

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2021-189431

(P2021-189431A)

(43) 公開日 令和3年12月13日(2021.12.13)

(51) Int.Cl.	F 1	テーマコード (参考)
G09C 1/00 (2006.01)	G09C 1/00	620Z
G06F 21/62 (2013.01)	G06F 21/62	318

審査請求 有 請求項の数 23 O L 外国語出願 (全 36 頁)

(21) 出願番号 特願2021-26236 (P2021-26236)
 (22) 出願日 令和3年2月22日 (2021.2.22)
 (31) 優先権主張番号 202010474245.3
 (32) 優先日 令和2年5月29日 (2020.5.29)
 (33) 優先権主張国・地域又は機関
 中国 (CN)

(71) 出願人 513224353
 バイドゥ オンライン ネットワーク テ
 クノロジー (ベイジン) カンパニー
 リミテッド
 中華人民共和国、100085 ベイジン
 ハイディエン ディストリクト、シャン
 ディ 10ティーエイチ ストリート、バ
 イドゥ キャンパス、ナンバー 10、3
 /フロア
 (74) 代理人 110001195
 特許業務法人深見特許事務所

最終頁に続く

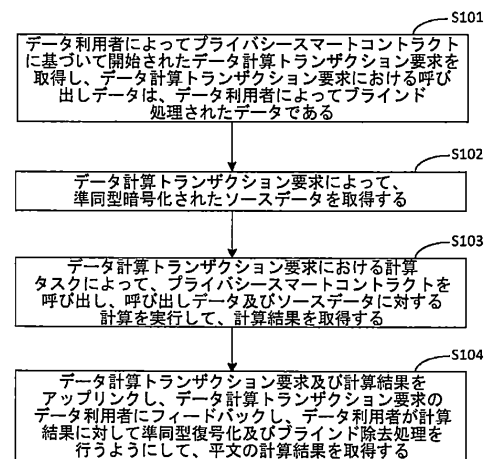
(54) 【発明の名称】 ブロックチェーンのプライバシーデータ処理方法、装置、デバイス及び記憶媒体

(57) 【要約】 (修正有)

【課題】ブロックチェーンのプライバシーデータ処理方法、装置、デバイス及び記憶媒体を提供する。

【解決手段】データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得するステップを含む。要求における呼び出しデータは、データ利用者によってブラインド処理されたデータである。方法はさらに、要求によって準同型暗号化されたソースデータを取得するステップと、要求における計算タスクによって、プライバシースマートコントラクトを呼び出し、呼び出しデータ及びソースデータに対する計算を実行して、計算結果を取得するステップと、要求及び計算結果をアップリンクして、要求のデータ利用者にフィードバックし、データ利用者が計算結果に対して準同型復号化及びブラインド除去処理を行うようにして、平文の計算結果を取得するステップと、を含む。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

ブロックチェーンノードによって実行される、ブロックチェーンのプライバシーデータ処理方法であって、

データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得するステップであって、前記データ計算トランザクション要求における呼び出しデータは、前記データ利用者によってブラインド処理されたデータである、ステップと、

前記データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得するステップと、

前記データ計算トランザクション要求における計算タスクによって、前記プライバシースマートコントラクトを呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行して、計算結果を取得するステップと、

前記データ計算トランザクション要求及び計算結果をアップリンクして、前記データ計算トランザクション要求のデータ利用者にフィードバックすることにより、前記データ利用者が前記計算結果に対して準同型復号化及びブラインド除去処理を行って、平文の計算結果を取得するステップとを含む、方法。

10

【請求項 2】

データ供給者によって前記プライバシースマートコントラクトに基づいて開始されたデータ公開トランザクション要求を取得するステップであって、前記データ公開トランザクション要求におけるソースデータは準同型暗号化されたデータである、ステップと、

前記プライバシースマートコントラクトを呼び出し前記データ公開トランザクション要求を実行して、前記ソースデータをアップリンク公開するステップとをさらに含む、請求項 1 に記載の方法。

20

【請求項 3】

前記ブラインド処理は呼び出しデータにランダム値を追加することを含み、前記ブラインド除去処理は計算結果から前記ランダム値を除去することを含む、請求項 1 に記載の方法。

【請求項 4】

データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得した後に、さらに、

前記データ計算トランザクション要求において指定されたソースデータに基づいて、前記データ利用者が前記ソースデータを使用する権限に対して認証操作を行うステップを含む、請求項 1 に記載の方法。

30

【請求項 5】

前記データ計算トランザクション要求において指定されたソースデータに基づいて、前記データ利用者が前記ソースデータを使用する権限に対して認証操作を行うステップは、

前記データ計算トランザクション要求において指定されたソースデータに基づいて、認証センターに前記データ利用者が前記ソースデータを使用する認証要求を送信して、データ供給者により設けられた権限によって前記認証要求を処理するように前記認証センターに要求するステップと、

前記認証センターからフィードバックされた認証結果を取得するステップとを含む、請求項 4 に記載の方法。

40

【請求項 6】

前記プライバシースマートコントラクトを呼び出し前記呼び出しデータ及び前記ソースデータに対する計算を実行する過程において、さらに、

前記プライバシースマートコントラクトを呼び出して仮想マシン上で実行するとともに、前記プライバシースマートコントラクトによって前記仮想マシンの組み込み関数を呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行するステップを含む、請求項 1 に記載の方法。

50

【請求項 7】

ブロックチェーンクライアントによって実行される、ブロックチェーンのプライバシーデータ処理方法であって、

ブロックチェーンで公開された準同型暗号化データから計算タスクに必要なソースデータを決定するステップと、

前記計算タスクの呼び出しデータをブラインド処理するステップと、

ブロックチェーンノードによって設けられたプライバシースマートコントラクトに基づいて、前記呼び出しデータ及びソースデータに対して前記計算タスクを実行するデータ計算トランザクション要求を開始することにより、前記プライバシースマートコントラクトを呼び出し前記計算タスクを実行して計算結果を取得するように、前記ブロックチェーンノードに要求するステップと、

アップリンクされた計算結果を取得するステップと、

前記ソースデータのデータ供給者に準同型暗号化公開鍵を提供するように要求するステップと、

前記準同型暗号化公開鍵を用いて前記計算結果に対して準同型復号化を行うとともに、前記計算結果に対してブラインド除去処理を行って、平文の計算結果を取得するステップとを含む、方法。

【請求項 8】

前記ブラインド処理は呼び出しデータにランダム値を追加することを含み、前記ブラインド除去処理は計算結果から前記ランダム値を除去することを含む、請求項 7 に記載の方法。

【請求項 9】

準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵と準同型暗号化公開鍵とを含む非対称準同型暗号化鍵を生成するステップと、

前記準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵を用いて、提供されるソースデータを準同型暗号化するステップと、

前記プライバシースマートコントラクトに基づいて、前記ソースデータをアップリンクするデータ公開トランザクション要求を開始するステップとをさらに含む、請求項 7 に記載の方法。

【請求項 10】

前記ソースデータをアップリンクするデータ公開トランザクション要求を開始するステップの後に、さらに、

データ利用者の前記ソースデータの使用に対する認証を行うために、前記ソースデータの使用権限を認証センターに設けるステップを含む、請求項 9 に記載の方法。

【請求項 11】

ブロックチェーンノードに設けられる、ブロックチェーンのプライバシーデータ処理装置であって、

データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得するためのトランザクション要求取得モジュールであって、前記データ計算トランザクション要求における呼び出しデータは、前記データ利用者によってブラインド処理されたデータである、トランザクション要求取得モジュールと、

前記データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得するためのソースデータ取得モジュールと、

前記データ計算トランザクション要求における計算タスクによって、前記プライバシースマートコントラクトを呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行して、計算結果を取得するための計算タスク処理モジュールと、

前記データ計算トランザクション要求及び計算結果をアップリンクして、前記データ計算トランザクション要求のデータ利用者にフィードバックすることにより、前記データ利用者が前記計算結果に対して準同型復号化及びブラインド除去処理を行って、平文の計算結果を取得するためのアップリンク処理モジュールとを備える、装置。

10

20

30

40

50

【請求項 1 2】

前記トランザクション要求取得モジュールは、さらに、データ供給者によって前記プライバシースマートコントラクトに基づいて開始されたデータ公開トランザクション要求を取得するように構成され、前記データ公開トランザクション要求におけるソースデータは準同型暗号化されたデータであり、

前記アップリンク処理モジュールは、さらに、前記プライバシースマートコントラクトを呼び出し前記データ公開トランザクション要求を実行して、前記ソースデータをアップリンク公開するように構成される、請求項 1 1 に記載の装置。

【請求項 1 3】

前記ブラインド処理は呼び出しデータにランダム値を追加することを含み、前記ブラインド除去処理は計算結果から前記ランダム値を除去することを含む、請求項 1 1 に記載の装置。

【請求項 1 4】

前記データ計算トランザクション要求において指定されたソースデータに基づいて、前記データ利用者が前記ソースデータを使用する権限に対して認証操作を行うための認証処理モジュールをさらに備える、請求項 1 1 に記載の装置。

【請求項 1 5】

前記認証処理モジュールは、

前記データ計算トランザクション要求において指定されたソースデータに基づいて、認証センターに前記データ利用者が前記ソースデータを使用する認証要求を送信して、データ供給者により設けられた権限によって前記認証要求を処理するように前記認証センターに要求するための認証要求送信ユニットと、

前記認証センターからフィードバックされた認証結果を取得するための認証結果取得ユニットとを含む、請求項 1 4 に記載の装置。

【請求項 1 6】

前記計算タスク処理モジュールは、

前記プライバシースマートコントラクトを呼び出して仮想マシン上で実行するとともに、前記プライバシースマートコントラクトによって前記仮想マシンの組み込み関数を呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行するように構成される、請求項 1 1 に記載の装置。

【請求項 1 7】

ブロックチェーンクライアントに設けられる、ブロックチェーンのプライバシーデータ処理装置であって、

ブロックチェーンで公開された準同型暗号化データから計算タスクに必要なソースデータを決定するためのソースデータ決定モジュールと、

前記計算タスクの呼び出しデータをブラインド処理するためのブラインド処理モジュールと、

ブロックチェーンノードによって設けられたプライバシースマートコントラクトに基づいて、前記呼び出しデータ及びソースデータに対して前記計算タスクを実行するデータ計算トランザクション要求を開始することにより、前記プライバシースマートコントラクトを呼び出して前記計算タスクを実行して計算結果を取得するように、前記ブロックチェーンノードに要求するための計算要求開始モジュールと、

アップリンクされた計算結果を取得するための計算結果取得モジュールと、

前記ソースデータのデータ供給者に準同型暗号化公開鍵を提供するように要求するための暗号化鍵取得モジュールと、

前記準同型暗号化公開鍵を用いて前記計算結果に対して準同型復号化を行うとともに、前記計算結果に対してブラインド除去処理を行って、平文の計算結果を取得するための計算結果処理モジュールとを含む、装置。

【請求項 1 8】

前記ブラインド処理は呼び出しデータにランダム値を追加することを含み、前記ブライ

10

20

30

40

50

ンド除去処理は計算結果から前記ランダム値を除去することを含む、請求項 17 に記載の装置。

【請求項 19】

準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵と準同型暗号化公開鍵とを含む非対称準同型暗号化鍵を生成するための暗号化鍵生成モジュールと、

前記準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵を用いて、提供されるソースデータを準同型暗号化するための準同型暗号化モジュールと、

前記プライバシースマートコントラクトに基づいて、前記ソースデータをアップリンクするデータ公開トランザクション要求を開始するためのアップリンク要求公開モジュールとをさらに含む、請求項 17 に記載の装置。

10

【請求項 20】

データ利用者の前記ソースデータの使用に対する認証を行うために、前記ソースデータの使用権限を認証センターに設けるための権限設置モジュールをさらに含む、請求項 19 に記載の装置。

【請求項 21】

少なくとも 1 つのプロセッサと、

前記少なくとも 1 つのプロセッサに通信可能に接続されるメモリとを備える電子機器であって、

前記メモリに前記少なくとも 1 つのプロセッサにより実行される指令が格納されており、前記指令が前記少なくとも 1 つのプロセッサにより実行されて、前記少なくとも 1 つのプロセッサに請求項 1～6 又は 7～10 のいずれか 1 項に記載のブロックチェーンのプライバシーデータ処理方法を実行させる、電子機器。

20

【請求項 22】

コンピュータ指令が格納されている非一時的コンピュータ可読記憶媒体であって、

前記コンピュータ指令は、前記コンピュータに請求項 1～6 又は 7～10 のいずれか 1 項に記載のブロックチェーンのプライバシーデータ処理方法を実行させる、非一時的コンピュータ可読記憶媒体。

【発明の詳細な説明】

【技術分野】

【0001】

30

本出願の実施例は、コンピュータ技術分野に関し、特に、ブロックチェーン技術に関するものである。

【背景技術】

【0002】

ブロックチェーン技術の発展に伴い、ブロックチェーンは多くのアプリケーションプログラムにおいて徐々に実現されている。ブロックチェーン技術はマルチコピー冗長モードを特徴として、チェーンにおいて処理されたトランザクション要求は全てのノードによって検証及び記憶される。このモードによって、ブロックチェーンにおけるプライバシーデータが非トランザクション参加者によって取得され、同様に、スマートコントラクトのデータも漏洩されるおそれがある。

40

【0003】

上記問題に対して、従来の解決手段は、信頼できる実行環境（Trust Execution Environment）に基づいてデータ計算を行ったり、又は、完全にオフチェーンでプライバシー計算を行ったりしている。

【0004】

上記手段の問題点は、TEEに基づく技術的手段のデプロイコストが比較的高く、ユーザが特別なハードウェアを購入する必要がある、オフチェーン計算の方法では計算が集中しすぎて、計算の公平性や安全性を保証することが困難である。

【発明の概要】

【課題を解決するための手段】

50

【0005】

本開示の実施例は、ブロックチェーンのプライバシーデータ処理手段を最適化するために、ブロックチェーンのプライバシーデータ処理方法、装置、デバイス及び記憶媒体を提供する。

【0006】

本開示の一態様によれば、ブロックチェーンノードによって実行される、ブロックチェーンのプライバシーデータ処理方法であって、当該方法は、データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得するステップであって、前記データ計算トランザクション要求における呼び出しデータは、前記データ利用者によってブラインド処理されたデータである、ステップと、前記データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得するステップと、前記データ計算トランザクション要求における計算タスクによって、前記プライバシースマートコントラクトを呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行して、計算結果を取得するステップと、前記データ計算トランザクション要求及び計算結果をアップリンクし、前記データ計算トランザクション要求のデータ利用者にフィードバックし、前記データ利用者が前記計算結果に対して準同型復号化及びブラインド除去処理を行って、平文の計算結果を取得するステップとを含む。

10

【0007】

本開示の別の一態様によれば、ブロックチェーンクライアントによって実行される、ブロックチェーンのプライバシーデータ処理方法であって、当該方法は、ブロックチェーンで公開された準同型暗号化データから計算タスクに必要なソースデータを決定するステップと、前記計算タスクの呼び出しデータをブラインド処理するステップと、ブロックチェーンノードが配置したプライバシースマートコントラクトに基づいて、前記呼び出しデータ及びソースデータに対して前記計算タスクを実行するデータ計算トランザクション要求を開始することにより、前記プライバシースマートコントラクトを呼び出し前記計算タスクを実行して計算結果を取得するように、前記ブロックチェーンノードに要求するステップと、アップリンクされた計算結果を取得するステップと、前記ソースデータのデータ供給者に準同型暗号化公開鍵を提供するように要求するステップと、前記準同型暗号化公開鍵を用いて前記計算結果に対して準同型復号化を行うとともに、前記計算結果に対してブラインド除去処理を行って、平文の計算結果を取得するステップとを含む。

20

30

【0008】

本開示の別の一態様によれば、ブロックチェーンノードに配置される、ブロックチェーンのプライバシーデータ処理装置であって、当該装置は、データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得するためのトランザクション要求取得モジュールであって、前記データ計算トランザクション要求における呼び出しデータは、前記データ利用者によってブラインド処理されたデータである、トランザクション要求取得モジュールと、前記データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得するためのソースデータ取得モジュールと、前記データ計算トランザクション要求における計算タスクによって、前記プライバシースマートコントラクトを呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行して、計算結果を取得するための計算タスク処理モジュールと、前記データ計算トランザクション要求及び計算結果をアップリンクし、前記データ計算トランザクション要求のデータ利用者にフィードバックし、前記データ利用者が前記計算結果に対して準同型復号化及びブラインド除去処理を行って、平文の計算結果を取得するためのアップリンク処理モジュールとを備える。

40

【0009】

本開示の別の一態様によれば、ブロックチェーンクライアントに配置される、ブロックチェーンのプライバシーデータ処理装置であって、当該装置は、ブロックチェーンで公開された準同型暗号化データから計算タスクに必要なソースデータを決定するためのソースデータ決定モジュールと、前記計算タスクの呼び出しデータをブラインド処理するための

50

ブラインド処理モジュールと、ブロックチェーンノードが配置したプライバシースマートコントラクトに基づいて、前記呼び出しデータ及びソースデータに対して前記計算タスクを実行するデータ計算トランザクション要求を開始することにより、前記プライバシースマートコントラクトを呼び出し前記計算タスクを実行して計算結果を取得するように、前記ブロックチェーンノードに要求するための計算要求開始モジュールと、アップリンクされた計算結果を取得するための計算結果取得モジュールと、前記ソースデータのデータ供給者に準同型暗号化公開鍵を提供するように要求するための暗号化鍵取得モジュールと、前記準同型暗号化公開鍵を用いて前記計算結果に対し準同型復号化を行うとともに前記計算結果に対しブラインド除去処理を行って、平文の計算結果を取得するための計算結果処理モジュールとを備える。

10

【0010】

本開示の別の一態様によれば、電子機器であって、当該電子機器は、少なくとも1つのプロセッサと、前記少なくとも1つのプロセッサに通信可能に接続されるメモリとを備え、前記メモリには前記少なくとも1つのプロセッサにより実行される指令が格納されており、前記指令は、前記少なくとも1つのプロセッサにより実行され、前記少なくとも1つのプロセッサに本出願のいずれかの実施例に記載のブロックチェーンのプライバシーデータ処理方法を実行させることができる。

【0011】

本開示の別の一態様によれば、コンピュータ指令が格納されている非一時的コンピュータ可読記憶媒体であって、前記コンピュータ指令は前記コンピュータに本出願のいずれかの実施例に記載のブロックチェーンのプライバシーデータ処理方法を実行させるために用いられる。

20

【0012】

本出願による技術は、従来技術においてブロックチェーンのプライバシーデータ処理を実行するときに、安全性及びプライバシーが保証されないという問題を解決し、ブロックチェーンのプライバシーデータ処理手段を最適化した。

【0013】

本部分において説明された内容は、本開示の実施例の重要な点又は重要な特徴を示すためのものではなく、また本開示の範囲を制限するためのものでもないことを理解されたい。本開示のその他特徴は以下の説明により容易に理解されるようになる。

30

【0014】

図面は本技術的手段をよりよく理解するためのものであって、本出願を限定するものではない。

【図面の簡単な説明】

【0015】

【図1】本出願の実施例によるブロックチェーンのプライバシーデータ処理方法のフローチャートである。

【図2】本出願の実施例による別のブロックチェーンのプライバシーデータ処理方法のフローチャートである。

【図3】本出願の実施例による別のブロックチェーンのプライバシーデータ処理方法のフローチャートである。

40

【図4】本出願の実施例による別のブロックチェーンのプライバシーデータ処理方法のフローチャートである。

【図5】本出願の実施例による別のブロックチェーンのプライバシーデータ処理方法のフローチャートである。

【図6】本出願の実施例による別のブロックチェーンのプライバシーデータ処理方法のフローチャートである。

【図7A】本出願の実施例によるブロックチェーンのプライバシーデータ処理方法のシグナリング図である。

【図7B】本出願の実施例によるブロックチェーンのプライバシーデータ処理システムフ

50

レームワークの概略図である。

【図 8】本出願の実施例によるブロックチェーンのプライバシーデータ処理装置の構造概略図である。

【図 9】本出願の実施例によるブロックチェーンのプライバシーデータ処理装置の構造概略図である。

【図 10】本出願の実施例のブロックチェーンのプライバシーデータ処理方法を実現するための電子機器のブロック図である。

【発明を実施するための形態】

【0016】

以下、理解を容易にするために本出願の実施例の様々な細部を含む例示的な実施例を添付図面を参照しながら説明し、それらは単なる例示的なものとして見なされるべきである。したがって、当業者は、本出願の範囲及び精神から逸脱することなく、本明細書に記載された実施例に対して様々な変更及び修正を行うことができることを理解されたい。また、以下の説明では、明確かつ簡潔にするために、公知の機能及び構造に対する説明を省略している。

【0017】

図 1 は、本出願の実施例によるブロックチェーンのプライバシーデータ処理方法のフローチャートである。本出願の実施例は、ブロックチェーンにおけるプライバシーデータに対して計算処理を実行する場合に適用する。該実施例はブロックチェーンノードに配置されたブロックチェーンのプライバシーデータ処理装置によって実行することができ、該装置はソフトウェア及び／又はハードウェアによって実装され、ブロックチェーンノードとして電子機器に統合され得る。

【0018】

図 1 に示すように、当該方法は以下のステップを含む。

ステップ S 101 において、データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得し、データ計算トランザクション要求における呼び出しデータは、データ利用者によってブラインド処理されたデータである。

【0019】

ここで、データ利用者は、ブロックチェーンに格納されたソースデータを使用してデータ処理操作を実行しようとするブロックチェーンユーザであってもよい。プライバシースマートコントラクトは、プライバシーデータ処理を実現するプログラムコレクションであってもよく、ユーザがデータを開始したりデータの様々なコンテンツに応答したりすることによって具体的なトランザクション要求を生成又は実行するように、インタラクティブインターフェイスを該プライバシースマートコントラクトに提供することができる。データ計算トランザクション要求は、データ利用者がプライバシースマートコントラクトに基づいて現在のブロックチェーンネットワークにおいて開始した、関連するデータ計算タスクを実行するようにブロックチェーンノードに要求するためのものであってもよい。

【0020】

選択的に、データ利用者が開始したデータ計算トランザクション要求には、今回実行すべき計算タスク及び該計算タスクの実行に必要なデータが含まれていてもよい。選択的に、計算タスクに必要なデータには、今回の計算タスクを実行する際に、データ利用者自身が提供すべきデータである呼び出しデータを含んでもよい。データ利用者自身のデータがプライバシーデータである可能性があるため、計算タスクの実行において公開されたくないの、本出願の実施例では、データ計算トランザクション要求における呼び出しデータはデータ利用者によってブラインド処理されたデータであってもよい。ここで、ブラインド処理は、データ利用者が自分で決定した規則に応じてその呼び出しデータを処理することで、処理されたデータが呼び出しデータ平文を漏らすことなく、データ計算タスクを続行できるようにしてもよい。ここで、該ブラインド処理の規則は可逆的であり、後続のブラインド処理された呼び出しデータに基づいて計算タスクを実行した後に、計算結果に対

しブラインド除去処理が必要となることに留意されたい。

【0021】

選択的に、本出願の実施例において、ブラインド処理の方法としていろいろあるが、これに対して特に限定せず、例えば、前記ブラインド処理は呼び出しデータにランダム値を追加することを含んでもよく、前記ブラインド除去処理は計算結果から前記ランダム値を除去することを含んでもよい。ここで、ランダム値を追加するプロセスは、加算、減算、乗算、除算などの演算の少なくとも一つであってもよいし、対応して、ランダム値を除去するプロセスはランダム値を追加するプロセスの逆プロセスであってもよい。例えば、呼び出しデータが5で、ランダム値が10であるとする、該呼び出しデータに対するブラインド処理は、呼び出しデータ5とランダム値10とを加算した結果15をブラインド処理された呼び出しデータとすることができる。計算結果が20の場合、計算結果20とランダム値10とを差分した結果10をブラインド除去処理された計算結果とする。前記ブラインド処理は、呼び出しデータ自体に対するべき乗、対数などの演算処理をさらにも含んでもよく、対応して、前記ブラインド除去処理は、計算結果に対する平方根、指数などの演算処理を含んでもよい。

10

【0022】

選択的に、本操作において、ローカルのブロックチェーンノードは、ローカルにおいてデータ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得してもよいし、ブロックチェーンネットワークを介して他のノードから伝送されたデータ計算トランザクション要求を受信してもよい。

20

【0023】

ステップS102において、データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得する。

【0024】

ここで、準同型暗号化されたソースデータは、準同型暗号化技術によって、データ供給者のソースデータを準同型暗号化処理して得たものであってもよい。いわゆるソースデータとは、例えば、従業員資料、顧客資料などデータ供給者内部のプライバシーデータであってもよい。ソースデータの安全性及びプライバシーを保証するために、データ供給者は通常そのソースデータを準同型暗号化してブロックチェーンに格納し、他のブロックチェーンユーザが使用するようにする。本出願の実施例においてソースデータに準同型暗号化を行う理由は、準同型暗号化されたソースデータを用いて計算タスクを実行した計算結果を復号化した後、暗号化していないソースデータ平文を用いて該計算タスクを実行した計算結果と同じであるからである。このようにして、データ供給者のソースデータ平文が漏洩しないことを保証しながら、データ利用者に提供されて計算タスクが実行される。

30

【0025】

選択的に、本出願の実施例では、データ供給者はそのソースデータを準同型暗号化した後ブロックチェーンネットワークにアップリンク格納することができる。ローカルのブロックチェーンノードがデータ利用者によって開始されたデータ計算トランザクション要求を受信した後、先に、ソースデータ識別ID、データ供給者、データ使用量など、該データ計算トランザクション要求から今回の計算タスクが指定するソースデータの関連情報を決定した後、ブロックチェーンネットワークから該関連情報が指定する準同型暗号化されたソースデータを検索して取得する。

40

【0026】

ステップS103において、データ計算トランザクション要求における計算タスクによって、プライバシースマートコントラクトを呼び出し、呼び出しデータ及びソースデータに対する計算を実行して、計算結果を取得する。

【0027】

ここで、計算タスクは、データ利用者が今回準同型暗号化されたソースデータ及びそれ自身の呼び出しデータを用いて実行する必要がある計算タスクであってもよい。例えば、該計算タスクには、モデルトレーニングタスク、データ統計タスク、データ予測タスクな

50

どが含まれてもよいが、これらに限定されない。

【0028】

選択的に、本操作において、ローカルのブロックチェーンノードは、まず、データ計算トランザクション要求から実行すべき計算タスクを取得した後、プライバシースマートコントラクトを呼び出し、データ計算トランザクション要求におけるブラインド処理された呼び出しデータと、ステップS102で取得した準同型暗号化されたソースデータとに対して、今回の計算タスクを実行して、計算結果を得るようにしてもよい。

【0029】

例えば、データ利用者によって公開された計算トランザクション要求が一つの顔認識ネットワークモデルのトレーニングであると仮定し、ローカルのブロックチェーンノードは、計算トランザクション要求からブラインド処理された訓練すべき顔認識モデルの関連データを呼び出しデータとして取得し、ブロックチェーンネットワークから大量の準同型暗号化されたユーザ顔画像をソースデータとして取得し、その後、プライバシースマートコントラクトでモデル訓練を実行する関連プログラムコードを呼び出し、ソースデータをトレーニングサンプルとし、呼び出しデータに対応する顔認識モデルをモデルパラメータ訓練し、訓練された顔認識モジュールを計算結果として取得する。

【0030】

ステップS104において、データ計算トランザクション要求及び計算結果をアップリンクし、データ計算トランザクション要求のデータ利用者にフィードバックし、データ利用者が計算結果に対して準同型復号化及びブラインド除去処理を行うようにして、平文の計算結果を取得する。

【0031】

選択的に、本操作では、ローカルのブロックチェーンノードが今回の計算タスクを実行して、計算結果を取得した後、プライバシースマートコントラクトにおけるアップリンク操作の関連プログラムコードを呼び出し、今回処理したデータ計算トランザクション要求と計算して得た計算結果とをアップリンク格納することができる。このとき、データ利用者はブロックチェーンからその開始したデータ計算トランザクション要求の計算結果を取得することができる。該計算結果はデータ供給者が準同型暗号化したソースデータと、ブラインド処理した呼び出しデータとを計算することで得たものであるため、データ利用者は当該計算結果に対して準同型復号化処理して、初期の平文の計算結果を得なければならない、該初期の平文の計算結果は、暗号化していないソースデータを用いて今回の計算タスクを行って得た結果と同様である。その後、再度自身が呼び出しデータをブラインド処理したときの操作と逆の操作に基づいて、初期の平文の計算結果に対しブラインド除去処理を行って、最終的な平文の計算結果を得る。

【0032】

選択的に、本出願の実施例は、計算結果に対して準同型復号化処理を行う際に、今回の計算タスクが使用するソースデータの供給者が該ソースデータを準同型暗号化する際に使用する準同型暗号化鍵（準同型暗号化公開鍵など）を取得して、計算結果を復号化処理するようにしてもよい。例えば、データ供給者とオフラインでやり取りして、データ供給者の準同型暗号化公開鍵の取得を要求するようにしてもよい。また、データ供給者の準同型暗号化公開鍵などを取得するために、ブロックチェーンネットワークにデータ供給者の暗号化鍵取得要求を発信するようにしてもよく、これに対して本発明の実施例は限定しない。

【0033】

本出願の実施例の技術的手段は、ブロックチェーンノードが、データ利用者が開始したデータ計算トランザクション要求を取得した後、今回の計算タスクを実行するのに必要な準同型暗号化されたソースデータとブラインド処理された呼び出しデータとを取得し、プライバシースマートコントラクトを呼び出し今回の計算タスクを実行して、計算結果を得、アップリンク格納する。本出願の実施例において計算タスクの実行に使用するソースデータはデータ供給者により準同型暗号化されたソースデータであり、データ供給者のデー

タの安全性を保証し、使用する呼び出しデータはデータ利用者によりブラインド処理されたデータであり、データ利用者のデータの安全性を保証し、最後に復号化処理及びブラインド除去処理を行うことにより計算結果の正確性を保証した。プライバシーデータ処理プロセス全体が通常のブロックチェーンノードを用いて完了することができ、且つデータ供給者及びデータ利用者のデータの漏洩を引き起こすことなく、プライバシーデータ処理プロセスの公平性及び安全性を保証した。従って、ブロックチェーンのプライバシーデータ処理プログラムが最適化される。

【0034】

図2は、本出願の実施例によるもう一つのブロックチェーンのプライバシーデータ処理方法のフローチャートである。本実施例は上記実施例に加えてさらなる最適化を行ったものであり、データ供給者のデータ公開トランザクション要求を処理する詳細について紹介する。図2に示すように、該方法は以下を含む。

10

【0035】

ステップS201において、データ供給者によってプライバシースマートコントラクトに基づいて開始されたデータ公開トランザクション要求を取得し、データ公開トランザクション要求におけるソースデータは準同型暗号化されたデータである。

【0036】

ここで、データ公開トランザクション要求は、データ供給者がプライバシースマートコントラクトに基づいて現在のブロックチェーンネットワークにおいて開始した、ブロックチェーンノードにそこに含まれるソースデータをアップリンク格納するように要求するためのものであってもよい。選択的に、本出願の実施例において、データ公開トランザクション要求に含まれるソースデータはデータ供給者自身のプライバシーデータであってもよく、且つ該ソースデータは準同型暗号化アルゴリズムを用いて暗号化されたソースデータである。

20

【0037】

選択的に、データ供給者がブロックチェーンネットワークにそのソースデータをアップリンクして他のブロックチェーンユーザが使用するようにする場合に、先にそのソースデータを準同型暗号化アルゴリズムを用いて暗号化した後、プライバシースマートコントラクトに基づいてブロックチェーンネットワークにデータ公開トランザクション要求を送信するようにしてもよい。ローカルのブロックチェーンノードは、ローカルにおいてデータ利用者がプライバシースマートコントラクトに基づいて送信したデータ公開トランザクション要求を取得してもよく、ブロックチェーンネットワークを介して他のノードから伝送されたデータ公開トランザクション要求を受信してもよい。

30

【0038】

ステップS202において、プライバシースマートコントラクトを呼び出してデータ公開トランザクション要求を実行し、ソースデータをアップリンク公開する。

【0039】

選択的に、ローカルのブロックチェーンノードは、データ公開トランザクション要求を受信した後、プライバシースマートコントラクトを呼び出して該データ公開トランザクション要求を実行し、その中から公開される準同型暗号化されたソースデータを取得し、それから、取得した当該ソースデータ及びデータ公開トランザクション要求をトランザクションデータとしてブロックチェーンネットワークに格納し、他のブロックチェーンアカウントが使用するようにしてもよい。

40

【0040】

選択的に、使用者が必要なソースデータを選択しやすくするために、本出願の実施例はデータ供給者がデータ公開トランザクション要求を開始する際に、公開されるソースデータに当該ソースデータを紹介する要約情報などを追加することもできる。これに対応して、本ステップは、プライバシー実行コントラクトを呼び出してデータ公開トランザクション要求を実行する際に、データ公開トランザクション要求、ソースデータ及びソースデータの要約情報を一括してアップリンク格納する。

50

【0041】

ステップS203において、データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得し、データ計算トランザクション要求における呼び出しデータは、データ利用者によってブラインド処理されたデータである。

【0042】

ステップS204において、データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得する。

【0043】

ステップS205において、データ計算トランザクション要求における計算タスクによって、プライバシースマートコントラクトを呼び出し、呼び出しデータ及びソースデータに対する計算を実行して、計算結果を取得する。

【0044】

ステップS206において、データ計算トランザクション要求及び計算結果をアップリンク操作し、データ計算トランザクション要求のデータ利用者にフィードバックし、データ利用者が計算結果に対して準同型復号化及びブラインド除去処理を行うようにして、平文の計算結果を取得する。

【0045】

本出願の実施例の技術的手段は、ブロックチェーンノードがデータ供給者によって開始されたデータ公開トランザクション要求を取得した後、当該データ公開トランザクション要求を実行して準同型暗号化されたソースデータを取得してアップリンクする。データ供給者のソースデータの安全性が保証される。ブロックチェーンノードは、データ利用者が開始したデータ計算トランザクション要求を取得した後、今回の計算タスクを実行するのに必要な準同型暗号化されたソースデータ及びブラインド処理された呼び出しデータを取得し、プライバシースマートコントラクトを呼び出して今回の計算タスクを実行し、計算結果を取得してアップリンク格納する。本出願の実施例は、ソースデータ及び呼び出しデータの平文を漏洩することなく、同時に、データ利用者が正常にデータ計算タスクを行うことを支援することができ、且つ後続の準同型復号化とブラインド除去処理によって正確な計算結果を得ることができる。計算プロセスの公平性及び安全性が保証される。

【0046】

選択的に、本出願の実施例は、上記ステップS202の操作を実行する際に、さらに、プライバシースマートコントラクトを呼び出しデータ公開トランザクション要求を実行して、データ利用者情報、ソースデータ説明情報、ソースデータ格納場所及びソースデータ要約情報を含むソースデータのデータ情報を取得し、データ公開トランザクション要求及びデータ情報をアップリンクするようにしてもよい。具体的に、本出願の実施例では、データ供給者はプライバシースマートコントラクトと、公開されるソースデータのデータ情報とに基づいてデータ公開トランザクション要求を開始する。ここで、公開されるソースデータのデータ情報には、データ使用権限のある使用者情報、今回公開されたソースデータの説明情報（データタイプ、データサイズなど）、ソースデータの具体的な格納場所及びソースデータの内容を紹介するソースデータ要約情報などが含まれていてもよい。このとき、ブロックチェーンノードはプライバシースマートコントラクトを呼び出して当該データ公開トランザクション要求を実行し、その中からソースデータのデータ情報を取得した後、取得したデータ公開トランザクション要求及びそれに含まれるソースデータのデータ情報をブロックチェーンネットワークに格納し、他のブロックチェーンユーザが使用するようにしてもよい。本出願の実施例では、ブロックチェーンネットワークにソースデータの具体的な内容ではなくデータのデータ情報を格納することを選択し、この設置の利点は、ブロックチェーンのメモリ空間を大幅に節約し且つ後続のソースデータ検索の効率を向上させることができる。

【0047】

図3は、本出願の実施例による別のブロックチェーンのプライバシーデータ処理方法の

10

20

30

40

50

フローチャートである。本実施例は、上記各実施例に加えてさらなる最適化を行ったものであり、データ計算トランザクション要求を取得した後、データ利用者を認証する詳細について紹介する。図3に示すように、該方法は以下を含む。

【0048】

ステップS301において、データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得し、データ計算トランザクション要求における呼び出しデータは、データ利用者によってブラインド処理されたデータである。

【0049】

ステップS302において、データ計算トランザクション要求において指定されたソースデータに基づいて、データ利用者がソースデータを使用する権限に対して認証操作を行う。

10

【0050】

選択的に、本出願の実施例では、ローカルのブロックチェーンノードは、データ計算トランザクション要求を取得した後、当該データ計算トランザクション要求を解析して、指定された今回使用すべきソースデータを取得した後、先に当該ソースデータを取得するのではなく、今回のデータ計算トランザクション要求を公開するデータ利用者を先に認証し、当該データ利用者が当該ソースデータを使用する権限があるか否かを判断する。具体的に、ブロックチェーンノードがデータ利用者を認証する方法は多く、本出願の実施例はこれに対し限定しない。

20

【0051】

実施形態1によれば、データ供給者がデータ公開トランザクション要求を開始する際に、当該データ公開トランザクション要求にデータ利用者情報を追加することができ、こうしてブロックチェーンノードがデータ公開トランザクション要求を実行する際に、既にソースデータ及びそれに対応するデータ利用者情報を一括してブロックチェーンネットワークに格納しており、このとき、ブロックチェーンノードはブロックチェーンネットワークにおいて今回のデータ計算トランザクション要求において指定されたソースデータに対応するデータ利用者情報を検索し、当該データ利用者情報に基づいて今回のデータ利用者に当該ソースデータを使用する権限があるか否かを判断することができる。例えば、データ利用者情報が当該ソースデータを使用可能な利用者の条件であれば、今回のデータ利用者が当該条件を備えているか否かを判断し、データ利用者情報がそのライセンス又はブラックリストの各データ利用者アカウントIDであれば、今回のデータ利用者がその中にあるか否かを判断するようにしてもよい。

30

【0052】

実施形態2によれば、データ計算トランザクション要求において指定されたソースデータに基づいて、認証センターにデータ利用者がソースデータを使用する認証要求を送信して、データ供給者により設けられた権限によって認証要求を処理するように認証センターに要求し、認証センターからフィードバックされた認証結果を取得する。ここで、認証センターはブロックチェーンネットワークにおいて専門的に認証鑑定を行うためのノードである。データ供給者は該認証センターにその公開するソースデータの使用権限を設置することができる。具体的に、この実施形態では、ブロックチェーンノードが、データ計算トランザクション要求に指定されたソースデータと今回のデータ利用者の関連情報とに基づいて、当該データ要求者に対してソースデータを使用する認証要求を認証センターに送信し、認証センターはその内部で当該ソースデータの供給者が設置した使用権限を検索し、今回のデータ利用者が当該使用権限に該当するか否かを判断し、該当すれば認証結果が通過となり、そうでなければ認証結果が失敗となる。ブロックチェーンノードは認証センターからフィードバックされた認証結果を取得する。

40

【0053】

実施形態3によれば、ブロックチェーンノードは前記データ計算トランザクション要求において指定されたソースデータに基づいて、該ソースデータに対応するデータ供給者を

50

特定し、プライバシースマートコントラクトを呼び出して今回のデータ利用者の認証トランザクション要求を生成して、データ供給者に送信し、今回のデータ利用者をオンライン認証するようにデータ供給者に要求し、データ供給者からフィードバックされた認証結果を取得するようにしてもよい。

【0054】

当該ステップは、データ計算トランザクション要求において指定されたソースデータに基づいて、データ利用者がソースデータを使用する権限を認証し、認証が通過となった後、ステップS303及び後続の操作を実行できることに留意されたい。

【0055】

ステップS303において、データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得する。

10

【0056】

ステップS304において、データ計算トランザクション要求における計算タスクによって、プライバシースマートコントラクトを呼び出し、呼び出しデータ及びソースデータに対する計算を実行して、計算結果を取得する。

【0057】

ステップS305において、データ計算トランザクション要求及び計算結果をアップリンクし、データ計算トランザクション要求のデータ利用者にフィードバックし、データ利用者が計算結果に対して準同型復号化及びブラインド除去処理を行うようにして、平文の計算結果を取得する。

20

【0058】

本出願の実施例の技術的手段は、ブロックチェーンノードが、データ利用者が開始したデータ計算トランザクション要求を取得した後、まず、データ利用者に必要なソースデータに基づいて、データ利用者が当該ソースデータを使用する権限に対して認証を行い、認証が通過であれば、今回の計算タスクに必要な準同型暗号化されたソースデータとブラインド処理された呼び出しデータとを取得することができ、プライバシースマートコントラクトを呼び出して今回の計算タスクを実行し、計算結果を得てアップリンク格納する。本出願の実施例はデータ計算トランザクション要求の計算タスクを処理する前に、まずデータ利用者がソースデータを使用する権限に対して認証を行う。ソースデータが許可されていないデータ利用者に使用されることを防止し、データ供給者のソースデータの安全性が一層保証される。

30

【0059】

図4は、本出願の実施例による別のブロックチェーンのプライバシーデータ処理方法のフローチャートである。本実施例は、上記実施例に加えてさらなる最適化を行ったものであり、前記プライバシースマートコントラクトを呼び出して、前記呼び出しデータと前記ソースデータとに対する計算プロセスを実行する詳細について紹介する。図4に示すように、該方法は以下を含む。

【0060】

ステップS401において、データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得するステップであって、データ計算トランザクション要求における呼び出しデータはデータ利用者によってブラインド処理されたデータである。

40

【0061】

ステップS402において、データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得する。

【0062】

ステップS403において、データ計算トランザクション要求における計算タスクによって、プライバシースマートコントラクトを呼び出して仮想マシン上で実行し、プライバシースマートコントラクトによって仮想マシンの組み込み関数を呼び出して、呼び出しデータ及びソースデータに対する計算を実行して、計算結果を取得する。

50

【0063】

ここで、仮想マシンの組み込み関数は内蔵関数及びインライン関数とも呼ばれる。組み込み関数を呼び出して計算操作を実行する際、仮想マシンの上位レベル呼び出し関数に対して透過的である。組み込み関数を用いて計算操作を実現することにより計算を高速化することができる。

【0064】

選択的に、ブロックチェーンノードはデータ計算タスクにおける計算タスクによって、プライバシースマートコントラクトを呼び出し計算タスクを実行する際に、先にスマートコントラクトを呼び出して仮想マシン上で実行してから、スマートコントラクトによって仮想マシンの組み込み関数を呼び出し、組み込み関数を用いてブラインドされた呼び出しデータと準同型暗号化されたソースデータとに対して今回の計算タスクを実行する必要がある。計算タスクを実行する本操作の組み込み関数はコンパイルプロセスにおいてメイン呼び出し関数に直接埋め込まれ、組み込み関数が計算操作を実行するときに、仮想マシンのメイン呼び出し関数を通しての必要がないため、組み込み関数を用いて計算タスクを実行することは、計算の実行時間を大幅に節約し、計算効率を向上させることができる。

【0065】

ステップS404において、データ計算トランザクション要求及び計算結果をアップリンクして、データ計算トランザクション要求のデータ利用者にフィードバックし、データ利用者が計算結果に対して準同型復号化及びブラインド除去処理を行うようにして、平文の計算結果を取得する。

【0066】

本出願の実施例の技術的手段は、ブロックチェーンノードが、データ利用者が開始したデータ計算トランザクション要求を取得した後、プライバシースマートコントラクトを呼び出して仮想マシンで実行し、スマートコントラクトに従って仮想マシンの組み込み関数を呼び出し、準同型暗号化されたソースデータとブラインド処理された呼び出しデータに対して特定の計算操作を実行し、取得した計算結果をアップリンク格納する。本出願の実施例は、仮想マシンの組み込み関数を介してソースデータ及び呼び出しデータを計算することによって、計算の実行時間を大幅に節約し、計算効率を向上させることができる。

【0067】

図5は本出願の実施例による別のブロックチェーンのプライバシーデータ処理方法のフローチャートである。本出願の実施例はブロックチェーンにおけるプライバシーデータに対して計算処理を実行する場合に適用可能である。該実施例はブロックチェーンクライアントを有するデバイスに配置されたブロックチェーンのプライバシーデータ処理装置によって実行することができ、該装置はソフトウェア及び／又はハードウェアによって実装され、ブロックチェーンクライアントを有する電子機器に統合され得る。選択的に、ブロックチェーンクライアントは、ブロックチェーンユーザ（データ利用者又はデータ供給者など）の電子機器にインストールされたブロックチェーンネットワークのクライアントであってもよい。ここで、本出願の実施例の実行主体はデータ利用者のブロックチェーンクライアントであってもよい。

【0068】

ステップS501において、ブロックチェーンに公開された準同型暗号化データから計算タスクに必要なソースデータを決定する。

【0069】

選択的に、本出願の実施例では、データ利用者がブロックチェーンにすでに公開された準同型暗号化データを用いて計算タスクを実行する必要がある場合、先にそのブロックチェーンクライアントを介してブロックチェーンネットワークにアクセスし、ブロックチェーンにすでに公開された準同型暗号化されたソースデータのデータ情報（例えば、ソースデータID、ソースデータ要約情報及びデータ利用者情報など）を取得して分析し、その中から今回の計算タスクに必要なソースデータを特定するようにしてもよい。具体的に、ブロックチェーンにすでに公開されている準同型暗号化データのデータID又はソースデ

ータ要約情報を調べて、その中から今回の計算タスクに必要なソースデータを特定するようにしてもよい。さらに、それに加えて、ソースデータのデータ利用者情報を組み合わせて、自身が当該ソースデータを使用できるか否かの権限を判断し、権限があれば、当該ソースデータが今回の計算タスクに必要なソースデータであると決定するようにしてもよい。

【0070】

ステップS502において、計算タスクの呼び出しデータをブラインド処理する。

選択的に、データ利用者はブロックチェーンに公開されたソースデータに対して計算タスクを実行しようとするとき、自身のデータ（すなわち、呼び出しデータ）を呼び出す必要がある、ブロックチェーンノードが計算タスクを実行する過程において、自身の呼び出しデータが漏洩しないようにするために、データ利用者はそのブロックチェーンクライアントを介して今回の計算タスクに使用する必要のある呼び出しデータをブラインド処理することができる。具体的なブラインド処理プロセスは上記の実施例で詳細に説明されており、この実施例では繰り返さない。例えば、ブラインド処理は呼び出しデータにランダム値を追加することを含むことができる。

10

【0071】

ステップS503において、ブロックチェーンノードが配置したプライバシースマートコントラクトに基づいて、呼び出しデータ及びソースデータに対して計算タスクを実行するデータ計算トランザクション要求を開始し、プライバシースマートコントラクトを呼び出し計算タスクを実行して計算結果を取得するように、ブロックチェーンノードに要求する。

20

【0072】

選択的に、データ利用者のブロックチェーンクライアントはブロックチェーンノードが配置したプライバシースマートコントラクトに基づいて、ブロックチェーンネットワークから選択されたソースデータ、ブラインド処理された呼び出しデータ、及び今回実行する必要のある計算タスクを組み合わせ、呼び出しデータとソースデータに対して計算タスクを実行するデータ計算トランザクション要求を開始し、それをブロックチェーンネットワークに送信する。ブロックチェーンノードは当該データ計算トランザクション要求を受信した後、プライバシースマートコントラクトを呼び出して当該データ計算トランザクション要求における計算タスクを実行し、計算結果を取得して、計算結果とデータ計算トランザクション要求とをアップリンク格納する。

30

【0073】

ステップS504において、アップリンクされた計算結果を取得する。

選択的に、ブロックチェーンノードがすでに処理されたデータ計算トランザクション要求及びその計算結果をアップリンク格納してあるため、この時点でデータ利用者のブロックチェーンクライアントは、ブロックチェーンでその開始したデータ計算トランザクション要求の計算結果がアップリンクしてあるかどうかを調べることができ、アップリンクされている場合は、アップリンクされた当該計算結果を取得する。

【0074】

ステップS505において、ソースデータのデータ供給者に準同型暗号化公開鍵を提供するように要求する。

40

【0075】

選択的に、ブロックチェーンノードが呼び出しデータ及びソースデータに対して計算タスクを実行する際、使用するソースデータがデータ供給者によって準同型暗号化処理されたソースデータであるので、正確な計算結果を得るためには、準同型暗号化処理時に使用した暗号化鍵を用いて当該計算結果を復号化する必要がある。従って、この際、データ利用者のブロックチェーンクライアントは、ソースデータのデータ供給者に準同型暗号化された公開鍵を提供するように要求する必要がある。

【0076】

具体的に、ブロックチェーンネットワークに各データ供給者の準同型暗号化公開鍵が格

50

納されている場合、このとき、ブロックチェーンネットワークにソースデータのデータ供給者の公開鍵取得要求を公開し、今回使用するソースデータのデータ供給者の準同型暗号化公開鍵をフィードバックするようにブロックチェーンノードに要求するようにしてもよい。ブロックチェーンネットワークに各データ供給者の準同型暗号化公開鍵が格納されていない場合、このとき、データ利用者のブロックチェーンクライアントはデータ供給者のブロックチェーンクライアントと直接やり取りしてデータ供給者に準同型暗号化公開鍵を提供するように要求することができる。

【0077】

ステップS506において、準同型暗号化公開鍵を用いて計算結果に対し準同型復号化を行うとともに、計算結果に対しブラインド除去処理を行って、平文の計算結果を取得する。

10

【0078】

選択的に、データ利用者のブロックチェーンクライアントがデータ供給者の準同型暗号化公開鍵を取得した後、プライバシースマートコントラクトを呼び出し、準同型暗号化公開鍵を用いて計算結果に対し準同型復号化を行い、初期の平文の計算結果を取得するようにしてもよい。当該初期の平文の計算結果は、暗号化していないソースデータ平文を用いて今回の計算タスクを実行して得られる結果と同様である。ブロックチェーンノードが呼び出しデータ及びソースデータに対し計算タスクを実行する際、使用する呼び出しデータが前のブラインド処理されたデータであるため、このときはさらに、自身が呼び出しデータをブラインド処理するときの逆操作に基づいて、初期の平文の計算結果に対してブラインド除去処理して、最終的な平文の計算結果を取得する必要がある。選択的に、ステップS502におけるブラインド処理が呼び出しデータにランダム値を追加することを含む場合、本ステップのブラインド除去処理は計算結果から前記ランダム値を除去することを含む。

20

【0079】

本出願の実施例の技術的手段は、データ利用者のブロックチェーンクライアントが、ブロックチェーンにすでに公開された準同型暗号化データから今回の計算に必要なソースデータを決定するとともに、今回の計算タスクのローカル呼び出しデータに対してブラインド処理を行い、呼び出しデータ及びソースデータに対し今回の計算タスクを実行するデータ計算トランザクション要求を開始し、ブロックチェーンノードに当該計算タスクを実行して計算結果を取得するように要求する。ブロックチェーンクライアントは計算結果を取得した後、まず、今回ソースデータを使用するデータ供給者の準同型暗号化公開鍵を取得するように要求した後、さらに計算結果に対して準同型復号化及びブラインド除去処理を実行し、最終的な平文の計算結果を取得する。本出願の実施例において、計算タスクの実行に使用されるデータ供給者のソースデータは準同型暗号化されたソースデータであり、データ供給者のデータの安全性を保証し、使用されるデータ利用者の呼び出しデータはブラインド処理されたデータであり、データ利用者のデータの安全性を保証し、最後に復号化処理とブラインド除去処理を行うことによって、計算結果の正確性を保証する。計算プロセス全体においてデータ供給者及びデータ利用者のデータの漏洩を引き起こすことがなく、計算プロセスの公平性及び安全性を保証した。従って、ブロックチェーンのプライバシーデータ処理手段が最適化される。

30

40

【0080】

図6は、本出願の実施例による別のブロックチェーンのプライバシーデータ処理方法のフローチャートである。本実施例は上記実施例に加えてさらなる最適化を行ったものであり、データ供給者のブロックチェーンクライアントがプライバシーデータ処理を実行する詳細について紹介する。図6に示すように、該方法は以下を含む。

【0081】

ステップS601において、準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵と準同型暗号化公開鍵とを含む非対称準同型暗号化鍵を生成する。

【0082】

50

選択的に、準同型暗号化モジュールは準同型暗号化に関連する操作を実行するモジュールであってもよい。本ステップでは、データ供給者が自身のソースデータをアップリンク格納して、他のブロックチェーンユーザに共有しようとするとき、準同型暗号化モジュールにおいて準同型暗号化鍵を生成する関連プログラムコードを呼び出して、一対の非対称準同型暗号化鍵、すなわち、準同型暗号化公開鍵と準同型暗号化秘密鍵を生成することができる。ここで、準同型暗号化秘密鍵は、他のブロックチェーンユーザに提供されて使用されるソースデータをローカルで暗号化するためのものであり、準同型暗号化公開鍵は、データ利用者に提供されて、データ利用者が準同型暗号化されたソースデータを用いて計算を行って取得した計算結果に対して準同型復号化処理するために用いられる。

【0083】

ステップS602において、準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵を用いて、提供されるソースデータを準同型暗号化する。

【0084】

選択的に、本ステップでは、データ供給者のブロックチェーンクライアントが非対称準同型暗号化鍵を生成した後、準同型暗号化モジュールを再度呼び出し、ステップS601で生成された準同型暗号化秘密鍵を用いて他のブロックチェーンユーザに提供されて使用されるソースデータに対して準同型暗号化を行って、準同型暗号化されたソースデータを取得するようにしてもよい。選択的に、本出願の実施例は、任意の準同型暗号化アルゴリズムを用いて準同型暗号化操作を実行することができ、これに対しては限定しない。例えば、Paillier準同型暗号化アルゴリズムであってもよい。

【0085】

ステップS603において、プライバシースマートコントラクトに基づいて、ソースデータをアップリンクするデータ公開トランザクション要求を開始する。

【0086】

選択的に、提供されるソースデータを準同型暗号化した後、データ供給者のブロックチェーンクライアントはプライバシースマートコントラクトを呼び出して、準同型暗号化されたソースデータを含むデータ公開トランザクション要求を生成してブロックチェーンネットワークに送信し、ブロックチェーンノードがプライバシースマートコントラクトを呼び出して該データ公開トランザクション要求を実行し、前記ソースデータをアップリンク格納するようにすることができる。

【0087】

選択的に、本ステップは、データ利用者が必要なソースデータを早く検索できるようにするために、プライバシースマートコントラクトに基づいて、開始されたデータ公開トランザクション要求に、ソースデータの説明情報及びソースデータ要約情報を含めることができる。ブロックチェーンのメモリ空間を節約するために、本ステップは、さらに、準同型暗号化されたソースデータをアップリンクするのではなく、ソースデータを予め設定された位置に格納した後、ソースデータの格納位置をブロックチェーンにアップリンク格納するようにしてもよい。すなわち、本ステップにより開始されたソースデータをアップリンクするデータ公開トランザクション要求にはソースデータ格納位置を含むことができる。

【0088】

ステップS604において、データ利用者のソースデータ使用に対し認証するように、ソースデータの使用権限を認証センターに配置する。

【0089】

選択的に、本出願の実施例では、データ供給者が準同型暗号化されたソースデータをアップリンク格納することを完了した後、認証センターにその提供するソースデータの使用権限を配置し、認証センターがソースデータを使用するデータ利用者に対し認証を行って、権限のない使用者によってソースデータが使用されることを防止し、ソースデータの安全性を一層保証することができる。

【0090】

選択的に、本ステップでは、ソースデータの使用権限を認証センターに配置するプロセスは多くあるが、これに対しては限定しない。例えば、当該ソースデータを使用可能なユーザアカウントIDを認証センターに設置してもよいし、当該ソースデータを使用可能なユーザ条件を認証センターに設置してもよいし、当該ソースデータを使用できないユーザアカウントIDを認証センターに設置してもよいなどであり得る。選択的に、本出願の実施例は、ソースデータの使用権限を事前に設置するのではなく、利用者が当該ソースデータを使用する際に、認証センターを介してデータ供給者とやり取りして、オンライン認証を行うようにしてもよい。

【0091】

本出願の実施例の技術的手段は、データ供給者がブロックチェーンネットワークにソースデータをアップリンクしようとソースデータを正常に使用することを保証しつつ、データ供給者のソースデータ平文の漏洩を回避し、計算プロセスの公平性及び安全性を保証している。なお、データ供給者はソースデータをアップリンクした後、さらにソースデータの使用権を認証センターに配置し、データ利用者がソースデータを使用する際に、認証センターがデータ利用者に対し認証を行うので、ソースデータの安全性が一層保証される。権限のないユーザが勝手にソースデータを使用することを防止する。

【0092】

図7Aは、本出願の実施例によるブロックチェーンのプライバシーデータ処理方法のシグナリング図である。図7Bは、本出願の実施例によるブロックチェーンのプライバシーデータ処理システムフレームワーク図である。本実施例は、上記各実施例に加えてさらなる最適化を行ったものであり、データ利用者のブロックチェーンクライアント、データ供給者のブロックチェーンクライアント及びブロックチェーンノードが相互協調して、ブロックチェーンのプライバシーデータ処理を実現する詳細について紹介する。図7A～図7Bに示すように、該方法は以下を含む。

【0093】

ステップS701において、データ供給者のブロックチェーンクライアントが準同型暗号化モジュールを呼び出し、準同型暗号化秘密鍵と準同型暗号化公開鍵とを含む非対称準同型暗号化鍵を生成する。

【0094】

ステップS702において、データ供給者のブロックチェーンクライアントが準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵を用いて、提供されるソースデータを準同型暗号化する。

【0095】

選択的に、ステップS701～S702は、図7Bにおけるブロックチェーンクライアント1によって実行されるようにしてもよく、このときのブロックチェーンクライアント1はデータ供給者のブロックチェーンクライアントであり、当該ブロックチェーンクライアント1はスーパーブロックチェーンソフトウェア開発キットSDKにしてもよい。その中にPaillier準同型秘密モジュールなどの準同型暗号化モジュールが統合されている。この時、ブロックチェーンクライアント1は、図7Bにおける矢印1の操作を実行し、内部の準同型暗号化モジュールを呼び出して、一対の非対称準同型暗号化鍵、つまり、準同型暗号化公開鍵と準同型暗号化秘密鍵を生成し、その後引き続き当該準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵を用いて、提供されるソースデータを準同型暗号化処理する。

【0096】

ステップS703において、データ供給者のブロックチェーンクライアントはプライバシースマートコントラクトに基づいて、ソースデータをアップリンクするデータ公開トランザクション要求を開始する。

【0097】

選択的に、本ステップは同様に図7Bにおけるブロックチェーンクライアント1によって実行され、このとき、ブロックチェーンクライアント1は図7Bにおける矢印2の操作

10

20

30

40

50

を実行し、プライバシースマートコントラクトに基づいて、ソースデータをアップリンクするデータ公開トランザクション要求を開始しブロックチェーンネットワークに送信する。

【0098】

ステップS704において、ブロックチェーンノードは、データ供給者によってプライバシースマートコントラクトに基づいて開始されたデータ公開トランザクション要求を取得するステップであって、データ公開トランザクション要求におけるソースデータは準同型暗号化されたデータである。

【0099】

ステップS705において、ブロックチェーンノードは、プライバシースマートコントラクトを呼び出してデータ公開トランザクション要求を実行し、ソースデータをアップリンク公開する。

【0100】

選択的に、図7Bには、二つのブロックチェーンノード、すなわち、ブロックチェーンノードAとブロックチェーンノードBとが示されており、二者の構造は同じである。本出願のブロックチェーンノードには仮想マシン（例えば、WebAssembly仮想マシン）が作成されており、仮想マシンには組み込み関数が埋め込まれており、組み込み関数がある実行環境において同期暗号化モジュールを呼び出して準同型暗号化されたソースデータの関連操作を実行する。

【0101】

選択的に、図7Bは、図7BにおけるブロックチェーンノードAとブロックチェーンノードBがステップS704～S705を実行する操作を示しており、具体的に、ブロックチェーンノードA及びブロックチェーンノードBは、プライバシースマートコントラクトを呼び出して仮想マシン上で実行し、プライバシースマートコントラクトによって仮想マシンの組み込み関数を呼び出し、組み込み関数によって同期暗号化モジュールを呼び出してこのときの矢印6の操作を実行する。すなわち、データ公開トランザクション要求を実行し、ソースデータをアップリンク公開する。選択的に、ソースデータをアップリンクする操作は、仮想マシンの上位関数によって実行するようにしてもよく、これに対し本実施例は限定しない。

【0102】

ステップS706において、データ供給者のブロックチェーンクライアントは、データ利用者の前記ソースデータの使用を認証すべく、ソースデータの使用権限を認証センターに配置する。

【0103】

選択的に、本ステップは図7Bにおける矢印3の操作に対応し、ブロックチェーンクライアント1は、提供されるソースデータに対し、認証センターに使用権限を配置し、後で、認証センターによりデータ利用者のソースデータの使用に対し認証を行う。

【0104】

ステップS707において、データ利用者のブロックチェーンクライアントは、ブロックチェーンに公開された準同型暗号化データから計算タスクに必要なソースデータを決定する。

【0105】

ステップS708において、データ利用者のブロックチェーンクライアントは計算タスクの呼び出しデータに対しブラインド処理を行う。

【0106】

ステップS709において、データ利用者のブロックチェーンクライアントは、ブロックチェーンノードが配置したプライバシースマートコントラクトに基づいて、呼び出しデータ及びソースデータに対して計算タスクを実行するデータ計算トランザクション要求を開始する。

【0107】

10

20

30

40

50

選択的に、ステップ S 7 0 7 ~ S 7 0 9 は、図 7 B におけるブロックチェーンクライアント 2 によって実行されるようにしてもよく、このときのブロックチェーンクライアント 2 はデータ利用者のブロックチェーンクライアントであり、当該ブロックチェーンクライアント 2 はスーパーブロックチェーン SDK にしてもよい。その中に、P a l l i e r 準同型秘密モジュールなどの準同型暗号化モジュールが統合されている。このとき、ブロックチェーンクライアント 2 は、図 7 B の矢印 4 の操作を実行することができ、まず、ブロックチェーンに公開された準同型暗号化データから今回の計算タスクに必要なソースデータを決定した後、データ利用者自身の呼び出しデータをブラインド処理し、ブロックチェーンノードが配置したプライバシースマートコントラクトに基づいて、ブロックチェーンネットワークに、呼び出しデータ及びソースデータに対して計算タスクを実行するデータ計算トランザクション要求を開始することができる。選択的に、前記ブラインド処理は呼び出しデータにランダム値を追加することを含む。

10

【0108】

ステップ S 7 1 0 において、ブロックチェーンノードは、データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得するステップであって、データ計算トランザクション要求における呼び出しデータは前記データ利用者によってブラインド処理されたデータである。

【0109】

ステップ S 7 1 1 において、ブロックチェーンノードは、データ計算トランザクション要求において指定されたソースデータに基づいて、データ利用者がソースデータを使用する権限に対して認証操作を行う。

20

【0110】

選択的に、図 7 B における矢印 5 は本ステップの操作を示しており、すなわち、ブロックチェーンノード A 及びブロックチェーンノード B は、データ計算トランザクション要求において指定されたソースデータに基づいて、認証センターにデータ利用者が当該ソースデータを使用する認証要求を送信して、データ供給者により配置された権限によって当該認証要求を処理するように認証センターに要求し、認証センターからフィードバックされた認証結果を取得する。

【0111】

ステップ S 7 1 2 において、ブロックチェーンノードは、データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得する。

30

【0112】

ステップ S 7 1 3 において、ブロックチェーンノードは、データ計算トランザクション要求における計算タスクによって、プライバシースマートコントラクトを呼び出し、呼び出しデータ及びソースデータに対する計算を実行して、計算結果を取得する。

【0113】

ステップ S 7 1 4 において、ブロックチェーンノードは、データ計算トランザクション要求及び計算結果をアップリンクする。

【0114】

選択的に、図 7 B のブロックチェーンノード A とブロックチェーンノード B がステップ S 7 1 2 ~ S 7 1 4 の操作を実行し、具体的に、ブロックチェーンノード A 及びブロックチェーンノード B は、プライバシースマートコントラクトを呼び出して仮想マシン上で実行し、プライバシースマートコントラクトによって仮想マシンの組み込み関数を呼び出し、組み込み関数によって同期暗号化モジュールを呼び出してこのときの矢印 6 の操作、すなわち、呼び出しデータ及びソースデータに対する計算を実行し、データ計算トランザクション要求及び計算結果をアップリンクする操作を実行することができる。

40

【0115】

ステップ S 7 1 0 ~ S 7 1 4 の操作は図 7 B におけるブロックチェーンノード A 及びブロックチェーンノード B によって実行されていることに留意し、ここで、ブロックチェーンノード A は、データ計算トランザクション要求を事前実行するプロセスで上記操作を実

50

行し、ブロックチェーンノード B は、ブロックチェーンノード A の実行結果を検証するプロセスにおいて上記操作を実行する。

【0116】

ステップ S 7 1 5 において、データ利用者のブロックチェーンクライアントはアップリンクされた計算結果を取得する。

【0117】

ステップ S 7 1 6 において、データ利用者のブロックチェーンクライアントは、ソースデータのデータ供給者に準同型暗号化公開鍵を提供するように要求する。

【0118】

ステップ S 7 1 7 において、データ利用者のブロックチェーンクライアントは、準同型暗号化公開鍵を用いて計算結果に対し準同型復号化を行うとともに計算結果に対しブラインド除去処理を行って、平文の計算結果を取得する。

【0119】

選択的に、ブロックチェーンノードは、データ計算トランザクション要求及び計算結果に対するアップリンク操作を実行すると、図 7 B の矢印 7 のトランザクションブロードキャスト操作を実行し、その計算結果を他のブロックチェーンノードに通知する。このときデータ利用者はそのブロックチェーンクライアント 2 を介して図 7 B における矢印 8 の操作を実行し、すなわち、アップリンクされた計算結果を取得することができる。計算結果に使用されるソースデータが準同型暗号化されたソースデータであるので、このとき、ブロックチェーンクライアント 2 は、ソースデータのデータ供給者の準同型暗号化公開鍵を先に要求する必要がある、その後、プライバシースマートコントラクトを呼び出して仮想マシン上で実行し、プライバシースマートコントラクトによって仮想マシンの組み込み関数を呼び出し、組み込み関数によって同期暗号化モジュールを呼び出して準同型暗号化公開鍵を用いて計算結果を準同型復号化し、計算結果に対してブラインド除去処理を行って、最終の平文計算結果を得る。

【0120】

選択的に、ステップ S 7 0 8 におけるブラインド処理が呼び出しデータにランダム値を追加することを含む場合、本ステップのブラインド除去処理は計算結果から前記ランダム値を除去することを含む。

【0121】

本出願の実施例の手段は、データ供給者、データ利用者及びブロックチェーンノードの三端子がやり取りしてプライバシーデータを処理する手段を示したものであり、本実施例では、データ供給者のソースデータは準同型暗号化された後ブロックチェーンにアップリンク格納され、データ利用者はデータ計算タスクを開始する際に、ブロックチェーンノードが計算タスクを実行するとき、ソースデータ平文が公開されることなく呼び出しデータ平文が公開されるように、呼び出し関数に対しブラインド処理を行、それによりデータ利用者とデータ供給者のデータ安全性が保証され、同時に、計算結果が準同型復号化及びブラインド除去処理されることで、正確な平文の計算結果を得ることができ、ブロックチェーンのプライバシーデータ処理手段を極めて最適化することができる。

【0122】

図 8 は、本出願の実施例によるブロックチェーンのプライバシーデータ処理装置の構造概略図である。本出願の実施例はブロックチェーンにおけるプライバシーデータに対し計算処理を実行する場合に適用可能である。該装置は、本出願の実施例においてブロックチェーンノードによって実行される各ブロックチェーンのプライバシーデータ処理方法を実現することができる。該装置は、ブロックチェーンノードとしての電子機器に統合されてもよく、該装置 8 0 0 は具体的に以下を含む。

【0123】

データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得するためのトランザクション要求取得モジュール 8 0 1 であって、前記データ計算トランザクション要求における呼び出しデータは、前記データ

10

20

30

40

50

利用者によってブラインド処理されたデータであるトランザクション要求取得モジュール 801 と、前記データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得するためのソースデータ取得モジュール 802 と、前記データ計算トランザクション要求における計算タスクによって、前記プライバシースマートコントラクトを呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行して、計算結果を取得するための計算タスク処理モジュール 803 と、前記データ計算トランザクション要求及び計算結果をアップリンクし、前記データ計算トランザクション要求のデータ利用者にフィードバックし、前記データ利用者が前記計算結果に対して準同型復号化及びブラインド除去処理を行って、平文の計算結果を取得するためのアップリンク処理モジュール 804 とを備える。

10

【0124】

本出願の実施例の技術的手段は、ブロックチェーンノードが、データ利用者が開始したデータ計算トランザクション要求を取得した後、今回の計算タスクを実行するのに必要な準同型暗号化されたソースデータとブラインド処理された呼び出しデータとを取得し、プライバシースマートコントラクトを呼び出して今回の計算タスクを実行し、計算結果を得てブロックチェーンにアップリンク格納する。本出願の実施例において計算タスクの実行に使用されるソースデータはデータ供給者により準同型暗号化されたソースデータであり、データ供給者のデータの安全性が保証され、使用する呼び出しデータはデータ利用者によりブラインド処理されたデータであり、データ利用者のデータの安全性が保証され、最後に復号化処理とブラインド除去処理を行うことにより計算結果の正確性が保証される。

プライバシーデータ処理プロセス全体は通常のブロックチェーンノードを使用して完成することができ、同時に、データ供給者及びデータ利用者のデータの漏洩を引き起こすことなく、プライバシーデータ処理プロセスの公平性及び安全性を保証する。従って、ブロックチェーンのプライバシーデータ処理プロセスが最適化される。

20

【0125】

さらに、前記トランザクション要求取得モジュール 801 は、データ供給者によって前記プライバシースマートコントラクトに基づいて開始されたデータ公開トランザクション要求を取得するためにさらに用いられ、前記データ公開トランザクション要求におけるソースデータは準同型暗号化されたデータであり、前記アップリンク処理モジュール 804 は、さらに、前記プライバシースマートコントラクトを呼び出して前記データ公開トランザクション要求を実行して、前記ソースデータをブロックチェーンにアップリンク公開するために用いられる。

30

【0126】

さらに、前記ブラインド処理は呼び出しデータにランダム値を追加することを含み、前記ブラインド除去処理は計算結果から前記ランダム値を除去することを含む。

【0127】

さらに、前記装置は以下をさらに備える。

前記データ計算トランザクション要求において指定されたソースデータに基づいて、前記データ利用者が前記ソースデータを使用する権限に対して認証操作を行うための認証処理モジュールを備える。

40

【0128】

さらに、前記認証処理モジュールは以下を含む。

前記データ計算トランザクション要求において指定されたソースデータに基づいて、認証センターに前記データ利用者が前記ソースデータを使用する認証要求を送信して、データ供給者により配置された権限によって前記認証要求を処理するように前記認証センターに要求するための認証要求送信ユニットと、

前記認証センターからフィードバックされた認証結果を取得するための認証結果取得ユニットとを含む。

【0129】

さらに、前記計算タスク処理モジュール 803 は具体的に以下に用いられる。

50

前記プライバシースマートコントラクトを呼び出して仮想マシン上で実行し、前記プライバシースマートコントラクトに基づいて前記仮想マシンの組み込み関数を呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行するために用いられる。

【0130】

図9は、本出願の実施例によるブロックチェーンのプライバシーデータ処理装置の構造概略図である。本出願の実施例はブロックチェーンにおけるプライバシーデータに対して計算処理を実行する場合に適用可能である。該装置は、本出願の実施例においてブロックチェーンクライアントによって実行される各ブロックチェーンのプライバシーデータ処理方法を実現することができる。該装置は、ブロックチェーンクライアントが配置されている電子機器に統合されてもよく、該装置900は具体的に以下を備える。

10

【0131】

ブロックチェーンに公開された準同型暗号化データから計算タスクに必要なソースデータを決定するためのソースデータ決定モジュール901と、前記計算タスクの呼び出しデータをブラインド処理するためのブラインド処理モジュール902と、ブロックチェーンノードが配置したプライバシースマートコントラクトに基づいて、前記呼び出しデータ及びソースデータに対し前記計算タスクを実行するデータ計算トランザクション要求を開始し、前記ブロックチェーンノードに前記プライバシースマートコントラクトを呼び出して前記計算タスクを実行するように要求し、計算結果を取得するための計算要求開始モジュール903と、ブロックチェーンにアップリンクされた計算結果を取得するための計算結果取得モジュール904と、前記ソースデータのデータ供給者に準同型暗号化公開鍵を提供するように要求するための暗号化鍵取得モジュール905と、前記準同型暗号化公開鍵を用いて前記計算結果に対し準同型復号化を行うとともに前記計算結果に対しブラインド除去処理を行って、平文の計算結果を取得するための計算結果処理モジュール906とを備える。

20

【0132】

本出願の実施例の技術的手段は、データ利用者のブロックチェーンクライアントが、ブロックチェーンにすでに公開された準同型暗号化データから今回の計算に必要なソースデータを決定するとともに、今回の計算タスクのローカル呼び出しデータをブラインド処理し、呼び出しデータ及びソースデータに対し今回の計算タスクを実行するデータ計算トランザクション要求を開始して、ブロックチェーンノードに当該計算タスクを実行して計算結果を取得するように要求し、ブロックチェーンクライアントは計算結果を取得した後、まず、今回ソースデータを使用するデータ供給者の準同型暗号化公開鍵を取得するように要求した後、さらに準同型復号化及びブラインド除去処理を実行して、最終の平文の計算結果を取得する。本出願の実施例において、計算タスクの実行に使用されるデータ供給者のソースデータは準同型暗号化されたソースデータであり、データ供給者のデータの安全性が保証され、使用されるデータ利用者の呼び出しデータはブラインド処理されたデータであり、データ利用者のデータの安全性が保証されており、最後に復号化処理とブラインド除去処理を行うことにより、計算結果の正確性が保証される。計算プロセス全体においてデータ供給者及びデータ利用者のデータの漏洩を引き起こすことなく、計算プロセスの公平性及び安全性を保証した。従って、ブロックチェーンのプライバシーデータ処理プログラムが最適化される。

30

40

【0133】

さらに、前記ブラインド処理は呼び出しデータにランダム値を追加することを含み、前記ブラインド除去処理は計算結果から前記ランダム値を除去することを含む。

【0134】

さらに、前記装置は以下をさらに備える。

準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵と準同型暗号化公開鍵とを含む非対称準同型暗号化鍵を生成するための暗号化鍵生成モジュールと、前記準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵を用いて、提供されるソースデータを準同型暗号化するための準同型暗号化モジュールと、前記プライバシースマートコントラク

50

トに基づいて、前記ソースデータをブロックチェーンにアップリンクするデータ公開トランザクション要求を開始するためのアップリンク要求公開モジュールとを含む。

【0135】

さらに、前記装置は以下をさらに備える。

データ利用者の前記ソースデータ使用に対する認証を行うように、前記ソースデータの使用権限を認証センターに配置するための権限配置モジュールを備える。

【0136】

本出願の実施例によれば、本出願はさらに電子機器及び可読記憶媒体を提供している。

図10に示されるように、本出願の実施例のブロックチェーンのプライバシーデータ処理方法の電子機器のブロック図である。電子機器は、ラップトップコンピューター、デスクトップコンピューター、ワークベンチ、パーソナル・デジタル・アシスタント、サーバー、ブレードサーバー、メインフレームコンピューター、その他の適切なコンピュータなど、様々な形態のデジタルコンピューターを表すことを目的としている。電子機器は、パーソナル・デジタル・アシスタント、携帯電話、スマートフォン、ウェアラブルデバイス、及びその他類似のコンピューティングデバイスなど、様々な形態のモバイルデバイスを表すこともできる。本明細書に示されている部品、それらの接続と関係、及びそれらの機能は単なる例であり、本明細書で説明及び／又は要求されている本出願の実施を制限するものではない。

【0137】

図10に示されるように、該電子機器は、1つ又は複数のプロセッサ1001、メモリ1002、並びに、高速インターフェース及び低速インターフェースを含む様々な部品を接続するためのインターフェースを含む。各部品は、互いに異なるバスで接続されており、共通のマザーボードに実装されていてもよく、又は必要に応じて他の形態で実装されていてもよい。プロセッサは、電子機器内で実行される指令を処理することができ、メモリ内又はメモリに格納されて外部の入力／出力装置（インターフェースなどに接続されたディスプレイデバイス）にGUIのグラフィック情報を表示させる指令を含む。他の実施形態では、必要に応じて、複数のプロセッサ及び／又は複数のバスを複数のメモリ及び複数のメモリと共に使用してもよい。同様に、複数の電子機器を接続することができ、それぞれの機器はいくつかの必要な操作（例えば、サーバレイ、一組のブレードサーバ、又はマルチプロセッサシステムとして）を提供する。図10では一つのプロセッサ1001を例とする。

【0138】

メモリ1002は本出願による非一時的コンピュータ可読記憶媒体である。前記メモリは、少なくとも1つのプロセッサによって実行される指令を格納しており、前記少なくとも1つのプロセッサに本出願によるブロックチェーンのプライバシーデータ処理方法を実行させる。本出願の非一時的コンピュータ可読記憶媒体は、本出願によるブロックチェーンのプライバシーデータ処理方法をコンピュータに実行させるためのコンピュータ指令を格納する。

【0139】

メモリ1002は、非一時的コンピュータ可読記憶媒体として、本出願の実施例におけるブロックチェーンのプライバシーデータ処理方法に対応するプログラム指令／モジュール（例えば、図8に示すトランザクション要求取得モジュール801、ソースデータ取得モジュール802、計算タスク処理モジュール803及びアップリンク処理モジュール804、又は図9に示すソースデータ決定モジュール901、ブラインド処理モジュール902、計算要求開始モジュール903、計算結果取得モジュール904、暗号化鍵取得モジュール905及び計算結果処理モジュール906）など、非一時的なソフトウェアプログラム、非一時的なコンピュータ実行可能プログラム、及びモジュールを格納することができる。プロセッサ1001は、メモリ1002に格納されている非一時的なソフトウェアプログラム、指令及びモジュールを実行することにより、サーバの様々な機能アプリケーション及びデータ処理を実行し、すなわち、上記方法の実施例におけるブロックチェー

ンのプライバシーデータ処理方法を実現する。

【0140】

メモリ1002は、オペレーティングシステム、少なくとも1つの機能を実行するために必要なアプリケーションプログラムを格納し得るストレージプログラム領域と、ブロックチェーンのプライバシーデータ処理方法の電子機器の使用によって作成されたデータなどを格納し得るストレージデータ領域とを含むことができる。また、メモリ1002は、高速ランダムアクセスメモリを含んでもよく、さらに、例えば、少なくとも1つの磁気ディスク記憶デバイス、フラッシュメモリデバイス、又はその他の非一時的な固体メモリデバイスなどの非一時的メモリを含むことができる。いくつかの実施例において、メモリ1002は、プロセッサ1001に対して遠隔に設けられたメモリを任意選択で含んでもよく、これらのリモートメモリは、ネットワークを介してブロックチェーンのプライバシーデータ処理方法の電子機器に接続されてもよい。上記ネットワークの実例はインターネット、イントラネット、ローカルエリアネットワーク、モバイル通信ネットワーク及びそれらの組み合わせを含むがこれらに限定されない。

10

【0141】

ブロックチェーンのプライバシーデータ処理方法の電子機器はさらに入力装置1003及び出力装置1004を含むことができる。プロセッサ1001、メモリ1002、入力装置1003及び出力装置1004は、バス又はその他の形態で接続されていてもよく、図10ではバスを介して接続されている例を示している。

【0142】

20

入力装置1003は、入力されたデジタル又は文字情報を受け取り、ブロックチェーンのプライバシーデータ処理方法の電子機器のユーザ設定や機能制御に関するキー信号入力を生成することができ、例えば、タッチスクリーン、キーパッド、マウス、トラックパッド、タッチパネル、ポインティングスティック、1つ又は複数のマウスボタン、トラックボール、ジョイスティックなどの入力装置を含む。出力装置1004は、表示装置、補助照明装置（例えば、LED）、触覚フィードバック装置（例えば、振動モータ）などを含み得る。該ディスプレイデバイスは、液晶ディスプレイ（LCD）、発光ダイオード（LED）ディスプレイ及びプラズマディスプレイを含むがこれらに限定されない。いくつかの実施形態において、ディスプレイデバイスはタッチスクリーンであってもよい。

【0143】

30

ここで説明されるシステム及び技術の様々な実施形態はデジタル電子回路システム、集積回路システム、専用ASIC（特定用途向け集積回路）、コンピュータハードウェア、ファームウェア、ソフトウェア、及び／又はそれらの組み合わせにおいて実現することができる。これら様々な実施形態は以下を含むことができる。一つ又は複数のコンピュータプログラムにおいて実施され、該一つ又は複数のコンピュータプログラムは少なくとも一つのプログラマブルプロセッサを含むプログラム可能なシステムで実行、及び／又は解釈されてもよく、該プログラマブルプロセッサは、専用又は汎用のプログラマブルプロセッサであってよく、ストレージシステム、少なくとも1つの入力装置、及び少なくとも1つの出力装置からデータ及び指令を受信するとともに、データ及び指令を該ストレージシステム、該少なくとも1つの入力装置、及び該少なくとも1つの出力装置に伝送することができる。

40

【0144】

これらのコンピュータプログラム（プログラム、ソフトウェア、ソフトウェアアプリケーション、又はコードとも呼ばれる）は、プログラマブルプロセッサの機械指令を含み、これらのコンピュータプログラムを高度なプロセス及び／又はオブジェクト指向プログラミング言語、及び／又はアセンブリ／機械言語で実施することができる。本明細書で使用されているように、用語「機械可読媒体」及び「コンピュータ可読媒体」は、機械指令及び／又はデータをプログラマブルプロセッサに提供するための任意のコンピュータプログラム製品、デバイス及び／又は装置（例えば、磁気ディスク、光ディスク、メモリ、プログラマブルロジックデバイス（PLD））を意味し、機械可読信号としての機械指令を受

50

信する機械可読媒体を含む。用語「機械可読信号」は機械指令及び／又はデータをプログラマブルプロセッサに提供するための任意の信号を指す。

【0145】

ユーザとのインタラクションを提供するために、コンピュータ上で、明細書で説明したシステム及び技術を実施してもよく、該コンピュータは、ユーザに情報を表示するための表示装置（例えば、CRT（カソードレイチューブ）又はLCD（液晶ディスプレイ）モニタ）、及びユーザがコンピュータに入力を提供するためのキーボード及びポインティングデバイス（例えば、マウス又はトラックボール）を有する。他の種類の装置はユーザとのインタラクションを提供するために用いられてもよく、例えば、ユーザへのフィードバックは任意の形態のセンシングフィードバック（例えば、視覚フィードバック、聴覚フィードバック、又は触覚フィードバック）であってもよく、任意の形態（音響入力、音声入力又は触覚入力を含む）でユーザからの入力を受信することができる。

10

【0146】

本明細書で説明されるシステム及び技術は、バックグラウンドコンポーネントを含むコンピューティングシステム（例えば、データサーバーとして）、又は、ミドルウェアコンポーネントを含むコンピューティングシステム（例えば、アプリケーションサーバー）、又は、フロントエンドコンポーネント（例えば、グラフィカルユーザインタフェース又はウェブブラウザを備えたユーザーコンピュータは、ユーザが該グラフィカルユーザインタフェース又は該ウェブブラウザを介して、本明細書で説明するシステム及び技術の実施形態と対話することができる）、又は、これらのバックグラウンドコンポーネント、ミドルウェアコンポーネント又はフロントエンドコンポーネントの任意の組み合わせを含むコンピューティングシステムで実施することができる。また、システムのコンポーネントは、任意の形態又は媒体のデジタルデータ通信（例えば、通信ネットワーク）を介して相互に接続することができる。通信ネットワークの例示として、ローカルエリアネットワーク（LAN）、ワイドエリアネットワーク（WAN）及びインターネットを含む。

20

【0147】

コンピュータシステムにはクライアント及びサーバを含むことができる。クライアントとサーバは一般的に互いに離れており、通常は通信ネットワークを介して相互作用する。クライアントとサーバとの関係は、対応するコンピュータにおいて実行されるとともに互いにクライアント-サーバの関係を持つコンピュータプログラムによって生成される。

30

【0148】

本出願の実施例の技術的手段によれば、データ利用者のブロックチェーンクライアントが、ブロックチェーンにすでに公開された準同型暗号化データから今回の計算に必要なソースデータを決定するとともに、今回の計算タスクのローカル呼び出しデータをブラインド処理し、呼び出しデータ及びソースデータに対し今回の計算タスクを実行するデータ計算トランザクション要求を開始して、ブロックチェーンノードに当該計算タスクを実行して計算結果を取得するように要求し、ブロックチェーンクライアントは計算結果を取得した後、まず、今回ソースデータを使用するデータ供給者の準同型暗号化公開鍵を取得するように要求した後、計算結果に対し準同型復号化及びブラインド除去処理を実行して、最終の平文の計算結果を取得する。本出願の実施例において、計算タスクの実行に使用されるデータ供給者のソースデータは準同型暗号化されたソースデータであり、データ供給者のデータの安全性が保証され、使用されるデータ利用者の呼び出しデータはブラインド処理されたデータであり、データ利用者のデータの安全性が保証され、最後に復号化処理とブラインド除去処理を行うことにより、計算結果の正確性が保証される。計算プロセス全体においてデータ供給者及びデータ利用者のデータの漏洩を引き起こすことなく、計算プロセスの公平性及び安全性を保証する。従って、ブロックチェーンのプライバシーデータ処理プログラムが最適化される。

40

【0149】

上記に示した様々な形態のプロセスを用いて、ステップを順番変更したり、追加したり又は削除したりすることができることを理解されたい。本出願が開示する技術的手段の望

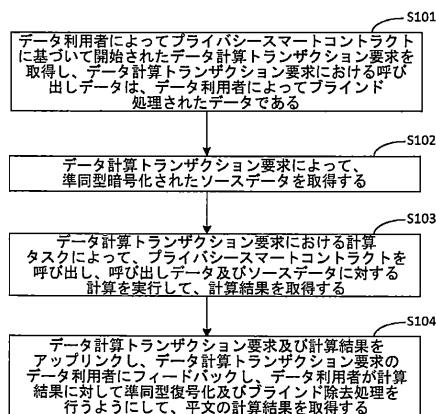
50

ましい結果を実現することができれば、例えば、本出願に記載された各ステップは並行して又は順番通りに又は異なる順番で実行されてもよく、本明細書はこれに対して制限しない。

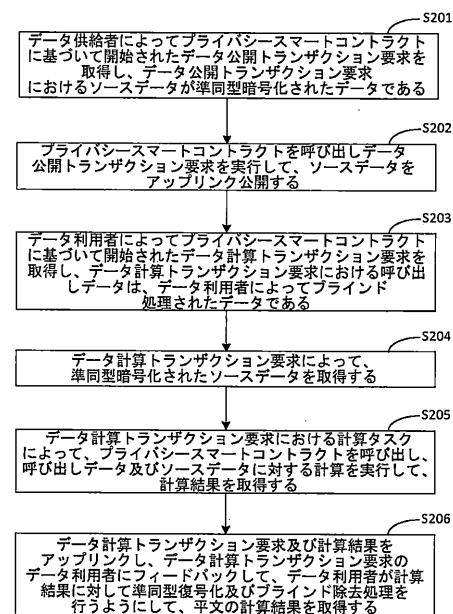
【0150】

上述した具体的な実施形態は、本出願の保護範囲を制限するものではない。当業者は、設計要件及び他の要因に応じて、様々な修正、組み合わせ、サブ組み合わせ及び置き換えが可能であることを理解すべきである。本出願の精神及び原則の範囲内で行われた如何なる修正、同等の置き換え及び改善などはいずれも本出願の保護範囲内に含まれるべきである。

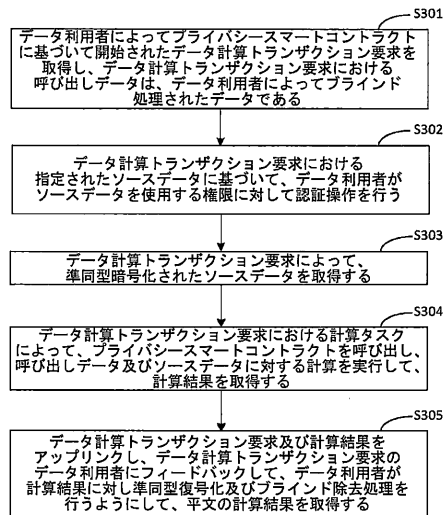
【図 1】



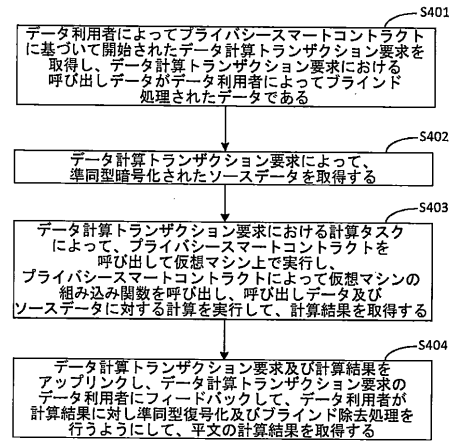
【図 2】



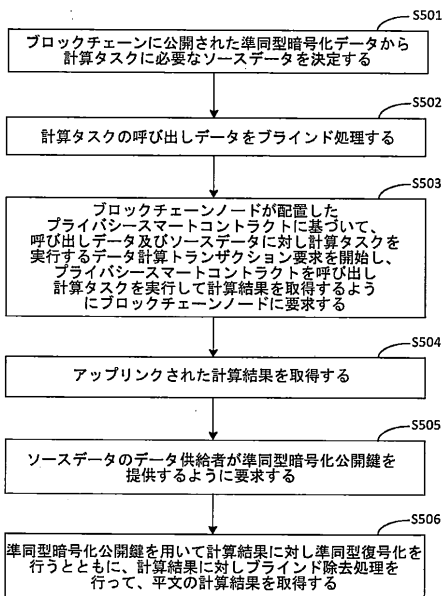
【図 3】



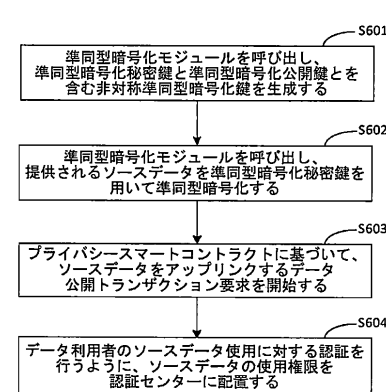
【図 4】



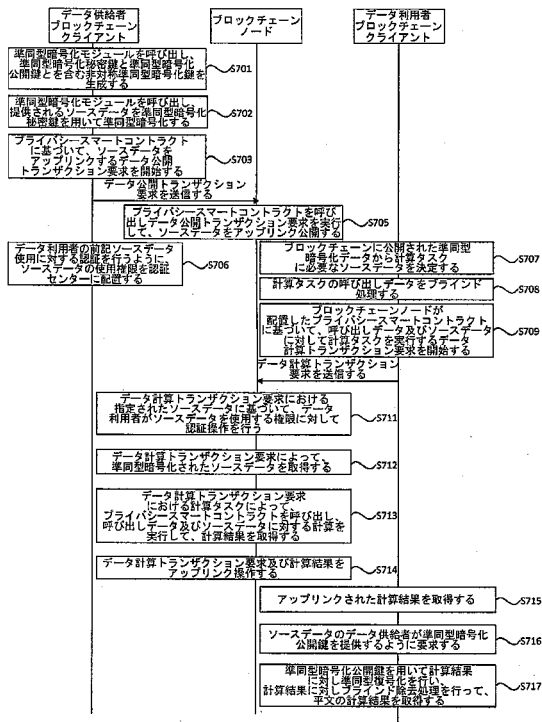
【図 5】



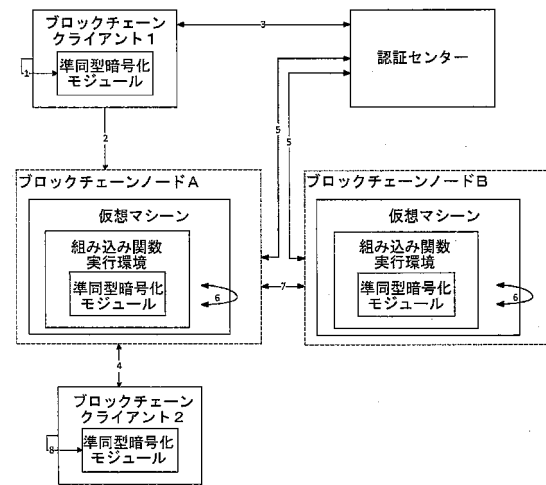
【図 6】



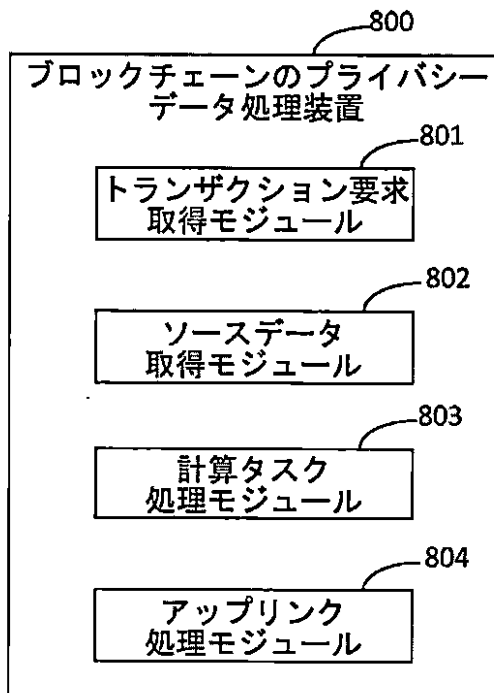
【図 7 A】



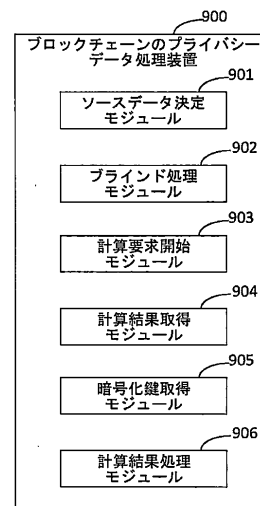
【図 7 B】



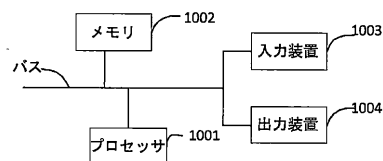
【図 8】



【図 9】



【図 10】



【手続補正書】

【提出日】令和3年5月14日(2021.5.14)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

ブロックチェーンノードによって実行される、ブロックチェーンのプライバシーデータ処理方法であって、

データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得するステップであって、前記データ計算トランザクション要求における呼び出しデータは、前記データ利用者によってブラインド処理されたデータである、ステップと、

前記データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得するステップと、

前記データ計算トランザクション要求における計算タスクによって、前記プライバシースマートコントラクトを呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行して、計算結果を取得するステップと、

前記データ計算トランザクション要求及び計算結果をアップリンクして、前記データ計算トランザクション要求のデータ利用者にフィードバックすることにより、前記データ利用者が前記計算結果に対して準同型復号化及びブラインド除去処理を行って、平文の計算結果を取得するステップとを含む、方法。

【請求項 2】

データ供給者によって前記プライバシースマートコントラクトに基づいて開始されたデータ公開トランザクション要求を取得するステップであって、前記データ公開トランザクション要求におけるソースデータは準同型暗号化されたデータである、ステップと、

前記プライバシースマートコントラクトを呼び出し前記データ公開トランザクション要求を実行して、前記ソースデータをアップリンク公開するステップとをさらに含む、請求項 1 に記載の方法。

【請求項 3】

前記ブラインド処理は呼び出しデータにランダム値を追加することを含み、前記ブラインド除去処理は計算結果から前記ランダム値を除去することを含む、請求項 1 に記載の方法。

【請求項 4】

データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得した後に、さらに、

前記データ計算トランザクション要求において指定されたソースデータに基づいて、前記データ利用者が前記ソースデータを使用する権限に対して認証操作を行うステップを含む、請求項 1 に記載の方法。

【請求項 5】

前記データ計算トランザクション要求において指定されたソースデータに基づいて、前記データ利用者が前記ソースデータを使用する権限に対して認証操作を行うステップは、

前記データ計算トランザクション要求において指定されたソースデータに基づいて、認証センターに前記データ利用者が前記ソースデータを使用する認証要求を送信して、データ供給者により設けられた権限によって前記認証要求を処理するように前記認証センターに要求するステップと、

前記認証センターからフィードバックされた認証結果を取得するステップとを含む、請求項 4 に記載の方法。

【請求項 6】

前記プライバシースマートコントラクトを呼び出し前記呼び出しデータ及び前記ソースデータに対する計算を実行する過程において、さらに、

前記プライバシースマートコントラクトを呼び出して仮想マシン上で実行するとともに、前記プライバシースマートコントラクトによって前記仮想マシンの組み込み関数を呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行するステップを含む、請求項 1 に記載の方法。

【請求項 7】

ブロックチェーンクライアントによって実行される、ブロックチェーンのプライバシーデータ処理方法であって、

ブロックチェーンで公開された準同型暗号化データから計算タスクに必要なソースデータを決定するステップと、

前記計算タスクの呼び出しデータをブラインド処理するステップと、

ブロックチェーンノードによって設けられたプライバシースマートコントラクトに基づいて、前記呼び出しデータ及びソースデータに対して前記計算タスクを実行するデータ計算トランザクション要求を開始することにより、前記プライバシースマートコントラクトを呼び出し前記計算タスクを実行して計算結果を取得するように、前記ブロックチェーンノードに要求するステップと、

アップリンクされた計算結果を取得するステップと、

前記ソースデータのデータ供給者に準同型暗号化公開鍵を提供するように要求するステップと、

前記準同型暗号化公開鍵を用いて前記計算結果に対して準同型復号化を行うとともに、前記計算結果に対してブラインド除去処理を行って、平文の計算結果を取得するステップとを含む、方法。

【請求項 8】

前記ブラインド処理は呼び出しデータにランダム値を追加することを含み、前記ブラインド除去処理は計算結果から前記ランダム値を除去することを含む、請求項 7 に記載の方法。

【請求項 9】

準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵と準同型暗号化公開鍵とを含む非対称準同型暗号化鍵を生成するステップと、

前記準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵を用いて、提供されるソースデータを準同型暗号化するステップと、

前記プライバシースマートコントラクトに基づいて、前記ソースデータをアップリンクするデータ公開トランザクション要求を開始するステップとをさらに含む、請求項 7 に記載の方法。

【請求項 10】

前記ソースデータをアップリンクするデータ公開トランザクション要求を開始するステップの後に、さらに、

データ利用者の前記ソースデータの使用に対する認証を行うために、前記ソースデータの使用権限を認証センターに設けるステップを含む、請求項 9 に記載の方法。

【請求項 11】

ブロックチェーンノードに設けられる、ブロックチェーンのプライバシーデータ処理装置であって、

データ利用者によってプライバシースマートコントラクトに基づいて開始されたデータ計算トランザクション要求を取得するためのトランザクション要求取得モジュールであって、前記データ計算トランザクション要求における呼び出しデータは、前記データ利用者によってブラインド処理されたデータである、トランザクション要求取得モジュールと、

前記データ計算トランザクション要求によって、準同型暗号化されたソースデータを取得するためのソースデータ取得モジュールと、

前記データ計算トランザクション要求における計算タスクによって、前記プライバシースマートコントラクトを呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行して、計算結果を取得するための計算タスク処理モジュールと、

前記データ計算トランザクション要求及び計算結果をアップリンクして、前記データ計算トランザクション要求のデータ利用者にフィードバックすることにより、前記データ利用者が前記計算結果に対して準同型復号化及びブラインド除去処理を行って、平文の計算結果を取得するためのアップリンク処理モジュールとを備える、装置。

【請求項 12】

前記トランザクション要求取得モジュールは、さらに、データ供給者によって前記プライバシースマートコントラクトに基づいて開始されたデータ公開トランザクション要求を取得するように構成され、前記データ公開トランザクション要求におけるソースデータは準同型暗号化されたデータであり、

前記アップリンク処理モジュールは、さらに、前記プライバシースマートコントラクトを呼び出し前記データ公開トランザクション要求を実行して、前記ソースデータをアップリンク公開するように構成される、請求項 11 に記載の装置。

【請求項 13】

前記ブラインド処理は呼び出しデータにランダム値を追加することを含み、前記ブラインド除去処理は計算結果から前記ランダム値を除去することを含む、請求項 11 に記載の装置。

【請求項 14】

前記データ計算トランザクション要求において指定されたソースデータに基づいて、前記データ利用者が前記ソースデータを使用する権限に対して認証操作を行うための認証処理モジュールをさらに備える、請求項 11 に記載の装置。

【請求項 15】

前記認証処理モジュールは、

前記データ計算トランザクション要求において指定されたソースデータに基づいて、認証センターに前記データ利用者が前記ソースデータを使用する認証要求を送信して、データ供給者により設けられた権限によって前記認証要求を処理するように前記認証センターに要求するための認証要求送信ユニットと、

前記認証センターからフィードバックされた認証結果を取得するための認証結果取得ユニットとを含む、請求項 14 に記載の装置。

【請求項 16】

前記計算タスク処理モジュールは、

前記プライバシースマートコントラクトを呼び出して仮想マシン上で実行するとともに、前記プライバシースマートコントラクトによって前記仮想マシンの組み込み関数を呼び出し、前記呼び出しデータ及び前記ソースデータに対する計算を実行するように構成される、請求項 11 に記載の装置。

【請求項 17】

ブロックチェーンクライアントに設けられる、ブロックチェーンのプライバシーデータ処理装置であって、

ブロックチェーンで公開された準同型暗号化データから計算タスクに必要なソースデータを決定するためのソースデータ決定モジュールと、

前記計算タスクの呼び出しデータをブラインド処理するためのブラインド処理モジュールと、

ブロックチェーンノードによって設けられたプライバシースマートコントラクトに基づいて、前記呼び出しデータ及びソースデータに対して前記計算タスクを実行するデータ計算トランザクション要求を開始することにより、前記プライバシースマートコントラクトを呼び出して前記計算タスクを実行して計算結果を取得するように、前記ブロックチェーンノードに要求するための計算要求開始モジュールと、

アップリンクされた計算結果を取得するための計算結果取得モジュールと、

前記ソースデータのデータ供給者に準同型暗号化公開鍵を提供するように要求するための暗号化鍵取得モジュールと、

前記準同型暗号化公開鍵を用いて前記計算結果に対して準同型復号化を行うとともに、前記計算結果に対してブラインド除去処理を行って、平文の計算結果を取得するための計算結果処理モジュールとを含む、装置。

【請求項 18】

前記ブラインド処理は呼び出しデータにランダム値を追加することを含み、前記ブラインド除去処理は計算結果から前記ランダム値を除去することを含む、請求項 17 に記載の装置。

【請求項 19】

準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵と準同型暗号化公開鍵とを含む非対称準同型暗号化鍵を生成するための暗号化鍵生成モジュールと、

前記準同型暗号化モジュールを呼び出して、準同型暗号化秘密鍵を用いて、提供されるソースデータを準同型暗号化するための準同型暗号化モジュールと、

前記プライバシースマートコントラクトに基づいて、前記ソースデータをアップリンクするデータ公開トランザクション要求を開始するためのアップリンク要求公開モジュールとをさらに含む、請求項 17 に記載の装置。

【請求項 20】

データ利用者の前記ソースデータの使用に対する認証を行うために、前記ソースデータの使用権限を認証センターに設けるための権限設置モジュールをさらに含む、請求項 19 に記載の装置。

【請求項 21】

少なくとも 1 つのプロセッサと、

前記少なくとも 1 つのプロセッサに通信可能に接続されるメモリとを備える電子機器であって、

前記メモリに前記少なくとも 1 つのプロセッサにより実行される指令が格納されており、前記指令が前記少なくとも 1 つのプロセッサにより実行されて、前記少なくとも 1 つのプロセッサに請求項 1～6 又は 7～10 のいずれか 1 項に記載のブロックチェーンのプライバシーデータ処理方法を実行させる、電子機器。

【請求項 22】

コンピュータ指令が格納されている非一時的コンピュータ可読記憶媒体であって、

前記コンピュータ指令は、前記コンピュータに請求項 1～6 又は 7～10 のいずれか 1 項に記載のブロックチェーンのプライバシーデータ処理方法を実行させる、非一時的コンピュータ可読記憶媒体。

【請求項 23】

コンピュータプログラムであって、

前記コンピュータプログラムがプロセッサにより実行されると、請求項 1～6 又は 7～10 のいずれか 1 項に記載のブロックチェーンのプライバシーデータ処理方法を実現させるコンピュータプログラム。

フロントページの続き

(72)発明者 ドゥアン・ビン

中華人民共和国、100085 ベイジン ハイディエン ディストリクト、シャンディ 10
イーエイチ ストリート、バイドゥ キャンパス、ナンバー 10、3／フロア

(72)発明者 シアオ・ウェイ

中華人民共和国、100085 ベイジン ハイディエン ディストリクト、シャンディ 10
イーエイチ ストリート、バイドゥ キャンパス、ナンバー 10、3／フロア

【外国語明細書】
2021189431000001.pdf