(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7598373号
(P7598373)

(45)発行日　令和6年12月11日(2024.12.11)

(24)登録日　令和6年12月3日(2024.12.3)

(51)国際特許分類

H04L 9/32 (2006.01)		H04L	9/32	200B
G06F 21/64 (2013.01)		H04L	9/32	200E
		G06F	21/64	

請求項の数　18　（全24頁）

(21)出願番号　特願2022-527107(P2022-527107)
(86)(22)出願日　令和2年11月2日(2020.11.2)
(65)公表番号　特表2023-500411(P2023-500411A)
(43)公表日　令和5年1月5日(2023.1.5)
(86)国際出願番号　PCT/US2020/058495
(87)国際公開番号　WO2021/096715
(87)国際公開日　令和3年5月20日(2021.5.20)
審査請求日　令和5年10月30日(2023.10.30)
(31)優先権主張番号　16/680,788
(32)優先日　令和1年11月12日(2019.11.12)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　518252568
ゼイジ セキュリティ インコーポレイテッド
アメリカ合衆国 カリフォルニア州 94306 パロ アルト シャーマン アヴェニュー 445 スイート 200
(74)代理人　100073184
弁理士　柳田 征史
(74)代理人　100175042
弁理士　高橋 秀明
(72)発明者　イルワン，スサント ジュナイディ
アメリカ合衆国 カリフォルニア州 94306 パロ アルト シャーマン アヴェニュー 445 スイート 200
(72)発明者　ゴー，バオ キュー

最終頁に続く

(54)【発明の名称】　多者安全なデータ管理のための多層台帳

(57)【特許請求の範囲】

【請求項１】

データがネットワーク内及びネットワーク間を流れる時のデータ管理を提供するコンピュータ実行方法であって、

階層を成すデジタル台帳内の複数のハッシュチェーンに記憶され複数の第１ゲートウェイ計算装置によって書き込まれたデータを第２ゲートウェイ計算装置によってアクセスするステップであって、前記複数のハッシュチェーンに記憶された前記データの有効性は書き込む前に検証されていない、ステップと、

前記第２ゲートウェイ計算装置によって前記複数のハッシュチェーンのそれぞれを前記複数のハッシュチェーンの他の全てのハッシュチェーンと比較し前記複数のハッシュチェーンが暗号上一致するかを判断することで、前記複数のハッシュチェーンに記憶された前記データの合意を検出するステップと、

前記複数のハッシュチェーンに記憶された前記データの合意を検出したことに応答して、前記複数のハッシュチェーンに記憶された前記データを使用して記憶されたブロックチェーンデータを前記第２ゲートウェイ計算装置によって更新するステップと

を含むコンピュータ実行方法。

【請求項２】

前記複数のハッシュチェーンのそれぞれを比較する前記ステップは、前記複数のハッシュチェーンのハッシュ値同士を比較することを含む、請求項１記載のコンピュータ実行方法。

【請求項３】
前記記憶されたブロックチェーンデータはブロックチェーンに記憶され、前記ブロックチェーンは分散されたデジタル台帳である、請求項１記載のコンピュータ実行方法。
【請求項４】
前記ブロックチェーンは前記階層を成すデジタル台帳内にある、請求項３記載のコンピュータ実行方法。
【請求項５】
前記ブロックチェーンは前記階層を成すデジタル台帳内の前記ハッシュチェーンが存在する１つ以上の層より高い１つの層に存在する、請求項４記載のコンピュータ実行方法。
【請求項６】
前記記憶されたブロックチェーンデータを第三者と共有する前に前記記憶されたブロックチェーンデータを非対称に暗号化するステップを更に含む請求項１記載のコンピュータ実行方法。
【請求項７】
データがネットワーク内及びネットワーク間を流れる時のデータ管理を提供するためにプログラムされた１つ以上の命令を記憶する１つ以上の持続性コンピュータ読取可能記憶媒体であって、前記１つ以上の命令は、１つ以上の計算装置によって実行される時、
階層を成すデジタル台帳内の複数のハッシュチェーンに記憶され複数の第１ゲートウェイ計算装置によって書き込まれたデータを第２ゲートウェイ計算装置によってアクセスするステップであって、前記複数のハッシュチェーンに記憶された前記データの有効性は書き込む前に検証されていない、ステップと、
前記第２ゲートウェイ計算装置によって前記複数のハッシュチェーンのそれぞれを前記複数のハッシュチェーンの他の全てのハッシュチェーンと比較し前記複数のハッシュチェーンが暗号上一致するかを判断することで、前記複数のハッシュチェーンに記憶された前記データの合意を検出するステップと、
前記複数のハッシュチェーンに記憶された前記データの合意を検出したことに応答して、前記複数のハッシュチェーンに記憶された前記データを使用して記憶されたブロックチェーンデータを前記第２ゲートウェイ計算装置によって更新するステップと
を実行させる、１つ以上の持続性コンピュータ読取可能記憶媒体。
【請求項８】
前記複数のハッシュチェーンのそれぞれを比較する前記ステップは、前記複数のハッシュチェーンのハッシュ値同士を比較することを含む、請求項７記載の１つ以上の持続性コンピュータ読取可能記憶媒体。
【請求項９】
前記記憶されたブロックチェーンデータはブロックチェーンに記憶され、前記ブロックチェーンは分散されたデジタル台帳である、請求項７記載の１つ以上の持続性コンピュータ読取可能記憶媒体。
【請求項１０】
前記ブロックチェーンは前記階層を成すデジタル台帳内にある、請求項９記載の１つ以上の持続性コンピュータ読取可能記憶媒体。
【請求項１１】
前記ブロックチェーンは前記階層を成すデジタル台帳内の前記ハッシュチェーンが存在する１つ以上の層より高い１つの層に存在する、請求項１０記載の１つ以上の持続性コンピュータ読取可能記憶媒体。
【請求項１２】
前記１つ以上の命令は、前記１つ以上の計算装置によって実行される時、前記記憶されたブロックチェーンデータを第三者と共有する前に前記記憶されたブロックチェーンデータを非対称に暗号化するステップを更に実行させる、請求項７記載の１つ以上の持続性コンピュータ読取可能記憶媒体。
【請求項１３】

データがネットワーク内及びネットワーク間を流れる時のデータ管理を提供するコンピュータシステムであって、
台帳データリポジトリと、
前記台帳データリポジトリに通信可能に結合され一組の命令を記憶する持続性データ記憶媒体を備えたグローバルゲートウェイ計算装置であって、前記一組の命令は、該グローバルゲートウェイ計算装置によって実行される時、
階層を成すデジタル台帳内の複数のハッシュチェーンに記憶され複数の第１ゲートウェイ計算装置によって書き込まれたデータを第２ゲートウェイ計算装置によってアクセスするステップであって、前記複数のハッシュチェーンに記憶された前記データの有効性は書き込む前に検証されていない、ステップと、
前記第２ゲートウェイ計算装置によって前記複数のハッシュチェーンのそれぞれを前記複数のハッシュチェーンの他の全てのハッシュチェーンと比較し前記複数のハッシュチェーンが暗号上一致するかを判断することで、前記複数のハッシュチェーンに記憶された前記データの合意を検出するステップと、
前記複数のハッシュチェーンに記憶された前記データの合意を検出したことに応答して、前記複数のハッシュチェーンに記憶された前記データを使用して記憶されたブロックチェーンデータを前記第２ゲートウェイ計算装置によって更新するステップと
を実行させる、グローバルゲートウェイ計算装置と
を備えるコンピュータシステム。
【請求項１４】
前記複数のハッシュチェーンのそれぞれを比較する前記ステップは、前記複数のハッシュチェーンのハッシュ値同士を比較することを含む、請求項１３記載のコンピュータシステム。
【請求項１５】
前記記憶されたブロックチェーンデータは、ブロックチェーンを備える前記台帳データリポジトリに記憶される、請求項１３記載のコンピュータシステム。
【請求項１６】
前記ブロックチェーンは前記階層を成すデジタル台帳内にある、請求項１５記載のコンピュータシステム。
【請求項１７】
前記ブロックチェーンは前記階層を成すデジタル台帳内の前記ハッシュチェーンが存在する１つ以上の層より高い１つの層に存在する、請求項１６記載のコンピュータシステム。
【請求項１８】
前記一組の命令は、前記グローバルゲートウェイ計算装置によって実行される時、前記記憶されたブロックチェーンデータを第三者と共有する前に前記記憶されたブロックチェーンデータを非対称に暗号化するステップを更に実行させる、請求項１３記載のコンピュータシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示の１つの技術分野は、データ機密保護の分野の方法、システム、コンピュータソフトウェア、及び／又はコンピュータハードウェアに関する。別の技術分野は不正アクセス及びデータ使用を防ぐサービスである。
【背景技術】
【０００２】
この項で記載される手法は追求されうる手法であるが、以前想到された又は追求された手法では必ずしもない。従って、特に断らない限り、この項で記載される手法のいずれもこの項に含まれているだけで従来技術と認定されると考えるべきではない。
【０００３】
物のインターネット（ＩｏＴ）装置の開発及び使用は、過去数年の間目覚ましいスピー

ドで進んだ。ＩｏＴ装置は多様であり、産業機器のコントローラからスマートウォッチ及び個人活動モニターまで全ての物を含む。しかし、セキュリティ基盤はこれらの装置の莫大な数と広範な使用に追い付けていない。複数のアナリストは、数年以内に数十億のそのような装置が動作し相互接続ネットワークに接続されるだろうと推定するが、ＩｏＴ装置が生成したデータを、特にデータが様々な仲介者を通って最終目的先に到着する場合、効率的に保護しうる効果的なセキュリティ体系は現在存在しない。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

従って、データは矛盾がなく信頼できることを保証する必要性がある。また、データを記憶しアクセスする安全な方法であって、機密保護違反に耐性のある方法が必要である。

【課題を解決するための手段】

【０００５】

添付の請求項が本発明の概要としての役割を果たすであろう。

【図面の簡単な説明】

【０００６】

本発明は、添付図面の図に限定としてではなく例として示されていて、同様の符号は類似の構成要素を指す。

【図１】幾つかの実施形態に係る一例のデータリポジトリを示す。

【図２】幾つかの実施形態に係る一例の階層を成す台帳を示す。

【図３】幾つかの実施形態に係る階層を成す台帳を実現する一例のネットワーク接続されたコンピュータシステムを示す。

【図４】幾つかの実施形態に係る階層を成す台帳を実現する別の例のネットワーク接続されたコンピュータシステムを示す。

【図５】幾つかの実施形態に係るデータがネットワーク内及びネットワーク間を流れる時のデータ管理を提供する一例の方法を示す。

【図６】本発明の実施形態がその上で実施されうるコンピュータシステムを例示する。

【発明を実施するための形態】

【０００７】

以下の記載において、説明目的のため、本発明の完全な理解を提供するために多数の特定の詳細が明らかにされる。しかし、これらの特定の詳細を欠いて本発明を実施してもよいことは明白であろう。他には、本発明を不必要に不明瞭にしないため、周知の構造及び装置はブロック図形態で示されている。

【０００８】

本明細書において、実施形態は以下の概要に従い項に分けて説明される：

【０００９】

１．０　総論

様々な実施形態によれば、データが同じネットワーク内及び異なるネットワーク間を流れる時の改善されたコンピュータ処理効率及びデータ管理を可能にする方法及びシステムが提供される。分散システムはアクセス制御、データ完全性、機密性、変更の追跡、及びデータの多者ノード検証のために階層を成す台帳を使用する。環境の必要及び／又は要求に依って、ノードは異なる台帳実施形態を使用することがある。例えば、ハッシュチェーンが高スループットを要求するデータを記憶するためにノードによって使用されてもよい。台帳内のデータの検証はそのデータを書き込む各ノードで起こる。台帳内のデータは、そのデータがネットワークから別の記憶システム又はネットワークに書き込まれる前に暗号化されてもよい。

【００１０】

１つの実施形態では、データがネットワーク内及びネットワーク間を流れる時のデータ管理を提供するコンピュータ実行方法は、階層を成すデジタル台帳内の複数のハッシュチェーンに記憶され複数の第１ゲートウェイ計算装置によって書き込まれたデータを第２ゲートウェイ計算装置によってアクセスするステップを含み、それら複数のハッシュチェーンに記憶されデータの有効性は書き込み前に検証されていない。この方法は、第２ゲートウェイ計算装置によって複数のハッシュチェーンのそれぞれを該複数のハッシュチェーンの他の全てのハッシュチェーンと比較しそれらのハッシュチェーンが暗号上一致するかを判断することで、該複数のハッシュチェーンに記憶されたデータの合意を検出するステップを更に含む。本方法は、ハッシュチェーンに記憶されたデータの合意を検出したことに応答して記憶されたブロックチェーンデータを複数のハッシュチェーンに記憶されたデータを使って第２ゲートウェイ計算装置によって更新するステップを更に含む。

【００１１】

２．０　デジタル台帳の種類

デジタル台帳は多数のエントリを追跡する。１つ以上のコンピュータに記憶された台帳全体の２つ以上のコピーが存在する場合がある。デジタル台帳の用途例が２０１７年４月１１日に出願された米国特許出願第１５／４８５０４７号、２０１７年4月１２日に出願され２０１９年１０月１日に発行された米国特許第１０４３２５８５号、２０１７年１０月６日に出願され２０１８年１０月１６日に発行された米国特許第１０１０４０７７号、２０１７年１１月１５日に出願された米国特許出願第１５／８１３４９３号、２０１８年４月１６日に出願され２０１８年９月２５日に発行された米国特許第１００８４６００号、２０１８年８月２３日に出願され２０１９年４月２３日に発行された米国特許第１０２７０７７０号、２０１８年５月１４日に出願され２０１８年９月２５日に発行された米国特許第１００８４８２６号、２０１８年９月１７日に出願された米国特許出願第１６／１３３３２３号、２０１８年９月１７日に出願され２０１９年９月３日に発行された米国特許第１０４０４６９６号、及び２０１８年１２月４日に出願され２０１９年６月１８日に発行された米国特許第１０３２６８０２号の各明細書に記載されている。これらの内容全体を本明細書に引用する。

【００１２】

デジタル台帳の異なる実施形態が存在する。それらの実施形態はブロックチェーン及びハッシュチェーンを含む。

【００１３】

２．１　ブロックチェーン

一例の台帳は分散された台帳、例えばブロックチェーンである。ブロックチェーンを実施する形態では、分散された台帳は多数のエントリを追跡しうる分散デジタル台帳として機能する。分散された台帳全体のコピーは、相互接続されたコンピュータの分散ネットワーク内の各コンピュータに記憶されてよい。分散された台帳への提出されたエントリはコンピュータの大多数によって検証のため検査されてもよい。例えば、１つのコンピュータが分散された台帳内の新しいエントリを生成しようと試みると、分散された台帳のコピーも記憶する相互接続されたコンピュータのネットワークは、先ずアルゴリズムを実行してハッシュを評価し、そのエントリの有効性を検証する。コンピュータの大多数がそのエン

トリが有効であると同意すると、そのエントリは分散された台帳内の新しいブロックとして加えられる。合意ネットワークの一部として、分散された台帳は高い実用的ビザンチン障害耐性（ＰＢＦＴ）及び他の種類の合意アルゴリズムを実施する。例えば、分散された台帳内の情報を変えようと試みる悪意のある攻撃は、合意を変えるために合意ネットワーク内のコンピュータの５０％超を制御する必要があるだろう。悪意を持って攻撃しそれだけ多くのコンピュータの制御を維持することは極めて困難であるので、分散された台帳データは、悪意のある攻撃に対して従来のデータ記憶方法より良く保護される。

【００１４】

図１は一例のデータリポジトリを示す。一例の実施形態では、データリポジトリ１００はデジタル台帳データベースである。データリポジトリ１００はブロック１１０、１２０、１３０を有する台帳からなる。台帳は任意の数のブロックを含んでもよい。図１の例では、各ブロック１１０、１２０、１３０は自身の指標数字１１１、１２１、１３１、時刻印１１２、１２２、１３２、データ１１３、１２３、１３３、ハッシュ値１１４、１２４、１３４、及び１つ前のハッシュ値１１５、１２５、１３５を含んでよい。

【００１５】

指標数字１１１、１２１、１３１はチェーン内のブロックの位置を示す数値指標であってよい。時刻印１１２、１２２、１３２は、ブロック１１０、１２０、１３０が作成された時の日付と時間であってよい。データ１１３、１２３、１３３はブロック１１０、１２０、１３０にそれぞれ“block0data”、“block1data”、及び“block2data”として記憶された暗号化された割当であってよい。ハッシュ値１１４、１２４、１３４は暗号化された割当のハッシュ値、例えばＭＤ５ハッシュ値、ＳＨＡ２５６ハッシュ値、又はＲＩＰＥＭＤハッシュ値であってよい。１つ前のハッシュ値１１５、１２５、１３５はブロックを順に繋ぐ１つ前のブロックのハッシュ値であってよい。図１の例では、ブロック１３０は１つ前のハッシュ値１２４の記録を記憶し、ブロック１２０は１つ前のハッシュ値１１４の記録を記憶する。１つ前のハッシュ値のこれらの記録は、各新しいブロックを１つ前のブロックに繋ぎ各ブロックの完全性検査を可能にするチェーンを形成する。

【００１６】

２．２　ハッシュチェーン

ハッシュチェーンは、提出されたエントリは複数のコンピュータによって検証されないことを除きブロックチェーンと同様に構成される。ハッシュチェーンを実施する形態では、新しいエントリは、コンピュータによって他のコンピュータによる検証なしに台帳内の新しいブロックとして加えられる。各エントリについて他のコンピュータによる検証は行われないので、ハッシュチェーンを実施する形態はブロックチェーンを実施する形態より速い、従って、より高いデータスループットが要求される（例えば、データをより高速で生成する）環境により適する場合がある。

【００１７】

１つの実施形態では、ソースからのデータは複数のハッシュチェーンに書き込まれ、そのデータをハッシュチェーンに書き込む当事者によって暗号化を使って署名されることがある。後で定期的に又は要求により２つ以上のハッシュチェーンは比較されエントリの有効性を暗号上一致するかに基づいて判定する。

【００１８】

３．０　階層台帳

階層を成す台帳は、同じネットワーク内又は異なるネットワーク内の異なる関係者を通って移動するデータの多者安全なデータ管理のために使用され、アクセス制御、完全性、機密性、変更の追跡、及び多者ノード検証を保証してよい。

【００１９】

図２は一例の階層を成す台帳を示す。一例の階層構成２００が２層、即ち、ローカル層とグローバル層２１２を有するとして図２に示されている。しかし、階層を成す台帳は、１つ以上の中間層を含む２つを超える層を有してもよい。

【００２０】

１つ以上の主体（例えば、ＩｏＴ装置。建物、車両など）によって生成されたデータはローカル台帳２０４に書き込まれてよい。定期的に又は要求によりローカル台帳２０４のデータは階層構成内でより上へ送られより上の台帳、例えばグローバル台帳２１４に書き込まれる。データが１つの台帳（例えば、ローカル台帳）から別の台帳（例えば、グローバル台帳）に書き込まれる前に、データ有効性を保証するためにその書き込むデータに関する合意がなければならない。

【００２１】

１つの実施形態では、ローカル台帳２０４からのデータはグローバル台帳２１４に統合され（例えば、そのデータの一致するバージョンだけが書き込まれ）てもよい。或いは、ローカル台帳２０４のデータはグローバル台帳２１４において集計され（例えば、全てのデータが結合され）てもよい。

【００２２】

異なる台帳実施形態が異なる層及び／又は各層（図２の点線２２６で分けられた）内で使用されてよい。例えば、ローカル台帳２０４はハッシュチェーンベースで、グローバル台帳２１４はブロックチェーンベースであってもよい。各層で及び内で使用される異なる台帳実施形態に拘らず、グローバル台帳２１４はローカル台帳２０４に記憶された全てのデータのグローバルな又は完全な眺めを結局は有する。

【００２３】

１つ以上の主体は１つのローカル台帳２０４に書き込まれるデータを生成してもよい。１つの主体はコンピュータ、ソフトウェア、ファームウェア、ハードウェア、又はそれらの任意の組み合わせであってよい。１つの実施形態では、主体はコンピュータ、仮想コンピュータ、及び／又は計算装置であってよい。例として、コンピュータは１つ以上のサーバーコンピュータ、クラウドベースコンピュータ、クラウドベースコンピュータ群、ドッカーコンテナ、仮想マシンインスタンス又は仮想マシン計算要素、例えば仮想プロセッサ、記憶部及びメモリ、データセンター、記憶装置、卓上コンピュータ、ラップトップコンピュータ、携帯装置、及び／又は任意の他の特殊用途計算装置であってよい。

【００２４】

１つの主体はまた、自身がデータを収集及び交換することを可能にするネットワーク接続能力を有する物理的装置であってもよい。例えば、主体はＩｏＴ装置を含んでも又はであってもよい。一例のＩｏＴ装置は産業ＩｏＴメーター、センサー、制御装置、カメラ、又は任意の他の産業ＩｏＴ装置である。

【００２５】

１つの実施形態では、主体は産業用制御システム、例えば監視制御及びデータ取得（ＳＣＡＤＡ）システム（一連のコンピュータ、プログラム可能論理制御装置、比例積分微分（ＰＩＤ）制御装置、プログラム可能論理制御装置（ＰＬＣ）、遠隔端末装置、及び産業環境内でプロセス制御用の他のネットワーク接続された装置を使用する）内のネットワーク接続された様々な計算装置のうちの１つ以上であってもよい。主体はまた、ソフトウェアアプリケーション又は任意の他の記憶され計算装置上で実行されるコンピュータ命令群であってもよい。

【００２６】

データは１つ以上のネットワーク内で主体と台帳の間及び台帳間を送信される。ネットワークは広くは１つ以上の無線又は有線ネットワークの組み合わせ、例えばローカルエリア・ネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、大都市圏ネットワーク（ＭＡＮ）、公衆インターネットなどの世界的な相互接続ネットワーク、又はそれらの組み合わせを表す。このような各ネットワークは、開放型システム間相互接続（ＯＳＩ）多層ネットワークモデルなどの規格に従って相互接続ネットワークプロトコルを実行する記憶されたプログラムを使用又は実行してよい。このモデルは、これらに限定されないが伝送制御プロトコル（ＴＣＰ）又はユーザー・データグラム・プロトコル（ＵＤＰ）、インターネット・プロトコル（ＩＰ）、ハイパーテキスト転送プロトコル（ＨＴＴＰ）などを含む。

【００２７】

３．１　完全性

１つの実施形態では、グローバル台帳２１４は企業によって、例えばその本社において使用及び／又は維持され、ローカル台帳２０４は１つ以上のローカルサイト（現場）によって使用及び／又は維持されてよい。現場が本社と常時は通信していないかも知れない間、１つ以上の主体からのデータが連続してローカル台帳２０４に書き込まれうる。全ての署名がローカル台帳２０４内の１つ前のブロック及び１つ前のブロックの対応する署名に依存するので、ローカル台帳２０４に書き込まれるデータのローカル検証が発生する。ローカル記憶部内のデータの完全性はブロック台帳内のエントリのハッシュをチェーンで繋ぎ、本社と共有される発展する対称鍵を使ってハッシュのＭＡＣを生成することにより達成される。

【００２８】

現場が本社に再び接続されると、その現場に関連する複数のローカル台帳２０４は独立して本社に送信され、グローバル台帳２１４に書き込まれてもよい。複数のローカル台帳２０４のデータはデータ矛盾がない場合だけグローバル台帳２１４に書き込まれるので、グローバル台帳２１４に書き込まれるデータのグローバル検証が発生する。言い換えると、現場から来るデータの完全性を保証するデータの合意がある場合だけ複数のローカル台帳２０４のデータはグローバル台帳２１４に書き込まれる。

【００２９】

例えば、現場によって使用される複数のローカルハッシュチェーン２０４は比較され、それらが暗号上一致するかを判断してもよい。１つの実施形態では、複数のハッシュチェーン２０４の最後ブロックが比較されてもよい。それらのローカルハッシュチェーン２０４が暗号上一致する場合、ローカルハッシュチェーン２０４内のデータの合意があるので、データはグローバル台帳２１４に入るのを許される。それらのローカルハッシュチェーン２０４が暗号上一致しない場合、データの合意がないので、データはグローバル台帳２１４に入るのを許されない場合がある。

【００３０】

別の例として、現場によって使用されるブロックチェーン２０４内のデータは、ローカルブロックチェーン２０４に書き込まれた時にデータの合意があったので追加の検証なしにグローバル台帳２１４に入るのを許される。ブロックチェーンを実施する形態では、相互接続されたコンピュータの分散ネットワーク内のコンピュータの大多数がエントリが有効だと同意する場合だけ、新しいエントリがブロックチェーン内の新しいブロックとして加えられる。

【００３１】

３．２　機密

多者信用は非対称暗号化を使用して可能にされてよい。１つの実施形態では、台帳２０４、２１４内のデータは、私企業ネットワークから別のネットワーク又は記憶システムに送信される時、意図された第三者２５０だけがそのデータを読むことができるように暗号化されてもよい。私企業ネットワークと公衆網などの外部ネットワークは図２で実線２２８によって分けられている。

【００３２】

例えば、本社はそのグローバル台帳２１４内のデータは顧客Ａだけによって読まれうると決定してもよい。データは、その私企業ネットワークの外に位置する顧客Ａの台帳にそのデータが入るのを認める前に、公開鍵台帳に記憶された顧客Ａの公開鍵を使って暗号化されてよい。顧客Ａはその台帳にアクセスし顧客Ａの秘密鍵を使ってデータを解読する。顧客Ａはそのデータを顧客Ｂと共有することを選び、顧客Ｂだけが顧客Ｂの台帳内のそのデータを読むことができるように公開鍵台帳に記憶された顧客Ｂの公開鍵を使ってそのデータを暗号化してもよい。顧客Ｂは顧客Ｂの秘密鍵を使うことで入着するデータを読み、その入着するデータの署名とグローバル台帳２１４内のデータの署名とを検証のために比較してもよい。

【００３３】

４．０　一例の分散されたコンピュータシステム実施形態

１つの実施形態では、本書に説明される図３及び図４のコンピュータシステム３００、４００は、少なくとも部分的に１つ以上のコンピュータ装置のハードウェア、例えば本書に記載された機能を実行するために１つ以上のメモリに記憶されたプログラム命令群を実行する１つ以上のハードウェアプロセッサにより実現される構成要素を備える。様々な実施形態において、本書に記載された全ての機能が、特殊用途コンピュータ又は汎用コンピュータ内のプログラミングを使用して実行される動作を表すように意図されている。「コンピュータ」は１つ以上の物理的コンピュータ、仮想コンピュータ、及び／又は計算装置であってよい。例として、コンピュータは１つ以上のサーバーコンピュータ、クラウドベースコンピュータ、クラウドベースコンピュータ群、ドッカーコンテナ、仮想マシンインスタンス又は仮想マシン計算要素、例えば仮想プロセッサ、記憶部及びメモリ、データセンター、記憶装置、卓上コンピュータ、ラップトップコンピュータ、携帯装置、及び／又は任意の他の特殊用途計算装置であってよい。特に明記されない限り、本書における「コンピュータ」へのいずれの言及も１つ以上のコンピュータを意味しうる。上記の命令群は実行可能な命令群であり、ＪＡＶＡ（登録商標）、Ｃ＋＋、ＯＢＪＥＣＴＩＶＥ‐Ｃ、又は任意の他の適切なプログラミング環境で作成されたソースコードに基づいてコンパイル又は他のやり方で作成された１つ以上の実行可能なファイル又はプログラムから成ってもよい。本書に記載した全てのコンピュータはネットワークに接続するように構成され、本開示は図３及び図４の全ての要素はネットワークを介して通信可能に結合されることを想定する。図３及び図４に描かれた様々な要素はまた、説明のために図３及び図４に描かれていない直接通信リンクを介して互いに通信してもよい。

【００３４】

図３及び図４はそれぞれ、本書に記載したプログラミングを実行するように構成された構成要素の多くの可能な配置の１つだけを示す。他の配置はより少ないか又は異なる構成要素を含み、構成要素間の働きの区分けはその配置に依って変わることがある。

【００３５】

４．１　多サイト例

図３は階層を成す台帳を実現する一例のネットワーク接続されたコンピュータシステムを示す。

【００３６】

主体３０２は高速度データを生成してもよい。主体３０２はコンピュータ、ソフトウェア、ファームウェア、ハードウェア、又はそれらの任意の組み合わせであってよい。１つの実施形態では、主体はコンピュータ、仮想コンピュータ、及び／又は計算装置であってよい。例として、コンピュータは１つ以上のサーバーコンピュータ、クラウドベースコンピュータ、クラウドベースコンピュータ群、ドッカーコンテナ、仮想マシンインスタンス又は仮想マシン計算要素、例えば仮想プロセッサ、記憶部及びメモリ、データセンター、記憶装置、卓上コンピュータ、ラップトップコンピュータ、携帯装置、及び／又は任意の他の特殊用途計算装置であってよい。

【００３７】

主体３０２はまた、自身がデータを収集及び交換することを可能にするネットワーク接続能力を有する物理的装置であるＩｏＴ装置であってもよい。１つの実施形態では、ＩｏＴ装置は産業ＩｏＴメーター、センサー、制御装置、カメラ、又は任意の他の産業ＩｏＴ装置である。

【００３８】

１つの実施形態では、主体３０２は産業用制御システム、例えば監視制御及びデータ取得（ＳＣＡＤＡ）システム（一連のコンピュータ、プログラム可能論理制御装置、比例積分微分（ＰＩＤ）制御装置、遠隔端末装置、及び産業環境内でプロセス制御用の他のネットワーク接続された装置を使用する）内のネットワーク接続された様々な計算装置のうちの１つ以上であってもよい。主体３０２はまた、ソフトウェアアプリケーション又は任意の他の記憶され計算装置上で実行されるコンピュータ命令群であってもよい。

【００３９】
ローカルノード３１０は企業の１つ以上のローカルサイト（現場）に位置してよい。１つの実施形態では、各現場は少なくとも２つのローカルノード３１０を含む。主体３０２によって生成されたデータは冗長性のために現場内の１つ以上のローカルノード３１０に送信又は一斉送信されてよい。システム３００はデータを生成する１つの主体３０２を含むとして図３に示されているが、システム３００はデータを生成しシステム３００内のローカルノード３１０へ送信する２つ以上の主体３０２を含んでもよい。
【００４０】
各ローカルノード３１０はローカルゲートウェイ３１２を含んでもよい。ローカルゲートウェイ３１２は、主体３０２によって生成されたデータを受信するように構成された受信命令群３１２ａ、データを暗号化するように構成された暗号化命令群３１２ｂ、及び主体３０２から受信したデータをローカル台帳に安全に転送するように構成された処理命令群３１２ｃを記憶するコンピュータ、ソフトウェア及び／又はハードウェア、又はそれらの組み合わせであってよい。ハッシュチェーンを実施する形態は高速度データが存在する環境により適しているので、ローカル台帳はハッシュチェーンであってもよい。ハッシュチェーンはコンピュータ３１４に記憶される。
【００４１】
１つの実施形態では、受信命令群３１２ａは主体３０２によって現場内の全てのローカルゲートウェイ３１２に一斉送信されたデータを受信してもよい。ローカルノード３１０がグローバルノード３２０と通信していないかもしれない時でも、ローカルノード３１０は主体からのデータを連続的に受信してもよい。暗号化命令群３１２ｂは、データを暗号化する当事者（例えば、現場）を特定する現場自身の秘密鍵を使って主体３０２からのデータを暗号化してよい。処理命令群３１２ｃはハッシュアルゴリズム、例えばＭＤ５、安全ハッシュアルゴリズム（ＳＨＡ）２５６、又は任意の他のハッシュ関数を暗号化されたデータに適用してハッシュ化されたデータ対象要素を生成してもよい。ハッシュは対象要素の数値表現として働いてもよい。当分野で理解される任意のハッシュ関数を使用してもよい。対象要素へのどんな変更もハッシュを変え、それにより前のハッシュに比べて現在のハッシュに違いを生じるであろう。ハッシュ化されたデータ対象要素は処理命令群３１２ｃを使った記憶のためにローカル台帳に送信される。処理命令群３１２ｃは、暗号化されたデータの新しいデータエントリを作ることでローカル台帳を更新する。
【００４２】
企業の本社に位置してよいグローバルノード３２０はグローバルゲートウェイ３２２を備えてもよい。グローバルゲートウェイ３２２は、現場のローカルノード３１０からデータを受信するように構成された受信命令群３２２ａ、複数のローカル台帳内のデータを比較してそれらのデータが暗号上一致するかを判断するように構成された分析命令群３２２ｂ、データを暗号化又は解読するように構成された暗号化命令群３２２ｃ、及び検証されたデータをグローバル台帳に安全に転送するように構成された処理命令群３２２ｄを記憶するコンピュータ、ソフトウェア及び／又はハードウェア、又はそれらの組み合わせであってよい。１つの実施形態では、グローバル台帳は分散台帳であり、グローバル分散台帳のコピーが複数のコンピュータ３２４に記憶される。
【００４３】
１つの実施形態では、ローカルノード３１０がグローバルノード３２０と通信する時、受信命令群３２２ａはローカルノード３１０に関連するローカル台帳内のデータを受信又はにアクセスしてよい。本書で説明したように、ハッシュチェーンを実施する形態は、エントリが有効であることをノード間で検証することなく新しいエントリがハッシュチェーン内の新しいブロックとして加えられる点でブロックチェーンを実施する形態と異なる。従って、エントリの完全性を検証するために、分析命令群３２２ｂはローカルノード３１０に関連する個々のローカル台帳からのハッシュ値を比較して一致する（例えば、暗号上一致する）かを判定する。ハッシュが一致する場合のみ、処理命令群３２２ｄを使用してデータはグローバル台帳に入るのを許される。一致しないハッシュは、データが失われた

か又は悪意を持って変えられたことを示す場合があり、グローバルゲートウェイ３２２はそのデータを廃棄しグローバル台帳に入るのを許さない場合がある。グローバルゲートウェイ３２２はローカルゲートウェイ３１２にデータ不一致を通知する。

【００４４】

グローバル台帳内のデータのアクセス制御を保証するために、企業ネットワークから別のネットワーク又は記憶システムへ書き込まれる時に、暗号化命令群３２２ｃはグローバル台帳内のデータを暗号化してもよい。

【００４５】

１つの実施形態では、グローバルノード３２０は、グローバル台帳が複数の現場中の全てのデータを全体的に又は完全に見れるように全ての現場のローカルノード３１０からデータを受信し検証されたデータをグローバル台帳に記憶してもよい。

【００４６】

１つの実施形態では、グローバルノード３２０はまた、施策及びユーザーインターフェースを管理するように構成された管理者コンピュータ３２８を備えてもよい。例えば、管理者コンピュータ３２８は装置ライフサイクル（例えば、鍵供給）、参加策、アクセス制御策、鍵管理（例えば、配布、生成、及び更新）、複数の台帳に亘るデータ集計、監査記録、システムイベントなどを生成及び／又は管理してもよい。グローバルノード３２０はまた、アクティブディレクトリなどの既存の機密保護サービスと通信し主体３０２の識別情報を検証するように構成されたブローカーコンピュータ３２６を備えてもよい。

【００４７】

４．２　ピアツーピア例

図４は階層を成す台帳を実現する別の例のネットワーク接続されたコンピュータシステムを示す。

【００４８】

主体４０２、例えば建物又は車両は電力を生成し蓄える能力を有してもよい。主体４０２の組み合わせは微小送電網４１０（図４でローカルノードとラベル付けされた）を形成してもよい。微小送電網４１０内の主体４０２同士は取引ができる。主体４０２は、主体４０２によるエネルギー消費及び生成を測定し報告するためのスマートエネルギー計器４０４を備えてもよい。主体４０２は、微小送電網４１０内及び／又外の主体ピアと進んで共用する余剰エネルギーを時々有する場合があり、他の時には微小送電網４１０内及び／又外の主体ピアから追加のエネルギーを取得する必要がある場合がある。主体４０２は、主体４０２が進んで共用する余剰エネルギーに関する申し出データと他の主体ピアから要求されたエネルギーに関する入札データとを示すための報告モジュール４０６を備えてもよい。１つの実施形態では、主体４０２からのデータは計器４０４によって生成されたエネルギーデータと報告モジュール４０６によって生成された申し出／入札データとを含む。

【００４９】

各微小送電網４１０は少なくとも１つのローカルゲートウェイ４１２を備えてもよい。ローカルゲートウェイ４１２は、参加策に基づいて微小送電網４１０内の参加主体４０２によって生成されたデータを受信するように構成された受信命令群４１２ａ、データを暗号化するように構成された暗号化命令群４１２ｂ、及び主体４０２から受信したデータを１つ以上のコンピュータ４１４に記憶されたローカル台帳に安全に転送するように構成された処理命令群４１２ｃを記憶するコンピュータ、ソフトウェア及び／又はハードウェア、又はそれらの組み合わせであってよい。ローカル台帳はハッシュチェーン又はブロックチェーンであってよい。１つの実施形態では、ローカルゲートウェイ４１２内の受信命令群４１２ａ、暗号化命令群４１２ｂ、及び処理命令群４１２ｃは図３のローカルゲートウェイ３１２内の受信命令群３１２ａ、暗号化命令群３１２ｂ、及び処理命令群３１２ｃと同様に構成されてよい。

【００５０】

ローカル台帳は、ピアツーピア取引を容易にするために微小送電網４１０の外に位置しうる調停者コンピュータ（不図示）によって使用されてもよい。調停者コンピュータは、

ローカル台帳に記憶された主体４０２からのデータに基づいてリアルタイムで決定を行ってよい。例えば、調停者コンピュータは申し出データからどの主体４０２がエネルギーを放出する予定かを判断し、その主体４０２にエネルギーをエネルギー網へ放出するよう指示してよい。ローカル取引は調停者コンピュータによってローカル台帳に書き込まれてよい。調停者コンピュータは、同意されたエネルギーがエネルギー網へ実際放出され、及び／又はエネルギー網から消費されたことを、ローカル台帳に記憶された主体４０２からのデータに基づいて確認してよい。

【００５１】

公益事業会社に位置しうるグローバルノード４２０は、少なくとも１つのグローバルゲートウェイ４２２を備えてよい。グローバルゲートウェイ４２２は、微小送電網４１０からデータを受信するように構成された受信命令群４２２ａ、データを暗号化又は解読するように構成された暗号化命令群４２２ｃ、及び微小送電網４１０から受信したデータをグローバル台帳に安全に転送するように構成された処理命令群４２２ｄを記憶するコンピュータ、ソフトウェア及び／又はハードウェア、又はそれらの組み合わせであってよい。１つの実施形態では、グローバル台帳は分散台帳であり、グローバル分散台帳のコピーが複数のコンピュータ４２４に記憶される。１つの実施形態では、グローバルゲートウェイ４２２内の受信命令群４２２ａ、暗号化命令群４２２ｃ、及び処理命令群４２２ｄは図３のグローバルゲートウェイ３２２内の受信命令群３２２ａ、暗号化命令群３２２ｃ、及び処理命令群３２２ｄと同様に構成されてよい。

【００５２】

１つの実施形態では、グローバル台帳は取引主体４０２間の金銭上の決済に使用されてもよく及び／又は監査目的に使用されてもよい。

【００５３】

１つの実施形態では、グローバルノード４２０はまた、施策及びユーザーインターフェースを管理するように構成された管理者コンピュータ４２８を備えてもよい。例えば、管理者コンピュータ４２８は、ピアツーピア取引に参加するのを許可された主体４０２の参加策であって、ローカルゲートウェイ４１２によるアクセス可能な参加策を生成及び／又は管理してもよい。グローバルノード４２０はまた、アクティブディレクトリなどの既存の機密保護サービスと通信し主体４０２の識別情報を検証するように構成されたブローカーコンピュータ４２６及び／又は調停者コンピュータを備えてもよい。

【００５４】

５．０　手順概要

図５は幾つかの実施形態に係るデータがネットワーク内及びネットワーク間を流れる時のデータ管理を提供する一例の方法５００を示す。図５は、方法５００をグローバルゲートウェイが実行しうる又は動作させうる１つ以上のコンピュータプログラム又は他のソフトウェア要素としてコード化する基礎として使用されうる。

【００５５】

方法５００はステップ５１０から始まり、このステップでは第２ゲートウェイ計算装置が階層を成すデジタル台帳内の複数のハッシュチェーンに記憶され複数の第１ゲートウェイ計算装置によって書き込まれるか又は更新されるデータにアクセスしてよい。第２ゲートウェイ計算装置は、例えばグローバルゲートウェイであってもよい。複数の第１ゲートウェイ計算装置は、例えば複数のローカルゲートウェイであってもよい。複数のハッシュチェーンに記憶されたデータの有効性は書き込み前には検証されていない。

【００５６】

ブロックチェーンと異なり、ハッシュチェーン内のエントリは相互接続されたコンピュータの分散ネットワーク内のコンピュータの大多数によって検証されない。エントリは他のコンピュータによる検証なしにハッシュチェーン内の新しいブロックとして加えられる。また、直列に接続されたコンピュータ（例えば、Xage Enforcement Point）又はゲートウェイは、データを生成する装置の認証をそのデータを受け入れる前に各装置の指紋を採る（ハードウェア、ソフトウェア、ファームウェア、ファイルシステムなど）ことで検

証できる。これはデータ生成者である装置を信用する方法である。

【００５７】

異なる台帳実施形態が、階層を成すデジタル台帳の異なる層で及び／又は各層内で使用されてよい。

【００５８】

第２ゲートウェイ計算装置はグローバルな又は中心の位置に位置し、第１ゲートウェイ計算装置はそのグローバルな位置に関連する１つ以上の場所に位置してよい。１つの実施形態では、場所は少なくとも２つの第１ゲートウェイ計算装置を備えてもよい。

【００５９】

ステップ５２０では、第２ゲートウェイ計算装置は、複数のハッシュチェーンのそれぞれを複数のハッシュチェーンの他の全てのハッシュチェーンと比較してそれらのハッシュチェーンが暗号上一致するかを判断することで、複数のハッシュチェーンに記憶されたデータの合意を検出してよい。例えば、第２ゲートウェイの分析命令群は、複数の第１デジタル台帳に記憶されたデータの合意を検出してもよい。１つの実施形態では、分析命令群はハッシュチェーンのハッシュ値を比較してそれらのハッシュチェーンが暗号上一致するかを判断してよい。それらのハッシュチェーンが暗号上一致するならば、それらのハッシュチェーンに記憶されたデータの合意が存在する。

【００６０】

ステップ５３０では、第２ゲートウェイ計算装置は記憶されたブロックチェーンデータを複数のハッシュチェーンに記憶されたデータを使って更新する。１つの実施形態では、記憶されたブロックチェーンデータはハッシュチェーンに記憶されたデータの合意を検出したことに応答して更新される。

【００６１】

記憶されたブロックチェーンデータは分散された台帳に記憶される。１つの実施形態では、その分散された台帳はブロックチェーンである。ブロックチェーンは階層を成すデジタル台帳内にある。１つの実施形態では、ブロックチェーンは、階層を成すデジタル台帳内のハッシュチェーンがいる１つ以上の層より高い１つの層に存在する。１つの実施形態では、ブロックチェーンは、ブロックチェーンが階層内の全てのデータを全体的に又は完全に見れるように階層内の全てのデジタル台帳のデータを記憶する。

【００６２】

１つの実施形態では、第２ゲートウェイの暗号化命令群は、意図された第三者だけがそのデータを読めるように記憶されたブロックチェーンデータを非対称に暗号化してよい。

【００６３】

上記手法を使用して、プログラムされたコンピュータは、データが様々な関係者を通過する時、アクセス制御、完全性、機密保護、変更の追跡、及び多者ノードデータ検証を保証しうる。本手法は階層を成す台帳を利用する。これらの台帳は異なる実施形態のものでありうる。ハッシュチェーンなどのより速い台帳を実施する形態は、生成された速いスループットのデータを記憶するためにローカルゲートウェイによって使用されてよい。定期的に又は要求により、ローカル台帳のデータは、グローバル台帳に記憶するためにグローバルゲートウェイに送信される。検証されたローカル台帳のデータだけがより上のグローバル台帳に書き込まれる。

【００６４】

本書に開示された手法はデータ完全性をローカルレベル及びグローバルレベルにおいて向上させる。全ての署名がローカル台帳内の１つ前のブロックに依存するので、ローカル台帳に書き込まれるデータのローカル検証が発生し、検証又は同意されたデータだけがグローバル台帳に書き込まれるので、グローバル台帳に書き込まれるデータのグローバル検証が発生する。グローバル台帳は、ローカル台帳に記憶された全てのデータを全体的に又は完全に見れる。

【００６５】

また、本書に開示された手法はデータ機密も向上させる。ゲートウェイは台帳内のデー

タをネットワークから別の記憶システム又はネットワークへ書き込む前に、意図された第三者だけがそのデータを読めるようにそのデータを非対称に暗号化してよい。

【００６６】

本開示の目的及び特徴はコンピュータ技術のプログラム、プロセス、メッセージング手法、データ記憶手法などの形態の実際的用途に向けられていて分散されネットワーク接続された装置、特にＩｏＴ装置によって生成されるデータの管理の向上を提供することは、本開示全体から明らかであろう。

【００６７】

６．０　ハードウェア概要

１つの実施形態によれば、本書に記載した手法は少なくとも１つの計算装置により実行される。本手法は少なくとも１つのサーバーコンピュータ及び／又はパケットデータネットワークなどのネットワークを使用して結合された他の複数の計算装置の組み合わせを使用して全体が又は一部が実行されてよい。計算装置はそれらの手法を実行するように配線されていても、又はデジタル電子装置、例えば少なくとも１つの特定用途向け集積回路（ＡＳＩＣ）又はそれらの手法を実行するように永続的にプログラムされたフィールド・プログラマブル・ゲートアレイ（ＦＰＧＡ）を備えていても、又はファームウェア、メモリ、他の記憶装置、又は組み合わせ内のプログラマ命令群に従ってそれらの手法を実行するようにプログラマされた少なくとも１つの汎用ハードウェアプロセッサを備えていてもよい。このような計算装置はまた、カスタム配線論理、ＡＳＩＣ、又はＦＰＧＡをカスタムプログラムと組み合わせて記載した手法を実現してもよい。これらの計算装置はサーバーコンピュータ、ワークステーション、パーソナルコンピュータ、携帯コンピュータシステム、ハンドヘルド装置、可搬計算装置、装着型装置、体に取り付けた又は埋め込み可能な装置、スマートフォン、スマート器具、ＬＡＮ間接続装置、自律又は半自律装置、例えばロボット又は無人地上又は空中車、配線接続された及び／又はプログラム論理を内蔵し記載された手法を実行する任意の他の電子装置、データセンター内の１つ以上の仮想コンピュータマシン又はインスタンス、及び／又はサーバーコンピュータ及び／又はパーソナルコンピュータのネットワークであってもよい。

【００６８】

図６は１つの実施形態が実施されてよい一例のコンピュータシステムを示すブロック図である。図６の例では、コンピュータシステム６００及び開示された技術をハードウェア、ソフトウェア、又はハードウェアとソフトウェアの組み合わせで実現するための命令群が概略的に例えば、箱又は円として、本開示が関係する技術の当業者により通常使用されるのと同じ詳細さのレベルでコンピュータアーキテクチャ及びコンピュータシステム実施形態について伝えるために表されている。

【００６９】

コンピュータシステム６００は、バス及び／又はコンピュータシステム６００の構成要素間で情報及び／又は命令群を電子信号路を通じて通信するための他の通信機構を含んでよい入力／出力（Ｉ／Ｏ）サブシステム６０２を含む。Ｉ／ＯサブシステムＩ／Ｏコントローラ、メモリコントローラ、及び少なくとも１つのＩ／Ｏポートを含んでもよい。電子信号路は図面において概略的に例えば、線、一方向矢印、又は双方向矢印として表されている。

【００７０】

少なくとも１つのハードウェアプロセッサ６０４がＩ／Ｏサブシステム６０２に情報及び命令群を処理するために結合される。ハードウェアプロセッサ６０４は、例えば汎用マイクロプロセッサ又はマイクロコントローラ、及び／又は埋め込みシステム又はグラフィック処理ユニット（ＧＰＵ）又はデジタル信号プロセッサ又はＡＲＭプロセッサなどの特殊用途マイクロプロセッサを含んでもよい。プロセッサ６０４は一体化された論理演算ユニット（ＡＬＵ）を備えても、又は別個のＡＬＵに結合されてもよい。

【００７１】

コンピュータシステム６００は、Ｉ／Ｏサブシステム６０２に結合されデータ及びプロ

セッサ６０４が実行する命令群を電子的にデジタルで記憶するための主メモリなどの１つ以上のメモリユニット６０６を含む。メモリ６０６は揮発性メモリ、例えば様々な形態のランダムアクセスメモリ（ＲＡＭ）又は他の動的記憶装置を含んでもよい。メモリ６０６も、プロセッサ６０４により命令群が実行される間一時的変数又は他の中間情報を記憶するために使用されてもよい。このような命令群は、プロセッサ６０４にとってアクセス可能な持続性コンピュータ読取可能記憶媒体に記憶されている場合、コンピュータシステム６００を命令群に指定された動作を実行するようにカスタマイズされた特殊用途マシンに変えうる。

【００７２】

コンピュータシステム６００は不揮発性メモリ、例えば読出し専用メモリ（ＲＯＭ）６０８又はＩ／Ｏサブシステム６０２に結合され情報及びプロセッサ６０４用の命令群を記憶するための他の静的記憶装置を更に含む。ＲＯＭ６０８は様々な形態のプログラマブルＲＯＭ（ＰＲＯＭ）、例えば消去可能ＰＲＯＭ（ＥＰＲＯＭ）又は電気的消去可能ＰＲＯＭ（ＥＥＰＲＯＭ）を含んでもよい。永続記憶ユニット６１０は様々な形態の不揮発性ＲＡＭ（ＮＶＲＡＭ）、例えばＦＬＡＳＨ（登録商標）メモリ、又は固体記憶装置、磁気ディスク又はＣＤ－ＲＯＭ又はＤＶＤ－ＲＯＭなどの光ディスクを含んでもよく、情報及び命令群を記憶するためにＩ／Ｏサブシステム６０２に結合されてもよい。記憶装置６１０は、命令群及びデータを記憶するために使用されてよい持続性コンピュータ読取可能媒体の例であり、それらの命令群はプロセッサ６０４により実行される時、コンピュータ実行方法を実行させ、本書の手法を実行する。

【００７３】

メモリ６０６、ＲＯＭ６０８、又は記憶装置６１０内の命令群は、モジュール、方法、オブジェクト、機能、ルーチン、又は呼び出しとして構成される１つ以上の組の命令を含んでよい。命令群は１つ以上のコンピュータプログラム、オペレーティングシステムサービス、又は携帯アプリを含むアプリケーションプログラムとして構成されてもよい。命令群はオペレーティングシステム及び／又はシステムソフトウェア；マルチメディア、プログラミング、又は他の機能を支える１つ以上のライブラリ；ＴＣＰ／ＩＰ、ＨＴＴＰ、又は他の通信プロトコルを実行するデータプロトコル命令群又はスタック；ＨＴＭＬ、ＸＭＬ、ＪＰＥＧ、ＭＰＥＧ、又はＰＮＧを使ってコード化されたファイルを解析又は解釈するファイルフォーマット処理命令群；グラフィカルユーザーインターフェース（ＧＵＩ）、コマンドラインインターフェース、又はテキストユーザーインターフェース用のコマンドを翻訳又は解釈するユーザーインターフェース命令群；アプリケーションソフトウェア、例えばオフィススイート、インターネットアクセスアプリケーション、設計及び製造アプリケーション、グラフィックアプリケーション、音声アプリケーション、ソフトウェア工学アプリケーション、教育アプリケーション、ゲーム、又は種々雑多なアプリケーションを含んでよい。命令群はウェブサーバー、ウェブアプリケーションサーバー、又はウェブクライアントを実現してもよい。命令群はプレゼンテーション層、アプリケーション層、及びデータ記憶層、例えば構造化照会言語（ＳＱＬ）を使用する又はＳＱＬを使用しない関係型データベースシステム、オブジェクトストア、グラフデータベース、フラットファイルシステム、又は他のデータ記憶として構成されてよい。

【００７４】

コンピュータシステム６００はＩ／Ｏサブシステム６０２を介して少なくとも１つの出力装置６１２に結合されてもよい。１つの実施形態では、出力装置６１２はデジタルコンピュータ表示器である。様々な実施形態で使用されてよい表示器の例は、タッチスクリーン表示器又は発光ダイオード（ＬＥＤ）表示器又は液晶表示器（ＬＣＤ）又は電子ペーパー表示器を含む。コンピュータシステム６００は表示装置に代えて又は加えて他の種類の出力装置６１２を含んでよい。他の出力装置６１２の例はプリンター、切符プリンター、プロッター、プロジェクター、音声カード又は映像カード、スピーカー、ブザー又は圧電素子又は他の可聴装置、ランプ又はＬＥＤ又はＬＣＤ指示器、触覚装置、作動装置又はサーボを含む。

【００７５】
少なくとも一つの入力装置６１４が、信号、データ、コマンド選択、又はジェスチャーをプロセッサ６０４ に伝えるためにＩ／Ｏサブシステム６０２に結合される。入力装置６１４の例は、タッチスクリーン、マイクロフォン、静止及びビデオデジタルカメラ、英数字及び他のキー、キーパッド、キーボード、グラフィックスタブレット、イメージスキャナー、ジョイスティック、クロック、スイッチ、ボタン、ダイヤル、スライド、及び／又は様々な種類のセンサー、例えば力センサー、動きセンサー、熱センサー、加速度計、ジャイロスコープ、及び慣性測定ユニット（ＩＭＵ）センサー、及び／又は様々な種類の送受信機、例えば携帯電話又はＷｉ－Ｆｉなどの無線装置、無線周波数（ＲＦ）又は赤外線（ＩＲ）送受信機、及び全地球測位システム（ＧＰＳ）送受信機を含む。

【００７６】
別の種類の入力装置は、入力機能に代えて又は加えて、表示画面上でのグラフィカルインターフェースにおけるナビゲーションなどのカーソル制御または他の自動化された制御機能を実行してよい制御装置６１６である。制御装置６１６は、方向情報及びコマンド選択をプロセッサ６０４に通信し、表示器６１２上のカーソル移動を制御するためのタッチパッド、マウス、トラックボール、又はカーソル方向キーであってもよい。入力装置は、第１軸（例えば、ｘ）と第２軸（例えば、ｙ）の２軸の少なくとも２自由度を有してもよく、これはその装置が平面内で位置を指定するのを許す。別の種類の入力装置は、ジョイスティック、ワンド、コンソール、操舵ホイール、ペダル、ギアシフト機構、又は他の種類の制御装置などの有線、無線、又は光学制御装置である。入力装置６１４は、ビデオカメラ及び奥行きセンサーなどの複数の異なる入力装置の組み合わせを含んでもよい。

【００７７】
別の実施形態では、コンピュータシステム６００は、出力装置６１２、入力装置６１４、及び制御装置６１６のうちの１つ以上が省略された物のインターネット（ＩｏＴ）装置を含んでもよい。或いは、そのような実施形態では、入力装置６１４は、１つ以上のカメラ、動き検出器、温度計、マイクロフォン、振動検出器、他のセンサー又は検出器、測定装置又はエンコーダーを含んでもよく、出力装置６１２は、単一ラインＬＥＤ又はＬＣＤ表示器などの特殊用途表示器、１つ以上の指示器、表示パネル、計器、バルブ、ソレノイド、作動装置、又はサーボを含んでもよい。

【００７８】
コンピュータシステム６００が携帯計算装置である時、入力装置６１４は、複数のＧＰＳ衛星に対して三角測量し、コンピュータシステム６００の地球物理的位置の緯度‐経度値などの地理位置データを測定し生成できるＧＰＳモジュールに結合された全地球測位システム（ＧＰＳ）受信機を含んでもよい。出力装置６１２は、位置報告パケット、通知、パルス又はハートビート信号、又は単独で又は他の特定用途向けデータと組み合わせてコンピュータシステム６００の位置を指定する他の繰り返しデータ送信であってホスト６２４又はサーバー６３０に向けられたデータ送信を生成するためのハードウェア、ソフトウェア、ファームウェア、及びインターフェースを含んでもよい。

【００７９】
コンピュータシステム６００は、カスタム配線論理、少なくとも１つのＡＳＩＣ又はＦＰＧＡ、ファームウェア、及び／又はロードされコンピュータシステムと共に使用又は実行される時、コンピュータシステムを特殊用途マシンとして動作させる又は動作するようにプログラムするプログラム命令群又は論理を使用して本書に記載された手法を実行してもよい。１つの実施形態によれば、本書の手法は、プロセッサ６０４が主メモリ６０６に収容された少なくとも１つの命令の少なくとも１つのシーケンスを実行するのに応答して、コンピュータシステム６００により実行される。このような命令群は主メモリ６０６に別の記憶媒体、例えば記憶装置６１０から読み込まれてもよい。主メモリ６０６に収容された命令シーケンスの実行はプロセッサ６０４に本書に記載されたプロセスステップを実行させる。別の実施形態では、配線回路がソフトウェア命令群の代わりに又はと組み合わせて使用されてもよい。

【００８０】
本書で使用する用語「記憶媒体」はデータ及び／又はマシンを特定のやり方で動作させる命令群を記憶する任意の持続性媒体を指す。このような記憶媒体は不揮発性媒体及び／又は揮発性媒体であってもよい。不揮発性媒体は、例えば記憶装置６１０などの光学又は磁気ディスクを含む。揮発性媒体は動的メモリ、例えばメモリ６０６を含む。一般的な形態の記憶媒体は、例えばハードディスク、半導体ドライブ、フラッシュドライブ、磁気データ記憶媒体、任意の光学又は物理的データ記憶媒体、メモリチップなどを含む。
【００８１】
記憶媒体は伝送媒体と異なるが、一緒に使用されてもよい。伝送媒体は記憶媒体間の情報の移送に関わる。例えば、伝送媒体は同軸ケーブル、銅線、及び光ファイバーを含み、Ｉ／Ｏサブシステム６０２のバスを成す配線も含む。伝送媒体はまた、電波及び赤外線データ通信時に発生させるような音波又は光波の形態を取りうる。
【００８２】
様々な形態の媒体が少なくとも１つの命令の少なくとも１つのシーケンスを実行のためにプロセッサ６０４に運ぶのに関わってもよい。例えば、命令群は最初遠隔のコンピュータの磁気ディスク又は半導体ドライブ上に搭載されてもよい。遠隔のコンピュータはその命令群をその動的メモリにロードして命令群を光ファイバー又は同軸ケーブル、又はモデムを使う電話回線などの通信回線を通じて送信できる。コンピュータシステム６００のモデム又はルーターは通信回線上のそのデータを受信してコンピュータシステム６００が読める形式に変換できる。例えば、無線周波数アンテナ又は赤外線検出器などの受信機は無線又は光信号で運ばれるデータを受信でき、適切な回路が、バス上にデータを載せるようにそのデータをＩ／Ｏサブシステム６０２に提供できる。Ｉ／Ｏサブシステム６０２はそのデータをメモリ６０６に運び、プロセッサ６０４はそのメモリからその命令群を読み出し実行する。メモリ６０６が受け取った命令群は、プロセッサ６０４による実行前か後かに任意選択で記憶装置６１０上に記憶されてもよい。
【００８３】
コンピュータシステム６００はまた、バス６０２に結合された通信インターフェース６１８を含む。通信インターフェース６１８は少なくとも１つの通信ネットワーク、例えばネットワーク６２２又はインターネット上の公開又は社内クラウドに直接又は間接的に接続されたネットワークリンク６２０への双方向データ通信結合を提供する。例えば、通信インターフェース６１８はＥｔｈｅｒｎｅｔ（登録商標）ネットワークインターフェース、総合デジタル通信網（ＩＳＤＮ）カード、ケーブルモデム、衛星モデム、又は対応する種類の通信回線、例えばＥｔｈｅｒｎｅｔケーブル又は任意の種類の金属ケーブル又は光ファイバー回線又は電話回線へのデータ通信接続を提供するモデムであってもよい。ネットワーク６２２は、広くはローカルエリア・ネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、キャンパスネットワーク、相互接続ネットワーク、又はそれらの任意の組み合わせを表わす。通信インターフェース６１８は、互換のＬＡＮへのデータ通信接続を提供するためのＬＡＮカード、又はセルラー無線電話ワイヤレスネットワーク規格に従ってセルラーデータを送信又は受信するように配線されたセルラー無線電話インターフェース、又は衛星ワイヤレスネットワーク規格に従ってデジタルデータを送信又は受信するように配線された衛星無線インターフェースを含んでよい。どんなそのような実施形態でも、通信インターフェース６１８は、様々な種類の情報を表わすデジタルデータストリームを運ぶ信号経路を通じて、電気信号、電磁信号、又は光信号を送信し受信する。
【００８４】
ネットワークリンク６２０は通常、例えば衛星、セルラー、Ｗｉ-Ｆｉ、又はＢＬＵＥＴＯＯＴＨ（登録商標）技術を使った、直接又は少なくとも１つのネットワークを介した他のデータ装置への電気、電磁、又は光データ通信を提供する。例えば、ネットワークリンク６２０は、ネットワーク６２２を通じたホストコンピュータ６２４への接続を提供してもよい。
【００８５】

また、ネットワークリンク６２０は、ネットワーク６２２を通じた、又はＬＡＮ間接続装置及び／又はインターネットサービスプロバイダー（ＩＳＰ）６２６によって運営されるコンピュータを介して他の計算装置への接続を提供してもよい。ＩＳＰ６２６は、インターネット６２８として表される世界規模のパケットデータ通信網を通じたデータ通信サービスを提供する。サーバーコンピュータ６３０はインターネット６２８に結合されてもよい。サーバー６３０は、広くは任意のコンピュータ、データセンター、ハイパーバイザーを有するか又は有しない仮想マシン又は仮想コンピュータインスタンス、又はＤＯＣＫＥＲ又はＫＵＢＥＲＮＥＴＥＳなどのコンテナ化されたプログラムシステムを実行するコンピュータを表わす。サーバー６３０は、２つ以上のコンピュータ又はインスタンスを使って実行され、ウェブサービス要求、ＨＴＴＰペイロード内にパラメータを持つユニフォームリソースロケータ（ＵＲＬ）文字列、ＡＰＩ呼び出し、アプリサービス呼び出し、又は他のサービス呼び出しを送信することでアクセスされ、使用される電子デジタルサービスを表わしてもよい。コンピュータシステム６００及びサーバー６３０は、他のコンピュータ、処理クラスター、サーバーファーム、又はタスクを実行するか又はアプリケーション又はサービスを実行するために協働するコンピュータの他の組織を含む分散コンピュータシステムの要素を成してもよい。サーバー６３０は、モジュール、メソッド、オブジェクト、関数、ルーチン、又は呼び出しとして構成された命令の１つ以上の組を備えてもよい。命令群は、１つ以上のコンピュータプログラム、オペレーティングシステムサービス、又はモバイルアプリを含むアプリケーションプログラムとして構成されてもよい。命令群は、オペレーティングシステム及び／又はシステムソフトウェア；マルチメディア、プログラミング、又は他の機能をサポートする１つ以上のライブラリ；ＴＣＰ／ＩＰ、ＨＴＴＰ、又は他の通信プロトコルを実行するデータプロトコル命令群又はスタック；ＨＴＭＬ、ＸＭＬ、ＪＰＥＧ、ＭＰＥＧ、又はＰＮＧを使ってコード化されたファイルを解析又は解釈するファイルフォーマット処理命令群；グラフィカルユーザーインターフェース（ＧＵＩ）、コマンドラインインターフェース、又はテキストユーザーインターフェース用のコマンドを翻訳又は解釈するユーザーインターフェース命令群；アプリケーションソフトウェア、例えばオフィススイート、インターネットアクセスアプリケーション、設計及び製造アプリケーション、グラフィックアプリケーション、音声アプリケーション、ソフトウェア工学アプリケーション、教育アプリケーション、ゲーム、又は種々雑多なアプリケーションを含んでよい。サーバー６３０は、プレゼンテーション層、アプリケーション層、及びデータ記憶層、例えば構造化照会言語（ＳＱＬ）を使用する又はＳＱＬを使用しない関係型データベースシステム、オブジェクトストア、グラフデータベース、フラットファイルシステム、又は他のデータ記憶の働きをするウェブアプリケーションサーバーを含んでもよい。

【００８６】

コンピュータシステム６００は、ネットワーク、ネットワークリンク６２０及び通信インターフェース６１８を通じて、メッセージを送り、プログラムコードを含むデータ及び命令群を受信できる。インターネットの例では、サーバー６３０は、インターネット６２８、ＩＳＰ６２６、ローカルネットワーク６２２、及び通信インターフェース６１８を通じて、アプリケーションプログラムの要求されたコードを送信してもよい。受信されたコードは、受信されながらプロセッサ６０４によって実行されても、及び／又は、後で実行するために記憶６１０又は他の不揮発性記憶装置に記憶されてもよい。

【００８７】

この項に説明された命令群の実行は、プログラムコード及びその現在の働きから成り実行されているコンピュータプログラムのインスタンスの形態でプロセスを実行してもよい。オペレーティングシステム（ＯＳ） に依って、プロセスは、命令群を同時に実行する複数の実行スレッドから構成されてもよい。この状況において、コンピュータプログラムは命令の受動的な集合である一方、プロセスはそれらの命令の実際の実行であってもよい。幾つかのプロセスは同じプログラムに関連してもよく、例えば、同じプログラムの幾つかのインスタンスを開始することは、２つ以上のプロセスが実行されていることをしばしば

意味する。マルチタスク処理が、複数のプロセスがプロセッサ６０４を共用することを許すために実行されてもよい。各プロセッサ６０４又はそのプロセッサの各コアは一度に１つだけのタスクを実行するが、コンピュータシステム６００は、各プロセッサが各タスクが終了するのを待つことなく、実行されているタスクを切り換えるのを許すようにマルチタスク処理を実行するようにプログラムされてもよい。１つの実施形態では、タスクが入出力動作を実行する時、タスクが切り換えられうることを示す時、又はハードウェア割り込み後に、切り換えが実行されてもよい。複数のプロセスが同時実行されていると見えるようにするためにコンテキスト切り替えを迅速に実行することで、対話型ユーザーアプリケーションの速い応答を可能にするように、時分割が実行されてもよい。１つの実施形態では、機密保護及び信頼性のために、オペレーティングシステムは、独立したプロセス間の直接通信を防止し、厳密に仲介され制御されたプロセス間通信機能を提供してもよい。

【００８８】

７．０　開示の他の態様

上記の明細書において、本発明の実施形態を、実施形態間で異なりうる多数の特定の詳細を参照して説明した。従って、何が本発明か、及び本出願人によって何が本発明であると意図されているかの唯一で専用の指標は、後で行われるどんな補正も含め、本願に提示された一組の特定の提示形態の請求項である。請求項に含まれる用語の本明細書に明記されたどんな定義も請求項で使用されるそれらの用語の意味を決定する。従って、請求項に明記されていないどんな限定、要素、特性、特徴、長所、又は属性も特許請求の範囲を決して限定すべきでない。従って、本明細書及び図面は、限定的な意味ではなく、例示の意味で理解されるべきである。

【００８９】

本明細書において用いられる用語「include」及び「comprise」（及びそれらの用語のバリエーション、例えば「including」、「includes」、「comprising」、「comprises」、「comprised」など）は、包含的であると意図され、追加の特徴、構成要素、ユニット、又はステップを除外するよう意図されていない。

【００９０】

フローチャートを使って様々な動作を説明した。ある場合は、特定のフローチャートステップの機能／処理は説明したのと異なるやり方で、及び／又は異なるシステム又はシステムモジュールによって実行されてもよい。また、幾つかの場合、フローチャートに描かれた特定の動作は複数の動作に分割され、及び／又は複数のフローチャート動作は結合され１つの動作になってもよい。また、ある場合は、フローチャートに描かれ説明される動作の順序は、本開示の範囲を逸脱することなく変更可能でありうる。

【００９１】

本明細書において開示及び規定された実施形態は、文章又は図面に記述された又はから明らかな個々の特徴のうち２つ以上の代わりの全ての組合せも含むことは理解されるであろう。これらの異なる組合せの全てが、実施形態の様々な別の態様を構成する。

以下、本発明の好ましい実施形態を項分け記載する。

実施形態１

データがネットワーク内及びネットワーク間を流れる時のデータ管理を提供するコンピュータ実行方法であって、

階層を成すデジタル台帳内の複数のハッシュチェーンに記憶され複数の第１ゲートウェイ計算装置によって書き込まれたデータを第２ゲートウェイ計算装置によってアクセスするステップであって、前記複数のハッシュチェーンに記憶された前記データの有効性は書き込む前に検証されていない、ステップと、

前記第２ゲートウェイ計算装置によって前記複数のハッシュチェーンのそれぞれを前記複数のハッシュチェーンの他の全てのハッシュチェーンと比較し前記複数のハッシュチェーンが暗号上一致するかを判断することで、前記複数のハッシュチェーンに記憶された前記データの合意を検出するステップと、

前記複数のハッシュチェーンに記憶された前記データの合意を検出したことに応答して

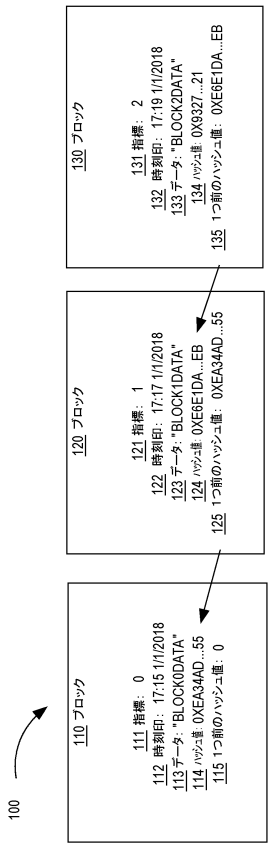
、前記複数のハッシュチェーンに記憶された前記データを使用して記憶されたブロックチェーンデータを前記第２ゲートウェイ計算装置によって更新するステップと
を含むコンピュータ実行方法。
実施形態２
前記複数のハッシュチェーンのそれぞれを比較する前記ステップは、前記複数のハッシュチェーンのハッシュ値同士を比較することを含む、実施形態１に記載のコンピュータ実行方法。
実施形態３
前記記憶されたブロックチェーンデータはブロックチェーンに記憶され、前記ブロックチェーンは分散されたデジタル台帳である、実施形態１に記載のコンピュータ実行方法。
実施形態４
前記ブロックチェーンは前記階層を成すデジタル台帳内にある、実施形態３に記載のコンピュータ実行方法。
実施形態５
前記ブロックチェーンは前記階層を成すデジタル台帳内の前記ハッシュチェーンが存在する１つ以上の層より高い１つの層に存在する、実施形態４に記載のコンピュータ実行方法。
実施形態６
前記記憶されたブロックチェーンデータを第三者と共有する前に前記記憶されたブロックチェーンデータを非対称に暗号化するステップを更に含む実施形態１に記載のコンピュータ実行方法。
実施形態７
データがネットワーク内及びネットワーク間を流れる時のデータ管理を提供するためにプログラムされた１つ以上の命令を記憶する１つ以上の持続性コンピュータ読取可能記憶媒体であって、前記１つ以上の命令は、１つ以上の計算装置によって実行される時、
階層を成すデジタル台帳内の複数のハッシュチェーンに記憶され複数の第１ゲートウェイ計算装置によって書き込まれたデータを第２ゲートウェイ計算装置によってアクセスするステップであって、前記複数のハッシュチェーンに記憶された前記データの有効性は書き込む前に検証されていない、ステップと、
前記第２ゲートウェイ計算装置によって前記複数のハッシュチェーンのそれぞれを前記複数のハッシュチェーンの他の全てのハッシュチェーンと比較し前記複数のハッシュチェーンが暗号上一致するかを判断することで、前記複数のハッシュチェーンに記憶された前記データの合意を検出するステップと、
前記複数のハッシュチェーンに記憶された前記データの合意を検出したことに応答して、前記複数のハッシュチェーンに記憶された前記データを使用して記憶されたブロックチェーンデータを前記第２ゲートウェイ計算装置によって更新するステップと
を実行させる、１つ以上の持続性コンピュータ読取可能記憶媒体。
実施形態８
前記複数のハッシュチェーンのそれぞれを比較する前記ステップは、前記複数のハッシュチェーンのハッシュ値同士を比較することを含む、実施形態７に記載の１つ以上の持続性コンピュータ読取可能記憶媒体。
実施形態９
前記記憶されたブロックチェーンデータはブロックチェーンに記憶され、前記ブロックチェーンは分散されたデジタル台帳である、実施形態７に記載の１つ以上の持続性コンピュータ読取可能記憶媒体。
実施形態１０
前記ブロックチェーンは前記階層を成すデジタル台帳内にある、実施形態９に記載の１つ以上の持続性コンピュータ読取可能記憶媒体。
実施形態１１
前記ブロックチェーンは前記階層を成すデジタル台帳内の前記ハッシュチェーンが存在

する１つ以上の層より高い１つの層に存在する、実施形態１０に記載の１つ以上の持続性コンピュータ読取可能記憶媒体。
実施形態１２
前記１つ以上の命令は、前記１つ以上の計算装置によって実行される時、前記記憶されたブロックチェーンデータを第三者と共有する前に前記記憶されたブロックチェーンデータを非対称に暗号化するステップを更に実行させる、実施形態７に記載の１つ以上の持続性コンピュータ読取可能記憶媒体。
実施形態１３
データがネットワーク内及びネットワーク間を流れる時のデータ管理を提供するコンピュータシステムであって、
台帳データリポジトリと、
前記台帳データリポジトリに通信可能に結合され一組の命令を記憶する持続性データ記憶媒体を備えたグローバルゲートウェイ計算装置であって、前記一組の命令は、該グローバルゲートウェイ計算装置によって実行される時、
階層を成すデジタル台帳内の複数のハッシュチェーンに記憶され複数の第１ゲートウェイ計算装置によって書き込まれたデータを第２ゲートウェイ計算装置によってアクセスするステップであって、前記複数のハッシュチェーンに記憶された前記データの有効性は書き込む前に検証されていない、ステップと、
前記第２ゲートウェイ計算装置によって前記複数のハッシュチェーンのそれぞれを前記複数のハッシュチェーンの他の全てのハッシュチェーンと比較し前記複数のハッシュチェーンが暗号上一致するかを判断することで、前記複数のハッシュチェーンに記憶された前記データの合意を検出するステップと、
前記複数のハッシュチェーンに記憶された前記データの合意を検出したことに応答して、前記複数のハッシュチェーンに記憶された前記データを使用して記憶されたブロックチェーンデータを前記第２ゲートウェイ計算装置によって更新するステップと
を実行させる、グローバルゲートウェイ計算装置と
を備えるコンピュータシステム。
実施形態１４
前記複数のハッシュチェーンのそれぞれを比較する前記ステップは、前記複数のハッシュチェーンのハッシュ値同士を比較することを含む、実施形態１３に記載のコンピュータシステム。
実施形態１５
前記記憶されたブロックチェーンデータは、ブロックチェーンを備える前記台帳データリポジトリに記憶される、実施形態１３に記載のコンピュータシステム。
実施形態１６
前記ブロックチェーンは前記階層を成すデジタル台帳内にある、実施形態１５に記載のコンピュータシステム。
実施形態１７
前記ブロックチェーンは前記階層を成すデジタル台帳内の前記ハッシュチェーンが存在する１つ以上の層より高い１つの層に存在する、実施形態１６に記載のコンピュータシステム。
実施形態１８
前記一組の命令は、前記グローバルゲートウェイ計算装置によって実行される時、前記記憶されたブロックチェーンデータを第三者と共有する前に前記記憶されたブロックチェーンデータを非対称に暗号化するステップを更に実行させる、実施形態１３に記載のコンピュータシステム。
【符号の説明】
【００９２】
１００　データリポジトリ
２００　階層構成

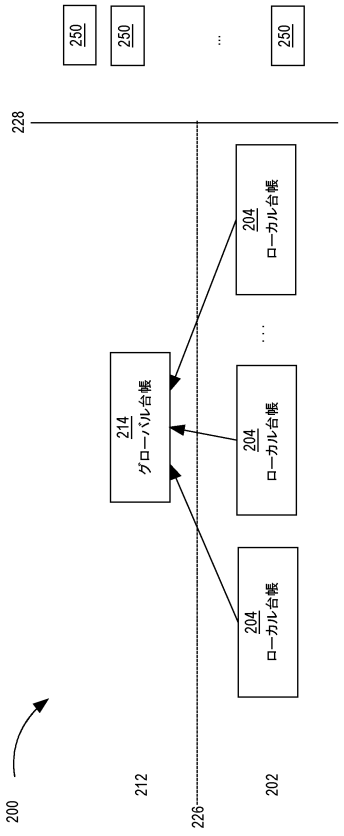
２０４　ローカル台帳
２１４　グローバル台帳
２５０　第三者
３００、４００、６００　コンピュータシステム
３０２　主体
３１０　ローカルノード
３１２　ローカルゲートウェイ
３１２ａ　受信命令群
３１２ｂ　暗号化命令群
３１２ｃ　処理命令群
３２０　グローバルノード
３２２　グローバルゲートウェイ
３２２ａ　受信命令群
３２２ｂ　分析命令群
３２２ｃ　暗号化命令群
３２２ｄ　処理命令群
３２４　コンピュータ
３２６　ブローカーコンピュータ
３２８　管理者コンピュータ

【図面】

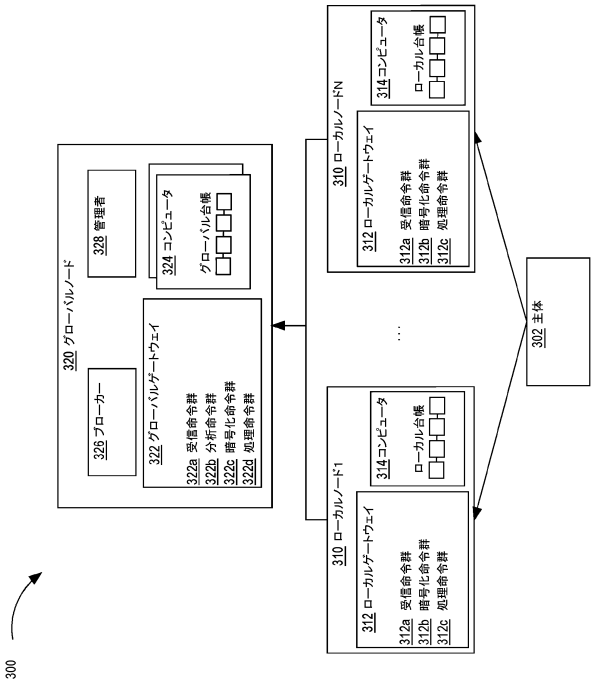
【図１】



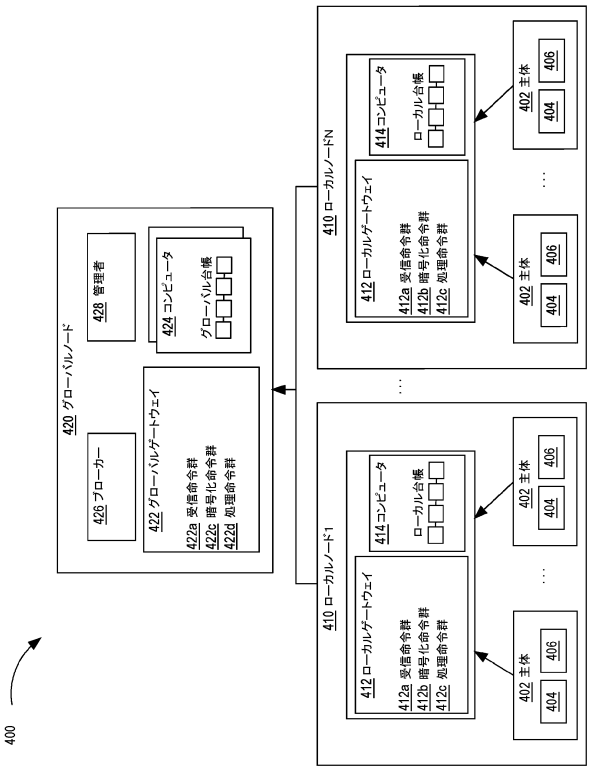
【図２】



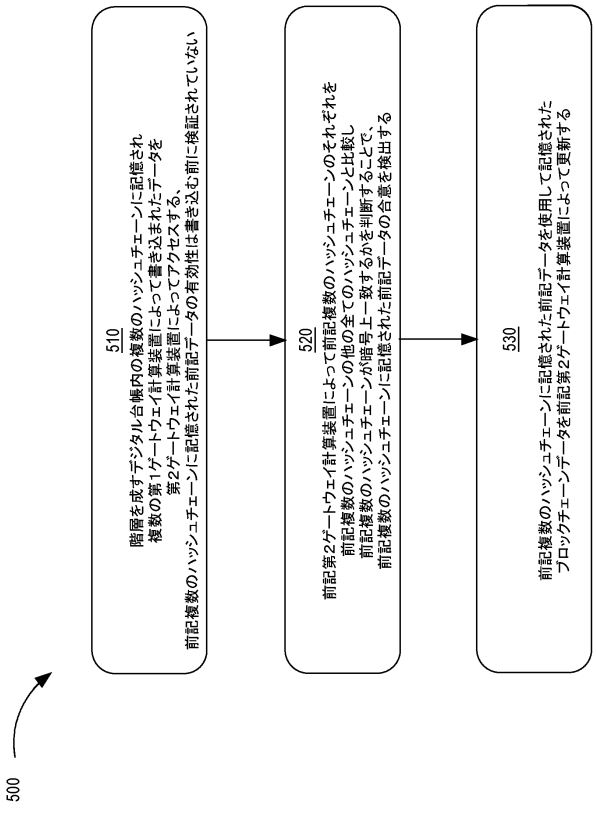
【図３】


300
320 グローバルノード
326 ブローカー
328 管理者
322 グローバルゲートウェイ
322a 受信命令群
322b 分析命令群
322c 暗号化命令群
322d 処理命令群
324 コンピュータ
グローバル台帳
310 ローカルノード1
312 ローカルゲートウェイ
312a 受信命令群
312b 暗号化命令群
312c 処理命令群
314 コンピュータ
ローカル台帳
310 ローカルノードN
312 ローカルゲートウェイ
312a 受信命令群
312b 暗号化命令群
312c 処理命令群
314 コンピュータ
ローカル台帳
302 主体

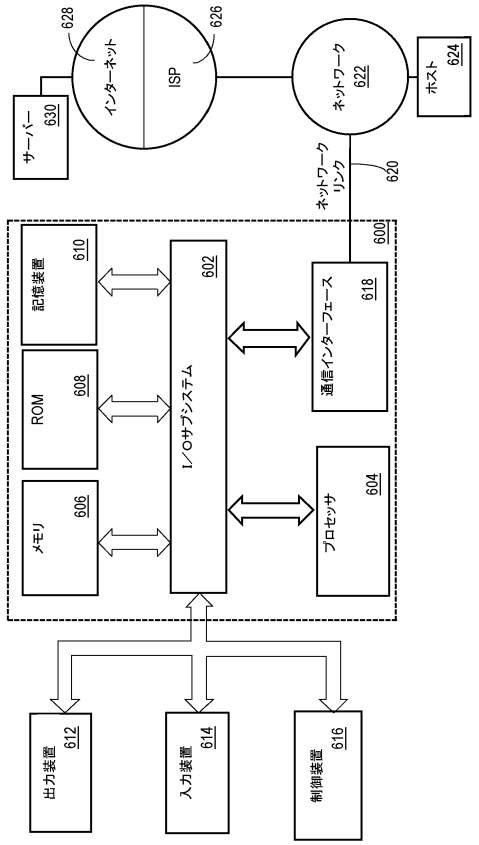
【図４】


400
420 グローバルノード
426 ブローカー
428 管理者
422 グローバルゲートウェイ
422a 受信命令群
422c 暗号化命令群
422d 処理命令群
424 コンピュータ
グローバル台帳
410 ローカルノード1
412 ローカルゲートウェイ
412a 受信命令群
412b 暗号化命令群
412c 処理命令群
414 コンピュータ
ローカル台帳
410 ローカルノードN
412 ローカルゲートウェイ
412a 受信命令群
412b 暗号化命令群
412c 処理命令群
414 コンピュータ
ローカル台帳
402 主体
404
406

【図５】


500
510
階層を成すデジタル台帳内の複数のハッシュチェーンに記憶され
複数の第1ゲートウェイ計算装置によって書き込まれたデータを
第2ゲートウェイ計算装置によってアクセスする、
前記複数のハッシュチェーンに記憶された前記データの有効性は書き込む前に検証されていない
520
前記第2ゲートウェイ計算装置によって前記複数のハッシュチェーンのそれぞれを
前記複数のハッシュチェーンの他の全てのハッシュチェーンと比較し
前記複数のハッシュチェーンが暗号上一致するかを判断することで、
前記複数のハッシュチェーンに記憶された前記データの合意を検出する
530
前記複数のハッシュチェーンに記憶された前記データを使用して記憶された
ブロックチェーンデータを前記第2ゲートウェイ計算装置によって更新する

【図６】


628
インターネット
ISP
626
サーバー
630
ネットワーク
622
ホスト
624
ネットワーク
リンク
620
600
記憶装置
610
ROM
608
メモリ
606
I／Oサブシステム
602
通信インターフェース
618
プロセッサ
604
出力装置
612
入力装置
614
制御装置
616

フロントページの続き

アメリカ合衆国 カリフォルニア州 ９４３０６ パロ アルト シャーマン アヴェニュー ４４５ スイート ２００
(72)発明者 ヴァルデラマ，アレクサンダー マイケル
アメリカ合衆国 カリフォルニア州 ９４３０６ パロ アルト シャーマン アヴェニュー ４４５ スイート ２００
(72)発明者 ジャオ，ティエンユィ
アメリカ合衆国 カリフォルニア州 ９４３０６ パロ アルト シャーマン アヴェニュー ４４５ スイート ２００
(72)発明者 ファム，トゥ
アメリカ合衆国 カリフォルニア州 ９４３０６ パロ アルト シャーマン アヴェニュー ４４５ スイート ２００

審査官 行田 悦資
(56)参考文献 米国特許出願公開第２０１９／０２８０８７０（ＵＳ，Ａ１）
米国特許出願公開第２０１９／０３１９７９２（ＵＳ，Ａ１）
特表２０２１－５２０７１４（ＪＰ，Ａ）
米国特許出願公開第２０１９／０２４３５７２（ＵＳ，Ａ１）
国際公開第２０１８／２０７０６４（WO，Ａ１）
特表２０２０－５１８９０７（ＪＰ，Ａ）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／６４