

(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9月3日(03.09.2020)



(10) 国際公開番号

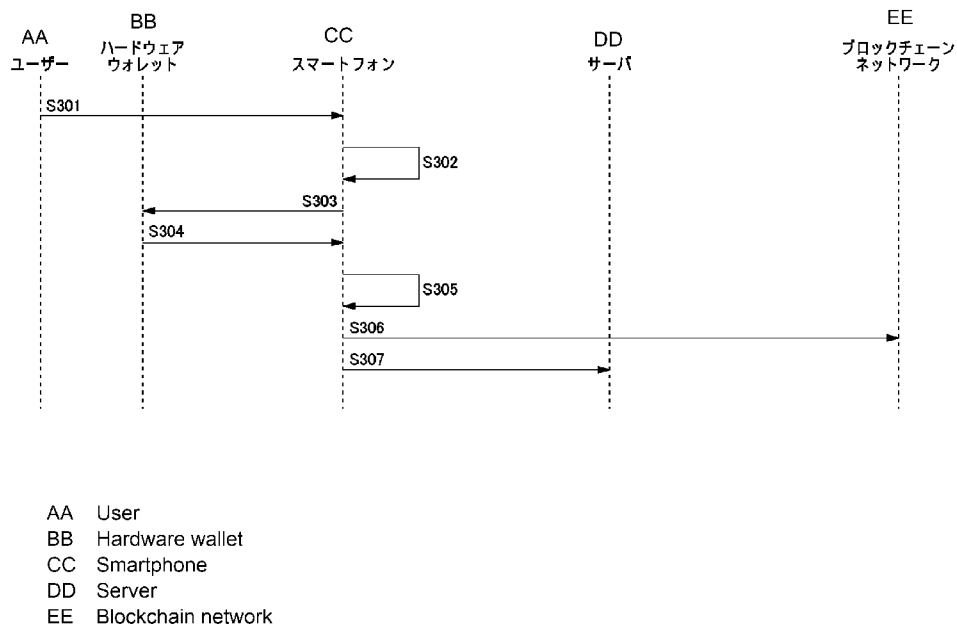
WO 2020/175312 A1

- (51) 国際特許分類:
G09C 1/00 (2006.01) *G06Q 20/38* (2012.01)
H04L 9/32 (2006.01) 4 柏の葉キャンパス 1 4 8 街区 2 ショップ & オフィス棟 K O I L 6 階 Chiba (JP).
- (21) 国際出願番号: PCT/JP2020/006779
- (22) 国際出願日: 2020年2月20日(20.02.2020)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2019-032392 2019年2月26日(26.02.2019) JP
- (71) 出願人: 株式会社 A n d G o (ANDGO, INC.)
[JP/JP]; 〒2770871 千葉県柏市若柴 1 7 8 番地
- (72) 発明者: 原 利 英 (HARA Toshihide); 〒2770871
千葉県柏市若柴 1 7 8 番地 4 柏の葉キャンパス 1 4 8 街区 2 ショップ & オフィス棟 K O I L 6 階 株式会社 A n d G o 内 Chiba (JP).
- (74) 代理人: 大谷 寛 (OTANI Kan); 〒1060032 東京都港区六本木六丁目 2 番 3 1 号六本木ヒルズノースタワー 1 7 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,

(54) Title: DEVICE AND METHOD FOR EVACUATING CRYPTOCURRENCY AND PROGRAM THEREFOR

(54) 発明の名称: 暗号通貨を避難するための装置、方法及びそのためのプログラム

【図3】



(57) Abstract: The present invention enables cryptocurrency for which the secret information needed for remittance is managed outside of an exchange to be evacuated without excessively increasing a user's burden. A device 110 generates remittance transaction data T and also generates evacuation transaction data E for remitting the remainder derived by subtracting an indicated amount of remittance from the amount remittable using secret information (S302) in accordance with a remittance indication (S301). Next, the device 110 transmits the hash value of the transaction data to an apparatus

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,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

添付公開書類：

- 一 国際調査報告 (条約第21条(3))

100 (S303). The apparatus 100 signs the hash value and transmits the signature to the device 110 (S304). Next, the device 110 generates signed remittance transaction data T' and signed evacuation transaction data E' (S305). The data T' is transmitted to a blockchain network 120 (S306), and the data E' is transmitted to a server 120 as preparation for evacuation (S307).

(57) 要約：送金に必要な秘密情報が取引所外で管理される暗号通貨をユーザー負担を過大にすることなく避難可能とする。装置 110 では、送金指示に応じて (S301)、送金トランザクションデータ T を生成するとともに、指示された送金額を秘密情報を用いて送金可能な金額から差し引いた残額を送金するための避難トランザクションデータ E を生成する (S302)。次に、装置 110 はトランザクションデータのハッシュ値を機器 100 に対して送信する (S303)。機器 100 では、ハッシュ値に対する署名を行い、当該署名を装置 110 に送信する (S304)。次いで、装置 110 は、署名済み送金トランザクションデータ T' 及び署名済み避難トランザクションデータ E' を生成する (S305)。データ T' は、ブロックチェーンネットワーク 120 に送信され (S306)、データ E' は、避難準備としてサーバ 120 に送信される (S307)。

明 細 書

発明の名称：

暗号通貨を避難するための装置、方法及びそのためのプログラム

技術分野

[0001] 本発明は、暗号通貨を避難するための装置、方法及びそのためのプログラムに関し、より詳細には、送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨を避難するための装置、方法及びそのためのプログラムに関する。

背景技術

[0002] 暗号通貨の急速な拡がりとともに、暗号通貨を安全に保管するための機器として「ハードウェアウォレット」と呼ばれるものが使用されている。ハードウェアウォレットには、暗号通貨を他者に送金するためのトランザクションに対する署名に必要な秘密鍵が格納されており、ブロックチェーンネットワークにアクセス可能なPC等の機器に一時的に接続される。送金時の限られた間以外はインターネットから遮断することによって、意図せず暗号通貨が他者に送金されるおそれを抑制している。

[0003] ハードウェアウォレットの一例としてLEDGER NANO S（登録商標）が挙げられる。この製品は、PCにUSB接続して使用するハードウェアウォレットであり、PCに最初に接続した初期設定時にPINコードを設定し、このPINコードを入力して秘密鍵へのアクセスを許容する。

[0004] 具体的には、この製品では、複数の秘密鍵が256ビットのシードと呼ばれる秘密情報を用いて階層的に生成可能な方式を採用しており、シードから各秘密鍵及びそれに関連づけられたアドレスを再現可能である。したがって、電源を入れるとシードからこれまでに使用した1又は複数のアドレスのための1又は複数の秘密鍵が再現され、PINコードを用いて当該1又は複数の秘密鍵が利用可能となる。ここで、シードは「セキュアエレメント」と呼ばれる耐タンパー性のある安全性の高いチップに格納されている。

[0005] このように、シードが極めて重要な役割を果たすため、初期設定時には P I N コードの設定に加えてシードの復元のための 2 4 個のリカバリーフレーズが表示され、これらを記録することが要求される。機器を紛失したような場合には、リカバリーフレーズによって、互換性のある新たな機器にシードを復元し、シードからこれまでに使用した 1 又は複数のアドレスのための 1 又は複数の秘密鍵を再現することができる。紛失した機器にはシードが記憶されているが、セキュアエレメント内のシードは P I N コードがなければアクセス不可能に記憶されている。

[0006] このように安全性に配慮されたハードウェアウォレットは存在するものの、いずれも P C に接続して用いるものであり、安全性に配慮しつつ、現在多くの人が持ち歩くスマートフォンを活用したハードウェアウォレットは従来存在しなかったことから、出願人は、スマートフォンとの通信を用いて安全性を確保するハードウェアウォレットを提供している。出願人によるハードウェアウォレットでは、そこで管理される秘密鍵へのアクセスを独自の多要素認証方式によって安全性の高いものとするとともに、シードの復元のために、復元コアと呼ぶ部品にシード自体又はこれと 1 対 1 に対応する情報を記憶することで、ユーザーが機器を紛失した際に備えている（非特許文献 1 参照）。

先行技術文献

非特許文献

[0007] 非特許文献 1：株式会社 AndGo ウェブページ <https://www.andgo.co.jp> [2019 年 2 月 17 日 検索]

発明の概要

発明が解決しようとする課題

[0008] シード及びそこから生成される秘密鍵は暗号通貨の保管において極めて重要であり、上述のようにリカバリーフレーズの記録、復元コアの使用等、いくつかの手法が試みられているものの、シード、秘密鍵等の暗号通貨の送金

に必要となる秘密情報の管理責任をユーザーにすべて課すこととなっている。仮想通貨取引所の外で安全に暗号通貨を保管することに対する需要は高まっているが、一方でその責任を各ユーザーがすべて自ら負うことの負担も大きい。

[0009] 本発明は、このような問題点に鑑みてなされたものであり、その目的は、必要に応じて、送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨をユーザー負担を過大にすることなく避難可能とすることにある。

[0010] ここで、本明細書において「避難 (evacuate)」とは、暗号通貨の全部又は一部に対応する額の暗号通貨の送金を暗号通貨の送金に必要な秘密情報を用いずに可能とすることを言い、「秘密情報」とは、暗号通貨を送金するためのトランザクションに対する署名に必要な秘密鍵又はそれを生成するための情報を言う。

[0011] また、本明細書において「遮断」とは、必要に応じて一時的にインターネットに接続されることを除外するものではない。

課題を解決するための手段

[0012] このような目的を達成するために、本発明の第1の態様は、送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨を避難するための方法であって、ユーザーから前記暗号通貨の一部の送金指示の入力を受け取るステップと、指示された送金額を送金するための送金トランザクションデータを取得するステップと、前記送金トランザクションデータの送金額を前記暗号通貨の全額から引いた残額の全部又は一部を避難するための避難トランザクションデータを取得するステップと、前記送金トランザクションデータのハッシュ値に対する前記秘密情報を用いた署名を受信又は付与するステップと、前記避難トランザクションデータのハッシュ値に対する前記秘密情報を用いた署名を受信又は付与するステップと、署名済み送金トランザクションデータをブロックチェーンネットワークに向けて送信するステップと、署名済み避難トランザクションデータを前記署名済み避難トランザクション

データを保管するためのサーバに送信するステップとを含むことを特徴とする。

[0013] また、本発明の第2の態様は、第1の態様において、前記サーバに、前記署名済み避難トランザクションデータを前記ブロックチェーンネットワークに向けて送信させる避難の実行指示を送信するステップをさらに含むことを特徴とする。

[0014] また、本発明の第3の態様は、第1又は第2の態様において、前記サーバは、仮想通貨取引所を提供するためのサーバ以外のサーバであることを特徴とする。

[0015] また、本発明の第4の態様は、第1から第3のいずれかの態様において、前記避難トランザクションデータは、避難先アドレスである送信先アドレスが、前記ユーザーの本人確認がなされているアドレスであることを特徴とする。

[0016] また、本発明の第5の態様は、第1の態様において、前記避難トランザクションデータは、避難先アドレスである送信先アドレスが、前記ユーザーが仮想通貨取引所から与えられたアドレスであることを特徴とする。

[0017] また、本発明の第6の態様は、第5の態様において、前記避難先アドレスを前記仮想通貨取引所が提供するAPIを呼び出して指定することを特徴とする。

[0018] また、本発明の第7の態様は、第1から第6のいずれかの態様において、前記各ステップは、携帯端末が行い、前記携帯端末が、前記秘密情報を記憶するインターネットから遮断された機器から、前記署名済み避難トランザクションデータのハッシュ値に対する署名を受信することを特徴とする。

[0019] また、本発明の第8の態様は、送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨を避難するための方法であって、前記暗号通貨の全部又は一部を避難するための避難トランザクションデータを取得するステップと、前記避難トランザクションデータのハッシュ値に対する前記秘密情報を用いた署名を受信又は付与するステップと、署名済み避難トランザク

ションデータを前記署名済み避難トランザクションデータを保管するためのサーバに送信するステップとを含むことを特徴とする。

[0020] また、本発明の第9の態様は、装置に、送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨を避難するための方法を実行させるためのプログラムであって、前記方法は、前記暗号通貨の全部又は一部を避難するための避難トランザクションデータを取得するステップと、前記避難トランザクションデータのハッシュ値に対する前記秘密情報を用いた署名を受信又は付与するステップと、署名済み避難トランザクションデータを前記署名済み避難トランザクションデータを保管するためのサーバに送信するステップとを含むことを特徴とする。

[0021] また、本発明の第10の態様は、送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨を避難するための装置であって、前記暗号通貨の全部又は一部を避難するための避難トランザクションデータを取得し、前記避難トランザクションデータのハッシュ値に対する前記秘密情報を用いた署名を受信又は付与して、署名済み避難トランザクションデータを前記署名済み避難トランザクションデータを保管するためのサーバに送信することを特徴とする。

発明の効果

[0022] 本発明の一態様によれば、送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨の全部又は一部を避難するための避難トランザクションデータEを生成し、当該避難トランザクションデータEに上記秘密情報を用いた署名を付加した署名済み避難トランザクションデータE'をブロードキャストせずに別途避難の実行指示があるまでサーバで保管して避難の準備をしておき、避難の実行指示によって署名済み避難トランザクションデータE'をブロードキャストすることによって、この避難サービスを提供する事業者は、各ユーザーの秘密情報にアクセスすることなく、また、各ユーザーの秘密情報の管理負担を過大にすることなく、必要に応じて暗号通貨の避難を可能とすることができる。

図面の簡単な説明

[0023] [図1]本発明の第1の実施形態にかかる暗号通貨を避難するための装置を示す図である。

[図2]本発明の第1の実施形態にかかる送金のための入力画面の一例を示す図である。

[図3]本発明の第1の実施形態にかかる暗号通貨を避難するための方法の流れ図である。

[図4A]本発明の第1の実施形態にかかる避難の実行手順を説明するための図である。

[図4B]本発明の第1の実施形態にかかる避難の実行手順を説明するための図である。

[図5]本発明の第2の実施形態にかかる避難準備指示のための入力画面の一例を示す図である。

発明を実施するための形態

[0024] 以下、図面を参照して本発明の実施形態を詳細に説明する。

(第1の実施形態)

[0025] 図1に、本発明の第1の実施形態にかかる暗号通貨を避難するための装置を示す。装置110は、暗号通貨の送金のためのトランザクションデータTを生成して、当該トランザクションデータT又はそれに基づくハッシュ値Hを、機器100に送信する。機器100では、当該機器100が管理する秘密情報を用いて、トランザクションデータTのハッシュ値に署名を行い、当該署名又は当該署名が付加された署名済みトランザクションデータT'を装置110に送信する。そして、装置110は、署名済みトランザクションデータT'をブロックチェーンネットワーク130にブロードキャストする。この際、ブロードキャストは装置110から直接行われる場合のほか、機器100にインストールされた暗号通貨の送金を行うためのアプリケーションが通信を行うサーバ120を介して行われる場合がある。

[0026] 機器100は、スマートフォン等の装置110からの要求に応じて、そこ

に記憶する秘密情報へのアクセスを可能にする。機器 100 は、一例として、その筐体の上面に表示画面 101 及びボタン等の入力部 102 を有することができるが、IC カードなどのように情報の入出力領域を有しないものとすることもできる。また、装置 110 との通信は、無線又は有線とすることができ、機器 100 と装置 110 との間にセキュアな通信路をいかに確立するか、装置 110 に機器 100 に記憶されている秘密情報へのアクセスをいかに許容するかについては、さまざまな手法を用いることが考えられる。

[0027] 装置 110 は、たとえばスマートフォン等の携帯端末としたり、PC 又はノート PC としたりすることができる。装置 110 は、通信インターフェースなどの通信部 111 と、プロセッサ、CPU 等の処理部 112 と、メモリ、ハードディスク等の記憶装置又は記憶媒体を含む記憶部 113 とを備え、各処理を行うためのプログラムを実行することによって構成することができる。当該プログラムは、1 又は複数のプログラムを含むことがあり、また、コンピュータ読み取り可能な記憶媒体に記録して非一過性のプログラムプロダクトとすることができる。サーバ 120 も同様の構成を有することができるが、簡単のため、図示はしない。

[0028] 装置 110 には、暗号通貨の送金を行うためのアプリケーションをインストールすることができる。図 2 に、装置 110 にインストールされたアプリケーションにおける入力画面の一例を示す。入力画面 200 には、送金先アドレスの入力欄 201 と金額の入力欄 202 があり、メモ欄 203 を設けることもできる。送金先アドレスは、QR コード（登録商標）を撮影して入力可能としてもよく、送金額は仮想通貨又は暗号通貨の種類を選択して入力可能としてもよい。ユーザーが「送金する」ボタン 204 をタップなどによって選択することにより、装置 110 に送金指示が与えられる。ユーザーは避難機能を有効又は無効にするための入力を行うことが可能であり、ユーザーが避難機能を ON にしている場合、図 2 に示すように、一例として「送金」ボタンの近傍に避難機能アイコン 205 を表示してもよい。OFF の場合、

当該アイコン205を非表示としたりグレーアウトしたりすることで、避難機能が有効ではなく無効であることを視覚的に表示してもよい。

[0029] 本実施形態では、装置110において、ユーザーによる暗号通貨の送金指示に応じて、指示された送金額を送金するための送金トランザクションTを生成することに加えて、指示された送金額を機器100が管理する秘密情報を用いて送金可能な金額から差し引いた残額の全部又は一部を送金するための避難トランザクションEを生成する。署名済み送金トランザクションT'はブロードキャストするものの、署名済み避難トランザクションE'はブロードキャストせずに、サーバ120で保管し、サーバ120は、別途正当な避難指示を受信した場合に署名済み避難トランザクションE'のブロードキャストを実行する。以下、さらに詳細する。

[0030] まず、装置110は、ユーザーから、送金先アドレス及び送金額を含む送金指示の入力を受け取る(S301)。装置110では、送金指示に応じて、指示された送金額を送金するための送金トランザクションデータTを生成する。加えて、装置110は、指示された送金額を機器100が管理する秘密情報を用いて送金可能な金額から差し引いた残額の全部又は一部を送金するための避難トランザクションデータEを生成する(S302)。ここで、送金トランザクションデータT及び避難トランザクションデータEは同時に生成してもよいし、いずれかを先に生成してもよい。図3では、装置110で生成を行うことで送金トランザクションデータTを取得するものとして説明するが、サーバ120に対する生成要求を送信し、生成された送金トランザクションデータTを受信することによって送金トランザクションデータTを取得することもでき、避難トランザクションデータEについても同様である。

[0031] 機器100で管理される秘密情報がシードSである場合につき、トランザクションデータの生成についてさらに説明する。シードSとは、そこから複数の秘密鍵を階層的に生成可能な情報であり、各秘密鍵に対応する公開鍵は、親秘密鍵である1階層目の秘密鍵に対応する公開鍵を親公開鍵S'として

、これに基づいて生成可能とすることができる。暗号通貨の送受金においては、各公開鍵に関連づけられたアドレスが用いられ、親公開鍵 S' が分かれば、シード S に関連づけられた複数のアドレスの特定を決定的に行うことができる。一例として、BIP32と呼ばれる規格を採用することが考えられる。ここで、公開鍵に関連づけられたアドレスは、公開鍵自体とすることが含まれる。親公開鍵 S' は、機器100と装置110との間の初期設定において装置110に記憶するものとする。機器100で管理するシード S を暗号化する場合には、シード S の暗号化に用いた暗号化キー P も装置110に記憶するものとする。装置110に記憶される親公開鍵 S' は、機器100が装置110と通信可能となるごとに装置110に記憶するようにしてもよく、暗号化キー P についても同様である。親公開鍵 S' ではなく、これに基づいて生成される各公開鍵を装置100で記憶するようにしてもよい。

[0032] 機器110は、親公開鍵 S' を用いて、シード S に関連づけられた複数のアドレスを出力とする複数のトランザクションデータのうちの当該送金額の送金に利用可能な1又は複数のUTXOを特定し、それらを送金元とするトランザクションデータ T を生成する。加えて、当該シード S に関連づけられた複数のアドレスを出力とする複数のトランザクションデータのうちのトランザクションデータ T に利用されていない1又は複数のUTXOを特定し、その全部又は一部を送金元とする避難トランザクションデータ E を生成する。避難トランザクションデータ E の送金先アドレスは、避難先アドレスとして登録しておくことができる。この点、後述する。

[0033] 機器100で管理される秘密情報が1又は複数の秘密鍵である場合、機器110は、当該1又は複数の秘密鍵に対応する1又は複数の公開鍵に関連づけられた1又は複数のアドレスの全部又は一部を送金元とするトランザクションデータ T を生成する。加えて、機器110は、トランザクションデータ T により送金される送金額を機器100が管理する1又は複数の秘密鍵を用いて送金可能な金額から差し引いた残額の全部又は一部を送金するための避難トランザクションデータ E を生成する。ここで、各公開鍵に関連づけられ

たアドレスは、公開鍵自体とすることが含まれる。各公開鍵は、初期設定として装置１１０に記憶しておくこともできるが、機器１００が装置１１０と通信可能となるごとに装置１１０に記憶するようにしてもよく、暗号化キーＰについても同様である。

[0034] 次に、装置１１０は、取得した送金トランザクションデータＴ及び避難トランザクションデータＥ又はこれらのハッシュ値を機器１００に対し、送信する（Ｓ３０３）。機器１００では、そこに記憶された秘密情報を用いて、送金トランザクションデータＴのハッシュ値及び避難トランザクションデータＥのハッシュ値に対する署名を行い、当該署名を装置１１０に送信する（Ｓ３０４）。

[0035] 次に、装置１１０は、送金トランザクションデータＴのハッシュ値に対する署名を付加した署名済み送金トランザクションデータＴ'を生成し、加えて、避難トランザクションデータＥのハッシュ値に対する署名を付加した署名済み避難トランザクションデータＥ'を生成する（Ｓ３０５）。

[0036] そして、装置１１０は、署名済み送金トランザクションデータＴ'をブロックチェーンネットワーク１２０に向けて送信する（Ｓ３０６）。これは「ブロードキャスト」と呼ばれることがある。この際、装置１１０は、直接ブロックチェーンネットワーク１２０のいずれかのノードに対して署名済み送金トランザクションデータＴ'を送信することができるが、サーバ１２０が提供するブロードキャストのための第１のＡＰＩを署名済み送金トランザクションデータＴ'を引数として呼び出すことによって、署名済み送金トランザクションデータＴ'をサーバ１２０を通じて送信することもできる。

[0037] 最後に、装置１１０は、署名済み避難トランザクションデータＥ'をサーバ１２０に向けて送信する（Ｓ３０７）。この際、装置１１０は、サーバ１２０が提供する避難のための第２のＡＰＩを署名済み避難トランザクションデータＥ'を引数として呼び出すことによって、署名済み避難トランザクションデータＥ'をサーバ１２０に送信することもできる。サーバ１２０では、署名済み避難トランザクションデータＥ'を別途避難実行指示を受信する

までブロードキャストせずに保管する。

[0038] サーバ120は、同一のユーザーから、新たな署名済み避難トランザクションデータE'を受信した場合、既に記憶している署名済み避難トランザクションデータE'があれば、古いものを破棄し、新たなもので更新することが好ましい。装置110が上記第2のAPIを呼び出して署名済み避難トランザクションデータE'をサーバ120に送信する場合には、サーバ120は、呼び出し元のアカウントに基づいて、ユーザーの同一性を判定可能である。

[0039] このように、本実施形態にかかる暗号通貨を避難するための方法においては、ユーザーが送金を行うための送金指示を行ったことに応じて、送金のための送金トランザクションデータTを取得し、それと同時に又はそれと関連づけて、残りの暗号通貨の全部又は一部の避難のための避難トランザクションデータEを取得する。そして、署名済み避難トランザクションデータE'をブロードキャストせずに別途避難の実行指示があるまでサーバ120で保管して、避難の準備をする。避難の実行指示によって、署名済み避難トランザクションデータE'がブロードキャストされ、ユーザーは、署名済み避難トランザクションデータE'の送金先アドレスから暗号通貨の移動が可能となる。したがって、この避難サービスを提供する事業者は、各ユーザーの秘密情報にアクセスすることなく、緊急時等、必要に応じて暗号通貨の避難を可能としており、各ユーザーに取引所の外で暗号通貨を自ら保管可能にしつつ、秘密情報の管理負担を大きく軽減する。

[0040] 加えて、本実施形態においては、ユーザーによる送金指示に応じて、署名済み避難トランザクションデータE'のサーバ120における保管を行い避難の準備をしていることから、ユーザーは暗号通貨の残額の避難について特別な注意を払う必要がなく、利便性が高い。

[0041] また、サーバ120は、仮想通貨取引所の外のサーバ、すなわち仮想通貨取引所を提供するためのサーバ以外のサーバとすることで、各ユーザーによる暗号通貨の取引所の外での保管を徹底することができる。

[0042] また、上述の説明では、機器１００において署名を行うものとして説明したが、装置１１０自体が送金に必要な秘密情報を安全性高く管理可能であれば、装置１１０に秘密情報を管理させて、装置１１０において署名を付与することも考えられる。換言すれば、トランザクションデータＴのハッシュ値又は避難トランザクションデータＥのハッシュ値に対する署名の取得は、機器１００からの受信により行う場合のほか、装置１１０における署名の実行により行う場合が考えられる。また、安全性高く管理可能であれば、秘密情報又はこれに対応する情報を機器１００又は装置１１０からコンピュータネットワークを介してアクセス可能な記憶装置又は記憶媒体に記憶しておき、署名に必要な際にアクセスするようにしてもよい。また、安全性高く管理可能であれば、秘密情報又はこれに対応する情報を機器１００又は装置１１０が読み取り可能な記憶装置又は記憶媒体に記憶しておき、署名に必要な際にアクセスするようにしてもよい。機器１００又は装置１１０が読み取り可能な記憶媒体には、USBメモリ、ＳＤカード等の他に紙媒体も含まれ、紙媒体の場合には二次元コードで秘密情報又はこれに対応する情報を表現して記録し、これを機器１００又は装置１１０の撮像素子によって撮影して読み取ることが考えられる。

[0043] なお、「××のみに基づいて」、「××のみに応じて」、「××のみの場合」というように「のみ」との記載がなければ、本明細書においては、付加的な情報も考慮し得ることが想定されていることに留意されたい。また、一例として、「ａの場合にｂする」という記載は、明示した場合を除き、「ａの場合に常にｂする」ことを必ずしも意味しないことに留意されたい。

[0044] また、念のため、なんらかの方法、プログラム、端末、装置、サーバ又はシステム（以下「方法等」）において、本明細書で記述された動作と異なる動作を行う側面があるとしても、本発明の各態様は、本明細書で記述された動作のいずれかと同一の動作を対象とするものであり、本明細書で記述された動作と異なる動作が存在することは、当該方法等を本発明の各態様の範囲外とするものではないことを付言する。

[0045] 避難先アドレスの指定の詳細

避難トランザクションデータEに含まれる避難先アドレスは、そのアドレス保有者の本人確認がなされていることが好ましい。具体的には、サーバ120により提供される避難サービスのユーザーがユーザー登録をしており、当該ユーザーと同一人物がアドレス保有者であることが確認されたアドレスを避難先アドレスとすることが考えられる。

[0046] 一例として、ユーザー登録しているユーザーと同一人物が仮想通貨取引所から与えられたアドレスを避難先アドレスとして許容することが考えられる。このため、避難先アドレスは、ユーザーが手入力不可として、仮想通貨取引所が提供するAPIを装置110又はサーバ120が呼び出して指定するようにするのが好ましい。装置110が当該APIを呼び出すためには、ユーザーが当該仮想通貨取引所のアカウント情報を用いて装置110にインストールされたアプリケーションが当該APIを呼び出し可能に設定することが必要である。API連携自体は、さまざまな手法を用いることが考えられる。

[0047] また、避難先アドレスは、機器100又は装置110にインストールされたアプリケーションが発行するアドレスとすることができる。ここで当該アドレスは、避難トランザクションデータEの入力を構成する1又は複数のUTXOの1又は複数のアドレスに関連づけられた第1のシードSとは異なる第2のシードS'を用いて生成したものとすることができる。こうすることで、第1のシードS又は第1のシードSを用いて生成された秘密鍵に不正のアクセスが生じたおそれがあっても、第1のシードSとは別個の第2のシードS'に関連づけられたアドレスに暗号通貨を移動させることができる。

[0048] 一例として、署名済み避難トランザクションデータE'をブロードキャストすると同時に、又はその前後に、サーバ120は、装置110にその旨を通知し、当該通知に応じて、装置110が機器100又は装置110にインストールされたアプリケーションに新たな第3のシードS''を生成させてもよい。移動された暗号通貨は、その後第2のシードS'に関連づけられた

1又は複数のアドレスの残高となり、第3のシードS' 'に関連づけられたアドレスが新たな避難先アドレスとなる。第3のシードS' 'の生成はこれ以外のさまざまなタイミングで行うことができる。いずれにしても、アプリケーション内でシードを切り替えることで、ユーザー負担を大きくすることなく、安全なシードに関連づけられた1又は複数のアドレスに暗号通貨を避難させることが可能となる。

[0049] 避難の実行指示の詳細

ユーザーは、サーバ120に保管した署名済み避難トランザクションデータE'をブロックチェーンネットワーク130にブロードキャストして暗号通貨を避難先アドレスに移したい場合、サーバ120に対し、避難の実行指示を与える。

[0050] 避難実行指示は、たとえば、装置110にインストールされたアプリケーションから送信することができるが、サーバ120が提供するウェブページにおいて、避難実行指示を送信するためのリンク生成要求を行い（図4A参照）、避難実行指示リンク（図4B参照）を受信してこれをタップ又はクリックすることで、避難実行指示をサーバ120に送信してもよい。ウェブページから避難実行指示を送信可能とすることには、装置110が紛失のおそれがあるスマートフォンなどの携帯端末である場合に、紛失が実際に生じても避難可能とする利点がある。この場合、避難先アドレスは、装置110にインストールされたアプリケーションが発行乃至生成するアドレスではなく、当該アプリケーションから独立したアドレスとするのが好ましい。

[0051] （第2の実施形態）

第1の実施形態においては、ユーザーによる暗号通貨の一部の送金指示の入力を装置110が受け取ったことに応じて、避難の準備を行っている。第2の実施形態においては、ユーザーが、サーバ120に保管されている署名済み避難トランザクションデータE'の更新を任意のタイミングを可能とする。たとえば、図5に示すように、コンピュータネットワークから遮断された機器100において送金に必要な秘密情報が管理されている暗号通貨の残

高表示画面500に更新ボタン501を表示し、ユーザーがこれをタップして更新指示、すなわち避難準備指示を装置110に与えられるようにしてもよい。ユーザーが避難させる金額を指定可能としてもよく、また、かかる指定を予め設定可能としてもよい。

[0052] また、必ずしもユーザーの操作ではなく、管理される秘密情報を用いて送金可能な金額に変化をもたらす処理を検知した際に、避難トランザクションEの取得を行うようにしてもよい。ユーザーによる送金指示又はそれに基づく送金トランザクションの取得等の当該秘密情報を用いて送金可能な送金元アドレスからの送金に関する処理のほか、当該秘密情報を用いて送金可能な送金元アドレスに対する入金に関する処理が検知対象として挙げられる。

[0053] (第3の実施形態)

第3の実施形態では、第1及び第2の実施形態で説明した避難サービスをユーザーが利用するためには、当該ユーザーは、サーバ120を用いて当該避難サービスを提供する事業者と利用契約を締結していることを必要とする。ユーザーは、サーバ120が提供するウェブサイト又は装置110にインストールしたアプリケーションから、ユーザー登録を行い、所要の利用料を支払う。当該利用料を月額費用とすることで、ユーザーは秘密情報をデータとして管理する労力から解放され管理負担が軽減されるとともに、費用に関しても管理負担が軽減される。さらに、ユーザーが用いる機器100の費用を月額利用料に含めた場合には、ユーザーの費用負担は一層軽減され、取引所に依拠しない暗号通貨の保管が大きく促進される。

[0054] (第4の実施形態)

第1から第3の実施形態においては、送金に必要な秘密情報が仮想通貨取引所の外で管理されていることを前提としたが、第1から第3の実施形態にて説明した避難トランザクションデータEによる避難は、仮想通貨取引所のためのサーバ上で送金に必要な秘密情報が管理されている場合にも適用することが考えられる。この場合、図1の装置110が仮想通貨取引所のためのサーバとなり、かかる変更に伴い矛盾しない範囲で第1から第3の実施形態

において説明したすべての態様が本実施形態においても同様に採用可能である。

符号の説明

[0055]	1 0 0	機器
	1 0 1	表示部
	1 0 2	入力部
	1 1 0	装置
	1 2 0	サーバ
	1 3 0	ブロックチェーンネットワーク
	2 0 0	入力画面
	2 0 1	送金先アドレス入力欄
	2 0 2	送金額入力欄
	2 0 3	メモ入力欄
	2 0 4	送金ボタン
	2 0 5	避難機能アイコン
	5 0 0	残高表示画面
	5 0 1	避難機能アイコン

請求の範囲

- [請求項1] 送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨を避難するための方法であって、装置が、
- ユーザーから前記暗号通貨の一部の送金指示の入力を受け取るステップと、
- 指示された送金額を送金するための送金トランザクションデータを取得するステップと、
- 前記送金トランザクションデータの送金額を前記暗号通貨の全額から引いた残額の全部又は一部を避難するための避難トランザクションデータを取得するステップと、
- 前記送金トランザクションデータのハッシュ値に対する前記秘密情報を用いた署名を取得するステップと、
- 前記避難トランザクションデータのハッシュ値に対する前記秘密情報を用いた署名を取得するステップと、
- 署名済み送金トランザクションデータをブロックチェーンネットワークに向けて送信するステップと、
- 署名済み避難トランザクションデータを前記署名済み避難トランザクションデータを保管するためのサーバに送信するステップとを含むことを特徴とする方法。
- [請求項2] 前記サーバに、前記署名済み避難トランザクションデータを前記ブロックチェーンネットワークに向けて送信させる避難の実行指示を送信するステップをさらに含むことを特徴とする請求項1に記載の方法。
- [請求項3] 前記サーバは、仮想通貨取引所を提供するためのサーバ以外のサーバであることを特徴とする請求項1又は2に記載の方法。
- [請求項4] 前記避難トランザクションデータは、避難先アドレスである送信先アドレスが、前記ユーザーの本人確認がなされているアドレスであることを特徴とする請求項1から3のいずれかに記載の方法。

- [請求項5] 前記避難トランザクションデータは、避難先アドレスである送信先アドレスが、前記装置にインストールされたアプリケーションが生成するアドレスであって、前記避難トランザクションデータの入力を構成する1又は複数のUTXOの1又は複数のアドレスに関連づけられた第1のシードとは異なる第2のシードを用いて生成されたものであることを特徴とする請求項1に記載の方法。
- [請求項6] 前記ユーザーから避難機能を有効にするための入力を受け取るステップをさらに含むことを特徴とする請求項1に記載の方法。
- [請求項7] 前記携帯端末が、前記秘密情報を記憶するインターネットから遮断された機器から、前記署名済み避難トランザクションデータのハッシュ値に対する署名を受信することを特徴とする請求項1から6のいずれかに記載の方法。
- [請求項8] 送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨を避難するための方法であって、装置が、
前記暗号通貨の全部又は一部を避難するための避難トランザクションデータを取得するステップと、
前記避難トランザクションデータのハッシュ値に対する前記秘密情報を用いた署名を取得するステップと、
署名済み避難トランザクションデータを前記署名済み避難トランザクションデータを保管するためのサーバに送信するステップとを含むことを特徴とする方法。
- [請求項9] 装置に、送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨を避難するための方法を実行させるためのプログラムであって、前記方法は、
前記暗号通貨の全部又は一部を避難するための避難トランザクションデータを取得するステップと、
前記避難トランザクションデータのハッシュ値に対する前記秘密情報を用いた署名を取得するステップと、

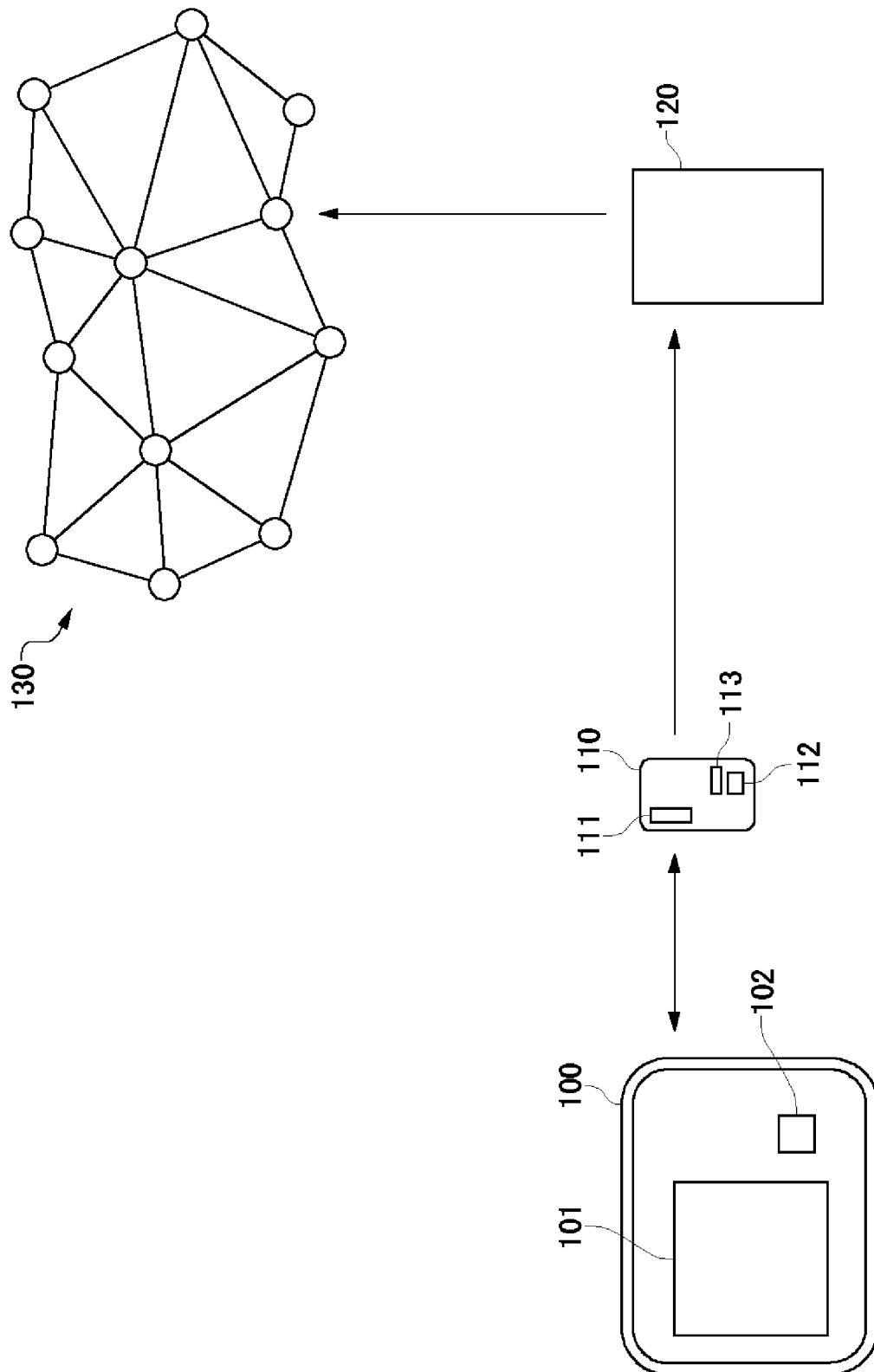
署名済み避難トランザクションデータを前記署名済み避難トランザクションデータを保管するためのサーバに送信するステップとを含むことを特徴とするプログラム。

[請求項10] 送金に必要な秘密情報が仮想通貨取引所の外で管理されている暗号通貨を避難するための装置であって、

前記暗号通貨の全部又は一部を避難するための避難トランザクションデータを取得し、

前記避難トランザクションデータのハッシュ値に対する前記秘密情報を用いた署名を取得して、署名済み避難トランザクションデータを前記署名済み避難トランザクションデータを保管するためのサーバに送信することを特徴とする装置。

[図1]



[図2]

200

取引履歴

ハードウェアウォレットから送金 ×

201 送金先 ☐

202 金 額 BTC

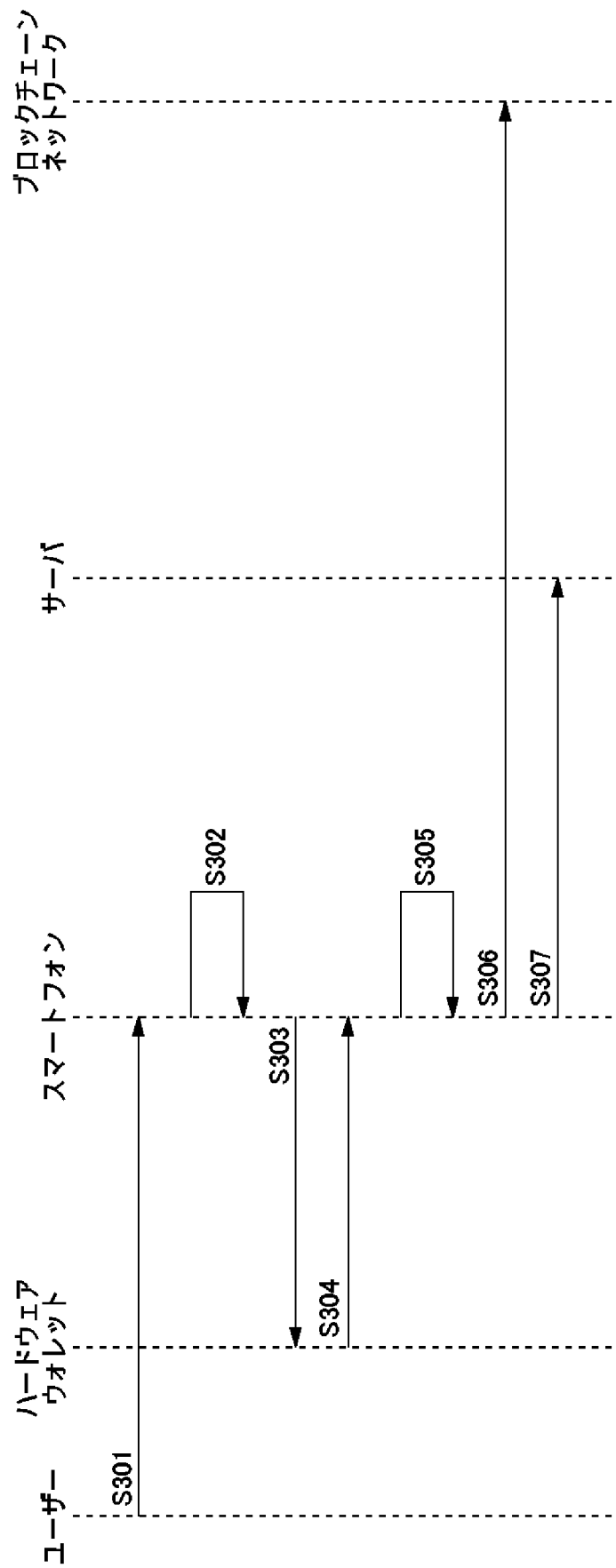
203 メ モ

204 送金する

205

The image shows a mobile application interface for managing cryptocurrency transactions. At the top, there is a header bar. Below it, a section titled '取引履歴' (Transaction History) contains three horizontal lines representing a list of transactions. A modal window titled 'ハードウェアウォレットから送金' (Send from Hardware Wallet) with a close button '×' is displayed. This modal contains three input fields: '送金先' (Recipient) with a radio button, '金 額' (Amount) with a 'BTC' unit selector, and 'メ モ' (Memo). At the bottom of the modal is a large button labeled '送金する' (Send) with an upward arrow icon.

[図3]



[図4A]

登録済みのメールアドレスを入力
してください

email@example.com

避難実行指示リンクを送信

[図4B]

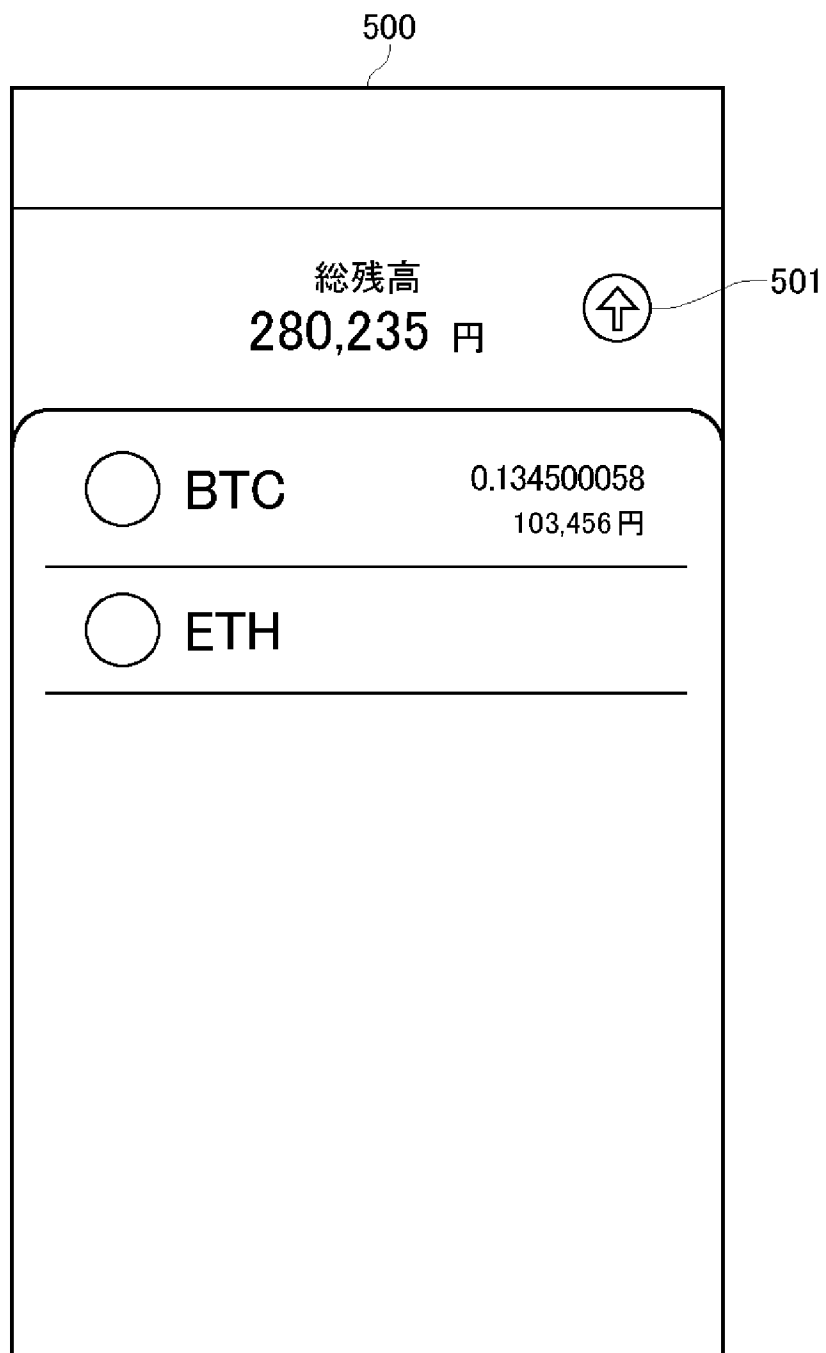
下記のリンクを5分以内に開くと、暗号通貨を
避難先に移動できます。

<https://self-rescue.xxxx.co.jp/a89fa79f>

登録済みの避難先

取引所A
1Po1oWkD2Lmo...

[図5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/006779

A. CLASSIFICATION OF SUBJECT MATTER

G09C 1/00 (2006.01) i; H04L 9/32 (2006.01) i; G06Q 20/38 (2012.01) i
 FI: G06Q20/38 310; H04L9/00 675B; G09C1/00 640D

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)

G09C1/00; H04L9/32; G06Q10/00-99/00

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.
A	WO 2017/201489 A1 (MOOG INC.) 23.11.2017 (2017-11-23) entire text, all drawings	1-10
A	加賀陽介、ほか 6 名、トランザクションの本人性を確認できる分散台帳技術の提案、情報処理学会論文誌[ONLINE], 16 January 2019 (accession date), vol. 60, no. 1, pp. 130-146, Internet <URL:https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_uri&item_id=193894&file_id=1&file_no=1>, entire text, all drawings, (KAGA, Yosuke et al., "Human Trusted Distributed Ledger Technology", Transactions of Information Processing Society of Japan [ONLINE])	1-10



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" 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
21 April 2020 (21.04.2020)

Date of mailing of the international search report
28 April 2020 (28.04.2020)

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.

PCT/JP2020/006779

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	JP 6526299 B1 (MERCARI, INC.) 05.06.2019 (2019-06-05) paragraphs [0001], [0015], [0018], [0024], [0058]-[0060], [0095]-[0098], [0101], [0102], fig. 8, 9	1-10
P, A	JP 2019-139542 A (NOMURA RESEARCH INSTITUTE, LTD.) 22.08.2019 (2019-08-22) entire text, all drawings	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/JP2020/006779

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2017/201489 A1	23 Nov. 2017	US 2018/0012311 A1 entire text, all drawings EP 3459029 A1 CA 3025064 A1 SG 11201810306X A KR 10-2019-0010628 A CN 109690589 A JP 2019-520638 A	
JP 6526299 B1	05 Jun. 2019	(Family: none)	
JP 2019-139542 A	22 Aug. 2019	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G09C 1/00(2006.01)i; H04L 9/32(2006.01)i; G06Q 20/38(2012.01)i FI: G06Q20/38 310; H04L9/00 675B; G09C1/00 640D		
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）） G09C1/00; H04L9/32; G06Q10/00-99/00 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
A	WO 2017/201489 A1 (MOOG INC.) 23.11.2017 (2017-11-23) 全文、全図	1-10
A	加賀陽介、ほか6名、トランザクションの本人性を確認できる分散台帳技術の提案、情報処理学会 論文誌 [ONLINE], 2019.01.16 (受入日), 第60巻, 第1号, p. 130-146, Internet<URL:https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_uri&item_id=193894&file_id=1&file_no=1> 全文、全図	1-10
P, X	JP 6526299 B1 (株式会社メルカリ) 05.06.2019 (2019-06-05) 第1, 15, 18, 24, 58-60, 95-98, 101, 102段落、図8, 9	1-10
P, A	JP 2019-139542 A (株式会社野村総合研究所) 22.08.2019 (2019-08-22) 全文、全図	1-10
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的な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 21.04.2020		国際調査報告の発送日 28.04.2020
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） 鈴木 和樹 5L 3252 電話番号 03-3581-1101 内線 3562

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2020/006779

引用文献			公表日	パテントファミリー文献	公表日
WO	2017/201489	A1	23.11.2017	US 2018/0012311 A1 全文, 全図	
				EP 3459029 A1	
				CA 3025064 A1	
				SG 11201810306X A	
				KR 10-2019-0010628 A	
				CN 109690589 A	
				JP 2019-520638 A	
JP	6526299	B1	05.06.2019	(ファミリーなし)	
JP	2019-139542	A	22.08.2019	(ファミリーなし)	