(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2025年5月8日(08.05.2025)

WIPO | PCT

(10) 国際公開番号
WO 2025/094279 A1

(51) 国際特許分類:
G06Q 20/06 (2012.01) *G06Q 40/04* (2012.01)

(21) 国際出願番号： PCT/JP2023/039295

(22) 国際出願日： 2023年10月31日(31.10.2023)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 (JP).

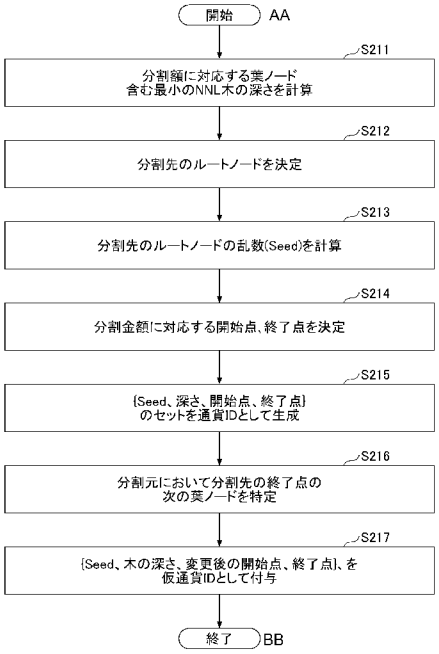
(72) 発明者: 奥田 哲矢(**OKUDA, Tetsuya**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 (JP). 山村 和輝(**YAMAMURA, Kazuki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 (JP). 阿部 正幸(**ABE, Masayuki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 (JP). 宮澤 俊之(**MIYAZAWA, Toshiyuki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 (JP). 福永 利徳(**FUKUNAGA, Toshinori**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 (JP).

(74) 代理人: 伊東 忠重, 外(**ITOH, Tadashige** et al.); 〒1000005 東京都千代田区丸の内二丁目１番１号 丸の内 ＭＹ ＰＬＡＺＡ （明治安田生命ビル） １６階 (JP).

(54) **Title:** CURRENCY PROCESSING DEVICE, CURRENCY PROCESSING METHOD, AND PROGRAM

(54) 発明の名称： 通貨処理装置、通貨処理方法及びプログラム

[図12]



S211 Calculate depth of minimum NNL tree including leaf nodes corresponding to divided amount
S212 Determine route node of divided tree
S213 Calculate random number (Seed) of route node of divided tree
S214 Determine start point and end point corresponding to divided amount
S215 Generate set of [Seed, depth, start point, end point] as currency ID
S216 Specify next leaf node of end point of divided tree in original tree of division
S217 Assign [Seed, depth of tree, changed start point, end point] as temporary currency ID
AA Start
BB End

(57) **Abstract:** This currency processing device efficiently implements a variable denomination system by including: a depth calculation unit configured to calculate a depth of an NNL tree including a specific number or more of leaf nodes, the specific number being obtained by dividing an amount to be transferred by the minimum unit of electronic currency; a root node determination unit configured to determine, in a first NNL tree added to first electronic currency, a root node of a second NNL tree, which is a partial tree of the first NNL tree, on the basis of the depth; a random number calculation

WO 2025/094279 A1

［続葉有］

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一　国際調査報告（条約第21条(3)）

unit configured to calculate a random number corresponding to the root node on the basis of a Seed of the first NNL tree; a leaf node determination unit configured to determine a range of leaf nodes corresponding to the amount from among the leaf nodes; and a currency addition information generation unit configured to generate information indicating the random number, the depth, and the range as information to be added to second electronic currency.

(57) 要約：通貨処理装置は、移転する金額を電子通貨の最小単位で除した値以上の数の葉ノードを含むＮＮＬ木の深さを計算するように構成されている深さ計算部と、第１の電子通貨に付加された第１のＮＮＬ木において、前記深さに基づいて前記第１のＮＮＬ木の部分木である第２のＮＮＬ木のルートノードを決定するように構成されているルートノード決定部と、前記第１のＮＮＬ木のＳｅｅｄに基づいて前記ルートノードに対応する乱数を計算するように構成されている乱数計算部と、前記葉ノードのうち、前記金額に対応させる葉ノードの範囲を決定するように構成されている葉ノード決定部と、前記乱数、前記深さ、前記範囲を示す情報を第２の電子通貨に付加する情報として生成するように構成されている通貨付加情報生成部と、を有することで、変動額面方式を効率的に実現可能とする。

明　細　書

発明の名称 ： 通貨処理装置、通貨処理方法及びプログラム

技術分野

[0001]　本発明は、通貨処理装置、通貨処理方法及びプログラムに関する。

背景技術

[0002]　電子現金については長年研究が行われている。また、各国政府が電子通貨の検討を進めている。電子現金の研究においては、通貨単位ごとに発行銀行による署名を打つことで、利用者間のみで取引を完結させることができるトークン型電子現金方式がある。

[0003]　トークン型電子現金方式には、電子通貨としてのトークンの金額を固定とする「固定額面方式」と、トークンの分割又は結合等によりトークンの金額の変動を許容する「変動額面方式」がある。

先行技術文献

特許文献

[0004] 特許文献1：国際公開第２０２２／２５４６２４号

発明の概要

発明が解決しようとする課題

[0005]　上記の従来技術は、固定額面方式を想定しており、変動額面方式を効率的に実現できないという問題があった。

[0006]　本発明は、上記の点に鑑みてなされたものであって、変動額面方式を効率的に実現可能とすること目的とする。

課題を解決するための手段

[0007]　そこで上記課題を解決するため、通貨処理装置は、移転する金額を電子通貨の最小単位で除した値以上の数の葉ノードを含むＮＮＬ木の深さを計算するように構成されている深さ計算部と、第１の電子通貨に付加された第１のＮＮＬ木において、前記深さに基づいて前記第１のＮＮＬ木の部分木である第２のＮＮＬ木のルートノードを決定するように構成されているルートノー

ド決定部と、前記第１のＮＮＬ木のＳｅｅｄに基づいて前記ルートノードに対応する乱数を計算するように構成されている乱数計算部と、前記葉ノードのうち、前記金額に対応させる葉ノードの範囲を決定するように構成されている葉ノード決定部と、前記乱数、前記深さ、前記範囲を示す情報を第２の電子通貨に付加する情報として生成するように構成されている通貨付加情報生成部と、を有する。

発明の効果

[0008] 変動額面方式を効率的に実現可能とすることができる。

図面の簡単な説明

[0009] [図1]ＮＮＬ木を説明するための図である。

[図2]本実施の形態における通貨に対するＮＮＬ木の適用方法を説明するための図である。

[図3]電子通貨システムのシステム構成の一例を示す図である。

[図4]発行銀行サーバの機能構成図である。

[図5]ルート認証局サーバの機能構成図である。

[図6]金融機関サーバの機能構成図である。

[図7]中間認証局サーバの機能構成図である。

[図8]利用者端末の機能構成図である。

[図9]通貨発行処理の流れの一例を示すシーケンス図である。

[図10]通貨発行時における通貨ＩＤの生成処理の処理手順の一例を説明するためのフローチャートである。

[図11]引出処理の流れの一例を示すシーケンス図である。

[図12]通貨の分割処理の処理手順の一例を説明するためのフローチャートである。

[図13]支払処理の流れの一例を示すシーケンス図である。

[図14]両替処理の流れの一例を示すシーケンス図である。

[図15]与信処理の流れの一例を示すシーケンス図である。

[図16]預入処理の流れの一例を示すシーケンス図である。

[図17]還収処理の流れの一例を示すシーケンス図である。

[図18]第２実施形態に係るマークルツリーのＭＨＴｒｅｅ関数について説明するための図である。

[図19]第２実施形態に係るマークルツリーのＭＨＰａｔｈ関数について説明するための第一の図である。

[図20]第２実施形態に係るマークルツリーのＭＨＶｅｒ関数について説明するための図である。

[図21]８枚の通貨が有る状態を示す図である。

[図22]８枚の通貨に対して同じ署名を含む通貨付加情報が付加された状態を示す図である。

[図23]コンピュータのハードウェア構成例を示す図である。

発明を実施するための形態

[0010] 以下、図面を参照して本発明の実施の形態（本実施の形態）を説明する。以下で説明する実施の形態は一例に過ぎず、本発明が適用される実施の形態は、以下の実施の形態に限られるわけではない。

[0011] （第１実施形態の概要）

第１実施形態に係る電子通貨システムは、特定の発行銀行にて発行する電子通貨のシステムである。電子通貨の価値は法定通貨と同じ価値が保証されるものが提唱されている。以下、日本円と同価値の電子通貨を例に説明するが、これに限られず、他の国に法定通貨と同価値の電子通貨であっても良いし、法定通貨と同価値の電子通貨でなくても良い。

[0012] 第１実施形態に係る電子通貨システムでは、発行銀行が管理するサーバが署名をして電子通貨（以下、単に通貨という）を発行する。また、発行銀行以外の金融機関（例えば市中銀行）にて取引の履歴データを管理する。また、利用者同士の取引では、お互いの利用者の端末同士が直接通信して、取引のための処理を実行する。

[0013] 本実施の形態において、通貨の金額は、最小単位（例えば、１円）の集合として表現される。最小単位未満への通貨の分解は許容されない。最小単位

が１円であれば、１円単位の固定額面方式を採用することで、（実質的に）変動額面方式（トークンの分割）を実現する。

[0014] 各通貨の真正性を保証するため、上記したように各通貨には発行銀行のサーバによる署名が付加される。１円の集合で通貨を表現する場合、例えば、１００００円の発行の際には、１００００回の署名が行われる必要がある。この場合、発行時・支払時などの署名生成及び検証コストが非現実的となる。そこで、本実施の形態では、最小単位（１円）をＬｅａｆ（葉ノード）とする１つの木構造で１つの通貨の金額を表現することで、発行時・支払時などの署名生成及び検証回数を１回とする。

[0015] 本実施の形態では、斯かる木構造としてＮＮＬ木（参考文献［１］）を採用し、発行時も署名を１回に、かつ、データサイズを非線形に圧縮する。

[0016] 図１は、ＮＮＬ木を説明するための図である。図１では、Ｓｅｅｄ（シード）としてのＩＤ（図１ではｎビットの乱数）に対して、入力された乱数から２倍の長さの乱数を生成する疑似乱数生成器Ｇ：｛０，１｝^{n}→｛０，１｝^{2n}を適用して、２ｎビットのＩＤを生成する。その２ｎビットの前半のｎビットと後半のｎビットとのそれぞれに対して疑似乱数生成器Ｇを適用することで更に２ｎビットの乱数を生成し、合計で４つのｎビットのＩＤ（乱数）が生成される例が示されている。

[0017] ＮＮＬ木よれば、Ｓｅｅｄさえ分かれば誰でも４つのＩＤを求めることができるため、４つのＩＤ（４ｎビット）の情報をｎビットの情報（Ｓｅｅｄ）のみで伝達可能となる。

[0018] なお、図１では、葉ノードが４つである例を示したが、ＮＮＬ木の深さは特定のものに限定されない。

[0019] 図２は、本実施の形態における通貨に対するＮＮＬ木の適用方法を説明するための図である。

[0020] 上記したように、本実施の形態において、通貨の金額はＮＮＬ木によって表現される。具体的には、ＮＮＬ木の葉ノードが最小単位（例えば、１円）に対応し、或るＮＮＬ木に属する葉ノードの数によって当該ＮＮＬ木に対応

する通貨の金額が決まる。但し、このままでは、ＮＮＬ木が２分木であることを前提とした場合、２の冪乗での金額しか表現できない。そこで、通貨に対応する葉ノードを指定可能とする。具体的には、ＮＮＬ木の全葉ノードのうち、通貨に対応する葉ノードの範囲を示す情報を指定可能とすることで、当該ＮＮＬ木に対応する通貨が、当該範囲に含まれる全葉ノードの数×１円であることを表現可能とする。本実施の形態では、斯かる範囲を示す情報として当該範囲の開始点及び終了点が用いられる例を示す。開始点とは、当該範囲の開始位置となる葉ノードをいう。終了点とは、当該範囲の終了位置となる葉ノードをいう。開始点及び終了点のいずれか一方は、葉ノードの並び順において端（最初又は最後）の葉ノードであるとする。但し、当該範囲を示す情報は開始点及び終了点に限られない。例えば、当該範囲に属する全ての葉ノードが指定されてもよいし、開始点と当該範囲の大きさ（つまり、金額）又は終了点と当該範囲の大きさが指定されてもよい。

[0021] 例えば、深さが１０である２分木のＮＮＬ木であれば、葉ノードの数は１０２４個である。１０００円を表現したいのであれば、例えば、開始点を１とし、終了点を１０００と指定すればよい。

[0022] また、上記したように、ＮＮＬ木は、Ｓｅｅｄと深さが分かれば、誰でも全ての葉ノードを導出することができる。そこで、本実施の形態では、１つの通貨の金額を４つのパラメータの組によって表現する。

[0023] {ＮＮＬ木のＳｅｅｄ、当該ＮＮＬ木の深さ、開始点、終了点}

以下、これら４つのパラメータの組を「通貨ＩＤ」という。

[0024] 通貨に対する署名（例えば、発行元又は分割元による署名）は、当該通貨に対応するＮＮＬ木のＳｅｅｄ単位で行うことで実現される。したがって、署名の数を通貨の最小単位（例えば、１円）ごとではなく、通貨（ＮＮＬ木）の数ごととすることができる。

[0025] 例えば、図２のＮＮＬ木の開始点がＩＤ１、終了点がＩＤ８である場合、当該ＮＮＬ木は８円を表現する。この８円から、ＩＤ１～ＩＤ４までの４円を分割したい場合、例えば、ＩＤ１～ＩＤ４までの全ての祖先ノードである

ノードｎ１に対応するＩＤ（乱数）が分割後の４円に対応する部分木（ＮＮＬ木）のルートノードとなる。したがって、この場合、分割後の４円の通貨の通貨ＩＤは以下のようになる。

｛０１１１０…１，２，ＩＤ１，ＩＤ４｝

分割後の部分木のルートノードのＳｅｅｄを計算しておくことで、その後における当該部分木の各ノードに対応する乱数の計算回数を削減することができる。この場合、発行銀行によって発行された通貨（後述のT_0）には署名の履歴に基づいて辿ることができる。

[0026] 但し、分割元のＮＮＬ木のルートノードを分割後のＮＮＬ木のルートノードとしてもよい。この場合、分割後の４円の通貨の通貨ＩＤは以下のようになる。

｛０１０１０…１，３，ＩＤ１，ＩＤ４｝

この場合、発行銀行によって発行された通貨（後述のT_0）まで辿って検証するための計算効率が良いという利点が有る。

[0027] なお、図２には、便宜上、各ノードに対応する乱数が示されているが、各ノードに対応する乱数は、通貨（ＮＮＬ木）の分割が行われるまでは管理されなくてよい。換言すれば、分割の際に分割元のＮＮＬ木のＳｅｅｄから、分割後のＳｅｅｄの乱数が計算されればよい。

[0028] また、ＮＮＬ木は２分木に限られず、２，５，１０分木でもよい。２分岐／５分岐・・・と繰り返せば、日常の現金に近い５０００円／１０００円等に葉ノードの数が完全に一致するＮＮＬ木を生成することができる。この場合、５分岐の箇所では疑似乱数生成器G_5：｛０，１｝^{n}→｛０，１｝^{5n}を使用し、１０分岐の箇所では疑似乱数生成器G_{10}：｛０，１｝^{n}→｛０，１｝^{10n}を使用すればよい。

[0029] 以下、第１実施形態に係る構成と動作を説明する。

[0030] （第１実施形態の詳細）

図３は、電子通貨システムのシステム構成の一例を示す図である。第１実施形態に係る電子通貨システム１は、発行銀行サーバ１０と、ルート認証局

サーバ１１と、金融機関サーバ２０と、中間認証局サーバ２５と、利用者端末３０と、を備える。これらの各装置は、インターネット等の通信ネットワークを介して、互いに通信可能に接続されている。

[0031] 発行銀行サーバ１０は、通貨を発行する発行銀行が管理する情報処理装置である。発行銀行サーバ１０は、通貨の発行を示すメッセージデータに署名データを付加して金融機関サーバ２０に送信する。他に、発行銀行サーバ１０は、金融機関サーバ２０からの還収の要求を受け付ける機能を有する。

[0032] ルート認証局サーバ１１は、暗号通信におけるルート認証局の機能を有する情報処理装置である。ルート認証局サーバ１１は、発行銀行サーバ１０と同一のハードウェアによって実現されても良く、発行銀行によって管理されることを想定するが、それに限られない。

[0033] ルート認証局サーバ１１は、通貨の発行の準備段階として、ルート認証鍵を生成してルート証明書を発行し、中間認証局サーバ１２に送信する。また、ルート認証局サーバ１１は、各金融機関を認証し、金融機関公開鍵証明書発行情報を生成し、生成された金融機関公開鍵証明書発行情報を発行銀行サーバ１０に送信する。

[0034] 金融機関サーバ２０は、金融機関（例えば市中銀行）が管理する情報処理装置である。金融機関サーバ２０は、ルート認証局サーバ１１による認証を受けて、発行銀行サーバ１０から通貨の発行を受け付ける。

[0035] また、金融機関サーバ２０は、利用者端末３０から、引出、両替、預入、与信などの取引の要求を受け付ける。さらに、金融機関サーバ２０は、発行銀行サーバ１０に還収を要求する。

[0036] なお、以下の説明において各金融機関サーバ２０を区別する時は、各金融機関サーバ２０を金融機関サーバ２０－１、金融機関サーバ２０－２等のように記載する。

[0037] 中間認証局サーバ２５は、暗号通信における中間認証局の機能を有する情報処理装置である。中間認証局サーバ２５は、金融機関サーバ２０と同一のハードウェアによって実現されても良く、金融機関によって管理されること

を想定するが、それに限られない。

[0038] 中間認証局サーバ２５は、通貨の発行の準備段階として、中間認証鍵を生成して中間証明書を発行し、利用者端末３０に送信する。また、中間認証局サーバ２５は、各利用者を認証し、利用者公開鍵証明書発行情報を生成する。

[0039] なお、以下の説明において各中間認証局サーバ２５を区別する時は、各中間認証局サーバ２５を中間認証局サーバ２５－１、中間認証局サーバ２５－２等のように記載する。

[0040] 利用者端末３０は、通貨を利用する利用者（個人消費者、店舗等）が利用する情報処理装置である。利用者端末３０は、取引を開始する前に、中間認証局サーバ２５による認証を受ける。また、利用者端末３０は、引出、両替、預入、与信などの取引を金融機関サーバ２０に要求する。

[0041] なお、以下の説明において各利用者端末３０を区別する時は、各利用者端末３０を利用者端末３０－１、利用者端末３０－２等のように記載する。

[0042] 利用者端末３０（例えば利用者端末３０－１）は、他の利用者端末３０（例えば利用者端末３０－２）に支払を要求したり、支払の要求を受け付けたりする。ここで、支払の要求とは、利用者が相手方に支払う「支払」取引の実行を受け付けるように要求することであり、相手方に利用者への支払いを要求することではない。

[0043] （第１実施形態に係る各装置の機能構成例）

次に、第１実施形態に係る各装置の機能構成例について説明する。

[0044] 図４は、発行銀行サーバの機能構成図である。発行銀行サーバ１０は、通貨発行鍵生成部１０１と、通貨発行証明書発行部１０２と、金融機関公開鍵証明書発行情報取得部１０３と、通貨発行部１０４と、還収受付部１０５と、通貨発行鍵記憶部１０６と、還収済通貨記憶部１０７と、を備える。

[0045] 通貨発行鍵生成部１０１は、通貨の発行を示すメッセージデータ（以下、通貨発行メッセージという）の正当性を保証するための暗号鍵データ（以下、通貨発行鍵という）を生成する。通貨発行鍵は、秘密鍵と公開鍵とを含む

。

[0046] 通貨発行証明書発行部１０２は、通貨発行鍵の公開鍵を証明するための証明書を示すデータ（以下、通貨発行証明書という）を生成して、生成された通貨発行証明書を各金融機関サーバ２０および各利用者端末３０に送信する。

[0047] 金融機関公開鍵証明書発行情報取得部１０３は、ルート認証局サーバ１１から金融機関公開鍵証明書発行情報を取得する。金融機関公開鍵証明書発行情報については、後述する。

[0048] 通貨発行部１０４は、通貨発行鍵および金融機関公開鍵証明書発行情報を使用して、通貨発行メッセージを生成し、生成した通貨発行メッセージを金融機関サーバ２０に送信する。

[0049] 還収受付部１０５は、金融機関サーバ２０から還収を受け付けて、還収済通貨記憶部１０７に還収された通貨を格納する。還収とは、各金融機関が当面使用しない通貨を発行銀行に預け入れて、流通に戻す取引である。

[0050] 通貨発行鍵記憶部１０６は、通貨発行鍵生成部１０１によって生成された通貨発行鍵を記憶する。

[0051] 還収済通貨記憶部１０７は、還収受付部１０５が還収を受け付けた通貨（以下、還収済通貨という）を記憶する。

[0052] 図５は、ルート認証局サーバの機能構成図である。ルート認証局サーバ１１は、ルート認証鍵生成部１１１と、ルート証明書発行部１１２と、金融機関認証部１１３と、金融機関公開鍵証明書発行情報送信部１１４と、ルート認証鍵記憶部１１５と、金融機関公開鍵証明書発行情報記憶部１１６と、を備える。

[0053] ルート認証鍵生成部１１１は、ルート認証局の正当性を保証するための暗号鍵データ（以下、ルート証明鍵という）を生成する。ルート証明鍵は、秘密鍵と公開鍵とを含む。

[0054] ルート証明書発行部１１２は、中間認証局の正当性を保証するための証明書データ（以下、中間証明書）の正当性を保証するための証明書データ（以

下、ルート証明書という）を発行して、各中間認証局サーバ２５に送信する。

[0055] 金融機関認証部１１３は、金融機関サーバ２０から各金融機関の正当性を保証するための暗号鍵データ（以下、金融機関鍵という）を受信して、認証の要求を受け付ける。そして、金融機関認証部１１３は、金融機関鍵の公開鍵を証明するための証明書を示すデータ（以下、金融機関公開鍵証明書という）を生成し、生成された金融機関公開鍵証明書を、認証を要求した金融機関サーバ２０に送信する。さらに、金融機関認証部１１３は、金融機関公開鍵証明書の発行を示す情報（以下、金融機関公開鍵証明書発行情報という）を、生成する。

[0056] 金融機関公開鍵証明書発行情報送信部１１４は、生成された金融機関公開鍵証明書発行情報を、発行銀行サーバ１０に送信する。なお、発行銀行サーバ１０とルート認証局サーバ１１とが同一のハードウェアによって実現される場合には、金融機関公開鍵証明書発行情報送信部１１４は不要である。

[0057] ルート認証鍵記憶部１１５は、ルート認証鍵生成部１１１によって生成されたルート認証鍵を記憶する。

[0058] 金融機関公開鍵証明書発行情報記憶部１１６は、金融機関認証部１１３によって生成された金融機関公開鍵証明書発行情報を記憶する。

[0059] 図６は、金融機関サーバの機能構成図である。金融機関サーバ２０は、通貨発行証明書発行受付部２０１と、金融機関鍵生成部２０２と、金融機関認証要求部２０３と、通貨発行受付部２０４と、引出受付部２０５と、更新処理部２０６と、両替・預入受付部２０７と、支払要求部２０８と、支払受付部２０９と、与信受付部２１０と、還収要求部２１１と、通貨発行証明書記憶部２１２と、金融機関鍵記憶部２１３と、金融機関公開鍵証明書記憶部２１４と、未使用通貨記憶部２１５と、使用中通貨記憶部２１６と、更新済通貨記憶部２１７と、使用済通貨記憶部２１８と、を備える。

[0060] 通貨発行証明書発行受付部２０１は、発行銀行サーバ１０から通貨発行証明書の発行を受け付ける。

[0061] 金融機関鍵生成部２０２は、金融機関鍵を生成する。金融機関鍵は、秘密鍵と公開鍵とを含む。

[0062] 金融機関認証要求部２０３は、ルート認証局サーバ１１に、金融機関鍵を送信して金融機関の認証を要求し、ルート認証局サーバ１１から金融機関公開鍵証明書を受信する。

[0063] 通貨発行受付部２０４は、発行銀行サーバ１０から通貨の発行を受け付ける。具体的には、通貨発行受付部２０４は、発行銀行サーバ１０から通貨発行メッセージを受信し、受信した通貨発行メッセージの署名を、通貨発行証明書に含まれる公開鍵を用いて検証する。

[0064] 引出受付部２０５は、利用者端末３０から引出の要求を受け付けて、利用者端末３０に通貨を送信する。

[0065] 更新処理部２０６は、利用者端末３０からの引出の要求に対して、必要に応じて使用済みの通貨（以下、使用済通貨という）を更新する。具体的には、更新処理部２０６は、使用済通貨に付加された情報（通貨付加情報）を削除する。なお、通貨付加情報は、後述する支払の取引によって付加される。引出受付部２０５は、未使用の通貨（以下、未使用通貨という）または更新処理部２０６によって更新された通貨を利用者端末３０に送信する。

[0066] 両替・預入受付部２０７は、利用者端末３０から両替または預入の要求を受け付ける。具体的には、両替・預入受付部２０７が、利用者端末３０から両替の要求を受け付けると、支払受付部２０９が、両替する額面の支払を受け付けて、支払要求部２０８が、合計が両替する額面となる複数の支払いを要求する。また、両替・預入受付部２０７が、預入の要求を受け付けると、支払受付部２０９が、預け入れる額面の支払を受け付ける。

[0067] 与信受付部２１０は、利用者端末３０から通貨を受信して与信の要求を受け付ける。与信受付部２１０は、通貨が使用中の通貨（以下、使用中通貨という）であるか否かを判定し、判定結果を利用者端末３０に送信する。

[0068] 還収要求部２１１は、発行銀行サーバ１０に通貨を送信して、還収を要求する。

[0069] 通貨発行証明書記憶部２１２は、通貨発行証明書発行受付部２０１が発行を受け付けた通貨発行証明書を記憶する。

[0070] 金融機関鍵記憶部２１３は、金融機関鍵生成部２０２が生成した金融機関鍵を記憶する。

[0071] 金融機関公開鍵証明書記憶部２１４は、金融機関認証要求部２０３がルート認証局サーバ１１から受信した金融機関公開鍵証明書を記憶する。

[0072] 未使用通貨記憶部２１５は、通貨発行受付部２０４が発行を受け付けた通貨を未使用通貨として記憶する。

[0073] 使用中通貨記憶部２１６は、引出受付部２０５が引出を受け付けた通貨を使用中通貨として記憶する。

[0074] 更新済通貨記憶部２１７は、更新処理部２０６によって更新された通貨（以下、更新済通貨という）を更新前の状態で記憶する。

[0075] 使用済通貨記憶部２１８は、使用された通貨であって、使用中でない通貨を記憶する。具体的には、使用済通貨記憶部２１８は、両替・預入受付部２０７が両替または預入の要求を受け付けて、支払受付部２０９によって支払を受け付けて受信した通貨を、使用済通貨として記憶する。

[0076] 図７は、中間認証局サーバの機能構成図である。中間認証局サーバ２５は、中間認証鍵生成部２５１と、中間証明書発行部２５２と、利用者認証部２５３と、中間認証鍵記憶部２５４と、利用者公開鍵証明書発行情報記憶部２５５と、を備える。

[0077] 中間認証鍵生成部２５１は、中間認証局の正当性を保証するための暗号鍵データ（以下、中間認証鍵という）を生成する。中間認証鍵は、秘密鍵と公開鍵とを含む。

[0078] 中間証明書発行部２５２は、中間証明書を発行して、各利用者端末３０に送信する。

[0079] 利用者認証部２５３は、利用者端末３０から各利用者の正当性を保証するための暗号鍵データ（以下、利用者鍵という）を受信して、認証の要求を受け付ける。そして、利用者認証部２５３は、利用者鍵の公開鍵を証明するた

めの証明書を示すデータ（以下、利用者公開鍵証明書という）を生成し、生成された利用者公開鍵証明書を、認証を要求した利用者端末３０に送信する。さらに、利用者認証部２５３は、利用者公開鍵証明書の発行を示す情報（以下、利用者公開鍵証明書発行情報という）を、生成する。

[0080] 中間認証鍵記憶部２５４は、中間認証鍵生成部２５１が生成した中間認証鍵を記憶する。

[0081] 利用者公開鍵証明書発行情報記憶部２５５は、利用者認証部２５３が生成した利用者公開鍵証明書発行情報を記憶する。

[0082] 図８は、利用者端末３０の機能構成図である。利用者端末３０は、通貨発行証明書発行受付部３０１と、中間証明書発行受付部３０２と、利用者鍵生成部３０３と、利用者認証要求部３０４と、引出要求部３０５と、支払要求部３０６と、支払受付部３０７と、両替・預入要求部３０８と、与信要求部３０９と、通貨発行証明書記憶部３１０と、中間証明書記憶部３１１と、利用者鍵記憶部３１２と、利用者公開鍵証明書記憶部３１３と、利用者通貨記憶部３１４と、を備える。

[0083] 通貨発行証明書発行受付部３０１は、発行銀行サーバ１０から通貨発行証明書の発行を受け付ける。

[0084] 中間証明書発行受付部３０２は、中間認証局サーバ２５から中間証明書の発行を受け付ける。

[0085] 利用者鍵生成部３０３は、利用者鍵を生成する。利用者鍵は、秘密鍵と公開鍵とを含む。

[0086] 利用者認証要求部３０４は、中間認証局サーバ２５に、利用者鍵を送信して利用者の認証を要求し、中間認証局サーバ２５から利用者公開鍵証明書を受信する。

[0087] 引出要求部３０５は、額面を指定して金融機関サーバ２０に引出を要求する。引出要求部３０５は、金融機関サーバ２０から引き出された通貨を受信する。

[0088] 支払要求部３０６は、支払う通貨を送信して、金融機関サーバ２０または

他の利用者端末３０に支払を要求する。

[0089] 支払受付部３０７は、支払われる通貨を受信して、金融機関サーバ２０または他の利用者端末３０から支払を受け付ける。

[0090] 両替・預入要求部３０８は、金融機関サーバ２０に両替または預入を要求する。具体的には、両替・預入要求部３０８が両替を要求し、金融機関サーバ２０が受け付けると、支払要求部３０６が、両替する額面の通貨を送信して、金融機関サーバ２０に支払を要求し、支払受付部３０７が、合計が両替する額面となる複数の支払いを金融機関サーバ２０から受け付ける。また、両替・預入要求部３０８が預入を要求し、金融機関サーバ２０が受け付けると、支払要求部３０６が、預け入れる通貨を送信して、金融機関サーバ２０に支払を要求する。

[0091] 与信要求部３０９は、通貨を送信して金融機関サーバ２０に与信を要求し、与信結果を受信する。

[0092] 通貨発行証明書記憶部３１０は、通貨発行証明書発行受付部３０１が発行を受け付けた通貨発行証明書を記憶する。

[0093] 中間証明書記憶部３１１は、中間証明書発行受付部３０２が発行を受け付けた中間証明書を記憶する。

[0094] 利用者鍵記憶部３１２は、利用者鍵生成部３０３によって生成された利用者鍵を記憶する。

[0095] 利用者公開鍵証明書記憶部３１３は、利用者認証要求部３０４が受信した利用者公開鍵証明書を記憶する。

[0096] 利用者通貨記憶部３１４は、利用者が使用中の通貨を記憶する。具体的には、利用者通貨記憶部３１４は、引出要求部３０５が金融機関サーバ２０から受信した通貨と、支払受付部３０７が金融機関サーバ２０または他の利用者端末３０から受信した通貨と、を記憶する。

[0097] （第１実施形態に係る電子通貨システムの動作）

次に、第１実施形態に係る電子通貨システム１の動作について説明する。以下、発行銀行をB_0、各金融機関をB_i（B_0，B_1，・・・）、ルート認証

局をA_0、各中間証明局をA_i（A_0，A_1，・・・）、各利用者をU_j（U_0，U_1，・・・）、という記号で概念を示しながら説明する。

[0098] 図９は、通貨発行処理の流れの一例を示すシーケンス図である。通貨発行処理は、定期的に、または担当者の操作等を受けて開始される。

[0099] 発行銀行サーバ１０の通貨発行鍵生成部１０１は、通貨発行鍵を生成する（ステップＳ１０１）。具体的には、通貨発行鍵生成部１０１は、発行年ｙと発行額ｖに対応する通貨発行鍵のペア（秘密鍵skB_{0vy}および公開鍵pkB_{0vy}）を生成する。

[0100] そして、通貨発行証明書発行部１０２は、公開鍵pkB_{0vy}を証明する通貨発行証明書ＣＥＲＴ（pkB_{0vy}）を各金融機関サーバ２０に送信し（ステップＳ１０２）、各利用者端末３０に送信する（ステップＳ１０３）。各金融機関サーバ２０の通貨発行証明書発行受付部２０１は、通貨発行証明書ＣＥＲＴ（pkB_{0vy}）を受信して、通貨発行証明書記憶部２１２に記憶させる。また、各利用者端末３０の通貨発行証明書発行受付部３０１は、通貨発行証明書ＣＥＲＴ（pkB_{0vy}）を受信して、通貨発行証明書記憶部３１０に記憶させる。

[0101] 発行額ｖは、最小単位（例えば、１円）の倍数である。例えば、２０２１年に１００００円の通貨を発行する場合、通貨発行証明書発行部１０２は、通貨発行証明書ＣＥＲＴ（$pkB_{0(10000円)(2021年)}$）を各金融機関サーバ２０および各利用者端末３０に送信する。

[0102] なお、通貨発行証明書発行部１０２は、通貨発行証明書ＣＥＲＴ（pkB_{0vy}）を直接に各金融機関サーバ２０および各利用者端末３０に送信しなくても良く、例えば、通信ネットワークで公開されているサーバ装置等にアップロードし、各金融機関サーバ２０および各利用者端末３０にダウンロードさせるようにしても良い。

[0103] 次に、ルート認証局サーバ１１のルート認証鍵生成部１１１は、ルート認証鍵を生成する（ステップＳ１０４）。ルート認証鍵は、秘密鍵skA_0および公開鍵pkA_0を含む。続いて、ルート証明書発行部１１２は、秘密鍵ｓｋ

A_0で署名してルート証明書Ａｕｔｈ（ｐｋA_0）を生成し、各金融機関サーバ２０に送信する（ステップＳ１０５）。

[0104] なお、ルート証明書発行部１１２は、直接にルート証明書Ａｕｔｈ（ｐｋA_0）を各金融機関サーバ２０に送信しなくても良く、例えば、通信ネットワークで公開されているサーバ装置等にアップロードし、各金融機関サーバ２０にダウンロードさせるようにしても良い。

[0105] 続いて、中間認証局サーバ２５の中間認証鍵生成部２５１は、中間認証鍵を生成する（ステップＳ１０６）。中間認証鍵は、秘密鍵ｓｋA_iおよび公開鍵ｐｋA_iを含む。

[0106] 次に、中間証明書発行部２５２は、秘密鍵ｓｋA_iで署名し、ルート証明書Ａｕｔｈ（ｐｋA_0）を使用して中間証明書Ａｕｔｈ（ｐｋA_i，ｐｋA_0）を生成する。以下、中間証明書Ａｕｔｈ（ｐｋA_i，ｐｋA_0）はＡｕｔｈ（ｐｋA_i）と表記する。そして、中間証明書発行部２５２は、生成した中間証明書Ａｕｔｈ（ｐｋA_i）を各利用者端末３０に送信する（ステップＳ１０７）。各利用者端末３０の中間証明書発行受付部３０２は、中間証明書Ａｕｔｈ（ｐｋA_i）を受信して、中間証明書記憶部３１１に記憶させる。

[0107] なお、中間証明書発行部２５２は、直接に中間証明書Ａｕｔｈ（ｐｋA_i）を各利用者端末３０に送信しなくても良く、例えば、通信ネットワークで公開されているサーバ装置等にアップロードし、各利用者端末３０にダウンロードさせるようにしても良い。

[0108] 続いて、利用者端末３０の利用者鍵生成部３０３は、利用者鍵を生成する（ステップＳ１０８）。利用者鍵は、秘密鍵ｓｋU_jおよび公開鍵ｐｋU_jを含む。次に、利用者認証要求部３０４は、公開鍵ｐｋU_jを送信して、利用者認証を中間認証局サーバ２５に要求する（ステップＳ１０９）。

[0109] 中間認証局サーバ２５の利用者認証部２５３は、ルート証明書Ａｕｔｈ（ｐｋA_0）および中間証明書Ａｕｔｈ（ｐｋA_i）を用いて、利用者公開鍵証明書Ａｕｔｈ（ｐｋU_j，ｐｋA_i，ｐｋA_0）を生成する（ステップＳ１１０）。以下、利用者公開鍵証明書Ａｕｔｈ（ｐｋU_j，ｐｋA_i，ｐｋA_0）はＡ

ｕｔｈ（ｐｋＵ$_j$）と表記する。利用者認証部２５３は、生成した利用者公開鍵証明書Ａｕｔｈ（ｐｋＵ$_j$）を利用者端末３０に送信する（ステップＳ１１１）。利用者端末３０は、秘密鍵ｓｋＵ$_j$および公開鍵ｐｋＵ$_j$および利用者公開鍵証明書Ａｕｔｈ（ｐｋＵ$_j$）を保持する。

[0110] さらに、利用者認証部２５３は、利用者公開鍵証明書発行情報（Ｕ$_j$，ｐｋＵ$_j$，Ａｕｔｈ（ｐｋＵ$_j$））を生成し、利用者公開鍵証明書発行情報記憶部２５５に記憶させる。利用者公開鍵証明書発行情報（Ｕ$_j$，ｐｋＵ$_j$，Ａｕｔｈ（ｐｋＵ$_j$））は、利用者の個人情報Ｕ$_j$を含んでいる。

[0111] 次に、金融機関サーバ２０の金融機関鍵生成部２０２は、金融機関鍵を生成する（ステップＳ１１２）。金融機関鍵は、秘密鍵ｓｋＢ$_i$および公開鍵ｐｋＢ$_i$を含む。次に、金融機関認証要求部２０３は、公開鍵ｐｋＢ$_i$を送信して、金融機関認証をルート認証局サーバ１１に要求する（ステップＳ１１３）。

[0112] ルート認証局サーバ１１の金融機関認証部１１３は、ルート証明書Ａｕｔｈ（ｐｋＡ$_0$）を用いて、金融機関公開鍵証明書Ａｕｔｈ（ｐｋＢ$_i$，ｐｋＡ$_0$）を生成する（ステップＳ１１４）。以下、金融機関公開鍵証明書Ａｕｔｈ（ｐｋＢ$_i$，ｐｋＡ$_0$）はＡｕｔｈ（ｐｋＢ$_i$）と表記する。金融機関認証部１１３は、生成した金融機関公開鍵証明書Ａｕｔｈ（ｐｋＢ$_i$）を金融機関サーバ２０に送信する（ステップＳ１１５）。金融機関サーバ２０は、秘密鍵ｓｋＢ$_i$および公開鍵ｐｋＢ$_i$および金融機関公開鍵証明書Ａｕｔｈ（ｐｋＢ$_i$）を保持する。

[0113] さらに、金融機関認証部１１３は、金融機関公開鍵証明書発行情報（Ｂ$_i$，ｐｋＢ$_i$，Ａｕｔｈ（ｐｋＢ$_i$））を生成し、金融機関公開鍵証明書発行情報記憶部１１６に記憶させる。なお、金融機関公開鍵証明書発行情報（Ｂ$_i$，ｐｋＢ$_i$，Ａｕｔｈ（ｐｋＢ$_i$））は、金融機関についての機関情報Ｂ$_i$を含んでいる。そして、金融機関公開鍵証明書発行情報送信部１１４は、金融機関公開鍵証明書発行情報（Ｂ$_i$，ｐｋＢ$_i$，Ａｕｔｈ（ｐｋＢ$_i$））を発行銀行サーバ１０に送信する（ステップＳ１１６）。

[0114] 発行銀行サーバ１０の金融機関公開鍵証明書発行情報取得部１０３は、金融機関公開鍵証明書発行情報（B_i，pkB_i，Ａｕｔｈ（pkB_i））を取得して、金融機関公開鍵証明書発行情報記憶部１１６に記憶させる。

[0115] なお、ステップＳ１０８からステップＳ１１１までの処理と、ステップＳ１１２からステップＳ１１６までの処理の順序は一例であって、逆でも良い。ステップＳ１０８からステップＳ１１１までの処理は、各利用者端末３０によってそれぞれ個別に実行される。またステップＳ１１２からステップＳ１１６までの処理は、各金融機関サーバ２０によってそれぞれ個別に実行される。

[0116] また、利用者端末３０は、利用者鍵を追加するため、ステップＳ１０８からステップＳ１１１までの処理を複数回実行しても良い。

[0117] 次に、発行銀行サーバ１０の通貨発行部１０４は、金融機関公開鍵証明書発行情報記憶部１１６に記憶された金融機関公開鍵証明書発行情報（B_i，pkB_i，Ａｕｔｈ（pkB_i））を使用し、発行額ｖに基づく通貨ＩＤであるid_0、発行年ｙ、金融機関B_iを指定した通貨発行メッセージ（id_0，ｙ，B_i，pkB_i）を生成する（ステップＳ１１７）。なお、通貨ＩＤの構造については図２において説明した通りであるが、その生成方法については後述される。ここで、通貨発行部１０４は、通貨発行鍵記憶部１０６に記憶された通貨発行鍵の秘密鍵skB_{0vy}を使用して（id_0，ｙ，B_i，pkB_i）に署名する。通貨発行部１０４は、署名S_0が付加された通貨発行メッセージ（id_0，ｙ，B_i，pkB_i）を、金融機関サーバ２０に送信する（ステップＳ１１８）。なお、後述より明らかなように、通貨発行メッセージは、発行対象の通貨の生成に利用される。したがって、通貨発行メッセージの生成は、実質的に、通貨の発行に相当する。

[0118] 金融機関サーバ２０の通貨発行受付部２０４は、署名S_0が付加された通貨発行メッセージ（id_0，ｙ，B_i，pkB_i）を受信して、通貨発行証明書記憶部２１２に記憶された通貨発行証明書ＣＥＲＴ（pkB_{0vy}）に含まれる公開鍵pkB_{0vy}を使用して署名S_0を検証する。そして、通貨発行受付部２０

４は、通貨T_0：＝（id_0，ｙ，B_i，pkB_i，S_0）を生成して未使用通貨記憶部２１５に記憶させる。

[0119] ステップＳ１１７の通貨発行メッセージの生成における通貨ＩＤの生成について説明する。

[0120] 図１０は、通貨発行時における通貨ＩＤの生成処理の処理手順の一例を説明するためのフローチャートである。

[0121] ステップＳ１２１において、通貨発行部１０４は、発行額ｖに対応する数以上の葉ノードを含む最小のＮＮＬ木の深さを計算する。当該深さの計算は、実質的に、当該ＮＮＬ木の構造の生成に相当する。発行額ｖに対応する数以上の葉ノードとは、発行額ｖを表現可能な数の葉ノードをいい、発行額ｖを最小単位（例えば、１円）で除した値以上の数の葉ノードをいう。最小単位が１円であり、ｖ＝８円であれば、８個の葉ノードが必要となる。ＮＮＬ木を２分木とした場合、８個の葉ノードを含みうる２分木の深さは３以上である。したがって、３以上の中で最小の値である３が当該ＮＮＬ木の深さとなる。

[0122] 続いて、通貨発行部１０４は、当該ＮＮＬ木のＳｅｅｄとなる乱数を生成する（Ｓ１２２）。

[0123] 続いて、通貨発行部１０４は、当該ＮＮＬ木の葉ノードのうち、発行額ｖに対応させる葉ノードの開始点及び終了点を決定する（Ｓ１２３）。開始点及び終了点のいずれか一方が、当該ＮＮＬ木の端の葉ノードであり、開始点から終了点までの連続する葉ノードの集合が発行額ｖに一致するように、開始点及び終了点が決定される。なお、開始点及び終了点の値は、ＮＮＬ木の葉ノードにおける順番を示す値によって表現されればよい。すなわち、ＮＮＬ木において開始点及び終了点に対応する乱数は計算されなくてよい。

[0124] 続いて、通貨発行部１０４は、｛Ｓｅｅｄ，深さ，開始点，終了点｝のセットを通貨ＩＤとして生成する。

[0125] 図１１は、引出処理の流れの一例を示すシーケンス図である。引出処理は、利用者U_jの引出を指示する操作に応じて開始される。

[0126] 利用者端末３０の引出要求部３０５は、引出の額面ｖを示す額面情報と、利用者鍵記憶部３１２に記憶された利用者鍵の公開鍵pkU_jと、を送信して、金融機関サーバ２０に引出を要求する（ステップＳ２０１）。

[0127] 金融機関サーバ２０の引出受付部２０５は、引出を受け付ける（ステップＳ２０２）。具体的には、引出受付部２０５は、未使用通貨記憶部２１５から額面ｖ分の未使用通貨T_0を取得して、通貨付加情報T_1：＝（id_1，pkU_j，S_1）を付加した使用中通貨（T_1，T_0）として、使用中通貨記憶部２１６に記憶させる。S_1は、金融機関鍵の秘密鍵skB_iを用いた（id_1，pkU_j，T_0）に対する署名である。また、id_1は使用中通貨（T_1，T_0）の額面に基づく、移転対象の通貨の通貨ＩＤである。通貨T_0が額面ｖに一致する場合には、id_1の値は、通貨T_0の通貨ＩＤであるid_0と同じでよい。また、複数の通貨T_0のセットが額面ｖに一致する場合には、引出受付部２０５は、これらの通貨T_0ごとに通貨（T_1，T_0）を生成すればよい。この場合、各T_1のid_1の値は、対応するid_1と同じでよい。

[0128] 一方、通貨T_0が額面ｖを超える場合、又は複数の通貨T_0のセットでは額面ｖを超える場合、引出受付部２０５は、通貨T_0の一部を分割して通貨（T_1，T_0）を生成する。例えば、額面ｖが１０００円であり通貨T_0が５０００円である場合、引出受付部２０５は、通貨T_0から１０００円分を分割して１０００円としての通貨（T_1，T_0）を生成する。また、例えば、額面ｖが７０００円であり、各通貨T_0が５０００円である場合、引出受付部２０５は、２枚の通貨T_0のうちの一方から２０００円分を分割して２０００円としての通貨（T_1，T_0）を生成する。通貨T_0の分割は、通貨T_0が含むid_0としてのＮＮＬ木の分割によって実現される。ＮＮＬ木は通貨の金額をも表現するからである。このような通貨の分割処理については後述される。

[0129] このように、通貨が引出や支払等によって移転するたびに、当該通貨には移転元によって署名された通貨付加情報が累積的に付与される。したがって、通貨付加情報は、通貨の移転の履歴を示す情報であるともいえる。

[0130] 続いて、引出受付部２０５は、使用中通貨（T_1，T_0）の通貨データと、

金融機関公開鍵証明書Ａｕｔｈ（ｐｋＢ$_{i}$）とを利用者端末３０に送信する（ステップＳ２０３）。利用者端末３０の引出要求部３０５は、使用中通貨（Ｔ$_{1}$，Ｔ$_{0}$）の通貨データと、金融機関公開鍵証明書Ａｕｔｈ（ｐｋＢ$_{i}$）とを検証し、使用中通貨（Ｔ$_{1}$，Ｔ$_{0}$）を利用者通貨記憶部３１４に記憶させる。（Ｔ$_{1}$，Ｔ$_{0}$）を未使用通貨と呼んでもよい。

[0131] なお、ステップＳ２０２において、引出受付部２０５は、必要に応じて、未使用通貨記憶部２１５に記憶された未使用通貨ではなく使用済通貨記憶部２１８に記憶された使用済通貨を使用しても良い。この場合、更新処理部２０６が、使用済通貨を更新し、通貨付加情報が削除された通貨に更新する。引出受付部２０５は、使用済通貨を使用するか否かを、あらかじめ定められた条件にしたがって決定する。例えば、引出受付部２０５は、使用済通貨が閾値以上のデータ量になった場合に、使用済通貨を使用するようにしても良い。

[0132] 例えば、引出受付部２０５が使用済通貨（Ｔ$_{n}$，・・・，Ｔ$_{0}$）を引出に対して利用する場合、更新処理部２０６は、更新前の状態の通貨（Ｔ$_{n}$，・・・，Ｔ$_{0}$）を更新済通貨記憶部２１７に記憶させる。そして、更新処理部２０６は、使用済通貨（Ｔ$_{n}$，・・・，Ｔ$_{0}$）を、通貨付加情報（Ｔ$_{n}$，・・・，Ｔ$_{1}$）が削除された通貨Ｔ$_{0}$に更新する。そして、引出受付部２０５は、更新された通貨Ｔ$_{0}$に通貨付加情報Ｔ$_{n+1}$：＝（ｉｄ$_{n+1}$，ｐｋＵ$_{j}$，Ｓ$_{n+1}$）を付加した使用中通貨（Ｔ$_{n+1}$，Ｔ$_{0}$）を、使用中通貨記憶部２１６に記憶させる。この際、ｉｄ$_{n+1}$の値（内容）は、Ｔ$_{n}$に含まれている通貨ＩＤと同じでよい。

[0133] 続いて、引出受付部２０５は、使用中通貨（Ｔ$_{n+1}$，Ｔ$_{0}$）の通貨データと、金融機関公開鍵証明書Ａｕｔｈ（ｐｋＢ$_{i}$）とを利用者端末３０に送信する（ステップＳ２０３）。利用者端末３０の引出要求部３０５は、使用中通貨（Ｔ$_{n+1}$，Ｔ$_{0}$）の通貨データと、金融機関公開鍵証明書Ａｕｔｈ（ｐｋＢ$_{i}$）とを検証し、使用中通貨（Ｔ$_{n+1}$，Ｔ$_{0}$）を利用者通貨記憶部３１４に記憶させる。

[0134] また、更新処理部２０６は、すでに１回以上更新された通貨を再度更新し

ても良い。この場合、更新処理部２０６は、以前の更新前の状態の通貨（T_n，・・・T_1，T_0）に、今回の更新前の状態の通貨（T_{n+k}，・・・，T_{n+1}，T_0）を結合した通貨（T_{n+k}，・・・，T_1，T_0）を更新済通貨記憶部２１７に記憶させる。

[0135] ステップＳ２０２において、通貨の分割が必要な場合に実行される通貨の分割処理の詳細について説明する。図１２は、通貨の分割処理の処理手順の一例を説明するためのフローチャートである。

[0136] ステップＳ２１１において、引出受付部２０５は、引出の額面ｖに対応する数以上の葉ノードを含む最小のＮＮＬ木（以下、「分割先のＮＮＬ木」という。）の深さを計算する。斯かる深さの計算方法は、図１０のステップＳ１２１と同様である。

[0137] 続いて、引出受付部２０５は、分割対象の通貨の通貨ＩＤとしてのＮＮＬ木（以下、「分割元のＮＮＬ木」という。）のノードの中から、分割先のＮＮＬ木のルートノードとするノードを決定する（Ｓ２１２）。ここで、分割先のＮＮＬ木は、分割元のＮＮＬ木の部分木である。分割先のＮＮＬ木の深さが計算されているため、分割先のＮＮＬ木のルートノードが分割元のＮＮＬ木のどの階層のノードであるかが特定できる。引出受付部２０５は、当該階層に属するノードのうち、端に位置する（分割元のＮＮＬ木の開始点の祖先である）ノードを分割先のＮＮＬ木のルートノードとして決定する。例えば、図２において説明した分割が行われるのであれば、図２のノードＮ２が分割先のＮＮＬ木のルートノードとして決定される。

[0138] 続いて、引出受付部２０５は、当該ルートノードに対応する乱数（すなわち、分割先のＮＮＬ木のＳｅｅｄ）を、分割元のＮＮＬ木のＳｅｅｄに基づいて計算する（Ｓ２１３）。具体的には、図１において説明したように、分割元のＮＮＬ木のＳｅｅｄに対して疑似乱数生成器Ｇを再帰的に適用することで、分割先のＮＮＬ木のＳｅｅｄを算出することができる。

[0139] 続いて、引出受付部２０５は、分割先のＮＮＬ木の葉ノードのうち、額面ｖに対応させる葉ノードの開始点及び終了点を決定する（Ｓ２１４）斯かる

葉ノードの決定方法は、図１０のステップＳ１２３において説明した方法と同様でよい。

[0140] 続いて、引出受付部２０５は、｛分割先のＮＮＬ木のＳｅｅｄ，分割先のＮＮＬ木の深さ，開始点，終了点｝のセットを分割先の通貨の通貨ＩＤ（つまり、ステップＳ２０２における通貨付加情報T_1：＝（id_1，pkU_j，S_1）のid_1として生成する（Ｓ２１５）。

[0141] 続いて、引出受付部２０５は、分割元の通貨（Ｓ２０２におけるT_0）を残高（額面ｖを差し引いた額）に対応させるため、分割元のＮＮＬ木において、分割先の通貨の終了点となった次の葉ノードを特定する（Ｓ２１５）。

[0142] 続いて、引出受付部２０５は、｛分割元のＮＮＬ木のＳｅｅｄ，分割元のＮＮＬ木の深さ，当該次の葉ノード，分割元のＮＮＬ木の終了点｝を仮通貨ＩＤとして、分割元の通貨に関連付けておく（Ｓ２１７）。当該仮通貨ＩＤは、残高分の分割元の通貨が引出、支払等により移転する際に、通貨付加情報の通貨ＩＤとして利用される。

[0143] 図１３は、第１実施形態に係る支払処理（送金者から着金者への送信処理）の流れの一例を示すシーケンス図である。支払処理は、送金側の利用者U_jによる着金側の利用者U_kへの支払を指示する操作に応じて開始される。

[0144] 利用者端末３０－１は、送金側の利用者U_jが操作する利用者端末３０である。利用者端末３０－２は、着金側の利用者U_kが操作する利用者端末３０である。利用者端末３０－１の支払要求部３０６は、支払い額ｖ以上の通貨（T_{n-1}，・・・，T_0）から通貨付加情報を除く通貨データである通貨T_0と、T_{n-1}＝（id_{n-1}，pkU_j，S_{n-1}）と、利用者公開鍵証明書Ａｕｔｈ（pkU_j）とを送信して、支払を利用者端末３０－２に要求する（ステップＳ３０１）。なお、通貨T_0は、通貨（T_{n-1}，・・・，T_0）の現在の額面を示すものではない。通貨（T_{n-1}，・・・，T_0）の現在の額面は、T_{n-1}のid_{n-1}としてのＮＮＬ木の開始点及び終了点から導出可能である。

[0145] 利用者端末３０－２の支払受付部３０７は、支払を受け付ける（ステップＳ３０２）。具体的には、支払受付部３０７は、通貨T_0と、T_{n-1}＝（id_n

$_{n-1}$，ｐｋＵ$_{j}$，Ｓ$_{n-1}$）のＳ$_{n-1}$と、利用者公開鍵証明書Ａｕｔｈ（ｐｋＵ$_{j}$）とを検証する。ここで、支払受付部３０７は、通貨の検証においては、通貨に含まれる署名データを検証する。例えば、支払受付部３０７は、通貨Ｔ$_{0}$：＝（ｉｄ$_{0}$，ｙ，Ｂ$_{i}$，ｐｋＢ$_{i}$，Ｓ$_{0}$）の署名Ｓ$_{0}$を検証する。また、支払受付部３０７は、Ｔ$_{n-1}$＝（ｉｄ$_{n-1}$，ｐｋＵ$_{j}$，Ｓ$_{n-1}$）のＳ$_{n-1}$をｐｋＵ$_{j}$を用いて検証する。

[0146] 次に、支払受付部３０７は、利用者端末３０－２の利用者鍵記憶部３１２に記憶された利用者鍵の公開鍵ｐｋＵ$_{k}$を利用者端末３０－１に送信する（ステップＳ３０３）。利用者端末３０－１の支払要求部３０６は、通貨ＩＤとしてのｉｄ$_{n}$を生成し、ｉｄ$_{n}$と、受信した公開鍵ｐｋＵ$_{k}$と、通貨データ（例えばＴ$_{n-1}$、あるいは、Ｔ$_{n-1}$のハッシュ値）を含む情報に、利用者端末３０－１の利用者鍵記憶部３１２に記憶された利用者鍵の秘密鍵ｓｋＵ$_{j}$を使用して署名（Ｓ$_{n}$）を計算し、通貨付加情報Ｔ$_{n}$：＝（ｉｄ$_{n}$，ｐｋＵ$_{k}$，Ｓ$_{n}$）を生成する（ステップＳ３０４）。通貨付加情報を通貨データと呼んでもよい。ここで、ｉｄ$_{n}$は、これから生成される通貨（Ｔ$_{n}$，・・・，Ｔ$_{0}$）の額面に基づく通貨ＩＤである。通貨（Ｔ$_{n-1}$，・・・，Ｔ$_{0}$）が支払い額ｖに一致する場合には、ｉｄ$_{n}$の値は、通貨（Ｔ$_{n-1}$，・・・，Ｔ$_{0}$）のＴ$_{n-1}$の通貨ＩＤであるｉｄ$_{n-1}$と同じでよい。また、複数の通貨（Ｔ$_{n-1}$，・・・，Ｔ$_{0}$）のセットが支払い額ｖに一致する場合には、支払要求部３０６は、これらの通貨（Ｔ$_{n-1}$，・・・，Ｔ$_{0}$）ごとに通貨付加情報Ｔ$_{n}$：＝（ｉｄ$_{n}$，ｐｋＵ$_{k}$，Ｓ$_{n}$）を生成すればよい。この場合、各Ｔｎのｉｄ$_{n}$の値は、対応するｉｄ$_{n-1}$と同じでよく、後述される通貨（Ｔ$_{n}$，・・・，Ｔ$_{0}$）は、通貨（Ｔ$_{n-1}$，・・・，Ｔ$_{0}$）ごとに生成される。

[0147] 一方、通貨（Ｔ$_{n-1}$，・・・，Ｔ$_{0}$）が支払い額ｖを超える場合、又は複数の通貨（Ｔ$_{n-1}$，・・・，Ｔ$_{0}$）$_{0}$のセットでは支払い額ｖを超える場合、支払要求部３０６は、通貨（Ｔ$_{n-1}$，・・・，Ｔ$_{0}$）の一部を分割してｉｄ$_{n}$を生成する。すなわち、この場合のｉｄ$_{n}$は、通貨（Ｔ$_{n-1}$，・・・，Ｔ$_{0}$）におけるＴ$_{n-1}$の通貨ＩＤであるｉｄ$_{n-1}$としてのＮＮＬ木を分割元として、支払要求

部３０６が支払い額ｖだけ分割することで得られる分割先のＮＮＬ木の｛Ｓｅｅｄ，深さ，開始点，終了点｝である。斯かる分割を実行するための処理手順は、図１２において説明した通りである。すなわち、ステップＳ３０４において、支払要求部３０６は、図１２の処理手順を実行することでid_nを生成する。

[0148] 支払要求部３０６は、通貨付加情報（T_{n-1}，・・・，T_1）に、生成した通貨付加情報T_n：＝（id_n，pkU_k，S_n）を付加した通貨付加情報（T_n，・・・，T_1）を、利用者端末３０－２に送信する（ステップＳ３０５）。

[0149] 利用者端末３０－２の支払受付部３０７は、通貨付加情報（T_n，・・・，T_1）を検証する。具体的には、支払受付部３０７は、公開鍵pkU_jを用いてS_nを検証する。支払受付部３０７は、通貨付加情報に含まれるそれぞれの署名データを検証してもよい。例えば、支払受付部３０７は、通貨付加情報T_n：＝（id_n，pkU_j，S_n）の署名S_nを検証する。支払受付部３０７は、受信した通貨T_0に通貨付加情報（T_n，・・・，T_1）を付加した通貨（T_n，・・・，T_0）を、利用者端末３０－２の利用者通貨記憶部３１４に記憶させる。

[0150] 図１４は、両替処理の流れの一例を示すシーケンス図である。両替処理は、利用者U_jの両替を指示する操作に応じて開始される。

[0151] 利用者端末３０の両替・預入要求部３０８は、両替の額面ｖを示す額面情報と、利用者鍵記憶部３１２に記憶された利用者鍵の公開鍵pkU_jと、を送信して、金融機関サーバ２０に両替を要求する（ステップＳ４０１）。

[0152] 金融機関サーバ２０の両替・預入受付部２０７は、両替を受け付ける（ステップＳ４０２）。両替・預入受付部２０７は、両替の受付を示す両替受付情報を利用者端末３０に送信する（ステップＳ４０３）。

[0153] 利用者端末３０の両替・預入要求部３０８が、両替受付情報を受信すると、支払要求部３０６は、図１３に示される支払処理にしたがって、金融機関サーバ２０に支払を要求する（ステップＳ４０４）。

[0154] また、金融機関サーバ２０の支払要求部２０８は、合計して両替額ｖとな

る額v_1，・・・，v_xに両替する場合、v_1，・・・，v_xのそれぞれについて、図１３に示される支払処理にしたがって利用者端末３０に支払を要求する（ステップＳ４０５－１，Ｓ４０５－２）。

[0155] 図１５は、与信処理の流れの一例を示すシーケンス図である。与信処理は、利用者U_jの与信を指示する操作に応じて開始される。

[0156] 利用者端末３０の与信要求部３０９は、利用可否を確認したい通貨T_0を送信して、金融機関サーバ２０に与信を要求する（ステップＳ５０１）。金融機関サーバ２０の与信受付部２１０は、与信を受け付ける（ステップＳ５０２）。具体的には、与信受付部２１０は、通貨T_0を使用中通貨記憶部２１６から検索して、T_0を含むレコード、例えば（T_1，T_0）が存在すれば、与信成功ａｃｋを示す与信結果を利用者端末３０に送信する（ステップＳ５０３）。

[0157] 図１６は、預入処理の流れの一例を示すシーケンス図である。預入処理は、利用者U_jの預入を指示する操作に応じて開始される。

[0158] 利用者端末３０の両替・預入要求部３０８は、預入の額面ｖを示す額面情報と、利用者鍵記憶部３１２に記憶された利用者鍵の公開鍵pkU_jと、を送信して、金融機関サーバ２０に両替を要求する（ステップＳ６０１）。

[0159] 金融機関サーバ２０の両替・預入受付部２０７は、預入を受け付ける（ステップＳ６０２）。両替・預入受付部２０７は、預入の受付を示す預入受付情報を利用者端末３０に送信する（ステップＳ６０３）。

[0160] 利用者端末３０の両替・預入要求部３０８が、預入受付情報を受信すると、支払要求部３０６は、図１３に示される支払処理にしたがって、金融機関サーバ２０に支払を要求する（ステップＳ６０４）。

[0161] 図１７は、還収処理の流れの一例を示すシーケンス図である。還収処理は、金融機関B_iの還収を指示する操作に応じて開始される。

[0162] 金融機関サーバ２０の還収要求部２１１は、還収する通貨データを送信して、発行銀行サーバ１０に還収を要求する（ステップＳ７０１）。還収する通貨データは、未使用通貨でも使用済通貨でも良い。未使用通貨を還収する

場合は、還収要求部２１１は、未使用通貨T_0を未使用通貨記憶部２１５から抜き出して、発行銀行サーバ１０に送信する。

[0163] また、使用済通貨を還収する場合は、還収要求部２１１は、使用済通貨（T_n，・・・，T_0）を使用済通貨記憶部２１８から抜き出して、発行銀行サーバ１０に送信する。また、使用済通貨（T_m，・・・，T_{k+1}，T_0）が更新済みである場合には、還収要求部２１１は、更新済通貨記憶部２１７から更新前の通貨付加情報（T_k，・・・，T_1）を読み出して、使用済通貨（T_m，・・・，T_{k+1}，T_0）に結合し、結合された通貨（T_m，・・・，T_0）を発行銀行サーバ１０に送信する。

[0164] 発行銀行サーバ１０の還収受付部１０５は、還収を受け付ける（ステップＳ７０２）。具体的には、還収受付部１０５は、受信した通貨データを還収済通貨記憶部１０７に記憶させる。この際、還収受付部１０５は、各通貨付加情報に含まれている署名を検証することで、還収を受け付けた通貨の正当性を確認してもよい。例えば、通貨付加情報T_nに含まれている署名S_nは、通貨付加情報T_{n-1}に含まれている公開鍵を用いて検証することができる。

[0165] （第１実施形態の効果）

上述したように、第１実施形態によれば、変動額面方式を効率的に実現可能とすることができる。具体的には、通貨の最小単位を固定としつつも、最小単位の倍数の通貨を発行することができ、最小単位ごとではなく、通貨単位で署名及び検証を可能とすることができる。また、ＮＮＬ木方式を採用することで、ハッシュ演算の回数を削減することもできる。

[0166] （第２実施形態）

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

[0167] 第１実施形態では、引出、支払等によって通貨が移転する際に、通貨単位で検証が行われる必要がある。したがって、例えば、２千円の通貨を２つ有している利用者が３千円を支払いたい場合、１つの２千円と、もう１つの２

千円から分割した千円との２つの通貨を支払えばよいが、この場合、支払う側は通貨ごとに署名を生成し、支払を受ける側は通貨ごとに検証を行う必要がある。取引される通貨の数が多くなればなるほど、このような署名及び検証の負担は大きくなる。第２実施形態では、このような負担を軽減するための方法が開示される。

[0168] 第２実施形態では、通貨のハッシュ木を生成して、そのハッシュ木のルートに署名することによって、対象とする通貨をまとめて署名する点が第１実施形態と異なる。以下の第２実施形態の説明において、第１実施形態と同様の機能構成を有するものには、第１実施形態の説明で用いた符号と同様の符号を付与し、その説明を省略する。

[0169] （第２実施形態において使用する基本技術）

まず、本実施例において使用する基本技術について説明する。本実施例においてマークルツリー（参考文献［２］）と呼ばれるハッシュ木を利用した４つの関数ＭＨＴｒｅｅ、ＭＨＰａｔｈ、ＭＨＶｅｒを使用する。

[0170] 図１８は、第２実施形態に係るマークルツリーのＭＨＴｒｅｅ関数について説明するための図である。ＭＨＴｒｅｅ関数は、データセットからハッシュ木を生成する関数である。

[0171] 具体的には、ＭＨＴｒｅｅ関数は、データセットＤを入力しＤを構成する各データのハッシュ値を葉ノードに対応付けることで生成される２分木であるハッシュツリーＬ＝｛（ｌｅａｆ＿ｉｄ，ｌｅａｆ＿ｖａｌ）｝を出力する関数である。ここで、頂点ｈをルートという。以下、ＭＨＴｒｅｅ（Ｄ）－＞Ｌのように記述する。なお、図１８は、ｎ＝６のデータセットである。各葉ノードの値は当該葉ノードに対応するデータのハッシュ値である。７番目と８番目の葉ノードには、２分木の構成を可能とするために”００”が補完されている。

[0172] 図１９は、第２実施形態に係るマークルツリーのＭＨＰａｔｈ関数について説明するための第一の図である。ＭＨＰａｔｈ関数は、部分データセットを認証するために必要なパスを生成する関数である。

[0173] 具体的には、ＭＨＰａｔｈ関数は、認証したい部分データセットＤ’（図１９の場合、Ｄ’＝｛ｄ０，ｄ４，ｄ５｝）を入力して、その認証に必要な認証用のパスＡＰ（図１９のｈ００１，ｈ０１，ｈ１１）とルートｈを出力する関数である。以下、ＭＨＰａｔｈ（Ｄ’，Ｌ）－＞（ＡＰ，ｈ）のように記述する。

[0174] 図２０は、第２実施形態に係るマークルツリーのＭＨＶｅｒ関数について説明するための図である。ＭＨＶｅｒ関数は、部分データセットの認証パスによる検証を行う関数である。

[0175] 具体的には、ＭＨＶｅｒ関数は、認証に必要なパスＡＰ（図２０のｈ００１，ｈ０１，ｈ１１）とルートｈから、サブデータＤ’（図２０の場合、Ｄ’＝｛ｄ０，ｄ４，ｄ５｝）を検証する関数である。以下、ＭＨｖｅｒ（ＡＰ，ｈ，Ｄ’）－＞Ｔ　ｏｒ　Ｆのように記述する。ＭＨｖｅｒ関数は、検証に成功した場合（Ｄ’が正しい場合）Ｔを出力し、検証に失敗した場合（Ｄ’が正しくない場合）Ｆを出力する。Ｄ’が正しいとは、Ｄ’に属する全てのデータが改ざんされていないことをいう。

[0176] （第２実施形態に係る電子通貨システムの動作例）

ここでは、図１１のステップＳ２０２において、額面ｖに一致する通貨が複数の通貨のセットT_0：＝（T_{0_t}）：＝（（id_{0_t}，$y_{\_t}$，B_i，pkB_i，S_{0_t}），ｔ＝１，・・・，ｓ，Σ$v_{_t}$＝ｖ）であったとする。なお、$v_{_t}$は、T_0を構成する通貨セットのうちのｔ番目の通貨T_{0_t}の金額である。例えば、各$v_{_t}$が１万円であり、８万円の引出を受け付けた場合、ｓ＝８である。図２１には、それぞれが１万円であるT_{0_t}が８枚有る状態が示されている。なお、例えば、金融機関サーバ２０の未使用通貨記憶部２１５に、１０万円の通貨しかない等のように、１万円×８の通貨が無い場合、引出受付部２０５は、図１２の処理を実行することで、既存の１０万円から８枚の１万円を分割すればよい。なお、第２実施形態において、各T_{0_t}は、発行直後の通貨に限らず、発行後の移転が行われた（つまり、通貨付加情報が付加された）通貨であってもよい。この場合、移転の過程に

おいて分割（つまり、通貨ＩＤのＮＮＬ木の分割）が行われた通貨であってもよい。

[0177] 金融機関サーバ２０の引出受付部２０５は、ハッシュ木L_1＝ＭＨＴｒｅｅ（｛T_0＿ｔ｝｛ｔ＝１，・・・，ｓ｝）を生成し、秘密鍵ｓｋB_iを用いてハッシュ木L_1のルートノードのハッシュ値ＲＨ（ＲｏｏｔＨａｓｈ）及びｐｋU_jのセットに対する署名S_1を生成する。すなわち、ハッシュ木L_1はその葉ノードに対してT_0を構成する各T_0＿ｔを割り当てることで生成されるハッシュ木である。引出受付部２０５は、T_0＿ｔごとに、当該T_0＿ｔ対して通貨付加情報T_1＿ｔ：＝（id_1＿ｔ，ｐｋU_j，ＲＨ，ＡＰ＿ｔ，S_1）を付加することで使用中通貨（T_1＿ｔ，T_0＿ｔ）を生成し、使用中通貨記憶部２１６に記憶させる。ここで、ＡＰ＿ｔは、ＭＨＰａｔｈ（T_0＿ｔ，L_1）－＞（ＡＰ＿ｔ，ＲＨ）によって得られるＲＨの認証に必要なパスである。また、各id_1＿ｔの値は、それぞれに対応するid_0＿ｔと同じでよい。この状態を図２２に示す。各T_1＿ｔが含む署名は同じS_1であることが分かる。以下、通貨（T_1＿ｔ，T_0＿ｔ）のセット（ここでは８個のセット）を（T_1，T_0）と記載する。

[0178] 続いて、引出受付部２０５は、使用中通貨セット（T_1，T_0）の通貨データセットと、金融機関公開鍵証明書Ａｕｔｈ（ｐｋB_i）とを利用者端末３０に送信する（ステップＳ２０３）。利用者端末３０の引出要求部３０５は、使用中通貨セット（T_1，T_0）の通貨データセットと、金融機関公開鍵証明書Ａｕｔｈ（ｐｋB_i）とを検証し、使用中通貨セット（T_1，T_0）を利用者通貨記憶部３１４に記憶させる。この際、引出要求部３０５は、通貨セット（T_1，T_0）の検証に関しては、（T_1，T_0）のうちのいずれか１つの通貨（T_1＿ｔ，T_0＿ｔ）についてのみを検証すればよい。具体的には、いずれか１つのT_1＿ｔについてＭＨｖｅｒ（ＡＰ＿ｔ，ＲＨ，T_0）がＴであることを検証し、かつ、当該T_1＿ｔが含むS_1を検証する。引出要求部３０５は、他のT_1＿ｔについては、検証対象としたT_1＿ｔと同じS_1を含むことを確認すればよい。

[0179] なお、利用者端末３０の利用者は、通貨セットとして引き出した（T_1，T_0）を構成していた各（T_1＿ｔ，T_0＿ｔ）を個別に（バラバラに）利用することができる。T_1＿ｔは、通貨セットの署名及び検証コストの軽減のためにＲＨ及びＡＰ＿ｔを含む点を除いて、第１実施形態における通貨付加情報と同様に通貨の持ち主（流通過程）の履歴を示すものであり、それぞれ個別に通貨の真正性が担保されているからである。

[0180] なお、上記した処理は、図１３において、複数の貨幣のセットで支払が行われる際におけるステップＳ３０４及びＳ３０５においても実行される。

[0181] また、図１４（両替時）及び図１６（預入時）から呼び出される図１３の処理においても実行される。

[0182] 更に、その他の全てのフェーズ（発行時及び還収時等）において図１３の処理は適用可能である。例えば、還収時であれば、還収対象の通貨の一括渡しを効率化することができる。

[0183] 上述したように、第２実施形態によれば、複数の通貨を移転する際の署名コスト及び検証コストを軽減することができる。

[0184] （ハードウェア構成例）

第１実施形態と第２実施形態に共通のハードウェア構成例を説明する。電子通貨システム１の備える各装置の各部は、例えば、コンピュータに、本実施の形態で説明する処理内容を記述したプログラムを実行させることにより実現可能である。なお、この「コンピュータ」は、物理マシンであってもよいし、クラウド上の仮想マシンであってもよい。仮想マシンを使用する場合、ここで説明する「ハードウェア」は仮想的なハードウェアである。

[0185] 上記プログラムは、コンピュータが読み取り可能な記録媒体（可搬メモリ等）に記録して、保存したり、配布したりすることが可能である。また、上記プログラムをインターネットや電子メール等、ネットワークを通して提供することも可能である。

[0186] 図２３は、上記コンピュータのハードウェア構成例を示す図である。図２３のコンピュータは、それぞれバスＢで相互に接続されているドライブ装置

１０００、補助記憶装置１００２、メモリ装置１００３、ＣＰＵ１００４、インタフェース装置１００５、表示装置１００６、入力装置１００７、出力装置１００８等を有する。

[0187] 当該コンピュータでの処理を実現するプログラムは、例えば、ＣＤ－ＲＯＭ又はメモリカード等の記録媒体１００１によって提供される。プログラムを記憶した記録媒体１００１がドライブ装置１０００にセットされると、プログラムが記録媒体１００１からドライブ装置１０００を介して補助記憶装置１００２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１００１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１００２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。

[0188] メモリ装置１００３は、プログラムの起動指示があった場合に、補助記憶装置１００２からプログラムを読み出して格納する。ＣＰＵ１００４は、メモリ装置１００３に格納されたプログラムに従って、当該装置に係る機能を実現する。インタフェース装置１００５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。表示装置１００６はプログラムによるＧＵＩ（Graphical User Interface）等を表示する。入力装置１００７はキーボード及びマウス、ボタン、又はタッチパネル等で構成され、様々な操作指示を入力させるために用いられる。出力装置１００８は演算結果を出力する。なお、上記コンピュータは、ＣＰＵ１００４の代わりにＧＰＵ（Graphics Processing Unit）またはＴＰＵ（Tensor processing unit）を備えていても良く、ＣＰＵ１００４に加えて、ＧＰＵまたはＴＰＵを備えていても良い。その場合、例えばニューラルネットワーク等の特殊な演算が必要な処理をＧＰＵまたはＴＰＵが実行し、その他の処理をＣＰＵ１００４が実行する、というように処理を分担して実行しても良い。

[0189] （参考文献）

［１］Revocation and Tracing Schemes for Stateless Receivers, Dalit

Naor, Moni Naor, and Jeff Lotspiech, CRYPTO2001

［２］Jakobsson M., Leighton T., Micali S., Szydlo M. (2003) Fractal Merkle Tree Representation and Traversal. In: Joye M. (eds) Topics in Cryptology - CT-RSA 2003. CT-RSA 2003. Lecture Notes in Computer Science, vol 2612. Springer, Berlin, Heidelberg.

なお、上記各実施の形態において、引出受付部２０５及び支払要求部３０６は、請求項１における深さ計算部、ルートノード決定部、乱数計算部、葉ノード決定部及び通貨付加情報生成部、並びに請求項３におけるマークルツリー生成部及び付加部の一例である。通貨発行部１０４は、請求項２における深さ計算部、乱数生成部、葉ノード決定部及び通貨付加情報生成部の一例である。金融機関サーバ２０、利用者端末３０及び発行銀行サーバ１０は、通貨処理装置の一例である。

[0190] 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

[0191] １　電子通貨システム

１０　発行銀行サーバ

１１　ルート認証局サーバ

２０　金融機関サーバ

２５　中間認証局サーバ

３０　利用者端末

１０１　通貨発行鍵生成部

１０２　通貨発行証明書発行部

１０３　金融機関公開鍵証明書発行情報取得部

１０４　通貨発行部

１０５　還収受付部

１０６　通貨発行鍵記憶部

１０７　還収済通貨記憶部

１１１　ルート認証鍵生成部

１１２　ルート証明書発行部

１１３　金融機関認証部

１１４　金融機関公開鍵証明書発行情報送信部

１１５　ルート認証鍵記憶部

１１６　金融機関公開鍵証明書発行情報記憶部

２０１　通貨発行証明書発行受付部

２０２　金融機関鍵生成部

２０３　金融機関認証要求部

２０４　通貨発行受付部

２０５　引出受付部

２０６　更新処理部

２０７　両替・預入受付部

２０８　支払要求部

２０９　支払受付部

２１０　与信受付部

２１１　還収要求部

２１２　通貨発行証明書記憶部

２１３　金融機関鍵記憶部

２１４　金融機関公開鍵証明書記憶部

２１５　未使用通貨記憶部

２１６　使用中通貨記憶部

２１７　更新済通貨記憶部

２１８　使用済通貨記憶部

２５１　中間認証鍵生成部

２５２　中間証明書発行部

２５３　利用者認証部

２５４　中間認証鍵記憶部

２５５　利用者公開鍵証明書発行情報記憶部

３０１　通貨発行証明書発行受付部

３０２　中間証明書発行受付部

３０３　利用者鍵生成部

３０４　利用者認証要求部

３０５　引出要求部

３０６　支払要求部

３０７　支払受付部

３０８　両替・預入要求部

３０９　与信要求部

３１０　通貨発行証明書記憶部

３１１　中間証明書記憶部

３１２　利用者鍵記憶部

３１３　利用者公開鍵証明書記憶部

３１４　利用者通貨記憶部

１０００　ドライブ装置

１００１　記録媒体

１００２　補助記憶装置

１００３　メモリ装置

１００４　ＣＰＵ

１００５　インタフェース装置

１００６　表示装置

１００７　入力装置

１００８　出力装置

請求の範囲

[請求項1] 移転する金額を電子通貨の最小単位で除した値以上の数の葉ノードを含むＮＮＬ木の深さを計算するように構成されている深さ計算部と、

第１の電子通貨に付加された第１のＮＮＬ木において、前記深さに基づいて前記第１のＮＮＬ木の部分木である第２のＮＮＬ木のルートノードを決定するように構成されているルートノード決定部と、

前記第１のＮＮＬ木のＳｅｅｄに基づいて前記ルートノードに対応する乱数を計算するように構成されている乱数計算部と、

前記葉ノードのうち、前記金額に対応させる葉ノードの範囲を決定するように構成されている葉ノード決定部と、

前記乱数、前記深さ、前記範囲を示す情報を第２の電子通貨に付加する情報として生成するように構成されている通貨付加情報生成部と、

を有することを特徴とする通貨処理装置。

[請求項2] 発行対象の電子通貨の金額を、電子通貨の最小単位で除した値以上の数の葉ノードを含むＮＮＬ木の深さを計算するように構成されている深さ計算部と、

前記ＮＮＬ木のＳｅｅｄとなる乱数を生成するように構成されている乱数生成部と、

前記葉ノードのうち、前記金額に対応させる葉ノードの範囲を決定するように構成されている葉ノード決定部と、

前記乱数、前記深さ、前記範囲を示す情報を前記発行対象の電子通貨に付加する情報として生成するように構成されている通貨付加情報生成部と、

を有することを特徴とする通貨処理装置。

[請求項3] 移転対象とする複数の電子通貨のそれぞれハッシュ値に基づいてマークルツリーを生成するように構成されているマークルツリー生成部

と、

前記マークルツリーのルートノードのハッシュ値と前記ハッシュ値に対する署名とを前記複数の電子通貨のそれぞれに付加するように構成されている付加部と、

を有することを特徴とする通貨処理装置。

[請求項4] 移転する金額を電子通貨の最小単位で除した値以上の数の葉ノードを含むＮＮＬ木の深さを計算する深さ計算手順と、

第１の電子通貨に付加された第１のＮＮＬ木において、前記深さに基づいて前記第１のＮＮＬ木の部分木である第２のＮＮＬ木のルートノードを決定するようにルートノード決定手順と、

前記第１のＮＮＬ木のＳｅｅｄに基づいて前記ルートノードに対応する乱数を計算する乱数計算手順と、

前記葉ノードのうち、前記金額に対応させる葉ノードの範囲を決定する葉ノード決定手順と、

前記乱数、前記深さ、前記範囲を示す情報を第２の電子通貨に付加する情報として生成する通貨付加情報生成手順と、

をコンピュータが実行する通貨処理方法。

[請求項5] 発行対象の電子通貨の金額を、電子通貨の最小単位で除した値以上の数の葉ノードを含むＮＮＬ木の深さを計算する深さ計算手順と、

前記ＮＮＬ木のＳｅｅｄとなる乱数を生成する乱数生成手順と、

前記葉ノードのうち、前記金額に対応させる葉ノードの範囲を決定する葉ノード決定手順と、

前記乱数、前記深さ、前記範囲を示す情報を前記発行対象の電子通貨に付加する情報として生成する通貨付加情報生成手順と、

をコンピュータが実行する通貨処理方法。

[請求項6] 移転対象とする複数の電子通貨のそれぞれハッシュ値に基づいてマークルツリーを生成するマークルツリー生成手順と、

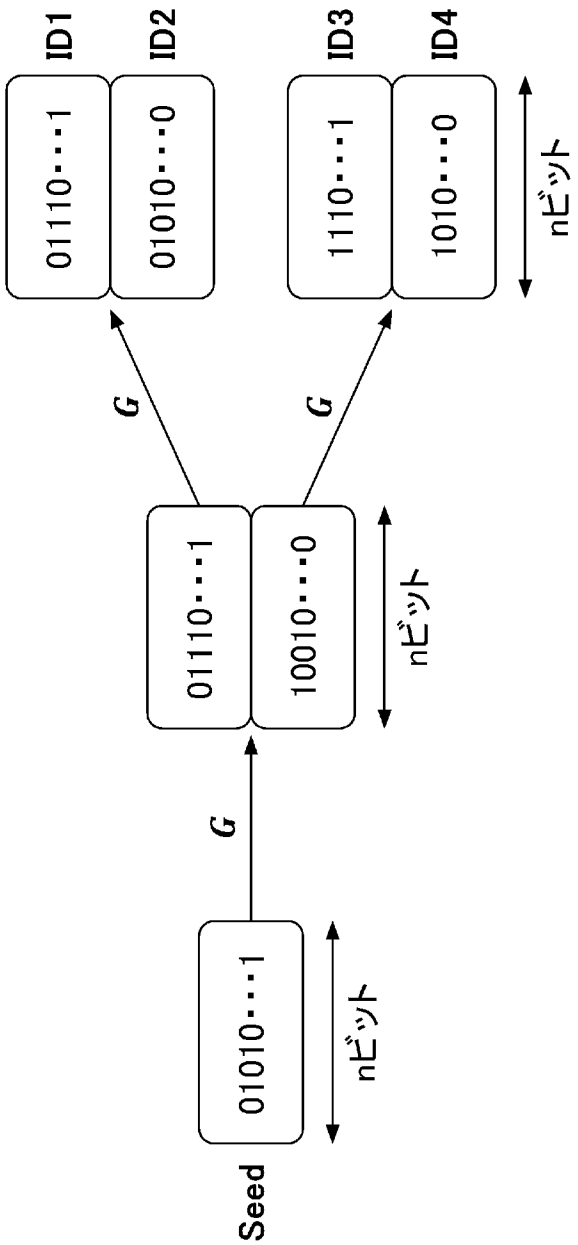
前記マークルツリーのルートノードのハッシュ値と前記ハッシュ値

に対する署名とを前記複数の電子通貨のそれぞれに付加する付加手順と、

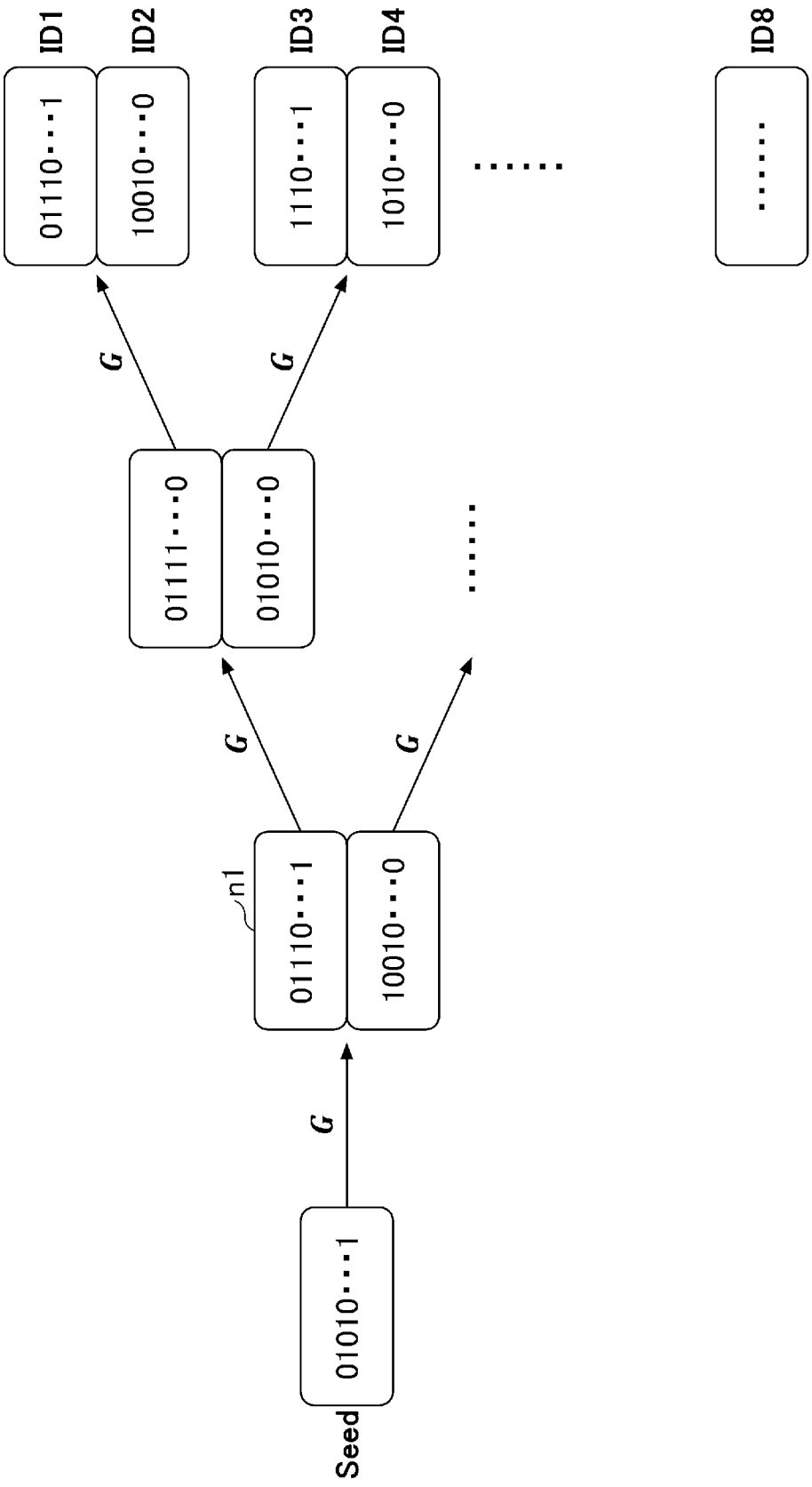
をコンピュータが実行する通貨処理方法。

[請求項7] 請求項４乃至６いずれか一項記載の通貨処理方法をコンピュータに実行させることを特徴とするプログラム。

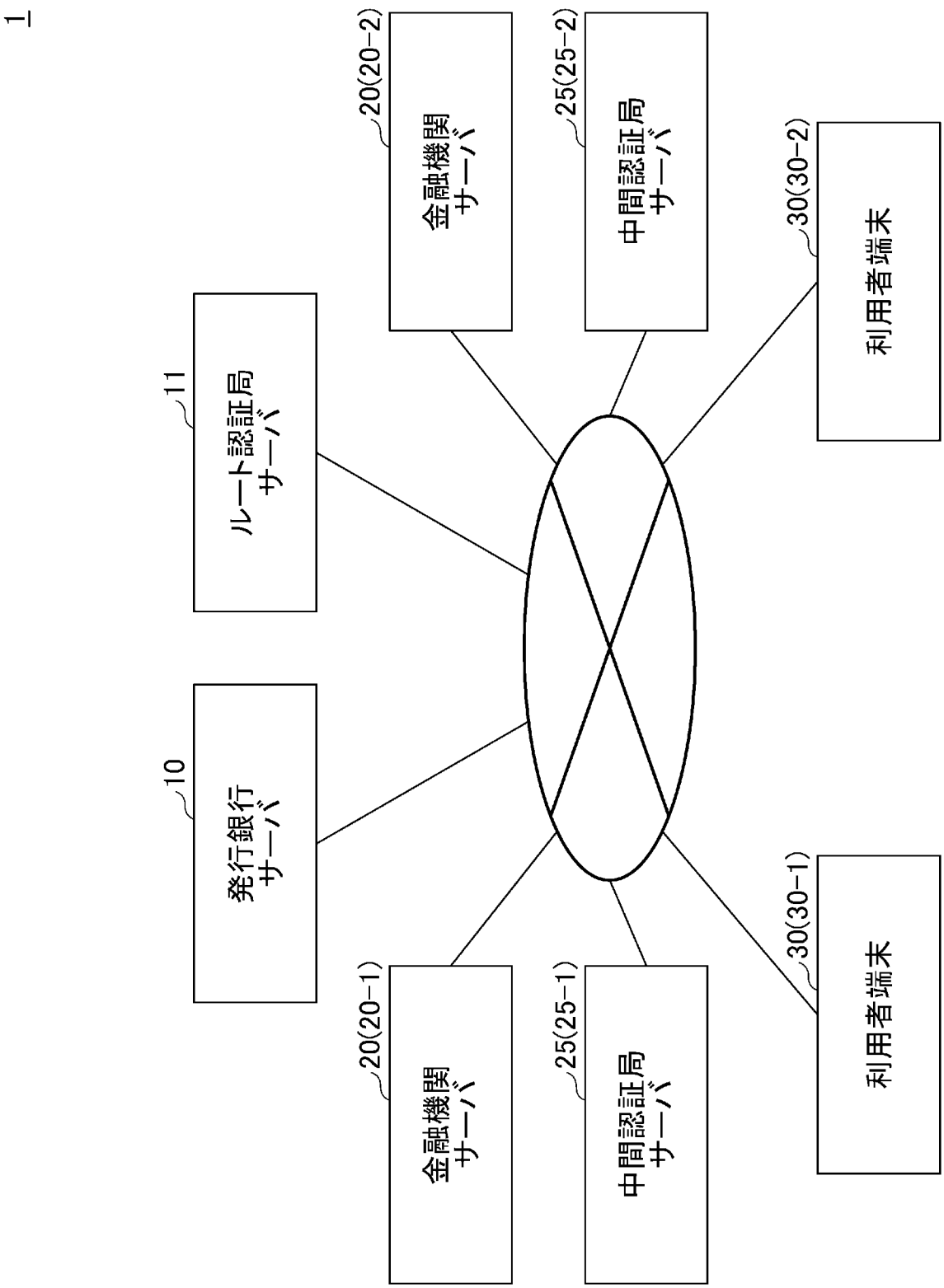
[図1]


ID1
ID2
ID3
ID4
01110・・・1
01010・・・0
1110・・・1
1010・・・0
nビット
G
G
01110・・・1
10010・・・0
nビット
G
01010・・・1
nビット
Seed

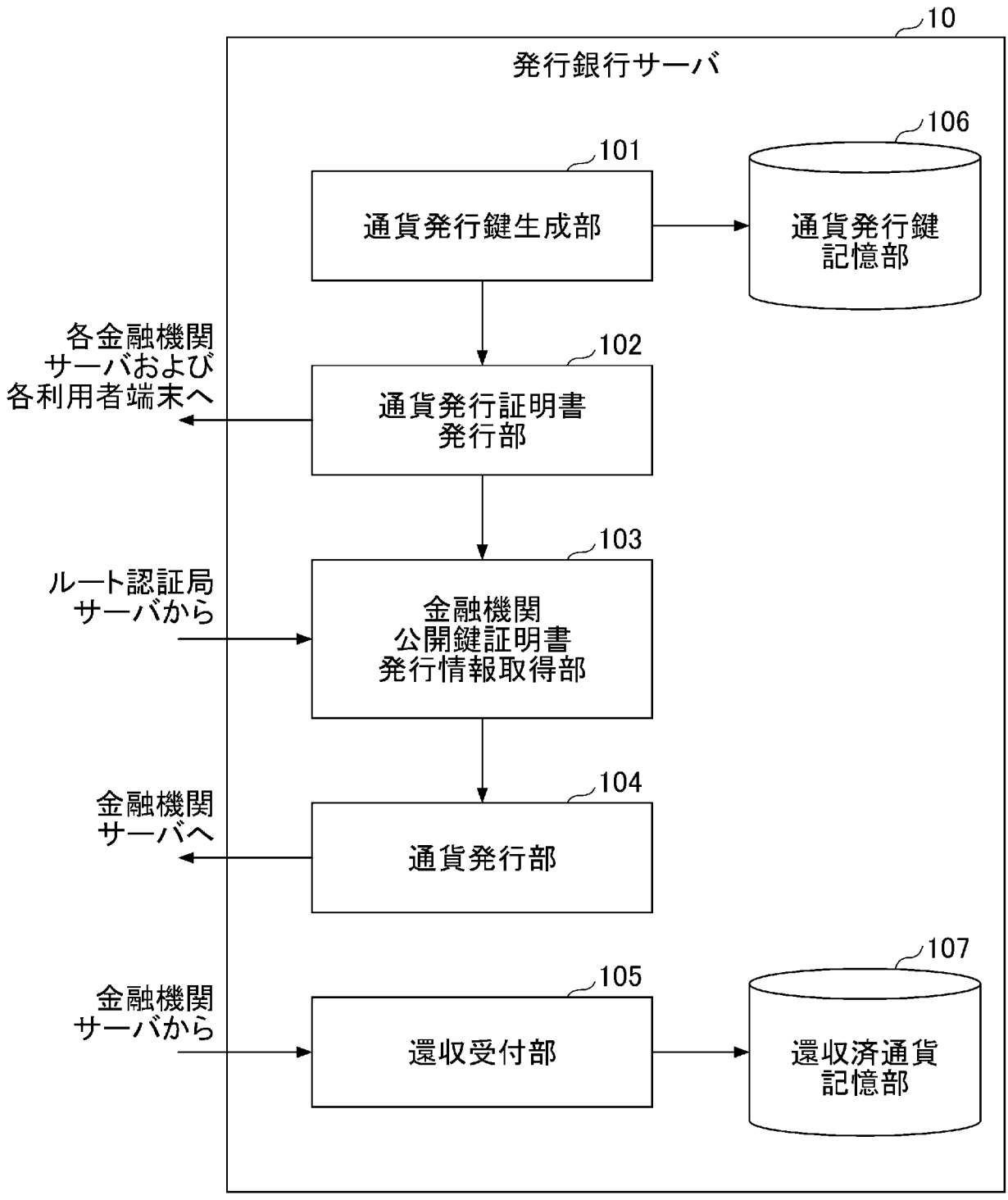
[図2]


ID1
ID2
ID3
ID4
ID8
01110・・・1
10010・・・0
1110・・・1
1010・・・0
・・・・・・
・・・・・・
01111・・・0
01010・・・0
・・・・・・
n1
01110・・・1
10010・・・0
G
G
G
G
G
01010・・・1
Seed

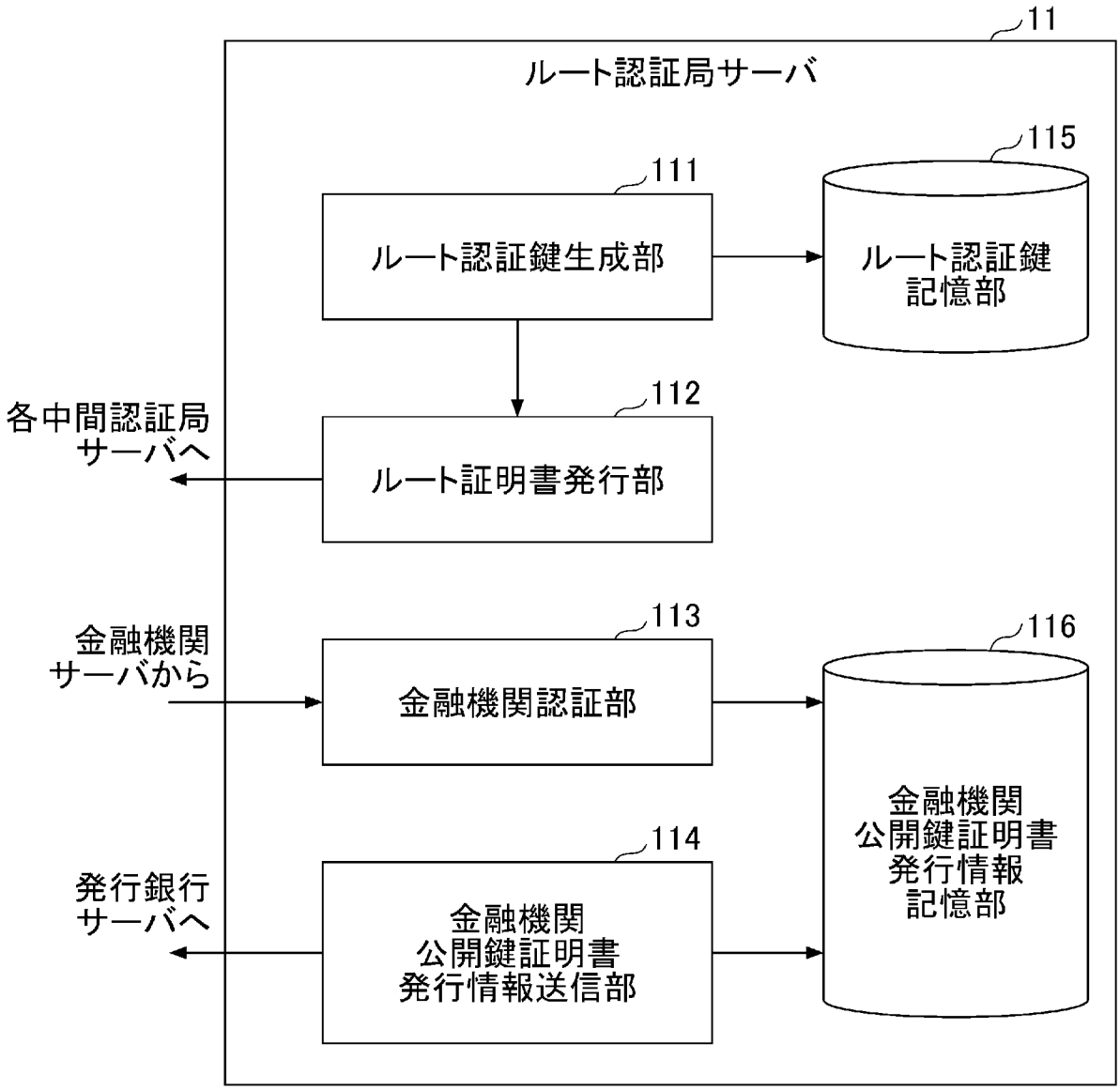
[図3]


1
11
ルート認証局
サーバ
10
発行銀行
サーバ
20(20-2)
金融機関
サーバ
20(20-1)
金融機関
サーバ
25(25-2)
中間認証局
サーバ
25(25-1)
中間認証局
サーバ
30(30-2)
利用者端末
30(30-1)
利用者端末

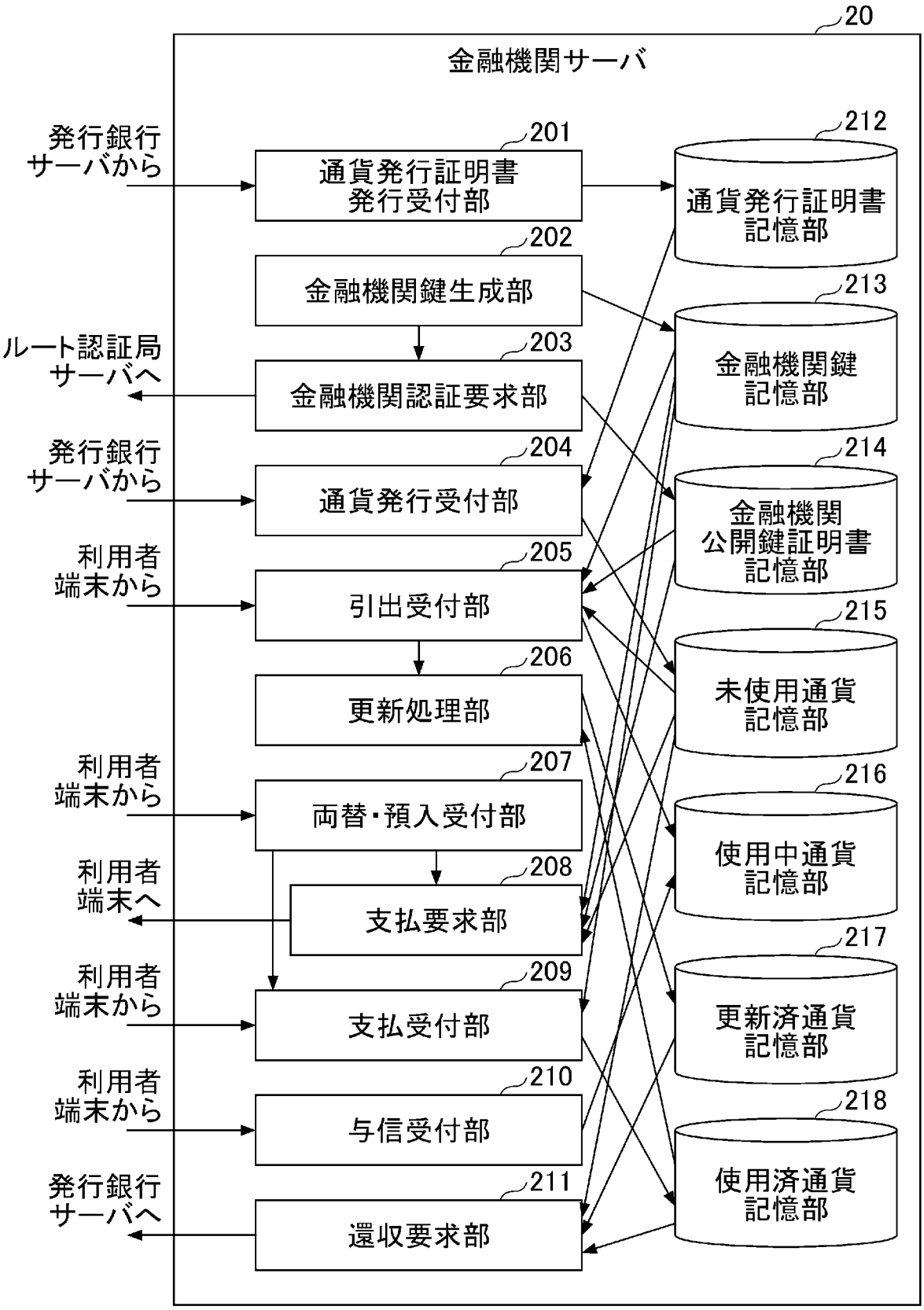
[図4]


10
発行銀行サーバ
101
通貨発行鍵生成部
106
通貨発行鍵
記憶部
各金融機関
サーバおよび
各利用者端末へ
102
通貨発行証明書
発行部
ルート認証局
サーバから
103
金融機関
公開鍵証明書
発行情報取得部
金融機関
サーバへ
104
通貨発行部
金融機関
サーバから
105
還収受付部
107
還収済通貨
記憶部

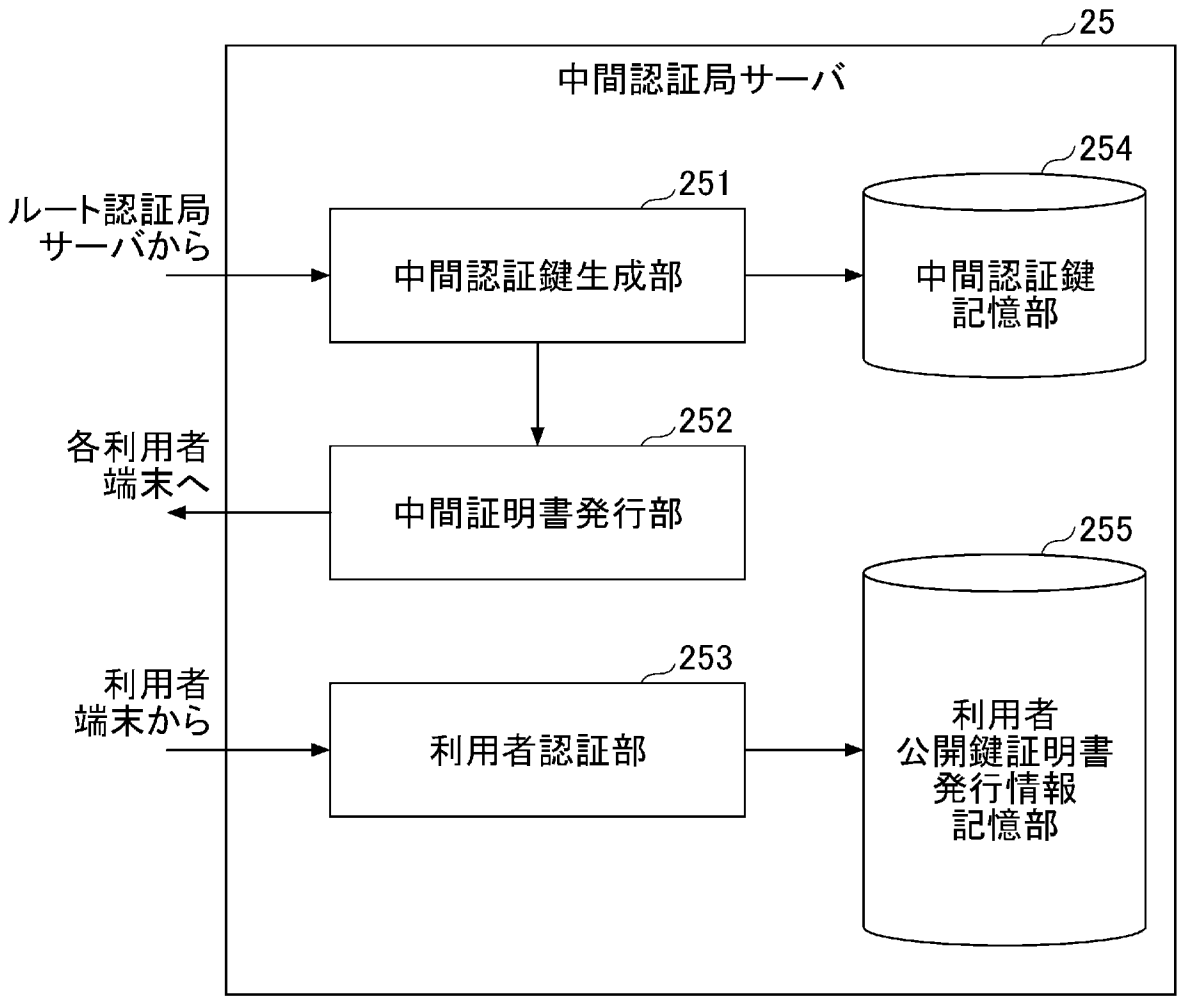
[図5]


11
ルート認証局サーバ
115
111
ルート認証鍵生成部
ルート認証鍵
記憶部
112
各中間認証局
サーバへ
ルート証明書発行部
113
116
金融機関
サーバから
金融機関認証部
金融機関
公開鍵証明書
発行情報
記憶部
114
発行銀行
サーバへ
金融機関
公開鍵証明書
発行情報送信部

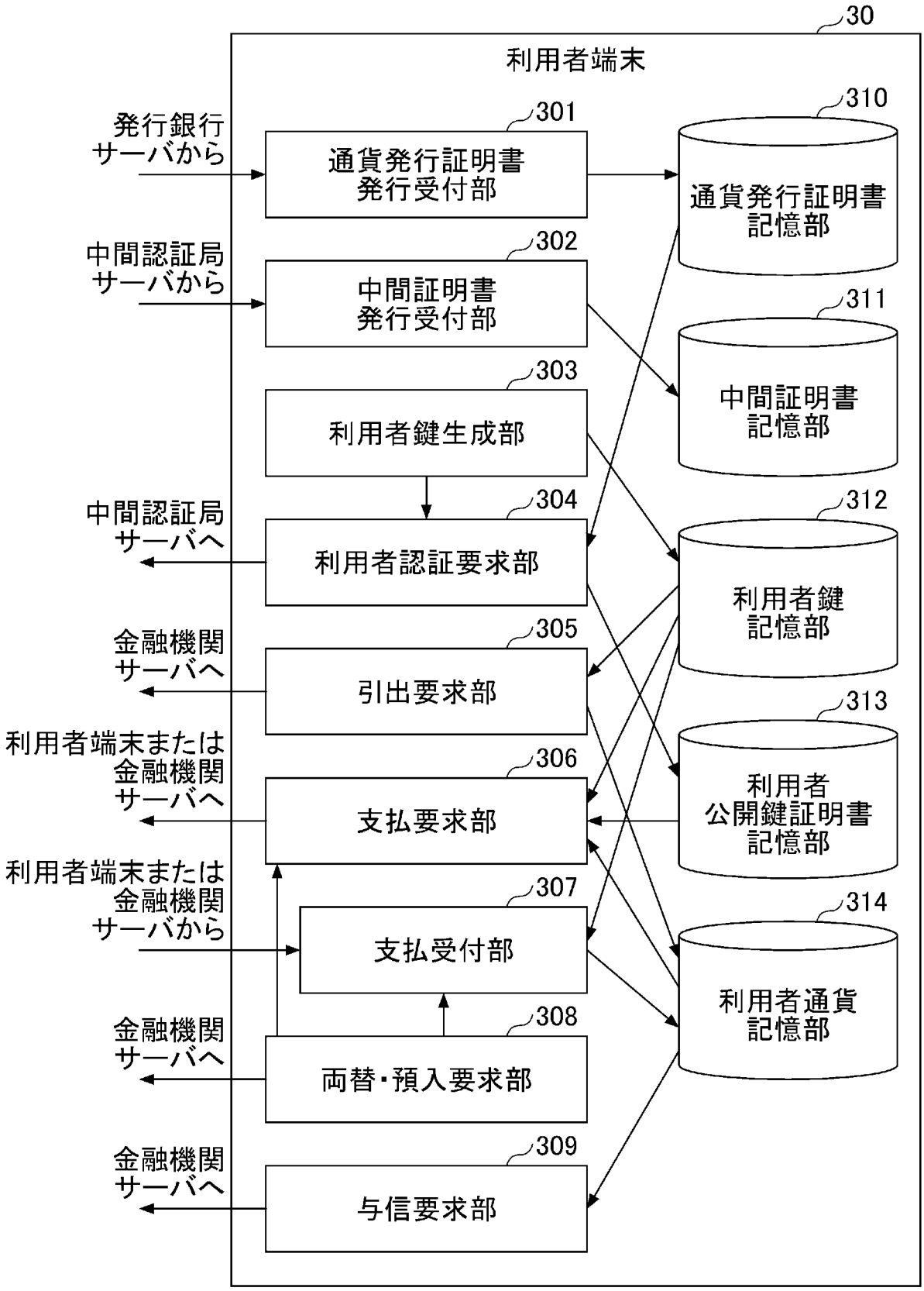
[図6]


20
金融機関サーバ
発行銀行サーバから
201
通貨発行証明書発行受付部
202
金融機関鍵生成部
ルート認証局サーバへ
203
金融機関認証要求部
発行銀行サーバから
204
通貨発行受付部
利用者端末から
205
引出受付部
206
更新処理部
利用者端末から
207
両替・預入受付部
利用者端末へ
208
支払要求部
利用者端末から
209
支払受付部
利用者端末から
210
与信受付部
発行銀行サーバへ
211
還収要求部
212
通貨発行証明書記憶部
213
金融機関鍵記憶部
214
金融機関公開鍵証明書記憶部
215
未使用通貨記憶部
216
使用中通貨記憶部
217
更新済通貨記憶部
218
使用済通貨記憶部

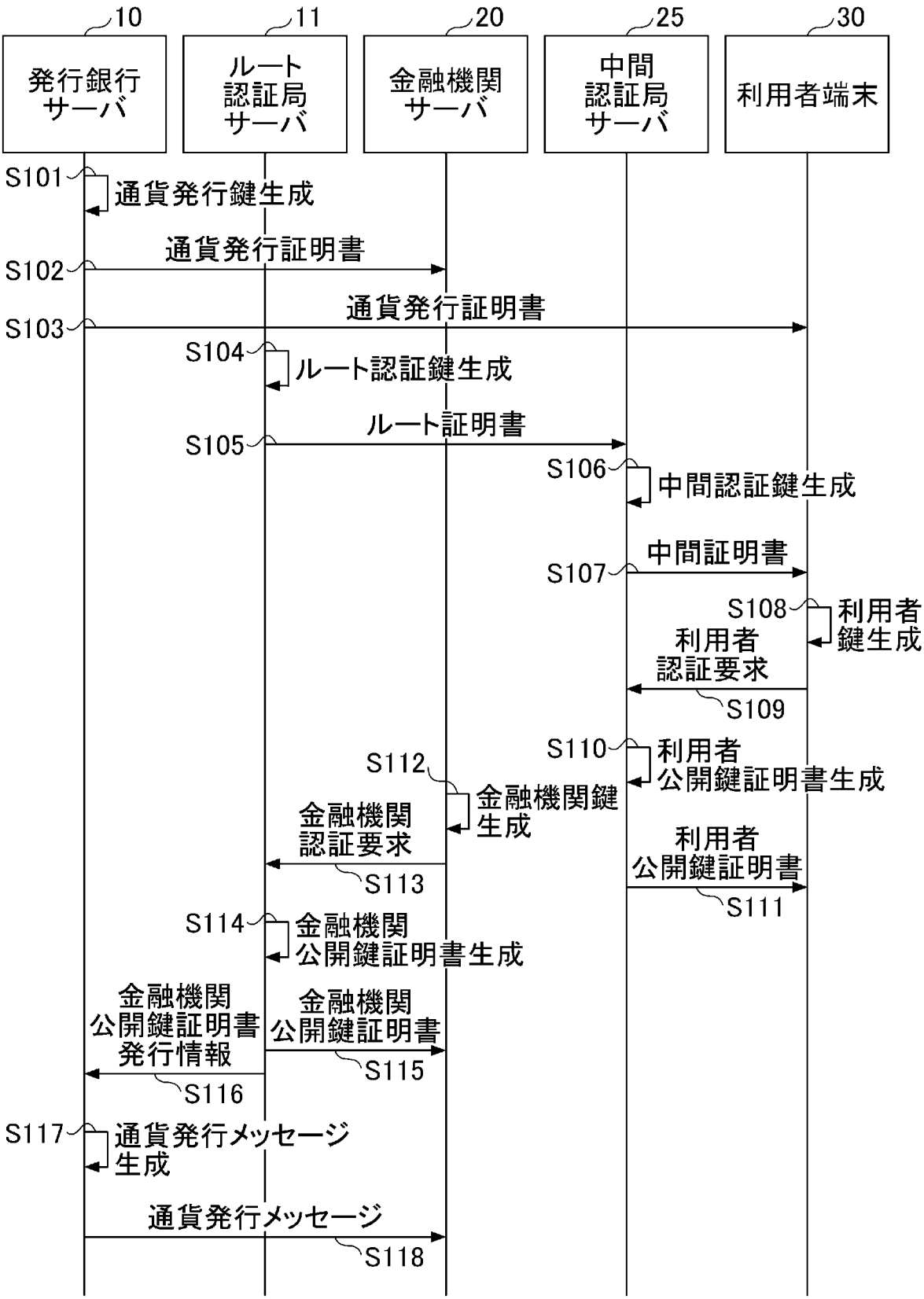
[図7]


25
中間認証局サーバ
254
251
ルート認証局
サーバから
中間認証鍵生成部
中間認証鍵
記憶部
252
各利用者
端末へ
中間証明書発行部
255
253
利用者
端末から
利用者認証部
利用者
公開鍵証明書
発行情報
記憶部

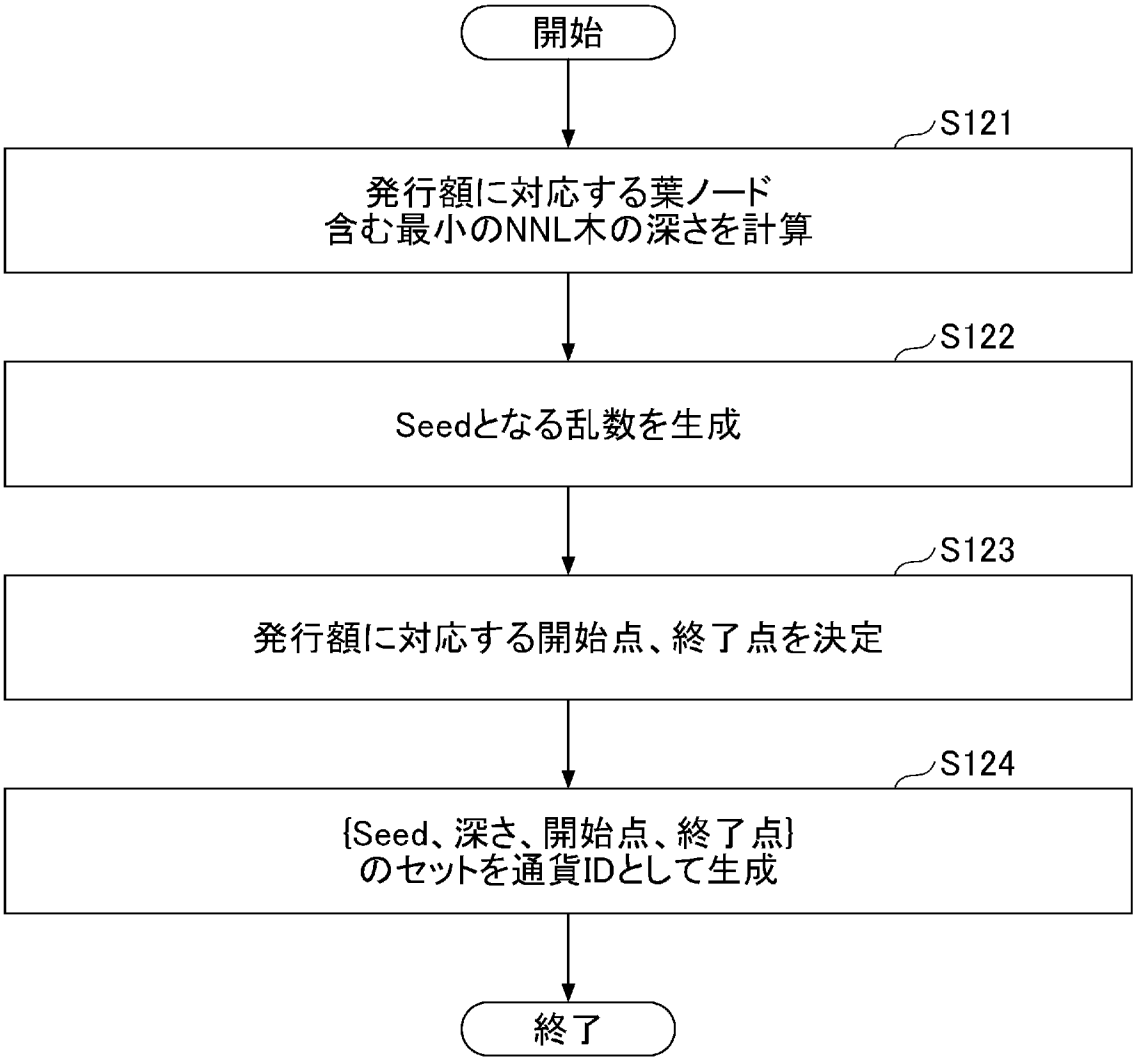
[図8]


30
利用者端末
301
通貨発行証明書
発行受付部
302
中間証明書
発行受付部
303
利用者鍵生成部
304
利用者認証要求部
305
引出要求部
306
支払要求部
307
支払受付部
308
両替・預入要求部
309
与信要求部
310
通貨発行証明書
記憶部
311
中間証明書
記憶部
312
利用者鍵
記憶部
313
利用者
公開鍵証明書
記憶部
314
利用者通貨
記憶部
発行銀行
サーバから
中間認証局
サーバから
中間認証局
サーバへ
金融機関
サーバへ
利用者端末または
金融機関
サーバへ
利用者端末または
金融機関
サーバから
金融機関
サーバへ
金融機関
サーバへ

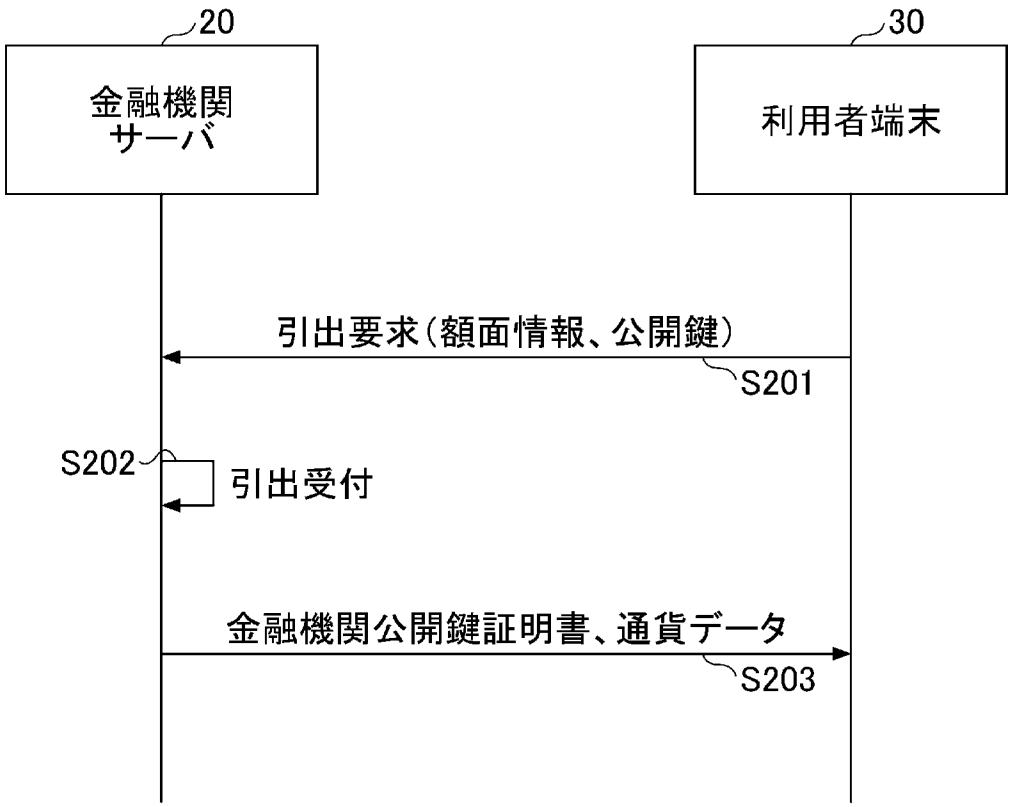
[図9]


10
11
20
25
30
発行銀行サーバ
ルート認証局サーバ
金融機関サーバ
中間認証局サーバ
利用者端末
S101
通貨発行鍵生成
通貨発行証明書
S102
通貨発行証明書
S103
S104
ルート認証鍵生成
ルート証明書
S105
S106
中間認証鍵生成
中間証明書
S107
S108
利用者鍵生成
利用者認証要求
S109
S110
利用者公開鍵証明書生成
S112
金融機関鍵生成
金融機関認証要求
S113
利用者公開鍵証明書
S111
S114
金融機関公開鍵証明書生成
金融機関公開鍵証明書発行情報
金融機関公開鍵証明書
S115
S116
S117
通貨発行メッセージ生成
通貨発行メッセージ
S118

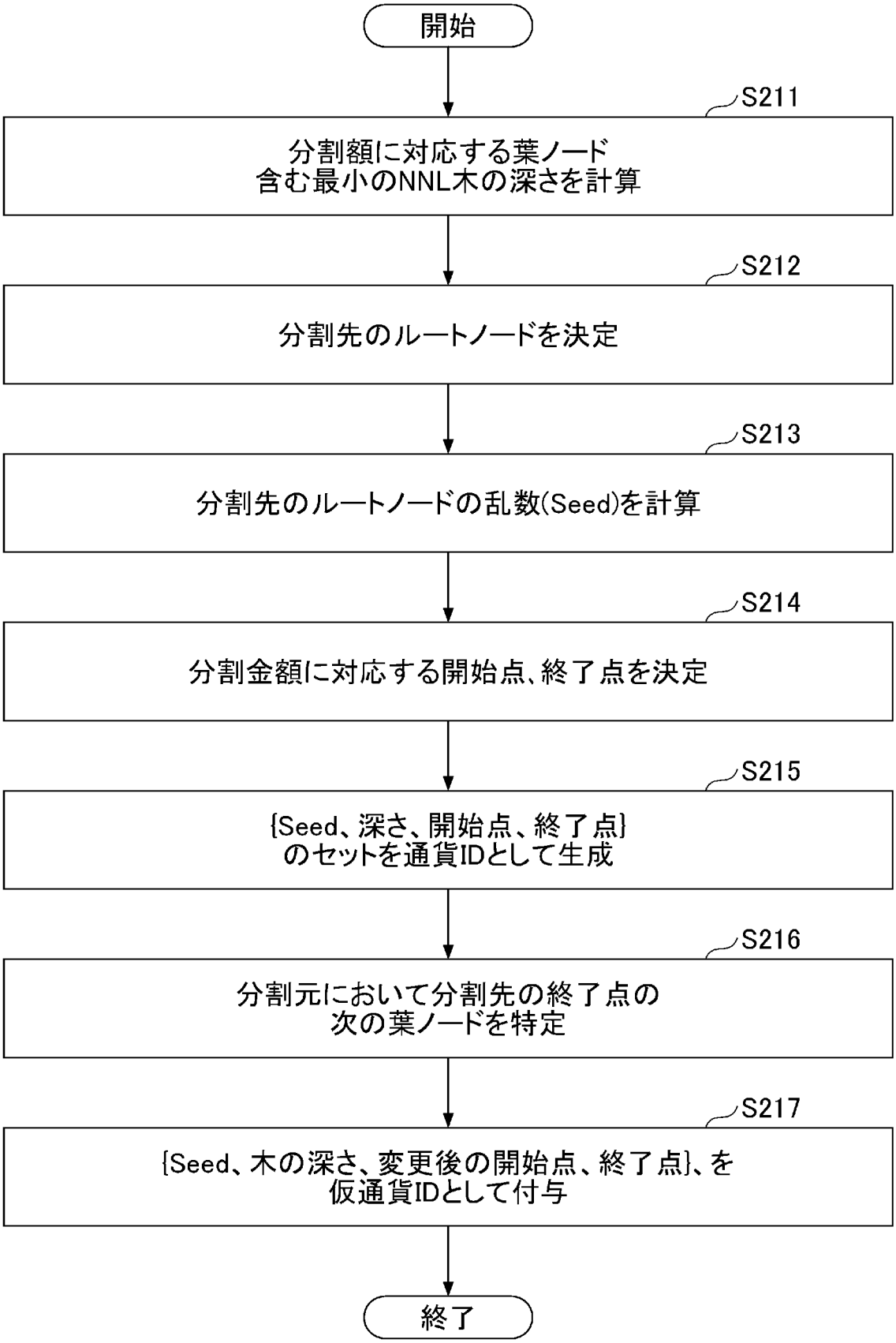
[図10]


開始
S121
発行額に対応する葉ノード
含む最小のNNL木の深さを計算
S122
Seedとなる乱数を生成
S123
発行額に対応する開始点、終了点を決定
S124
{Seed、深さ、開始点、終了点}
のセットを通貨IDとして生成
終了

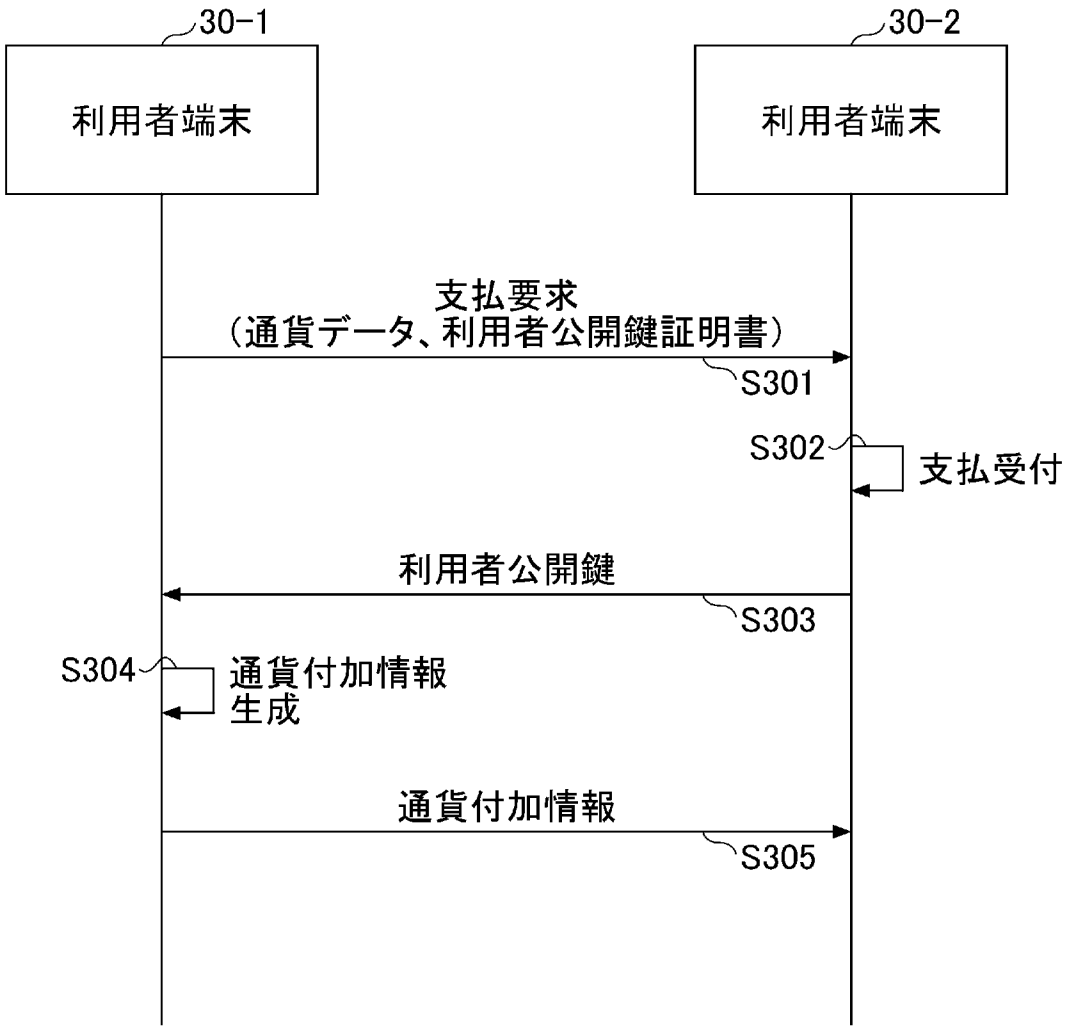
[図11]


20
金融機関
サーバ
30
利用者端末
引出要求（額面情報、公開鍵）
S201
S202
引出受付
金融機関公開鍵証明書、通貨データ
S203

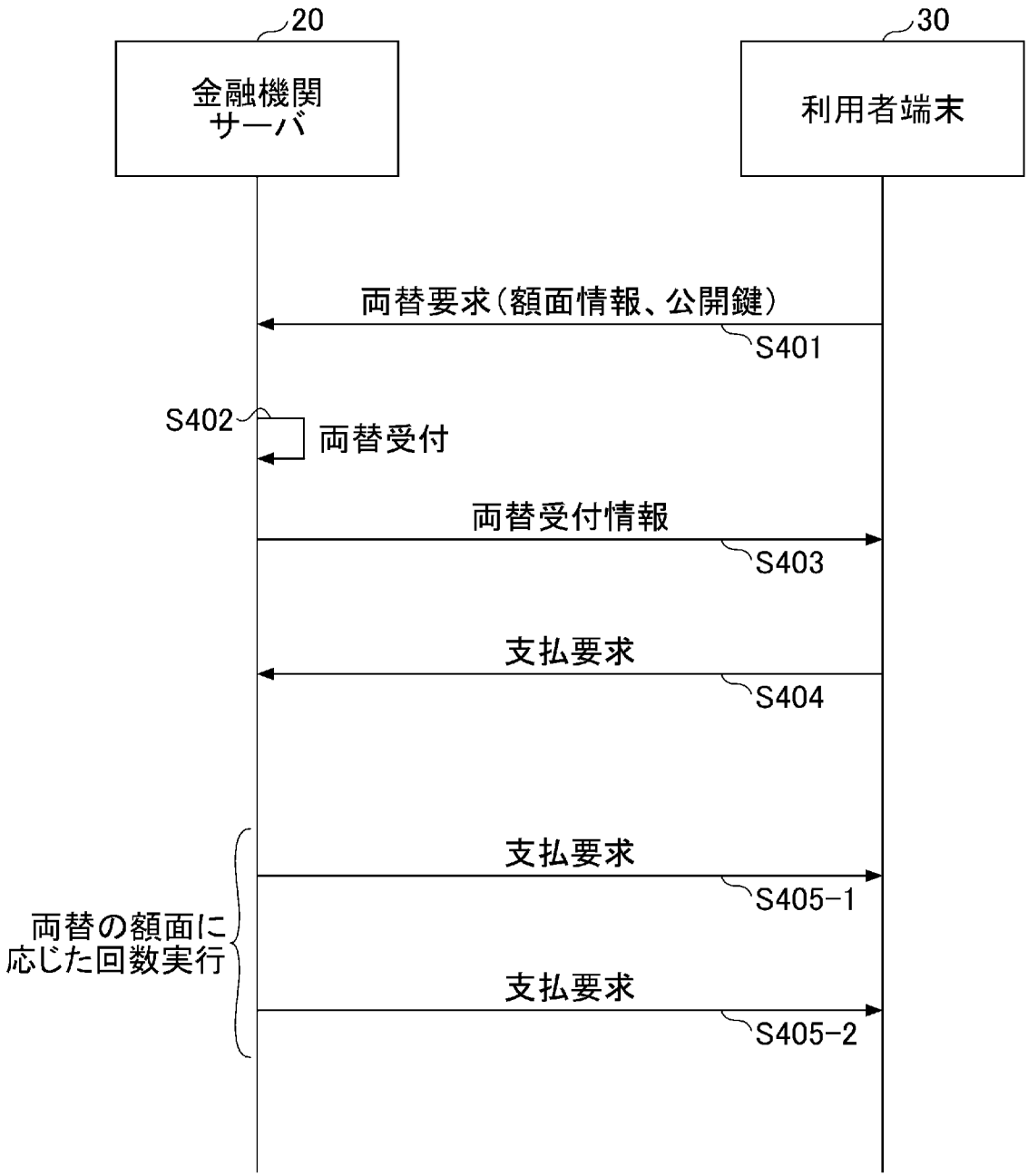
[図12]


開始
S211
分割額に対応する葉ノード
含む最小のNNL木の深さを計算
S212
分割先のルートノードを決定
S213
分割先のルートノードの乱数(Seed)を計算
S214
分割金額に対応する開始点、終了点を決定
S215
{Seed、深さ、開始点、終了点}
のセットを通貨IDとして生成
S216
分割元において分割先の終了点の
次の葉ノードを特定
S217
{Seed、木の深さ、変更後の開始点、終了点}、を
仮通貨IDとして付与
終了

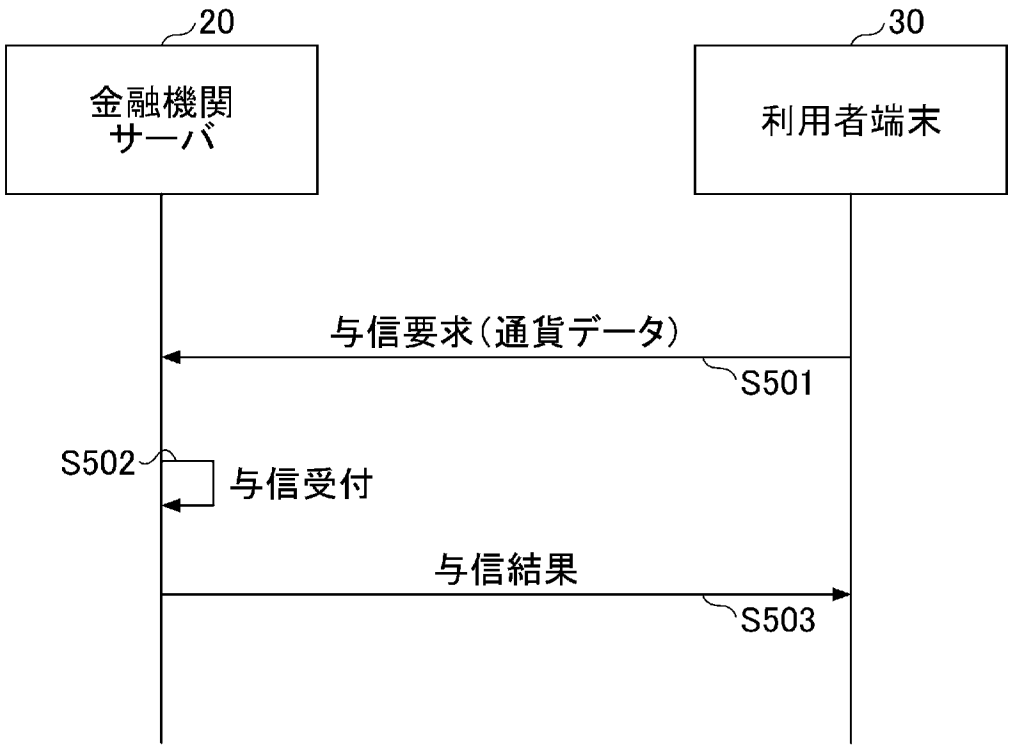
[図13]


30-1
利用者端末
30-2
利用者端末
支払要求
（通貨データ、利用者公開鍵証明書）
S301
S302
支払受付
利用者公開鍵
S303
S304
通貨付加情報
生成
通貨付加情報
S305

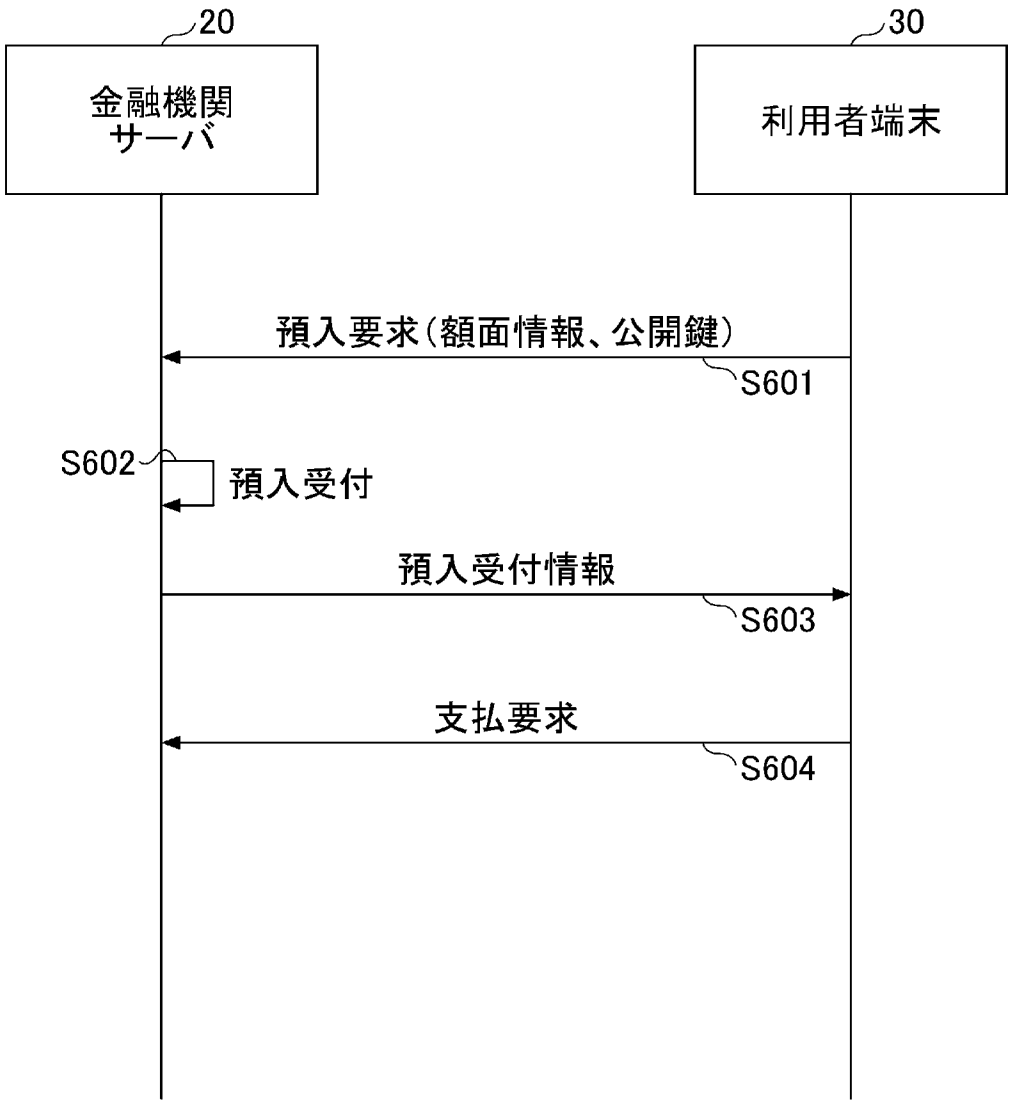
[図14]


20
金融機関
サーバ
30
利用者端末
両替要求(額面情報、公開鍵)
S401
S402
両替受付
両替受付情報
S403
支払要求
S404
支払要求
S405-1
両替の額面に
応じた回数実行
支払要求
S405-2

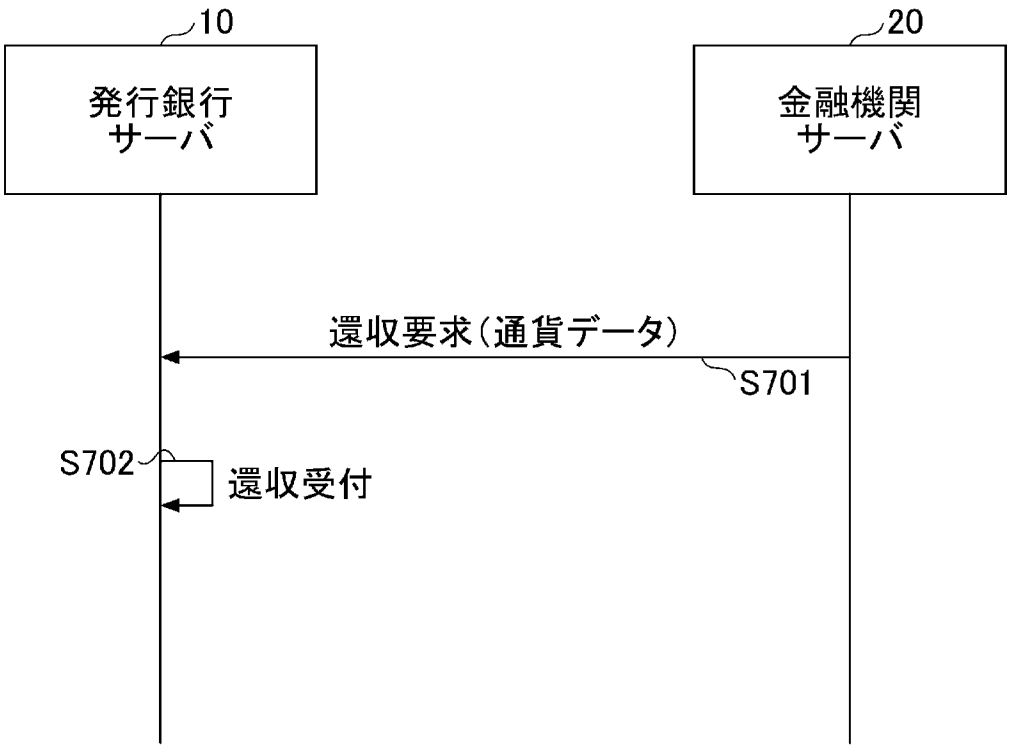
[図15]



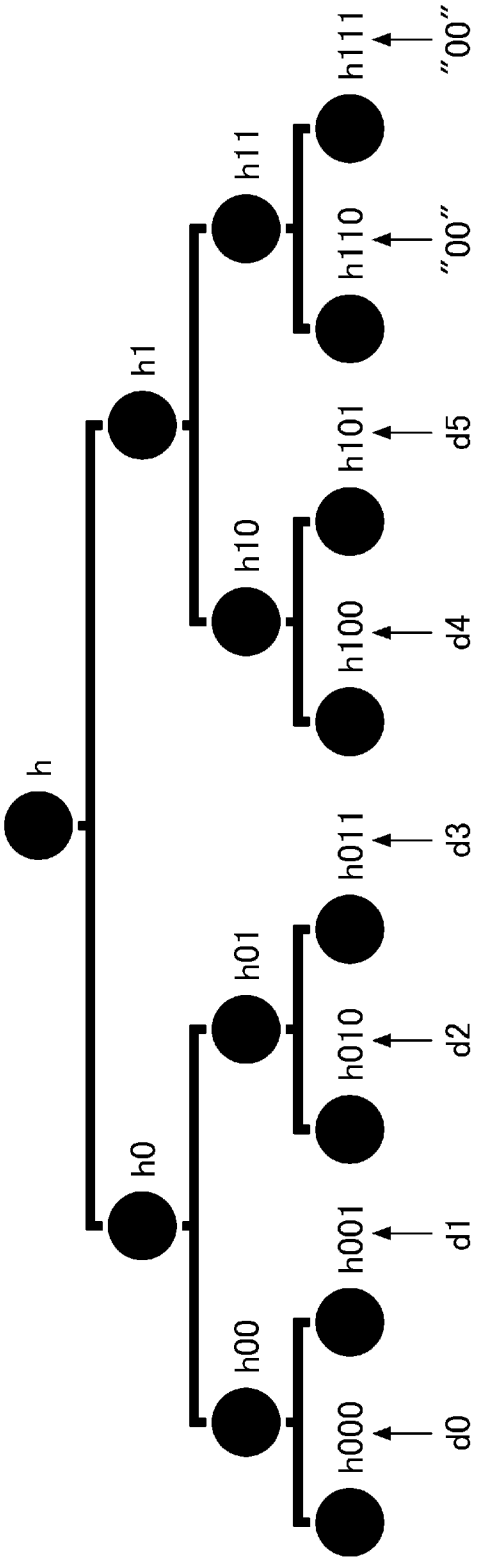
[図16]


20
金融機関
サーバ
30
利用者端末
預入要求(額面情報、公開鍵)
S601
S602
預入受付
預入受付情報
S603
支払要求
S604

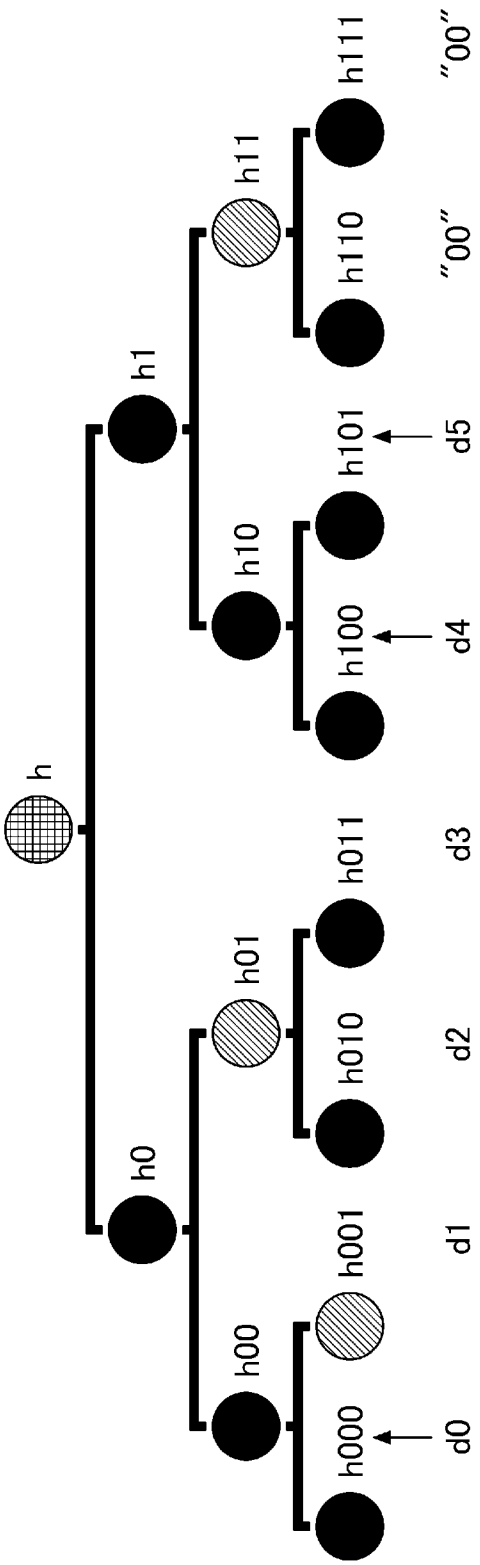
[図17]



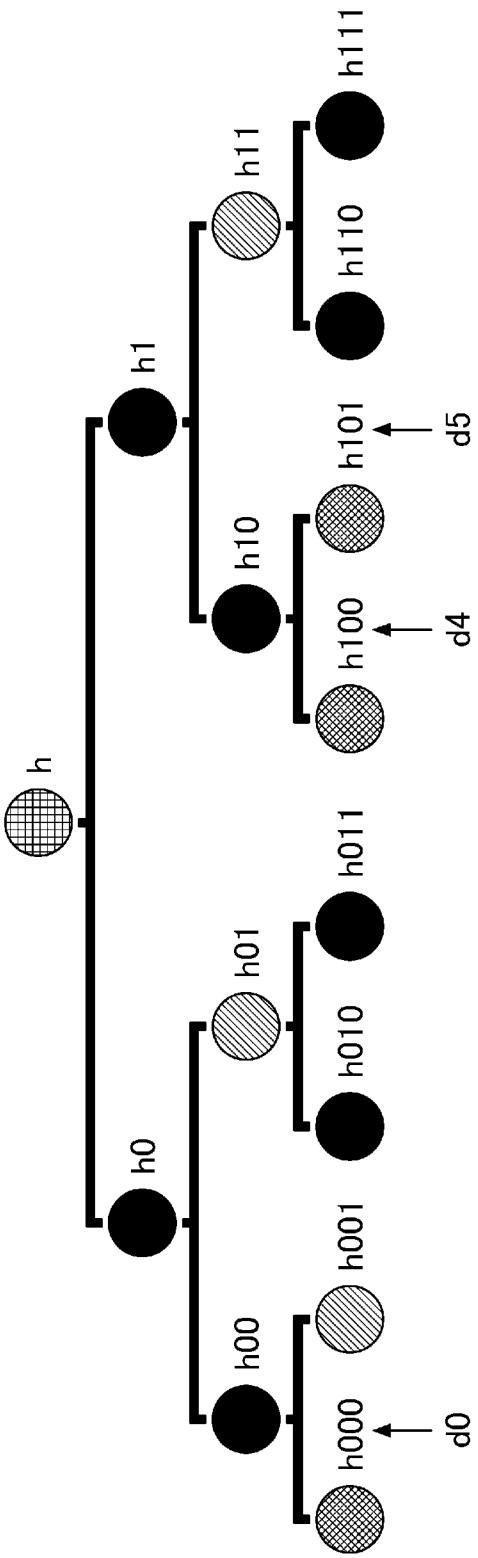
[図18]


h
h0
h1
h00
h01
h10
h11
h000
h001
h010
h011
h100
h101
h110
h111
d0
d1
d2
d3
d4
d5
"00"
"00"
"00"

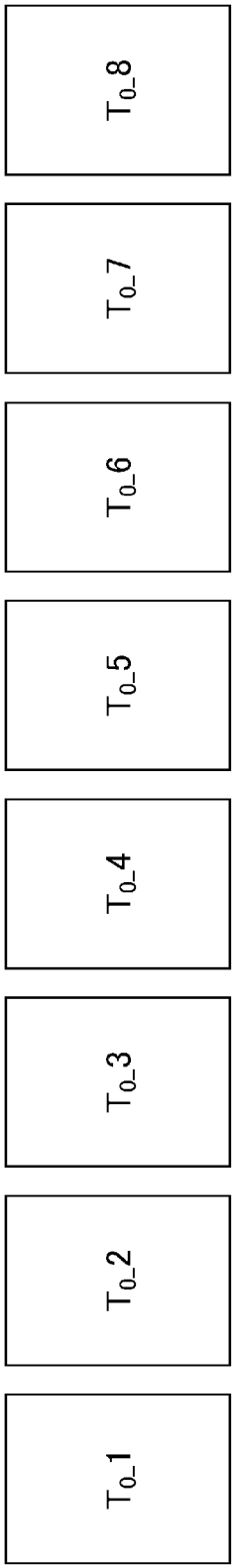
[図19]


h
h0
h1
h00
h01
h10
h11
h000
h001
h010
h011
h100
h101
h110
h111
d0
d1
d2
d3
d4
d5
"00"
"00"

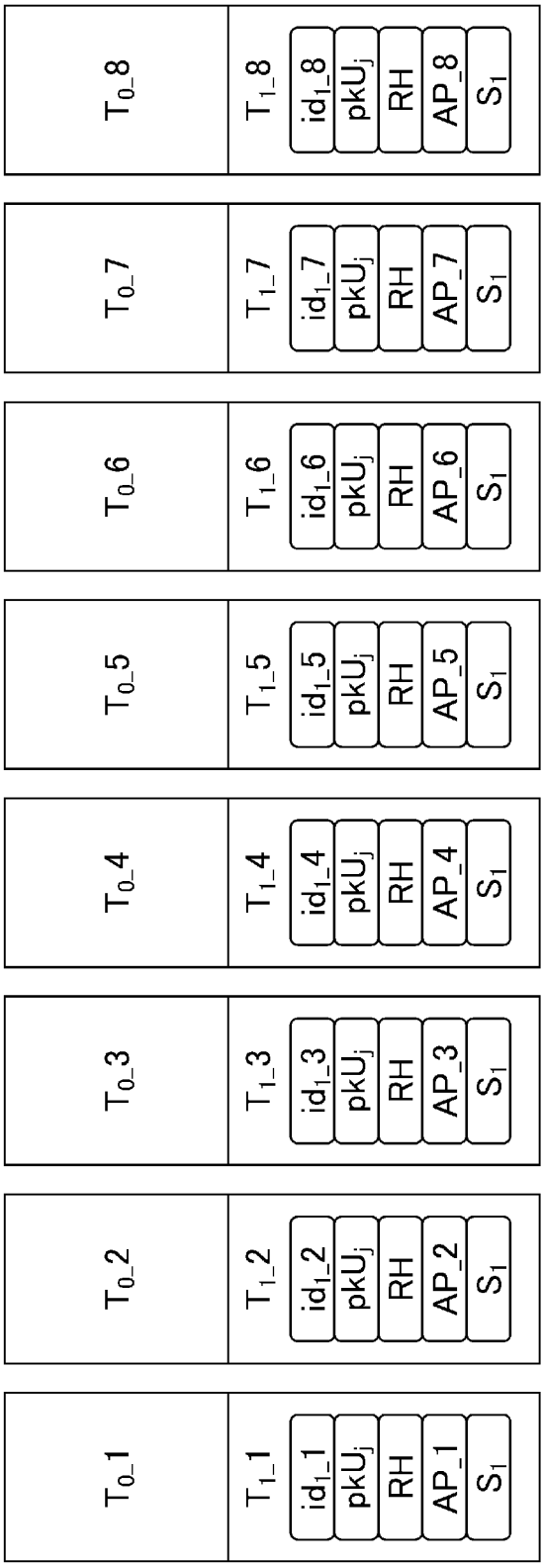
[図20]


h
h0
h1
h00
h01
h10
h11
h000
h001
h010
h011
h100
h101
h110
h111
d0
d4
d5

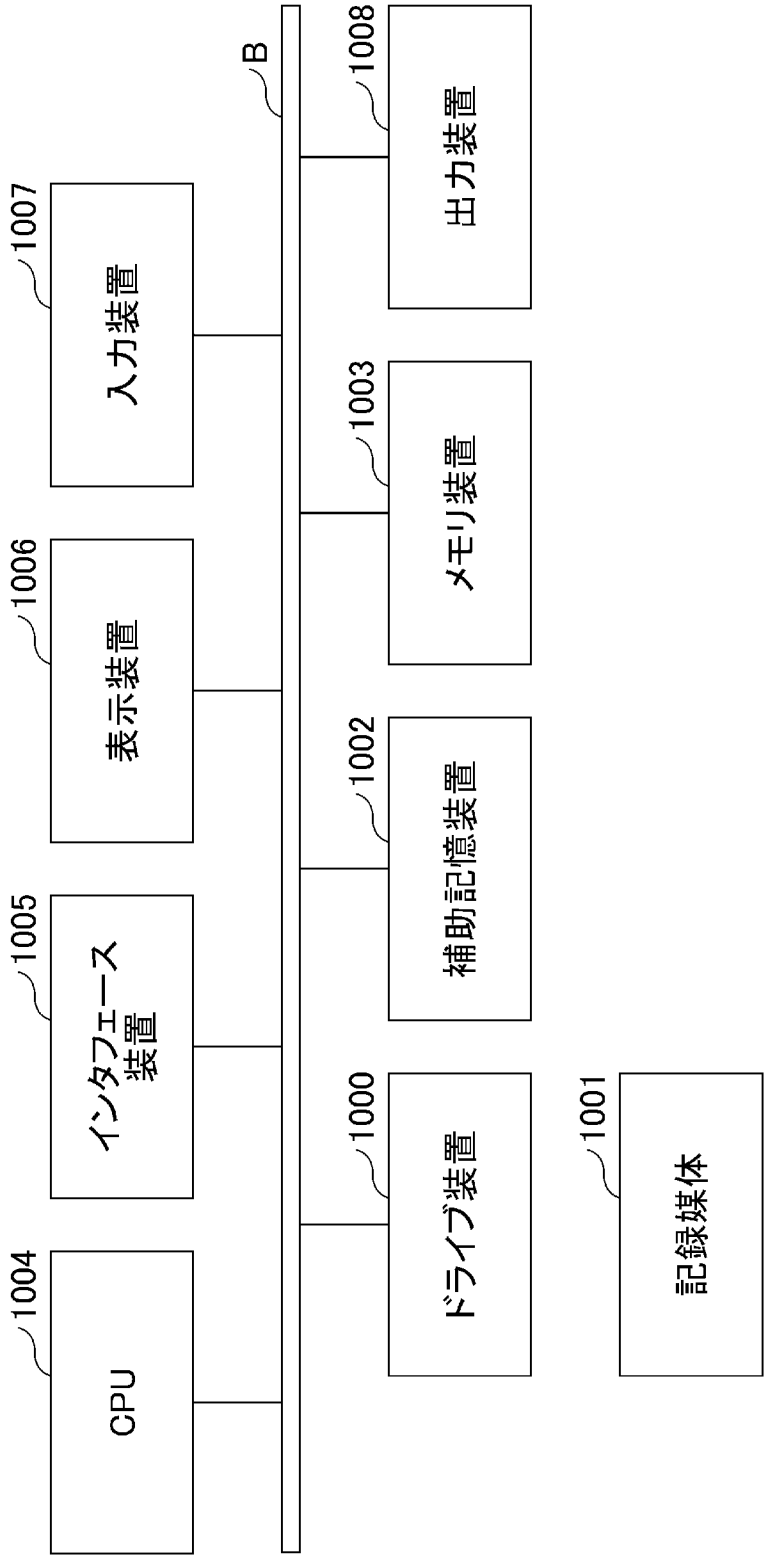
[図21]



[図22]


T0_1
T1_1
id1_1
pkUj
RH
AP_1
S1
T0_2
T1_2
id1_2
pkUj
RH
AP_2
S1
T0_3
T1_3
id1_3
pkUj
RH
AP_3
S1
T0_4
T1_4
id1_4
pkUj
RH
AP_4
S1
T0_5
T1_5
id1_5
pkUj
RH
AP_5
S1
T0_6
T1_6
id1_6
pkUj
RH
AP_6
S1
T0_7
T1_7
id1_7
pkUj
RH
AP_7
S1
T0_8
T1_8
id1_8
pkUj
RH
AP_8
S1

[図23]


B
1004
CPU
1005
インタフェース装置
1006
表示装置
1007
入力装置
1000
ドライブ装置
1002
補助記憶装置
1003
メモリ装置
1008
出力装置
1001
記録媒体

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/039295

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/06(2012.01)i; ***G06Q 40/04***(2012.01)i
FI: G06Q20/06; G06Q40/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q20/06; G06Q40/04

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2023
Registered utility model specifications of Japan 1996-2023
Published registered utility model applications of Japan 1994-2023

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2022-75522 A (FUJITSU LIMITED) 18 May 2022 (2022-05-18) paragraphs [0022]-[0039], fig. 2	3, 6-7
A		1-2, 4-5
Y	JP 2023-509006 A (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) 06 March 2023 (2023-03-06) paragraphs [0100]-[0103], fig. 4	3, 6-7
A	BHATTACHERJEE, Sanjay et.al., Reducing Communication Overhead of the Subset Diffence Scheme, IEEE Transactions on Computers, vol. 65, no. 8, August 2016, pp. 2575-2587 entire text, all drawings	1-2, 4-5, 7
A	JP 7-302288 A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 14 November 1995 (1995-11-14) paragraphs [0076]-[0077], fig. 8	1-2, 4-5, 7

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 November 2023	**28 November 2023**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/039295

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

(Invention 1) Claims 1-2 and 4-5

The invention in claims 1-2 and 4-5 has the special technical feature of "currency processing comprising: depth calculation for calculating the depth of an NNL tree that includes leaf nodes in a number equal to or greater than a value obtained by dividing a sum of money by the smallest unit of an electronic currency; route node determination for determining, on a first NNL tree added to a first electronic currency, a root node of a second NNL tree, which is a partial tree of the first NNL tree, on the basis of the depth; leaf node determination for calculating a random number corresponding to the root node on the basis of a seed of the first NNL tree, and determining a range of leaf nodes corresponding to the sum of money from among the leaf nodes; and currency addition information generation for generating information indicating the random number, the depth, and the range as information to be added to a second electronic currency",
and therefore said invention is classified as invention 1.

(Invention 2) Claims 3 and 6

Claims 3 and 6 share, with claim 1 classified as invention 1, the technical feature of currency processing.

However, this technical feature does not make a contribution over the prior art in the light of the content disclosed in document 1, and thus cannot be said to be a special technical feature. Moreover, these inventions do not share any other same or corresponding special technical feature.

Additionally, claims 3 and 6 are not dependent from claim 1. Furthermore, claims 3 and 6 are not substantially identical to or similarly closely related to any of the claims classified as invention 1.

Therefore, claims 3 and 6 cannot be classified as invention 1.

Claims 3 and 6 have the special technical feature of "currency processing comprising: Merkle tree generation for generating a Merkle tree on the basis of respective hash values of a plurality of electronic currencies to be transferred; and adding the hash value of a root node of the Merkle tree and a signature for the hash value to each of the plurality of electronic currencies", and therefore said claims are classified as invention 2.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☑ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/039295

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2022-75522 A	18 May 2022	CN 114445073 A paragraphs [0022]-[0039], fig. 2	
JP 2023-509006 A	06 March 2023	US 2022/0214995 A1 paragraphs [0133]-[0136], fig. 4 WO 2021/213065 A1	
JP 7-302288 A	14 November 1995	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2023/039295

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06Q 20/06(2012.01)i; G06Q 40/04(2012.01)i
FI: G06Q20/06; G06Q40/04

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

G06Q20/06; G06Q40/04

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２３年
日本国実用新案登録公報	１９９６－２０２３年
日本国登録実用新案公報	１９９４－２０２３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2022-75522 A (富士通株式会社) 18.05.2022 (2022-05-18) [0022]-[0039],図２	3,6-7
A		1-2,4-5
Y	JP 2023-509006 A (▲騰▼▲訊▼科技（深▲セン▼）有限公司) 06.03.2023 (2023-03-06) 段落 [0100] －段落 [0103] 、図４	3,6-7
A	BHATTACHERJEE, Sanjay et.al., Reducing Communication Overhead of the Subset Diffence Scheme, IEEE Transactions on Computers , Vol.65, No.8, 2016.08, pp.2575-2587 全文、全図	1-2,4-5,7
A	JP 7-302288 A (日本電信電話株式会社) 14.11.1995 (1995-11-14) 段落 [0076] －段落 [0077] ,図8	1-2,4-5,7

☐ Ｃ欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー
“A” 特に関連のある文献ではなく、一般的技術水準を示すもの
“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
“O” 口頭による開示、使用、展示等に言及する文献
“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの
“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
“Y” 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
“&” 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
20.11.2023	28.11.2023

名称及びあて先

日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）

太田　龍一 5R 3462

電話番号 03-3581-1101 内線 3562

国際調査報告

国際出願番号
PCT/JP2023/039295

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

（発明１）請求項１－２，４－５
請求項１－２，４－５に係る発明は、「金額を電子通貨の最小単位で除した値以上の数の葉ノードを含むＮＮＬ木の深さを計算するように構成されている深さ計算し、第１の電子通貨に付加された第１のＮＮＬ木において、前記深さに基づいて前記第１のＮＮＬ木の部分木である第２のＮＮＬ木のルートノードを決定するように構成されているルートノード決定し、前記第１のＮＮＬ木のＳｅｅｄに基づいて前記ルートノードに対応する乱数を計算し、前記葉ノードのうち、前記金額に対応させる葉ノードの範囲を決定するように構成されている葉ノードを決定し、前記乱数、前記深さ、前記範囲を示す情報を第２の電子通貨に付加する情報として生成するように構成されている通貨付加情報を生成する、通貨処理」
という特別な技術的特徴を有しているので、発明１に区分する。

（発明２）請求項３，６
請求項３，６は、発明１に区分された請求項１と、通貨処理という共通の技術的特徴を有している。
しかしながら、当該技術的特徴は、文献１の開示内容に照らして、先行技術に対する貢献をもたらすものではないから、当該技術的特徴は、特別な技術的特徴であるとはいえない。また、これらの発明の間には、他に同一の又は対応する特別な技術的特徴は存在しない。
さらに、請求項３，６は、請求項１の従属請求項ではない。また、請求項３，６は、発明１に区分されたいずれの請求項に対しても実質同一又はそれに準ずる関係にはない。
したがって、請求項３，６は発明１に区分できない。
そして、請求項３，６は、「移転対象とする複数の電子通貨のそれぞれハッシュ値に基づいてマークルツリーを生成するように構成されているマークルツリーを生成し、前記マークルツリーのルートノードのハッシュ値と前記ハッシュ値に対する署名とを前記複数の電子通貨のそれぞれに付加する、通貨処理」という特別な技術的特徴を有しているので、発明２に区分する。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求項について作成した。

2. ☑ 追加調査手数料を要求するまでもなく、すべての調査可能な請求項について調査することができたので、追加調査手数料の納付を求めなかった。

3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求項のみについて作成した。

4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求項について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。

☐ 追加調査手数料の納付はあったが、異議申立てはなかった。

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2023/039295

引用文献	公表日	パテントファミリー文献	公表日
JP 2022-75522 A	18.05.2022	CN 114445073 A [0022]-[0039],図２	
JP 2023-509006 A	06.03.2023	US 2022/0214995 A1 [0133]-[0136],FIG.4 WO 2021/213065 A1	
JP 7-302288 A	14.11.1995	（ファミリーなし）	