

明 細 書

発明の名称：

情報処理システム、情報処理方法、サーバ、ブロックチェーンノード、及びプログラム

技術分野

[0001] 本開示は、情報処理システム、情報処理方法、サーバ、ブロックチェーンノード、及びプログラムに関する。

背景技術

[0002] 従来、移動対象のアイテムのトラッキング情報のデータ量を低減させつつ、アイテムのトラッキング情報をブロックチェーンへ記録する技術が知られている（例えば、特開2021-64219号公報）。特開2021-64219号公報に開示されている技術では、サーバが、追跡対象のアイテムの識別情報を含む要求信号を受け付けた場合、要求信号に含まれる識別情報に対応するアイテムの移動を行ったトランザクションデータの系列と、トランザクションデータの系列に対応するアキュムレータの系列とをブロックチェーンから取得する。そして、サーバは、取得したアキュムレータの系列のうちの各アキュムレータに追跡対象のアイテムの識別情報が格納されているか否かの検証を行い、検証結果を出力する。

発明の概要

発明が解決しようとする課題

[0003] ところで、商品又はサービスであるアイテムを利用するユーザは、そのアイテムがどのような要素によって構成されているのか知りたい場合がある。例えば、ある工業製品が製造される場合を考える。なお、工業製品は様々な原料（例えば、レアメタル等）を含んで構成されることが多い。

[0004] 特に、近年では国際連合によって持続可能な開発目標（SDGs：Sustainable Development Goals）が定められ、地球環境に配慮したアイテムの提供が求められている。このため、アイテムを構成する要素が地球環境に配慮したも

のであるかを検証することができれば、その検証結果をSDGs指標として利用することもできると考えられる。しかし、同種の原料を使った加工品又は工業製品に関しては、その外観等から違いを見分けることは難しい。その一方で、アイテムの原料に関する情報（又はエネルギーが供給された過程に関する情報）が追跡可能な状態となれば、それらの情報に基づく指標の設定、測定、及び評価が可能になり、それらの指標が所定の基準を満たさないアイテムの移動を制限することも可能になる。

[0005] なお、工業製品が消費者へ供給されるまでには、複数の事業者により原料及び中間素材のサプライチェーンが形成されることが多い。例えば、ある事業者Aは、複数の原料a 1, a 2, a 3を調達し、それらの原料a 1, a 2, a 3から中間素材M_Aを製造する。次に、事業者Bは、事業者Aから中間素材M_Aを調達し、その中間素材M_Aに対して原料b 1, b 2を添加して中間素材M_Bを製造する。次に、事業者Cは、事業者Bから中間素材M_Bを調達し、その中間素材M_Bと他のいくつかの異なる中間素材とを組み合わせる工業製品M_Cを製造する。そして、事業者Cから消費者へ工業製品M_Cが供給される。

[0006] この場合、例えば、消費者又は品質検査を行う機関等は、工業製品M_Cに含まれている原料の原産地、リサイクル素材の含有率、精製過程で測定された純度、及び元素又は分子等の成分の配合比率等に関する情報を知りたい場合がある。さらに、消費者又は流通を監督する機関等は、工業製品M_Cがどのような事業者を経て製造及び供給されたのかに関する情報も知りたい場合がある。また、各事業者も、自らが調達した原料又は部品に関する情報を知りたい場合がある。

[0007] 仮に、このような取引対象のアイテムに関連するデータをブロックチェーン等のネットワーク技術を用いて公開すれば、複数の事業者及び消費者は、取引対象に関連する情報を自由に閲覧することができる。例えば、複数の事業者及び消費者は、ある部品に含まれている原料の原産地、リサイクル素材の含有率、精製過程で測定した純度、及び元素又は分子等の成分の配合比率等に関する情報を閲覧することにより、自らが取得した部品又は中間素材等

がどのような原料によって構成されているのかを確認して、自らが出荷する製品の表示に利用することや、自らが目標に設定した基準に適合しない部品又は中間素材等を見分けることに利用することができる。

[0008] しかし、このようなデータがブロックチェーンに記録され、そのデータが公開されると、不特定多数の第三者がそのデータを自由に閲覧することが可能となる。例えば、ブロックチェーンに記録されそのデータに工業製品を製造する際のノウハウに関するデータが含まれてしまうと、その事業者の競争力が損なわれてしまう可能性がある。

[0009] 例えば、ある特定の事業者は、原料の配合比率に関する情報を競合する事業者には秘密にしたいと考え、その情報は直接取引する契約関係にある事業者へは開示してもよいが契約関係にない第三者へは開示したくない、と考えている場合もある。

[0010] 本開示は、上記の事情を鑑みてなされたもので、アイテムに含まれている原料の数量を秘密にしつつ、アイテムに含まれる原料の取引に不正がないことを検証することを目的とする。

課題を解決するための手段

[0011] 上記の目的を達成するために本開示に係る情報処理システムは、サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムであって、前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、前記サーバが、前記原料に対応するパラメータ値と前記数量データとに基づき秘密計算をすることにより、前記生成対象アイテムのコミットメント値を計算し、前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含

まれているトランザクションデータである第1トランザクションデータを取得し、前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、複数のブロックチェーンノードの各々が、前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの前記原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、情報処理システムである。

[0012] また、本開示のサーバは、サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムにおける前記サーバであって、前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、前記サーバが、前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムのコミットメント値を計算し、前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、前記ブロックチェーンノードの記憶部に格納されている

ブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得し、前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、複数のブロックチェーンノードの各々が、前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基いて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの前記原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、サーバである。

[0013] また、本開示のブロックチェーンノードは、サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムにおける前記ブロックチェーンノードであって、前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、前記サーバが、前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムの

コミットメント値を計算し、前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得し、前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、複数のブロックチェーンノードの各々が、前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの前記原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、ブロックチェーンノードである。

[0014] また、本開示の情報処理方法は、サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムが実行する情報処理方法であって、前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテム

の識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、前記サーバが、前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムのコミットメント値を計算し、前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得し、前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、複数のブロックチェーンノードの各々が、前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの前記原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、情報処理方法である。

[0015] 本開示のプログラムは、サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムにおける前記サーバに実行させるためのプログラムであって、前記端末が、生成対象アイテムの識別情報を表す生成

対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、前記サーバが、前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムのコミットメント値を計算し、前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得し、前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクシヨ

ンデータを、複数のブロックチェーンノードへブロードキャストし、複数のブロックチェーンノードの各々が、前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの前記原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、プログラムである。

[0016] 本開示のプログラムは、サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムにおける前記ブロックチェーンノードに実行させるためのプログラムであって、前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、前記サーバが、前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムのコミットメント値を計算し、前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得し、前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、複数のブロックチェーンノードの各々が、前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トラン

ザクションデータの前記原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、プログラムである。

発明の効果

[0017] 本開示によれば、アイテムに含まれている原料の数量を秘密にしつつ、アイテムに含まれる原料の取引に不正がないことを検証することができる、という効果が得られる。

図面の簡単な説明

[0018] [図1]本実施形態の情報処理システムの概略構成の一例を示す図である。
[図2]情報処理システムを構成する各装置として機能するコンピュータの概略ブロック図である。
[図3]本実施形態の情報処理システムの処理を説明するための説明図である。
[図4]本実施形態を説明するための図である。

発明を実施するための形態

[0019] 以下、図面を参照して実施形態を詳細に説明する。

[0020] <情報処理システムのシステム構成>

[0021] 図1は、本実施形態の情報処理システム10を示すブロック図である。図1に示されるように、本実施形態の情報処理システム10は、端末12と、サーバ14と、ブロックチェーンノード16とを含んで構成されている。情報処理システム10の各装置は、例えばインターネット等のネットワーク20によって接続されている。なお、複数のブロックチェーンノード16A、16B、16Cのうちの特定のノードを説明する場合以外は、ブロックチェーンノードを単に「ブロックチェーンノード16」と表記する。また、複数の端末12A、12B、12C、・・・、12Xのうちの特定の端末を説明する場合以外は、端末を単に「端末12」と表記する。

[0022] なお、図1には、3つのブロックチェーンノードが示されているが、より多くのブロックチェーンノードが含まれていても良い。また、図1には、4つの端末が示されているが、より多くの端末が含まれていても良い。

- [0023] 近年、商品又はサービス（以下、単に「アイテム」とも称する。）の生産又は流通の過程で起きた事象の一部を公開するように求められるケースが増加している。例えば、環境問題への取り組みのエビデンスとして、各事業者がアイテムを提供した際の再生エネルギーの利用率、CO₂排出量、又はそのアイテムに用いられている原料のリサイクル率の数値を公開するように求められる場合もある。
- [0024] 現在、このような情報の公開は、一定期間（例えば、１年間）における企業活動の総和として報告されることが多い。その一方で、個々のアイテムに対して明細を付加すれば、それらの情報はアイテムの付加価値とみなすこともできる。また、アイテムに対して明細を付加することにより、そのアイテムが国際社会での流通規制に対して適合していることを証明することも可能となる。
- [0025] そこで、ある事業者U１から別の事業者U２へアイテムXが引き渡され、事業者U２がアイテムXに基づいて新たなアイテムYを製造した場合に、それら一連の事象を１つの取引伝票を表すデータとして表現する場合を考える。そして、取引伝票を表すデータをブロックチェーンへ記録する。取引伝票を表すデータは複数のブロックチェーンノード16A、16B、16Cの記憶部（図示省略）へ格納されるため、ブロックチェーンに記録されたトランザクションデータは公開される。第三者はそのトランザクションデータを閲覧可能となる。これにより、アイテムに明細が付与され、アイテムが製造又は提供される際の一連の情報が公開されることになる。
- [0026] しかし、その一方で、アイテムが製造又は提供される際の情報の中には秘匿しておきたい情報も存在する。例えば、複数の原料を混合させて中間素材を製造している事業者にとっては、原料の混合比率に関する情報は自社のノウハウでもあり、秘匿しておきたいと考えることが想定される。これらのノウハウに関する情報は、各事業者の知的財産でもあるため、各事業者はその知的財産が第三者に無償で公開されるのは避けたいと考えることが一般的である。

- [0027] そこで、本実施形態の情報処理システム１０では、アイテムに含まれている原料の数量に関する情報はブロックチェーンに記録せずに、アイテムに含まれている原料の数量を秘密にしつつ、アイテムに含まれる原料の取引に不正がないことを検証する。
- [0028] 具体的には、本実施形態の情報処理システム１０では、アイテムに含まれている原料の数量を表す数量データと原料毎に設定されたパラメータ値とに基づいて、所定の秘密計算を実行することにより、アイテム毎のコミットメント値を計算する。本実施形態の情報処理システム１０では、このコミットメント値をブロックチェーンに記録し、コミットメント値に基づいて各アイテムに含まれる原料の取引に不正がないことを検証する。これにより、アイテムに含まれている原料の数量に関する情報はブロックチェーンに記録せずに、アイテムに含まれている原料の数量を秘密にしつつ、アイテムに含まれる原料の取引に不正がないことを検証することが可能となる。
- [0029] 情報処理システム１０に含まれる各装置は、ＣＰＵ（Central Processing Unit）、各処理ルーチンを実現するためのプログラム等を記憶したＲＯＭ（Read Only Memory）、データを一時的に記憶するＲＡＭ（Random Access Memory）、記憶手段としてのメモリ、ネットワークインタフェース等を含んだコンピュータによって実現される。
- [0030] 端末１２、サーバ１４、及びブロックチェーンノード１６は、例えば、図２に示すコンピュータ７０で実現することができる。コンピュータ７０はＣＰＵ７１、一時記憶領域としてのメモリ７２、及び不揮発性の記憶部７３を備える。また、コンピュータ７０は、入出力装置等（図示省略）が接続される入出力interface（Ｉ／Ｆ）７４、及び記録媒体に対するデータの読み込み及び書き込みを制御するread/write（Ｒ／Ｗ）部７５を備える。また、コンピュータ７０は、インターネット等のネットワークに接続されるネットワークＩ／Ｆ７６を備える。ＣＰＵ７１、メモリ７２、記憶部７３、入出力Ｉ／Ｆ７４、Ｒ／Ｗ部７５、及びネットワークＩ／Ｆ７６は、バス７７を介して互いに接続される。

[0031] 記憶部 73 は、Hard Disk Drive (HDD)、solid state drive (SSD)、フラッシュメモリ等によって実現できる。記憶媒体としての記憶部 73 には、コンピュータ 70 を機能させるためのプログラムが記憶されている。CPU 71 は、プログラムを記憶部 73 から読み出してメモリ 72 に展開し、プログラムが有するプロセスを順次実行する。

[0032] <情報処理システム 10 の作用>

[0033] 次に、本実施形態の情報処理システム 10 の作用について説明する。本実施形態では、情報処理システム 10 が、プロダクト C の明細をブロックチェーンへ記録する場合を例に説明する。

[0034] なお、プロダクト C は、その原料としてコバルトとニッケルとマンガンとを含んで構成されているものとする。以下では、プロダクト A 及びプロダクト B から、プロダクト C の原料であるコバルトとニッケルとマンガンとを抽出し、抽出された原料を利用してプロダクト C を生成する場合を例に説明する。なお、プロダクト C が生成される過程において、プロダクト A を構成する原料の一部（又は全部）又はプロダクト B を構成する原料の一部（又は全部）が消費されず、消費されない余りの原料に相当するプロダクト D が生成される場合を例に説明する。このため、プロダクト A、B は生成元アイテムの一例であり、プロダクト C は生成対象アイテムの一例である。

[0035] 本実施形態では、アイテムであるプロダクトとその原料（例えば、プロダクト C は、原料であるコバルト：5，ニッケル：4，マンガン：9 によって構成されている点）との組み合わせが追跡可能となる。なお、その際には、原料の数量データは秘匿される必要がある。その一方で、第三者に対しては、例えば、プロダクト C はプロダクト A とプロダクト B とから生成されていることを証明する必要がある。

[0036] そこで、本実施形態では、アイテムを構成する原料の数量データを秘匿しつつ、アイテムが適切に製造されていることを証明可能とする。以下、具体的に説明する。

[0037] 端末 12 を操作するユーザが、生成対象アイテムであるプロダクト C に関

する情報を端末１２へ入力すると、図３に示されるシーケンスが実行される。

[0038] ステップＳ１００において、端末１２は、ユーザから入力されたアイテムに関する情報を受け付ける。なお、このアイテムに関する情報には、例えば、生成対象のアイテムであるプロダクトＣを構成する原料の数量を表す数量データが含まれている。なお、例えば、プロダクトＣを構成している原料の数量（又は構成比）は以下であるとする。

[0039] コバルト：５
ニッケル：４
マンガン：９

[0040] また、生成元アイテムであるプロダクトＡを構成している原料の数量は以下であるとする。

[0041] コバルト：３
ニッケル：７
マンガン：５

[0042] また、生成元アイテムであるプロダクトＢを構成している原料の数量は以下であるとする。

[0043] コバルト：４
マンガン：８

[0044] また、消費されない余りの原料に相当するプロダクトＤを構成している原料の数量は以下であるとする。

[0045] コバルト：２
ニッケル：３
マンガン：４

[0046] ステップＳ１０２において、端末１２は、生成対象のプロダクトＣの識別情報を表すアイテム識別データ（以下、単に「アイテムＩＤ」と称する。）と、生成元のプロダクトＡのアイテムＩＤと、生成元のプロダクトＢのアイテムＩＤと、プロダクトＣを構成する原料の識別情報である原料識別データ

(以下、単に「原料 I D」と称する。)と、プロダクト C を生成する際に消費される原料の数量 (又は比率) を表す数量データとを、サーバ 14 へ送信する。

[0047] ステップ S 104 において、サーバ 14 は、ステップ S 102 で端末 12 から送信されたデータを受信する。また、ステップ S 104 において、サーバ 14 は、受信した原料 I D の原料に対応するパラメータ値と、ブラインドファクターに対応するブラインドパラメータ値 G と、ブラインドパラメータ値 G に対するランダムな係数 r とを取得する。ブラインドファクター $r G$ は、プロダクト C には実際には含まれていない仮想的な原料を表すデータである。ブラインドパラメータ値 G に対するランダムな係数 r は、ブラインドファクターの数量に対応するブラインド数量データの値でもある。

[0048] なお、このパラメータ値及びブラインドパラメータ値 G は、加法準同型性のあるコミットメントスキームを用いた計算によって求められる。例えば、既知の手法の一例である Pedersen commitment (例えば、https://link.springer.com/content/pdf/10.1007%2F3-540-46766-1_9.pdf#page=3! の Section 3 を参照。)を用いて、パラメータ値及びブラインドパラメータ値 G が計算される。Pedersen commitment を用いてパラメータ値及びブラインドパラメータ値 G が計算される場合、楕円曲線上の離散対数が未知の点 (座標) が各原料に対応するパラメータ値及びブラインドパラメータ値 G として選択される。これにより、加法準同型性を有するパラメータ値及びブラインドパラメータ値 G が取得される。例えば、各原料のパラメータ値として以下が取得される。

[0049] コバルト : H_C

ニッケル : H_N

マンガン : H_M

ブラインドパラメータ値 : G

[0050] なお、生成元アイテムであるプロダクト A のコミットメント値 C_A と、生成元アイテムであるプロダクト B のコミットメント値 C_B とは、以下の式に従っ

て計算される。 r_1 , r_2 は、ブラインドパラメータ値Gに対するランダムな係数である。これらコミットメント値 C_A , C_B は、後述するようにブロックチェーンにおける過去のトランザクションデータに記録されている。

[0051] [数1]

$$C_A = r_1 G + 3H_C + 7H_N + 5H_M$$

$$C_B = r_2 G + 4H_C + 0H_N + 8H_M$$

[0052] ステップS106において、サーバ14は、以下の式に示されているように、各原料に対応するパラメータ値 H_C , H_N , H_M 及びブラインドパラメータ値Gと、各原料の数量データ及びブラインドパラメータ値Gに対するランダムな係数 r_3 とを積和演算する秘密計算を実行することにより、プロダクトCのコミットメント値 C_C を計算する。

[0053] [数2]

$$C_C = r_3 G + 5H_C + 4H_N + 9H_M$$

[0054] なお、上記のコミットメント値は、離散対数が未知である楕円曲線上の1点に相当する。このため、上記のコミットメント値 C_C からは、プロダクトCに原料がどれくらい含まれているのかを計算することはできない。

[0055] また、ステップS106において、サーバ14は、以下の式に示されているように、各原料に対応するパラメータ値 H_C , H_N , H_M 及びブラインドパラメータ値Gと、各原料の数量データ及びブラインドパラメータ値Gに対するランダムな係数 r_4 とを積和演算する秘密計算を実行することにより、プロダクトDのコミットメント値 C_D を計算する。

[0056] [数3]

$$C_D = r_4 G + 2H_C + 3H_N + 4H_M$$

[0057] なお、ブラインドファクター r Gを導入せずにコミットメント値を計算する場合には、異なるアイテムが同一数量の原料又は同一の原料比によって構

成されている場合にコミットメント値が同一の値となる。ブラインドファクター r_G を導入することにより、異なるアイテムが同一数量の原料又は同一の原料比によって構成されている場合であっても、異なるアイテムのコミットメント値を異なるものとすることが可能となる。

[0058] また、後述する以下の式 (A) を成立させるために、以下の式 (B) が満たされるように、ランダムな係数 r_1, r_2, r_3, r_4 は予め調整されて設定される。

[0059] [数4]

$$C_A + C_B - (C_C + C_D) = 0G$$

(A)

$$r_1 + r_2 - (r_3 + r_4) = 0$$

(B)

[0060] ステップS108において、サーバ14は、プロダクトCのアイテムIDと各原料の原料IDとの組み合わせを、例えば、特開2021-064219号公報に開示されているアキュムレータへ格納する。アキュムレータに各種データが格納されることにより、アイテムのトラッキング情報のデータ量を低減させつつ、アイテムのトラッキング情報をブロックチェーンへ記録することが可能となる。また、サーバ14は、同様に、プロダクトDのアイテムIDと各原料の原料IDとの組み合わせも、所定のデータ構造に格納する。

[0061] なお、前述したように、サーバ14は、パラメータ値 H_C, H_N, H_M 及びブラインドパラメータ値 G を設定する。パラメータ値 H_C, H_N, H_M 及びブラインドパラメータ値 G と、原料の組み合わせに対応する数量データ及びランダ

ムな係数とに基づいて計算されたコミットメント値は、他の原料の組み合わせで計算されたコミットメント値と異なりユニークである。このため、コミットメント値は、識別データとしても利用可能である。コミットメント値を計算する際に使用されたパラメータ値 H_C 、 H_N 、 H_M 及びブラインドパラメータ値 G は、サーバ14の記憶部（図示省略）へ格納され管理される。

[0062] 次に、サーバ14は、ブロックチェーンノード16へアクセスすることにより、生成元のプロダクトAのアイテムIDをアウトプットデータに含むアキュムレータが記録されているトランザクションデータと、生成元のプロダクトBのアイテムIDをアウトプットデータに含むアキュムレータが記録されているトランザクションデータとを取得する。なお、サーバ14は、トランザクションデータに付与されているトランザクションIDに基づき、トランザクションデータを取得する。

[0063] 具体的には、ステップS110において、サーバ14は、生成元のプロダクトAのアイテムIDと生成元のプロダクトBのアイテムIDとをアウトプットデータに含むアキュムレータが記録されているトランザクションデータを取得するために、ブロックチェーンノード16に対して要求信号を送信する。

[0064] ステップS112において、ブロックチェーンノード16は、上記ステップS110でサーバ14から送信された要求信号を受信すると、プロダクトAのアイテムIDがアウトプット情報として記録されている過去のトランザクションデータと、プロダクトBのアイテムIDがアウトプットデータとして記録されている過去のトランザクションデータとを、サーバ14へ送信する。本実施形態では、このような過去のトランザクションデータを第1トランザクションデータとも称する。

[0065] ステップS114において、サーバ14は、ブロックチェーンノード16から出力された第1トランザクションデータを取得する。

[0066] ステップS116において、サーバ14は、生成対象のアイテムであるプロダクトCの送り元を表すアドレスとプロダクトCの送り先を表すアドレス

と上記のデータ構造とを含むトランザクションデータである第2トランザクションデータを生成する。

[0067] 具体的には、サーバ14は、第2トランザクションデータのインプットデータに、過去の第1トランザクションデータのアウトプットデータを含める。なお、サーバ14は、過去の第1トランザクションデータに関するブロックチェーン上でのトランザクションIDも、第2トランザクションデータのインプットデータに含めるようにして第2トランザクションデータを生成する。また、サーバ14は、第2トランザクションデータを構成するアウトプットデータに、プロダクトCのアイテムIDと原料IDとコミットメント値とを含める。なお、上述したように、プロダクトCのアイテムIDと原料IDとは、所定のデータ構造であるアキュムレータに格納される。なお、コミットメント値をアキュムレータへ更に格納してもよい。本実施形態では、アイテムIDと原料IDとをアキュムレータへ格納する場合を例に説明するが、アイテムIDと原料IDとをアキュムレータへは格納せずに、そのまま第2トランザクションデータを構成するアウトプットデータに記録するようにしてもよい。

[0068] なお、上述したように、プロダクトCを生成する過程において、原料の一部（又は全部）が消費されない場合には、消費されない余りの原料に相当するプロダクトDに関するデータもアキュムレータに含ませる。この記録の方法は、インプットデータが表す原料とアウトプットデータが表す原料との間の保存則を1つのトランザクションデータ内において表現する実装例の1つである。他の方法としては、生成対象のアイテムを生成する際に発生した余りの原料である廃棄物を別のブロックチェーンに記録し、異なるブロックチェーンの間で参照する実装例も考えられる。

[0069] 図4に、トランザクションデータのデータ構造を説明するための図を示す。図4に示されているように、トランザクションデータTX2には、プロダクトの送り元を表すアドレスとプロダクトの送り先を表すアドレスが含まれている。

- [0070] さらに、図4に示されているように、トランザクションデータTX2のインプットデータには、過去のトランザクションデータTX1-1のアウトプットデータと、過去のトランザクションデータTX1-2のアウトプットデータとが含まれている。
- [0071] 一方で、図4に示されているように、トランザクションデータTX2のアウトプットデータには、生成対象のプロダクトCのアイテムIDと原料IDを含むアキュムレータが含まれている。さらに、このアキュムレータには、余りの原料により生成されるプロダクトDのアイテムID及び原料IDも含まれている。また、生成元アイテムのトランザクションデータであるトランザクションデータTX1-1とトランザクションデータTX1-2のアウトプットデータには、過去に生成対象であったプロダクトA、BのアイテムIDと原料IDとが格納されているアキュムレータが含まれている。
- [0072] ステップS118において、サーバ14は、ステップS118で生成された第2トランザクションデータを、複数のブロックチェーンノード16へブロードキャストする。
- [0073] ステップS120において、複数のブロックチェーンノード16の各々は、第2トランザクションデータを受信する。ステップS120において、複数のブロックチェーンノード16の各々は、第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出す。具体的には、複数のブロックチェーンノード16の各々は、第2トランザクションデータに含まれている、過去の第1トランザクションデータに関するブロックチェーン上での識別データに基づいて、所定のプロトコルに則り、ブロックチェーンから第1トランザクションデータの各々を読み出す。
- [0074] ステップS122において、複数のブロックチェーンノード16の各々は、第2トランザクションデータTX2に含まれるプロダクトCのコミットメント値C_c及び余りのプロダクトDのコミットメント値C_dと、第1トランザクションデータTX1-1に含まれるプロダクトAのコミットメント値C_a及

び第1トランザクションデータTX1-2に含まれるプロダクトBのコミットメント値C_Bとの間の関係性に基づいて、第2トランザクションデータTX2の生成対象アイテムであるプロダクトCが、第1トランザクションデータTX1-1, TX1-2の生成元アイテムであるプロダクトA, Bの原料によって構成されているか否かを検証する。

[0075] 上述したように、Pedersen commitmentによって各パラメータ値及びブラインドファクターが生成されている場合には、第2トランザクションデータ内のインプットデータに含まれる過去のトランザクションデータのコミットメント値と、アウトプットデータに含まれるコミットメント値とが等しくなるはずである。このため、例えば、第2トランザクションデータ内のインプットデータに含まれるコミットメント値の総和と、第2トランザクションデータ内のアウトプットデータに含まれるコミットメント値の総和とが等しくない場合には、生成対象のアイテムは何らかの事情により適切に生成されていないことになる。

[0076] このため、複数のブロックチェーンノード16の各々は、第1トランザクションデータ内のアウトプットデータに含まれるコミットメント値の総和（第2トランザクションデータ内のインプットデータに含まれるコミットメント値の総和）と、第2トランザクションデータ内のアウトプットデータに含まれるコミットメント値の総和とが等しい場合に、第2トランザクションデータをブロックチェーンへ記録する。

[0077] 一方、複数のブロックチェーンノード16の各々は、第1トランザクションデータ内のアウトプットデータに含まれるコミットメント値の総和（第2トランザクションデータ内のインプットデータに含まれるコミットメント値の総和）と、第2トランザクションデータ内のアウトプットデータに含まれるコミットメント値の総和とが等しくない場合には、第2トランザクションデータをブロックチェーンへ記録せずに破棄する。

[0078] なお、例えば、アウトプットデータに複数のアイテムIDが含まれている場合には、トランザクションデータのアウトプットデータに含まれている複

数のコミットメント値の合計値がブロックチェーン上において公開される。

- [0079] 具体的には、複数のブロックチェーンノード16の各々は、以下の計算式に示されているように、第2トランザクションデータTX2に含まれるプロダクトCのコミットメント値 C_C とプロダクトCを生成する際に発生する原料の余りに相当するコミットメント値 C_D との和が、複数の第1トランザクションデータTX1-1, TX-2に含まれる原料のコミットメント値の総和(C_A と C_B との和)と等しい場合に、第2トランザクションデータTX2のプロダクトCが複数の第1トランザクションデータTX1-1, TX-2の原料によって構成されていると判定する。

- [0080] [数5]

$$C_A + C_B - (C_C + C_D) = 0$$

- [0081] ステップS124において、複数のブロックチェーンノード16の各々は、第2トランザクションデータTX2のプロダクトCが、第1トランザクションデータTX1-1, TX-2の原料によって構成されていると判定した場合に、第2トランザクションデータTX2をブロックチェーンへ記録する。

- [0082] なお、トランザクションデータに記載されるコミットメント値によっては、各ブロックチェーンノード16が実施するコミットメント値の加算処理の際にオーバーフローが発生し、誤った計算結果が得られる可能性がある。そのため、コミットメント値が適正な範囲内にあることの証明(プルーフ)を含める方が好ましい。この実施に、例えば、Range proofを含めることができる。既知の手法の一例として、Borromean Ring Signatures (<https://www.semanticscholar.org/paper/Borromean-Ring-Signatures-%E2%88%97-Maxwell-Poelstra/4160470c7f6cf05ffc81a98e8fd67fb0c84836ea>) や、Bulletproofs (<https://eprint.iacr.org/2017/1066.pdf>) などの証明スキームを利用できる。

- [0083] なお、サーバ14は、原料IDに対応するパラメータ値の開示要求を表す

要求信号を端末12から受け付けた場合、要求信号の送信元の端末12との間において認証処理を実行する。そして、サーバ14は、要求信号の送信元の端末12が、パラメータ値の開示について予め許可されている端末である場合に、要求信号の送信元の端末12へパラメータ値を開示する。この端末12は、開示されたパラメータ値と、トランザクションデータに記録されているコミットメント値とに基づいて、プロダクトCが適切に製造されたものであるか否かを検証する。

[0084] 例えば、生成対象のプロダクトCを受け取ったユーザは、プロダクトCが適切な原料に基づいて製造されたのか否かを確かめるために、ブロックチェーンに記録されているコミットメント値を用いてデコミットを実施する。

[0085] なお、コミットメント値の計算にPedersen commitmentを用いた場合には、以下の手順に従ってデコミットが実施され得る。

[0086] 具体的には、例えば、プロダクトCを受け取ったユーザ又は第三者であるユーザが操作する端末12Xは、ユーザの操作に応じてサーバ14に対して所定の要求信号を送信する。サーバ14は、要求信号に応答して、上述した認証処理を経て、パラメータ値 H_C 、 H_N 、 H_M と、原料の数量データ（コバルト：5、ニッケル：4、マンガン：9）と、ブラインドファクター r_G とを、当該ユーザが操作する端末12Xへ送信する。また、端末12Xは、ブロックチェーンノード16へアクセスし、第2トランザクションデータに記録されているプロダクトCのコミットメント値 C_C を取得する。

[0087] 端末12Xは、パラメータ値 H_C 、 H_N 、 H_M と、原料の数量データ（コバルト：5、ニッケル：4、マンガン：9）と、ブラインドファクター r_G と、ブロックチェーンに記録されている第2トランザクションデータのコミットメント値 C_C とに基づいて、既知のデコミット方法を用いて、プロダクトCはプロダクトA、Bから適切に製造されたものか否かを表す検証結果を生成する。端末12Xは、第2トランザクションデータに記録されているプロダクトCのコミットメント値 C_C が原料の数量データに基づいて算出されており、

かつ、プロダクトCがプロダクトA、Bから適切に製造されたもの（以下、単に「プロダクトCが適切に生成」と称する）である場合には、その旨の検証結果を表示部（図示省略）へ表示する。一方、端末12Xは、プロダクトCが適切に生成されたものでない場合には、その旨の検証結果を表示部（図示省略）へ表示する。

[0088] なお、プロダクトCを受け取ったユーザは、プロダクトCを生成したユーザからプロダクトCの成分表等を受け取っている可能性が高い。そのため、プロダクトCを受け取ったユーザが操作する端末12Xは、成分表等に記録されている原料の数量データ（コバルト：5、ニッケル：4、マンガン：9）と、パラメータ値 H_C 、 H_N 、 H_M と、ブラインドファクター r_G とに基づいて、プロダクトCのコミットメント値 C_C' を自ら計算することも可能である。このため、プロダクトCを受け取ったユーザが操作する端末12Xは、自ら計算したコミットメント値 C_C' とブロックチェーンに記録されているコミットメント値 C_C とを比較して、プロダクトCが適切に生成されたものか否かを表す検証結果を生成するようにしてもよい。

[0089] なお、ブラインドファクター r_G に関しては、プロダクトCを受け取るユーザが操作する端末12Xが生成し、生成した各値をサーバ14へ送信するようにしてもよい。この場合には、ステップS104において、プロダクトCを受け取るユーザが操作する端末12Xがブラインドファクター r_G をサーバ14へ送信する。

[0090] また、ブラインドファクター r_G を端末12Xへは開示せずに、既知のデコミット方法を用いて、各コミットメント値からブラインドファクター r_G を減算した減算値と、ブラインドファクター r_G から生成したデジタル署名とに基づいて、プロダクトCが適切に生成されたものか否かを表す検証結果を生成することもできる。

[0091] なお、コミットメント値の計算にKZG commitment（例えば、<https://www.iaacr.org/archive/asiacrypt2010/6477178/6477178.pdf>を参照。）を用いることも可能である。Pedersen commitmentを利用した場合、デコミットする際は

、コミットメント値に含まれる原料の数量データを公開する必要がある。これに対し、多項式を利用したコミットメントスキームであるKZG commitmentを利用すると、一部の原料の数量データのみを公開することも可能である。

[0092] 具体的には、コミットメント値の計算にKZG commitmentを用いた場合には、アイテムを構成する一部の原料に限って数量データを公開することが可能一方で、その他の原料の数量データは秘匿することが可能となる。コミットメント値の計算にKZG commitmentを用いる場合には、多項式を用いてコミットメント値が計算される。なお、コミットメント値の計算にKZG commitmentを用いた場合には、加法準同型性の性質により、異なる多項式を用いて計算されたコミットメント値を加算することができる。

[0093] コミットメント値の計算にKZG commitmentを用いる場合、対象の原材料を表すパラメータ値とブラインドパラメータ値とを x とし、多項式 $f(x)$ によって計算される値を対象の原材料の量及びブラインドファクター値として、多項式 $f(x)$ を構成し、その多項式についてKZG commitmentを生成して、原材料とその量を秘匿したコミットメント値を作成する。

[0094] なお、多項式を構成する際に上述したブラインドパラメータ値を含めないようにしてもよい。

[0095] なお、上述した例では、Pedersen commitment及びKZG commitmentをコミットメント値の計算に利用する場合を例に説明したが、加法準同型性のあるコミットメントスキームであればどのようなコミットメントスキームであっても利用することができる。

[0096] 以上説明したように、本実施形態に係る情報処理システムの端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとをサーバへ送信する。サーバは、原料に対応するパラメータ値と数量データとに基づく秘密計算をすることにより、生成対象アイテ

ムのコミットメント値を計算する。サーバは、コミットメント値と原料識別データと生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納する。サーバは、ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得する。そして、サーバは、生成対象アイテムの送り元を表すアドレスと生成対象アイテムの送り先を表すアドレスとデータ構造とを含むトランザクションデータであって、生成元アイテム識別データがインプットデータに含まれ、かつ生成対象アイテム識別データを含むデータ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストする。複数のブロックチェーンノードの各々は、サーバによりブロードキャストされた第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出す。複数のブロックチェーンノードの各々は、第2トランザクションデータに含まれる生成対象アイテムのコミットメント値と、第1トランザクションデータに含まれる生成元アイテムのコミットメント値との間の関係性に基づいて、第2トランザクションデータのアイテムが、第1トランザクションデータの生成元アイテムに含まれる原料によって構成されているか否かを検証し、第2トランザクションデータの生成対象アイテムが第1トランザクションデータの原料によって構成されていると判定した場合に、第2トランザクションデータをブロックチェーンへ記録する。これにより、アイテムに含まれている原料の数量を秘密にしつつ、アイテムに含まれる原料の取引に不正がないことを検証することができる。

[0097] また、アイテムのコミットメント値を計算する際に、ブラインドファクター rG を導入することにより、異なるアイテムのコミットメント値が同一の値となることを防止することができる。

[0098] なお、本開示は、上述した実施形態に限定されるものではなく、この発明

の要旨を逸脱しない範囲内で様々な変形や応用が可能である。

[0099] 例えば、アイテムとしては現実物に限らず特定のデータも含まれる。

[0100] また、上記実施形態では、コミットメント値を計算する際に、ブラインドファクター r_G を導入する場合を例に説明したが、これに限定されるものではない。ブラインドファクター r_G を導入せずに、コミットメント値を計算するようにしてもよい。

[0101] また、上記実施形態では、上記式 (B) が満たされるように、ランダムな係数 r_1, r_2, r_3, r_4 は予め調整される場合を例に説明したが、これに限定されるものではない。ランダムな係数 r_1, r_2, r_3, r_4 が上記式 (B) を満たさない場合には、以下の式の右辺に相当する値に対してデジタル署名を付加することにより、既知の手法を用いて、生成対象のプロダクトが生成元のプロダクトから適切に製造されているか否かを検証することもできる。

[0102] [数6]

$$C_A + C_B - (C_C + C_D) = (r_1 + r_2 - (r_3 + r_4))G$$

[0103] この場合には、上述したように、サーバ14は、生成対象のプロダクトCのコミットメント値を計算する際に、ブラインドファクター r_G を用いて生成対象のプロダクトCのコミットメント値 C_C を計算する。そして、サーバ14は、第2トランザクションデータに含まれる生成対象のプロダクトCのコミットメント値 C_C と、原料の余りに相当するコミットメント値 C_D との和 ($C_C + C_D$) と、複数の第1トランザクションデータに含まれる生成元のプロダクトA, Bのコミットメント値の総和 ($C_A + C_B$) との間の差分を表す情報に対して、サーバ14のデジタル署名を生成し、そのデジタル署名を第2トランザクションデータへ追加する。これにより、 $(C_A + C_B) - (C_C + C_D)$ の演算結果が0とならない場合であっても、その演算結果にはデジタル署名が付加されているため、そのデジタル署名を元に生成対象のプロダクトが生成元のプロダクトから適切に製造されているか否かを検証することができ

る。

- [0104] また、上記実施形態では、プロダクトCを生成する際に消費されない余りの原料に相当するプロダクトDが生成される場合を例に説明したが、これに限定されるものではなく、余りの原料が発生しない場合であっても本実施形態を適用することが可能である。
- [0105] また、上記実施形態では、サーバ14が各種処理を実行する場合を例に説明したが、それらの各種処理の一部又は全部を、端末12又はブロックチェーンノード16が実行するようにしてもよい。
- [0106] また、本願明細書中において、プログラムが予めインストールされている実施形態として説明したが、当該プログラムを、コンピュータ読み取り可能な記録媒体に格納して提供することも可能である。例えば、プログラムは、CD-ROM (Compact Disk Read Only Memory)、DVD-ROM (Digital Versatile Disk Read Only Memory)、及びUSB (Universal Serial Bus) メモリ等の非一時的 (non-transitory) 記憶媒体に記憶された形態で提供されてもよい。また、プログラムは、ネットワークを介して外部装置からダウンロードされる形態としてもよい。
- [0107] なお、上記実施形態でCPUがソフトウェア (プログラム) を読み込んで実行した処理を、CPU以外の各種のプロセッサが実行してもよい。この場合のプロセッサとしては、FPGA (Field-Programmable Gate Array) 等の製造後に回路構成を変更可能なPLD (Programmable Logic Device)、及びASIC (Application Specific Integrated Circuit) 等の特定の処理を実行させるために専用に設計された回路構成を有するプロセッサである専用電気回路等が例示される。または、プロセッサとしては、GPGPU (General-purpose graphics processing UNIT) を用いてもよい。また、各処理を、これらの各種のプロセッサのうちの1つで実行してもよいし、同種又は異種の2つ以上のプロセッサの組み合わせ (例えば、複数のFPGA、及びCPUとFPGAとの組み合わせ等) で実行してもよい。また、これらの各種のプロセッサのハードウェア的な構造は

、より具体的には、半導体素子等の回路素子を組み合わせた電気回路である。

[0108] また、本実施形態の各処理を、汎用演算処理装置及び記憶装置等を備えたコンピュータ又はサーバ等により構成して、各処理がプログラムによって実行されるものとしてもよい。このプログラムは記憶装置に記憶されており、磁気ディスク、光ディスク、半導体メモリ等の記録媒体に記録することも、ネットワークを通して提供することも可能である。もちろん、その他いかなる構成要素についても、単一のコンピュータやサーバによって実現しなければならないものではなく、ネットワークによって接続された複数のコンピュータに分散して実現してもよい。

[0109] 本明細書に記載された全ての文献、特許出願、および技術規格は、個々の文献、特許出願、および技術規格が参照により取り込まれることが具体的かつ個々に記された場合と同程度に、本明細書中に参照により取り込まれる。

[0110] なお、上記実施形態においては、「××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。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。

[0111] また、何らかの方法、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、開示の技術の各態様は、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、当該方法等を本開示の技術の各態様の範囲外とするものではない。

[0112] 2022年3月31日に出願された日本国特許出願2022-061015号及び2023年2月9日に出願された日本国特許出願2023-018759号の開示は、その全体が参照により本明細書に取り込まれる。本明細書に記載された全ての文献、特許出願、および技術規格は、個々の文献、特許出願、および技術規格が参照により取

り込まれることが具体的かつ個々に記された場合と同程度に、本明細書中に参照により取り込まれる。

請求の範囲

- [請求項1] サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムであって、
- 前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、
- 前記サーバが、
- 前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムのコミットメント値を計算し、
- 前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、
- 前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得し、
- 前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、
- 複数のブロックチェーンノードの各々が、
- 前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、

前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの前記原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、
情報処理システム。

[請求項2]

前記複数のブロックチェーンノードは、前記第2トランザクションデータの前記生成対象アイテムが複数の前記第1トランザクションデータの前記原料によって構成されているか否かを検証する際に、

前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と前記生成対象アイテムを生成する際に発生する前記原料の余りに相当するコミットメント値との和が、複数の前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値の総和と等しい場合に、前記第2トランザクションデータの前記生成対象アイテムが複数の前記第1トランザクションデータの前記原料によって構成されていると判定する、

請求項1に記載の情報処理システム。

[請求項3]

前記サーバは、前記パラメータ値の開示要求を表す要求信号を受け付けた場合、前記要求信号の送信元の端末との間において認証処理を実行し、前記要求信号の送信元の端末が前記パラメータ値の開示について予め許可されている端末である場合に、前記要求信号の送信元の端末へ前記パラメータ値を開示する、

請求項1又は請求項2に記載の情報処理システム。

[請求項4]

前記サーバは、前記生成対象アイテムのコミットメント値を計算す

る際に、

前記生成対象アイテムには実際には含まれていない原料を表すブラインドファクターに対応するブラインドパラメータ値と予め調整された前記ブラインドファクターの数量を表すブラインド数量データとの積和演算の結果を、前記パラメータ値と前記数量データとの積和演算の結果へ加算することにより、前記生成対象アイテムのコミットメント値を計算する、

請求項 1 ～請求項 3 の何れか 1 項に記載の情報処理システム。

[請求項5]

前記サーバは、前記生成対象アイテムのコミットメント値を計算する際に、

前記生成対象アイテムには実際には含まれていない原料を表すブラインドファクターに対応するブラインドパラメータ値とランダムな前記ブラインドファクターの数量を表すブラインド数量データとの積和演算の結果を、前記パラメータ値と前記数量データとの積和演算の結果へ加算することにより、前記生成対象アイテムのコミットメント値を計算し、

前記第 2 トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と前記生成対象アイテムを生成する際に発生する前記原料の余りに相当するコミットメント値との和と、複数の前記第 1 トランザクションデータに含まれる前記生成元アイテムのコミットメント値の総和との間の差分を表す情報に対して、前記サーバのデジタル署名を生成し、前記デジタル署名を前記第 2 トランザクションデータへ追加する、

請求項 1 ～請求項 3 の何れか 1 項に記載の情報処理システム。

[請求項6]

前記サーバは、前記生成対象アイテムのコミットメント値を計算する際に、

前記生成対象アイテムには実際には含まれていない原料を表すブラインドファクターに対応するブラインドパラメータ値と予め調整され

た前記ブラインドファクターの数量を表すブラインド数量データとを前記秘密計算の入力に追加して、前記生成対象アイテムのコミットメント値を計算することで秘匿性を向上させる、

請求項 1 ～請求項 3 の何れか 1 項に記載の情報処理システム。

[請求項 7]

前記コミットメント値を計算する際に、多項式を利用したコミットメントスキームである KZG commitment を利用して、一部の原料の数量データのみを公開可能とする、

請求項 1 に記載の情報処理システム。

[請求項 8]

サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムにおける前記サーバであって、

前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、

前記サーバが、

前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムのコミットメント値を計算し、

前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、

前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第 1 トランザクションデータを取得し、

前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデ

ータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、

複数のブロックチェーンノードの各々が、

前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、

前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、

サーバ。

[請求項9]

サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムにおける前記ブロックチェーンノードであって、

前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、

前記サーバが、

前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムのコミットメント値を計算し、

前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、

前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得し、

前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、

複数のブロックチェーンノードの各々が、

前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、

前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの前記原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、

ブロックチェーンノード。

[請求項10]

サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムが実行する情報処理方法であって、

前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、

前記サーバが、

前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムのコミットメント値を計算し、

前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、

前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得し、

前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、

複数のブロックチェーンノードの各々が、

前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、

前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、

前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの前記原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、

情報処理方法。

[請求項11]

サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムにおける前記サーバに実行させるためのプログラムであって、

前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、

前記サーバが、

前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムのコミットメント値を計算し、

前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、

前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得し、

前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデ

ータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、

複数のブロックチェーンノードの各々が、

前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、

前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、

プログラム。

[請求項12]

サーバと、複数のブロックチェーンノードと、複数の端末とを含む情報処理システムにおける前記ブロックチェーンノードに実行させるためのプログラムであって、

前記端末が、生成対象アイテムの識別情報を表す生成対象アイテム識別データと、生成対象アイテムを生成する際に使用される原料の識別情報である原料識別データと、前記原料の数量を表す数量データと、生成元アイテムの識別情報を表す生成元アイテム識別データとを前記サーバへ送信し、

前記サーバが、

前記原料に対応するパラメータ値と前記数量データとに基づく秘密計算をすることにより、前記生成対象アイテムのコミットメント値を

計算し、

前記原料識別データと前記生成対象アイテム識別データとの組み合わせを所定のデータ構造へ格納し、

前記ブロックチェーンノードの記憶部に格納されているブロックチェーンに記録されているトランザクションデータであって、かつ前記生成元アイテム識別データがアウトプットデータに含まれているトランザクションデータである第1トランザクションデータを取得し、

前記生成対象アイテムの送り元を表すアドレスと前記生成対象アイテムの送り先を表すアドレスと前記データ構造とを含むトランザクションデータであって、前記生成元アイテム識別データがインプットデータに含まれ、かつ前記生成対象アイテム識別データを含む前記データ構造がアウトプットデータに含まれる第2トランザクションデータを、複数のブロックチェーンノードへブロードキャストし、

複数のブロックチェーンノードの各々が、

前記サーバによりブロードキャストされた前記第2トランザクションデータに紐づく過去のトランザクションデータである第1トランザクションデータの各々をブロックチェーンから読み出し、

前記第2トランザクションデータに含まれる前記生成対象アイテムのコミットメント値と、前記第1トランザクションデータに含まれる前記生成元アイテムのコミットメント値との間の関係性に基づいて、前記第2トランザクションデータの前記生成対象アイテムが、前記第1トランザクションデータの前記生成元アイテムに含まれる前記原料によって構成されているか否かを検証し、前記第2トランザクションデータの前記生成対象アイテムが前記第1トランザクションデータの前記原料によって構成されていると判定した場合に、前記第2トランザクションデータを前記ブロックチェーンへ記録する、

プログラム。