(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8月6日(06.08.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/158953 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G06F 21/64* (2013.01)
G06Q 20/06 (2012.01)

(21) 国際出願番号： PCT/JP2020/003840

(22) 国際出願日： 2020年2月2日(02.02.2020)

(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：
特願 2019-017542 2019年2月3日(03.02.2019) JP

(71) 出願人: 株式会社ｂｉｔＦｌｙｅｒ Ｂｌｏｃｋｃｈａｉｎ (**BITFLYER BLOCKCHAIN, INC.**) [JP/JP]; 〒1076237 東京都港区赤坂九丁目７番１号 Tokyo (JP).

(72) 発明者: 小宮山 峰史 (**KOMIYAMA Takafumi**); 〒1076237 東京都港区赤坂九丁目７番１号 株式会社ｂｉｔＦｌｙｅｒ Ｂｌｏｃｋｃｈａｉｎ内 Tokyo (JP).

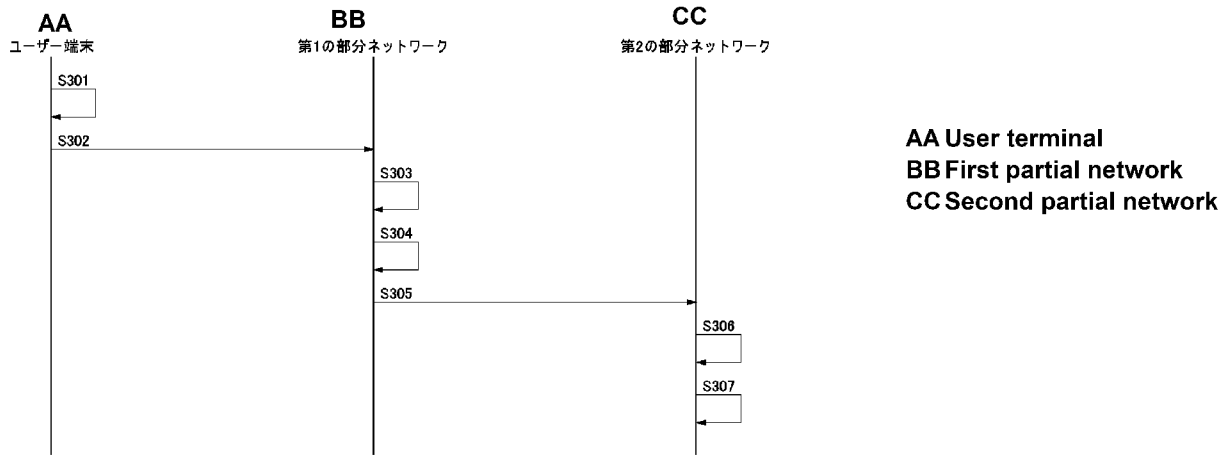
(74) 代理人: 大谷 寛 (**OTANI Kan**); 〒1060032 東京都港区六本木六丁目２番３１号 六本木ヒルズノースタワー１７階 Tokyo (JP).

(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, JO, 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,

WO 2020/158953 A1

(54) **Title:** METHOD FOR STORING TRANSACTION THAT REPRESENTS ASSET TRANSFER TO DISTRIBUTED NETWORK AND PROGRAM FOR THE SAME

(54) 発明の名称： 分散ネットワークに資産の移転を表すトランザクションを記憶する方法及びそのためのプログラム



(57) **Abstract:** A method for storing a transaction that represents asset transfer to a distributed network, wherein a transaction processing speed is greatly improved. A first partial network 110 constituting the distributed network receives a transaction 200 generated by a user terminal 140 and representing the transfer of assets 203 from a source of transfer identifier 201 to a destination of transfer identifier 202, generates a block that includes the transaction 200, and performs

[続葉有]

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, 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))

a consensus building process in the first partial network 110 for adoption of the block (S303). Each node, having the asset states of the source of transfer identifiers processable by each node stored, records the transfer of assets from the source of transfer identifier written in one or a plurality of transactions included in a block having been added through consensus building (S304). Owing to the fact that the source of transfer identifiers processable in each partial network are defined in advance, transactions are processed in parallel.

(57) 要約:分散ネットワークに資産の移転を表すトランザクションを記憶する方法において、トランザクション処理速度を大幅に向上する。ユーザー端末１４０において生成された、資産２０３の移転元識別子２０１から移転先識別子２０２への移転を表すトランザクション２００を、分散ネットワークを構成する第１の部分ネットワーク１１０が受信し、トランザクション２００を含むブロックを生成して、その採択のための第１の部分ネットワーク１１０における合意形成処理を行う(Ｓ３０３)。各ノードは、各ノードが処理可能な移転元識別子の資産の状態を記憶しており、合計形成を経て追加されたブロックに含まれる１又は複数のトランザクションに記述された移転元識別子からの資産の移転を記録する(Ｓ３０４)。各部分ネットワークにおいて処理可能な移転元識別子を定めておくことによって、トランザクションの並列処理を行う。

明　細　書

発明の名称 ：

分散ネットワークに資産の移転を表すトランザクションを記憶する方法及びそのためのプログラム

技術分野

[0001] 本発明は、複数のノードを有する分散ネットワークに資産の移転を表すトランザクションを記憶する方法及びそのためのプログラム並びに当該分散ネットワークを構成するためのノードに関する。

背景技術

[0002] データベースを複数のノードによって構成される分散ネットワーク上に構築するブロックチェーンネットワークは、その非中央集権的性格から改ざん耐性が高い。いずれかのノードにおいてデータベースが改ざんされても分散ネットワーク全体を書き換えることは困難だからである。各ノードに記憶されるブロックチェーンが互いに同期してデータベースとして機能している。

[0003] ノード数の増大は改ざん耐性を高める反面、各ノードに同一のブロックチェーンを記憶する必要性からブロックの採択のための処理速度を一般に低下させる。直観的にはノード数を増やすことで単位時間当たりの処理速度を向上可能であるとおもわれるが、ブロックチェーンにおいては逆に低下してしまうことから、ブロックサイズの増大、ブロックに含まれる１又は複数のトランザクションのデータ容量の低減等、さまざまな試みがなされているのが現状である。

発明の概要

発明が解決しようとする課題

[0004] しかしながら、現状のさまざまな試みの中には、拡張性（スケーラビリティ）を大幅に向上可能なものを見出すことは出来ない。特に、仮想通貨、実通貨、株等の資産の移転を分散ネットワーク上のデータベースにおいて管理することを現実的に考えた場合、１秒間に処理可能なトランザクションの数

が数件と言われるビットコインを筆頭に、スケーラビリティはブロックチェーンの実用化において喫緊の課題である。

[0005] 本発明は、このような問題点に鑑みてなされたものであり、その目的は、複数のノードを有する分散ネットワークに資産の移転を表すトランザクションを記憶する方法及びそのためのプログラム並びに当該分散ネットワークを構成するためのノードにおいて、単位時間当たりのトランザクション処理速度を大幅に向上することにある。

課題を解決するための手段

[0006] このような目的を達成するために、本発明の第１の態様は、複数の部分ネットワークを有する分散ネットワークに資産の移転を表すトランザクションを記憶する方法であって、前記複数の部分ネットワークのうちの第１の部分ネットワークを構成するノードが、前記第１の部分ネットワークで処理可能な移転元識別子から前記第１の部分ネットワークで処理可能ではない移転先識別子への資産の移転を表す第１のトランザクションを受信するステップと、前記第１のトランザクションを含むブロックを生成するステップと、前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記移転元識別子の資産の状態を更新するステップと、前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記第１のトランザクションにより表される前記移転先識別子への前記資産の移転を反映させるための第２のトランザクションを、前記第１のトランザクションの前記移転先識別子と一致する移転元識別子を処理可能な第２の部分ネットワークに送信するステップとを含むことを特徴とする。

[0007] また、本発明の第２の態様は、第１の態様において、前記第１のトランザクションは、前記移転元識別子の秘密鍵による署名が付加されていることを特徴とする。

[0008] また、本発明の第３の態様は、第１又は２の態様において、移転される前記資産の額は、正の値であることを特徴とする。

[0009] また、本発明の第４の態様は、第１から第３のいずれかの態様において、

前記第２のトランザクションは、前記第１の部分ネットワークにおいて合意形成がなされたことを示す署名が付加されていることを特徴とする。

[0010] また、本発明の第５の態様は、第４の態様において、前記第２のトランザクションの署名は、単一の署名であることを特徴とする。

[0011] また、本発明の第６の態様は、第４又は第５の態様において、前記第２のトランザクションの署名は、前記ブロック内の前記第１のトランザクションを含む複数のトランザクションに基づくマークルツリーのマークルルートを含むブロックヘッダに対する署名であることを特徴とする。

[0012] また、本発明の第７の態様は、複数の部分ネットワークのうちの第１の部分ネットワークを構成するノードに、前記複数の部分ネットワークを有する分散ネットワークに資産の移転を表すトランザクションを記憶する方法を実行させるためのプログラムであって、前記方法は、前記ノードが、前記第１の部分ネットワークで処理可能な移転元識別子から前記第１の部分ネットワークで処理可能ではない移転先識別子への資産の移転を表す第１のトランザクションを受信するステップと、前記第１のトランザクションを含むブロックを生成するステップと、前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記移転元識別子の資産の状態を更新するステップと、前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記第１のトランザクションにより表される前記移転先識別子への前記資産の移転を反映させるための第２のトランザクションを、前記第１のトランザクションの前記移転先識別子と一致する移転元識別子を処理可能な第２の部分ネットワークに送信するステップとを含むことを特徴とする。

[0013] また、本発明の第８の態様は、複数の部分ネットワークを有する分散ネットワークに資産の移転を表すトランザクションを記憶するための、前記複数の部分ネットワークのうちの第１の部分ネットワークを構成するノードであって、前記第１の部分ネットワークで処理可能な移転元識別子から前記第１の部分ネットワークで処理可能ではない移転先識別子への資産の移転を表す

第１のトランザクションを受信して、前記第１のトランザクションを含むブロックを生成し、前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記移転元識別子の資産の状態を更新し、前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記第１のトランザクションにより表される前記移転先識別子への前記資産の移転を反映させるための第２のトランザクションを、前記第１のトランザクションの前記移転先識別子と一致する移転元識別子を処理可能な第２の部分ネットワークに送信することを特徴とする。

[0014] また、本発明の第９の態様は、複数の部分ネットワークを有する分散ネットワークに資産の移転を表すトランザクションを記憶する方法であって、前記複数の部分ネットワークのうちの第１の部分ネットワークを構成するノードが、前記第１の部分ネットワークで処理可能な移転元識別子から前記第１の部分ネットワークで処理可能ではない移転先識別子への資産の移転を表す第１のトランザクションを受信するステップと、前記第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ステップと、前記第１のブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記移転元識別子の資産の状態を更新するステップと、前記第１のブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記第１のトランザクションにより表される前記移転先識別子への前記資産の移転を反映させるための第２のトランザクションを、前記第１のトランザクションの前記移転先識別子と一致する移転元識別子を処理可能な第２の部分ネットワークに送信するステップとを含み、前記第２の部分ネットワークを構成するノードが、前記第２のトランザクションを受信するステップと、前記第２のトランザクションを含む第２のブロックを生成するステップと、前記第２のブロックの採択についての前記第２の部分ネットワークにおける合意形成後、前記第２のトランザクションの移転先識別子の資産の状態を更新するステップとを含むことを特徴とする。

[0015] また、本発明の第１０の態様は、資産の移転を表すトランザクションを記

憶するための複数の部分ネットワークを有する分散ネットワークであって、前記複数の部分ネットワークのうちの第１の部分ネットワーク及び第２の部分ネットワークを備え、前記第１の部分ネットワークを構成するノードが、前記第１の部分ネットワークで処理可能な移転元識別子から前記第１の部分ネットワークで処理可能ではない移転先識別子への資産の移転を表す第１のトランザクションを受信して、前記第１のトランザクションを含む第１のブロックを生成し、前記第１のブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記移転元識別子の資産の状態を更新し、前記第１のブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記第１のトランザクションにより表される前記移転先識別子への前記資産の移転を反映させるための第２のトランザクションを、前記第１のトランザクションの前記移転先識別子と一致する移転元識別子を処理可能な第２の部分ネットワークに送信し、前記第２の部分ネットワークを構成するノードが、前記第２のトランザクションを受信して、前記第２のトランザクションを含む第２のブロックを生成し、前記第２のブロックの採択についての前記第２の部分ネットワークにおける合意形成後、前記第２のトランザクションの移転先識別子の資産の状態を更新することを特徴とする。

発明の効果

[0016] 本発明の一態様によれば、分散ネットワークを複数の部分ネットワークにより構成し、各部分ネットワークにおいて処理可能な移転元識別子を定めておくことによって、トランザクションの並列処理を行い、同時に複数のトランザクションの処理が実行可能となる。

図面の簡単な説明

[0017] [図1]本発明の一実施形態にかかる分散ネットワークを示す図である。

[図2]本発明の一実施形態にかかる通常トランザクションの模式図である。

[図3]本発明の一実施形態にかかるトランザクションを記憶する方法の流れを説明するための図である。

[図4]本発明の一実施形態にかかるペグトランザクションの模式図である。

[図5]本発明の一実施形態における合意形成処理を説明するための図である。

[図6]本発明の一実施形態における合意形成のための鍵生成方法の流れ図である。

[図7]本発明の一実施形態におけるブロックの採択についての確定方法の流れ図である。

[図8]本発明の別実施形態にかかるペグトランザクションの模式図である。

[図9]本発明の別実施形態にかかるマークルツリーデータを説明するための図である。

[図10]本発明の別実施形態にかかるペグトランザクションの模式図である。

発明を実施するための形態

[0018] 以下、図面を参照して本発明の実施形態を詳細に説明する。

[0019] 図１は、本発明の一実施形態にかかる分散ネットワークを示す。分散ネットワーク１００は、分散ネットワーク１００上に構築されたデータベースに記憶すべきトランザクションにおける資産の移転元に応じて動作が異なる複数の部分ネットワークを有する。図１では、第１の部分ネットワーク１１０と、第２の部分ネットワーク１２０と、第３の部分ネットワーク１３０とを示しているが、部分ネットワーク数は３に限られるものではない。

[0020] 各部分ネットワークは、複数のノードにより構成されており、各ノードは、通信インターフェースなどの通信部１１１Ａと、プロセッサ、ＣＰＵ等の処理部１１１Ｂと、メモリ、ハードディスク等の記憶装置又は記憶媒体を含む記憶部１１１Ｃとを備え、各処理を行うためのプログラムを実行することによって構成することができる。各ノードは、１又は複数の装置ないしサーバを含むことがあり、また当該プログラムは１又は複数のプログラムを含むことがあり、また、コンピュータ読み取り可能な記憶媒体に記録して非一過性のプログラムプロダクトとすることができる。

[0021] ユーザー端末１４０では、資産２０３の移転元アドレスなどの移転元識別子２０１から移転先アドレスなどの移転先識別子２０２への移転を表すトランザクションが生成される。こうしたトランザンクションの生成をするため

のアプリケーションがユーザー端末１４０にインストールされるか、インターネットなどのコンピュータ・ネットワークを介してユーザー端末１４０において利用可能である。

[0022] 図３を参照して、本実施形態にかかる資産の移転を表すトランザクションを記憶する方法を説明する。まず、ユーザー端末１４０において仮想通貨等の資産２０３の移転元識別子２０１から移転先識別子２０２への移転を表すトランザクション２００が生成される（Ｓ３０１）。トランザクション２００には、移転元識別子２０１、移転先識別子２０２、移転される資産２０３の額が記述され、移転元識別子２０１に関連づけられた秘密鍵による署名２０４が付加される。たとえば、移転元識別子２０１の秘密鍵は、ユーザー端末１４０又はユーザー端末１４０のユーザーのみがアクセス可能に管理されており、当該ユーザーのみが移転先識別子２０１からの資産の移転を正当に実行可能である。

[0023] 次に、ユーザー端末１４０は、分散ネットワーク１００に向けてトランザクション２００の記録依頼要求を送信する（Ｓ３０２）。各部分ネットワークには、受け取ったトランザクションを自ら処理可能な移転元識別子の値又は範囲が設定されているところ、本実施形態において、ユーザー端末１４０のアプリケーションは、移転元識別子と各部分ネットワークが処理可能な移転元識別子の値又は範囲との対応づけを参照して、トランザクション２００の記録依頼要求の送信先を判定する。図１及び２の例では、第１の部分ネットワーク１１０がトランザクション２００を受信することとなる。

[0024] より詳細には、第１の部分ネットワーク１１０にトランザクション２００を送信するという場合、第１の部分ネットワーク１１０を構成する１又は複数のノードに対して送信を行う。トランザクション２００を受信したノード１１１は、その記憶部１１１Ｃ又は当該ノードからアクセス可能な記憶媒体又は記憶装置にトランザクション２００をその後処理するため記憶する。必要に応じてトランザクション２００を受信したノード１１１は、第１の部分ネットワーク１１０を構成するその他のノードにトランザクション２００を

送信し、第１の部分ネットワーク１１０を構成する複数のノードのうち、ブロック採択の合意形成に参加するノードにおいて記憶されることとなる。

[0025] そして、第１の部分ネットワーク１１０を構成するいずれかのノード１１１が、それまでに記憶したトランザクションのうちの１又は複数のトランザクションを含むブロックを生成し、その採択のための第１の部分ネットワーク１１０における合意形成処理を行う（Ｓ３０３）。合意形成が行われた場合、合意形成に参加する各ノードは、各ノードが記憶するブロックチェーンに当該ブロックを追加する。第１の部分ネットワーク１１０の各ノードは、第１の部分ネットワーク１１０で処理可能な移転元識別子の秘密鍵に対応する公開鍵を記憶しており、トランザクションの受信時又はブロックの生成時に署名２０４の有効性を検証することが可能である。第１の部分ネットワーク１１０において行われる合意形成処理の詳細については後述する。公開鍵は、事前に各ノードが記憶しているのではなく、トランザクション２００が当該トランザクション２００に付加された署名２０４の秘密鍵に対応する公開鍵を含んでいるか、トランザクション２００に当該公開鍵が付加されているか、署名２０４から計算可能であってもよい。

[0026] 各ノードは、ブロックチェーンに加えて、各ノードが処理可能な移転元識別子に関連づけられた資産の状態を保持する識別子と資産の状態との対応づけを記憶しており、ブロックチェーンに当該ブロックを追加した後、追加されたブロックに含まれる１又は複数のトランザクションに記述された移転元識別子からの資産の移転を記録する（Ｓ３０４）。当該対応づけは、テーブル形式に限るものではないが便宜上「アセットテーブル」と呼ぶことがある。また、対応づけは、各ノードからアクセス可能な記憶媒体又は記憶装置に記憶してもよい。

[0027] より詳細には、一例として、分散ネットワーク１００で処理可能な移転元識別子及び移転先識別子が「Ａ」で始まる１０桁の記号列、「Ｂ」で始まる１０桁の記号列、そして「Ｃ」で始まる１０桁の記号列である場合を考える。そして、第１の部分ネットワーク１１０は「Ａ」で始まる移転元識別子、

第２の部分ネットワーク１２０は「Ｂ」で始まる移転元識別子、第３の部分ネットワーク１３０は「Ｃ」で始まる移転元識別子を処理可能と設定されているものとする。第１の部分ネットワーク１１０において「Ａ１３ａｆｂ３ｓｄｆ」という移転元識別子２０１が記述されたトランザクション２００を含むブロックに関する合意形成がなされたことを受けて、第１の部分ネットワーク１１０の各ノード１１１は、それぞれが記憶するアセットテーブル内の識別子「Ａ１３ａｆｂ３ｓｄｆ」の資産残高を更新する。具体的には、移転元識別子「Ａ１３ａｆｂ３ｓｄｆ」の資産残高を１０ＢＴＣ減少させる。

[0028] 次いで、追加されたブロックを生成したノード又は第１の部分ネットワークのその他のノードが、追加されたブロックに含まれる１又は複数のトランザクションのうち移転先識別子が第１の部分ネットワーク１１０で処理可能な移転元識別子に一致しないトランザクションに対応するトランザクション４００を、当該移転先識別子が自ネットワークにおいて処理可能な移転元識別子と一致する部分ネットワークに送信する（Ｓ３０５）。

[0029] ここで、トランザクション４００の生成がアセットテーブルの更新後に行われるものとして説明したが、これらは逆にすることも考えられる。合意形成処理（Ｓ３０３）に、ブロックに含まれる各トランザクションの移転元識別子から移転される資産の額が当該移転元識別子の残高以上であることの検証が含まれる場合には順序を逆にしてもよいが、含まれない場合にはアセットテーブルの更新処理（Ｓ３０４）に、移転される資産の額が残高以上であることの検証を含め、検証結果が肯定的であることを条件にトランザクション４００の送信が実行されるようにしてもよい。

[0030] 図２に示したトランザクション２００に対応する図４のトランザクション４００を例にすると、トランザクション４００は、第１の部分ネットワーク１１０に記憶されたトランザクション２００により表される資産２０３の移転を、移転先識別子２０２と一致する移転元識別子を処理可能な第２の部分ネットワーク１２０において反映させるものであり、移転元識別子４０１、移転先識別子４０２、移転される資産４０３の額が記述されている。図２の

トランザクション２００とは異なり、図４のトランザクション４００においては、付加される署名４０４が、トランザクション２００を含むブロックが第１の部分ネットワーク１１０においてその採択について合意形成がなされたこと、すなわち、ブロックチェーンに追加されたことを示す署名である。図４においては、署名４０４を「Ａ」として図示している。署名４０４の詳細は後述する。

[0031] 以下において、トランザクション４００は部分ネットワーク間での資産の状態の整合性を保つためのものであり、いわゆるペグさせるものであるため、「ペグトランザクション」と呼ぶことがあり、署名４０４は「ペグ署名」と呼ぶことがある。

[0032] ペグトランザクション４００を受信した第２の部分ネットワーク１２０では、ペグトランザクション４００を含むブロックをいずれかのノードが生成し、当該ブロックの採択についての合意形成処理（Ｓ３０６）がなされた後に各ノードのブロックチェーンに追加される。第２の部分ネットワーク１２０の各ノードは、第２の部分ネットワーク１２０で処理可能な移転元識別子の秘密鍵に対応する公開鍵を記憶するとともに、他の部分ネットワークによるペグ署名に関連づけられた公開鍵を記憶している。当該公開鍵によってトランザクション４００のペグ署名４０４を有効なものとして検証することで、トランザクション４００がペグトランザクションであることを判定することができる。公開鍵は、事前に各ノードが記憶しているのではなく、ペグトランザクション４００が当該トランザクション４００に付加された署名４０４の秘密鍵に対応する公開鍵を含んでいるか、トランザクション２００に当該公開鍵が付加されていてもよい。いずれにしても、各部分ネットワークは、ペグトランザクション４００に付加される署名４０４の秘密鍵に対応する公開鍵が、いずれの部分ネットワークで署名可能な秘密鍵に対応するものであるのか、換言すれば、公開鍵のいわゆる保有者がいずれの部分ネットワークであるのかを確認可能であるものとする。

[0033] ある部分ネットワークが受信したトランザクションが通常のトランザクシ

ョン２００であるかペグトランザクション４００であるかを区別するためには、上記のように署名の検証に用いた公開鍵によって判定することが考えられるが、識別子に基づいて判定することも考えられる。すなわち、移転元識別子が自ネットワークにおいて処理可能な移転元識別子ではなく、移転先識別子が自ネットワークにおいて処理可能な移転元識別子のいずれかと一致する場合、当該トランザクションをペグトランザクション４００と判定することが可能である。

[0034] ブロックが追加された後、当該ブロックに含まれるペグトランザクション４００について、各ノードはペグトランザクション４００の移転先識別子４０２の資産残高を更新して資産２０３の移転を記録する（Ｓ３０７）。通常トランザクション２００では、上述したように資産２０３の移転元識別子２０１の資産残高を更新するところ、ペグトランザクション４００では、移転先識別子４０２の資産残高を更新する。ペグトランザクション４００の移転先識別子４０２は第２の部分ネットワーク１２０で処理可能な移転元識別子のいずれかと一致し、第２の部分ネットワーク１２０の各ノードは、各ノードの記憶部又は各ノードからアクセス可能な記憶媒体又は記憶装置に、自ネットワークで処理可能な移転元識別子と当該識別子に関連づけられた資産の状態との対応づけを参照し、更新することができる。

[0035] 以上のように、分散ネットワークを複数の部分ネットワークにより構成し、各部分ネットワークにおいて処理可能な移転元識別子を定めておくことによって、トランザクションの並列処理を行い、同時に複数のトランザクションの処理が実行可能となる。よって、単位時間当たりのトランザクション処理速度を大幅に向上させることができる。

[0036] 上述の説明では、ユーザー端末１４０が用いるアプリケーションにおいて、移転元識別子と処理可能な移転元識別子の値又は範囲との対応づけを参照して、トランザクション２００の記録依頼要求の送信先を判定するものとして記述したが、１又は複数の部分ネットワークに向けて送信をして、トランザクション２００が受信した部分ネットワークにおいて自ら処理可能なトラ

ンザクションでなければトランザクション２００を処理可能な部分ネットワークに転送してもよい。また、分散ネットワーク１００に転送ノード（図示せず）を設けて、転送ノードにおいて最初にユーザー端末１４０から送信されたトランザクション２００を受信し、送信元識別子２０１の値に応じてトランザクション２００を処理可能な部分ネットワークを判定してもよい。

[0037] また、上述の説明では、ペグトランザクション４００の送信先を第１の部分ネットワーク１１０において定めるものとして記述したが、通常トランザクション２００の送信先と同様の態様で送信を行うことが考えられる。

[0038] また、上述の説明では、資産２０３の額は特段制約を課していないが、正の値として、トランザクション２００の検証の際に残高不足があれば無効なトランザクションとして処理することが好ましい。負の値とした場合、すなわち移転元識別子２０１が資産２０３を受け取る場合には、移転先識別子２０２の資産残高を第１のネットワーク１１０のアセットテーブルでは管理していないことから、残高不足か否かを検証することが出来ず、第１の部分ネットワーク１１０において当該トランザクションを含むブロックが追加されたにも関わらず第２の部分ネットワーク１２０では移転先識別子２０２の残高不足によって無効と処理される恐れが生じる。

[0039] なお、「××のみに基づいて」、「××のみに応じて」、「××のみの場合」というように「のみ」との記載がなければ、本明細書においては、付加的な情報も考慮し得ることが想定されていることに留意されたい。また、一例として、「ａの場合にｂする」という記載は、明示した場合を除き、「ａの場合に常にｂする」ことを必ずしも意味しないことに留意されたい。

[0040] また、念のため、なんらかの方法、プログラム、端末、装置、サーバ又はシステム（以下「方法等」）において、本明細書で記述された動作と異なる動作を行う側面があるとしても、本発明の各態様は、本明細書で記述された動作のいずれかと同一の動作を対象とするものであり、本明細書で記述された動作と異なる動作が存在することは、当該方法等を本発明の各態様の範囲外とするものではないことを付言する。

[0041] 合意形成の詳細

部分ネットワークにおける合意形成は、さまざまな合意アルゴリズムの下で行うことができるところ、一例として、合意形成に参加するＮ個（Ｎは２以上の整数）のノードのうちｋ個（ｋは２≦ｋ≦Ｎを満たす整数）のノードによる署名を必要とするものが挙げられる。Ｎ＝５、ｋ＝３の例を考えれば、これは合意形成に参加するノードの過半数による署名が必要となることを意味する。そして、合意形成がなされ、合意形成対象のブロックについてその採択が確定したことを示すためには、根拠としてｋ個以上の署名を付すことが必要となる。

[0042] このようにｋ個のノードによる署名が当該合意アルゴリズムにおける所定の条件を満たすことのできるノードの組み合わせはＮ及びｋの値によっては数多く考えられ、このことは、合意が形成されたブロックについて、署名の取り扱いを複雑にしている側面がある。たとえば、あるブロックの署名を事後的に検証（ｖｅｒｉｆｙ）するためには、当該ブロックに付された複数の署名が所定の条件を満たしているか否かを個別に確認しなければならないからである。そこで、以下に述べるような単一の署名によって、部分ネットワークにおいて、ブロックの採択にかかる合意がなされたことを示すことが好ましい。このことは、ブロックの採択についての合意形成だけでなく、ペグトランザクション４００にペグ署名４０４を付加するための合意形成についても同様である。

[0043] 図５に示すネットワーク５００は、例示としてＮが５であり、第１のノード５１０、第２のノード５２０、第３のノード５３０、第４のノード５４０及び第５のノード５５０を有する。各ノードは、第１のノード５１０について図示するように、通信インターフェースなどの通信部５１１と、プロセッサ、ＣＰＵ等の処理部５１２と、メモリ、ハードディスク等の記憶装置又は記憶媒体を含む記憶部５１３とを備えるコンピュータであり、所定のプログラムを実行することによって、以下で説明する各処理を実現することができ、当該ノード５１０は、１又は複数の装置ないしサーバを含むことがあり、

また当該プログラムは、１又は複数のプログラムを含むことがあり、また、コンピュータ読み取り可能な記憶媒体に記録して非一過性のプログラムプロダクトとすることができる。その他のノードについても、そのハードウェアの構成は同様である。以下では第１のノード５１０を中心に説明するが、他のノードにおいても、同様の処理を行い得る。また、合意形成に参加しないノードがネットワーク５００に含まれることもある。

[0044] 所定のプログラムには、合意アルゴリズムにかかるルール及びセットアップにかかるルールが定められており、記憶部５１３又は第１のノード５１０からネットワークを介してアクセス可能な記憶装置又は記憶媒体に記憶しておくことができる。

[0045] 合意形成に参加するＮ個のノードが、互いに通信可能な状態から、ブロックの採択にかかる合意形成を実行可能な状態に遷移するために実行させるべきプロセスを「セットアップ」と呼ぶ。セットアップは、ネットワーク５００の外部又は内部においてセットアップの要求を受けて開始され、図５では、外部から当該要求が送信される例を示している。当該要求には、合意形成に必要となる署名の数ｋを含むことができ、また予めセットアップにかかるルールの中で定めておいてもよい。また、当該要求には、合意形成に参加するＮ個のノードの指定を含むことができ、またこの指定は予めセットアップにかかるルールの中で定めておいてもよい。

[0046] いずれかの形でＮ及びｋの値が定まり、セットアップ・プロセスの実行が進むと、各ノードは、合意形成に参加するノード全体に割り当てられた１個の公開鍵、合意形成に参加する各ノードに割り当てられたＮ個の公開鍵シェア、そして当該ノードに割り当てられた１個の秘密鍵シェアを保持することとなる。また、各ノードは、Ｎ及びｋの値又はｋ／Ｎの値も保持することとなる。Ｎの値は、公開鍵シェアの数から求めることもできる。

[0047] 秘密鍵と公開鍵は、当該秘密鍵により署名した平文を当該公開鍵により検証できるという関係にあり、秘密鍵シェアとそれに対応する公開鍵シェアについても同様である。ここで、「秘密鍵シェア」とは、Ｎ個の一組の秘密鍵

シェアのうち所定の数ｋ個の秘密鍵シェアによる署名を用いて秘密鍵による署名を生成可能であるように、生成された一組の秘密鍵シェアのうちのいずれかを指す。したがって、当該秘密鍵を知ることなく、ｋ個の秘密鍵シェアに基づいて公開鍵に対応する署名を生成し、合意形成の対象であるブロックに当該署名を付加することができる。付加された署名は、公開鍵によってその検証可能である。

[0048] 図５の例についてさらに説明すると、ネットワーク５００全体に割り当てられる１個の公開鍵をＰＫ（Ｐｕｂｌｉｃ　Ｋｅｙの略）、当該公開鍵に対応する秘密鍵をＳＫ（Ｓｅｃｒｅｔ　Ｋｅｙの略）、第１のノード５１０、第２のノード５２０、第３のノード５３０、第４のノード５４０、第５のノード５５０のそれぞれに割り当てられる公開鍵シェア及び秘密鍵シェアをそれぞれＰＫ１及びＳＫ１、ＰＫ２及びＳＫ２、ＰＫ３及びＳＫ３、ＰＫ４及びＳＫ４、ＰＫ５及びＳＫ５と表記する。セットアップ後には、たとえば第１のノードは、ＰＫ、ＰＫ１乃至ＰＫ５及びＳＫ１をその記憶部５１３又は当該ノードと通信可能な記憶装置又は記憶媒体に記憶していることになる。記憶されたこれらのデータは、後の合意形成又はその確定プロセスにおいて当該ノードからアクセス可能となる。

[0049] ここで、公開鍵ＰＫは、最終的に付加される署名の検証に必要となるところ、セットアップの段階では生成しない場合もある。署名の検証を行うノード又は装置が検証時に公開鍵ＰＫを有していればよく、初期設定の時点で必ずしもネットワーク５００の各ノードが有していることは必要ではないからである。

[0050] 図６に、本実施形態にかかるこれらの鍵生成方法の流れを示す。ここでは一例として、（ｋ－１）次多項式ｆ（ｘ）を考え、ｆ（ｘｉ）の値（ｉはｉ番目のノードを表す１からＮの整数であり、ｘｉは任意の整数）を各ノードに対する秘密鍵シェアＳＫｉとするものとする。

[0051] まず、ｉ番目のノードは、ａｉｍ（ｍは０からｋ－１の整数）を係数とする（ｋ－１）次多項式ｆｉ（ｘ）を決定する（Ｓ６０１）。各ノードは、セ

ットアップルールに従って、ａｉｍを選択ないし生成して記憶することによってｆｉ（ｘ）を計算することができる。

[0052] [数1]

$$f_i(x) = \sum_{m=0}^{k-1} a_{im} x^m$$

[0053] 次に、ｉ番目のノードは、巡回群Ｇ１の生成元ｇ１を用いて、０からｋ－１の各ｍにおけるａｉｍ・ｇ１の値又はそれを含むメッセージを他のノードに送信する（Ｓ６０２）。また、ｉ番目のノードは、ｊ番目のノード（ｊは１からＮの整数）に対して、ｆｉ（ｘｊ）の値又はそれを含むメッセージを送信する。ここで、ｆｉ（ｘｊ）の送信は、ｍ及びａｉｍ・ｇ１より前に送信してもよく、またこれと同時に送信してもよい。

生成元ｇ１は、各ノードに記憶されて既知であるか、いずれかのノードから合意形成に参加するＮ個のノードに与えられることによって、Ｎ個のノードそれぞれがアクセス可能であり、用いることができるものとする。同様に、ｉ番目のノードに秘密鍵シェアｆ（ｘｉ）を与える整数ｘｉの値についても、Ｎ個のノードそれぞれがアクセス可能であり、用いることができるものとする。たとえば、これらの値は、各ノードの記憶部又は各ノードからアクセス可能な記憶装置又は記憶媒体に記憶しておけばよい。

[0054] そして、ｊ番目のノードにおいて、１からＮのｉについてｆｉ（ｘｊ）を加算して、ｆ（ｘｊ）、すなわち秘密鍵シェアＳＫｊを算出する（Ｓ６０４）。多項式ｆ（ｘ）を次式のように定義すれば、

[0055] [数2]

$$f(x) = \sum_{m=0}^{k-1} a_m x^m$$

[0056] これは、いずれのノードに対しても知らされていないものの、次式のようにｆ（ｘｊ）を考えることによって、ｆ（ｘ）自体を各ノードが知ることなく、ｆ（ｘｊ）の値を各ノードにおいて算出可能である。

[0057]

[数3]

$$f(x_j)=\sum_{i=1}^{N} f_i(x_j)=\sum_{i=1}^{N}\left(\sum_{m=0}^{k-1} a_{im}\,{x_j}^m\right)=\sum_{m=0}^{k-1}\left(\sum_{i=1}^{N} a_{im}\right){x_j}^m=\sum_{m=0}^{k-1} a_m {x_j}^m$$

[0058] また、各ノードは、ｍ及びａｉｍ・ｇ１を自ノードにおいては算出可能であるとともに他ノードのものについては既に受信していることから、次式に従って、公開鍵シェアＰＫｊとしてＳＫｊ・ｇ１を算出することができる（Ｓ２０６）。

[0059] [数4]

$$SKj\cdot g_1=f(x_j)\cdot g_1=\left(\sum_{m=0}^{k-1} a_m {x_j}^m\right)\cdot g_1=\left(\sum_{m=0}^{k-1}\left(\sum_{i=1}^{N} a_{im}\right){x_j}^m\right)\cdot g_1=\sum_{m=0}^{k-1} {x_j}^m\left(\sum_{i=1}^{N} a_{im}\cdot g_1\right)$$

[0060] この式による公開鍵シェアＰＫｉの算出は、ｍ及びａｉｍ・ｇ１並びにｘｉがすべてのｉについて既知であることから、ｆ（ｘ）を知ることなくすべてのノードについて可能である。

[0061] このようにして得られた公開鍵シェアと秘密鍵シェアのペアは、合意形成対象のブロックのハッシュ値ｈを与えるハッシュ関数を任意のデータからｇ２を生成元とする巡回群Ｇ２への写像とし、ｈにＳＫｊを乗じたＳＫｊ・ｈを署名ｓｊとして、Ｇ１×Ｇ２からｇＴを生成元とする巡回群ＧＴへの写像ｅであって、次式を満たす双線形写像を定義することによって、暗号方式として成り立つことが分かる。ここで、ａ及びｂは任意の整数である。

[0062] [数5]

$$e(a\cdot g_1, b\cdot g_2)=\ g_T^{ab}$$

[0063] すなわち、ｉ番目のノードにおいて、合意形成対象のブロックのハッシュ値ｈ及び署名ｓｊをｊ番目のノードより受け取ったとき、上述のアルゴリズムによって既知の公開鍵シェアＰＫｊを用いて、

[0064] [数6]

$$e(PKj,h)=\ e(SKj\cdot g_1,h)=e(g_1,SKj\cdot h)=e\left(g_1,s_j\right)$$

[0065] となるため、既知の生成元ｇ１を用いて、ｊ番目のノードより受け取った署名ｓｊの検証を行うことができる。ハッシュ値は、セットアップルールの中にハッシュ関数を定めておくことで、各ノードにおいて、合意形成対象のブロックから算出してもよい。

[0066] 生成元ｇ１、ｇ２の位数は素数であることが好ましく、各生成元により生成される巡回群Ｇ１、Ｇ２の元の数は一例として３２バイト、すなわち２５６ビット程度以上であることが好ましい。ここで、巡回群Ｇ１、Ｇ２における演算は加法的に記述しており、たとえば、生成元ｇ１をａ回繰り返し加算する演算をａ・ｇ１を表記し、「ａを生成元ｇ１に乗じる」と呼ぶ。なお、ａｘのように整数の集合の元同士の乗算も本明細書において表記として用いられるが、これは巡回加法群における乗算とは異なるものであることを念のため付言する。

[0067] 上述の説明では、（ｋ－１）次多項式関数ｆ（ｘ）の値を秘密鍵シェアとして定め、当該秘密鍵シェアを巡回群の生成元に乗じた値を公開鍵シェアとする署名方式を前提としているところ、Ｎ個の一組の秘密鍵シェアのうち所定の数ｋ個の秘密鍵シェアによる署名を用いて秘密鍵による署名を生成可能であれば、異なる署名方式を採用することもできる。また、この際には、ネットワーク５００のいずれかのノード又はその外部のノードが生成した一組の秘密鍵シェアを各ノードに与えるのではなく、各秘密鍵シェアが各ノードにおいて分散して生成可能であることが望ましい。

[0068] また、上述の説明では、ｊ番目のノードにおける公開鍵シェアＰＫｊ及び秘密鍵シェアＳＫｊを例に説明したが、ｉ番目のノードを中心にそこで行われる処理を記述する場合には、当然ではあるが、添え字が適宜変更されることを付言する。

[0069] 図７に、本発明の一実施形態にかかるブロックの採択についての確定方法の流れを示す。セットアップが完了した状態から、第１のノード５１０が、ブロックを生成して当該ブロックを含む第１のメッセージを合意形成に参加するＮ個のノードに送信する（Ｓ７０１）。送信ノードも自ら当該ブロック

を受信することができる。ここで、ノード間では、メッセージが直接的又は間接的に送受信可能であり、ネットワーク１００を構成する他のノードに合意形成に関連するデータを伝え、また、他のノードからデータを受け取ることができる。

[0070] 第１のメッセージを受信した各ノードは、それぞれが有するプログラムに定められた合意形成のルールに基づいて、当該ブロックの有効性を評価する（Ｓ７０２）。有効性の評価の詳細は、送信者が正当な送信ノードであるか、ブロックのデータ形式が用途に応じた所定の形式その他の所定の条件を満たしているか、分岐が生じていないかなど、さまざまなルールを含むことができ、ノードによって異なるルールが存在してもよい。また、有効性の評価を行う上で、他のノードとのメッセージの送受信を必要としてもよい。

[0071] 有効と評価された場合、当該ノードは、当該ノードがアクセス可能な秘密鍵シェアｆ（ｘｉ）による合意形成対象のブロックのハッシュ値ｈに対する署名ｓｉを有する第２のメッセージを各ノードに送信する（Ｓ７０３－１）。署名は、当該ノードに与えられた秘密鍵シェアをハッシュ値に乗じることによって行うことができる。送信先には、自ノードを含めてもよい。無効と評価された場合には、当該ブロックは却下される（Ｓ７０３－２）。

[0072] ｊ番目のノードにおいてｋ個の署名が集まった後、当該ノードは、これらの署名を合成して、公開鍵ＰＫに対応する署名を生成する（Ｓ７０４）。具体的には、各ノードは、定期的又は断続的に、ｋ／Ｎの条件が充足されたか否かを判定し、充足された場合には、受け取ったｋ個又はｋ個以上の秘密鍵シェアによる署名から、ｆ（０）・ｈを公開鍵ＰＫに対応する秘密鍵ＳＫによる署名ＳＫ・ｈとして算出することができる。ここでは、（ｋ－１）次多項式ｆ（ｘ）は、ｋ個以上の点（ｘｉ，ｆ（ｘｉ））が既知であれば一意に定めることができ、ｆ（０）の値を未知の秘密鍵ＳＫの値と考えられることを用いている。ｋ個の署名からｋ個の点（ｘｉ，ｆ（ｘｉ）・ｈ）が既知であれば、関数ｆ（ｘ）・ｈが定まることになる。ｆ（０）・ｈの算出は、たとえば、ラグランジュ補間を用いて行うことができる。

[0073] なお、公開鍵ＰＫは、ｋ個以上の点（ｘｊ，ＰＫｊ）＝（ｘｊ，ｆ（ｘｊ）・ｇ１）から、たとえば、ラグランジュ補間によって算出可能であり、これはセットアップの段階で行っておいて必要に応じて配布しておいてもよいし、署名の検証を行うネットワーク５００の内部又は外部のノード又は装置が検証時又は検証前にｋ個の公開鍵シェアＰＫｊに基づいて生成してもよい。

[0074] そして、必要であれば、生成された単一の署名ＳＫ・ｈが他のノードにブロードキャスト乃至送信される（Ｓ７０５）。既にｋ個以上のノードによる有効性の評価が済んでいることから、合成に成功した時点でブロックを当該ノードが有するブロックチェーンに追加可能としてもよいが、一例として、合成に成功したノードは他のノードに当該合成後の署名を送信し、そして、所定の数以上の合成後の署名を受け取ったことに応じて、各ノードはブロックを追加可能としてもよい。

[0075] 最後に、合意形成対象のブロックは、署名ＳＫ・ｈが付加されて各ノードのブロックチェーンに追加される（Ｓ７０６）。これにより、当該ブロックのネットワーク７００における採択が確定する。

[0076] 上述の説明では、各ノードに１つの秘密鍵シェアが与えられる場合を考えているが、１つのノードに与えるシェア数を複数とすることも考えられる。また、上述の説明では、有効性の評価対象となるブロックの詳細について触れていないが、１又は複数のトランザクションを含むものとすることができ、あるいは、任意の１又は複数のデータを含むとすることもできる。そして、必ずしもチェーンを形成しない１又は複数のデータに対する複数のノードを有するコンピュータ・ネットワークによる有効性の評価につき、本発明の精神を適用することも可能である。

[0077] ペグ署名の詳細

ペグ署名４０４は、第１の部分ネットワーク１１０におけるブロックの採択にかかる合意形成に用いられる合意アルゴリズムと同一又はこれに対応する合意アルゴリズムによって生成することができる。あるいは、第１の部分

ネットワーク１１０におけるブロックの採択で採用される合意アルゴリズムとは異なる合意アルゴリズムによって生成することができる。

[0078] いずれの場合においても、ペグ署名４０４は、一例として、ペグトランザクション４００又はその一部のハッシュ値に対する１又は複数の秘密鍵による１又は複数の署名とすることができる。ペグトランザクション４００を受信した第２の部分ネットワーク１２０では、ペグトランザクション４００の受信時又はペグトランザクション４００を含むブロックの生成時に、ペグ署名４０４の有効性を検証する。

[0079] この方式であると、ブロックの採択のために一度合意形成がなされているにもかかわらず、当該ブロックに含まれる、移転先識別子が第１の部分ネットワーク１１０で処理可能な移転元識別子に一致しないすべてのトランザクションについて、それらに対応するペグトランザクション４００を生成し、それぞれについて第１の部分ネットワーク１１０として署名するための合意形成を行わなければならない。部分ネットワークの数が増えれば増えるほど、移転先識別子が第１の部分ネットワーク１１０で処理可能な移転元識別子に一致しないトランザクションの数も増え、合意形成処理が増加することとなる。

[0080] そのため、別方式では、マークルツリーを用いる。ペグ署名４０４を生成するために、まず、第１の部分ネットワーク１１０において追加されたブロックに含まれる複数のトランザクション又は当該トランザクションのうちの移転先識別子が第１の部分ネットワーク１１０で処理可能な移転元識別子に一致しないトランザクションに基づくマークルツリーのマークルルートを算出する。そして、当該マークルルートに対する秘密鍵による署名をペグ署名４０４とする。

[0081] ペグトランザクション４００は、移転先識別子が第１の部分ネットワーク１１０で処理可能な移転元識別子に一致しない通常トランザクション２００に対応し、ペグ署名４０４に加えて、ペグ署名４０４の有効性を検証するために必要な１又は複数のノードにかかるマークルツリーデータＭが付加され

る。ここで、本明細書において「マークルツリーデータ」とは、マークルツリーを構成する１又は複数のノードのデータであり、具体的には、１又は複数のハッシュ値である。ペグトランザクション４００は、通常トランザクション２００に一致するか通常トランザクション２００を含むデータであり、ペグトランザクション４００又はその一部のハッシュ値を生成し、当該ハッシュ値とペグトランザクション４００と共に受信したマークルツリーデータＭとを用いてマークルルートを算出して、ペグ署名４０４が当該マークルルートに対する署名であるか否かを第１の部分ネットワーク１１０の公開鍵を用いて検証を行うことができる。一例として、暗号方式はＥＣＤＳＡを用いることができる。ＥＣＤＳＡの場合には、公開鍵を署名から計算可能である。

[0082] 図９に、マークルツリーの一例を示す。第１の部分ネットワーク１１０において、４つのトランザクションを含むブロックが追加されたものとする。そして、第２のトランザクションｔｘ２に対応するペグトランザクション４００が第２の部分ネットワーク１２０に送信されるものとする。この場合、ペグトランザクション４００又はその一部のハッシュ値として第２のトランザクションｔｘ２のハッシュ値が得られるから、ノード１のハッシュ値とノード６のハッシュ値とをマークルツリーデータＭとしてペグトランザクション４００に付加しておけば、第２の部分ネットワーク１２０においてノード７のマークルルートを算出することができる。

[0083] 第１の部分ネットワーク１１０において追加されたブロックに対する署名が、当該ブロックのブロックヘッダに対する署名であり、当該署名に当該ブロックのマークルツリーのマークルルートが含まれていれば、ブロックに対する署名をそのままペグ署名４０４として用いることができる。ペグトランザクション４００にはこの場合、マークルツリーデータＭに加えて、当該ブロックヘッダ又は当該ブロックヘッダからマークルツリールートを除いたデータＢを付加し、第２の部分ネットワーク１２０において、ブロックヘッダを生成して、ペグ署名４０４が当該ブロックヘッダに対する署名であるか否

かを第１の部分ネットワーク１１０の公開鍵を用いて検証を行うことができる。

[0084] さらに別方式として、第１の部分ネットワーク１１０において追加されたブロック全体をペグトランザクション４００として第２の部分ネットワーク１２０に送信することが考えられる。この場合、当該ブロックには、移転先識別子が、第２の部分ネットワーク１２０で処理可能な移転元識別子に一致しないトランザクションが含まれるため、不必要なデータを送信することとなるものの、第１の部分ネットワーク１１０におけるペグトランザクション４００への追加的な署名を省略し、ブロックの採択についての合意形成において付加された署名をそのままペグ署名４０４と考えることができる。

[0085] この方式では、当該ブロック（「第１のブロック」に相当）を受信した第２の部分ネットワーク１２０において、当該ブロックに含まれる、移転先識別子が、第２の部分ネットワーク１２０で処理可能な移転元識別子に一致する１又は複数のトランザクション又はこれらの対応するトランザクションを含むブロック（「第２のブロック」に相当）を生成し、合意形成の対象とする。

符号の説明

[0086] １００　分散ネットワーク

１１０　第１の部分ネットワーク

１１１　第１の部分ネットワークのノード

１１１Ａ　通信部

１１１Ｂ　処理部

１１１Ｃ　記憶部

１２０　第２の部分ネットワーク

１３０　第３の部分ネットワーク

１４０　ユーザー端末

２００　通常トランザクション

２０１　移転元識別子

２０２　移転先識別子

２０３　資産

２０４　署名

４００　ペグトランザクション

４０１　移転元識別子

４０２　移転先識別子

４０３　資産

４０４　ペグ署名

５００　ネットワーク

５１０　第１のノード

５１１　通信部

５１２　処理部

５１３　記憶部

５２０　第２のノード

５３０　第３のノード

５４０　第４のノード

５５０　第５のノード

Ｂ　ブロックヘッダ又は又はブロックヘッダからマークルツリールートを除いたデータ

Ｍ　マークルツリーデータ

１乃至７　マークルツリーのノード

請求の範囲

[請求項1] 複数の部分ネットワークを有する分散ネットワークに資産の移転を表すトランザクションを記憶する方法であって、前記複数の部分ネットワークのうちの第１の部分ネットワークを構成するノードが、

前記第１の部分ネットワークで処理可能な移転元識別子から前記第１の部分ネットワークで処理可能ではない移転先識別子への資産の移転を表す第１のトランザクションを受信するステップと、

前記第１のトランザクションを含むブロックを生成するステップと、

前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記移転元識別子の資産の状態を更新するステップと、

前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記第１のトランザクションにより表される前記移転先識別子への前記資産の移転を反映させるための第２のトランザクションを、前記第１のトランザクションの前記移転先識別子と一致する移転元識別子を処理可能な第２の部分ネットワークに送信するステップと

を含むことを特徴とする方法。

[請求項2] 前記第１のトランザクションは、前記移転元識別子の秘密鍵による署名が付加されていることを特徴とする請求項１に記載の方法。

[請求項3] 移転される前記資産の額は、正の値であることを特徴とする請求項１又は２に記載の方法。

[請求項4] 前記第２のトランザクションは、前記第１の部分ネットワークにおいて合意形成がなされたことを示す署名が付加されていることを特徴とする請求項１から３のいずれかに記載の方法。

[請求項5] 前記第２のトランザクションの署名は、単一の署名であることを特徴とする請求項４に記載の方法。

[請求項6] 前記第２のトランザクションの署名は、前記ブロック内の前記第１のトランザクションを含む複数のトランザクションに基づくマークルツリーのマークルルートを含むブロックヘッダに対する署名であることを特徴とする請求項４又は５に記載の方法。

[請求項7] 複数の部分ネットワークのうちの第１の部分ネットワークを構成するノードに、前記複数の部分ネットワークを有する分散ネットワークに資産の移転を表すトランザクションを記憶する方法を実行させるためのプログラムであって、前記方法は、前記ノードが、

前記第１の部分ネットワークで処理可能な移転元識別子から前記第１の部分ネットワークで処理可能ではない移転先識別子への資産の移転を表す第１のトランザクションを受信するステップと、

前記第１のトランザクションを含むブロックを生成するステップと、

前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記移転元識別子の資産の状態を更新するステップと、

前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記第１のトランザクションにより表される前記移転先識別子への前記資産の移転を反映させるための第２のトランザクションを、前記第１のトランザクションの前記移転先識別子と一致する移転元識別子を処理可能な第２の部分ネットワークに送信するステップと

を含むことを特徴とするプログラム。

[請求項8] 複数の部分ネットワークを有する分散ネットワークに資産の移転を表すトランザクションを記憶するための、前記複数の部分ネットワークのうちの第１の部分ネットワークを構成するノードであって、

前記第１の部分ネットワークで処理可能な移転元識別子から前記第１の部分ネットワークで処理可能ではない移転先識別子への資産の移

転を表す第１のトランザクションを受信して、前記第１のトランザクションを含むブロックを生成し、

前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記移転元識別子の資産の状態を更新し、

前記ブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記第１のトランザクションにより表される前記移転先識別子への前記資産の移転を反映させるための第２のトランザクションを、前記第１のトランザクションの前記移転先識別子と一致する移転元識別子を処理可能な第２の部分ネットワークに送信することを特徴とするノード。

[請求項9] 複数の部分ネットワークを有する分散ネットワークに資産の移転を表すトランザクションを記憶する方法であって、前記複数の部分ネットワークのうちの第１の部分ネットワークを構成するノードが、

前記第１の部分ネットワークで処理可能な移転元識別子から前記第１の部分ネットワークで処理可能ではない移転先識別子への資産の移転を表す第１のトランザクションを受信するステップと、

前記第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ステップと、

前記第１のブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記移転元識別子の資産の状態を更新するステップと、

前記第１のブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記第１のトランザクションにより表される前記移転先識別子への前記資産の移転を反映させるための第２のトランザクションを、前記第１のトランザクションの前記移転先識別子と一致する移転元識別子を処理可能な第２の部分ネットワークに送信するステップとを含み、前記第２の部分ネットワークを構成するノードが、

前記第２のトランザクションを受信するステップと、

前記第２のトランザクションを含む第２のブロックを生成するステップと、

前記第２のブロックの採択についての前記第２の部分ネットワークにおける合意形成後、前記第２のトランザクションの移転先識別子の資産の状態を更新するステップと

を含むことを特徴とする方法。

[請求項10] 資産の移転を表すトランザクションを記憶するための複数の部分ネットワークを有する分散ネットワークであって、

前記複数の部分ネットワークのうちの第１の部分ネットワーク及び第２の部分ネットワークを備え、

前記第１の部分ネットワークを構成するノードが、

前記第１の部分ネットワークで処理可能な移転元識別子から前記第１の部分ネットワークで処理可能ではない移転先識別子への資産の移転を表す第１のトランザクションを受信して、前記第１のトランザクションを含む第１のブロックを生成し、

前記第１のブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記移転元識別子の資産の状態を更新し、

前記第１のブロックの採択についての前記第１の部分ネットワークにおける合意形成後、前記第１のトランザクションにより表される前記移転先識別子への前記資産の移転を反映させるための第２のトランザクションを、前記第１のトランザクションの前記移転先識別子と一致する移転元識別子を処理可能な第２の部分ネットワークに送信し、

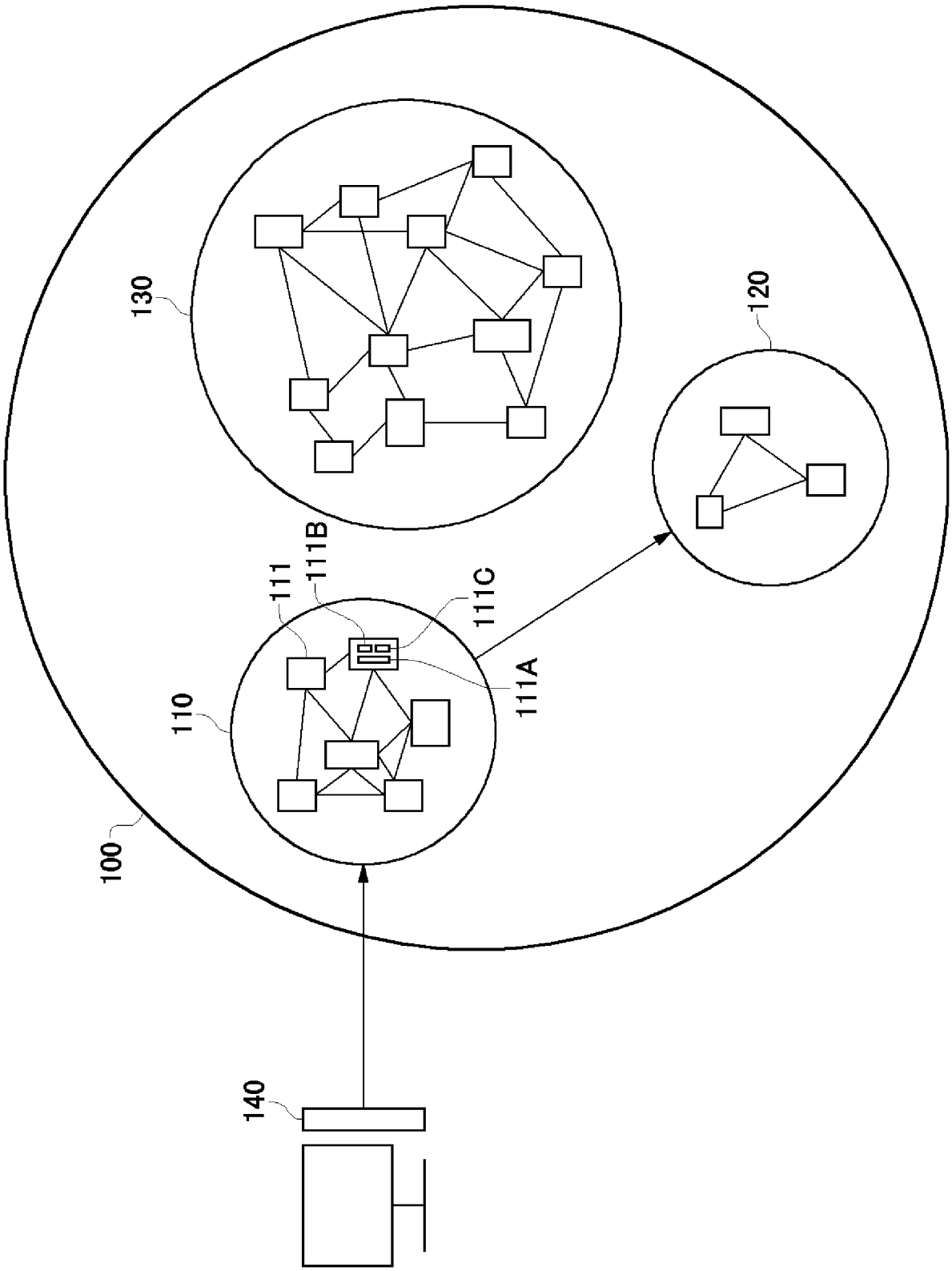
前記第２の部分ネットワークを構成するノードが、

前記第２のトランザクションを受信して、前記第２のトランザクションを含む第２のブロックを生成し、

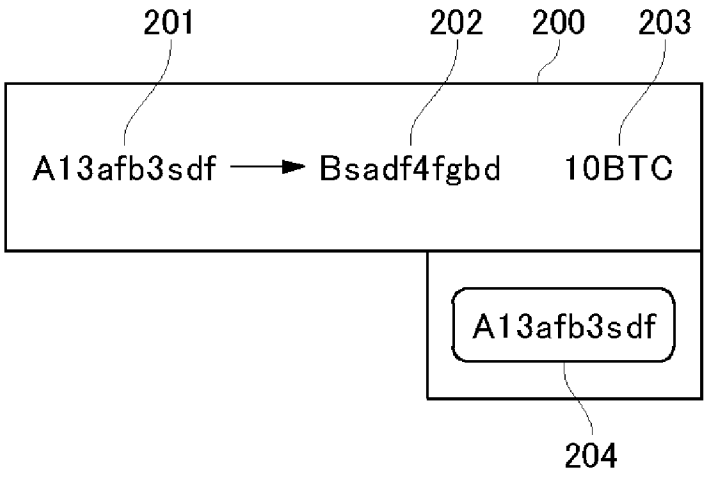
前記第２のブロックの採択についての前記第２の部分ネットワークにおける合意形成後、前記第２のトランザクションの移転先識別子の

資産の状態を更新することを特徴とする分散ネットワーク。

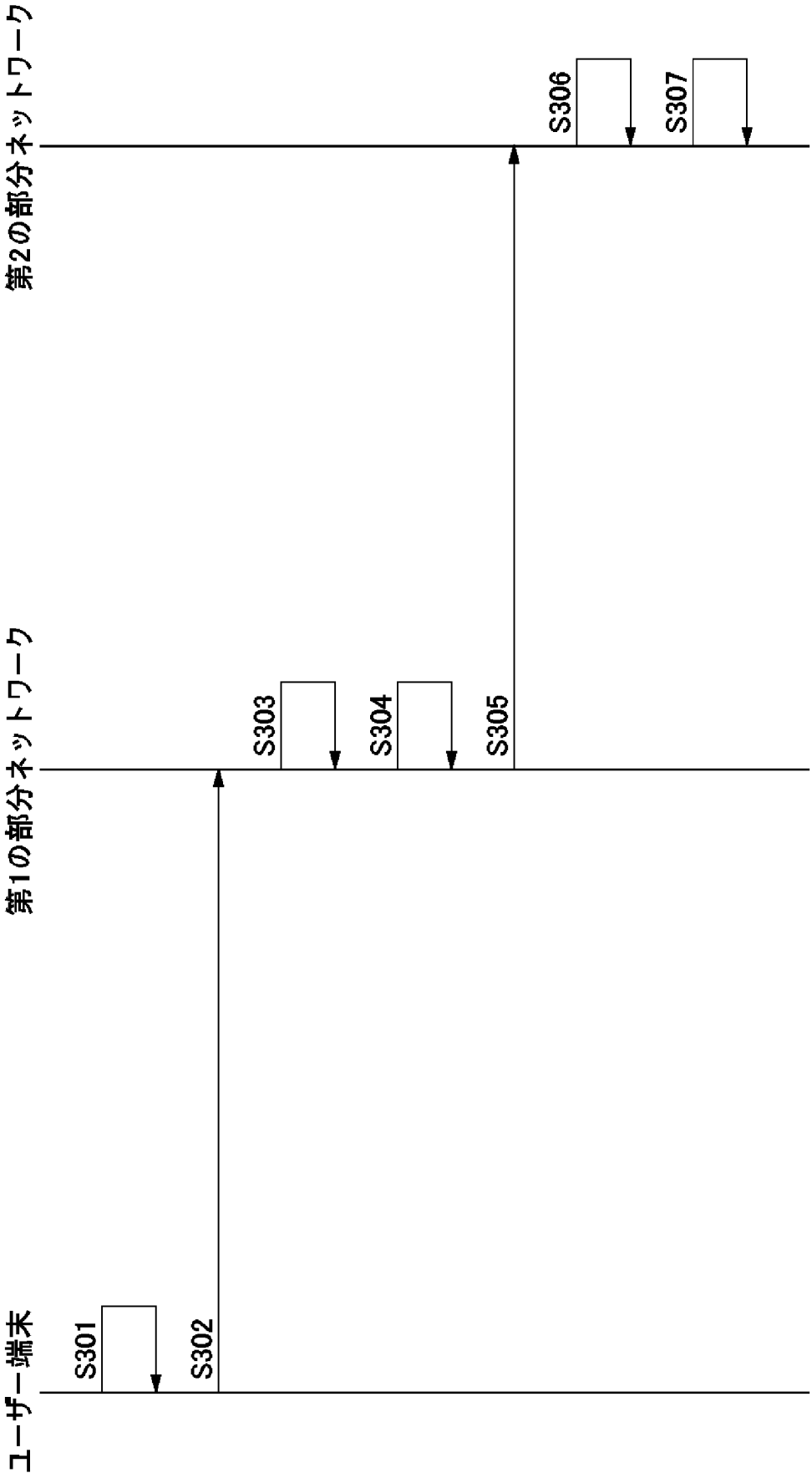
[図1]



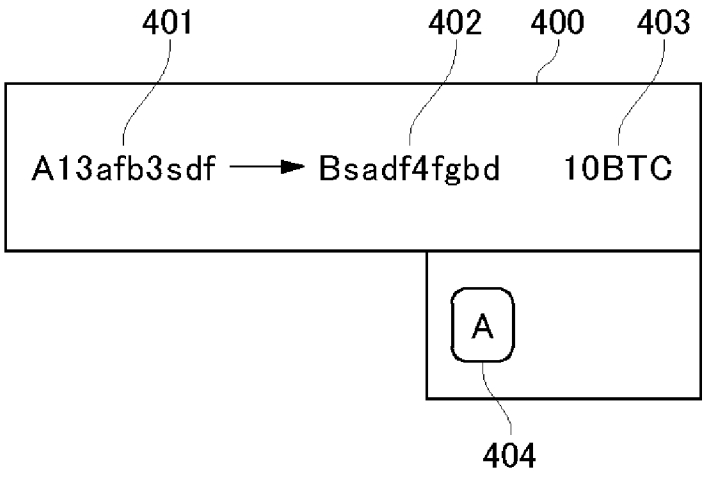
[図2]


201
202
200
203
A13afb3sdf
Bsadf4fgbd
10BTC
A13afb3sdf
204

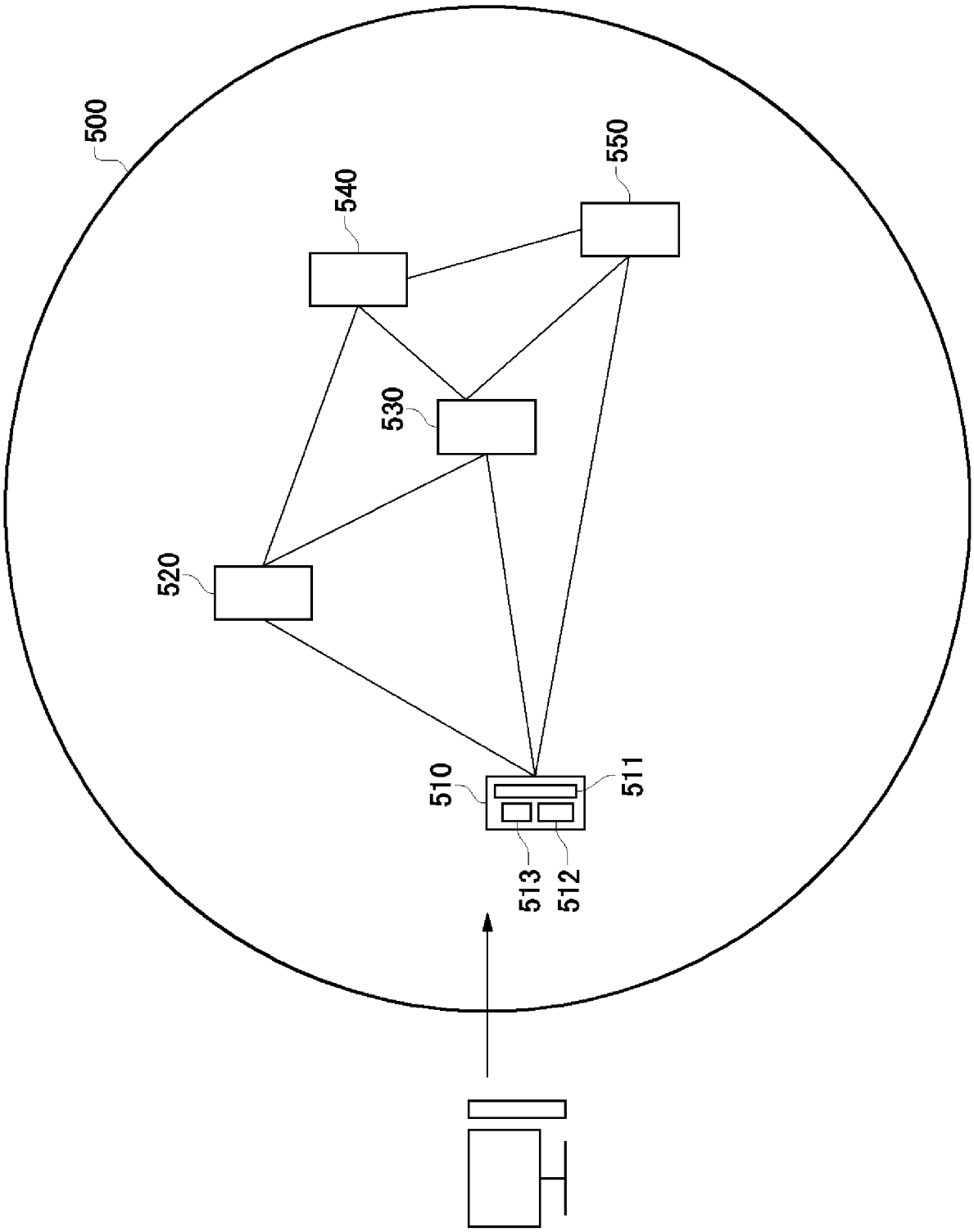
[図3]


第2の部分ネットワーク
第1の部分ネットワーク
ユーザー端末
S301
S302
S303
S304
S305
S306
S307

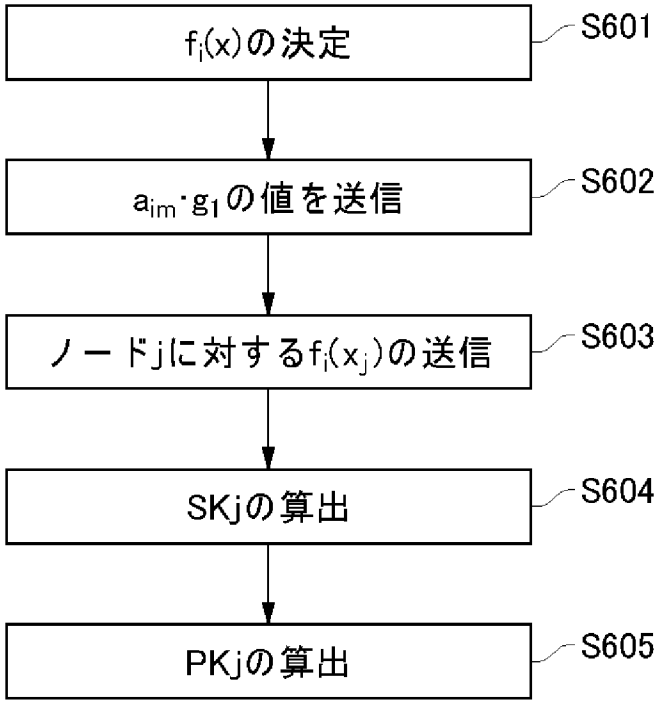
[図4]



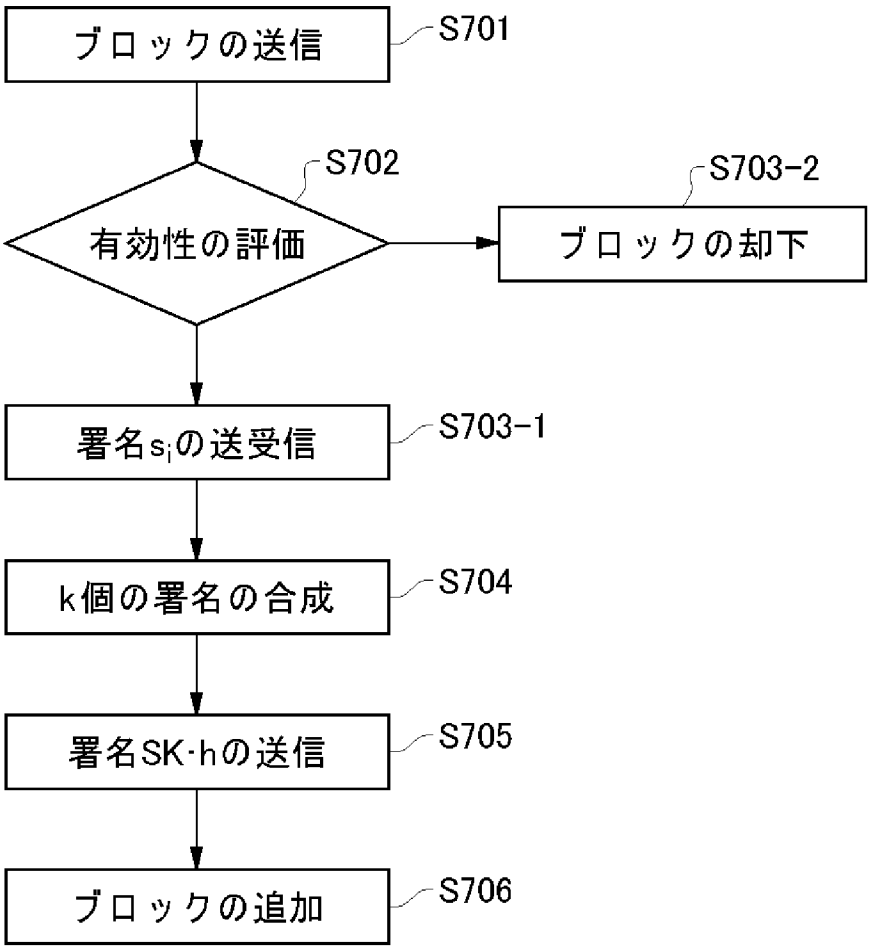
[図5]



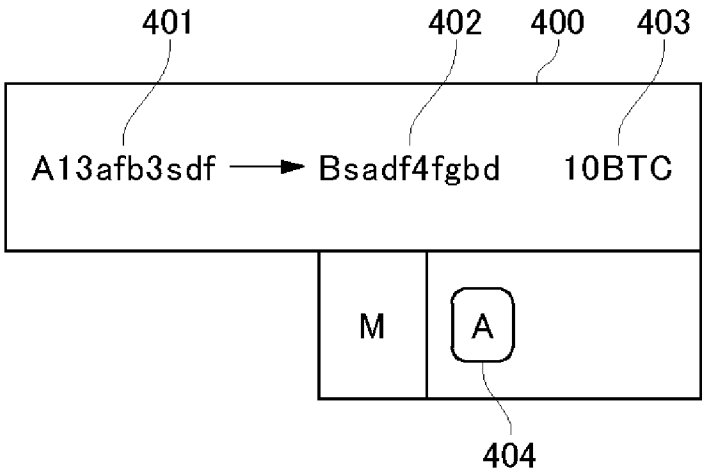
[図6]


$f_i(x)$の決定
S601
$a_{im} \cdot g_1$の値を送信
S602
ノードjに対する$f_i(x_j)$の送信
S603
SKjの算出
S604
PKjの算出
S605

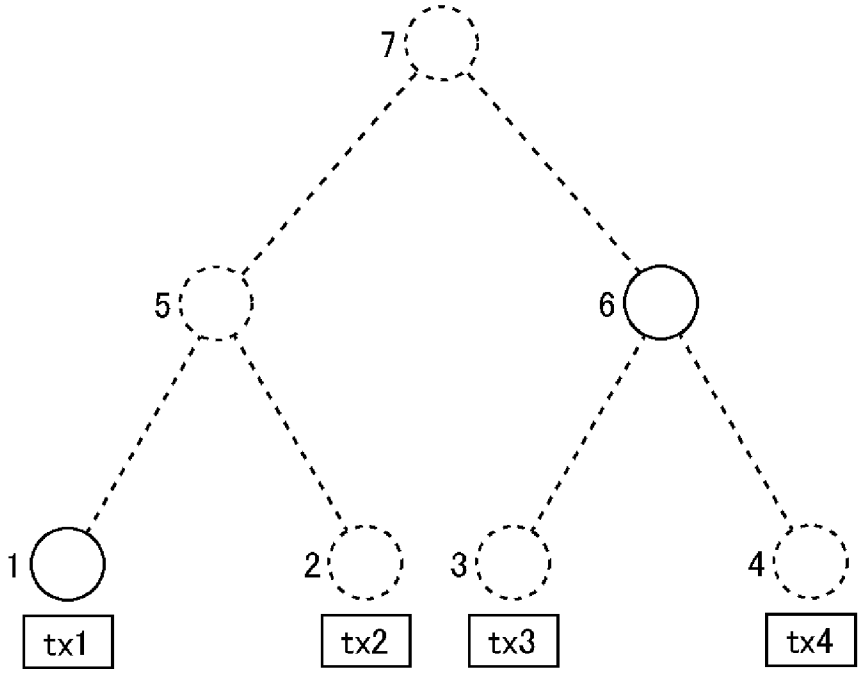
[図7]


ブロックの送信
S701
S702
有効性の評価
S703-2
ブロックの却下
署名s_iの送受信
S703-1
k個の署名の合成
S704
署名SK-hの送信
S705
ブロックの追加
S706

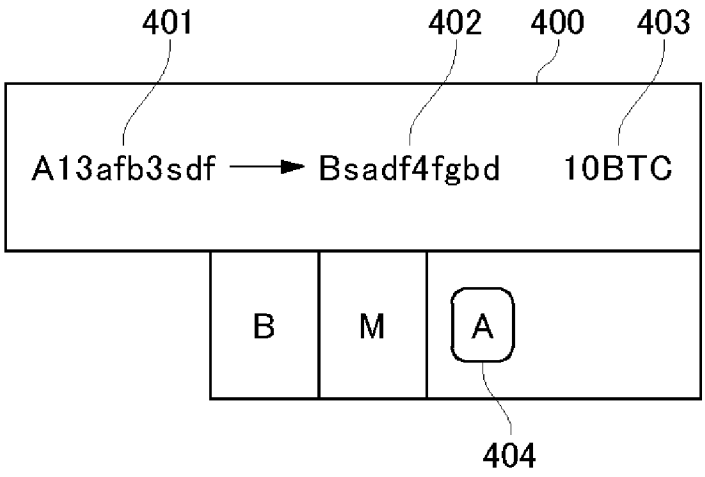
[図8]


401
402
400
403
A13afb3sdf
Bsadf4fgbd
10BTC
M
A
404

[図9]


7
5
6
1
2
3
4
tx1
tx2
tx3
tx4

[図10]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/003840

A. CLASSIFICATION OF SUBJECT MATTER
H04L 9/32(2006.01)i; G06Q 20/06(2012.01)i; G06F 21/64(2013.01)i
FI: H04L9/00 675Z; H04L9/00 675B; G06F21/64; G06Q20/06 300

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; G06Q20/06; G06F21/64

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)
JSTPlus/JMEDPlus/JST7580 (JDreamIII); IEEE Xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 6389542 B1 (DAIWA INSTITUTE OF RESEARCH BUSINESS INNOVATION LTD.) 12.09.2018 (2018-09-12) paragraphs [0045]-[0051], [0516]-[0575], fig. 37-42	1-10
A	WO 2018/215951 A1 (NCHAIN HOLDINGS LIMITED) 29.11.2018 (2018-11-29) page 19, line 7 to page 20, line 22, fig. 1	1-10
A	CN 107528886 A (INSTITUTE OF COMPUTING TECHNOLOGY CHINESE ACADEMY OF SCIENCES) 29.12.2017 (2017-12-29) paragraphs [0044]-[0049], [0065]-[0090], fig. 1-8	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	Date of mailing of the international search report
11 March 2020 (11.03.2020)	24 March 2020 (24.03.2020)

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/003840

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	東角 芳樹 ほか, コンソーシアムチェーンにおける証明書管理に関する一考察, 2017 年暗号と情報セキュリティシンポジウム(SCIS2017)予稿集 [USB], 24 January 2017, 1F2-3, pp. 1-4, see "3.3 Operation of chain management", non-official translation (HIGASHIKADO, Yoshiki et al., "A Study on Certificate Management in Consortium Chain", Preprints of the 2017 Symposium on Cryptography and Information Security(SCIS2017) [USB])	1-10
A	稲村 勝樹 ほか, 回覧文書閲覧確認に適した階層表記型多重署名方式の提案と実装評価, 電子情報通信学会論文誌 B, 01 October 2010, vol. J93-B, no. 10, pp. 1378-1387, see "2.2 BLS signature by pairing", "2.3 GDH multiple signature", (INAMURA Masaki et al., "Proposal and Evaluation of a Hierarchical Multisignature Adapted to Browsing Verification of a Document for Circulating", Proceedings of IEICE B)	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/003840

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 6389542 B1	12 Sep. 2018	JP 2018-156612 A	
WO 2018/215951 A1	29 Nov. 2018	TW 201901575 A	
CN 107528886 A	29 Dec. 2017	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2020/003840

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/32(2006.01)i; G06Q 20/06(2012.01)i; G06F 21/64(2013.01)i
FI: H04L9/00 675Z; H04L9/00 675B; G06F21/64; G06Q20/06 300

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））

H04L9/32; G06Q20/06; G06F21/64

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）

JSTPlus/JMEDPlus/JST7580 (JDreamIII); IEEE Xplore

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 6389542 B1 (株式会社大和総研ビジネス・イノベーション) 12.09.2018 (2018-09-12) 段落[0045]-[0051], [0516]-[0575], 図37-42	1-10
A	WO 2018/215951 A1 (NCHAIN HOLDINGS LIMITED) 29.11.2018 (2018-11-29) 第19頁第7行-第20頁第22行, 図1	1-10
A	CN 107528886 A (INSTITUTE OF COMPUTING TECHNOLOGY CHINESE ACADEMY OF SCIENCES) 29.12.2017 (2017-12-29) 段落[0044]-[0049], [0065]-[0090], 図1-8	1-10
A	東角　芳樹　ほか, コンソーシアムチェーンにおける証明書管理に関する一考察, ２０１７年 暗号と情報セキュリティシンポジウム（ＳＣＩＳ２０１７）予稿集 [USB], 2017.01.24, 1F2-3, p. 1-4 「3.3　管理用チェーンの動作」を参照	1-10
A	稲村　勝樹　ほか, 回覧文書閲覧確認に適した階層表記型多重署名方式の提案と実装評価, 電子情報通信学会論文誌　B, 2010.10.01, 第J93-B巻 第10号, p. 1378-1387 「２．２ペアリングによるＢＬＳ署名」、「２．３　ＧＤＨ多重署名」を参照	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
"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
11.03.2020	24.03.2020

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）
青木　重徳 5S 4229
電話番号 03-3581-1101 内線 3546

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/JP2020/003840

引用文献	公表日	パテントファミリー文献	公表日
JP 6389542 B1	12.09.2018	JP 2018-156612 A	
WO 2018/215951 A1	29.11.2018	TW 201901575 A	
CN 107528886 A	29.12.2017	（ファミリーなし）	