

(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
2019年6月13日(13.06.2019)



(10) 国際公開番号

WO 2019/111338 A1

(51) 国際特許分類:
G06Q 20/06 (2012.01)

(21) 国際出願番号: PCT/JP2017/043716

(22) 国際出願日: 2017年12月5日(05.12.2017)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: G V E 株式会社 (**GVE LTD.**) [JP/JP]; 〒1030026 東京都中央区日本橋兜町 1 3 番 1 号 Tokyo (JP).

(72) 発明者: 日下部 佑(**KUSAKABE Yu**); 〒1030026 東京都中央区日本橋兜町 1 3 番 1 号 G V E 株式会社内 Tokyo (JP). 房 広治(**FUSA Koji**); 〒1030026 東京都中央区日本橋兜町 1 3 番 1 号 G V E 株式会社内 Tokyo (JP). 高松 圭太(**TAKAMATSU Keita**); 〒1030026 東京都中央区日本橋兜町 1 3 番 1 号 G V E 株式会社内 Tokyo (JP).

(74) 代理人: 蟹 田 昌 之 (**KANIDA Masayuki**); 〒1006208 東京都千代田区丸の内 1 - 1 1 - 1 パシフィックセンチュリープレイス丸の内 8 階 Tokyo (JP).

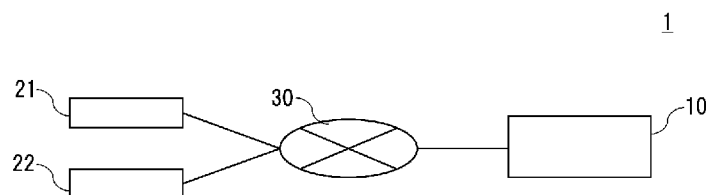
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, 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,

(54) **Title:** MANAGEMENT DEVICE, VIRTUAL CURRENCY SYSTEM, AND SYSTEM

(54) 発明の名称: 管理装置、仮想通貨システム、及びシステム

[図1]



(57) **Abstract:** [Problem] To provide a management device and a virtual currency system capable of smoothly managing an entire system by detecting fraud relating to a virtual currency without spending an enormous calculation amount. [Solution] Provided is a management device connected to a plurality of user devices via a network, the management device having: an issuance information storage area in which a virtual currency ID of an issued virtual currency is stored; an account information storage area in which account information is associated with one or a plurality of virtual currency IDs and stored; and a history information storage area in which history information of the virtual currency is associated with the virtual currency ID and stored.

(57) 要約: 【課題】膨大な計算量を費やすことなく仮想通貨に関する不正を検知することにより、システム全体を円滑に運営可能な管理装置及び仮想通貨システムを提供する。【解決手段】複数のユーザ装置にネットワークを介して接続される管理装置であって、発行済仮想通貨の仮想通貨IDを記憶する発行情報記憶領域と、口座情報を1つまたは複数の仮想通貨IDに対応付けて記憶する口座情報記憶領域と、仮想通貨の履歴情報を仮想通貨IDに対応付けて記憶する履歴情報記憶領域と、を有する管理装置。

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)）

明 細 書

発明の名称：管理装置、仮想通貨システム、及びシステム

技術分野

[0001] 本発明は管理装置、仮想通貨システム、及びシステムに関する。

背景技術

[0002] 複数のユーザ装置間で過去から現在にわたるすべての取引履歴データを共有し、これら共有される取引履歴データの改ざんが困難となるよう、既に共有されている取引履歴データに付加される新たな取引履歴データに対して、マイニング（採掘）と呼ばれる処理により生成された特殊なハッシュ値を付け加える仮想通貨システムが知られている（非特許文献1参照）。

先行技術文献

非特許文献

[0003] 非特許文献1：フリー百科事典「ウィキペディア（Wikipedia）」、ブロックチェーン、[平成29年12月3日検索]、インターネット<URL：<https://ja.wikipedia.org/wiki/ブロックチェーン>>

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、上記従来の仮想通貨システムでは、マイニング（採掘）による特殊なハッシュ値の計算量が過大となり、システム全体を円滑に運営できなくなる虞がある。

課題を解決するための手段

[0005] 上記の課題は、例えば、次の手段により解決することができる。

[0006] 複数のユーザ装置にネットワークを介して接続される管理装置であって、発行済仮想通貨の仮想通貨IDを記憶する発行情報記憶領域と、口座情報を1つまたは複数の仮想通貨IDに対応付けて記憶する口座情報記憶領域と、仮想通貨の履歴情報を仮想通貨IDに対応付けて記憶する履歴情報記憶領域

と、を有する管理装置。

[0007] 複数のユーザ装置にネットワークを介して接続された管理装置であって、発行済仮想通貨の仮想通貨IDを記憶する発行情報記憶領域と、資産残高を記憶する資産情報記憶領域と、を備え、前記ユーザ装置から口座情報を指定する仮想通貨発行要求を受信した場合、仮想通貨の対価の受け取りを条件に含む発行条件の成否を判断し、前記発行条件が成立する場合に、前記発行情報記憶領域に新たな仮想通貨IDを記憶し、一の前記ユーザ装置から口座情報を指定する売り注文を受信した場合、対象価格が所定の買い介入設定価格以下であるとの条件を含む買い介入条件の成否を判断し、前記買い介入条件が成立する場合に、前記資産情報記憶領域に記憶されている資産残高から前記買い介入が成立した対価を減算する管理装置。

発明の効果

[0008] 本発明の一実施形態によれば、管理装置が、仮想通貨IDを用いて、膨大な計算量を費やすことなく仮想通貨に関する不正を検知することができる。したがって、システム全体を円滑に運営可能な管理装置及び仮想通貨システムを提供することができる。

図面の簡単な説明

[0009] [図1]実施形態1に係る仮想通貨システムの構成例を示す模式図である。

[図2]実施形態1に係る管理装置の構成例を示す模式図である。

[図3A]発行情報記憶領域の一例を示す模式図である。

[図3B]口座情報記憶領域の一例を示す模式図である。

[図3C]履歴情報記憶領域の一例を示す模式図である。

[図3D]資産情報記憶領域の一例を示す模式図である。

[図3E]履歴情報記憶領域の一例を示す模式図である。

[図4]実施形態1に係る管理装置の動作例（仮想通貨の発行）を説明するシーケンス図である。

[図5]実施形態1に係る管理装置の動作例（仮想通貨の売買仲介）を説明するシーケンス図である。

[図6]実施形態１に係る管理装置の動作例（仮想通貨の買い介入）を説明するシーケンス図である。

[図7]実施形態１に係る管理装置の動作例（仮想通貨の売り介入）を説明するシーケンス図である。

[図8]実施形態２に係る仮想通貨システムの動作例を説明するシーケンスである。

[図9]実施形態３に係る仮想通貨システムの動作例を説明するシーケンスである。

発明を実施するための形態

[0010] [実施形態１に係る仮想通貨システム１]

図１は実施形態１に係る仮想通貨システムの構成例を示す模式図である。図１に示すように、実施形態１に係る仮想通貨システム１は、管理装置１０と、管理装置１０にネットワーク３０介して接続される複数のユーザ装置２１、２２と、を備えている。以下、詳細に説明する。

[0011] (ユーザ装置２１、２２)

ユーザ装置２１、２２はユーザが管理する装置である。ユーザには個人や法人のほか、世界各国の中央銀行、民間の銀行、及び取引所などの機関が含まれる。ユーザ装置２１、２２にはデスクトップコンピュータやラップトップコンピュータのほか、スマートフォンなどを用いることができる。ユーザ装置２１、２２と管理装置１０を接続するネットワーク３０は例えばインターネットなどである。

[0012] (管理装置１０)

管理装置１０は仮想通貨を管理する装置である。管理には、例えば、発行の管理、売買の管理、価値の管理（仮想通貨の価値を維持することなど）、及び履歴の管理が含まれる。本実施形態では、管理装置１０が仮想通貨ＩＤを用いて一元的に仮想通貨の管理を行うため、システム全体の計算量を抑制しつつ、仮想通貨に関する不正を容易に検知することができる。

[0013] 管理装置１０は仮想通貨の管理者により管理される。管理者とは、例えば

、世界各国の中央銀行、民間の銀行、取引所などの機関である。管理者に個人は含まれない。管理者が管理装置 10 の管理に責任を有している限り、管理者自身が管理装置 10 を直接に操作しているか、管理者から委託などされた者が管理者の指示などに従って管理装置 10 を操作しているかなどは問わない。

[0014] 管理装置 10 は、1 つの装置であってもよいし、1 つの装置が動作しているとみなすことができるよう共同して動作する複数の装置であってもよい。また、管理装置 10 は、ネットワーク 30 上に複数配置することもできる。この場合、複数の管理装置 10 の各々は、1 つの装置であってもよいし、1 つの装置が動作しているように見えるよう共同して動作する複数の装置であってもよい。

[0015] 図 2 は実施形態 1 に係る管理装置の構成例を示す模式図である。図 2 に示すように、管理装置 10 は演算装置 12 と記憶装置 14 を有している。演算装置 12 は例えば CPU であり、記憶装置 14 は例えば RAM やハードディスクなどの情報の読み込みと書き込みが可能な装置である。記憶装置 14 は管理装置 10 に内蔵されていてもよいし（図 2 参照）、管理装置 10 に外付けされていてもよい。また、記憶装置 14 は、ネットワーク 30 を介して管理装置 10 の演算装置 12 にアクセスされる装置であってもよい。演算装置 12 や記憶装置 14 それぞれは、1 つの装置であってもよいし、1 つの装置が動作しているとみなすことができるよう共同して動作する複数の装置であってもよい。

[0016] 図 3 A は発行情報記憶領域の一例を示す模式図であり、図 3 B は口座情報記憶領域の一例を示す模式図であり、図 3 C は履歴情報記憶領域の一例を示す模式図である。管理装置 10 の記憶装置 14 には、図 3 A から図 3 C に示すような、発行済仮想通貨の仮想通貨 ID を記憶する発行情報記憶領域 141 と、口座情報を 1 つまたは複数の仮想通貨 ID に対応付けて記憶する口座情報記憶領域 142 と、仮想通貨の履歴情報を仮想通貨 ID に対応付けて記憶する履歴情報記憶領域 143 と、が設けられている。

[0017] (発行情報記憶領域 1 4 1)

発行情報記憶領域 1 4 1 には発行済仮想通貨の仮想通貨 I D が記憶されている。仮想通貨 I D とは個々の仮想通貨に固有のデータであり、1 つの仮想通貨 I D を特定することにより 1 つの仮想通貨を一意に特定することができる。仮想通貨 I D は、すべての発行済の仮想通貨に対して割り当てられる。

[0018] 発行情報記憶領域 1 4 1 においては、仮想通貨 I D に対応付けて、発行情報を記憶することができる。発行情報には、例えば、個々の仮想通貨の発行価格や、仮想通貨の対価を受け取り済みであるかどうかの情報や、仮想通貨の発行日時などが含まれる。

[0019] 個々の仮想通貨の発行価格は、発行数が増えるごとに増額されていることが好ましい。例えば 3 つの仮想通貨が発行されているとすると、1 番目に発行された仮想通貨の発行価格が 1 0 0 円であり、2 番目に発行された仮想通貨の発行価格が 2 0 0 円であり、3 番目に発行された仮想通貨の発行価格が 3 0 0 円である場合などのようにである。このようにすれば、先に仮想通貨の発行を受けるほどより安価に仮想通貨を手に入れることができるため、仮想通貨の普及を促進することができる。

[0020] (口座情報記憶領域 1 4 2)

口座情報記憶領域 1 4 2 には、管理者やユーザの口座情報が 1 つまたは複数の仮想通貨 I D に対応付けて記憶される。口座情報とは、仮想通貨の発行先や送金元や送金先を特定する情報である。口座情報には、例えば、仮想通貨を預け入れる口座番号や預入アドレスなどのほか、氏名や名称などの仮想通貨の所有者情報などが含まれる。なお、口座情報に所有者情報を含め且つそれを公開する場合は、仮想通貨の所有者が明らかとなるため、マネーロンダリングなどを効果的に防止することができる。他方、口座情報に所有者情報を含めない場合あるいは含まれているが公開しない場合は、仮想通貨の発行や送金などはできるが、所有者は明らかにならないため、仮想通貨に関して匿名性を保つことができる。

[0021] (履歴情報記憶領域 1 4 3)

履歴情報記憶領域 143 には、仮想通貨の履歴情報が仮想通貨 ID に対応付けて記憶される。管理装置 10 は、仮想通貨 ID を用いて履歴情報記憶領域 143 に記憶されている履歴情報間の整合性を検証することにより、個々の仮想通貨に関する不正を容易に検知することができる。また、履歴情報記憶領域 143 に記憶されている情報を、発行情報記憶領域 141 に記憶されている情報や口座情報記憶領域 142 に記憶されている情報を突き合わせて矛盾がないかどうかを判断することにより、履歴情報記憶領域 143 に記憶されている情報が改ざんされていないかどうかを判断することができる。この判断にあたり、膨大な計算量を要する特殊なハッシュ値を計算する必要はない。

[0022] 仮想通貨の履歴情報には例えば履歴の種別と履歴に係する口座情報と履歴の日時が含まれる。履歴の種別には、例えば、仮想通貨が発行されたことを示す情報、仮想通貨の売買取引（例：ユーザの口座番号の間で仮想通貨を送金すること）が成立したことを示す情報、仮想通貨に対して買い介入（例：ユーザの口座番号から管理装置の口座番号へ仮想通貨を送金すること）が行われたことを示す情報、または仮想通貨に対して売り介入（例：管理装置の口座番号からユーザの口座番号へ仮想通貨を送金すること）が行われたことを示す情報などが含まれる。これにより、どの仮想通貨 ID の仮想通貨に関して、どの口座情報により（例えば口座情報 A から B に対して）、どのような履歴種別の処理が（例えば仮想通貨の移動が）、何時行われたのかを判断することができる。図 3C 中、「0000」は管理者の口座番号を示す。また、（出）は送金元の口座番号を示し、（入）は送金先の口座番号を示す。なお、送金とは仮想通貨を移動させることをいう。

[0023] 以上のとおり、管理装置 10 の記憶装置 14 は発行情報記憶領域 141 と口座情報記憶領域 142 と履歴情報記憶領域 143 という 3 つの記憶領域を有している。そして、これら 3 つの記憶領域それぞれには仮想通貨 ID が記憶されている。このようにすれば、履歴情報記憶領域 143 に記憶されている情報の整合性のみに依存するのではなく、仮想通貨 ID をキーにして、履

歴情報記憶領域 1 4 3 に記憶されている情報を、発行情報記憶領域 1 4 1 に記憶されている情報及び／又は口座情報記憶領域 1 4 2 に記憶されている情報に突き合わせて矛盾がないかどうかを判断することにより、発行情報記憶領域 1 4 1 に記憶されている情報、口座情報記憶領域 1 4 2 に記憶されている情報、及び履歴情報記憶領域 1 4 3 に記憶されている情報が改ざんされていないことを確認することができる。例えば、履歴情報記憶領域 1 4 3 に、仮想通貨 I D = 3 に対応付けて口座情報 A から口座情報 B への売却を示す履歴情報が記載されているのに、口座情報記憶領域 1 4 2 には、仮想通貨 I D = 3 に対応付けて口座情報 A が記憶されている場合は、口座情報記憶領域 1 4 2 と履歴情報記憶領域 1 4 3 のいずれか一方の情報が改ざんされている可能性があるとして判断して、管理装置 1 0 は、仮想通貨 I D = 3 の仮想通貨に関する処理を中断や停止などすることができる。また、たとえ 3 つの記憶領域のうち 1 つが改ざんされても、残る 2 つの記憶領域に記憶されている情報を用いて改ざんされた情報を正しい情報に修復することが可能となる。

[0024] (資産情報記憶領域 1 4 4、発行済数記憶領域 1 4 5)

図 3 D は資産情報記憶領域 1 4 4 の一例を示す模式図であり、図 3 E は履歴情報記憶領域 1 4 3 の一例を示す模式図である。図 3 D、図 3 E に示すように、管理装置 1 0 の記憶装置 1 4 には、資産残高を記憶する資産情報記憶領域 1 4 4 や、仮想通貨の発行済数を記憶する発行済数記憶領域 1 4 5 などを設けることもできる。資産残高とは仮想通貨の対価としてユーザから管理者に払い込まれた価値の合計を示す情報である。図 3 D に示す例では、最新の受取日時に対応付けられている資産残高が最新の資産残高を示している。

[0025] 例えば、仮想通貨が合計で 3 つ発行されている場合であって、1 つ目の仮想通貨の発行価格が 1 0 0 0 円であり、2 つ目の仮想通貨の発行価格が 1 5 0 0 円であり、3 つ目の仮想通貨の発行価格が 2 0 0 0 円であり、これらの対価がユーザから管理者へ払い込まれている場合、資産残高は例えば 4 5 0 0 円であり、発行済数は例えば 3 である。なお、仮想通貨の対価は、仮想通貨の発行価格に応じて定められる値であり、例えば仮想通貨の発行価格に等

しい。対価には円やドルなどの通貨のほか、電子マネーやポイントなどのバリューを用いることができる。

[0026] 資産残高には仮想通貨の対価や仮想通貨の対価を払い込んだユーザの口座情報や対価を受け取った受け取り日時などを対応付けて記憶することができる。このようにすれば、誰が、何時、いくらに対価を払い込んだのかを特定することが容易になる。管理装置 10 は、例えば、既に対価を受け取り済みである場合や、対価の受け取りが確実と見込まれる場合に、発行の対価を資産残高に加算することができる。また、管理装置 10 は、その加算後の資産残高に対応付けてその対価とユーザの口座情報とを記憶することができる。

[0027] 以上説明した各記憶領域は、物理的に 1 つの記憶領域であってもよいし、演算装置 12 が所定の処理を行うことにより実質的に 1 つの領域として取り扱われる複数の記憶領域であってもよい。

[0028] 本実施形態においても、マイニングを行う場合と同様に、記憶領域に記憶される過去から現在にわたるすべての情報を用いて演算量の多いハッシュ値を生成し、これを新たに記憶領域に記憶される情報に含めてもよい。このようにすれば、より記憶領域に記憶されている情報の改ざんを防止することができる。ただし、上記のとおり、本実施形態によれば、このような演算量の多いハッシュ値を用いた改ざん防止装置によらずとも、仮想通貨に関する不正を検知することができる。したがって、ハッシュ値を用いるにしても、演算量が多いハッシュ値ではなく、演算量が少ないハッシュ値などを用いることが好ましい。

[0029] (管理装置 10 の動作例：仮想通貨の発行)

図 4 は実施形態 1 に係る管理装置の動作例（仮想通貨の発行）を説明するシーケンス図である。以下、図 4 を参照しつつ、ユーザ装置 21 に対して仮想通貨が発行される場合における、管理装置 10 の動作例について説明する。

[0030] (ステップ S 11)

まず、管理装置 10 は、ユーザ装置 21 から口座情報を指定する仮想通貨

発行要求を受信する。これにより、ユーザ装置 21 から管理者に対して、仮想通貨の発行が要求される。仮想通貨発行要求は口座情報に加えて発行希望数を指定するものであってもよい。

[0031] (ステップ S 12)

管理装置 10 は、管理者がユーザから仮想通貨の対価を受け取った場合、記憶装置 14 の資産情報記憶領域 144 の資産残高に対価を加算することが好ましい (ステップ S 12)。これにより、仮想通貨の発行と管理者の資産残高を正確にリンクさせることができる。また、後述する買い介入が無制限に行われることを防止することができる。なお、本工程は、対価の受け取り前や仮想通貨の発行処理後に実行することもできる。

[0032] (ステップ S 13、S 14)

次に、管理装置 10 は、仮想通貨の対価の受け取り条件を含む発行条件の成否を判断し (ステップ S 13)、この発行条件が成立する場合に、仮想通貨の発行処理 (ステップ S 14) を実行する。対価の受け取りを条件とすることにより、対価を仮想通貨の価値の裏付けとして、仮想通貨の価値を安定させることができる。また、後述する買い介入の実行に制限をかけることができる。

[0033] 受け取り条件の成否は、仮想通貨の対価が既に受け取り済みであるか、あるいは、受け取りが確実であると見込まれるかどうかにより判断することができる。具体的な判断の態様は特に限定されるものではないが、例えば、資産情報記憶領域 144 に、仮想通貨発行要求で指定された口座情報に対応して対価が記憶されているかどうか、ユーザの信用力を示す数値、あるいは信用力がある者としてあらかじめ記憶装置 14 に記憶されているユーザであるかどうか、仮想通貨の対価を実質的に受け取り済みと評価できるかどうかなどにより判断することができる。

[0034] 発行条件は、さらに、発行済数記憶領域 145 に記憶されている発行済数が所定の上限値以下である、あるいは、仮想通貨発行要求に N ($N \geq 2$) の発行希望数が指定されている場合は発行済数記憶領域 145 に記憶されてい

る発行済数と発行希望数との和が所定の上限値以下である、との条件を含んでいることが好ましい。所定の上限値は、市場の動向に応じて決定される。

[0035] また、発行条件は、さらに、仮想通貨の市場価格が発行価格以上であるとの条件を含むことが好ましい。このようにすれば、市場価格に応じて仮想通貨の発行数（供給量）を制限し、仮想通貨の価値を容易に維持することができる。市場価格、例えば、ネットワーク 30 上のサーバなどから管理装置 10 に送信される

[0036] 以下、仮想通貨の発行処理（ステップ S 14）について説明する。

[0037] （ステップ S 141）

まず、管理装置 10 は、新たな仮想通貨 I D を発行情報記憶領域 141 に記憶する。これにより、新たな仮想通貨 I D が発行され、その旨が管理装置 10 に記録される。本工程には、新たな仮想通貨 I D を発行情報記憶領域 141 に文字通り記憶する場合のほか、発行情報記憶領域 141 に既に記憶されている未発行の仮想通貨 I D を発行済の仮想通貨 I D として以後取り扱うよう、発行情報記憶領域 141 の情報を書き換える場合が含まれる。前者の文字通り記憶する場合に用いる新たな仮想通貨 I D は、本工程において管理装置 10 がその都度生成してもよいし、使用可能な未発行の仮想通貨 I D を管理装置 10 の記憶装置 14 などに管理者があらかじめ記憶しておき、管理装置 10 がその中からその都度ランダムにあるいは所定のルールに基づいて選択してもよい。

[0038] （ステップ S 142）

次に、管理装置 10 は、新たな仮想通貨 I D を仮想通貨発行要求が指定する口座情報に対応付けて口座情報記憶領域 142 に記憶する。これにより、新たに発行された仮想通貨の所有者が管理装置 10 に記録される。

[0039] （ステップ S 143）

次に、管理装置 10 は、新たな仮想通貨 I D と新たに仮想通貨を発行したことを示す履歴情報とを対応付けて履歴情報記憶領域に記憶する。これにより、新たに仮想通貨を発行したという事実が管理装置 10 に記録される。

[0040] (ステップS 1 4 4)

管理装置 1 0 は、発行済数記憶領域 1 4 5 に記憶されている発行済数を増やすことが好ましい。このようにすれば、仮想通貨の発行済数を管理することができるため、発行数を制限することが可能となる。管理装置 1 0 は、仮想通貨発行要求に発行希望数が指定されていない場合、あるいは、仮想通貨発行要求に 1 の発行希望数が指定されている場合、発行済数を 1 つ増やす。また、管理装置 1 0 は、仮想通貨発行要求に N ($N \geq 2$) の発行希望数が指定されている場合は発行済数を N 増やす。

[0041] (ステップS 1 4 5)

管理装置 1 0 は、仮想通貨発行通知をユーザ装置 2 1 に送信することが好ましい。これにより、ユーザ装置 2 1 のユーザに仮想通貨の発行が通知される。

[0042] (仮想通貨の売買仲介)

図 5 は実施形態 1 に係る管理装置の動作例（仮想通貨の売買仲介）を説明するシーケンス図である。以下、図 5 を参照しつつ、ユーザ装置 2 1 とユーザ装置 2 2 との間で仮想通貨の売買が行われる場合における、管理装置 1 0 の動作例について説明する。

[0043] (ステップS 2 1、S 2 2)

まず、管理装置 1 0 は、一のユーザ装置 2 1 から口座情報を指定する売り注文を受信し（ステップS 2 1）、且つ、他のユーザ装置 2 2 から口座情報を指定する買い注文を受信する（ステップS 2 2）。これにより、一のユーザ装置 2 1 から管理装置 1 0 に対して仮想通貨の売却が要求され、他のユーザ装置 2 2 から管理装置 1 0 に対して仮想通貨の購入が要求される。売り注文は口座情報に加えて売却希望数を指定するものであってもよい。買い注文は口座情報に加えて購入希望数を指定するものであってもよい。

[0044] (ステップS 2 3、S 2 4)

次に、管理装置 1 0 は、売り注文で指定される口座情報が口座情報記憶領域 1 4 2 に対応付けて記憶されており、売り注文で指定される口座情報に対

応付けて口座情報記憶領域 142 に記憶されている仮想通貨 I D が発行情報記憶領域 141 に記憶されており、且つ、売り注文で指定される口座情報に対応付けて口座情報記憶領域 142 に記憶されている仮想通貨 I D が履歴情報に対応付けて履歴情報記憶領域 143 に記憶されているとの条件を含む売買仲介条件の成否を判断し（ステップ S 23）、成立している場合に、売り注文が指定する口座情報に対応付けて口座情報記憶領域 142 に記憶されている仮想通貨 I D について売買が成立するものとして売買仲介処理（ステップ S 24）を実行する。売り注文が指定する口座情報に対応付けて口座情報記憶領域 142 に複数の仮想通貨 I D が記憶されている場合には、そのうちの 1 つまたは複数の仮想通貨 I D について売買が成立するものとして、1 つまたは複数の仮想通貨 I D それぞれについて売買仲介処理（ステップ S 24）を実行することができる。以下、売買仲介処理（ステップ S 24）について説明する。

[0045] （ステップ S 241）

まず、管理装置 10 は、売り注文で指定される口座情報と売買が成立した仮想通貨 I D とを口座情報記憶領域 142 から削除するとともに、買い注文で指定される口座情報と、売買が成立した仮想通貨 I D とを対応付けて口座情報記憶領域 142 に記憶する（ステップ S 241）。これにより、仮想通貨が売り主である一のユーザ装置 21 のユーザから買い主である他のユーザ装置 21 のユーザへ移転し（送金が完了し）、その旨が管理装置 10 に記録される。

[0046] （ステップ S 242）

次に、管理装置 10 は、売買が成立した仮想通貨 I D と仮想通貨の売買が成立したことを示す履歴情報とを対応付けて履歴情報記憶領域 143 に記憶する。これにより、仮想通貨の売買（送金）が成立したという事実が管理装置 10 に記録される。

[0047] （ステップ S 243、S 244）

管理装置 10 は、売買成立通知をユーザ装置 21、ユーザ装置 22 に送信

することが好ましい。これにより、ユーザ装置 2 1、ユーザ装置 2 2 のユーザに仮想通貨の売買成立が通知される。

[0048] (仮想通貨の買い介入)

図 6 は実施形態 1 に係る管理装置の動作例（買い介入処理）を説明するシーケンス図である。以下、図 6 を参照しつつ、管理装置 1 0 が買い介入する場合における、管理装置 1 0 の動作例について説明する。

[0049] (ステップ S 3 1)

まず、管理装置 1 0 は、口座情報を指定する売り注文を受信する。これにより、一のユーザ装置 2 1 から管理者に対して仮想通貨の売却が要求される。売り注文は口座情報に加えて売却希望数を指定するものであってもよい。

[0050] (ステップ S 3 2)

次に、管理装置 1 0 は、対象価格が所定の買い介入設定価格以下であり、売り注文で指定される口座情報が口座情報記憶領域 1 4 2 に対応付けて記憶されており、売り注文で指定される口座情報に対応付けて口座情報記憶領域 1 4 2 に記憶されている仮想通貨 I D が発行情報記憶領域 1 4 1 に記憶されており、且つ、売り注文で指定される口座情報に対応付けて口座情報記憶領域 1 4 2 に記憶されている仮想通貨 I D が履歴情報に対応付けて履歴情報記憶領域 1 4 3 に記憶されているとの条件を含む買い介入条件の成否を判断し（ステップ S 3 2）、買い介入条件が成立する場合には、売り注文が指定する口座情報に対応付けて口座情報記憶領域 1 4 2 に記憶されている仮想通貨 I D について買い介入が成立するものとして買い介入処理（ステップ S 3 3）を実行する。売り注文が指定する口座情報に対応付けて口座情報記憶領域 1 4 2 に複数の仮想通貨 I D が記憶されている場合には、そのうちの 1 つまたは複数の仮想通貨 I D について買い介入が成立するものとして、1 つまたは複数の仮想通貨 I D それぞれについて買い介入処理（ステップ S 3 3）を実行することができる。このようにすれば、管理装置 1 0 が、所定の条件の成立により買い介入処理を自動的に（人の手を介さずに）実行することが可能となり、仮想通貨の価値下落防止を迅速かつ的確に図ることができる。以

下、買い介入処理（ステップS 3 3）について説明する。

[0051] 買い介入条件は、資産情報記憶領域 1 4 4 に記憶されている資産残高に記憶されている資産残高が対象価格以上である、あるいは、売り注文に N ($N \geq 2$) の売却希望数が指定されている場合は、資産情報記憶領域 1 4 4 に記憶されている資産残高が売却希望数と対象価格との積以上であるとの条件を含んでいることが好ましい。このようにすれば、買い介入処理の実行を、管理者が資産を有している資産残高の範囲内に制限することができる。したがって、無制限に買い介入が行われることを防止することができる。

[0052] 対象価格は、例えば、ネットワーク 3 0 上のサーバなどから管理装置 1 0 に送信される仮想通貨の市場価格であってもよいし、売り注文で指定される売り注文価格であってもよい。買い介入設定価格は、例えば、あらかじめ管理者により管理装置 1 0 に入力され、管理装置 1 0 の記憶装置 1 4 に記憶されている。

[0053] (ステップS 3 3 1)

まず、管理装置 1 0 は、売り注文で指定された口座情報と買い介入が成立した仮想通貨 I D とを口座情報記憶領域 1 4 2 から削除するとともに、管理装置 1 0 の口座情報と買い介入が成立した仮想通貨 I D とを対応付けて口座情報記憶領域 1 4 2 に記憶する（ステップS 3 3 1）。これにより、仮想通貨が売り主である一のユーザ装置 2 1 のユーザから買い主である管理者へ移転し、その旨が管理装置 1 0 に記録される。

[0054] (ステップS 3 3 2)

次に、管理装置 1 0 は、買い介入が成立した仮想通貨 I D と買い介入が行われたことを示す履歴情報とを対応付けて履歴情報記憶領域 1 4 3 に記憶する。これにより、仮想通貨の買い介入が行われたという事実が管理装置 1 0 に記録される。

[0055] (ステップS 3 3 3)

管理装置 1 0 は、資産情報記憶領域 1 4 4 に記憶されている資産残高から買い介入が成立した対価を減算することが好ましい（ステップS 3 3 3）。

売り注文に N ($N \geq 2$) の売却希望数が指定されている場合は、資産情報記憶領域 144 に記憶されている資産残高から売却希望数と買い介入が成立した対価との積を減算する。これにより、管理者の資産残高を正確に管理することができる。

[0056] (ステップ S 334)

管理装置 10 は、売買成立通知をユーザ装置 21 に送信することが好ましい。これにより、ユーザ装置 21 のユーザに仮想通貨の売買成立が通知される。

[0057] (仮想通貨の売り介入)

図 7 は実施形態 1 に係る管理装置の動作例 (売り介入処理) を説明するシーケンス図である。以下、図 7 を参照しつつ、管理装置 10 が売り介入する場合における、管理装置 10 の動作例について説明する。

[0058] (ステップ S 41)

まず、管理装置 10 は、一のユーザ装置 21 から口座情報を指定する買い注文を受信する。これにより、一のユーザ装置 21 から管理者に対して仮想通貨の購入が要求される。買い注文は口座情報に加えて購入希望数を指定するものであってもよい。

[0059] (ステップ S 42、ステップ S 43)

次に、管理装置 10 は、対象価格が所定の売り介入設定価格以上であるとの条件を含む売り介入条件の成否を判断し (ステップ S 42)、売り介入条件が成立する場合に、管理装置 10 の口座情報に対応付けて口座情報記憶領域 142 に記憶されている仮想通貨 ID について売り介入が成立するものとして売り介入処理 (ステップ S 43) を実行する。管理装置 10 の口座情報に対応付けて口座情報記憶領域 142 に複数の仮想通貨 ID が記憶されている場合には、そのうちの 1 つまたは複数の仮想通貨 ID について売り介入が成立するものとして、1 つまたは複数の仮想通貨 ID それぞれについて売り介入処理 (ステップ S 43) を実行することができる。このようにすれば、管理装置 10 が、所定の条件の成立により売り介入処理を自動的に (人手を

介さずに）実行できる。以下、売り介入処理（ステップＳ４３）について説明する。

[0060] 売り介入条件には、さらに、対象価格が、最後に発行された仮想通貨の仮想通貨ＩＤに対応付けて発行情報記憶領域に記憶されている仮想通貨の発行価格以上であるとの条件を含むことが好ましい。

[0061] 対象価格は、例えば、ネットワーク３０上のサーバなどから管理装置１０に送信される仮想通貨の市場価格であってもよいし、買い注文で指定される買い注文価格であってもよい。売り介入設定価格は、例えば、あらかじめ管理者により管理装置１０に入力され、管理装置１０の記憶装置１４に記憶されている。

[0062] （ステップＳ４３１）

まず、管理装置１０は、管理装置１０の口座情報と売り介入が成立した仮想通貨ＩＤとを口座情報記憶領域１４２から削除するとともに、買い注文で指定された口座情報と、売買が成立した仮想通貨ＩＤとを対応付けて口座情報記憶領域１４２に記憶する。これにより、仮想通貨が売り主である管理者から買い主である一のユーザ装置２１のユーザへ移転し、その旨が管理装置１０に記録される。

[0063] （ステップＳ４３２）

次に、管理装置１０は、売り介入が成立した仮想通貨ＩＤと売り介入が行われたことを示す履歴情報とを対応付けて履歴情報記憶領域１４３に記憶する。これにより、仮想通貨の売り介入が行われたという事実が管理装置１０に記録される。

[0064] （ステップＳ４３３）

管理装置１０は、資産情報記憶領域１４４に記憶されている資産残高に売り介入が成立した価格を加算することが好ましい。これにより、管理者の資産残高を正確に管理することができる。

[0065] （ステップＳ４３４）

管理装置１０は、売買成立通知をユーザ装置２１に送信することが好まし

い。これにより、ユーザ装置 21 のユーザに仮想通貨の売買成立が通知される。

[0066] 以上説明した実施形態 1 によれば、仮想通貨 I D を用いて、膨大な計算量を費やすことなく仮想通貨に関する不正を検知することができる。したがって、システム全体を円滑に運営可能な管理装置 10 及び仮想通貨システム 1 を提供することができる。

[0067] また、本実施形態の売買仲介条件や買い介入条件によれば、仮想通貨の不正な売買や買い介入の誤った行使を防止することができる。すなわち、売り注文で指定される口座情報が口座情報記憶領域 142 に対応付けて記憶されていることを条件とすることにより、口座情報を有していない者による仮想通貨の不正な売却を防止することができる。また、売り注文で指定される口座情報に対応付けて記憶されている仮想通貨 I D が発行情報記憶領域 141 に記憶されていることを条件とすることにより、未発行の仮想通貨が売却されることを防止することができる。また、売り注文で指定される口座情報に対応付けて記憶されている仮想通貨 I D が履歴情報に対応付けて履歴情報記憶領域 143 に記憶されていることを条件とすることにより、履歴情報のない仮想通貨（例：発行の履歴がない仮想通貨）が不正に売却されることを防止することができる。また、3つの記憶領域のいずれか1つの記憶領域に不正がある場合には条件が成立しないため、3つの記憶領域のいずれか1つの記憶領域の情報が改ざんなどされた場合における、売買仲介処理や買い介入処理の実行を効果的に防止することができる。

[0068] ビットコインに代表される既存の仮想通貨には、価値を保管する機能が備わっていないため、価格が急落する虞がある。しかし、本実施形態によれば、仮想通貨の発行が対価と交換により実行されるため、価値の保管機能を備えた仮想通貨を創造することができる。また、売買の仲介において不正を検知することにより、仮想通貨の価値を担保することができる。さらに、買い介入の実行により、価値の急落を直接的に抑制することができる。したがって、本実施形態によれば、発行される仮想通貨に、広く流通する通貨として

必要な要素の一つとして価値の保管機能を付与して、安定した価値を有する仮想通貨を提供することができる。

[0069] 本実施形態によれば、ネットワーク30上の管理装置10（複数の管理装置10がネットワーク30に接続される場合は、例えば後述する最上位層に属する管理装置51。以下、本段落において同じ。）を中央銀行と位置づけ、この中央銀行として位置づけられる管理装置10から唯一の仮想通貨を発行することができる。現在主流の仮想通貨は、マイニング（採掘）という概念で、CPUタイム、電力、及び人件費を使ったマイナー（採掘者）が仮想通貨の発行の対価を受け取ってしまうため、仮想通貨自身の価値を裏付ける価値が存在しない。これに対して、本実施形態によれば、管理装置10が発行する仮想通貨の発行や流通するCPUタイム、電力、及び人件費を効果的に抑制することができる。また、管理装置10が発行した仮想通貨は、個人や法人などのユーザが他の通貨を交換して市場に出回る。その結果、発行と同時に管理装置10の資産情報記憶領域には資産残高（外貨の準備高）が蓄積される。資産残高（外貨の準備高）ができることにより、管理装置10は、自らが発行する仮想通貨の市場価格が下がると、市場から仮想通貨を買い上げること（買い介入）ができる。また、本実施形態によれば、仮想通貨が発行されるごとに発行価格を上昇させることにより、他の仮想通貨に比べて、価格が急激に下落することを抑制しやすい。また、本実施形態によれば、仮想通貨の価格を市場の需給に任せ、仮想通貨の発行数を市場価格に基づき自動的に定め、システムの維持に必要な労働力を削減することもできる。管理者は、管理装置10による仮想通貨との引き換えに、ユーザから、ドル、ユーロ、SDR、円、元、ポンドなどの様々な対価を受け取ることができ、これらの対価は資産残高に加算される。このような資産残高は外貨準備高としての性質を持ち、仮想通貨に価値を保管する機能を持つ。

[0070] [実施形態2に係る仮想通貨システム2]

図8は実施形態2に係る仮想通貨システムの動作例を説明するシーケンスである。図8に示すように、実施形態2に係る仮想通貨システム2は、管理

装置 10 が、ユーザ装置 21 から口座情報を指定する仮想通貨発行要求を受信（ステップ S 51）した場合、仮想通貨の対価の受け取り条件を含む発行条件の成否を判断し（ステップ S 52）、発行条件が成立する場合に、発行情報記憶領域 141 に新たな仮想通貨 ID を記憶する（ステップ S 53）。また、管理装置 10 は、一のユーザ装置 21 から口座情報を指定する売り注文を受信（ステップ S 54）した場合、対象価格が所定の買い介入設定価格以下であるとの条件を含む買い介入条件の成否を判断し（ステップ S 55）、この買い介入条件が成立する場合に、資産情報記憶領域 144 に記憶されている資産残高から買い介入が成立した対価を減算する（ステップ S 56）。管理装置 10 は、ステップ S 56 の完了後、売買成立通知をユーザ装置 21 に送信することが好ましい（ステップ S 56）。実施形態 2 によれば、管理装置 10 が、所定の条件の成立により買い介入処理を自動的に（人手を介さずに）実行できるため、仮想通貨の価値急落防止を迅速かつ的確に図ることができる。

[0071] [実施形態 3 に係る仮想通貨システム 3]

図 9 は実施形態 3 に係る仮想通貨システムの動作例を説明するシーケンスである。図 9 に示すように、実施形態 3 に係る仮想通貨システム 3 は、ツリー状に階層化されて相互に接続される複数の管理装置 51 から 57 を備えた仮想通貨システムである。一の階層に属する管理装置は、自装置用の発行情報記憶領域と他装置用の発行情報記憶領域と、を備えている。他装置用の発行情報記憶領域には、一の階層の 1 つ下の階層に属する管理装置の自装置用の発行情報記憶領域に記憶されている情報が記憶されている。つまり、他装置用の発行情報記憶領域と、一の階層の 1 つ下の階層に属する管理装置の自装置用の発行情報記憶領域との間で情報が共有（または同期）されている。第 1 階層に属する管理装置 51 の直下には第 2 階層に属する管理装置 52、53 が接続され、第 2 階層に属する管理装置 52 の直下には第 3 階層に属する管理装置 54、55、56、57 が接続されている。

[0072] 具体的に説明すると、最上位層の管理装置 51 は、自装置用の発行情報記

憶領域Aと他装置用の発行情報記憶領域B、Cとを備えている。また、第2階層に属する管理装置52は、自装置用の発行情報記憶領域Bと他装置用の発行情報記憶領域D、E、F、Gとを備えている。また、第2階層に属する管理装置53は、自装置用の発行情報記憶領域Cと他装置用の発行情報記憶領域H、I、J、Kとを備えている。さらに、第3階層に属する管理装置54、55、56、57は、自装置用の発行情報記憶領域D、E、F、Gをそれぞれ備え、且つ、他装置用の発行情報記憶領域をそれぞれ備えている。最上位層の管理装置51が備える他装置用の発行情報記憶領域B、Cには、第2階層に属し最上位層の管理装置51の直下に接続される管理装置52、53が有する自装置用の発行情報記憶領域B、Cに記憶されている情報が記憶されている。また、第2階層に属する管理装置52が備える他装置用の発行情報記憶領域D、E、F、Gには、第3階層に属し第2階層に属する管理装置52の直下に接続される管理装置54、55、56、57が備える自装置用の発行情報記憶領域D、E、F、Gに記憶されている情報がそれぞれ記憶されている。

[0073] 実施形態3によれば、ユーザ装置は、複数の管理装置51から57のいずれかに仮想通貨発行要求を送信したり、売り注文や買い注文を送信したりなどすることができるため、仮想通貨システム3におけるトラフィックの負荷を分散することができる。また、一の階層に属する管理装置とその1つ下の階層に属する管理装置との間で、発行情報記憶領域が共有されるため、一の階層に属する管理装置が備える他装置用の発行情報記憶領域を、その下の階層に属する管理装置が備える自装置用の発行情報記憶領域に記憶される内容に対比させ、両者が一致するかどうかを判断することにより、不正の検出を容易に図ることができる。

[0074] なお、図示及び詳細な説明は省略するが、口座情報記憶領域と履歴情報記憶領域についても、発行情報記憶領域の場合と同様に、一の階層に属する管理装置とその下の階層に属する管理装置との間で共有（または同期）させることができる。

[0075] 実施形態3においては、自装置用の発行情報記憶領域、自装置用の口座情報記憶領域、及び自装置用の履歴情報記憶領域の少なくとも1つの記憶領域への書き込み禁止及び／又は読み込み禁止が設定されており、他装置用の発行情報記憶領域、他装置用の口座情報記憶領域、及び他装置用の履歴情報記憶領域の少なくとも1つの記憶領域への書き込み禁止及び／又は読み込み禁止が設定されていてもよい。このようにすれば、下位の階層に属する管理装置の管理者の権限に応じて、下位の階層に属する管理装置の機能を制限することができるため、下位の階層に属する管理装置の管理者が、売買の仲介を行う権限は有しているが、仮想通貨の発行の権限は有していない場合などにおいて、下位の階層に属する管理装置の機能を適切に制限することができる。

[0076] 複数の管理装置51から57は、直接的に接続されてもよいし、他の装置を介して接続されていてもよいし、インターネットや専用の回線などのネットワークを介して接続されていてもよい。

[0077] [その他]

本明細書において、一の情報を指定する一の要求や一の注文を送信または受信するとは、例えば、一の情報そのものを含む一の要求や一の注文を受信する場合のほか、一の要求に関連して当該一の要求を受信する前及び／又は後に当該一の情報が受信する場合や、一の情報そのものは受信されないが、受信した当該一の要求から当該一の情報を特定できる場合などをいう。

[0078] また、本明細書において、ある領域に記憶されるある情報やあるデータなどの削除には、当該領域において当該情報や当該データなどを文字通り削除する場合（例：当該情報や当該データなどが格納されているレコード（行）などを文字通り削除する場合）のほか、当該領域において当該情報や当該データなどを削除することなく無効化することにより実質的に削除する場合（例：当該情報や当該データなどが格納されているレコード（行）などに無効を示す旨の他の情報や他のデータを格納する場合）が含まれる。

[0079] また、本明細書において、一の要求や一の注文などは1つのデータとして

送受信されるものであってもよいし、複数のデータに分割されて送受信されるものであってもよい。また、一の要求や一の注文などは１回で送受信されてもよいし、複数回に分けて送受信されてもよい。また、一の要求や一の注文などは単独で送受信されてもよいし、他の情報とともに送信されてもよい。例えば、上記した一の要求や一の注文などにヘッダなどの情報を付加して１つまたは複数のパケットを構成し、この１つまたは複数のパケットを送受信することにより、上記した一の要求や一の注文などを送受信することとしてもよい。

[0080] 各国の中央銀行や民間の銀行などは、管理装置１０により発行される仮想通貨に価値を裏付けられた、さらに新たな仮想通貨や現実の通貨を発行することができる。

[0081] 以上、実施形態について説明したが、これらの説明によって特許請求の範囲に記載された構成は何ら限定されるものではない。

符号の説明

[0082] １、２、３ 仮想通貨システム

１０ 管理装置

１２ 演算装置

１４ 記憶装置

１４１ 発行情報記憶領域

１４２ 口座情報記憶領域

１４３ 履歴情報記憶領域

１４４ 資産情報記憶領域

１４５ 発行済数記憶領域

２１、２２ ユーザ装置

３０ ネットワーク

５１から５７ 管理装置

請求の範囲

- [請求項1] 複数のユーザ装置にネットワークを介して接続される管理装置であって、
- 発行済仮想通貨の仮想通貨IDを記憶する発行情報記憶領域と、
- 口座情報を1つまたは複数の仮想通貨IDに対応付けて記憶する口座情報記憶領域と、
- 仮想通貨の履歴情報を仮想通貨IDに対応付けて記憶する履歴情報記憶領域と、を有する管理装置。
- [請求項2] 前記ユーザ装置から口座情報を指定する仮想通貨発行要求を受信した場合、仮想通貨の対価の受け取りを条件に含む発行条件の成否を判断し、前記発行条件が成立する場合に、仮想通貨の発行処理を実行し、
- 前記仮想通貨の発行処理は、
- 新たな仮想通貨IDを前記発行情報記憶領域に記憶する工程と、
- 前記新たな仮想通貨IDを前記仮想通貨発行要求が指定する口座情報に対応付けて前記口座情報記憶領域に記憶する工程と、
- 前記新たな仮想通貨IDを新たに仮想通貨を発行したことを示す履歴情報に対応付けて前記履歴情報記憶領域に記憶する工程と、
- を有する請求項1に記載の管理装置。
- [請求項3] 仮想通貨の発行済数を記憶する発行済数記憶領域を備え、
- 前記発行条件は、前記発行済数記憶領域に記憶されている発行済数が所定の上限値以下である、あるいは、前記仮想通貨発行要求にN（ $N \geq 2$ ）の発行希望数が指定されている場合は前記発行済数記憶領域に記憶されている発行済数と前記発行希望数との和が前記所定の上限値以下である、との条件を含む請求項1または2に記載の管理装置。
- [請求項4] 一の前記ユーザ装置から口座情報を指定する売り注文を受信し、且つ、他の前記ユーザ装置から口座情報を指定する買い注文を受信した場合、

前記売り注文が指定する口座情報が前記口座情報記憶領域に記憶されており、

前記売り注文が指定する口座情報に対応付けて前記口座情報記憶領域に記憶されている仮想通貨 I D が前記発行情報記憶領域に記憶されており、且つ、

前記売り注文が指定する口座情報に対応付けて前記口座情報記憶領域に記憶されている仮想通貨 I D が履歴情報に対応付けて前記履歴情報記憶領域に記憶されている、

との条件を含む売買仲介条件の成否を判断し、前記売買仲介条件が成立する場合に、前記売り注文が指定する口座情報に対応付けて前記口座情報記憶領域に記憶されている仮想通貨 I D について売買が成立するものとして売買仲介処理を実行し、

前記売買仲介処理は、

前記売り注文が指定する口座情報と前記売買が成立した仮想通貨 I D とを前記口座情報記憶領域から削除するとともに、前記買い注文が指定する口座情報と、前記売買が成立した仮想通貨 I D とを対応付けて前記口座情報記憶領域に記憶する工程と、

前記売買が成立した仮想通貨 I D と仮想通貨の売買が成立したことを示す履歴情報とを対応付けて前記履歴情報記憶領域に記憶する工程と、

を有する請求項 1 から 3 のいずれか 1 項に記載の管理装置。

[請求項5]

一の前記ユーザ装置から口座情報を指定する売り注文を受信した場合、

対象価格が所定の買い介入設定価格以下であり、

前記売り注文が指定する口座情報が前記口座情報記憶領域に記憶されており、

前記売り注文が指定する口座情報に対応付けて前記口座情報記憶領域に記憶されている仮想通貨 I D が前記発行情報記憶領域に記憶され

ており、且つ、

前記売り注文が指定する口座情報に対応付けて前記口座情報記憶領域に記憶されている仮想通貨 I D が履歴情報に対応付けて前記履歴情報記憶領域に記憶されている、

との条件を含む買い介入条件の成否を判断し、前記買い介入条件が成立する場合に、前記売り注文が指定する口座情報に対応付けて前記口座情報記憶領域に記憶されている仮想通貨 I D について買い介入が成立するものとして買い介入処理を実行し、

前記買い介入処理は、

前記売り注文が指定する口座情報と前記買い介入が成立した仮想通貨 I D とを前記口座情報記憶領域から削除するとともに、前記管理装置の口座情報と前記買い介入が成立した仮想通貨 I D とを対応付けて前記口座情報記憶領域に記憶する工程と、

前記買い介入が成立した仮想通貨 I D と買い介入が行われたことを示す履歴情報とを対応付けて前記履歴情報記憶領域に記憶する工程と、

を有する請求項 1 から 4 のいずれか 1 項に記載の管理装置。

[請求項6]

前記買い介入条件は、前記資産情報記憶領域に記憶されている資産残高に記憶されている資産残高が前記対象価格以上である、あるいは、前記売り注文に N ($N \geq 2$) の売却希望数が指定されている場合は、前記資産情報記憶領域に記憶されている資産残高が前記売却希望数と前記対象価格との積以上であるとの条件を含み、

前記買い介入処理は、前記資産情報記憶領域に記憶されている資産残高から前記対象価格を減算する、あるいは、前記売り注文に N ($N \geq 2$) の売却希望数が指定されている場合は、前記資産情報記憶領域に記憶されている資産残高から前記売却希望数と前記対象価格との積を減算する工程を含む請求項 5 に記載の管理装置。

[請求項7]

一の前記ユーザ装置から口座情報を指定する買い注文を受信した場

合、

対象価格が所定の売り介入設定価格以上であるとの条件を含む売り介入条件の成否を判断し、前記売り介入条件が成立する場合に、前記管理装置の口座情報に対応付けて前記口座情報記憶領域に記憶されている仮想通貨 I D について売り介入が成立するものとして売り介入処理を実行し、

前記売り介入処理は、

前記管理装置の口座情報と前記売り介入が成立した仮想通貨 I D とを前記口座情報記憶領域から削除するとともに、前記買い注文が指定する口座情報と前記売り介入が成立した仮想通貨 I D とを対応付けて前記口座情報記憶領域に記憶する工程と、

前記売り介入が成立した仮想通貨 I D と売り介入が行われたことを示す履歴情報とを対応付けて前記履歴情報記憶領域に記憶する工程と、

を有する請求項 1 から 6 のいずれか 1 項に記載の管理装置。

[請求項 8]

複数のユーザ装置にネットワークを介して接続された管理装置であって、

発行済仮想通貨の仮想通貨 I D を記憶する発行情報記憶領域と、
資産残高を記憶する資産情報記憶領域と、を備え、

前記ユーザ装置から口座情報を指定する仮想通貨発行要求を受信した場合、仮想通貨の対価の受け取りを条件に含む発行条件の成否を判断し、前記発行条件が成立する場合に、前記発行情報記憶領域に新たな仮想通貨 I D を記憶し、

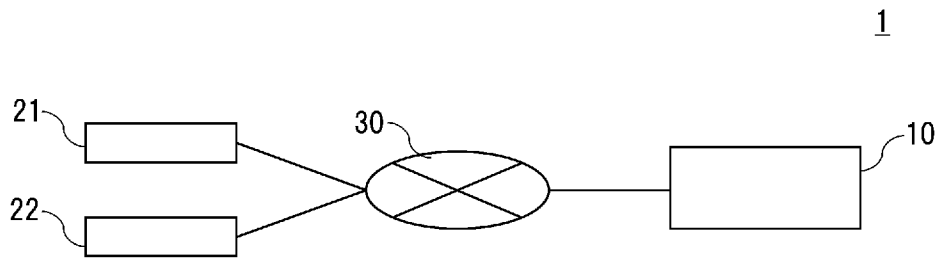
一の前記ユーザ装置から口座情報を指定する売り注文を受信した場合、対象価格が所定の買い介入設定価格以下であるとの条件を含む買い介入条件の成否を判断し、前記買い介入条件が成立する場合に、前記資産情報記憶領域に記憶されている資産残高から前記買い介入が成立した対価を減算する管理装置。

- [請求項9] 請求項 1 から 8 のいずれか 1 項に記載の管理装置と、
前記管理装置にネットワーク介して接続される複数のユーザ装置と、
、
を備える仮想通貨システム。
- [請求項10] ツリー状に階層化されて相互に接続される複数の請求項 1 から 8 の
いずれか 1 項に記載の管理装置を備えた仮想通貨システムであって、
一の階層に属する前記管理装置は、
自装置用の前記発行情報記憶領域、自装置用の前記口座情報記憶領域、
及び自装置用の前記履歴情報記憶領域と、
他装置用の前記発行情報記憶領域、他装置用の前記口座情報記憶領域、
及び他装置用の前記履歴情報記憶領域と、を備え、
一の階層に属する前記管理装置が備える他装置用の前記発行情報記憶領域、
他装置用の前記口座情報記憶領域、及び他装置用の前記履歴情報記憶領域には、
前記一の階層の 1 つ下の階層に属する前記管理装置の自装置用の前記発行情報記憶領域、
自装置用の前記口座情報記憶領域、及び自装置用の前記履歴情報記憶領域に記憶されている情報が
それぞれ記憶される仮想通貨システム。
- [請求項11] 前記管理装置は、
自装置用の前記発行情報記憶領域、自装置用の前記口座情報記憶領域、
及び自装置用の前記履歴情報記憶領域の少なくとも 1 つの記憶領域への書き込み禁止及び／又は読み込み禁止が設定されており、
他装置用の前記発行情報記憶領域、他装置用の前記口座情報記憶領域、
及び他装置用の前記履歴情報記憶領域の少なくとも 1 つの記憶領域への書き込み禁止及び／又は読み込み禁止が設定されている請求項 10 に記載の仮想通貨システム。
- [請求項12] ツリー状に階層化されて相互に接続される複数の管理装置を備えたシステムであって、
前記管理装置は、

自装置用の記憶領域と他装置用の記憶領域を備え、

一の階層に属する前記管理装置が備える前記他装置用の記憶領域には、前記一の階層の1つ下の階層に属する1つまたは複数の前記管理装置が備える前記自装置用の記憶領域に記憶されている情報が記憶されるシステム。

[図1]



[図2]



[図3A]

仮想通貨ID	発行日時	発行金額	対価を受け取り済
0001	2018/01/02 01:02:03	100円	YES
0002	2018/01/03 18:01:02	200円	YES

141

[図3B]

仮想通貨ID	口座番号	所有者の氏名又は名称
0001	1111	AAA
0002	2222	BBB

142

[図3C]

仮想通貨ID	履歴の種別	口座番号	履歴の日時
0001	発行	0000(出), 1111(入)	2018/01/02 01:02:03
0001	売買	1111(出), 3333(入)	2018/01/04 03:03:03

143

[図3D]

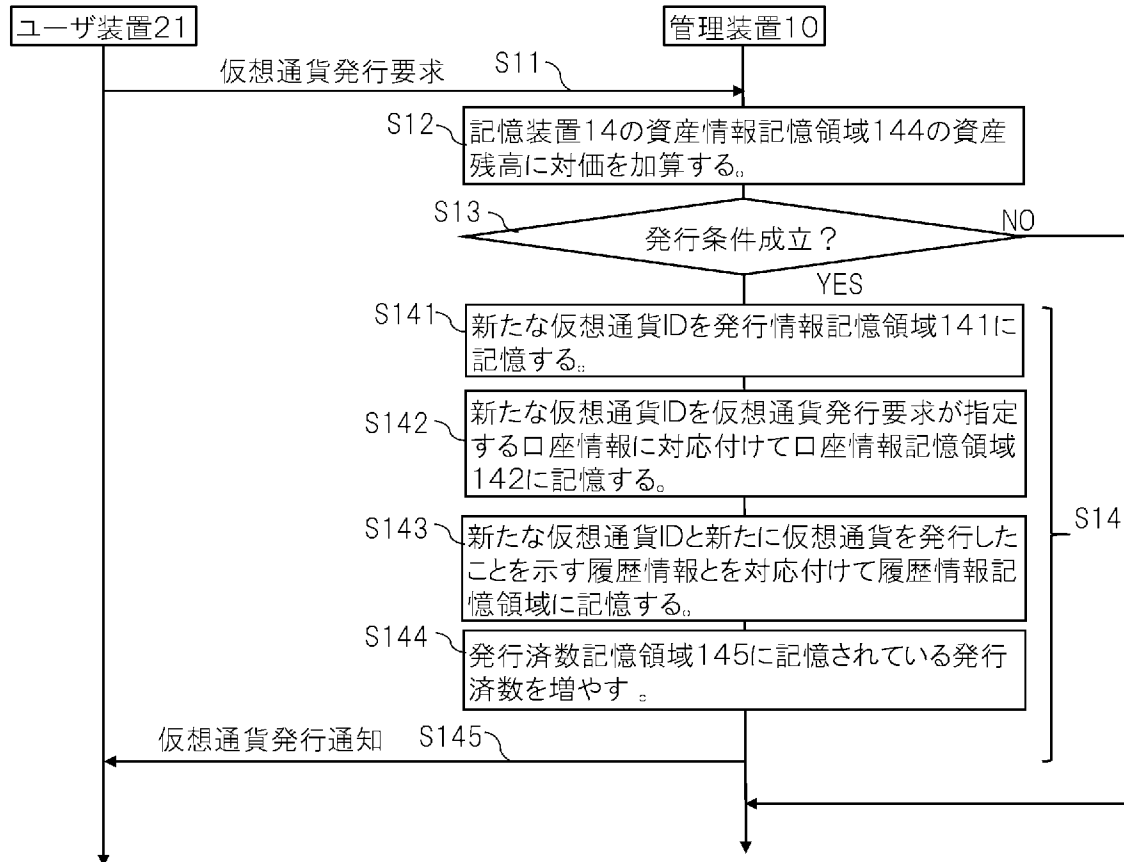
資産残高	口座番号	受取日時
100円	1111	2018/01/02 01:02:03
300円	2222	2018/01/03 18:01:02

144

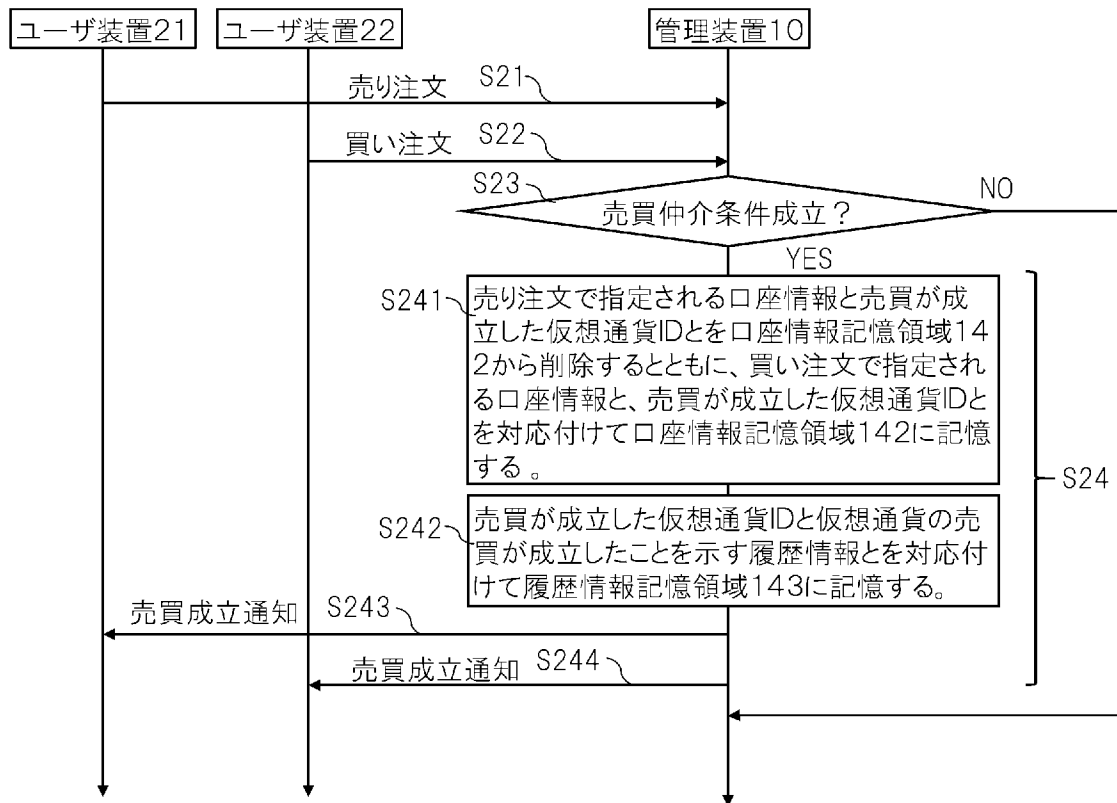
[図3E]

発行済数	145
2	

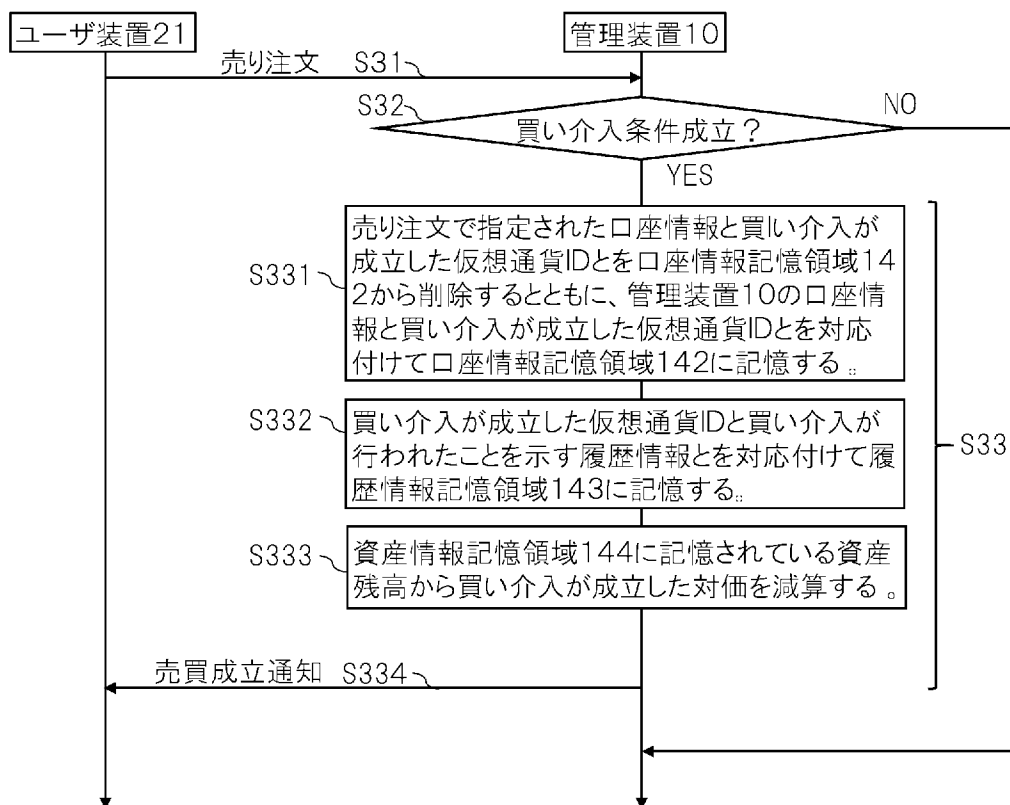
[図4]



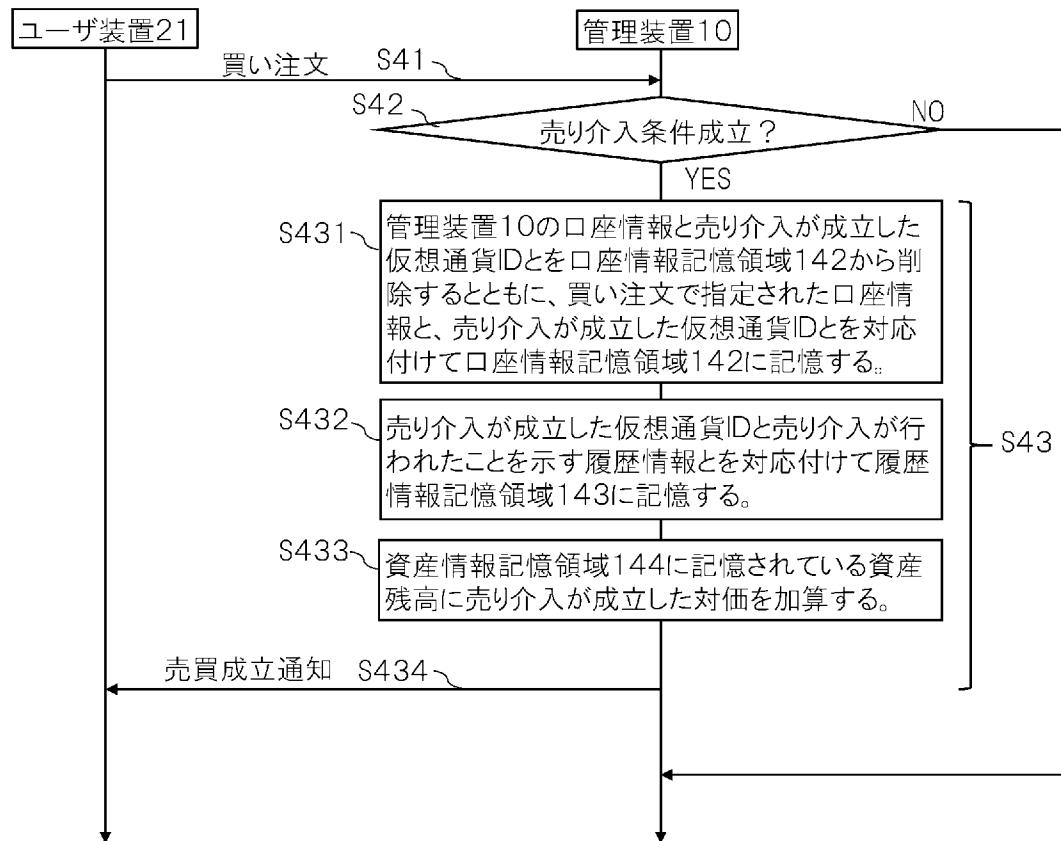
[図5]



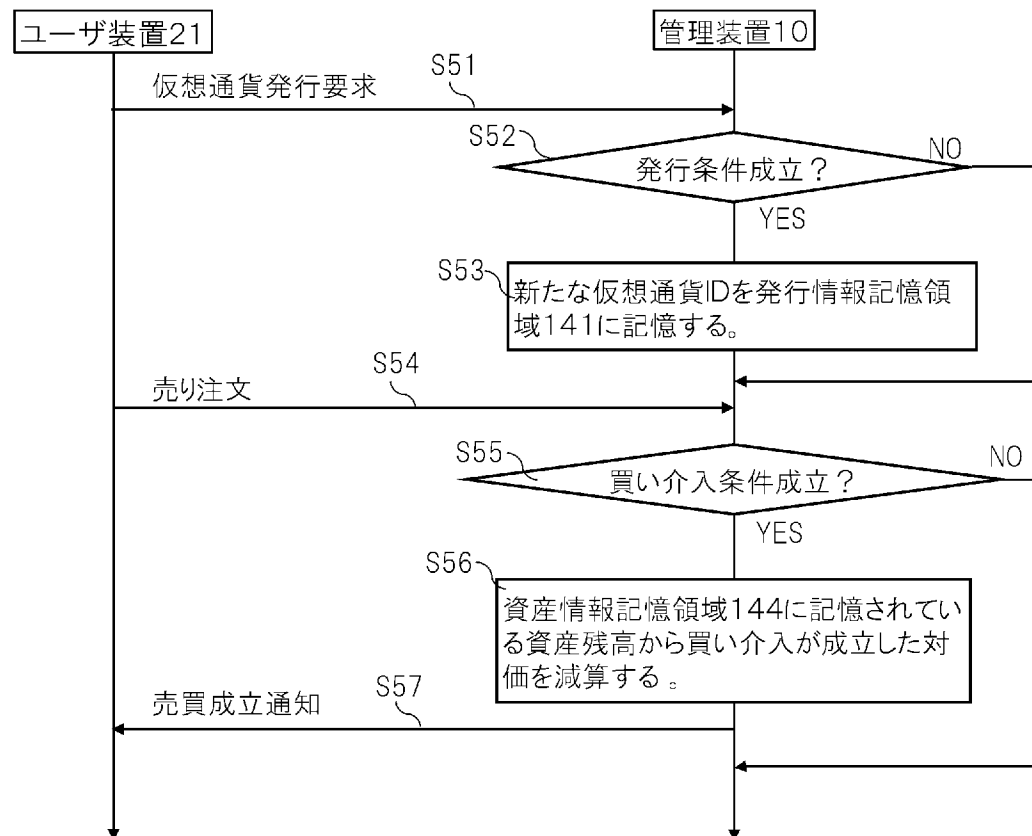
[図6]



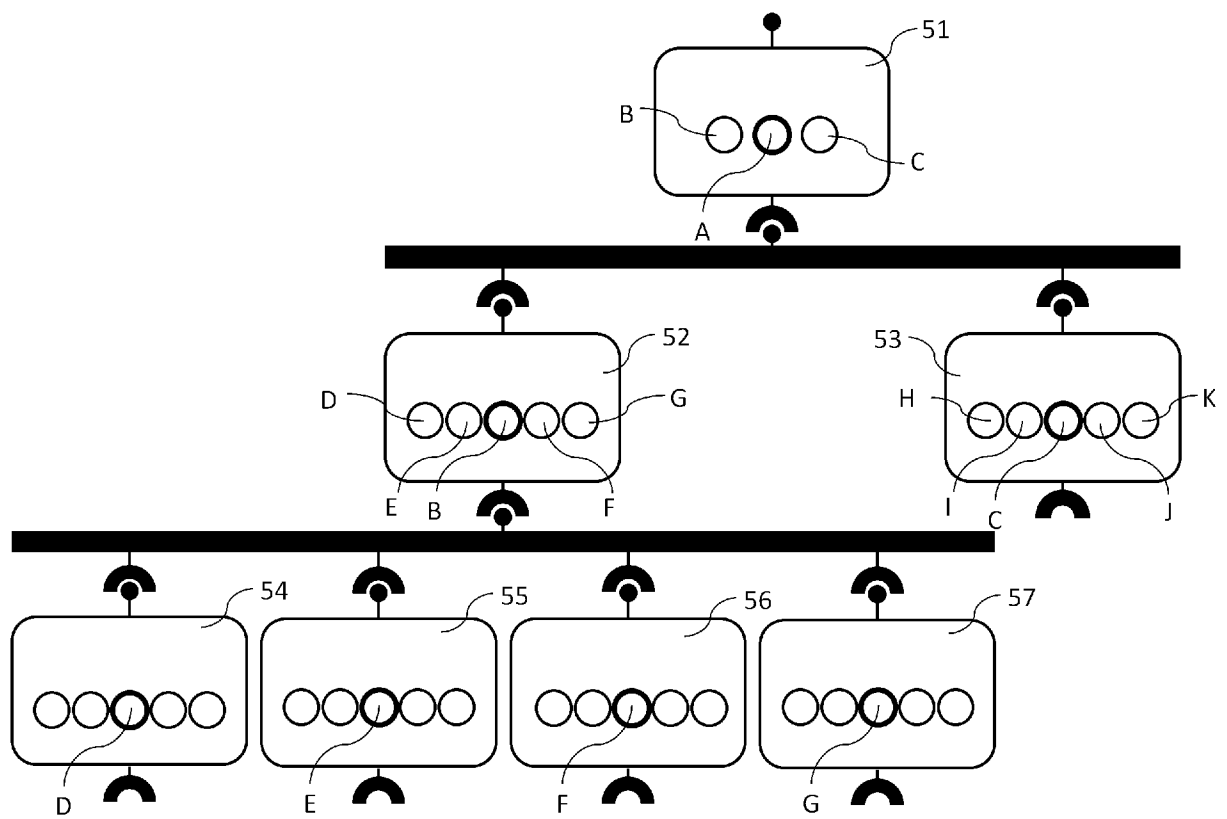
[図7]



[図8]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/043716

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. G06Q20/06 (2012.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl. G06Q20/06

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 1971-2018

Registered utility model specifications of Japan 1996-2018

Published registered utility model applications of Japan 1994-2018

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	JP 2016-151802 A (IMUSIC TECH LTD) 22 August 2016,	1-3
Y	paragraphs [0074]-[0086], [0090], [0113], [0118],	7-9
A	[0127]-[0129], (Family: none)	4-6, 10-11, 12
Y	JP 2017-54339 A (ATOM SOLUTIONS) 16 March 2017,	7-9
	paragraphs [0024], [0025], [0038]-[0045], (Family: none)	
X	JP 4-92597 A (FUJITSU LTD.) 25 March 1992, page 3, lower left column, line 11 to page 4, upper right column, line 9, fig. 2, (Family: none)	12
A	JP 2002-288573 A (HAMADA, Hiroshi) 04 October 2002, entire text, all drawings, (Family: none)	1-12

☐

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
10.01.2018

Date of mailing of the international search report
23.01.2018

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

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06Q20/06 (2012.01) i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. G06Q20/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2018年
日本国実用新案登録公報	1996-2018年
日本国登録実用新案公報	1994-2018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 Y A	JP 2016-151802 A（科韻動力有限公司）2016.08.22, 段落 [0074] ～ [0086]、[0090]、[0113]、 [0118]、[0127] ～ [0129] （ファミリーなし）	1～3 7～9 4～6, 10～11, 12
Y	JP 2017-54339 A（株式会社アトムソリューションズ）2017.03.16, 段落 [0024] ～ [0025]、[0038] ～ [0045] （ファミリーなし）	7～9

☒ 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

10.01.2018

国際調査報告の発送日

23.01.2018

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

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）

山本 雅士

5 L

3786

電話番号 03-3581-1101 内線 3562

C (続き) . 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	JP 4-92597 A (富士通株式会社) 1992. 03. 25, 第 3 頁左下欄第 1 1 行～第 4 頁右上欄第 9 行、図 2 (ファミリーなし)	1 2
A	JP 2002-288573 A (浜田 宏) 2002. 10. 04, 全文, 全図 (ファミリーなし)	1 - 1 2