

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7188606号
(P7188606)

(45)発行日 令和4年12月13日(2022.12.13)

(24)登録日 令和4年12月5日(2022.12.5)

(51)国際特許分類

F I

G 0 6 Q 20/40 (2012.01)

G 0 6 Q 20/40 3 0 0

請求項の数 5 (全13頁)

(21)出願番号	特願2021-544997(P2021-544997)	(73)特許権者	000005223
(86)(22)出願日	令和1年9月10日(2019.9.10)		富士通株式会社
(86)国際出願番号	PCT/JP2019/035472		神奈川県川崎市中原区上小田中4丁目1番1号
(87)国際公開番号	WO2021/048911	(74)代理人	100107766
(87)国際公開日	令和3年3月18日(2021.3.18)		弁理士 伊東 忠重
審査請求日	令和4年2月15日(2022.2.15)	(74)代理人	100070150
			弁理士 伊東 忠彦
		(72)発明者	東角 芳樹
			神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
		(72)発明者	森永 正信
			神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
		(72)発明者	藤本 真吾
			最終頁に続く

(54)【発明の名称】 制御方法、情報処理装置、情報処理システム及び制御プログラム

(57)【特許請求の範囲】

【請求項1】

店舗の商品を購入する購入者が利用する購入者端末が前記店舗において読み取ったコード情報に含まれている、前記商品の購入の決済に関する第1の情報を前記購入者端末から受信し、

前記購入者端末から受信する処理において受信された前記第1の情報に基づく第3の情報を前記購入者端末へ送信し、

前記店舗において前記商品の購入の決済に利用される店舗端末から商品の購入の決済に関する情報であって、前記店舗端末の署名が付加された第2の情報を受信し、

前記店舗端末から受信する処理において、前記第2の情報と共に、前記購入者端末が前記第3の情報に基づいて生成したコード情報を読み取った前記店舗端末から前記第3の情報が受信されたか否かと前記署名の検証とに基づいて、前記第1の情報と前記第2の情報とが同一の決済に関する情報であるか否かを判定し、

判定結果が肯定的である場合に、前記購入者から前記店舗への前記購入の支払いに関する情報についてブロックチェーンへの記録を制御する、
処理をコンピュータが実行することを特徴とする制御方法。

【請求項2】

前記第3の情報は、前記第1の情報を識別する情報を含む、
ことを特徴とする請求項1記載の制御方法。

【請求項3】

店舗の商品を購入する購入者が利用する購入者端末が前記店舗において読み取ったコード情報に含まれている、前記商品の購入の決済に関する第1の情報を前記購入者端末から受信する第1の受信部と、

前記購入者端末から受信する処理において受信された前記第1の情報に基づく第3の情報を前記購入者端末へ送信する送信部と、

前記店舗において前記商品の購入の決済に利用される店舗端末から商品の購入の決済に関する情報であって、前記店舗端末の署名が付加された第2の情報を受信する第2の受信部と、

前記店舗端末から受信する処理において、前記第2の情報と共に、前記購入者端末が前記第3の情報に基づいて生成したコード情報を読み取った前記店舗端末から前記第3の情報が受信されたか否かと前記署名の検証とに基づいて、前記第1の情報と前記第2の情報とが同一の決済に関する情報であるか否かを判定する判定部と、

判定結果が肯定的である場合に、前記購入者から前記店舗への前記購入の支払いに関する情報についてブロックチェーンへの記録を制御する制御部と、
を有することを特徴とする情報処理装置。

【請求項4】

店舗の商品を購入する購入者が利用する購入者端末と、前記店舗において前記商品の購入の決済に利用される店舗端末と、情報処理装置とを含む情報処理システムであって、

前記情報処理装置は、

前記購入者端末が前記店舗において読み取ったコード情報に含まれている、前記商品の購入の決済に関する第1の情報を前記購入者端末から受信する第1の受信部と、

前記購入者端末から受信する処理において受信された前記第1の情報に基づく第3の情報を前記購入者端末へ送信する送信部と、

前記店舗において前記商品の購入の決済に利用される店舗端末から商品の購入の決済に関する情報であって、前記店舗端末の署名が付加された第2の情報を受信する第2の受信部と、

前記店舗端末から受信する処理において、前記第2の情報と共に、前記購入者端末が前記第3の情報に基づいて生成したコード情報を読み取った前記店舗端末から前記第3の情報が受信されたか否かと前記署名の検証とに基づいて、前記第1の情報と前記第2の情報とが同一の決済に関する情報であるか否かを判定する判定部と、

判定結果が肯定的である場合に、前記購入者から前記店舗への前記購入の支払いに関する情報についてブロックチェーンへの記録を制御する制御部と、
を有することを特徴とする情報処理システム。

【請求項5】

店舗の商品を購入する購入者が利用する購入者端末が前記店舗において読み取ったコード情報に含まれている、前記商品の購入の決済に関する第1の情報を前記購入者端末から受信し、

前記購入者端末から受信する処理において受信された前記第1の情報に基づく第3の情報を前記購入者端末へ送信し、

前記店舗において前記商品の購入の決済に利用される店舗端末から商品の購入の決済に関する情報であって、前記店舗端末の署名が付加された第2の情報を受信し、

前記店舗端末から受信する処理において、前記第2の情報と共に、前記購入者端末が前記第3の情報に基づいて生成したコード情報を読み取った前記店舗端末から前記第3の情報が受信されたか否かと前記署名の検証とに基づいて、前記第1の情報と前記第2の情報とが同一の決済に関する情報であるか否かを判定し、

判定結果が肯定的である場合に、前記購入者から前記店舗への前記購入の支払いに関する情報についてブロックチェーンへの記録を制御する、
処理をコンピュータに実行させることを特徴とする制御プログラム。

【発明の詳細な説明】

【技術分野】

10

20

30

40

50

【0001】

本発明は、制御方法、情報処理装置、情報処理システム及び制御プログラムに関する。

【背景技術】

【0002】

QRコード（登録商標）等の2次元コードを使った決済（以下、「コード決済」という。）が普及しつつある。コード決済では、店舗の決済端末に表示される2次元コード、又は紙に印字されて店舗に提示されている2次元コードを、購入者が所持するスマートフォン等の端末に読み取らせるといった簡単な操作で決済を完了できる。なお、2次元コードには決済口座（振り込み先の口座）の口座番号等が含まれている。

【先行技術文献】

【特許文献】

【0003】

【文献】特開2009-124311号公報

特開2003-323512号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

しかしながら、コード決済は便利な反面、セキュリティ面で問題が指摘されている。例えば、紙によって提示されている2次元コードについては、当該2次元コードの上に、偽の2次元コードが印字されたシールが悪意者によって貼られるといった事例が報告されている。

【0005】

また、店員が偽の決済端末を使用して、当該決済端末に表示される偽の2次元コードを購入者の端末に読み取らせるといった事例も報告されている

これらの事例の場合、購入者の端末は偽の2次元コードを読み取ることになる。その結果、購入者は、偽の口座に代金を振り込むといったような、不正請求を受けることになる。

【0006】

そこで、一側面では、コード決済における不正請求の発生を抑制することを目的とする。

【課題を解決するための手段】

【0007】

一つの案では、店舗の商品を購入する購入者が利用する購入者端末が前記店舗において読み取ったコード情報に含まれている、前記商品の購入の決済に関する第1の情報を前記購入者端末から受信し、前記購入者端末から受信する処理において受信された前記第1の情報に基づく第3の情報を前記購入者端末へ送信し、前記店舗において前記商品の購入の決済に利用される店舗端末から商品の購入の決済に関する情報であって、前記店舗端末の署名が付加された第2の情報を受信し、前記店舗端末から受信する処理において、前記第2の情報と共に、前記購入者端末が前記第3の情報に基づいて生成したコード情報を読み取った前記店舗端末から前記第3の情報が受信されたか否かと前記署名の検証とに基づいて、前記第1の情報と前記第2の情報とが同一の決済に関する情報であるか否かを判定し、判定結果が肯定的である場合に、前記購入者から前記店舗への前記購入の支払いに関する情報についてブロックチェーンへの記録を制御する、処理をコンピュータが実行する。

【発明の効果】

【0008】

一態様によれば、コード決済における不正請求の発生を抑制することができる。

【図面の簡単な説明】

【0009】

【図1】第1の実施の形態における決済システム1の構成例を示す図である。

【図2】第1の実施の形態における仲介装置10のハードウェア構成例を示す図である。

【図3】第1の実施の形態における仲介装置10の機能構成例を示す図である。

【図4】第1の実施の形態の決済システム1において実行される処理手順の一例を説明す

10

20

30

40

50

るためのシーケンス図である。

【図５】第２の実施の形態における決済システム１の構成例を示す図である。

【図６】第２の実施の形態の決済システム１において実行される処理手順の一例を説明するためのシーケンス図である。

【発明を実施するための形態】

【００１０】

以下、図面に基づいて本発明の実施の形態を説明する。図１は、第１の実施の形態における決済システム１の構成例を示す図である。図１において、決済システム１は、店舗端末３０、購入者端末２０、仲介装置１０及びブロックチェーンＣａ等を含む。仲介装置１０は、店舗端末３０、購入者端末２０及びブロックチェーンＣａ等とインターネット等のネットワークを介して接続される。

10

【００１１】

店舗端末３０は、例えば、コード決済の加盟店として予め登録された或る店舗（以下、「店舗Ｙ」という。）に設置されているコード決済用の端末である。店舗端末３０は、商品の購入の決済時に決済用のコード情報（本実施の形態では、ＱＲコード（登録商標）等の２次元コードを一例とする。）を表示したり、後述されるワンタイムパスワードの入力を受け付けたりする。当該２次元コードには、購入金額と振込先の店舗口座を示す情報（以下、「店舗口座情報」という。）が含まれている。店舗端末３０は、ワンタイムパスワードが入力されると、当該ワンタイムパスワード及び決済に関する情報（購入金額及び振込先の銀行口座（以下、「店舗口座」という。）を示す情報を仲介装置１０へ送信する。

20

【００１２】

購入者端末２０は、店舗Ｙにおいて商品を購入する或る購入者（以下、「購入者Ｘ」という。）が所持（携帯）するスマートフォン等の端末である。購入者端末２０は、デジタルカメラを備え、当該デジタルカメラを用いて２次元コードを読み取ることができる。購入者端末２０には、決済システム１に対応したアプリケーションプログラムがインストールされており、当該アプリケーションプログラムによる制御により、購入者端末２０のデジタルカメラで読み取られた２次元コードに含まれる情報を仲介装置１０へ送信したり、当該情報に応じて仲介装置１０から返信されるワンタイムパスワードを受信及び表示したりする。

【００１３】

仲介装置１０は、購入者から店舗への購入金額の支払いに関する取引の仲介を行う１以上のコンピュータである。仲介装置１０は、２次元コードを読み取った購入者端末２０から送信される、当該２次元コードに含まれる情報（後述のトランザクション情報）が、店舗端末３０からワンタイムパスワードと共に送信される情報と同一の決済に係る情報であることが判定されるまで、決済の実行を保留することで、エスクロー取引を実現する。

30

【００１４】

ブロックチェーンＣａは、決済取引に関する各種の取引等が記録されるブロックチェーンである。

【００１５】

なお、図１には、購入者端末２０及び店舗端末３０のそれぞれが１台しか示されていないが、決済システム１は、複数の購入者のそれぞれの購入者端末２０、及び複数の店舗のそれぞれの１以上の店舗端末３０を含んでもよい。

40

【００１６】

図２は、第１の実施の形態における仲介装置１０のハードウェア構成例を示す図である。図２の仲介装置１０は、それぞれバスで相互に接続されているドライブ装置１００、補助記憶装置１０２、メモリ装置１０３、ＣＰＵ１０４、及びインタフェース装置１０５等を有する。

【００１７】

仲介装置１０での処理を実現するプログラムは、記録媒体１０１によって提供される。プログラムを記録した記録媒体１０１がドライブ装置１００にセットされると、プログラ

50

ムが記録媒体１０１からドライブ装置１００を介して補助記憶装置１０２にインストールされる。但し、プログラムのインストールは必ずしも記録媒体１０１より行う必要はなく、ネットワークを介して他のコンピュータよりダウンロードするようにしてもよい。補助記憶装置１０２は、インストールされたプログラムを格納すると共に、必要なファイルやデータ等を格納する。

【００１８】

メモリ装置１０３は、プログラムの起動指示があった場合に、補助記憶装置１０２からプログラムを読み出して格納する。ＣＰＵ１０４は、メモリ装置１０３に格納されたプログラムに従って仲介装置１０に係る機能を実行する。インタフェース装置１０５は、ネットワークに接続するためのインタフェースとして用いられる。

10

【００１９】

なお、記録媒体１０１の一例としては、ＣＤ－ＲＯＭ、ＤＶＤディスク、又はＵＳＢメモリ等の可搬型の記録媒体が挙げられる。また、補助記憶装置１０２の一例としては、ＨＤＤ（Hard Disk Drive）又はフラッシュメモリ等が挙げられる。記録媒体１０１及び補助記憶装置１０２のいずれについても、コンピュータ読み取り可能な記録媒体に相当する。

【００２０】

図３は、第１の実施の形態における仲介装置１０の機能構成例を示す図である。図３において、仲介装置１０は、認証部１１、トランザクション情報受信部１２、引き落とし制御部１３、保留部１４、ワンタイムパスワード生成部１５、決済情報受信部１６、検証部１７、振込制御部１８及び決済取消部１９等を有する。これら各部は、仲介装置１０にインストールされた１以上のプログラムが、ＣＰＵ１０４に実行させる処理により実現される。仲介装置１０は、また、ユーザ情報記憶部１２１、トランザクション情報記憶部１２２及びワンタイムパスワード記憶部１２３等を利用する。これら各記憶部は、例えば、補助記憶装置１０２、又は仲介装置１０にネットワークを介して接続可能な記憶装置等を用いて実現可能である。

20

【００２１】

認証部１１は、購入者端末２０のユーザ（すなわち、購入者Ｘ）について、ユーザ情報記憶部１２１に記憶されている情報に基づいて認証を行う。ユーザ情報記憶部１２１には、決済システム１のユーザとして予め登録されているユーザごとに、ユーザＩＤ及びパスワード等が記憶されている。

30

【００２２】

トランザクション情報受信部１２は、店舗Ｙにおいて２次元コードを読み取った購入者端末２０から送信されるトランザクション情報を受信する。トランザクション情報には、各決済に係るトランザクションを識別するための情報であるトランザクションＩＤ、購入された商品の金額（購入金額）、及び店舗口座情報等を含む。

【００２３】

引き落とし制御部１３は、トランザクション情報受信部１２が受信したトランザクション情報に基づいて、購入金額について、購入者Ｘの銀行口座（以下、「購入者口座」という。）からの引き落としを制御する。

【００２４】

保留部１４は、トランザクション情報受信部１２が受信したトランザクション情報をトランザクション情報記憶部１２２に記憶することで、当該トランザクション情報に係る決済取引を保留する。

40

【００２５】

ワンタイムパスワード生成部１５は、トランザクション情報受信部１２が受信したトランザクション情報に含まれるトランザクションＩＤ等に基づいてワンタイムパスワードを生成し、当該ワンタイムパスワードを購入者端末２０へ送信する。購入者端末２０は、受信したワンタイムパスワードを出力（例えば、表示）する。なお、ワンタイムパスワード生成部１５によって生成されたワンタイムパスワードは、トランザクションＩＤに関連付けられてワンタイムパスワード記憶部１２３に記憶される。

50

【0026】

決済情報受信部16は、店舗端末30へ入力されたワンタイムパスワードと、店舗端末30へ入力された決済を示す情報（購入金額及び店舗口座情報を含む情報。以下「決済情報」という。）を店舗端末30から受信する。すなわち、購入者端末20において出力されたワンタイムパスワードが店舗端末30へ入力されると、店舗端末30は、当該ワンタイムパスワード及び決済情報を仲介装置10へ送信する。当該決済情報には、店舗端末30の秘密鍵を用いた署名が付加される。

【0027】

検証部17は、ワンタイムパスワードと共に受信された決済情報の正当性を、当該ワンタイムパスワード及び当該決済情報に付加された署名等に基づいて検証（判定する）。

10

【0028】

振込制御部18は、当該決済情報の正当性の判定結果が肯定的である場合に、トランザクション情報記憶部122に記憶されているトランザクション情報に基づいて、店舗口座への購入金額の振り込みを制御する。

【0029】

決済取消部19は、該決済情報の正当性の判定結果が否定的である場合に、トランザクション情報記憶部122に記憶されているトランザクション情報に係る決済を取り消すための処理を制御する。具体的には、決済取消部19は、当該トランザクション情報に基づいて、購入者口座への購入金額の振込を制御する。その結果、購入者口座からの購入金額の引き落としは、実質的に行われなかったことになる。

20

【0030】

以下、決済システム1において実行される処理手順について説明する。図4は、第1の実施の形態の決済システム1において実行される処理手順の一例を説明するためのシーケンス図である。

【0031】

店舗Yのレジにおいて、例えば、購入金額が店員によって店舗端末30に対して入力されると（S110）、店舗端末30は、購入金額及び店舗口座情報が構成する情報（以下、「決済情報」という。）を含む2次元コードを液晶ディスプレイ等に表示する（S120）。

【0032】

30

続いて、購入者Xによる購入者端末20の操作に応じ、購入者端末20は、購入者端末20が備えるデジタルカメラ等によって当該2次元コードを読み取る（S130）。続いて、購入者端末20は、当該2次元コードに含まれている決済情報と、当該決済情報に係る決済に関するトランザクション（以下、「トランザクションα」という。）のトランザクションIDとを含むトランザクション情報を仲介装置10へ送信する（S140）。

【0033】

なお、例えば、2次元コードの読み取り前又は読み取り後に、購入者XのユーザID及びパスワードが購入者端末20に対して入力され、購入者端末20は、仲介装置10へ当該ユーザID及びパスワードを送信する。仲介装置10の認証部11は、当該ユーザID及びパスワードについてユーザ情報記憶部121を参照して認証を行う。すなわち、ユーザ情報記憶部121には、決済システム1に対して予め登録されたユーザごとに、ユーザID、パスワード及びユーザの銀行口座を示す情報が記憶されている。認証に成功した場合、認証部11は、購入者XのユーザIDをログインユーザIDとしてメモリ装置103に記憶すると共に、トランザクションIDを生成し、購入者端末20へ送信する。当該トランザクションIDが、ステップS140において購入者端末20から送信されるトランザクション情報に含まれる。また、当該トランザクションIDは、ログインユーザIDに関連付けられて仲介装置10のメモリ装置103に記憶される。

40

【0034】

仲介装置10のトランザクション情報受信部12が当該トランザクション情報を受信すると、引き落とし制御部13は、ログインユーザID（購入者XのユーザID）に係る購

50

入者口座を示す情報を当該トランザクション情報に追加し、当該トランザクション情報をブロックチェーンC aへ送信する（S 1 5 0）。購入者口座を示す情報とは、メモリ装置1 0 3に記憶されているログインユーザIDに関連付けられてユーザ情報記憶部1 2 1に記憶されている銀行口座を示す情報である。

【0 0 3 5】

ブロックチェーンC aは、当該トランザクション情報の受信に応じ、購入者口座からの当該購入金額の引き落としのトランザクションを台帳に記録する（S 1 6 0）。すなわち、購入者Xの購入者口座から購入金額が引き落とされたことを示す情報が台帳に記録される。当該トランザクションの記録後、ブロックチェーンC aは、当該トランザクション情報を仲介装置1 0へ転送する（S 1 7 0）。 10

【0 0 3 6】

続いて、保留部1 4は、当該トランザクション情報を受信すると、当該トランザクション情報をトランザクション情報記憶部1 2 2に記憶しておくことで、トランザクションαの即時的な実行を回避し、エスクロー取引を実現する（S 1 8 0）。

【0 0 3 7】

続いて、ワンタイムパスワード生成部1 5は、トランザクション情報記憶部1 2 2に記憶された当該トランザクション情報のトランザクションID（トランザクションαのトランザクションID）と現在日時とに基づいて、ワンタイムパスワードを生成する（S 1 9 0）。なお、ワンタイムパスワード生成部1 5は、当該ワンタイムパスワードを当該トランザクションIDに関連付けてワンタイムパスワード記憶部1 2 3に記憶しておく。例えば、トランザクションIDを示す文字列と現在日時を示す文字列とを任意の方法で接続することで得られる文字列がワンタイムパスワードとして生成されてもよい。又は、トランザクションIDを示す文字列と現在日時を示す文字列とを含む文字列を可逆変換することで得られる文字列がワンタイムパスワードとして生成されてもよい。ワンタイムパスワードからトランザクションIDが復元又は抽出可能であれば、その他の方法でワンタイムパスワードが生成されてもよい。また、ワンタイムパスワードの生成に現在日時は利用されなくてもよい。但し、現在日時を利用することで、同一のトランザクションIDに対するワンタイムパスワードのランダム性を高めることができる。 20

【0 0 3 8】

続いて、ワンタイムパスワード生成部1 5は、当該ワンタイムパスワードを購入者端末2 0へ送信する（S 2 0 0）。購入者端末2 0は、当該ワンタイムパスワードを受信すると、当該ワンタイムパスワードを購入者端末2 0の液晶ディスプレイ等に表示する（S 2 1 0）。そこで、購入者Xは、当該ワンタイムパスワードを店舗端末3 0に対して入力する（S 2 2 0）。例えば、店舗端末3 0が備えるテンキーを利用して当該ワンタイムパスワードが入力されてもよい。 30

【0 0 3 9】

なお、購入者端末2 0は、受信したワンタイムパスワードをそのまま表示するのではなく、例えば、店舗端末3 0の公開鍵でワンタイムパスワードを暗号化し、暗号化されたワンタイムパスワードを示す2次元コードを生成して、当該2次元コードを液晶ディスプレイ等に表示してもよい。この場合、店舗端末3 0は、2次元コードスキャナによって当該2次元コードを読み取り、当該2次元コードが示す暗号化されたワンタイムパスワードを、店舗端末3 0の秘密鍵で復号することで、ワンタイムパスワードの入力を受け付けてもよい。 40

【0 0 4 0】

ワンタイムパスワードの入力に応じ、店舗端末3 0は、当該ワンタイムパスワードと、店舗端末3 0の秘密鍵で署名した決済情報とを仲介装置1 0へ送信する（S 2 3 0）。

【0 0 4 1】

仲介装置1 0の決済情報受信部1 6が当該ワンタイムパスワード（以下、「受信ワンタイムパスワード」という。）及び当該決済情報を受信すると、検証部1 7は、当該決済情報の正当性を検証（判定）する（S 2 4 0）。具体的には、検証部1 7は、まず、受信ワ 50

ンタイムパスワードからトランザクションIDを復元又は抽出する。検証部17は、復元又は抽出されたトランザクションID（以下、「受信トランザクションID」という。）と一致するトランザクションIDをワンタイムパスワード記憶部123から検索し、検索されたトランザクションIDに関連付けられているワンタイムパスワードと受信ワンタイムパスワードとを比較する。両者が一致し、かつ、決済情報に付加された署名を店舗端末30の公開鍵で検証することができれば、検証部17は、当該決済情報は正当であると判定し、そうでない場合、当該決済情報は不正であると判定する。ここで、当該決済情報が正当であるとは、当該決済情報が、ステップS140において受信されたトランザクション情報と同一の決済に関する情報であることを示す。

【0042】

当該決済情報が正当であると判定されると、振込制御部18は、エスクロー取引の保留を解除する。具体的には、振込制御部18は、トランザクション情報記憶部122に記憶されているトランザクション情報の中で、受信トランザクションIDを含むトランザクション情報に基づいて、店舗口座への購入金額の振り込み（すなわち、購入金額の支払い）の実行指示をブロックチェーンCaに送信すると共に、当該トランザクション情報をトランザクション情報記憶部122から削除する（S250）。ブロックチェーンCaは、店舗口座への購入金額の振り込みを示すトランザクションを台帳に記録する。

【0043】

一方、当該決済情報が正当でないと判定されると、決済取消部19は、決済不可を受信トランザクションIDにログインユーザIDに対応する購入者端末20に通知する（S260）、続いて、決済取消部19は、受信トランザクションIDを含むトランザクション情報に含まれている購入金額について、当該ログインユーザIDに係る購入者口座への振り込みの実行指示をブロックチェーンCaに送信すると共に、当該トランザクション情報をトランザクション情報記憶部122から削除する（S270）。ブロックチェーンCaは、当該購入者口座への当該購入金額の振り込みを示すトランザクションを台帳に記録する。その結果、ステップS160において記録された引き落としは実質的に取り消される。

【0044】

上述したように、第1の実施の形態によれば、購入者端末20から受信したトランザクション情報に基づいて疑いなく購入金額の支払いを実行するのではなく、当該トランザクション情報と店舗端末30から受信した決済情報とが同一の決済に関する情報である場合に、当該支払いが実行される。したがって、購入者端末20が偽の2次元コードを読み取らされた場合であっても、店舗端末30が正当であれば、購入者端末20から受信したトランザクション情報が、店舗端末30から受信した決済情報と異なる決済に関する情報であることを検知することができる。その結果、コード決済における不正請求の発生を抑制することができる。

【0045】

また、本実施の形態では、2次元コードに基づくトランザクションの送信元の購入者端末20に対して、現在日時及びトランザクションIDから生成されたワンタイムパスワードが送信され、当該ワンタイムパスワードが店舗端末30に入力される。店舗端末30は、当該ワンタイムパスワードと共に決済情報を仲介装置10へ送信する。仲介装置10は、当該ワンタイムパスワードに基づいて当該決済情報の正当性を確認する。したがって、店舗端末30が不正な場合であっても、コード決済における不正請求の発生を抑制することができる。

【0046】

次に、第2の実施の形態について説明する。第2の実施の形態では第1の実施の形態と異なる点について説明する。第2の実施の形態において、特に言及されない点については、第1の実施の形態と同様でもよい。

【0047】

第2の実施の形態では、購入者Xが利用する通貨と店舗Yが使用する通貨とが異なる場合について説明する。具体的には、購入者Xは仮想通貨A（以下、単に「通貨A」という

10

20

30

40

50

。)を使用し、店舗Yは仮想通貨B（以下、単に「通貨B」という。）を使用する。

【0048】

図5は、第2の実施の形態における決済システム1の構成例を示す図である。図5の決済システム1では、更に、ブロックチェーンCbがインターネット等のネットワークを介して仲介装置10に接続される。ブロックチェーンCbは、通貨Bによる取引に関するトランザクションを記録する分散台帳である。一方、第2の実施の形態において、ブロックチェーンCaは、通貨Aによる取引に関するトランザクションを記録する分散台帳である。なお、購入者Xが使用する通貨が通貨Aであり、店舗Yが使用する通貨が通貨Bであることは、予め仲介装置10に設定されている。

【0049】

図6は、第2の実施の形態の決済システム1において実行される処理手順の一例を説明するためのシーケンス図である。図6中、図4と同一ステップには同一ステップ番号を付し、その説明は省略する。

【0050】

店舗Yのレジにおいて、例えば、通貨Bでの購入金額が店員によって店舗端末30に対して入力されると（S110a）、店舗端末30は、購入金額及び店舗口座情報が構成する決済情報を含む2次元コードを店舗端末30の液晶ディスプレイ等に表示する（S120a）。したがって、ステップS140aでは、通貨Bでの購入金額を含むトランザクション情報が購入者端末20から仲介装置10へ送信される。

【0051】

仲介装置10のトランザクション情報受信部12が当該トランザクション情報を受信すると、引き落とし制御部13は、当該トランザクション情報に含まれている購入金額について、通貨Bから通貨Aへの金額に換算する（S145）。すなわち、第2の実施の形態において、仲介装置10は、通貨の換算機能を有する。その結果、ステップS150では、通貨Aでの購入金額を含むトランザクション情報がブロックチェーンCaへ送信される。

【0052】

ブロックチェーンCaにおいて購入者口座からの通貨Aでの購入金額の引き落としのトランザクションを台帳に記録されると（S160、S170）、引き落とし制御部13は、ブロックチェーンCaにおいて予め用意されている仲介装置10の指示でブロックチェーンCaの通貨Aのプール口座へ通貨Aでの購入金額の振り込みを実行する（S175）。

【0053】

続いて、購入金額については通貨Aが使用されてステップS180～S240が実行される。

【0054】

ステップS240において、決済情報が正当であると判定されると、振込制御部18は、トランザクション情報記憶部122に記憶されているトランザクション情報の中で、受信トランザクションIDを含むトランザクション情報に含まれている購入金額について、通貨Aから通貨Bへの換算を実行する（S241）。

【0055】

続いて、振込制御部18は、ブロックチェーンCbにおいて予め用意されている仲介装置10からの指示で、ブロックチェーンCbの通貨Bのプール口座からの通貨Bでの購入金額の引き落としを実行する（S175）。続いて、振込制御部18は、当該トランザクション情報に基づいて、店舗口座への通貨Bの購入金額の支払いの実行指示をブロックチェーンCbに送信すると共に、当該トランザクション情報をトランザクション情報記憶部122から削除する（S250a）。

【0056】

なお、ステップS270は、通貨Aに基づいて実行される。

【0057】

なお、第2の実施の形態における仲介装置10は、例えば、「F U J I T S U J O U R N A L / 2 0 1 8 年 1 月 2 4 日 通貨間の取引を安全に支えるブロックチェーン新技術

10

20

30

40

50

(<https://blog.global.fujitsu.com/jp/2018-01-24/01/>)」において開示されている、コネクションチェーンを用いて実現されてもよい。

【0058】

上述したように、第2の実施の形態によれば、購入者が使用する通貨と店舗が使用する通貨とが異なる場合であっても、第1の実施の形態と同様の効果を得ることができる。

【0059】

なお、上記各実施の形態において、トランザクション情報は、第1の情報の一例である。決済情報は、第2の情報の一例である。ワンタイムパスワードは、第3の情報の一例である。仲介装置10は、情報処理装置の一例である。トランザクション情報受信部12は、第1の受信部の一例である。決済情報受信部16は、第2の受信部の一例である。検証部17は、判定部の一例である。振込制御部18は、制御部の一例である。ワンタイムパスワード生成部15は、送信部の一例である。

【0060】

以上、本発明の実施の形態について詳述したが、本発明は斯かる特定の実施形態に限定されるものではなく、請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

【符号の説明】

【0061】

1	決済システム
10	仲介装置
11	認証部
12	トランザクション情報受信部
13	引き落とし制御部
14	保留部
15	ワンタイムパスワード生成部
16	決済情報受信部
17	検証部
18	振込制御部
19	決済取消部
20	購入者端末
30	店舗端末
100	ドライブ装置
101	記録媒体
102	補助記憶装置
103	メモリ装置
104	CPU
105	インタフェース装置
121	ユーザ情報記憶部
122	トランザクション情報記憶部
123	ワンタイムパスワード記憶部
Ca	ブロックチェーン
Cb	ブロックチェーン

10

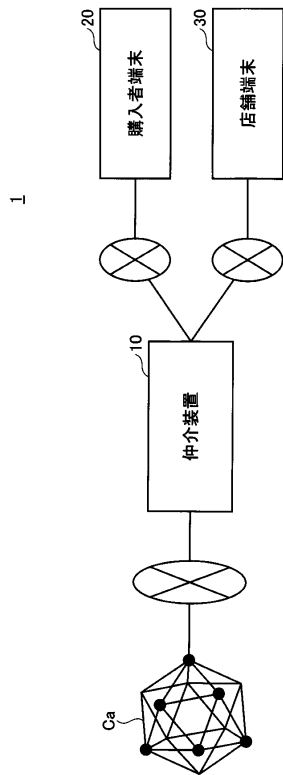
20

30

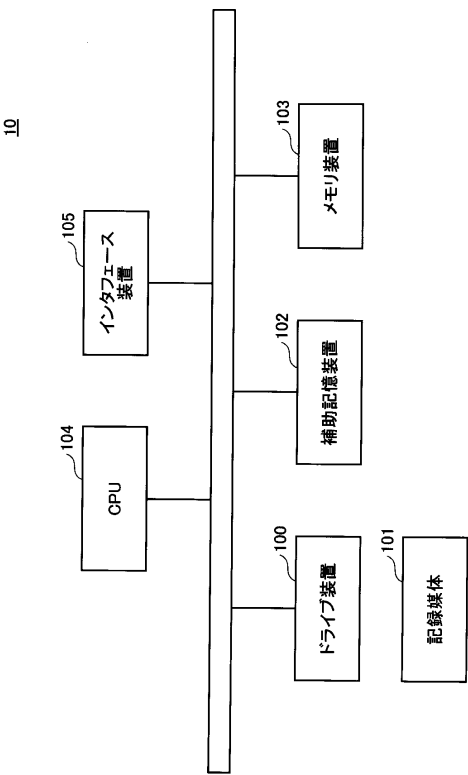
40

50

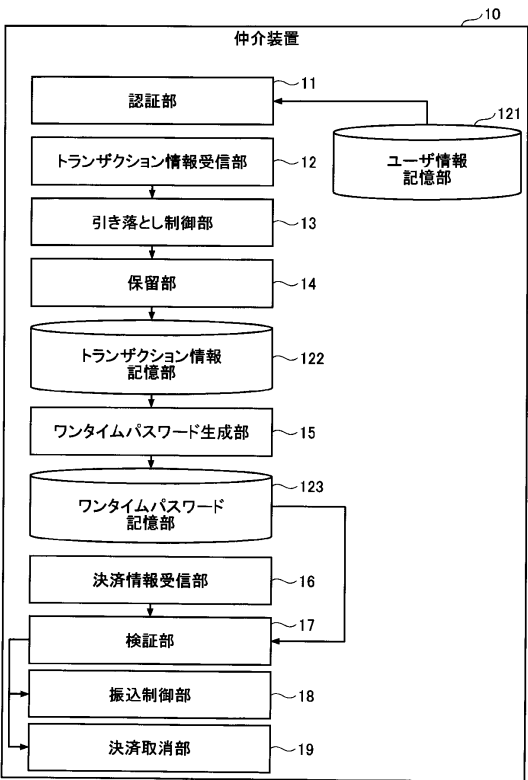
【図面】
【図 1】



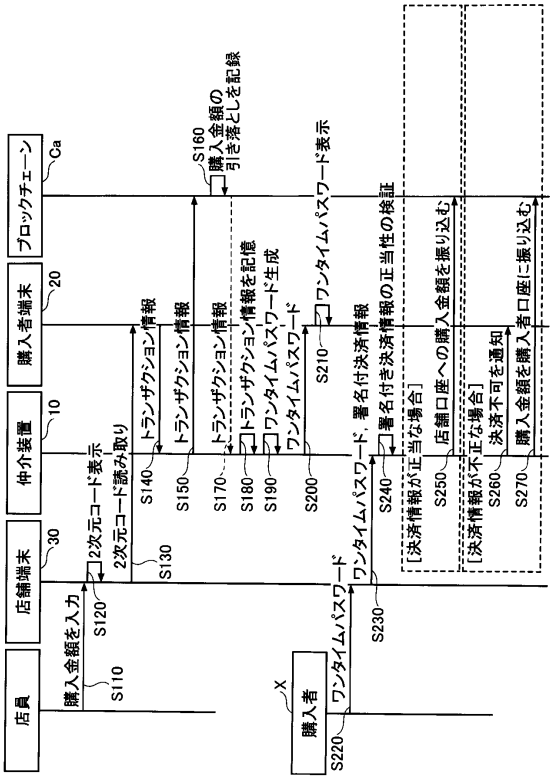
【図 2】



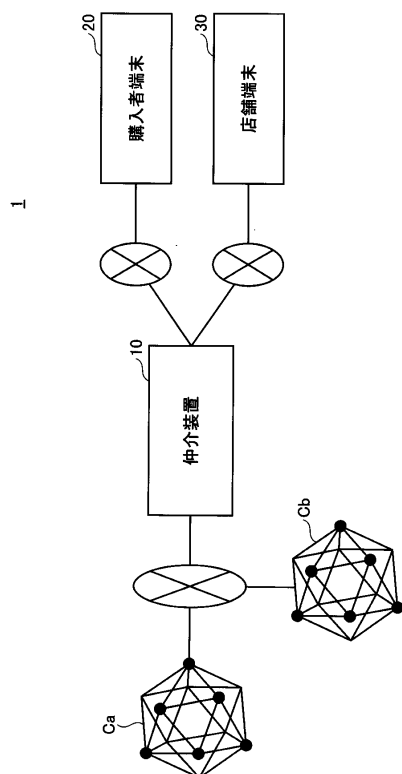
【図 3】



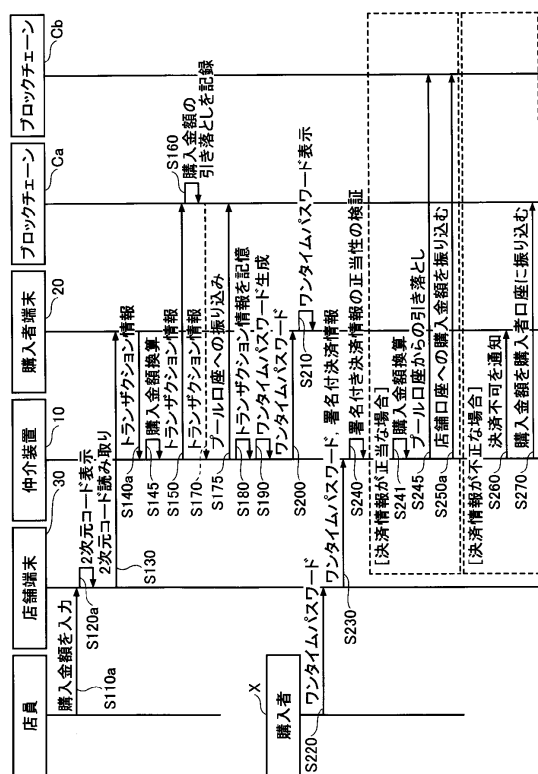
【図 4】



【図 5】



【図 6】



フロントページの続き

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

審査官 田付 徳雄

- (56)参考文献 国際公開第2001/088785 (WO, A1)
特開2012-216155 (JP, A)
特開2018-088076 (JP, A)
特開2002-163584 (JP, A)
特開2005-301896 (JP, A)
米国特許出願公開第2015/0058145 (US, A1)
- (58)調査した分野 (Int.Cl., DB名)
G06Q 10/00 - 99/00