(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2017-207979
(P2017-207979A)
(43)公開日　平成29年11月24日(2017.11.24)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/64	(2013.01)	G06F	21/64	
G06F 17/30	(2006.01)	G06F	17/30	120Z
G06F 21/62	(2013.01)	G06F	21/62	327

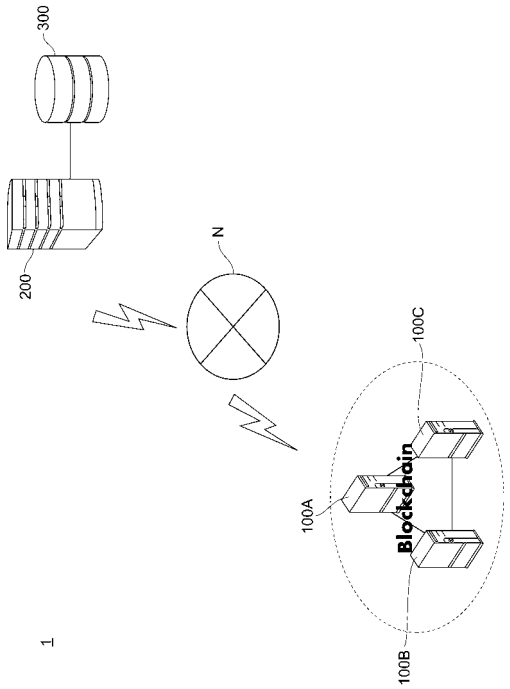
審査請求 未請求　請求項の数 5　ＯＬ　（全 14 頁）

(21)出願番号　特願2016-100794 (P2016-100794)
(22)出願日　平成28年5月19日 (2016.5.19)

(71)出願人　000155469
株式会社野村総合研究所
東京都千代田区大手町一丁目９番２号
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100080953
弁理士　田中　克郎
(72)発明者　渕上　達也
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内
(72)発明者　冨樫　寛隆
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内

(54)【発明の名称】改ざん検知システム、及び改ざん検知方法

(57)【要約】
【課題】データベースに記録されているデータに対して行われた改ざんを、検知可能になる。
【解決手段】所定のデータに対してハッシュ関数を用いて計算したダイジェストを記憶するブロックチェーンデータベースと、所定のデータを記憶するデータベースと、所定のデータに対する参照要求を受信した場合に、データベースから所定のデータを抽出し、抽出した当該所定のデータからハッシュ関数を用いてハッシュ値を計算し、当該ハッシュ値が、前記ブロックチェーンデータベースに記憶された、所定のデータに対応するダイジェストと一致するか否かを判定し、抽出した所定のデータを出力する参照処理部と、を備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
所定のデータに対してハッシュ関数を用いて計算したダイジェストを記憶するブロックチェーンデータベースと、
前記所定のデータを記憶するデータベースと、
前記所定のデータに対する参照要求を受信した場合に、前記データベースから前記所定のデータを抽出し、抽出した当該所定のデータから前記ハッシュ関数を用いてハッシュ値を計算し、当該ハッシュ値が、前記ブロックチェーンデータベースに記憶された、前記所定のデータに対応するダイジェストと一致するか否かを判定し、抽出した前記所定のデータを出力する参照処理部と、
を備える改ざん検知システム。
【請求項２】
前記改ざん検知システムは、さらに
前記所定のデータに対する更新要求を受信した場合に、前記データベース上において、前記所定のデータを更新済みデータに更新するとともに、当該更新済みデータに対して前記ハッシュ関数を用いて計算した更新ダイジェストを出力する更新処理部を備え、
前記ブロックチェーンデータベースは、
前記更新処理部が送信した前記更新ダイジェストをさらに記憶する、
請求項１に記載の改ざん検知システム。
【請求項３】
前記ブロックチェーンデータベースは、
互いにＰ２Ｐ接続された複数のノード上に分散して構築される、
請求項１または２に記載の改ざん検知システム。
【請求項４】
所定のデータに対してハッシュ関数を用いて計算したダイジェストを記憶するダイジェスト記憶ステップと、
前記所定のデータを記憶するデータ記憶ステップと、
前記所定のデータに対する参照要求を受信した場合に、前記データ記憶ステップにおいて記憶された前記所定のデータを抽出し、抽出した当該所定のデータから前記ハッシュ関数を用いてハッシュ値を計算し、当該ハッシュ値が、前記ダイジェスト記憶ステップにおいて記憶された、前記所定のデータに対応するダイジェストと一致しするか否かを判定し、抽出した前記所定のデータを出力する読出しステップと、
を備える改ざん検知方法。
【請求項５】
前記改ざん検知方法は、さらに
前記所定のデータに対する更新要求を受信した場合に、前記データ記憶ステップにおいて記憶された、前記所定のデータを更新済みデータに更新するとともに、当該更新済みデータに対して前記ハッシュ関数を用いて計算した更新ダイジェストを出力する書込みステップを備え、
前記ダイジェスト記憶ステップは、
出力した前記更新ダイジェストをさらに記憶する、
請求項４に記載の改ざん検知方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、改ざん検知システム、及び改ざん検知方法等に関する。
【背景技術】
【０００２】
複数の電子計算機を分散して構築した分散システムにおいて、従来は、データベースを１箇所に集中させて管理を行っていた。データベースを１箇所に集中させる構成の場合には

、トランザクション制御が行われる。この場合、システム規模が大きくなると、待ち時間が増え応答性が劣化してしまう。

【０００３】

特許文献１には、分散システムにおいて、データベース間の共通データの整合性をリアルタイムに維持し、かつ、システム構成にあわせてデータベースを分散管理する技術が開示されている。特許文献１に記載の分散システムでは、通信手段を介して情報を送受可能に分散して設けられた複数の計算機システムにそれぞれデータベースを設けている。これらのデータベースには、他のデータベースと重複する共通データ項目が含まれている。このような分散システムを管理する方法として、特許文献１には、まず重複する共通データ項目に当該データの内容を変更できる権限を有する唯一の計算機システムの識別情報を含める。次に、共通データの内容変更要求に対し、その権限を有する計算機システムが当該データの内容を変更し、変更後の共通データの内容を当該共通データを保有する他の計算機システムに伝送して変更後の内容に書替えさせている。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開平５－２２５０２７号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

しかし、特許文献１に記載されるような従来の技術では、データベースに記録されているデータに対して改ざんが行われた場合、容易に検知することができない。

【０００６】

そこで、本発明は、上記事情に鑑み、データベースに記録されているデータに対して行われた改ざんを、検知可能にすることを目的とする。

【課題を解決するための手段】

【０００７】

本発明による改ざん検知システムは、所定のデータに対してハッシュ関数を用いて計算したダイジェストを記憶するブロックチェーンデータベースと、所定のデータを記憶するデータベースと、所定のデータに対する参照要求を受信した場合に、データベースから所定のデータを抽出し、抽出した当該所定のデータからハッシュ関数を用いてハッシュ値を計算し、当該ハッシュ値が、前記ブロックチェーンデータベースに記憶された、所定のデータに対応するダイジェストと一致するか否かを判定し、抽出した所定のデータを出力する参照処理部と、を備える。

【０００８】

なお、本明細書等において、「部」とは、単に物理的構成を意味するものではなく、その構成が有する機能をソフトウェアによって実現する場合も含む。また、１つの構成が有する機能が２つ以上の物理的構成により実現されても、２つ以上の構成の機能が１つの物理的構成により実現されてもよい。

【発明の効果】

【０００９】

本発明によれば、データベースに記録されているデータに対して行われた改ざんを、検知可能になる。

【図面の簡単な説明】

【００１０】

【図１】本発明の一実施形態における改ざん検知システムのシステム構成の一例を示す構成図である。

【図２】本発明の一実施形態におけるＷＥＢサーバ及びデータベースの機能ブロックの一例を示す図である。

【図３】本発明の一実施形態における銘柄情報テーブルの一例を示す図である。

【図４】本発明の一実施形態における顧客情報テーブルの一例を示す図である。
【図５】本発明の一実施形態における所有権情報テーブルの一例を示す図である。
【図６】本発明の一実施形態におけるノードの機能ブロックの一例を示す図である。
【図７】本発明の一実施形態におけるブロックチェーンの構造の一部を示す図である。
【図８】本発明の一実施形態における改ざん検知システムの処理フローを示すシーケンス図である。
【図９】本発明の一実施形態における管理サーバ、及び端末のハードウェア構成の一例を示す図である。
【発明を実施するための形態】
【００１１】
［実施形態］
以下、本発明の実施の形態の１つについて詳細に説明する。なお、以下の実施の形態は、本発明を説明するための例示であり、本発明をその実施の形態のみに限定する趣旨ではない。また、本発明は、その要旨を逸脱しない限り、さまざまな変形が可能である。さらに、当業者であれば、以下に述べる各要素を均等なものに置換した実施の形態を採用することが可能であり、かかる実施の形態も本発明の範囲に含まれる。またさらに、必要に応じて示す上下左右等の位置関係は、特に断らない限り、図示の表示に基づくものとする。さらにまた、図面における各種の寸法比率は、その図示の比率に限定されるものではない。
【００１２】
＜１．システム構成の概要＞
図１は、本実施形態に係る改ざん検知システム１のシステム構成の一例を示している。本実施形態に係る改ざん検知システム１は、データベースに蓄積されるデータに施される改ざんを検知することができる。本実施形態では、一例として、データベースに蓄積されるデータは株主名簿関係情報であるとして説明する。データベースに蓄積される他のデータとしては、保険証券情報、与信情報、銀行取引情報、不動産取引情報等がある。
【００１３】
図１に示すように改ざん検知システム１は、インターネット等のネットワークＮに接続されたＷＥＢサーバ２００と、信託銀行ノード１００Ａ、証券会社ノード１００Ｂ、発行体（株式の発行体）ノード１００Ｃ（以下、これらのノードをまとめて単に「ノード１００」とも呼ぶ。）と、データベース３００とを備えている。例えば、株を保有する投資家が株主名簿に登録された情報を変更したい場合には、信託銀行ノード１００Ａ、又は証券会社ノード１００Ｂに変更を依頼することで、名簿の更新が行われる。
【００１４】
ネットワークＮは、無線ネットワークや有線ネットワークにより構成される。通信ネットワークの一例としては、携帯電話網や、ＰＨＳ（Ｐｅｒｓｏｎａｌ Ｈａｎｄｙ－ｐｈｏｎｅ Ｓｙｓｔｅｍ）網、無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、３Ｇ（３ｒｄ Ｇｅｎｅｒａｔｉｏｎ）、ＬＴＥ（Ｌｏｎｇ Ｔｅｒｍ Ｅｖｏｌｕｔｉｏｎ）、４Ｇ（４ｔｈ Ｇｅｎｅｒａｔｉｏｎ）、ＷｉＭａｘ（登録商標）、赤外線通信、Ｂｌｕｅｔｏｏｔｈ（登録商標）、有線ＬＡＮ、電話線、電灯線ネットワーク、ＩＥＥＥ１３９４等に準拠したネットワークがある。
【００１５】
ノード１００は、ネットワークＮに接続されたコンピュータであり、例えばＰＣやサーバ装置等が挙げられる。また、ノード１００は、例えば携帯電話やスマートフォン、ＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔｓ）、タブレット、ウェアラブル（Ｗｅａｒａｂｌｅ）端末、ゲーム機等でもよい。信託銀行ノード１００Ａ、証券会社ノード１００Ｂ、及び発行体ノード１００Ｃは、互いにＰ２Ｐ（Ｐｅｅｒ ｔｏ Ｐｅｅｒ）接続されており、ブロックチェーンを構成している。
【００１６】

ＷＥＢサーバ２００は、ネットワークＮに接続されたコンピュータであり、例えばＰＣやサーバ装置等が挙げられる。なお、ＷＥＢサーバ２００は、ノード１００それぞれともＰ２Ｐ接続をしている。

【００１７】

データベース３００は、本実施形態ではＷＥＢサーバ２００の外部ストレージとして、ＷＥＢサーバ２００に接続され、管理されるストレージ装置である。なお、データベース３００は、ＷＥＢサーバ上に構築される構成に限定されず、ネットワークＮに接続される、ストレージ管理用のサーバに構築される構成でもよい。

【００１８】

＜２．ＷＥＢサーバ２００、データベース３００＞

図２を用いてＷＥＢサーバ２００、及びデータベース３００の機能構成について説明する。図２は、本実施形態に係るＷＥＢサーバ２００及びデータベース３００の機能ブロック図である。

【００１９】

（２－１．データベース３００）

データベース３００は、それぞれＩＤをキーとして正規化された、銘柄情報テーブル３３１と、顧客情報テーブル３３２と、所有権情報テーブル３３３とを有している。

【００２０】

図３は銘柄情報テーブル３３１の一例を示す図である。銘柄情報テーブル３３１には、図３に示すように、銘柄ＩＤに，銘柄コード、銘柄名、及び売買単位等が対応付けられて保存されている。さらに、本実施形態では、銘柄情報テーブル３３１の各レコードには、後述するＷＥＢサーバ２００の処理によって、そのレコードを更新したトランザクションのＩＤが対応付けられて保存されている。

【００２１】

図４は顧客情報テーブル３３２の一例を示す図である。顧客情報テーブル３３２には、図４に示すように、顧客ＩＤに、顧客コード、顧客名、及び住所等が対応付けられて保存されている。さらに、本実施形態では、顧客情報テーブル３３２の各レコードには、後述するＷＥＢサーバ２００の処理によって、そのレコードを更新したトランザクションのＩＤが対応付けられて保存されている。

【００２２】

また、図５は所有権情報テーブル３３３の一例を示す図である。所有権情報テーブル３３３には、図５に示すように、所有権ＩＤに、銘柄ＩＤが対応付けられて保存されている。さらに、本実施形態では、所有権情報テーブル３３３の各レコードには、後述するＷＥＢサーバ２００の処理によって、そのレコードを更新したトランザクションのＩＤが対応付けられて保存されている。

【００２３】

（２－２．ＷＥＢサーバ２００）

図２に示すように、ＷＥＢサーバ２００は、更新処理部２０１と、参照処理部２０２とを備えている。

（２－２－１．更新処理部２０１）

更新処理部２０１は、ノード１００からデータベース３００への更新要求を受信した場合に、書込み処理を実行する。更新処理部２０１は、書込み処理として、

・データベース３００への書込み処理
・ブロックチェーンＤＢ１３１への書込み処理

を行う。

【００２４】

・データベース３００への書込み処理

更新処理部２０１は、データベース３００への書込み処理として、ノード１００からの更新要求に従い、データベース３００上のレコードを更新する。レコードの更新には、例えば既存のＳＱＬ等の言語を用いることが好ましい。

【００２５】
・ブロックチェーンＤＢ１３１への書込み処理
更新処理部２０１は、後述するブロックチェーンＤＢ１３１への書込み処理として、データベース３００への書込み処理において更新したレコードについて、所定のハッシュ関数を用いてハッシュ値（以下、「更新レコードダイジェスト」とも呼ぶ。更新ダイジェストの一例である。）を計算する。
【００２６】
次に、更新処理部２０１は、計算した更新レコードダイジェストを含むトランザクションを作成する。このとき、更新処理部２０１は、作成したトランザクションに対して一意なＩＤ（トランザクションＩＤ）を割り当て、更新が行われたテーブルの該当するレコードに、当該トランザクションのＩＤを対応付けて保存する。なお、トランザクションの詳細については、図７を用いて後述する。さらに、更新処理部２０１は、作成したトランザクションを、Ｐ２Ｐネットワークを介して、ノード１００へブロードキャストする（出力の一例である。）。
【００２７】
ブロードキャストされたトランザクションは、後述するノード１００のマイニング部１０４の処理によって、ブロックに格納され、ブロックチェーンにつなげられる。
【００２８】
（２－２－２．参照処理部２０２）
参照処理部２０２は、ノード１００からデータベース３００に格納されたデータの参照要求を受信した場合に、読出し処理を実行する。参照処理部２０２は、読出し処理として、
・データベース３００に対する抽出処理
・ブロックチェーンＤＢ１３１に対する抽出処理
・突合処理
を行う。
【００２９】
・データベース３００に対する抽出処理
参照処理部２０２は、ノード１００から参照要求を受信した場合に、該当するレコード（生データ）を、データベース３００から抽出する。さらに、参照処理部２０２は、データベース３００から抽出したレコードからダイジェスト（以下、「参照レコードダイジェスト」とも呼ぶ。）を計算する。
【００３０】
・ブロックチェーンＤＢ１３１に対する抽出処理
参照処理部２０２は、ノード１００から参照要求を受信した場合に、該当するレコードの更新レコードダイジェストを、ブロックチェーンＤＢ１３１から抽出する。具体的には、参照処理部２０２は、データベース３００に対する抽出処理によって抽出したレコードを参照し、当該レコードに対応するトランザクションＩＤを取得する。次に、参照処理部２０２は、ノード１００に対して、トランザクションＩＤを指定して、データ参照要求をＰ２Ｐネットワークを介して送信する。これによって参照処理部２０２は、後述するノード１００の処理によって、指定したトランザクションＩＤに対応する更新レコードダイジェストを取得することができる。
【００３１】
・突合処理
次に、参照処理部２０２は、データベース３００から抽出したレコードから計算した参照レコードダイジェストと、ブロックチェーンＤＢ１３１から抽出した更新レコードダイジェストとを突合する。上述のとおり、ブロックチェーンＤＢ１３１に格納されているデータは、改ざんされていないデータである。従って、データベース３００から抽出したレコードのダイジェストと、ブロックチェーンＤＢ１３１に格納されていたダイジェストとを突合することで、データベース３００への改ざんを検知することができる。

【００３２】
参照処理部２０２は、例えば、突合させたダイジェスト同士が一致した場合には、データベース３００から抽出したレコード（生データ）を、参照要求を行ったノード１００に対して送信する。また、例えば参照処理部２０２は、突合させたダイジェスト同士が一致しなかった場合には、アラートとともにレコードを出力することも可能である。
【００３３】
＜３．ノード１００＞
次に、図６を用いてノード１００の機能構成について説明する。図６は、本実施形態に係るノード１００の機能ブロック図である。図６に示すように、ノード１００は、ブロードキャスト通信部１０１と、要求部１０２と、応答部１０３と、マイニング部１０４と、記憶部１３０とを備える。さらに、図６に示すように、記憶部１３０には、ブロックチェーンＤＢ１３１が記録されている。ブロックチェーンＤＢ１３１は、信託銀行ノード１００Ａ、証券会社ノード１００Ｂ、及び発行体ノード１００Ｃのすべてのノードに格納される分散型データベースである。
【００３４】
（３－１．ブロックチェーン）
図７は、ノード１００が構成するブロックチェーンＤＢ１３１で管理するデータ構造の一部を模式的に示す図である。ブロックチェーンＤＢ１３１では、複数のブロックが、１列に連なった数珠つなぎの構造で管理されている。
【００３５】
図７はブロックチェーンＤＢ１３１において管理されるブロックのうち、Ｎ＋１番目のブロックの構造の一例を示す図である。Ｎ＋１番目のブロックヘッダーには、例えば、以下の値が格納されている。
・Ｎ番目のブロックのダイジェスト
・タイムスタンプ
・ターゲット
・ナンス
【００３６】
ターゲットは、ノード１００が既存のＰｏＷ（Ｐｒｏｏｆ　ｏｆ　Ｗｏｒｋ）の技術を用いてマイニングを行う際に、用いる値である。ナンスは、任意の値をいう。マイニングについて具体的に説明すると、ノード１００は、ブロックヘッダーのダイジェストがターゲット以下となるナンスを発見することを目的に、ナンスの値を変更しながら、繰り返しブロックヘッダーのダイジェストの計算（マイニング）を行う。なお、任意のナンスを含んだブロックヘッダーのダイジェストが、ターゲット以下となる確率は極めて小さいため、マイニングは過大なコストがかかる作業である。
【００３７】
ブロックチェーンＤＢ１３１において管理されているブロックを改ざんが行われた場合の挙動について説明する。例えばＮ番目のブロックに対して改ざんが行われたとすると、Ｎ＋１番目のブロックヘッダーの値（Ｎ番目のブロックのダイジェスト）が変わることになる。この場合、Ｎ＋１番目のブロックヘッダーのダイジェストがターゲットの値以下でなくなってしまう。従って、Ｎ番目のブロックに対して改ざんを行ったことを秘匿にするには、Ｎ＋１番目以降のすべてのブロックについて、再度マイニングをやり直し、適切なナンスを発見し直す必要がある。しかし、任意のナンスを含んだブロックヘッダーのダイジェストが、ターゲット以下となる確率は極めて小さいため、この作業は非常に困難である。
【００３８】
このようにブロックチェーンＤＢ１３１では、ブロックの作成にＰｏＷの技術を用いることで、ブロックの生成にかかるコストを増大させることで、ブロックチェーンで管理されているデータに対して、改ざんが行われることを防ぐことができる。
【００３９】

次に、ブロックのボディ部分の構成について説明する。図７の例では、ブロックのボディには単一のトランザクションが格納されている。トランザクションは、上述のとおり、ＷＥＢサーバ２００における更新処理部２０１によってＰ２Ｐネットワークにブロードキャストされるものである。

【００４０】

図７に示すように、トランザクションにはＩＤが割り当てられている。また、トランザクションには、上述した銘柄情報テーブル３３１、顧客情報テーブル３３２、又は所有権情報テーブル３３３のうちのいずれかのテーブルのレコードの更新レコードダイジェストが含まれている。なお、１つのトランザクションの中に、複数のテーブルの複数のレコードの更新レコードダイジェストが含まれる構成でもよい。

【００４１】

（３－２．ブロードキャスト通信部１０１）

ブロードキャスト通信部１０１は、Ｐ２Ｐ接続している他ノードに対して、ブロードキャスト通信を介してデータの送受信を行う。具体的には、ブロードキャスト通信部１０１は、後述するマイニング部１０４の処理によって生成されたブロックを送受信する。また、ブロードキャスト通信部１０１は、ＷＥＢサーバ２００の更新処理部２０１、及び参照処理部２０２から、それぞれトランザクション及び参照要求を受信することができる。

【００４２】

（３－３．要求部１０２）

要求部１０２は、データベース３００上の、銘柄情報テーブル３３１、顧客情報テーブル３３２、又は所有権情報テーブル３３３に対して更新処理を行う場合、ＷＥＢサーバ２００に更新要求を送信する。更新要求は、例えばレコードの追加・変更・削除等である。

【００４３】

（３－４．応答部１０３）

応答部１０３は、ＷＥＢサーバ２００の参照処理部２０２から、データ参照要求があった場合に、指定されたＩＤのトランザクションを参照して、該当するトランザクションに含まれる更新レコードダイジェストを送信する。なお、すべてのノード１００が、ダイジェストをＷＥＢサーバ２００に送信することが好ましい。しかし、これに限定されず、他のノード１００から応答データを受信したノード１００は、応答データの送信をおこなわない構成でもよい。この場合、最も応答の早かったノード１００のみが応答データを送信することができる。

【００４４】

（３－５．マイニング部１０４）

マイニング部１０４は、ＷＥＢサーバ２００の処理によって、トランザクションがブロードキャストされ場合に、当該トランザクションに対してマイニング処理を行う。

具体的には、マイニング処理は、マイニング部１０４は、図７に示した構造のブロックを作成する作業である。ノード１００は、マイニング処理として、ナンスの値を順次変更しながら、上述した適切なナンスを発見するまで、繰り返しブロックヘッダーのダイジェストの計算を行う。なお、図７に示したブロックヘッダーに含まれるタイムスタンプは、例えば、ノード１００がトランザクションを受信した時刻であることが好ましい。しかしこれに限定されず、ノード１００のマイニング部１０４は、任意のタイムスタンプをブロックヘッダーに格納することも可能である。

【００４５】

さらに、マイニング部１０４は、ブロードキャスト通信部１０１が、新しいブロックを受信した場合に、当該ブロックの検証処理を行うことも可能である。検証処理として、マイニング部１０４は、例えば、ブロックヘッダーのダイジェストがターゲット値を下回っているか、及び、トランザクションＩＤは一意な値であるか、等を検証することができる。

【００４６】

＜５．処理シーケンス＞

図８を用いて本実施形態に係る改ざん検知システム１の書込み処理及び読出し処理のシーケンスについて説明する。図８は、本実施形態に係る改ざん検知システム１の処理の流れを示すシーケンス図である。なお、図８に示す、Ｓ０１，Ｓ１１，Ｓ２１～Ｓ２２の処理は、データの書込み処理であり、Ｓ１３，Ｓ２３～Ｄ２６の処理は、データの読出し処理である。

【００４７】

例えば、投資家Ｕから、顧客情報テーブル３３２に登録されている住所の変更請求等（Ｓ０１）が、ノード１００のいずれかのノードにあった場合（例えば、信託銀行ノード１００Ａに対して請求が送信されたとする）、信託銀行ノード１００Ａは、顧客情報テーブル３３２の更新要求をＷＥＢサーバ２００に対して送信する（Ｓ１１）。

【００４８】

更新要求を受信したＷＥＢサーバ２００の更新処理部２０１は、データベース３００における顧客情報テーブル３３２の対応するレコードに対して更新処理を行う（Ｓ２１）。さらにこのとき、更新処理部２０１は、更新したレコードから更新レコードダイジェストを計算し、当該更新レコードダイジェストを含むトランザクションを作成する。さらに、更新処理部２０１は、更新したレコードに作成したトランザクションのＩＤを対応付けて記憶させる。更新処理部２０１は、作成したトランザクションをＰ２Ｐネットワークにブロードキャストで送信する（Ｓ２２）。なお、ここで、更新処理部２０１の処理対象は更新したレコードであったが、レコードへの更新操作（テーブルのあるデータ項目の値を他の値に変更するという操作）を処理対象とし、更新操作ダイジェストを計算し、当該更新操作ダイジェストを含むトランザクションを作成する構成であってもよい。つまり、データの正当性検証の対象は、データそのものであってもよいし、データに対する操作であってもよい。この場合、更新処理部２０１は、銘柄情報テーブル３３１、顧客情報テーブル３３２、及び所有権情報テーブル３３３に対して、更新操作を行う度に、行った更新操作に関する情報を追加する。

【００４９】

作成されたトランザクションがブロードキャストされると、各ノード１００のマイニング部１０４は、それぞれマイニング処理を実行する。最も早くマイニングが完了したノード１００は、マイニングによって作成したブロックをブロードキャストすることで、ブロックチェーンの末尾に作成したブロックを登録する（Ｓ１２）。

【００５０】

次に、データベース３００に登録されたデータを照会する場合、まず、ノード１００は、登録内容の参照要求を、ネットワークＮを介してＷＥＢサーバ２００へ送信する（Ｓ１３）。ＷＥＢサーバ２００における参照処理部２０２は、参照要求があったレコードをデータベース３００から抽出し、抽出したレコードをハッシュ化して参照レコードダイジェストを計算する（Ｓ２３）。また、参照処理部２０２は、抽出したレコードに対応するトランザクションＩＤを指定して、ノード１００に対してデータ参照要求を送信する。これによって、参照処理部２０２は、ノード１００から更新レコードダイジェストを取得する（Ｓ２４）。

【００５１】

参照処理部２０２は、計算した参照レコードダイジェストと、取得した更新レコードダイジェストとを突き合わせ、データの正当性を検証する（Ｓ２５）。正当性が検証できた場合には、参照処理部２０２は、データベース３００から抽出した生データを、ノード１００へ送信する（Ｓ２６）。なお、更新処理部２０１の処理対象が更新操作である場合には、参照処理部２０２は、参照要求の対象となったテーブルの更新操作に関する情報からダイジェストを計算する。さらに参照処理部２０２は、トランザクションＩＤを指定してノード１００から取得したダイジェスト（更新操作ダイジェスト）と、計算したダイジェストとを突合する。

【００５２】

このように、本実施形態に係る改ざん検知システム１においては、データベース３００

に登録するデータを、ハッシュ化し、ブロックチェーン上においても登録する。これによって、データベース３００上のデータのハッシュ値と、対応するブロックチェーン上のダイジェストとを突合させることによって、改ざんを検知することができる。

【００５３】

＜ハードウェア構成＞

以下、図９を参照しながら、第１の実施形態及び第２の実施形態において上述してきたノード１００、及びＷＥＢサーバ２００をコンピュータ８００により実現する場合のハードウェア構成の一例を説明する。なお、それぞれの装置の機能は、複数台の装置に分けて実現することもできる。

【００５４】

図９に示すように、コンピュータ８００は、プロセッサ８０１、メモリ８０３、記憶装置８０５、入力Ｉ／Ｆ部８０７、データＩ／Ｆ部８０９、通信Ｉ／Ｆ部８１１、及び表示装置８１３を含む。

【００５５】

プロセッサ８０１は、メモリ８０３に記憶されているプログラムを実行することによりコンピュータ８００における様々な処理を制御する。例えば、ノード１００のブロードキャスト通信部１０１や要求部１０２、応答部１０３、マイニング部１０４、ＷＥＢサーバ２００の更新処理部２０１や参照処理部２０２、などは、メモリ８０３に一時記憶された上で、主にプロセッサ８０１上で動作するプログラムとして実現可能である。

【００５６】

メモリ８０３は、例えばＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等の記憶媒体である。メモリ８０３は、プロセッサ８０１によって実行されるプログラムのプログラムコードや、プログラムの実行時に必要となるデータを一時的に記憶する。

【００５７】

記憶装置８０５は、例えばハードディスクドライブ（ＨＤＤ）やフラッシュメモリ等の不揮発性の記憶媒体である。記憶装置８０５は、オペレーティングシステムや、上記各構成を実現するための各種プログラムを記憶する。この他、記憶装置８０５は、銘柄情報テーブル３３１や、顧客情報テーブル３３２、所有権情報テーブル３３３、及びブロックチェーンＤＢ１３１を記憶することも可能である。このようなプログラムやデータは、必要に応じてメモリ８０３にロードされることにより、プロセッサ８０１から参照される。

【００５８】

入力Ｉ／Ｆ部８０７は、ユーザからの入力を受け付けるためのデバイスである。入力Ｉ／Ｆ部８０７の具体例としては、キーボードやマウス、タッチパネル、各種センサ、ウェアラブル・デバイス等が挙げられる。入力Ｉ／Ｆ部８０７は、例えばＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）等のインタフェースを介してコンピュータ８００に接続されても良い。

【００５９】

データＩ／Ｆ部８０９は、コンピュータ８００の外部からデータを入力するためのデバイスである。データＩ／Ｆ部８０９の具体例としては、各種記憶媒体に記憶されているデータを読み取るためのドライブ装置等がある。データＩ／Ｆ部８０９は、コンピュータ８００の外部に設けられることも考えられる。その場合、データＩ／Ｆ部８０９は、例えばＵＳＢ等のインタフェースを介してコンピュータ８００へと接続される。

【００６０】

通信Ｉ／Ｆ部８１１は、コンピュータ８００の外部の装置と有線又は無線により、インターネットＮを介したデータ通信を行うためのデバイスである。通信Ｉ／Ｆ部８１１は、コンピュータ８００の外部に設けられることも考えられる。その場合、通信Ｉ／Ｆ部８１１は、例えばＵＳＢ等のインタフェースを介してコンピュータ８００に接続される。

【００６１】

表示装置８１３は、各種情報を表示するためのデバイスである。表示装置８１３の具体例としては、例えば液晶ディスプレイや有機ＥＬ（Ｅｌｅｃｔｒｏ－Ｌｕｍｉｎｅｓｃｅ

ｎｃｅ）ディスプレイ、ウェアラブル・デバイスのディスプレイ等が挙げられる。表示装置８１３は、コンピュータ８００の外部に設けられても良い。その場合、表示装置８１３は、例えばディスプレイケーブル等を介してコンピュータ８００に接続される。

【００６２】

［その他の実施形態］

以上説明した各実施形態は、本発明の理解を容易にするためのものであり、本発明を限定して解釈するためのものではない。本発明は、その趣旨を逸脱することなく、変更／改良され得るとととともに、本発明にはその等価物も含まれる。また、各実施形態は例示であり、異なる実施形態で示した構成の部分的な置換または組み合わせが可能であることは言うまでもなく、これらも本発明の特徴を含む限り本発明の範囲に包含される。

【００６３】

例えば、既述の実施形態において、改ざん検知システム１は、ＷＥＢサーバ２００を備える構成を説明した。しかし、これに限定されず、改ざん検知システム１は、ＷＥＢサーバ２００を備えなくてもよい。この場合、ＷＥＢサーバ２００において実装されていた各機能は、ノード１００上に実装される。

【００６４】

また、記述の実施形態において、ブロックチェーンＤＢ１３１のトランザクションに含まれるダイジェストはレコード単位であるとして説明したが、これに限定されない。例えば、トランザクションは、銘柄情報テーブル３３１、顧客情報テーブル３３２、及び所有権情報テーブル３３３の、テーブル単位に計算されたダイジェスト含む構成でもよい。また、トランザクションは全テーブルから計算されたダイジェストを含む構成でもよい。トランザクションがテーブル単位に計算されたダイジェストを含む場合、ＷＥＢサーバ２００の更新処理部２０１は、更新したレコードを含むテーブルからダイジェストを計算し、トランザクションを作成する。他方、参照処理部２０２は、参照要求の対象となったレコードを含むテーブルからダイジェストを計算し、ノード１００から取得したダイジェスト（テーブルのダイジェスト）と突合する。

【００６５】

さらに、更新処理部２０１は、更新レコードダイジェストを、更新後のレコードのすべての項目からではなく、更新後のレコードのうち、改ざんを検知したい項目のみから計算する構成でもよい。この場合、トランザクションは、改ざんを検知したい項目について計算されたダイジェストを含む構成でもよい。このとき、銘柄情報テーブル３３１、顧客情報テーブル３３２、及び所有権情報テーブル３３３は、項目ごとにトランザクションＩＤが割り当てられる。参照処理部２０２は、参照要求の対象となった項目それぞれからダイジェストを計算し、トランザクションＩＤを指定してノード１００から取得したダイジェスト（項目それぞれのダイジェスト）と突合する。

【００６６】

また、記述の実施形態において、更新処理部２０１はトランザクションを作成する際に、一意なＩＤを割り当てる構成を説明した。しかしこれに限定されず、更新処理部２０１は、データベース３００への書き込み処理において更新したレコードに割り当てられているＩＤ（銘柄ＩＤ、顧客ＩＤ、所有権ＩＤ）を作成したトランザクションに割り当てる構成でもよい。

【００６７】

さらに記述の実施形態において、マイニングにはＰｏＷの技術を用いる構成を説明したがこれに限定されない。例えばマイニング部１０４は、作成したブロックヘッダーがターゲットの値以下になるか否かにかかわらず、ブロックをブロックチェーンの末尾に追加する構成でもよい。この場合、ブロックチェーンＤＢ１３１において管理されるブロックは、ターゲット及びナンスを含まない構成でもよい。

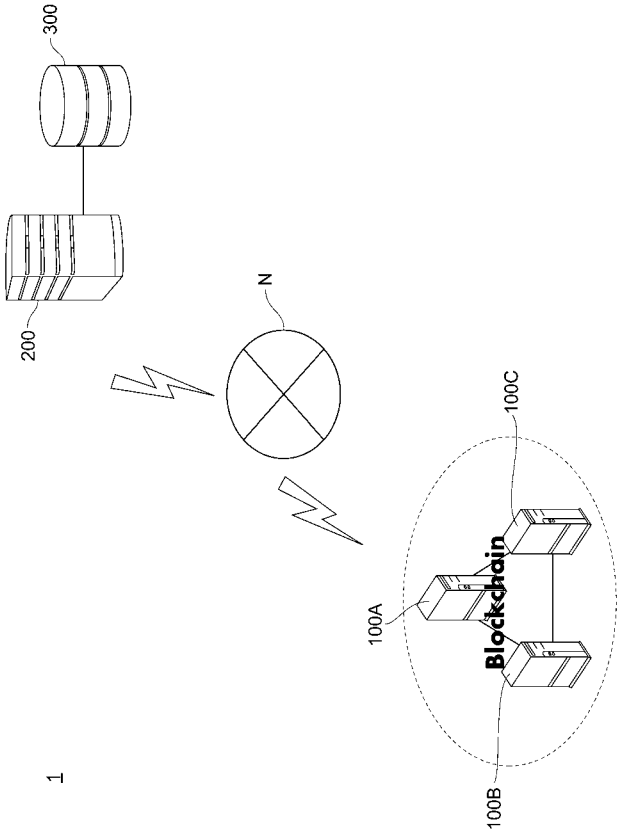
【符号の説明】

【００６８】

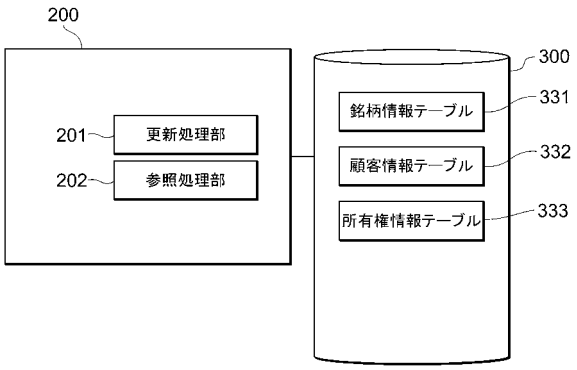
１　　改ざん検知システム

１００	ノード
１０１	ブロードキャスト通信部
１０２	要求部
１０３	応答部
１０４	マイニング部
１３１	ブロックチェーンＤＢ
２００	ＷＥＢサーバ
２０１	更新処理部
２０２	参照処理部
３００	データベース
３３１	銘柄情報テーブル
３３２	顧客情報テーブル
３３３	所有権情報テーブル

【図１】



【図２】



【図３】

銘柄ID	銘柄コード	銘柄名	売買単位	トランザクションID
S0001	C100	●●株	100	Tx001
S0002	C150	××株	20	Tx102
・・・	・・・	・・・	・・・	・・・

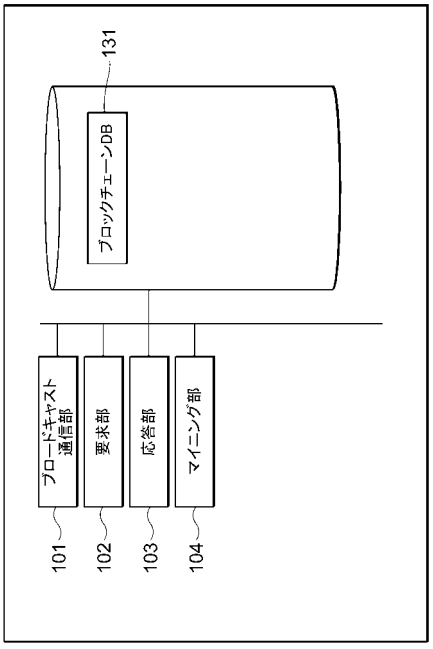
【図４】

顧客ID	顧客コード	顧客名	住所	トランザクションID
G0001	M100	山田太郎	東京都港区・・・	Tx012
G0002	M120	田中花子	大阪府大阪市・・・	Tx122
・・・	・・・	・・・	・・・	・・・

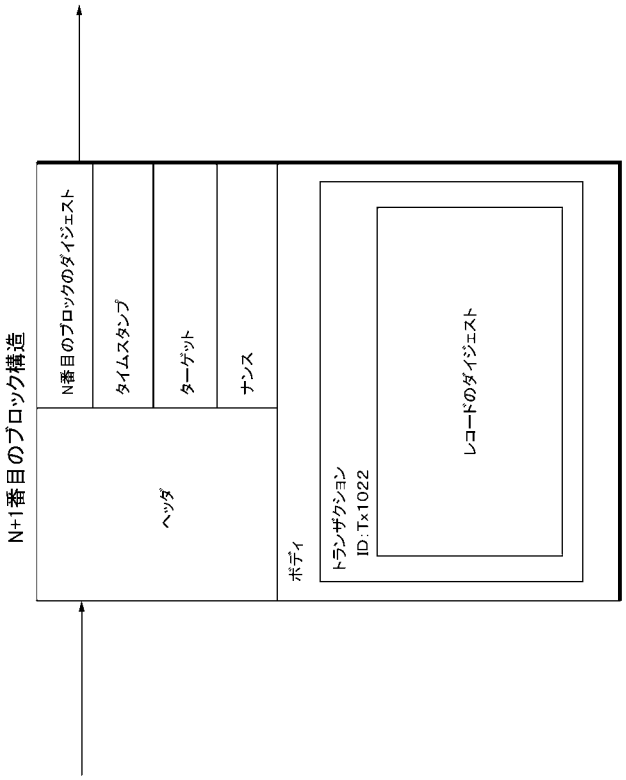
【図５】

所有権ID	銘柄ID	トランザクションID
G0001	S0002	Tx032
G0002	S0001	Tx219
・・・	・・・	・・・

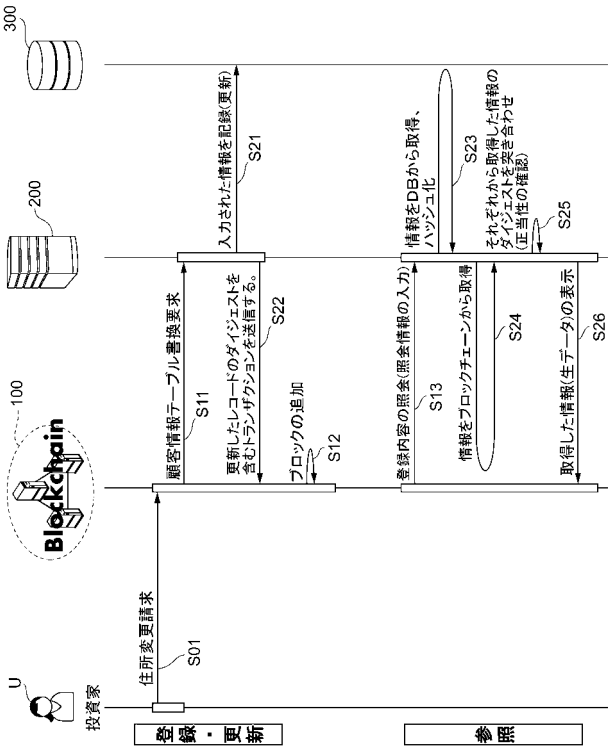
【図６】



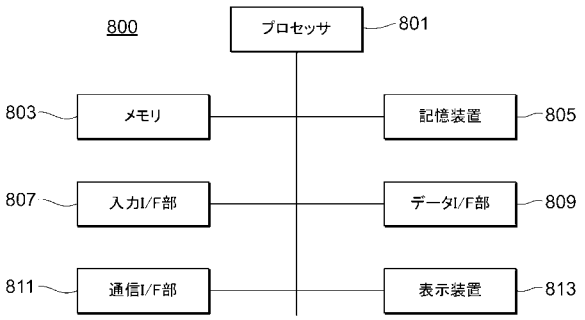
【図７】


N+1番目のブロック構造
N番目のブロックのダイジェスト
タイムスタンプ
ターゲット
ナンス
ヘッダ
ボディ
トランザクション
ID:Tx1022
レコードのダイジェスト

【図８】


300
200
100
U
投資家
Blockchain
住所変更請求
S01
顧客情報テーブル書換要求
S11
更新したレコードのダイジェストを含むトランザクションを送信する。
S22
ブロックの追加
S12
入力された情報を記録(更新)
S21
登録内容の照会(照会情報の入力)
S13
情報をブロックチェーンから取得
S24
情報をDBから取得、ハッシュ化
S23
それぞれから取得した情報のダイジェストを突き合わせ(正当性の確認)
S25
取得した情報(生データ)の表示
S26
登録・更新
参照

【図９】


800
プロセッサ
801
803
メモリ
記憶装置
805
807
入力I/F部
データI/F部
809
811
通信I/F部
表示装置
813