

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7465764号
(P7465764)

(45)発行日 令和6年4月11日(2024.4.11)

(24)登録日 令和6年4月3日(2024.4.3)

(51)国際特許分類

F I

G 0 6 Q 20/38 (2012.01)

G 0 6 Q 20/38 3 1 0

H 0 4 L 9/32 (2006.01)

H 0 4 L 9/32 2 0 0 B

H 0 4 L 9/32 2 0 0 E

請求項の数 5 (全37頁)

(21)出願番号	特願2020-145947(P2020-145947)	(73)特許権者	000005108
(22)出願日	令和2年8月31日(2020.8.31)		株式会社日立製作所
(65)公開番号	特開2022-40968(P2022-40968A)		東京都千代田区丸の内一丁目6番6号
(43)公開日	令和4年3月11日(2022.3.11)	(74)代理人	110001689
審査請求日	令和5年1月25日(2023.1.25)		青稜弁理士法人
		(72)発明者	長洞 卓
			神奈川県横浜市西区みなとみらい二丁目2番1号 株式会社日立ハイシステム 21内
		(72)発明者	山田 仁志夫
			東京都千代田区丸の内一丁目6番6号
			株式会社日立製作所内
		(72)発明者	橋本 康範
			東京都千代田区丸の内一丁目6番6号
			株式会社日立製作所内

最終頁に続く

(54)【発明の名称】 電子決済システムおよび電子決済方法

(57)【特許請求の範囲】

【請求項1】

資産／資金に関するトランザクションを発行するトランザクション発行装置と、
前記トランザクション発行装置とネットワークにより接続され、前記トランザクション発行装置の発行するトランザクションに基づいて資産／資金の決済を行う資産／資金決済装置とからなる電子決済システムであって、
前記トランザクションは、資産／資金の数量と、トランザクション発行元の電子署名を含むロック解除情報と、取引者の公開鍵を含むロック解除条件とを有し、
第一のトランザクションは、複数の連続してなるロック解除条件を保持するレコードからなり、
前記第一のトランザクションのロック解除条件には、前記トランザクション発行元と異なる電子署名に関する公開鍵情報を含み、
前記資産／資金決済装置は、前記トランザクション発行装置の発行する第一のトランザクションを台帳に転記して、前記第一のトランザクション後に発行された第二のトランザクションの実行の可否を、前記台帳に転記されたロック解除情報とロック解除条件と、第二のトランザクションの台帳のロック解除情報とロック解除条件とを、第一のトランザクションの複数の連続してなるロック解除条件の順序に従って、照合させることにより判定して、実行可と判定された前記第二のトランザクションを実行することを特徴とする電子決済システム。

【請求項2】

前記トランザクションのロック解除情報は、さらに、秘密情報を有し、前記トランザクションのロック解除条件は、前記トランザクションのロック解除情報の秘密情報に対するハッシュ値を有し、

前記第一のトランザクションのロック解除条件には、前記トランザクション発行元の保持する秘密情報と異なるハッシュ値を含むことを特徴とする請求項1記載の電子決済システム。

【請求項3】

第一の資産／資金を所有する第一の取引者と、第二の資産／資金を所有する第二の取引者が、それぞれ第一の資産／資金と第二の資産／資金とを交換する取引であって、

前記第一の取引者が取引をキャンセルする場合に発行されるトランザクションのロック解除情報に、前記第二の取引者の発行したトランザクションに含まれる電子署名と、秘密情報を含むことを特徴とする請求項2記載の電子決済システム。

10

【請求項4】

前記トランザクション発行装置は、前記トランザクション発行装置の発行するトランザクションに対応した取引状況管理テーブルを有し、

取引状況管理テーブルのレコードは、「急」・「不急」が区分されており、

前記トランザクション発行装置は、「急」とされたレコードに対応するトランザクションを優先して発行することを特徴とする請求項1記載の電子決済システム。

【請求項5】

資産／資金に関するトランザクションを発行するトランザクション発行装置と、

20

前記トランザクション発行装置とネットワークにより接続され、前記トランザクション発行装置の発行するトランザクションに基づいて資産／資金の決済を行う資産／資金決済装置とからなる電子決済システムによる電子決済方法であって、

前記トランザクションは、資産／資金の数量と、トランザクション発行元の電子署名と秘密情報とを含むロック解除情報と、取引者の公開鍵と前記ロック解除情報のハッシュ値とを含むロック解除条件とを有し、

第一のトランザクションは、複数の連続してなるロック解除条件を保持するレコードからなり、

前記第一のトランザクションのロック解除条件には、前記トランザクション発行元と異なる電子署名に関する公開鍵情報を含み、

30

前記資産／資金決済装置が、前記トランザクション発行装置の発行する第一のトランザクションを台帳に転記するステップと、

前記資産／資金決済装置が、前記第一のトランザクション後に発行された第二のトランザクションの実行の可否を、前記台帳に転記されたロック解除情報とロック解除条件と、第二のトランザクションの台帳のロック解除情報とロック解除条件とを、第一のトランザクションの複数の連続してなるロック解除条件の順序に従って、照合させることにより判定して、実行可と判定された前記第二のトランザクションを実行するステップとを有することを特徴とする電子決済方法。

【発明の詳細な説明】

【技術分野】

40

【0001】

本発明は、電子決済システムおよび電子決済方法に係り、特に、資産・資金を預託して、電子決済取引をする場合に、取引の安全性を担保しながら、資産・資金の流動性の低下を防止するのに好適な電子決済システムおよび電子決済方法に関する。

【背景技術】

【0002】

情報処理技術の進展により、株式などの証券の取引を、サーバなどの情報処理装置とそれらを接続したネットワーク回線により構成されたシステムを介して行う電子商取引が一般的に普及してきている。

【0003】

50

このような電子商取引の一例として、非特許文献1には、D v P (Delivery Versus Payment) 取引において、H T L C (Hashed Timelock Contract) を実現するメカニズムが記載されている。この非特許文献1には、秘密情報やハッシュ関数、また、タイムアウトといった仕組みを活用した、資産/資金のアトミックな交換方法について記載されている。

【0004】

ここで、D v P 取引とは、証券と資金の授受をリンクさせ、代金の支払いが行われることを条件に証券の引渡しを行い、逆に、証券の引渡しが行われることを条件に代金の支払いを行うことにより、仮に決済不履行が生じても、両者において取りはぐれが生じない決済取引の方法である。

【0005】

また、H T L C とは、まず、取引者の資産/資金をそれぞれエスクロー (Escrow: 預託) 用の領域に移動させ、その後、一方の資産/資金が相手に渡ると、もう一方の資産/資金も相手に移動可能とし、資産が移動されないままに一定時間たつと、タイムアウトとなり、エスクロー用の領域の資産をそれぞれ元の保有者が引き戻せるようにする取引メカニズムに関するものである。

また、非特許文献2には、このようなH T L C の問題点が指摘されている。

【先行技術文献】

【非特許文献】

【0006】

【文献】TierNolan, Bitcoin Forum > Bitcoin > Development & Technical Discussion > Alt chains and atomic transfers、[online]、July 18, 2020、[令和02年7月18日検索]、インターネット<URL: <https://bitcointalk.org/index.php?topic=193281.0>>

【文献】日本銀行、欧州中央銀行、“Project Stella: 日本銀行・欧州中央銀行による分散型台帳技術に関する共同調査報告書(第2フェーズ)”、2018年3月27日、[令和02年7月18日検索]、インターネット<URL: https://www.boj.or.jp/announcements/release_2018/data/rel180327a1.pdf, https://www.boj.or.jp/announcements/release_2018/data/rel180327a3.pdf, https://www.boj.or.jp/announcements/release_2018/data/rel180327a2.pdf, https://www.boj.or.jp/announcements/release_2018/data/rel180327a4.pdf>

【発明の概要】

【発明が解決しようとする課題】

【0007】

上記非特許文献1には、複数の資産/資金決済装置をまたがり、かつ、仲介者なくD v P 取引を実現するH T L C のメカニズムについて記載されている。

【0008】

しかしながら、非特許文献1に記載されている技術は、取引不成立時の資産/資金の流動性の低下という課題がある。この点について、非特許文献2においては、「流動性の利用という観点からは、複数台帳H T L C 方式の方が、単一台帳方式と比べて効率性が低くなる傾向にある。特に、資産のロックが行われたものの、決済が未了となり、タイムアウト時間経過後に元の所有者に戻る場合には、こうした傾向が強くなる。」と記載されている。

【0009】

本発明の目的は、取引者が資産を預託する電子決済を利用したD v P 取引において、ロック中の資産をタイムアウトによらずに安全に引き戻すことができ、取引の安全性を担保しつつ、取引不成立時における資産/資金の流動性を低下させることを回避することができる電子決済システムおよび電子決済方法を提供することにある。

【課題を解決するための手段】

【0010】

10

20

30

40

50

本発明の電子決済システムの構成は、好ましくは、資産／資金に関するトランザクションを発行するトランザクション発行装置と、トランザクション発行装置とネットワークにより接続され、トランザクション発行装置が発行するトランザクションに基づいて資産／資金の決済を行う資産／資金決済装置とからなる電子決済システムであって、トランザクションは、資産／資金の数量と、トランザクション発行元の電子署名を含むロック解除情報と、取引者の公開鍵を含むロック解除条件とを有し、第一のトランザクションは、複数の連続してなるロック解除条件を保持するレコードからなり、第一のトランザクションのロック解除条件には、トランザクション発行元と異なる電子署名に関する公開鍵情報を含み、資産／資金決済装置は、トランザクション発行装置が発行する第一のトランザクションを台帳に転記して、第一のトランザクション後に発行された第二のトランザクションの実行の可否を、台帳に転記されたロック解除情報とロック解除条件と、第二のトランザクションの台帳のロック解除情報とロック解除条件とを、第一のトランザクションの複数の連続してなるロック解除条件の順序に従って、照合させることにより判定して、実行可と判定された第二のトランザクションを実行するようにしたものである。

10

【発明の効果】

【0011】

本発明によれば、取引者が資産を預託する電子決済を利用したD v P取引において、ロック中の資産をタイムアウトによらずに安全に引き戻すことができ、取引の安全性を担保しつつ、取引不成立時における資産／資金の流動性を低下させることを回避することができる。

20

【図面の簡単な説明】

【0012】

【図1】電子決済システムの全体構成図である。

【図2】トランザクション発行装置のハードウェア・ソフトウェア構成図である。

【図3】資産／資金決済装置のハードウェア・ソフトウェア構成図である。

【図4】台帳の一例を示す図である。

【図5】鍵情報テーブルの一例を示す図である。

【図6】初期トランザクションテンプレートの一例を示す図である。

【図7】初期トランザクション実行結果テンプレートの一例を示す図である。

【図8A】パラメータテンプレートの一例を示す図である（その一）。

30

【図8B】パラメータテンプレートの一例を示す図である（その二）。

【図9】取引状況管理情報テンプレートの一例を示す図である。

【図10】取引が成立しないときのD v P取引パターンの一例を示す図である。

【図11】取引が成立したときのD v P取引パターンの一例を示す図である。

【図12】電子決済システムにおける第一の初期トランザクション実行処理を示すフローチャートである。

【図13】第一の初期トランザクションに利用する資産／資金を選択する処理の一例を示す図である。

【図14A】パラメータの情報を取得する処理の一例を示す図である（その一）。

【図14B】パラメータの情報を取得する処理の一例を示す図である（その二）。

40

【図15A】第一の初期トランザクション作成処理の一例を示す図である（その一）。

【図15B】第一の初期トランザクション作成処理の一例を示す図である（その二）。

【図16】第一の初期トランザクションの実行可否を判定する処理の一例を示す図である。

【図17】第一の初期トランザクションの実行処理の一例を示す図である。

【図18】第一の初期トランザクションの実行結果を確認する処理の一例を示す図である。

【図19】電子決済システムにおける第二の初期トランザクション実行処理を示すフローチャートである。

【図20】第二の初期トランザクションに利用する資産／資金を選択する処理の一例を示す図である。

【図21A】パラメータの情報を取得する処理の一例を示す図である（その一）。

50

【図 2 1 B】パラメータの情報を取得する処理の一例を示す図である（その二）。

【図 2 2】第一の初期トランザクション実行結果を検証する処理の一例を示す図である。

【図 2 3】第二の初期トランザクションの実行処理の一例を示す図である。

【図 2 4】第二の初期トランザクションの実行結果を確認する処理の一例を示す図である。

【図 2 5 A】第二の初期トランザクションの実行結果を検証する処理の一例を示す図である（その一）。

【図 2 5 B】第二の初期トランザクションの実行結果を検証する処理の一例を示す図である（その二）。

【図 2 5 C】第二の初期トランザクションの実行結果を検証する処理の一例を示す図である（その三）。

【図 2 6】電子決済システムの初期トランザクション後の通常トランザクションを発行するときの動作を示すフローチャートである。

【図 2 7】ユーザが取引を選択する一例を示す図である。

【図 2 8】秘密情報を更新する処理の一例を示す図である。

【図 2 9】選択した取引状況管理情報が示す案件について、実行可否を判定する処理の一例を示す図である。

【図 3 0】トランザクションの実行処理（取引が成立した場合の一連のトランザクションと台帳の様子）を説明する図である。

【図 3 1】トランザクションの実行処理（取引が成立しなかった場合のトランザクションと台帳の様子）を説明する図である。

【図 3 2】取引が成立した場合の取引の全体の一連のトランザクションと台帳の様子を示す図である。

【図 3 3】取引が成立しなかった場合の取引の全体の一連のトランザクションと台帳の様子を示す図である。

【発明を実施するための形態】

【0013】

以下、本発明に係る一実施形態を、図 1 ないし図 3 3 を用いて説明する。

【0014】

まず、図 1 ないし図 3 を用いて一実施形態に係る電子決済システムの構成について説明する。

【0015】

本実施形態の電子決済システム 100 は、分散型台帳技術（DLT：Distributed Ledger Technology）を前提とするものである。分散型台帳技術では、市場における取引参加者（取引者）が共通の取引モデルに基づいたトランザクションと台帳を前提として、取引者がトランザクションを発行し、システム側でそのトランザクションを台帳に反映させ、かつ、発行されたトランザクションの成否を判断して取引が進められる。

【0016】

本実施形態では、取引者としては、ユーザ A、ユーザ B が参加し、ユーザ A が株式を提供し、その代価としてユーザ B から通貨「円」を受取る取引のモデル（ユーザ B は、通貨「円」により、ユーザ A から株式を購入する）の取引イメージを例として説明する。

【0017】

電子決済システム 100 は、二つ以上のトランザクション発行装置 110（図 1 では、二つのトランザクション発行装置を有しており、それぞれ 110 A、110 B と表記）、二つ以上の資産／資金決済装置 150（図 1 では、三つの資産／資金決済装置を有しており、それぞれ取り扱う資産／資金 L、資産／資金 M、資産／資金 N ごとに、150 L、150 M、150 N と表記）、共有領域 180 を有しており、それぞれネットワーク 5 により接続されている。ネットワーク 5 は、LAN（Local Area Network）でもよいし、インターネットのようなグローバルネットワークであってもよい。

【0018】

トランザクション発行装置 110 は、取引の単位としてのトランザクションを発行する

10

20

30

40

50

情報処理装置である。トランザクション発行装置 110A、110B は、ユーザ A、B のアクセス端末 10A、10B のみから操作できるように、それぞれネットワーク 7A、7B により接続されている。また、各トランザクション発行装置 110A、110B は、それぞれ複数の資産／資金決済装置 150 とデータを授受できるようにネットワーク 5 により接続されている。また、各トランザクション発行装置 110A、110B は、それぞれ共有領域 180 とデータを授受できるよう接続されている。共有領域 180 は、図示していないが、各トランザクション発行装置 110A、110B から共通にアクセスできるファイルサーバやデータベースサーバが提供する領域であり、DvP 取引テンプレート記憶部 181 を有している。

【0019】

トランザクション発行装置 110 は、それぞれのデータを記憶する記憶部として、鍵情報記憶部 121、パラメータ記憶部 122、取引状況管理情報記憶部 123、作成中トランザクション記憶部 124 を有し、それぞれデータを処理する機能部として、資産／資金決済装置アクセス部 111、共有領域アクセス部 112、トランザクション発行部 113、取引状況管理部 114 を有する。

【0020】

資産／資金決済装置アクセス部 111 は、資産／資金決済装置 150 にネットワーク 5 を介してアクセスする機能部である。共有領域アクセス部 112 は、共有領域 180 のデータにアクセスする機能部である。トランザクション発行部 113 は、取引に係るトランザクションを発行する機能部である。取引状況管理部 114 は、取引を管理して、その情報をユーザに提示する機能部である。

【0021】

なお、トランザクション発行装置 110 で扱うデータ構造は、後に詳説する。

【0022】

資産／資金決済装置 150 は、トランザクションを受信し、トランザクションの内容を台帳に転記したり、そのトランザクションにより取引を進め決済を行う装置である。本実施形態では、資産／資金決済装置 150L、160M、170N は、それぞれ異なる資産／資金である資産／資金 L、資産／資金 M、資産／資金 N について、各ユーザの保有残高を管理している。ここでいう資産／資金は、株式や国債などの証券や、通貨「円」、「ドル」、「ユーロ」などの取引の価値を担う単位である。ここでは、それぞれの装置が異なる資産／資金の台帳を有するようにしたが、一つの資産／資金決済装置 150 で複数の資産／資金を取り扱えるようにしてもよい。

【0023】

資産／資金決済装置 150 は、それぞれのデータを記憶する記憶部として、台帳記憶部 154、実行済トランザクション記憶部 155、実行前トランザクション記憶部 156 を有し、それぞれデータを処理する機能部として、トランザクション受信部 151、トランザクション実行可否判定部 152、トランザクション実行部 153 を有する。

【0024】

トランザクション受信部 151 は、トランザクション発行装置 110 が発行するトランザクションをネットワーク 5 を介して受信する機能部である。トランザクション実行可否判定部 152 は、受信したトランザクションの取引における可否を判定する機能部である。トランザクション実行部 153 は、取引が可と判定されたトランザクションを実行する機能部である。

【0025】

なお、資産／資金決済装置 150 で扱うデータ構造は、後に詳説する。

【0026】

本実施形態においては、ユーザ A がユーザ B へ資産／資金管理システム 150 で管理されている資産／資金 L（株式）を引き渡し、対価として、ユーザ B がユーザ A へ資産／資金管理システム 160 で管理されている資産／資金 M（通貨「円」）を引き渡すというシナリオに基づき説明する。

10

20

30

40

50

【0027】

次に、図2および図3を用いてトランザクション発行装置と資産／資金決済装置のハードウェア・ソフトウェア構成について説明する。

【0028】

トランザクション発行装置110のハードウェア構成としては、例えば、図2に示されるパーソナルコンピュータのような一般的な情報処理装置で実現される。

【0029】

トランザクション発行装置110は、CPU (Central Processing Unit) 4002、主記憶装置4004、ネットワークI/F (InterFace) 4006、表示I/F 4008、入出力I/F 4010、補助記憶I/F 4012が、バスにより結合された形態になっている。

10

【0030】

CPU 4002は、トランザクション発行装置110の各部を制御し、主記憶装置4004に必要なプログラムをロードして実行する。

【0031】

主記憶装置4004は、通常、RAMなどの揮発メモリで構成され、CPU 4002が実行するプログラム、参照するデータが記憶される。

【0032】

ネットワークI/F 4006は、ネットワーク5と接続するためのインタフェースである。

20

【0033】

表示I/F 4008は、LCD (Liquid Crystal Display) などの表示装置4020を接続するためのインタフェースである。

【0034】

入出力I/F 4010は、入出力装置を接続するためのインタフェースである。図2の例では、キーボード4030とポインティングデバイスのマウス4032が接続されている。

【0035】

補助記憶I/F 4012は、HDD (Hard Disk Drive) 4050やSSD (Solid State Drive) などの補助記憶装置を接続するためのインタフェースである。

30

【0036】

HDD 4050は、大容量の記憶容量を有しており、本実施形態を実行するためのプログラムが格納されている。トランザクション発行装置110には、資産／資金決済装置アクセスプログラム4051、共有領域アクセスプログラム4052、トランザクション発行プログラム4053、取引状況管理プログラム4054がインストールされている。

【0037】

資産／資金決済装置アクセスプログラム4051、共有領域アクセスプログラム4052、トランザクション発行プログラム4053、取引状況管理プログラム4054は、それぞれ資産／資金決済装置アクセス部111、共有領域アクセス部112、トランザクション発行部113、取引状況管理部114の機能を実現するプログラムである。

40

【0038】

また、HDD 4050には、鍵情報テーブル400、パラメータテーブル910、取引状況管理情報テーブル1010、作成中トランザクション200Mが格納されている。

【0039】

また、資産／資金決済装置150のハードウェア構成としては、例えば、図3に示されるサーバ装置のような一般的な情報処理装置で実現される。

【0040】

各機能部は、図2に示した資産／資金決済装置の各部の機能と同様である。

【0041】

資産／資金決済装置150のHDD 5050は、トランザクション受信プログラム50

50

5 1、トランザクション実行可否判定プログラム 5 0 5 2、トランザクション実行プログラム 5 0 5 3 がインストールされている。

【0 0 4 2】

トランザクション受信プログラム 5 0 5 1、トランザクション実行可否判定プログラム 5 0 5 2、トランザクション実行プログラム 5 0 5 3 は、それぞれトランザクション受信部 1 5 1、トランザクション実行可否判定部 1 5 2、トランザクション実行部 1 5 3 の機能を実現するプログラムである。

【0 0 4 3】

また、資産／資金決済装置 1 5 0 の HDD 5 0 5 0 には、台帳、実行済トランザクション、実行前トランザクションが格納されている。

【0 0 4 4】

次に、図 4 ないし図 9 を用いて本実施形態の電子決済システムにおけるデータ構造について説明する。

【0 0 4 5】

まず、図 4 を用いて台帳の一例について説明する。

台帳 3 0 0 は、トランザクション発行装置 1 1 0 の発行したトランザクションを反映し、かつ、そのトランザクションの実行の可否を判定するために、資産／資金決済装置 1 5 0 が保持するデータである。

【0 0 4 6】

台帳 3 0 0（図 4 は、資産／資金 L の例）は、データ属性 3 1 0 として、資産／資金 ID 3 1 1、残高 3 1 2、ロック解除条件 3 1 3 を有する。ロック解除条件 3 1 3 は、項番 3 1 4、公開鍵 3 1 5、ハッシュ値 3 1 6、時刻 3 1 7 のサブ属性によって構成される。また、台帳 3 0 0 は、データ属性 3 1 0 の各要素に対応するデータをもつ行単位の情報であるレコードを一つ以上有する。

【0 0 4 7】

なお、ロック解除条件 3 1 3 に関し、公開鍵 3 1 5 に対応するデータは、「当該レコードの資産を移転するには、発行されたトランザクションに、その記載のデータに対応する電子署名が必要」ということを意味する。また、ハッシュ値 3 1 6 に対応するデータは、「当該レコードの資産を移転するには、発行されたトランザクションに、ハッシュ関数の出力結果が記載のデータになるような入力となる秘密情報が必要」ということを意味する。時刻 3 1 7 に対応するデータは、「当該レコードの資産を移転するには、現在時刻が記載のデータが示す時刻以降であることが必要」ということを意味する。

【0 0 4 8】

また、ロック解除条件 3 1 3 に関し、項番 3 1 4 は、各条件の適用可能順序を示している。例えば、図 4 に示した例では、資産／資金 ID 3 1 1 が「L 0 8 0 1」であるレコードについては、以下のいずれかの順序で、ロック解除条件に対応するトランザクションを実行する必要があることを意味する。

- ・「1，－」の条件
- ・「2，－」の条件
- ・「3，－」の条件後、「3，1」の条件
- ・「3，－」の条件後、「3，2」の条件

【0 0 4 9】

次に、図 5 を用いて鍵情報テーブルの一例について説明する。

鍵情報テーブル 4 0 0（図 5 は、ユーザ A の例）は、ユーザの秘密鍵と公開鍵の情報を格納するテーブルであり、図 5 に示されるように、データ属性 4 1 0 として、システム 4 1 1、ユーザ 4 1 2、秘密鍵 4 1 3、公開鍵 4 1 4 を有する。また、鍵情報テーブル 4 0 0 は、データ属性 4 1 0 に対応するデータをもつ行単位の情報であるレコードを一つ以上要する。

【0 0 5 0】

システム 4 1 1 には、資産／資金決済装置のシステム名称が格納される。以下の例では

10

20

30

40

50

、資産／資金の名称と同一視している。ユーザ４１２には、ユーザ名称が格納される。本実施形態では、取引のユーザは、「ユーザＡ」、「ユーザＢ」である。秘密鍵４１３、公開鍵４１４には、それぞれ公開鍵技術における秘密鍵のデータと、その秘密鍵に対応する公開鍵のデータが格納される。秘密鍵は、そのユーザ自身のみが知る暗号鍵であり、公開鍵は、取引に参加する者の全てが知ることを許される暗号鍵である。

【００５１】

なお、ユーザ名４１２が「Me」であるレコードは、当該レコードが、当該情報保有者自身に関するレコードであることを意味（ユーザＡなら、「ユーザＡ」、ユーザＢなら、「ユーザＢ」）し、秘密鍵４１３に対応するデータとして有効な値が記憶されているものとする。また、ユーザ名４１２が「Me」でないレコードは、当該レコードが、他社に関するレコードであることを意味し、秘密鍵４１３に対応するデータは空欄であるものとする。

10

【００５２】

次に、図６を用いて初期トランザクションテンプレートの一例について説明する。

初期トランザクションテンプレート７００は、トランザクション発行装置において、初期トランザクションを生成するためのテンプレートであり、共有領域１８０のＤｖＰ取引テンプレート記憶部１８１に保持される。ここで、初期トランザクションとは、取引の流れを台帳に転記するためのテンプレートであり、それ以降のトランザクションが発行されときには、転記された台帳のレコードとマッチングさせ、実行可否のときには、トランザクションが実行され、その対応する台帳のレコードは、実行後に抹消される（具体例は、後述）。なお、本実施形態では、初期トランザクション後に発行されるトランザクションを通常トランザクションということにする。

20

【００５３】

本実施形態の初期トランザクションテンプレート７００は、第一の初期トランザクションテンプレート７００Ａと、第二の初期トランザクションテンプレート７００Ｂがあるものとする。

【００５４】

第一の初期トランザクションテンプレート７００Ａは、データ属性７２０として、トランザクションＩＤ７２１、資産／資金ＩＤ７２２、金額７２３、ロック解除情報７２４、ロック解除条件７２５を有する。このうちロック解除情報７２４は、電子署名７２６、秘密情報７２７のサブ属性によって構成され、トランザクションを発行した主体を明らかにするためのデータである。また、ロック解除条件７２５は、項番７２８、公開鍵７２９、ハッシュ値７３０、時刻７３１のサブ属性によって構成される。また、第一の初期トランザクションテンプレート７００Ａは、データ属性７２０の各要素に対応するデータを有する行単位の情報であるレコードを一つ以上有する。

30

【００５５】

第一の初期トランザクションテンプレート７００Ａにおいて、ロック解除条件７２５に対応するデータは、図４に示した台帳３００におけるロック解除条件３１３と同様の意味を有する。

【００５６】

また、第二の初期トランザクションテンプレート７００Ｂについても、データそのものは異なるものの、各々の意味は、第一の初期トランザクションテンプレート７００Ａと同様である。

40

【００５７】

次に、図７を用いて初期トランザクション実行結果テンプレートの一例について説明する。

初期トランザクション実行結果テンプレートは、初期トランザクション発行後に、取引に参加するユーザが、その取引パターンを検証するためのテンプレートであり、共有領域１８０のＤｖＰ取引テンプレート記憶部１８１に保持される。

【００５８】

50

本実施形態の初期トランザクション実行結果テンプレート800は、第一の初期トランザクション実行結果テンプレート800Aと、第二の初期トランザクション実行結果テンプレート800Bがあるものとする。

【0059】

第一のトランザクション実行結果テンプレート800Aは、データ属性820として、資産／資金ID821、残高822、ロック解除条件823を有する。このうちロック解除条件823は、項番824、公開鍵825、ハッシュ値826、時刻827のサブ属性によって構成される。また、第一のトランザクション実行結果テンプレート800Aは、データ属性820の各要素に対応するデータをもつ行単位の情報であるレコードを一つ以上有する。

10

【0060】

第一の初期トランザクション実行結果テンプレートに800Aにおいて、ロック解除条件823に対応するデータは、図3の台帳300におけるロック解除条件313と同様の意味を有する。

【0061】

第二の初期トランザクション実行結果テンプレート800Bについても、データそのものは異なるものの、その意味は、第一の初期トランザクション実行結果テンプレート800Aと同様である。

【0062】

次に、図8Aおよび図8Bを用いてパラメータテンプレートについて説明する。

20

パラメータテンプレート900は、他のテンプレートで参照されるパラメータに関する情報を保持するテンプレートであり、共有領域180のDvP取引テンプレート記憶部181に保持される。本実施形態では、パラメータテンプレート900の値を埋めたデータ構造を、パラメータテーブルといい、パラメータテーブルに格納されている値をパラメータということにする。

【0063】

本実施形態のパラメータテンプレート900は、第一のパラメータテンプレート900Aと、第二のパラメータテンプレート900Bがあるものとする。

【0064】

第一のパラメータテンプレート900Aは、データ属性920として、資産／資金921、変数名922、区分923、取得手段924、値925を有する。このうち資産／資金921は、資産／資金1：920、資産／資金2：921によって構成される。資産／資金1：920、資産／資金2：921は、それぞれサブ属性として、システム930、資産／資金ID931のサブ属性を有する。

30

【0065】

変数名922には、テンプレートとして参照されるときの変数の名称が格納される。区分は、「公開鍵」、「秘密情報」、「ハッシュ値」などの変数のカテゴリである。取得手段924は、システムが値を求めるときの方法が格納される。

【0066】

値920は、区分923が「公開鍵」であるレコードに限り、資産／資金1：928、資産／資金2：929のサブ属性に分けることも可能とする。資産／資金1：928、資産／資金2：929は、資産／資金1：920、資産／資金2：921によって定義されたシステム、それぞれのシステム、資産／資金IDに対応して、それぞれのレコードに定義された変数名の値が格納されることを意味する。

40

【0067】

また、第一のパラメータテンプレート900Aは、データ属性920の各要素に対応するデータを有する行単位の情報であるレコードを一つ以上有する。

【0068】

なお、変数名922のデータは、図6の初期トランザクションテンプレート700のロック解除条件725のデータや、図7の初期トランザクション実行結果テンプレート80

50

0のロック解除条件823のデータと対応する。区分923のデータは、本実施形態においては、「公開鍵」「秘密情報」「ハッシュ値」「時刻」の4種類が定義し得るものとする。取得手段924のデータは、本実施形態においては「参照」「作成」の2種類が定義し得るものとする。

【0069】

第二のパラメータテンプレート900Bについても、データそのものは異なるものの、その意味は、第一のパラメータテンプレート900Aと同様である。

【0070】

次に、図9を用いて取引状況管理情報テンプレートについて説明する。

取引状況管理情報テンプレート1000は、ユーザがとり得る取引をシステム側から提示するためのテンプレートであり、共有領域180のDvP取引テンプレート記憶部181に保持される。取引状況管理情報テンプレート1000は、取引状況管理情報記憶部123に取引状況管理情報テーブルとして保持される。

【0071】

本実施形態の取引状況管理情報テンプレート1000は、第一の取引状況管理情報テンプレート1000Aと、第二の取引状況管理情報テンプレート1000Bによって構成される。

【0072】

第一の取引状況管理情報テンプレート1000Aは、図9に示されるように、データ属性1020として、資産／資金1021、項番1022、至急フラグ1023、区分1024を有する。資産／資金1021、サブ属性として、システム1030、資産／資金ID1031のサブ属性を有する。

【0073】

また、第一の取引状況管理情報テンプレート1000Aは、データ属性1020の各要素に対応するデータを有する行単位の情報であるレコードを一つ以上有する。

【0074】

なお、項番1022のデータは、図6の初期トランザクションテンプレート700の項番728のデータや、図7の初期トランザクション実行結果テンプレート800の項番824のデータと対応する。区分1024は、取引の結果をユーザに教示する欄であり、本実施形態においては「成立」「不成立」の2種類が登場し得るものとする。

【0075】

至急フラグ1023がONの取引は、ユーザからトランザクションの選択をまたずに、システムがただちに実行する取引であるとする。

【0076】

第二の取引状況管理情報テンプレート1000Bについても、データそのものは異なるものの、その意味は、第一の取引状況管理情報テンプレート1000Aと同様である。

【0077】

以上、各種テンプレートについて説明したが、図においては、テンプレートから生じたテーブル、トランザクションについても、分かりやすくするため、元のテンプレートと同じ符号を引用している所がある。

【0078】

次に、図10および図11を用いて本実施形態の電子決済システムにおける取引パターンの一例について説明する。

【0079】

図10に示されるのは、取引が成立しないときのDvP取引パターンであり、このときのDvP取引パターン600は、第一の資産／資金移転フロー610と、第二の資産移転フロー640で表現される。本実施形態においては、第一の資産／資金移転フローが資産／資金Lに対応する取引の流れを表現しており、また、第二の資産／資金移転フローが資産／資金Mに対応する取引の流れを表現している。

【0080】

資産移転フロー 610、640 は、状態をノードとし、そのノードをつなぐ状態遷移（遷移条件）で表現されるエッジからなる有向グラフの形態で表現される。

【0081】

状態遷移（遷移条件）は、図 6 で示した初期トランザクションテンプレート 700 のロック解除情報とロック解除条件で表現される。

【0082】

第一の資産移転フロー 610 は、状態として、初期状態 611、エスクロー状態 612、キャンセルエスクロー状態 613、終了状態 614、615 状態を有し、それらのノードの状態遷移（遷移条件）621～626 を有する。エスクロー状態 612 は、資産／資金 L が取引のために預託された状態を意味する。キャンセルエスクロー状態 613 は、預託のキャンセル待ち状態であることを意味する。

10

【0083】

第一の資産移転フロー 610 において、エスクロー状態 612 からは、状態遷移（遷移条件）622 または状態遷移（遷移条件）623 に記載の条件を満たした場合に、終了状態 614、615 に遷移でき、また、状態遷移（遷移条件）624 に記載の条件を満たした場合に、キャンセルエスクロー状態 613 に遷移できることを意味する。また、途中状態 613 からは、状態遷移（遷移条件）625 または状態遷移（遷移条件）626 の条件を満たした場合に終了状態 615 に遷移できることを意味する。

【0084】

第二の資産移転フロー 640 についても、データそのものは異なるものの、その意味は、第一の資産移転フロー 610 と同様である。

20

【0085】

ここで、状態遷移（遷移条件）622 に記載されている「・電子署名：S_{b1} for P_b、・秘密情報：x₁ for y₁」というのは、トランザクションのロック解除情報として、公開鍵 P_b に対応する電子署名 S_{b1} と、ハッシュ値 y₁ をとる秘密情報 x₁ を有するトランザクションが発行され、状態が遷移することを意味する。

【0086】

また、状態遷移（遷移条件）623 に記載されている「・電子署名：S_{a1} for P_a、・時刻：T₁以降」というのは、トランザクションのロック解除情報として、公開鍵 P_a に対応する電子署名 S_{a1} を有するトランザクションが、時刻 T₁ 以降に発行されたときに、状態が遷移することを意味する。

30

【0087】

キャンセルエスクロー状態 613 に関する遷移についても同様であるが、ここで、第一の資産移転フロー 610 に関する状態遷移（遷移条件）624 には、「・電子署名：S_{b2} for P_b、・秘密情報：x₂ for y₂」となっており、第二の資産移転フロー 640 に関する状態遷移（遷移条件）654 には、「・電子署名：S_{a5} for P_a、・秘密情報：x₂ for y₂」となっていることに留意する。

【0088】

これは、秘密情報 x₂ を知っているのが、ユーザ A であるとする、資産／資金 L の取引の状態をキャンセルエスクロー状態にし（すなわち、資産／資金 L の取引の状態をキャンセルにするトランザクションを発行し）、ユーザ B は、そのトランザクションによって開示された秘密情報 x₂ を知った後に、対価としての資産／資金 M の取引の状態をキャンセルエスクロー状態に（すなわち、資産／資金 M の取引の状態をキャンセルにするトランザクションを発行）できることを意味する。

40

【0089】

このようなトランザクションにおけるロック解除情報と、ロック解除条件を規定することにより、ユーザ A とユーザ B が相対取引をするとき的一方のみ資産／資金を両取りする事態が発生するのを防止することができる。

【0090】

なお、形態においては、S201 での合意結果に基づき、ユーザ A の指示によって図 1

50

0のDvP取引パターンが選択され、図6の第一の初期トランザクションテンプレート700A、図8Aの第一のパラメータテンプレート900A、図9の第一の取引状況管理情報テンプレート1000Aが、それぞれトランザクション、パラメータテーブル、取引状況管理情報テーブルとして、それぞれ作成中トランザクション記憶部124、パラメータ記憶部122、取引状況管理情報記憶部123に書き込まれたものとする。

【0091】

また、第一の初期トランザクションテンプレート600Aにおいて、ロック解除条件725に対応する値は、図10の第一のDvP取引パターンにおける状態遷移（遷移条件）622～状態遷移（遷移条件）626に対応した内容となっている。

【0092】

図11に示されるのは、取引が成立したときのDvP取引パターンであり、このときのDvP取引パターン1100は、第一の資産／資金移転フロー1110と、第二の資産移転フロー1140で表現される。これは、通常のHTLCによる取引を実現するためのDvP取引パターンである。本実施形態においては、第一の資産／資金移転フローが資産／資金Lに対応する取引の流れを表現しており。また、第二の資産／資金移転フローが資産／資金Mに対応する取引の流れを表現している。

【0093】

第一の資産移転フロー1110において、エスクロー状態1112からは、状態遷移（遷移条件）1122または状態遷移（遷移条件）1123に記載の条件を満たした場合に、終了状態1114、1115に遷移できることを意味する。

【0094】

第二の資産移転フロー640についても、データそのものは異なるものの、その意味は、第一の資産移転フロー1110と同様である。

【0095】

エスクロー状態1112に関する遷移について、第一の資産移転フロー1110に関する状態遷移（遷移条件）1122には、「・電子署名：S_{b1} for P_b、・秘密情報：x₁ for y₁」となっており、第二の資産移転フロー1140に関する状態遷移（遷移条件）1152には、「・電子署名：S_{a4} for P_a、・秘密情報：x₁ for y₁」となっていることに留意する。

【0096】

これは、秘密情報x₁を知っているのが、ユーザAであるとする、資産／資金Lの預託している状態を、解除状態にし（すなわち、資産／資金Lを取得するトランザクションを発行し）、ユーザBは、そのトランザクションによって開示された秘密情報x₁を知った後に、対価としての資産／資金Mの預託している状態を、解除状態に（すなわち、資産／資金Mを取得するトランザクションを発行）できることを意味する。

【0097】

このようなトランザクションにおけるロック解除情報と、ロック解除条件を規定することにより、ユーザAとユーザBが相対取引をするとき的一方のみ資産／資金を両取りする事態が発生するのを防止することができる。

【0098】

次に、上記で説明したデータ構造、各テンプレート、および、想定される取引パターンを前提として、図12ないし図33を用いて電子決済システムが行う処理について説明する。

【0099】

まず、図12のフローチャートの流れに従って、適宜必要な図を参照して電子決済システムにおける第一の初期トランザクション実行処理について説明する。

【0100】

第一の初期トランザクションは、ユーザAがユーザBへ引き渡す資産／資金Lをロックし確保するとともに処理条件の設定をおこなうトランザクションである。

【0101】

10

20

30

40

50

まず、取引の当事者間で、取引内容について合意する（S 2 0 1）。具体的な取引内容として、授受する資産の数量や、取引手順について合意する。このS 2 0 1のステップは、本実施形態の電子決済システムを介することなく、ユーザAとユーザBとの間で実施される処理である。

【0 1 0 2】

本実施形態では、ユーザAがユーザBに渡す資産／資金Lの数量を「5 0」とし、ユーザBがユーザAに対価として渡す資産／資金Mの数量を「3 0」とする旨について、ユーザA・B間で確認し合意したものとする。

【0 1 0 3】

S 2 0 2からS 2 0 6は、トランザクション発行装置1 1 0を介し、ユーザAによって実施されるステップである。

【0 1 0 4】

まず、トランザクション発行装置（ユーザA）1 1 0 Aは、第一の初期トランザクションに利用する資産／資金を選択する（S 2 0 2）。

【0 1 0 5】

この処理では、トランザクション発行装置（ユーザA）1 1 0 Aのトランザクション発行部1 1 3が、資産／資金決済装置アクセス部1 1 1を介し、資産／資金決済装置1 5 0が保有する資産／資金Lの台帳の情報を読み出す。さらに、ユーザAの指示に基づき、第一の初期トランザクションに関する資産を選択する。

【0 1 0 6】

以下、図1 3を用いてS 2 0 2の処理を、説明する。

トランザクション発行部1 1 3は、鍵情報記憶部1 2 1から読みだした鍵情報テーブル4 0 0のレコードのうち、システム名4 1 1が「L」、ユーザが「Me」（すなわち、「ユーザA」）であるレコードを取得し、その公開鍵4 1 4の情報である「A 0 1 2 3」を取得する。

【0 1 0 7】

さらに、トランザクション発行部1 1 3は、資産／資金決済装置アクセス部1 1 1を介し、資産／資金決済装置1 5 0の台帳記憶部1 5 4に記憶された資産／資金Lに関する台帳3 0 0を読み出す。そして、読みだした台帳3 0 0のレコードのうち、ロック解除条件3 1 3に対応する情報が1行であり、かつ、公開鍵3 1 5に対応する情報が前記「A 0 1 2 3」と一致し、かつ、ハッシュ値3 1 6および時刻3 1 7に対応する情報が空欄であるレコードを取得する。

【0 1 0 8】

さらに、トランザクション発行部1 1 3は、ユーザから必要数量の指示を受け、その取得したレコードから残高3 1 2が指示された数量以上になるようにレコードを選択する。これは、ユーザAが取引したい資産／資金Lの数量である「5 0」以上の資産／資金Lを担保するレコードを選択することを意味する。なお、レコードの選択は、残高3 1 2が指示数量以上であるレコード1件を選択するのでもよいし、残高3 1 2が指示数量未満であるレコードを複数選択し、それらの残高3 1 2の合計が指示数量以上になるようにするのでもよい。

【0 1 0 9】

なお、取得されたレコードの残高3 1 2の合計が指示数量未満であった場合には（S 2 1 0：YES）、取引が不可能であることから、図1 2に示された電子決済システムにおける第一の初期トランザクション実行処理を終了する。

【0 1 1 0】

本実施形態においては、ユーザAは、S 2 0 1で合意した資産／資金Lの取引数量である「5 0」を指示し、トランザクション発行部1 1 3は、資産／資金ID 3 1 1に対応する値が「L 0 0 0 1」であるレコードを選択したものとする。

【0 1 1 1】

次に、トランザクション発行装置（ユーザA）1 1 0 Aは、D v P取引パターンを選択

10

20

30

40

50

する（S 2 0 3）。

【0 1 1 2】

この処理では、トランザクション発行装置（ユーザ A）1 1 0 A のトランザクション発行部 1 1 3 が、共有領域アクセス部 1 1 2 を介し、共有領域 1 8 0 に格納された D v P 取引パターンを取得する。さらに、ユーザ A の指示に基づき、ユーザ A が取引しようとする D v P 取引パターンを選択する。なお、D v P 取引パターンは、初期トランザクションテンプレート、初期トランザクション実行結果テンプレート、パラメータテンプレート、取引状況管理情報テンプレートによって表現され、それぞれの可変な値を埋めることにより実現される。

【0 1 1 3】

さらに、トランザクション発行部 1 1 3 は、読み出した D v P 取引パターンの初期トランザクションテンプレート 7 0 0 のうち、第一の初期トランザクションテンプレート 7 0 0 A を、作成中トランザクション記憶部 1 2 4 に書き込む。また、読み出した D v P 取引パターンのパラメータテンプレート 9 0 0 のうち、第一のパラメータテンプレート 9 0 0 A を、パラメータ記憶部 1 2 2 に書き込む。また、読み出した D v P 取引パターンの取引状況管理情報テンプレート 1 0 0 0 のうち、第一の取引状況管理情報テンプレート 1 0 0 0 A を、取引状況管理情報記憶部 1 2 3 に書き込む。

【0 1 1 4】

次に、トランザクション発行装置（ユーザ A）1 1 0 A は、トランザクション作成に必要なパラメータを取得する（S 2 0 4）。

【0 1 1 5】

トランザクション発行装置（ユーザ A）1 1 0 A のトランザクション発行部 1 1 3 は、鍵情報記憶部 1 2 1 の情報を参照するとともに、追加で必要な情報を生成し、その結果をパラメータとしてパラメータ記憶部 1 2 2 に書き込む。

【0 1 1 6】

以下、図 1 4 A および図 1 4 B を用いてこの S 2 0 4 の処理を説明する。

【0 1 1 7】

図 1 4 A に示されるように、第一のシステム名、第二のシステム名については、S 2 0 1 の合意結果に基づき、それぞれ「L」「M」を入力する。区分 9 2 3 が「公開鍵」、取得手段 9 2 4 が「参照」であるレコードの値 9 2 5 については、鍵情報テーブル 4 0 0 から対応する情報を読み出し、書き込む。

【0 1 1 8】

次に、図 1 4 B に示されるように、区分 9 2 3 が「秘密情報」、取得手段が「作成」であるレコードの値 9 2 5 については、ランダムな数値を生成し書き込む。また、区分 9 2 3 が「ハッシュ値」、取得手段が「作成」であるレコードの値 9 2 5 については、対応する「秘密情報」を入力とし、既定のハッシュ関数の出力結果を書き込む。図 1 4 B に示される例では、秘密情報 x_1 として、ランダムに生成された値である「3 4 5 6」が書き込まれ、それに対応するハッシュ値 y_1 として、「3 a 4 b 5 c 6 d」が書き込まれている。時刻については、システムクロックを参照し、取引により規定された一定のタイムアウト時間を、現在時刻に足した時刻を算出して書き込む。

【0 1 1 9】

書き込みが完了したパラメータテンプレートは、パラメータテーブルとしてパラメータ記憶部 1 2 2 に書き込まれる。

【0 1 2 0】

次に、トランザクション発行装置（ユーザ A）1 1 0 A は、トランザクションを作成し送信する（S 2 0 5）。

【0 1 2 1】

この処理では、トランザクション発行装置（ユーザ A）1 1 0 A のトランザクション発行部 1 1 3 が、作成中トランザクション記憶部 1 2 4 から読み出したトランザクションを、鍵情報記憶部から読み出した鍵情報、および、パラメータ記憶部から読み出したパラメ

10

20

30

40

50

ータで補完し完成させた上で、資産／資金決済装置アクセス部 1 1 1 を介し、資産／資金決済装置 1 5 0 L に送信する。

【0 1 2 2】

送信されたトランザクションは、資産／資金決済装置 1 5 0 L のトランザクション受信部 1 5 1 によって、実行前トランザクション記憶部 1 5 6 に記憶された後、順次、トランザクション実行可否判定部 1 5 2 により、実行可否を判定される。トランザクション実行可否判定部によって実行可能と判断されたトランザクションは、トランザクション実行部 1 5 3 によって、台帳記憶部 1 5 4 の台帳 3 0 0 に反映されるとともに、実行済トランザクション記憶部 1 5 5 に書き込まれる。そして、その結果は、トランザクション発行装置 1 1 0 A に通知される。

10

【0 1 2 3】

以下、図 1 5 A および図 1 5 B を用いて本実施形態における第一の初期トランザクション作成処理を説明する。

【0 1 2 4】

図 1 5 A に示されるように、S 2 0 3 で取得した初期トランザクションテンプレート 7 0 0 A のデータのうち、トランザクション ID 7 2 1 に対応する値について、ユニークな値、資産／資金 ID 7 2 2 に対応する値について、S 2 0 2 で選択したレコードの資産／資金 ID 3 1 1 の値、金額 7 2 3 に対応する値は、S 2 0 1 の合意結果である数量「5 0」を、それぞれ書き込む。

【0 1 2 5】

20

次に、図 1 5 B に示されるように、初期トランザクションテンプレート 7 0 0 A のデータのうち、ロック解除条件 7 2 5 のデータを、パラメータ記憶部 1 2 2 から読み出したパラメータテーブルを参照し、対応するデータを反映する。

【0 1 2 6】

次に、電子署名 7 2 4 に対応する値については、鍵情報テーブル 4 0 0 に保持された秘密鍵 4 1 3 に対応する値を利用して、作成した電子署名を書き込む。この電子署名の平文データは、例えば、この初期トランザクションテンプレート 7 0 0 A より生成される初期トランザクションレコードのトランザクション ID 7 2 1、資産／資金 ID 7 2 2、金額 7 2 3、ロック解除条件 7 2 5 のバイナリデータとし、これをユーザ A の所持する秘密鍵によって、ハッシュ値を取り、暗号化することによって、電子署名を生成し、それを検証する者は、その秘密鍵に対応する公開鍵によって検証することができる。

30

【0 1 2 7】

次に、図 1 6 を用いて第一の初期トランザクションの実行可否を判定する処理について説明する。

資産／資金決済装置 1 5 0 L のトランザクション実行可否判定部 1 5 2 は、実行前トランザクション記憶部 1 5 6 からトランザクションを 1 件読み込み、記載された資産／資金 ID 7 2 2 のデータに対応するレコードを、台帳記憶部 1 5 4 から読み出す。さらに、残高 3 1 2 の数値がトランザクションの金額 7 2 3 の数値以上であること（取引をするユーザ A が指定された資産／資金を保有していること）、また、ロック解除条件 3 1 3 の内容がトランザクションのロック解除情報 7 2 4 の内容で満たされていることを確認する。ここでは、ロック解除条件 3 1 3 に対応するデータは「公開鍵 A 0 1 2 3 に対応する電子署名があること」のみであることから、トランザクション実行可否判定部 1 5 2 は、トランザクションに記載の電子署名 7 2 0 のデータを読み出した公開鍵で検証することにより、トランザクションの実行可否を判定する。すなわち、トランザクション実行可否判定部 1 5 2 は、電子署名を公開鍵で復号化した値と、そのレコードのトランザクション ID 7 2 1、資産／資金 ID 7 2 2、金額 7 2 3、ロック解除条件 7 2 5 のバイナリデータのハッシュ値が一致するか否かを検証する。実行可能と判定された場合には、当該トランザクションをトランザクション実行部 1 5 3 に引き渡す。

40

【0 1 2 8】

次に、図 1 7 を用いて本実施形態における第一の初期トランザクションの実行処理につ

50

いて説明する。

資産／資金決済装置 150L のトランザクション実行部 153 は、トランザクション実行可否判定部 152 から引き渡されたトランザクションの内容を台帳へ反映する。

【0129】

台帳 300 のレコードのうち、トランザクションに記載の資産／資金 ID 722 のデータと同一の資産／資金 ID 311 のデータを有するレコードを取得する。そして、取得したレコードにおいて、ロック解除条件 313 のデータが 1 行である場合には、以下の処理をおこなう。

【0130】

まず、取得したレコードについて、残高 312 の金額を、トランザクションの金額 723 に記載の数値で減算する（図 17 では、「L005」のレコードの残高は、0 になった）。その後、台帳 300 に新規レコードを作成し追加する。追加したレコードについて、資産／資金 ID 311 のデータは、ユニークな値（図 17 では、「L0005」）を生成し書き込む。残高 312 のデータは、トランザクションの金額 723 に記載の数値を転記する。ロック解除条件 313 については、トランザクションのロック解除条件 725 の内容を転記する。処理が完了したら、トランザクションを実行済トランザクション記憶部 155 に書き込むとともに、作成された台帳の資産／資金 ID 312 の情報をトランザクション発行装置 110A に通知する。

【0131】

なお、取得したレコードにおいて、ロック解除条件 313 のデータが複数行である場合の動作については、後述する。

【0132】

次に、トランザクション発行装置 110A は、取引状況を更新する（S206）。

この処理では、トランザクション発行装置 110A の取引状況管理部 114 が、資産／資金決済装置 アクセス部 111 を介し、資産／資金決済装置 150L から通知された結果に基づき、パラメータ記憶部 122 が保持するパラメータテーブル、および、取引状況管理情報記憶部 123 が保持する取引状況管理情報テーブルを更新する。

【0133】

以下、図 18 を用いて本実施形態における第一の初期トランザクションの実行結果による取引状況を更新する処理を説明する。

トランザクション発行装置 110A の取引状況管理部 114 は、資産／資金決済装置 アクセス部 111 を介し、トランザクション実行結果として、台帳に作成されたレコードの資産／資金 ID 「L0005」を受信する。さらに、パラメータ記憶部 122 からパラメータテーブルを読み出し、第一の資産／資金 ID として「L0005」を書き込む。さらに、取引状況管理情報記憶部 123 から取引管理情報テーブルを読み出し、第一の資産／資金 ID として「L0005」を書き込む。

【0134】

次に、図 19 のフローチャートの流れに従って、適宜必要な図を参照して電子決済システムにおける第二の初期トランザクション実行処理について説明する。

【0135】

第二の初期トランザクションは、ユーザ B がユーザ A へ引き渡す資産／資金 M をロックし確保するとともに処理条件の設定をおこなうためのトランザクションである。

【0136】

まず、取引の同時者間で、取引状況について情報共有を行う（S1901）。具体的には、ユーザ A がトランザクションを実行した結果として、台帳に資産／資金 ID 「L0005」のレコードが追加されていることについて、ユーザ B と情報共有する。

【0137】

この S1901 のステップは、本実施形態の電子決済システムを介することなく、ユーザ A とユーザ B との間で実施される処理である。

【0138】

S 1 9 0 2 から S 1 9 0 8 は、ユーザ B によってトランザクション発行装置 1 1 0 B が実行する処理である。

【0 1 3 9】

まず、トランザクション発行装置 1 1 0 B は、第二の初期トランザクションに利用する資産／資金を選択する（S 1 9 0 2）。

【0 1 4 0】

以下、図 2 0 を用いて本実施形態の第二の初期トランザクションに利用する資産／資金を選択する処理について説明する。

【0 1 4 1】

トランザクション発行装置 1 1 0 B のトランザクション発行部 1 1 3 は、鍵情報記憶部 1 2 1 から読みだした鍵情報テーブル 4 0 0 のレコードのうち、システム名 4 1 1 が「M」、ユーザが「Me」（ユーザ B）であるレコードを取得し、その公開鍵 4 1 4 の情報である「B 0 9 8 7」を取得する。

【0 1 4 2】

さらに、トランザクション発行部 1 1 3 は、資産／資金決済装置アクセス部 1 1 1 を介し、資産／資金決済装置 1 5 0 の台帳記憶部 1 5 4 から、資産／資金 L に関する台帳 3 0 0 を読み出す。読みだした台帳 3 0 0 のレコードのうち、ロック解除条件 3 1 3 に対応する情報が 1 行であり、かつ、公開鍵 3 1 5 に対応する情報が読み出した「B 0 9 8 7」と一致し、かつ、ハッシュ値 3 1 6 および時刻 3 1 7 に対応する情報が空欄であるレコードを取得する。

【0 1 4 3】

さらに、トランザクション発行部 1 1 3 は、ユーザから必要数量の指示を受け、取得したレコードから残高 3 1 2 が指示された数量以上になる（取引をするユーザ B が指定された資産／資金を保有している）ようにレコードを選択する。なお、レコードの選択は、残高 3 1 2 が指示数量以上であるレコード 1 件を選択するのでもよいし、残高 3 1 2 が指示数量未満であるレコードを複数選択し、それらの残高 3 1 2 の合計が指示数量以上になるようにするのでもよい。

【0 1 4 4】

なお、取得されたレコードの残高 3 1 2 の合計が指示数量未満であった場合には、取引が不可能であることから、図 1 9 に示された第二の初期トランザクション実行処理を終了する。

【0 1 4 5】

本実施形態においては、ユーザ B は、S 2 0 1 で合意した資産／資金 M の取引数量である「3 0」を指示し、トランザクション発行部 1 1 3 は、資産／資金 I D 3 1 1 に対応する値が「M 0 0 0 4」であるレコードを選択したものとする。

【0 1 4 6】

次に、トランザクション発行装置 1 1 0 B は、D v P 取引パターンを選択する（S 1 9 0 3）。

【0 1 4 7】

この処理では、トランザクション発行装置 1 1 0 B のトランザクション発行部 1 1 3 が、共有領域アクセス部 1 1 2 を介し、共有領域 1 8 0 に格納された D v P 取引パターンを取得し、さらに、ユーザ B の指示に基づき、D v P 取引パターンを選択する。

【0 1 4 8】

さらに、トランザクション発行部 1 1 3 は、読み出した D v P 取引パターンの初期トランザクションテンプレートのうち、第二の初期トランザクションテンプレート 7 0 0 B を、作成中トランザクション記憶部 1 2 4 に書き込む。また、読みだした D v P 取引パターンのパラメータテンプレートのうち、第二のパラメータテンプレート 9 0 0 B を、パラメータ記憶部 1 2 2 に書き込む。また、読みだした D v P 取引パターンの取引状況管理情報テンプレートのうち、第二の取引状況管理情報テンプレート 1 0 0 0 B を、取引状況管理情報記憶部 1 2 3 に書き込む。

【0149】

本実施形態においては、S201での合意結果に基づき、ユーザBの指示によって図10のDvP取引パターンの資産移転フロー640が選択され、図7の第二の初期トランザクションテンプレート700B、図8Bの第二のパラメータテンプレート900B、図9の第二の取引状況管理情報テンプレート1000Bが、それぞれトランザクション、パラメータテーブル、取引状況管理情報テーブルとして、それぞれ作成中トランザクション記憶部124、パラメータ記憶部122、取引状況管理情報記憶部123に書き込まれたものとする。

【0150】

次に、トランザクション発行装置110Bは、トランザクション作成に必要なパラメータを取得あるいは作成する（前半：S1904）。

10

【0151】

この処理では、トランザクション発行装置110Bのトランザクション発行部113が、鍵情報記憶部121の鍵情報テーブルを参照するとともに、必要な情報をパラメータ記憶部122によりパラメータテーブルに書き込む。

【0152】

以下、図21Aを用いて本実施形態におけるトランザクション作成に必要なパラメータを取得あるいは作成する処理の前半について説明する（後半は、図21Bにより後に説明）。

【0153】

20

第一のシステム名、第二のシステム名については、図12のS201の合意結果に基づき、それぞれ「L」「M」を入力する。第一の資産／資金IDについては、S1901で通知された「L0005」を入力する。また、区分923が「公開鍵」、取得手段924が「参照」であるレコードの値925については、鍵情報テーブル400から対応する情報を読み出し、書き込む。

【0154】

次に、トランザクション発行装置110Bは、ユーザAによる資産／資金Lのトランザクション実行結果を検証する（S1905）。

【0155】

この処理は、トランザクション発行装置110Bのトランザクション発行部113が、S1903で読み出したDvP取引パターンの第一の初期トランザクション実行結果テンプレート800Aを、パラメータ記憶部122から読み出したパラメータで補完する。補完した結果を、資産／資金アクセス部111を介して読み出した資産／資金管理システム150の台帳と比較することにより、トランザクションの実行結果を検証する。

30

【0156】

なお、台帳から読み出した情報と、初期トランザクション実行結果テンプレートを補完した結果との間に不一致が認められた場合には、問題ありとして（S1920：YES）、取引内容について認識の相違があり、取引継続は不可能であることから、図19に示された第二の初期トランザクション実行処理を終了する。

【0157】

40

以下、図22を用いて本実施形態における第一の初期トランザクション実行結果を検証する処理を説明する。

S1903で読み出したDvP取引パターンの、第一の初期トランザクション実行結果テンプレート800Aのうち、資産／資金ID821および残高822を、図12のS201で合意した内容に基づき、補完する。さらに、ロック解除条件823に記載の変数名を、パラメータ記憶部122から読み出したパラメータで補完する。補完が完了した第一の初期トランザクション実行結果テンプレート800Aと、台帳から読み出した対応するレコードの内容とを比較し一致することを確認する。

【0158】

なお、ロック解除条件823のうち、対応するパラメータを補完できなかった部分につ

50

いては、比較検証をスキップする。図 2 2 においては、初期トランザクション実行結果テンプレート 8 0 0 A のハッシュ値 8 2 6 および時刻 8 2 7 のデータについて補完できていないものがあることから、台帳のハッシュ値 3 1 6 および時刻 3 1 7 について、対応するデータの検証はスキップされる。

【0 1 5 9】

次に、トランザクション発行装置 1 1 0 B は、トランザクション作成に必要なパラメータを取得あるいは作成する（後半：S 1 9 0 4）。

【0 1 6 0】

この処理は、トランザクション発行装置 1 1 0 B が、資産／資金決済装置アクセス部 1 1 1 を介して台帳から読み出した情報を利用し、パラメータ記憶部 1 2 2 から読み出したパラメータを補完する処理である。

10

【0 1 6 1】

以下、図 2 1 B を用いて本実施形態におけるトランザクション作成に必要なパラメータを取得あるいは作成する処理の後半について説明する（前半は、図 2 1 A により既に説明した）。

【0 1 6 2】

区分 9 2 3 が「ハッシュ値」あるいは「時刻」、かつ、取得手段 9 2 4 が「参照」であるレコードの値 9 2 5 について、第一の初期トランザクション実行結果テンプレート 8 0 0 B のロック解除条件 8 2 3 に記載の変数名を踏まえ、台帳の対応するレコードのロック解除条件のうち対応する値を抽出し、反映する。また、区分「9 2 3」が「時刻」、かつ、取得手段 9 2 4 が「作成」であるレコードについては、適切な値を入力する。

20

【0 1 6 3】

なお、パラメータについて、区分 9 2 3 が「秘密情報」、かつ、取得手段 9 2 4 が「参照」であるレコードについては、本ステップの時点では値を取得することができないため、空欄となる。

【0 1 6 4】

次に、トランザクション発行装置 1 1 0 B は、トランザクションを作成し送信する（S 1 9 0 7）。

【0 1 6 5】

この処理は、トランザクション発行装置 1 1 0 B のトランザクション発行部 1 1 3 が、作成中トランザクション記憶部 1 2 4 から読み出したトランザクションを、鍵情報記憶部から読み出した鍵情報テーブル、パラメータ記憶部から読み出したパラメータで補完し完成させた上で、資産／資金決済装置アクセス部 1 1 1 を介し、資産／資金決済装置 1 5 0 に送信する。送信されたトランザクションは、資産／資金決済装置 1 5 0 の中で処理され、結果は、台帳記憶部 1 5 4 の台帳に反映されるとともに、トランザクション発行装置 1 1 0 B に通知される。

30

【0 1 6 6】

以下、図 2 3 を用いて本実施形態における第二の初期トランザクションの実行処理を説明する。

本実施形態における第二の初期トランザクションの実行処理は、図 1 7 の第一の初期トランザクションの実行処理と同様である。

40

【0 1 6 7】

ここでは、資産／資金 M に関するものであることから、資産／資金 I D や残高などが異なっている。

【0 1 6 8】

次に、トランザクション発行装置 1 1 0 B は、取引状況を更新する（S 1 9 0 8）。

【0 1 6 9】

この処理は、トランザクション発行装置 1 1 0 B の取引状況管理部 1 1 4 が、資産／資金決済装置アクセス部 1 1 1 を介し、資産／資金決済装置 1 5 0 M から通知された結果に基づき、パラメータ記憶部 1 2 2 が保持するパラメータ、および、取引状況管理情報記憶

50

部 1 2 3 が保持する取引状況管理情報テーブルを更新する。

【0 1 7 0】

以下、図 2 4 を用いて本実施形態における第二の初期トランザクションの実行結果により取引状況を更新する処理を説明する。

【0 1 7 1】

トランザクション発行装置 1 1 0 B の取引状況管理部 1 1 4 は、資産／資金決済装置アクセス部 1 1 1 を介し、トランザクション実行結果として、台帳 3 0 0 に作成されたレコードの資産／資金 ID 「M 0 0 0 8」を受信する。さらに、パラメータ記憶部 1 2 2 からパラメータを読み出し、第二の資産／資金 ID として「M 0 0 0 8」を書き込む。また、取引状況管理情報記憶部 1 2 3 から取引管理情報テーブルを読み出し、第二の資産／資金 ID として「M 0 0 0 8」を書き込む。

10

【0 1 7 2】

次に、取引の同時者間で、取引状況について共有する（S 1 9 0 9）。具体的には、ユーザ B がトランザクションを実行した結果として、台帳に資産／資金 ID 「M 0 0 0 8」のレコードが追加されていることについて、ユーザ A に伝える。

【0 1 7 3】

この S 1 9 0 9 の処理は、本実施形態の電子決済システムを介することなく、ユーザ A とユーザ B との間で実施されるステップである。

【0 1 7 4】

次に、トランザクション発行装置 1 1 0 A は、ユーザ B による資産／資金 M のトランザクション実行結果を検証する（S 1 9 1 0）。

20

【0 1 7 5】

この S 1 9 1 0 の処理は、ユーザ A によってトランザクション発行装置 1 1 0 A が、実行する処理である。

【0 1 7 6】

この処理では、トランザクション発行装置 1 1 0 A が、S 2 0 3 で読み出した D v P 取引パターンの、第二の初期トランザクション実行結果テンプレート 8 0 0 B を、パラメータ記憶部 1 2 2 から読み出したパラメータで補完し、補完した結果を、資産／資金アクセス部を介して読み出した資産／資金管理システム 1 6 0 の台帳と比較することで、トランザクションの実行結果を検証する。

30

【0 1 7 7】

なお、台帳から読み出した情報と、初期トランザクション実行結果テンプレートを補完した結果との間に不一致が認められた場合には、取引内容について認識の相違があり、取引継続は不可能であることから、ユーザ A は、取引状況管理情報記憶部 1 2 3 の取引管理情報を編集することにより、第一の初期トランザクションに係る資産／資金 L を引き戻すよう設定する（図示せず）。

【0 1 7 8】

以下、図 2 5 A ないし図 2 5 C を用いて本実施形態における第二の初期トランザクションの実行結果を検証する処理を説明する。

【0 1 7 9】

第二の初期トランザクションの実行結果を検証する処理では、S 2 0 3 で読み出した D v P 取引パターンの、第二の初期トランザクション実行結果テンプレート 8 0 0 A のうち、図 2 5 A に示されるように、資産／資金 ID 8 2 1 および残高 8 2 2 を、図 1 2 の S 2 0 1 で合意した内容に基づき、補完する。さらに、ロック解除条件 8 2 3 に記載の変数名を、パラメータ記憶部 1 2 2 から読み出したパラメータで補完する。そして、トランザクション発行装置 1 1 0 A は、補完が完了した第二の初期トランザクション実行結果テンプレート 8 0 0 A と、台帳から読み出した対応するレコードの内容とを比較し一致することを確認する。

40

【0 1 8 0】

次に、トランザクション発行装置 1 1 0 A は、パラメータ記憶部 1 2 2 のパラメータテ

50

ーブルの第二の資産／資金ID927に、「M0008」を書き込む。

【0181】

また、取引状況管理情報記憶部123の取引状況管理情報テーブルの第二の資産／資金ID1021に、「M0008」を書き込む。

【0182】

次に、トランザクション発行装置110Aは、検証の結果、問題があった場合には、図25Cに示されるように、取引状況管理情報記憶部123から取引管理情報テーブルを読み出し、区分1024が「成立」であるレコードを削除する。

【0183】

次に、図26のフローチャートの流れに従って、適宜必要な図を参照して電子決済システムにおける通常トランザクション実行処理について説明する。

S2901は、ユーザBが実行するステップである。

また、S2910、S2902、S2903、S2920、S2930、S2905、S2906の処理は、トランザクション発行装置110Aまたはトランザクション発行装置110により、独立に実行されるステップである。

【0184】

以降、本実施形態では、トランザクション発行装置110Bで実行されるケースを念頭に、これらのステップについて説明する。

【0185】

まず、トランザクション発行装置110Bは、取引状況管理情報記憶部123に格納された取引状況管理情報テーブルを表示し、ユーザBは、トランザクションの実行を検討する取引案件を選択する(S2901)。

【0186】

取引状況管理情報テーブルの全案件が終了している場合には(S2910:YES)、図26に示された通常トランザクション実行処理を終了し、取引状況管理情報が追加され次第、再度、通常トランザクション実行処理を開始する。

【0187】

以下、図27を用いて取引状況管理情報テーブルから取引案件を選択する処理について説明する。

本実施形態においては、第一の資産／資金IDが「L0005」、第二の資産／資金IDが「M0008」である取引状況管理情報テーブルの案件が選択されたものとする。

【0188】

次に、トランザクション発行装置110Bは、パラメータ記憶部122が保持するパラメータのうち、秘密情報を更新する(S2902)。

【0189】

この処理では、トランザクション発行装置110Bの取引状況管理部114は、資産／資金決済装置アクセス部111を介し、資産／資金管理システム150、160の実行済トランザクション記憶部155、165が保持するトランザクションを読み出す。さらに、S2901で選択した取引状況管理情報テーブルの第一の資産／資金IDもしくは第二の資産／資金IDに一致する資産／資金IDを有するトランザクションを、読み出したトランザクションから抽出する。

【0190】

並行して、パラメータ記憶部122から、S2901で選択した取引状況管理情報テーブルの第一の資産／資金IDおよび第二の資産／資金IDを有するパラメータを抽出する。

【0191】

抽出したトランザクションの秘密情報727が、抽出したパラメータのハッシュ値と対応関係にある場合には、当該ハッシュ値に対応する秘密情報のデータとして、秘密情報727のデータをパラメータテーブルに書き込む。

【0192】

以下、図28を用いて本実施形態の秘密情報を更新する処理について説明する。

10

20

30

40

50

トランザクション発行装置 110B は、実行済トランザクション記憶部が保持するトランザクションのうち、「L0005」または「M0008」を資産／資金ID722の値として有するトランザクションを抽出する。

【0193】

ここで、抽出されたトランザクションの秘密情報727である「3456」が、パラメータのレコードのうち、区分923が「ハッシュ値」であるレコードの値925の「3A4B5c6d」（既に初期実行結果テンプレート800Aより値を設定済み、図21B参照）と、ハッシュ関数における入出力値の関係にある（ハッシュ関数を、Hashとすると、 $y_1 = \text{Hash}(x_1)$ である）ことから、そのレコードと対応関係にある区分923が「秘密情報」であるレコードの値925として、「3456」を書き込む。

10

【0194】

次に、トランザクション発行装置 110B は、S2901で選択した取引状況管理情報が示す案件について、実行可否を判定する（S2603）。

【0195】

以下、図29を用いてS2901で選択した取引状況管理情報が示す案件について、実行可否を判定する処理について説明する。

S2901で選択した取引状況管理情報テーブルのレコードのうち、1行を選択する。さらに、選択したレコードに対応する資産／資金IDおよびロック解除条件を有するレコードを、資産／資金決済装置アクセス部111を介し、資産／資金管理システムの台帳記憶部154の台帳300から取得する。さらに、パラメータ記憶部から読み出したパラメータと台帳のロック解除条件とを比較することで、トランザクションの実行可能性を確認する。図29では、ロック解除条件のハッシュ値「3A4B5c6d」に対応する秘密情報「3456」がパラメータに載っていることから、トランザクションが実行可能と判断できる。

20

【0196】

当該処理を、S2901で選択した取引状況管理情報の全レコードについて実施することで、選択された案件の実行可否を判定することができる。

【0197】

次に、ユーザBは、S2903で実行可能と判定されたトランザクションについて、実行要否を判断する（S2904）。

30

【0198】

本実施形態においては、取引状況管理情報テーブルのレコードのうち、項番1022が「1, -」と、「3, -」であるレコードに対応するトランザクションを実行すると判断するものとする。

【0199】

なお、取引状況管理情報テーブルのレコードのうち、至急フラグ1023が空でないもの（図では「●」であるもの）については、ユーザの判断を介することなく、機械的に実行要と判断する。

【0200】

次に、トランザクション発行装置 110B は、S2904で実行要と判断されたトランザクションを作成し実行する（S2905）。

40

【0201】

以下、図30および図31を用いてトランザクションの実行処理を説明する。

【0202】

図30は、取引が成立した場合の一連のトランザクションと台帳の様子示している。

ここで、ユーザBが、取引状況管理情報テーブルのレコードのうち、項番1022が「1, -」の取引を選択したものとする。

【0203】

資産／資金決済装置 150L のトランザクション実行部 153 は、トランザクションの資産／資金722およびロック解除情報724に対応する資産／資金ID311およびロ

50

ック解除条件 3 1 3 を有するレコードを、台帳記憶部 1 5 4 が保持する台帳 3 0 0 から抽出する。さらに、抽出したレコードのロック解除条件 3 1 3 が、トランザクションのロック解除情報 7 2 4 で満たされていること（電子署名が公開鍵で正当であり、秘密情報のハッシュ値が対応していること）を確認した上で、台帳 3 0 0 を更新する。

【0 2 0 4】

具体的な更新方法として、更新前のロック解除条件 3 1 3 において、後続するレコードが存在しない場合には、新規の資産／資金 ID のレコードを追加し、残高 3 1 2 に更新前の残高 3 1 2 の値を、ロック解除条件 3 1 3 にトランザクションのロック解除条件 7 2 5 の情報を、それぞれ記載する。また、更新前の資産／資金 ID のレコードについては、残高 3 1 2 をゼロに、ロック解除条件 3 1 3 を空値に、それぞれ更新する（図 3 0 の台帳（トランザクション実行後））。

10

【0 2 0 5】

次に、ユーザ B が、取引状況管理情報テーブルのレコードのうち、項番 1 0 2 2 が「3，－」の取引を選択したものとする。

【0 2 0 6】

図 3 1 は、取引が成立しなかった場合のトランザクションと台帳の様子を示している。

資産／資金決済装置 1 5 0 L のトランザクション実行部 1 5 3 は、トランザクションの資産／資金 7 2 2 およびロック解除情報 7 2 4 に対応する資産／資金 ID 3 1 1 およびロック解除条件 3 1 3 を有するレコードを、台帳記憶部 1 5 4 が保持する台帳 3 0 0 から抽出する。

20

【0 2 0 7】

図 4 で説明したように、項番の条件として、「3，－」の条件後、「3，1」の条件または、「3，－」の条件後、「3，2」の条件であるようにトランザクションの実行が規定されている。

【0 2 0 8】

このときには、「3，－」に対応するトランザクションを実行されたときには、図 3 1 に示されるように、「3，－」、「3，1」、「3，2」の台帳のロック解除条件 3 1 3 を、「3，1」、「3，2」の台帳のロック解除条件 3 1 3 に置き換える。

【0 2 0 9】

これにより、資産／資金 ID が「L 0 0 0 5」のトランザクションとして、「3，－」のトランザクション実行後に、「3，1」、「3，2」に対応する資産／資金 ID が「L 0 0 0 5」のトランザクションが実行されることが担保される。

30

【0 2 1 0】

次に、トランザクション発行装置 1 1 0 B は、取引管理情報を更新する（S 2 9 0 6）。

【0 2 1 1】

トランザクション発行装置 1 1 0 B の取引状況管理部 1 1 4 は、S 2 9 0 1 で読み出した取引状況管理情報から、資産／資金 ID を読み出す。読み出した各資産／資金 ID について、対応する資産／資金 ID を有する台帳のレコードを、資産／資金決済装置 1 5 0 L の資産／資金決済装置アクセス部 1 1 1 を介し、取得する。取得したレコードにおいて、残高 3 1 2 の値が「0」であった場合には、取引状況管理情報のレコードのうち、当該資産／資金 ID を有するレコードを削除する。

40

【0 2 1 2】

以上、S 2 9 0 1 から S 2 9 0 6 を繰り返すことで、順次台帳を更新し、資産／資金 L および資産／資金 M の移転を実施する。

【0 2 1 3】

次に、図 3 2 および図 3 3 を用いて本実施形態における D v P 取引における取引の全体の一連のトランザクションと台帳の様子について説明する。

【0 2 1 4】

まず、図 3 2 を用いて D v P 取引が成立した場合の取引の全体の一連のトランザクションと台帳の様子について説明する。

50

図12に示した電子決済システムにおける第一の初期トランザクション実行処理、図19に示した電子決済システムにおける第二の初期トランザクション実行処理の一連の処理の結果、それぞれ台帳レコード3501、3502が、それぞれ資産／資金決済装置150L、資産／資金決済装置150Mの台帳記憶部154に記憶されている。その後、ユーザAのトランザクション発行装置110が保持する情報（パラメータテーブルと鍵情報テーブルによる）3503を利用し、トランザクション3504を作成し送信する。

【0215】

一方、資産／資金決済装置150Mがトランザクション3504を処理した結果、台帳が台帳レコード3505の通り更新されるとともに、実行済トランザクションの情報から、ユーザBのトランザクション発行装置110Bが保持する情報3506が更新される。トランザクション発行装置が保持する情報3506が更新された結果、ユーザBがトランザクション3507を発行できるようになり、台帳が台帳レコード3508の通り更新される。

【0216】

台帳レコード3505は、ユーザAの電子署名によって移転できる、すなわち、ユーザAが保有する資産／資金Mである。また、台帳レコード3508は、ユーザBの電子署名によって移転できる、すなわち、ユーザBが保有する資産／資金Lである。

【0217】

次に、図33を用いて取引が成立しなかった場合の取引の全体の一連のトランザクションと台帳の様子について説明する。

基本的な処理の流れの考え方は、図32で示したDvP取引が成立した場合の取引と同様である。

【0218】

ここで、台帳レコード3601、台帳レコード3602がエスクロー状態であり、台帳3608、台帳3605がキャンセルエスクロー状態であることに留意する。

【0219】

台帳レコード3611は、ユーザAの電子署名によって移転できる、すなわち、ユーザAが保有する資産／資金Lである。また、台帳レコード3614は、ユーザBの電子署名によって移転できる、すなわち、ユーザBが保有する資産／資金Mである。

【0220】

本実施形態に係る電子決済システムの特徴を説明すると以下ようになる。

従来の取引では、図11の取引が成立しないときのDvP取引パターンに示されるように、トランザクションの発行者（電子署名主）と資金／資産の移動先は同じものでなければならなかった（図11：エスクロー状態1112→終了状態1113における状態遷移（遷移条件）1122など）。

【0221】

本実施形態に係る電子決済システムでは、トランザクションの発行者（電子署名主）と資金／資産の移動先は異なったものでも許容される（図10：エスクロー状態612→キャンセルエスクロー状態613における状態遷移（遷移条件）624など）。

【0222】

これを実現するために、本実施形態に係る電子決済システムでは、トランザクションにロック解除条件を設け、そこに移動先（公開鍵がこれに対応する）を含めたことと、トランザクションの取引パターンとして、「3. -」、「3. 1」または「3. -」、「3. 2」のように、連続して実行しなければならない取引パターンを定義できるようにしている。

【0223】

これにより、本実施形態の電子決済システムでは、HTLCを拡張し、ロック中の資産をタイムアウトによらずに安全に引き戻す仕組みを提供している。すなわち、例えば、取引の当事者は、複数の資産／資金決済装置をまたがり、かつ、仲介者なくDvP取引する際に、取引の安全性を担保しつつも、取引不成立時における資産／資金の流動性低下を回

10

20

30

40

50

避することが可能となる。

【符号の説明】

【 0 2 2 4 】

1 0 0 …電子決済システム

1 1 0 …トランザクション発行装置

1 1 1 …資産／資金決済装置アクセス部

1 1 2 …共有領域アクセス部

1 1 3 …トランザクション発行部

1 1 4 …取引状況管理部

1 2 1 …鍵情報記憶部

1 2 2 …パラメータ記憶部

1 2 3 …取引状況管理情報記憶部

1 2 4 …作成中トランザクション記憶部

1 5 0 …資産／資金決済装置

1 5 1 …トランザクション受信部

1 5 2 …トランザクション実行可否判定部

1 5 3 …トランザクション実行部

1 5 4 …台帳記憶部

1 5 5 …実行済トランザクション記憶部

1 5 6 …実行前トランザクション記憶部

1 8 0 …共有領域

1 8 1 …D v P取引テンプレート記憶部

10

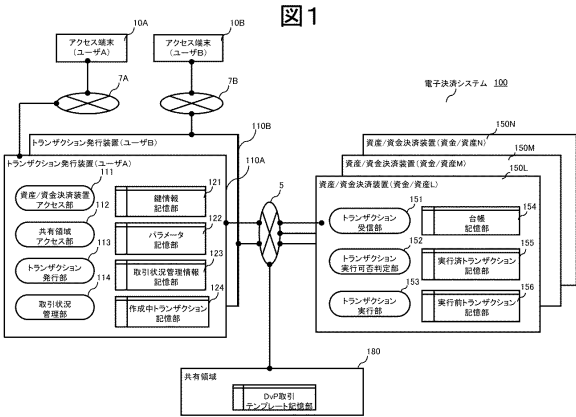
20

30

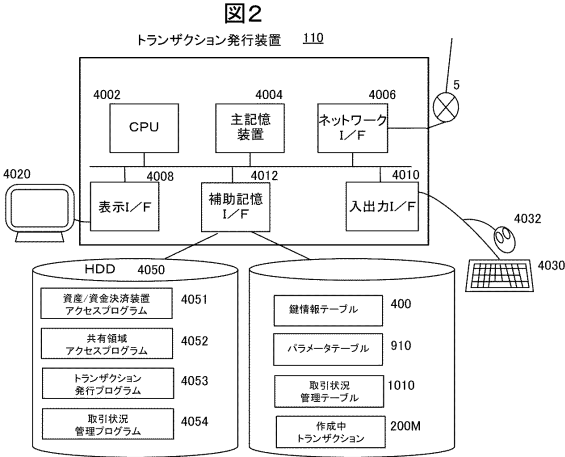
40

50

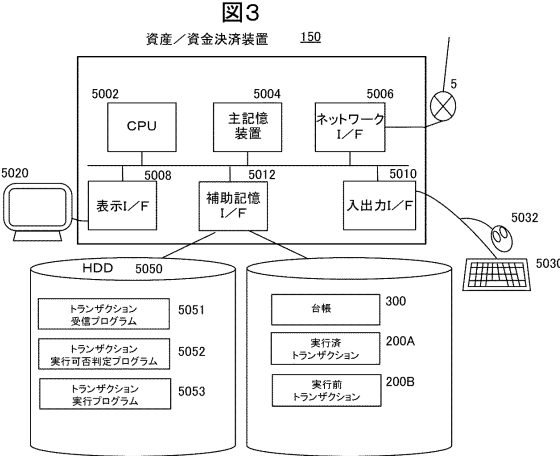
【図面】
【図 1】



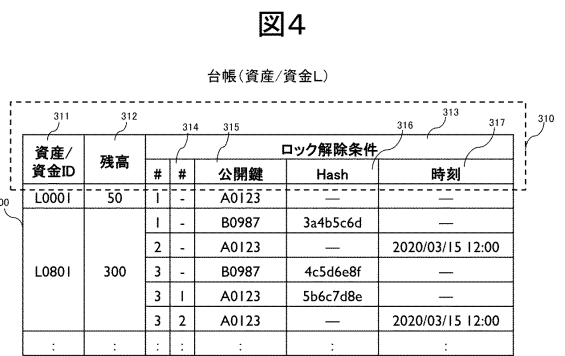
【図 2】



【図 3】



【図 4】



10

20

30

40

50

【図 5】

図5

鍵情報テーブル(ユーザA)

システム	ユーザ	秘密鍵	公開鍵
L	Me	1a2b3c0d	A0123
M	Me	1a2b3c0d	A0123
N	Me	1a2b3c0d	A0123
L	ユーザB	—	B0987
M	ユーザB	—	B0987
⋮		⋮	⋮

【図 6】

図6 初期トランザクションテンプレート 700

トランザクションID	資産/資金ID	金額	ロック解除情報		ロック解除条件		
			電子署名	秘密情報	#	#	時刻
700A					1	-	[P _a]
					2	-	[P _b]
					3	-	[P _c]
					3	1	[P _c]
700B					1	-	[P _a]
					2	-	[P _b]
					3	-	[P _c]
					3	2	[P _b]

【図 7】

図7 初期トランザクション実行結果テンプレート 800

資産/資金ID	残高	ロック解除条件				
		#	#	公開鍵	Hash	時刻
800A	*	1	-	[P _a]	[Y ₁]	—
		2	-	[P _b]	—	[T ₁]
		3	-	[P _b]	[Y ₂]	—
		3	1	[P _a]	[Y ₃]	—
800B	*	3	2	[P _a]	—	[T ₁]
		1	-	[P _a]	[Y ₁]	—
		2	-	[P _b]	—	[T ₁ -T ₂]
		3	-	[P _a]	[Y ₂]	—
800B	*	3	1	[P _b]	[Y ₃]	—
		3	2	[P _b]	—	[T ₁ -T ₂]

【図 8 A】

図8A

パラメータテンプレート 900

資産/資金1	資産/資金2	変数名	区分	取得手段	値	
					資産/資金1	資産/資金2
930	900A	P _a	公開鍵	参照		
		P _b	公開鍵	参照		
		x ₁	秘密情報			
		y ₁	ハッシュ値	作成		
		x ₂	秘密情報			
		y ₂	ハッシュ値	作成		
		x ₃	秘密情報			
		y ₃	ハッシュ値	作成		
931	900A	T ₁	時刻	作成		

10

20

30

40

50

【図 8 B】

図8B

資金/資産		変数名	区分	取得手段	値	
資産/資金1	資産/資金2				資産/資金1	資産/資金2
900B		P_a	公開鍵	参照		
		P_b	公開鍵	参照		
		x_1	秘密情報	参照		
		y_1	ハッシュ値	参照		
		x_2	秘密情報	参照		
		y_2	ハッシュ値	参照		
		x_3	秘密情報	参照		
		y_3	ハッシュ値	参照		
		T_1	時刻	参照		
		T_2	時刻	作成		

【図 9】

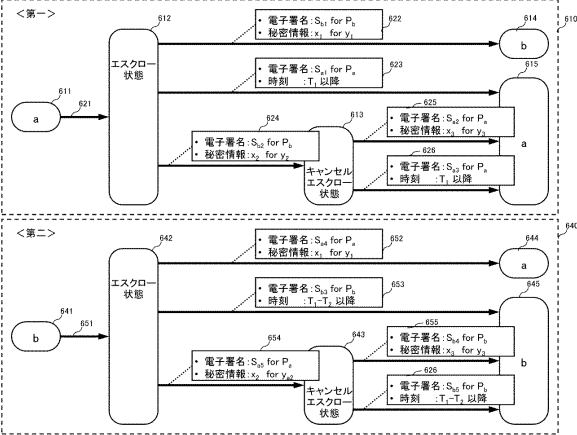
図9

取引状況管理情報テンプレート					1000
1021	1022	1023	1024	1020	
資金/資産	#	#	急	区分	
1030	2	-	●	不成立	
	3	1		不成立	
	3	2	●	不成立	
1031	1	-	●	成立	
	3	-	-	不成立	
1000A					

資金/資産	#	#	急	区分
	1	-	●	成立
	3	-	-	不成立
	2	-	●	不成立
	3	1		不成立
	3	2	●	不成立

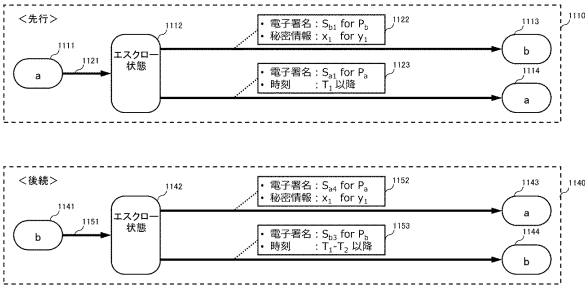
【図 1 0】

図10



【図 1 1】

図11



10

20

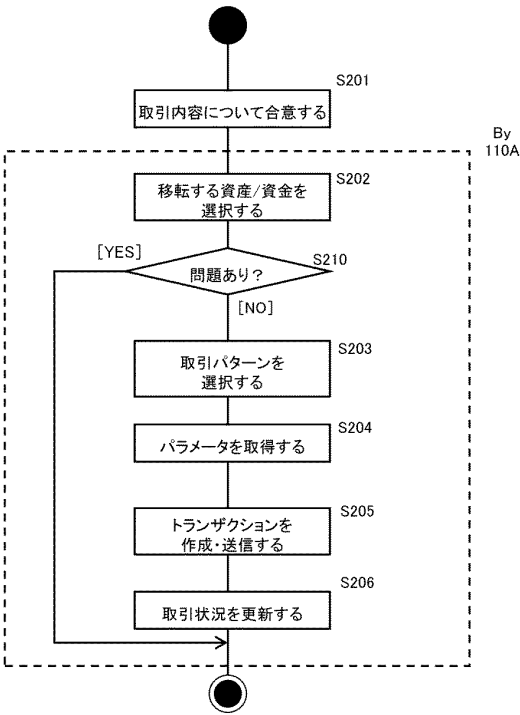
30

40

50

【図 1 2】

図12



【図 1 3】

図13

411

412

413

414

システム

ユーザ

秘密鍵

公開鍵

L

Me

1a2b3c0d

A0123

:

:

:

:

400

:

311

312

314

315

316

313

317

資産/
資金ID

残高

#

公開鍵

ロック解除条件

Hash

時刻

L0001

50

1

A0123

—

—

—

L0801

300

1

—

B0987

3a4b5c6d

—

—

2

—

A0123

—

2020/03/15 12:00

—

—

3

—

B0987

4c5d6e8f

—

—

—

3

1

A0123

5b6c7d8e

—

—

—

3

2

A0123

—

2020/03/15 12:00

—

—

:

:

:

:

:

:

:

300

≥ 50

空欄

310

【図 1 4 A】

図14A

資金/資産		変数名	区分	取得手段	値	
資産/資金1	資産/資金2				資産/資金1	資産/資金2
P _a	公開鍵	参照			A0123	A0123
P _b	公開鍵	参照			B0987	B0987
x ₁	秘密情報	作成				
y ₁	ハッシュ値					
x ₂	秘密情報	作成				
y ₂	ハッシュ値					
x ₃	秘密情報	作成				
y ₃	ハッシュ値					
T ₁	時刻	作成				

システム	ユーザ	秘密鍵	公開鍵
L	Me	1a2b3c0d	A0123
M	Me	1a2b3c0d	A0123
N	Me	1a2b3c0d	A0123
L	ユーザB	—	B0987
M	ユーザB	—	B0987
:	:	:	:

【図 1 4 B】

図14B

資金/資産		変数名	区分	取得手段	値	
資産/資金1	資産/資金2				資産/資金1	資産/資金2
P _a	公開鍵	参照			A0123	A0123
P _b	公開鍵	参照			B0987	B0987
x ₁	秘密情報				3456	
y ₁	ハッシュ値	作成			3a4b5c6d	
x ₂	秘密情報	作成			4567	
y ₂	ハッシュ値	作成			4c5d6e8f	
x ₃	秘密情報	作成			5678	
y ₃	ハッシュ値	作成			5b6c7d8e	
T ₁	時刻	作成			2020/03/15 12:00	

10

20

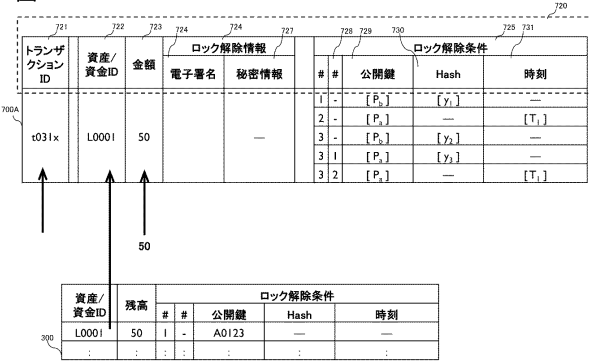
30

40

50

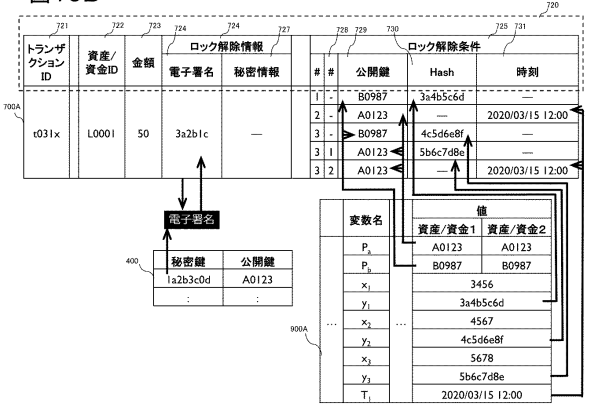
【図 15 A】

図15A



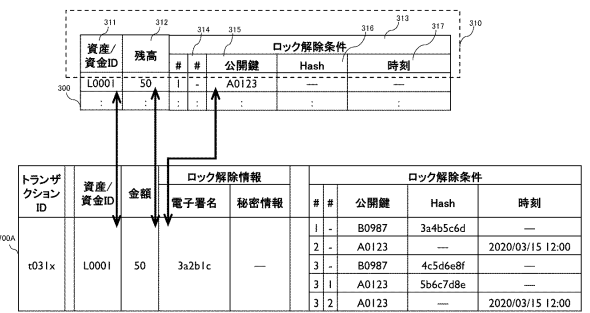
【図 15 B】

図15B



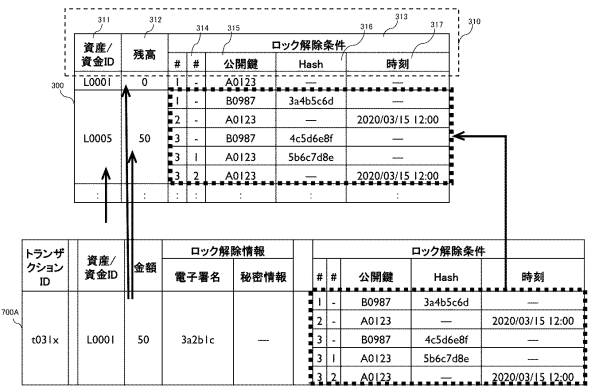
【図 16】

図16



【図 17】

図17



10

20

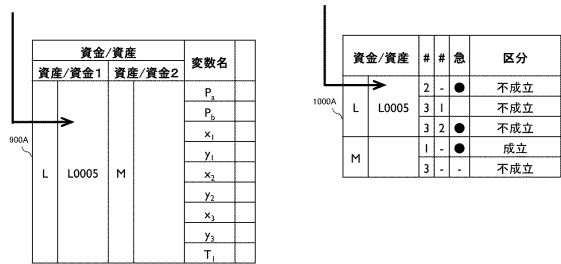
30

40

50

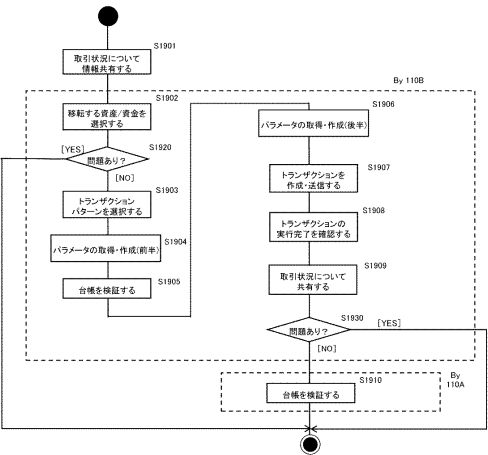
【図 18】

図18



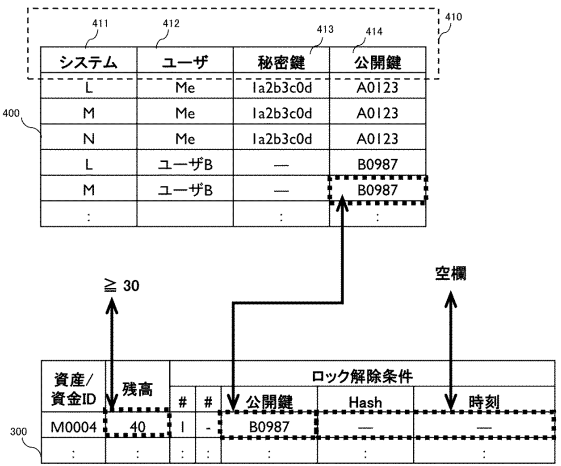
【図 19】

図19



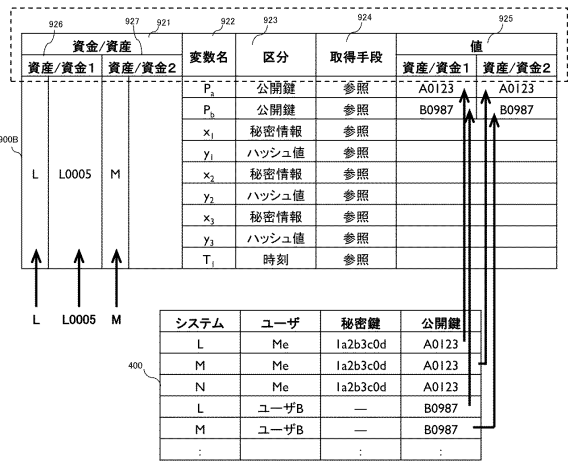
【図 20】

図20



【図 21 A】

図21A



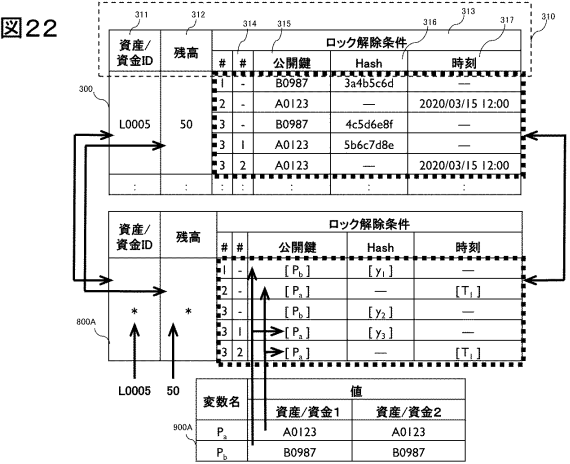
【図 2 1 B】

図21B



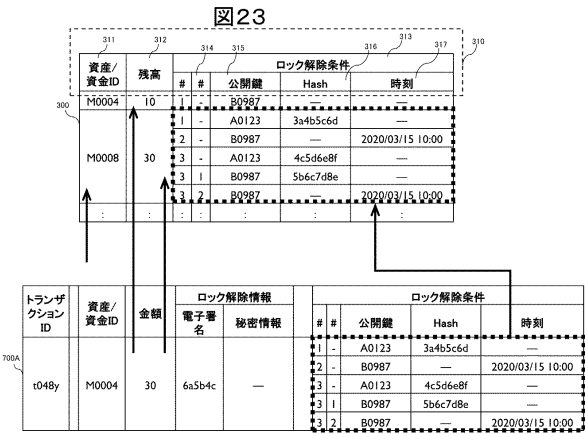
【図 2 2】

図22



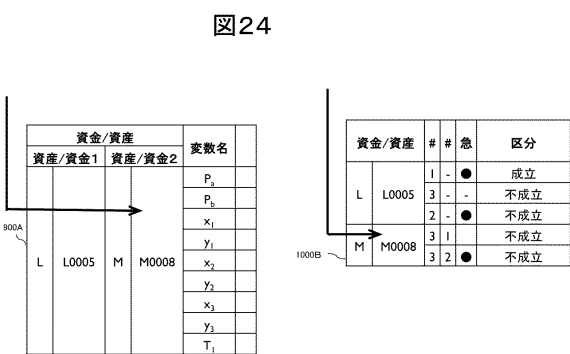
【図 2 3】

図23



【図 2 4】

図24



10

20

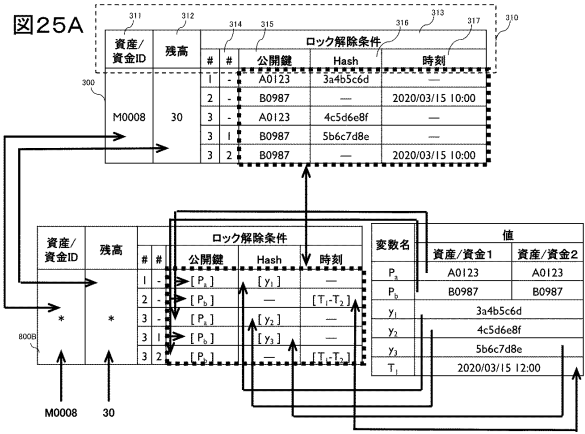
30

40

50

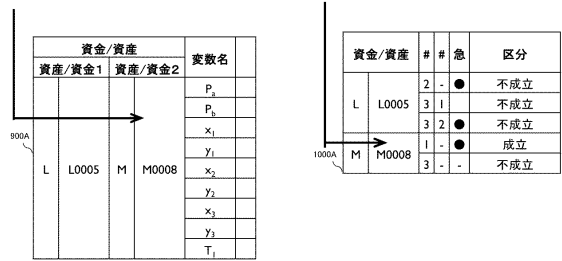
【図 2 5 A】

図25A



【図 2 5 B】

図25B



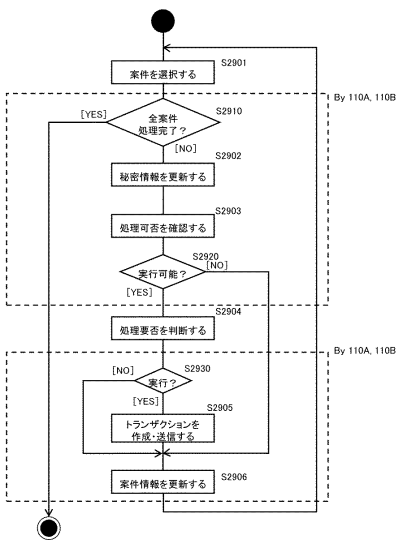
【図 2 5 C】

図25C



【図 2 6】

図26



10

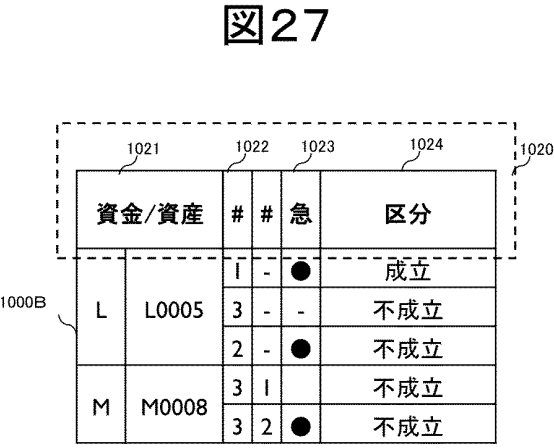
20

30

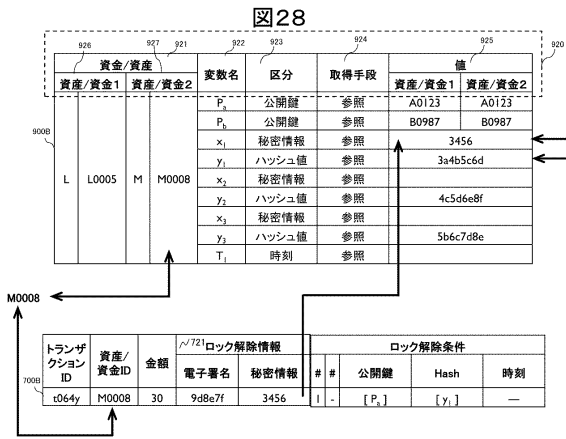
40

50

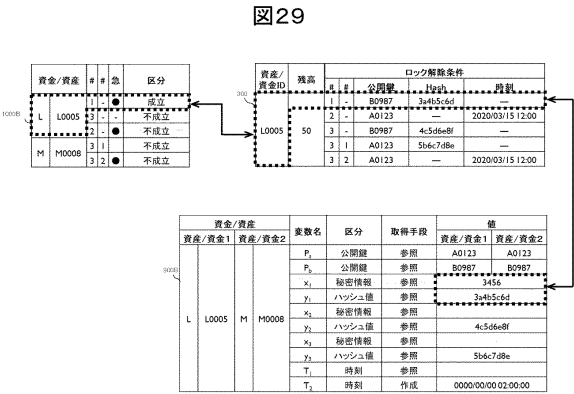
【図 2 7】



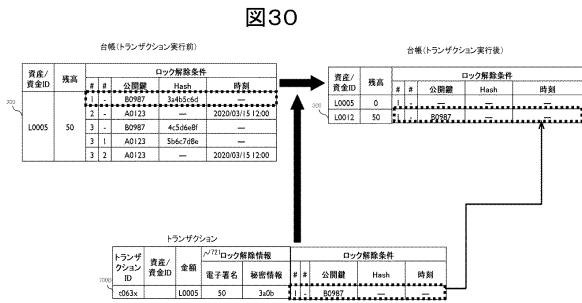
【図 2 8】



【図 2 9】



【図 3 0】



10

20

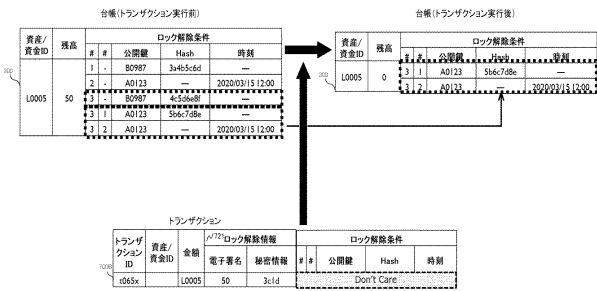
30

40

50

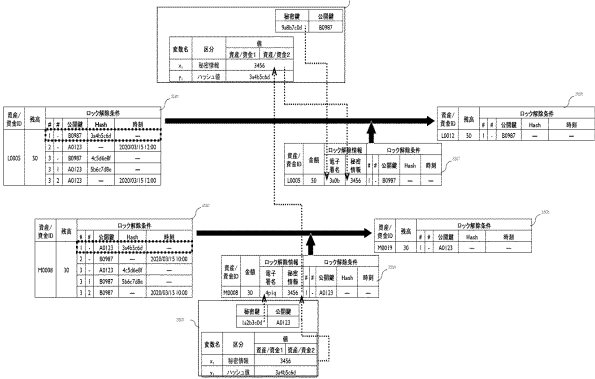
【図 3 1】

図31



【図 3 2】

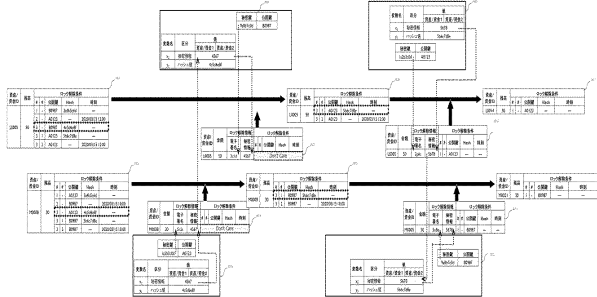
図32



10

【図 3 3】

図33



20

30

40

50

フロントページの続き

- (72)発明者 境 丈利
東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内
- (72)発明者 福地 開帆
東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内
- 審査官 貝塚 涼
- (56)参考文献 特開2020-67806 (JP, A)
特開2002-24532 (JP, A)
国際公開第2019/104250 (WO, A1)
特開2020-123265 (JP, A)
- (58)調査した分野 (Int.Cl., DB名)
G06Q 10/00 - 99/00
H04L 9/32