

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7463543号
(P7463543)

(45)発行日 令和6年4月8日(2024.4.8)

(24)登録日 令和6年3月29日(2024.3.29)

(51)国際特許分類

F I

G 0 6 Q 20/20 (2012.01)

G 0 6 Q 20/20 3 3 0

G 0 6 Q 20/38 (2012.01)

G 0 6 Q 20/38

請求項の数 15 (全16頁)

(21)出願番号	特願2022-556180(P2022-556180)	(73)特許権者	500041363
(86)(22)出願日	令和3年3月19日(2021.3.19)		マスターカード インターナショナル イ
(65)公表番号	特表2023-518760(P2023-518760		ンコーポレイテッド
	A)		アメリカ合衆国ニューヨーク州 パーチ
(43)公表日	令和5年5月8日(2023.5.8)		エイス パーチエイス ストリート 2 0
(86)国際出願番号	PCT/US2021/023071		0 0
(87)国際公開番号	WO2021/188853	(74)代理人	100147485
(87)国際公開日	令和3年9月23日(2021.9.23)		弁理士 杉村 憲司
審査請求日	令和4年10月31日(2022.10.31)	(74)代理人	230118913
(31)優先権主張番号	62/992,842		弁護士 杉村 光嗣
(32)優先日	令和2年3月20日(2020.3.20)	(74)代理人	100224683
(33)優先権主張国・地域又は機関	米国(US)		弁理士 齋藤 詩織
		(72)発明者	ラケッシュ ヤダフ
			アメリカ合衆国 メイン州 0 4 1 0 7
			ケーブ エリザベス ペンウッド サークル
			最終頁に続く

(54)【発明の名称】 物理的カードとの間でデジタルトークンを転送するための方法及びシステム

(57)【特許請求の範囲】

【請求項 1】

物理的決済カードとの間でデジタルトークンを転送するための処理サーバによって使用される方法であって、前記方法は、
前記処理サーバの記憶部上に、中央銀行から発行された複数のデジタルトークンを格納することと、
通信ネットワークを介して前記処理サーバから、前記複数のデジタルトークンを前記物理的決済カードに転送することと、
前記複数のデジタルトークンを前記物理的決済カードに前記転送することについて、前記中央銀行から発行された前記複数のデジタルトークンに関連付けられたトークンプロフィールを格納するブロックチェーンネットワークと通信することと、
前記ブロックチェーンネットワーク内に、前記処理サーバとの間のデジタルトークンの各転送を記録することと、を含む、方法。

【請求項 2】

請求項 1 に記載の方法において、
前記物理的決済カード上の前記複数のデジタルトークンについて、デジタル署名と暗号鍵とを含むこと、
を含む、方法。

【請求項 3】

請求項 2 に記載の方法において、

販売時点情報管理（POS）での前記物理的決済カードの提示の際に、前記デジタル署名と前記暗号鍵とを検証すること、
を含む、方法。

【請求項 4】

請求項 1 に記載の方法において、

販売時点情報管理（POS）への前記物理的決済カードの提示の際に、前記複数のデジタルトークンからデジタルトークンを差し引くこと、
を含む、方法。

【請求項 5】

請求項 1 に記載の方法において、

現金自動支払い機（ATM）を介して、前記物理的決済カードに、前記複数のデジタルトークンをアップロードすること、
を含む、方法。

【請求項 6】

請求項 1 に記載の方法において、前記処理サーバは、発行体に関連付けられる、方法。

【請求項 7】

請求項 1 に記載の方法において、前記物理的決済カードは、個々のデジタルトークンを有する EMV カードである、方法。

【請求項 8】

物理的決済カードとの間でデジタルトークンを転送するためのシステムであって、前記システムは、処理サーバを含み、前記処理サーバは、

中央銀行から発行された複数のデジタルトークンを、記憶部に格納することと、
通信ネットワークを介して、前記物理的決済カードに前記複数のデジタルトークンを転送することと、

前記複数のデジタルトークンを前記物理的決済カードに前記転送することに続いて、前記中央銀行から発行された前記複数のデジタルトークンに関連付けられたトークンプロファイルを格納するブロックチェーンネットワークと通信することと、

前記ブロックチェーンネットワーク内に、前記処理サーバとの間のデジタルトークンの各転送を記録することと、

を実行するように構成される、システム。

【請求項 9】

請求項 8 に記載のシステムにおいて、

前記物理的決済カード上の前記複数のデジタルトークンについて、デジタル署名と暗号鍵とを含むこと、
を含む、システム。

【請求項 10】

請求項 9 に記載のシステムにおいて、販売時点情報管理（POS）での前記物理的決済カードの提示の際に、前記デジタル署名と前記暗号鍵とが検証される、システム。

【請求項 11】

請求項 8 に記載のシステムにおいて、販売時点情報管理（POS）への前記物理的決済カードの提示の際に、デジタルトークンが、前記複数のデジタルトークンから差し引かれる、システム。

【請求項 12】

請求項 8 に記載のシステムにおいて、前記複数のデジタルトークンは、現金自動支払い機（ATM）を介して、前記物理的決済カードにアップロードされる、システム。

【請求項 13】

請求項 8 に記載のシステムにおいて、前記処理サーバは、発行体に関連付けられる、システム。

【請求項 14】

請求項 8 に記載の方法において、前記物理的決済カードは、個々のデジタルトークンを

10

20

30

40

50

有する E M V カードである、方法。

【請求項 15】

請求項 4 に記載の方法において、

前記複数のデジタルトークンから前記デジタルトークンを差し引くことは、前記デジタルトークンが有効であると検証されると実行される、方法。

【発明の詳細な説明】

【関連出願の相互参照】

【0001】

本出願は、2020年3月20日に出願された米国仮特許出願第62/992,842号の利益を主張する。その仮出願の内容は、あらゆる目的のために参照により本明細書に組み込まれる。

10

【技術分野】

【0002】

本開示は、物理的決済カードとの間でデジタルトークンを転送するための方法及びシステムに関する。より具体的には、デジタルトークンを、中央銀行から物理的決済カードの1つ以上の保険会社(insurer)に転送するための方法及びシステムに関する。

【背景技術】

【0003】

決済手段は、例えば、クレジットカード、仮想決済カード、小切手などを含む。決済手段は、取引口座に対応する決済認証情報を用いて符号化される、決済認証情報を含む、又は決済認証情報に関連付けられることができる。決済認証情報は、関連した取引口座を介して資金供給される取引のために、取引処理の一部として通信しなければならない任意のデータを含むことができ、例えば、代表口座番号、有効期限、及びセキュリティコードである。

20

【0004】

販売時点情報管理(P O S)を用いて使用されることができるデジタルトークンを含む物理的決済カードを決済ネットワークが提供することを可能にする技術システムを有することが望ましい。

【発明の概要】

【0005】

本開示は、物理的決済カードとの間でデジタルトークンを転送するためのシステム及び方法の説明を提供する。

30

【0006】

物理的決済カードとの間でデジタルトークンを転送するための方法が開示される。本方法は、処理サーバ上で、中央銀行から発行された複数のデジタルトークンを受信することと、処理サーバから、複数のデジタルトークンを物理的決済カードに転送することとを含む。物理的決済カードは、P O Sを用いて使用されるように構成される。

【0007】

物理的決済カードとの間でデジタルトークンを転送するためのシステムが開示される。本システムは、処理サーバを含む。本処理サーバは、中央銀行から発行された複数のデジタルトークンを受信することと、複数のデジタルトークンを物理的決済カードに転送することとを実行するように構成される。物理的決済カードは、販売時点情報管理(P O S)を用いて使用されるように構成される。

40

【0008】

例示的な実施形態は、添付の図面と併せて読まれるとき、以下の詳細な説明から最も良く理解される。これらは例示的な実施形態であり、特許請求される発明はそれらに限定されないことが強調される。図面に含まれるのは、以下の図である。

【図面の簡単な説明】

【0009】

【図1】例示的な実施形態による、物理的決済カードとの間でデジタルトークンを転送するための高位レベルのシステムアーキテクチャを示すブロック図である。

50

【図 2】物理的決済カードとの間でデジタルトークンを転送するための図 1 の処理サーバを示すブロック図である。

【図 3】例示的な実施形態による、例示的な方法を示すフローチャートである。

【図 4】例示的な実施形態による、コンピュータシステムアーキテクチャを示すブロック図である。

【発明を実施するための形態】

【0010】

本開示のさらなる適用分野は、以下に提供される詳細な説明から明らかになるであろう。例示的な実施形態の詳細な説明は、例示の目的のみを意図するものであり、したがって、必ずしも本開示の範囲を限定することを意図するものではないことを理解されたい。

10

【0011】

用語集

ブロックチェーン - ブロックチェーンに基づく通貨又はネットワークのすべての取引の公開台帳。1つ以上のコンピューティング装置はブロックチェーンネットワークを含むことができ、これは、ブロックチェーン内のブロックの一部として取引を処理及び記録するように構成されることができる。ブロックが完成されると、ブロックは、ブロックチェーンに追加され、取引記録がそれにより更新される。多くの事例では、ブロックチェーンは、時系列順の取引の台帳とすることができる、又はブロックチェーンネットワークによる使用のために適し得る任意の他の順序で提示されることができる。ある構成では、ブロックチェーン内に記録された取引は、宛先アドレス及び通貨額を含むことができ、ブロックチェーンは、どのくらいの通貨が特定のアドレスに帰属可能であるかを記録する。ある事例では、ある取引は金融であり、他の取引は金融ではない、又は取引は、ソースアドレス、タイムスタンプなどの追加の若しくは異なる情報を含むかもしれない。ある実施形態では、ブロックチェーンは、さらに又は代替的に、操作者によるものでさえ、改竄及び修正に対して強化されたデータ記録の連続的に成長する一覧を維持する分散データベース内に配置される、又は配置される必要がある取引の形態として、ほぼ任意の種類のデータを含むことができる。ブロックチェーンは、プルーフオブワーク(proof of work)及び/又はそれに関連付けられた任意の他の適切な検証技術を通じてブロックチェーンネットワークによって確認及び検証されることができる。ある場合では、所与の取引に関するデータは、取引データに付加された取引の直接的に一部ではない追加のデータをさらに含むことができる。ある事例では、ブロックチェーンにそのようなデータを含めることは、取引を構成することができる。そのような事例では、ブロックチェーンは、特定のデジタル通貨、仮想通貨、不換通貨、又は他の種類の通貨に直接関連付けられないことがある。

20

30

【0012】

決済ネットワーク - 所与の期間中に、数千、数百万、さらには数十億の取引のために、現金代替物の使用を介して、金銭の移転のために使用されるシステム又はネットワーク。決済ネットワークは、様々な種類の取引について金銭の移転を処理するために、様々な異なるプロトコル及び手順を使用することができる。決済ネットワークを介して実行され得る取引は、製品又はサービスの購入、信用購入、デビット取引、資金振替、口座引き落としなどを含むことができる。決済ネットワークは、決済カード、信用状、小切手、取引口座などを含み得る現金代替物を介して取引を実行するように構成されることができる。決済ネットワークとして実行するように構成されたネットワーク又はシステムの例は、Mastercard (登録商標)、VISA (登録商標)、Discover (登録商標)、American Express (登録商標)、PayPal (登録商標) などによって動作されるものを含む。本明細書における用語「決済ネットワーク」の使用は、エンティティとしての決済ネットワークと、決済ネットワークを含む機器、ハードウェア、及びソフトウェアなどの物理的決済ネットワークとの両方を指すことができる。

40

【0013】

ペイメントレール - 決済取引の処理と、取引メッセージの通信と、決済ネットワークと所与の期間中に数千、数百万、さらには数十億の取引を処理する決済ネットワークに相互

50

接続された他のエンティティとの間の他の同様のデータの通信と、において使用される決済ネットワークに関連付けられたインフラストラクチャ。ペイメントレールは、決済ネットワークと、決済ネットワークと他の関連付けられたエンティティ（金融機関、ゲートウェイプロセッサなど）との間の相互接続と、を確立するために使用されるハードウェアから構成されることができる。また、ある事例では、ペイメントレールは、通信ハードウェアとペイメントレールを含む装置との特別なプログラムを介してなど、ソフトウェアによる影響を受け得る。例えば、ペイメントレールは、特別に構成されたコンピューティング装置を含むことができる。この装置は、取引メッセージの経路指定のために特別に構成される。この取引メッセージは、以下でより詳細に論じられるように、ペイメントレールを介して電子的に送信される、特別にフォーマットされたデータメッセージとすることができる。

10

【 0 0 1 4 】

第三者の供給者又は販売者 - 消費者又は別の販売者などの別のエンティティによる購入のために製品（例えば、商品及び／又はサービス）を提供するエンティティ。販売者は、消費者、小売業者、卸売業者、製造業者、又は当業者には明らかであるような、購入のための製品を提供し得る任意の他の種類のエンティティとすることができる。ある事例では、販売者は、購入のために提供される商品及び／又はサービスにおいて特別な知識を有することができる。他の事例では、販売者は、提供される製品においていかなる特別な知識を有さない、又は必要としないとすることができる。ある実施形態では、単一の取引に関するエンティティは、販売者と見なされることができる。ある事例では、本明細書において使用されるように、用語「販売者」は、販売者のエンティティの機器又は装置を指すことができる。

20

【 0 0 1 5 】

発行体 - 受益者のために信用状又は信用限度額を設定（例えば、開設）し、信用状又は信用限度額に指定された金額に対して、受益者が振り出した為替手形を受領するエンティティ。多くの事例では、発行体は、銀行、又は信用限度額を開設することを許可された他の金融機関とすることができる。ある事例では、受益者に信用限度額を拡大することができる任意のエンティティが発行体と見なされることができる。発行体によって開設された信用限度額は、決済口座の形態で表されてもよく、決済カードの使用を介して受益者によって引き出されてもよい。また、発行体は、デビット口座、プリペイド口座、電子財布口座、貯蓄口座、当座預金口座など、当業者に明らかであるような追加の種類の決済口座を消費者に提供することができ、デビットカード、プリペイドカード、現金自動支払い機カード、電子財布、小切手などのような、そのような口座にアクセスし、及び／又はそのような口座を利用するための物理的又は非物理的手段を消費者に提供することができる。

30

【 0 0 1 6 】

アクワイアラ(acquirer: 加盟店契約会社) - 販売者に代わって決済カード取引を処理することができるエンティティ。アクワイアラは、銀行、又は販売者に代わって決済カード取引を処理することを許可される他の金融機関とすることができる。多くの事例では、アクワイアラは、販売者を受益者とする信用限度額を開設することができる。アクワイアラは、消費者（これは、発行体によって提供される信用限度額に対する受益者であり得る）が、アクワイアラにより表される販売者と決済カードを介して取引を行う場合に、発行体と資金を交換することができる。

40

【 0 0 1 7 】

中央銀行 - 一般に、ある国家若しくは国家のグループ、又は他の資産及び他のグループ（例えば、不換通貨、暗号通貨、人々のグループによって使用される他の物理的及びデジタル的な資産）のための金銭及び信用の製造及び分配に関する特権的な制御を与えられた金融機関。この文書の文脈において、この用語は、文脈においては法的エンティティを意味する場合を除き、中央銀行のコンピュータシステム及びインフラストラクチャを指す。

【 0 0 1 8 】

決済取引 - あるエンティティから他方のエンティティに金銭又は他の金銭的利益が交換

50

される、2つのエンティティ間の取引。決済取引は、商品若しくはサービスの購入のための、負債の返済のための、又は当業者に明らかであるような任意の他の金銭的利益の交換のための資金の移転とすることができる。ある事例では、決済取引は、クレジットカード取引などの決済カード及び/又は決済口座を介して資金提供される取引を指すことができる。そのような決済取引は、発行体、決済ネットワーク、及びアクワイアラを介して処理されることができる。そのような決済取引を処理するための処理は、承認、バッチ処理、清算、決済、及び資金提供のうちの少なくとも1つを含むことができる。承認は、消費者による販売者への決済詳細の提供と、販売者からアクワイアラへの取引詳細（例えば、決済詳細を含む）の提出と、取引に資金を提供するために使用される消費者の決済口座の発行体との決済詳細の検証とを含むことができる。バッチ処理は、アクワイアラへの分配のために、バッチ処理における承認された取引を、他の承認された取引と共に格納することを指すことができる。清算は、処理のために、アクワイアラから決済ネットワークへのバッチ処理された取引の送信を含むことができる。決済は、発行体の受益者が関与する取引のための、決済ネットワークによる発行体の引き落としを含むことができる。ある事例では、発行体は、決済ネットワークを介してアクワイアラに支払うことができる。他の事例では、発行体は、アクワイアラに直接支払うことができる。資金提供は、清算され、決済された決済取引について、アクワイアラから販売者への決済を含むことができる。決済取引処理の一部として実行される上述の工程の順序及び/又は分類化は当業者には明らかであろう。

10

【0019】

20

販売時点情報管理 - 商品及び/又はサービスの購入及び/又は決済のために、取引データ、決済データ、及び/又は他の適切な種類のデータを入力するための、ユーザ（例えば、消費者、従業員など）との対話を受信するように構成されたコンピューティング装置又はコンピューティングシステム。販売時点情報管理は、「店舗販売を行う」店舗などにおける取引の一部として顧客が訪問する物理的位置の物理的な装置（例えば、金銭登録器、キオスク、デスクトップコンピュータ、スマートフォン、タブレットコンピュータなど）とすることができ、又はインターネットなどのネットワークを介して顧客からの通信を受信するオンライン小売業者などの電子商取引環境における仮想とすることができる。販売時点情報管理が仮想であり得る事例において、取引を開始するためにユーザによって操作されるコンピューティング装置、又は取引の結果としてデータを受信するコンピューティングシステムは、適用可能な場合、販売時点情報管理とみなされることができる。

30

【0020】

取引口座 - 当座預金口座、貯蓄口座、掛売り口座、仮想決済口座など、取引に資金を提供するために使用されることができる金融口座。取引口座は、消費者に関連付けられることができ、消費者は、決済口座に関連付けられた任意の適切な種類のエンティティとすることができる。このエンティティは、個人、家族、会社、法人、政府のエンティティなどを含むことができる。ある事例では、取引口座は、PayPal（登録商標）などによって動作される口座などの仮想とすることができる。

【0021】

決済カード - 取引口座に関連付けられたカード又はデータであり、関連付けられた取引口座を介して金融取引に資金を提供するために販売者に提供され得る。決済カードは、クレジットカード、デビットカード、チャージカード、ストアードバリューカード、プリペイドカード、フリートカード、仮想決済番号、仮想カード番号、制御された決済番号(controlled payment number)などを含むことができる。決済カードは、販売者に提供され得る物理的なカードとすることができ、又は（例えば、スマートフォン若しくはコンピュータなどの通信装置に格納されるような）関連付けられた取引口座を表すデータとすることができる。例えば、ある事例では、決済口座番号を含むデータは、関連付けられた取引口座によって資金提供される取引の処理のための決済カードと見なされることができる。ある場合では、小切手は、適用可能な場合には決済カードとみなされることができる。

40

【0022】

50

デジタルトークンを転送するためのシステム

図 1 は、物理的決済カードとの間でデジタルトークンを転送するためのシステム 100 を示す。

【0023】

一実施形態では、システム 100 は、1つ以上の発行体 108 を含むことができる。発行体 108 は、発行する銀行などの金融機関、又は決済手段（すなわち、物理的決済手段又は物理的決済カード）110 を用いて決済取引に資金提供する際に使用するため、ユーザ 106 に取引口座を発行するように構成された他の適切なエンティティとすることができる。発行体又は発行機関 108 は、取引口座の発行の一部として、デジタルトークンを有する決済手段 110、例えば、個々のデジタルトークンを有する銀行発行 E M V（登録商標）カード、を発行することができる。デジタルトークンの各々は、例えば、通貨に変換されることができる不換金銭とすることができる。決済手段 110 は、取引口座に対応する決済認証情報を用いて符号化される、決済認証情報を含む、又は決済認証情報に関連付けられることができる。決済認証情報は、関連した取引口座を介して資金供給される取引のために、取引処理の一部として通信しなければならない任意のデータを含むことができ、例えば、代表口座番号、有効期限、及びセキュリティコードである。一実施形態によれば、デジタルトークンの各々は、マイクロ取引に関連付けられた値を有することができ、マイクロ取引は、デジタルトークンの値が比較的小さく、取引を処理するコストがより少ない。

【0024】

また、システム 100 は、1つ以上の発行体 108 及び/又は中央銀行 109 の各々に関連付けられた処理サーバ 102 を含むことができる。処理サーバ 102 は、ブロックチェーンネットワーク 104 を含む複数のノード又はプロセッサのうちの1つとすることができる。ブロックチェーンネットワーク 104 は、1つ以上のブロックチェーンに関連付けられることができる。このブロックチェーンは、発行体 108（例えば、銀行）、中央銀行 109、及び/又は第三者の供給者（又は販売者）112 に関連付けられたデータを格納して、中央銀行 109 から1つ以上の発行体 108 の各々への、及び中央銀行 109 から各消費者又はユーザ 106 の物理的決済手段 110 への、デジタルトークンの転送を伴う取引を記録するために使用されることができる。処理サーバ 102 は、ブロックチェーンに追加される新しいブロックを生成して検証するように構成されることができる。新しいブロックの検証処理は、ブロックチェーンネットワーク 104 を含む複数のノードにわたって格納されたデータの数学的検証を含むことができる。

【0025】

一実施形態によれば、中央銀行 109 は、例えば、デジタルトークンの形態におけるデジタル通貨を、複数の発行体 108 に発行することができる。次に、複数の発行体 108 の各々は、第三者の供給者又は販売者 112 において販売時点情報管理（POS）114 を用いて使用されることができる個々のデジタルトークンを有する E M V カードの形態で、決済手段 110 を発行することができる。一実施形態によれば、物理的決済手段 110 上のデジタルトークンは、例えば、セキュリティ目的のためのデジタル署名及び暗号鍵（すなわち、トークンプロファイル）を含むことができる。

【0026】

一実施形態によれば、物理的決済手段 110 に発行されたデジタルトークンは、プリペイドカードに関連付けられることができ、このプリペイドカードは、消費者又はユーザ 106 が、発行体 108 と以前に決済した、又は発行体 108 とデジタルトークンの支払いを行ったものである。例えば、デジタルトークン（例えば、1000 デジタルトークン）は、現金自動支払い機（ATM）116 を介して物理的決済手段 110 に読み込まれることができる。代替的に、デジタルトークンは、決済手段 110 に搭載されることができる。さらに、通貨（例えば、特定の国において使用するための米ドル又は他の金銭システム）について第三者の供給者 112 と発行体 108 との間のペイメントレールを介してデジタルトークンのグループ又はデジタルトークンの集合を交換する際に、ユーザ 106 は、

10

20

30

40

50

決済手段 110 に記載されるような条件及び条項に従って発行体と決済することができる。

【0027】

例示的な実施形態によれば、処理サーバ 102 に関連付けられたブロックチェーンネットワーク 104 は、中央銀行 109 によって発行体 108 及び / 又は物理的決済手段 110 に発行された、デジタル化された決済トークンに関連付けられたトークンプロファイルを格納するように構成されることができる。各トークンプロファイルは、デジタル化された決済トークン又はその識別における情報（例えば、デジタルトークン数）、それぞれデジタル化された決済トークンを有する物理的決済カードの形態である関連付けられた決済手段を含むことができる。ある事例では、処理サーバ 102 は、トークン分配プラットフォームとすることができ、又はトークン分配プラットフォームとして動作するように構成されたコンピューティングシステムの一部とすることができる。さらに、処理サーバ 102 は、それに関連して実行される機能の結果として、トークンプロファイルのデータを識別することができる。

10

【0028】

システム 100 において、例えば、ユーザ 106 は、第三者の供給者若しくは販売者 112、又は例えば、決済手段（すなわち、物理的決済カード）110 を有する他のエンティティからの金融取引又はサービス若しくは製品の購入に従事することができる。システム 100 において、ユーザ（又は消費者）106 は、複数のデジタルトークン（例えば、1000 デジタルトークン）を有する決済カード又は決済手段 110 を販売時点情報管理（POS）114 に提示する。POS 114 は、例えば、発行体 108 の処理サーバ 102 及びブロックチェーンネットワーク 104 を介して、決済手段 110 上の複数のデジタルトークンのデジタル署名を検証するように構成されることができる。

20

【0029】

デジタルトークンが有効であることが検証されると、POS 114 は、第三者の供給者においてユーザ又は消費者 106 によって購入されたサービス又は製品について、物理的決済手段 110 上の複数のデジタルトークン（例えば、1000 デジタルトークン）からいくつかのトークン（例えば、50 デジタルトークン）を差し引くことができる。差し引かれたトークン（例えば、50 デジタルトークン）は、次に、個別に、又は例えば非金融通信のようなペイメントレールを介してデジタルトークンのグループ若しくは集合を用いて、のいずれかで交換されるまで、第三者の供給者 112 によって格納されることができる。

30

【0030】

処理サーバ

図 2 は、システム 100 内の処理サーバ 102 の一実施形態を示す。図 2 に示される処理サーバ 102 の実施形態は、例示としてのみ提供され、本明細書で論じられるような機能を実行するのに適した処理サーバ 102 のすべての可能な構成を網羅し得るものではないことが、当業者には明らかであろう。例えば、図 4 に示され、以下でより詳細に論じられるコンピュータシステム 400 は、処理サーバ 102 の適切な構成とすることができる。

【0031】

処理サーバ 102 は、受信装置 202 を含むことができる。受信装置 202 は、1 つ以上のネットワークプロトコルを介して 1 つ以上のネットワーク上のデータを受信するように構成されることができる。ある事例では、受信装置 202 は、1 つ以上の通信方法を介して、発行体 108 と、第三者の供給者又は販売者のシステム 112 と、他のシステム及びエンティティとからデータを受信するように構成されることができる。この通信方法は、例えば、無線周波数、構内通信網、無線エリアネットワーク、セルラー通信ネットワーク、Bluetooth、インターネットなどである。ある実施形態では、受信装置 202 は、複数の装置から構成されることができる。これは、例えば、異なるネットワークを介してデータを受信するための異なる受信装置であり、構内通信網を介してデータを受信するための第 1 の受信装置及びインターネットを介してデータを受信するための第 2 の受信装置などである。受信装置 202 は、電子的に送信されたデータ信号を受信することが

40

50

できる。このデータは、データ信号に重ねられる、又は符号化される、及び受信装置 202 によるデータ信号の受信を介して、復号される、構文解析される、読み取られる、又は取得されることができる。ある事例では、受信装置 202 は、構文解析モジュールを含むことができる。構文解析モジュールは、受信されたデータ信号を構文解析して、重ねられたデータを取得する。例えば、受信装置 202 は、パーサプログラムを含むことができる。パーサプログラムは、受信して、受信されたデータ信号を、処理装置によって実行される機能のための使用可能な入力に変換して、本明細書で説明される方法及びシステムを実行するように構成される。

【0032】

受信装置 202 は、発行体 108 によって電子的に送信されたデータ信号を受信するように構成されることができる。これには、発行体 108（すなわち、発行機関）をデータの出所として認証するための認証情報が伴うことができ、ある事例では発行体 108（又は発行機関）に関連付けられた秘密鍵を介して生成されたデジタル署名を含むことができる。また、受信装置 202 は、適用可能な場合、第三者の供給者又は販売者のシステム 112 によって電子的に送信されたデータ信号を受信するように構成されることができる。

【0033】

また、処理サーバ 102 は、通信モジュール 204 を含むことができる。通信モジュール 204 は、本明細書で論じられる機能を実行するために、モジュールと、エンジンと、データベースと、記憶部と、処理サーバ 102 の他の構成要素との間でデータを送信するように構成されることができる。通信モジュール 204 は、1 つ以上の通信種別から構成されることができ、コンピューティング装置内の、通信のための様々な通信方法を利用することができる。例えば、通信モジュール 204 は、バス、コンタクトピンコネクタ、電線などから構成されることができる。また、ある実施形態では、通信モジュール 204 は、処理サーバ 102 の内部構成要素と、外部接続データベース、表示装置、入力装置などの処理サーバ 102 の外部構成要素との間で通信するように構成されることができる。また、処理サーバ 102 は、処理装置を含むことができる。処理装置は、本明細書で論じられる処理サーバ 102 の機能を実行するように構成されることができる。ある実施形態では、処理装置は、複数のエンジン及び/又はモジュールを含む、及び/又はそれらから構成されることができ、これは、クエリモジュール 214、生成モジュール 216、検証モジュール 218 など、処理装置の 1 つ以上の機能を実行するように特別に構成される。本明細書で使用されるように、用語「モジュール」は、ハードウェア上で実行されるソフトウェア、又は入力を受信し、入力を使用して 1 つ以上の処理を実行し、出力を提供するように構成されたハードウェアとすることができる。様々なモジュールによって実行される入力、出力、及び処理は、本開示に基づいて当業者には明らかであろう。

【0034】

処理サーバ 102 は、記憶部 206 を含むことができる。記憶部 206 は、本明細書で論じられる機能を実行する際に、処理サーバ 102 によって使用するためのデータを格納するように構成されることができ、例えば、公開鍵及び秘密鍵、対称鍵などである。記憶部 206 は、適切なデータフォーマット方法及びスキーマを使用してデータを格納するように構成されることができ、読取り専用メモリ、ランダムアクセスメモリなどの任意の適切な種類のメモリとすることができる。記憶部 206 は、例えば、暗号鍵及びアルゴリズムと、通信プロトコル及び規格と、データフォーマット規格及びプロトコルと、処理装置のモジュール及びアプリケーションプログラムのためのプログラムコードと、当業者には明らかであるような、本明細書で開示される機能の実行の際に処理サーバ 102 による使用に適し得る他のデータとを含むことができる。ある実施形態では、記憶部 206 は、関連データベースから構成されることができ、又はそれを含むことができる。関連データベースは、格納された構造化データ集合の記憶、識別、修正、更新、アクセスなどのために構造化クエリ言語を利用する。

【0035】

記憶部 206 は、ブロックチェーンを格納するように構成されることができる。上述し

10

20

30

40

50

たように、ブロックチェーンは、複数のブロックから構成されることができる。各ブロックは、少なくともブロックヘッダと1つ以上のデータ値とから構成されることができる。各ブロックヘッダは、タイムスタンプと、ブロックチェーン内の前のブロックを参照するブロック参照値と、それぞれのブロック内に含まれる1つ以上のデータ値を参照するデータ参照値とを含むことができる。また、記憶部は、本明細書で論じられる機能を実行する際に処理サーバ102によって使用され得る任意の追加データを格納するように構成されることができる。例えば、ブロックチェーンの参照値を生成するためのハッシュアルゴリズム、他のブロックチェーンノード及び他のコンピューティング装置と通信するための通信データ、ブロックチェーンデータに対する第三者の供給者又は販売者のシステム112へのアクセスを提供するためのアクセスデータ、デジタル署名の検証のために発行体108に対してプロビジョニングされた秘密鍵に対応する公開鍵などである。

10

【0036】

処理サーバ102は、クエリモジュール214を含むことができる。クエリモジュール214は、データベース上でクエリを実行して、情報を識別するように構成されることができる。クエリモジュール214は、1つ以上のデータ値又はクエリ文字列を受信することができる。記憶部206などの示されたデータベース上で、それに基づくクエリ文字列を実行して、そこに格納された情報を識別することができる。次に、クエリモジュール214は、必要に応じて、識別された情報を、処理サーバ102の適切なエンジン又はモジュールに出力することができる。クエリモジュール214は、例えば、記憶部206上でクエリを実行して、新しいブロックを生成する際の処理の一部として、（例えば、タイムスタンプに基づいて）ブロックチェーンに追加された最新のブロックを識別することができ、又は記憶部206上でクエリを実行して、認証のために、発行体108、中央銀行109、及び/若しくは第三者の供給者112によって提供されたサービス若しくは機能の種類に関連付けられたデータに提供されたデジタル署名を検証する際に使用するために、発行体108に対応する公開鍵を識別することができる。

20

【0037】

また、処理サーバ102は、生成モジュール216を含むことができる。生成モジュール216は、本明細書で論じられる機能を実行する際に使用するために、処理サーバ102のためのデータを生成するように構成されることができる。生成モジュール216は、入力として命令を受信することができ、命令に基づいてデータを生成することができ、生成されたデータを、処理サーバ102の1つ以上のモジュール又はエンジンに出力することができる。例えば、生成モジュール216は、確認及びブロックチェーンへの追加のために、新しいブロックと新しいブロックヘッダとを生成するように構成されることができる。また、生成モジュール216は、新たに生成されたブロックのブロックヘッダに含まれる参照値の生成のためなど、データへのハッシュアルゴリズムの適用を介してハッシュ値を生成するように構成されることができる。ある場合では、ハッシュ値の生成は、処理サーバ102に含まれる別個のハッシュモジュールを介して実行されることができる。

30

【0038】

また、処理サーバ102は、検証モジュール218を含むことができる。検証モジュール218は、本明細書で論じられる機能を実行する際に使用するために、処理サーバ102及び発行体108のためのデータを検証するように構成されることができる。検証モジュール218は、入力として命令を受信することができ、命令されたデータを検証することができ、検証の結果を、処理サーバ102の別のモジュール又はエンジンに出力することができる。

40

【0039】

また、処理サーバ102は、送信装置220を含むことができる。送信装置220は、1つ以上のネットワークプロトコルを介して、1つ以上のネットワーク上のデータを送信するように構成されることができる。ある事例では、送信装置220は、1つ以上の通信方法を介して、ブロックチェーンネットワーク104内のデータを、発行体108及び他のエンティティに送信するように構成されることができる。この通信方法は、構内通信網

50

、無線エリアネットワーク、セルラー通信、Bluetooth、無線周波数、インターネットなどである。ある実施形態では、送信装置220は、複数の装置から構成されることができる。これは、例えば、異なるネットワークを介してデータを送信するための異なる送信装置であり、構内通信網を介してデータを送信するための第1の送信装置及びインターネットを介してデータを送信するための第2の送信装置などである。送信装置220は、受信するコンピューティング装置によって構文解析され得る、データが重ねられたデータ信号を電子的に送信することができる。ある事例では、送信装置220は、データを送信に適したデータ信号に重ねる、符号化する、又はフォーマットするための1つ以上のモジュールを含むことができる。

【0040】

処理フロー

図3は、例示的な実施形態による、物理的決済カードとの間でデジタルトークンを転送するための例示的な方法を示すフローチャートである。方法300は、処理サーバ上で、中央銀行から発行された複数のデジタルトークンを受信すること(310)と、処理サーバから、複数のデジタルトークンを物理的決済カードに転送することであって、物理的決済カードは、POSを用いて使用されるように構成されることが(320)とを含む。また、本方法は、物理的決済カード上の複数のデジタルトークンについて、デジタル署名と暗号鍵とを含むことを含むことができる。また、本方法は、POSでの物理的決済カードの提示の際に、デジタル署名と暗号鍵とを検証することを含むことができる。さらに、本方法は、POSへの物理的決済カードの提示の際に、複数のデジタルトークンからデジタルトークンを差し引くことを含むことができる。さらに、本方法は、現金自動支払い機(ATM)を介して、物理的決済カードに、複数のデジタルトークンをアップロードすることを含むことができる。加えて、本方法は、ブロックチェーンネットワーク104内に、処理サーバとの間のデジタルトークンの各転送を記録することをさらに含むことができる。ここで、処理サーバ102は、発行体108に関連付けられることができる。また、物理的決済手段110は、個々のデジタルトークンを有するEMVカードとすることができる。

【0041】

コンピュータシステムアーキテクチャ

図4は、本開示の実施形態又はその一部がコンピュータ可読コードとして実装され得るコンピュータシステム400を示す。例えば、図1の処理サーバ102は、ハードウェア、ハードウェア上で実行されるソフトウェア、ファームウェア、命令が格納された非一時的コンピュータ可読媒体、又はそれらの組み合わせを使用して、コンピュータシステム400内に実装されることができる。図1の処理サーバ102は、1つ以上のコンピュータシステム又は他の処理システム内に実装されることができる。ハードウェア、ハードウェア上で実行されるソフトウェア、又はそれらの任意の組合せは、本明細書で開示される処理を実装するために使用されるモジュール及び構成要素を具体化することができる。

【0042】

プログラマブルロジックが使用される場合、そのようなロジックは、実行可能ソフトウェアコードによって特に構成された市販の処理プラットフォーム上で実行して、特定の目的のコンピュータ又は特別の目的の装置(例えば、プログラマブルロジックアレイ、特定用途向け集積回路など)になることができる。当業者は、開示された主題の実施形態が、様々なコンピュータシステムの構成を用いて実施され得ることを理解することができる。このコンピュータシステムは、マルチコアマルチプロセッサシステム、ミニコンピュータ、メインフレームコンピュータ、分散機能を用いてリンク又はクラスタ化されたコンピュータ、ならびに仮想的に任意の装置に埋め込まれ得るパーペシブ又は小型コンピュータを含む。例えば、少なくとも1つのプロセッサ装置及び記憶部が、上述の実施形態を実施するために使用されることができる。

【0043】

本明細書で論じられるプロセッサユニット又は装置は、単一のプロセッサ、複数のプロセッサ、又はそれらの組み合わせとすることができる。プロセッサ装置は、1つ以上のプ

10

20

30

40

50

ロセッサ「コア」を有することができる。本明細書で論じられる用語「コンピュータプログラム媒体」、「非一時的コンピュータ可読媒体」、及び「コンピュータ使用可能媒体」は、概して、有形媒体を指すために使用され、例えば、取り外し可能記憶ユニット 4 1 8、取り外し可能記憶ユニット 4 2 2、及びハードディスクドライブ 4 1 2 にインストールされたハードディスクなどである。

【 0 0 4 4 】

本開示の様々な実施形態は、この例示的なコンピュータシステム 4 0 0 に関して説明される。この説明を読んだ後、他のコンピュータシステム及び／又はコンピュータアーキテクチャを使用して、どのように本開示を実施するかが当業者には明らかになるであろう。動作は連続的な処理として説明され得るが、動作のいくつかは、実際には、並列に、同時に、及び／又は分散環境において、単一又はマルチプロセッサ機械によるアクセスのためにローカルに又は遠隔に格納されたプログラムコードを用いて、実行されることができる。加えて、ある実施形態では、動作の順序は、開示される主題の趣旨から逸脱することなく、再構成されることができる。

10

【 0 0 4 5 】

プロセッサ装置 4 0 4 は、本明細書で論じられる機能を実行するように特に構成された専用又は汎用プロセッサ装置とすることができる。プロセッサ装置 4 0 4 は、通信インフラストラクチャ 4 0 6 に接続されることができ、例えば、バス、メッセージキュー、ネットワーク、マルチコアメッセージパッシング方式などである。ネットワークは、本明細書で開示されるような機能を実行するのに適した任意のネットワークとすることができ、構内通信網（LAN）、広域通信網（WAN）、無線ネットワーク（例えば、Wi-Fi）、移動体通信網、衛星ネットワーク、インターネット、光ファイバ、同軸ケーブル、赤外線、無線周波数（RF）、又はそれらの任意の組合せを含むことができる。他の適切なネットワークの種類及び構成は、当業者には明らかであろう。また、コンピュータシステム 4 0 0 は、主記憶部 4 0 8（例えば、ランダムアクセスメモリ、読み出し専用メモリなど）を含むことができ、補助記憶部 4 1 0 も含むことができる。補助記憶部 4 1 0 は、ハードディスクドライブ 4 1 2 と、フロッピーディスクドライブ、磁気テープドライブ、光ディスクドライブ、フラッシュメモリなどの取り外し可能記憶ドライブ 4 1 4 とを含むことができる。

20

【 0 0 4 6 】

取り外し可能記憶ドライブ 4 1 4 は、周知の方法で、取り外し可能記憶ユニット 4 1 8 から読み取り、及び／又はそれに書き込むことができる。取り外し可能記憶ユニット 4 1 8 は、取り外し可能記憶ドライブ 4 1 4 によって読み書きされ得る取り外し可能記憶媒体を含むことができる。例えば、取り外し可能記憶ドライブ 4 1 4 がフロッピーディスクドライブ又はユニバーサルシリアルバスポートである場合、取り外し可能記憶ユニット 4 1 8 は、それぞれフロッピーディスク又はポータブルフラッシュドライブとすることができる。一実施形態では、取り外し可能記憶ユニット 4 1 8 は、非一時的コンピュータ可読記録媒体とすることができる。

30

【 0 0 4 7 】

ある実施形態では、補助記憶部 4 1 0 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 4 0 0 に読み込むことを可能にするための代替手段、例えば、取り外し可能記憶ユニット 4 2 2 及びインタフェース 4 2 0 を含むことができる。そのような手段の例は、プログラムカートリッジ及びカートリッジインタフェース（例えば、ビデオゲームシステムに見られるようなもの）と、取り外し可能メモリチップ（例えば、EEPROM、PROMなど）及び関連付けられたソケットと、当業者には明らかであるような他の取り外し可能記憶ユニット 4 2 2 及びインタフェース 4 2 0 とを含むことができる。

40

【 0 0 4 8 】

コンピュータシステム 4 0 0（例えば、主記憶部 4 0 8 及び／又は補助記憶部 4 1 0）に格納されたデータは、任意の種類の適切なコンピュータ可読媒体に格納されることができ、例えば、光学記憶装置（例えば、コンパクトディスク、デジタル多用途ディスク、ブ

50

ルレーディスクなど）又は磁気テープ記憶装置（例えば、ハードディスクドライブ）である。データは、任意の種類の適切なデータベース構成で構成されることができ、例えば、関係データベース、構造化クエリ言語（SQL）データベース、分散データベース、オブジェクトデータベースなどである。適切な構成及び記憶装置の種類は、当業者には明らかであろう。

【0049】

また、コンピュータシステム400は、通信インタフェース424を含むことができる。通信インタフェース424は、ソフトウェア及びデータを、コンピュータシステム400と外部装置との間で転送することを可能にするように構成されることができ、例示的な通信インタフェース424は、モデム、ネットワークインタフェース（例えば、イーサネットカード）、通信ポート、PCMCIAスロット及びカードなどを含むことができる。通信インタフェース424を介して転送されるソフトウェア及びデータは、信号の形態とすることができ、これは、電子信号、電磁信号、光信号、又は当業者には明らかであるような他の信号とすることができ、信号は、通信経路426を介して伝送することができる。この通信経路426は、信号を送信するように構成されることができ、電線、ケーブル、光ファイバ、電話回線、携帯電話リンク、無線周波数リンクなどを使用して実装されることができ、

10

【0050】

コンピュータシステム400は、表示インタフェース402をさらに含むことができる。表示インタフェース402は、データをコンピュータシステム400と外部表示装置430との間で転送することを可能にするように構成されることができ、例示的な表示インタフェース402は、高解像度マルチメディアインタフェース（HDMI）、デジタルビジュアルインタフェース（DVI）、ビデオグラフィックスアレイ（VGA）などを含むことができる。表示装置430は、コンピュータシステム400の表示インタフェース402を介して送信されたデータを表示するための任意の適切な種類の表示装置とすることができ、陰極線管（CRT）表示装置、液晶表示装置（LCD）、発光ダイオード（LED）表示装置、静電タッチ表示装置、薄膜トランジスタ（TFT）表示装置などを含む。

20

【0051】

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は、主記憶部408及び補助記憶部410などのメモリを指すことができ、これは、メモリ半導体（例えば、DRAMなど）とすることができ、これらのコンピュータプログラム製品は、コンピュータシステム400にソフトウェアを提供するための手段とすることができ、コンピュータプログラム（例えば、コンピュータ制御ロジック）は、主記憶部408及び/又は補助記憶部410内に格納されることができ、また、コンピュータプログラムは、通信インタフェース424を介して受信されることができ、そ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400が、本明細書で論じられる本方法を実施することを可能にすることができる。特に、コンピュータプログラムは、実行されると、プロセッサ装置404が、本明細書で論じられるように、図1によって示されるシステムを実行することを可能にすることができる。したがって、そ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400の制御装置を表すことができる。本開示がソフトウェアを使用して実装される場合、ソフトウェアは、コンピュータプログラム製品内に格納され、取り外し可能記憶ドライブ414、インタフェース420、及びハードディスクドライブ412、又は通信インタフェース424を使用してコンピュータシステム400内に読み込まれることができる。

30

40

【0052】

プロセッサ装置404は、コンピュータシステム400の機能を実行するように構成された1つ以上のモジュール又はエンジンを含むことができる。モジュール又はエンジンの各々は、ハードウェアを使用して実装されることができ、ある事例では、主記憶部408又は補助記憶部410内に格納されたプログラムコード及び/又はプログラムに対応するようなソフトウェアを利用することもできる。そのような事例では、プログラムコードは

50

、コンピュータシステム 400 のハードウェアによる実行の前に、プロセッサ装置 404 によって（例えば、コンパイルするモジュール又はエンジンによって）コンパイルされることができる。例えば、プログラムコードは、プロセッサ装置 404 及び／又はコンピュータシステム 400 の任意の追加のハードウェア構成要素による実行のために、アセンブリ言語又は機械コードなどの低水準言語に翻訳されるプログラミング言語で書かれたソースコードとすることができる。コンパイルする処理は、字句解析と、前処理と、構文解析と、意味解析と、構文指向翻訳と、コード生成と、コード最適化と、コンピュータシステム 400 を制御して本明細書で開示される機能を実行するのに適した低水準言語へのプログラムコードの翻訳に適し得る任意の他の技術との使用を含むことができる。そのような処理の結果、コンピュータシステム 400 が、上述の機能を実行するように一意にプログラムされた、特別に構成されたコンピュータシステム 400 となることは、当業者には明らかであろう。

10

【0053】

本開示と一致する技術は、他の特徴の中でも、ブロックチェーンネットワーク内のサービスノードを提供するためのシステム及び方法を提供する。開示されたシステム及び方法の様々な例示的な実施形態が上述されてきたが、それらは限定ではなく、例示のみを目的として提示されたことを理解されたい。それは、網羅的ではなく、開示された厳密な形態に本開示を限定しない。上記の教示に照らして、修正及び変形が可能であり、又は、修正及び変形は、広さ又は範囲から逸脱することなく、本開示の実施から得られることができる。

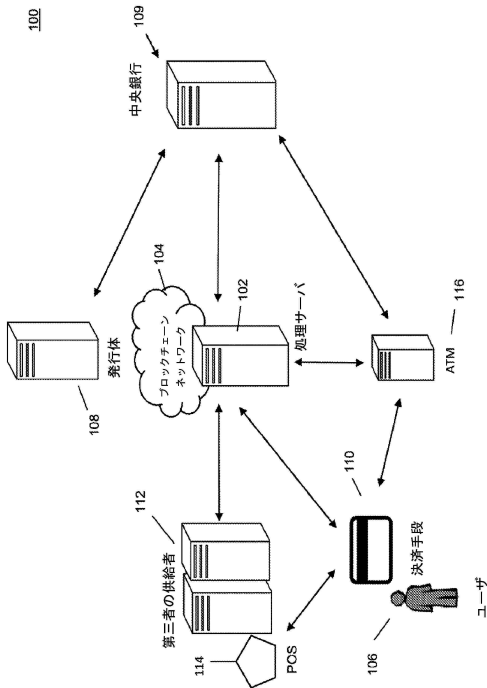
20

30

40

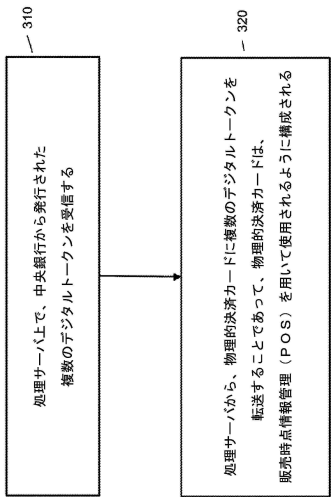
50

【図面】
【図 1】

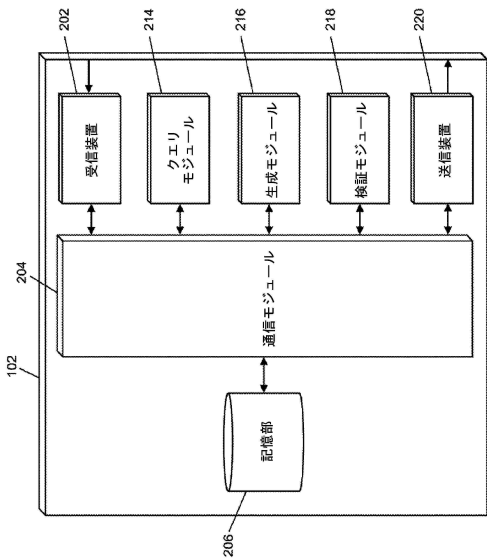


【図 3】

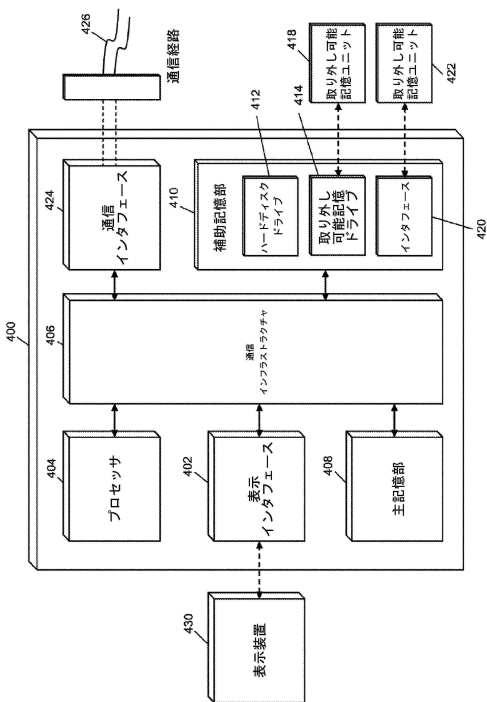
300



【図 2】



【図 4】



10

20

30

40

50

フロントページの続き

- 7
- (72)発明者 サララ ブラダグンタ
 アメリカ合衆国 ニュージャージー州 07052 ウェスト オレンジ クレストウッド ドライブ 30
- (72)発明者 セバスティアン ル キャロネック
 アイルランド国 カウンティ ウィックロー グレイストーンズ チャールズランド パーク 94
- 審査官 塩田 徳彦
- (56)参考文献 特開2019-128932(JP,A)
 特開2009-020848(JP,A)
 国際公開第95/024690(WO,A1)
 特表2021-524074(JP,A)
 米国特許出願公開第2020/0334668(US,A1)
 特開2002-123771(JP,A)
 特表2021-504773(JP,A)
 国際公開第2020/039771(WO,A1)
- (58)調査した分野 (Int.Cl., DB名)
 G06Q 10/00-99/00