

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7066096号

(P7066096)

(45)発行日 令和4年5月13日(2022.5.13)

(24)登録日 令和4年5月2日(2022.5.2)

(51)国際特許分類

F I

G 0 6 F 21/64 (2013.01)

G 0 6 F 21/64

H 0 4 L 9/32 (2006.01)

H 0 4 L 9/32

2 0 0 Z

請求項の数 16 (全30頁)

(21)出願番号	特願2020-562577(P2020-562577)	(73)特許権者	517392436
(86)(22)出願日	令和1年6月21日(2019.6.21)		▲騰▼▲訊▼科技(深▲セン▼)有限公
(65)公表番号	特表2021-524084(P2021-524084		司
	A)		中華人民共和國518057▲広▼▲東
(43)公表日	令和3年9月9日(2021.9.9)		▼省深▲セン▼市南山区高新区科技中一
(86)国際出願番号	PCT/CN2019/092410		路 ▲騰▼▲訊▼大厦35▲層▼
(87)国際公開番号	WO2020/007209	(74)代理人	100110364
(87)国際公開日	令和2年1月9日(2020.1.9)		弁理士 実広 信哉
審査請求日	令和2年11月6日(2020.11.6)	(74)代理人	100150197
(31)優先権主張番号	201810731377.2		弁理士 松尾 直樹
(32)優先日	平成30年7月5日(2018.7.5)	(72)発明者	汪 ▲東▼▲艶▼
(33)優先権主張国・地域又は機関	中国(CN)		中華人民共和國518057▲広▼▲東
			▼省深▲セン▼市南山区高新区科技中一
			路 ▲騰▼▲訊▼大厦35▲層▼
		(72)発明者	李 茂材

最終頁に続く

(54)【発明の名称】 データ記憶方法、データ検証方法、装置、機器及びコンピュータプログラム

(57)【特許請求の範囲】

【請求項1】

データ記憶システムの第1ノードが実行する、データ記憶方法であって、
対象物の第1データを取得するステップと、
前記対象物の第2データを取得するステップであって、前記第1データと前記第2データ
は異なる次元のデータであり、前記次元は、生成から存続期間までの前記対象物の任意の
側面の情報を測定するために使用される、ステップと、
前記第1データと前記第2データとを相互比較し、前記第1データと前記第2データと
の間に所定の関数関係が存在するか否かを判定するステップと、
前記第1データと前記第2データとの間に所定の関数関係が存在する場合、前記対象物
の前記第1データ及び前記第2データを前記第1ノードに記憶するステップと、
を含む、データ記憶方法。

【請求項2】

前記対象物の第1データは、現在の段階での前記対象物のライフサイクル余剰を含み、前
記対象物の第2データは、前記現在の段階での前記対象物のトランザクションデータを含む
ことを特徴とする、請求項1に記載のデータ記憶方法。

【請求項3】

前記対象物の第1データは、現在の段階での前記対象物のリソース消費余剰を含み、前記
対象物の第2データは、前記現在の段階での前記対象物のトランザクションデータを含む
ことを特徴とする、請求項1に記載のデータ記憶方法。

【請求項 4】

前記データ記憶方法が、
前記対象物の第 3 データを取得するステップであって、前記第 3 データは、前記第 1 データ及び前記第 2 データに関連付けられる、ステップと、
前記対象物の前記第 1 データ及び前記第 2 データを第 1 ノードに記憶するとき、前記対象物の前記第 3 データを前記第 1 ノードに記憶するステップと、
を更に含むことを特徴とする、請求項 1 ないし 3 のいずれか一項に記載のデータ記憶方法。

【請求項 5】

前記対象物の第 3 データは、現在の段階での前記対象物のリソース消費余剰を含むことを特徴とする、請求項 4 に記載のデータ記憶方法。

10

【請求項 6】

前記リソース消費余剰は、炭素排出余剰である
ことを特徴とする、請求項 3 に記載のデータ記憶方法。

【請求項 7】

前記データ記憶方法は、
前記第 1 ノードの監査情報を取得するステップであって、前記監査情報は、前記第 1 ノードによって記憶されたデータを指示するものである、ステップと、
前記第 1 ノードの監査情報を前記データ記憶システムの複数の第 2 ノードにブロードキャストするステップと、
を更に含むことを特徴とする、請求項 1 に記載のデータ記憶方法。

20

【請求項 8】

前記監査情報は、プリセットされた期間内に前記第 1 ノードによって記憶されたデータを含む
ことを特徴とする、請求項 7 に記載のデータ記憶方法。

【請求項 9】

前記監査情報は、前記第 1 ノードが秘密鍵を用いて現在の段階でのコンテキスト情報に署名して得られたコンテキスト署名データを更に含み、前記コンテキスト情報は、タイムスタンプ、地理的アドレス情報、及びネットワークアドレス情報のうちの少なくとも 1 つを含む
ことを特徴とする、請求項 7 に記載のデータ記憶方法。

30

【請求項 10】

前記対象物の前記第 1 データ及び前記第 2 データを前記第 1 ノードに記憶する前記ステップは、
前記対象物の前記第 1 データ及び前記第 2 データを前記第 1 ノードのリソースプールに記憶するステップと、
任意の第 2 ノードによって送信されたコンセンサス確認通知を受信した場合、前記リソースプールに記憶された前記第 1 データ及び前記第 2 データを、前記第 1 ノードのプリセットされた記憶空間に記憶するステップと、
を含むことを特徴とする、請求項 7 に記載のデータ記憶方法。

【請求項 11】

前記データ記憶方法は、
任意の段階で生産された製品にバーコードを提供するステップであって、前記バーコードが指示するアドレスは、前記対象物の最新の第 1 データ、最新の第 2 データ、及び最新の第 3 データのうちの少なくとも 1 つを提供するために使用される、ステップ
を更に含むことを特徴とする、請求項 4 に記載のデータ記憶方法。

40

【請求項 12】

前記バーコードは、スキャン端末が、スキャンして得たデータを第 2 ノードに送信して検証するように、複数の前記第 2 ノードのネットワークアドレスを更に提供すること
を特徴とする、
請求項 11 に記載のデータ記憶方法。

50

【請求項 13】

データ記憶装置であって、

対象物の第1データを取得するように構成される第1データ取得モジュールと、
前記対象物の第2データを取得するように構成される第2データ取得モジュールであって、
前記第1データと前記第2データは異なる次元のデータであり、前記次元は、生成から
存続期間までの前記対象物の任意の側面の情報を測定するために使用される、第2データ
取得モジュールと、

前記第1データと前記第2データとを相互比較し、前記第1データと前記第2データと
の間に所定の関数関係が存在するか否か判定する、比較モジュールと、

前記第1データと前記第2データとの間に所定の関数関係が存在する場合、前記対象物
の前記第1データと前記第2データを第1ノードに記憶するように構成される記憶モジュ
ールと、

を備えることを特徴とする、データ記憶装置。

【請求項 14】

プロセッサとメモリとを備える、コンピュータ機器であって、

少なくとも1つの命令が前記メモリに記憶され、前記命令が前記プロセッサによりロード
および実行されると、請求項1ないし12のいずれか一項に記載のデータ記憶方法を実現
する

ことを特徴とする、コンピュータ機器。

【請求項 15】

コンピュータプログラムであって、

実行されると、請求項1ないし12のいずれか一項に記載のデータ記憶方法を実行するよ
うに構成される、コンピュータプログラム。

【請求項 16】

データ記憶システムであって、前記システムは、複数の第1ノード及び複数の第2ノード
を含み、前記データ記憶システムの複数の第2ノードには、コンセンサスメカニズムが配
置されており、

前記複数の第1ノードの各第1ノードは、対象物の第1データを取得し、前記対象物の第
2データを取得し、前記第1データと前記第2データとを相互比較し、前記第1データと
前記第2データとの間に所定の関数関係が存在するか否か判定し、前記第1データと前記
第2データとの間に所定の関数関係が存在する場合、前記対象物の前記第1データ及び前
記第2データを前記第1ノードに記憶し、前記第1ノードの監査情報を取得し、前記第1
ノードの監査情報を前記データ記憶システムの複数の第2ノードにブロードキャストする
ように構成され、前記第1データと前記第2データは異なる次元のデータであり、前記次
元は、生成から存続期間までの前記対象物の任意の側面の情報を測定するために使用され
、前記監査情報は、前記第1ノードによって記憶されたデータを指示するものであり、
前記複数の第2ノードの各第2ノードは、前記第1ノードの監査情報を受信し、少なくと
も1つのターゲット第1ノードのターゲット監査情報に基づいて前記監査情報を検証し、
検証に合格した場合、前記データ記憶システムにおいて検証合格通知をブロードキャスト
し、受信した検証合格通知がコンセンサス達成条件を満たす場合、前記監査情報に対する
コンセンサスが達成されたと決定するように構成され、前記監査情報は、前記第1ノード
に記憶されたデータを指示するものである

ことを特徴とする、データ記憶システム。

【発明の詳細な説明】

【技術分野】

【0001】

(関連出願の相互参照)

本願は、2018年07月05日に中国特許局に提出された、出願番号が2018107
31377.2であり、発明の名称が「データ記憶方法、データ検証方法、装置、機器及
び媒体」である中国特許出願の優先権を主張し、当該中国特許出願の全ての内容が参照に

10

20

30

40

50

より本願に組み込まれている。

【 0 0 0 2 】

本願は、ネットワーク技術分野に関し、特に、データ記憶方法、データ検証方法、装置、機器及び記憶媒体に関するものである。

【背景技術】

【 0 0 0 3 】

ブロックチェーン技術の発展に伴い、ますます多くのサービスがブロックチェーンをデータ記憶及び共有のための記憶媒体として使用し始めている。ただし、ブロックチェーン技術の適用中は、チェーン上のデータの追跡可能性のみを保証でき、チェーン上のデータの真正性を保証できない。つまり、チェーン上のデータは実際の生産及び生活とは関係ないものである。したがって、このような技術は非常に制限されており、実際の生産を支援できない。

10

【発明の概要】

【発明が解決しようとする課題】

【 0 0 0 4 】

本願実施例は、データ記憶方法、データ検証方法、装置、機器及び記憶媒体を開示する。

【課題を解決するための手段】

【 0 0 0 5 】

データ記憶方法であって、データ記憶システムの第 1 ノードによって実行され、前記方法は、

20

対象物の第 1 データを取得するステップと、

前記対象物の第 2 データを取得するステップであって、前記第 1 データと前記第 2 データは異なる次元のデータであり、前記次元は、生成から存続期間までの前記対象物の任意の側面の情報を測定するために使用される、ステップと、

前記対象物の前記第 1 データ及び前記第 2 データを前記第 1 ノードに記憶するステップと、を含む。

【 0 0 0 6 】

データ記憶システムの任意の第 2 ノードが実行する、データ検証方法であって、前記データ記憶システムの複数の第 2 ノードには、コンセンサスメカニズムが配置されており、前記方法は、

30

第 1 ノードの監査情報を受信するステップであって、前記監査情報は、前記第 1 ノードに記憶されたデータを指示する、ステップと、

少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報に基づいて前記監査情報を検証するステップと、

検証に合格した場合、前記データ記憶システムにおいて検証合格通知をブロードキャストするステップと、

受信した検証合格通知がコンセンサス達成条件を満たす場合、前記監査情報に対するコンセンサスが達成されたと決定するステップと、を含む。

【 0 0 0 7 】

データ記憶装置であって、前記装置は、

40

対象物の第 1 データを取得するように構成される第 1 データ取得モジュールと、

前記対象物の第 2 データを取得するように構成される第 2 データ取得モジュールであって、前記第 1 データと前記第 2 データは異なる次元のデータであり、前記次元は、生成から存続期間までの前記対象物の任意の側面の情報を測定するために使用される、第 2 データ取得モジュールと、

前記対象物の前記第 1 データ及び前記第 2 データを前記第 1 ノードに記憶するように構成される記憶モジュールと、を備える。

【 0 0 0 8 】

データ検証装置であって、前記装置は、

第 1 ノードの監査情報を受信するように構成される受信モジュールであって、前記監査情

50

報は、前記第 1 ノードに記憶されたデータを指示する受信モジュールと、少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報に基づいて前記監査情報を検証するように構成される検証モジュールと、検証に合格した場合、データ記憶システムにおいて検証合格通知をブロードキャストするように構成される送信モジュールと、を備え、前記検証モジュールは、更に、受信した検証合格通知がコンセンサス達成条件を満たす場合、前記監査情報に対するコンセンサスが達成されたと決定するように構成される。

【 0 0 0 9 】

コンピュータ機器であって、前記コンピュータ機器は、プロセッサとメモリとを備え、少なくとも 1 つの命令が前記メモリに記憶され、前記命令が前記プロセッサによりロードおよび実行されると、上記のデータ記憶方法におけるステップを実現し、又は前記命令が前記プロセッサよりロードおよび実行されると、上記のデータ検証方法におけるステップを実現する。

10

【 0 0 1 0 】

コンピュータ可読記憶媒体であって、少なくとも 1 つの命令が前記記憶場体に記憶され、前記命令が前記プロセッサによりロードおよび実行されると、上記のデータ記憶方法におけるステップを実現し、又は前記命令が前記プロセッサによりロードおよび実行されると、上記のデータ検証方法におけるステップを実現する。

【 0 0 1 1 】

データ記憶システムであって、前記システムは複数の第 1 ノード及び複数の第 2 ノードを備え、前記データ記憶システムの複数の第 2 ノードには、コンセンサスメカニズムが配置されており、

20

前記複数の第 1 ノードの各第 1 ノードは、対象物の第 1 データを取得し、前記対象物の第 2 データを取得し、前記対象物の前記第 1 データ及び前記第 2 データを前記第 1 ノードに記憶し、前記第 1 ノードの監査情報を取得し、前記第 1 ノードの監査情報を前記データ記憶システムの複数の第 2 ノードにブロードキャストするように構成され、前記第 1 データと前記第 2 データは異なる次元のデータであり、前記次元は、生成から存続期間までの前記対象物の任意の側面の情報を測定するために使用され、前記監査情報は、前記第 1 ノードによって記憶されたデータを指示するものであり、

前記複数の第 2 ノードの各第 2 ノードは、前記第 1 ノードの監査情報を受信し、少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報に基づいて前記監査情報を検証し、検証に合格した場合、前記データ記憶システムにおいて検証合格通知をブロードキャストし、受信した検証合格通知がコンセンサス達成条件を満たす場合、前記監査情報に対するコンセンサスが達成されたと決定するように構成され、前記監査情報は、前記第 1 ノードに記憶されたデータを指示するものである。

30

【 0 0 1 2 】

本願の 1 つ又は複数の実施例の詳細は、以下の添付の図面及び説明で開示される。本願の他の特徴、目的及び利点は、明細書、添付の図面及び特許請求の範囲からより明らかになる。

【図面の簡単な説明】

40

【 0 0 1 3 】

本願実施例における技術的解決策をより明確にするために、下記において、実施例の説明に必要な図面を簡単に説明する。勿論、下記の図面は本願の一部の実施例に過ぎず、当業者は、創造的な労力を要することなく、これらの図面に基づいて他の図面を得ることもできる。

【 0 0 1 4 】

【図 1】本願実施例によるデータ記憶システムの構造を示す概略図である。

【図 2】本願実施例によるコンピュータ機器を示す概略図である。

【図 3】本願実施例によるデータ記憶方法を示すフローチャートである。

【図 4】本願実施例によるデータ検証方法を示すフローチャートである。

50

【図 5】本願実施例によるデータ検証プロセスにおけるデータ相関ネットワークを示す概略図である。

【図 6】本願実施例による、乳製品の生産から流通までの異なる段階、及び各段階における異なるリンクに関する実施プロセスを示す概略図である。

【図 7】本願実施例によるデータ記憶装置の構造を示す概略図である。

【図 8】本願実施例によるデータ検証装置の構造を示す概略図である。

【発明を実施するための形態】

【0015】

本願の目的、技術的解決策及び利点をより明確に説明するために、添付の図面を参照して本開示の実施形態を以下に詳細に説明する。

【0016】

図 1 は、本願実施例によるデータ記憶システムの構造を示す概略図である。当該システムは、複数の第 1 ノード 101 及び複数の第 2 ノード 102 を含む。

【0017】

当該複数の第 1 ノードの各第 1 ノードは、対象物の第 1 データを取得し、当該対象物の第 2 データを取得し、当該対象物の第 1 データ及び当該第 2 データを当該第 1 ノードに記憶し、当該第 1 ノードの監査情報を取得し、当該第 1 ノードの監査情報を当該データ記憶システムの複数の第 2 ノードにブロードキャストするように構成され、当該第 1 データと第 2 データは異なる次元のデータであり、当該監査情報は、当該第 1 ノードによって記憶されたデータを指示するものである。

【0018】

当該複数の第 2 ノードは、当該第 1 ノードの監査情報を受信し、少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報に基づいて当該監査情報を検証し、検証に合格した場合、当該データ記憶システムにおいて検証合格通知をブロードキャストし、受信した検証合格通知がコンセンサス達成条件を満たす場合、当該監査情報に対するコンセンサスが達成されたと決定するように構成され、当該監査情報は、当該第 1 ノードによって記憶されたデータを指示するものである。

【0019】

ここで、当該複数の第 1 ノード 101 は、異なる事業体のノードであってもよく、対応する事業体の生産及びトランザクションに関連するデータを記憶するように構成されてもよく、各第 1 ノード 101 は、それ自体のデータをデータベース又はブロックに記憶してもよい。データベースにデータを記憶することは、各データにインデックスを付け、インデックスに基づいてデータを対応する記憶空間に記憶することである。ブロックにデータを記憶することは、第 1 ノードに記憶されているデータの各部分がある程度関連付けられ、ブロックチェーンと同様のブロックの形で、データが改ざんされないように保証できることを意味する。上記の複数の第 1 ノード 101 は、データ記憶システムの基礎データ層を構成でき、対応する事業体にそれぞれデータクエリ機能を提供して、他のノードとのトランザクション及びそれら自体の生産活動を追跡することもできる。具体的には、複数の第 1 ノード 101 は、トランザクションを実行するために互いに通信することができる。例えば、第 1 ノード 1 は、第 1 ノード 2 とトランザクションすることにより、当該第 1 ノード 1 のアカウントから当該第 1 ノード 2 に対応するアカウントへの口座振替、製品配達、及び情報交換などのプロセスを実行して、第 1 ノード 2 とのトランザクションを完了できる。勿論、当該トランザクションの完了は、オンライントランザクションの完了を指し得、実際のトランザクションプロセスでは、関連するオフライン運送などを含んでもよく、本願実施例は、これを限定するものではない。更に、当該第 1 ノードは、事業体のプロキシノードであってもよく、1 つ又は複数の事業体に代わってオンライントランザクション及びデータ記憶などを実行するために使用され、当該第 1 ノードが 1 つ又は複数の事業体のプロキシノードとして機能する場合、異なる事業体のためにそれぞれデータ記憶を実行し、キーを設定するなどの方法で、各事業体のデータプライバシーを保証できることを留意されたい。

10

20

30

40

50

【 0 0 2 0 】

複数の第 2 ノード 1 0 2 は、生産及びトランザクションプロセス中に複数の第 1 ノードによって生成されたデータを検証し、検証結果に基づいて第 1 ノードのデータの真正性を指示するように構成されてもよい。当該複数の第 2 ノード 1 0 に同じブロックチェーンを配備してもよく、つまり、当該複数の第 2 ノード 1 0 2 は、同じコンセンサスメカニズムに従うことができ、第 1 ノード 1 0 1 のデータをそれぞれ検証し、コンセンサスメカニズム及び複数の第 2 ノード 1 0 2 の検証結果に基づいて、コンセンサスによってデータを検証することができることを留意されたい。検証結果がコンセンサス達成条件（例えば、検証に合格した第 2 ノードの数が合計の 2 / 3 を超えるなど）を満たす場合、当該複数の第 2 ノード 1 0 2 はコンセンサスに達し、第 1 ノード 1 0 1 のデータが真実であると決定し、検証結果がコンセンサス達成条件を満たさない場合、当該複数の第 2 ノード 1 0 2 はコンセンサスに達しておらず、第 1 ノード 1 0 1 のデータが真実ではないと決定する。本願実施例は、採用される特定のコンセンサスメカニズムを限定するものではないことを留意されたい。

10

【 0 0 2 1 】

上記の複数の第 1 ノード 1 0 1 は、データ記憶システムの基礎データ層を構成し、それら自体のデータを記憶するために使用され、当該複数の第 2 ノード 1 0 2 は、当該データ記憶システムの監査層を構成し、複数の第 1 ノード 1 0 1 に検証サービスを提供するために使用される。各第 1 ノード 1 0 1 のデータは、ある程度隔離されていてもよく、例えば、第 1 ノード 1 のトランザクションデータは、第 1 ノード 2 には見えず、第 1 ノード 1 は、アカウント情報を運ぶトランザクション要求を第 2 ノードに送信できる。各第 1 ノード 1 0 1 のデータは、当該複数の第 2 ノード 1 0 2 に対して透過的又は比較的透過的である。つまり、第 2 ノード 1 0 2 は、第 1 ノード 1 0 1 に記憶されたデータ又はデータの固有値（ハッシュ値など）を取得でき、データ又は固有値を取得する具体的なプロセスについては、後で詳述する。

20

【 0 0 2 2 】

ここで、第 1 ノード又は第 2 ノードは、任意のタイプのコンピュータ機器として提供されてもよく、例えば、図 2 は、本願実施例によるコンピュータ機器 2 0 0 を示す概略図である。当該コンピュータ機器 2 0 0 は、異なる構成又は性能により比較的大きな差異を有し得る。当該コンピュータ機器 2 0 0 は、1 つ又は複数のプロセッサ（CPU: c e n t r a l p r o c e s s i n g u n i t s）2 0 1 と 1 つ又は複数のメモリ 2 0 2 とを備えてもよく、ここで、前記メモリ 2 0 2 に少なくとも 1 つの命令が記憶されており、前記少なくとも 1 つの命令が前記プロセッサ 2 0 1 によりロードおよび実行されることにより、下記各実施例によるデータ記憶方法又はデータ検証方法を実現する。勿論、当該コンピュータ装置は、入力出力を行うために、有線又は無線ネットワークインタフェース、キーボード及び入力出力インタフェース等の部材を備えてもよい。当該コンピュータ機器は、機器の機能を実現するための他のコンポーネントをさらに備えてもよく、ここでは詳細な説明を省略する。

30

【 0 0 2 3 】

図 3 は、本願実施例によるデータ記憶方法を示すフローチャートである。当該データ記憶方法は、図 1 に示される任意の第 1 ノードに適用されることができ、図 3 を参照すると、当該方法は、以下のステップを含み得る。

40

【 0 0 2 4 】

ステップ S 3 0 1 において、対象物の第 1 データを取得する。

【 0 0 2 5 】

ここで、対象物は、オフライン又はオンラインで、トランザクション又は流通できる任意の製品であってもよい。当該対象物は、有形のプロダクトであってもよく、当該有形のプロダクトは、手動生産又は機械生産により取得でき、例えば、当該有形のプロダクトは、食品、日常品、家庭用品、家電などであってもよく、本出願実施例では具体的に限定しない。当該対象物はまた、手形類の製品、すなわち、手形の形で表現される製品であっても

50

よく、例えば、当該対象物は、株式、債券、ファンドシェアなどの金融商品であってもよい。勿論、当該対象物はまた、仮想製品、すなわち、一定の実際の通貨値又は仮想通貨値に対応できる電子データの形の製品であってもよく、当該通貨値は、固定されることなく、市場のルールに従って変動してもよく、例えば、当該仮想製品は、オンラインファンドプロダクト又はオンライン株式プロダクトなどの金融製品であってもよい。

【0026】

当該第1データは、当該対象物の一次元のデータであってもよく、当該次元は、生成から存続期間までの対象物の任意の態様を測定するための情報を指す。例えば、次元は、時間次元、トランザクション次元、環境保護次元などを含み得る。ここで、時間次元は、対象物の存続された時間、対象物の消滅までの残りの時間、対象物の決済又は期限切れまでの残りの時間などを含み得る。トランザクション次元は、生成から存続期間までの対象物に関連付けられたトランザクション行為におけるトランザクション両方、トランザクション金額、トランザクション時間などを含み得る。環境保護次元は、炭素排出状況、ホルムアルデヒド生成状況、産業廃棄物生成状況などの有害物質の排出又は生成状況を含み得る。

10

【0027】

ステップS302において、当該対象物の第2データを取得し、当該第1データと第2データは異なる次元のデータであり、次元は、生成から存続期間までの対象物の任意の側面の情報を測定するために使用される。

【0028】

ここで、当該第2データは、第1データとは異なる次元のデータを指し得る。例えば、第1データが時間次元のデータである場合、第2データは、トランザクション次元又は環境保護次元であり得る。

20

【0029】

ステップS303において、当該対象物の第1データ及び当該第2データを第1ノードに記憶する。

【0030】

第1ノードは、当該ノードの生産又はトランザクションに関連するデータを記憶でき、当該データは、当該ノードに対応する対象物の生産段階又は流通段階で発生された任意のトランザクションの情報を含み得る。

【0031】

データの記憶中、第1ノードは、クエリのために第1データ及び第2データを対応して記憶することができることを留意されたい。例えば、第1ノードは、第1データ及び第2データを第1ノードのデータベース内の1つのデータ項目又は関連データ項目に記憶してもよいし、第1データ及び第2データを1つのブロックに記憶してもよいし、又は第1データ及び第2データを異なるブロックにそれぞれ記憶し、クエリのために同じデータ識別子を付けてもよい。

30

【0032】

いくつかの実施例では、第1ノードは、データを記憶する前に、取得した少なくとも2つの次元のデータを相互比較し、前記取得された少なくとも2つの次元のデータが一致する場合、ステップS303における記憶操作を実行してもよい。各次元のデータが特定の関数関係に準拠する必要があるため、当該次元間の関数関係に基づいて、少なくとも2つの次元のデータを相互比較することができ、比較結果が一致である場合、前記少なくとも2つの次元のデータを記憶でき、比較結果が不一致である場合、記憶操作を実行しない。例えば、ライフサイクルと炭素排出量の間には特定の関数関係が存在する必要がある。例えば、ライフサイクルが2日間減少すると、炭素排出量を10単位増加する必要がある、上記の多次元データが関数関係を満たさない場合、データが正しくなく、比較結果が不一致であることを意味する。

40

【0033】

上記の相互比較は、本願実施例で開示される任意の次元のデータを対象とすることができ、つまり、取得されたデータが第1データ及び第2データである場合、第1データ及び第

50

2 データに基づいて比較し、取得されたデータが第 1 データ、第 2 データ、及び第 3 データである場合、第 1 データ、第 2 データ、及び第 3 データに基づいて比較し、同様に、取得されたデータが他のデータを更に含む場合、上記の原則に従って比較プロセスを実行することを留意されたい。勿論、上記の比較は、特定の比較プロセスの単なる例に過ぎず、本願実施例では、多次元データに基づいて他の比較プロセスを実行することもでき、本願実施例はこれを限定するものではない。

【 0 0 3 4 】

本願実施例では、主に、対象物の異なる次元のデータを取得することにより、生産段階から流通段階までの対象物の各段階および各リンクを複数の次元から記憶でき、オンラインデータを実際の生産及び生活と密接に関連付けるといった目的を達成できる。このようにして、オンラインデータに実用的な重要性が与えられ、オンラインデータがもはや仮想通貨の単なる表現ではないようにすることができる。更に、本願の各実施例では、各段階に対応する第 1 ノードによって記録された複数の次元のデータが互いに関連付けられるため、各段階及び各リンクのデータを相互に検証できるだけでなく、複数の次元のデータも相互に検証でき、ストーリーミングシームレスデータチェーンを形成し、且つ各第 1 ノードのデータがすべてノード自体に記憶されるため、データのセキュリティが向上する。

【 0 0 3 5 】

対象物は、生産から流通に至る複数の段階を経ることができ、実際の需要に応じて当該複数の段階を分割することができる。食品を例にとると、原料生産段階、対象物生産段階、運送段階、販売段階などを経ることができる。ここで、販売段階は更に、異なる販売方式に応じた異なる段階を含み得る。例えば、E コマース販売方式を使用する場合、販売段階は、E コマース段階、倉庫保管段階、物流段階、及び消費者段階を含み得、直接販売方式を使用する場合、販売段階は、発売段階及び消費者段階を含み得る。別の例では、仮想製品を例にとると、販売段階は、設計段階、試運転段階又はプリセール段階、正式リリース段階などを含み得る。

【 0 0 3 6 】

図 3 に示される実施例に基づいて、いくつかの実施例では、当該対象物の第 1 データは、現在の段階での当該対象物のライフサイクル余剰を含んでもよく、当該対象物の第 2 データは、当該現在の段階での当該対象物のトランザクションデータを含んでもよい。

【 0 0 3 7 】

ここで、ライフサイクルとは、対象物の元の状態から対象物の生成、そして対象物の存続期間満了、対象物の使用期限切れ、又は対象物の枯渇までの期間を指す。例えば、食品のライフサイクルは、賞味期間として表すことができ、牛乳を例にとると、その賞味期間は 30 日であり得る。仮想製品のライフサイクルは、有効期間として表すことができ、金融製品を例にとると、その有効期間 60 日であり得る。ソフトウェア製品を例にとると、その有効期間は使用許諾の有効期間として表すことができ、例えば、プレミアムメンバーシップの有効期間は 1 か月であり得る。電子製品のライフサイクルは、廃棄期限又は使用回数として表すことができ、例えば、洗濯機廃棄期限は、5 年又は 10、000 回の使用回数に達することであり得る。ライフサイクルの上記の説明に基づいて、ライフサイクル余剰は、現時点での当該対象物のライフサイクルの残量であることが分かる。例えば、上記の食品のライフサイクルは 30 日であり、この時点で 10 日間流通された場合、そのライフサイクル余剰は 20 日である。対象物の各段階で、一定の消費が発生する可能性があり、当該対象物の使用又は存続に影響を与える可能性があるため、このような影響を記録するために、対象物のライフサイクル余剰を取得することができる。

【 0 0 3 8 】

いくつかの実施例では、対象物の各段階が、すべて対応するライフサイクル余剰を有してもよく、勿論、対象物のいくつかの段階のみが、対応するライフサイクル余剰を有してもよく、これは、対象物の特性に応じて具体的に決定されてもよい。例えば、原材料を含むいくつかの対象物の場合、原材料の生産段階で対応するライフサイクル余剰が既にあり、その後の各段階では、そのライフサイクル余剰は、すべて原材料の生産段階のサイクル余

10

20

30

40

50

剰に基づいて削減され、原材料のない一部の対象物の場合、ライフサイクルという概念が特定の段階からのみ現れることができ、本願実施例はこれを限定するものではない。上記の説明から、当該第1ノードに対応する段階がライフサイクルの開始段階である場合、当該ライフサイクル余剰の値はライフサイクルの長さに等しいことが分かる。

【0039】

いくつかの実施例では、当該ライフサイクル余剰は、任意の時間粒度で表現されてもよく、使用される特定の時間粒度は、対象物のタイプに従って異なって設定できる。いくつかの実施例では、直観的な時点を提供して対象物の存続可能性又は使用可能性を更に示すために、当該ライフサイクル余剰は、ライフサイクル余剰の値とライフサイクルの開始時間を更に含んでもよい。

10

【0040】

いくつかの実施例では、現在の段階での当該対象物のライフサイクル余剰は、前の段階でのライフサイクル余剰と当該現在の段階での消費時間との間の差であってもよい。

【0041】

ここで、現在の段階での対象物のライフサイクル余剰の取得プロセスは、前の段階でのライフサイクル余剰及び当該現在の段階での消費時間を取得し、その後、前の段階でのライフサイクル余剰と当該現在の段階での消費時間との間の差を、現在の段階でのライフサイクル余剰として取得することを含み得る。

【0042】

第1ノードの場合、現在の段階での処理を開始する前に、当該対象物の前の段階に対応する第1ノードによって送信されたライフサイクル余剰を取得でき、当該ライフサイクル余剰は、前の段階に対応する第1ノードとのトランザクションが完了した時に取得され、前の段階に対応する第1ノードによって当該現在の段階に対応する第1ノードに送信されてもよく、ライフサイクル余剰を送信する場合、当該前の段階に対応する第1ノードは、秘密鍵を用いてライフサイクル余剰に署名して得られた署名データ及び当該前の段階に対応する第1ノードの公開鍵を送信してもよい。

20

【0043】

いくつかの実施例では、当該現在の段階の消費時間は、当該現在の段階の特性に従って設定されてもよい。各段階は、人的資源、生産、梱包、運送、電力供給、及び水供給などの異なる入力活動又は支出活動のリンクに関連付けることができ、各リンクが異なる消費時間に対応できるため、異なる段階の消費時間が異なる可能性があり、各段階に関連付けられたリンクの消費時間を分析して、当該段階の消費時間を決定する必要がある。勿論、いくつかの実施例では、経験に基づいて各段階の消費時間を設定してもよく、各段階の履歴処理時間の分析に基づいて、各段階の消費時間を設定してもよい。勿論、ライフサイクル余剰をより正確に計算するために、各段階に関連付けられた各リンクの履歴処理時間の分析に従って、各段階の消費時間を設定してもよい。いくつかの実施例では、実際のデータに基づいてより真実であるライフサイクル余剰を取得するために、各段階の消費時間をリアルタイムでカウントしてもよい。

30

【0044】

いくつかの実施例では、当該現在の段階での当該対象物のトランザクションデータは、当該現在の段階の各リンクでの当該対象物のトランザクションデータを含んでもよく、前記現在の段階での対象物のトランザクションデータは、前記現在の段階の各リンクでの前記対象物のトランザクションデータの署名データを更に含んでもよい。当該第1ノードは、現在の段階の各リンクにおいて、各リンクで発生するトランザクションのトランザクション情報を記録する。例えば、運送リンクにおいて、当該第1ノードのアカウント1から運送業務を行うノードであるアカウント2に転送された費用EXを記録でき、各リンクのトランザクション相手がトランザクションを受け入れた後に提供された署名データも取得でき、当該署名データは、当該トランザクション相手に対応する第1ノードが秘密鍵を用いてトランザクション情報に署名して得られたものであってもよい。例えば、当該署名データは、Sig__(EX(アカウント1 to アカウント2))であり得る。例示的に、ト

40

50

ランザクション相手と署名データを検証するために、ランザクション相手は、署名データを返信する時に、ランザクション相手の公開鍵も一緒に返信してもよい。

【 0 0 4 5 】

いくつかの実施例では、前記対象物の第 1 データは、前記現在の段階での前記対象物のリソース消費余剰を含んでもよく、前記対象物の第 2 データは、前記現在の段階での前記対象物のランザクションデータを含んでもよい。

【 0 0 4 6 】

対象物の場合、対象物の各段階で、一定のリソース消費が発生する可能性があり、環境に影響を与える可能性があるため、このような影響を制限するために、このようなデータを記録する必要がある。

10

【 0 0 4 7 】

ここで、リソース消費とは、対象物の元の状態から対象物の生成、そして対象物の存続期間満了、対象物の使用期限切れ、又は対象物の枯渇までのいくつかの制限付きリソースの消費状況を指す。例えば、工業製品の場合、リソース消費は、工業生産活動によるリソースの消費に伴う付随的な物質の排出量として表されることができ、例えば、炭素排出量又はホルムアルデヒド排出量などの生産付随的物質の排出量であり得る。

【 0 0 4 8 】

いくつかの実施例では、当該現在の段階での当該対象物のリソース消費余剰は、前の段階でのリソース消費余剰と当該現在の段階でのリソース消費量との間の差であってもよい。

【 0 0 4 9 】

20

ここで、現在の段階での対象物のリソース消費余剰の取得プロセスは、第 1 ノードが前の段階でのリソース消費余剰及び当該現在の段階でのリソース消費量を取得し、その後、前の段階でのリソース消費余剰と当該現在の段階でのリソース消費量との間の差を、現在の段階でのリソース消費余剰として取得することを含み得る。

【 0 0 5 0 】

第 1 ノードの場合、現在の段階での処理を開始する前に、当該対象物の前の段階に対応する第 1 ノードによって送信されたリソース消費余剰を取得でき、当該リソース消費余剰は、前の段階に対応する第 1 ノードとのランザクションが完了した時に取得され、前の段階に対応する第 1 ノードによって当該第 1 ノードに送信されてもよく、リソース消費余剰を送信する場合、当該前の段階に対応する第 1 ノードは、秘密鍵を用いてリソース消費余剰に署名して得られた署名データ及び当該前の段階に対応する第 1 ノードの公開鍵を送信してもよい。

30

【 0 0 5 1 】

いくつかの実施例では、当該現在の段階でのリソース消費量は、当該現在の段階の各リンクでの当該対象物在のリソース消費量の合計であってもよい。当該第 1 ノードは、現在の段階の各リンクにおいて、各リンクで発生するランザクションのランザクション情報、及びランザクションに基づいて取得されたリソース消費量を記録する。例えば、運送リンクにおいて、当該第 1 ノードのアカウント 1 から運送業務を行うノードであるアカウント 2 に転送された費用 E X を記録でき、各リンクのランザクション相手がランザクションに基づいて提供された炭素排出量 C C も取得でき、これに対して、取得された署名データは、ランザクション情報及びリソース消費量に基づいて署名して得られた署名データであり得る。

40

【 0 0 5 2 】

説明を加えないといけない点は、上記のリソース消費余剰は、単一対象物に正規化されたリソース消費余剰であってもよく、例えば、炭素排出余剰の場合、当該炭素排出余剰は、単一の製品に正規化された炭素排出余剰であり得る。説明を加えないといけないもう 1 つの点は、任意のタイプの対象物は、そのリソース消費指標を設定することにより、リソース消費指標に従って実際の生成をガイドするようにしてもよく、例えば、炭素排出量の場合、国際会議で指定された炭素排出量の上限に基づいて炭素排出量を設定できる。

【 0 0 5 3 】

50

いくつかの実施例では、当該方法は、第1ノードが当該対象物の第3データを取得するステップであって、当該第3データは、当該第2データに関連付けられる、ステップと、当該対象物の第1データ及び当該第2データを第1ノードに記憶するとき、当該対象物の第3データを当該第1ノードに記憶するステップとを更に含んでもよい。

【0054】

ここで、第3データの次元は、第1データ及び第2データの次元とは異なってもよい。第3データの生成は、第2データの生成に関連付けられてもよい。第2データは、現在の段階での対象物のトランザクションデータであってもよく、対象物の生成又は流通プロセスに対する投入行為又は支出行為に基づいて生成されたデータであってもよい。第3データも、対象物の生成又は流通プロセスにおける投入行為又は支出行為に基づいて生成されたデータであってもよく、第2データの生成により、対応する第3データが生成されることができる。

10

【0055】

第2データは、必ずしも関連付けられる第3データを有する必要はなく、第3データは、必然的に第2データの生成により生成されるデータであることを留意されたい。例えば、任意の支出行為の発生は、トランザクションの両方の当事者が資金トランザクションを実行したことを意味し、対応するリソース消費次元のトランザクションも完了したことを意味する（例えば、当該トランザクションにより、販売者の炭素排出量が購入者に転送される）。

【0056】

データの記憶中、第1ノードは、第1データ、第2データ、及び第3データを1つのブロックに記憶してもよく、第1データ、第2データ、及び第3データを異なるブロックにそれぞれ記憶し、クエリのために同じデータ識別子を付けてもよいことを留意されたい。勿論、第2データ及び第3データを1つのブロックに記憶し、第1データを別のブロックに記憶し、同じデータ識別子を付けてもよく、本願実施例はこれを限定するものではない。

20

【0057】

いくつかの実施例では、当該対象物の第3データは、当該現在の段階での当該対象物のリソース消費余剰を含んでもよい。例えば、第1データは、現在の段階でのライフサイクル余剰であり得、第2データは、現在の段階でのトランザクションデータであり得、第3データは、当該現在の段階での対象物のリソース消費余剰であり得、前記リソース消費余剰は、炭素排出余剰であり得る。

30

【0058】

いくつかの実施例では、第1ノードは、前記第1ノードの監査情報を取得し、前記第1ノードの監査情報を前記データ記憶システムの複数の第2ノードにブロードキャストしてもよく、前記監査情報は、前記第1ノードによって記憶されたデータを指示するものであり得る。

【0059】

第1ノードの場合、第1データ及び第2データを記憶する前に、上記の第1ノードの監査情報を取得するステップを実行でき、つまり、ステップS301及びS302を実行した後、監査情報を取得及びブロードキャストする上記のステップを実行でき、これにより、コンセンサス確認通知を受信してから、前記対象物の第1データ及び前記第2データを前記第1ノードに記憶するステップを実行することができることを留意されたい。

40

【0060】

いくつかの実施例では、第1ノードは、データを一時的に記憶するためのリソースプールを有してもよく、つまり、第1データ及び第2データを取得する場合、先ず前記対象物の第1データ及び前記第2データを前記第1ノードのリソースプールに記憶し、任意の第2ノードによって送信されたコンセンサス確認通知を受信した場合、前記リソースプールに記憶された第1データ及び第2データを前記第1ノードのプリセットされた記憶空間に記憶してもよい。

【0061】

50

いくつかの実施例では、前記監査情報は、前記第 1 ノードによって記憶されたデータを含んでもよく、又は、前記監査情報は、プリセットされた期間内に前記第 1 ノードによって記憶されたデータを含んでもよい。このような実施形態では、監査情報は、固有値ではなく、第 1 ノードによって記憶されたデータ自体であり得るため、第 2 ノードは、トランザクションの元のデータを取得でき、第 2 ノードの検証精度が大幅に向上する。

【 0 0 6 2 】

いくつかの実施例では、前記監査情報は、前記第 1 ノードによって記憶されたデータの固有値を含んでもよく、又は、前記監査情報は、プリセットされた期間内に前記第 1 ノードによって記憶されたデータの固有値を含んでもよい。ここで、比較的大きな生産規模又は比較的高い生産頻度による過度に頻繁なデータ送信を回避するために、当該プリセットされた期間に記憶されたデータは、特定の生産プロセスで取得されたデータだけでなく、少なくとも 1 回の生産プロセスで第 1 ノードによって取得されたデータであってもよい。

10

【 0 0 6 3 】

ここで、固有値は、ハッシュ値又は不可逆アルゴリズムに基づいて計算して得られた任意のタイプの固有値であり得る。

【 0 0 6 4 】

いくつかの実施例では、当該監査情報は、署名データであってもよく、当該署名データは、当該第 1 ノードが当該第 1 ノードの秘密鍵を用いて、第 1 ノードに記憶されたデータに署名して得られたものであってもよい。当該署名により、第 2 ノードが当該監査情報のソースノードを認識することができる。いくつかの実施例では、当該監査情報は、当該第 1 ノードの公開鍵を更に含んでもよい。第 2 ノードは、当該公開鍵と署名データに基づいて検証を実行して、当該監査情報が当該第 1 ノードからのものであると決定し、その後、署名データの圧縮解除後に得られた固有値又は他のデータに基づいて、特定の検証プロセスを実行できる。

20

【 0 0 6 5 】

いくつかの実施例では、当該監査情報は、当該第 1 ノードが秘密鍵を用いて現在の段階のコンテキスト情報に署名して得られたコンテキスト署名データを更に含んでもよく、当該コンテキスト情報は、タイムスタンプ、地理的アドレス情報、及びネットワークアドレス情報のうちの少なくとも 1 つを含んでもよい。コンテキスト情報は、当該監査されるデータに対応する発生時間及び発生環境などの情報を提供でき、データの追跡可能性を保証できる。

30

【 0 0 6 6 】

監査層の第 2 ノードの場合、図 4 と図 5 に示されるようなデータ相互作用を有し得る。図 4 は、本願実施例によるデータ検証方法を示すフローチャートであり、図 5 は、本願実施例によるデータ検証プロセスにおけるデータ相関ネットワークを示す概略図である。図 4 に示されるように、当該データ検証方法は、複数の第 2 ノードが第 1 ノードの監査情報を受信するステップ S 4 0 1 と、各第 2 ノードが、監査情報に従って、少なくとも 1 つのターゲット第 1 ノードによってアップロードされたターゲット監査情報を取得するステップ S 4 0 2 と、各第 2 ノードが、前記少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報を当該監査情報と比較するステップ S 4 0 3 と、一致する場合、当該第 2 ノードは、当該監査情報が検証に合格したと決定し、検証合格通知を当該複数の第 2 ノードにブロードキャストするステップ S 4 0 4 と、複数の第 2 ノードがコンセンサスプロセスを実行し、受信した検証合格通知がコンセンサス達成条件を満たす場合、監査情報に対するコンセンサスが達成されたと決定するステップ S 4 0 5 とを含み得る。

40

【 0 0 6 7 】

図 4 と図 5 を参照すると、第 2 ノードが第 1 ノードの監査情報を受信し、前記監査情報は、前記第 1 ノードに記憶されたデータを指示し、少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報に基づいて前記監査情報を検証し、検証に合格した場合、第 2 ノードが前記データ記憶システムにおいて検証合格通知をブロードキャストし、受信した検証合格通知がコンセンサス達成条件を満たす場合、前記第 1 監査情報に対するコンセンサス

50

が達成されたと決定する。前記監査情報に対するコンセンサスが達成された場合、第 2 ノードは更に、コンセンサス確認通知を前記第 1 ノードに送信することができる。

【 0 0 6 8 】

ここで、上記の記憶されたデータは、第 1 データ及び第 2 データであってもよいし、第 1 データ、第 2 データ、及び第 3 データであってもよいし、第 2 データ及び第 3 データであってもよく、勿論、異なるデータ需要に応じて、第 1 データと第 3 データの組み合わせであってもよく、本願実施例はこれを限定するものではない。

【 0 0 6 9 】

前記第 1 ノードは、前記ターゲット第 1 ノードを含み、前記ターゲット第 1 ノードは、前記複数の第 1 ノードの 1 つである。ターゲット第 1 ノードは、当該第 1 ノードの現在の生産活動に関連付けられる 1 つ又は複数のノードであり得る。例えば、当該ターゲット第 1 ノードは、特定のタイプの対象物の生産又は流通プロセスにおける当該第 1 ノードの上流ノードであってもよく、又は、当該ターゲット第 1 ノードは、当該第 1 ノードの特定の生産リンク（すなわち、特定の生産要素である）に参加するノード（例えば、当該第 1 ノードに運送サービスを提供する会社に対応する第 1 ノードなど）であってもよい。したがって、前記ターゲットノードに対応する前記ターゲット監査情報は、前記第 1 ノードとトランザクションする各ターゲット第 1 ノードによって記憶されたデータを指示するものである。

10

【 0 0 7 0 】

本願の各実施例では、監査層によってデータ記憶システムの各第 1 ノードに検証機能を提供し、監査層の複数の第 2 ノードが各第 1 ノードの監査情報を取得できるため、監査情報の相互比較により、記憶されるデータの真正性と正確性を決定でき、これにより、データのセキュリティを保証しながら、データの真正性と正確性を保証することができる。

20

【 0 0 7 1 】

いくつかの実施例では、第 2 ノードは、第 1 ノード自体によって提供される監査情報内の多次元データに従って相互比較実行してもよく、多次元データがプリセットされた関数関係に準拠する場合、当該監査情報が検証に合格したと決定してもよい。したがって、少なくとも 1 つのターゲット第 1 ノードは、前記第 1 ノード自体であってもよく、少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報は、前記第 1 ノード自体の監査情報であってもよい。

30

【 0 0 7 2 】

いくつかの実施例では、第 2 ノード少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報に基づいて前記監査情報を検証する上記のステップは、第 2 ノード前記監査情報に従って、前記少なくとも 1 つのターゲット第 1 ノードによってアップロードされたターゲット監査情報を取得するステップであって、当該ターゲット監査情報は、当該第 1 ノードとのトランザクションを実行した後に、各ターゲット第 1 ノードによってアップロードされた監査情報であり得る、ステップと、第 2 ノードが前記少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報を当該監査情報と比較し、前記少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報が当該監査情報と一致する場合、当該監査情報が検証に合格したと決定するステップと、を含んでもよい。

40

【 0 0 7 3 】

ここで、前記第 2 ノードが前記監査情報に従って、前記少なくとも 1 つのターゲット第 1 ノードによってアップロードされたターゲット監査情報を取得する前記ステップは、第 2 ノードが、前記監査情報の少なくとも 1 つの署名データの公開鍵を取得するステップと、第 2 ノードが、取得された公開鍵に対応する第 1 ノードを前記少なくとも 1 つのターゲット第 1 ノードとして使用するステップと、前記公開鍵に従って、前記公開鍵に対応する第 1 ノードを含む監査情報を取得し、前記取得した監査情報を前記少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報として使用するステップと、を含み得る。

【 0 0 7 4 】

ここで、第 2 ノードが、前記少なくとも 1 つのターゲット第 1 ノードのターゲット監査情

50

報を第1ノードの監査情報と比較するプロセスにおいて、いくつかの実施例では、ターゲット監査情報及び監査情報が、ノードによって記憶された元のデータではなく、データの固有値の署名である場合、当該比較プロセスは、まず、各ノードの公開鍵に基づいて署名をそれぞれ圧縮解除して、少なくとも1つのターゲット第1ノードのターゲット固有値及び当該第1ノードの固有値を取得し、次に、当該第1ノードの固有値に上記の少なくとも1つのターゲット第1ノードのターゲット固有値が含まれているか否かを判断し、含まれている場合、トランザクションが1対1対応し、且つトランザクションの内容も1対1対応することを意味し、前記少なくとも1つのターゲット第1ノードのターゲット監査情報が当該監査情報と一致すると決定し、一致する場合、当該監査情報が検証に合格したと決定してもよい。

10

【0075】

いくつかの実施例では、監査情報は、第1ノードによって記憶された署名付きのデータであり得、この場合、第2ノードは、各異なるノードによって提供される監査情報内の多次元データを相互比較することができ、多次元データがプリセットされた関数関係に準拠する場合、前記少なくとも1つのターゲット第1ノードのターゲット監査情報が当該監査情報と一致すると決定でき、一致する場合、当該監査情報が検証に合格したと決定できる。

【0076】

いくつかの実施例では、前記少なくとも1つのターゲット第1ノードは、前記監査情報によって指示されるトランザクションのトランザクション相手であってもよい。

【0077】

20

いくつかの実施例では、前記少なくとも1つのターゲット第1ノードは、前記現在の段階の各生産要素に対応するノード及び前記現在の段階の前の段階での前記対象物に対応するノードを含んでもよい。

【0078】

いくつかの実施例では、当該方法は、第1ノードが、任意の段階で生産された製品にバーコードを提供するステップを更に含んでもよく、前記バーコードが指示するアドレスは、前記対象物の最新の第1データ及び最新の第3データのうちの少なくとも1つを提供するために使用されてもよい。当該バーコードは、一次元コード、QRコード（登録商標）などの形であってもよい。バーコードは、特定のネットワークリソースのアドレスを指示でき、当該アドレスに記憶されたデータは、現在の段階での対象物の第1データを更新することにより、コードをスキャンするたびに、当該対象物の最新の第1データ、第1ノードの第2データ、及び最新の第3データのうちの少なくとも1つを取得することができる。このようにして、バーコードによってデータ記憶システム内のデータへのポイントを形成することにより、実際の製品をその製品に対応するオンラインデータと関連付けることができる。ユーザ指向のバーコードの場合、トランザクションのプライバシーに関連する第2データを提供しなくてもよいが、監査作業指向のバーコードの場合、当該バーコードが指示するアドレスで対象物の第2データを提供してもよい。例えば、生乳生産プロセスにおける第1ノードのトランザクションデータなどを提供してもよく、具体的に提供するデータは、実際のニーズに応じて決定されてもよく、本願実施例はこれを限定するものではない。

30

40

【0079】

当該アドレスに記憶されたデータを更新することは、第1ノードによって実行されてもよく、第1データの更新を例にとると、任意の第1ノードがトランザクションを完了した場合、第1データを当該アドレスに更新できる。勿論、当該アドレスに含まれるコンテンツは、更新タイムスタンプを含んでもよく、第1ノードは、更新タイムスタンプを、アップロードされる第1データのタイムスタンプと比較することができ、アップロードされる第1データのタイムスタンプが当該更新タイムスタンプより遅い場合、第1データをアップロードして、当該アドレスに既に記憶された第1データを上書きし、アップロードされる第1データのタイムスタンプが当該更新タイムスタンプより遅くない場合、第1データをアップロードしないことを留意されたい。また、上記の更新は第2ノードによって実行さ

50

れてもよく、その具体的な実行プロセスは、第2ノードが第1ノードの監査情報を受信し、コンセンサスに達成された後に監査情報をアップロードすることであってもよく、これにより、当該アドレスに記憶された第1データの信頼性を保証する。

【0080】

ここで、当該ネットワークリソースのアドレスは、ユニフォームリソース識別子(URI: Uniform Resource Identifier)の形を採用してもよい。

【0081】

例えば、乳製品生産、且つ第1データとしてライフサイクル余剰を例にとると、出荷時に生乳のパッケージにQRコード(登録商標)を印刷又は貼り付けることができ、当該QRコード(登録商標)が、ターゲットURIに基づいて生成されたコードである場合、ユーザが端末で当該QRコード(登録商標)をスキャンすると、ターゲットURIにリダイレクトされ、当該生乳のライフサイクル余剰が15日であることを確認することができる。あるいは、当該ターゲットURIが炭素排出余剰を記憶するために使用される場合、ユーザは更に、当該ターゲットURIを介して、当該生乳の炭素排出余剰を確認することができる。

10

【0082】

勿論、当該バーコードは、複数の第2ノードのネットワークアドレスを更に提供してもよく、当該端末は、スキャンによって得られたデータを複数の第2ノードに送信し、複数の第2ノードは、検証を行い、検証に合格した場合、情報検証合格通知を返信し、このように、ユーザは、当該データが真実で正確であることを確認でき、トランザクションが真実で信頼できるものであることを保証できる。

20

【0083】

本願の実装では、異なる対象物に関連する異なる段階に従って分析を実行し、各段階の生産要素分解して、データチェーン図を形成することができ、各段階のために対応するリソース消費指標を設定し、各生産要素の特性に従って、各段階の消費時間、トランザクション金額、及びリソース消費量などを決定してもよく、上記の3つのタイプのデータは、各段階でストリームの形式で表現され、経済活動におけるデータ間の実際の相関関係に従う。例えば、UCXO(Unspent Carbon Transaction Output、炭素排出余剰)と、UTXO(Unspent Transaction Output、トランザクション余剰)及びUCLO(Unspent Life Cycle Output、ライフサイクル余剰)との間に一定の関連関係があり、ライフサイクルの消費とバリュー消費は必然的に同等のリソース消費を持たせ、UCLOと、UCXO及びUTXOとの間にも一定の関連関係があり、リソース消費とバリュー消費も、必然的にライフサイクルの消費と同等であり、このような潜在的な関連関係により、データが密接に接続され、各第1ノード間でシームレスなデータチェーンを形成するため、データは改ざんできず、実際のデータ値を有し得る。

30

【0084】

更に、当該各第1ノードによって構成される基礎データ層は、各生産要素と関連付けられて、シームレスなデータチェーン層を形成し、且つ、当該基礎データ層は更に、監査層と関連付けられて、二重層のデータチェーン層の構造を形成でき、これにより、データの真正性を保証しながら、データの改ざん防止も保証し、データのセキュリティが大幅に向上する。

40

【0085】

図6を参照すると、乳製品の生産から流通までの異なる段階及び各段階の異なるリンクに関する実施プロセス、且つ関連するリソース消費が炭素排出である場合を例として説明する。

【0086】

まず、下記の具体的な説明に現れるいくつかの用語を以下に紹介する。

【0087】

CC: Carbon Cost、炭素排出消費量

50

U L C O : U n s p e n t L i f e C y c l e O u t p u t、ライフサイクル余剰
E X : e x p e n s e、費用。

【 0 0 8 8 】

次に、乳製品の各段階を紹介する。乳製品のプロセス全体は、生乳（A）——乳製品生産（B）——運送（C）——Eコマース（D）——倉庫保管（E）——物流（F）——消費者（G）などの段階を含み得る。生産から流通までの上記のプロセスに基づいて、生乳は、生産された後、運送により、乳製品生産段階に入ることができ、乳製品の生産が完了した後、運送により、Eコマース段階に入ることができ、Eコマース段階で発売した後、倉庫保管段階に入ることができ、乳製品が注文されると、物流段階に入ることができ、物流段階を完了した後、消費者段階に入る。

10

【 0 0 8 9 】

生乳段階Aでは、関連する異なるリンクに対応する生産要素が、A．HP人的資源、A．PL生産ライン、A．PA包装工場、A．VE運送車両、A．EN発電所、及びA．WA水場などを含むと仮定すると、生乳段階の事業体に対応するノードが第1ノードAで表され、乳製品生産段階の第1ノードが第1ノードBで表される場合、次のプロセスがあり得る。

【 0 0 9 0 】

1、第1ノードAは、生乳を生産する各リンクにおいて、各生産要素に費用EX（A．HP）、EX（A．PL）、EX（A．PA）、EX（A．VE）、EX（A．EN）、EX（A．WA）を支払い、トランザクションが完了した後、当該第1ノードAは、下記の署名データを取得し、そのデータを当該第1ノードAに記憶する。

20

【 0 0 9 1 】

HPがAのトランザクションHASH署名Sig__EX（HP2A）、Sig__CC（HP2A）、及びHPの公開鍵Pubkey（HP）を受け入れ、
PLがAのトランザクションHASH署名Sig__EX（PL2A）、Sig__CC（PL2A）、及びPLの公開鍵Pubkey（PL）を受け入れ、
PAがAのトランザクションHASH署名Sig__EX（PA2A）、Sig__CC（PA2A）、及びPAの公開鍵Pubkey（PA）を受け入れ、
VEがAのトランザクションHASH署名Sig__EX（VE2A）、Sig__CC（VE2A）、及びVEの公開鍵Pubkey（VE）を受け入れ、
ENがAのトランザクションHASH署名Sig__EX（EN2A）、Sig__CC（EN2A）、及びENの公開鍵Pubkey（EN）を受け入れ、及び
WAがAのトランザクションHASH署名Sig__EX（WA2A）、Sig__CC（WA2A）、及びWAの公開鍵Pubkey（WA）を受け入れる。

30

【 0 0 9 2 】

ここで、Pubkey（）は、ノードの公開鍵を指し、Sig__EX（it oj）は、ノードiからノードjに支払われたEXの署名データを指し、Sig__CC（it oj）は、ノードiからノードjに転送されたCCの署名データを指し、上記の署名データは、第1ノードAが資金トランザクションを実行するとき、対応する炭素排出トランザクションも完了することを示す。

40

【 0 0 9 3 】

2、第1ノードAは、炭素排出量指標及び当該段階の炭素排出消費量に従って、生乳段階の炭素排出余剰を取得し、その炭素排出余剰を当該第1ノードAに記憶する。

【 0 0 9 4 】

ここで、炭素排出余剰の具体的な計算式は下記の通りであってもよい。

【 0 0 9 5 】

$$U C X O (A) = U C X O (R e q) - C C (A . H P) - C C (A . P L) - C C (A . P A) - C C (A . V E) - C C (A . E N) - C C (A . W A)$$

【 0 0 9 6 】

ここで、UCXO（A）は、当該生乳段階の炭素排出余剰であり、UCXO（Req）は

50

、プロセス全体の炭素排出余剰指標である。例えば、この指標は、国際会議又は業界標準などによって決定された炭素排出量の総量に従って、各経済リンクの炭素排出割当額に分解できる。 $CC(A, HP)$ は、段階Aの人的資源の炭素排出消費量であり、その値は $CC(HP, 2A)$ と同じである。 $CC(A, PL)$ は、段階Aの生産ラインの炭素排出消費量であり、その値は $CC(PL, 2A)$ と同じである。 $CC(A, PA)$ は、段階Aの包装工場の炭素排出消費量であり、その値は $CC(PA, 2A)$ と同じである。 $CC(A, VE)$ は、段階Aの運送車両の炭素排出消費量であり、その値は $CC(VE, 2A)$ と同じである。 $CC(A, EN)$ は、段階Aの発電所の炭素排出消費量であり、その値は $CC(EN, 2A)$ と同じである。 $CC(A, WA)$ は、段階Aの水場の炭素排出消費量であり、その値は $CC(WA, 2A)$ と同じである。

10

【0097】

例示的に、 $UCXO(A)$ は、単一の製品に正規化された炭素排出余剰であってもよい。

【0098】

3、第1ノードAは第1ノードBとトランザクションを実行し、製造業者Bは、生乳供給者Aに、生乳を購入するための費用 $EX(B, 2A)$ を支払い、トランザクションが完了した後、当該第1ノードAは、出力された生乳のライフサイクル余剰 $ULCO(A)$ を第1ノードBに送信し、下記の署名データを取得して、当該第1ノードAに記憶する。

【0099】

BがAからの生乳のトランザクションHASH署名 $Sig_ULCO(A, 2B)$ 、 $Sig_EX(B, toA)$ 、 $Sig_CC(B, toA)$ 、及びBの公開鍵 $Pubkey(B)$ を受け入れる。

20

【0100】

ここで、 $Sig_ULCO(i, toj)$ は、ノードiからノードjに提供された対象物の $ULCO$ の署名データを指す。

【0101】

上記のプロセス1、2、及び3のいずれかにおいて、当該第1ノードAは、取得した少なくとも2つの次元のデータを相互比較し、前記取得された少なくとも2つの次元のデータが一致する場合、前記少なくとも2つの次元のデータデータを記憶する。

【0102】

4、第1ノードAは、第1ノードの監査情報を取得し、当該第1ノードの監査情報を当該データ記憶システムの複数の第2ノードにブロードキャストする。

30

【0103】

具体的には、当該第1ノードAは、記憶されたデータに基づいて、当該データのハッシュ(HASH)値を生成し、その後、第1ノードAの秘密鍵に基づいて当該ハッシュ値に署名して、署名データを取得し、当該データは、第1ノードAに対応する段階の各リンクの各生産要素の支出と炭素排出余剰を含み、例えば、当該監査情報は下記のコンテンツを含み得る。

【0104】

$Sig((Sig_EX(HP, 2A), Sig_CC(HP, 2A), Pubkey(HP)),$
 $Sig_EX(PL, 2A), Sig_CC(PL, 2A), Pubkey(PL),$
 $Sig_EX(PA, 2A), Sig_CC(PA, 2A), Pubkey(PA),$
 $Sig_EX(VE, 2A), Sig_CC(VE, 2A), Pubkey(VE),$
 $Sig_EX(EN, 2A), Sig_CC(EN, 2A), Pubkey(EN),$
 $Sig_EX(WA, 2A), Sig_CC(WA, 2A), Pubkey(WA),$
 $Sig_ULCO(A, 2B), Pubkey(B))$

40

【0105】

例示的に、上記のコンテンツに加えて、当該監査情報は、第1ノードAの公開鍵 $Pubkey(A)$ 、又は、当該第1ノードAが秘密鍵を用いて現在の段階のコンテキスト情報に署名して得られたコンテキスト署名データを更に含んでもよく、当該コンテキスト情報は

50

、タイムスタンプ、地理的アドレス情報、及びネットワークアドレス情報のうちの少なくとも1と含んでもよい。当該コンテキスト署名データは、`Sig ( loc , time stamp , ip )`として表すことができ、ここで、`loc`は地理的アドレス情報を表し、`time stamp`はタイムスタンプを表し、`ip`はネットワークアドレス情報を表す。

【0106】

この例では、署名データを含む当該監査情報のみを例として説明し、当該署名データは、第1ノードAの秘密鍵に基づいて第1ノードAに記憶された署名データに署名して得られたデータである。別の実施例では、当該監査情報は、第1ノードAの記憶されたデータ、すなわち、各リンクにおける第1ノードAのトランザクション情報を更に含んでもよく、これにより、複数の第2ノードが実際のトランザクションの元のデータを使用して、監査情報をより直観的に検証できるようにする。

10

【0107】

5、複数の第2ノードは、監査情報を受信した後、コンセンサス処理を実行し、コンセンサスに達成された場合、当該第1ノードAによって今回記憶されたデータが真実で正確であると決定する。

【0108】

当該コンセンサスプロセスは、各第2ノードが、監査情報で運ばれる各生産要素の公開鍵に基づいて、当該生産要素が当該第1ノードAと正常にトランザクションした後に送信されたターゲット監査情報を取得し、各生産要素のターゲット監査情報に基づいて、当該第1ノードの監査情報を検証し、監査情報が一致する場合、第1ノードAの監査情報は、当該第2ノードによることによって実行された検証に合格し、第2ノードは、検証合格通知を他の第2ノードにブロードキャストし、任意の第2ノードによって受信された検証合格通知がコンセンサス達成条件に準拠する場合、コンセンサスに達成されたと決定する。

20

【0109】

いくつかの実施例では、上記の各生産要素の監査情報に基づいて当該第1ノードの監査情報を検証するプロセスは、前記監査情報に従って、前記少なくとも1つのターゲット第1ノードによってアップロードされたターゲット監査情報を取得するステップであって、当該ターゲット監査情報は、当該第1ノードとのトランザクションを実行したあとに、各ターゲット第1ノードによってアップロードされた監査情報である、ステップと、前記少なくとも1つのターゲット第1ノードのターゲット監査情報を当該監査情報と比較し、比較結果が一致である場合、当該監査情報が検証に合格したと決定するステップと、を含んでもよい。ここで、前記監査情報に従って、前記少なくとも1つのターゲット第1ノードによってアップロードされたターゲット監査情報を取得する前記ステップは、前記監査情報の少なくとも1つの署名データの公開鍵を取得するステップと、取得された公開鍵に対応する第1ノードを前記少なくとも1つのターゲット第1ノードとして使用するステップと、前記第1ノードの公開鍵に従って、前記少なくとも1つのターゲット第1ノードの監査情報のうちの前記第1ノードの公開鍵を含む監査情報を取得し、取得した監査情報を前記少なくとも1つのターゲット第1ノードのターゲット監査情報として使用するステップと、を含んでもよい。

30

【0110】

例えば、第1ノードAと、生産要素PLに対応する第1ノードPLとの間のトランザクションを例にとると、第1ノードAの監査情報は、`Sig __ EX ( PL 2 A )`と`Sig __ CC ( PL 2 A )`を含み、トランザクションが真実で正確である場合、第1ノードPLの監査情報は、`Sig __ EX ( PL 2 A )`と`Sig __ CC ( PL 2 A )`含むべきである。監査情報の比較による比較結果が一致である場合、当該トランザクションが実際に存在するものであり、且つトランザクションの内容が正確であることを意味する。第1ノードAとすべての生産要素との間の監査情報が、上記のように比較され、比較結果が一致であると確認された場合、当該第2ノードは、前記監査情報が検証に合格したと決定できる。この例では、特定の生産要素の監査情報に対する比較のみを例として説明したが、実際には、第2ノードが検証を実行する場合、各生産要素及び上流の第1ノードによってアップロード

40

50

された監査情報に従って当該監査情報を検証することができ、その具体的なプロセスは、上記の例と同様であり、ここでは繰り返して説明しない。

【 0 1 1 1 】

6、複数の第2ノードは、監査情報を受信した後、コンセンサス処理を実行し、コンセンサスに達しない場合、当該第1ノードAによって今回記憶されたデータに問題があると決定する。

【 0 1 1 2 】

具体的には、コンセンサスに達しないことは、当該第1ノードAに記憶されたデータが真正なデータと一致せず、当該第1ノードに記憶されたデータが偽造されたものなどである可能性があることを意味する。したがって、第2ノードは、後続の処理のために、当該第1ノードAのデータ歪みイベントを記録することができる。データ歪みイベントの発生回数が一定条件を満たす場合、第1ノードに対応する事業体が信用不良の事業体としてマークされか、又は他の処理により、罰と公表の目的に達することができ、本願は、採用される特定の方式を限定するものではない。

10

【 0 1 1 3 】

各第1ノードは、ノードによって実行されたトランザクションに関連する情報を記録し、例えば、トランザクション両方、トランザクション金額、トランザクション位置、及びトランザクション時間などを記録でき、本願実施例では詳細な説明を省略することを留意されたい。

【 0 1 1 4 】

20

生産段階Bでは、関連する異なるリンクに対応する生産要素が、B・HP人的資源、B・PL生産ライン、B・PA包装工場、B・VE運送車両、B・EN発電所、及びB・WA水場などを含むと仮定すると、乳製品の生産段階の第1ノードが第1ノードBで表される場合、次のプロセスがあり得る。

【 0 1 1 5 】

1、第1ノードBは、第1ノードAとトランザクションを実行し、取得された乳製品のライフサイクル余剰はULCO(B)であり(例えば、乳製品の賞味期間が6か月であるなど)、取得された炭素排出余剰はUCXO(A)である。

【 0 1 1 6 】

2、生乳を生産する各リンクにおいて、各生産要素に費用EX(B・HP)、EX(B・PL)、EX(B・PA)、EX(B・VE)、EX(B・EN)、EX(B・WA)を支払い、トランザクションが完了した後、当該第1ノードAB、下記の署名データを取得し、そのデータを当該第1ノードBに記憶する。

30

【 0 1 1 7 】

HPがBのトランザクションHASH署名Sig__EX(HP2B)、Sig__CC(HP2B)、及びHPの公開鍵Pubkey(HP)を受け入れ、
PLがBのトランザクションHASH署名Sig__EX(PL2B)、Sig__CC(PL2B)、及びPLの公開鍵Pubkey(PL)を受け入れ、
PAがBのトランザクションHASH署名Sig__EX(PA2B)、Sig__CC(PA2B)、及びPAの公開鍵Pubkey(PA)を受け入れ、
VEがBのトランザクションHASH署名Sig__EX(VE2B)、Sig__CC(VE2B)、及びVEの公開鍵Pubkey(VE)を受け入れ、
ENがBのトランザクションHASH署名Sig__EX(EN2B)、Sig__CC(EN2B)、及びENの公開鍵Pubkey(EN)を受け入れ、及び
WAがBのトランザクションHASH署名Sig__EX(WA2B)、Sig__CC(WA2B)、及びWAの公開鍵Pubkey(WA)を受け入れる。

40

【 0 1 1 8 】

トランザクションが完了した後、本段階の炭素排出余剰を更に取得でき、当該炭素排出余剰UCXO(B)は、下記の式で計算されてもよい。

【 0 1 1 9 】

50

$$UCXO(B) = UCXO(A) - CC(B, HP) - CC(B, PL) - CC(B, PA) - CC(B, VE) - CC(B, EN) - CC(B, WA)$$

【0120】

ここで、 $CC(B, HP)$ は段階Bの人的資源の炭素排出消費量であり、 $CC(B, PL)$ は段階Bの生産ラインの炭素排出消費量であり、 $CC(B, PA)$ は段階Bの包装工場の炭素排出消費量であり、 $CC(B, VE)$ は段階Bの運送車両の炭素排出消費量であり、 $CC(B, EN)$ は段階Bの発電所の炭素排出消費量であり、 $CC(B, WA)$ は段階Bの水場の炭素排出消費量である。上記の炭素排出消費量の数値関係は、上記の生乳段階の数値関係と同様であり、ここでは繰り返して説明しない。例示的に、 $UCXO(B)$ は、単一の製品に正規化された炭素排出余剰であってもよい。

10

【0121】

乳製品生産段階の資金余剰 $UTXO(B)$ は、下記の式で計算されてもよい。

【0122】

$$UTXO(B) = UTXO(Cap) - ex(B, HP) - ex(B, PL) - ex(B, PA) - ex(B, VE) - ex(B, EN) - ex(B, WA)$$

【0123】

ここで、 $UTXO(Cap)$ は、乳製品生産工場の未使用のトランザクション出力であり、例えば、乳製品生産工場への投資に対応することができる。

【0124】

3、第1ノードBは、第1ノードCとトランザクションを実行し、 $ULCO(B)$ を第1ノードCに出力し、これにより、生産が完了した後、運送車両B・VEで運送を完了できる。これに対して、第1ノードBは、下記の情報を記録する。

20

【0125】

CがBからの乳製品のトランザクションHASH署名 $Sig_ULCO(B2C)$ 、 $Sig_EX(BtoC)$ 、 $Sig_CC(BtoC)$ 、及びCの公開鍵 $Pubkey(C)$ を受け入れる。

【0126】

第1ノードBは、運送前の任意の時点で第1ノードCとトランザクションすることができ、Eコマース会社Cは、製造業者Bに、乳製品を購入するための費用 $EX(D2B)$ を支払い、その後、第1ノードBは、当該トランザクションに関する情報を記憶することを留意されたい。

30

【0127】

4、第1ノードBは、第1ノードの監査情報を取得し、当該第1ノードの監査情報を当該データ記憶システムの複数の第2ノードにブロードキャストする。例えば、当該監査情報は下記のコンテンツを含み得る。

【0128】

$$\begin{aligned} &Sig((Sig_EX(HP2B), Sig_CC(HP2B), Pubkey(HP)), \\ &Sig_EX(PL2B), Sig_CC(PL2B), Pubkey(PL), \\ &Sig_EX(PA2B), Sig_CC(PA2B), Pubkey(PA), \\ &Sig_EX(VE2B), Sig_CC(VE2B), Pubkey(VE), \\ &Sig_EX(EN2B), Sig_CC(EN2B), Pubkey(EN), \\ &Sig_EX(WA2B), Sig_CC(WA2B), Pubkey(WA), \\ &Sig_ULCO(B2C), Pubkey(C)) \end{aligned}$$

40

【0129】

例示的に、監査情報に含まれる他の情報は、前の段階と同様であってもよく、ここでは繰り返して説明しない。同様に、乳製品の各段階は、上記と同様な簿記プロセスを含んでもよく、ここでは繰り返して説明しない。

【0130】

$ULCO(F)$ は、物流段階Dを介して消費者に達した時の乳製品のライフサイクル余剰

50

である。

【 0 1 3 1 】

乳製品は、最終段階、すなわち消費者段階 G を更に含む。消費者段階 G は、個人の炭素排出余剰定格指標 $UCXO(Ind)$ を含んでもよい。例えば、当該指標は、G 2 0 の全球炭素排出の総合指標に基づいて個人に割り当てられた割当額であり得る。更に、本願実施例における乳製品のパッケージに QR コード（登録商標）などをマークしてもよく、消費者段階 G では、消費者は、コードをスキャンして、当該乳製品の $UCLO(F)$ 、すなわち、残りの賞味期間を取得でき、当該 $UCLO(F)$ を乳製品の賞味期間と比較して、当該乳製品の賞味期限が切れているか否かを判断できる。勿論、QR コード（登録商標）に対応するアドレスに記憶された異なるデータに基づいて、消費者は、上記の消費者段階 G に対応する $UCXO(F)$ 、すなわち、本乳製品の炭素排出余剰 $UCXO$ を取得してもよく、消費者が様々な炭素排出余剰の商品を購入すると、消費者自身の $UCXO$ が影響を受ける。当該段階では、 $UCXO(Ind)$ と $UCXO(F)$ を比較して、消費者の炭素消費量が基準を超えているか否かを判断でき、基準を超えているか否かに基づいて、当該消費者の炭素消費余剰定格指標を調整できる。例えば、当該消費者の炭素消費量がプリセットされた期間に基準を超えない場合、当該消費者の炭素消費余剰定格指標が報酬として増加できる。

10

【 0 1 3 2 】

例えば、消費者自身の炭素排出余剰は、 $UCXO(ind) + (UCXO(G) - UCXO(ave))$ であり、ここで、 $UCXO(ave)$ は、プリセットされた平均余剰であり、消費者が消費した商品の炭素排出余剰が業界平均よりも高い場合、当該消費者自身の炭素排出余剰は増加し、消費者が消費した商品の炭素排出余剰が業界平均よりも低い場合、当該消費者自身の炭素排出余剰は減少する。

20

【 0 1 3 3 】

勿論、当該消費者段階 G も、データの記憶を含み、その具体的な原理は上記のプロセスと同様であり、ここでは繰り返して説明しない。

【 0 1 3 4 】

図 7 は、本願実施例によるデータ記憶装置の構造を示す概略図であり、データ記憶システムの第 1 ノードに適用され、図 7 を参照すると、前記装置は、第 1 データ取得モジュール 7 0 1 と、第 2 データ取得モジュール 7 0 2 と、記憶モジュール 7 0 3 と、を備えてもよい。

30

【 0 1 3 5 】

前記第 1 データ取得モジュール 7 0 1 は、対象物の第 1 データを取得するように構成される。

【 0 1 3 6 】

前記第 2 データ取得モジュール 7 0 2 は、前記対象物の第 2 データを取得するように構成され、前記第 1 データと第 2 データは異なる次元のデータであり、次元は、生成から存続期間までの対象物の任意の側面の情報を測定するために使用される。

【 0 1 3 7 】

前記記憶モジュール 7 0 3 は、前記対象物の第 1 データと前記第 2 データを前記第 1 ノードに記憶するように構成される。

40

【 0 1 3 8 】

いくつかの実施例では、前記対象物の第 1 データは、現在の段階での前記対象物のライフサイクル余剰を含んでもよく、前記対象物の第 2 データは、前記現在の段階での前記対象物のトランザクションデータを含んでもよい。

【 0 1 3 9 】

いくつかの実施例では、現在の段階での前記対象物のライフサイクル余剰は、前の段階でのライフサイクル余剰と前記現在の段階での消費時間との間の差であってもよい。

【 0 1 4 0 】

いくつかの実施例では、前記現在の段階の消費時間は、前記現在の段階の特性に従って設

50

定されてもよい。

【0141】

いくつかの実施例では、前記現在の段階での前記対象物のトランザクションデータは、前記現在の段階の各リンクでの前記対象物のトランザクションデータを含んでもよい。

【0142】

いくつかの実施例では、前記現在の段階での前記対象物のトランザクションデータは、前記現在の段階の各リンクでの前記対象物のトランザクションデータの署名データを含んでもよい。

【0143】

いくつかの実施例では、前記対象物の第1データは、前記現在の段階での前記対象物のリソース消費余剰を含んでもよく、前記対象物の第2データは、前記現在の段階での前記対象物のトランザクションデータを含んでもよい。

10

【0144】

いくつかの実施例では、前記装置は、前記対象物の第3データを取得するように構成される第3データ取得モジュールを更に備えてもよく、前記第3データは、前記第1データ及び前記第2データに関連付けられる。

【0145】

前記記憶モジュールは、更に、前記対象物の第1データと前記第2データを第1ノードに記憶するとき、前記対象物の第3データを前記第1ノードに記憶するように構成されてもよい。

20

【0146】

いくつかの実施例では、前記対象物の第3データは、前記現在の段階での前記対象物のリソース消費余剰を含んでもよい。

【0147】

いくつかの実施例では、前記現在の段階での前記対象物のリソース消費余剰は、前の段階でのリソース消費余剰と前記現在の段階でのリソース消費量との間の差であってもよい。

【0148】

いくつかの実施例では、前記現在の段階でのリソース消費量は、前記現在の段階の各リンクでの前記対象物の在のリソース消費量の合計であってもよい。

【0149】

いくつかの実施例では、前記リソース消費余剰は、炭素排出余剰であってもよい。

30

【0150】

いくつかの実施例では、前記装置は、前記第1ノードの監査情報を取得するように構成される監査情報取得モジュールであって、前記監査情報は、前記第1ノードによって記憶されたデータを指示するものである監査情報取得モジュールと、前記第1ノードの監査情報を前記データ記憶システムの複数の第2ノードにブロードキャストするように構成される送信モジュールと、を更に備えてもよい。

【0151】

いくつかの実施例では、前記監査情報は、前記第1ノードによって記憶されたデータを含んでもよい。

40

【0152】

いくつかの実施例では、前記監査情報は、プリセットされた期間内に前記第1ノードによって記憶されたデータを含んでもよい。

【0153】

いくつかの実施例では、前記監査情報は、前記第1ノードによって記憶されたデータの固有値を含んでもよい。

【0154】

いくつかの実施例では、前記監査情報は、プリセットされた期間内に前記第1ノードによって記憶されたデータの固有値を含んでもよい。

50

【 0 1 5 5 】

いくつかの実施例では、固有値は、ハッシュ値であってもよい。

【 0 1 5 6 】

いくつかの実施例では、前記監査情報は、署名データを含んでもよく、前記署名データは、前記第 1 ノードが前記第 1 ノードの秘密鍵を用いて、前記第 1 ノードによって記憶されたデータに署名して得られたものであってもよい。

【 0 1 5 7 】

いくつかの実施例では、前記監査情報は、前記第 1 ノードの公開鍵を更に含んでもよい。

【 0 1 5 8 】

いくつかの実施例では、前記監査情報は、前記第 1 ノードが秘密鍵を用いて現在の段階でのコンテキスト情報に署名して得られたコンテキスト署名データを更に含んでもよく、前記コンテキスト情報は、タイムスタンプ、地理的アドレス情報、及びネットワークアドレス情報のうちの少なくとも 1 つを含んでもよい。

10

【 0 1 5 9 】

いくつかの実施例では、当該記憶モジュールは、前記対象物の第 1 データと前記第 2 データを前記第 1 ノードのリソースプールに記憶し、任意の第 2 ノードによって送信されたコンセンサス確認通知を受信した場合、前記リソースプールに記憶された第 1 データ及び第 2 データを前記第 1 ノードのプリセットされた記憶空間に記憶するように構成されてもよい。

【 0 1 6 0 】

20

いくつかの実施例では、当該記憶モジュールは、任意の第 2 ノードによって送信されたコンセンサス確認通知を受信した場合、前記対象物の第 1 データと前記第 2 データを前記第 1 ノードに記憶するように構成されてもよい。

【 0 1 6 1 】

いくつかの実施例では、当該装置は、比較モジュールを更に備えてもよく、前記比較モジュールは、取得した少なくとも 2 つの次元のデータを相互比較し、前記取得された少なくとも 2 つの次元のデータが一致すると決定した時に、記憶操作を実行するように当該記憶モジュールをトリガするように構成される。

【 0 1 6 2 】

いくつかの実施例では、前記装置は、任意の段階で生産された製品にバーコードを提供するように構成されるバーコードモジュールを更に備えてもよく、前記バーコードが指示するアドレスは、最新の第 1 データ、最新の第 2 データ、及び最新の第 3 データのうちの少なくとも 1 つを前記対象物に提供するために使用される。

30

【 0 1 6 3 】

いくつかの実施例では、前記バーコードは、スキャン端末が、スキャンによって得られたデータを前記複数の第 2 ノードに送信して検証するように、複数の第 2 ノードのネットワークアドレスを更に提供してもよい。

【 0 1 6 4 】

図 8 は、本願実施例によるデータ検証装置の構造を示す概略図であり、データ記憶システムの任意の第 2 ノードに適用され、前記データ記憶システムの複数の第 2 ノードには、コンセンサスメカニズムが配置されており、図 8 を参照すると、当該装置は、受信モジュール 8 0 1 と、検証モジュール 8 0 2 と、送信モジュール 8 0 3 と、を備えてもよい。

40

【 0 1 6 5 】

前記受信モジュール 8 0 1 は、第 1 ノードの監査情報を受信するように構成され、前記監査情報は、前記第 1 ノードに記憶されたデータを指示する。

【 0 1 6 6 】

前記検証モジュール 8 0 2 は、少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報に基づいて前記監査情報を検証するように構成される。

【 0 1 6 7 】

50

前記送信モジュール 803 は、検証に合格した場合、前記データ記憶システムにおいて検証合格通知をブロードキャストするように構成される。

【0168】

前記検証モジュール 802 は、更に、受信した検証合格通知がコンセンサス達成条件を満たす場合、前記監査情報に対するコンセンサスが達成されたと決定するように構成される。

【0169】

いくつかの実施例では、送信モジュール 802 は、更に、前記監査情報に対するコンセンサスが達成された場合、コンセンサス確認通知を前記第 1 ノードに送信するように構成されてもよい。前記ターゲット監査情報は、前記第 1 ノードとランザクションする各ターゲット第 1 ノードによって記憶されたデータを指示するものであり得る。

10

【0170】

いくつかの実施例では、検証モジュール 802 は、前記監査情報に従って、前記少なくとも 1 つのターゲット第 1 ノードによってアップロードされたターゲット監査情報を取得し、前記少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報を当該監査情報と比較し、前記少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報が前記監査情報と一致する場合、前記監査情報が検証に合格したと決定するように構成されてもよい。

【0171】

いくつかの実施例では、前記検証モジュール 802 は、前記監査情報の少なくとも 1 つの署名データの公開鍵を取得し、取得された公開鍵に対応する第 1 ノードを前記少なくとも 1 つのターゲット第 1 ノードとして使用し、前記公開鍵に従って、前記公開鍵に対応する第 1 ノードを含む監査情報を取得し、前記取得した監査情報を前記少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報として使用するよう構成されてもよい。

20

【0172】

いくつかの実施例では、前記少なくとも 1 つのターゲット第 1 ノードは、前記監査情報によって指示されるランザクションのランザクション相手であってもよい。

【0173】

いくつかの実施例では、前記少なくとも 1 つのターゲット第 1 ノードは、前記現在の段階の各生産要素に対応するノード及び前記現在の段階の前の段階での前記対象物に対応するノードを含んでもよい。

30

【0174】

いくつかの実施例では、データ記憶システムを開示し、前記システムは、複数の第 1 ノードと、複数の第 2 ノードを備え、前記データ記憶システムの複数の第 2 ノードには、コンセンサスメカニズムが配置されており、

前記複数の第 1 ノードの各第 1 ノードは、対象物の第 1 データを取得し、前記対象物の第 2 データを取得し、前記対象物の第 1 データと前記第 2 データを前記第 1 ノードに記憶し、前記第 1 ノードの監査情報を取得し、前記第 1 ノードの監査情報を前記データ記憶システムの複数の第 2 ノードにブロードキャストするように構成され、前記第 1 データと前記第 2 データは異なる次元のデータであり、前記監査情報は、前記第 1 ノードによって記憶されたデータを指示するものであり、

40

前記複数の第 2 ノードの各第 2 ノードは、前記第 1 ノードの監査情報を受信し、少なくとも 1 つのターゲット第 1 ノードのターゲット監査情報に基づいて前記監査情報を検証し、検証に合格した場合、前記データ記憶システムにおいて検証合格通知をブロードキャストし、受信した検証合格通知がコンセンサス合格条件を満たす場合、前記監査情報がコンセンサスに合格したと決定するように構成され、前記監査情報は、前記第 1 ノードに記憶されたデータを指示する。

【0175】

上記全ての任意選択的な技術的解決手段において、任意の組み合わせにより本出願の任意選択的な実施例を構成することができる。ここで詳しく説明しないようにする。

【0176】

50

いくつかの実施例では、コンピュータ機器を開示し、前記コンピュータ機器は、プロセッサとメモリとを備え、少なくとも1つの命令が前記メモリに記憶され、前記命令が前記プロセッサによりロードおよび実行されると、上記のデータ記憶方法のステップを実現する。ここでのデータ記憶方法のステップは、上記の各実施例におけるデータ記憶方法のステップであってもよい。

【0177】

いくつかの実施例では、コンピュータ可読記憶媒体を開示し、少なくとも1つの命令が前記記憶媒体に記憶され、前記命令がプロセッサによりロードおよび実行されると、上記のデータ記憶方法のステップを実現する。ここでのデータ記憶方法のステップは、上記の各実施例におけるデータ記憶方法のステップであってもよい。

10

【0178】

いくつかの実施例では、コンピュータ機器を開示し、前記コンピュータ機器は、プロセッサとメモリとを備え、少なくとも1つの命令が前記メモリに記憶され、前記命令が前記プロセッサによりロードおよび実行されると、上記のデータ検証方法のステップを実現する。ここでのデータ検証方法のステップは、上記の各実施例におけるデータ検証方法のステップであってもよい。

【0179】

いくつかの実施例では、コンピュータ可読記憶媒体を開示し、少なくとも1つの命令が前記記憶媒体に記憶され、前記命令がプロセッサによりロードおよび実行されると、上記のデータ検証方法のステップを実現する。ここでのデータ検証方法のステップは、上記の各実施例におけるデータ検証方法のステップであってもよい。

20

【0180】

いくつかの実施例では、データ記憶システムを開示し、前記システムは、複数の第1ノード及び複数の第2ノードを含み、前記データ記憶システムの複数の第2ノードは、コンセンサスメカニズムを備え、ここで、

前記複数の第1ノードの各第1ノードは、対象物の第1データを取得し、対象物の第2データを取得し、前記対象物の前記第1データ及び前記第2データを第1ノードに記憶し、前記第1ノードの監査情報を取得し、前記第1ノードの監査情報を前記データ記憶システムの複数の第2ノードにブロードキャストするように構成され、前記第1データと前記第2データは異なる次元のデータであり、前記次元は、生成から存続期間までの前記対象物の任意の側面の情報を測定するために使用され、前記監査情報は、前記第1ノードによって記憶されたデータを指示するものであり、

30

前記複数の第2ノードの各第2ノードは、前記第1ノードの監査情報を受信し、少なくとも1つのターゲット第1ノードのターゲット監査情報に基づいて前記監査情報を検証し、検証に合格した場合、前記データ記憶システムにおいて検証合格通知をブロードキャストし、受信した検証合格通知がコンセンサス達成条件を満たす場合、前記監査情報に対するコンセンサスが達成されたと決定するように構成され、前記監査情報は、前記第1ノードに記憶されたデータを指示するものである。

【0181】

例示的な実施例において、命令を含むメモリのようなコンピュータ可読記憶媒体を更に提供する。上記命令は、端末におけるプロセッサにより実行され、上記実施例の任意の方法を実現させる。例えば、前記コンピュータ可読記憶媒体はROM、ランダムアクセスメモリ(RAM)、CD-ROM、磁気テープ、フレキシブルディスク及び光学データ記憶装置などであってもよい。

40

【0182】

上記実施例の全て又は一部の工程はハードウェアにより実行されてもよいし、プログラム命令に係るハードウェアにより実行されてもよく、当該プログラムは、コンピュータ可読記憶媒体に記憶されてもよく、上記言及した記憶媒体は、読み取り専用メモリ、磁気ディスク又は光ディスクなどであってもよいことは当業者であれば理解されるべきである。

【0183】

50

上記は本願の好ましい実施例に過ぎず、本願を限定することを意図するものではなく、本願の精神及び原則内で行われるあらゆる修正、同等の置換、改善などは、本願の保護範囲に含まれるべきである。

【符号の説明】

【 0 1 8 4 】

200 コンピュータ機器

201 プロセッサ

202 メモリ

701 第1データ取得モジュール

702 第2データ取得モジュール

703 記憶モジュール

801 受信モジュール

802 検証モジュール

803 送信モジュール

10

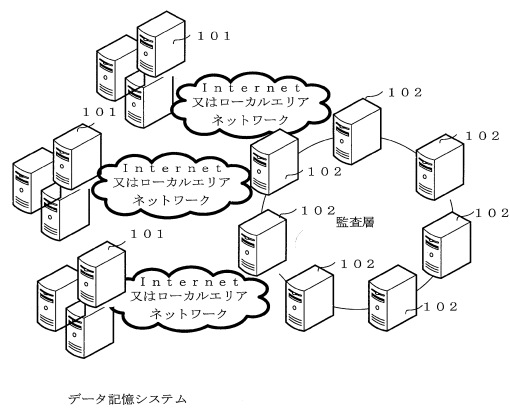
20

30

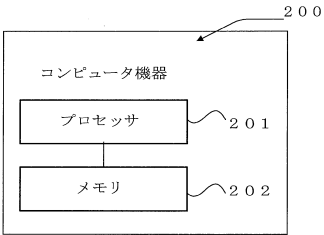
40

50

【図面】
【図 1】

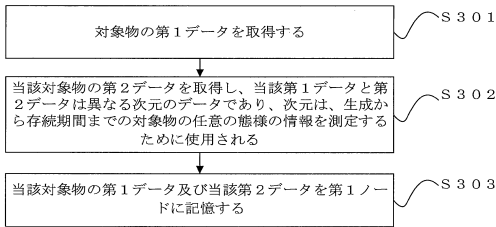


【図 2】

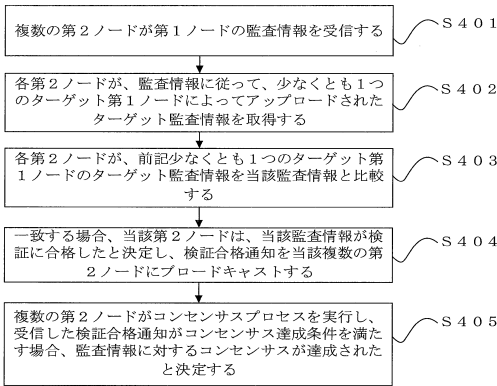


10

【図 3】



【図 4】



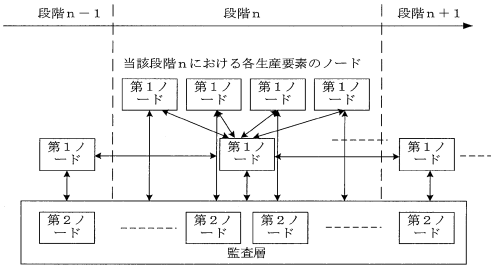
20

30

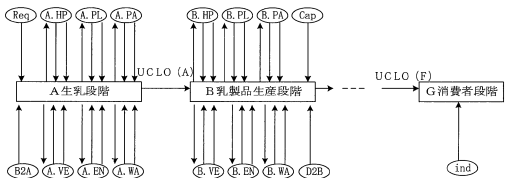
40

50

【図 5】

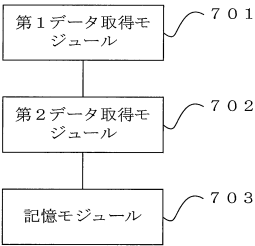


【図 6】

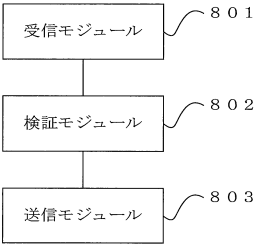


10

【図 7】



【図 8】



20

30

40

50

フロントページの続き

- 中華人民共和国 5 1 8 0 5 7 ▲広▼▲東▼省深▲セン▼市南山区高新区科技中一路 ▲騰▼▲訊▼
大廈 3 5 ▲層▼
- (72)発明者 郭 ▲銳▼
中華人民共和国 5 1 8 0 5 7 ▲広▼▲東▼省深▲セン▼市南山区高新区科技中一路 ▲騰▼▲訊▼
大廈 3 5 ▲層▼
- (72)発明者 ▲ ▼ ▲海▼涛
中華人民共和国 5 1 8 0 5 7 ▲広▼▲東▼省深▲セン▼市南山区高新区科技中一路 ▲騰▼▲訊▼
大廈 3 5 ▲層▼
- (72)発明者 李 波
中華人民共和国 5 1 8 0 5 7 ▲広▼▲東▼省深▲セン▼市南山区高新区科技中一路 ▲騰▼▲訊▼
大廈 3 5 ▲層▼
- (72)発明者 王 宗友
中華人民共和国 5 1 8 0 5 7 ▲広▼▲東▼省深▲セン▼市南山区高新区科技中一路 ▲騰▼▲訊▼
大廈 3 5 ▲層▼
- (72)発明者 ▲張▼ 建俊
中華人民共和国 5 1 8 0 5 7 ▲広▼▲東▼省深▲セン▼市南山区高新区科技中一路 ▲騰▼▲訊▼
大廈 3 5 ▲層▼
- 審査官 宮司 卓佳
- (56)参考文献 特開 2 0 0 3 - 0 4 4 6 6 2 (J P , A)
韓国登録特許第 1 8 7 1 4 6 8 (K R , B 1)
米国特許出願公開第 2 0 1 0 / 0 1 2 7 8 6 8 (U S , A 1)
- (58)調査した分野 (Int.Cl. , D B 名)
G 0 6 F 2 1 / 6 4
H 0 4 L 9 / 3 2