(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7469133号
(P7469133)

(45)発行日　令和6年4月16日(2024.4.16)

(24)登録日　令和6年4月8日(2024.4.8)

(51)国際特許分類
G06F 21/64 (2013.01)
G06F 21/60 (2013.01)

FI
G06F 21/64
G06F 21/60 320

請求項の数 31 外国語出願 （全39頁）

(21)出願番号　特願2020-79266(P2020-79266)
(22)出願日　令和2年4月28日(2020.4.28)
(65)公開番号　特開2020-184335(P2020-184335A)
(43)公開日　令和2年11月12日(2020.11.12)
審査請求日　令和4年12月9日(2022.12.9)
(31)優先権主張番号　16/404,147
(32)優先日　令和1年5月6日(2019.5.6)
(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　ギャン・ワン
アメリカ合衆国 コネチカット州 ０６２６９ ストーズ ユニット ４１５５ フェアフィールド ウェイ ３７１
(72)発明者　マーク・ジェイ・ニクソン

最終頁に続く

(54)【発明の名称】　分散型台帳を使用するプライバシー保護型のビッグデータ共有のための枠組み

(57)【特許請求の範囲】

【請求項１】

分散型台帳を使用して記憶センターでプロセスプラント内の測定データを安全に記憶するための方法であって、

プロセスプラント内の工業プロセスを制御するための物理的機能を行うフィールドデバイスによって、前記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、前記プロセスプラント内の前記パラメータの前記測定値を取得することと、

前記測定値を暗号化することと、

前記暗号化された測定値を、前記暗号化された測定値を記憶する記憶センターに送信することと、

前記コンピューティングデバイスによって、前記暗号化された測定値のために前記記憶センターによって行われた記憶動作を表すトランザクションを取り出すための識別情報を取得することであって、前記トランザクションは分散型台帳内に含まれる、取得することと、

前記コンピューティングデバイスで、データ契約者から、前記測定値を取得するための要求を受信することと、

前記データ契約者に、前記トランザクションを取り出すための前記識別情報を送信することと、

前記データ契約者に、前記暗号化された測定値を復号するための復号情報を送信するこ

と、を含む、方法。
【請求項２】
前記データ契約者が、前記暗号化された測定値を取り出し、前記暗号化された測定値を、前記分散型台帳内に含まれる前記暗号化された測定値に対応する暗号ハッシュ値と比較して、前記暗号化された測定値の信頼性を検証する、請求項１に記載の方法。
【請求項３】
前記トランザクションが、前記暗号化された測定データを記憶する前記記憶センターの識別子と、前記暗号化された測定データを生成した前記コンピューティングデバイスの識別子と、前記暗号化された測定データを取り出すための識別子と、前記暗号化された測定データに対応する暗号ハッシュ値と、を含む、請求項１または請求項２に記載の方法。
【請求項４】
前記データ契約者に、前記トランザクションを取り出すための前記識別情報を送信することが、前記データ契約者に、前記暗号化された測定値を含む前記分散型台帳内の前記トランザクションに対応するトランザクション識別子を送信することを含む、請求項１から請求項３のいずれかに記載の方法。
【請求項５】
前記暗号化された測定値を復号するための復号情報を送信することが、前記データ契約者に、前記暗号化された測定値を復号するためのワンタイム暗号鍵を送信することを含む、請求項１から請求項４のいずれかに記載の方法。
【請求項６】
前記コンピューティングデバイスによって、前記プロセスプラント内の複数のパラメータの複数の測定値を取得することと、
前記複数の測定値の各々を暗号化することと、
前記複数の暗号化された測定値を複数の記憶センターに送信することと、をさらに含む、請求項１から請求項５のいずれかに記載の方法。
【請求項７】
前記データ契約者からの、前記複数の測定値のうちの少なくともいくつかを取得するための要求に応答して、前記データ契約者に、前記少なくともいくつかの測定値を記憶する前記複数の記憶センターのうちの少なくともいくつかの識別子を含むトランザクションを取り出すための識別情報を送信する、請求項６に記載の方法。
【請求項８】
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測定データを記憶するための方法であって、
コンピューティングデバイスで、前記測定データを生成および暗号化したデータ提供者から、暗号化された測定データを取得することと、
前記暗号化された測定データを記憶することと、
前記暗号化された測定データの表示を含むトランザクションを生成することと、
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内の少なくとも１人の他の参加者に、前記トランザクションを送信することと、
前記データ提供者に、前記暗号化された測定データを取り出すための識別情報を送信することと、
前記コンピューティングデバイスで、データ契約者から、前記暗号化された測定データの識別子を含む、前記暗号化された測定データの要求を受信することと、
前記要求に応答して、前記暗号化された測定データを前記データ契約者に送信することと、を含む、方法。
【請求項９】
トランザクションを生成することが、前記暗号化された測定データを記憶する前記コンピューティングデバイスの識別子と、前記暗号化された測定データを生成した前記データ提供者の識別子と、前記暗号化された測定データを取り出すための識別子と、前記暗号化された測定データに対応する暗号ハッシュ値と、を含む前記トランザクションを生成する

ことを含む、請求項８に記載の方法。
【請求項１０】
前記データ契約者が、前記暗号化された測定データを前記暗号ハッシュ値と比較して、前記暗号化された測定データの信頼性を検証する、請求項９に記載の方法。
【請求項１１】
前記暗号化された測定データを取り出すための識別情報を送信することが、前記データ提供者に、前記暗号化された測定データを含む前記分散型台帳内の前記トランザクションに対応するトランザクション識別子を送信することを含む、請求項８から請求項１０のいずれかに記載の方法。
【請求項１２】
前記トランザクションを生成することが、
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、を含む、請求項８から請求項１１のいずれかに記載の方法。
【請求項１３】
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内の少なくとも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１２に記載の方法。
【請求項１４】
分散型台帳ネットワーク上の検証ネットワークノードであって、
各々が測定データを生成および暗号化する１つ以上のデータ提供者と通信し、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するように構成された送受信機であって、前記分散型台帳データが、暗号化された測定データのセットの記憶動作を表すトランザクションを含む、送受信機と、
前記分散型台帳のコピーを記憶するように構成された記憶媒体と、
前記ピアネットワークノードから受信した前記分散型台帳データに合意ルールのセットを適用するように構成された検証器であって、前記分散型台帳データが前記合意ルールを満たす場合に、前記ピアネットワークノードから受信した前記分散型台帳データを前記分散型台帳の前記コピーに付加するようにさらに構成されている、検証器と、を備える、検証ネットワークノード。
【請求項１５】
前記ピアネットワークノードから受信した前記分散型台帳データが、前記暗号化された測定データのセットのうちの１つを記憶し、前記暗号化された測定データのセットの記憶動作を表す前記トランザクションのうちの１つを生成する記憶センターのアイデンティティ証明を含む、請求項１４に記載の検証ネットワークノード。
【請求項１６】
前記ピアネットワークノードから受信した分散型台帳データを付加するために、前記検証器が、
トランザクションのブロックに基づいて、暗号パズルを解くことと、
前記暗号パズルの解を前記トランザクションのブロックに追加することと、
前記トランザクションのブロックを前記分散型台帳の前記コピーに付加することと、
前記トランザクションのブロックを、前記分散型台帳ネットワーク内の前記ピアネットワークノードのうちの少なくとも１つに送信することと、を行うように構成されている、請求項１４または請求項１５に記載の検証ネットワークノード。
【請求項１７】
前記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のフォーマット要件、
前記ピアネットワークノードのうちのどれが、前記分散型台帳に、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ためのメカニズム、または
前記トランザクションの各々に含まれる前記暗号化された測定データのセットをハッシュするための暗号ハッシュアルゴリズム、のうちの少なくとも１つを含む、請求項１４から請求項１６のいずれかに記載の検証ネットワークノード。
【請求項１８】
各トランザクションが、暗号化された測定データのセットのための識別子と、前記暗号化された測定データのセットを記憶する記憶センターの識別子と、前記暗号化された測定データのセットを生成したデータ提供者の識別子と、前記暗号化された測定データのセットに対応する暗号ハッシュ値と、を含む、請求項１４から請求項１７のいずれかに記載の検証ネットワークノード。
【請求項１９】
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測定データを記憶するためのシステムであって、
プロセスプラント内に配設され、各々が工業プロセスを制御するための物理的機能を行う、１つ以上のデバイスと、
前記プロセスプラント内で実行されるコンピューティングデバイスであって、
１つ以上のプロセッサと、
通信ユニットと、
前記１つ以上のプロセッサおよび前記通信ユニットに連結され、かつ命令を記憶した、非一時的コンピュータ可読媒体と、を含む、コンピューティングデバイスと、を備え、
前記命令が、前記１つ以上のプロセッサによって実行されると、前記コンピューティングデバイスに、
前記プロセスプラント内のパラメータの測定値を前記１つ以上のデバイスから取得することと、
前記測定値を暗号化することと、
前記暗号化された測定値を、前記暗号化された測定値を記憶する記憶センターに送信することと、
前記暗号化された測定値のために前記記憶センターによって行われた記憶動作を表すトランザクションを取り出すための識別情報を取得することであって、前記トランザクションは分散型台帳内に含まれる、取得することと、
データ契約者から、前記測定値を取得するための要求を受信することと、
前記データ契約者に、前記トランザクションを取り出すための前記識別情報を送信することと、
前記データ契約者に、前記暗号化された測定値を復号するための復号情報を送信することと、を行わせる、システム。
【請求項２０】
前記データ契約者が、前記暗号化された測定値を取り出し、前記暗号化された測定値を、前記分散型台帳内に含まれる前記暗号化された測定値に対応する暗号ハッシュ値と比較して、前記暗号化された測定値の信頼性を検証する、請求項１９に記載の方法。
【請求項２１】
前記トランザクションが、前記暗号化された測定データを記憶する前記記憶センターの識別子と、前記暗号化された測定データを生成した前記コンピューティングデバイスの識別子と、前記暗号化された測定データを取り出すための識別子と、前記暗号化された測定データに対応する暗号ハッシュ値と、を含む、請求項１９または請求項２０に記載のシステム。
【請求項２２】
前記トランザクションを取り出すための前記識別情報を送信するために、前記命令は、前記コンピューティングデバイスに、前記データ契約者に、前記暗号化された測定値を含む前記分散型台帳内の前記トランザクションに対応するトランザクション識別子を送信させる、請求項１９から請求項２１のいずれかに記載のシステム。

【請求項２３】
前記暗号化された測定値を復号するための復号情報を送信するために、前記命令は、前記コンピューティングデバイスに、前記データ契約者に、前記暗号化された測定値を復号するためのワンタイム暗号鍵を送信させる、請求項１９から請求項２２のいずれかに記載のシステム。
【請求項２４】
前記命令が、前記コンピューティングデバイスに、
前記プロセスプラント内の複数のパラメータの複数の測定値を取得することと、
前記複数の測定値の各々を暗号化することと、
前記複数の暗号化された測定値を複数の記憶センターに送信することと、をさらに行わせる、請求項１９から請求項２３のいずれかに記載のシステム。
【請求項２５】
前記データ契約者からの、前記複数の測定値のうちの少なくともいくつかを取得するための要求に応答して、前記命令は、前記コンピューティングデバイスに、前記データ契約者に、前記少なくともいくつかの測定値を記憶する前記複数の記憶センターのうちの少なくともいくつかの識別子を含むトランザクションを取り出すための識別情報をさらに送信させる、請求項２４に記載のシステム。
【請求項２６】
前記少なくともいくつかの測定値が、データセット内に含まれ、前記データセットのサブセットとして異なる記憶センター内に記憶されている、請求項２５に記載のシステム。
【請求項２７】
安全に記憶された測定データを記憶センターおよび分散型台帳から取得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、データ提供者によって生成された測定データの要求を送信することと、
前記データ提供者から、暗号化された測定データの表示を含む分散型台帳内のトランザクションに対応するトランザクション識別子を受信することを含む、前記暗号化された測定データを記憶する記憶センターから前記測定データの暗号化バージョンを取り出すための識別情報を受信することと、
前記データ提供者から、前記暗号化された測定データを復号するための復号情報を受信することと、
前記暗号化された測定データを記憶する前記記憶センターの識別子を含む、前記分散型台帳から前記トランザクション識別子に関連付けられたトランザクションデータを取得することと、
前記識別された記憶センターに、前記暗号化された測定データの要求を送信することと、
前記暗号化された測定データを前記記憶センターから受信することと、
前記暗号化された測定データを前記分散型台帳内に含まれる前記暗号化された測定データの前記表示と比較することと、
前記暗号化された測定データが前記分散型台帳内に含まれる前記暗号化された測定データの前記表示に対応すると決定することに応答して、前記測定データを取得するために前記復号情報を使用して前記暗号化された測定データを復号することと、を含む、方法。
【請求項２８】
前記測定データが、測定データの複数のサブセットを有する測定データのセットであり、各サブセットは、異なる記憶センターに記憶されており、
前記データ提供者から、暗号化された測定データの各サブセットの表示を含む、前記分散型台帳内のトランザクションに対応するトランザクション識別子を受信することを含む、複数の記憶センターから測定データの各サブセットの暗号化バージョンを取り出すための識別情報を受信することと、
前記データ提供者から、前記暗号化された測定データの各サブセットを復号するための復号情報を受信することと、

前記複数の記憶センターの各々に、前記暗号化された測定データの対応するサブセットの要求を送信することと、
前記暗号化された測定データのサブセットを前記複数の記憶センターから受信することと、
前記測定データのサブセットを取得するために、前記サブセットのための前記対応する復号情報を使用して、前記暗号化された測定データの各サブセットを復号することと、
前記測定データのセットを生成するために、前記測定データの複数のサブセットを組み合わせることと、をさらに含む、請求項２７に記載の方法。
【請求項２９】
トランザクションデータを取得することが、前記暗号化された測定データを記憶する前記記憶センターの識別子と、前記暗号化された測定データを生成した前記データ提供者の識別子と、前記暗号化された測定データを取り出すための識別子と、前記暗号化された測定データに対応する暗号ハッシュ値と、を取得することを含む、請求項２７または請求項２８に記載の方法。
【請求項３０】
前記暗号化された測定データを前記分散型台帳内に含まれる前記暗号化された測定データの前記表示と比較することが、前記暗号化された測定データを前記暗号化された測定データに対応する前記暗号ハッシュ値と比較することを含む、請求項２９に記載の方法。
【請求項３１】
復号情報を受信することが、前記データ提供者から、前記暗号化された測定データを復号するためのワンタイム暗号鍵を受信することを含む、請求項２７から請求項３０のいずれかに記載の方法。
【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、より詳細には、プロセスプラント等のデータ提供者によって生成されたデータを安全に記憶するための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、一般に、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、一般に、「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り利用されるデータハイウェイは、有線通信パス、無線通信パス、または有線および無線通信パスの組み合わせを含むことができる。

【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、それら異なるデバイスによって実行される複数のアプリケーションを含む。１つ以上のワークステーションまたはコンピューティングデバイス内に備わる構成アプリケーションは、ユーザによる、プロセス制御モジュールの作成または変更、およびデータハイウェイを経由した、これらのプロセス制御モジュールの、専用分散型コントローラへのダウンロードを可能にする。典型的には、これらの制御モジュールは、通信可能に相互接続された機能ブロックで構成され、これらの機能ブロックは、それに対する入力に基づき制御スキーム内で機能を実行し、出力を制御スキーム内の他の機能ブロックに提供するオブジェクト指向プログラミングプロトコル内のオブジェクトである。また、構成アプリケーションは、データをオペレータに対して表示するため、かつオペレータによるプロセス制御ルーチン内の設定点等の設定の変更を可能にするために閲覧アプリケーションが使用するオペレータインターフェースを、構成設計者が作成または変更することを可能にし得る。各専用コントローラ、および一部の場合においては、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。

【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／または外部ネットワークおよびシステムへの相互接続は、企業および／または外部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】

「ビッグデータ」とは、一般に、従来のデータベース管理ツールおよび／またはデータ処理アプリケーション（例えば、関係データベースおよびデスクトップ統計パッケージ）が許容時間内にデータセットを管理できないほど非常に大規模、または複雑な１つ以上のデータセットの集合を指す。典型的には、ビッグデータを使用するアプリケーションはトランザクション型であり、エンドユーザ主導または集中型である。例えば、ウェブ検索エンジン、ソーシャルメディアアプリケーション、マーケティングアプリケーション、および小売アプリケーションは、ビッグデータを使用および操作する場合がある。ビッグデータは、最新のマルチプロセス、マルチコアサーバの並列処理能力を完全に利用できるようにする分散型データベースによってサポートされ得る。

【０００７】

現在、これらの大規模なデータセットを生成するプロセスプラント、病院等のデータ提供者と、大規模なデータセットを記憶する記憶センターとの間には信頼の欠落が存在する。典型的には、データ提供者は、単一の記憶センターと契約して大規模なデータセットを記憶する。しかしながら、単一の記憶センターのセキュリティが侵害されると、脆弱性が発生する。データ提供者は、プライバシーに対する懸念から、記憶センターとデータを共有することも望んでいない。さらに、分析会社およびディープラーニング会社等のデータ契約者は、典型的には、記憶センターによって提供されるデータセットの完全性を信頼しない。

【発明の概要】

【０００８】

プロセス制御システムおよび記憶センター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、構成要素、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。

【０００９】

プロセスプラント、記憶センター、およびデータ契約者等のデータ提供者間の信頼、プ

ライバシー、およびセキュリティの問題に対処するために、データ提供者は、生データを送信するのではなく、暗号化されたデータを記憶センターに送信する。データには、バルブ、タンク、ミキサ、ポンプ、熱交換器等の物理的物質を包含、変形、生成、または移送するプロセスの一部分で使用するためのプロセスプラント内のデバイスを含むフィールドデバイスまたはプロセスプラントエンティティによって生成された測定データを含み得る。測定データは、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み得る。測定データはまた、製品の温度、製品の体積、製品の質量、製品の密度、製品の圧力等を含む、プロセスプラントによって生産された物理的物質または製品の特性等の製品パラメータ値も含み得る。

【００１０】

データを暗号化し、暗号化されたデータを記憶センターに送信することにより、ハッカーが記憶センターに不正アクセスすることにより生データを取得できないため、データは攻撃を受けにくくなる。

【００１１】

さらに、暗号化された測定データを記憶センターに記憶することに加えて、記憶センターは、分散型台帳ネットワークにブロードキャストされる記憶動作に関するトランザクションを生成および検証することにより、分散型台帳を保守する。いくつかのシナリオでは、トランザクションは、暗号化された測定データを記憶する記憶センターの識別子と、暗号化された測定データを生成したデータ提供者の識別子と、暗号化された測定データを対応する記憶センターから取り出すための、暗号化された測定データの識別子と、暗号化された測定データの表示と、を含む。いくつかの実装形態では、暗号化された測定データの表示は、暗号化された測定データに対応する暗号ハッシュ値である。

【００１２】

次に、分析会社またはディープラーニング会社等のデータ契約者は、記憶センターから暗号化された測定データを取り出し、分散型台帳から暗号化された測定データの表示を取り出し、両者を比較して、暗号化された測定データの信頼性を検証することができる。さらに、データ提供者は、データ契約者がワンタイムパッド等の暗号化された測定データを復号するための復号情報を提供する。

【００１３】

いくつかの実装形態では、データ提供者は、暗号化された測定データのセットをいくつかのサブセットに分割する。次に、データ提供者は、暗号化されたサブセットを記憶する、異なる記憶センターに各サブセットを提供し、分散型台帳に記録されている暗号化されたサブセットの表示を含むトランザクションを生成する。次に、データ契約者が測定データまたは測定データのセットのうちの少なくともいくつかを要求すると、データ提供者は、それぞれの暗号化されたサブセットを記憶している記憶センターから、各暗号化されたサブセットを取り出すための識別情報をデータ契約者に提供する。また、データ提供者は、データ契約者がワンタイムパッド等の各暗号化されたサブセットを復号するための復号情報も提供する。次に、データ契約者は、各暗号化されたサブセットを復号し、このサブセットを結合して測定データのセットを生成する。

【００１４】

プロセスプラント、またはプロセスプラントによって生成された、暗号化された測定データを記憶する記憶センターで分散型台帳を利用することにより、各記憶センターまたは記憶センターのネットワークは、信頼できる、安全な、かつ不変の測定データの記録を提供することができる。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。さらに、分散型台帳の安全な、不変の、かつ信頼できない性質はまた、データ提供者とデータ契約者の両方が、データの完全性を保守し、プライバシーを確保するために記憶センターを信頼しない、記憶センター内でも特に重要である。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】
【００１５】
【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６】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例示的な分散型台帳を示す。
【図７】測定データのセットに対してデータ提供者によって行われる例示的な暗号化および分割技術を示す。
【図８】例示的な記憶センター、および記憶センターに記憶されている、対応する測定データセットまたはサブセットのブロック図を示す。
【図９】ブロックチェーン内に含まれる記憶センターによって生成される例示的なトランザクションを示す。
【図１０】測定データのセットを取り出すためのデータ提供者と、記憶センターと、データ契約者との間の例示的な対話を示す。
【図１１】測定データのセットを収集、記憶、および取り出すための、データ提供者と、記憶センターと、データ契約者との間の例示的な対話を示すメッセージ図である。
【図１２】プロセスプラント内の測定データを分散型台帳を使用して記憶センターに安全に記憶するための例示的な方法を表す流れ図を示す。
【図１３】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測定データを記憶するための例示的な方法を表す流れ図を示す。
【図１４】記憶センターと分散型台帳から安全に記憶された測定データを取得するための例示的な方法を表す流れ図を示す。
【発明を実施するための形態】
【００１６】
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。

【００１７】
台帳を共有するノードは、ここで分散型台帳ネットワークと称されるものを形成する。分散型台帳ネットワーク内のノードは、合意ルールのセットに従ってブロックチェーンへの変更を検証する（例えば、新しいトランザクションおよび／またはブロックが作成されるとき等）。合意ルールは、ブロックチェーンによって追跡される情報に依存し、チェーン自体に関するルールを含み得る。例えば、合意ルールは、変更の発生者がアイデンティ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）。
【００１８】
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。
【００１９】
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、様々な形態を採り得る。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。
【００２０】
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。
【００２１】
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。
【００２２】
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。

【００２３】

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層または個別のブロックチェーンを含む。第１の層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の層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。

【００２４】

一例では、分散型台帳は、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、リモートシステムにデータを送信するノードを検証することによって、保守され得る。検証ノードは、例えば、記憶センター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る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。次に、検証ノードは、ブロードキャストされたトランザクションを検証する。いくつかの実装形態では、記憶センターはまた、記憶センターが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、ブロードキャストされたトランザクションを検証するようにノードを検証している。

【００２５】

図１は、本明細書に記載される新規な分散型台帳技術のうちのいずれか１つ以上を利用し得る例示的なプロセスプラント１０のブロック図である。プロセスプラント１０（本明細書では、プロセス制御システム１０またはプロセス制御環境１０と言い換え可能である）は、フィールドデバイスによって作成されたプロセス測定値を表示する信号を受信し、この情報を処理して制御ルーチンを実装し、有線または無線プロセス制御通信リンクまたはネットワークを経由して他のフィールドデバイスへ送信されて、プラント１０内のプロセスの動作を制御する、１つ以上のプロセスコントローラを含む。典型的には、少なくとも１つのフィールドデバイスが物理的機能（例えば、バルブの開閉、温度の上昇または下降、測定、状況の検知等）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。

【００２６】

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、イーサネットプロトコル等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等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等、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。

【００２７】

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。ある実施形態においては、プロセス制御データハイウェイ１０５に対して通信可能に接続されるのに加えて、コントローラ１１はまた、例えば標準的な４～２０ｍＡデバイス、Ｉ／Ｏカード２６、２８、および／またはＦＯＵＮＤＡＴＩＯＮ（登録商標）Ｆｉｅｌｄｂｕｓプロトコル、ＨＡＲＴ（登録商標）プロトコル、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）プロトコル等の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も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。

【００２８】

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、ファンクションロックダイアグラム、または任意の他のソフトウェアプログラミング言語もしくは設計パラダイムを使用したもの等の任意の所望のソフトウェアフォーマットにおいて実装されてもよい。制御ルーチン３８は、ランダムアクセスメモリ（ＲＡＭ）または読み取り専用メモリ（ＲＯＭ）等の任意の所望のタイプのメモリ３２に記憶され得る。同様に、制御ルーチン３８は、例えば１つ以上のＥＰＲＯＭ、ＥＥＰＲＯＭ、特定用途向け集積回路（ＡＳＩＣ）、または任意の他のハードウェアもしくはファームウェア要素にハードコードされてもよい。したがって、コントローラ１１は、任意の所望の様式で制御ストラテジまたは制御ルーチンを実装するように構成することができる。

【００２９】

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もしくはそれと関連するときに成り立ち、または機能ブロックは、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。

【００３０】

有線フィールドデバイス１５～２２は、センサ、バルブ、トランスミッタ、ポジショナ等の任意のタイプのデバイスであってよく、一方でＩ／Ｏカード２６および２８は、任意の所望の通信またはコントローラプロトコルに適合する任意のタイプのＩ／Ｏデバイスであってもよい。図１では、フィールドデバイス１５～１８は、アナログラインまたは組み合わされたアナログおよびデジタルラインを経由してＩ／Ｏカード２６へ通信する、標準的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。

【００３１】

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。

【００３２】

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等を行う。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。

【００３３】

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、図１の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、ＷｉｒｅｌｅｓｓＨＡＲＴ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。

【００３４】

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。

【００３５】

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

【００３６】

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、例えば近距離通信（ＮＦＣ）およびＢｌｕｅｔｏｏｔｈ、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。

【００３７】

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。

【００３８】

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。

【００３９】

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、ならびに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。

【００４０】

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

参照すると、バックエンド環境は、例えば、オペレータワークステーション８、サーバコンピューティングデバイス１２、および／またはプロセスプラント１０のランタイム動作をサポートする機能を含む。いくつかの構成では、プロセスプラント１０のバックエンド環境に含まれる様々なコンピューティングデバイス、データベース、および他の要素および機材は、異なる物理位置に物理的に位置し得、それらのいくつかは、プロセスプラント１０に対してローカルであってもよく、それらのいくつかは遠隔していてもよい。

【００４１】

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。

【００４２】

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。

【００４３】

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、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）のうちのいずれか、および図示されていない他のコンポーネントは、記憶センター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。

【００４４】

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で実行またはホストされてもよい。より具体的には、リモートシステムは、プロセスプラント１０で生成されたデータを記憶する記憶センター２１０を含み得る。リモートシステムはまた、データを取り出し、リモートアプリケーション２０８を実行するデータ契約者も含み得る。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。リモートシステムで実行またはホストされ得、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で発生する状況および／またはイベントを監視および／または感知するアプリケーション、ならびにプロセスプラント１０で実行されているオンラインプロセス

自体の少なくとも一部分を監視するアプリケーションまたはサービスが挙げられる。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。

【００４５】

記憶センター２１０は、ネットワーク化されたサーバのリモートバンク、クラウドコンピューティングシステム、ネットワーク等、記憶センターのコンピューティングデバイスを含む任意の所望の方法で実装されてもよい。

【００４６】

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が設置され、かつ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、かつ動作させ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へ、エンドツーエンドの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が使用するために記憶センター２１０を含むリモートシステム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と無線ゲートウェイ２０５Ｂとの間）と記憶センター２１０との間に配設されたエッジゲートウェイ２１８を含む。

【００４７】

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。

【００４８】

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産業用プロトコルまたは他の好適な無線プロトコルを使用して通信してもよい。例えば、無線ＨＡＲＴ産業用プロトコルは１２８ビットＡＥＳ暗号化を提供し、それに応じて通信パス２０４Ａ、２０４Ｂが保護され得る。

【００４９】

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。

【００５０】

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。

【００５１】

エッジゲートウェイ２１８から記憶センター２１０に中継するデータは、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、配信され得る。重要なことには、エッジゲートウェイ２１８から記憶センター２１０へ中継するデータは、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保護される。より具体的には、エッジゲートウェイ２１８から記憶センター２１０に配信されるデータトラフィックの各セットまたはサブセットは、暗号鍵で暗号化され得る。いくつかの実装形態では、暗号鍵は、データのセットまたはサブセットを暗号化するために一度使用されるワンタイム暗号鍵またはワンタイムパッドである。記憶センター２１０は、ワンタイムパッドにアクセスできない場合がある。代わりに、記憶センター２１０は、暗号化されたデータセットまたはサブセットを記憶する。データ契約者がプロセスプラント１０または別のデータ提供者によって生成された特定のデータセットを要求すると、例えば、エッジゲートウェイ２１８は、ワンタイムパッドをデータ契約者に提供して、データ契約者が記憶センターから取り出す暗号化されたデータセットまたはサブセットを復号する。

【００５２】

いくつかの実装形態では、記憶センター２１０で、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データ契約者のコンピューティングデバイス等の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によって生成されたデータを含む、記憶センター２１０で利用可能なデータのうちの少なくともいくつかへのアクセスを達成することができる。

【００５３】

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記憶センター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によって動作される。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。

【００５４】

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典型的に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。

【００５５】

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。

【００５６】

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２１２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、記憶センター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。

【００５７】

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

図２は、記憶センター２１０を示しているが、各々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記憶センター２１０を含むことができる。図３は、暗号化された測定データに関連する記憶動作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。暗号化された測定データは、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、ユーザとの対話データ、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。暗号化された測定データにはまた、病院または任意の他の好適なデータ提供者によって生成されたデータも含まれる。

【００５８】

システム３００は、分散型台帳３１２と、記憶センター２１０等の記憶センターであり得るか、またはプロセスプラント１０で動作する、またはプロセスプラント１０で動作するデバイスと通信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。

【００５９】

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。

【００６０】

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、点線の左側および右側によってそれぞれ表される２つの時間枠４２０および４２２、ノードＡ４０２およびノードＢ４０４（２つの記憶センターであってもよい）、トランザクション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。

【００６１】

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成するノードを決定する。他の実施形態では、ブロックを形成するのに十分な数のトランザクションがプール内に存在するまで、トランザクション４０６をトランザクションのプールに追加してもよい。ノードＡ４０２は、新たに作成されたブロック４０８を時間４１２にネットワークへ送信してもよい。ブロック４０８を伝播する前または後に、ノードＡ４０２は、ノードＡ４０２の、ブロックチェーン４１８のコピーに、ブロック４０８を追加してもよい。

【００６２】

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

【００６３】

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

をそのブロックチェーン４１８に追加し、ブロック４０８のトランザクションによって拒否された状態データベース４１６に更新を行い得る。ノードＢ４０４は、次いで、時間３１４でブロック４０８をネットワークの残りへ送信し得る。

【００６４】

図５は、暗号化された測定データの記憶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の例示的なコンポーネントを示す。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。

【００６５】

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。

【００６６】

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。

【００６７】

図６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。

【００６８】

言い換えれば、トランザクションは、前述のアルゴリズム等の暗号ハッシュアルゴリズムを使用してハッシュされ、各トランザクションのハッシュはツリーに記憶され得る。ツリーが構築されると、同じレベルにある各隣接ノードのハッシュがまとめてハッシュされて、ツリー内のより高いレベルに存在する新しいノードを作成する。したがって、ツリーの最上位にあるノードまたはマークルルートは、ツリーの下に記憶されている各トランザクションのハッシュに依存する。各トランザクションはデータのセットを含み得る。デー

タのセットは、トランザクションのデータの識別、およびトランザクションの性質とトランザクションに伴う内容とを識別するトランザクションデータ（例えば、入力および出力アドレス、トランザクション値、ドキュメントハッシュ値、タイムスタンプ、トランザクション料金値等）を含み得る。

【００６９】

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。

【００７０】

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。

【００７１】

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、暗号化された測定データが記憶センター２１０に記憶されると、プロセスパラメータデータまたは製品パラメータデータ等の暗号化された測定データに関する記憶動作がブロックチェーン６００にアップロードされ得る。データ契約者等のチェーン外の当事者がデータを取得した場合でも、暗号化された測定データがブロックチェーンを使用して検証できるように、暗号化された測定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。

【００７２】

検証ネットワークノードは、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、暗号化された測定データを記憶する記憶センター２１０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検証することができる。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、新たな記憶動作データを追加するために、認可されたアイデンティティと一致する暗号アイデンティティ証明なしで新たな記憶動作データを追加しようと試みるいかなる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。各記憶センター２１０には、ブロックチェーンネットワークで記憶センター２１０に対応するものとして識別される公開鍵／秘密鍵の対を割り当てることができる。検証ネットワークノードが、認可された記憶センター２１０からではない記憶動作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。

【００７３】

分散型台帳を使用する安全な記憶システム

上述のように、プロセスプラント１０または別のデータ提供者は、暗号化された測定データを記憶センター２１０に送信する前に、測定データを生成および暗号化する。例えば、図２に示すように、フィールドデバイス２０２は、フィールドゲートウェイ２１２を介

してエッジゲートウェイ２１８に提供される測定データを生成する。次に、エッジゲートウェイは、例えば、ワンタイムパッド等の暗号鍵を使用して測定データを暗号化する。いくつかの実装形態では、データ提供者は、測定データのセットを生成し、測定データの各セットをサブセットに分割する。次に、データ提供者は、各サブセットを暗号化し、暗号化されたサブセットを異なる記憶センター２１０に送信する。

【００７４】

図７は、測定データのセットに対してプロセスプラント１０等のデータ提供者が行う例示的な暗号化および分割技術を示す。データ提供者１０は、第１のデータセット７０４（ＤＳ１）、第２のデータセット７０６（ＤＳ２）、第３のデータセット７０８（ＤＳ３）、および第ｎのデータセット７１０（ＤＳｎ）を含む測定データ７０２のセットを生成する。データ提供者１０は、各データセット７０４～７１０をいくつかのサブセットに分割する。例えば、データ提供者１０は、第１のデータセット７０４を第１のサブセット７０４ａ（ＥＤ１１）、第２のサブセット７０４ｂ（ＥＤ１２）、第３のサブセット７０４ｃ（ＥＤ１３）、および第ｎのサブセット７０４ｎ（ＥＤ１ｎ）に分割する。データ提供者１０はまた、異なる秘密鍵７２０～７２６（ＳＫ１、ＳＫ２、ＳＫ３、ＳＫｎ）を使用して測定データの各サブセットも暗号化する。いくつかの実装形態では、秘密鍵は、測定データの対応するサブセットを暗号化するために一度使用されるワンタイム暗号鍵である。次に、データ契約者が特定のサブセットを含む測定データのうちの少なくともいくつかを要求すると、データ提供者１０は、特定のサブセットを暗号化するために使用されるワンタイム暗号鍵をデータ契約者に提供して、特定のサブセットを復号する。そのワンタイム暗号鍵は、任意の他のサブセットまたは測定データのセットを復号するために使用することはできない。

【００７５】

次に、測定データの暗号化されたサブセットは、異なる記憶センター２１０に記憶される。これは、ＳＣ０００００１（参照番号２１０ａ）、ＳＣ０００１０（参照番号２１０ｂ）、ＳＣ１０００００（参照番号２１０ｃ）、ＳＣ０１１０１（参照番号２１０ｄ）、ＳＣ０１００１（参照番号２１０ｅ）、ＳＣ００１０１（参照番号２１０ｆ）、ＳＣ０１０１１（参照番号２１０ｇ）、ＳＣ０１０１０（参照番号２１０ｈ）、ＳＣ１０１０１（参照番号２１０ｉ）、およびＳＣ０１１１０（参照番号２１０ｊ）を含むいくつかの記憶センター２１０ａ～２１０ｊを示す図８に示されている。暗号化された測定データ８０２（ＥＤｉ１）のｉ番目のセットの第１のサブセットは、ＳＣ０１００１（参照番号２１０ｅ）に記憶され、暗号化された測定データ８０４（ＥＤｉ２）のｉ番目のセットの第２のサブセットは、ＳＣ１０００００（参照番号２１０ｃ）に記憶され、暗号化された測定データ８０６（ＥＤｉ３）のｉ番目のセットの第３のサブセットは、ＳＣ０００１０（参照番号２１０ｂ）に記憶され、暗号化された測定データ８０８（ＥＤｉｎ）のｉ番目のセットの第ｎのサブセットは、ＳＣ１０１０１（参照番号２１０ｉ）に記憶されている。

【００７６】

暗号化された測定データのセットまたはサブセットが特定の記憶センターに記憶されると、記憶センターは、記憶動作を表すトランザクションを生成し、その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する。次に、トランザクションは、他の記憶センター等の検証ノードによって検証され、ブロックに含まれる。図９は、ブロックチェーン等の分散型台帳９０２に含めることができる例示的なトランザクション９０４～９１０を示す。分散型台帳９０２は、図６を参照して上述した分散型台帳６００と同様であり得る。いずれにしても、各トランザクション９０４～９１０は、トランザクション識別子（ＩＤ）（例えば、「１」）、暗号化された測定データのセットまたはサブセットを生成したデータ提供者のデータ提供者ＩＤ（例えば、「ＤＣ」）、暗号化された測定データの特定のセットまたはサブセットを識別するデータセットＩＤ（例えば、「ＥＤｉ１」）、暗号化された測定データのセットまたはサブセットを記憶する記憶センターを識別する記憶センターＩＤ（例えば、「ＳＣ０１００１」）、および暗号化された測定データのセットまたはサブセットに対応する暗号ハッシュ値等の、暗号化された測定データのセット

またはサブセットの表示を含むことができる。

【００７７】

いくつかの実装形態では、記憶センター２１０は、トランザクションＩＤ等のトランザクションデータをデータ提供者１０に提供する。次に、データ契約者が測定データのセットを要求すると、データ提供者１０は、分散型台帳から必要な情報を取り出すためにトランザクションＩＤをデータ契約者に提供することができる。この一例が図１０に示されている。図１０に示すように、データ契約者１０００は、データ提供者１０からの測定データのセットを要求する。測定データのセットは、暗号化された測定データのサブセットとして、いくつかの記憶センターＳＣ０１００１（参照番号２１０ｅ）、ＳＣ１００００（参照番号２１０ｃ）、ＳＣ０００１０（参照番号２１０ｂ）、およびＳＣ１０１０１（参照番号２１０ｉ）に記憶される。暗号化された測定データの各サブセットは、分散型台帳内のトランザクションでも参照される。

【００７８】

要求に応答して、データ提供者１０は、データ契約者１０００に、セット内の暗号化された測定データのサブセットを参照する、分散型台帳内のトランザクションのブロック情報またはトランザクションデータを提供する。これには、分散型元帳から、対応するトランザクションを取り出すために使用できるトランザクションＩＤを含むことができる。各トランザクションについて、データ契約者１０００は、暗号化された測定データのセットまたはサブセットを生成したデータ提供者のデータ提供者ＩＤ（例えば、「ＤＣ」）、暗号化された測定データの特定のセットまたはサブセットを識別するデータセットＩＤ（例えば、「ＥＤｉ１」）、暗号化された測定データのセットまたはサブセットを記憶する記憶センターを識別する記憶センターＩＤ（例えば、「ＳＣ０１００１」）、および暗号化された測定データのセットまたはサブセットに対応する暗号ハッシュ値等の、暗号化された測定データのセットまたはサブセットの表示を取得することができる。

【００７９】

データ提供者１０はまた、データ契約者１０００に、暗号化された測定データの各サブセットを復号するためのワンタイム暗号鍵またはワンタイムパッドを提供する。上記のように、データ提供者１０は、サブセットに固有のワンタイム暗号鍵を使用して、暗号化された測定データの各サブセットを暗号化することができる。したがって、データ提供者１０は、これらのワンタイム暗号鍵をデータ契約者１０００に提供し、それにより、データ契約者１０００は、暗号化された測定データの各サブセットを復号し、測定データのサブセットを組み合わせて測定データのセットを生成することができる。

【００８０】

いくつかの実装形態では、データ契約者１０００は、セット内の暗号化された測定データのサブセットを参照するトランザクションＩＤの各々をデータ提供者１０から取得し、対応するトランザクションを分散型元帳から取り出す。取り出した各トランザクションについて、データ契約者１０００は、記憶センターＩＤに基づいて、暗号化された測定データのサブセットを記憶する記憶センターのアイデンティティを取得する。次に、データ契約者１０００は、データセットＩＤに対応する暗号化された測定データのサブセットの要求を、識別された記憶センター２１０に送信する。したがって、記憶センター２１０は、データセットＩＤに対応する暗号化された測定データのサブセットを取り出し、それをデータ契約者１０００に提供する。

【００８１】

さらに、データ契約者１０００は、暗号化された測定データのサブセットを、トランザクションに含まれる暗号化された測定データのサブセットに対応する暗号ハッシュ値と比較する。例えば、データ契約者１０００は、暗号化された測定データのサブセットに対して暗号ハッシュアルゴリズムを行い、その結果の出力がトランザクションに含まれる暗号ハッシュ値と同じであるかどうかを決定することができる。その結果の出力が暗号ハッシュ値と同じである場合、データ契約者１０００は、暗号化された測定データのサブセットが改ざんされていないと決定し、その信頼性を検証することができる。一方、その結果の

出力が暗号ハッシュ値と異なる場合、データ契約者１０００は、暗号化された測定データのサブセットが改ざんされていると決定し、その分析に測定データを使用しないか、または測定データをそれ以上処理しない。

【００８２】

その結果の出力が暗号ハッシュ値と同じである場合、データ契約者１０００は、ワンタイム暗号鍵等、データ提供者１０によって提供された復号情報を使用して、暗号化された測定データのサブセットを復号する。データ契約者１０００は、暗号化された測定データの各サブセットについてこのプロセスを繰り返して測定データのサブセットを生成し、サブセットを組み合わせて測定データのセットを生成することができる。

【００８３】

図１１は、このプロセスを、データ提供者１０と、記憶センター２１０と、データ契約者１０００と、の間の例示的な対話を示す通信図１１００で、より詳細に示している。プロセスプラント等のデータ提供者１０は、１１０２で、例えば、フィールドデバイス２０２、またはプロセスプラント１０で動作するプロセスプラントエンティティから測定データを取得する。測定データは、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プロセスパラメータ値を含み得る。測定データはまた、製品の温度、製品の体積、製品の質量、製品の密度、製品の圧力等を含むプロセスプラントが生産した物理的物質または製品の特性等の製品パラメータ値を含み得る。次に、データ提供者１０は、１１０４で、暗号鍵を使用して測定データを暗号化する。いくつかの実装形態では、データ提供者１０は、同時にまたは時間間隔内（例えば、３０秒の時間間隔内、１分の時間間隔内等）で収集したいくつかの測定値を含む測定データのセットを生成する。次に、データ提供者１０は、測定データのセットをいくつかのサブセットに分割する。例えば、測定データのセットは、１００個の測定値と、測定の時間、プロセスパラメータ、プロセスプラントエンティティ、および／または測定値に対応するフィールドデバイス等の測定値に関する、対応する情報と、を含むことができる。データ提供者１０は、１００個の測定値を、各々が１００個の測定値のうちの２５個を含む、測定データの４つのサブセットに分割することができる。次に、データ提供者１０は、異なる暗号鍵または固有のワンタイム暗号鍵を使用して、測定データの各サブセットを暗号化することができる。

【００８４】

次いで、データ提供者１０は、１１０６で、暗号化された測定データのセットまたは暗号化された測定データのセットのサブセットを記憶センター２１０に提供する。いくつかの実装形態では、データ提供者１０は、暗号化された測定データの各サブセットを異なる記憶センター２１０に提供するか、またはサブセットのうちの少なくとも２つを異なる記憶センター２１０に提供することができる。いずれにしても、記憶センター２１０は、１１０８で暗号化された測定データを記憶し、１１１０で記憶動作を表すトランザクションを生成する。トランザクションは、トランザクションＩＤ（例えば、「１」）、暗号化された測定データのセットまたはサブセットを生成したデータ提供者のデータ提供者ＩＤ（例えば、「ＤＣ」）、暗号化された測定データの特定のセットまたはサブセットを識別するデータセットＩＤ（例えば、「ＥＤｉ１」）、暗号化された測定データのセットまたはサブセットを記憶する記憶センターを識別する記憶センターＩＤ（例えば、「ＳＣ０１０００１」）、および暗号化された測定データのセットまたはサブセットに対応する暗号ハッシュ値等の、暗号化された測定データのセットまたはサブセットの表示を含むことができる。

【００８５】

記憶センター２１０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、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分散型台帳のブロック内に含めることができる。次に、記憶センター２１０は、１１１２で、トランザクションのトランザクションＩＤ、または分散型台帳内のトランザクションを識別する任意の他の好適な情報等のブロック情報をデータ提供者１０に提供する。

【００８６】
データ契約者１０００が１１１４で測定データのセットを含むデータ提供者１０からの測定データを要求すると、データ提供者１０は、１１１６で、分散型台帳からの暗号化された測定データのセットを含むトランザクションを取り出すためのトランザクションＩＤおよび暗号化された測定データのセットを復号するためのワンタイム暗号鍵等のブロック情報を提供する。測定データのセットがいくつかのサブセットに分割されると、データ提供者１０は、暗号化された測定データの各サブセットを取り出し、かつ復号するためのトランザクションＩＤおよびワンタイム暗号鍵を提供することができる。いずれにしても、データ契約者１０００は、トランザクションＩＤに対応するトランザクションを分散型台帳から取り出す。取り出した各トランザクションについて、データ契約者１０００は、記憶センターＩＤに基づいて、暗号化された測定データのサブセットを記憶する記憶センターのアイデンティティを取得する。次に、データ契約者１０００は、１１１８で、データセットＩＤに対応する暗号化された測定データのサブセットの要求を、識別された記憶センター２１０に送信する。したがって、記憶センター２１０は、データセットＩＤに対応する暗号化された測定データのサブセットを取り出し、それを１１２０でデータ契約者１０００に提供する。
【００８７】
さらに、データ契約者１０００は、暗号化された測定データのサブセットを、トランザクション内に含まれる暗号化された測定データのサブセットに対応する暗号ハッシュ値と比較する。例えば、データ契約者１０００は、暗号化された測定データのサブセットに対して暗号ハッシュアルゴリズムを行い、その結果の出力がトランザクションに含まれる暗号ハッシュ値と同じであるかどうかを決定することができる。その結果の出力が暗号ハッシュ値と同じである場合、データ契約者１０００は、暗号化された測定データのサブセットが改ざんされていないと決定し、その信頼性を検証することができる。一方、その結果の出力が暗号ハッシュ値と異なる場合、データ契約者１０００は、暗号化された測定データのサブセットが改ざんされていると決定し、その分析に測定データを使用しないか、または測定データをそれ以上処理しない。
【００８８】
その結果の出力が暗号ハッシュ値と同じである場合、データ契約者１０００は、１１２２で、ワンタイム暗号鍵等、データ提供者１０によって提供された復号情報を使用して、暗号化された測定データのサブセットを復号する。データ契約者１０００は、暗号化された測定データの各サブセットについてこのプロセスを繰り返して測定データのサブセットを生成し、サブセットを組み合わせて測定データのセットを生成することができる。
【００８９】
図１２は、プロセスプラント内の測定データを分散型台帳を使用して記憶センターに安全に記憶するための例示的な方法１２００を表す流れ図を示す。方法１２００は、プロセスプラント１０内のエッジゲートウェイ２１８、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。
【００９０】
ブロック１２０２において、プロセス制御要素に関連するデータは、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。測定データは、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）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、製品のため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。いくつかの実装形態では、エッジゲートウェイ２１８は、同時にまたは時間間隔内（例えば、３０秒の時間間隔内、１分の時間間隔内等

）で収集したいくつかの測定値を含む測定データのセットを取得する。次に、エッジゲートウェイ２１８は、測定データのセットをいくつかのサブセットに分割する。次に、ブロック１２０４において、測定データは暗号化される。例えば、エッジゲートウェイ２１８は、異なる暗号鍵または固有のワンタイム暗号鍵を使用して、測定データの各サブセットを暗号化することができる。

【００９１】

ブロック１２０６において、暗号化された測定データのセットは、記憶センター２１０に送信される。いくつかの実装形態では、暗号化された測定データの各サブセットは、異なる記憶センター２１０に送信されるか、またはサブセットのうちの少なくとも２つは、異なる記憶センター２１０に送信される。暗号化された測定データのセットの受信に応答して、記憶センター２１０は、そのセットを記憶し、記憶動作を表すトランザクションを生成する。記憶センター２１０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て、分散型台帳に含める。次に、ブロック１２０８において、エッジゲートウェイ２１８は、トランザクションのトランザクションＩＤ、または分散型台帳内のトランザクションを識別する任意の他の好適な情報等のブロック情報を記憶センターから受信する。

【００９２】

データ契約者１０００からの測定データのセットの要求に応答して（ブロック１２１０）、エッジゲートウェイ２１８は、分散型台帳からの暗号化された測定データのセットを含むトランザクションを取り出すためのトランザクションＩＤを送信し（ブロック１２１２）、暗号化された測定データのセットを復号するためのワンタイム暗号鍵等のブロック情報を送信する（ブロック１２１４）。測定データのセットがいくつかのサブセットに分割されると、エッジゲートウェイ２１８は、暗号化された測定データの各サブセットを取り出し、かつ復号するためのトランザクションＩＤおよびワンタイム暗号鍵を提供することができる。

【００９３】

このようにして、データ契約者１０００は、分散型台帳からトランザクションＩＤ（複数可）に対応するトランザクション（複数可）を取り出し、暗号化された測定データを記憶する記憶センター（複数可）を識別し、暗号化された測定データの識別情報を識別された記憶センター（複数可）に提供して暗号化された測定データを取り出すことができる。データ契約者はまた、暗号化された測定データを分散型台帳内のトランザクション（複数可）に含まれる暗号化された測定データに対応する暗号化ハッシュ値（複数可）と比較することによって、暗号化された測定データの信頼性を検証することもできる。さらに、データ契約者１０００は、ワンタイム暗号鍵（複数可）を使用して、暗号化された測定データを復号することができる。

【００９４】

図１３は、複数の参加者が保守する分散型台帳を使用して測定データを記憶するための例示的な方法１３００を表す流れ図を示す。方法１３００は、記憶センターのコンピューティングデバイス等の記憶センター２１０によって実行され得る。

【００９５】

ブロック１３０２において、記憶センター２１０は、暗号化された測定データのセットまたは暗号化された測定データのサブセットであり得る、暗号化された測定データを取得し、他のサブセットは異なる記憶センターに提供される。暗号化された測定データは、プロセスプラント、病院、または任意の他の好適な大規模なデータセットのソース等のデータ提供者１０から取得することができる。

【００９６】

次に、ブロック１３０４において、記憶センター２１０は、暗号化された測定データを、データセットＩＤ等の暗号化された測定データを取り出すための識別子とともに記憶する。暗号化された測定データを記憶することに加えて、記憶センター２１０は、記憶動作を表し、暗号化された測定データの表示を含むトランザクションを生成する（ブロック１

３０６）。トランザクションは、トランザクションＩＤ、暗号化された測定データのセットまたはサブセットを生成したデータ提供者のデータ提供者ＩＤ、暗号化された測定データの特定のセットまたはサブセットを識別するデータセットＩＤ、暗号化された測定データのセットまたはサブセットを記憶する記憶センターを識別する記憶センターＩＤ、および暗号化された測定データのセットまたはサブセットに対応する暗号ハッシュ値等の、暗号化された測定データのセットまたはサブセットの表示を含むことができる。

【００９７】

記憶センター２１０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、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分散型台帳のブロック内に含めることができる。（ブロック１３０８）。次に、記憶センター２１０は、トランザクションのトランザクションＩＤ、または分散型台帳内のトランザクションを識別する任意の他の好適な情報等のブロック情報をデータ提供者１０に提供する（ブロック１３１０）。

【００９８】

暗号化された測定データの、暗号化された測定データを識別するデータセットＩＤを含む、データ契約者１０００からの要求に応答して（ブロック１３１２）、記憶センター２１０は、暗号化された測定データをデータ契約者に提供する（ブロック１３１４）。

【００９９】

図１４は、記憶センターと分散型台帳から安全に記憶された測定データを取得するための例示的な方法１４００を表す流れ図を示す。流れ図１４００は、データ契約者のコンピューティングデバイス等のデータ契約者１０００によって実行され得る。

【０１００】

ブロック１４０２において、データ契約者１０００は、プロセスプラント等のデータ提供者１０からの測定データの要求を送信する。測定データの要求は、最新の時間間隔（例えば、直前の３０秒）に対応する測定データのセット等、特定の測定データのセットに対するものであり得る。ブロック１４０４において、データ契約者１０００は、記憶センター２１２に記憶された測定データのセットの暗号化バージョンを参照する、分散型台帳内のトランザクションを取り出すためのトランザクションＩＤ、および暗号化された測定データを復号するためのワンタイム暗号鍵を含むブロック情報を受信する。測定データのセットがいくつかのサブセットに分割されると、データ提供者１０は、暗号化された測定データの各サブセットを取り出し、かつ復号するためのトランザクションＩＤおよびワンタイム暗号鍵を提供することができる。

【０１０１】

データ契約者１０００は、トランザクションＩＤに対応するトランザクションを分散型台帳から取り出す（ブロック１４０６）。取り出した各トランザクションについて、データ契約者１０００は、記憶センターＩＤに基づいて、暗号化された測定データのサブセットを記憶する記憶センターのアイデンティティおよびデータセットＩＤ等の、暗号化された測定データのサブセットの識別子を取得する。次に、データ契約者１０００は、データセットＩＤに対応する暗号化された測定データのサブセットの要求を、識別された記憶センター２１０に送信する（ブロック１４０８）。したがって、記憶センター２１０は、データセットＩＤに対応する暗号化された測定データのサブセットを取り出し、それをデータ契約者１０００に提供する（ブロック１４１０）。

【０１０２】

さらに、データ契約者１０００は、暗号化された測定データのサブセットを、トランザクションに含まれる暗号化された測定データのサブセットに対応する暗号ハッシュ値と比較する（ブロック１４１２）。例えば、データ契約者１０００は、暗号化された測定データのサブセットに対して暗号ハッシュアルゴリズムを行い、その結果の出力が暗号ハッシュ値と同じであるかどうかを決定することができる。その結果の出力が暗号ハッシュ値と同じである場合、データ契約者１０００は、暗号化された測定データのサブセットが改ざんされていないと決定し、その信頼性を検証することができる。一方、その結果の出力が

暗号ハッシュ値と異なる場合、データ契約者１０００は、暗号化された測定データのサブセットが改ざんされていると決定し、その分析に測定データを使用しないか、または測定データをそれ以上処理しない。

【０１０３】

その結果の出力が暗号ハッシュ値と同じである場合、データ契約者１０００は、ワンタイム暗号鍵等、データ提供者１０によって提供された復号情報を使用して、暗号化された測定データのサブセットを復号する（ブロック１４１４）。データ契約者１０００は、暗号化された測定データの各サブセットについてこのプロセスを繰り返して測定データのサブセットを生成し、サブセットを組み合わせて測定データのセットを生成することができる。

【０１０４】

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。

【０１０５】

１．分散型台帳を使用して記憶センターでプロセスプラント内の測定データを安全に記憶するための方法であって、プロセスプラント内の工業プロセスを制御するための物理的機能を行う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、プロセスプラント内のパラメータの測定値を取得することと、測定値を暗号化することと、暗号化された測定値を、暗号化された測定値を記憶する記憶センターに送信することと、コンピューティングデバイスによって、暗号化された測定値のために記憶センターによって行われた記憶動作を表すトランザクションを取り出すための識別情報を取得することであって、トランザクションは分散型台帳内に含まれる、取得することと、コンピューティングデバイスで、データ契約者から、測定値を取得するための要求を受信することと、データ契約者に、トランザクションを取り出すための識別情報を送信することと、データ契約者に、暗号化された測定値を復号するための復号情報を送信することと、を含む、方法。

【０１０６】

２．データ契約者が、暗号化された測定値を取り出し、暗号化された測定値を、分散型台帳内に含まれる暗号化された測定値に対応する暗号ハッシュ値と比較して、暗号化された測定値の信頼性を検証する、態様１に記載の方法。

【０１０７】

３．トランザクションが、暗号化された測定データを記憶する記憶センターの識別子と、暗号化された測定データを生成したコンピューティングデバイスの識別子と、暗号化された測定データを取り出すための識別子と、暗号化された測定データに対応する暗号ハッシュ値と、を含む、態様１または２のいずれか１つに記載の方法。

【０１０８】

４．データ契約者に、トランザクションを取り出すための識別情報を送信することが、データ契約者に、暗号化された測定値を含む分散型台帳内のトランザクションに対応するトランザクション識別子を送信することを含む、態様１～３のいずれか１つに記載の方法。

【０１０９】

５．暗号化された測定値を復号するための復号情報を送信することが、データ契約者に、暗号化された測定値を復号するためのワンタイム暗号鍵を送信することを含む、態様１～４のいずれか１つに記載の方法。

【０１１０】

６．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複数のパラメータの複数の測定値を取得することと、複数の測定値の各々を暗号化することと、複数の暗号化された測定値を複数の記憶センターに送信することと、をさらに含む、態様１～５のいずれか１つに記載の方法。

【０１１１】

７．データ契約者からの、複数の測定値のうちの少なくともいくつかを取得するための

要求に応答して、データ契約者に、少なくともいくつかの測定値を記憶する複数の記憶センターのうちの少なくともいくつかの識別子を含むトランザクションを取り出すための識別情報を送信する、態様１～６のいずれか１つに記載の方法。

【０１１２】

８．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測定データを記憶するための方法であって、コンピューティングデバイスで、測定データを生成および暗号化したデータ提供者から、暗号化された測定データを取得することと、暗号化された測定データを記憶することと、暗号化された測定データの表示を含むトランザクションを生成することと、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内の少なくとも１人の他の参加者に、トランザクションを送信することと、データ提供者に、暗号化された測定データを取り出すための識別情報を送信することと、コンピューティングデバイスで、データ契約者から、暗号化された測定データの識別子を含む、暗号化された測定データの要求を受信することと、要求に応答して、暗号化された測定データをデータ契約者に送信することと、を含む、方法。

【０１１３】

９．トランザクションを生成することが、暗号化された測定データを記憶するコンピューティングデバイスの識別子と、暗号化された測定データを生成したデータ提供者の識別子と、暗号化された測定データを取り出すための識別子と、暗号化された測定データに対応する暗号ハッシュ値と、を含むトランザクションを生成することを含む、態様８に記載の方法。

【０１１４】

１０．データ契約者が、暗号化された測定データを暗号ハッシュ値と比較して、暗号化された測定データの信頼性を検証する、態様８または態様９のいずれか１つに記載の方法。

【０１１５】

１１．暗号化された測定データを取り出すための識別情報を送信することが、データ提供者に、暗号化された測定データを含む分散型台帳内のトランザクションに対応するトランザクション識別子を送信することを含む、態様８～１０のいずれか１つに記載の方法。

【０１１６】

１２．トランザクションを生成することが、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８～１１のいずれか１つに記載の方法。

【０１１７】

１３．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内の少なくとも１人の他の参加者へ送信することと、をさらに含む、態様８～１２のいずれか１つに記載の方法。

【０１１８】

１４．分散型台帳ネットワーク上の検証ネットワークノードであって、各々が測定データを生成および暗号化する１つ以上のデータ提供者と通信し、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するように構成された送受信機であって、分散型台帳データが、暗号化された測定データのセットの記憶動作を表す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検証器であって、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、検証器と、を備える、検証ネットワークノード。

【０１１９】

１５．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が、暗号化された測定データのセットのうちの１つを記憶し、暗号化された測定データのセットの記憶動作を表す

トランザクションのうちの１つを生成する記憶センターのアイデンティティ証明を含む、態様１４に記載の検証ネットワークノード。

【０１２０】

１６．ピアネットワークノードから受信した分散型台帳データを付加するために、検証器が、トランザクションのブロックに基づいて、暗号パズルを解くことと、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のコピーに付加することと、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内のピアネットワークノードのうちの少なくとも１つに送信することと、を行うように構成されている、態様１４または態様１５のいずれか１つに記載の検証ネットワークノード。

【０１２１】

１７．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のフォーマット要件、ピアネットワークノードのうちのどれが、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ためのメカニズム、またはトランザクションの各々に含まれる暗号化された測定データのセットをハッシュするための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１４～１６のいずれか１つに記載の検証ネットワークノード。

【０１２２】

１８．各トランザクションが、暗号化された測定データのセットのための識別子と、暗号化された測定データのセットを記憶する記憶センターの識別子と、暗号化された測定データのセットを生成したデータ提供者の識別子と、暗号化された測定データのセットに対応する暗号ハッシュ値と、を含む、態様１４～１７のいずれか１つに記載の検証ネットワークノード。

【０１２３】

１９．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測定データを記憶するためのシステムであって、プロセスプラント内に配設され、各々が工業プロセスを制御するための物理的機能を行う、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、非一時的コンピュータ可読媒体と、を含む、コンピューティングデバイスと、を備え、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パラメータの測定値を１つ以上のデバイスから取得することと、測定値を暗号化することと、暗号化された測定値を、暗号化された測定値を記憶する記憶センターに送信することと、暗号化された測定値のために記憶センターによって行われた記憶動作を表すトランザクションを取り出すための識別情報を取得することであって、トランザクションは分散型台帳内に含まれる、取得することと、データ契約者から、測定値を取得するための要求を受信することと、データ契約者に、暗号化された測定値を記憶センターから取り出すための識別情報を送信することと、データ契約者に、暗号化された測定値を復号するための復号情報を送信することと、を行わせる、システム。

【０１２４】

２０．データ契約者が、暗号化された測定値を取り出し、暗号化された測定値を、分散型台帳内に含まれる暗号化された測定値に対応する暗号ハッシュ値と比較して、暗号化された測定値の信頼性を検証する、態様１９に記載のシステム。

【０１２５】

２１．トランザクションが、暗号化された測定データを記憶する記憶センターの識別子と、暗号化された測定データを生成したコンピューティングデバイスの識別子と、暗号化された測定データを取り出すための識別子と、暗号化された測定データに対応する暗号ハッシュ値と、を含む、態様１９または態様２０のいずれか１つに記載の方法。

【０１２６】

２２．トランザクションを取り出すための識別情報を送信するために、命令は、コンピ

ューティングデバイスに、データ契約者に、暗号化された測定値を含む分散型台帳内のトランザクションに対応するトランザクション識別子を送信させる、態様１９～２１のいずれか１つに記載のシステム。

【０１２７】

２３．暗号化された測定値を復号するための復号情報を送信するために、命令は、コンピューティングデバイスに、データ契約者に、暗号化された測定値を復号するためのワンタイム暗号鍵を送信させる、態様１９～２２のいずれか１つに記載のシステム。

【０１２８】

２４．命令が、コンピューティングデバイスに、プロセスプラント内の複数のパラメータの複数の測定値を取得することと、複数の測定値の各々を暗号化することと、複数の暗号化された測定値を複数の記憶センターに送信することと、をさらに行わせる、態様１９～２３のいずれか１つに記載のシステム。

【０１２９】

２５．データ契約者からの、複数の測定値のうちの少なくともいくつかを取得するための要求に応答して、命令は、コンピューティングデバイスに、データ契約者に、少なくともいくつかの測定値を記憶する複数の記憶センターのうちの少なくともいくつかの識別子を含むトランザクションを取り出すための識別情報をさらに送信させる、態様１９～２４のいずれか１つに記載のシステム。

【０１３０】

２６．少なくともいくつかの測定値が、データセット内に含まれ、データセットのサブセットとして異なる記憶センター内に記憶されている、態様２５に記載のシステム。

【０１３１】

２７．安全に記憶された測定データを記憶センターおよび分散型台帳から取得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、データ提供者によって生成された測定データの要求を送信することと、データ提供者から、暗号化された測定データの表示を含む分散型台帳内のトランザクションに対応するトランザクション識別子を受信することを含む、暗号化された測定データを記憶する記憶センターから測定データの暗号化バージョンを取り出すための識別情報を受信することと、データ提供者から、暗号化された測定データを復号するための復号情報を受信することと、暗号化された測定データを記憶する記憶センターの識別子を含む、分散型台帳からトランザクション識別子に関連付けられたトランザクションデータを取得することと、識別された記憶センターに、暗号化された測定データの要求を送信することと、暗号化された測定データを記憶センターから受信することと、暗号化された測定データを分散型台帳内に含まれる暗号化された測定データの表示と比較することと、暗号化された測定データが分散型台帳内に含まれる暗号化された測定データの表示に対応すると決定することに応答して、測定データを取得するために復号情報を使用して暗号化された測定データを復号することと、を含む、方法。

【０１３２】

２８．測定データが、測定データの複数のサブセットを有する測定データのセットであり、各サブセットは、異なる記憶センターに記憶されており、データ提供者から、暗号化された測定データの各サブセットの表示を含む、分散型台帳内のトランザクションに対応するトランザクション識別子を受信することを含む、複数の記憶センターから測定データの各サブセットの暗号化バージョンを取り出すための識別情報を受信することと、データ提供者から、暗号化された測定データの各サブセットを復号するための復号情報を受信することと、複数の記憶センターの各々に、暗号化された測定データの対応するサブセットの要求を送信することと、暗号化された測定データのサブセットを複数の記憶センターから受信することと、測定データのサブセットを取得するために、サブセットのための対応する復号情報を使用して、暗号化された測定データの各サブセットを復号することと、測定データのセットを生成するために、測定データの複数のサブセットを組み合わせることと、をさらに含む、態様２７に記載の方法。

【０１３３】

２９．トランザクションデータを取得することが、暗号化された測定データを記憶する記憶センターの識別子と、暗号化された測定データを生成したデータ提供者の識別子と、暗号化された測定データを取り出すための識別子と、暗号化された測定データに対応する暗号ハッシュ値と、を取得することを含む、態様２７または態様２８のいずれか１つに記載の方法。

【０１３４】

３０．暗号化された測定データを分散型台帳内に含まれる暗号化された測定データの表示と比較することが、暗号化された測定データを暗号化された測定データに対応する暗号ハッシュ値と比較することを含む、態様２７～２９のいずれか１つに記載の方法。

【０１３５】

３１．復号情報を受信することが、データ提供者から、暗号化された測定データを復号するためのワンタイム暗号鍵を受信することを含む、態様２７～３０のいずれか１つに記載の方法。

【０１３６】

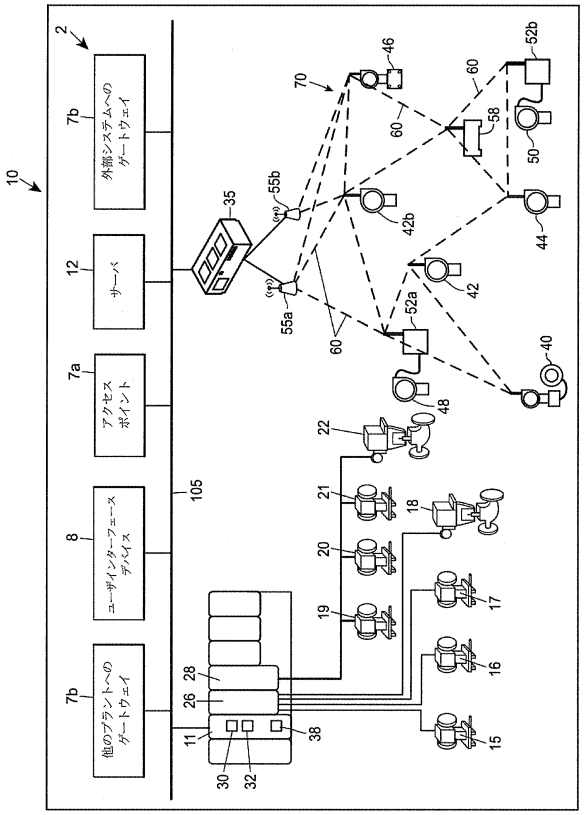
ソフトウェアに実装される場合、本明細書に記載されるアプリケーション、サービス、およびエンジンはいずれも、コンピュータもしくはプロセッサのＲＡＭもしくはＲＯＭ等における磁気ディスク、レーザディスク、固体メモリデバイス、分子メモリ記憶デバイス、または他の記憶媒体等の、任意の有形の非一時的コンピュータ可読メモリに記憶され得る。本明細書に開示される例示的システムは、他の構成要素の中でも、ハードウェア上で実行されるソフトウェアおよび／またはファームウェアを含むように開示されているが、そのようなシステムは単に例示的であるに過ぎず、限定的であると見なされるべきではないことに留意されたい。例えば、これらのハー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

【０１３７】

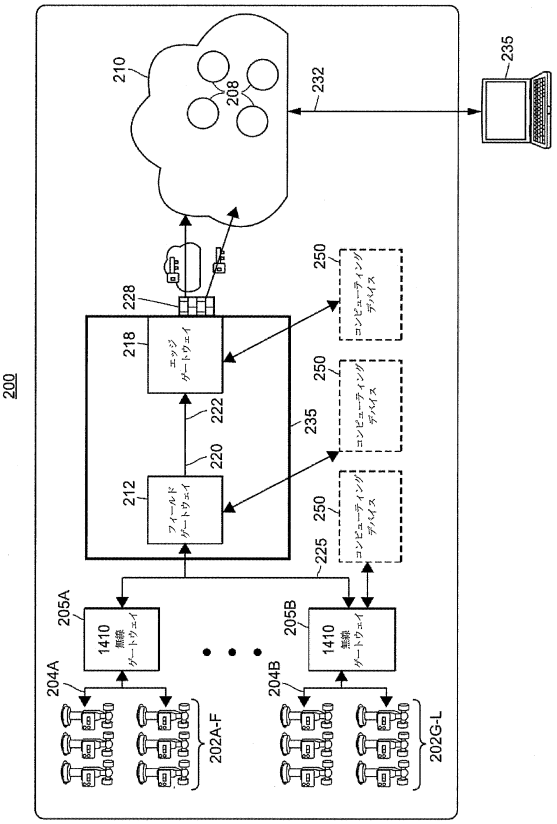
したがって、本発明は具体的な例に関して記載されてきたが、これらの例は例解的であるに過ぎず、本発明の限定であることを意図せず、変更、追加、または削除が、本発明の趣旨および範囲から逸脱することなく、開示される実施形態に対して行われ得ることが当業者には明らかであろう。

【図面】

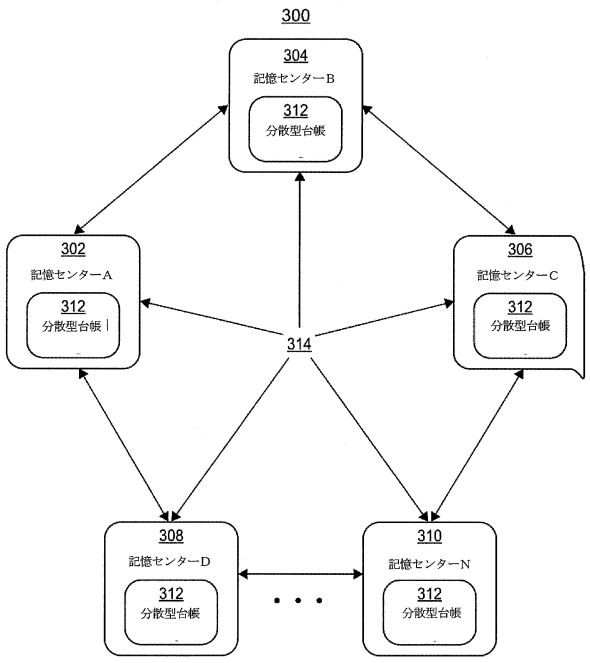
【図１】


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

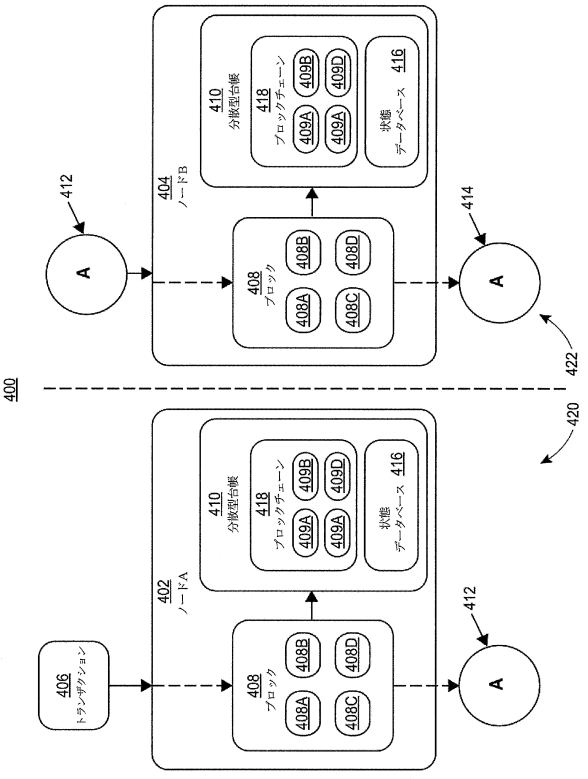
【図２】


200
210
208
232
235
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
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

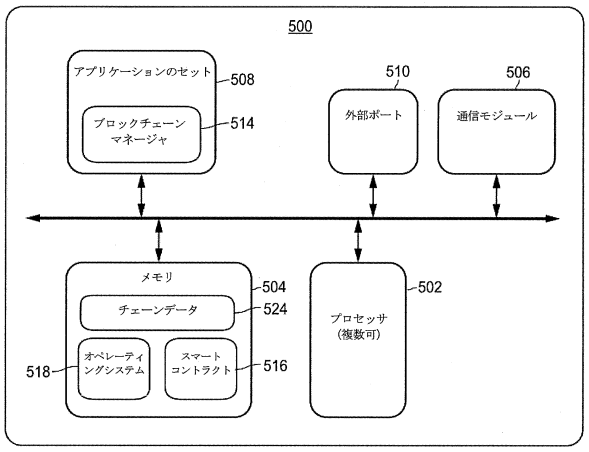
【図３】


300
304
記憶センターB
312
分散型台帳
302
記憶センターA
306
記憶センターC
314
308
記憶センターD
310
記憶センターN

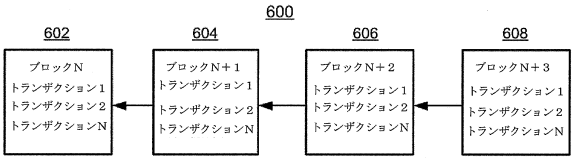
【図４】


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

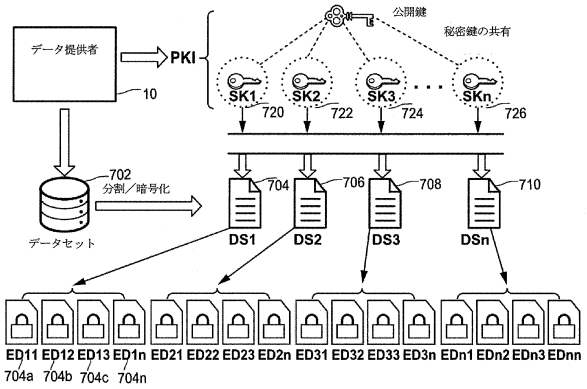
【図５】


500
アプリケーションのセット
508
ブロックチェーン
マネージャ
514
510
外部ポート
506
通信モジュール
メモリ
504
チェーンデータ
524
オペレーティ
ングシステム
518
スマート
コントラクト
516
プロセッサ
(複数可)
502

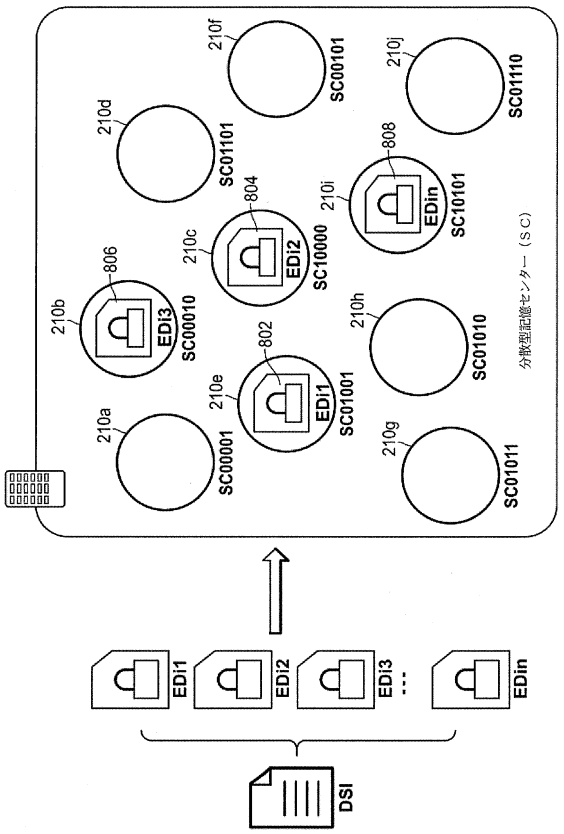
【図６】


600
602
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
604
ブロックN+1
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
606
ブロックN+2
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
608
ブロックN+3
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

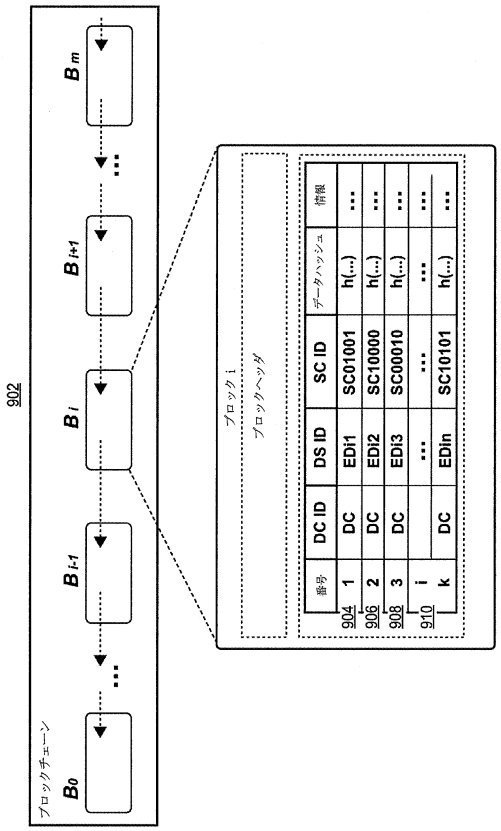
【図７】


データ提供者
10
PKI
公開鍵
秘密鍵の共有
SK1
720
SK2
722
SK3
724
SKn
726
702
分割／暗号化
データセット
704
706
708
710
DS1
DS2
DS3
DSn
ED11 ED12 ED13 ED1n ED21 ED22 ED23 ED2n ED31 ED32 ED33 ED3n EDn1 EDn2 EDn3 EDnn
704a 704b 704c 704n

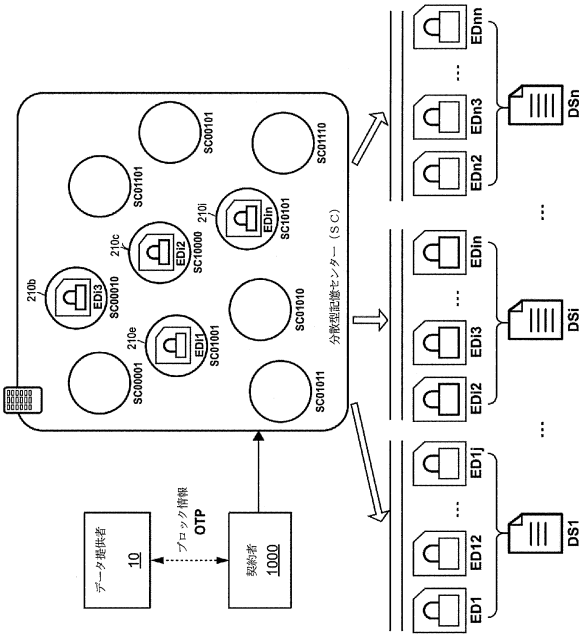
【図８】


210f
SC00101
210j
SC01110
210d
SC01101
808
210i
EDin
SC10101
804
210c
EDi2
SC10000
806
210b
EDi3
SC00010
802
210e
EDi1
SC01001
210h
SC01010
210a
SC00001
210g
SC01011
分散型記憶センター（SC）
EDi1
EDi2
EDi3
EDin
DSI

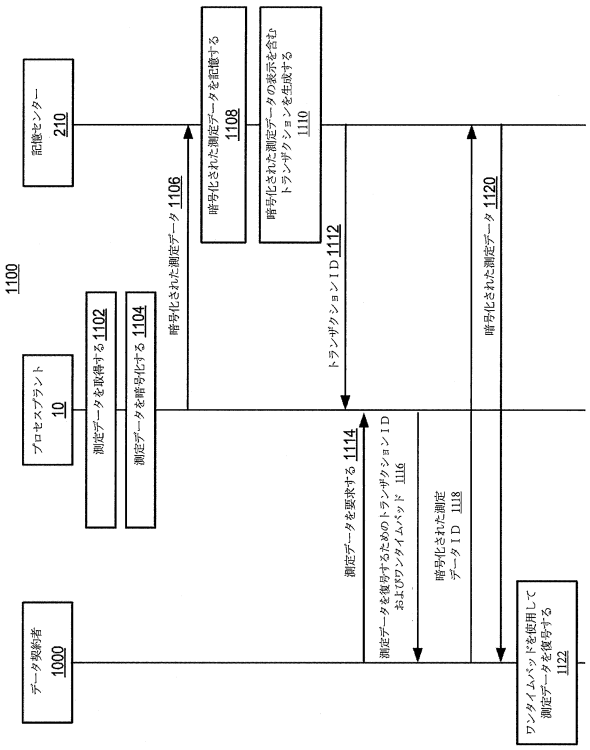
【図９】



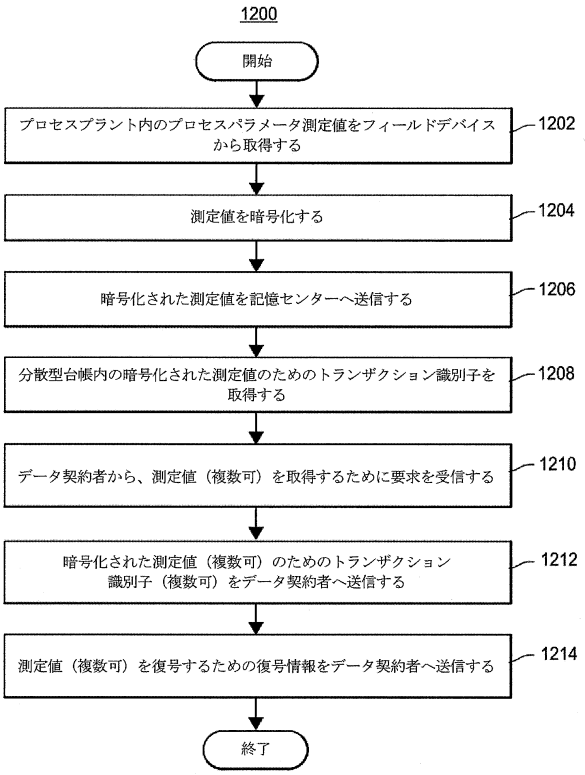
【図１０】



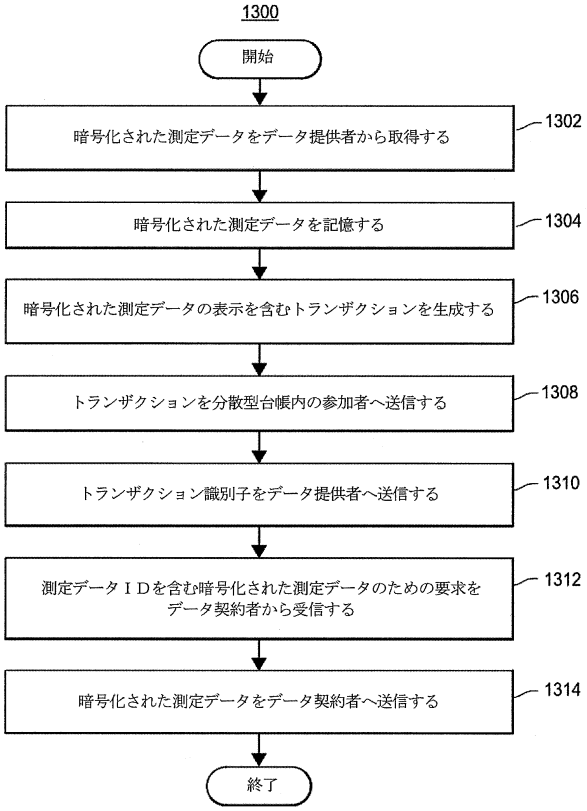
【図１１】



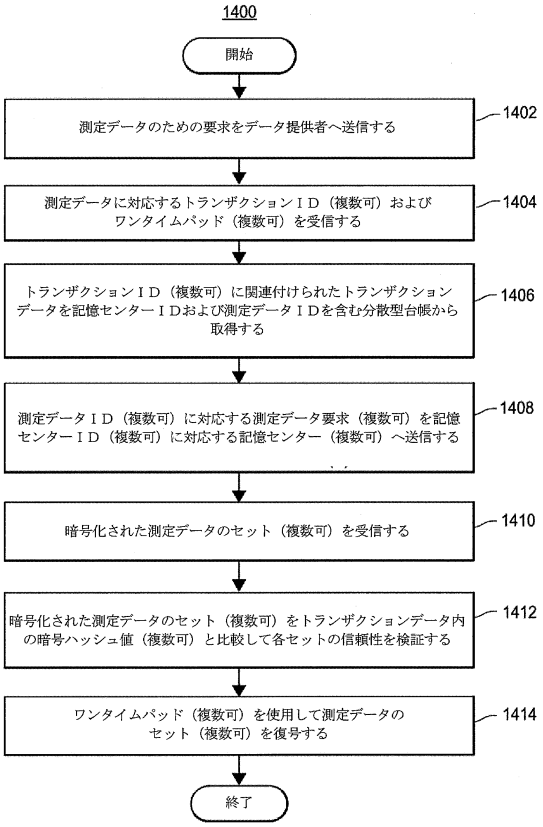
【図１２】



【図１３】


1300
開始
暗号化された測定データをデータ提供者から取得する
1302
暗号化された測定データを記憶する
1304
暗号化された測定データの表示を含むトランザクションを生成する
1306
トランザクションを分散型台帳内の参加者へ送信する
1308
トランザクション識別子をデータ提供者へ送信する
1310
測定データＩＤを含む暗号化された測定データのための要求を
データ契約者から受信する
1312
暗号化された測定データをデータ契約者へ送信する
1314
終了

【図１４】


1400
開始
測定データのための要求をデータ提供者へ送信する
1402
測定データに対応するトランザクションＩＤ（複数可）および
ワンタイムパッド（複数可）を受信する
1404
トランザクションＩＤ（複数可）に関連付けられたトランザクション
データを記憶センターＩＤおよび測定データＩＤを含む分散型台帳から
取得する
1406
測定データＩＤ（複数可）に対応する測定データ要求（複数可）を記憶
センターＩＤ（複数可）に対応する記憶センター（複数可）へ送信する
1408
暗号化された測定データのセット（複数可）を受信する
1410
暗号化された測定データのセット（複数可）をトランザクションデータ内
の暗号ハッシュ値（複数可）と比較して各セットの信頼性を検証する
1412
ワンタイムパッド（複数可）を使用して測定データの
セット（複数可）を復号する
1414
終了

フロントページの続き

アメリカ合衆国 テキサス州 ７８６８１ ラウンド ロック ブラックジャック ドライブ １５０３
(72)発明者 アンソニー・ジュニア・アマロ
アメリカ合衆国 テキサス州 ７８６８１ ラウンド ロック ウエスト ルイス ヘナ ブルバード １１００ ビルディング １ 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 エマーソン プロセス マネージメント内

審査官 平井 誠

(56)参考文献 特開２０１８－０８１４６４（ＪＰ，Ａ）
米国特許出願公開第２０１８／０１３９０５６（ＵＳ，Ａ１）
国際公開第２０１９／０８２４４２（WO，Ａ１）
国際公開第２０１８／０１１８０２（WO，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／００－８８