(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 5 月 18 日(18.05.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/082237 A1

(51) 国際特許分類:
G06Q 20/06 (2012.01)

(21) 国際出願番号: PCT/JP2016/083062

(22) 国際出願日: 2016 年 11 月 8 日(08.11.2016)

(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 2015-219424 2015 年 11 月 9 日(09.11.2015) JP

(71) 出願人: 日本電信電話株式会社(NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 渡邊 大喜(WATANABE Hiroki); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 阿久津 明人(AKUTSU Akihito); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 宮崎 泰彦(MIYAZAKI Yasuhiko); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 中平 篤(NAKADAIRA Atsushi); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 藤村 滋(FUJIMURA Shigeru); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 岸上 順一(KISHIGAMI Junichi); 〒0508585 北海道室蘭市水元町２７番１号 Hokkaido (JP).

(74) 代理人: 三好 秀和, 外(MIYOSHI Hidekazu et al.); 〒1050001 東京都港区虎ノ門１丁目２番８号 虎ノ門琴平タワー 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, KE, KG, 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.

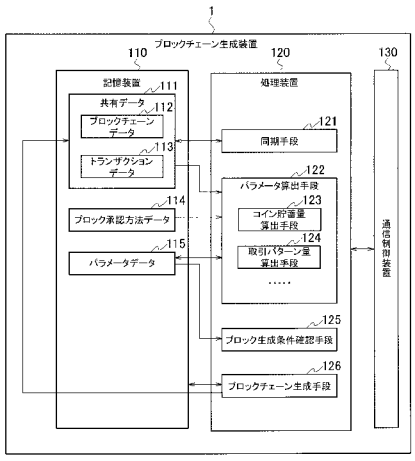
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW,

[続葉有]

(54) **Title**: BLOCK CHAIN GENERATION DEVICE, BLOCK CHAIN GENERATION METHOD, BLOCK CHAIN VERIFICATION DEVICE, BLOCK CHAIN VERIFICATION METHOD AND PROGRAM

(54) 発明の名称 : ブロックチェーン生成装置、ブロックチェーン生成方法、ブロックチェーン検証装置、ブロックチェーン検証方法およびプログラム

[図5]



1 Block chain generation device
110 Storage device
111 Shared data
112 Block chain data
113 Transaction data
114 Block authentication method data
115 Parameter data
120 Processing device
121 Synchronizing means
122 Parameter calculation means
123 Coin accumulated amount calculation means
124 Transaction pattern amount calculation means
125 Block generation condition confirmation means
126 Block chain generation means
130 Communication control device

(57) **Abstract**: This block chain generation device 1 is provided with: a parameter calculation means 122 which, on the basis of block authentication method data 114, specifies a parameter type to be used when linking a new block, and which, from transaction data relating to an identifier of the creator, calculates a value of the specified parameter type; a block generation condition confirmation means 125 which, on the basis of the value calculated by the parameter calculation means 122, confirms whether or not the creator is qualified to generate new block chain data; and a block chain generation means 126 which, if the block generation condition confirmation means 125 determines that said creator is qualified, attempts to create a new block chain. An identifier of a blend pattern contained in the block authentication method data 114 specifies a combination of multiple parameter types opposed to each other.

(57) 要約: ブロックチェーン生成装置１は、ブロック承認方法データ１１４に基づいて、新たなブロックを連結する際に用いられるパラメータ種別を特定し、生成者の識別子に関連するトランザクションデータから、特定されたパラメータ種別の値を算出するパラメータ算出手段１２２と、パラメータ算出手段１２２が算出した値に基づいて、生成者が、新たなブロックチェーンデータを生成する資格を有しているか否かを判定するブロック生成条件確認手段１２５と、ブロック生成条件確認手段１２５が資格を有していると判定した場合、新たなブロックチェーンの生成を試みるブロックチェーン生成手段１２６とを備える。ブロック承認方法データ１１４に含まれるブレンドパターンの識別子は、互いに相反する複数のパラメータ種別の組み合わせを特定する。

WO 2017/082237 A1

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:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

ブロックチェーン生成装置、ブロックチェーン生成方法、ブロックチェーン検証装置、ブロックチェーン検証方法およびプログラム

技術分野

[0001] 本発明は、複数のトランザクション生成装置によって生成されたトランザクションデータを含むブロックを連結したブロックチェーンデータを生成するブロックチェーン生成装置およびブロックチェーン生成方法、ブロックチェーンデータを検証するブロックチェーン検証装置およびブロックチェーン検証方法、ならびプログラムに関する。

背景技術

[0002] 近年、ビットコイン（登録商標）などのデジタル仮想通貨が普及しつつある。このような仮想通貨では、中央集権的な管理を必要とせずに、信頼性を担保可能な仕組みが導入されている。ビットコイン（登録商標）などの仮想通貨において、ブロックチェーンと呼ばれる技術が用いられている。ブロックチェーン技術において、参加者間でやり取りされる情報の信頼性は、参加者全体で形成されるネットワーク内での合意形成のプロセスによって担保される。また改ざんや二重使用などの不正を系全体で防ぐことで、ブロックチェーンの健全性が保たれる。ブロックチェーンは、参加者間の仮想通貨の取引情報（トランザクション）がブロックと呼ばれる単位でまとめられたものである。ブロックチェーンは、Ｐ２Ｐ（Ｐｅｅｒ　Ｔｏ　Ｐｅｅｒ）ネットワークにおいて参加者が共有する一つの巨大な元帳として、機能する。

[0003] 非特許文献１によれば、ブロックチェーンでは、デジタル署名を図２のように使用し、署名の連鎖によりコインの取引情報を表現する。

[0004] ところでブロックチェーンの仕組みによるデジタル仮想通貨において、ネットワークに参加する一つの端末が代表して、ネットワーク内にブロードキャストされた取引データをまとめて承認して、その取引情報を含めたブロッ

クを生成し、他の端末に通知する。また、このプロセスに不正がないことを、システム全体、より具体的には、ブロックを生成する端末以外の複数の端末で検証する。ブロックを生成する端末は、ブロックの生成においてコストを必要とするものの、ブロックを生成した報酬として新規のコインを得ることが出来るため、ブロック生成の権利を得ようと参加者間では競争的プロセスが働く。

[0005] ここで、同時に複数の端末がブロックを生成すると、ブロックチェーンが分岐する可能性があるが、その後より長くブロックを伸ばしたチェーンが正式なチェーンとされる。即ち、最も生成コストをかけたブロックチェーンが、共有される唯一のブロックチェーンとして選ばれる。従って、攻撃者が改ざんや二重使用を行うためには、他のブロックチェーンよりも長くブロックをつながなければならないので、攻撃者はその分多くのコストをかける必要があり、攻撃が困難となる。

[0006] ブロックを生成する際に、参加者が提供するコストに関して、複数の手法が提案されている。例えば、Ｐｒｏｏｆ　ｏｆ　Ｗｏｒｋ　（ＰｏＷ）と呼ばれる手法や、Ｐｒｏｏｆ　ｏｆ　Ｓｔａｋｅ　（ＰｏＳ）と呼ばれる手法が提案されている。ＰｏＷでは、数学的な問題をいち早く解いた参加者がブロックを生成する。問題を解くために、参加者は計算機パワーをコストとして提供することとなる。一方で、ＰｏＷにおいて、報酬を得るためだけに問題を解くという非生産的であり、電力資源の浪費する問題がある。

[0007] このような問題を解決するために、ＰｏＷに代替する手法としてＰｏＳが提案されている。ＰｏＳは、数学的な条件に当てはまる参加者に、ブロックを生成する権利が与えられる。条件に当てはまるか否かを決める難易度は、参加者の所持するコインの貯蓄量に応じて調整されることが知られている（Kourosh Davarpanah , Dan Kaufman, Ophelie Pubellier “NeuCoin: the First Secure, Cost-efficient and Decentralized Cryptocurrency”、[online]、２０１５年６月１５日、２０１５年１０月２０日検索、インターネット＜URL: http://www.neucoin.org/en/whitepaper/download＞）。具体的には

、ＰｏＳでは、数学的な条件に当てはまる参加者に、ブロックを生成する権利（資格）が与えられる。条件の難易度は参加者のコインの所持量に応じて調整されるので、コインの貯蓄量が多いほどブロックが生成しやすい。具体的には、参加者のアドレスと前ブロックのハッシュ値と現在時刻を含めてハッシュ値を取り、そのハッシュ値がコインの貯蓄量に比例する値よりも小さくなる条件の時に、その参加者がブロックを生成する権利を持つ。条件の判定は現在時刻をパラメータに含めることにより、１秒に１回実施される。このようなＰｏＳにおいて、参加者は、大量のコインを保持するリスクをコストとして提供している。

[0008] 一方でブロックチェーンには、不正に支払いを行ったり過去の履歴を改ざんしたりするために、「５１％攻撃」と呼ばれる攻撃方法が存在する。この攻撃方法では、悪意のある攻撃者が全体のブロック生成速度の５１％以上を支配すると、正規のブロックの生成速度を上回るため、理論的には不正が成功すると考えられている。ブロック生成速度はＰｏＷやＰｏＳにおける提供リソースの大きさに比例している。例えばＰｏＷでは計算機パワーの５１％以上を、ＰｏＳでは全コイン量の５１％以上を独占することで、攻撃が実現すると考えられている。

先行技術文献

非特許文献

[0009] 非特許文献1：斉藤賢爾，ビットコイン－人間不在のデジタル巨石貨幣，WIDEテクニカルレポート

発明の概要

発明が解決しようとする課題

[0010] 昨今では、計算機パワーを集結させ組織的にブロック生成を行うマイニングプールや、ＡＳＩＣなどを用いたＰｏＷ専用の集積回路の登場を背景に、ＰｏＷにおいて、計算機リソースの５１％以上が独占されることが現実味を帯びてきている。

[0011] 一方、後継のアルゴリズムのＰｏＳでは、コイン資産の独占に要するコストが計算機リソースの独占よりもはるかに高コストであり、また攻撃によりコイン価格の暴落が予測される。従って、ＰｏＳでは、コストをかけて独占したコインの価値がなくなるリスクが大きいため、攻撃者が５１％攻撃を実施する動機が薄く、抑止力があると考えられていた。

[0012] ここで、ブロックチェーンは参加者全ての取引の内容を記録した一つの元帳であると捉えると、通貨以外の様々な取引に応用することが考えられる。例えば、複数者間で契約書を交わす際の証跡としてブロックチェーンを用いる方法が考えられる。契約書の内容をメタデータとして、コインの取引を絡めて、トランザクションのデータに含めて取引を行うことで、契約を交わした証跡をブロックチェーンに書き込むことが可能になる。

[0013] しかしながら、ブロックチェーンに契約の証跡を記録する方法において、ＰｏＳを採用した場合、問題が生じる場合がある。従来の仮想通貨のＰｏＳにおいては、攻撃者がコインの不正取引や履歴の改ざんを目的として攻撃を仕掛けると、その攻撃のためにむしろ独占したコインの価値が暴落するというリスクが攻撃の抑止力として働いていた。しかしながら、契約の証跡を記録する方法において、攻撃者の目的はコインの不正利用よりも、ブロックチェーンに書き込んだ契約の取り消しや内容の書き換えにあると考えられる。すなわちこのような方法においてＰｏＳを導入した場合、コインの価値を暴落させても、契約を取り消すことができれば、暴落で失ったコインの価値を上回る利益を得るといった状況が成り立つため、従来のような抑止力が働かず、攻撃の動機が生まれる可能性がある。

[0014] 従って本発明の目的は、より安全で信頼性の高いデジタル仮想通貨のブロックチェーンデータを生成可能な、ブロックチェーンデータを生成するブロックチェーン生成装置およびブロックチェーン生成方法、ブロックチェーンデータを検証するブロックチェーン検証装置およびブロックチェーン検証方法、ならびにプログラムを提供することである。

課題を解決するための手段

[0015] 上記課題を解決するために、本発明の第１の特徴は、複数のトランザクション生成装置によって生成されたトランザクションデータを含むブロックを連結したブロックチェーンデータに、新たなブロックを連結して、新たなブロックチェーンデータを生成するブロックチェーン生成装置に関する。本発明の第１の特徴に係るブロックチェーン生成装置は、ブロックチェーンデータと、ブロックチェーンデータに含まれていないトランザクションデータとを含む共有データを取得する同期手段と、ブロックチェーンデータにおいて複数のブロックを連結する資格の有無を判定する際に用いられる複数のパラメータ種別のブレンドパターンを特定するブロック承認方法データに基づいて、新たなブロックを連結する際に用いられるパラメータ種別を特定し、ブロックチェーンデータのトランザクションデータのうち、当該ブロックチェーン生成装置を用いる生成者の識別子に関連するトランザクションデータから、特定されたパラメータ種別の値を算出するパラメータ算出手段と、パラメータ算出手段が算出した値に基づいて、生成者が、新たなブロックチェーンデータを生成する資格を有しているか否かを判定するブロック生成条件確認手段と、ブロック生成条件確認手段が資格を有していると判定した場合、共有データを参照して、新たなブロックチェーンの生成を試みるブロックチェーン生成手段とを備える。ここでブロック承認方法データに含まれるブレンドパターンの識別子は、互いに相反する複数のパラメータ種別の組み合わせを特定する。

[0016] ブロック承認方法データは、第１のパラメータ種別を第１の数だけ繰り返した後、第１のパラメータ種別と相反する第２のパラメータ種別を第２の数だけ繰り返すブレンドパターンを特定しても良い。

[0017] ブロック承認方法データは、連続する所定の数のパラメータ種別の組み合わせにおいて、少なくとも、第１のパラメータ種別および第２のパラメータ種別をそれぞれ１つずつ含むブレンドパターンを特定しても良い。

[0018] ここで、所定の数は、所定のブロックについて完全な取引の完了が保証されるために必要なブロックの数であっても良い。

[0019] 本発明の第２の特徴は、複数のトランザクション生成装置によって生成されたトランザクションデータを含むブロックを連結したブロックチェーンデータに、新たなブロックを連結して、新たなブロックチェーンデータを生成するブロックチェーン生成方法に関する。本発明の第２の特徴に係るブロックチェーン生成方法は、コンピュータが、ブロックチェーンデータと、ブロックチェーンデータに含まれていないトランザクションデータとを含む共有データを取得するステップと、コンピュータが、ブロックチェーンデータにおいて複数のブロックを連結する資格の有無を判定する際に用いられる複数のパラメータ種別のブレンドパターンを特定するブロック承認方法データに基づいて、新たなブロックを連結する際に用いられるパラメータ種別を特定するステップと、コンピュータが、ブロックチェーンデータのトランザクションデータのうち、当該コンピュータを用いる生成者の識別子に関連するトランザクションデータから、特定されたパラメータ種別の値を算出するステップと、コンピュータが、算出するステップが算出した値に基づいて、生成者が、新たなブロックチェーンデータを生成する資格を有しているか否かを判定するステップと、コンピュータが、資格を有していると判定した場合、共有データを参照して、新たなブロックチェーンの生成を試みるステップとを備える。ここでブロック承認方法データに含まれるブレンドパターンの識別子は、互いに相反する複数のパラメータ種別の組み合わせを特定する。

[0020] 本発明の第３の特徴は、複数のトランザクション生成装置によって生成されたトランザクションデータを含むブロックを連結したブロックチェーンデータを検証するブロックチェーン検証装置に関する。本発明の第３の特徴に係るブロックチェーン検証装置は、ブロックチェーンデータを含む共有データを取得する同期手段と、ブロックチェーンデータにおいて複数のブロックを連結する資格の有無を判定する際に用いられる複数のパラメータ種別のブレンドパターンを特定するブロック承認方法データに基づいて、ブロックを連結する際に用いられるパラメータ種別を特定し、ブロックチェーンデータが、特定されたパラメータ種別に基づいて生成されているか否かを判定する

ブロック承認方法検証手段と、ブロックチェーンデータのトランザクションデータのうち、ブロックチェーンデータを生成した装置を用いる生成者の識別子に関連するトランザクションデータから、ブロック承認方法検証手段で特定されたパラメータ種別の値を算出するパラメータ算出手段と、パラメータ算出手段が算出した値に基づいて、生成者が、ブロックチェーンデータを生成する資格を有しているか否かを判定するブロック生成条件検証手段と、ブロック承認方法検証手段が、ブロックチェーンデータが特定されたパラメータ種別に基づいて生成されていると判定し、かつブロック生成条件検証手段が、生成者がブロックチェーンデータを生成する資格を有していると判定した場合、ブロックチェーンデータを承認するブロックチェーン検証手段とを備える。ここでブロック承認方法データに含まれるブレンドパターンの識別子は、互いに相反する複数のパラメータ種別の組み合わせを特定する。

[0021] 本発明の第４の特徴は、複数のトランザクション生成装置によって生成されたトランザクションデータを含むブロックを連結したブロックチェーンデータを検証するブロックチェーン検証方法に関する。本発明の第４の特徴に係るブロックチェーン検証方法は、コンピュータが、ブロックチェーンデータを含む共有データを取得するステップと、コンピュータが、ブロックチェーンデータにおいて複数のブロックを連結する資格の有無を判定する際に用いられる複数のパラメータ種別のブレンドパターンを特定するブロック承認方法データに基づいて、ブロックを連結する際に用いられるパラメータ種別を特定し、ブロックチェーンデータが、特定されたパラメータ種別に基づいて生成されているか否かを判定するステップと、コンピュータが、ブロックチェーンデータのトランザクションデータのうち、ブロックチェーンデータを生成した装置を用いる生成者の識別子に関連するトランザクションデータから、特定されたパラメータ種別の値を算出するステップと、コンピュータが、特定されたパラメータ種別の値に基づいて、生成者が、ブロックチェーンデータを生成する資格を有しているか否かを判定するステップと、コンピュータが、ブロックチェーンデータが特定されたパラメータ種別に基づいて

生成されていると判定し、かつ、生成者がブロックチェーンデータを生成する資格を有していると判定した場合、ブロックチェーンデータを承認するステップとを備える。ここでブロック承認方法データに含まれるブレンドパターンの識別子は、互いに相反する複数のパラメータ種別の組み合わせを特定する。

[0022] 本発明の第５の特徴は、コンピュータを、本発明の第１の特徴および第３の特徴に記載の各手段として機能させるためのプログラムに関する。

発明の効果

[0023] 本発明によれば、より安全で信頼性の高いデジタル仮想通貨のブロックチェーンデータを生成可能な、ブロックチェーンデータを生成するブロックチェーン生成装置およびブロックチェーン生成方法、ブロックチェーンデータを検証するブロックチェーン検証装置およびブロックチェーン検証方法、ならびにプログラムを提供することができる。

図面の簡単な説明

[0024] [図1]本発明の実施の形態に係る取引支援システムのシステム構成を説明する図である。

[図2]一般的な仮想通貨における署名を説明する図である。

[図3]一般的な仮想通貨におけるブロックチェーンを説明する図である。

[図4]本発明の実施の形態に係るトランザクション生成装置のハードウエア構成と機能ブロックを説明する図である。

[図5]本発明の実施の形態に係るブロックチェーン生成装置のハードウエア構成と機能ブロックを説明する図である。

[図6]本発明の実施の形態に係るブロックチェーン生成装置によるブロックチェーン生成処理を説明するフローチャートである。

[図7]本発明の実施の形態に係るブロックチェーン検証装置のハードウエア構成と機能ブロックを説明する図である。

[図8]本発明の実施の形態に係るブロックチェーン検証装置によるブロックチェーン検証処理を説明するフローチャートである。

[図9]本発明の実施の形態に係る取引支援システムにおいて用いられるブロック承認方法データのブレンドパターンの一例を説明する図である。

[図10]本発明の実施の形態に係る取引支援システムにおける、取引パターン量の算出の一例を説明する図である。

[図11]本発明の実施の形態に係る取引支援システムにおける、取引パターン量算出手段による取引パターン量算出処理を説明するフローチャートである。

発明を実施するための形態

[0025] 次に、図面を参照して、本発明の実施の形態を説明する。以下の図面の記載において、同一または類似の部分には同一または類似の符号を付している。

[0026] （取引支援システム）

図１を参照して、本発明の実施の形態に係る取引支援システム５を説明する。取引支援システム５は、複数のコンピュータを備え、各コンピュータは、各コンピュータに設けられた通信制御装置およびＰ２Ｐネットワーク４を介して、自律分散的に接続されている。なお、図１に示す取引支援システム５において接続されるコンピュータの数は、一例であって、これに限るものではない。

[0027] 取引支援システム５を構成する各コンピュータに、デジタル仮想通貨における取引を実現するためのプログラムがインストールされる。各コンピュータは、それぞれ、Ｐ２Ｐネットワーク４を介して、ブロックチェーンデータとトランザクションデータを取得し、ネットワークに参加する端末群全体が、不正を監視し、唯一のブロックチェーンを共有する。

[0028] 各コンピュータは、取引支援システム５における各場面における役割に応じて、ブロックチェーン生成装置１として機能したり、ブロックチェーン検証装置２として機能したり、トランザクション生成装置３として機能したりする。

[0029] 本発明の実施の形態において、取引支援システム５における仮想通貨を利

用する者を、「参加者」と記載する。ブロックチェーン生成装置を用いる参加者を、「生成者」と記載する。

[0030] ブロックチェーン生成装置１は、所定の条件を満たした場合、複数のトランザクション生成装置３によって生成されたトランザクションデータを含むブロックを連結した既存のブロックチェーンデータに、新たなブロックを連結して、新たなブロックチェーンデータを生成する。新たなブロックは、既存のブロックチェーンの生成後に発生したトランザクションのデータを含む。ブロックチェーン生成装置１が生成した新たなブロックチェーンデータは、Ｐ２Ｐネットワーク４を介して、他の端末に共有される。

[0031] ブロックチェーン検証装置２は、ブロックチェーン生成装置１が生成したブロックチェーンデータを検証する。ブロックチェーン検証装置２は、複数のトランザクション生成装置３によって生成されたトランザクションデータを含むブロックを連結したブロックチェーンデータを検証する。ブロックチェーン検証装置２が検証した結果は、Ｐ２Ｐネットワーク４を介して、他の端末に共有される。

[0032] 本発明の実施の形態に係る取引支援システム５において、所定のブロックの完全な取引の完了には、所定のブロックが連結され承認された後に一定数のブロックが続き、これらの各ブロックが連結され検証されることを要する。例えば、あるブロックＡが承認されブロックチェーンに連結された後、５つの連続するブロックが認証され連結された場合、すなわち、６個の連続するブロックが認証され連結された場合、この６個の先頭ブロックであるブロックＡについて完全に取引が終了したと見なされる。ここで、完全な取引終了が認められるブロック数「６」は、「承認ブロック数」と称される。これは、攻撃の成功確率はブロック差が拡がるほど指数関数的に下がることが証明されていることに基づく（Satoshi Nakamoto, “Bitocoin: A Peer-to-Peer Electronic Cash System,”、[online]、２００８年、２０１５年１０月２０日検索、インターネット＜URL: https://bitcoin.org/bitcoin.pdf＞）。最終的に攻撃によって作られたチェ

ーンがネットワークに受け入れられるためには、正規のチェーンの長さを追い抜く必要があり、攻撃者がブロックを生成している間にも、正規のチェーンの長さは伸びていくため、攻撃者はシステムにおける過半数以上（すなわち正規のチェーン以上）のブロック生成速度がなければ差を縮めることができないからである。

[0033] トランザクション生成装置３は、仮想通貨や契約などの取引によって、各ブロックに含まれるトランザクションデータを生成する。トランザクション生成装置３が生成したトランザクションデータは、Ｐ２Ｐネットワーク４を介して、他の端末に共有される。

[0034] 図２を参照して、本発明の実施の形態における取引支援システム５において、第２の参加者が、第３の参加者にコインを支払う場合の取引（トランザクション）を説明する。トランザクション生成装置３は、最新のトランザクション（第１のトランザクションＴ１）のデータと第３の参加者の公開鍵を合わせたデータに対して暗号学的ハッシュ関数を適用し、第２の参加者の秘密鍵を用いて署名を施して、第２のトランザクションＴ２のデータを生成する。コインを受け取る第３の参加者は、そのひとつ手前の取引（第１のトランザクションＴ１）における受け手（第２の参加者）の公開鍵を用いて、第２のトランザクションＴ２の署名を検証するとともに、ハッシュ値を再計算することで、コインが正当な所有者から渡されたことを確かめる。また各トランザクションのデータには、取引された仮想通貨の値などのトランザクションの内容や、トランザクションを生成する参加者の公開鍵に対応するアドレスが含まれる。

[0035] 図２に示すように生成された複数のトランザクションのデータは、所定条件下で、図３に示すように、ブロックチェーン生成装置１によってブロックにまとめられ、既存のブロックチェーンに連結され、各コンピュータで共有される。このとき、ブロックチェーン生成装置１は、新たなブロック（第ｎ＋１のブロック）を生成する際、ブロックチェーンに含まれていないトランザクションのデータを収集し、新たなブロック（第ｎ＋１のブロック）に、

収集したトランザクションのデータと、現在のブロックチェーンの末尾のブロック（第ｎのブロック）のハッシュ値（２５６ビット）を含める。さらに現在生成中のブロック（第ｎ＋１のブロック）に対して、暗号学的ハッシュ関数（ＳＨＡ－２５６）を適用した場合のハッシュ値の先頭のｋビットがすべて“０”になるように、ブロックチェーン生成装置１は、現在生成中のブロック（第ｎ＋１のブロック）に含める適切値を探索する。適切値が見つかると、その適切値を含むブロック（第ｎ＋１のブロック）を、現在のブロックチェーンの末尾に連結して、ブロードキャストする。ここで、適切値の算出条件となる「ｋビット」のｋの数値を変更することにより、適切値を求める難易度が適宜決定される。

[0036] その後、ブロックチェーン検証装置２は、ブロックチェーン生成装置１から送信されたブロックチェーンデータを検証し、その検証結果を他の端末と共有する。

[0037] （トランザクション生成装置）

図４を参照して、トランザクション生成装置３を説明する。トランザクション生成装置３は、記憶装置３１０、処理装置３２０および通信制御装置３３０を備える一般的なコンピュータである。一般的なコンピュータが所定の機能を実現するためのプログラムを実行することによって、トランザクション生成装置３は、図４に示す各機能を実現する。

[0038] 記憶装置３１０は、共有データ３１１を記憶する。共有データ３１１は、ブロックチェーンデータ３１２と、ブロックチェーンに含まれていないトランザクションデータ３１３とを含む。共有データ３１１は、図１に示す取引支援システム５において共有されるデータである。

[0039] 処理装置３２０は、同期手段３２１およびトランザクション生成手段３２２を備える。

[0040] 同期手段３２１は、Ｐ２Ｐネットワーク４を介して、ブロックチェーンデータ３１２と、ブロックチェーンに含まれていないトランザクションデータ３１３とを含む共有データ３１１を取得する。同期手段３２１は、Ｐ２Ｐネ

ットワーク４を介して他の装置と通信して共有データ３１１を取得し、最新のデータに同期して共有する。

[0041] 同期手段３２１はさらに、当該コンピュータ内でブロックチェーンデータ３１２やトランザクションデータ３１３が更新された場合、Ｐ２Ｐネットワーク４を介して、他の装置に更新後のデータをブロードキャストする。これにより、当該コンピュータ内で生成された最新のデータが、他のコンピュータとの間で共有される。

[0042] トランザクション生成手段３２２は、仮想通貨や契約に関するトランザクションを遂行し、このトランザクションに関するトランザクションデータを生成する。生成されたトランザクションデータは、Ｐ２Ｐネットワーク４を介して他のコンピュータにも送信され、共有される。

[0043] （ブロックチェーン生成装置）

図５を参照して、ブロックチェーン生成装置１を説明する。ブロックチェーン生成装置１は、記憶装置１１０、処理装置１２０および通信制御装置１３０を備える一般的なコンピュータである。一般的なコンピュータが所定の機能を実現するためのプログラムを実行することによって、ブロックチェーン生成装置１は、図４に示す各機能を実現する。

[0044] 記憶装置１１０は、共有データ１１１、ブロック承認方法データ１１４およびパラメータデータ１１５を記憶する。共有データ１１１は、図４を参照して説明したトランザクション生成装置３の共有データ３１１と同様であって、ブロックチェーンデータ１１２およびトランザクションデータ１１３を含む。

[0045] ブロック承認方法データ１１４は、ブロックチェーンデータ１１２において複数のブロックを連結する資格の有無を判定する際に用いられる複数のパラメータ種別のブレンドパターンを特定する。ブロック承認方法データ１１４は、ブロックチェーンデータ１１２において連続する複数のブロックのそれぞれと、各ブロックの連結に用いられるパラメータ種別を対応づけることを可能とする。本発明の実施の形態において、ブロック承認方法データで特

定される複数のパラメータ種別は、互いに相反する。

[0046] ブロック承認方法データ１１４は、例えば、本発明の実施の形態に係るブロックチェーン生成装置１およびブロックチェーン検証装置２を実現するために用いられるプログラムに記載されるなどにより、ブロックチェーン生成装置１およびブロックチェーン検証装置２間で共有される。

[0047] 本発明の実施の形態において、ブロックを生成し連結する際のブロックチェーン生成装置１における生成者の資格の有無は、単一のパラメータ種別によって判定されるものではなく、複数のパラメータ種別のいずれかによって判定されるのが好ましい。本発明の実施の形態において、連続するブロックにおける各ブロックの承認方法は、複数のパラメータ種別がブレンドされており、ブロック承認方法データ１１４は、各ブロックを生成する際に、いずれのパラメータ種別を用いるかを特定する。

[0048] 本発明の実施の形態において、複数のブロックの承認方法で用いられる「複数のパラメータ種別」は、相反するパラメータ種別である。「相反するパラメータ種別」は、片方のリソースを独占したとしても、もう片方のリソースの独占に影響を及ぼさない関係を有するパラメータ種別である。例えば、「コインの貯蓄量」と「コインの消費量」は、両方の条件を満たすことは困難であるので、相反するパラメータ種別となる。

[0049] またＰｏＷとＰｏＳについて、ＰｏＷが外的リソースに関するパラメータであるのに対し、ＰｏＳが内的リソースに関するパラメータである。従って、ＰｏＷとＰｏＳは、一人のブロック生成者が両方の条件を満たすことは困難であり、相反するパラメータ種別となる。

[0050] なお、本発明の実施の形態において、相反するパラメータ種別が２種類である場合を説明したが、３種類のパラメータ種別間で、互いに相反する関係が成り立つ場合、相反するパラメータ種別が３種類であっても良い。

[0051] また本発明の実施の形態において、相反するパラメータ種別として、「コインの貯蓄量」と「取引経路パターンの量」が考えられる。「取引経路パターンの量」は、コインを使用することによって、生成者が、どれだけ多様な

取引を行ったかを示す指標である。これに対し「コインの貯蓄量」はコインを保有することによって得られる。従って、「コインの貯蓄量」と「取引経路パターンの量」は、コインの保有と使用の相反する性質を有するので、一人のブロック生成者がこれらの二つのパラメータを同時に独占することは難しい。従って、「コインの貯蓄量」と「取引経路パターンの量」の各パラメータ種別は、相反する。

[0052] ブロック承認方法データ１１４の具体例は、後に詳述される。

[0053] パラメータデータ１１５は、ブロックチェーン生成装置１が新たに生成するブロックを承認するためのパラメータ種別の値が設定される。パラメータデータ１１５は、パラメータ算出手段１２２により算出され、記憶装置１１０に記憶される。

[0054] 処理装置１２０は、同期手段１２１、パラメータ算出手段１２２、ブロック生成条件確認手段１２５およびブロックチェーン生成手段１２６を備える。同期手段１２１は、図４を参照して説明したトランザクション生成装置３の同期手段３２１と同様である。

[0055] パラメータ算出手段１２２は、ブロックチェーンデータ１１２およびブロック承認方法データ１１４に基づいて、新たなブロックを連結する際に用いられるパラメータ種別を特定する。パラメータ算出手段１２２は、ブロック承認方法データ１１４を参照して、ブロックチェーンデータ１１２における各ブロックの承認方法および新たに連結するブロックの承認方法が、ブロック承認方法データ１１４で特定されるブレンドパターンにあうように、新たに連結するブロックの承認方法（パラメータ種別）を特定する。このときパラメータ算出手段１２２は、既に連結されたブロックのうち、新たにブロックを連結する際にパラメータ種別を特定することが必要な各ブロックの所定ビットのデータを参酌して、各ブロックの連結時に用いられたパラメータ種別を特定する。

[0056] パラメータ算出手段１２２は、さらに、ブロックチェーンデータ１１２のトランザクションデータのうち、当該ブロックチェーン生成装置１を用いる

生成者の識別子に関連するトランザクションデータから、特定されたパラメータ種別の値を算出する。

[0057] パラメータ算出手段１２２において、ブロックを新たに追加する生成者の資格の承認に用いるパラメータ種別を特定する方法は、後に詳述される。

[0058] ここでパラメータ算出手段１２２は、ブレンドパターンで特定される各パラメータ種別について算出するための各算出手段を有する。例えば、ブロック承認方法データ１１４のブレンドパターンが、相反するパラメータ種別として、コイン貯蓄量と取引パターン量を設定する場合、パラメータ算出手段１２２は、コイン貯蓄量を算出するコイン貯蓄量算出手段１２３と、取引パターン量算出手段１２４を備える。ブロック承認方法データ１１４のブレンドパターンが指定するパラメータ種別によっては、他のパラメータ種別を算出するための算出手段を備えても良い。

[0059] ブロック生成条件確認手段１２５は、パラメータ算出手段１２２が算出した値に基づいて、新たなブロックチェーンの生成者が、新たなブロックチェーンデータを生成する資格を有しているか否かを判定する。パラメータ算出手段１２２が、コインの貯蓄量、コインの消費量、ＰｏW、ＰｏＳなどの一般的なパラメータ種別の値を算出した場合、ブロック生成条件確認手段１２５は、一般的な方法で、新たなブロックチェーンデータを生成する資格を有しているか否かを判定する。

[0060] ここで、取引パターン量算出手段１２４の処理や、取引パターン量に基づいて新たなブロックチェーンデータを生成する資格を有しているか否かを判定する処理は、後に詳述される。

[0061] ブロックチェーン生成手段１２６は、ブロック生成条件確認手段１２５が資格を有していると判定した場合、共有データ１１１を参照して、新たなブロックチェーンの生成を試みる。具体的には、ブロックチェーン生成手段１２６は、パラメータデータ１１５で設定された値を用いて、図３に示す「適切値」の探索を試みる。適切値が見つかった場合、その適切値を用いて新たなブロックを生成する。このときブロックチェーン生成手段１２６は、生成

した新たなブロックの所定ビットに、このブロックを生成する際に用いられたパラメータ種別の識別子を設定する。ブロックチェーン生成手段１２６は、既存のブロックチェーンデータ１１２の末尾に、生成した新たなブロックを連結して、新たなブロックチェーンデータを生成し、共有データ１１１を更新する。新たなブロックチェーンの生成に成功した場合、他の端末と共有するために、新たなブロックチェーンのデータは、Ｐ２Ｐネットワークにブロードキャストされる。

[0062] ブロックチェーン生成手段１２６が、適切値を探索している間に、他の装置によってブロックが生成され新たなブロックチェーンが共有される場合もある。この場合、ブロックチェーン生成手段１２６は、古いブロックチェーンにおける適切値の探索を中止し、新たに共有されたブロックチェーンについて、適切値の探索を繰り返す。

[0063] 図６を参照して、ブロックチェーン生成装置１によるブロックチェーン生成方法を説明する。

[0064] まずステップＳ１０１においてブロックチェーン生成装置１は、ブロック承認方法データ１１４を参照して、新たにブロックを生成する際の承認に用いるパラメータ種別を特定する。ステップＳ１０２においてブロックチェーン生成装置１は、共有データ１１１を参照して、ステップＳ１０１で特定されたパラメータ種別に対応する値を算出する。

[0065] ステップＳ１０３においてブロックチェーン生成装置１は、ステップＳ１０２で算出された値に基づいて、当該ブロックチェーン生成装置１の生成者がブロックを生成する資格を有しているか否かを判定する。ブロックの生成資格がないと判定された場合、そのまま処理を終了する。

[0066] 一方、ステップＳ１０３においてブロックの生成資格があると判定された場合、ステップＳ１０４においてブロックチェーン生成装置１は、ステップＳ１０３で算出されたパラメータに基づいて、適切値の算出を開始する。適切値の算出に成功した場合、ブロックチェーン生成装置１は、算出した適切値を用いて、新たなブロックを生成し、既存のブロックチェーンに連結した

新たなブロックチェーンデータを記憶する。

[0067] （ブロックチェーン検証装置）

図７を参照して、ブロックチェーン検証装置２を説明する。ブロックチェーン検証装置２は、記憶装置２１０、処理装置２２０および通信制御装置２３０を備える一般的なコンピュータである。一般的なコンピュータが所定の機能を実現するためのプログラムを実行することによって、ブロックチェーン生成装置１は、図４に示す各機能を実現する。

[0068] 記憶装置２１０は、共有データ２１１、ブロック承認方法データ２１４およびパラメータデータ２１５を記憶する。共有データ２１１は、図４を参照して説明したトランザクション生成装置３の共有データ３１１と同様であって、ブロックチェーンデータ２１２およびトランザクションデータ２１３を含む。なお、ブロックチェーン検証装置２は、既存のブロックチェーンデータ２１２を検証するものであるので、トランザクションデータ２１３の有無は問わない。

[0069] ブロック承認方法データ２１４およびパラメータデータ２１５は、図５を参照して説明したブロック承認方法データ１１４およびパラメータデータ１１５と同様である。

[0070] 処理装置２２０は、同期手段２２１、ブロック承認方法検証手段２２２、パラメータ算出手段２２３、ブロック生成条件検証手段２２６およびブロックチェーン検証手段２２７を備える。同期手段２２１は、図４を参照して説明したトランザクション生成装置３の同期手段３２１と同様である。

[0071] ブロック承認方法検証手段２２２は、ブロック承認方法データ２１４に基づいて、ブロックを連結する際に用いられるパラメータ種別を特定し、ブロックチェーンデータ２１２が、特定されたパラメータ種別に基づいて生成されているか否かを判定する。ブロック承認方法検証手段２２２は、ブロックチェーンデータ２１２における各ブロックの承認方法が、ブロック承認方法データ２１４で特定されるブレンドパターンに適合するか否かを判定する。このときブロック承認方法検証手段２２２は、検証対象のブロックチェーン

データ２１２において、ブレンドパターンの適合性を確認するために必要な各ブロックの所定ビットのデータを参酌して、各ブロックの連結時に用いられたパラメータ種別を特定する。

[0072] ブロックチェーンデータ２１２のブロックの生成に用いるパラメータ種別が、ブロック承認方法データ２１４で特定されるパラメータ種別であるか否かを判定する処理は、後に詳述される。

[0073] パラメータ算出手段２２３は、ブロックチェーンデータ２１２のトランザクションデータのうち、ブロックチェーンデータ２１２を生成した装置を用いる生成者の識別子に関連するトランザクションデータから、ブロック承認方法検証手段２２２で特定されたパラメータ種別の値を算出する。算出した値は、パラメータデータ２１５として記憶装置２１０に記憶される。

[0074] パラメータ算出手段２２３は、図５を参照して説明したブロックチェーン生成装置１のパラメータ算出手段１２２と同様に、コイン貯蓄量算出手段２２４、取引パターン量算出手段２２５などの、各パラメータ種別の値を算出するための算出手段を備える。

[0075] ブロック生成条件検証手段２２６は、パラメータ算出手段２２３が算出した値に基づいて、ブロックチェーンの生成者が、ブロックチェーンデータ２１２を生成する資格を有しているか否かを判定する。

[0076] パラメータ算出手段２２３が、コインの貯蓄量、コインの消費量、ＰｏＷ、ＰｏＳなどの一般的なパラメータ種別の値を算出した場合、ブロック生成条件検証手段２２６は、一般的な方法で、新たなブロックチェーンデータを生成する資格を有しているか否かを判定する。

[0077] ここで、取引パターン量算出手段２２５の処理や、取引パターン量に基づいて新たなブロックチェーンデータを生成する資格を有しているか否かを判定する処理は、後に詳述される。

[0078] ブロックチェーン検証手段２２７は、ブロック承認方法検証手段２２２、ブロック生成条件検証手段２２６の結果に基づいて、ブロックを検証する。具体的にはブロックチェーン検証手段２２７は、ブロック承認方法検証手段

２２２が、ブロックチェーンデータ２１２が特定されたパラメータ種別に基づいて生成されていると判定し、かつブロック生成条件検証手段２２６が、生成者がブロックチェーンデータ２１２を生成する資格を有していると判定した場合、ブロックチェーンデータ２１２を承認する。ブロックチェーン検証手段２２７は、検証結果を他の端末に通達する。ここで承認されなかった旨の検証結果を受けた端末は、不正なブロックチェーンとして、周囲の端末に通達するなどの処理を行う。

[0079] 図８を参照して、ブロックチェーン検証装置２によるブロックチェーン検証方法を説明する。

[0080] まずステップＳ２０１においてブロックチェーン検証装置２は、ブロック承認方法データ２１４を参照して、新たにブロックを生成する際に用いるパラメータ種別を特定する。

ステップＳ２０２においてブロックチェーン検証装置２は、ブロックチェーンデータ２１２におけるブロックが、ステップＳ２０１で特定されたパラメータ種別で承認されているか否かを判定する。特定されたパラメータ種別で承認されていないと判定された場合、ステップＳ２０６においてブロックチェーン検証装置２は、当該ブロックチェーンデータを承認しないことを決定する。

[0081] 一方、特定されたパラメータ種別で承認されていると判定された場合、ステップＳ２０３においてブロックチェーン検証装置２は、共有データ１１１を参照して、ステップＳ２０１で特定されたパラメータ種別に対応する値を算出する。

[0082] ステップＳ２０４においてブロックチェーン生成装置１は、ステップＳ２０３で算出された値に基づいて、ブロックチェーンデータ２１２のブロックが生成された端末の生成者がブロックを生成する資格を有しているか否かを判定する。ブロックの生成資格がないと判定された場合、ステップＳ２０６においてブロックチェーン検証装置２は、当該ブロックチェーンデータを承認しないことを決定する。

[0083] 一方、ブロックの生成資格があると判定された場合、ステップＳ２０５においてブロックチェーン検証装置２は、当該ブロックチェーンデータを承認することを決定する。さらにステップＳ２０７においてブロックチェーン検証装置２は、検証結果を他の端末に通知する。

[0084] （ブレンドパターン）

ブロックチェーン生成装置１が参照するブロック承認方法データ１１４と、ブロックチェーン検証装置２が参照するブロック承認方法データ２１４は、同様のデータである。このブロック承認方法データは、例えば、図６に示すいずれかの承認方法のブレンドパターンを特定する。

[0085] 図９に示す例における四角の連結は、ブロックチェーンデータにおいて連続するブロックの連結を表している。白抜きの四角は、各ブロックを生成し連結される際に用いられるパラメータ種別が、「第１のパラメータ種別」であることを示し、斜線ハッチの四角は、「第２のパラメータ種別」であることを示す。ここで、第１のパラメータ種別と第２のパラメータ種別は、互いに相反する関係を有する。

[0086] 図９を参照して、ブロック承認方法データ１１４が特定するブレンドパターンについて詳述する。図９に示す各ブレンドパターンの例は、下記に大別される。

ブレンドパターンＡ：第１のパラメータ種別を第１の数だけ繰り返した後、第２のパラメータ種別を第２の数だけ繰り返す（図９（ａ）ないし（ｃ））

ブレンドパターンＢ：連続する所定の数のパラメータ種別の繰り返しにおいて、少なくとも、第１のパラメータ種別および第２のパラメータ種別をそれぞれ１つずつ含む（図９（ｄ）および（ｅ））

[0087] 図９（ａ）のブレンドパターンは、第１のパラメータ種別を第１の数（１）だけ繰り返した後、第２のパラメータ種別を第２の数（１）だけ繰り返す。この場合、ブロック承認方法データ１１４に、図９（ａ）のブレンドパターンの識別子を含む。ブロックチェーンにおける各ブロックは、第１のパラメータ種別による承認と第２のパラメータ種別による承認を交互に繰り返し

ながら、それぞれの新たなブロックが生成されブロックチェーンに連結される。

[0088] 図９（ａ）に示すブロック承認方法が設定された場合、ブロックチェーン生成装置１は、最後尾のブロックの生成で用いられたパラメータ種別とは異なるパラメータ種別を用いて、ブロックの生成資格の有無を判定する。またブロックチェーン検証装置２は、直近の２個のブロックが、図９（ａ）のブレンドパターンに一致する場合、最後尾のブロックが、ブロック承認方法データ２１４に基づいて承認されていると判定する。

[0089] 図９（ｂ）のブレンドパターンは、第１のパラメータ種別を第１の数（Ｎ＝３）だけ繰り返した後、第２のパラメータ種別を第２の数（１）だけ繰り返す。この場合、ブロック承認方法データ１１４に、図９（ｂ）のブレンドパターンの識別子のほか、第１の数（Ｎ）も含む。ブロックチェーンにおける各ブロックは、第１のパラメータ種別による承認をＮ回繰り返した後、第２のパラメータ種別による承認を経て、それぞれ新たなブロックが生成されブロックチェーンに連結される。

[0090] 図９（ｂ）に示すブロック承認方法が設定された場合、ブロックチェーン生成装置１は、直近のＮ個のブロックの生成で用いられたパラメータ種別が、全て第１のパラメータ種別の場合、新たなブロックの生成において、第２のパラメータ種別を用いる。ブロックチェーン生成装置１は、それ以外の場合、すなわち最後尾のブロックの生成で用いられたパラメータ種別が、第２のパラメータ種別の場合、または、直近のＮ個のブロックの生成で用いられたパラメータ種別に第２のパラメータ種別が含まれる場合、新たなブロックの生成において、第１のパラメータ種別を用いる。またブロックチェーン検証装置２は、直近のＮ＋１個のブロックが、図９（ｂ）のブレンドパターンに一致する場合、最後尾のブロックがブロック承認方法データ２１４に基づいて承認されていると判定する。

[0091] 図９（ｃ）のブレンドパターンは、第１のパラメータ種別を第１の数（Ｎ＝３）だけ繰り返した後、第２のパラメータ種別を第２の数（Ｍ＝２）だけ

繰り返す。この場合、ブロック承認方法データ１１４に、図９（ｃ）のブレンドパターンの識別子のほか、第１の数（Ｎ）および第２の数（Ｍ）も含む。ブロックチェーンにおける各ブロックは、第１のパラメータ種別による承認をＮ回繰り返した後、第２のパラメータ種別による承認をＭ回繰り返して、それぞれ新たなブロックが生成されブロックチェーンに連結される。

[0092] 図９（ｃ）に示すブロック承認方法が設定された場合、ブロックチェーン生成装置１は、直近のＭ個のブロックの生成で用いられたパラメータ種別が、全て第２のパラメータ種別の場合、新たなブロックの生成において、第１のパラメータ種別を用いる。ブロックチェーン生成装置１は、直近のＮ個のブロックの生成で用いられたパラメータ種別が、全て第１のパラメータ種別の場合、新たなブロックの生成において、第２のパラメータ種別を用いる。それ以外の場合、ブロックチェーン生成装置１は、直近のブロックの生成で用いられたパラメータ種別を用いる。またブロックチェーン検証装置２は、直近のＮ＋Ｍ個のブロックが、図９（ｃ）のブレンドパターンに一致する場合、最後尾のブロックがブロック承認方法データ２１４に基づいて承認されていると判定する。

[0093] 図９（ｄ）のブレンドパターンは、連続する所定の数（Ｎ＝６）のパラメータ種別の繰り返しにおいて、少なくとも、第１のパラメータ種別および第２のパラメータ種別をそれぞれ１つずつ含む。この場合、ブロック承認方法データ１１４に、図９（ｄ）のブレンドパターンの識別子のほか、所定の数（Ｎ）も含む。ブロックチェーンにおける各ブロックは、直近のＮ－１個の各ブロックの生成時に用いられたパラメータ種別を参酌してパラメータ種別が決定され、決定されたパラメータ種別で生成された新たなブロックがブロックチェーンに連結される。

[0094] 図９（ｄ）に示すブロック承認方法が設定された場合、ブロックチェーン生成装置１は、直近のＮ－１個のブロックの生成で用いられたパラメータ種別が、全て第１のパラメータ種別の場合、新たなブロックの生成において、第２のパラメータ種別を用いる。ブロックチェーン生成装置１は、直近のＮ

－１個のブロックの生成で用いられたパラメータ種別が、全て第２のパラメータ種別の場合、新たなブロックの生成において、第１のパラメータ種別を用いる。それ以外の場合、ブロックチェーン生成装置１は、乱数による抽選などの所定のアルゴリズムに基づいて、第１のパラメータ種別および第２のパラメータ種別のうちのいずれかを選択して、選択したパラメータ種別で、新たなブロックの生成しブロックチェーンに連結する。またブロックチェーン検証装置２は、直近のＮ個のブロックにおいて、相反するパラメータ種別を少なくとも一つずつ含む場合、最後尾のブロックがブロック承認方法データ２１４に基づいて承認されていると判定する。

[0095] 図９（ｅ）は、図９（ｄ）に示す例の変形例であって、連続する所定の数（Ｎ）に、承認ブロック数を設定する方法である。承認ブロック数は、あるブロックの完全な取引終了が認められるための、連続するブロックの生成数である。すなわち、あるブロックＡが生成され連結された後、５個のブロックがそれぞれ連結された際にブロックＡについて完全な取引終了が認められる場合、承認ブロック数は「６」となる。連続する所定の数（Ｎ）に、承認ブロック数を設定する場合、ブロックＡが完全に取引終了したと認められるために、互いに相反する複数のパラメータ種別による承認が必ずブレンドされていることが保証されるので、悪意のある参加者による攻撃をさらに適切に回避することができる。

[0096] なお、ブロックチェーンデータ１１２における各ブロックを生成する際に用いられたパラメータ種別は、ブロックチェーン内の各ブロックにおいて特定されることが好ましい。例えば、ブロック内の所定ビットに、このブロックを生成する際に用いられたパラメータ種別の識別子が設定される。ブロックチェーン生成装置１は、既に連結されたブロックのうち、新たにブロックを連結する際にパラメータ種別を特定することが必要な各ブロックの所定ビットのデータを参酌して、各ブロックの連結時に用いられたパラメータ種別を特定する。ここで、「新たにブロックを連結する際にパラメータ種別を特定することが必要な各ブロック」は、ブロック承認方法データにおいて指定

されるブレンドパターンの識別子やＮ、Ｍなどの設定情報などによって異なる。またブロックチェーン検証装置２は、検証対象のブロックチェーンデータ２１２において、ブレンドパターンの適合性を確認するために必要な各ブロックの所定ビットのデータを参酌して、各ブロックの連結時に用いられたパラメータ種別を特定して、ブレンドパターンに適合しているか否かを判定する。ここで、「ブレンドパターンの適合性を確認するために必要な各ブロック」は、ブロック承認方法データにおいて指定されるブレンドパターンの識別子やＮ、Ｍなどの設定情報などによって異なる。

[0097] （取引パターン量算出手段）

図５のブロックチェーン生成装置１の取引パターン量算出手段１２４および図６のブロックチェーン検証装置２の取引パターン量算出手段２２５を説明する。

[0098] 取引パターン量算出手段１２４（取引パターン量算出手段２２５）は、ブロックチェーンデータ１１２のトランザクションデータのうち、ブロックチェーン生成装置１を用いる生成者の識別子に関連するトランザクションデータから、生成者の取引パターン量を算出する。ここで、「取引パターン量」は、生成者の信用の指標である。

[0099] 取引パターン量は、取引は互いに素性を明らかにし、相手がどういった人物であるかを把握した上で相手を信用して取引することに着目して算出された、信用スコアに相当する。多様なノードと取引を行った参加者は、多くのノードから信用を受けて取引していると推定され、その信用の大きい承認者が５１％攻撃を実施すれば、その人物は特定され社会的にも信用を失うこととなる。従ってこのような参加者は、信用の暴落が攻撃の抑止力となると考えられる。「取引経路パターンの量」は、ブロックチェーンデータ１１２を参照して、どれだけ多様なノードと取引を行ったのかをスコアリングすることで得られる。また「取引経路パターンの量」は、取引においてコインを使用することにより得られる値であるので、「コインの貯蓄量」に相反するパラメータ種別として採用される。

[0100] ここで、「取引」は、トランザクション生成装置３が生成するトランザクションデータによって特定され、仮想通貨の譲渡はもちろん、複数者間で契約書を交わす際の証跡としてブロックチェーンを応用する場合の契約も含まれる。証跡としてのブロックチェーンを応用する際の契約は、物品や役務等の売買契約、譲渡、申込書、使用許諾などを指し、二者間以上の個人または機関において交わされる。

[0101] ＰｏＳの場合、「コインの貯蓄量」がコストになる。従って、ブロックチェーンで証跡が残された契約の価値が、ブロックの生成者のコインの貯蓄量以上の価値がある状況において、ＰｏＳでブロックを生成する生成者が承認される場合、コストの貯蓄量を無駄にしても攻撃を挑む動機付けが生じる。そこで本発明の実施の形態において、取引経路パターンの量を、ブロックを生成する生成者を承認するためのパラメータ種別として採用する。これにより、取引パターンの量を増加させるためには、コインを使用して多様な取引を行なって信用を得なければならないので、このような信用を得たブロックの生成者が、攻撃することの抑止力につながる。

[0102] 図１０を参照して、本発明の実施の形態に係る取引パターン量を説明する。図１０（ａ）に示すように、ある参加者が過去に発行した経路パターンの集合をａとし、このａに含まれる経路パターンｐに含まれるノード数をｎｐ，ａとする場合、ａの全ての経路パターのノー度数の和（取引パターン量：スコア）は、式（１）で表現される。

[0103] この場合、取引パターン量は、ブロックの生成者（ブロックチェーン生成装置１を用いる生成者）の識別子に関連するトランザクションデータにおける、取引相手の識別子の各組み合わせにおける、取引相手の識別子の合計である。具体的には、図１０（ｂ）に示すように、参加者Ａが過去に、Ｂのみを相手とする取引と、Ｃのみを相手とする取引と、ＢおよびＣのみを相手とする取引を行った場合を考える。各取引におけるノード数（取引相手の識別子の合計）は、それぞれ、１、１、２であるので、この場合の取引パターン量は、「４」となる。

[0104] また他の方法として、取引パターン量が、ブロックの生成者の識別子に関連するトランザクションデータにおける、取引相手の識別子のユニーク数であっても良い。具体的には、図１０（ｂ）に示すように、参加者Ａが過去に、Ｂのみを相手とする取引と、Ｃのみを相手とする取引と、ＢおよびＣのみを相手とする取引を行った場合、参加者Ａの取引相手は、Ａ、ＢおよびＣであるので、この場合の取引パターン量は、「３」となる。

[0105] なお、取引パターン量を算出する場合、同じ取引相手、または同じ取引相手の組み合わせで、数度取引があったとしても、取引パターン量が増えないように算出される。これにより、悪意のある複数の参加者が協力して、取引パターン量を増やすような不正を回避することができる。

[0106] 図１０（ｃ）は、このように算出された取引パターン量（ｓｃｏｒｅ（ａ））に基づいて、ブロックの生成者となりうるアドレスの条件式の一例を示す。図１０（ｃ）は、ＰｏＳに基づいてブロックの生成者となりうるアドレスの条件式において、コインの貯蓄量を、取引パターン量に変換したものである。

[0107] 図１１を参照して、取引パターン量算出手段１２４の処理を算出する取引パターン量算出処理を説明する。なお、取引パターン量算出手段２２５の処理も同様である。

[0108] まずステップＳ１５１においてブロックチェーン生成装置１は、ブロックチェーンデータ１１２の過去のトランザクションから、ブロックの生成者（ブロックチェーン生成装置１を用いる参加者）に関連するトランザクションを抽出する。

[0109] ステップＳ１５２においてブロックチェーン生成装置１は、ステップＳ１５１で抽出したトランザクションから、取引相手の識別子を特定する。ステップＳ１５３において、ステップＳ１５２において特定された取引相手の識別子に基づいて、ブロックの生成者の取引パターン量を算出する。

[0110] 上述したように、本発明の実施の形態に係るブロックチェーン生成装置１は、複数の相反するパラメータ種別のうちの一つのパラメータ種別に基づい

て、ブロックチェーンに新たなブロックを連結する資格があるか否かを判定する。本発明の実施の形態において、複数の相反するパラメータ種別がブレンドされるブレンドパターンに基づいて各ブロックが生成され、ブロックチェーンが生成される。この「複数の相反するパラメータ種別」は、片方のリソースを独占したとしても、もう片方のリソースの独占に影響を及ぼさない関係、同一人が両立して条件を満たすことが難しい関係を有する。

[0111] さらに、本発明の実施の形態に係るブロックチェーン検証装置２は、ブロックチェーンでの複数のブロックの生成で用いられた各パラメータ種別が、複数の相反するパラメータ種別をブレンドするブレンドパターンに合致する場合に、このブロックチェーンデータを承認する。

[0112] これにより、本発明の実施の形態は、悪意のある生成者が連続してブロックを連結して、攻撃することを回避することができる。

[0113] また、ブロックチェーンにおいて、連続する承認ブロック数のブロックが、複数の相反するパラメータ種別に基づいて生成されることにより、悪意のある生成者が連続してブロックを連結した状態で、完全な取引の完了が保証されることを回避することができる。

[0114] さらに、本発明の実施の形態において、新たなブロックを連結する資格があるか否かを判断するために、生成者の信用スコアに対応する取引パターン量を用いる。取引パターン量は、長い時間をかけて積み上げた実績に基づくものであるので、この信用の暴落が攻撃の抑止力となる。さらに、取引パターン量によるブロック生成の承認は、仮想通貨の譲渡はもちろん、複数者間で契約書を交わす際の証跡としてブロックチェーンを応用する場合にも適用することができる。

[0115] また、相反するパラメータ種別として、取引パターン量と、取引パターン量に相反するコインの貯蓄量を設定することにより、悪意のある生成者が連続してブロックを連結して、攻撃することを回避することができる。

[0116] （その他の実施の形態）

上記のように、本発明の実施の形態によって記載したが、この開示の一部

をなす論述および図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施の形態、実施例および運用技術が明らかとなる。

[0117] 例えば、本発明の実施の形態に記載したブロックチェーン生成装置１およびブロックチェーン検証装置２は、図５および図７にそれぞれ示すように一つのハードウエア上に構成されても良いし、その機能や処理数に応じて複数のハードウエア上に構成されても良い。また、既存の情報処理システム上に実現されても良い。

[0118] 本発明はここでは記載していない様々な実施の形態等を含むことは勿論である。従って、本発明の技術的範囲は上記の説明から妥当な請求の範囲に係る発明特定事項によってのみ定められるものである。

符号の説明

[0119] １　ブロックチェーン生成装置

２　ブロックチェーン検証装置

３　トランザクション生成装置

４　Ｐ２Ｐネットワーク

５　取引支援システム

１１０、２１０、３１０　記憶装置

１１１、２１１、３１１　共有データ

１１２、２１２、３１２　ブロックチェーンデータ

１１３、２１３、３１３　トランザクションデータ

１１４、２１４　ブロック承認方法データ

１１５、２１５　パラメータデータ

１２０、２２０、３２０　処理装置

１２１、２２１、３２１　同期手段

１２２、２２３　パラメータ算出手段

１２３、２２４　コイン貯蓄量算出手段

１２４、２２５　取引パターン量算出手段

１２５　ブロック生成条件確認手段

１２６　ブロックチェーン生成手段

１３０、２３０、３３０　通信制御装置

２２２　ブロック承認方法検証手段

２２６　ブロック生成条件検証手段

２２７　ブロックチェーン検証手段

請求の範囲

[請求項1] 複数のトランザクション生成装置によって生成されたトランザクションデータを含むブロックを連結したブロックチェーンデータに、新たなブロックを連結して、新たなブロックチェーンデータを生成するブロックチェーン生成装置であって、

前記ブロックチェーンデータと、前記ブロックチェーンデータに含まれていないトランザクションデータとを含む共有データを取得する同期手段と、

前記ブロックチェーンデータにおいて複数のブロックを連結する資格の有無を判定する際に用いられる複数のパラメータ種別のブレンドパターンを特定するブロック承認方法データに基づいて、前記新たなブロックを連結する際に用いられるパラメータ種別を特定し、

前記ブロックチェーンデータの前記トランザクションデータのうち、当該ブロックチェーン生成装置を用いる生成者の識別子に関連するトランザクションデータから、特定された前記パラメータ種別の値を算出するパラメータ算出手段と、

前記パラメータ算出手段が算出した値に基づいて、前記生成者が、前記新たなブロックチェーンデータを生成する資格を有しているか否かを判定するブロック生成条件確認手段と、

前記ブロック生成条件確認手段が資格を有していると判定した場合、前記共有データを参照して、前記新たなブロックチェーンの生成を試みるブロックチェーン生成手段

とを備え、

前記ブロック承認方法データに含まれるブレンドパターンの識別子は、互いに相反する複数のパラメータ種別の組み合わせを特定することを特徴とするブロックチェーン生成装置。

[請求項2] 前記ブロック承認方法データは、

第１のパラメータ種別を第１の数だけ繰り返した後、前記第１のパ

ラメータ種別と相反する第２のパラメータ種別を第２の数だけ繰り返すブレンドパターンを特定する

ことを特徴とする請求項１に記載のブロックチェーン生成装置。

[請求項3] 前記ブロック承認方法データは、

連続する所定の数のパラメータ種別の組み合わせにおいて、少なくとも、第１のパラメータ種別および第２のパラメータ種別をそれぞれ１つずつ含むブレンドパターンを特定する

ことを特徴とする請求項１に記載のブロックチェーン生成装置。

[請求項4] 前記所定の数は、所定のブロックについて完全な取引の完了が保証されるために必要なブロックの数である

ことを特徴とする請求項３に記載のブロックチェーン生成装置。

[請求項5] 複数のトランザクション生成装置によって生成されたトランザクションデータを含むブロックを連結したブロックチェーンデータに、新たなブロックを連結して、新たなブロックチェーンデータを生成するブロックチェーン生成方法であって、

コンピュータが、前記ブロックチェーンデータと、前記ブロックチェーンデータに含まれていないトランザクションデータとを含む共有データを取得するステップと、

前記コンピュータが、前記ブロックチェーンデータにおいて複数のブロックを連結する資格の有無を判定する際に用いられる複数のパラメータ種別のブレンドパターンを特定するブロック承認方法データに基づいて、前記新たなブロックを連結する際に用いられるパラメータ種別を特定するステップと、

前記コンピュータが、前記ブロックチェーンデータの前記トランザクションデータのうち、当該コンピュータを用いる生成者の識別子に関連するトランザクションデータから、特定された前記パラメータ種別の値を算出するステップと、

前記コンピュータが、算出するステップが算出した値に基づいて、

前記生成者が、前記新たなブロックチェーンデータを生成する資格を有しているか否かを判定するステップと、

前記コンピュータが、資格を有していると判定した場合、前記共有データを参照して、前記新たなブロックチェーンの生成を試みるステップ

とを備え、

前記ブロック承認方法データに含まれるブレンドパターンの識別子は、互いに相反する複数のパラメータ種別の組み合わせを特定することを特徴とするブロックチェーン生成方法。

[請求項6] 複数のトランザクション生成装置によって生成されたトランザクションデータを含むブロックを連結したブロックチェーンデータを検証するブロックチェーン検証装置であって、

前記ブロックチェーンデータを含む共有データを取得する同期手段と、

前記ブロックチェーンデータにおいて複数のブロックを連結する資格の有無を判定する際に用いられる複数のパラメータ種別のブレンドパターンを特定するブロック承認方法データに基づいて、前記ブロックを連結する際に用いられるパラメータ種別を特定し、前記ブロックチェーンデータが、特定されたパラメータ種別に基づいて生成されているか否かを判定するブロック承認方法検証手段と、

前記ブロックチェーンデータの前記トランザクションデータのうち、前記ブロックチェーンデータを生成した装置を用いる生成者の識別子に関連するトランザクションデータから、前記ブロック承認方法検証手段で特定された前記パラメータ種別の値を算出するパラメータ算出手段と、

前記パラメータ算出手段が算出した値に基づいて、前記生成者が、前記ブロックチェーンデータを生成する資格を有しているか否かを判定するブロック生成条件検証手段と、

前記ブロック承認方法検証手段が、前記ブロックチェーンデータが前記特定されたパラメータ種別に基づいて生成されていると判定し、かつ前記ブロック生成条件検証手段が、前記生成者が前記ブロックチェーンデータを生成する資格を有していると判定した場合、前記ブロックチェーンデータを承認するブロックチェーン検証手段

とを備え、

前記ブロック承認方法データに含まれるブレンドパターンの識別子は、互いに相反する複数のパラメータ種別の組み合わせを特定することを特徴とするブロックチェーン検証装置。

[請求項7] 複数のトランザクション生成装置によって生成されたトランザクションデータを含むブロックを連結したブロックチェーンデータを検証するブロックチェーン検証方法であって、

コンピュータが、前記ブロックチェーンデータを含む共有データを取得するステップと、

前記コンピュータが、前記ブロックチェーンデータにおいて複数のブロックを連結する資格の有無を判定する際に用いられる複数のパラメータ種別のブレンドパターンを特定するブロック承認方法データに基づいて、前記ブロックを連結する際に用いられるパラメータ種別を特定し、前記ブロックチェーンデータが、特定されたパラメータ種別に基づいて生成されているか否かを判定するステップと、

前記コンピュータが、前記ブロックチェーンデータの前記トランザクションデータのうち、前記ブロックチェーンデータを生成した装置を用いる生成者の識別子に関連するトランザクションデータから、前記特定されたパラメータ種別の値を算出するステップと、

前記コンピュータが、前記特定されたパラメータ種別の値に基づいて、前記生成者が、前記ブロックチェーンデータを生成する資格を有しているか否かを判定するステップと、

前記コンピュータが、前記ブロックチェーンデータが前記特定され

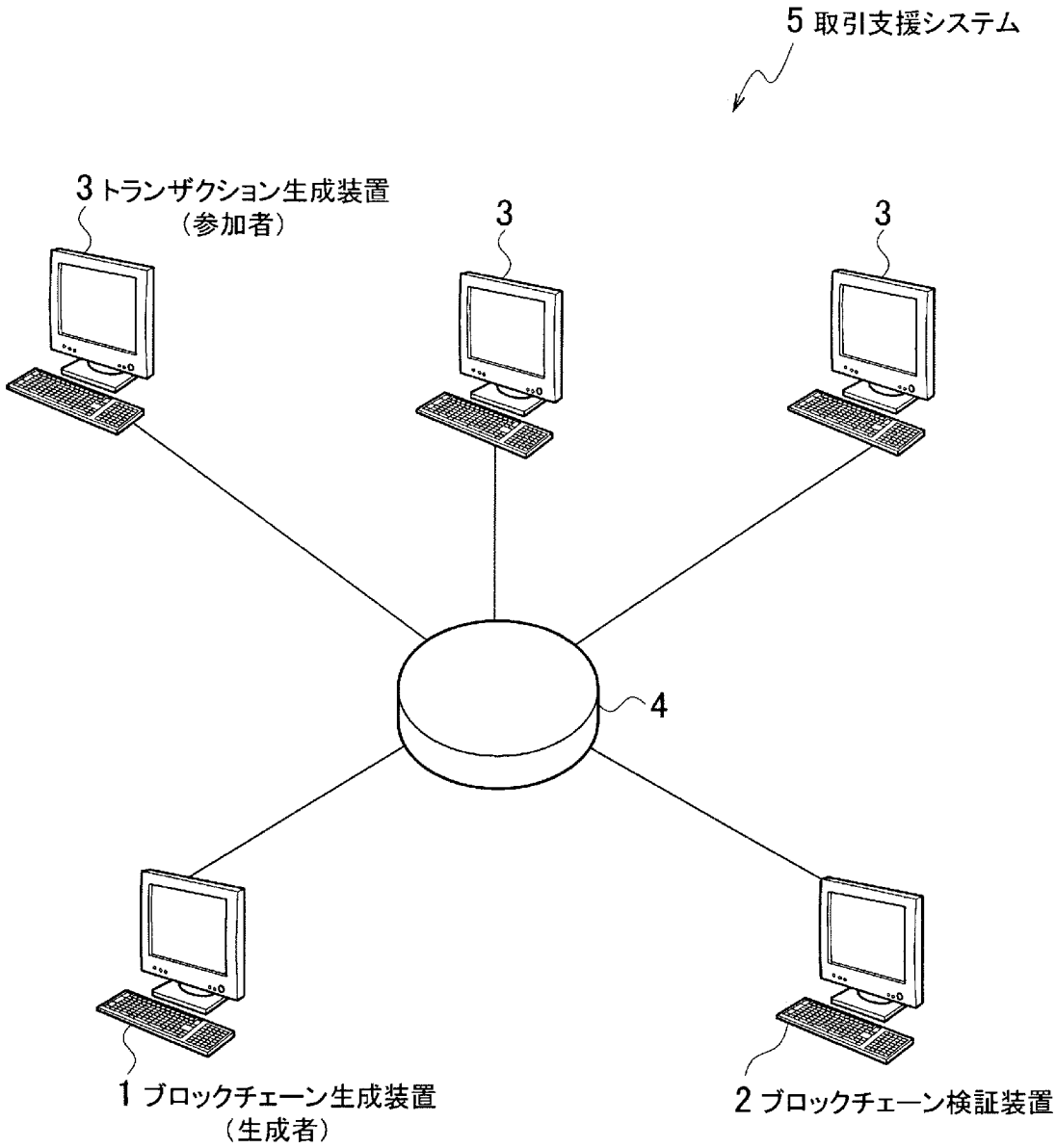
たパラメータ種別に基づいて生成されていると判定し、かつ、前記生成者が前記ブロックチェーンデータを生成する資格を有していると判定した場合、前記ブロックチェーンデータを承認するステップ

とを備え、

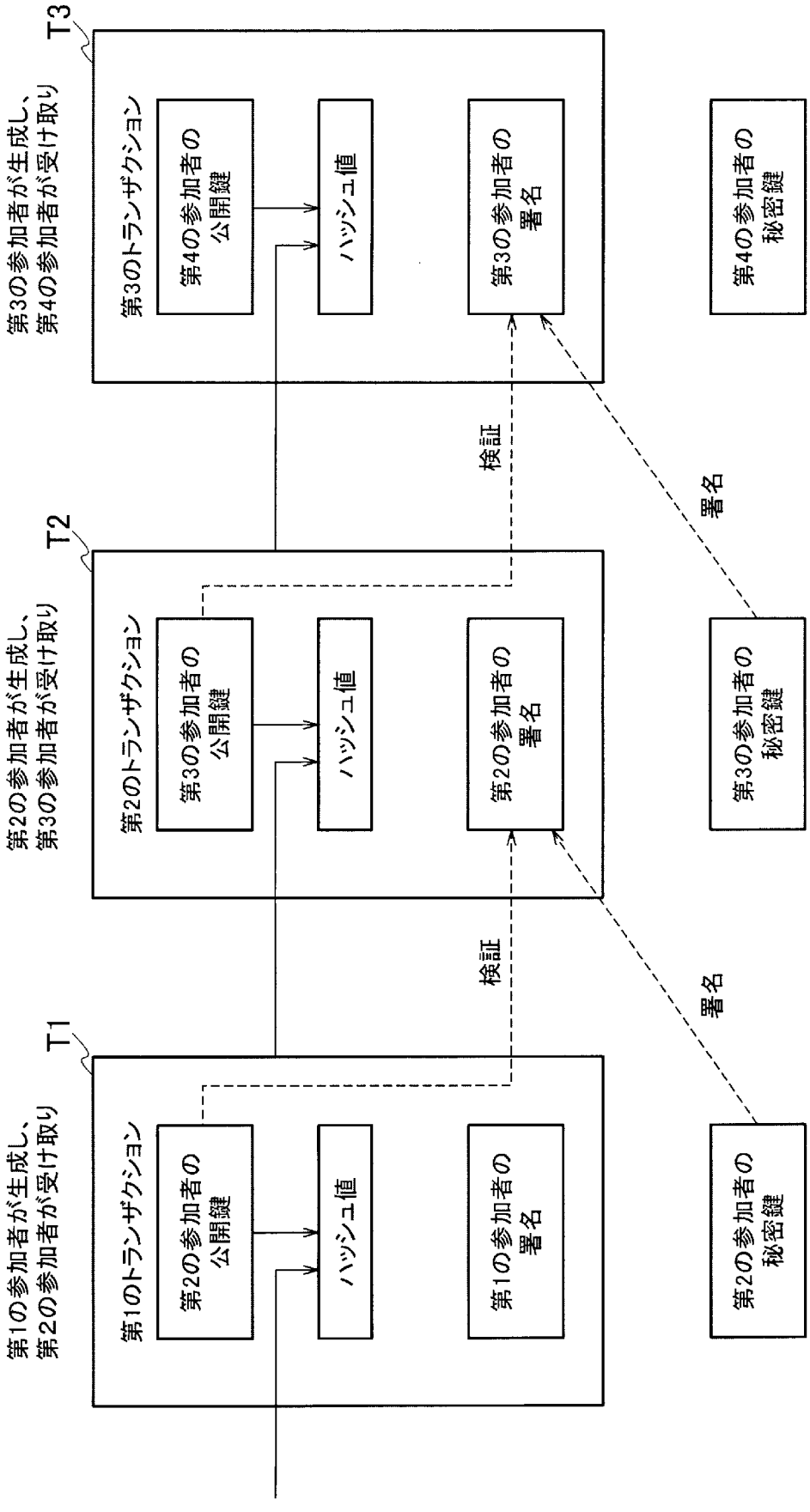
前記ブロック承認方法データに含まれるブレンドパターンの識別子は、互いに相反する複数のパラメータ種別の組み合わせを特定することを特徴とするブロックチェーン検証方法。

[請求項8] コンピュータに、請求項１ないし請求項４および請求項６のいずれか１項に記載の手段として機能させるためのプログラム。

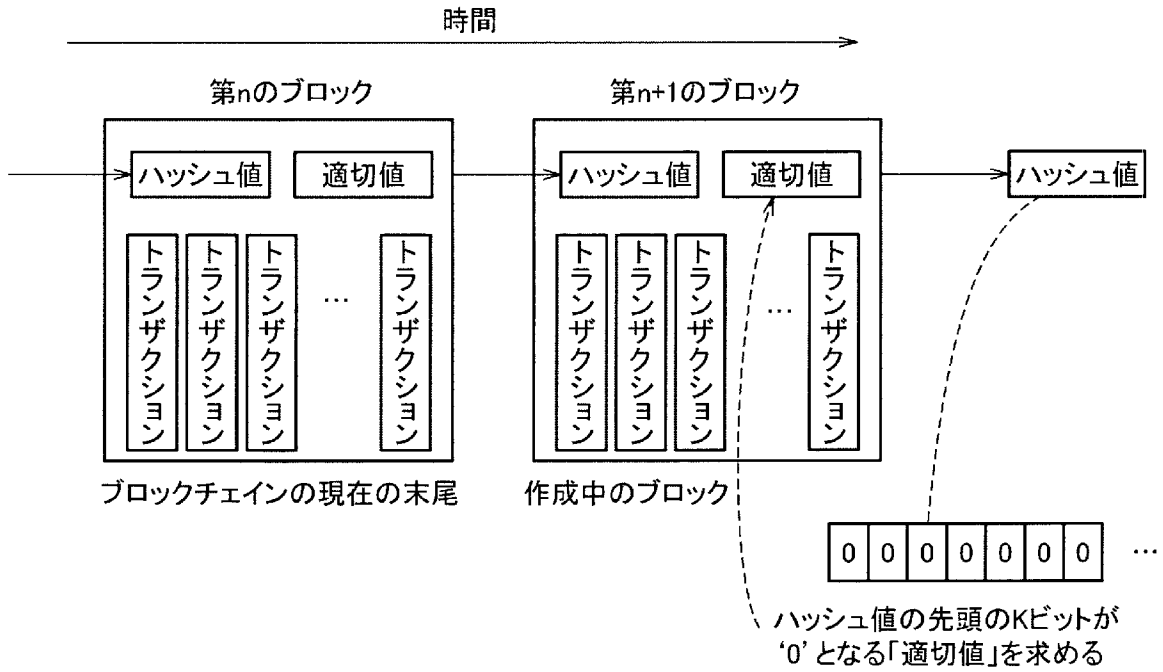
[図1]


5 取引支援システム
3 トランザクション生成装置
（参加者）
3
3
4
1 ブロックチェーン生成装置
（生成者）
2 ブロックチェーン検証装置

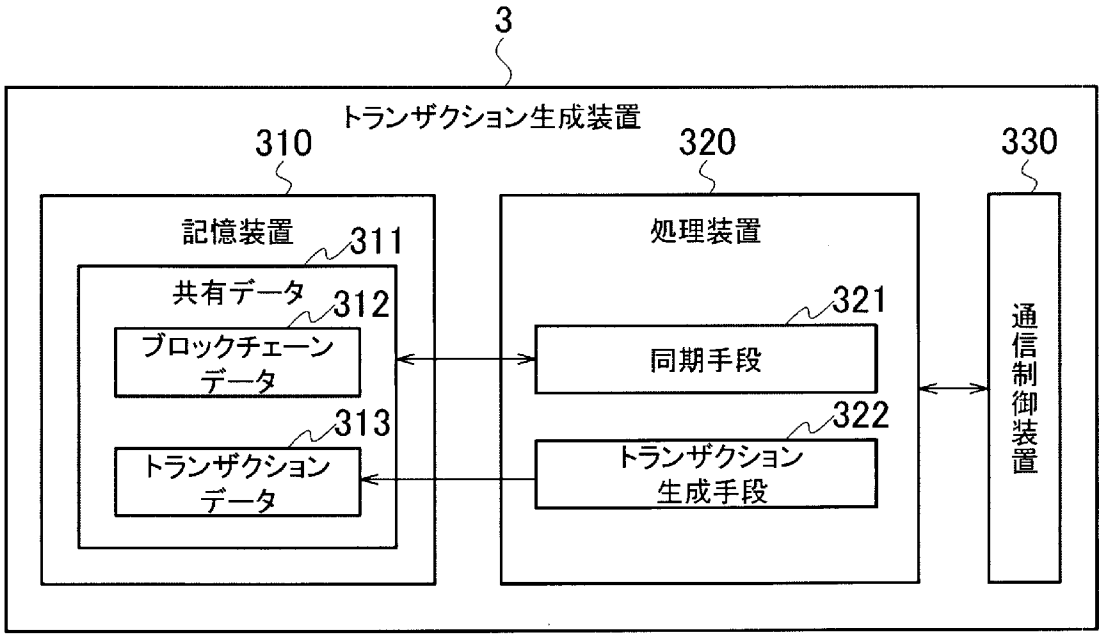
[図2]


T3
第3の参加者が生成し、
第4の参加者が受け取り
第3のトランザクション
第4の参加者の
公開鍵
ハッシュ値
第3の参加者の
署名
第4の参加者の
秘密鍵
検証
署名
T2
第2の参加者が生成し、
第3の参加者が受け取り
第2のトランザクション
第3の参加者の
公開鍵
ハッシュ値
第2の参加者の
署名
第3の参加者の
秘密鍵
検証
署名
T1
第1の参加者が生成し、
第2の参加者が受け取り
第1のトランザクション
第2の参加者の
公開鍵
ハッシュ値
第1の参加者の
署名
第2の参加者の
秘密鍵

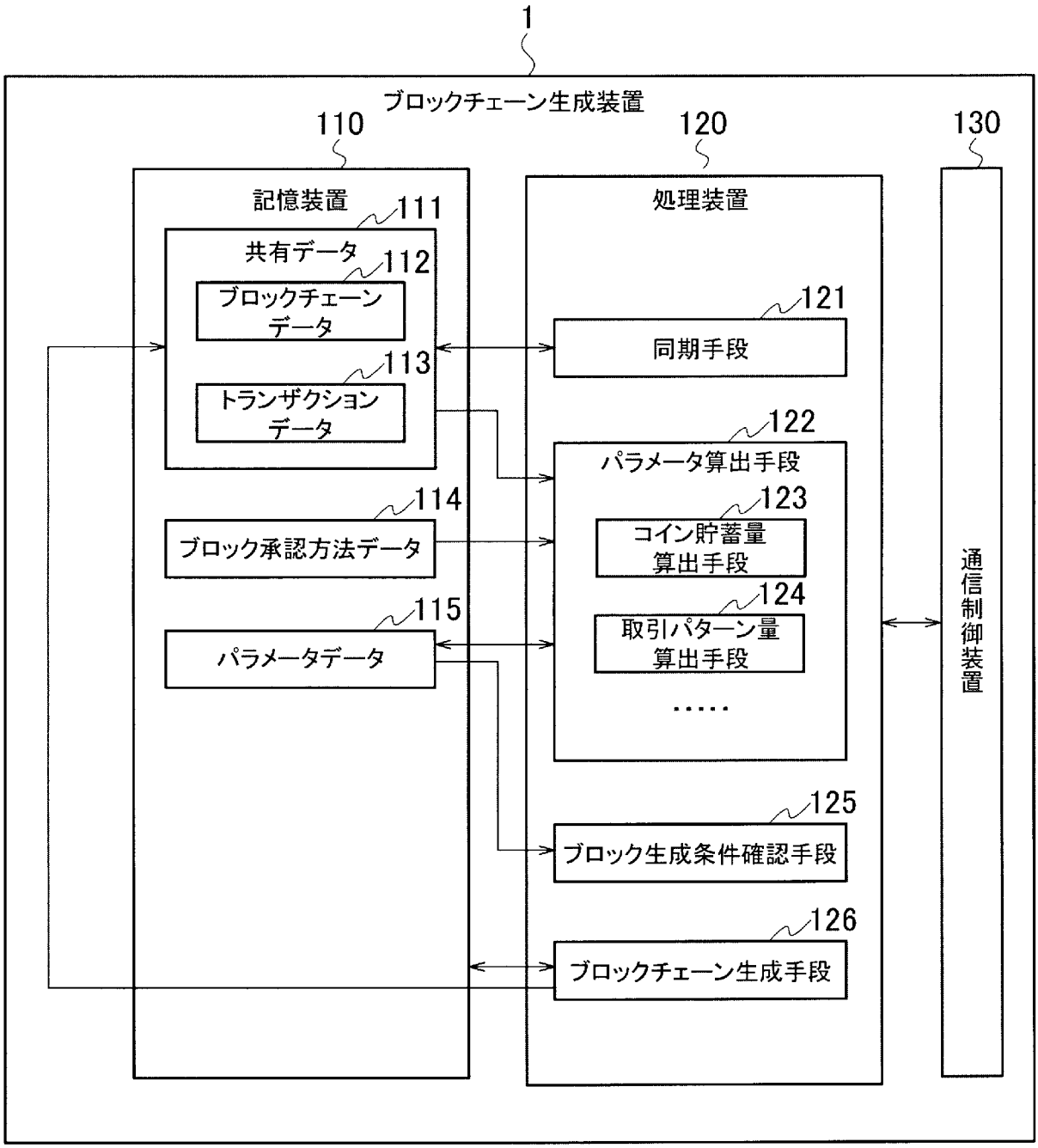
[図3]


時間
第nのブロック
第n+1のブロック
ハッシュ値
適切値
ハッシュ値
適切値
ハッシュ値
トランザクション
トランザクション
トランザクション
…
トランザクション
トランザクション
トランザクション
トランザクション
…
ブロックチェインの現在の末尾
作成中のブロック
0 0 0 0 0 0 0 …
ハッシュ値の先頭のKビットが
‘0’となる「適切値」を求める

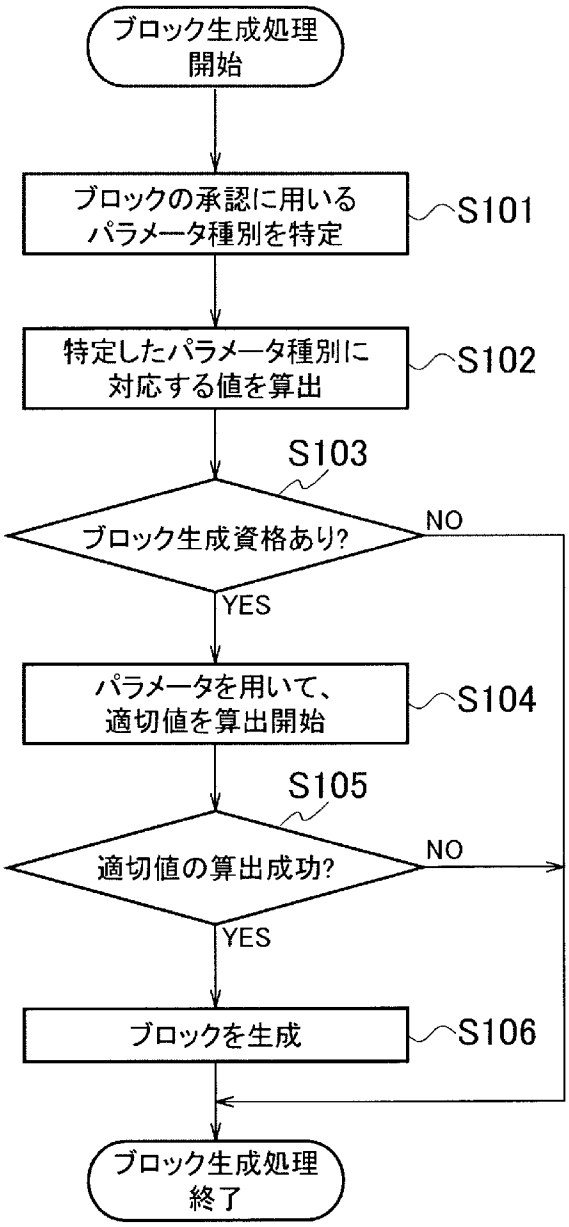
[図4]


3
トランザクション生成装置
310
320
330
記憶装置
311
共有データ
312
ブロックチェーン
データ
313
トランザクション
データ
処理装置
321
同期手段
322
トランザクション
生成手段
通信制御装置

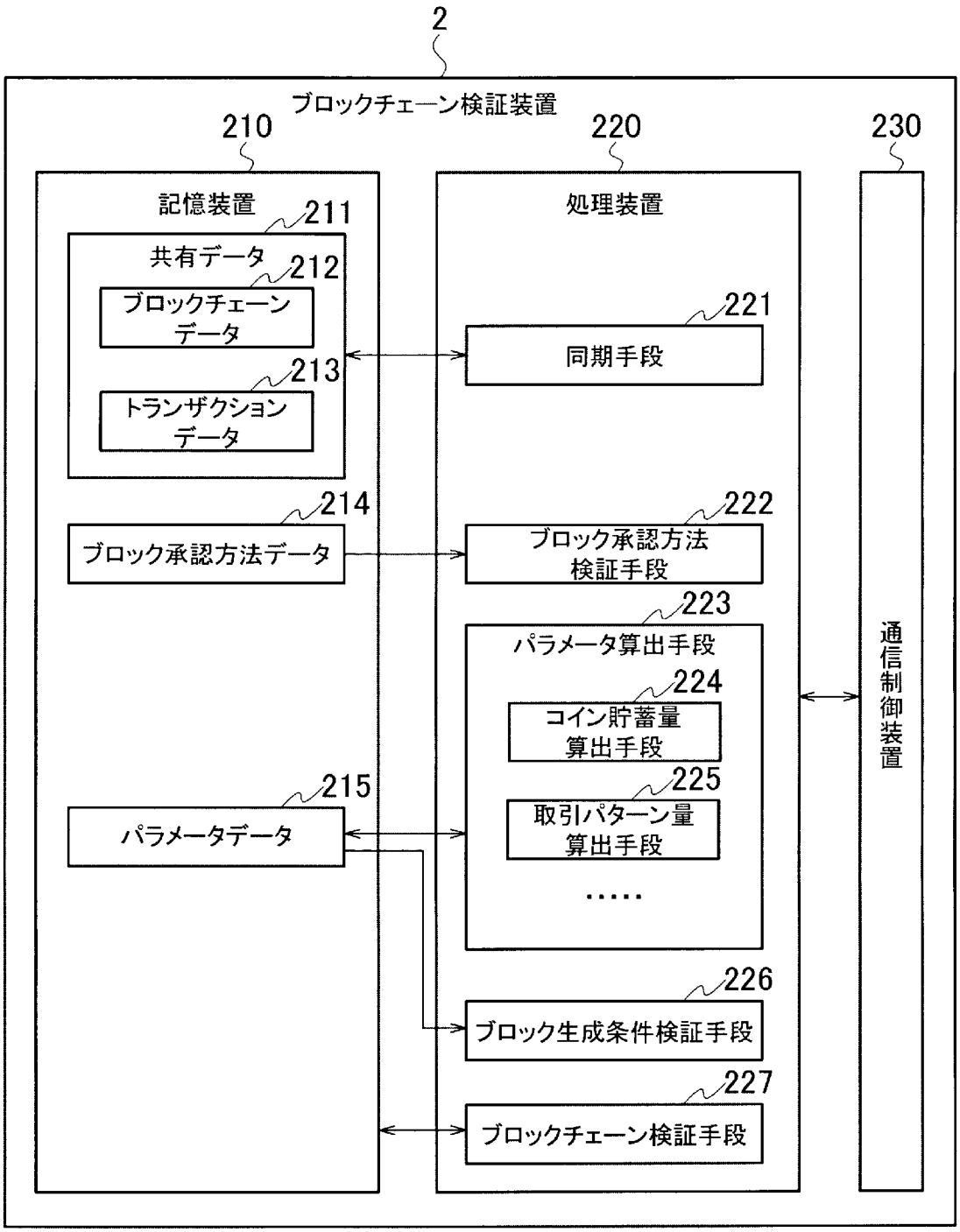
[図5]


1
ブロックチェーン生成装置
110
記憶装置
111
共有データ
112
ブロックチェーン
データ
113
トランザクション
データ
114
ブロック承認方法データ
115
パラメータデータ
120
処理装置
121
同期手段
122
パラメータ算出手段
123
コイン貯蓄量
算出手段
124
取引パターン量
算出手段
.....
125
ブロック生成条件確認手段
126
ブロックチェーン生成手段
130
通信制御装置

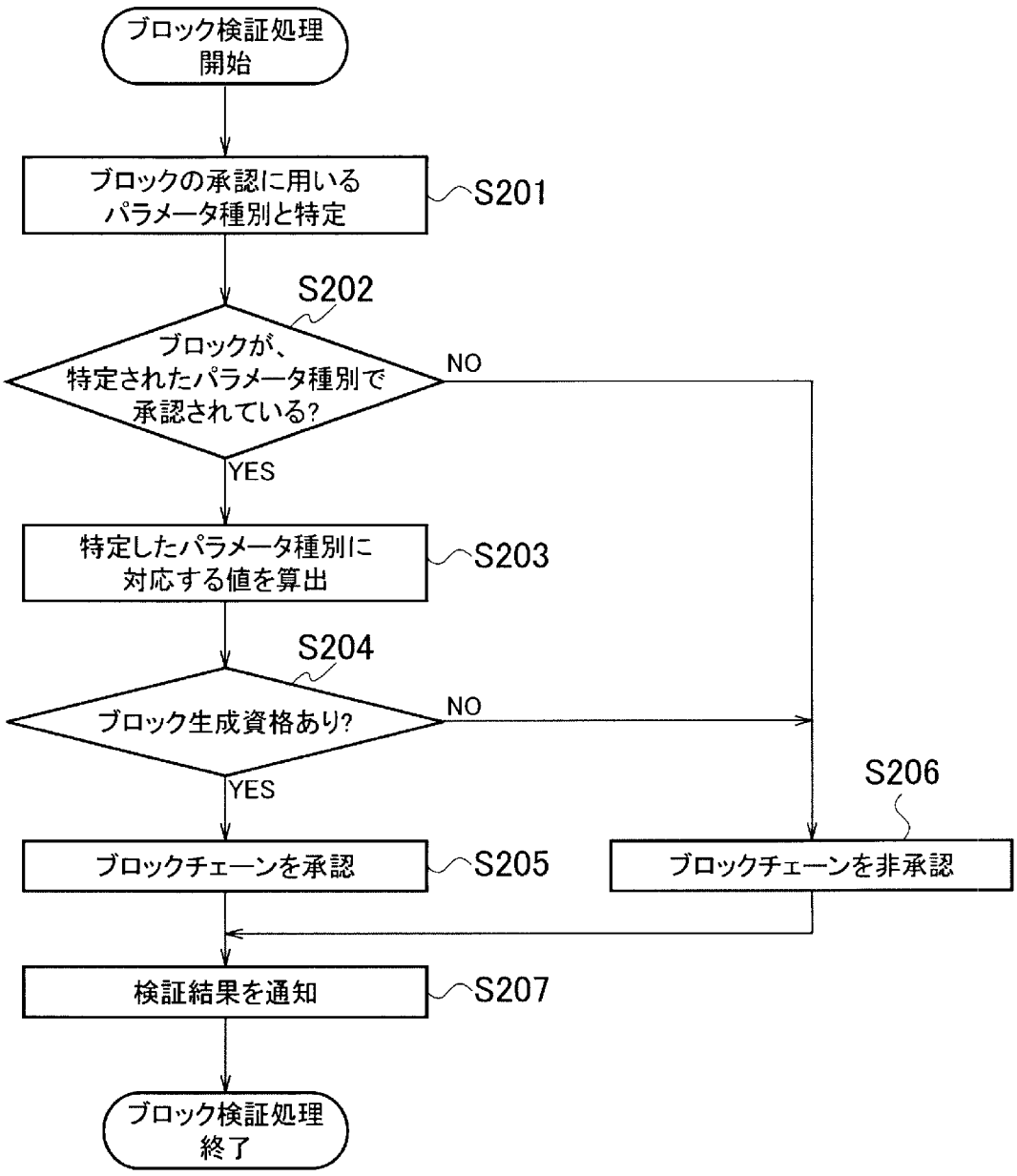
[図6]


ブロック生成処理
開始
ブロックの承認に用いる
パラメータ種別を特定
S101
特定したパラメータ種別に
対応する値を算出
S102
S103
ブロック生成資格あり?
NO
YES
パラメータを用いて、
適切値を算出開始
S104
S105
適切値の算出成功?
NO
YES
ブロックを生成
S106
ブロック生成処理
終了

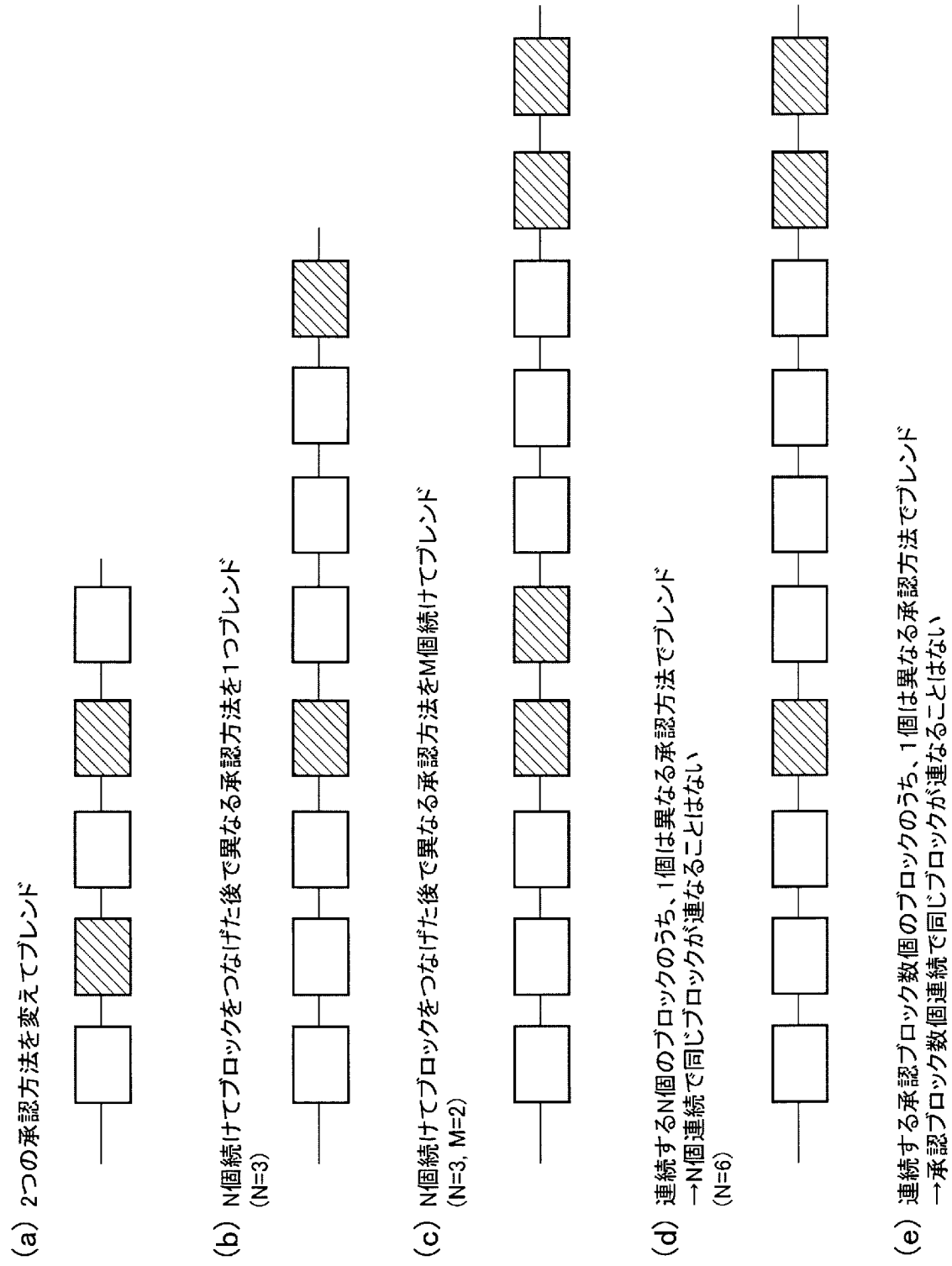
[図7]


2
ブロックチェーン検証装置
210
220
230
記憶装置
211
共有データ
212
ブロックチェーン
データ
213
トランザクション
データ
214
ブロック承認方法データ
215
パラメータデータ
処理装置
221
同期手段
222
ブロック承認方法
検証手段
223
パラメータ算出手段
224
コイン貯蓄量
算出手段
225
取引パターン量
算出手段
.....
226
ブロック生成条件検証手段
227
ブロックチェーン検証手段
通信制御装置

[図8]


ブロック検証処理
開始
ブロックの承認に用いる
パラメータ種別と特定
S201
S202
ブロックが、
特定されたパラメータ種別で
承認されている?
NO
YES
特定したパラメータ種別に
対応する値を算出
S203
S204
ブロック生成資格あり?
NO
YES
S206
ブロックチェーンを承認
S205
ブロックチェーンを非承認
検証結果を通知
S207
ブロック検証処理
終了

[図9]


(a) 2つの承認方法を変えてブレンド
(b) N個続けてブロックをつなげた後で異なる承認方法を1つブレンド
(N=3)
(c) N個続けてブロックをつなげた後で異なる承認方法をM個続けてブレンド
(N=3, M=2)
(d) 連続するN個のブロックのうち、1個は異なる承認方法でブレンド
→N個連続で同じブロックが連なることはない
(N=6)
(e) 連続する承認ブロック数個のブロックのうち、1個は異なる承認方法でブレンド
→承認ブロック数個連続で同じブロックが連なることはない

[図10]

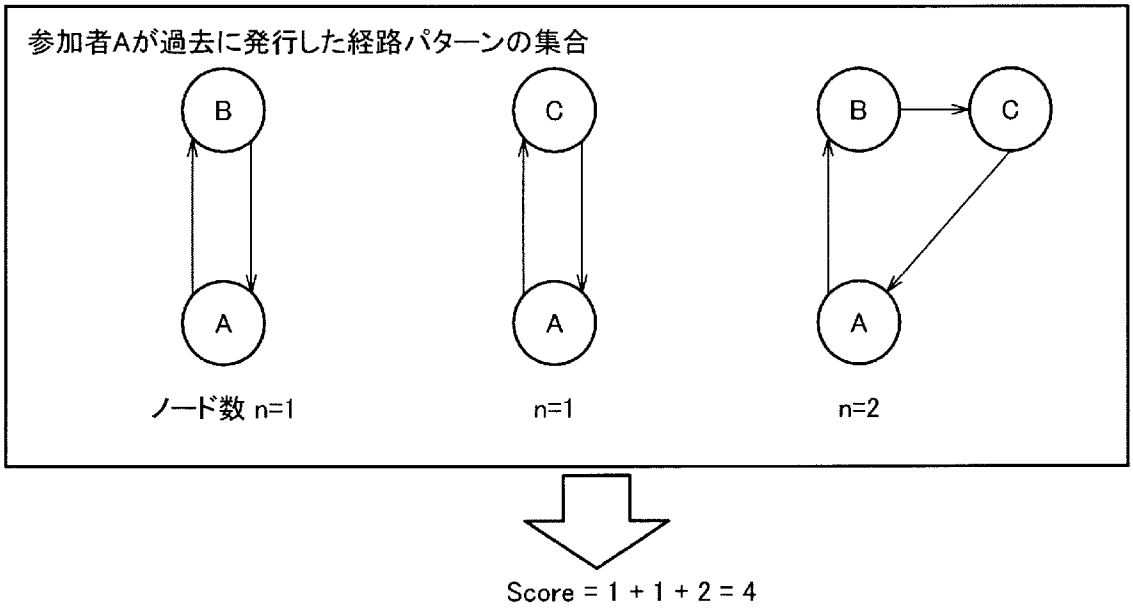
(a)

・ある参加者が過去に発行した経路パターンの集合：a

・aに含まれるある経路パターンpに含まれるノード数：$n_{p,a}$

・aの全ての経路パターンのノード数の和(スコア)：$score(a) = \sum_{s \in a} n_{s,a}$ …式(1)

(b)

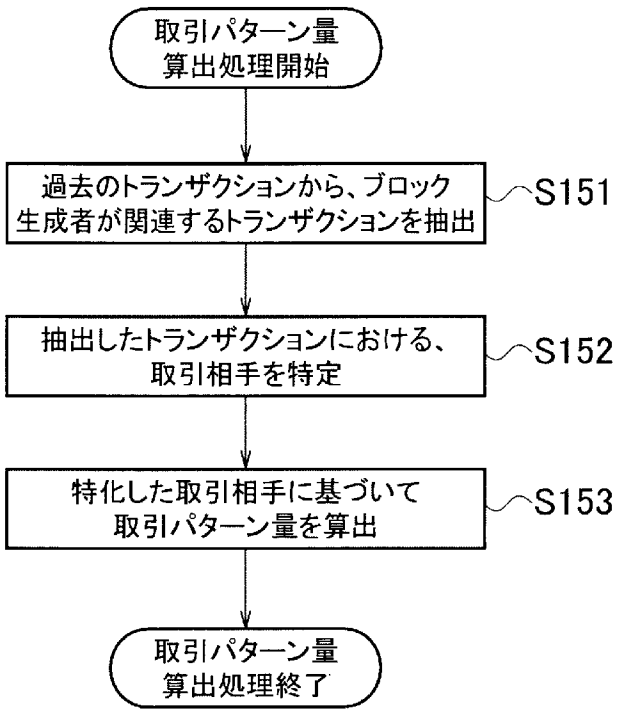


(c)

承認者addressの条件式例

SHA256(prevhash + address + timestamp)≦2^256*score(a)/difficulty

[図11]


取引パターン量
算出処理開始
過去のトランザクションから、ブロック
生成者が関連するトランザクションを抽出
S151
抽出したトランザクションにおける、
取引相手を特定
S152
特化した取引相手に基づいて
取引パターン量を算出
S153
取引パターン量
算出処理終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/083062

A. CLASSIFICATION OF SUBJECT MATTER
G06Q20/06(2012.01)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)
G06Q20/06

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.
A	Yasuyuki FUCHITA, "Innovation to Kin'yu", Nomura Capital Markets Quarterly Autumn 2015, 01 November 2015 (01.11.2015), vol.19, no.2, pages 11 to 35, ISSN 2185-4629	1-8
A	US 2015/0046337 A1 (Hu Chin-hao), 12 February 2015 (12.02.2015), paragraphs [0026] to [0029] (Family: none)	1-8
A	FinTech Kin'yu o Kaeru nowa Ginko dewa Nai, Nikkei Computer, 04 August 2015 (04.08.2015), no.892, pages 28 to 31, ISSN 0285-4619	1-8

☐ 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	Date of mailing of the international search report
23 January 2017 (23.01.17)	31 January 2017 (31.01.17)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０８３０６２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06Q20/06(2012.01)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（ＩＰＣ））

Int.Cl.　G06Q20/06

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
Ａ	淵田　康之，イノベーションと金融，野村資本市場クォータリー　２０１５年秋号，2015.11.01，第１９巻　第２号，pp.11～35，ISSN 2185～4629	１～８
Ａ	US 2015/0046337 A1 (Hu Chin-hao) 2015.02.12，段落[0026]～[0029]（ファミリーなし）	１～８
Ａ	ＦｉｎＴｅｃｈ　金融を変えるのは銀行ではない，日経コンピュータ，2015.08.04，第892号，pp.28～31，ISSN 0285～4619	１～８

☐　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	国際調査報告の発送日
２３．０１．２０１７	３１．０１．２０１７

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
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）　５Ｌ　３７８６
山本　雅士
電話番号　０３－３５８１－１１０１　内線　３５６２