(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6389350号
(P6389350)

(45)発行日　平成30年9月12日(2018.9.12)　(24)登録日　平成30年8月24日(2018.8.24)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675Z
G06F 21/64 (2013.01)　　H04L 9/00 675B
　　G06F 21/64

請求項の数 10　(全 18 頁)

(21)出願番号　特願2018-509457(P2018-509457)
(86)(22)出願日　平成29年3月30日(2017.3.30)
(86)国際出願番号　PCT/JP2017/013365
(87)国際公開番号　WO2017/170912
(87)国際公開日　平成29年10月5日(2017.10.5)
審査請求日　平成30年2月27日(2018.2.27)
(31)優先権主張番号　特願2016-71342(P2016-71342)
(32)優先日　平成28年3月31日(2016.3.31)
(33)優先権主張国　日本国(JP)

早期審査対象出願

(73)特許権者　514231103
株式会社ｂｉｔＦｌｙｅｒ
東京都港区赤坂九丁目７番１号
(74)代理人　100174078
弁理士　大谷　寛
(72)発明者　加納　裕三
東京都港区赤坂九丁目７番１号　株式会社ｂｉｔＦｌｙｅｒ内
(72)発明者　小宮山　峰史
東京都港区赤坂九丁目７番１号　株式会社ｂｉｔＦｌｙｅｒ内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】トランザクション処理装置、トランザクション処理方法、及びそのためのプログラム

(57)【特許請求の範囲】
【請求項１】
複数のトランザクションが含まれ、資産の保持元アドレスが複数存在する複合トランザクションの記録をブロックチェーンの分散ネットワークに対して依頼する方法であって、
受け取った複合トランザクションに自己が署名をすべき保持元アドレスが含まれる場合に、前記分散ネットワークを構成する第１のノードが、前記複合トランザクションを前記第１のノードの秘密鍵により署名するステップと、
前記秘密鍵による署名後に前記複合トランザクションに署名がされるべき保持元アドレスが残っている場合に、前記第１のノードが、前記分散ネットワークを構成する第２のノードに前記複合トランザクションを送信するステップと、
前記秘密鍵による署名後に前記複合トランザクションに署名がされるべき保持元アドレスが残っていない場合に、前記第１のノードが、前記分散ネットワークを構成する第３のノードに前記複合トランザクションを送信し、前記分散ネットワークに対する記録を依頼するステップと
を含み、
前記複合トランザクションに対する各署名は、前記複合トランザクションに含まれる複数のトランザクション全体を対象として付与することを特徴とする方法。
【請求項２】
前記分散ネットワークは、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ことを特徴とする請求項１に記載の方法。

【請求項３】
前記第１のノード及び前記第２のノードは、前記パブリックノード群を構成するノードであることを特徴とする請求項２に記載の方法。
【請求項４】
前記第３のノードは、前記プライベートノード群を構成するノードであることを特徴とする請求項２又は３に記載の方法。
【請求項５】
受け取った複合トランザクションに自己が署名をすべき保持元アドレスが含まれない場合に、前記第１のノードが、前記分散ネットワークを構成する第４のノードに前記受け取った複合トランザクションを転送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４のいずれかに記載の方法。
【請求項６】
前記第４のノードは、前記パブリックノード群を構成するノードであることを特徴とする請求項５に記載の方法。
【請求項７】
前記第１のノードが、前記分散ネットワークに対する記録が完了したことの通知を受領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６のいずれかに記載の方法。
【請求項８】
前記複合トランザクションは、資産の保持元アドレスが三以上であることを特徴とする請求項１乃至７のいずれかに記載の方法。
【請求項９】
ブロックチェーンの分散ネットワークを構成する第１のノードに、複数のトランザクションが含まれ、資産の保持元アドレスが複数存在する複合トランザクションの記録を前記分散ネットワークに対して依頼する方法を実行させるためのプログラムであって、前記方法は、
受け取った複合トランザクションに自己が署名をすべき保持元アドレスが含まれる場合に、前記第１のノードが、前記複合トランザクションを前記第１のノードの秘密鍵により署名するステップと、
前記秘密鍵による署名後に前記複合トランザクションに署名がされるべき保持元アドレスが残っている場合に、前記第１のノードが、前記分散ネットワークを構成する第２のノードに前記複合トランザクションを送信するステップと、
前記秘密鍵による署名後に前記複合トランザクションに署名がされるべき保持元アドレスが残っていない場合に、前記第１のノードが、前記分散ネットワークを構成する第３のノードに前記複合トランザクションを送信し、前記分散ネットワークに対する記録を依頼するステップと
を含み、
前記複合トランザクションに対する各署名は、前記複合トランザクションに含まれる複数のトランザクション全体を対象として付与することを特徴とするプログラム。
【請求項１０】
複数のトランザクションが含まれ、資産の保持元アドレスが複数存在する複合トランザクションの記録をブロックチェーンの分散ネットワークに対して依頼する第１のノードであって、
受け取った複合トランザクションに自己が署名をすべき保持元アドレスが含まれる場合に、前記複合トランザクションを前記第１のノードの秘密鍵により署名し、
前記秘密鍵による署名後に前記複合トランザクションに署名がされるべき保持元アドレスが残っている場合に、前記分散ネットワークを構成する第２のノードに前記複合トランザクションを送信し、
前記秘密鍵による署名後に前記複合トランザクションに署名がされるべき保持元アドレスが残っていない場合に、前記分散ネットワークを構成する第３のノードに前記複合トランザクションを送信して、前記分散ネットワークに対する記録を依頼し、

前記複合トランザクションに対する各署名は、前記複合トランザクションに含まれる複数のトランザクション全体を対象として付与することを特徴とする第１のノード。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、トランザクション処理装置およびトランザクション処理用コンピュータプログラムに係り、特に、一つのトランザクションにて扱うことができる取引形態の拡張に関する。

【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】

従来のブロックチェーン技術において、１つのトランザクションにて扱うことができる取引形態は、例えば「ＡからＢに１００円を渡す」といった如く、１つの資産移動に限られている。そのため、例えば、「ＡからＢに１００円を渡す代わりに、ＢからＡに１ドルを渡す」といった交換、すなわち、複数の資産移動を伴う複合的な取引形態については、１つのトランザクションで扱うことはできなかった。

【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、トランザクションに記された取引内容の信頼性を確保しつつ、１つのトランザクションで複合的な取引形態を扱うことを可能にすることである。

【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、ネットワーク上のノードからの依頼に基づいて、取引情報が記されたトランザクションをデータベースに記録するトランザクション処理装置を提供する。このトランザクション処理装置は、署名検証部と、トランザクション

処理部とを有する。署名検証部は、資産の保持元が複数存在する複合的な取引が記されたトランザクションについて、トランザクションに付された複数の署名であって、複数の保持元のそれぞれが管理するアドレスの秘密鍵による署名の正当性を、秘密鍵のそれぞれに対応する公開鍵を用いて検証する。トランザクション処理部は、複数の署名のすべてが正当であることを条件に、トランザクションをデータベースに記録する。

【０００８】

ここで、第１の発明において、上記トランザクション処理部は、ブロック生成部と、承認依頼部と、ブロック確定部とを有していてもよい。ブロック生成部は、トランザクションを含むブロックを生成する。承認依頼部は、ブロックに自ノードの秘密鍵による署名を付した上で、ｍ（ｍ≧２）個のノードに対して、ブロックの承認依頼を送信する。ブロック確定部は、承認の依頼先となるノード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公開鍵を用いて検証した上で、ｍ個のノードのうちのｎ（ｍ≧ｎ≧１）個以上の承認が得られたことを条件として、このブロックについて、トランザクションをブロック単位で記録するデータベースに追加することを確定する。

【０００９】

第２の発明は、取引情報が記されたトランザクションを生成して、ネットワーク上のノードにトランザクションの記録を依頼するトランザクション処理装置を提供する。このトランザクション処理装置は、転送部と、記録依頼部とを有する。転送部は、資産の保持元が複数存在する複合的な取引が記されたトランザクションについて、自己の管理するアドレスが署名を付すべき保持元のアドレスのいずれかに該当し、かつ、自己が管理するアドレス以外に署名を付すべき保持元のアドレスが残っている場合、トランザクションに自ノード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し、他ノードに転送する。記録依頼部は、トランザクションについて、自己の管理するアドレスが署名を付すべき保持元のアドレスのいずれかに該当し、かつ、自己が管理するアドレス以外に署名を付すべき保持元のアドレスが残っていない場合、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、すべての保持元の署名が付されたトランザクションを送信し、トランザクションをデータベースに記録すべき旨を、データベースへの記録権限を有するノードに依頼する。

【００１０】

第３の発明は、ネットワーク上のノードからの依頼に基づいて、取引情報が記されたトランザクションをデータベースに記録するトランザクション処理用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、資産の保持元が複数存在する複合的な取引が記されたトランザクションについて、トランザクションに付された複数の署名であって、複数の保持元のそれぞれが管理するアドレスの秘密鍵による署名の正当性を、秘密鍵のそれぞれに対応する公開鍵を用いて検証する第１のステップと、複数の署名のすべてが正当であることを条件に、トランザクションをデータベースに記録する第２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。

【００１１】

ここで、第３の発明において、上記第２のステップは、トランザクションを含むブロックを生成するステップと、ブロックに自ノードの秘密鍵による署名を付した上で、ｍ（ｍ≧２）個のノードに対して、ブロックの承認依頼を送信するステップと、承認の依頼先となるノードよりブロックの承認結果を受信した場合、当該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、ブロックについて、トランザクションをブロック単位で記録するデータベースに追加することを確定するステップとを有していてもよい。

【００１２】

第４の発明は、取引情報が記されたトランザクションを生成して、ネットワーク上のノードにトランザクションの記録を依頼するトランザクション処理用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、資産の保持元が複数存在する複合的な取引が記されたトランザクションについて、自己の管理するアドレスが署名を付すべき保持元のアドレスのいずれかに該当し、かつ、自己が管理するアドレス以外に署名を付すべき保持元のアドレスが残っている場合、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し、他のノードに転送する第１のステップと、トランザクションについて、自己が管理するアドレスが署名を付すべき保持元のアドレスのいずれかに該当し、かつ、自己が管理するアドレス以外に署名を付すべき保持元のアドレスが残っていない場合、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、すべての保持元の署名が付されたトランザクションを送信し、トランザクションをデータベースに記録すべき旨を、データベースへの記録権限を有するノードに依頼する第２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】

第１から第４の発明において、上記データベースは、ネットワーク上の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であることが好ましい。また、上記ネットワークは、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、データベースへの記録権限を有するノード数が制限された複数のプライベートノードとを有し、上記資産の保持元は、パブリックノードが管理するアドレスであることが好ましい。

【発明の効果】

【００１４】

本発明によれば、複合的な取引に関する取引情報を一つのトランザクションに記すことを許容する。そして、複合的な取引に関するトランザクションをデータベースに記録する場合、なりすまし（取引主体となる当事者を含む）を防止すべく、資産の保持元の全署名が正当であることが記録の条件の一つとされる。これにより、複合的な取引を構成する個々の取引について、データベースに同時かつ一体で記録されることが保証され、一方のみが記録され、他方が未記録といった状況が一時的であれ生じることを回避できる。その結果、トランザクションに記された取引内容の信頼性を確保しつつ、単一のトランザクションで多様な取引形態を扱うことができる。

【図面の簡単な説明】

【００１５】

【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】単一トランザクションおよび複合トランザクションの説明図
【図５】パブリックノード用のトランザクション処理装置の機能的なブロック図
【図６】複合トランザクションの署名フローの説明図
【図７】プライベートノード用のトランザクション処理装置の機能的なブロック図
【図８】トランザクションの記録処理のフローを示す図
【図９】トランザクションの処理待ち状態を示す図
【図１０】多重署名によるブロック承認の説明図
【図１１】データベース構造の説明図

【発明を実施するための形態】

【００１６】

図１は、本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。

【００１７】

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。この取引形態では、資産の移動元Ａは資産の保持元であり、資産の移動先Ｂは資産の新たな保持元となる。「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。この資産の状態の保持（ストック）の場合、複数の資産の移動元（保持元）は存在するものの、実際には資産は移動しないというステータスを管理することにより、資産の移転（フロー）と同様に複合的な取引を記述することができる。「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。「資産の移動元が複数存在する複合的な取引」といった場合、複数の資産の移転（フロー）、複数の資産の状態の保持（ストック）、あるいは複数の資産の移転（フロー）と状態の保持（ストック）が混在した取引を意味する。

【００１８】

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。

【００１９】

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、資産の保持元（移動元）のすべてが、自己が管理するアドレスの秘密鍵による署名を付することを条件に、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。

【００２０】

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。

【００２１】

図２は、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。

【００２２】

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。

【００２３】

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。

【００２４】

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。

【００２５】

図４は、単一トランザクションおよび複合トランザクションの説明図である。本トランザクション処理ネットワーク１が取り扱うトランザクションには、単一トランザクションと、複合トランザクションとが存在する。２つのタイプのトランザクションは、どちらもシステム処理上は同じ一つのトランザクションとして取り扱われ、すべての資産の保持元（一つを含む）について、その保有者の署名が必要となる。単一トランザクションは、同図（ａ）に示すように、「移動元Ａ（保持元）から移動先Ｂ（新たな保持元）へ１００円を移動する」といった如く、１つの資産の移動について記されており、資産の移動元Ａが管理するアドレスの秘密鍵による署名が付される。一方、複合トランザクションは、同図（ｂ）に示すように、「移動元Ａ（保持元）から移動先Ｂ（新たな保持元）へ１００円を移動すると共に、移動元Ｂ（保持元）から移動先Ａ（新たな保持元）へ１ドルを移動する」といった２つの資産移動を伴う取引、すなわち、資産の交換について記されている。こ

の場合、資産の移動元が２つ存在するため、一方の資産の移動元Ａ（保持元）が管理するアドレスの秘密鍵による署名、および、他方の資産の移動元Ｂ（保持元）が管理するアドレスの秘密鍵による署名の双方が要求される。

【００２６】

複合トランザクションに記すことができる資産移動は２つに限らず、３つ以上の資産移動を伴う取引形態についても記すことができる。例えば、移動元Ａから移動先Ｂへ１００円、移動元Ｂから移動先Ｃへ１ドル、移動元Ｃから移動先Ａへ飲料１本をそれぞれ移動させるといった如くである（３者間の交換）。この取引形態は、３つの資産移動を伴うので、３つの移動元Ａ～Ｃが管理するアドレスの秘密鍵による署名（３つ）が要求される。また、複合トランザクションをさらに複合させることも可能である。この場合、トランザクションには資産の移動以外にもメタデータを記載できるエリアがあるので、これを活用すればよい。

【００２７】

図５は、パブリックノード２ａ用のトランザクション処理装置の機能的なブロック図である。このトランザクション処理装置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、転送部２０ｄ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（単一トランザクションまたは複合トランザクション）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。

【００２８】

単一トランザクションの場合、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】

一方、複合トランザクションの場合、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は、図６に示す署名フローを経て、プライベートノード２ｂ群に送信される。まず、あるノード２ａにおいて、資産の保持元Ａ，Ｂよりなる複合的な取引を記した複合トランザクションが、トランザクション生成部２０ａによって生成される（同図（ａ））。この段階では、「移動元Ａから移動先Ｂへ１００円の資金移動」について、移動元Ａの署名欄、および、「移動元Ｂから移動先Ａへの１ドルの資金移動」について、移動元Ｂの署名欄は、共にブランクとされる。ただし、自己が管理するアドレスが移動元Ａ，Ｂのいずれかに該当する場合には、この段階で、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が付される（同図（ｂ））。生成された複合トランザクションは、Ｐ２Ｐ通信によって他のパブリックノード２ａに転送される。

【００３０】

複合トランザクションのフォーマットは、複数のトランザクションを格納可能なデータ構造であり、各トランザクションに対応した複数の電子署名も格納可能となっている。あるトランザクションにより表される資産の保持元による署名は、当該トランザクションのみでなく、複数のトランザクション全体を対象として行うことができ、これにより、一部の保持元による署名の後に、複数のトランザクションの一部又は全てに改竄がなされた場合に無効として取り扱うことができる。

【００３１】

複合トランザクションを受け取ったノード２ａにおいて、転送部２０ｄは、自己の管理するアドレスが署名を付すべきアドレスＡ，Ｂのいずれかに該当する場合、該当する署名欄（ブランク）に、自己が管理するアドレスの秘密鍵による署名を記入する。例えば、同図（ｂ）に示したように、自己が管理するアドレスがＡの場合、「移動元Ａから移動先Ｂ

へ１００円の資金移動」の署名欄に署名「Ａ」が記入される。そして、転送部２０ｄは、自己が管理するアドレス以外に署名を付すべきアドレスが残っている場合（本ケースでは署名「Ｂ」が未記入）、署名「Ａ」が付されたトランザクションを、Ｐ２Ｐ通信によって他のパブリックノード２ａに転送する。なお、この転送は、Ｐ２Ｐネットワークを介さない他の転送・交換手段（例えば、外部のネットワークを用いたデータ転送等）で行ってもよい。

【００３２】

一方、複合トランザクションを受け取ったノード２ａにおいて、転送部２０ｄは、自己の管理するアドレスが署名を付すべきアドレスＡ，Ｂのいずれかにも該当しない場合、このノード２ａは単なる中継ノードにすぎないので、受け取った複合トランザクションをそのまま他のパブリックノード２ａに転送する（同図（ｃ））。

【００３３】

そして、複合トランザクションを受け取ったノード２ａにおいて、自己の管理するアドレスがＡ，Ｂのいずれかに該当し、かつ、自己が管理するアドレス以外に署名を付すべきアドレスが残っていない場合、記録依頼部２０ｂは、自己が管理するアドレスの秘密鍵による署名を、トランザクションに記入する。例えば、同図（ｄ）に示したように、自己の管理するアドレスがＢの場合、「移動元Ｂから移動先Ａへ１ドルの資金移動」の署名欄に署名「Ｂ」が記入される。そして、記録依頼部２０ｂは、すべての署名「Ａ」，「Ｂ」が付された複合トランザクションを送信し、プライベートノード２ｂ群に対して、複合トランザクションを分散データベース４に記録すべき旨を依頼する。プライベートノード２ｂ群は、分散データベース４への記録権限を有しており、かつ、秘密鍵による署名「Ａ」，「Ｂ」を検証する公開鍵を有している。

【００３４】

図７は、プライベートノード２ｂ用のトランザクション処理装置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検証する。具体的には、単一トランザクションの場合には、トランザクションに付された一つの署名の正当性が、この秘密鍵に対応する公開鍵を用いて検証される。また、複合トランザクションの場合には、複数の署名の正当性が、それぞれの秘密鍵に対応する公開鍵を用いて検証される。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。

【００３５】

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、および、その他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。

【００３６】

ここで、トランザクション処理装置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。

【００３７】

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。ブロックの生成において、単一トランザクション／複合トランザクションの区別はなく、どちらも同等の一つのトランザクションとして取り扱われる。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。承認の依頼先のノードには、自ノードを含めてもよい。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。

【００３８】

［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

【００３９】

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。

【００４０】

ｍは、一桁、二桁等の限られた数以下であることが好ましく、ブロック確定条件に応じて、５個、９個等の奇数個であることが好ましいことがある。ｎは、ｍの過半数であることに加えて、過半数以上の指定された所定の数であることが好ましいことがある。

【００４１】

ブロック確定条件としては、上述の説明では一ノード一票の承認が可能とされているところ、各ノードに任意の正の実数の票を与え、その過半数によって承認が得られたことと判定することもできる。この場合、「過半数」とは、総票数に対する半数を超える数であることを付言する。

【００４２】

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。

【００４３】

全ノード２に直接的又は間接的に通知されることが求められるが、ブロックの確定に伴い新たなブロックを追加する旨が全ノード２に直接的に通知される場合のほか、プライベートノード２ｂの全て及びパブリックノード２ａの一部、プライベートノード２ｂの全て、プライベートノード２ｂの一部及びパブリックノード２ａの一部、又はプライベートノード２ｂの一部に通知される場合も考えられる。

【００４４】

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。

【００４５】
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、すなわち、プライベートノード２ｂがハッキングされたときのために、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。
【００４６】
つぎに、図８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９に示すように、資産の移動元ｅに係る単一トランザクションＴｒ２については、この移動元ｅが管理するアドレスの秘密鍵による署名「ｅ」が付され、資産の移動元ｇに係る単一トランザクションＴｒ３については、移動元ｇが管理するアドレスの秘密鍵による署名「ｇ」が付される。また、資産の移動元ａ，ｂに係る複合トランザクションＴｒ１については、図６に示した署名フローを経て、これらの移動元が管理するアドレスの秘密鍵による署名「ａ」，「ｂ」が付される。
【００４７】
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９に示したように、単一トランザクションＴｒ２，Ｔｒ３に付された署名「ｅ」，「ｇ」については、移動元ｅ，ｇの秘密鍵に対応する公開鍵を用いて検証される。また、複合トランザクションＴｒ１に付された署名「ａ」，「ｂ」については、移動元ａ，ｂの秘密鍵に対応した公開鍵を用いて検証される。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、自己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、依頼元／資産の移動元が正当でないとされた場合、依頼元／資産の移動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。
【００４８】
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（単一／複合の種別は問わず。）をまとめたものである。そして、ステップ６において、図１０（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１０（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。
【００４９】
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。トランザクション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。

【００５０】

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）。

【００５１】

［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）

【００５２】

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１０（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。

【００５３】

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。

【００５４】

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１０（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。

【００５５】

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指示が送信される。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。

【００５６】
図１１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、それ以降の全ブロックのハッシュを再計算しなければならず、この作業は現実的には非常に困難である。
【００５７】
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。
【００５８】
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。
【００５９】
このように、本実施形態によれば、資産の移動元が複数存在する複合的な取引について、複合トランザクションとして単一のトランザクションにまとめて記すことを許容する。これにより、複合的な取引について、データベース４ａ（または４）に同時かつ一体で記録されることが保証される。複合的な取引について、それぞれの取引を別個のトランザクションとして作成とした場合、一方のトランザクションがブロックチェーンに組み込まれ、他方のトランザクションがブロックチェーンに未だ組み込まれていないという不整合が生じ得る。これに対して、本実施形態のように、両者を一つのトランザクションで取り扱えば、そのような不整合は生じない。その結果、記録状況に不整合を生じることなく、単一のトランザクションで、交換に代表されるような多様な取引形態を扱うことが可能となる。
【００６０】
また、本実施形態によれば、複合トランザクションについて、資産の移動元のそれぞれが署名を付することを正当性の条件の一つとしているので、なりすまし（取引主体となる当事者を含む）を防止でき、トランザクションに記された取引内容の信頼性を確保できる。また、取引Ａの成立を条件として取引Ｂを成立させるような形態（交換）を取り扱うことも可能となる。なお、上述したように、トランザクションの正当性の条件としては、他にも、その資産が二重使用されていないことが存在する。
【００６１】
また、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。

【００６２】

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。

【００６３】

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。

【００６４】

なお、上述した実施形態では、パブリックノード２ａと、プライベートノード２ｂとを有するトランザクション処理システム１について説明した。しかしながら、複合トランザクションの導入による取引形態の拡張という概念は、これに限定されるものではなく、パブリックノード方式やプライベートの方式といったブロックチェーン技術全般に広く適用することができる。また、プライベートノード２ｂ間のコンセンサスアルゴリズムは、公開鍵暗号を用いた多重署名（マルチシグ）のみならず、ＰＯＷやＰＯＳなどを含めて、その方式は問わない。

【００６５】

また、本発明は、上述したパブリックノード２ａ用／プライベートノード２ｂ用のトランザクション処理装置２０，２１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。

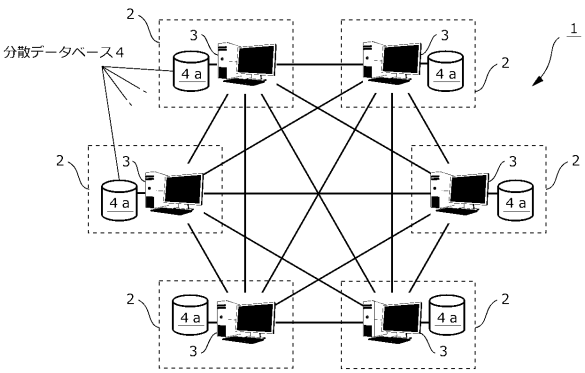
【符号の説明】

【００６６】

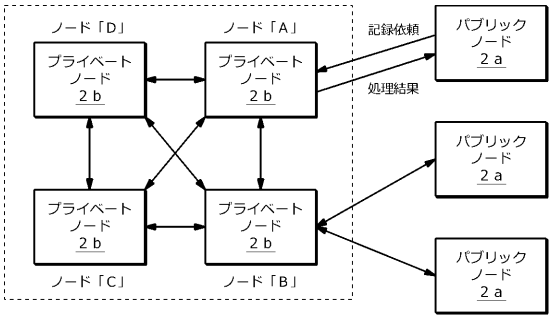
１　トランザクション処理ネットワーク
２　ノード
２ａ　パブリックノード
２ｂ　プライベートノード
３　コンピュータ
４　分散データベース
４ａ　データベース
２０　パブリックノード用のトランザクション処理装置
２０ａ　トランザクション生成部
２０ｂ　記録依頼部
２０ｃ　結果受領部
２０ｄ　転送部
２１　プライベートノード用のトランザクション処理装置
２２　署名検証部
２３　トランザクション処理部
２３ａ　ブロック生成部
２３ｂ　承認依頼部
２３ｃ　ブロック確定部

２３ｄ　承認応答部

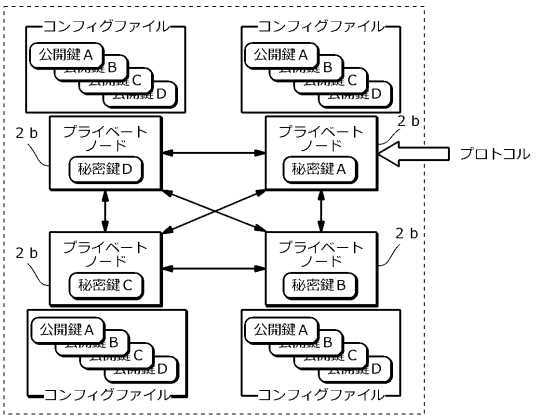
【図１】



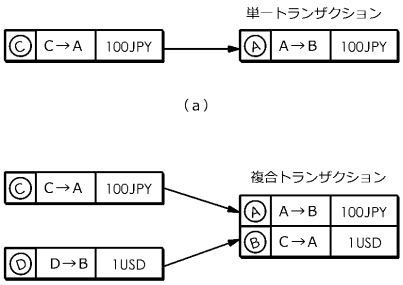
【図２】



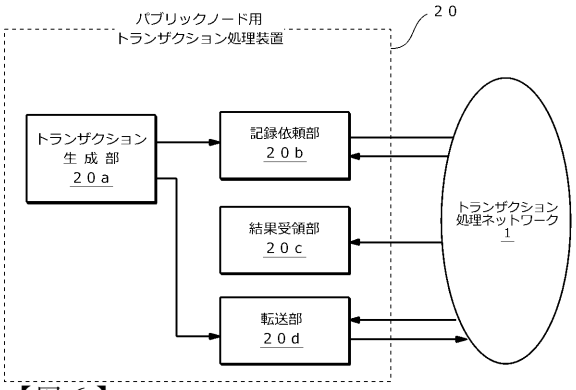
【図３】



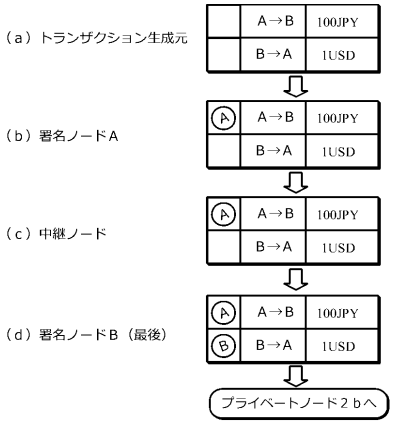
【図４】



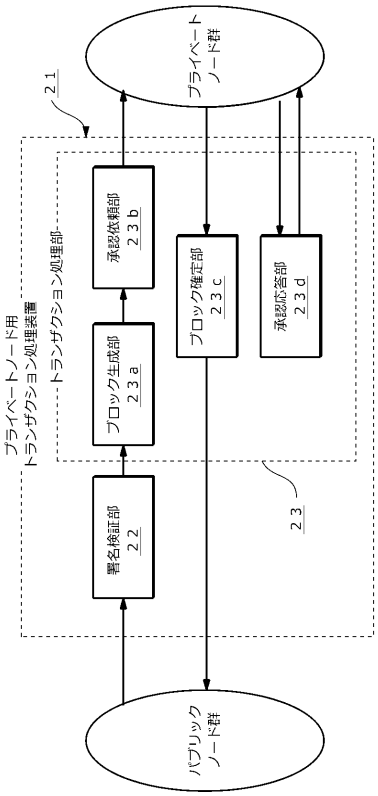
【図５】



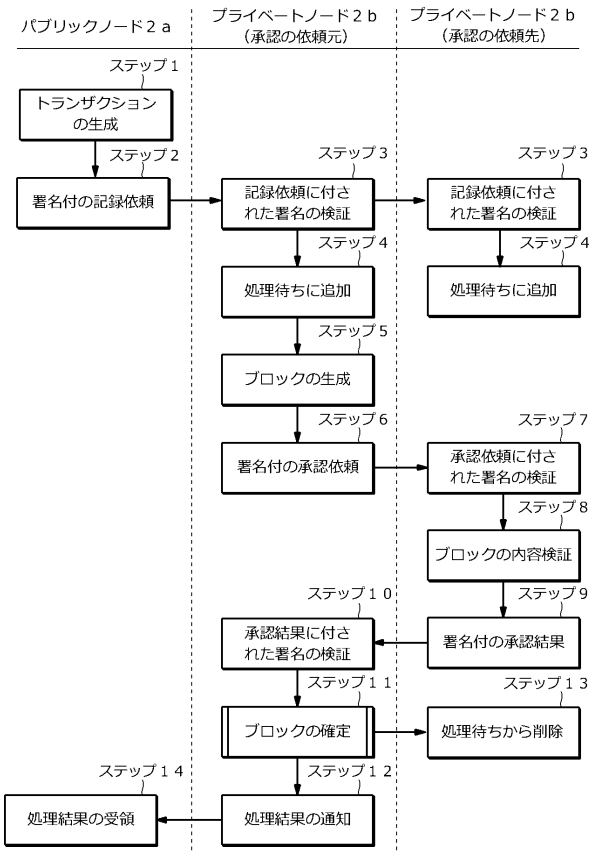
【図６】



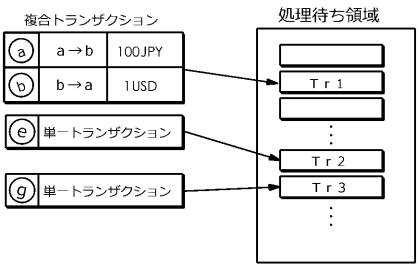
【図７】



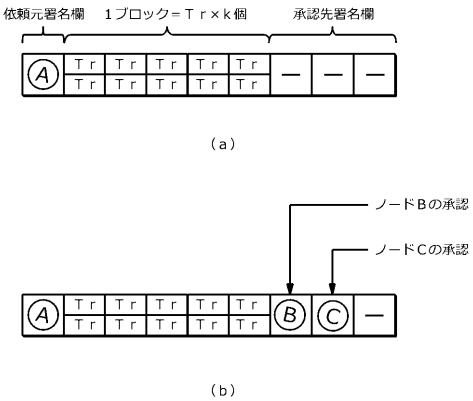
【図８】



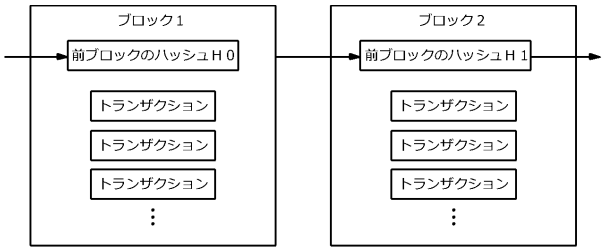
【図９】



【図１０】



【図１１】


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

フロントページの続き

(56)参考文献 米国特許第０９２９８８０６（ＵＳ，Ｂ１）
特開２０００－０４１０３５（ＪＰ，Ａ）
特開２００８－１３１６３２（ＪＰ，Ａ）
米国特許出願公開第２０１５／０２４４６９０（ＵＳ，Ａ１）
米国特許出願公開第２０１５／０３３２２８３（ＵＳ，Ａ１）
淵田 康之，特集：イノベーションと金融 ブロックチェーンと金融取引の革新，野村資本市場クォータリー，日本，株式会社野村資本市場研究所，２０１５年１１月 １日，第１９巻第２号（通巻７４号），ｐｐ．１１－３５
森岡 剛，Special Report 1 決済拡大の鍵は「サービスとの融合」 自動車分野に見るカード決済の未来像，ＣａｒｄＷａｖｅ，日本，株式会社カード・ウェーブ，２０１６年 2月２５日，第２９巻 第1号，ｐｐ．３２－３５
Xiwei Xu, et al., The Blockchain as a Software Connector, 2016 13th Working IEEE/IFIP Conference on Software Architecture, 米国, IEEE, ２０１６年 4月, pp.182-191

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／６４