

(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
2021年11月18日(18.11.2021)



(10) 国際公開番号

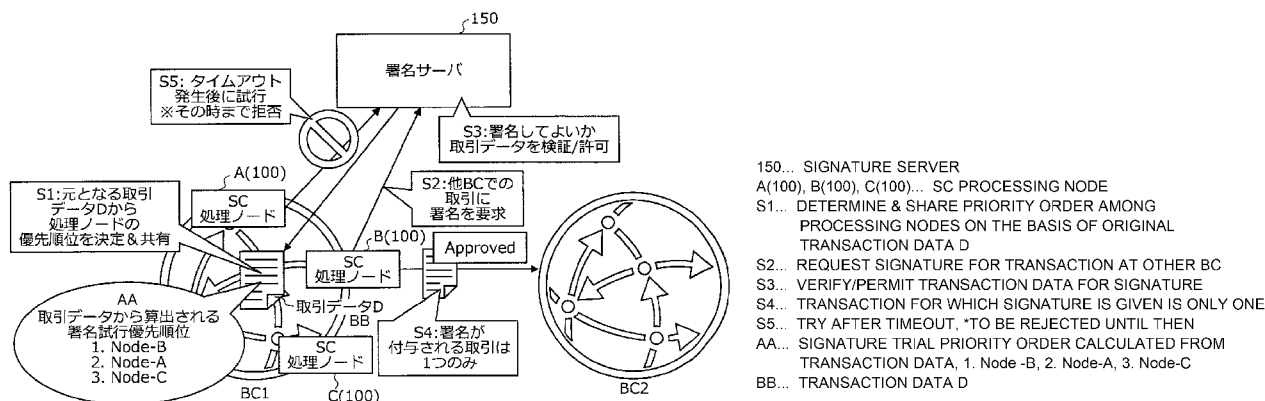
WO 2021/229691 A1

- (51) 国際特許分類:
G06F 11/20 (2006.01) G06Q 20/38 (2012.01)
- (21) 国際出願番号: PCT/JP2020/019003
- (22) 国際出願日: 2020年5月12日(12.05.2020)
- (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: 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).
- (72) 発明者: 藤本 真吾 (FUJIMOTO, Shingo); 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 森永 正信 (MORINAGA, Masanobu); 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).
- (74) 代理人: 酒井 昭徳 (SAKAI, Akinori); 〒1020094 東京都千代田区紀尾井町3番12号 紀尾井町ビル7階 酒井総合特許事務所 Tokyo (JP).
- (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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, GH, GM, KE, LR, LS,

(54) Title: CONTROL METHOD, CONTROL PROGRAM, AND INFORMATION PROCESSING DEVICE

(54) 発明の名称: 制御方法、制御プログラムおよび情報処理装置

[図1]



(57) Abstract: A plurality of processing nodes (100) are arranged so as to be in a redundant configuration in a first block chain (BC1). Each of the processing nodes (100) detects occurrence of transaction data (D) relating to a first transaction on the first block chain (BC1), and controls, on the basis of the detected transaction data, whether to transmit, to a second block chain (BC2), a remote transaction to be carried out after the first transaction. For example, the processing nodes (100) carry out hash calculations for data contents of the transaction data (D), and determine the priority order for executing remote transactions by the processing nodes (100). Then, if the priority order of an own processing node A (100) is highest, a remote transaction is transmitted to the second block chain (BC2). If the priority order of the own processing node A (100) is second highest or lower, transmission of the remote transaction to the second block chain (BC2) is set to stand by. Thus, no special exclusive control is necessary in the redundant configuration.

WO 2021/229691 A1

MW, MZ, NA, RW, 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, 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)）

(57) 要約：処理ノード（100）は、第1のブロックチェーン（BC1）に冗長構成で複数配置される。各処理ノード（100）は、第1のブロックチェーン（BC1）上での第1の取引に関する取引データ（D）の発生を検知し、検知した取引データに基づき、第1の取引後に行うべき遠隔取引を第2のブロックチェーン（BC2）に送信するか否かを制御する。例えば、複数の処理ノード（100）は、取引データ（D）のデータ内容に対するハッシュ演算を行い、複数の処理ノード（100）による遠隔取引の実行の優先順位を決定する。そして、自処理ノードA（100）の優先順位が最上位であれば、遠隔取引を第2のブロックチェーン（BC2）に送信し、自処理ノードA（100）の優先順位が次位以下であれば、遠隔取引を第2のブロックチェーン（BC2）に送信することを待機することで、冗長構成での特別な排他制御を必要としない。

明 細 書

発明の名称： 制御方法、制御プログラムおよび情報処理装置

技術分野

[0001] 本発明は、複数のブロックチェーンの連携による取引を制御する制御方法、制御プログラムおよび情報処理装置に関する。

背景技術

[0002] 近年、分散台帳管理技術として、ブロックチェーンの有用性が期待されている。例えば、分散台帳のブロックチェーンでは、仮想通貨やデジタル債券などの重要なデジタル資産を、暗号技術で保護して安全に取引および管理できる。一方、ブロックチェーンの運用においては、資産取引の正当性検証の必要があり、資産の種類によって正当性検証の手順（ロジック）が大きく異なることから、用途別のブロックチェーンがそれぞれ個別に構築されることによる市場の分断が問題になりつつある。

[0003] この市場分断の問題の解決策として、複数のブロックチェーン台帳を連携および統合するブロックチェーンの連携サービスが注目されている。連携サービスとして、例えば、ブロックチェーン間にスマートコントラクトが仲介することで、資産管理用の台帳を管理するブロックチェーンと、サービスへの対価決済の台帳を管理するブロックチェーンとを連携させることができる。

[0004] 従来、台帳管理に関連する技術として、例えば、ブロックチェーン内の異なる処理ノードで同じ処理が発生する場合、分散データベースの更新により処理ノード間での排他制御を行うことで処理ノード間の処理競合を防ぐ技術がある。また、負荷分散され多重化されたデバイスが取引報告メッセージに基づき、取引の増減処理の履歴を参照し同一の取引の重複を防ぐ技術がある。また、P2P（Peer to Peer）による直接取引の管理において、分散台帳技術を用いてスマートコントラクトを管理し、複数のメンバー管理処理ノードが電子署名等の同じ情報を共有することで障害発生に対処す

る冗長性を担保する技術がある（例えば、下記特許文献1～3参照。）。

先行技術文献

特許文献

- [0005] 特許文献1：特開2018-166000号公報
特許文献2：特開2008-276692号公報
特許文献3：特開2019-074910号公報

発明の概要

発明が解決しようとする課題

- [0006] ブロックチェーン台帳の連携として、例えば、証券・債権管理等の制御システムでは、一方のブロックチェーンで確定した取引に連動した形で他方のブロックチェーンへ遠隔取引を発行（実行）することがある。ここで、ブロックチェーンの複数の処理ノードを冗長構成にすることを考える。この冗長構成によれば、複数の処理ノードがそれぞれ遠隔取引を発行可能となり、通信障害等が生じても遠隔取引の発行を確実に行え、制御システムの運用継続性の確保が期待できる。
- [0007] しかしながら、単にブロックチェーンの複数の処理ノードがそれぞれ遠隔取引を発行する冗長構成にした場合、スマートコントラクトが遠隔取引を実行すると処理ノード間での処理の待ち合わせがなく、各処理ノード（サーバ群）が同じロジックで動作してしまう。この場合、処理ノード間で排他制御を行わないと、同じ遠隔取引が複数の処理ノードから複数回発行されてしまうという問題が生じる。ここで、排他制御のために処理ノード間での通信等を行う構成とした場合、各処理ノードでは、処理ノード間での通信および処理負荷が増大する問題を生じる。
- [0008] 一つの側面では、本発明は、ブロックチェーンの処理ノードの冗長化による取引の確実性が得られ、かつ、特別な排他制御を不要にできることを目的とする。

課題を解決するための手段

[0009] 本発明の一側面によれば、第1のブロックチェーンに冗長構成で配置される複数の処理ノードの制御方法であって、複数の前記処理ノードは、それぞれが記憶する前記第1のブロックチェーン上での第1の取引に関する取引データの発生を検知し、前記検知した取引データに基づき、前記第1の取引後に行うべき第2の取引を第2のブロックチェーンに送信するか否かを制御する、処理を実行する制御方法が提案される。

発明の効果

[0010] 本発明の一態様によれば、ブロックチェーンの処理ノードの冗長化による取引の確実性が得られ、かつ、特別な排他制御を不要にできるという効果を奏する。

図面の簡単な説明

[0011] [図1]図1は、実施の形態にかかる遠隔取引の制御例の説明図である。

[図2]図2は、実施の形態にかかる制御システムの各機能を説明するブロック図である。

[図3]図3は、実施の形態にかかる情報処理装置のハードウェア構成例を示す図である。

[図4]図4は、実施の形態にかかる遠隔取引の実行手順を説明する図である。

[図5]図5は、実施の形態にかかる各処理ノードの自律的な排他制御を説明する図である。

[図6]図6は、実施の形態にかかる取引データおよび優先順位の決定を説明する図である。

[図7]図7は、実施の形態にかかる処理ノードが行う処理例を示すフローチャートである。

[図8]図8は、実施の形態にかかる署名サーバが行う処理例を示すフローチャートである。

[図9]図9は、実施の形態にかかる遠隔取引を実行する優先順位の他の決定方法を説明する図である。

発明を実施するための形態

[0012] 以下に図面を参照して、開示の制御方法、制御プログラム、情報処理装置および制御システムの実施の形態を詳細に説明する。

[0013] 実施の形態では、一方のブロックチェーン（BC）での取引に連動した形で他方のBCへ遠隔取引を発行（実行とも言う）する、というBC間の連携において、遠隔取引を発行する一方のBCの複数の処理ノードを冗長構成にする。この冗長構成により、通信障害等が生じても遠隔取引の発行を確実にを行い、制御システムの運用継続性を確保する。

[0014] そして、実施の形態の処理ノードは、遠隔取引の元となる取引データに関する情報に基づき、遠隔取引を発行する優先順位を決定する。この優先順位は、取引データに基づき各処理ノードがそれぞれ自律的に決定する。これにより、一方のBCの複数の処理ノードは、冗長構成であっても各処理ノード間での遠隔取引の競合を防ぐ排他制御として同期データベースへのアクセス等の特別な処理を不要にし、遠隔取引を効率的かつ確実に発行する。

[0015] （実施の形態）

図1は、実施の形態にかかる遠隔取引の制御例の説明図である。実施の形態の制御システムは、第1のブロックチェーンBC1と、BC1に配置される複数の処理ノードA～C（100）と、第2のブロックチェーンBC2と、署名サーバ150と、を含む。情報処理装置とは、図1に示す各処理ノードA～C（100）、および署名サーバ150を指す。

[0016] 第1のBC1は、第1の分散台帳（例えば、ローカル台帳）を管理するブロックチェーンであり、第2のBC2は、第2の分散台帳（例えば、リモート台帳）を管理するブロックチェーンである。処理ノードA～C（100）は、それぞれが記憶するBC1上での第1の取引に関する取引データDが記録されたことを検知すると、取引データDに基づき、第1の取引後に行うべき第2の取引をBC2に送信するか否かを制御する。

[0017] 図1に示す制御システムは、例えば、証券・債券管理等、BC1、BC2を連携させBC1からBC2に遠隔取引を実行する各種の制御システムに適用できる。図1に示す制御システムにおいて、BC1に配置する複数の処理

ノードA～C（100）は、それぞれサーバによって構成できる。BC1とBC2との間には、後述するスマートコントラクト（SC）が配置される。

[0018] 各処理ノードA～C（100）は、SCによる制御に基づき、BC1での第1の取引とBC2での第2の取引とを連携させた遠隔取引を行う。SCは、各処理ノードA～C（100）を構成するサーバ内に配置、あるいは個別のサーバで構成できる。

[0019] 例えば、BC1は資産管理用の第1の分散台帳を管理し、BC2は決済トークン管理用の第2の分散台帳を管理する。この場合、BC1の処理ノードA～C（100）は、SCを介して第1の取引としての資産移動の取引データDに基づき、BC2に対する第2の取引として遠隔取引（決済トークンの発行）を行う。これにより、BC1の第1の分散台帳からBC2の第2の分散台帳に資産移動（トークンの払い出し）を行うことができる。

[0020] 実施の形態では、BC1上に複数の処理ノードA～C（100）を配置している。BC1に複数の処理ノードA～C（100）を配置することで、各処理ノードA～C（100）がそれぞれ遠隔取引が実行可能な冗長構成となる。この冗長構成により、遠隔取引を行う一つの処理ノードA～C（100）に通信や故障等の障害が生じて、他の処理ノードA～C（100）を用いて遠隔取引が可能となり、制御システムの運用継続性を確保できる。

[0021] 署名サーバ150は、冗長構成の各処理ノードA～C（100）の一つから第2の取引（遠隔取引）を実行するための署名要求を受けると、まず受信した取引データDを検証する。署名サーバ150は、検証結果、許可（承認）した取引データDに署名（電子署名）を付与し署名要求した処理ノードA～C（100）に返答する。

[0022] 例えば、署名サーバ150は、署名要求された取引データDの内容が正しいものであれば取引実行を許可する署名を付与した取引データDと処理の処理成功ステータスを返却し、取引データDの内容（例えば、譲渡額、同一取引の回数、日時等）に誤りや不備があればエラー・ステータスを返却して署名を許可しない。署名要求した一つの処理ノードA～C（100）は、署名

サーバ150により処理成功ステータスの返答を受けると、署名が付与された取引データDを用いてBC2に対する遠隔取引を行う。

[0023] そして、冗長構成の各処理ノードA～C(100)は、取引データDに基づき、遠隔取引を担当する処理ノードA～C(100)の優先順位を自律的に決定する。以下、処理ノードA～C(100)における遠隔取引の優先順位の決定～遠隔取引の実行を処理順に説明する。

[0024] (1)はじめに、BC1の各処理ノードA～C(100)は、第1の分散台帳への取引データDの記録があったとする。例えば、ユーザの端末(不図示)との間のP2P通信等により各処理ノードA～C(100)のそれぞれは、遠隔取引の元となる取引データDを受信する。取引データDの詳細は後述するが、取引ID(識別子)、取引種別、取引量(資産の移転量等)、移転元、移転先等の項目を有する。

[0025] そして、各処理ノードA～C(100)は、受信した取引データDを契機(トリガー)として、遠隔処理を行う一つの処理ノードA～C(100)を決定する。ここで、各処理ノードA～C(100)は、それぞれ、受信した同一の取引データDに対する所定の演算を行うことで、各処理ノードA～C(100)の遠隔取引の処理の実行順序(優先順位)を決定する(ステップS1)。

[0026] 上記所定の演算としては、例えば、各処理ノードA～C(100)は、同一の取引データDの内容(例えば、全データ)に対する同一の関数演算、例えば、同一のハッシュ値演算を行う。これにより、各処理ノードA～C(100)のうち、自処理ノードA(100)は、自処理ノードA(100)における遠隔取引の処理の実行順序(優先順位)を決定(認識)できる。

[0027] また、自処理ノードA(100)は、他処理ノードB, C(100)におけるそれぞれの遠隔取引の処理の実行順序(優先順位)を決定できる。同様に、処理ノードB, C(100)においても、同様の関数演算を行うことで各処理ノードA～C(100)の優先順位を決定できる。

[0028] 上記所定の演算の他の例としては、例えば、各処理ノードA～C(100)

)は、取引データDに対する第1の取引を検証した際に付与するタイムスタンプが早い順を優先順位として決定してもよい(詳細は後述する)。

[0029] このように、各処理ノードA~C(100)は、取引データDに基づき、遠隔処理を実行する処理順序の優先順位を決定する。また、各処理ノードA~C(100)は、それぞれが決定した優先順位を互いに共有することができる。

[0030] ここで、図1に示すように、優先順位の1番が処理ノードB(100)、2番目が処理ノードA(100)、最後が処理ノードC(100)に決定されたとする。なお、この段階で決定された優先順位は、署名サーバ150による署名検証が未実行であるため、各処理ノードA~C(100)から署名サーバ150に対する署名要求の実行順序(試行順位)に相当する。

[0031] (2)そして、各処理ノードA~C(100)のうち、優先順位が最も上位(1番)の処理ノードB(100)が、署名サーバ150に対し、BC2での遠隔取引の署名要求を行う(ステップS2)。署名要求は、取引データDを含む。

[0032] (3)署名サーバ150は、署名要求を受けた処理ノードB(100)からの署名要求に対し、署名してよいものであるか取引データDを検証する(ステップS3)。ここで、署名サーバ150においても、各処理ノードA~C(100)で実行した、取引データDの内容(データ列)に対する同一の関数演算、例えば、同一のハッシュ値演算を行ってもよい。この場合、署名サーバ150においても、各処理ノードA~C(100)の優先順位を算出する。

[0033] そして、署名サーバ150は、算出した優先順位に基づき、署名要求を受けた処理ノードB(100)からの署名要求に対する署名の付与を検証する。ここで、署名サーバ150は、算出した優先順位によって最も上位(1番)の処理ノード100が処理ノードB(100)であるため、はじめに署名要求した処理ノード100が処理ノードB(100)であるかを検証する。そして、署名サーバ150は、はじめに署名要求した処理ノード100が処

理ノードB（100）であれば、この処理ノードB（100）に対する署名を付与する。

[0034] 署名サーバ150は、署名の情報を付与した取引データDを処理ノードB（100）に返信する。そして、署名サーバ150は、優先順位が2番以降の処理ノードA、C（100）については、仮に署名要求があってもこの署名要求を拒否する。

[0035] （4）これにより、BC1上の各処理ノードA～C（100）のうちその時点で最も優先順位が上位の一つの処理ノードB（100）の取引データDに署名が付与されることになる（ステップS4）。そして、BC1上では、複数の処理ノードA～C（100）のうち、一つの処理ノードB（100）がBC2に対して取引データDを用いた遠隔取引を実行する。

[0036] （5）ここで、処理ノードB（100）による遠隔取引の発行に失敗したとする。この場合、遠隔取引の処理タイムアウト後に、次位以降の処理ノードA、C（100）について、先に算出しておいた優先順位にしたがって署名要求を署名サーバ150に発行する（ステップS5）。処理タイムアウトは、例えば、遠隔取引を発行した処理ノードB（100）とBC2との間の通信障害等により、処理ノードB（100）がBC2側から取引結果を受け取れない場合等に発生する。

[0037] 例えば、処理ノードB（100）は、この遠隔取引の発行時に所定時間のタイマを起動させ、BC2からの返答がタイムアウトした時、遠隔取引が失敗した旨をBC1の第1の分散台帳（ローカル台帳）に記録する。他の処理ノードA、C（100）は、定期的にローカル台帳を参照することで、遠隔取引の実行状態を判断でき、優先順位にしたがい自身の処理ノードA、C（100）が遠隔取引の実行順であるか否かを判断できる。

[0038] これにより、未処理分の取引データDについて、処理タイムアウト時間が経過した後、次位以降の処理ノードA、C（100）が優先順位にしたがって、署名サーバ150に署名要求を試行できる。そして、署名サーバ150は、この次位以降の処理ノードA、C（100）に対する署名発行を検証し

て一つの処理ノードA（100）に対する署名発行を許可する。

[0039] これにより、遠隔取引を発行する処理ノードB（100）での取引が完了できない場合（例えば処理途中での停止）が生じても、順次優先順位が下位の一つの処理ノードA～C（100）が遠隔取引を引き継いで実行できるようになる。

[0040] なお、各処理ノードA～C（100）間で、ある処理ノードB（100）に対する優先順位の決定後、遠隔取引を実施し処理タイムアウトが発生するまでの期間中、署名サーバ150は、他の処理ノードA，C（100）からの署名要求を拒否する。例えば、他の処理ノードA，C（100）が、署名サーバ150に対し署名要求を誤ったタイミングで送信しても、署名サーバ150は自身で算出した優先順位にしたがって、これら他の処理ノードA，C（100）に対する署名発行を拒否する。

[0041] 実施の形態の制御システムでは、クラスタ型の冗長構成で稼働する複数の処理ノードA～C（100）が、BC1，BC2間の連携に必要な遠隔取引を発行する際、遠隔取引の発行を承認（許可）する署名サーバ150へのアクセスを自律的に排他制御する。

[0042] この排他制御は、各処理ノードA～C（100）のいずれもが遠隔取引の発行の元となる連携元のBC1の取引データDに含まれる情報により一意に決定する優先順位で実現できる。これにより、BC1の複数の処理ノードA～C（100）を冗長構成とした場合でも、各処理ノードA～C（100）からBC2への遠隔取引を優先順位にしたがった一つの処理ノードA～C（100）のみから発行できるようになる。

[0043] また、優先順位の決定の処理は、各処理ノードA～C（100）だけではなく、署名サーバ150でも独立して決定できる。この場合、署名サーバ150が決定した優先順位と、各処理ノードA～C（100）が決定した優先順位との一致に基づき、上位の処理ノードA～C（100）から順に署名要求を検証できるようになる。すなわち、署名要求の優先順位を各処理ノードA～C（100）と、署名サーバ150とでダブルチェックできるようにな

る。これにより、BC1の複数の処理ノードA~C(100)を冗長構成とした場合でも、各処理ノードA~C(100)からBC2への遠隔取引を優先順位にしたがった一つの処理ノードA~C(100)のみから発行できるようになる。

[0044] また、署名が付与された処理ノードB(100)に通信等の障害が発生し、遠隔取引を発行した処理ノードB(100)での遠隔取引が完了せず失敗したとする。この場合には、処理タイムアウト時間の経過後に、次位以降の処理ノードA, C(100)が優先順位にしたがって署名要求を署名サーバ150に発行し、未完状態の遠隔取引を継続できるようになる。また、遠隔取引は、常にある一つの処理ノードA~C(100)から一回だけ確実性を有して行えるようになる。

[0045] 上記のように、BC1上の処理ノードA~C(100)は、取引を「発行」してから署名サーバ150によって「発行」した取引が承認されると、BC2への遠隔取引を「実行」する。そして、実施の形態によれば、BC1に複数の処理ノードA~C(100)を冗長構成で配置することで、複数の処理ノードA~C(100)のいずれかからBC2に遠隔取引を確実に実行できるようになる。また、処理ノードA~C(100)がそれぞれ共有する取引データDに基づき優先順位を自律的に決定することで、冗長構成における特別な排他制御を不要にできる。また、取引データDのデータ内容に基づいて優先順位を決定するため、新たな取引データD毎に優先順位が異なって最上位の処理ノードA~C(100)が決定されることとなる。これにより、遠隔取引発行の処理負担を複数の処理ノードA~C(100)で均等に分散できる水平処理スケールアップを実現できるようになる。

[0046] 図2は、実施の形態にかかる制御システムの各機能を説明するブロック図である。図2に示す制御システムでは、デジタル債券の分散台帳2を管理するブロックチェーンBC2(債券BC)と、決済トークンの分散台帳1を管理するブロックチェーンBC1(決済BC)を連携させる。

[0047] そして、ユーザU1が保有するデジタル債券Xの所有権を、Y単位の決済

トークンの委譲に基づきユーザU 2に移転する。債券BC (BC 2)と決済BC (BC 1)で実行される取引の順序は重要ではないが、実施の形態では、決済BC (BC 1)での決済トークンの委譲が完了してから、債券BC (BC 2)での所有権移転が実行制御されるものとした。この所有権移転にかかる実行制御の手順は連携シナリオに設定しておく。

[0048] 上記連携シナリオに沿ったBC 1, BC 2間の連携動作は、決済BC (BC 1)を構成する処理ノード群100上で稼働中のスマートコントラクト(SC) 200が実行制御する。SC 200は、図2に示すように、制御システム上に一つのSC 200を配置し、各処理ノード100を制御する構成とする他に、SC 200を各処理ノード100に備える構成としてもよい。

[0049] SC 200は、ユーザ(例えばU 1, U 2とする)間の債券取引が指示されると、買い手ユーザU 2の口座から売り手ユーザU 1の口座へ指定された取引単位分の決済トークンの移転取引を発行する。SC 200は、取引発行が確定したのち、債券BC (BC 2)上で売り手ユーザU 1から買い手ユーザU 2への権利移転を遠隔取引として実行する。

[0050] SC 200は、連携シナリオ記憶手段201、連携シナリオ実行手段202、トリガー監視手段203、の各機能を含む。連携シナリオ実行手段202とトリガー監視手段203は、SC 200の制御部として機能する。

[0051] 連携シナリオ記憶手段201は、取引データDの発生毎に、決済BC (BC 1)での決済トークンの委譲が完了してから、債券BC (BC 2)での所有権移転までの実行制御の手順(連携シナリオ)を記憶する。トリガー監視手段203は、遠隔取引の元となる取引データDの発生を検出する。連携シナリオ実行手段202は、トリガー監視手段203で検出された取引データDの取引内容にしたがい、BC 1上の複数の処理ノード100に対して遠隔取引の実行を指示する。

[0052] 処理ノード100は、BC 1上に複数(n個)配置され、それぞれ同様の機能を有する。処理ノードA(100)を例に説明すると、遠隔取引受付手段211、トリガー取引参照手段212、実行優先順位決定手段213、承

認署名取得手段 214、遠隔取引発行手段 215、タイムアウト計時手段 216、の各機能を含む。これら遠隔取引受付手段 211～タイムアウト計時手段 216 の下記機能は、処理ノード A (100) の制御部として機能する。

[0053] 遠隔取引受付手段 211 は、SC 200 からの遠隔取引の実行の指示を受けると、処理ノード A (100) 内の各機能部を起動させる。トリガー取引参照手段 212 は、遠隔取引の元となる取引データ D の発生時、取引データ D を BC 1 の分散台帳 1 から取得する。

[0054] 実行優先順位決定手段 213 は、取得した取引データ D のデータ内容を用いた所定の演算処理に基づき、BC 1 上における複数 (n 個) の処理ノード 100 それぞれについて遠隔取引の発行の優先順位を決定する。この優先順位は、より厳密には、署名サーバ 150 に対する署名要求の優先順位を示す。

[0055] 実行優先順位決定手段 213 は、各処理ノード 100 にそれぞれ設けられ、いずれも同一の取引データ D の内容 (例えば、全データ) に対する同一の演算、例えば、同一のハッシュ値を用いた関数演算を行う。この決定により、実行優先順位決定手段 213 は、複数全ての処理ノード n (100) のうち、自処理ノード A (100) の優先順位を認識する。

[0056] 承認署名取得手段 214 は、自処理ノード A (100) が現時点で最も上位の優先順位であれば、署名サーバ 150 に取引データ D を送信し、遠隔取引の実行に必要な署名 (電子署名) を要求する。承認署名取得手段 214 は、署名サーバ 150 による承認時には、署名サーバ 150 から署名が付与された取引データ D を取得する。

[0057] 遠隔取引発行手段 215 は、署名サーバ 150 から署名を取得できれば、この署名を用いて取引データ D の取引内容に基づき BC 2 に対する遠隔取引を実行する。タイムアウト計時手段 216 は、自処理ノード A (100) による遠隔取引の実行時から起動するタイマ計時を行い、遠隔取引の処理終了までの期間に対応して設定した所定のタイムアウトを監視する。

- [0058] 署名サーバ150は、トリガー取引参照手段221、署名許可ルール記憶手段222、実行優先順位決定手段223、承認署名付与手段224、の各機能を含む。トリガー取引参照手段221、実行優先順位決定手段223、承認署名付与手段224の各機能は、署名サーバ150の制御部として機能する。
- [0059] トリガー取引参照手段221は、署名要求した処理ノードA(100)が送信する取引データDの取得に基づき、署名サーバ150内の各機能部を起動させる。署名許可ルール記憶手段222は、取引データD毎に、署名要求した処理ノード100のそれぞれに対する署名付与の優先順位を含む許可ルールの情報を記憶する。許可ルールは、上記の処理ノード100が実施する、取引データDのデータ内容を用いた所定の演算処理と同じ演算処理の情報を含む。
- [0060] 実行優先順位決定手段223は、署名許可ルール記憶手段222に記憶された許可ルールに基づき、BC1上の複数の処理ノード100に対する遠隔取引の発行(実行)の優先順位を決定する。実行優先順位決定手段223は、各処理ノード100に設けられる実行優先順位決定手段213と同一の演算を行う。すなわち、実行優先順位決定手段223は、同一の取引データDの内容(例えば、全データ)に対する、同一のハッシュ値演算を行う。これにより、署名サーバ150が算出する優先順位は、BC1上に配置された複数の処理ノード100がそれぞれ決定する遠隔取引の発行(実行)の優先順位と同じものとなる。
- [0061] 承認署名付与手段224は、現時点で最上位の優先順位であり、署名要求した一つの処理ノード100に対し、取引データDに基づく遠隔取引の実行に必要な署名(電子署名)の付与を承認し、取引データDに署名を付与して該当の処理ノード100に送る。ここで、承認署名付与手段224は、現時点で次位以下の優先順位の処理ノード100からの署名要求があっても、これら処理ノード100に対する署名の付与を行わない。
- [0062] 図2に示した制御システムにおける全体の処理は、下記(1)~(5)の

手順を有して実行される。下記の説明では、BC1上のn個の処理ノード100は、取引データDの発生に基づき、ブロックデータを生成する。

[0063] (1) 取引の合意

BC1で債券の買い手であるユーザU2の口座から、債券の売り手であるユーザU1の口座へY単位の決済トークンの移転を行う署名済みの取引データDが発行 (Submit) される。これにより、SC200は、BC1上の取引データDの発生をトリガーとして取引の発生を検出する (ステップS11)。また、各処理ノード100は、BC1上の取引データDの発生をトリガーとして取引の発生を検出する (ステップS12)。各処理ノード100は、取引データDが示す取引の正当性検証を行った後、取引データDをブロックデータの一部として取り込む。

[0064] (2) 優先順位の決定

各処理ノード100が上記ステップS12で取り込むブロックデータは、SC200によって常時モニターされる。SC200は、決済トークンの移転の取引データDの発生を検出すると、記憶している連携シナリオを実行する (ステップS13)。そして、SC200は、連携シナリオの実行に基づき、ユーザU1とユーザU2との間の債券売買の一連取引の一部であると認識する。そしてSC200は、一連の取引の次のステップとして、BC1でユーザU1の所有する債券の所有権をユーザU2に移転する遠隔取引が必要と判断し、連携シナリオに沿った遠隔取引の実行を各処理ノード100へ指示する (ステップS14)。

[0065] 各処理ノード100は、遠隔取引を実行する前に、ステップS12で検出した取引データDを入力とし、各処理ノード100間の優先順位を決定する演算 (関数演算) を実行する。この演算の実行により、取引を実行する優先順位として、例えば、「1位: 処理ノードA、2位: 処理ノードB、3位: 処理ノードC」を算出する。算出した優先順位で1位となった処理ノードAを除く、他の処理ノードB、Cは、処理ノードAでの遠隔取引の実行がタイムアウトとなるまで待機状態となる。

[0066] (3) 署名要求を送信

例えば、優先順位1位となった処理ノードA(100)は、BC1上で管理されている売り手のユーザU1の所有する債券Xの所有権を買い手のユーザU2に移転するために必要な署名を、署名サーバ150に対し署名要求する(ステップS15)。処理ノードA(100)は署名要求とともに取引データDを署名サーバ150に送信する。

[0067] (4) 署名を許可

署名サーバ150は、署名要求した処理ノードA(100)から取引データDを取得する(ステップS16)。そして、署名サーバ150は、取引データDを入力とし、各処理ノードA~C(100)の優先順位を決定する関数演算を実行する。そして、署名サーバ150は、算出した優先順位に基づき、署名要求した処理ノードA(100)からの署名要求を承認(許可)可能か否かを判断する。承認可能な場合には受信した取引データDに電子署名を付与し、署名済みの取引データを処理ノードA(100)へ返信する。

[0068] 署名が付与された取引データDを受け取った処理ノードA(100)は、受け取った取引データDを用いてBC2への遠隔取引を実行する(ステップS17)。BC2上の各参加処理ノードによる検証を経て、遠隔取引の正当性が確認された取引データDは、ブロックデータに取り込まれ、遠隔取引にかかる上記一連の処理が正常に完了する。

[0069] ところで、署名要求について、優先順位が1位の処理ノードA(100)の署名要求時に、優先順位が2位の処理ノードB(100)が誤って署名サーバ150に署名要求したとする。この場合、署名サーバ150は、処理ノードB(100)は、現時点では優先順位が最上位ではないと判断し、処理ノードB(100)からの署名要求を拒絶し、処理ノードB(100)に対しエラー応答を返す。

[0070] (5) タイムアウトの発生時

署名済みの取引データDを受信した処理ノードA(100)に障害が発生したとする。ここで、遠隔取引を実行した処理ノードA(100)にタイム

アウトが発生し、BC2上で債券XのU1からU2への所有権移転が確認できなかった場合が生じたとする。この場合、待機状態になっていた優先順位が2位の処理ノードB(100)が署名要求(ステップS15)以降の処理を実行する。また、優先順位が2位の処理ノードB(100)での遠隔取引の実行にタイムアウトが生じた場合には、優先順位が3位の処理ノードC(100)が署名要求(ステップS15)以降の処理を実行する。

[0071] 図3は、実施の形態にかかる情報処理装置のハードウェア構成例を示す図である。上述した処理ノードA~C(100)は、それぞれ図3に示すハードウェアで構成されたサーバ等を用いることができる。

[0072] 例えば、処理ノードA(100)は、CPU(Central Processing Unit)301、メモリ302、ネットワークインタフェース(IF)303、記録媒体IF304、記録媒体305、を含む。300は各部を接続するバスである。

[0073] CPU301は、処理ノードA(100)の全体の処理を司る制御部として機能する演算処理装置である。メモリ302は、不揮発性メモリおよび揮発性メモリを含む。不揮発性メモリは、例えば、CPU301のプログラムを格納するROM(Read Only Memory)である。揮発性メモリは、例えば、CPU301のワークエリアとして使用されるDRAM(Dynamic Random Access Memory)、SRAM(Static Random Access Memory)等である。

[0074] ネットワークIF303は、LAN(Local Area Network)、WAN(Wide Area Network)、インターネットなどのネットワーク310に通信接続するインタフェースである。このネットワークIF303を介して、処理ノードA(100)は、他の処理ノードB、C(100)、SC200、署名サーバ150、ユーザの端末等に通信接続する。

[0075] 記録媒体IF404は、CPU301が処理した情報を記録媒体305との間で読み書きするためのインタフェースである。記録媒体305は、メモ

リ302を補助する記録装置である。記録媒体305は、例えば、HDD (Hard Disk Drive) や、SSD (Solid State Drive)、USB (Universal Serial Bus) フラッシュドライブ等を用いることができる。

[0076] メモリ302または記録媒体305に記録されたプログラムをCPU301が実行することにより、図2に示した各処理ノードA~C(100)の各機能(制御部)を実現することができる。

[0077] 図3に示したハードウェア構成は、図2に示したSC200や、署名サーバ150、さらにはユーザの端末(例えば、PCやスマートフォン等)にも適用でき、実施の形態の制御システムは、汎用のハードウェア構成を用いて実現できる。また、図3に示したハードウェア構成により、1台のサーバが各処理ノードA~C(100)とSC200の機能を有する構成とすることもできる。

[0078] SC200の連携シナリオ記憶手段201や署名サーバ150の署名許可ルール記憶手段222は、例えば、メモリ302や記憶媒体305を用いて構成できる。また、各処理ノードA~C(100)の実行優先順位決定手段213、および署名サーバ223の実行優先順位決定手段223は、優先順位を算出するための演算式をメモリ302や記憶媒体305に記憶保持している。

[0079] 図4は、実施の形態にかかる遠隔取引の実行手順を説明する図である。BC1上に複数の処理ノードA~C(100)を冗長構成で配置した場合における取引データDの発生から遠隔取引の実行までの実行手順の例を示す。各手順のステップ番号は、図1記載のステップ番号を用いている。

[0080] (a) はじめに、ユーザによる取引で生成された取引データDを各処理ノードA~C(100)が受信する。各処理ノードA~C(100)は、それぞれこの取引データDが示す取引に合意する(ステップS1-1)。

[0081] (b) 各処理ノードA~C(100)は、合意した取引データDを用いた所定の演算(関数演算)により、処理ノードA~C(100)間の優先順位を

決定する（ステップS 1-2）。この演算の実行により、取引実行の優先順位として、例えば、「1位：処理ノードB、2位：処理ノードC、3位：処理ノードA」、という優先順位を算出する。

[0082] (c) 次に優先順位で上位の処理ノードA~C（100）から署名サーバ150に署名要求する。図4の例では、優先順位1位となった処理ノードB（100）が、遠隔取引の実行に必要な署名を、署名サーバ150に対し署名要求する（ステップS 2）。ここで、署名サーバ150は、署名要求により処理ノードB（100）から受信した取引データDに対し、処理ノードA~C（100）と同様の演算（関数演算）により、処理ノードA~C（100）間の優先順位を決定する。

[0083] そして、署名サーバ150は、署名要求した処理ノードB（100）の優先順位に齟齬がなければ処理ノードB（100）に対する署名を許可する（ステップS 3）。図4の例では、署名サーバ150は、「1位：処理ノードB、2位：処理ノードC、3位：処理ノードA」、という優先順位を算出している。したがって、現時点で優先順位1位となった処理ノードB（100）からの署名要求を許可する（ステップS 3）。そして、この処理ノードB（100）に対して取引承認を返答する。

[0084] この時点で、BC1上の各処理ノードA~C（100）のうち優先順位が1位の一つの処理ノードB（100）の取引データDに署名が付与されることになる（ステップS 4）。署名が付与された取引データDを受け取った処理ノードB（100）は、受け取った取引データDを用いてBC2への遠隔取引を実行できる。

[0085] ここで、署名サーバ150は、算出した優先順位で1位となった処理ノードB（100）を除く、他の処理ノードA、C（100）は、処理ノードB（100）での遠隔取引の実行がタイムアウトとなるまで待機状態にさせる。このため、最上位の処理ノードB（100）の署名要求時に、処理ノードA（100）が誤って署名サーバ150に署名要求したとする。この場合、署名サーバ150は、算出した優先順位が下位の処理ノードA（100）か

らの署名要求を拒絶し、処理ノードA（100）に対しエラー応答を返す。

[0086] (d) この後、署名済みの取引データDの受信後、処理ノードB（100）に障害が発生したとする。この場合、遠隔取引を実行すべき処理ノードB（100）にタイムアウトが発生し、処理ノードB（100）は、BC2に対する遠隔取引を完了できなくなる。優先順位が1位の処理ノードB（100）でのタイムアウトの発生により、待機状態になっていた次位（優先順位が2位）の処理ノードC（100）が署名サーバ150に署名要求する（ステップS5）。ここで、署名サーバ150は、署名要求した処理ノードC（100）の優先順位に齟齬がなければ処理ノードC（100）に対する署名を許可する。

[0087] 図5は、実施の形態にかかる各処理ノードの自律的な排他制御を説明する図である。図5を用いて複数の処理ノードA～C（100）がそれぞれ自律的に優先順位を決定することで、一つの処理ノードB（100）が遠隔取引を実行する例を説明する。

[0088] BC1内に冗長構成で配置された各処理ノードA～C（100）は、発生した取引データDをそれぞれ承認すると、各処理ノードA～C（100）が取引データDを承認した旨をブロックデータD1に記録する（ステップS51）。ブロックデータD1は、BC1が管理するローカル台帳に記録される。

[0089] 次に、各処理ノードA～C（100）は、それぞれブロックデータD1に含まれる承認済みの取引データDを用い、優先順位の決定ロジックを実行し、優先順位を決定する（ステップS52）。この決定ロジックでは、各処理ノードA～C（100）が取引データDに対する同一の所定の演算（関数演算）を行う。これにより、各処理ノードA～C（100）は、自処理ノードおよび他の処理ノードにおける優先順位を決定する。

[0090] 例えば、処理ノードA～C（100）は、取引データDに対して同一のハッシュ値演算を行うことで、各処理ノードA～C（100）それぞれ遠隔取引の処理について、自処理ノードでの優先順位、および他の処理ノードでの

優先順位を決定する。この優先順位は、各処理ノードA～C（100）における遠隔取引の実行順序に相当し、より厳密には、各処理ノードA～C（100）から署名サーバ150に対する署名要求の実行順序を示す。これにより、また、各処理ノードA～C（100）は、相互に通信等を行うことなく、取引データDに基づき自律的に優先順位（遠隔取引の実行順序）を共有できる。

[0091] そして、優先順位が最上位の処理ノードB（100）が署名サーバ150に対して取引データDに対する署名要求を行い、署名サーバ150の承認後、BC2に対する遠隔取引を発行（実行）する（ステップS53）。ここで、署名サーバ150は、自ら算出した優先順位に基づき、優先順位が上位の処理ノード100からの署名要求であるか否かを判断（優先順位の齟齬をチェック）する（ステップS54）。そして、上述したように、現時点で最も優先順位が高い一つの処理ノードA～C（100）からの署名要求のみを承認する。

[0092] 実施の形態によれば、各処理ノードA～C（100）が取引データDに対する同一の演算を行うことで、各処理ノードA～C（100）間での優先順位を共有でき、この優先順位にしたがって一つの処理ノードA～C（100）が遠隔取引を実行する。このようにBC1上に複数の処理ノードA～C（100）を配置することで、BC1からBC2に対する遠隔取引の発行を冗長化でき、遠隔取引を確実に実行できるようになる。

[0093] また、各処理ノードA～C（100）は、優先順位の決定により、冗長構成にした構成においても、各処理ノードA～C（100）による遠隔取引の多重発行を防ぐことができる。加えて、署名サーバ150側でも各処理ノードA～C（100）と同一の演算により各処理ノードA～C（100）の優先順位を算出する。これにより、各処理ノードA～C（100）からの署名要求を署名サーバ150でもダブルチェックでき、遠隔取引の多重発行を防ぐことができる。

[0094] さらに、BC1上の処理ノードA～C（100）の処理負担を簡単に分散

できるようになる。この点、実施の形態では、優先順位の決定に処理ノードA～C（100）間の通信を用いた連携を行う必要がなく、取引データDを用いて各処理ノードA～C（100）が自律的に優先順位を決定することで、簡単な構成で排他制御を実現できる。

[0095] なお、冗長構成において、予め処理ノードA～Cに優先順位を付与しておくシステム構成が考えられる。しかし、この場合には常時、所定の処理ノードAが最上位の優先順位に固定されることとなり、この処理ノードAのみに処理負担が掛かるため、冗長構成にした複数の処理ノードA～Cでの分散処理はできない。この点、実施の形態によれば、上記のタイムアウト発生時の処理の如く、優先順位にしたがって待機中の処理ノードA（100）もリソースとして使用することができる構成であるため、複数の処理ノードA～C（100）を有効利用できるようになる。

[0096] 図6は、実施の形態にかかる取引データおよび優先順位の決定を説明する図である。上述した取引データDのデータ例と、この取引データDに対する所定の関数演算による各処理ノードA～C（100）の優先順位の決定、等について説明する。

[0097] BC1上で生成される取引データDは、例えば、取引ID（識別子）600a、資産種別600b、移転量600c、移転元600d、移転先600e、取引承認署名600fを有する。取引ID600aは、取引データDの生成時に生成され、取引内容を識別する識別子である。資産種別600bは、図2に示したBC1上でユーザU1の取引内容（決済トークン）を示す。移転量600cは、デジタル債券の決済トークン量（譲渡額）を示す。移転元600dは、デジタル債券の所有元のユーザU1を示し、移転先600eは、デジタル債券の移転先のU2を示す。取引承認署名600fは、この取引データDに対する署名要求に基づき、署名サーバ150が付与した電子署名である。

[0098] 各処理ノードA～C（100）は、受信した取引データDに対する同一の関数演算Oを行う。例えば、「hash（生の取引データ）mod6」とい

うハッシュ演算（符号610a）を実行する。「生の取引データ」は、取引データDの実質的なデータ内容、例えば、取引ID（識別子）600a～移転先600eまでのデータ列である。各処理ノードA～C（100）は、このハッシュ演算610aを実行することで、「3：B→C→A」の処理結果（符号610b）を得たとする。この処理結果は、上述した優先順位に相当し、最上位が処理ノードB、2位が処理ノードC、最下位が処理ノードAを示す。図中の「0」～「5」は、3つの処理ノードA～C（100）の組合せ（の識別子）である。なお、署名サーバ150もこの取引データDに対して同一の関数演算Oを行い、優先順位を算出する。

[0099] 符号D'は、遠隔取引時の取引データの内容を示す。この遠隔取引時の取引データD'は、BC2上で用いるデータであるため、BC1上で生成した上記の取引データDと項目の一部が入れ替わっている。例えば、取引データD'は、取引ID（識別子）600aと、移転元600d、移転先600eは、取引データDと同じであり、移転量600cはない。その他、資産種別600bは、BC2上でのユーザU2の債券トークンを示す。取引承認署名600fは、この取引データDに対する署名要求に基づき、署名サーバ150が遠隔取引時に付与した電子署名である。資産ID600gは、ユーザU2の債券台帳である。

[0100] 上記のように、処理ノードA～C（100）、および署名サーバ150は、一つの取引データDに対するハッシュ演算を行うことで、同じ優先順位を算出できる。このようにして算出した優先順位を用いることで、BC1上に複数の処理ノードA～C（100）を冗長構成で配置した時の排他制御を簡単に実施できる。すなわち、制御システム内の各処理ノードA～C（100）は優先順位にしたがった署名要求を行い、署名サーバ150においても、各処理ノードA～C（100）からの署名要求を優先順位に基づき検算できる。署名サーバ150は、取引データDに基づき所定の演算で算出した優先順位にしたがって常に一つの処理ノードA～C（100）に対してのみ署名を付与する。

- [0101] したがって、実施の形態によれば、各処理ノードA～C（100）を冗長構成にした場合でも、各処理ノードA～C（100）間での通信等の特別な排他制御を行うことなく、簡単な構成で排他制御が行えるようになる。そして、BC1上の各処理ノードA～C（100）から同じ取引が複数回発行されることを防ぎ、常に一つの処理ノードA～C（100）による遠隔取引を実行できるようになる。
- [0102] 図7は、実施の形態にかかる処理ノードが行う処理例を示すフローチャートである。処理ノードA～C（100）の制御部（図3のCPU301）は、BC1上でユーザの取引データDの受信毎に以下の処理をそれぞれ並行して実行する。
- [0103] はじめに、制御部は、BC1上でユーザの取引データDを受信する（ステップS701）。ユーザの端末が生成した取引データDを各処理ノードA～C（100）の制御部がP2Pにより受信する。
- [0104] 次に、制御部は、取引データDが正当であるか判断する（ステップS702）。例えば、制御部は、図6に示す取引データDの各項目の内容で正常取引できるか判断する。判断の結果、制御部は、取引データDが正当であれば（ステップS702：Yes）、ステップS703の処理に移行し、取引データDが正当でなければ（ステップS702：No）、ステップS704の処理に移行する。
- [0105] ステップS703では、制御部は、取引データDによる取引の承認メッセージをBC1上に送信し（ステップS703）、ステップS705の処理に移行する。一方、ステップS704では、制御部は、取引データDによる取引が正当でないため、受信した取引データDを破棄し（ステップS704）、以上の処理を終了する。
- [0106] 各処理ノードA～C（100）それぞれの制御部は、承認メッセージを送信した取引データDをBC1上のブロックデータD1にまとめる（図5参照）。ブロックデータD1は、各処理ノードA～C（100）が今回の取引データDの取引に合意したことを示す。ステップS705では、各処理ノード

A～C（100）の制御部は、BC1上から承認済みの取引データDを一つにまとめたブロックデータD1を受信する（ステップS705）。

[0107] 次に、制御部は、取引データDの処理結果（取引が正当である旨）をBC1上のローカル台帳に反映させる（ステップS706）。次に、制御部は、取引データDは遠隔取引が必要なものであるかを判断する（ステップS707）。ここで、制御部は、取引データDの項目にBC2への資産移転が設定されているかを判断する。

[0108] 判断の結果、制御部は、遠隔取引が必要であれば（ステップS707：Yes）、ステップS708の処理に移行し、遠隔取引が必要でなければ（ステップS707：No）、ステップS701の処理に戻る。例えば、図6に示した取引データDの移転元600dにBC1上のユーザU1が設定され、移転先600eにBC2上のユーザU2が設定されていれば、制御部は、遠隔取引が必要と判断する。

[0109] ステップS708では、制御部は、遠隔取引実行のための優先順位を決定する（ステップS708）。この優先順位は、上述したように、各処理ノードA～C（100）の制御部が、それぞれ取引データDを用いた所定の演算により算出する。

[0110] 次に、制御部は、自身の処理ノード100の優先順位であるかを判断する（ステップS709）。ここで、制御部は、ステップS708で算出した優先順位により、自処理ノード100および他の処理ノード100の優先順位を認識しており、署名サーバ150に対する署名要求を行う順番を優先順位にしたがい行う。

[0111] 判断結果、制御部は、自身の処理ノード100の優先順位であれば（ステップS709：Yes）、ステップS711の処理に移行する。一方、自身の処理ノード100の優先順位でなければ（ステップS709：No）、自身の処理ノード100の順番が来るまで待機し（ステップS710）、ステップS709の処理に戻る。ここで、制御部は、自身の処理ノード100の順番であるか否かは、現時点で自処理ノード100が最も高い優先順位であ

るか否かに基づき判断する。

[0112] より詳細には、自身よりも上位の処理ノード100が遠隔取引を実行した後のタイムアウト発生により、次位の優先順位の処理ノード100が自身であるか否かを判断する。例えば、遠隔処理を実行した処理ノード100は、遠隔取引の実行時に所定時間のタイマを起動させ、BC2からの返答がタイムアウトした時、遠隔取引が失敗した旨をBC1の第1の分散台帳（ローカル台帳）に記録する。他の処理ノード100は、定期的にローカル台帳を参照することで、遠隔取引の実行状態を判断でき、優先順位にしたがい自身の処理ノード100が遠隔取引の実行順であるか否かを判断できる。

[0113] ステップS711では、制御部は、署名サーバ150に遠隔取引実行の承認を依頼する（ステップS711）。具体的には、制御部は、自身の処理ノード100が遠隔取引を実行するために必要な署名を署名サーバ150に署名要求する。次に、制御部は、遠隔取引が承認されたか否かを判断する（ステップS712）。具体的には、制御部は、署名サーバ150への署名要求が承認されたか否かを判断する。

[0114] 判断の結果、遠隔取引が承認されれば（ステップS712：Yes）、制御部は、ステップS713の処理に移行する。一方、遠隔取引が承認されなければ（ステップS712：No）、制御部は、現時点では自身の処理ノード100による実行順ではないと判断し、以上の処理を終了する。

[0115] ステップS713では、制御部は、取引データDに基づきBC2に対する遠隔取引を実行する（ステップS713）。次に、制御部は、遠隔取引が処理タイムアウトであるか否かを判断する（ステップS714）。ここで、遠隔取引の実行がタイムアウト時間が経過するまでの間に完了した場合には（ステップS714：No）、ステップS715の処理に移行する。一方、制御部は、遠隔取引の実行後、タイムアウト時間が経過しても処理が完了しない場合には（ステップS714：Yes）、遠隔取引が完了しない（失敗）の旨をBC1上の分散台帳に記録し、以上の処理を終了する。

[0116] ステップS715では、制御部は、実行した遠隔取引の結果をローカル台

帳に記録し（ステップS715）、以上の処理を終了する。

[0117] 図8は、実施の形態にかかる署名サーバが行う処理例を示すフローチャートである。署名サーバ150の制御部（図3のCPU301）は、処理ノードA～C（100）からの署名要求の受信毎に以下に示す処理を実行する。

[0118] はじめに、制御部は、処理ノードA～C（100）から署名要求を受信する（ステップS801）。各処理ノードA～C（100）は、正常時には、優先順位にしたがって一つの処理ノード100からのみ署名要求を受信する。

[0119] 次に、制御部は、署名要求に含まれる元になった取引データDから各処理ノードA～C（100）の優先順位を決定する（ステップS802）。署名サーバ150の制御部は、各処理ノードA～C（100）の制御部と同一の演算により優先順位を決定するため、署名サーバ150側で決定した優先順位は、各処理ノードA～C（100）側で決定した優先順位と同じになる。

[0120] 次に、制御部は、署名要求した処理ノード100は、優先順位内で担当の処理ノードであるか否かを判断する（ステップS803）。ここで、制御部は、署名要求した処理ノード100が現時点で遠隔処理を実行する最上位の優先順位であるかを判断する。

[0121] 判断結果、署名要求した処理ノード100が優先順位内で担当の処理ノードであれば（ステップS803：Yes）、制御部は、ステップS804の処理に移行する。一方、署名要求した処理ノード100が優先順位内で担当の処理ノードでなければ（ステップS803：No）、制御部は、ステップS806の処理に移行する。

[0122] ステップS804では、制御部は、署名要求に含まれる取引データDに承認用の署名（電子署名）を付与する（ステップS804）。次に、制御部は、承認済みの取引データDを署名要求した処理ノード100に返答し（ステップS805）、以上の処理を終了する。ステップS806では、現時点で署名要求した処理ノード100が優先順位内で担当の処理ノードでないため、この署名要求した処理ノード100にエラー発生を返答し（ステップS8

06)、以上の処理を終了する。承認済みの取引データDを受信した処理ノード100は、遠隔取引を実行する。一方、エラー返答を受けた処理ノード100は、エラー返答により遠隔取引の待機状態となる。

[0123] (優先順位決定の他の方法)

図9は、遠隔取引を実行する優先順位の他の決定方法を説明する図である。上述した実施の形態では、各処理ノードA~C(100)が取引データDのデータ内容を用いた同一の演算により、優先順位を決定した。これ以外の他の優先順位の決定方法を説明する。

[0124] 各処理ノードA~C(100)は、取引データDの取引を検証した際にタイムスタンプ(時刻)を署名として取引データDに付与する。図9の例では、BC1上で遠隔取引のための取引内容(図6の移転量に相当する「金額」、移転元および移転先に対応する「口座a→口座b」等)が設定された取引データDが発生したとする。

[0125] この取引データDを各処理ノードA~C(100)が承認した際(図7のステップS703の処理相当)、各処理ノードA~C(100)は、取引データDを承認した旨のタイムスタンプを付与する。

[0126] 図9の符号D1は、各処理ノードA~C(100)が取引データDの承認結果であり、例えば、BC1上で各処理ノードA~C(100)が共有する上記ブロックデータD1に相当する。このブロックデータD1上のタイムスタンプが早い順番は、処理ノードB, C, Aであるとする。この場合、各処理ノードA~C(100)は、遠隔取引の発行を処理ノードB, C, Aの順に試行することができる。

[0127] 図9で説明した優先順位の決定によれば、各処理ノードA~C(100)、および署名サーバ150において、取引データDを用いた所定の演算による優先順位の決定の処理を行う必要がない。なお、図9の如く、タイムスタンプを用いた優先順位の情報(ブロックデータD1)を署名サーバ150が共有することで、署名サーバ150においても、タイムスタンプの順に各処理ノードA~C(100)からの署名要求をダブルチェックすることができ

る。

[0128] 以上説明した実施の形態によれば、第1のブロックチェーンに冗長構成で配置される複数の処理ノード100は、それぞれが記憶する第1のブロックチェーン上での第1の取引に関する取引データの発生を検知する。検知した取引データに基づき、第1の取引後に行うべき第2の取引を第2のブロックチェーンに送信するか否かを制御する。これにより、第1のブロックチェーン上の複数の処理ノードが同じ取引データを共有できる。第1のブロックチェーンに複数の処理ノードを冗長構成で配置することで、取引データに基づいて、いずれか一つの処理ノードにより第2の取引を確実に実行できるようになる。

[0129] また、複数の処理ノード100は、それぞれが取引データのデータ内容に基づき、複数の処理ノードによる第2の取引（例えば、BC2への遠隔取引）の実行の優先順位を決定する。自処理ノードの優先順位が最上位であれば、第2の取引を第2のブロックチェーンに送信し、自処理ノードの優先順位が次位以下であれば、第2の取引を第2のブロックチェーンに送信することを待機する。これにより、複数の処理ノードがそれぞれ共有する取引データに基づき優先順位を自律的に決定することができ、冗長構成における特別な排他制御を不要にできる。また、取引データのデータ内容に基づいて優先順位を決定するため、新たな取引データ毎に優先順位が異なって最上位の処理ノードが決定されることとなる。これにより、第2の取引の実行にかかる処理負担を複数の処理ノードで均等に分散できる水平処理スケールアップを実現できるようになる。

[0130] また、複数の処理ノード100は、自処理ノードB、Cの優先順位が次位以下であり、第2の取引を実行した処理ノードAでのタイムアウトが発生したとする。この場合、タイムアウト発生時に、自処理ノードBの優先順位が最上位であれば、第2の取引を第2のブロックチェーンに送信する処理を実行する。これにより、遠隔取引を実行した処理ノードAが故障や通信等の障害で遠隔取引を完了できない場合に、優先順位に基づき、次位以下の処理ノ

ードによる遠隔取引を継続できるようになる。

[0131] また、複数の処理ノード100は、それぞれが取引データのデータ内容に対するハッシュ演算を行うことで、自処理ノードおよび他処理ノードにおける第2の取引の実行の優先順位を決定してもよい。これにより、複数の処理ノードは、共有する取引データに基づき、自処理ノードおよび他処理ノードの優先順位を識別でき、この優先順位にしたがった遠隔取引を実行できるようになる。

[0132] また、複数の処理ノード100は、それぞれが取引データの検知時にタイムスタンプを付与し、タイムスタンプの時刻の順序に基づき、自処理ノードおよび他処理ノードにおける第2の取引の実行の優先順位を決定してもよい。これにより、複数の処理ノードは、共有する取引データに基づき、自処理ノードおよび他処理ノードの優先順位を識別でき、この優先順位にしたがった遠隔取引を実行できるようになる。

[0133] また、複数の処理ノード100は、第2の取引の発生時に、署名サーバ150に対し取引データの署名要求を行い、署名サーバからの署名許可を受けて第2の取引を行い、署名サーバからの署名許可がない場合には第2の取引を待機する、処理を実行してもよい。例えば、署名サーバにおいても、処理ノードと同様に取引データに基づく優先順位を決定することで、処理ノードで決定した遠隔取引の実行順序を署名サーバ150でもダブルチェックでき、遠隔取引を確実に実行できるようになる。

[0134] 以上のことから、実施の形態によれば、第1のブロックチェーンと第2のブロックチェーンとを連携させた遠隔取引を行う場合において、ブロックチェーンの処理ノードの冗長化による取引の確実性を得ることができる。また、冗長化した構成であっても複数の処理ノードが自律的に優先順位に基づく遠隔取引を実行することで、複数のブロックチェーン間の特別な排他制御を不要にでき、各処理ノードは、簡単な処理で遠隔処理を実行できるようになる。

[0135] なお、本発明の実施の形態で説明した制御方法は、予め用意されたプログ

ラムをサーバ等のプロセッサに実行させることにより実現することができる。本制御方法は、ハードディスク、フレキシブルディスク、CD-ROM (Compact Disc-Read Only Memory)、DVD (Digital Versatile Disk)、フラッシュメモリ等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。また本制御方法は、インターネット等のネットワークを介して配布してもよい。

符号の説明

- [0136] 100 処理ノード
- 150 署名サーバ
- 200 SC (スマートコントラクト)
- 201 連携シナリオ記憶手段
- 202 連携シナリオ実行手段
- 203 トリガー監視手段
- 211 遠隔取引受付手段
- 212 トリガー取引参照手段
- 213 実行優先順位決定手段
- 214 承認署名取得手段
- 215 遠隔取引発行手段
- 216 タイムアウト計時手段
- 221 トリガー取引参照手段
- 222 署名許可ルール記憶手段
- 223 実行優先順位決定手段
- 224 承認署名付与手段
- 301 CPU
- 302 メモリ
- 303 ネットワークインタフェース
- 305 記録媒体

- 310 ネットワーク
- BC1 第1のブロックチェーン
- BC2 第2のブロックチェーン
- D 取引データ

請求の範囲

- [請求項1] 第1のブロックチェーンに冗長構成で配置される複数の処理ノードの制御方法であって、
複数の前記処理ノードは、
それぞれが記憶する前記第1のブロックチェーン上での第1の取引に関する取引データの発生を検知し、
前記検知した取引データに基づき、前記第1の取引後に行うべき第2の取引を第2のブロックチェーンに送信するか否かを制御する、
処理を実行することを特徴とする制御方法。
- [請求項2] 複数の前記処理ノードは、
それぞれが前記取引データのデータ内容に基づき、複数の前記処理ノードによる前記第2の取引の実行の優先順位を決定し、
自処理ノードの前記優先順位が最上位であれば、前記第2の取引を前記第2のブロックチェーンに送信し、
自処理ノードの前記優先順位が次位以下であれば、前記第2の取引を前記第2のブロックチェーンに送信することを待機する、
処理を実行することを特徴とする請求項1に記載の制御方法。
- [請求項3] 複数の前記処理ノードは、
自処理ノードの前記優先順位が次位以下であり、前記第2の取引を実行した前記処理ノードでのタイムアウト発生時には、
前記タイムアウト発生時に、自処理ノードの前記優先順位が最上位であれば、前記第2の取引を前記第2のブロックチェーンに送信する、
処理を実行することを特徴とする請求項2に記載の制御方法。
- [請求項4] 複数の前記処理ノードは、
それぞれが前記取引データの前記データ内容に対するハッシュ演算を行うことで、自処理ノードおよび他処理ノードにおける前記第2の取引の実行の優先順位を決定する、

処理を実行することを特徴とする請求項 2 に記載の制御方法。

[請求項5]

複数の前記処理ノードは、

それぞれが前記取引データの前記検知時にタイムスタンプを付与し、前記タイムスタンプの時刻の順序に基づき、自処理ノードおよび他処理ノードにおける前記第 2 の取引の実行の優先順位を決定する、
処理を実行することを特徴とする請求項 2 に記載の制御方法。

[請求項6]

複数の前記処理ノードは、

前記第 2 の取引の発生時に、署名サーバに対し前記取引データの署名要求を行い、
前記署名サーバからの署名許可を受けて前記第 2 の取引を行い、
前記署名サーバからの署名許可がない場合には前記第 2 の取引を待機する、
処理を実行することを特徴とする請求項 1 に記載の制御方法。

[請求項7]

前記署名サーバは、

前記取引データのデータ内容に基づき、複数の前記処理ノードによる前記第 2 の取引の実行の優先順位を決定し、
前記署名要求を行った前記処理ノードの前記優先順位が最上位であれば、前記署名要求を署名許可し、
前記署名要求を行った前記処理ノードの前記優先順位が次位以下であれば、前記署名要求を署名許可しない、
処理を実行することを特徴とする請求項 6 に記載の制御方法。

[請求項8]

第 1 のブロックチェーンに冗長構成で配置される複数の処理ノードのコンピュータが実行する制御プログラムであって、
複数の前記処理ノードのコンピュータに、
それぞれが記憶する前記第 1 のブロックチェーン上での第 1 の取引に関する取引データの発生を検知させ、
検知した前記取引データに基づき、前記第 1 の取引後に行うべき第 2 の取引を第 2 のブロックチェーンに送信するか否かを制御させる、

処理を実行させることを特徴とする制御プログラム。

[請求項9]

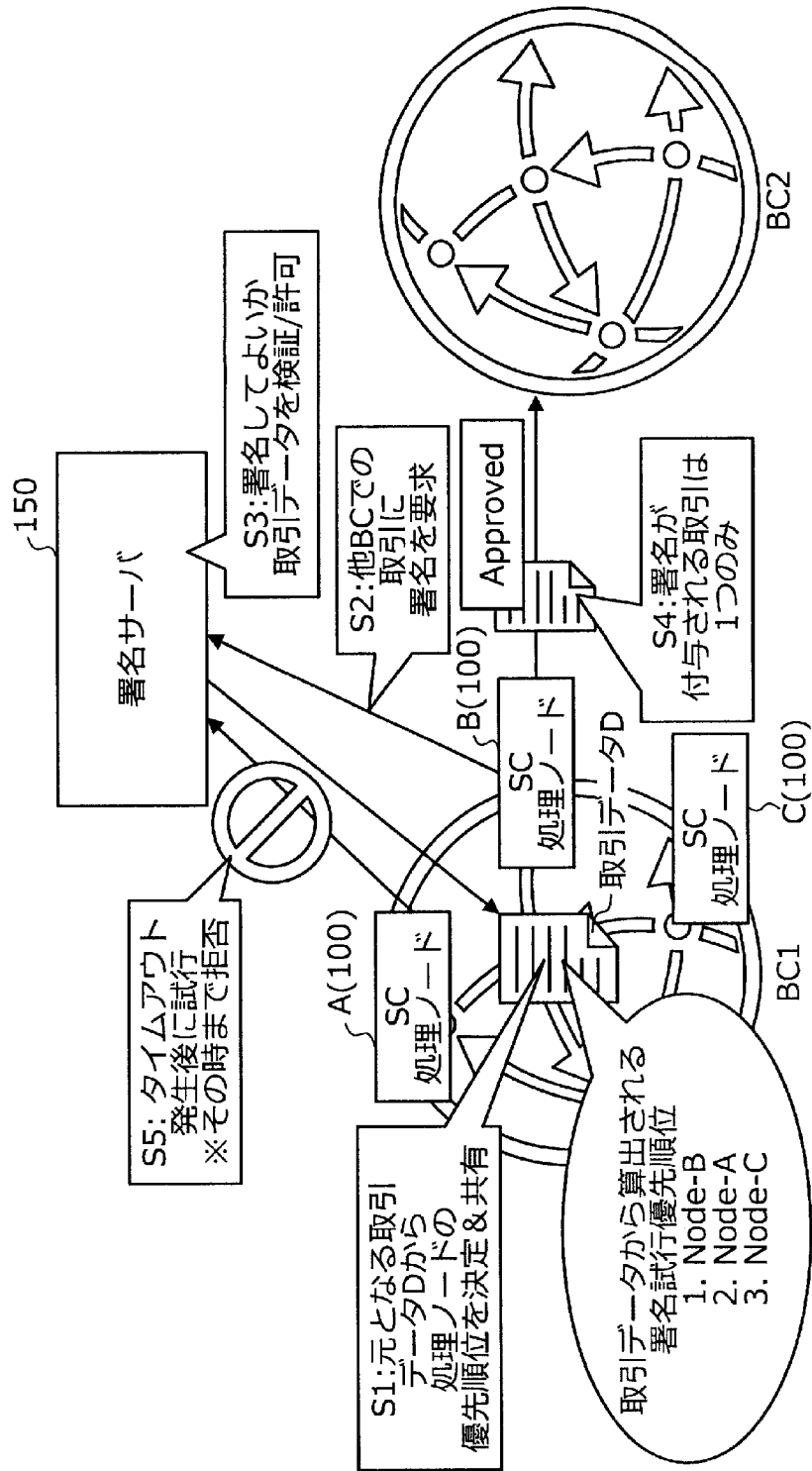
第1のブロックチェーンに冗長構成で配置される複数の処理ノードを構成する情報処理装置であって、

前記第1のブロックチェーン上での第1の取引に関する取引データの発生を検知し、

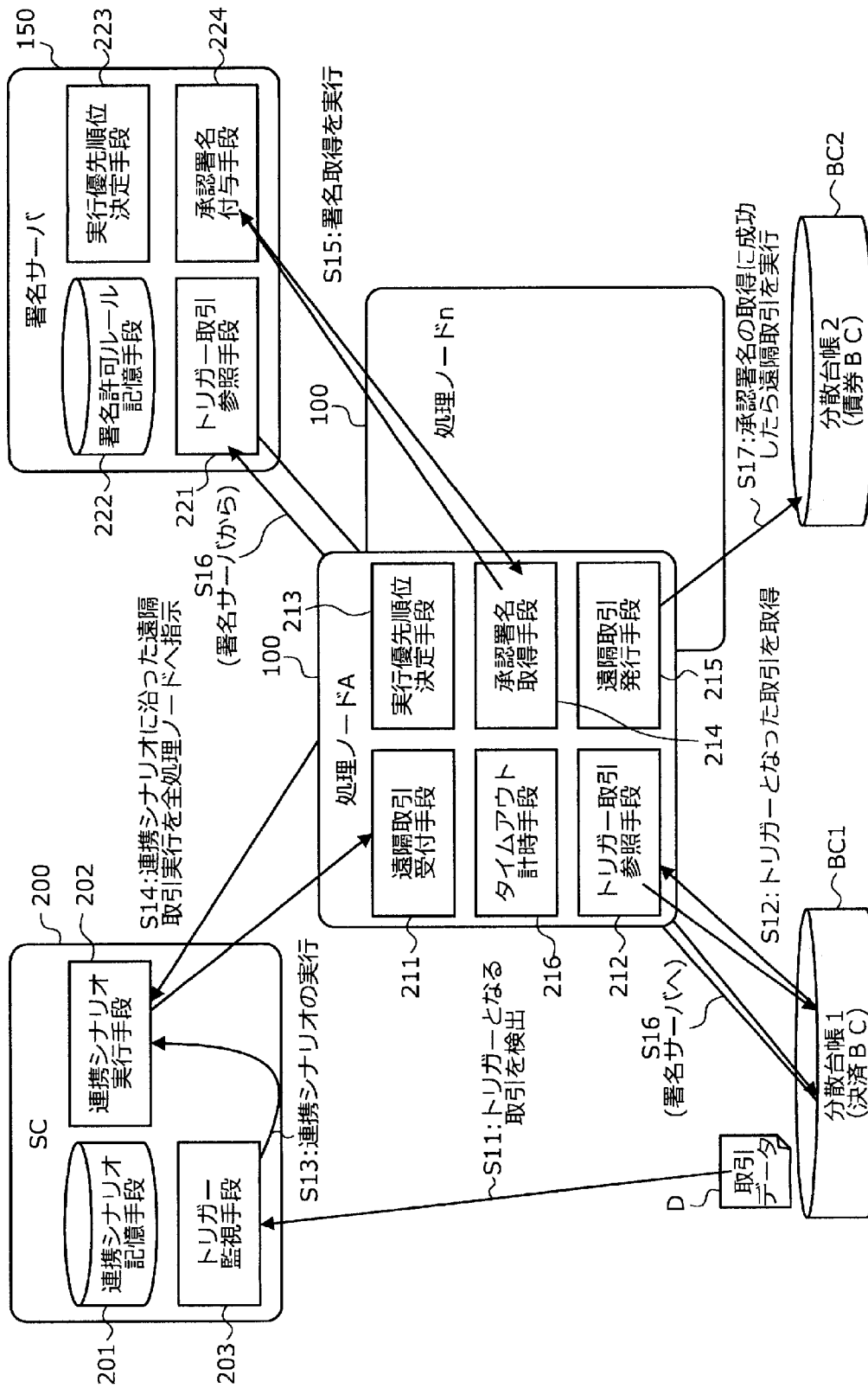
検知した前記取引データに基づき、前記第1の取引後に行うべき第2の取引を第2のブロックチェーンに送信するか否かを制御する制御部、

を備えたことを特徴とする情報処理装置。

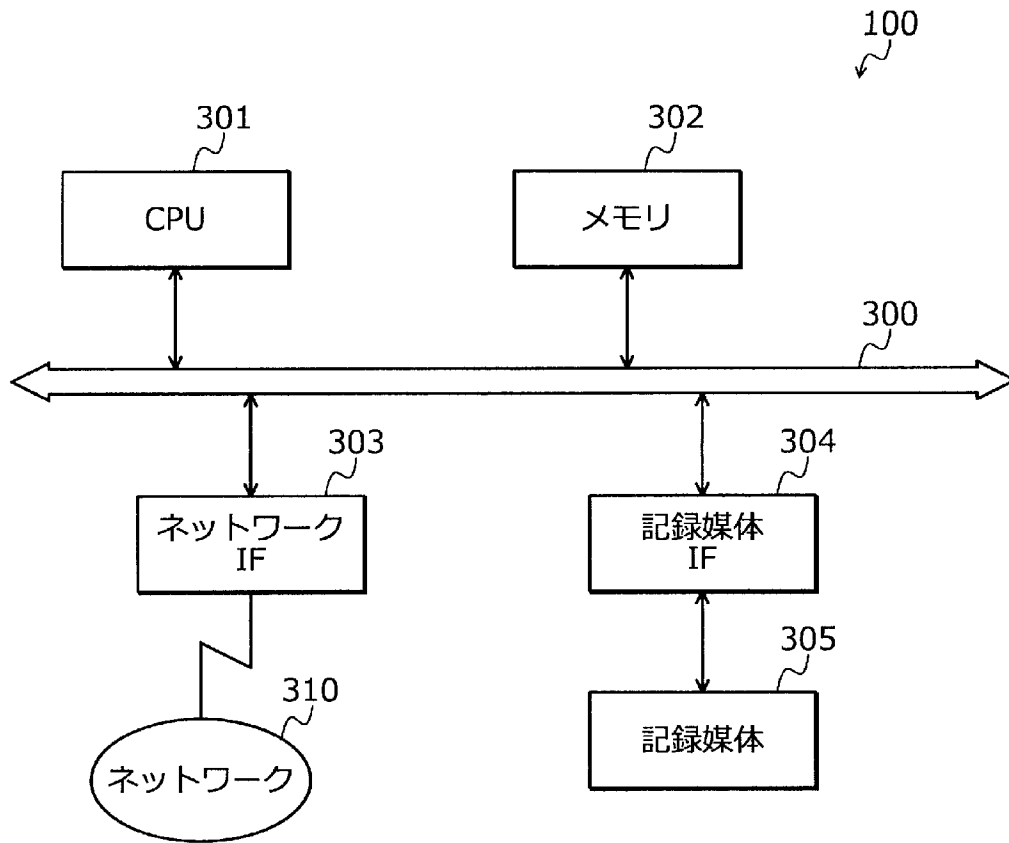
[図1]



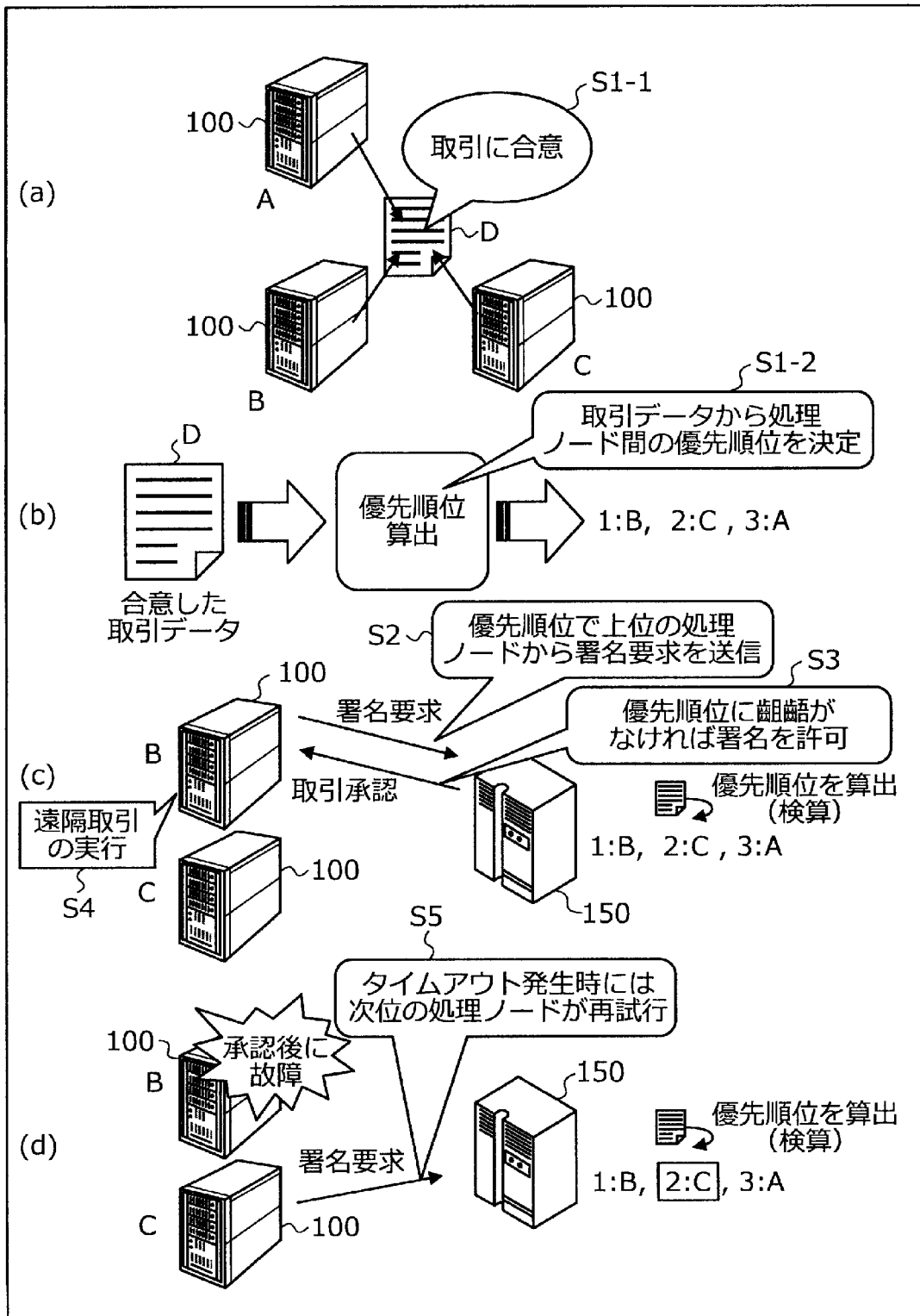
[図2]



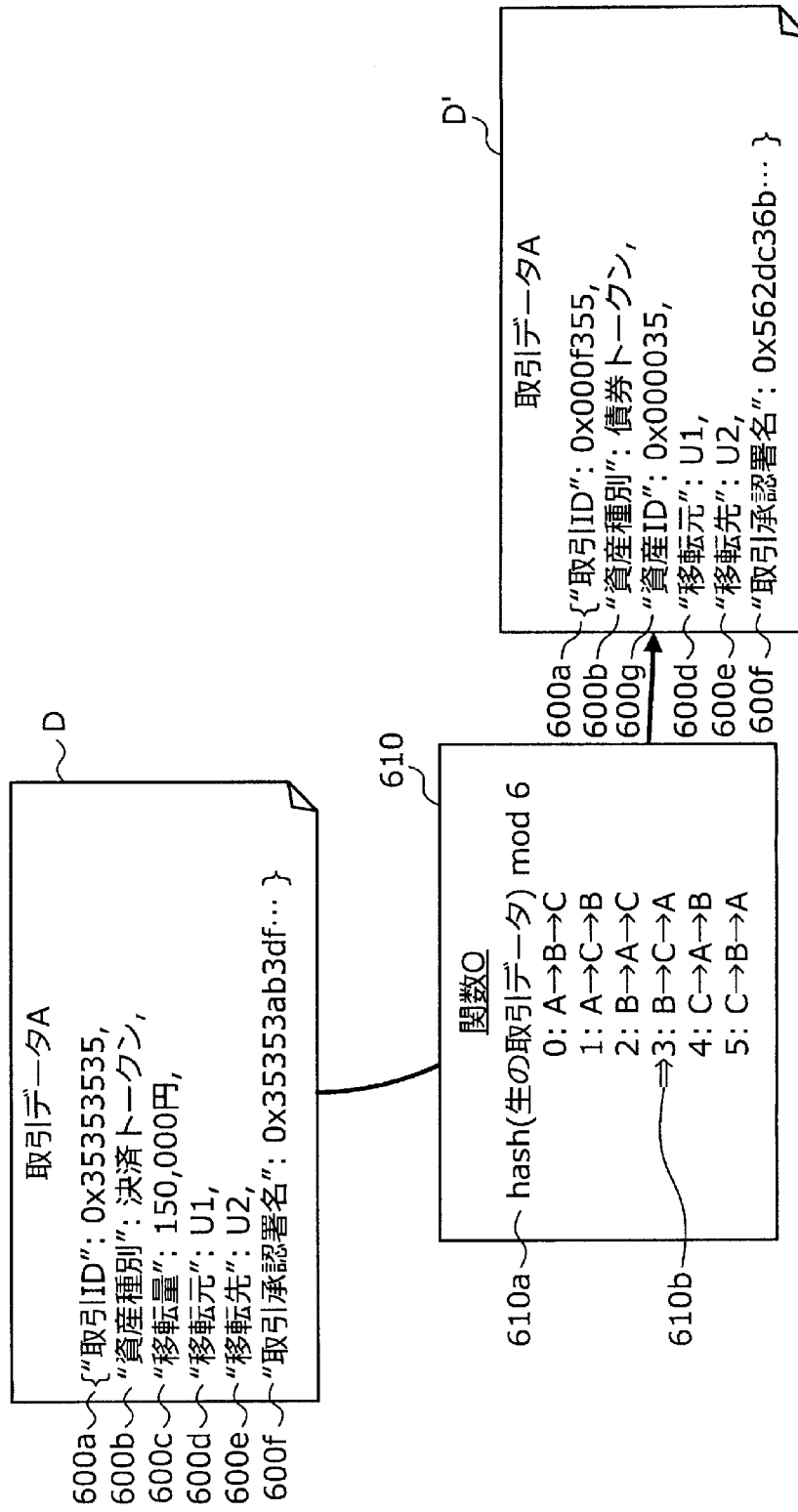
[図3]



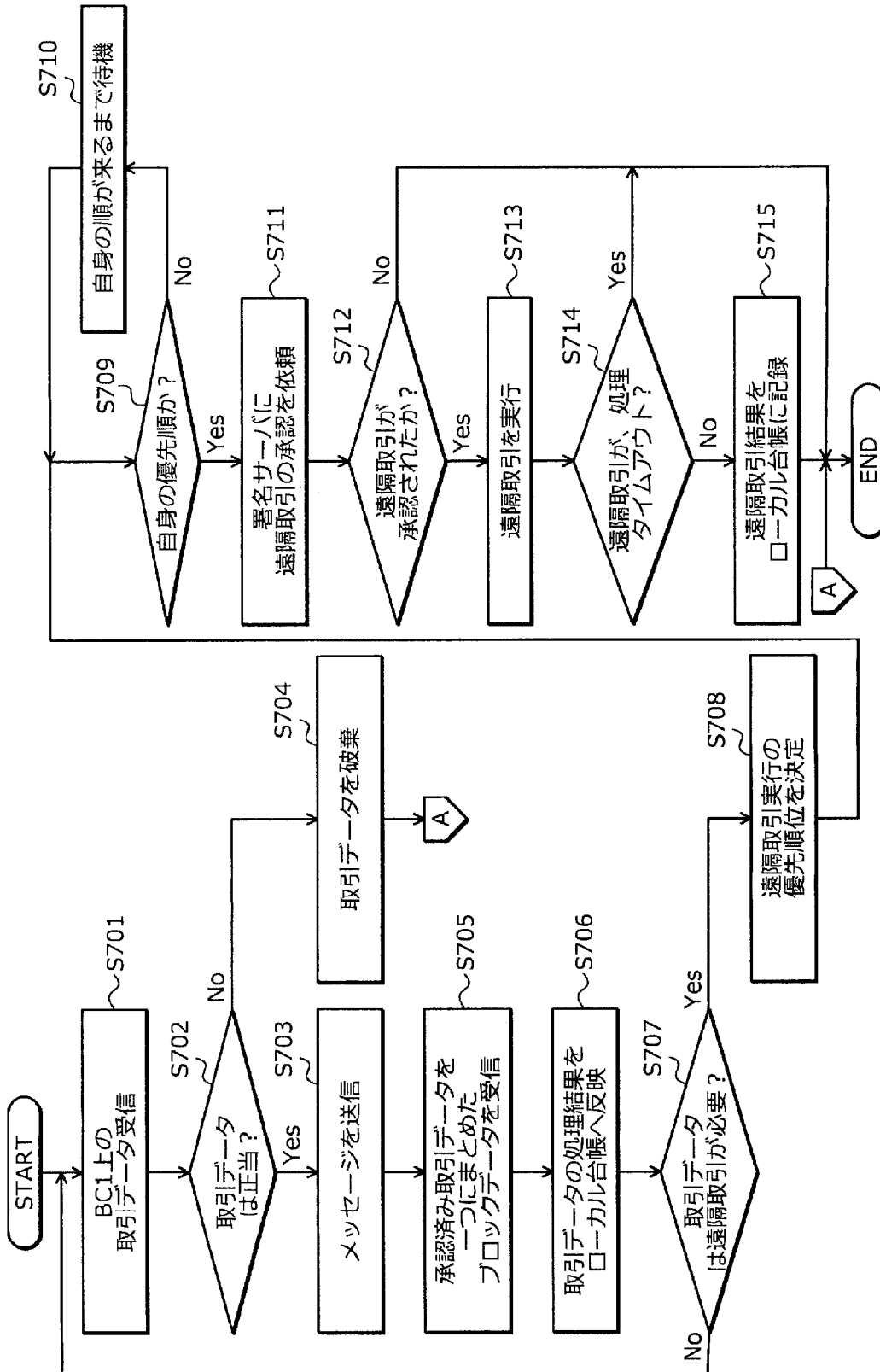
[図4]



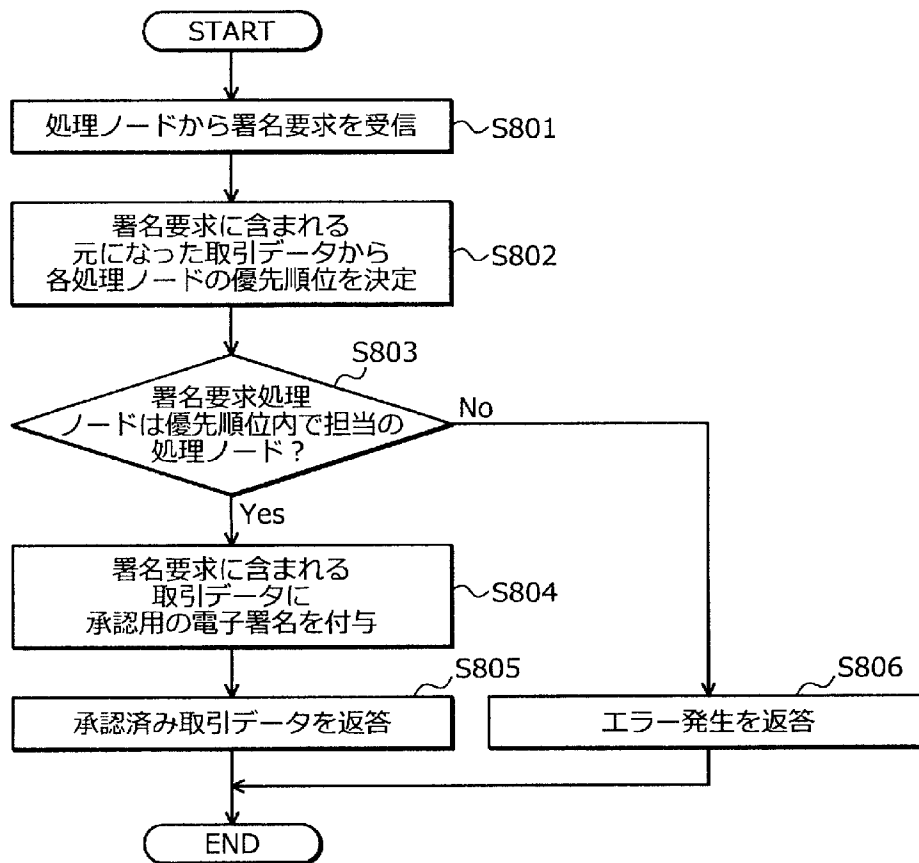
[図6]



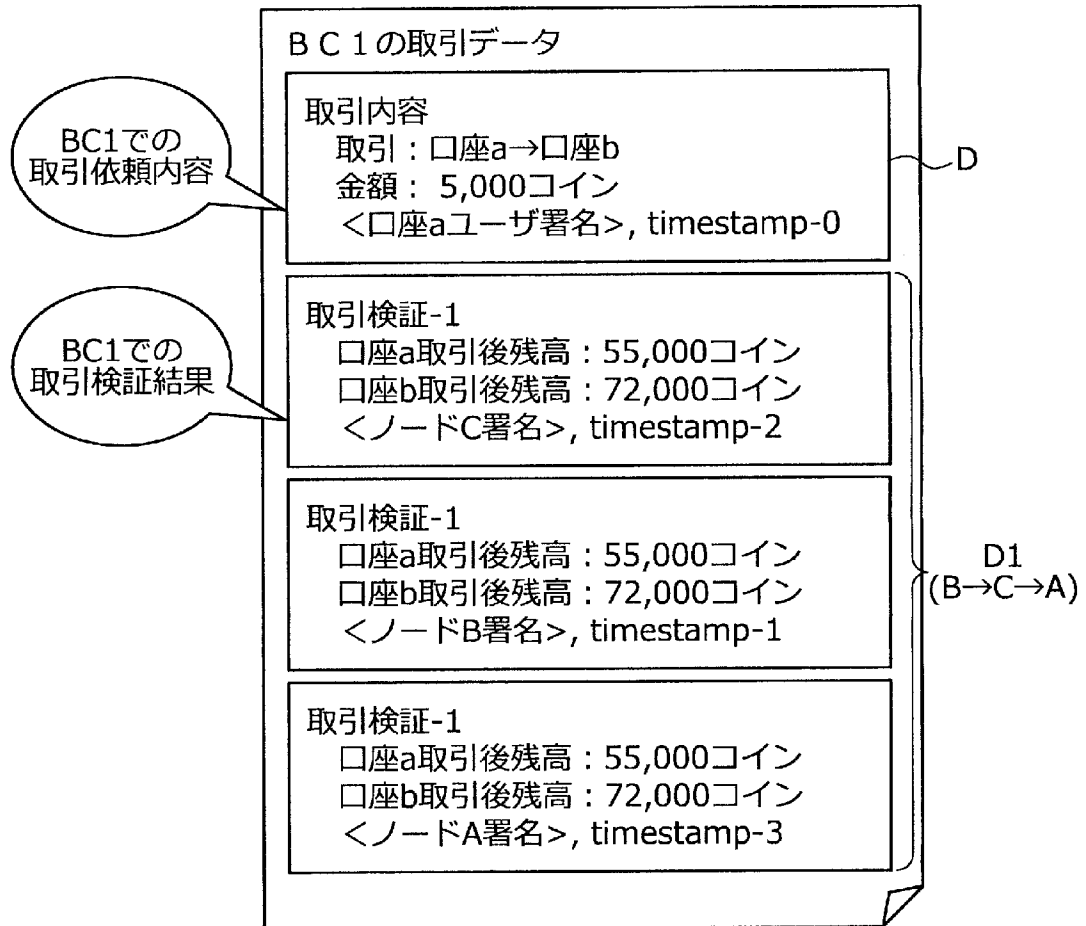
[図7]



[図8]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/019003

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. G06F11/20 (2006.01) i, G06Q20/38 (2012.01) i
 FI: G06F11/20 620, G06Q20/38 310

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)

Int. Cl. G06F11/16-11/20, G06Q10/10-50/20, G06Q50/26-99/00, G16Z99/00,
 G09C1/00-5/00, H04K1/00-3/00, H04L9/00-9/32, G06F16/00-16/958, G06F12/14,
 G06F21/00-21/88, G06F11/07, G06F11/28-11/36, G06F11/14

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 1971-2020
 Registered utility model specifications of Japan 1996-2020
 Published registered utility model applications of Japan 1994-2020

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.
A	東角芳樹, 竹内琢磨, 藤本真吾. パブリックチェーンとコンソーシアムチェーンとの安全な連携方式の提案. 2019年暗号と情報セキュリティシンポジウム (SCIS2019) 予稿集 [USB]. 15 January 2019, no. 2G4-3, pp. 1-7, p. 5, left column, line 11 to p. 5, right column, line 12, fig. 10, non-official translation (HIGASHIKADO, Yoshiki, TAKEUCHI, Takuma, FUJIMOTO, Shingo. Proposal for Secure Linkage Method for Public Chains and Consortium Chains. Proceedings of the 2019 Symposium on Cryptography and Information Security (SCIS2019) [USB].)	1-9
A	JP 2019-53712 A (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 04 April 2019, paragraphs [0100]-[0111], fig. 10	1-9

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
29.09.2020

Date of mailing of the international search report
06.10.2020

Name and mailing address of the ISA/
 Japan Patent Office
 3-4-3, Kasumigaseki, Chiyoda-ku,
 Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/019003

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FUJIMOTO, Shingo. HIGASHIKADO, Yoshiki. TAKEUCHI, Takuma. ConnectionChain the Secure Interworking of Blockchains. Proceedings of Sixth International Conference on Internet of Things Systems, Management and Security (IOTSMS), 22 October 2019, pp. 514-518, in particular, p. 515, right column, line 13 to p. 516, left column, line 22	1-9
A	WATANABE, Hiroki. OHASHI, Shigenori. FUJIMURA, Shigeru. KISHIGAMI, Jay. Niji: Autonomous Payment Bridge between Bitcoin and Consortium Blockchain. Proceedings of International Conference on Internet of Things. Green Computing and Communications. Cyber. Physical and Social Computing. Smart Data. Blockchain. Computer and Information Technology. Congress on Cybermatics, 30 July 2018, pp. 1448-1455, in particular, p. 1450, right column, line 8 to p. 1451, left column, line 13	1-9

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/019003

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
JP 2019-53712 A	04.04.2019	US 2019/0088063 A1 paragraphs [0117]- [0128], fig. 10 EP 3457622 A1 CN 109509287 A	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 11/20(2006.01)i; G06Q 20/38(2012.01)i FI: G06F11/20 620; G06Q20/38 310		
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）） G06F11/16-11/20, G06Q10/10-50/20, G06Q50/26-99/00, G16Z99/00, G09C1/00-5/00, H04K1/00-3/00, H04L9/00-9/32, G06F16/00-16/958, G06F12/14, G06F21/00-21/88, G06F11/07, G06F11/28-11/36, G06F11/14 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 1971-2020年 日本国実用新案登録公報 1996-2020年 日本国登録実用新案公報 1994-2020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
A	東角芳樹, 竹内琢磨, 藤本真吾, パブリックチェーンとコンソーシアムチェーンとの安全な連携方式の提案, 2019年暗号と情報セキュリティシンポジウム(SCIS2019)予稿集[USB], 2019.01.15, No.2G4-3, pp.1-7 特にp.5, 左欄, 第11行-p.5, 右欄, 第12行, 図10	1-9
A	JP 2019-53712 A (パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ) 04.04.2019 (2019-04-04) 段落[0100]-[0111], 図10	1-9
A	FUJIMOTO, Shingo, HIGASHIKADO, Yoshiki, TAKEUCHI, Takuma, ConnectionChain : the Secure Interworking of Blockchains, Proceedings of Sixth International Conference on Internet of Things : Systems, Management and Security (IOTSMS), 2019.10.22, pp.514-518 特にp.515, 右欄, 第13行-p.516, 左欄, 第22行	1-9
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input checked="" type="checkbox"/> 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	“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	
“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		
国際調査を完了した日	国際調査報告の発送日	
29.09.2020	06.10.2020	
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） 清木 泰 5B 9643 電話番号 03-3581-1101 内線 3545	

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
A	WATANABE, Hiroki, OHASHI, Shigenori, FUJIMURA, Shigeru, KISHIGAMI, Jay, Niji : Autonomous Payment Bridge between Bitcoin and Consortium Blockchain, Proceedings of International Conference on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, 2018.07.30, pp.1448-1455 特にp.1450, 右欄, 第8行-p.1451, 左欄, 第13行	1-9

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/JP2020/019003

引用文献	公表日	パテントファミリー文献	公表日
JP 2019-53712 A	04.04.2019	US 2019/0088063 A1 段落[0117]-[0128], 図10 EP 3457622 A1 CN 109509287 A	