(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7467126号
(P7467126)

(45)発行日　令和6年4月15日(2024.4.15)

(24)登録日　令和6年4月5日(2024.4.5)

(51)国際特許分類

Ｇ０５Ｂ　23/02　(2006.01)		Ｇ０５Ｂ	23/02	Ｚ
Ｇ０６Ｑ　10/20　(2023.01)		Ｇ０６Ｑ	10/20	

ＦＩ

請求項の数　32　（全67頁）

(21)出願番号　特願2020-4354(P2020-4354)
(22)出願日　令和2年1月15日(2020.1.15)
(65)公開番号　特開2020-113282(P2020-113282A)
(43)公開日　令和2年7月27日(2020.7.27)
審査請求日　令和4年12月19日(2022.12.19)
(31)優先権主張番号　16/248,388
(32)優先日　平成31年1月15日(2019.1.15)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　512132022
フィッシャー－ローズマウント システムズ，インコーポレイテッド
アメリカ合衆国 テキサス ７８６８１－７４３０ ラウンド ロック ウェスト ルイス ヘナ ブルバード １１００ ビルディング １ エマーソン プロセス マネージメント
(74)代理人　100096091
弁理士　井上 誠一
(72)発明者　ロイド・ケネス・タグボー
フィリピン共和国 マニラ パシグ シティ ソレント オアシス コンド ビルディング Ｄ ユニット ５２７
(72)発明者　ギアン・マルコ・ティー

最終頁に続く

(54)【発明の名称】　プロセス制御システムにおける分散型台帳を使用するマシンツーマシントランザクション

(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たプロセス制御システムでのスマートコントラクトを作製する方法であって、

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であって、

（ｉ）前記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スマートコントラクト、

（ｉｉ）障害が発生した前記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、かつ前記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、前記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、または、

（ｉｉｉ）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、かつ前記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前記ＳＩＳデバイスに前記パラメータを書き込むスマートコントラクト、

の少なくともいずれかのスマートコントラクトを生成することと、

前記１つ以上のプロセッサによって、前記スマートコントラクトを、分散型台帳ネットワークへの前記複数の参加者によって保守される前記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。

【請求項２】

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前記第１のプロセスプラントに移送されたと判定し、および前記トークン値を前記第２のプロセスプラントへ提供する、請求項１に記載の方法。

【請求項３】

前記スマートコントラクトが、製品が前記第２のプロセスプラントから前記第１のプロセスプラントに移送されたことを、前記製品が前記第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判定する、請求項２に記載の方法。

【請求項４】

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、前記製品が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、かつ前記製品が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、前記トークン値を前記第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、請求項３に記載の方法。

【請求項５】

前記スマートコントラクトが、前記製品が１つ以上の品質指標を満たすか、または超えると、前記証拠オラクルから、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、かつ前記製品パラメータ値または前記プロセスパラメータ値を、前記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判定する、請求項３または請求項４に記載の方法。

【請求項６】

前記スマートコントラクトが、前記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りデバイス情報を取得する、請求項１に記載の方法。

【請求項７】

前記スマートコントラクトが、前記デバイス情報を共有する要求を、前記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前記要求を含むトランザクションを受信することによって受信し、前記スマートコントラクトが、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、前記分散型台帳ネットワークが前記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、前記デバイス情報を前記デバイスサプライヤへ提供する、請求項１に記載の方法。

【請求項８】

前記スマートコントラクトが、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、前記トランザクションを提供した前記オペレータのアイデンティティデータとともに前記パラメータを含み、前記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、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、請求項１に記載の方法。

【請求項９】

前記ＳＩＳデバイスに関連付けられた前記パラメータが、前記ＳＩＳデバイスをロックする要求である、請求項１に記載の方法。

【請求項１０】

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、

前記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、前記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、
前記トランザクションを、分散型台帳ネットワークへの前記複数の参加者によって保守される前記分散型台帳に記憶された前記スマートコントラクトへ送信することと、を含む、方法。
【請求項１１】
前記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、
前記１つ以上のプロセッサにおいて、前記コンピューティングデバイス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１０に記載の方法。
【請求項１２】
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１０または請求項１１に記載の方法。
【請求項１３】
前記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前記第１のプロセスプラントに移送されたと判定し、前記トークン値を前記第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、
前記製品が前記第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、
前記第１のプロセスプラントの識別情報、前記製品の識別情報、および前記製品が前記第２のプロセスプラントから前記第１のプロセスプラントで受領されたという表示を含む前記トランザクションを生成することと、を含む、請求項１０から請求項１２のいずれかに記載の方法。
【請求項１４】
前記製品が前記第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、
前記製品の１つ以上の製品パラメータ値または前記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つ以上の製品パラメータ値を取得することと、
前記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前記トランザクションを生成することと、をさらに含む、請求項１３に記載の方法。
【請求項１５】
前記スマートコントラクトが、障害が発生した前記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、前記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前記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、
前記デバイスのデバイス情報を取得することと、
前記デバイスの識別情報および前記デバイス情報を含む前記トランザクションを生成することと、を含む、請求項１０から請求項１４のいずれかに記載の方法。
【請求項１６】
前記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、前記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、前記パラメータを前記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、

前記ＳＩＳデバイスの識別情報、前記変更されたパラメータ、および前記変更されたパラメータの新たなパラメータ値を含む前記トランザクションを生成することと、を含む、請求項１０から請求項１５のいずれかに記載の方法。

【請求項１７】

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製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、

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であって、

（ｉ）前記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スマートコントラクト、

（ｉｉ）障害が発生した前記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、かつ前記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、前記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、または、

（ｉｉｉ）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、かつ前記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前記ＳＩＳデバイスに前記パラメータを書き込むスマートコントラクト、

の少なくともいずれかのスマートコントラクトを生成させ、

前記スマートコントラクトを、分散型台帳ネットワークへの前記複数の参加者によって保守される前記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。

【請求項１８】

前記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前記第１のプロセスプラントに移送されたと判定し、前記トークン値を前記第２のプロセスプラントへ提供する、請求項１７に記載のコンピューティングデバイス。

【請求項１９】

前記スマートコントラクトが、製品が前記第２のプロセスプラントから前記第１のプロセスプラントに移送されたことを、前記製品が前記第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判定する、請求項１８に記載のコンピューティングデバイス。

【請求項２０】

前記スマートコントラクトが、前記製品が１つ以上の品質指標を満たすか、または超えると判定し、前記製品が前記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、前記トークン値を前記第２のプロセスプラントへ提供する、請求項１９に記載のコンピューティングデバイス。

【請求項２１】

前記スマートコントラクトが、前記製品が１つ以上の品質指標を満たすか、または超えると、前記証拠オラクルから、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、かつ前記製品パラメータ値または前記プロセスパラメータ値を、前記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判定する、請求項２０に記載のコンピューティングデバイス。

【請求項２２】

前記スマートコントラクトが、前記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りデバイス情報を取得する、請求項１７に記載のコンピューティングデバイス。

【請求項２３】
前記スマートコントラクトが、前記デバイス情報を共有する要求を、前記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前記要求を含むトランザクションを受信することによって受信し、前記スマートコントラクトが、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、前記分散型台帳ネットワークが前記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、前記デバイス情報を前記デバイスサプライヤへ提供する、請求項１７または請求項２２に記載のコンピューティングデバイス。
【請求項２４】
前記スマートコントラクトが、前記パラメータを含むトランザクションを前記トランザクションを提供した前記オペレータのアイデンティティデータとともに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、前記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、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、請求項１７に記載のコンピューティングデバイス。
【請求項２５】
前記ＳＩＳデバイスに関連付けられた前記パラメータが、前記ＳＩＳデバイスをロックする要求である、請求項１７に記載のコンピューティングデバイス。
【請求項２６】
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つ以上のデバイスと、
前記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、
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、前記コンピューティングデバイスに、
前記１つ以上のデバイスを介して、前記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、
前記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、前記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、
前記トランザクションを、分散型台帳ネットワークへの前記複数の参加者によって保守される前記分散型台帳に記憶された前記スマートコントラクトへ送信することと、を実行させる、システム。
【請求項２７】
前記命令が、前記コンピューティングデバイスに、
前記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、
前記コンピューティングデバイス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、をさらに実行させる、請求項２６に記載のシステム。
【請求項２８】
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、をさらに実行させる、請求項２７に記載のシステム。
【請求項２９】
前記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前記第１のプロセスプラントに移送されたと判定し、前記トークン値を前記第２のプロセスプラントへ提供し、前記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、前記命令が前記コンピューティングデバイスに、
前記製品が前記第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、
前記第１のプロセスプラントの識別情報、前記製品の識別情報、および前記製品が前記第２のプロセスプラントから前記第１のプロセスプラントで受領されたという表示を含む前記トランザクションを生成することと、を実行させる、請求項２６から請求項２８のいずれかに記載のシステム。
【請求項３０】
前記製品が前記第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、前記命令が前記コンピューティングデバイスに、
前記製品の１つ以上の製品パラメータ値または前記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つ以上の製品パラメータ値を取得することと、
前記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前記トランザクションを生成することと、を実行させる、請求項２９に記載のシステム。
【請求項３１】
前記スマートコントラクトが、障害が発生した前記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、前記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前記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、前記命令が前記コンピューティングデバイスに、
前記デバイスのデバイス情報を取得することと、
前記デバイスの識別情報および前記デバイス情報を含む前記トランザクションを生成することと、を実行させる、請求項２６から請求項３０のいずれかに記載のシステム。
【請求項３２】
前記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、前記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、前記パラメータを前記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、前記命令が前記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することと、
前記ＳＩＳデバイスの識別情報、前記変更されたパラメータ、および前記変更されたパラメータの新たなパラメータ値を含む前記トランザクションを生成することと、を実行させる、請求項２６から請求項３１のいずれかに記載のシステム。
【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）、ＷｉｒｅｌｅｓｓＨＡＲＴ（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分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。

【０００４】

例として、Ｅｍｅｒｓｏｎ　Ｐｒｏｃｅｓｓ　Ｍａｎａｇｅｍｅｎｔによって販売されているＤｅｌｔａＶ（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、それらの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製または変更、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、構成設計者が作製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、および一部の場合においては、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た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。

【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。

【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。

【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。

【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。

【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、石油が供給される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。

【図７Ｃ】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（ＳＩＳ）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。

【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。

【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製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とは対照的に、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。
【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製されるとき等）。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ず、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ープロトコルである。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へルーティングし得る。

【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が、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、セルラルータ、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製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ＩＥＥＥ８０２．１１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）、ＷｉｒｅｌｅｓｓＨＡＲＴ（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ＤｅｌｔａＶ（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）フィールドバスプロトコル、ＨＡＲＴ（登録商標）プロトコル、ＷｉｒｅｌｅｓｓＨＡＲＴ（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する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。制御ベースの機能ブロックは、典型的には、トランスミッタ、センサまたは他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もよく、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４０～１６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４～２０ｍＡ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５２Ａ、５２Ｂ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５２Ａ、５２Ｂ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５５Ａ、５５Ｂ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を含み得る。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ヘースデバイス８上で実行し得、ユーザが、プロセス制御モジュールを作製または変更し、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製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、作製された（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ＩＥＥＥ８０２．１１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、異なる物理的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２０５Ａ、２０５Ｂに通信可能に接続される。ゲートウェイ２０５Ａ、２０５Ｂとデバイス２０２との間の通信接続は、参照番号２０４Ａ、２０４Ｂで示されている。

【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２０５Ａ、２０５Ｂ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５２Ａ、５２Ｂ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。

【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に限定されず、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７ａ～７ｃ、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。

【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２０５Ａ、２０５Ｂ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２０５Ａ、２０５Ｂ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２０５Ａ、２０５Ｂ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２０４Ａ、２０４Ｂが保護され得る。

【００４６】

加えて、無線ゲートウェイ２０５Ａ、２０５Ｂ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２０４Ａ、２０４Ｂ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、ＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ、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２０５Ａ、２０５Ｂは、フィールドゲートウェイ２１２への中継のためにＴＬＳラッパによって保護されるＨＡＲＴ－ＩＰフォーマットのパケットを生成する。

【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パケットは、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２０５Ａ、２０５Ｂへの中継２０４Ａ、２０４Ｂ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２０５Ａ、２０５Ｂ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によって保護されてもよい。

【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ＳＡＳ（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、ＳＡＳ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、ＳＡＳ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ＡＭＱＰ（Ａｄｖａｎｃｅｄ Ｍｅｓｓａｇｅ Ｑｕｅｕｉｎｇ Ｐｒｏｔｏｃｏｌ、アドバンスト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。

【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。

【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２０５Ａ、２０５Ｂ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２０５Ａ、２０５Ｂ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用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／分析動作用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、安全な態様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製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】

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。

【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。

【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。

【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、プ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製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、新たに作製されたブロック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。

【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製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製する。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製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、新たに作製されたブロック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６０２～６０８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。

【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製する。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。

【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を

、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、マークルルートを、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、ブロックチェーン上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。

【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。

【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。

【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。

【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。

【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。
【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の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１個以下のトークンを有する限り、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。
【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を維持し得る。例えば、ブロックチェーン６００内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プルーニングし得る。

【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（参照番号７４０）。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から除去またはプルーニングする。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のみを含む（参照番号７４６）。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）を除去またはプルーニングする。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Ｂ　７７０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を組み合わせて、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を作製する。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。

【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ガロンの石油を取り出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得して、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。

【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。

【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（ｓａｆｅｔｙ　ｉｎｓｔｒｕｍｅｎｔｅｄ　ｓｙｓｔｅｍ、ＳＩＳ）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（ｃｙｃｌｉｃａｌ　ｒｅｄｕｎｄａｎｃｙ　ｃｈｅｃｋ、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ＳＩＳ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製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、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、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、ＣＲＣ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ＣＲＣ値を生成し、予想されるＣＲＣ値を、受信したＣＲＣ値と比較し得る。予想されるＣＲＣ値が受信したＣＲＣ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、ＳＩＳデバイスをロック／ロック解除するパラメータ、ＳＩＳ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ＳＩＳ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ＳＩＳデバイスまたはＳＩＳ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ＳＩＳデバイスまたはターゲットＳＩＳ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ＣＲＣ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ＳＩＳ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ＳＩＳ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ＳＩＳ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ＳＩＳ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ＳＩＳ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。

【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。

【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。

【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

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。
【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ベントに応答して、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、イベントに関与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、イベントに関与する製品の製品パラメータ値等、トリガ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。

【０１０７】

いくつかの実施形態では、トリガ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ベントを通知し、トリガ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ベントの同じ一意の識別子を含む。

【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。

【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】

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　°Ｃである）を含み得る。トランザクション１１０６がトリガ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、トリガイベントの識別情報と、トリガイベントの時間、トリガイベントの持続時間、および／またはトリガイベントの説明等のトリガ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か、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。いくつかの実施形態では、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応答して、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

トリガイベ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、トリガイベ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ベ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。

【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。

【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。

【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。

【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プルーニングし得る。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製する。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、トリガイベントを検出する。

【０１３４】

いずれにしても、ブロック１４０４で、トリガ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、トリガイベントの一意の識別子、トリガイベントの時間、トリガイベントの継続期間、トリガイベントの説明、トリガ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、トリガイベント発生時の製品の製品パラメータデータ、トリガ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。
【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。
【０１３６】
上述のように、トランザクションは、トリガイベントのイベントデータの暗号ハッシュ、および／またはトリガイベントのイベントデータとトリガ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）。
【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。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製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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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プ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】

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ロ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プ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ベントを検出することと、トリガイベントの時間、トリガイベントの継続期間、トリガ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であって、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することと、をさらに含む、態様６５または態様６６のいずれか１つに記載の方法。

【０２１９】

６８．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６５～６７のいずれか１つに記載の方法。

【０２２０】

６９．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６５～６８のいずれか１つに記載の方法。

【０２２１】

７０．トリガイベントが、リリーフバルブの開放であり、トリガ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６５～６のいずれか１つに記載の方法。

【０２２２】

７１．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６５～７０のいずれか１つに記載の方法。

【０２２３】

７２．分散型台帳が、パブリックブロックチェーンである、態様６５～７１のいずれか１つに記載の方法。

【０２２４】

７３．トランザクションが、トリガイベントの一意の識別子をさらに含む、態様６５～７２のいずれか１つに記載の方法。

【０２２５】

７４．トリガイベントの一意の識別子を含む検出されたトリガイベントの表示を、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６５～７３のいずれか１つに記載の方法。

【０２２６】

７５．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ベントを検出させ、トリガイベントの時間、トリガイベントの継続期間、トリガ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。

【０２２７】

７６．トリガイベントが、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７５に記載のシステム。

【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させる、態様７５～７８のいずれか１つに記載のシステム。

【０２３１】

８０．トリガイベントが、リリーフバルブの開放であり、トリガ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。

【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、トリガイベントの一意の識別子を含む検出されたトリガイベントの表示を、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。

【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。

【０２３７】

８６．イベントデータが、トリガイベントの時間、トリガイベントの継続時間、トリガ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ード。

【０２３８】

８７．トリガイベントが、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され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、トランザクションは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、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。

【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。

【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。

【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。

【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。

【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。
【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。
【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】
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製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。
【０２７２】
１２１．スマートコントラクトが、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ことを、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。
【０２７４】
１２３．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、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。

【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。

【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１１８～１２６のいずれか１つに記載の方法。

【０２７９】

１２８．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１１８～１２７のいずれか１つに記載の方法。

【０２８０】

１２９．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１１８～１２８のいずれか１つに記載の方法。

【０２８１】

１３０．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。

【０２８２】

１３１．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１３０に記載の方法。

【０２８３】

１３２．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１３０または態様１３１のいずれか１つに記載の方法。

【０２８４】

１３３．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１３０～１３２のいずれか１つに記載の方法。

【０２８５】

１３４．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１３０～１３３のいずれか１つに記載の方法。

【０２８６】

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製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ことを、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、製品が１つ以上の品質指標を満たすか、または超えると、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１３７～１２２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。

【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。

【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。

【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。

【０３０７】

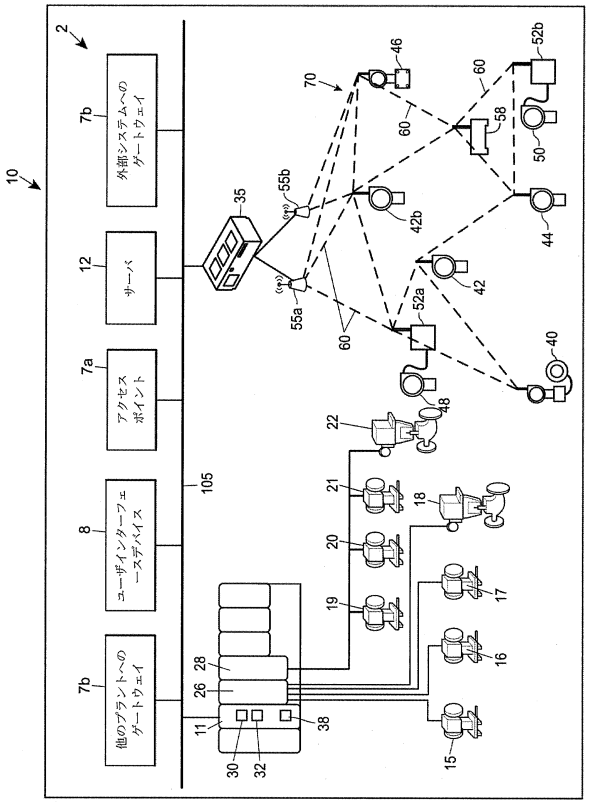
ソフトウェアに実装される場合、本明細書に記載されるアプリケーション、サービス、およびエンジンはいずれも、コンピュータもしくはプロセッサのＲＡＭもしくはＲＯＭなどにおける磁気ディスク、レーザディスク、固体メモリデバイス、分子メモリ記憶デバイス、または他の記憶媒体などの、任意の有形の非一時的コンピュータ可読メモリに記憶され得る。本明細書に開示される例示的システムは、他の構成要素の中でも、ハードウェア上で実行されるソフトウェアおよび／またはファームウェアを含むように開示されているが、そのようなシステムは単に例示的であるに過ぎず、限定的であると見なされるべきではないことに留意されたい。例えば、これらのハードウェア、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】

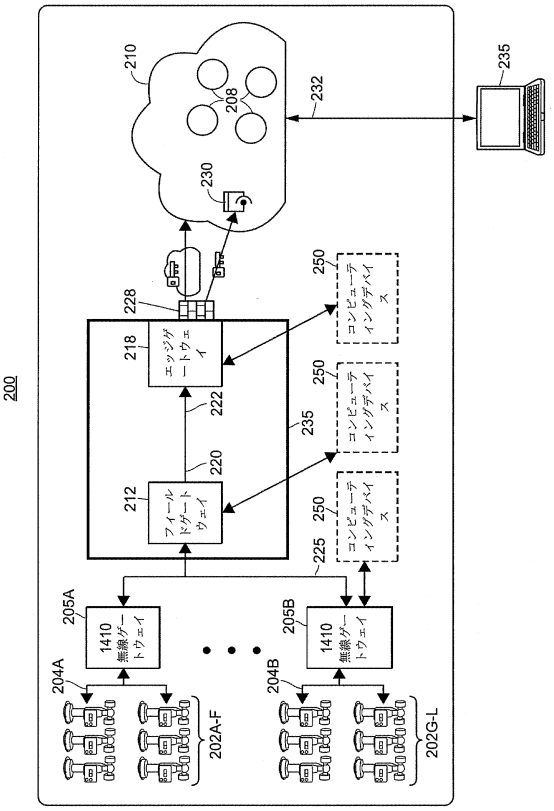
したがって、本発明は具体的な例に関して記載されてきたが、これらの例は例解的であるに過ぎず、本発明の限定であることを意図せず、変更、追加、または削除が、本発明の趣旨および範囲から逸脱することなく、開示される実施形態に対して行われ得ることが当業者には明らかであろう。

【図面】

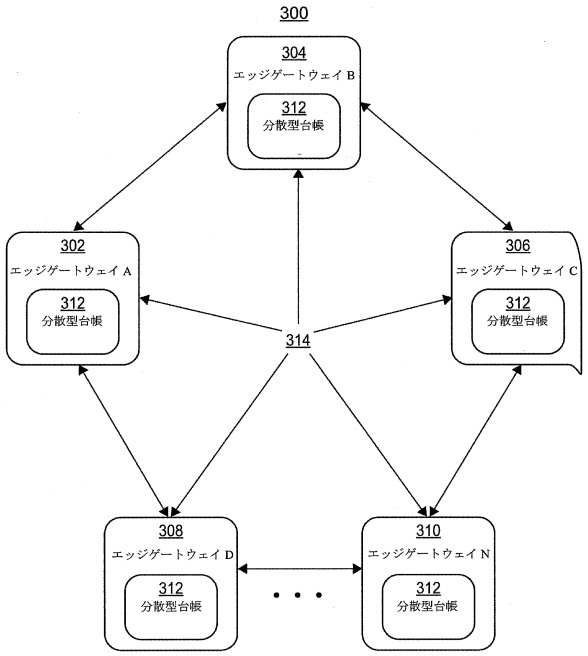
【図１】


10
2
外部システムへのゲートウェイ
7b
サーバ
12
アクセスポイント
7a
ユーザインターフェースデバイス
8
他のプラントへのゲートウェイ
7b
105
35
55b
55a
70
46
60
52b
58
50
42b
44
42
52a
40
48
22
21
18
20
19
17
16
15
28
26
11
38
30
32

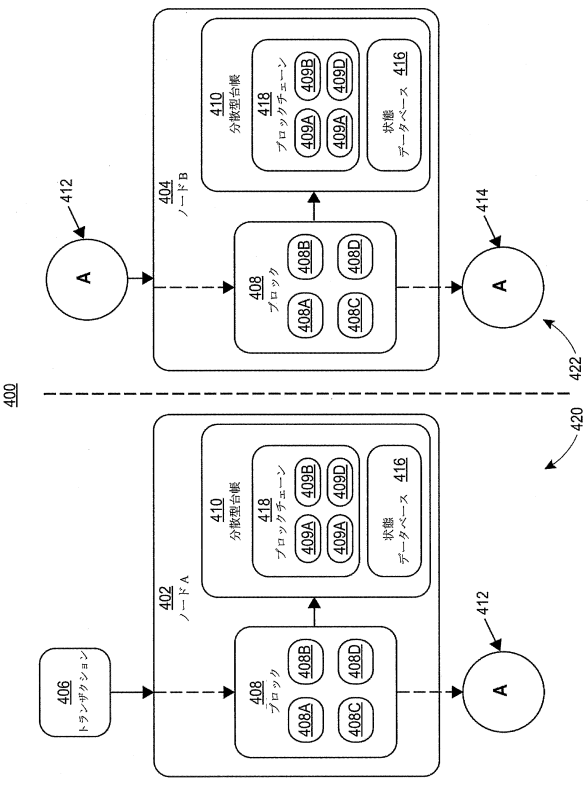
【図２】


200
210
208
232
235
230
228
218
エッジゲートウェイ
222
220
212
フィールドゲートウェイ
235
250
コンピューティングデバイス
225
205A
205B
1410
無線ゲートウェイ
204A
204B
202A-F
202G-L

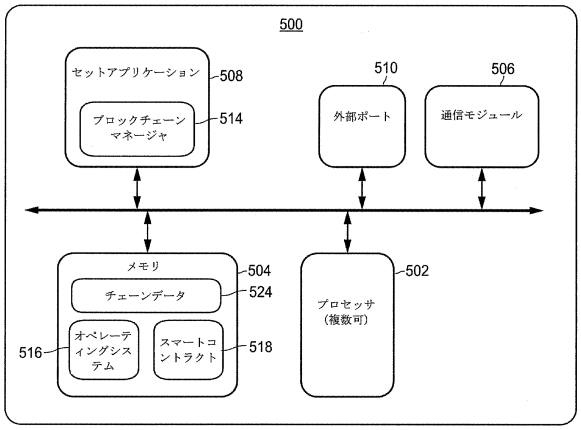
【図３】


300
304
エッジゲートウェイ B
312
分散型台帳
302
エッジゲートウェイ A
306
エッジゲートウェイ C
314
308
エッジゲートウェイ D
310
エッジゲートウェイ N

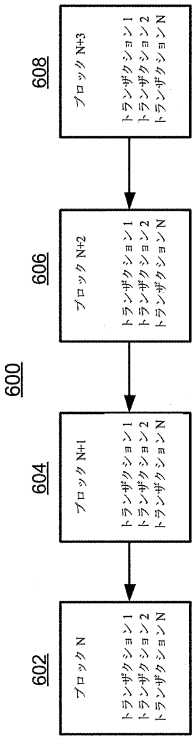
【図４】


400
404
ノードB
402
ノードA
410
分散型台帳
418
ブロックチェーン
409A
409B
409C
409D
状態
データベース
416
408
ブロック
408A
408B
408C
408D
406
トランザクション
412
414
420
422
A

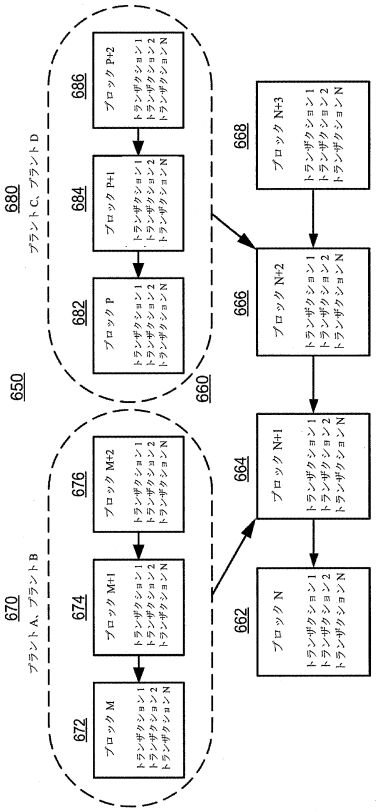
【図５】



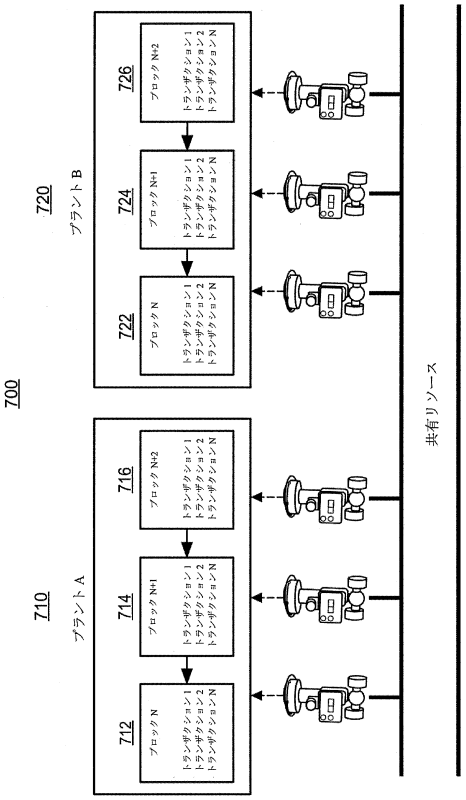
【図６Ａ】



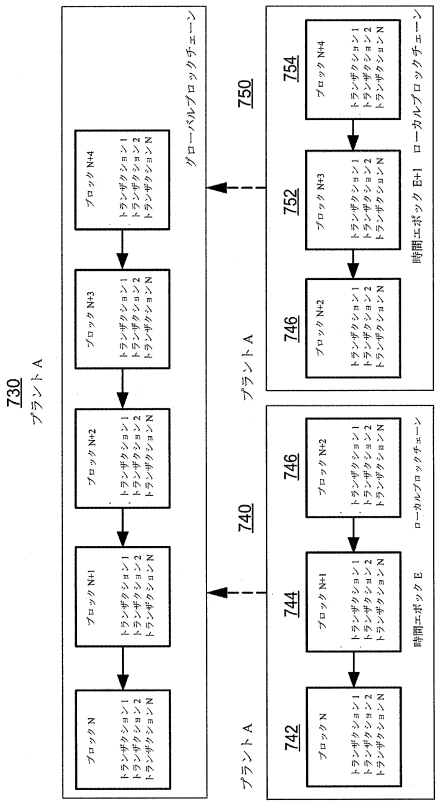
【図６Ｂ】



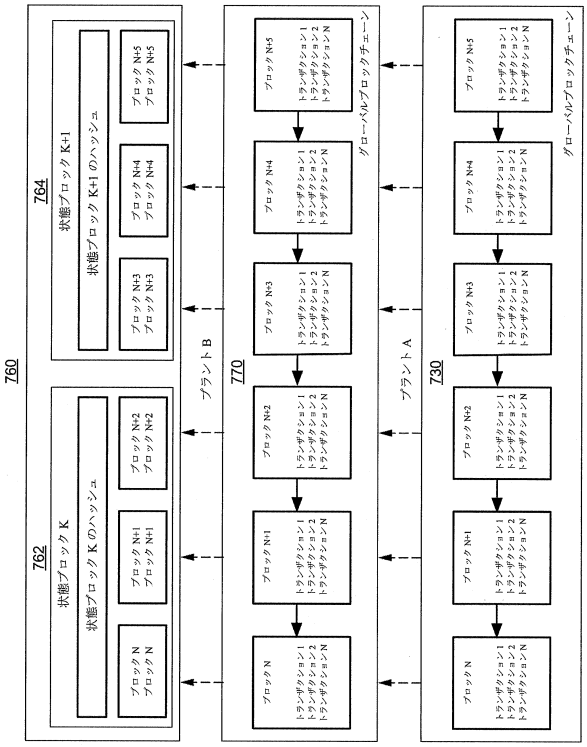
【図７Ａ】



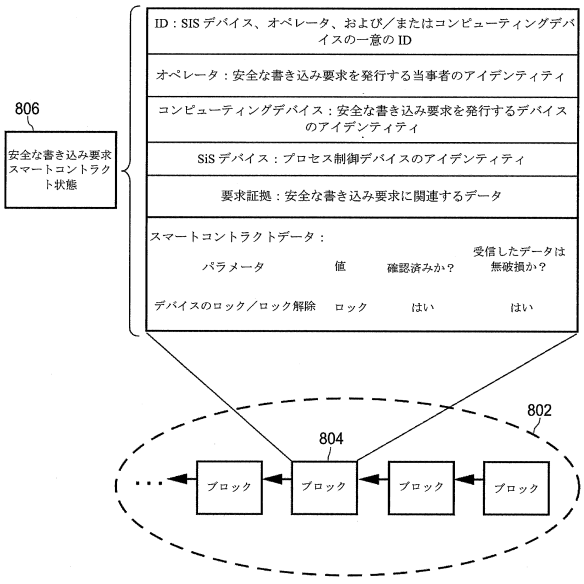
【図７Ｂ】


730
プラントA
グローバルブロックチェーン
ブロック N+4
ブロック N+3
ブロック N+2
ブロック N+1
ブロック N
トランザクション1
トランザクション2
トランザクションN
740
742
744
746
ローカルブロックチェーン
時間エポック E
750
752
754
時間エポック E+1

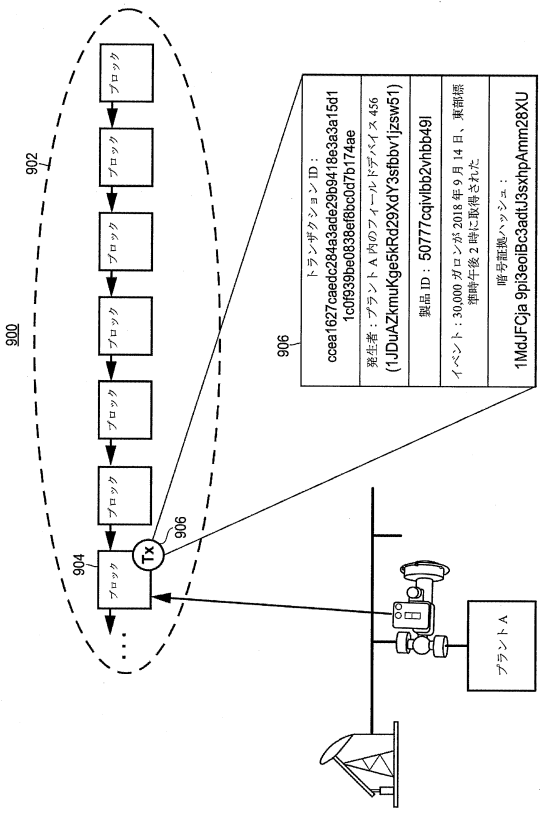
【図７Ｃ】


760
762
状態ブロック K のハッシュ
764
状態ブロック K+1 のハッシュ
770
プラントB
730
プラントA
グローバルブロックチェーン
ブロック N+5
ブロック N+4
ブロック N+3
ブロック N+2
ブロック N+1
ブロック N
トランザクション1
トランザクション2
トランザクションN

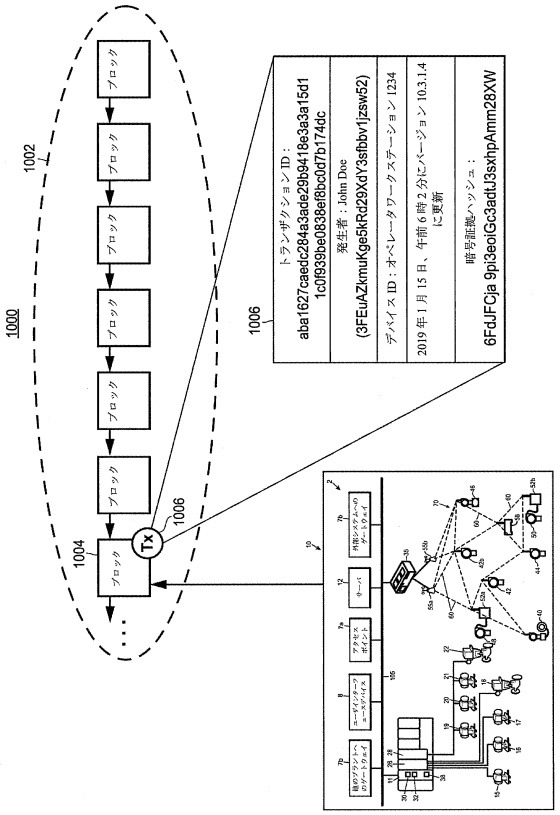
【図８】


806
安全な書き込み要求
スマートコントラクト状態
ID：SIS デバイス、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一意の ID
オペレータ：安全な書き込み要求を発行する当事者のアイデンティティ
コンピューティングデバイス：安全な書き込み要求を発行するデバイスのアイデンティティ
SiS デバイス：プロセス制御デバイスのアイデンティティ
要求証拠：安全な書き込み要求に関連するデータ
スマートコントラクトデータ：
パラメータ
値
確認済みか？
受信したデータは無破損か？
デバイスのロック／ロック解除
ロック
はい
はい
802
804
ブロック

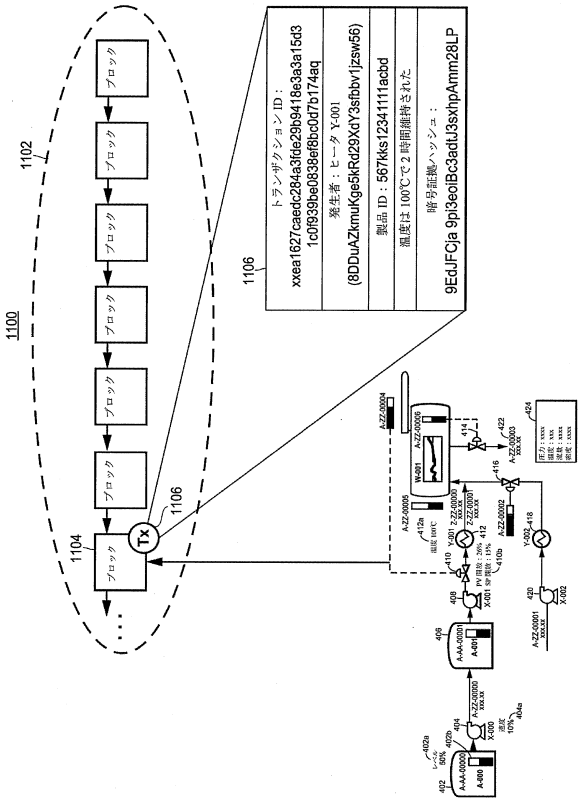
【図９】


900
902
904
906
Tx
ブロック
トランザクション ID：
ccea1627caaedc2844a3ade29b94118e3a3a15d1
1cdf939be0838ef8bc0d7b174ae
発生者：プラント A 内のフィールドデバイス 456
(1JDuAZkmuKge5kRd29XdY3sfbbv1jzsw51)
製品 ID： 50777cqivlbb2vhbb49I
イベント：30,000 ガロンが 2018 年 9 月 14 日、東都標準時午後 2 時に取得された
暗号証拠ハッシュ：
1MdJFCja 9pi3eoiBc3adtJ3sxhpAmm28XU
プラントA

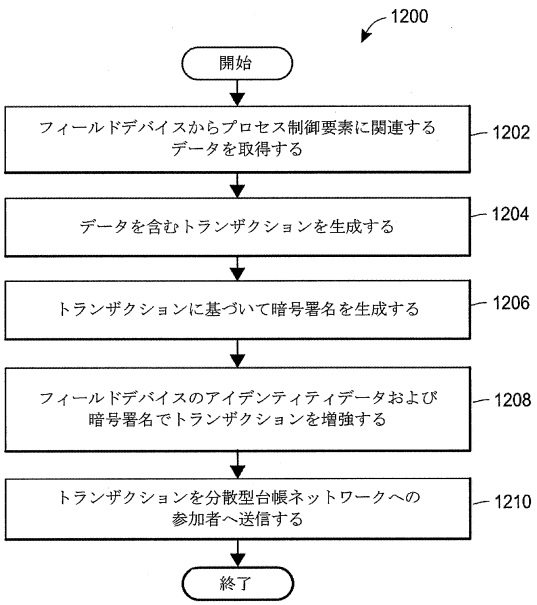
【図１０】



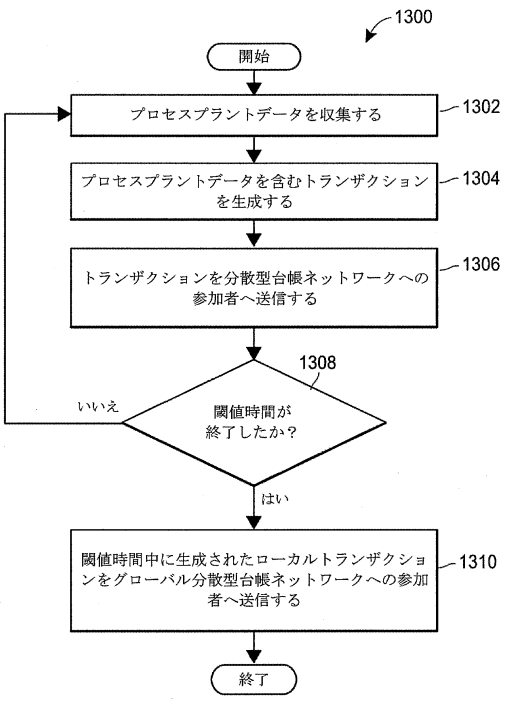
【図１１】



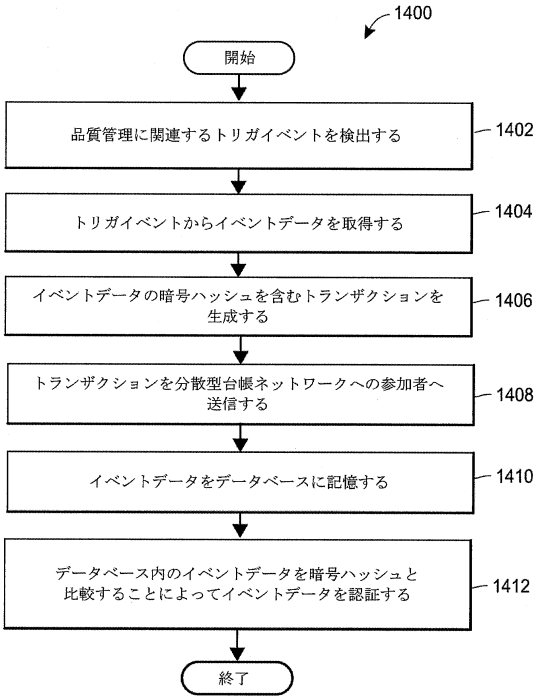
【図１２】



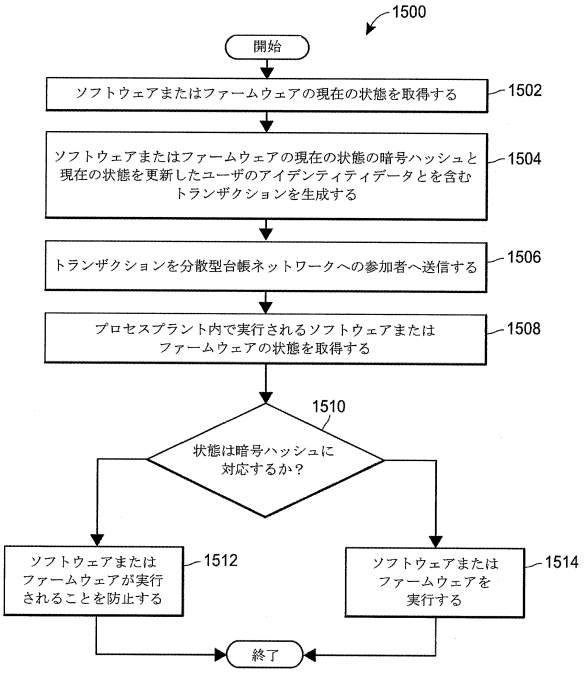
【図１３】



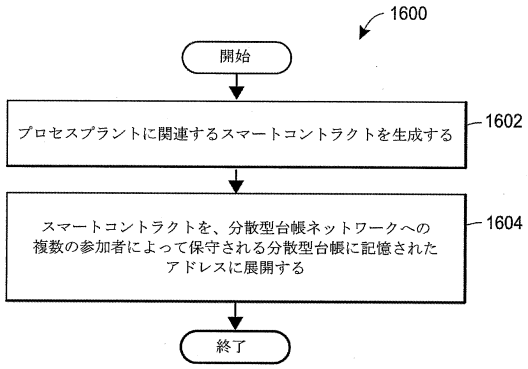
【図１４】



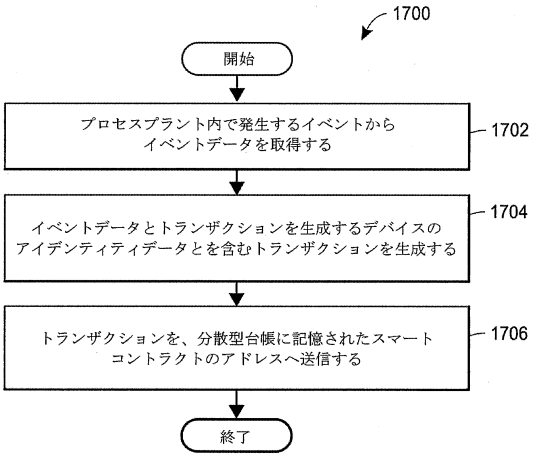
【図１５】



【図１６】



【図１７】



フロントページの続き

フィリピン共和国 マニラ パシグ シティ オルティガス センター ゴールドランド ミレニア スイーツ ユニット ２８０９
(72)発明者 レゼリー・レイブ
フィリピン共和国 マリキナ サン ロケ ミッドタウン サブデビジョン カプワ ストリート 7
審査官 田中 友章
(56)参考文献 国際公開第２０１８／１７７５２０（WO，A１）
米国特許出願公開第２０１８／０２８７７８０（ＵＳ，Ａ１）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０５Ｂ ２３／０２
Ｇ０６Ｑ １０／２０