマスター公開鍵（P_{1C}）を第２のノード（Ｓ）及び／又は他のノードに送信するステップと、第１のノード（Ｃ）に関連付けられた第１のデータストアに、第１のノードのマスター私有鍵（V_{1C}）を記憶するステップを更に含んでいてもよい。

【００２８】

ｋの方法は、また、通信ネットワークを介して、第２のノードに、共通秘密（ＣＳ）を決定する方法のためにベースポイント（Ｇ）と共に共通楕円曲線暗号（ＥＣＣ）システムを用いることを示す通知を送信することを含むことができる。第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を作成するステップは、共通ＥＣＣシステムにおいて指定される許容可能な範囲におけるランダムな整数に基づいて第１のノードのマスター私有鍵（V_{1C}）を作成することと、以下の式

$$P_{1C}=V_{1C}\times G$$

によって、第１のノードのマスター私有鍵（V_{1C}）とベースポイント（Ｇ）との楕円曲線点乗算に基づいて第１のノードのマスター公開鍵（P_{1C}）を決定することとを含むことができる。

【００２９】

この方法は、メッセージ（Ｍ）のハッシュの決定に基づいて発生器値（ＧＶ）を決定することを更に含むことができ、第１のノードの第２の私有鍵（V_{2C}）を決定するステップは、以下の式

$$V_{2C}=V_{1C}+GV$$

によって、第１のノードのマスター私有鍵（V_{1C}）及び発生器値（ＧＶ）のスカラー加算に基づいている。

【００３０】

第２のノードの第２の公開鍵（Ｐ２Ｓ）を決定するステップは、以下の式、

$$P_{2S}=P_{1S}+GV\times G$$

によって、第２のノードのマスター公開鍵（P_{1S}）であるが、に、発生器値（ＧＶ）とベースポイント（Ｇ）との楕円曲線点乗算に楕円曲線点加算した公開鍵に基づくことができる。

【００３１】

発生器値（ＧＶ）は、以前の発生器値（ＧＶ）のハッシュを決定することに基づくことができる。

【００３２】

第１の非対称暗号対及び第２の非対称暗号対は、それぞれの以前の第１の非対称暗号対及び以前の第２の非対称暗号対の関数に基づいている。

【００３３】

換言すれば、本発明は、

検証要素を複数のシェアに分割するステップと、

第１のノードにおいて、第１のマスター非対称鍵の対に基づいて導出された（又は第２の）私有暗号鍵を作成するステップと、

導出された私有鍵を、検証要素の少なくとも１つのシェアの暗号化及び／又はセキュアな送信のために用いるステップと、

を含む方法を提供することができる。

【００３４】

この方法は、第２のノードにおいて、同じ導出された私有鍵を作成するステップも含むことができ、これは第１のノードと独立して、第２のマスター非対称鍵の対を用いて作成される。

【００３５】

導出される私有鍵は、私有鍵及び公開鍵を含む非対称鍵対の一部とすることができる。

第１及び／又は第２のノードは、楕円曲線暗号（ＥＣＣ）を用いて私有鍵（及びその対応する公開鍵）を作成することができる。

【００３６】

本方法は、

・　第１のノードと第２のノードとの間で、ベースポイント（Ｇ）を用いて標準ＥＣＣシステムについて合意するステップ、及び／又は、

・　第１及び／又は第２のノードにおいて、合意された標準ＥＣＣシステムを用いて公開鍵／私有鍵対を作成し、公開鍵を公開するステップであって、これは公開鍵を公開で利用可能にすることを意味するステップ、及び／又は、

・　第１のノードのマスター公開鍵（P_{MC}）を第２のノード又は別の場所において登録し、及び／又は第２のノードのマスター公開鍵（P_{MC}）を第１のノード又は別の場所において登録するステップ、及び／又は、

・　第１のノードから第２のノードに、及び／又はその逆にメッセージ（Ｍ）を送信し、メッセージのハッシュを生成するステップであって、このメッセージは、導出された私有鍵を用いて署名を付けることができ、このステップは、１）ノード間の共有秘密を確立し、２）それらの間でセキュアにされた通信を開始するのに必要とされる送信のみを表すことができ、第１のノード又は第２のノードは、受信されたメッセージＭを用いて、独自の導出された（二次）公開／私有鍵対を作成し、これにより、ノードは他のノードの導出された公開鍵を計算することができるステップ、及び／又は、

・　このメッセージを受信し、メッセージＭ（例えば、ＳＨＡ－２５６（Ｍ））のハッシュを独立して計算するステップ、及び／又は、

・　マスター鍵（P_{MC}）から導出可能な公開鍵（P_{2C}）を計算するステップ、及び／又は、

・　計算されたP_{2C}に対し署名（$Sig-V_{2C}$）を検証するステップ、

を含むことができる。

【００３７】

導出された私有鍵は、第１のノード又は第２のノードのマスター公開鍵から決定論的に導出することができる。

【００３８】

本発明は、また、上記の方法の任意の実施形態を実施するように配置及び構成されたコンピュータ実施システム備えていてもよい。このシステムは、ブロックチェーンネットワーク又はプラットフォームを備えるか又は利用することができる。それに加えて、又はそれに代えて、システムは、デジタルウォレットプロバイダ又は管理システムを備えていてもよい。

【００３９】

本発明の１つの態様又は実施形態に関連して上記で説明された任意の特徴は、任意の他の態様又は実施形態に関連して用いることもできる。例えば、本方法に関連して説明された特徴は、システムに適用することができ、逆も同様である。

【００４０】

本発明のこれらの態様及び他の態様は、本明細書に記載の実施形態から明らかであり、実施形態を参照して説明される。

【００４１】

例示てきであるが、添付の図面を参照して本発明の実施形態を説明する。

【図面の簡単な説明】

【００４２】

【図１】私有鍵の共有の如き機密性の高い情報のセキュアな送信のために、本発明に従って用いることができる第１のノード及び第２のノードのための共通秘密を決定するための例示的なシステムの概略図である。

【図２】私有鍵の共有の如き機密性の高い情報のセキュアな送信のために、本発明に従って用いることができるような共通秘密を決定するためのコンピュータ実施方法のフローチ

ャートである。
【図３】第１のノード及び第２のノードを登録するためのコンピュータ実施方法のフローチャートである。
【図４】私有鍵のシェアの如き機密性の高い情報のセキュアな送信のために、本発明に従って用いることができる共通秘密を決定するためのコンピュータ実施方法の別のフローチャートである。
【図５】第１のノードと第２のノードとの間のセキュアな通信のコンピュータ実施方法のフローチャートである。
【発明を実施するための形態】
【００４３】
上記で説明したように、暗号鍵等の秘密、又は鍵を生成するのに用いることができる秘密の記憶及び／又は交換の向上が必要とされている。この秘密は、ウォレットニーモックのためのシード、又は他のセキュリティ関連項目とすることができる。本発明は、そのような解決策を提供する。１つの実施形態が理解の目的で以下に説明するが、この実施形態は、ブロックチェーン上で実施されるデジタルウォレットの状況を用いる。しかし、本発明はこのような実施に限定されることはなく、任意のコンピュータ実施ネットワーク又はシステムに関して実施することができる。
【００４４】
上記のように、公開鍵暗号は、デジタルウォレットとの関連でしばしば用いられる。エンドユーザ（「クライアント」又は単に「ユーザ」と称する）が自身の私有鍵を記憶する責任がある場合には、ユーザ又はユーザのハードウェアが利用不可能になるとき、これにより私有鍵が、このためウォレットの資金がアクセス不能になるため、問題が生じる場合がある。しかし、ウォレットプロバイダの側（「サーバー側」と称することができる）での鍵の記憶は、プロバイダ及びプロバイダのセキュリティメカニズムにおけるあるレベルの信頼を必要とする。このため、認可されていない者が取得することができないが、必要に応じて再生成することもできるような形で私有鍵を記憶する必要がある。「ユーザ」という用語は、人間のユーザであってもよいし、コンピュータ実施リソースであってもよい。
【００４５】
「シャミアの秘密分散法」（４Ｓ）として知られる１つの既知の暗号アルゴリズムは、秘密を一意の部分又はシェアに分割し、次いでこれらが異なる関係者に分散されることを教示している。その後、このシェアは、秘密を再構成するのに用いることができる。各個々のシェアは、１つ又は複数の他のシェアと組み合わされるまで単独では価値がなく、役に立たない。秘密を再構成するのに必要なシェアの数は、状況の必要性に応じて変動することができる。ある場合には、全てのシェアが必要とされる場合があるが、他の場合には、十分な数のみが必要とされる。これは、閾値方式として知られ、ここで、シェアのうちの任意のｋ個があれば、元の秘密を再構成するのに十分である。
【００４６】
この例示的な実施形態において、私有鍵又はニーモニックシードの如き秘密を複数の部分に分割するのに４Ｓが用いられる。この際、４Ｓは、一定の数の部分から鍵又はニーモニックシードを再作成するのにも用いられる。ニーモニックの使用は、デジタルウォレットと併せて既知である。ニーモニックは、ウォレット又はデータの作成のためにバイナリシードにすることができる、人間が使いやすいコード又は単語グループである。
【００４７】
本明細書において、以下の用語が用いられる。
・　「秘密」（Ｓ）は、関係者間でセキュアに共有される必要がある秘密（例えば、番号又は値）である。
・　「シェア」は、秘密の断片である。秘密は、断片に分割され、各断片がシェアと呼ばれる。シェアは所与の秘密から計算される。秘密を復元するには、一定の数のシェアを得る必要がある。

・　「閾値」（ｋ）は、秘密を再作成又は復元するのに必要なシェアの最小数である。秘密は、ｋ個以上のシェアを有するときにのみ再作成することができる。
・　「プライム（ｐｒｉｍｅ）」（ｐ）はランダムな素数である。

【００４８】

広い観点から、例示的な実施形態は、以下のような方法を含むことができる。この例において、「２－ｏｆ－３」方式を用いる（すなわち、ｋ＝２）。
・　ユーザは、ウォレットプロバイダに登録し、そのユーザに関連付けられた新たなウォレットを作成しセットアップする。この例では、ウォレットは、ブロックチェーンを利用するビットコインウォレットである。
・　公開鍵－私有鍵の対が作成され、ユーザのウォレットに関連付けられる。
・　私有鍵が、４Ｓを用いてシェアに分割される。
・　私有鍵の１つのシェアが、セキュアな送信によりユーザに送信される。
・　私有鍵の別のシェアが、サービスプロバイダによって保持され、サーバーに記憶される。
・　別のシェアは、セキュアな送信により、安全な記憶のために遠隔の場所に送信される。「遠隔」という用語は、特定の地理的距離又は場所を意味するものではない。そうではなく、本明細書では、シェアが、ウォレットプロバイダ又はユーザ、好ましいくは双方からある意味で独立したセキュアな記憶施設又はリソースにおいて（ｉｎ，　ａｔ　ｏｒ　ｏｎ）保持されることを意味する。「独立している」とは、物理的、論理的、財政的、政治的及び／又は組織的に独立していることを含む。例えば、安全な記憶は、料金と引き換えに安全な記憶サービスを提供する商用エンティティに外注することができるか、又はユーザの弁護士によって保持することができるか、又は、必要な場合に要求に応じてシェアを記憶し供給する役割を受け入れる他の選出された（かつ信頼される）関係者によって保持することができる。
・　ウォレットプロバイダは、完全な私有鍵のうちのいくつか又は全てのコピーを、それらがもはや必要ないことに起因して、破壊することができる。私有鍵がユーザの後続の認証に必要である場合（例えば、ユーザが次に取引を行うことを望んでいるため）、鍵は、ユーザが必要に応じてウォレットプロバイダに提供するユーザのシェアと、ウォレットプロバイダのシェアとから再構成することができる。

【００４９】

この利点は、ウォレットプロバイダのセキュリティが侵害されている場合であっても、認可されていない者がユーザの私有鍵に対するアクセスを得ることができないことである。なぜなら、私有鍵はウォレットプロバイダのシステムにおいてどこにも記憶されておらず、ウォレットプロバイダのシステム単独では私有鍵の再構成を可能にするのに十分なシェアを含まないためである。この同じ利点は、クライアントのセキュリティが侵害されている状況にも当てはまる。

【００５０】

別の利点は、安全な記憶場所にシェアを記憶することによって、安全な記憶からそのシェアを取り出し、これをウォレットプロバイダのシェアと組み合わせることにより、私有鍵を再構成することができることである。このため、ユーザが死亡するかもしくは行動不能になった場合、又はユーザのハードウェア（及びこのためシェア）がなくなるか、損傷を受けるか、又は盗まれた場合、ウォレット内の資金に依然としてアクセスすることができる。そのような状況において、ユーザのアイデンティティが検証される。いくつかの例において、遺産管理人又は弁護士の如き実績のある信頼された関係者のアイデンティティが実証される。これは、例として、死亡証明書、パスポート、法的文書又は他の形態の身分証明書等の証書の作成時に達成される。認可されたアイデンティティであることが検証されると、秘密のシェアが安全な記憶から取り出される。従って、安全な記憶は、例外的な、又は所定の環境において用いることができるある種のバックアップ施設として機能する。

【００５１】

従って、本発明は、向上したシステム／データセキュリティと利便性との有利な組み合わせを提供する。本発明は、アクセス制御の単純で効果的でセキュアな解決策を提供する。

【００５２】

上記の例において、私有鍵は、ウォレットサービスプロバイダによって作成され、それぞれのパーツがユーザ及び安全な記憶リソースに送信されることに留意されたい。しかし、これは他の実施形態には当てはまらない場合がある。「ノード」と称される関係者間のパーツの送信は、セキュアな方式で行われなくてはならないことに留意することも重要である。なぜなら、複数のシェアの任意の認可されていない傍受により、傍受者が秘密（例えば、ニーモニック又は鍵）を再構成することが可能になり得るためである。以下で説明されるように、このセキュアな交換の問題も、本発明によって対処される。

【００５３】

本発明の更なる詳細な態様を例示の目的で説明する。シャミアの秘密分散法は、当該技術分野において既知の技法であり、当業者であれば、これを認識し、理解し、用いることができることに留意するべきである。従って、以下は、完全性の目的のみで提供される。

【００５４】

複数のシェアへの秘密の分割

秘密Ｓ、参加者の数ｎ、閾値数ｋ、及び素数ｐとすると、定数項Ｓを用いて以下の多項式が構成される。

次数ｋ－１のｙ＝ｆ（ｘ）（プライムｐをモジュロ（法）とする）

【００５５】

次に、１とｐ－１との間（１及びｐ－１を含む）のｎ個の一意のランダムな整数を選択し、これらのｎ個の点において多項式を評価する。ｎ人の参加者の各々に（ｘ，ｙ）対が与えられる。これは、以下のステップにより達成することができる。

【００５６】

１．整数への変換

４Ｓアルゴリズムの場合、秘密は整数である必要がある。このため、秘密が何らかの他の形式（例えば、文字列、１６進数等）をとる場合、これは、まず整数に変換されなくてはならない。秘密がすでに整数である場合、このステップは省略することができる。この例の場合、Ｓ＝１２３４とする。

【００５７】

２．シェアの数（ｎ）及び閾値（ｋ）の決定

秘密を再作成するためにｋ個のパーツが必要とされることに留意されたい。このため、秘密を復元する間にｋ個のパーツを常に得ることができるようにＳ及びｋを選択する。この例の場合、ｎ＝６、ｋ＝３とする。

【００５８】

３．多項式の生成

形式ｙ＝ｆ（ｘ）ｍｏｄ　ｐの多項式を生成する必要がある。

ｉ．多項式の定数項及び次数の決定

$$f(x)=a_0+a_1x+a_2x^2+a_3x^3+\ldots+a_{k-1}x^{k-1}$$

－　定数項$a_0=S$

－　多項式の次数＝ｋ－１

【００５９】

このため、ｋ＝３及びＳ＝１２３４について、次数２及びa_0＝１２３４を有する多項式を構築する必要がある。

$$f(x)=1234+a_1x+a_1x^2$$

【００６０】

ｉｉ．係数の決定

以下となるようにｋ－１個の乱数（乱数（疑似乱数）発生器を用いる）を選択する。

$$0<a_n<S$$

a_1＝１６６；a_2＝９４とする。
このため、ｆ｛ｘ）＝１２３４＋１６６ｘ＋９４x^2である。
【００６１】
ｉｉｉ．ランダムな素数の選択
以下となるようにランダムな素数（ｐ）を選択する。
ｐ＞ｍａｘ（Ｓ，ｎ）
ｐ＝１６１３とする。
【００６２】
ｉｖ．最終的な多項式
ｙ＝ｆ（ｘ）ｍｏｄ　ｐ
ｙ＝（１２３４＋１６６ｘ＋９４x^2）ｍｏｄ　１６１３
【００６３】
シェアの作成
シナリオをｎ個のシェアに分割するために、多項式を用いてｎ個の点（シェア）を構成する必要がある。
ｙ＝（１２３４＋１６６ｘ＋９４x^2）ｍｏｄ　１６１３
【００６４】
この例について、ｎ＝６であるため、６つの点を有することになる。ｘ＝０ではなく、ｘ＝１で開始することに留意されたい。
【００６５】
ｘ＝１～６について、６つの点は以下のとおりである。
（１，１４９４）；（２，３２９）；（３，９６５）；（４，１７６）；（５，１１８８）；（６，７７５）
【００６６】
これらのｎ（６）個の点のうち、任意のｋ（３）個の点を用いて秘密鍵を再作成することができる。
【００６７】
所与の数のシェアからの秘密の再構成
ｉ．秘密の整数の取得
秘密を再構成するために、以下の情報を必要とする。
ｎ＝６、ｋ＝３、ｐ＝１６１３、
ｋ個のシェア
（ｘ０，ｙ０）＝（１，１４９４）；（ｘ１，ｙ１）＝（２，３２９）；（ｘ２，ｙ２）＝（３，９６５）
【００６８】
上記の情報を手に入れると、当該技術分野において既知であり、当業者には容易に理解されるラグランジュ補間等の技法を用いることができる。この技法を用いて、多項式全体を再構築することができる。係数は、以下の式に従って計算することができる。
$a_i(x)=[\Sigma^{k-1}_{i=0} y_i \Pi_{0\leq j\leq k-1,\ j\neq i}(x-x_j)/(x_i-x_j)]\ mod\ p$
しかし、Ｓ＝a_0であるため、$a_0=a_0(0)$を得るのみでよい。

$$a_0=\left[\sum_{i=0}^{k-1} y_i \prod_{0\leq j\leq k-1,\ j\neq i}\frac{-x_j}{x_i-x_j}\right] \bmod p$$

ここで、$x_i-x_j\neq 0$である。
【００６９】
当業者であれば、上記において、指数－１は逆数をとることを表すことを理解するであろう。ほとんどのプログラミング言語は、逆数等の数学演算を行う内蔵パッケージを含ん

でいる。

【００７０】

ｉｉ．所望の形式への整数の変換

特定の形式を整数に変換するためにステップ１が行われた場合、逆の手順を辿って、整数を所望の形式に戻す。

【００７１】

シェアのセキュアな送信

上述したように、認可されていない者が秘密を再構成できないようにするために、秘密のシェアがセキュアな方式でそれぞれの受信者に送信されることが重要である。好ましい実施形態では、セキュアな送信は、以下で説明されるように達成することができる。

【００７２】

２者の関係者間で共通秘密（ＣＳ）を確立することができ、次にこれを用いてシェアのうちの１つ又は複数を送信するためのセキュアな暗号化鍵を生成することができる。この共通秘密（ＣＳ）は、上記で参照した秘密（Ｓ）と混同されるべきでない。共通秘密（ＣＳ）は、秘密（Ｓ）、例えば鍵又はそのシェアのセキュアな交換を可能にするために作成され用いられる。

【００７３】

２者の関係者は、ウォレットサービスプロバイダ、ユーザ、安全な記憶リソース、又は何らかの他の正規の関係者のうちの任意の２つとすることができる。以後、便宜上、これらは第１のノード（Ｃ）、第２のノード（Ｓ）と称する。その目的は、双方のノードが知っている共通（ＣＳ）秘密を生成することであるが、その共通秘密は通信チャネルを介して送信されておらず、このため、認可されていない発見の可能性が排除される。秘密の分割及び安全な記憶の技法は、以下で説明されるような安全な送信技法と組み合わせて、セキュアな鍵管理解決法を提供する。

【００７４】

本発明のセキュアな送信技法は、各送信終了時にＣＳが独立した方式で生成されることを伴い、このため、双方のノードがＣＳを知っている一方で、ＣＳは、潜在的にセキュアでない通信チャネルを介して移送される必要がなかった。ＣＳが双方の終端で確立されると、ＣＳを用いてセキュアな暗号化鍵を生成することができ、この暗号化鍵は、双方のノードがその後の通信に用いることができる。これは、ある関係者から別の関係者への分割私有鍵の送信にとって、ウォレット登録プロセス中に特に利点を有する。

【００７５】

図１は、通信ネットワーク５を介して第２のノード７と通信する第１のノード３を備えるシステム１を示す。第１のノード３は、関連付けられた第１の処理デバイス２３を有し、第２のノード５は、関連付けられた第２の処理デバイス２７を有する。第１のノード３及び第２のノード７は、コンピュータ、電話、タブレットコンピュータ、モバイル通信デバイス、コンピュータサーバーの如き電子デバイスを含むことができる。１つの例において、第１のノード３は、クライアント（ユーザ）デバイスとすることができ、第２のノード７は、サーバーとすることができる。サーバーは、デジタルウォレットプロバイダのサーバーとすることができる。

【００７６】

第１のノード３は、第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を有する第１の非対称暗号対に関連付けられている。第２のノード（７）は、第２のノードのマスター私有鍵（V_{1S}）及び第２のノードのマスター公開鍵（P_{1S}）を有する第２の非対称暗号対に関連付けられている。換言すれば、第１のノード及び第２のノードは各々、それぞれの公開鍵－私有鍵対を保有している。

【００７７】

それぞれ第１のノード３及び第２のノード７のための第１及び第２の非対称暗号対は、ウォレットの登録の如き登録プロセス中に作成することができる。各ノードの公開鍵は、例えば通信ネットワーク５を介して、公開で共有することができる。

【００７８】
第１のノード３及び第２のノード７の双方において共通秘密（ＣＳ）を決定するために、ノード３、７は、通信ネットワーク５を介して私有鍵を通信することなく、それぞれのメソッド３００、４００のステップを行う。
【００７９】
第１のノード３によって行われるメソッド３００は、少なくとも、第１のノードのマスター私有鍵（V_{1C}）及び発生器値（ＧＶ）に基づいて、第１のノードの第２の私有鍵（V_{2C}）を決定すること（３３０）を含む。発生器値は、第１のノードと第２のノードとの間で共有されるメッセージ（Ｍ）に基づいている。これは、以下で更に詳細に説明するように、通信ネットワーク５を介してメッセージを共有することを含むことができる。メソッド３００は、少なくとも、第２のノードのマスター公開鍵（P_{1S}）及び発生器値（ＧＶ）に基づいて、第２のノードの第２の公開鍵（P_{2S}）を決定すること（３７０）も含む。メソッド３００は、第１のノードの第２の私有鍵（V_{2C}）及び第２のノードの第２の公開鍵（P_{2S}）に基づいて、共通秘密（ＣＳ）を決定すること（３８０）を含む。
【００８０】
重要なことであるが、同じ共通秘密（ＣＳ）を、メソッド４００によって第２のノード７において決定することもできる。メソッド４００は、第１のノードのマスター公開鍵（P_{1C}）及び発生器値（ＧＶ）に基づいて、第１のノードの第２の公開鍵（P_{2C}）を決定すること（４３０）を含む。メソッド４００は、第２のノードのマスター私有鍵（V_{1S}）及び発生器値（ＧＶ）に基づいて、第２のノードの第２の私有鍵（V_{2S}）を決定すること（４７０）を更に含む。メソッド４００は、第２のノードの第２の私有鍵（V_{2S}）及び第１のノードの第２の公開鍵（P_{2C}）に基づいて、共通秘密（ＣＳ）を決定すること（４８０）を含む。
【００８１】
通信ネットワーク５は、ローカルエリアネットワーク、広域ネットワーク、セルラーネットワーク、無線通信ネットワーク、インターネット等を含むことができる。電気配線、光ファイバーの如き通信媒体を介して、又は無線でデータを送信することができるこれらのネットワークは、盗聴者１１によって行われるような盗聴を受けやすい場合がある。メソッド３００、４００は、第１のノード３及び第２のノード７が共に、通信ネットワーク５を介して共通秘密を送信することなく共通秘密を独立して決定することを可能にする。
【００８２】
従って、１つの利点は、潜在的にセキュアでない通信ネットワーク５を介して私有鍵を送信する必要なく、各ノードによってセキュアにかつ独立して共通秘密（ＣＳ）を決定することができることである。一方、この共通秘密は、通信ネットワーク５を介して、第１のノード３と第２のノード７との間の暗号化された通信のための秘密鍵（又は秘密鍵の基礎）として用いることができる。
【００８３】
メソッド３００、４００は、追加のステップを含むことができる。メソッド３００は、第１のノード３において、メッセージ（Ｍ）及び第１のノードの第２の私有鍵（V_{2C}）に基づいて、署名付きメッセージ（ＳＭ１）を作成することを含むことができる。このメソッド３００は、通信ネットワークを介して、第２のノード７に第１の署名付きメッセージ（ＳＭ１）を送信すること（３６０）を更に含んでいる。一方、第２のノード７は、第１の署名付きメッセージ（ＳＭ１）を受信するステップ４４０を行うことができる。メソッド４００は、第１のノードの第２の公開鍵（P_{2C}）を用いて第１の署名付きメッセージ（ＳＭ２）の有効性を確認し（４５０）、第１の署名付きメッセージ（ＳＭ１）の有効性確認結果に基づいて第１のノード３を認証する（４６０）ステップも含んでいる。有利には、これによって、第２のノード７が、（第１の署名付きメッセージが作成された）第１のノードとされているノードが第１のノード３であることを認証することが可能になる。これは、第１のノード３のみが第１のノードのマスター私有鍵（V_{1C}）へのアクセスを有し、従って、第１のノード３のみが第１の署名付きメッセージ（ＳＭ１）を作成する

ための第１のノードの第２の私有鍵（V_{2C}）を決定することができるという仮定に基づいている。同様に、第２の署名付きメッセージ（ＳＭ２）を第２のノード７において作成し、第１のノード３に送信することができ、それによって、ピアツーピアのシナリオの如くして、第１のノード３が第２のノード７を認証することができることが理解されよう。

【００８４】

第１のノードと第２のノードとの間でのメッセージ（Ｍ）の共有は、種々の方法で達成することができる。１つの例において、メッセージは、第１のノード３において作成することができ、このメッセージは、次に、通信ネットワーク５を介して、第２のノード７に送信される。それに代えて、メッセージは、第２のノード７において作成され、次いで、通信ネットワーク５を介して第２のノード７に送信してもよい。更に別の例では、メッセージは、第３のノード９において生成され、このメッセージが第１のノード３及び第２のノード７の双方に送信されてもよい。更に別の代替形態では、ユーザは、ユーザインタフェース１５を通して、第１のノード３及び第２のノード７によって受信されるメッセージを入力してもよい。更に別の例では、メッセージ（Ｍ）は、データストア１９から取り出され、第１のノード３及び第２のノード７に送信されてもよい。いくつかの例では、メッセージ（Ｍ）は公開であってもよく、従って、セキュアでないネットワーク５を介して送信してもよい。

【００８５】

更なる例では、１つ又は複数のメッセージ（Ｍ）を、データストア１３、１７、１９に記憶することができ、これらのデータストアにおいて、メッセージは、デジタルウォレット如き何らかのエンティティ、又は第１のノード３と第２のノード７との間で確立される通信セッションと関連付けることができる。このため、メッセージ（Ｍ）を取り出し、それぞれ第１のノード３及び第２のノード７において、そのウォレット又はセッションに関連付けられた共通秘密（ＣＳ）を再現するのに用いることができる。

【００８６】

有利には、共通秘密（ＣＳ）の再現を可能にするレコードは、レコード自体がプライベートに記憶されるか又はセキュアに送信される必要なく保持することができる。これは、第１のノード３及び第２のノード７において多数のトランザクションが行われ、全てのメッセージ（Ｍ）をノード自体に記憶することが実際的でない場合に有利である。

【００８７】

登録メソッド１００、２００

登録メソッド１００、２００の例を、図３を参照して説明すると、メソッド１００は、第１のノード３によって行われ、メソッド２００は、第２のノード７によって行われる。これは、それぞれ第１のノード３及び第２のノード７について第１及び第２の非対称暗号対を確立することを含んでいる。

【００８８】

非対称暗号対は、公開鍵暗号化において用いられるような、関連付けられた私有鍵及び公開鍵を含んでいる。この例において、非対称暗号対は、楕円曲線暗号（ＥＣＣ）及び楕円曲線演算の特性を用いて作成される。

【００８９】

ＥＣＣ用の規格は、ＳＥＣＧ（Ｓｔａｎｄａｒｄｓ ｆｏｒ Ｅｆｆｉｃｉｅｎｔ Ｃｒｙｐｔｏｇｒａｐｈｙ Ｇｒｏｕｐ）（ｗｍｖ．ｓｃｅｇ．ｏｒｇ）によって記載されているような既知の規格を含むことができる。楕円曲線暗号については、米国特許第５，６００，７２５号、米国特許第５，７６１，３０５号、米国特許第５，８８９，８６５号、米国特許第５，８９６，４５５号、米国特許第５，９３３，５０４号、米国特許第６，１２２，７３６号、米国特許第６，１４１，４２０号、米国特許第６，６１８，４８３号、米国特許第６，７０４，８７０号、米国特許第６，７８５，８１３号、米国特許第６，０７８，６６７号、米国特許第６，７９２，５３０号にも記載されている。

【００９０】

メソッド１００、２００において、これは、第１及び第２のノードが共通ＥＣＣシステ

ムについて合意し、ベースポイント（Ｇ）を用いること（１１０、２１０）を含んでる。（注：ベースポイントは、共通発生器と称されるが、発生器値ＧＶとの混同を避けるために「ベースポイント」という用語が用いられる。）１つの例において、共通ＥＣＣシステムは、ビットコインによって用いられるＥＣＣシステムであるｓｅｃｐ２５６Ｋｌに基づくことができる。ベースポイント（Ｇ）は、選択されるか、ランダムに作成されるか、又は割り当てられる。

【００９１】

第１のノード３の説明に戻すと、メソッド１００は、共通ＥＣＣシステムとベースポイント（Ｇ）について確定すること（１１０）を含んでいる。これは、第２のノード７又は第３のノード９から、共通ＥＣＣシステムとベースポイントを受信することを含むことができる。それに代えて、ユーザインタフェース１５は、第１のノード３に関連付けられてもよく、これによって、ユーザは、共通ＥＣＣシステム及び／又はベースポイント（Ｇ）を選択的に提供することができる。更に別の代替形態では、共通ＥＣＣシステム及び／又はベースポイント（Ｇ）の一方又は双方が、第１のノード３によってランダムに選択されてもよい。第１のノード３は、通信ネットワーク５を介して、ベースポイント（Ｇ）と共に共通ＥＣＣシステムを用いることを示す通知を第２のノード７に送信することができる。そして、第２のノード７は、確認応答を示す通知を送信することによって、共通ＥＣＣシステム及びベースポイント（Ｇ）を用いることについて確定する（２１０）ことができる。

【００９２】

メソッド１００は、第１のノード３が第１のノードのマスター私有鍵（V_{1C}）と第１のノードのマスター公開鍵（P_{1C}）を含む第１の非対称暗号対を作成すること（１２０）も含んでいる。これは、少なくとも部分的に、共通ＥＣＣシステムにおいて指定される許容可能な範囲におけるランダムな整数に基づいて第１のノードのマスター私有鍵（V_{1C}）を作成することを含んでいる。これは、以下の式

$$P_{1C}=V_{1C}\times G \quad （式１）$$

による、第１のノードのマスター私有鍵（V_{1C}）とベースポイント（Ｇ）との楕円曲線点乗算に基づいて第１のノードのマスター公開鍵（P_{1C}）を決定することも含んでいる。

【００９３】

従って、第１の非対称暗号対は以下を含んでいる。

V_{1C}：第１のノードによって秘密にされている第１のノードのマスター私有鍵。

P_{1C}：公開で知られている第１のノードのマスター公開鍵。

【００９４】

第１のノード３は、第１のノード３に関連付けられた第１のデータストア１３に第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を記憶することができる。セキュリティのために、第１のノードのマスター私有鍵（V_{1C}）は、第１のデータストア１３のセキュアな部分に記憶され、鍵がプライベートなままであることを確実にすることができる。

【００９５】

メソッド１００は、第１のノードのマスター公開鍵（P_{1C}）を、通信ネットワーク５を介して第２のノード７に送信すること（１３０）を更に含んでいる。第２のノード７は、第１のノードのマスター公開鍵（P_{1C}）を受信する際（２２０）、第１のノードのマスター公開鍵（P_{1C}）を、第２のノード７に関連付けられた第２のデータストア１７に記憶する（２３０）ことができる。

【００９６】

第１のノード３と同様に、第２のノード７のメソッド２００は、第２のノードのマスター私有鍵（V_{1S}）及び第２のノードのマスター公開鍵（P_{1S}）を含む第２の非対称暗号対を作成すること（２４０）を含んでいる。第２のノードのマスター私有鍵（V_{1S}）は、許容可能な範囲内のランダムな整数でもある。一方、第２のノードのマスター公開鍵

（P_{1S}）は、以下の式によって決定される。

$$P_{1S}=V_{1S}\times G \quad （式２）$$

【００９７】

従って、第２の非対称暗号対は、以下を含んでいる。

V_{1S}：第２のノードによって秘密にされている第２のノードのマスター私有鍵。

P_{1S}：公開で知られている第２のノードのマスター公開鍵。

【００９８】

第２のノード７は、第２のデータストア１７に第２の非対称暗号対を記憶することができる。メソッド２００は、第２のノードのマスター公開鍵（P_{1S}）を第１のノード３に送信すること（２５０）を更に含んでいる。一方、第１のノード３は、第２のノードのマスター公開鍵（P_{1S}）を受信し（１４０）、記憶する（１５０）ことができる。

【００９９】

いくつかの代替形態において、それぞれの公開マスター鍵を受信して第３のノード９（信頼された第三者等）に関連付けられた第３のデータストア１９に記憶してもよいことが理解されよう。これは、認証局の如き公開ディレクトリとしての役割を果たす第三者を含んでいてもよい。従って、いくつかの例では、第１のノードのマスター公開鍵（P_{1C}）は、共通秘密（ＣＳ）を決定することが必要とされているときにのみ第２のノード７によって要求及び受信される場合がある（逆もまた同様）。

【０１００】

登録ステップは、例えばデジタルウォレットの初期セットアップとして一度のみ行われればよい。

【０１０１】

第１のノード３によるセッション開始及び共通秘密の決定

ここで、図４を参照して、共通秘密（ＣＳ）を決定する例を説明する。共通秘密（ＣＳ）は、第１のノード３と第２のノード７との間の特定のセッション、時間、トランザクション、又は他の目的のために用いられる場合があり、同じ共通秘密（ＣＳ）を用いることは、望ましくないか、又はセキュアでない場合がある。このため、異なるセッション、時間、トランザクション等の間で共通秘密（ＣＳ）を変更することができる。

【０１０２】

以下の説明は、上記したセキュアな送信技法の例示のために提供される。

【０１０３】

メッセージ（Ｍ）の作成３１０

この例において、第１のノード３によって行われるメソッド３００は、メッセージ（Ｍ）を作成すること（３１０）を含んでいる。メッセージ（Ｍ）は、ランダムであるか、疑似ランダムであるか、又はユーザにより定義されてもよい。１つの例では、メッセージ（Ｍ）は、Ｕｎｉｘ時間及びノンス（及び任意の値）に基づいている。例えば、メッセージ（Ｍ）は、以下のように提供することができる。

$$メッセージ（M）＝UnixTime＋ノンス \quad （式３）$$

【０１０４】

いくつかの例において、メッセージ（Ｍ）は任意である。しかし、このメッセージ（Ｍ）は、いくつかの用途において有用であり得る選択的値（Ｕｎｉｘ時間等）を有していてもよいことが理解されよう。

【０１０５】

メソッド３００は、通信ネットワーク３を介して第２のノード７にメッセージ（Ｍ）を送信すること（３１５）を含んでいる。このメッセージ（Ｍ）は、私有鍵に関する情報を含んでいないので、セキュアでないネットワークを介して送信することができる。

【０１０６】

発生器値（ＧＶ）３２０の決定

メソッド３００は、メッセージ（Ｍ）に基づいて発生器値（ＧＶ）を決定するステップ３２０を更に含んでいる。この例において、これは、メッセージの暗号学的ハッシュを決

定することを含んでいる。暗号学的ハッシュアルゴリズムの例は、２５６ビット発生器値（ＧＶ）を生成するためのＳＨＡ－２５６を含む。すなわち、以下の通りとなる。

ＧＶ＝ＳＨＡ－２５６（Ｍ）　（式４）

【０１０７】

他のハッシュアルゴリズムを用いてもよいことが理解されよう。これは、セキュアハッシュアルゴリズム（ＳＨＡ）ファミリーにおける他のハッシュアルゴリズムを含むことができる。いくつかの特定の例は、ＳＨＡ３－２２４、ＳＨＡ３－２５６、ＳＨＡ３－３８４、ＳＨＡ３－５１２、ＳＨＡＫＥ１２８、ＳＨＡＫＥ２５６を含む、ＳＨＡ－３サブセットにおけるインスタンスを含んでいる。他のハッシュアルゴリズムは、ＲＡＣＥ完全性プリミティブ評価メッセージダイジェスト（ＲＩＰＥＭＤ）ファミリーにおけるハッシュアルゴリズムを含むことができる。特定の例は、ＲＩＰＥＭＤ－１６０を含むことができる。他のハッシュ関数は、Ｚｅｍｏｒ－Ｔｉｌｌｉｃｈハッシュ関数及びナップサックベースのハッシュ関数に基づくファミリーを含むことができる。

【０１０８】

第１のノードの第２の私有鍵の決定３３０

更に、メソッド３００は、第２のノードのマスター私有鍵（V_{1C}）及び発生器値（ＧＶ）に基づいて第１のノードの第２の私有鍵（V_{2C}）を決定するステップ３３０を含んでいる。これは、以下の式

$$V_{2C}=V_{1C}+GV \quad （式５）$$

による、第１のノードのマスター私有鍵（V_{1C}）と発生器値（ＧＶ）とのスカラー加算に基づくことができる。

【０１０９】

このため、第１のノードの第２の私有鍵（V_{2C}）は、ランダムな値ではなく、代わりに、第１のノードのマスター私有鍵から決定論的に導出される。暗号対における対応する公開鍵、すなわち、第１のノードの第２の公開鍵（P_{2C}）は、以下の関係を有する。

$$P_{2C}=V_{2C}\times G \quad （式６）$$

【０１１０】

式５からのV_{2C}を式６に代入することにより、以下が得られる。

$$P_{2C}=(V_{1C}+GV)\times G \quad （式７）$$

ここで、「＋」演算子は楕円曲線点加算を意味する。楕円曲線暗号代数が分配的であることに留意すると、式７は、以下のように表すことができる。

$$P_{2C}=V_{1C}\times G+GV\times G \quad （式８）$$

【０１１１】

最後に、式１を式７に代入し、以下を得ることができる。

$$P_{2C}=P_{1C}+GV\times G \quad （式９．１）$$

$$P_{2C}=P_{1C}+SHA-256(M)\times G \quad （式９．２）$$

【０１１２】

従って、対応する第１のノードの第２の公開鍵（P_{2C}）は、第１のノードのマスター公開鍵（P_{1C}）及びメッセージ（Ｍ）の知識を与えられると導出可能とすることができる。メソッド４００に関して以下で更に詳細に述べられているように、第２のノード７は、そのような知識を有して、第１のノードの第２の公開鍵（P_{2C}）を独立して決定することができる。

【０１１３】

メッセージ及び第１のノードの第２の私有鍵に基づく第１の署名付きメッセージ（ＳＭ１）の生成３５０

メソッド３００は、メッセージ（Ｍ）及び決定された第１のノードの第２の私有鍵（V_{2C}）に基づいて、第１の署名付きメッセージ（ＳＭ１）を作成すること（３５０）を更に含んでいる。署名付きメッセージを作成することは、デジタル署名アルゴリズムを適用して、メッセージ（Ｍ）にデジタル署名することを含む。１つの例において、これは、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）において第１のノードの第２の私有鍵（

V_{2C}）をメッセージに適用して、第１の署名付きメッセージ（ＳＭ１）を得ることを含んでいる。

【０１１４】

ＥＣＤＳＡの例は、ｓｅｃｐ２５６ｋｌ、ｓｅｃｐ２５６ｒｌ、ｓｅｃｐ３８４ｒｌ、ｓｅ３ｃｐ５２１ｒｌを有するＥＣＣシステムに基づくものを含む。

【０１１５】

第１の署名付きメッセージ（ＳＭ１）は、第２のノード７において、対応する第１のノードの第２の公開鍵（P_{2C}）を用いて検証することができる。第１の署名付きメッセージ（ＳＭ１）のこの検証は、第２のノード７によって、第１のノード３を認証するのに用いることができる。これについては、メソッド４００において以下に述べる。

【０１１６】

第２のノードの第２の公開鍵の決定３７０’

更に、第１のノード３は、第２のノードの第２の公開鍵（P_{2S}）を決定することができる（３７０）。上記したように、第２のノードの第２の公開鍵（P_{2S}）は、少なくとも、第２のノードのマスター公開鍵（P_{1S}）及び発生器値（ＧＶ）に基づくことができる。この例において、公開鍵は、ベースポイント（Ｇ）との楕円曲線点乗算により私有鍵として決定されるので（３７０’）、第２のノードの第２の公開鍵（P_{2S}）は、式６と同様の方式で、以下のように表すことができる。

$$P_{2S}=V_{2S}\times G \quad \text{（式１０．１）}$$

$$P_{2S}=P_{1S}+GV\times G \quad \text{（式１０．２）}$$

【０１１７】

式１０．２の数学的証明は、第１のノードの第２の公開鍵（P_{2C}）について式９．１を導出するために上記で説明したのと同じである。第１のノード３は、第２のノード７と独立して第２のノードの第２の公開鍵を決定する（３７０）ことができることが理解されよう。

【０１１８】

第１のノード３における共通秘密の決定３８０

更に、第１のノード３は、決定された第１のノードの第２の私有鍵（V_{2C}）及び決定された第２のノードの第２の公開鍵（P_{2S}）に基づいて共通秘密（ＣＳ）を決定する（３８０）ことができる。この共通秘密（ＣＳ）は、第１のノード３によって、以下の式により決定することができる。

$$S=V_{2C}\times P_{2S} \quad \text{（式１１）}$$

【０１１９】

第２のノード７において行われるメソッド４００

ここで、第２のノード７において行われる対応するメソッド４００を説明する。これらのステップのうちのいくつかは、第１のノード３によって行われた上記で述べたステップと類似していることが理解されよう。

【０１２０】

メソッド４００は、通信ネットワーク５を介して、第１のノード３からメッセージ（Ｍ）を受信すること（４１０）を含んでいる。これは、ステップ３１５において第１のノード３によって送信されたメッセージ（Ｍ）を含むことができる。次に、第２のノード７は、メッセージ（Ｍ）に基づいて発生器値（ＧＶ）を決定する（４２０）。第２のノード７によって発生器値（ＧＶ）を決定するステップ４２０は、上記で説明した第１のノードによって行われるステップ３２０と類似している。この例では、第２のノード７は、この決定するステップ４２０を、第１のノード３と独立して行う。

【０１２１】

次のステップは、第１のノードのマスター公開鍵（P_{1C}）及び発生器値（ＧＶ）に基づいて第１のノードの第２の公開鍵（P_{2C}）を決定すること（４３０）を含む。この例において、公開鍵は、ベースポイント（Ｇ）との楕円曲線点乗算により私有鍵として決定されるので（４３０’）、第１のノードの第２の公開鍵（P_{2C}）は、式９と同様の方式

で、以下のように表すことができる。

$P_{2C}=V_{2C}\times G$　（式１２．１）

$P_{2C}=P_{1C}+GV\times G$　（式１２．２）

【０１２２】

式１２．１及び式１２．２の数学的証明は、式１０．１及び式１０．２について上記で説明されたのと同じである。

【０１２３】

第２のノード７による第１のノード３の認証

メソッド４００は、第２のノード７によって、推定の（alleged）第１のノード３が第１のノード３であることを認証することによって行われるステップを含むことができる。上記で述べたように、これは、第１のノード３から第１の署名付きメッセージ（ＳＭ１）を受信すること（４４０）を含む。次に、第２のノード７は、ステップ４３０において決定された第１のノードの第２の公開鍵（P_{2C}）を用いて、第１の署名付きメッセージ（ＳＭ１）における署名の有効性を確認する（４５０）ことができる。

【０１２４】

上記したように、デジタル署名の検証は、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）に従って行うことができる。重要なことであるが、第１のノードの第２の私有鍵（V_{2C}）で署名された第１の署名付きメッセージ（ＳＭ１）は、対応する第１のノードの第２の公開鍵（P_{2C}）によってのみ正しく検証されるべきである。なぜなら、V_{2C}及びP_{2C}は暗号対を形成するためである。これらの鍵は、第１のノード３の登録時に生成された第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）に対し決定性であるので、第１の署名付きメッセージ（ＳＭ１）を検証することは、第１の署名付きメッセージ（ＳＭ１）を送信する推定の第１のノードが登録中に同じ第１のノード３であることを認証する基礎として用いることができる。このため、第２のノード７は、第１の署名付きメッセージの有効性を確認した（４５０）結果に基づいて、第１のノード３を認証するステップ（４６０）を更に行うことができる。

【０１２５】

上記の認証は、２つのノードのうちの一方が信頼されるノードであり、ノードのうちの一方のみが認証される必要があるシナリオに好適である。例えば、第１のノード３は、クライアントであり、第２のノード７は、ウォレットプロバイダ等のクライアントによって信頼されているサーバーであってもよい。従って、サーバー（第２のノード７）は、サーバーシステムへのクライアントアクセスを許可するために、クライアント（第１のノード３）の信用証明書を認証する必要がある場合がある。サーバーがクライアントに対しサーバーの信用証明書を認証する必要がない場合がある。しかし、いくつかのシナリオでは、ピアツーピアシナリオにおけるように、双方のノードが互いに対し認証されることが望ましい場合がある。

【０１２６】

第２のノード７による共通秘密の決定

メソッド４００は、第２のノード７が、第２のノードのマスター私有鍵（V_{1S}）及び発生器値（ＧＶ）に基づいて第２のノードの第２の私有鍵（V_{2S}）を決定すること（４７０）を更に含むことができる。第１のノード３によって行われるステップ３３０と同様に、第２のノードの第２の私有鍵（V_{2S}）は、以下の式

$V_{2S}=V_{1S}+GV$　（式１３．１）

$V_{2S}=V_{1S}+SHA-256(M)$　（式１３．２）

による第２のノードのマスター私有鍵（V_{1S}）と発生器値（ＧＶ）とのスカラー加算に基づくことができる。

【０１２７】

更に、第２のノード７は、第１のノード３と独立して、以下の式に基づいて、第２のノードの第２の私有鍵（V_{2S}）及び第１のノードの第２の公開鍵（P_{2C}）に基づいて共通秘密（ＣＳ）を決定することができる（４８０）。

$S = V_{2S} \times P_{2C}$ （式１４）

【０１２８】

第１のノード３及び第２のノード７によって決定される共通秘密（ＣＳ）の証明

第１のノード３によって決定される共通秘密（ＣＳ）は、第２のノード７において決定される共通秘密（ＣＳ）と同じである。ここで、式１１及び式１４が同じ共通秘密（ＣＳ）をもたらすことの数学的証明を説明する。

【０１２９】

第１のノード３によって決定される共通秘密（ＣＳ）に説明を戻すと、式１０．１は、以下のように式１１に代入することができる。

$S = V_{2C} \times P_{2S}$ （式１１）

$S = V_{2C} \times (V_{2S} \times G)$

$S = (V_{2C} \times V_{2S}) \times G$ （式１５）

【０１３０】

第２のノード７によって決定される共通秘密（ＣＳ）に説明を戻すと、式１２．１は、以下のように式１４に代入することができる。

$S = V_{2S} \times P_{2C}$ （式１４）

$S = V_{2S} \times (V_{2C} \times G)$

$S = (V_{2S} \times V_{2C}) \times G$ （式１６）

【０１３１】

ＥＣＣ代数は交換可能であるため、式１５及び式１６は等価である。従って、以下の式が成り立つ。

$S = (V_{2C} \times V_{2S}) \times G = (V_{2S} \times V_{2C}) \times G$ （式１７）

【０１３２】

共通秘密（ＣＳ）及び秘密鍵

共通秘密（ＣＳ）は、第１のノード３と第２のノード７との間のソース通信のための対称鍵アルゴリズムにおける秘密鍵として、又は秘密鍵の基礎として用いることができる。この通信は、私有鍵の一部、私有鍵の表現もしくは識別子、又は私有鍵のニーモニックを伝達するために用いることができる。従って、本発明が、例えば、デジタルウォレット又は他の制御されたリソースのセットアップ中に用いられると、その後、関係者間のセキュアな通信を行うことができる。

【０１３３】

共通秘密（ＣＳ）は、楕円曲線点（ｘｓ，ｙｓ）の形態をとることができる。これは、ノード３、７によって合意された標準的な公開で既知の演算を用いて標準的な鍵形式に変換することができる。例えば、ｘｓ値は、AES_{256}暗号化のための鍵として用いることができる２５６ビットの整数とすることができる。これは、この長さの鍵を必要とする任意の用途について、ＲＩＰＥＭＤ１６０を用いて１６０ビットの整数に変換することもできる。

【０１３４】

共通秘密（ＣＳ）は、要求に応じて決定することができる。重要なことであるが、第１のノード３は、共通秘密（ＣＳ）を記憶する必要がない。なぜなら、これはメッセージ（Ｍ）に基づいて再決定することができるためである。いくつかの例では、用いられるメッセージ（Ｍ）は、マスター私有鍵に必要とされるのと同じレベルのセキュリティを有することなく、データストア１３、１７、１９（又は他のデータストア）に記憶することができる。いくつかの例では、メッセージ（Ｍ）は、公開で入手可能である場合がある。

【０１３５】

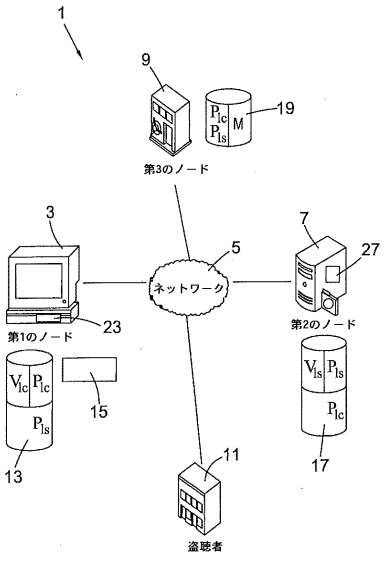
しかし、用途によっては、共通秘密（ＣＳ）が第１のノードのマスター私有鍵（V_{1C}）としてセキュアに保持されている限り、共通秘密（ＣＳ）は、第１のノードに関連付けられた第１のデータストア（Ｘ）に記憶され得る。

【０１３６】

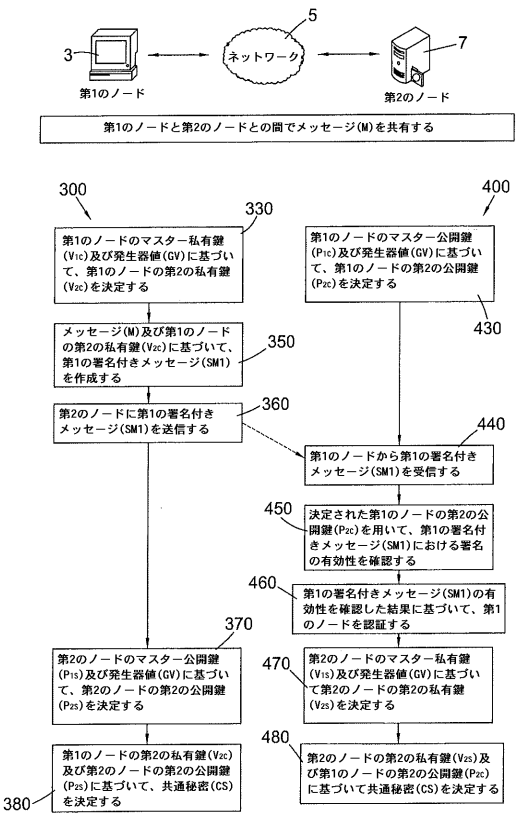
上述した実施形態は、本発明を限定するのではなく、当業者は、添付の特許請求の範囲

によって定義されるような本発明の範囲から逸脱することなく、任意の代替的な実施形態を設計することが可能であることに留意されたい。特許請求の範囲において、括弧に入れられた任意の参照符号は、特許請求の範囲を限定するものとみなされない。「備える」等の語は、任意の請求項又は明細書に全体として列挙されるもの以外の要素又はステップの存在を除外しない。本明細書において、「備える」は「含んでいる」又は「からなる」を意味する。要素の単数の参照は、そのような要素の複数の参照を除外するものではなく、逆もまた同様である。本発明は、いくつかの別個の要素を備えるハードウェア及び適切にプログラムされたコンピュータによって実施することができる。いくつかの手段を列挙しているデバイス請求項において、これらの手段のうちのいくつかは、同一のハードウェアによって具現化することができる。単に、いくつかの手段が互いに異なる独立請求項に挙げられていることは、これらの手段の組み合わせを有利に用いることができないことを示すものではない。

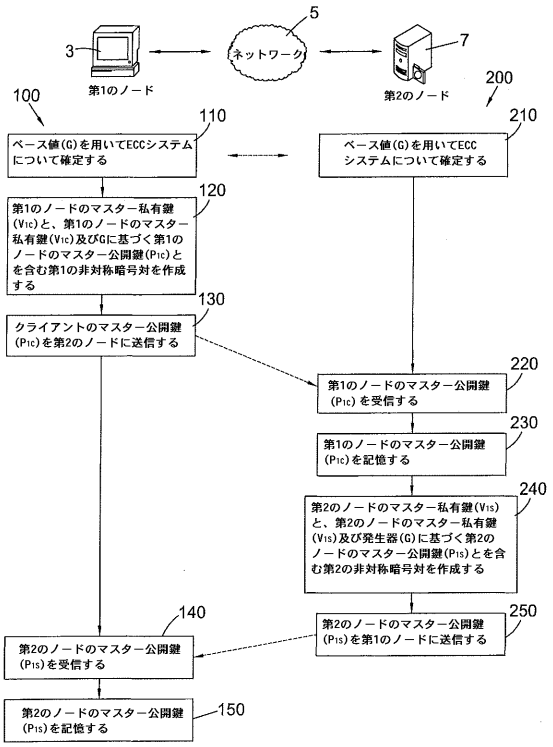
【図１】



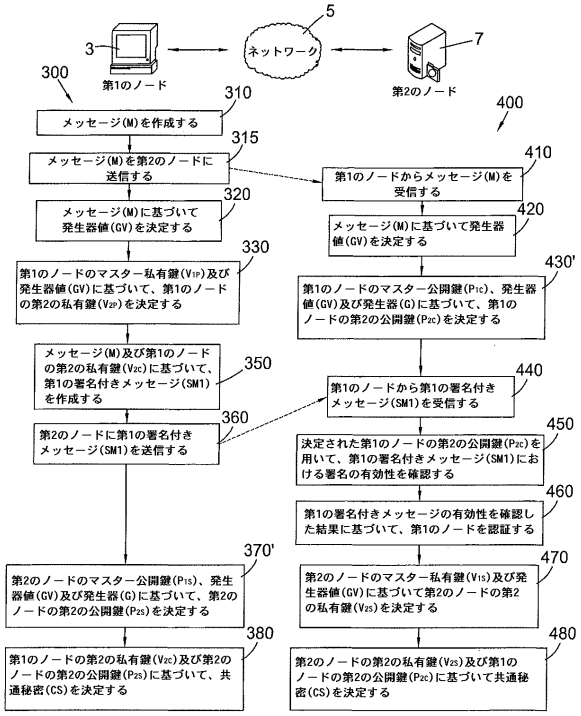
【図２】



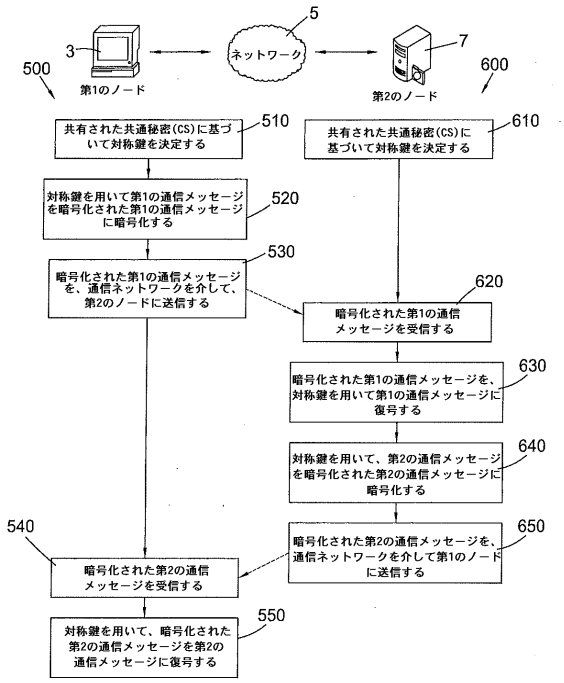
【図３】


3
第1のノード
5
ネットワーク
7
第2のノード
100
200
110
ベース値(G)を用いてECCシステムについて確定する
210
ベース値(G)を用いてECCシステムについて確定する
120
第1のノードのマスター私有鍵(V1C)と、第1のノードのマスター私有鍵(V1C)及びGに基づく第1のノードのマスター公開鍵(P1C)とを含む第1の非対称暗号対を作成する
130
クライアントのマスター公開鍵(P1C)を第2のノードに送信する
220
第1のノードのマスター公開鍵(P1C)を受信する
230
第1のノードのマスター公開鍵(P1C)を記憶する
240
第2のノードのマスター私有鍵(V1S)と、第2のノードのマスター私有鍵(V1S)及び発生器(G)に基づく第2のノードのマスター公開鍵(P1S)とを含む第2の非対称暗号対を作成する
250
第2のノードのマスター公開鍵(P1S)を第1のノードに送信する
140
第2のノードのマスター公開鍵(P1S)を受信する
150
第2のノードのマスター公開鍵(P1S)を記憶する

【図４】


3
第1のノード
5
ネットワーク
7
第2のノード
300
400
310
メッセージ(M)を作成する
315
メッセージ(M)を第2のノードに送信する
410
第1のノードからメッセージ(M)を受信する
320
メッセージ(M)に基づいて発生器値(GV)を決定する
420
メッセージ(M)に基づいて発生器値(GV)を決定する
330
第1のノードのマスター私有鍵(V1P)及び発生器値(GV)に基づいて、第1のノードの第2の私有鍵(V2P)を決定する
430'
第1のノードのマスター公開鍵(P1C)、発生器値(GV)及び発生器(G)に基づいて、第1のノードの第2の公開鍵(P2C)を決定する
350
メッセージ(M)及び第1のノードの第2の私有鍵(V2C)に基づいて、第1の署名付きメッセージ(SM1)を作成する
440
第1のノードから第1の署名付きメッセージ(SM1)を受信する
360
第2のノードに第1の署名付きメッセージ(SM1)を送信する
450
決定された第1のノードの第2の公開鍵(P2C)を用いて、第1の署名付きメッセージ(SM1)における署名の有効性を確認する
460
第1の署名付きメッセージの有効性を確認した結果に基づいて、第1のノードを認証する
370'
第2のノードのマスター公開鍵(P1S)、発生器値(GV)及び発生器(G)に基づいて、第2のノードの第2の公開鍵(P2S)を決定する
470
第2のノードのマスター私有鍵(V1S)及び発生器値(GV)に基づいて第2のノードの第2の私有鍵(V2S)を決定する
380
第1のノードの第2の私有鍵(V2C)及び第2のノードの第2の公開鍵(P2S)に基づいて、共通秘密(CS)を決定する
480
第2のノードの第2の私有鍵(V2S)及び第1のノードの第2の公開鍵(P2C)に基づいて共通秘密(CS)を決定する

【図５】


3
第1のノード
5
ネットワーク
7
第2のノード
500
600
510
共有された共通秘密(CS)に基づいて対称鍵を決定する
610
共有された共通秘密(CS)に基づいて対称鍵を決定する
520
対称鍵を用いて第1の通信メッセージを暗号化された第1の通信メッセージに暗号化する
530
暗号化された第1の通信メッセージを、通信ネットワークを介して、第2のノードに送信する
620
暗号化された第1の通信メッセージを受信する
630
暗号化された第1の通信メッセージを、対称鍵を用いて第1の通信メッセージに復号する
640
対称鍵を用いて、第2の通信メッセージを暗号化された第2の通信メッセージに暗号化する
540
650
暗号化された第2の通信メッセージを、通信ネットワークを介して第1のノードに送信する
暗号化された第2の通信メッセージを受信する
550
対称鍵を用いて、暗号化された第2の通信メッセージを第2の通信メッセージに復号する

フロントページの続き

(31)優先権主張番号 1619301.3
(32)優先日 平成28年11月15日(2016.11.15)
(33)優先権主張国・地域又は機関
英国(GB)

(74)代理人 100070150
弁理士 伊東 忠彦
(74)代理人 100091214
弁理士 大貫 進介
(72)発明者 クレイグ ステヴァン ライト
英国、 ＣＦ１０ ２ＨＨ カーディフ、 チャーチル ウェイ、 チャーチル ハウス ７階、 アークハート－ダイクス アンド ロード エルエルピー内
(72)発明者 ステファン サヴァナー
英国、 ＣＦ１０ ２ＨＨ カーディフ、 チャーチル ウェイ、 チャーチル ハウス ７階、 アークハート－ダイクス アンド ロード エルエルピー内

審査官 行田 悦資

(56)参考文献 特開平１１－２３９１２４（ＪＰ，Ａ）
ANTONOPOULOS, A. M., Chapter 4. Keys, Addresses, Wallets, Mastering Bitcoin, O'REILLY MEDIA INC., ２０１４年１２月, First Edition, p.1-23, [令和1年9月19日検索], インターネット<URL:https://www.oreilly.com/library/view/mastering-bitcoin/978141902639/ch04.html>

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／０８