(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第7857640号
(P7857640)
(45)発行日　令和8年5月13日(2026.5.13)　(24)登録日　令和8年4月30日(2026.4.30)

(51)Int.Cl.　F I
G06Q 40/04 (2012.01)　G06Q 40/04

請求項の数 3　(全 9 頁)

(21)出願番号　特願2025-175333(P2025-175333)
(22)出願日　令和7年10月17日(2025.10.17)
審査請求日　令和7年10月17日(2025.10.17)

早期審査対象出願

(73)特許権者　525404556
WEA　JAPAN株式会社
東京都千代田区大手町１丁目６番１号　大手町ビル　Ｓｐａｃｅｓ大手町２４６号室
(74)代理人　110004646
弁理士法人Ｔ．ＬＡＢＯ国際特許事務所
(72)発明者　阮　安邦
東京都港区西新橋二丁目４番３号プロス西新橋ビル７０９室
(72)発明者　魏　明
東京都港区西新橋二丁目４番３号プロス西新橋ビル７０９室
(72)発明者　王　佳師
東京都港区西新橋二丁目４番３号プロス西新橋ビル７０９室
最終頁に続く

(54)【発明の名称】為替レート特定システム、為替レート特定方法、決済システム及び決済方法

(57)【特許請求の範囲】
【請求項１】
支払いゲートウェイ、複数のオラクルマシン、コントラクトを有するブロックチェーンネットワーク及び通貨支払い実行部を備える決済システムであって、
前記支払いゲートウェイは、リクエストを複数の前記オラクルマシンに送信し、
各前記オラクルマシンは、リクエストに基づいて、為替レートデータが含まれる応答パケットを生成して前記支払いゲートウェイに送信し、
前記支払いゲートウェイは、受信した応答パケットに基づいて、前記コントラクトを呼び出し、
前記コントラクトは、故障していない複数の前記オラクルマシンの為替レートデータのうちの中間値を信頼可能為替レートとして特定して前記通貨支払い実行部に送信し、
前記通貨支払い実行部は、受信した信頼可能為替レートを用いてユーザの支払いを実行する、
決済システム。
【請求項２】
レート規制機器をさらに備え、
前記レート規制機器は、受信したリクエストに基づいて、所定の時間内におけるリクエストの数をカウントし、リクエストの数が所定の数以下である場合に、リクエストを複数の前記オラクルマシンに送信する、
請求項１に記載の決済システム。

【請求項３】
支払いゲートウェイ、複数のオラクルマシン、コントラクトを有するブロックチェーンネットワーク及び通貨支払い実行部を備える決済システムにおいて実行される決済方法であって、
支払いゲートウェイがリクエストを複数のオラクルマシンに送信することと、
各前記オラクルマシンがリクエストに基づいて、為替レートデータが含まれる応答パケットを生成して前記支払いゲートウェイに送信することと、
前記支払いゲートウェイが受信した応答パケットに基づいて、コントラクトを呼び出すことと、
前記コントラクトが故障していない複数の前記オラクルマシンの為替レートデータのうちの中間値を信頼可能為替レートとして特定して通貨支払い実行部に送信することと、
前記通貨支払い実行部が受信した信頼可能為替レートを用いてユーザの支払いを実行することと、を含む、
決済方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、為替レート特定システム、為替レート特定方法、決済システム及び決済方法に関する。
【背景技術】
【０００２】
特許文献１には、暗号資産及び法定通貨を統合した決済システムが開示されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特許７７２０５１４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
このような特許文献１に記載の決済システムでは、為替レートの取得については具体的に言及していないが、一般的には、単一のオラクルマシンから取得することが考えられる。しかしながら、単一のオラクルマシンの故障等による支払い金額の計算ミスが発生し得る。
【０００５】
そこで、本発明は、この問題点に着目してなされたものであり、単一のオラクルマシンの故障等による支払い金額の計算ミスを抑制することができる為替レート特定システム、為替レート特定方法、決済システム及び決済方法を提供することを目的とする。
【課題を解決するための手段】
【０００６】
本発明のある態様によれば、支払いゲートウェイ、複数のオラクルマシン及びコントラクトを備える為替レート特定システムであって、前記支払いゲートウェイは、リクエストを複数の前記オラクルマシンに送信し、各前記オラクルマシンは、リクエストに基づいて、為替レートデータが含まれる応答パケットを生成して前記支払いゲートウェイに送信し、前記支払いゲートウェイは、受信した応答パケットに基づいて、前記コントラクトを呼び出し、前記コントラクトは、複数の前記オラクルマシンの為替レートデータに基づいて、信頼可能為替レートを特定する為替レート特定システムが提供される。
【０００７】
本発明の他の態様によれば、支払いゲートウェイ、複数のオラクルマシン、コントラクト及び通貨支払い実行部を備える決済システムであって、前記支払いゲートウェイは、リクエストを複数の前記オラクルマシンに送信し、各前記オラクルマシンは、リクエストに

基づいて、為替レートデータが含まれる応答パケットを生成して前記支払いゲートウェイに送信し、前記支払いゲートウェイは、受信した応答パケットに基づいて、前記コントラクトを呼び出し、前記コントラクトは、複数の前記オラクルマシンの為替レートデータに基づいて、信頼可能為替レートを特定して前記通貨支払い実行部に送信し、前記通貨支払い実行部は、受信した信頼可能為替レートを用いてユーザの支払いを実行する決済システムが提供される。

【０００８】

本発明の他の態様によれば、支払いゲートウェイがリクエストを複数のオラクルマシンに送信することと、各前記オラクルマシンがリクエストに基づいて、為替レートデータが含まれる応答パケットを生成して前記支払いゲートウェイに送信することと、前記支払いゲートウェイが受信した応答パケットに基づいて、コントラクトを呼び出すことと、前記コントラクトが複数の前記オラクルマシンの為替レートデータに基づいて、信頼可能為替レートを特定することと、を含む為替レート特定方法が提供される。

【０００９】

本発明の他の態様によれば、支払いゲートウェイがリクエストを複数のオラクルマシンに送信することと、各前記オラクルマシンがリクエストに基づいて、為替レートデータが含まれる応答パケットを生成して前記支払いゲートウェイに送信することと、前記支払いゲートウェイが受信した応答パケットに基づいて、コントラクトを呼び出すことと、前記コントラクトが複数の前記オラクルマシンの為替レートデータに基づいて、信頼可能為替レートを特定して通貨支払い実行部に送信することと、前記通貨支払い実行部が受信した信頼可能為替レートを用いてユーザの支払いを実行することと、を含む決済方法が提供される。

【発明の効果】

【００１０】

これらの態様によれば、一部のオラクルマシンの故障等による支払い金額の計算ミスを抑制することができる。

【図面の簡単な説明】

【００１１】

【図１】図１は、本実施形態に係る決済システムの構成を示すブロック図である。

【図２】図２は、本実施形態に係る決済システムが行う処理を示すシーケンスである。

【発明を実施するための形態】

【００１２】

以下、添付図面を参照しながら本発明の実施形態（以下、本実施形態と称する）について説明する。本明細書においては、全体を通じて、同一の要素には同一の符号を付する。

【００１３】

（決済システム）

まず、図１を参照しながら本実施形態に係る決済システム１００を説明する。

【００１４】

図１は、本実施形態に係る決済システム１００の構成を示すブロック図である。

【００１５】

図１に示すように、本実施形態に係る決済システム１００は、支払いゲートウェイ１、クラウドフレア（Ｃｌｏｕｄｆｌａｒｅ　ＷＡＦ（Ｗｅｂ　Ａｐｐｌｉｃａｔｉｏｎ　Ｆｉｒｅｗａｌｌ／ウェブ　アプリケーション　ファイアウォール））２、レート規制機器３、Ｎｏｎｃｅサーバ４、オラクルマシン５、データソースサーバ６、ブロックチェーンネットワーク７、コントラクト８及び通貨支払い実行部９を備える。なお、支払いゲートウェイ１、クラウドフレア２、レート規制機器３、Ｎｏｎｃｅサーバ４、オラクルマシン５、データソースサーバ６、ブロックチェーンネットワーク７（コントラクト８）及び通貨支払い実行部９は、ネットワークＮによって、互いに通信可能に接続されている。

【００１６】

本実施形態では、支払いゲートウェイ１、クラウドフレア２、レート規制機器３、Ｎｏ

ｎｃｅサーバ４、オラクルマシン５、データソースサーバ６、ブロックチェーンネットワーク７及びコントラクト８は、為替レート特定システム１０を構成している。オラクルマシン５は、ＳＧＸ（Ｓｏｆｔｗａｒｅ　Ｇｕａｒｄ　Ｅｘｔｅｎｓｉｏｎｓ／ソフトウェア　ガード　エックステンションズ）　Ｅｎｃｌａｖｅ（エンクレーブ）において運用されている。データソースサーバ６は、為替レートデータが含まれるデータソースを記憶している。コントラクト８は、人又はＡＩが作成したものであって、ブロックチェーンネットワーク７において運用されている。

【００１７】

（決済方法）

次に、図２を参照しながら決済システム１００による決済方法（処理）を詳細に説明する。

【００１８】

図２は、本実施形態に係る決済システム１００が行う処理を示すシーケンスである。

【００１９】

図２に示すように、まず、ステップＳ１０１において、支払いゲートウェイ１は、リクエストを生成し、生成したリクエストをクラウドフレア２送信し、ステップＳ１０２に進む。ここでは、リクエストは、ＨＭＡＣ（Ｈａｓｈ－ｂａｓｅｄ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を含む。

【００２０】

ステップＳ１０２において、クラウドフレア２は、支払いゲートウェイ１から送信されたリクエストを受信し、フィルタリングし、フィルタリング済みのリクエストをレート規制機器３に送信し、ステップＳ１０３に進む。

【００２１】

ステップＳ１０３において、レート規制機器３は、所定の時間内（例えば、１ｓ）におけるリクエスト（具体的には、フィルタリング済みのリクエスト）の回数をカウントし、所定の時間内におけるリクエストの回数が所定の回数（例えば、１０回）に達したか否かを判定する。そして、所定の時間内におけるリクエストの回数が所定の回数に達していない場合（Ｎｏの場合に）に、ステップＳ１０４に進む。一方、所定の時間内におけるリクエストの回数が所定の回数に達した場合（Ｙｅｓの場合）に、ステップＳ１０１に戻る。これにより、過剰のリクエストが支払いゲートウェイ１から送信されることを抑制することができるため、抗ＤＤｏＳ性を高めることができる。

【００２２】

ステップＳ１０４において、レート規制機器３は、フィルタリング済みのリクエストをＮｏｎｃｅサーバ４に送信し、ステップＳ１０５に進む。

【００２３】

ステップＳ１０５において、Ｎｏｎｃｅサーバ４は、受信したフィルタリング済みのリクエストの唯一性を検証する。これにより、重複攻撃を抑制することができる。そして、Ｎｏｎｃｅサーバ４は、リクエストの唯一性を検証した場合に、ステップＳ１０６に進む。

【００２４】

ステップＳ１０６において、Ｎｏｎｃｅサーバ４は、ＡＷＳ（Ａｍａｚｏｎ　Ｗｅｂ　Ｓｅｒｖｉｃｅｓ／アマゾン　ウェブ　サービス）　ＫＭＳ（Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　Ｓｅｒｖｉｃｅ／キー管理サービス）　ＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ／ハードウェア　セキュリティ　モジュール）に記憶されたＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍｍｉｎｇ　Ｉｎｔｅｒｆａｃｅ／アプリケーション　プログラミング　インターフェイス）秘密鍵（すなわち、一部のシェアキー）を用いて、リクエストにＡＰＩ署名し、ＡＰＩ署名済みのリクエストをオラクルマシン５に送信し、ステップＳ１０７に進む。ここでは、ＡＰＩ秘密鍵は、第１所定の周期（例えば、１ｈ毎）をもって自動更新されている。

【００２５】

ステップＳ１０７において、オラクルマシン５は、ＳＧＸ　Ｅｎｃｌａｖｅに記憶されたＴＬＳ（Ｔｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ／トランスポート　レイヤー　セキュリティ）プライベートキー（すなわち、他部のシェアキー）を用いて、受信したＡＰＩ署名済みのリクエストにＴＬＳ署名し、ＡＰＩ署名及びＴＬＳ署名済みのリクエストに基づいて、ＨＭＡＣを検証し、ステップＳ１０８に進む。これにより、リクエストを送信した支払いゲートウェイ１が合法の支払いゲートウェイであることを特定することができるため、オラクルマシン５が攻撃されることを抑制することができる。ここでは、ＴＬＳプライベートキーは、第２所定の周期（例えば、シーズン毎）をもって自動更新されている。

【００２６】

ステップＳ１０８において、オラクルマシン５は、リクエストの唯一性を検証する。これにより、重複攻撃を抑制することができる。そして、オラクルマシン５は、リクエストの唯一性を検証した場合に、ステップＳ１０９に進む。

【００２７】

ステップＳ１０９において、オラクルマシン５は、為替レートデータを要求するための指令をデータソースサーバ６に送信し、ステップＳ１１０に進む。

【００２８】

ステップＳ１１０において、データソースサーバ６は、受信した指令に基づいて、データソースから為替レートデータを選択してオラクルマシン５に送信し、ステップＳ１１１に進む。

【００２９】

ステップＳ１１１において、オラクルマシン５は、ネットワークと通信不可なハードウェア（具体的には、Ｌｅｄｇｅｒ　ＨＳＭ）に記憶された秘密鍵（具体的には、ＥＣＤＳＡ（Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ／楕円曲線デジタル署名アルゴリズム）秘密鍵）を用いて、受信した為替レートデータに署名し、署名済み（具体的には、ＥＣＤＳＡ署名済み）の為替レートデータに基づいて応答パケットを生成して支払いゲートウェイ１に送信し、ステップＳ１１２に進む。

【００３０】

ステップＳ１１２において、支払いゲートウェイ１は、受信した応答パケットに基づいて、コントラクト８を呼び出し、ステップＳ１１３に進む。

【００３１】

ステップＳ１１３において、コントラクト８は、署名済みの為替レートデータのアドレスがコントラクト８に記憶した所定のアドレスリストに存在しているか否かを検証する。これにより、データソースの合法性を検証することができるため、為替レートデータの改ざんを抑制することができる。そして、コントラクト８は、署名済みの為替レートデータのアドレスが所定のアドレスリストに存在していることを検証した場合に、ステップＳ１１４に進む。

【００３２】

ステップＳ１１４において、コントラクト８は、複数（例えば、五つ）のオラクルマシン５の為替レートデータに基づいて、信頼可能為替レートを特定して通貨支払い実行部９に送信し、ステップＳ１１５に進む。これにより、複数のオラクルマシン５のうちの一部が故障した場合であって、複数のオラクルマシン５のうちの他部が故障していなければ、信頼可能為替レートを特定することができるため、一部のオラクルマシン５の故障等による支払い金額の計算ミスを抑制することができる。

【００３３】

具体的には、ステップＳ１１４において、コントラクト８は、署名済みの為替レートデータのアドレスが所定のアドレスリストに存在していることを検証した場合に、複数のオラクルマシン５（具体的には、故障していないオラクルマシン５）の為替レートデータのうちの中間値を信頼可能為替レートとして特定する。これにより、ノイズ（すなわち、異

常値）を除去して支払いの計算に必要な為替レートの信頼性を高めることができる。

【００３４】

一方、ステップＳ１１４において、コントラクト８は、署名済みの為替レートデータのアドレスが所定のアドレスリストに存在していることを検証した場合、かつ、すべてのオラクルマシン５の為替レートデータが存在していない場合（すなわち、複数のオラクルマシン５がすべて故障した場合）に、コントラクト８にキャッシュした歴史為替レート（例えば、特定された前回の信頼可能為替レート）を信頼可能為替レートとして特定する。これにより、複数のオラクルマシン５がすべて故障した場合であっても、信頼可能為替レートを特定することができるため、すべてのオラクルマシン５の故障等による支払い金額の計算ミスを抑制することができる。

【００３５】

ステップＳ１１５において、通貨支払い実行部９は、受信した信頼可能為替レートを用いて、ユーザの支払いを実行し、本処理を終了させる。

【００３６】

（作用効果）

次に、上述した実施形態による作用効果について説明する。

【００３７】

上述した実施形態に係る為替レート特定システム１０は、支払いゲートウェイ１、複数のオラクルマシン５及びコントラクト８を備えるものであって、支払いゲートウェイ１は、リクエストを複数のオラクルマシン５に送信し、各オラクルマシン５は、リクエストに基づいて、為替レートデータが含まれる応答パケットを生成して支払いゲートウェイ１に送信し、支払いゲートウェイ１は、受信した応答パケットに基づいて、コントラクト８を呼び出し、コントラクト８は、複数のオラクルマシンの為替レートデータに基づいて、信頼可能為替レートを特定する。

【００３８】

また、上述した実施形態に係る決済システム１００は、支払いゲートウェイ１、複数のオラクルマシン５、コントラクト８及び通貨支払い実行部９を備えるものであって、支払いゲートウェイ１は、リクエストを複数のオラクルマシン５に送信し、各オラクルマシン５は、リクエストに基づいて、為替レートデータが含まれる応答パケットを生成して支払いゲートウェイ１に送信し、支払いゲートウェイ１は、受信した応答パケットに基づいて、コントラクト８を呼び出し、コントラクト８は、複数のオラクルマシンの為替レートデータに基づいて、信頼可能為替レートを特定して通貨支払い実行部９に送信し、通貨支払い実行部９は、受信した信頼可能為替レートを用いてユーザの支払いを実行する。

【００３９】

また、上述した実施形態に係る為替レート特定方法は、支払いゲートウェイ１がリクエストを複数のオラクルマシン５に送信することと、各オラクルマシン５がリクエストに基づいて、為替レートデータが含まれる応答パケットを生成して支払いゲートウェイ１に送信することと、支払いゲートウェイ１が受信した応答パケットに基づいて、コントラクト８を呼び出すことと、コントラクト８が複数のオラクルマシン５の為替レートデータに基づいて、信頼可能為替レートを特定することと、を含む。

【００４０】

また、上述した実施形態に係る決済方法は、支払いゲートウェイ１がリクエストを複数のオラクルマシン５に送信することと、各オラクルマシン５がリクエストに基づいて、為替レートデータが含まれる応答パケットを生成して支払いゲートウェイ１に送信することと、支払いゲートウェイ１が受信した応答パケットに基づいて、コントラクト８を呼び出すことと、コントラクト８が複数のオラクルマシン５の為替レートデータに基づいて、信頼可能為替レートを特定して通貨支払い実行部９に送信することと、通貨支払い実行部９が受信した信頼可能為替レートを用いてユーザの支払いを実行することと、を含む。

【００４１】

これらの構成によれば、複数のオラクルマシン５のうちの一部が故障した場合であって

、複数のオラクルマシン５のうちの他部が故障していなければ、信頼可能為替レートを特定することができるため、一部のオラクルマシン５の故障等による支払い金額の計算ミスを抑制することができる。

【００４２】

また、上述した実施形態では、コントラクト８は、複数のオラクルマシン５の為替レートデータのうちの中間値を信頼可能為替レートとして特定する。

【００４３】

この構成によれば、ノイズ（すなわち、異常値）を除去して支払いの計算に必要な為替レートの信頼性を高めることができる。

【００４４】

また、上述した実施形態では、コントラクト８は、複数のオラクルマシン５がすべて故障した場合に、キャッシュした歴史為替レートを信頼可能為替レートとして特定する。

【００４５】

この構成によれば、複数のオラクルマシン５がすべて故障した場合であっても、信頼可能為替レートを特定することができるため、すべてのオラクルマシン５の故障等による支払い金額の計算ミスを抑制することができる。

【００４６】

また、上述した実施形態では、各オラクルマシン５は、リクエストに基づいて、信頼可能データソースから為替レートデータを取得し、ネットワークと通信不可なハードウェアに記憶された秘密鍵を用いて、取得した為替レートデータに署名し、応答パケットを生成して支払いゲートウェイ１に送信し、支払いゲートウェイ１は、受信した応答パケットに基づいて、コントラクト８を呼び出し、コントラクト８は、署名済みの為替レートデータのアドレスが所定のアドレスリストに存在しているか否かを検証し、署名済みの為替レートデータのアドレスが所定のアドレスリストに存在していることを検証した場合に、複数のオラクルマシン５の為替レートデータに基づいて、信頼可能為替レートを特定する。

【００４７】

この構成によれば、データソースの合法性を検証することができるため、為替レートデータの改ざんを抑制することができる。この結果、信頼可能為替レートの信頼性をより高めることができる。

【００４８】

また、上述した実施形態では、為替レート特定システム１０は、レート規制機器３をさらに備え、レート規制機器３は、受信したリクエストに基づいて、所定の時間内におけるリクエストの数をカウントし、リクエストの数が所定の数以下である場合に、リクエストを複数のオラクルマシン５に送信する。

【００４９】

この構成によれば、過剰のリクエストが支払いゲートウェイ１から送信されることを抑制することができるため、抗ＤＤｏＳ性を高めることができる。

【００５０】

以上、本実施形態について説明したが、上述した実施形態は、本発明の適用例の一部を示したに過ぎず、本発明の技術的範囲を上述した実施形態の具体的構成に限定する趣旨ではない。

【符号の説明】

【００５１】

１　支払いゲートウェイ
５　オラクルマシン
８　コントラクト
１０　為替レート特定システム
１００　決済システム

【要約】

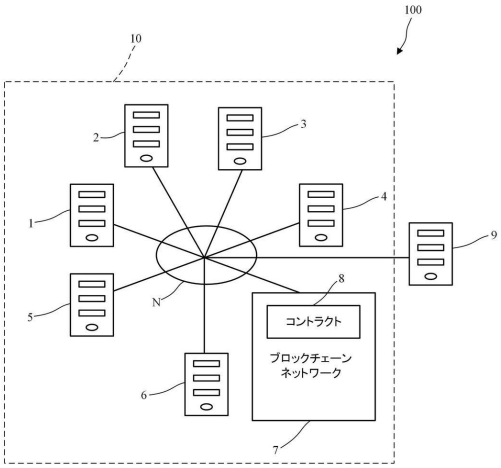
【課題】単一のオラクルマシンの故障等による支払い金額の計算ミスを抑制することがで

きる為替レート特定システム、為替レート特定方法、決済システム及び決済方法を提供する。

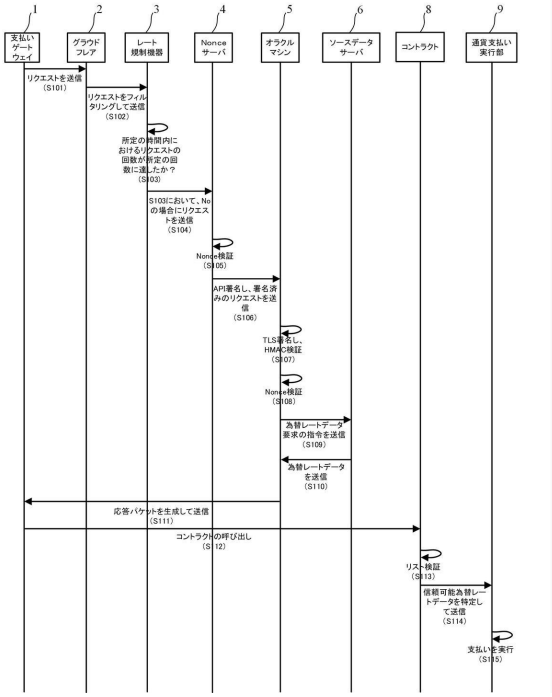
【解決手段】支払いゲートウェイ１、複数のオラクルマシン５及びコントラクト８を備える為替レート特定システム１０であって、支払いゲートウェイ１は、リクエストを複数のオラクルマシン５に送信し、各オラクルマシン５は、リクエストに基づいて、為替レートデータが含まれる応答パケットを生成して支払いゲートウェイ１に送信し、支払いゲートウェイ１は、受信した応答パケットに基づいて、コントラクト８を呼び出し、コントラクト８は、複数のオラクルマシン５の為替レートデータに基づいて、信頼可能為替レートを特定する。

【選択図】図２

【図１】



【図２】



フロントページの続き

(72)発明者　劉　達
東京都港区西新橋二丁目４番３号プロス西新橋ビル７０９室
(72)発明者　朱　軍
東京都港区西新橋二丁目４番３号プロス西新橋ビル７０９室

審査官　野口　俊明

(56)参考文献　特開２０１５－２１０６７５（ＪＰ，Ａ）
米国特許出願公開第２０２１／０１９２５００（ＵＳ，Ａ１）
特開２０１９－２０４３０７（ＪＰ，Ａ）
特表２００４－５２０６４５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　　１０／００－９９／００