

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2017年10月5日(05.10.2017)



(10) 国際公開番号

WO 2017/170679 A1

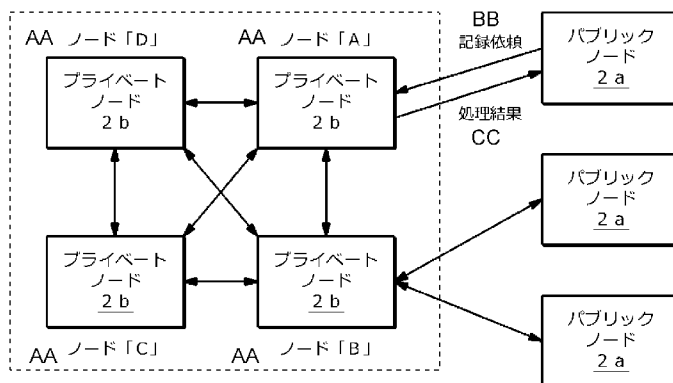
- (51) 国際特許分類:
H04L 9/32 (2006.01) G06Q 20/38 (2012.01)
G06F 21/64 (2013.01) G09C 1/00 (2006.01)
- (21) 国際出願番号: PCT/JP2017/012875
- (22) 国際出願日: 2017年3月29日(29.03.2017)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2016-071341 2016年3月31日(31.03.2016) JP
- (71) 出願人: 株式会社 **b i t F l y e r** (BITFLYER, INC.) [JP/JP]; 〒1070052 東京都港区赤坂三丁目5番5号 Tokyo (JP).
- (72) 発明者: 加納 裕三(KANO Yuzo); 〒1070052 東京都港区赤坂三丁目5番5号 株式会社 **b i t F l y e r** 内 Tokyo (JP). 小宮山 峰史(KOMIYAMA Takafumi); 〒1070052 東京都港区赤坂三丁目5番5号 株式会社 **b i t F l y e r** 内 Tokyo (JP).
- (74) 代理人: 大谷 寛(OTANI Kan); 〒1060032 東京都港区六本木六丁目1番20号 六本木電気ビル7階 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) Title: PRIVATE NODE, PROCESSING METHOD FOR PRIVATE NODE, AND PROGRAM FOR SAME

(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

[図2]



2a Public node
2b Private node
AA Node
BB Recording request
CC Processing result

(57) Abstract: The present invention achieves reliability of recording as well as expanding the fields of application in a network wherein transactions for which transaction information is noted are divided into blocks and imported into a distributed database. Nodes of which the network is composed are classified as a public node 2a and a private node 2b. The public node 2a fulfills the role of generating a transaction to be recorded, and processing for recording to the distributed database thereafter is carried out through the cooperation of a plurality of private nodes 2b. Transaction generation is allowed on a broad basis for the public node 2a which may include unreliable nodes, while processing for recording to the distributed database is restricted to the reliable private nodes 2b.

(57) 要約: 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。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。

WO 2017/170679 A1



添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

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

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、取引に関する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 ($m \geq 2$) 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より第1の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 個のプライベートノード群のうちの n ($m \geq n \geq 1$) 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 ($m \geq 2$) 個のプライベートノードのうちの n ($m \geq n \geq 1$) 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 ($m \geq 2$) 個のプライベートノードに対して、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より第1の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 個のプライベートノードのうちの n ($m > n \geq 1$) 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 ($m \geq 2$) 個のプライベートノードのうちの n ($m \geq n \geq 1$) 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 2 a の一部において、データベース 4 a 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 2 b 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 2 a 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 2 b 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 2 a に通知される。プライベートノード 2 b 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 2 b 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 2 b 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 2 b 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 2 b 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 2 a 用のノード装置（以下、「パブリックノード装置 2 0」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 2 0 は、トランザクション生成部 2 0 a と、記録依頼部 2 0 b 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 23 d が存在する。このように、プライベートノード 2 b は、自ノード 2 b が生成したブロックの承認を他ノード 2 b に依頼する依頼方、および、他ノード 2 b によって生成されたブロックの承認を自ノード 2 b が行う承認方のどちらにもなり得る。

[0032] ブロック生成部 23 a 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 2 a 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 23 b は、ブロック生成部 23 a によって生成されたブロックに自ノード 2 b 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 ($m \geq 2$) 個の他のプライベートノード群 2 b 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 23 c は、承認の依頼先となるプライベートノード 2 b 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 ($m \geq 2$) 個のプライベートノード 2 b のうち、

n ($m \geq n \geq 1$) 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 2 b が存在するケースでは、3 個 ($m = 3$) のプライベートノード 2 b 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] 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。

[0036] 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。

[0037] 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。

[0038] 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。

[0039] 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2

bに送信する。

[0040] 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。

[0041] 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。

[0042] 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2 aに対して、その旨が通知される。

[0043] ステップ5では、いずれかのプライベートノード2 b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2 b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T r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T r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2 b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）は空白とされる。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2 b、すなわち、3つのノードB～Dに送信される。

[0044] 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2 b、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2 bのみならず、すべてのパブリックノード2 a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。

[0045] 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2 b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）。

[0046] [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T rが自ノード2 b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T rの内容が、自ノード2 bの処理待ち領域に格納されたトランザクションT r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T rの資産が未使用であること（資産の二重使用の禁止）

[0047] 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2 b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。

[0048] 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2 b、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。

[0049] 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（ $m \geq n \geq 1$ ）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、 $n/m = 2/3$ となつ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。

[0050] 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 T_r 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 4 a 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 T_r 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 T_r 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 T_r 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。

[0051] 図 9 は、データベース 4 a 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 H_1 が含まれている。そして、ブロック 2 のハッシュ H_2 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 H_1 とを含めた形で算出され、このハッシュ H_2 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（ $H_0, H_1, \dots$ ）、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。

[0052] 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。

[0053] 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。

[0054] 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 2 b 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。

[0055] 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 2 b 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。

[0056] さらに、本実施形態によれば、特定のプライベートノード 2 b によるブロックの生成頻度が極端に高くないように、同一のプライベートノード 2 b 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 2 b 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。

[0057] 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

- [0058]
- 1 トランザクション処理ネットワーク
 - 2 ノード
 - 2 a パブリックノード
 - 2 b 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
 - 4 a データベース
 - 20 パブリックノード装置
 - 20 a トランザクション生成部

- 2 0 b 記録依頼部
- 2 0 c 結果受領部
- 2 1 プライベートノード装置
- 2 2 署名検証部
- 2 3 トランザクション処理部
- 2 3 a ブロック生成部
- 2 3 b 承認依頼部
- 2 3 c ブロック確定部
- 2 3 d 承認応答部

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、
- 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又は2に記載の処理方法。
- [請求項4] 前記プライベートノードの数は、二桁であることを特徴とする請求項3に記載の処理方法。
- [請求項5] 前記所定の数値は、一桁の奇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プライベートノード群の全て及び前記パブリックノード群の一部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] 前記ブロックの前記追加がなされた旨を前記プライベートノード群

の一部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、

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

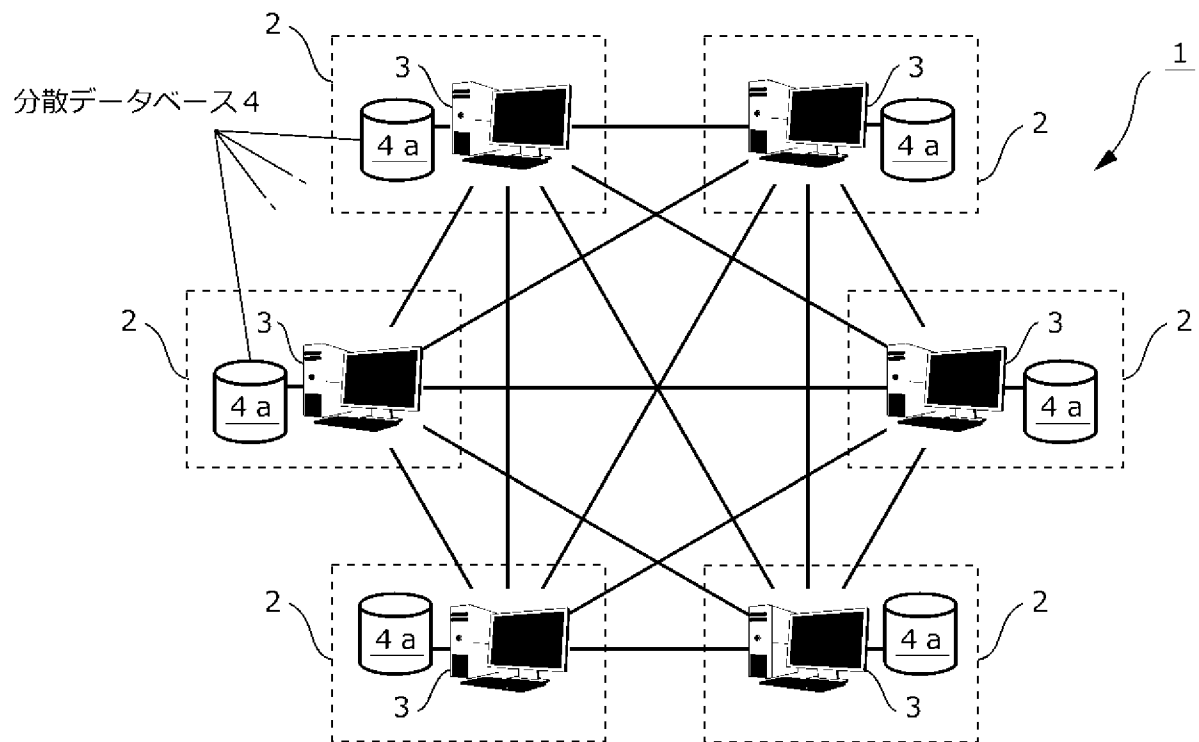
を含むことを特徴とするプログラム。

[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、

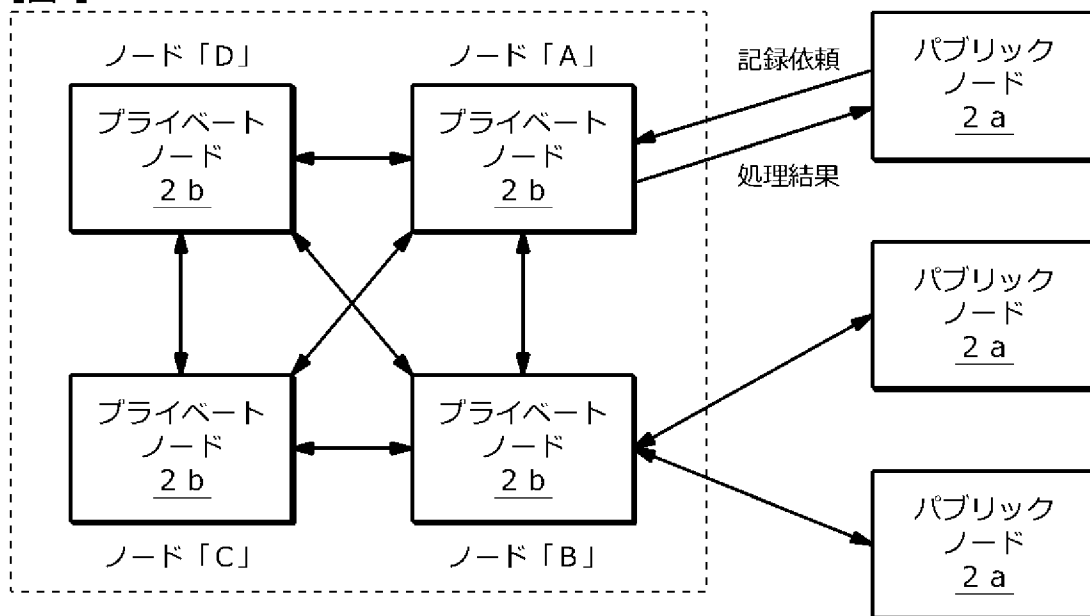
複数のトランザクションを有するブロックを生成して、前記ブロックの承認依頼を前記プライベートノード群に送信し、

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ブ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。

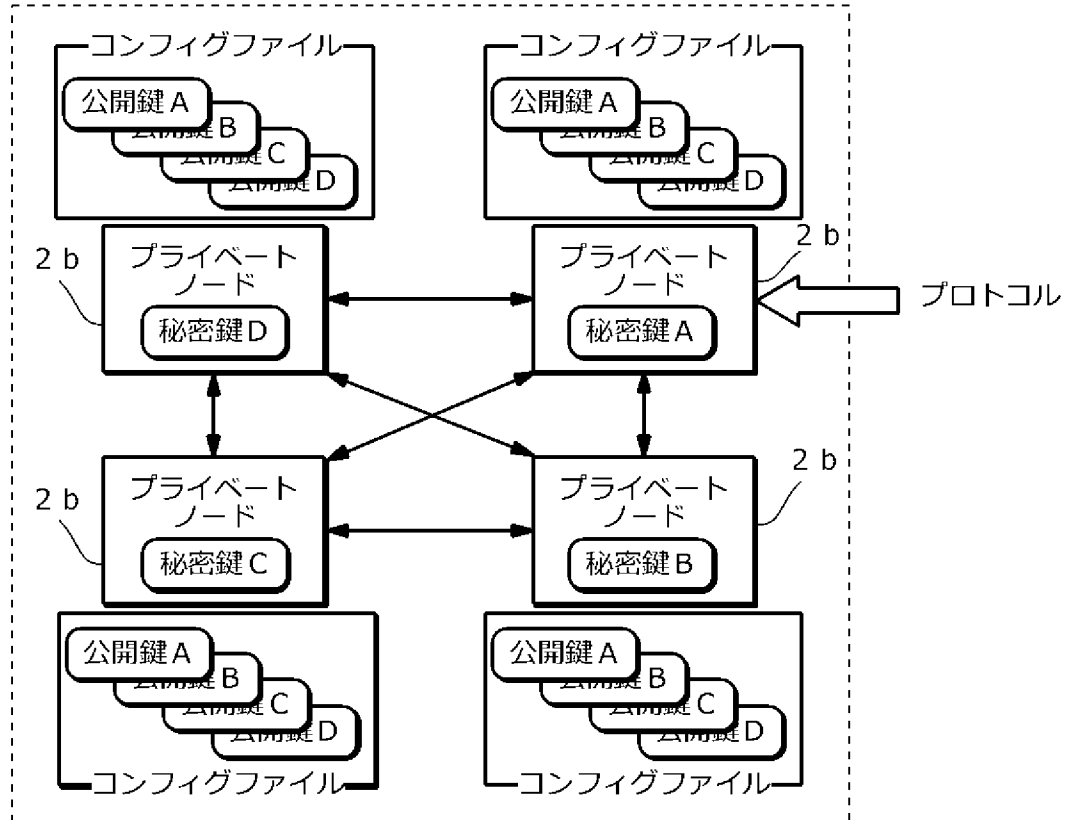
[図1]



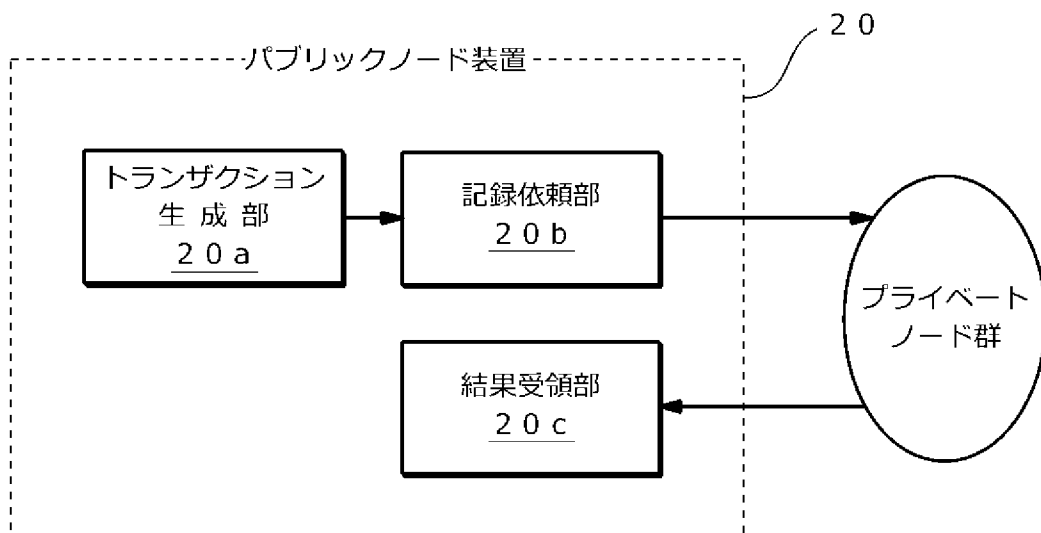
[図2]



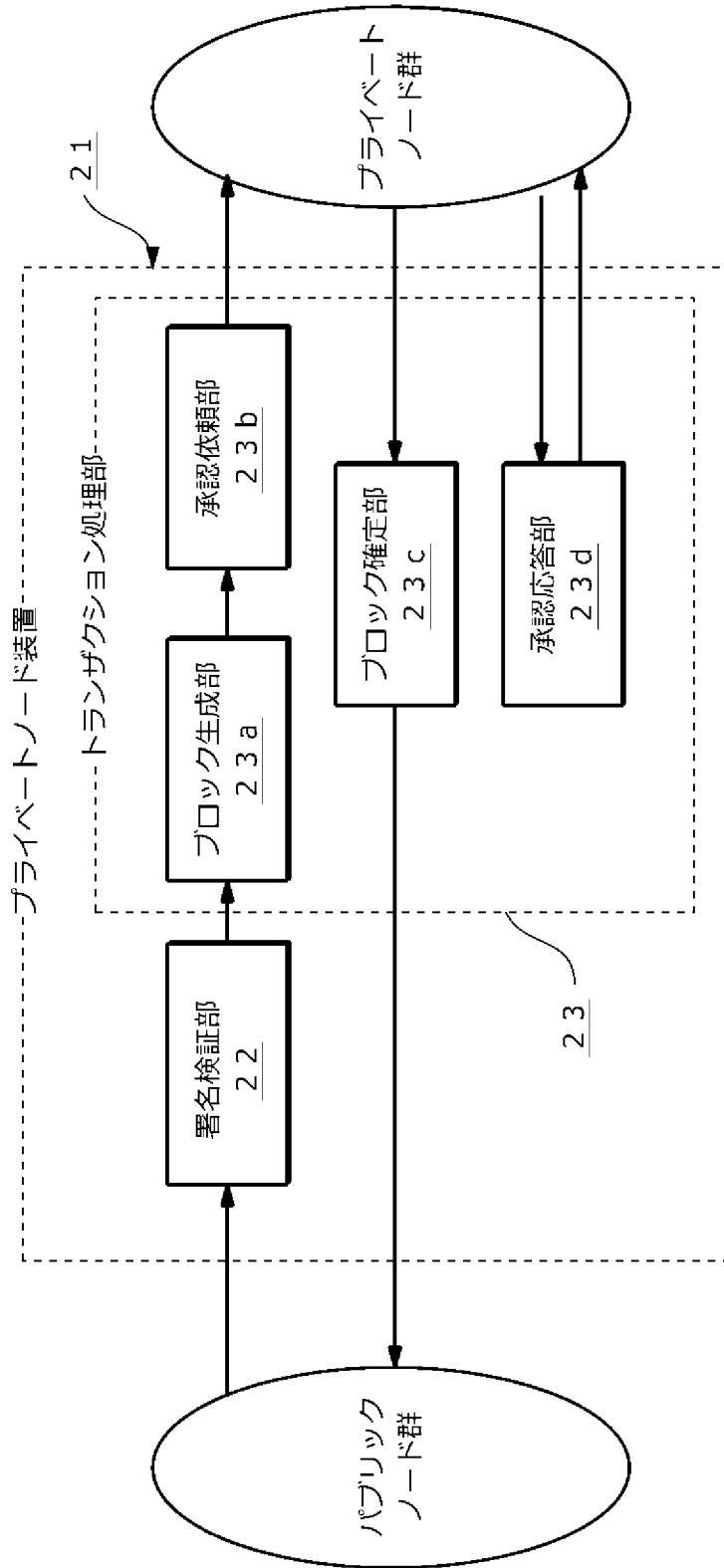
[図3]



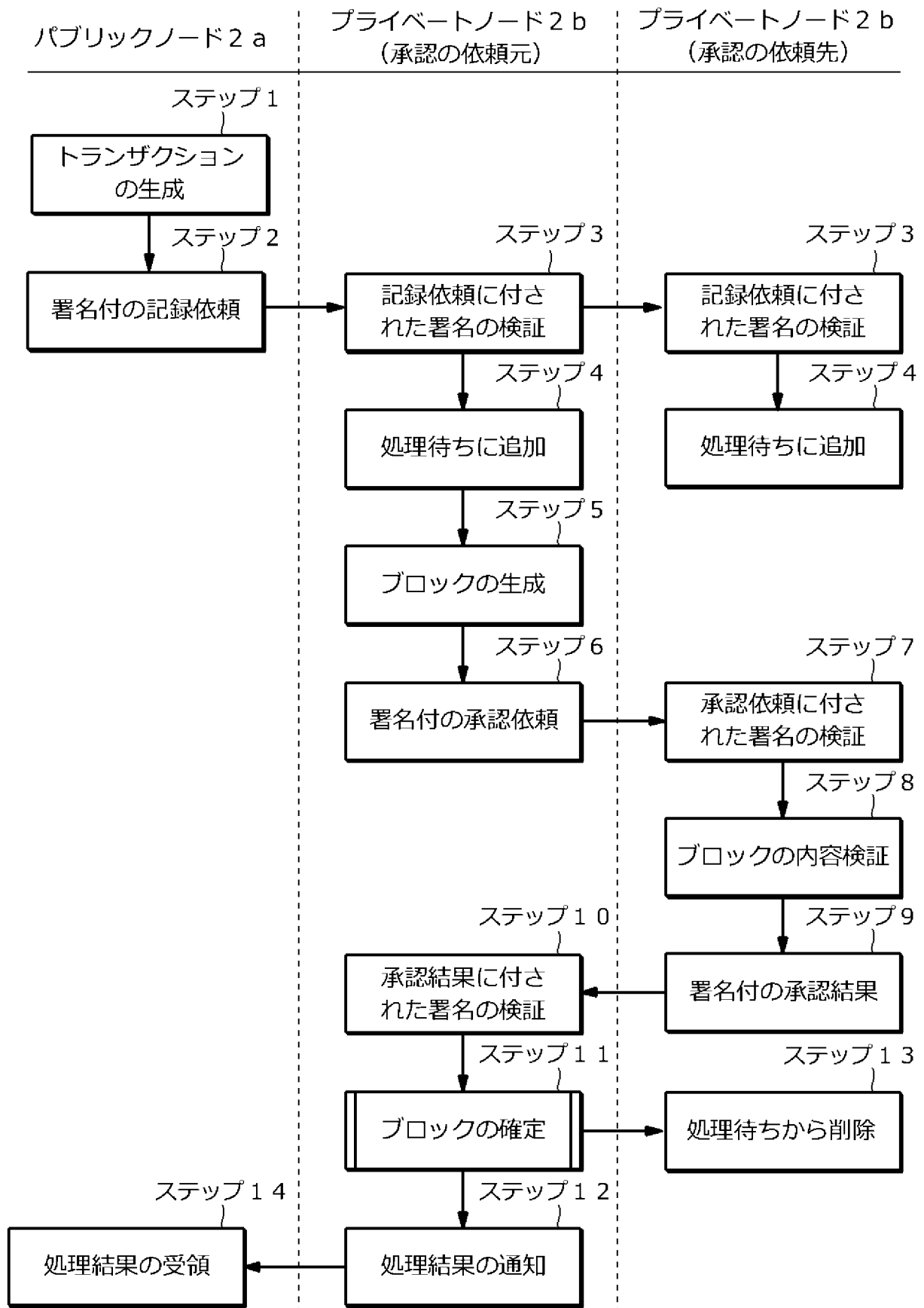
[図4]



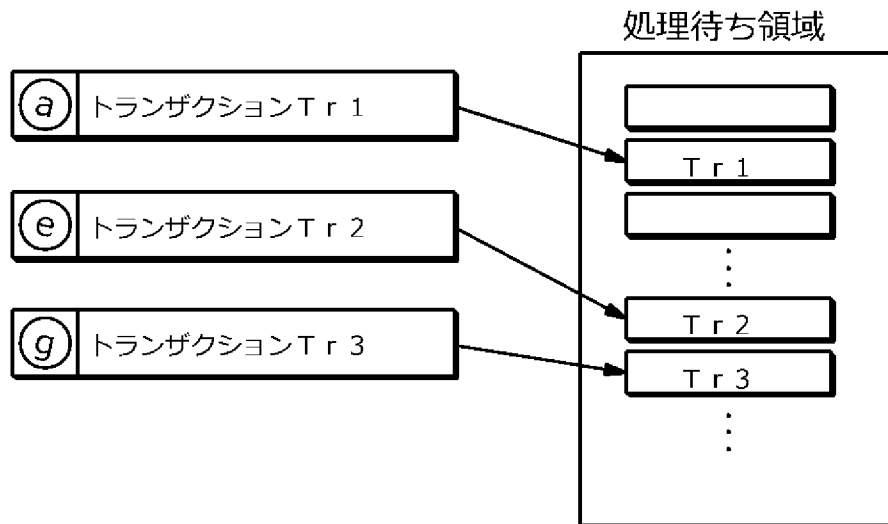
[図5]



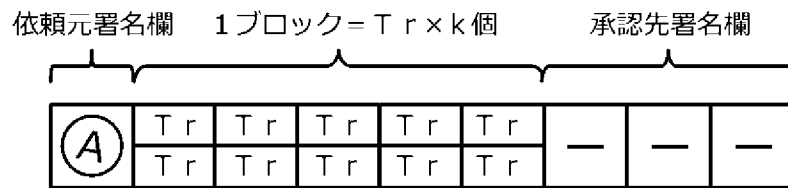
[図6]



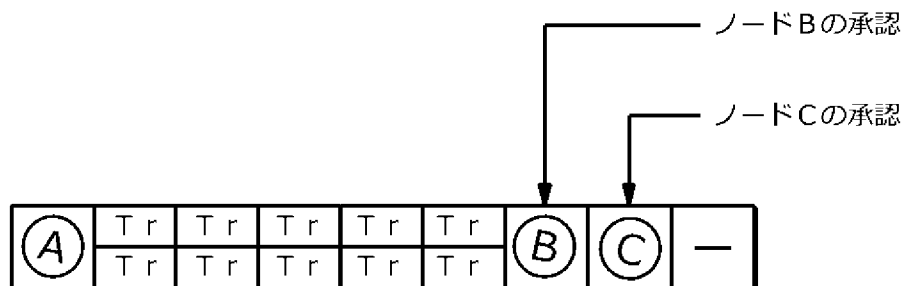
[図7]



[図8]

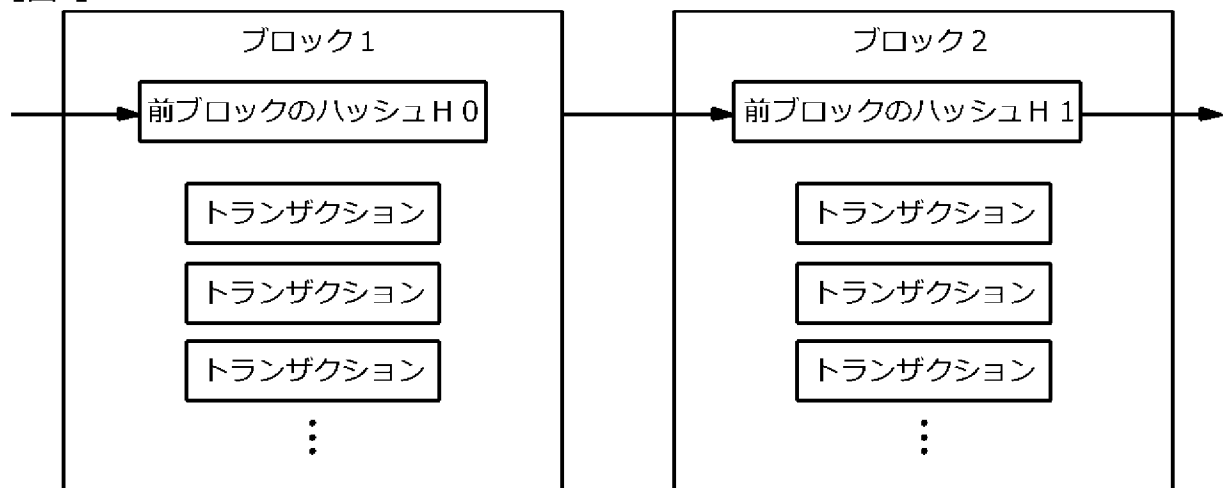


(a)



(b)

[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/012875

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32(2006.01)i, G06F21/64(2013.01)i, G06Q20/38(2012.01)i, G09C1/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/32, G06F21/64, G06Q20/38, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2015/0332283 A1 (NANT HOLDINGS IP, LLC), 19 November 2015 (19.11.2015), paragraphs [0029], [0031], [0036] to [0041], [0045] to [0051]; fig. 1 & WO 2015/175722 A1	1-10
Y	Akihito AKUTSU et al., "User o Kando saseru Epoch Making na Service Soshutsu eno Chosen Kyogi no Kando o Sekaiju de Kyoyu dekiru Service ni", NTT Gijutsu Journal, 01 May 2015 (01.05.2015), vol.27, no.5, pages 10 to 14	1-10
A	JP 5858506 B1 (Kabushiki Kaisha Orb), 25 December 2015 (25.12.2015), paragraphs [0014] to [0035]; fig. 1 & JP 2016-200954 A	1-10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
05 June 2017 (05.06.17)

Date of mailing of the international search report
13 June 2017 (13.06.17)

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

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04L9/32(2006.01)i, G06F21/64(2013.01)i, G06Q20/38(2012.01)i, G09C1/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. H04L9/32, G06F21/64, G06Q20/38, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2017年
日本国実用新案登録公報	1996-2017年
日本国登録実用新案公報	1994-2017年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	US 2015/0332283 A1 (NANT HOLDINGS IP, LLC) 2015.11.19, 段落 [0029]、[0031]、[0036] - [0041]、 [0045] - [0051]、FIG. 1 & WO 2015/175722 A1	1-10
Y	阿久津 明人 ほか、ユーザを感動させるエポックメイキングなサ ービス創出への挑戦 競技の感動を世界中で共有できるサービス に、N T T技術ジャーナル、2015.05.01、第27巻 第5号、pp.10-14	1-10

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

05.06.2017

国際調査報告の発送日

13.06.2017

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

青木 重徳

5 S

4229

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 5858506 B1 (株式会社O r b) 2015.12.25, 段落 [0 0 1 4] – [0 0 3 5]、[図1] & JP 2016-200954 A	1 – 1 0