

明 細 書

発明の名称：電子通貨基盤を実現するための方法およびシステム

技術分野

[0001] 本開示は、電子通貨基盤を実現するための方法およびシステムに関する。

背景技術

[0002] 現実の貨幣による取引だけではなく、様々な仮想通貨を用いた取引が行われている。このような仮想通貨の一例として、ビットコインと称される仮想通貨が知られている。例えば、日本国特許第5871347号公報（特許文献1）は、マイナーに対して報酬を無限に支払い続けることが可能であり、価値の変動の少ない仮想通貨を提供する構成を開示する。

先行技術文献

特許文献

[0003] 特許文献1：日本国特許第5871347号公報

発明の概要

発明が解決しようとする課題

[0004] ビットコインは、暗号証明（c r y p t o g r a p h i c p r o o f s）を行うネットワークを基盤とする。そのため、暗号証明には大量のコミットメントが必要であり、多くのリソースが消費される。また、仮想通貨の取引は高コストで処理が遅く、仮想通貨を直接渡すようなこともできない。

[0005] 本開示は、ネットワークなどのリソースを大きく消費することなく、安全な通貨流通を実現できる電子通貨基盤を提供する。

課題を解決するための手段

[0006] 本開示のある実施の形態に従えば、電子通貨基盤を実現するためのコンピュータによって実行される方法が提供される。方法は、予め定められた財産的価値を付与された電子ファイルを生成するステップと、電子ファイルに中央銀行の秘密鍵を用いて生成された第1の署名データを追加するステップと、第1の署名データが追加された後、電子ファイルを第1のエンティティが

ら第2のエンティティに移転するために、第1のエンティティの秘密鍵を用いて生成された第2の署名データを電子ファイルに追加するステップと、電子ファイルの内容の少なくとも一部を台帳に記録するステップと、少なくとも台帳に記録された内容に基づいて、電子ファイルの不正な移転の有無を判断するステップとを含む。

[0007] 電子ファイルの不正な移転の有無を判断するステップは、電子ファイルに関連付けて、第1のエンティティから複数のエンティティに電子ファイルをそれぞれ移転する記録が存在するか否かを判断するステップを含んでもよい。

[0008] 方法は、第1のエンティティから第2のエンティティに電子ファイルを送信した後に、第2のエンティティから第2のエンティティの秘密鍵を用いて生成された第3の署名データが追加された電子ファイルを受信すると、第1のエンティティが格納している電子ファイルを削除するステップをさらに含んでもよい。

[0009] 方法は、第2のエンティティが、第1のエンティティの公開鍵を用いて、電子ファイルに含まれる第2の署名データを検証するステップをさらに含んでもよい。

[0010] 電子ファイルは、有効期限の設定を含んでもよい。方法は、電子ファイルを第1のエンティティから第2のエンティティに移転する前に、第1のエンティティおよび第2のエンティティの少なくとも一方が電子ファイルの有効期限が切れていないことを検証するステップをさらに含んでもよい。

[0011] 方法は、第2のエンティティが第1のエンティティから電子ファイルを受信した後に実行される、電子ファイルの内容と台帳に記録された内容とを照合するステップをさらに含んでもよい。

[0012] 方法は、電子ファイルの有効期限が切れている場合に、中央銀行が当該電子ファイルを回収するステップをさらに含んでもよい。

[0013] 本開示の別の実施の形態に従えば、電子通貨基盤を実現するためのシステ

ムが提供される。システムは、予め定められた財産的価値を付与された電子ファイルを生成するための手段と、電子ファイルに中央銀行の秘密鍵を用いて生成された第1の署名データを追加するための手段と、第1の署名データが追加された後、電子ファイルを第1のエンティティから第2のエンティティに移転するために、第1のエンティティの秘密鍵を用いて生成された第2の署名データを電子ファイルに追加するための手段と、電子ファイルの内容の少なくとも一部を記録するための台帳と、少なくとも台帳に記録された内容に基づいて、電子ファイルの不正な移転の有無を判断する手段とを含む。

発明の効果

- [0014] 本開示によれば、ネットワークなどのリソースを大きく消費することなく、安全な通貨流通を実現できる。

図面の簡単な説明

- [0015] [図1]本実施の形態に従う電子通貨基盤の構成例を示す模式図である。
- [図2]本実施の形態に従う電子通貨基盤において用いられる情報処理装置のハードウェア構成例を示す模式図である。
- [図3]本実施の形態に従う電子通貨基盤において用いられるモバイル装置のハードウェア構成例を示す模式図である。
- [図4]本実施の形態に従う電子通貨基盤における電子通貨の流通の一例を説明するための図である。
- [図5]本実施の形態に従う電子通貨のデータ構造の一例を示す模式図である。
- [図6]本実施の形態に従う電子通貨基盤における信頼チェーンの一例を示す模式図である。
- [図7]本実施の形態に従う電子通貨の信頼コントロールセクション（信頼認証セクション）のデータ構造の一例を示す模式図である。
- [図8]本実施の形態に従う電子通貨のトランザクションコントロールセクションのトランザクションデータのデータ構造の一例を示す模式図である。
- [図9]本実施の形態に従う電子通貨のスペシャルセクションのチェックポイントデータのデータ構造の一例を示す模式図である。

[図10]本実施の形態に従う電子通貨基盤の台帳のデータ構造一例を示す模式図である。

[図11]本実施の形態に従う電子通貨基盤におけるエンティティ間の電子通貨の移転の基本的な処理手順例を説明するための図である。

[図12]本実施の形態に従う電子通貨基盤におけるプランニングを含む電子通貨の移転の基本的な処理手順例を説明するための図である。

[図13]本実施の形態に従う電子通貨基盤における電子通貨の流通の処理手順を示すシーケンス図である。

[図14]本実施の形態に従う電子通貨基盤における電子通貨の流通の別の処理手順を示すシーケンス図である。

[図15]本実施の形態に従う電子通貨基盤の台帳における処理手順の一例を示すフローチャートである。

[図16]本実施の形態に従う電子通貨基盤の台帳における整合性の検証の一例を説明するための図である。

発明を実施するための形態

[0016] 本開示に係る実施の形態について、図面を参照しながら詳細に説明する。
なお、図中の同一または相当部分については、同一符号を付してその説明は繰り返さない。

[0017] < A. 用語 >

本明細書において、「通貨」は、国家によって強制通用力が認められている通貨（法定通貨）に加えて、法定通貨と同様の価値を有する電子マネーを包含する。また、「通貨」は、仮想通貨または暗号資産と称される財産的価値を包含することもある。

[0018] < B. 概要 >

本開示は、電子通貨基盤を実現するためのコンピュータによって実行される方法およびシステムを含む。まず、本実施の形態に従う電子通貨基盤 1 の概要について説明する。電子通貨基盤 1 において、紙幣および硬貨などの物理的な通貨と同じ財産的価値を有する電子通貨 10 が流通する。電子通貨 1

0は、デジタル通貨と称することもできる。電子通貨10の各々は、1つの電子ファイルであってもよい。

[0019] 電子通貨基盤1において、電子通貨10は、中央銀行が認める通貨の単位で、電子署名により真正性および流通の信頼性が担保される。電子通貨10の各々に与えられる財産的価値は、物理的な通貨と同様に、予め定められた額面のうちいずれかであってもよいし、物理的な通貨より多くの種類の額面が存在してもよい。

[0020] 図1は、本実施の形態に従う電子通貨基盤1の構成例を示す模式図である。図1を参照して、電子通貨基盤1は、例えば、1または複数の発行局2と、中央銀行3と、1または複数の金融機関4と、1または複数の販売者5と、1または複数の消費者6とを含む。電子通貨基盤1において、中央銀行3が電子通貨10の真正性を担保するエンティティ（主体）である。

[0021] 発行局2は、電子通貨10を発行する機関である。発行局2は、中央銀行3により信頼された電子通貨の発行者に相当する。発行局2は、秘密鍵22Aと公開鍵22Bとからなる鍵ペア22を有している。発行局2は、予め定められた条件に従って、または、中央銀行3などからの指示に従って、電子通貨10の実体である電子ファイルを生成する。

[0022] 生成される電子ファイルには、予め定められた財産的価値が付与されている。生成される電子ファイル（電子通貨11）は、後述するような初期データを含んでもよい。生成された電子通貨11は、発行局2から中央銀行3に移転する（ステップS1）。発行局2は、物理的な通貨が流通する基盤との対比において、印刷局または造幣局に相当する。

[0023] 中央銀行3は、市中への電子通貨10の提供、市中から電子通貨10の回収、市中に流通する電子通貨10の総量の管理などを行う。中央銀行3は、連邦準備銀行（Federal Reserve Bank）であってもよい。中央銀行3は、秘密鍵23Aと公開鍵23Bとからなる鍵ペア23を有している。電子通貨11が市中へ提供される前に、中央銀行3の公開鍵23Bを用いて生成された署名データが電子通貨11に追加される（電子通貨1

2)。電子通貨12は、例えば、1または複数の金融機関4を介して市中に提供される（ステップS2）。

[0024] このように、中央銀行3（のコンピュータ）は、電子通貨10（電子ファイル）に中央銀行3の秘密鍵23Aを用いて生成された署名データ（第1の署名データ）を追加する。

[0025] 図1に示す構成例において、発行局2が予め定められた財産的価値を付与された電子通貨10（電子ファイル）を生成する。電子通貨10（電子ファイル）の生成は、発行局2（のコンピュータ）に限らず、中央銀行3（のコンピュータ）であってもよいし、中央銀行3が委任した別の機関（のコンピュータ）であってもよい。

[0026] 金融機関4は、販売者5および消費者6への電子通貨10の提供、販売者5および消費者6から電子通貨10の回収、販売者5および消費者6に対する各種決済などを行う。金融機関4は、秘密鍵24Aと公開鍵24Bとからなる鍵ペア24を有している。

[0027] 例えば、消費者6が自身の預金口座から指定された金額の引き出しを金融機関4に要求すると、金融機関4は、指定された金額の財産的価値を有する電子通貨13を消費者6に提供する（ステップS3）。金融機関4は、秘密鍵24Aと公開鍵24Bとからなる鍵ペア24を有している。金融機関4は、後述のトランザクションデータに加えて、電子通貨10の移転を証明するための情報（以下、「チェックポイントデータ」とも称す。）を電子通貨12に追加する（チェックポイントデータ31）。後述するように、チェックポイントデータ31は、金融機関4の秘密鍵24Aを用いて生成された署名データを含む。

[0028] 電子通貨10に含まれるチェックポイントデータは、電子通貨10のこれまでの流通経路を完全に保証するエビデンスとなる。そのため、チェックポイントデータには、電子通貨10を取り扱うエンティティの署名データが追加される。チェックポイントデータ31に含まれる署名データは、電子通貨10の移転に対する否認防止性を担保する。

- [0029] チェックポイントデータ 3 1 が追加された電子通貨 1 3 は、消費者 6 に提供される。消費者 6 が自身の預金口座から指定された金額の引き出す際には、ATM (Automatic Teller Machine) などが用いられてもよいし、金融機関 4 のコンピュータと消費者 6 のコンピュータとがネットワークを介して電子通貨 1 0 を受け取るようにしてもよい。
- [0030] 消費者 6 は、商品およびサービスの購入の対価として、金融機関 4 から提供された電子通貨 1 3 を販売者 5 に提供する。例えば、消費者 6 は、販売者 5 が購入を希望する商品またはサービスに対する対価の金額を販売者 5 に通知する。消費者 6 は、通知された金額を了承すると、トランザクションデータに加えて、チェックポイントデータ 3 2 を了承した金額の財産的価値を有する電子通貨 1 3 に追加する。
- [0031] チェックポイントデータ 3 2 が追加された電子通貨 1 4 は、消費者 6 から販売者 5 に移転する（ステップ S 4）。チェックポイントデータ 3 2 は、消費者 6 の秘密鍵 2 6 A を用いて生成された署名データを含む。
- [0032] 電子通貨 1 0 が有している財産的価値は、発行局 2 により発行される時に決定されている場合もある。そのため、消費者 6 は、対価と同一の財産的価値を有する電子通貨 1 0 を所有しているとは限らない。このような場合には、物理的な通貨で支払うのと同様に、消費者 6 は、必要な対価の金額になるように、一度の取引で複数の電子通貨 1 0 を販売者 5 に送信するようにしてもよい。あるいは、販売者 5 が「おつり」に相当する電子通貨 1 0 を消費者 6 に送信するようにしてもよい。
- [0033] 販売者 5 は、秘密鍵 2 5 A と公開鍵 2 5 B とからなる鍵ペア 2 4 を有している。販売者 5 は、任意のタイミングで、所有している電子通貨 1 0 を換金でき、または、所有している電子通貨 1 0 が有する財産的価値を自身の預金口座に入金できる。例えば、販売者 5 は、金融機関 4 が換金または入金を了承すると、トランザクションデータに加えて、チェックポイントデータ 3 3 を電子通貨 1 4 に追加する。
- [0034] チェックポイントデータ 3 3 が追加された電子通貨 1 5 は、販売者 5 から

金融機関4に移転する（ステップS5）。チェックポイントデータ33は、販売者5の秘密鍵25Aを用いて生成された署名データを含む。

[0035] 金融機関4は、受け取った電子通貨15が有している財産的価値に相当する物理的な通貨を販売者5に提供し、または、受け取った電子通貨15が有している財産的価値を販売者5の預金口座の残高に加算する。

[0036] 消費者6も同様に、所有している電子通貨10を換金でき、または、所有している電子通貨10が有する財産的価値を自身の預金口座に入金できる。

[0037] このように、金融機関4（のコンピュータ）、販売者5（のコンピュータ）、消費者6（のコンピュータ）の各々は、中央銀行3が中央銀行3の秘密鍵23Aを用いて生成された署名データ（第1の署名データ）を電子通貨10に追加した後、当該電子通貨10を自身から他のエンティティに移転するために、自身の秘密鍵を用いて生成された署名データ（第2の署名データ）を当該電子ファイルに追加する。

[0038] 電子通貨基盤1において、電子通貨10には有効期限（有効日時）が設定されている。電子通貨10に設定された有効期限が切れると（設定された有効日時が到来すると）、それ以降、電子通貨10は市中を流通できない。有効期限が切れた電子通貨10は、中央銀行3に戻される。中央銀行3（または、発行局2）は、新たに電子通貨10を発行する。有効期限は、中央銀行3による電子通貨10の流通ポリシーなどに基づいて任意に決定してもよい。例えば、有効期限の長さは、電子通貨10の発行から6ヶ月程度に設定してもよい。

[0039] 中央銀行3が市中に提供した電子通貨10は、所定の条件が満たされるまで、金融機関4、販売者5および消費者6などの間を流通することになる。所定の条件は、例えば、電子通貨10の有効期限が切れた場合、および、電子通貨10のチェックポイントデータを記録する領域が不足する場合などを含む。

[0040] 電子通貨10が市中を流通することができなくなると、中央銀行3は、電子通貨10を回収する。このように、電子通貨10の有効期限が切れている

場合に、中央銀行 3 は、当該電子通貨 10 を回収する。

- [0041] 金融機関 4 は、任意のタイミングで、所有している電子通貨 10 が有する財産的価値を中央銀行 3 にある自身の預金口座に入金できる。例えば、金融機関 4 は、中央銀行 3 が入金を了承すると、チェックポイントデータ 34 を電子通貨 15 に追加する。チェックポイントデータ 34 は、金融機関 4 の秘密鍵 24 A を用いて生成された署名データを含む。
- [0042] チェックポイントデータ 34 を含む電子通貨 16 は、金融機関 4 から中央銀行 3 に移転する（ステップ S 6）。中央銀行 3 は、受け取った電子通貨 16 が有している財産的価値を金融機関 4 の預金口座の残高に加算する。
- [0043] 説明の便宜上、金融機関 4 から消費者 6 への電子通貨 10 の移転、消費者 6 から販売者 5 への電子通貨 10 の移転、および、販売者 5 から金融機関 4 への電子通貨 10 の移転が順次実行される例を説明したが、一般的には、販売者 5 と消費者 6 との間では、電子通貨 10 を媒介とする取引が繰り返される。そのため、電子通貨 10 は、1 または複数の販売者 5 と 1 または複数の消費者 6 との間で、複数回に亘って移転することもある。
- [0044] また、金融機関 4 は、販売者 5 または消費者 6 から受け取った電子通貨 10 を中央銀行 3 に移転するのではなく、要求に応じて、販売者 5 または消費者 6 に再度提供してもよい。
- [0045] 電子通貨基盤 1 は、台帳 8 を含む。台帳 8 は、電子通貨 10 の取引または移転に関する履歴情報を格納する。図 1 に示す構成例において、台帳 8 は、1 または複数の発行局 2 と、中央銀行 3 と、1 または複数の金融機関 4 と、1 または複数の販売者 5 とからネットワークアクセス可能になっている。台帳 8 は、発行局 2 および／または中央銀行 3 によって管理されてもよい。
- [0046] 図 1 には、1 つの台帳 8 を図示するが、複数のサーバで構成される分散型台帳を採用してもよい。また、マスターとなる台帳 8 を用意するとともに、クローンまたはスレーブとなる 1 または複数の台帳 8 を用意してもよい。
- [0047] 1 または複数の発行局 2 と、中央銀行 3 と、1 または複数の金融機関 4 と、1 または複数の販売者 5 との各々は、他のエンティティから電子通貨 10

を受け取った場合、および、電子通貨10を他のエンティティに提供した場合などに、当該取引の内容を示す情報を台帳8に格納する。台帳8は、電子通貨10（電子ファイル）の内容の少なくとも一部を記録する。なお、すべての販売者5が台帳8にネットワークアクセス可能でなくてもよい。

[0048] 説明を簡素化するために、図1には、発行局2から中央銀行3への電子通貨10の移転、および、中央銀行3から金融機関4への電子通貨10の移転については、電子通貨10にチェックポイントデータが追加されていないが、電子通貨10がエンティティ間を移転する場合には、電子通貨10に必ずチェックポイントデータが追加されてもよい。

[0049] 電子通貨基盤1の少なくとも一部のエンティティは、少なくとも台帳8に記録された内容に基づいて、電子通貨10（電子ファイル）の不正な移転の有無を判断できる。仮想通貨とは異なり、任意のタイミングで台帳8を参照することで、電子通貨10の不正な移転の有無を判断できるので、ネットワークなどのリソースを大きく消費することがない。一方で、電子通貨10の不正な移転を確実に検知できるので、安全な通貨流通を実現できる。

[0050] < C. ハードウェア構成例 >

次に、本実施の形態に従う電子通貨基盤1において用いられるハードウェアの構成例について説明する。

[0051] 図2は、本実施の形態に従う電子通貨基盤1において用いられる情報処理装置100のハードウェア構成例を示す模式図である。図2に示す情報処理装置100は、例えば、発行局2、中央銀行3、金融機関4、販売者5、および、台帳8などの各々における情報処理を実行するために用いられる。

[0052] 図2を参照して、情報処理装置100は、公知のコンピュータアーキテクチャに従っており、1または複数のプロセッサ102と、メモリ104と、入力部106と、表示部108と、ストレージ110と、ネットワークインターフェイス120とを含む。

[0053] プロセッサ102は、コンピュータ可読命令（computer-readable instructions）を順次読み出して実行する。プロ

セッサ１０２は、例えば、CPU (Central Processing Unit) などで構成される。プロセッサ１０２は、複数のコアを有していてもよい。

[0054] 本明細書において、「プロセッサ」との用語は、少なくとも、CPU、GPU (Graphics Processing Unit)、ASIC (Application Specific Integrated Circuit)、および、FPGA (Field-Programmable Gate Array) を包含する。さらに、本明細書において、「プロセッサ」との用語は、SoC (System on Chip) も包含する。「プロセッサ」は、処理回路 (processing circuitry) と言い換えることもできる。

[0055] メモリ１０４は、例えば、DRAM (Dynamic Random Access Memory) やSRAM (Static Random Access Memory) などの揮発性記憶装置である。ストレージ１１０は、例えば、HDD (Hard Disk Drive) やSSD (Solid State Drive) などの不揮発性記憶装置である。

[0056] 本明細書において、「メモリ」との用語は、メモリおよびストレージを包含する。

ストレージ１１０には、各種プログラムおよび各種データが格納されている。プロセッサ１０２は、指定された部分またはコンピュータ可読命令を、ストレージ１１０に格納されたプログラムから読み出して、メモリ１０４上に展開して順次実行することで、後述するような様々な処理を実現する。

[0057] ストレージ１１０には、例えば、OS １１２と、アプリケーションプログラム１１４と、鍵ペア１１６とが格納されている。OS １１２は、情報処理装置１００で各種処理を実行するための環境を提供するプログラムである。アプリケーションプログラム１１４は、本実施の形態に従う電子通貨基盤１に必要な処理を実行するためのコンピュータ可読命令を含む。鍵ペア１１６は、ストレージ１１０のセキュア領域に格納されてもよいし、ストレージ１

１０とは別のセキュアデバイス（図示しない）に格納されていてもよい。

[0058] 入力部１０６は、情報処理装置１００に対するユーザ操作などを受け付ける。入力部１０６は、例えば、キーボード、マウス、表示部１０８に対応付けて配置されたタッチパネル、情報処理装置１００の筐体のいずれかの位置に配置されたスイッチなどであってもよい。入力部１０６は、入力装置と通信するためのインターフェイスを含んでいてもよい。

[0059] 表示部１０８は、プロセッサ１０２による処理結果などを視覚化する。表示部１０８は、例えば、LCD（Liquid Crystal Display）や有機EL（Electro-Luminescence）ディスプレイなどであってもよい。表示部１０８は、表示デバイスと通信するためのインターフェイスを含んでいてもよい。

[0060] ネットワークインターフェイス１２０は、他のデバイスとの通信を仲介する。ネットワークインターフェイス１２０は、例えば、イーサネット（登録商標）ポート、USB（Universal Serial Bus）ポート、IEEE 1394などのシリアルポート、レガシーなパラレルポートなどであってもよい。ネットワークインターフェイス１２０は、無線通信するための処理回路およびアンテナなどを含んでいてもよい。

[0061] 図３は、本実施の形態に従う電子通貨基盤１において用いられるモバイル装置２００のハードウェア構成例を示す模式図である。図３に示すモバイル装置２００は、例えば、販売者５および消費者６などの各々における情報処理を実行するために用いられる。

[0062] 図３を参照して、モバイル装置２００は、公知のコンピュータアーキテクチャに従っており、１または複数のプロセッサ２０２と、メモリ２０４と、入力部２０６と、表示部２０８と、ストレージ２１０と、カメラ２２０と、スピーカ２２２と、無線通信部２２４と、近距離通信部２２６とを含む。

[0063] プロセッサ２０２と、メモリ２０４と、入力部２０６と、表示部２０８と、ストレージ２１０とは、図２に示すプロセッサ１０２と、メモリ２０４と、入力部２０６と、表示部２０８と、ストレージ２１０とそれぞれ同様であ

るので、詳細な説明は繰り返さない。

- [0064] ストレージ 210 には、例えば、OS 212 と、アプリケーションプログラム 214 と、鍵ペア 216 とが格納されている。
- [0065] カメラ 220 と、モバイル装置 200 の筐体に設けられており、静止画および動画を撮像する。
- [0066] スピーカ 222 は、モバイル装置 200 の筐体に設けられており、プロセッサ 202 からの指示に従って音声を発生する。
- [0067] 無線通信部 224 は、公衆回線などを介して、他の情報処理装置などとの通信を仲介する。無線通信部 224 は、例えば、5G、4G、LTE、3G などであってもよい。
- [0068] 近距離通信部 226 は、モバイル装置 200 の近傍に存在する他のモバイル装置などとの通信を仲介する。近距離通信部 226 は、例えば、無線 LAN、Bluetooth（登録商標）、ZigBee（登録商標）などの通信規格に従うインターフェイスであってもよい。
- [0069] 情報処理装置 100 および／またはモバイル装置 200 は、コンピュータ可読命令および／またはデータが格納された非一過性（non-volatile）のメディアからコンピュータ可読命令および／またはデータを読み出すためのコンポーネントをさらに有していてもよい。メディアは、例えば、DVD（Digital Versatile Disc）などの光学メディア、USBメモリなどの半導体メディアなどであってもよい。情報処理装置 100 および／またはモバイル装置 200 は、ネットワーク上の配信サーバから必要なコンピュータ可読命令および／またはデータを取得してもよい。
- [0070] なお、電子通貨基盤 1 に必要な処理は、任意のコンピューティングリソースを用いて実現できる。コンピューティングリソースには、図 2 および図 3 に示すハードウェア構成例に限らず、任意のハードウェアを用いることができる。
- [0071] 以下の説明において、「エンティティ」との用語は、電子通貨基盤 1 に関

係するいずれかの意思表示が可能な個人または法人（発行局 2、中央銀行 3、金融機関 4、販売者 5、消費者 6 を含む）、ならびに、個人または法人が使用するコンピュータ（情報処理装置 100 および／またはモバイル装置 200 を含む）を包含する。すなわち、各エンティティは、何らかの意思表示が可能な個人または法人と、当該個人または法人が使用するコンピュータとを一体化した概念を包含する。

[0072] さらに、「エンティティ」との用語は、AI (Artificial Intelligence) によって意思決定されるコンピュータを包含し得る。

[0073] 後述する多くの処理は、個人、法人または AI により決定された意思に従って開始および実行される。ただし、電子通貨 10 を取り扱う処理自体は、コンピュータによって実現される。

[0074] <D. 電子通貨の流通の一例>

次に、本実施の形態に従う電子通貨基盤 1 における電子通貨 10 の流通の一例について説明する。

[0075] 図 4 は、本実施の形態に従う電子通貨基盤 1 における電子通貨 10 の流通の一例を説明するための図である。図 4 においては、台帳 8 にネットワークアクセス可能な範囲をネットワーク化ゾーン 60 と称し、台帳 8 にネットワークアクセス不可能な範囲を非ネットワークゾーン 62 と称す。

[0076] ネットワーク化ゾーン 60 に存在するエンティティは、電子通貨 10 の内容を台帳 8 に記録し、また、台帳 8 に記録された電子通貨の内容を参照できる。そのため、電子通貨 10 の流通に伴って、電子通貨 10 自体にチェックポイントデータを含む履歴が追加されるとともに、電子通貨 10 のチェックポイントデータの内容は台帳 8 にも順次反映される。

[0077] 一方、非ネットワークゾーン 62 に存在するエンティティは、台帳 8 にネットワークアクセスできないので、電子通貨 10 の流通は、他のユーザまたは他のユーザが保持するエンティティとの間に推認される信頼に基づくことになる。そのため、電子通貨 10 のチェックポイントデータを含む履歴は、

電子通貨 10 自体にのみ追加される。ただし、電子通貨 10 の内容は、任意のタイミングで台帳 8 に反映され得る。

[0078] 電子通貨 10 のチェックポイントデータは、電子通貨 10 を所有するエンティティによる行為（電子通貨 10 の移転）に対する否認防止性を担保するための署名データを含む。

[0079] 図 4 を参照して、まず、発行局 2 が電子通貨 10 を発行する（ステップ S 5 1）。具体的には、発行局 2 は、電子通貨 10 として必要な情報を生成し、生成された情報を含む電子ファイルを生成する。発行局 2 は、予め定められた財産的価値を付与された電子通貨 10（電子ファイル）を生成する。

[0080] 中央銀行 3 は、発行局 2 が発行した電子通貨 10 を受け取ると、受け取った電子通貨 10 のレコードを台帳 8 に追加する（ステップ S 5 2）。このように、中央銀行 3 は、電子通貨 10 の内容の少なくとも一部を台帳 8 に記録する。追加されるレコードは、電子通貨 10 を特定するための識別情報を含む。電子通貨 10 の識別情報は、電子通貨 10 のファイル名として用いられてもよい。

[0081] 中央銀行 3 は、電子通貨 10 を市中に提供する。具体的には、中央銀行 3 は、中央銀行 3 の秘密鍵 2 3 A を用いて生成された署名データを電子通貨 10 に追加する（ステップ S 5 3）。このように、中央銀行 3 は、電子通貨 10（電子ファイル）に中央銀行 3 の秘密鍵 2 3 A を用いて生成された署名データを追加する。

[0082] 金融機関 4 は、中央銀行 3 から電子通貨 10 を受け取ると、受け取った電子通貨 10 の情報を台帳 8 に反映する（ステップ S 5 4）。このように、金融機関 4 は、電子通貨 10 の内容の少なくとも一部を台帳 8 に記録する。

[0083] 金融機関 4 は、金融機関 4 の預金者である消費者 6 A からの請求に応じて、消費者 6 A の預金から指定された金額の電子通貨 10 を消費者 6 A に払い出す。具体的には、金融機関 4 は、金融機関 4 の秘密鍵 2 4 A を用いて生成された署名データを電子通貨 10 に追加した上で、電子通貨 10 を消費者 6 A に移転する（ステップ S 5 5）。このように、金融機関 4 は、電子通貨 1

0を金融機関4（第1のエンティティ）から消費者6A（第2のエンティティ）に移転するために、金融機関4の秘密鍵24Aを用いて生成された署名データを電子通貨10に追加する。

[0084] また、金融機関4は、消費者6Aに移転した電子通貨10の情報を台帳8に反映する（ステップS56）。このように、金融機関4は、電子通貨10の内容の少なくとも一部を台帳8に記録する。

[0085] 続いて、消費者6Aが電子通貨10を消費者6Bに渡す場合を想定する。この場合には、消費者6Aは、消費者6Aの秘密鍵26AAを用いて生成された署名データを電子通貨10に追加した上で、電子通貨10を消費者6Bに移転する（ステップS57）。このように、消費者6Aは、電子通貨10を消費者6A（第1のエンティティ）から消費者6B（第2のエンティティ）に移転するために、消費者6Aの秘密鍵26AAを用いて生成された署名データを電子通貨10に追加する。なお、この時点での電子通貨10の移転は、消費者6Aと消費者6Bとの間の信頼に基づくことになる。

[0086] 続いて、消費者6Bが、商品およびサービスの購入の対価として、消費者6Aから受け取った電子通貨10を販売者5に支払う場合を想定する。なお、販売者5は、ネットワーク化ゾーン60に存在するとする。この場合には、消費者6Bは、販売者5に対して、電子通貨10での支払いを申し出る。具体的には、消費者6Bは、チェックポイントデータを追加した上で、支払い予定の電子通貨10を販売者5に送信する（ステップS58）。

[0087] 販売者5は、消費者6Bが申し出た電子通貨10の内容を台帳8に反映する（ステップS59）。このように、販売者5は、電子通貨10の内容の少なくとも一部を台帳8に記録する。

[0088] 販売者5は、台帳8に対する情報の反映結果を取得する（ステップS60）。このように、販売者5（第2のエンティティ）が消費者6B（第1のエンティティ）から電子通貨10（電子ファイル）を受信した後に、電子通貨10の内容と台帳8に記録された内容とを照合する。このとき、台帳8に記録されている電子通貨10の内容と、消費者6Bが申し出た電子通貨10の

内容とが整合しなければ、販売者 5 は、消費者 6 B の申し出を拒絶してもよい。すなわち、販売者 5 は、少なくとも台帳 8 に記録された内容に基づいて、電子通貨 10 の不正な移転の有無を判断する。

[0089] 台帳 8 に記録された情報との整合性に問題がなければ、販売者 5 は、消費者 6 B の申し出を受け入れる旨を消費者 6 B に回答する（ステップ S 6 1）。消費者 6 B は、消費者 6 B が保持している電子通貨 10 を削除する。このように、消費者 6 B は、電子通貨 10 を消費者 6 B（第 1 のエンティティ）から販売者 5（第 2 のエンティティ）に移転するために、消費者 6 B の秘密鍵 2 6 A B を用いて生成された署名データを電子通貨 10 に追加する。電子通貨 10 が消費者 6 B から販売者 5 に移転することで、電子通貨 10 による支払いが完了する。

[0090] その後、販売者 5 は、消費者 6 B などから受け取った電子通貨 10 を金融機関 4 にある販売者 5 の預金口座に入金する。具体的には、販売者 5 は、販売者 5 の秘密鍵 2 5 A を用いて生成された署名データを電子通貨 10 に追加した上で、電子通貨 10 を金融機関 4 に移転する（ステップ S 6 2）。金融機関 4 は、販売者 5 から受け取った電子通貨 10 の金額に応じて、販売者 5 の預金口座の残高を更新する。

[0091] なお、販売者 5 は、電子通貨 10 を現金に両替する場合においても、同様の処理を実行する。両替の場合には、金融機関 4 は、販売者 5 から受け取った電子通貨 10 の金額に相当する現金を販売者 5 に渡す。

[0092] 金融機関 4 は、販売者 5 から受け取った電子通貨 10 を、消費者 6 および／または販売者 5 への払い出しに再利用することもできる。

[0093] その後、金融機関 4 は、販売者 5 から受け取った電子通貨 10 を中央銀行 3 に戻す。具体的には、金融機関 4 は、金融機関 4 の秘密鍵 2 4 A を用いて生成された署名データを電子通貨 10 に追加した上で、電子通貨 10 を中央銀行 3 に移転する（ステップ S 6 3）。中央銀行 3 は、金融機関 4 から受け取った電子通貨 10 の金額に応じて、中央銀行 3 にある金融機関 4 の預金口座の残高を更新する。あるいは、中央銀行 3 は、金融機関 4 から受け取った

電子通貨 10 の金額に応じて、新たな電子通貨 10 を金融機関 4 に渡してもよい。

[0094] 最終的に、中央銀行 3 は、所定の条件が成立すると、金融機関 4 から回収した電子通貨 10 を廃棄する（ステップ S 6 4）。電子通貨 10 の廃棄は、電子ファイル自体の削除であってもよいし、電子通貨 10 を再流通させないように管理することであってもよい。

[0095] < E. データ構造 >

次に、電子通貨 10（電子ファイル）のファイル形式の一例について説明する。電子通貨 10 は、バイナリ形式で保存されてもよい。

[0096] 図 5 は、本実施の形態に従う電子通貨 10 のデータ構造の一例を示す模式図である。図 5 を参照して、電子通貨 10 は、例えば、以下のセクションを含んでいてもよい。

- (1) ドキュメントルートコントロールセクション 40
- (2) 信頼コントロールセクション 42
- (3) トランザクションコントロールセクション 44
- (4) スペシャルセクション 46

各セクションのデータは、ヘッダ情報として、当該セクションの種類を示すセクションタイプと、当該セクションの状態を示すセクションフラグと、当該セクションの長さを示すセクション長とを含んでいてもよい。

[0097] (e 1 : ドキュメントルートコントロールセクション 40)

発行局 2 が生成する電子通貨 10 のドキュメントルートコントロールセクション 40 は、以下のような設定を含む初期データ 41 を含んでいてもよい。

- (a) 作成時刻 (Creation Time) (例えば、T A I 6 4 N 形式)
- (b) 有効期限 (Spent at Time) (例えば、T A I 6 4 N 形式)
- (c) 通貨コード (例えば、USD や J P Y などの I S O 4 2 1 7 に従う

3バイト)

(d) 通貨単位 (Currency Denomination) (例えば、非ゼロの符号無し整数)

(e) 連続識別子 (Sequential Identifier) (例えば、13バイト)

(f) 小数点位置 (Decimal Place) (小数点位置、または、サブ単位インジータ位置 (Subunit Indicator Position) を示す桁数: 例えば、USDにおいては2が設定され、JPYにおいては0が設定される)

(g) 発行局2の公開鍵

(h) 中央銀行3が発行局2の公開鍵を承認するための署名データ (ランダムノンス (random nonce) が追加されていてもよい)

(i) 電子通貨10のキー文字列のハッシュ値 (例えば、特定のキーワードから算出されたハッシュ文字列)

(j) 電子通貨10のシリアル番号 (例えば、(1) ~ (9) の初期データのハッシュ値)

(e2: 信頼コントロールセクション42)

信頼コントロールセクション42には、信頼認証セクション43 (Trust Authorization Section: TAS) を含む。信頼認証セクション43は、メタデータであってもよく、公開鍵を中央銀行3 (電子通貨10のルート) に繋げるための情報が格納されてもよい。

[0098] 本実施の形態に従う電子通貨基盤1は、中央銀行3が市中に提供する通貨を利用する、金融機関4、販売者5、および消費者6を含むデジタル署名を用いて、電子通貨10の完全な信頼チェーンが形成される。形成される信頼チェーンは、電子通貨10の流通に関与するエンティティを含む。

[0099] 署名者の完全性 (integrity) は、中央銀行3に対する信頼を拡張する中間機関 (例えば、ローカル発行局、国務省、財務省、公証人など) の署名によって裏付けられてもよい。

- [0100] 図6は、本実施の形態に従う電子通貨基盤1における信頼チェーンの一例を示す模式図である。図6を参照して、ルート（ROOT）として機能する中央銀行3には、第1の中間エンティティ（INTERMEDIATE L0）が繋がっている。第1の中間エンティティは、例えば、ローカル発行局51と、国務省52と、財務省53とを含んでいてもよい。第1の中間エンティティには、第2の中間エンティティ（INTERMEDIATE L1）が繋がっている。第2の中間エンティティは、例えば、金融機関4と、公証人54とを含んでいてもよい。第2の中間エンティティには、ユーザが繋がっている。ユーザは、ATM56と、販売者5と、消費者6と、政府機関55とを含んでいてもよい。
- [0101] 電子通貨10の流通を示す信頼チェーンを構成するリンクは、信頼認証セクション43に格納される署名データによって完全性が保証される。信頼チェーンを構成するリンクは、電子通貨10内に定義される。信頼チェーンを構成するリンクは、電子通貨10が順次移転するのに伴って、必要に応じて順次更新または追加される。
- [0102] 図7は、本実施の形態に従う電子通貨10の信頼コントロールセクション42（信頼認証セクション43）のデータ構造の一例を示す模式図である。図7を参照して、信頼認証セクション43は、有効期間開始時刻431と、有効期間終了時刻432と、ロールコード433と、発行者公開鍵434と、エンティティ公開鍵435と、署名データ436とを含む。
- [0103] 有効期間開始時刻431は、初期データ41に含まれる作成時刻と同じ値である。電子通貨10のチェックポイントデータに含まれる処理時刻は、有効期間開始時刻431以降（on or after）でなければならない。すなわち、有効期間開始時刻431より古い時刻であれば、無効な手続きまたは処理として取り扱われる。
- [0104] 有効期間終了時刻432は、初期データ41に含まれる有効期限と同じ値である。電子通貨10のチェックポイントデータに含まれる処理時刻は、有効期間終了時刻432以前（on or before）の時刻でなければならない。

ならない。すなわち、有効期間開始時刻4 3 1より新しい時刻であれば、無効な手続きまたは処理として取り扱われる。

[0105] ロールコード4 3 3は、図6に示す信頼チェーンのうちいずれのリンクに相当するのかわかる情報を示す情報を含む。例えば、ロールコード4 3 3は、第1の中間エンティティとして機能するローカル発行局5 1がルートとして機能する中央銀行3に対する信頼であることを示す情報を含む。

[0106] 発行者公開鍵4 3 4は、ルートとして機能する中央銀行3の公開鍵である。

エンティティ公開鍵4 3 5は、信頼を示すエンティティの公開鍵である。信頼を示すエンティティは、第1の中間エンティティ、第2の中間エンティティ、ユーザのいずれかに属するエンティティである。

[0107] 署名データ4 3 6は、エンティティ公開鍵4 3 5のペアとなる秘密鍵を用いて、信頼認証セクション4 3に含まれる情報（有効期間開始時刻4 3 1、有効期間終了時刻4 3 2、ロールコード4 3 3、発行者公開鍵4 3 4、および、エンティティ公開鍵4 3 5）から生成される。すなわち、信頼認証セクション4 3に含まれる情報（署名データ4 3 6を除く）をハッシュ関数に入力して算出されるハッシュ値を、エンティティ公開鍵4 3 5のペアとなる秘密鍵で暗号化することで、署名データ4 3 6が生成される。

[0108] 第三者は、信頼認証セクション4 3の情報を参照することで、ルートとして機能する中央銀行3に繋がる信頼チェーンを確認および検証できる。信頼認証セクション4 3は、図6に示す信頼チェーンを構成するリンク毎に生成される。図6に示す信頼チェーンを構成するすべてのリンクについて信頼認証セクション4 3を生成することが好ましいが、一部のリンクについてのみ信頼認証セクション4 3が生成されてもよい。

[0109] ただし、後述するように、電子通貨1 0の流通には、信頼コントロールセクション4 2に登録されている公開鍵が要求される。

[0110] （e 3：トランザクションコントロールセクション4 4）

トランザクションコントロールセクション4 4は、電子通貨1 0を受け渡すエンティティと、電子通貨1 0を受け取るエンティティとの間のやり取り

の情報であるトランザクションデータ45を含む。トランザクションデータ45は、例えば、あるエンティティから別のエンティティへの電子通貨10の移転の履歴を示す。

[0111] 図8は、本実施の形態に従う電子通貨10のトランザクションコントロールセクション44のトランザクションデータ45のデータ構造の一例を示す模式図である。図8を参照して、トランザクションデータ45は、Offerエントリ451と、Acceptエントリ452とを含む。後述するように、Offerエントリ451およびAcceptエントリ452は、異なるエンティティにより異なるタイミングで追加されてもよい。

[0112] Offerエントリ451は、「Offer」の種別453と、トランザクションID454と、エンティティ公開鍵455とを含む。Acceptエントリ452は、「Accept」の種別453と、トランザクションID454と、エンティティ公開鍵455とを含む。

[0113] Offerエントリ451は、電子通貨10を所有しているエンティティが別のエンティティに対して、電子通貨10の移転を申し出る際に、電子通貨10を所有しているエンティティによって追加される。そのため、エンティティ公開鍵455は、電子通貨10を所有しているエンティティの公開鍵である。

[0114] Acceptエントリ452は、電子通貨10の移転の申し出を了承する際に、電子通貨10を受け取るエンティティによって追加される。そのため、エンティティ公開鍵455は、電子通貨10を受け取るエンティティの公開鍵である。

[0115] トランザクションコントロールセクション44には、電子通貨10の移転毎に、図8に示すトランザクションデータ45が追加されてもよい。

[0116] トランザクションコントロールセクション44は、電子通貨10に既知の公開鍵を提供するための情報と、新たな公開鍵において電子通貨10を受け入れるための情報とを含んでいてもよい。例えば、いずれかのエンティの鍵ペア（公開鍵）の有効期限が切れると、新たな鍵ペア（公開鍵）が発行され

る。トランザクションコントロールセクション４４には、このような鍵ペア（公開鍵）の更新のための情報が格納されてもよい。

[0117] （e ４：スペシャルセクション４６）

スペシャルセクション４６は、無効管理セクション４７と、チェックポイントデータ４８とを含む。

[0118] 無効管理セクション４７には、電子通貨１０の有効期限が切れていないか否かの判断結果が格納される。電子通貨１０の有効期限が切れていれば、電子通貨１０をさらに流通されることはできず、中央銀行３に戻すことのみが許容される。

[0119] チェックポイントデータ４８には、チェックポイントデータが順次格納される。署名済のチェックポイントデータは、電子通貨１０の流通経路の各ポイントを示す。すなわち、チェックポイントデータ４８は、電子通貨１０の移転が成功した後に署名される。

[0120] チェックポイントデータ４８に格納されたチェックポイントデータは、以下の要件が満たされなければ破棄される。

（１）署名者公開鍵がトランザクションコントロールセクション４４に登録されていること

（２）新たに生成されたチェックポイントデータ４８の処理時刻４８１は、生成済のチェックポイントデータ４８の処理時刻４８１より新しいこと

（３）新たに生成されたチェックポイントデータ４８の処理時刻４８１は、有効期間終了時刻４３２を過ぎていないこと

（４）新たに生成されたチェックポイントデータ４８の処理時刻４８１は、

（１）～（３）を含めた一連の検証を行う処理が実行される現在時刻より古いこと

上述の（１）～（４）の要件は、電子通貨１０を受信したエンティティが評価してもよいし、台帳８において評価されてもよい。

[0121] 図９は、本実施の形態に従う電子通貨１０のスペシャルセクション４６のチェックポイントデータ４８のデータ構造の一例を示す模式図である。図９

を参照して、チェックポイントデータ４８は、処理時刻４８１と、ランダム
ノンス４８２と、署名者公開鍵４８３と、署名データ４８４とを含む。

[0122] 処理時刻４８１は、チェックポイントデータ４８が生成された時刻である。
。

ランダムノンス４８２は、処理時刻４８１と組み合わせることで、セキュ
リティ強度を高めるために用いられる。

[0123] 署名者公開鍵４８３には、電子通貨１０を渡す側のエンティティ（ソース
エンティティ）の公開鍵が格納される。

[0124] 署名データ４８４は、署名者公開鍵４８３のペアとなる秘密鍵を用いて、
チェックポイントデータ４８に含まれる情報（処理時刻４８１、ランダムノ
ンス４８２、および、署名者公開鍵４８３）から生成される。すなわち、署
名データ４８４に含まれる情報（署名データ４８４を除く）をハッシュ関数
に入力して算出されるハッシュ値を、署名者公開鍵４８３のペアとなる秘密
鍵で暗号化することで、署名データ４８４が生成される。

[0125] チェックポイントデータ４８は、電子通貨１０がエンティティ間を流通す
るたびに生成される。

[0126] （e 5：電子通貨１０のファイル名）

電子通貨１０のファイル名は、例えば、通貨コードと、額面（最小単位の
整数倍として表現）と、シリアル番号とを連結した文字列と、ファイル拡張
子（例えば、「s n o t e」）とから構成してもよい。

[0127] 例えば、日本円で１０，０００円の額面を示す電子通貨１０のファイル名
は、「JPY-10000-5891b5b522d5df086d0ff0b110fbd9d21bb4fc7163af34d08286a
2e846f6be03.snote」と設定できる。また、米ドルで１００，００ドルの額面
を示す電子通貨１０のファイル名は、「USD-10000-48ae15fd45c3ae607e41a72
d153d6c051f267c42f5ea11f26e1b33b183eaf0e8.snote」と設定できる。このと
き、米ドルの最小単位はセントであるので、額面はセントの整数倍で表現さ
れる。

[0128] ＜F. 台帳８＞

次に、本実施の形態に従う電子通貨基盤 1 に含まれる台帳 8 について説明する。

[0129] 図 10 は、本実施の形態に従う電子通貨基盤 1 の台帳 8 のデータ構造一例を示す模式図である。図 10 を参照して、台帳 8 には、中央銀行 3 が市中に提供した電子通貨 10 の内容が順次反映される。

[0130] 台帳 8 は、電子通貨 10 の各々に含まれる、ドキュメントルートコントロールセクション 40、信頼コントロールセクション 42、トランザクションコントロールセクション 44、および、スペシャルセクション 46 の内容を記録する。

[0131] ネットワーク化ゾーン 60 に配置されたエンティティは、他のエンティティから電子通貨 10 を受け取ったことをトリガとして、受け取った電子通貨 10 の内容を台帳 8 に記録する。

[0132] 台帳 8 は、電子通貨 10 のスペシャルセクション 46 に含まれる無効管理セクション 47 に格納された値（電子通貨 10 の有効期限が切れていないか否かの判断結果）を検証するためのエンジンと、電子通貨 10 のスペシャルセクション 46 に含まれるチェックポイントデータ 48 の整合性を検証するためのエンジンとを含んでいてもよい。これらのエンジンは、台帳 8 に新たにデータが書き込まれたタイミングで、検証する処理を実行してもよい。

[0133] チェックポイントデータ 48 の整合性を検証する処理例については、後述する。

<G. 処理手順>

次に、本実施の形態に従う電子通貨基盤 1 における処理手順の一例について説明する。

[0134] （g 1：エンティティ間の電子通貨 10 の移転）

まず、エンティティ間の電子通貨 10 の移転について説明する。

[0135] 図 11 は、本実施の形態に従う電子通貨基盤 1 におけるエンティティ間の電子通貨 10 の移転の基本的な処理手順例を説明するための図である。図 11 には、あるエンティティ（以下、「ソースエンティティ」とも称す。）か

ら別のエンティティ（以下、「ターゲットエンティティ」とも称す。）に電子通貨10の所有が変更される例を示す。

- [0136] 図11を参照して、ソースエンティティは、ターゲットエンティティに渡す予定の電子通貨10に、Offerエントリ451（トランザクションデータ45）を追加するとともに、ソースエンティティの秘密鍵を用いて生成された署名データを含むチェックポイントデータ48Aを追加する（ステップS10）。ソースエンティティは、Offerエントリ451およびチェックポイントデータ48Aが追加された電子通貨10をターゲットエンティティに送信する（ステップS11）。
- [0137] ターゲットエンティティは、ソースエンティティから受信した電子通貨10の移転を了承すると、受信した電子通貨10に、Acceptエントリ452（トランザクションデータ45）を追加するとともに、ターゲットエンティティの秘密鍵を用いて生成された署名データを含むチェックポイントデータ48Bを追加する（ステップS12）。ターゲットエンティティは、Acceptエントリ452およびチェックポイントデータ48Bが追加された電子通貨10をソースエンティティに送信する（ステップS13）。
- [0138] ソースエンティティは、Acceptエントリ452およびチェックポイントデータ48Bを含む電子通貨10を受信すると、ソースエンティティに格納されている電子通貨10のファイル、および、ターゲットエンティティから受信した電子通貨10のファイルを削除する（ステップS14）。
- [0139] このように、ソースエンティティ（第1のエンティティ）からターゲットエンティティ（第2のエンティティ）に電子通貨10（電子ファイル）を送信した後に、ターゲットエンティティからターゲットエンティティの秘密鍵を用いて生成されたチェックポイントデータ48B（署名データ）が追加された電子通貨10を受信すると、ソースエンティティは、ソースエンティティが格納している電子通貨10を削除する。
- [0140] 以上のような処理により、ソースエンティティからターゲットエンティティへの電子通貨10の移転が完了する。

- [0141] 商品およびサービスの購入の対価として電子通貨１０が利用される場合には、支払うべき対価と同額の電子通貨１０が存在しない場合もある。すなわち、エンティティ間で、おつりも含めたやり取りが必要になる場合もある。このような場合には、エンティティ間では、どのような電子通貨１０の組み合わせで取引を完了させるのかを事前に調整する処理が実行される。このような調整する処理を、以下では「プランニング」とも称す。プランニングにおいて、エンティティ間で移転させる複数の電子通貨１０が決定される。また、複数の電子通貨１０の移転をすべて完了させる必要があるため、一連の移転を管理するためのトランザクションＩＤが生成される。
- [0142] 図１２は、本実施の形態に従う電子通貨基盤１におけるプランニングを含む電子通貨１０の移転の基本的な処理手順例を説明するための図である。図１２を参照して、一例として、エンティティ１が¥８００をエンティティ２に支払う場合を想定する。しかしながら、エンティティ１は、¥８００と同額の電子通貨１０を所有していない。そのため、エンティティ１およびエンティティ２は、プランニングを行う。
- [0143] プランニングの結果、エンティティ１は、¥１，０００の価値を有する電子通貨１０－１をエンティティ２に移転するとともに、エンティティ２は、各々が¥１００の価値を有する電子通貨１０－６，１０－７をエンティティ１に移転することが決定したとする。
- [0144] 電子通貨１０－１，１０－６，１０－７の移転は、同一のトランザクションＩＤに関連付けられる。
- [0145] 電子通貨１０－１については、エンティティ１がソースエンティティとなり、図１１に示す処理が実行される。一方、電子通貨１０－６，１０－７については、エンティティ２がソースエンティティとなり、図１１に示す処理がそれぞれ実行される。
- [0146] 電子通貨１０－１，１０－６，１０－７の各々に追加されるトランザクションデータ４５（図８）には、共通のトランザクションＩＤが設定される。
- [0147] 複数の電子通貨１０の移転を共通のトランザクションＩＤに関連付けるこ

とで、おつりが必要な取引であっても、電子通貨１０の移転を確実に完了できる。

[0148] トランザクションＩＤは、いずれかのエンティティによって都度決定されてもよい。あるいは、対象となる１または複数の電子通貨１０のシリアル番号を予め定められた順序でソートし、ソートされた結果を連結し、連結された結果から算出されたハッシュ値をトランザクションＩＤとして決定してもよい。

[0149] 後者の方法で決定されたトランザクションＩＤは、台帳８に記録された内容に基づいても検証できる。例えば、ある取引に関与した１または複数の電子通貨１０を台帳８から抽出した上で、抽出した１または複数の電子通貨１０のシリアル番号に基づいてトランザクションＩＤを算出した上で、算出されたトランザクションＩＤが台帳８に記録されるトランザクションＩＤと一致するか否かを評価できる。このようなトランザクションＩＤの評価によって、電子通貨１０の不正な移転の有無を判断できる。

[0150] プランニングにおいては、対象となる電子通貨１０の有効期限が切れていないことも検証される。有効期限が切れている電子通貨１０は、プランニングの対象から除外される。すなわち、電子通貨１０（電子ファイル）をソースエンティティ（第１のエンティティ）からターゲットエンティティ（第２のエンティティ）に移転する前に、ソースエンティティおよびターゲットエンティティの少なくとも一方が電子通貨１０の有効期限が切れていないことを検証する。このような検証によって、市中を流通できない電子通貨１０が移転の対象として選択されることを防止できる。

[0151] （ｇ２：ネットワーク化ゾーン６０における電子通貨１０の流通）

次に、中央銀行３が市中に提供した電子通貨１０の流通について説明する。

[0152] 図１３は、本実施の形態に従う電子通貨基盤１における電子通貨１０の流通の処理手順を示すシーケンス図である。図１３には、エンティティ１からエンティティ２に財産的価値が移転する処理例を示す。

- [0153] 典型的には、エンティティ 1 はソースエンティティであり、エンティティ 2 はターゲットエンティティである。図 1 3 に示す処理例において、エンティティ 1 およびエンティティ 2 は、ネットワーク化ゾーン 6 0 に存在している。
- [0154] 図 1 3 を参照して、まず、エンティティ 1 とエンティティ 2 との間で通信が確立される（シーケンス S Q 1 0 0）。
- [0155] エンティティ 1 およびエンティティ 2 の少なくとも一方が移転すべき財産的価値（金額）の指定を受けると（シーケンス S Q 1 0 2）、エンティティ 1 およびエンティティ 2 は、プランニングにより、トランザクション ID と移転対象の 1 または複数の電子通貨 1 0 とを決定する（シーケンス S Q 1 0 4）。プランニングにおいて、エンティティ 1 およびエンティティ 2 は、対象となる電子通貨 1 0 の有効期限が切れていないことも検証する。
- [0156] エンティティ 1 は、エンティティ 2 への移転対象である 1 または複数の電子通貨 1 0 の各々に、O f f e r エントリ 4 5 1 およびチェックポイントデータ 4 8 を追加する（シーケンス S Q 1 0 6）。エンティティ 1 は、O f f e r エントリ 4 5 1 およびチェックポイントデータ 4 8 が追加された 1 または複数の電子通貨 1 0 をエンティティ 2 に送信する（シーケンス S Q 1 0 8）。
- [0157] エンティティ 2 は、受信した 1 または複数の電子通貨 1 0 のチェックポイントデータ 4 8 に含まれる署名データをエンティティ 1 の公開鍵を用いて検証する（シーケンス S Q 1 1 0）。エンティティ 2 は、署名データの検証が問題なければ、受信した 1 または複数の電子通貨 1 0 の内容を台帳 8 に送信する（シーケンス S Q 1 1 2）。エンティティ 2 は、エンティティ 1 から電子通貨 1 0（電子ファイル）を受信した後に、電子通貨 1 0 の内容と台帳 8 に記録された内容とを照合する。
- [0158] エンティティ 2 は、送信した 1 または複数の電子通貨 1 0 の内容について整合性に問題がある旨の通知を台帳 8 から受信すると（シーケンス S Q 1 1 4 において Y E S）、エンティティ 1 に処理の中止を通知する（シーケンス

S Q 1 1 6)。

- [0159] エンティティ 2 は、送信した 1 または複数の電子通貨 1 0 の内容について整合性に問題がある旨の通知を台帳 8 から受信しなければ (シーケンス S Q 1 1 4 において N O)、受信した 1 または複数の電子通貨 1 0 の各々に、A c c e p t エントリ 4 5 2 およびチェックポイントデータ 4 8 を追加する (シーケンス S Q 1 1 8)。エンティティ 2 は、A c c e p t エントリ 4 5 2 およびチェックポイントデータ 4 8 が追加された 1 または複数の電子通貨 1 0 をエンティティ 1 に送信する (シーケンス S Q 1 2 0)。
- [0160] おつりとして 1 または複数の電子通貨 1 0 をエンティティ 2 からエンティティ 1 に移転する必要がある場合には、シーケンス S Q 1 2 2 ~ S Q 1 3 6 の処理も実行される。
- [0161] エンティティ 2 は、エンティティ 1 への移転対象である 1 または複数の電子通貨 1 0 の各々に、O f f e r エントリ 4 5 1 およびチェックポイントデータ 4 8 を追加する (シーケンス S Q 1 2 2)。エンティティ 1 は、O f f e r エントリ 4 5 1 およびチェックポイントデータ 4 8 が追加された 1 または複数の電子通貨 1 0 をエンティティ 1 に送信する (シーケンス S Q 1 2 4)。
- [0162] エンティティ 1 は、受信した 1 または複数の電子通貨 1 0 のチェックポイントデータ 4 8 に含まれる署名データをエンティティ 2 の公開鍵を用いて検証する (シーケンス S Q 1 2 6)。エンティティ 1 は、署名データの検証が問題なければ、受信した 1 または複数の電子通貨 1 0 の内容を台帳 8 に送信する (シーケンス S Q 1 2 8)。エンティティ 1 は、エンティティ 2 から電子通貨 1 0 (電子ファイル) を受信した後に、電子通貨 1 0 の内容と台帳 8 に記録された内容とを照合する。
- [0163] エンティティ 1 は、送信した 1 または複数の電子通貨 1 0 の内容について整合性に問題がある旨の通知を台帳 8 から受信すると (シーケンス S Q 1 3 0 において Y E S)、エンティティ 2 に処理の中止を通知する (シーケンス S Q 1 3 2)。

- [0164] エンティティ 1 は、送信した 1 または複数の電子通貨 10 の内容について整合性に問題がある旨の通知を台帳 8 から受信しなければ（シーケンス SQ 130 において NO）、受信した 1 または複数の電子通貨 10 の各々に、Accept エントリ 452 およびチェックポイントデータ 48 を追加する（シーケンス SQ 134）。エンティティ 1 は、Accept エントリ 452 およびチェックポイントデータ 48 が追加された 1 または複数の電子通貨 10 をエンティティ 2 に送信する（シーケンス SQ 136）。
- [0165] エンティティ 1 は、プランニングにおいて決定された、移転すべき 1 または複数の電子通貨 10 のすべてについて、Accept エントリ 452 およびチェックポイントデータ 48 が追加されたファイルを受信していれば（シーケンス SQ 138 において YES）、移転すべき 1 または複数の電子通貨 10 の内容を台帳 8 に送信し（シーケンス SQ 140）、当該移転すべき 1 または複数の電子通貨 10 をエンティティ 1 のストレージから削除する（シーケンス SQ 142）。
- [0166] 同様に、エンティティ 2 は、プランニングにおいて決定された、移転すべき 1 または複数の電子通貨 10 のすべてについて、Accept エントリ 452 およびチェックポイントデータ 48 が追加されたファイルを受信していれば（シーケンス SQ 144 において YES）、移転すべき 1 または複数の電子通貨 10 の内容を台帳 8 に送信し（シーケンス SQ 146）、当該移転すべき 1 または複数の電子通貨 10 をエンティティ 2 のストレージから削除する（シーケンス SQ 148）。
- [0167] 以上のような処理によって、エンティティ 1 からエンティティ 2 への財産的価値が移転する。なお、エンティティ 1 およびエンティティ 2 は、電子通貨 10 の移転後のそれぞれが所有する電子通貨 10 の合計額を更新してもよい。
- [0168] （g 3：非ネットワークゾーン 62 における電子通貨 10 の流通）
次に、中央銀行 3 が市中に提供した電子通貨 10 の流通について説明する。

- [0169] 図14は、本実施の形態に従う電子通貨基盤1における電子通貨10の流通の別の処理手順を示すシーケンス図である。図14には、エンティティ1からエンティティ2に財産的価値を移転する処理例を示す。
- [0170] 典型的には、エンティティ1はソースエンティティであり、エンティティ2はターゲットエンティティである。図14に示す処理例において、エンティティ1およびエンティティ2は、いずれも非ネットワークゾーン62に存在している。
- [0171] 図14を参照して、まず、エンティティ1とエンティティ2との間で通信が確立される（シーケンスSQ200）。
- [0172] エンティティ1およびエンティティ2の少なくとも一方が移転すべき財産的価値（金額）の指定を受けると（シーケンスSQ202）、エンティティ1およびエンティティ2は、プランニングにより、トランザクションIDと移転対象の1または複数の電子通貨10とを決定する（シーケンスSQ204）。プランニングにおいて、エンティティ1およびエンティティ2は、対象となる電子通貨10の有効期限が切れていないことも検証する。
- [0173] エンティティ1は、エンティティ2への移転対象である1または複数の電子通貨10の各々に、Offerエントリ451およびチェックポイントデータ48を追加する（シーケンスSQ206）。エンティティ1は、Offerエントリ451およびチェックポイントデータ48が追加された1または複数の電子通貨10をエンティティ2に送信する（シーケンスSQ208）。
- [0174] エンティティ2は、受信した1または複数の電子通貨10のチェックポイントデータ48に含まれる署名データをエンティティ1の公開鍵を用いて検証する（シーケンスSQ210）。エンティティ2は、署名データの検証が問題なければ、受信した1または複数の電子通貨10の各々に、Acceptエントリ452およびチェックポイントデータ48を追加する（シーケンスSQ212）。エンティティ2は、Acceptエントリ452およびチェックポイントデータ48が追加された1または複数の電子通貨10をエン

ティティ 1 に送信する（シーケンス S Q 2 1 4）。

[0175] おつりとして 1 または複数の電子通貨 1 0 をエンティティ 2 からエンティティ 1 に移転する必要がある場合には、シーケンス S Q 2 1 6 ～ S Q 2 2 4 の処理も実行される。

[0176] エンティティ 2 は、エンティティ 1 への移転対象である 1 または複数の電子通貨 1 0 の各々に、O f f e r エントリ 4 5 1 およびチェックポイントデータ 4 8 を追加する（シーケンス S Q 2 1 6）。エンティティ 1 は、O f f e r エントリ 4 5 1 およびチェックポイントデータ 4 8 が追加された 1 または複数の電子通貨 1 0 をエンティティ 1 に送信する（シーケンス S Q 2 1 8）。

[0177] エンティティ 1 は、受信した 1 または複数の電子通貨 1 0 のチェックポイントデータ 4 8 に含まれる署名データをエンティティ 2 の公開鍵を用いて検証する（シーケンス S Q 2 2 0）。エンティティ 1 は、受信した 1 または複数の電子通貨 1 0 の各々に、A c c e p t エントリ 4 5 2 およびチェックポイントデータ 4 8 を追加する（シーケンス S Q 2 2 2）。エンティティ 1 は、A c c e p t エントリ 4 5 2 およびチェックポイントデータ 4 8 が追加された 1 または複数の電子通貨 1 0 をエンティティ 2 に送信する（シーケンス S Q 2 2 4）。

[0178] エンティティ 1 は、プランニングにおいて決定された、移転すべき 1 または複数の電子通貨 1 0 のすべてについて、A c c e p t エントリ 4 5 2 およびチェックポイントデータ 4 8 が追加されたファイルを受信していれば（シーケンス S Q 2 2 6 において Y E S）、移転すべき 1 または複数の電子通貨 1 0 をエンティティ 1 のストレージから削除する（シーケンス S Q 2 2 8）。

[0179] 同様に、エンティティ 2 は、プランニングにおいて決定された、移転すべき 1 または複数の電子通貨 1 0 のすべてについて、A c c e p t エントリ 4 5 2 およびチェックポイントデータ 4 8 が追加されたファイルを受信していれば（シーケンス S Q 2 3 0 において Y E S）、移転すべき 1 または複数の

電子通貨10をエンティティ2のストレージから削除する（シーケンスSQ232）。

[0180] 以上のような処理によって、エンティティ1からエンティティ2への財産的価値が移転する。なお、エンティティ1およびエンティティ2は、電子通貨10の移転後のそれぞれが所有する電子通貨10の合計額を更新してもよい。

[0181] （g4：台帳8における処理手順）

図15は、本実施の形態に従う電子通貨基盤1の台帳8における処理手順の一例を示すフローチャートである。

[0182] 図15を参照して、台帳8は、エンティティから要求を受け付けると（ステップS100においてYES）、要求の種類を判断する（ステップS102）。

[0183] 台帳8を参照するための要求であれば（ステップS102において「参照」）、台帳8は、初期データ41に含まれる連続識別子などにより指定された電子通貨10に対応する登録内容を応答する（ステップS104）。そして、ステップS100以下の処理が繰り返される。

[0184] 台帳8にデータを追加するための要求であれば（ステップS102において「追加」）、台帳8は、初期データ41に含まれる連続識別子などにより指定された電子通貨10に対応する登録内容と追加を要求されたデータとの整合性を検証する（ステップS106）。整合性に問題があれば（ステップS106においてFAIL）、台帳8は、整合性に問題がある旨を応答する（ステップS108）。そして、ステップS100以下の処理が繰り返される。

[0185] 整合性に問題がなければ（ステップS106においてOK）、台帳8は、指定された電子通貨10に対応付けて要求されたデータを登録する（ステップS110）。そして、ステップS100以下の処理が繰り返される。

[0186] 図16は、本実施の形態に従う電子通貨基盤1の台帳8における整合性の検証の一例を説明するための図である。図16には、電子通貨10の二重譲

渡の一例を示す。

- [0187] 図16(A)を参照して、エンティティAが同一の電子通貨10をエンティティBおよびエンティティCにそれぞれ渡した場合を想定する。
- [0188] 図16(B)に示すように、この場合には、エンティティAからエンティティBへの電子通貨10の移転を示すチェックポイントデータ48-1と、エンティティAからエンティティCへの電子通貨10の移転を示すチェックポイントデータ48-2とが電子通貨10に生成される。
- [0189] チェックポイントデータ48を処理時刻481に基づいてソートすると、チェックポイントデータ48-1の署名者公開鍵483と、チェックポイントデータ48-2の署名者公開鍵483とが同一となる。このような署名者公開鍵483の値に基づいて、電子通貨10の二重譲渡などの発生を検知できる。また、同一となった公開鍵の所有者が二重譲渡を行った者であると特定できる。
- [0190] すなわち、電子通貨10の不正な移転の有無を判断する処理は、電子通貨10に関連付けて、あるエンティティから複数のエンティティに電子通貨10をそれぞれ移転する記録（チェックポイントデータ48）が存在するか否かを判断する処理を含む。
- [0191] このように、台帳8または他のエンティティは、同一の電子通貨10に登録された複数のチェックポイントデータに基づいて、チェックポイントデータ48の整合性を検証する。
- [0192] (g5: 電子通貨10の有効期限)
- 本実施の形態に従う電子通貨基盤1においては、電子通貨10に有効期限が設定されている。中央銀行3（または、発行局2）は、有効期限が切れた電子通貨10に対応して、新たな電子通貨10を発行してもよい。
- [0193] 新たな電子通貨10は、有効期限が切れた電子通貨10を受信したタイミングで発行されてもよいし、当該タイミングとは独立して発行されてもよい。例えば、有効期限が切れた電子通貨10を受信すると、予め発行された電子通貨10（十分な有効期限が残っている）のうち、対応する金額の電子通貨10

貨１０を選択して提供してもよい。

[0194] なお、新たに提供される電子通貨１０の金額は、有効期限が切れた電子通貨１０の金額とは同一でなくてもよい。例えば、何らかの税金を予め控除してもよい。この場合には、新たに提供される電子通貨１０の金額は、有効期限が切れた電子通貨１０の金額から所定の税額が控除された金額となる。あるいは、インフレーションまたは金利などを反映してもよい。この場合には、新たに提供される電子通貨１０の金額は、有効期限が切れた電子通貨１０の金額より大きくなる。

[0195] このように、中央銀行３（または、発行局２）は、市中に流通する通貨の総額などを管理することもできる。

[0196] <Ｈ．電子通貨基盤１におけるチェックポイントデータの利用>

本実施の形態に従う電子通貨基盤１においては、電子通貨１０の各々の流通を完全にトレースできる。そのため、例えば、マネー・ローンダリングなどの犯罪行為または不法行為の発生を防止できる。

[0197] また、電子通貨１０の流通を統計的に処理することで、市中における経済活動の状態などを推定することもできる。さらに、電子通貨１０の流通に関与したエンティティを匿名化した上で統計情報を生成することで、経済指標などを算出することもできる。また、匿名化された統計情報を有償または無償で提供することもできる。

[0198] このように、本実施の形態に従う電子通貨基盤１においては、従来の通貨とは異なり、電子通貨１０の流通を完全にトレースできるので、経済的な分析などをより高精度に行うことができる。

[0199] 例えば、中央銀行３が台帳８に基づく監視を常時行うことで、電子通貨１０の不正な移転が発見されると、当該不正な移転を治安組織（例えば、警察など）に即座に通報するようにしてもよい。また、中央銀行３（または、中央銀行３から委託された機関）は、台帳８の登録内容に基づいて、裁判（刑事裁判および／または民事裁判）用の証拠を生成および提供するようにしてもよい。

- [0200] また、マネー・ローンダリングなどを防止するために、移転目的などを示す情報を電子通貨１０に追加するようにしてもよい。例えば、ＩＳＩＣ（International Standard Industrial Classification of All Economic Activities）に従うコードを用いてもよい。ユーザは、商品およびサービスの購入の対価として、電子通貨１０を支払う場合には、当該商品またはサービスを示すコードを電子通貨１０に付加してもよい。あるいは、電子通貨１０を受け取るエンティティが対象の商品またはサービスを示すコードを電子通貨１０に付加してもよい。
- [0201] なお、商品またはサービスを示すコードについては、上述のＩＳＩＣに限られず、任意のコード体系を用いることができる。国際的に標準化されたコード体系を用いてもよいし、特定の国において適用されるコード体系を用いてもよい。
- [0202] トランザクションＩＤと商品またはサービスを示すコード（すなわち、使用用途）とを組み合わせた情報を分析することで、マネー・ローンダリングの可能性などを推定できる。また、商品またはサービスを示すコードに基づいて、テロの可能性なども推定できる。
- [0203] また、中央銀行３（または、中央銀行３から委託された機関）は、台帳８の登録内容に基づいて、商品およびサービスの状況などを分析して、定期的にレポートを出力してもよい。このようなレポートは、経済状況や経済動向の分析に有効な情報となる。
- [0204] また、中央銀行３（または、中央銀行３から委託された機関）、または、税金の賦課徴収を担当する機関は、台帳８に基づいて、商品およびサービスに係る対価の支払いに応じた税金（例えば、付加価値税、物品税、消費税など）の課税を行ってもよい。本実施の形態に従う電子通貨基盤においては、商品およびサービスの対価の支払い元および支払い先のエンティティを管理できるので、各エンティティが支払うべき税金額を算出できる。さらに、中央銀行３または賦課徴収を担当する機関は、算出された額の税金を都度また

は機関毎に徴収してもよい。税金の徴収は、各エンティティの預金口座からの引き落としで行われてもよいし、各エンティティに対して算出された額の電子通貨の支払いを要求する形で行われてもよい。

[0205] このように、本実施の形態に従う電子通貨基盤は、少なくとも、行政機関による各種事務手続きおよび各種処理を支援できる。

[0206] <1. 利点>

本実施の形態に従う電子通貨基盤1によれば、少なくとも一部のエンティティは、少なくとも台帳8に記録された内容に基づいて、電子通貨10の不正な移転の有無を判断できる。仮想通貨とは異なり、任意のタイミングで台帳8を参照することで、電子通貨10の不正な移転の有無を判断できるので、ネットワークなどのリソースを大きく消費することがない。一方で、電子通貨10の不正な移転の有無を確実に判断できるので、安全な通貨流通を実現できる。

[0207] 今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて請求の範囲によって示され、請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

符号の説明

[0208] 1 電子通貨基盤、2 発行局、3 中央銀行、4 金融機関、5 販売者、6, 6A, 6B 消費者、8 台帳、10, 11, 12, 13, 14, 15, 16 電子通貨、22, 23, 24, 116, 216 鍵ペア、22A, 23A, 24A, 25A, 26A, 26AA, 26AB 秘密鍵、22B, 23B, 24B, 25B 公開鍵、31, 32, 33, 34, 48, 48A, 48B チェックポイントデータ、40 ドキュメントルートコントロールセクション、41 初期データ、42 信頼コントロールセクション、43 信頼認証セクション、44 トランザクションコントロールセクション、45 トランザクションデータ、46 スペシャルセクション、47 無効管理セクション、51 ローカル発行局、52 国務省、53 財務

省、54 公証人、55 政府機関、60 ネットワーク化ゾーン、62 非ネットワークゾーン、100 情報処理装置、102, 202 プロセッサ、104, 204 メモリ、106, 206 入力部、108, 208 表示部、110, 210 ストレージ、112, 212 OS、114, 214 アプリケーションプログラム、120 ネットワークインターフェイス、200 モバイル装置、220 カメラ、222 スピーカ、224 無線通信部、226 近距離通信部、431 有効期間開始時刻、432 有効期間終了時刻、433 ロールコード、434 発行者公開鍵、435, 455 エンティティ公開鍵、436, 484 署名データ、451 O f f e r エントリ、452 A c c e p t エントリ、453 種別、454 トランザクションID、481 処理時刻、482 ランダムノンス、483 署名者公開鍵。

請求の範囲

- [請求項1] 電子通貨基盤を実現するためのコンピュータによって実行される方法であって、
- 予め定められた財産的価値を付与された電子ファイルを生成するステップと、
- 前記電子ファイルに中央銀行の秘密鍵を用いて生成された第1の署名データを追加するステップと、
- 前記第1の署名データが追加された後、前記電子ファイルを第1のエンティティから第2のエンティティに移転するために、前記第1のエンティティの秘密鍵を用いて生成された第2の署名データを前記電子ファイルに追加するステップと、
- 前記電子ファイルの内容の少なくとも一部を台帳に記録するステップと、
- 少なくとも前記台帳に記録された内容に基づいて、前記電子ファイルの不正な移転の有無を判断するステップとを備える、方法。
- [請求項2] 前記電子ファイルの不正な移転の有無を判断するステップは、前記電子ファイルに関連付けて、前記第1のエンティティから複数のエンティティに前記電子ファイルをそれぞれ移転する記録が存在するか否かを判断するステップを含む、請求項1に記載の方法。
- [請求項3] 前記第1のエンティティから前記第2のエンティティに前記電子ファイルを送信した後に、前記第2のエンティティから前記第2のエンティティの秘密鍵を用いて生成された第3の署名データが追加された前記電子ファイルを受信すると、前記第1のエンティティが格納している前記電子ファイルを削除するステップをさらに備える、請求項1または2に記載の方法。
- [請求項4] 前記第2のエンティティが、前記第1のエンティティの公開鍵を用いて、前記電子ファイルに含まれる前記第2の署名データを検証するステップをさらに備える、請求項1～3のいずれか1項に記載の方法

。

- [請求項5] 前記電子ファイルは、有効期限の設定を含み、
前記方法は、前記電子ファイルを前記第1のエンティティから前記第2のエンティティに移転する前に、前記第1のエンティティおよび前記第2のエンティティの少なくとも一方が前記電子ファイルの有効期限が切れていないことを検証するステップをさらに備える、請求項1～4のいずれか1項に記載の方法。
- [請求項6] 前記第2のエンティティが前記第1のエンティティから前記電子ファイルを受信した後に実行される、前記電子ファイルの内容と前記台帳に記録された内容とを照合するステップをさらに備える、請求項1～5のいずれか1項に記載の方法。
- [請求項7] 前記電子ファイルの有効期限が切れている場合に、前記中央銀行が当該電子ファイルを回収するステップをさらに備える、請求項1～6のいずれか1項に記載の方法。
- [請求項8] 電子通貨基盤を実現するためのシステムであって、
予め定められた財産的価値を付与された電子ファイルを生成するための手段と、
前記電子ファイルに中央銀行の秘密鍵を用いて生成された第1の署名データを追加するための手段と、
前記第1の署名データが追加された後、前記電子ファイルを第1のエンティティから第2のエンティティに移転するために、前記第1のエンティティの秘密鍵を用いて生成された第2の署名データを前記電子ファイルに追加するための手段と、
前記電子ファイルの内容の少なくとも一部を記録するための台帳と、
少なくとも前記台帳に記録された内容に基づいて、前記電子ファイルの不正な移転の有無を判断する手段とを備える、システム。