

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6963613号
(P6963613)

(45) 発行日 令和3年11月10日(2021.11.10)

(24) 登録日 令和3年10月19日(2021.10.19)

(51) Int. Cl.	F I
G06F 21/12 (2013.01)	G06F 21/12 310
G06F 9/455 (2006.01)	G06F 9/455 150
G06F 21/60 (2013.01)	G06F 21/60 320
G06F 21/64 (2013.01)	G06F 21/60 340
	G06F 21/64

請求項の数 29 (全 26 頁)

(21) 出願番号	特願2019-527877 (P2019-527877)	(73) 特許権者	390009531
(86) (22) 出願日	平成29年12月7日 (2017.12.7)		インターナショナル・ビジネス・マシーンズ・コーポレーション
(65) 公表番号	特表2020-503598 (P2020-503598A)		INTERNATIONAL BUSINESS MACHINES CORPORATION
(43) 公表日	令和2年1月30日 (2020.1.30)		アメリカ合衆国10504 ニューヨーク州 アーモンク ニュー オーチャードロード
(86) 国際出願番号	PCT/EP2017/081786		New Orchard Road, Armonk, New York 10504, United States of America
(87) 国際公開番号	W02018/108685	(74) 代理人	100108501
(87) 国際公開日	平成30年6月21日 (2018.6.21)		弁理士 上野 剛史
審査請求日	令和2年6月24日 (2020.6.24)		
(31) 優先権主張番号	15/379,196		
(32) 優先日	平成28年12月14日 (2016.12.14)		
(33) 優先権主張国・地域又は機関	米国 (US)		

最終頁に続く

(54) 【発明の名称】 コンテナベースのオペレーティング・システムおよび方法

(57) 【特許請求の範囲】

【請求項1】

ブロックチェーン内のトランザクションを記録するパブリックな台帳を含んでいる前記ブロックチェーンの1つまたは複数のシステム・インスタンスをホストするのに適した構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワークであって、前記分散ネットワークが、

1つまたは複数のシステム・インスタンスを備えており、各システム・インスタンスが、仮想マシンおよびコンテナのセットを備えており、前記コンテナが前記仮想マシン上で実行されるよう機能し、各コンテナが、前記コンテナ上で前記ブロックチェーンを実行するよう機能するブロックチェーン・サブシステムを備えており、前記セットの各コンテナが前記パブリックな台帳を参照して前記分散ネットワーク内の別のコンテナも前記セットに属しているかどうかを判定し、前記セット内にはない他のコンテナとの望ましくない情報のやりとりを防ぐためのバリアとして機能する前記コンテナのセットのシステム境界を作成できるように、前記セットの前記コンテナが前記ブロックチェーンのメンバーになり、前記パブリックな台帳が、前記セットの各コンテナの少なくとも選択された一部の暗号化されたコピーを記録するように、前記ブロックチェーンが定義されている、分散ネットワーク。

【請求項2】

システム・インスタンスごとに1つのコンテナが、システム・インスタンス・コントローラの役割を持つように、どの時点においても指定され、前記システム・インスタンス・

コントローラが、前記セットの新しいコンテナを作成するための独占権を持っており、前記システム・インスタンス・コントローラが、そのような新しいコンテナを作成するよう機能する、請求項 1 に記載の分散ネットワーク。

【請求項 3】

前記システム・インスタンス・コントローラの役割が、前記セットの前記コンテナのうちの異なるコンテナ間で時間と共に交代されるように、前記ブロックチェーンが構成されている、請求項 2 に記載の分散ネットワーク。

【請求項 4】

コンテナがソフトウェアの更新を受信するときに常に、前記更新されたコンテナの暗号化されたコピーが前記パブリックな台帳に記録されるように、前記ブロックチェーンが構成されている、請求項 1 に記載の分散ネットワーク。

10

【請求項 5】

前記セットのコンテナが、前記セット内にある可能性がある、またはない可能性がある他のコンテナとの通信を開始するよう機能し、前記コンテナが、前記パブリックな台帳で、前記パブリックな台帳内の前記他のコンテナの暗号化されたコピーを検索することによって、前記他のコンテナが前記セット内にあるかどうかをチェックすることができる、請求項 1 に記載の分散ネットワーク。

【請求項 6】

前記セットの前記コンテナが、前記他のコンテナが前記セット内にはないということを決めた場合、前記コンテナが、前記他のコンテナが前記セット内にはないということの前記パブリックな台帳に記録するよう機能する、請求項 5 に記載の分散ネットワーク。

20

【請求項 7】

前記複数のシステム・インスタンスが前記分散ネットワーク上で共存する、請求項 1 に記載の分散ネットワーク。

【請求項 8】

前記分散ネットワークが、前記システム・インスタンスのいずれにも属せず、前記ブロックチェーンの一部ではないコンテナをさらに含んでいる、請求項 1 に記載の分散ネットワーク。

【請求項 9】

前記ブロックチェーンが、前記セットの各コンテナが別のブロックチェーンに属しているということが起きないように定義される、請求項 1 に記載の分散ネットワーク。

30

【請求項 10】

前記システム境界が、前記分散ネットワークを形成する構成可能なコンピューティング・リソースの前記共有プールにおいて、前記コンテナが存在できる場所に対して物理的制限を課す地理的制約になるように、前記ブロックチェーンが定義される、請求項 1 に記載の分散ネットワーク。

【請求項 11】

仮想マシン上で実行されるよう機能するコンテナを備えているシステムであって、前記コンテナが、

メモリ・リソースと、
処理リソースと、

40

前記処理リソースを使用して前記コンテナ上でブロックチェーンを実行するよう機能するブロックチェーン・サブシステムであって、前記ブロックチェーンがパブリックな台帳を含んでいる、前記ブロックチェーン・サブシステムと、

前記メモリ・リソースに格納された前記パブリックな台帳のコピーとを備えており、

前記パブリックな台帳が、前記コンテナおよび 1 つまたは複数の他のコンテナそれぞれの選択された一部の暗号化されたコピーを記録するように、前記ブロックチェーンが定義されており、前記他のコンテナが、前記ブロックチェーンのメンバーであるコンテナのセットを集合的に構成する、システム。

【請求項 12】

50

前記ブロックチェーンの新しいコンテナを作成するための独占権が、前記コンテナに属するものと見なされる、請求項 1 1 に記載のシステム。

【請求項 1 3】

前記コンテナを格納するコンピュータ・プログラム製品をさらに備えている、請求項 1 1 に記載のシステム。

【請求項 1 4】

ブロックチェーンのシステム・インスタンスが存在している構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワーク内で実行される新しいコンテナを作成する方法であって、前記ブロックチェーンのメンバーがコンテナであり、前記ブロックチェーンが、前記ブロックチェーン内のトランザクションを記録するパブリックな台帳を含んでおり、前記パブリックな台帳がセットの各コンテナの 1 つまたは複数の選択された一部の暗号化されたコピーを記録するように、前記ブロックチェーンが定義されており、前記方法が、

システム・インスタンス・コントローラの役割を持つように、前記コンテナのうちの 1 つを指定することであって、前記システム・インスタンス・コントローラが、前記セットの新しいコンテナを作成するための独占権を持っている、前記指定することと、

前記システム・インスタンス・コントローラによって新しいコンテナを作成することと、

前記新しいコンテナの作成がブロックチェーン・トランザクションとして実行されるように、前記新しいコンテナの選択された一部のコピーを暗号化することと、

前記暗号化されたコピーを前記パブリックな台帳に記録することとを含んでいる、方法

【請求項 1 5】

ブロックチェーンのシステム・インスタンスが存在している構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワーク内に存在するコンテナ上でソフトウェアの更新を実行する方法であって、前記ブロックチェーンのメンバーが、前記ソフトウェアの更新が実行される前記コンテナを含んでいる複数のコンテナであり、前記ブロックチェーンが、前記ブロックチェーン内のトランザクションを記録するパブリックな台帳を含んでおり、前記方法が、

前記コンテナ上で前記ソフトウェアの更新を実行することと、

前記ソフトウェアの更新がブロックチェーン・トランザクションとして実行されるように、前記更新されたコンテナの 1 つまたは複数の選択された一部のコピーを暗号化することと、

前記更新されたコンテナの前記 1 つまたは複数の選択された一部の暗号化されたコピーを前記パブリックな台帳に記録することとを含んでいる、方法。

【請求項 1 6】

コンテナの同じセットに第 2 のコンテナが属しているかどうかを第 1 のコンテナが決定するための方法であって、前記方法が、ブロックチェーンのシステム・インスタンスが存在している構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワーク内で実行され、前記ブロックチェーンのメンバーが、少なくとも前記第 1 のコンテナを含んでいる前記コンテナのセットの前記コンテナであり、前記ブロックチェーンが、前記ブロックチェーン内のトランザクションを記録するパブリックな台帳を含んでおり、前記パブリックな台帳が前記セットの各コンテナの少なくとも選択された一部の暗号化されたコピーを記録するように、前記ブロックチェーンが定義されており、前記方法が、

前記第 1 のコンテナが、ソフトウェア・コマンドのシーケンスを実行する過程において、前記第 2 のコンテナにアクセスするためのコマンドを識別することと、

前記第 1 のコンテナが、前記第 2 のコンテナへのネットワーク接続を確立し、前記第 2 のコンテナの識別番号に関する情報を取得することと、

前記第 1 のコンテナが、前記パブリックな台帳を参照して、前記第 2 のコンテナが前記ブロックチェーンのトランザクションに記録されているかどうかを判定することと、

そのようなトランザクションが存在しない場合に、前記第2のコンテナが前記ブロックチェーンのメンバーでないということを推測し、前記第2のコンテナにアクセスするための前記コマンドを実行することを抑制することと、

そのようなトランザクションが存在する場合に、前記第2のコンテナが前記ブロックチェーンのメンバーであることを推測し、前記第2のコンテナにアクセスするための前記コマンドを実行することとを含んでいる、方法。

【請求項17】

前記第2のコンテナが前記ブロックチェーンのメンバーでない場合、前記第2のコンテナが前記ブロックチェーンのメンバーでないというこの前記決定がブロックチェーン・トランザクションとして処理されるように、前記第2のコンテナがメンバーでないということを前記パブリックな台帳に記録する、請求項16に記載の方法。

10

【請求項18】

前記セットの前記第1のコンテナが、前記セット内にある可能性がある、またはない可能性がある他のコンテナとの通信を開始するよう機能し、前記第1のコンテナが、前記パブリックな台帳で、前記パブリックな台帳内の前記他のコンテナの暗号化されたコピーを検索することによって、前記他のコンテナが前記セット内にあるかどうかを判定することを実行できる、請求項16に記載の方法。

【請求項19】

前記セットの前記第1のコンテナが、前記他のコンテナが前記セット内にはないということを決定した場合、前記コンテナが、前記他のコンテナが前記セット内にはないということを前記パブリックな台帳に記録するよう機能する、請求項18に記載の方法。

20

【請求項20】

前記ブロックチェーンが、前記セットの各コンテナが別のブロックチェーンに属しているということが起きないように定義される、請求項16に記載の方法。

【請求項21】

ブロックチェーン内のトランザクションを記録するパブリックな台帳を含んでいる前記ブロックチェーンの1つまたは複数のシステム・インスタンスをホストするのに適した構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワーク内で動作できる方法であって、前記分散ネットワークが、1つまたは複数のシステム・インスタンスを備えており、各システム・インスタンスが仮想マシンおよびコンテナのセットを備えており、前記コンテナが、前記仮想マシン上で実行されるよう機能し、各コンテナが、前記コンテナ上で前記ブロックチェーンを実行するよう機能するブロックチェーン・サブシステムを備えており、前記セットの前記コンテナが前記ブロックチェーンのメンバーになって、前記パブリックな台帳が前記セットの各コンテナの少なくとも選択された一部の暗号化されたコピーを記録するように、前記ブロックチェーンが定義されており、前記方法が、

30

前記セットの各コンテナが、別のコンテナと情報をやりとりする前に、前記パブリックな台帳を参照して、前記分散ネットワーク内の前記別のコンテナも前記セットに属しているかどうかを判定し、それによって、前記セット内にはない他のコンテナとの望ましくない情報のやりとりを防ぐためのバリアとして機能する、前記コンテナのセットのシステム境界を作成することを含んでいる、方法。

40

【請求項22】

第1のコンテナが、ソフトウェア・コマンドのシーケンスを実行する過程において、第2のコンテナにアクセスするためのコマンドを識別することと、

前記第1のコンテナが、前記第2のコンテナへのネットワーク接続を確立し、前記第2のコンテナの識別番号に関する情報を取得することと、

前記第1のコンテナが、前記パブリックな台帳を参照して、前記第2のコンテナが前記ブロックチェーンのトランザクションに記録されているかどうかを判定することと、

そのようなトランザクションが存在しない場合に、前記第2のコンテナが前記ブロックチェーンのメンバーでないということを推測し、前記第2のコンテナにアクセスするため

50

の前記コマンドを実行することを抑制することと、

そのようなトランザクションが存在する場合に、前記第2のコンテナが前記ブロックチェーンのメンバーであることを推測し、前記第2のコンテナにアクセスするための前記コマンドを実行することとを含んでいる、請求項21に記載の方法。

【請求項23】

前記第2のコンテナが前記ブロックチェーンのメンバーでない場合、前記第2のコンテナが前記ブロックチェーンのメンバーでないということの推測がブロックチェーン・トランザクションとして処理されるように、前記第2のコンテナがメンバーでないということとを前記パブリックな台帳に記録する、請求項22に記載の方法。

【請求項24】

前記セットの前記第1のコンテナが、前記セット内にある可能性がある、またはない可能性がある他のコンテナとの通信を開始するよう機能し、前記第1のコンテナが、前記パブリックな台帳で、前記パブリックな台帳内の前記他のコンテナの暗号化されたコピーを検索することによって、前記他のコンテナが前記セット内にあるかどうかを判定することとを実行できる、請求項22に記載の方法。

【請求項25】

前記セットの前記第1のコンテナが、前記他のコンテナが前記セット内にはないということとを決定した場合、前記コンテナが、前記他のコンテナが前記セット内にはないということとを前記パブリックな台帳に記録するよう機能する、請求項24に記載の方法。

【請求項26】

前記ブロックチェーンが、前記セットの各コンテナが別のブロックチェーンに属しているということが起きないように定義される、請求項22に記載の方法。

【請求項27】

システム・インスタンス・コントローラの役割を持つように、前記コンテナのうちの1つを指定することとあって、前記システム・インスタンス・コントローラが、前記セットの新しいコンテナを作成するための独占権を持っている、指定することと、

前記システム・インスタンス・コントローラによって新しいコンテナを作成することと、

前記新しいコンテナの作成がブロックチェーン・トランザクションとして実行されるように、前記新しいコンテナの選択された一部のコピーを暗号化することと、

前記暗号化されたコピーを前記パブリックな台帳に記録することとを含んでいる、請求項21に記載の方法。

【請求項28】

コンテナ上でソフトウェアの更新を実行することと、

前記ソフトウェアの更新がブロックチェーン・トランザクションとして実行されるように、前記更新されたコンテナの1つまたは複数の選択された一部のコピーを暗号化することと、

前記更新されたコンテナの前記1つまたは複数の選択された一部の暗号化されたコピーを前記パブリックな台帳に記録することとを含んでいる、請求項21に記載の方法。

【請求項29】

プログラム・コードを含んでいるコンピュータ・プログラムであって、前記プログラムがコンピュータ上で実行された場合に、前記コンピュータに、請求項14ないし28のいずれか1項に記載の前記方法を実行させる、コンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワークのためのコンテナベースのオペレーティング・システム(container-based operating system)および方法に関連する。

【背景技術】

10

20

30

40

50

【 0 0 0 2 】

クラウド・コンピューティング関連の定義および規格が、米国のアメリカ国立標準技術研究所（NIST: National Institute of Standards and Technology）によって開発されている。本文書は、特に、"The NIST Definition of Cloud Computing" (September 20 11) by Peter Mell and Timothy Grance, NIST Special Publication 800-145を参照して解釈される。

【 0 0 0 3 】

クラウド・コンピューティングのNISTの定義は、構成可能なコンピューティング・リソース（例えば、ネットワーク、サーバ、ストレージ、アプリケーション、およびサービス）の共有プールへの偏在する便利なオンデマンドのネットワーク・アクセスを可能にするためのモデルであり、このモデルによって、管理上の手間またはサービス・プロバイダとのやりとりを最小限に抑えて、これらのリソースを迅速にプロビジョニングおよび解放することができる。

10

【 0 0 0 4 】

現在の形態でのクラウド・ストレージは、データを安全にホストするために、顧客によって信頼されたサードパーティを構成するサービス・プロバイダによって支配される。言い換えると、従来のインターネット・バンキングなどでは、または車両登録、不動産所有権などのための中央データベースを提供する政府機関によって、信頼された中央機関モデルが使用されている。

20

【 0 0 0 5 】

図1は、標準的なクラウド・ストレージ・アーキテクチャの概略図である。2人の例示的なユーザ14が示されており、これらのユーザは、クラウド・プロバイダによって所有されているクラウド（すなわち、仮想化サーバ12）に格納したいファイル16を含んでいるコンピュータ・デバイス25をそれぞれ持っている。クラウド・プロバイダは、アプリケーション18をユーザ14に提供し、ユーザ14は、アプリケーション18を介してファイル16を仮想化サーバ12に対してアップロード（すなわち、格納）およびダウンロード（すなわち、アクセス）することができる。次に、仮想化サーバ12は、各クライアントのファイルのデータを格納して、少なくとも最小限の冗長性を保証するために、少なくとも3つの物理サーバ20を使用する。このアーキテクチャ内でエンドツーエンド暗号化を実行する標準的な方法が存在しないため、このアーキテクチャは、セキュリティ脅威に対して脆弱である。基本的な形態では、コンピュータ25、アプリケーション18、およびクラウド・プロバイダのサーバ12、20の間で転送されているクライアントのデータは暗号化されないため、伝送線（スヌーピング）、ユーザ・コンピュータ25、アプリケーション18、およびサーバ12、20の攻撃がすべて起こり得る。

30

【 0 0 0 6 】

この従来のアーキテクチャを避けて、より安全な環境を提供するために、ピアツーピア・ネットワーク構造に基づくブロックチェーン技術を使用することがすぐに行われた。

【 0 0 0 7 】

図2は、例示的なピアツーピア・ネットワーク55を、クラウド・コンピューティング環境の一部として示している。このネットワークはネットワーク・ノード10を含んでおり、各ネットワーク・ノード10は、ユーザが情報をやりとりできる1つまたは複数の物理ハードウェア・ネットワーク・エンティティまたは仮想ハードウェア・ネットワーク・エンティティである。ネットワーク・ノード10は、通信線15によって接続される。ネットワーク・エンティティは、例えば、メインフレーム61、さまざまな種類のサーバ62、63、64、マス・ストレージ・デバイス65であってよく、あるいはパーソナル・コンピュータ、タブレット、スマートフォンなどのより消費者志向のデバイス、または白物家電（冷蔵庫、冷凍庫、洗濯機）、IPカメラ、プリンタ、工場設備、テレビ録画装置などの、モノのインターネット（IoT: internet of things）に関連するデバイスであってよい。

40

【 0 0 0 8 】

50

ブロックチェーン技術は、信頼された中央機関モデルを使用せず、むしろ、図4に示されているように、参加者(すなわち、ピアツーピア・ネットワークの各ノードにいるブロックチェーンのメンバー)間で発生したすべてのトランザクションまたはイベントのパブリックにアクセスできる台帳を含んでいる、記録の分散データベースを提供する。各メンバーは、そのメンバーのアドレスとして機能する公開キー、およびそのメンバーがトランザクションにデジタル署名するために使用する秘密キーを持っている。トランザクションは、秘密キーを使用してそのトランザクションにデジタル署名し、メンバーの公開キーをアドレスとして使用してそのトランザクションを別のメンバーに送信する、1人のメンバーによって有効にされる。次に、受信側メンバーが、送信側メンバーの公開キーを使用して、トランザクションのデジタル署名を検証する。トランザクションは、ブロックチェーン・ネットワークのすべてのノードにブロードキャストされるブロック内に配置され、他のメンバーによって実行される「マイニング」と呼ばれる問題を解くプロセスを通じて、トランザクションおよび同じブロック内のいずれかの他のトランザクションが、有効であるとして検証される。その後、ブロックをチェーンに追加することが許可され、それによって、ブロックがパブリックなトランザクション台帳の一部になる。ブロックチェーンのブロックは、台帳に格納されたリンクされたイベントの常に拡張可能なシーケンスの要素である。1つのブロックをチェーン内の前のブロックにリンクするものは、前のブロックのハッシュである。このハッシュは、マイニングするメンバーが総当たりによって問題を解き、トランザクションのハッシュを決定することにおいて実行した作業の証明であるトークンであると見なすことができる。各ブロックは、タイムスタンプおよびトランザクションの数を含む。各ブロックは、チェーンに埋め込まれると、意図的であろうと、ハッキングによってであろうと、編集することが事実上不可能になり、ブロックが最後のブロックから遠くに移動するにつれて、編集に対するセキュリティが急速に向上する。

【0009】

ブロックチェーン技術は、記事"Blockchain Technology Beyond Bitcoin" by Michael Crosby et al, October 16, 2015 (<http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>) において説明されている。

【0010】

図3は、前述したブロックチェーン57の断片の概略図である。ブロックチェーン57の中間にある3つの隣接するブロック2が、N、N+1、およびN+2というラベル付きで示されており、3つのブロックのうちでブロックNが最も古く、ブロックN+2が最も若い。ブロックNは、連続するブロックチェーン・トランザクションT×S「c」~「f」を記録する、タイムスタンプ付きの台帳の一部4を含む。ブロックN+1は、トランザクションの次のグループ「g」~「m」を記録し、ブロックN+2は、その後のトランザクション「n」~「w」を記録する。「ハッシュ」というラベル付きの斜め方向の矢印は、隣接するブロックを接続し、すなわち、その後のブロック(例えば、ブロックN+2)が、前のブロックN+1に対するハッシュを格納する。

【0011】

信頼は、台帳のパブリックな性質によって、およびブロックチェーンのブロックを変更できないことを保証するためにそのようなシステムに組み込まれるセキュリティ対策によって、自動化される。単一の信頼された機関が、信頼していない取引中の関係者間を仲介する必要性が、排除される。

【0012】

図4は、Storjによって提供されるブロックチェーン・クラウド・ストレージ・システム(blockchain cloud storage system)の概略図である。Storjシステムは、MetaDiskを使用する。Storjアーキテクチャでは、図2に示されている種類のピアツーピア・ネットワーク55が、ブロックチェーン57および関連するパブリックな台帳26を含む。ブロックチェーンの2人の例示的なメンバー14は、関連するコンピュータ・デバイス25を持っており、それらの各コンピュータ・デバイス25は、ネットワーク55のノードの一部である。1人のメンバー14がデータ・ファイル16をブロッ

10

20

30

40

50

クチェーン・クラウド・ストレージ・ネットワーク (blockchain cloud storage network) に格納したい場合、そのメンバーは、そのファイルを扱いやすい部分 (シャードと呼ばれる) にさらに分割し、秘密キー 22 を使用して暗号化し、その後、それらのファイルは、ネットワーク内で格納するために、同じブロックチェーンの仲間のメンバー間で分配される。スペースをクラウド・ストア (cloud store) に提供するブロックチェーンのメンバーは、ファーマーと呼ばれる。ブロックチェーンのメンバーは、クラウド・ストレージ・ユーザまたはファーマーあるいはその両方であることができる。Meta Disk は、顧客のデータを受信して、ネットワーク内のストレージ位置にルーティングする仲介者であり、3 ロケーション (3-locations) などの適切なデータ冗長性ルールを適用できる。

【 0 0 1 3 】

10

図 5 は、Storj システムによって使用されるシャーディング・プロセスを示す概略図である。前述したように、シャードは、ファイルの暗号化された部分として格納される。シャードは、シャードのサイズが、ハッカーにとって助けになることがある情報を含まないように、未使用のスペースが埋められて、固定サイズに維持される。70 MB のサイズを有するデータ・ファイル 16 を例にとると、このファイルが、32 MB として示されている固定サイズの、複数のより小さいファイル 30 に分割され、これらのファイルが最初のシャードになる。より小さい各ファイル 30 は、メンバーの秘密キー 22 を使用して暗号化され、その後、そのハッシュと共に、格納するためにブロックチェーン・ネットワーク 55、57 に送信される。

【 0 0 1 4 】

20

Storj システムは、記事 "Storj A Peer-to-Peer Cloud Storage Network" by Shawn Wilkinson et al, December 15, 2014 v1.01 (<https://storj.io/storj.pdf>) において説明されている。

【 0 0 1 5 】

上で参照されたファイルは、コンテナ・ファイル (以下では、コンテナと呼ぶ) であってよい。クラウドベースのインフラストラクチャに移行するシステムが増えるにつれて、コンテナ上で実行されるデータおよびサービスがますます重要になった。ソフトウェア・コンテナまたはコンテナは、互いに分離され、ハードウェアとオペレーティング・システムの間の中間層として、ハードウェア・ノード上で同時に実行される仮想マシン・インスタンスである。そのような仮想マシン・インスタンスを作成して実行するソフトウェア、ファームウェア、またはハードウェアは、ハイパーバイザまたは仮想マシン・モニタ (VMM: virtual machine monitor) と呼ばれる。本文書では、ハイパーバイザという用語を主に使用する。

30

【 0 0 1 6 】

このアプローチは、コンテナベースの仮想化、サーバ仮想化、またはオペレーティング・システム仮想化と呼ばれる。各コンテナは、実際に利用できるハードウェアとは無関係であり、オペレーティング・システムを構成するための基盤として機能するハードウェア・リソースの定義されたセットを含んでいる仮想環境を表す。コンテナの例は、ドッカー・コンテナである。ドッカー・コンテナは、Linux (R) アプリケーション上で実行され、常に同じ方法で実行されるようにオペレーティング・システム、システム・ツール、システム・ライブラリなどの実行に必要なものをすべて含んでいる自己完結型の 1 つのソフトウェアを包含する。Linux は、米国またはその他の国あるいはその両方における、Linus Torvalds の登録商標である。

40

【 0 0 1 7 】

クラウドと、国内のデータ保護法の法令順守との間に特有の緊張関係が存在することがよく知られている。クラウド・ストレージまたはクラウドベースのアプリケーションの分散性は、本質的に、地理的制約を受けずに、ネットワークを経由してデータを柔軟に分散することを含む。一方、データ保護に関する国内法令は、地域的に定義された定義による。欧州では、「Article 29 Working Party」が、特に、クラウド・ストレージが EU データ保護指令 (95 / 46 / EC) および EU e-プライバシー指令 (2002 / 58 / E

50

C) にどのように収まることができるかを検討する任務を負い、2012年にその見解を公表した。ドイツには、考慮する必要のある個人データを保護しないことに対する厳しい刑事制裁 (German Criminal Code StGBのセクション203) も存在する。クラウド・プロバイダおよびクラウド・ユーザ (企業および政府機関など) による法令順守および法的リスク管理は、クラウドベースのインフラストラクチャ上で実行される特定のデータおよびサービスが特定の国内または地域内にあること、または特定の関係者のみが特定のデータおよびサービスにアクセスできること、あるいはその両方を保証することを伴うことがある。

【0018】

ITインフラストラクチャの一部にコンテナベースのシステムを包含しており、1つだけでなく複数のクラウド・サービス・プロバイダを使用している企業を例にとる。そのような企業では、コンテナまたはその他のファイル・タイプが、複数のクラウド・プロバイダに散在しており、各コンテナが複数のサーバに分散されている。法的データ保護の問題を管理することが、極めて急速に非常に複雑になる可能性がある、ということが理解され得る。

【0019】

図6は、コンテナの3つのグループが各クラウド・ストレージ・プロバイダに関連付けられているシステム例を示している。1つの企業が、これらのコンテナ・グループを所有しており、地理的境界などのシステム境界28内でそれらを運用する必要があると仮定する。コンテナの3つのグループ40__1、40__2、および40__3は、各仮想サーバ12__1、12__2、および12__3を所有している3つの異なるクラウド・ストレージ・プロバイダを使用してそれぞれ格納され、各仮想サーバは、顧客のデータを、何らかの複雑な方法で複数の物理サーバ (図示されていない) にまたがって格納する。コンテナの所有者は、クラウド・ストレージ・プロバイダが、これらのコンテナを構成するデータを格納する方法および場所を、どうすれば制御できるであろうか。

【先行技術文献】

【非特許文献】

【0020】

【非特許文献1】 "The NIST Definition of Cloud Computing" (September 2011) by Peter Mell and Timothy Grance, NIST Special Publication 800-145

【非特許文献2】 "Blockchain Technology Beyond Bitcoin" by Michael Crosby et al, October 16, 2015

【非特許文献3】 "Storj A Peer-to-Peer Cloud Storage Network" by Shawn Wilkinson et al, December 15, 2014 v1.01

【発明の概要】

【発明が解決しようとする課題】

【0021】

本発明の目的は、地理的制約および権利管理などの法令順守問題に対処するように設計されたブロックチェーンの1つまたは複数のシステム・インスタンスをホストするのに適した構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワークを提供することである。

【課題を解決するための手段】

【0022】

好ましい実施形態に従って、地理的制約および権利管理などの法令順守問題に対処するように設計されたクラウドベースのサービスのブロックチェーンの実装が提供されている。

【0023】

本発明の態様によれば、ブロックチェーン内のトランザクションを記録するパブリックな台帳を含んでいるブロックチェーンの1つまたは複数のシステム・インスタンスをホストするのに適した構成可能なコンピューティング・リソースの共有プールをホストする分

10

20

30

40

50

分散ネットワークが提供されており、この分散ネットワークが少なくとも1つのそのようなシステム・インスタンスを備えており、各システム・インスタンスが、仮想マシンおよびコンテナのセットを備えており、これらのコンテナが仮想マシン上で実行されるよう機能し、それぞれ、コンテナ上でブロックチェーンを実行するよう機能するブロックチェーン・サブシステムを備えており、セットの各コンテナがパブリックな台帳を参照して分散ネットワーク内の別のコンテナもこのセットに属しているかどうかを判定できるように、パブリックな台帳が、セットの各コンテナの少なくとも選択された一部の暗号化されたコピーを記録することで、セットのコンテナがブロックチェーンのメンバーになるように、このブロックチェーンが定義されており、それによって、このセット内にはない他のコンテナとの望ましくない情報のやりとりを防ぐためのバリアとして機能する、コンテナのセットのシステム境界を作成する。

10

【0024】

このブロックチェーン・システムは、新しいコンテナをブロックチェーン内に作成するための柔軟性を提供できる。つまり、特定の実施形態では、各システム・インスタンス内で1つのコンテナが、システム・インスタンス・コントローラの役割を持つように指定される。システム・インスタンス・コントローラは、セットの新しいコンテナを作成するための独占権を持っており、システム・インスタンス・コントローラは、そのような新しいコンテナを作成するよう機能する。このようにして、新しいコンテナの作成は、ブロックチェーン・トランザクションとして処理される。システム・インスタンス・コントローラの役割は、複数のコンテナのうちの異なるコンテナ間で、時間と共に交代されるのが好ましい。柔軟性を提供できるその他の領域は、コンテナ上でソフトウェアの更新を処理することである。つまり、特定の実施形態では、コンテナがソフトウェアの更新を受信するときに常に、更新されたコンテナの暗号化されたコピーが、パブリックな台帳に記録される。このようにして、ソフトウェアの更新は、ブロックチェーン・トランザクションとして処理される。このようにして、パブリックな台帳は、各コンテナの最新バージョンのコピーを維持するとともに、以前のすべてのバージョンのコピーを維持し、それによって、完全に監査可能な履歴を提供する。

20

【0025】

使用中に、システム境界では、次のように規制されるのが好ましい。セットのあるコンテナが、別のコンテナと情報をやりとりする必要がある場合（例えば、コンテナ上で実行されているコードが、別のコンテナに対する関数呼び出しを含んでいる場合）、このコンテナは、関数呼び出しを実行する前に、他のコンテナが同じセットの一部であるかどうかをチェックする。セットのコンテナは、他のコンテナとの通信を開始して、識別情報を取得する。次にこのコンテナは、パブリックな台帳で、他のコンテナの暗号化されたコピーを含んでいるトランザクションを検索することによって、他のコンテナがセット内にあるかどうかをチェックする。そのようなトランザクションが検出されない場合、コンテナは、他のコンテナがセット内にはないということを知り、そのため、他のコンテナと情報をやりとりするべきではない（例えば、関数呼び出しを実行しない）ということを知る。セットのコンテナが、他のコンテナがセット内にはないということを決定した場合、セットのコンテナは、そのことをパブリックな台帳に記録してもよく、そのため、セット内の他のすべてのコンテナは、パブリックな台帳全体で他のコンテナのコピーを検索するプロセスを繰り返さずに、この記録の他のコンテナをファイアウォールで遮断するべきであるということを知る。

30

40

【0026】

このシステムは、任意の数のシステム・インスタンス、およびシステム・インスタンスのいずれにも属せず、ブロックチェーンの一部ではない他のコンテナが、分散ネットワーク上で共存することを許可することが好ましい。このシステムでは、あるシステム・インスタンスに属しているコンテナが、別のシステム・インスタンスに属しているということが起きないようにする、ということが理解されるであろう。

【0027】

50

分散ネットワークを形成する構成可能なコンピューティング・リソースの共有プールにおいて、コンテナが存在できる場所に対する物理的制限が存在するように、地理的制約を課すために、システム境界が定義され得る。例えば、すべてのコンテナが、欧州連合、ドイツ、デラウェア州、米国、英領ヴァージン諸島などの、特定の管轄区域または管轄区域のグループに制限されてよい。システム境界は、ユーザのタイプなどの、何らかの他の制約と共に定義されてもよい。

【 0 0 2 8 】

本発明の別の態様によれば、仮想マシン上で実行されるよう機能するソフトウェア・コンテナが提供されており、このコンテナは、メモリ・リソースと、処理リソースと、処理リソースを使用してコンテナ上でブロックチェーンを実行するよう機能するブロックチェーン・サブシステムであって、ブロックチェーンがパブリックな台帳を含んでいる、ブロックチェーン・サブシステムと、メモリ・リソースに格納されたパブリックな台帳のコピーであって、パブリックな台帳が前述のコンテナの少なくとも選択された一部および少なくとも1つの他の各コンテナの暗号化されたコピーを記録するように、ブロックチェーンが定義される、パブリックな台帳のコピーとを備えており、これらのコンテナが、ブロックチェーンのメンバーであるコンテナのセットを集合的に構成する。コンテナは、ブロックチェーンの新しいコンテナを作成するための独占権を持っていてよい。

10

【 0 0 2 9 】

本発明のさらに別の態様によれば、本明細書に記載されたソフトウェア・コンテナを格納するコンピュータ・プログラム製品が提供されている。

20

【 0 0 3 0 】

本発明の別の態様によれば、ブロックチェーンのシステム・インスタンスが存在している構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワーク内で実行される新しいコンテナを作成する方法が提供されており、このブロックチェーンのメンバーがコンテナであり、このブロックチェーンが、ブロックチェーン内のトランザクションを記録するパブリックな台帳を含んでおり、パブリックな台帳がセットの各コンテナの少なくとも選択された一部の暗号化されたコピーを記録するように、ブロックチェーンが定義されており、この方法が、

システム・インスタンス・コントローラの役割を持つように、コンテナのうちの1つを指定することであって、システム・インスタンス・コントローラが、セットの新しいコンテナを作成するための独占権を持っている、指定することと、

30

システム・インスタンス・コントローラによって新しいコンテナを作成することと、新しいコンテナの作成がブロックチェーン・トランザクションとして処理されるように、新しいコンテナの少なくとも選択された一部のコピーを暗号化することと、

暗号化されたコピーをパブリックな台帳に記録することとのうちの1つまたは複数を含んでいる。

【 0 0 3 1 】

本発明のさらに別の態様によれば、ブロックチェーンのシステム・インスタンスが存在している構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワーク内に存在するコンテナ上でソフトウェアの更新を実行する方法が提供されており、ブロックチェーンのメンバーが、ソフトウェアの更新が実行されるコンテナを含んでいる複数のコンテナであり、ブロックチェーンが、ブロックチェーン内のトランザクションを記録するパブリックな台帳を含んでおり、この方法が、

40

コンテナ上でソフトウェアの更新を実行することと、

ソフトウェアの更新がブロックチェーン・トランザクションとして処理されるように、更新されたコンテナの少なくとも選択された一部のコピーを暗号化することと、

暗号化されたコピーをパブリックな台帳に記録することとのうちの1つまたは複数を含んでいる。

【 0 0 3 2 】

本発明のさらに別の態様によれば、ブロックチェーンのシステム・インスタンスが存在

50

している構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワーク内で実行されるコンテナの同じセットに第2のコンテナが属しているかどうかを第1のコンテナがチェックするための方法が提供されており、このブロックチェーンのメンバーが、少なくとも第1のコンテナを含んでいる前述のセットのコンテナであり、このブロックチェーンが、ブロックチェーン内のトランザクションを記録するパブリックな台帳を含んでおり、パブリックな台帳がセットの各コンテナの少なくとも選択された一部の暗号化されたコピーを記録するように、ブロックチェーンが定義されており、この方法が、

第1のコンテナが、ソフトウェア・コマンドのシーケンスを実行する過程において、第2のコンテナにアクセスするためのコマンドに達することと、

第1のコンテナが、第2のコンテナへのネットワーク接続を確立し、第2のコンテナの識別番号に関する情報を取得することと、

第1のコンテナが、パブリックな台帳を参照して、第2のコンテナがブロックチェーンのトランザクションに記録されているかどうかを判定することと、

そのようなトランザクションが存在しない場合に、第2のコンテナがブロックチェーンのメンバーでないということを推測し、第2のコンテナにアクセスするためのコマンドを実行することを抑制し、一方、

そのようなトランザクションが存在する場合に、第2のコンテナがブロックチェーンのメンバーであることを推測し、第2のコンテナにアクセスするためのコマンドを実行することとのうちの1つまたは複数を含んでいる。

【0033】

一部の実施形態では、第2のコンテナがブロックチェーンのメンバーでない場合、この方法は、第2のコンテナがブロックチェーンのメンバーでないという決定がブロックチェーン・トランザクションとして処理されるように、そのこともパブリックな台帳に記録する。

【0034】

本発明の態様によれば、ブロックチェーン内のトランザクションを記録するパブリックな台帳を含んでいるブロックチェーンの1つまたは複数のシステム・インスタンスをホストするのに適した構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワーク内で動作できる方法が提供されており、この分散ネットワークが、1つまたは複数のシステム・インスタンスを備えており、各システム・インスタンスが仮想マシンおよびコンテナのセットを備えており、それらのコンテナが、仮想マシン上で実行されるよう機能し、各コンテナが、コンテナ上でブロックチェーンを実行するよう機能するブロックチェーン・サブシステムを備えており、セットのコンテナがブロックチェーンのメンバーになって、パブリックな台帳がセットの各コンテナの少なくとも選択された一部の暗号化されたコピーを記録するように、ブロックチェーンが定義されており、この方法が、セットの各コンテナが、別のコンテナと情報をやりとりする前に、パブリックな台帳を参照して、分散ネットワーク内の他のコンテナもこのセットに属しているかどうかを判定し、それによって、このセット内にはない他のコンテナとの望ましくない情報のやりとりを防ぐためのバリアとして機能する、コンテナのセットのシステム境界を作成することを含んでいる。

【0035】

それによって、このシステムは、さまざまな実施形態に従って、複数のホスティング・プロバイダにまたがる、1つのシステム・インスタンスとしてのコンテナベースのシステムの集合の定義を可能にし、ブロックチェーンを使用して同じシステム・インスタンスのすべてのコンテナを一緒に結合して、完全に制御可能かつ検証可能なシステム境界を定義することによって、コンテナが安全かつ監査可能になる。

【0036】

以下では、図に示された実施形態例を単に例として参照し、本発明がさらに説明される。

【図面の簡単な説明】

【 0 0 3 7 】

【図 1】標準的なクラウド・ストレージ・アーキテクチャの概略図である。

【図 2】例示的なピアツーピア・ネットワークを、クラウド・コンピューティング環境の一部として示す図である。

【図 3】ブロックチェーンの断片の概略図である。

【図 4】既知のブロックチェーン・クラウド・ストレージ・システムの概略図である。

【図 5】図 4 のブロックチェーン・クラウド・ストレージ・システムによって使用されるシャーディング・プロセスを示す概略図である。

【図 6】コンテナの 3 つのグループが各クラウド・ストレージ・プロバイダに関連付けられ、システム境界内に制限される必要があるシステム例を示す図である。

10

【図 7】本開示の実施形態をホストするのに適した例示的なクラウド・コンピューティング環境を示す図である。

【図 8】図 7 のクラウド・コンピューティング環境によって提供される機能的抽象レイヤのセットを示す図である。

【図 9】本発明の実施形態に記載されたクラウド環境のシステム図である。

【図 10】本発明の実施形態に記載された、図 9 のシステムのコンテナである。

【図 11】本発明の一実施形態に記載された、新しいコンテナを追加するためのプロセスを示す図である。

【図 12】本発明の一実施形態に記載された、既存のコンテナ上でソフトウェアの更新を実行するためのプロセスを示す図である。

20

【図 13】本発明の一実施形態に記載された、コンテナが、別のコンテナがシステム境界内にあるかどうかをチェックするプロセスを示す図である。

【図 14】一般的コンピュータ・デバイスを示す図である。

【発明を実施するための形態】

【 0 0 3 8 】

以下の詳細な説明では、本開示をよく理解するために、説明の目的で特定の詳細が示されるが、それらに限定されない。これらの特定の詳細から逸脱する他の実施形態において本開示が実施されてよいということが、当業者にとって明らかであろう。

【 0 0 3 9 】

図 7 は、例示的なクラウド・コンピューティング環境 50 を示している。図示されているように、クラウド・コンピューティング環境 50 は、クラウドの利用者によって使用されるローカル・コンピューティング・デバイス（例えば、携帯情報端末（PDA：personal digital assistant）または携帯電話 54A、デスクトップ・コンピュータ 54B、ラップトップ・コンピュータ 54C、または自動車コンピュータ・システム 54N、あるいはその組み合わせなど）が通信できる 1 つまたは複数のクラウド・コンピューティング・ノード 10 を含んでいる。ノード 10 は、互いに通信することができる。ノード 10 は、本明細書において前述されたプライベート・クラウド、コミュニティ・クラウド、パブリック・クラウド、またはハイブリッド・クラウドなどの、1 つまたは複数のネットワーク内で物理的または仮想的にグループ化されてよい（図示されていない）。これによって、クラウド・コンピューティング環境 50 は、クラウドの利用者がローカル・コンピューティング・デバイス上でリソースを維持する必要のないインフラストラクチャ、プラットフォーム、または SaaS（Software as a Service）、あるいはその組み合わせを提供できる。図 1 に示されたコンピューティング・デバイス 54A～N の種類は、例示のみが意図されており、コンピューティング・ノード 10 およびクラウド・コンピューティング環境 50 は、任意の種類ネットワークまたはネットワーク・アドレス可能な接続（例えば、Web ブラウザを使用した接続）あるいはその両方を經由して任意の種類コンピュータ制御デバイスと通信できるということが理解される。

30

40

【 0 0 4 0 】

図 8 は、図 7 のクラウド・コンピューティング環境 50 によって提供される機能的抽象レイヤのセットを示している。図 8 に示されたコンポーネント、レイヤ、および機能は、

50

例示のみが意図されており、本開示の実施形態がこれらに限定されないということが、あらかじめ理解されるべきである。図示されているように、次のレイヤおよび対応する機能が提供される。

【 0 0 4 1 】

ハードウェアおよびソフトウェア・レイヤ 6 0 は、ハードウェア・コンポーネントおよびソフトウェア・コンポーネントを含む。ハードウェア・コンポーネントの例としては、メインフレーム 6 1、RISC (Reduced Instruction Set Computer) アーキテクチャベースのサーバ 6 2、サーバ 6 3、ブレード・サーバ 6 4、ストレージ・デバイス 6 5、ならびにネットワークおよびネットワーク・コンポーネント 6 6 が挙げられる。一部の実施形態では、ソフトウェア・コンポーネントは、ネットワーク・アプリケーション・サーバ・ソフトウェア 6 7 およびデータベース・ソフトウェア 6 8 を含む。

10

【 0 0 4 2 】

仮想化レイヤ 7 0 は、仮想サーバ 7 1、仮想ストレージ 7 2、仮想プライベート・ネットワークを含む仮想ネットワーク 7 3、仮想アプリケーションおよびオペレーティング・システム 7 4、ならびに仮想クライアント 7 5 などの仮想的実体を提供できる抽象レイヤを備える。

【 0 0 4 3 】

一例を挙げると、管理レイヤ 8 0 は、以下で説明される機能を提供することができる。リソース・プロビジョニング 8 1 は、クラウド・コンピューティング環境内でタスクを実行するために利用されるコンピューティング・リソースおよびその他のリソースの動的調達を行う。計測および価格設定 8 2 は、クラウド・コンピューティング環境内でリソースが利用される際のコスト追跡、およびそれらのリソースの利用に対する請求書の作成と送付を行う。一例を挙げると、それらのリソースは、アプリケーション・ソフトウェア・ライセンスを含んでよい。セキュリティは、クラウドの利用者およびタスクの ID 検証を行うとともに、データおよびその他のリソースの保護を行う。ユーザ・ポータル 8 3 は、クラウド・コンピューティング環境へのアクセスを利用者およびシステム管理者に提供する。サービス・レベル管理 8 4 は、必要なサービス・レベルを満たすように、クラウドのコンピューティング・リソースの割り当てと管理を行う。サービス水準合意 (SLA: Service Level Agreement) 計画および実行 8 5 は、今後の要求が予想されるクラウドのコンピューティング・リソースの事前準備および調達を、SLA に従って行う。

20

30

【 0 0 4 4 】

ワークロード・レイヤ 9 0 は、クラウド・コンピューティング環境で利用できる機能の例を示している。このレイヤから提供されてよいワークロードおよび機能の例としては、マッピングおよびナビゲーション 9 1、ソフトウェア開発およびライフサイクル管理 9 2、仮想クラスルーム教育の配信 9 3、データ分析処理 9 4、トランザクション処理 9 5、およびモバイル・デスクトップ 9 6 が挙げられる。

【 0 0 4 5 】

図 9 は、本開示の実施形態による、クラウド環境のシステム図である。クラウド環境は、背景のセクションおよび上の詳細な説明の一部においてすでに説明されているように、標準的なクラウド・コンピューティング環境の一部として、ピアツーピア・ネットワーク 5 5 内に存在する。ハイパーバイザ 4 2 によって実行されるコンテナのセット 4 0 の所有者は、ハイパーバイザおよびコンテナのセットに基づいてシステム・インスタンス 1 1 0 を定義する。コンテナ 4 0 は、ハイパーバイザ 4 2 上で実行される仮想マシンとして存在する。ハイパーバイザ 4 2 は、カーネル (図示されていない) への共有アクセスを複数のコンテナに提供し、各カーネルは、そのカーネルに関連付けられたグループのコンテナが実行されることを許可するオペレーティング・システムを含む。システム・インスタンス 1 1 0 は、システム境界 2 8 _ 1 内に制限される要素であると考えられてよい。システム境界は、コンテナのいずれかを実行するための特定のシステム・インスタンスを提供するように、コンテナの任意のセットの周囲に定義され得る。システム境界は、そのシステム・インスタンス内のどのコンテナも従わなければならないルールによって概念的

40

50

に定義されるか、または地理的境界などの物理的なものであってよく、物理的境界である場合でも、ルールセットによって定義される。別のシステム境界 2 8 _ 2 によって示されているように、同じ所有者または別の所有者が、さらにシステム・インスタンス 1 2 0 を、それ自身のハイパーバイザ 4 2 およびコンテナ 4 0 と共に作成してよい。

【 0 0 4 6 】

ブロックチェーン技術は、パブリックな台帳を、互いに共存して情報をやりとりすることを許可されているコンテナのセットの一部である（システム境界内にあると呼ばれる）コンテナの記録にすることによって、使用される。システム境界または領域は、ブロックチェーン内のシステム・インスタンスとして作成される。各コンテナは、ブロックチェーンのメンバーである。

10

【 0 0 4 7 】

図 1 0 は、コンテナ 4 0 を示している。各コンテナ 4 0 は、パブリックな台帳 4 4 のコピーおよびコンテナ上で実行されるブロックチェーン・ソフトウェアのコピーを保持する。このブロックチェーン・ソフトウェアのコピーを、ブロックチェーン・サブシステム 4 6 と呼ぶ。コンテナのブロックチェーン・サブシステム 4 6 は、そのコンテナのブロックチェーンのパブリックな台帳のローカル・コピーを管理するため、およびその他のブロックチェーン固有のネットワーク・タスクを実行するために、コンテナ上でローカル・サービスのセットを提供する役割を担う。各コンテナはブロックチェーン・サブシステム 4 6 を実行し、同じブロックチェーンのメンバーであるすべてのコンテナが互いに情報をやりとりできるように、ブロックチェーンのパブリックな台帳 4 4 のコピーを維持する。ブロックチェーン・サブシステム 4 6 は、ネットワーク上の他のコンテナを識別する能力を有しており、パブリックな台帳 4 4 の維持に関連するメッセージをブロードキャストおよび受信することができる。各ブロックチェーン・サブシステム 4 6 は、そのコンテナ 4 0 上で実行されるサービスとして存在し、コンテナ間の通信が、ブロックチェーンの更新を行うために使用される。ブロックチェーンはネットワークを形成し、このネットワークは、コンテナがピアツーピアで互いに通信することの結果として生じる「発生した」ネットワークである。システム境界または領域は、ブロックチェーンの分散台帳 4 4 を使用して定義される機能的なシステム境界または領域であり、システム・インスタンス 1 1 0（または 1 2 0）内の特定のコンテナのセットのすべてのコンテナ 4 0 が、この台帳 4 4 を利用できる。コンテナのセットは、データ保護法を順守するために特定の管轄区域内（すなわち、特定の地理的境界内）で使用されるコンテナであるか、あるいは特定のユーザまたはユーザのタイプのみによってアクセスされるべきであるデータまたはサービスを提供するコンテナであってよい。

20

30

【 0 0 4 8 】

想定されるブロックチェーンでは、トランザクションはコンテナのデータである。ブロックチェーン内のブロックは、コンテナがシステム・インスタンスに追加されるときに、最初にコンテナの状態を格納するが、各更新の後にもコンテナの状態を格納する。つまり、ソフトウェアの更新がコンテナ上で実行されるたびに、更新されたコンテナの状態を表すトランザクションをパブリックな台帳に追加することによって、ブロックチェーンが更新される。コンテナの現在の状態は、`/etc`、`/bin`、または`/sbin`などの、コンテナ内の特定のターゲットにされるディレクトリをハッシュすることによって、記録され得る。`md5deep` (<http://md5deep.sourceforge.net/>) などのツールを使用して、これらのディレクトリのハッシュのセットを作成できる。

40

【 0 0 4 9 】

トランザクションがブロックチェーン内で記録されているコンテナのみが、システム境界内にあると見なされ、トランザクションがブロックチェーン内で記録されているコンテナのみが、ブロックをブロックチェーンに追加することを許可されるということは、コンテナがブロックチェーンのメンバーであるという概念と一致している。すべてのコンテナがこのことをチェックできるが、それはすべてのコンテナがパブリックな台帳にアクセスできるためである。ブロックチェーン内にあることがすでに確認されたコンテナのみが、

50

ブロックをブロックチェーンに追加できる。

【0050】

その他のコンテナに関連する情報（例えば、コンテナのタイプ（データベース/ Webサーバなど））もブロックチェーンに格納できるということに留意する。

【0051】

各システム・インスタンス内の少なくとも1つのコンテナが、システム・インスタンス・コントローラ（SIC：system instance controller）として指名される。SICは、システム・インスタンス内で新しいコンテナを作成する権利を持っている唯一のコンテナ・タイプである。新しいコンテナが作成された後に、新しいコンテナの内容をハッシュすることによって、そのコンテナの初期状態が、SICによってトランザクションとしてブロックチェーンに追加されることに加えて、SICがそのコンテナの作成者だったことの記録を提供するために、作成元のSICのハッシュもブロックチェーンに追加される。

10

【0052】

SICは、他の指名されたノードによって、周期的に監査され得る。サービスを分散するために、SICの権利は、システム・インスタンス内の複数のコンテナ間で交代され得る。SICに対する更新または変更も、ブロックチェーン内でトランザクションとして記録され得る。したがって、パブリックな台帳に記録されるときに、作成元のSICがコンテナの最初のトランザクション内で参照されるため、いずれかのコンテナの作成日のスタンプおよび発生元をたどって、そのコンテナを作成したSICに遡ることができる。

【0053】

20

例えば、図9を参照すると、SIC SIC 1 aが、システム・インスタンス110に対して現在指名されているコントローラである場合、SIC SIC 1 aは、破線で示されている新しい「標準」コンテナC 1 cを作成している最中であることがある。あるとき、SIC 1 aは、その制御中の状態を交代し、SIC 1 bというラベルの付いたコンテナに渡すことを決定してよい。やはり図9を参照すると、第2のシステム・インスタンス120も、「標準」コンテナC 2 aおよびSIC（SIC 2）を含んでいるコンテナ40ならびにそれ自身のハイパーバイザ42を含む。これら2つのシステム・インスタンスが、それらを分離して情報のやりとりがない状態に保つ各ブロックチェーンを含んでいるため、コンテナ40は、これら2つのシステム・インスタンス間で共有されない。

【0054】

30

このアプローチは、複数の世代を伝搬することができるため、例えば、あるコンテナから、その作成元のSICコンテナに遡ることができ、この作成元のSICコンテナ自体が、別のSICコンテナによって作成されたコンテナである可能性が高い、などとなる。いずれの場合も、システム・インスタンスの最初の作成までに、いかに多くの世代が存在したとしても、パブリックな台帳を介して、それらの世代を通る系統を常にたどることができる。

【0055】

ネットワーク上のコンテナが、別のコンテナと共に何かの作業を実行したいときに、そのネットワーク上のコンテナは、他のコンテナがシステム境界内にあるかどうかに関して、それ自身のシステム・インスタンスのパブリックな台帳に問い合わせることができるため、システム境界は効果的である。他のコンテナのトランザクションがパブリックな台帳にない場合、コンテナは、この他のコンテナがシステム・インスタンスの一部ではない（すなわち、システム境界内にない）ということを知り、そのため、この他のコンテナとのすべての通信が中断され得る。ブロックチェーンは、システム内のすべてのコンテナベースの活動の、監査可能な不正開封防止機能付きの台帳としても利用できる。したがって、特定のシステム・インスタンスに属するコンテナは、このシステム・インスタンスのパブリックな台帳を参照して、いずれかの他のコンテナが同じシステム・インスタンスに属しているかどうかを検証できる。

40

【0056】

このシステムは、クラウドに100%基づいたまま、基礎になるハイパーバイザまたは

50

コンテナのホスト・システムあるいはその両方から分離した状態で、企業のコンテナベースのシステムの安全を保証するための方法を企業に提供する。どのハイパーバイザにもホスティング・プロバイダにも依存しない。企業は、企業のコンテナが、クラウド内にあるか、従来のホスティング・サーバとして存在するかに関わらず、データが格納されている場所またはサービスが提供される人に関連する特定の契約上の条件またはその他の法律上の条件を順守することを保証するために、特定のホスティング・プロバイダに拘束されない。むしろ企業は、企業が使用するホスティング・プロバイダと連携する必要がなく、ネットワークがクラウドタイプであるか、従来型であるかに関わらず、データがネットワーク内で格納される方法の機構を考慮せずに、完全に制御できるブロックチェーンを介して、企業のコンテナの法令順守を自律的に保証することができる。また、ブロックチェーンのストレージの分散性は、通常のブロックチェーンのセキュリティ上の利点を得られるということ、すなわち、脆弱性の単一点である単一の中央データベース・サーバに依存しないということの意味する。また、パブリックな台帳の性質は、ブロックチェーンの履歴全体にわたる完全なトレーサビリティが存在することを意味し、これは、法令順守が確実に行われていることをチェックするための監査可能性を考慮する、さらなる長所になる。ブロックチェーンのパブリックな台帳の不正開封防止の性質は、セキュリティをさらに向上させる。

10

【 0 0 5 7 】

コンテナの性質は、定義によれば、各コンテナが、実行するために必要なものをすべて含んでいる自己完結型の1つのソフトウェアであるということの意味している。コンテナをブロックチェーンの1つのブロックにカプセル化することによって、関連するブロックの内容を調べて、任意のコンテナの内容をいつでも簡単にチェックすることが可能になる。

20

【 0 0 5 8 】

このアプローチを使用すると、ネットワーク上のすべてのコンテナ間の通信が許可されるため、ネットワークはオープンであり続けることができる。ただし、前述したように、同じブロックチェーンのシステム・インスタンスの一部であるネットワーク上のコンテナの場合、それらのコンテナは、このシステム・インスタンスに属している他のすべてのコンテナを確実に認識することができ、友人であるか敵であるかの単なる識別を超えて、「異質な」コンテナとの情報のやりとりを制限するか、または防ぐことができる。

30

【 0 0 5 9 】

地理的制約が多くの政府活動の基本的要件であり、すなわち、政府およびその法律が、通常、管轄区域自体にのみ適用され、法律または公共政策が、データが管轄区域外で格納されるのを禁止することがあるため、コンテナのセットを特定の地理的制約に結び付ける能力は、応用の可能性にとって重要な意味を持っている。地理的制約は、銀行の業務を制約する法律を通じた銀行取引などの、厳しく規制されているサービスの要件でもある。例えば、コンテナが現実の（すなわち、デジタルではない）通貨を管理するために使用される場合、おそらく地理的制約が要件になる。

【 0 0 6 0 】

ブロックチェーンのデータの分散性は、コンテナベースのシステムの大部分で障害または停止あるいはその両方が発生した場合でも、同じシステム・インスタンス内のすべてのコンテナの履歴および識別番号の全体が、いずれか1つのコンテナから利用可能である、ということの意味する。これによって、事業の継続性に関連するリスクを低減する。

40

【 0 0 6 1 】

このようにして、ブロックチェーン技術は、独立したコンテナベースのソフトウェア・システムを定義するために使用され、このソフトウェア・システムは、ネットワーク上のコンテナの活動を監査する能力を有する、ネットワークの複数のノードにまたがって利用できるパブリックな台帳に基づいて、真に分散される。

【 0 0 6 2 】

図 1 1 は、新しいコンテナを追加するためのプロセスを示している。

50

【 0 0 6 3 】

ステップ1で、現在指名されているシステム・インスタンス・コントローラが、新しいコンテナを追加することの要求を受信し、この要求は、通常、ネットワークのリソースを監視し、ネットワークの負荷が、追加リソースを要求するアクションを正当化するほど十分に大きい場合に、追加リソース（この場合は、コンテナ）を要求する役割を持っているサーバである、負荷バランサー・サーバ（load balancer server）から送信される。ただし、原則的に、クラウド環境内の任意のネットワーク・ノードが要求元として機能することができる。

【 0 0 6 4 】

ステップ2で、システム・インスタンス・コントローラが、新しいコンテナを作成する。

10

【 0 0 6 5 】

ステップ3で、システム・インスタンス・コントローラが、初期状態にある新しいコンテナの内容の指紋（すなわち、ハッシュ）を受け取り、このシステム・インスタンス・コントローラが作成者であることを永続的に記録するために、それ自身のデータの何らかの側面もハッシュする。

【 0 0 6 6 】

ステップ4で、システム・インスタンス・コントローラが、ブロックチェーン・サブシステムに接触し、この新しいコンテナのトランザクションの新しいセットが追加される。

【 0 0 6 7 】

ステップ5で、新しいコンテナに関連付けられたブロックチェーンの新しいブロックが、ネットワークの他のノードにブロードキャストされ、したがって、一般にネットワーク・ノードのサブセットを表すブロックチェーンのすべてのメンバーによって受信される。

20

【 0 0 6 8 】

図12は、既存のコンテナ上でソフトウェアの更新を実行するためのプロセスを示している。

【 0 0 6 9 】

ステップ1で、コンテナのオペレーティング・システムが、システムの更新を受信し、更新を実行した後に、少なくとも、更新による影響を受けたディレクトに関して、その更新された内容をハッシュする。

30

【 0 0 7 0 】

ステップ2で、コンテナのオペレーティング・システムが、ブロックチェーン・サブシステムを介してブロックチェーンに接触し、更新を反映しているトランザクションの新しいセットがブロックチェーン（すなわち、パブリックな台帳）に追加される。

【 0 0 7 1 】

図13は、コンテナが、別のコンテナがシステム・インスタンス内（すなわち、システム境界内）にあるかどうかをチェックするために使用するプロセスを示している。

【 0 0 7 2 】

ステップ1で、第2のコンテナのオペレーティング・システムが、データを処理しており、第1のコンテナのオペレーティング・システムからのリソースにアクセスする必要がある。

40

【 0 0 7 3 】

ステップ2で、第2のコンテナが、第1のコンテナがシステム境界内にあるかどうかを検証する必要があるということを理解する。

【 0 0 7 4 】

ステップ3で、第2のコンテナが、第1のコンテナに属しているトランザクションについて、ブロックチェーン・サブシステムに問い合わせる。パブリックな台帳は、第1のコンテナに関連するトランザクションを含んでおらず、このことから、第2のコンテナは、第1のコンテナがシステム境界の外側にあるということを推測する。

【 0 0 7 5 】

50

ステップ4で、第2のコンテナのシステム・インスタンスに属している他のすべてのネットワーク・ノードが第1のコンテナをファイアウォールで遮断するように、第2のコンテナが、第1のコンテナがシステム境界内にないということをネットワークにブロードキャストする。

【0076】

図14は、前述したように、クライアントまたはサーバなどのネットワーク・ノードを実装するために使用されてよい、コンピュータ・システム501の構造およびコンピュータ・プログラム507を示している。コンピュータ・システム501は、グラフィック・オブジェクトの要求を管理できる、1つまたは複数のI/Oインターフェイス509を介して1つまたは複数のハードウェア・データ・ストレージ・デバイス(hardware data storage devices)511および1つまたは複数のI/Oデバイス513に結合されたプロセッサ・リソースを提供するための、プロセッサ503と、グラフィック・オブジェクトを表示できるディスプレイ515とを備えている。プロセッサ503は、1つまたは複数のメモリ・デバイス505に接続されてもよい。メモリ・リソースを提供するための少なくとも1つのメモリ・デバイス505は、コンピュータ実行可能命令を含んでいるコンピュータ・プログラムである、格納されたコンピュータ・プログラム507を含む。データ・ストレージ・デバイス511は、コンピュータ・プログラム507を格納してよい。ストレージ・デバイス511に格納されたコンピュータ・プログラム507は、メモリ・デバイス505を介してプロセッサ503によって実行されるように構成される。プロセッサ503は、格納されたコンピュータ・プログラム507を実行する。

10

20

【0077】

好ましい実施形態の論理プロセスのステップの全部または一部が、方法の論理プロセスのステップを実行するように配置された論理要素を備えている1つまたは複数の論理装置において代替的に具現化されてよいということ、およびそのような論理要素が、ハードウェア・コンポーネント、ファームウェア・コンポーネント、またはこれらの組み合わせを備えてよいということが、当業者にとって明らかであろう。

【0078】

同様に、好ましい実施形態の論理コンポーネントの全部または一部が、方法のステップを実行するように論理要素を備えている論理装置において代替的に具現化されてよいということ、およびそのような論理要素が、例えばプログラマブル・ロジック・アレイまたは特定用途向け集積回路内の論理ゲートなどのコンポーネントを備えてよいということが、当業者にとって明らかであろう。そのような論理配置は、例えば、固定された媒体または伝送可能な搬送媒体を使用して格納または送信されてよい仮想ハードウェア記述言語(virtual hardware descriptor language)を使用して、そのようなアレイまたは回路内で一時的または永続的に論理構造を確立するために要素を有効化することにおいて、さらに具現化されてよい。

30

【0079】

さらに別の代替的实施形態では、本開示は、コンピュータ・インフラストラクチャ内にデプロイされて実行されたときに、コンピュータ・システムに方法のすべてのステップを実行させるよう機能するコンピュータ・プログラムをデプロイするステップを含んでいる、サービスをデプロイするコンピュータ実装方法の形態で実現されてよい。

40

【0080】

好ましい実施形態の方法およびコンポーネントが、代替として、並列ソフトウェアを実行するために2つ以上のプロセッサを備えている並列コンピューティング・システムにおいて、完全に、または部分的に具現化されてよいということが、理解されるであろう。

【0081】

本開示のさらに別の実施形態は、システムおよび方法に関して定義されたコンピュータ・プログラム製品である。コンピュータ・プログラム製品は、プロセッサに本開示の態様を実行させるためのコンピュータ可読プログラム命令を含んでいるコンピュータ可読記憶媒体を含んでよい。

50

【 0 0 8 2 】

コンピュータ可読記憶媒体は、命令実行デバイスによって使用するための命令を保持および格納できる有形のデバイスにすることができる。

【 0 0 8 3 】

本開示は、システム、方法、またはコンピュータ・プログラム製品、あるいはその組み合わせであってよい。コンピュータ・プログラム製品は、プロセッサに本開示の態様を実行させるためのコンピュータ可読プログラム命令を含んでいるコンピュータ可読記憶媒体を含んでよい。

【 0 0 8 4 】

コンピュータ可読記憶媒体は、命令実行デバイスによって使用するための命令を保持および格納できる有形のデバイスにすることができる。コンピュータ可読記憶媒体は、例えば、電子ストレージ・デバイス、磁気ストレージ・デバイス、光ストレージ・デバイス、電磁ストレージ・デバイス、半導体ストレージ・デバイス、またはこれらの任意の適切な組み合わせであってよいが、これらに限定されない。コンピュータ可読記憶媒体のさらに具体的な例の非網羅的リストは、ポータブル・フロッピー（R）・ディスク、ハード・ディスク、ランダム・アクセス・メモリ（RAM：random access memory）、読み取り専用メモリ（ROM：read-only memory）、消去可能プログラマブル読み取り専用メモリ（EPROM：erasable programmable read-only memoryまたはフラッシュ・メモリ）、スタティック・ランダム・アクセス・メモリ（SRAM：static random access memory）、ポータブル・コンパクト・ディスク読み取り専用メモリ（CD-ROM：compact disc read-only memory）、デジタル多用途ディスク（DVD：digital versatile disk）、メモリ・スティック、フロッピー（R）・ディスク、パンチカードまたは命令が記録されている溝の中の隆起構造などの機械的にエンコードされるデバイス、およびこれらの任意の適切な組み合わせを含む。本明細書において使用されているコンピュータ可読記憶媒体は、それ自体が、電波またはその他の自由に伝搬する電磁波、導波管またはその他の送信媒体を伝搬する電磁波（例えば、光ファイバ・ケーブルを通過する光パルス）、あるいはワイヤを介して送信される電気信号などの一時的信号であると解釈されるべきではない。

【 0 0 8 5 】

本明細書に記載されたコンピュータ可読プログラム命令は、コンピュータ可読記憶媒体から各コンピューティング・デバイス/処理デバイスへ、またはネットワーク（例えば、インターネット、ローカル・エリア・ネットワーク、広域ネットワーク、または無線ネットワーク、あるいはその組み合わせ）を介して外部コンピュータまたは外部ストレージ・デバイスへダウンロードされ得る。このネットワークは、銅伝送ケーブル、光伝送ファイバ、無線送信、ルータ、ファイアウォール、スイッチ、ゲートウェイ・コンピュータ、またはエッジ・サーバ、あるいはその組み合わせを備えてよい。各コンピューティング・デバイス/処理デバイス内のネットワーク・アダプタ・カードまたはネットワーク・インターフェイスは、コンピュータ可読プログラム命令をネットワークから受信し、それらのコンピュータ可読プログラム命令を各コンピューティング・デバイス/処理デバイス内のコンピュータ可読記憶媒体に格納するために転送する。

【 0 0 8 6 】

本開示の処理を実行するためのコンピュータ可読プログラム命令は、アセンブラ命令、命令セット・アーキテクチャ（ISA：instruction-set-architecture）命令、マシン命令、マシン依存命令、マイクロコード、ファームウェア命令、状態設定データ、あるいは、Smalltalk、C++などのオブジェクト指向プログラミング言語、および「C」プログラミング言語または同様のプログラミング言語などの従来の手続き型プログラミング言語を含む1つまたは複数のプログラミング言語の任意の組み合わせで記述されたソース・コードまたはオブジェクト・コードであってよい。コンピュータ可読プログラム命令は、ユーザのコンピュータ上で全体的に実行すること、ユーザのコンピュータ上でスタンドアロン・ソフトウェア・パッケージとして部分的に実行すること、ユーザのコンピュータ上およびリモート・コンピュータ上でそれぞれ部分的に実行すること、あるいはリモ

10

20

30

40

50

ート・コンピュータ上またはサーバ上で全体的に実行されてよい。後者のシナリオでは、リモート・コンピュータは、任意の種類ネットワークを介してユーザのコンピュータに接続されてよく、または接続は、（例えば、インターネット・サービス・プロバイダを使用してインターネットを介して）外部コンピュータに対して行われてよい。一部の実施形態では、本開示の態様を実行するために、例えばプログラマブル論理回路、フィールドプログラマブル・ゲート・アレイ（FPGA：field-programmable gate arrays）、またはプログラマブル・ロジック・アレイ（PLA：programmable logic arrays）を含む電子回路は、コンピュータ可読プログラム命令の状態情報を利用することによって、電子回路をカスタマイズするためのコンピュータ可読プログラム命令を実行してよい。

【0087】

10

本開示の態様は、本明細書において、本開示の実施形態に従って、方法、装置（システム）、およびコンピュータ・プログラム製品のフローチャート図またはブロック図あるいはその両方を参照して説明される。フローチャート図またはブロック図あるいはその両方の各ブロック、ならびにフローチャート図またはブロック図あるいはその両方に含まれるブロックの組み合わせが、コンピュータ可読プログラム命令によって実装され得るということが理解されるであろう。

【0088】

これらのコンピュータ可読プログラム命令は、コンピュータまたはその他のプログラム可能なデータ処理装置のプロセッサを介して実行される命令が、フローチャートまたはブロック図あるいはその両方のブロックに指定される機能/動作を実施する手段を作り出すべく、汎用コンピュータ、専用コンピュータ、または他のプログラム可能なデータ処理装置のプロセッサに提供されてマシンを作り出すものであってよい。これらのコンピュータ可読プログラム命令は、命令が格納されたコンピュータ可読記憶媒体がフローチャートまたはブロック図あるいはその両方のブロックに指定される機能/動作の態様を実施する命令を含んでいる製品を備えるように、コンピュータ可読記憶媒体に格納され、コンピュータ、プログラム可能なデータ処理装置、または他のデバイス、あるいはその組み合わせに特定の方式で機能するように指示できるものであってもよい。

20

【0089】

コンピュータ可読プログラム命令は、コンピュータ上、その他のプログラム可能な装置上、またはその他のデバイス上で実行される命令が、フローチャートまたはブロック図あるいはその両方のブロックに指定される機能/動作を実施するように、コンピュータ、その他のプログラム可能なデータ処理装置、またはその他のデバイスに読み込まれてもよく、それによって、一連の動作可能なステップを、コンピュータ上、その他のプログラム可能な装置上、またはコンピュータ実装プロセスを生成するその他のデバイス上で実行させる。

30

【0090】

上の詳細な説明では、構成可能なコンピューティング・リソースの共有プールをホストする分散ネットワーク内で、ブロックチェーンの1つまたは複数のシステム・インスタンスがどのように提供され得るかについて説明した。各システム・インスタンスは、仮想マシンおよびコンテナのセットを備える。コンテナは、ブロックチェーンのパブリックな台帳が、各コンテナの少なくとも選択されたディレクトリの暗号化されたコピーを記録することで、ブロックチェーンのメンバーになる。したがって、パブリックな台帳に記録されたトランザクションが、セットのコンテナの暗号化されたコピーであるため、セット内の各コンテナは、パブリックな台帳を参照して、いずれかの他のコンテナも同じセットの一部であるかどうかを検証できる。このようにブロックチェーンを使用して、ブロックチェーンの初期仕様によって、コンテナのセットの周囲にシステム境界を定義できる。これは、コンテナのセットが地理的制約または権利管理などの法的必要条件を順守することを保証するようにシステム境界を定義できるため、役立つ。

40

【0091】

本開示の範囲を逸脱することなく、前述の実施形態例に対して多くの改良および変更が

50

行われ得るといことが、当業者にとって明らかであろう。

【符号の説明】

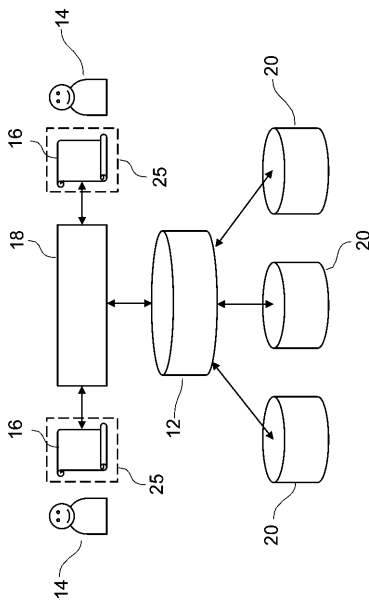
【0092】

- 10 クラウド・コンピューティング・ノード
- 28_1, 28_2 システム境界
- 40 コンテナ
- 42 ハイパーバイザ
- 44 パブリックな台帳のコピー
- 46 ブロックチェーン・サブシステム
- 50 クラウド・コンピューティング環境
- 54 A ~ N クラウド・コンピューティング・デバイス
- 55 ピアツーピア・ネットワーク
- 110, 120 システム・インスタンス
- 501 コンピュータ・システム
- 503 プロセッサ
- 505 メモリ・デバイス
- 507 コンピュータ・プログラム
- 509 I/Oインターフェイス
- 511 ハードウェア・データ・ストレージ・デバイス
- 513 I/Oデバイス
- 515 ディスプレイ

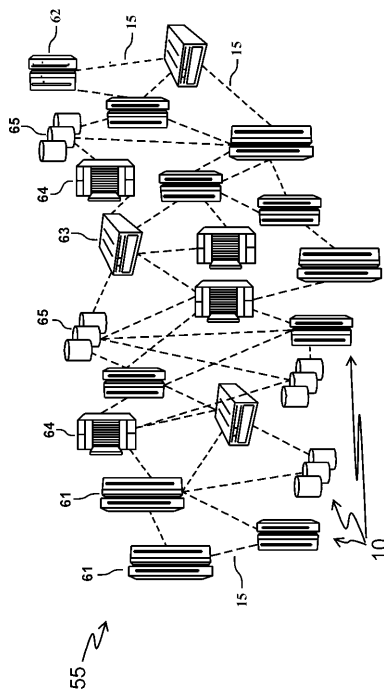
10

20

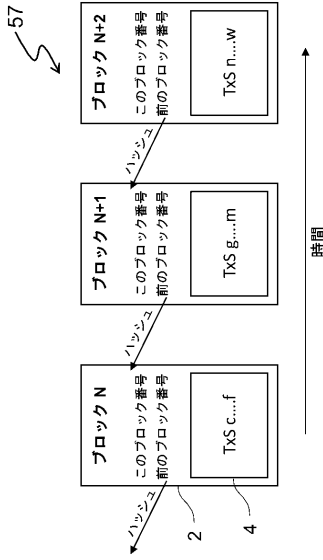
【図1】



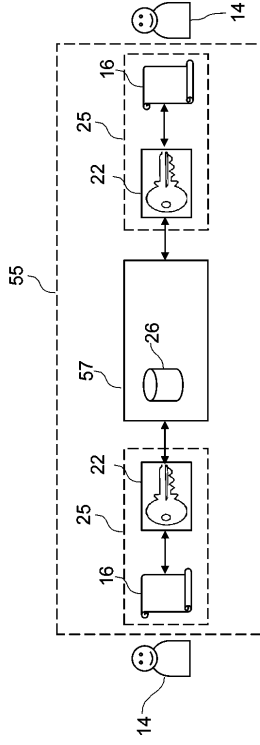
【図2】



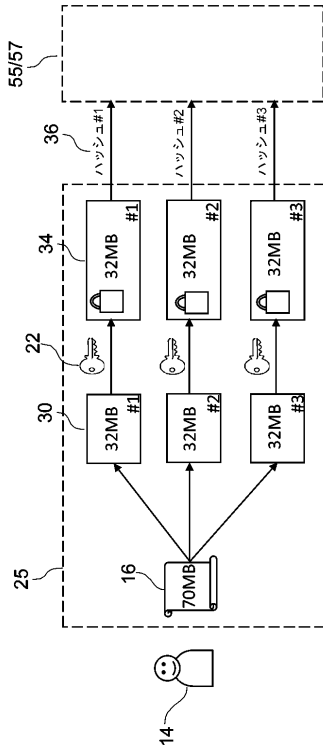
【図3】



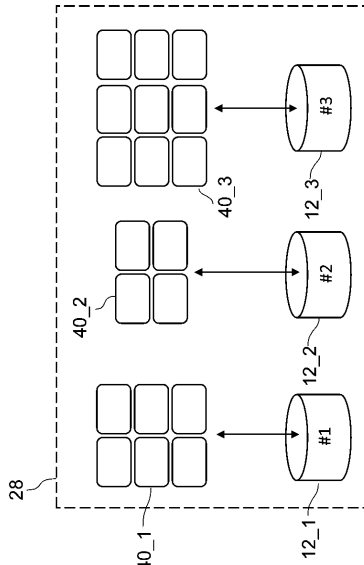
【図4】



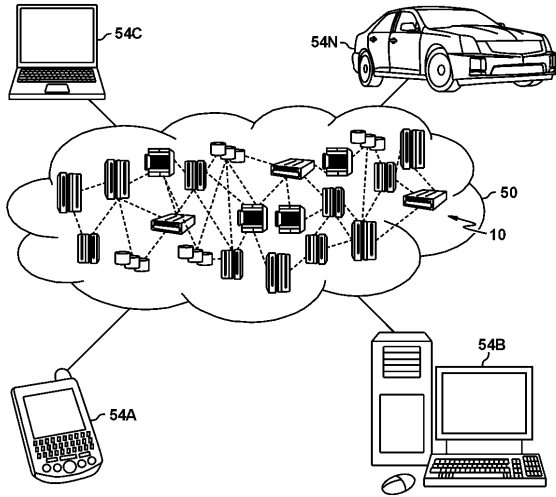
【図5】



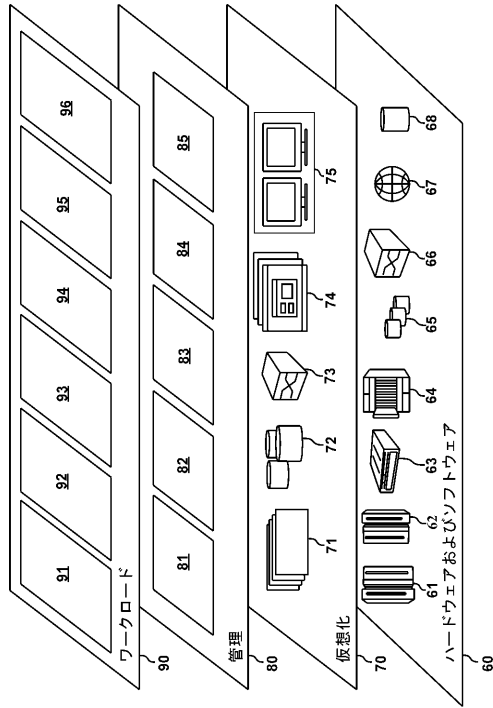
【図6】



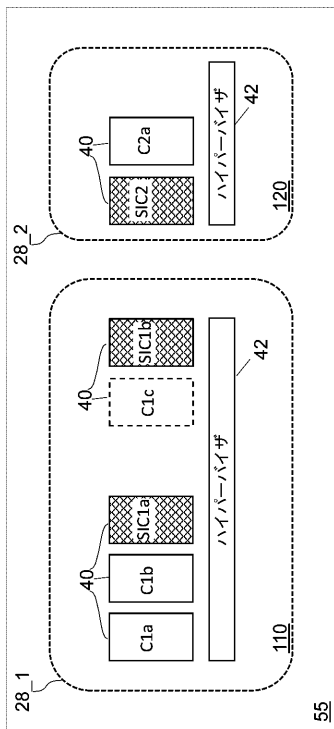
【図7】



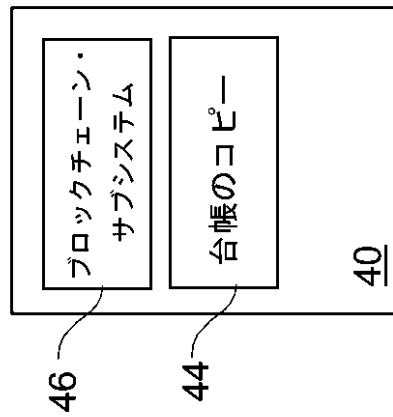
【図8】



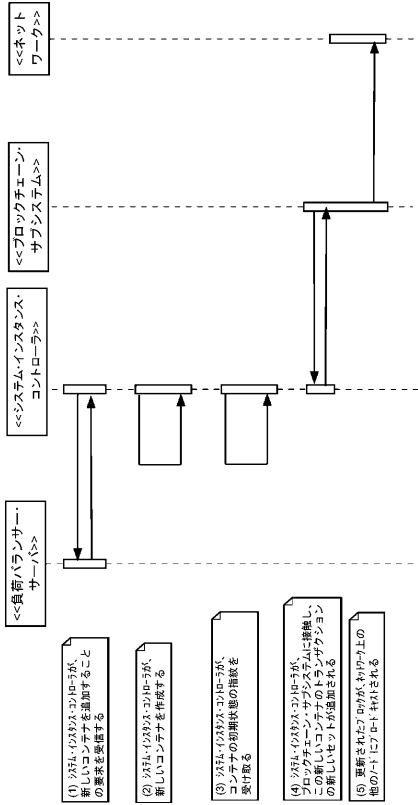
【図9】



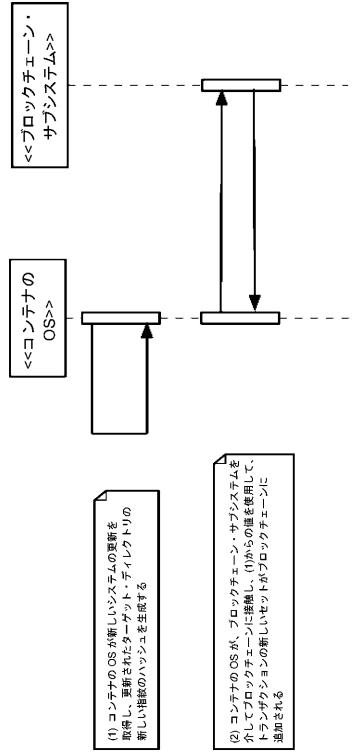
【図10】



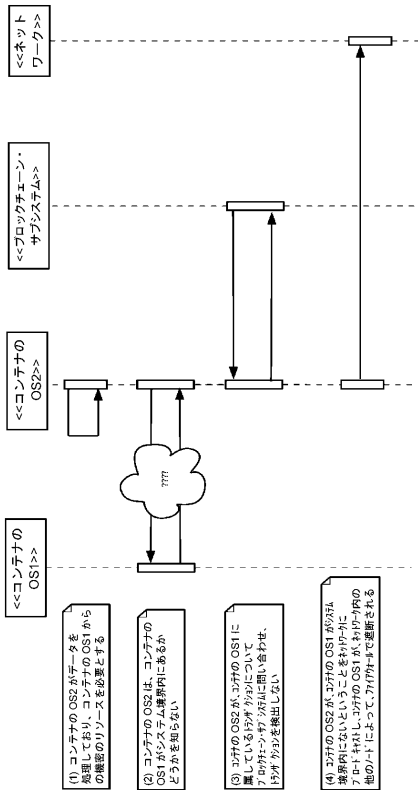
【図 1 1】



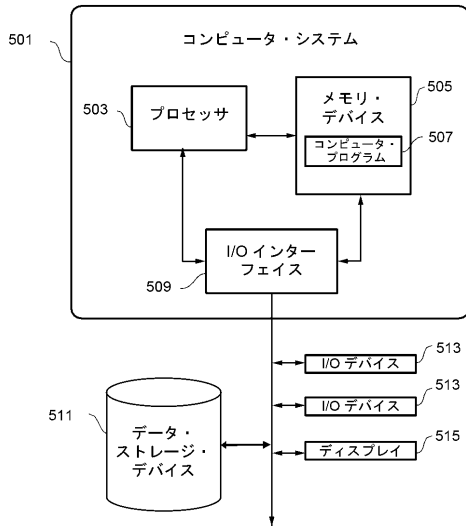
【図 1 2】



【図 1 3】



【図 1 4】



フロントページの続き

- (74)代理人 100112690
弁理士 太佐 種一
- (72)発明者 ブレディ、サイモン
アイルランド ダブリン モルハダート 15 ダマスタウン インダストリアル エステイト
テクノロジーキャンパス
- (72)発明者 ハリウッド、バリー
アイルランド ダブリン モルハダート 15 ダマスタウン インダストリアル エステイト
テクノロジーキャンパス
- (72)発明者 プライラート、ジョナス、エリック
アイルランド ダブリン モルハダート 15 ダマスタウン インダストリアル エステイト
テクノロジーキャンパス
- (72)発明者 ゴロトウ、クレア
アメリカ合衆国 8 0 3 0 1 - 6 1 0 8 コロラド州ボルダー ダイアゴナル・ハイウェイ 6 3 0 0
- (72)発明者 デラニー、ジョン
アイルランド 15 ダブリン モルハダート ダマスタウン インダストリアル エステイト テ
クノロジーキャンパス

審査官 小林 秀和

- (56)参考文献 特開 2 0 1 6 - 1 8 1 1 8 5 (J P , A)
米国特許出願公開第 2 0 1 6 / 0 2 5 9 9 3 7 (U S , A 1)
米国特許出願公開第 2 0 1 6 / 0 2 6 0 0 9 5 (U S , A 1)

- (58)調査した分野(Int.Cl. , DB名)
- | | |
|---------|-----------|
| G 0 6 F | 2 1 / 1 2 |
| G 0 6 F | 9 / 4 5 5 |
| G 0 6 F | 2 1 / 6 0 |
| G 0 6 F | 2 1 / 6 4 |