(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4月23日(23.04.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/079973 A1

(51) 国際特許分類:
H04W 12/10 (2009.01) *H04W 84/22* (2009.01)

(21) 国際出願番号： PCT/JP2019/034359

(22) 国際出願日： 2019年9月2日(02.09.2019)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

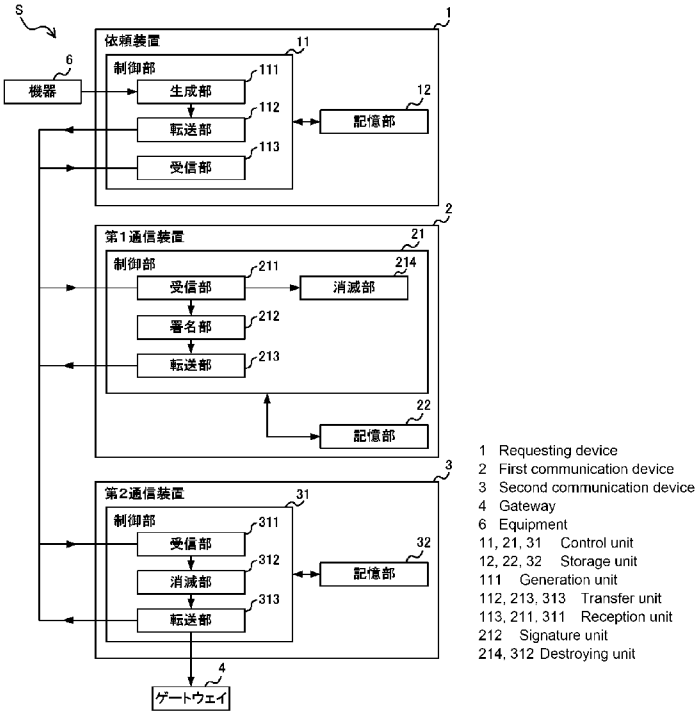
(30) 優先権データ：
特願 2018-195050 2018年10月16日(16.10.2018) JP

(71) 出願人: ＺＥＲＯＢＩＬＬＢＡＮＫ ＪＡＰＡＮ株式会社(**ZEROBILLBANK JAPAN INC.**) [JP/JP]; 〒1000004 東京都千代田区大手町二丁目６番１号 朝日生命大手町ビル２Ｆ Tokyo (JP). 沖電気工業株式会社(**OKI ELECTRIC INDUSTRY CO., LTD.**) [JP/JP]; 〒1058460 東京都港区虎ノ門一丁目７番１２号 Tokyo (JP).

(72) 発明者: 堀 口 純 一 (**HORIGUCHI Junichi**); 〒1000004 東京都千代田区大手町二丁目６番１号 朝日生命大手町ビル２Ｆ ＺＥＲＯＢＩＬＬＢＡＮＫ ＪＡＰＡＮ株式会社内 Tokyo (JP). 茂木 健一(**MOGI Kenichi**); 〒1000004 東京都千代田区大手町二丁目６番１号 朝日生命大手町ビル２Ｆ ＺＥＲＯＢＩＬＬＢＡＮＫ ＪＡＰＡＮ株式会社内 Tokyo (JP). 福永 茂(**FUKUNAGA Shigeru**); 〒1058460 東京都港区虎ノ門一丁目７番１２号 沖電気工業株式会社内 Tokyo (JP). 小杉 篤史(**KOSUGI Atsushi**);

(54) **Title:** COMMUNICATION SYSTEM AND COMMUNICATION METHOD

(54) 発明の名称： 通信システム及び通信方法



(57) **Abstract:** A communication system S according to an embodiment of the present invention includes a plurality of first communication devices 2 and a second communication device 3 connected to the first communication devices and to a wide area network, wherein each of the plurality of first communication devices is provided with: a reception unit 211 that receives a block chain; a signature unit 212 that, if the number of signatures is less than a predetermined threshold value, outputs a block chain obtained by adding a signature to the block chain and that, if the number of signatures has

WO 2020/079973 A1

［続葉有］

〒1058460 東京都港区虎ノ門一丁目７番１２号 沖電気工業株式会社内 Tokyo (JP).

(74) 代理人：泉 通博(IZUMI Michihiro)；〒1010047 東京都千代田区内神田一丁目１７番９号 ＴＣＵビル８Ｆ 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, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

— 国際調査報告（条約第21条(3)）

reached the predetermined threshold value, outputs the block chain; and a transfer unit 213 that transfers the block chain to another communication device, and wherein the second communication device is provided with: a reception unit 311 that receives the block chain; and a transfer unit 313 that, if the number of signatures is less than the predetermined threshold value, transfers the block chain to another communication device and that, if the number of signatures has reached the predetermined threshold value, transfers the block chain to the wide area network.

(57) 要約：本発明の一実施形態に係る通信システムＳは、複数の第１通信装置２と、第１通信装置及び広域ネットワークに接続する第２通信装置３とを含み、複数の第１通信装置それぞれは、ブロックチェーンを受信する受信部２１１と、署名の数が所定の閾値未満である場合にブロックチェーンに署名を付加したブロックチェーンを出力し、署名の数が所定の閾値に到達している場合にブロックチェーンを出力する署名部２１２と、ブロックチェーンを他の通信装置に転送する転送部２１３と、を備え、第２通信装置は、ブロックチェーンを受信する受信部３１１と、署名の数が所定の閾値未満である場合にブロックチェーンを他の通信装置に転送し、署名の数が所定の閾値に到達している場合にブロックチェーンを広域ネットワークに転送する転送部３１３と、を備える。

明　細　書

発明の名称 ： 通信システム及び通信方法

技術分野

[0001]　本発明は、無線通信によってデータを伝送するための通信システム及び通信方法に関する。

背景技術

[0002]　従来、無線通信を行う複数の通信装置がリレー方式でデータを中継することによって、広範囲にデータを伝送可能にするマルチホップネットワーク（マルチホップ通信）が知られている（例えば特許文献１参照）。

先行技術文献

特許文献

[0003] 特許文献1：特開２０１７－５０５８１号公報

発明の概要

発明が解決しようとする課題

[0004]　マルチホップネットワークを構成する複数の通信装置のうち、一部の通信装置のみがインターネット等の広域ネットワークに接続されている場合がある。この場合に、センサ等によって取得されたデータは、広域ネットワークに接続されている通信装置までマルチホップネットワークを介して伝送され、その後広域ネットワーク上の管理装置に記録され得る。しかしながら、マルチホップネットワークでは、複数の通信装置がデータを中継するため、データは伝送される途中で改ざんされる可能性がある。そのため、複数の通信装置の間で伝送されるデータの改ざんを抑制するための技術が求められている。

[0005]　本発明は上述の点に鑑みてなされたものであり、複数の通信装置の間で伝送されるデータの改ざんを抑制できる通信システム及び通信方法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

[0006] 本発明の第１の態様の通信システムは、互いに通信可能な複数の第１通信装置と、前記第１通信装置及び広域ネットワークに接続する第２通信装置とを含む通信システムであって、前記複数の第１通信装置それぞれは、他の通信装置からブロックチェーンを受信する第１受信部と、前記第１受信部が受信した前記ブロックチェーンに含まれている署名の数が所定の閾値未満である場合に前記第１受信部が受信した前記ブロックチェーンに署名を付加した前記ブロックチェーンを出力し、前記署名の数が前記所定の閾値に到達している場合に前記第１受信部が受信した前記ブロックチェーンを出力する署名部と、前記署名部が出力した前記ブロックチェーンを他の通信装置に転送する第１転送部と、を備え、前記第２通信装置は、他の通信装置から前記ブロックチェーンを受信する第２受信部と、前記第２受信部が受信した前記ブロックチェーンに含まれている署名の数が前記所定の閾値未満である場合に前記第２受信部が受信した前記ブロックチェーンを他の通信装置に転送し、前記署名の数が前記所定の閾値に到達している場合に前記第２受信部が受信した前記ブロックチェーンを前記広域ネットワークに転送する第２転送部と、を備える。

[0007] 前記複数の第１通信装置それぞれは、前記第１受信部が受信した前記ブロックチェーンに含まれている署名の数が前記所定の閾値未満であり、かつ前記第１受信部が受信した前記ブロックチェーンの生成時刻から所定の時間が経過している場合に、前記第１受信部が受信した前記ブロックチェーンを消滅させる消滅部をさらに有してもよい。

[0008] 前記通信システムは、前記複数の第１通信装置に処理の実行を依頼する依頼装置をさらに含み、前記複数の第１通信装置それぞれは、指定された処理を実行する実行部をさらに備え、前記依頼装置は、実行依頼を含む前記ブロックチェーンを生成する生成部と、前記生成部が生成した前記ブロックチェーンを他の通信装置に転送する第３転送部と、所定の署名が付加された前記ブロックチェーンを受信する第３受信部と、を備え、前記依頼装置において、前記生成部は、前記第３受信部が受信した前記所定の署名が付加された前

記ブロックチェーンを含む第２ブロックチェーンを生成し、前記第３転送部は、前記生成部が生成した前記第２ブロックチェーンを他の通信装置に転送し、前記複数の第１通信装置それぞれにおいて、前記第１受信部は、前記依頼装置から前記第２ブロックチェーンを受信し、前記実行部は、前記第１受信部が受信した前記第２ブロックチェーンに含まれている前記実行依頼に対応する処理を実行可能な場合に、前記処理を実行し、前記署名部は、前記実行部が前記処理を実行した場合に前記第１受信部が受信した前記第２ブロックチェーンに署名及び前記処理の実行結果を付加した前記第２ブロックチェーンを出力し、前記第１受信部が受信した前記第２ブロックチェーンに含まれている署名の数が所定の閾値未満である場合に前記第１受信部が受信した前記第２ブロックチェーンに署名を付加した前記第２ブロックチェーンを出力し、前記署名の数が前記所定の閾値に到達している場合に前記第１受信部が受信した前記第２ブロックチェーンを出力し、前記第１転送部は、前記署名部が出力した前記第２ブロックチェーンを他の通信装置に転送してもよい。

[0009] 前記依頼装置において、前記第３受信部は、前記実行結果が付加された前記第２ブロックチェーンを受信してもよい。

[0010] 前記通信システムは、前記広域ネットワークに接続しており、メインブロックチェーンを管理する管理装置をさらに含み、前記管理装置は、前記ブロックチェーンを受信した場合に、前記ブロックチェーンに含まれている前記実行依頼を生成した第１主体の債務を示す情報を前記メインブロックチェーンに付加し、前記管理装置は、前記第２ブロックチェーンを受信した場合に、前記第２ブロックチェーンに含まれている前記実行結果を生成した第２主体の債権を示す情報を前記メインブロックチェーンに付加してもよい。

[0011] 前記管理装置は、前記ブロックチェーンを受信した場合に、前記第１主体に関連付けられた金銭に対応する値から減算する値を示す情報を前記メインブロックチェーンに付加し、前記管理装置は、前記第２ブロックチェーンを受信した場合に、前記第２主体に関連付けられた金銭に対応する値に加算す

る値を示す情報を前記メインブロックチェーンに付加してもよい。

[0012] 本発明の第２の態様の通信方法は、互いに通信可能な複数の第１通信装置と、前記第１通信装置及び広域ネットワークに接続する第２通信装置とを含む通信システムにおいて、前記複数の第１通信装置それぞれのプロセッサが、他の通信装置からブロックチェーンを受信するステップと、前記受信するステップが受信した前記ブロックチェーンに含まれている署名の数が所定の閾値未満である場合に前記受信するステップが受信した前記ブロックチェーンに署名を付加した前記ブロックチェーンを出力し、前記署名の数が前記所定の閾値に到達している場合に前記受信するステップが受信した前記ブロックチェーンを出力するステップと、前記出力するステップが出力した前記ブロックチェーンを他の通信装置に転送するステップと、を実行し、前記第２通信装置のプロセッサが、他の通信装置から前記ブロックチェーンを受信するステップと、前記受信するステップが受信した前記ブロックチェーンに含まれている署名の数が前記所定の閾値未満である場合に前記受信するステップが受信した前記ブロックチェーンを他の通信装置に転送し、前記署名の数が前記所定の閾値に到達している場合に前記受信するステップが受信した前記ブロックチェーンを前記広域ネットワークに転送するステップと、を実行する。

発明の効果

[0013] 本発明によれば、複数の通信装置の間で伝送されるデータの改ざんを抑制できるという効果を奏する。

図面の簡単な説明

[0014] [図1]第１の実施形態に係る通信システムの模式図である。

[図2]第１の実施形態に係る通信システムのブロック図である。

[図3]第１の実施形態に係る通信システムが実行する通信方法の模式図である。

[図4]第１の実施形態で用いられるブロックチェーンの模式図である。

[図5]第１の実施形態で用いられるブロックチェーン及びメインブロックチェ

ーンの模式図である。

[図6]第１の実施形態に係る第１通信装置が実行する通信方法のフローチャートを示す図である。

[図7]第１の実施形態に係る第２通信装置が実行する通信方法のフローチャートを示す図である。

[図8]第２の実施形態に係る通信システムが実行する通信方法の前半部分の模式図である。

[図9]第２の実施形態で用いられるブロックチェーンの模式図である。

[図10]第２の実施形態に係る通信システムが実行する通信方法の後半部分の模式図である。

[図11]第２の実施形態で用いられるブロックチェーン及びメインブロックチェーンの模式図である。

[図12]第２の実施形態に係る第１通信装置が実行する通信方法のフローチャートを示す図である。

発明を実施するための形態

[0015] （第１の実施形態）

［通信システムＳの概要］

図１は、本実施形態に係る通信システムＳの模式図である。通信システムＳは、依頼装置１と、複数の第１通信装置２（第１通信装置２Ａ、２Ｂ、２Ｃ）と、第２通信装置３と、ゲートウェイ４と、複数の管理装置５とを含む。通信システムＳは、その他のサーバ、端末等の機器を含んでもよい。

[0016] 依頼装置１、複数の第１通信装置２及び第２通信装置３は、それぞれ通信を行うことが可能な通信装置である。依頼装置１、第１通信装置２及び第２通信装置３は、処理を行うためのコンピュータを有するとともに、所定の周波数帯で無線通信を行うためのアンテナ、プロセッサ、コネクタ等の通信部材を有する。

[0017] 依頼装置１、複数の第１通信装置２及び第２通信装置３は、マルチホップネットワークを構成している。すなわち、依頼装置１、複数の第１通信装置

２及び第２通信装置３のそれぞれは、依頼装置１、複数の第１通信装置２及び第２通信装置３のうち１つからデータを受信し、さらに受信したデータを複数の第１通信装置２及び第２通信装置３のうち別の１つに転送（中継）する。これにより、依頼装置１、複数の第１通信装置２及び第２通信装置３は、インターネット等の広域ネットワークＮを介さずに、データを遠隔地に到達させることができる。

[0018] 第２通信装置３には、広域ネットワークＮに接続するためのゲートウェイ４が接続されている。すなわち、マルチホップネットワークにおいて、第２通信装置３のみが広域ネットワークＮと通信可能である。そのため、依頼装置１が送出したデータは、依頼装置１及び複数の第１通信装置２がデータの転送を繰り返すことによって、第２通信装置３を介して広域ネットワークＮへ到達する。逆に、広域ネットワークＮからのデータは、第２通信装置３及び複数の第１通信装置２がデータの転送を繰り返すことによって、依頼装置１へ到達する。通信システムＳは、２つ以上の第２通信装置３を含んでもよい。

[0019] 第１通信装置２と第２通信装置３とは異なる種類の通信装置であってもよい。あるいは複数の第１通信装置２のうちゲートウェイ４に接続されている少なくとも１つの第１通信装置２が、第２通信装置３として機能してもよい。この場合には、第２通信装置３は、第１通信装置の機能もあわせ持つ。

[0020] 依頼装置１及び複数の第１通信装置２のうち少なくとも一部には、機器６が接続されている。機器６は、依頼装置１又は第１通信装置２に対して情報を入力するか、あるいは依頼装置１又は第１通信装置２から受け取った情報に応じて動作する機器であり、例えばセンサ、コンピュータ、アクチュエータ等である。

[0021] ゲートウェイ４は、第２通信装置３と広域ネットワークＮとを接続するコンピュータである。ゲートウェイ４は、有線通信又は無線通信を行うためのアンテナ、プロセッサ、コネクタ等の通信部材を有する。ゲートウェイ４は、第２通信装置３から受信したデータを広域ネットワークＮに転送するとと

もに、広域ネットワークＮから受信したデータを第２通信装置３に転送する。

[0022] 複数の管理装置５は、それぞれ通信を行うことが可能なコンピュータである。管理装置５は、有線通信又は無線通信を行うためのアンテナ、プロセッサ、コネクタ等の通信部材を有する。管理装置５のそれぞれは、メインブロックチェーンを記憶部上に記憶して管理している。複数の管理装置５のいずれかは、追加対象のデータに対して既知のマイニング処理を行い、所定の条件を満たすナンス値及びハッシュ値を用いて追加対象のデータをメインブロックチェーンに追加する。

[0023] 本実施形態に係る通信システムＳが実行する通信方法の概要を以下に説明する。まず依頼装置１は、追加対象のデータ及び依頼装置１の署名を含むブロックチェーンを生成する（ａ）。依頼装置１は、生成したブロックチェーンを複数の第１通信装置２のいずれか（ここでは第１通信装置２Ａ）に転送する。

[0024] 第１通信装置２Ａは、依頼装置１から受信したブロックチェーンに対して所定の条件を満たすナンス値及びハッシュ値を算出し、算出したナンス値及びハッシュ値を用いて、第１通信装置２Ａの署名をブロックチェーンに付加する。そして第１通信装置２Ａは、署名を付加したブロックチェーンを複数の第１通信装置２のいずれかに転送する（ｂ）。

[0025] 複数の第１通信装置２それぞれは、受信したブロックチェーンの署名数が所定の閾値未満である場合には第１通信装置２Ａと同様にブロックチェーンに署名を付加して転送し、ブロックチェーンの署名数が所定の閾値に到達している場合にはブロックチェーンに署名を付加せずに転送する。ここで、複数の第１通信装置２それぞれは、受信したブロックチェーンが所定の消滅条件を満たす場合、具体的には署名数が所定の閾値未満でありかつブロックチェーンの生成時刻から所定時間が経過している条件を満たす場合に、ブロックチェーンを消滅させる（ｃ）。

[0026] 複数の第１通信装置２が転送を繰り返すことによってブロックチェーンが

第２通信装置３へ到達すると、第２通信装置３は、受信したブロックチェーンを、ゲートウェイ４を介して広域ネットワークＮ上の管理装置５に転送する（ｄ）。

[0027] 管理装置５は、広域ネットワークＮを介して、第２通信装置３が送信したブロックチェーンを受信する。そして管理装置５は、受信したブロックチェーンに対して所定の条件を満たすナンス値及びハッシュ値を算出し、算出したナンス値及びハッシュ値を用いて、受信したブロックチェーンをメインブロックチェーンに追加する（ｅ）。これにより、依頼装置１が送出した追加対象のデータは、メインブロックチェーンに追加される。

[0028] このように、本実施形態に係る通信システムＳにおいて、依頼装置１、第１通信装置及び第２通信装置は、マルチホップネットワークにおいて追加対象のデータを含むブロックチェーンに所定時間内に所定数の署名を付加して広域ネットワークＮに転送し、消滅条件を満たすブロックチェーンは広域ネットワークＮに転送せずに消滅させる。そのため、第三者がマルチホップネットワーク内でブロックチェーンを改ざんしようとしても、ブロックチェーンに所定数の署名を付加することは消滅条件が定める所定時間内では困難であるため、複数の通信装置の間で伝送される追加対象のデータが改ざんされるのを抑制できる。

[0029] ［通信システムＳの構成］

図２は、本実施形態に係る通信システムＳのブロック図である。図２において、矢印は主なデータの流れを示しており、図２に示したもの以外のデータの流れがあってよい。図２において、各ブロックはハードウェア（装置）単位の構成ではなく、機能単位の構成を示している。そのため、図２に示すブロックは単一の装置内に実装されてよく、あるいは複数の装置内に分かれて実装されてよい。ブロック間のデータの授受は、データバス、ネットワーク、可搬記憶媒体等、任意の手段を介して行われてよい。

[0030] 依頼装置１は、制御部１１と、記憶部１２とを有する。制御部１１は、生成部１１１と、転送部１１２と、受信部１１３とを有する。記憶部１２は、

ＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）、ハードディスクドライブ等を含む記憶媒体である。記憶部１２は、制御部１１が実行するプログラムを予め記憶している。

[0031] 制御部１１は、例えばＣＰＵ（Central Processing Unit）等のプロセッサであり、記憶部１２に記憶されたプログラムを実行することにより、生成部１１１、転送部１１２及び受信部１１３として機能する。制御部１１の機能の少なくとも一部は、電気回路によって実行されてもよい。

[0032] 第１通信装置２は、制御部２１と、記憶部２２とを有する。制御部２１は、受信部２１１と、署名部２１２と、転送部２１３と、消滅部２１４とを有する。記憶部２２は、ＲＯＭ、ＲＡＭ、ハードディスクドライブ等を含む記憶媒体である。記憶部２２は、制御部２１が実行するプログラムを予め記憶している。

[0033] 制御部２１は、例えばＣＰＵ等のプロセッサであり、記憶部２２に記憶されたプログラムを実行することにより、受信部２１１、署名部２１２、転送部２１３及び消滅部２１４として機能する。制御部２１の機能の少なくとも一部は、電気回路によって実行されてもよい。

[0034] 第２通信装置３は、制御部３１と、記憶部３２とを有する。制御部３１は、受信部３１１と、消滅部３１２と、転送部３１３とを有する。記憶部３２は、ＲＯＭ、ＲＡＭ、ハードディスクドライブ等を含む記憶媒体である。記憶部３２は、制御部２１が実行するプログラムを予め記憶している。

[0035] 制御部３１は、例えばＣＰＵ等のプロセッサであり、記憶部３２に記憶されたプログラムを実行することにより、受信部３１１、消滅部３１２及び転送部３１３として機能する。制御部３１の機能の少なくとも一部は、電気回路によって実行されてもよい。

[0036] 本実施形態に係る通信システムＳは、図２に示す具体的な構成に限定されない。依頼装置１、第１通信装置２及び第２通信装置はそれぞれの機能に基づいて定義されており、１つの装置が依頼装置１、第１通信装置２及び第２通信装置のうち２つ以上として機能するように構成されてもよい。第２通信

装置３及びゲートウェイ４は、一体化されて１つの装置として構成されてもよい。

[0037] ［通信方法の説明］

図３は、本実施形態に係る通信システムＳが実行する通信方法の模式図である。図４は、本実施形態で用いられるブロックチェーンＡ１、Ａ２、Ａ３の模式図である。図５は、本実施形態で用いられるブロックチェーンＡ４及びメインブロックチェーンＭの模式図である。

[0038] まず依頼装置１において、生成部１１１は、機器６からメインブロックチェーンＭへの追加対象のデータを取得する。例えば機器６はセンサ（温度センサ、気圧センサ等）であり、追加対象のデータはセンサ値である。そして生成部１１１は、署名Ａ１１と、装置識別情報Ａ１２と、データＡ１３と、証明書作成時刻Ａ１４とを含むブロックチェーンＡ１を生成する。

[0039] 署名Ａ１１は、依頼装置１の秘密鍵に基づく電子署名であり、既知の署名方法によって生成される。署名Ａ１１の正当性は、依頼装置１の公開鍵によって検証可能である。装置識別情報Ａ１２は、ブロックチェーンＡ１を生成した依頼装置１を識別する情報であり、例えばデバイスＩＤである。

[0040] データＡ１３は、追加対象のデータそのものであってもよく、あるいは追加対象のデータに所定の処理（例えば暗号化）を行ったものであってもよい。証明書作成時刻Ａ１４は、署名Ａ１１を生成した時刻である。ブロックチェーンＡ１は、ここに示したデータに限定されず、トランザクションＩＤやデータ取得時刻を含んでもよい。

[0041] 転送部１１２は、生成したブロックチェーンＡ１を複数の第１通信装置２のいずれかに転送する。転送先の第１通信装置２を示す経路情報は、予め記憶部１２に記憶されている。あるいは経路情報は、受信したデータに基づいて動的に更新されてもよい。

[0042] それぞれの第１通信装置２において、受信部２１１は、依頼装置１、他の第１通信装置２又は第２通信装置３が送信したブロックチェーンを受信して取得する。ここで、第１通信装置２は、少なくとも依頼装置１が生成したブ

ロックチェーンＡ１の内容を含むブロックチェーンを受信して処理する。少なくとも依頼装置１が生成したブロックチェーンＡ１の内容を含むブロックチェーンは、ブロックチェーンＡ１そのものであってもよく、ブロックチェーンＡ１に基づいて生成されたブロックチェーンであってもよい。署名部２１２は、受信したブロックチェーンの署名数が所定の閾値（ここでは３個）未満である場合に、受信したブロックチェーンに対して、既知の方法を用いて所定の条件を満たすナンス値及びハッシュ値を算出する。

[0043] 具体的には、署名部２１２は、受信したブロックチェーンにナンス値を付加してハッシュ値を算出した際に、ハッシュ値が所定の条件を満たすようにナンス値及びハッシュ値の組を算出する。署名部２１２がナンス値及びハッシュ値を算出する方法は、具体的な方法に限定されない。

[0044] そして署名部２１２は、受信したブロックチェーンに、算出したナンス値Ａ１５と、署名Ａ２１と、装置識別情報Ａ２２と、証明書作成時刻Ａ２３と、算出したハッシュ値Ａ２４とを付加したブロックチェーンを出力する。署名Ａ２１は、ナンス値Ａ１５を算出した第１通信装置２の秘密鍵に基づく電子署名であり、既知の署名方法によって生成される。署名Ａ２１の正当性は、第１通信装置２の公開鍵によって検証可能である。装置識別情報Ａ２２は、第１通信装置２を識別する情報であり、例えばデバイスＩＤである。証明書作成時刻Ａ２３は、署名Ａ２１を生成した時刻である。ブロックチェーンＡ２は、ここに示したデータに限定されず、トランザクションＩＤ等を含んでもよい。

[0045] 転送部２１３は、署名部２１２が署名を付加したブロックチェーンを、複数の第１通信装置２のいずれか又は第２通信装置３に転送する。一方、署名部２１２及び転送部２１３は、受信したブロックチェーンの署名数が所定の閾値に到達している場合には、受信したブロックチェーンに署名を付加せずに、そのまま複数の第１通信装置２のいずれか又は第２通信装置３に転送する。転送先の第１通信装置２又は第２通信装置３を示す経路情報は、予め記憶部２２に記憶されている。あるいは経路情報は、受信したデータに基づい

て動的に更新されてもよい。

[0046] また、それぞれの第１通信装置２において、消滅部２１４は、受信したブロックチェーンが所定の消滅条件を満たす場合、具体的には署名数が所定の閾値（ここでは３個）未満でありかつブロックチェーンの生成時刻（例えば証明書作成時刻Ａ１４）から所定時間（ここでは１分）が経過している場合に、受信したブロックチェーンを消滅させる。消滅部２１４は、ブロックチェーンが第２通信装置３に到達するまで、ブロックチェーンを消滅させなくてもよい。

[0047] ここで所定時間は、署名部２１２が署名を生成するのに必要な時間に、署名数の閾値から１を減算した値（すなわち閾値－１）を乗算した第１値以上であり、該値に所定のバッファ（例えば０％～２０％）を加えた第２値以下である。例えば署名部２１２が署名を生成するのに必要な時間が３０秒であり、署名数の閾値が３個である場合に、所定時間は１分に設定される。消滅条件としての署名数の閾値及び所定時間は、その他の値に設定されてもよい。

[0048] この場合に、複数の第１通信装置２は、依頼装置１が生成した署名に加えて、２個の署名を付加する。このとき、複数の第１通信装置２において署名部２１２が２個の署名を生成するためにはおおよそ合計１分掛かる。そのため、消滅部２１４は、所定数の署名を含んでいないブロックチェーンの生成時刻から１分を経過している場合に、ブロックチェーンを消滅させ、ブロックチェーンの転送を行わない。このような構成により、仮にマルチホップネットワークに第三者が介入してブロックチェーンのデータを改ざんした場合には、所定数の署名を付加するために所定時間よりも長い時間が掛かるためブロックチェーンは消滅し、改ざんされたブロックチェーンがメインブロックチェーンＭに追加されることを抑制できる。

[0049] 図３の例では、第１通信装置２Ａが依頼装置１から取得したブロックチェーンＡ１に署名を付加することによってブロックチェーンＡ２を生成して転送し、第１通信装置２Ｂが第１通信装置２Ａから取得したブロックチェーン

Ａ２に署名を付加することによってブロックチェーンＡ３を生成して転送する。このときブロックチェーンＡ３に含まれている署名数が３個に到達しているため、その他の複数の第１通信装置２は、これ以上署名を付加することなく、ブロックチェーンＡ３を第２通信装置３に到達するまで繰り返し転送する。

[0050] 複数の第１通信装置２が転送を繰り返すことによってブロックチェーンＡ３が第２通信装置３へ到達すると、第２通信装置３の受信部３１１は、いずれかの第１通信装置２が送信したブロックチェーンＡ３を受信して取得する。ここで、第２通信装置３は、少なくとも依頼装置１が生成したブロックチェーンＡ１の内容を含むブロックチェーンを受信して処理する。少なくとも依頼装置１が生成したブロックチェーンＡ１の内容を含むブロックチェーンは、ブロックチェーンＡ１そのものであってもよく、ブロックチェーンＡ１に基づいて生成されたブロックチェーンであってもよい。消滅部３１２は、受信したブロックチェーンＡ３が消滅部２１４と同様の消滅条件を満たす場合に、受信したブロックチェーンＡ３を消滅させる。

[0051] 転送部３１３は、受信したブロックチェーンＡ３の署名数が所定の閾値（ここでは３個）に到達している場合に、受信したブロックチェーンＡ３を、ゲートウェイ４を介して広域ネットワークＮ上の管理装置５に転送する。転送先の広域ネットワークＮ上の管理装置５を示す経路情報は、予めゲートウェイ４に記憶されている。あるいは経路情報は、受信したデータに基づいて動的に更新されてもよい。転送部３１３は、受信したブロックチェーンＡ３の署名数が所定の閾値未満である場合に、受信したブロックチェーンＡ３を複数の第１通信装置２のいずれかに転送する。

[0052] 管理装置５は、広域ネットワークＮを介して、第２通信装置３が送信したブロックチェーンＡ３を受信する。そして管理装置５は、予め記憶されたメインブロックチェーンＭに対して、既知の方法を用いて所定の条件を満たすナンス値及びハッシュ値を算出する。具体的には、管理装置５は、メインブロックチェーンＭにナンス値を付加してハッシュ値を算出した際に、ハッシ

ュ値が所定の条件を満たすようにナンス値及びハッシュ値の組を算出する。管理装置５がナンス値及びハッシュ値を算出する方法は、具体的な方法に限定されない。

[0053] そして管理装置５は、メインブロックチェーンＭに、算出したナンス値Ｍ１を付加するとともに、署名Ａ４１と、算出したハッシュ値Ａ４２と、実行情報Ａ４３と、受信したブロックチェーンＡ３とを含むブロックチェーンＡ４を追加する。署名Ａ４１は、ナンス値Ｍ１を算出した管理装置５の秘密鍵に基づく電子署名であり、既知の署名方法によって生成される。署名Ａ４１の正当性は、管理装置５の公開鍵によって検証可能である。実行情報Ａ４３は、追加対象のデータがメインブロックチェーンＭに追加されたか否かを示す情報である。これにより、依頼装置１が送出した追加対象のデータは、メインブロックチェーンＭに追加される。

[0054] さらに管理装置５は、生成したブロックチェーンＡ４を、ゲートウェイ４、第２通信装置３及び複数の第１通信装置２を介して依頼装置１まで転送する。依頼装置１の受信部１１３は、複数の第１通信装置２のいずれかからブロックチェーンＡ４を受信して取得する。これにより、依頼装置１は、追加対象のデータがメインブロックチェーンＭに追加されたか否かを知ることができる。

[0055] 図３の例では、ＰｏＷ（Proof of Work）によってブロックチェーンを生成しているが、ＰｏＡ（Proof of Authority）によってブロックチェーンを生成してもよい。

[0056] 図３の例では、依頼装置１及び第１通信装置２は、ブロックチェーンをいずれか１つの第１通信装置２に転送しているが、複数の第１通信装置２に転送（ブロードキャスト）してもよい。この場合には、管理装置５は、最も早く受信したブロックチェーンをメインブロックチェーンＭに追加し、既にメインブロックチェーンＭに追加されたブロックチェーンのデータを含む他のブロックチェーンを破棄する。

[0057] 第１通信装置２は、受信したブロックチェーンの署名数が所定の閾値に到

達していた場合であっても、ブロックチェーンにさらに追加の署名を付加して転送してもよい。この場合には、管理装置５は、同じデータを含む複数のブロックチェーンのうち、最も署名数が多いブロックチェーンをメインブロックチェーンＭに追加し、その他のブロックチェーンを破棄する。

[0058] ［通信方法のフローチャート］

図６は、本実施形態に係る第１通信装置２が実行する通信方法のフローチャートを示す図である。第１通信装置２において、受信部２１１は、依頼装置１、他の第１通信装置２又は第２通信装置３が送信したブロックチェーンを受信して取得する（Ｓ１１）。

[0059] 受信したブロックチェーンが所定の消滅条件を満たす場合に（Ｓ１２のＹＥＳ）、消滅部２１４は、受信したブロックチェーンを転送せずに消滅させる（Ｓ１３）。消滅条件は、署名数が所定の閾値（例えば３個）未満であり、かつブロックチェーンの生成時刻から所定時間（例えば１分）が経過していることである。

[0060] 受信したブロックチェーンが所定の消滅条件を満たさない場合であって（Ｓ１２のＮＯ）、受信したブロックチェーンの署名数が所定の閾値に到達している場合に（Ｓ１４のＮＯ）、第１通信装置２はステップＳ１７へ進む。

[0061] 受信したブロックチェーンが所定の消滅条件を満たさない場合であって（Ｓ１２のＮＯ）、受信したブロックチェーンの署名数が所定の閾値未満である場合に（Ｓ１４のＹＥＳ）、署名部２１２は、所定の条件を満たすナンス値及びハッシュ値を算出する（Ｓ１５）。そして署名部２１２は、受信したブロックチェーンに、算出したナンス値及びハッシュ値と、第１通信装置２の署名とを付加したブロックチェーンを出力する（Ｓ１６）。

[0062] 転送部２１３は、署名数が所定の閾値に到達しているブロックチェーン又は署名部２１２が署名を付加したブロックチェーンを、複数の第１通信装置２のいずれか又は第２通信装置３に転送する（Ｓ１７）。

[0063] 図７は、本実施形態に係る第２通信装置３が実行する通信方法のフローチャートを示す図である。第２通信装置３において、受信部３１１は、いずれ

かの第１通信装置２が送信したブロックチェーンを受信して取得する（Ｓ２１）。

[0064] 受信したブロックチェーンが所定の消滅条件を満たす場合に（Ｓ２２のＹＥＳ）、消滅部３１２は、受信したブロックチェーンを転送せずに消滅させる（Ｓ２３）。

[0065] 受信したブロックチェーンが所定の消滅条件を満たさない場合であって（Ｓ２２のＮＯ）、受信したブロックチェーンの署名数が所定の閾値未満である場合に（Ｓ２４のＹＥＳ）、転送部３１３は、受信したブロックチェーンを複数の第１通信装置２のいずれかに転送する（Ｓ２５）。

[0066] 受信したブロックチェーンが所定の消滅条件を満たさない場合であって（Ｓ２２のＮＯ）、受信したブロックチェーンの署名数が所定の閾値に到達している場合に（Ｓ２４のＮＯ）、転送部３１３は、受信したブロックチェーンを、ゲートウェイ４を介して広域ネットワークＮ上の管理装置５に転送する（Ｓ２６）。

[0067] ［適用例］

本実施形態に係る通信システムＳは、例えばＩｏＴ（Internet of Things）保険に適用される。この場合に、機器６は、例えば保険の対象とする自動車や自転車等の移動装置に搭載されている。移動装置は、さまざまな場所を移動するため、広域ネットワークＮに常に接続されるとは限らない。そこで依頼装置１は、移動装置に搭載された機器６から、移動装置の稼動データを取得する。そして依頼装置１は、移動装置の稼動データを、本実施形態に係る通信方法を用いてマルチホップネットワーク上で転送する。

[0068] これにより通信システムＳは、保険の対象とする移動装置が広域ネットワークＮに接続されていない場合であっても、移動装置の稼動データをマルチホップネットワーク上で改ざんを抑制しつつ収集でき、保険の対象とする移動装置の稼動状況を監視できる。

[0069] ［実施形態の効果］

本実施形態に係る通信システムＳは、マルチホップネットワークにおいて

追加対象のデータを含むブロックチェーンに所定時間内に所定数の署名を付加して広域ネットワークＮに転送し、所定時間内に所定数の署名が付加されなかったブロックチェーンを広域ネットワークＮに転送せずに消滅させる。そのため、第三者がマルチホップネットワーク内でブロックチェーンを改ざんしようとしても、ブロックチェーンに所定数の署名を付加することは消滅条件が定める所定時間内では困難であるため、複数の通信装置の間で伝送される追加対象のデータが改ざんされるのを抑制できる。

[0070]（第２の実施形態）

本実施形態に係る通信システムＳは、第１の実施形態に係る通信システムＳを応用することによって、２つの主体の間の契約を自動化する。以下では第１の実施形態と異なる点を主に説明する。

[0071] 本実施形態に係る第１通信装置２の制御部２１は、図２の構成に加えて、実行部２１５をさらに有する。実行部２１５は、受信部２１１が受信したブロックチェーンが所定の条件を満たす場合に、該ブロックチェーンに含まれる実行依頼に対応する処理を実行する。

[0072] 図８は、本実施形態に係る通信システムＳが実行する通信方法の前半部分の模式図である。図９は、本実施形態で用いられるブロックチェーンＢ１、Ｂ４及びメインブロックチェーンＭの模式図である。

[0073] まず依頼装置１において、生成部１１１は、機器６から実行依頼情報を取得する。依頼装置１に接続された機器６は、処理を依頼する第１主体に関連付けられており、例えば第１主体としてのユーザによって操作される端末である。実行依頼情報は、第２主体が有する機器６に実行を依頼する処理（例えばセンサ値の取得）と、第２主体へ支払う金額又はトークン数と、第１主体に関連付けられた口座情報とを示す。口座情報は、第１主体が有する金銭又は金銭に対応するトークンを管理する口座（ウォレット）の識別情報を示す。口座情報は、依頼装置１の記憶部１２に予め記憶されてもよく、依頼装置１に接続されている機器６から入力されてもよい。

[0074] そして生成部１１１は、署名Ｂ１１と、装置識別情報Ｂ１２と、実行依頼

情報Ｂ１３と、証明書作成時刻Ｂ１４とを含むブロックチェーンＢ１を生成する。署名Ｂ１１、装置識別情報Ｂ１２及び証明書作成時刻Ｂ１４は、図４の署名Ａ１１、装置識別情報Ａ１２及び証明書作成時刻Ａ１４と同様である。実行依頼情報Ｂ１３は、口座情報Ｂ１３１と、処理内容を表す実行コードＢ１３２と、支払い金額Ｂ１３３（又はトークン数）とを含む。実行依頼情報Ｂ１３は、機器６から取得した実行依頼情報そのものであってもよく、あるいは実行依頼情報に所定の処理（例えば暗号化）を行ったものであってもよい。転送部１１２は、生成したブロックチェーンＢ１を複数の第１通信装置２のいずれかに転送する。

[0075] 次に複数の第１通信装置２は、第１の実施形態と同様に、依頼装置１が生成したブロックチェーンＢ１に署名を付加して転送することを繰り返す。ここで、第１通信装置２は、少なくとも依頼装置１が生成したブロックチェーンＢ１の内容を含むブロックチェーンを受信して処理する。少なくとも依頼装置１が生成したブロックチェーンＢ１の内容を含むブロックチェーンは、ブロックチェーンＢ１そのものであってもよく、ブロックチェーンＢ１に基づいて生成されたブロックチェーンであってもよい。所定時間内（ここでは１分以内）に所定数（ここでは３個）の署名が付加されなかったブロックチェーンＢ１は消滅する。そして所定時間内に所定数の署名が付加されたブロックチェーンＢ３は、第２通信装置３に到達する。第２通信装置３は、ブロックチェーンＢ３を、ゲートウェイ４を介して広域ネットワークＮ上の管理装置５に転送する。ここで、第２通信装置３は、少なくとも依頼装置１が生成したブロックチェーンＢ１の内容を含むブロックチェーンを受信して処理する。少なくとも依頼装置１が生成したブロックチェーンＢ１の内容を含むブロックチェーンは、ブロックチェーンＢ１そのものであってもよく、ブロックチェーンＢ１に基づいて生成されたブロックチェーンであってもよい。

[0076] 管理装置５は、広域ネットワークＮを介して、第２通信装置３が送信したブロックチェーンＢ３を受信する。そして管理装置５は、メインブロックチェーンＭに、ナンス値Ｍ１を付加するとともに、署名Ｂ４１と、ハッシュ値

Ｂ４２と、実行情報Ｂ４３と、債務情報Ｂ４４と、受信したブロックチェーンＢ３とを含むブロックチェーンＢ４を追加する。ナンス値Ｍ１、署名Ｂ４１、ハッシュ値Ｂ４２及び実行情報Ｂ４３は、図５のナンス値Ｍ１、署名Ａ４１、ハッシュ値Ａ４２及び実行情報Ａ４３と同様である。

[0077] 債務情報Ｂ４４は、処理を依頼した第１主体が有する債務を記録した情報であり、例えば実行依頼情報が示す第１主体の口座から実行依頼情報が示す金額又はトークン数（すなわち金銭に対応する値）を減算するトランザクション（デポジット情報）を示す。これにより、メインブロックチェーンＭには、第１主体が依頼した処理が第２主体によって実行される前に、第１主体の債務を記録できるため、第２主体が処理を実行した後に第１主体が支払い等の債務を免れる事態を予防できる。

[0078] メインブロックチェーンＭにデポジット情報が記録された後、所定時間が経過しても実行依頼情報が示す処理が実行されない場合には、管理装置５は、デポジット情報の金額又はトークン数を第１主体の口座に加算するトランザクションをメインブロックチェーンＭに記録することによって、第１主体に返金してもよい。

[0079] さらに管理装置５は、生成したブロックチェーンＢ４を、ゲートウェイ４、第２通信装置３及び複数の第１通信装置２を介して依頼装置１まで転送する。依頼装置１の受信部１１３は、複数の第１通信装置２のいずれかからブロックチェーンＢ４を受信して取得する。これにより、依頼装置１は、メインブロックチェーンＭに第１主体の債務（デポジット情報）が正常に追加されたか否かを知ることができる。メインブロックチェーンＭに第１主体の債務が正常に追加された場合に、通信システムＳは通信方法の後半部分の処理へ進む。

[0080] 図１０は、本実施形態に係る通信システムＳが実行する通信方法の後半部分の模式図である。図１１は、本実施形態で用いられるブロックチェーンＣ１、Ｃ２、Ｃ５及びメインブロックチェーンＭの模式図である。

[0081] 依頼装置１において、生成部１１１は、管理装置５からブロックチェーン

Ｂ４を取得する。そして生成部１１１は、署名Ｃ１１と、装置識別情報Ｃ１２と、実行依頼ブロックチェーンＣ１３と、証明書作成時刻Ｃ１４とを含むブロックチェーンＣ１を生成する。署名Ｃ１１、装置識別情報Ｃ１２及び証明書作成時刻Ｃ１４は、図９の署名Ｂ１１、装置識別情報Ｂ１２及び証明書作成時刻Ｂ１４と同様である。

[0082] 実行依頼ブロックチェーンＣ１３は、管理装置５から取得したブロックチェーンＢ４である。すなわち、実行依頼ブロックチェーンＣ１３は、依頼装置１が出力した実行依頼情報に加えて、管理装置５の署名が含まれている。そのため、実行依頼ブロックチェーンＣ１３の正当性は、管理装置５の公開鍵によって検証可能である。転送部１１２は、生成したブロックチェーンＣ１を複数の第１通信装置２のいずれかに転送する。

[0083] それぞれの第１通信装置２において、受信部２１１は、依頼装置１が送信したブロックチェーンＣ１を受信して取得する。受信したブロックチェーンＣ１に含まれる実行依頼情報が示す処理が未実行である場合（すなわちブロックチェーンＣ１が実行結果情報を含まない場合）に、実行部２１５は、受信したブロックチェーンＣ１に含まれる実行依頼情報が示す処理が実行可能か否かを判定する。例えば実行依頼情報がセンサ値の取得を示している場合に、第１通信装置２にセンサを含む機器６が接続されていれば、実行部２１５は、処理を実行可能であると判定する。実行部２１５は、実行依頼情報が示す金額又はトークン数が所定値以上であることを条件として、処理を実行可能であると判定してもよい。

[0084] 実行部２１５が実行可能でないと判定した場合に、転送部２１３は、受信したブロックチェーンＣ１を他の第１通信装置２に署名を付加することなく転送する。ブロックチェーンＣ１は、実行依頼情報が示す処理を実行可能な第１通信装置２に到達するまで、繰り返し転送される。

[0085] 実行部２１５は、実行可能であると判定した場合に、機器６を用いて実行依頼情報が示す処理を実行する。そして実行部２１５は、実行した処理の実行結果（例えばセンサ値）を機器６から取得する。

[0086] 署名部２１２は、受信したブロックチェーンＣ１に、ナンス値Ｃ１５と、署名Ｃ２１と、装置識別情報Ｃ２２と、実行結果情報Ｃ２３と、証明書作成時刻Ｃ２４と、ハッシュ値Ｃ２５とを付加したブロックチェーンＣ２を出力する。ナンス値Ｃ１５、署名Ｃ２１、装置識別情報Ｃ２２、証明書作成時刻Ｃ２４及びハッシュ値Ｃ２５は、図４のナンス値Ａ１５、署名Ａ２１、装置識別情報Ａ２２、証明書作成時刻Ａ２３及びハッシュ値Ａ２４と同様である。

[0087] 実行結果情報Ｃ２３は、実行部２１５が取得した実行結果と、処理を実行した機器６を有する第２主体に関連付けられた口座情報とを示す。口座情報は、第２主体が有する金銭又は金銭に対応するトークンを管理する口座（ウォレット）の識別情報を示す。口座情報は、第１通信装置２の記憶部２２に予め記憶されてもよく、第１通信装置２に接続されている機器６から入力されてもよい。

[0088] 転送部２１３は、署名部２１２が署名及び実行結果を付加したブロックチェーンＣ２を、複数の第１通信装置２のいずれかに転送する。

[0089] 複数の第１通信装置２は、第１の実施形態と同様に、署名及び実行結果が付加されたブロックチェーンＣ２に、署名を付加して転送することを繰り返す。ここで、第１通信装置２は、少なくとも署名及び実行結果が付加されたブロックチェーンＣ２の内容を含むブロックチェーンを受信して処理する。少なくとも署名及び実行結果が付加されたブロックチェーンＣ２の内容を含むブロックチェーンは、ブロックチェーンＣ２そのものであってもよく、ブロックチェーンＣ２に基づいて生成されたブロックチェーンであってもよい。所定時間内（ここでは１分３０秒以内）に所定数（ここでは４個）の署名が付加されなかったブロックチェーンＣ２は消滅する。ここで消滅条件とする署名の数は、第１の実施形態よりも１個増加している。これは、第１通信装置２によって実行結果が付加された後に（すなわちブロックチェーンＣ２を起点として）、第１の実施形態と同等の保護を与えるためである。

[0090] そして所定時間内に所定数の署名が付加されたブロックチェーンＣ４は、

第２通信装置３に到達する。第２通信装置３は、ブロックチェーンＣ４を、ゲートウェイ４を介して広域ネットワークＮ上の管理装置５に転送する。ここで、第２通信装置３は、少なくとも署名及び実行結果が付加されたブロックチェーンＣ２の内容を含むブロックチェーンを受信して処理する。少なくとも署名及び実行結果が付加されたブロックチェーンＣ２の内容を含むブロックチェーンは、ブロックチェーンＣ２そのものであってもよく、ブロックチェーンＣ２に基づいて生成されたブロックチェーンであってもよい。

[0091] 管理装置５は、広域ネットワークＮを介して、第２通信装置３が送信したブロックチェーンＣ４を受信する。そして管理装置５は、メインブロックチェーンＭに、ナンス値Ｍ１を付加するとともに、署名Ｃ５１と、ハッシュ値Ｃ５２と、実行情報Ｃ５３と、債権情報Ｃ５４と、受信したブロックチェーンＣ４とを含むブロックチェーンＣ５を追加する。ナンス値Ｍ１、署名Ｃ５１、ハッシュ値Ｃ５２及び実行情報Ｃ５３は、図９のナンス値Ｍ１、署名Ｂ４１、ハッシュ値Ｂ４２及び実行情報Ｂ４３と同様である。

[0092] 債権情報Ｃ５４は、処理を実行した第２主体が有する債権を記録した情報であり、例えば実行結果情報が示す第２主体の口座に実行依頼情報が示す金額又はトークン数（すなわち金銭に対応する値）を加算するトランザクションを示す。これにより、メインブロックチェーンＭには、第１主体が依頼した処理が第２主体によって実行された後に第１主体の債務に対応する第２主体の債権を記録できるため、第２主体が処理を実行したことが確認された後に第１主体から第２主体への支払い等を実行できる。

[0093] さらに管理装置５は、生成したブロックチェーンＣ５を、ゲートウェイ４、第２通信装置３及び複数の第１通信装置２を介して依頼装置１まで転送する。依頼装置１の受信部１１３は、複数の第１通信装置２のいずれかからブロックチェーンＣ５を受信して取得する。これにより、依頼装置１は、いずれかの第１通信装置２によって実行された処理の実行結果を知ることができる。

[0094] 図８～図１１の例では第１主体と第２主体との間でメインブロックチェー

ンM上に記録されたトランザクションによって金銭又はトークンの授受が行われているが、第１主体の口座から管理装置５の口座へ送金し、管理装置５の口座から第２主体の口座へ送金することによって、金銭又はトークンの授受が行われてもよい。

[0095] 図１２は、本実施形態に係る第１通信装置２が実行する通信方法のフローチャートを示す図である。第１通信装置２において、受信部２１１は、依頼装置１、他の第１通信装置２又は第２通信装置３が送信したブロックチェーンを受信して取得する（Ｓ３１）。

[0096] 受信したブロックチェーンが所定の消滅条件を満たす場合に（Ｓ３２のＹＥＳ）、消滅部２１４は、受信したブロックチェーンを転送せずに消滅させる（Ｓ３３）。消滅条件は、ブロックチェーンに実行結果情報が含まれているか否かで異なる。具体的には、実行結果情報が含まれていないブロックチェーンの消滅条件は、署名数が３個未満であり、かつブロックチェーンの生成時刻から１分が経過していることである。実行結果情報が含まれているブロックチェーンの消滅条件は、署名数が４個未満であり、かつブロックチェーンの生成時刻から１分３０秒が経過していることである。

[0097] 受信したブロックチェーンが所定の消滅条件を満たさない場合であって（Ｓ３２のＮＯ）、受信したブロックチェーンに含まれる実行依頼情報が示す処理が未実行である場合に（Ｓ３４のＮＯ）、実行部２１５は、受信したブロックチェーンに含まれる実行依頼情報が示す処理が実行可能か否かを判定する。

[0098] 実行部２１５が実行可能でないと判定した場合に（Ｓ３５のＮＯ）、第１通信装置２はステップＳ４０へ進む。実行部２１５が実行可能であると判定した場合に（Ｓ３５のＹＥＳ）、実行部２１５は、機器６を用いて実行依頼情報が示す処理を実行し、実行した処理の実行結果を機器６から取得する（Ｓ３６）。

[0099] 受信したブロックチェーンに含まれる実行依頼情報が示す処理が実行済である場合であって（Ｓ３４のＹＥＳ）、受信したブロックチェーンの署名数

が所定の閾値に到達している場合に（Ｓ３７のＮＯ）、第１通信装置２はステップＳ４０へ進む。

[0100] 受信したブロックチェーンに含まれる実行依頼情報が示す処理が実行済である場合であって（Ｓ３４のＹＥＳ）、受信したブロックチェーンの署名数が所定の閾値未満である場合に（Ｓ３７のＹＥＳ）、又はステップＳ３６で実行部２１５が処理を実行した場合に、署名部２１２は、所定の条件を満たすナンス値及びハッシュ値を算出する（Ｓ３８）。そして署名部２１２は、受信したブロックチェーンに、算出したナンス値及びハッシュ値と、第１通信装置２の署名とを付加したブロックチェーンを出力する（Ｓ３９）。署名部２１２は、ステップＳ３６で実行部２１５が処理を実行した場合には、処理の実行結果を示す実行結果情報をブロックチェーンにさらに付加する。

[0101] 転送部２１３は、署名数が所定の閾値に到達しているブロックチェーン又は署名部２１２が署名を付加したブロックチェーンを、複数の第１通信装置２のいずれか又は第２通信装置３に転送する（Ｓ４０）。

[0102] ［適用例］

本実施形態に係る通信システムＳは、例えば駐車場の予約システムに適用される。この場合に、機器６は、例えば駐車場の監視装置に搭載されている。ユーザが端末を用いて駐車場の予約を希望すると、依頼装置１は駐車場の予約を依頼するブロックチェーンを生成し、本実施形態に係る通信方法を用いてマルチホップネットワーク上で転送する。これにより、メインブロックチェーンには、ユーザの口座から所定の金額（デポジット）が減算されるトランザクションが記録される。

[0103] ユーザの口座からデポジットが引き落とされた後に、依頼装置１は駐車場の予約を依頼するブロックチェーンを再び本実施形態に係る通信方法を用いてマルチホップネットワーク上で転送する。いずれかの駐車場に設置された監視装置が予約の受付が可能である（例えば空きスペースがある）と判定した場合に、監視装置は予約を受け付ける処理を行う。

[0104] その後、監視装置は、駐車場の予約結果（例えば駐車可能なスペースの場

所）を示すブロックチェーンをマルチホップネットワーク上で転送する。そしてメインブロックチェーンには、ユーザのデポジットから駐車場の管理者の口座へ料金を加算するトランザクションが記録される。ユーザが実際に駐車したことを監視装置が検出したことを条件として、メインブロックチェーンに、ユーザのデポジットから駐車場の管理者の口座へ料金を加算するトランザクションが記録されてもよい。

[0105] これにより通信システムＳは、ユーザの端末及び駐車場に設置された監視装置が広域ネットワークＮに接続されていない場合であっても、駐車場の予約データをマルチホップネットワーク上で改ざんを抑制しつつ転送でき、駐車可能なスペースを予約し、料金の支払いを行うことができる。

[0106] ［実施形態の効果］

本実施形態に係る通信システムＳは、第一の実施形態と同様に、第三者がマルチホップネットワーク内でブロックチェーンを改ざんしようとしても、ブロックチェーンに所定数の署名を付加することは消滅条件が定める所定時間内では困難であるため、複数の通信装置の間で伝送される追加対象のデータが改ざんされるのを抑制できる。さらに通信システムＳは、１回目のブロックチェーンの転送で第１主体の債務をメインブロックチェーンに記録してから、２回目のブロックチェーンの転送でいずれかの第２主体に処理を実行させるため、第２主体が処理を実行した後に第１主体が支払い等の債務を免れる事態を予防できる。

[0107] 以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されず、その要旨の範囲内で種々の変形及び変更が可能である。例えば、装置の分散・統合の具体的な実施の形態は、以上の実施の形態に限られず、その全部又は一部について、任意の単位で機能的又は物理的に分散・統合して構成することができる。また、複数の実施の形態の任意の組み合わせによって生じる新たな実施の形態も、本発明の実施の形態に含まれる。組み合わせによって生じる新たな実施の形態の効果は、もとの実施の形態の効果を合わせ持つ。

[0108] 第１通信装置２及び第２通信装置３のプロセッサは、図６、７、１２に示す通信方法に含まれる各ステップ（工程）の主体となる。すなわち、第１通信装置２及び第２通信装置３のプロセッサは、図６、７、１２に示す通信方法を実行するためのプログラムを記憶部から読み出し、該プログラムを実行して通信システムＳの各部を制御することによって、図６、７、１２に示す通信方法を実行する。図６、７、１２に示す通信方法に含まれるステップは一部省略されてもよく、ステップ間の順番が変更されてもよく、複数のステップが並行して行われてもよい。

符号の説明

[0109] Ｓ　通信システム

１　依頼装置

１１　制御部

１１１　生成部

１１２　転送部

１１３　受信部

２　第１通信装置

２１　制御部

２１１　受信部

２１２　署名部

２１３　転送部

２１４　消滅部

２１５　実行部

３　第２通信装置

３１　制御部

３１１　受信部

３１３　転送部

５　管理装置

請求の範囲

[請求項1] 互いに通信可能な複数の第１通信装置と、前記第１通信装置及び広域ネットワークに接続する第２通信装置とを含む通信システムであって、

前記複数の第１通信装置それぞれは、

他の通信装置からブロックチェーンを受信する第１受信部と、

前記第１受信部が受信した前記ブロックチェーンに含まれている署名の数が所定の閾値未満である場合に前記第１受信部が受信した前記ブロックチェーンに署名を付加した前記ブロックチェーンを出力し、前記署名の数が前記所定の閾値に到達している場合に前記第１受信部が受信した前記ブロックチェーンを出力する署名部と、

前記署名部が出力した前記ブロックチェーンを他の通信装置に転送する第１転送部と、

を備え、

前記第２通信装置は、

他の通信装置から前記ブロックチェーンを受信する第２受信部と、

前記第２受信部が受信した前記ブロックチェーンに含まれている署名の数が前記所定の閾値未満である場合に前記第２受信部が受信した前記ブロックチェーンを他の通信装置に転送し、前記署名の数が前記所定の閾値に到達している場合に前記第２受信部が受信した前記ブロックチェーンを前記広域ネットワークに転送する第２転送部と、

を備える通信システム。

[請求項2] 前記複数の第１通信装置それぞれは、前記第１受信部が受信した前記ブロックチェーンに含まれている署名の数が前記所定の閾値未満であり、かつ前記第１受信部が受信した前記ブロックチェーンの生成時刻から所定の時間が経過している場合に、前記第１受信部が受信した前記ブロックチェーンを消滅させる消滅部をさらに有する、請求項１

に記載の通信システム。

[請求項3] 前記通信システムは、前記複数の第１通信装置に処理の実行を依頼する依頼装置をさらに含み、

前記複数の第１通信装置それぞれは、指定された処理を実行する実行部をさらに備え、

前記依頼装置は、

実行依頼を含む前記ブロックチェーンを生成する生成部と、

前記生成部が生成した前記ブロックチェーンを他の通信装置に転送する第３転送部と、

所定の署名が付加された前記ブロックチェーンを受信する第３受信部と、を備え、

前記依頼装置において、

前記生成部は、前記第３受信部が受信した前記所定の署名が付加された前記ブロックチェーンを含む第２ブロックチェーンを生成し、

前記第３転送部は、前記生成部が生成した前記第２ブロックチェーンを他の通信装置に転送し、

前記複数の第１通信装置それぞれにおいて、

前記第１受信部は、前記依頼装置から前記第２ブロックチェーンを受信し、

前記実行部は、前記第１受信部が受信した前記第２ブロックチェーンに含まれている前記実行依頼に対応する処理を実行可能な場合に、前記処理を実行し、

前記署名部は、前記実行部が前記処理を実行した場合に前記第１受信部が受信した前記第２ブロックチェーンに署名及び前記処理の実行結果を付加した前記第２ブロックチェーンを出力し、前記第１受信部が受信した前記第２ブロックチェーンに含まれている署名の数が所定の閾値未満である場合に前記第１受信部が受信した前記第２ブロックチェーンに署名を付加した前記第２ブロックチェーンを出力し、前

記署名の数が前記所定の閾値に到達している場合に前記第１受信部が受信した前記第２ブロックチェーンを出力し、

前記第１転送部は、前記署名部が出力した前記第２ブロックチェーンを他の通信装置に転送する、請求項１又は２に記載の通信システム。

[請求項4] 前記依頼装置において、前記第３受信部は、前記実行結果が付加された前記第２ブロックチェーンを受信する、請求項３に記載の通信システム。

[請求項5] 前記通信システムは、前記広域ネットワークに接続しており、メインブロックチェーンを管理する管理装置をさらに含み、

前記管理装置は、前記ブロックチェーンを受信した場合に、前記ブロックチェーンに含まれている前記実行依頼を生成した第１主体の債務を示す情報を前記メインブロックチェーンに付加し、

前記管理装置は、前記第２ブロックチェーンを受信した場合に、前記第２ブロックチェーンに含まれている前記実行結果を生成した第２主体の債権を示す情報を前記メインブロックチェーンに付加する、請求項３又は４に記載の通信システム。

[請求項6] 前記管理装置は、前記ブロックチェーンを受信した場合に、前記第１主体に関連付けられた金銭に対応する値から減算する値を示す情報を前記メインブロックチェーンに付加し、

前記管理装置は、前記第２ブロックチェーンを受信した場合に、前記第２主体に関連付けられた金銭に対応する値に加算する値を示す情報を前記メインブロックチェーンに付加する、請求項５に記載の通信システム。

[請求項7] 互いに通信可能な複数の第１通信装置と、前記第１通信装置及び広域ネットワークに接続する第２通信装置とを含む通信システムにおいて、

前記複数の第１通信装置それぞれのプロセッサが、

他の通信装置からブロックチェーンを受信するステップと、

前記受信するステップが受信した前記ブロックチェーンに含まれている署名の数が所定の閾値未満である場合に前記受信するステップが受信した前記ブロックチェーンに署名を付加した前記ブロックチェーンを出力し、前記署名の数が前記所定の閾値に到達している場合に前記受信するステップが受信した前記ブロックチェーンを出力するステップと、

前記出力するステップが出力した前記ブロックチェーンを他の通信装置に転送するステップと、

を実行し、

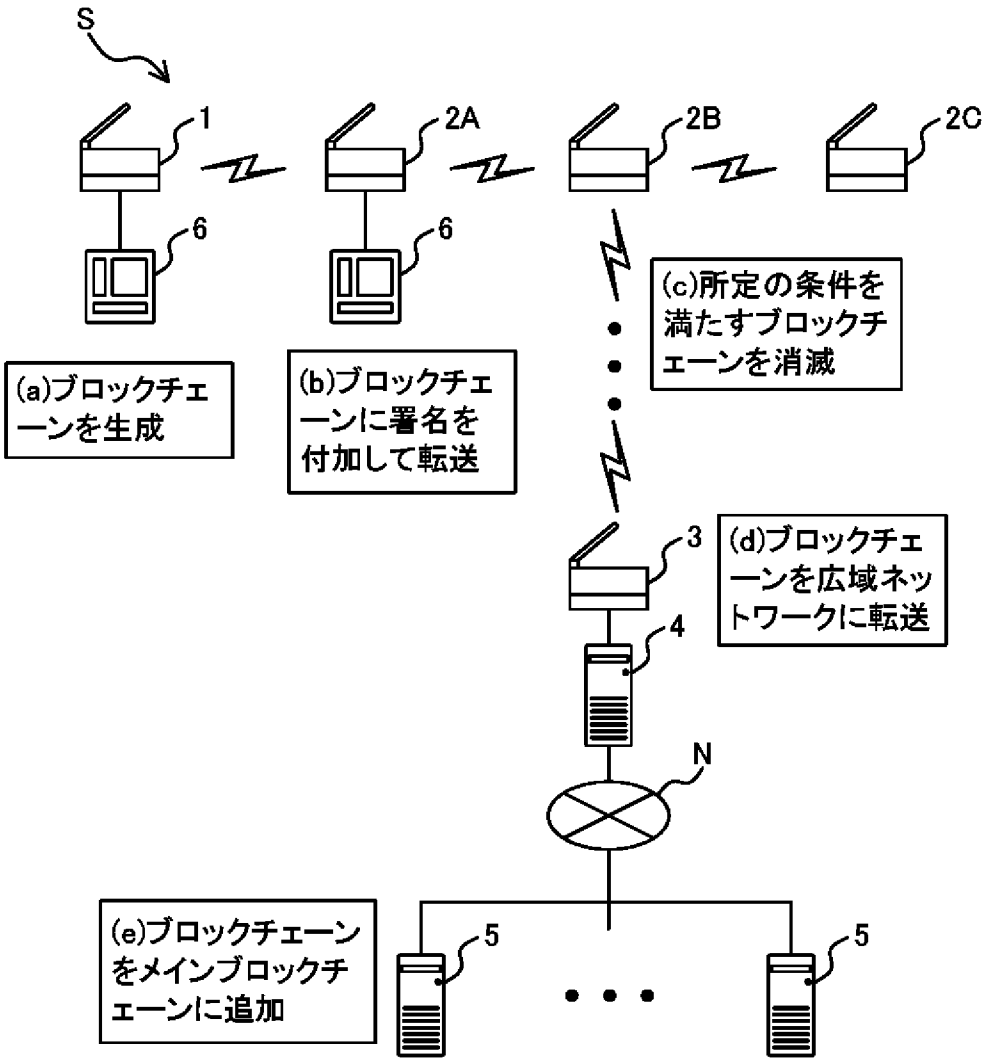
前記第２通信装置のプロセッサが、

他の通信装置から前記ブロックチェーンを受信するステップと、

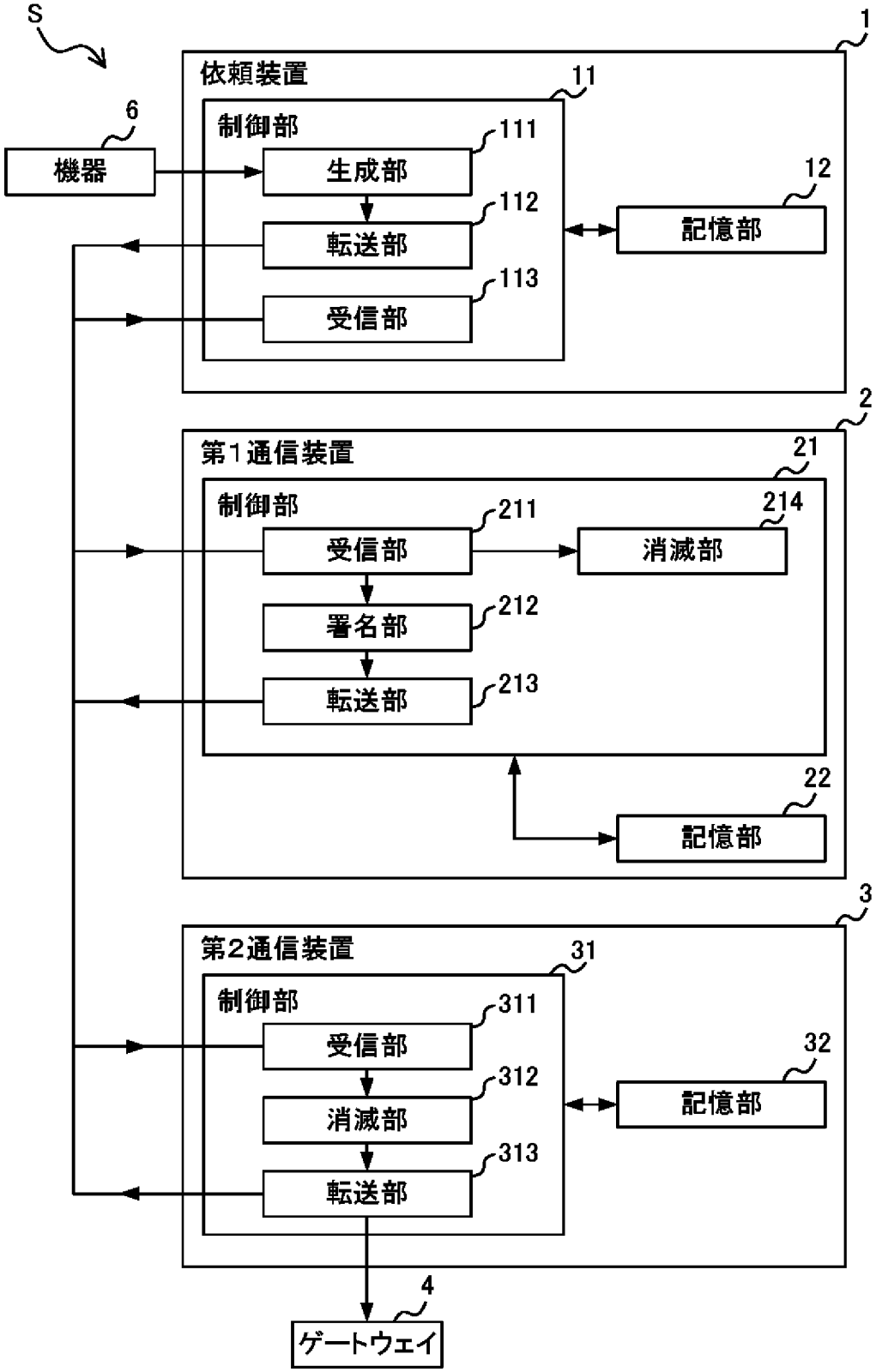
前記受信するステップが受信した前記ブロックチェーンに含まれている署名の数が前記所定の閾値未満である場合に前記受信するステップが受信した前記ブロックチェーンを他の通信装置に転送し、前記署名の数が前記所定の閾値に到達している場合に前記受信するステップが受信した前記ブロックチェーンを前記広域ネットワークに転送するステップと、

を実行する、通信方法。

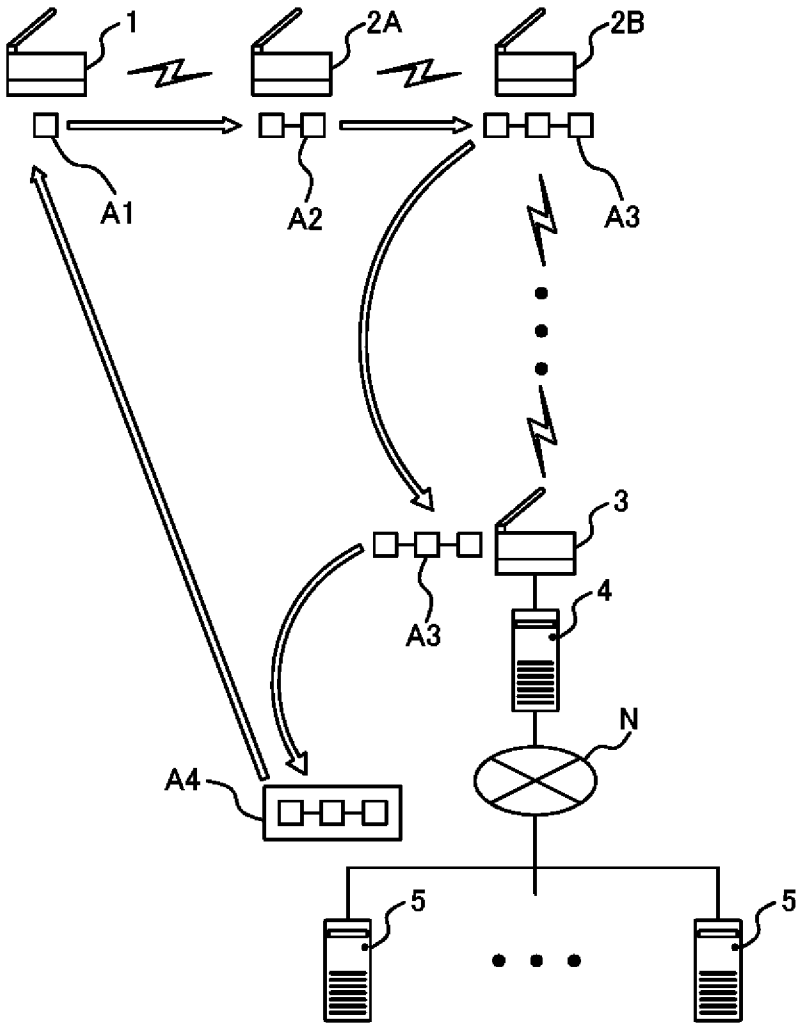
[図1]


S
1
2A
2B
2C
6
6
(a)ブロックチェーンを生成
(b)ブロックチェーンに署名を付加して転送
(c)所定の条件を満たすブロックチェーンを消滅
3
(d)ブロックチェーンを広域ネットワークに転送
4
N
(e)ブロックチェーンをメインブロックチェーンに追加
5
5

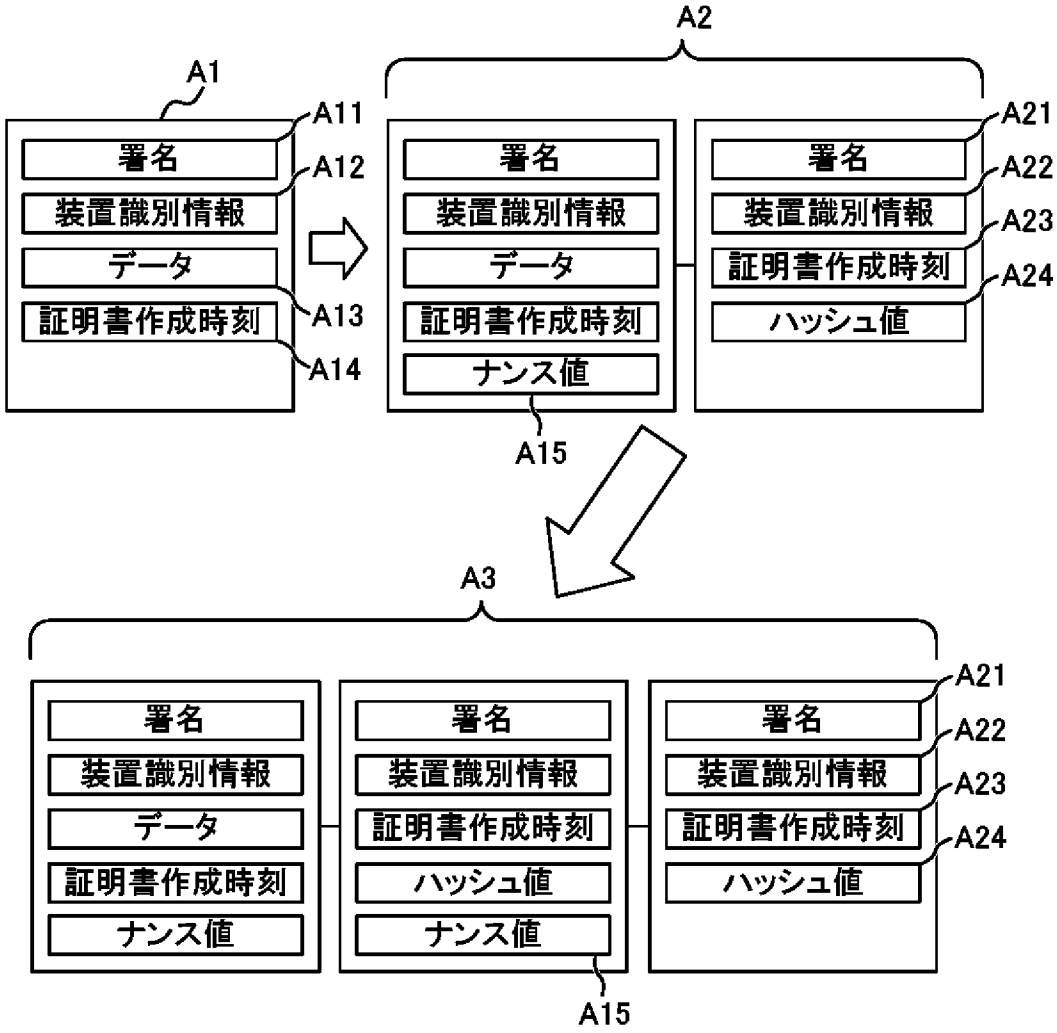
[図2]


S
1
依頼装置
11
制御部
6
機器
111
生成部
12
112
転送部
記憶部
113
受信部
2
第1通信装置
21
制御部
211
214
受信部
消滅部
212
署名部
213
転送部
22
記憶部
3
第2通信装置
31
制御部
311
受信部
32
312
消滅部
記憶部
313
転送部
4
ゲートウェイ

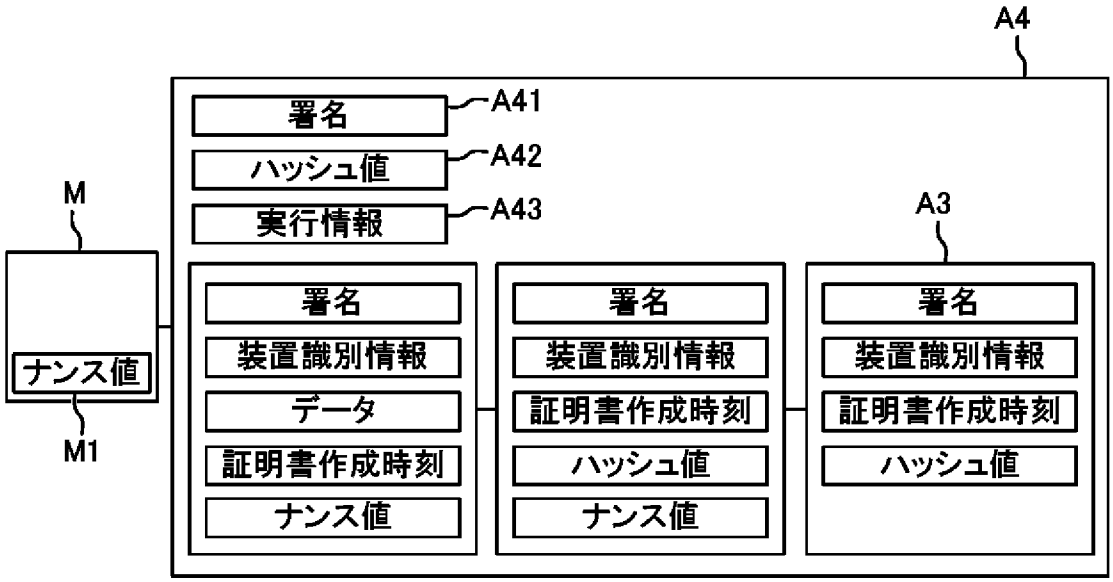
[図3]



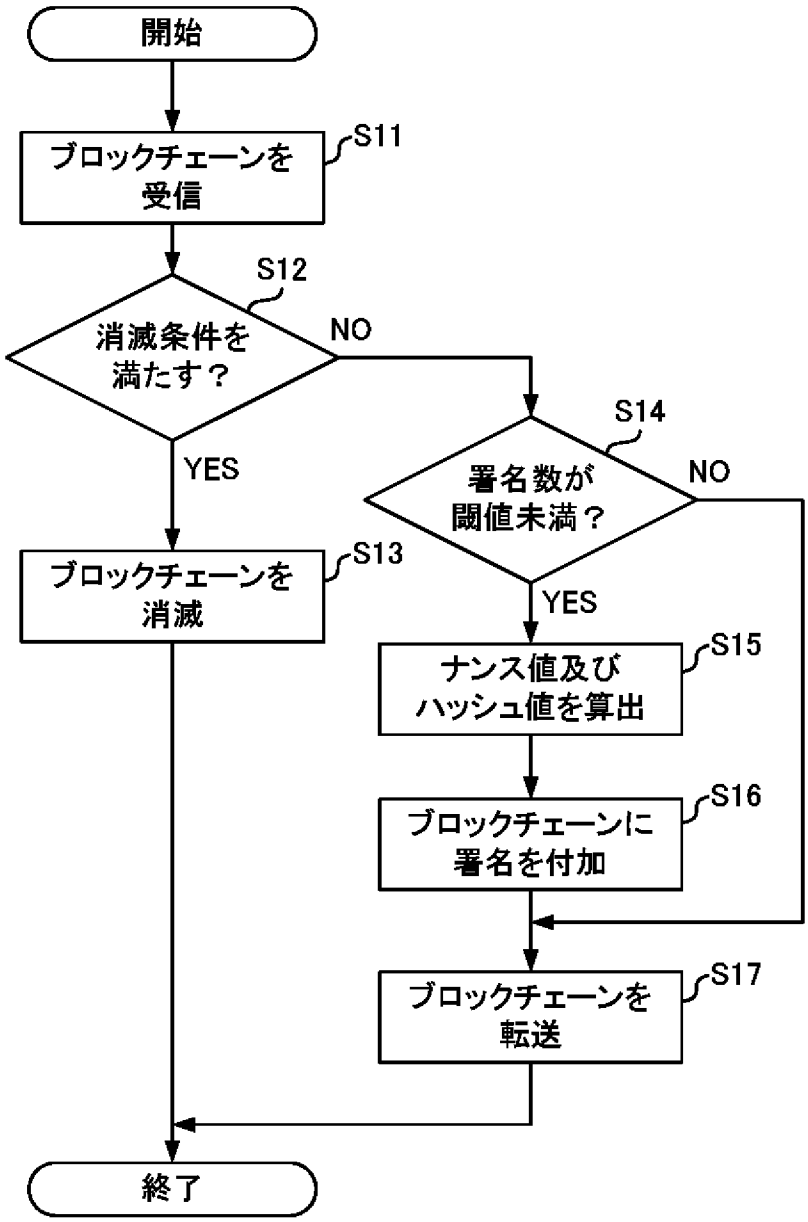
[図4]


A1
A2
A3
A11
A12
A13
A14
A15
A21
A22
A23
A24
署名
装置識別情報
データ
証明書作成時刻
ナンス値
ハッシュ値

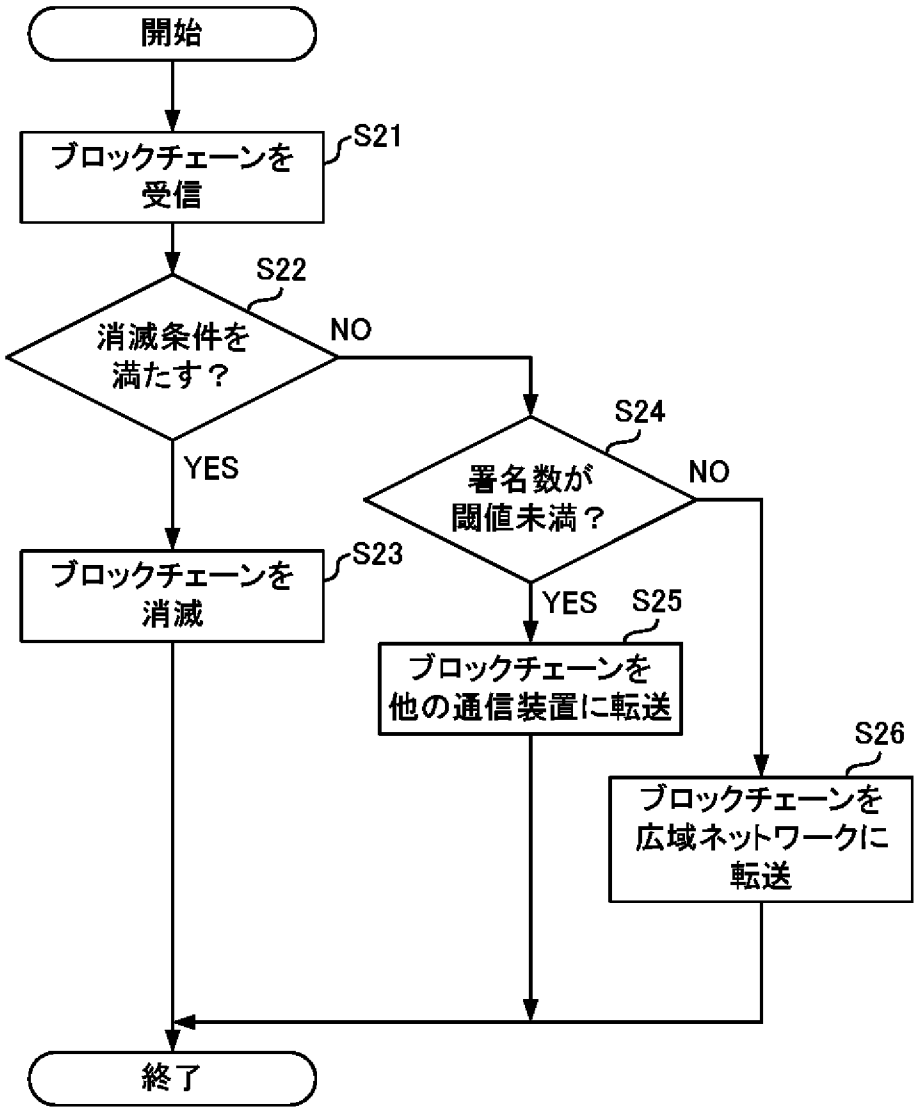
[図5]


A4
A41
A42
A43
M
M1
A3
署名
ハッシュ値
実行情報
ナンス値
装置識別情報
データ
証明書作成時刻

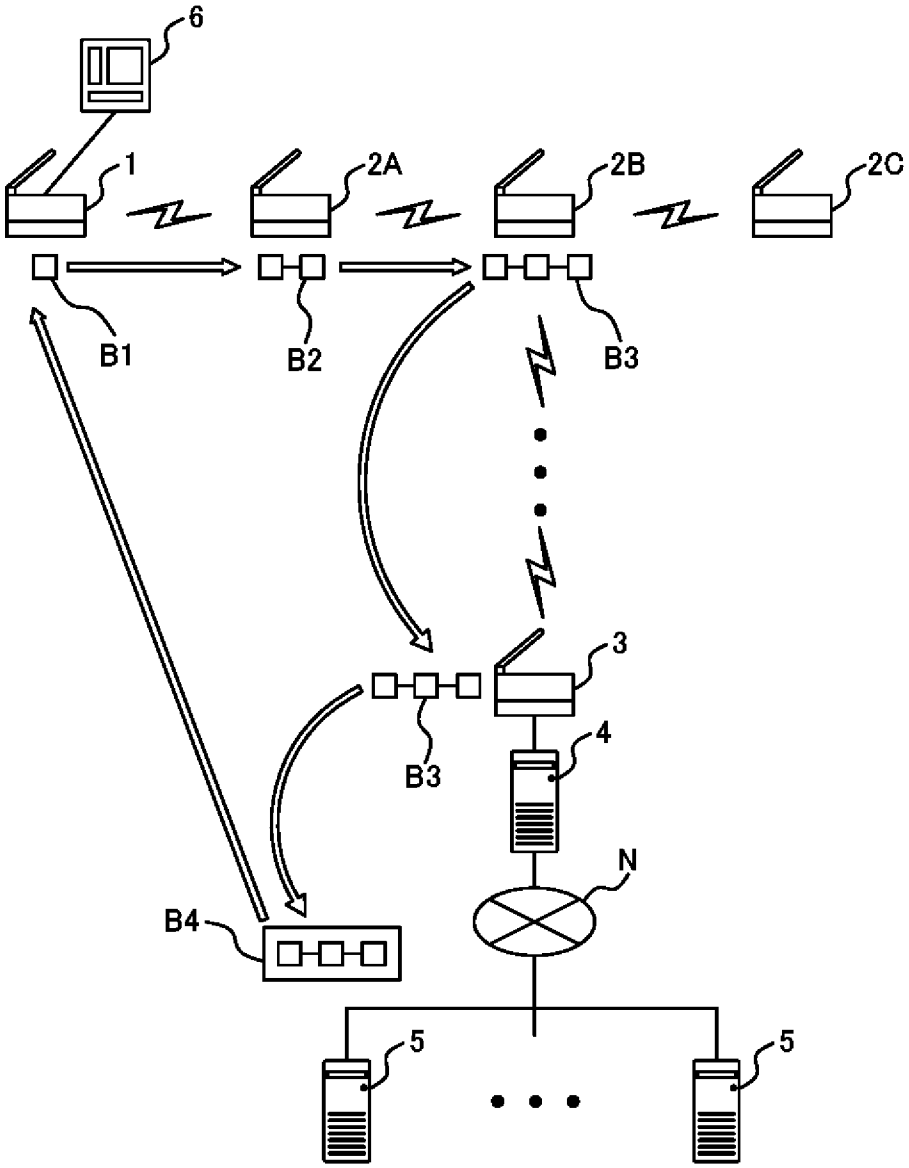
[図6]


開始
ブロックチェーンを受信
S11
S12
消滅条件を満たす？
NO
YES
S13
ブロックチェーンを消滅
S14
署名数が閾値未満？
NO
YES
S15
ナンス値及びハッシュ値を算出
S16
ブロックチェーンに署名を付加
S17
ブロックチェーンを転送
終了

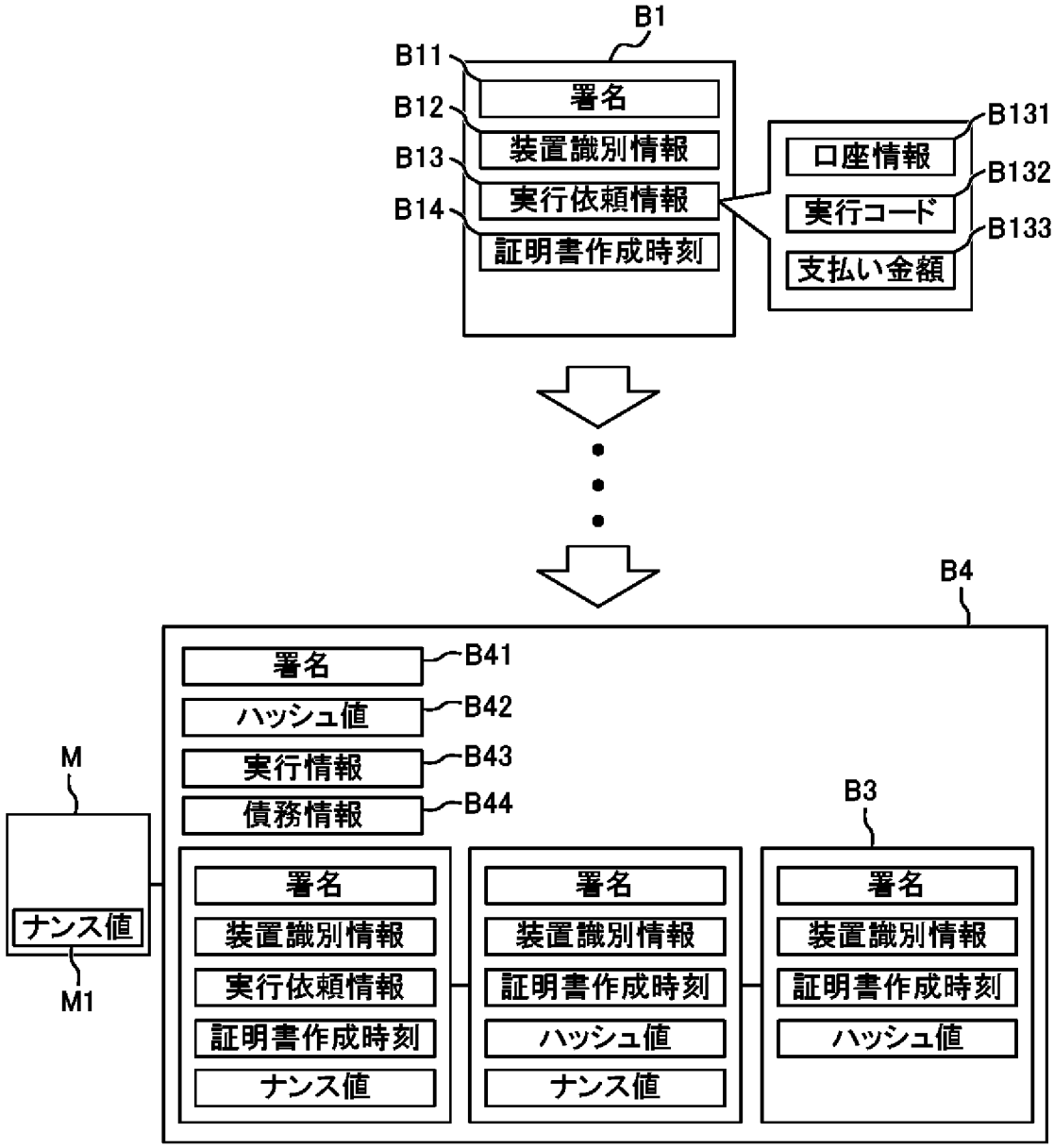
[図7]


開始
ブロックチェーンを受信
S21
S22
消滅条件を満たす？
NO
YES
S24
署名数が閾値未満？
NO
YES
S25
ブロックチェーンを消滅
S23
ブロックチェーンを他の通信装置に転送
S26
ブロックチェーンを広域ネットワークに転送
終了

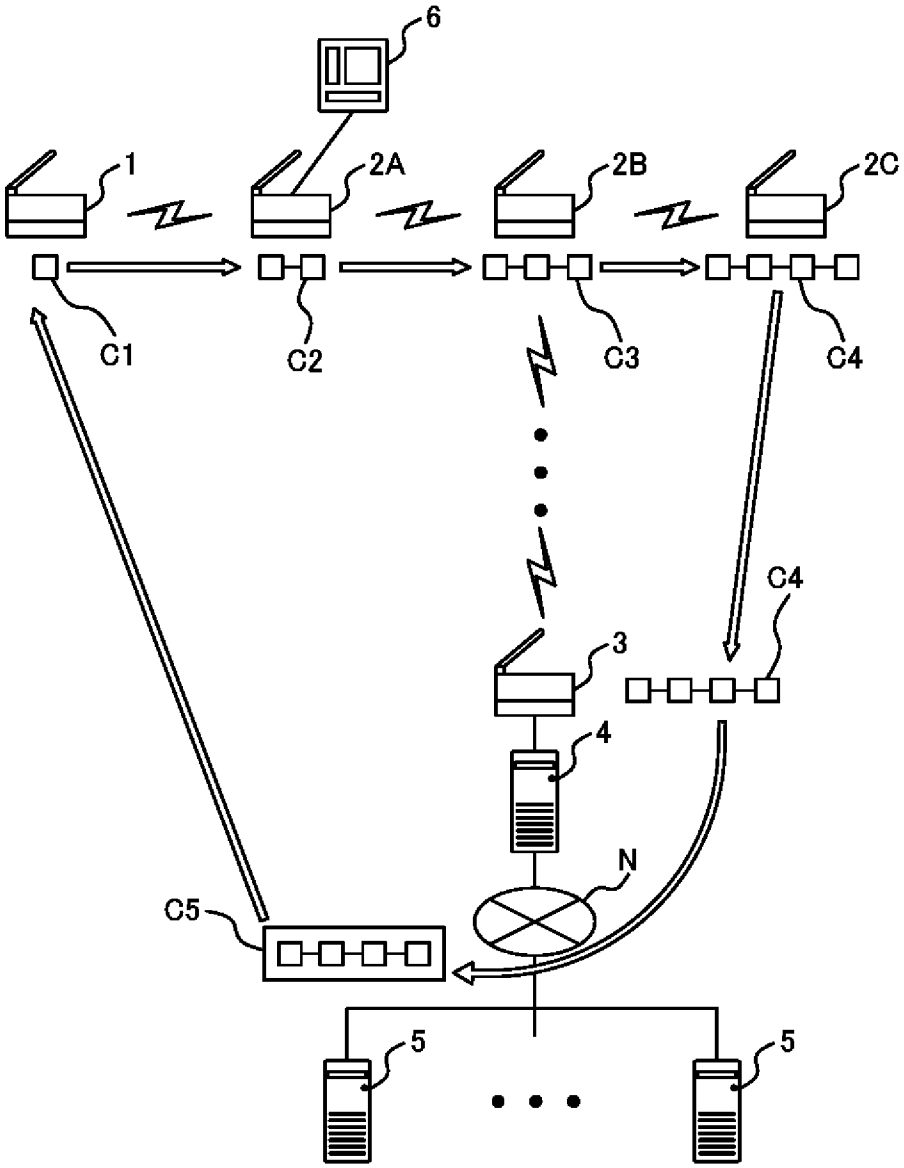
[図8]



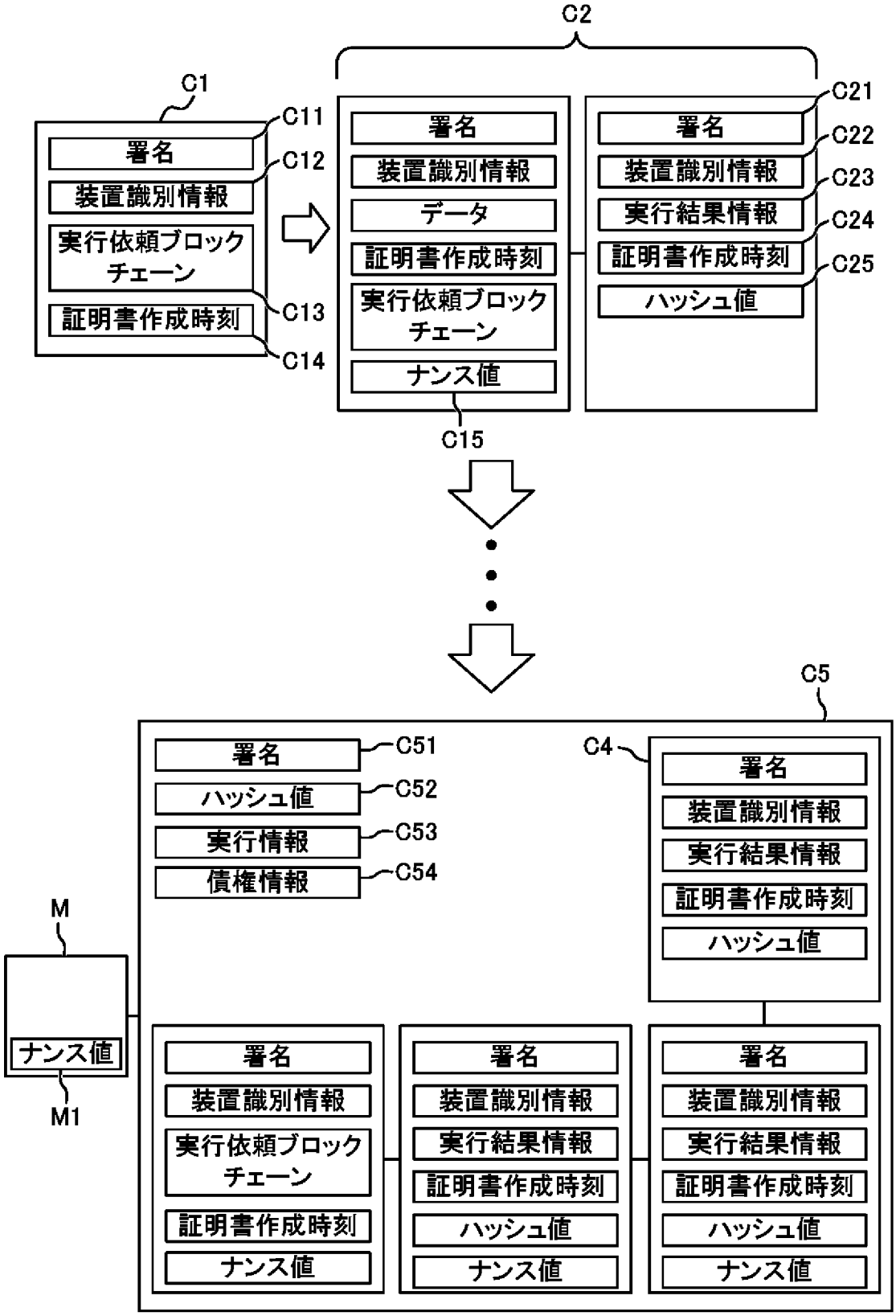
[図9]


B1
B11
署名
B12
装置識別情報
B13
実行依頼情報
B14
証明書作成時刻
B131
口座情報
B132
実行コード
B133
支払い金額
B4
署名
B41
ハッシュ値
B42
実行情報
B43
債務情報
B44
M
ナンス値
M1
B3
署名
装置識別情報
実行依頼情報
証明書作成時刻
ナンス値
署名
装置識別情報
証明書作成時刻
ハッシュ値
ナンス値
署名
装置識別情報
証明書作成時刻
ハッシュ値

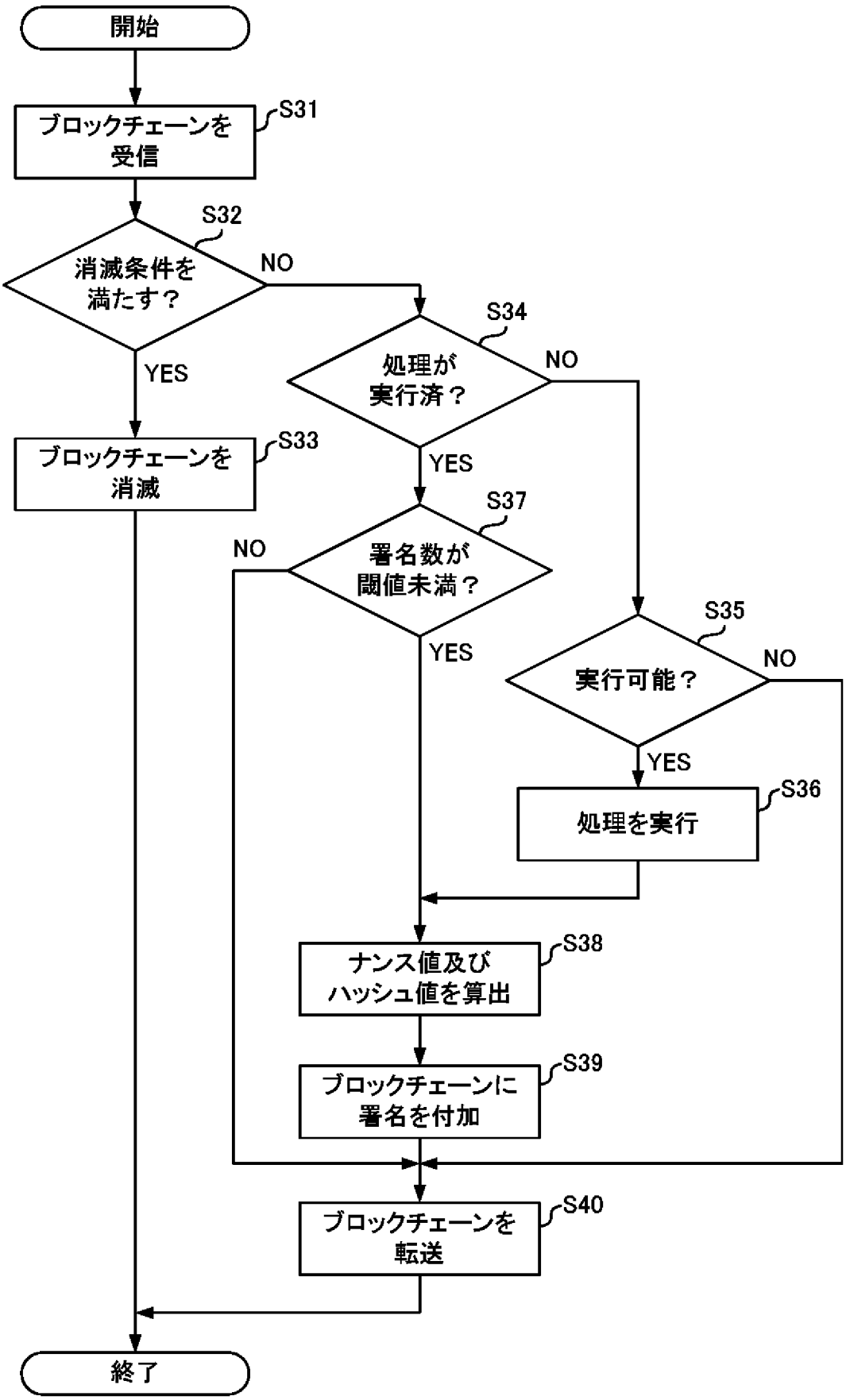
[図10]



[図11]


C1
C11
署名
C12
装置識別情報
実行依頼ブロック
チェーン
C13
証明書作成時刻
C14
C2
署名
装置識別情報
データ
証明書作成時刻
実行依頼ブロック
チェーン
ナンス値
C15
C21
署名
C22
装置識別情報
C23
実行結果情報
C24
証明書作成時刻
C25
ハッシュ値
C5
署名
C51
ハッシュ値
C52
実行情報
C53
債権情報
C54
C4
署名
装置識別情報
実行結果情報
証明書作成時刻
ハッシュ値
M
ナンス値
M1
署名
装置識別情報
実行依頼ブロック
チェーン
証明書作成時刻
ナンス値
署名
装置識別情報
実行結果情報
証明書作成時刻
ハッシュ値
ナンス値
署名
装置識別情報
実行結果情報
証明書作成時刻
ハッシュ値
ナンス値

[図12]


開始
ブロックチェーンを受信
S31
S32
消滅条件を満たす？
NO
YES
S34
処理が実行済？
NO
YES
S33
ブロックチェーンを消滅
S37
署名数が閾値未満？
NO
YES
S35
実行可能？
NO
YES
S36
処理を実行
S38
ナンス値及びハッシュ値を算出
S39
ブロックチェーンに署名を付加
S40
ブロックチェーンを転送
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/034359

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04W12/10(2009.01)i, H04W84/22(2009.01)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)
Int.Cl. H04B7/24-7/26, H04W4/00-99/00, H04L1/00-29/14

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 1971-2019
Registered utility model specifications of Japan 1996-2019
Published registered utility model applications of Japan 1994-2019

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	WO 2018/073482 A1 (NOKIA TECHNOLOGIES OY) 26 April 2018, paragraphs [0021]-[0030] (Family: none)	1-7
A	CN 107508859 A (UNIV BEIJING JIAOTONG) 22 December 2017, paragraphs [0044]-[0049] (Family: none)	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
"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
12.11.2019	26.11.2019
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０３４３５９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04W12/10(2009.01)i, H04W84/22(2009.01)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.　H04B7/24-7/26, H04W4/00-99/00, H04L1/00-29/14

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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	WO 2018/073482 A1 (NOKIA TECHNOLOGIES OY) 2018.04.26, 段落[0021]-[0030] (ファミリーなし)	1-7
A	CN 107508859 A (UNIV BEIJING JIAOTONG) 2017.12.22, 段落[0044]-[0049] (ファミリーなし)	1-7

☐　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
１２．１１．２０１９	２６．１１．２０１９

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）　５Ｊ　３８６３
横田　有光
電話番号　０３－３５８１－１１０１　内線　３５３４