

明 細 書

発明の名称：

トランザクション委任方法、トランザクション委任システム、及びコンピュータプログラム

技術分野

[0001] 本出願は、2019年12月26日に出願された米国仮特許出願62/953734号の優先権の利益を主張し、参照によってその全体が組み込まれる。

[0002] 本発明は、ブロックチェーンにおけるトランザクション委任方法、トランザクション委任システム、及びコンピュータプログラムに関する。

背景技術

[0003] ブロックチェーンを利用したシステムでは、ユーザがブロックチェーンシステムを構成するノード又はスマートコントラクトへトランザクションを要求する場合、手数料トークン（以下、fee tokenともいう）による手数料を、トランザクションの対価として支払うことが必要である（特許文献1等）。

[0004] ブロックチェーンシステムで要求されるトランザクションは、アセット（暗号資産等）の移動を目的としたもののみならず、スマートコントラクトが実行するデータ保存又は演算を含む。

[0005] ブロックチェーンを利用したシステムでは、上述したような手数料トークン以外にも、システムの利用に際してユーティリティトークン（以下、utility tokenともいう）の支払いを要求するスマートコントラクトが存在する。

先行技術文献

特許文献

[0006] 特許文献1：特開2020-080061号公報

発明の概要

発明が解決しようとする課題

[0007] ブロックチェーン技術をベースとしたサービスの利用には、ユーザにとっては煩雑な手数料トークン及びユーティリティトークン等の管理が必要であり、ブロックチェーンシステムの広範囲への普及は爆発的とはなりにくい。

[0008] 本発明は、斯かる事情を鑑みてなされたものであり、ブロックチェーンシステムの普及を支援するトランザクション委任方法、トランザクション委任システム及びコンピュータプログラム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

[0009] 本開示の一実施形態のトランザクション委任方法は、ユーザが使用する第1装置から、ブロックチェーンシステムにおけるアカウントデータを記憶する第2装置が、前記ブロックチェーンシステムにおける前記ユーザの所望のトランザクションの実行を委任する委任データを、前記ブロックチェーンシステム外の通信によって受信し、前記第1装置から送信された委任データに基づき、前記所望のトランザクションを、前記ブロックチェーンシステムにおける前記ユーザのアカウントから実行する実行スマートコントラクトに実行させる委任トランザクションを作成し、前記アカウントデータに基づき、トランザクションの実行に要する手数料トークン又はユーティリティトークンの支払いを伴う前記委任トランザクションを、前記ブロックチェーンシステムへブロードキャストする。

発明の効果

[0010] 本開示によれば、サービスの提供を受けるユーザは、サービスのベースとなっているブロックチェーンシステムにおけるアカウント、及び、ブロックチェーンシステムで流通するトークンの運用を意識することなくサービスを楽しむことができる。

図面の簡単な説明

[0011] [図1]本開示のシステムの概要図である。

[図2]本開示のシステムにおけるトランザクションの委任処理手順の概要図である。

[図3]第1装置1の構成を示すブロック図である。

[図4]中継者の第2装置2の構成を示すブロック図である。

[図5]ブロックチェーンシステムにおけるノードの構成を示すブロック図である。

[図6]システムにおける処理の概要図である。

[図7]委任トランザクション作成処理手順の一例を示すシーケンス図である。

[図8]トランザクションの委任実行処理手順の一例を示すシーケンス図である。

[図9]実施例1におけるトランザクションの委任処理の一例を示すシーケンス図である。

[図10]実施例3におけるトランザクションの委任処理の一例を示すシーケンス図である。

[図11]実施例4におけるトランザクションの委任処理の一例を示すシーケンス図である。

[図12]実施例5におけるトランザクションの委任処理の一例を示すシーケンス図である。

[図13]実施例6におけるトランザクションの委任処理の一例を示すシーケンス図である。

発明を実施するための形態

[0012] 本開示をその実施の形態を示す図面を参照して具体的に説明する。

[0013] 本開示において「ブロックチェーンシステム」は、相互に通信接続が可能な複数のコンピュータ及び複数のコンピュータを接続するネットワークを含み、前記複数のコンピュータの分散処理によってブロックチェーンを作成するシステムを言う。ブロックチェーンには、要求されるトランザクションの内容が取り込まれる。

[0014] ブロックチェーンを利用したシステムでは、ユーザの第1装置が、ブロックチェーンシステムへトランザクションを要求する場合、そのブロックチェーン技術に応じた特定のトークン（fee token）による手数料を、対価として支払うことが必要である。

- [0015] 例えば、Bitcoin（登録商標）ベースのブロックチェーンシステムでユーザがアセットの移動（売買の登録）処理を要求する場合、トランザクションの入力と出力との間に差額が設けられ、その差額分のBTC単位の手数料がマイナーに対し支払われる。Ethereum（登録商標）ベースのブロックチェーンシステムでは、トランザクションの実行の際、指定されたガス費用にしたがって、トランザクションのブロックチェーンへの取り込みに要したガス量に相当するETH単位の手数料がマイナーに対して支払われる。BitcoinでもEthereumでも、手数料が少なく設定してあるトランザクションは、ブロックチェーンに取り込まれにくい。
- [0016] EOSベースのブロックチェーンシステムでは、トランザクションの要求主体が、トランザクションに要するストレージ容量と、演算（コンピューティング）リソースとを事前に確保しておく必要がある。具体的には、トランザクションを要求するユーザが、使用する装置を介し、ブロックチェーンシステムにおけるストレージ容量をEOSトークンで購入しておき、処理を実行するブロックチェーンアカウントに対してEOSトークンをステーク（預ける）しておくことが必要である。
- [0017] ブロックチェーンを利用したシステムを継続稼働するにあたり、このような手数料の支払いを求める仕組みは、インセンティブデザインやDOS攻撃耐性の向上の観点で重要である。ユーザは、サービスを利用するために、ブロックチェーンシステムのアカウントによって取引所を介して必要なトークン（手数料トークン又はユーティリティトークン）を購入し、送付するといったトークン管理を行なう必要がある。サービスによっては、特別なトークンを発行して配布するようなこともあるが、これらの特別なトークンがあっても、手数料トークン又はユーティリティトークンと取引することが必要な場合もある。これらの多様なトークンの管理は、専門性の高い知識を要求し、一般ユーザにはハードルが高い。ブロックチェーン技術に馴染みがないユーザがブロックチェーンを利用したサービスを利用しない状況は、ブロックチェーンのマスアダプションに対する大きな課題である。

- [0018] 本開示のトランザクション委任方法は、ユーザが使用する第1装置から、ブロックチェーンシステムにおけるアカウントデータを記憶する第2装置が、前記ブロックチェーンシステムにおける前記ユーザの所望のトランザクションの実行を委任する委任データを、前記ブロックチェーンシステム外の通信によって受信し、前記第1装置から送信された委任データに基づき、前記所望のトランザクションを、前記ブロックチェーンシステムにおける前記ユーザのアカウントから実行する実行スマートコントラクトに実行させる委任トランザクションを作成し、前記アカウントデータに基づき、トランザクションの実行に要する手数料トークン又はユーティリティトークンの支払いを伴う前記委任トランザクションを、前記ブロックチェーンシステムへブロードキャストする。
- [0019] 本開示のトランザクション委任方法では、実際にサービスの提供を受けるユーザが使用する装置（第1装置）が、サービスを実現するブロックチェーンシステムにおける手数料トークン又はユーティリティトークンを所有する中継者（relay）の装置（第2装置）へ、ユーザが実行することを希望するトランザクション（user transaction、以下user txともいう）を委任すること、即ちトランザクション委任（tx delegation）が可能である。
- [0020] これにより、ユーザが実行を希望するトランザクション（user tx）に対し必要な手数料トークン又はユーティリティトークンを管理する権限（アカウント）を有さない場合であっても、トランザクションの実行結果を得ることができる。ユーザは、サービスのベースとなっているブロックチェーンにおける手数料トークン若しくはユーティリティトークンの運用を意識する必要がない。権限を有している任意のトークンを委任手数料トークン（delegation fee token）として使用するか、又は委任手数料の支払いが不要である。
- [0021] トランザクション委任（tx delegation）は、ブロックチェーン外で実行され、形式は問われない。しかしながら、ユーザから中継者への委任には、ユーザが実行を希望するトランザクション（user tx）を、委任される中継者が実行するために十分なデータが含まれることが必要である。

- [0022] トランザクションの委任には、入れ子構造を有する特殊トランザクション (nested tx) を採用してもよい。第1装置から第2装置へ送信される特殊トランザクションは、ユーザが実行を希望するトランザクション (user tx) を内部に含む意味で入れ子構造の構成を有する。特殊トランザクションは、ユーザが実行を希望するトランザクション (user tx) を決定するために必要なデータ及び、トランザクションの実行主体となるブロックチェーンアカウント (以下、executer accountともいう) とを含む。特殊トランザクションは、複数のトランザクション (user tx) を含んでもよい。この場合、特殊トランザクションは、トランザクション (user tx) 毎に、必要なデータ及びブロックチェーンアカウントのデータを含む。
- [0023] ユーザの第1装置から中継者の第2装置へ送信される特殊トランザクションは、委任条件 (delegation condition、以下condともいう) と、署名 (signature、以下sigともいう) とを含んでもよい。
- [0024] 中継者の第2装置は、ユーザからのトランザクション委任に基づいて、ユーザが実行を希望するトランザクション (user tx) を入れ子構造で含む特殊トランザクションの形式で、委任のトランザクション (以下、委任トランザクション (delegation tx) という) を作成する。委任トランザクションは、ユーザから実行を希望されるトランザクション (user tx)、委任条件 (cond)、及び署名 (sig) を含んでよい。
- [0025] 中継者の第2装置は、中継ユーザが権限を有するアカウント (Relayer Account) に基づいて委任トランザクションをブロックチェーンシステムへ要求する。委任トランザクションは、ブロックチェーンシステムに所属するスマートコントラクトであるアカウント呼び出しコントラクト (Account Caller Contract) に対して実行される。中継者の第2装置は、後述するように、委任トランザクションの実行をアカウント呼び出しコントラクトのみならず、トランザクションの実行主体となるブロックチェーンアカウントの実行者アカウントコントラクト (Executor Account Contract) へ直接的に要求してもよい。このときのブロックチェーンシステムへのトランザクションの実行要

求に必要な手数料トークン又はユーティリティトークンのステーク等は、中継者のアカウントから実行される。

[0026] アカウント呼び出しコントラクトは、委任トランザクション (delegation tx) に基づき、ユーザのアカウントとして動作する実行者アカウントコントラクトに対してトランザクション (user tx) の実行をリクエストする。実行者アカウントコントラクトは、リクエストされたトランザクション (user tx) を実行すると共に、委任手数料トークンのユーザから中継者への支払いを実行する。

[0027] これにより、サービスの提供を受けるユーザは、サービスのベースとなっているブロックチェーンシステムにおける多様なトークンの運用を意識することなくサービスを享受することができる。

[0028] 図1は、本開示のシステム100の概要図である。システムは、ブロックチェーンシステム300外のユーザ (user) の第1装置1と、第1装置1からアクセスが可能な、中継者が管理する第2装置2とを含む。システム100は、ブロックチェーンシステム300内に、アカウント呼び出しコントラクト (Account Caller Contract) 301、及び、実行者アカウントコントラクト (Executor Account Contract) 302のインスタンスを含む。本開示において「ブロックチェーンシステム」は、相互に通信接続が可能な複数のコンピュータ及び複数のコンピュータを接続するネットワークを含み、前記複数のコンピュータの分散処理によってブロックチェーンを作成するシステムを言う。

[0029] 本開示のシステム100では、ユーザの第1装置1は、ブロックチェーンシステム300に対応する秘密鍵を記憶しているが、ブロックチェーンシステム300の手数料トークン又はユーティリティトークンが対応付けられたアカウントを記憶していなくてよい。ただし、第1装置1は、ブロックチェーンをベースとしたサービスの提供を受けるため、ブロックチェーンシステム300における処理の結果を取得することができる。例えば第1装置1は、ブロックチェーンシステム300から、処理結果をWebベースで取得で

きる。また第1装置1は、第2装置2との間でデータの送受信が可能である。

[0030] 第2装置2は、ブロックチェーンシステム300における手数料トークン及びユーティリティトークンの移動が可能なアカウント (relayer account) を持つ中継者によって管理される。第2装置2は、ユーザの第1装置1との間でデータの送受信が可能であり、中継者のアカウント (relayer account) に基づきブロックチェーンシステム300にてトランザクションを実行できる。つまり第2装置2は、手数料トークン又はユーティリティトークンの支払い (ステーク) が可能である。

[0031] 本開示のシステム100におけるブロックチェーンシステム300は、アカウントに対してスマートコントラクトをデプロイ (実行可能な状態とする) できる種類のブロックチェーン技術を用いる。以下の例では、ブロックチェーンシステム300はEthereumのブロックチェーン技術を用いるとして説明するが、これに限られない。ブロックチェーンシステム300はEOSベースであってもよい。

[0032] ブロックチェーンシステム300には、アカウント呼び出しコントラクト301、実行者アカウントコントラクト302のインスタンスが生成される。後述するように (実施例4, 6)、これらは同一のインスタンスであってもよい。ブロックチェーンシステム300は、複数のアプリケーションに対応する多様な複数のコントラクト303のインスタンスを含む。またブロックチェーンシステムは、委任手数料トークンを管理する委任手数料トークン管理コントラクト304が各々生成されている。

[0033] ブロックチェーンシステム300に存在する多様なアプリケーションに対応するスマートコントラクト303の内、ユーザが希望する処理を実行する対象コントラクト (Target Contract) 303に対し、その処理をリクエストするためには、手数料トークン又はユーティリティトークンを支払うための管理権限を有するアカウントによるトランザクション実行処理が必要である。しかしながら、ブロックチェーンシステム300における手数料トークン

又はユーティリティトークンを含む多様なトークンの取引には、ユーザにブロックチェーン技術に対する知識等が必要である。

[0034] 本開示のシステム100では、実際にサービスの提供を受けるユーザの装置（第1装置）1は、サービスを実現するブロックチェーンシステム300の手数料トークン又はユーティリティトークンを所有し移転できる中継者の装置（第2装置）2へ、ユーザが実行を希望するトランザクション（user tx）を委任する。委任により、ユーザがトークンを管理できなくとも、ブロックチェーンシステム300におけるトランザクションの実行結果の享受が可能となる。

[0035] 図2は、本開示のシステム100におけるトランザクションの委任処理手順の概要図である。

[0036] （1）サービスにおける処理を希望するユーザ（第1装置1）は、ブロックチェーンで実行したいトランザクション（user tx）の実行主体となるブロックチェーンアカウント（実行者アカウント：executer account）を特定するデータを決定、又は作成する。

[0037] （1）の段階でユーザ（第1装置1）は、ブロックチェーンシステム300で実行者アカウントコントラクトによって実行されるトランザクション（user tx）を構成するためのデータを決定、又は作成する。

[0038] サービスが例えばゲームである場合、ユーザは、ブロックチェーンシステム300の分散アプリケーションによって実現されるゲームでのアイテムの生成又は譲渡のトランザクションの実行を希望することが考えられる（勿論、サービスはゲームに限られない）。この場合、ユーザが実行を希望するトランザクション（user tx）を実行するためのブロックチェーンアカウント（executer account）は例えば、ユーザのブロックチェーンシステムにおけるアカウントである。また、希望のトランザクション（user tx）が、アイテムの生成又は譲渡である場合、トランザクション（user tx）を構成するためのデータは、アイテムを特定するデータ、譲渡先を特定するデータ等を含むとよい。

- [0039] (1) の段階でユーザ（第1装置1）は、ユーザのブロックチェーンアカウント（executer account）と、実行を希望するトランザクション（user tx）とをユーザ自身が指定したことを、検証できる方法（例えば電子署名）によってこの検証に必要なデータ（sig）を取得する。
- [0040] (2) ユーザの第1装置1は、ユーザのブロックチェーンアカウント（executer account）と、実行を希望するトランザクション（user tx）と、検証に必要なデータとを、ブロックチェーンシステム300外で中継者の第2装置2へ送信する。これにより、中継者にブロックチェーンアカウント（executer account）と、希望するトランザクション（user tx）とが伝わる。
- [0041] (3) 中継者の第2装置2は、ユーザの第1装置1から受信したデータに基づいて、ユーザに対応するブロックチェーンアカウント（executer account）と、希望するトランザクション（user tx）とを埋め込んだ委任トランザクション（delegation tx）を作成する。中継者の第2装置2は、中継者のアカウント、又は、中継者が使用できる他のアカウント（任意のアカウント）の権限によって、委任トランザクションをブロックチェーンシステム300へブロードキャストする。
- [0042] (4) ブロードキャストの伝達によって、ブロックチェーンシステム300内のユーザに対応するブロックチェーンアカウント（executer account）によるユーザが実行を希望するトランザクション（user tx）の実行が実現される。このトランザクション（user tx）の実行に必要な手数料トークン又はユーティリティトークンは、中継者が委任トランザクションをブロードキャストする際に指定したアカウント（中継者のアカウント、又は他のアカウント）から支払われる。
- [0043] このようにして、実際にサービスの提供を受けるユーザが使用する装置（第1装置）1が、ブロックチェーンシステム300における手数料トークン又はユーティリティトークンを所有する中継者の装置（第2装置）2へ、ユーザが実行を希望するトランザクション（user tx）を委任する。委任により、ユーザが手数料トークン又はユーティリティトークンを管理する権限を有

していなくとも、ブロックチェーンシステム300におけるトランザクションの実行が可能となる。

[0044] これにより、サービスの提供を受けるユーザは、サービスのベースとなっているブロックチェーンシステム300の手数料トークン又はユーティリティトークンの運用を意識することなく、トランザクションを実行させることができる。

[0045] このような処理を実現するためのシステムの具体的な構成について説明する。

[0046] 図3は、第1装置1の構成を示すブロック図である。第1装置1は、例えばスマートフォン、又はタブレット端末である。第1装置1は、処理部10、記憶部11、通信部12、表示部13、及び操作部14を備える。

[0047] 処理部10は、CPU (Central Processing Unit)、GPU (Graphics Processing Unit) 等のプロセッサと、メモリ等を用いる。なお処理部10は、プロセッサ、メモリ、更には記憶部11及び通信部12を集積した1つのハードウェア (SoC: System On a Chip) として構成されていてもよい。

[0048] 記憶部11はフラッシュメモリを用い、第1プログラム1Pを始めとする処理部10が参照するプログラム、データが記憶される。第1プログラム1Pは、コンピュータを、本開示のシステム100の第1装置1として機能させるためのプログラムである。記憶部11には、図3に示すように、ブロックチェーンシステム300におけるユーザの秘密鍵を記憶していてもよい。秘密鍵は、処理部10のメモリ又は記憶部11に書き換え不可に記憶されているとよい (ウォレットのチップ化)。

[0049] 記憶部11に記憶されている第1プログラム1Pは、コンピュータから読み取り可能な記憶媒体8に記憶されていた第1プログラム8Pを処理部10が読み出して記憶部11に記憶したものであってもよい。

[0050] 通信部12は、第2装置2及び他の通信装置との通信接続を実現する通信モジュールである。通信部12は、ネットワークカード、無線通信デバイス又はキャリア通信用モジュールを用いる。

- [0051] 表示部 1 3 は液晶パネル又は有機 E L ディスプレイ等のディスプレイ装置を用いる。操作部 1 4 は、ユーザの操作を受け付けるインタフェースであり、物理ボタン、ディスプレイ内蔵のタッチパネルデバイス、スピーカ及びマイクロフォン等を用いる。操作部 1 4 は、物理ボタン又はタッチパネルにて表示部 1 3 で表示している画面上で操作を受け付けてもよいし、マイクロフォンにて入力音声から操作内容を認識し、スピーカで出力する音声との対話形式で操作を受け付けてもよい。
- [0052] 図 4 は、中継者の第 2 装置 2 の構成を示すブロック図である。第 2 装置 2 も第 1 装置 1 同様、スマートフォン又はタブレット端末等の通信端末機器である。第 2 装置 2 は、第 2 コンピュータであってもよいし、デスクトップ型又はラップトップ型パーソナルコンピュータであってもよい。第 2 装置 2 は、処理部 2 0、記憶部 2 1、及び通信部 2 2 を備える。
- [0053] 処理部 2 0 は、C P U、G P U 等のプロセッサと、メモリ等を用いる。処理部 2 0 は、記憶部 2 1 に記憶されている第 2 プログラム 2 P に基づき、第 1 装置 1 から送信されたデータを取得し、委任トランザクションの作成、トランザクションの実行を実現する。記憶部 2 1 は、ハードディスク又はフラッシュメモリを用い、第 2 プログラム 2 P を始めとする処理部 2 0 が参照するプログラム、データを記憶する。
- [0054] 記憶部 2 1 に記憶されている第 2 プログラム 2 P は、コンピュータから読み取り可能な記憶媒体 9 に記憶されていた第 2 プログラム 9 P を処理部 1 0 が読み出して記憶部 1 1 に記憶したものであってもよい。
- [0055] 通信部 2 2 は、第 1 装置 1 又はブロックチェーンシステム 3 0 0 との通信接続を実現する通信モジュールである。通信部 2 2 は、ネットワークカード、無線通信デバイス又はキャリア通信用モジュールを用いる。
- [0056] 図 5 は、ブロックチェーンシステム 3 0 0 におけるノード 3 0 の構成を示すブロック図である。ノード 3 0 は、サーバコンピュータであってもよいし、デスクトップ型又はラップトップ型パーソナルコンピュータであってもよいし、スマートフォン等の通信端末機器であってもよい。ノード 3 0 は、処

理部 31、記憶部 32 及び通信部 33 を備える。またノード 30 は、少なくとも処理部 31 及び通信部 33 を備える装置であれば、処理部 31 の一部によってノードの一部又は全部を構成することができる。

[0057] 処理部 31 は、CPU、GPU 等のプロセッサと、メモリ等を用いる。処理部 31 は、プロセッサ、メモリ、更には記憶部 32 及び通信部 33 を集積した 1 つのハードウェアとして構成されていてもよい。処理部 31 のメモリには、ノード 3 夫々独自に所有する秘密鍵が記憶されているとよい。そして処理部 31 は、記憶部 32 に記憶されているノードプログラムに基づいた各処理を実行し、汎用コンピュータをブロックチェーンシステム 300 におけるノードとして機能させる。

[0058] 記憶部 32 は、ハードディスク又はフラッシュメモリを用い、ノードプログラムを始めとする処理部 31 が参照するプログラム、データを記憶する。記憶部 32 は、ブロックチェーンを記憶する。ノードプログラムには、後述するスマートコントラクト（トランザクション実行に対する所定の演算処理を実行する処理部 31）として機能させるためのプログラムが含まれる。上述の秘密鍵は記憶部 32 に記憶されてもよい。記憶部 32 は、秘密鍵に基づく公開鍵及びアドレスを記憶してもよい。

[0059] 通信部 33 は、ノード 30 の相互通信を実現する通信モジュールである。通信部 33 は、ネットワークカード、光通信用デバイス、又は無線通信デバイス等を用いる。

[0060] 図 6 は、システム 100 における処理の概要図である。ユーザの第 1 装置 1 は、トランザクションの委任を目的として、ユーザが実行を希望するトランザクション（user tx）を作成するために必要なデータ及び、トランザクションの実行主体となるブロックチェーンアカウント（executer account）とを含む中継者宛てのデータを作成する（図 2 中の（1）に対応）。図 6 に示す例では、このユーザのトランザクション（user tx）と、ユーザに対応するブロックチェーンアカウント（executer account）とを含み、且つ、トランザクション条件（cond）及び検証方法（sig）とが作成され、中継者の第 2 装

置 2 へ送信される（図 2 中の（2）に対応）。

- [0061] 中継者の第 2 装置 2 は、第 1 装置 1 から送信されたデータの内容を元に、委任トランザクション（delegation tx）を作成する（図 2 中の（3）に対応）。委任トランザクションは、ユーザが実行を希望するトランザクション（user tx）、委任条件（cond）、及び署名（sig）を入れ子構造で含む特殊トランザクション（nested tx）である。
- [0062] 第 2 装置 2 は、ブロックチェーンシステム 300 に対し、トランザクションを実行できる手数料トークン又はユーティリティトークンを所有している。第 2 装置 2 は、中継者が権限を有するアカウント（relay account）に基づいて委任トランザクションを実行する（図 2 中の（3）に対応）。委任トランザクションは、ブロックチェーン内のアカウント呼び出しコントラクト 301 に対して実行される。
- [0063] アカウント呼び出しコントラクト 301 は、委任トランザクション（delegation tx）に基づき、ユーザのアカウントとして動作する実行者アカウントコントラクト 302 に対してトランザクション（user tx）の実行をリクエストする。実行者アカウントコントラクト 302 は、リクエストされたトランザクション（user tx）を対象コントラクト 303 で実行する。実行者アカウントコントラクト 302 は、リクエストされたトランザクション（user tx）を実行すると共に、委任手数料トークン管理コントラクト 304 に対し、委任手数料の中継者への支払（移転）を含むトランザクションを実行する。委任手数料は、手数料トークン又はユーティリティトークンと異なる。
- [0064] 図 7 は、委任トランザクション作成処理手順の一例を示すシーケンス図である。図 7 のシーケンス図が示す処理手順は、図 2 又は図 6 における（2）までの処理手順の詳細に対応する。
- [0065] 第 1 装置 1 の処理部 10 は、記憶部 11 に記憶されている第 1 プログラム 1P に基づき、ユーザが実行を希望するトランザクション（user tx）の内容、委任条件（cond）の初期値を作成する（ステップ S101）。トランザクション（user tx）の内容は、トランザクションの対象コントラクト 303 の

アドレス、対象コントラクト303における対象関数(target function)の識別子、及び対象関数の引数データを含む。トランザクションの委任条件は、ユーザの秘密鍵に対応するアドレス、実行者アカウントコントラクト302のアドレスを決定するために必要なデータを含む。委任条件は更に、委任手数料トークン管理コントラクト304のアドレス、委任手数料(トークン)の支払先のアドレス、及び手数料の決定に必要なデータを含む。

[0066] 処理部10は、作成したトランザクション(user tx)の内容及び委任条件(cond)の初期値を表示部13に表示する(ステップS102)。ステップS102で表示されるトランザクションの内容は、アドレス、識別子及び引数データを、それらをテキストで出力したものであってもよいし、コントラクトの名称、識別するアイコン等によって出力したものであってもよい。表示される委任条件も、テキストで出力したものであってもよいし、アイコンで出力したものであってもよい。

[0067] 処理部10は、ユーザによるトランザクション(user tx)の内容及び委任条件(cond)の編集を受け付ける(ステップS103)。変更がない場合にはステップS103の処理はスキップされる。

[0068] 処理部10は、実行が希望されるトランザクション(user tx)の内容及び委任条件(cond)の確定を受け付ける(ステップS104)。

[0069] 処理部10は、確定されたトランザクション(user tx)の内容及び委任条件(cond)のデータに対し、ユーザの秘密鍵に基づく電子署名を生成する(ステップS105)。秘密鍵は、第1装置1の記憶部11に安全に記憶されていてもよいし、ユーザからの入力を受け付けたものであってもよい。

[0070] 処理部10は、確定されたトランザクション(user tx)の内容、委任条件(cond)及びステップS105で取得した電子署名を中継者の第2装置2へ送信する(ステップS106)。トランザクション(user tx)の内容は、トランザクションの対象コントラクト303のアドレス、対象関数(target function)の識別子、及び対象関数の引数データを含む。

[0071] 第2装置2の処理部20は、トランザクション(user tx)の内容、委任条

件 (cond) を電子署名付きで受信する (ステップ S 2 0 1)。ステップ S 2 0 1 において処理部 2 0 は、送信された内容に基づいて、引き受けることができる委任であるか否かを判断し、引き受けられない委任である場合には、ユーザの第 1 装置へ返答するようにしてもよい。

[0072] 処理部 2 0 は、受信したトランザクション (user tx) の内容、委任条件 (cond) 及び電子署名を埋め込んだ委任トランザクション (delegation tx) を作成する (ステップ S 2 0 2)。ステップ S 2 0 2 で作成される委任トランザクション (delegation tx) は、入れ子構造を有する特殊トランザクション (nested tx) である。

[0073] 処理部 2 0 は、ステップ S 2 0 2 で作成した委任トランザクションに対し、第 2 装置 2 を管理する中継者に対応付けられているブロックチェーンシステム 3 0 0 におけるブロックチェーンアカウント (relayer account) の秘密鍵で電子署名を生成する (ステップ S 2 0 3)。

[0074] 処理部 2 0 は、ステップ S 2 0 2 で作成した委任トランザクション (delegation tx) に、ステップ S 2 0 3 で生成した電子署名を埋め込み (ステップ S 2 0 4)、委任トランザクション (delegation tx) の作成処理が完了する。

[0075] ステップ S 2 0 2 で作成される委任トランザクションは、委任トランザクションの対象であるアカウント呼び出しコントラクトのアドレス及び呼び出し関数 (call function) の識別子を含む。委任トランザクションには、呼び出し関数の引数として実行したいユーザのトランザクション (user tx) の内容を含む。このトランザクションの内容は、対象コントラクトのアドレスと、そのコントラクトにおける対象の関数 (target function) の識別子と、関数 (target function) に入力するデータとである。委任条件は、ユーザの秘密鍵に対応するアドレスと、実行アカウントコントラクトのアドレスの決定に必要なデータとを含む。実行アカウントコントラクトのアドレスの決定に必要なデータは、アドレスそのもの、又は、仮想アカウントコントラクト (virtual account contract) を利用する場合の任意の値若しくは文字列 (いわ

ゆるsalt)である。委任条件は更に、委任手数料に関する条件を含む。委任手数料は、手数料トークン又はユーティリティトークンと異なる。委任手数料に関する条件は、委任手数料として支払うトークンを管理する委任手数料トークン管理コントラクト304のアドレスを含む。委任手数料に関する条件は、委任手数料の支払先、即ち中継者が受け取るためのアドレスと、委任手数料の決定に必要なデータを含む。委任手数料の決定に必要なデータは例えば、委任手数料として支払うトークン(delegation fee token)と手数料トークンとのレート、ユーティリティトークンとのレートである。

[0076] 委任トランザクション(delegation tx)に含まれるべき委任手数料に関する条件が指定されない場合、又は、無指定に相当する条件が設定されていると判断される場合であっても、ユーザが実行を希望するトランザクション(user tx)の実行に必要な手数料トークン、又はユーティリティトークンは、中継者のアカウントに基づいて支払われる。ユーザは、委任手数料を支払わない場合がある。また、委任手数料として支払うトークン(delegation fee token)として指定できるのは、ユーザが実行したいと希望するトランザクションの対象コントラクト303と同一のブロックチェーンシステム300に存在するトークン、即ち流通可能なトークンである。

[0077] 図8は、トランザクションの委任実行処理手順の一例を示すシーケンス図である。図8のシーケンス図が示す処理手順は、図2又は図6における(3)から(4)までの処理手順を含む。

[0078] 中継者の第2装置2は、作成した委任トランザクション(delegation tx)をブロードキャストする(ステップS205)。

[0079] ステップS205による委任トランザクションがブロードキャストされると、ブロックチェーンシステム300のノード30によって、委任トランザクションはブロックチェーンに取り込まれる。ブロックチェーンに取り込まれた委任トランザクションを基に、委任トランザクションに含まれているアドレスのアカウント呼び出しコントラクト301の呼び出し関数が実行され、以下の処理が進行する。以下の処理は、署名の正当性の検証(S302)

で失敗しない限り、アトミックに、分割できないものとして実行される。

- [0080] アカウント呼び出しコントラクト301のインスタンス（以下、単にアカウント呼び出しコントラクトという）は、呼び出し関数の実行により、委任トランザクションに含まれる実行者アカウントコントラクト302のアドレスの決定に必要なデータに基づいてアドレスを決定する（ステップS301）。
- [0081] アカウント呼び出しコントラクト301は、委任トランザクションに含まれる、ユーザが実行を希望するトランザクション（user tx）の内容及び委任条件に対する電子署名の正当性を検証する（ステップS302）。
- [0082] ステップS302の検証にて、署名が正当であると成功した場合、アカウント呼び出しコントラクト301は、次の処理を実行する。ステップS302の検証にて、署名が正当でないと判断された場合、アカウント呼び出しコントラクト301はそのまま処理を終了する。
- [0083] アカウント呼び出しコントラクト301は、ステップS301で決定したアドレスの実行者アカウントコントラクト302に対して、ユーザが実行を希望するトランザクションに基づき、対象コントラクト303における対象関数（target function）の実行を指示する（ステップS303）。ステップS303においてアカウント呼び出しコントラクトは、ユーザが実行を希望するトランザクションの対象コントラクト303のアドレス、対象関数（target function）の識別子及び対象関数に入力するデータを、実行者アカウントコントラクトへ渡す。
- [0084] 実行者アカウントコントラクト302は、渡されたアドレス及び識別子に基づき、対象コントラクト303の対象関数に、渡されたデータを引数として入力してこれを実行する（ステップS401）。
- [0085] これにより、ユーザが実行を希望するトランザクションの対象コントラクト303で、対象関数の実行によって規定された処理が実行される（ステップS501）。規定された処理の実行により、ユーザが実行を希望するトランザクション（アセットの移動、データ保存、又はコンピューティング）の

結果が得られる。

- [0086] アカウント呼び出しコントラクト301は、委任トランザクションに含まれていた委任条件中の、委任手数料の決定に必要なデータに基づいて、ユーザが支払うべき委任手数料 (delegation fee token) の量を決定する (ステップS304)。
- [0087] アカウント呼び出しコントラクト301は、決定した量の委任手数料の支払いを、実行者アカウントコントラクト302へ指示する (ステップS305)。ステップS305においてアカウント呼び出しコントラクト301は、指示と共に、委任手数料トークン管理コントラクト304のアドレス及び委任手数料の支払先のアドレスを指定する。
- [0088] 実行者アカウントコントラクト302は、指定された委任手数料トークン管理コントラクト304に対し、指定された支払先のアドレスへの委任手数料の支払いを指示する (ステップS402)。
- [0089] ステップS402の指示により、委任手数料トークン管理コントラクト304は、指定された支払先のアドレスに対する委任手数料の支払い処理を実行する (ステップS601)。委任手数料の量は、ゼロの場合がある。これにより、委任トランザクションの実行処理を終了する。
- [0090] 図7及び図8のシーケンス図に示した処理により、ユーザがブロックチェーンシステム300における手数料トークン又はユーティリティトークンを移動する権限を有したアカウントを所有していなくても、ブロックチェーンシステム300における対象コントラクト303での処理の実行結果を享受できる。
- [0091] 図8のシーケンス図に示した処理は、あるコントラクト302の関数を呼び出すとその関数の呼び出しによって他の関数が呼び出されていく、というアトミックな繋がりのある処理であり、署名の検証以外は、各コントラクト301, 302, 303, 304での判断はなく、一連の処理として実行される。これは、委任トランザクション (delegation tx) は、ユーザが希望するトランザクション (user tx) を入れ子構造に含む特殊トランザクション (

nested tx) の態様で実現される。

[0092] 上述の説明では、アカウント呼び出しコントラクト301と、実行者アカウントコントラクト302とは別のインスタンスであるとして説明した。しかしながら、これらのコントラクト301, 302は同一のコントラクトであってもよい。また、委任手数料のユーザからの徴収方法は、委任手数料トークンで徴収する方法と、委任手数料を徴収しないという方法の2つがある。以下、これらのバリエーションに基づき、複数の実施例を説明する。

[0093] アカウント呼び出しコントラクト301と、実行者アカウントコントラクト302とが別のインスタンスとして存在する場合、実行者アカウントコントラクト302は仮想アカウントコントラクト(virtual account contract)であるか否かのバリエーションが考えられる。仮想アカウントコントラクトは、実際にユーザが実行を希望するトランザクション(user tx)の処理、呼び出し関数が実行されるまでは実体がない特殊なコントラクトである。

[0094] 仮想アカウントコントラクトを利用するメリットは、第1に、仮想アカウントコントラクトは、実体が存在しない場合であってもトークンを保有することができる。つまり、実体化(activation)前にはユーザに対して手数料が発生しない。ブロックチェーンシステム300における一般的なコントラクトは、トークンを保有するコントラクトは先に存在している必要があるため、そのデプロイの手数料が必要になる。また、実体化に関するコストも小さい。仮想アカウントコントラクトのインスタンスは、非常に軽量、即ち、プログラムのデータ量が少ないので、デプロイの手数料が小さい。トランザクションの委任(tx delegation)の一連の処理の中でデプロイを実行することにより、デプロイの手数料を中継者が肩代わりすることが可能である。

[0095] 仮想アカウントコントラクトを利用するメリットは、第2に、資産の安全性が高いことである。実体化前の仮想アカウントコントラクトは、実体化されていないわけであるから、攻撃を受ける可能性が極めて低い。仮想アカウントコントラクトの保有者の公開鍵をブロックチェーンに保存する必要があったとしても、ハッシュ化することで隠蔽が可能であるから、保有者に対す

る攻撃は実質不可能である。この性質は、仮想アカウントコントラクト単体で利用される場合であっても同様である。

[0096] アカウント呼び出しコントラクト301と実行者アカウントコントラクト302とが同一であるか否かと、別とする場合に仮想アカウントコントラクトを利用するか否かとの3通りが存在する。委任手数料についても、徴収する方法と徴収せずに中継者が肩代わりする方法との2通りが存在する。したがって、トランザクション委任の実行について6つ(3×2)の実施例を挙げて、以下に説明する。ブロックチェーンシステム300、ユーザの第1装置1及び中継者の第2装置2のハードウェア構成、及び基本処理は同一であるから、上述した構成と共通の符号を付して詳細な処理手順の説明を実行する。

[0097] [実施例1]

実施例1では、アカウント呼び出しコントラクト301と実行者アカウントコントラクト302とが別のインスタンスであって、実行者アカウントコントラクトは仮想アカウントコントラクトであり、且つ、委任手数料(delegation fee token)を任意のトークンで徴収する。ここで任意のトークンとは、ユーザがブロックチェーンシステム300のブロックチェーンアカウントで所有するトークンであり、手数料トークン又はユーティリティトークンではない。

[0098] 実施例1では、ユーザの第1装置1及び中継者の第2装置2との間では、図7のシーケンス図で示した委任トランザクションの作成処理を実行し、以下に示すトランザクションの委任処理が実行される。図9は、実施例1におけるトランザクションの委任処理の一例を示すシーケンス図である。図9のシーケンス図に示す処理手順の内、図8のシーケンス図に示した処理手順については、同一のステップ番号を付した詳細な説明を省略する。

[0099] アカウント呼び出しコントラクト301は、取り込まれた委任トランザクションを基に、ユーザが実行を希望するトランザクションの電子署名の正当性を検証し(S302)、検証に成功すると、ステップS302で決定した

アドレスの実行者アカウントコントラクト 302 をデプロイする（ステップ S312）。

[0100] アカウント呼び出しコントラクト 301 は、デプロイした実行者アカウントコントラクト 302 に対して、対象コントラクト 303 における対象関数（target function）の実行を指示する（S303）。ステップ S304 以降の処理は、図 8 のシーケンス図を参照した処理と同様である。

[0101] なお、図 9 のシーケンス図に示した処理は、実行者アカウントコントラクト 302 を呼び出す初回のみ実行され、2 回目以降は、図 8 のシーケンス図に示した処理が実行される。

[0102] 上述したように、仮想アカウントコントラクトを使用するので、最初に呼び出して（activation）実行者アカウントコントラクト 302 をデプロイするまではデプロイの手数料の支払いが不要である。

[0103] [実施例 2]

実施例 2 では、アカウント呼び出しコントラクト 301 と実行者アカウントコントラクト 302 とが別のインスタンスであって、実行者アカウントコントラクト 302 は仮想アカウントコントラクトでなく、且つ、委任手数料を任意のトークンで徴収する。

[0104] 実施例 2 における各コントラクトによる処理内容は、図 7 及び 8 のシーケンス図に示した処理手順と同様であるから図示を省略する。

[0105] 実施例 2 では、ステップ S402 の実行者アカウントコントラクト 302 による委任手数料トークン管理コントラクト 304 への委任手数料の支払いにより、ゼロでない委任手数料の中継者への支払い処理が実行される。

[0106] [実施例 3]

実施例 3 では、アカウント呼び出しコントラクト 301 と実行者アカウントコントラクト 302 とが同一のインスタンスであって、それは仮想アカウントコントラクトではなく、且つ、委任手数料を任意のトークンで徴収する。

[0107] 実施例 3 では、アカウント呼び出しコントラクト 301 と実行者アカウン

トコントラクト 302 とが同一のインスタンスである。ユーザの第 1 装置 1 及び中継者の第 2 装置 2 の間では、図 7 のシーケンス図で示した委任トランザクションの作成処理を実行するが、その際、委任条件中の実行者アカウントコントラクト 302 のアドレスの決定に必要なデータは不要である。

[0108] 図 10 は、実施例 3 におけるトランザクションの委任処理の一例を示すシーケンス図である。図 10 のシーケンス図で示す処理手順の内、図 8 のシーケンス図に示した処理手順と共通する処理については同一のステップ番号を付して詳細な説明を省略する。

[0109] 実施例 3 では、アカウント呼び出しコントラクト 301 と実行者アカウントコントラクト 302 とが同一である。したがって、ブロードキャストされた委任トランザクション (delegation tx) に対し、実行者アカウントコントラクト 302 のアドレスを決定するステップ S301 の処理は省略される。

[0110] 実施例 3 では、委任トランザクションに含まれているアドレスに基づき、実行者アカウントコントラクト 302 (アカウント呼び出しコントラクト 301) は、呼び出し関数に実行により、ユーザが実行を希望するトランザクション (user tx) の内容及び委任条件に対する電子署名の正当性の検証を実行する (S302)。

[0111] ステップ S302 の検証にて、署名が正当であると成功した場合、実行者アカウントコントラクト 302 は、以下の処理を実行する。実行者アカウントコントラクト 302 は、ユーザが実行を希望するトランザクションに含まれる対象コントラクト 303 のアドレス及び対象関数 (target function) の識別子に基づき、対象コントラクト 303 の対象関数に、入力データを引数として入力してこれを実行する (ステップ S333)。

[0112] これにより、ユーザが実行を希望するトランザクションの対象コントラクト 303 では、対象関数の実行によって規定された処理が実行される (S501)。規定された処理の実行により、ユーザが実行を希望するトランザクション (アセットの移動、データ保存、又はコンピューティング) の結果が得られる。

[0113] 実行者アカウントコントラクト302は、ユーザが支払うべき委任手数料トークンの量を決定する(S304)。実行者アカウントコントラクト302は、ステップS304で決定した量の支払先のアドレスへの委任手数料の支払いを、委任トランザクションに含まれるアドレスに基づいて委任手数料トークン管理コントラクト304へ指示する(ステップS335)。実行者アカウントコントラクト302は、委任トランザクションの実行処理を終了する。

[0114] ステップS335の指示により、委任手数料トークン管理コントラクト304は、指定された支払先(中継者)のアドレスに対する委任手数料の支払い処理を実行する。

[0115] [実施例4]

実施例4では、アカウント呼び出しコントラクト301と実行者アカウントコントラクト302とが別のインスタンスであって、実行者アカウントコントラクト302は仮想アカウントコントラクトであり、且つ、委任手数料は徴収しない。この場合、ユーザはブロックチェーンシステム300におけるアカウントさえ所有していなくてもよい。

[0116] 実施例4では、ユーザの第1装置1及び中継者の第2装置2との間では、図7のシーケンス図で示した委任トランザクションの作成処理を実行するが、委任手数料を徴収しない。したがって、作成される委任トランザクション(delegation tx)では、委任条件に、委任手数料管理コントラクト(delegation fee token contract)のアドレス、委任手数料の支払先のアドレス、及び、委任手数料の決定に必要なデータは不要である。

[0117] 図11は、実施例4におけるトランザクションの委任処理の一例を示すシーケンス図である。図11のシーケンス図で示す処理手順の内、図8のシーケンス図に示した処理手順と共通する手順については同一のステップ番号を付して詳細な説明を省略する。

[0118] アカウント呼び出しコントラクト301は、取り込まれた委任トランザクションを基に、ユーザが実行を希望するトランザクションの電子署名の正当

性を検証し（S 3 0 2）、検証に成功すると、ステップS 3 0 2で決定したアドレスの実行者アカウントコントラクト3 0 2をデプロイする（ステップS 3 4 2）。

[0119] アカウント呼び出しコントラクト3 0 1は、デプロイした実行者アカウントコントラクト3 0 2に対して、対象コントラクト3 0 3における対象関数（target function）の実行を指示する（S 3 0 3）。

[0120] 実行者アカウントコントラクト3 0 2は、渡されたアドレス及び識別子に基づき、対象のコントラクトの対象関数に、渡されたデータを引数として入力してこれを実行し（S 4 0 1）、処理が終了する。図8のシーケンス図に示した処理手順におけるステップS 3 0 4以降の処理は実行されない。

[0121] ステップS 4 0 1の処理により、ユーザが実行を希望するトランザクションの対象コントラクト3 0 3では、対象関数の実行によって規定された処理が実行される（S 5 0 1）。規定された処理の実行により、ユーザが実行を希望するトランザクション（アセットの移動、データ保存、又はコンピューティング）の結果が得られる。

[0122] [実施例5]

実施例5では、アカウント呼び出しコントラクト3 0 1と実行者アカウントコントラクト3 0 2とが別のインスタンスであって、実行者アカウントコントラクト3 0 2は仮想アカウントコントラクトでなく、且つ、委任手数料は徴収しない。

[0123] 実施例5では、ユーザの第1装置1及び中継者の第2装置2との間では、図7のシーケンス図で示した委任トランザクションの作成処理を実行するが、委任手数料を徴収しない。したがって、作成される委任トランザクション（delegation tx）では、委任条件に、委任手数料トークン管理コントラクト3 0 4のアドレス、委任手数料の支払先のアドレス、及び、委任手数料の決定に必要なデータは不要である。

[0124] 図12は、実施例5におけるトランザクションの委任処理の一例を示すシーケンス図である。図12のシーケンス図で示す処理手順の内、図8のシー

ケンス図に示した処理手順と共通する手順については同一のステップ番号を付して詳細な説明を省略する。

[0125] アカウント呼び出しコントラクト301は、取り込まれた委任トランザクションを基に、実行者アカウントコントラクト302のアドレスを決定する(S301)。アカウント呼び出しコントラクト301は、トランザクション(user tx)の電子署名の正当性を検証する(S302)。

[0126] アカウント呼び出しコントラクト301は、ステップS301で決定したアドレスの実行者アカウントコントラクト302に対して、対象コントラクト303における対象関数(target function)の実行を指示する(S303)。

[0127] 指示を受けた実行者アカウントコントラクト302は、渡されたアドレス及び識別子に基づき、対象コントラクト303の対象関数に、渡されたデータを引数として入力してこれを実行し(S401)、処理が終了する。図8のシーケンス図に示した処理手順におけるステップS304以降の処理は実行されない。

[0128] [実施例6]

実施例6では、アカウント呼び出しコントラクト301と実行者アカウントコントラクト302とが同一のインスタンスであって、それは仮想アカウントコントラクトではなく、且つ、委任手数料は徴収しない。

[0129] 実施例6では、ユーザの第1装置1及び中継者の第2装置2との間では、図7のシーケンス図で示した委任トランザクションの作成処理を実行するが、アカウント呼び出しコントラクト301と実行者アカウントコントラクト302とが同一コントラクトであり、委任手数料を徴収しない。したがって、作成される委任トランザクション(delegation tx)では、委任条件に、実行者アカウントコントラクト302のアドレスの決定に必要なデータは含まれない。委任条件に、委任手数料トークン管理コントラクト304のアドレス、委任手数料の支払先(中継者)のアドレス、及び、委任手数料の決定に必要なデータも不要である。実施例6では、委任条件は、ユーザの秘密鍵に

対応するアドレスを含めば足りる。

- [0130] 図13は、実施例6におけるトランザクションの委任処理の一例を示すシーケンス図である。図13のシーケンス図で示す処理手順の内、図8のシーケンス図に示した処理手順と共通する処理については同一のステップ番号を付して詳細な説明を省略する。
- [0131] 実施例6では、アカウント呼び出しコントラクト301と実行者アカウントコントラクト302とが同一である。したがって、ブロードキャストされた委任トランザクション (delegation tx) に対し、実行者アカウントコントラクト302のアドレスを決定するステップS301の処理は省略される。
- [0132] 実施例6では、委任トランザクションに含まれているアドレスに基づき、実行者アカウントコントラクト302 (アカウント呼び出しコントラクト301) が、呼び出し関数に実行により、ユーザが実行を希望するトランザクション (user tx) の内容及び委任条件に対する電子署名の正当性の検証を実行する (S302)。
- [0133] ステップS302の検証にて、署名が正当であると成功した場合、アカウント呼び出しコントラクト301でもある実行者アカウントコントラクト302は、以下の処理を実行する。実行者アカウントコントラクト302は、ユーザが実行を希望するトランザクションに含まれる対象コントラクト303のアドレス及び対象関数 (target function) の識別子に基づき、対象コントラクト303の対象関数に、入力データを引数として入力してこれを実行する (ステップS363)。委任処理は終了する。図8のシーケンス図に示した処理手順におけるステップS304以降の処理は実行されない。
- [0134] 上述したアカウント呼び出しコントラクト301及び実行者アカウントコントラクト302が、ブロックチェーンシステム300のあらゆるブロックチェーンアカウントからのトランザクション実行指示を許容する構成は非現実的である。したがって、実行者アカウントコントラクト302は、アカウント呼び出しコントラクト301からの指示のみを受け付けるように設定し、アカウント呼び出しコントラクト301は、自身の呼び出し関数の実行指

示権限を有するアカウント（中継者）をホワイトリスト型で記憶しておくともよい。実施例3及び実施例6のように、アカウント呼び出しコントラクト301と実行者アカウントコントラクト302とが同一のインスタンスである場合、アカウント呼び出しコントラクト301（実行者アカウントコントラクト302）は、実行指示権限を有するアカウント（中継者）をホワイトリスト型で記憶しておき、権限を有していないアカウントからの委任トランザクションを拒否できるようにするとよい。

- [0135] 図8－図13のシーケンス図で示したトランザクションの委任処理では、委任内容の正当性の検証を、ユーザが実行を希望するトランザクション（user tx）の内容及び委任条件に対する電子署名によって検証する例を挙げた。しかしながら、電子署名に限られない。事前にユーザが実行を希望するトランザクションが何らかの認証を通過するように設定し、ステップS301の検証処理を省略してもよい。また、ステップS301の検証処理に代替して、ブロックチェーンシステム300内に他の検証用コントラクトをデプロイさせておき、この検証用コントラクトで検証させてから処理が進むようにしてもよい。更にステップS301の検証処理に代替して、図7の委任トランザクションの作成処理手順において、中継者の第2装置2が、第1装置1から受信した電子署名を、ブロックチェーンシステム300の外で検証してもよい。
- [0136] 委任手数料の徴収方法についても、他のバリエーションが許容される。図8及び図9のシーケンス図では、実行者アカウントコントラクト302が委任手数料トークン管理コントラクト304に対し、支払い処理を実行した。しかしながら、ユーザから許諾を受けた他のコントラクト、例えばアカウント呼び出しコントラクト301が委任トランザクションの委任処理の中で引き出し処理を実行するような形式で行なってもよい。また、委任処理の中では委任手数料は徴収されず、一定期間分の委任トランザクションの実行（tx delegation）に対してまとめて前払い・後払いするような形式で実現されてもよい。ユーザをログインさせ、中央集権的にユーザのウォレット（秘密鍵

）を管理するサービスでは、委任手数料を徴収するに際して、法定通貨での前払い・後払いに対応することも可能となる。後払いで徴収を行なう場合には、支払が実行されないリスクを考慮して、ユーザが保有する資産を担保とするようにしてもよい。ここでいう資産は、ブロックチェーンシステム 300 で流通可能な資産（トークン）であってもよい。ブロックチェーンシステム 300 外に存在する様々な資産（現金、証券、不動産等）であってもよい。ブロックチェーンシステム 300 で流通可能な資産である場合、後払い、担保に関する契約自体をスマートコントラクト化することで、仲介者、契約放棄のリスクなしで執行が可能となり、大きなメリットになる。

[0137] 上述したシステム 100 により、ユーザは、ユーティリティトークン又は手数料トークンを保有していなくてもブロックチェーンシステム 300 でのトランザクションの実行が可能になる。これにより、ユーザの負担は大きく軽減される。中継者は、任意のトークン（委任手数料トークン）で委任手数料を徴収することが可能である。本開示では、委任手数料トークン管理コントラクト 304 は、トランザクションの委任対応のための改変を行なわなくても上述の処理を実行できるため、既にブロックチェーンシステム 300 に存在する多数のトークンを利用することが可能である。委任手数料トークンは、例えばEthereumではERC20、ERC721、又はERC1155等の標準規格に準拠した既存のトークンでの徴収が可能である。ERC1155の場合、複数種類のトークンでの徴収も可能である。つまり、トランザクションの委任手数料をユーザから徴収するための手続きを柔軟に調整することによって、ユーザの負担を緩和することが可能である。勿論、完全に肩代わりすることも可能であり、完全に肩代わりする場合、負担は相当軽減される。

[0138] ユーザから中継者（委任される者）へ安全に委任を実施するために電子署名を用いて委任内容の正当性の検証を行なう場合であっても、ユーザは始めに 1 度だけその実行を希望するトランザクション（user tx）に対して電子署名を生成する処理をしておけばよい。これにより、そのトランザクション（user tx）の委任に関し、後の処理の中で再度承認処理を求められることはな

く、通常のトランザクションの実行と変わらない。したがって、本開示のトランザクションの委任によってユーザの作業負担が増加することはない。

[0139] 本開示のシステム 100 により、中継者は、ユーザの秘密情報（ユーザの第 1 装置 1 が記憶している秘密鍵等）を知らないまま、ユーザのブロックチェーンアカウント（実行者アカウントコントラクト）から指定されたトランザクション（user tx）を実行することが可能である。ユーザは、実行者アカウントコントラクト 302 の権限を中継者に使用させつつも、自身の秘密情報を保護することが可能である。ユーザは他者（中継者）にユーザの権限を使用させたい場合、他者にユーザの秘密情報（ユーザの第 1 装置 1 が記憶する秘密鍵等）を知らせる必要があるが、秘密情報を秘匿したまま、他者への委任が可能になる。

[0140] 中継者が、ユーザが実行を希望するトランザクション（user tx）の内容を改変できないようにすることが可能である。例えばユーザが、ユーザが実行を希望するトランザクションの内容に対して電子署名を付加し、スマートコントラクトでその検証を行なってもよい。ユーザが希望するトランザクション（user tx）の実行と委任手数料の徴収をアトミックに実行することも可能である。委任される中継者の不正によってユーザが不利益を被る可能性を低減させることもできる。詐欺防止に大きく貢献できる。委任された委任トランザクション（delegation tx）が実行されないという事態が発生した場合、他の中継者を經由して対応することも可能である。ユーザが実行を希望するトランザクション（user tx）と委任手数料の徴収とをアトミックに実行するためには、ユーザはブロックチェーンシステム 300 にて何等かの委任手数料として使用できるトークン（delegation fee token）を保有する必要がある。委任手数料として使用できるトークンに、ステーブルコインを適用することによって、委任手数料として使用できるトークンの価格低下リスクからユーザを保護することも可能である。特に法定通貨担保型のステーブルコインは、投機性のない価格の安定したトークンであるから、ブロックチェーンシステム 300 で流通する多様なトークンに馴染みのないユーザであっても

扱いやすい保有リスクの小さい資産であり、利用価値が高い。

[0141] 委任される中継者は、例えば中央省庁から正式な手続きを経て認可を受けている企業であってもよい。この企業が顧客の暗号資産（秘密鍵）の管理に責任を負い、ユーザが希望するトランザクション（user tx）を実行することも可能である。なお、その企業管理下にあるユーザの顧客アカウントに対して予め手数料トークン又はユーティリティトークンを分配しておき、これをもとにユーザが希望するトランザクションを実行しても実現は可能である。しかしながら手数料トークン又はユーティリティトークンのユーザへの分配を実行するトランザクション処理にも当然手数料トークンが必要であり、トランザクションの承認にも一定時間を要する。この分配を全顧客に対して継続的に行なうことは金銭的及び時間的なコストが高い。本開示のシステムにより、委任トランザクション（delegation tx）を実行するアカウント（中継者、例えば金融企業）に手数料トークン又はユーティリティトークンを集約させておけば、分配処理は不要であるから、金銭的及び時間的コストを削減できる。中継者となる企業にとってもメリットが大きい。

[0142] 委任される中継者は、上述したような認可を受けた企業に限らない。中小企業、個人であっても中継者になり得る。本開示のシステムを適用することにより、中継者は、ユーザの負担を安全に肩代わりすることが可能になる。これまでは顧客（ユーザ）の資産管理に携わることができなかったために、顧客に作業負担及び手数料負担をさせるしかなかった負担を、中継者が担うことによって、顧客の負担を軽減することができる。完全に手数料を肩代わりすることができない場合、顧客からはブロックチェーンシステム300において顧客が扱える暗号資産、又は、ブロックチェーンシステム300外の委任手数料を徴収することによって柔軟に負担を分配することも可能である。委任手数料の支払いに、ブロックチェーンシステム300内のアプリによって実現されユーザが享受するサービスでの何らかのインセンティブを設定してもよい。これにより、顧客（ユーザ）同士で委任手数料を支払い合ってトランザクション委任を実行するといったスキームを構築することも可能で

ある。

[0143] 本開示のシステム１００（手法）の適用対象は例えば、Dapps（分散アプリケーション）運営者、又はウォレットアプリ開発者になる。例えば、ゲームDappsは、ブロックチェーンシステム３００に馴染みのない一般層のユーザを、そのゲームのユーザとして取り込める見込みがあるはずであるにも関わらず、手数料トークンの支払のための手続き及び管理が煩雑である。本開示のシステム１００を適用することにより、手数料トークンの管理ができないユーザであっても、そのゲームのユーザになる敷居を低くすることができる。また、ゲームのみならず、運営者がマーケティングキャンペーンの一環として発行した特定のトークンを無償でユーザに分配した場合、これらの特定のトークンを、ユーザがブロックチェーンシステム３００で取引しようとした場合、手数料トークンが必要になる取引所がある。このような場合、本開示のシステム１００の適用により、ユーザ及び運営者にとってサービス利用が促進され得る。

[0144] 本開示のシステム１００（手法）は、Dapps運営者、ウォレットアプリの開発者のみならずブロックチェーンシステム３００の関連サービスを提供するクラウドベンダー又はS I（System Integration）ベンダー等のB 2 B課金に適用されてもよい。ブロックチェーンシステム３００の普及フェーズでは、Dappsのユーザ同様に、各ベンダーの顧客もほとんどはブロックチェーンシステム３００に馴染みがなく、多数のトークンを使い分けるまでには至らないことがほとんどである。ブロックチェーンシステム３００を活用して構築されたサービスの運用のために、手数料トークン又はユーティリティトークンの支払をベンダーが肩代わりするスキームの必要性は高まることが予想される。このようなエンタープライズ領域におけるユースケースでも、法定通貨担保型のステーブルコインを利用することが非常に有効となる。

[0145] 本開示のシステム１００（手法）を利用したトランザクション委任（tx delegation）を、「手数料トークン又はユーティリティトークンと、ユーザから徴収し得る委任手数料トークンとの間の取引」として解釈すれば、その取

引市場が生まれる。取引のマッチングなどまで加味すると普及には課題が残るものの、オープンなトランザクションプールを形成するだけで取引市場の要件を満たす。取引市場が機能し、中継者となることがビジネスとして成立することも可能になる。

[0146] 上述のように開示された実施の形態は全ての点で例示であって、制限的なものではない。本発明の範囲は、請求の範囲によって示され、請求の範囲と均等の意味及び範囲内での全ての変更が含まれる。

符号の説明

- [0147]
- 1 第1装置
 - 10 処理部
 - 11 記憶部
 - 13 表示部
 - 14 操作部
 - 1P 第1プログラム
 - 2 第2装置
 - 20 処理部
 - 21 記憶部
 - 2P 第2プログラム
 - 300 ブロックチェーンシステム
 - 30 ノード
 - 301 アカウント呼び出しコントラクト
 - 302 実行者アカウントコントラクト
 - 303 対象コントラクト
 - 304 委任手数料管理コントラクト