(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2017-200196
(P2017-200196A)
(43)公開日　平成29年11月2日(2017.11.2)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| H04L 9/32 | (2006.01) | H04L | 9/00 | 675B | 5J104 |
| G09C 1/00 | (2006.01) | G09C | 1/00 | 640D | |
| G06F 21/62 | (2013.01) | G06F | 21/62 | 318 | |
| G06F 21/64 | (2013.01) | G06F | 21/64 | | |

審査請求 未請求　請求項の数 10　ＯＬ　（全 14 頁）

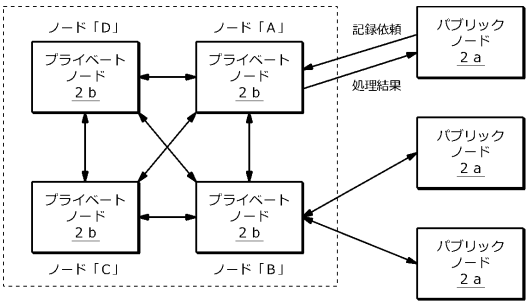
(21)出願番号　特願2017-108921 (P2017-108921)
(22)出願日　平成29年6月1日 (2017.6.1)
(62)分割の表示　特願2017-58095 (P2017-58095)の分割
原出願日　平成28年3月31日 (2016.3.31)

(71)出願人　514231103
株式会社ｂｉｔＦｌｙｅｒ
東京都港区赤坂三丁目５番５号
(74)代理人　100174078
弁理士　大谷　寛
(72)発明者　加納　裕三
東京都港区赤坂３－５－５　ストロング赤坂ビル８階　株式会社ｂｉｔＦｌｙｅｒ内
(72)発明者　小宮山　峰史
東京都港区赤坂３－５－５　ストロング赤坂ビル８階　株式会社ｂｉｔＦｌｙｅｒ内

Ｆターム(参考)　5J104 AA09　LA03　LA06　NA02　NA37　NA38　PA10

(54)【発明の名称】プライベートノード、プライベートノードにおける処理方法、及びそのためのプログラム

(57)【要約】　（修正有）
【課題】取引情報が記されたトランザクションをブロック化して分散データベースに取り込むネットワークにおいて、記録の信頼性と応用分野の拡張性との両立を図る。
【解決手段】ネットワークを構成するノードを、パブリックノード２ａと、プライベートノード２ｂとに区分する。パブリックノード２ａは、記録すべきトランザクションを生成する役割を担い、その後の分散データベースへの記録処理は、複数のプライベートノード２ｂが協働することによって行われる。トランザクションの生成については、信頼できないノードを含み得るパブリックノード２ａとして広く認めつつ、分散データベースへの記録処理については信頼できるプライベートノード２ｂに限定する。
【選択図】図２



【特許請求の範囲】
【請求項１】
パブリックノード群とプライベートノード群とを有するネットワークにおいて前記プライベートノード群を構成するプライベートノードにおける処理方法であって、　前記パブリックノード群から受信した複数のトランザクションを有するブロックを生成するステップと、　前記ブロックの承認依頼を前記プライベートノード群に送信するステップと、　前記プライベートノード群のうちの少なくともいずれかから承認結果を受け取るステップと、　前記プライベートノード群のうちの所定の数により承認が得られたことを条件に前記ブロックを確定させてブロックチェーンに追加するステップとを含むことを特徴とする処理方法。
【請求項２】
ブロックの新たな承認依頼は、前記プライベートノード群を構成する他のプライベートノードにおけるブロックの確定がなされるまで待機することを特徴とする請求項１に記載の処理方法。
【請求項３】
前記プライベートノード群を構成するプライベートノード間でブロック生成の順番が割り当てられていることを特徴とする請求項１に記載の処理方法。
【請求項４】
前記プライベートノード群は、それを構成するプライベートノードの数が制限されていることを特徴とする請求項１乃至３のいずれかに記載の処理方法。
【請求項５】
前記所定の数は、過半数であることを特徴とする請求項１乃至４のいずれかに記載の処理方法。
【請求項６】
前記ブロックの前記追加がなされた旨を前記ネットワークのノードに通知するステップをさらに含むことを特徴とする請求項１乃至５のいずれかに記載の処理方法。
【請求項７】
前記承認依頼は、前記プライベートノードの秘密鍵により署名されており、　前記承認結果は、前記承認依頼の依頼先の秘密鍵により署名されていることを特徴とする請求項１乃至６のいずれかに記載の処理方法。
【請求項８】
前記プライベートノード群を構成するプライベートノード間でそれぞれの公開鍵が共有されることを特徴とする請求項７に記載の処理方法。
【請求項９】
コンピュータに、パブリックノード群とプライベートノード群とを有するネットワークにおいて前記プライベートノード群を構成するプライベートノードにおける処理方法を実行されるためのプログラムであって、前記処理方法は、　前記パブリックノード群から受信した複数のトランザクションを有するブロックを生成するステップと、　前記ブロックの承認依頼を前記プライベートノード群に送信するステップと、　前記プライベートノード群のうちの少なくともいずれかから承認結果を受け取るステップと、　前記プライベートノード群のうちの所定の数により承認が得られたことを条件に前記プロックを確定させてブロックチェーンに追加するステップとを含むことを特徴とするプログラム。
【請求項１０】
パブリックノード群とプライベートノード群とを有するネットワークにおいて前記プライベートノード群を構成するプライベートノードであって、　前記パブリックノード群から受信した複数のトランザクションを有するブロックを生成して、前記ブロックの承認依頼を前記プライベートノード群に送信し、　前記プライベートノード群のうちの少なくともいずれかから承認結果を受け取って、前記プライベートノード群のうちの所定の数により承認が得られたことを条件に前記プロックを確定させてブロックチェーンに追加することを特徴とするプライベートノード。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、プライベートノード／パブリックノード用のノード装置およびコンピュータプログラムに係り、特に、取引情報を記したトランザクションをブロック化した上で、分散データベースに取り込むネットワークの仕組みに関する。
【背景技術】
【０００２】
従来、ブロックチェーンと称される技術が知られている。この技術は、ネットワーク上の多数のノード間で同一の記録を同期させる仕組みであって、既存の記録に新しい記録を追加する場合、記録単位となるブロックが、直前のブロックの内容（ハッシュ）を引き継ぎながら、チェーン状に次々と追加されていくことから、このように称されている。一般に、ブロックチェーンという用語は、ブロックがチェーン状に繋がったデータベースの構造を指すこともあるが、Ｐ２Ｐネットワークとして稼働する仕組みや、トランザクションの承認の仕組みなども含めた広義の意味で用いられることもあり、現時点において、その定義は定かではない。そこで、本明細書では、両者の混同を防ぐために、前者の狭義の意味で用いる場合は「ブロックチェーン」、後者の広義の意味で用いる場合は「ブロックチェーン技術」とそれぞれ称することとする。
【０００３】
ブロックチェーン技術は、ゼロダウンタイム、改ざんの困難性、低コストといった多くの利点を有しているため、ビットコイン（bitcoin）やその派生通貨を含む仮想通貨にとどまらず、様々な資産（asset）に関する情報をトランザクションとして管理する手法としても注目され始めている。例えば、非特許文献１には、信頼性確立のために重要な役割を果たし得るブロックチェーンを、様々な文書の存在証明やアイデンティティ証明に使うことが記載されている。
【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】ブロックチェーンはサイバー空間での信頼関係を築く――「存在証明」や「アイデンティティ証明」が持つ重要な意味、［online］、［平成２８年3月２８日検索］、インターネット＜URL：http://diamond.jp/articles/-/53050＞
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ブロックチェーン技術には、主に、パブリックノード方式と、プライベートノード方式とが存在する。パブリックノード方式は、ネットワーク上のノードとして誰もが参加可能な方式であり、ビットコインなどでも採用されている。誰もが参加可能であるということは、信頼できないノードが存在し得るため、データの改ざん等を防止するために、ＰＯＷ（Proof Of Work）やＰＯＳ（Proof Of Stake）といった高コストで遅いコンセンサスアルゴリズムが必要になる。一方、プライベートノード方式は、ネットワーク上のノードとして許可された者のみが参加可能な方式である。この方式は、信頼できるノードのみで構成されることから、パブリック方式のような高度なコンセンサスアルゴリズムを用いなくとも、十分な信頼性を確保できる。ブロックチェーン技術を用いて、様々な資産の取引に対応可能なシステムを構築する場合、高度な信頼性を確保するためには、プライベートノード方式の方が優れているが、上記のようなノードの制約上、応用分野が限られてしまうといった不都合がある。一方、パブリックノード方式は、様々な応用分野に柔軟に対応できる反面、信頼できないノードによるデータの改ざん等が問題となり、記録の信頼性の点で難がある。
【０００６】
本発明は、かかる事情に鑑みてなされたものであり、その目的は、取引情報が記されたト

ランザクションをブロック化して分散データベースに取り込むネットワークにおいて、記録の信頼性と応用分野の拡張性との両立を図ることである。

【課題を解決するための手段】

【０００７】

かかる課題を解決すべく、第１の発明は、取引情報を記したトランザクションを生成する複数のパブリックノードと、ノード数が制限された複数のプライベートノードと、それぞれのノードが同一の記録内容を同期して保持し、かつ、記録単位となるブロックが記録順序にしたがい繋がった分散データベースとを有するトランザクション処理ネットワークにおける、プライベートノード用のノード装置を提供する。このノード装置は、ブロック生成部と、承認依頼部と、ブロック確定部とを有する。ブロック生成部は、第１のパブリックノードによって生成された第１のトランザクションを含む第１のブロックを生成する。承認依頼部は、第１のブロックに自ノードの秘密鍵による署名を付した上で、予め設定されたｍ（ｍ≧２）個のプライベートノード群に対して、第１のブロックの承認依頼を送信する。ブロック確定部は、承認の依頼先となるプライベートノード群より第１のブロックの承認結果を受け取った場合、この承認結果に付された署名の正当性を承認の依頼先の公開鍵を用いて検証した上で、ｍ個のプライベートノードのうちのｎ（ｍ≧ｎ≧１）個以上の承認が得られたことを条件として、分散データベースに第１のブロックを追加することを確定する。

【０００８】

ここで、第１の発明において、上記ブロック確定部は、分散データベースに第１のブロックを追加することが確定した場合、第１のパブリックノードに対して、第１のトランザクションの処理結果を通知することが好ましい。

【０００９】

第１の発明において、承認応答部をさらに設けてもよい。この承認応答部は、承認の依頼元となるプライベートノードより第１のブロックの承認依頼を受信した場合、この承認依頼に付された署名の正当性を承認の依頼元の公開鍵を用いて検証した上で、自ノードの処理待ち領域に格納されたトランザクションに関するデータを参照して、承認依頼に係る第１のブロックの内容を検証すると共に、自ノードの秘密鍵による署名を付した承認結果を承認の依頼元となるプライベートノードに送信する。

【００１０】

第１の発明において、上記ｎは、上記ｍの過半数であることが好ましい。また、上記ブロック生成部は、自ノードで第１のブロックを生成した場合、少なくとも、他ノードによって生成された他のブロックを分散データベースに追加することが確定するまで、新たなブロックの承認依頼を連続して送信することなく待機してもよい。さらに、トランザクション処理ネットワークにおいて、プライベートノードの公開鍵を追加または失効させるプロトコルが予め用意されていることが好ましい。

【００１１】

第２の発明は、取引情報を記したトランザクションを生成する複数のパブリックノードと、ノード数が制限された複数のプライベートノードと、それぞれのノードが同一の記録内容を同期して保持し、かつ、記録単位となるブロックが記録順序にしたがい繋がった分散データベースとを有するトランザクション処理ネットワークにおける、パブリックノード用のノード装置を提供する。このノード装置は、トランザクション生成部と、記録依頼部と、結果受領部とを有する。トランザクション生成部は、第１のトランザクションを生成する。記録依頼部は、第１のトランザクションを少なくとも一つのプライベートノードに送信して、第１のトランザクションの記録を依頼する。結果受領部は、第１のトランザクションを受信したプライベートノードのいずれかにおいて生成され、かつ、第１のトランザクションを含む第１のブロックについて、ブロック確定条件を満たすことで、分散データベースに追加することが確定した場合、第１のトランザクションを受信したプライベートノードのいずれかより送信される、第１のトランザクションの記録が完了した旨の処理結果を受領する。ブロック確定条件は、公開鍵暗号による多重署名を用いたプライベート

ノード間の承認プロトコルによって、予め設定されたｍ（ｍ≧２）個のプライベートノードのうちのｎ（ｍ≧ｎ≧１）個以上の承認が得られたことである。

【００１２】

第３の発明は、取引情報を記したトランザクションを生成する複数のパブリックノードと、ノード数が制限された複数のプライベートノードと、それぞれのノードが同一の記録内容を同期して保持し、かつ、記録単位となるブロックが記録順序にしたがい繋がった分散データベースとを有するトランザクション処理ネットワークにおける、プライベートノード用のコンピュータプログラムを提供する。このコンピュータプログラムは、第１のパブリックノードによって生成された第１のトランザクションを含む第１のブロックを生成する第１のステップと、第１のブロックに自ノードの秘密鍵による署名を付した上で、予め設定されたｍ（ｍ≧２）個のプライベートノード群に対して、第１のブロックの承認依頼を送信する第２のステップと、承認の依頼先となるプライベートノード群より第１のブロックの承認結果を受け取った場合、この承認結果に付された署名の正当性を承認の依頼先の公開鍵を用いて検証した上で、ｍ個のプライベートノード群のうちのｎ（ｍ＞ｎ≧１）個以上の承認が得られたことを条件として、分散データベースに第１のブロックを追加することを確定する第３のステップとを有する処理をコンピュータに実行させる。

【００１３】

ここで、第３の発明において、上記第３のステップは、分散データベースに第１のブロックを追加することが確定した場合、第１のパブリックノードに対して、第１のトランザクションの処理結果を通知するステップを含むことが好ましい。

【００１４】

第３の発明において、承認の依頼元となるプライベートノードより第１のブロックの承認依頼を受信した場合、この承認依頼に付された署名の正当性を承認の依頼元の公開鍵を用いて検証した上で、自ノードの処理待ち領域に格納されたトランザクションに関するデータを参照して、承認依頼に係る第１のブロックの内容を検証すると共に、自ノードの秘密鍵による署名を付した承認結果を承認の依頼元となるプライベートノードに送信する第４のステップをさらに設けてもよい。

【００１５】

第３の発明において、上記ｎは、上記ｍの過半数であることが好ましい。また、上記第１のステップは、自ノードで第１のブロックを生成した場合、少なくとも、他ノードによって生成された他のブロックを分散データベースに追加するまで、新たなブロックの承認依頼を連続して送信することなく待機するステップを含んでいてもよい。さらに、上記トランザクション処理ネットワークにおいて、プライベートノードの公開鍵を追加または失効させるプロトコルが予め用意されていることが好ましい。

【００１６】

第４の発明は、取引情報を記したトランザクションを生成する複数のパブリックノードと、ノード数が制限された複数のプライベートノードと、それぞれのノードが同一の記録内容を同期して保持し、かつ、記録単位となるブロックが記録順序にしたがい繋がった分散データベースとを有するトランザクション処理ネットワークにおける、パブリックノード用のコンピュータプログラムを提供する。このコンピュータプログラムは、第１のトランザクションを生成する第１のステップと、第１のトランザクションを少なくとも一つのプライベートノードに送信して、第１のトランザクションの記録を依頼する第２のステップと、第１のトランザクションを受信したプライベートノードのいずれかにおいて生成され、かつ、第１のトランザクションを含むブロックについて、公開鍵暗号による多重署名を用いたプライベートノード間の承認プロトコルによって、予め設定されたｍ（ｍ≧２）個のプライベートノードのうちのｎ（ｍ≧ｎ≧１）個以上の承認が得られたことを条件として、分散データベースに第１のブロックを追加する場合、第１のトランザクションを受信したプライベートノードのいずれかより送信される、第１のトランザクションの記録が完了した旨の処理結果を受領する第３のステップとを有する処理をコンピュータに実行させる。

【発明の効果】
【００１７】
本発明によれば、トランザクション処理ネットワークを構成するノードを、パブリックノードと、プライベートノードとに区分している。パブリックノードは、取引情報を記したトランザクションを生成する役割を担い、その後の処理は、公開鍵暗号を用いた多重署名（マルチシグ）という低コストかつ高速なコンセンサスアルゴリズムを用いて、プライベートノード同士が協働することによって行われる。トランザクションの生成については、信頼できないノードを含み得るパブリックノードとして広く認めつつ、その後のブロックの生成や確定といった処理は、信頼できるプライベートノードに制限する。これにより、パブリックノード方式の利点である応用分野の拡張性と、プライベートノード方式の利点である記録の信頼性との両立を図ることができる。
【図面の簡単な説明】
【００１８】
【図１】トランザクション処理ネットワークの物理的な構成図
【図２】トランザクション処理ネットワークの論理的な構成図
【図３】プライベートノードにおける公開鍵の設定方法の説明図
【図４】パブリックノード用のノード装置の機能的なブロック図
【図５】プライベートノード用のノード装置の機能的なブロック図
【図６】トランザクションの記録処理のフローを示す図
【図７】トランザクションの処理待ち状態を示す図
【図８】多重署名によるブロック承認の説明図
【図９】データベース構造の説明図
【発明を実施するための形態】
【００１９】
図１は、本発明の一実施形態に係るトランザクション処理ネットワークの物理的な構成図である。このトランザクション処理ネットワーク１は、取引に関する情報を管理する管理システムとして用いられる。どのような取引を管理の対象とするかは、その用途に応じて、システムの仕様として予め決められている。例えば、銀行システムであれば、実通貨の取引が対象となり、証券システムであれば証券の取引が対象となる。本明細書において、「取引」とは、実通貨、仮想通貨、証券、不動産等の資産ないしこの資産の状態の保持（ストック）、資産の移転（フロー）はもとより、契約も含む概念をいい、契約は、資産にも負債にもなり得る。また、デリバティブの概念を導入することで、より広い範囲の取引を定義できる。
【００２０】
例えば、「ＡからＢへ１億円を送金する」や「ＡからＢへ特定株を５００株受け取る」といったことは、資産の移転（フロー）と同義であり、１方向の取引として捉えることができる。「Ａは１億円の預金を保有している」や「Ａは特定株を５００株持っている」といったことは、資産そのものとも捉えることができるし、資産の状態の保持（ストック）という概念としても捉えることができる。「ＡはＢから米ドルを１億円分購入する」や「ＡはＢから特定株を５００株分、１株１０００円で購入する」といったことは、資産の移転（フロー）が２つ同時に起こる２方向の取引として捉えることができる。
【００２１】
トランザクション処理ネットワーク１は、Ｐ２Ｐ（Peer to Peer）型のネットワークであり、純粋なＰ２Ｐのみならず、いわゆるハイブリッド型（一部にクライアントサーバ型の構成を含むもの）も含まれる。トランザクション処理ネットワーク１に参加（接続）するノード２は、１対１の対等の関係で通信（Ｐ２Ｐ通信）を行う。それぞれのノード２は、ノード装置として、コンピュータ３と、データベース４ａとを有している。取引に関する情報は、ネットワーク１上の分散データベース４、すなわち、ノード２毎に設けられたデータベース４ａの集合体によって管理される。ネットワーク１上に存在するすべてのデータベース４ａは、ブロックチェーン技術によって同期しており、基本的に、同一の記録内

容を保持している。権限を有するノード２が分散データベース４を更新する場合、自ノード２に接続されている他ノード２にその旨が通知され、以後、ノード間のＰ２Ｐ通信が繰り返されることによって、最終的に、ネットワーク１の全体に通知が行き渡る。これにより、すべてのノード２のデータベース４ａが更新され、同一の記録内容として共有されることになる。

【００２２】

ネットワーク１におけるＰ２Ｐ通信は、セキュリティを確保すべく、ＳＳＬ通信にて行われる。また、ノード２間で受け渡しされるトランザクションの正当性については、公開鍵暗号を用いた電子署名によって検証される。その前提として、それぞれのノード２は、自己が管理するアドレスの秘密鍵（暗証番号）を保持している（ネットワークアドレスの所有者＝秘密鍵の保有者）。公開鍵は、秘密鍵より一義的に特定される。ネットワークアドレスは、公開鍵そのものを用いてもよいし、ビットコイン等と同様、公開鍵をハッシュしてチェックサムを加えたものを用いてもよい。トランザクションの送り手（資産の移動元）は、送ろうとするトランザクションに自己が管理するアドレスの秘密鍵による署名を付した上で送信する。トランザクションの受け手は、受け取ったトランザクションに付された署名の正当性を、この秘密鍵に対応する公開鍵にて検証する。なお、ここで用いられる公開鍵暗号は、後述するブロックの承認に関する多重署名（マルチシグ）の公開鍵暗号とは別個のものである。マルチシグの秘密鍵は、上記のネットワークアドレスとは関係なく、プライベートノード２ｂのみが保有する。

【００２３】

なお、図１は、個々のノード２が他の全ノード２に接続されたフルコネクト型を示しているが、これは一例であって、どのようなトポロジーを採用してもよい。また、特定のノード２に情報を送信する場合、Ｐ２Ｐ通信による間接的な送信ではなく、アドレスを指定して送信先に直接送信できるようなプロトコルを導入してもよい。

【００２４】

図２は、一実施形態におけるトランザクション処理ネットワーク１の論理的な構成図である。本実施形態において、トランザクション処理ネットワーク１を構成するノード２には、パブリックノード２ａと、プライベートノード２ｂとが存在する。パブリックノード２ａは、取引の主体となるアプリケーションノードである（信頼できないノードを含み得る）。パブリックノード２ａは、取引に関する情報を記したトランザクションを生成し、これに署名した上で、プライベートノード２ｂ群に直接的または間接的に送信する。パブリックノード２ａは、プライベートノード２ｂ群へのトランザクションの記録依頼のみ行い、自身では、分散データベース４への記録処理は行わない。パブリックノード２ａにとって重要なことは、（最新でなくてもいいので）クエリーができること、新規に作成したトランザクションに署名すること、および、トランザクションの承認をプライベートノード２ｂ群に依頼することである。

【００２５】

なお、例えば、あるアドレスの残高を算出するといった検索時に、処理の高速化を図るべく、複数のパブリックノード２ａの一部において、データベース４ａの記録内容をインデックス付きで管理してもよい。分散データベース４のデータは基本的にKey-Value型なので、条件付の照会に非常に時間がかかるという欠点がある。その解決のために検索用の独自のインデックスを持ったノードを設けることで、応用範囲を拡張できる。

【００２６】

プライベートノード２ｂは、ノード数が制限された信頼できるノードであって、パブリックノード２ａより依頼されたトランザクションについて、分散データベース４への記録処理を行う。この記録処理は、後述するように、プライベートノード２ｂ群が協働することによって行われる。記録処理が完了した場合、処理結果が依頼元のパブリックノード２ａに通知される。プライベートノード２ｂにとって重要なことは、トランザクションを承認してブロック化した上で、分散データベース４に追加することであって、ビットコインなどの仮想通貨で採用されているマイニングや手数料といった報酬（インセンティブ）は、

必ずしも必要ではない。
【００２７】
複数のプライベートノード２ｂは、公開鍵暗号を用いて、ブロックの承認に関する多重署名（マルチシグ）によるブロックの承認を行う。そのため、図３に示すように、それぞれのプライベートノード２ｂは、自ノードの秘密鍵を有している。それとともに、公開鍵が記述されたコンフィグファイルをシステムの起動時に読み込むことによって、プライベートノード２ｂの間で公開鍵が共有されている。また、プライベートノード２ｂの公開鍵を追加または失効させるプロトコルが用意されており、このプロトコルを実行することで、コンフィグファイルを書き換えなくても、公開鍵を追加または失効させることができる。この公開鍵に関する情報は、厳密な管理が要求されるので、安全性を確保すべく、ＳＳＬ等によってやり取りされる。
【００２８】
図４は、パブリックノード２ａ用のノード装置（以下、「パブリックノード装置２０」という。）の機能的なブロック図である。このパブリックノード装置２０は、トランザクション生成部２０ａと、記録依頼部２０ｂと、結果受領部２０ｃとを有する。トランザクション生成部２０ａは、所定のフォーマットにしたがい、取引に関する情報が記されたトランザクションを生成する。取引に関する情報は、例えば、表示画面の指示にしたがいユーザが入力した入力情報より、あるいは、別のネットワークを通じて受信した受信情報より取得される。記録依頼部２０ｂは、トランザクション生成部２０ａによって生成されたトランザクションに、自己が管理するアドレスの秘密鍵による署名を付した上で、ノード2間のＰ２Ｐ通信を介してプライベートノード２ｂ群に送信し、トランザクションを記録すべき旨をプライベートノード２ｂ群に依頼する。結果受領部２０ｃは、いずれかのプライベートノード２ｂより送信されたトランザクションの処理結果を受領し、これをユーザに提示する。
【００２９】
図５は、プライベートノード２ｂ用のノード装置（以下、「プライベートノード装置２１」という。）の機能的なブロック図である。このプライベートノード装置２１は、署名検証部２２と、トランザクション処理部２３とを有する。署名検証部２２は、パブリックノード２ａより記録依頼として受け付けたトランザクションに付された署名の正当性を、秘密鍵に対応する公開鍵を用いて検証する。なお、署名の他に、その資産が二重使用されていないことなども併せて検証される。
【００３０】
トランザクション処理部２３は、署名が正当であると検証できたことを前提として、所定の条件を満たす場合に、トランザクションを分散データベース４に記録する。このトランザクション処理部２３は、ブロック生成部２３ａと、承認依頼部２３ｂと、ブロック確定部２３ｃと、承認応答部２３ｄとを有する。
【００３１】
ここで、プライベートノード装置２１は、２つの役割を担っている。一つは、自ノード２ｂがブロックを生成し、他ノード２ｂにブロックの承認を依頼する役割であり、そのための構成として、ブロック生成部２３ａと、承認依頼部２３ｂと、ブロック確定部２３ｃとが存在する。そして、もう一つは、他のプライベートノード２ｂが生成したブロックを承認する役割であり、そのための構成として、承認応答部２３ｄが存在する。このように、プライベートノード２ｂは、自ノード２ｂが生成したブロックの承認を他ノード２ｂに依頼する依頼方、および、他ノード２ｂによって生成されたブロックの承認を自ノード２ｂが行う承認方のどちらにもなり得る。
【００３２】
ブロック生成部２３ａは、トランザクションの記録の依頼元となるパブリックノード２ａより記録処理の依頼を受けたトランザクションを複数まとめることによって、ブロックを生成する。承認依頼部２３ｂは、ブロック生成部２３ａによって生成されたブロックに自

ノード２ｂの秘密鍵による署名を付した上で、システムのコンフィグとして予め設定されたｍ（ｍ≧２）個の他のプライベートノード２ｂに対して、ブロックの承認依頼を送信する。ブロック確定部２３ｃは、承認の依頼先となるプライベートノード２ｂよりブロックの承認結果を受信した場合、この承認結果に付された署名の正当性を、承認の依頼先の秘密鍵に対応する公開鍵を用いて検証した上で、以下のブロック確定条件を満たすか否かを判定する。

【００３３】

［ブロック確定条件］　ｍ（ｍ≧２）個のプライベートノード２ｂのうち、　ｎ（ｍ≧ｎ≧１）個以上の承認が得られたこと

【００３４】

このブロック確定条件において、ｎはｍの過半数であることが好ましい。これにより、合理的かつ現実的な範囲で承認の信頼性を確保することができる。例えば、図２に示した４つのプライベートノード２ｂが存在するケースでは、３個（ｍ＝３）のプライベートノード２ｂに承認を依頼し、そのうちの２個（ｎ＝２）以上の承認が得られたことをもって、ブロック確定条件が満たされることになる。

【００３５】

承認依頼に係るブロックがブロック確定条件を満たす場合には、このブロックを分散データベース４に追加することが確定し、これを満たさない場合には、分散データベース４へのブロックの追加は行われない。ブロック確定部２３ｃは、トランザクションの記録の依頼元となるパブリックノード２ａに対して、トランザクションの処理結果（ＯＫ／ＮＧ）を通知する。分散データベース４へのブロックの追加が確定した場合、自ノード２ｂのデータベース４ａにブロックが追加されると共に、ブロックの確定に伴い新たなブロックを追加する旨が、トランザクション処理ネットワーク１の全ノード２に通知される。この通知によって、すべてのノード２のデータベース４ａ、すなわち、分散データベース４が更新される。

【００３６】

一方、承認応答部２３ｄは、承認の依頼元となるプライベートノード２ｂよりブロックの承認依頼を受信した場合、この承認依頼に付された署名の正当性を、公開鍵（承認の依頼元の秘密鍵に対応するもの）を用いて検証する。また、承認応答部２３ｄは、自ノード２ｂに記録されているトランザクションに関するデータを参照して、承認依頼に係るブロックの内容(ブロック中のトランザクションの整合性を含む。)を検証する。そして、内容が正当であるとの検証結果が得られた場合、承認応答部２３ｄは、自ノード２ｂの秘密鍵による署名を付した承認結果を承認の依頼元となるプライベートノード２ｂに送信する。

【００３７】

なお、ブロック生成部２３ａは、プライベートノード２ｂのハッキング対策として、自ノード２ｂで一のブロックを生成した場合、少なくとも、他ノード２ｂによって生成された他のブロックを分散データベース４に追加することが確定するまで、新たなブロックの承認依頼を連続して送信することなく待機する。すなわち、同一のプライベートノード２ｂにおいて、ブロック確定の処理を連続して行うことは禁止されている。

【００３８】

つぎに、図６を参照しながら、トランザクションの記録処理のフローについて説明する。まず、あるパブリックノード２ａにおいて、取引に関する情報が記されたトランザクションＴｒが生成され（ステップ１）、このトランザクションＴｒに自己が管理するアドレスの秘密鍵による署名を付した上で、プライベートノード２ｂ群にトランザクションＴｒの記録依頼が送信される（ステップ２）。例えば、図７に示すように、資産の移動元ａに関するトランザクションＴｒ１については、移動元ａが管理するアドレスの秘密鍵による署名「ａ」が付され、トランザクションＴｒ２，Ｔｒ３についても同様に署名される。

【００３９】

トランザクションＴｒの記録依頼を受信したプライベートノード２ｂのそれぞれは、記録依頼に付された署名を、移動元の秘密鍵に対応する公開鍵を用いて検証する（ステップ３

）。図７に示したように、トランザクションＴｒ１に付された署名「ａ」については、移動元ａの秘密鍵に対応する公開鍵を用いて検証され、トランザクションＴｒ２，Ｔｒ３についても同様に検証される。なお、署名の他に、その資産が二重使用されていないことなども併せて検証されることは上述したとおりである。それぞれのプライベートノード２ｂにおいて、署名の正当性などが確認できた場合、トランザクションＴｒ１～Ｔｒ３は、自ノード２ｂの記憶装置における所定の記憶領域（処理待ち領域）に一時的に格納される（ステップ４）。また、このステップ４において、資産の移動元が正当でないとされた場合、依頼元となるパブリックノード２ａに対して、その旨が通知される。

【００４０】

ステップ５では、いずれかのプライベートノード２ｂにおいて、ブロックが生成される。このブロックは、自ノード２ｂの処理待ち領域に格納されている複数のトランザクションＴｒをまとめたものである。そして、ステップ６において、図８（ａ）に示すようなデータ構造を有する署名付の承認依頼が生成される。このデータ構造は、ブロックの承認を依頼する依頼元の署名欄と、複数のトランザクションＴｒをまとめたブロック本体と、ブロックの承認先の署名欄とを有する。ただし、同図の構成は、説明の便宜上のものであって、実際には、依頼元／承認先の署名欄を別ける必要はない。図２に示した４つのプライベートノード２ｂ群（ノード名をＡ～Ｄとする。）のうち、ノードＡがブロックを生成した場合、図８（ａ）の依頼元署名欄には、ノードＡの秘密鍵による署名「Ａ」が記入され、承認先署名欄（ノードＢ～Ｄの署名が記入される欄）はブランクとされる。ノードＡにて生成された承認依頼は、他のプライベートノード２ｂ、すなわち、３つのノードＢ～Ｄに送信される。

【００４１】

ステップ７～９は、ブロックの承認依頼を受信したプライベートノード２ｂ、すなわち、承認の依頼先Ｂ～Ｄの処理である。まず、ステップ７において、承認依頼に付された署名「Ａ」等の正当性が、承認の依頼元であるノードＡ等の公開鍵を用いて検証される（ステップ７）。このステップ７では、ノードＡだけでなく、その検証時点で付されている他の署名も一緒に検証される。基本的に、ノードＡ→Ｂ→Ｃ→Ｄのように順番に署名していき、過半数（ｎ）の署名が得られた時点で確定する。どのようにして順番を保つかについては、様々な実装方法が考えられる。なお、ブロックの署名の検証自体は、ハッキングされたブロックを信用することがないように、プライベートノード２ｂのみならず、すべてのパブリックノード２ａでも行われる。承認の依頼元が正当であるとされた場合には、ステップ８に進み、正当でないとされた場合には、ステップ８以降の処理は行われない。

【００４２】

ステップ８において、承認依頼に係るブロックの内容が検証される。具体的には、自ノード２ｂの処理待ち領域に格納されたトランザクションを参照して、ブロックの内容が少なくとも以下の承認条件を満たす場合に、ブロックを承認する。ブロックの内容が正当であるとされた場合には、ステップ９に進み、正当でないとされた場合には、ステップ９の処理は行われない（処理結果＝ＮＧ）。

【００４３】

［ブロックの承認条件］（１）ブロック中のすべてのトランザクションＴｒが自ノード２ｂにおいて未処理であること（重複記録の防止）（２）ブロック中のすべてのトランザクションＴｒの内容が、自ノード２ｂの処理待ち領域に格納されたトランザクションＴｒの内容と一致すること（データの改ざん防止）（３）個々のトランザクションＴｒの資産が未使用であること（資産の二重使用の禁止）

【００４４】

ステップ９において、署名付の承認結果が生成される。承認可の場合には、図８（ｂ）に示すように、承認先署名欄のうちの自ノード２ｂに割り当てられた欄に自己の秘密鍵による署名が記入される。署名が付された承認結果は、承認の依頼元Ａに送信される。

【００４５】

ステップ１０～１２は、ブロックの承認結果を受信したプライベートノード２ｂ、すなわ

ち、承認の依頼元Ａの処理である。まず、ステップ１０において、承認結果に付された署名の正当性が、承認の依頼元Ｂ～Ｄの公開鍵を用いて検証される（ステップ１０）。承認の依頼先が正当であるとされた場合には、ステップ１１に進み、正当でないとされた場合には、ステップ１２以降の処理は行われない。

【００４６】

ステップ１１において、ｍ個のプライベートノードのうちのｎ（ｍ≧ｎ≧１）個以上の承認が得られた場合、ブロック確定条件が満たされて、分散データベース４にブロックを追加することが確定する。図８（ｂ）の例では、承認を依頼した３つのノードＢ～Ｄのうち、２つのノードＢ，Ｃの承認は得られたが、ノードＤの承認は得られなかったことを意味している。この場合、ブロック確定条件が過半数以上の承認であるならば、ｎ／ｍ＝２／３となって条件を満たすことになる。逆に、ｎ＝０，１の場合には、ブロック確定条件は満たされない。

【００４７】

ブロック確定条件が満たされた場合、承認の依頼元Ａによって、確定したブロックを分散データベース４に記録する処理が行われる。具体的には、まず、自ノードＡにおいて、処理待ち領域から確定ブロックに含まれるトランザクションＴｒが削除され、自己のデータベース４に確定したブロックが追加される。また、自ノードＡに接続されている他ノードＢ～Ｄを含めて、トランザクション処理ネットワーク１の全体に、確定したブロックを新規に追加する旨の通知が送信される。すべてのノード２は、この確定ブロックの通知を受けた時点で、通知元の署名の検証を行った上で、自己のデータベース４ａに確定ブロックを追加する。また、処理待ち領域に未処理トランザクションＴｒを保持しているすべてのノード２（ノードＢ～Ｄを含む。）は、この通知をもって、確定ブロックに含まれるトランザクションＴｒを処理待ち領域から削除する（ステップ１３）。これに対して、ブロック確定条件が満たされない場合、今回生成したブロックはキャンセルされる。これによって、処理待ち領域の未処理トランザクションＴｒは引き続き保持され、次回以降のブロックの生成機会を待つことになる。

【００４８】

図９は、データベース４ａの構造の説明図である。この構造において、記録単位となるブロックは記録順序にしたがいチェーン状に繋がっている。それぞれのブロック（確定ブロック）は、複数のトランザクションと、直前のブロックのハッシュとを有している。具体的には、あるブロック２には、その前のブロック１から引き継いだ前ブロック１のハッシュＨ１が含まれている。そして、ブロック２のハッシュＨ２は、自ブロック２のトランザクション群と、前ブロック１から引き継がれたハッシュＨ１とを含めた形で算出され、このハッシュＨ２は、その次のブロックに引き継がれる。このように、直前のブロックの内容をハッシュとして引き継ぎながら（Ｈ０，Ｈ１，・・・）、記録順序にしたがい個々のブロックをチェーン状に繋げ、記録内容に一貫した連続性を持たせることで、記録内容の改ざんを有効に防止する。過去の記録内容が変更された場合、ブロックのハッシュが変更前と異なる値になり、改ざんしたブロックを正しいものとみせかけるには、それ以降のブロックすべてを作り直さなければならず、この作業は現実的には非常に困難である。

【００４９】

そして、ステップ１２において、いずれかのプライベートノード２ｂ（承認の依頼元Ａ）から、トランザクションＴｒの記録の依頼元となるパブリックノード２ａに、記録依頼に係るトランザクションＴｒの処理結果（ＯＫ／ＮＧ）が通知される。このパブリックノード２ａは、処理結果を受領し、ユーザに対して処理結果を提示する（ステップ１４）。以上の一連のプロセスを経て、トランザクションの記録処理が完了する。

【００５０】

なお、以上のようなトランザクションの記録処理では、複数のプライベートノード２ｂが同一のトランザクションを含む別個のブロックを同時に生成してしまう可能性、すなわち、プライベートノード２ｂ同士の処理の競合が生じる可能性がある。かかる問題は、例え

ば、ラウンドロビン（round robin）のように、プライベートノード２ｂ間でブロック生成の順番を割り当てて排他制御を行うことで、解決することができる。また、プライベートノード２ｂ群に優先順位を割り当てて、上記競合が生じた場合には、優先順位の高いプライベートノード２ｂのみに、競合したトランザクションの再処理を認めてもよい。

【００５１】

このように、本実施形態によれば、トランザクション処理ネットワーク１を構成するノード２を、パブリックノード２ａと、プライベートノード２ｂとに区分している。パブリックノード２ａは、記録すべきトランザクションを生成する役割を担い、その後の分散データベース４への記録処理は、プライベートノード２ｂ群が協働することによって行われる。トランザクションの生成については、信頼できないノードを含み得るパブリックノード２ａとして広く認めつつ、分散データベース４への記録処理については信頼できるプライベートノード２ｂに限定する。このように、パブリックノード２ａの役割と、プライベートノード２ｂの役割とを別けることで、パブリックノード方式の利点である応用分野の拡張性と、プライベートノード方式の利点である記録の信頼性との両立を図ることができる。

【００５２】

また、本実施形態によれば、信頼できるプライベートノード２ｂ相互の認証手法として、ＰＯＷやＰＯＳといった高コストで遅いコンセンサスアルゴリズムではなく、公開鍵暗号を用いた多重署名（マルチシグ）という比較的簡素なコンセンサスアルゴリズムを用いている。これにより、記録の信頼性を損なうことなく、大量のトランザクションを高速かつ確実に処理することが可能になる。

【００５３】

さらに、本実施形態によれば、特定のプライベートノード２ｂによるブロックの生成頻度が極端に高くならないように、同一のプライベートノード２ｂがブロックの承認依頼を連続して送信することを禁止している。これにより、特定のプライベートノード２ｂにブロックを常に生成させ続けて過剰な負荷をかけるなどのハッキング行為に対しても、有効に対処することができる。

【００５４】

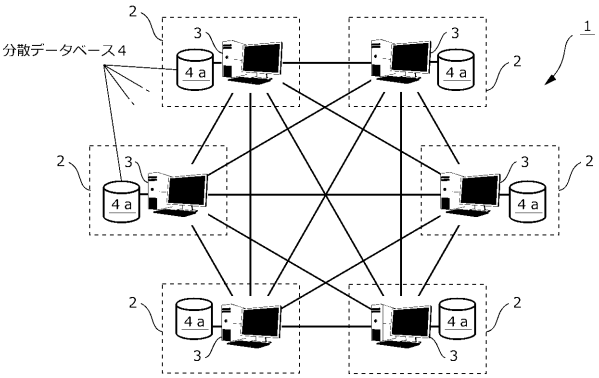
なお、本発明は、上述したパブリックノード装置２０またはプライベートノード装置２１を実現するコンピュータプログラムとしても捉えることができる。

【符号の説明】

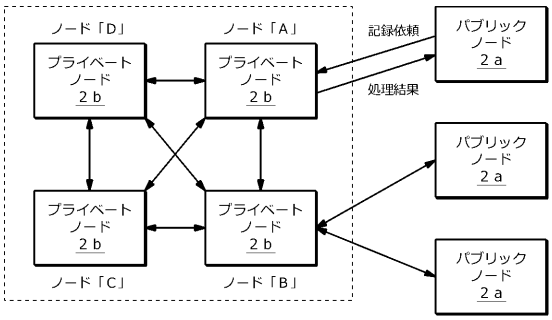
【００５５】

１　トランザクション処理ネットワーク　２　ノード　２ａ　パブリックノード　２ｂ　プライベートノード　３　コンピュータ　４　分散データベース　４ａ　データベース　２０　パブリックノード装置　２０ａ　トランザクション生成部　２０ｂ　記録依頼部　２１ｃ　結果受領部　２１　プライベートノード装置　２２　署名検証部　２３　トランザクション処理部　２３ａ　ブロック生成部　２３ｂ　承認依頼部　２３ｃ　ブロック確定部　２３ｄ　承認応答部

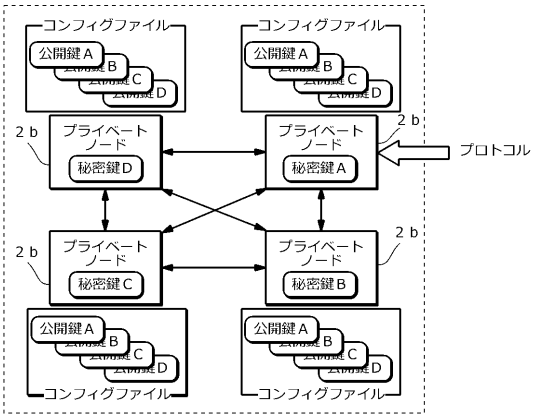
【図１】



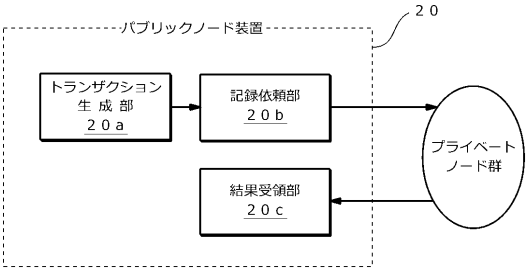

【図２】



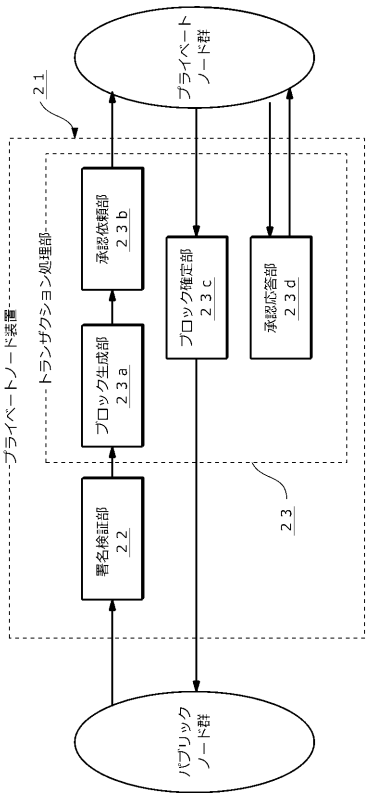

【図３】



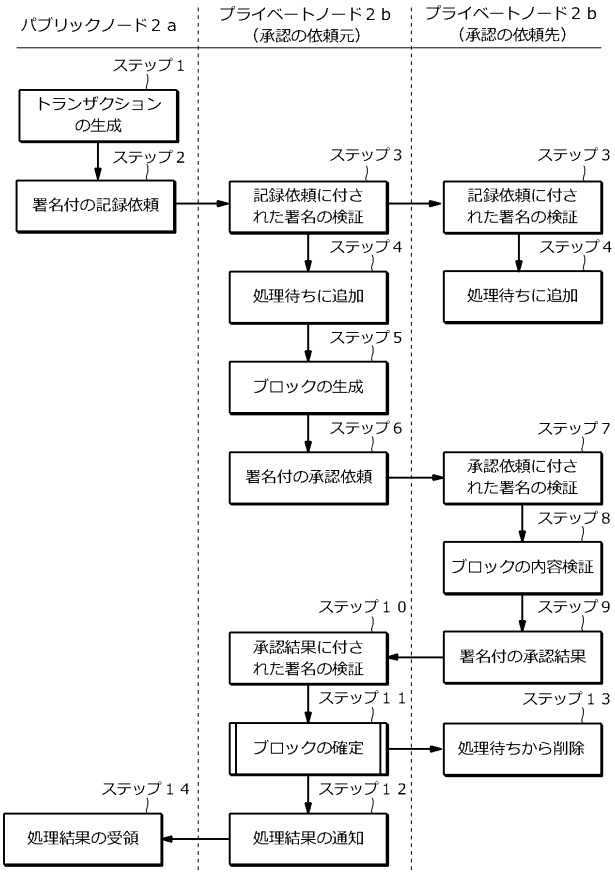

【図４】



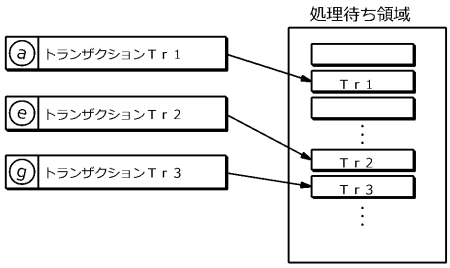

【図５】



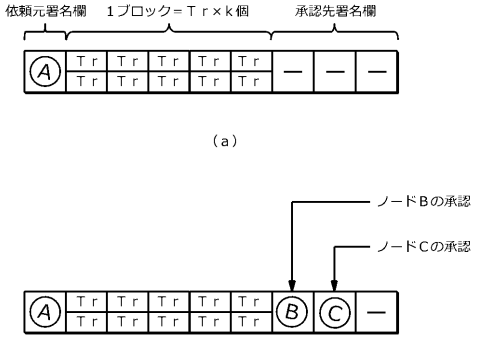

【図６】



【図７】


処理待ち領域
ａ
トランザクションＴｒ１
ｅ
トランザクションＴｒ２
ｇ
トランザクションＴｒ３
Ｔｒ１
Ｔｒ２
Ｔｒ３

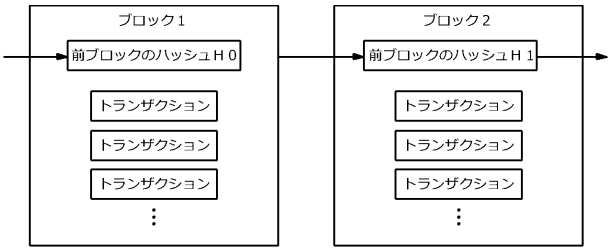
【図８】


依頼元署名欄
１ブロック＝Ｔｒ×ｋ個
承認先署名欄
Ａ
Ｔｒ
ー
ノードＢの承認
ノードＣの承認
Ｂ
Ｃ

（ａ）

（ｂ）

【図９】


ブロック１
前ブロックのハッシュＨ０
トランザクション
ブロック２
前ブロックのハッシュＨ１