

(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5月22日(22.05.2020)



(10) 国際公開番号

WO 2020/100602 A1

(51) 国際特許分類:
G06F 16/17 (2019.01) G06F 16/182 (2019.01)

(21) 国際出願番号: PCT/JP2019/042658

(22) 国際出願日: 2019年10月30日(30.10.2019)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

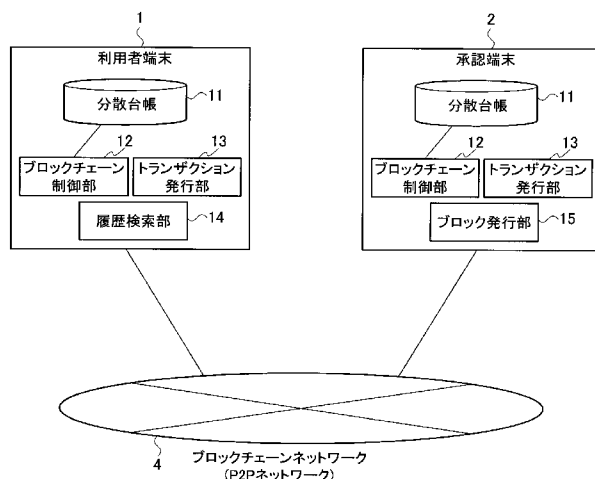
(30) 優先権データ:
特願 2018-213190 2018年11月13日(13.11.2018) JP

(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9-1 1 N T T 知的財産センタ内 Tokyo (JP). 石田 達郎 (ISHIDA Tatsuro); 〒1808585 東京都武蔵野市緑町3丁目9-1 1 N T T 知的財産センタ内 Tokyo (JP). 大橋 盛徳 (OHASHI Shigenori); 〒1808585 東京都武蔵野市緑町3丁目9-1 1 N T T 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9-1 1 N T T 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9-1 1 N T T 知的財産センタ内 Tokyo (JP).

(54) Title: BLOCKCHAIN SYSTEM, APPROVAL TERMINAL, USER TERMINAL, HISTORY MANAGEMENT METHOD, AND HISTORY MANAGEMENT PROGRAM

(54) 発明の名称: ブロックチェーンシステム、承認端末、利用者端末、履歴管理方法、および、履歴管理プログラム



- 1 User terminal
- 2 Approval terminal
- 4 Blockchain network (P2P network)
- 11 Distributed ledger
- 12 Blockchain control unit
- 13 Transaction issuance unit
- 14 History search unit
- 15 Block issuance unit

(57) Abstract: The present invention enables a data history to be easily tracked in a blockchain. Provided is a blockchain system comprising a user terminal 1 and an approval terminal 2, wherein: the user terminal 1 includes a transaction issuance unit 13 for issuing a transaction to update the value of a smart contract variable; and the approval terminal 2 includes a block generation unit 153 for generating a block that includes a transaction, updating a variable value, and causing the block and an update block number of the block for which the variable value has been updated to be reflected in a distributed ledger 11 of the terminals of the blockchain system.

(57) 要約: ブロックチェーン上で、データの履歴を容易に追跡することを可能とする。利用者端末1と、承認端末2とを備えるブロックチェーンシステムであって、利用者端末1は、スマートコントラクトの変数の値を更新するトランザクションを発行するトランザクション発行部13を備え、承認端末2は、トランザクションを含むブロックを生成するとともに変数の値を更新し、前記ブロックと、前記変数の値を更新した当該ブロックの更新ブロック番号とをブロックチェーンシステムの端末の分散台帳11に反映させるブロック生成部153を備える。

(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, 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))

明 細 書

発明の名称：

ブロックチェーンシステム、承認端末、利用者端末、履歴管理方法、および、履歴管理プログラム

技術分野

[0001] 本発明は、スマートコントラクト型のブロックチェーンの履歴を管理する技術に関する。

背景技術

[0002] 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デジタル仮想通貨ビットコインを中心に普及しつつある。ブロックチェーンと呼ばれるこの仕組みにおいては、やり取りされる情報の信頼性が分散ネットワーク内の合意形成のプロセスによって担保され、かつ、改ざんや二重使用などの不正を系全体で防ぐことで健全性が保たれる。

[0003] ブロックチェーンでは、参加者間の取引情報（トランザクション）が「ブロック」という単位でまとめられ、各ブロックは数珠つなぎとなって時系列順に管理される。新たなブロックの承認は、Proof of Workなどの分散ネットワークにおける合意アルゴリズムによって形成される。新たなブロックの承認は、ブロック内部に記録された取引が系全体で合意されたことを示す。

[0004] このブロックチェーンを用いて管理される一連の取引情報の帳簿を「分散台帳」と呼び、ネットワークに参加する各端末は同一の分散台帳を保持している。近年では、分散台帳に高度なスクリプトコードを登録し、スクリプトコードの実行とその結果についても合意を得るブロックチェーン基盤技術も開発されている。例えばEthereumと呼ばれるブロックチェーン基盤は、トランザクションを入力としてスクリプトコードを実行し、その実行結果をツリー構造のキーバリュー型ストア（ステートDBと呼ぶ）に格納し、その時のストアの代表値もブロックに記録する分散台帳を持つ。このようにブロックチェーン上に登録され、各端末に登録および実行されるスクリプトコードは「

スマートコントラクト」と呼ばれている。

- [0005] スマートコントラクト型のブロックチェーンは、各ブロックと、そのブロック時点でスマートコントラクトのステートDBとが対応づけて管理されている（非特許文献1）。

先行技術文献

非特許文献

- [0006] 非特許文献1：「JavaScript API・ethereum/wiki Wiki・GitHub」、<https://github.com/ethereum/wiki/wiki/JavaScript-API#contract-methods>

発明の概要

発明が解決しようとする課題

- [0007] ブロックチェーンのデータ構造上、ブロック番号を指定し、そのブロック時点のステートを参照することは容易である。しかしながら、当該ブロックのステートの値が、過去のどのブロックでどのように遷移したのかを知るとは困難である。特に、情報のトレーサビリティを確保するという観点において、この問題は重要である。
- [0008] 例えば、ステートのある値の変化を追跡する等の高度な探索・追跡を行う場合、RDBMS等の外部データベースを用意して、ブロックチェーンから抽出した全てのデータを外部データベースに落とし込み、外部データベース上でインデックスを構築し所望のデータを探索・追跡する方法が考えられる。しかしながら、外部データベースを用いた探索システムを構築および維持することは、一般ユーザにとって高いコストを要することになる。
- [0009] 本発明は、上記課題を鑑みてなされたものであり、本発明の目的は、ブロックチェーン上で、データの履歴を容易に追跡することを可能とする技術を提供することにある。

課題を解決するための手段

- [0010] 上記目的を達成するため、本発明の一態様は、利用者端末と、承認端末とを備えるブロックチェーンシステムであって、前記利用者端末は、スマート

コントラクトの変数の値を更新するトランザクションを発行するトランザクション発行部を備え、前記承認端末は、前記トランザクションを含むブロックを生成するとともに前記変数の値を更新し、前記ブロックと、前記変数の値を更新した当該ブロックの更新ブロック番号とを前記ブロックチェーンシステムの端末の分散台帳に反映させるブロック生成部を備える。

[0011] 本発明の一態様は、ブロックチェーンシステムにおいてトランザクションを承認する承認端末であって、スマートコントラクトの変数の値を更新するトランザクションを受信する受信部と、前記トランザクションを含むブロックを生成するとともに前記変数の値を更新し、前記ブロックと、前記変数の値を更新した当該ブロックの更新ブロック番号とを前記ブロックチェーンシステムの端末の分散台帳に反映させるブロック生成部と、を備える。

[0012] 本発明の一態様は、ブロックチェーンシステムにおける利用者端末であって、ブロックチェーンの分散台帳と、スマートコントラクトの変数の値を更新するトランザクションを発行するトランザクション発行部と、前記分散台帳から前記変数の値が更新されたブロックの更新ブロック番号を取得し、前記更新ブロック番号から算出される検索ブロック番号を指定して、前記検索ブロック番号の時点のブロックにおける前記スマートコントラクトの変数の値および更新ブロック番号を、前記分散台帳から取得する履歴検索部と、を備える。

[0013] 本発明の一態様は、ブロックチェーンの履歴を管理する履歴管理方法であって、利用者端末は、スマートコントラクトの変数の値を更新するトランザクションを発行するトランザクション発行ステップを行い、承認端末は、前記トランザクションを含むブロックを生成し、前記変数の値を更新する生成ステップと、前記ブロックと、前記変数の値を更新した当該ブロックの更新ブロック番号とを、ブロックチェーンネットワークに接続された端末の分散台帳に反映させる同期ステップとを行う。

[0014] 本発明の一態様は、上記承認端末として、コンピュータを機能させることを特徴とするスマートコントラクト登録プログラムである。

発明の効果

[0015] 本発明によれば、ブロックチェーン上で、データの履歴を容易に追跡することを可能とする技術を提供することができる。

図面の簡単な説明

[0016] [図1]本発明の実施形態に係るブロックチェーンシステムの全体構成を示す図である。

[図2]分散台帳の構成を示す図である。

[図3]ブロック発行部の構成を示す構成図である。

[図4]ステートDBの更新ブロック番号の設定方法を説明する説明図である。

[図5]ブロック生成および履歴検索を示すシーケンス図である。

[図6]トランザクションの一例を示す図である。

発明を実施するための形態

[0017] 以下、本発明の実施の形態について、図面を参照して説明する。

[0018] 図1は、本実施形態のブロックチェーンシステムの全体構成を示す図である。本実施形態のブロックチェーンは、スマートコントラクト型ブロックチェーンであって、ブロックチェーン基盤技術の1つであるEthereumを用いる。Ethereumは、ブロックチェーンを、状態遷移を記録する分散台帳として用いるためのアプリケーション開発プラットフォームである。ただし、本願発明は、Ethereumに限定されるものではなく、Ethereum以外のブロックチェーンに用いてもよい。

[0019] 図1に示すブロックチェーンシステムは、利用者端末1と、承認端末2とを備える。これらの端末1、2は、P2Pネットワークであるブロックチェーンネットワーク4（以下、「ネットワーク」という）に自律分散的に接続される。なお、ネットワーク4には、図示する端末1、2の他にも、複数の端末が接続される。例えば、複数の利用者端末1、および、複数の承認端末2が接続されていてもよい。ネットワーク4に接続される端末は、後述する分散台帳11、ブロックチェーン制御部12およびトランザクション発行部13を備え、分散台帳11に記録されたデータおよびトランザクションを相互に

検証し、系を維持している。

[0020] 利用者端末 1 は、ブロックチェーンおよびスマートコントラクトを利用する利用者が使用する端末（ノード）である。利用者端末 1 は、分散台帳 1 1 と、ブロックチェーン制御部 1 2 と、トランザクション発行部 1 3 と、履歴検索部 1 4 とを備える。

[0021] 分散台帳 1 1 には、ブロックチェーン制御部 1 2 を介して、ネットワーク 4 に接続された全ての端末と緩やかに同期することによって、リアルタイムに近い形で最新状態のブロックチェーンが記憶されている。本実施形態の分散台帳 1 1 には、ブロックチェーンと、ブロックチェーンで管理されるデータ集合とが記憶されている。

[0022] ブロックチェーン制御部 1 2 は、ネットワーク 4 に接続された端末と自律分散的に協調してブロックチェーンの系を維持する。ブロックチェーン制御部 1 2 は、分散台帳 1 1 にアクセスし、分散台帳 1 1 のブロックチェーンおよびデータ集合を読み出し、または、更新する。

[0023] トランザクション発行部 1 3 は、トランザクションをネットワーク 4 に発行する。本実施形態では、トランザクション発行部 1 3 は、スマートコントラクトのステート（変数）の値を更新するトランザクションを発行する。

[0024] 履歴検索部 1 4 は、自身の分散台帳 1 1 からスマートコントラクトのステートの値が更新されたブロックの更新ブロック番号を取得し、更新ブロック番号から算出される検索ブロック番号を指定して、検索ブロック番号の時点のブロックにおけるスマートコントラクトのステートの値および更新ブロック番号を、分散台帳 1 1 から取得する。履歴検索部 1 4 は、ブロックチェーン制御部 1 2 を介して、分散台帳 1 1 にアクセスする。

[0025] 承認端末 2 は、例えばマイナーと呼ばれるトランザクションの検証者が使用する端末であって、ネットワーク 4 に送信されたトランザクションを収集し、正当性を確認後に、承認作業を通じてブロックを生成する。承認端末 2 は、分散台帳 1 1 と、ブロックチェーン制御部 1 2 と、トランザクション発行部 1 3 と、ブロック発行部 1 5 とを備える。承認端末 2 の分散台帳 1 1、

ブロックチェーン制御部 12 およびトランザクション発行部 13 は、利用者端末 1 の分散台帳 11、ブロックチェーン制御部 12 およびトランザクション発行部 13 と同様である。

[0026] ブロック発行部 15 は、ネットワーク 4 上に発行されたトランザクションを検証し、Proof of Workなどのブロック生成のためのコンセンサスアルゴリズム（合意アルゴリズム）に従い、ブロックの生成を試みる。

[0027] 図 2 は、承認端末 2 が備えるブロック発行部 15 の構成を示す構成図である。図示するブロック発行部 15 は、コンセンサス実行部 151 と、トランザクション検証部 152 と、ブロック生成部 153 とを備える。

[0028] コンセンサス実行部 151 は、ハッシュ演算などコンセンサス（合意）に必要な計算を実施する。コンセンサスアルゴリズムは、ビットコインで用いられているProof of Work以外にも、所持コイン量をリソースとしたProof of Stake、ビザンチン故障における合意アルゴリズムであるPBFTなど、その他のブロック生成のためのコンセンサスアルゴリズムを用いても良い。

[0029] トランザクション検証部 152 は、ネットワーク 4 よりトランザクションを受け取ると、受け取ったトランザクションの電子署名の正当性などのトランザクションの検証を行う。

[0030] ブロック生成部 153 は、所定の時間内にネットワーク 4 上で発行されたトランザクションをまとめて1つのブロックを生成する。すなわち、ブロック生成部 153 は、トランザクション検証部 152 による検証に成功した場合、当該トランザクションを含むブロックを生成し、ネットワーク 4 に接続される全ての端末の分散台帳 11 に生成したブロックを反映させる。

[0031] 本実施形態のブロック生成部 153 は、スマートコントラクトのステート（変数）の値を更新するトランザクションを含むブロックを生成するとともに前記ステートの値を更新し、前記ブロックと、前記ステートの値を更新した当該ブロックの更新ブロック番号とをブロックチェーンシステムの端末の分散台帳に反映させる。

[0032] 具体的には、ブロック生成部 153 は、スマートコントラクトのステート

の値を更新するトランザクションに基づいて、自身の分散台帳 1 1 のデータ集合の 1 つであるステートDBを更新し、更新後のステートDBのハッシュ値を、生成するブロックのブロックヘッダに設定する。すなわち、ブロック生成部 1 5 3 は、トランザクションに従って更新したステートの値と、更新を行った当該ブロックの更新ブロック番号とをステートDBに設定する。

[0033] 図 3 は、各端末の分散台帳 1 1 の構成を示す。本実施形態の分散台帳 1 1 は、複数のブロック 1 1 1 から構成されるブロックチェーンと、各ブロックに対応して管理されるデータ集合 1 1 2 とを備える。

[0034] ブロック 1 1 1 は、ブロックヘッダ 1 1 3、トランザクションリスト 1 1 4 などを有する。ブロックヘッダ 1 1 3 には、当該ブロックの時点の分散台帳 1 1 全体の要約が設定される。図示する例では、ブロックヘッダ 1 1 3 には、データ集合 1 1 2 のある時点のスナップショットとして、データ集合 1 1 2 の要約値（ステートDBのハッシュ値、トランザクション集合のハッシュ値など）が設定される。例えば、データ集合がマークルツリーなどのツリー構造で格納されている場合、要約値として、マークルツリーのルートハッシュが設定される。トランザクションリスト 1 1 4 は、当該ブロック 1 1 1 に含まれるトランザクションのリストである。

[0035] データ集合 1 1 2 は、その用途および目的は限定されない。図示する分散台帳 1 1 では、データ集合 1 1 2 として、ステートDBと、トランザクション集合DBとを備える。

[0036] ステートDBは、あるブロックの時点でのスマートコントラクトのステート（変数）の値または状態を管理するためのDBである。また、ステートDBには、スマートコントラクトのバイトコードが格納される。本実施形態では、トークンというデータ単位でステートDBに情報が記録されている。ここでトークンとはスマートコントラクトで表現されるデータ構造であり、少なくとも「トークンID」と「所有者のアドレス」といったパラメータを持ち、トークンの移転が所有者の権限によってブロックチェーン上で管理されるデータを示す。すなわち、本実施形態のステートDBには、トークン毎に、スマートコ

ントラクトのステート（例えば、所有者のアドレス等）の値が格納される。

[0037] また、本実施形態のステートDBは、承認端末2のブロック生成部153により、トークン毎に、ステートの値が更新されたブロックのブロック番号である更新ブロック番号が更新後のステートの値と対応付けて設定される。ステートDBは、Key-Value Store(KVS)として機能し、トークンを一意に指定する識別情報（例えば、トークンID）が入力されると、当該トークンのステートの値および更新ブロック番号を出力する。

[0038] なお、Ethereumでは、スマートコントラクトのバイトコードを、分散台帳11（ステートDB）に登録すると、当該スマートコントラクトを示す識別情報が付与される。識別情報に対して、トランザクションを送信することができるため、スマートコントラクトの識別情報はアドレスとも呼ばれる。ユーザのアドレスへの送金との違いは、スマートコントラクトのアドレス宛てにトランザクションを送信すると、当該スマートコントラクトが実行されることである。

[0039] トランザクション集合DBは、あるブロックの時点でのトランザクションの集合を示すDBである。トランザクションの集合は、あるブロックの時点での全てのトランザクションによって構成されるマークルツリーを意味する。

[0040] 次に、承認端末2が、ステートDBのステートの値を更新する際に、更新時点の更新ブロック番号を、当該ステートに付与する処理を説明する。

[0041] 図4は、更新ブロック番号をステートの値に付与する処理を説明するための模式図である。図示する例では、各端末の分散台帳11には、#26001番までのブロックが登録されているものとする。

[0042] 本実施形態の分散台帳11には、前述のとおり、ブロックと、ステートDBとが対応付けて保持されている。図示する例では、#25768のブロックのステートDB51と、#25770のブロックのステートDB52と、#26000のステートDB53と、#26001のステートDB54とを示している。

[0043] 図示する各ステートDBは、トークン毎に、トークンIDと、所有者アドレスと、更新ブロック番号とを有する。本実施形態では、ステートのキーとして

トークンIDを用いるが、ステートのキーはトークンIDに限定されない。また、トークンは、代替不可能なトークン（Non-Fungible Token）であっても、代替可能なトークン（Fungible Token）であってもよい。

[0044] 所有者アドレスは、ステート（変数）である。所有者アドレスは、対応するブロックの時点における、トークンの所有者のアドレスが設定される。更新ブロック番号には、トークンの所有者が更新（変更）された際のブロック番号が設定される。

[0045] 例えば、#25768のステートDB 5 1を見ると、トークンID：0005については、所有者は利用者Cで、所有者が利用者Cに更新されたトランザクションを含む更新ブロック番号は#25007であることがわかる。また、トークンID：0006については、所有者は利用者Dで、所有者が利用者Dに更新されたトランザクションを含む更新ブロック番号は#24991であることがわかる。

[0046] 次に、ブロック#25769では、当該ブロックに含まれるトランザクションにより、トークンID：0005および0006の所有者アドレスは更新されないものとする。この場合、図示しないステートDBのトークンID：0005および0006の更新ブロック番号には、直前のブロック#25768の更新ブロック番号に設定されたブロック番号が引き続き設定されている。また、トークンID：0005、0006の所有者アドレスには、直前のブロックの所有者アドレスに設定されたアドレスが引き続き設定されている。

[0047] そして、ブロック#25770に含まれるトランザクションにより、トークンID：0005および0006の所有者アドレスが更新される。この場合、承認端末2は、トークンID：0005および0006の所有者アドレスを更新するとともに、更新ブロック番号を更新する。具体的には、承認端末2は、当該ブロックのブロック番号（#25770）を、トークンID：0005および0006の更新ブロック番号に設定する。

[0048] そして、ブロック#25771から#25999では、各ブロックに含まれるトランザクションにより、トークンID：0005および0006の所有者アドレスは更新されないものとする。この場合、直前のブロックの更新ブロック番号に設定され

たブロック番号が、引き続き設定されている。すなわち、ブロック#25771から#25999のステートDBでは、トークンID：0005、0006については、#25770のステートDB 5 2と同じ所有者アドレスおよび更新ブロック番号が引き続き設定されている。

[0049] そして、ブロック#26000に含まれるトランザクションにより、トークンID：0005の所有者アドレスが更新される。この場合、承認端末2は、トークンID：0005の所有者アドレスを更新するとともに、更新ブロック番号を更新する。具体的には、承認端末2は、当該ブロックのブロック番号（#26000）を、トークンID：0005更新ブロック番号に設定する。なお、トークンID：0006については、承認端末2は、直前のブロックと同じ所有者アドレスおよび更新ブロック番号を設定する。

[0050] このように、本実施形態では、キー（トークンID）に対するステート（所有者アドレス）の値とともに、更新ブロック番号を設定する。これにより、本実施形態では、利用者端末1は、最新のステートDB 5 4を参照すると、最後に変更があった更新ブロック番号を取得することができる。例えば、トークンID：0006の場合は#25770を取得することができる。

[0051] そして、利用者端末1は、更新ブロック番号から算出される検索ブロック番号を指定して、検索ブロック番号で指定された所有者アドレスおよび更新ブロック番号を取得する。例えば、検索ブロック番号は、更新ブロック番号から1減算したブロック番号とする。例えば、トークンID：0006の場合は更新ブロック番号#25770から1減算した検索ブロック番号#25769を指定して当該ブロック番号に設定された所有者アドレス（利用者D）および更新ブロック番号（#24991）を取得する。このように、本実施形態では、ステートの値に変更があったブロックの付近のブロックのみを辿ることで、探索コストを大幅に低減し、容易にステートの値の変更履歴を取得することができる。

[0052] 図5は、本実施形態のブロック生成および履歴検索を示すシーケンス図である。

[0053] 図示する処理では、利用者Aが利用者Bにトークンを移動（譲渡）し、利

用者Bが利用者Aから受け取ったトークンの履歴を探索する処理を示す。

[0054] 利用者Aの利用者端末1Aは、所定のトークンを利用者Aから利用者Bに移動するためのトランザクションを生成し、を発行する(S11)。具体的には、利用者端末1Aはトランザクションをネットワーク4上にブロードキャストする。これにより、トランザクションは、ネットワーク4に接続された全ての端末に伝搬される。

[0055] 図6は、S11のトランザクションの一例を示す図である。図示するトランザクションは、宛先と、支払額と、データと、電子署名とを有する。宛先には、スマートコントラクトのアドレスが設定される。支払額には、スマートコントラクトを実行するために支払われる金額(手数料)が設定される。

[0056] データには、スマートコントラクト内の「指定されたアドレスへ所定のトークンの所有権を移動する」機能を提供する関数を実行することを指定するデータが設定される。なお、引数としてトークンのIDと利用者Bのアドレスを指定する。電子署名には、トランザクションの発行者である利用者Aの秘密鍵で当該トランザクションが署名された署名値が設定される。

[0057] そして、承認端末2(ブロック発行部15)は、S11で送信されたトランザクションを検証(マイニング)する(S12)。そして、承認端末2は、当該トランザクションを、所定の時間内に発生した他のトランザクションとまとめて1つのブロックを生成する。当該ブロックは、ナンスのマイニングを経て自身の分散台帳11のブロックチェーンに追加される(S13)。承認端末2がブロックの生成に成功することにより、S11で送信されたトランザクションが確定(承認)される。

[0058] ここで、承認端末2は、S11のトランザクションに基づいて、自身の分散台帳11のデータ集合の各DBを更新し、更新後の各DBのハッシュ値を、生成するブロックのブロックヘッダに設定する。

[0059] また、承認端末2は、データ集合のステートDBを更新する際に、S11のトランザクションに従って、所有権を移動したトークンの所有者アドレスを、利用者Aのアドレスから利用者Bのアドレスに更新・変更する。また、本

実施形態では、承認端末2は、所有者アドレスを更新した当該ブロックのブロック番号を、ステートDBに記憶する。例えば、図4のステートDB54に示すように、所有権を移動するトークンのトークンIDが0005で、生成するブロックが#26000の場合、承認端末2は、所有者アドレスに利用者Bのアドレスを設定し、更新ブロック番号に当該ブロックの番号#26000をステートDBに設定する。

[0060] そして、承認端末2は、更新後のステートDBのハッシュ値を、生成するブロックのブロックヘッダに設定する。なお、S13は、ネットワークに接続された全ての端末のうち、最も早くブロックの生成に成功した端末によって行われる処理である。

[0061] そして、端末間のゆるやかな同期により、S11で送信されたトランザクションを含むブロックが、ネットワーク4に接続された全ての端末の分散台帳11に反映される（S14、S15）。すなわち、全ての端末のブロックチェーン制御部12は、自身が保持する分散台帳11に、S11のトランザクションを含むブロックを追加する。また、全ての端末のブロックチェーン制御部12は、承認端末2と同様に、ブロックに含まれるトランザクションに基づいて、自身の分散台帳11のデータ集合のステートDBを更新する。

[0062] 次に、トークンの所有権となった利用者Bが、利用者Aから譲渡されたトークンの過去の履歴を探索する場合、S16以降の処理を行う。具体的には、利用者端末1Bは、最新のブロックにおける、前記トークンの所有者アドレス（ステートの値）を自身の分散台帳に問合せ（S16）、分散台帳から最新のブロックの所有者アドレスと、更新ブロック番号とを取得する（S17）。

[0063] 例えば、最新ブロックが図4に示す#26001で、問い合わせ対象のトークンIDが0005の場合、利用者端末1Bは、自身の分散台帳のステートDB54を参照し、所有者として利用者Bのアドレスと、更新ブロック番号として#26000とを取得する。これにより、利用者Bは、現在のトークンの所有者が自分であり、また、所有者の更新が#26000のブロックで行われたことを確認すること

ができる。

[0064] そして、利用者Bは、トークンの過去の履歴を検索したい場合、S 1 8およびS 1 9の処理を繰り返し行う。すなわち、利用者端末1 Bは、S 1 7で取得した更新ブロック番号に基づいて検索ブロック番号を算出する。ここでは、更新ブロック番号から「1」減算したブロック番号を検索ブロック番号とする。そして、利用者端末1 Bは、検索ブロック番号を指定し、検索ブロック番号における、トークンの所有者アドレスを自身の分散台帳に問合せ（S 1 8）、分散台帳から指定したブロックにおける所有者アドレスと、更新ブロック番号とを取得する（S 1 9）。

[0065] 例えば、図4のステートDBにおいて、S 1 7取得した更新ブロック番号が#26000でトークンIDが0005の場合、利用者端末1 Bは、#26000から「1」減算したブロック番号#25999を指定して、分散台帳に問い合わせる。#25999のステートDBは、図4に示していないが、トークンID：0005に対する更新は#25771から#25999までは行われていないため、トークンID：0005に関する#25999のステートは、#25770のステートDB 5 2と同じである。したがって、利用者端末1 Bは、#25999の分散台帳のステートDBを参照し、所有者アドレスとして利用者Aのアドレス、および、更新ブロック番号として#25770を取得する。これにより、利用者Bは、トークンID：0005の前の所有者が利用者Aであり、また、利用者Aへの所有者の変更が#25770のブロックで行われたことを確認することができる。

[0066] そして、利用者端末1 Bは、それ以前の過去の履歴を検索したい場合は、S 1 8およびS 1 9の処理を繰り返し行う。これにより、利用者Bは、トークンの過去の履歴を効率よく辿ることができる。

[0067] 以上説明した本実施形態では、利用者端末1と、承認端末2とを備えるブロックチェーンシステムであって、利用者端末1は、スマートコントラクトのステート（変数）の値を更新するトランザクションを発行するトランザクション発行部13を備え、承認端末2は、前記トランザクションを含むブロックを生成するとともに前記ステートの値を更新し、前記ブロックと、前記

ステートの値を更新した当該ブロックの更新ブロック番号とをブロックチェーンシステムの端末の分散台帳 11 に反映させるブロック生成部 153 を備える。

[0068] このように、本実施形態では、各端末の分散台帳 11 のステートDBには、スマートコントラクトのステートの値が更新された時点で、更新のあったブロックの更新ブロック番号を、更新されたステートの値に付与する。これにより、利用者は、更新ブロック番号を辿ることで、過去の全てのブロックおよびトランザクションを参照することなく、分散台帳（ブロックチェーン）上で、データの履歴を容易に追跡することができる。すなわち、本実施形態では、スマートコントラクトのステートの値の過去の履歴および変遷を容易に取得することができる。

[0069] また、本実施形態では、スマートコントラクトの利用者に対して、トレーサビリティを向上することができる。従来のステートDBでは、過去のどのブロックでステートの値が更新または変更されたかの情報は保持されていなく、ステートの値がどのブロックの時点で遷移したのかを利用者は知ることは容易ではない。従来では、変更のあったブロック番号を知るためには、全てのブロックまたはトランザクションを探索する必要があり、利用者にとって大きな負荷となっていた。これに対して、本実施形態では、ステートDBにステートの値の変化点として、ブロック生成時点（採掘時点）のブロック番号を追跡したいステートの値に付加することで、当該ステートのトレーサビリティを向上することができる。

[0070] なお、上記説明した利用者端末 1 および承認端末 2 は、例えば、CPU（Central Processing Unit、プロセッサ）と、メモリと、ストレージ（HDD：Hard Disk Drive、SSD：Solid State Drive）と、通信装置と、入力装置と、出力装置とを備える汎用的なコンピュータシステムを用いることができる。このコンピュータシステムにおいて、CPUがメモリ上にロードされた所定のプログラムを実行することにより、各装置の各機能が実現される。例えば、利用者端末 1 および承認端末 2 の各機能は、利用者端末 1 用のプログラムの場合は

利用者端末 1 のCPUが、承認端末 2 用のプログラムの場合は承認端末 2 のCPUが、それぞれ実行することにより実現される。

[0071] また、利用者端末 1 用のプログラムおよび承認端末 2 用のプログラムは、HDD、SSD、USBメモリ、CD-ROM、DVD-ROM、MOなどのコンピュータ読取り可能な記録媒体に記憶することも、ネットワークを介して配信することもできる。

[0072] また、本発明は上記実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

[0073] 例えば、本実施形態では、承認端末 2 は、更新ブロック番号として、ステートの値が更新されたブロックのブロック番号を更新ブロック番号としてステートDBに設定した。しかしながら、更新ブロック番号の代わりに、検索用ブロック番号をステートDBに設定することとしてもよい。すなわち、承認端末 2 は、更新ブロック番号の代わりに、更新ブロック番号から「1」減算した検索ブロック番号をステートDBに設定することとしてもよい。この場合、利用者端末 1 は、ステートの過去の履歴を取得する際（図 5 の S 18）に、更新ブロック番号から検索ブロック番号を算出することなく、分散台帳から取得した検索ブロック番号をそのまま用いて、過去の履歴を辿ることができる。

[0074] また、本実施形態のステートDBは、図 4 に示すように 1 つのステート（所有者アドレス）を保持し、当該ステートに対応する 1 つの更新ブロック番号を保持することとした。しかしながら、ステートDBは複数のステートを保持することとしてもよい。この場合、複数のステートのそれぞれの追跡を行う場合、ステートDBは、各ステートごとに更新ブロック番号を備えるものとする。

符号の説明

- [0075] 1 : 利用者端末
 2 : 承認端末
 1 1 : 分散台帳
 1 2 : ブロックチェーン制御部

- 1 3 : トランザクション発行部
- 1 4 : 履歴検索部
- 1 5 : ブロック発行部
- 1 5 1 : コンセンサス実行部
- 1 5 2 : トランザクション検証部
- 1 5 3 : ブロック生成部
- 4 : ブロックチェーンネットワーク

請求の範囲

- [請求項1] 利用者端末と、承認端末とを備えるブロックチェーンシステムであって、
- 前記利用者端末は、
- スマートコントラクトの変数の値を更新するトランザクションを発行するトランザクション発行部を備え、
- 前記承認端末は、
- 前記トランザクションを含むブロックを生成するとともに前記変数の値を更新し、前記ブロックと、前記変数の値を更新した当該ブロックの更新ブロック番号とを前記ブロックチェーンシステムの端末の分散台帳に反映させるブロック生成部を備えること
- を特徴とするブロックチェーンシステム。
- [請求項2] 請求項1記載のブロックチェーンシステムであって、
- 前記分散台帳は、前記変数の値をトークン毎に格納するステートデータベースを備え、
- 前記ブロック生成部は、前記トークン毎に前記更新ブロック番号を前記ステートデータベースに設定すること
- を特徴とするブロックチェーンシステム。
- [請求項3] 請求項1または2記載のブロックチェーンシステムであって、
- 前記利用者端末は、
- 自身の前記分散台帳から前記更新ブロック番号を取得し、前記更新ブロック番号から算出される検索ブロック番号を指定して、前記検索ブロック番号の時点のブロックにおける前記変数の値および更新ブロック番号を、自身の前記分散台帳から取得する履歴検索部を備えること
- を特徴とするブロックチェーンシステム。
- [請求項4] 請求項1または2記載のブロックチェーンシステムであって、
- 前記ブロック生成部は、前記更新ブロック番号の代わりに、前記更

新ブロック番号から算出される検索ブロック番号を、前記ブロックチェーンシステムの端末の前記分散台帳に反映させること

を特徴とするブロックチェーンシステム。

[請求項5] ブロックチェーンシステムにおいてトランザクションを承認する承認端末であって、

 スマートコントラクトの変数の値を更新するトランザクションを受信する受信部と、

 前記トランザクションを含むブロックを生成するとともに前記変数の値を更新し、前記ブロックと、前記変数の値を更新した当該ブロックの更新ブロック番号とを前記ブロックチェーンシステムの端末の分散台帳に反映させるブロック生成部と、を備えること

を特徴とする承認端末。

[請求項6] ブロックチェーンシステムにおける利用者端末であって、

 ブロックチェーンの分散台帳と、

 スマートコントラクトの変数の値を更新するトランザクションを発行するトランザクション発行部と、

 前記分散台帳から前記変数の値が更新されたブロックの更新ブロック番号を取得し、前記更新ブロック番号から算出される検索ブロック番号を指定して、前記検索ブロック番号の時点のブロックにおける前記スマートコントラクトの変数の値および更新ブロック番号を、前記分散台帳から取得する履歴検索部と、を備えること

を特徴とする利用者端末。

[請求項7] ブロックチェーンの履歴を管理する履歴管理方法であって、利用者端末は、

 スマートコントラクトの変数の値を更新するトランザクションを発行するトランザクション発行ステップを行い、

承認端末は、

 前記トランザクションを含むブロックを生成し、前記変数の値を

更新する生成ステップと、

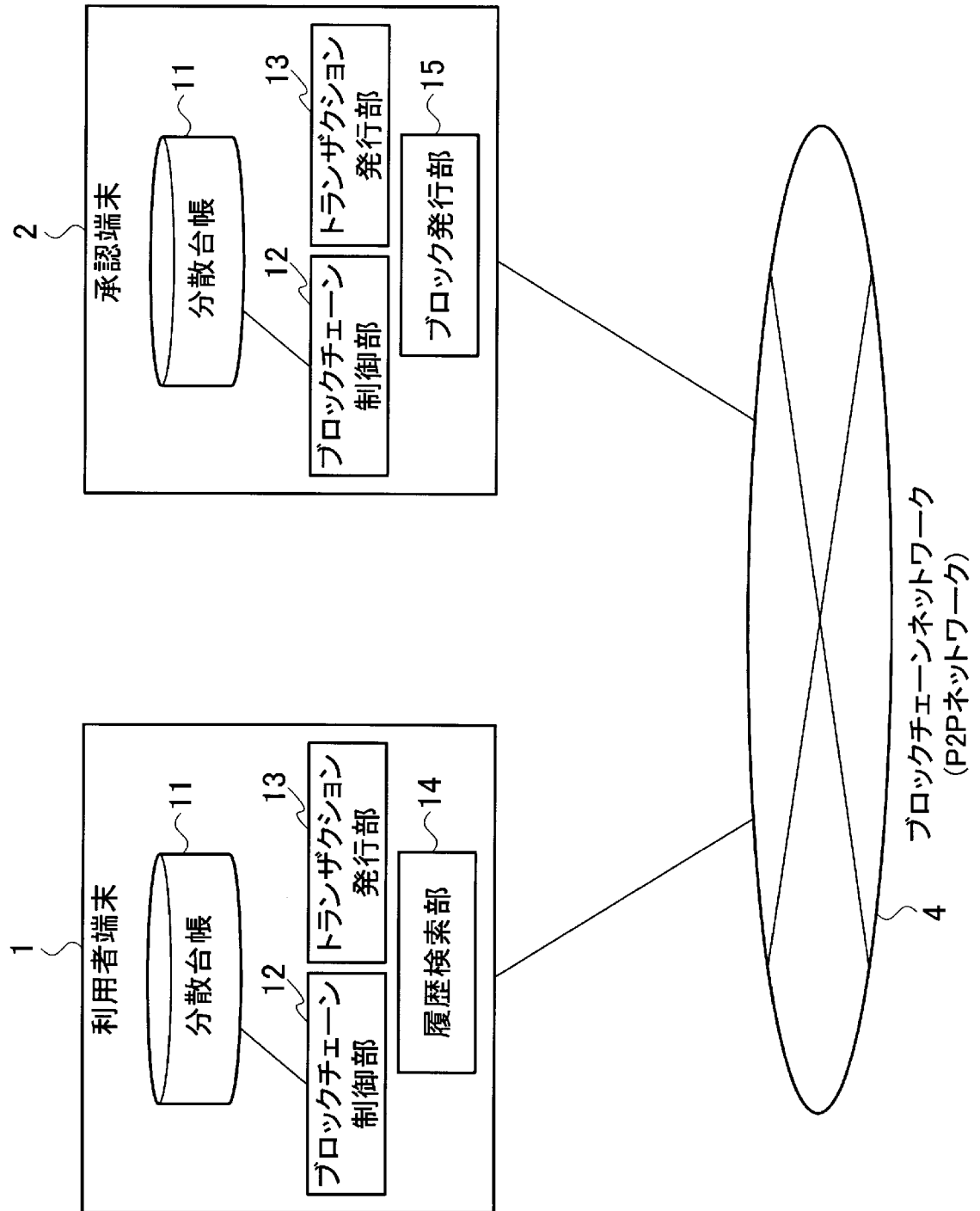
前記ブロックと、前記変数の値を更新した当該ブロックの更新ブロック番号とを、ブロックチェーンネットワークに接続された端末の分散台帳に反映させる同期ステップとを行うこと

を特徴とする履歴管理方法。

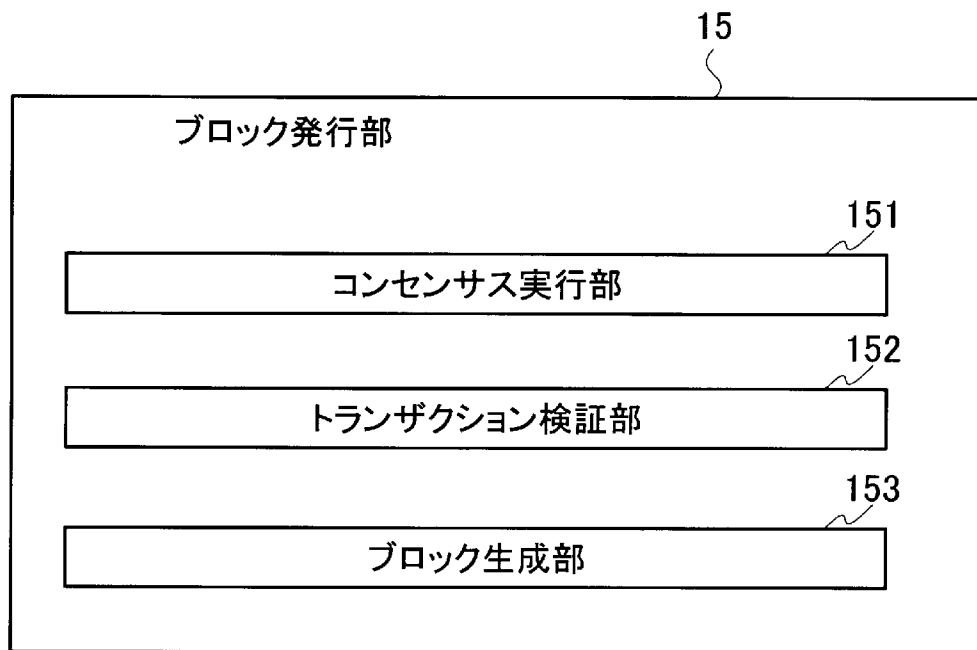
[請求項8]

請求項5に記載の承認端末として、コンピュータを機能させることを特徴とする履歴管理プログラム。

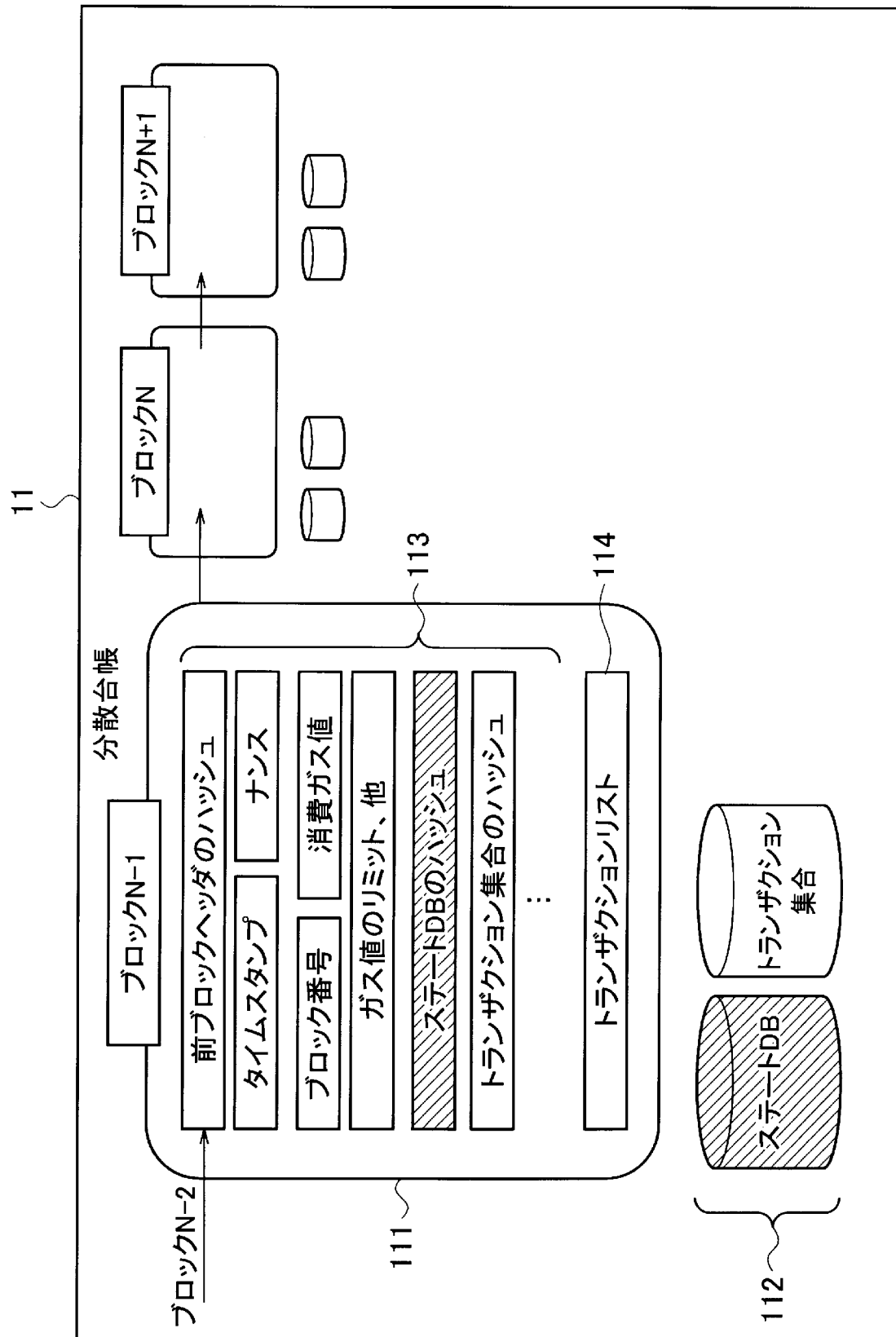
[図1]



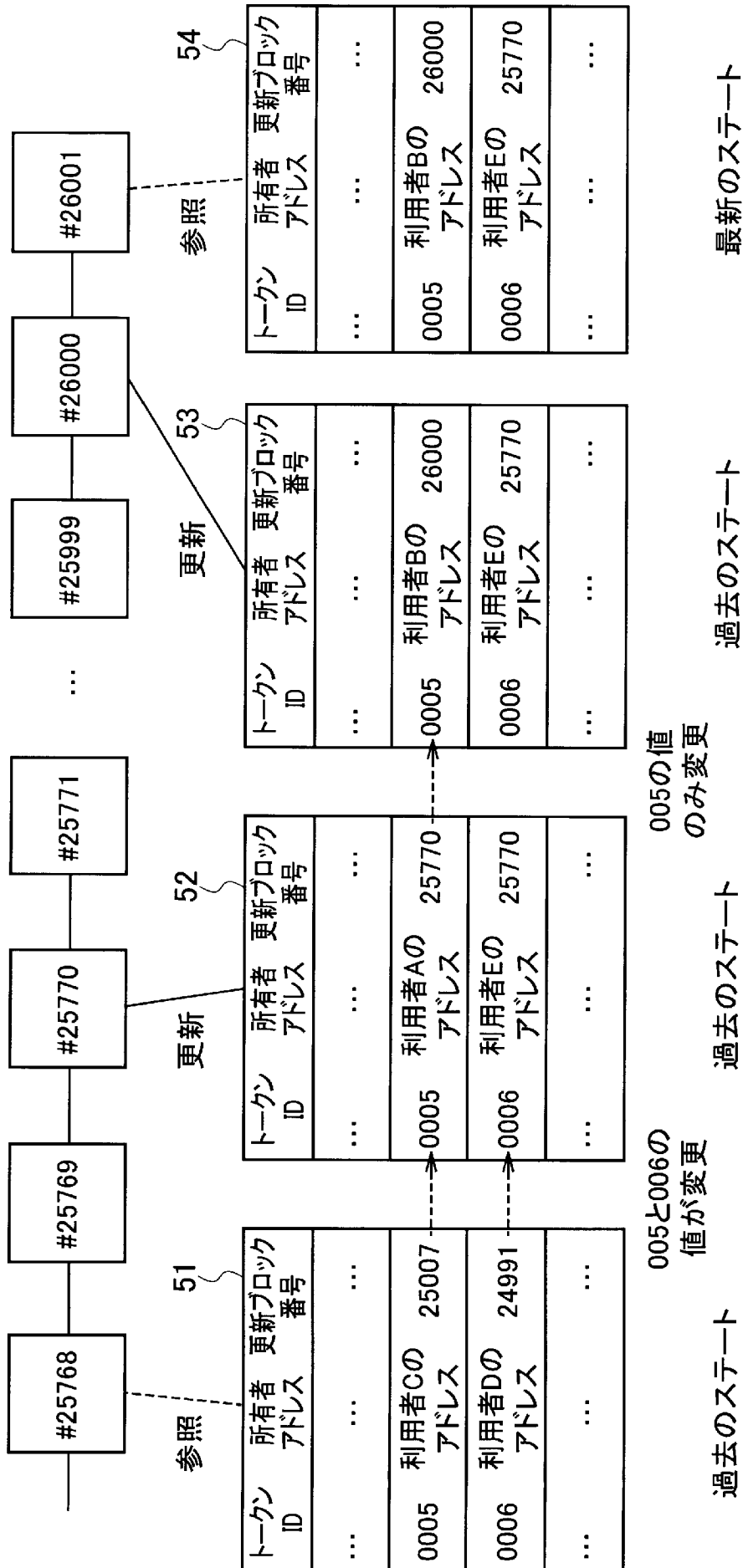
[図2]



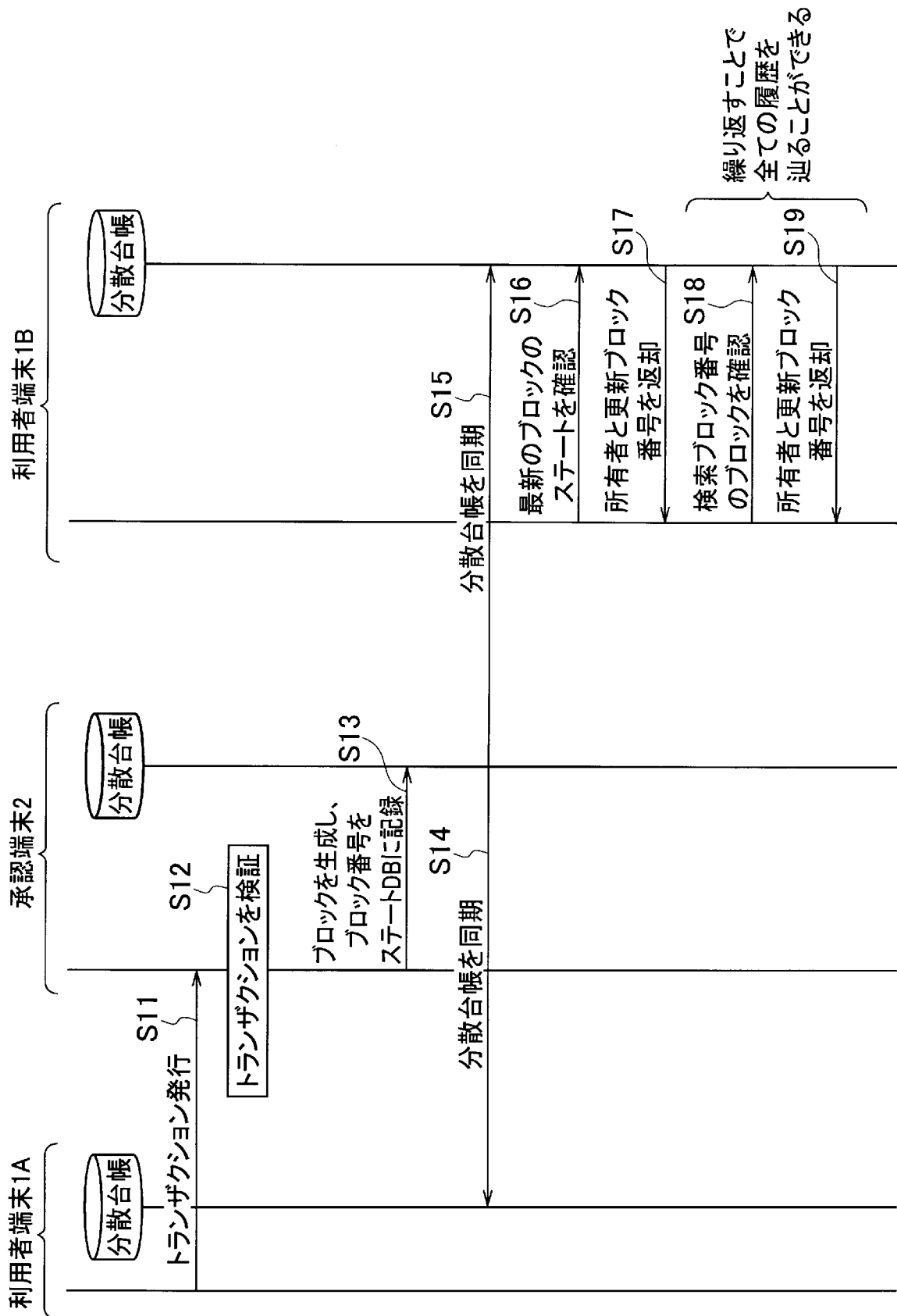
[図3]



[図4]



[図5]



[図6]

フィールド	説明
宛先	コントラクトのアドレス
支払額	コントラクトを実行するために支払われる金額(手数料)
データ	コントラクト内の「指定されたアドレスへのトークンの所有権を移動する」機能を提供する関数を実行することを指定するデータ。 引数としてトークンIDおよび利用者Bのアドレスを指定する。
電子署名	利用者Aの秘密鍵で署名された署名値

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/042658

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. G06F 16/17 (2019.01) i, G06F 16/182 (2019.01) i
 FI: G06F16/182, G06F16/17 200

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. G06F16/17, G06F16/182

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

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2020

Registered utility model specifications of Japan 1996-2020

Published registered utility model applications of Japan 1994-2020

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	佐藤聖, なるほど IoT 新技術ブロックチェーン, Interface, 01 August 2018, vol. 44, no. 8, pp. 29-39, p.30, right column to p. 32, right column, p. 36, left column, fig. 6(a), fig. 8, non-official translation (SATO, Sei, New IoT Technology, Blockchains, of course)	1, 3-8



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
24.01.2020

Date of mailing of the international search report
04.02.2020

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

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	フォンヤオカイ外, 次世代暗号通貨プラットフォーム Ethereum の実験的評価, CSS2015 コンピュータセキュリティシンポジウム 2015 論文集合同開催 マルウェア対策研究人材育成ワークショップ 2015 プライバシーワークショップ 2015 情報処理学会シンポジウムシリーズ, vol. 2015, no. 3 [CD-ROM], 14 October 2015, pp. 1151-1158, entire text, all drawings, FENG, Yaokai et al., Next-Generation Cryptocurrency Platform Ethereum and Its Evaluation, non-official translation (CSS 2015 Computer Security Symposium, 2015, 2015 proceedings and anti-malware research human resources development workshop, 2015 privacy workshop, 2015 IPSJ Symposium Series)	1-8
A	JP 6362805 B1 (BITFLYER INC.) 25 July 2018, entire text, all drawings	1-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/JP2019/042658

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
JP 6362805 B1	25.07.2018	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 16/17(2019.01)i; G06F 16/182(2019.01)i FI: G06F16/182; G06F16/17 200		
B. 調査を行った分野 調査を行った最小限資料（国際特許分類（IPC）） G06F16/17; G06F16/182 最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2020年 日本国実用新案登録公報 1996-2020年 日本国登録実用新案公報 1994-2020年 国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X	佐藤 聖, なるほどIoT新技術ブロックチェーン, Interface, 2018.08.01, 第44巻 第8号, pp. 29-39 p. 30 右欄~p. 32 右欄, p. 36 左欄, 図6(a), 図8	1, 3-8
A	フォン ヤオカイ 外, 次世代暗号通貨プラットフォームEthereumの実験的評価, CSS2015 コンピュータセキュリティシンポジウム2015 論文集 合同開催 マルウェア対策研究人材育成ワークショップ2015 プライバシーワークショップ2015 情報処理学会シンポジウムシリーズ Vol. 2015 No. 3 [CD-ROM], 2015.10.14, 第2015巻 第3号, pp. 1151-1158 全文全図	1-8
A	JP 6362805 B1 (株式会社bitFlyer) 25.07.2018 (2018-07-25) 全文全図	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 24.01.2020		国際調査報告の発送日 04.02.2020
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 原 秀人 5N 9644 電話番号 03-3581-1101 内線 3586

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2019/042658

引用文献	公表日	パテントファミリー文献	公表日
JP 6362805 B1	25.07.2018	(ファミリーなし)	