(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2025-521092
(P2025-521092A)
(43)公表日　令和7年7月8日(2025.7.8)

(51)国際特許分類			FI			テーマコード（参考）
G06Q	*20/38*	*(2012.01)*	G06Q	20/38	310	5L020
G06Q	*20/34*	*(2012.01)*	G06Q	20/34	400	

審査請求　未請求　予備審査請求　未請求　（全25頁）

(21)出願番号　特願2024-566398(P2024-566398)
(86)(22)出願日　令和5年6月14日(2023.6.14)
(85)翻訳文提出日　令和6年11月8日(2024.11.8)
(86)国際出願番号　PCT/IL2023/050615
(87)国際公開番号　WO2023/248213
(87)国際公開日　令和5年12月28日(2023.12.28)
(31)優先権主張番号　294174
(32)優先日　令和4年6月21日(2022.6.21)
(33)優先権主張国・地域又は機関
イスラエル(IL)
(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　523452997
ナヤックス リミテッド
イスラエル ヘルツリーヤ アリク アインシュタイン ストリート 3
(74)代理人　100103610
弁理士　▲吉▼田 和彦
(74)代理人　100109070
弁理士　須田 洋之
(74)代理人　100119013
弁理士　山崎 一夫
(74)代理人　100067013
弁理士　大塚 文昭
(74)代理人　100120525
弁理士　近藤 直樹
(74)代理人　100139712
最終頁に続く

(54)【発明の名称】　決済有効性を検証するためのシステム、デバイス及び方法

(57)【要約】
決済有効性検証のためのプログラム命令を含む１つ以上の実体的なコンピュータ可読で非一過性のストレージ媒体を含む決済端末であって、１つ以上のプロセッサによるプログラム命令の実行により、決済端末に、無線デバイスに配置されたソフトウエアディベロップメントキット（ＳＤＫ）により発行された公開－秘密鍵ペアの第１の公開鍵及び消費者識別情報を含む決済トークンを受信させ、取引情報メッセージを含む決済リクエストを生成し、当該第１の決済リクエストメッセージ及び当該決済トークンを少なくとも１つのデータベースに蓄積されるための少なくとも１つのバックエンドプラットフォームに伝達させ、当該少なくとも１つのバックエンドプラットフォームにより生成された決済承認に基づいて当該少なくとも１つのバックエンドプラットフォームからの決済及び取引確認メッセージを受信させ、当該第１の公開鍵の所有権を検証することが、署名された取引情報メッセージの公開鍵と当該決済トークンの公開鍵との比較に基づいて少なくとも１つのバックエンドプラットフォームで実行される、決済端末。

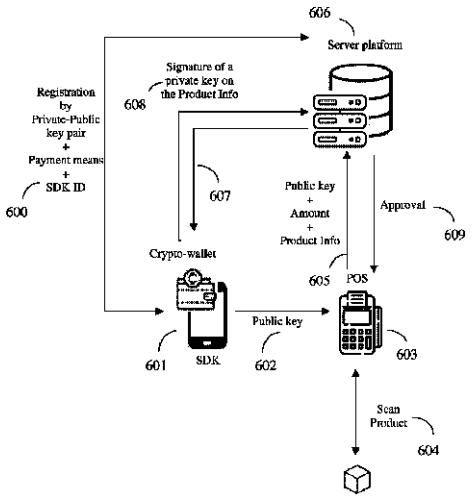

FIG. 6

【特許請求の範囲】
【請求項１】
無線デバイスにより実行された決済有効性を検証するための方法であって、
クリプトウォレットにより公開－秘密鍵ペアを作り出すことと、
前記公開－秘密鍵ペアの公開鍵を含む決済トークンを生成することと、
販売時点情報管理システムで、決済の取引情報メッセージ及び前記決済トークンを含む決済リクエストを生成するように構成され、少なくとも１つのバックエンドプラットフォームへその後、前記決済リクエストを伝達するように構成されている決済端末に、前記決済トークンを伝達することと、
前記取引情報メッセージに基づく前記少なくとも１つのバックエンドプラットフォームによって取引検証メッセージを生成することと、
前記決済トークンの前記公開鍵に関連付けられたデバイスへ前記取引検証メッセージを提供することと、
前記公開－秘密鍵ペアの秘密鍵で前記取引検証メッセージを署名すること及び前記少なくとも１つのバックエンドプラットフォームへ署名された前記取引検証メッセージを送付することと、
少なくとも１つのバックエンドプラットフォームによって、前記無線デバイスにより署名された前記取引検証メッセージの公開鍵と前記決済端末により生成された決済リクエストメッセージにおいて含まれた前記公開鍵とを比較することにより前記第１の公開鍵の所有権を検証することと、
少なくとも１つの金融エンティティの顧客プラットフォームで前記決済を承認することと、
前記少なくとも１つのバックエンドプラットフォームから、取引確認メッセージを送付することにより前記少なくとも１つのバックエンドプラットフォームによる決済検証結果を前記決済端末、前記無線デバイス、及び前記顧客プラットフォームのいずれかに通知すること、を含む、方法。
【請求項２】
前記決済トークンの消費者識別情報は、前記少なくとも１つのバックエンドプラットフォームに蓄積されたランダム数、消費者に関連付けられた情報のハッシュ値及び一意のシリアル番号のうちの少なくとも１つである、請求項１に記載の方法。
【請求項３】
前記取引情報メッセージは、支払期日、製品リスト及び加盟店ＩＤの中の少なくとも１つを含む、
請求項１に記載の方法。
【請求項４】
前記決済トークンを生成することは、
ランダム数である前記秘密鍵を生成することと、
前記秘密鍵をハッシュすることにより前記公開鍵を生成することと、
消費者コンタクト情報、無線デバイスＩＤ、決済情報、地理位置情報、及び消費者ｉｄ番号のうちの少なくとも１つを含む消費者識別情報をハッシュすることと、
前記公開鍵及び前記消費者識別情報のハッシュ値で前記決済トークンを構築することと、
を含む請求項１に記載の方法。
【請求項５】
決済有効性を検証するためのプログラム命令を含んでいる１つ以上の実体的なコンピュータ可読非一過性ストレージ媒体を含んでいる決済端末であって、
１つ以上のプロセッサによる前記プログラム命令の実行により、前記決済端末に、
無線デバイスに配置されたソフトウエアディベロップメントキット（ＳＤＫ）により発行されたものであって、クリプトウォレットにより作り出された一組の公開－秘密鍵の公開鍵を含む決済トークンを受信させ、

取引情報メッセージ及び前記決済トークンを含む決済リクエストを生成し、及び少なくとも１つのバックエンドプラットフォームに前記決済リクエストを伝達させ、
前記少なくとも１つのバックエンドプラットフォームにより生成された決済承認に基づいて前記少なくとも１つのバックエンドプラットフォームから決済及び取引確認メッセージを受信させ、
無線デバイス内の前記公開－秘密鍵ペアの秘密鍵により署名された取引検証メッセージの前記公開鍵と前記決済端末により生成され前記決済リクエストにおいて含まれている前記公開鍵との比較に基づいて、前記公開鍵の所有権を検証することが、少なくとも１つのバックエンドプラットフォームにより実行される、
決済端末。
【請求項６】
１つ以上のプロセッサにより前記プログラム命令が実行されることにより、無線周波数識別（ＲＦＩＤ）通信、短距離無線通信、及び近距離無線通信（ＮＦＣ）の内、少なくとも１つを介して前記決済トークンを受信する、
請求項５に記載の決済端末。
【請求項７】
前記決済トークンは、バックエンドプラットフォームに蓄積されたランダム数、ユーザに関連付けられた情報のハッシュ値、一意のシリアル番号のうちの少なくとも１つを含む消費者識別情報を備える、
請求項５に記載の決済端末。
【請求項８】
前記取引情報メッセージは、支払期日、製品リスト、及び加盟店ＩＤのうちの少なくとも１つを含む、
請求項５に記載の決済端末。
【請求項９】
決済有効性を検証するためのプログラム命令を含むアプリケーションがインストールされた１つ以上の実体的なコンピュータ可読非一過性ストレージ媒体を含む無線デバイスであって、
１つ以上のプロセッサにより前記プログラム命令の実行により、結果として、
クリプトウォレットにより公開－秘密鍵ペアが作り出されることと、
前記公開－秘密鍵ペアの公開鍵を含んでいる決済トークンを生成することと、
販売時点情報管理システムの決済端末に前記決済トークンを伝達することと、
前記決済端末から取引情報メッセージを受信することと、
少なくとも１つのバックエンドプラットフォームから取引検証メッセージを受信することと、
前記決済端末から受信した前記取引情報メッセージと少なくとも１つのバックエンドプラットフォームにより生成された前記取引検証メッセージとの比較に基づいて、
前記公開－秘密鍵ペアの秘密鍵で前記取引検証メッセージを署名することと、
前記少なくとも１つのバックエンドプラットフォームに前記署名された取引検証メッセージを送付することと、
前記少なくとも１つのバックエンドプラットフォームによって、前記署名された取引検証メッセージの前記公開鍵と、前記決済トークンの比較に基づいて、前記公開鍵の所有権を検証した後、取引確認を受信することを生じることとなる、
無線デバイス。
【請求項１０】
前記決済トークンは、少なくとも１つのバックエンドプラットフォームに蓄積されたランダム数、消費者に関連付けられた情報のハッシュ値の内、少なくとも１つで構成されている消費者識別情報を含む、
請求項９に記載の無線デバイス。
【請求項１１】

前記ストレージ媒体の前記プログラム命令により、１つ以上のプロセッサにより実行されたとき、結果として、検証される各々の決済の前に前記決済トークンを生成することとなる、
請求項９に記載の無線デバイス。
【請求項１２】
前記ストレージ媒体の前記プログラム命令により、１つ以上のプロセッサにより実行されたとき、結果として、前記少なくとも１つのバックエンドプラットフォームでの消費者の第１の登録において前記公開－秘密鍵ペアを生成することになる、
請求項９に記載の無線デバイス。
【請求項１３】
前記ストレージ媒体の前記プログラム命令により、１つ以上のプロセッサにより実行されたとき、結果として、前記決済トークンにおいての使用のために既存の公開－秘密鍵ペアをインポートすることとなる、
請求項９に記載の無線デバイス。
【請求項１４】
前記ストレージ媒体の前記プログラム命令により、１つ以上のプロセッサにより実行されたとき、署名される取引が、事前設定許容量を超えようと超えまいと、無線デバイスの地理位置情報が前記決済端末の既知の地理位置情報の事前に決められた範囲内であるとき、結果として、前記無線デバイスをロック解除するイベントの少なくとも１つにおいて前記取引検証メッセージを署名することとなる、
請求項９に記載の無線デバイス。
【請求項１５】
前記既知の地理位置情報の事前に決められた範囲は、前記既知の地理位置情報の中心からゼロと５メートルの間である、
請求項１４に記載の無線デバイス。
【請求項１６】
１つ以上のプロセッサにより実行されたとき、前記ストレージ媒体の前記プログラム命令により、結果として、
ランダム数である前記秘密鍵を生成することと、
前記秘密鍵をハッシュすることにより前記公開鍵を生成することと、
消費者識別情報をハッシュすることと、
前記決済トークンを前記公開鍵と前記消費者識別情報のハッシュ値で構築することを生じることとなる、
請求項９に記載の無線デバイス。
【請求項１７】
前記消費者識別情報は、消費者コンタクト情報、無線デバイスＩＤ、決済情報、地理位置情報及び消費者ｉｄ番号の内、少なくとも１つを含む、
請求項１０に記載の無線デバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書で説明された、いくつかのものは、一般に、決済有効性の検証のための方法、システム及び装置に関する。さらに、具体的には、本開示は、金融取引の検証に関する。
【背景技術】
【０００２】
例えば、クレジットカードやデビットカードのようなペイメントカードは、詐欺行為を受けやすいということが広く知られている一方で、消費者と企業の両方にとって、大変有利であることを証明している。
【０００３】
詐欺防止及び決済クレジットカード保有者のための安全な買い物環境の構成は、２０世

紀における決済カードの設立以来、その分野で多くの努力の目的であった。
【０００４】
ユーロペイ、ＶＩＳＡ、Ｍａｓｔｅｒｃａｒｄ（ＥＭＶ）スタンダードは、カード発行者により、検証のための販売時点情報管理（ＰＯＳ）から、決済カード番号及び４デジットＰＩＮナンバの安全な伝達を介して、カード保有者の同一性の検証を可能にする。ひとたび、決済カード番号及び４桁のＰＩＮ、有効期限の詳細が権限のない人に曝されたら、この人は、商品やサービスを購入するためにクレジットカードを使用するだろう。
【０００５】
こうして、上記で述べた不備を直すために、より安全なシステム及び方法の必要性がある。
【０００６】
決済有効性の検証をすることのためのシステム、方法、製品に関する本発明は、例示の方法のみによって以下に説明されている。
【０００７】
目下、開示された主題の態様によると、本発明は、決済有効性の検証のためのプログラム命令を含む１つ以上の実体的なコンピュータ可読の非一過性のストレージ媒体を含む決済端末を含むことができ、１つ以上のプロセッサによるプログラム命令の実行によって、決済端末は、無線デバイスに配置されたソフトウエアディベロップメントキット（ＳＤＫ）により発行された公開－秘密鍵ペアの公開鍵を含む、決済トークンを受信し、取引情報メッセージを含んでいる決済リクエストを生成し、少なくとも１つのデータベースに蓄積されるために少なくとも１つのバックエンドプラットフォームへ当該決済リクエスト及び当該決済トークンを伝達し、当該少なくとも一つのバックエンドプラットフォームによる決算承認に基づいて当該少なくとも１つのバックエンドプラットフォームから決済及び取引確認メッセージを受信し、当該公開鍵の所有権を検証することは、無線デバイスの秘密鍵により署名された取引情報メッセージの公開鍵と、少なくとも１つのバックエンドプラットフォームによる当該決済トークンの公開鍵の比較に基づくものである。
【０００８】
例えば、当該ストレージ媒体の当該プログラム命令は、当該決済を開始した無線デバイスへの当該取引情報メッセージのハッシュ値を伝達することを含み、取引確認は、無線デバイスが、取引検証メッセージを当該取引情報メッセージの当該ハッシュ値と比較した後、受信される。
【０００９】
例えば、当該ストレージ媒体の当該プログラム命令は、実行されたとき、結果として、無線周波数識別（ＲＦＩＤ）通信、短距離無線通信、及び近距離無線通信（ＮＦＣ）の内、少なくとも１つを介して、当該決済トークンを受信することになる。
【００１０】
例えば、当該決済トークンの当該消費者識別情報は、当該少なくとも１つのバックエンドプラットフォームに蓄積されたランダム数、ユーザに関連付けられた情報のハッシュ値、及び一意のシリアル番号の内、少なくとも１つを含む。
【００１１】
例えば、当該取引情報は、支払期日、製品リスト、及び加盟店ＩＤの内、少なくとも１つを含む。
【００１２】
一実施形態では、決済有効性の検証をするための方法を含むことができ、当該公開－秘密鍵ペアの公開鍵及び消費者識別情報を含む決済トークンを生成し、販売時点情報管理システムで、決済の取引情報メッセージを含む第１の決済リクエストメッセージを生成及び少なくとも一つのバックエンドプラットフォームへ決済リクエストメッセージ及び当該決済トークンを伝達する決済端末へ、当該決済トークンを供給する、無線デバイスにより公開－秘密鍵ペアを提供することと、当該少なくとも一つのバックエンドプラットフォームによって、当該取引情報メッセージから、取引検証メッセージを生成することと、当該決

済トークンの当該公開鍵に関連付けられたデバイスへ取引検証メッセージを提供することと、公開－秘密鍵ペアの秘密鍵で取引検証メッセージに署名をすること及び当該少なくとも一つのバックエンドプラットフォームへ署名された取引検証メッセージを送付することと、無線デバイスにおいて秘密鍵により署名された第２の取引情報により提供された第２の公開鍵を、少なくとも１つのバックエンドプラットフォームによりなされた当該第１の公開鍵と比較することにより、当該第１の公開鍵の所有権を検証することと、少なくとも一つの金融エンティティの顧客プラットフォームとの当該取引を承認することと、当該少なくとも１つのバックエンドプラットフォームが、当該少なくとも１つのバックエンドプラットフォームから取引確認メッセージを送付することにより、決済検証結果を当該決済端末、無線デバイス及び当該顧客プラットフォームに通知すること、を含む、方法。

【００１３】

例えば、当該決済トークンの当該消費者識別情報は、当該少なくとも１つのバックエンドプラットフォームに蓄積されたランダム数、ユーザに関連付けられた情報のハッシュ値、一意のシリアル番号のうちの少なくとも１つである。

【００１４】

例えば、当該取引情報は、少なくとも１つの支払期日、製品リスト及び加盟店ＩＤを含む。

【００１５】

例えば、ランダム数である秘密鍵を生成すること、当該秘密鍵をハッシュすることによる公開鍵を生成すること、消費者コンタクト情報、無線デバイスＩＤ、決済情報、地理位置情報及び消費者ｉｄナンバのうちの少なくとも１つを含む、消費者識別情報をハッシュすること、当該公開鍵及び消費者識別情報のハッシュ値で当該決済トークンを構築すること、により当該決済トークンは生成される。

【００１６】

他の１つの実施形態では、決済有効性を検証するためのプログラム命令を含むアプリケーションがインストールされた１つ以上の実体的なコンピュータ可読の非一過性のストレージ媒体を含んでいる無線デバイスを含むことができ、１つ以上のプロセッサによるプログラム命令の実行により、結果として公開－秘密鍵ペアを提供し、当該公開－秘密鍵ペアの公開鍵を含む決済トークンを生成し、当該決済トークンを当該販売時点情報管理システムの決済端末に提供し、当該決済端末から取引情報メッセージを受信し、少なくとも１つのバックエンドプラットフォームから取引検証メッセージを受信し、取引検証メッセージと取引情報メッセージの比較に基づいて、公開－秘密鍵ペアの秘密鍵で取引検証メッセージを署名し、当該少なくとも１つのバックエンドプラットフォームへそれを送信し、署名された取引メッセージと当該決済トークンの公開鍵の比較に基づいて当該公開鍵の所有権の検証した後、取引確認を受信し、当該取引確認は、少なくとも１つの金融エンティティの顧客プラットフォームで当該取引を承認した後、受信されることとなる。

【００１７】

例えば、当該決済トークンは、少なくとも１つのバックエンドプラットフォームに蓄積されたランダム数、ユーザに関連付けられた情報のハッシュ値のうちの少なくとも１つを含む消費者識別情報を含む。

【００１８】

例えば、当該ストレージ媒体の当該プログラム命令が、実行されたとき、結果として検証される各々の決済の前に決済トークンを生成することとなる。

【００１９】

例えば、当該ストレージ媒体の当該プログラム命令が実行されたとき、結果として、当該少なくとも１つのバックエンドプラットフォームでの消費者での第１の登録において秘密－公開鍵ペアを生成することとなる。

【００２０】

例えば、当該ストレージ媒体の当該プログラム命令が実行されたとき、結果として、当該決済トークンにおいて使用のために既存の公開－秘密鍵ペアをインポートすることとな

る。
【００２１】
例えば、当該ストレージ媒体の当該プログラム命令が実行されたとき、結果として、無線デバイスの地理位置情報が、決済端末の地理位置情報と類似しているとき、及び署名されるための取引があらかじめセットされた許容額を超えないとき、ロック解除している当該無線デバイスの少なくとも１つのイベントにおいて当該取引検証メッセージに署名することとなる。
【００２２】
例えば、当該ストレージ媒体の当該プログラム命令が実行されたとき、結果として、ランダム数である秘密鍵を生成すること、当該秘密鍵をハッシュすることにより公開鍵を生成すること、消費者コンタクト情報、無線デバイスＩＤ、決済情報、地理位置情報及び消費者ｉｄナンバのうちの少なくとも１つを含む消費者識別情報をハッシュすること、当該公開鍵及び消費者識別情報のハッシュ値で当該決済トークンを構築することとなる。
【００２３】
本発明の様々な物、特徴及び態様は、同様の数字は、同様の構成要素を表す添付した図面とともに、この発明の好ましい実施形態の詳述された説明から、さらに明白になるだろう。
本明細書で開示された主題をよりよく理解するために、また、それをいかに実際に実施されることができるかを例示するために、非限定の例のみの方法により、添付図面を参照して、実施形態は、今説明されるだろう。
【図面の簡単な説明】
【００２４】
【図１】図１は、いくつかの例示的実施形態のとおり、決済有効性を検証するためのシステムのブロック図を示す。
【図２】図２は、いくつかの例示的実施形態のとおり、決済有効性を検証するための方法のフローチャートを示す。
【図３】図３は、いくつかの例示的実施形態のとおり、決済有効性を検証するための方法のフローチャートを示す。
【図４】図４は、いくつかの例示的実施形態のとおり、決済有効性を検証するための方法のフローチャートを示す。
【図５】図５は、いくつかの例示的実施形態のとおり、製造製品を示す。
【図６】図６は、いくつかの例示的実施形態のとおり、決済有効性を検証することのためのシステムのブロック図を示す。
【発明を実施するための形態】
【００２５】
次の詳述された説明において、多数の具体的な詳細は、いくつかの実施形態の完全な理解を提供するために、明らかにされる。しかしながら、その分野における当業者により、いくつかの実施形態がこれらの具体的な詳細がなく実行されることができるということが理解されるだろう。他の例では、周知の方法、手順、構成要素、ユニット、及び／又は回路が、この議論を曖昧にしないように、詳細に説明されなかった。
【００２６】
例えば、"processing（処理すること）"、"computing（コンピュータ処理をすること）"、"calculating（計算すること）"、"determining（判定すること）"、"establishing（確立すること）"、"analyzing（分析する事）"、"checking（チェックすること）"、などのような用語を活用する本明細書でなされた議論は、コンピュータのレジスタ及び／又はメモリ内で、物理的な（例えば、電子的な）量として、表されたデータを、コンピュータのレジスタ及び／又はメモリ又は作動及びプロセスを実行するための命令を蓄積することができる他の情報ストレージ媒体内で物理的な量として、同様に表された他のデータへ操作及び／又は変換するコンピュータ、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システム又は他の電子コンピューティングデバイスの作動及び／

又は処理を指すことができる。

【００２７】

本明細書で使用されているように、”plurality（複数）”及び”a plurality（複数）”という用語は、例えば、”multiple（複数）”又は”two or more（２又はそれ以上）”を含む。例えば、"a plurality of items（複数の項目）"は、２つ又はそれ以上の項目を含む。

【００２８】

"one embodiment（１つの実施形態）"、"an embodiment（１つの実施形態）"、"demonstrative embodiment（例示的実施形態）"、"various embodiments（様々な実施形態）"、などを参照すると、このように説明された実施形態は、特定の特徴、構造又は特質を含むが、全ての実施形態が特定の特徴、構造又は特質を必ず含むものではないことを示す。さらに、"in one embodiment（１つの実施形態では）"という語の繰り返しの使用は、同じ実施形態を参照することはできるが、必ずしも必要ではない。

【００２９】

本明細書で使用されているように、さもなければ特定されない場合、共通の物を説明するための序列形容詞である、"first（第１の）"、"second（第２の）"、"third（第３の）"等の使用は、同様の物の異なる例が、参照されていることを示すだけであり、このように説明された物が時間的、空間的のいずれか一方、順位付け又は任意の他の方法で、与えられた順序でなければならないということを意味することを意図していないことを示すだけである。

【００３０】

本明細書で使用されているように、"circuitry（回路）"という用語は、１以上のソフトウェア又は、ファームプログラムを実行する、特定用途向け集積回路（ＡＳＩＣ）、集積回路、電子回路、プロセッサ（共有、専用又はグループ）及び／又はメモリ（共有、専用又はグループ）組み合わせ論理回路、及び／又は説明された機能性を提供するその他の適切なハードウェア構成要素の一部を指し又は含むことができる。いくつかの例示的実施形態では、回路は１つ以上のソフトウェア又はファームウェアモジュール内に、実装されることができ、又は１つ以上のソフトウェア又はファームウェアモジュールによって、回路に関連付けられた機能が、実装されることができる。いくつかの例示的実施形態では、回路はハードウェアにおいて、少なくとも部分的に動作可能なロジックを含むことができる。

【００３１】

"logic（ロジック）"という用語は、例えば、コンピューティング装置の回路において埋め込まれたコンピューティングロジック及び／又はコンピューティング装置のメモリに蓄積されたコンピューティングロジックを指すことができる。例えば、ロジックは、コンピューティング機能及び／又は作動を実行するためにコンピューティングロジックを実行するコンピューティング装置のプロセッサによって、アクセス可能になることができる。１つの例では、ロジックは、様々なタイプのメモリ及び／又はファームウェア、例えば、様々なチップ及び／又はプロセッサのシリコンブロックにおいて組み込まれることができる。ロジックは、様々な回路、例えば、ラジオ回路、受信回路、制御回路、送信回路、トランシーバ回路、プロセッサ回路及び／又は同様のものの一部として含まれ及び／又は実装されることができる。１つの例では、ロジックは、ランダムアクセスメモリ、リードオンリーメモリ、プログラム可能メモリ、磁気メモリ、フラッシュメモリ、永続メモリ及び同様のものを含む揮発性メモリ及び／又は非揮発性メモリにおいて組み込まれることができる。ロジックは、例えば、ロジックを実行するために必要に応じて、１つ以上のプロセッサと連結されたメモリ、例えば、レジスタ、スタック、バッファ及び／又は同様のものを使用して１つ以上のプロセッサによって実行されることができる。

【００３２】

以下で使用されるように、"module（モジュール）"という用語は、実行カーネル環境

を拡張するためにコードを含むオブジェクトファイルのことである。
【００３３】
本明細書で使用されるように、"software engine（ソフトウェアエンジン）"という用語は、以下に使用されるように、実行カーネル環境を拡張するためにコードを含むオブジェクトファイルのことである。
【００３４】
以下で使用されるように、"digital wallet（デジタルウォレット）"という用語は、ソフトウェアと情報コンポーネントの両方のことである。デジタルウォレットは、クライアント側に蓄積されることができる。デジタルウォレットは店舗で決済端末にスマートフォンをタッチすることにより、支払い金額を転送するために、例えば、スマートフォンの近距離無線通信（ＮＦＣ）を使用することができる。
【００３５】
以下で使用されるように、"loyalty club customer（ロイヤリティクラブカストマー）"という用語は、ロイヤリティクラブの特典を有し、ロイヤリティベースのモバイルサービス、例えば、顧客ベースのロイヤリティカードアプリケーションを管理する企業間取引（Ｂ２Ｂ）の顧客のことである。
【００３６】
以下で使用されるように、"Back-End Platform（バックエンドプラットフォーム）"という用語は、デジタルウォレットサービスを管理し、制御するように構成され、選択されたサードパーティシステム、デジタルウォレットモジュール及び／又はデジタルウォレットエンジン及び／又はデジタルウォレットＳＤＫと相互作用するように構成されたデジタルウォレットシステムのクラウドプラットフォーム、バックエンドサーバのことである。
【００３７】
以下で使用されるように、"digital wallet SDK（デジタルウォレットＳＤＫ）"という用語は、デジタルウォレットモジュール及び／又はデジタルウォレットエンジンを含むことができる。デジタルウォレットＳＤＫは、顧客モバイルアプリケーション内に属し、統合される、デジタルウォレットソフトウエアプログラムのフロントエンドのことである。デジタルウォレットＳＤＫは、顧客のモバイルアプリケーションを通じて、エンドユーザのフロントエンド決済のインタラクションを管理することができる。デジタルウォレットＳＤＫは、デジタルウォレットプラットフォームに代わってベンダＰＯＳのＰＯＳ端末と通信するＮＦＣプロトコルを使用することができる。
【００３８】
以下で使用されるように、"customer relationship manager (CRM) application programming interface (API)（顧客関係管理（ＣＲＭ）アプリケーションプログラムインターフェース（ＡＰＩ））"という用語は、ＣＲＭと通信するように構成されたＡＰＩのことである。ＣＲＭは、１つ以上の顧客特典プログラムを管理するように構成されている。
【００３９】
以下で使用されるように、"Payment terminal（決済端末）"という用語は、例えば、エンドユーザが自身の消費者モバイルアプリケーションを使用して決済取引を実行することを決断するとき、様々な決済取引がなされることができる具体的な取引先及び／又はベンダ及び／又は店及び／又はその他のクレジットカード端末を含むことができる。
【００４０】
以下で使用されるように、"Customer Platform（顧客プラットフォーム）"は、例えば、デジタルウォレットプラットフォームを通じて、決済の準備のためにデジタルウォレットと連動するように構成されているパートナーの顧客のテクノロジープラットフォームを含むことができる。バックエンドテクノロジープラットフォームは、顧客及び／又はパートナーにより選択された決済の設定に応じて、デジタルウォレットＳＤＫと同様に、顧客モバイルアプリケーションと通信する。例えば、このプラットフォームは、例えば、

アマゾンウェブサービス（ＡＷＳ）及び／又はマイクロソフトＡＺＵＲＥ上で稼働するクラウドベースであるだろう。

【００４１】

以下で使用されるように、"cryptowallet module（クリプトウォレットモジュール）"は、公開鍵から生成されたそれぞれのクリプトウォレットのアドレスでランダムな公開－秘密鍵ペアを生成し、蓄積するように構成されたアプリケーション又はＳＤＫを指すことができる。クリプトウォレットのモジュールは、さらに、イーサリアムブロックチェーンやビットコイン、ソラナ、カルダノ、ポルカドット、アバランチ等のようなその他の同様のブロックチェーンネットワークなどの少なくとも１つのブロックチェーンネットワークと相互に作用するように構成されることができる。

【００４２】

"hash value（ハッシュ値）"という用語は、インプットにおいて、ごくわずかの違いですら完全に異なるアウトプットのハッシュ値を結果として生じるが、同じインプットにハッシュ関数を適用することで、結果としていつも同じハッシュ値が生じるように、任意長のインプットを取り、それを固定長に変換する数学の関数のアウトプットを指す。ハッシュ値は、メッセージの内容を有効化するために使用されている。内容が変更されたとき、新しいメッセージのハッシュ値は、オリジナルのメッセージから異なるだろう。

【００４３】

以下で使用されるように、"Payment token（決済トークン）"という用語は、例えば、リベスト－シャミア－エイドルマン－「ＲＳＡ」アルゴリズムのような既知の公開－秘密アルゴリズムで暗号化された、ユーザを一意に識別する情報を含むように構成された決済トークンと呼ばれた一意のプレースホルダを含むことができる。

【００４４】

いくつかの実施形態では、決済トークンは、ユーザによって所有されているブロックチェーンネットワーク上のアドレスを表す公開鍵及び例えば、名前、コンタクト情報、モバイルデバイスメタデータ、時間、地理位置情報データ等のようなその他の識別情報から構成されることができる。

【００４５】

例えば、もし、ユーザの一意の同一視できる情報は、以下のものを含む単純なＪＳＯＮフォーマットにおいて解析される場合。

【００４６】

{“address”:“0xb794f5ea0ba39494ce839613fffba74279579268”,“name”=“John Smith”}、決済トークンはそのとき、次の暗号化された文字列を含むことができる。

【００４７】

NjXlHoGdktQHFF5hJOPsy+SJmOhCTEgcYFVvpJCwuoR6TDQjmTMJI6G+ZlCf2mWYswjCz/6pSW/90EQmzp6Xiv4x8maycBsVwNIPa2t4dcWAGK0D9n5mkU aA2tz+pk1FrOYq4ttrLZc7pNzCaDpcNyOa8ZEnwAA7TSqNfsvqXfw=.

【００４８】

別の実装例では、同一視できる情報のみ暗号化されるが一方で、公開アドレスが現状のままでＪＳＯＮファイルにおいて解析される。識別文字列が「名前：ジョン＝スミス」であるところは、ＪＳＯＮファイルは次にように読み取る。

【００４９】

{“address”:“0xb794f5ea0ba39494ce839613fffba74279579268”,“idlnfo”:“XFftAh5RGXtlzJ622+vrg2nUBozV97KdyHRL300xBIGdiCRzf4h+bsxbYGFqCxHzLp4HidpJAc3PvzjPwE1AuQ==”}

【００５０】

上記は、本明細書で使用される専門用語を明らかにするための単なる例である。実際には、追加のパラメータは、ハッシュされた決済トークンの一部がそれぞれの使用のために一意のままであることを保証するためにバックエンドプラットフォームのデータベースに

おいてもまた蓄積される使い捨てのランダム数を含んでいる決済トークンの中に含まれることができる。

【００５１】

以下で使用されるように、"mobile application（モバイルアプリケーション）"という用語は、例えば、ロイヤリティクラブアプリケーション、ｅ－ウォレットアプリケーションなどの顧客の無線デバイス上にインストールされた少なくとも１つのアプリケーションを含むことができる。顧客アプリケーションは、デジタルウォレットＳＤＫを含むことができ、デジタルウォレットプラットフォーム及び顧客プラットフォームと相互に作用することができる。顧客モバイルアプリケーションは、例えば、ｉＯＳ及び／又はアンドロイド(登録商標)のような無線デバイスオペレーティングシステム上で稼働するように構成されることができる。

【００５２】

いくつかの例示的実施形態は、ｗｅｂ３エコシステムコンセプト及びブロックチェーン技術上に築くことができる。例えば、ｗｅｂ３エコシステムコンセプト及びブロックチェーン技術は、安全で、透明性のある分散型の決済システムを設立する。ブロックチェーンの使用は、仲介人なしのクリプトウォレットを介して、例えば、ビットコイン及びイーサリアムのような暗号通貨を、消費者及び企業が直接的に交換することを可能にする。決済は、検証され、分散型台帳上で、匿名で登録され、その中で例えば、そのコピーがクリプトウォレット上に蓄積されることができる。

【００５３】

例えば、一意のウォレット識別子としての使用のために公開鍵を利用可能にし、クリプトウォレットの所有者のみが秘密鍵にアクセスできるということが基本的な前提であるが、クリプトウォレット及びその資金の所有権の検証は、秘密鍵－公開鍵を使用することによって、達成することがきる。

【００５４】

ビットコインブロックチェーンの第１の実装の１０年以上後、技術は、消費者決済方法として採択を得ようともがき、ほとんど、投機的な投資チャネルのままである。

【００５５】

ブロックチェーン技術及び暗号化通貨が伝統的な集中的な決済手段及び法貨の実行可能な代替になる目的をまだ達成していない多くの理由がある。

【００５６】

これらの理由のいくつかは、例えば、ブロックチェーン設計において固有のエネルギの非効率に関係する。他の理由は、マネーロンダリング活動のためのプラットフォームを持ち出す取引の匿名性の性質に関連し、それでも別の理由は、取引検証機に与えられた高い取引手数料に関係する。

【００５７】

本開示の実施形態は、機密扱いのクレジットカード情報の伝送を扱うことのために複雑な標準の使用を避ける、決済有効性を検証するためのシステム、装置及び方法に関することができる。例えば、機密扱いのクレジットカードを伝達すること又は使用することの代わりに公開鍵を処理し、所有権及び決済を有効化するように構成された販売時点情報管理システムの端末の組み合わせにおける暗号化公開－秘密鍵認証を使用することは、機密扱いのクレジットカード情報（例えば、ＥＭＶ）の伝送を扱う複雑な標準の使用が現在避けられているので、節約につながり、また、よりシンプルなシステムにつながるだろう。

【００５８】

他の実施形態は、公開された一意の消費者識別子の所有権検証を可能にするシステム、装置、及び方法に関係させることができる。例えば、公開－秘密暗号技術の性質によると、クレジットカードナンバ、有効期限、ＣＶＣの数字及び所有権を証明するための４桁の暗証番号のような機密情報を伝達する理由はないのである。その代わりとして、公開鍵は、追加の情報と共に伝達されることができるが、本開示は、消費者が伝達された公開鍵の所有権を証明することを可能にする装置、システム及び方法を紹介する。

【００５９】
しかしながら、いくつかの実施形態は、またブロックチェーンに関する手数料コストなしで、クリプトウォレットベース決済検証を可能にするように構成されることができる。ブロックチェーンベースの決済は、安全と考えられることができるが、決済検証目的で、公開分散型台帳において各々の決済を記録しなければならないことは、非効率と考えられることができる。本開示の使用でブロックチェーンネットワーククライアントとして、クリプトウォレットに既にアクセス権を有する公衆の多数の人は、自身らの購入は、分散型公衆台帳で公開されないので、暗号化取引に関連付けられる手数料なく、プライバシーの懸念がなしで自身らのクリプトウォレットで商品及びサービスを購入するためにウォレットを使用することができる。

【００６０】
有利なことに、デバイス及びシステムの設定は、その中に、複数の要因の認証において決済アカウントの所有権を認証することを許可する一方で、ユーザからは、１つのアクションを要求するのみである。

【００６１】
例えば、ユーザがチェックアウト時にスマートフォンの近距離無線通信（ＮＦＣ）チップを決済端末の近くに持ってくるとき、自身は、一つのアクションを実行するだけである。ソフトウェアディベロップメントキット（ＳＤＫ）を含むアプリケーションは、ユーザを表す公開鍵で決済トークンを決済端末に送付し、決済端末からサーバへチェックアウト情報が中継されるだろう。受信した決済トークンと公開鍵をユーザデータベースで相互参照し、ユーザをそれと関連付けた後、サーバは、取引情報をユーザと事前に関連付けられたスマートフォンに中継することができる。

【００６２】
事前にセットされた条件（例えば、もし、スマートフォンスクリーンがロック解除になれば、スマートフォンの地理位置情報が決済端末と類似である）が実現した際に、ＳＤＫは、公開鍵に対応する秘密鍵を使用し、事前に受信した取引メッセージに署名し、署名された取引メッセージを元のサーバへ返す。サーバは、そのとき、受信され署名されたメッセージを復号し、署名されたメッセージの複数のパラメータをデータベースエントリと比較することができる。複数のパラメータは、署名されたメッセージから得た公開鍵及び決済トークンと共に事前に受信された公開鍵、決済端末から受信された、署名付きメッセージ及び取引情報の内容、決済端末から受信した決済トークンのユーザ情報及び第１の登録において集められたユーザ情報のうちの少なくとも１つ含む。

【００６３】
見ての通り、ユーザが１つのアクションのみ実行することが要求されていたが、２つの異なる視点から公開－秘密認証の特性を活用して、自身の同一性及び取引は、複数の要因の認証で検証された。第１の視点は、決済トークンの公開鍵と登録の間に提供された公開鍵を比較するときである。第２の視点は、決済トークンの公開鍵と対応する秘密鍵により署名されたメッセージとを比較するときである。

【００６４】
最初に本発明の例示的な実施形態を描写する図１を参照すると、決済有効性を検証するためのシステム１０が示されている。システム１０は、少なくとも１つの消費者無線デバイス１００、バックエンドプラットフォーム１１０、少なくとも１つの決済端末１２０及び金融エンティティ１３０の顧客プラットフォーム１３１を含むことができる。

【００６５】
いくつかの例示的な実施形態では、無線デバイス１００は、プロセッサ１０１、ＮＦＣ通信スイート１０２、インターネットモデム１０３、クリプトウォレットアプリケーション１０４、デジタルウォレットＳＤＫ１０５、決済トークンストレージモジュール１０６を含むことができる。プロセッサ１０１は、デジタルウォレットＳＤＫ１０５及びクリプトウォレットモジュール１０４を含むことができるモバイルアプリケーション１０７の少なくとも１つを稼働するように構成されることができる。モバイルアプリケーション１０

７は、例えば、イーサリアムブロックチェーンのようなブロックチェーンネットワークと相互に作用するように構成されることができる。

【００６６】

いくつかの例示的な実施形態では、クリプトウォレット１０４は、少なくとも１つの公開－秘密鍵ペア１０８を含むことができ、決済トークンストレージモジュール１０６は、少なくとも１つの決済トークン１０９を含む。

【００６７】

いくつかの例示的な実施形態では、インターネットモデム１０３は、例えば、６０Ｇｈｚ、５Ｇ、６Ｇ、ＷｉＦｉ、セルラー通信プロトコルの任意の一つ、ＩＥＥＥ８１１プロトコルの任意の一つ等のような共有無線通信プロトコルを使用することができる。

【００６８】

いくつかの例示的な実施形態では、取引先のＰＯＳの決済端末１２０は、例えば、処理回路１２１、ＮＦＣ通信スイート１２２、インターネットモデム１２３、少なくとも１つの決済リクエストメッセージを生成するためのトランザクショジェネレータモジュール１２４、及び決済トークントランシーバモジュール１２５を含むことができる。

【００６９】

例えば、処理回路１２１は、トランザクショジェネレータモジュール１２４及び決済トークントランシーバモジュール１２５を含むアプリケーションを稼働するように構成されることができる。

【００７０】

決済端末１２０は、バックエンドプラットフォーム１１０及び消費者無線デバイス１００とデジタル通信内に存在することができる。

【００７１】

例えば、バックエンドプラットフォーム１１０は１つ以上の決済端末１２０、消費者無線デバイス１００及び様々な金融エンティティ１３０の顧客プラットフォーム１３１とのデジタル通信内に存在することができる。バックエンドプラットフォーム１１０は、取引データベース１１１、メッセージ生成モジュール１１２、消費者データベース１１６、決済トークン復号モジュール１１３、メッセージ署名復号モジュール１１４及び取引検証モジュール１１５の機能を実行するように構成された処理回路（示されていない）を含むことができる。

【００７２】

図２を参照すると、いくつかの実施形態の代表的な実装は、以下の方法から理解されるだろう。この方法は、本発明の他の実施形態で実行されることができるが、明確にするために、構造的構成要素は、図１においてそれらの照合により参照される。

【００７３】

決済有効性を検証するために方法は、例えば、消費者無線デバイス１００上にインストールされたモバイルアプリケーション１０７を使用することによって、公開－秘密鍵ペア１０８を提供することを含むことができる（テキストボックス２０１）。

【００７４】

いくつかの例示的な実施形態では、ユーザがモバイルアプリケーションにサインインすると、コマンドは、クリプトウォレットモジュール１０４に渡され、公開鍵と秘密鍵を含むことができる公開－秘密鍵ペア１０８（図１）を生成するように設定されることができる。いくつかの実施形態では、公開－秘密鍵ペア１０８の公開鍵（図１）は、少なくとも１つのブロックチェーンネットワークを準拠したプロセスにおいてクリプトウォレットアドレスを作成するために使用されることができる。

【００７５】

その他のいくつかの例示的な実施形態では、公開－秘密鍵ペア１０８（図１）は、各々の決済を検証するまえに生成されることができる。さらに他の実施形態では、公開－秘密鍵ペア１０８は、ユーザのモバイルアプリケーション１０７への第１の登録において生成されることができる。他の実施形態では、ユーザは、存在する公開－秘密鍵ペアをクリプ

トウォレットモジュール１０４（図１）へインポートすることができる。
【００７６】
いくつかの例示的な実施形態では、本方法は、消費者無線デバイス１００（図１）上でインストールされることができるモバイルアプリケーション１０７（図１）によって決済有効性検証のための決済トークン１０９を生成することを進行していくことができる（テキストボックス２０２）。いくつかの実施形態では、公開鍵及び／又はクリプトウォレットアドレス及び／又は任意の他のユーザ識別情報は、決済トークンを生成するために決済端末１２０（図１）に渡されることができる。
【００７７】
いくつかの例示的な実施形態では、決済トークン１０９（図１）は、公開鍵及び消費者無線デバイスに関連付けられたユーザＩＤを含む。
【００７８】
他の例示的な実施形態では、決済トークン１０９（図１）は、デジタルウォレットＳＤＫ１０５（図１）によって生成されることができ、決済トークンストレージデータベース１０６（図１）内に蓄積されることができる。
【００７９】
いくつかの実施形態では、デジタルウォレットＳＤＫ１０５（図１）は、クリプトウォレットモジュール１０４（図１）から公開－秘密鍵ペア１０８（図１）の公開鍵を取得することができ、その後、これにより決済トークン１０９（図１）を生成することができる。この実施形態では、公開－秘密鍵ペア１０８（図１）の秘密鍵は、消費者無線デバイス１００（図１）上のデータベース内に安全に蓄積されたままであることができ、公開－秘密鍵ペア１０８（図１）の公開鍵は、またバックエンドプラットフォーム１１０上（図１）の消費者データベース１１６（図１）内及び決済端末１２０（図１）上で後に転送され蓄積されることができる。
【００８０】
いくつかの例示的な実施形態では、本方法は、決済端末１２０（図１）に消費者無線デバイス１００（図１）の決済トークン１０９（図１）を提供することで続行することができる（テキストボックス２０３）。いくつかの実施形態では、決済トークンは、ＮＦＣラジオ１０２（図１）及び／又はインターネットモデム１０３（図１）（例えば、ＬＴＥ、ＧＳＭ、ＷｉＦｉ、Ｂｌｕｅｔｏｏｔｈラジオ）のうちの少なくとも１つを介して、消費者無線デバイス１００（図１）から、決済端末１２０（図１）へ送信されることができる。
【００８１】
いくつかの例示的な実施形態では、本方法は、取引情報を提供することで続行することができる（テキストボックス２０４）。例えば、決済端末１２０（図１）の処理回路１２１（図１）は、例えば、支払期日、製品リスト及び／又は加盟店ＩＤのような取引情報メッセージ及び決済トークン１０９（図１）を含む決済リクエスト１２６（図１）を生成するように構成されることができる。決済リクエスト１２６は、インターネットモデム１２３（図１）を介して消費者無線デバイス１００によって提供されたバックエンドプラットフォーム１１０（図１）に送信されることができる。
【００８２】
次に述べることは、実例である。すなわち製品をスキャンしているとき、それらの価格及びその他の情報は決済端末１２０（図１）によって、取得される。消費者が、決済端末１２０（図１）のより近くに、自身の無線デバイス１００（図１）を結び付け、及び／又は近づけ、ＮＦＣ通信を介して、決済端末１２０（図１）に自身の決済トークン１０９（図１）を提供した後、決済リクエストに関連する情報は、決済端末１２０（図１）に表示されることができる。決済端末１２０（図１）は、取引情報メッセージを含む決済リクエスト１２６（図１）合計し、提供することができる。例えば、取引情報は、支払期日、加盟店ＩＤを含むことができる。いくつかの実施形態では、決済端末１２０（図１）は、メッセージを署名する前に有効性のために、消費者無線デバイス１００（図１）にもまた取

引情報メッセージ、及び／又はそのハッシュ値を送信するように構成されることができる。

【００８３】

いくつかの例示的な実施形態では、本方法は、決済トークン１０９（図１）データ及び決済リクエストメッセージの取引情報メッセージを解釈し、蓄積することで続行することができる（テキストボックス２０５）。例えば、解釈することは、決済トークン復号モジュール１１３（図１）によって、行われることができ、蓄積することは、バックエンドプラットフォーム１１０（図１）上の取引データベース内で行われることができる。

【００８４】

いくつかの例示的な実施形態では、決済トークン１０９（図１）が、サービスプロバイダと関連付けられた公開鍵で暗号化されることができるところでは、決済トークン１０９（図１）は、決済トークン復号モジュール１１３（図１）によって取得された対応する秘密鍵で復号されることができる。

【００８５】

いくつかの例示的な実施形態では、本方法は、金融エンティティ１３０（図１）との取引を承認することで続行することができる（テキストボックス２０６）。例えば、取引情報及び消費者の同一性は、金融エンティティ１３０（図１）の顧客プラットフォーム１３１（図１）へデジタルに転送されることができる。いくつかの例示的な実施形態では、消費者は、金融エンティティ１３０によって発行されたクレジットカード、銀行口座を保有し、及び／又は自身は、金融エンティティ１３０（図１）によって、管理された消費者ロイヤリティプログラムのメンバである。

【００８６】

例えば、消費者が、取引のためにカバーするのに十分な信用又は資産を有するか否かのような、取引が事前に定義された規則に一致するかを検証した後、金融エンティティ１３０（図１）は、事前に決められたコードメッセージを返すことにより取引を確認することができる。

【００８７】

いくつかの例示的な実施形態では、取引情報メッセージは、例えば、購入された製品が適格な製品のリストに掲載されることができるか否か、及び／又は取引先が、適格なビジネスの特定リストに掲載されることができるかどうかのような様々な規則を比較されることができる。

【００８８】

いくつかの例示的な実施形態では、本方法は、バックエンドプラットフォーム１１０（図１）によって取引検証メッセージを生成し、対応する決済トークン１０９（図１）で関連付けられた消費者にそれを提供することで続行できる（テキストボックス２０７）。

【００８９】

例えば、取引検証メッセージは、加盟店ＩＤ及び支払期日を含むことができる決済に関連する情報を含む。取引検証メッセージは、メッセージ生成モジュール１１２（図１）によって生成されることができ、例えば、消費者の無線デバイス１００（図１）上にインストールされることができるモバイルアプリケーション１０７（図１）、電話番号、及び／又は電子メールアドレスのような消費者に関連付けられたアドレスへ送信されることができる。

【００９０】

いくつかの例示的な実施形態では、本方法は、取引検証メッセージに署名することと、復号のためにバックエンドプラットフォーム１１０（図１）にそれを送信することとで続行することができる（テキストボックス２０８）。例えば、メッセージに署名する前に、自身の確認のために（例えば、確認ボタンを押すこと）、モバイルアプリケーション１０７（図１）のユーザインターフェースを使用して、取引の詳細は消費者に提示されることができる。

【００９１】

別の例では、デジタルウォレットＳＤＫは、少なくとも１つの条件又は規則の実現の上でメッセージを署名することで続行することができる。例えば、その規則は、この取引に関して、決済端末から事前に受信した第１のメッセージのハッシュ値と同一である第２のメッセージのハッシュ値のための規則と、消費者無線デバイスがロック解除されたときの規則であり、無線デバイスの地理位置情報が決済端末の既知の地理位置情報の事前に決められた範囲内であるか否かの規則と、署名されるための取引が消費者又はその代わりの者等によって設定された定期の許容額を超えないか否かの規則を含むことができる。

【００９２】

いくつかの実施形態では、当該既知の地理位置情報の事前に決められた範囲が、既知の地理位置情報の中心から０から５メータの間である。

【００９３】

いくつかの例示的な実施形態では、取引検証メッセージは、公開－秘密鍵ペアの秘密鍵で署名されることができ、バックエンドプラットフォーム１１０（図１）に送り返されることができる。

【００９４】

いくつかの例示的な実施形態では、メッセージ復号モジュール１１４（図１）は、消費者と関連付けられた公開鍵で署名された取引検証メッセージを復号することができる。

【００９５】

他の実施形態では、メッセージ復号モジュール１１４（図１）は、署名された取引検証メッセージの内容及び同一の秘密鍵を全て明らかにすることなく、メッセージに署名するために使用されることができる秘密鍵に対応する公開鍵を引き出すための適切なアルゴリズムを適用することができる。秘密鍵によって署名されたメッセージを復号するプロセスは、例えば、ＥＩＰ７１２イーサリアム標準に従うことができる。当然、その他の適切なアルゴリズムは、同様の結果を達成するのに熟考されることができる。

【００９６】

いくつかの例示的な実施形態では、本方法は、取引検証メッセージの署名者の同一性及び取引の有効性を検証することで続行することができる（テキストボックス２０９）。例えば、取引検証モジュール１１５（図１）は、復号された検証メッセージを決済端末から事前に受信した取引情報メッセージを比較することができる。受信された署名付きメッセージは、消費者の秘密鍵を使用して署名され、取引データベース１１１（図１）から消費者の公開鍵で復号されることできるので、もし一致が見つかれば、そのとき取引情報でメッセージを署名した人の同一性は、検証される。

【００９７】

別の例では、取引検証モジュール１１５（図１）は、復号された署名付きメッセージからの公開鍵パラメータ及び検証メッセージを取引データベース１１１（図１）からの同一のものと比較することができる。

【００９８】

いくつかの例示的な実施形態では、本方法は、取引結果を通知することで続行することができる（テキストボックス２１０）。例えば、バックエンドプラットフォーム１１０（図１）は、取引確認メッセージを送信することによって消費者、取引先及び金融エンティティ１３０（図１）に決済有効性検証の結果を通知することができ、こうして商品、サービス及び金銭の交換を可能にし、又は検証されない取引を防止する。

【００９９】

本方法は、異なる順序で又は同時に実行されることができるため、上記で説明された方法の実施の順序は、重要ではないことを理解されるべきである。

【０１００】

図３を参照すると、図３は、いくつかの例示的な実施形態のとおり、決済トークンを生成するための方法のフローチャートの実例である。いくつかの例示的な実施形態では、この方法は、消費者無線デバイス１００（図１）上にインストールされたモバイルアプリケーション１０７（図１）に含まれたデジタルウォレットＳＤＫ１０５（図１）によって実

行されることができる。いくつかの他の実施形態では、次の方法は、決済端末１２０（図１）によって、実行されることができる。

【０１０１】

いくつかの実施形態では、消費者無線デバイス１００のクリプトウォレットモジュール１０４は、ランダムな公開－秘密鍵ペア１０８を生成し、蓄積することができる。

【０１０２】

いくつかの例示的な実施形態では、本方法は、公開鍵を生成するために使用されるアルゴリズムへのインプットとして、適切であることができるランダム数を生成することにより秘密鍵を生成することを始めることができる（テキストボックス３０１）。

【０１０３】

いくつかの例示的な実施形態では、本方法は、例えば、楕円曲線デジタル署名アルゴリズムのようなアルゴリズムで秘密鍵をハッシュすることにより秘密鍵に基づいて公開鍵を生成することで続行することができる（テキストボックス３０２）。

【０１０４】

いくつかの例示的な実施形態では、本方法は、クリプトウォレットアドレスとして１組の文字を識別するために使用される事前に決められた形式に公開鍵をフォーマットすることによって、公開鍵のウォレットアドレスを生成することで続行することができる（テキストボックス３０３）。例えば、公開鍵の最後の２０バイトを抜き取ること及び先頭に、「Ｏｘ」を追加する。

【０１０５】

いくつかの例示的な実施形態では、本方法は、一意の消費者識別情報を取得し、ハッシュすることで続行することができる（テキストボックス３０４）。いくつかの実施形態では、識別情報は、消費者コンタクト情報（例えば、名前、電話番号、電子メール）、無線デバイスＩＤ（例えば、ＩＭＥＩ番号）、決済情報（例えば、銀行口座、クレジットカード）、地理位置情報及び消費者ＩＤ番号のうちの少なくとも１つを含むことができる。

【０１０６】

いくつかの例示的な実施形態では、バックエンドプラットフォーム１１０（図１）は、一意のランダム数を生成し、ユーザデータベース内に一意のランダム数を蓄積し、決済トークンが構築されるとき、ノンスとして包含するために安全に送信することができる。この特徴は、識別情報に変化がなかった場合に、同一の決済トークンを生成することを防ぐ。

【０１０７】

本方法は、公開鍵及び一意のユーザ情報のハッシュ値を含む決済トークンを構築することで続行することができる（テキストボックス３０５）。いくつかの実施形態では、公開鍵又はクリプトウォレットアドレスは、例えば、バックエンドプラットフォーム１１０のより読み取り可能なＪＳＯＮファイルのような共通の適切なデータ構造に消費者識別情報のハッシュ値を構造化されることができる。

【０１０８】

図４を参照すると、図４は、いくつかの例示的な実施形態のとおり、サービスの初期ユーザ登録のための方法のフローチャートの実例である。いくつかの例示的な実施形態では、この方法は、消費者無線デバイス１００（図１）上にインストールされたモバイルアプリケーション１０７（図１）内に含まれることができるデジタルウォレットＳＤＫ１０５（図１）によって実行される。

【０１０９】

いくつかの例示的な実施形態では、本方法は、デジタルウォレットＳＤＫ１０５（図１）及びクリプトウォレットでランダム公開－秘密鍵ペア１０８（図１）を生成し、蓄積することを開始し（テキストボックス４０１）、ユーザの個人情報からインプットを受信することで続行することができる（テキストボックス４０２）。例えば、個人情報は、名前、電話番号、アドレス、電子メールアドレス、誕生日及び／又は顔写真のうちの少なくとも１つを含むことができる。

【０１１０】
いくつかの例示的な実施形態では、本方法は、無線デバイスの固有識別子及びメタデータを取り出すことで続行することができる（テキストボックス４０３）。この情報は、デジタルウォレットＳＤＫを実行する無線デバイスのＩＭＥＩ番号、デバイスモデル、オペレーティングシステムバージョン、及びＳＤＫバージョンのうちの少なくとも１つを含むことができる。
【０１１１】
いくつかの例示的な実施形態では、本方法は、決済情報のインプットを受信することで続行することができる（テキストボックス４０４）。この情報は、クレジットカード情報、銀行口座番号、ロイヤリティプログラム情報のうちの少なくとも１つを含むことができる。
【０１１２】
いくつかの実施形態では、決済情報は、例えば、銀行モバイルアプリケーション、ロイヤリティプログラムモバイルアプリケーション等のような無線デバイス上にインストールされた金融エンティティのアプリケーションへのインターフェースを介して受信されることができる。
【０１１３】
いくつかの実施形態は、決済情報は、金融エンティティのウエブサイトで記録されるとき、無線デバイス上にインストールされたブラウザへのインターフェースを介して受信されることができる。
【０１１４】
任意の方法で、バックエンドプラットフォームからノンスをリクエストし、受信する（テキストボックス４０５）。
【０１１５】
例えば、個人情報、デバイス情報、決済情報及びノンスを含む情報を、バックエンドプラットフォーム１１０の公開鍵で暗号化する（テキストボックス４０６）。
【０１１６】
いくつかの例示的な実施形態では、本方法は、バックエンドプラットフォーム１１０（図１）に暗号化された情報及びデジタルウォレットＳＤＫ１０５（図１）によって、生成された公開鍵を送信すること、要求された秘密鍵で暗号化された情報を復号すること、バックエンドプラットフォーム１１０（図１）内の消費者データベース１１６（図１）に全ての情報を蓄積することで続行することができる（テキストボックス４０７）。
【０１１７】
いくつかの実施形態では、本方法は、さらに決済情報に関連付けられた金融エンティティ１３０（図１）とのクレジットのためにユーザを承認することを含む（テキストボックス４０８）。例えば、もし銀行口座情報が入力されたら、バックエンドプラットフォーム１１０（図１）は、銀行がユーザによってリクエストされた取引をカバーすること及びどんな規則下でカバーするのか（例えば、国内の取引のみ受け入れる）を確認するために銀行の関連付けられた顧客プラットフォーム１３１（図１）に照会することができる。
【０１１８】
いくつかの例示的な実施形態では、本方法は、承認され及び／又は登録されたユーザのためにユーザＩＤを生成することと、ユーザによって提供された公開－秘密鍵ペア１０８（図１）の公開鍵でそれを暗号化することと、公開－秘密鍵ペア１０８（図１）の適切な秘密鍵での復号のためにユーザの無線デバイス１００（図１）に、暗号化されたユーザＩＤを送信することと及び将来の取引において決済トークン１０９（図１）として使用のための決済トークンストレージ１０６（図１）内に公開鍵を保存することを含むことができる。
【０１１９】
いくつかの実施形態では、ユーザＩＤは、ランダム数、一意のシリアル番号、特定の順序で配列されたユーザ情報のハッシュ値の内、少なくとも１つを含むことができる。

【０１２０】
ここで、図５を参照すると、図５は、いくつかの例示的な実施形態のとおり、製造の製品５００の概要の実例である。製品５００は、処理デバイス５２０によって実装され、動作可能であり、コンピュータで実行可能な命令５３０を含むことができる１つ以上の実体的なコンピュータ可読の非一過性のストレージ媒体５１０を含むことができ、少なくとも１つのコンピュータプロセッサのよって実行されたとき、少なくとも１つの処理回路１２１（図１）が、決済有効性を検証するための１つ以上のプログラム命令を実装することを可能にすることができ、及び／又は図１～４の参照により上記で説明されたように、１つ以上の作動、通信及び／又は機能性を実行し、引き出し及び／又は実装することを可能にすることができる。"non-transitory machine-readable medium（非実体的で機械可読の媒体）"という語句は、一過性の伝搬信号であることを唯一の例外として全てのコンピュータで可読の媒体を含むことを指示している。

【０１２１】
いくつかの例示的な実施形態では、製品５００及び／又は機械可読ストレージ媒体５１０は、メモリ、非揮発性メモリ、取り外し可能又は取り外し不可能なメモリ、消去可能又は消去不可能なメモリ、書き込み可能又は再書き込み不可能なメモリ等を含む、データを蓄積することができる１つ以上の種類のコンピュータ可読ストレージ媒体を含むことができる。例えば、機械可読ストレージ媒体５１０は、例えば、ＲＡＭ、ＤＲＡＭ、ＲＯＭ、プログラム可能なＲＯＭ（ＰＲＯＭ）、消去可能でプログラム可能なＲＯＭ（ＥＰＲＯＭ）、電子的に消去可能でプログラム可能なＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリ、ハードディスクドライブ（ＨＤＤ）、ソリッドステートドライブ（ＳＤＤ）、フュージョンドライブ等のような任意の種類のメモリを含むことができる。コンピュータ可読ストレージ媒体は、通信リンク、例えば、モデム、ラジオ又はネットワーク接続を介して搬送波又は他の伝播媒体において統合されたデータ信号によって搬送されるリモートコンピュータから要求するコンピュータへ、コンピュータプログラムをダウンロードし、転送することに関係する任意の適切な媒体を含むことができる。

【０１２２】
いくつかの例示的な実施形態では、処理デバイス５２０は、ロジックを含むことができる。ロジックは、もし機械により実行されれば、本明細書で記載の方法、処理及び／又は作動を機械に実行させることができる命令、データ及び／又はコードを含むことができる。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デバイス、処理デバイス、コンピューティングシステム、処理システム、コンピュータ、プロセッサ等を含むことができ、ハードウェア、ソフトウェア、ファームウェア等の任意の適切な組合せを使用して実装されることができる。

【０１２３】
いくつかの例示的な実施形態では、処理デバイス５２０は、ソフトウェア、ファームウェア、ソフトウェアモジュール、アプリケーション、プログラム、サブルーチン、命令、命令セット、コンピューティングコード、ワード、値、記号等を含むことができ、それらとして実装されることができる。命令５４０は、ソースコード、コンパイルコード、インタープリターコード、実行可能コード、静的コード、動的コード等のような任意の適切な種類のコードを含むことができる。特定の機能を実行するプロセッサを命令するために事前に定義されたコンピュータ言語、方法又は構文により、命令は、実装されることができる。命令は、Ｃ言語、Ｃ＋＋、Ｃ＃、Ｊａｖａ、Ｐｙｔｈｏｎ、ＢＡＳＩＣ、Ｍａｔｌａｂ、アセンブリ言語、機械コード等のような任意の適切な高レベルの、低レベルの、オブジェクト指向の、ビジュアルの、コンパイルされた及び／又はインタープリターされた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。

【０１２４】
図６を参照すると、図６は、本発明の例示的な実施形態を描写している。本明細書で描写された典型的なプロセスは、クリプトウォレットからの公開－秘密鍵ペアのような消費者情報６００、クレジットカード情報のような支払い手段、及び一意の識別子であること

ができるＳＤＫ－ＩＤを収集し、サーバプラットフォーム６０６に送信するＳＤＫ６０１を含むことができる登録段階６００でまず始めることができる。

【０１２５】

消費者が、スキャンされた製品６０４を購入するために、ＰＯＳ６０３に近づくとき、結果として消費者は、決済トークンにある公開鍵をＰＯＳ６０３の決済端末に送付することとなることができるＳＤＫ６０１を搭載するデバイスを表示することができる。

【０１２６】

このプロセスは、ＰＯＳが公開鍵及び取引情報メッセージ（例えば、支払総額）６０５を含むことができる決済リクエストをサーバプラットフォーム６０６へ送信することで続行することができる。

【０１２７】

このプロセスは、サーバプラットフォーム６０６が決済トークン又は公開鍵によって識別されたＳＤＫ６０１、取引情報メッセージによって事前に提供されたそのような詳細を含むことができる取引検証メッセージ６０７を送信することで続行することができる。

【０１２８】

このプロセスは、ＳＤＫ６０１が、消費者の承認後に取引検証メッセージを署名し６０８をサーバプラットフォーム６０６へ伝達することで続行することができる。

【０１２９】

このプロセスは、サーバプラットフォーム６０６が、ＳＤＫ６０１により署名された取引検証メッセージ、ＰＯＳ６０３によって提供された取引情報メッセージとの間の情報の比較に基づいて決済を有効化することで続行することができる。

【０１３０】

このプロセスは、サーバプラットフォーム６０６が決済の承認又は拒否をＰＯＳ６０９へ通知することで続行することができる。上記で説明された主題は、実例の方法によって提供されただけであり、限定的なものとして解釈されるべきではない。また、次の特許請求の範囲において明らかにしており、図解され説明された例示の実施形態及び適用に従うことなく、本発明の真実の精神及び範囲から外れることなく、本明細書で説明された主題に様々な修正及び変更が行われることができる。

【図面】

【図１】

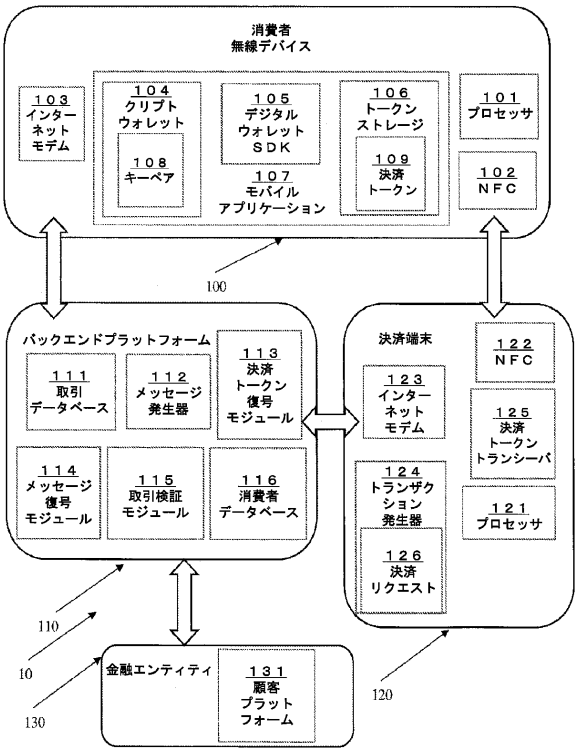

FIG. 1

【図２】

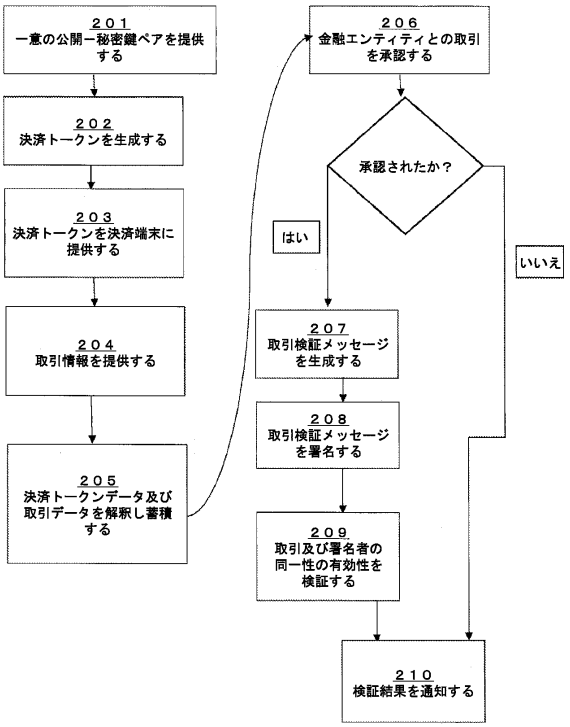

FIG. 2

【図３】

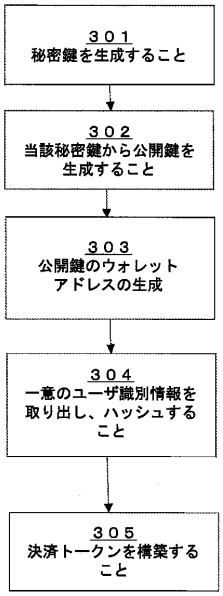

FIG. 3

【図４】

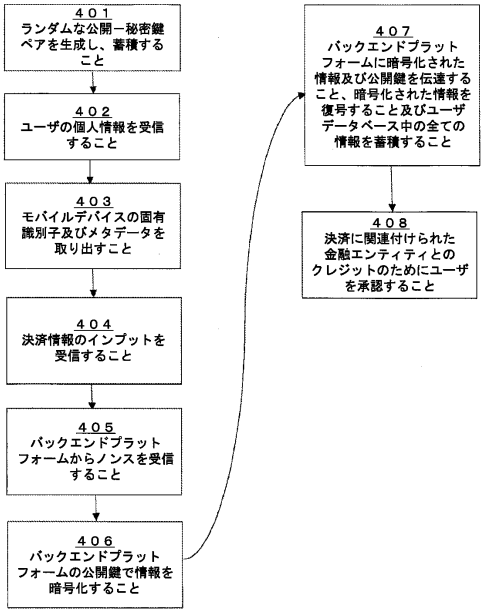

FIG. 4

【図５】

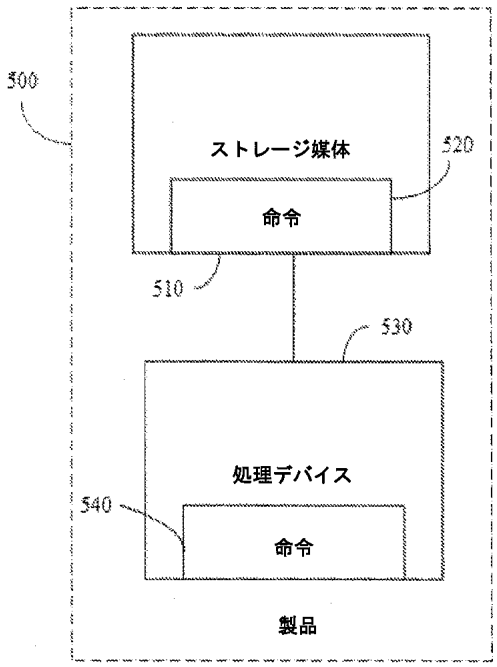

FIG. 5

【図６】

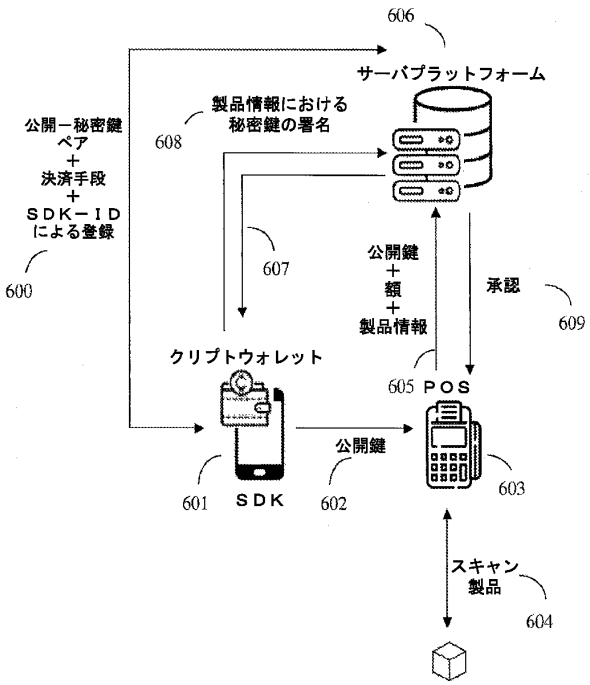

FIG. 6

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2023/050615

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(2023.01)i; ***G06Q 20/32***(2023.01)i; ***G06Q 20/36***(2023.01)i
CPC:G06Q 20/3829; G06Q 20/38; G06Q 20/3223; G06Q 20/36

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 20/38; G06Q 20/32; G06Q 20/36
CPC:G06Q 20/3829; G06Q 20/38; G06Q 20/3223; G06Q 20/36

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)

Databases consulted: Esp@cenet, Google Patents, Google Scholar, Derwent Innovation, Similari (AI-based) Search terms used: verify, POS, compare, public key, backend, generated, payment terminal, private key, crypto wallet, message, sign

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016125402 A1 (LEE et al.) 05 May 2016 (2016-05-05) The whole document	1-17
A	US 2020311289 A1 (Cooper et al.) 01 October 2020 (2020-10-01) The whole document	1-17

☐ Further documents are listed in the continuation of Box C. ☑ 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
"D" document cited by the applicant in the international application
"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
16 July 2023	**18 July 2023**
Name and mailing address of the ISA/IL **Israel Patent Office** **Technology Park, Bldg.5, Malcha, Jerusalem, 9695101,** **Israel** **Israel** Telephone No. **972-73-3927220** Email: **petoffice@justice.gov.il**	Authorized officer **GORBUNOVA Yelena** Telephone No.

Form PCT/ISA/210 (second sheet) (July 2022)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2023/050615

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2016125402 A1	05 May 2016	US 2016125402 A1	05 May 2016
		KR 20160052015 A	12 May 2016
		KR 102305825 B1	27 September 2021
US 2020311289 A1	01 October 2020	US 2020311289 A1	01 October 2020
		US 11475139 B2	18 October 2022
		CA 3135088 A1	01 October 2020
		CN 113924751 A	11 January 2022
		EP 3716566 A1	30 September 2020
		EP 3716566 B1	07 June 2023
		EP 3716566 C0	07 June 2023
		IL 273628 A	30 September 2020
		WO 2020193793 A1	01 October 2020

Form PCT/ISA/210 (patent family annex) (July 2022)

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,MU,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,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

（特許庁注：以下のものは登録商標）
１．ＢＬＵＥＴＯＯＴＨ
２．ＪＡＶＡ
３．ＰＹＴＨＯＮ
４．ＭＡＴＬＡＢ
５．ｉＯＳ

弁理士　那須 威夫
(74)代理人　100141553
弁理士　鈴木 信彦
(74)代理人　100233504
弁理士　北岡 尚子
(72)発明者　ベン－アヴィ デヴィッド
イスラエル ４６５９０７１ ヘルツリーヤ アリク アインシュタイン ストリート ３
(72)発明者　ローゼンホイズ ガイ
イスラエル ４６５９０７１ ヘルツリーヤ アリク アインシュタイン ストリート ３

Ｆターム（参考）　5L020　AA66 AA72