

(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
2020年10月29日(29.10.2020)

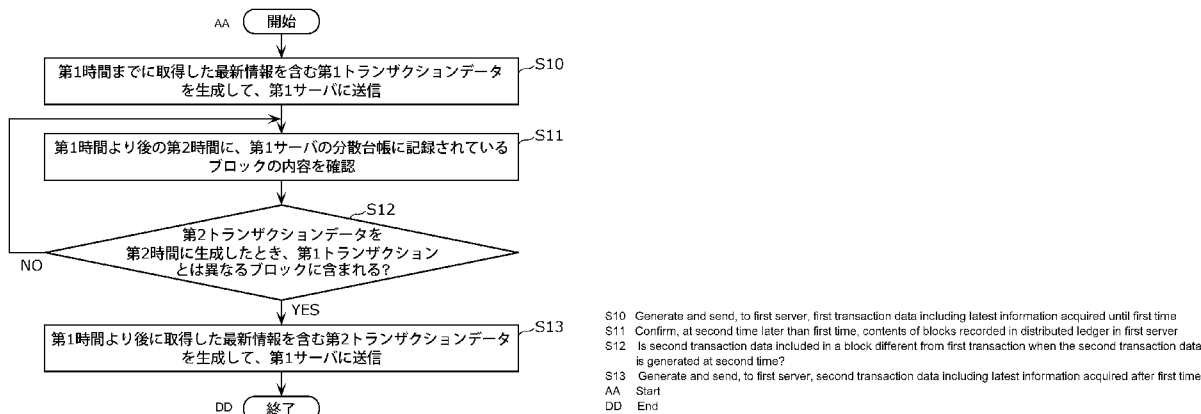


(10) 国際公開番号
WO 2020/218550 A1

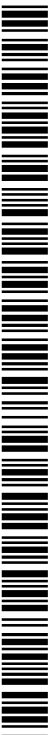
- (51) 国際特許分類:
G06F 16/182 (2019.01)
- (21) 国際出願番号: PCT/JP2020/017789
- (22) 国際出願日: 2020年4月24日(24.04.2020)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
62/838,436 2019年4月25日(25.04.2019) US
- (71) 出願人: パナソニック インテレクチュアル
プロパティ コーポレーション オブ アメリ
カ(PANASONIC INTELLECTUAL PROPER-
TY CORPORATION OF AMERICA) [US/US];
90503 カリフォルニア州 トーランス, ス
イート 200, マリナー アベニュー
20000 California (US).
- (72) 発明者: 西田 直央 (NISHIDA, Naohisa);
〒5718501 大阪府門真市大字門真 1 0 0
- 6 番地 パナソニック株式会社内 Osaka
(JP), 海上 勇二 (UNAGAMI, Yuji), 道山 淳
児(MICHIYAMA, Junji).
- (74) 代理人: 新居 広守, 外 (NII, Hiromori et al.);
〒5320011 大阪府大阪市淀川区西中島 5 丁目
3 番 1 0 号タナカ・イトーピア新大阪ビル 6
階新居国際特許事務所内 Osaka (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, JO, 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,

(54) Title: CONTROL METHOD, DATA GENERATION DEVICE, AND PROGRAM

(54) 発明の名称: 制御方法、データ生成装置、及びプログラム



(57) Abstract: A control method generates and sends, to a first server of a plurality of servers, first transaction data including latest information acquired until a first time (S10); confirms, at one or more second times later than the first time, the contents of blocks recorded in a distributed ledger in the first server, and thereby confirms, when second transaction data after the first transaction data is generated at the second time, whether a first block, which is included when the first transaction data is recorded in the distributed ledger, and a second block, which is included when the second transaction data is recorded in the distributed ledger, are different or not (S11); and, when the first block and the second block are different (Yes in S12), generates and transmits, to the first server at and after the second time, the second transaction data including latest information acquired after the first time (S13).



WO 2020/218550 A1

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, 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).

添付公開書類:

- 一 国際調査報告 (条約第21条(3))

(57) 要約: 制御方法は、第1時間までに取得した最新情報を含む第1トランザクションデータを生成して、複数のサーバのうち第1サーバに送信し (S 1 0)、第1時間より後の1以上の第2時間に、第1サーバの分散台帳に記録されているブロックの内容を確認することで、第1トランザクションデータの1つ後の第2トランザクションデータを第2時間に生成したときに、第1トランザクションデータが分散台帳に記録されるときに含まれる第1ブロックと、第2トランザクションデータが分散台帳に記録されるときに含まれる第2ブロックとが異なるか否かを確認し (S 1 1)、第1ブロックと第2ブロックとが異なる場合 (S 1 2でYes)、第1時間より後に取得した最新情報を含む第2トランザクションデータを、当該第2時間以降生成して、第1サーバに送信する (S 1 3)。

明 細 書

発明の名称： 制御方法、データ生成装置、及びプログラム

技術分野

[0001] 本開示は、制御方法、データ生成装置、及びプログラムに関する。

背景技術

[0002] ビットコインから生まれた技術としてブロックチェーン技術がある（例えば非特許文献1参照）。ブロックチェーンは、ブロックと呼ばれるデータの単位を一定時間ごとに生成し、鎖のように連結していくことによりデータを保管するデータベースである。ブロックチェーンを利用することで、誰もが参加可能なピアツーピア（Peer to Peer：P2P）ネットワークで取引履歴（トランザクションデータ）を共有し、相互に監視することで、信頼性を担保し、データの改ざんを防ぐことができる。

[0003] なお、非特許文献1に記載のビットコインのブロックチェーンでは、ブロックのサイズが1MBに制限されており、ブロック生成間隔が約10分とされている。

[0004] このため、ブロックチェーンの仕様を変更し、ブロック生成間隔を約2分にすることで、データの処理量を増加させることも行われている（例えば非特許文献2参照）

先行技術文献

非特許文献

[0005] 非特許文献1：Satoshi Nakamoto, “Bitcoin:A Peer-to-Peer Electronic Cash System” ,2009

非特許文献2：BitcoinCandy, “Bitcoin Candy Whitepaper” , (<https://cdy.one/whitepaper.pdf>)

発明の概要

発明が解決しようとする課題

[0006] ところで、非特許文献1及び非特許文献2に記載のブロックチェーンでは

、1ブロックに複数のトランザクションデータが含まれて生成される。このため、ブロック生成間隔によっては、同一のユーザないし同一事業者により複数時点に送信された複数のトランザクションデータが1ブロックに含まれてしまう場合がある。

[0007] しかしながら、トランザクションデータに含める情報の種別によっては、1ブロックに、同一のユーザないし同一事業者により複数時点に送信された複数のトランザクションデータが含まれても無意味な場合がある。一例を挙げると、ブロックチェーンに記録される最新の天気情報のみを参考に価格を決める場合、最新以外の天気情報も1ブロックに含まれる場合である。つまり、ブロックに含まれる複数のトランザクションデータのうち最新情報が含まれるトランザクションデータだけを利用して、過去の情報が含まれるトランザクションデータを利用しない場合である。このような場合、ブロックチェーンのブロックには、利用しない無駄なトランザクションデータが記録されることになる。これは、限られたネットワーク帯域の無駄使いになるだけでなく、ブロック生成の電力等を含むリソースの無駄使いとなる。

[0008] 本開示は、上述の事情を鑑みてなされたもので、ネットワーク帯域及びリソースの無駄使いを抑制することができる制御方法等を提供することを目的とする。

課題を解決するための手段

[0009] 上記目的を達成するために、本開示の制御方法は、機器と、それぞれ、前記機器と通信可能に接続され、所定のタイミング毎に当該所定のタイミングまでに保持しているトランザクションデータのうち選択したトランザクションデータをブロックに含めて分散台帳に記録する複数のサーバとを備えるシステムにおける前記機器によって実行される制御方法であって、第1時間までに取得した最新情報を含む第1トランザクションデータを生成して、前記複数のサーバのうち第1サーバに送信し、前記第1時間より後の1以上の第2時間に、前記第1サーバの前記分散台帳に記録されているブロックの内容を確認することで、前記第1トランザクションデータの1つ後の第2トラン

ザクションデータを前記第2時間に生成したときに、前記第1トランザクションデータが前記分散台帳に記録されるときに含まれる第1ブロックと、前記第2トランザクションデータが前記分散台帳に記録されるときに含まれる第2ブロックとが異なるか否かを確認し、前記第1ブロックと前記第2ブロックとが異なる場合、前記第1時間より後に取得した最新情報を含む前記第2トランザクションデータを、当該第2時間以降に生成して、前記第1サーバに送信する。

[0010] なお、これらの包括的または具体的な態様は、システム、集積回路、コンピュータプログラムまたはコンピュータで読み取り可能なCD-ROMなどの記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。

発明の効果

[0011] 本開示の制御方法等によれば、ネットワーク帯域及びリソースの無駄使いを抑制することができる。

図面の簡単な説明

[0012] [図1]図1は、ブロックチェーンの概念を示す説明図である。

[図2]図2は、図1に示すブロックチェーンのデータ構造を示す説明図である。

[図3]図3は、図1に示すブロックチェーンのブロック生成間隔で行われる処理の説明図である。

[図4]図4は、図3に示すコンセンサスアルゴリズムを実行することで行われる処理を示すフローチャートの一例である。

[図5]図5は、実施の形態に係る制御システムの構成を模式的に示す図である。

[図6]図6は、実施の形態に係る機器の構成を模式的に示すブロック図である。

[図7]図7は、実施の形態に係る機器の機能を、ソフトウェアにより実現するコンピュータのハードウェア構成の一例を示す図である。

[図8]図8は、実施の形態に係る認証サーバ装置の機能構成を示すブロック図である。

[図9]図9は、実施の形態に係る機器の動作を示すフローチャートである。

[図10]図10は、実施例1に係る制御システムの処理のシーケンス図である。

[図11]図11は、実施例2に係る機器の処理を示すフローチャートである。

[図12]図12は、実施の形態に係る効果について説明するためのフロー図である。

[図13]図13は、実施の形態に係る効果について説明するためのフロー図である。

[図14]図14は、図13に示すフロー図の別観点での説明図である。

発明を実施するための形態

[0013] (本開示の基礎となった知見)

まず、ブロックチェーンについて説明する。

[0014] 図1は、ブロックチェーンの概念を示す説明図である。

[0015] ブロックチェーンは、「1個のブロック」を記録単位として、ブロックをチェーン（鎖）状に繋げていくものであり、分散台帳に記録される。図1では、ブロックB0より時間的に後に生成したブロックB1をブロックB0に接続し、ブロックB1より時間的に後に生成したブロックB2をブロックB1に接続する・・・という例が示されている。つまり、図1には、ブロックB0～ブロックB3がチェーン状に繋がられているブロックチェーンの例が示されている。

[0016] 図2は、図1に示すブロックチェーンのデータ構造を示す説明図である。

[0017] 図1に示すブロックチェーンのブロックは、複数のトランザクションデータと、直前のブロックのハッシュ値とを有している。具体的には、ブロックB2には、その前のブロックB1のハッシュ値が含まれている。そして、ブロックB2に含まれる複数のトランザクションデータと、ブロックB1のハッシュ値とから演算されたハッシュ値が、ブロックB2のハッシュ値として

、ブロックB3に含められる。

[0018] このように、ブロックチェーン技術では、前のブロックの内容をハッシュ値として含めながら、ブロックをチェーン状に接続することで、接続されたトランザクションデータの改ざんを有効に防止する。なぜなら、仮に過去のトランザクションデータが変更されると、ブロックのハッシュ値が変更前と異なる値になる。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ので、事実上改ざん不可と言えるからである。さらに、ブロックチェーンが記録される分散台帳は、物理的に異なった多数の拠点それぞれに設置されることから、ある地点の台帳に対する改ざんが発生しても他の台帳から改ざんを検知できる。このことから、ブロックチェーンは事実上改ざん不可と言える。

[0019] 次に、ブロック生成間隔における処理すなわちブロックが生成されてブロックチェーンに接続される（書き込まれる）までの処理について、図を用いて説明する。なお、ブロックが生成されてブロックチェーンに書き込まれるまでの処理は、ブロックチェーンのブロックが生成されて分散台帳に記録されるまでの処理に相当する。

[0020] 図3は、図1に示すブロックチェーンのブロック生成間隔で行われる処理の説明図である。なお、図3では、トランザクションデータをTxデータと表記し、トランザクションプールをTxプールと表記している。図3では、ブロック生成間隔は、例えばブロックチェーンのブロックB0に、ブロックB1が接続されてから、次のブロックB2が接続されるまでの間隔である。

[0021] トランザクションプールは、ブロックチェーンのまだ検証されていない取引（トランザクションデータ）を溜めている貯蔵庫である。図3に示すように、トランザクションプールには、1以上のユーザから取得した複数のトランザクションデータが未検証の状態保持される。

[0022] コンセンサスアルゴリズムは、ブロックチェーンにブロックを書き込める「代表者」を選定するためのルールであり、合意形成アルゴリズムとも称さ

れる。コンセンサスアルゴリズムの実行には時間を要するため、ブロック生成間隔とはコンセンサスアルゴリズムの実行開始から実行完了までの時間で規定される。

[0023] コンセンサスアルゴリズムは、実行開始時まで、トランザクションプールで選択された1以上のトランザクションデータに対して実行される。コンセンサスアルゴリズムの実行が完了すると、当該ブロックがブロックチェーンに書き込まれる。なお、トランザクションプールに保持されているすべてのトランザクションデータを含めることができるブロックの容量があれば、トランザクションプールに保持されているすべてのトランザクションデータに対してコンセンサスアルゴリズムが実行されてもよい。

[0024] 図4は、図3に示すコンセンサスアルゴリズムを実行することで行われる処理を示すフローチャートの一例である。

[0025] コンセンサスアルゴリズムが実行されると、まず、トランザクションプールで選択された1以上のトランザクションデータの検証が行われる（S91）。ここでは、当該1以上のトランザクションデータの正当性の検証が行われる。

[0026] 次に、当該1以上のトランザクションデータを含むブロックが生成され（S92）、ブロックチェーンに書き込まれる（S93）。なお、以下では、新たなブロックがブロックチェーンに書き込まれることを、新たなブロックが分散台帳に記録されることと表現する場合がある。

[0027] このように、ブロック生成間隔は、コンセンサスアルゴリズムの実行に要する時間により規定される。なお、非特許文献1で開示されるビットコインでは、コンセンサスアルゴリズムの実行に約10分要することから、ブロック生成間隔が約10分とされている。

[0028] また、このようなブロックチェーンでは、ブロックチェーンに書き込むために送信されたトランザクションデータを保持するトランザクションプールにおいて選択されたトランザクションデータが書き込まれることになる。

[0029] ところで、このようなブロックチェーンでは、ブロック生成間隔によって

は、同一のユーザないし同一事業者により複数時点に送信された複数のトランザクションデータがトランザクションプールに保持されることになる。つまり、同一のユーザないし同一事業者により複数時点に送信された複数のトランザクションデータが1ブロックに含まれる場合がある。

[0030] しかしながら、トランザクションデータに含まれる情報の種別によっては、1ブロックに、同一のユーザないし同一事業者により複数時点に送信された複数のトランザクションデータが含まれても無意味な場合がある。このような場合、ブロックチェーンのブロックに利用しない無駄なトランザクションデータが記録されることになる。これは、限られたネットワーク帯域の無駄使いになるだけでなく、ブロック生成の電力等を含むリソースの無駄使いとなる。

[0031] そこで、本開示の一形態に係る制御方法は、機器と、それぞれ、前記機器と通信可能に接続され、所定のタイミング毎に当該所定のタイミングまでに保持しているトランザクションデータのうち選択したトランザクションデータをブロックに含めて分散台帳に記録する複数のサーバとを備えるシステムにおける前記機器によって実行される制御方法であって、第1時間までに取得した最新情報を含む第1トランザクションデータを生成して、前記複数のサーバのうち第1サーバに送信し、前記第1時間より後の1以上の第2時間に、前記第1サーバの前記分散台帳に記録されているブロックの内容を確認することで、前記第1トランザクションデータの1つ後の第2トランザクションデータを前記第2時間に生成したときに、前記第1トランザクションデータが前記分散台帳に記録されるときに含まれる第1ブロックと、前記第2トランザクションデータが前記分散台帳に記録されるときに含まれる第2ブロックとが異なるか否かを確認し、前記第1ブロックと前記第2ブロックとが異なる場合、前記第1時間より後に取得した最新情報を含む前記第2トランザクションデータを、当該第2時間以降に生成して、前記第1サーバに送信する。

[0032] このように、分散台帳に記録されたブロックの内容を確認してから1つの

機器すなわち同一のユーザないし同一事業者は、最新情報を含む1つのトランザクションデータを送信する。これにより、分散台帳に記録される1つのブロックには、1つの機器が送信する1つのトランザクションデータのみが含まれることになる。よって、利用しない無駄なトランザクションデータが、ブロックに記録されることを抑制することができるので、ネットワーク帯域及びリソースの無駄使いを抑制することができる。

[0033] また、前記ブロックの内容を確認する際、前記ブロックの内容として、前記ブロックに前記第1トランザクションデータの1つ前に生成された第3トランザクションデータが含まれているかを確認してもよい。

[0034] これにより、分散台帳に記録されるブロックごとに、1つの機器が送信する1つのトランザクションデータのみが含まれることになる。よって、ブロックに利用されないトランザクションデータを含めて分散台帳に記録されることを抑制できるだけでなく、当該機器にとっての空白ブロックが分散台帳に記録されることを抑制できる。よって、ネットワーク帯域及びリソースの無駄使いを、さらに抑制することができる。

[0035] ここで、さらに、前記第1サーバが単位時間あたりに受信するトランザクションデータ数である受信総数と、前記第1サーバが、前記分散台帳に記録する際、単位時間あたりに処理可能なトランザクションデータ数である処理可能数とを取得し、前記処理可能数が前記受信総数により定められる閾値以上の場合、前記ブロックの内容として、前記ブロックに前記第3トランザクションデータが含まれているかを確認してもよい。

[0036] これにより、第1サーバの処理能力に応じて、分散台帳に記録されるブロックごとに、1つの機器が送信する1つのトランザクションデータのみが含まれるようにすることができる。

[0037] また、前記ブロックの内容を確認する際、前記ブロックの内容として、前記ブロックに前記第1トランザクションデータが含まれているかを確認してもよい。

[0038] これにより、当該1つの機器にとっての空白ブロックが分散台帳に記録さ

れる場合が発生するものの、分散台帳に記録される空白ブロックでない1つのブロックには、1つの機器により送信される1つのトランザクションデータのみが含まれることになる。よって、利用しない無駄なトランザクションデータがブロックに記録されることを抑制することができるので、ネットワーク帯域及びリソースの無駄使いを抑制することができる。

[0039] ここで、さらに、前記第1サーバが単位時間あたりに受信するトランザクションデータ数である受信総数と、前記第1サーバが、前記分散台帳に記録する際、単位時間あたりに処理可能なトランザクションデータ数である処理可能数とを取得し、前記処理可能数が前記受信総数により定められる閾値より小さい場合、前記ブロックの内容として、前記ブロックに前記第1トランザクションデータが含まれているかを確認してもよい。

[0040] これにより、第1サーバの処理能力に応じて、分散台帳に記録される1つのブロックには、1つの機器により送信される1つのトランザクションデータのみが含まれるようにすることができる。

[0041] また、本開示の一態様に係るデータ生成装置は、それぞれ、所定のタイミング毎に当該所定のタイミングまでに保持しているトランザクションデータのうち選択したトランザクションデータをブロックに含めて分散台帳に記録する複数のサーバと通信可能に接続されるデータ生成装置であって、プロセッサと、メモリと、を備え、前記プロセッサは、第1時間までに取得した最新情報を含む第1トランザクションデータを生成して、前記複数のサーバのうち第1サーバに送信し、前記プロセッサは、前記第1時間より後の1以上の第2時間に、前記第1サーバの前記分散台帳に記録されているブロックの内容を確認することで、前記第1トランザクションデータの1つ後の第2トランザクションデータを前記第2時間に生成したときに、前記第1トランザクションデータが前記分散台帳に記録されるときに含まれる第1ブロックと、前記第2トランザクションデータが前記分散台帳に記録されるときに含まれる第2ブロックとが異なるか否かを確認し、前記プロセッサは、前記第1ブロックと前記第2ブロックとが異なることを確認した場合、前記第1時間

より後に取得した最新情報を含む前記第2トランザクションデータを、当該第2時間以降に生成して、前記第1サーバに送信する。

[0042] 以下、図面を参照しながら、実施の形態について説明する。なお、以下で説明する実施の形態は、いずれも本開示の好ましい一具体例を示す。つまり、以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置及び接続形態、ステップ、ステップの順序などは、一例であり、本開示を限定する主旨ではない。本開示は、請求の範囲の記載に基づいて特定される。したがって、以下の実施の形態における構成要素のうち、本開示の最上位概念を示す独立請求項に記載されていない構成要素は、本開示の課題を達成するために必ずしも必要ではないが、より好ましい形態を構成する構成要素として説明される。

[0043] (実施の形態)

以下では、図面を参照しながら、実施の形態に係る制御システムについて説明する。

[0044] 本開示の制御システムでは、最新の分散台帳に記録されるブロックの内容を確認した結果に応じて、次のトランザクションデータを送信させる。これにより、定期的に情報を分散台帳に記録したいものの、分散台帳に記録された過去の情報を参照せず、最新情報だけを利用したい場合、分散台帳に記録される1つのブロックには、利用され得る最新情報を含む1つのトランザクションデータのみが含まれることになる。

[0045] [制御システムの構成]

図5は、本実施の形態に係る制御システムの構成を模式的に示す図である。

[0046] 制御システムは、図5に示されるように、機器100と、認証サーバ装置210、220、230とを備える。これらは通信可能に接続されている。これらの通信は、有線のインターネット線、無線通信及び専用通信等のいずれかであればよい。

[0047] なお、図5では、本実施の形態に係る制御システムが、3つのサーバと1

つの機器とを備える場合の例が示されているが、これに限らない。すなわち、本実施の形態に係る制御システムは、4つ以上の認証サーバ装置を備えてもよいし、2つ以上の機器を備えていてもよい。なお、後述するが、1つの機器は、一のユーザないし一の事業者が利用する機器を代表し、サーバ機能を有する機器であってもよい。

[0048] [機器100]

機器100は、一のユーザないし一の事業者が利用する機器を代表している。機器100は、サーバ機能を有していてもよい。

[0049] 図6は、本実施の形態に係る機器100の構成を模式的に示すブロック図である。

[0050] 機器100は、プロセッサと、プロセッサに所定の処理を実行させるプログラムが記憶されたメモリとを備える。つまり、機器100は、プロセッサがメモリを用いて所定のプログラムを実行することで実現される。本実施の形態では、機器100は、センサ情報取得部101と、トランザクションデータ生成部102と、トランザクションデータ確認部103と、確認方法決定部104と、通信部105と、を備える。なお、確認方法決定部104は必須の構成ではなく、機器100に備えられていなくてもよい。以下、各構成要素について説明する。

[0051] <センサ情報取得部101>

センサ情報取得部101は、図示しないIoT (Internet of Things) 機器に搭載されたセンサからの情報 (センサ情報) を定期的に取得する。つまり、センサ情報取得部101は、定期的に最新のセンサ情報 (以下、最新情報とも称する) を取得する。ここで、センサ情報は、例えば天気情報または生体情報であるが、これらに限らない。センサ情報は、センサから直接取得されるデータであってもよいし、例えばインターネットを介してセンサから取得されるデータであってもよい。また、センサ情報は、インターネット上から取得されるデータであっても定期的に更新または追加されるデータであってもよい。

[0052] <トランザクションデータ生成部102>

トランザクションデータ生成部102は、トランザクションデータ確認部103の確認結果に基づいて、トランザクションデータを生成する。トランザクションデータ生成部102は、生成したトランザクションデータを、通信部105を介して、認証サーバ装置210、220、230の少なくとも1つに送信する。

[0053] より具体的には、トランザクションデータ生成部102は、第1時間までにセンサ情報取得部101が取得した最新情報を含む第1トランザクションデータを生成して、生成した第1トランザクションデータを、例えば認証サーバ装置210に送信したとする。この場合、トランザクションデータ生成部102は、トランザクションデータ確認部103による最新の分散台帳に記録されているブロックの内容に応じて、第1時間より後に取得した最新情報を含む第2トランザクションデータを生成する。そして、トランザクションデータ生成部102は、生成した第2トランザクションデータを、認証サーバ装置210に送信する。

[0054] <トランザクションデータ確認部103>

トランザクションデータ確認部103は、最新の分散台帳に記録されているブロックに、トランザクションデータ生成部102が1つ前または2つ前に生成して、送信されたトランザクションデータが含まれたかどうかを確認する。最新の分散台帳に記録されているブロックの内容を確認することで、トランザクションデータ生成部102が次に生成するトランザクションデータが、先に生成したトランザクションデータと異なるブロックに記録されるタイミングになったかを確認することができる。

[0055] より具体的には、トランザクションデータ確認部103は、第1時間より後の1以上の第2時間に、分散台帳に記録されているブロックの内容を確認することで、第1ブロックと、第2ブロックとが異なるか否かを確認する。

[0056] ここで、第1トランザクションデータが分散台帳に記録されるときに含まれるブロックを第1ブロックと称している。第1トランザクションデータの

1つ後の第2トランザクションデータを第2時間に生成したときに、第2トランザクションデータが分散台帳に記録されるときに含まれるブロックを第2ブロックと称している。

[0057] そして、トランザクションデータ確認部103は、第1ブロックと第2ブロックとが異なることを確認した場合、トランザクションデータ生成部102に、第1時間より後に取得した最新情報を含む第2トランザクションデータを、当該第2時間以降に、生成させる。

[0058] ここで、トランザクションデータ確認部103は、最新の分散台帳に記録されているブロックの内容として、例えば当該ブロックに第1トランザクションデータの1つ前に生成された第3トランザクションデータが含まれているかを確認してもよい。そして、トランザクションデータ確認部103は、当該ブロックに第3トランザクションデータが含まれていることを確認したら、トランザクションデータ生成部102に、第2トランザクションデータを生成させればよい。これにより、分散台帳に記録されるブロックごとに、機器100が生成した1つの第2トランザクションデータのみが含まれることになる。

[0059] また、トランザクションデータ確認部103は、最新の分散台帳に記録されているブロックの内容として、例えば、当該ブロックに第1トランザクションデータが含まれているかを確認してもよい。そして、トランザクションデータ確認部103は、当該ブロックに第1トランザクションデータが含まれていることを確認したら、トランザクションデータ生成部102に、第2トランザクションデータを生成させればよい。これにより、第2トランザクションデータが含まれない空白ブロックが分散台帳に記録されてしまう場合が発生するものの、分散台帳に記録される空白ブロックでない1つのブロックには、機器100が生成した1つの第2トランザクションデータのみが含まれることになる。

[0060] <確認方法決定部104>

確認方法決定部104は、認証サーバ装置210の処理能力に応じて、ト

ランザクションデータ確認部 103 が行う最新の分散台帳に記録されているブロックの内容の確認方法を決定してもよい。

[0061] より具体的には、確認方法決定部 104 は、第 1 サーバが単位時間当たり受信するランザクションデータ数である受信総数と、第 1 サーバが、分散台帳に記録する際、単位時間当たり処理可能なランザクションデータ数である処理可能数とを取得する。

[0062] 確認方法決定部 104 は、処理可能数が受信総数により定められる閾値以上の場合、ランザクションデータ確認部 103 に、最新の分散台帳に記録されているブロックの内容として、ブロックに第 3 ランザクションデータが含まれているかを確認させてもよい。

[0063] また、確認方法決定部 104 は、処理可能数が受信総数により定められる閾値より小さい場合、ランザクションデータ確認部 103 に、最新の分散台帳に記録されているブロックの内容として、ブロックに第 1 ランザクションデータが含まれているかを確認させてもよい。

[0064] これらにより、確認方法決定部 104 は、ランザクションデータ確認部 103 に、最新の分散台帳に記録されているブロックに、ランザクションデータ生成部 102 が 1 つ前または 2 つ前に生成して、送信されたランザクションデータが含まれたかどうかを確認させることができる。

[0065] なお、機器 100 を含めた複数の機器から送信されるランザクションデータの数は、認証サーバ装置 210 等に確認すれば、正確な数でなくとも上記の確認ができる程度には大まかに取得することができる。また、単位時間当たり処理可能なランザクションデータ数は、認証サーバ装置 210 等それぞれで予め決まっている。

[0066] <通信部 105>

通信部 105 は、認証サーバ装置 210、220、230 との通信を行う。

[0067] 本実施の形態では、通信部 105 は、ランザクションデータ生成部 102 で生成したランザクションデータを認証サーバ装置 210、220、2

30の少なくとも1つに送信する。また、通信部105は、認証サーバ装置210、220、230の処理能力として、受信総数と処理可能数とを取得して、確認方法決定部104に送信してもよい。また、通信部105は、認証サーバ装置210、220、230の最新の分散台帳の内容を取得して、トランザクションデータ確認部103に送信してもよい。

[0068] [機器100のハードウェア構成]

次に、本実施の形態に係る機器100のハードウェア構成について、図7を用いて説明する。図7は、本実施の形態に係る機器100の機能をソフトウェアにより実現するコンピュータ1000のハードウェア構成の一例を示す図である。

[0069] コンピュータ1000は、図7に示すように、入力装置1001、出力装置1002、CPU1003、内蔵ストレージ1004、RAM1005、読取装置1007、送受信装置1008及びバス1009を備えるコンピュータである。入力装置1001、出力装置1002、CPU1003、内蔵ストレージ1004、RAM1005、読取装置1007及び送受信装置1008は、バス1009により接続される。

[0070] 入力装置1001は入力ボタン、タッチパッド、タッチパネルディスプレイなどといったユーザインタフェースとなる装置であり、ユーザの操作を受け付ける。なお、入力装置1001は、ユーザの接触操作を受け付ける他、音声での操作、リモコン等での遠隔操作を受け付ける構成であってもよい。

[0071] 内蔵ストレージ1004は、フラッシュメモリなどである。また、内蔵ストレージ1004は、機器100の機能を実現するためのプログラム、及び、機器100の機能構成を利用したアプリケーションの少なくとも一方が、予め記憶されていてもよい。

[0072] RAM1005は、ランダムアクセスメモリ (Random Access Memory) であり、プログラム又はアプリケーションの実行に際してデータ等の記憶に利用される。

[0073] 読取装置1007は、USB (Universal Serial Bus) メモリなどの記録

媒体から情報を読み取る。読取装置1007は、上記のようなプログラムやアプリケーションが記録された記録媒体からそのプログラムやアプリケーションを読み取り、内蔵ストレージ1004に記憶させる。

[0074] 送受信装置1008は、無線又は有線で通信を行うための通信回路である。送受信装置1008は、例えばネットワークに接続されたサーバ装置と通信を行い、サーバ装置から上記のようなプログラムやアプリケーションをダウンロードして内蔵ストレージ1004に記憶させる。

[0075] CPU1003は、中央演算処理装置（Central Processing Unit）であり、内蔵ストレージ1004に記憶されたプログラム、アプリケーションをRAM1005にコピーし、そのプログラムまたはアプリケーションに含まれる命令をRAM1005から順次読み出して実行する。

[0076] 次に、認証サーバ装置210について説明する。

[0077] [認証サーバ装置210]

認証サーバ装置210、220及び230は同様の構成であるため、認証サーバ装置210を例に挙げて説明する。

[0078] 図8は、本実施の形態に係る認証サーバ装置210の機能構成を示すブロック図である。

[0079] 認証サーバ装置210は、機器100と通信可能に接続され、所定のタイミング毎に当該所定のタイミングまでに保持しているトランザクションデータのうち選択したトランザクションデータをブロックに含めて分散台帳に記録する。認証サーバ装置210は分散台帳に記録する第1サーバの一例である。

[0080] 本実施の形態では、認証サーバ装置210は、図8に示すように、トランザクションデータ格納部211と、トランザクションデータ検証部212と、台帳格納部213と、通信部214とを備える。認証サーバ装置210は、プロセッサがメモリを用いて所定のプログラムを実行することで実現される。以下、各構成要素について説明する。

[0081] <トランザクションデータ格納部211>

トランザクションデータ格納部 211 は、ブロックチェーンのまだ検証されていないトランザクションデータを溜めているトランザクションプールとして機能する。

[0082] 本実施の形態では、トランザクションデータ格納部 211 は、機器 100 から取得した例えば第 1 トランザクションデータ、第 2 トランザクションデータ、または第 3 トランザクションデータを格納し、一時的に保持する。トランザクションデータ格納部 211 は、保持しているトランザクションデータのうち、選択され分散台帳に書き込まれたトランザクションデータを削除したり、不要になったトランザクションデータを破棄したりする。

[0083] なお、トランザクションデータ格納部 211 は、機器 100 からトランザクションデータを取得したとき、当該トランザクションデータに含まれる電子署名の検証と、トランザクションデータの正当性の検証とを行ってもよい。そして、トランザクションデータ格納部 211 は、機器 100 から取得したトランザクションデータの検証が成功した場合のみ、機器 100 から取得したトランザクションデータを保持するとしてもよい。なお、この検証はスキップされてもよい。

[0084] <トランザクションデータ検証部 212>

トランザクションデータ検証部 212 は、コンセンサスアルゴリズムを実行することで、トランザクションデータ格納部 211 に保持されているトランザクションデータのうち選択したトランザクションデータの正当性を検証する。

[0085] ここで、コンセンサスアルゴリズムには、PBFT (Practical Byzantine Fault Tolerance) が用いられてもよいし、その他の公知のコンセンサスアルゴリズムが用いられてもよい。公知のコンセンサスアルゴリズムとしては、例えば POW (Proof Of Work) または POS (Proof Of Stake) などがある。コンセンサスアルゴリズムに PBFT が用いられる場合、トランザクションデータ検証部 212 は、他の複数の認証サーバ装置 220 及び 230 のそれ

それぞれからトランザクションデータの検証が成功したか否かを示す報告を受け取り、当該報告の数が所定の数を超えたか否かを判定する。そして、トランザクションデータ検証部 212 は、当該報告の数が所定の数を超えたとき、コンセンサスアルゴリズムによってトランザクションデータの正当性が検証されたと判定すればよい。

[0086] <台帳格納部 213>

台帳格納部 213 は、分散台帳に格納すべき新しいトランザクションデータを分散台帳に格納する処理部である。

[0087] 本実施の形態では、台帳格納部 213 は、トランザクションデータ検証部 212 により正当性が検証されたトランザクションデータを含むブロックを生成し、生成したブロックを分散台帳に格納する。換言すると、台帳格納部 213 は、トランザクションデータ検証部 212 により正当性が検証されたトランザクションデータを含むブロックを生成し、分散台帳に格納されているブロックチェーンに書き込む。

[0088] <通信部 214>

通信部 214 は、認証サーバ装置 220、230 との通信を行ったり、機器 100 との通信を行ったりする。

[0089] 本実施の形態では、通信部 214 は、トランザクションデータ検証部 212 が検証対象のトランザクションデータを、認証サーバ装置 220 及び 230 に送信する。また、通信部 214 は、機器 100 と通信し、トランザクションデータを取得したり、認証サーバ装置 210 自身の処理能力として、受信総数と処理可能数とを機器 100 に送信したりしてもよい。また、通信部 214 は、認証サーバ装置 210 自身が有する分散台帳の内容を、機器 100 に送信してもよい。

[0090] [動作]

続いて、以上のように構成された制御システムに含まれる機器 100 の動作について説明する。

[0091] 図 9 は、本実施の形態に係る機器 100 の動作を示すフローチャートであ

る。

[0092] 図9には、分散台帳に記録される1つのブロックに含まれる1以上のトランザクションデータの中に、機器100にとって機器100が送信する1つのトランザクションデータのみが含まれるようにする動作が示されている。

[0093] まず、機器100は、第1時間までに取得した最新情報を含む第1トランザクションデータを生成して、第1サーバに送信する(S10)。上述したように、第1サーバは例えば認証サーバ装置210に該当する。

[0094] 次に、機器100は、第1時間より後の第2時間に、第1サーバの分散台帳に記録されているブロックの内容を確認する(S11)。より具体的には、機器100は、分散台帳に記録されているブロックの内容を確認し、第1トランザクションデータの1つ後の第2トランザクションデータを第2時間に生成したとき、第1トランザクションデータとは異なるブロックに含まれるか否かを確認する。

[0095] 次に、機器100は、第2トランザクションデータを第2時間に生成した場合、第1トランザクションデータとは異なるブロックに含まれる場合(S12でYES)、第1時間より後に取得した最新情報を含む第2トランザクションデータを生成して、第1サーバに送信する(S13)。本実施の形態では、機器100は、第2時間以降から、第2時間時点で実行されているコンセンサスアルゴリズムの実行完了までに、第2トランザクションデータを生成して、第1サーバに送信する。

[0096] なお、機器100は、第2トランザクションデータを第2時間に生成したとき、第1トランザクションデータと同じブロックに含まれる場合(S12でNO)、ステップS11に戻って処理をやり直す。

[0097] (実施例1)

続いて、機器100が、ブロックの内容として、最新の分散台帳に記録されているブロックに、機器100自身が2つ前に送信したトランザクションデータが含まれたかどうかを確認する場合の制御システムの処理を実施例1として説明する。

[0098] 図10は、実施例1に係る制御システムの処理のシーケンス図である。図10には、図9に示すS11以降の制御システムの処理の一例が示されている。

[0099] ここで、機器100は、第1時間までに取得した最新情報を含む第1トランザクションデータを生成して、認証サーバ装置210、220、230に送信しており、認証サーバ装置210、220、230で第1トランザクションデータが少なくともプール（格納）されているとする。

[0100] 次に、第1時間より後の第2時間に、機器100は、認証サーバ装置210の最新の分散台帳を確認する（S21）。本実施例では、機器100は、例えば認証サーバ装置210に最新の分散台帳を要求し、認証サーバ装置210により送信された最新の分散台帳を取得することで、最新の分散台帳を確認する。

[0101] 次に、機器100は、取得した最新の分散台帳のブロックを参照（確認）し、機器100自身が2つ前に送信した第3トランザクションデータが含まれたかを確認する（S22）。ここで、機器100が、1つ前に送信したトランザクションデータを第1トランザクションデータとしている。また、機器100が、2つ前に送信したすなわち第1トランザクションデータの1つ前に送信したトランザクションデータを第3トランザクションデータとしている。換言すると、機器100が、これから（つまり第2時間以降に）生成して送信する第2トランザクションデータを基準として、1つ前に送信されたトランザクションデータを、第1トランザクションデータと称している。また、機器100が、これから送信する第2トランザクションデータを基準として、2つ前に送信されたトランザクションデータを、第3トランザクションデータと称している。

[0102] ステップS22において、機器100は、機器100自身が2つ前に送信した第3トランザクションデータが、最新の分散台帳に含まれた場合（S22でYES）、第1時間より後に取得した最新情報を含む第2トランザクションデータを生成する（S23）。なお、ステップS22において、機器1

00は、機器100自身が2つ前に送信した第3トランザクションデータが、最新の分散台帳に含まれていない場合（S22でNO）、ステップS21に戻って処理をやり直す。

[0103] 次に、機器100は、ステップS23において生成した第2トランザクションデータを、認証サーバ装置210、220、230に送信する（S24）。

[0104] すると、認証サーバ装置210、220、230はそれぞれ、機器100から取得した第2トランザクションデータを、プール（格納）する（S25）。

[0105] （実施例2）

続いて、機器100が、認証サーバ装置210の処理能力に応じて、認証サーバ装置210の最新の分散台帳に記録されているブロックの内容の確認方法を決定する場合の処理を実施例2として説明する。また、本実施例では、ブロックの内容の確認方法は、最新の分散台帳に記録されているブロックに、機器100自身が2つ前または1つ前に送信したトランザクションデータが含まれたかどうかを確認する方法であるとして説明する。

[0106] 図11は、実施例2に係る機器100の処理を示すフローチャートである。

[0107] 機器100は、以下で説明するステップS31を行う前において、第1時間までに取得した最新情報を含む第1トランザクションデータを生成して、認証サーバ装置210に送信しており、認証サーバ装置210で第1トランザクションデータが少なくともプール（格納）されているとする。

[0108] まず、機器100は、認証サーバ装置210から、認証サーバ装置210における単位時間当たりの処理可能数と、受信総数とを取得する（S31）。

[0109] 次に、機器100は、ステップS31で取得した処理可能数が閾値以上か（つまり、処理可能数 \geq 閾値）を確認する（S32）。ここでの閾値は、機器100が、ステップS31で取得した受信総数から定められ、例えば受信

総数の数%～数十%前後の値に定められる。

[0110] ステップS32において、処理可能数が閾値より小さい場合（S32でN O）、第1時間より後の第2時間に、機器100は、認証サーバ装置210の最新の分散台帳を確認する（S33）。本実施例でも機器100は、例えば認証サーバ装置210に最新の分散台帳を要求し、認証サーバ装置210により送信された最新の分散台帳を取得することで、最新の分散台帳を確認する。

[0111] 一方、ステップS32において、処理可能数が閾値以上である場合（S32でY E S）、ステップS33に進む。以降の処理すなわちステップS33、ステップS35、及びステップS36の処理は、図10のステップS21～ステップS24で説明した通りであるので、説明を省略する。

[0112] なお、機器100は、ステップS31の前に、最新情報を含む第1トランザクションデータを生成して認証サーバ装置210に送信するとして説明したが、これに限らない。ステップS31及びS32の後、かつ、ステップS33の前に最新情報を含む第1トランザクションデータを生成して認証サーバ装置210に送信するとしてもよい。

[0113] [効果等]

以上、実施の形態に係る制御システム等によれば、分散台帳に記録されたブロックの内容を確認してから1つの機器100すなわち同一のユーザないし同一事業者は、最新情報を含む1つのトランザクションデータを送信する。換言すると、実施の形態に係る制御システム等では、機器100は、トランザクションデータをPUSH型で送信せず、ASK型で1つずつ送信する。これにより、分散台帳に記録される1つのブロックには、機器100にとって1つの機器100が送信する1つのトランザクションデータのみが含まれることになる。よって、利用しない無駄なトランザクションデータがブロックに記録されることを抑制することができるので、ネットワーク帯域及びリソースの無駄使いを抑制することができる。

[0114] ここで、図12～図14を用いて、実施の形態に係る効果について説明す

る。図12及び図13は、実施の形態に係る効果について説明するためのフロー図である。図14は、図13に示すフロー図の別観点での説明図である。

- [0115] まず、図12を用いて、機器100が、次に生成予定の第2トランザクションデータを基準に、1つ前に生成した第1トランザクションデータが、最新の分散台帳に記録されたブロックに含まれたことを確認後に、第2トランザクションデータを生成して送信する場合について説明する。
- [0116] 図12において、第1トランザクションデータを $T_{x_{n-1}}$ と表記し、第2トランザクションデータを T_{x_n} と表記する。また、コンセンサスアルゴリズムが実行される期間をコンセンサスと表記する。コンセンサスアルゴリズムが実行される期間は、ブロックチェーンにブロックを書き込むために要する期間として示されている。図12に示すブロックチェーンでは、コンセンサスアルゴリズムの開始前までに送信されたトランザクションデータに対してコンセンサスアルゴリズムが実行され、コンセンサスアルゴリズムの実行完了後に、ブロックに含まれてブロックチェーンに書き込まれることが示されている。コンセンサスアルゴリズムの開始前までに送信されたトランザクションデータは、トランザクションプールに保持されている。
- [0117] 図12に示されるように、機器100は、生成後に送信した $T_{x_{n-1}}$ がブロックチェーンに書き込まれたブロックに含まれたかを定期的に確認してもよい。この場合、機器100は、ブロックチェーンに書き込まれたブロックに $T_{x_{n-1}}$ が含まれたことを確認したら、 T_{x_n} を生成して送信する。すると、連続するブロックそれぞれに機器100が生成して送信したトランザクションデータが含まれない（機器100にとっての空白ブロックが発生する）。しかし、空白ブロックではないブロックには、機器100にとって機器100が生成して送信した1つのトランザクションデータのみが含まれることになる。
- [0118] つまり、機器100は、ブロックチェーンに書き込まれたブロックに、機器100が1つ前に送信したトランザクションデータが含まれたことを確認

してから次のトランザクションデータを送信してもよい。これにより、機器100は、ブロックチェーンに書き込まれるブロックに機器100にとっての空白ブロックが発生する場合があるものの機器100が送信した2以上のトランザクションデータが1つのブロックに含まれてしまうことを抑制することができる。

[0119] このように、機器100にとって空白ブロックが分散台帳に記録される場合が発生するものの、分散台帳に記録される1つのブロックには、機器100にとって機器100により送信される1つのトランザクションデータのみが含まれることになる。

[0120] よって、利用しない無駄なトランザクションデータがブロックに記録されることを抑制することができるので、ネットワーク帯域及びリソースの無駄使いを抑制することができる。

[0121] 次に、図13及び図14を用いて、機器100が、次に生成予定の第2トランザクションデータを基準に、2つ前に生成した第3トランザクションデータが、最新の分散台帳に記録されたブロックに含まれたことを確認後に、第2トランザクションデータを生成して送信する場合について説明する。ここで、図13及び図14において、第1トランザクションデータは、次に生成予定の第2トランザクションデータを基準に1つ前に生成したトランザクションデータであり、 $T \times_{n-1}$ と表記している。また、第2トランザクションデータを $T \times_n$ と表記し、第1トランザクションデータの1つ前に生成された第3トランザクションデータを $T \times_{n-2}$ と表記する。また、第2トランザクションデータの1つ後に生成される予定のトランザクションデータを $T \times_{n+1}$ と表記する。

[0122] 図13及び図14に示されるように、機器100は、 $T \times_n$ の生成及び送信タイミングを確認するため、 $T \times_{n-1}$ の送信後には、 $T \times_{n-2}$ がブロックチェーンに書き込まれたブロックに含まれたかを確認している。そして、機器100は、ブロックチェーンに書き込まれたブロックに $T \times_{n-2}$ が含まれたことを確認したら、 $T \times_n$ を生成して送信している。

- [0123] 次に、機器100は、 $T \times_{n+1}$ の生成及び送信タイミングを確認するため、 $T \times_n$ の送信後には、 $T \times_{n-1}$ がブロックチェーンに書き込まれたブロックに含まれたかを確認している。そして、機器100は、ブロックチェーンに書き込まれたブロックに $T \times_{n-1}$ が含まれたことを確認したら、 $T \times_{n+1}$ を生成して送信している。このため、連続するブロックそれぞれに機器100が生成して送信したトランザクションデータを含むことになる（機器100にとっての空白ブロックが発生しない）。
- [0124] このように、機器100は、ブロックチェーンに書き込まれたブロックに、機器100が2つ前に送信したトランザクションデータが含まれたことを確認してから次のトランザクションデータを送信する。これにより、1つのブロックには、機器100にとって機器100が生成して送信した1つのトランザクションデータのみが含まれることになる。つまり、機器100が送信した2以上のトランザクションデータが1つのブロックに含まれてしまうことを抑制することができる。また、ブロックごとに機器100にとって機器100が生成して送信した1つのトランザクションデータのみが含まれるので、機器100にとって空白ブロックが発生してしまうことも抑制することができる。
- [0125] 換言すると、利用されない1以上のトランザクションデータがブロックに含まれて分散台帳に記録されることを抑制できるだけでなく、当該機器にとっての空白ブロックが分散台帳に記録されることを抑制できる。よって、ネットワーク帯域及びリソースの無駄使いをさらに抑制することができる。
- [0126] また、分散台帳を有する認証サーバ装置の処理能力に応じて、最新の分散台帳に記録されたブロックに、第1トランザクションデータが含まれたこと、または、第1トランザクションデータの1つ前に生成された第3トランザクションデータが含まれたことを確認してもよい。これにより、認証サーバ装置の処理能力に応じて、機器100にとっての空白ブロックが分散台帳に記録される場合が発生することを許容するか否かを選択することができる。
- [0127] [その他変形例]

なお、本開示を上記各実施の形態に基づいて説明してきたが、本開示は、上記各実施の形態に限定されないのはもちろんである。以下のような場合も本開示に含まれる。

[0128] (1) 上記の実施の形態に係る各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAMまたはハードディスクユニットには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わせられて構成されたものである。

[0129] (2) 上記の実施の形態に係る各装置は、構成する構成要素の一部または全部は、1個のシステムLSI (Large Scale Integration: 大規模集積回路) から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムLSIは、その機能を達成する。

[0130] また、上記の各装置を構成する構成要素の各部は、個別に1チップ化されていても良いし、一部またはすべてを含むように1チップ化されてもよい。

[0131] また、ここでは、システムLSIとしたが、集積度の違いにより、IC、LSI、スーパーLSI、ウルトラLSIと呼称されることもある。また、集積回路化の手法はLSIに限るものではなく、専用回路または汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA (Field Programmable Gate Array) や、LSI内部の回路セルの接続や設定を再構成可能なリプログラブル

・プロセッサを利用しても良い。

[0132] さらには、半導体技術の進歩または派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

[0133] (3) 上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なICカードまたは単体のモジュールから構成されているとしてもよい。前記ICカードまたは前記モジュールは、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ICカードまたは前記モジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ICカードまたは前記モジュールは、その機能を達成する。このICカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

[0134] (4) 本開示は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

[0135] また、本開示は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータで読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blue-ray (登録商標) Disc)、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

[0136] また、本開示は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

[0137] また、本開示は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記録しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動

作するとしてもよい。

[0138] また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を、前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

[0139] (5) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0140] 本開示は、分散台帳に記録するトランザクションデータの制御方法及びデータ生成装置に利用でき、特に最新情報を定期的に分散台帳に記録するものの最新情報だけを利用し、過去の情報を利用しない分散台帳に記録するトランザクションデータの制御方法及びデータ生成装置に利用できる。

符号の説明

- [0141] 100 機器
- 101 センサ情報取得部
 - 102 トランザクションデータ生成部
 - 103 トランザクションデータ確認部
 - 104 確認方法決定部
 - 105、214 通信部
 - 210、220、230 認証サーバ装置
 - 211 トランザクションデータ格納部
 - 212 トランザクションデータ検証部
 - 213 台帳格納部

請求の範囲

[請求項1]

機器と、それぞれ、前記機器と通信可能に接続され、所定のタイミング毎に当該所定のタイミングまでに保持しているトランザクションデータのうち選択したトランザクションデータをブロックに含めて分散台帳に記録する複数のサーバとを備えるシステムにおける前記機器によって実行される制御方法であって、

第1時間までに取得した最新情報を含む第1トランザクションデータを生成して、前記複数のサーバのうち第1サーバに送信し、

前記第1時間より後の1以上の第2時間に、前記第1サーバの前記分散台帳に記録されているブロックの内容を確認することで、前記第1トランザクションデータの1つ後の第2トランザクションデータを前記第2時間に生成したときに、前記第1トランザクションデータが前記分散台帳に記録されるときに含まれる第1ブロックと、前記第2トランザクションデータが前記分散台帳に記録されるときに含まれる第2ブロックとが異なるか否かを確認し、

前記第1ブロックと前記第2ブロックとが異なる場合、前記第1時間より後に取得した最新情報を含む前記第2トランザクションデータを、当該第2時間以降に生成して、前記第1サーバに送信する、

制御方法。

[請求項2]

前記ブロックの内容を確認する際、

前記ブロックの内容として、前記ブロックに前記第1トランザクションデータの1つ前に生成された第3トランザクションデータが含まれているかを確認する、

請求項1に記載の制御方法。

[請求項3]

さらに、前記第1サーバが単位時間当たりに受信するトランザクションデータ数である受信総数と、前記第1サーバが、前記分散台帳に記録する際、単位時間当たりに処理可能なトランザクションデータ数である処理可能数とを取得し、

前記処理可能数が前記受信総数により定められる閾値以上の場合、前記ブロックの内容として、前記ブロックに前記第3トランザクションデータが含まれているかを確認する、

請求項2に記載の制御方法。

[請求項4]

前記ブロックの内容を確認する際、

前記ブロックの内容として、前記ブロックに前記第1トランザクションデータが含まれているかを確認する、

請求項1に記載の制御方法。

[請求項5]

さらに、前記第1サーバが単位時間当たりに受信するトランザクションデータ数である受信総数と、前記第1サーバが、前記分散台帳に記録する際、単位時間当たりに処理可能なトランザクションデータ数である処理可能数とを取得し、

前記処理可能数が前記受信総数により定められる閾値より小さい場合、前記ブロックの内容として、前記ブロックに前記第1トランザクションデータが含まれているかを確認する、

請求項3または4に記載の制御方法。

[請求項6]

それぞれ、所定のタイミング毎に当該所定のタイミングまでに保持しているトランザクションデータのうち選択したトランザクションデータをブロックに含めて分散台帳に記録する複数のサーバと通信可能に接続されるデータ生成装置であって、

プロセッサと、

メモリと、を備え、

前記プロセッサは、第1時間までに取得した最新情報を含む第1トランザクションデータを生成して、前記複数のサーバのうち第1サーバに送信し、

前記プロセッサは、前記第1時間より後の1以上の第2時間に、前記第1サーバの前記分散台帳に記録されているブロックの内容を確認することで、前記第1トランザクションデータの1つ後の第2トラン

ザクションデータを前記第2時間に生成したときに、前記第1トランザクションデータが前記分散台帳に記録されるときに含まれる第1ブロックと、前記第2トランザクションデータが前記分散台帳に記録されるときに含まれる第2ブロックとが異なるか否かを確認し、

前記プロセッサは、前記第1ブロックと前記第2ブロックとが異なることを確認した場合、前記第1時間より後に取得した最新情報を含む前記第2トランザクションデータを、当該第2時間以降に生成して、前記第1サーバに送信する、

データ生成装置。

[請求項7]

機器と、それぞれ、前記機器と通信可能に接続され、所定のタイミング毎に当該所定のタイミングまでに保持しているトランザクションデータのうち選択したトランザクションデータをブロックに含めて分散台帳に記録する複数のサーバとを備えるシステムにおける前記機器によって実行される制御方法をコンピュータに実行させるためのプログラムであって、

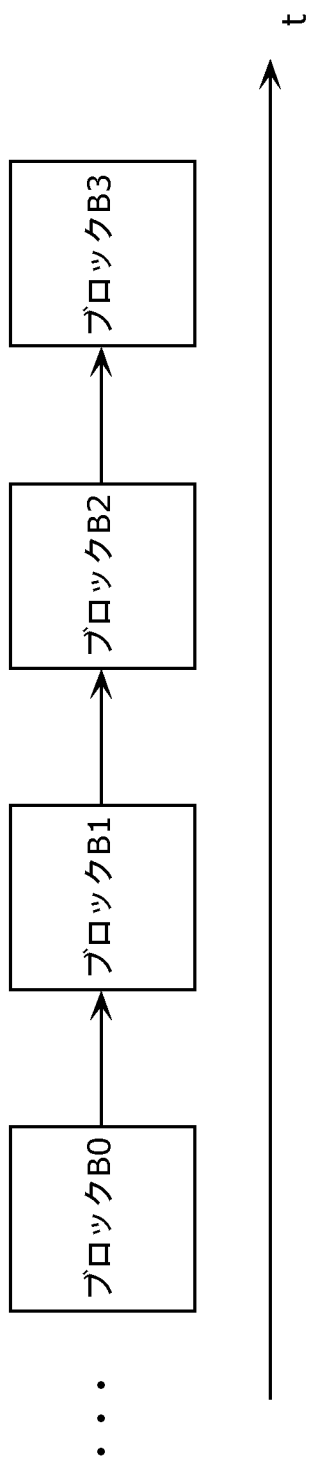
第1時間までに取得した最新情報を含む第1トランザクションデータを生成して、前記複数のサーバのうち第1サーバに送信し、

前記第1時間より後の1以上の第2時間に、前記第1サーバの前記分散台帳に記録されているブロックの内容を確認することで、前記第1トランザクションデータの1つ後の第2トランザクションデータを前記第2時間に生成したときに、前記第1トランザクションデータが前記分散台帳に記録されるときに含まれる第1ブロックと、前記第2トランザクションデータが前記分散台帳に記録されるときに含まれる第2ブロックとが異なるか否かを確認し、

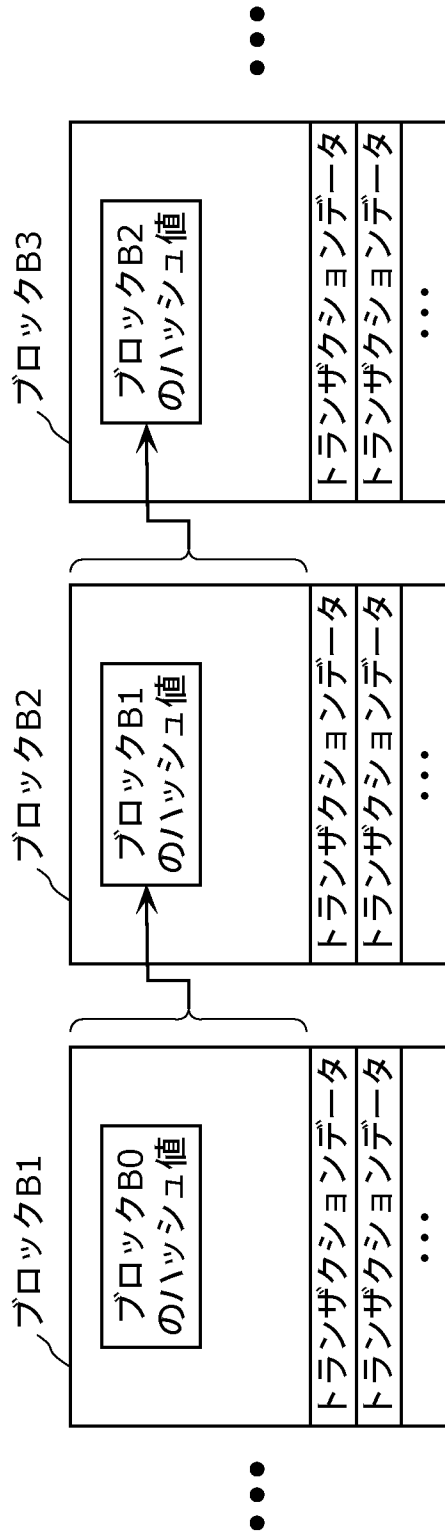
前記第1ブロックと前記第2ブロックとが異なることを確認した場合、前記第1時間より後に取得した最新情報を含む前記第2トランザクションデータを、当該第2時間以降に生成して、前記第1サーバに送信することを、

コンピュータに実行させるためのプログラム。

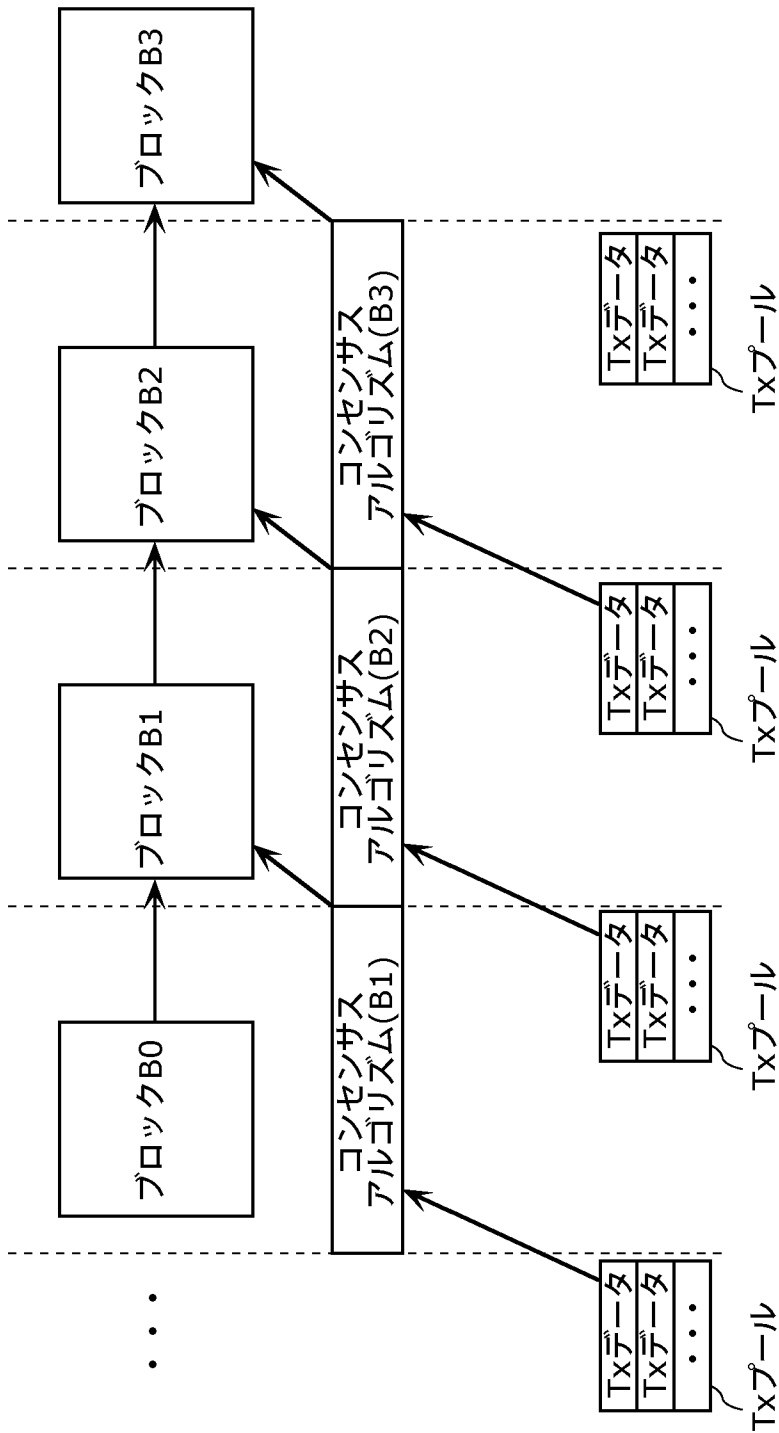
[図1]



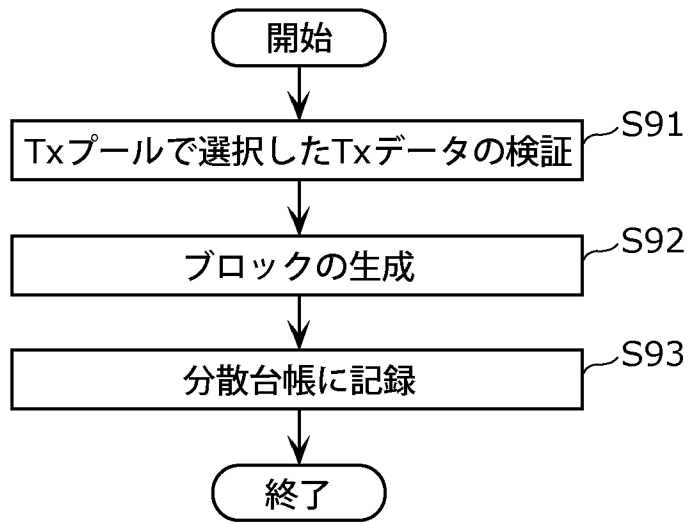
[図2]



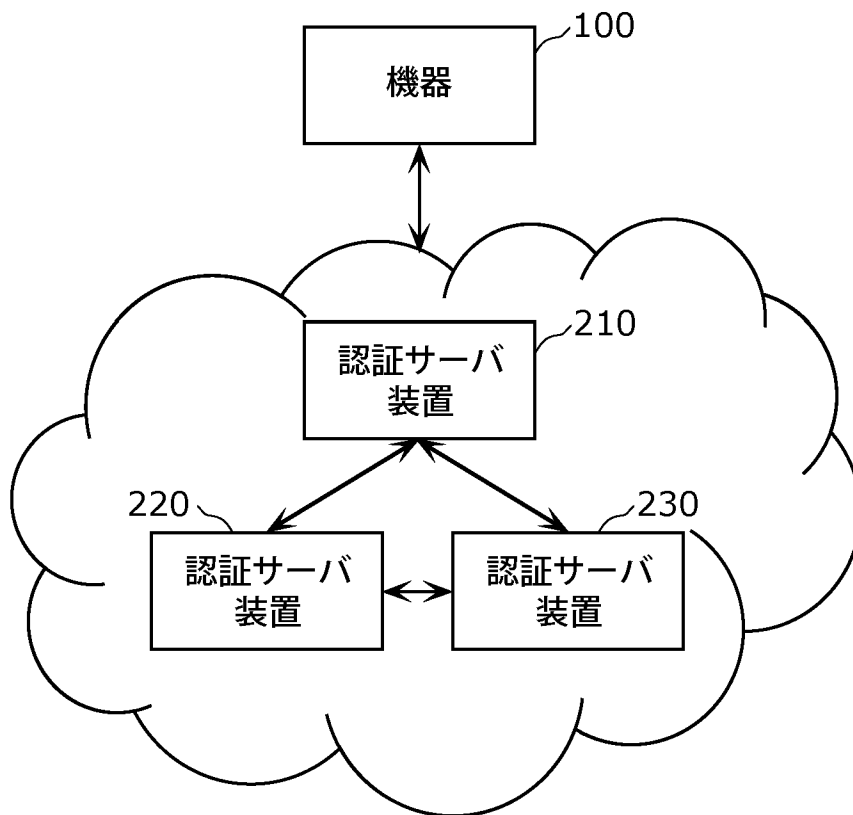
[図3]



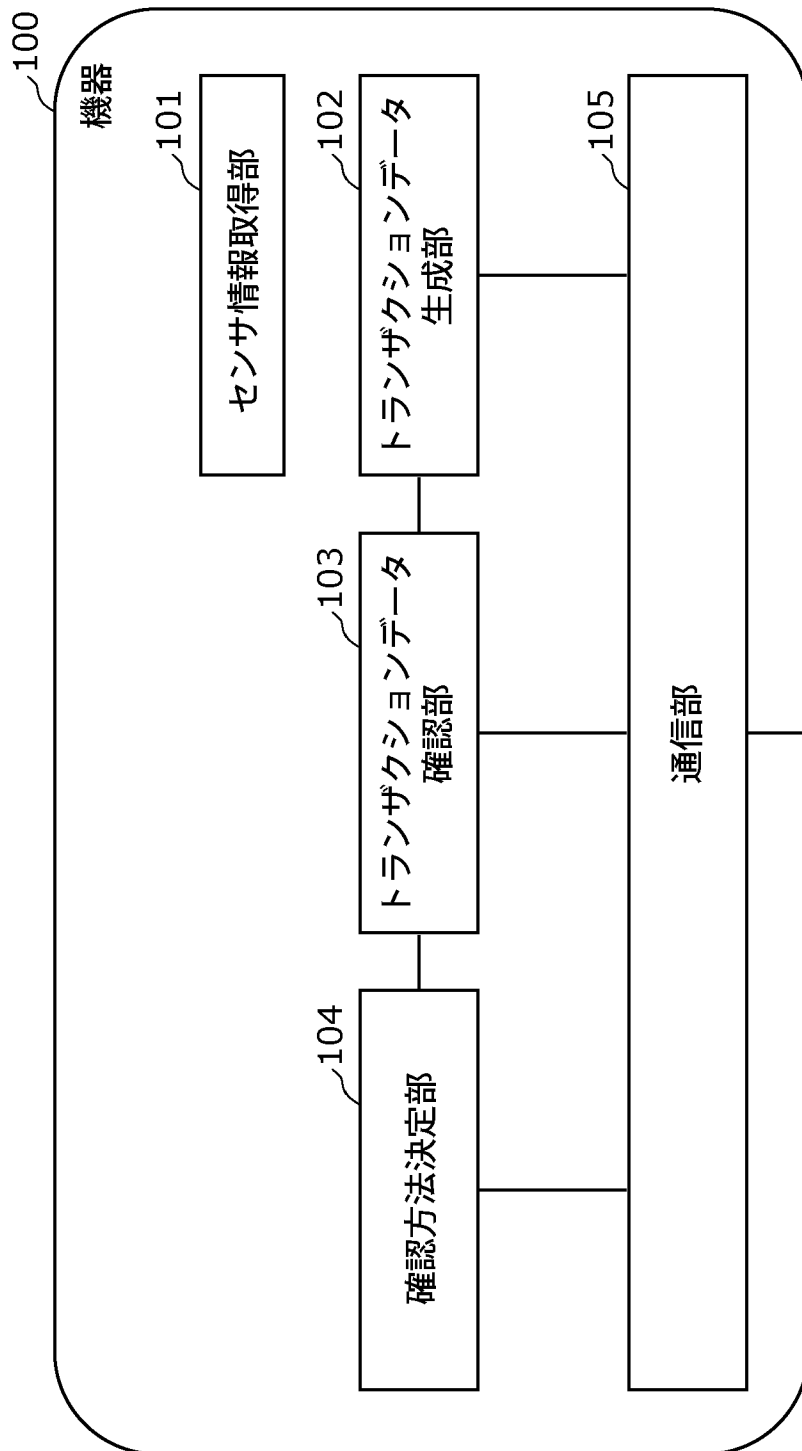
[図4]



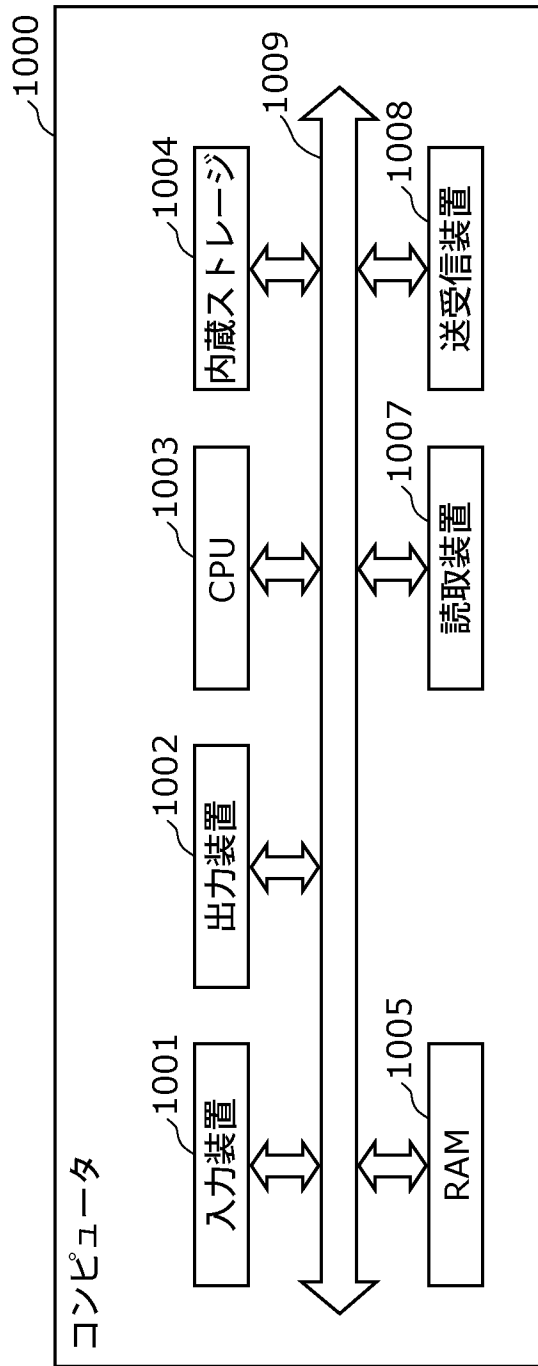
[図5]



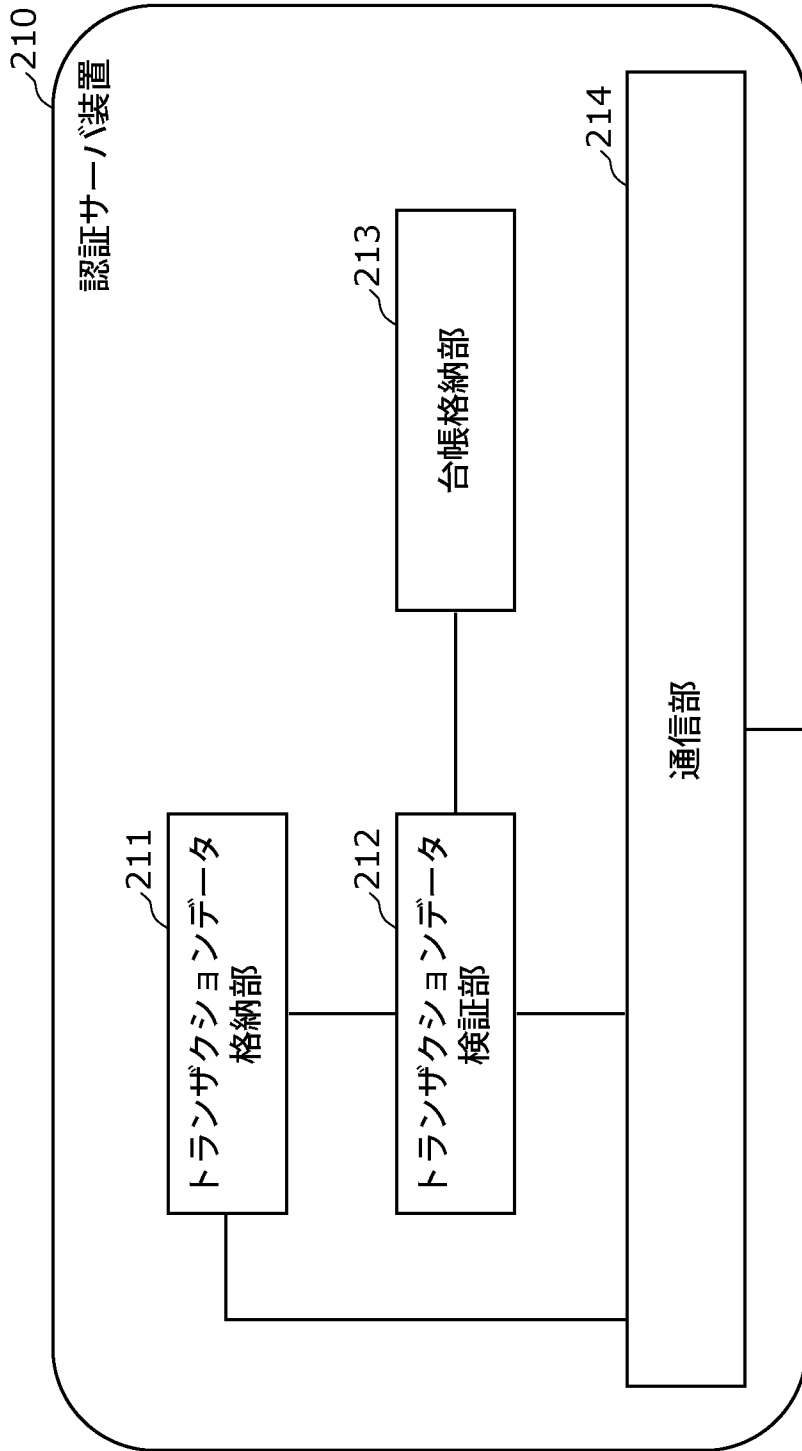
[図6]



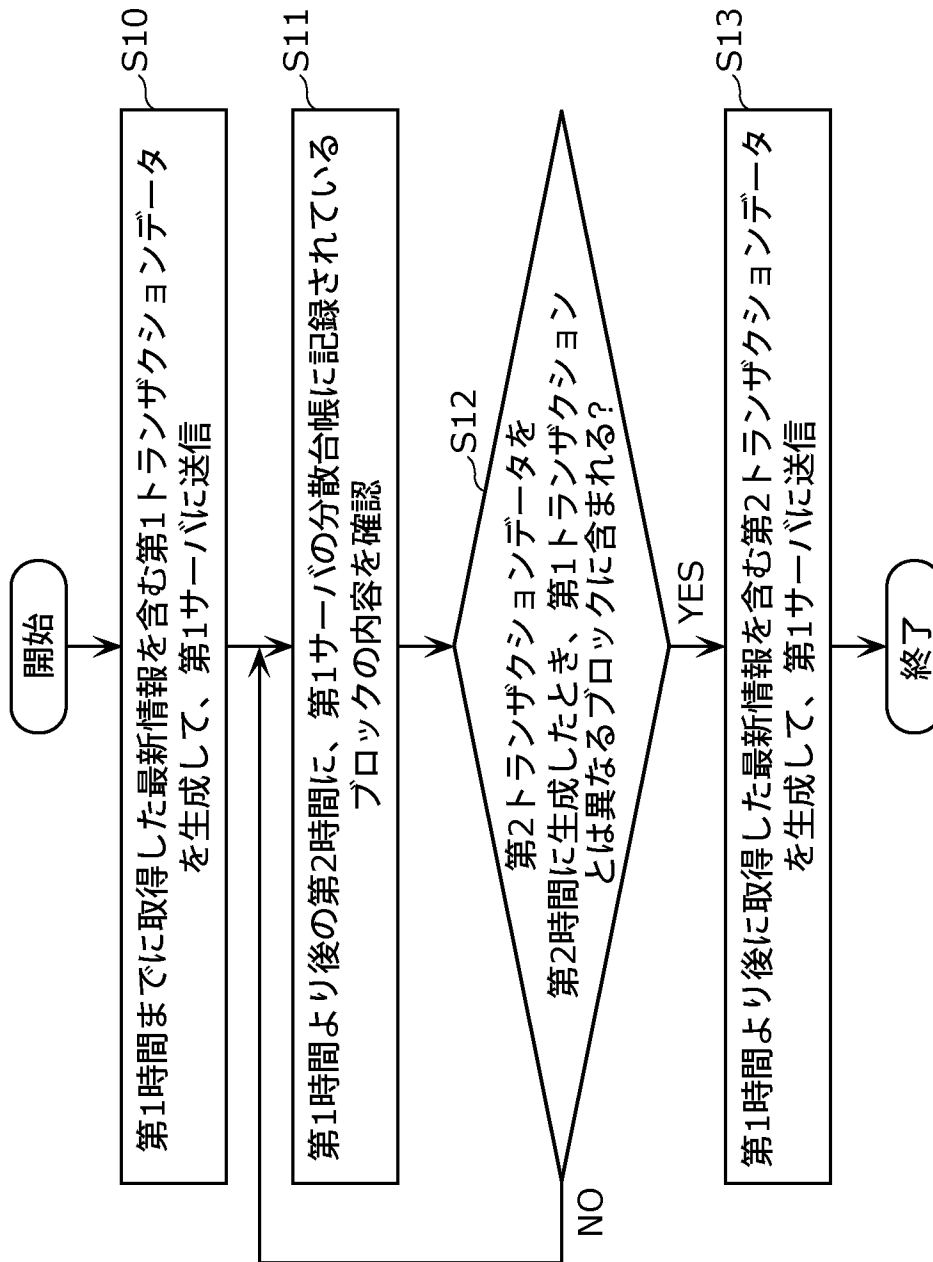
[図7]



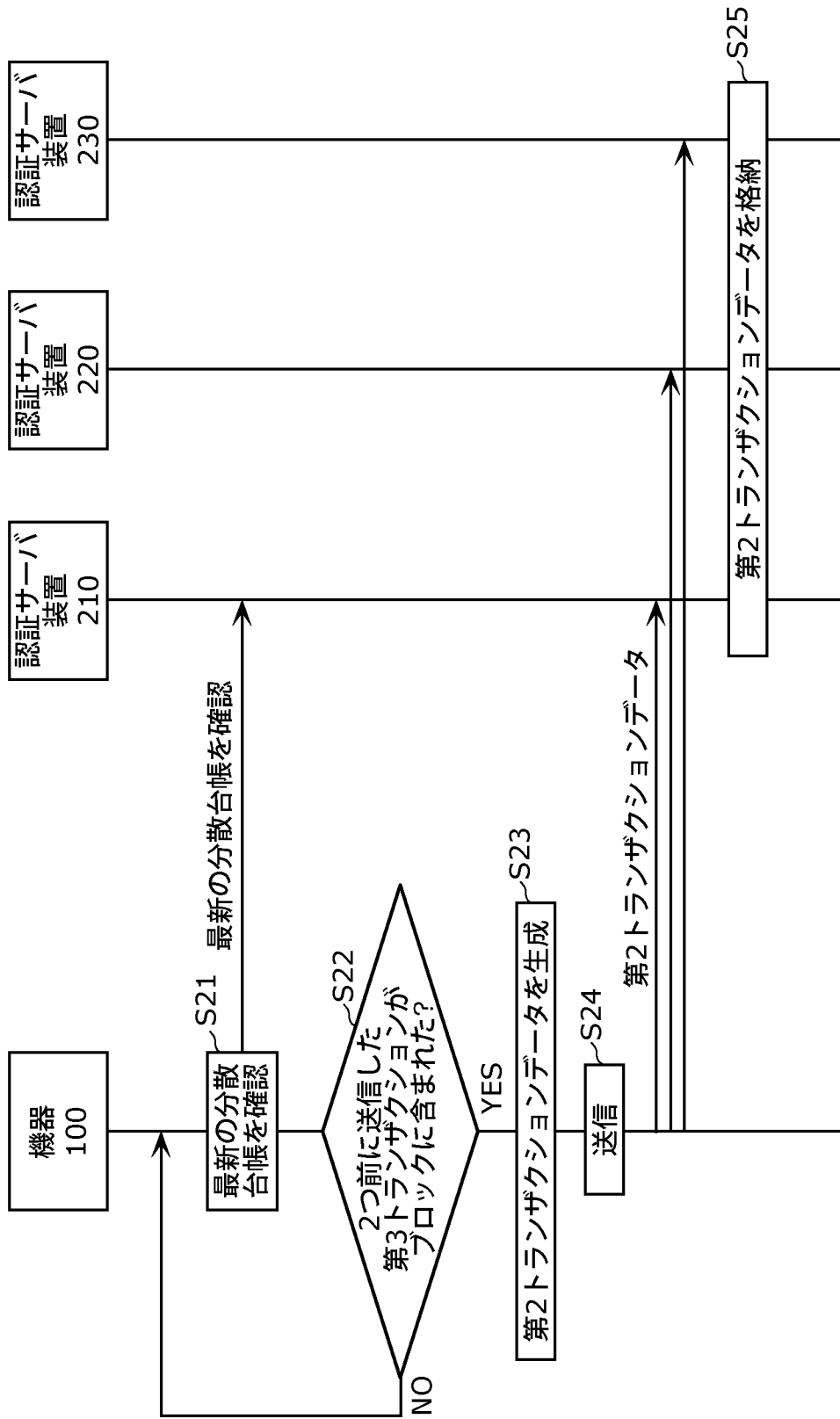
[図8]



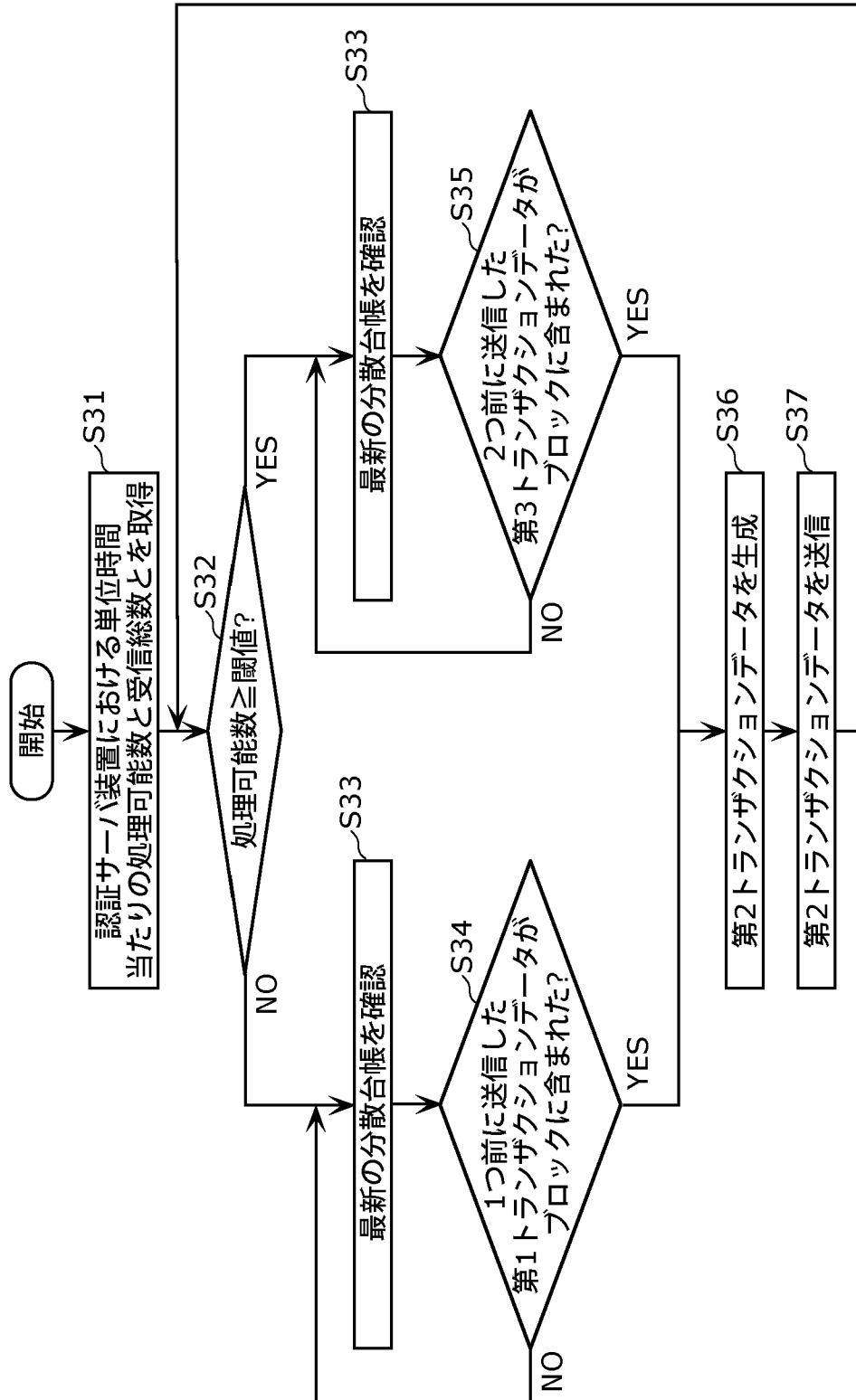
[図9]



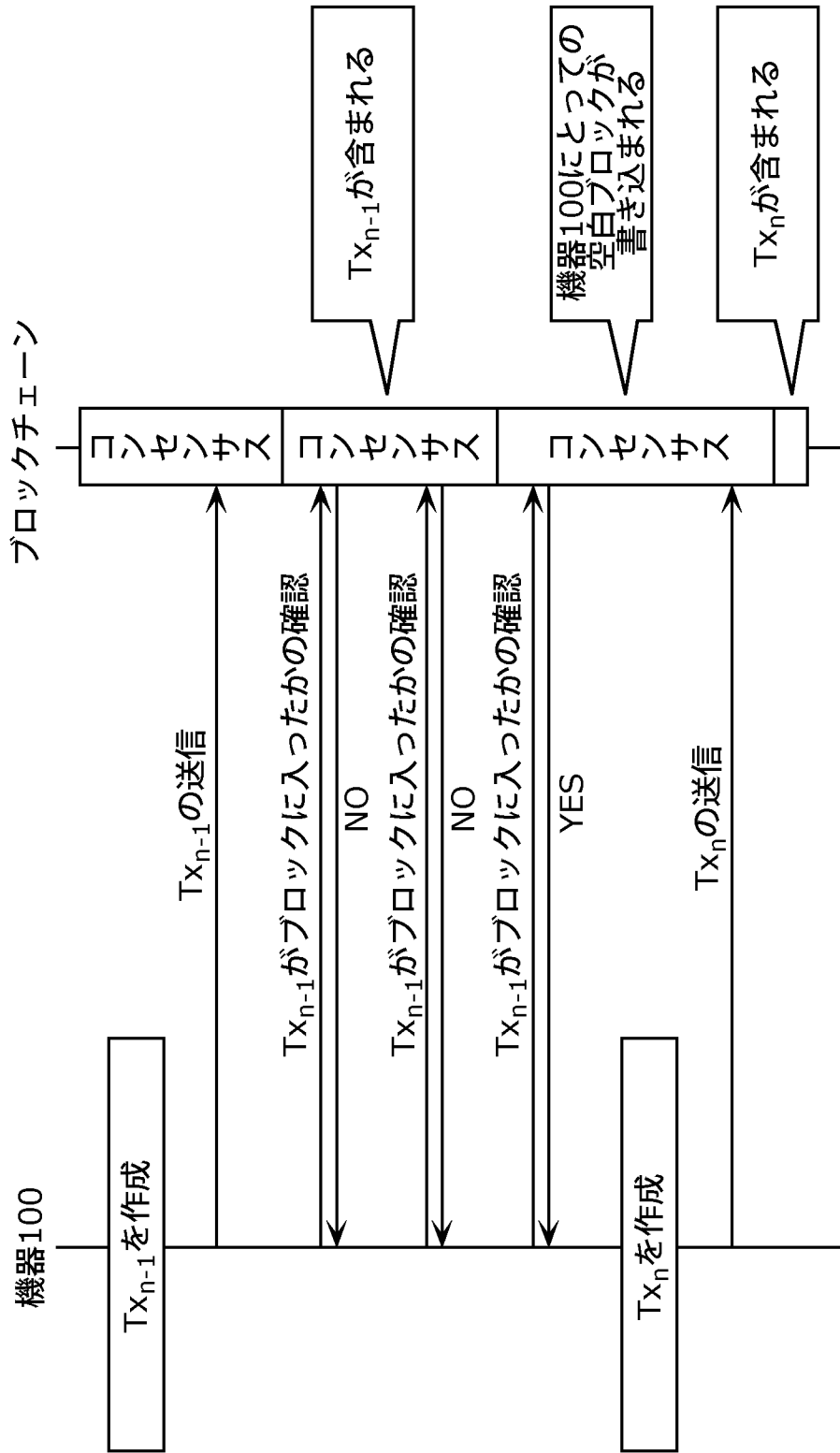
[図10]



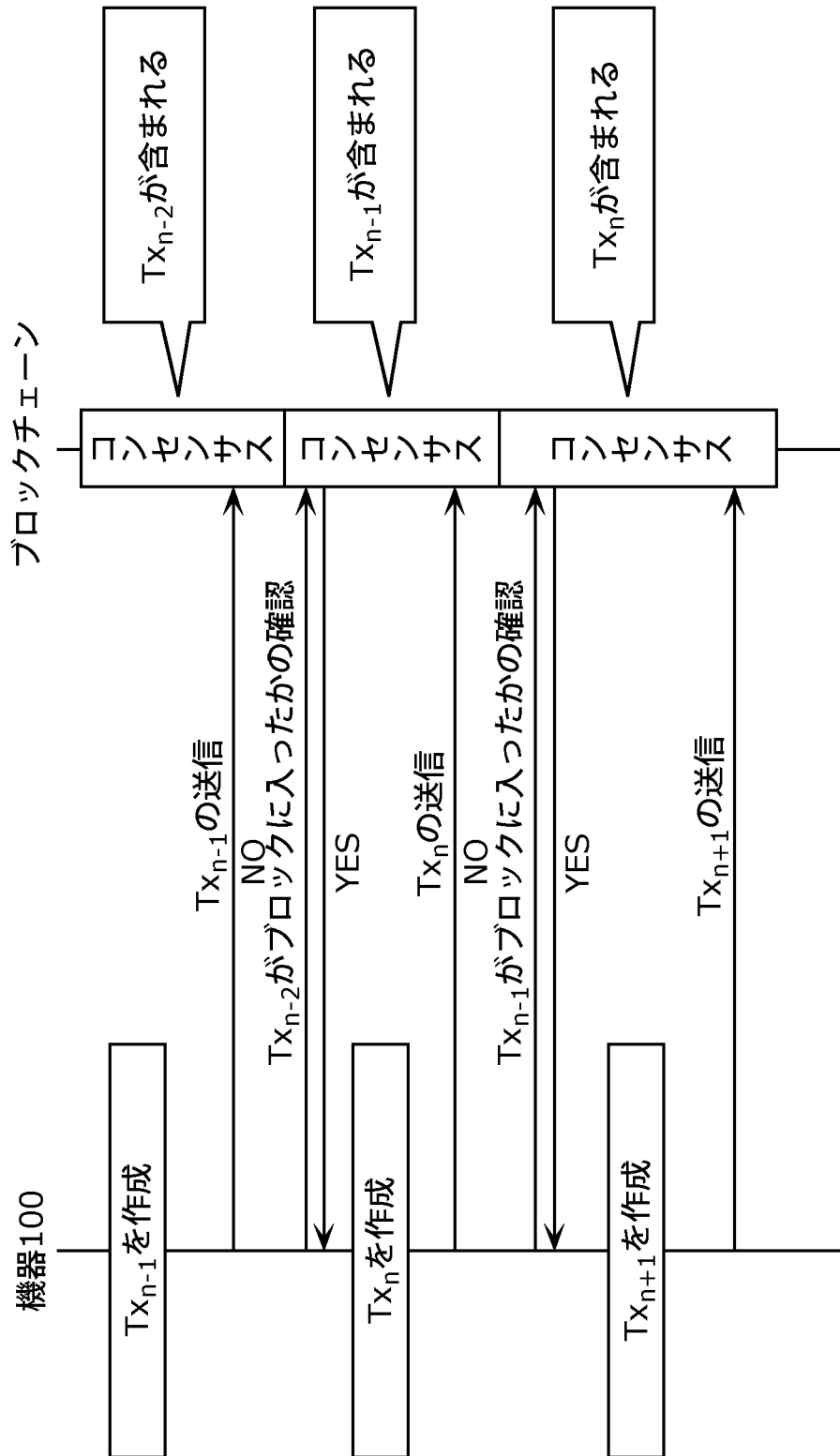
[図11]



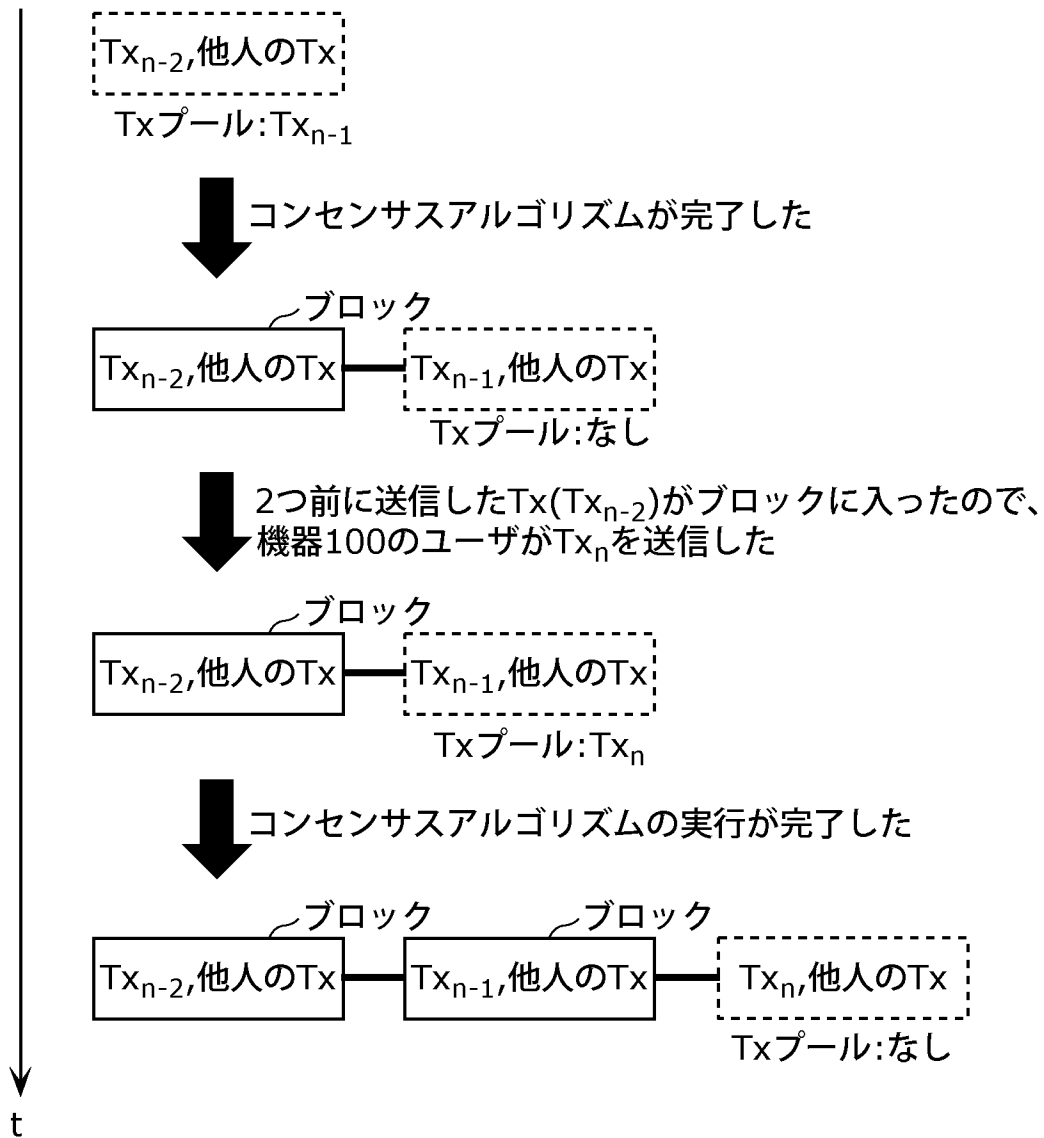
[図12]



[図13]



[図14]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/017789

A. CLASSIFICATION OF SUBJECT MATTER

G06F 16/182 (2019.01) i

FI: G06F16/182

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)

G06F16/00

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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.
A	JP 2019-28525 A (HITACHI, LTD.) 21.02.2019 (2019-02-21) entire text, all drawings	1-7
A	JP 2009-26029 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 05.02.2009 (2009-02-05) entire text, all drawings	1-7

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

“I” 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
17 July 2020 (17.07.2020)

Date of mailing of the international search report
04 August 2020 (04.08.2020)

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

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/017789

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	今村 光良外, ブロックチェーン技術に関する分析および評価, FIT2017 第16回情報科学技術フォーラム講演論文集 第4分冊 選奨論文・一般論文 ネットワーク・セキュリティユビキタス・モバイルコンピューティング教育・人文科学情報システム, 05 September 2017, pp. 103-108, entire text, all drawings, non-official translation (IMAMURA, Mitsuyoshi et al., "Analysis and evaluation of blockchain technology", Selected papers and general papers of 4th volume of lecture proceedings of 16th Forum on Information Technology (FIT) 2017, Network-Security Ubiquitous-Mobile Computing Education-Humanities Information System)	1-7

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/017789

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2019-28525 A	21 Feb. 2019	WO 2019/021792 A1 entire text, all drawings	
JP 2009-26029 A	05 Feb. 2009	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 16/182(2019.01)i FI: G06F16/182		
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（IPC）） G06F16/00		
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 - 2020年	
日本国実用新案登録公報	1996 - 2020年	
日本国登録実用新案公報	1994 - 2020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
A	JP 2019-28525 A (株式会社日立製作所) 21.02.2019 (2019 - 02 - 21) 全文全図	1-7
A	JP 2009-26029 A (日本電信電話株式会社) 05.02.2009 (2009 - 02 - 05) 全文全図	1-7
A	今村 光良 外, ブロックチェーン技術に関する分析および評価, FIT2017 第 16回情報科学技術フォーラム 講演論文集 第4分冊 選奨論文・一般論文 ネット ワーク・セキュリティ ユビキタス・モバイルコンピューティング 教育・人文科学 情報システム, 2017.09.05, pp. 103-108 全文全図	1-7
<input type="checkbox"/> C欄の続きにも文献が列挙されている。 <input checked="" type="checkbox"/> 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	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの “A” 特に関連のある文献ではなく、一般的な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 “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	17.07.2020	国際調査報告の発送日 04.08.2020
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 原 秀人 5N 9644 電話番号 03-3581-1101 内線 3586	

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2020/017789

引用文献	公表日	パテントファミリー文献	公表日
JP 2019-28525 A	21.02.2019	WO 2019/021792 A1 全文全図	
JP 2009-26029 A	05.02.2009	(ファミリーなし)	