(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7166453号
(P7166453)

(45)発行日　令和4年11月7日(2022.11.7)

(24)登録日　令和4年10月27日(2022.10.27)

(51)国際特許分類

H04L 9/32 (2006.01)		H04L	9/32	200C
G06Q 20/38 (2012.01)		G06Q	20/38	322
		H04L	9/32	200Z

請求項の数　15　（全38頁）

(21)出願番号　特願2021-525733(P2021-525733)
(86)(22)出願日　令和1年12月11日(2019.12.11)
(65)公表番号　特表2022-510790(P2022-510790A)
(43)公表日　令和4年1月28日(2022.1.28)
(86)国際出願番号　PCT/US2019/065621
(87)国際公開番号　WO2020/123591
(87)国際公開日　令和2年6月18日(2020.6.18)
審査請求日　令和3年6月30日(2021.6.30)
(31)優先権主張番号　16/217,734
(32)優先日　平成30年12月12日(2018.12.12)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　520107951
アメリカン エキスプレス トラヴェル リレイテッド サーヴィシーズ カンパニー， インコーポレイテッド
AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY， INC.
アメリカ合衆国 １０２８５－４９００ ニューヨーク州、ニューヨーク、ヴィージー ストリート ２００
２００ Vesey Street， New York， NY １０２８５－４９００ U. S. A.
(74)代理人　100083116
弁理士　松浦 憲三

最終頁に続く

(54)【発明の名称】　ブロックチェーンを使用するゼロ知識証明支払い

(57)【特許請求の範囲】

【請求項１】

支払い処理中、販売者システムによって呼び出されたことに応じて、ゼロ知識証明（ＺＫＰ）スマート・コントラクトによって、検証関数を実行することであって、前記販売者システムは、証明、顧客ハッシュ、販売者ハッシュ、及び購入金額を前記ＺＫＰスマート・コントラクトに送信することによって前記ＺＫＰスマート・コントラクトを呼び出し、前記検証関数は、検証鍵、前記証明、及び前記顧客ハッシュを、前記検証関数に入力することによって実行され、前記検証関数は、ゼロ知識証明アルゴリズムに関連付けられる、実行することと、

前記検証関数が成功したことに応じて、前記ＺＫＰスマート・コントラクトによって、前記顧客ハッシュに関連付けられた顧客口座残高を調整することであって、前記顧客口座残高は、前記購入金額に基づいて調整され、前記顧客口座残高は、ブロックチェーン上で維持される、調整することと、

前記ＺＫＰスマート・コントラクトによって、前記販売者ハッシュに関連付けられた販売者口座残高を調整することであって、前記販売者口座残高は、前記購入金額に基づいて調整され、前記販売者口座残高は、ブロックチェーン上で維持される、調整することと、

前記ＺＫＰスマート・コントラクトによって、成功通知を前記ブロックチェーンに書き込むことであって、前記成功通知は、前記支払い処理が正常に完了したことを示すデータを含む、書き込むことと

を含む、方法。

【請求項２】
前記販売者システムが、顧客デバイスから前記証明及び前記顧客ハッシュを受信したことに応じて、前記ＺＫＰスマート・コントラクトを呼び出し、
前記顧客デバイスが、前記ゼロ知識証明アルゴリズムに関連付けられた証明関数を実行することによって、前記証明を生成し、
前記証明関数が、証明鍵、前記顧客ハッシュ、及び支払いハッシュを前記ゼロ知識証明アルゴリズムに入力することによって、実行される、
請求項１に記載の方法。
【請求項３】
前記顧客デバイスが、前記支払い購入を前記販売者システムで開始したことに応じて、前記証明を生成し、
前記支払いハッシュが、顧客識別データ及び顧客ナンスをハッシュ化アルゴリズムに入力することによって、生成される、
請求項２に記載の方法。
【請求項４】
発行者システムが、前記ゼロ知識証明アルゴリズムを作成し、
前記ゼロ知識証明アルゴリズムが、鍵生成関数、前記証明関数、及び前記検証関数を含み、
前記発行者システムが、前記鍵生成関数を実行することによって、前記証明鍵及び前記検証鍵を生成し、
前記鍵生成関数が、乱数を前記鍵生成関数に入力することによって、実行され、
前記発行者システムが、前記検証関数を含むように前記ＺＫＰスマート・コントラクトを生成する、
請求項３に記載の方法。
【請求項５】
前記発行者システムが、前記販売者システムから販売者登録要求を受信したことに応じて、前記販売者ハッシュを生成し、
前記販売者ハッシュが、販売者識別データ及び販売者ナンスをハッシュ化アルゴリズムに入力することによって、生成される、
請求項４に記載の方法。
【請求項６】
前記ＺＫＰスマート・コントラクトによって、前記販売者ハッシュ及び前記販売者口座残高を前記ブロックチェーンに書き込むことであって、前記ＺＫＰスマート・コントラクトが前記書き込みを完了したことに応じて、前記発行者システムが、前記販売者ハッシュ及び前記販売者ナンスを前記販売者システムに送信する、書き込むことを更に含む、請求項５に記載の方法。
【請求項７】
前記発行者システムが、前記顧客デバイスから顧客登録要求を受信したことに応じて、前記顧客ハッシュを生成し、
前記顧客ハッシュが、前記顧客識別データ及び前記顧客ナンスを前記ハッシュ化アルゴリズムに入力することによって、生成される、
請求項４乃至６のいずれか一項に記載の方法。
【請求項８】
前記ＺＫＰスマート・コントラクトによって、前記顧客ハッシュ及び前記顧客口座残高を前記ブロックチェーンに書き込むことであって、前記ＺＫＰスマート・コントラクトが前記書き込みを完了したことに応じて、前記発行者システムが、前記顧客ハッシュ及び前記顧客ナンスを前記顧客デバイスに送信する、書き込むことを更に含む、請求項７に記載の方法。
【請求項９】
プロセッサと、

前記プロセッサと通信するように構成された有形の非一時的メモリと
を備える、コンピュータ・ベースのシステムであって、前記有形の非一時的メモリには命令が記憶されており、前記命令は、前記プロセッサによって実行されたことに応じて、ゼロ知識証明（ＺＫＰ）スマート・コントラクトに、
支払い処理中、販売者システムによって呼び出されたことに応じて、前記ＺＫＰスマート・コントラクトによって、検証関数を実行することであって、前記販売者システムは、証明、顧客ハッシュ、販売者ハッシュ、及び購入金額を前記ＺＫＰスマート・コントラクトに送信することによって前記ＺＫＰスマート・コントラクトを呼び出すように構成され、前記検証関数は、検証鍵、前記証明、及び前記顧客ハッシュを、前記検証関数に入力することによって実行されるように構成され、前記検証関数は、ゼロ知識証明アルゴリズムに関連付けられる、実行することと、
前記検証関数が成功したことに応じて、前記ＺＫＰスマート・コントラクトによって、前記顧客ハッシュに関連付けられた顧客口座残高を調整することであって、前記顧客口座残高は、前記購入金額に基づいて調整され、前記顧客口座残高は、ブロックチェーン上で維持される、調整することと、
前記ＺＫＰスマート・コントラクトによって、前記販売者ハッシュに関連付けられた販売者口座残高を調整することであって、前記販売者口座残高は、前記購入金額に基づいて調整され、前記販売者口座残高は、ブロックチェーン上で維持される、調整することと、
前記ＺＫＰスマート・コントラクトによって、成功通知を前記ブロックチェーンに書き込むことであって、前記成功通知は、前記支払い処理が正常に完了したことを示すデータを含む、書き込むことと
を含む動作を実行させる、コンピュータ・ベースのシステム。
【請求項１０】
前記販売者システムが、顧客デバイスから前記証明及び前記顧客ハッシュを受信したことに応じて、前記ＺＫＰスマート・コントラクトを呼び出すように構成され、
前記顧客デバイスが、前記ゼロ知識証明アルゴリズムに関連付けられた証明関数を実行することによって、前記証明を生成するように構成され、
前記証明関数が、証明鍵、前記顧客ハッシュ、及び支払いハッシュを前記ゼロ知識証明アルゴリズムに入力することによって、実行されるように構成される、
請求項９に記載のコンピュータ・ベースのシステム。
【請求項１１】
前記顧客デバイスが、前記支払い購入を前記販売者システムで開始したことに応じて、前記証明を生成するように構成され、
前記支払いハッシュが、顧客識別データ及び顧客ナンスをハッシュ化アルゴリズムに入力することによって、生成される、
請求項１０に記載のコンピュータ・ベースのシステム。
【請求項１２】
発行者システムが、前記ゼロ知識証明アルゴリズムを作成するように構成され、
前記ゼロ知識証明アルゴリズムが、鍵生成関数、前記証明関数、及び前記検証関数を含み、
前記発行者システムが、前記鍵生成関数を実行することによって、前記証明鍵及び前記検証鍵を生成するように構成され、
前記鍵生成関数が、乱数を前記鍵生成関数に入力することによって、実行されるように構成され、
前記発行者システムが、前記検証関数を含むように前記ＺＫＰスマート・コントラクトを生成するように構成される、
請求項１１に記載のコンピュータ・ベースのシステム。
【請求項１３】
前記発行者システムが、前記販売者システムから販売者登録要求を受信したことに応じて、前記販売者ハッシュを生成するように構成され、

前記販売者ハッシュが、販売者識別データ及び販売者ナンスをハッシュ化アルゴリズムに入力することによって、生成される、
請求項１２に記載のコンピュータ・ベースのシステム。
【請求項１４】
前記ＺＫＰスマート・コントラクトによって、前記販売者ハッシュ及び前記販売者口座残高を前記ブロックチェーンに書き込むことであって、前記ＺＫＰスマート・コントラクトが前記書き込みを完了したことに応じて、前記発行者システムが、前記販売者ハッシュ及び前記販売者ナンスを前記販売者システムに送信するように構成される、書き込むことを更に含む、請求項１３に記載のコンピュータ・ベースのシステム。
【請求項１５】
前記発行者システムが、前記顧客デバイスから顧客登録要求を受信したことに応じて、前記顧客ハッシュを生成するように構成され、
前記顧客ハッシュが、前記顧客識別データ及び前記顧客ナンスを前記ハッシュ化アルゴリズムに入力することによって、生成される、
請求項１２乃至１４のいずれか一項に記載のコンピュータ・ベースのシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、２０１８年１２月１２日に提出された「ＺＥＲＯ－ＫＮＯＷＬＥＤＧＥ　ＰＲＯＯＦ　ＰＡＹＭＥＮＴＳ　ＵＳＩＮＧ　ＢＬＯＣＫＣＨＡＩＮ」と題される米国特許出願第１６／２１７，７３４号の優先権及びその利益を主張するものである。
【０００２】
本開示は、一般的に支払いシステムに関し、より詳細には分散台帳を使用するゼロ知識証明支払い及び処理に関する。
【背景技術】
【０００３】
消費者は、様々な方法を用いて販売者との取引を開始するよう望む可能性がある。例えば、消費者は、実店舗型の小売店を訪れることにより対面で、販売者のウェブサイトを通じてオンラインで、又は任意の他の適切な手段を介して、販売者と取引を開始することができる。取引を完了するために、消費者は、取引口座番号、消費者の氏名、消費者の連絡先情報などを含み得る重要な情報をサブミットする場合がある。販売者は、取引口座番号、有効期限、セキュリティ・コード（ＣＶＶ：ｃａｒｄ　ｖｅｒｉｆｉｃａｔｉｏｎ　ｖａｌｕｅ）などを、発行者システム又は支払いプロセッサに送信することにより、取引の認可を要求する場合がある。発行者システム又は支払いプロセッサは、取引口座データを検証し、消費者が支払いを完了するために十分な資金を有していることを確認し、認可の承認又は却下を送信し戻すことができる。技術的問題は、通常の取引処理では、取引口座データ及び消費者データを含む重要なデータが、セキュアではない可能性がある複数のチャネルに渡って明らかになることである。通常の取引処理において重要なデータが明らかになることにより、重要なデータがサード・パーティによって傍受される、又は盗まれる可能性がある。
【発明の概要】
【課題を解決するための手段】
【０００４】
ブロックチェーンを使用するゼロ知識証明支払いのための、システム、方法、及びコンピュータ可読媒体（総称して「システム」）が開示される。システムは、支払い処理中、販売者システムによって呼び出されたことに応じて、検証関数を実行することであって、販売者システムは、証明、顧客ハッシュ、販売者ハッシュ、及び購入金額をＺＫＰスマート・コントラクトに送信することによってＺＫＰスマート・コントラクトを呼び出し、検証関数は、検証鍵、証明、及び顧客ハッシュを、検証関数に入力することによって実行さ

れ、検証関数は、ゼロ知識証明アルゴリズムに関連付けられる、実行することと、検証関数が成功したことに応じて、顧客ハッシュに関連付けられた顧客口座残高を調整することであって、顧客口座残高は、購入金額に基づいて調整され、顧客口座残高は、ブロックチェーン上で維持される、調整することと、販売者ハッシュに関連付けられた販売者口座残高を調整することであって、販売者口座残高は、購入金額に基づいて調整され、販売者口座残高は、ブロックチェーン上で維持される、調整することと、成功通知をブロックチェーンに書き込むことであって、成功通知は、支払い処理が正常に完了したことを示すデータを含む、書き込むこととを行うように構成された、ゼロ知識証明（ＺＫＰ）スマート・コントラクトを含むことができる。

【０００５】

様々な実施形態において、販売者システムは、顧客デバイスから証明及び顧客ハッシュを受信したことに応じて、ＺＫＰスマート・コントラクトを呼び出すことができる。顧客デバイスは、ゼロ知識証明アルゴリズムに関連付けられた証明関数を実行することによって、証明を生成することができる。証明関数は、証明鍵、顧客ハッシュ、及び支払いハッシュを証明アルゴリズムに入力することによって、実行され得る。顧客デバイスは、支払い購入を販売者システムで開始したことに応じて、証明を生成することができる。支払いハッシュは、顧客識別データ及び顧客ナンスをハッシュ化アルゴリズムに入力することによって、生成され得る。

【０００６】

様々な実施形態において、発行者システムは、ゼロ知識証明アルゴリズムを作成することができる。ゼロ知識証明アルゴリズムは、鍵生成関数、証明関数、及び検証関数を含むことができる。発行者システムは、鍵生成関数を実行することによって、証明鍵及び検証鍵を生成することができる。鍵生成関数は、乱数を鍵生成関数に入力することによって、実行され得る。発行者システムは、検証関数を含むようにＺＫＰスマート・コントラクトを生成することができる。

【０００７】

様々な実施形態において、発行者システムは、販売者システムから販売者登録要求を受信したことに応じて、販売者ハッシュを生成することができる。販売者ハッシュは、販売者識別データ及び販売者ナンスをハッシュ化アルゴリズムに入力することによって、生成され得る。ＺＫＰスマート・コントラクトは、販売者ハッシュ及び販売者口座残高をブロックチェーンに書き込むことができる。ＺＫＰスマート・コントラクトが書き込みを完了したことに応じて、発行者システムは、販売者ハッシュ及び販売者ナンスを販売者システムに送信することができる。様々な実施形態において、発行者システムは、顧客デバイスから顧客登録要求を受信したことに応じて、顧客ハッシュを生成することができる。顧客ハッシュは、顧客識別データ及び顧客ナンスをハッシュ化アルゴリズムに入力することによって、生成され得る。ＺＫＰスマート・コントラクトは、顧客ハッシュ及び顧客口座残高をブロックチェーンに書き込むことができる。ＺＫＰスマート・コントラクトが書き込みを完了したことに応じて、発行者システムは、顧客ハッシュ及び顧客ナンスを顧客デバイスに送信することができる。

【０００８】

先の特徴及び要素は、本明細書においてそうではないと明確に示されない限り、排他的ではなく、様々な組み合わせとして組み合わせることができる。これらの特徴及び要素、並びに開示される実施形態の動作は、以下の説明及び添付の図面を考慮するとより明らかとなろう。

【０００９】

本開示の主題は、明細書の結論部分において、特に示され、明確に特許請求される。しかしながら、本開示の更に完全な理解は、詳細な説明及び特許請求の範囲を参照して図面と併せて考慮することにより得ることができ、図面では同一の数字は同一の要素を表す。

【図面の簡単な説明】

【００１０】

【図１】様々な実施形態による、ゼロ知識証明支払いシステムを図示する例示的なブロック図である。
【図２】様々な実施形態による、ゼロ知識証明アルゴリズムを初期化するための例示的な処理の流れである。
【図３】様々な実施形態による、ゼロ知識証明支払い用の販売者登録のための例示的な処理の流れである。
【図４】様々な実施形態による、ゼロ知識証明支払い用の顧客登録のための例示的な処理の流れである。
【図５】様々な実施形態による、ゼロ知識証明支払い処理のための例示的な処理の流れである。
【発明を実施するための形態】
【００１１】
本明細書における様々な実施形態の詳細な説明は、図示により様々な実施形態を示す添付の図面及び画像を参照する。これらの様々な実施形態は、当業者が本開示を実践できるよう十分詳細に説明されるが、本開示の思想及び範囲から逸脱することなく、他の実施形態が実現される場合があること、及び論理的且つ機械的な変更が成され得ることを理解されたい。したがって、本明細書における詳細な説明は、単なる例示の目的のために提示され、限定のためではない。例えば、方法又は処理の説明のいずれかにおいて述べられるステップは、あらゆる順序で実行されてもよく、提示される順序に限定されない。その上、機能又はステップのいずれも、一つ若しくは複数のサード・パーティにアウトソースされること、又は一つ若しくは複数のサード・パーティによって実施される場合がある。本開示の範囲から逸脱することなく、本明細書に説明されるシステム、装置、及び方法に対して、修正、追加、又は省略が成される場合がある。例えば、システム及び装置のコンポーネントは一体化されてもよく、又は別個にされてもよい。その上、本明細書で開示されるシステム及び装置の動作は、より多くの、より少ない、又は他のコンポーネントによって実施される場合があり、説明される方法は、より多くの、より少ない、又は他のステップを含む場合がある。追加的に、ステップは、あらゆる適切な順序で実施される可能性がある。本明細書において使用される際、「それぞれ」は、ある集合の各メンバ、又はある集合の部分集合の各メンバを指す。更には、単数形へのあらゆる言及は複数形の実施形態を含み、二つ以上のコンポーネントへのあらゆる言及は単数形の実施形態を含むことができる。本明細書において具体的な利点が列挙されるが、様々な実施形態は列挙される利点のうち、いくつかを含む、いずれも含まない、又はすべてを含む場合がある。
【００１２】
ゼロ知識証明支払いシステム及び処理は、顧客が取引口座データを含む重要なデータを明らかにする必要なく、顧客と販売者との間の取引を完了するために使用することができる。システムは、例えばｚｋ－ＳＮＡＲＫなどのゼロ知識証明アルゴリズムを実装することができる。このアルゴリズムは、当事者間で実際の情報を開示又は交換することを必要とせずに、顧客が特定の情報（例えば、取引口座データ）を知っている又は所有していることを証明すること、及び販売者がその情報を知っている又は所有していることを検証することを可能にする。発行者システムは、ゼロ知識証明アルゴリズムを確立することができ、販売者及び顧客が、ゼロ知識証明支払いに参加できるよう、発行者システムに登録できるようにすることができる。顧客口座残高、販売者口座残高、及び取引データは、ブロックチェーン上に維持されている場合がある。スマート・コントラクトは、ゼロ知識証明支払い処理の間、エンドツーエンドのデータ・フローを制御し、認可及び／又は取引が成功したことに応じて顧客口座残高及び販売者口座残高を更新するために使用することができる。
【００１３】
このシステムは、コンピュータの機能性を更に改善する。例えば、本明細書において説明されるプロセスを使用してデータを送信、記憶、アクセスすることにより、データのセキュリティが向上し、コンピュータ、ネットワーク、及び／又は重要なデータが危険にさ

らされるリスクを低下させる。例えば、本明細書において提供されるゼロ知識証明方法を用いて、顧客の個人情報は発行者システムだけに記憶される。個人情報が販売者と共有されないため、取引口座番号を含む機密情報及び資格情報が、支払い処理の間、明らかにされない。その上、販売者が個人情報を受信しないため、販売者はペイメント・カード業界データ・セキュリティ基準（ＰＣＩ　ＤＳＳ：Ｐａｙｍｅｎｔ　Ｃａｒｄ　Ｉｎｄｕｓｔｒｙ　Ｄａｔａ　Ｓｅｃｕｒｉｔｙ　Ｓｔａｎｄａｒｄ）コンプライアンスを証明する必要がない場合がある。

【００１４】

本明細書において説明されるシステム、方法、及びコンピュータ可読媒体（総称して「システム」）は、様々な実施形態によると、ピアツーピア・ネットワーク上で、複数のコンピューティング・デバイス（例えば、ノード）によって維持される分散台帳を使用する場合がある。各コンピューティング・デバイスは、分散台帳の複製及び／又は部分複製を保持し、ネットワーク内の一つ又は複数の他のコンピューティング・デバイスに通信して、データを検証して分散台帳に書き込む。分散台帳は、例えば合意ベースの検証、不変性、及び暗号法的なつながりを持つデータのブロックを含む、ブロックチェーン技術の特徴と機能性を使用することができる。ブロックチェーンは、データを含む相互接続されたブロックである台帳を含むことができる。各ブロックが個々の取引及びあらゆるブロックチェーン実行可能物の結果を保持するため、ブロックチェーンは、高度なセキュリティを提供することができる。各ブロックは、先行するブロックにリンクすることができ、タイムスタンプを含むことができる。各ブロックがブロックチェーン内の先行するブロックのハッシュを含むことができるため、ブロック同士をリンクすることができる。リンクしたブロックはチェーンを形成し、単一のチェーンに対して、一つの後続ブロックだけが他の一つの先行ブロックにリンクすることができる。フォークは、先行する一様なブロックチェーンから分岐チェーンが確立される際に可能な場合があるが、典型的には分岐チェーンのうちの一つだけが合意チェーンとして維持される。様々な実施形態において、ブロックチェーンは、非中央集権的な様式でデータのワークフローを執行するスマート・コントラクトを実装することができる。システムは、例えばコンピュータ、タブレット、スマートフォン、モノのインターネットのデバイス（「ＩｏＴ」デバイス）などのユーザ・デバイスに展開されるアプリケーションを含むこともできる。アプリケーションは、ブロックチェーンと通信して（例えば、直接的に、又はブロックチェーン・ノードを介して）、データを送信及び検索することができる。様々な実施形態において、組織又はコンソーシアムを統制することは、ブロックチェーン上に記憶されたデータへのアクセスを制御することであり得る。管理組織に登録することにより、ブロックチェーン・ネットワークに参加できる場合がある。

【００１５】

システムを通じて実施されるデータ転送は、実装される具体的なブロックチェーン技術のブロックチェーン作成時間によって決定され得る持続時間中、ブロックチェーン内の接続ピアに伝搬する。例えば、ＥＴＨＥＲＥＵＭ（登録商標）ベースのネットワークでは、新しいデータ・エントリは書き込み時点で約１３から２０秒のうちに利用可能になる可能性がある。ＨＹＰＥＲＬＥＤＧＥＲ（登録商標）Ｆａｂｒｉｃ１．０ベースのプラットフォームでは、持続時間は選択される具体的な合意アルゴリズムによって決まり、数秒のうちに実施され得る。この点で、システム内において、伝搬時間、及びデータを転送し、購入を開始して購入を完了する速度は、既存のシステムに比べて改善される可能性があり、市場投入までの実装コスト及び時間も劇的に短縮され得る。システムは、ブロックチェーンに記憶されるデータの不変的な性質により、様々なデータの入力及び出力の改竄の可能性を低減し、少なくとも部分的に向上したセキュリティを更に提供する。その上、データをブロックチェーンに記憶することに先立って、暗号法的処理をデータに対して実施することにより、システムは購入時要求及び購入の向上したセキュリティを更に提供することができる。したがって、本明細書において説明されるシステムを使用してデータを送信、記憶、アクセスすることにより、データのセキュリティが向上し、コンピュータ又はネッ

トワークが危険にさらされるリスクを低下させる。

【００１６】

様々な実施形態において、システムは、共通のデータ構造を設けることにより、データベースの同期エラーを低減することもできるため、記憶されたデータの整合性を少なくとも部分的に改善する。更には、関与する当事者とリアルタイムで（又は、ほぼリアルタイムで）データを同期させることにより、システムは、データの完全性、データの信頼性、及びデータのセキュリティを改善することができ、これにより業務プロセスの速度を向上させることもできる。システムにより、各ノードが記憶されたデータの完全な複製を用いて動作することができるため、従来型のデータベース（例えば、リレーショナル・データベース、分散型のデータベースなど）よりも信頼性及び耐障害性が更に向上し、それによって局所的なネットワーク停止及びハードウェア障害によるダウンタイムを少なくとも部分的に削減する。システムにより、各ノードがすべての接続ピアにメッセージをブロードキャストするため、信頼できるピアと信頼できないピアを有するネットワーク環境におけるデータ転送の信頼性が更に向上し、また各ブロックが先行ブロックへのリンクを含むため、ノードは欠落ブロックを迅速に検出し、欠落ブロックの要求をブロックチェーン内の他のノードに伝搬することができる。

【００１７】

図１を参照すると、様々な実施形態による、ゼロ知識証明支払いシステム１００が描かれている。システム１００は、互いに通信する、様々なコンピューティング・デバイス、ソフトウェア・モジュール、ネットワーク、及びデータ構造を含む可能性がある。システム１００は、ウェブ・サービス、ユーティリティ・コンピューティング、汎用及び個別化されたコンピューティング、セキュリティ及び識別ソリューション、自律的コンピューティング、クラウド・コンピューティング、コモディティ・コンピューティング、移動性及びワイヤレス・ソリューション、オープン・ソース、バイオメトリクス、グリッド・コンピューティング、並びに／又はメッシュ・コンピューティングと連携した使用も企図している。本明細書において説明されるブロックチェーンに基づくシステム１００は、分散型の耐改竄性データ記憶としてブロックチェーンを使用することにより、支払い処理及び関連する処理を簡略化及び自動化することができる。特定の金融機関の代わりに、例えば自律分散型組織（ＤＡＯ）によって記憶されるデータを使用して検証が行われるため、連合型又はパブリック型のブロックチェーンを使用する様々な実施形態については、透明性が非常に高い。

【００１８】

様々な実施形態において、システム１００は、顧客デバイス１１０、販売者システム１２０、発行者システム１３０、及び／又はブロックチェーン・ネットワーク１４０のうちの、一つ又は複数を含む場合がある。ブロックチェーン・ネットワーク１４０は、本明細書において更に議論されるように、一つ又は複数のブロックチェーン・ノード、ＡＰＩなどを介して、発行者システム１３０と電子的に通信することができる。ブロックチェーン・ネットワーク１４０は、本明細書において更に議論されるように、販売者システム１２０がスマート・コントラクト（例えば、ゼロ知識証明スマート・コントラクト１４５）を呼び出すことに応じて、販売者システム１２０によりアクセス可能である場合がある。ブロックチェーン・ネットワーク１４０は、性質として、プライベート型、コンソーシアム型、及び／又はパブリック型のブロックチェーン・ネットワーク又はピアツーピアのネットワークであり得る（例えば、ＥＴＨＥＲＥＵＭ（登録商標）、Ｂｉｔｃｏｉｎ、ＨＹＰＥＲＬＥＤＧＥＲ（登録商標）Ｆａｂｒｉｃなど）。コンソーシアム型及びプライベート型のネットワークは、ブロックチェーンの内容に対して制御の改善を提供することができ、パブリック型のネットワークは、セキュリティを改善するために蓄積されたネットワークの計算能力を活用することができる。ブロックチェーン・ネットワーク１４０は、本明細書において更に議論されるように、互いに電子的に通信する様々なブロックチェーン・ノードを含むことができる。

【００１９】

ブロックチェーン・ネットワーク１４０は、ブロックチェーン及びブロックチェーンへの書き込みに対する合意を維持するよう構成された複数のブロックチェーン・ノードを含むことができる。ブロックチェーンは、レコードを可読の状態で維持し、改竄に耐性がある、分散型台帳であり得る。ブロックチェーンは、例えば、ＥＴＨＥＲＥＵＭ（登録商標）、Ｏｐｅｎ Ｃｈａｉｎ、Ｃｈａｉｎ Ｏｐｅｎ Ｓｔａｎｄａｒｄ、ＨＹＰＥＲＬＥＤＧＥＲ（登録商標）Ｆａｂｒｉｃ、ＣＯＲＤＡ ＣＯＮＮＥＣＴ（登録商標）、ＩＮＴＥＬ（登録商標）Ｓａｗｔｏｏｔｈなどのブロックチェーン技術に基づくことができる。ブロックチェーンは、データを含む相互接続されたブロックである台帳を含むことができる。各ブロックは、先行するブロックにリンクすることができ、タイムスタンプを含むことができる。システム１００のサポートとして実装される場合、ブロックチェーンは、システム１００におけるゼロ知識証明支払いの不変なログとして機能することができる。ブロックチェーンは、本明細書において更に議論されるように、ブロックチェーンの複製、又は部分的な複製の形態で、様々なブロックチェーン・ノード上で維持することができる。ブロックチェーン・ノード同士で合意を確立することにより、ブロックを、ブロックチェーンへ書き込むことができる。例えば、合意は、プルーフ・オブ・ワーク、プルーフ・オブ・ステーク、実際のビザンチン・フォールト・トレランス、委任型（ｄｅｌｅｇａｔｅｄ）プルーフ・オブ・ステーク、又は他の適切な合意アルゴリズムに基づいて確立することができる。

【００２０】

様々な実施形態において、ブロックチェーン・ネットワーク１０１は、一つ又は複数のスマート・コントラクトをホスト及び／又は実装することができる。スマート・コントラクトは、システム１００においてエンドツーエンドのデータ・フローを制御し、様々な取引データの実行及び記録をサポートすることにより、支払い処理を自律的に統制することができる。例えば、様々な実施形態によると、ブロックチェーン・ネットワーク１４０は、一つ又は複数のゼロ知識証明支払い（ＺＫＰ）スマート・コントラクト１４５をホストすることができる。ＺＫＰスマート・コントラクト１４５は、以下で更に議論されるように、ＡＰＩコールなどによって渡される所定の関数パラメータに基づいて、データを所定のフォーマットでブロックチェーンに書き込む実行可能物を含むことができる。ＺＫＰスマート・コントラクト１４５は、例えばＳｏｌｉｄｉｔｙ又はあらゆる他の適切なスマート・コントラクト用プログラミング言語などのプログラミング言語で記述されたプログラムを含む場合がある。

【００２１】

ＺＫＰスマート・コントラクト１４５は、以下で更に議論されるように、様々なゼロ知識支払い関数及び機能を提供するように構成されたスマート・コントラクトを含む場合がある。例えば、様々な実施形態によると、以下で更に議論されるように、ＺＫＰスマート・コントラクト１４５は、ゼロ知識証明購入ワークフローを制御すること、ブロックチェーンにデータを書き込むこと、一つ又は複数の実体に通知を送信することなどを行うように構成することができる。例えば、以下で更に議論されるように、ＺＫＰスマート・コントラクト１４５は、取引中、販売者システム１２０からデータを受信すること、販売者と取引している顧客の識別情報を検証するために検証関数を実行すること、ブロックチェーン上に維持される顧客口座残高及び販売者口座残高を取引に基づいて調整すること、並びに以下で更に議論されるように口座残高を正常に調整したことに応じて成功通知を書き込み及び送信すること、を行うように構成することができる。

【００２２】

様々な実施形態において、顧客１１５は、販売者１２５から一つ又は複数の商品又はサービスを購入したいと思う場合がある。例えば、顧客１１５は、販売者１２５に関連付けられる実店舗型の小売店に出かけて商品及びサービスを購入する可能性がある。顧客１１５は、顧客デバイス１１０を使用して販売者１２５との購入を完了することができる。顧客デバイス１１０は、本明細書において更に議論されるように、販売者システム１２０と対話して購入についてのデータを送信することができる。更なる例として、顧客１１５は

、販売者１２５からの商品又はサービスを、ウェブ・ブラウザ、モバイル・アプリケーションなどを介してオンラインで購入する場合がある。その点において、顧客１１５は、顧客デバイス１１０と対話して購入を完了することができる。顧客デバイス１１０は、本明細書において更に議論されるように、販売者システム１２０と電子的に通信して商品又はサービスのデータを検索し、購入を完了することができる。

【００２３】

様々な実施形態において、顧客デバイス１１０は、販売者システム１２０及び／又は発行者システム１３０と電子的に通信している場合がある。顧客デバイス１１０は、データを送信、受信、及び／又は記憶することが可能な、あらゆる適切なハードウェア、ソフトウェア、及び／又はデータベース若しくはメモリ・コンポーネントを含む場合がある。顧客デバイス１１０は、例えばコンピュータ若しくはプロセッサ、又はコンピュータ及び／若しくはプロセッサのセットなどの、一つ又は複数のコンピューティング・デバイスを含む場合があるが、他のタイプのコンピューティング・ユニット又はシステムも使用することができる。例えば、顧客デバイス１１０は、ロジックを実装することができる、プロセッサ、及び一つ又は複数の有形の非一時的メモリを含むことができる。プロセッサは、命令、例えば本明細書において更に議論されるような非一時的な有形のコンピュータ可読媒体に記憶された命令の実行に応答して、様々な論理演算を実装するように構成することができる。顧客デバイス１１０は、ラップトップ、タブレット、ハンドヘルド・コンピュータ、携帯情報端末、携帯電話、スマートフォン（例えば、ＩＰＨＯＮＥ（登録商標）、ＢＬＡＣＫＢＥＲＲＹ（登録商標）など）、ＩｏＴデバイスなどを含むことができる。顧客デバイス１１０は、例えば、ＷＩＮＤＯＷＳ（登録商標）モバイル・オペレーティング・システム、ＡＮＤＲＯＩＤ（登録商標）オペレーティング・システム、ＡＰＰＬＥ（登録商標）ＩＯＳ（登録商標）、ＢＬＡＣＫＢＥＲＲＹ（登録商標）オペレーティング・システム、ＬＩＮＵＸ（登録商標）オペレーティング・システムなどのオペレーティング・システムを含むことができる。顧客デバイス１１０は、顧客デバイス１１０にインストールされ、顧客デバイス１１０が、販売者システム１２０及び／又は発行者システム１３０に、アクセスすること及び／又はそれと対話することを、可能にするように構成されたソフトウェア・コンポーネントを含むこともできる。例えば、顧客デバイス１１０は、ウェブ・ブラウザ（例えば、ＭＩＣＲＯＳＯＦＴ　ＩＮＴＥＲＮＥＴ　ＥＸＰＬＯＲＥＲ（登録商標）、ＧＯＯＧＬＥ　ＣＨＲＯＭＥ（登録商標）など）、アプリケーション、マイクロアプリ、又はモバイル・アプリケーションなどを含むことができ、顧客デバイス１１０が、販売者システム１２０及び／又は発行者システム１３０に、アクセスして対話することを可能にするように構成することができる。

【００２４】

様々な実施形態において、販売者システム１２０は、顧客デバイス１１０及び／又は発行者システム１３０と電子的に通信している場合がある。様々な実施形態において、本明細書において更に議論されるように、販売者システム１２０は、ブロックチェーン・ネットワーク１４０を介してＺＫＰスマート・コントラクト１４５を呼び出し、ゼロ知識証明購入を完了するように構成することもできる。販売者システム１２０は、一つ又は複数の販売者１２５の実店舗型の小売店、オンライン・ストアなどに関連付けられる場合がある。販売者システム１２０は、ハードウェア、ソフトウェア、及び／又はデータベース・コンポーネントのあらゆる適切な組み合わせを含むことができる。例えば、販売者システム１２０は、一つ又は複数のネットワーク環境、サーバ、コンピュータ・ベースのシステム、プロセッサ、データベース、データ・センタなどを含む場合がある。販売者システム１２０は、グラフィカル・ユーザ・インターフェース（「ＧＵＩ」）、ソフトウェア・モジュール、ロジック・エンジン、様々なデータベースなどを含むことができ、顧客１１５が、顧客デバイス１１０を介して、販売者システム１２０にアクセスできるように構成される。様々な実施形態において、販売者システム１２０は、コンピュータ・ベースであってもよく、プロセッサ、有形の非一時的コンピュータ可読メモリ、及び／又はネットワーク・インターフェースを、他の適切なシステム・ソフトウェア及びハードウェア・コンポー

ネントと共に含むことができる。有形の非一時的メモリに記憶された命令により、販売者システム１２０は、本明細書に説明されるような様々な動作を実施することができる。

【００２５】

様々な実施形態において、販売者システム１２０は、取引を行うためのメカニズムとして構成された販売時点情報管理端末を含む場合もある。例えば、販売時点情報管理は、レジ、クレジット及び／又はデビット・カードのリーダ、ＥＭＶカード・リーダなどを含む場合がある。販売時点情報管理は、近接場通信（ＮＦＣ）端末、又はデータの無線送信を可能にする（例えば、ＢＬＵＥＴＯＯＴＨ（登録商標）、Ｗｉ－Ｆｉなど）あらゆる他の適切な端末を含む場合がある。ＮＦＣ端末は、例えば顧客デバイス１１０などの、ＮＦＣ対応ユーザ・デバイスから情報の転送を可能にすることができる。

【００２６】

様々な実施形態において、販売者システム１３０は、顧客デバイス１１０、販売者システム１２０、及び／又はブロックチェーン・ネットワーク１４０と電子的に通信している場合がある。発行者システム１３０は、ハードウェア、ソフトウェア、及び／又はデータベース・コンポーネントのあらゆる適切な組み合わせを含むことができる。例えば、発行者システム１３０は、一つ又は複数のネットワーク環境、サーバ、コンピュータ・ベースのシステム、プロセッサ、データベースなどを含む場合がある。発行者システム１３０は、コンピュータ若しくはプロセッサの形態の少なくとも一つのコンピューティング・デバイス、又はコンピュータ／プロセッサのセットを含むことができるが、例えば、サーバ、ウェブ・サーバ、プール・サーバなどの、他のタイプのコンピューティング・ユニット又はシステムを使用することもできる。発行者システム１３０は、一つ又は複数のデータ・センタ、クラウド・ストレージなどを含む場合もあり、本明細書において議論される様々な動作を実施するように構成されたＡＰＩなどのソフトウェアを含んでもよい。発行者システム１３０は、一つ又は複数のブロックチェーン・ノード、アプリケーション・プログラミング・インターフェース（ＡＰＩ）、ソフトウェア開発キット（ＳＤＫ）なども含むことができ、発行者システム１３０が、ブロックチェーン・ネットワーク１４０と対話し、データを検索してブロックチェーンに書き込み、一つ又は複数のＺＫＰスマート・コントラクト１４５を展開することができるように構成される。様々な実施形態において、発行者システム１３０は、一つ若しくは複数のプロセッサ、及び／又は一つ若しくは複数の有形の非一時的メモリを含むことができ、ロジックを実装することが可能である。プロセッサは、命令、例えば本明細書において更に議論されるような非一時的な有形のコンピュータ可読媒体に記憶された命令の実行に応答して、様々な論理演算を実装するように構成することができる。

【００２７】

様々な実施形態において、発行者システム１３０は、購入及び支払いを容易にする、取引を認可する、並びに取引を決済するなどのために、従来型の支払いネットワーク又は取引ネットワークを含むか、又はそれと対話する。例えば、発行者システム１３０は、クレジット・カード、デビット・カード、及び／又は他のタイプの取引口座若しくは取引機器向けの取引に現在対応している既存のプロプライエタリなネットワークを表すことがある。発行者システム１３０は、盗聴者から安全な閉じられたネットワークである場合がある。様々な実施形態において、発行者システム１３０には、ＡＭＥＲＩＣＡＮ　ＥＸＰＲＥＳＳ（登録商標）、ＶＩＳＡＮＥＴ（登録商標）、ＭＡＳＴＥＲＣＡＲＤ（登録商標）、ＤＩＳＣＯＶＥＲ（登録商標）、ＩＮＴＥＲＡＣ（登録商標）、Ｃａｒｔｅｓ　Ｂａｎｃａｉｒｅｓ、ＪＣＢ（登録商標）などの例示的な取引ネットワーク、プライベート・ネットワーク（例えば、百貨店内ネットワーク）、及び／又はあらゆる他の支払いネットワーク、取引ネットワーク、発行者システムなどが含まれる場合がある。発行者システム１３０は、金融並びに／又は取引用のシステム及び処理に関連する、例えば一つ又は複数の認可エンジン、認証エンジン及びデータベース、決済エンジン及びデータベース、売掛金システム及びデータベース、買掛金システム及びデータベースなどの、システム及びデータベースを含むことができる。様々な実施形態において、発行者システム１３０は、本明細

書において更に議論されるように、取引を認可することができる取引口座発行者のクレジット認可システム（ＣＡＳ：Ｃｒｅｄｉｔ Ａｕｔｈｏｒｉｚａｔｉｏｎ Ｓｙｓｔｅｍ）を含む場合もある。発行者システム１３０は、取引を認可して決済すること、及び取引口座メンバ・データベース、売掛金データベース、買掛金データベースなどを維持すること、を行うように構成することができる。

【００２８】

本開示は発行者システム１３０を参照するが、本開示の原理は、あらゆる適切な数の発行者システムを有するゼロ知識証明支払いシステムに適用可能であることを理解されたい。例えば、システム１００は、それぞれが異なる発行者システム若しくはネットワークに対応するか、又はそれに関連付けられる、一つ又は複数の発行者システム１３０を含むことができる。様々な実施形態において、各発行者システムは、関連付けられたブロックチェーン・ネットワークを含むことができるか、又はそれと対話することもできる。

【００２９】

本明細書において使用される際、「送信する」には、電子データの少なくとも一部を一つのシステム１００コンポーネントから別のものに送信することが含まれる場合がある。加えて、本明細書において使用される際、「データ」、「情報」などには、デジタル又は任意の他の形態のコマンド、クエリ、ファイル、メッセージ、記憶用のデータなどの情報を包含することが含まれる場合がある。

【００３０】

本明細書において使用される際、「電子的通信」には、システム１００コンポーネントがデータを送受信することを可能にする、物理的な結合及び／又は非物理的な結合が含まれる場合がある。例えば、「電子的通信」は、ＣＡＮバス・プロトコル、イーサネット物理層プロトコル（例えば、１０ＢＡＳＥ－Ｔ、１００ＢＡＳＥ－Ｔ、１０００ＢＡＳＥ－Ｔなどを使用するもの）、ＩＥＥＥ１３９４インターフェース（例えば、ＦｉｒｅＷｉｒｅ）、サービス総合デジタル網（ＩＳＤＮ）、デジタル加入者線（ＤＳＬ）、８０２．１１ａ／ｂ／ｇ／ｎ／ａｃ信号（例えば、Ｗｉ－Ｆｉ）、短波長ＵＨＦ電波を用いてＩＥＥＥ８０２．１５．１（例えば、Ｂｌｕｅｔｏｏｔｈ Ｓｐｅｃｉａｌ Ｉｎｔｅｒｅｓｔ Ｇｒｏｕｐによって維持されるＢＬＵＥＴＯＯＴＨ（登録商標）プロトコル）により少なくとも部分的に定義された無線通信プロトコル、ＩＥＥＥ８０２．１５．４（例えば、ＺｉｇＢｅｅ ａｌｌｉａｎｃｅによって維持されるＺＩＧＢＥＥ（登録商標）プロトコル）により少なくとも部分的に定義された無線通信プロトコル、セルラ・プロトコル、赤外プロトコル、光学プロトコル、又は有線若しくは無線接続を介して情報を送信することができるあらゆる他のプロトコルなどの、有線又は無線プロトコルを指す場合がある。

【００３１】

システム１００コンポーネントのうちの一つ又は複数は、ネットワークを介して電子的に通信することができる。本明細書で使用される際、用語「ネットワーク」は、あらゆるクラウド、クラウド・コンピューティング・システム、又はハードウェア及び／若しくはソフトウェア・コンポーネントを組み込む電子的通信システム若しくは方法を更に含む場合がある。ノード間の通信は、例えば電話網、エクストラネット、イントラネット、インターネット、加盟店端末装置（携帯情報端末、携帯電話、キオスク、タブレットなど）、オンライン通信、衛星通信、オフライン通信、無線通信、トランスポンダ通信、ローカル・エリア・ネットワーク（ＬＡＮ）、ワイド・エリア・ネットワーク（ＷＡＮ）、仮想プライベート・ネットワーク（ＶＰＮ）、ネットワーク化若しくはリンク化デバイス、キーボード、マウス、及び／又はあらゆる適切な通信若しくはデータ入力様式などのあらゆる適切な通信チャネルを通じて実現することができる。その上、本明細書においてシステムはＴＣＰ／ＩＰ通信プロトコルで実装されるように説明されることが多いが、システムはインターネットワーク・パケット交換（ＩＰＸ）、ＡＰＰＬＥＴＡＬＫ（登録商標）プログラム、ＩＰ－６、ＮｅｔＢＩＯＳ、ＯＳＩ、あらゆるトンネリング・プロトコル（例えば、ＩＰｓｅｃ、ＳＳＨなど）、又はあらゆる数の既存の若しくは将来的なプロトコルを使用して実装することもできる。ネットワークが性質として、インターネットなどのパブ

リックなネットワークである場合、ネットワークはセキュアではなく盗聴者に対してオープンであると想定することが有利な場合がある。インターネットに関連して利用されるプロトコル、規格、及びアプリケーション・ソフトウェアに関する具体的な情報は、一般的に当業者に既知であるため、本明細書において詳しく述べる必要はない。

【００３２】

「クラウド」又は「クラウド・コンピューティング」は、構成可能なコンピューティング・リソース（例えば、ネットワーク、サーバ、ストレージ、アプリケーション、及びサービス）の共有プールへの便利でオンデマンドのネットワーク・アクセスを可能にするためのモデルを含み、最小限の管理努力又はサービス・プロバイダとの対話で、迅速にプロビジョニングされリリースされる。クラウド・コンピューティングは、共有サーバが、リソース、ソフトウェア、データをオンデマンドでコンピュータ及び他のデバイスに提供する、場所独立的なコンピューティングを含むことができる。クラウド・コンピューティングに関する更なる情報は、ＮＩＳＴ（Ｎａｔｉｏｎａｌ Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｓｔａｎｄａｒｄｓ ａｎｄ Ｔｅｃｈｎｏｌｏｇｙ）のクラウド・コンピューティングの定義を参照されたい。

【００３３】

様々なシステム・コンポーネントは独立的に、別個に、集合的に、データ・リンクを介して、ネットワークに適切に結合され得、データ・リンクには例えば通常、標準モデム通信、ケーブル・モデム、ＤＩＳＨ ＮＥＴＷＯＲＫＳ（登録商標）、ＩＳＤＮ、ＤＳＬ、又は様々な無線通信方法に関して用いられるようなローカル・ループ上のインターネット・サービス・プロバイダ（ＩＳＰ）への接続が含まれる。ネットワークは、対話型テレビジョン（ＩＴＶ）ネットワークなど他のタイプのネットワークとして実装される場合もあることに留意されたい。その上、システムは、本明細書において説明される類似の機能性を有するあらゆるネットワーク上での、あらゆる商品、サービス、又は情報の、使用、販売、又は配信を企図している。

【００３４】

ネットワークは、セキュアではない場合がある。したがって、ネットワーク上の通信はデータ暗号化を利用することがある。暗号化は、現在当分野で利用可能な、又は利用可能になる可能性がある技法のうちのいずれかを用いて実施することができる。例えば、Ｔｗｏｆｉｓｈ、ＲＳＡ、エルガマル、ショア署名、ＤＳＡ、ＰＧＰ、ＰＫＩ、ＧＰＧ（ＧｎｕＰＧ）、ＨＰＥフォーマット保持暗号化（ＦＰＥ）、Ｖｏｌｔａｇｅ、Ｔｒｉｐｌｅ ＤＥＳ、Ｂｌｏｗｆｉｓｈ、ＡＥＳ、ＭＤ５、ＨＭＡＣ、ＩＤＥＡ、ＲＣ６、並びに対称及び非対称暗号化システムなどである。ネットワーク通信は、ＳＨＡ系暗号化法、楕円曲線暗号化法（例えば、ＥＣＣ、ＥＣＤＨ、ＥＣＤＳＡなど）、及び／又は開発中の他のポスト量子暗号化アルゴリズムを組み込む場合もある。

【００３５】

簡単にするため、従来のデータ・ネットワーキング、アプリケーション開発、及びシステム１００の他の機能上の態様は、本明細書において詳細には説明しない場合がある。更には、本明細書に含まれる様々な図面に示される連結線は、様々な要素間の例示的な機能上の関係性及び／又は電子的通信を表現することを意図されている。現実のシステムにおいては、多くの代替的又は追加的な機能上の関係性又は電子的通信が存在し得ることに留意されたい。

【００３６】

次に図２～図５を参照すると、描かれている処理の流れ及びスクリーンショットは、単なる実施形態であり、本開示の範囲を限定することは意図されていない。例えば、方法又は処理の説明のいずれかにおいて述べられるステップは、あらゆる順序で実行されてもよく、提示される順序に限定されない。以下の説明は、図２～図５に描かれるステップ及びユーザ・インターフェースの要素だけでなく、図１を参照して上述したような様々なシステム・コンポーネントにも適当な参照を行うことを諒解されたい。まず、例示の実施形態が図面及び以下の説明で示されるが、本開示の原理は、現在知られていても知られていな

くても、あらゆる数の技法を用いて実装することができることが理解されるべきである。本開示は、例示の実装形態、並びに図面及び以下の説明で示される技法に決して限定されるべきではない。そうではないと具体的に述べられない限り、図面に描かれる物品は必ずしも縮尺通りに描かれていない。

【００３７】

具体的に図２を参照すると、様々な実施形態による、ゼロ知識証明アルゴリズムを初期化するための処理２０１が開示されている。発行者システム１３０は、顧客及び販売者がゼロ知識証明支払いに参加することができるよう、ゼロ知識証明アルゴリズムを初期化することができる。

【００３８】

発行者システム１３０は、ゼロ知識証明アルゴリズムを検索する（ステップ２０２）。ゼロ知識証明アルゴリズムは、各顧客が取引中にあらゆる個人情報（例えば、取引口座データ、顧客データなど）を提供する必要なく、顧客が自身の個人情報を所有していることを、販売者が確認することを可能にする、あらゆる適切なアルゴリズムを含むことができる。例えば、ゼロ知識証明アルゴリズムは、ｚｋ－ＳＮＡＲＫであってもよく、又はあらゆる他の類似のゼロ知識証明アルゴリズムであってもよい。ゼロ知識証明アルゴリズムは、例えば鍵生成関数、証明関数、及び検証関数などの、一つ又は複数の、関数、プログラム、又はアルゴリズムを含むことができる。鍵生成関数は、本明細書において更に議論されるように、証明鍵ｐｋ及び検証鍵ｖｋを生成するように構成することができる。証明関数は、本明細書において更に議論されるように、証明（例えば証明ブロブ）を生成するように構成することができる。検証関数は、本明細書において更に議論されるように、ゼロ知識証明支払い処理の間、顧客を認可するためのその証明を検証するように構成することができる。様々な関数が、ＪＡＶＡＳＣＲＩＰＴ（登録商標）、又はあらゆる他の適切なプログラミング言語を使用してプログラミングすることができる。

【００３９】

発行者システム１３０は、ゼロ知識証明アルゴリズムからの鍵生成関数を使用して、証明鍵ｐｋ及び検証鍵ｖｋを生成する（ステップ２０４）。例えば、発行者システム１３０は、乱数（例えば、シークレット・パラメータ、ラムダ）を生成して、証明鍵ｐｋ及び検証鍵ｖｋを生成するよう乱数を鍵生成関数に入力する。様々な実施形態において、鍵を正常に生成したことに応じて、発行者システム１３０は、生成した鍵のセキュリティを高めるために乱数を削除する場合がある。様々な実施形態において、発行者システム１３０は、様々な支払いタイプ（例えば、クレジット・カード、デビット・カード、ギフト・カード、ロイヤルティ・ポイント、サード・パーティ支払いプロバイダなど）に基づいて、異なる鍵を生成する場合がある。発行者システム１３０は、証明鍵ｐｋ及び検証鍵ｖｋを発行する（ステップ２０６）。様々な実施形態において、発行者システム１３０は、公にアクセス可能なウェブ・サーバ、ウェブサイトなどで鍵を利用可能にすることによって、鍵を発行する場合がある。様々な実施形態において、発行者システム１３０は、ゼロ知識証明支払い用に登録された販売者及びユーザに鍵を送信する（例えば、検証鍵ｖｋを販売者システム１２０に送信し、証明鍵ｐｋを顧客デバイス１１０に送信する）ことによって、鍵を発行する場合がある。様々な実施形態において、発行者システム１３０は、ゼロ知識証明支払い処理の間、鍵のセキュリティを高めるために、任意の所望の間隔で（例えば、毎週、毎月など）新しい鍵を生成する場合がある。

【００４０】

発行者システム１３０は、ゼロ知識証明（ＺＫＰ）スマート・コントラクト１４５をブロックチェーン・ネットワーク１４０に展開する（ステップ２０８）。ＺＫＰスマート・コントラクト１４５は、発行者システム１３０によって、ゼロ知識証明アルゴリズムからの検証関数を含むように生成され得る。発行者システム１３０は（ブロックチェーン・ノード、ＡＰＩなどを介して）、ブロックチェーン書き込みを、ブロックチェーン・ネットワーク１４０の少なくとも一つの第２のブロックチェーン・ノードに伝搬させることにより、ＺＫＰスマート・コントラクト１４５をブロックチェーン・ネットワーク１４０に展

開することができる。ブロックチェーン・ノードは、あらゆる適切な技法及び合意アルゴリズムを使用して、書き込みに対して合意することができる。

【００４１】

具体的に図３を参照すると、様々な実施形態による、ゼロ知識証明支払い用の販売者登録のための処理３０１が開示されている。販売者システム１２０は、ウェブ・ブラウザ、モバイル・アプリケーションなどを介して、発行者システム１３０にアクセスする（ステップ３０２）。発行者システム１３０へのアクセスは、例えば販売者資格証明（例えば、ユーザ名、又は販売者識別子、パスワード、バイオメトリックな入力など）などの、あらゆる適切なアクセス制御を使用して制御することができる。様々な実施形態において、販売者システム１２０は、最初の販売者登録の一部として、発行者システム１３０にもアクセスする場合があり、将来的なアクセスのために販売者資格証明を受け取ることができる。販売者システム１２０は、ゼロ知識証明支払いについて発行者システム１３０への登録を要求する（ステップ３０４）。発行者システム１３０は、販売者１２５の識別情報を検証する（ステップ３０６）。例えば、販売者システム１２０は、販売者ＩＤ、販売者住所、販売者名などの、販売者識別情報を提供するよう促される場合がある。発行者システム１３０は、提供された販売者識別情報を記憶された販売者データと比較することにより、販売者１２５の識別情報を検証することができる。

【００４２】

様々な実施形態において、発行者システム１３０は、販売者ハッシュを生成する（ステップ３０８）。販売者ハッシュは、販売者１２５（及び販売者システム１２０）の一意な識別子として機能するよう生成され得る。発行者システム１３０は、一つ又は複数の販売者データ要素に基づいて販売者ハッシュを生成することができる。例えば、販売者ハッシュは、販売者事業名、販売者所有者名、販売者ＩＤ、販売者ナンスなどのうちの、一つ又は複数の一方向暗号化ハッシュを含む場合がある。販売者ナンスは、一つ又は複数の英数字を含む場合があり、販売者１２５に一意となるようにランダムに生成され得る（例えば、「ｃ９Ｌａ５」など、様々な任意の英数字を含む暗号法的ナンス）。発行者システム１３０は、暗号法ＳＨＡ－２シリーズからの暗号化アルゴリズム（例えば、ＳＨＡ２５６、ＳＨＡ５１２など）などの、あらゆる適切なハッシュ化アルゴリズムを使用して販売者ハッシュを生成することができる。発行者システム１３０は、総当たり攻撃、レインボー・テーブル攻撃などに対して、販売者ハッシュのセキュリティを高めるために、鍵ストレッチング技法及び又はあらゆる他の技法を使用して、販売者ハッシュを生成することもできる。様々な実施形態において、販売者ハッシュは、ランダムに生成された文字列、ブロックチェーン・アドレス、及び／又はあらゆる他の適切な一意な識別子を含むようにも生成することができる。

【００４３】

様々な実施形態において、発行者システム１３０は、販売者ハッシュをＺＫＰスマート・コントラクト１４５に渡すことによって、ＺＫＰスマート・コントラクト１４５を呼び出す（ステップ３１０）。ＺＫＰスマート・コントラクト１４５は、呼び出されたことに応じて、販売者ハッシュをブロックチェーンに書き込み、販売者ハッシュをブロックチェーンの販売者口座残高エントリに関連付ける。ＺＫＰスマート・コントラクト１４５は、ブロックチェーン書き込みを、ブロックチェーン・ネットワーク１４０内の少なくとも一つの第２のブロックチェーン・ノードに伝搬することができる。ブロックチェーン・ノードは、あらゆる適切な技法及び合意アルゴリズムを使用して、書き込みに対して合意することができる。ブロックチェーン書き込みが完了したことに応じて、ＺＫＰスマート・コントラクト１４５は、発行者システム１３０に書き込み通知を返すことができる。

【００４４】

発行者システム１３０は、販売者システム１２０を認可して、ＺＫＰスマート・コントラクト１４５を呼び出す（ステップ３１２）。例えば、ブロックチェーンが許可されたブロックチェーンである場合、発行者システム１３０は、販売者システム１２０を許可されたブロックチェーン・ネットワークに追加することができる。様々な実施形態において、

発行者システムは、一意な識別子及び／又はデジタル証明書をブロックチェーンの構成に追加して、販売者システム１２０がＺＫＰスマート・コントラクト１４５を呼び出すよう認可されていることを指定することができる。この点では、販売者システムによるＺＫＰスマート・コントラクト１４５の呼び出しは、特定の販売者システムの署名を含むことができる。発行者システム１３０は、販売者ハッシュ及び販売者ナンスを販売者システム１２０に送信する（ステップ３１４）。販売者システム１２０は、販売者ハッシュ及び販売者ナンスを、セキュアなローカル・リポジトリに記憶することができる。販売者システム１２０は、検証鍵ｖｋを検索する（ステップ３１６）。様々な実施形態において、販売者システム１２０は、ゼロ知識証明支払いの登録処理の間、検証鍵ｖｋを発行者システム１３０から検索することができる。様々な実施形態において、発行者システム１３０は、販売者ハッシュ及び販売者ナンスと共に、検証鍵ｖｋを販売者システム１２０に送信することもできる。

【００４５】

具体的に図４を参照すると、様々な実施形態による、ゼロ知識証明支払い用の顧客登録のための処理４０１が開示されている。顧客デバイス１１０は、ウェブ・ブラウザ、モバイル・アプリケーションなどを介して、発行者システム１３０にアクセスする（ステップ４０２）。発行者システム１３０へのアクセスは、例えば顧客資格証明（例えば、ユーザ名、パスワード、バイオメトリックな入力など）などの、あらゆる適切なアクセス制御を使用して制御することができる。様々な実施形態において、顧客デバイス１１０は、最初の顧客登録（例えば、ウェブサイト上での登録、取引口座の申請など）の一部として、発行者システム１３０にもアクセスする場合があり、将来的なアクセスのために顧客資格証明を受け取ることができる。顧客デバイス１１０は、ゼロ知識証明支払いについて発行者システム１３０への登録を要求する（ステップ４０４）。様々な実施形態において、登録要求は、顧客１１５がゼロ知識証明支払い用に使用したいと思う口座（例えば、取引口座、ギフト・カード、ロイヤルティ・ポイント口座、暗号通貨口座など）を含む可能性がある。登録要求は、顧客１１５がゼロ知識証明支払い用に使用可能にしたいと思う、口座の口座残高を含む場合もある。

【００４６】

発行者システム１３０は、顧客１１５の識別情報を検証する（ステップ４０６）。例えば、顧客デバイス１１０は、顧客名、顧客住所、取引口座番号、取引口座有効期限、取引口座セキュリティ・コード（ＣＶＶ）などの顧客識別情報を提供するよう促される場合がある。発行者システム１３０は、提供された顧客識別情報を記憶された顧客データと比較することにより、販売者１１５の識別情報を検証することができる。

【００４７】

様々な実施形態において、発行者システム１３０は、顧客ハッシュを生成する（ステップ４０８）。顧客ハッシュは、顧客１１５（及び／又は顧客デバイス１０）の一意な識別子として機能するよう生成され得る。発行者システム１３０は、一つ又は複数の顧客データ要素に基づいて顧客ハッシュを生成することができる。例えば、顧客ハッシュは、顧客名、顧客住所、取引口座番号、顧客ナンスなどのうちの、一つ又は複数の一方向暗号化ハッシュを含む場合がある。顧客ナンスは、一つ又は複数の英数字を含む場合があり、顧客１１５に一意となるようにランダムに生成され得る（例えば、「ａ８Ｋｎ４」など、様々な任意の英数字を含む暗号法的ナンス）。発行者システム１３０は、暗号法ＳＨＡ－２シリーズからの暗号化アルゴリズム（例えば、ＳＨＡ２５６、ＳＨＡ５１２など）などの、あらゆる適切なハッシュ化アルゴリズムを使用して顧客ハッシュを生成することができる。発行者システム１３０は、総当たり攻撃、レインボー・テーブル攻撃などに対して、顧客ハッシュのセキュリティを高めるために、鍵ストレッチング技法及び又はあらゆる他の技法を使用して、顧客ハッシュを生成することもできる。様々な実施形態において、顧客ハッシュは、ランダムに生成された文字列、ブロックチェーン・アドレス、及び／又はあらゆる他の適切な一意な識別子を含むようにも生成することができる。

【００４８】

発行者システム１３０は、顧客ハッシュをＺＫＰスマート・コントラクト１４５に渡すことによって、ＺＫＰスマート・コントラクト１４５を呼び出す（ステップ４１０）。様々な実施形態において、発行者システム１３０は、登録要求内で顧客１１５によって定められた口座残高を渡すこともできる。ＺＫＰスマート・コントラクト１４５は、呼び出されたことに応じて、顧客ハッシュをブロックチェーンに書き込み、顧客ハッシュをブロックチェーンの顧客口座残高エントリに関連付ける。顧客口座残高は、登録要求内で顧客１１５によって定められた口座残高によって定めることもできる。ＺＫＰスマート・コントラクト１４５は、ブロックチェーン書き込みを、ブロックチェーン・ネットワーク１４０内の少なくとも一つの第２のブロックチェーン・ノードに伝搬することができる。ブロックチェーン・ノードは、あらゆる適切な技法及び合意アルゴリズムを使用して、書き込みに対して合意することができる。ブロックチェーン書き込みが完了したことに応じて、ＺＫＰスマート・コントラクト１４５は、発行者システム１３０に書き込み通知を返すことができる。

【００４９】

発行者システム１３０は、顧客ハッシュ及び顧客ナンスを顧客デバイス１１０に送信する（ステップ４１２）。顧客デバイス１１０は、顧客ハッシュ及び顧客ナンスを、ローカルでセキュアなデバイス・リポジトリに記憶することができる。顧客デバイス１１０は、発行者システム１３０によって展開された場所から証明鍵ｐｋを検索する（ステップ４１４）例えば、様々な実施形態によると、証明鍵ｐｋは、販売者１２５から商品又はサービスを購入するために、顧客１１５によって使用されるモバイル・アプリケーション、ウェブサイトなどに統合することができる。様々な実施形態において、発行者システム１３０は、証明関数を顧客デバイス１１０に送信する、及び／又はゼロ知識証明支払い処理の間、顧客デバイス１１０内のソフトウェアが証明関数を実行できるようにする場合もある。様々な実施形態において、顧客デバイス１１０は、ゼロ知識証明支払い処理の間に証明関数を実行するように構成される、ネイティブなアプリケーションをダウンロード及び／又はインストールすることができるか、或いはブラウザベースのアプリケーションを使用することができる。

【００５０】

具体的に図５を参照すると、様々な実施形態による、ゼロ知識証明支払いのための処理５０１が開示されている。顧客１１５は、販売者１２５において買い物をする（ステップ５０２）。例えば、顧客１１５は、販売者１２５に関連付けられる実店舗型の小売店を訪れること、顧客デバイス１１０を介してオンライン・ストアを訪れることなどにより、販売者１２５で買い物をすることができる。顧客１１５が、一つ又は複数の、商品及び／又はサービスを購入したいと所望することに応じて、顧客１１５は販売者１２５と取引を開始する（ステップ５０４）。例えば、販売者１２５（及び／又は販売者システム１２０）は、顧客１１５（及び／又は顧客デバイス１１０）に支払い方法を選択するよう促す場合がある。顧客１１５は、ゼロ知識証明支払い方法を選択して取引を開始する可能性がある。

【００５１】

様々な実施形態において、顧客デバイス１１０は、購入ハッシュを生成する（ステップ５０６）。購入ハッシュは、顧客名、顧客住所、取引口座番号、顧客ナンスなどのうちの、一つ又は複数の一方向暗号化ハッシュを含む場合がある。顧客デバイス１１０は、暗号法ＳＨＡ－２シリーズからの暗号化アルゴリズム（例えば、ＳＨＡ２５６、ＳＨＡ５１２など）などの、あらゆる適切なハッシュ化アルゴリズムを使用して顧客ハッシュを生成することができる。顧客デバイス１１０は、総当たり攻撃、レインボー・テーブル攻撃などに対して、顧客ハッシュのセキュリティを高めるために、鍵ストレッチング技法及び又はあらゆる他の技法を使用して、顧客ハッシュを生成することもできる。

【００５２】

顧客デバイス１１０は、ゼロ知識証明アルゴリズムからの証明関数を使用して証明を生成する（ステップ５０８）。証明は、バイナリ・ラージ・オブジェクト（ＢＬＯＢ）ファイルを含むように生成することができる。顧客デバイス１１０は、証明鍵ｐｋ、顧客ハッ

シュ、及び購入ハッシュを証明関数に入力して、証明を生成することができる。顧客デバイス１１０は、証明及び顧客ハッシュを販売者システム１２０に送信する（ステップ５１０）。

【００５３】

証明及び顧客ハッシュを受信したことに応じて、販売者システム１２０は、証明、顧客ハッシュ、購入金額、検証鍵ｖｋ、及び販売者ハッシュを渡すことによりＺＫＰスマート・コントラクト１４５を呼び出す（ステップ５１２）。ＺＫＰスマート・コントラクト１４５は、呼び出されたことに応じて、ゼロ知識証明アルゴリズムからの検証関数を実行する（ステップ５１４）。ＺＫＰスマート・コントラクト１４５は、検証鍵ｖｋ、顧客ハッシュ、及び証明を入力することによって、検証関数を実行する。検証関数は、実行されたことに応じて、検証が成功したかどうかを示すブール値を返すことができる。例えば、ブール値１（例えば、「真」）は、検証が成功したことを示し、ブール値０（例えば、「偽」）は、検証が失敗したことを示す。様々な実施形態において、販売者システム１２０は、検証関数を実行するように構成することができ、検証関数の結果をＺＫＰスマート・コントラクト１４５に送信することができる。検証が失敗したことに応じて、ＺＫＰスマート・コントラクト１４５は、販売者システム１２０に検証失敗通知を返す場合がある。検証が成功したことに応じて、ＺＫＰスマート・コントラクト１４５は、支払いの処理を進めることができる。

【００５４】

例えば、様々な実施形態により、ＺＫＰスマート・コントラクト１４５は、顧客１１５の口座残高を決定する（ステップ５１６）。例えば、ＺＫＰスマート・コントラクト１４５は、顧客ハッシュに関連付けられた顧客口座残高を決定するために、顧客ハッシュに基づいてブロックチェーンに問い合わせを行う場合がある。ＺＫＰスマート・コントラクト１４５は、顧客口座残高を購入金額と比較して、ゼロ知識証明取引を完了するために顧客１１５が十分な資金を有しているかどうかを判断することができる。その顧客１１５が有する資金は購入を完了するためには不十分であると判断したことに応じて、ＺＫＰスマート・コントラクト１４５は、資金不十分通知を販売者システム１２０に返すことができる。その顧客１１５が有する資金は購入を完了するために十分であると判断したことに応じて、ＺＫＰスマート・コントラクト１４５は、購入金額に基づいて顧客１１５の口座残高を調整する（ステップ５１８）。例えば、ＺＫＰスマート・コントラクト１４５は、口座残高を購入金額と同額分減少させることにより、顧客口座残高を調整することができる。ＺＫＰスマート・コントラクト１４５は、購入金額に基づいて販売者１２５の口座残高を調整する（ステップ５２０）。ＺＫＰスマート・コントラクト１４５は、販売者ハッシュに関連付けられた販売者口座残高の場所を探すために、販売者ハッシュに基づいてブロックチェーンに問い合わせを行う場合がある。ＺＫＰスマート・コントラクト１４５は、口座残高をあらゆる適用可能な取引手数料を購入金額から引いた分を増加させることにより、販売者口座残高を調整することができる。

【００５５】

様々な実施形態において、ＺＫＰスマート・コントラクト１４５は、顧客１１５及び販売者１２５の口座残高を正常に調整したことに応じて、成功通知をブロックチェーンに書き込む（ステップ５２２）。ＺＫＰスマート・コントラクト１４５は、ブロックチェーン書き込みを、ブロックチェーン・ネットワーク１４０内の少なくとも一つの第２のブロックチェーン・ノードに伝搬することができる。ブロックチェーン・ノードは、あらゆる適切な技法及び合意アルゴリズムを使用して、書き込みに対して合意することができる。ブロックチェーン書き込みが完了したことに応じて、ＺＫＰスマート・コントラクト１４５は、販売者システム１２０に成功通知を返すことができる（ステップ５２４）。販売者１２５は、成功通知を受信したことに応じて、顧客１１５との取引を完了する（ステップ５２６）。例えば、販売者１２５は、商品及び／又はサービスを顧客１１５に提供することによって、取引を完了する場合がある。

【００５６】

様々な実施形態において、ゼロ知識証明支払い処理を完了したことに基づく販売者１２５への支払いは、処理の完了後、任意の適切な時間（例えば、リアルタイムに、ほぼリアルタイムに、バッチ処理で、など）において発行者システム１３０によって完了され得る。例えば、発行者システム１３０は、販売者口座残高を（例えば、販売者ハッシュに基づいてブロックチェーンに問い合わせすることにより）決定することができ、通常の決済処理にしたがって、販売者口座残高と同額の資金を販売者１２５に送信することができる。

【００５７】

システム、方法、及びコンピュータ・プログラム製品が提供される。本明細書における詳細な説明では、「様々な実施形態」、「一実施形態」、「実施形態」、「例示の実施形態」などの言及は、説明される実施形態が、特定の特徴、構造又は特性を含む可能性があるが、すべての実施形態がその特定の特徴、構造又は特性を必ずしも含まないことを示す。更には、そのような言い回しは、必ずしも同一の実施形態に言及しない。更には、特定の特徴、構造又は特性がある実施形態と併せて説明される場合、明示的に説明されるかどうかにかかわらず、他の実施形態と併せてそのような特徴、構造又は特性に影響することは当業者の知識のうちであると思われる。説明を読めば、関連分野の当業者には、代替的な実施形態においてどのように本開示を実装するかが明らかとなろう。

【００５８】

本明細書において使用される場合、「満足する」、「満たす」、「一致する」、「に関連付けられる」又は類似の言い回しには、同一の一致、部分的な一致、一定の基準を満たすこと、データの部分集合を一致させること、相関関係、一定の基準を満足すること、対応関係、関連付け、アルゴリズム上の関連性などが含まれる場合がある。同様に、本明細書において使用される際、「認証」又は類似の用語には、完全な認証、部分的な認証、データの部分集合を認証すること、対応関係、一定の基準を満足すること、関連付け、アルゴリズム上の関連性などが含まれる場合がある。

【００５９】

「関連付ける」及び／又は「関連付けること」に類似した用語及び言い回しには、タグ付けすること、フラグを立てること、相関付けること、ルックアップ・テーブルを使用すること、又は例えば（ｉ）取引口座と（ｉｉ）項目（例えば、提案、報酬ポイント、ディスカウントなど）及び／若しくはデジタル・チャネルとの要素間などの関連性を示す若しくは作るための、あらゆる他の方法若しくはシステムが含まれる場合がある。その上、関連付けは、あらゆる適切な行為、事象、又は期間に応じてあらゆる時点で生じる可能性がある。関連付けは、所定の間隔で、定期的に、ランダムに、一度だけ、複数回、又は適切な要求若しくは行為に応じて生じる場合がある。情報のいずれも、ソフトウェア対応リンクを介して配信及び／又はアクセスされる場合があり、リンクは電子メール、テキスト、投稿、ソーシャル・ネットワーク入力、及び／又は当分野で既知のあらゆる他の方法により送信される場合がある。

【００６０】

「項目」に類似した言い回し及び用語には、あらゆる商品、サービス、情報、体験、娯楽、データ、提案、ディスカウント、払い戻し、ポイント、仮想通貨、コンテンツ、アクセス、レンタル、リース、寄付、勘定、クレジット、デビット、利益、権利、報酬、ポイント、クーポン、クレジット、金銭的等価物、何らかの価値があるもの、最小限の価値のもの又は価値がないもの、金銭的価値、金銭的価値がないものなどが含まれる場合がある。その上、本明細書において議論される「取引」又は「購入」は、項目に関連付けられる場合がある。更には、「報酬」は項目であり得る。

【００６１】

「顧客」、「ユーザ」、「取引口座保有者」、「取引口座受取人」、「取引口座アフィリエイト」、「消費者」、「顧客」、「カードメンバ」などの言い回しは、取引口座を使用して一人若しくは複数の販売者により提供される販売者提供物を買う、及び／又は物理的なカードが取引口座に関連付けられているかどうかにかかわらず取引口座に対して取引を行うために合法的に指定される、あらゆる人物、実体、事業体、政府組織、事業体、ソ

フトウェア、ハードウェア、又は取引口座に関連付けられたマシンを含むものである。例えば、ユーザには、取引口座の所有者、取引口座のユーザ、口座アフィリエイト、子供用口座のユーザ、子会社口座ユーザ、口座の受取人、口座の管理人、及び／又は取引口座に関係する、若しくは関連付けられた、他の人物若しくは実体が含まれる場合がある。

【００６２】

本明細書において使用される際、「取引口座」、「口座番号」、「口座コード」、又は「消費者口座」に類似した言い回し及び用語には、消費者がシステムにアクセスできるように、システムと対話若しくは通信できるように、適切に構成された、あらゆるデバイス、コード（例えば、認可／アクセス・コード、個人識別番号（「ＰＩＮ」）、インターネット・コード、他の識別コードなどのうちの一つ又は複数）、数字、文字、記号、デジタル証明、スマート・チップ、デジタル信号、アナログ信号、バイオメトリック、又は他の識別子／インデックスが含まれる場合がある。取引口座番号は、任意選択的に、報酬口座、掛売口座、クレジット口座、デビット口座、プリペイド口座、テレホン・カード、エンボス・カード、スマート・カード、磁気ストライプ・カード、バーコード・カード、トランスポンダ、無線周波カード又は関連する口座に、配置又は関連付けられる場合がある。

【００６３】

取引口座番号は、自分自身から第２のデバイスに対して、データを送信又はダウンロードすることが可能な、あらゆる形態のプラスチック、電子的、磁気的、無線周波数、ワイヤレス、音声、及び／又は光学的なデバイスとして、配布され、記憶することができる。取引口座番号は、例えば、１６桁の口座番号であり得るが、各取引口座発行者は、ＡＭＥＲＩＣＡＮ　ＥＸＰＲＥＳＳ（登録商標）社によって使用される１５桁の番号体系など、独自の番号体験を有している。この点において、取引口座発行者の取引口座番号のそれぞれは、その取引口座発行者の標準化されたフォーマットに準ずることができ、それにより、１５桁フォーマットを使用する取引口座発行者は、数字「００００　０００００　０００００」として表現されるような、三つのスペースを伴う一組の数字を、一般的に使用することができる。先頭の５桁から７桁は、処理目的用に予約済であり得、取引口座発行者、口座タイプなどを特定する。この例では、最終桁（１５桁目）は、１５桁の数についてのチェック・サムとして使用され、中間の８桁から１１桁はユーザを一意に特定するために使用される。販売者識別子は、例えば、口座の受付、口座の精算、レポーティングなどの目的で、特定の販売者を特定する、あらゆる数字又は英数字であり得る。

【００６４】

「金融機関」、「発行者システム」、又は「取引口座発行者」に類似した言い回し及び用語には、取引口座サービスを提供するあらゆる実体が含まれる場合がある。よく「金融機関」と称されるが、金融機関は、あらゆるタイプの銀行、貸し手、又はクレジット・カード会社、カード・スポンサ会社、若しくは金融機関と提携しているサード・パーティ発行者など他のタイプの口座発行機関を表す場合がある。取引の一部のフェーズには中間決済機関など他の関係者が関与する場合があることに更に留意されたい。

【００６５】

「販売者」、「事業体」、「売り手」又は「サプライヤ」に類似した言い回し及び用語は、互いに互換的に使用される場合があり、あらゆる人物、実体、配信システム、ソフトウェア、並びに／又は、商品若しくはサービスの配信チェーン内のプロバイダ、ブローカ、及び／若しくは任意の他の実体であるハードウェアを意味する。例えば、販売者は、食料品店、小売店、旅行代理店、サービス・プロバイダ、オンライン販売者などであり得る。販売者は、取引口座発行者の取引口座を保有するユーザ向けに売られる商品又はサービスに対する支払いを要求することがある。

【００６６】

様々な実施形態において、顧客デバイス１１０は、一つ又は複数のスマート・デジタル・アシスタント技術と統合される場合がある。例えば、例示的なスマート・デジタル・アシスタント技術としては、ＡＭＡＺＯＮ（登録商標）社によって開発されたＡＬＥＸＡ（登録商標）システム、Ａｌｐｈａｂｅｔ，Ｉｎｃ．によって開発されたＧＯＯＧＬＥ　Ｈ

ＯＭＥ（登録商標）システム、ＡＰＰＬＥ（登録商標）社のＨＯＭＥＰＯＤ（登録商標）システム、及び／又は類似のデジタル・アシスタント技術を挙げることができる。ＡＬＥＸＡ（登録商標）システム、ＧＯＯＧＬＥ　ＨＯＭＥ（登録商標）システム、及びＨＯＭＥＰＯＤ（登録商標）システムは、タスク、エンターテインメント、一般的な情報、他を支援することができるクラウドベースの音声アクティベーション・サービスをそれぞれ提供することができる。ＡＭＡＺＯＮ　ＥＣＨＯ（登録商標）、ＡＭＡＺＯＮ　ＥＣＨＯ　ＤＯＴ（登録商標）、ＡＭＡＺＯＮ　ＴＡＰ（登録商標）及びＡＭＡＺＯＮ　ＦＩＲＥ（登録商標）ＴＶなどのすべてのＡＬＥＸＡ（登録商標）デバイスは、ＡＬＥＸＡ（登録商標）システムへのアクセスを有する。ＡＬＥＸＡ（登録商標）システム、ＧＯＯＧＬＥ　ＨＯＭＥ（登録商標）システム、及びＨＯＭＥＰＯＤ（登録商標）システムは、その音声アクティベーション技術により、音声コマンドを受信すること、他の機能をアクティブ化すること、スマート・デバイスを制御すること、及び／又は情報を集めることができる。例えば、スマート・デジタル・アシスタント技術は、音楽、電子メール、テキスト、電話呼、質問応答、家庭内改善情報、スマート・ホーム通信／アクティベーション、ゲーム、ショッピング、ｔｏ－ｄｏリストの作製、アラーム設定、ポッドキャストのストリーミング、音声ブックの再生、並びに気象情報、交通情報、及びニュースなどの他のリアルタイム情報などの提供と対話するために使用することができる。更にＡＬＥＸＡ（登録商標）、ＧＯＯＧＬＥ　ＨＯＭＥ（登録商標）、及びＨＯＭＥＰＯＤ（登録商標）システムにより、すべてのデジタル・アシスタント対応デバイスをまたいでユーザがオンライン口座にリンクされた対象取引口座についての情報にアクセスできるようになる場合がある。

【００６７】

本明細書において議論されるあらゆる通信、送信及び／又はチャネルには、コンテンツ（例えば、データ、情報、メタデータなど）を配信するためのあらゆるシステム若しくは方法、及び／又はコンテンツそのものが含まれる場合がある。コンテンツは、あらゆる形態で、又はあらゆる媒体に存在することができ、様々な実施形態において、コンテンツは電子的に配信することができる、及び／又は電子的に提示することができる。例えば、チャネルはウェブサイト、又はデバイス（例えば、Ｆａｃｅｂｏｏｋ（登録商標）、ＹＯＵＴＵＢＥ（登録商標）、ＡＰＰＬＥ（登録商標）ＴＶ（登録商標）、ＰＡＮＤＯＲＡ（登録商標）、ＸＢＯＸ（登録商標）、ＳＯＮＹ（登録商標）ＰＬＡＹＳＴＡＴＩＯＮ（登録商標））、ｕｎｉｆｏｒｍ　ｒｅｓｏｕｒｃｅ　ｌｏｃａｔｏｒ（「ＵＲＬ」）、文書（例えば、ＭＩＣＲＯＳＯＦＴ（登録商標）Ｗｏｒｄ（登録商標）文書、ＭＩＣＲＯＳＯＦＴ（登録商標）Ｅｘｃｅｌ（登録商標）文書、ＡＤＯＢＥ（登録商標）．ｐｄｆ文書など）、「電子ブック」、「電子雑誌」、アプリケーション若しくはマイクロ・アプリケーション（本明細書において説明されるようなもの）、ＳＭＳ若しくは他のタイプのテキスト・メッセージ、電子メール、ＦＡＣＥＢＯＯＫ（登録商標）メッセージ、ＴＷＩＴＴＥＲ（登録商標）ツイート、ＭＭＳ、及び／又は他のタイプの通信技術を含むことができる。様々な実施形態において、チャネルはデータ・パートナによってホストされ得る又は提供され得る。様々な実施形態において、配信チャネルは、販売者ウェブサイト、ソーシャル・メディア・ウェブサイト、アフィリエイト若しくはパートナのウェブサイト、外部ベンダ、モバイル・デバイス通信、ソーシャル・メディア・ネットワーク、及び／又はロケーション・ベースのサービスのうちの少なくとも一つを含む場合がある。配信チャネルは、販売者ウェブサイト、ソーシャル・メディア・サイト、アフィリエイト若しくはパートナのウェブサイト、外部ベンダ、及びモバイル・デバイス通信のうちの少なくとも一つを含む場合がある。ソーシャル・メディア・サイトの例としては、ＦＡＣＥＢＯＯＫ（登録商標）、ＦＯＵＲＳＱＵＡＲＥ（登録商標）、ＴＷＩＴＴＥＲ（登録商標）、ＭＹＳＰＡＣＥ（登録商標）、ＬＩＮＫＥＤＩＮ（登録商標）などが挙げられる。アフィリエイト若しくはパートナのウェブサイトの例としては、ＡＭＥＲＩＣＡＮ　ＥＸＰＲＥＳＳ（登録商標）、ＧＲＯＵＰＯＮ（登録商標）、ＬＩＶＩＮＧＳＯＣＩＡＬ（登録商標）などが挙げられる。その上、モバイル・デバイス通信の例としては、テキスト送信、電子メール、及びスマートフォン用モバイル・アプリケーションが挙げられる。

【００６８】
様々な実施形態において、本明細書において説明される方法は、本明細書において説明される様々な特定のマシンを使用して実装される。本明細書において説明される方法は、当業者がすぐに理解できるように、以下の特定のマシン及び今後開発されるマシンを使用して、あらゆる適当な組み合わせで実装することができる。更には、本開示から明白なように、本明細書において説明される方法は、ある物品の様々な変形形態をもたらす可能性がある。
【００６９】
簡単にするため、従来のデータ・ネットワーキング、アプリケーション開発、及びシステム（並びに、システムの個々の動作中の構成要素の構成要素）の他の機能上の態様は、本明細書において詳細には説明しない場合がある。更には、本明細書に含まれる様々な図面に示される連結線は、様々な要素間の例示的な機能上の関係性及び／又は物理的な連結を表現することを意図されている。現実のシステムにおいては、多くの代替的又は追加的な機能上の関係性又は物理的な接続が存在し得ることに留意されたい。
【００７０】
本明細書において議論される様々なシステム・コンポーネントは次のうちの一つ又は複数を含むことができる：デジタル・データを処理するためのプロセッサを含むホスト・サーバ又は他のコンピューティング・システム；デジタル・データを記憶するためにプロセッサに結合されたメモリ；デジタル・データを入力するためにプロセッサに結合された入力デジタイザ；プロセッサによるデジタル・データの処理を指示するための、メモリに記憶されプロセッサからアクセス可能なアプリケーション・プログラム；プロセッサによって処理されたデジタル・データから導かれた情報を表示するための、プロセッサ及びメモリに結合されたディスプレイ・デバイス；及び複数のデータベース。本明細書で使用される様々なデータベースには、クライアント・データ、販売者データ、金融機関データ、及び／又はシステムの動作に有用なデータが含まれる場合がある。当業者であれば、ユーザ・コンピュータは、オペレーティング・システム（例えば、ＷＩＮＤＯＷＳ（登録商標）、ＯＳ２、ＵＮＩＸ（登録商標）、ＬＩＮＵＸ（登録商標）、ＳＯＬＡＲＩＳ（登録商標）、ＭａｃＯＳなど）、並びに通常コンピュータに関連付けられた様々な従来型のサポート・ソフトウェア及びドライバを含む可能性があることを諒解されよう。
【００７１】
本システム、又はそのあらゆる部分若しくは機能は、ハードウェア、ソフトウェア、又はその組み合わせを使用して実装されてもよく、一つ又は複数の、コンピュータ・システム又は他の処理システムに実装することができる。しかしながら、実装形態によって実施される操作は、一致する又は選択するなどの用語で言及されることが多く、これらは一般的に人間オペレータにより行われる精神的な作用に関連付けられる。本明細書において説明される操作のいずれにおいても、人間オペレータのそのような能力は、必要ないか、又はたいていの場合、望ましくない。むしろ、操作は機械操作である可能性があるか、又は操作のいずれも人工知能（ＡＩ）若しくは機械学習によって行うことができる若しくは拡張することができる。様々な実施形態を実施するために有用な機械には、汎用のデジタル・コンピュータ又は類似のデバイスが含まれる。
【００７２】
実際、様々な実施形態によると、実施形態は、本明細書において説明される機能性を遂行することができる、一つ又は複数のコンピュータ・システムを対象としている。コンピュータ・システムは、プロセッサなど、一つ又は複数のプロセッサを含む。プロセッサは、通信インフラストラクチャに接続される（例えば、通信バス、クロス・オーバ・バー、又はネットワーク）。様々なソフトウェア実施形態を、この例示的なコンピュータ・システムの観点から説明する。本説明を読めば、当業者には、他のコンピュータ・システム及び／又はアーキテクチャを使用して様々な実施形態をどのように実装するか、明らかとなろう。コンピュータ・システムは、グラフィック、テキスト、及び通信インフラストラクチャから（又は、図示されていないフレーム・バッファから）のディスプレイ・ユニット

上での表示用の他のデータを転送する、ディスプレイ・インターフェースを含むことができる。

【００７３】

コンピュータ・システムは、例えば、ランダム・アクセス・メモリ（ＲＡＭ）などの主メモリも含むことができ、セカンダリ・メモリ又はインメモリ（非スピニング）ハード・ドライブを含むこともできる。セカンダリ・メモリとしては、例えばハード・ディスク・ドライブ及び／又はリムーバブル記憶ドライブを挙げることができ、フロッピ・ディスク・ドライブ、磁気テープ・ドライブ、光学ディスク・ドライブなどがある。リムーバブル記憶ドライブは、周知のやり方で、リムーバブル記憶ユニットから読み出し、及び／又はリムーバブル記憶ユニットに書き込みを行う。リムーバブル記憶ユニットには、フロッピ・ディスク、磁気テープ、光学ディスクなどがあり、これらはリムーバブル記憶ドライブによって読み出し及び書き込みが行われる。理解されるように、リムーバブル記憶ユニットは、コンピュータ・ソフトウェア及び／又はデータが記憶されている、コンピュータ使用可能な記憶媒体を含む。

【００７４】

様々な実施形態において、セカンダリ・メモリは、コンピュータ・プログラム又は他の命令をコンピュータ・システムにロードできるようにする、他の類似のデバイスを含むことができる。そのようなデバイスとしては、例えば、リムーバブル記憶ユニット及びインターフェースが挙げられる。そのような例としては、プログラム・カートリッジとカートリッジ・インターフェース（ビデオゲーム機で見られるようなもの）、リムーバブル・メモリ・チップ（消去可能プログラマブル読み出し専用メモリ（ＥＰＲＯＭ）、又はプログラマブル読み出し専用メモリ（ＰＲＯＭ）など）と関連するソケット、及び他のリムーバブル記憶ユニットとインターフェースを挙げることができ、これらはソフトウェア及びデータを、リムーバブル記憶ユニットからコンピュータ・システムに転送できるようにする。

【００７５】

コンピュータ・システムには通信インターフェースも含まれる場合がある。通信インターフェースにより、コンピュータ・システムと外部デバイスとの間で、ソフトウェア及びデータを転送することができる。通信インターフェースの例としては、モデム、ネットワーク・インターフェース（イーサネット・カードなど）、通信ポート、パーソナル・コンピュータ・メモリ・カード国際協会（ＰＣＭＣＩＡ）スロット及びカードなどを挙げることができる。通信インターフェースを介して転送されるソフトウェア及びデータ・ファイルは、電子的、電磁気的、光学的、又は通信インターフェースによって受信可能な他の信号であり得る信号の形態である。これらの信号は通信経路（例えば、チャネル）を介して通信インターフェースに与えられる。このチャネルは、信号を搬送し、ワイヤ、ケーブル、光ファイバ、電話線、セルラ・リンク、無線周波数（ＲＦ）リンク、ワイヤレス、及び他の通信チャネルを使用して実装することができる。

【００７６】

用語「コンピュータ・プログラム媒体」及び「コンピュータ使用可能媒体」及び「コンピュータ可読媒体」は、一般的にリムーバブル記憶ドライブ及びハード・ディスク・ドライブに設置されたハード・ディスクなどの媒体を称するために使用される。これらのコンピュータ・プログラム製品は、ソフトウェアをコンピュータ・システムへ与える。

【００７７】

コンピュータ・プログラム（コンピュータ制御ロジックとも称される）は、主メモリ及び／又はセカンダリ・メモリに記憶される。コンピュータ・プログラムは、通信インターフェースを介して受信することもできる。このようなコンピュータ・プログラムは、実行されると、コンピュータ・システムが、本明細書において議論されるような特徴を実施できるようにする。特に、コンピュータ・プログラムは、実行されると、プロセッサが、様々な実施形態の特徴を実施できるようにする。したがって、このようなコンピュータ・プログラムは、コンピュータ・システムのコントローラを代表する。

【００７８】

様々な実施形態において、ソフトウェアは、コンピュータ・プログラム製品に記憶され、リムーバブル記憶ドライブ、ハード・ディスク・ドライブ、又は通信インターフェースを使用して、コンピュータ・システムにロードすることができる。制御ロジック（ソフトウェア）は、プロセッサによって実行されると、プロセッサに、本明細書において説明されるような様々な実施形態の機能を実施させる。様々な実施形態において、特定用途向け集積回路（ＡＳＩＣ）などの、ハードウェア構成要素。本明細書において説明される機能を実施するためのハードウェア状態機械の実装形態は、当業者には明らかである。

【００７９】

様々な実施形態において、サーバには、アプリケーション・サーバ（例えば、ＷＥＢＳＰＨＥＲＥ（登録商標）、ＷＥＢＬＯＧＩＣ（登録商標）、ＪＢＯＳＳ（登録商標）、ＥＤＢ（登録商標）ＰＯＳＴＧＲＥＳ ＰＬＵＳ ＡＤＶＡＮＣＥＤ ＳＥＲＶＥＲ（登録商標）（ＰＰＡＳ）など）が含まれる場合がある。様々な実施形態において、サーバには、ウェブ・サーバ（例えば、ＡＰＡＣＨＥ（登録商標）、ＩＩＳ、ＧＷＳ、ＳＵＮ ＪＡＶＡ（登録商標）ＳＹＳＴＥＭ ＷＥＢ ＳＥＲＶＥＲ、ＬＩＮＵＸ（登録商標）又はＷＩＮＤＯＷＳ（登録商標）上で動作するＪＡＶＡ（登録商標）仮想マシン）が含まれる場合がある。

【００８０】

ウェブ・クライアントは、例えば本明細書において議論されるネットワークなどのあらゆるネットワークを介して通信する、あらゆるデバイス（例えば、パーソナル・コンピュータ）を含む。このようなブラウザ・アプリケーションには、オンライン取引及び／又は通信を行うためにコンピューティング・ユニット又はシステムにインストールされたインターネット閲覧ソフトウェアが含まれる場合がある。これらのコンピューティング・ユニット又はシステムは、一つのコンピュータ、又は一組のコンピュータの形態を取ることができるが、他のタイプのコンピューティング・ユニット又はシステムを使用することもでき、ラップトップ、ノートブック、タブレット、ハンド・ヘルドのコンピュータ、携帯情報端末、セットトップ・ボックス、ワークステーション、コンピュータ・サーバ、メーンフレーム・コンピュータ、ミニコンピュータ、ＰＣサーバ、パーベイシブ・コンピュータ、コンピュータのネットワーク・セット、ＩＰＡＤＳ（登録商標）、ＩＭＡＣＳ（登録商標）、及びＭＡＣＢＯＯＫＳ（登録商標）などのパーソナル・コンピュータ、キオスク、端末、販売時点情報管理（ＰＯＳ）デバイス若しくは端末、テレビジョン、又はネットワーク上でデータを受信することができるあらゆる他のデバイスを含む。ウェブ・クライアントは、ＭＩＣＲＯＳＯＦＴ（登録商標）ＩＮＴＥＲＮＥＴ ＥＸＰＬＯＲＥＲ（登録商標）、ＭＯＺＩＬＬＡ（登録商標）ＦＩＲＥＦＯＸ（登録商標）、ＧＯＯＧＬＥ（登録商標）ＣＨＲＯＭＥ（登録商標）、ＡＰＰＬＥ（登録商標）Ｓａｆａｒｉ、又はインターネットを閲覧するために利用可能な数々のソフトウェア・パッケージのうちの任意の他のものを実行することもある。

【００８１】

当業者であれば、ウェブ・クライアントは、アプリケーション・サーバと直接接していてもよく、直接接していなくてもよいことを諒解されよう。例えば、ウェブ・クライアントは、インターネット・サーバへの直接又は間接の接続を有する場合がある別のサーバ及び／又はハードウェア・コンポーネントを通じてアプリケーション・サーバのサービスにアクセスすることができる。例えば、ウェブ・クライアントは、ロード・バランサを介してアプリケーション・サーバと通信する場合がある。様々な実施形態において、アクセスは、市販のウェブ・ブラウザのソフトウェア・パッケージを通じてネットワーク又はインターネットを通じたものである。

【００８２】

当業者であれば、ウェブ・クライアントはオペレーティング・システム（例えば、ＷＩＮＤＯＷＳ（登録商標）ＯＳ、ＯＳ２、ＵＮＩＸ（登録商標）ＯＳ、ＬＩＮＵＸ（登録商標）ＯＳ、ＳＯＬＡＲＩＳ（登録商標）、ＭａｃＯＳなど）、並びに通常コンピュータに関連付けられた様々な従来型のサポート・ソフトウェア及びドライバを含むことを諒解さ

れよう。ウェブ・クライアントには、あらゆる適切なパーソナル・コンピュータ、ネットワーク・コンピュータ、ワークステーション、携帯情報端末、携帯電話、スマートフォン、ミニコンピュータ、メーンフレームなどが含まれ得る。ウェブ・クライアントは、ネットワークへのアクセスを有する家庭用又は事業用の環境内にあることができる。様々な実施形態において、アクセスは、市販のウェブ・ブラウザのソフトウェア・パッケージを通じてネットワーク又はインターネットを通じたものである。ウェブ・クライアントは、セキュア・ソケット・レイヤ（ＳＳＬ）及びトランスポート層セキュリティ（ＴＬＳ）などのセキュリティ・プロトコルを実装することができる。ウェブ・クライアントは、ｈｔｔｐ、ｈｔｔｐｓ、ｆｔｐ及びｓｆｔｐを含むいくつかのアプリケーション層プロトコルを実装することができる。

【００８３】

様々な実施形態において、システム１００のコンポーネント、モジュール、及び／又はエンジンは、マイクロ・アプリケーション又はマイクロアプリとして実装される場合がある。マイクロアプリは通常、例えばＷＩＮＤＯＷＳ（登録商標）モバイル・オペレーティング・システム、ＡＮＤＲＯＩＤ（登録商標）オペレーティング・システム、ＡＰＰＬＥ（登録商標）ＩＯＳ（登録商標）、ＢＬＡＣＫＢＥＲＲＹ（登録商標）オペレーティング・システムなどを含む、モバイルのオペレーティング・システムのコンテキストで展開される。マイクロアプリは、より大きいオペレーティング・システムのリソース並びに所定の規則のセットにより様々なオペレーティング・システム及びハードウェア・リソースを管理する関連付けられたハードウェアを活用するように構成され得る。例えば、マイクロアプリがモバイル・デバイス又はモバイル・オペレーティング・システム以外のデバイス又はネットワークと通信したい場合、マイクロアプリはモバイル・オペレーティング・システムの所定の規則の下、オペレーティング・システム及び関連付けられたデバイス・ハードウェアの通信プロトコルを活用することができる。その上、マイクロアプリがユーザからの入力を所望する場合、マイクロアプリは様々なハードウェア・コンポーネントをモニタリングし、ハードウェアからの検出した入力をマイクロアプリに通信するオペレーティング・システムに、応答を要求するように構成することができる。

【００８４】

本明細書において使用される場合、「識別子」は、ある項目を一意に特定する、あらゆる適切な識別子であり得る。例えば、識別子は、グローバル一意識別子（「ＧＵＩＤ」）であってもよい。ＧＵＩＤは、ユニバーサル一意識別子規格の下で作製される及び／又は実装される識別子であり得る。その上、ＧＵＩＤは、３２桁の１６進表記として表示することができる１２８ビット値として記憶することができる。識別子は、メジャー番号及びマイナー番号を含む場合がある。メジャー番号及びマイナー番号は、それぞれ１６ビットの整数であり得る。

【００８５】

本明細書において議論されるあらゆるデータベースは、リレーショナル、階層的、グラフィカル、ブロックチェーン、又はオブジェクト指向構造、及び／若しくはあらゆる他のデータベース構成を含むことができる。あらゆるデータベースは、フラット・ファイル構造を含む場合もあり、フラット・ファイル構造では、データは、インデックス付けの構造がなくレコード間に構造的なリレーションシップのない行列形式で単一ファイルに記憶することができる。例えば、フラット・ファイル構造は、区切られたテキストのファイル、ＣＳＶ（カンマ区切り値）ファイル、及び／又はあらゆる他の適切なフラット・ファイル構造を含むことができる。データベースを実装するために使用することができる一般的なデータベース製品には、ＩＢＭ（登録商標）（Ａｒｍｏｎｋ、ＮＹ）のＤＢ２、ＯＲＡＣＬＥ（登録商標）コーポレーション（Ｒｅｄｗｏｏｄ Ｓｈｏｒｅｓ、ＣＡ）から市販の様々なデータベース製品、ＭＩＣＲＯＳＯＦＴ（登録商標）コーポレーション（Ｒｅｄｍｏｎｄ、Ｗａｓｈｉｎｇｔｏｎ）からのＭＩＣＲＯＳＯＦＴ Ａｃｃｅｓｓ（登録商標）又はＭＩＣＲＯＳＯＦＴ ＳＱＬ ＳＥＲＶＥＲ（登録商標）、ＭｙＳＱＬ ＡＢ（Ｕｐｐｓａｌａ、Ｓｗｅｄｅｎ）のＭｙＳＱＬ（登録商標）、ＭＯＮＧＯＤＢ（登録商標）、Ｒ

ＥＤＩＳ（登録商標）、ＡＰＡＣＨＥ　ＣＡＳＳＡＮＤＲＡ（登録商標）、ＡＰＡＣＨＥ（登録商標）からのＨＢａｓｅ、ＭａｐＲ－ＤＢ、又はあらゆる他の適切なデータベース製品が挙げられる。その上、データベースは、例えばデータ・テーブル又はルックアップ・テーブルとして、あらゆる適切な様式で編成することができる。各レコードは、単一ファイル、一連のファイル、リンクされた一連のデータ・フィールド、又はあらゆる他のデータ構造であり得る。

【００８６】

一定のデータの関連付けは、当分野で既知又は実用化されるもののような、あらゆる所望のデータ関連付け手法を通じて実現することができる。例えば、関連付けは、手動又は自動のいずれでも実現することができる。自動の関連付け手法としては、例えばデータベース検索、データベースのマージ、ＧＲＥＰ、ＡＧＲＥＰ、ＳＱＬ、検索を高速化するためにテーブルでキー・フィールドを使用すること、すべてのテーブル及びファイルを通る順次検索、ルックアップを簡略化するために既知の順序にしたがってファイル内でレコードをソートすることなどを挙げることができる。関連付けステップは、データベースのマージ機能によって実現することができ、例えば予め選択されたデータベース又はデータ・セクタ内で「キー・フィールド」を使用する。様々なデータベース・チューニングのステップが、データベースのパフォーマンスを最適化するために企図される。例えば、インデックスなどの頻繁に使用されるファイルは、ｉｎ／Ｏｕｔ（「Ｉ／Ｏ」）ボトルネックを低減するために別個のファイル・システムに配置される場合がある。

【００８７】

より詳細には、「キー・フィールド」は、そのキー・フィールドによって定義されるオブジェクトの高次クラスにしたがってデータベースを分割する。例えば、特定のタイプのデータは、複数の関連データ・テーブル内でキー・フィールドとして指定することができ、次いでデータ・テーブルはキー・フィールド内のデータのタイプに基づいてリンクされる場合がある。リンク済データ・テーブルのそれぞれにおけるキー・フィールドに対応するデータは、同一であるか、又は同一のタイプのデータであることが好ましい。しかしながら、キー・フィールドにおいて類似しているが同一ではないデータを有するデータ・テーブルは、例えばＡＧＲＥＰを用いてリンクすることもできる。一実施形態によると、あらゆる適切なデータ記憶技法を利用して、標準フォーマットを伴わずデータを記憶することができる。データ・セットは、あらゆる適切な技法を用いて記憶することができ、例えばＩＳＯ／ＩＥＣ７８１６－４ファイル構造を使用して個々のファイルを記憶すること；一つ又は複数のデータ・セットを含む一つ又は複数の基本ファイルを公開する専用ファイルが選択されるドメインを実装すること；階層的なファイル・システムを使用して個々のファイルに記憶されたデータ・セットを使用すること；単一ファイル内のレコードとして記憶されたデータ・セット（圧縮、ＳＱＬアクセス可能、一つ又は複数のキーでハッシュ化、数字、第１のタプルによるアルファベット順などを含む）；Ｂｉｎａｒｙ　Ｌａｒｇｅ　Ｏｂｊｅｃｔ（ＢＬＯＢ）；ＩＳＯ／ＩＥＣ７８１６－６データ要素を用いてエンコードされた未グループ化のデータ要素として記憶される；ＩＳＯ／ＩＥＣ８８２４及び８８２５におけるようにＩＳＯ／ＩＥＣ　Ａｂｓｔｒａｃｔ　Ｓｙｎｔａｘ　Ｎｏｔａｔｉｏｎ（ＡＳＮ．１）を用いてエンコードされた未グループ化のデータ要素として記憶される；及び／又はフラクタル圧縮法、画像圧縮法などを含む可能性がある他のプロプライエタリな技法を挙げることができる。

【００８８】

様々な実施形態において、異なるフォーマットの多様な情報を記憶する機能は、情報をＢＬＯＢとして記憶することにより容易になる。そのため、あらゆるバイナリ情報をデータ・セットに関連付けられた記憶空間に記憶することができる。上で議論したように、バイナリ情報は、システムに関連付けられて記憶することができ、又はシステムと連携しているが外部にあってもよい。ＢＬＯＢの方法は、データ・セットを、固定記憶割り当て、環状キュー技法、又はメモリ管理に関するベスト・プラクティス（例えば、メモリのページング、ｌｅａｓｔ　ｒｅｃｅｎｔｌｙ　ｕｓｅｄなど）のうちのいずれかを用いる固定メ

モリ・オフセットによりバイナリのブロックとしてフォーマットされた未グループ化のデータ要素として記憶することができる。ＢＬＯＢ方法を用いることにより、異なるフォーマットを有する様々なデータ・セットを記憶する機能は、データ・セットの複数且つ関連性のない所有者による、データベースにおける、又はシステムに関連付けられるデータの記憶を容易にする。例えば、記憶され得る第１のデータ・セットは第１のパーティによって提供される可能性があり、記憶され得る第２のデータ・セットは関連性のない第２のパーティによって提供される可能性があり、更に記憶され得る第３のデータ・セットは第１のパーティ及び第２のパーティと関連性のない第３のパーティによって提供される可能性がある。これら三つの例示的なデータ・セットのそれぞれは、異なるデータ記憶フォーマット及び／又は技法を用いて記憶される異なる情報を含む可能性がある。更には、それぞれのデータ・セットは、データの部分集合を含む可能性があり、データの部分集合はやはり他の部分集合とは異なっている可能性がある。

【００８９】

上述のように、様々な実施形態において、データは共通フォーマットとは無関係に記憶することができる。しかしながら、データ・セット（例えば、ＢＬＯＢ）は、データベース又はシステムにおけるデータの操作のために与えられる際、標準様式で注釈がつけられる場合がある。注釈には、短いヘッダ、トレイラ、又は様々なデータ・セットを管理するのに有用な情報を伝達するように構成された各データ・セットに関連する他の適当なインジケータが含まれ得る。例えば、注釈は本明細書では「条件ヘッダ」、「ヘッダ」、「トレイラ」、又は「ステータス」と呼ばれることがあり、データ・セットのステータスの指標を含むことができるか、又は具体的な発行者若しくはデータの所有者に相関する識別子を含む場合がある。一例では、それぞれのデータ・セットＢＬＯＢの最初の３バイトは、その特定のデータ・セットのステータス、例えば、ＬＯＡＤＥＤ、ＩＮＩＴＩＡＬＩＺＥＤ、ＲＥＡＤＹ、ＢＬＯＣＫＥＤ、ＲＥＭＯＶＡＢＬＥ、又はＤＥＬＥＴＥＤを示すように構成することができる、又は構成可能である。データの後続のバイトは、例えば、発行者の身元、ユーザ、取引／メンバーシップ口座識別子などを示すために使用することができる。これらの条件注釈のそれぞれを、本明細書において更に議論する。

【００９０】

データ・セット注釈は、他のタイプのステータス情報のため、並びに様々な他の目的のために使用することもできる。例えば、データ・セット注釈は、アクセス・レベルを定めるセキュリティ情報を含む場合がある。アクセス・レベルは、例えば、特定の個人、従業員のクラス、会社、又は他の実体にのみデータ・セットへのアクセスを許可するように、或いは取引、販売者、発行者、又はユーザなどに基づいて具体的なデータ・セットへのアクセスを許可するように構成することができる。更には、セキュリティ情報は、データ・セットのアクセス、修正、及び／又は削除などの特定の行為のみ制限／許可する場合がある。一例では、データ・セットの注釈は、データ・セットの所有者又はユーザだけがデータ・セットを削除することを許可されること、様々な識別済ユーザがデータ・セットの読み取りのためにアクセスすることを許可され得ること、及びその他は完全にデータ・セットへのアクセスから除外されることを示す。しかしながら、他のアクセス制限パラメータを使用して様々な実体に、適宜様々なパーミッション・レベルでデータ・セットへのアクセスを許可することもできる。

【００９１】

ヘッダ又はトレイラを含むデータは、ヘッダ又はトレイラにしたがってデータを追加、削除、修正、又は強化するように構成されたスタンドアロン対話デバイスによって受信することができる。そのようにして、一実施形態では、ヘッダ又はトレイラは取引デバイスに関連付けられる発行者所有データと共に記憶されず、代わりにスタンドアロンのデバイスにおいて取るべき行為の適当な選択肢をユーザに提供することにより、適当な行為が取られる場合がある。システムは、データ記憶配置を企図することができ、データのヘッダ若しくはトレイラ、又はヘッダ若しくはトレイラ履歴は、適当なデータに関連して、システム、デバイス又は取引機器に記憶される。

【００９２】
当業者であれば、セキュリティ上の理由で、あらゆるデータベース、システム、デバイス、サーバ、又はシステムの他のコンポーネントは、一か所又は複数の場所において、あらゆるその組み合わせから構成され得、各データベース、又はシステムは、ファイアウォール、アクセス・コード、暗号化、復号化、圧縮、解凍などの様々な適切なセキュリティ特徴のいずれか含むことを更に諒解されよう。
【００９３】
暗号化は、現在当分野で利用可能な、又は利用可能になる可能性がある技法のうちのいずれかを用いて実施することができる。例えば、Ｔｗｏｆｉｓｈ、ＲＳＡ、エルガマル、ショア署名、ＤＳＡ、ＰＧＰ、ＰＫＩ、ＧＰＧ（ＧｎｕＰＧ）、ＨＰＥフォーマット保持暗号化（ＦＰＥ）、Ｖｏｌｔａｇｅ、並びに対称及び非対称暗号化システムなどである。システム及び方法は、ＳＨＡ系暗号化法、並びにＥＣＣ（楕円曲線暗号化法）、及び開発中の他の量子可読暗号化アルゴリズムを組み込む場合もある。
【００９４】
ウェブ・クライアントのコンピューティング・ユニットは、標準のダイヤルアップ、ケーブル、ＤＳＬ、又は当分野で既知のあらゆる他のインターネット・プロトコルを使用して、インターネット又はイントラネットに接続されたインターネット・ブラウザを更に備える場合がある。ウェブ・クライアントから始まる取引は、他のネットワークのユーザからの認可されないアクセスを防ぐために、ファイアウォールを通過する場合がある。更には、更にセキュリティを高めるために、追加的なファイアウォールを、ＣＭＳの多様な構成要素の間に展開することができる。
【００９５】
ファイアウォールは、ＣＭＳコンポーネント及び／又は企業用コンピューティング・リソースを他のネットワークのユーザから保護するように適切に構成されたあらゆるハードウェア及び／又はソフトウェアを含むことができる。更には、ファイアウォールは、ファイアウォールの内側で、ウェブ・サーバを通じて接続するウェブ・クライアントについて、様々なシステム及びコンポーネントへのアクセスを限定又は制限するように構成することができる。ファイアウォールは、ステートフル・インスペクション、プロキシベース、アクセス制御リスト、及びとりわけパケット・フィルタリングを含む様々な構成で存在する場合がある。ファイアウォールは、ウェブ・サーバ又はあらゆる他のＣＭＳコンポーネント内に一体化されてもよく、或いは別個の実体として更に存在することもできる。ファイアウォールは、ネットワーク・アドレス変換（「ＮＡＴ」）及び／又はネットワーク・アドレス・ポート変換（「ＮＡＰＴ」）を実装することができる。ファイアウォールは、様々なトンネリング・プロトコルに対応して、仮想プライベート・ネットワーキングで使用される通信のようなセキュアな通信を容易にすることができる。ファイアウォールは、非武装地帯（「ＤＭＺ」）を実装して、インターネットなどのパブリックなネットワークとの通信を容易にすることができる。ファイアウォールは、インターネット・サーバ、あらゆる他のアプリケーション・サーバ・コンポーネント内にソフトウェアとして一体化されてもよく、又は別のコンピューティング・デバイス内で存在してもよく、又はスタンドアロンのハードウェア・コンポーネントの形態を取ることもできる。
【００９６】
本明細書において議論されるコンピュータは、ユーザからアクセス可能な、適切なウェブサイト又は他のインターネットベースのグラフィカル・ユーザ・インターフェースを提供することができる。一実施形態では、ＭＩＣＲＯＳＯＦＴ（登録商標） ＩＮＴＥＲＮＥＴ ＩＮＦＯＲＭＡＴＩＯＮ ＳＥＲＶＩＣＥＳ（登録商標）（ＩＩＳ）、ＭＩＣＲＯＳＯＦＴ（登録商標） Ｔｒａｎｓａｃｔｉｏｎ Ｓｅｒｖｅｒ（ＭＴＳ）、及びＭＩＣＲＯＳＯＦＴ（登録商標） ＳＱＬ Ｓｅｒｖｅｒは、ＭＩＣＲＯＳＯＦＴ（登録商標）オペレーティング・システム、ＭＩＣＲＯＳＯＦＴ（登録商標）ＮＴ ウェブ・サーバ・ソフトウェア、ＭＩＣＲＯＳＯＦＴ（登録商標） ＳＱＬ Ｓｅｒｖｅｒのデータベース・システム、及びＭＩＣＲＯＳＯＦＴ（登録商標）Ｃｏｍｍｅｒｃｅ Ｓｅｒｖｅｒと併せて使用

される。追加的に、Ａｃｃｅｓｓ又はＭＩＣＲＯＳＯＦＴ（登録商標）ＳＱＬ Ｓｅｒｖｅｒ、ＯＲＡＣＬＥ（登録商標）、Ｓｙｂａｓｅ、Ｉｎｆｏｒｍｉｘ ＭｙＳＱＬ、Ｉｎｔｅｒｂａｓｅなどのコンポーネントを使用して、Ａｃｔｉｖｅ Ｄａｔａ Ｏｂｊｅｃｔ（ＡＤＯ）準拠のデータベース管理システムを提供することもできる。一実施形態では、Ａｐａｃｈｅウェブ・サーバは、Ｌｉｎｕｘオペレーティング・システム、ＭｙＳＱＬデータベース、並びにＰｅｒｌ、ＰＨＰ、Ｒｕｂｙ及び／又はＰｙｔｈｏｎプログラミング言語と併せて使用される。

【００９７】

本明細書において議論される通信、入力、ストレージ、データベース、又はディスプレイのいずれも、ウェブ・ページを有するウェブサイトを通じて容易にすることができる。本明細書において使用されるような用語「ウェブ・ページ」は、ユーザと対話するために使用され得る文書及びアプリケーションのタイプを限定するよう意図されていない。例えば、典型的なウェブサイトは、標準的なＨＴＭＬ文書に加えて、様々なフォーム、ＪＡＶＡ（登録商標）アプレット、ＪＡＶＡＳＣＲＩＰＴ（登録商標）、アクティブ・サーバ・ページ（ＡＳＰ）、コモン・ゲートウェイ・インターフェース（ＣＧＩ）スクリプト、拡張可能マークアップ言語（ＸＭＬ）、ダイナミックＨＴＭＬ、カスケード・スタイル・シート（ＣＳＳ）、ＡＪＡＸ（非同期ＪＡＶＡＳＣＲＩＰＴ（登録商標） Ａｎｄ ＸＭＬ）、ヘルパ・アプリケーション、プラグインなどを含む可能性がある。サーバは、ウェブ・サーバから要求を受信するウェブ・サービスを含む場合があり、要求にはＵＲＬ及びＩＰアドレス（例えば、１０．０．０．２）が含まれる。ウェブ・サーバは適当なウェブ・ページを検索し、そのウェブ・ページ用のデータ又はアプリケーションをそのＩＰアドレスに送信する。ウェブ・サービスは、インターネットなどの通信手段により他のアプリケーションと対話することができるアプリケーションである。ウェブ・サービスは、通常ＸＭＬ、ＳＯＡＰ、ＡＪＡＸ、ＷＳＤＬ及びＵＤＤＩなどの規格又はプロトコルに基づいている。ウェブ・サービス方法は、当分野で周知であり、多くの標準的なテキストでカバーされている。例えば、ｒｅｐｒｅｓｅｎｔａｔｉｏｎａｌ ｓｔａｔｅ ｔｒａｎｓｆｅｒ（ＲＥＳＴ）、すなわちＲＥＳＴｆｕｌなウェブ・サービスは、アプリケーション間の相互運用性を可能にする一方法を与えることができる。

【００９８】

ミドルウェアは、異なるコンピューティング・システム間での通信を容易にするように、及び／又は取引を処理するように適切に構成されたあらゆるハードウェア及び／又はソフトウェアを含む場合がある。ミドルウェア・コンポーネントは市販されており、当分野で既知である。ミドルウェアは市販のハードウェア及び／又はソフトウェアにより、カスタムのハードウェア及び／又はソフトウェアにより、或いはその組み合わせにより実装することができる。ミドルウェアは、様々な構成で存在することができ、スタンドアロンのシステムとして存在することができるか、又はインターネット・サーバ上に存在するソフトウェア・コンポーネントであってもよい。ミドルウェアは、本明細書において開示されるあらゆる目的のために、アプリケーション・サーバの様々なコンポーネントとあらゆる数の内部又は外部のシステムとの間での取引を処理するように構成することができる。市販のミドルウェア製品の例としては、ＩＢＭ（登録商標）Ｉｎｃ．（Ａｒｍｏｎｋ、ＮＹ）のＷＥＢＳＰＨＥＲＥ（登録商標）ＭＱＴＭ（以前のＭＱシリーズ）がある。ミドルウェアの別の例としては、Ｅｎｔｅｒｐｒｉｓｅ Ｓｅｒｖｉｃｅ Ｂｕｓ（「ＥＳＢ」）アプリケーションがある。

【００９９】

実務者であれば、ブラウザベースの文書内にデータを表示するためには複数の方法が存在することも諒解されたい。データは、標準的なテキストとして、又は固定リスト、スクロール可能リスト、ドロップダウン・リスト、編集可能テキスト・フィールド、固定テキスト・フィールド、ポップアップ・ウィンドウなどの内部で表現され得る。同様に、例えばキーボードを使用したフリー・テキスト入力、メニュ項目、チェック・ボックス、オプション・ボックスの選択など、ウェブ・ページ内のデータを修正するために使用可能な方

法が複数ある。
【０１００】
システム及び方法は、本明細書において、機能的なブロック・コンポーネント、スクリーン・ショット、任意選択の選択、及び様々な処理ステップの観点で説明することができる。そのような機能的なブロックは、指定された機能を実施するように構成された任意の数のハードウェア及び／又はソフトウェア・コンポーネントによって実現され得ることを諒解されたい。例えば、システムは、例えばメモリ素子、処理素子、論理素子、ルックアップ・テーブルなどの様々な集積回路コンポーネントを採用することができ、これらは一つ又は複数のマイクロプロセッサ或いは他の制御デバイスの制御の下、多様な機能を実行することができる。同様に、システムのソフトウェア要素は、データ構造、オブジェクト、処理、ルーチン、又は他のプログラミング要素のあらゆる組み合わせで実装される様々なアルゴリズムを用いたＣ、Ｃ＋＋、Ｃ＃、ＪＡＶＡ（登録商標）、ＪＡＶＡＳＣＲＩＰＴ、ＪＡＶＡＳＣＲＩＰＴ Ｏｂｊｅｃｔ Ｎｏｔａｔｉｏｎ（ＪＳＯＮ）、ＶＢＳｃｒｉｐｔ、Ｍａｃｒｏｍｅｄｉａ Ｃｏｌｄ Ｆｕｓｉｏｎ、ＣＯＢＯＬ、ＭＩＣＲＯＳＯＦＴ（登録商標）Ａｃｔｉｖｅ Ｓｅｒｖｅｒ Ｐａｇｅｓ、アセンブリ、ＰＥＲＬ、ＰＨＰ、ａｗｋ、Ｐｙｔｈｏｎ、Ｖｉｓｕａｌ Ｂａｓｉｃ、ＳＱＬストアドプロシージャ、ＰＬ／ＳＱＬ、あらゆるＵＮＩＸシェル・スクリプト、及び拡張可能マークアップ言語（ＸＭＬ）などの、あらゆるプログラミング言語又はスクリプト言語で実装することができる。更には、システムは、データ送信、シグナリング、データ処理、ネットワーク制御などについて、任意の数の従来技法を採用することができることに留意されたい。なお更には、システムは、ＪＡＶＡＳＣＲＩＰＴ、ＶＢＳｃｒｉｐｔなどのクライアントサイドのスクリプト言語を用いてセキュリティ問題を検出する又は防ぐために使用することができる。暗号化及びネットワーク・セキュリティの方法は、当分野でよく知られており、多くの標準的なテキストでカバーされている。
【０１０１】
様々な実施形態において、システムのソフトウェア要素は、ＮＯＤＥ．ｊｓ（登録商標）を使用して実装することもできる。ＮＯＤＥ．ｊｓ（登録商標）は、いくつかのモジュールを実装して様々なコアな機能性を扱うことができる。例えば、ＮＰＭ（登録商標）などのパッケージ管理モジュールを、オープン・ソース・ライブラリとして実装して、サード・パーティＮＯＤＥ．ｊｓ（登録商標）プログラムのインストール及び管理の統制を支援することができる。ＮＯＤＥ．ｊｓ（登録商標）は、例えばＰａｒａｌｌｅｌ Ｍｕｌｔｉｔｈｒｅａｄｅｄ Ｍａｃｈｉｎｅ（「ＰＭ２」）などのプロセス・マネージャ；例えばＮｏｄｅ Ａｐｐｌｉｃａｔｉｏｎ Ｍｅｔｒｉｃｓ（「ａｐｐｍｅｔｒｉｃｓ」）などのリソース及びパフォーマンス監視ツール；例えばＲｅａｃｈＪＳ（登録商標）などのユーザ・インターフェースをビルドするためのライブラリ・モジュール、並びに／又はあらゆる他の適切な及び／若しくは所望のモジュールを実装することもできる。
【０１０２】
当業者であれば諒解されるように、システムは、既存システムのカスタマイゼーション、アドオン製品、アップグレードしたソフトウェアを実行する処理装置、スタンドアロンのシステム、分散システム、方法、データ処理システム、データ処理用デバイス、及び／又はコンピュータ・プログラム製品として具体化することができる。したがって、システム又はモジュールのあらゆる部分は、コードを実行する処理装置、インターネットベースの実施形態、完全にハードウェアの実施形態、又はインターネット、ソフトウェア及びハードウェアの態様を組み合わせた実施形態の形態を取ることができる。更には、システムは、記憶媒体上に具体化されたコンピュータ可読プログラムコード手段を有するコンピュータ可読記憶媒体上のコンピュータ・プログラム製品の形態を取ることができる。ハード・ディスク、ＣＤ－ＲＯＭ、ＢＬＵ－ＲＡＹ、光学記憶装置、磁気記憶装置などを含む、あらゆる適切なコンピュータ可読記憶媒体を利用することができる。
【０１０３】
システム及び方法を、様々な実施形態による、方法、装置（例えば、システム）、及び

コンピュータ・プログラム製品の、スクリーン・ショット、ブロック図、及びフローチャート図を参照して、本明細書において説明する。ブロック図及びフローチャート図の各機能ブロック、並びにブロック図及びフローチャート図における機能ブロックの組み合わせは、それぞれコンピュータ・プログラム命令により実装することができることを理解されたい。

【０１０４】

次に図２～図５を参照すると、描かれている処理の流れ及びスクリーンショットは、単なる実施形態であり、本開示の範囲を限定することは意図されていない。例えば、方法又は処理の説明のいずれかにおいて述べられるステップは、あらゆる順序で実行されてもよく、提示された順序に限定されない。

【０１０５】

これらのコンピュータ・プログラム命令は、コンピュータ、又は他のプログラム可能データ処理装置で実行される命令が、フローチャートの一つ又は複数のブロックで指定される機能を実装するための手段を作出するべく、汎用コンピュータ、特殊目的コンピュータ、又は他のプログラム可能データ処理装置にロードされ、マシンを作り出すものであってよい。このようなコンピュータ・プログラム命令は、コンピュータ可読メモリに記憶された命令により、フローチャートの一つ又は複数のブロックで指定される機能を実装する命令手段を含んだ製造物品を作り出すべく、コンピュータ可読メモリに記憶され、コンピュータ、又は他のプログラム可能データ処理装置に特定の方式で機能するように指示するものであってもよい。コンピュータ・プログラム命令は、コンピュータ又は他のプログラム可能データ処理装置で実行される命令がフローチャートの一つ又は複数のブロックで指定される機能を実装するためのステップを提供するように、コンピュータ実装の処理を作出するべく、コンピュータ又は他のプログラム可能データ処理装置にロードされ、コンピュータ又は他のプログラム可能データ処理装置上で一連の動作ステップを実行させるものであってもよい。

【０１０６】

したがって、ブロック図及びフローチャート図の機能ブロックは、指定された機能を実施するための手段の組み合わせ、指定された機能を実施するためのステップの組み合わせ、及び指定された機能を実施するためのプログラム命令手段をサポートする。ブロック図及びフローチャート図の各機能ブロック、並びにブロック図及びフローチャート図における機能ブロックの組み合わせは、指定された機能若しくはステップを実行する特殊目的ハードウェアベースのコンピュータ・システム、又は特殊目的ハードウェアとコンピュータ命令との適切な組み合わせのいずれかによって実装可能であることも理解されたい。更には、処理の流れの図面、及びその説明は、ユーザのＷＩＮＤＯＷＳ（登録商標）、ウェブ・ページ、ウェブサイト、ウェブ・フォーム、プロンプトなどに言及する場合がある。実務者であれば、本明細書において説明される図示のステップは、ＷＩＮＤＯＷＳ（登録商標）、ウェブ・ページ、ウェブ・フォーム、ポップアップＷＩＮＤＯＷＳ（登録商標）、プロンプトなどの使用を含むあらゆる数の構成を含むことを諒解されよう。図示及び説明されるような複数のステップは、単一のウェブ・ページ及び／又はＷＩＮＤＯＷＳ（登録商標）に組み合わせることができるが、簡略のため分けたままであることを更に諒解されたい。他の場合では、単一の処理ステップとして図示及び説明されるステップは、複数のウェブ・ページ及び／又はＷＩＮＤＯＷＳ（登録商標）として別個にすることができるが、簡略のため組み合わせたままである。

【０１０７】

用語「非一時的な」は、伝搬する一時的な信号そのものだけを特許請求される範囲から除外するよう理解されるべきであり、一時的な信号そのものだけを伝搬しているのではないすべての標準的なコンピュータ可読媒体に対する権利を放棄するものではない。別の言い方をすると、用語「非一時的コンピュータ可読媒体」及び「非一時的コンピュータ可読記憶媒体」の意味は、米国特許法第１０１条の下、ナウテン判決で特許可能な対象の範囲外であると判明したタイプの一時的なコンピュータ可読媒体のみを除外するものと解釈さ

れるべきである。
【０１０８】
本明細書において、恩恵、他の利点、及び問題に対する解決策を具体的な実施形態に関して説明した。しかしながら、恩恵、利点、問題に対する解決策、及びあらゆる恩恵、利点、又は解決策を、生じ得る又はより顕著にさせ得るあらゆる要素は、本開示の重要な、要求される、又は必須の特徴若しくは要素として解釈されるべきではない。したがって、本開示の範囲は、何よりも添付の特許請求の範囲によって限定されるべきであり、添付の特許請求の範囲では単数形での要素への言及は、明示的に述べられない限り「一つ、且つ一つだけ」を意味することを意図されるのではなく、むしろ「一つ又は複数」を意味することを意図される。その上、「Ａ、Ｂ、及びＣのうちの少なくとも一つ」又は「Ａ、Ｂ、又はＣのうちの少なくとも一つ」に類似した言い回しが請求項又は明細書で使用される場合、この言い回しは、実施形態にはＡだけが存在し得る、実施形態にはＢだけが存在し得る、実施形態にはＣだけが存在し得る、或いは単一の実施形態に要素Ａ、Ｂ、及びＣの任意の組み合わせ、例えばＡとＢ、ＡとＣ、ＢとＣ、又はＡとＢとＣとが存在し得ることを意味するものと解釈されるよう意図される。本開示は方法を含むが、磁気若しくは光学メモリ又は磁気若しくは光学ディスクなどの有形のコンピュータ可読キャリア上でコンピュータ・プログラム命令として具体化され得ることが企図される。
【０１０９】
その上、デバイス又は方法は、本特許請求の範囲によって包含されるため、本開示によって解決しようとするそれぞれ及びすべての問題に対処する必要はない。更には、要素、コンポーネント、又は方法ステップが特許請求の範囲に明示的に記載されているかどうかにかかわらず、本開示におけるどの要素、コンポーネント、又は方法ステップも、一般公衆に捧げることを意図されていない。本明細書で使用される際、用語「を含む」、「を含んでいる」、又はそのあらゆる他の変形は、非排他的な包含をカバーするよう意図されており、それにより要素の列挙を含むプロセス、方法、物品、又は装置は、それらの要素だけを含むのではなく、明示的に列挙されなかった他の要素、又はそのようなプロセス、方法、物品、若しくは装置に固有な他の要素を含むことができる。
【０１１０】
様々な実施形態の例を、以下の段落で説明する。以下の実施形態は、様々な例の実装形態を例示することを意図されているが、本開示の可能な実施形態のみを特定するものではない。本開示の他の実施形態もまた、例示的な目的で与えられる実施形態の範囲外の係属出願により包含される。
【０１１１】
実施形態１－１
支払い処理中、販売者システムによって呼び出されたことに応じて、ゼロ知識証明（ＺＫＰ）スマート・コントラクトによって、検証関数を実行することであって、販売者システムは、証明、顧客ハッシュ、販売者ハッシュ、及び購入金額をＺＫＰスマート・コントラクトに送信することによってＺＫＰスマート・コントラクトを呼び出し、検証関数は、検証鍵、証明、及び顧客ハッシュを、検証関数に入力することによって実行され、検証関数は、ゼロ知識証明アルゴリズムに関連付けられる、実行することと、検証関数が成功したことに応じて、ＺＫＰスマート・コントラクトによって、顧客ハッシュに関連付けられた顧客口座残高を調整することであって、顧客口座残高は、購入金額に基づいて調整され、顧客口座残高は、ブロックチェーン上で維持される、調整することと、ＺＫＰスマート・コントラクトによって、販売者ハッシュに関連付けられた販売者口座残高を調整することであって、販売者口座残高は、購入金額に基づいて調整され、販売者口座残高は、ブロックチェーン上で維持される、調整することと、ＺＫＰスマート・コントラクトによって、成功通知をブロックチェーンに書き込むことであって、成功通知は、支払い処理が正常に完了したことを示すデータを含む、書き込むこととを含む、方法。
【０１１２】
実施形態２

販売者システムが、顧客デバイスから証明及び顧客ハッシュを受信したことに応じて、ＺＫＰスマート・コントラクトを呼び出し、顧客デバイスが、ゼロ知識証明アルゴリズムに関連付けられた証明関数を実行することによって、証明を生成し、証明関数が、証明鍵、顧客ハッシュ、及び支払いハッシュを証明アルゴリズムに入力することによって、実行される、実施形態１に記載の方法。

【０１１３】

実施形態３

顧客デバイスが、支払い購入を販売者システムで開始したことに応じて、証明を生成し、支払いハッシュが、顧客識別データ及び顧客ナンスをハッシュ化アルゴリズムに入力することによって、生成される、実施形態２に記載の方法。

【０１１４】

実施形態４

発行者システムが、ゼロ知識証明アルゴリズムを作成し、ゼロ知識証明アルゴリズムが、鍵生成関数、証明関数、及び検証関数を含み、発行者システムが、鍵生成関数を実行することによって、証明鍵及び検証鍵を生成し、鍵生成関数が、乱数を鍵生成関数に入力することによって、実行され、発行者システムが、検証関数を含むようにＺＫＰスマート・コントラクトを生成する、実施形態１乃至３のいずれか一項に記載の方法。

【０１１５】

実施形態５

発行者システムが、販売者システムから販売者登録要求を受信したことに応じて、販売者ハッシュを生成し、販売者ハッシュが、販売者識別データ及び販売者ナンスをハッシュ化アルゴリズムに入力することによって、生成される、実施形態１乃至４のいずれか一項に記載の方法。

【０１１６】

実施形態６

ＺＫＰスマート・コントラクトによって、販売者ハッシュ及び販売者口座残高をブロックチェーンに書き込むことであって、ＺＫＰスマート・コントラクトが書き込みを完了したことに応じて、発行者システムが、販売者ハッシュ及び販売者ナンスを販売者システムに送信する、書き込むことを更に含む、実施形態５に記載の方法。

【０１１７】

実施形態７

発行者システムが、顧客デバイスから顧客登録要求を受信したことに応じて、顧客ハッシュを生成し、顧客ハッシュが、顧客識別データ及び顧客ナンスをハッシュ化アルゴリズムに入力することによって、生成される、実施形態１乃至６のいずれか一項に記載の方法。

【０１１８】

実施形態８

ＺＫＰスマート・コントラクトによって、顧客ハッシュ及び顧客口座残高をブロックチェーンに書き込むことであって、ＺＫＰスマート・コントラクトが書き込みを完了したことに応じて、発行者システムが、顧客ハッシュ及び顧客ナンスを顧客デバイスに送信する、書き込むことを更に含む、実施形態７に記載の方法。

【０１１９】

実施形態９

プロセッサと、プロセッサと通信するように構成された有形の非一時的メモリとを備える、コンピュータ・ベースのシステムであって、有形の非一時的メモリには命令が記憶されており、命令は、プロセッサによって実行されたことに応じて、ゼロ知識証明（ＺＫＰ）スマート・コントラクトに、支払い処理中、販売者システムによって呼び出されたことに応じて、ＺＫＰスマート・コントラクトによって、検証関数を実行することであって、販売者システムは、証明、顧客ハッシュ、販売者ハッシュ、及び購入金額をＺＫＰスマート・コントラクトに送信することによってＺＫＰスマート・コントラクトを呼び出すように構成され、検証関数は、検証鍵、証明、及び顧客ハッシュを、検証関数に入力すること

によって実行されるように構成され、検証関数は、ゼロ知識証明アルゴリズムに関連付けられる、実行することと、検証関数が成功したことに応じて、ＺＫＰスマート・コントラクトによって、顧客ハッシュに関連付けられた顧客口座残高を調整することであって、顧客口座残高は、購入金額に基づいて調整され、顧客口座残高は、ブロックチェーン上で維持される、調整することと、ＺＫＰスマート・コントラクトによって、販売者ハッシュに関連付けられた販売者口座残高を調整することであって、販売者口座残高は、購入金額に基づいて調整され、販売者口座残高は、ブロックチェーン上で維持される、調整することと、ＺＫＰスマート・コントラクトによって、成功通知をブロックチェーンに書き込むことであって、成功通知は、支払い処理が正常に完了したことを示すデータを含む、書き込むこととを含む動作を実行させる、コンピュータ・ベースのシステム。

【０１２０】

実施形態１０

販売者システムが、顧客デバイスから証明及び顧客ハッシュを受信したことに応じて、ＺＫＰスマート・コントラクトを呼び出すように構成され、顧客デバイスが、ゼロ知識証明アルゴリズムに関連付けられた証明関数を実行することによって、証明を生成するように構成され、証明関数が、証明鍵、顧客ハッシュ、及び支払いハッシュを証明アルゴリズムに入力することによって、実行されるように構成される、実施形態９に記載のコンピュータ・ベースのシステム。

【０１２１】

実施形態１１

顧客デバイスが、支払い購入を販売者システムで開始したことに応じて、証明を生成するように構成され、支払いハッシュが、顧客識別データ及び顧客ナンスをハッシュ化アルゴリズムに入力することによって、生成される、実施形態１０に記載のコンピュータ・ベースのシステム。

【０１２２】

実施形態１２

発行者システムが、ゼロ知識証明アルゴリズムを作成するように構成され、ゼロ知識証明アルゴリズムが、鍵生成関数、証明関数、及び検証関数を含み、発行者システムが、鍵生成関数を実行することによって、証明鍵及び検証鍵を生成するように構成され、鍵生成関数が、乱数を鍵生成関数に入力することによって、実行されるように構成され、発行者システムが、検証関数を含むようにＺＫＰスマート・コントラクトを生成するように構成される、実施形態９乃至１１のいずれか一項に記載のコンピュータ・ベースのシステム。

【０１２３】

実施形態１３

発行者システムが、販売者システムから販売者登録要求を受信したことに応じて、販売者ハッシュを生成するように構成され、販売者ハッシュが、販売者識別データ及び販売者ナンスをハッシュ化アルゴリズムに入力することによって、生成される、実施形態９乃至１２のいずれか一項に記載のコンピュータ・ベースのシステム。

【０１２４】

実施形態１４

ＺＫＰスマート・コントラクトによって、販売者ハッシュ及び販売者口座残高をブロックチェーンに書き込むことであって、ＺＫＰスマート・コントラクトが書き込みを完了したことに応じて、発行者システムが、販売者ハッシュ及び販売者ナンスを販売者システムに送信するように構成される、書き込むことを更に含む、実施形態１３に記載のコンピュータ・ベースのシステム。

【０１２５】

実施形態１５

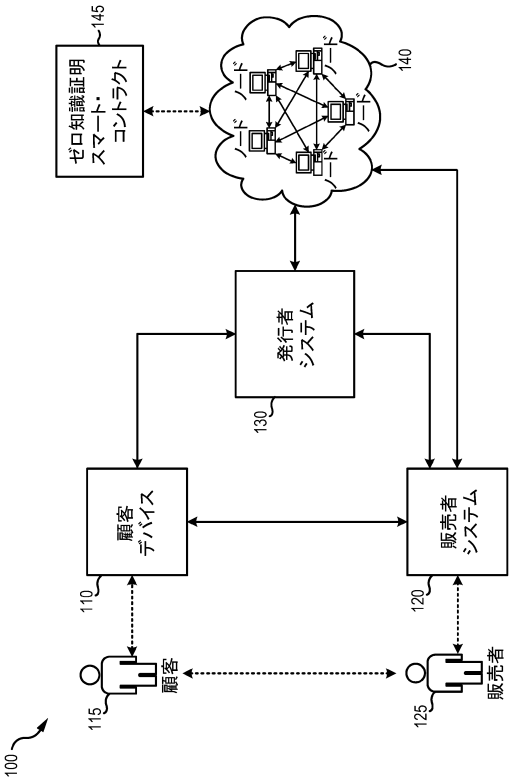
発行者システムが、顧客デバイスから顧客登録要求を受信したことに応じて、顧客ハッシュを生成するように構成され、顧客ハッシュが、顧客識別データ及び顧客ナンスをハッシュ化アルゴリズムに入力することによって、生成される、実施形態９乃至１４のいずれ

か一項に記載のコンピュータ・ベースのシステム。
【０１２６】
実施形態１６
ＺＫＰスマート・コントラクトによって、顧客ハッシュ及び顧客口座残高をブロックチェーンに書き込むことであって、ＺＫＰスマート・コントラクトが書き込みを完了したことに応じて、発行者システムが、顧客ハッシュ及び顧客ナンスを顧客デバイスに送信する、書き込むことを更に含む、実施形態１５に記載のコンピュータ・ベースのシステム。
【０１２７】
実施形態１７
命令が記憶された非一時的な有形のコンピュータ可読記憶媒体を含む製造物品であって、命令は、コンピュータ・ベースのシステムによって実行されることに応じて、ゼロ知識証明（ＺＫＰ）スマート・コントラクトに、支払い処理中、販売者システムによって呼び出されたことに応じて、ＺＫＰスマート・コントラクトによって、検証関数を実行することであって、販売者システムは、証明、顧客ハッシュ、販売者ハッシュ、及び購入金額をＺＫＰスマート・コントラクトに送信することによってＺＫＰスマート・コントラクトを呼び出すように構成され、検証関数は、検証鍵、証明、及び顧客ハッシュを、検証関数に入力することによって実行されるように構成され、検証関数は、ゼロ知識証明アルゴリズムに関連付けられる、実行することと、検証関数が成功したことに応じて、ＺＫＰスマート・コントラクトによって、顧客ハッシュに関連付けられた顧客口座残高を調整することであって、顧客口座残高は、購入金額に基づいて調整され、顧客口座残高は、ブロックチェーン上で維持される、調整することと、ＺＫＰスマート・コントラクトによって、販売者ハッシュに関連付けられた販売者口座残高を調整することであって、販売者口座残高は、購入金額に基づいて調整され、販売者口座残高は、ブロックチェーン上で維持される、調整することと、ＺＫＰスマート・コントラクトによって、成功通知をブロックチェーンに書き込むことであって、成功通知は、支払い処理が正常に完了したことを示すデータを含む、書き込むこととを含む動作を実行させる、製造物品。
【０１２８】
実施形態１８
販売者システムが、顧客デバイスから証明及び顧客ハッシュを受信したことに応じて、ＺＫＰスマート・コントラクトを呼び出すように構成され、顧客デバイスが、ゼロ知識証明アルゴリズムに関連付けられた証明関数を実行することによって、証明を生成するように構成され、証明関数が、証明鍵、顧客ハッシュ、及び支払いハッシュを証明アルゴリズムに入力することによって、実行されるように構成され、顧客デバイスが、支払い購入を販売者システムで開始したことに応じて、証明を生成するように構成され、支払いハッシュが、顧客識別データ及び顧客ナンスをハッシュ化アルゴリズムに入力することによって、生成される、実施形態１７に記載の製造物品。
【０１２９】
実施形態１９
発行者システムが、ゼロ知識証明アルゴリズムを作成するように構成され、ゼロ知識証明アルゴリズムが、鍵生成関数、証明関数、及び検証関数を含み、発行者システムが、鍵生成関数を実行することによって、証明鍵及び検証鍵を生成するように構成され、鍵生成関数が、乱数を鍵生成関数に入力することによって、実行されるように構成され、発行者システムが、検証関数を含むようにＺＫＰスマート・コントラクトを生成するように構成される、実施形態１７又は１８に記載の製造物品。
【０１３０】
実施形態２０
発行者システムが、販売者システムから販売者登録要求を受信したことに応じて、販売者ハッシュを生成するように構成され、販売者ハッシュが、販売者識別データ及び販売者ナンスをハッシュ化アルゴリズムに入力することによって生成され、発行者システムが、顧客デバイスから顧客登録要求を受信したことに応じて、顧客ハッシュを生成するように

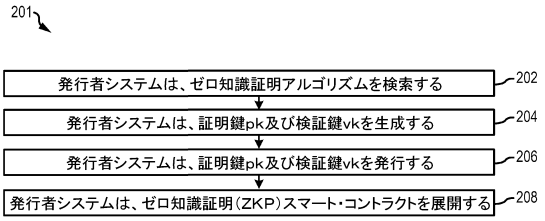
構成され、顧客ハッシュが、顧客識別データ及び顧客ナンスをハッシュ化アルゴリズムに入力することによって、生成される、実施形態１７乃至１９のいずれか一項に記載の製造物品。

【図面】

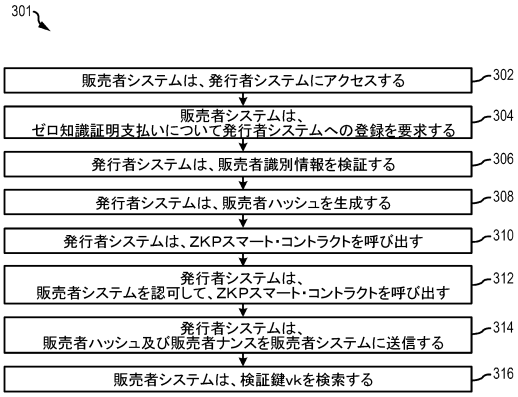
【図１】



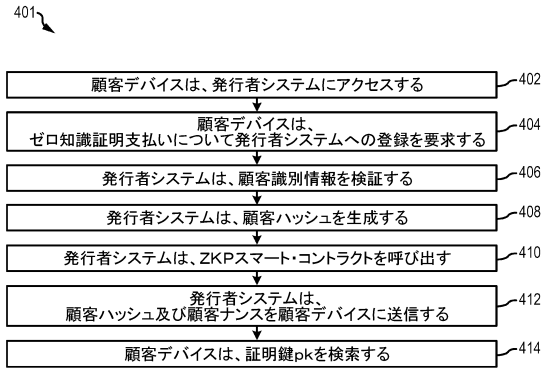
【図２】



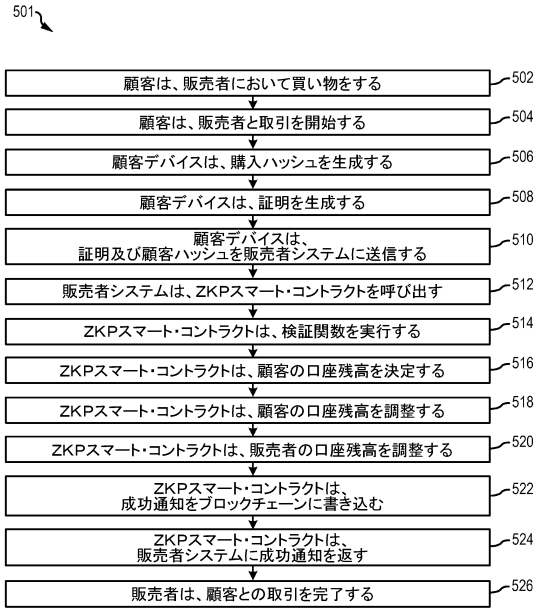
【図３】



【図４】



【図５】


501
顧客は、販売者において買い物をする
502
顧客は、販売者と取引を開始する
504
顧客デバイスは、購入ハッシュを生成する
506
顧客デバイスは、証明を生成する
508
顧客デバイスは、
証明及び顧客ハッシュを販売者システムに送信する
510
販売者システムは、ZKPスマート・コントラクトを呼び出す
512
ZKPスマート・コントラクトは、検証関数を実行する
514
ZKPスマート・コントラクトは、顧客の口座残高を決定する
516
ZKPスマート・コントラクトは、顧客の口座残高を調整する
518
ZKPスマート・コントラクトは、販売者の口座残高を調整する
520
ZKPスマート・コントラクトは、
成功通知をブロックチェーンに書き込む
522
ZKPスマート・コントラクトは、
販売者システムに成功通知を返す
524
販売者は、顧客との取引を完了する
526

フロントページの続き

(72)発明者　フェレンツィ， アンドラス エル．
アメリカ合衆国 １０２８５－４９００ ニューヨーク州、ニューヨーク、ヴィージー ストリート ２００、アメリカン エキスプレス トラヴェル リレイテッド サーヴィシーズ カンパニー， インコーポレイテッド 内
(72)発明者　ゲイル， ダラス エル．
アメリカ合衆国 １０２８５－４９００ ニューヨーク州、ニューヨーク、ヴィージー ストリート ２００、アメリカン エキスプレス トラヴェル リレイテッド サーヴィシーズ カンパニー， インコーポレイテッド 内
(72)発明者　ジャドハヴ， ニーレシュ ワイ．
アメリカ合衆国 １０２８５－４９００ ニューヨーク州、ニューヨーク、ヴィージー ストリート ２００、アメリカン エキスプレス トラヴェル リレイテッド サーヴィシーズ カンパニー， インコーポレイテッド 内
(72)発明者　ナーイク， ハリッシュ アール．
アメリカ合衆国 １０２８５－４９００ ニューヨーク州、ニューヨーク、ヴィージー ストリート ２００、アメリカン エキスプレス トラヴェル リレイテッド サーヴィシーズ カンパニー， インコーポレイテッド 内

審査官　行田 悦資

(56)参考文献
米国特許出願公開第２０１８／００８３７８０（ＵＳ，Ａ１）
米国特許出願公開第２０１６／０２５３６６３（ＵＳ，Ａ１）
特開２０１８－００７１６８（ＪＰ，Ａ）
米国特許出願公開第２０１８／０１０１６８４（ＵＳ，Ａ１）
安坂 祐紀 ほか，プライバシーを考慮したブロックチェーンの取引者間事前合意プロトコル，コンピュータセキュリティシンポジウム２０１８論文集 ，日本，一般社団法人情報処理学会，2018年10月15日，Vol.2018, No.2，pp.850-856
NARAYANAN, A. et al.，仮想通貨の教科書，第1版，日本，日経ＢＰ社，2016年12月09日，pp.276-288
宇根 正志，暗号資産における取引の追跡困難性と匿名性：研究動向と課題，金融研究所ディスカッション・ペーパー・シリーズ，日本，日本銀行，2018年12月06日，No.2018-J-20，pp.1-25

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｇ０６Ｑ　２０／３８