

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)公開番号

特開2022-135984

(P2022-135984A)

(43)公開日 令和4年9月15日(2022.9.15)

(51)国際特許分類

H 0 4 L 9/32 (2006.01)

F I

H 0 4 L 9/32 2 0 0 B

H 0 4 L 9/32 2 0 0 Z

審査請求 有 請求項の数 18 O L 外国語出願 (全21頁)

(21)出願番号	特願2022-27882(P2022-27882)	(71)出願人	390039413
(22)出願日	令和4年2月25日(2022.2.25)		シーメンス アクチエンゲゼルシャフト
(31)優先権主張番号	21161018		Siemens Aktiengesellschaft
(32)優先日	令和3年3月5日(2021.3.5)		ドイツ連邦共和国 D-80333 ミュンヘン ヴェアナーフォンシーメンスシュトラッセ 1
(33)優先権主張国・地域又は機関	欧州特許庁(EP)	(74)代理人	110003317
			特許業務法人山口・竹本知的財産事務所
		(74)代理人	100075166
			弁理士 山口 巖
		(74)代理人	100133167
			弁理士 山本 浩
		(74)代理人	100169627
			弁理士 竹本 美奈

最終頁に続く

(54)【発明の名称】 製品関連エンティティのESGデータに関する情報を交換するエコシステム

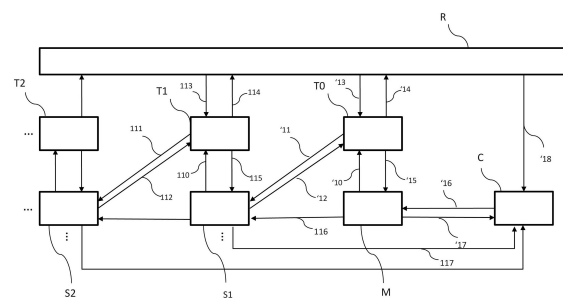
(57)【要約】

【課題】製品関連エンティティのESGデータに関する情報を交換するエコシステム

【解決手段】本発明は、サブジェクト参加者と、製品関連エンティティのESGデータに関する情報を交換する通信ネットワークの少なくとも1つのサートファイヤ参加者と、対応する方法とを備え、サブジェクト参加者の少なくとも1つは、通信ネットワークを介してESGクレデンシャルから導出された少なくとも1つのプルーフを提供するように構成され、少なくとも1つのサブジェクト参加者は、ESGクレデンシャルを提供する少なくとも1人のサートファイヤの真正性を割り当てるように構成され、プルーフは、ESGデータの完全性またはESGデータの一部を割り当てるようにさらに具体化され、分散レジストリのシステムは、少なくとも1人のサートファイヤの少なくとも1つの公開鍵を管理するように構成される。

【選択図】図1

Fig. 1



【特許請求の範囲】

【請求項 1】

製品関連エンティティの ESG データに関する情報を交換する通信ネットワークの、複数のサブジェクト参加者 (M、S1、S2)、少なくとも 1 つのベリファイヤ参加者 (C)、および少なくとも 1 つのサートファイヤ参加者 (T、T0) を含むシステムであって、

少なくとも 1 つの前記サブジェクト参加者 (M) が、前記通信ネットワークを介して ESG クレデンシャルから導出された少なくとも 1 つのプルーフを提供するように構成され、少なくとも 1 つの前記ベリファイヤ参加者 (C) が、前記通信ネットワークを介して少なくとも 1 つのプルーフを受信するように構成され、前記少なくとも 1 つのサブジェクト参加者 (M) が、前記少なくとも 1 つのサートファイヤ参加者 (T、T0) から前記 ESG クレデンシャルを受信するように構成され、

前記プルーフが、前記 ESG クレデンシャルを提供する前記少なくとも 1 つのサートファイヤ参加者 (T、T0) の真正性を割り当てるように具体化され、

前記プルーフが、前記 ESG データの完全性、又は前記 ESG データの一部、又は前記 ESG データの属性を、割り当てるように具体化され、

前記システムが、分散レジストリ (R) のノードをさらに含み、前記分散レジストリ (R) が、前記少なくとも 1 つのサートファイヤ参加者 (T、T0) の少なくとも 1 つの公開鍵を管理するように構成され、

前記少なくとも 1 つのベリファイヤ参加者 (C) が、前記ベリファイヤ参加者 (C) の計算構成要素を介して公開鍵との真正性および完全性を暗号的に検証できるように、前記分散レジストリ (R) が、前記プルーフに対応する前記少なくとも 1 つのサートファイヤ参加者 (T、T0) の公開鍵を、前記少なくとも 1 つのベリファイヤ参加者 (C) に提供する、

システム。

【請求項 2】

前記少なくとも 1 つのサートファイヤ参加者 (T、T0) が、さらなるサブジェクト参加者 (S1) のさらなるベリファイヤ参加者として、付加的に具体化される、請求項 1 に記載のシステム。

【請求項 3】

前記少なくとも 1 つのサブジェクト参加者 (M) が、前記少なくとも 1 つのサートファイヤ参加者 (T、T0) またはさらなるサートファイヤ参加者として、追加的に具体化される、請求項 1 または 2 に記載のシステム。

【請求項 4】

前記少なくとも 1 つのサートファイヤ参加者 (T、T0) が、前記ノードを介して前記分散レジストリ (R) への読み出しおよび書き込みアクセスを有するように構成され、

前記少なくとも 1 つのベリファイヤ参加者 (C) が、前記ノードを介して少なくとも 1 つの読み出しアクセスを有するように構成されている、

前記請求項の 1 項に記載のシステム。

【請求項 5】

製品関連エンティティの ESG データに関する情報を交換する通信ネットワークの、少なくとも 1 つのサブジェクト参加者 (M) によって、ESG クレデンシャルから導出された少なくとも 1 つの暗号プルーフを提供するためのコンピュータ実装方法であって、

前記ネットワークが、複数のサブジェクト参加者 (M、S1、S2)、少なくとも 1 つのベリファイヤ参加者 (C) 及び少なくとも 1 つのサートファイヤ参加者 (T、T0) を含み、

前記方法が、前記少なくとも 1 つのサブジェクト参加者 (M) によって、前記プルーフを生成することを含み、

前記プルーフが、前記 ESG クレデンシャルを提供する前記少なくとも 1 つのサートファイヤ参加者 (T、T0) の真正性を割り当て、前記 ESG クレデンシャルが、前記

10

20

30

40

50

少なくとも1つのサートィファイヤ参加者（T、T0）から、前記少なくとも1つのサブジェクト参加者（M）によって受信され、

前記少なくとも1つのサートィファイヤ参加者（T、T0）の公開鍵は、分散レジストリ（R）を介して、前記プルーフから少なくとも1つのベリファイヤ参加者（C）によって導出され、前記真正性を検証するために前記少なくとも1つのベリファイヤ参加者（C）によって使用され、

前記プルーフが、前記ESGデータの完全性、またはESGデータの一部、または前記ESGデータの属性を、さらに割り当て、

前記少なくとも1つのサートィファイヤ参加者（T、T0）の公開鍵が、前記ベリファイヤ参加者（C）によって、前記完全性を検証するために使用される、
方法。

10

【請求項6】

前記ESGクレデンシャルが、前記少なくとも1つのサートィファイヤ参加者（T、T0）によって生成される、請求項5に記載の方法。

【請求項7】

前記ESGクレデンシャルを生成するために、前記少なくとも1つのサートィファイヤ参加者（T、T0）が、前記製品関連エンティティのESGデータに関連するさらなるサブジェクト参加者（S1）の少なくとも1つのさらなるプルーフを検証するとともに、再帰的ESGクレデンシャルを生成する、請求項6に記載の方法。

【請求項8】

前記再帰的ESGクレデンシャルが、前記サブジェクト参加者のESGデータのためのローカルESGセクションと、前記さらなるサブジェクト参加者のESGデータのための外部ESGセクションを含む、請求項7に記載の方法。

20

【請求項9】

前記少なくとも1つのサブジェクト参加者（M）が、要求メッセージの送信によって、前記少なくとも1つのサートィファイヤ参加者（T、T0）から前記ESGクレデンシャルを要求する、請求項5から8のいずれか1項に記載の方法。

【請求項10】

前記少なくとも1つのサートィファイヤ参加者（T、T0）が、公開アドレスおよび対応する公開鍵を前記分散レジストリ（R）に登録する、請求項5から9のいずれか1項に記載の方法。

30

【請求項11】

前記少なくとも1つのサートィファイヤ参加者（T、T0）が、前記少なくとも1つのサブジェクト参加者（M）のためのクレデンシャル定義を定義し、前記クレデンシャル定義を前記分散レジストリ（R）に登録する、請求項5から10のいずれか1項に記載の方法。

【請求項12】

前記完全性を割り当てるための第1の暗号署名メカニズムが、前記少なくとも1つのサートィファイヤ参加者（T、T0）の秘密鍵で生成された第1の暗号署名に基づいており、第1の暗号検証メカニズムが、前記少なくとも1人のサートィファイヤ参加者（T、T0）の前記公開鍵で前記第1の暗号署名を検証することに基づいている、請求項5から11のいずれか1項に記載の方法。

40

【請求項13】

前記完全性を割り当てるための第1の暗号署名メカニズムが、前記サートィファイヤ参加者の信頼されたグループに共通の秘密鍵で生成された暗号グループ署名に基づいているか、または信頼されたサートィファイヤ参加者のグループの2以上のサートィファイヤ参加者によって生成された暗号しきい値署名に基づいており、第1の暗号検証メカニズムが、サートィファイヤ参加者の信頼されたグループの公開鍵で前記第1の暗号署名を検証することに基づいている、請求項5から12のいずれか1項に記載の方法。

【請求項14】

50

前記第 1 の暗号署名メカニズムがゼロ知識プルーフに基づいている、請求項 5 から 13 のいずれか 1 項に記載の方法。

【請求項 15】

前記少なくとも 1 つのサブジェクト参加者 (M) が、前記少なくとも 1 つのサートファイヤ参加者 (T、T0) またはさらに別のサートファイヤ参加者として追加的に具体化され、前記 ESG クレデンシャルが、ルートオブトラスト技術を使用して前記少なくとも 1 つのサブジェクト参加者 (M) によって生成される、請求項 5 から 14 のいずれか 1 項に記載の方法。

【請求項 16】

前記少なくとも 1 つのサブジェクト参加者 (M) が、前記ネットワーク内の複数の通信メッセージに対して複数の仮名を使用する、請求項 5 から 15 のいずれか 1 項に記載の方法。

【請求項 17】

前記少なくとも 1 つのサブジェクト参加者 (M) が、第 2 の暗号署名メカニズムおよび前記少なくとも 1 つのサブジェクト参加者 (M) の秘密鍵を使用することによって、前記 ESG クレデンシャルから前記プルーフを導出する、請求項 5 から 16 のいずれか 1 項に記載の方法。

【請求項 18】

前記第 2 の暗号署名メカニズムがゼロ知識プルーフに基づいている、請求項 5 から 17 のいずれか 1 項に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、サブジェクト参加者 (subject participant)、少なくとも 1 つのベリファイヤ参加者 (verifier participant)、および製品関連エンティティの ESG データに関する情報を交換する通信ネットワークの少なくとも 1 つのサートファイヤ参加者 (certifier participant) と、対応する方法とを含むシステムに関する。

【背景技術】

【0002】

企業の財務パフォーマンスは、企業のサステナビリティや社会への影響とますます結びついているため、多くの企業は、環境、社会及び企業のガバナンス (略して、ESG)、目標を宣言し、そのような基準を管理ボードの報奨スキームに含めている。さらに、産業活動の環境外部性は、税金やキャップ、取引システムを持ついくつかの市場において、ますます金額化されている。ESG の重要な目標の 1 つは、脱炭素化であり、これは、企業、生産および製品レベルで CO₂ 換算、略して CO₂e として報告される温室効果ガス (GHG) の排出を削減することを指す。世界経済は、気候変動による深刻な影響から社会や経済を保護するために、脱炭素化されなければならない。GHG 排出量を削減する必要性は、世界的には、CO₂ 課税と排出量取引スキームに関する法規制に導かれている。両スキームとも、排出関連の損害の負担を、それに責任を負う者に転換し、それを削減または補償できる者に移すことを目的としている。

【0003】

環境負荷の透明性へのニーズに応えるため、ISO 14040 シリーズ (製品ライフサイクル LCA) や ISO / TS 14072 (組織 LCA) などの会計基準が策定され、企業、製造サイト (組織)、製品、サービスの特定の排出量算定基準：温室効果ガス (GHG) プロトコル、PAS 2050、ISO 14067 が策定されている。これは、主体が自らの運営を確実に説明するのに役立つ。

【0004】

ESG 情報の計算と編集には、ライフサイクルアセスメント (LCA) データベースを使用する。例えば、LCA データベースは、製品の CO₂ フットプリント (略して PCF)、部品の一般的なタイプの値を検索するために使用され、製品に関する実際の情報はデー

10

20

30

40

50

データベース内の一般的な情報と等しいと想定する。このようなデータベースシステムは、スフィアラ（Sphera）またはエコインヴェント（Ecoinvent）によって販売されている。

【0005】

仮定に基づくアプローチは、与えられた製品のバッチの生産と物流におけるサプライヤ固有の変動を無視し、従って、共有ESGデータの誤りを導く。

【発明の概要】

【発明が解決しようとする課題】

【0006】

したがって、最先端技術における前述の欠点を考慮すると、参加者の機密性とプライバシーを保護しつつ、エコシステムの参加者間でESG情報を確実かつ認証可能に共有する方法とシステムを提供することが本開示の目的である。

【課題を解決するための手段】

【0007】

これらの目的は、独立クレームの技術的事項によって対処される。有利な実施形態は、従属クレームにおいて提案される。

【0008】

本発明は、製品関連エンティティのESGデータに関する情報を交換する通信ネットワークの、複数のサブジェクト参加者、少なくとも1つのベリファイヤ参加者、および少なくとも1つのサートィファイヤ参加者を含むシステムであって、少なくとも1つのサブジェクト参加者が、通信ネットワークを介してESGクレデンシャルから導出された少なくとも1つのブルーフを提供するように構成され、少なくとも1つのベリファイヤ参加者が、通信ネットワークを介して少なくとも1つのブルーフを受信するように構成され、少なくとも1つのサブジェクト参加者が、少なくとも1つのサートィファイヤ参加者からESGクレデンシャルを受信するように構成され、

ブルーフが、ESGクレデンシャルを提供する少なくとも1つのサートィファイヤ参加者の真正性（authenticity）を割り当てるように具体化され、

ブルーフが、ESGデータの完全性（integrity）、又はESGデータの一部、又はESGデータの属性を、割り当てるように具体化され、

システムが、分散レジストリのノードをさらに含み、分散レジストリが、少なくとも1つのサートィファイヤ参加者の少なくとも1つの公開鍵を管理するように構成され、

少なくとも1つのベリファイヤ参加者が、ベリファイヤ参加者のコンピューティング構成要素を介して公開鍵との真正性および完全性を暗号的に検証できるように、分散レジストリが、ブルーフに対応する少なくとも1つのサートィファイヤ参加者の公開鍵を、少なくとも1つのベリファイヤ参加者に提供する。

【0009】

このシステムは、例えば、複数のサブジェクト参加者と、複数のベリファイヤ参加者と、複数のサートィファイヤ参加者とを含む。システムは、好ましくは、柔軟に拡張可能であり、追加のサブジェクト参加者、ベリファイヤ参加者またはサートィファイヤ参加者が、時間とともに通信ネットワークに追加され得る。システム内の通信チャネルとして、例えば任意の適切なインターネットプロトコルに基づく任意の適切なチャネルが使用される。システムは、たとえば、特定の製品やサービスの製造や提供のために相互作用する生態系や組織のネットワークである。

【0010】

参加者、特にベリファイヤ参加者とサブジェクト参加者は、製品関連エンティティのESGデータに関する情報を共有する。製品関連エンティティは、たとえば、該当する製品のサプライチェーンのサプライヤ、製造者、ユーティリティ・プロバイダ、または物流プロバイダであるサブジェクト参加者である。製品をサービスにすることもできる。製品関連エンティティは、さらに、たとえば、成果物、たとえば、会社、製造サイト、製品、サービス、製品の一部またはコンポーネント、製品提供に関連する、または製品開発プロセ

10

20

30

40

50

スに關与するアーティファクトである。

【0011】

例えば、あるサプライヤが一定の条件下で1つの製品コンポーネントのみを製造し、提供する場合、そのサプライヤはサブジェクト参加者として製品関連エンティティと見なすことができる。たとえば、サプライヤが異なる条件（異なるプロダクションサイトなど）でプロデュースする場合、同じサプライヤの各プロダクションサイトは、異なる製品関連エンティティと見なすことができる。

【0012】

たとえば、製品関連エンティティは、サートیفアイヤ参加者によって生成されるESGクレデンシャル定義で定義される。このクレデンシャル定義は、サートیفアイヤ参加者によって認定される属性に依存する。製品関連エンティティが製造者の製造現場などの場合、ESGデータまたはこの製造現場の製造者の責任にあるESGデータの一部が認定される。クレデンシャル定義は、そのデータに関するすべてのメタデータを記述する。つまり、将来発行されるクレデンシャルのスキーマを定義する。クレデンシャル定義は、例えば、サブジェクト参加者によるクレデンシャルの要求に基づいて、サートیفアイヤ参加者によって作成される。ここで、サブジェクト参加者は、認証されるべきデータまたは属性を定義する。

【0013】

ESG情報は、環境、社会、および／または企業のガバナンス情報に関するものである。これは、例えば、気体ガス排出量の値、CO₂設置面積指標、作業条件、材料源指標に関するものである。

【0014】

分散レジストリは、少なくとも1つのサートیفアイヤ参加者の公開鍵を管理するために使用される。例えば、各サートیفアイヤ参加者について、対応する公開鍵が、分散レジストリに保管される。分散レジストリは、分散型データベース、例えば分散台帳技術に基づくデータベース、特にブロックチェーンデータベースである。分散レジストリは、システム内の信頼されたレジストリである。分散レジストリの主な機能は、サートیفアイヤ参加者の公開鍵を信頼できる方法で保存し、提供することである。分散型レジスタは、エコシステム参加者のみがアクセス可能であることが好ましい。分散レジストリは、例えば、それぞれの公開鍵にそれぞれの公開アドレスまたは仮名または識別子を割り当て、この割り当てを格納することによって、公開鍵を管理する。

【0015】

参加者は例えば公開アドレスで表され、通信ネットワーク内の参加者間の通信は公開アドレスを用いて実現される。通信は、例えば公開アドレスを使用するプロトコルによって実現される。通信ネットワーク内でメッセージを処理するために、参加者は、好ましくは、計算構成要素または処理ユニットを含む。例えば、計算構成要素は、中央処理装置と、CPUに動作可能に接続されたメモリとを含んでもよい。

【0016】

たとえば、分散レジストリには、サートیفアイヤ参加者によって登録されたクレデンシャル定義が保存される。サートیفアイヤ参加者は、サブジェクト参加者に対して発行するESGクレデンシャルのスキーマを定義する。これにより、認証者は、分散データベースのノードを介してアクセス可能なESGクレデンシャル定義を使用して、認証されたデータを処理できるようになる。

【0017】

例えば、参加者の通信ネットワークは、ノードと対話するために使用される。このようにして、参加者を含むシステムが構築され、好ましくは、すべての参加者がそれぞれの計算構成要素とノードとを含む。少なくとも1つのサートیفアイヤ参加者またはすべてのサートیفアイヤ参加者が、少なくとも1つのノードと対話するか、ノードを構成する。さらに、少なくとも1つのペリファイヤ構成要素またはすべてのペリファイヤ構成要素は、少なくとも1つのノードと対話するか、またはノードを含む。例えば、サブジェクト参

10

20

30

40

50

加者は、少なくとも1つのノードと相互作用するか、あるいは、サブジェクト参加者がサブジェクト参加者およびサートファイヤ参加者として同時に部分的または完全に具体化されている、特に実施形態では、ノードを含む。

【0018】

分散レジストリネットワーク内のノードは、レジストリデータを処理する機能を有するサーバまたは端末装置であってもよい。たとえば、ブロックチェーンネットワーク内の各ノードは、トランザクションデータの検証者、現在のブロックへのトランザクションデータの追加、ブロックのコミット、新しいブロックの既存ブロックへのリンクなどの機能を実行する。

【0019】

例えば、サブジェクト参加者としての製造者は、ベリファイヤ参加者として製造された製品の顧客にブルーフを提供する。ESGデータに関する信頼できる情報を取得するために、顧客はブルーフを検証する。したがって、顧客は、好ましくは、サートファイヤ参加者に関する情報をブルーフから抽出する。彼は、このブルーフは、特定のサートファイヤ参加者によって発行されたESGクレデンシャルに基づいており、このサートファイヤ参加者の公開鍵を分散レジストリで要求することを導き出した。公開鍵によりブルーフが検証できるため、メーカーが提供する製品のESGデータに関する信用に値する声明を顧客が入手できる。これは、ESGデータの完全性もしくはESGデータの一部もしくはESGデータの属性について、認定書発行者、すなわち、サートファイヤ参加者の真正性についての信用に値する声明を含む。そのため、お客様は製造者の製品のESGデータに関する信頼できる情報を受け取る。

【0020】

したがって、サブジェクト参加者の間接的な環境または社会的影響に関する情報は、有利にはあいまいな仮定に基づくものではなく、エコシステムの信頼された当事者によって認証され、ベリファイヤ参加者が信頼できる方法で検証可能である。

【0021】

提案システムでは、好ましくは、擬似名または公開アドレスは、エコシステムの複数の参加者の相互作用のために使用される。

【0022】

分散レジストリは、好ましくは、サブジェクト参加者の擬似名または公開アドレスを、サブジェクト参加者の対応する公開鍵とマッピングするだけである。例えば、サートファイヤ参加者は、自身の公開鍵を、その本物の身元へのマッピングと共に、サートファイヤとして登録するか、あるいは、仮名を使う。実施形態では、サブジェクト参加者がサートファイヤ参加者としても機能し、それ自体がESGクレデンシャルを作成する場合、分散レジスタ内の公開鍵は、好ましくは、仮名にマッピングされる。

【0023】

例えば、ESGクレデンシャルは、サブジェクト参加者の少なくともESGデータに関する認証され検証可能な情報を含む。これは、特に、サブジェクト参加者によって提供されたすべてのESGデータ、またはESGデータの一部もしくはESGデータの属性のいずれかを認定する。さらなるサブジェクト参加者を伴う実施形態では、ESGクレデンシャルは、さらに、さらなるサブジェクト参加者のESGデータに関する認証され検証可能な情報を含む。ここでも、特に、サブジェクト参加者によって提供されたすべてのESGデータ、またはESGデータの一部もしくはESGデータの属性が認定される。ESGサートファイヤ情報の所有者としてのサブジェクト参加者は、ベリファイヤに送信するブルーフに含める内容を決定する。

【0024】

実施形態におけるESGクレデンシャルは、さらに、ブルーフを提供するサブジェクト参加者によって署名される。それゆえ、そのサートファイヤの公開鍵に加えて、サブジェクト参加者の公開鍵も、ベリファイヤ参加者によって要求され、例えば、分散レジストリにおいて検索されるか、あるいは、他の通信チャネルを通じて提供される。

【0025】

好ましくは、サブジェクト参加者は、公開アドレスまたは仮名のみを使用し、さらに、署名メカニズム内のその特定のベリファイヤ参加者との通信のために仮名のみを使用して、将来の検証プロセスのための機密性を可能にする。例えば、サプライチェーンのさらなる参加者、例えば、さらなる階層の別の顧客または別の購入者が将来、プルーフを検証する場合、プルーフおよび使用される署名メカニズムから、サブジェクト参加者の身元について抽出可能な情報はなく、すべてのプルーフのための仮名の更新のために、さらにサブジェクト／ベリファイヤまたはサブジェクト／サーティファイヤの関係についての追跡抽出可能な情報はない。

【0026】

提案システムは、ESG情報のためのアカウントティングアプローチを可能にし、サプライチェーンの利害関係者としてのすべての参加者が、少なくとも自身のESG関連データを評価し、リンク不能な仮名が使用される場合には匿名の方法で、上記のすべてのアカウントティング標準に適用可能であるが、排他的ではない場合には、信頼できる認証可能な方法でこの情報を共有する。

【0027】

認証されたESG情報は、株主、規制、またはNGOの報告、監査、税申告、調達シミュレーション、またはサプライチェーン・エンジニアリングのために使用され、より高い復元力を得るか、製品またはサービスの総コストまたはサービス・コストを削減することができる。

【0028】

一実施形態によれば、少なくとも1つのサーティファイヤ参加者は、追加的に、さらなるサブジェクト参加者のさらなるベリファイヤ参加者として具体化される。製品のサプライチェーン内では、例えば、製造者、異なる階層のサプライヤ、ユーティリティ・プロバイダなどの複数のサブジェクト参加者が、それぞれのESGデータのプルーフ、例えば、製品コンポーネントのPCFへの貢献を、次の階層、エンド顧客、規制インスタンス、または非政府組織（NGO）に提供することを望んでいる。

【0029】

有利な方法では、ESGクレデンシャルから派生したプルーフを提供したいサブジェクト参加者は、最初に、自身のESGインパクトに関連するESG情報、例えば、自身のPCFインパクト、又は製造工程で 사용되는材料に関するデータ、又は自身の製造施設又は場所又は現在の雇用条件等を提供する。さらに、サプライチェーンの他のサブジェクト参加者からのESGデータに関する情報は、プルーフに含めることが望ましい。

【0030】

有利なことに、例えばライフサイクルアセスメントデータベースや一般化されたデータベースからのPCF値、いわゆる二次データを介して、それ以上のサブジェクト参加者のESGデータについての推定は必要ない。代わりに、さらなるサブジェクト参加者、特にサプライチェーンまたはライフ・サイクルのすべてのサブジェクト参加者からのESG情報（製品の使用フェーズおよび寿命の終わりを含む可能性がある）は、サーティファイヤ参加者によって提供されるESGクレデンシャルについて考慮される。

【0031】

したがって、サーティファイヤ参加者は、ESGクレデンシャルを要求する実際のサブジェクト参加者からのESGデータの内容を持つESGクレデンシャルを発行するだけでなく、実際のサブジェクト参加者によって提供される製品またはサービスの全体的なESG情報に関連するESGデータをさらに含んでいる。これは、供給元となる製品、材料、製品、サービスの一部またはコンポーネントが存在する場合で、実際のサブジェクト参加者によって生産または提供されず、他のエコシステム参加者から供給されたものである。

【0032】

サーティファイヤは、さらなるベリファイヤであると同時に、さらなるサブジェクト参加者によって提供されるさらなるプルーフを要求するか又は受信する。さらに、サブジェ

10

20

30

40

50

クト参加者自身が、同じサーティファイヤまたはさらに別のサーティファイヤによって E S G クレデンシャルを受信される。

【 0 0 3 3 】

関連する E S G 情報または関連するサブジェクトとそれらの E S G データを導出するために、実際のサブジェクト参加者は、例えば、E S G クレデンシャルを要求すると共に、部品表 (B O M) または処理表 (B O P) に関するデータをサーティファイヤ参加者に送信する。このデータに基づいて、例えば、サーティファイヤ参加者は、B O M または B O P データに従って、関与するさらなるサブジェクト参加者からのさらなる E S G クレデンシャルから派生したさらなるプルーフを要求する。あるいは、サーティファイヤ参加者は、例えば、さらなるサブジェクト参加者のためのサーティファイヤ参加者であるように、すでに、さらなるサブジェクト参加者のそれらのさらなる E S G クレデンシャルを所有している。

10

【 0 0 3 4 】

さらなる E S G クレデンシャル、またはさらなるサブジェクト参加者のさらなる E S G クレデンシャルから導出されるさらなるプルーフを、実際のサブジェクト参加者の E S G クレデンシャルと組み合わせることにより、再帰的 E S G クレデンシャルが生成される。再帰的 E S G クレデンシャルには、たとえば、ローカル E S G 情報のセクションと外部 E S G 情報のセクションがある。外部セクションのエントリには、例えば、さらなるプルーフの入力を計算または加重または正規化する方法や、さらなるプルーフへのポイントを含める方法などの情報が含まれる。外部プルーフへのポイントは、例えば、仮名、例えば、公開アドレスまたは公開識別子、そして好ましくは、追加のインターネットサービスエンドポイント、例えば、U R L または I P アドレスの組合せによって実装される。

20

【 0 0 3 5 】

サーティファイヤ参加者によって発行された再帰的 E S G クレデンシャルに基づいて、サブジェクト参加者は再帰的 E S G クレデンシャルから再帰的プルーフを導出する。ベリファイヤが再帰的プルーフを検証するとき、再び、そのサーティファイヤ参加者の公開鍵が使われる。

【 0 0 3 6 】

再帰的 E S G クレデンシャルがエコシステムの信頼された団体によって発行されているので、ベリファイヤは、サーティファイヤへのリンクを構成する E S G クレデンシャルから派生したプルーフに頼ることができる。さらに、ベリファイヤ参加者は、実際のサブジェクト参加者によって生成されたプルーフの真正性と完全性だけでなく、サプライチェーンのさらなるサブジェクト参加者によって生成されたさらなるプルーフも検証するオプションを持っている。したがって、ベリファイヤ参加者は、再帰的プルーフにおける情報を使用することができ、プルーフに含まれる E S G クレデンシャルの外部セクションをより特定し、さらなるサブジェクト参加者、例えば、製造者にコンポーネントを配送するサプライヤからのさらなる E S G クレデンシャルから派生したさらなるプルーフを直接要求するために提供される仮名およびサービスエンドポイントを使用することができる。ベリファイヤは、追加のサブジェクト参加者に対して追加の E S G クレデンシャルを発行したサーティファイヤ参加者の公開鍵を使用して再度実行される。さらなるサーティファイヤがさらなるプルーフを発行した場合、さらなるサーティファイヤの公開鍵は、レジストリからも導き出すことができる。

30

40

【 0 0 3 7 】

あるいは、ベリファイヤは、実際のサブジェクト参加者のために再帰的 E S G クレデンシャルを発行したサーティファイヤ参加者に依存することができ、このプロセスにおいて、さらなるサブジェクト参加者によって提供されるさらなるプルーフの真正性と完全性をベリファイヤした。次に、例えば、外部セクションに関して、サーティファイヤ参加者によって発行された再帰的クレデンシャルの中に含まれる情報は、ベリファイヤ参加者によって、提供された E S G データまたは E S G データの一部を、プルーフのチェーン全体をトレースすることなく、処理または解釈するために使用することができる。

50

【0038】

例えば、再帰的 E S G 情報には、P C F、C O₂、C O₂ e 関連の値が含まれる。この場合、ローカル情報には、使用されている C O₂ 排出基準、データ入力方法（手動、自動）、日付または計算、地理位置情報、または企業担当者などのメタデータ情報がある。

【0039】

関連実施形態では、ローカル情報は、G H G プロトコルに従って K g C O₂ e で測定された実際のスコープ 1 とスコープ 2 の値を含む。スコープ 1 には、製造者が所有または管理する排出源からの直接 G H G 排出量、例えば、実際のサブジェクト参加者が含まれる。スコープ 2 は、サブジェクト参加者が購入した電力の発電からの G H G 排出量を算定する。この情報は、実際のサブジェクト参加者によっても提供される。

10

【0040】

最後に、スコープ 3 には、その他の間接的な G H G 排出量も含まれる。スコープ 1、スコープ 2、およびアップストリームスコープ 3 の合計は、製品の生産フェーズのプロダクトカーボンフットプリントまたは P C F と呼ばれる。たとえば、外部情報とは、サプライチェーンからのリサイクル、使用材料、製造前、ロジスティックなどの影響を考慮した、P C F 全体の価値に対するスコープ 3 の貢献を指す。再帰的 E S G クレデンシャルの外部セクションは、P C F 値または C O₂ e 値に関する情報を提供する他のプルーフへのポイントと、部品表で定義されたユニット数など、それらの他のプルーフに基づいて全 P C F を計算する方法の情報で構成される。他の実施形態は、P A S 2 0 5 0 および I S O 1 4 0 6 7 のようなさらなる P C F 規格に関連するデータを含む。

20

【0041】

さらなる E S G クレデンシャルへのポイント、またはさらなる E S G クレデンシャルから導かれるさらなるプルーフへのポイントは、好ましくは、リンク不能な仮名のみを参照する。これは特に、通信ネットワーク内の任意のメッセージに対して新規または新規の仮名を使用することによって実現される。好ましくは、真のアイデンティティの推論は不可能である。たとえば、メーカーの再帰的 E S G クレデンシャルの外部セクションは、サプライヤに対して発行された追加の E S G クレデンシャルを参照する。E S G クレデンシャルに対するサプライヤの貢献が信頼できる限り、再帰的 E S G クレデンシャルから導出されたプルーフのベリファイヤがサプライヤの実際の身元について学習する必要はない。したがって、さらなるサブジェクト参加者によって提供されるさらなる E S G クレデンシャルから導出されるさらなるプルーフも、サーティファイヤ参加者の公開鍵を介して検証可能であり、これは、再帰的クレデンシャルを発行したものと同一サーティファイヤ参加者である可能性があるか、あるいは、さらなるサーティファイヤ参加者である可能性がある。

30

【0042】

プルーフを生成するために、実施形態における再帰的 E S G クレデンシャルは、プルーフを提供するサブジェクト参加者によって署名される。実施形態において、E S G クレデンシャルは、そのプルーフから抽出可能であり、そのサーティファイヤの真正性と、その E S G クレデンシャルの完全性は、そのサーティファイヤの公開鍵によって認証可能であり、加えて、そのプルーフを提供するサブジェクト参加者の真正性は、検証可能である。

40

【0043】

有利な方法では、E S G クレデンシャルと再帰的 E S G クレデンシャルから導かれたプルーフの連鎖をもつ提案システムにおいて、交換された排出量は意図せずに「二重計上」されず、これは排出量インベントリを報告するときに、供給元の供給者によって、そして再び受け取った購入者または実際のサブジェクト参加者によって数えられることを意味する。したがって、同じ排出量に対するサプライチェーンの関係者による税金の二重支払いは防止される。さらに、サプライヤから受信者への排出量の誤った移送により、自らの約束された労力を満たすために自らの排出量を削減し、その後、受信者が再び約束された労力を満たすために同じ削減量を要求することも防止される。その場合、および従来の方法では、実際には 1 回の削減しか発生していないが、2 回主張することができた。

50

【0044】

確立された基準に従って、任意の種類のコ₂オフセットをPCFとは別に報告する。たとえ別々に説明したとしても、提案されているエコシステムを用いたコ₂オフセット・アプリケーションの場合、全く同じオフセットの二重販売は、有利に妨げられる。

【0045】

実施形態によれば、少なくとも1つのサブジェクト参加者は、少なくとも1つのサートィファイヤ参加者またはさらなるサートィファイヤ参加者として具体化される。これは、有利には、例えば、信頼された実行環境、セキュアメモリ等のルートオブトラスト技術が、サブジェクト参加者側にインストールされる場合である。このような技術により、例えば、処理ステップ、材料消費、製品識別、機械識別又は排出に関して、耐タンパー性又は耐タンパブルーフの証拠が提供される。さらに、サブジェクト参加者は、例えば、そのサブジェクト参加者がエコシステムの信頼されたインスタンスによって定期的に認証されている場合、サートィファイヤとして具体化することができる。例えば、製造者、製造者のサイト又は製造者のプロセスの認証は、暗号的に検証可能であるため、製造者の署名は信用に値する。

10

【0046】

これらの実施形態において、および再帰的ESGクレデンシャルが使用される場合、サートィファイヤ参加者としてのサブジェクト参加者も、さらなるサブジェクト参加者のさらなるベリファイヤ参加者である。次に、サブジェクト参加者は、さらなる参加者、例えば、その供給者から受け取ったブルーフを検証し、それから、自身のESG情報と外部ESG情報のための再帰的ESGクレデンシャルを発行する。

20

【0047】

一実施形態によれば、少なくとも1つのサートィファイヤ参加者は、ノードを介して分散レジストリへの読み出しおよび書き込みアクセスを有するように構成され、少なくとも1つのベリファイヤ参加者は、ノードを介して少なくとも読み出しアクセスを有するように構成される。

【0048】

公開アドレスや仮名を、サブジェクト参加者となる可能性のあるサートィファイヤ参加者が同時に登録する場合は、分散レジストリにデータを書き込む必要がある。たとえば、公開アドレス／仮名と対応する公開鍵に関する情報を持つトランザクションは、分散データベースに送信される。たとえば、トランザクションはブロックチェーンデータベースに送信され、合意されたコンセンサスメカニズムでネットワークコミュニティによって検証される。公開鍵のレジストレーションを成功させるためには、参加者は適切な鍵で自分自身を識別しなければならない。ブロックチェーン上のアドレスが作成されると、公開鍵が表示される。アドレス自体が参加者の「仮名」である。

30

【0049】

ベリファイヤ参加者の場合、関心のある公開鍵を受信するには読み取りアクセスのみが必要である。それにもかかわらず、ベリファイヤ参加者が将来のサートィファイヤ参加者としても行動する場合、書き込みアクセスは有利である可能性がある。

【0050】

さらに、本発明は、製品関連エンティティのESGデータに関する情報を交換する通信ネットワークの、少なくとも1つのサブジェクト参加者によって、ESGクレデンシャルから導出された少なくとも1つの暗号ブルーフを提供するためのコンピュータ実装方法であって、

40

ネットワークが、複数のサブジェクト参加者、少なくとも1つのベリファイヤ参加者及び少なくとも1つのサートィファイヤ参加者を含み、

方法が、少なくとも1つのサブジェクト参加者によって、ブルーフを生成することを含み、

ブルーフが、ESGクレデンシャルを提供する少なくとも1つのサートィファイヤ参加者の真正性を割り当て、ESGクレデンシャルが、少なくとも1つのサートィファイヤ

50

参加者から、少なくとも1つのサブジェクト参加者によって受信され、

少なくとも1つのサーティファイヤ参加者の公開鍵は、分散レジストリを介して、ブルーフから少なくとも1つのベリファイヤ参加者によって導出され、真正性を検証するために少なくとも1つのベリファイヤ参加者によって使用され、

ブルーフが、ESGデータの完全性、またはESGデータの一部、またはESGデータの属性を、さらに割り当て、

少なくとも1つのサーティファイヤ参加者の公開鍵が、ベリファイヤ参加者によって、完全性を検証するために使用される。

【0051】

提案された方法は、好ましくは、上述のようにエコシステムで実行される。いくつかのサブジェクト参加者と、少なくとも1つのサーティファイヤ参加者と、少なくとも1つのベリファイヤ参加者を含むシステムは、好ましくは、上記または以下に記載する実施形態の1つ以上に従って方法を実行するように実施される。有利な方法では、この方法は、サブジェクト参加者とシステムのベリファイヤ参加者との間で製品関連エンティティに関するESG情報を交換することを可能にする。サーティファイヤ参加者からのESGクレデンシャルの使用により、中央の信頼された認証局や認証局を必要とせずに、ESG関連データに関する信頼できる認定書が有効になる。

【0052】

少なくとも1つのサブジェクト参加者によって生成されたブルーフは、例えば、少なくとも1つのベリファイヤ参加者に送られる。生成されたブルーフの送信は、たとえば、ベリファイヤ構成要素からサブジェクト構成要素に送信された招待メッセージによってトリガされる。代替実施形態では、サブジェクト参加者は、製品提供によってトリガされたブルーフを提供する。

【0053】

実施形態によれば、ESGクレデンシャルは、少なくとも1つのサーティファイヤ参加者によって生成される。ESGクレデンシャルは、たとえば、ESGクレデンシャルを要求するサブジェクト参加者が特定の製品またはサービスに寄与するESGデータで構成される。ESGクレデンシャルは、ESGデータの完全性とサーティファイヤの真正性を割り当てる。例えば、ESGクレデンシャルは、フォームのサブジェクト参加者によってベリファイヤ参加者にブルーフとして転送され、それがサーティファイヤ参加者から受信された範囲まで転送される。

【0054】

一実施形態によれば、ESGクレデンシャルを生成するために、少なくとも1人のサーティファイヤ参加者は、製品関連エンティティのESGデータに関連するさらなるサブジェクト参加者の少なくとも1つのさらなるブルーフを検証し、再帰的ESGクレデンシャルを生成する。ESGクレデンシャルの発行プロセスにさらなるブルーフを含めることで、サーティファイヤ参加者は信頼の連鎖を構築する。ESGクレデンシャルを要求しているサブジェクト参加者のESGデータに加えて、さらに別のサブジェクト参加者、特に同じ階層または異なる階層のすべてのサブジェクト参加者のESGデータに関する情報も、サーティファイヤによって発行されたESGクレデンシャルに含まれる。したがって、サブジェクト参加者のESGデータに関する情報と、さらなるサブジェクト参加者のESGデータに関する情報は、サーティファイヤ参加者によって検証される。サブジェクト参加者によって生成されたブルーフは、再帰的ESGクレデンシャルから導出される。例えば、再帰的ESGクレデンシャルは、フォーム中のサブジェクト参加者によってベリファイヤ参加者にブルーフとして転送され、それがサーティファイヤ参加者から受信された範囲まで転送される。サーティファイヤ参加者の公開鍵を用いて、ベリファイヤ参加者は再びサーティファイヤの真正性とESGデータの完全性を検証できる。この場合のESGデータは、サブジェクト参加者のESGデータと、さらなるサブジェクト参加者のさらなるESGデータから成る。

【0055】

実施形態によれば、再帰的 E S G クレデンシャルは、サブジェクト参加者の E S G データのためのローカル E S G セクションと、さらなるサブジェクト参加者の E S G データのための外部 E S G セクションとを含む。したがって、ベリファイヤにとっては透過的であり、ベリファイヤは、製品やサービスに関する全体的な E S G 情報にどの程度貢献したかがわかる。再帰的クレデンシャルを発行するときに暗号メカニズムを適用するために、E S G データに関する明快な情報も信頼できる。

【0056】

一実施形態によれば、少なくとも1つのサブジェクト参加者は、要求メッセージを送信することによって、少なくとも1つのサートィファイヤ参加者から E S G クレデンシャルを要求する。要求メッセージは、例えば、サートィファイヤ参加者からプルーフを提供するための招待メッセージが受信されるとすぐに、サートィファイヤに送信される。要求メッセージは、好ましくは、認証されるべき E S G データを含む。また、好ましくは、他のエコシステム参加者によるソース製品、コンポーネントまたはサービスのために、サブジェクトの製品またはサービスの全体的な E S G 情報に寄与するデータが、要求メッセージに含まれる。それにより、サートィファイヤ参加者は、さらなるサブジェクト参加者のさらなる E S G 情報についてのさらなるプルーフを検証することができ、そして、正常にベリファイヤされた場合、さらなるプルーフを E S G クレデンシャルに含めることができる。

10

【0057】

一実施形態によれば、少なくとも1つのサートィファイヤ参加者は、公開アドレスと、対応する公開鍵とを、分散レジストリに登録する。例えば、少なくとも1つのサートィファイヤ参加者は、将来のベリファイヤ参加者がプルーフを検証することを可能にするために、自身の公開鍵に登録する。例えば、E S G クレデンシャルは、その秘密鍵でサートィファイヤによって署名され、サブジェクト参加者は、ベリファイヤ参加者のプルーフとして、サブジェクトの署名によって自身の秘密鍵で補完された、署名された E S G クレデンシャルを提供する。

20

【0058】

実施形態によれば、少なくとも1人のサートィファイヤ参加者は、サブジェクト参加者のためのクレデンシャル定義を定義し、そのクレデンシャル定義を分散レジストリに登録する。サートィファイヤ情報定義は、認証される E S G データに関するメタデータを記述する。つまり、将来発行されるクレデンシャルのスキーマを定義する。クレデンシャル定義は、例えば、サブジェクト参加者によるクレデンシャルの要求に基づいて、サートィファイヤ参加者によって作成される。ここで、サブジェクト参加者は、認証されるべきデータまたは属性を定義する。これは、どのような種類のデータがコード化されるか、どの署名メカニズムが適用されるかななどを定義する。

30

【0059】

一実施形態によれば、完全性を割り当てるための第1の暗号署名メカニズムは、少なくとも1人のサートィファイヤ参加者の秘密鍵で生成された第1の暗号署名に基づいており、第1の暗号検証メカニズムは、少なくとも1つのサートィファイヤ参加者の公開鍵で第1の暗号署名を検証することに基づいている。第1の暗号署名メカニズムは、例えば、サートィファイヤによって選ばれる。これにより、サートィファイヤ参加者をネットワークに統合する柔軟性が得られる。署名メカニズムは、計算能力または利用可能な暗号プリミティブに従って選択することができる。例えば、最初の暗号署名メカニズムは、エコシステム内のすべてのサートィファイヤ参加者について固定されている。その後、サートィファイヤ参加者は、暗号メカニズムを適用するための所定の基準を満たす必要がある。

40

【0060】

サートィファイヤ参加者の署名は、その秘密鍵を使用して、例えば、署名されたデータ (E S G データ) が操作されたかどうか、および、主張された送信者が正しい送信者、すなわち、信頼されたサートィファイヤであるかどうかの検証を可能にする。

【0061】

50

一実施形態によれば、完全性を割り当てるための第1の暗号署名メカニズムは、サーティファイヤ参加者の信頼されたグループに共通の秘密鍵で生成された暗号グループ署名、または信頼されたサーティファイヤ参加者のグループの2人以上のサーティファイヤ参加者によって生成された暗号しきい値署名に基づいており、第1の暗号検証メカニズムは、サーティファイヤ参加者の信頼されたグループの公開鍵で第1の暗号署名を検証することに基づいている。グループ署名を使用する場合、実際の認証は匿名に保つことができ、ESGクレデンシャルは引き続き信頼できる。これは、例えば、ESGクレデンシャルの発信元がサプライチェーンの参加者の国に関する情報を明らかにし、それらのIDを再び明らかにする可能性があるシナリオで利点となる可能性がある。しきい値署名メカニズムを使うとき、完全性は、単一のサーティファイヤ参加者が、例えば、相互作用するしきい値署名の性質上、ハッキングされたり、他の方法で操作されたりするシナリオについても、補償される。これは、気づかれないままではない。

10

【0062】

グループ署名または参加者の信頼されたグループを使用する場合、公開鍵はレジストリによって引き続き簡単に提供できる。そのため、ペリファイヤは公開鍵を読み取り、プールの完全性またはESGクレデンシャル自体の完全性を検証できる。

【0063】

一実施形態によれば、第1の暗号署名メカニズムは、ゼロ知識プルーフに基づいている。ゼロ知識プルーフメカニズムの使用は、サーティファイヤが、ESGデータを必ずしもそのように、あるいは、完全に、あるいは、詳細に提供することなく、ESGクレデンシャルを発行することを可能にする。例えば、「閾値より低い値」や「特定の国で製造されていない」など、ESGデータの属性のみが提供される。しかし、これらの属性は、検証可能に提供されるので、その属性の完全性と、そのサーティファイヤの真正性は、保証される。

20

【0064】

ゼロ知識プルーフを生成するために、サーティファの秘密鍵がゼロプルーフ署名メカニズムで使用され、検証のために、対応する公開鍵が使用される。ESGクレデンシャルがプルーフとしてサブジェクト参加者によって転送されるユースケースの場合、ESGクレデンシャルを生成するためのゼロ知識署名メカニズムの使用は、適用される標準の基準を満たすためにペリファイヤに開示される必要がないPCF値に関する詳細など、ESGデータに関する特定の詳細情報を保持することを可能にする。

30

【0065】

ゼロ知識プルーフメカニズムを使用して、ESG情報に関する特定の提示された属性または条件ステートメント（たとえば、より大きい値、より小さい値、包含、除外など）を実証する場合、真正性は、たとえば、サブジェクト参加者の秘密の使用によって証明される。サブジェクトが発行者にESGクレデンシャルを要求すると、その要求にシークレットも含まれる。サーティファイヤはまた、その秘密にサインする。この署名付きシークレットは、サブジェクトがサーティファイヤから取得するサーティファイヤ情報の一部である。サブジェクトによってサーティファイヤ情報からプルーフを作成する場合、この署名付きシークレットも含まれる。ペリファイヤは、レジストリ上にある公開鍵を使用してこの秘密を検証し、プルーフが送信者、すなわちサブジェクト参加者から来たという確認を受け取ることができる。プルーフは、クレデンシャル定義IDを作成した人によって発行されたESGクレデンシャルに基づいている。クレデンシャル定義IDは、サーティファがサブジェクトのクレデンシャル定義を分散レジストリに登録するときに作成される。

40

【0066】

一実施形態によれば、少なくとも1つのサブジェクト参加者は、追加的に、少なくとも1つのサーティファイヤ参加者またはさらなるサーティファイヤ者参加者として具体化され、クレデンシャルは、ルートオプトラスト技術を使用して、少なくとも1つのサブジェクト参加者によって生成される。サブジェクト参加者は、例えば、認証された参加者であり、サーティファ参加者又はエコシステムの他の信用に値するインスタンスによって定期

50

的に制御される。

【0067】

一実施形態によれば、少なくとも1つのサブジェクト参加者は、ネットワーク内の複数の通信メッセージに対して複数の仮名を使用する。特に、製品に貢献する複数のサブジェクトを持つ製品のサプライチェーンなど、それぞれのESG情報を実証するサブジェクトのチェーンを持つシナリオでは、サブジェクト参加者が仮名で行動する場合、通信ネットワーク内でプライバシーと機密性が保証される。サプライヤなどのサブジェクト参加者は、サプライチェーンの次の階層（製造者）と直接通信し、要求されたプルーフを提供する。顧客などの次の階層は、製造者の身元を知っている。顧客はサプライヤの身元を知らず、サプライチェーン全体の身元をオープンにすることを意図していない。

10

【0068】

材料、部品、コンポーネント、またはサービスを提供するエコシステム参加者の本当の身元は、公開鍵の形式で、参加者がリンク不能な仮名で表され、2人の参加者間のコミュニケーションのコンテキストでのみ使用され、しかも、好ましくは1回のみであるため、公開されていない。仮名を使用する場合、例えば、ベリファイヤとサティファイヤにプルーフを提供する場合や、サティファイヤにESGクレデンシャルを要求する場合や、クレデンシャル定義IDを生成する場合、実身元は有利には秘密に保たれる。それでもなお、再帰的ESGクレデンシャルのプルーフの検証、特に秘密／公開鍵ペアが信頼できる方法で分散レジストリに登録されることの検証を含む、プルーフの完全性の検証が可能である。

20

【0069】

参加者の仮名化を拡張することができ、分散レジストリは、少数の特定されたエコシステム参加者、例えば監視官、審査州の関係者などが、定義されたエコシステムガバナンス規制に従って、仮名を参加者およびアーティファクトの実際の身元にマッピングすることを可能にする。

【0070】

一実施形態によれば、少なくとも1つのサブジェクト参加者は、第2の暗号署名メカニズムと、少なくとも1つのサブジェクト参加者の秘密鍵とを使用することによって、ESGクレデンシャルからプルーフを導出する。サブジェクト参加者は、プルーフの完全性と真正性を割り当てるために、サブジェクト自身の署名で補足されたESGクレデンシャルを提供することができる。他の実施形態では、サブジェクトとベリファイヤとの間のセキュアな通信が使用され、これは第2の暗号署名メカニズムを分配する。

30

【0071】

一実施形態によれば、第2の暗号署名メカニズムは、ゼロ知識プルーフに基づいている。ゼロ知識プルーフメカニズムはまた、有利には、サブジェクト参加者によって使用され得る。サティファイヤ参加者が詳細なESGデータを開示するESGクレデンシャルを提供するユースケースでは、サブジェクト参加者はベリファイヤ参加者に提供する情報量を決定できる。例えば、特定の標準要件が満たされているという証拠を提供するために必要な情報のみを提供することができる。ゼロ知識プルーフは、暗号鍵ペア、すなわち、サブジェクトの公開鍵と対応する秘密鍵に基づいている。サブジェクト参加者によるゼロ知識署名メカニズムの使用は、サブジェクト参加者によって提供されたESGデータの完全性とサブジェクト参加者の真正性を割り当てる。さらに、ゼロ知識プルーフに開示されたデータに依存して、サティファの真正性とESGデータが提供されるESGクレデンシャルの完全性はゼロ知識プルーフによって決定される。

40

【0072】

提案した方法とシステムにより、エコシステム内の参加者全体にわたる企業、生産サイト、製品またはサービスに関するESGデータまたはESGデータの属性の透明性が改善される一方で、参加者の身元の機密性とプライバシーが保持される。

【0073】

本発明のさらなる可能な実施形態または代替ソリューションは、実施形態に関して上

50

たは下に記載された特徴の組合せ—ここで明示的に言及されていない—も含む。また、当業者は、本発明の最も基本的な形態に、個々のまたは分離された態様および特徴を追加することができる。

【0074】

本発明の以下の異なる態様において、添付の図面を参照してより詳細に説明する。

【図面の簡単な説明】

【0075】

【図1】本発明の第1の実施形態による製品関連エンティティのESGデータに関する情報を交換するシステムの概略図である。

【図2】本発明の第2の実施形態による製品のサプライチェーンにおけるシステムの参加者の概略図である。

【図3】本発明の第3の実施形態による再帰的ESGクレデンシャルの概略図である。

【図4】本発明の第4の実施形態による製品関連エンティティのESGデータに関する情報を交換するエコシステムの概略図である。

【発明を実施するための形態】

【0076】

図1は、製品の顧客Cがベリファイヤ参加者として機能する、第1の実施形態による提案されたシステムの概略図を示す。顧客Cは、システムのサブジェクト参加者として機能する製造者Mに、製品に関するESG情報を要求する'16。ESG情報は、具体的な製品が環境、社会、および企業のガバナンスに与える影響の全体的なスコアに対する製品の影

10

20

【0077】

製品のESG情報が要求された検証可能なプルーフを提供できるように、製造者Mは、サーティファイヤT0からサーティファイヤ参加者としてESGクレデンシャルを要求する'10。信頼されたサーティファイヤT0は、IDと公開鍵を持つ識別子を分散レジストリRに登録する'14。ブロックチェーンベースのレジストリは、例えば、サーティファイヤの公開鍵を分散保存し、後の暗号検証ステップのために顧客Cのようなベリファイヤにそれらを提供するために使用される。T0は、さらに、分散レジストリR内の製造者Mの製品のクレデンシャルを定義する。

【0078】

要求されたESGクレデンシャルを提供するために、信頼されたサーティファイヤT0は、製造者MのESGデータの完全性を割り当てるだけでなく、製品のサプライチェーンに關与する他の参加者からも割り当てなければならない。第1の実施形態では、一例として、2つの複数の階層の2つのサプライヤS1、S2は、材料またはコンポーネントを配送する際に、製品の全体的なESGスコアに対して考慮されるべきである。したがって、信頼されたサーティファイヤT0は、製品のコンポーネントに関する情報をS1に要求する'11。S1は、さらなる信頼されたサーティファイヤT1によって発行されたさらなるESGクレデンシャルから、選択された製品のコンポーネント情報を返信する'12。それは、さらなるプルーフの中で具体化された選択された情報を提供する。

30

【0079】

信頼されたサーティファイヤT0は、第1階層サプライヤS1から受け取ったさらなるプルーフに関して、エコシステムのベリファイヤ参加者として機能する。特にクレデンシャル定義IDのように、さらなるプルーフにおけるデータに基づいて、信頼されたサーティファイヤT0は、そのクレデンシャル定義と、ブロックチェーン中のさらなる信頼されたサーティファイヤT1の公開鍵を検索する'13。信頼されたサーティファイヤT0は、さらにプルーフを検証し、製品の署名付きESGクレデンシャルを製造者Mに発行する'15。この署名付きESGクレデンシャルは、再帰的サーティファイヤ情報であり、製造者のESGインパクトに関するローカルESGデータと、第1階層サプライヤS1の製品コンポーネントによるESGインパクトに関する外部ESGデータが含まれる。

40

【0080】

50

エコシステムと合意され、エコシステム内で使用されている基準によれば、E S G クレデンシャルは、複数のサブジェクトからのE S G データを互いに比較可能にするための細目を含む。重み付け係数は、特に全体的なE S G 値の判定を可能にするために使用される可能性がある。全体的なE S G 値は、たとえば、直接示すことができる。さらに、E S G 全体の値を決定するための方法またはアルゴリズムを、E S G 認定書に含めることができる。特に、以下の段落で説明する再帰的E S G クレデンシャルの場合、重み付け係数または互換性または変換に関する情報は、E S G クレデンシャルの一部であることが推奨される。

【0081】

製造者Mは、信頼されたサートファイヤT0から受け取ったE S G クレデンシャルからブルーフを導き出し、顧客Cに送る'17。顧客はブルーフのベリファイヤとして働き、したがって、クレデンシャル定義とT0の公開鍵を読み取る'18。ブロックチェーンRからの情報を使用して、顧客Cは製造者Mから提供されたブルーフを検証する。

10

【0082】

S1が、さらなる信頼されたサートファイヤT1によって発行されたさらなるE S G クレデンシャルからの選択された製品のコンポーネント情報を返信する'12と、サプライチェーンの参加者のシステムにおいて、次のステップが起こった。第1階層サプライヤS1は、さらなる信頼されたサートファイヤT1から製品のコンポーネントのE S G クレデンシャルを要求する110。さらに信頼されたサートファイヤT1は、そのIDおよび公開鍵と共にブロックチェーンRに登録し114、ブロックチェーンR内の第1階層サプライヤS1の製品のコンポーネントのクレデンシャルを定義する。

20

【0083】

信頼されたサートファイヤT0は、第1階層サプライヤS1のE S G ブルーフのベリファイヤ参加者であるのと同様に、再び、さらなる信頼されたサートファイヤT1は、第2階層サプライヤS2のベリファイヤ参加者である。第1階層サプライヤS1のE S G クレデンシャルを発行するには、さらに信頼されたサートファイヤT1が要求する111ブルーフを検証し、第2階層サプライヤS2によって受信112する必要がある。さらに信頼されたサートファイヤT1は、第2階層サプライヤS2によって提供されたブルーフから派生可能なクレデンシャル定義と、サートファイヤT2に信頼された第2階層サプライヤからの公開鍵とを読み込む113。さらなるサートファイヤT1は、ブルーフを検証する。さらなる信頼されたサートファイヤT1によって再び発行されるさらなるE S G クレデンシャルは、再帰的クレデンシャルであり、有利には、製品のサプライチェーンにおけるサプライヤのE S G 貢献もカバーする。

30

【0084】

再帰構造は柔軟に継続することができ、それは図1のさらなる矢印と参加者で示される。

【0085】

提供されたブルーフを一方で検証する参加者は、ブルーフの基礎となるE S G クレデンシャルの発行者として動作する信頼できるサートファイヤT0が、ブロックチェーンRから導き出された公開鍵に基づいて、ブルーフの完全性と真正性を暗号で検証することができる。さらに、ベリファイヤは、信頼されたサートファイヤT0がサプライチェーンのさらなるサブジェクト参加者のさらなるE S G クレデンシャルから派生したブルーフに関するベリファイヤとしても機能したため、サプライチェーンのさらなる参加者から発信されたブルーフから抽出可能なあらゆるE S G 情報の完全性に依存することができる。

40

【0086】

実施形態の拡張では、顧客Cによって導出されたさらなるE S G クレデンシャルまたはそれから導出されたブルーフのさらなる検証を可能にするために実施されるオプションのループがある。このような拡張では、製造者Mは、顧客Cが選択した製品情報を、さらなる信頼されたサートファイヤT1によって発行されたさらなるE S G クレデンシャル、すなわちさらなるブルーフから直接送るように、第1階層サプライヤS1に要求する11

50

6. 第1階層サプライヤS1は、顧客Cにさらなるプルーフを送り117、顧客は追加的に役割を引き継ぎ、さらなるプルーフを検証する。これらの実施形態では、関与する参加者の機密性を保護するために、適切な手段が実施されなければならない。第1階層サプライヤS1は、オニオンルーティングメカニズムや一時的なDNS名などの対策を使用して、顧客Cに対して匿名のままにしたいと考えている。

【0087】

図2は、本発明の第2の実施形態によるサプライチェーンにおけるESG情報の共有を示す。たとえば、製造者MはESGアカウンティング情報に焦点を当て、製品のESGデータに関するプルーフESGを顧客Cに提供するため、ESG情報を共有するエコシステムのサプライヤと協力する。製造者Mは、第1の第1階層サプライヤ1S1および第2の第1階層サプライヤ2S1と連携しており、より詳しくは、第1の第1階層サプライヤ1S1が、第1の第2階層サプライヤ1S2から、材料およびコンポーネントを入手し、第2の第1階層サプライヤ2S1が、第1の第2階層サプライヤ2S2及び第3の第2階層サプライヤ3S2から、材料およびコンポーネントを入手する。第2階層サプライヤはすべて、それぞれのプルーフ1ESG2、2ESG2、3ESG2を提供する。リバーズツリー構造は、複数の階層と階層ごとの複数の参加者に柔軟に拡張できる。

【0088】

図2に示すように、ESG情報はエコシステム内で共有されるため、顧客Cはライフサイクルを通じて製品が特定の環境要件または社会要件／基準を満たしていることを確認できる。たとえば、その生産に子供や強制労働が含まれていない、製品にコンフリクト・ミネラルとして分類された材料が含まれていない、または製品の総排出量が所定の値を下回っている、などである。このような情報は、顧客以外にも、企業、規制、NGOの報告、監査、税金または税申告、ソーシング・シミュレーション、サプライチェーン・エンジニアリングなどにも使用できる。これにより、復元力が向上し、製品の総費用が削減される。

【0089】

同時に、ESG情報全体に貢献する参加者の関心があり、エコシステム内のESG情報の従来の検証に必要とされるすべての情報をオープンに共有することを強制されるわけではない。サプライヤおよび物流プロバイダの身元、原材料、コンポーネントおよびコンポーネントの国、コンポーネントおよびコンポーネントのシリアル番号およびバッチ番号、または正確なカーボンオフセットスキームなどの情報は、2つの直接的なビジネスパートナー間でのみ秘密に保持する必要がある。たとえば、製品の購入者は、製品の階層1、階層2、階層3、・・・のサプライヤの実際のIDを学習してはならない。

【0090】

図3は、再帰的ESGクレデンシャルrESGの図を示している。それは、ローカルセクションESG1をもつ信頼されたサートファイアのESGクレデンシャルESG0を含み、GHGプロトコルに従ってKgCO₂で測定された実際のスコープ1とスコープ2の値を含む。外部セクションESGeは、PCFまたはCO₂e値を持つ他の再帰的ESGクレデンシャルESG1へのポインタの形式で、すべてのアップストリームスコープ3入力に関する外部情報と、部品表に定義されている単位の数など、これらの他のESGクレデンシャルESG1に基づいて、全PCFを計算する方法の情報で構成される。

【0091】

再帰的ESGクレデンシャルrESGは、サートファイア参加者Tの署名SigTと、サブジェクト参加者としての製造者Mの署名SigMによって補完される。製造者は、エコシステム内のベリファイヤにプルーフとして署名済みの再帰的ESGクレデンシャルを提供する。

【0092】

図4は、サプライ・チェーン・エコシステムの参加者と、製造者M、顧客C、規制当局A、非政府組織NGO、いくつかのサプライヤS1、Sn、サートファイアT、ユーティリティ・プロバイダU、naアダプタYとの相互作用と、別の共有ネットワークXへの

アダプタ Y、およびカーソル・シンク Z の図を示している。

【0093】

製造者 M におけるローカル ESG 情報は、オペレーション技術領域 OT、インターネットモノ領域 IoT、および情報技術領域 IT のようなデータソース 30 から収集される。すべてのドメインにおいて、信頼されたエコシステム参加者、例えば、複数の参加者を認証することに責任のあるサートィファイヤ T による外部検査 100 が実行され、好ましくは、すべてのドメインにおいて、ルートオブトラストメカニズムが埋め込まれる。このようにして、クレデンシャルに含まれ、製造者 M によって共有されるローカル ESG 情報における信頼は、(i) ルートオブトラスト技術を使用したトランザクションの耐タンパー署名または不正開封防止署名、(ii) グループまたはしきい値署名を使用した、信頼された参加者 T による製造者、製造者サイト、製造者処理および／または製造処理トランザクションの署名、および (iii) 製造者自身による製造者処理または製造処理トランザクションの署名に基づいている。後者の場合は、製造者、製造者の施設及び／又は製造者のプロセスの認証が暗号的に検証可能であるとき、合理的である。

10

【0094】

製造者 M のコンピューティングおよびデータ管理システム M' 内に、データプラットフォーム 40 が設置されて、70 のローカル ESG 情報を収集し、例えばサプライヤ S1、Sn、から受け取った ESG クレデンシャルをユーティリティ・プロバイダ U から検証し、例えば、しきい値 GHG 値以下に残っているような独自の ESG データの属性と、例えば、再び異なるしきい値 GHG レベル以下に残っているような外部 ESG データの属性とを含む再帰的 ESG クレデンシャルを生成する。ESG クレデンシャルを生成するために製造者 M から受信されたデータは、例えばセキュアな通信プロトコルを介して直接のビジネスパートナーをリンクするエコシステム内の通信パスを介して受信される。製造者 M は、すべての参加者が少なくとも読み取りアクセス権を持つ分散レジストリから、検証ステップを実行するために必要なデータ、特に公開鍵を取得する。エコシステムは、ビジネスパートナーを結びつける通信システムと、規制インスタンス A、NGO と、少なくとも製造者や OEM などの主要なサブジェクト参加者とを結びつけることによって包含される。エコシステムは、さらに、分散レジストリネットワーク、例えばブロックチェーンネットワークによって包含される。これは、エコシステムで使用されるクレデンシャルの統一された構造と作業可能性を補償するためだけでなく、ネットワーク参加者のアイデンティティと仮名およびそれらに対応する公開鍵を管理するために主に使用される。

20

30

【0095】

例えば、製造者 M の計算及びデータ管理システム M' は、例えば製造者 M の特定の製品の現在の GHG 値を監視するためにダッシュボードサービス 50 のようなアプリケーションにアクセスするためのインターフェース 60 をさらに含む。

【0096】

矢印は、ESG 情報を共有する経路と方向を示し、これは、好ましくは、ESG クレデンシャルから導出されたプールの形態である。

【0097】

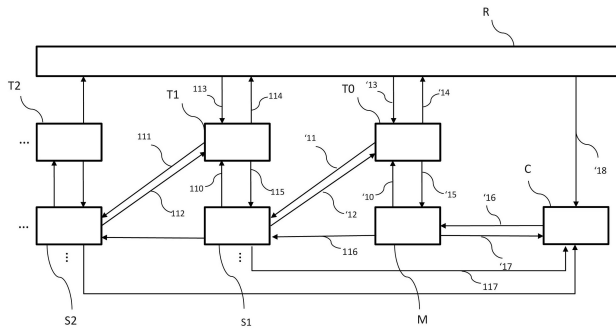
本発明は、好ましい実施形態に従って説明されているが、当業者にとっては、すべての実施形態において修正が可能であることは自明である。

40

【凶面】

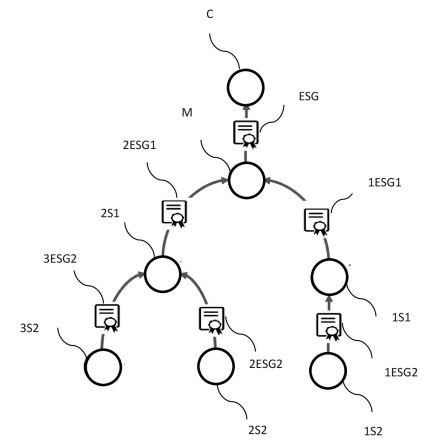
【図 1】

Fig. 1



【図 2】

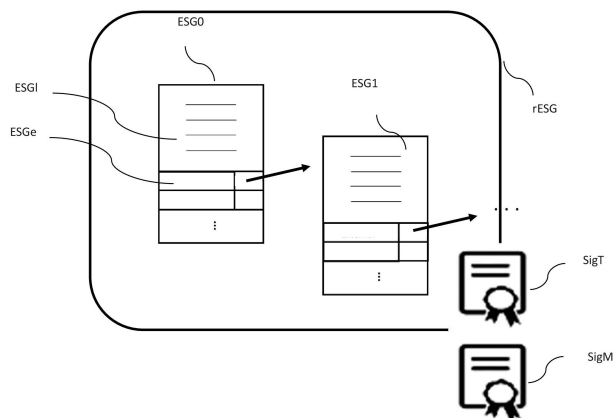
Fig. 2



10

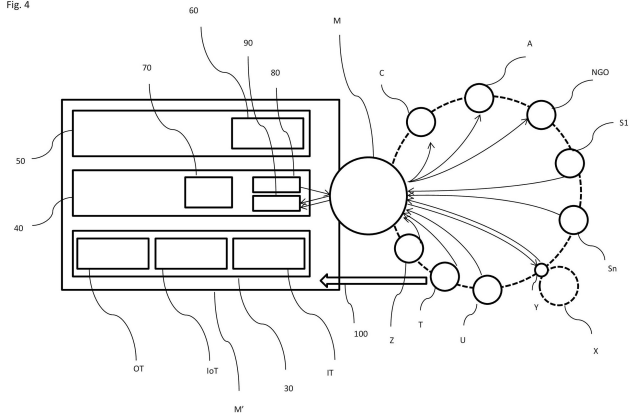
【圖 3】

Fig. 3



【図 4】

Fig. 4



20

30

【外国語明細書】

2022135984000006.pdf

フロントページの続き

- (72)発明者 アンドレアス キント
 スイス連邦 08005 チューリッヒ, フェルリリブックシュトラッセ
- (72)発明者 マクシミリアン ヴァインホルト
 ドイツ連邦共和国 81541 ミュンヘン, ヴェルフエンシュトラッセ14ベ
- (72)発明者 フロリアン ゼバスティアン アルブレヒト
 ドイツ連邦共和国 81679 ミュンヘン, クーフシュタイナーシュトラッセ1
- (72)発明者 マルティン ディーツ
 ドイツ連邦共和国 92224 アンベルク, フリッツーゾイスシュトラッセ11
- (72)発明者 ギュンター バイティンガー
 ドイツ連邦共和国 92224 アンベルク エーグルゼー, ヘッケンヴェーク8
- (72)発明者 トーマス ホルツナー
 ドイツ連邦共和国 13465 ベルリン, バルトシュトラッセ12ベ
- (72)発明者 ヨヌツ アレクサンドル レオンテ
 ルーマニア 022174 ブカレスト, ストラダヘルツァ, ナンバー16, ビルディングエック
 ス4, アパートメント15
- (72)発明者 フロリアン アンスガー イエーガー
 ドイツ連邦共和国 10961 ベルリン, ブリュッヒャーシュトラッセ34
- (72)発明者 ヨナス ホールベック
 ドイツ連邦共和国 81929 ミュンヘン, プロダーセンシュトラッセ11