

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2020-46961

(P2020-46961A)

(43) 公開日 令和2年3月26日(2020.3.26)

(51) Int.Cl.
G06Q 20/38 (2012.01)F I
G06Q 20/38 310テーマコード (参考)
5L055

審査請求 未請求 請求項の数 5 O L (全 18 頁)

(21) 出願番号 特願2018-175132 (P2018-175132)
(22) 出願日 平成30年9月19日(2018.9.19)(71) 出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号
(74) 代理人 100107766
弁理士 伊東 忠重
(74) 代理人 100070150
弁理士 伊東 忠彦
(72) 発明者 島 常和
石川県金沢市増泉3丁目4番30号 株式会社富士通北陸システムズ内
(72) 発明者 小暮 淳
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
Fターム(参考) 5L055 AA71

(54) 【発明の名称】 取引管理装置、取引管理方法及び取引管理プログラム

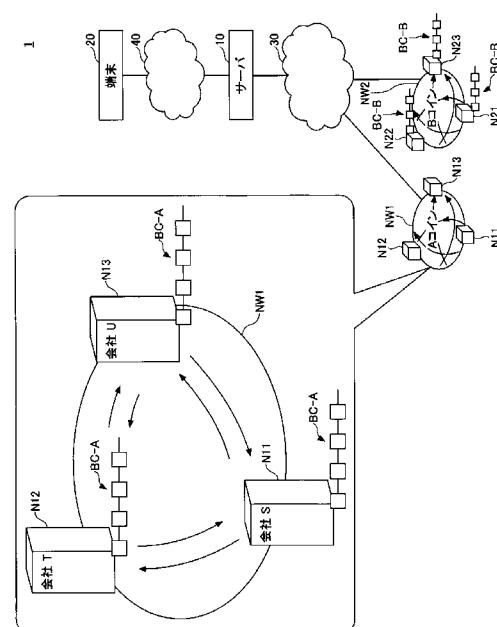
(57) 【要約】

【課題】異なるブロックチェーンネットワークのブロックチェーン間での価値移転の取引の進捗を把握する。

【解決手段】異なるブロックチェーンネットワーク間において一のブロックチェーンの対象データと他のブロックチェーンの対象データとの間で価値の移転を実行する取引実行部と、前記価値の移転にかかる前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けて記憶した記憶部を参照して、各ブロックチェーンの対象データの価値の移転の確定状態を監視する監視部と、を有する取引管理装置が提供される。

【選択図】 図1

一実施形態に係る取引管理システムの全体構成の一例を示す図



【特許請求の範囲】**【請求項 1】**

異なるブロックチェーンネットワーク間において一のブロックチェーンの対象データと他のブロックチェーンの対象データとの間で価値の移転を実行する取引実行部と、

前記価値の移転にかかる前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けて記憶した記憶部を参照して、各ブロックチェーンの対象データの価値の移転の確定状態を監視する監視部と、
を有する取引管理装置。

【請求項 2】

前記監視部は、

前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けてユーザ毎に記憶した前記記憶部を参照して、ユーザ毎の各ブロックチェーンの対象データの価値の移転の確定状態を監視する、

請求項 1 に記載の取引管理装置。

【請求項 3】

前記監視部は、

監視した前記各ブロックチェーンの対象データの価値の移転の確定状態に基づき、前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とにより対応付けられたブロックチェーンの対象データのいずれかの価値の移転が確定していないと判定した場合、前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とにより対応付けられた確定しているブロックチェーンの対象データの価値の移転をキャンセルした状態におけるユーザ毎の各ブロックチェーンの対象データの価値を参照させる、

請求項 2 に記載の取引管理装置。

【請求項 4】

異なるブロックチェーンネットワーク間において一のブロックチェーンの対象データと他のブロックチェーンの対象データとの間で価値の移転を実行し、

前記価値の移転にかかる前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けて記憶した記憶部を参照して、各ブロックチェーンの対象データの価値の移転の確定状態を監視する、

処理をコンピュータが実行する取引管理方法。

【請求項 5】

異なるブロックチェーンネットワーク間において一のブロックチェーンの対象データと他のブロックチェーンの対象データとの間で価値の移転を実行し、

前記価値の移転にかかる前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けて記憶した記憶部を参照して、各ブロックチェーンの対象データの価値の移転の確定状態を監視する、

処理をコンピュータに実行させる取引管理プログラム。

【発明の詳細な説明】**【技術分野】****【0001】**

本開示は、取引管理装置、取引管理方法及び取引管理プログラムに関する。

【背景技術】**【0002】**

P2Pネットワークに流通しているブロックチェーンデータから取得される、評価対象に関する対象データに基づいて、評価対象を評価する技術が知られている（例えば、特許文献 1 参照）。ブロックチェーンデータとしては、例えば、ビットコイン等の仮想通貨のデータのやり取りに用いられるブロックチェーンデータが挙げられる。

【先行技術文献】**【特許文献】**

10

20

30

40

50

【0003】

【特許文献1】国際公開第2017/090329号パンフレット

【発明の概要】

【発明が解決しようとする課題】

【0004】

異なるブロックチェーンネットワークの一方のブロックチェーンから他方のブロックチェーンに仮想通貨等の対象データの価値の移転（例えば両替）を行うと、各ブロックチェーンのブロック上のトランザクション処理は非同期で確定する。また、各ブロックチェーン上でトランザクション処理を実行してからその処理が確定するまでの時間は異なる。そのため、任意のタイミングで対象データの残高（価値の総量）を参照すると、実際よりも残高が多くなったり、少なくなったりする場合がある。例えば、出金側の仮想通貨のブロックチェーンでの処理が入金側の仮想通貨のブロックチェーンでの処理よりも早く確定すると、一時的に総資産が少なくなる。

10

【0005】

本発明では、異なるブロックチェーンネットワークのブロックチェーン間での価値移転の取引の進捗を把握できる手法を提供する。

【課題を解決するための手段】

【0006】

1つの実施態様では、異なるブロックチェーンネットワーク間において一のブロックチェーンの対象データと他のブロックチェーンの対象データとの間で価値の移転を実行する取引実行部と、前記価値の移転にかかる前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けて記憶した記憶部を参照して、各ブロックチェーンの対象データの価値の移転の確定状態を監視する監視部と、を有する取引管理装置が提供される。

20

【発明の効果】

【0007】

1つの側面では、本開示は、異なるブロックチェーンネットワークのブロックチェーン間での価値移転の取引の進捗を把握できる。

【図面の簡単な説明】

【0008】

30

【図1】一実施形態に係る取引管理システムの全体構成の一例を示す図。

【図2】ブロックチェーンを説明する図。

【図3】異なるブロックチェーンネットワーク間におけるブロックチェーン間での価値移転を説明する図。

【図4】一実施形態に係るサーバ及び端末の機能構成の一例を示す図。

【図5】一実施形態に係る取引確定テーブル及び取引中テーブルの一例を示す図。

【図6】一実施形態に係るサーバのハードウェア構成の一例を示す図。

【図7】一実施形態に係る価値移転及び参照処理の一例を示すフローチャート。

【図8】一実施形態に係る価値移転処理の一例を示すフローチャート。

【図9】一実施形態に係る価値移転処理を説明する図。

40

【図10】一実施形態に係る取引実行処理の一例を示すフローチャート。

【図11】一実施形態に係る参照処理の一例を示すフローチャート。

【図12】一実施形態に係る参照処理を説明する図。

【発明を実施するための形態】

【0009】

以下、一実施形態について添付の図面を参照しながら説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複した説明を省く。

【0010】

〔取引管理システムの全体構成〕

50

まず、一実施形態に係る取引管理システム 1 の構成の一例について、図 1 を参照しながら説明する。図 1 は、一実施形態に係る取引管理システム 1 の全体構成の一例を示す図である。一実施形態に係る取引管理システム 1 は、サーバ 10 及び端末 20 を有する。

【0011】

サーバ 10 は、ネットワーク 40 を介してユーザ（ブロックチェーン利用者）の端末 20 に接続されている。サーバ 10 は、インターネット等のネットワーク 30 を介して複数の異なるブロックチェーンネットワーク NW1、NW2 に接続されている。図 1 では、サーバ 10 は、異なる 2 つのブロックチェーンネットワーク NW1、NW2 に接続されているが、これに限られず、3 つ以上の異なるブロックチェーンネットワークに接続され得る。

10

【0012】

端末 20 は、異なる複数のブロックチェーンネットワーク NW1、NW2 等に通信可能であり、端末 20 上で動作するアプリケーションにて異なるブロックチェーンネットワーク NW1、NW2 等に対して取引を実行する手段を有する。

【0013】

各ブロックチェーンネットワーク NW1、NW2 では、ピアツーピア（P2P）ネットワークにてそれぞれの対象データが流通している。例えば、図 1 では、ブロックチェーンネットワーク NW1 で流通するブロックチェーン BC-A の対象データは、仮想通貨の A コインであり、ブロックチェーンネットワーク NW2 で流通するブロックチェーン BC-B の対象データは、仮想通貨の B コインである。ただし、ブロックチェーンの取引（トランザクション）の対象データは、仮想通貨に限らず、株、証券、債権、不動産、ポイント等のすべての商品を対象とすることができる。

20

【0014】

ブロックチェーンネットワーク NW1 を拡大した図を参照すると、ブロックチェーンネットワーク NW1 では、同じブロックチェーン BC の対象データを共有するノード群がネットワーク NW1 で接続されている。

【0015】

ここでは、対象データの一例である仮想通貨の取引をそれぞれのブロックチェーン BC-A で管理する。ブロックチェーン BC-A を管理する者は、人（ユーザ）であってもよいし、企業、団体、学校であってもよい。ここでは、対象データが A コインのブロックチェーン BC-A を共有するノード群 N11、N12、N13 が会社 S、会社 T、会社 U により管理されているが、これに限られず、ブロックチェーン BC-A は異なる対象データのブロックチェーンであってもよい。

30

【0016】

同様にして、ブロックチェーンネットワーク NW1 と異なるブロックチェーンネットワーク NW2 には、対象データが B コインのブロックチェーン BC-B を共有するノード群 N21、N22、N23 が存在する。ただし、これに限られず、ブロックチェーン BC-B は異なる対象データのブロックチェーンであってもよい。

【0017】

なお、サーバ 10 は、異なるブロックチェーンネットワーク間において一のブロックチェーンの対象データと他のブロックチェーンの対象データとの間の価値の移転を管理する取引管理装置の一例である。

40

【0018】

ただし、これに限られず、サーバ 10 の替わりに端末 20 が上記価値の移転を管理してもよい。この場合、取引管理システム 1 は、サーバ 10 を有さなくてもよい。例えば、端末 20 が以下に説明するサーバ 10 の機能を有し、端末 20 がネットワーク 30 を介してブロックチェーンネットワーク NW1、NW2 に接続されるシステムが構築されてもよい。かかる構成の取引管理システム 1 において、端末 20 は、上記取引管理装置の一例となる。

【0019】

50

サーバ 10 及び端末 20 は、パーソナルコンピュータ、タブレット型端末、スマートフォン、PDA (Personal Digital Assistants) 等の情報処理装置のいずれであってもよい。サーバ 10 及び端末 20 には、HMD (Head Mount Display)、FMD (Face Mount Display)、時計型等のウェアラブルデバイスの情報処理装置が適用されてもよい。

【0020】

[ブロックチェーン]

本実施形態に係るブロックチェーン上での取引の対象データについて、図 2 を参照しながら説明する。ブロックチェーンにおけるブロックチェーンデータは、複数のブロック (例えば、 B_{n-1} 、 $B_n \cdots$) が、鎖のように繋がって管理されるデータである。それぞれのブロックには、1 又は 2 以上のトランザクションデータが格納されている。トランザクションデータは、仮想通貨の入金や出金、債券や株の売買等の取引の内容を示すデータである。例えば、ブロック B_{n-1} には、6 つのトランザクション ($TX_1 \sim TX_6$) のデータが格納されている。

10

【0021】

本実施形態では、例えばビットコイン等の仮想通貨 (A コインと B コインとする) のデータのやり取りに用いられるブロックチェーンデータを例に挙げて説明する。本実施形態に使用されるブロックチェーンデータでは、例えばナンス (Nonce) と呼ばれる値によって、改ざんが防止される。

20

【0022】

新たなブロック (例えば、図 5 の B_{n+1} ブロック) を生成する際、ブロックチェーンに含まれていないトランザクションのデータを収集する。新たなブロック B_{n+1} に、収集したトランザクションのデータ (例えば $TX_{21} \sim TX_{26}$) と、現在のブロックチェーンの末尾のブロック B_n のハッシュ値 (256 ビット) を含める。ナンスの計算では、現在生成中のブロック B_{n+1} に対して、暗号学的ハッシュ関数を適用した場合のハッシュ値の先頭の k ビットがすべて “0” になる条件を満たすような値を設定する。これにより、ブロックの改ざんが防止される。

【0023】

[価値の総量の不整合]

図 1 に示す取引管理システム 1 において、ブロックチェーンネットワーク NW1 とブロックチェーンネットワーク NW2 とは異なるブロックチェーンネットワークであり、基本的にブロックチェーン BC-A の対象データである A コインと、ブロックチェーン BC-B の対象データである B コインとのデータは共有されない。

30

【0024】

そして、本実施形態では、同じブロックチェーンネットワーク NW1 内における各コインの価値の移転について対象としない。本実施形態では、ブロックチェーンネットワーク NW1 内でブロックチェーン BC-A により管理されている A コインと、ブロックチェーンネットワーク NW2 内でブロックチェーン BC-B により管理されている B コインの一方から他方へ価値を移転する場合を対象とする。このとき、A コイン又は B コインの一方のコインの出金と他方のコインの入金との間で非同期に取引が確定する。以下、ブロックチェーン BC-A を単に BC-A と表記し、ブロックチェーン BC-B を単に BC-B と表記し、BC-A、BC-B を含むブロックチェーンを総称して BC とも表記する。

40

【0025】

図 3 を参照して具体的に説明する。端末 20 において動作するアプリケーションによって、ユーザ A が BC-B で管理されている 5 枚の B コインを、BC-A で管理されている 5 枚の A コインへの価値移転の要求 (以下、「価値移転リクエスト」ともいう。) をしたとする。これに応じて、各コインの価値の移転のトランザクションが実行される。

【0026】

ここでは説明を簡単にするために、A コインと B コインの価値の比は、1 : 1 とする。また、BC-A では 60 秒毎にトランザクションが確定し、BC-B では 20 秒毎にトラ

50

ンザクションが確定することとする。なお、BC-AとBC-Bとのトランザクションの確定タイミングは非同期であり、連動していない。

【0027】

図3の例では、BC-BにおいてユーザAが所持する100枚のBコインから5枚のBコインを出金するトランザクションが実行され（Bコイン：-5）、時刻t1にこの取引の処理が確定する。また、BC-AにおいてユーザAが所持する100枚のAコインに5枚のAコインを入金するトランザクションが実行され（Aコイン：+5）、時刻t3にこの取引の処理が確定する。

【0028】

このように各取引の処理が非同期に確定するため、ユーザAの所持するコインの総数は、時刻t1と時刻t3との間の時刻t2では195コインとなり、時刻t3後の時刻t4では200コインとなる。

【0029】

以上のように、ブロックチェーンは取引を実行してから非同期で処理が確定する仕組みであり、取引を実行してからその処理が確定するまでに一定の時間が必要である。つまり、ユーザAが入金及び出金の操作をしてから直ぐにその処理が確定せず、しばらくしてからそのリクエスト処理が確定する仕組みになっている。このため、任意のタイミングであるユーザが自分のAコインとBコインの価値の総量を参照すると、実際より価値の総量が多くなったり、少なくなったりして、ブロックチェーン間で価値の総量を維持した状態で各コインの価値を参照できない場合が生じる。例えば、出金側のBコインのブロックチェーンBC-Bでの処理が入金側のAコインのブロックチェーンBC-Aでの処理よりも早く確定すると、一時的に総資産が少なくなる。

【0030】

この不整合は、サーバ10が、異なるブロックチェーンネットワークNW1、NW2の取引を時系列に管理したときに生じる。つまり、例えば同じブロックチェーンネットワークNW1内の取引を時系列に管理したときや、同じブロックチェーンネットワークNW2内の取引を時系列に管理したときには生じない。

【0031】

ユーザは、決算などのときに移転中のコインの価値が実際より減らないように価値の総量を参照したい。そこで、以下に説明する一実施形態に係る取引管理方法では、異なるブロックチェーンネットワークのブロックチェーン間で価値の総量を維持した状態でコインの残高を参照することが可能な技術を提供する。

【0032】

なお、ブロックチェーンBCのトランザクション（TX）が確定するとは、図2に示すブロックが任意の計算機によって生成されるときを意味する。ブロックの生成ルールとしては、ブロックチェーンBCはトランザクションが実行されると、あるタイミングでそのトランザクションをまとめてブロックとする。

【0033】

上記あるタイミングは、ブロックチェーンBCに対してトランザクションが実行されたときに、ブロック生成間隔（時間）及びブロックサイズに基づき以下の2つの条件のいずれかを満たしたときであり、このときにトランザクションが確定する。1つ目の条件は、まだブロックに含まれないトランザクションの総量がブロックサイズを超えておらず、かつブロック生成間隔を経過したときであり、このときにブロックが生成されトランザクションが確定する。2つ目の条件は、まだブロックに含まれないトランザクションの総量がブロックサイズを超えたときであり、このときにブロックが生成されトランザクションが確定する。

【0034】

〔機能構成〕

次に、一実施形態に係る取引管理方法を実行するサーバ10及び端末20の機能構成の一例について、図4を参照しながら説明する。図4は、一実施形態に係るサーバ10及び

10

20

30

40

50

端末 20 の機能構成の一例を示す図である。

【0035】

端末 20 は、要求送信部 21、制御部 22 及び記憶部 23 を有する。記憶部 23 には、アプリケーションプログラム 24 が格納されている。アプリケーションプログラム 24 は、ユーザが所持する端末 20 で動作し、価値移転及び参照処理を要求するためのプログラム（以下、「アプリ 24」ともいう。）である。アプリ 24 は、取引所にある端末 20 で動作してもよい。

【0036】

制御部 22 は、アプリ 24 を動作させ、ユーザ操作に応じて出金取引や入金取引等の価値移転リクエストを出力する。また、制御部 22 は、アプリ 24 を動作させ、ユーザ操作に応じて各ブロックチェーンのコインの残高の参照要求（以下、「価値参照リクエスト」ともいう。）を出力する。要求送信部 21 は、価値移転リクエスト及び価値参照リクエストを受け付け、サーバに通知する。

【0037】

サーバ 10 は、要求受信部 11、移転処理部 12、参照処理部 13、取引実行部 14、監視部 15 及び記憶部 16 を有する。記憶部 16 は、取引確定テーブル 17、取引中テーブル 18 及び取引管理プログラム 19 を記憶する。

【0038】

図 5（a）は、一実施形態に係る取引確定テーブル 17 の一例を示す図である。図 5（b）は、一実施形態に係る取引中テーブル 18 の一例を示す図である。各テーブルにはユーザ毎に各種データが記憶されている。各ユーザの識別子は、アカウント名（ユーザ ID、会社 ID 等）であってもよい。

【0039】

図 5（a）に示す取引確定テーブル 17 は、取引が確定したデータを記憶する。取引確定テーブル 17 は、価値移転 ID、移転元 BC 識別子、移転元 TX（トランザクション）確定ブロック、移転元 TX ID、移転先 BC 識別子、移転先 TX 確定ブロック、移転先 TX ID の各データを記憶する。価値移転 ID は、異なるブロックチェーンネットワーク NW1、NW2 のそれぞれのブロックチェーン BC-A、BC-B においてペアとなる A コイン及び B コインの価値移転を紐付ける価値移転識別情報の一例である。

【0040】

図 5（a）の例では、BC-A のブロック 10 の TX ID「b b b b」のトランザクションと、BC-B のブロック 246 の TX ID「a a a a」のトランザクションとが、価値移転 ID「x x x x」により紐付けられている。

【0041】

図 5（b）に示す取引中テーブル 18 は、取引中のデータを記憶する。取引中テーブル 18 は、価値移転 ID、移転元 BC 識別子、移転元 TX 確定ブロック、移転元 TX ID の各データを記憶する。図 5（b）の例では、BC-A のブロック 10 の TX ID「c c c c」のトランザクションが、価値移転 ID「y y y y」に紐付けられている。

【0042】

図 4 に戻り、要求受信部 11 は、端末 20 の要求送信部 21 から送信された価値移転リクエスト及び価値参照リクエストを受信する。

【0043】

移転処理部 12 は、受信した価値移転リクエストに従い、A コイン及び B コインの出金や入金のトランザクション処理を実行する。

【0044】

参照処理部 13 は、受信した価値参照リクエストに従い、A コイン及び B コインの残高の参照処理を実行する。

【0045】

取引実行部 14 は、異なるブロックチェーンネットワークの一方のブロックチェーンデータと他方のブロックチェーンデータとの間の価値移転の取引を実行する。本実施形態で

10

20

30

40

50

は、取引実行部 14 は、価値移転リクエストに従った A コイン及び B コインの出金や入金
のトランザクション処理を実行する。

【0046】

監視部 15 は、価値移転 ID を記憶した取引確定テーブル 17 及び取引中テーブル 18
を参照して、BC-A 及び BC-B 間における各コインの出金や入金
のトランザクション
処理の確定状態を監視する。

【0047】

また、監視部 15 は、監視した BC-A 及び BC-B の各コインの価値の移転の確定状
態に基づき、価値移転 ID により紐付けられた BC-A 及び BC-B の各コインのいずれ
かのトランザクションが確定していないか（つまり、取引中か）を判定する。監視部 15
は、取引中を判定した場合、価値参照リクエストに対して価値移転 ID により紐付けられ
た確定しているブロックチェーンの対象データのトランザクションをキャンセルした状態
を計算し、BC-A 及び BC-B の各コインの価値又は当該価値の総量を参照させる。

【0048】

〔ハードウェア構成〕

次に、一実施形態に係るサーバ 10 のハードウェア構成の一例について、図 6 を参照し
ながら説明する。図 6 は、一実施形態に係るサーバ 10 のハードウェア構成の一例を示す
図である。なお、端末 20 のハードウェア構成は、サーバ 10 のハードウェア構成と同一
であるため、説明を省略する。

【0049】

サーバ 10 は、入力装置 101、表示装置 102、外部 I/F 103 を有する。また、
サーバ 10 は、RAM (Random Access Memory) 104、ROM (Read Only Memory)
105、CPU (Central Processing Unit) 106、通信 I/F 107 及び HDD
(Hard Disk Drive) 108 を有し、それぞれがバス B で相互に接続されている。

【0050】

入力装置 101 は、キーボードやマウスなどを含み、サーバ 10 に各操作信号を入力す
るために用いられる。表示装置 102 は、LCD (Liquid crystal Display) モニタ等
のディスプレイ、プリンタ、CRT (Cathode Ray Tube) などを含み、各種の処理結果
を表示する。

【0051】

通信 I/F 107 は、サーバ 10 をネットワーク 30、40 に接続するインターフェー
スである。これにより、サーバ 10 は、通信 I/F 107 を介して端末 20 やブロックチ
ェーンネットワーク NW1、NW2 のブロックチェーン BC-A、BC-B のトランザク
ションのデータをやり取りする。

【0052】

HDD 108 は、プログラムやデータを格納している不揮発性の記憶装置である。HDD
108 に格納されるプログラムやデータには、サーバ 10 の全体を制御するソフトウェ
ア及びアプリケーションソフトウェアがある。HDD 108 には、取引確定テーブル 17
、取引中テーブル 18 及び取引管理プログラム 19 が格納されてもよい。

【0053】

外部 I/F 103 は、外部装置とのインターフェースである。外部装置には、記録媒体
103a などがある。これにより、サーバ 10 は、外部 I/F 103 を介して記録媒体 1
03a の読み取り及び／又は書き込みを行うことができる。記録媒体 103a は、CD (Compact Disk)、DVD (Digital Versatile Disk) であってもよい。記録媒体 10
3a は、SD メモリカード (SD Memory card) や USB メモリ (Universal Serial Bus memory) 等であってもよい。

【0054】

ROM 105 は、電源を切っても内部データを保持することができる不揮発性の半導体
メモリである。ROM 105 には、基本プログラム及びデータが格納されている。RAM
104 は、データを一時保持する揮発性の半導体メモリであり、取引管理プログラム 19

10

20

30

40

50

、取引確定テーブル１７、取引中テーブル１８を一時的に保持してもよい。ＣＰＵ１０６は、ＨＤＤ１０８やＲＯＭ１０５などの記憶装置から、取引管理プログラム１９及び各種データをＲＡＭ１０４上に読み出し、所定の処理を実行することで、装置全体の制御や搭載機能を実現する演算装置である。

【００５５】

なお、図４は機能に着目したブロック図を描いており、これらの機能ブロックで示した各部のソフトウェアを実行するプロセッサはハードウェアである。例えば、移転処理部１２、参照処理部１３、取引実行部１４、監視部１５の機能は、取引管理プログラム１９がＣＰＵ１０６に実行させる取引実行処理、価値移転処理、参照処理により実現される。

【００５６】

要求受信部１１の機能は、例えば、通信Ｉ／Ｆ１０７により実現可能である。記憶部１６の機能は、例えば、ＲＡＭ１０４、ＲＯＭ１０５及びＨＤＤ１０８により実現可能である。取引確定テーブル１７及び取引中テーブル１８に記憶されているデータは、ＲＡＭ１０４、ＲＯＭ１０５、ＨＤＤ１０８又はサーバ１０に接続されるクラウド上のサーバ等に格納されてもよい。

【００５７】

〔価値移転及び参照処理〕

次に、本実施形態に係る価値移転及び参照処理の一例について図７を参照して説明する。図７は、一実施形態に係る価値移転及び参照処理の一例を示すフローチャートである。本処理が開始されると、要求受信部１１は、価値移転リクエスト又は価値参照リクエストの少なくともいずれかの要求を端末２０から受信する（ステップＳ１０）。

【００５８】

次に、要求受信部１１は、受信した要求の処理内容を判定する（ステップＳ１１）。要求受信部１１は、受信した要求の処理内容が「価値移転」か否かを判定する（ステップＳ１２）。要求受信部１１が、受信した要求の処理内容が「価値移転」と判定した場合、移転処理部１２は、価値移転処理を実行する（ステップＳ１３）。価値移転処理の具体的内容の一例は、図８のフローチャートを参照して次に説明される。

【００５９】

要求受信部１１は、受信した要求の処理内容が「価値移転」でないと判定した場合、参照処理部１３は、参照処理を実行する（ステップＳ１４）。参照処理の具体的内容の一例は図１１のフローチャートを参照して後述される。

【００６０】

〔価値移転処理〕

次に、本実施形態に係る価値移転処理の一例について図８及び図９を参照して説明する。図８は、一実施形態に係る価値移転処理の一例を示すフローチャートである。図９は、一実施形態に係る価値移転処理を説明する図である。なお、価値移転処理は、ユーザ毎に実行される。ここでは、ユーザＡの操作に従い、端末２０からの価値移転リクエストに応じて、サーバ１０は、ユーザＡの異なるブロックチェーンネットワークＮＷ１，ＮＷ２間におけるＢＣ－ＡのＡコインとＢＣ－ＢのＢコインとの間の価値移転のトランザクションを実行する。

【００６１】

ＢＣ－ＡのＡコインは、一のブロックチェーンネットワークで管理される一のブロックチェーンの対象データの一例である。ＢＣ－ＢのＢコインは、一のブロックチェーンネットワークと異なる他のブロックチェーンネットワークで管理される他のブロックチェーンの対象データの一例である。

【００６２】

本処理は、図７のステップＳ１３において呼び出されることで開始される。移転処理部１２は、端末２０からの価値移転リクエストに従って価値移転リクエストを一意に特定できる価値移転ＩＤを発行する（ステップＳ２０）。例えば、図９の例では、移転元ＢＣ識別子がＢＣ－Ｂのブロック番号「２４６」のＴＸＩＤ「aaaa」のトランザクションと

10

20

30

40

50

、移転先 B C 識別子が B C - A のブロック番号「10」の T X I D 「b b b b」のトランザクションとを紐付ける価値移転 I D 「x x x x」が発行されている。

【0063】

次に、取引実行部 14 に対して各トランザクションの実行を要求する（ステップ S 22、S 28）。ステップ S 22 では、移転処理部 12 は、価値移転元 B C の B C - B に出金要求を行う。出金要求のトランザクションの実行処理については、図 10 を参照して後述される。

【0064】

次に、移転処理部 12 は、B C - A 及び B C - B を監視し、出金のトランザクションの処理結果が成功（正常終了）であるかを判定する（ステップ S 24）。移転処理部 12 は、価値移転 I D 「x x x x」に紐付けられたトランザクションを含むブロックが作成されると、トランザクションの処理結果が成功（正常終了）であると判定する。移転処理部 12 は、出金のトランザクションの処理結果が成功であると判定すると、トランザクション（T X）の結果（処理済の確定ブロックとトランザクション I D）と価値移転 I D を紐付けて取引中テーブル 18 に保存し（ステップ S 26）ステップ S 28 に進む。

【0065】

例えば、図 9 の例では、B C - A の処理済の確定ブロック「10」のトランザクション I D 「c c c c」が価値移転 I D 「y y y y」に紐付けられ、取引中テーブル 18 に記憶されている。

【0066】

なお、ステップ S 24 において、移転処理部 12 は、出金のトランザクションの処理結果が成功でないと判定すると本処理を終了する。

【0067】

ステップ S 28 において、移転処理部 12 は、価値移転先 B C に入金要求を行う。移転処理部 12 は、B C - A 及び B C - B を監視し、入金のトランザクションの処理結果が成功（正常終了）であるかを判定する（ステップ S 30）。移転処理部 12 は、入金のトランザクションの処理結果が成功であると判定すると、取引中テーブル 18 の当該価値移転 I D に関するレコードを取引確定テーブル 17 に移動し、更に入金のトランザクションの結果を追記し（ステップ S 32）、本処理を終了する。

【0068】

例えば、入金と出金のトランザクションの処理結果が成功であると判定されると、図 9 に示すように、入金と出金のトランザクションの処理結果が価値移転 I D に紐付けられて取引確定テーブル 17 に記憶され、取引中テーブル 18 から対応するデータが削除される。ここでは、B C - A の処理済の確定ブロック「10」のトランザクション I D 「b b b b」及び B C - B の処理済の確定ブロック「246」のトランザクション I D 「a a a a」が価値移転 I D 「x x x x」により紐付けられて記憶されている。

【0069】

ステップ S 30 において、移転処理部 12 が、トランザクションの処理結果が成功でないと判定すると、価値移転元 B C に入金要求（ステップ S 22 にて要求された出金要求をキャンセルするための返金要求）を行う（ステップ S 34）。なお、トランザクションの処理結果が成功でない場合は、通信異常や取引の残高が足りないときに発生する。

【0070】

次に、移転処理部 12 は、取引中テーブル 18 から、トランザクションの処理結果が成功でないと判定された価値移転 I D、処理済の確定ブロック及びブロックチェーン上のトランザクション I D を削除し（ステップ S 36）、本処理を終了する。

【0071】

図 9 の例では、端末 20 上のアプリを動作させ、価値移転リクエストが通知されると、サーバ 10 はかかる価値移転リクエストを受け付け、図 8 のステップ S 22 及びステップ S 28 の要求に応じて、図 10 に一例を示すように、出金と入金の取引が実行される。図 9 の例では、5 枚の B コインと 5 枚の A コインを移転する取引と、1 枚の A コインと 1 枚

10

20

30

40

50

のBコインを移転する取引が実行される。AコインとBコインの価値の比は、1：1である。

【0072】

価値移転リクエストに応じた取引実行処理は、取引実行部14により実行される。図10に一例を示すように、取引実行部14は、指定のブロックチェーンにトランザクションを実行させ、変数startに現在時刻を設定する（ステップS15）。

【0073】

例えば、図8のステップS22の出金要求では、価値移転元のブロックチェーンに出金のトランザクションを実行させる。また、図8のステップS28の入金要求では、価値移転先のブロックチェーンに入金のトランザクションを実行させる。

10

【0074】

次に、取引実行部14は、トランザクションの実行が確定したかを判定する（ステップS16）。取引実行部14は、当該トランザクションを含むブロックが作成されると、取引が確定したと判定し、トランザクションの処理結果が成功したと判断して本処理を終了する（正常終了）。

【0075】

一方、ステップS16において、取引実行部14は、当該ブロックが作成されておらず、トランザクションの実行が確定していないと判定すると、変数startにタイムアウトの時間を加算した値よりも現在時刻が大きいかを判定する（ステップS17）。

【0076】

20

取引実行部14は、変数startにタイムアウトの時間を加算した値と比較して現在時刻が小さい又は等しいと判定した場合、所定の時間待って（ステップS18：スリープ）、ステップS16に戻り、再度ステップS16以降の処理を実行する。

【0077】

取引実行部14は、変数startにタイムアウトの時間を加算した値よりも現在時刻が大きいと判定した場合、トランザクションの処理結果が失敗したと判断して本処理を終了する（異常終了）。

【0078】

図10のトランザクション処理の実行に従い、図9の例では、現在時刻 t_n の時点では、ブロックチェーンBC-Bのブロック番号246の5枚のBコインの出金のトランザクションが確定している。また、ブロックチェーンBC-Aのブロック番号10の5枚のAコインの入金のトランザクションが確定している。これらの2つのトランザクションは、価値移転ID「xxxx」により紐付けられている。よって、現在時刻 t_n において、取引確定テーブル17には、価値移転ID「xxxx」にて紐付けられたブロック番号10のトランザクションID「bbbb」と、ブロック番号246のトランザクションID「aaaa」が記憶された状態になる。

30

【0079】

更に、現在時刻 t_n の時点では、ブロックチェーンBC-Aのブロック10の1枚のBコインの出金のトランザクションが確定している。しかし、この時点では、価値移転ID「yyyy」により紐付けられている、ブロックチェーンBC-Bの1枚のBコインの入金のトランザクション（TXID「dddd」）は確定していない。従って、取引中テーブル18には、価値移転ID「yyyy」により紐付けられている、ブロックチェーンBC-Aの1枚のAコインの出金のトランザクション（TXID「cccc」）が記憶された状態になる。

40

【0080】

〔参照処理〕

次に、本実施形態に係る参照処理の一例について図11及び図12を参照して説明する。図11は、一実施形態に係る参照処理の一例を示すフローチャートである。図12は、一実施形態に係る参照処理を説明する図である。なお、参照処理は、ユーザ毎に実行される。

50

ここでは、ユーザ A の操作に従い、端末 20 からの価値参照リクエストに応じて、サーバ 10 は、ユーザ A の複数のブロックチェーンネットワーク間における各ブロックチェーンデータの価値の総量（残高）を算出する。そして、サーバ 10 は、端末 20 に残高を表示させ、ユーザ A に残高を参照させる。例えば、図 12 の例では、価値参照リクエストが現在時刻 t_n に通知されているとする。

【0081】

本処理は、図 7 のステップ S 14 において呼び出されることで開始される。参照処理部 13 は、取引確定テーブル 17 及び取引中テーブル 18 からデータを取得する（ステップ S 40）。

【0082】

次に、参照処理部 13 は、変数 i に 1 を設定する（ステップ S 42）。次に、参照処理部 13 は、取引確定テーブル 17 に変数 i が示す順番に記憶されているブロックチェーンから取引が確定している確定済の最新ブロックの番号を抽出する（ステップ S 44）。図 12 の右上に示す取引確定テーブル 17 の例では、変数 i が示す 1 番目に記憶されている BC-A の確定済の最新ブロックの番号「10」が抽出される。

【0083】

図 11 に戻り、次に、参照処理部 13 は、当該最新ブロックのブロックチェーンの残高を取得する（ステップ S 46）。図 12 の例では、現在時刻 t_n においてブロックチェーン BC-A のユーザ A の所持コイン数（残高）は 104 コインである。

【0084】

次に、参照処理部 13 は、取引中テーブル 18 に、当該最新ブロックまでのブロックについて取引中のトランザクションが存在するかを判定する（ステップ S 48）。図 12 の右上に示す取引中テーブル 18 には、BC-A の最新ブロック番号「10」のブロックまでについて取引中のトランザクション「cccc」が存在する。

【0085】

参照処理部 13 は、当該最新ブロックまでの取引中のトランザクションが存在すると判定すると、取引中テーブル 18 から取引中のトランザクションを取得する（ステップ S 50）。図 12 の例では、ブロックの番号「10」の取引中のトランザクション「cccc」が取得される。

【0086】

次に、参照処理部 13 は、最新ブロック番号の残高に対して、取得したトランザクションの取引をキャンセル（反映）した残高を算出する（ステップ S 52）。図 12 の例では、取得したトランザクション「cccc」では、A コインを -1（1 枚出金）している。この場合、参照処理部 13 は、最新ブロック番号の残高に対して、取得したトランザクションの取引をキャンセル、つまり、A コインを +1（1 枚返却）して残高を算出する。その結果、A コインの残高は、105（ $= 104 + 1$ ）コインになる。

【0087】

次に、参照処理部 13 は、変数 i を一つ加算し、変数 i が取引確定テーブル 17 に記憶されたブロックチェーンの個数以下であるかを判定する（ステップ S 56）。図 12 の例では、取引確定テーブル 17 には 2 つのブロックチェーン BC-A、BC-B が記憶されている。

【0088】

よって、変数 i が 2 の場合、参照処理部 13 は、ステップ S 56 において「Yes」と判定し、ステップ S 44 に戻り、取引確定テーブル 17 のデータから取引が確定している最新ブロックの番号（確定済ブロック番号）を抽出する（ステップ S 44）。例えば、図 12 の例では、変数 i が示す 2 番目に記憶されている BC-B の確定済の最新ブロックの番号「246」が抽出される。

【0089】

図 11 に戻り、次に、参照処理部 13 は、当該最新ブロックのブロックチェーンの残高を取得する（ステップ S 46）。図 12 の例では、現在時刻 t_n においてブロックチェー

10

20

30

40

50

ンBC-BのユーザAの所持コイン数（残高）は95コインである。

【0090】

次に、参照処理部13は、取引中テーブル18に、当該最新ブロックまでのブロックについて取引中のトランザクションが存在するかを判定する（ステップS48）。図12の右上に示す取引中テーブル18には、BC-Bの最新ブロック番号「246」のブロックまたはそれ以前のブロックに取引中のトランザクションは存在しない。

【0091】

この場合、ステップS48において、参照処理部13は「No」と判定し、変数iを一つ加算し、変数iが取引確定テーブル17に記憶されたブロックチェーンの個数以下であるかを判定する（ステップS56）。図12の例では、取引確定テーブル17には2つのブロックチェーンBC-A、BC-Bが記憶されているため、変数iが3の場合、参照処理部13は、ステップS56において「No」と判定し、ステップS58に進む。ステップS58において、参照処理部13は、価値参照リクエストを送信した端末20に残高を参照させ（ステップS58）、本処理を終了する。

【0092】

以上により、図12の現在時刻 t_n において、ブロックチェーンBC-BのユーザAの所持コイン数（残高）は95コインであり、S52において算出されたブロックチェーンBC-AのユーザAの所持コイン数の105コインとともに端末20に残高「200」が表示される。これにより、ユーザAは、異なるブロックチェーンネットワークNW1、NW2のブロックチェーンBC-A、BC-B間での価値移転の取引の進捗を把握することができる。

【0093】

以上に説明したように、一実施形態に係る取引管理システム1によれば、価値移転時、サーバ10は、ブロックチェーンBC-A及びBC-Bの価値移転のトランザクションのペアに対し一意な価値移転IDを割り当てる。そして、サーバ10は、価値移転の対象となるブロックチェーンBCのブロック内のトランザクションを実行する。これと共に、サーバ10は、取引確定及び取引中状態を価値移転IDに紐づけて取引確定テーブル17及び取引中テーブル18にて管理する。

【0094】

価値参照時、サーバ10は、取引確定テーブル17を参照して、価値移転IDにより紐付けられる価値移転のトランザクションペアが両方確定している時点までのブロックチェーンBCの確定済みブロックを読みだす。そして、サーバ10は、取引中テーブル18を参照して、確定済みブロック又はそれ以前のブロックにかかる取引中のトランザクションが存在するかを判定する。サーバ10は、取引中のトランザクションが存在すると判定した場合、当該取引が未実施のものとして残高を計算する。これにより、ユーザは、異なるブロックチェーンネットワークのブロックチェーン間で価値が移転されたときの価値移転の取引の進捗を把握することができる。

【0095】

なお、当該取引が未実施のものとして残高を計算する処理は、出金のトランザクションが確定しているが、価値移転IDにより紐付けられる入金のトランザクションが確定していない場合に、出金のトランザクションをキャンセルし、未実施のものとして残高を計算する。

【0096】

また、当該取引が未実施のものとして残高を計算する処理は、入金のトランザクションが確定しているが、価値移転IDにより紐付けられる出金のトランザクションが確定していない場合に、入金のトランザクションをキャンセルし、未実施のものとして残高を計算する。

【0097】

以上、取引管理装置、取引管理方法及び取引管理プログラムを上記実施形態により説明したが、本開示に係る取引管理装置、取引管理方法及び取引管理プログラムは上記実施形

態に限定されるものではなく、本開示の範囲内で種々の変形及び改良が可能である。また、上記実施形態及び変形例が複数存在する場合、矛盾しない範囲で組み合わせることができる。

【0098】

例えば、上記実施形態に係る取引管理システム1の構成は一例であり、本開示の範囲を限定するものではなく、用途や目的に応じて様々なシステム構成例があることは言うまでもない。例えば、サーバ10及び端末20がネットワーク30、40を介して異なるブロックチェーンネットワークに接続されているシステム形態は、本実施形態に係る取引管理システム1の一態様であり、これに限定されない。例えば、本実施形態に係る取引管理システム1に含まれるサーバ10及び端末20の個数は複数であってもよい。また、接続される異なるブロックチェーンネットワークの個数は2つ以上であればよく、可変であり得る。

10

【0099】

サーバ10によって実行される処理の一部がクラウドコンピュータで実行され、他の処理が端又はクラウドコンピュータと端末との間に配置されるフォグコンピュータで実行されるようなネットワークシステム内の複数のコンピュータが連携して一連の処理が行われてもよい。

【0100】

以上の説明に関し、更に以下の項を開示する。

(付記1)

20

異なるブロックチェーンネットワーク間において一のブロックチェーンの対象データと他のブロックチェーンの対象データとの間で価値の移転を実行する取引実行部と、

前記価値の移転にかかる前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けて記憶した記憶部を参照して、各ブロックチェーンの対象データの価値の移転の確定状態を監視する監視部と、
を有する取引管理装置。

(付記2)

前記監視部は、

前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けてユーザ毎に記憶した前記記憶部を参照して、ユーザ毎の各ブロックチェーンの対象データの価値の移転の確定状態を監視する、

30

付記1に記載の取引管理装置。

(付記3)

前記監視部は、

監視した前記各ブロックチェーンの対象データの価値の移転の確定状態に基づき、前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とにより対応付けられたブロックチェーンの対象データのいずれかの価値の移転が確定していないと判定した場合、前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とにより対応付けられた確定しているブロックチェーンの対象データの価値の移転をキャンセルした状態におけるユーザ毎の各ブロックチェーンの対象データの価値を参照させる、

40

付記2に記載の取引管理装置。

(付記4)

異なるブロックチェーンネットワーク間において一のブロックチェーンの対象データと他のブロックチェーンの対象データとの間で価値の移転を実行し、

前記価値の移転にかかる前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けて記憶した記憶部を参照して、各ブロックチェーンの対象データの価値の移転の確定状態を監視する、

処理をコンピュータが実行する取引管理方法。

(付記5)

50

前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けてユーザ毎に記憶した前記記憶部を参照して、ユーザ毎の各ブロックチェーンの対象データの価値の移転の確定状態を監視する、

付記 4 に記載の取引管理方法。

(付記 6)

監視した前記各ブロックチェーンの対象データの価値の移転の確定状態に基づき、前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とにより対応付けられたブロックチェーンの対象データのいずれかの価値の移転が確定していないと判定した場合、前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とにより対応付けられた確定しているブロックチェーンの対象データの価値の移転をキャンセルした状態におけるユーザ毎の各ブロックチェーンの対象データの価値を参照させる、

10

付記 5 に記載の取引管理方法。

(付記 7)

異なるブロックチェーンネットワーク間において一のブロックチェーンの対象データと他のブロックチェーンの対象データとの間で価値の移転を実行し、

前記価値の移転にかかる前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けて記憶した記憶部を参照して、各ブロックチェーンの対象データの価値の移転の確定状態を監視する、

処理をコンピュータに実行させる取引管理プログラム。

20

(付記 8)

前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とを対応付けてユーザ毎に記憶した前記記憶部を参照して、ユーザ毎の各ブロックチェーンの対象データの価値の移転の確定状態を監視する、

付記 7 に記載の取引管理プログラム。

(付記 9)

監視した前記各ブロックチェーンの対象データの価値の移転の確定状態に基づき、前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とにより対応付けられたブロックチェーンの対象データのいずれかの価値の移転が確定していないと判定した場合、前記一のブロックチェーンの対象データに対する取引と前記他のブロックチェーンの対象データに対する取引とにより対応付けられた確定しているブロックチェーンの対象データの価値の移転をキャンセルした状態におけるユーザ毎の各ブロックチェーンの対象データの価値を参照させる、

30

付記 8 に記載の取引管理プログラム。

【符号の説明】

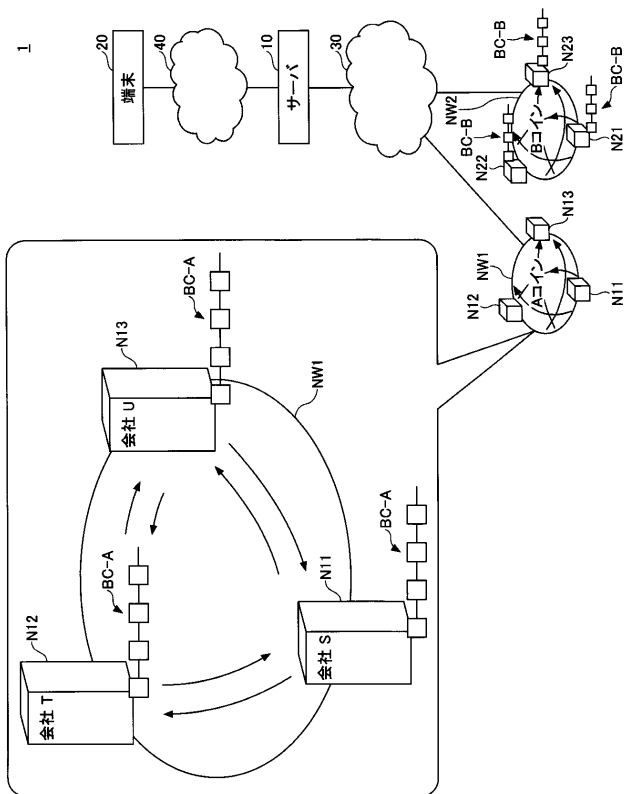
【0 1 0 1】

- 1 取引管理システム
- 1 0 サーバ
- 1 1 要求受信部
- 1 2 移転処理部
- 1 3 参照処理部
- 1 4 取引実行部
- 1 5 監視部
- 1 6 記憶部
- 1 7 取引確定テーブル
- 1 8 取引中テーブル
- 1 9 取引管理プログラム
- 2 0 端末
- 2 1 要求送信部

40

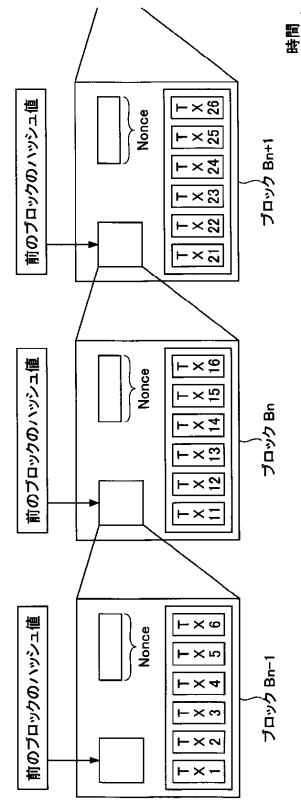
【 図 1 】

一実施形態に係る取引管理システムの全体構成の一例を示す図



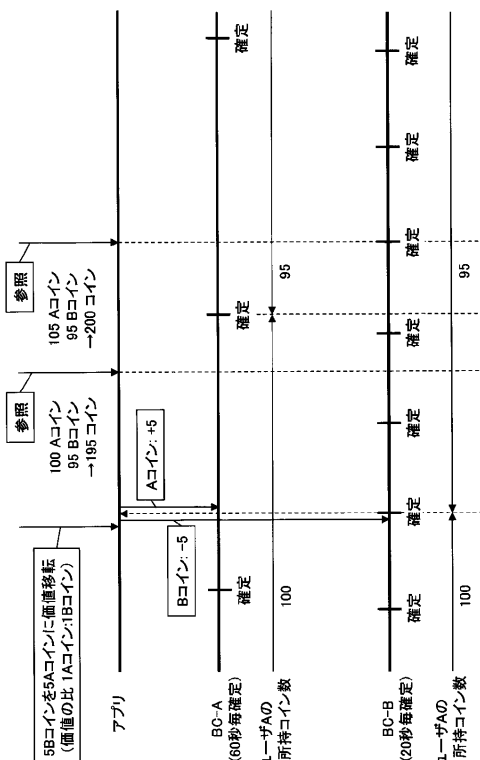
【図 2】

ブロックチェーンを説明する図



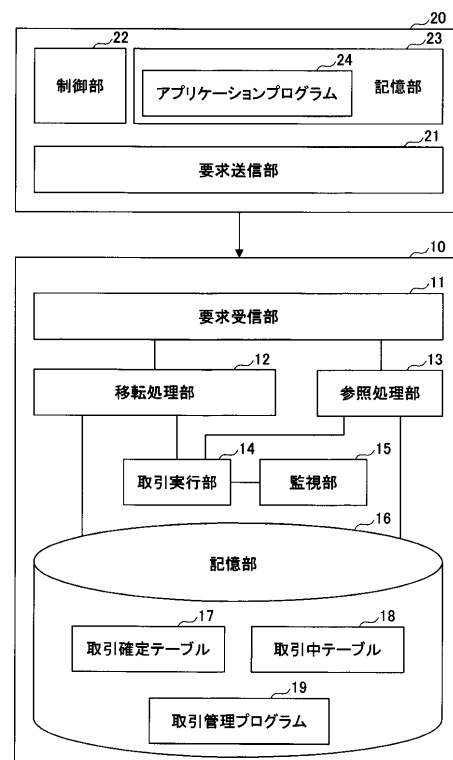
【 図 3 】

異なるブロックチェーンネットワーク間における
ブロックチェーン間での価値移転を説明する図



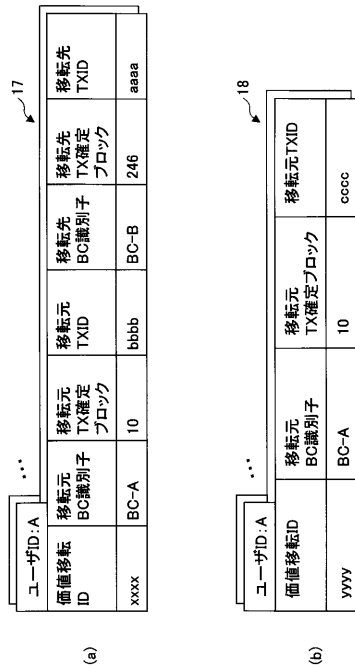
【图 4】

一実施形態に係るサーバ及び端末の機能構成の一例を示す図



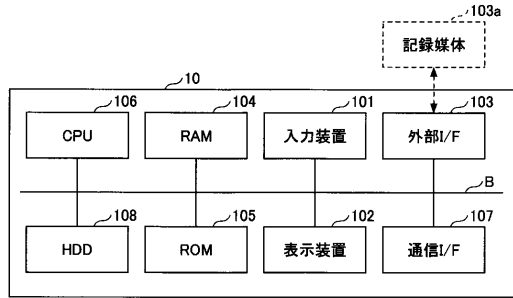
【図 5】

一実施形態に係る取引確定テーブル及び取引中テーブルの一例を示す図



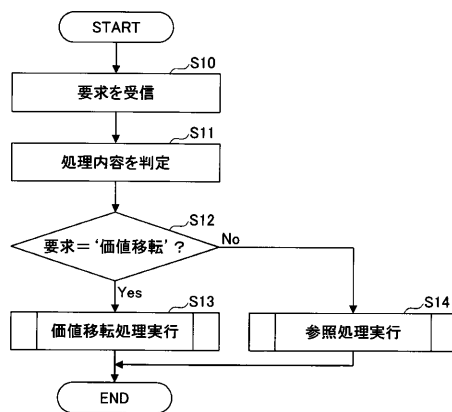
【図 6】

一実施形態に係るサーバのハードウェア構成の一例を示す図



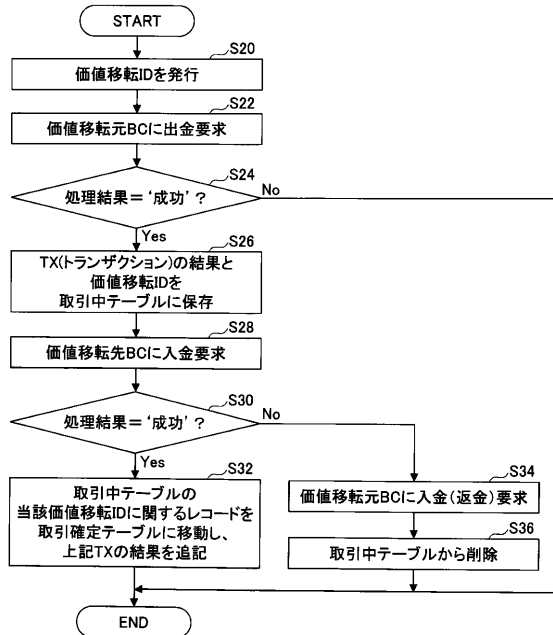
【図 7】

一実施形態に係る価値移転及び参照処理の一例を示すフローチャート



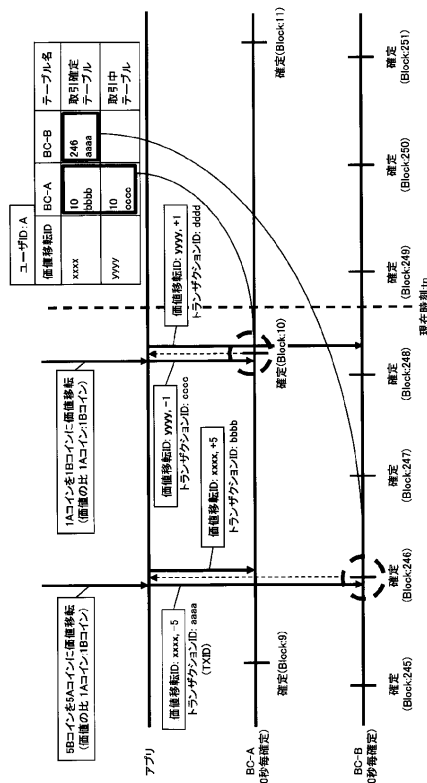
【図 8】

一実施形態に係る価値移転処理の一例を示すフローチャート



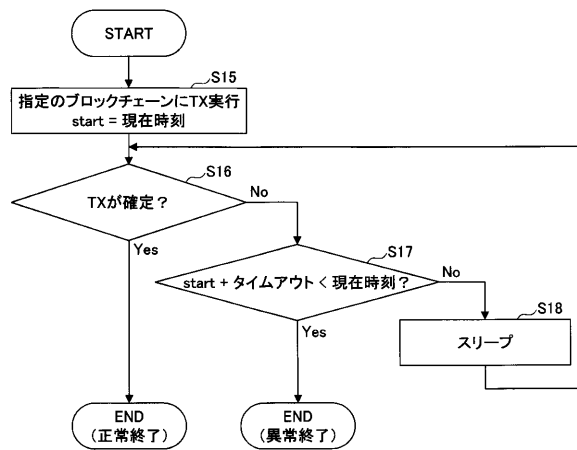
【図 9】

一実施形態に係る価値転処理を説明する図



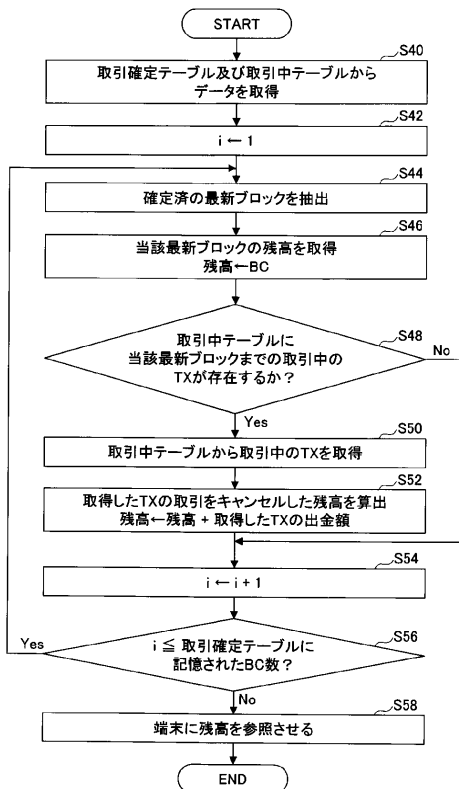
【図 10】

一実施形態に係る取引実行処理の一例を示すフローチャート



【図 11】

一実施形態に係る参照処理の一例を示すフローチャート



【図 12】

一実施形態に係る参照処理を説明する図

