(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2025-500248
(P2025-500248A)
(43)公表日　令和7年1月9日(2025.1.9)

(51)国際特許分類　FI
H04L 9/08 (2006.01)　H04L 9/08 Z
H04L 9/32 (2006.01)　H04L 9/32 100E

審査請求　未請求　予備審査請求　未請求　（全38頁）

(21)出願番号　特願2024-535919(P2024-535919)
(86)(22)出願日　令和4年11月23日(2022.11.23)
(85)翻訳文提出日　令和6年8月13日(2024.8.13)
(86)国際出願番号　PCT/US2022/050885
(87)国際公開番号　WO2023/113986
(87)国際公開日　令和5年6月22日(2023.6.22)
(31)優先権主張番号　17/551,670
(32)優先日　令和3年12月15日(2021.12.15)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　AP(BW,CV,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV
最終頁に続く

(71)出願人　519111877
キャピタル・ワン・サービシーズ・リミテッド・ライアビリティ・カンパニー
Ｃａｐｉｔａｌ Ｏｎｅ Ｓｅｒｖｉｃｅｓ，ＬＬＣ
アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０番
(74)代理人　100145403
弁理士　山尾 憲人
(74)代理人　100135703
弁理士　岡部 英隆
(74)代理人　100109139
弁理士　今井 孝弘
(72)発明者　オズボーン，ケビン
最終頁に続く

(54)【発明の名称】　非接触カード認証に基づく鍵回復

(57)【要約】
非接触カード暗号に基づくキー回復のためのシステム、方法、装置、およびコンピュータ読み取り可能なメディア。サーバは、アプリケーションから、デジタル・ウォレットの秘密鍵を回復するための要求を受信し得るものであり、前記要求には、前記非接触カードによって生成された第１の暗号文が含まれる。前記サーバは、前記非接触カードの鍵に基づいて第１の暗号文を復号化し得る。前記サーバは、前記復号化に基づいて、前記非接触カードの固有識別子と、前記デジタル・ウォレットに関連付けられた多様化係数を決定し得る。前記サーバは、前記固有識別子と前記多様化係数に基づいて秘密鍵を生成し得る。前記サーバは、ネットワーク経由で前記アプリケーションに前記秘密鍵を送信し得る。
【選択図】図１Ａ

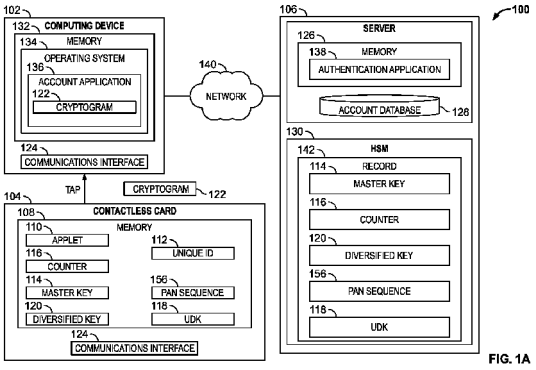


FIG. 1A

【特許請求の範囲】
【請求項１】
方法であって、
サーバによって、アプリケーションから、デジタル・ウォレットの秘密鍵を回復する要求を受信することであって、該要求は、非接触カードによって生成された第１の暗号文を備えることと、
前記サーバによって、前記非接触カードの鍵に基づいて、前記第１の暗号文を復号化することと、
前記復号化に基づいて、前記サーバによって、前記非接触カードの固有識別子と、前記デジタル・ウォレットに関連する多様化係数とを決定することと、
前記固有識別子と前記多様化係数に基づいて、前記サーバによって、秘密鍵を生成することと、
ネットワーク経由で前記サーバによって、前記アプリケーションに前記秘密鍵を送信することと、
を備える方法。
【請求項２】
多様化係数は、非接触カードのアプリケーション・プライマリ口座番号（ＰＡＮ）シーケンス番号を備える、
請求項１に記載の方法。
【請求項３】
多様化係数は、非接触カードのアプリケーション取引カウンタ（ＡＴＣ）を備える、
請求項１に記載の方法。
【請求項４】
前記要求を受信する前に、さらに、
前記サーバによって、前記アプリケーションから、前記非接触カードによって生成された第２の暗号文を受信することと、
前記サーバによって、前記第２の暗号文を復号化することと、
前記第２の暗号文の復号化に基づいて、前記サーバによって秘密鍵を生成することと、
前記秘密鍵に基づいて前記サーバが公開鍵を生成し、前記公開鍵に基づいて前記デジタル・ウォレットのウォレット・アドレスを生成することと、
前記サーバが前記アプリケーションに前記秘密鍵、前記公開鍵、前記ウォレット・アドレスを送信することと、
を備える請求項１に記載の方法。
【請求項５】
前記非接触カードの前記固有識別子および前記多様化係数は、前記デジタル・ウォレットの前記ウォレット・アドレスに基づいて決定される、
請求項４に記載の方法。
【請求項６】
前記第１の暗号文の復号化に基づいて前記デジタル・ウォレットの前記ウォレット・アドレスを生成すること、
をさらに含む、請求項５に記載の方法。
【請求項７】
前記サーバは、前記デジタル・ウォレットに関連付けられたソルト値をさらに決定し、
前記サーバは、前記ソルト値に基づいて秘密鍵をさらに生成し、
前記方法は、
前記秘密鍵に基づいて前記アプリケーションによって、前記デジタル・ウォレットにアクセスすること、
をさらに備える請求項１に記載の方法。
【請求項８】
非一過性のコンピュータ読み取り可能な記憶媒体であって、プロセッサによって実行さ

れると、前記プロセッサに、
アプリケーションから、デジタル・ウォレットの秘密鍵を回復する要求を受信することであって、前記要求は、非接触カードによって生成された第１の暗号文を備えることと、
前記非接触カードの鍵に基づいて、前記第１の暗号文を復号化することと、
前記復号化に基づいて、前記非接触カードの固有識別子と前記デジタル・ウォレットに関連する多様化係数を決定することと、
前記固有識別子と前記多様化係数に基づいて秘密鍵を生成することと、
ネットワーク経由で前記秘密鍵をアプリケーションに送信することと、
を行わせる命令を含む、コンピュータ読み取り可能な記憶媒体。
【請求項９】
前記多様化係数は、前記非接触カードのアプリケーション・プライマリ口座番号（ＰＡＮ）シーケンス番号からなる、
請求項８に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１０】
前記多様化係数は、前記非接触カードのアプリケーション取引カウンタ（ＡＴＣ）を備える、
請求項８に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１１】
前記命令は、前記要求を受信する前に、前記プロセッサに、さらに、
アプリケーションから、非接触カードによって生成された第２の暗号文を受信することと、
前記第２の暗号文を復号化することと、
前記第２の暗号文の復号化に基づいて秘密鍵を生成することと、
前記秘密鍵に基づいて公開鍵を生成し、前記公開鍵に基づいて前記デジタル・ウォレットのウォレット・アドレスを生成することと、
前記アプリケーションに前記秘密鍵、前記公開鍵、前記ウォレット・アドレスを送信することと、
を行わせる、請求項８に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１２】
前記非接触カードの前記固有識別子および前記多様化係数は、前記デジタル・ウォレットの前記ウォレット・アドレスに基づいて決定される、
請求項１１に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１３】
前記命令はさらに、
前記第１の暗号文の復号化に基づいて、前記デジタル・ウォレットの前記ウォレット・アドレスを生成するようにコンピュータを構成する、
請求項１２に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１４】
前記プロセッサは、前記デジタル・ウォレットに関連するソルト値をさらに決定し、前記プロセッサは、前記ソルト値に基づいて前記秘密鍵をさらに生成する、
請求項８に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１５】
プロセッサと、
前記プロセッサによって実行されると、前記プロセッサに以下を行わせる命令を記憶するメモリと、を備えるコンピューティング装置であって、
前記命令は、前記プロセッサに
アプリケーションから、デジタル・ウォレットの秘密鍵を回復する要求を受信することであって、前記要求は、非接触カードによって生成された第１の暗号文を備えることと、
前記非接触カードの鍵に基づいて第１の暗号文を復号化することと、
前記復号化に基づいて、前記非接触カードの固有識別子と前記デジタル・ウォレットに

関連する多様化係数を決定することと、
前記固有識別子と前記多様化係数に基づいて秘密鍵を生成することと、
ネットワーク経由で前記秘密鍵をアプリケーションに送信することと、
を行わせるコンピューティング装置。
【請求項１６】
前記多様化係数は、前記非接触カードのアプリケーション・プライマリ口座番号（ＰＡＮ）シーケンス番号を備える、
請求項１５に記載のコンピューティング装置。
【請求項１７】
前記多様化係数は、前記非接触カードのアプリケーション取引カウンタ（ＡＴＣ）を備えている、
請求項１５に記載のコンピューティング装置。
【請求項１８】
前記命令は、前記要求を受信する前に、前記コンピューティング装置を、
前記アプリケーションから、前記非接触カードによって生成された第２の暗号文を受信することと、
前記第２の暗号文を復号化することと、
前記第２の暗号文の復号化に基づいて秘密鍵を生成することと、
前記秘密鍵に基づいて公開鍵を生成し、前記公開鍵に基づいてデジタル・ウォレットのウォレット・アドレスを生成することと、
前記秘密鍵、前記公開鍵、前記ウォレット・アドレスを前記アプリケーションに送信することと、
を行うようにさらに構成する、請求項１５に記載のコンピューティング装置。
【請求項１９】
前記非接触カードの前記固有識別子および前記多様化係数は、前記デジタル・ウォレットの前記ウォレット・アドレスに基づいて決定され、前記命令は、前記第１の暗号文の復号化に基づいて前記デジタル・ウォレットの前記ウォレット・アドレスを生成するように前記プロセッサをさらに構成する、
請求項１８に記載のコンピューティング装置。
【請求項２０】
前記プロセッサは、前記デジタル・ウォレットに関連付けられたソルト値をさらに決定し、前記プロセッサは、前記ソルト値に基づいて秘密鍵をさらに生成する、
請求項１５に記載のコンピューティング装置。
【発明の詳細な説明】
【技術分野】
【０００１】
この出願は、２０２１年１２月１５日に提出された「非接触カード認証に基づく鍵回復」と題する米国特許出願番号１７／５５１，６７０に対する優先権を主張する。前述の出願の内容は、その全体が参照により本明細書に援用される。
【背景技術】
【０００２】
デジタル・ウォレットには多くの利点があるが、セキュリティとプライバシーの課題もある。最も一般的なリスクには、盗難やアクセス鍵の紛失（または忘れ）などがある。さらに、カストディ・ウォレットは特定の機関に結び付けられており、移植性が許可されない。プロキシ・ウォレットには、セキュリティ侵害や盗難のリスクがあり、アクセス鍵が危険にさらされる可能性がある。ハードウェア・ウォレットは回復シードを提供する場合があるが、これらのシードは盗難やその他の種類の損失（たとえば、ユーザがシードを思い出せない場合やシードの記録を見つけられない場合）が発生しやすくなる。
【発明の概要】
【０００３】

非接触カード認証に基づく鍵回復のためのシステム、方法、装置、およびコンピュータ読み取り可能なメディア。

一態様では、方法は、

サーバがアプリケーションからデジタル・ウォレットの秘密鍵を回復するための要求を受信することであって、前記要求には非接触カードによって生成された第１の暗号文が含まれることと、

前記サーバが前記非接触カードの鍵に基づいて第１の暗号文を復号化することと、

前記サーバは、前記復号化に基づいて、前記非接触カードの固有識別子と、ハードウェア・セキュリティ・モジュール内のデジタル・ウォレットに関連付けられた多様化係数とを決定することと、

前記サーバは、前記固有識別子と前記多様化係数に基づいて前記秘密鍵を生成することと、

前記サーバがネットワーク経由で前記アプリケーションに前記秘密鍵を送信することと、

を含む。

【０００４】

特定の要素または行為の説明を簡単に識別できるように、参照番号の最上位の数字は、その要素が最初に導入される図の番号を参照する。

【図面の簡単な説明】

【０００５】

【図１Ａ】図１Ａは、一実施形態による主題の一態様を示す。

【図１Ｂ】図１Ｂは、一実施形態による主題の一態様を示す。

【図１Ｃ】図１Ｃは、一実施形態による主題の一態様を示す。

【図２Ａ】図２Ａは、一実施形態による主題の一態様を示す。

【図２Ｂ】図２Ｂは、一実施形態による主題の一態様を示す。

【図２Ｃ】図２Ｃは、一実施形態による主題の一態様を示す。

【図３Ａ】図３Ａは、一実施形態による主題の一態様を示す。

【図３Ｂ】図３Ｂは、一実施形態による主題の一態様を示す。

【図４】図４は、一実施形態に従ったルーチン４００を示す。

【図５】図５は、一実施形態に従ったルーチン５００を示す。

【図６】図６は、一実施形態に従ったルーチン６００を示す。

【図７Ａ】図７Ａは、一実施形態による非接触カードを示す。

【図７Ｂ】図７Ｂは、一実施形態による非接触カード１０４を示す。

【図８】図８は、一実施形態に従ったデータ構造８００を示す。

【図９】図９は、実施形態に従ったシステム９００の例を示す。

【図１０】図１０は、実施形態に従った論理モデル１０００の例を示す。

【図１１】図１１は、実施形態に従った論理モデル１１００の例を示す。

【図１２】図１２は、一実施形態に従ったコンピュータ・アーキテクチャ１２００を示す。

【発明を実施するための形態】

【０００６】

本明細書に開示される実施形態は、非接触カードを使用して暗号通貨ウォレットなどのデジタル・ウォレットにアクセスするために使用される暗号鍵を安全に回復するための技術を提供する。デジタル・ウォレットを作成するには、コンピューティング装置が非接触カードに暗号文を生成するよう指示し得る。コンピューティング装置上で実行されるアプリケーションは、非接触カードとの無線通信を介して暗号文を受信し、検証のために暗号文をサーバに送信し得る。サーバが暗号文を検証すると、サーバはデジタル・ウォレットにアクセスしたり、デジタル・ウォレットを使用して操作を実行したりするために必要な秘密鍵を作成し得る。次に、サーバは秘密鍵に対応する公開鍵を作成し、公開鍵に基づいてデジタル・ウォレットのウォレット・アドレスを生成し得る。その後、サーバは、秘密

鍵を作成するために使用される暗号化アルゴリズムへの１つ以上の入力をハードウェア・セキュリティ・モジュール（ＨＳＭ）に保存し得る。入力には、非接触カードに関連付けられた１つ以上の鍵、非接触カードの固有識別子、および多様化係数が含まれ得る。いくつかの実施形態では、鍵はＨＳＭに格納され、一方、固有識別子および多様化係数は、秘密鍵を多様化するためのＨＳＭへの入力として提供され得る（たとえば、固有識別子および多様化係数はＨＳＭに格納される必要はない）。

【０００７】

サーバは、秘密鍵、公開鍵、およびウォレット・アドレスをアプリケーションに安全に送信し、アプリケーションはデジタル・ウォレットを生成し、その中に秘密鍵、公開鍵、およびウォレット・アドレスを保存し得る。いくつかの実施形態では、ユーザがデジタル・ウォレットにアクセスしようとすると、非接触カードを使用した暗号検証を使用してデジタル・ウォレットへのアクセスを認証し得る。暗号検証が成功しない場合、ユーザはウォレットへのアクセスを制限され、ウォレットのセキュリティが向上し得る。

【０００８】

デジタル・ウォレットには難読化されたバージョンの秘密鍵が保存されるため、ユーザは秘密鍵を紛失したり、忘れたり、あるいはデジタル・ウォレットで取引（暗号通貨の転送など）を実行するための前提条件として秘密鍵を提供できなくなる可能性があり得る。有利なことに、本明細書に開示される実施形態は、非接触カードを使用して秘密鍵を回復するための安全なソリューションを提供する。通常、秘密鍵を回復するために、非接触カードはサーバによって検証される暗号文を生成し得る。サーバが暗号文を検証できる場合、秘密鍵の生成に使用された入力がＨＳＭに提供され得る。その後、サーバは秘密鍵を再作成し、再作成された秘密鍵を１つ以上の部分に分けて要求元のアプリケーションおよび／または装置に送信し得る。

【０００９】

有利なことに、本明細書に開示された実施形態は、非接触カードによって生成された暗号を使用してデジタル・ウォレットにアクセスするために使用される秘密鍵を回復するための安全な技術を提供する。暗号文を活用することにより、本発明の実施形態は、不正行為のリスクを最小限に抑えながら、ユーザの身元を安全に検証し得る。さらに、そうすることで、ユーザがサーバとの暗号検証を容易にする非接触カードにアクセスできる場合にのみ、秘密鍵が復元されることが保証される。さらに、デジタル・ウォレットへのアクセスや秘密鍵の回復の前提条件として暗号検証を要求することで、デジタル・ウォレットのセキュリティが強化される。

【００１０】

本明細書で使用されている表記法および命名法を一般的に参照すると、本明細書の詳細な説明は、コンピュータまたはコンピュータのネットワーク上で実行されるプログラム手順の観点から提示され得る。これらの手順の説明と表現は、当業者が自分の作業の内容を他の当業者に効果的に伝えるために使用される。

【００１１】

ここでの手順は、一般的には、望ましい結果につながる一貫した一連の操作であると考えられている。これらの操作は、物理量の物理的な操作を必要とする操作である。通常、これらの量は、保存、転送、結合、比較、その他の操作が可能な電気信号、磁気信号、または光信号の形式をとるが、必ずしもそうとは限らない。主に一般的な使用上の理由から、これらの信号をビット、値、要素、シンボル、文字、用語、数値などと呼ぶことが便利な場合がある。ただし、これらすべての用語および類似の用語は適切な物理量に関連付けられるものであり、それらの量に適用される便利なラベルにすぎないことに注意する必要がある。

【００１２】

さらに、実行される操作は、多くの場合、加算や比較などの用語で表現されますが、これらは通常、人間のオペレータが実行する精神的な操作に関連付けられる。本明細書で説明される、１つまたは複数の実施形態の一部を構成するいずれの操作においても、人間の

オペレータのそのような能力は必要なく、またほとんどの場合望ましくもない。むしろ、操作は機械操作である。さまざまな実施形態の操作を実行するために有用な機械には、デジタルコンピュータまたは同様の装置が含まれる。

【００１３】

いくつかの実施形態は、「結合された」および「接続された」という表現とその派生語を使用して説明され得る。これらの用語は、必ずしも同義語として意図されているわけではない。たとえば、いくつかの実施形態は、２つ以上の要素が互いに直接物理的または電気的に接触していることを示すために、「接続された」および／または「結合された」という用語を使用して説明され得る。ただし、「結合された」という用語は、２つ以上の要素が直接接触していないものの、相互に協力したり相互作用したりすることを意味し得る。

【００１４】

さまざまな実施形態は、これらの操作を実行するための装置またはシステムにも関係する。この装置は、必要な目的のために特別に構築されるか、またはコンピュータに格納されたコンピュータ・プログラムによって選択的に起動または再構成されるコンピュータを備え得る。ここで紹介する手順は、本質的に特定のコンピュータやその他の装置に関連するものではない。本明細書の教示に従って記述されたプログラムでは、さまざまなマシンを使用し得るが、必要な方法のステップを実行するために、より特殊な装置を構築することが便利な場合もある。これらのさまざまなマシンに必要な構造は、説明から明らかになる。

【００１５】

ここで図面を参照すると、図面全体にわたって同様の要素を指すために同様の参照番号が使用されている。以下の説明では、説明の目的で、十分な理解が得られるように多数の具体的な詳細が記載されている。しかしながら、これらの具体的な詳細がなくても、新規な実施形態を実践することは可能である。他の例では、構造および装置は、説明を容易にするためにブロック図形式で示される。意図は、請求された主題と一致するすべての修正、同等物、および代替物を網羅することである。

【００１６】

図および付随する説明では、「ａ」、「ｂ」、「ｃ」（および同様の指定子）は、任意の正の整数を表す変数であることが意図されている。したがって、たとえば、実装でａの値を５に設定した場合、コンポーネント１２３－１から１２３－ａ（または１２３ａ）として示されるコンポーネント１２３の完全なセットには、コンポーネント１２３－１、１２３－２、１２３－３、１２３－４、および１２３－５が含まれ得る。実施形態はこの文脈に限定されない。

【００１７】

図１Ａは、開示された実施形態と一致する、システムとも呼ばれる例示的なコンピューティング・アーキテクチャ１００を示している。図１Ａ～１Ｃに示すコンピューティング・アーキテクチャ１００には、特定のトポロジ内の要素の数が限られているが、コンピューティング・アーキテクチャ１００には、特定の実装の必要に応じて、代替トポロジ内の要素の数を増やすことも減らすこともし得ることは理解できる。

【００１８】

コンピューティング・アーキテクチャ１００は、１つ以上のコンピューティング装置１０２、１つ以上のサーバ１０６、および１つ以上の非接触カード１０４を備える。非接触カード１０４は、クレジット・カード、デビット・カード、ＡＴＭカード、ギフト・カード、支払いカード、スマート・カードなどのあらゆるタイプのカードを表す。非接触カード１０４は、ＮＦＣ、ＥＭＶ標準、または無線通信におけるその他の短距離プロトコルを介してコンピューティング装置１０２の通信インターフェイス１２４（ここでは「カード・リーダ」、「ワイヤレス・カード・リーダ」、および／または「無線通信インターフェイス」とも呼ばれる）と通信するように構成された、無線周波数識別（ＲＦＩＤ）チップなどの１つ以上の通信インターフェイス１２４を含み得る。ここでは通信プロトコルの例

としてＮＦＣが使用されていますが、本開示は、ＥＭＶ標準、Ｂｌｕｅｔｏｏｔｈ（登録商標）、および／またはＷｉ－Ｆｉ（登録商標）などの他の種類の無線通信にも同様に適用できる。

【００１９】

コンピューティング装置１０２は、スマートフォン、タブレット・コンピュータ、ウェアラブル装置、ラップトップ、ポータブル・ゲーム装置、仮想化コンピューティング・システム、マーチャント端末、ＰＯＳシステム、サーバ、デスクトップ・コンピュータなど、あらゆる数および種類のコンピューティング装置を表す。モバイル装置は、コンピューティング装置１０２の例として使用できるが、本開示を制限するものとは見なされない。サーバ１０６は、サーバ、ワークステーション、コンピューティング・クラスタ、クラウド・コンピューティング・プラットフォーム、仮想化コンピューティング・システムなどのあらゆるタイプのコンピューティング装置を表す。明確にするために図示されていないが、コンピューティング装置１０２、非接触カード１０４、およびサーバ１０６には、それぞれ、プログラム、コード、および／または命令を実行するための１つ以上のプロセッサ回路が含まれる。

【００２０】

図に示すように、非接触カード１０４のメモリ１０８には、アプレット１１０、カウンタ１１６、１つ以上のマスター鍵１１４、１つ以上の多様化鍵１２０、固有ＩＤ１１２、プライマリ口座番号（ＰＡＮ：Ｐｒｉｍａｒｙ　Ａｃｃｏｕｎｔ　Ｎｕｍｂｅｒ）シーケンス番号１５６、および1つ以上の固有派生鍵（ＵＤＫ：Ｕｎｉｑｕｅ　Ｄｅｒｉｖｅｄ　Ｋｅｙｓ）１１８が含まれる。固有ＩＤ１１２は、非接触カード１０４を他の非接触カード１０４と比較して一意に識別する任意の識別子である。ＰＡＮシーケンス１５６には、非接触カード１０４によって保存されたカウンタ値が含まれ得る。アプレット１１０は、本明細書で説明する操作の一部またはすべてを実行するように構成された実行可能コードである。カウンタ１１６は、非接触カード１０４とサーバ１０６の間で同期される値である。カウンタ１１６は、非接触カード１０４とサーバ１０６（および／または非接触カード１０４とコンピューティング装置１０２）の間でデータが交換されるたびに変化する数値を備え得る。カウンタ１１６、マスター鍵１１４、多様化鍵１２０、ＵＤＫ１１８、ＰＡＮシーケンス１５６、および／または固有ＩＤ１１２は、以下でより詳細に説明するように、システム１００のセキュリティを提供するために使用される。

【００２１】

図に示すように、コンピューティング装置１０２のメモリ１３２には、オペレーティング・システム１３４のインスタンスが含まれている。オペレーティング・システムの例としては、Ａｎｄｒｏｉｄ（登録商標）ＯＳ、ｉＯＳ（登録商標）、ｍａｃＯＳ（登録商標）、Ｌｉｎｕｘ（登録商標）、Ｗｉｎｄｏｗｓ（登録商標）オペレーティング・システムなどがある。図に示すように、オペレーティング・システム１３４には口座アプリケーション１３６が含まれる。口座アプリケーション１３６を使用すると、ユーザは、デジタル・ウォレットの管理、ウォレットを使用した取引の処理、ブロックチェーンおよび／または暗号通貨取引の処理、支払いカードの有効化、口座残高の表示、アイテムの購入、支払いの処理など、さまざまな口座関連の操作を実行できる。いくつかの実施形態では、ユーザは認証資格情報を使用して認証し、口座アプリケーション１３６の特定の機能にアクセスできる。たとえば、認証資格情報には、ユーザ名（またはログイン）とパスワード、生体認証資格情報（指紋、Ｆａｃｅ　ＩＤなど）などが含まれ得る。

【００２２】

図に示すように、サーバ１０６のメモリ１２６には、認証アプリケーション１３８と口座データベース１２８が含まれる。口座データベース１２８には、通常、口座所有者（たとえば、１人以上のユーザ）、口座所有者の１つ以上の口座、および口座の１つ以上の非接触カード１０４に関連する情報が含まれる。

【００２３】

前述のように、口座アプリケーション１３６は、デジタル・ウォレットを作成、管理、

アクセス、またはその他の方法で使用するために使用し得る。デジタル・ウォレットを使用すると、一方の当事者がもう一方の当事者と電子取引を行うことができる。いくつかの実施形態では、デジタル・ウォレットは、暗号通貨の秘密鍵および／または公開鍵を保存する暗号通貨ウォレットである。暗号通貨は、ビットコイン、イーサリアムなど、あらゆるタイプの暗号通貨である。デジタル・ウォレットを作成するには、ユーザは認証資格情報を使用して口座に認証する必要がある。次に、口座アプリケーション１３６は、非接触カード１０４をコンピューティング装置１０２にタップするようにユーザに指示する。

【００２４】

図１Ａに示す実施形態では、ユーザは非接触カード１０４をコンピューティング装置１０２にタップできる（または、非接触カード１０４を装置１０２の通信インターフェイス１２４の通信範囲内に持ち込む）。次に、口座アプリケーション１３６は、アプレット１１０に暗号文１２２を生成するように指示する。暗号文１２２は、任意の適切な暗号化技術に基づいて生成し得る。いくつかの実施形態では、暗号文１２２は、非接触カード１０４の固有ＩＤ１１２に基づくものであってもよい。いくつかの実施形態では、アプレット１１０には、暗号文１２２と、暗号文１２２を含むデータ・パッケージの一部として暗号化されていない識別子（例えば、カウンタ１１６、ＰＡＮシーケンス１５６、固有ＩＤ１１２、および／またはその他の固有識別子）が含まれ得る。少なくとも１つの実施形態では、データ・パッケージはＮＤＥＦファイルである。

【００２５】

前述のように、コンピューティング・アーキテクチャ１００は、データを保護するために鍵の多様化を実装するように構成されており、これを本明細書では鍵の多様化技術と呼ぶことがある。一般に、サーバ１０６（または他のコンピューティング装置）と非接触カード１０４には、同じマスター鍵１１４（マスター対称鍵とも呼ばれる）がプロビジョニングされ得る。より具体的には、各非接触カード１０４には、サーバ１０６のハードウェア・セキュリティ・モジュール（ＨＳＭ）１３０内に対応するペアを持つ個別のマスター鍵１１４がプログラムされている。たとえば、非接触カード１０４が製造されるとき、固有のマスター鍵１１４が非接触カード１０４のメモリ１０８にプログラムされ得る。同様に、固有マスター鍵１１４は、ＨＳＭ１３０内のレコード１４２に格納され得る。

【００２６】

さらに、特定のカード１０４が製造されるとき、多様化係数とＨＳＭ１３０内のマスター鍵１１４インデックスへの参照（たとえば、レコード１４２へのインデックス）を入力として受け取るＨＳＭ関数を介して、ＵＤＫ１１８がマスター鍵１１４から多様化され得る。いくつかの実施形態では、多様化係数は、非接触カード１０４の固有ＩＤ１１２およびＰＡＮシーケンス１５６であり得る。

ＵＤＫ１１８は、非接触カード１０４およびＨＳＭ１３０のレコード１４２に格納され得る。マスター鍵１１４およびＵＤＫ１１８は、非接触カード１０４およびサーバ１０６以外のすべての関係者から秘密に保持できるため、システム１００のセキュリティが強化される。レコード１４２に格納されているように示されているが、一部の実施形態では、カウンタ１１６および／またはＰＡＮシーケンス１５６はＨＳＭ　１３０に格納されない。たとえば、固有ＩＤ１１２、カウンタ１１６、およびＰＡＮシーケンス１５６は、口座データベース１２８に格納され得る。

【００２７】

いくつかの実施形態では、暗号文１２２を生成するために、アプレット１１０は、ＵＤＫ１１８、固有ＩＤ１１２、および多様化係数を暗号化アルゴリズムへの入力として提供し、それによって多様化鍵１２０を生成し得る。いくつかの実施形態では、多様化係数はカウンタ１１６である。他の実施形態では、ＰＡＮシーケンス１５６が多様化係数である。多様化鍵１２０は、多様化係数（たとえば、カウンタ１１６および／またはＰＡＮシーケンス１５６）やその他の機密データなどの一部のデータを暗号化するために使用され得る。アプレット１１０とサーバ１０６は、暗号文の復号化および／または検証処理を容易にするために、同じタイプのデータを暗号化するように構成し得る。

【００２８】
前述のように、非接触カード１０４およびサーバ１０６のＵＤＫ１１８は、鍵の多様化を使用してセキュリティを強化するために、カウンタ１１６と組み合わせて使用し得る。前述のように、カウンタ１１６は、非接触カード１０４とサーバ１０６の間で同期される値で構成される。カウンタ１１６は、非接触カード１０４とサーバ１０６（および／または非接触カード１０４とコンピューティング装置１０２）との間でデータが交換されるたびに変化する数値を含み得る。データ（例えば、サーバ１０６および／または装置１０２）を送信する準備をするとき、非接触カード１０４のアプレット１１０はカウンタ１１６を増分し得る。非接触カード１０４のアプレット１１０は、ＵＤＫ１１８、固有ＩＤ１１２、およびカウンタ１１６を暗号化アルゴリズムへの入力として提供し、暗号化アルゴリズムは出力として多様化鍵１２０を生成する。暗号化アルゴリズムには、暗号化アルゴリズム、ハッシュ・ベースのメッセージ認証コード（ＨＭＡＣ：Ｈａｓｈ－ｂａｓｅｄ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）アルゴリズム、暗号ベースのメッセージ認証コード（ＣＭＡＣ：Ｃｉｐｈｅｒ－ｂａｓｅｄ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）アルゴリズムなどが含まれる。暗号化アルゴリズムの非限定的な例としては、３ＤＥＳやＡＥＳ１０７などの対称暗号化アルゴリズム、ＨＭＡＣ－ＳＨＡ－２５６などの対称ＨＭＡＣアルゴリズム、ＡＥＳ－ＣＭＡＣなどの対称ＣＭＡＣアルゴリズムなどが挙げられる。主要な多様化技術の例については、２０１８年１１月２９日に提出された米国特許出願１６／２０５，１１９で詳しく説明されている。前述の特許出願は、その全体が参照により本明細書に援用される。いくつかの実施形態では、カウンタ１１６の代わりにＰＡＮシーケンス１５６が暗号化アルゴリズムへの入力として使用され、たとえば、ＵＤＫ１１８、固有ＩＤ１１２、およびＰＡＮシーケンス１５６を暗号化することによって、多様化鍵１２０が生成される。

【００２９】
次に、アプレット１１０は、多様化鍵１２０とデータを暗号化アルゴリズムへの入力として使用して、一部のデータ（たとえば、固有ＩＤ１１２、カウンタ１１６、ＰＡＮシーケンス１５６、コマンド、および／またはその他のデータ）を暗号化する。たとえば、多様化鍵１２０を使用して固有ＩＤ１１２を暗号化すると、暗号化された固有ＩＤ１１２（たとえば、暗号文１２２）が生成され得る。前述のように、アプレット１１０とサーバ１０６は同じデータを暗号化するように構成し得る。

【００３０】
いくつかの実施形態では、例えば、暗号化関数への入力の１つ以上の部分に基づいて、２つの多様化鍵１２０が生成され得る。いくつかの実施形態では、２つの多様化鍵１２０は、２つの異なるマスター鍵１１４、２つの異なるＵＤＫ１１８、固有ＩＤ１１２、およびカウンタ１１６（またはＰＡＮシーケンス１５６）に基づいて生成される。このような実施形態では、多様化鍵１２０の１つを使用してメッセージ認証コード（ＭＡＣ）が生成され、多様化鍵１２０の他の１つを使用してＭＡＣが暗号化され得る。ＭＡＣは、機密データ、固有ＩＤ１１２、カウンタ１１６、および／またはＰＡＮシーケンス１５６など、ＭＡＣアルゴリズムに入力される任意の適切なデータに基づいて生成し得る。より一般的には、アプレット１１０とサーバ１０６は、同じデータに基づいてＭＡＣを生成するように構成され得る。いくつかの実施形態では、暗号文１２２は、ＮＤＥＦファイルなどのデータ・パッケージに含まれる。その後、口座アプリケーション１３６は、コンピューティング装置１０２の通信インターフェイス１２４を介して、暗号文１２２を含むデータ・パッケージを読み取り得る。

【００３１】
図１Ｂは、口座アプリケーション１３６が暗号文１２２をサーバ１０６に送信する実施形態を示す。サーバ１０６は、サーバ１０６によって保存されたマスター鍵１１４および／またはＵＤＫ１１８のインスタンスに基づいて、少なくとも部分的に検証のために、暗号文１２２を認証アプリケーション１３８および／またはＨＳＭ１３０に提供し得る。いくつかの実施形態では、認証アプリケーション１３８および／またはＨＳＭ１３０は、サ

ーバ１０６に提供された暗号化されていない固有ＩＤ１１２を使用して、ＵＤＫ１１８（またはマスター鍵１１４）およびカウンタ１１６を識別し得る。ＰＡＮシーケンス１５６を使用して暗号文１２２を生成する例では、サーバ１０６は、暗号化されていない固有ＩＤ１１２を使用して、口座データベース１２８および／またはＨＳＭ１３０内のＰＡＮシーケンス１５６を識別し得る。いくつかの例では、認証アプリケーション１３８は、ＵＤＫ１１８、固有ＩＤ１１２、およびカウンタ１１６をＨＳＭ１３０の暗号化機能への入力として提供し、ＨＳＭ１３０は１つ以上の多様化鍵１２０を出力として生成する。他の実施形態では、サーバは、ＵＤＫ１１８、固有ＩＤ１１２、およびＰＡＮシーケンス１５６を暗号化して、多様化鍵１２０を生成する。結果として得られる多様化鍵１２０は、非接触カード１０４の多様化鍵１２０に対応する可能性があり、これを使用して暗号文１２２を復号化し、および／または復号化されたＭＡＣを検証し得る。たとえば、サーバ１０６は、アプレット１１０と同じデータ、例えば機密データ、固有ＩＤ１１２、カウンタ１１６、および／またはＰＡＮシーケンス１５６に基づいてＭＡＣを生成し得る。サーバ１０６によって生成されたＭＡＣが暗号文１２２内の復号化されたＭＡＣと一致する場合、サーバ１０６は暗号文１２２を検証または認証し得る。

【００３２】

使用される復号化技術に関係なく、認証アプリケーション１３８および／またはＨＳＭ１３０は暗号文１２２を正常に復号化し、ＭＡＣを検証して、暗号文１２２を検証または認証し得る。復号化および／またはＭＡＣ検証が成功した場合、認証アプリケーション１３８および／またはＨＳＭ１３０は、ユーザ用のデジタル・ウォレット１４４を生成し得る。一般的に、デジタル・ウォレット１４４を作成するには、秘密鍵１４６を生成する必要がある。いくつかの実施形態では、ランダムな数字が、ＳＨＡ－２アルゴリズムやその他の適切なアルゴリズムなどの暗号化（またはハッシュ）アルゴリズムへの入力として提供され、任意の長さの秘密鍵１４６が生成される。他の実施形態では、非接触カード１０４の固有ＩＤ１１２とＰＡＮシーケンス１５６が連結され、ハッシュ・アルゴリズムへの入力として提供され、秘密鍵１４６が生成される。他の実施形態では、非接触カード１０４の固有ＩＤ１１２とカウンタ１１６が連結され、ハッシュ・アルゴリズムへの入力として提供され、秘密鍵１４６が生成される。

【００３３】

他の実施形態では、非接触カード１０４のマスター鍵１１４、固有ＩＤ１１２、およびカウンタ１１６が連結され、ハッシュ・アルゴリズムへの入力として提供され、秘密鍵１４６が生成される。マスター鍵１１４を使用して秘密鍵１４６を生成する実施形態では、非接触カード１０４の第１マスター鍵１１４を使用して暗号文１２２を生成し、非接触カード１０４の第２マスター鍵１１４を使用して秘密鍵１４６を生成し得るものであり、第１マスター鍵１１４と第２マスター鍵１１４は異なる鍵である。他の実施形態では、多様化鍵１２０の１つ、固有ＩＤ１１２、および非接触カード１０４のカウンタ１１６が連結され、ハッシュ・アルゴリズムへの入力として提供され、秘密鍵１４６が生成される。他の実施形態では、ＵＤＫ１１８の１つ、固有ＩＤ１１２、および非接触カード１０４のカウンタ１１６が連結され、ハッシュ・アルゴリズムへの入力として提供され、秘密鍵１４６が生成される。秘密鍵１４６を生成するために使用される入力に関係なく、いくつかの実施形態では、秘密鍵１４６を生成するためのハッシュ・アルゴリズムへの入力にソルト（たとえば、ランダム・データ）が含まれる。

【００３４】

次に、秘密鍵１４６を使用して、対応する公開鍵１４８を生成し得る。いくつかの実施形態では、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ：Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ）を使用して秘密鍵１４６に基づいて公開鍵１４８が生成され得る。いくつかの実施形態では、公開鍵１４８は、例えばハッシュ・アルゴリズムを使用して連結（または圧縮）され得る。いくつかの実施形態では、ソルトを使用して公開鍵１４８を生成する。ウォレット・アドレス１５０は、公開鍵１４８に基づいて、たとえば公開鍵１４８をハッシュすることによって、デジタ

ル・ウォレット１４４用に生成され得る。デジタル・ウォレット１４４はＨＳＭ１３０に格納されているように示されているが、一部の実施形態では、デジタル・ウォレット１４４はＨＳＭ１３０に永続的に格納されるわけではない。代わりに、本明細書でより詳細に説明するように、秘密鍵１４６を再作成するために使用される要素は、ＨＳＭ１３０および／または口座データベース１２８に格納され得る。たとえば、固有ＩＤ１１２およびカウンタ１１６は、ＨＳＭ１３０および／または口座データベース１２８に格納され得る。別の例では、固有ＩＤ１１２およびＰＡＮシーケンス１５６は、ＨＳＭ１３０および／または口座データベース１２８に格納され得る。

【００３５】

いくつかの実施形態では、秘密鍵１４６および／または公開鍵１４８は、例えば階層的な決定論的鍵を作成するために、さらに多様化される場合がある。たとえば、秘密鍵１４６は、カウンタ１１６、固有ＩＤ１１２、ソルト値１５４、またはその他の所定のシード値を使用して多様化し得る。そうすることで、秘密鍵１４６が多様化する可能性があり得る。同様に、公開鍵１４８は、カウンタ１１６、固有ＩＤ１１２、ソルト値１５４、またはその他の所定のシード値を使用して多様化され、多様化された公開鍵１４８が作成される。このような実施形態では、秘密鍵１４６および／または公開鍵１４８を多様化するために使用される任意のシード値は、口座データベース１２８および／またはＨＳＭ１３０の回復レコード１５２に格納され得る。より一般的には、秘密鍵１４６および／または公開鍵１４８は、シード値を複数回使用して多様化され、それによって、多様化された秘密鍵１４６および／または多様化された公開鍵１４８のツリー（または階層）が生成される。このような実施形態では、ツリー（または階層）の１つ以上のパスを使用して、異なる多様化されたキーを指定し得る。より一般的には、ツリーの各ノードは、多様化された公開鍵および／または多様化された子鍵に対応し得る。ツリーのノードの秘密鍵と公開鍵が与えられれば、ツリー内のすべての子孫ノードの多様な秘密鍵と公開鍵を導出し得る。さらに、ツリー内の各リーフ・ノードは、多様化された公開鍵および／または多様化された子鍵に対応し得る。いくつかの実施形態では、パスはさらに、通貨、通貨の額、取引の第１のウォレット・アドレス（例：送信ウォレット・アドレス）、取引の第２のウォレット・アドレス（例：受取人のウォレット・アドレス）、およびその他の属性などの取引の属性を指定するために使用される。これらの属性は、ツリーの特定のノードに格納され得る。

【００３６】

復号化に戻ると、認証アプリケーション１３８が暗号文１２２を復号化できない場合（および／またはＭＡＣを検証できない場合）、認証アプリケーション１３８は暗号文１２２を検証しない。このような例では、認証アプリケーション１３８は、デジタル・ウォレットの生成を控えることを決定する。認証アプリケーション１３８は、失敗した復号化および／または検証の指示をコンピューティング装置１０２に送信し得る。

【００３７】

図１Ｃは、認証アプリケーション１３８がデジタル・ウォレット１４４をコンピューティング装置１０２に送信する実施形態を示す。図に示すように、口座アプリケーション１３６は、秘密鍵１４６、公開鍵１４８、およびウォレット・アドレス１５０を含むデジタル・ウォレット１４４　（メモリ１３２および／または不揮発性ストレージ（明瞭性のために図示されていない）を保存し得る。口座アプリケーション１３６は、秘密鍵１４６、公開鍵１４８、および／またはウォレット・アドレス１５０をハッシュ化、暗号化、またはその他の方法で難読化し得る。口座アプリケーション１３６は、ユーザ名やパスワード、生体認証情報などの認証制御を使用してデジタル・ウォレット１４４を保護し得る。さらに、および／または代わりに、口座アプリケーション１３６は、デジタル・ウォレット１４４（例えば、非接触カード１０４は、本明細書で説明されているように、サーバ１０６によって検証される暗号文を生成する）にアクセスするために、非接触カード１０４を使用した暗号の復号化および／または検証を要求し得る。さらに、いくつかの実施形態では、口座アプリケーション１３６は、デジタル・ウォレット１４４にアクセスしたり、デ

ジタル・ウォレット１４４を使用して操作を実行したりするために、ユーザに秘密鍵１４６の提供を要求し得る。より一般的には、口座アプリケーション１３６は、デジタル・ウォレット１４４にアクセスしたり、使用したり、その他の方法で管理したりするためのさまざまなインターフェイスを提供し得る。

【００３８】

いくつかの実施形態では、デジタル・ウォレット１４４は、たとえば、サーバ１０６またはクライアントにクラウド・ベースのウォレット・サービスを提供する別のコンピューティング・システムなどのクラウド・ベースのウォレットに保存され得る。実施形態はこの文脈に限定されない。クラウド・ベースのウォレットは、たとえば口座アプリケーション１３６を介してデジタル・ウォレット１４４にアクセスしたり、その他の方法で使用したりするためのインターフェイスを提供し得る。

【００３９】

図に示すように、サーバ１０６は、デジタル・ウォレット１４４の作成に基づいて、口座データベース１２８に回復レコード１５２を作成した。回復レコード１５２には、固有ＩＤ１１２、多様化係数１５８（たとえば、カウンタ１１６および／またはＰＡＮシーケンス１５６）、および秘密鍵１４６を生成するためのソルト１５４（使用されている場合）が含まれる。いくつかの実施形態では、回復レコード１５２は、ウォレット１４４のウォレット・アドレス１５０に基づいてインデックス付けされ得る。他の実施形態では、回復レコード１５２は、非接触カード１０４のキーを格納するＨＳＭ１３０のレコード１４２に基づいてインデックス付けされ得る。他の実施形態では、回復レコード１５２は、非接触カード１０４の固有ＩＤ１１２に基づいてインデックス付けされる。次に、回復レコード１５２を使用して、たとえば、固有ＩＤ１１２、多様化係数１５８、および／またはソルト１５４と適切なアルゴリズムに基づいて、秘密鍵１４６を再作成し得る。多様化鍵１２０、ＵＤＫ１１８、またはマスター鍵１１４を使用して秘密鍵１４６を生成する実施形態では、セキュリティを向上させるために、多様化鍵１２０、ＵＤＫ１１８、またはマスター鍵１１４は回復レコード１５２に保存されないという利点がある。このような実施形態では、ＨＳＭ１３０は、秘密鍵１４６を再作成するために使用されるマスター鍵１１４、ＵＤＫ１１８、および／または多様化鍵１２０を格納し、一方、固有ＩＤ１１２、多様化係数１５８、および／またはソルト１５４は、口座データベース１２８に格納され得る。

【００４０】

図２Ａは、ユーザが秘密鍵１４６の回復を要求する実施形態を示す概略図２００である。図に示すように、秘密鍵１４６を回復するために、口座アプリケーション１３６は、非接触カード１０４をコンピューティング装置１０２にタップするようにユーザに指示し、これにより非接触カード１０４は暗号文２０８を生成する。暗号文２０８は、暗号文１２２を参照して上で説明したように生成し得る。たとえば、アプレット１１０は、カウンタ１１６を増分し、１つ以上のＵＤＫ１１８、固有ＩＤ１１２、およびカウンタ１１６を暗号化して、１つ以上の多様化鍵１２０を生成し得る。１つ以上の多様化鍵１２０は、何らかのデータに基づいてＭＡＣを生成し、ＭＡＣおよび／またはデータを暗号化するために使用し得る。いくつかの実施形態では、ウォレット・アドレス１５０と多様化鍵１２０の１つに基づいてＭＡＣが生成される。このような実施形態では、ウォレット・アドレス１５０とＭＡＣは、多様化鍵１２０のもう１つを使用して暗号化され、暗号文２０８が生成される。別の例として、公開鍵１４８を使用してＭＡＣを生成し、公開鍵１４８をＭＡＣで暗号化し得る。

【００４１】

図２Ｂは、口座アプリケーション１３６が検証のために暗号文２０８をサーバ１０６に送信する実施形態を示す。一般的に、サーバ１０６は、カウンタ１１６を増分し、非接触カード１０４のＵＤＫ１１８、固有ＩＤ１１２、およびカウンタ１１６を暗号化して、非接触カード１０４によって生成された鍵に対応する１つ以上の多様化鍵１２０を生成し得る。１つ以上の多様化鍵１２０は、暗号文２０８を復号化し、および／またはＭＡＣを検

証するために使用し得る。

【００４２】

サーバ１０６が暗号文２０８を復号化でき、かつ／またはＭＡＣを検証できる場合、サーバ１０６は回復レコード１５２に基づいて秘密鍵１４６を再作成し得る。ウォレット・アドレス１５０が暗号文２０８で暗号化されている実施形態では、ウォレット・アドレス１５０に基づいて回復レコード１５２がインデックス付け（検索など）され、サーバ１０６は復号化されたウォレット・アドレス１５０を使用して回復レコード１５２にアクセスし得る。公開鍵１４８が暗号文２０８で暗号化されている実施形態では、サーバ１０６は公開鍵１４８を使用してウォレット・アドレス１５０を再生成し、再生成されたウォレット・アドレス１５０を使用して口座データベース１２８をインデックス化し得る。他の実施形態では、口座データベース１２８は、回復レコード１５２を識別するために固有ＩＤ１１２を使用してインデックス付けされる。このような実施形態では、固有ＩＤ１１２は、暗号文２０８に含まれる固有ＩＤ１１２の暗号化されていないバージョンに基づいて決定される。

【００４３】

サーバ１０６が回復レコード１５２を識別すると、回復レコード１５２を使用して秘密鍵１４６を再作成し得る。たとえば、回復レコード１５２の固有ＩＤ１１２、多様化係数１５８、およびソルト１５４（使用されている場合）は、秘密鍵１４６を最初に作成するために使用されるＨＳＭ１３０の機能への入力として提供され得る。こうすることで、秘密鍵１４６が再作成される。

【００４４】

いくつかの実施形態では、サーバ１０６は、マスター鍵１１４またはＵＤＫ１１８に基づいて秘密鍵１４６をさらに再作成する。たとえば、サーバ１０６は、非接触カード１０４のマスター鍵１１４と回復レコード１５２（たとえば、ユニークＩＤ１１２、多様化係数１５８、任意のソルト１５４）内のデータを、秘密鍵１４６の作成に使用されるＨＳＭ１３０の機能への入力として提供し得る。こうすることで、秘密鍵１４６が再作成される。別の例として、サーバ１０６は、非接触カード１０４のＵＤＫ１１８と回復レコード１５２（例えば、ユニークＩＤ１１２、多様化係数１５８、任意のソルト１５４）内のデータを、秘密鍵１４６の作成に使用されるＨＳＭ１３０の機能への入力として提供し得る。これにより、秘密鍵１４６も再作成される。

【００４５】

いくつかの実施形態では、ＵＤＫ１１８、固有ＩＤ１１２、多様化係数１５８、および任意のソルト１５４がＨＳＭ１３０の機能に入力され、秘密鍵１４６を生成するために使用される多様化鍵１２０が生成される。多様化鍵１２０、多様化係数１５８、および任意のソルト１５４は、秘密鍵１４６を再作成するためのＨＳＭ１３０の機能への入力として提供され得る。

【００４６】

一方、ＨＳＭ１３０が暗号文１２２を復号化できない場合、および／またはＭＡＣを検証できない場合、ＨＳＭ１３０は暗号文１２２を検証しない。このような例では、認証アプリケーション１３８は、秘密鍵１４６の回復を控えることを決定する。認証アプリケーション１３８は、失敗した復号化および／またはＭＡＣ検証の指示をコンピューティング装置１０２に送信し得る。このような実施形態では、ユーザは回復レコード１５２を使用して秘密鍵１４６を回復することが制限される。

【００４７】

図２Ｃは、ＨＳＭ１３０が回復レコード１５２に基づいて秘密鍵１４６を再作成し、秘密鍵１４６を口座アプリケーション１３６に送信する実施形態を示す。いくつかの実施形態では、サーバ１０６は、秘密鍵１４６を１つ以上のデータ部分で送信し得る。より一般的には、サーバ１０６は、コンピューティング装置１０２とのセキュリティ保護された接続を使用して秘密鍵１４６を送信し得る。その後、コンピューティング装置１０２は秘密鍵１４６を表示し、ユーザが秘密鍵１４６を回復できるようにする。その後、ユーザは秘

密鍵１４６を使用して、デジタル・ウォレット１４４および／またはデジタル・ウォレット１４４に関連付けられた任意の暗号通貨を使用して１つ以上の操作を実行し得る。たとえば、秘密鍵１４６は、ブロックチェーン９０６内で取引を生成するために使用され得る。

【００４８】

いくつかの実施形態では、秘密鍵１４６はコンピューティング装置１０２に送信されない。たとえば、クラウド・ベースのウォレットの実施形態では、秘密鍵１４６を使用して取引または他の種類のデータに署名し得る。このような例では、ユーザは口座認証資格情報を使用して口座アプリケーション１３６で自分の口座を認証し、意図した取引の詳細（例：購入、暗号通貨の送金など）を提供し得る。口座アプリケーション１３６は、取引の詳細をサーバ１０６に提供し得る。いくつかの実施形態では、口座アプリケーション１３６は、暗号文および／または暗号文を含むデータ・パッケージで取引の詳細を提供する。暗号文は、暗号文１２２および／または暗号文２０８に類似し得る。その後、サーバ１０６は、回復レコード１５２（例えば、ユニークＩＤ１１２、カウンタ１１６、ＰＡＮシーケンス１５６、および／またはソルト１５４）から鍵を多様化するために使用されるデータを取得し得る。回復レコード１５２からのデータはＨＳＭ１３０に提供され、ＨＳＭ１３０は回復レコードのデータとマスター鍵１１４および／またはＵＤＫ１１８を使用して取引のデジタル署名を生成する。こうすることで、取引に必要な署名が生成される。たとえば、有効な署名を生成することにより、公開鍵１４８を使用して取引を検証できる。このような例では、検証された取引を反映するために、取引がブロックチェーンに追加され得る。

【００４９】

図３Ａは、たとえば秘密鍵１４６を回復するために、非接触カード１０４をコンピューティング装置１０２にタップする実施形態を示す概略図３００ａである。前述のように、非接触カード１０４がコンピューティング装置１０２にタップされると、アプレット１１０は暗号文（たとえば、暗号文１２２および／または暗号文２０８）を生成し得る。暗号文およびその他のデータ（例：暗号化されていない固有ＩＤ１１２）は、コンピューティング装置１０２によって読み取られるＮＤＥＦファイルなどのデータ・パッケージに含まれ得る。次に、コンピューティング装置１０２は、本明細書で説明されているように、検証（例：復号化および／またはＭＡＣ検証）のために暗号文をサーバ１０６に送信し得る。

【００５０】

図３Ｂは、サーバ１０６が図３Ａで生成された暗号文を検証した実施形態を示す概略図３００ｂである。検証に基づいて、サーバ１０６は回復レコード１５２に基づいて秘密鍵１４６を再作成し得る。その後、サーバ１０６は秘密鍵１４６を口座アプリケーション１３６に送信し得る。図に示すように、口座アプリケーション１３６は、秘密鍵１４６を文字列としてディスプレイに表示する。いくつかの実施形態では、秘密鍵１４６を表すためにマトリックス・コード３０２が生成され得る。そうすることで、マトリックス・コード３０２をスキャンして秘密鍵１４６を判別できるようになる。

【００５１】

開示された実施形態の動作は、以下の図を参照してさらに説明し得る。一部の図にはロジック・フローが含まれ得る。ここで提示される図には特定のロジック・フローが含まれ得るが、ロジック・フローは、ここで説明する一般的な機能がどのように実装されるかの例を単に提供するものであることがわかる。さらに、特に明記しない限り、特定のロジック・フローは必ずしも提示された順序で実行される必要はない。さらに、一部の実施形態では、ロジック・フローに示されたすべての動作が必要なわけではない。さらに、与えられたロジック・フローは、ハードウェア要素、プロセッサによって実行されるソフトウェア要素、またはそれらの任意の組み合わせによって実装され得る。実施形態はこの文脈に限定されない。

【００５２】

図４は、ロジック・フローまたはルーチン４００の実施形態を示す。ロジック・フロー４００は、本明細書で説明する１つ以上の実施形態によって実行される操作の一部またはすべてを表し得る。たとえば、ロジック・フロー４００には、デジタル・ウォレットを作成するための操作の一部またはすべてが含まれ得る。実施形態はこの文脈に限定されない。

【００５３】

ブロック４０２では、サーバ１０６は、コンピューティング装置１０２上で実行されている口座アプリケーション１３６から、デジタル・ウォレットを生成するための要求を受信し得る。要求には、非接触カード１０４によって生成され、コンピューティング装置１０２に送信された暗号文が含まれ得る。ブロック４０４では、サーバは、マスター鍵１１４、ＵＤＫ１１８、およびカウンタ１１６に基づいて１つ以上の多様化鍵１２０を生成することによって暗号文を復号化し得る。サーバ１０６は、暗号文をさらに検証し、たとえば、サーバ１０６によって生成されたＭＡＣが復号化された暗号文内のＭＡＣと一致するかどうかを判断する。

【００５４】

ブロック４０６では、サーバ１０６は、ブロック４０４での暗号文の復号化および／または検証の成功に基づいて秘密鍵１４６を生成する。秘密鍵１４６は、ＨＳＭ１３０の暗号化機能への入力に基づき得る。入力には、固有ＩＤ１１２と多様化係数１５８（たとえば、非接触カード１０４のカウンタ１１６および／またはＰＡＮシーケンス１５６）が含まれ得る。いくつかの実施形態では、入力には、マスター鍵１１４、ＵＤＫ１１８、および／または多様化鍵１２０がさらに含まれ得る。ブロック４０８では、サーバ１０６は秘密鍵１４６に基づいて公開鍵１４８を生成し得る。サーバはさらに、公開鍵１４８に基づいてデジタル・ウォレット１４４のウォレット・アドレス１５０をさらに作成し得る。ブロック４１０では、サーバは、秘密鍵１４６、公開鍵１４８、およびウォレット・アドレス１５０をアプリケーションに送信し得る。ブロック４１２では、サーバ１０６は、秘密鍵を生成するために使用された１つ以上の入力を口座データベース１２８（例えば、固有ＩＤ１１２と多様化係数１５８）に格納する。

【００５５】

図５は、ロジック・フローまたはルーチン５００の実施形態を示す。ロジック・フロー５００は、本明細書で説明する１つ以上の実施形態によって実行される操作の一部またはすべてを表し得る。たとえば、ロジック・フロー５００には、デジタル・ウォレットにアクセスするための操作の一部またはすべてが含まれ得る。実施形態はこの文脈に限定されない。

【００５６】

ブロック５０２では、ルーチン５００は、サーバ１０６によって、コンピューティング装置１０２上で実行されている口座アプリケーション１３６から、暗号文を含むデジタル・ウォレット１４４へのアクセス要求を受信する。ブロック５０４では、サーバ１０６は、マスター鍵１１４、ＵＤＫ１１８、およびカウンタ１１６に基づいて１つ以上の多様化鍵１２０を生成することによって暗号文を復号化し得る。サーバ１０６は、暗号文をさらに検証し、たとえば、サーバ１０６によって生成されたＭＡＣが復号化された暗号文内のＭＡＣと一致するかどうかを判断する。ブロック５０６では、サーバは成功した復号化と検証に基づいて認証を生成し得る。認証は、通常、デジタル・ウォレット１４４への要求されたアクセスが許可されることを示す。ブロック５０８では、サーバは口座アプリケーション１３６に認証を送信する。認証により、口座アプリケーション１３６は、デジタル・ウォレット１４４への要求されたアクセスを許可する。ただし、一部の実施形態では、デジタル・ウォレット１４４にアクセスするために秘密鍵１４６がさらに必要になる。

【００５７】

図６は、ロジック・フローまたはルーチン６００の実施形態を示す。ロジック・フロー６００は、本明細書で説明する１つ以上の実施形態によって実行される操作の一部またはすべてを表し得る。たとえば、ロジック・フロー６００には、デジタル・ウォレットの秘

密鍵を回復するための操作の一部またはすべてが含まれ得る。実施形態はこの文脈に限定されない。

【００５８】

ブロック６０２では、ルーチン６００は、サーバ１０６によって口座アプリケーション１３６から、デジタル・ウォレット１４４の秘密鍵１４６を回復するための要求を受信する。要求には、鍵の多様化に基づいて（たとえば、マスター鍵１１４、ＵＤＫ１１８、および１つ以上の多様化鍵１２０に基づいて）非接触カード１０４によって生成された暗号文が含まれ得る。ブロック６０４では、サーバ１０６は、マスター鍵１１４、ＵＤＫ１１８、およびカウンタ１１６に基づいて１つ以上の多様化鍵１２０を生成することによって暗号文を復号化し得る。サーバ１０６は、暗号文をさらに検証し、たとえば、サーバ１０６によって生成されたＭＡＣが復号化された暗号文内のＭＡＣと一致するかどうかを判断する。

【００５９】

ブロック６０６では、サーバ１０６は、復号化および検証に基づいて、非接触カード１０４の固有ＩＤ１１２と、口座データベース１２８内の多様化係数１５８（たとえば、カウンタ１１６および／またはＰＡＮシーケンス１５６）を決定し得る。ブロック６０８では、サーバ１０６は、固有ＩＤ１１２、多様化係数１５８、および任意のソルト１５４に基づいて秘密鍵１４６を再作成する。いくつかの実施形態では、サーバ１０６は、マスター鍵１１４、固有ＩＤ１１２、多様化係数１５８、および任意のソルト１５４に基づいて秘密鍵１４６を再作成する。いくつかの実施形態では、サーバ１０６は、ＵＤＫ１１８、固有ＩＤ１１２、多様化係数１５８、および任意のソルト１５４に基づいて秘密鍵１４６を再作成する。いくつかの実施形態では、サーバ１０６は、多様化鍵１２０、固有ＩＤ１１２、多様化係数１５８、および任意のソルト１５４に基づいて秘密鍵１４６を再作成する。ブロック６１０では、サーバ１０６は、再作成された秘密鍵１４６をネットワーク経由で口座アプリケーション１３６に送信する。

【００６０】

図７Ａは、非接触カード１０４の構成例を示す概略図７００であり、非接触カード１０４には、非接触カード１０４の前面または背面にサービス・プロバイダのマーク７０２として表示される、サービス・プロバイダによって発行されたクレジット・カード、デビット・カード、ギフト・カードなどの支払いカードが含まれ得る。いくつかの例では、非接触カード１０４は支払いカードとは関係がなく、限定されないが、身分証明書を含み得る。いくつかの例では、取引カードには、デュアル・インターフェイスの非接触支払いカード、ポイント・カードなどが含まれ得る。非接触カード１０４には基板７０４が含まれ、基板７０４にはプラスチック、金属、その他の材料で構成された単層または１つ以上の積層層が含まれ得る。例示的な基板材料としては、ポリ塩化ビニル、ポリ塩化ビニルアセテート、アクリロニトリルブタジエンスチレン、ポリカーボネート、ポリエステル、陽極酸化チタン、パラジウム、金、炭素、紙、および生分解性材料が挙げられる。いくつかの例では、非接触カード１０４は、ＩＳＯ／ＩＥＣ７８１６規格のＩＤ－１形式に準拠した物理的特性を有し、取引カードは、ＩＳＯ／ＩＥＣ１４４４３規格に準拠していることがあり得る。しかしながら、本開示による非接触カード１０４は異なる特性を有する場合があり、本開示では取引カードを支払いカードに実装する必要がないことが理解される。

【００６１】

非接触カード１０４には、カードの表面および／または裏面に表示される識別情報７０６と、接触パッド７０８も含まれ得る。接触パッド７０８には１つ以上のパッドが含まれ、取引カードを介してＡＴＭ、ユーザ装置、スマートフォン、ラップトップ、デスクトップ、またはタブレット・コンピュータなどの別のクライアント装置との接続を確立するように構成し得る。接触パッドは、ＩＳＯ／ＩＥＣ７８１６標準などの１つ以上の標準に従って設計され、ＥＭＶプロトコルに従った通信を可能にする。非接触カード１０４には、図７Ｂでさらに説明するように、処理回路、アンテナ、およびその他のコンポーネントも含まれ得る。これらのコンポーネントは、接触パッド７０８の背後、または基板７０４上

の他の場所（たとえば、基板７０４の別の層内）に配置され、接触パッド７０８と電気的および物理的に結合され得る。非接触カード１０４には、磁気ストリップまたはテープも含まれており、これらはカードの裏面に配置され得る（図７Ａには示されていない）。非接触カード１０４には、ＮＦＣプロトコルを介して通信可能なアンテナと結合された近距離無線通信（ＮＦＣ）装置も含まれ得る。実施形態は、この方法に限定されるわけではない。

【００６２】

図７Ｂに示すように、非接触カード１０４の接触パッド７０８には、プロセッサ７１２、メモリ１０８、および１つ以上の通信インターフェイス１２４を含む、情報を保存、処理、および通信するための処理回路７１０が含まれ得る。処理回路７１０には、本明細書で説明する機能を実行するために必要な、プロセッサ、メモリ、エラーおよびパリティ／ＣＲＣチェッカー、データ・エンコーダ、衝突防止アルゴリズム、コントローラ、コマンド・デコーダ、セキュリティ・プリミティブ、および改ざん防止ハードウェアなどの追加コンポーネントが含まれる場合があることが理解される。

【００６３】

メモリ１０８は、読み取り専用メモリ、追記型メモリ、読み取り／書き込み型メモリ、たとえばＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭなどであり、非接触カード１０４にはこれらのメモリが１つ以上含まれ得る。読み取り専用メモリは、読み取り専用または１回限りのプログラム可能として工場でプログラムし得る。ワンタイム・プログラミングにより、一度書き込んでから何度も読み取る機会が提供される。一度書き込み／複数回読み取り可能なメモリは、メモリ・チップが工場を出荷された後の時点でプログラムされ得る。メモリは一度プログラムされると、書き換えることはできないが、何度も読み取り得る。読み取り／書き込みメモリは、工場出荷後、何度もプログラムおよび再プログラムされ得る。読み取り／書き込みメモリは、工場出荷後も何度も読み取られ得る。場合によっては、メモリ１０８は、プロセッサ７１２によって実行される暗号化アルゴリズムを使用してデータを暗号化する暗号化メモリであり得る。

【００６４】

メモリ１０８は、１つ以上のアプレット１１０、１つ以上のカウンタ１１６、固有ＩＤ１１２、マスター鍵１１４、ＵＤＫ１１８、多様化鍵１２０、およびＰＡＮシーケンス１５６を格納するように構成し得る。１つ以上のアプレット１１０は、Ｊａｖａ（登録商標）Ｃａｒｄアプレットなど、１つ以上の非接触カード１０４上で実行するように構成された１つ以上のソフトウェア・アプリケーションで構成される。ただし、アプレット１１０はＪａｖａ　Ｃａｒｄアプレットに限定されず、非接触カードまたはメモリが制限された他の装置上で動作可能な任意のソフトウェア・アプリケーションであってもよいことが理解される。１つ以上のカウンタ１１６は、整数を格納するのに十分な数値カウンタを含み得る。固有ＩＤ１１２は、非接触カード１０４に割り当てられた固有の英数字識別子で構成され、この識別子によって非接触カード１０４が他の非接触カード１０４と区別される。いくつかの例では、固有ＩＤ１１２は、顧客とその顧客に割り当てられたアカウントの両方を識別し得る。

【００６５】

前述の例示的な実施形態のプロセッサ７１２およびメモリ要素は、接触パッド７０８を参照して説明されているが、本開示はこれに限定されない。これらの要素は、接触パッド７０８の外部に実装することも、完全に別個に実装することも、または接触パッド７０８内に配置されたプロセッサ７１２およびメモリ１０８要素に加えて追加の要素として実装することもできることが理解される。

【００６６】

いくつかの例では、非接触カード１０４は１つ以上のアンテナ７１４を備え得る。１つまたは複数のアンテナ７１４は、非接触カード１０４内および接触パッド７０８の処理回路７１０の周囲に配置され得る。たとえば、１つ以上のアンテナ７１４は、処理回路７１０と一体化されていてもよく、１つ以上のアンテナ７１４は、外部ブースタ・コイルと共

に使用され得る。別の例として、１つ以上のアンテナ７１４は、接触パッド７０８および処理回路７１０の外部にあってもよい。

【００６７】

一実施形態では、非接触カード１０４のコイルは、空芯変圧器の二次側として機能し得る。端末は、電力を遮断するか、振幅変調することによって非接触カード１０４と通信し得る。非接触カード１０４は、１つ以上のコンデンサを通じて機能的に維持される非接触カード１０４の電源接続のギャップを使用して、端末から送信されたデータを推測し得る。非接触カード１０４は、非接触カード１０４のコイルの負荷を切り替えるか、負荷変調することによって通信を返信し得る。干渉により端末のコイルで負荷変調が検出され得る。より一般的には、アンテナ７１４、プロセッサ７１２、および／またはメモリ１０８を使用して、非接触カード１０４は、ＮＦＣ、Ｂｌｕｅｔｏｏｔｈ、および／またはＷｉ－Ｆｉ通信を介して通信するための通信インターフェイスを提供する。

【００６８】

上述したように、非接触カード１０４は、スマート・カードまたはＪａｖａ　Ｃａｒｄなどのメモリが制限された他の装置上で動作可能なソフトウェア・プラットフォーム上に構築され、１つ以上のアプリケーションまたはアプレットを安全に実行し得る。アプレット１１０を非接触カードに追加して、さまざまなモバイル・アプリケーションベースのユース・ケースで多要素認証（ＭＦＡ：ＭｕｌｔｉＦａｃｔｏｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）用のワンタイム・パスワード（ＯＴＰ：Ｏｎｅ－Ｔｉｍｅ　Ｐａｓｓｗｏｒｄ）を提供し得る。アプレット１１０は、モバイルＮＦＣリーダ（モバイル・コンピューティング装置１０２またはＰＯＳ端末など）などのリーダからの１つ以上の要求（近距離データ交換要求など）に応答し、ＮＤＥＦテキスト・タグとしてエンコードされた暗号化された安全なＯＴＰを含むＮＤＥＦメッセージを生成するように構成し得る。ＮＤＥＦメッセージには、暗号文１２２や暗号文２０８などの暗号文やその他のデータが含まれ得る。

【００６９】

ＮＤＥＦ　ＯＴＰの一例は、ＮＤＥＦショートレコードレイアウト（ＳＲ＝１）である。このような例では、１つ以上のアプレット１１０が、ＯＴＰをＮＤＥＦタイプ４の既知のタイプのテキスト・タグとしてエンコードするように構成され得る。いくつかの例では、ＮＤＥＦメッセージは１つ以上のレコードで構成され得る。アプレット１１０は、ＯＴＰレコードに加えて１つ以上の静的タグレコードを追加するように構成し得る。

【００７０】

いくつかの例では、１つ以上のアプレット１１０は、ＲＦＩＤタグをエミュレートするように構成され得る。ＲＦＩＤタグには、１つ以上の多形性タグが含まれ得る。いくつかの例では、タグが読み取られるたびに、非接触カードの信頼性を示す可能性のある異なる暗号データが提示される。１つ以上のアプレット１１０に基づいて、タグのＮＦＣ読み取りが処理され、データが銀行システムのサーバなどのサーバに送信され、データがサーバで検証され得る。

【００７１】

いくつかの例では、非接触カード１０４およびサーバには、カードが適切に識別されるように特定のデータが含まれ得る。非接触カード１０４には、１つ以上の固有識別子（図示せず）が含まれ得る。読み取り操作が行われるたびに、カウンタ１１６が増加するように構成され得る。いくつかの例では、非接触カード１０４からのデータが読み取られるたびに（たとえば、モバイル装置によって）、カウンタ１１６が検証のためにサーバに送信され、カウンタ１１６が（検証の一部として）サーバのカウンタと等しいかどうかが判断される。

【００７２】

１つ以上のカウンタ１１６は、リプレイ攻撃を防止するように構成され得る。たとえば、暗号文が取得され再生された場合、カウンタ１１６が読み取られたり、使用されたり、あるいはその他の方法で渡されたりすると、その暗号文は直ちに拒否される。カウンタ１１６が使用されていない場合は、再プレイし得る。いくつかの例では、非接触カード１０

４上で増加されるカウンタは、取引に対して増加されるカウンタとは異なる。非接触カード１０４上のアプレット１１０間に通信がないため、非接触カード１０４はアプリケーション取引カウンタ１１６を判別できない。いくつかの例では、非接触カード１０４は、取引アプレットである第１アプレット４４０－１と、第２アプレット４４０－２とを含み得る。各アプレット４４０－１および４４０－２は、それぞれカウンタ１１６を含み得る。

【００７３】

いくつかの例では、カウンタ１１６が同期しなくなり得る。いくつかの例では、斜めからの読み取りなど、取引を開始する偶発的な読み取りを考慮すると、カウンタ１１６は増加するが、アプリケーションはカウンタ１１６を処理しないことがあり得る。いくつかの例では、装置１０２が起動されると、ＮＦＣが有効になり、コンピューティング装置１０２は利用可能なタグを読み取るように構成され得るが、読み取りに応答するアクションは実行されない。

【００７４】

カウンタ１１６を同期状態に保つために、バックグラウンド・アプリケーションなどのアプリケーションが実行され、コンピューティング装置１０２が起動したことを検知し、検知によって読み取りが発生したことを示す銀行システムのサーバと同期してカウンタ１１６を進めるように構成される。他の例では、ハッシュ化されたワンタイム・パスワードが利用され、誤った同期のウィンドウが受け入れられ得る。たとえば、しきい値１０以内の場合、カウンタ１１６は前進するように構成し得る。ただし、異なるしきい値数内、たとえば１０または６００以内であれば、ユーザが装置を介して１回以上タップ、ジェスチャ、またはその他の方法で指示する１つ以上のアプリケーションを介して要求される再同期の実行要求が処理され得る。カウンタ１１６が適切な順序で増加すると、ユーザがその操作を実行したことを知り得る。

【００７５】

カウンタ１１６、マスター鍵１１４、ＵＤＫ１１８、および多様化鍵１２０を参照して本明細書で説明する鍵多様化技術は、暗号化および／または復号化鍵多様化技術の一例である。この例の鍵多様化手法は、他の種類の鍵多様化手法にも同様に適用されるため、開示を制限するものとは見なされない。

【００７６】

非接触カード１０４の作成プロセス中に、カードごとに２つの暗号鍵が一意に割り当てられ得る。暗号鍵は、データの暗号化と復号化の両方に使用できる対称鍵で構成され得る。ＥＭＶではトリプルＤＥＳ（３ＤＥＳ）アルゴリズムが使用され得るものであり、これは非接触カード１０４のハードウェアによって実装される。鍵多様化プロセスを使用すると、鍵を必要とする各エンティティの一意に識別可能な情報に基づいて、マスター鍵から１つ以上の鍵を派生し得る。

【００７７】

いくつかの例では、脆弱性の影響を受けやすい可能性がある３ＤＥＳアルゴリズムの欠陥を克服するために、セッション鍵が導出され得る（セッションごとに固有鍵など）が、マスター鍵を使用するのではなく、固有のカード導出鍵（ＵＤＫ１１８など）とカウンタが多様化データとして使用され得る。たとえば、非接触カード１０４が動作中に使用されるたびに、メッセージ認証コード（ＭＡＣ）の作成と暗号化の実行に異なる鍵が使用され得る。これにより、暗号化は３層になる。セッション鍵は、１つ以上のアプレットによって生成され、１つ以上のアルゴリズム（ＥＭＶ　４．３　Ｂｏｏｋ　２　Ａ１．３．１共通セッション鍵導出の定義）を備えたアプリケーション取引カウンタを使用して導出される。

【００７８】

さらに、各カードの増分は一意であり、パーソナライゼーションによって割り当てられるか、または何らかの識別情報によってアルゴリズム的に割り当てられる。たとえば、奇数カードは２増加し、偶数カードは５増加し得る。いくつかの例では、増分は連続読み取りでも変化する可能性があり、１枚のカードが１、３、５、２、２、…　と順番に増加し

、それが繰り返され得る。特定のシーケンスまたはアルゴリズム・シーケンスは、パーソナライゼーション時に定義することも、固有識別子から派生した１つ以上のプロセスから定義し得る。これにより、リプレイ攻撃者が少数のカード・インスタンスから一般化することが難しくなる。

【００７９】

認証メッセージは、１６進ＡＳＣＩＩ形式のテキストＮＤＥＦレコードの内容として配信され得る。別の例では、ＮＤＥＦレコードは１６進形式でエンコードされ得る。

【００８０】

図８は、一実施例によるＮＤＥＦショートレコードレイアウト（ＳＲ＝１）データ構造８００を示す。１つ以上のアプレット１１０は、ＯＴＰをＮＤＥＦタイプ４の既知のタイプのテキスト・タグとしてエンコードするように構成し得る。一部の例では、ＮＤＥＦメッセージは１つ以上のレコードで構成される。アプレットは、ＯＴＰレコードに加えて１つ以上の静的タグレコードを追加するように構成し得る。例示的なタグには、以下が含まれる。タグ・タイプ：既知のタイプ、テキスト、エンコード英語（ｅｎ）；アプレットＩＤ：Ｄ２７６０００００８５０１０１；機能：読み取り専用アクセス；エンコード：認証メッセージはＡＳＣＩＩ１６進数としてエンコードし得る；タイプ長値（ＴＬＶ：Ｔｙｐｅ－Ｌｅｎｇｔｈ－Ｖａｌｕｅ）データは、ＮＤＥＦメッセージの生成に使用できるパーソナライズパラメータとして提供され得る（ただし、これらに限定されない）。一実施形態では、認証テンプレートは、実際の動的認証データを提供するための既知のインデックスを備えた最初のレコードを含み得る。データ構造８００には、暗号文１２２や暗号文２０８などの暗号文、およびアプレット１１０によって提供されるその他のデータが含まれ得る。

【００８１】

図９は、開示された実施形態と一致する例示的なシステム９００の概略図を示す。システム９００は、ネットワーク９０２を介してブロックチェーン９０６にアクセスできるシステムで構成され得る。

【００８２】

システム９００は、ブロックチェーン９０６を使用して、信頼性のないやり取りの記録を生成し得る。さらに、ブロックチェーン９０６は複数のコンピューティング・システムに分散でき、ブロックチェーン９０６に格納された記録の有効性に対する信頼を高めることができる。このように、開示されたシステムは、従来のシステムにおける少なくとも上記の技術的問題に対する革新的な技術的解決策を提供する。

【００８３】

ユーザ・システム９０４には、コンピューティング装置１０２が含まれ得る。ユーザ・システム９０４は、開示された実施形態に従って、デジタル・ウォレット１４４を使用して取引を処理するように構成され得る。ユーザ・システム９０４は、サーバ、ワークステーション、デスクトップ、またはモバイル装置（ラップトップ、タブレット、ファブレット、スマートフォン、スマートウォッチ、または同様のモバイル・コンピューティング装置など）などのコンピューティング装置で構成され得る。図１２に関して以下で説明するように、ユーザ・システム９０４は、ディスプレイおよび入出力インターフェイスを備えて構成され得る。ユーザ・システム９０４は、ディスプレイおよび入出力インターフェイスを使用してユーザ（図示せず）と対話するように構成し得る。

【００８４】

メンバ・システム９０８は、開示された実施形態に従って取引を処理するように構成され得る。メンバ・システム９０８には、サーバ、ワークステーション、デスクトップ・コンピュータ、または専用コンピューティング装置などの１つ以上のコンピューティング装置が含まれ得る。メンバ・システム９０８はスタンドアロンである場合もあれば、サブシステムの一部である場合もあり、サブシステムはより大きなシステムの一部である場合もある。たとえば、メンバ・システム９０８は商業機関に関連付けられ得る。メンバ・システム９０８には、リモートに配置され、パブリック・ネットワークまたは専用のプライベ

ート・ネットワークを介して金融機関の他のシステムと通信する分散サーバが含まれ得る。

【００８５】

メンバ・システム９０８は、デジタル・ウォレット１４４の暗号通貨を使用して取引を処理する要求を受信するように構成され得る。いくつかの実施形態では、メンバ・システム９０８は、別のメンバ・システム９０８やユーザ・システム９０４など、システム９００の別の要素からの要求を受信するように構成され得る。メンバ・システム９０８は、ブロックチェーン９０６と対話して取引要求を処理するように構成され得る。

【００８６】

メンバ・システム９０８は、開示された実施形態に従って、ブロックチェーン９０６にメッセージを格納するように構成し得る。いくつかの側面では、メンバ・システム９０８は、メッセージを含むブロックをブロックチェーン９０６に追加するように構成され得る。さまざまな側面において、メンバ・システム９０８は、許可されたシステムにメッセージを提供するように構成され得る。認証されたシステムは、メッセージを含むブロックをブロックチェーン９０６に追加するように構成され得る。図１０に関して以下で説明するように、メッセージは取引記録を含み得る。

【００８７】

ブロックチェーン９０６は、開示された実施形態と一致する分散データ構造を備え得る。ブロックチェーン９０６はプライベート・ブロックチェーンであり得る。たとえば、認証されたシステムはブロックチェーン９０６のコピーを保存し得る。これらの認証されたシステムは、ブロックチェーン９０６にブロックを追加し、そのブロックを他の認証されたシステムに公開するように構成し得る。認証されたシステムは、ブロックチェーン９０６に公開するために他のシステムからメッセージを受信するように構成し得る。これらの他のシステムは、ブロックチェーン９０６への読み取り専用アクセス権を持ち得る。いくつかの実施形態では、１つ以上のメンバ・システム９０８は、認証されたシステムである。いくつかの実施形態では、１つ以上のユーザ・システム９０４は、認証されたシステムである。図９に関して詳細に説明したように、ブロックチェーン９０６は、メンバ・システムからのメッセージ（取引を含む）を格納するように構成し得る。

【００８８】

ネットワーク９０２は、図９のコンポーネント間の通信を提供するように構成され得る。たとえば、ネットワーク９０２は、インターネット、ローカル・エリア・ネットワーク、または認証システム９００が認証システム９００のコンポーネント間で情報を送受信できるようにするその他の適切な接続など、通信を提供し、情報を交換し、および／または情報交換を容易にする任意のタイプのネットワーク（インフラストラクチャを含む）であり得る。

【００８９】

図１０は、開示された実施形態と一致する例示的なブロックチェーン９０６の論理モデル１０００を示す。ブロックチェーン９０６は、多くの異なるシステム（たとえば、メンバ・システム９０８または他のシステム）によって維持される多数のこのようなブロックチェーンを備え得る。このような例示的なブロックチェーンは、ブロック１００６ａからブロック１００６ｄなどのブロックを備え得る。ブロックには、メッセージ１００８ａからメッセージ１００８ｄなどのメッセージが含まれ得る。一般に、ブロックには、各ブロックを一意に識別するヘッダ（ヘッダ１００２ａから１００２ｄなど）が含まれ得る。ヘッダ１００２ａから１００２ｄには、ハッシュ関数によって生成されたハッシュ値が含まれ得る。ハッシュ関数は、任意のサイズの入力データを固定サイズのハッシュ値にマッピングするために使用できる関数である。たとえば、ヘッダには、前のブロックのハッシュ値、ブロック内のメッセージに基づいて生成されたハッシュ値（Ｍｅｒｋｌｅルートなど）、およびタイムスタンプの少なくとも１つが含まれ得る。開示された実施形態と一致して、システム９００は、ブロックチェーン９０６に追加されたブロックが作業証明条件とデジタル署名条件の少なくとも１つを満たすことを要求し得る。たとえば、ヘッダ１００

２ａから１００２ｄには、ヘッダがプルーフ・オブ・ワーク条件１００４ａから１００４ｄを満たすことを保証するために選択されたｎｏｎｃｅが含まれる場合があります。限定されない例として、プルーフ・オブ・ワーク条件１００４ａから１００４ｄでは、ヘッダのハッシュが所定の値の範囲内に収まることが要求され得る。追加の例として、ヘッダは、認証されたシステムの暗号鍵（例えば、秘密鍵１４６）を使用してデジタル署名され、デジタル署名がヘッダ内に含まれ得る。このデジタル署名は、システム９００のメンバが利用できる鍵を使用して検証し得る。

【００９０】

図１１は、開示された実施形態と一致する、ブロックチェーン（例えば、ブロックチェーン９０６の要素）に格納されたメッセージ１００８ｂの論理モデル１１００を示す。いくつかの実施形態では、メッセージ１００８ｂはインデックス情報１１０２を備え得る。特定の態様では、インデックス情報１１０２は、ユーザを識別する情報を備え得る。たとえば、インデックス情報１１０２は、ユーザのフルネーム、電子メールアドレス、電話番号、またはその他の機密性のない個人情報のうちの少なくとも１つであり得る。さまざまな側面において、インデックス情報１１０２には、プライベート・ブロックチェーン内の以前のブロックへの１つ以上の参照が含まれ得る。たとえば、インデックス情報１１０２には、同じユーザに関連付けられた１つ以上の以前のブロックへの１つ以上の参照が含まれ得る。参照には、限定されない例として、同じユーザに関連付けられたブロックチェーン内の前のブロックのハッシュが含まれ得る。いくつかの側面では、インデックス情報１１０２は、当業者に知られている方法に従って難読化または暗号化され得る。たとえば、インデックス情報１１０２は、秘密鍵１４６などの暗号鍵を使用して暗号化され得る。追加の例として、インデックス情報１１０２は、ユーザのフルネーム、電子メールアドレス、電話番号、またはその他の機密性のない個人情報のうちの少なくとも１つのハッシュを備え得る。

【００９１】

メッセージ１００８ｂは、開示された実施形態に従って、追加情報１１０４を備え得る。追加情報１１０４には、あるデジタル・ウォレット１４４から別のデジタル・ウォレット１４４に転送される暗号通貨の金額などの取引の詳細が含まれ得る。さまざまな側面において、追加情報１１０４は、当業者に知られている方法に従って難読化または暗号化され得る。たとえば、ルートシステム情報１１０４は、秘密鍵１４６などの暗号化鍵を使用して暗号化され得る。

【００９２】

メッセージ１００８ｂは、開示された実施形態と一致して、認証レコード１１０６を備え得る。いくつかの側面では、認証レコード１１０６は、取引のその後の監査を可能にする情報を備え得る。たとえば、認証レコード１１０６は、メンバ・システム９０８、メンバ・システム９０８に関連付けられた商業機関、認証レコード１１０６の目的（例：取引の詳細）のうち少なくとも１つを識別し得る。いくつかの側面では、認証レコード１１０６は、当業者に知られている方法に従って難読化または暗号化され得る。たとえば、認証レコード１１０６は、秘密鍵１４６などの暗号化鍵を使用して暗号化され得る。

【００９３】

開示された実施形態と一致して、秘密鍵１４６などの暗号化鍵は、ブロック内のメッセージの要素を暗号化するために使用し得る。いくつかの側面では、このような暗号鍵は、認証システム９００のメンバ（たとえば、メンバ・システム９０８）に関連付けられ得る。さまざまな側面において、少なくとも一部の暗号鍵は、認証されたシステムに関連付けられ得る。開示された実施形態と一致して、公開鍵１４８などの対応する暗号化鍵を使用して、暗号化されたメッセージ要素を復号化できる場合がある。たとえば、ブロック内のメッセージの要素が対称鍵で暗号化されている場合、同じ対称鍵を使用して暗号化された要素を復号化できる場合がある。別の例として、ブロック内のメッセージの要素が秘密鍵１４６で暗号化されている場合、対応する公開鍵１４８を使用して暗号化された要素を復号化できる場合がある。いくつかの側面では、対応する暗号鍵は、認証システムのメンバ

ー（たとえば、メンバ・システム９０８）が利用できる場合がある。
【００９４】
図１２は、前述の様々な実施形態を実装するのに適した例示的なコンピュータ・アーキテクチャ１２００の実施形態を示す。一実施形態では、コンピュータ・アーキテクチャ１２００は、コンピューティング・アーキテクチャ１００を含むか、またはコンピューティング・アーキテクチャ１００の一部として実装され得る。
【００９５】
このアプリケーションで使用される「システム」および「コンポーネント」という用語は、ハードウェア、ハードウェアとソフトウェアの組み合わせ、ソフトウェア、または実行中のソフトウェアのいずれかのコンピュータ関連のエンティティを指すことを意図しており、その例は、例示的なコンピューティング・コンピュータアーキテクチャ１２００によって提供される。たとえば、コンポーネントには、プロセッサ上で実行されるプロセス、プロセッサ、ハード・ディスク・ドライブ、複数のストレージ・ドライブ（光学式および／または磁気式ストレージ・メディア）、オブジェクト、実行可能ファイル、実行スレッド、プログラム、および／またはコンピュータなどがありますが、これらに限定されない。例として、サーバ上で実行されているアプリケーションとサーバの両方がコンポーネントになることができる。１つ以上のコンポーネントがプロセスおよび／または実行スレッド内に存在でき、コンポーネントは１台のコンピュータにローカライズすることも、２台以上のコンピュータに分散することもできまる。さらに、コンポーネントは、操作を調整するために、さまざまな種類の通信メディアによって相互に通信的に結合され得る。調整には、一方向または双方向の情報交換が含まれ得る。たとえば、コンポーネントは、通信メディアを介して通信される信号の形式で情報を通信し得る。情報は、さまざまな信号線に割り当てられた信号として実装できる。このような割り当てでは、各メッセージは信号になる。しかしながら、さらなる実施形態では、データ・メッセージを代わりに使用し得る。このようなデータ・メッセージは、さまざまな接続を介して送信される可能性があります。例示的な接続には、パラレル・インターフェイス、シリアル・インターフェイス、およびバス・インターフェイスが含まれます。
【００９６】
コンピュータ・アーキテクチャ１２００には、１つ以上のプロセッサ、マルチ・コア・プロセッサ、コ・プロセッサ、メモリ・ユニット、チップ・セット、コントローラ、周辺機器、インターフェイス、発振器、タイミング装置、ビデオ・カード、オーディオ・カード、マルチメディア入出力（Ｉ／Ｏ）コンポーネント、電源などのさまざまな一般的なコンピューティング要素が含まれる。しかしながら、実施形態は、コンピューティング・コンピュータ・アーキテクチャ１２００による実装に限定されない。
【００９７】
図１２に示すように、コンピュータ・アーキテクチャ１２００は、プロセッサ１２０２、システム・メモリ１２０４、およびシステム・バス１２０６を含むコンピュータ１２１２を含む。プロセッサ１２０２は、市販されているさまざまなプロセッサのいずれかになり得る。コンピュータ１２１２は、コンピューティング装置１０２および／またはサーバ１０６を表し得る。
【００９８】
システム・バス１２０６は、システム・メモリ１２０４からプロセッサ１２０２までを含むシステム・コンポーネント用のインターフェイスを提供する。システム・バス１２０６は、市販されているさまざまなバス・アーキテクチャのいずれかを使用して、メモリ・バス（メモリ・コントローラの有無にかかわらず）、周辺バス、およびローカル・バスにさらに相互接続できる、いくつかの種類のバス構造のいずれかになり得る。インターフェイス・アダプタは、スロット・アーキテクチャを介してシステム・バス１２０６に接続し得る。スロット・アーキテクチャの例には、Ａｃｃｅｌｅｒａｔｅｄ　Ｇｒａｐｈｉｃｓ　Ｐｏｒｔ　（ＡＧＰ）、カード・バス、（拡張）業界標準アーキテクチャ（（Ｅ）ＩＳＡ）、マイクロ・チャネル・アーキテクチャ（ＭＣＡ）、ＮｕＢｕｓ、Ｐｅｒｉｐｈｅｒａ

ｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ （Ｅｘｔｅｎｄｅｄ） （ＰＣＩ（Ｘ））、ＰＣＩ Ｅｘｐｒｅｓｓ、Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ Ｍｅｍｏｒｙ Ｃａｒｄ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ａｓｓｏｃｉａｔｉｏｎ（ＰＣＭＣＩＡ）などが含まれるが、これらに限定されない。

【００９９】

コンピュータ・アーキテクチャ１２００には、さまざまな製造品が含まれたり、実装されたりする場合がある。製造物には、ロジックを保存するためのコンピュータ読み取り可能な記憶媒体が含まれ得る。コンピュータ読み取り可能な記憶媒体の例には、揮発性メモリまたは不揮発性メモリ、取り外し可能または取り外し不可能なメモリ、消去可能または消去不可能なメモリ、書き込み可能または再書き込み可能なメモリなど、電子データを保存できる任意の有形媒体が含まれる。ロジックの例には、ソース・コード、コンパイルされたコード、解釈されたコード、実行可能コード、静的コード、動的コード、オブジェクト指向コード、ビジュアル・コードなどの任意の適切なタイプのコードを使用して実装された実行可能なコンピュータ・プログラム命令が含まれ得る。実施形態は、少なくとも部分的に、非一時的なコンピュータ読み取り可能な媒体に含まれる命令として実装されることもあり、その命令は、１つ以上のプロセッサによって読み取られ、実行されて、本明細書で説明される操作の実行をし得る。

【０１００】

システム・メモリ１２０４には、読み取り専用メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、ダイナミックＲＡＭ （ＤＲＡＭ）、ダブル・データ・レートＤＲＡＭ （ＤＤＲＡＭ）、同期ＤＲＡＭ （ＳＤＲＡＭ）、スタティックＲＡＭ （ＳＲＡＭ）、プログラマブルＲＯＭ （ＰＲＯＭ）、消去可能プログラマブルＲＯＭ （ＥＰＲＯＭ）、電気的に消去可能プログラマブルＲＯＭ （ＥＥＰＲＯＭ）、フラッシュ・メモリ、強誘電体ポリマー・メモリなどのポリマー・メモリ、オボニック・メモリ、相変化または強誘電体メモリ、シリコン酸化物窒化物酸化物シリコン（ＳＯＮＯＳ）メモリ、磁気カードまたは光カード、冗長独立ディスク・アレイ（ＲＡＩＤ）ドライブなどの装置のアレイ、ソリッド・ステート・メモリ装置（ＵＳＢメモリ、ソリッド・ステート・ドライブ（ＳＳＤ）など）、および情報の保存に適したその他のタイプのストレージ・メディアなど、１つ以上の高速メモリ・ユニットの形式でさまざまな種類のコンピュータ読み取り可能なストレージ・メディアが含まれ得る。図１２に示す実施形態では、システム・メモリ１２０４は不揮発性メモリ１２０８および／または揮発性メモリ１２１０を含むことができる。基本入出力システム（ＢＩＯＳ）は不揮発性メモリ１２０８に保存できる。

【０１０１】

コンピュータ１２１２には、内部（または外部）ハード・ディスク・ドライブ１２１４、取り外し可能な磁気ディスク１２１８の読み取りまたは書き込みを行う磁気ディスク・ドライブ１２１６、取り外し可能な光ディスク１２２２（ＣＤ－ＲＯＭやＤＶＤなど）の読み取りまたは書き込みを行う光ディスク・ドライブ１２２０など、１つ以上の低速メモリ・ユニットの形式でさまざまな種類のコンピュータ読み取り可能な記憶媒体が含まれ得る。ハード・ディスク・ドライブ１２１４、磁気ディスク・ドライブ１２１６、および光ディスク・ドライブ１２２０は、それぞれＨＤＤインターフェイス１２２４、ＦＤＤインターフェイス１２２６、および光ディスク・ドライブ・インターフェイス１２２８によってシステム・バス１２０６に接続できる。外部ドライブ実装用のＨＤＤインターフェイス１２２４には、ユニバーサル・シリアル・バス（ＵＳＢ）インターフェイス・テクノロジとＩＥＥＥ １３９４インターフェイス・テクノロジの少なくとも１つまたは両方を含めることができる。

【０１０２】

ドライブおよび関連するコンピュータ読み取り可能なメディアは、データ、データ構造、コンピュータ実行可能命令などの揮発性および／または不揮発性ストレージを提供する。たとえば、オペレーティング・システム１２３０、１つ以上のアプリケーション１２３２、その他のプログラム・モジュール１２３４、およびプログラム・データ１２３６を含

む多数のプログラム・モジュールをドライブおよび不揮発性メモリ１２０８と揮発性メモリ１２１０に格納できる。一実施形態では、１つ以上のアプリケーション１２３２、他のプログラム・モジュール１２３４、およびプログラム・データ１２３６には、例えば、システム１００のさまざまなアプリケーションおよび／またはコンポーネントが含まれ得る。

【０１０３】

ユーザは、キーボード１２３８やマウス１２４０などのポインティング装置など、１つ以上の有線／無線入力装置を介して、コンピュータ１２１２にコマンドや情報を入力できる。その他の入力装置には、マイク、赤外線（ＩＲ）リモート・コントロール、無線周波数（ＲＦ）リモート・コントロール、ゲーム・パッド、スタイラス・ペン、カード・リーダ、ドングル、指紋リーダ、手袋、グラフィック・タブレット、ジョイスティック、キーボード、網膜リーダ、タッチ・スクリーン（静電容量式、抵抗式など）、トラックボール、トラック・パッド、センサ、スタイラスなどが含まれる。これらおよびその他の入力装置は、システム・バス１２０６に結合された入力装置インターフェイス１２４２を介してプロセッサ１２０２に接続されることが多いが、パラレル・ポート、ＩＥＥＥ１３９４シリアル・ポート、ゲーム・ポート、ＵＳＢポート、ＩＲインターフェイスなどの他のインターフェイスによって接続することもできる。

【０１０４】

モニタ１２４４または他のタイプのディスプレイ装置も、ビデオ・アダプタ１２４６などのインターフェイスを介してシステム・バス１２０６に接続される。モニタ１２４４はコンピュータ１２１２の内部または外部に配置し得る。コンピュータには通常、モニタ１２４４に加えて、スピーカ、プリンタなどの他の周辺出力装置が含まれる。

【０１０５】

コンピュータ１２１２は、リモート・コンピュータ１２４８などの１台以上のリモート・コンピュータへの有線および／または無線通信による論理接続を使用して、ネットワーク環境で動作し得る。リモート・コンピュータ１２４８は、ワークステーション、サーバ・コンピュータ、ルータ、パーソナル・コンピュータ、ポータブル・コンピュータ、マイクロプロセッサ・ベースのエンターテイメント機器、ピア装置、またはその他の共通ネットワーク・ノードであり、通常はコンピュータ１２１２に関連して説明した要素の多くまたはすべてを含むが、簡潔にするために、メモリおよび／またはストレージ装置１２５０のみが示されている。図示の論理接続には、ローカル・エリア・ネットワーク１２５２や、たとえばワイド・エリア・ネットワーク１２５４などのより大規模なネットワークへの有線／無線接続が含まれる。このようなＬＡＮおよびＷＡＮネットワーク環境は、オフィスや企業では一般的であり、イントラネットなどの企業全体のコンピュータ・ネットワークを促進し、これらのネットワークはすべて、インターネットなどのグローバル通信ネットワークに接続し得る。

【０１０６】

ローカル・エリア・ネットワーク１２５２のネットワーク環境で使用される場合、コンピュータ１２１２は、有線および／または無線通信ネットワーク・インターフェイスまたはネットワーク・アダプタ１２５６を介してローカル・エリア・ネットワーク１２５２に接続される。ネットワーク・アダプタ１２５６は、ローカル・エリア・ネットワーク１２５２への有線および／または無線通信を容易にでき、ローカル・エリア・ネットワーク１２５２には、ネットワーク・アダプタ１２５６の無線機能と通信するために、その上に配置された無線アクセスポイントも含み得る。

【０１０７】

ワイド・エリア・ネットワーク１２５４のネットワーキング環境で使用される場合、コンピュータ１２１２は、モデム１２５８を含むことができ、またはワイド・エリア・ネットワーク１２５４上の通信サーバに接続され、またはインターネットによるなど、ワイド・エリア・ネットワーク１２５４を介して通信を確立するための他の手段を有する。モデム１２５８は、内部または外部、および有線装置および／または無線装置であることがで

き、入力装置インターフェイス１２４２を介してシステム・バス１２０６に接続する。ネットワーク化された環境では、コンピュータ１２１２に関連して描かれたプログラム・モジュール、またはその一部は、リモート・メモリおよび／またはストレージ装置１２５０に記憶され得る。示されたネットワーク接続は例示的なものであり、コンピュータ間の通信リンクを確立する他の手段を使用できることが理解されよう。

【０１０８】

コンピュータ１２１２は、ワイヤレス通信（例：ＩＥＥＥ８０２．１１無線変調技術）で動作可能に配置されたワイヤレス装置など、ＩＥＥＥ８０２ファミリの規格を使用する有線およびワイヤレス装置またはエンティティと通信するように動作可能である。これには、少なくともＷｉ－Ｆｉ（登録商標）（またはＷｉｒｅｌｅｓｓ　Ｆｉｄｅｌｉｔｙ）、ＷｉＭａｘ、およびＢｌｕｅｔｏｏｔｈ（登録商標）ワイヤレス技術などが含まれる。このように、通信は、従来のネットワークのようにあらかじめ定義された構造であることも、少なくとも２つの装置間の単なるアドホック通信であることもあり得る。Ｗｉ－Ｆｉネットワークは、ＩＥＥＥ８０２．１１（ａ、ｂ、ｇ、ｎ、ａｃ、ａｘなど）と呼ばれる無線技術を使用し、安全で信頼性が高く、高速なワイヤレス接続を提供する。Ｗｉ－Ｆｉネットワークは、コンピュータ同士やインターネット、有線ネットワーク（ＩＥＥＥ８０２．３関連のメディアと機能を使用するもの）との接続に使用できる。

【０１０９】

図１Ａ～図１２を参照して先に説明したような装置の様々な要素は、様々なハードウェア要素、ソフトウェア要素、または両方の組み合わせを含み得る。ハードウェア要素の例としては、装置、論理装置、コンポーネント、プロセッサ、マイクロプロセッサ、回路、プロセッサ、回路要素（たとえば、トランジスタ、抵抗器、コンデンサ、インダクタなど）、集積回路、特定用途向け集積回路（ＡＳＩＣ）、プログラマブル論理装置（ＰＬＤ）、デジタル信号プロセッサ（ＤＳＰ）、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、メモリ・ユニット、論理ゲート、レジスタ、半導体装置、チップ、マイクロチップ、チップ・セットなどを含み得る。ソフトウェア要素の例としては、ソフトウェア・コンポーネント、プログラム、アプリケーション、コンピュータ・プログラム、アプリケーション・プログラム、システム・プログラム、ソフトウェア開発プログラム、マシン・プログラム、オペレーティング・システム・ソフトウェア、ミドルウェア、ファームウェア、ソフトウェア・モジュール、ルーチン、サブルーチン、関数、方法、手順、ソフトウェア・インターフェイス、アプリケーション・プログラム・インターフェイス（ＡＰＩ）、命令セット、コンピューティング・コード、コンピュータ・コード、コード・セグメント、コンピュータ・コード・セグメント、ワード、値、シンボル、またはそれらの任意の組み合わせを含み得る。しかし、実施形態がハードウェア要素および／またはソフトウェア要素を使用して実装されるかどうかを決定することは、所与の実装に対して所望される計算速度、電力レベル、熱許容範囲、処理サイクル予算、入力データ速度、出力データ速度、メモリ・リソース、データバス速度、および他の設計または性能制約など、任意の数の要因に従って変化し得る。

【０１１０】

少なくとも１つの実施形態の１つまたは複数の側面は、プロセッサ内のさまざまなロジックを表す機械可読媒体に格納された代表的な命令によって実装されてもよく、この命令は、機械によって読み取られると、本明細書で説明する技術を実行するロジックを機械に作製させる。「ＩＰコア」として知られるこのような表現は、有形の機械可読媒体に格納され、論理またはプロセッサを製造する製造機械にロードするために、さまざまな顧客または製造施設に供給され得る。いくつかの実施形態は、例えば、機械によって実行されると、実施形態に従った方法および／または動作を機械に実行させる命令または命令セットを記憶できる機械可読媒体または物品を使用して実装され得る。そのような機械は、例えば、任意の適切な処理プラットフォーム、コンピューティング・プラットフォーム、コンピューティング装置、プロセッシング装置、コンピューティング・システム、プロセッシングシステム、コンピュータ、プロセッサなどを含むことができ、任意の適切なハードウ

ェアおよび／またはソフトウェアの組み合わせを使用して実装されることができる。機械可読媒体または物品は、例えば、任意の適切なタイプのメモリ・ユニット、メモリ装置、メモリ物品、メモリ媒体、ストレージ装置、記憶物品、記憶媒体および／または記憶ユニット、例えば、メモリ、取り外し可能または取り外し不可能な媒体、消去可能または消去不可能な媒体、書き込み可能または再書き込み可能な媒体、デジタルまたはアナログ媒体、ハード・ディスク、フロッピー・ディスク、コンパクト・ディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、コンパクト・ディスク記録可能（ＣＤ－Ｒ）、コンパクト・ディスク書き換え可能（ＣＤ－ＲＷ）、光ディスク、磁気媒体、光磁気媒体、取り外し可能なメモリカードまたはディスク、様々なタイプのデジタル多用途ディスク（ＤＶＤ）、テープ、カセットなど。命令は、ソース・コード、コンパイル済みコード、解釈済みコード、実行可能コード、静的コード、動的コード、暗号化コードなど、任意の適切なタイプのコードを含むことができ、任意の適切な高レベル、低レベル、オブジェクト指向、視覚的、コンパイル済みおよび／または解釈済みプログラミング言語を使用して実装されることができる。

【０１１１】

上述した装置の構成要素および機能は、ディスクリート回路、特定用途向け集積回路（ＡＳＩＣ）、論理ゲートおよび／またはシングル・チップ・アーキテクチャの任意の組み合わせを使用して実装し得る。さらに、装置の特徴は、マイクロコントローラ、プログラマブル・ロジック・アレイおよび／またはマイクロプロセッサ、または好適には前述の任意の組み合わせを使用して実装され得る。本明細書では、ハードウェア、ファームウェア、および／またはソフトウェア要素は、「論理」または「回路」と総称または個別に呼ばれる場合があることに留意されたい。

【０１１２】

上述したブロック図に示された例示的な装置は、多くの潜在的な実装の１つの機能的説明例を表す可能性があることが理解されよう。したがって、添付の図に描かれているブロック機能の分割、省略、または包含は、これらの機能を実装するためのハードウェア構成要素、回路、ソフトウェア、および／または要素が、実施形態において必ずしも分割、省略、または包含されることを推論するものではない。

【０１１３】

少なくとも１つのコンピュータ読み取り可能な記憶媒体は、実行されると、本明細書に記載されるコンピュータ実装方法のいずれかをシステムに実行させる命令を含み得る。

【０１１４】

いくつかの実施形態は、「一実施形態（ｏｎｅ　ｅｍｂｏｄｉｍｅｎｔ）」または「一実施形態（ａｎ　ｅｍｂｏｄｉｍｅｎｔ）」という表現を、それらの派生語とともに用いて説明される場合がある。これらの用語は、実施形態に関連して説明される特定の特徴、構造、または特性が、少なくとも１つの実施形態に含まれることを意味する。本明細書中のさまざまな場所で「１つの実施形態において」という表現が現れるが、必ずしもすべてが同じ実施形態を指すわけではない。さらに、特に断らない限り、上述した特徴は、任意の組み合わせで一緒に使用可能であると認識される。したがって、別々に説明した特徴は、特徴が互いに互換性がないと指摘されない限り、互いに組み合わせて採用し得る。

【０１１５】

本開示の要約は、読者が技術開示の性質を迅速に把握できるように提供されることを強調する。これは、特許請求の範囲または意味を解釈または制限するために使用されないことを理解した上で提出される。さらに、前述の詳細な説明では、開示を合理化する目的で、様々な特徴が単一の実施形態にまとめられていることが分かる。この開示方法は、特許請求される実施形態が各請求項に明示的に記載されているよりも多くの特徴を必要とするという意図を反映していると解釈されるものではない。むしろ、以下の請求項が反映するように、発明的主題は、単一の開示された実施形態のすべての特徴よりも少ない特徴にある。したがって、以下の特許請求の範囲は、各請求項が別個の実施形態としてそれ自体で成り立つ状態で、本明細書に組み込まれる。添付の特許請求の範囲において、用語「を含

む」および「において」は、それぞれ、それぞれの用語「からなる」および「において」の平易な英語での等価物として使用される。さらに、「第１」、「第２」、「第３」などの用語は、単にラベルとして使用されており、その対象に数値要件を課すことを意図していない。

【０１１６】

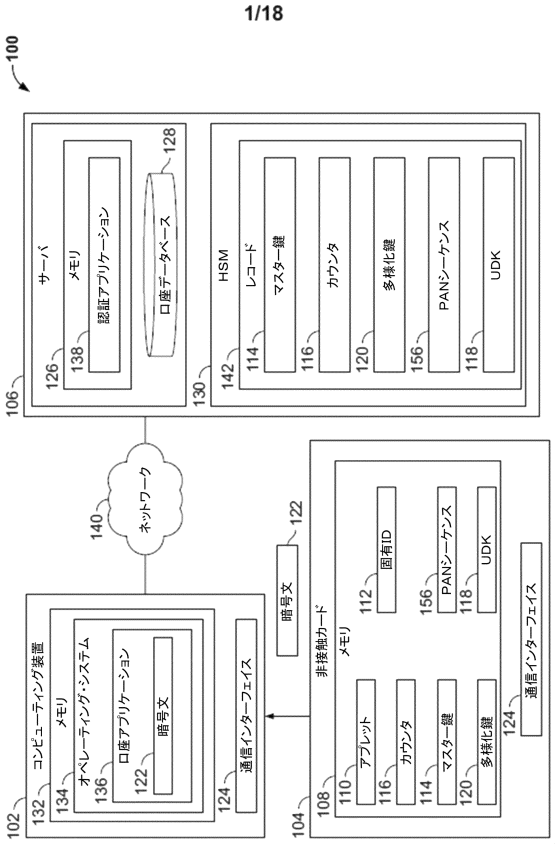
上述したことは、開示されたアーキテクチャの例を含む。もちろん、構成要素および／または方法論の考えられるすべての組み合わせを説明することは不可能であるが、当業者であれば、多くのさらなる組み合わせおよび順列が可能であることを認識できるであろう。したがって、新規なアーキテクチャは、添付の特許請求の範囲の精神および範囲内に入る、すべてのそのような変更、修正および変形を包含することが意図される。

【０１１７】

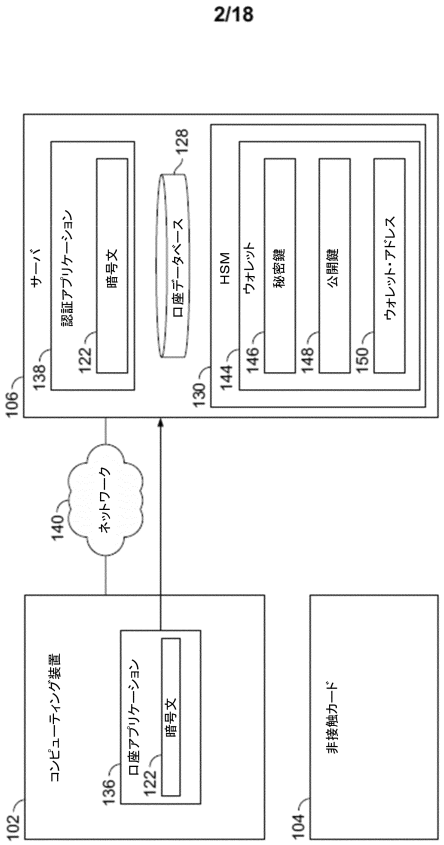
例示的な実施形態の前述の説明は、例示および説明の目的で提示されたものである。網羅的であること、または本開示を開示された正確な形態に限定することは意図されていない。本開示に照らして多くの修正および変形が可能である。本開示の範囲は、この詳細な説明によってではなく、むしろ本明細書に添付された特許請求の範囲によって限定されることが意図される。本出願の優先権を主張する将来出願される出願は、異なる態様で開示された主題を主張でき、一般に、本明細書において様々に開示されるか、または別様に示されるような１つまたは複数の制限の任意のセットを含むことができる。

【図面】

【図１Ａ】

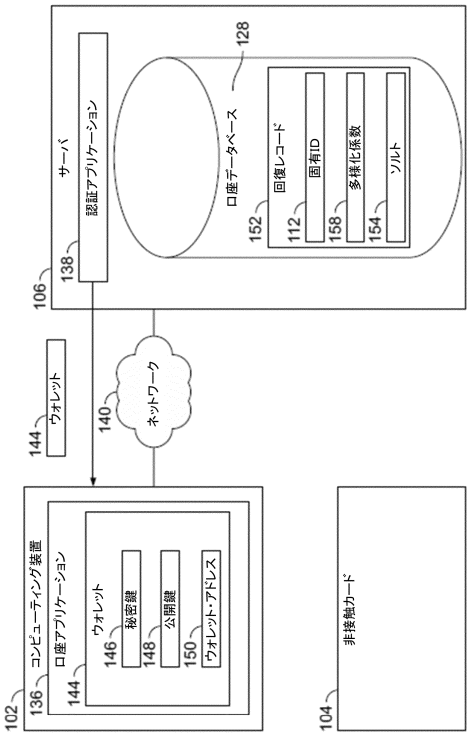


【図１Ｂ】



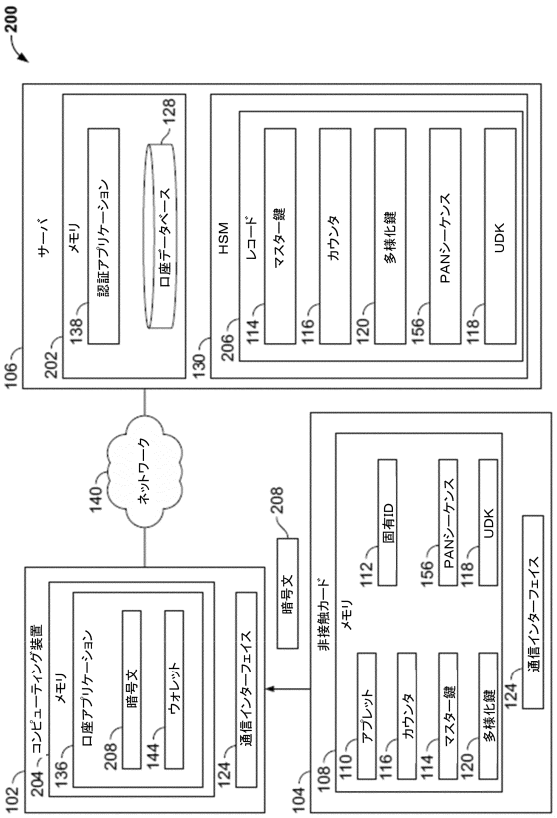
【図１Ｃ】

3/18



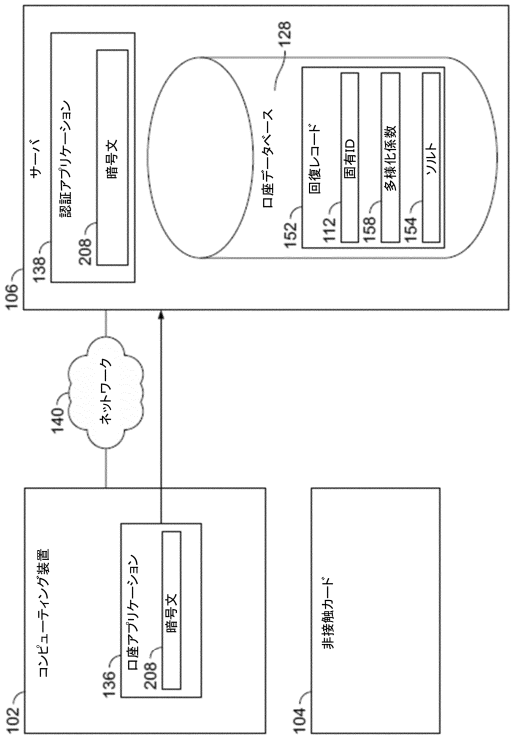
【図２Ａ】

4/18



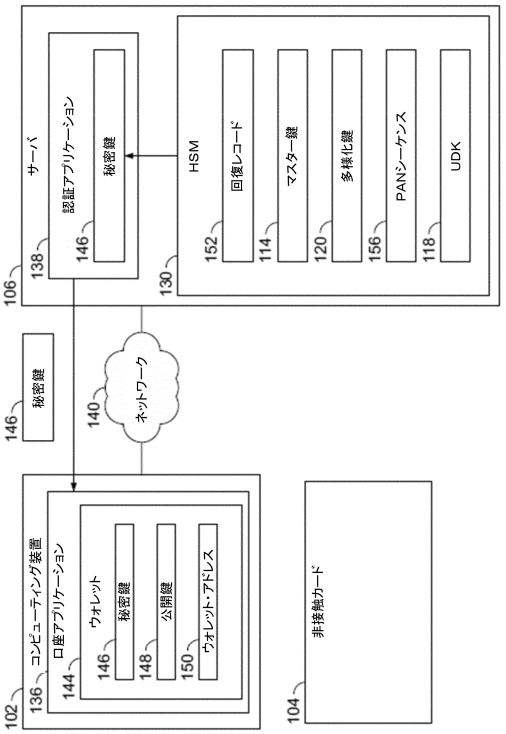
【図２Ｂ】

5/18

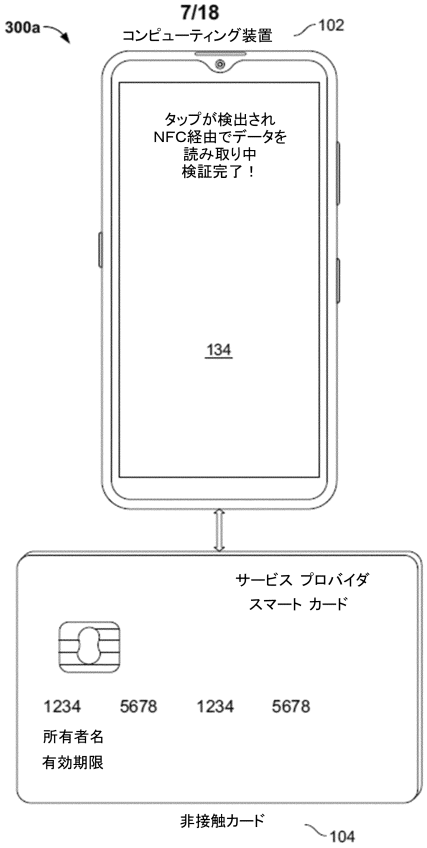


【図２Ｃ】

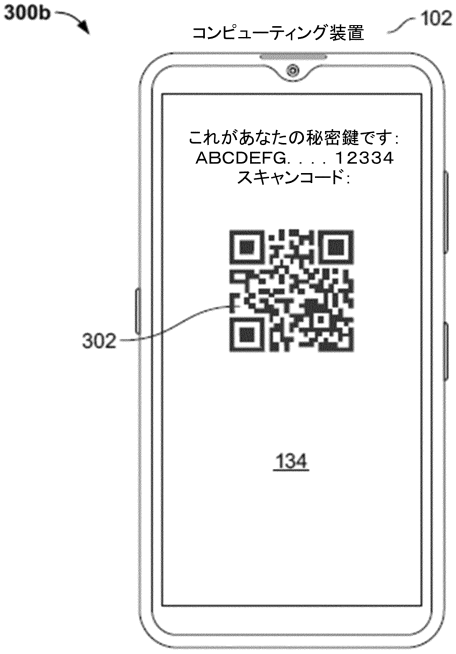
6/18



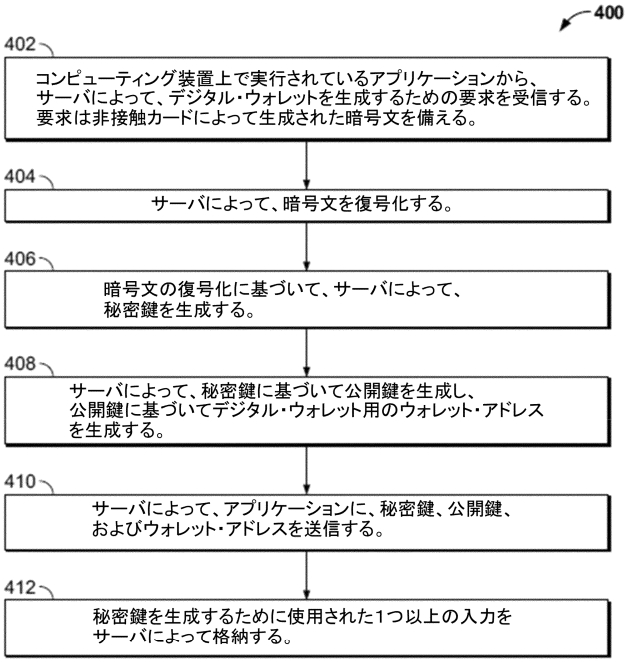
【図３Ａ】


300a
コンピューティング装置
102
タップが検出され
NFC経由でデータを
読み取り中
検証完了！
134
サービス プロバイダ
スマート カード
1234 5678 1234 5678
所有者名
有効期限
非接触カード
104

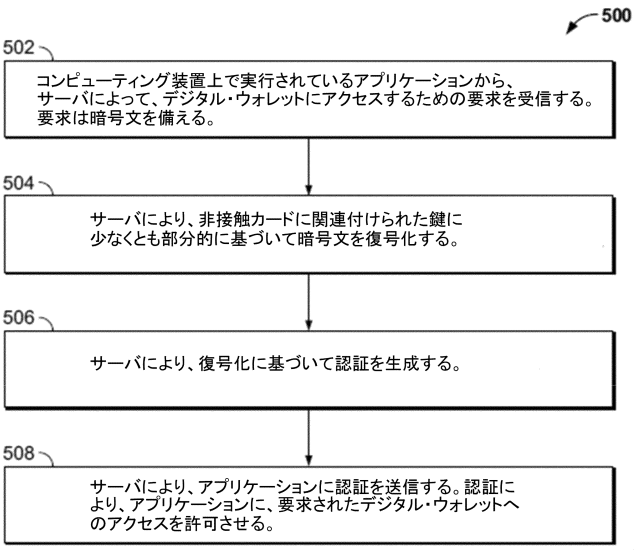
【図３Ｂ】


300b
コンピューティング装置
102
これがあなたの秘密鍵です:
ABCDEFG. . . . 12334
スキャンコード:
302
134

【図４】

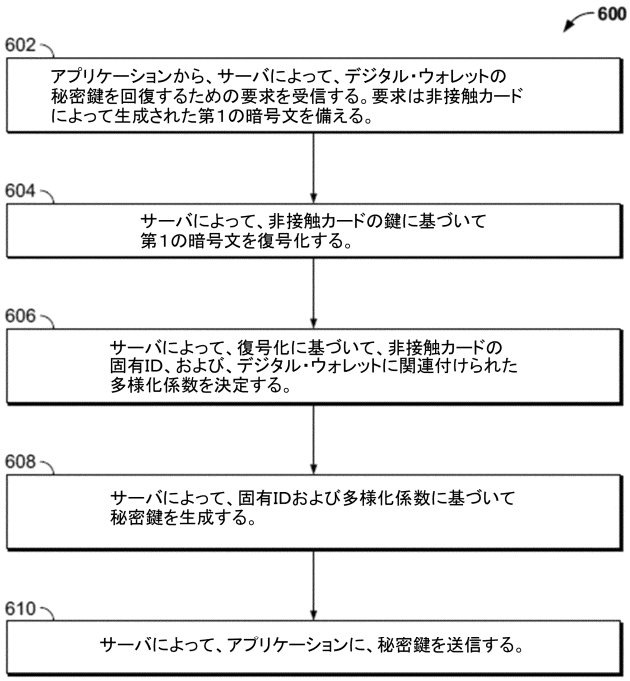

400
402
コンピューティング装置上で実行されているアプリケーションから、
サーバによって、デジタル・ウォレットを生成するための要求を受信する。
要求は非接触カードによって生成された暗号文を備える。
404
サーバによって、暗号文を復号化する。
406
暗号文の復号化に基づいて、サーバによって、
秘密鍵を生成する。
408
サーバによって、秘密鍵に基づいて公開鍵を生成し、
公開鍵に基づいてデジタル・ウォレット用のウォレット・アドレス
を生成する。
410
サーバによって、アプリケーションに、秘密鍵、公開鍵、
およびウォレット・アドレスを送信する。
412
秘密鍵を生成するために使用された1つ以上の入力を
サーバによって格納する。

【図５】


500
502
コンピューティング装置上で実行されているアプリケーションから、
サーバによって、デジタル・ウォレットにアクセスするための要求を受信する。
要求は暗号文を備える。
504
サーバにより、非接触カードに関連付けられた鍵に
少なくとも部分的に基づいて暗号文を復号化する。
506
サーバにより、復号化に基づいて認証を生成する。
508
サーバにより、アプリケーションに認証を送信する。認証に
より、アプリケーションに、要求されたデジタル・ウォレットへ
のアクセスを許可させる。

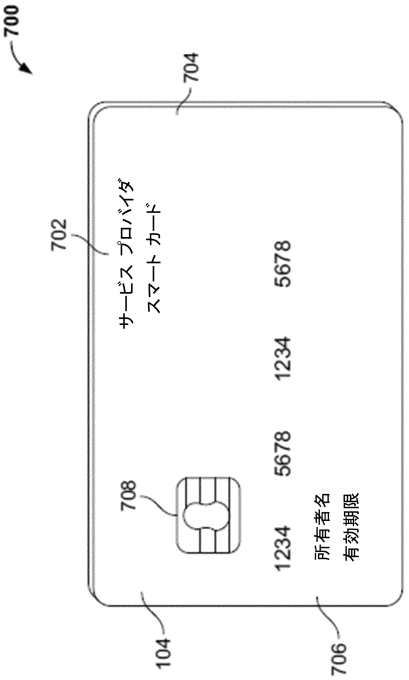
【図６】

11/18



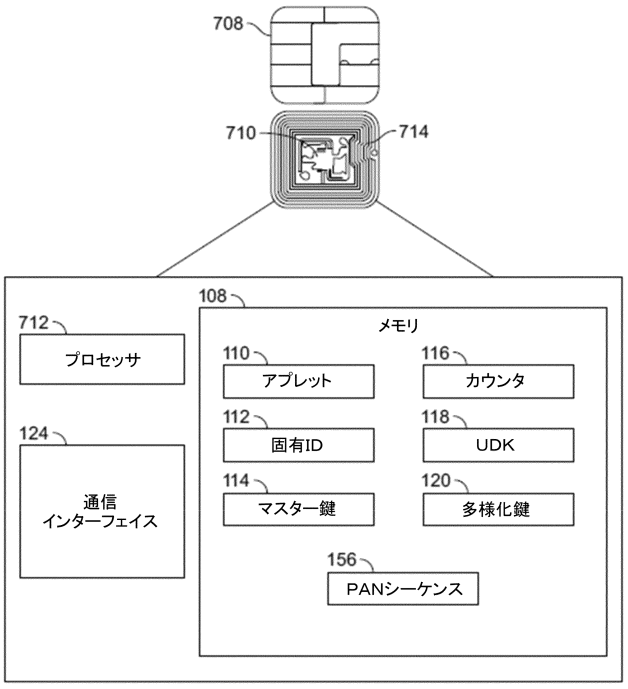
【図７Ａ】

12/18



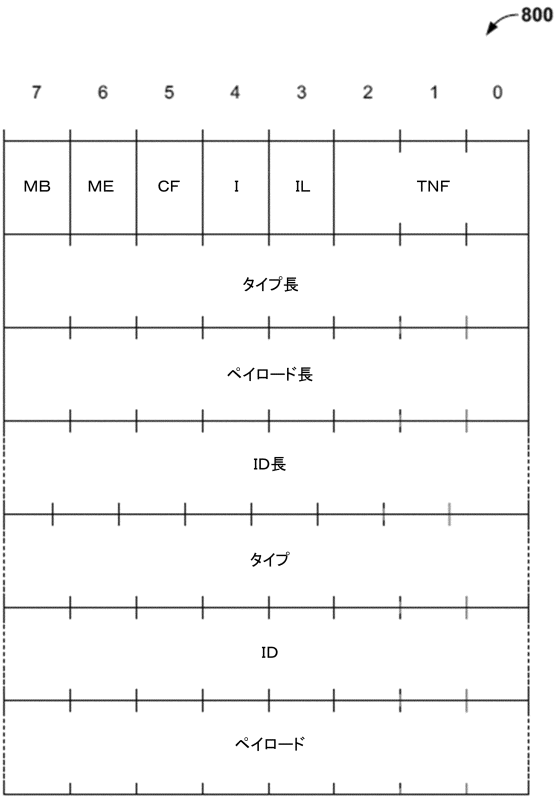
【図７Ｂ】

13/18



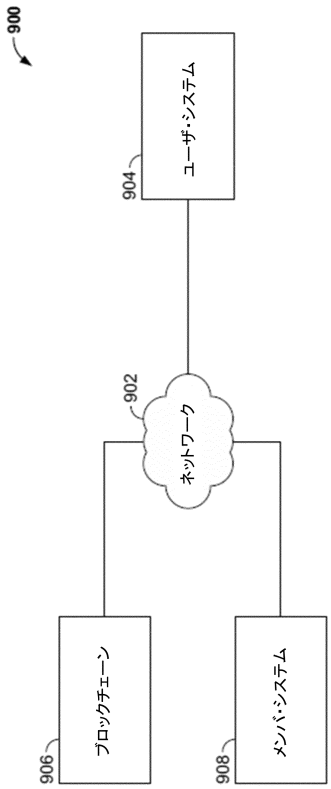
【図８】

14/18



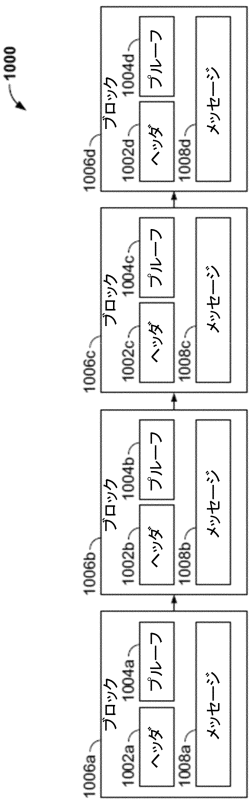
【図９】

15/18



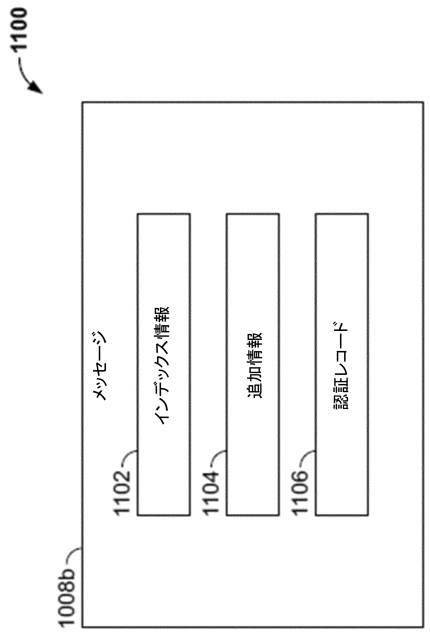
【図１０】

16/18



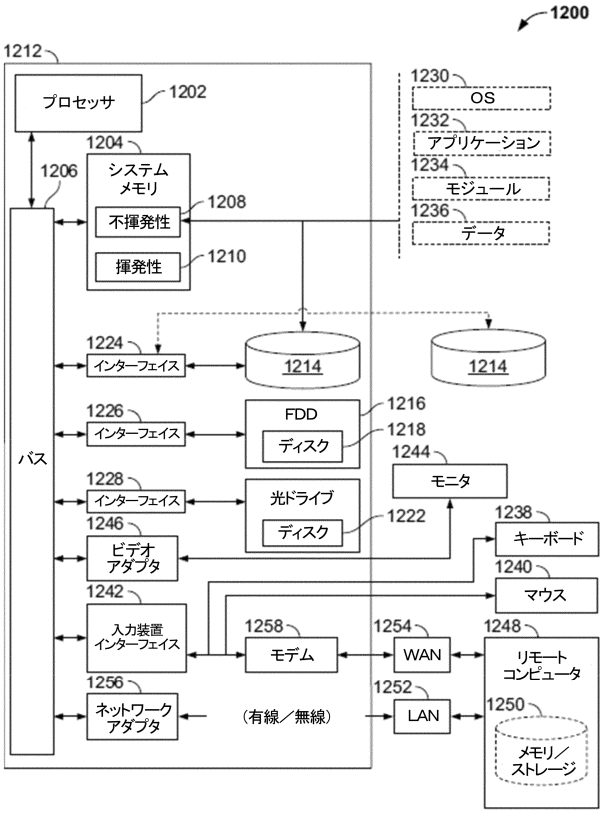
【図１１】

17/18



【図１２】

18/18



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/050885

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/38 G06Q20/32 G06Q20/34 G06Q20/36
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7 080 259 B1 (NAKANISHI YOSHIAKI [JP] ET AL) 18 July 2006 (2006-07-18) abstract; figures column 5, line 19 - column 21, line 36 column 25, line 57 - column 26, line 38	1-20
A	KR 2019 0045753 A (KOREAMINT [KR]; COINPLUG INC [KR]) 3 May 2019 (2019-05-03) abstract; claims; figures paragraphs [0026] - [0045]	1-20
A	WO 2020/110079 A1 (CEEVO BLOCKCHAIN VENTURE LTD [LI]; KOURIE KEITH DERRICK [ZA]) 4 June 2020 (2020-06-04) abstract; claims; figures page 16, paragraph 3 page 22, paragraph 4 - page 25, paragraph 2	1-20

-/--

[x] Further documents are listed in the continuation of Box C. [x] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 March 2023	04/04/2023

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Schöndienst, Thilo

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/050885

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2020/106619 A1 (OSBORN KEVIN [US] ET AL) 2 April 2020 (2020-04-02) abstract; figures paragraphs [0027] - [0066]	1-20
A	US 2015/324789 A1 (DVORAK JOHN [US] ET AL) 12 November 2015 (2015-11-12) abstract; figures paragraphs [0060], [0098], [0164] - [0172]	1-20
A	US 2021/365938 A1 (RADU CRISTIAN [BE]) 25 November 2021 (2021-11-25) abstract; figures paragraphs [0083] - [0152]	1-20

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/050885

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7080259 B1	18-07-2006	CN 1327566 A	19-12-2001
		CN 1722166 A	18-01-2006
		EP 1130528 A1	05-09-2001
		KR 20010080103 A	22-08-2001
		US 7080259 B1	18-07-2006
		WO 0113293 A1	22-02-2001
KR 20190045753 A	03-05-2019	NONE	
WO 2020110079 A1	04-06-2020	NONE	
US 2020106619 A1	02-04-2020	AU 2019354372 A1	01-04-2021
		BR 112021004541 A2	08-06-2021
		CA 3112346 A1	09-04-2020
		CN 112602300 A	02-04-2021
		CN 112639857 A	09-04-2021
		CN 112805735 A	14-05-2021
		CN 112805736 A	14-05-2021
		CN 112805757 A	14-05-2021
		CN 112805967 A	14-05-2021
		CN 112823335 A	18-05-2021
		CN 113168634 A	23-07-2021
		CN 113168747 A	23-07-2021
		CN 113169870 A	23-07-2021
		CN 113170299 A	23-07-2021
		CN 113228556 A	06-08-2021
		CN 113243024 A	10-08-2021
		EP 3861434 A1	11-08-2021
		EP 3861501 A1	11-08-2021
		EP 3861503 A1	11-08-2021
		EP 3861506 A1	11-08-2021
		EP 3861507 A1	11-08-2021
		EP 3861513 A1	11-08-2021
		EP 3861538 A1	11-08-2021
		EP 3861539 A1	11-08-2021
		EP 3861673 A1	11-08-2021
		EP 3861685 A1	11-08-2021
		EP 3861703 A1	11-08-2021
		EP 3861704 A1	11-08-2021
		EP 3861773 A1	11-08-2021
		JP 2022501890 A	06-01-2022
		KR 20210065946 A	04-06-2021
		SG 11202102474W A	29-04-2021
		US 10581611 B1	03-03-2020
		US 2020104826 A1	02-04-2020
		US 2020106619 A1	02-04-2020
		US 2020366490 A1	19-11-2020
		US 2021344495 A1	04-11-2021
		US 2023051390 A1	16-02-2023
		WO 2020072476 A1	09-04-2020
		WO 2020072551 A1	09-04-2020
US 2015324789 A1	12-11-2015	CA 2985040 A1	03-12-2015
		US 2015324789 A1	12-11-2015
		WO 2015183497 A1	03-12-2015
US 2021365938 A1	25-11-2021	CN 108027926 A	11-05-2018
		EP 3326132 A1	30-05-2018

Form PCT/ISA/210 (patent family annex) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/050885

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		JP 2018522353 A	09-08-2018
		US 2017017957 A1	19-01-2017
		US 2021365938 A1	25-11-2021
		WO 2017014863 A1	26-01-2017
		ZA 201708474 B	26-06-2019

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

,MC,ME,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０、キャピタル・ワン・サービシーズ・リミテッド・ライアビリティ・カンパニー内

(72)発明者　プラサド，ジャイキシャン

アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０、キャピタル・ワン・サービシーズ・リミテッド・ライアビリティ・カンパニー内

(72)発明者　カタラ カステリャル，ホセ

アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０、キャピタル・ワン・サービシーズ・リミテッド・ライアビリティ・カンパニー内