

明 細 書

発明の名称：通貨管理システム及び電子署名装置

技術分野

[0001] 本発明は、通貨の管理及び電子署名に関する。

背景技術

[0002] 通貨を管理するシステムが提案されている（特許文献1 参照）。

先行技術文献

特許文献

[0003] 特許文献1：特許第6316530号

発明の概要

発明が解決しようとする課題

[0004] 本発明の一実施形態では、法定通貨を管理対象に含む、セキュリティに優れた通貨管理システム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

[0005] 本発明は、次の一実施形態を含む。

[0006] トランザクション情報管理装置、口座情報管理装置、及び通貨情報管理装置を備えた通貨管理システムであって、

前記トランザクション情報管理装置は、ユーザ端末から、第1 トランザクション情報を受信し、

前記口座情報管理装置は、前記トランザクション情報管理装置から、第2 トランザクション情報を受信し、

前記トランザクション情報管理装置は、前記口座情報管理装置から、第3 トランザクション情報を受信し、

前記通貨情報管理装置は、前記トランザクション情報管理装置から、第4 トランザクション情報を受信し、

前記トランザクション情報管理装置は、前記通貨情報管理装置から、第5 トランザクション情報を受信し、

前記トランザクション情報管理装置は、前記ユーザ端末に対して、第6トランザクション情報を送信し、

前記トランザクション情報管理装置は、前記第1乃至第6トランザクション情報を自装置内に記憶し、

前記口座情報管理装置は、前記トランザクション情報管理装置から、前記第1乃至第6トランザクション情報を受信し、これらを自装置内に記憶し、

前記通貨情報管理装置は、前記トランザクション情報管理装置から、前記第1乃至第6トランザクション情報を受信し、これらを自装置内に記憶する通貨管理システム。

発明の効果

[0007] 本発明の一実施形態によれば、法定通貨を管理対象に含む、セキュリティに優れた通貨管理システムを提供することができる。

図面の簡単な説明

[0008] [図1A]実施形態1に係る通貨管理システムの構成例を示す図である。

[図1B]トランザクション情報の一例を示す図である。

[図1C]口座情報の一例を示す図である。

[図1D]通貨情報の一例を示す図である。

[図1E]実施形態1に係る通貨管理システムの動作例を示す図である。

[図1F]トランザクション情報が記憶される様子を説明する図である。

[図1G]口座情報が更新される様子を説明する図である。

[図1H]通貨情報が更新される様子を説明する図である。

[図2A]実施形態2に係る通貨管理システムの構成例を示す図である。

[図2B]電子署名が付与されたトランザクション情報の一例を示す図である。

[図3]実施形態3におけるトランザクション情報の一例を示す図である。

[図4]電子署名が付与された口座情報の一例を示す図である。

[図5]電子署名が付与された通貨情報の一例を示す図である。

[図6]電子署名装置の構成例を示す図である。

発明を実施するための形態

[0009] [実施形態１に係る通貨管理システム１００]

図１Ａは、実施形態１に係る通貨管理システム１００の構成例を示す図である。図１Ａに示すように、実施形態１に係る通貨管理システム１００は、トランザクション情報管理装置１１０、口座情報管理装置１２０、及び通貨情報管理装置１３０を備えている。

[0010] (通貨管理システム１００)

通貨管理システム１００は、通貨を管理するシステムである。本実施形態では、すべての通貨に通貨番号を付すことにより、通貨を管理している。通貨の種類は限定されない。通貨は法定通貨であってもよいし、法定されていない通貨であってもよい。また、通貨は暗号通貨であってもよいし、暗号化されていない通貨であってもよい。また、通貨は、国家が管理するものであってもよいし、特定の団体や企業などが管理するものであってもよい。また、通貨の一例には、ポイントや地域振興券が含まれる。

[0011] (通貨の送金)

通貨の管理には、通貨の送金が含まれる。本実施形態において、通貨の送金は、口座情報Ｂ及び通貨情報Ｃを変更することにより行われる。本明細書では、このような口座情報Ｂや通貨情報Ｃを変更するにあたり生じた要求及び応答をトランザクションといい、このトランザクションの履歴をトランザクション情報Ａという。トランザクション情報Ａは、口座情報Ｂ及び通貨情報Ｃを変更するにあたり生じた要求及び応答の履歴ということもできる。

[0012] (トランザクション情報管理装置１１０)

トランザクション情報管理装置１１０は、トランザクション情報Ａを管理する装置である。トランザクション情報管理装置１１０の一例には、サーバ装置が含まれる。

[0013] (トランザクション情報Ａ)

トランザクション情報Ａを用いれば、口座情報Ｂ及び通貨情報Ｃの正しい変更の履歴を辿ることができるため、口座情報Ｂや通貨情報Ｃの不正な変更を発見し、不正に変更された口座情報Ｂや通貨情報Ｃを正しい内容へとリカ

バリーすることができる。ただし、その逆に、口座情報Bや通貨情報Cを用いてトランザクション情報Aの不正な変更を発見し、不正に変更されたトランザクション情報Aを正しい内容へとリカバリーすることはできない。そこで、本実施形態では、トランザクション情報管理装置110だけでなく、口座情報管理装置120及び通貨情報管理装置130にも、トランザクション情報Aが記憶されるものとした。このようにすれば、トランザクション情報管理装置110、口座情報管理装置120、及び通貨情報管理装置130のうちの1つの装置に記憶されるトランザクション情報Aが不正に変更された場合でも、残り2つの装置に記憶されるトランザクション情報Aを用いることにより、当該不正を発見し、不正に変更されたトランザクション情報Aを正しい内容へとリカバリーすることができる。例えば、トランザクション情報管理装置110内のトランザクション情報Aが不正に変更された場合であれば、口座情報管理装置120内のトランザクション情報Aと通貨情報管理装置130内のトランザクション情報Aを用いて、トランザクション情報管理装置110内のトランザクション情報Aを正しい内容に戻すことができる。したがって、本実施形態によれば、トランザクション情報A、口座情報B、及び通貨情報Cのいずれが不正に変更されたとしても、その不正を発見して、不正に変更された情報を正しい内容へとリカバリーできる。例えば、口座情報管理装置120内の口座情報Bが不正に変更された場合には、トランザクション情報管理装置110、口座情報管理装置120、及び通貨情報管理装置130内にそれぞれ記憶されているトランザクション情報Aのいずれか1つ以上を用いて、不正に変更された口座情報Bを正しい内容に戻すことができる。また、上記のとおり、例えば、トランザクション情報管理装置110内のトランザクション情報Aが不正に変更された場合であれば、口座情報管理装置120内のトランザクション情報Aと通貨情報管理装置130内のトランザクション情報Aを用いて、トランザクション情報管理装置110内のトランザクション情報Aを正しい内容に戻すことができる。さらに、例えば、トランザクション情報管理装置110内のトランザクション情報Aと

通貨情報管理装置 130 内の通貨情報 C が不正に変更された場合には、口座情報管理装置 120 内のトランザクション情報 A と通貨情報管理装置 130 内のトランザクション情報 A を用いて、トランザクション情報管理装置 110 内のトランザクション情報 A を正しい内容へと戻し、また、口座情報管理装置 120 内のトランザクション情報 A と通貨情報管理装置 130 内のトランザクション情報 A（あるいは、さらに、正しい内容へとリカバリーされたトランザクション情報管理装置 110 内のトランザクション情報 A）の 1 つ以上を用いて、通貨情報管理装置 130 内の通貨情報 C を正しい内容へと戻すことができる。よって、本実施形態によれば、法定通貨を管理対象に含む、セキュリティに優れた通貨管理システム 100 を提供することができる。

[0014] 図 1 B は、トランザクション情報 A の一例を示す図である。図 1 B に示すように、トランザクション情報 A には、例えば、トランザクション番号、トランザクション種別、送金元口座番号、送金先口座番号、送金額、及び日時が含まれる。これらの情報は、例えばテーブル形式により、互いに対応付けて記憶することができる。具体的には、これらの情報は、テーブルの同じ行の異なる列に格納して記憶することができる。これらの情報は一例であるので、トランザクション情報 A には、上記の情報以外の情報が含まれていてもよい。また、送金元口座番号、送金先口座番号、及び送金額は、トランザクション情報 A に含まれていなくてもよい。上記のとおり、本実施形態によれば、これらの情報を、トランザクション情報管理装置 110、口座情報管理装置 120、及び通貨情報管理装置 130 がそれぞれ記憶する。

[0015] <トランザクション番号>

トランザクション番号は、トランザクションを特定する番号である。トランザクション番号の一例には、例えば数列や文字列が含まれる。

[0016] <トランザクション種別>

トランザクション種別は、トランザクションの種別を特定する番号である。トランザクションの種別の一例には、送金要求、口座情報確認要求、口座情報確認応答、通貨情報確認要求、通貨情報確認応答、及び送金応答が含ま

れる。

[0017] <送金元口座番号>

送金元口座番号は、送金元の口座番号を特定する番号である。送金元口座番号の一例には、数列や文字列が含まれる。送金元口座番号は、トランザクション情報に電子署名を付与する場合であって、当該電子署名の付与や検証に秘密鍵暗号方式を用いる場合（各装置の間でユーザや各装置の暗号鍵を共有する場合）には、送金元となるユーザの暗号鍵を特定できる情報（例：鍵番号）であることが好ましい。また、送金元口座番号は、トランザクション情報に電子署名を付与する場合であって、当該電子署名の付与や検証に公開鍵暗号方式を用いる場合には、送金元となるユーザの公開鍵を特定できる情報であることが好ましい。

[0018] <送金先口座番号>

送金先口座番号は、送金先の口座番号を特定する番号である。送金先口座番号の一例には、数列や文字列が含まれる。送金元口座番号の場合と同様に、送金先口座番号は、送金先となるユーザの暗号鍵を特定できる情報（例：鍵番号）や、送金先となるユーザの公開鍵を特定できる情報であることが好ましい。

[0019] <送金額>

送金額は、送金する額を特定する情報である。送金額の一例には数列が含まれる。

[0020] <日時>

日時は、トランザクションが生じた日時である。日時には、例えば、トランザクション情報Aの送信時刻である。

[0021] （口座情報管理装置120）

口座情報管理装置120は、口座情報Bを管理する装置である。口座情報管理装置120の一例には、サーバ装置が含まれる。口座情報管理装置120は、例えばネットワークを介して、トランザクション情報管理装置110に接続されている。ネットワークの一例には、インターネットやイントラネ

ットが含まれる。

[0022] (口座情報B)

口座情報Bとは、口座と残高の関係を特定する情報である。

[0023] 図1Cは口座情報Bの一例を示す図である。図1Cに示すように、口座情報Bには、口座番号、残高、及び最終更新日時が含まれる。これらの情報は、例えばテーブル形式により、互いに対応付けて記憶することができる。具体的には、これらの情報は、テーブルの同じ行の異なる列に格納して記憶することができる。これらの情報は一例であるので、口座情報Bには、上記の情報以外の情報が含まれていてもよい。

[0024] <口座番号>

口座番号は、口座を特定する番号である。口座番号の一例には、数列や文字列が含まれる。

[0025] <残高>

残高は、口座が保有している通貨の額を特定する情報である。残高の一例には、数列が含まれる。

[0026] <最終更新日時>

最終更新日時は、口座情報Bが最後に更新された日時である。

[0027] (通貨情報管理装置130)

通貨情報管理装置130は、通貨情報Cを管理する装置である。通貨情報管理装置130の一例には、例えばサーバ装置が含まれる。通貨情報管理装置130は、例えばネットワークを介して、トランザクション情報管理装置110に接続されている。通貨情報管理装置130は、例えばネットワークを介して、口座情報管理装置120に接続されていてもよいし、されていなくてもよい。ネットワークの一例には、インターネットやイントラネットが含まれる。

[0028] (通貨情報C)

通貨情報Cとは、通貨を管理するための情報をいう。

[0029] 図1Dは通貨情報Cの一例を示す図である。図1Dに示すように、通貨情

報Cには、通貨番号、通貨種別、通貨価値、口座番号、及び最終更新日時が含まれる。これらの情報は、例えばテーブル形式により、互いに対応付けて記憶することができる。具体的には、これらの情報は、テーブルの同じ行の異なる列に格納して記憶することができる。これらの情報は一例であるので、通貨情報Cには、上記の情報以外の情報が含まれていてもよい。また、通貨価値は、通貨情報Cに含まれていなくてもよい。

[0030] <通貨番号>

通貨番号は、通貨を特定する番号である。上記したとおり、本実施形態では、すべての通貨に通貨番号が付されている。

[0031] <通貨種別>

通貨種別は、通貨の種別を特定する情報である。通貨の種別の一例には、日本円、USドル、ユーロ、人民元、特定の地域や企業などにおいて交換価値を持つポイントが含まれる。なお、1種類の通貨のみを管理する場合、通貨種別は通貨情報に含まれていなくてもよい。また、通貨番号が通貨種別を特定できる情報である場合には（例：「yen1111」や「1111 yen」などのように、通貨の種別を特定する情報（yen）が通貨番号の一部として通貨番号の先頭や末尾に含まれる場合）、通貨種別は通貨情報に含まれていなくてもよい。

[0032] <通貨価値>

通貨価値は、1つの通貨が持つ価値を特定する情報である。例えば、2つの通貨が発行されており、1つ目の通貨には通貨番号1が付与され、2つ目の通貨には通貨番号2が付与されている場合を想定する。この場合、通貨番号1に対応付けて、通貨種別として日本円が、通貨価値として500が記憶されている場合、通貨番号1の通貨は500円の価値がある。また、通貨番号2に対応付けて、通貨種別としてUSドルが、通貨価値として100が記憶されている場合、通貨番号2の通貨は100USドルの価値がある。

[0033] <口座番号>

口座番号は、通貨番号で特定される通貨を保有するユーザの口座番号であ

る。口座番号の一例には、数列や文字列が含まれる。

[0034] <最終更新日時>

最終更新日時は、通貨情報Cが最後に更新された日時である。

[0035] (ユーザ端末210、220)

トランザクション情報管理装置110には、例えばネットワークを介して、複数のユーザ端末210、220が接続される。ユーザ端末210、220の一例には、スマートフォン、ラップトップコンピュータ、デスクトップコンピュータが含まれる。ネットワークの一例には、インターネットやイントラネットが含まれる。

[0036] トランザクション情報管理装置110は、ユーザ端末210、220に対するインターフェースとして機能している。口座情報管理装置120や通貨情報管理装置130は、トランザクション情報管理装置110を介することなく、ユーザ端末210、220とデータの送受信を行うことはできない。ユーザ端末210、220からの要求はトランザクション情報管理装置110が受信する。トランザクション情報管理装置110は、ユーザ端末210、220からの要求に基づいて、口座情報管理装置120や通貨情報管理装置130に要求を送信する。また、口座情報管理装置120や通貨情報管理装置130からの応答はトランザクション情報管理装置110が受信する。そして、それらの応答に基づいて、トランザクション情報管理装置110は、ユーザ端末210、220に対して応答を送信する。

[0037] (実施形態1に係る通貨管理システム100の動作例)

図1Eは、実施形態1に係る通貨管理システム100の動作例を示す図である。以下、図1Eを参照しつつ、実施形態1に係る通貨管理システム100の動作例を説明する。以下の例では、ユーザ端末210のユーザが持つ口座番号が1であり、ユーザ端末210のユーザが持つ口座番号が2であり、ユーザ端末210からの送金要求に応じて、口座番号1の口座から口座番号2の口座へ500円が送金されるものとする。

[0038] (ステップS101)

まず、トランザクション情報管理装置 110 は、ユーザ端末 210 から、第 1 トランザクション情報 a 1 を受信する。第 1 トランザクション情報 a 1 はトランザクション情報 A の一例である。第 1 トランザクション情報 a 1 の一例には、例えば送金要求や口座発行要求が含まれる。本実施形態では、第 1 トランザクション情報 a 1 は送金要求であるものとする。

[0039] (ステップ S 102)

次に、口座情報管理装置 120 は、トランザクション情報管理装置 110 から、第 2 トランザクション情報 A を受信する。第 2 トランザクション情報 a 2 はトランザクション情報 A の一例である。第 2 トランザクション情報 a 2 の一例には、口座情報更新要求や口座情報確認要求が含まれる。第 2 トランザクション情報 a 2 が口座情報更新要求である場合、口座情報管理装置 120 は、第 2 トランザクション情報 a 2 を受信した後、口座情報 B を更新する。これにより、口座情報管理装置 120 に記憶されている口座情報 B は、例えば、図 1 G に示す更新前から更新後へと変化する。また、第 2 トランザクション情報 a 2 が口座情報確認要求である場合、口座情報管理装置 120 は、第 2 トランザクション情報 a 2 を受信した後、口座情報 B を確認し、例えば、送金額以上の残高が口座に保有されているかどうかを確認する。

[0040] (ステップ S 103)

次に、トランザクション情報管理装置 110 は、口座情報管理装置 120 から、第 3 トランザクション情報 a 3 を受信する。第 3 トランザクション情報 a 3 はトランザクション情報 A の一例である。第 3 トランザクション情報 a 3 の一例には、例えば、口座情報更新応答や口座情報確認応答が含まれる。口座情報更新応答は、例えば、口座情報が正常に更新されたかどうかを示す応答である。口座情報確認応答は、例えば、送金額以上の残高が口座に保有されているかどうかの確認結果を示す応答である。

[0041] (ステップ S 104)

次に、通貨情報管理装置 130 は、トランザクション情報管理装置 110 から、第 4 トランザクション情報 a 4 を受信する。第 4 トランザクション情

報 a 4 はトランザクション情報 A の一例である。第 4 トランザクション情報 a 4 は、例えば通貨情報更新要求や通貨情報確認要求である。第 4 トランザクション情報 a 4 が通貨情報更新要求である場合、通貨情報管理装置 130 は、第 4 トランザクション情報 a 4 を受信した後、通貨情報 C を更新する。これにより、通貨情報管理装置 130 に記憶されている通貨情報 C は、例えば、図 1 H に示す更新前から更新後へと変化する。また、第 4 トランザクション情報 a 4 が通貨情報確認要求である場合、通貨情報管理装置 130 は、第 4 トランザクション情報 a 4 を受信した後、通貨情報 C を確認し、例えば、送金元のユーザの口座番号に対応付けられた通貨が存在するかどうかを確認する。

[0042] (ステップ S 105)

次に、トランザクション情報管理装置 110 は、通貨情報管理装置 130 から、第 5 トランザクション情報 a 5 を受信する。第 5 トランザクション情報 a 5 はトランザクション情報 A の一例である。第 5 トランザクション情報 a 5 の一例には、通貨情報更新応答や通貨情報確認応答が含まれる。通貨情報更新応答は、例えば、通貨情報が正常に更新されたかどうかを示す応答である。通貨情報確認応答は、例えば、送金元のユーザの口座番号に対応付けられた通貨が存在するかどうかの確認結果を示す応答である。

[0043] (ステップ S 106)

次に、トランザクション情報管理装置 110 は、ユーザ端末 210 に対して、第 6 トランザクション情報 a 6 を送信する。第 6 トランザクション情報 a 6 はトランザクション情報 A の一例である。第 6 トランザクション情報 a 6 の一例には、送金応答や口座発行応答が含まれる。本実施形態では、第 6 トランザクション情報 a 6 は送金応答であるものとする。送金応答は例えば送金が正常に行われたかどうかを示す応答である。

[0044] (ステップ S 107)

次に、トランザクション情報管理装置 110 は、第 1 乃至第 6 トランザクション情報を自装置内に記憶する。これにより、トランザクション情報管理

装置 110 に記憶されるトランザクション情報 A は、例えば、図 1 F に示す記憶前から記憶後へと変化する。

[0045] (ステップ S 108、S 109)

次に、口座情報管理装置 120 は、トランザクション情報管理装置 110 から、第 1 乃至第 6 トランザクション情報を受信し、これらを自装置内に記憶する。これにより、口座情報管理装置 120 に記憶されるトランザクション情報 A は、例えば、図 1 F に示す記憶前から記憶後へと変化する。

[0046] 口座情報管理装置 120 は、ステップ S 102 の後、口座情報 B の更新ではなく口座情報 B の確認を実行した場合、トランザクション情報管理装置 110 から、第 1 乃至第 6 トランザクション情報を受信した後に、口座情報 B を更新する。これにより、口座情報管理装置 120 に記憶される口座情報 B は、例えば、図 1 G に示す更新前から更新後へと変化する。

[0047] (ステップ S 110、S 111)

次に、通貨情報管理装置 130 は、トランザクション情報管理装置 110 から、第 1 乃至第 6 トランザクション情報を受信し、これらを自装置内に記憶する。これにより、通貨情報管理装置 130 に記憶されるトランザクション情報 A は、例えば、図 1 H に示す記憶前から記憶後へと変化する。

[0048] 通貨情報管理装置 130 は、ステップ S 104 の後、通貨情報 C の更新ではなく通貨情報 C の確認を実行した場合、トランザクション情報管理装置 110 から、第 1 乃至第 6 トランザクション情報を受信した後に、通貨情報 C を更新する。これにより、通貨情報管理装置 130 に記憶される通貨情報 C は、例えば、図 1 H に示す更新前から更新後へと変化する。

[0049] なお、本実施形態では、トランザクション情報 A が、トランザクション情報管理装置 110 (ステップ S 107)、口座情報管理装置 120 (ステップ S 108)、通貨情報管理装置 130 (ステップ S 110) の順に記憶されるものとしたが、トランザクション情報 A が記憶される順序 (ステップ S 107、108、110 の順序) は問わない。

[0050] 以上説明したとおり、トランザクション情報 A を用いれば、口座情報 B 及

び通貨情報Cの正しい変更の履歴を辿ることができるため、口座情報Bや通貨情報Cの不正な変更を発見し、不正に変更された口座情報Bや通貨情報Cを正しい内容へとリカバリーすることができる。ただし、その逆に、口座情報Bや通貨情報Cを用いてトランザクション情報Aの不正な変更を発見し、不正に変更されたトランザクション情報Aを正しい内容へとリカバリーすることはできない。そこで、本実施形態では、トランザクション情報管理装置110だけでなく、口座情報管理装置120及び通貨情報管理装置130にも、トランザクション情報Aが記憶されるものとした。このようにすれば、トランザクション情報管理装置110、口座情報管理装置120、及び通貨情報管理装置130のうちの1つの装置に記憶されるトランザクション情報Aが不正に変更された場合でも、残り2つの装置に記憶されるトランザクション情報Aを用いることにより、当該不正を発見し、不正に変更されたトランザクション情報Aを正しい内容へとリカバリーすることができる。例えば、トランザクション情報管理装置110内のトランザクション情報Aが不正に変更された場合であれば、口座情報管理装置120内のトランザクション情報Aと通貨情報管理装置130内のトランザクション情報Aを用いて、トランザクション情報管理装置110内のトランザクション情報Aを正しい内容に戻すことができる。したがって、本実施形態によれば、トランザクション情報A、口座情報B、及び通貨情報Cのいずれが不正に変更されたとしても、その不正を発見して、不正に変更された情報を正しい内容へとリカバリーできる。例えば、口座情報管理装置120内の口座情報Bが不正に変更された場合には、トランザクション情報管理装置110、口座情報管理装置120、及び通貨情報管理装置130内にそれぞれ記憶されているトランザクション情報Aのいずれか1つ以上を用いて、不正に変更された口座情報Bを正しい内容に戻すことができる。また、上記のとおり、例えば、トランザクション情報管理装置110内のトランザクション情報Aが不正に変更された場合であれば、口座情報管理装置120内のトランザクション情報Aと通貨情報管理装置130内のトランザクション情報Aを用いて、トランザクシ

ン情報管理装置 110 内のトランザクション情報 A を正しい内容に戻すことができる。さらに、例えば、トランザクション情報管理装置 110 内のトランザクション情報 A と通貨情報管理装置 130 内の通貨情報 C が不正に変更された場合には、口座情報管理装置 120 内のトランザクション情報 A と通貨情報管理装置 130 内のトランザクション情報 A を用いて、トランザクション情報管理装置 110 内のトランザクション情報 A を正しい内容へと戻し、また、口座情報管理装置 120 内のトランザクション情報 A と通貨情報管理装置 130 内のトランザクション情報 A（あるいは、さらに、正しい内容へとリカバリーされたトランザクション情報管理装置 110 内のトランザクション情報 A）の 1 つ以上を用いて、通貨情報管理装置 130 内の通貨情報 C を正しい内容へと戻すことができる。よって、本実施形態によれば、法定通貨を管理対象に含む、セキュリティに優れた通貨管理システム 100 を提供することができる。

[0051] [実施形態 2 に係る通貨管理システム 400]

図 2 A は実施形態 2 に係る通貨管理システム 400 の構成例を示す図である。図 2 A に示すように、実施形態 2 に係る通貨管理システム 400 では、トランザクション情報管理装置 110、口座情報管理装置 120、及び通貨情報管理装置 130 それぞれが、電子署名装置 310 乃至 330 を備えている。また、ユーザ端末 210、220 も電子署名装置 340、350 をそれぞれ備えている。実施形態 2 では、これら電子署名装置 310 乃至 350 を用いて作成された電子署名がトランザクション情報 A に対して付与される点で、実施形態 1 と相違する。電子署名の一例には、ハッシュ関数を用いて算出されるハッシュ値が含まれる。電子署名装置 310 乃至 350 は、耐タンパ性を有していることが好ましい。

[0052] トランザクション情報 A に電子署名が付与される場合には、トランザクション情報 A に付与されている電子署名を検証することにより、トランザクション情報 A が不正に変更されているかどうかを発見することができる。このため、たとえば、トランザクション情報管理装置 110、口座情報管理装置

120、及び通貨情報管理装置130のうちの2つの装置におけるトランザクション情報Aが不正に変更されたとしても、残る1つの装置におけるトランザクション情報Aを用いて、不正に変更された2つの装置におけるトランザクション情報Aをリカバリーすることができる。例えば、トランザクション情報管理装置110と口座情報管理装置120におけるトランザクション情報Aが不正に変更された場合を想定する。この場合、トランザクション情報管理装置110と口座情報管理装置120においては、それぞれのトランザクション情報Aに付与されている電子署名を検証することにより、不正を発見することができる。その一方、通貨情報管理装置130に記憶されているトランザクション情報Aについては、これに付与されている電子署名を検証することにより、不正に変更されていないと判断することができる。このため、通貨情報管理装置130に記憶されているトランザクション情報Aを用いて、トランザクション情報管理装置110と口座情報管理装置120に記憶されているトランザクション情報Aを正しい内容へとリカバリーすることができる。

[0053] 電子署名装置310乃至350は、電子署名の作成及び検証を実行する装置である。電子署名の作成方法及び検証方法は、特に限定されない。これらの方法は、例えば、公開鍵暗号方式により行うことができるほか、秘密鍵暗号方式により行うこともできる。実施形態2では、公開鍵暗号方式により行われるものとする。

[0054] 図2Bは、電子署名が付与されたトランザクション情報Aの一例を示す図である。図2Bに示すように、本実施形態では、個々のトランザクション情報Aに電子署名が付与されている。第nトランザクション情報Aには第n電子署名が付与される。ただし、nは1以上の整数である。個々のトランザクション情報Aに付与される電子署名は、個々のトランザクション情報Aを送信する装置の暗号鍵を用いて作成される。例えば、上記した第1トランザクション情報a1に付与される電子署名は、ユーザ端末210の暗号鍵を用いて作成される。また、第2、第4、第6トランザクション情報a2、a4、

a 6 に付与される電子署名は、トランザクション情報管理装置 1 1 0 の暗号鍵を用いて作成される。また、第 3 トランザクション情報 a 3 に付与される電子署名は、口座情報管理装置 1 2 0 の暗号鍵を用いて作成される。また、第 5 トランザクション情報 a 5 に付与される電子署名は、通貨情報管理装置 1 3 0 の暗号鍵を用いて作成される。なお、ユーザ端末 2 1 0 の暗号鍵の一例には、ユーザ端末 2 1 0 を操作したり所有したりなどするユーザの暗号鍵が含まれる。また、各装置の暗号鍵の一例には、本実施形態の運営者が各装置用に所有したり割り当てたりなどする暗号鍵が含まれる。

[0055] 以上説明したとおり、本実施形態によれば、トランザクション情報管理装置 1 1 0、口座情報管理装置 1 2 0、及び通貨情報管理装置 1 3 0 のうちの 2 つの装置におけるトランザクション情報 A が不正に変更されたとしても、残る 1 つの装置におけるトランザクション情報 A を用いて、不正に変更された 2 つの装置におけるトランザクション情報 A をリカバリーすることができる。よって、少なくとも 1 つの装置に記憶されるトランザクション情報 A が正しい内容で保護されていれば、口座情報 B と通貨情報 C を含めた、すべての情報を正しい内容へとリカバリーすることができる。例えば、トランザクション情報管理装置 1 1 0 内のトランザクション情報 A 以外のすべての情報が不正に変更された場合、つまり、口座情報管理装置 1 2 0 内の口座情報 B 及びトランザクション情報 A、通貨情報管理装置 1 3 0 内の通貨情報 C 及びトランザクション情報 A が不正に変更された場合を想定する。このような場合であっても、トランザクション情報 A に付与されている電子署名を用いて、トランザクション情報管理装置 1 1 0 内のトランザクション情報 A が正しい内容であり、口座情報管理装置 1 2 0 内と通貨情報管理装置 1 3 0 内のトランザクション情報 A が不正に変更されていることを判断することができる。したがって、トランザクション情報管理装置 1 1 0 内のトランザクション情報 A を用いて、残り 2 つの装置内のトランザクション情報 A を正しい内容に戻すことができる。また、トランザクション情報管理装置 1 1 0 内のトランザクション情報 A (あるいは、さらに、口座情報管理装置 1 2 0 と通貨情

報管理装置 130 内における正しい内容にリカバリーされたトランザクション情報 A) を用いて、口座情報管理装置 120 内の口座情報 B と通貨情報管理装置 130 内の通貨情報 C が不正に変更された事実を発見することができる。そして、トランザクション情報管理装置 110 内のトランザクション情報 A (あるいは、さらに、口座情報管理装置 120 と通貨情報管理装置 130 内における正しい内容にリカバリーされたトランザクション情報 A) を用いて、口座情報管理装置 120 内の口座情報 B と通貨情報管理装置 130 内の通貨情報 C を正しい内容に戻すことができる。

[0056] [実施形態 3 に係る通貨管理システム]

実施形態 3 に係る通貨管理システムは、第 n 電子署名が、第 n トランザクション情報 A と第 $n-1$ 電子署名を用いて作成される点で、実施形態 2 に係る通貨管理システム 100 と相違する。また、実施形態 3 に係る通貨管理システムは、第 n トランザクション情報 A に付与されている第 n 電子署名の検証が、第 n トランザクション情報 A と第 $n-1$ 電子署名を用いて作成される電子署名を、第 n 電子署名と比較することにより行われる点で、実施形態 2 に係る通貨管理システムと相違する。ここで、「 $n-1$ 」とは、 n マイナス 1、つまり、 n より 1 つ小さい数を意味する。実施形態 3 では、例えば、第 3 トランザクション情報 a_3 に付与する第 3 電子署名は、第 3 トランザクション情報 a_3 と第 2 電子署名を用いて作成することができる。また、例えば、第 3 トランザクション情報 a_3 に付与されている第 3 電子署名は、第 3 トランザクション情報 a_3 と第 2 電子署名を用いて作成される電子署名を、当該付与されている第 3 電子署名と比較することにより検証することができる。

[0057] 本実施形態によれば、図 3 に示すように、第 4 電子署名 (#3) であれば、第 4 トランザクション情報 a_4 (#1) と第 3 電子署名 (#2) を用いて作成される。例えば、第 4 トランザクション情報 a_4 (#1) と第 3 電子署名 (#2) とトランザクション情報管理装置 110 の暗号鍵を用いて所定の演算を行うことにより、第 4 電子署名 (#3) を作成することができる。ま

た、第4電子署名（＃3）の検証は、第4トランザクション情報a4（＃1）と第3電子署名（＃2）を用いて実行することができる。例えば、第4トランザクション情報（＃1）と第3電子署名（＃2）とトランザクション情報管理装置110の暗号鍵を用いて所定の演算を行うことにより検証用の電子署名を作成し、この検証用の電子署名が第4トランザクション情報a4に付与されている第4電子署名（＃3）と一致する場合には、第4トランザクション情報a4に正しい電子署名が付与されているものと判断することができる。所定の演算の一例には、ハッシュ関数を用いた計算が含まれる。

[0058] なお、第0電子署名は初期値として予め定められた値であるものとする。

[0059] 本実施形態によれば、第n電子署名を変更するためには、第n-1電子署名を変更しなくてはならず、第n-1電子署名を変更するためには、第n-2電子署名を変更しなければならず、このような関係が第1電子署名までに続くため、第1電子署名から変更しなければ、第n電子署名を変更できなくなる。したがって、トランザクション情報Aが不正に変更される可能性を低減させることができる。

[0060] なお、本実施形態の場合、第n電子署名の検証には第n-1電子署名が必要となる。このため、上記した図1Eに示す例では、第2トランザクション情報a2とともに、第1電子署名を特定することができる情報、例えば、第1電子署名が付与されている第1トランザクション情報a1が送信されることが好ましい。このようにすれば、口座情報管理装置120は、第2電子署名を検証する際に必要な第1電子署名を迅速に利用することができる。

[0061] 同様に、本実施形態においては、第4トランザクション情報a4とともに、第3電子署名を特定することができる情報、例えば、第3電子署名が付与されている第3トランザクション情報a3が送信されることが好ましい。このようにすれば、通貨情報管理装置130は、第4電子署名を検証する際に必要な第3電子署名を迅速に利用することができる。

[0062] 同様に、本実施形態においては、第6トランザクション情報a6とともに、第5電子署名を特定することができる情報、例えば、第5電子署名が付与

されている第5トランザクション情報a5が送信されることが好ましい。このようにすれば、ユーザ端末210は、第6電子署名を検証する際に必要な第5電子署名を迅速に利用することができる。

[0063] なお、第1電子署名の検証には第0電子署名が必要となるが、第0電子署名は初期値である。このため、トランザクション情報管理装置110が予めこれを記憶しているものとしておけば、第1トランザクション情報とともに第0電子署名を特定可能な情報が送信されなくても、トランザクション情報管理装置110は、第1電子署名を検証する際に必要な第0電子署名を迅速に利用することができる。

[0064] また、第3電子署名の検証には第2電子署名が必要となるが、第2署名はトランザクション情報管理装置110により付与された電子署名である。このため、トランザクション情報管理装置110が第2電子署名の作成後、これを自装置内に記憶しているものとするれば、第3トランザクション情報とともに第2電子署名を特定可能な情報（例：第2トランザクション情報a2）が送信されなくても、トランザクション情報管理装置110は、第3電子署名を検証する際に必要な第2電子署名を迅速に利用することができる。

[0065] また、第5電子署名の検証には第4電子署名が必要となるが、第4署名はトランザクション情報管理装置110により付与された電子署名である。このため、トランザクション情報管理装置110が第4電子署名の作成後、これを自装置内に記憶しているものとするれば、第5トランザクション情報とともに第4電子署名を特定可能な情報（例：第4トランザクション情報a4）が送信されなくても、トランザクション情報管理装置110は、第5電子署名を検証する際に必要な第4電子署名を迅速に利用することができる。

[0066] [実施形態4に係る通貨管理システム]

図4は電子署名が付与された口座情報Bの一例を示す図である。実施形態4に係る通貨管理システムは、図4に示すように、口座情報Bに電子署名が付与される点で、実施形態1に係る通貨管理システム100と相違する。口座情報Bに付与される電子署名は、電子署名が付与される口座情報Bと口座

情報管理装置 120 の暗号鍵とを用いて作成することができる。例えば、口座番号 2 で特定される口座情報 B であれば、当該口座番号 2 で特定される口座情報 B と口座情報管理装置 120 の暗号鍵とを用いて所定の演算を行うことにより、口座番号 2 で特定される口座情報 B に付与する電子署名を算出することができる。所定の演算の一例には、ハッシュ関数を用いた計算が含まれる。

[0067] 口座情報 B に対する不正は、上記のとおり、トランザクション情報 A により発見し、リカバリーすることができる。しかし、トランザクション情報 A を用いて発見する場合、トランザクション情報 A をさかのぼって、口座情報 B の変更履歴を一から確認していかなければならない。例えば、トランザクション情報が 100 個ある場合、1 番目のトランザクション情報から順に口座情報 B が正しく変更されているかどうかを辿っていかなければならない。このため、多数のトランザクションが積み重なっている場合、例えば通貨の送金は何回も行われた後になると、口座情報 B が不正に変更されているかどうかの判断に膨大な処理が必要となり、不正の発見が遅れてしまう虞がある。また、このように不正の発見に膨大な処理が必要となると、トランザクション情報 A を用いた口座情報 B の不正発見処理の実行を頻繁に行うことが困難となる。そこで、本実施形態では、口座情報 B に電子署名が付与されるものとしている。このようにすれば、口座情報 B に付与された電子署名を検証することにより、トランザクション情報 A を用いなくても、口座情報 B が不正に変更されているかどうかを発見することができるため、口座情報 B が不正に変更された場合には、これを早期に発見することができる。不正を発見した後は、トランザクション情報 A を用いて、口座情報 B を正しい内容へとリカバリーすることができる。

[0068] [実施形態 5 に係る通貨管理システム]

図 5 は電子署名が付与された通貨情報 C の一例を示す図である。実施形態 5 に係る通貨管理システムは、図 5 に示すように、通貨情報 C に電子署名が付与される点で、実施形態 1 に係る通貨管理システム 100 と相違する。通

貨情報Cに付与される電子署名は、電子署名が付与される通貨情報Cと通貨情報管理装置130の暗号鍵とを用いて作成することができる。例えば、通貨番号3で特定される通貨情報Cであれば、当該通貨番号3で特定される通貨情報Cと通貨情報管理装置130の暗号鍵とを用いて所定の演算を行うことにより、通貨番号3で特定される通貨情報Cに付与する電子署名を算出することができる。所定の演算の一例には、ハッシュ関数を用いた計算が含まれる。

[0069] 本実施形態によれば、実施形態4で説明した口座情報Bに電子署名を付与する場合と同様に、トランザクション情報Aを用いることなく、通貨情報Cに対する不正を早期に発見することができる。通貨情報Cに不正が発見された場合には、トランザクション情報Aを用いて、通貨情報Cを正しい内容へとリカバリーすることができる。

[0070] [実施形態6に係る通貨管理システム]

図6は電子署名装置310の構成例を示す図である。図6に示すように、電子署名装置310は、暗号鍵と権限とを対応付けて記憶し、暗号鍵を用いた処理のうち、権限に応じた処理のみを実行することができることが好ましい。電子署名装置320乃至350も、権限の内容が異なる点を除いて、電子署名装置310と同様に構成することができる。実施形態2では、電子署名装置310乃至350が、公開鍵暗号方式に基づいて電子署名の作成・検証を行うものとした。しかし、公開鍵暗号方式の場合は、公開鍵と秘密鍵があり、公開鍵は非常に長いものとなる（例：2048ビット）。他方、秘密鍵方式の場合、秘密鍵（例：256ビット）で暗号と検証を行う。このため、秘密鍵方式の場合は、長い公開鍵を使わずに済むため、電子署名の作成・付与や検証の時間を短縮できる。ただし、秘密鍵方式を採用する場合は、複数の電子署名装置の間で暗号鍵（秘密鍵）を共有しなければならない。このため、ある暗号鍵で作成された電子署名の検証だけしか行なわない電子署名装置であっても、その暗号鍵を用いて電子署名の作成までできてしまうことになり、セキュリティ上の問題がある。例えば、上記の例でいうと、トラン

ザクション情報管理装置 110 は、トランザクション情報管理装置 110 の暗号鍵に加えて、ユーザ端末 210、220、口座情報管理装置 120、及び通貨情報管理装置 130 の暗号鍵も所有することになる。しかし、トランザクション情報管理装置 110 において、ユーザ端末 210、220、口座情報管理装置 120、及び通貨情報管理装置 130 の暗号鍵は、電子署名の検証に用いられるに過ぎない。にもかかわらず、トランザクション情報管理装置 110 は、ユーザ端末 210、220、口座情報管理装置 120、及び通貨情報管理装置 130 の暗号鍵を用いて、電子署名を作成できてしまう。換言すると、トランザクション情報管理装置 110 は、ユーザ端末 210、220、口座情報管理装置 120、及び通貨情報管理装置 130 になりすますることができてしまう。そこで、本実施形態では、電子署名装置 310 乃至 350 が秘密鍵方式を採用し、暗号鍵（秘密鍵）が複数の電子署名装置 310 乃至 350 で共有されるものとする。ただし、本実施形態では、セキュリティ上の問題が生じないように、共有される複数の暗号鍵（秘密鍵）に権限が付与されるものとし、電子署名装置 310 乃至 350 は、複数の暗号鍵（秘密鍵）それぞれをその権限に応じた処理でしか使用できないものとする。このようにすれば、セキュリティを確保しつつ、電子署名の作成・付与や検証の時間を短縮できる。例えば、トランザクション情報管理装置 110 の電子署名装置 310 であれば、図 6 に示すように、トランザクション情報管理装置 110 の暗号鍵だけでなく、ユーザ端末 210、220、口座情報管理装置 120、及び通貨情報管理装置 130 の暗号鍵を有している。しかし、トランザクション情報管理装置 110 の暗号鍵に対しては付与及び検証の権限が与えられており、その他の装置の暗号鍵に対しては検証の権限のみが与えられているものとする。このようにすれば、トランザクション情報管理装置 110 の電子署名装置 310 は、トランザクション情報管理装置 110 の暗号鍵を用いては、電子署名の作成・付与及び検証の双方を実行できるが、他の装置の暗号鍵を用いては、電子署名の検証しか実行できない。なお、本実施形態で説明した電子署名装置、つまり、暗号鍵と権限とを対応付けて

記憶し、暗号鍵を用いた処理（例：電子署名の作成や検証）のうち、権限に応じた処理のみを実行する電子署名装置（例：暗号鍵Eに対応付けて記憶されている権限が電子署名の検証のみである電子署名装置は、当該暗号鍵Eを用いて電子署名の検証を実行することはできるが、当該暗号鍵Eを用いて電子署名の作成を実行することはできない。他方、暗号鍵Eに対応付けて記憶されている権限が電子署名の作成及び検証である電子署名装置は、当該暗号鍵Eを用いた電子署名の作成及び検証のいずれをも実行することができる。）

）は、トランザクション情報管理装置110、口座情報管理装置120、通貨情報管理装置130、及びユーザ端末210、220それぞれが備える電子署名装置310乃至350として好ましく用いることができる。しかし、当該電子署名装置は、通貨を管理するシステムの使用に限定されず、秘密鍵方式を採用する、上記で説明した装置やシステム以外の様々な装置やシステムに広く用いることができる。

[0071] 以上、実施形態について説明したが、これらの説明によって本発明は何ら限定されるものではない。

符号の説明

- [0072] 100、400 通貨管理システム
- 110 トランザクション情報管理装置
- 120 口座情報管理装置
- 130 通貨情報管理装置
- 210 ユーザ端末
- 220 ユーザ端末
- 310乃至350 電子署名装置
- A トランザクション情報
- B 口座情報
- C 通貨情報

請求の範囲

- [請求項1] トランザクション情報管理装置、口座情報管理装置、及び通貨情報管理装置を備えた通貨管理システムであって、
- 前記トランザクション情報管理装置は、ユーザ端末から、第1トランザクション情報を受信し、
- 前記口座情報管理装置は、前記トランザクション情報管理装置から、第2トランザクション情報を受信し、
- 前記トランザクション情報管理装置は、前記口座情報管理装置から、第3トランザクション情報を受信し、
- 前記通貨情報管理装置は、前記トランザクション情報管理装置から、第4トランザクション情報を受信し、
- 前記トランザクション情報管理装置は、前記通貨情報管理装置から、第5トランザクション情報を受信し、
- 前記トランザクション情報管理装置は、前記ユーザ端末に対して、第6トランザクション情報を送信し、
- 前記トランザクション情報管理装置は、前記第1乃至第6トランザクション情報を自装置内に記憶し、
- 前記口座情報管理装置は、前記トランザクション情報管理装置から、前記第1乃至第6トランザクション情報を受信し、これらを自装置内に記憶し、
- 前記通貨情報管理装置は、前記トランザクション情報管理装置から、前記第1乃至第6トランザクション情報を受信し、これらを自装置内に記憶する通貨管理システム。
- [請求項2] 第 n トランザクション情報には第 n 電子署名が付与される請求項1に記載の通貨管理システム。ただし、 n は1以上の整数である。
- [請求項3] 第 n 電子署名は、第 n トランザクション情報と第 $n-1$ 電子署名を用いて作成される請求項2に記載の通貨管理システム。ただし、第0電子署名は初期値として予め定められた値である。

- [請求項4] 第 n トランザクション情報に付与されている第 n 電子署名の検証は、第 n トランザクション情報と第 $n-1$ 電子署名を用いて作成される電子署名を、第 n 電子署名と比較することにより行われる請求項3に記載の通貨管理システム。
- [請求項5] 前記口座情報管理装置は、口座情報に、前記口座情報と前記口座情報管理装置の暗号鍵とを用いて作成された電子署名を対応付けて記憶する請求項1乃至4のいずれか一項に記載の通貨管理システム。
- [請求項6] 前記通貨情報管理装置は、通貨情報に、前記通貨情報と前記通貨情報管理装置の暗号鍵とを用いて作成された電子署名を対応付けて記憶する請求項1乃至5のいずれか一項に記載の通貨管理システム。
- [請求項7] 暗号鍵と権限とを対応付けて記憶し、
前記暗号鍵を用いた処理のうち、前記権限に応じた処理のみを実行することができる電子署名装置。