(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2020-503598
(P2020-503598A)
(43)公表日　令和2年1月30日(2020.1.30)

| (51)Int.Cl. | | F I | | テーマコード（参考） |
|---|---|---|---|---|
| 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 | |

審査請求 未請求　予備審査請求 未請求　（全 34 頁）

(21)出願番号　特願2019-527877 (P2019-527877)
(86)(22)出願日　平成29年12月7日 (2017.12.7)
(85)翻訳文提出日　令和1年5月23日 (2019.5.23)
(86)国際出願番号　PCT/EP2017/081786
(87)国際公開番号　WO2018/108685
(87)国際公開日　平成30年6月21日 (2018.6.21)
(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)

(71)出願人　390009531
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
INTERNATIONAL BUSINESS MACHINES CORPORATION
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
New Orchard Road, Armonk, New York 10504, United States of America
(74)代理人　100108501
弁理士　上野　剛史

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)【要約】
【課題】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・インスタンスを提供する。
【解決手段】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に属してい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。コンテナのセットが地理的制約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。

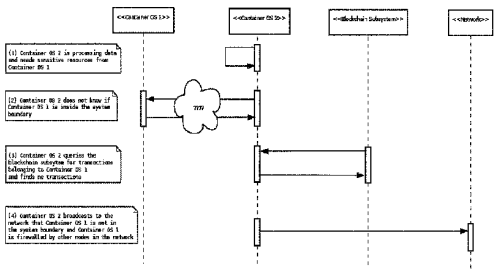


Fig. 12

【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。
【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５に記載の分散ネットワーク。
【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。
【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、
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】
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１１に記載のシステム。
【請求項１３】
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１１に記載のシステム。
【請求項１４】
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１５】
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１６】

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と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。

【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。

【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、

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他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。

【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１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、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、請求項１４ないし２８の前記方法を実行する、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】

【０００２】

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 2011) by Peter Mell and Timothy Grance, NIST Special Publication 800-145を参照して解釈される。

【０００３】

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。

【０００４】

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。

【０００５】

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。

【０００６】

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。

【０００７】

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。

【０００８】

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"Bitchain 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ＴｘＳ「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。ＭｅｔａＤｉｓｋ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。

【００１３】

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。７０ＭＢ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、３２ＭＢ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。

【００１４】

Ｓｔｏｒｊシステムは、記事"Storj A Peer-to-Peer Cloud Storage Network" by Shawn Wilkinson et al, December15, 2014 v1.01（https://storj.io/storj.pdf）において説明されている。

【００１５】

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。

【００１６】

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。

【００１７】

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／ＥＣ）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】"Bitchain 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, December15, 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。
【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。
【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。

【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】

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。

【００２８】

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。

【００２９】

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。

【００３０】

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、
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。

【００３１】

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、
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。

【００３２】

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ことの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】

【００３７】

【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。

【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。

【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】

【００３８】

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。

【００３９】

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、任意の種類の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経由して任意の種類の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。

【００４０】

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、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。

【００４１】

ハードウェアおよびソフトウェア・レイヤ６０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６１、ＲＩＳＣ（Reduced Instruction Set Computer）アーキテクチャベースのサーバ６２、サーバ６３、ブレード・サーバ６４、ストレージ・デバイス６５、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６６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６７およびデータベース・ソフトウェア６８を含む。

【００４２】

仮想化レイヤ７０は、仮想サーバ７１、仮想ストレージ７２、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７３、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７４、ならびに仮想クライアント７５などの仮想的実体を提供できる抽象レイヤを備える。

【００４３】

一例を挙げると、管理レイヤ８０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８１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８２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８３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８４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８５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。

【００４４】
ワークロード・レイヤ９０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９１、ソフトウェア開発およびライフサイクル管理９２、仮想クラスルーム教育の配信９３、データ分析処理９４、トランザクション処理９５、およびモバイル・デスクトップ９６が挙げられる。
【００４５】
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５５内に存在する。ハイパーバイザ４２によって実行されるコンテナのセット４０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１１０を定義する。コンテナ４０は、ハイパーバイザ４２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４２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１１０は、システム境界２８＿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のセットによって概念的に定義されるか、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、ルールのセットによって定義される。別のシステム境界２８＿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１２０を、それ自身のハイパーバイザ４２およびコンテナ４０と共に作成してよい。
【００４６】
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。
【００４７】
図１０は、コンテナ４０を示している。各コンテナ４０は、パブリックな台帳４４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４６と呼ぶ。コンテナのブロックチェーン・サブシステム４６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４６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４４のコピーを維持する。ブロックチェーン・サブシステム４６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４４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４６は、そのコンテナ４０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４４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１１０（または１２０）内の特定のコンテナのセットのすべてのコンテナ４０が、この台帳４４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。

【００４８】

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。

【００４９】

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、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。

【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】

例えば、図９を参照すると、ＳＩＣ　ＳＩＣ１ａ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　ＳＩＣ１ａは、破線で示されている新しい「標準」コンテナＣ１ｃを作成している最中であることがある。あるとき、ＳＩＣ１ａは、その制御中の状態を交代し、ＳＩＣ１ｂ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Ｃ２ａおよびＳＩＣ（ＳＩＣ２）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】

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。

【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が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を意味する。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。

【００５７】

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を意味している。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。

【００５８】

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。

【００５９】
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。
【００６０】
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、ということを意味する。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。
【００６１】
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。
【００６２】
図１１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。
【００６３】
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。
【００６４】
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。
【００６５】
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。
【００６６】
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。
【００６７】
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。
【００６８】
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。
【００６９】
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。

【００７０】
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。
【００７１】
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。
【００７２】
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。
【００７３】
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。
【００７４】
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。
【００７５】
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。
【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。

【００７９】

さらに別の代替的実施形態では、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。

【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。

【００８２】

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。

【００８３】

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。

【００８４】

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。

【００８５】

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。

【００８６】

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、任意の種類の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】

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。

【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。

【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。

【００９１】

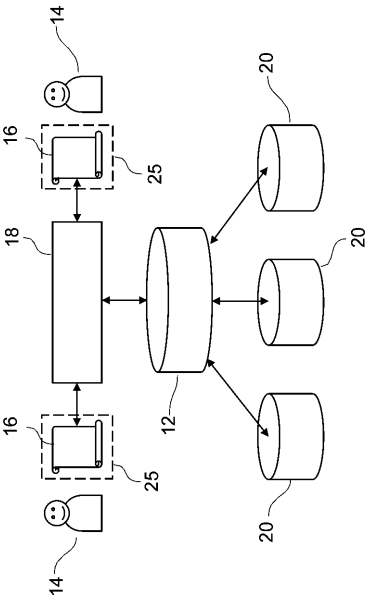
本開示の範囲を逸脱することなく、前述の実施形態例に対して多くの改良および変更が行われ得るということが、当業者にとって明らかであろう。

【符号の説明】

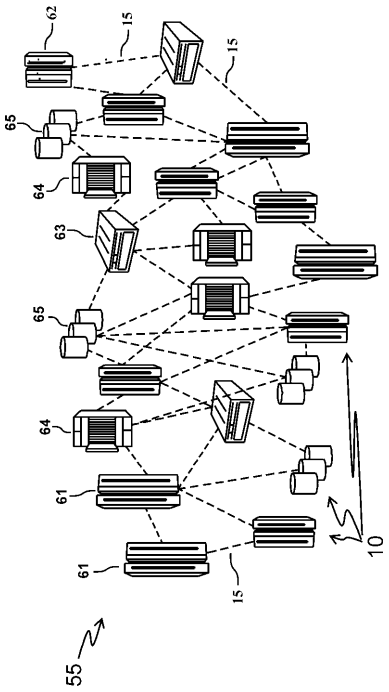
【００９２】

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
５４Ａ～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

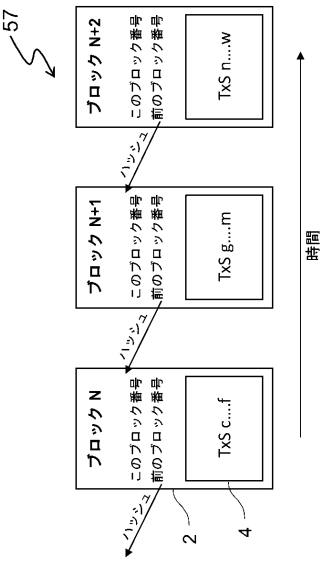
【図１】


14
16
25
18
20
12
20
20
16
25
14

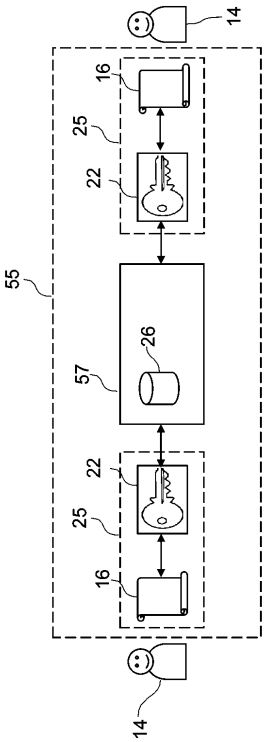
【図２】


62
15
15
65
64
63
65
64
61
61
15
10
55

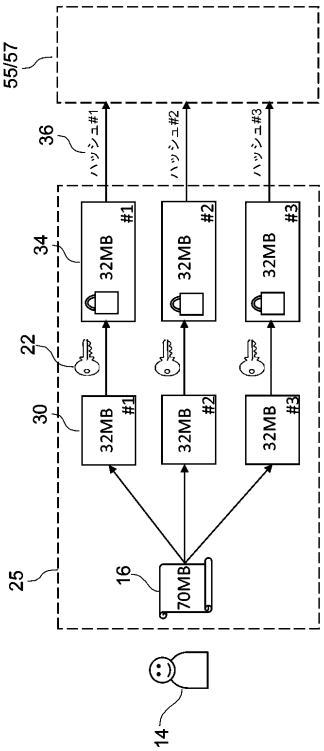
【図３】


57
ブロック N+2
このブロック番号
前のブロック番号
TxS n....w
ハッシュ
ブロック N+1
このブロック番号
前のブロック番号
TxS g....m
ハッシュ
ブロック N
このブロック番号
前のブロック番号
TxS c....f
ハッシュ
時間
2
4

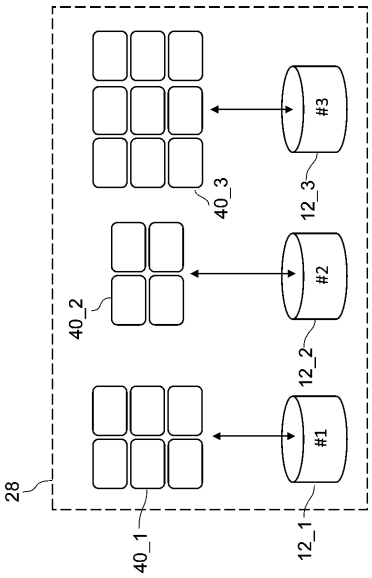
【図４】


14
16
25
22
55
57
26
22
25
16
14

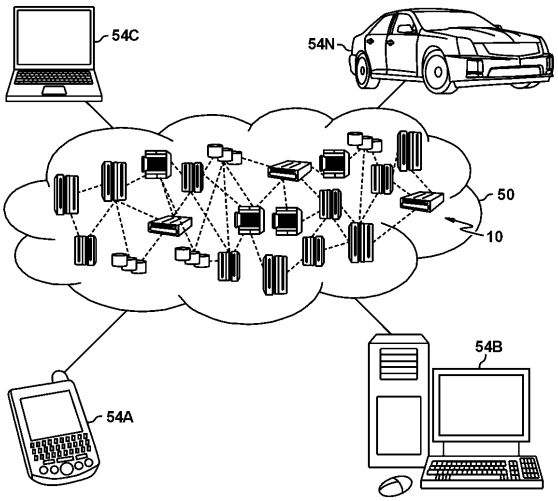
【図５】


55/57
36
ハッシュ#1
ハッシュ#2
ハッシュ#3
34
32MB #1
32MB #2
32MB #3
22
30
32MB #1
32MB #2
32MB #3
25
16
70MB
14

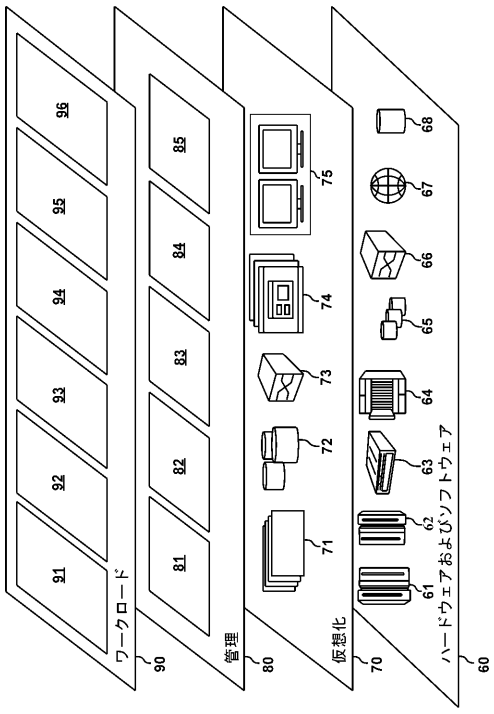
【図６】


28
40_1
40_2
40_3
12_1
12_2
12_3
#1
#2
#3

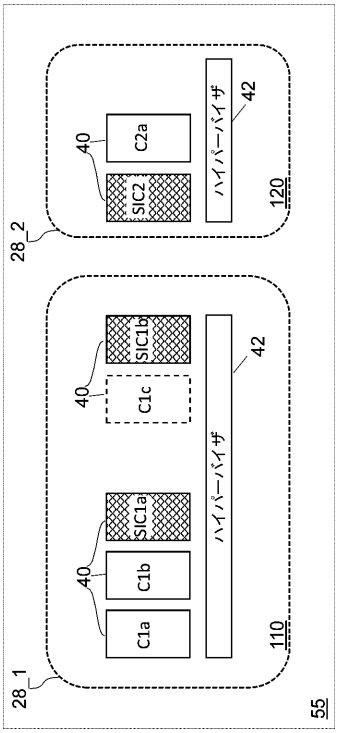
【図７】


54C
54N
50
10
54B
54A

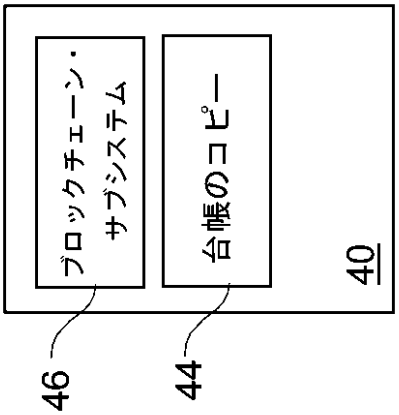
【図８】


ワークロード
90
91
92
93
94
95
96
管理
80
81
82
83
84
85
仮想化
70
71
72
73
74
75
ハードウェアおよびソフトウェア
60
61
62
63
64
65
66
67
68

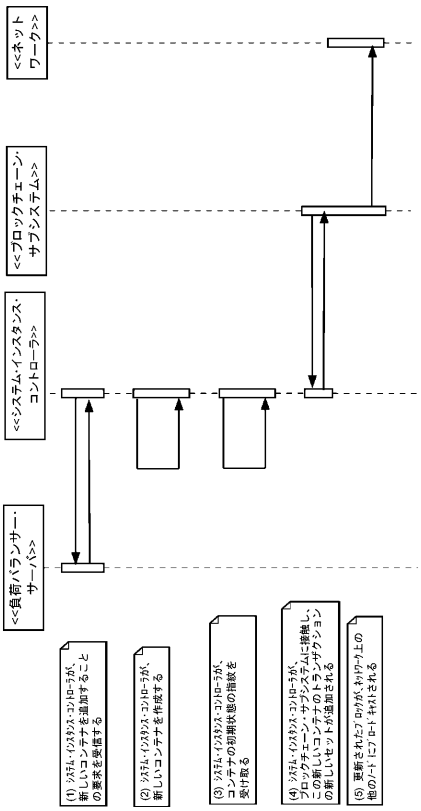
【図９】



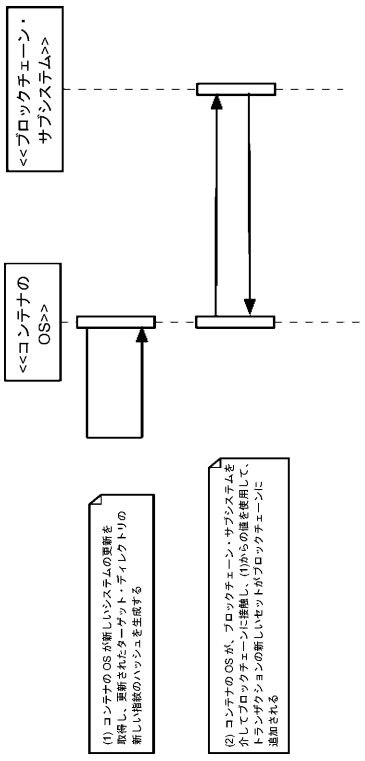

【図１０】



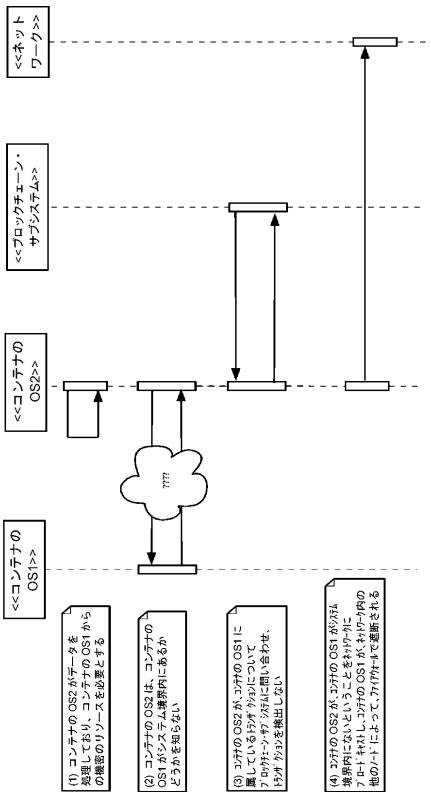

【図１１】



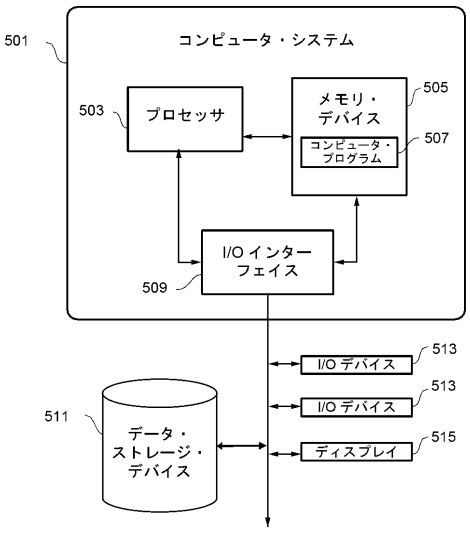

【図１２】



【図１３】




【図１４】




【手続補正書】
【提出日】令和1年9月19日(2019.9.19)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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。

【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５に記載の分散ネットワーク。

【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。

【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、

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】
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１１に記載のシステム。
【請求項１３】
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１１に記載のシステム。
【請求項１４】
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１５】
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１６】
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と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。
【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。
【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、
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他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。
【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、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、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する、コンピュータ・プログラム。

【国際調査報告】

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/081786

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/12 H04L29/08
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 2016/260095 A1 (FORD DANIEL A [US])<br>8 September 2016 (2016-09-08)<br>paragraph [0011] - paragraph [0016];<br>figure 1<br>----- | 1-29 |
| A | Shawn Wilkinson ET AL: "Metadisk: Blockchain-Based Decentralized File Storage Application",<br>,<br>20 August 2014 (2014-08-20), XP055454921,<br>Retrieved from the Internet:<br>URL:https://storj.io/metadisk.pdf<br>[retrieved on 2018-02-26]<br>the whole document<br>-----<br>-/-- | 1-29 |

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 1 March 2018 | 09/03/2018 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Vinck, Bart |

1

Form PCT/ISA/210 (second sheet) (April 2005)

## INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/081786

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | Shawn Wilkinson: "Storj A Peer-to-Peer Cloud Storage Network", , 15 December 2014 (2014-12-15), pages 1-18, XP055429592, Retrieved from the Internet: URL:https://storj.io/storj2014.pdf [retrieved on 2017-11-28] the whole document ----- | 1-29 |

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/081786

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2016260095 A1 | 08-09-2016 | NONE | |

フロントページの続き

(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT

（特許庁注：以下のものは登録商標）
１．ＳＭＡＬＬＴＡＬＫ

(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　ブライラート、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　ゾロトウ、クレア
アメリカ合衆国８０３０１－６１０８　コロラド州ボルダー　ダイアゴナル・ハイウェイ６３００
(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

【要約の続き】
【選択図】図１２