

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7530175号
(P7530175)

(45)発行日 令和6年8月7日(2024.8.7)

(24)登録日 令和6年7月30日(2024.7.30)

(51)国際特許分類		F I	
G 0 6 F	21/64 (2013.01)	G 0 6 F	21/64
G 0 5 B	23/02 (2006.01)	G 0 5 B	23/02 V
H 0 4 L	43/00 (2022.01)	H 0 4 L	43/00
G 0 6 F	21/12 (2013.01)	G 0 6 F	21/12 3 1 0
H 0 4 L	9/32 (2006.01)	H 0 4 L	9/32 2 0 0 B
請求項の数 20 (全66頁) 最終頁に続く			
(21)出願番号	特願2020-4353(P2020-4353)	(73)特許権者	512132022
(22)出願日	令和2年1月15日(2020.1.15)		フィッシャー・ローズマウント システ
(65)公開番号	特開2020-113281(P2020-113281 A)		ムズ, インコーポレイテッド
(43)公開日	令和2年7月27日(2020.7.27)		アメリカ合衆国 テキサス 7 8 6 8 1 -
審査請求日	令和4年12月19日(2022.12.19)		7 4 3 0 ラウンド ロック ウェスト ル
(31)優先権主張番号	16/248,377		イス ヘナ ブルバード 1 1 0 0 ビルデ
(32)優先日	平成31年1月15日(2019.1.15)		イング 1 エマーソン プロセス マネー
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	100096091
			弁理士 井上 誠一
		(72)発明者	ジェームス・エス・ケイヒル
			アメリカ合衆国 テキサス州 7 8 7 3 4
			オースティン ウィンディ ハーバー ド
			ライブ 3 4 0 0
		審査官	岸野 徹
			最終頁に続く

(54)【発明の名称】 ブロックチェーンベースの自動化アーキテクチャサイバーセキュリティ

(57)【特許請求の範囲】
【請求項1】

複数の参加者によって保守される分散型台帳を使用して、プロセス制御システムおよび接続された計装にソフトウェアまたはファームウェアの状態を記録するための方法であって、

コンピューティングデバイスによって、各々が物理的機能を実行して産業プロセスを制御する1つ以上のフィールドデバイスを有するプロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態を取得することであって、前記ソフトウェアまたはファームウェアが、前記プロセスプラント内のネットワークまたはプロセス制御デバイス内で実行される、取得することと、

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記現在の状態に対応する暗号ハッシュ値を含むトランザクションを生成することであって、前記トランザクションが前記分散型台帳に記憶される、生成することと、

前記分散型台帳を保守する参加者の分散型台帳ネットワークへの少なくとも1人の他の参加者へ前記トランザクションを送信することと、

前記ソフトウェアまたはファームウェアを実行する前記ネットワークまたはプロセス制御デバイスから、前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの状態を取得することと、

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記状態を前記分散型台帳からの前記暗号ハッシュ値と比較して、前記ソフトウェアまたはファ

ームウェアが改ざんされていないことを確認することと、
を含む、方法。

【請求項 2】

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記現在の状態が、前記現在の状態を更新したユーザのコンピューティングデバイスから取得され、前記トランザクションを生成することが、

前記ユーザのアイデンティティデータを取得することと、

1つ以上のプロセッサにおいて、前記ユーザの前記アイデンティティデータで前記トランザクションを増強することと、

前記1つ以上のプロセッサにおいて、前記トランザクションに基づいて暗号署名を生成することと、

前記1つ以上のプロセッサにおいて、前記暗号署名で前記トランザクションを増強することと、をさらに含む、請求項1に記載の方法。

【請求項 3】

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記状態が、前記暗号ハッシュ値に従って、前記分散型台帳に記憶された前記ソフトウェアまたはファームウェアの前記現在の状態と一致しないと判定することに応答して、前記ソフトウェアまたはファームウェアが前記プロセスプラント内で実行されるのを防止することをさらに含む、請求項1に記載の方法。

【請求項 4】

前記ソフトウェアまたはファームウェアを以前の状態に戻すことをさらに含む、請求項3に記載の方法。

【請求項 5】

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記状態が、前記暗号ハッシュ値に従って、前記分散型台帳に記憶された前記ソフトウェアまたはファームウェアの前記現在の状態と一致すると判定することに応答して、前記ネットワークまたはプロセス制御デバイスに前記ソフトウェアまたはファームウェアを実行させることをさらに含む、請求項3または請求項4に記載の方法。

【請求項 6】

前記トランザクションをトランザクションのブロックに追加することと、

前記トランザクションのブロックに基づいて暗号パズルを解くことと、

前記暗号パズルの解を前記トランザクションのブロックに追加することと、

前記トランザクションのブロックを、前記分散型台帳ネットワークへの少なくとも1人の他の参加者へ送信することと、をさらに含む、請求項2に記載の方法。

【請求項 7】

前記トランザクション内の前記アイデンティティデータを、前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記状態を更新することを認可されたユーザに対応するアイデンティティデータの複数のセットと比較することと

前記アイデンティティデータが前記アイデンティティデータの複数のセット内に含まれる場合に、前記トランザクションを前記トランザクションのブロックに追加することと、
をさらに含む、請求項6に記載の方法。

【請求項 8】

前記分散型台帳が、許可されたブロックチェーンである、請求項1から請求項7のいずれかに記載の方法。

【請求項 9】

複数の参加者によって保守される分散型台帳を使用して、プロセス制御システムおよび接続された計装にソフトウェアまたはファームウェアの状態を記録するためのシステムであって、

プロセスプラント内に配設された、各々が工業プロセスを制御する物理的機能を実行する1つ以上のデバイスと、

10

20

30

40

50

前記プロセスプラント内で実行されるコンピューティングデバイスであって、
1つ以上のプロセッサと、
通信ユニットと、

前記1つ以上のプロセッサおよび前記通信ユニットに連結され、かつ命令を記憶した、非一過性コンピュータ可読媒体と、を含む、コンピューティングデバイスとを含み、前記命令が、前記1つ以上のプロセッサによって実行されると、前記コンピューティングデバイスに、

前記プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態を取得することであって、前記ソフトウェアまたはファームウェアが、前記プロセスプラント内に配設された前記1つ以上のデバイスのうちの少なくとも1つまたは前記プロセスプラント内のネットワークデバイス内で実行される、取得することと、

10

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記現在の状態に対応する暗号ハッシュ値を含むトランザクションを生成することであって、前記トランザクションが前記分散型台帳に記憶される、生成することと、

前記分散型台帳の前記トランザクションを検証および記録するために、前記分散型台帳を保守する参加者の分散型台帳ネットワークへの少なくとも1人の他の参加者へ、前記トランザクションを送信することと、を行わせるシステムであって、

サーバデバイスは、

1つ以上のプロセッサと、

前記1つ以上のプロセッサに連結され、かつ命令を記憶した、非一過性コンピュータ可読媒体と、を含み、前記命令が、前記1つ以上のプロセッサによって実行されると、前記サーバデバイスに、

20

前記ネットワークデバイスまたは、前記ソフトウェアまたはファームウェアを実行する前記1つ以上のデバイスから、前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの状態を取得することと、

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記状態を前記分散型台帳からの前記暗号ハッシュ値と比較して、前記ソフトウェアまたはファームウェアが改ざんされていないことを確認することと、
を行わせる、システム。

【請求項10】

30

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記現在の状態が、前記現在の状態を更新したユーザのコンピューティングデバイスから取得され、前記トランザクションを生成するために、前記命令が前記コンピューティングデバイスに、

前記ユーザのアイデンティティデータを取得することと、

前記ユーザの前記アイデンティティデータで前記トランザクションを増強することと、

前記トランザクションに基づいて暗号署名を生成することと、

前記暗号署名で前記トランザクションを増強することと、を行わせる、請求項9に記載のシステム。

【請求項11】

40

前記命令が、前記サーバデバイスに、

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記状態が、前記暗号ハッシュ値に従って、前記分散型台帳に記憶された前記ソフトウェアまたはファームウェアの前記現在の状態と一致しないと判定することに応答して、前記ソフトウェアまたはファームウェアが前記プロセスプラント内で実行されるのを防止することをさらに行わせる、請求項9に記載のシステム。

【請求項12】

前記命令が、前記サーバデバイスに、

前記ソフトウェアまたはファームウェアを以前の状態に戻すことをさらに行わせる、請求項11に記載のシステム。

50

【請求項 13】

前記命令が、前記サーバデバイスに、

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記状態が、前記暗号ハッシュ値に従って、前記分散型台帳に記憶されたソフトウェアまたはファームウェアの前記現在の状態と一致すると判定することに対応して、前記ネットワークデバイスまたはプロセス制御デバイスに前記ソフトウェアまたはファームウェアを実行させることをさらに行わせる、請求項 11 または請求項 12 に記載のシステム。

【請求項 14】

前記命令が、前記コンピューティングデバイスに、

前記トランザクションをトランザクションのブロックに追加することと、

前記トランザクションのブロックに基づいて暗号パズルを解くことと、

前記暗号パズルの解を前記トランザクションのブロックに追加することと、

前記トランザクションのブロックを、前記分散型台帳ネットワークへの少なくとも 1 人の他の参加者へ送信することと、をさらに行わせる、請求項 10 に記載のシステム。

【請求項 15】

前記命令が、前記コンピューティングデバイスに、

前記トランザクション内の前記アイデンティティデータを、前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記状態を更新することを認可されたユーザに対応するアイデンティティデータの複数のセットと比較することと

前記アイデンティティデータが前記アイデンティティデータの複数のセット内に含まれる場合に、前記トランザクションを前記トランザクションのブロックに追加することと、をさらに行わせる、請求項 14 に記載のシステム。

【請求項 16】

前記分散型台帳が、許可されたブロックチェーンである、請求項 9 から請求項 15 のいずれかに記載のシステム。

【請求項 17】

分散型台帳ネットワーク上のプロセスプラント内の検証ネットワークノードであって、

1 つ以上のフィールドデバイスと通信するように構成された送受信機であって、各フィールドデバイスが物理的機能を実行して前記プロセスプラント内の産業プロセスを制御し、かつ分散型台帳データをピアネットワークノードと交換し、前記分散型台帳データが、前記プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態に対応する暗号ハッシュ値を表すデータを有するトランザクションを含む、送受信機と、

分散型台帳のコピーを記憶するように構成された記憶媒体と、

前記ピアネットワークノードから受信した前記分散型台帳データに合意ルールのセットを適用するように構成されたプロセスデータ検証器であって、前記分散型台帳データが前記合意ルールを満たす場合に、前記ピアネットワークノードから受信した前記分散型台帳データを前記分散型台帳の前記コピーに付加するようにさらに構成された、プロセスデータ検証器と、を備え、

前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの状態を取得し、前記分散型台帳からの前記暗号ハッシュ値と比較して、前記ソフトウェアまたはファームウェアが改ざんされていないことを確認することと、

を含む、検証ネットワークノード。

【請求項 18】

ピアネットワークノードから受信した分散型台帳データを付加するために、前記プロセスデータ検証器が、

トランザクションのブロックに基づいて暗号パズルを解くことと、

前記暗号パズルの解を前記トランザクションのブロックに追加することと、

前記トランザクションのブロックを、前記分散型台帳のコピーに付加することと、

前記トランザクションのブロックを前記分散型台帳ネットワークの前記ピアネットワークノードの少なくとも 1 つへ送信することと、を行うように構成されている、請求項 17

10

20

30

40

50

に記載の検証ネットワークノード。

【請求項 19】

前記合意ルールが、

トランザクションもしくはトランザクションのブロックに対するフォーマット要件、

前記ピアネットワークノードのうちのいずれが前記分散型台帳に次のトランザクションもしくはトランザクションのブロックを追加するかを決定するメカニズム、

または前記トランザクションの各々に含まれるソフトウェアもしくはファームウェア状態データをハッシュする暗号ハッシュアルゴリズム、のうちの少なくとも1つを含む、請求項 17 または請求項 18 に記載の検証ネットワークノード。

【請求項 20】

前記ピアネットワークノードから受信した前記分散型台帳データが、前記プロセスプラント内で実行される前記ソフトウェアまたはファームウェアの前記現在の状態を表すデータを有するトランザクションを生成するデバイスのユーザのアイデンティティ証明を含む、請求項 17 から請求項 19 のいずれかに記載の検証ネットワークノード。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、一般に、プロセスプラントおよびプロセス制御システムに関し、より具体的には、データおよびイベントを記録するためのプロセス制御システムにおける分散型台帳の使用に関する。

【背景技術】

【0002】

化学、石油、または他のプロセスプラントにおいて使用されるもの等の分散型プロセス制御システムは、典型的には、アナログバス、デジタルバス、またはアナログ／デジタル連結バスを介して、あるいは無線通信リンクまたはネットワークを介して、1つ以上のフィールドデバイスと通信可能に連結される、1つ以上のプロセスコントローラを含む。例えば、バルブ、バルブポジショナ、スイッチ、およびトランスミッタ（例えば、温度、圧力、レベルおよび流量センサ）であり得るフィールドデバイスは、プロセス環境内に位置付けられ、概して、バルブの開閉、圧力、温度、等のプロセスパラメータの測定等の物理的またはプロセス制御機能を行って、プロセスプラントまたはシステム内で実行中の1つ以上のプロセスを制御する。周知の `Fieldbus` プロトコルに準拠するフィールドデバイス等のスマートフィールドデバイスはまた、制御計算、アラーム機能、およびコントローラ内で一般に実装される他の制御機能も実行し得る。プロセスコントローラも典型的にはプラント環境内に配置され、このプロセスコントローラは、フィールドデバイスによって行われるプロセス測定を示す信号および／またはフィールドデバイスに関する他の情報を受信し、例えば、プロセス制御判断を行い、受信した情報に基づき制御信号を生成し、`HART`（登録商標）、`Wireless HART`（登録商標）、および `FOUNDATION`（登録商標）`Fieldbus` フィールドデバイス等のフィールドデバイスで行われる制御モジュールまたはブロックと連携する、異なる制御モジュールを実行するコントローラアプリケーションを実行する。コントローラ内の制御モジュールは、通信ラインまたはリンクを経由して、フィールドデバイスに制御信号を送信し、それによって、プロセスプラントまたはシステムの少なくとも一部分の動作を制御する。本明細書で利用されるように、フィールドデバイスおよびコントローラは、概して、「プロセス制御デバイス」と呼ばれる。

【0003】

フィールドデバイスおよびコントローラからの情報は、制御室もしくはより厳しいプラント環境から離れた他の場所に典型的に配置される、オペレータワークステーション、パーソナルコンピュータもしくはコンピューティングデバイス、データヒストリアン、レポートジェネレータ、集中データベース、または他の集中管理コンピューティングデバイス等の1つ以上の他のハードウェアデバイスに対して、通常、データハイウェイを通じて利

10

20

30

40

50

用可能にされる。これらのハードウェアデバイスの各々は、典型的には、プロセスプラントにわたって、またはプロセスプラントの一部にわたって集中化される。これらのハードウェアデバイスは、例えば、オペレータが、プロセス制御ルーチンの設定の変更、コントローラもしくはフィールドデバイス内の制御モジュールの動作の修正、プロセスの現在の状態の閲覧、フィールドデバイスおよびコントローラによって生成されたアラームの閲覧、担当者の訓練もしくはプロセス制御ソフトウェアの試験を目的としたプロセスの動作のシミュレーション、構成データベースの保守および更新等の、プロセスの制御および／またはプロセスプラントの動作に関する機能を行うことを可能にし得るアプリケーションを実行する。ハードウェアデバイス、コントローラ、およびフィールドデバイスによって利用されるデータハイウェイは、有線通信経路、無線通信経路、または有線および無線通信経路の組み合わせを含み得る。

10

【0004】

例として、Emerson Process Managementによって販売されているDelta V（商標）制御システムは、プロセスプラント内の多様な場所に位置付けられている異なるデバイス内に記憶され、それら異なるデバイスによって実行される複数のアプリケーションを含む。1つ以上のワークステーションまたはコンピューティングデバイス内に備わる構成アプリケーションは、ユーザによる、プロセス制御モジュールの作成または変更、およびデータハイウェイを経由した、これらのプロセス制御モジュールの、専用分散型コントローラへのダウンロードを可能にする。典型的には、これらの制御モジュールは、通信可能に相互接続された機能ブロックで構成され、これらの機能ブロックは、それに対する入力に基づき制御スキーム内で機能を実行し、出力を制御スキーム内の他の機能ブロックに提供するオブジェクト指向プログラミングプロトコル内のオブジェクトである。また、構成アプリケーションは、データをオペレータに対して表示するため、かつオペレータによるプロセス制御ルーチン内の設定点等の設定の変更を可能にするために閲覧アプリケーションが使用するオペレータインターフェースを、構成設計者が作成または変更することを可能にし得る。各専用コントローラ、および一部の場においては、1つ以上のフィールドデバイスは、実際のプロセス制御機能を実装するために、それらに割り当てられてダウンロードされた制御モジュールを実行するそれぞれのコントローラアプリケーションを記憶および実行する。視認アプリケーションは、1つ以上のオペレータワークステーション（またはオペレータワークステーションおよびデータハイウェイと通信可能に接続された1つ以上のリモートコンピューティングデバイス）上で実行され得、この視認アプリケーションは、コントローラアプリケーションからデータハイウェイを経由してデータを受信し、ユーザインターフェースを使用してこのデータをプロセス制御システム設計者、オペレータ、またはユーザに表示して、オペレータのビュー、エンジニアのビュー、技師のビュー等のいくつかの異なるビューのうちのいずれかを提供し得る。データヒストリアンアプリケーションが、典型的には、データハイウェイにわたって提供されるデータの一部または全てを収集および記憶するデータヒストリアンデバイスに記憶され、それによって実行される一方で、構成データベースアプリケーションが、現在のプロセス制御ルーチン構成およびそれと関連付けられたデータを記憶するために、データハイウェイに取り付けられたなおさらに離れたコンピュータで作動され得る。代替的に、構成データベースは、構成アプリケーションと同じワークステーションに配置されてもよい。

20

30

40

【発明の概要】

【発明が解決しようとする課題】

【0005】

一般的に言って、プロセスプラントのプロセス制御システムは、フィールドデバイス、コントローラ、ワークステーション、および階層化されたネットワークとバスとのセットによって相互接続されたその他のデバイスを含む。次に、プロセス制御システムは、例えば、製造および運用コストを削減し、生産性および効率を高め、プロセス制御および／またはプロセスプラント情報等に適時にアクセスできるようにするために、様々なビジネスおよび外部ネットワークに接続され得る。一方、プロセスプラントおよび／またはプロセ

50

ス制御システムの、企業および／または外部のネットワークおよび／またはシステムへの相互接続は、企業および／または外部のネットワークで使用されるもの等、商用システムおよびアプリケーションにおいて予想される脆弱性から生じ得るサイバー侵入および／または悪意のあるサイバー攻撃のリスクを増加させる。プロセスプラント、ネットワーク、および／または制御システムのサイバー侵入と悪意のあるサイバー攻撃とは、情報資産の機密性、完全性、および／または可用性に悪影響を与える可能性があり、これは一般的に言って、汎用コンピューティングネットワークのものと類似した脆弱性である。ただし、汎用コンピュータネットワークとは異なり、プロセスプラント、ネットワーク、および／または制御システムのサイバー侵入は、プラント機器、製品、および他の物理的資産の損害、破壊、および／または損失だけでなく、人命の損失をももたらし得る。例えば、サイバー侵入は、プロセスを制御不能にし、それによって爆発、火災、洪水、危険物への暴露等を発生させ得る。したがって、プロセス制御プラントおよびシステムに関連する通信を保護することは極めて重要である。

10

【0006】

プロセス制御システムにおいて分散型台帳またはブロックチェーンを利用するための技術、システム、装置、コンポーネント、デバイス、および方法が開示される。そのような技術、システム、装置、構成要素、デバイス、および方法は、工業プロセス制御システム、環境、および／またはプラントに対して適用することができ、これらは本明細書においては交換可能に、「工業制御」、「プロセス制御」、もしくは「プロセス」システム、環境、および／またはプラントとも呼ばれる。典型的には、そのようなシステムおよびプラントは、分散型の様式で、物理的物質または生産物を製造、精製、変形、生成、または生産するように動作する、1つ以上のプロセスの制御を提供する。

20

【課題を解決するための手段】

【0007】

例えば、プロセス制御システムでは、分散型台帳は、本明細書で「エッジゲートウェイ」と呼ばれるノードによって保守される。このノードは、フィールドデバイス、コントローラ、オペレータワークステーション、またはプロセスプラント内で動作する他のデバイスへブロードキャストされたトランザクションを受信する。いくつかのシナリオでは、トランザクションは、プロセスプラントエンティティに対応するプロセスパラメータのためのプロセスパラメータ値を含む。プロセスプラントエンティティは、バルブ、タンク、ミキサ、ポンプ、熱交換器等の物理的材料を包含、変換、生成、または移送するプロセスの一部で使用するプロセスプラント内のデバイスを含み得る。トランザクションはまた、製品の温度、製品の体積、製品の質量、製品の密度、製品の圧力等、プロセスプラントによって生産される物理的材料または製品の特性等の製品パラメータ値を含み得る。

30

【0008】

その後、記録されたプロセスパラメータ値および製品パラメータ値を取り出して、製品の品質を確認し得る。例えば、第1のプロセスプラントは、製品を製造、精製、変換、生成、または生産し、その後、第2のプロセスプラントへ出荷され得る。第2のプロセスプラントは、記録されたプロセスパラメータ値および製品パラメータ値を分散型台帳から取り出すことによって、製品が特定の品質基準を満たしていると判定し得る。加えて、分散型台帳に規制データが記録され得る。例えば、アラーム、エラー、リーク、修復イベント、プロセスマイルストーン、是正措置等のトリガイイベントに応答して、フィールドデバイスやコントローラ等のプロセス制御要素は、イベントが発生した時間、イベントの期間、イベントに関与するプロセスプラントエンティティのためのプロセスパラメータ値等のトリガイイベントからのデータを含むトランザクションを生成し得る。その後、規制データが分散型台帳に記録されるため、規制当局はデータをレビューすることができる。

40

【0009】

さらにまた、分散型台帳を使用して、スマートコントラクトを実行してもよく、これについては、以下でより詳細に記載する。プロセス制御システムは、分散型台帳にスマートコントラクトを展開して、例えば良好な状態で製品を受領する際に値を交換することがで

50

きる。また、スマートコントラクトを分散型台帳に展開して、フィールドデバイス等のマシンが人間の介入なしで自ら処理することを可能にし得る。例えば、スマートコントラクトの条件に従って、第1のプロセスプラント内のコンピューティングデバイスは、第1のプロセスプラント内の1つ以上のフィールドデバイスから、製品が第2のプロセスプラントから納入され、製品が特定の品質基準を満たしていることの表示を受信すると、所定のトークン量を第2のプロセスプラント内のコンピューティングデバイスへ自動的に提供し得る。また、以下で詳細に説明する他の多数のアプリケーションのプロセスプラントにおいてスマートコントラクトが利用され得る。

【0010】

分散型台帳を利用する、いくつかのシナリオでは、プロセスプラント内でスマートコントラクトを利用することによって、各プロセスプラント、またはプロセスプラントのネットワークは、プロセスプラント内のトランザクションの、信頼できる、安全な、かつ不変の記録を提供し得る。分散型台帳の安全な、不変の、かつ信頼できない性質は、サイバー侵入がプラント機器、製品、および他の物理的資産の損害、破壊、および／または損失のみならず、人間の生活の損失にもつながり得るプロセス制御システム内で特に重要である。加えて、分散型台帳は、プロセスプラントが、原材料から完成品までの製品系統を追跡し、原材料が加工された後の製品をさらに追跡できるようにする。その上、競合するエンティティが共通のリソースを利用または転送する場合、分散型台帳を使用して、エンティティのうちの1つが利用するリソースの量を決定し、リソースの使用に対する競合エンティティへの公正な補償を行うことができる。例えば、石油精製所は、石油パイプラインを介していくつかのエンティティまたはプロセスプラントへ供給される石油を生産し得る。各プロセスプラントは、プロセスプラントが石油パイプラインから受領した石油の量を石油精製所に補償する責任がある。分散型台帳を使用して、各プロセスプラントが、石油が供給されたときに石油の量を測定するデバイスから受領した石油の量を記録することができる。分散型台帳内の記録されたデータを変更することは困難であるため、競合するエンティティは、このデータが信頼できることを確信する必要はない。

【図面の簡単な説明】

【0011】

【図1】とりわけ、プロセス制御システム、プロセス制御システム自体、および他のシステムおよび／またはネットワークの様々な例示的なコンポーネント間の相互接続を示す、例示的なプロセスプラントまたはプロセス制御システムのブロック図である。

【図2】プロセスプラントまたはプロセス制御システムの例示的なセキュリティアーキテクチャのブロック図である。

【図3】プロセス制御システムにおいてトランザクションを記録し、スマートコントラクトを実行するための例示的な分散型台帳システムである。

【図4】プロセス制御システム内の分散型台帳ネットワーク上の、例示的な検証ネットワークノードおよび例示的なトランザクションフローを示す。

【図5】プロセス制御システム内の分散型台帳ネットワーク上のネットワークノードの例示的なコンポーネントを示す。

【図6A】プロセス制御システム内のトランザクションのブロックを有するブロックチェーンを含む分散型台帳の例を示す。

【図6B】複数のサイドブロックチェーンまたは異なるプロセスプラントによって保守されるサイドチェーンと、サイドチェーンからのトランザクションデータを組み込むいくつかのプロセスプラントによって保守されるメインブロックチェーンと、を含む別の分散型台帳の例を示す。

【図7A】各々が異なるプロセスプラントによって保守される複数のローカルブロックチェーンを含む、さらに別の分散型台帳の例を示す。

【図7B】いくつかのプロセスプラントによって保守され、かつローカルブロックチェーンからのブロックを組み込むプロセスプラントのためのグローバルブロックチェーンを示す。

10

20

30

40

50

【図 7 C】各プロセスプラントにグローバルブロックチェーンの各々からのブロックを組み込むいくつかのプロセスプラントによって保守されるスーパーブロックチェーンを示す。

【図 8】安全な計装システム（S I S）デバイスにプロセスパラメータを書き込むために、プロセスプラントにおいて安全な書き込み動作を実行するための分散型台帳ネットワークにおける例示的なスマートコントラクト状態を示す。

【図 9】石油パイプラインから受領した石油の量を報告するフィールドデバイスである証拠オラクルによって生成された証拠トランザクションを表す例示的なトランザクションを示す。

【図 10】ソフトウェアまたはファームウェアの更新を報告するコンピューティングデバイスである証拠オラクルによって生成された証拠トランザクションを表す例示的なトランザクションを示す。

10

【図 11】プロセスパラメータまたは製品パラメータデータを報告するプロセスプラントエンティティである証拠オラクルによって生成された証拠トランザクションを表す例示的なトランザクションを示す。

【図 12】分散型台帳を使用してプロセス制御システムにデータを記録するための例示的な方法を表すフロー図を示す。

【図 13】分散型台帳を使用してプロセス制御システムでの信頼できないデータの安全な計量のための例示的な方法を表すフロー図を示す。

【図 14】分散型台帳を使用してプロセス制御システムに品質管理、生産、または規制データを記録するための例示的な方法を表すフロー図を示す。

20

【図 15】分散型台帳を使用して、プロセス制御システムおよび接続された計装にソフトウェアまたはファームウェアの状態を記録するための例示的な方法を表すフロー図を示す。

【図 16】分散型台帳を使用してプロセス制御システム内のスマートコントラクトを作成するための例示的な方法を表すフロー図を示す。

【図 17】分散型台帳を使用してプロセス制御システム内のスマートコントラクトとインタラクションするための例示的な方法を表すフロー図を示す。

【発明を実施するための形態】

【0012】

分散型台帳は、いく人かの参加者によって保守されるデータ、イベント、トランザクション等の記憶メカニズムである。より具体的には、分散型台帳は、分散型台帳に記録された情報の有効性または無効性に関する分散合意を達成する方法である。つまり、分散型台帳は、参加者およびオブザーバへ分散型の信頼を提供する。中央機関に依存するのは対照的に、分散型台帳は、台帳への変更のトランザクション記録がピアツーピアネットワークの各ノードによって保守および検証される分散型データベースである。分散型台帳の 1 つのタイプであるブロックチェーンは、「ブロック」にまとめられたトランザクションのグループで構成され、順番に並べられる（したがって、「ブロックチェーン」という用語）。ここで説明する分散型台帳は、ブロックチェーンに関連して言及されるが、これは分散型台帳の単なる一例である。分散型台帳はまた、もつれ、ブロックラティス、または他の有向非循環グラフ（*directed acyclic graph*、*DAG*）を含み得る。いずれにせよ、ノードは時間の経過とともにブロックチェーンネットワークに参加し、およびブロックチェーンネットワークを離脱してもよく、ノードが存在しない間に伝播されたピアノードからブロックを取得し得る。ノードは、他のノードのアドレスを保持し、既知のノードのアドレスを互いに交換して、分散型のピアツーピア方式でネットワークを介した新しい情報の伝播を促進し得る。

30

40

【0013】

台帳を共有するノードは、ここで分散型台帳ネットワークと称されるものを形成する。分散型台帳ネットワーク内のノードは、合意ルールのセットに従ってブロックチェーンへの変更を検証する（例えば、新しいトランザクションおよび／またはブロックが作成されるとき等）。合意ルールは、ブロックチェーンによって追跡される情報に依存し、チェーン自体に関するルールを含み得る。例えば、合意ルールは、変更の発生者がアイデンティ

50

ティ証明を供給して、承認されたエンティティのみがチェーンの変更を発生し得るようにすることを含み得る。合意ルールは、ブロックおよびトランザクションがフォーマット要件を遵守し、変更に関する特定のメタ情報を供給することを要求し得る（例えば、ブロックはサイズ制限未満でなければならない、トランザクションは多数のフィールドを含まなければならない、等）。合意ルールは、新たなブロックがチェーンに追加される順序を決定するメカニズムを含み得る（例えば、作業の証明システム、ステークの証明等）。

【0014】

合意ルールを満たすブロックチェーンへの追加は、検証ノードが認識している他のノードへの追加を検証したノードから伝播される。ブロックチェーンへの変更を受信するノードのうちの全てが新たなブロックを検証する場合に、分散型台帳は全てのノード上に記憶されている新たな変更を反映し、新たなブロックとそこに含まれる情報とに関して分散合意に達したと言える。合意ルールを満たさない変更はいずれも、変更を受信するノードを検証することによって無視され、変更は他のノードに伝播されない。したがって、中央当局を使用する従来のシステムとは異なり、合意ルールを満たす方法で単一の当事者が変更することができない限り、単一の当事者は分散型台帳を一方的に変更することができない。過去のトランザクションを修正することができないため、ブロックチェーンは一般的に、信頼され、安全で、かつ不変であるように記述される。

【0015】

ブロックチェーンネットワークに対して合意ルールを適用するノードの検証アクティビティは、様々な形態をとり得る。一実装形態では、ブロックチェーンは、資産の所有権等のデータを追跡する共有スプレッドシートとして表示され得る。別の実装形態では、検証ノードは、「スマートコントラクト」に含まれるコードを実行し、分散合意は、実行されたコードの出力に同意するネットワークノードとして表される。

【0016】

スマートコントラクトは、異なる当事者間の合意の自動実行および／または自動実施を可能にするコンピュータプロトコルである。特に、スマートコントラクトは、ブロックチェーン上の特定のアドレスに位置するコンピュータコードであり得る。場合によっては、スマートコントラクトが記憶されているアドレスにブロックチェーンへの参加者が資金（ビットコイン、イーサ、その他のデジタル／仮想通貨等の暗号通貨）を送信すると、スマートコントラクトが自動的に稼働し得る。加えて、スマートコントラクトは、そのアドレスに記憶されている資金の残高のバランスを保守し得る。いくつかのシナリオでは、このバランスがゼロに達すると、スマートコントラクトは機能しなくなり得る。

【0017】

スマートコントラクトは、満たされると1つ以上のアクションに対応する1つ以上のトリガ条件を含み得る。いくつかのスマートコントラクトに対して、実行されるアクション（複数可）は1つ以上の決定条件に基づいて決定され得る。場合によっては、スマートコントラクトは、トリガ条件が発生したことを検出し、および／または決定条件を分析し得るように、データストリームをスマートコントラクトヘルペティングし得る。

【0018】

ブロックチェーンが、公開され、分散された、許可のない態様で展開されてもよく、つまり、いかなる当事者も、分散型台帳を表示し、台帳に追加される新たな情報を送信し、または検証ノードとしてネットワークに参加し得る。他のブロックチェーンは、ブロックチェーンネットワークに参加することが許可されたエンティティのグループ間でチェーンデータをプライベートに保つプライベート（例えば、許可された台帳等）である。他のブロックチェーンの実装形態は、許可されている場合と許可されていない場合との両方があるため、参加者を検証することが必要になり得るが、ネットワークへの参加者が公開したい情報のみが公開される。

【0019】

いくつかの実装形態では、分散型台帳は、メインブロックチェーンおよびメインブロックチェーンとは独立して動作するいくつかのサイドチェーン等の複数のブロックチェーン

10

20

30

40

50

を含む。次に、サイドチェーンはメインブロックチェーンとインタラクションして、サイドチェーンからメインブロックチェーンへトランザクションデータのうちのいくつかを提供する。このようにして、メインブロックチェーンがパブリックであるか、サイドチェーンよりも多数のエンティティが利用できる一方で、サイドチェーンをプライベートにすることができる。サイドチェーンからの非機密情報は、メインブロックチェーン上で共有され得る。また、いくつかの実装形態では、分散型台帳は、同じ検証ノードによって保守される、並行して実行される複数のレイヤまたは個別のブロックチェーンを含む。第1のレイヤのためのブロックチェーンからのトランザクションデータのうちのいくつかは、第2のレイヤのためのブロックチェーンへ提供されるか、またはその逆であり得る。

【0020】

一例では、プライベートエンタープライズネットワーク、インターネット、セルラータ、バックホールインターネット、またはその他のタイプのバックホール接続等の、1つ以上のパブリックおよび／またはプライベートネットワークを使用して他のプロセスプラント等のリモートシステムへデータを送信する「エッジゲートウェイ」と称されるノードを検証することによって、プロセス制御システム内の分散型台帳が保守され得る。エッジゲートウェイは、例えば、プロセスプラント内で動作するフィールドデバイスまたはコントローラ等のプロセス制御デバイスによって、分散型台帳ネットワークにブロードキャストされたトランザクションを受信する。オペレータワークステーション、サーバデバイス、またはプロセスプラント内の他のユーザインターフェースデバイス等の他のコンピューティングデバイスも、トランザクションを分散型台帳ネットワークにブロードキャストし得る。その後、エッジゲートウェイは、ブロードキャストされたトランザクションを検証する。

【0021】

別の例では、エッジゲートウェイは「スマートコントラクト」に包含されたコードを実行し、フィールドデバイスは、品質管理、規制の遵守、製品の配達または受領、および配達／受領量等に関連する証拠をブロックチェーンへ提供する「証拠オラクル」として機能する。

【0022】

図1は、本明細書で記載する新規な分散型台帳技術のうちのいずれか1つ以上を利用し得る例示的なプロセスプラント10のブロック図である。プロセスプラント10（本明細書では、プロセス制御システム10またはプロセス制御環境10と言い換え可能である）は、フィールドデバイスによって作成されたプロセス測定値を表示する信号を受信し、この情報を処理して制御ルーチンを実装し、有線または無線プロセス制御通信リンクまたはネットワークを経由して他のフィールドデバイスへ送信されて、プラント10内のプロセスの動作を制御する、1つ以上のプロセスコントローラを含む。典型的には、少なくとも1つのフィールドデバイスが物理的機能（例えば、バルブの開閉、温度の上昇または下降、測定、状況の検知など）を実行し、プロセスの動作を制御する。フィールドデバイスのうちのいくつかのタイプは、I/Oデバイスを使用してコントローラと通信する。プロセスコントローラ、フィールドデバイスおよびI/Oデバイスは、有線または無線であってもよく、任意の数および組み合わせの有線および無線プロセスコントローラ、フィールドデバイスおよびI/Oデバイスが、プロセスプラント環境またはシステム10内に含まれてもよい。

【0023】

例えば、図1は、プロセスコントローラ11を示し、このプロセスコントローラは、入力／出力（I/O）カード26および28を介して、有線フィールドデバイス15～22と通信可能に接続され、無線ゲートウェイ35およびプロセス制御データハイウェイまたはバックボーン105を介して、無線フィールドデバイス40～46と通信可能に接続される。プロセス制御データハイウェイ105は、1つ以上の有線および／または無線通信リンクを含むことができ、例えば、イーサネット（登録商標）プロトコルなどの任意の所望のまたは好適なまたは通信プロトコルを使用して実装することができる。いくつかの構

10

20

30

40

50

成（図示せず）では、コントローラ 11 は、1 つ以上の通信プロトコル、例えば Wi-Fi または他の IEEE 802.11 準拠の無線ローカルエリアネットワークプロトコル、モバイル通信プロトコル（例えば、WiMAX、LTE、または他の ITU-R 互換プロトコル）、Bluetooth（登録商標）、HART（登録商標）、Wireless HART（登録商標）、Profibus、FOUNDATION（登録商標）Fieldbus、など、をサポートする任意の数の他の有線または無線通信リンクを使用することによってなど、バックボーン 105 以外の 1 つ以上の通信ネットワークを使用して、無線ゲートウェイ 35 に通信可能に接続され得る。

【0024】

コントローラ 11 は、例として、Emerson Process Management より販売されている Delta V（商標）コントローラであってもよく、フィールドデバイス 15～22 および 40～46 のうちの少なくともいくつかを用いて、バッチプロセスまたは連続的プロセスを実施するように動作し得る。実施形態では、プロセス制御データハイウェイ 105 に通信可能に接続されているのに加えて、コントローラ 11 はまた、例えば、標準的な 4～20mA デバイス、I/O カード 26、28、および／または FOUNDATION（登録商標）Fieldbus プロトコル、HART（登録商標）プロトコル、Wireless HART（登録商標）プロトコル、等のような任意のスマート通信プロトコルと関連付けられた、任意の所望のハードウェアおよびソフトウェアを使用して、フィールドデバイス 15～22 および 40～46 のうちの少なくともいくつかと通信可能に接続される。図 1 において、コントローラ 11、フィールドデバイス 15～22 および I/O カード 26、28 は、有線デバイスであり、フィールドデバイス 40～46 は、無線フィールドデバイスである。当然ながら、有線フィールドデバイス 15～22 および無線フィールドデバイス 40～46 は、任意の他の所望の規格（複数可）またはプロトコル、例えば今後開発される任意の規格またはプロトコルを含む任意の有線または無線プロトコルに適合することができる。

【0025】

図 1 のプロセスコントローラ 11 は、1 つ以上のプロセス制御ルーチン 38（例えば、メモリ 32 内に記憶されている）を実装または監督するプロセッサ 30 を含む。プロセッサ 30 は、フィールドデバイス 15～22 および 40～46 と、およびコントローラ 11 に通信可能に接続された他のノードと通信するように構成されている。本明細書に記載される任意の制御ルーチンまたはモジュールは、そのように所望される場合は、その一部を異なるコントローラまたは他のデバイスによって実装または実行させてもよいことに留意されたい。同様に、プロセス制御システム 10 内で実装される本明細書に記載の制御ルーチンまたはモジュール 38 は、ソフトウェア、ファームウェア、ハードウェア等を含む任意の形態を取ってもよい。制御ルーチンは、オブジェクト指向プログラミング、ラダー論理、シーケンシャルファンクションチャート、機能ブロックダイアグラム、または任意の他のソフトウェアプログラミング言語もしくは設計パラダイムを使用したもの等の任意の所望のソフトウェアフォーマットにおいて実装されてもよい。制御ルーチン 38 は、ランダムアクセスメモリ（RAM）または読み取り専用メモリ（ROM）等の任意の所望のタイプのメモリ 32 に記憶され得る。同様に、制御ルーチン 38 は、例えば 1 つ以上の EPROM、EEPROM、特定用途向け集積回路（ASIC）、または任意の他のハードウェアもしくはファームウェア要素にハードコードされてもよい。したがって、コントローラ 11 は、任意の所望の様式で制御ストラテジまたは制御ルーチンを実装するように構成することができる。

【0026】

コントローラ 11 は、一般に機能ブロックと称されるものを使用して制御ストラテジを実施し、この場合、各機能ブロックは、制御ルーチン全体のオブジェクトまたは他の部分（例えばサブルーチン）であり、プロセス制御システム 10 内でプロセス制御ループを実施するために（リンクと呼ばれる通信を介して）他の機能ブロックと協働して動作する。制御ベースのファンクションブロックは、典型的には、トランスミッタ、センサまたは他

10

20

30

40

50

のプロセスパラメータ測定デバイスに関連付けられている入力機能、PID、ファジー論理等の制御を行う制御ルーチンに関連付けられている制御機能、またはバルブ等のいくつかのデバイスの動作を、プロセス制御システム10内のいくつかの物理的機能を実施するように制御する出力機能のうちの1つを実施する。当然のことながら、ハイブリッドおよび他のタイプの機能ブロックが存在する。機能ブロックはコントローラ11内に記憶され、それによって実行されてもよく、これは典型的には、これらの機能ブロックが標準的な4～20mAデバイスおよびHART（登録商標）デバイス等のいくつかのタイプのスマートフィールドデバイス用に使用されるかあるいはそれと関連するときに成り立ち、あるいは機能ブロックは、フィールドデバイスそのものの内部に記憶され、それによって実装されてもよく、これはFOUNDATION（登録商標）Fieldbusデバイスの場合に成り立ち得る。コントローラ11は、機能ブロックのうちの1つ以上を実行することによって行われる1つ以上の制御ループを実施し得る1つ以上の制御ルーチン38を含み得る。

【0027】

有線フィールドデバイス15～22は、センサ、バルブ、トランスミッタ、ポジショナ等の任意のタイプのデバイスであってよく、一方でI/Oカード26および28は、任意の所望の通信またはコントローラプロトコルに適合する任意のタイプのI/Oデバイスであってもよい。図1では、フィールドデバイス15～18は、アナログラインまたは組み合わされたアナログおよびデジタルラインを経由してI/Oカード26へ通信する、標準的な4～20mAデバイスまたはHART（登録商標）デバイスであり、一方でフィールドデバイス19～22は、FOUNDATION（登録商標）Fieldbusフィールドデバイスのような、FOUNDATION（登録商標）Fieldbus通信プロトコルを使用して、デジタルバスを経由してI/Oカード28へ通信するスマートデバイスである。しかし、いくつかの実施形態では、有線フィールドデバイス15、16および18～21のうちの少なくともいくつかならびに／またはI/Oカード26、28のうちの少なくともいくつかは、加えてまたは代わりに、プロセス制御データハイウェイ105を使用して、および／または他の好適な制御システムプロトコル（例えば、Profibus、DeviceNet、Foundation Fieldbus、ControlNet、Modbus、HART等）を使用することによって、コントローラ11と通信し得る。

【0028】

図1では、無線フィールドデバイス40～46は、WirelessHART（登録商標）プロトコル等の無線プロトコルを使用して、無線プロセス制御通信ネットワーク70を介して通信する。そのような無線フィールドデバイス40～46は、（例えば、無線プロトコルまたは別の無線プロトコルを使用して）無線通信するようにも構成される無線ネットワーク70の1つ以上の他のデバイスまたはノードと直接通信し得る。無線通信するように構成されていない1つ以上の他のノードと通信するために、無線フィールドデバイス40～46は、プロセス制御データハイウェイ105に、または別のプロセス制御通信ネットワークに接続された無線ゲートウェイ35を利用し得る。無線ゲートウェイ35は、無線通信ネットワーク70の様々な無線デバイス40～58へのアクセスを提供する。特に、無線ゲートウェイ35は、無線デバイス40～58、有線デバイス15～28、および／またはプロセス制御プラント10の他のノードまたはデバイス間の通信可能な連結を提供する。例えば、無線ゲートウェイ35は、プロセス制御データハイウェイ105を使用することによって、および／またはプロセスプラント10の1つ以上の他の通信ネットワークを使用することによって、通信可能な連結を提供し得る。

【0029】

有線フィールドデバイス15～22と同様に、無線ネットワーク70の無線フィールドデバイス40～46は、プロセスプラント10内の物理的制御機能、例えば、バルブの開閉、プロセスパラメータの測定値の取得、などを行う。しかしながら、無線フィールドデバイス40～46は、ネットワーク70の無線プロトコルを使用して通信するように構成されている。このように、無線フィールドデバイス40～46、無線ゲートウェイ35、

および無線ネットワーク 70 の他の無線ノード 52 ～ 58 は、無線通信パケットの生産者でありコンシューマである。

【0030】

プロセスプラント 10 のいくつかの構成では、無線ネットワーク 70 は、非無線デバイスを含む。例えば、図 1 では、フィールドデバイス 48 は、レガシ 4 ～ 20 mA デバイスであり、フィールドデバイス 50 は、有線 HART（登録商標）デバイスである。ネットワーク 70 内で通信するために、フィールドデバイス 48 および 50 は、無線アダプタ 52 A、52 B を介して無線通信ネットワーク 70 に接続される。無線アダプタ 52 A、52 B は、無線 HART 等の無線プロトコルをサポートし、かつ Foundation（登録商標）Fieldbus、PROFIBUS、DeviceNet 等の 1 つ以上の他の通信プロトコルもサポートし得る。加えて、いくつかの構成では、無線ネットワーク 70 は、無線ゲートウェイ 35 と有線通信する独立した物理デバイスであり得るか、または一体型デバイスとして無線ゲートウェイ 35 内に提供され得る、1 つ以上のネットワークアクセスポイント 55 A、55 B を含む。また、無線ネットワーク 70 はまた、無線通信ネットワーク 70 内の 1 つの無線デバイスから別の無線デバイスにパケットを転送するための 1 つ以上のルータ 58 を含む得る。図 1 では、無線デバイス 40 ～ 46 および 52 ～ 58 は、無線通信ネットワーク 70 の無線リンク 60 を経由して、および／またはプロセス制御データハイウェイ 105 を介して、互いに、および無線ゲートウェイ 35 と通信する。

【0031】

図 1 では、プロセス制御システム 10 は、データハイウェイ 105 に通信可能に接続された 1 つ以上のオペレータワークステーションまたはユーザインターフェースデバイス 8 を含む。オペレータワークステーション 8 を介して、オペレータは、プロセスプラント 10 のリアルタイム動作の閲覧および監視に加えて、必要であり得る任意の診断、是正、保守、および／または他の処置を取り得る。オペレータワークステーション 8 のうちの少なくともいくつかは、プラント 10 内またはその近くの様々な防護領域内に位置し得、いくつかの状況では、オペレータワークステーション 8 のうちの少なくともいくつかは、遠隔して位置するが、それにもかかわらずプラント 10 と通信可能に接続され得る。オペレータワークステーション 8 は、有線または無線コンピューティングデバイスであってもよい。

【0032】

プロセス制御システム 10 の例は、構成アプリケーション（図示せず）および構成データベース（図示せず）をさらに含むことができ、これらもそれぞれデータハイウェイ 105 に通信可能に接続される。上述のように、構成アプリケーション（図示せず）の様々なインスタンスを 1 つ以上のユーザインターフェースデバイス 8 上で実行し得、ユーザが、プロセス制御モジュールを作成または変更し、データハイウェイ 105 を介してこれらのモジュールをコントローラ 11 にダウンロードすることを可能にし、かつ、ユーザが、オペレータインターフェースを作成または変更することを可能にし、それを介して、オペレータは、データを閲覧し、プロセス制御ルーチン内のデータ設定を変更することができる。構成データベース（図示せず）は、作成された（例えば、構成された）モジュールおよび／またはオペレータインターフェースを記憶する。

【0033】

いくつかの構成では、プロセス制御システム 10 は、他の無線プロトコル、例えば Wi-Fi または他の IEEE 802.11 準拠の無線ローカルエリアネットワークプロトコル、モバイル通信プロトコル、例えば WiMAX（Worldwide Interoperability for Microwave Access）、LTE（Long Term Evolution）または他の ITU-R（国際電気通信連合無線通信部門（International Telecommunication Union Radio Communication Sector））互換性プロトコル、短波無線通信、例えば近距離無線通信（NFC）および Bluetooth（登録商標）、または他の無線通信プロトコルを用いて、他のデバイスと通信する 1 つ以上の他の無線アクセスポイント 7a を含む。典型的には、そのような無線アクセスポイント 7a は、ハンドヘル

ドまたは他のポータブルコンピューティングデバイスが、無線ネットワーク 70 とは異なる、かつ無線ネットワーク 70 とは異なる無線プロトコルをサポートするそれぞれの無線プロセス制御通信ネットワークを経由して通信することを可能にする。例えば、無線またはポータブルユーザインターフェースデバイス 8 は、オペレータによってプロセスプラント 10 内で利用されるモバイルワークステーションまたは診断試験機であってもよい。いくつかのシナリオでは、ポータブルコンピューティングデバイスに加えて、1 つ以上のプロセス制御デバイス（例えば、コントローラ 11、フィールドデバイス 15～22、または無線デバイス 35、40～58）もまた、アクセスポイント 7a によってサポートされている無線プロトコルを使用して通信する。

【0034】

いくつかの構成では、プロセス制御システム 10 は、近接したプロセス制御システム 10 の外部のシステムへの 1 つ以上のゲートウェイ 7b、7c を含む（本明細書では「エッジゲートウェイ」とも称され、以下でより詳細に説明する）。典型的には、そのようなシステムは、プロセス制御システム 10 によって生成されるか、または有効化される情報のカスタマまたはサプライヤである。例えば、プロセス制御プラント 10 は、近接したプロセスプラント 10 を別のプロセスプラントに通信可能に接続するためのゲートウェイノード 7b を含み得る。加えてまたは代わりに、プロセス制御プラント 10 は、近接したプロセスプラント 10 を、外部のパブリックまたはプライベートシステム、例えば研究所システム（例えば、研究所情報管理システムまたは LIMS）、オペレータラウンドデータベース、荷役システム、保守管理システム、製品在庫管理システム、製造スケジュール管理システム、天気データシステム、出荷および運搬システム、包装システム、インターネット、別のプロバイダのプロセス制御システム、または他の外部システムと通信可能に接続するためのゲートウェイノード 7c を含み得る。

【0035】

図 1 は、プロセスプラント 10 の例に含まれる有限数のフィールドデバイス 15～22 および 40～46、無線ゲートウェイ 35、無線アダプタ 52、アクセスポイント 55、ルータ 58、および無線プロセス制御通信ネットワーク 70 を有する単一のコントローラ 11 のみを図示しているが、この例は、単なる例示であり、非限定的な実施形態であることに留意されたい。任意の数のコントローラ 11 が、プロセス制御プラントまたはシステム 10 に含まれてもよく、コントローラ 11 のいずれもが、プラント 10 内のプロセスを制御するために、任意の数の有線または無線デバイスおよびネットワーク 15～22、40～46、35、52、55、58、および 70 と通信してもよい。

【0036】

さらに、図 1 のプロセスプラントまたは制御システム 10 は、フィールド環境（例えば、「プロセスプラントフロア」）およびデータハイウェイ 105 によって通信可能に接続されるバックエンド環境（例えば、サーバ 12）を含むことに留意されたい。図 1 に示すように、フィールド環境は、その内部に配設され、設置され、および相互接続されて、ランタイム中にプロセスを制御するように動作する物理的構成要素（例えば、プロセス制御デバイス、ネットワーク、ネットワーク素子、等）を含む。例えば、コントローラ 11、I/O カード 26、28、フィールドデバイス 15～22、および他のデバイスおよびネットワーク構成要素 40～46、35、52、55、58 および 70 は、プロセスプラント 10 のフィールド環境内に位置付けられるか、配設されるか、さもなければ他の方法で含まれる。一般的に言って、プロセスプラント 10 のフィールド環境においては、その中に配設された物理的構成要素を使用して原料が受領されて処理され、1 つ以上の製品を生成する。

【0037】

プロセスプラント 10 のバックエンド環境は、フィールド環境の過酷な状況および材料から遮蔽および／または保護された様々な要素、例えばコンピューティングデバイス 12、オペレータワークステーション 8、データベースまたはデータバンク等を含む。図 1 を参照すると、バックエンド環境は、例えば、オペレータワークステーション 8、サーバコ

ンピューティングデバイス 12、および／またはプロセスプラント 10 のランタイム動作をサポートする機能を含む。いくつかの構成では、プロセスプラント 10 のバックエンド環境に含まれる様々なコンピューティングデバイス、データベース、および他の要素および機材は、異なる物理位置に物理的に位置し得、それらのいくつかは、プロセスプラント 10 に対してローカルであってもよく、それらのいくつかは遠隔していてもよい。

【0038】

図 2 は、プロセスプラント 10 の例示的なセキュリティアーキテクチャ 200 のブロック図を含む。図 2 に示すように、1 つ以上のデバイス 202 は、例えば図 1 の無線ゲートウェイ 35 のインスタンスであり得る 1 つ以上の無線ゲートウェイ 205 A、205 B に通信可能に接続される。ゲートウェイ 205 A、205 B とデバイス 202 との間の通信接続は、参照番号 204 A、204 B で示されている。

10

【0039】

デバイス 202 のセットは、有限数の無線フィールドデバイスを含むものとして示されている。ただし、デバイス 202 に関して本明細書に記載する概念および特徴は、プロセスプラント 10 の任意の数のフィールドデバイス、および任意のタイプのフィールドデバイスに容易に適用できることが理解される。例えば、フィールドデバイス 202 は、プロセスプラント 10 の 1 つ以上の有線通信ネットワークを介して無線ゲートウェイ 205 A、205 B に通信可能に接続される 1 つ以上の有線フィールドデバイス 15 ~ 22 を含むことができ、および／またはフィールドデバイス 202 は、無線アダプタ 52 A、52 B に連結された有線フィールドデバイス 48、50 を含むことができる。

20

【0040】

さらに、デバイス 202 のセットは、フィールドデバイスのみ限定されず、プロセスプラント 10 がオンラインプロセスを制御するプロセスプラント 10 の結果としてデータを生成するプロセスプラント 10 内の任意のデバイスまたはコンポーネントを、加えてまたは代わりに含み得ることが理解される。例えば、デバイス 202 のセットは、診断データを生成する診断デバイスまたはコンポーネント、プロセスプラント 10 の様々なコンポーネント間で情報を送信するネットワークルーティングデバイスまたはコンポーネント等を含み得る。実際、図 1 に示すコンポーネント（例えば、コンポーネント 7 a ~ 7 c、8、11、12、15 ~ 22、26、28、35、40 ~ 46、52、55、58、60、および 70）および図示しない他のコンポーネントのいずれもが、リモートシステム 210 に配信するためのデータを生成するデバイスであってもよい。したがって、デバイス 202 のセットは、本明細書では「データソース 202」または「データソースデバイス 202」と言い換え可能である。

30

【0041】

図 2 は、プロセスプラント 10 のために利用され得る、および／またはプロセスプラント 10 が利用する、リモートアプリケーションまたはサービス 208 のセットをさらに示す。リモートアプリケーションまたはサービス 208 のセットは、1 つ以上のリモートシステム 210 で実行またはホストされてもよい。リアルタイムデータがプロセスプラント 10 によって生成され、かつアプリケーションまたはサービス 208 によって受信されると、アプリケーションまたはサービス 208 のうちの少なくともいくつかは、リアルタイムデータ上でリアルタイムで動作する。他のアプリケーションまたはサービス 208 は、より厳格でないタイミング要件を伴う、プロセスプラントで生成されたデータに対して、動作し、または実行され得る。リモートシステム 210 で実行またはホストされ、かつプロセスプラント 10 によって生成されたデータのコンシューマであるアプリケーション／サービス 208 の例として、プロセスプラント 10 で発生する条件および／またはイベントを監視および／または検知するアプリケーションと、プロセスプラント 10 で実行されているオンラインプロセス自体の少なくとも一部を監視するアプリケーションまたはサービスと、が挙げられる。アプリケーション／サービス 208 の他の例として、記述的および／または規範的分析が挙げられ、これはプロセスプラント 10 によって生成されたデータに対して動作し、場合によっては、プロセスプラントで生成されたデータの分析から収

40

50

集または発見された知識に対して、さらには他のプロセスプラントによって生成され、および他のプロセスプラントから受信したデータに対して、動作し得る。アプリケーション／サービス 208 のさらに他の例は、例えば別のサービスまたはアプリケーションの結果としてプロセスプラント 10 に実装される規範的な機能および／または変更を実装する 1 つ以上のルーチンを含む。アプリケーションおよびサービス 208 の他の例は、プロセスプラントおよび／または他のプロセスプラントによって生成された履歴データの分析から、またはプロセスプラントエンティティのデータを同じまたは同様のタイプのデータプロセスプラントエンティティと比較することから収集した知識に対して動作する。

【0042】

1 つ以上のリモートシステム 210 は、ネットワークサーバのリモートバンク、1 つ以上のクラウドコンピューティングシステム、1 つ以上のネットワーク等によって、任意の所望の態様で実装され得る。説明を簡単にするために、本明細書では、単数形を使用して 1 つ以上のリモートシステム 210、すなわち「リモートシステム 210」を指すが、該用語は 1 つのシステム、複数のシステム、または任意の数のシステムを指し得ることが理解される。いくつかのシナリオでは、プロセスプラントデータを分析するコンピューティングデバイス 250 がリモートシステム 210 内に含まれてもよい。

【0043】

一般的に言って、セキュリティアーキテクチャ 200 は、デバイス 202 がインストールされて動作するプロセスプラント 10 のフィールド環境から、プロセスプラント 10 によって生成されたデータを消費し、およびデータに対して動作するアプリケーションおよび／またはサービス 208 を提供するリモートシステム 210 へ、エンドツーエンドセキュリティを提供する。したがって、サイバー攻撃、侵入、および／またはその他の悪意のあるイベントからプラント 10 を保護しながら、デバイス 202 およびプロセスプラント 10 の他のコンポーネントによって生成されたデータを、リモートアプリケーション／サービス 208 が使用するためにリモートシステム 210 に安全に転送することができる。特に、セキュリティアーキテクチャ 200 は、フィールドゲートウェイ 212 と、プロセスプラント 10（例えば、プロセスプラント 10 の無線ゲートウェイ 205 A、205 B 間）とリモートシステム 210 との間に配設されたエッジゲートウェイ 218 を含む。

【0044】

プロセスプラント 10 から出て、入力ポート 220 から出力ポート 222 へ送信されるデータは、暗号化によってさらに保護されてもよい。一例では、フィールドゲートウェイ 212 はデータを暗号化し、暗号化されたデータを入力ポート 220 へ配信する。暗号化されて転送されるデータトラフィックは、ある例では UDP (User Datagram Protocol、ユーザデータグラムプロトコル) データトラフィックであってもよく、別の例では JSON データトラフィックまたはその他の汎用通信フォーマットであってもよい。

【0045】

フィールドゲートウェイ 212 は、プロセス制御プラント 10 に通信可能に接続する。図 2 に示すように、フィールドゲートウェイ 212 は、プロセスプラント 10 のフィールド環境内に配設され、かつ 1 つ以上のデバイスまたはデータソース 202 に通信可能に接続された、ワイヤレスゲートウェイ 205 A、205 B に通信可能に接続されている。前述のように、デバイスまたはデータソース 202 およびワイヤレスゲートウェイ 205 A、205 B は、1 つ以上のセキュリティメカニズムを介して安全な通信を提供するように構成された、無線 HART 産業用プロトコルまたは他の好適な無線プロトコルを使用して通信してもよい。例えば、無線 HART 産業用プロトコルは 128 ビット AES 暗号化を提供し、それに応じて通信パス 204 A、204 B が保護され得る。

【0046】

加えて、無線ゲートウェイ 205 A、205 B とフィールドゲートウェイ 212 との間の通信接続 225 は、通信接続 204 A、204 B に利用されるのと同じまたは異なるセキュリティメカニズムを使用してそれぞれ保護される。一例では、通信接続 225 は、T

10

20

30

40

50

L S (T r a n s p o r t L a y e r S e c u r i t y、トランスポート層セキュリティ) ラッパによって保護される。例えば、無線ゲートウェイ 205 A、205 B は、フィールドゲートウェイ 212 への中継のために T L S ラッパによって保護される H A R T - I P フォーマットの packets を生成する。

【0047】

したがって、上記のように、実施形態では、デバイス 202 によって生成されたデータまたは packets は、第 1 のセキュリティメカニズムを使用して、無線ゲートウェイ 205 A、205 B への中継 204 A、204 B のために保護され、その後、第 2 のセキュリティメカニズムを使用して、無線ゲートウェイ 205 A、205 B からフィールドゲートウェイ 212 への中継 225 のために保護され、さらにその後、第 3 のセキュリティメカニズムを使用して、エッジゲートウェイ 218 への中継のために保護され得る。加えてまたは代わりに、図 2 に示すように、エッジゲートウェイ 218 はファイアウォール 228 に

10

【0048】

エッジゲートウェイ 218 からリモートシステム 210 へ移行するデータは、プライベートエンタープライズネットワーク、インターネット、セルラルータ、バックホールインターネットまたは他のタイプのバックホール接続等の 1 つ以上のパブリックおよび／またはプライベートネットワークを使用して配信され得る。重要なことには、エッジゲートウェイ 218 からリモートシステム 210 へ移行するデータは、第 4 のセキュリティメカニズムを使用することによって、または前述のセキュリティメカニズムのうちの 1 つを使用することによって、保護される。図 2 は、リモートシステム 210 で提供されるトークンサービス 230 を通じて管理され得る S A S (共有アクセス署名) トークンを介して保護されるものとして、エッジゲートウェイ 218 からリモートシステム 210 へ配信されるデータトラフィックを示す。エッジゲートウェイ 218 は、トークンサービス 230 に対して認証を行い、S A S トークンを要求するが、これは、例えば 2 分、5 分、30 分、1 時間以下等の限られた期間のみ有効であり得る。エッジゲートウェイ 218 は、S A S トークンを受信および使用して、コンテンツデータがエッジゲートウェイ 218 からリモートシステム 210 へ送信されるリモートシステム 210 への A M Q P (A d v a n c e d M e s s a g e Q u e u i n g P r o t o c o l、アドバンスドメッセージキューイングプロトコル) 接続を保護および認証する。

20

30

【0049】

リモートシステム 210 では、ドメイン認証サービス 232 を介してセキュリティが提供される。したがって、ドメイン認証サービス 232 を介して認証および認可されたユーザインターフェースデバイス 235 のみが、とりわけ、デバイス 202 によって生成されるデータを含む、リモートシステム 210 で利用可能なデータの少なくとも一部へのアクセスを達成することができる。

【0050】

したがって、上述のように、セキュリティアーキテクチャ 200 は、プロセスプラント 10 でプロセスを制御するように動作しながら、デバイスまたはデータソース 202 によって生成されたデータへエンドツーエンドセキュリティを提供し、例えばデータソース 202 によるデータの開始からリモートシステム 210 へのその送信は、1 つ以上のリモートアプリケーションまたはサービス 208 によって有効化される。重要なことに、セキュリティアーキテクチャ 200 は、プロセスプラント 10 で悪意のある攻撃が発生するのを防止しながら、このエンドツーエンドのセキュリティを提供する。

40

【0051】

図 2 は、デバイスまたはデータソース 202 をフィールドゲートウェイ 212 に通信可能に接続するものとしてワイヤレスゲートウェイ 205 A、205 B を示しているが、いくつかの構成では、ワイヤレスゲートウェイ 205 A、205 B のうちの 1 つ以上が省略され、ソースデータがデータソース 202 からフィールドゲートウェイ 212 へ直接送信されることに留意されたい。例えば、データソース 202 は、プロセスプラント 10 のビ

50

ッグデータネットワークを介してフィールドゲートウェイ 212 へソースデータを直接送信してもよい。一般的に言って、プロセスプラント 10 のビッグデータネットワークは、バックボーンプラントネットワーク 105 ではなく、産業用通信プロトコルネット（例えば、Profibus、DeviceNet、Foundation Fieldbus、ControlNet、Modbus、HART 等）を使用してデバイス間で制御信号を送信するために使用される産業用プロトコルネットワークのビッグデータネットワークでもない。むしろ、プロセスプラント 10 のビッグデータネットワークは、例えば、データ処理および分析目的でノード間でデータをストリーミングするプロセスプラント 10 用に実装されたオーバーレイネットワークであり得る。ビッグデータネットワークのノードは、例えば、データソース 202、ワイヤレスゲートウェイ 205A、205B、およびフィールドゲートウェイ 212、ならびに、図 1 に示すコンポーネント 7a~7c、8、11、12、15~22、26、28、35、40~46、52、55、58、60、および 70 のいずれか 1 つ以上および他のコンポーネントを含み得る。したがって、プロセスプラントデータネットワークの多くのノードは、それぞれ、産業用通信プロトコルを通常利用するプロセスプラント動作の専用インターフェースと、例えばストリーミングプロトコルを利用し得るデータ処理／分析動作の別の専用インターフェースを含む。

【0052】

図 2 に関して、いくつかの実施形態では、無線ゲートウェイ 205A、205B の一方の代わりに有線ゲートウェイ（図示せず）を利用できることにさらに留意されたい。またさらに、図 2 に示すボックス 235 で示すように、フィールドゲートウェイ 212 およびエッジゲートウェイ 218 を物理的に同じ場所に配置してもよく、コンポーネント 212 および 218 を複数の場所にわたって物理的に配置してもよい。例えば、フィールドゲートウェイ 212 またはエッジゲートウェイ 218、のうちの 1 つ以上をプロセスプラント 10 に配設してもよい。加えてまたは代わりに、フィールドゲートウェイ 212 またはエッジゲートウェイ 218、のうちの 1 つ以上は、プロセスプラント 10 から遠隔に配設されてもよい。

【0053】

プロセスプラント 10 は、必要に応じて複数のフィールドゲートウェイ 212 によってサービスされてもよく、任意の数のフィールドゲートウェイ 210 が単一のエッジゲートウェイ 218 によってサービスされてもよい。いくつかの実施形態では、必要に応じて、リモートシステム 210 は複数のエッジゲートウェイ 218 によってサービスされる。

【0054】

上記の例は、リモートシステム 210 のコンポーネントとしてプロセスプラントデータを分析するためのコンピューティングデバイス 250 に言及しているが、コンピューティングデバイス 250 は、安全な状態で任意の好適な通信コンポーネントと通信することによってプロセスプラントデータを受信してもよい。例えば、コンピューティングデバイス 250 は、無線ゲートウェイ 205A、205B、フィールドゲートウェイ 212、またはエッジゲートウェイ 218 に通信可能に接続されてもよい。通信パスは、暗号化技術、ファイアウォール、データダイオードを介して、または他の好適なセキュリティメカニズムを使用して、デバイス 202 からコンピューティングデバイス 250 まで保護されてもよい。

【0055】

プロセスプラントデータがコンピューティングデバイス 250 で受信されると、コンピューティングデバイスはプロセスプラントデータを分析して、対応するプロセスプラントエンティティの状態を識別する。次いで、条件の表示は、例えば、ドメイン認証サービスを介してユーザインターフェースデバイス 235 へ送信される。このようにして、オペレータは、プロセスプラント内の様々なプロセスプラントエンティティで発生する状態を閲覧し得る。次いで、オペレータは、これらの条件によって作成された問題を解決するために適切なアクションを実行してもよい。

【0056】

10

20

30

40

50

プロセス制御システムにおける分散型台帳アーキテクチャ

プロセスプラント10は、単一のエッジゲートウェイ218を含むものとして図2に示されているが、プロセスプラント10は、それぞれが分散型台帳ネットワーク内の検証ノードとして機能するいくつかのエッジゲートウェイを含んでもよい。図3は、プロセスプラントデータを記録するための例示的な分散型台帳システム300を示す。プロセスプラントデータは、プロセスパラメータデータ、製品パラメータデータ、構成データ、ユーザインタラクションデータ、保守データ、試運転データ、プラントネットワークデータ、製品追跡データ、アラーム、リーク、障害、エラー等のプロセスプラント10内のイベントに関連するイベントデータ、または1つまたはいくつかのプロセスプラントで生成される、またはプロセスプラントに関連する任意の他の好適なデータを含み得る。

10

【0057】

システム300は、分散型台帳312と、エッジゲートウェイ218等のプロセスプラント10内のエッジゲートウェイであり得るか、フィールドデバイスであり得るか、またはプロセスプラント10または他のプロセスプラントで動作する任意の好適なコンピューティングデバイスであり得る、複数のノード302、304、306、308、および310と、を含む。各ノードは、分散型台帳312のコピーを保守する。分散型台帳312に変更が加えられると、各ノードはネットワーク314を介して変更を受信し、各ノードの、分散型台帳312のそれぞれのコピーを更新する。合意メカニズムは、分散型台帳システム300内のノード302～310によって使用され、分散型台帳312に対して受信した変更を行うことが適切かどうかを決定してもよい。

20

【0058】

したがって、システム内の各ノードは、分散型台帳312の独自のコピーを有し、これはその他のノードによって記憶された分散型台帳312の他の全てのコピーと同一である。分散型台帳システム300は、分散型台帳の分散化された性質のため、中央当局データベースシステムよりも堅牢であり得る。したがって、集中型システムに存在するような分散型台帳システム300には単一障害点は存在しない。

【0059】

図4は、トランザクションを解決するための例示的な検証ネットワークノード、および分散型台帳ネットワーク上の例示的なトランザクションフロー400を示す。図4は、それぞれ点線の左側および右側で表される2つの時間フレーム420および422、ノードA402およびノードB404（プロセスプラント10内の2つのエッジゲートウェイであってもよく、同じまたは異なるプロセスプラント内の2つのエッジゲートウェイであってもよい、等）、トランザクションのセット408A～408Dのセット、トランザクション409A～409Dのブロックのセット、分散型台帳410、およびブロックチェーン418を含む。

30

【0060】

ブロック伝播フロー400は、ノードA402が時間420でトランザクション406を受信することで開始し得る。ノードA402が、トランザクション406が有効であることを確認すると、ノードA402は、トランザクションを新たに生成されたブロック408に追加し得る。ブロック408にトランザクション406を追加することの一部として、ノードA402が暗号パズルを解き、ブロック408を生成するために行われた作業の証明として新たに生成されたブロック408に解を含めてもよい。代わりに、ブルーフオブステークアルゴリズムを使用してブロック408を生成してもよく、それによりノードA402はネットワーク上で使用されるデジタルトークンの量を「ステーク」するが、ネットワーク自体が新たなブロックを作成するノードを決定する。他の実施形態では、ブロックを形成するのに十分な数のトランザクションがプール内に存在するまで、トランザクション406をトランザクションのプールに追加してもよい。ノードA402は、新たに作成されたブロック408を時間412にネットワークへ送信してもよい。ブロック408を伝播する前または後に、ノードA402は、ノードA402の、ブロックチェーン418のコピーに、ブロック408を追加してもよい。

40

50

【0061】

作業の証明およびステークの証明は、新たなブロックを作成するためのノードを選択するための合意アルゴリズムとして本明細書に記載されているが、これらはほんの数例の合意アルゴリズムであり、限定することは意図されていない。デリゲートされたステークの証明などの、追加の合意アルゴリズムを利用してもよく、この場合に、例えば、ノードが、検証を実行するためにデリゲートと称されるノードのサブセットを選択し、デリゲートが、交代で新たなブロックを作成する。合意アルゴリズムとしてまた、権限証明、重量証明、ビザンチンフォールトトレランス、もつれ合意アルゴリズム、ブロック格子合意アルゴリズム等が挙げられ得る。

【0062】

いずれにしても、トランザクション409A～409Dは、状態データベース416の更新を含み得る。状態データベース416は、ブロックチェーン418上に展開されたスマートコントラクトによって作成された変数の現在の値を含み得る。ブロック408等の検証されたブロックは、状態データベース416内の状態変数に影響を与えるトランザクションを含み得る。時間422で、ノードB404は、412でネットワークを介して、新たに作成されたブロック408を受信し得る。ノードB404は、ブロック408で提供される暗号パズルの解をチェックすることによって、トランザクションのブロック408が有効であることを確認し得る。解が正確な場合、ノードB404は、ブロック408をそのブロックチェーン418に追加し、ブロック408のトランザクションによって拒否された状態データベース416に更新を行い得る。ノードB404は、次いで、時間314でブロック408をネットワークの残りへ送信し得る。

【0063】

図5は、プロセスプラントデータを記録するための分散型台帳ネットワーク上の検証ネットワークノード500の例示的な構成要素を示す。ノード500は、少なくとも1つのプロセッサ502、メモリ504、通信モジュール506、アプリケーション508のセット、外部ポート510、ブロックチェーンマネージャ514、スマートコントラクト516、およびオペレーティングシステム518を含み得る。いくつかの実施形態では、ノード500は、トランザクションの新たなブロックを生成してもよく、またはブロックチェーンマネージャ514を使用することによって、他のネットワークノードにトランザクションをブロードキャストしてもよい。同様に、ノード500は、メモリ504に記憶されたスマートコントラクト516とともにブロックチェーンマネージャ514を使用して、本明細書で開示される機能を実行し得る。メモリ504は、例えば、その上に展開されたスマートコントラクトの状態を記憶するためのブロックチェーンの状態データベースを含むチェーンデータ524をさらに含み得る。

【0064】

他の実施形態では、スマートコントラクト516は、ブロックチェーンマネージャ514または他のアプリケーションとは独立して動作する。いくつかの実施形態では、ノード500は、ブロックチェーンマネージャ514、またはノードに記憶されたスマートコントラクト516を有さない。いくつかの実施形態では、ノード500は、記載されているよりも多いまたは少ないコンポーネントを有し得る。ノード500の構成要素は、以下により詳細に説明される。

【0065】

ノード500は、分散型台帳システム300または別の分散型または集中型ネットワークの一部として、1つまたはいくつかのプロセスプラントで発生するデータまたはイベントに関連付けられたトランザクションとインタラクションし、および／またはトランザクションを操作するシステムの一部として使用され得る。

【0066】

図6Aは、プロセス制御システム内のトランザクションのブロック602～608を有するブロックチェーンを含む例示的な分散型台帳600を示す。いくつかの実施形態では、ブロックチェーン600は、互いに接続されてトランザクションのブロック602～6

10

20

30

40

50

08のチェーンを形成するいくつかのブロック602～608を含む。ブロックおよびトランザクションを暗号でリンクするために、ブロックチェーン600の各ブロックは、そのトランザクションをマークルツリーに編成する。マークルツリーでは、各トランザクションが暗号ハッシュアルゴリズム（例えば、SHA-256）に従ってハッシュされ、次いで、結果の出力ハッシュが別のトランザクションのハッシュと結合される。次に、暗号ハッシュアルゴリズムに従って、結合された結果もハッシュされる。次に、この出力は2つの他のトランザクションのハッシュと結合され、ブロック内のトランザクションの全てが結合およびハッシュされるまでこのプロセスが繰り返され、ブロック602～608のヘッダで使用されるマークルルートを生成する。ブロック内の任意の単一のトランザクションが改ざんされる場合、マークルルートはブロック内の全てのトランザクションのハッシュの組み合わせであるため、異なるマークルルートが生成される。

10

【0067】

言い換えれば、トランザクションは、前述のアルゴリズム等の暗号ハッシュアルゴリズムを使用してハッシュされ、各トランザクションのハッシュはツリーに記憶され得る。ツリーが構築されると、同じレベルにある各隣接ノードのハッシュがまとめてハッシュされて、ツリー内のより高いレベルに存在する新しいノードを作成する。したがって、ツリーの最上位にあるノードまたはマークルルートは、ツリーの下に記憶されている各トランザクションのハッシュに依存する。各トランザクションはデータのセットを含み得る。データのセットは、トランザクションのデータの識別、およびトランザクションの性質とトランザクションに伴う内容とを識別するトランザクションデータ（例えば、入力および出力アドレス、トランザクション値、ドキュメントハッシュ値、タイムスタンプ、トランザクション料金値等）を含み得る。

20

【0068】

ブロックが有効であることを確認するために、ノードは、ブロックのマークルルート、ブロックチェーンの他のノードのコピーに含まれる同じブロックのマークルルートと比較し得る。したがって、マークルルート、ブロックに含まれるトランザクションの証明として、またブロックの各ノードのコピーでマークルルートが同じ場合にブロックの内容が改ざんされていないことの証明として使用することができる。

【0069】

一実装形態では、ブロックチェーン「上に」記憶されるドキュメントは、暗号ハッシュアルゴリズム（例えば、SHA-256）に従ってハッシュされたドキュメントであり、結果の出力ハッシュは、ブロックチェーンの合意ルールを満たすネットワークノードによって受け入れられている。したがって、ドキュメントのハッシュを、ブロックチェーンに記憶されているハッシュと比較することによって、ドキュメントを後で確認または検証され得る。例えば、ドキュメントのセットが、特定の日付にブロックチェーン上に記録されたSHA-256ハッシュをもたらす場合、次いでブロックチェーンはその日付の時点でドキュメントが存在したという暗号証明を提供する。

30

【0070】

ドキュメントをブロックチェーン上に記憶する1つの方法は、ドキュメントのハッシュを含むトランザクションをネットワークにブロードキャストすることであり、トランザクションは、ネットワークの合意ルールの全てを満たす場合にブロックに含まれる。いくつかの実装形態では、ブロックチェーンは許可された台帳であり、認可されたネットワーク参加者のみがトランザクションをブロードキャストし得ることを意味する。他の実装形態では、一部の認可されたネットワーク参加者のみが特定のトランザクションを実行し得る。例えば、プロセスプラント10で生成された製品の特性を示す製品パラメータデータは、フィールドデバイスが製品の特性（例えば、製品の温度、製品の体積、製品の質量、製品の密度、製品の圧力等）を決定するときに、フィールドデバイスによってブロックチェーン600にアップロードされ得る。チェーン外の当事者によって取得された場合でもブロックチェーンを使用してデータが検証され得るように、データの暗号ハッシュのみをブロックチェーン600に含めてもよい。

40

50

【0071】

ネットワークノードの検証は、署名されたトランザクションまたは署名されたメッセージが、測定値を収集するフィールドデバイスが所有する公開された公開暗号鍵に対応する秘密暗号鍵によって署名されたことを確認し得る。少なくとも1つの実装形態では、ブロックチェーンネットワークによって合意ルールとして有効なアイデンティティ証明が適用され得る。したがって、新たな製品パラメータデータを追加することを認可されたアイデンティティと一致する暗号のアイデンティティ証明なしで新たな製品パラメータデータを追加しようとするいずれのトランザクションも、合意ルールに準拠していないとしてネットワークによって拒否される。プロセスプラント10内の各フィールドデバイスには、フィールドデバイスに対応するものとしてブロックチェーンネットワーク内で識別される公開鍵／秘密鍵のペアを割り当てられ得る。加えて、各フィールドデバイスは、特定のタイプの測定値を収集することを認可され得る。例えば、第1のフィールドデバイスは製品の温度測定値を収集することを認可され、また第2のフィールドデバイスは製造された製品の体積を示す体積測定値を収集することを認可され得る。検証ネットワークノードが、認可されたフィールドデバイスからではない、またはフィールドデバイスが収集することを認可されていないタイプの測定を含む製品パラメータデータに関するトランザクションを受信する場合、検証ネットワークノードはトランザクションを拒否する。

10

【0072】

図6Bは、図6Aに記載したアーキテクチャとは異なるアーキテクチャを含む、別の例示的な分散型台帳650を示す。図6Bの分散型台帳650は、図6Aの分散型台帳600と同様に、プロセス制御システム内のトランザクションのブロック662～668を有するブロックチェーン660を含む。ブロックチェーン660は、分散型台帳650内のメインブロックチェーンと称され得る。メインブロックチェーン660に加えて、分散型台帳650は、トランザクションのブロック672～676、682～686を有する異なるプロセスプラントによって保守される複数のサイドブロックチェーン670、680またはサイドチェーンを含む。例えば、サイドチェーン670は、2つのプロセスプラント、すなわちプラントAおよびプラントBによって保守されて、2つのプロセスプラント内またはプロセスプラント間で発生するイベントに関連するトランザクションを記録し得る。これらのトランザクションは、プラントAがプラントBに製品を出荷するときに、プラントBがトークン値の形態で支払いをプラントAに送信することを含み得る。サイドチェーン680はまた、プラントCおよびプラントD内、またはプラントCとプラントDとの間で発生するイベントに関連するトランザクションを記録するために、プラントCおよびプラントDの2つのプロセスプラントによって保守され得る。これらのトランザクションは、プラントDが、特定の期間内にプラントCから受領した石油の量を記録することを含み得る。

20

30

【0073】

いくつかの実施形態では、メインブロックチェーン660は、プラントA～Dを含むいくつかのプロセスプラントおよびいくつかの他のプロセスプラントによって保守される。また、いくつかの実施形態では、サイドチェーン670、680は、メインブロックチェーン660とインタラクションして、それらのそれぞれのブロック672～676、682～686のトランザクションのうちの少なくともいくつかをメインブロックチェーン660へ提供する。このようにして、サイドチェーン670、680は、それらを保守するプロセスプラントに関連するトランザクションからのデータを含み得る。メインブロックチェーン660は、プロセスプラントの各々に関連するトランザクションからのデータを含み得る。加えて、サイドチェーン670、680は、特定のサイドチェーンを保守するプロセスプラントの外部で共有されることを意図されていないプライベートまたは機密データを含み得る。プライベートまたは機密でないサイドチェーン670からのデータはメインブロックチェーン660へ提供される一方、プライベートまたは機密データはメインブロックチェーン660へ提供されない。例えば、サイドチェーン670は、プラントAがプラントBから特定の品質基準を満たす製品を受領するとトークン値をプラントAから

40

50

プラントBに転送する、プラントAとプラントBとの間のスマートコントラクトを実行し得る。プラントAおよびBは、スマートコントラクトをメインブロックチェーン660に展開することによってスマートコントラクトの条件のうちの全てを開示したくない場合があるか、または製品の特性の各測定値をパブリックまたは大規模グループのプロセスプラントに開示されたくない場合がある。加えて、メインブロックチェーン660に、より多くのトランザクションが追加されると、メインブロックチェーン660のメモリ記憶要件が増加する。したがって、分散型台帳ネットワーク内のノードを検証して、メインブロックチェーン660からいくつかのトランザクションを記憶するためのメモリ要件を低減し得る。いずれにしても、プラントAが必要な品質基準を満たす製品をプラントBから受領したとスマートコントラクトが判定する場合、トークン値をプラントAからプラントBへ転送するトランザクションは、メインブロックチェーン660へ提供され得る。

10

【0074】

いくつかの実施形態では、メインブロックチェーン660は、任意の当事者が分散型台帳を閲覧するか、台帳に追加される新たな情報を提出するか、または検証ノードとしてネットワークに参加することができることを意味するパブリックブロックチェーンである。サイドチェーン670、680は、サイドブロックチェーンネットワークへ参加することを認可されたエンティティのグループ間でチェーンデータをプライベートに保つプライベートまたは許可されたブロックチェーンである（例えば、サイドチェーン670はプラントAとプラントBとの間でプライベートであり得る）。他の実施形態において、メインブロックチェーン660も、許可されたブロックチェーンであるが、メインブロックチェーンは、サイドチェーン670、680よりも多数の、ブロックチェーンネットワークに参加することを認可されたエンティティを有する。例えば、メインブロックチェーン660はプラントA～Dおよびいくつかの他のプロセスプラントを含む多数のプロセスプラント間でプライベートであってもよいのに対して、サイドチェーン670はプラントAとプラントBとの間でプライベートである。

20

【0075】

サイドチェーンに加えてまたは代えて、分散型台帳650は、メインブロックチェーン660の一部ではないオフチェーンを発生する他の形態のトランザクションを含み得る。例えば、プラントAおよびプラントB等の2つの当事者が支払いチャネルを開いてもよく、この場合に、プラントAとプラントBとの間で閾値量のトークンを交換する最初のトランザクションがメインブロックチェーン660へ提供される。その後、プラントAおよびプラントBは、閾値量の一部を相互に送信し、かつトランザクションのうちのいずれも、プロセスプラントのうち的一方が閾値量より多くを有する結果とならない限り、メインブロックチェーン660上に何も記録せずに相互に処理し得る。2つのプロセスプラントが相互のトランザクションを完了すると、支払いチャネルを閉じて、メインブロックチェーン660内の各プロセスプラントの最終トークン量を提供する。例えば、プラントAがプラントBへ2つのトークンを送信すると、プラントAおよびプラントBが支払いチャネルを開き得る。次いで、各プロセスプラントが1つのトークンを有するように、プラントBが1つのトークンをプラントAに送り返すことができるため、いずれのプロセスプラントも2個を超えるトークンを有しない限り、プラントBは0.5個のトークンをプラントAに送り戻す。他の実施形態では、分散型台帳650は、互いに独立して動作する別個のブロックチェーンを含む複数のブロックチェーン層を含み得る。例えば、第1のブロックチェーンレイヤは、サプライチェーンに関連するトランザクションを記録し、第2のブロックチェーンレイヤは、トークンの交換に関連するトランザクションを記録し得る。第1のブロックチェーンレイヤはパブリックである一方、第2のブロックチェーンレイヤはプライベートであり、その逆もある。

30

40

【0076】

サイドチェーンまたはオフチェーントランザクションを介してプライバシーを保護することに加えて、いくつかの実施形態では、図6Aに示すブロックチェーン600等のパブリックブロックチェーン上でプライバシーを維持し得る。例えば、ブロックチェーン600内

50

のトランザクションは、様々な暗号化技術によって、トランザクションの当事者のアイデンティティおよびトランザクション量を難読化し得る。

【0077】

図7A～図7Cは、図6Aに記載したアーキテクチャとは異なるアーキテクチャを含む、別の例示的な分散型台帳700を示す。図7A～図7Cの分散型台帳700は、複数のローカルブロックチェーン710、720を含み、各ローカルブロックチェーン710、720は、異なる当事者またはプロセスプラントによって保守される。各ローカルブロックチェーン710、720は、プロセス制御システム内のトランザクションのブロック712～716、722～726を含む。例えば、複数のプロセスプラントは、石油パイプラインからの石油、発電システムからの電気、鉄道、自動車、海上、または空輸輸送を介した製品、液体、ガス、蒸気、燃料、または材料パイプラインを介した製品、または配水システムからの水等のリソースを共有し得る。プラントAのフィールドデバイスは、パイプラインから取得した石油の量等の共有リソースに関する測定値を収集し、トランザクションで測定データをプラントAのローカルブロックチェーンにブロードキャストし得る。同様に、プラントBのフィールドデバイスは、共有リソースに関する測定値を収集し、トランザクションで測定データをプラントBのローカルブロックチェーンにブロードキャストし得る。

【0078】

図7Bに示すように、各ローカルブロックチェーン710、720からのトランザクションは、それぞれの当事者またはプロセスプラントのグローバルブロックチェーン730へ提供され、グローバルブロックチェーン730は、いくつかのプロセスプラントによって、および／またはいくつかのクラウドコンピューティングシステムを有するクラウドサービスを介して保守される。例えば、プラントAのローカルブロックチェーン710からのブロックは、プラントAのグローバルブロックチェーン730へ提供され、プラントBのローカルブロックチェーン720からのブロックは、プラントBのグローバルブロックチェーン等へ提供される。閾値期間またはエポック後に、ローカルブロックチェーンから対応するグローバルブロックチェーンへ提供され得る。このようにして、各ローカルブロックチェーンを保守する特定のプロセスプラント内のノードを検証すると、記憶要件を削減するために、最新のブロック以外のグローバルブロックチェーンへ提供されたローカルブロックチェーンからブロックを除去またはブルーニングし得る。

【0079】

図7Bに示すように、ブロックN（参照番号742）、ブロックN+1（参照番号746）、およびブロックN+2（参照番号748）は、時間エポックE（参照番号740）の間にプラントAのローカルブロックチェーン710に追加される。時間エポックEの閾値期間が終了した後、プラントAのローカルブロックチェーン710を保守する検証ノードは、ブロックN～N+2（参照番号742～746）をプラントAのグローバルブロックチェーン730へ提供する。次いで、プラントAのローカルブロックチェーン710を保守する検証ノードは、ストレージ要件を削減するために、ブロックN（参照番号742）およびブロックN+1（参照番号744）をローカルブロックチェーン710から除去またはブルーニングする。この時点でのローカルブロックチェーン710は、最新のブロックであるブロックN+2（参照番号746）のみを含む。次いで、時間エポックE+1（参照番号750）の間に、ブロックN+3（参照番号752）およびブロックN+4（参照番号754）がローカルブロックチェーン710に追加される。時間エポックE+1の閾値期間が終了した後、プラントAのローカルブロックチェーン710を保守する検証ノードは、ブロックN+3～N+4（参照番号752～754）をプラントAのグローバルブロックチェーン730へ提供する。次いで、プラントAのローカルブロックチェーン710を保守している検証ノードは、ローカルブロックチェーン710からブロックN+2～N+3（参照番号746、752）を除去またはブルーニングする。この時点でのローカルブロックチェーン710は、最新のブロックであるブロックN+4（参照番号754）のみを含む。

【0080】

図7Cに示すように、プラントA730のグローバルブロックチェーンおよびプラントB770のグローバルブロックチェーン等のグローバルブロックチェーンを保守する検証ノードは、グローバルブロックチェーン730、770を組み合わせ、状態ブロック762、764を有するスーパーブロックチェーン760を作成する。各状態ブロック762、764は、特定の期間のグローバルブロックチェーン730、770からのブロックの各々を含む。例えば、状態ブロックK（参照番号762）は、各グローバルブロックチェーン730、770からのそれぞれのブロックN、ブロックN+1、およびブロックN+2を含む。状態ブロックK+1（参照番号764）は、各グローバルブロックチェーン730、770からのそれぞれのブロックN+3、ブロックN+4、およびブロックN+5を含む。

10

【0081】

ブロックおよびトランザクションを暗号的に互いにリンクさせるために、スーパーブロックチェーン760の各状態ブロック762、764は、そのトランザクションをマークルツリーに編成する。状態ブロックブロック内の任意の単一のトランザクションが改ざんされる場合、マークルルートはブロック内のトランザクションのうちの全てのハッシュの組み合わせであるため、異なるマークルルートが生成される。各状態ブロック762、764のマークルルートは、状態ブロック762、764のヘッダに含まれる。

【0082】

ローカルブロックチェーン、グローバルブロックチェーン、およびスーパーブロックチェーンを有する、図7A～図7Cに記載された分散型台帳アーキテクチャ700は、競合するエンティティが測定データの精度を確認することを可能にする。例えば、プラントAがプラントBに、プラントAが2つのエンティティ間で共有されている石油パイプラインから30,000ガロンの石油を取得したことを報告する場合、プラントBはスーパーブロックチェーンから測定データを取り出して、この測定の精度を確認し得る。測定データはまた、測定データを含む状態ブロックのヘッダの予想されるマークルルートを計算し、状態ブロックのヘッダの実際のマークルルートを予想されるマークルルートと比較することによって、スーパーブロックチェーン760内で暗号的に検証され得る。これにより、スーパーブロックチェーン760を分析する競合エンティティが、スーパーブロックチェーン760内の状態ブロック762、764が改ざんされていないことを検証することが可能になる。

20

【0083】

プロセス制御システム内のスマートコントラクト

上述のように、プロセス制御システムは、例えば良好な状態で製品を受領するときに、価値を交換するために分散型台帳にスマートコントラクトを展開することができまる。また、スマートコントラクトを分散型台帳に展開して、フィールドデバイス等のマシンが人間の介入なしで自ら処理することを可能にし得る。

30

【0084】

図8は、プロセス制御システム内の分散型台帳ネットワークにおける例示的なスマートコントラクト状態806を示す。図8は、ブロックチェーン802、トランザクションのブロック804、および安全な書き込み要求スマートコントラクト状態806を含む。分散型台帳ネットワークまたはブロックチェーンネットワークへの参加者（例えば、プラントオペレータ、構成エンジニア、プロセス制御システム設計者等）がスマートコントラクトを展開して、例えば安全な書き込み要求のコントラクト状態806を確立し得る。展開されたスマートコントラクトは、ブロックチェーンネットワークへの他の参加者にメソッドおよびデータを公開し得る。スマートコントラクト状態のデータの一部は、スマートコントラクトのメソッドを呼び出すことによってのみ変更され得るプライベートデータ、または認可されたブロックチェーン参加者によってのみ変更され得るプライベートデータであり得る。スマートコントラクト状態を変更する1つの方法は、トランザクションを分散型台帳ネットワークへブロードキャストすることである。ブロードキャストされたトラン

40

50

ザクションが合意ルールを満たす場合、ネットワーク検証器はトランザクションをブロックに含め得る。データをスマートコントラクトへ送信するトランザクションのブロックチェーンに含めると、検証ノードがスマートコントラクトの状態データベースを更新し、したがって、ネットワーク参加者がリッチ状態メカニズムにアクセスして、安全な書き込み要求を管理し、最終的にパラメータデータを安全計装システム (s a f e t y i n s t r u m e n t e d s y s t e m、S I S) デバイスに書き込むことを可能にする。

【0085】

安全な書き込み要求スマートコントラクト状態806は、安全な書き込み要求を送信するオペレータ、安全な書き込み要求を送信するためにオペレータが使用するコンピューティングデバイス、および／または安全な書き込み要求のターゲットであるSISデバイスを識別するためのデータを含み得る。いくつかの実施形態では、オペレータは、オペレータの電子財布に割り当てられた暗号公開鍵によって識別され得る。オペレータの電子財布がオペレータのコンピューティングデバイス上で動作する場合、オペレータのコンピューティングデバイスは、オペレータと同じ暗号公開鍵によって識別され得る。他の実施形態では、オペレータのコンピューティングデバイスは、他のネットワーク参加者によって、オペレータのコンピューティングデバイスに属することが知られている他の暗号公開鍵によって識別され得る。

【0086】

いくつかの実施形態では、コントラクト所有者は、スマートコントラクトへ送信される後続のトランザクションおよびデータがID番号によってSISデバイスを識別することができるように、SISデバイスの一意のIDを選択し得る。例えば、各SISデバイスは、スマートコントラクトで異なる一意の識別子を有し得る。コントラクト所有者は、安全な書き込みの実行を認可されたオペレータおよび／またはコンピューティングデバイスの識別子を指定し得る。スマートコントラクトへ送信される後続のデータは、スマートコントラクトのオペレータおよび／またはコンピューティングデバイスを識別する公開鍵に対応する秘密鍵によって署名されたメッセージを含み、したがって、トランザクションが、認可されたオペレータおよび／または認可されたコンピューティングデバイスによって発生されたことの暗号証明を提供し得る。秘密鍵および公開鍵は、トランザクションを偽造しようとする任意の攻撃者の攻撃対象を最小限に抑えるために、オペレータ／コンピューティングデバイスによってのみ管理され得る（例えば、オペレータ／コンピューティングデバイスは、公開／秘密暗号鍵ペアをオフラインで生成し、他のネットワーク参加者へ公開鍵のみを提供する）。オペレータおよび／またはコンピューティングデバイスの秘密鍵は、安全に記憶されたシード値に従って（例えば、物理的な紙または紙の複数のコピー上に）生成されてもよく、その結果、データロスの場合に秘密鍵が回復され得る。

【0087】

パラメータデータをSISデバイスに書き込むために、安全な書き込み要求スマートコントラクト状態806は、安全な書き込み要求の証拠を取得し得る。安全な書き込み要求の証拠は、SISデバイスで変更されるパラメータの名称および／またはパラメータのパス情報を含み得る。証拠はまた、新たなパラメータ値を含んでもよく、いくつかの実施形態では、証拠は、パラメータ情報が破損していないことが損なわれていないことを確保するために、新たなパラメータ値とともに巡回冗長検査 (c y c l i c a l r e d u n d a n c y c h e c k、CRC) 値または他のエラーチェック値を含み得る。いくつかの実施形態では、パラメータ情報を受信することに応答して、スマートコントラクトは、SISデバイスの名称、SISデバイスで変更されるパラメータの名称および／またはパス、新たなパラメータ値、およびオペレータが安全な書き込み要求を確認するための確認ボタンを含む確認ダイアログを、オペレータのコンピューティングデバイスへ提供し得る。このシナリオでは、証拠は、オペレータが確認ボタンを選択したかどうかの表示を含み得る。

【0088】

オペレータおよび／またはオペレータのコンピューティングデバイスは、証拠を含むト

10

20

30

40

50

ランザクションをブロックチェーン 802 にブロードキャストし得る。証拠は、安全な書き込み要求を実行することを認可されたオペレータおよび／またはオペレータのコンピューティングデバイスから来たという暗号のアイデンティティ証明を提供するために、暗号で署名され得る。したがって、スマートコントラクトは、提供されたアイデンティティを、安全な書き込み要求を実行することを認可されたオペレータおよび／またはコンピューティングデバイスのリストと比較し得る。いくつかの実施形態では、スマートコントラクトは、提供されたアイデンティティを、安全な書き込み要求のターゲットである特定の S I S デバイスに対する安全な書き込み要求を実行することを認可されたオペレータおよび／またはコンピューティングデバイスのリストと比較し得る。

【0089】

安全な書き込み要求のスマートコントラクト状態 806 の別の態様は、スマートコントラクトデータである。スマートコントラクトデータがオブジェクトの外部から直接更新され得るか、またはスマートコントラクトデータが、スマートコントラクトのメソッドを呼び出すこと等によって、限られた方法でのみ更新され得る点で、スマートコントラクトデータは、オブジェクト指向プログラミングパラダイムに従って作成されたオブジェクトのプライベートデータおよびパブリックデータのように考えられてもよい。スマートコントラクトデータは、S I S デバイスで変更されるパラメータの名称および／またはパス、および新たなパラメータ値を含め得る。いくつかの実施形態では、スマートコントラクトデータは、パラメータ情報が破損せずに受信されたかどうかの表示を含み得る。例えば、変更されるパラメータとパラメータ情報とを含むトランザクションはまた、C R C 値または他のエラーチェック値を含み得る。スマートコントラクトは、変更されるパラメータとパラメータ情報とに基づいて予想される C R C 値を生成し、予想される C R C 値を、受信した C R C 値と比較し得る。予想される C R C 値が受信した C R C 値と一致する場合、スマートコントラクトはパラメータ情報が破損せずに受信されたと判定し得る。また、いくつかの実施形態では、スマートコントラクトデータは、安全な書き込み要求が確認されたかどうかの表示を含み得る。例えば、スマートコントラクトが、オペレータおよび／またはオペレータのコンピューティングデバイスによって、オペレータが確認ボタンを選択したことを示すトランザクションを受信した場合、スマートコントラクトは安全な書き込み要求が確認されたと判定し得る。

【0090】

例えば、図 8 に示すように、スマートコントラクトデータは、S I S デバイスをロック／ロック解除するパラメータ、S I S デバイスをロックするパラメータを設定することを表示する「1」または「ロック」のパラメータ値、安全な書き込み要求が確認されたことを示す「1」、「yes」、または「true」の確認済み値、およびパラメータ情報が損なわれていないことを示す「1」、「yes」または「true」の受信データ無破損値を含み得る。したがって、スマートコントラクトは、新たなパラメータ値を S I S デバイスへ提供すべきであると判定し得る。次に、スマートコントラクトは、パラメータ情報を S I S デバイスまたは S I S デバイスに通信可能に連結されたコントローラへ提供して、安全なデータ書き込みを実行し得る。

【0091】

いくつかの実施形態では、安全な書き込み要求のスマートコントラクトは、安全な書き込み要求を送信するオペレータおよび／またはコンピューティングデバイスが安全なデータ書き込みを実行することを認可され、パラメータ情報が損なわれておらず、かつ安全な書き込み要求が確認されるときに、ターゲット S I S デバイスまたはターゲット S I S デバイスに通信可能に接続されたコントローラへパラメータ情報を提供し得る。他の実施形態では、安全な書き込み要求のスマートコントラクトは、パラメータ情報が破損せずに受信されたかどうかを判定しない。代わりに、安全な書き込み要求のスマートコントラクトは、安全な書き込み要求を受信することに応答して、パラメータ名および／またはパラメータパス、新たなパラメータ値、および C R C 値を含むパラメータ情報の第 1 のインスタンスをターゲット S I S デバイスまたはコントローラへ提供する。安全な書き込み要求の

スマートコントラクトはまた、安全な書き込み要求の確認を受信することに応答して、パラメータ情報の第2のインスタンスをターゲットS I Sデバイスまたはコントローラへ提供する。次いで、コントローラまたはターゲットS I Sデバイスは、両方のインスタンスのパラメータ情報が同じかどうか、およびパラメータ情報が破損せずに受信されたかどうかを判定する。両方のインスタンスのパラメータ情報が同じで、パラメータ情報が破損せずに受信されると、コントローラまたはターゲットS I Sデバイスは、パラメータの新たなパラメータ値をターゲットS I Sデバイスに書き込む。

【0092】

図8は、安全な書き込み要求のためのスマートコントラクト状態806を示しているが、これは、単に説明を簡単にするための単なるスマートコントラクトの一例である。分散型台帳ネットワークへの参加者（例えば、プラントオペレータ、構成エンジニア、プロセス制御システム設計者等）は、プロセス制御に関連する任意の好適なスマートコントラクトを展開し得る。

【0093】

別の例では、障害が発生するプロセスプラント10内のデバイスのデバイス情報を取得し、かつデバイス情報を共有する要求を受信することに応答してデバイス情報をデバイスサプライヤへ提供するスマートコントラクトを展開し得る。より具体的には、プロセスプラントエンティティのようなプロセスプラント10内のデバイスに障害が発生する場合、デバイスは、分散型台帳に記憶されたスマートコントラクトのアドレスへトランザクションを送信し得る。トランザクションがデバイスから来たものであることを示す暗号のアイデンティティ証明を提供するために、暗号で署名され得る。他の実施形態では、プロセスプラントエンティティは、証拠オラクルとして機能し、かつトランザクションを生成するコントローラ、フィールドデバイス、または他のプロセス制御デバイスへ障害の表示を送信し得る。いずれにしても、トランザクションは、デバイスの識別情報、デバイスの製造元、モデル、年、デバイスの保守履歴、障害のタイプ、デバイス内の損傷部品等、デバイスのデバイス情報を含み得る。

【0094】

いくつかの実施形態では、スマートコントラクトは、保守担当者がデバイス情報をレビューするために、プロセスプラント10内の保守担当者のコンピューティングデバイスへデバイス情報を送信する。デバイス情報をレビューすると、保守担当者は、障害の詳細な調査および／または交換デバイスまたは交換部品の提供のために、デバイス情報をデバイスサプライヤがレビューする必要があると判定し得る。したがって、保守担当者のコンピューティングデバイスは、スマートコントラクトに、デバイス情報をデバイスサプライヤへ提供することを要求するトランザクションを生成し得る。トランザクションは、トランザクションが保守担当者から来たものであることの暗号のアイデンティティ証明を提供するために、暗号で署名され得る。デバイスサプライヤへデバイス情報を提供する要求が、認可された保守担当者から来たとの判定に応答して、スマートコントラクトはデバイスサプライヤのコンピューティングデバイスへデバイス情報を提供し得る。

【0095】

別の例示的なスマートコントラクトは、第1のプロセスプラントからトークン値を取得し、特定の品質基準を満たす製品が第2のプロセスプラントから第1のプロセスプラントへ移送されたと判定し、トークン値を第2のプロセスプラントへ提供するスマートコントラクトである。いくつかの実施形態では、スマートコントラクトは、第1のプロセスプラントのフィールドデバイス等の証拠オラクルから第1のプロセスプラントで製品が受領されたという表示を受信し得る。フィールドデバイスはまた、製品が品質基準を満たすかどうかを判定するためにスマートコントラクトが品質メトリックのセットと比較する、製品に関連するパラメータデータを提供し得る。製品が品質基準を満たす場合、スマートコントラクトはトークン値を第2のプロセスプラントへ提供する。それ以外の場合、スマートコントラクトは、トークン値を第1のプロセスプラントに返し得る。

【0096】

プロセス制御システム内の分散型台帳に記録されるトランザクションのタイプ

プロセス制御システムの分散型台帳は、プロセス制御に関連する多くの異なるタイプのトランザクションを含み得る。これらのトランザクションは、1) プロセスプラント10での製品の配送または受領、および配送／受領された数量に関連するトランザクション、2) オペレータワークステーション、サーバデバイス、コントローラ、I/Oデバイス、ネットワークデバイス、フィールドデバイス等、プロセスプラント10内のデバイスでのソフトウェアまたはファームウェアの更新に関連するトランザクション、3) プロセスプラント10での品質管理、生産、または規制報告に関連するトランザクション、4) プロセスプラントデータを記録するトランザクション、および5) 製品追跡データを介して管理のチェーンを記録するトランザクションを含み得る。

10

【0097】

いくつかのシナリオでは、例えばスマートコントラクト状態を変更するために、トランザクションがスマートコントラクトへ提供される。他のシナリオでは、トランザクションは、スマートコントラクトへ提供されず、1つまたはいくつかのプロセスプラントに関連する情報の安全で不変の、信頼できない記録として分散型台帳に記録されるにすぎない。

【0098】

製品の配送または受領に関連するトランザクション、および配送／受領される数量

図9は、プロセスプラント10で石油パイプラインから受領した石油の量を報告する証拠トランザクションを表す例示的な取引906を示す。図9の例示的なトランザクション906は、石油パイプラインからの石油の量を報告するが、これは単に例示を容易にするための単なる一例である。また、発電システムからの電気、鉄道、自動車、海上または空輸輸送を介した製品、液体、ガス、蒸気、燃料、または材料パイプラインを介した製品、または配水システムからの水等の、他のソースからの他の材料または製品が報告され得る。いずれにしても、トランザクション906は、証拠オラクルとして機能するフィールドデバイスによって生成され得る。フィールドデバイスがバルブを通して流れる石油を検出すると、フィールドデバイスはトランザクション906を、ブロック904等のブロックに含まれるブロックチェーン902にブロードキャストする。

20

【0099】

トランザクション906は、トランザクションIDと、プラントA内のフィールドデバイス456（暗号のアイデンティティ証明によって識別される）等の発生者と、を含み得る。トランザクション906はまた、製品に関連する識別情報、製品のプロバイダ（例えば、石油生産者）、および受領した製品の量に関する情報を含み得る。例えば、フィールドデバイスは、特定の期間（例えば、1時間、1日等）にわたってプラントAで取得された石油の量を判定し、トランザクションにその量を含める流量センサであり得る。他の実施形態では、フィールドデバイスは、一連のトランザクションの様々な期間におけるいくつかの流量を含めてもよく、時間の関数としての流量を使用して、プラントAで受領した石油の量を判定し得る。さらに、トランザクション906は、イベント、製品識別子、および製品プロバイダ識別子に関する情報の暗号ハッシュを含み得る。別の実装形態では、イベント、製品識別子、および製品プロバイダ識別子に関する情報は暗号ハッシュとして記憶されないが、オブザーバまたは他のネットワーク参加者によってブロック904で直接アクセス可能である。

30

40

【0100】

この例では、製品を受領するプロセスプラント10のフィールドデバイスはトランザクションを生成するが、プロセスプラント10または製品を提供する他のエンティティのフィールドデバイスは、トランザクションを生成し得る。このトランザクションは、製品を受領するプロセスプラント10のフィールドデバイスによるトランザクションに加えて、またはトランザクションの代わりに生成され得る。

【0101】

プロセスプラント内のデバイスでのソフトウェアまたはファームウェアの更新に関連するトランザクション

50

認可されていないソフトウェアまたはファームウェアがプロセスプラント10に導入されるのを防止するため、プロセスプラント10内のデバイスに対するソフトウェアおよびファームウェアの更新は、上述の分散型台帳等の分散型台帳にデジタルで記録され得る。分散型台帳は、更新の日時、(暗号のアイデンティティ証明を介して)更新を実行するユーザのアイデンティティ、ソフトウェアの以前のバージョンおよび/またはソフトウェアの新しいバージョンの変更を含む、プロセスプラント10内のデバイスの各ソフトウェアおよびファームウェア更新の記録を保守し得る。プロセスプラント10内のサーバデバイス12または他のコンピューティングデバイスは、連続的または定期的に(例えば、1秒に1回、1分に1回、1時間に1回、1日に1回等)、プロセスプラント10内のデバイスで稼働するソフトウェアおよびファームウェアの現在のバージョンを取得する。サーバデバイス12はまた、分散型台帳からトランザクションを取り出し、デバイス内の現在のソフトウェアまたはファームウェアを、分散型台帳に記録されたソフトウェアまたはファームウェアの最新バージョンと比較し得る。いくつかの実施形態では、分散型台帳は、ソフトウェアまたはファームウェアの新たなバージョンの暗号ハッシュを記憶し、デバイスで実行されている現在のソフトウェアまたはファームウェアを暗号ハッシュ値と比較して、ソフトウェアまたはファームウェアが改ざんされていないことを確認する。

【0102】

デバイスの現在のソフトウェアまたはファームウェアが、分散型台帳に記録されているソフトウェアまたはファームウェアの最新バージョンと一致しない場合、サーバデバイス12は、デバイスが現在のソフトウェアまたはファームウェアを実行することを防止し得る。いくつかの実施形態では、サーバデバイス12は、例えば、以前のバージョンをデバイスにダウンロードすることによって、デバイス内のソフトウェアまたはファームウェアを以前のバージョンに戻し得る。このようにして、認可されていないユーザは、プロセスプラント10で実行されているソフトウェアまたはファームウェアを改ざんすることができない。

【0103】

図10は、プロセスプラント10内のデバイス内のソフトウェアまたはファームウェア更新を報告する証拠トランザクションを表す例示的なトランザクション1006を示す。トランザクション1006は、オペレータワークステーション、別のユーザインターフェースデバイス8、サーバデバイス12、コントローラ11、I/Oデバイス26、28、ネットワークデバイス、フィールドデバイス15~22、40~46等の、更新を受信するデバイスによって生成され得る。プロセスプラント10内のネットワークデバイスは、例えば、無線ゲートウェイ35、ルータ58、無線アクセスポイント7a、55、エッジゲートウェイ、無線アダプタ52等を含み得る。

【0104】

トランザクション1006は、トランザクションIDと、John Doe(暗号のアイデンティティ証明によって識別される)等のソフトウェアまたはファームウェアを変更する発生者と、を含み得る。トランザクション1006はまた、ソフトウェアまたはファームウェアを実行するデバイスの識別情報(オペレータワークステーション1234)(暗号のアイデンティティ証明によって識別される)と、バージョン番号および更新の日時を含む記述(「2019年1月15日午前6時2分にバージョン10.3.1.4へ更新」と、を含み得る。さらに、トランザクション1006は、ソフトウェアの新しいバージョンのソフトウェア命令の暗号ハッシュを含み得る。別の実装形態では、ソフトウェアの新しいバージョンは暗号ハッシュとして記憶されないが、オブザーバまたは他のネットワーク参加者によってブロック1004で直接アクセス可能である。いくつかの実施形態では、合意ルールは、認可されたユーザのみが分散型台帳にソフトウェアまたはファームウェア更新を記録し得ることを表示する。したがって、トランザクション1006が分散型台帳にブロードキャストされるとき、発生者が、認可されたユーザである場合、検証ノードはトランザクション1006を検証する。発生者が、認可されたユーザでない場合、トランザクション1006は分散型台帳に含まれず、ソフトウェアの更新は分散型台帳に

記録されたソフトウェアの最新バージョンと一致しない。

【0105】

例示的なシナリオでは、2019年1月15日午前6時3分に、プロセスプラント10内のサーバデバイス12は、オペレータワークステーション1234で実行されるソフトウェアの状態を取得し、例えば、オペレータワークステーション1234で実行されるソフトウェア命令の暗号ハッシュを実行することによって、ソフトウェアを、分散型台帳内の新しいバージョンのソフトウェアのソフトウェア命令の暗号ハッシュと比較する。暗号ハッシュが同じである場合、サーバデバイス12は、ソフトウェアが改ざんされていないと判定する。一方、暗号ハッシュが異なる場合、サーバデバイスは、ソフトウェアが改ざんされていると判定し、オペレータワークステーション1234が現在の状態でソフトウェアを実行することを防止する。次いで、サーバデバイス12は、ソフトウェアの以前の状態をオペレータワークステーション1234にダウンロードし、オペレータワークステーション1234は、以前の状態でソフトウェアの実行を再開する。

10

【0106】

プロセスプラントでの品質管理、生産、または規制報告に関連するトランザクション

プロセスプラントは、環境保護局（Environmental Protection Agency、EPA）等の規制機関に準拠するための報告およびレコードキーピングの要件を有する。例えば、EPAは、プロセスプラント内のバルブ、ポンプ、およびコネクタ等のリークしている機器からの、漏脱性の揮発性有機化合物と有害な大気汚染物質との放出を最小限に抑えるために、リーク検出および修理（Leak Detection and Repair、LDAR）規制を公布した。規制を遵守し、かつ安全で不変の信頼できない記録を提供するために、規制データが分散型台帳に記録され得る。例えば、アラーム、エラー、リーク、修復イベント、プロセスマイルストーン、是正措置等のトリガイイベントにตอบสนองして、フィールドデバイス、コントローラ、プロセスプラントエンティティ等のプロセス制御要素が、イベントが発生した時間、イベントの期間、イベントに関連するプロセスプラントエンティティのプロセスパラメータ値、イベントに関連する製品の製品パラメータ値等、トリガイイベントからのデータを含むトランザクションを生成し得る。その後、規制データは分散型台帳に記録されるため、規制当局はデータをレビューすることができる。

20

【0107】

いくつかの実施形態では、トリガイイベントが発生すると、プロセス制御要素の1つによってトリガイイベントが検出される。次いで、プロセス制御要素は、他のプロセス制御要素にトリガイイベントを通知し、トリガイイベントに一意の識別子を割り当てる。このようにして、プロセス制御要素の各々は、トリガイイベントに関連する測定値を収集し、トランザクションを分散型台帳にブロードキャストすることができ、各トランザクションはトリガイイベントの同じ一意の識別子を含む。

30

【0108】

いくつかの実施形態では、誰でもプロセスプラント10から規制データを閲覧することができるように、規制データはパブリックブロックチェーンに記録される。他の実施形態では、規制データは、プロセスプラント10および規制機関にアクセス可能なプライベートまたは許可されたブロックチェーンに記録される。さらに他の実施形態では、規制データは、規制当局とともにプロセスプラントネットワーク内のいくつかのプロセスプラントにアクセス可能なプライベートまたは許可されたブロックチェーンに記録される。

40

【0109】

図11は、プロセスパラメータまたは製品パラメータデータを報告する証拠トランザクションを表す、例示的なトランザクション1106を示す。トランザクション1106は、バルブ、タンク、ミキサ、ポンプ、ヒータ等の、物理的材料を収容、変換、生成、または移送するプロセスの一部分に使用される、プロセスプラント10内のデバイスであり得るプロセスプラントエンティティによって生成され得る。

【0110】

50

トランザクション1106は、トランザクションIDと、製品またはプロセスパラメータ測定値を収集する発生者（ヒータY-001）と、を含み得る（暗号のアイデンティティ証明によって識別される）。トランザクション1106はまた、製品に関連する識別情報、製品パラメータデータ（例えば、製品の温度が100℃で2時間維持されている）、およびプロセスパラメータデータ（例えば、ヒータY-001の温度が120℃である）を含み得る。トランザクション1106がトリガイイベントに応答して生成される場合、トランザクション1106は、トリガイイベントの識別情報と、トリガイイベントの時間、トリガイイベントの持続時間、および／またはトリガイイベントの説明等のトリガイイベントからのイベントデータと、を含み得る。いくつかのシナリオでは、複数のプロセスプラントエンティティが、同じトリガイイベントに応答してトランザクションを生成し、相互に通信してトリガイイベントに一意の識別子を割り当てる。このようにして、分散型台帳をレビューする規制機関等の当事者は、同じトリガイイベントに関連付けられたトランザクションの各々を閲覧し得る。

【0111】

さらに、トランザクション1106は、トリガイイベントに関連するデータとともに、製品および／またはプロセスパラメータデータの暗号ハッシュを含み得る。別の実装形態では、製品パラメータデータ、プロセスパラメータデータ、およびトリガイイベントに関連する他のデータは、暗号ハッシュとして記憶されないが、オブザーバまたは他のネットワーク参加者によってブロック1104で直接アクセス可能である。

【0112】

上述のように、トリガイイベントは、アラーム、エラー、リーク、修復イベント、是正措置等を含み得る。例示的なシナリオでは、トリガイイベントは、リリーフバルブの開放によって引き起こされるプロセスプラント10内のリークであり得る。プロセス制御システム内の圧力が圧力の閾値量を超えると、リリーフバルブが開いてもよい、または、リリーフバルブが、バルブで検出された圧力の量に比例して開いてもよい。リリーフバルブが開くと、リリーフバルブまたは1つまたはいくつかの他のフィールドデバイスが、開放の時間、開放の継続時間、開放のサイズ、リリーフバルブが開いたときの圧力、リリーフバルブからリークする流体の流量、および／または流体の温度等の流体の特性、流体のタイプ等を検出し得る。いくつかの実装形態では、リリーフバルブからリークする流体の量はまた、リリーフバルブの、流量、開放のサイズ、および開放の継続時間に基づいて決定され得る。次いで、リリーフバルブおよび／または1つまたはいくつかの他のフィールドデバイスは、トリガイイベントの同じ一意の識別子、および／または、リリーフバルブの開放によって引き起こされるリークのトリガイイベントに対する同じ記述を含むトランザクション1106と同様のトランザクションを生成し得る。トランザクションの各々はまた、開放の時間、開放のサイズ、リリーフバルブの圧力、リリーフバルブからリークする流体の流量等のプロセスパラメータデータを含み得る。トランザクションはまた、流体の特性等の製品パラメータデータを含み得る。次いで、トランザクションを生成するデバイスは、エッジゲートウェイ等のノードを検証するために分散型台帳ネットワークにトランザクションをブロードキャストして、トランザクションが有効であることを確認し、分散型台帳にトランザクションを含める。

【0113】

インシデントをレビューする規制当局は、トリガイイベント識別子を有するトランザクションに含まれるイベントデータを分散型台帳から、要求および取得し得る。次いで、図2に示すコンピューティングデバイス235等の規制当局のコンピューティングデバイスは、イベントデータをユーザインターフェース上に提示し得る。他の実施形態では、分散型台帳は、イベントデータを認証する要求に응答して、規制当局のコンピューティングデバイス235へ提供されるイベントデータの暗号ハッシュを含む。イベントデータは、プロセスプラント10内のサーバデバイス12に通信可能に連結されたデータベース等の他のデータソースから取得される。次いで、規制当局のコンピューティングデバイス235は、取得したイベントデータの暗号ハッシュを計算し、取得したイベントデータの暗号ハッ

10

20

30

40

50

シュを分散型台帳からのイベントデータの暗号ハッシュと比較する。暗号ハッシュが同じである場合、規制当局のコンピューティングデバイス235は、データベースからのイベントデータが改ざんされていないと判定する。そうでない場合、規制当局のコンピューティングデバイス235は、データベースからのイベントデータが信頼できないと判定する。

【0114】

トランザクション記録プロセスプラントデータ

トリガイメントに関連するトランザクションでのプロセスパラメータデータおよび製品パラメータデータを記録することに加えて、例えばプロセスプラント10の動作の正確な記録を保守するために、トリガイメントに関連しないトランザクションにプロセスおよび製品パラメータデータを含め得る。構成データ、ユーザインタラクションデータ、保守データ、試運転データ、プラントネットワークデータ、製品追跡データ、または1つまたはいくつかのプロセスプラントで生成される、またはプロセスプラントに関連する任意の他の好適なデータ等の、他のタイプのプロセスプラントデータもトランザクションに含め得る。ユーザインタラクションデータは、例えばオペレータのワークステーションで、オペレータまたは構成エンジニアによって実行される動作を含み得る。オペレータは、ユーザインタラクションデータとしてトランザクションに含まれ得るオペレータワークステーションのユーザコントロールを介して、設定点を調整する、アラームに応答する等し得る。このようにして、競合するエンティティがプロセスプラント10で製造された製品の品質に疑問を投げかけると、プロセスプラント10は、製品に関連する分散型台帳からプロセスプラントデータを取り出し得る。次に、プロセスプラント10は、製品の製造に関与するプロセスプラントエンティティの各々の記録、製品が製造されたときのプロセスプラントエンティティのパラメータ値、製造プロセスの様々な段階での製品のパラメータ値を、製品の製造中等に発生したトリガイメント等をレビューし得る。したがって、プロセスプラント10は、特定の品質基準を満たすように製品が適切に製造されたかどうか、または製品が品質基準を満たさない原因となる異常が生産中に発生したかどうかを判定し得る。

【0115】

また、プロセスプラントデータを使用して、製品の根本原因分析を実行し得る。例えば、製品は、半減期が1か月未満であるガソリンのように、予測される貯蔵寿命を有し得る。いくつかの実施形態では、コンピューティングデバイスは、製品の製造中に分散型台帳に記録されたプロセスパラメータデータおよび製品パラメータデータを含む製品の特性に基づいて製品の貯蔵寿命を予測し得る。コンピューティングデバイスはまた、製造中の類似のコンポーネントおよび／またはプロセスパラメータデータおよび製品パラメータデータを有する類似製品の履歴データに基づいて製品の貯蔵寿命を予測し得る。より具体的には、コンピューティングデバイスは、同じタイプの製品（例えば、ガソリン）の平均貯蔵寿命に基づいて製品の貯蔵寿命を予測し得る。

【0116】

次いで、コンピューティングデバイスは、製品中のコンポーネントの品質に基づいて、予測される貯蔵寿命を平均貯蔵寿命から増減させることができる。例えば、コンポーネントは平均超、平均、または平均未満に分類され得る。コンポーネントの表示は、関連するランキングまたは品質スコアとともにデータベースに記憶され得る。第1の閾値スコアを下回る品質スコア、または第1の閾値ランキングを下回るランキングを有するコンポーネントは、平均未満として分類され得る。第1の閾値スコアを上回り、かつ第2の閾値スコアを下回る品質スコア、または第1の閾値ランキングを上回り、かつ第2の閾値ランキングを下回るランキングを有するコンポーネントは、平均として分類され得る。第2の閾値スコアを上回る品質スコア、または第2の閾値ランキングを上回るランキングを有するコンポーネントは、平均超に分類され得る。

【0117】

コンピューティングデバイスは、製品の温度、製品の体積、製品の質量、製品の密度、製品の圧力、製品の粘度、製品の化学組成等の、製品の特性に応じて、予測される貯蔵寿命をさらに増加または減少させ得る。例えば、コンピューティングデバイスは、各プロパ

ティに品質スコアを割り当て、品質スコアの各々に基づいて予測される貯蔵寿命を調整し得る。

【0118】

いくつかの実施形態では、コンピューティングデバイスは、機械学習モデルを生成して、以前の製品の実際の貯蔵寿命、以前の製品のコンポーネント、および以前の製品の特性に基づいて、製品の貯蔵寿命を予測し得る。

【0119】

さらに、製品の実際の貯蔵寿命が、予測される貯蔵寿命と異なる場合、コンピューティングデバイスは、製品に関連するプロセスプラントデータを分散型台帳から取り出して、原因を特定し得る。例えば、実際の貯蔵寿命は、製品の品質が悪いために予測される貯蔵寿命よりも短い場合がある。別の例では、実際の貯蔵寿命は、製品を望ましくない温度に加熱するプロセスプラント10内のヒータによって、予測される貯蔵寿命よりも短い場合がある。

【0120】

製品追跡データを介した管理のチェーンを記録するトランザクション

サプライチェーン内の製品の管理のチェーンの正確な記録を提供するために、製品のソースまたはサプライヤ、および製造業者、流通業者、流通施設、小売業者、および製品を購入する顧客等の、製品を取り扱ったエンティティの識別情報を含むトランザクションが生成され得る。より具体的には、トランザクションは、製品の識別情報、製品のサプライヤ／製造業者の識別情報、製品のコンポーネントの各々の製造業者／プロバイダの識別情報、製品を受領して取り扱う、サプライ内のエンティティの識別情報、製品を販売する小売業者の識別情報、および／または製品を購入する顧客の識別情報を有する、製品追跡データを含み得る。製品が1つのエンティティ（例えば、プロセスプラント）から別のエンティティ（例えば、倉庫）に配送されると、配送エンティティは、配送エンティティの識別情報、受領エンティティの識別情報、および製品が受領エンティティに移送されていることの表示を生成し得る。

【0121】

したがって、顧客等のユーザは、ユーザインターフェースデバイスを介して、製品の識別情報を使用して、分散型台帳から特定の製品に関連するトランザクションの各々を取り出し得る。次いで、ユーザインターフェースデバイスは、ユーザインターフェースを介して、製品のサプライヤまたはソース、および製造業者、流通業者、流通施設、小売業者、製品を購入する顧客等、製品を取り扱ったエンティティの表示を表示し得る。ユーザインターフェースデバイスはまた、ユーザインターフェースを介して製品のコンポーネントの表示を表示し得る。次いで、ユーザは、コンポーネントの識別情報を使用して、分散型台帳から製品の特定のコンポーネントに関連するトランザクションの各々を取り出し得る。次いで、ユーザインターフェースデバイスは、ユーザインターフェースを介して、コンポーネントのサプライヤまたはソース、および製造業者、流通業者、流通施設等のコンポーネントを取り扱ったエンティティの表示を表示し得る。

【0122】

いくつかの実施形態では、製品パッケージングは、スキャンされると製品の分散型台帳からデータを提供する、バーコードまたは無線周波数識別（radio frequency identification、RFID）タグ等の製品識別子を含み得る。例えば、ユーザがモバイルデバイスを介してバーコードまたはRFIDタグをスキャンしてもよく、次いで、モバイルデバイスが、製品のサプライヤまたはソース、および製品を取り扱ったエンティティの表示をモバイルデバイス上に提示する。

【0123】

図12は、分散型台帳を使用してプロセス制御システムにデータを記録する例示的な方法1200を表すフロー図を示す。方法1200は、プロセスプラント10内のフィールドデバイス15～22、40～46、プロセスプラント10内のコントローラ11、または、オペレータワークステーション、サーバデバイス12、ユーザインターフェースデバ

イス 8、I/O デバイス 26、28、ネットワークデバイス 35 等のプロセスプラント 10 内の別のコンピューティングデバイスによって実行され得る。

【0124】

ブロック 1202 で、プロセス制御要素に関連するデータが、フィールドデバイスから取得される。プロセス制御要素は、フィールドデバイス、コントローラ、または、バルブ、タンク、ミキサ、ポンプ、熱交換器等のプロセスプラントエンティティであり得る。データは、プロセス制御要素のパラメータのプロセスパラメータデータ（例えば、タンク充填レベル、ポンプ速度、熱交換器内の温度）等のプロセスプラントデータと、プロセス制御要素に入る、プロセス制御要素を出る、プロセス制御要素内の、および／またはプロセス制御要素によって制御される、製品の製品パラメータデータ（例えば、タンク内の流体の温度、バルブを出る流体の流量）と、を含み得る。次に、ブロック 1204 で、プロセス制御要素に関連するプロセスプラントデータを含むトランザクションが生成される。トランザクションを生成するエンティティ（例えば、フィールドデバイス）は、エンティティに固有の暗号署名でトランザクションに署名し（ブロック 1206）、エンティティが所有する公開暗号鍵等のエンティティのアイデンティティデータでトランザクションを増強する（ブロック 1208）。例えば、トランザクションは、エンティティが所有する公開暗号鍵に対応する秘密暗号鍵によって署名され得る。

10

【0125】

ブロック 1210 で、トランザクションは、分散型台帳ネットワークへの参加者へ送信される。例えば、フィールドデバイスは、トランザクションを分散型台帳ネットワークにブロードキャストし得る。エッジゲートウェイ等の検証ノードは、トランザクションが有効であることを確認し、トランザクションをトランザクションのブロックに追加し、暗号パズルを解き、ブロックを生成するために行われた作業の証明として、新たに生成されたブロックに解を含め得る。次いで、検証ノードは、分散型台帳のそれぞれのコピーに新たに生成されたブロックを含めるために、分散型台帳ネットワーク内の他の検証ノードの各々へ、新たに生成されたブロックを提供し得る。

20

【0126】

いくつかの実施形態では、検証ノードは、合意ルールのセットに対してトランザクションを確認し、トランザクションが合意ルールの各々を満たす場合にトランザクションをブロックに追加する。例えば、合意ルールは、承認されたエンティティのみが分散型台帳にトランザクションを発生し得るように、トランザクションの発生者がアイデンティティ証明を提供することを含み得る。合意ルールは、ブロックおよびトランザクションがフォーマット要件を順守し、トランザクションに関する特定のメタ情報を供給することを要求し得る（例えば、ブロックはサイズ制限未満でなければならない、トランザクションはフィールドの数を含まなければならない、等）。合意ルールを満たさないいずれのトランザクションも、トランザクションを受信するノードの検証によって無視され、トランザクションは他のノードに伝播されない。

30

【0127】

検証ノードは、プロセスプラントデータ等の分散型台帳データを有するトランザクションをブロードキャストするプロセスプラント 10 内のフィールドデバイス、コントローラ、または他のコンピューティングデバイスと通信する送受信機を含む。加えて、検証ノードは、分散型台帳に展開されたスマートコントラクトの状態を記憶する状態データベースを含む、分散型台帳のコピーを記憶するためのメモリを含み得る。さらに、検証ノードは、合意ルールのセットを分散型台帳データに適用し、分散型台帳データが合意ルールを満たす場合に分散型台帳データを検証ノードの分散型台帳のコピーに付加するプロセスデータ検証器等のアプリケーションを含み得る。

40

【0128】

図 13 は、分散型台帳を使用してプロセス制御システムでの信頼できないデータの安全な計量のための例示的な方法 1300 を表すフロー図を示す。方法 1300 は、プロセスプラント 10 内のフィールドデバイス 15～22、40～46、プロセスプラント 10 内

50

のコントローラ 11、またはオペレータワークステーション、サーバデバイス 12、ユーザインターフェースデバイス 8、I/O デバイス 26、28、ネットワークデバイス 35 等の、プロセスプラント 10 内の別のコンピューティングデバイスによって実行され得る。方法 1300 はまた、エッジゲートウェイ等の検証ノード、またはフィールドデバイスと検証ノードとの組み合わせによって実行され得る。

【0129】

ブロック 1302 で、プロセス制御要素に関連するデータがフィールドデバイスから取得される。プロセス制御要素は、フィールドデバイス、コントローラ、または、バルブ、タンク、ミキサ、ポンプ、熱交換器等のプロセスプラントエンティティであり得る。データは、プロセス制御要素のパラメータのプロセスパラメータデータ（例えば、タンク充填レベル、ポンプ速度、熱交換器内の温度）等のプロセスプラントデータと、プロセス制御要素に入る、プロセス制御要素を出る、プロセス制御要素内の、および／またはプロセス制御要素によって制御される、製品の製品パラメータデータ（例えば、タンク内の流体の温度、バルブを出る流体の流量）と、を含み得る。次いで、ブロック 1304 で、プロセス制御要素に関連するプロセスプラントデータを含むトランザクションが生成される。トランザクションを生成するエンティティ（例えば、フィールドデバイス）は、エンティティに固有の暗号署名でトランザクションに署名し、エンティティが所有する公開暗号鍵等のエンティティのアイデンティティデータでトランザクションを増強する。例えば、トランザクションは、エンティティが所有する公開暗号鍵に対応する秘密暗号鍵によって署名され得る。

【0130】

ブロック 1306 で、トランザクションはローカル分散型台帳ネットワークへの参加者へ送信される。いくつかのローカル分散型台帳が存在してもよく、この場合に、各ローカル分散型台帳は異なる当事者またはプロセスプラントによって保守される。例えば、プラント A のローカル分散型台帳ネットワークは、プラント A 内のエッジゲートウェイで構成され得る。エッジゲートウェイは、プラント A 内のイベントおよびデバイスに関連するプロセスプラントデータを含むトランザクションを記録し得る。次いで、トランザクションは、閾値期間または時間エポックに、ローカル分散型台帳に追加される。閾値期間が終了した後（ブロック 1308）、ローカル分散型台帳を保守する検証ノードは、閾値期間中に生成されたトランザクションまたはトランザクションのブロックをグローバル分散型台帳ネットワークへ提供する（ブロック 1310）。グローバル分散型台帳ネットワークは、いくつかのクラウドコンピューティングシステムを有するクラウドサービス等の、複数のプロセスプラントにわたる検証ノードを含み得る。検証ノードは、プロセスプラントごとにグローバル分散型台帳（例えば、グローバルブロックチェーン）を保守し得る。次いで、ローカル分散型台帳ネットワーク内の検証ノードは、最新のブロック以外のグローバル分散型台帳へ提供されたローカル分散型台帳からブロックを除去またはブルーニングし得る。ローカル分散型台帳の検証ノードは、ブロックを生成し、時間エポックが終了するたびにグローバル分散型台帳ネットワークにブロックをブロードキャストし、ブロックがグローバルブロックチェーンに追加されたときにブロックのローカルコピーを除去する、ことを継続し得る。

【0131】

また、いくつかの実施形態では、それぞれのエンティティまたはプロセスプラントのグローバルブロックチェーンの各々が組み合わされて、状態ブロックを有するスーパーブロックチェーンを作成する。各状態ブロックは、特定の期間または時間エポックに対応するグローバルブロックチェーンからのブロックの各々を含む。

【0132】

図 14 は、分散型台帳を使用してプロセス制御システムに品質管理、生産、または規制データを記録するための例示的な方法 1400 を表すフロー図を示す。方法 1400 は、プロセスプラント 10 内のフィールドデバイス 15～22、40～46、プロセスプラント 10 内のコントローラ 11、または、オペレータワークステーション、サーバデバイス

12、ユーザインターフェースデバイス8、I/Oデバイス26、28、ネットワークデバイス35等のプロセスプラント10内の別のコンピューティングデバイスによって実行され得る。

【0133】

ブロック1402で、品質管理に関連するトリガイイベントがプロセス制御要素によって検出される。トリガイイベントは、アラーム、エラー、リーク、修復イベント、プロセスマイルストーン、是正措置等であり得る。いくつかの実施形態では、トリガイイベントの表示は、プロセスプラント10内のフィールドデバイス、コントローラ、または他のコンピューティングデバイスへ提供される。他の実施形態では、フィールドデバイス、コントローラ、または他のコンピューティングデバイスは、トリガイイベントを検出する。

10

【0134】

いずれにしても、ブロック1404で、トリガイイベントのイベントデータが取得される。イベントデータは、トリガイイベントの一意の識別子、トリガイイベントの時間、トリガイイベントの継続期間、トリガイイベントの説明、トリガイイベントに含まれるプロセス制御要素の識別情報、トリガイされたイベントの間にプロセス制御要素によって製造されている製品の識別情報等を含み得る。次いで、ブロック1406で、イベントデータ、および／またはトリガイイベントのイベントデータの暗号ハッシュを含むトランザクションが生成される。トランザクションはまた、トランザクションの発生者の識別情報、トリガイイベント発生時の製品の製品パラメータデータ、トリガイイベント中のプロセス制御要素のプロセスパラメータデータ、またはその他の好適な情報を含み得る。いくつかの実施形態では、プロセスプラント10内のいくつかのフィールドデバイス、コントローラ、または他のコンピューティングデバイスが、トリガイイベントに関連するトランザクションを生成し得る。例えば、第1のフィールドデバイスが、トリガイイベントの時点でヒータ内の温度を含むトランザクションを生成する一方、第2のフィールドデバイスが、トリガイイベントの時点でポンプの速度を含むトランザクションを生成し得る。

20

【0135】

ブロック1408で、トランザクションは分散型台帳ネットワークへの参加者へ送信される。例えば、フィールドデバイスは、トランザクションを分散型台帳ネットワークにブロードキャストし得る。次いで、エッジゲートウェイ等の検証ノードは、トランザクションが有効であることを確認し、トランザクションをトランザクションのブロックに追加し、暗号パズルを解き、ブロックを生成するために行われた作業の証明として、新たに生成されたブロックに解を含め得る。次いで、検証ノードは、分散型台帳のそれぞれのコピーに新たに生成されたブロックを含めるために、分散型台帳ネットワーク内の他の検証ノードの各々へ、新たに生成されたブロックを提供し得る。

30

【0136】

上述のように、トランザクションは、トリガイイベントのイベントデータの暗号ハッシュ、および／またはトリガイイベントのイベントデータとトリガイイベントに関連する他のプロセスプラントデータとの組み合わせを含み得る。トランザクションを生成することに加えて、フィールドデバイスは、例えばデータベースに記憶される、イベントデータまたはトリガイイベントに関連する他のプロセスプラントデータをサーバデバイス12へ提供し得る（ブロック1410）。

40

【0137】

次いで、イベントデータを認証するために、データベースに記憶されたイベントデータは、分散型台帳に含まれる暗号ハッシュと比較される（ブロック1412）。一致する場合、イベントデータは改ざんされていない。例えば、インシデントをレビューする規制当局は、トリガイイベント識別子を有するトランザクションに含まれる分散型台帳からイベントデータの暗号ハッシュを要求および取得し得る。イベントデータは、プロセスプラント10内のサーバデバイス12に通信可能に連結されたデータベース等の他のデータソースから取得される。次いで、規制当局のコンピューティングデバイスは、取得したイベントデータの暗号ハッシュを計算し、取得したイベントデータの暗号ハッシュを分散型台帳が

50

らのイベントデータの暗号ハッシュと比較する。暗号ハッシュが同じである場合、規制当局のコンピューティングデバイスは、データベースのイベントデータが改ざんされていないと判定する。それ以外の場合、規制機関のコンピューティングデバイスは、データベースからのイベントデータが信頼できないと判定する。他の実施形態では、プロセスプラント10内のコンピューティングデバイスは、データベースに記憶されたイベントデータと分散型台帳からのイベントデータの暗号ハッシュとを取り出し、イベントデータを暗号ハッシュと比較してイベントデータを認証する。

【0138】

図15は、プロセス制御システム内のソフトウェアまたはファームウェアの状態を記録するための例示的な方法1500と、分散型台帳を使用する接続された計装と、を表すフロー図を示す。方法1500は、プロセスプラント10内のフィールドデバイス15～22、40～46、プロセスプラント10内のコントローラ11、または、オペレータワークステーション、サーバデバイス12、ユーザインターフェースデバイス8、I/Oデバイス26、28、ネットワークデバイス35等のプロセスプラント10内の別のコンピューティングデバイスによって実行され得る。

【0139】

ブロック1502で、プロセスプラント10内のデバイス上で実行されるソフトウェアまたはファームウェアの現在の状態が取得される。例えば、ソフトウェアまたはファームウェア更新を受信するプロセスプラント10内のデバイスは、ソフトウェアまたはファームウェアの新しいバージョンを取得し得る。デバイスは、オペレータワークステーション、別のユーザインターフェースデバイス8、サーバデバイス12、コントローラ11、I/Oデバイス26、28、ネットワークデバイス35、フィールドデバイス15～22、40～46等であり得る。次いで、ブロック1504で、デバイスは、ソフトウェアまたはファームウェアの現在の状態の表示を含むトランザクションを生成し得る。例えば、表示は、ソフトウェアの新しいバージョンのソフトウェア命令の暗号ハッシュであり得る。トランザクションはまた、暗号のアイデンティティ証明によって識別されたソフトウェアまたはファームウェアを変更する発生者、ソフトウェアまたはファームウェアを実行するデバイスの識別情報、更新の説明、更新の日時等を含み得る。

【0140】

ブロック1506で、トランザクションは、分散型台帳ネットワークへの参加者へ送信される。例えば、コンピューティングデバイスは、トランザクションを分散型台帳ネットワークにブロードキャストし得る。次いで、エッジゲートウェイ等の検証ノードは、トランザクションが有効であることを確認し、トランザクションをトランザクションのブロックに追加し、暗号パズルを解き、ブロックを生成するために行われた作業の証明として、新たに生成されたブロックに解を含め得る。次いで、検証ノードは、分散型台帳のそれぞれのコピーに新たに生成されたブロックを含めるために、分散型台帳ネットワーク内の他の検証ノードの各々へ、新たに生成されたブロックを提供し得る。

【0141】

いくつかの実施形態では、検証ノードは、合意ルールのセットに対してトランザクションを確認し、トランザクションが合意ルールの各々を満たす場合にトランザクションをブロックに追加する。また、いくつかの実施形態では、合意ルールは、認可されたユーザのみが分散型台帳にソフトウェアまたはファームウェア更新を記録し得ることを示す。したがって、トランザクションが分散型台帳にブロードキャストされると、発生者が認可されたユーザである場合、検証ノードはトランザクションを検証する。発生者が認可されたユーザでない場合、トランザクションは分散型台帳に含まれず、ソフトウェアの更新は分散型台帳に記録されたソフトウェアの最新バージョンと一致しない。

【0142】

いずれにしても、ブロック1508で、プロセスプラント10内のデバイス上で実行されているソフトウェアまたはファームウェアの状態が取得される。例えば、プロセスプラント10内のサーバデバイス12または他のコンピューティングデバイスは、連続的また

10

20

30

40

50

は定期的に（例えば、1秒に1回、1分に1回、1時間に1回、1日に1回等）、プロセスプラント10内のデバイスで稼働中のソフトウェアおよびファームウェアの現在のバージョンを取得し得る。次いで、サーバデバイス12で取得されたソフトウェアまたはファームウェアの状態は、分散型台帳に記憶されたソフトウェアまたはファームウェアの暗号ハッシュ値と比較されて、ソフトウェアまたはファームウェアが改ざんされていないことを確認する（ブロック1510）。ソフトウェアまたはファームウェアの状態が、分散型台帳に記憶されているソフトウェアまたはファームウェアの暗号ハッシュ値と一致する場合、ソフトウェアまたはファームウェアはデバイス上で実行を継続する（ブロック1514）。そうでない場合、サーバデバイス12は、ソフトウェアが改ざんされていると判定し、デバイスが現在の状態でソフトウェアを実行することを防止する（ブロック1512）。いくつかの実施形態では、次いで、サーバデバイス12は、ソフトウェアの以前の状態をデバイスにダウンロードし、デバイスは以前の状態でソフトウェアの実行を再開する。

【0143】

図16は、分散型台帳を使用して、プロセス制御システムでスマートコントラクトを作成するための例示的な方法1600を表すフロー図を示す。方法1600は、プロセスプラント10内のフィールドデバイス15～22、40～46、プロセスプラント10内のコントローラ11、または、オペレータワークステーション、サーバデバイス12、ユーザインターフェースデバイス8、I/Oデバイス26、28、ネットワークデバイス35等のプロセスプラント10内の別のコンピューティングデバイスによって実行され得る。

【0144】

ブロック1602で、1つまたはいくつかのプロセスプラントに関連するスマートコントラクトが生成される。例えば、スマートコントラクトは、プラントAが特定の品質基準を満たす製品をプラントBから受領すると、トークン値をプラントAからプラントBに転送し得る。プロセス制御システムにおける別の例示的なスマートコントラクトは、プラント担当者がプロセスプラント10内のSISデバイスにパラメータデータを書き込むことを可能にする安全な書き込み要求スマートコントラクトを含み得る。プロセス制御システムのさらに別の例示的なスマートコントラクトは、障害が発生しているデバイスからデバイス情報を取得し、デバイス情報を共有する要求を受信することに応答してデバイス情報をデバイスサプライヤへ提供するデバイス情報スマートコントラクトを含み得る。

【0145】

ブロック1604で、スマートコントラクトは、分散型台帳に記憶されたアドレスに展開される。展開されたスマートコントラクトは、分散型台帳ネットワークへの他の参加者にメソッドおよびデータを公開し得る。スマートコントラクト状態のデータの一部は、スマートコントラクトのメソッドを呼び出すことによってのみ変更され得るプライベートデータ、または認可された分散型台帳参加者によってのみ変更され得るプライベートデータであり得る。スマートコントラクト状態を変更する1つの方法は、トランザクションを分散型台帳ネットワークへブロードキャストすることである。ブロードキャストされたトランザクションが合意ルールを満たす場合、ネットワーク検証器は分散型台帳にトランザクションを含め得る。

【0146】

いくつかの実施形態では、エッジゲートウェイ等の検証ノードは、スマートコントラクトに包含されたコードを実行し、フィールドデバイスは、証拠オラクルとして機能し、スマートコントラクト状態を変更する証拠トランザクションを提供する。

【0147】

図17は、分散型台帳を使用してプロセス制御システム内のスマートコントラクトとインタラクションするための例示的な方法1700を表すフロー図を示す。方法1700は、プロセスプラント10内のフィールドデバイス15～22、40～46、プロセスプラント10内のコントローラ11、または、オペレータワークステーション、サーバデバイス12、ユーザインターフェースデバイス8、I/Oデバイス26、28、ネットワークデバイス35等のプロセスプラント10内の別のコンピューティングデバイスによって実

行され得る。

【0148】

ブロック1702では、プロセスプラント10内で発生するイベントからイベントデータが取得される。イベントは、プロセスプラント10によって配送される、またはプロセスプラント10で受領される製品、プロセスプラント10で製造される製品の完成、製品の特性の変更、プロセスパラメータ値の変更、アラーム、エラー、リーク、修復イベント、是正措置等のトリガイベント、SISデバイスへの書き込み要求などのユーザインタラクション、デバイス情報をデバイスサプライヤへ提供する要求、または特定の製品を受領したときのトークン値を転送する要求、またはプロセスプラント10内で発生する任意の他の好適なイベントであり得る。イベントデータは、プロセスパラメータデータ、製品パラメータデータ、構成データ、ユーザインタラクションデータ、保守データ、試運転データ、プラントネットワークデータ、製品追跡データ、または、イベントの日時、イベントの期間、イベントの説明等のイベントに関連する任意の他の好適なデータを含み得る。

10

【0149】

次いで、ブロック1704で、エンティティに割り当てられた暗号公開鍵等の、トランザクションを生成するエンティティのイベントデータおよび識別情報を含むトランザクションが生成される。トランザクションは、トランザクションを生成するエンティティの暗号のアイデンティティ証明を提供するために、暗号で署名され得る。ブロック1706で、トランザクションは、スマートコントラクトが展開される分散型台帳上のアドレスへ送信される。このようにして、エッジゲートウェイ等の検証ノードは、トランザクションに含まれるイベントデータに従ってスマートコントラクト状態を変更する。

20

【0150】

例えば、スマートコントラクトは、プラントAが特定の品質基準を満たす製品をプラントBから受領すると、プラントAからプラントBにトークン値を転送し得る。プラントA内のフィールドデバイスは、プラントAの識別情報、製品の識別情報、製品がプラントBから受領されたことの表示、および、製品の特性（例えば、製品の温度、製品の体積、製品の密度、製品の粘度、または製品の化学組成）を記述する製品パラメータデータ等の、製品の品質に関連するイベントデータを含むトランザクションを生成し得る。フィールドデバイスは、スマートコントラクトのアドレスへトランザクションを提供してもよく、検証ノードは、スマートコントラクト状態を変更して製品パラメータデータを含み得る。いくつかの実施形態では、スマートコントラクトは、製品パラメータデータに含まれる製品の特性を、製品が適切な品質基準を満たすための一連の最小閾値要件と比較する。製品が品質基準を満たす場合、スマートコントラクトはトークン値をプラントBに転送し得る。いくつかの実施形態では、プラントB内のフィールドデバイスは、プロセスパラメータデータ等の製品の品質に関連するイベントデータを含むトランザクションを生成してもよく、プロセスパラメータデータは、製品の製造に関与するプラントB内のプロセスプラントエンティティのパラメータ値を記述し、パラメータ値は、製品の製造中に収集される。

30

【0151】

本開示に記載されている技術の実施形態は、任意の数の下記の態様を、単独でまたは組み合わせのいずれかで含んでもよい。

40

【0152】

1. 分散型台帳ネットワーク上のプロセスプラント内の検証ネットワークノードであって、1つ以上のフィールドデバイスと通信するように構成された送受信機であって、各フィールドデバイスが物理的機能を実行してプロセスプラント内の産業プロセスを制御し、かつ分散型台帳データをピアネットワークノードと交換し、分散型台帳データが、プロセスプラントデータを有するトランザクションを含む、送受信機と、分散型台帳のコピーを記憶するように構成された記憶媒体と、ピアネットワークノードから受信した分散型台帳データに合意ルールのセットを適用するように構成されたプロセスデータ検証器と、を含み、プロセスデータ検証器が、分散型台帳データが合意ルールを満たす場合に、ピアネットワークノードから受信した分散型台帳データを分散型台帳のコピーに付加するようにさ

50

らに構成されている、検証ネットワークノード。

【0153】

2. ピアノードから受信した分散型台帳データが、プロセスプラントデータを有するトランザクションを生成するエンティティのアイデンティティ証明を含む、態様1に記載の検証ネットワークノード。

【0154】

3. ピアノードから受信した分散型台帳データを付加するために、トランザクション検証器が、トランザクションのブロックに基づいて暗号パズルを解き、暗号パズルの解をトランザクションのブロックに追加し、トランザクションのブロックを分散型台帳のコピーに付加し、トランザクションのブロックを分散型台帳ネットワーク内のピアネットワークノードのうちの少なくとも1つへ送信する、ように構成されている、先行態様のいずれか1つに記載の検証ネットワークノード。

10

【0155】

4. 合意ルールのセットが、トランザクションまたはトランザクションのブロックに対するフォーマット要件、ピアネットワークノードのうちのいずれが分散型台帳に次の、トランザクションまたはトランザクションのブロックを追加するかを決定するメカニズム、またはトランザクションの各々に含まれるプロセスプラントデータをハッシュする暗号ハッシュアルゴリズム、のうちの少なくとも1つを含む、先行する態様のいずれか1つに記載の検証ネットワークノード。

【0156】

5. プロセスデータ検証器が、スマートコントラクト内のコードを実行し、かつスマートコントラクトの状態データベースを更新するようにさらに構成されている、先行する態様のいずれか1つに記載の検証ネットワークノード。

20

【0157】

6. プロセスデータ検証器が、分散型台帳データが合意ルールを満たさない場合に、ピアネットワークノードから受信した分散型台帳データを無視するようにさらに構成されている、先行する態様のいずれか1つに記載の検証ネットワークノード。

【0158】

7. 検証ネットワークノードおよびピアネットワークノードが、同じプロセスプラント内のデバイスである、先行する態様のいずれか1つに記載の検証ネットワークノード。

30

【0159】

8. 検証ネットワークノードおよびピアネットワークノードが、複数のプロセスプラント内のデバイスである、先行する態様のいずれか1つに記載の検証ネットワークノード。

【0160】

9. 複数の参加者によって保守される分散型台帳を使用してプロセス制御システムにデータを記録する方法であって、コンピューティングデバイスによって、プロセスプラント内のプロセス制御要素に関連するプロセスプラントデータを取得することと、プロセスプラントデータを含むトランザクションを生成することであって、トランザクションが分散型台帳に記憶される、生成することと、分散型台帳を保守する参加者の分散型台帳ネットワークへの少なくとも1人の他の参加者へトランザクションを送信することと、を含む、方法。

40

【0161】

10. トランザクションを生成することは、トランザクションに基づいて暗号署名を生成することと、暗号署名でトランザクションを増強することと、を含む、態様9に記載の方法。

【0162】

11. データが、プロセスプラント内のフィールドデバイスから取得され、トランザクションを生成することが、フィールドデバイスのアイデンティティデータを取得することと、アイデンティティデータでトランザクションを増強することと、をさらに含む、態様9または態様10のいずれか1つに記載の方法。

50

【0163】

12. トランザクションのブロックにトランザクションを追加することと、トランザクションのブロックに基づいて暗号パズルを解くことと、暗号パズルの解をトランザクションのブロックに追加することと、トランザクションのブロックを分散型台帳ネットワークへの少なくとも1人の他の参加者へ送信することと、をさらに含む、態様9～11のいずれか1つに記載の方法。

【0164】

13. データが、製品追跡データであり、トランザクションを生成することが、プロセスプラントから別のエンティティに製品が移送されたことを表示するトランザクションを生成することを含む、態様9～12のいずれか1つに記載の方法。

10

【0165】

14. データが、製品の温度、製品の体積、または製品の化学組成、のうちの少なくとも1つを含む製品パラメータデータであり、製品パラメータデータが分散型台帳に記憶されて、製品が別のエンティティへ提供されるときに製品のパラメータデータの真正性を確認する、態様9～13のいずれか1つに記載の方法。

【0166】

15. 分散型台帳ネットワークが複数の層を含み、第1のインスタンスにおいて、分散型台帳の第1のレイヤに記憶されるトランザクションを生成することと、第2のインスタンスにおいて、分散型台帳の第2のレイヤに記憶されるトランザクションを生成することと、をさらに含む、態様9～14のいずれか1つに記載の方法。

20

【0167】

16. 分散型台帳の第1のレイヤはパブリックであり、分散レイヤの第2のレイヤはプライベートである、態様9～15のいずれか1つに記載の方法。

【0168】

17. 分散型台帳が、ブロックチェーン、もつれ、ブロック格子、または他の有向非周期グラフ、のうちの少なくとも1つである、態様9～16のいずれか1つに記載の方法。

【0169】

18. プロセスプラントデータが、製品パラメータデータ、構成データ、製品追跡データ、またはプロセスパラメータデータ、のうちの少なくとも1つを含む、態様9～17のいずれか1つに記載の方法。

30

【0170】

19. トランザクションを生成することが、プロセスプラントデータに対応する暗号ハッシュ値を含むトランザクションを生成することを含む、態様9～18のいずれか1つに記載の方法。

【0171】

20. 複数の参加者によって保守される分散型台帳を使用してプロセス制御システムにデータを記録するシステムであって、プロセスプラントに配設された1つ以上のデバイスであって、各々が物理的機能を実行して産業プロセスを制御する、プロセスプラント内に配設された1つ以上のデバイスと、プロセスプラント内で実行するコンピューティングデバイスと、を含み、コンピューティングデバイスが、1つ以上のプロセッサと、通信ユニットと、1つ以上のプロセッサおよび通信ユニットに連結され、かつ命令を記憶した非一過性コンピュータ可読媒体を含み、命令が、1つ以上のプロセッサによって実行されると、コンピューティングデバイスに、プロセスプラント内の1つ以上のデバイスに関連するプロセスプラントデータを取得させ、プロセスプラントデータを含むトランザクションを生成させ、分散型台帳内でトランザクションを検証および記録するために、分散型台帳を保守する参加者の分散型台帳ネットワークへの少なくとも1人の他の参加者へトランザクションを送信させる、システム。

40

【0172】

21. トランザクションを生成するために、命令がコンピューティングデバイスに、トランザクションに基づいて暗号署名を生成させ、暗号署名でトランザクションを増強させ

50

る、態様 20 に記載のシステム。

【0173】

22. データがプロセスプラント内のフィールドデバイスから取得され、トランザクションを生成するために、命令がコンピューティングデバイスに、フィールドデバイスのアイデンティティデータを取得させ、アイデンティティデータでトランザクションを増強させる、態様 20 または態様 21 のいずれか 1 つに記載のシステム。

【0174】

23. 命令がコンピューティングデバイスに、さらに、トランザクションのブロックにトランザクションを追加させ、トランザクションのブロックに基づいて暗号パズルを解かせ、暗号パズルの解をトランザクションのブロックに追加させ、分散型台帳ネットワークへの少なくとも 1 人の他の参加者へトランザクションのブロックを送信させる、態様 20 ~ 22 のいずれか 1 つに記載のシステム。

【0175】

24. 分散型台帳ネットワークが複数のレイヤを含み、命令がコンピューティングデバイスに、さらに、第 1 のインスタンスにおいて、分散型台帳の第 1 のレイヤに記憶されるトランザクションを生成させ、第 2 のインスタンスにおいて、分散型台帳の第 2 のレイヤに記憶されるトランザクションを生成させる、態様 20 ~ 23 のいずれか 1 つに記載のシステム。

【0176】

25. 分散型台帳の第 1 のレイヤがパブリックブロックチェーンであり、分散レイヤの第 2 のレイヤはプライベートブロックチェーンである、態様 20 ~ 24 のいずれか 1 つに記載のシステム。

【0177】

26. 分散型台帳は、ブロックチェーン、もつれ、ブロック格子、または他の有向非周期グラフ、のうちの少なくとも 1 つである、態様 20 ~ 25 のいずれか 1 つに記載のシステム。

【0178】

27. プロセスプラントデータが、製品パラメータデータ、構成データ、製品追跡データ、またはプロセスパラメータデータ、のうちの少なくとも 1 つを含む、態様 20 ~ 26 のいずれか 1 つに記載のシステム。

【0179】

28. トランザクションを生成することが、プロセスプラントデータに対応する暗号ハッシュ値を含むトランザクションを生成することを含む、態様 20 ~ 27 のいずれか 1 つに記載のシステム。

【0180】

29. 1 つ以上のプロセッサに連結され、かつ命令を記憶した非一過性コンピュータ可読メモリであって、命令が、1 つ以上のプロセッサによって実行されると、1 つ以上のプロセッサに、1 つ以上のフィールドデバイスによって生成されるプロセスプラントデータを含むトランザクションを受信させ、各フィールドデバイスが、物理的機能を実行してプロセスプラント内の産業プロセスを制御し、分散型台帳のコピーを記憶させ、受信したトランザクションに合意ルールのセットを適用させ、受信したトランザクションが合意ルールを満たす場合に、受信したトランザクションの 1 つを分散型台帳のコピーに付加させ、分散型台帳のコピーを記憶する少なくとも 1 つのピアネットワークノードへ、付加されたトランザクションを送信させる、非一過性コンピュータ可読メモリ。

【0181】

30. 受信したトランザクションが、トランザクションを生成するエンティティのアイデンティティ証明を含む、態様 29 に記載のコンピュータ可読メモリ。

【0182】

31. 受信したトランザクションの 1 つを付加するために、命令が 1 つ以上のプロセッサに、受信したトランザクションを含むトランザクションのブロックに基づいて暗号パズ

10

20

30

40

50

ルを解かせ、暗号パズルの解をトランザクションのブロックに追加させ、トランザクションのブロックを分散型台帳のコピーに付加させ、トランザクションのブロックをピアネットワークノードへ送信させる、態様 29 または 態様 30 のいずれか 1 つに記載のコンピュータ可読メモリ。

【0183】

32. 合意ルールのセットが、トランザクションまたはトランザクションのブロックに対するフォーマット要件、ピアネットワークノードのうちのいずれが分散型台帳に次の、トランザクションまたはトランザクションのブロックを追加するかを決定するメカニズム、またはトランザクションの各々に含まれるプロセスプラントデータをハッシュする暗号ハッシュアルゴリズム、のうちの少なくとも 1 つを含む、態様 29 ～ 31 のいずれか 1 つに記載のコンピュータ可読メモリ。

10

【0184】

33. 命令が 1 つ以上のプロセッサに、さらに、分散型台帳データが合意ルールを満たさない場合に、ピアネットワークノードから受信した分散型台帳データを無視させる、態様 29 ～ 32 のいずれか 1 つに記載のコンピュータ可読メモリ。

【0185】

34. ピアネットワークノードが、同じプロセスプラント内のデバイスである、態様 29 ～ 33 のいずれか 1 つに記載のコンピュータ可読メモリ。

【0186】

35. ピアネットワークノードが、複数のプロセスプラント内のデバイスである、態様 29 ～ 34 のいずれか 1 つに記載のコンピュータ可読メモリ。

20

【0187】

36. 複数の参加者によって保守される分散型台帳を使用したプロセス制御システムでの信頼できないデータの安全な計量のための方法であって、物理的機能を実行してプロセスプラント内の産業プロセスを制御するフィールドデバイスによって、プロセスプラント内のパラメータの測定値を収集することと、コンピューティングデバイスによって、パラメータの測定値を取得することと、測定値を含むトランザクションを生成することと、ローカル分散型台帳を保守する参加者のローカル分散型台帳ネットワークへの少なくとも 1 人の他の参加者へトランザクションを送信することと、閾値期間後に、閾値期間中に生成された複数のトランザクションを、グローバル分散型台帳を保守する参加者のグローバル分散型台帳ネットワークへの少なくとも 1 人の参加者へ送信することと、を含む、方法。

30

【0188】

37. トランザクションをトランザクションのローカルブロックに追加することと、トランザクションのローカルブロックに基づいて暗号パズルを解くことと、暗号パズルの解をトランザクションのローカルブロックに追加することと、トランザクションのローカルブロックを、ローカル分散型台帳ネットワークへの少なくとも 1 人の他の参加者へ送信することと、をさらに含む、態様 36 に記載の方法。

【0189】

38. 閾値期間後に、閾値期間中に生成されたトランザクションの 1 つ以上のローカルブロックを、グローバル分散型台帳ネットワークへの少なくとも 1 人の参加者へ送信することをさらに含む、態様 36 または 態様 37 のいずれか 1 つに記載の方法。

40

【0190】

39. 閾値期間後に、閾値期間中に生成された複数のトランザクションのうちの少なくともいくつかをローカル分散型台帳ネットワークからブルーニングすることをさらに含む、態様 36 ～ 38 のいずれか 1 つに記載の方法。

【0191】

40. グローバル分散型台帳が、複数のプロセスプラントを動作させる複数のエンティティによって閲覧可能な許可されたブロックチェーンである、態様 36 ～ 39 のいずれか 1 つに記載の方法。

【0192】

50

41．パラメータが、複数のプロセスプラントを動作させる複数のエンティティ間の共有リソースに関連する、態様36～40のいずれか1つに記載の方法。

【0193】

42．グローバル分散型台帳が、複数のエンティティに対応する複数のグローバル分散型台帳を含み、各グローバル分散型台帳が、グローバル分散型台帳と同じそれぞれのエンティティのローカル分散型台帳に記憶されたトランザクションを含む、態様36～41のいずれか1つに記載の方法。

【0194】

43．閾値期間中に生成されたトランザクションについて、複数のグローバル分散型台帳の各々からのトランザクションをトランザクションの状態ブロックに追加することと、トランザクションの状態ブロックに基づいて暗号パズルを解くことと、暗号パズルの解をトランザクションの状態ブロックに追加することと、トランザクションの状態ブロックを、スーパーブロックチェーンを保守する参加者のスーパーブロックチェーンネットワークへの少なくとも1人の他の参加者へ送信することと、をさらに含む、態様36～42のいずれか1つに記載の方法。

【0195】

44．ローカル分散型台帳が、プロセスプラントを動作させるエンティティによって閲覧可能なプライベートブロックチェーンである、態様36～43のいずれか1つに記載の方法。

【0196】

45．測定値を含むトランザクションを生成することが、測定値に対応する暗号ハッシュ値を含むトランザクションを生成することを含む、態様36～44のいずれか1つに記載の方法。

【0197】

46．複数のプロセスプラントを動作させる複数のエンティティ間の共有リソースが、流体パイプライン内の流体であり、パラメータ測定値が、流体パイプラインから複数のエンティティのうちの1つによって取得される流体の量である、態様36～45のいずれか1つに記載の方法。

【0198】

47．複数の参加者によって保守される分散型台帳を使用したプロセス制御システムでの信頼できないデータの安全な計量のためのシステムであって、プロセスプラントに配設された1つ以上のデバイスであって、各々が物理的機能を実行して産業プロセスを制御する、プロセスプラント内に配設された1つ以上のフィールドデバイスであって、プロセスプラント内のパラメータの測定値を収集し、かつパラメータ測定値を1つ以上のゲートウェイデバイスへ提供する、ように構成された、1つ以上のフィールドデバイスと、を含み、プロセスプラント内で実行する1つ以上のエッジゲートウェイは、各々、1つ以上のプロセッサと、通信ユニットと、1つ以上のプロセッサおよび通信ユニットに連結され、かつ命令を記憶した非一過性コンピュータ可読媒体を含み、命令が、1つ以上のプロセッサによって実行されると、エッジゲートウェイデバイスに、パラメータ測定値のうちの少なくとも1つを取得させ、測定値を含むトランザクションを生成させ、トランザクションを、分散型台帳を保守するエッジゲートウェイのローカル分散型台帳ネットワーク内の少なくとも1つの他のエッジゲートウェイへ送信させ、閾値期間後に、閾値期間中に生成された複数のトランザクションを、グローバル分散型台帳を保守する参加者のグローバル分散型台帳ネットワークへの少なくとも1人の参加者へ送信させる、システム。

【0199】

48．命令がエッジゲートウェイに、さらに、トランザクションをトランザクションのローカルブロックに追加させ、トランザクションのローカルブロックに基づいて暗号パズルを解かせ、暗号パズルの解をトランザクションのローカルブロックに追加させ、トランザクションのローカルブロックを、ローカル分散型台帳ネットワーク内の少なくとも1つの他のエッジゲートウェイへ送信させる、態様47に記載のシステム。

【0200】

49. 命令がエッジゲートウェイに、さらに、閾値期間後に、閾値期間中に生成されたトランザクションの1つ以上のローカルブロックを、グローバル分散型台帳ネットワークへの少なくとも1人の参加者へ送信させる、態様47または態様48のいずれか1つに記載のシステム。

【0201】

50. 命令がエッジゲートウェイに、閾値期間後に、閾値期間中に生成された複数のトランザクションのうちの少なくともいくつかをローカル分散型台帳ネットワークからプルーニングさせる、態様47～49のいずれか1つに記載のシステム。

【0202】

51. グローバル分散型台帳が、複数のプロセスプラントを動作させる複数のエンティティによって閲覧可能な許可されたブロックチェーンである、態様47～50のいずれか1つに記載のシステム。

【0203】

52. パラメータが、複数のプロセスプラントを動作させる複数のエンティティ間の共有リソースに関連する、態様47～51のいずれか1つに記載のシステム。

【0204】

53. グローバル分散型台帳が、複数のエンティティに対応する複数のグローバル分散型台帳を含み、各グローバル分散型台帳が、グローバル分散型台帳と同じそれぞれのエンティティのローカル分散型台帳に記憶されたトランザクションを含む、態様47～52のいずれか1つに記載のシステム。

【0205】

54. グローバル分散型台帳を保守するグローバル分散型台帳ネットワーク内のコンピューティングデバイスをさらに含み、コンピューティングデバイスが、1つ以上のプロセッサと、通信ユニットと、1つ以上のプロセッサおよび通信ユニットに連結され、かつ命令を記憶した非一過性コンピュータ可読媒体を含み、命令が、1つ以上のプロセッサによって実行されると、コンピューティングデバイスに、閾値期間中に生成されたトランザクションについて、トランザクションを、複数のグローバル分散型台帳の各々からトランザクションの状態ブロックに追加させ、トランザクションの状態ブロックに基づいて暗号パズルを解かせ、暗号パズルの解をトランザクションのローカルブロックに追加させ、トランザクションの状態ブロックを、スーパーブロックチェーンを保守する参加者のスーパーブロックチェーンネットワークへの少なくとも1人の他の参加者へ送信させる、態様47～53のいずれか1つに記載のシステム。

【0206】

55. ローカル分散型台帳が、プロセスプラントを動作させるエンティティによって閲覧可能なプライベートブロックチェーンである、態様47～54のいずれか1つに記載のシステム。

【0207】

56. トランザクションが、測定値に対応する暗号ハッシュ値を含む、態様47～55のいずれか1つに記載のシステム。

【0208】

57. 複数のプロセスプラントを動作させる複数のエンティティ間の共有リソースが、流体パイプライン内の流体であり、パラメータ測定値が、流体パイプラインから複数のエンティティのうちの1つによって取得される流体の量である、態様47～56のいずれか1つに記載のシステム。

【0209】

58. ローカル分散型台帳ネットワーク上のプロセスプラント内の検証ネットワークノードであって、(i) 各々が物理的機能を実行してプロセスプラント内の産業プロセスを制御し、かつプロセスプラント内のパラメータの測定値を収集する1つ以上のフィールドデバイスと通信し、および(ii) パラメータ測定値を有するトランザクションを含む口

10

20

30

40

50

ーカル分散型台帳データをピアネットワークノードと交換する、ように構成された送受信機と、分散型台帳のコピーを記憶するように構成された記憶媒体と、ピアネットワークノードから受信した分散型台帳データに合意ルールのセットを適用するように構成されたプロセスデータ検証器と、を含み、プロセスデータ検証器は、分散型台帳データが合意ルールを満たす場合に、ピアネットワークノードから受信した分散型台帳データを分散型台帳のコピーに付加するようにさらに構成され、送受信機が、閾値期間後に、閾値期間中に生成された複数のトランザクションを、グローバル分散型台帳を保守する参加者のグローバル分散型台帳ネットワークへの少なくとも1人の参加者へ送信するように構成されている、検証ネットワークノード。

【0210】

59. 検証ネットワークノードが、閾値期間後に、ローカル分散型台帳のコピーから、閾値期間中に生成された複数のトランザクションのうちの少なくともいくつかをブルーニングするように構成されている、態様58に記載の検証ネットワークノード。

【0211】

60. グローバル分散型台帳が、複数のプロセスプラントを動作させる複数のエンティティによって閲覧可能な許可されたブロックチェーンである、態様58または態様59のいずれか1つに記載の検証ネットワークノード。

【0212】

61. パラメータのうちの少なくとも1つが、複数のプロセスプラントを動作させる複数のエンティティ間の共有リソースに関連する、態様58～60のいずれか1つに記載の検証ネットワークノード。

【0213】

62. グローバル分散型台帳が、複数のエンティティに対応する複数のグローバル分散型台帳を含み、各グローバル分散型台帳が、グローバル分散型台帳と同じそれぞれのエンティティのローカル分散型台帳に記憶されたトランザクションを含む、態様58～61のいずれか1つに記載の検証ネットワークノード。

【0214】

63. ローカル分散型台帳が、プロセスプラントを動作させるエンティティによって閲覧可能なプライベートブロックチェーンである、態様58～62のいずれか1つに記載の検証ネットワークノード。

【0215】

64. トランザクションが、パラメータ測定値に対応する暗号ハッシュ値を含む、態様58～63のいずれか1つに記載の検証ネットワークノード。

【0216】

65. 複数の参加者によって保守される分散型台帳を使用してプロセス制御システムでの品質管理、生産、または規制データを記録するための方法であって、各々が物理的機能を実行して産業プロセスを制御する1つ以上のフィールドデバイスを介して、プロセスプラント内の品質管理に関連するトリガイイベントを検出することと、トリガイイベントの時間、トリガイイベントの継続期間、トリガイイベントに関連する製品パラメータデータ、またはトリガイイベントに関連するプロセスパラメータデータ、のうちの少なくとも1つを含むイベントデータをトリガイイベントから取得することと、イベントデータを含むトランザクションを生成することと、トランザクションが分散型台帳に記憶される、トランザクションを生成することと、トランザクションを、分散型台帳を保守する参加者の分散型台帳ネットワークへの少なくとも1人の他の参加者へ送信することと、を含む、方法。

【0217】

66. トリガイイベントが、アラーム、エラー、リーク、修復イベント、プロセスマイルストーン、または是正措置、のうちの少なくとも1つである、態様65に記載の方法。

【0218】

67. 特定のトリガイイベントからイベントデータの要求を受信することと、分散型台帳からイベントデータを取得することと、特定のトリガイイベントからのイベントデータをユ

10

20

30

40

50

ーザインターフェース上に提示することと、をさらに含む、態様 6 5 または態様 6 6 のいずれか 1 つに記載の方法。

【0 2 1 9】

6 8 . イベントデータを含むトランザクションを生成することが、イベントデータのうちの少なくともいくつかに対応する暗号ハッシュ値を含むトランザクションを生成することを含む、態様 6 5 ~ 6 7 のいずれか 1 つに記載の方法。

【0 2 2 0】

6 9 . イベントデータをデータベースに記憶することと、イベントデータを認証する要求に応答して、データベースからのイベントデータとともに分散型台帳からのイベントデータの少なくとも一部に対応する暗号ハッシュ値を提供して、イベントデータの真正性を確認することと、をさらに含む、態様 6 5 ~ 6 8 のいずれか 1 つに記載の方法。

10

【0 2 2 1】

7 0 . トリガイイベントが、リリーフバルブの開放であり、トリガイイベントからのイベントデータが、リリーフバルブが開放された時間、リリーフバルブが開放された継続時間、リリーフバルブが開放されたときの圧力値、またはリリーフバルブが開放されている間に除去された液体の量、のうちの少なくとも 1 つを含む、態様 6 5 ~ 6 9 のいずれか 1 つに記載の方法。

【0 2 2 2】

7 1 . 分散型台帳が、プロセスプラントおよび規制当局によってアクセス可能なプライベートブロックチェーンである、態様 6 5 ~ 7 0 のいずれか 1 つに記載の方法。

20

【0 2 2 3】

7 2 . 分散型台帳が、パブリックブロックチェーンである、態様 6 5 ~ 7 1 のいずれか 1 つに記載の方法。

【0 2 2 4】

7 3 . トランザクションが、トリガイイベントの一意の識別子をさらに含む、態様 6 5 ~ 7 2 のいずれか 1 つに記載の方法。

【0 2 2 5】

7 4 . トリガイイベントの一意の識別子を含む検出されたトリガイイベントの表示を、プロセスプラント内の 1 つ以上の他のプロセス制御要素へ、他のプロセス制御要素がトリガイイベントに関連する追加のイベントデータを含むトランザクションを生成するために送信することをさらに含む、態様 6 5 ~ 7 3 のいずれか 1 つに記載の方法。

30

【0 2 2 6】

7 5 . 複数の参加者によって保守される分散型台帳を使用してプロセス管理システムでの品質管理、生産、または規制データを記録するシステムであって、各々が物理的機能を実行して産業プロセスを制御する、プロセスプラント内に配設された 1 つ以上のデバイスと、プロセスプラント内で実行するコンピューティングデバイスと、を含み、コンピューティングデバイスが、1 つ以上のプロセッサと、通信ユニットと、1 つ以上のプロセッサおよび通信ユニットに連結され、かつ命令を記憶した非一過性コンピュータ可読媒体を含み、命令が、1 つ以上のプロセッサによって実行されると、コンピューティングデバイスに、1 つ以上のデバイスを介して、プロセスプラント内の品質管理に関連するトリガイイベントを検出させ、トリガイイベントの時間、トリガイイベントの継続期間、トリガイイベントに関連する製品パラメータデータ、またはトリガイイベントに関連するプロセスパラメータデータ、のうちの少なくとも 1 つを含むイベントデータをトリガイイベントから取得させ、イベントデータを含むトランザクションを生成させ、トランザクションが分散型台帳に記憶され、分散型台帳内でトランザクションを検証および記録するために、トランザクションを、分散型台帳を保守する参加者の分散型台帳ネットワークへの少なくとも 1 人の他の参加者へ送信させる、システム。

40

【0 2 2 7】

7 6 . トリガイイベントが、アラーム、エラー、リーク、修復イベント、プロセスマイルストーン、または是正措置、のうちの少なくとも 1 つである、態様 7 5 に記載のシステム。

50

【0228】

77. 命令がコンピューティングデバイスに、さらに、特定のトリガイイベントからイベントデータの要求を受信させ、分散型台帳からイベントデータを取得させ、特定のトリガイイベントからのイベントデータをユーザインターフェース上に提示させる、態様75または態様76のいずれか1つに記載のシステム。

【0229】

78. トランザクションが、イベントデータの少なくとも一部に対応する暗号ハッシュ値を含む、態様75～77のいずれか1つに記載のシステム。

【0230】

79. 命令がコンピューティングデバイスに、さらに、イベントデータをデータベースに記憶させ、イベントデータを認証する要求に回答して、データベースからのイベントデータとともに分散型台帳からのイベントデータの少なくとも一部に対応する暗号ハッシュ値を提供して、イベントデータの真正性を確認させる、態様75～78のいずれか1つに記載のシステム。

10

【0231】

80. トリガイイベントが、リリーフバルブの開放であり、トリガイイベントからのイベントデータが、リリーフバルブが開放された時間、リリーフバルブが開放された継続時間、リリーフバルブが開放されたときの圧力値、またはリリーフバルブが開放されている間に除去された液体の量、のうちの少なくとも1つを含む、態様75～79のいずれか1つに記載のシステム。

20

【0232】

81. 分散型台帳が、プロセスプラントおよび規制当局によってアクセス可能なプライベートブロックチェーンである、態様75～80のいずれか1つに記載のシステム。

【0233】

82. 分散型台帳が、パブリックブロックチェーンである、態様75～81のいずれか1つに記載のシステム。

【0234】

83. トランザクションが、トリガイイベントの一意の識別子をさらに含む、態様75～82のいずれか1つに記載のシステム。

【0235】

84. 命令がコンピューティングデバイスに、さらに、トリガイイベントの一意の識別子を含む検出されたトリガイイベントの表示を、プロセスプラント内の1つ以上のデバイスへ、トリガイイベントに関連する追加のイベントデータを含むトランザクションを1つ以上のデバイスが生成するために、送信させる、態様75～83のいずれか1つに記載のシステム。

30

【0236】

85. 分散型台帳ネットワーク上のプロセスプラント内の検証ネットワークノードであって、1つ以上のフィールドデバイスと通信するように構成された送受信機であって、各フィールドデバイスが物理的機能を実行してプロセスプラント内の産業プロセスを制御し、かつ分散型台帳データをピアネットワークノードと交換し、分散型台帳データが、トリガイイベントからのイベントデータを有するトランザクションを含む、送受信機と、分散型台帳のコピーを記憶するように構成された記憶媒体と、ピアネットワークノードから受信した分散型台帳データに合意ルールのセットを適用するように構成されたプロセスデータ検証器と、を含み、プロセスデータ検証器が、分散型台帳データが合意ルールを満たす場合に、ピアネットワークノードから受信した分散型台帳データを分散型台帳のコピーに付加するようにさらに構成されている、検証ネットワークノード。

40

【0237】

86. イベントデータが、トリガイイベントの時間、トリガイイベントの継続時間、トリガイイベントに関連する製品パラメータデータ、またはトリガイイベントに関連するプロセスパラメータデータ、のうちの少なくとも1つを含む、態様85に記載の検証ネットワークノ

50

ード。

【0238】

87. トリガイイベントが、アラーム、エラー、リーク、修復イベント、または是正措置、のうちの少なくとも1つである、態様85または態様86のいずれか1つに記載の検証ネットワークノード。

【0239】

88. ピアノードから受信した分散型台帳データが、イベントデータを有するトランザクションを生成する1つ以上のフィールドデバイスのうちの1つのアイデンティティ証明を含む、態様85～87のいずれか1つに記載の検証ネットワークノード。

【0240】

89. ピアノードから受信した分散型台帳データを付加するために、トランザクション検証器が、トランザクションのブロックに基づいて暗号パズルを解き、暗号パズルの解をトランザクションのブロックに追加し、トランザクションのブロックを分散型台帳のコピーに付加し、トランザクションのブロックを分散型台帳ネットワーク内のピアネットワークノードのうちの少なくとも1つのへ送信する、ように構成されている、態様85～88のいずれか1つに記載の検証ネットワークノード。

【0241】

90. 合意ルールのセットが、トランザクションまたはトランザクションのブロックに対するフォーマット要件、ピアネットワークノードのうちのいずれが分散型台帳に次の、トランザクションまたはトランザクションのブロックを追加するかを決定するメカニズム、またはトランザクションの各々に含まれるプロセスプラントデータをハッシュする暗号ハッシュアルゴリズム、のうちの少なくとも1つを含む、態様85～89のいずれか1つに記載の検証ネットワークノード。

【0242】

91. 分散型台帳が、プロセスプラントおよび規制当局によってアクセス可能なプライベートブロックチェーンである、態様85～90のいずれか1つに記載の検証ネットワークノード。

【0243】

92. 分散型台帳が、パブリックブロックチェーンである、態様85～91のいずれか1つに記載の検証ネットワークノード。

【0244】

93. トランザクションが、トリガイイベントの一意の識別子をさらに含む、態様85～92のいずれか1つに記載の検証ネットワークノード。

【0245】

94. 複数の参加者によって保守される分散型台帳を使用してプロセス制御システム内のソフトウェアまたはファームウェアの状態を記録するための方法であって、コンピューティングデバイスによって、各々が物理的機能を実行して産業プロセスを制御する1つ以上のフィールドデバイスを有するプロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態を取得することであって、ソフトウェアまたはファームウェアは、プロセスプラント内のネットワークまたはプロセス制御デバイス内で実行される、取得することと、プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態を含むトランザクションを生成することであって、トランザクションが分散型台帳に記憶される、生成することと、分散型台帳を保守する参加者の分散型台帳ネットワークへの少なくとも1人の他の参加者へトランザクションを送信することと、を含む、方法。

【0246】

95. プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態が、現在の状態を更新したユーザのコンピューティングデバイスから取得され、トランザクションを生成することが、ユーザのアイデンティティデータを取得することと、1つ以上のプロセッサにおいて、ユーザのアイデンティティデータでトランザクションを増強することと、1つ以上のプロセッサにおいて、トランザクションに基づいて暗号署名を生

10

20

30

40

50

成することと、1つ以上のプロセッサにおいて、暗号化署名でトランザクションを増強することと、をさらに含む、態様94に記載の方法。

【0247】

96. プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態を含むトランザクションを生成することが、プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態に対応する暗号ハッシュ値を含むトランザクションを生成することを含む、態様94または態様95のいずれか1つに記載の方法。

【0248】

97. ソフトウェアまたはファームウェアを実行するネットワークまたはプロセス制御デバイスから、プロセスプラント内で実行されるソフトウェアまたはファームウェアの状態を取得することと、プロセスプラント内で実行されるソフトウェアまたはファームウェアの状態を分散型台帳からの暗号ハッシュ値と比較して、ソフトウェアまたはファームウェアが改ざんされていないことを確認することと、をさらに含む、態様94～96のいずれか1つに記載の方法。

【0249】

98. プロセスプラント内で実行されるソフトウェアまたはファームウェアの状態が、暗号ハッシュ値に従って、分散型台帳に記憶されたソフトウェアまたはファームウェアの現在の状態と一致しないと判定することに応答して、ソフトウェアまたはファームウェアがプロセスプラント内で実行されるのを防止することをさらに含む、態様94～97のいずれか1つに記載の方法。

【0250】

99. ソフトウェアまたはファームウェアを以前の状態に戻すことをさらに含む、態様94～98のいずれか1つに記載の方法。

【0251】

100. プロセスプラント内で実行されるソフトウェアまたはファームウェアの状態が、暗号ハッシュ値に従って、分散型台帳に記憶されたソフトウェアまたはファームウェアの現在の状態と一致すると判定することに応答して、ネットワークまたはプロセス制御デバイスにソフトウェアまたはファームウェアを実行させることをさらに含む、態様94～99のいずれか1つに記載の方法。

【0252】

101. トランザクションをトランザクションのブロックに追加することと、トランザクションのブロックに基づいて暗号パズルを解くことと、暗号パズルの解をトランザクションのブロックに追加することと、トランザクションのブロックを分散型台帳ネットワークへの少なくとも1人の他の参加者へ送信することと、をさらに含む、態様94～100のいずれか1つに記載の方法。

【0253】

102. トランザクション内のアイデンティティデータを、プロセスプラント内で実行されるソフトウェアまたはファームウェアの状態を更新することを認可されたユーザに対応するアイデンティティデータの複数のセットと比較することと、アイデンティティデータが複数のアイデンティティデータのセット内に含まれる場合に、トランザクションをトランザクションのブロックに追加することと、をさらに含む、態様94～101のいずれか1つに記載の方法。

【0254】

103. 分散型台帳が、許可されたブロックチェーンである、態様94～102のいずれか1つに記載の方法。

【0255】

104. 複数の参加者によって保守される分散型台帳を使用して、プロセス制御システムおよび接続された計装内のソフトウェアまたはファームウェアの状態を記録するためのシステムであって、各々が物理的機能を実行して産業プロセスを制御する、プロセスプラント内に配設された1つ以上のデバイスと、プロセスプラント内で実行するコンピューテ

10

20

30

40

50

イングデバイスと、を含み、コンピューティングデバイスが、1つ以上のプロセッサと、通信ユニットと、1つ以上のプロセッサおよび通信ユニットに連結され、かつ命令を記憶した非一過性コンピュータ可読媒体を含み、命令が、1つ以上のプロセッサによって実行されると、コンピューティングデバイスに、プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態を取得させ、ソフトウェアまたはファームウェアは、プロセスプラントまたはプロセスプラント内のネットワークデバイス内に配設された1つ以上のデバイスのうちの少なくとも1つ内で実行され、プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態を含むトランザクションを生成させ、分散型台帳内でトランザクションを検証および記録するために、トランザクションが分散型台帳に記憶され、分散型台帳を保守する参加者の分散型台帳ネットワークへの少なくとも1人の他の参加者へトランザクションを送信させる、システム。

10

【0256】

105. プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態が、現在の状態を更新したユーザのコンピューティングデバイスから取得され、トランザクションを生成するために、命令がコンピューティングデバイスに、ユーザのアイデンティティデータを取得させ、ユーザのアイデンティティデータでトランザクションを増強させ、トランザクションに基づいて暗号署名を生成させ、暗号署名でトランザクションを増強させる、態様104に記載のシステム。

【0257】

106. トランザクションが、プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態に対応する暗号ハッシュ値で生成される、態様104または態様105のいずれか1つに記載のシステム。

20

【0258】

107. 1つ以上のプロセッサと、通信ユニットと、1つ以上のプロセッサおよび通信ユニットに連結され、かつ命令を記憶した非一過性コンピュータ可読媒体を含むサーバデバイスをさらに含み、命令が、1つ以上のプロセッサによって実行されると、サーバデバイスに、ソフトウェアまたはファームウェアを実行するネットワークまたはプロセス制御デバイスから、プロセスプラント内で実行されるソフトウェアまたはファームウェアの状態を取得させ、プロセスプラント内で実行されるソフトウェアまたはファームウェアの状態を分散型台帳からの暗号ハッシュ値と比較して、ソフトウェアまたはファームウェアが改ざんされていないことを確認させる、態様104～106のいずれか1つに記載のシステム。

30

【0259】

108. 命令がサーバデバイスに、さらに、プロセスプラント内で実行されるソフトウェアまたはファームウェアの状態が、暗号ハッシュ値に従って、分散型台帳に記憶されたソフトウェアまたはファームウェアの現在の状態と一致しないと判定することに応答して、ソフトウェアまたはファームウェアがプロセスプラント内で実行されるのを防止する、態様104～107のいずれか1つに記載のシステム。

【0260】

109. 命令がサーバデバイスに、さらに、ソフトウェアまたはファームウェアを以前の状態に戻す、態様104～108のいずれか1つに記載のシステム。

40

【0261】

110. 命令がサーバデバイスに、さらに、プロセスプラント内で実行されるソフトウェアまたはファームウェアの状態が、暗号ハッシュ値に従って、分散型台帳に記憶されたソフトウェアまたはファームウェアの現在の状態と一致する判定することに応答して、ネットワークまたはプロセス制御デバイスにソフトウェアまたはファームウェアを実行させる、態様104～109のいずれか1つに記載のシステム。

【0262】

111. 命令がコンピューティングデバイスに、さらに、トランザクションをトランザクションのブロックに追加させ、トランザクションのブロックに基づいて暗号パズルを解

50

かせ、暗号パズルの解をトランザクションのブロックに追加させ、トランザクションのブロックを分散型台帳ネットワークへの少なくとも1人の他の参加者へ送信させる、態様104～110のいずれか1つに記載のシステム。

【0263】

112. 命令がコンピューティングデバイスに、さらに、トランザクション内のアイデンティティデータを、プロセスプラント内で実行されるソフトウェアまたはファームウェアの状態を更新することを認可されたユーザに対応するアイデンティティデータの複数のセットと比較させ、アイデンティティデータがアイデンティティデータの複数のセット内に含まれる場合に、トランザクションをトランザクションのブロックに追加させる、態様104～111のいずれか1つに記載のシステム。

10

【0264】

113. 分散型台帳が、許可されたブロックチェーンである、態様104～112のいずれか1つに記載のシステム。

【0265】

114. 分散型台帳ネットワーク上のプロセスプラント内の検証ネットワークノードであって、1つ以上のフィールドデバイスと通信するように構成された送受信機であって、各フィールドデバイスが物理的機能を実行してプロセスプラント内の産業プロセスを制御し、かつ分散型台帳データをピアネットワークノードと交換し、分散型台帳データが、プロセスプラント内のソフトウェアまたはファームウェアの現在の状態を表すデータを有するトランザクションを含む、送受信機と、分散型台帳のコピーを記憶するように構成された記憶媒体と、ピアネットワークノードから受信した分散型台帳データに合意ルールのセットを適用するように構成されたプロセスデータ検証器と、を含み、プロセスデータ検証器が、分散型台帳データが合意ルールを満たす場合に、ピアネットワークノードから受信した分散型台帳データを分散型台帳のコピーに付加するようにさらに構成されている、検証ネットワークノード。

20

【0266】

115. ピアノードから受信した分散型台帳データを付加するために、トランザクション検証器が、トランザクションのブロックに基づいて暗号パズルを解き、暗号パズルの解をトランザクションのブロックに追加し、トランザクションのブロックを分散型台帳のコピーに付加し、トランザクションのブロックを分散型台帳ネットワーク内のピアネットワークノードのうちの少なくとも1つへ送信する、ように構成されている、態様114に記載の検証ネットワークノード。

30

【0267】

116. 合意ルールのセットが、トランザクションまたはトランザクションのブロックに対するフォーマット要件、ピアネットワークノードのうちのいずれが分散型台帳に次の、トランザクションまたはトランザクションのブロックを追加するかを決定するメカニズム、またはトランザクションの各々に含まれるソフトウェアまたはファームウェア状態をハッシュする暗号ハッシュアルゴリズム、のうちの少なくとも1つを含む、態様114または態様115のいずれか1つに記載の検証ネットワークノード。

【0268】

40

117. ピアノードから受信した分散型台帳データが、プロセスプラント内で実行されるソフトウェアまたはファームウェアの現在の状態を表すデータを有するトランザクションを生成するデバイスのユーザのアイデンティティ証明を含む、態様114～116のいずれか1つに記載の検証ネットワークノード。

【0269】

118. 複数の参加者によって保守される分散型台帳を使用してプロセス制御システム内のスマートコントラクトを作成するための方法であって、1つ以上のプロセッサによって、各々が物理的機能を実行して産業プロセスを制御する1つ以上のフィールドデバイスを有するプロセスプラントに関連するスマートコントラクトを生成することと、1つ以上のプロセッサによって、スマートコントラクトを、分散型台帳ネットワークへの複数の参

50

加者によって保守される分散型台帳に記憶されたアドレスに展開することと、を含む、方法。

【0270】

119. スマートコントラクトが、プロセスプラント内で発生するイベントに従ってトークン値を受信または提供する、態様118に記載の方法。

【0271】

120. プロセスプラントに関連するスマートコントラクトを生成することが、第1のプロセスプラントからトークン値を取得するスマートコントラクトを生成することを含み、製品が第2のプロセスプラントから第1のプロセスプラントに移送されたと判定し、およびトークン値を第2のプロセスプラントへ提供する、態様118または態様119のいずれか1つに記載の方法。

10

【0272】

121. スマートコントラクトが、製品が第1のプロセスプラントで受領されたことを表示する証拠オラクルからトランザクションを受信することによって、製品が第2のプロセスプラントから第1のプロセスプラントに移送されたと判定する、態様118～120のいずれか1つに記載の方法。

【0273】

122. プロセスプラントに関連するスマートコントラクトを生成することが、製品が1つ以上の品質指標を満たすか、または超えていると判定し、かつ製品が1つ以上の品質指標を満たしている、または超えると判定することに応答して、トークン値を第2のプロセスプラントへ提供する、スマートコントラクトを生成することをさらに含む、態様118～121のいずれか1つに記載の方法。

20

【0274】

123. スマートコントラクトが、証拠オラクルから、各々が製品パラメータ値またはプロセスパラメータ値を含む1つ以上のトランザクションを受信し、かつ製品パラメータ値またはプロセスパラメータ値を、1つ以上の品質指標に含まれる製品またはプロセスパラメータ閾値と比較することによって、製品が1つ以上の品質指標を満たす、または超えると判定する、態様118～122のいずれか1つに記載の方法。

【0275】

124. プロセスプラントに関連するスマートコントラクトを生成することが、障害が発生するプロセスプラント内のデバイスのデバイス情報を取得し、かつデバイス情報を共有する要求を受信することに応答して、デバイス情報をデバイスサプライヤへ提供するスマートコントラクトを生成することを含む、態様118～123のいずれか1つに記載の方法。

30

【0276】

125. スマートコントラクトが、デバイス情報を含む証拠オラクルからトランザクションを受信することによってデバイス情報を取得する、態様118～124のいずれか1つに記載の方法。

【0277】

126. スマートコントラクトが、要求を発行したユーザのアイデンティティデータとともに要求を含むトランザクションを受信することによって、デバイス情報を共有する要求を受信し、スマートコントラクトが、トランザクション内のアイデンティティデータを、分散型台帳ネットワークがデバイス情報を共有することを要求することを認可されたユーザに対応するアイデンティティデータの複数のセットと比較し、およびアイデンティティデータがアイデンティティデータの複数のセット内に含まれる場合に、デバイス情報をデバイスサプライヤへ提供する、態様118～125のいずれか1つに記載の方法。

40

【0278】

127. プロセスプラントに関連するスマートコントラクトを生成することが、安全計装システム（SIS）デバイスに関連付けられたパラメータを受信し、かつパラメータを提供したオペレータが認可されたオペレータであると判定することに応答してSISデバ

50

イスにパラメータを書き込む、スマートコントラクトを生成することを含む、態様 1 1 8 ~ 1 2 6 のいずれか 1 つに記載の方法。

【0 2 7 9】

1 2 8 . スマートコントラクトが、トランザクションを提供したオペレータのアイデンティティデータとともにパラメータを含むトランザクションを受信することによって、S I S デバイスに関連付けられたパラメータを受信し、パラメータを提供したオペレータが認可されたオペレータであると判定することが、トランザクション内のアイデンティティデータを、S I S デバイスに関連付けられたパラメータを調整することを認可されたオペレータに対応するアイデンティティデータの複数のセットと比較することを含む、態様 1 1 8 ~ 1 2 7 のいずれか 1 つに記載の方法。

10

【0 2 8 0】

1 2 9 . S I S デバイスに関連付けられたパラメータが、S I S デバイスをロックする要求である、態様 1 1 8 ~ 1 2 8 のいずれか 1 つに記載の方法。

【0 2 8 1】

1 3 0 . 複数の参加者によって保守される分散型台帳を使用してプロセス制御システム内のスマートコントラクトとインタラクションするための方法であって、各々が物理的機能を実行して産業プロセスを制御する 1 つ以上のフィールドデバイスを有するプロセスプラント内で発生するイベントからイベントデータを取得することと、分散型台帳に記憶されたアドレスにスマートコントラクトを展開することに応答して、コンピューティングデバイスによって、イベントデータを含むトランザクションを生成することと、トランザクションを、分散型台帳ネットワークへの複数の参加者によって保守される分散型台帳に記憶されたスマートコントラクトへ送信することと、を含む、方法。

20

【0 2 8 2】

1 3 1 . コンピューティングデバイスのアイデンティティデータを取得することと、1 つ以上のプロセッサにおいて、コンピューティングデバイスのアイデンティティデータでトランザクションを増強することと、1 つ以上のプロセッサにおいて、トランザクションに基づいて暗号署名を生成することと、1 つ以上のプロセッサにおいて、暗号署名でトランザクションを増強することと、をさらに含む、態様 1 3 0 に記載の方法。

【0 2 8 3】

1 3 2 . トランザクションをトランザクションのブロックに追加することと、トランザクションのブロックに基づいて暗号パズルを解くことと、暗号パズルの解をトランザクションのブロックに追加することと、トランザクションのブロックを分散型台帳ネットワークへの少なくとも 1 人の他の参加者へ送信することと、をさらに含む、態様 1 3 0 または態様 1 3 1 のいずれか 1 つに記載の方法。

30

【0 2 8 4】

1 3 3 . スマートコントラクトが、第 1 のプロセスプラントからトークン値を取得し、製品が第 2 のプロセスプラントから第 1 のプロセスプラントに移送されたと判定し、トークン値を第 2 のプロセスプラントへ提供し、プロセスプラント内で発生するイベントからイベントデータを取得することが、製品が第 1 のプロセスプラントで受領されたという表示を取得することと、第 1 のプロセスプラントの識別情報、製品の識別情報、および、製品が第 2 のプロセスプラントから第 1 のプロセスプラントで受領されたという表示を含むトランザクションを生成することと、を含む、態様 1 3 0 ~ 1 3 2 のいずれか 1 つに記載の方法。

40

【0 2 8 5】

1 3 4 . 製品が第 1 のプロセスプラントで受領されたという表示を取得することが、製品の 1 つ以上の製品パラメータ値、または製品の製造に関与したプロセスプラントエンティティの 1 つ以上のプロセスパラメータ値を取得することと、1 つ以上の製品パラメータ値または 1 つ以上のプロセスパラメータ値を含むトランザクションを生成することと、をさらに含む、態様 1 3 0 ~ 1 3 3 のいずれか 1 つに記載の方法。

【0 2 8 6】

50

135. スマートコントラクトが、障害が発生するプロセスプラント内のデバイスのデバイス情報を取得し、デバイス情報を共有する要求を受信することに応答してデバイス情報をデバイスサプライヤに提供し、プロセスプラント内で発生するイベントからイベントデータを取得することが、デバイスのデバイス情報を取得することと、デバイスの識別情報およびデバイス情報を含むトランザクションを生成することと、を含む、態様130～134のいずれか1つに記載の方法。

【0287】

136. スマートコントラクトが、安全計装システム（SIS）デバイスに関連付けられたパラメータを受信し、パラメータを提供したオペレータが認可されたオペレータであると判定することに応答して、パラメータをSISデバイスに書き込み、プロセスプラント内で発生するイベントからイベントデータを取得することが、SISデバイスに関連付けられたパラメータを変更する要求を取得することと、SISデバイスの識別情報、変更されたパラメータ、および変更されたパラメータの新たなパラメータ値を含むトランザクションを生成することと、を含む、態様130～135のいずれか1つに記載の方法。

【0288】

137. 複数の参加者によって保守される分散型台帳を使用してプロセス制御システム内のスマートコントラクトを作成するためのコンピューティングデバイスであって、1つ以上のプロセッサと、通信ユニットと、1つ以上のプロセッサおよび通信ユニットに連結され、かつ命令を記憶した非一過性コンピュータ可読媒体を含み、命令が、1つ以上のプロセッサによって実行されると、コンピューティングデバイスに、各々が物理的機能を実行して産業プロセスを制御する1つ以上のフィールドデバイスを有するプロセスプラントに関連するスマートコントラクトを生成させ、スマートコントラクトを、分散型台帳ネットワークへの複数の参加者によって保守される分散型台帳に記憶されたアドレスに展開させる、コンピューティングデバイス。

【0289】

138. スマートコントラクトが、プロセスプラント内で発生するイベントに従ってトークン値を受信または提供する、態様137に記載のコンピューティングデバイス。

【0290】

139. スマートコントラクトが、第1のプロセスプラントからトークン値を取得し、製品が第2のプロセスプラントから第1のプロセスプラントに移送されたと判定し、トークン値を第2のプロセスプラントへ提供する、態様137または態様138のいずれか1つに記載のコンピューティングデバイス。

【0291】

140. スマートコントラクトが、製品が第1のプロセスプラントで受領されたことを表す証拠オラクルからトランザクションを受信することによって、製品が第2のプロセスプラントから第1のプロセスプラントに移送されたと判定する、態様137～139のいずれか1つに記載のコンピューティングデバイス。

【0292】

141. スマートコントラクトが、製品が1つ以上の品質指標を満たすか、または超えると判定し、製品が1つ以上の品質指標を満たすか、または超えると判定することに応答して、トークン値を第2のプロセスプラントへ提供する、態様137～140のいずれか1つに記載のコンピューティングデバイス。

【0293】

142. スマートコントラクトが、証拠オラクルから、各々が製品パラメータ値またはプロセスパラメータ値を含む1つ以上のトランザクションを受信し、かつ製品パラメータ値またはプロセスパラメータ値を、1つ以上の品質指標に含まれる製品またはプロセスパラメータ閾値と比較することによって、製品が1つ以上の品質指標を満たす、または超えると判定する、態様137～141のいずれか1つに記載のコンピューティングデバイス。

【0294】

143. スマートコントラクトが、障害が発生するプロセスプラント内のデバイスのデ

10

20

30

40

50

バイス情報を取得し、デバイス情報を共有する要求を受信することに応答してデバイス情報をデバイスサプライヤへ提供する、態様 137～142 のいずれか 1 つに記載のコンピューティングデバイス。

【0295】

144. スマートコントラクトが、デバイス情報を含む証拠オラクルからトランザクションを受信することによって、デバイス情報を取得する、態様 137～143 のいずれか 1 つに記載のコンピューティングデバイス。

【0296】

145. スマートコントラクトが、要求を発行したユーザのアイデンティティデータとともに要求を含むトランザクションを受信することによって、デバイス情報を共有する要求を受信し、スマートコントラクトが、トランザクション内のアイデンティティデータを、分散型台帳ネットワークがデバイス情報を共有することを要求することを認可されたユーザに対応するアイデンティティデータの複数のセットと比較し、およびアイデンティティデータがアイデンティティデータの複数のセット内に含まれる場合に、デバイス情報をデバイスサプライヤへ提供する、態様 137～144 のいずれか 1 つに記載のコンピューティングデバイス。

【0297】

146. スマートコントラクトが、安全計装システム（SIS）デバイスに関連付けられたパラメータを受信し、パラメータを提供したオペレータが認可されたオペレータであると判定することに応答して、パラメータを SIS デバイスに書き込む、態様 137～145 のいずれか 1 つに記載のコンピューティングデバイス。

【0298】

147. スマートコントラクトが、トランザクションを提供したオペレータのアイデンティティデータとともにパラメータを含むトランザクションを受信することによって、SIS デバイスに関連付けられたパラメータを受信し、パラメータを提供したオペレータが認可されたオペレータであると判定することが、トランザクション内のアイデンティティデータを、SIS デバイスに関連付けられたパラメータを調整することを認可されたオペレータに対応するアイデンティティデータの複数のセットと比較することを含む、態様 137～146 のいずれか 1 つに記載のコンピューティングデバイス。

【0299】

148. SIS デバイスに関連付けられたパラメータが、SIS デバイスをロックする要求である、態様 137～147 のいずれか 1 つに記載のコンピューティングデバイス。

【0300】

149. 複数の参加者によって保守される分散型台帳を使用してプロセス制御システム内のスマートコントラクトとインタラクションするためのシステムであって、各々が物理的機能を実行して産業プロセスを制御する、プロセスプラント内に配設された 1 つ以上のデバイスを含み、プロセスプラント内で実行するコンピューティングデバイスが、1 つ以上のプロセッサと、通信ユニットと、1 つ以上のプロセッサおよび通信ユニットに連結され、かつ命令をその上に記憶した非一過性コンピュータ可読媒体を含み、命令が、1 つ以上のプロセッサによって実行されると、コンピューティングデバイスに、1 つ以上のデバイスを介して、プロセスプラント内で発生しているイベントからイベントデータを取得させ、分散型台帳に記憶されたアドレスにスマートコントラクトを展開することに応答して、イベントデータを含むトランザクションを生成させ、トランザクションを、分散型台帳ネットワークへの複数の参加者によって保守される分散型台帳に記憶されたスマートコントラクトへ送信させる、システム。

【0301】

150. 命令がコンピューティングデバイスに、さらに、コンピューティングデバイスのアイデンティティデータを取得させ、コンピューティングデバイスのアイデンティティデータでトランザクションを増強させ、トランザクションに基づいて暗号署名を生成させ、暗号署名でトランザクションを増強させる、態様 149 に記載のシステム。

10

20

30

40

50

【0302】

151. 命令がコンピューティングデバイスに、さらに、トランザクションをトランザクションのブロックに追加させ、トランザクションのブロックに基づいて暗号パズルを解かせ、暗号パズルの解をトランザクションのブロックに追加させ、トランザクションのブロックを分散型台帳ネットワークへの少なくとも1人の他の参加者へ送信させる、態様149または態様150のいずれか1つに記載のシステム。

【0303】

152. スマートコントラクトが、第1のプロセスプラントからトークン値を取得し、製品が第2のプロセスプラントから第1のプロセスプラントに移送されたと判定し、トークン値を第2のプロセスプラントへ提供し、プロセスプラント内で発生するイベントからイベントデータを取得するために、命令がコンピューティングデバイスに、製品が第1のプロセスプラントで受領されたという表示を取得させ、第1のプロセスプラントの識別情報、製品の識別情報、および製品が第2のプロセス工場から第1のプロセス工場で受領されたという表示を含むトランザクションを生成させる、態様149～151のいずれか1つに記載のシステム。

10

【0304】

153. 製品が第1のプロセスプラントで受領されたという表示を取得するために、命令がコンピューティングデバイスに、製品の1つ以上の製品パラメータ値、または製品の製造に関与するプロセスプラントエンティティの1つ以上の製品パラメータ値を取得させ、1つ以上の製品パラメータ値または1つ以上のプロセスパラメータ値を含むトランザクションを生成させる、態様149～152のいずれか1つに記載のシステム。

20

【0305】

154. スマートコントラクトが、障害が発生するプロセスプラント内のデバイスのデバイス情報を取得し、デバイス情報を共有する要求を受信することに応答してデバイス情報をデバイスサプライヤに提供し、プロセスプラント内で発生するイベントからイベントデータを取得するために、命令がコンピューティングデバイスに、デバイスのデバイス情報を取得させ、デバイスの識別情報およびデバイス情報を含むトランザクションを生成させる、態様149～153のいずれか1つに記載のシステム。

【0306】

155. スマートコントラクトが、安全計装システム（SIS）デバイスに関連付けられたパラメータを受信し、パラメータを提供したオペレータが認可されたオペレータであると判定することに応答して、パラメータをSISデバイスに書き込み、プロセスプラント内で発生するイベントからイベントデータを取得するために、命令がコンピューティングデバイスに、SISデバイスに関連付けられたパラメータを変更する要求を取得させ、SISデバイスの識別情報、変更されたパラメータ、および変更されたパラメータの新たなパラメータ値を含むトランザクションを生成させる、態様149～154のいずれか1つに記載のシステム。

30

【0307】

ソフトウェアに実装される場合、本明細書に記載されるアプリケーション、サービス、およびエンジンはいずれも、コンピュータもしくはプロセッサのRAMもしくはROMなどにおける磁気ディスク、レーザディスク、固体メモリデバイス、分子メモリ記憶デバイス、または他の記憶媒体などの、任意の有形の非一時的コンピュータ可読メモリに記憶され得る。本明細書に開示される例示的システムは、他の構成要素の中でも、ハードウェア上で実行されるソフトウェアおよび／またはファームウェアを含むように開示されているが、そのようなシステムは単に例示的であるに過ぎず、限定的であると見なされるべきではないことに留意されたい。例えば、これらのハードウェア、ソフトウェア、およびファームウェア構成要素のうちのいずれかまたは全てが、ハードウェアにのみ、ソフトウェアにのみ、あるいはハードウェアおよびソフトウェアの任意の組み合わせで、埋め込まれ得ることが企図される。したがって、本明細書に記載される例示的なシステムは、1つ以上のコンピュータデバイスのプロセッサで実行されるソフトウェアで実装されるものとして

40

50

記載されているが、提供される例がかかるシステムを実装する唯一の方法ではないことを当業者は容易に理解するであろう。

【0308】

したがって、本発明は具体的な例に関して記載されてきたが、これらの例は例解的であるに過ぎず、本発明の限定であることを意図せず、変更、追加、または削除が、本発明の趣旨および範囲から逸脱することなく、開示される実施形態に対して行われ得ることが当業者には明らかであろう。

10

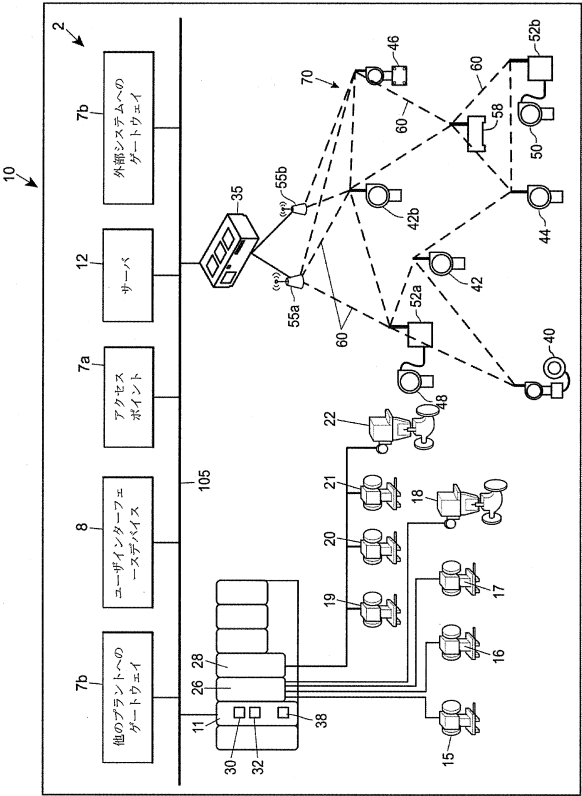
20

30

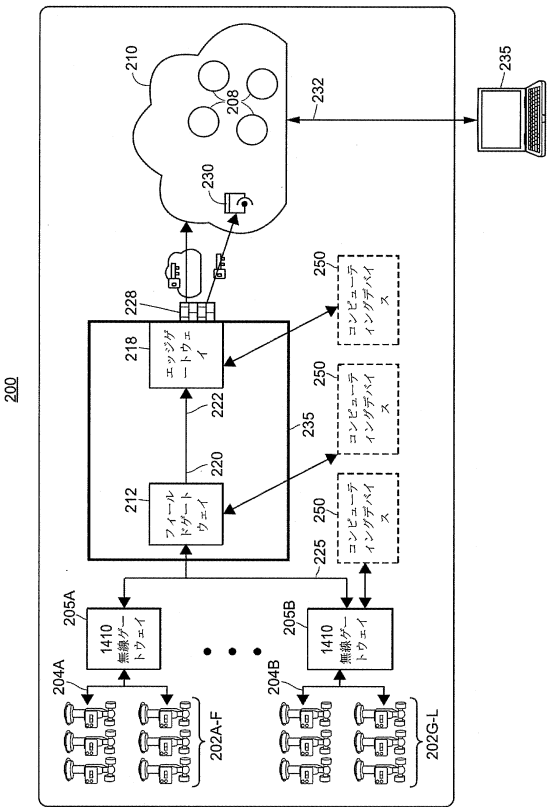
40

50

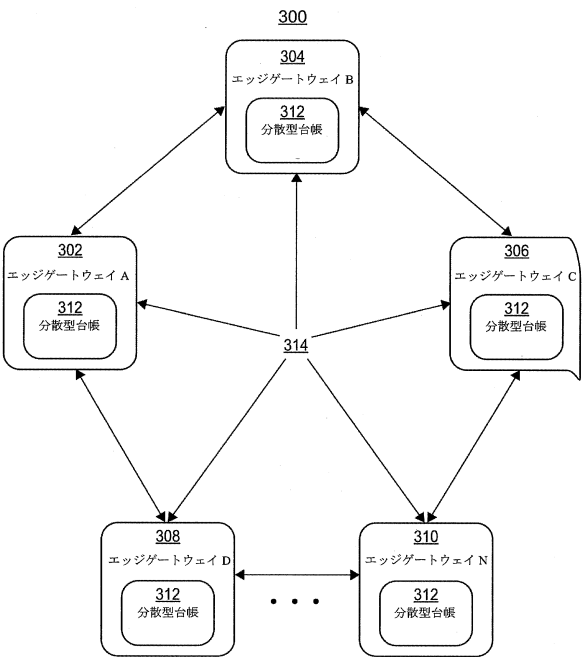
【図面】
【図 1】



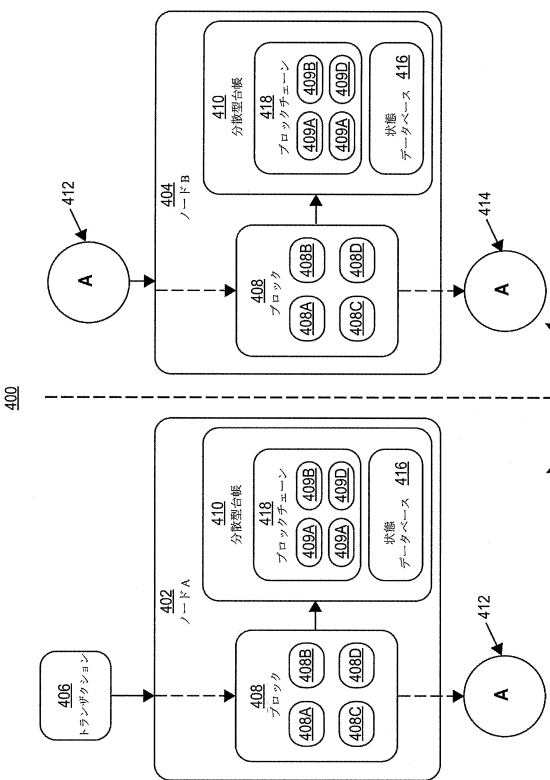
【図 2】



【図 3】



【図 4】



10

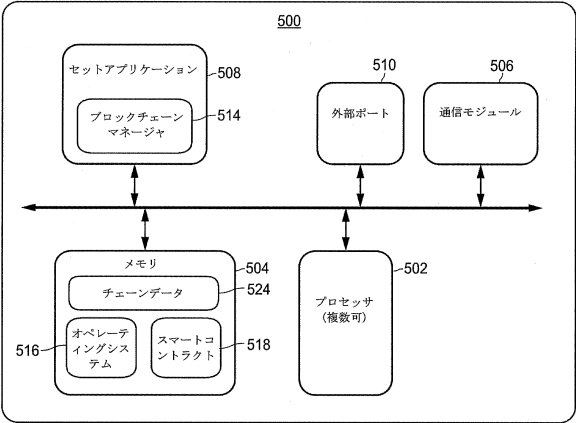
20

30

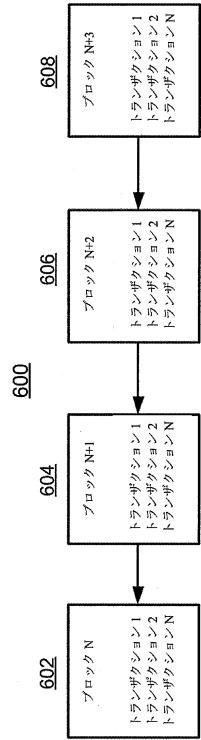
40

50

【図 5】



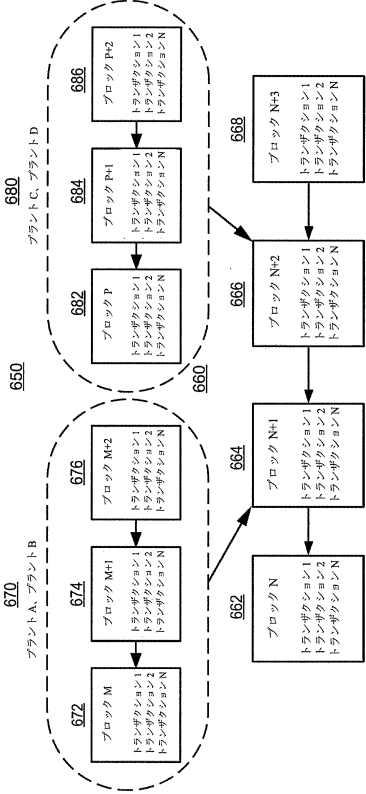
【図 6 A】



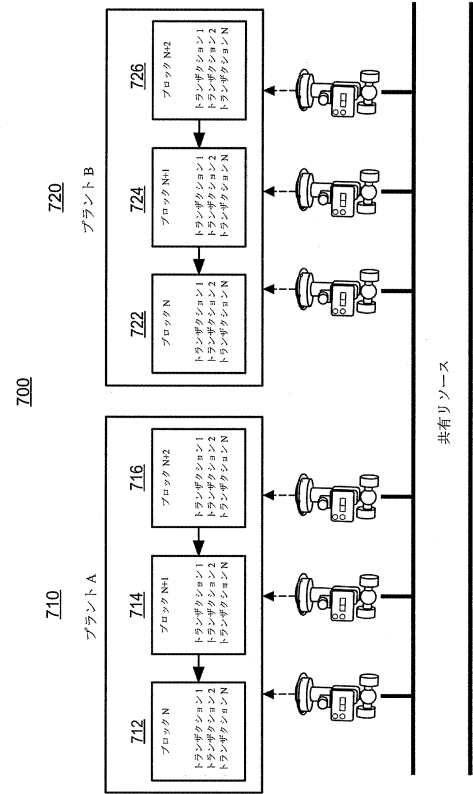
10

20

【図 6 B】



【図 7 A】

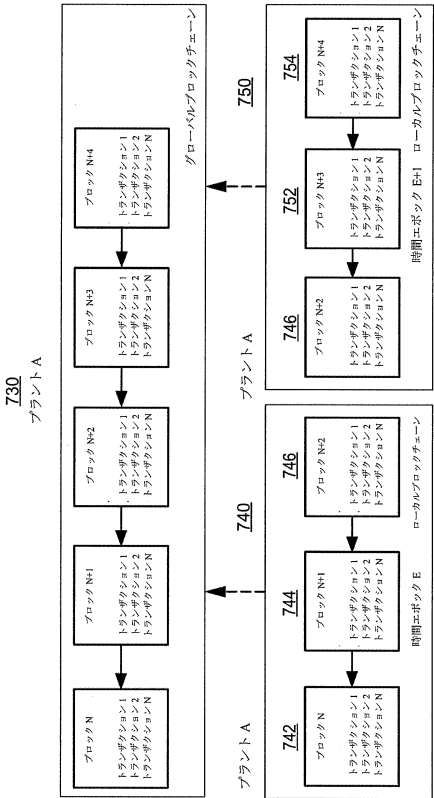


30

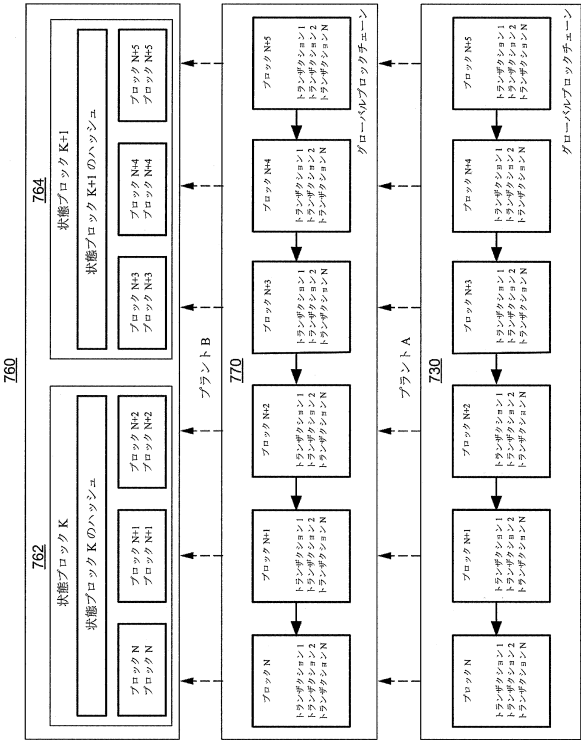
40

50

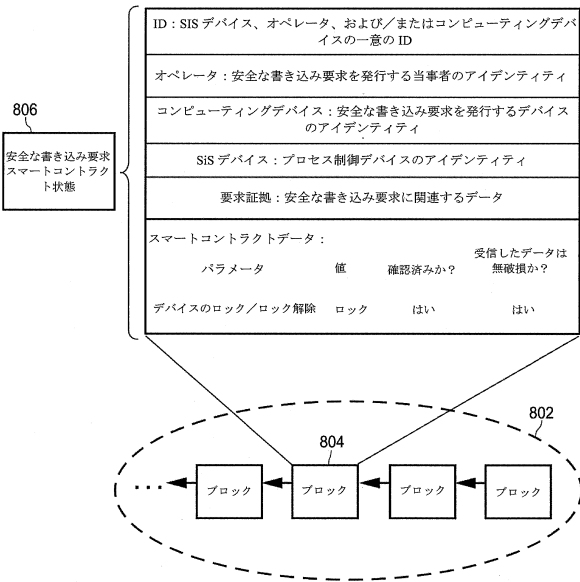
【図 7 B】



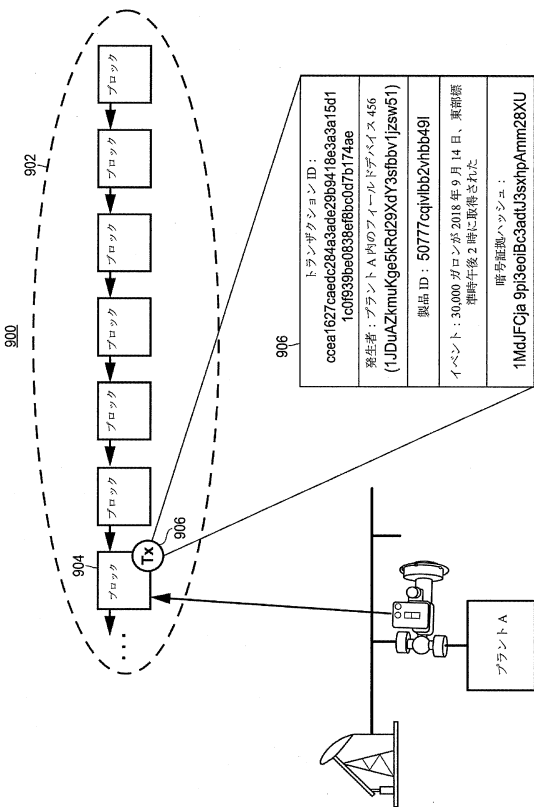
【図 7 C】



【図 8】



【図 9】



10

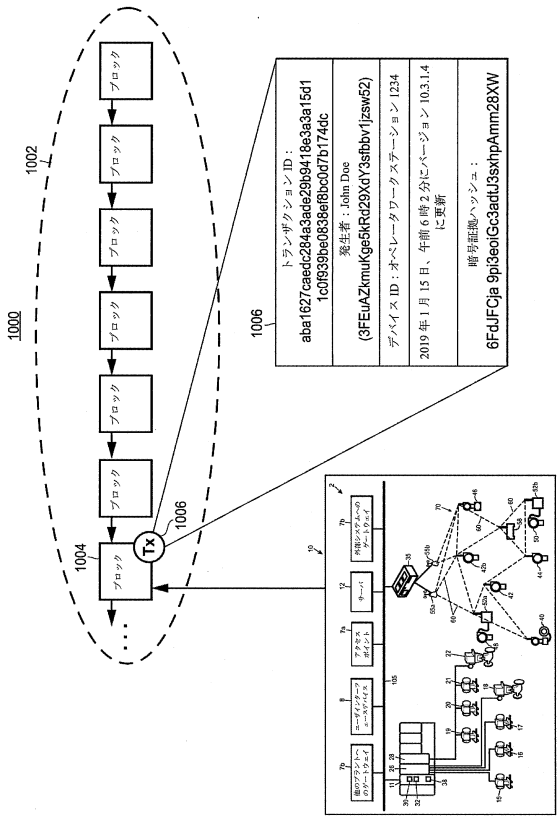
20

30

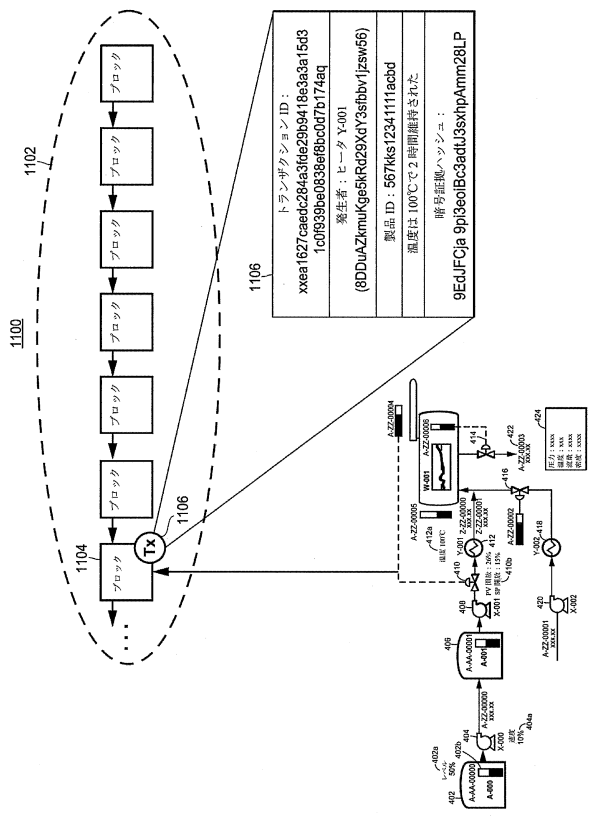
40

50

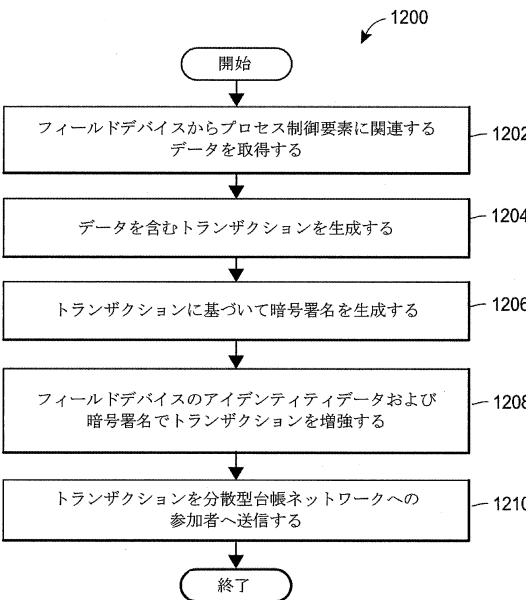
【図 10】



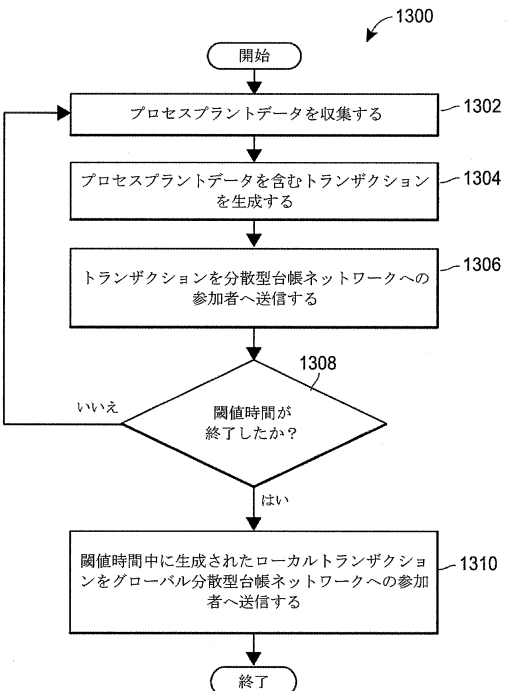
【図 11】



【図 12】



【図 13】



10

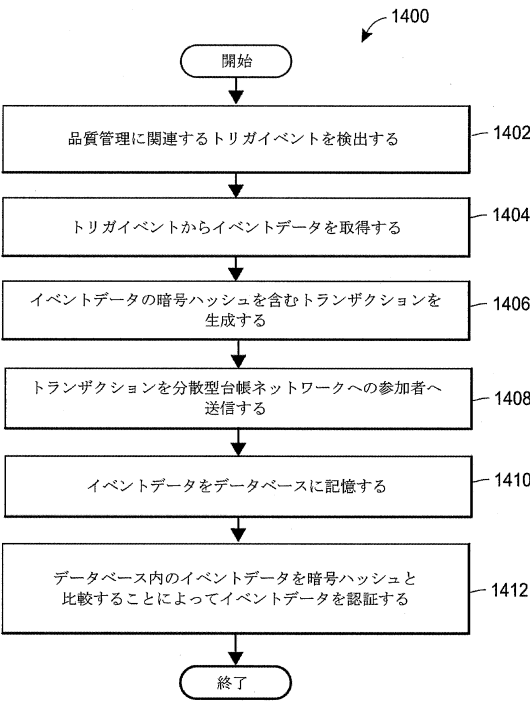
20

30

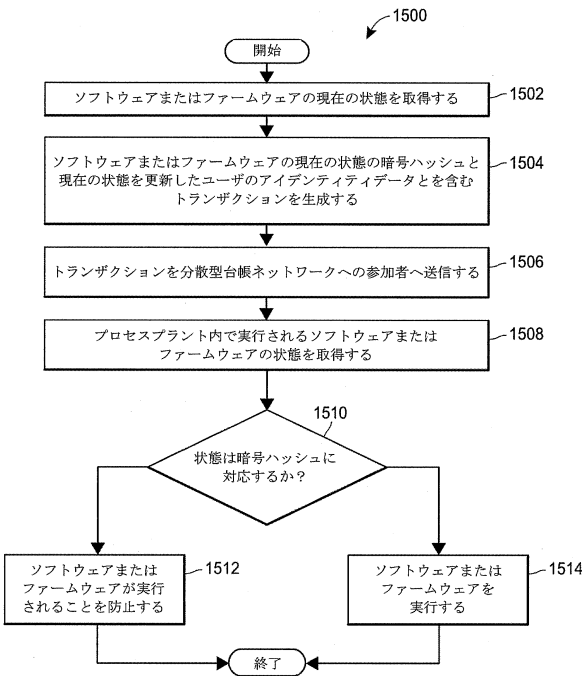
40

50

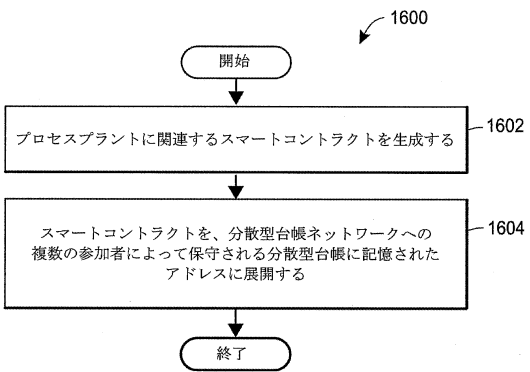
【図 1 4】



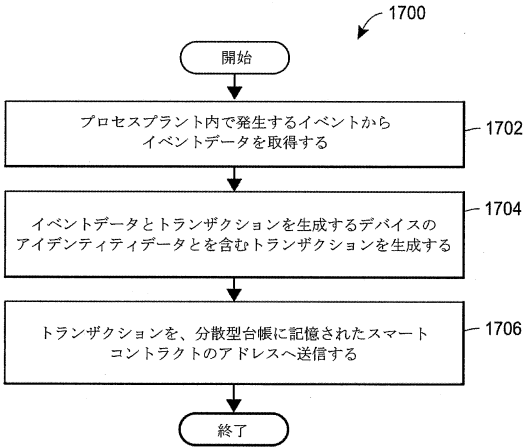
【図 1 5】



【図 1 6】



【図 1 7】



10

20

30

40

50

フロントページの続き

(51)国際特許分類

F I

H 0 4 L	67/00 (2022.01)	H 0 4 L	67/00
H 0 4 L	67/01 (2022.01)	H 0 4 L	67/01
H 0 4 L	67/2866(2022.01)	H 0 4 L	67/2866

(56)参考文献

特開 2 0 1 8 - 1 7 3 7 9 4 (J P , A)
米国特許出願公開第 2 0 1 8 / 0 2 5 3 4 6 4 (U S , A 1)
特開 2 0 1 1 - 1 0 8 1 6 7 (J P , A)
特開 2 0 1 8 - 1 8 1 3 4 5 (J P , A)
特表 2 0 1 9 - 5 1 4 0 8 7 (J P , A)
特表 2 0 1 9 - 5 1 9 1 3 7 (J P , A)
米国特許出願公開第 2 0 1 8 / 0 1 7 6 2 2 9 (U S , A 1)
国際公開第 2 0 1 7 / 1 9 5 1 6 4 (W O , A 1)
国際公開第 2 0 1 7 / 1 9 2 8 3 7 (W O , A 1)
米国特許出願公開第 2 0 1 7 / 0 2 7 9 7 7 4 (U S , A 1)

(58)調査した分野 (Int.Cl., D B名)

G 0 6 F 2 1 / 6 4
G 0 5 B 2 3 / 0 2
G 0 6 F 1 3 / 0 0
G 0 6 F 2 1 / 1 2
H 0 4 L 9 / 3 2