(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-516389
(P2024-516389A)
(43)公表日　令和6年4月15日(2024.4.15)

(51)国際特許分類　FI
H04L 9/32 (2006.01)　H04L 9/32 200Z
H04L 9/08 (2006.01)　H04L 9/08 F
G06F 21/33 (2013.01)　G06F 21/33

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2023-564192(P2023-564192)
(86)(22)出願日　令和4年4月20日(2022.4.20)
(85)翻訳文提出日　令和5年10月19日(2023.10.19)
(86)国際出願番号　PCT/EP2022/060366
(87)国際公開番号　WO2022/228960
(87)国際公開日　令和4年11月3日(2022.11.3)
(31)優先権主張番号　17/244,391
(32)優先日　令和3年4月29日(2021.4.29)
(33)優先権主張国・地域又は機関
米国(US)
(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,
最終頁に続く

(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　100112690
弁理士　太佐 種一
最終頁に続く

(54)【発明の名称】　コンピューティング・ネットワークへの許可型ブロックチェーン・アクセスのためのシステムおよび方法

(57)【要約】
コンピューティング・ノードのネットワークへのアクセスを提供するコンピュータ実施システム、方法およびコンピュータ・プログラム製品であって、クライアントによって、ネットワーク、好ましくは私設ネットワーク内のホスト・ノードへのアクセスをリクエストすること、デジタル証明書発行器を選択すること、デジタル証明書発行器によって、クライアントのトークンの識別を確認すること、証明書発行器によって、分散台帳にノンスを追加すること、およびネットワーク内のホスト・ノードへのアクセスをクライアントに許可することを含む、コンピュータ実施システム、方法およびコンピュータ・プログラム製品。一実施形態では、コンピューティング・ノードがＣＰＵ容量に基づいてランク付けされ、最も高いＣＰＵ容量ランクを有するコンピューティング・ノードが、ノンスに対する解を見つけるプルーフ・オブ・キャパシティ・コンセンサスに参加するように選択される。

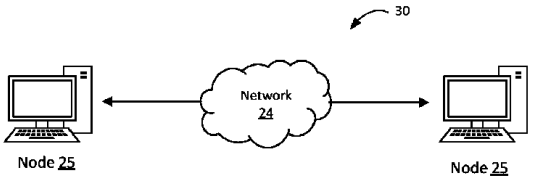


Fig. 1

【特許請求の範囲】
【請求項１】
コンピューティング・ノードのネットワークへのアクセスを提供するコンピュータ実施方法であって、前記方法が、
クライアントによって、前記ネットワーク内のホスト・ノードへのアクセスをリクエストすること、
デジタル証明書発行器を選択すること、
前記デジタル証明書発行器によって、クライアントのトークンの識別を確認すること、
前記デジタル証明書発行器によって、分散台帳にノンスを追加すること、および
前記ネットワーク内の前記ホスト・ノードへのアクセスを前記クライアントに許可すること
を含むコンピュータ実施方法。
【請求項２】
前記ネットワーク内の前記コンピューティング・ノードをランク付けすること、および前記ネットワーク内の前記コンピューティング・ノードのランクに従って、前記ノンスに対する解を見つけるプルーフ・オブ・キャパシティ・コンセンサスに参加する１つまたは複数のコンピューティング・ノードを選択することをさらに含む、請求項１に記載のコンピュータ実施方法。
【請求項３】
前記ネットワーク内の前記コンピューティング・ノードをランク付けすることが、前記コンピューティング・ノードの使用されていないＣＰＵ容量に基づく、請求項２に記載のコンピュータ実施方法。
【請求項４】
最も高いランクを有する前記コンピューティング・ノードをメイン・マイナーとして選択すること、および前記メイン・マイナーによって、前記メイン・マイナー上にインストールされたプラグインからデッドラインを取り出すことをさらに含む、請求項２に記載のコンピュータ実施方法。
【請求項５】
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノード上のノンス解ストアに、前記ノンスに対する可能な全ての解を格納することをさらに含む、請求項４に記載のコンピュータ実施方法。
【請求項６】
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノードによって、前記ノンスに対する解を見つける前記プルーフ・オブ・キャパシティ・コンセンサスを計算することをさらに含む、請求項５に記載のコンピュータ実施方法。
【請求項７】
前記ノンスに対する前記解を含む前記ノードを、前記デジタル証明書発行器であるとして選択することをさらに含む、請求項６に記載のコンピュータ実施方法。
【請求項８】
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノードによって、前記ノンスに対する解を見つける前記プルーフ・オブ・キャパシティ・コンセンサスを計算すること、および
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された前記コンピューティング・ノードがいずれも、前記デッドラインまでに前記ノンスに対する解を見つけなかったことに応答して、前記メイン・マイナーを前記デジタル証明書発行器として選択すること
をさらに含む、請求項５に記載のコンピュータ実施方法。
【請求項９】
前記ネットワークに新たなホスト・ノードを追加することをさらに含み、前記ネットワ

ークに新たなホスト・ノードを追加することが、
前記ネットワーク上の全ての前記コンピューティング・ノードによって、前記新たなホスト・ノードが一組の定められたネットワーク特性を有するかどうかを判定すること、
前記新たなホスト・ノードが一組の定められたネットワーク特性を有すると判定したことに応答して、前記新たなホスト・ノードから状態情報を取り出すこと、および
前記状態情報を、前記ネットワーク上の全ての前記コンピューティング・ノードと共有すること
を含む、請求項１に記載のコンピュータ実施方法。
【請求項１０】
前記ネットワークに新たなホスト・ノードを追加することが、前記分散台帳を前記新たなホスト・ノードと共有することをさらに含む、請求項９に記載のコンピュータ実施方法。
【請求項１１】
前記ネットワークに新たなホスト・ノードを追加することが、
前記新たなホスト・ノードが、前記コンピューティング・ノードと同じネットワークに追加されることを保証すること、
前記新たなホスト・ノード上にプラグインをインストールすること、
前記プラグインによって前記ネットワークを検出すること、および
前記ネットワークに新たなホスト・ノードが加わったことを、前記ネットワーク上の全ての前記コンピューティング・ノードに通知すること
をさらに含む、請求項１０に記載のコンピュータ実施方法。
【請求項１２】
前記分散台帳を前記新たなホスト・ノードと共有することが、ＲＡＦＴプロトコルを利用することを含み、ＲＡＦＴリーダー・ノード内の前記分散台帳を含むデータベースが、前記新たなホスト・ノードと共有される、請求項１０に記載のコンピュータ実施方法。
【請求項１３】
命令を含む非一過性コンピュータ可読媒体であって、前記命令が、少なくとも１つのハードウェア・プロセッサによって実行されたときに、
クライアントによって、コンピューティング・ノードのネットワーク内のホスト・ノードへのアクセスをリクエストすること、
デジタル証明書を発行する前記コンピューティング・ノードのうちの１つのコンピューティング・ノードを選択すること、
前記デジタル証明書を発行する選択された前記コンピューティング・ノードによって、クライアントのトークンの識別を確認すること、
前記デジタル証明書を発行する選択された前記コンピューティング・ノードによって、分散台帳にノンスを追加すること、および
前記ネットワーク内の前記ホスト・ノードへのアクセスを前記クライアントに許可すること
を実行するように、前記少なくとも１つのハードウェア・プロセッサを構成する、非一過性コンピュータ可読媒体。
【請求項１４】
少なくとも１つのハードウェア・プロセッサによって実行されたときに、
前記ネットワーク内の前記コンピューティング・ノードをランク付けすること、および
前記ネットワーク内の前記コンピューティング・ノードのランクに従って、前記ノンスに対する解を見つけるプルーフ・オブ・キャパシティ・コンセンサスに参加する１つまたは複数のコンピューティング・ノードを選択すること
を実行するように前記少なくとも１つのハードウェア・プロセッサを構成する命令
をさらに含む、請求項１３に記載の非一過性コンピュータ可読媒体。
【請求項１５】
前記ネットワーク内の前記コンピューティング・ノードをランク付けすることが、前記

コンピューティング・ノードの使用されていないＣＰＵ容量に基づき、使用されていない最も大きなＣＰＵ容量を有する少なくとも３つのコンピューティング・ノードが、前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択される、請求項１４に記載の非一過性コンピュータ可読媒体。

【請求項１６】

少なくとも１つのハードウェア・プロセッサによって実行されたときに、

前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノード上のノンス解ストアに、前記ノンスに対する可能な全ての解を格納すること、

前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノードによって、前記ノンスに対する解を見つける前記プルーフ・オブ・キャパシティ・コンセンサスを計算すること、および

前記ノンスに対する前記解を含む前記ノードを、前記デジタル証明書を発行する前記コンピューティング・ノードであるとして選択すること

を実行するように前記少なくとも１つのハードウェア・プロセッサを構成する命令

をさらに含む、請求項１４に記載の非一過性コンピュータ可読媒体。

【請求項１７】

少なくとも１つのハードウェア・プロセッサによって実行されたときに、

最も高いランクを有する前記コンピューティング・ノードをメイン・マイナーとして選択すること、

前記メイン・マイナーによって、前記メイン・マイナー上にインストールされたプラグインからデッドラインを取り出すこと、

前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノードによって、前記ノンスに対する解を見つける前記プルーフ・オブ・キャパシティ・コンセンサスを計算すること、および

前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された前記コンピューティング・ノードがいずれも、前記デッドラインまでに前記ノンスに対する解を見つけなかったことに応答して、前記メイン・マイナーを、前記デジタル証明書を発行する前記コンピューティング・ノードとして選択すること

を実行するように前記少なくとも１つのハードウェア・プロセッサを構成する命令

をさらに含む、請求項１６に記載の非一過性コンピュータ可読媒体。

【請求項１８】

少なくとも１つのハードウェア・プロセッサによって実行されたときに、前記ネットワークに新たなホスト・ノードを追加するように前記少なくとも１つのハードウェア・プロセッサを構成する命令をさらに含み、前記ネットワークに新たなホスト・ノードを追加することが、前記少なくとも１つのハードウェア・プロセッサによって実行されたときに、

前記ネットワーク上の全ての前記コンピューティング・ノードによって、前記新たなホスト・ノードが一組の定められたネットワーク特性を有するかどうかを判定すること、

前記新たなホスト・ノードが一組の定められたネットワーク特性を有すると判定したことに応答して、前記新たなホスト・ノードから状態情報を取り出すこと、および

前記状態情報を、前記ネットワーク上の全ての前記コンピューティング・ノードと共有すること

を実行するように前記少なくとも１つのハードウェア・プロセッサを構成する命令

を含む、請求項１３に記載の非一過性コンピュータ可読媒体。

【請求項１９】

前記ネットワークに新たなホスト・ノードを追加することが、前記少なくとも１つのハードウェア・プロセッサによって実行されたときに、前記分散台帳を前記新たなホスト・ノードと共有するように前記少なくとも１つのハードウェア・プロセッサを構成する命令をさらに含む、請求項１８に記載の非一過性コンピュータ可読媒体。

【請求項２０】

前記ネットワークに新たなホスト・ノードを追加することが、前記少なくとも１つのハードウェア・プロセッサによって実行されたときに、
前記新たなホスト・ノードが他の計算ノードと同じネットワークに追加されるかどうかを判定すること、
前記新たなホスト・ノードが他の計算ノードと同じネットワークに追加されると判定したことに応答して、前記新たなホスト・ノード上にプラグインをインストールすること、
前記プラグインによって前記ネットワークを検出すること、および
前記ネットワークに新たなホスト・ノードが加わったことを、前記ネットワーク上の全ての前記コンピューティング・ノードに通知すること
を実行するように前記少なくとも１つのハードウェア・プロセッサを構成する命令
をさらに含む、請求項１９に記載の非一過性コンピュータ可読媒体。

【請求項２１】

コンピューティング・ノードのネットワークを構成するためのコンピュータ実施システムであって、
プログラム命令を格納したメモリ・ストレージ・デバイスと、
前記コンピューティング・ノードのネットワークを構成するための前記プログラム命令を実行するための回路および論理を有するハードウェア・プロセッサと
を備え、前記ハードウェア・プロセッサが、前記メモリ・ストレージ・デバイスに結合されており、前記プログラム命令を実行したことに応答して、
クライアントによって、前記コンピューティング・ノードのネットワーク内のホスト・ノードへのリモート・アクセスをリクエストすること、
デジタル証明書発行器としてコンピューティング・ノードを選択すること、
前記デジタル証明書発行器によって、クライアントのトークンの識別を確認すること、
前記証明書発行器によって、分散台帳にノンスを追加すること、および
前記ネットワーク内の前記ホスト・ノードへのアクセスを前記クライアントに許可すること
を実行するように構成されている、コンピュータ実施システム。

【請求項２２】

使用されていないＣＰＵ容量の量に従って、前記ネットワーク内の前記コンピューティング・ノードをランク付けすること、
前記使用されていないＣＰＵ容量の量の前記ランク付けに基づいて、前記ノンスに対する解を見つけるプルーフ・オブ・キャパシティ・コンセンサスに参加する複数のコンピューティング・ノードを選択すること、
前記ノンスに対する解を見つける前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記複数のコンピューティング・ノードによって、前記プルーフ・オブ・キャパシティ・コンセンサスを計算すること、および
前記ノンスに対する前記解を含む前記ノードを、前記デジタル証明書発行器であるとして選択すること
を実行するようにさらに構成されている、請求項２１に記載のコンピュータ実施システム。

【請求項２３】

最も高いランクを有する前記コンピューティング・ノードをメイン・マイナーとして選択すること、
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノードによって、前記ノンスに対する解を見つける前記プルーフ・オブ・キャパシティ・コンセンサスを計算すること、および
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された前記コンピューティング・ノードがいずれも、デッドラインまでに前記ノンスに対する解を見つけなかったことに応答して、前記メイン・マイナーを前記デジタル証明書発行器として選択すること

を実行するようにさらに構成されている、請求項２２に記載のコンピュータ実施システム。

【請求項２４】

前記ネットワークに新たなホスト・ノードを追加するようにさらに構成されており、前記ネットワークに新たなホスト・ノードを追加することが、

前記ネットワーク上の全ての前記コンピューティング・ノードによって、前記新たなホスト・ノードが一組の定められたネットワーク特性を有するかどうかを判定すること、および

前記新たなホスト・ノードが一組の定められたネットワーク特性を有すると判定したことに応答して、前記新たなホスト・ノードから状態情報を取り出すこと、および

前記状態情報を、前記ネットワーク上の全ての前記コンピューティング・ノードと共有すること

を実行するように前記システムを構成することを含む、請求項２１に記載のコンピュータ実施システム。

【請求項２５】

前記ネットワークに新たなホスト・ノードを追加することがさらに、

前記新たなホスト・ノードが他のコンピューティング・ノードと同じネットワークに追加されるかどうかを判定すること、

前記新たなホスト・ノードが他のコンピューティング・ノードと同じネットワークに追加されると判定したことに応答して、前記新たなホスト・ノード上にプラグインをインストールすること、

前記プラグインによって前記ネットワークを検出すること、

前記ネットワークに新たなホスト・ノードが加わったことを、前記ネットワーク上の全ての前記コンピューティング・ノードに通知すること、および

前記分散台帳を前記新たなホスト・ノードと共有すること

を実行するように前記システムを構成することを含み、前記プラグインが、証明書発行器モジュール、ランク付けアルゴリズム・モジュール、ノンス生成器、前記分散台帳および状態情報を含むドキュメント・データベース、ならびにキーバリュー・データベースを含む、

請求項２４に記載のコンピュータ実施システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本出願は一般に、情報ハンドリングもしくはデータ処理ネットワークまたはその両方に関し、より詳細には、ネットワーク内でユーザを認証すること、およびコンピューティング・ネットワークへのアクセス（例えばリモート・アクセス）を、好ましくは改良された許可型ブロックチェーン・プロセス（permissioned blockchain process）を使用して提供することに関する。

【背景技術】

【０００２】

セキュア・シェル（Secure Shell）またはセキュア・ソケット・シェル（Secure Socket Shell）としても知られるＳＳＨは、セキュアでないネットワークを介してコンピュータにアクセスするセキュアな手段をユーザに提供する暗号ネットワーク・プロトコルである。ＳＳＨは、１台のコンピュータから別のコンピュータへのセキュアなリモート・ログインの方法であって、強力な認証を提供し、強力な暗号化を用いて通信を保護する方法である。セキュア・シェル（ＳＳＨ）証明書は、コンピューティング・ネットワーク内の１つまたは複数のホストに対して多数のユーザを認証するスケーラブルな手段である。全てのホストは、認証局（Certificate Authority）の公開鍵によって署名された証明書を信用するように構成されている。認証局は伝統的に、単一のホストから発行される鍵対（公開鍵と秘密鍵）である。その単一のホストによる障害、例えばその単一のホスト

の停止がある場合には、ネットワークにサインインする試みが失敗に終わるという問題が生じる。言い換えると、その単一のホストがデジタル証明書（例えばサーティフィケート・オブ・オーソリティ（Certificate of Authority）（ＣＡ））を発行することができない場合には、クライアント／ピア・コンピューティング・デバイスはネットワークに加わることができず、したがって、１つの中心認証局を有することが、単一の、潜在的に破壊的な障害発生点となりうる。私有のＣＡサーバを使用することは、その唯一のサーバで何か不都合が生じたときには、サーバを稼働可能に戻すのにかかる時間の間、ＳＳＨ認証が遮断されるため、リスクとなりうる。サーティフィケート・オブ・オーソリティ、例えばＳＳＨ証明書を発行する唯一の単一のコンピューティング・ノードを有することの不利益を克服するシステムもしくは方法またはその両方を有することは有利であろう。

【０００３】

さらに、唯一のサーバにサーティフィケート・オブ・オーソリティを発行させることは、ネットワークへオンボード中の新たな計算ノードの非効率なプロセスも提供する。ネットワークに新たなノードが追加されるたびに、その新たなノードが、ＣＡサーバからの署名された証明書を受け取ることを可能にするため、いくつかのステップが必要となる。新たなノードごとに、サーティフィケート・オブ・オーソリティの公開鍵のアップロードおよびＳＳＨＤ構成の変更が必要となる。これらのステップは、サーティフィケート・オブ・オーソリティ公開鍵を変更しなければならないときにも必要となる。単一のＣＡサーバを有することは、これらの全てのタスクをハンドリングする際に非効率でありうる。新たなノードがネットワークにアクセスすることを可能にするための全てのタスクをハンドリングする単一のサーバまたはコンピューティング・ノードを有することの不利益を克服するシステムもしくは方法またはその両方を有することは有益であろう。

【発明の概要】

【０００４】

本開示の理解を助けるため、本開示を限定する意図なしに、本開示の概要を示す。本開示は、当業者を対象としている。本開示のさまざまな態様および特徴は、いくつかの状況または例では別々に、あるいは他の状況または例では、本開示の他の態様、実施形態もしくは特徴またはそれらの組合せと組み合わせて、有利に使用することができることを理解すべきである。したがって、異なる効果を達成するため、これらのシステムもしくは方法またはその両方に変形および変更を加えることができる。この点に関して、本開示は、１つまたは複数の発明を提示および説明すること、ならびに複数の態様において、本発明は、特許請求項によって定義された数多くの発明を含むことが理解される。

【０００５】

コンピューティング・ノードのネットワーク、好ましくはコンピューティング・ノードのクローズド・ネットワークへのアクセスを提供するシステム、方法もしくはコンピュータ・プログラム製品またはこれらの組合せが開示される。１つまたは複数の実施形態では、このシステム、方法もしくはコンピュータ・プログラムまたはこれらの組合せが、クライアントによって、ネットワーク、好ましくは私設ネットワーク内のホスト・ノードへのアクセスをリクエストすること、デジタル証明書発行器（digital certificate issuer）を選択すること、デジタル証明書発行器によって、クライアントのトークンの識別を確認すること、証明書発行器によって、分散台帳（distributed ledger）にノンス（nonce）を追加すること、およびネットワーク内のホスト・ノードへのアクセスをクライアントに許可することを含む。一実施形態では、このシステム、方法もしくはコンピュータ・プログラム製品またはこれらの組合せが、ネットワーク内のコンピューティング・ノードをランク付けすること、およびネットワーク内のコンピューティング・ノードのランクに従って、ノンスに対する解を見つけるプルーフ・オブ・キャパシティ・コンセンサス（proof-of-capacity consensus）に参加する１つまたは複数の（好ましくは少なくとも３つの）コンピューティング・ノードを選択することを含む。ネットワーク内のコンピューティング・ノードをランク付けすることは、コンピューティング・ノードの使用されていないＣＰＵ容量に基づくことが好ましい。一実施形態では、このシステム、方法もし

くはコンピュータ・プログラム製品またはこれらの組合せがさらに、最も高いランクを有するコンピューティング・ノードをメイン・マイナー（main miner）として選択すること、およびメイン・マイナーによって、メイン・マイナー上にインストールされたプラグインからデッドラインを取り出すことを含む。一態様では、このシステム、方法もしくはコンピュータ・プログラム製品またはこれらの組合せがさらに、プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全てのコンピューティング・ノード上のノンス解ストア（nonce solution store）に、ノンスに対する可能な全ての解を格納することを含む。

【０００６】

一態様では、このシステム、方法もしくはコンピュータ・プログラム製品またはこれらの組合せがさらに、プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全てのコンピューティング・ノードによって、ノンスに対する解を見つけるプルーフ・オブ・キャパシティ・コンセンサスを計算することを含む。一態様では、このシステム、方法もしくはコンピュータ・プログラム製品またはこれらの組合せがさらに、ノンスに対する解を含むノードを、デジタル証明書発行器であるとして選択することを含む。追加の態様では、このシステム、方法もしくはコンピュータ・プログラム製品またはこれらの組合せがさらに、プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全てのコンピューティング・ノードによって、ノンスに対する解を見つけるプルーフ・オブ・キャパシティ・コンセンサスを計算すること、およびプルーフ・オブ・キャパシティ・コンセンサスに参加するように選択されたコンピューティング・ノードがいずれも、デッドラインまでにノンスに対する解を見つけなかったことに応答して、メイン・マイナーをデジタル証明書発行器として選択することを含む。

【０００７】

１つまたは複数の実施形態では、このシステム、方法もしくはコンピュータ・プログラム製品またはこれらの組合せがさらに、ネットワークに新たなホスト・ノードを追加することをさらに含み、ネットワークに新たなホスト・ノードを追加することは、ネットワーク上の全てのコンピューティング・ノードによって、新たなホスト・ノードが一組の定められたネットワーク特性を有するかどうかを判定すること、新たなホスト・ノードが一組の定められたネットワーク特性を有すると判定したことに応答して、新たなホスト・ノードから状態情報を取り出すこと、および状態情報を、ネットワーク上の全てのコンピューティング・ノードと共有することを含む。一態様では、ネットワークに新たなホスト・ノードを追加することが、分散台帳を新たなホスト・ノードと共有することをさらに含み、追加の態様では、新たなホスト・ノードが、コンピューティング・ノードと同じネットワークに追加されることを保証すること、新たなホスト・ノード上にプラグインをインストールすること、プラグインによってネットワークを検出すること、およびネットワークに新たなホスト・ノードが加わったことを、ネットワーク上の全てのコンピューティング・ノードに通知することを含む。一実施形態では、分散台帳を新たなホスト・ノードと共有することが、ＲＡＦＴプロトコルを利用することを含み、ＲＡＦＴリーダー・ノード内の分散台帳を含むデータベースが、新たなホスト・ノードと共有される。

【０００８】

命令を含む非一過性コンピュータ可読媒体であって、それらの命令が、少なくとも１つのハードウェア・プロセッサによって実行されたときに、上で論じたプロセスもしくはステップまたはその両方を実行するように、少なくとも１つのハードウェア・プロセッサを構成する、非一過性コンピュータ可読媒体も開示される。１つまたは複数の態様では、コンピューティング・ノードのネットワークを構成するためのコンピュータ実施システムもしくは方法またはその両方であって、コンピュータ実施システムもしくは方法またはその両方が、プログラム命令を格納したメモリ・ストレージ・デバイスと、コンピューティング・ノードのネットワークを構成するための前記プログラム命令を実行するための回路および論理を有するハードウェア・プロセッサとを含み、ハードウェア・プロセッサが、前記メモリ・ストレージ・デバイスに結合されており、前記プログラム命令を実行したこと

に応答して、上で論じたプロセスもしくはステップまたはその両方を実行するように構成されている、コンピュータ実施システムもしくは方法またはその両方が開示される。１つまたは複数の実施形態では、このシステム、方法もしくはコンピュータ・プログラム製品またはこれらの組合せが、ネットワークに新たなホスト・ノードを追加し、このシステム、方法もしくはコンピュータ・プログラム製品またはこれらの組合せが、新たなホスト・ノードが他のコンピューティング・ノードと同じネットワークに追加されるかどうかを判定すること、新たなホスト・ノードが他のコンピューティング・ノードと同じネットワークに追加されると判定したことに応答して、新たなホスト・ノード上にプラグインをインストールすること、プラグインによってネットワークを検出すること、ネットワークに新たなホスト・ノードが加わったことを、ネットワーク上の全てのコンピューティング・ノードに通知すること、および分散台帳を新たなホスト・ノードと共有することを実行するように構成されており、もしくはこれらのことを実行するための命令を含み、またはその両方を達成する。一実施形態では、このプラグインが、証明書発行器モジュール、ランク付けアルゴリズム・モジュール、ノンス生成器、分散台帳および状態情報を含むドキュメント・データベース、およびキーバリュー（Key-Value）・データベースを含む。

【０００９】

本発明の上記の目的、特徴もしくは利点またはこれらの組合せ、およびその他の目的、特徴もしくは利点またはこれらの組合せは、添付図面に示された本発明の下記のより詳細な説明および例示的な実施形態から明らかになる。添付図面では、同じ参照符号が一般に本発明の例示的な実施形態の同じ部分を表す。

【００１０】

ネットワークにホストを追加し、もしくはネットワーク、例えばノードのコンピューティング・ネットワーク内のノードにリモート・アクセスすることを、好ましくは許可型ブロックチェーン技術を使用してクライアントに許可し、またはこの両方を実行するシステムもしくは方法またはその両方、および一態様では、ノードを追加し、もしくはクローズド・ネットワーク内のノードにリモート・アクセスし、またはこの両方を実行するシステムもしくは方法またはその両方のさまざまな態様、特徴もしくは実施形態またはこれらの組合せは、提示された図ともに読んだときにより十分に理解されるであろう。これらのシステムおよび方法の態様、特徴もしくはさまざまな詳細またはこれらの組合せを示すため、これらの図には実施形態が提供されているが、特許請求項は、示された正確な配置、特徴、態様、実施形態、システム、モジュール、機能ユニット、プログラミング、命令、方法、プロセス、技術もしくはデバイスまたはこれらの組合せに限定されるべきではなく、示された配置、特徴、態様、実施形態、システム、モジュール、機能ユニット、プログラミング、命令、方法、プロセス、技術もしくはデバイスまたはこれらの組合せは、単独で、あるいは他の配置、特徴、態様、実施形態、システム、モジュール、機能ユニット、プログラミング、命令、方法、技術、プロセスもしくはデバイスまたはこれらの組合せと組み合わせて使用することができる。

【図面の簡単な説明】

【００１１】

【図１】本開示の一実施形態による、ピア・ネットワーク上で接続された２つのピア・デバイスを示す図である。

【図２】ネットワークを介して接続された１つのピア・グループ内の複数のピア・デバイスを示す図である。

【図３】ネットワークを介して他のピア・デバイスに接続可能な本開示による例示的なピア・デバイスを示す図である。

【図４】本開示の１つまたは複数の実施形態に従って接続可能ないくつかのピア・デバイスを有する例示的なピア・ネットワークを概略的に示す図である。

【図５】本開示の１つまたは複数の実施形態を実施するためのピア・デバイスまたはノードへのプラグインの概観図の一実施形態を概略的に示す図である。

【図６】本開示の１つまたは複数の実施形態による、図５のプラグインの部分としての証

明書発行器モジュールを概略的に示す図である。
【図７】本開示の一実施形態による、ネットワークにコンピューティング・ノード、例えばホスト・ノードを追加する方法の概略フローチャートである。
【図８】本開示の一実施形態による、ノード、例えばクライアントがネットワーク内のノードの１つにアクセスする方法の概略フローチャートである。
【図９】本開示の一実施形態による、サーティフィケート・オブ・オーソリティ（ＣＡ）発行器を選択する方法の概略フローチャートである。
【図１０】本開示の一実施形態による、ネットワーク内のノード間でデータを同期させる方法の概略フローチャートである。
【発明を実施するための形態】
【００１２】
以下の説明は、本発明の全体的な原理を示すためになされたものであり、以下の説明が、本明細書に記載された本発明の発想を限定することは意図されていない。以下の詳細な説明には、コンピューティング・ネットワーク内のノードもしくはピア・デバイスまたはその両方にセキュアにアクセスし、一態様ではノードを追加し、コンピューティング・ネットワークにリモート・アクセスする、本発明のシステム、方法もしくは技術またはこれらの組合せの理解を提供するために、数多くの詳細が記載されている。しかしながら、特定の詳細がなくても、本発明のシステムもしくは方法またはその両方の異なる数多くの実施形態を実施することができること、ならびに特許請求項および本開示は、本明細書に具体的に記載および図示された配置、システム、デバイス、モジュール、機能ユニット、プログラミング、命令、実施形態、特徴、態様、プロセス、方法、技術もしくは詳細またはこれらの組合せに限定されるべきでないことが当業者には理解される。さらに、本明細書に記載された特定の特徴、態様、実施形態、配置、システム、デバイス、モジュール、機能ユニット、プログラミング、命令、方法、プロセス、技術、詳細などを、さまざまな可能な組合せおよび置換の各々で、記載された他の特徴、態様、実施形態、配置、構造体、システム、デバイス、モジュール、機能ユニット、プログラミング、命令、技術、方法、プロセス、詳細などと組み合わせて使用することもできる。
【００１３】
当業者は、ネットワーク化されたコンピューティング環境、例えばコンピューティング・ノードのネットワークに、例えばＳＳＨプロトコルを使用してセキュアにアクセスすることを含むネットワーク化されたコンピューティング環境を含む、コンピューティング環境に精通していると仮定される。さらに、当業者は、許可型ブロックチェーン技術にも精通していると仮定される。以下の議論では、コンピューティング・ネットワーク・アーキテクチャ、許可型ブロックチェーン技術、コンピュータ・ノードへのリモート・アクセス（例えばＳＳＨリモート・アクセス）、およびそれらの動作を含む、当業者には明白であるはずのコンピューティング・ネットワークの従来の特徴は省き、または簡単にしか説明しない。符号が付けられた要素は、その要素が導入された図に従って符号付けされており、通常は、後続の図を通してその符号によって呼ばれることに留意されたい。
【００１４】
図１は、コンピューティング・ネットワーク３０内で接続された、コンピューティング・ノードとも呼ばれる２つのピア・デバイス２５Ａおよび２５Ｂを示している。ピア・デバイス２５は、コンピュータ、仮想コンピュータもしくは仮想機械（ＶＭ）またはノードであることができる。２つのピア・デバイス２５はいずれも、他方のピア・デバイスに対するホストまたはクライアントの役割を果たすことができる。図２は、コンピューティング・ネットワーク３０内でネットワーク２４を介して接続されたいくつかのピア・デバイス２５を示している。コンピューティング・ネットワーク３０内において、ピア・デバイス２５はいずれも、他のピア・デバイスのホストまたはクライアントの役割を果たすことができる。ピア・デバイス２５はノードとも呼ばれ、図示されているように、多くの形態、例えばコンピュータ３２、ラップトップ３３、スマート・フォン３４、パーソナル・アシスタント３５、端末３６、仮想機械またはその他の形態をとることができる。

【００１５】
図３は、コンピューティング・ネットワーク内でノード２５として使用することができる、本開示による例示的なコンピューティング・システムを示している。図示のコンピュータ・システムまたはコンピューティング・ノード２５は、適当な電子コンピュータ・システムの一例に過ぎず、本発明の実施形態の使用または機能の範囲に関する限定を暗示することを意図したものではないことを理解すべきである。例えば、示されたシステムは、数多くの他の汎用または専用コンピューティング・システム環境または構成とともに動作することがある。図３に示されたシステムとともに使用するのに適していることがあるよく知られたコンピューティング・システム、環境もしくは構成またはこれらの組合せの例には、限定はされないが、メインフレーム・コンピュータ・システム、サーバ・コンピュータ・システム、シン・クライアント、シック・クライアント、パーソナル・コンピュータ、ネットワーク化されたコンピュータ、ミニコンピュータ・システム、ハンドヘルドまたはラップトップ・デバイス、タブレット、スマート・フォン、マルチプロセッサ・システム、マイクロプロセッサ・ベースのシステム、セット・トップ・ボックス、プログラム可能なコンシューマ電子機器、および上記のシステムまたはデバイスのいずれかを含む分散型クラウド・コンピューティング環境などが含まれることがある。
【００１６】
いくつかの実施形態では、コンピュータ・システムまたはノード２５が、メモリ１６に格納されたプログラム・モジュールまたはソフトウェア・プログラムとして実装された、コンピュータ・システムによって実行されているコンピュータ・システム実行可能命令の一般的な文脈で説明されることがある。一般に、プログラム・モジュールは、本発明に従って特定のタスクを実行し、ならびに／または特定の入力データおよび／もしくはデータ・タイプを実施するルーチン、プログラム、オブジェクト、コンポーネント、論理、データ構造などを含むことがある。
【００１７】
コンピュータ・システム２５のコンポーネントには、限定はされないが、１つまたは複数のプロセッサまたは処理ユニット１２、メモリ１６、およびメモリ１６を含むさまざまなシステム・コンポーネントをプロセッサ１２に動作可能に結合するバス１４が含まれることがある。いくつかの実施形態では、プロセッサ１２が、メモリ１６からロードされた１つまたは複数のプログラム・モジュール１５を実行することができ、これらのプログラム・モジュールは、本発明の１つまたは複数の方法実施形態をプロセッサに実行させるソフトウェア（プログラム命令）を実装する。いくつかの実施形態では、プログラム・モジュール１５、例えばソフトウェア・プログラムを、プロセッサ１２の回路にプログラムすること、およびメモリ１６、ストレージ・デバイス１８、ネットワーク２４もしくはこれらの組合せ、またはこれらの組合せからロードすることができる。一般に、プロセッサ１２は、集積回路を含む、プロセッサ１２の動作を実行するための回路を含むことが理解される。
【００１８】
バス１４は、メモリ・バスまたはメモリ・コントローラ、周辺バス、アクセラレーテッド・グラフィクス・ポート（accelerated graphics port）、およびさまざまなバス・アーキテクチャのうちの任意のバス・アーキテクチャを使用するプロセッサまたはローカル・バスを含む、いくつかのタイプのバス構造体のうちの任意の１つまたは複数のタイプのバス構造体を表しうる。例として、限定はされないが、このようなアーキテクチャには、インダストリアル・スタンダード・アーキテクチャ（ＩＳＡ）バス、マイクロ・チャネル・アーキテクチャ（ＭＣＡ）バス、エンハンストＩＳＡ（ＥＩＳＡ）バス、ビデオ・エレクトロニクス・スタンダーズ・アソシエーション（ＶＥＳＡ）ローカル・バスおよびペリフェラル・コンポーネント・インターコネクツ（ＰＣＩ）バスが含まれる。
【００１９】
コンピュータ・システム２５は、さまざまなコンピュータ・システム可読媒体を含むことができる。このような媒体は、コンピュータ・システムによるアクセスが可能な使用可

能な任意の媒体であることができ、揮発性媒体と不揮発性媒体の両方、および取外し可能媒体と非取外し可能媒体の両方を含むことができる。メモリ１６（時にシステム・メモリと呼ばれる）は、ランダム・アクセス・メモリ（ＲＡＭ）、キャッシュ・メモリもしくは他の形態のメモリまたはこれらの組合せなどの揮発性メモリの形態のコンピュータ可読媒体を含むことができる。コンピュータ・システム２５はさらに、取外し可能／非取外し可能な揮発性／不揮発性の他のコンピュータ・システム・ストレージ媒体を含むことができる。単なる例として、非取外し可能な不揮発性磁気媒体（例えば「ハード・ドライブ」）から読み取るため、および非取外し可能な不揮発性磁気媒体（例えば「ハード・ドライブ」）に書き込むために、ストレージ・システム１８を提供することができる。図示されてはいないが、取外し可能な不揮発性磁気ディスク（例えば「フロッピー（Ｒ）・ディスク」）から読み取るため、および取外し可能な不揮発性磁気ディスク（例えば「フロッピー（Ｒ）・ディスク」）に書き込むための磁気ディスク・ドライブ、ならびにＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭもしくは他の光学式媒体などの取外し可能な不揮発性光ディスクから読み取るため、またはＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭもしくは他の光学式媒体などの取外し可能な不揮発性光ディスクに書き込むための光ディスク・ドライブを提供することができる。このような例では、１つまたは複数のデータ媒体インターフェースによって各々をバス１４に接続することができる。

【００２０】

コンピュータ・システム２５はさらに、１つもしくは複数の外部デバイス２６、例えばキーボード、ポインティング・デバイス、ディスプレイ２８など；ユーザがコンピュータ・システムと対話することを可能にする１つもしくは複数のデバイス；またはコンピュータ・システムが他の１つもしくは複数のコンピューティング・デバイスと通信することを可能にする任意のデバイス（例えばネットワーク・カード、モデムなど）、あるいはこれらの組合せと通信することができる。このような通信は入力／出力（Ｉ／Ｏ）インターフェース２０を介して実施することができる。

【００２１】

コンピュータ・システムまたはノード２５は、ネットワーク・アダプタ２２を介して、ローカル・エリア・ネットワーク（ＬＡＮ）、一般的なワイド・エリア・ネットワーク（ＷＡＮ）、私設ネットワーク、公衆ネットワーク（例えばインターネット）もしくはクローズド・ネットワークまたはこれらの組合せなどの１つまたは複数のネットワーク２４と通信することができる。本開示では、コンピュータ・システム２５がそれによって通信することになるネットワーク２４のうちの１つまたは複数のネットワーク２４が、ノード２５を、ネットワーク内および一実施形態ではクローズド・ネットワーク内の他の１つまたは複数のノードに接続することになる。図示されているように、ネットワーク・アダプタ２２は、バス１４を介してコンピュータ・システムの他のコンポーネントと通信する。図示されてはいないが、このコンピュータ・システムとともに、他のハードウェアもしくはソフトウェア・コンポーネントまたはその両方を使用することができることを理解すべきである。それらのコンポーネントの例には、限定はされないが、マイクロコード、デバイス・ドライバ、冗長処理ユニット、外部ディスク－ドライブ・アレイ、ＲＡＩＤシステム、テープ・ドライブおよびデータ・アーカイバル・ストレージ・システムなどが含まれる。

【００２２】

１つまたは複数の実施形態では、高可用性ＳＳＨ認証のために、ネットワーク内のコンピュータ・ノード間の許可型ピア・ツー・ピアＳＳＨ認証局認証が提供され、一態様では、ネットワーク内の全てのホストに、ネットワーク・ホストのいずれかにアクセスするため、例えばログインするために使用されるサーティフィケート・オブ・オーソリティ（ＣＡ）の署名に参加する許可が与えられる。１つまたは複数の実施形態では、ネットワークが、その識別の適当な確認の後であればネットワークに加わることを誰にでも許可する許可型ブロックチェーン技術を使用する。１つまたは複数の態様では、署名されたサーティフィケート・オブ・オーソリティをコンセンサスによって確認すること、共有台帳にアク

セスすること、および署名されたサーティフィケート・オブ・オーソリティ（ＣＡ）のレコードを格納することを全てのホストに許可するために、許可型ブロックチェーン技術が使用される。一実施形態では、ネットワーク内のあらゆるノードが一緒に動作してサーティフィケート・オブ・オーソリティを発行する。そのため、単一のまたは唯一のノードに依存してサーティフィケート・オブ・オーソリティ（ＣＡ）を発行することが排除される。許可型ブロックチェーンを利用して、クライアント・ノードにリモート・ホストへＳＳＨする資格を与え、それによって伝統的なＣＡアーキテクチャにおける潜在的な単一の障害発生点を回避することができる。

【００２３】

一実施形態では、ネットワーク内のノードのうちのいずれかのノードにアクセスすること、例えばＳＳＨアクセスすることを望んでいるクライアントにサーティフィケート・オブ・オーソリティを発行する能力を保持した分散または共有ドキュメント（台帳）を、多数のノードが格納する。一態様では、ネットワーク内の全てのノードが、ブロックチェーン・コンセンサス・アルゴリズムを実行して、そのクライアントがネットワークへのアクセスを有することを確認したときに、サーティフィケート・オブ・オーソリティ（ＣＡ）が発行される。一実施形態によれば、クローズド・ネットワーク内のリモート・ホストのうちのいずれかのリモート・ホストへのアクセスを有する、アクセスを有していた、またはアクセスが拒絶されている全てのクライアントを格納するために共有台帳が使用される。一態様では、あらゆるホスト・ノードが、アクセスが許可された全てのノードのコピーを有し、このことは監査能力を向上させる。

【００２４】

追加の実施形態では、ブロックチェーン・コンセンサス・アルゴリズムを実行するために、ネットワーク内の計算ノードの使用されていないＣＰＵが監視およびランク付けされる。ブロックチェーン・コンセンサス・アルゴリズムを解く際には、より使用されていない計算容量を有するノードが優先されることが好ましい。このようにすると、他の動作、例えばミッション・クリティカルな動作に利用されているＣＰＵが、ブロックチェーン・プロセスによって妨害されたり、または停滞したりしない。１つまたは複数の実施形態では、システムもしくは方法またはその両方が、計算ノードを確認し、計算ノードが、容易にネットワークに加わりもしくはネットワークを去り、またはその両方を実行することを可能にするための一組のノード特性を使用する。

【００２５】

高可用性ＳＳＨ認証のために、コンピューティング・ネットワーク内の計算ノード間の認証のための許可型ブロックチェーン用のシステム（例えばピア・ツー・ピアＳＳＨ認証局）が開示される。一実施形態では、全てのホストが、署名されたデジタル証明書をコンセンサスによって確認すること、署名されたデジタル証明書のレコードを格納すること（例えば、ネットワーク（例えばクローズド・ネットワーク）内のホストのうちのいずれかのホストへのアクセスを有する、アクセスを有していた、およびアクセスが拒絶されている全てのクライアントを格納すること）、ならびに共有分散台帳にアクセスすることができる。１つまたは複数の態様では、多数のノード、好ましくは使用されていない容量を有する多数のノードが、ネットワーク内のノードのうちのいずれかのノードにアクセス（例えばＳＳＨアクセス）することを望んでいるユーザ（クライアント）にデジタル証明書を発行することができる。追加の態様では、多数のノードが共有分散台帳を格納しており、ネットワーク内のノードが、プルーフ・オブ・キャパシティ・コンセンサス・アルゴリズムを実行して、ノードもしくはネットワークまたはその両方にアクセスする許可をユーザ（クライアント）が受けていることを確認したときに、デジタル証明書が発行される。

【００２６】

図４は、ピア・ツー・ピア・デバイスとも呼ばれるコンピューティング・ノード２５のコンピューティング・ネットワーク３０を示している。１つまたは複数の実施形態では、ネットワーク３０がクローズド・ネットワークであることが好ましく、図４では、ネットワーク３０が、クローズド・リング・ネットワーク・トポロジを示している。例えば、そ

れぞれのノード２５は、コンピュータもしくは仮想機械またはその両方であることができる。それぞれのノードはホストまたはクライアントであることができる。ホストは通常、他のデバイス、例えばコンピュータに接続されたコンピュータ・ハードウェア・デバイスまたはソフトウェアであって、他のデバイス、例えばコンピュータに、データまたはサービスを、好ましくはコンピューティング・ネットワークを介して提供するコンピュータ・ハードウェア・デバイスまたはソフトウェアである。ネットワーク３０上に接続されたあらゆるノード２５（例えばコンピュータ）は、ネットワーク３０上の他のピアまたはノード２５に対するホストとして機能しうる。ホストは例えば、コンピュータ、仮想機械、ピア・デバイスもしくはノードまたはこれらの組合せであることができる。クライアントは通常、サーバまたはホストによって使用可能にされたサービスまたはデータにアクセスするコンピュータ・ハードウェア・デバイスまたはソフトウェアである。サーバまたはホストはしばしば、クライアントとは別の物理コンピュータ上に置かれており、クライアントは、データもしくはサービスまたはその両方にネットワーク経由でアクセスする。このホストは例えば、コンピュータ、仮想機械、ピア・デバイスもしくはノードまたはこれらの組合せであることができる。

【００２７】

ネットワーク３０内のそれぞれのコンピュータ・ノード２５は、オペレーティング・システム（Ｏ／Ｓ）ソフトウェア・プラグイン４０を備える。１つまたは複数の実施形態では、それぞれの計算ノード２５がプラグイン４０をインストールし、プラグインは、好ましくはオペレーティング・システム（Ｏ／Ｓ）によって利用される適切なパッケージ・マネージャを使用してインストール、維持および更新される。１つまたは複数の実施形態では、プラグイン４０が、ノード監視、ランク付けアルゴリズム、ノード情報捕捉、ブロックチェーン・プルーフ・オブ・キャパシティ・アルゴリズム、ＲＡＦＴプロトコル、および非対称ＣＡ鍵の共有コピーを含む。例示的な一実施形態では、それぞれのプラグイン４０が、図５に示されているように、ノンス解生成器４２、ランク付けアルゴリズム・モジュール４４、ＲＡＦＴプロトコル・モジュール４６、ドキュメント・データベース５０、キーバリュー・データベース６０、および証明書発行器モジュール７０を含む。プラグイン４０および開示されたモジュールは、一実施形態では、ネットワーク３０にノード２５、例えばホスト・ノードをセキュアに追加することをハンドリングするように、もしくは容易にするように、またはその両方を実行するように回路を動作させるため命令および論理を提供し、一態様では、クライアントがネットワーク３０内のノード２５の１つにセキュアにアクセスすること、例えばＳＳＨリモート・アクセスすることをハンドリングするように、もしくは容易にするように、またはその両方を実行するように回路を動作させるための命令および論理を提供することが理解される。一実施形態では、クライアントがネットワーク内にある必要はないことを理解することができる。

【００２８】

ネットワーク３０に加わる最初のノード２５のプラグイン４０は、ブロックチェーンのジェネシス・ブロック（例えば分散台帳）を生成する。ネットワーク３０に加わる最初のノード２５は、オンボード・ノードを確認するための必要な全ての構成および判定基準（例えば、サーティフィケート・オブ・オーソリティ構成、コンセンサスに必要なノードの最小数など）を生成もしくは作成し、または生成および作成する。オンボード・ノードを確認するための判定基準は、プラグイン４０をダウンロードすることによって取得された構成ファイルに格納される。新たなノード２５は、一組の特性を有していると成功のうちに確認された後にネットワーク３０に加わることができる。これらの特性には、限定はされないが、ホスト名、新たなホストのドメイン・ネーム・システム（ＤＮＳ）、新たなホストのサブネット、ネットマスク、新たなホストのネットワーク・インターフェース、インバウンド／アウトバウンド・ネットワーク帯域幅などが含まれうる。一実施形態では、ネットワークに加わっている他のノードが、ネットワークに加わる最初のノードの構成を自動的にピックアップする。

【００２９】

１つまたは複数の実施形態では、クライアントが、ネットワーク３０内のいずれかのノード２５（例えばリモート・ホスト）へのアクセスをリクエストしたときに、署名されたデジタル証明書を発行する１つのノード２５が選択される。一態様では、共有サーティフィケート・オブ・オーソリティ（ＣＡ）鍵を用いてクライアントの公開鍵に署名するノードがランダムに選択される。一実施形態では、ネットワークへのアクセスがクライアントに許可される前に、リクエストの真正性を確認するために、使用可能なリソースを有するノードがコンセンサス・アルゴリズムを計算する。リクエストの真正性が確認されると、デジタル証明書（ＣＡ）に署名され、ブロックが生成され、署名されたデジタル証明書（例えばＣＡ）がブロックとしてブロックチェーンに追加される（例えば分散台帳内に新たなエントリが作られる）。追加の実施形態では、署名されたデジタル証明書を発行するためおよびコンセンサス・アルゴリズムを計算するために計算ノードが使用することができるフリーの容量もしくは使用されていない容量またはフリーの使用されていない容量がどれくらいあるのかに基づいて、ネットワーク内の計算ノードがランク付けされる。一態様では、コンセンサス・アルゴリズムを実行してクライアント・リクエストの真正性を確認するのに、使用されていないコンピューティング容量もしくはフリーのコンピューティング容量または使用されていないフリーのコンピューティング容量を最も多く持っているノードが使用される。このようにすると、ブロックチェーン動作に使用されることによるミッション・クリティカルな動作用の計算リソースの消費を回避するために、ブロックチェーン動作に対して使用可能なリソースを有する計算ノードが、ブロックチェーン・セキュリティ・プロトコルを計算しもしくは解きまたは計算し解くために使用される。一実施形態では、ネットワーク内のそれぞれの計算ノードが、ブロックチェーン（分散台帳）の現在のコピーを格納している。

【００３０】

図５のプラグイン４０の実施形態の詳細をさらに参照すると、図６でより詳細に説明される証明書発行器モジュール７０は、デジタル証明書、例えばサーティフィケート・オブ・オーソリティ（ＣＡ）を生成および発行する。一実施形態では、証明書発行器モジュール７０が、デジタル証明書を発行するように回路を動作させるための命令および論理を含む。１つまたは複数の実施形態では、１つのノードがサーティフィケート・オブ・オーソリティ（ＣＡ）を発行する代わりに、ネットワーク、例えばネットワーク３０内のあらゆるノードがサーティフィケート・オブ・オーソリティ（ＣＡ）を発行することができる。一態様では、ランク付けアルゴリズム・モジュール４２が、ノード２５のＣＰＵ容量を決定もしくは計算または決定および計算し、最大ＣＰＵ容量、例えば使用されていないコンピューティング・パワーを有するネットワーク３０内のノード２５を識別もしくはランク付けし、または識別およびランク付けする。一態様では、ランク付けアルゴリズム・モジュール４２が、ブロックチェーン・コンセンサス問題を解くのにどのノードが参加し、デジタル証明書を発行することができるかを決定もしくは選択し、または決定および選択する。一実施形態では、ランク付けアルゴリズム・モジュール４２が、ネットワーク３０内のノード２５のＣＰＵコンピューティング・パワーを決定、計算、識別もしくはランク付けまたはこれらの組合せを実行するように回路を動作させるための命令および論理を有する。一態様では、それぞれのプラグイン４０内のランク付けアルゴリズム４２が、その対応するそれぞれのノード２５のＣＰＵコンピューティング・パワーを決定し、ネットワーク内の他のノードのＣＰＵコンピューティング・パワーを受け取る。１つまたは複数の実施形態では、ミッション・クリティカルな動作を実行していないノードによって許可型ブロックチェーン動作を実行することができるように、ランク付けアルゴリズム・モジュール４２が、ミッション・クリティカルなプロセスを実行していないノードを探している。

【００３１】

ノンス解生成器４４は、ノンスに対する可能な解を生成し、それらの可能な解をノンス解ストア６６に格納する。ノンスは、「ナンバー・オンリー・ユーズド・ワンス（number only used once）」の略であり、数学的暗号問題に対する解を表す。ノンスは、ブロックチェーン・マイナーがそれに対する解を探している数（例えばハッシュ）である。

一実施形態では、ノンス解生成器４４が、暗号ノンスを生成し、その解を見つけるように回路を動作させるための命令および論理を有する。ノンスに対する解を生成することができるどのノードであっても、そのノードは、ブロックチェーンへのブロックをマイニングし、デジタル証明書（ＣＡ）を生成するように選択される。ノンス解生成器は当技術分野でよく知られている。ＲＡＦＴプロトコル・モジュール４６は、ネットワーク内の全てのノードにわたってデータを同期させる。ＲＡＦＴは、コンピューティング・ノードのクラスタ／ネットワークの全体にわたって状態機械を分散させるコンセンサス・アルゴリズムであり、クラスタ／ネットワーク内のそれぞれのノードが、同じ一連の状態遷移について合意に達することを保証する。ＲＡＦＴプロトコル・モジュール４６は、ネットワーク内の全てのコンピューティング・ノードにわたってデータを同期させるように回路を動作させるための命令および論理を含む。

【００３２】

プラグイン４０はさらにドキュメント・データベース５０を含み、ドキュメント・データベース５０は、ブロックチェーン・データベース５２および状態データベース５４を含む。ブロックチェーン・データベース５２は、ブロックチェーン、例えば発行されたサーティフィケート・オブ・オーソリティ（ＣＡ）の分散台帳を含む。状態データベース５４は、ネットワーク３０内の機械の状態、例えばノード情報、例えばメモリ、ストレージ、ワークロード（プロセス）、ホスト名、ＩＰアドレスなどを含む。プラグイン４０はさらにキーバリュー・データベース６０を含み、キーバリュー・データベース６０は、デッドライン・データベース６２、ノンス採掘難易度（nonce difficulty）データベース６４およびノンス解ストア６６を含む。デッドライン・データベース６２は、デッドライン、例えばマイナー（プルーフ・オブ・キャパシティ・アルゴリズムに参加しているノード）のいずれかがノンスに対する解を見つける時間を格納している。ノンス採掘難易度データベース６４は、ノンスに対する解を提供する判定基準を含む。例えば、ノンス採掘難易度は、３つのゼロ（０）から始まる１６桁のランダム数としてセットすることができる。ノンス解ストア６６は、ノンスに対する全ての解（可能な推定）のリストを含む。

【００３３】

証明書発行器モジュール７０は、図６に示されているように、証明書生成器（Certificate Generator）モジュール７２、ＣＡ非対称鍵モジュール７４、デジタル署名器（Digital Signer）モジュール７５、認証提供器（Auth Provider）モジュール７６、および識別確認モジュール７８を含む。証明書生成器モジュール７２は、デジタル証明書を生成するように回路を動作させるための命令および論理を有する。証明書生成器モジュール７２は、ノードが暗号ノンスに対する解を見つけるときに呼び出される（例えばデジタル証明書を発行するノードを選択するプルーフ・オブ・キャパシティ・プロセス）。証明書生成器の出力はデジタル証明書である。

【００３４】

認証提供器７６は、正当なユーザの認証を提供もしくは決定しまたは提供および決定するように回路を動作させるための命令および論理を有する。認証提供器モジュール７６は、ユーザ、例えばリモート・アクセスしようとしているクライアントの識別を確認するために識別確認モジュール７８から入力を受け取る。識別確認モジュール７８は、ユーザ、例えばユーザのトークンの識別を確認するように回路を動作させるための命令および論理を有する。識別確認モジュール７８は、認証提供器モジュール７６からの認証提供器（例えばＭｉｃｒｏｓｏｆｔ Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ、Ｇｏｏｇｌｅ Ｓｕｉｔｅ、Ｏｋｔａ、Ｔｏｋｅｎｓ）およびクライアント・クレデンシャル（client credential）を受け入れる。識別確認モジュール７８は、クライアントを成功のうちに認証することができるかどうかを示すブーリアン（例えば真／偽の指標）を出力する。クライアントは、ネットワーク内のノードへのＳＳＨアクセスを試みる前にクレデンシャルおよび認証方法を指定する必要がある。

【００３５】

ＣＡ非対称鍵モジュール７４は、ネットワーク内のそれぞれのノードの公開および秘密

鍵を格納している。これらの２つの鍵は、デジタル署名器モジュール７５への入力として使用される。デジタル署名器モジュール７５は、サーティフィケート・オブ・オーソリティ（ＣＡ）に署名するように回路を動作させるための命令および論理を有する。デジタル証明書が生成されると、デジタル署名器モジュール７５は、ＣＡ非対称鍵モジュール７４から受け取った秘密鍵を用いてデジタル証明書に署名する。デジタル署名器モジュール７５は、ＣＡ非対称鍵モジュール７４から入力（秘密鍵）を受け取り、証明書生成器７２からデジタル証明書（例えばＣＡ）を受け取り、デジタル証明書（例えばＣＡ）に秘密鍵を付加する。デジタル署名器モジュール７５は、ブロックチェーンに追加する新たなブロック内のデータとして追加する署名されたデジタル証明書（例えばＣＡ）を出力し、さらにこの証明書は、クライアントに返されて、ターゲット・ノードにログインする許可として使用される。ターゲット・ノードは、クライアントによって使用される証明書が正当なものであるかどうかを判断することができる。

【００３６】

プラグイン４０、ならびにランク付けアルゴリズム４２、ノンス解生成器４４、ＲＡＦＴプロトコル・モジュール４６、ドキュメント・データベース５０、キーバリュー・データベース６０および証明書発行器モジュール７０については、図７～１０に関してさらに詳細に論じる。

【００３７】

図７は、一実施形態による、ネットワークにノードを追加する方法７００を図示および説明する例示的なフローチャートであり、一態様では、この方法が、ネットワーク、好ましくはクローズド・ネットワーク内の一群のホストにホスト・ノードをセキュアに追加することを含む。方法７００は、便宜上、本開示を限定する意図なしに、一連のステップもしくはいくつかのステップまたは一連のいくつかのステップを含むものとして説明されるが、プロセスが一連のステップとして実行される必要はなく、もしくはステップが、図７に関して示し説明する順序で実行される必要はなく、またはその両方であるが、プロセスを統合すること、または１つもしくは複数のステップを一緒に同時に実行すること、あるいはその両方を実行することができること、あるいは開示された順序でもしくは代替の順序でステップを実行することができることが理解される。

【００３８】

１つまたは複数の態様では、ネットワークに新たなノード、例えばホスト・ノードを追加する方法７００が、７０５で、追加する新たなノードが、残りのノード、例えば残りのホスト・ノードと同じネットワーク上にあることをチェックもしくは確認またはチェックおよび確認することを含む。１つまたは複数の実施形態では、追加するノードが、同じプライマリ・ドメイン・ネーム・システム（ＤＮＳ）、同じサブネットもしくは同じネットワーク・インターフェースまたはこれらの組合せ上にある／に対するものであるかどうかを判定するためにチェックが実施される。１つまたは複数の実施形態ではこのネットワークがクローズド・ネットワークである。７１０で、新たなノード上に、ソフトウェア・プラグイン、例えばプラグイン４０をインストールする。７２０で、新たなノード、例えばノード２５上のプラグインが、このネットワークを検出し、ネットワークに新たなノードが加わったことをネットワーク上の他のノードに通知する。７３０で、新たなノードが一組の定められたネットワーク特性を有するかどうかを、ネットワーク内の全てのノードが確認する。新たなノード、例えば新たなホスト・ノードがノードのネットワーク、例えばクローズド・ネットワークに加わり、許可型ブロックチェーン機能に参加することができるようにするためには、その前に、一組の定められた特性に対してその新たなノードを確認する必要がある。これらの特性には、限定はされないが、ホスト名、新たなノード（例えばホスト・ノード）のドメイン・ネーム・システム（ＤＮＳ）、新たなノード（例えばホスト・ノード）のサブセット、ネットマスク、新たなノード（例えば新たなホスト・ノード）のネットワーク・インターフェース、インバウンド／アウトバウンド・ネットワーク帯域幅などが含まれうる。

【００３９】

プラグイン、例えばプラグイン４０は、７４０で、新たなノードから状態情報を取り出し、ネットワーク、例えばネットワーク内の他のノードの各々と状態情報を共有する。一態様では、プラグイン４０のドキュメント・データベース５０内の状態データベース５４から状態情報を取り出して、その状態情報をネットワーク内の他のノードに送信する。ネットワーク内で状態情報を分散させる方法および手法は、ＲＡＦＴプロトコルを利用することを含み、一実施形態では、この方法および手法が、図１０の方法１０００およびフローチャートに記載されている。７５０で、ブロックチェーン、例えば分散台帳が新たなノードと共有される。一態様では、ネットワーク内の他のノードによって分散台帳が新たなノードに送られ、もしくはネットワーク内の他のノードから分散台帳が取得され、またはその両方が達成される。このようにして、１つまたは複数の実施形態では許可型ブロックチェーン機能を有するネットワーク、好ましくはクローズド・ネットワークに、新たなノード、好ましくはホスト・ノードが追加される。新たなノードは、分散型／共有台帳の全体、例えばブロックチェーンの全体のコピーを有することが好ましい。

【００４０】

図８は、ネットワーク内のノードにリモート・アクセスする、好ましくはネットワーク内のノードにセキュア・シェル（ＳＳＨ）リモート・アクセスする方法８００を説明する例示的なフローチャートである。方法８００は、便宜上、本開示を限定する意図なしに、一連のステップもしくはいくつかのステップまたは一連のいくつかのステップを含むものとして説明されるが、プロセスが一連のステップとして実行される必要はなく、もしくはステップが、図８に関して示し説明する順序で実行される必要はなく、またはその両方であるが、プロセスを統合すること、または１つもしくは複数のステップを一緒に同時に実行すること、あるいはその両方を実行することができること、あるいは開示された順序でもしくは代替の順序でステップを実行することができることが理解される。

【００４１】

一実施形態では、方法８００が、ネットワーク内のノードにリモート・アクセスすることを対象とし、一態様では、特に、ネットワークにセキュア・シェル（ＳＳＨ）リモート・アクセスすることを対象とする。８０５で、クライアントが、ネットワーク内のノードへのリモート・アクセスをリクエストする。一実施形態では、クライアントが、ネットワーク内のノードへのセキュア・シェル（ＳＳＨ）に対するリクエストを発行する。１つまたは複数の態様ではネットワークがクローズド・ネットワークである。８１０で、サーティフィケート・オブ・オーソリティ（ＣＡ）発行器を選択する。サーティフィケート・オブ・オーソリティ（ＣＡ）発行器を選択する実施形態が、図９のフローチャートおよび方法９００に関してより詳細に記載されている。

【００４２】

８１５で、選択された証明書発行器が、クライアントのトークンの識別を確認する。この点に関して、ネットワーク内のノードにリモート・アクセスしたいクライアントは、そのクライアントのトークンを、プラグイン４０内の選択された証明書発行器７０に送る。クライアントのトークンは、クライアント・ノードで生成され、そこで、選択された認証提供器がクライアント・クレデンシャルを認証し、トークンを発行することが確立される。クライアントは、クライアントのクレデンシャルの組合せである。クライアントは、認証提供器モジュール７６内の既存のクレデンシャルを有しているべきである。一実施形態では、８１５で、証明書発行器７０内の識別確認モジュール７８を使用して、クライアントのトークン（クライアントのクレデンシャル）を、認証提供器モジュール７６の中に指定された認証提供器に対して確認する。すなわち、一態様では、８１５で、識別確認モジュール７８によってクライアントの識別が確認される（識別確認モジュールが、クライアントのトークンが有効であるかどうかをチェックする）。８２０で、証明書発行器が、新たな証明書、前のブロックのハッシュ、タイムスタンプおよびノンスをブロックチェーンに追加する。ブロックチェーンは、ネットワーク、例えばクローズド・ネットワーク内の全てのノード上にインストールされたソフトウェア・プラグイン４０のドキュメント・データベース５０内のブロックチェーン・データベース５２に格納されている。この情報を

、プラグイン４０のＲＡＦＴプロトコル・モジュールを使用してネットワーク内の他のノードと同期させる。８２５で、クライアントがノードにアクセスする。

【００４３】

一実施形態では、８１５～８２５で、クライアント／ユーザがネットワークにリモート・アクセスすることを許可するために、許可型ブロックチェーン・プロセスが実行される。一態様では、１つの単一のノードに依存してＣＡを発行することを排除するために、ネットワーク内のそれぞれのノードが一緒に動作して、認証局に署名し／認証局を発行する。ネットワーク内のあらゆるホストは、リモート・ホストのうちのいずれかのリモート・ホストへのアクセスが許可された全てのクライアントのコピーを有する。全てのホストは、ネットワーク内のリモート・ホストのうちのいずれかのリモート・ホストへのアクセスを有する、アクセスを有していた、またはアクセスが拒絶されている全てのクライアントを識別する共有台帳のコピーを有する。

【００４４】

図９は、証明書発行器を選択する、好ましくはネットワーク内のノードにセキュア・シェル（ＳＳＨ）リモート・アクセスするために証明書発行器を選択する方法９００を説明する例示的なフローチャートである。方法９００は、便宜上、本開示を限定する意図なしに、一連のステップもしくはいくつかのステップまたは一連のいくつかのステップを含むものとして説明されるが、プロセスが一連のステップとして実行される必要はなく、もしくはステップが、図９に関して示し説明する順序で実行される必要はなく、またはその両方であるが、プロセスを統合すること、または１つもしくは複数のステップを一緒に同時に実行すること、あるいはその両方を実行することができること、あるいは開示された順序でもしくは代替の順序でステップを実行することができることが理解される。１つまたは複数の実施形態では、方法８００の８１０で証明書発行器を選択するのに方法９００が使用される。証明書発行器を選択する他の方法も企図される。

【００４５】

９０５で、ノード・ランク付けを使用して、どの１つまたは複数のノードが、プルーフ・オブ・キャパシティ・コンセンサス、例えばブロックチェーン・プルーフ・オブ・キャパシティ・コンセンサスに参加するのかを選択する。一実施形態では、プルーフ・オブ・キャパシティ・コンセンサスに参加する複数のノード、好ましくは奇数のノードが選択される。プルーフ・オブ・キャパシティ・コンセンサスは、暗号問題に対する解であり、この暗号問題を解くことは、暗号問題に対する解を計算するために、ノードのストレージ、例えばハード・ドライブ上の使用可能スペースを使用する。１つまたは複数の実施形態では、ランク付けアルゴリズム・モジュール４２内で、ネットワーク内のノードのＣＰＵ容量が計算およびランク付けされる。９０５では、ノードＣＰＵ容量ランク付けを使用して、プルーフ・オブ・キャパシティ・コンセンサスを解くために使用される１つまたは複数のノード、好ましくは３つ以上のノードを選択する。

【００４６】

９１０で、最もランクの高いノードがメイン・マイナーとして選択される。９１５で、メイン・マイナーがプラグインからデッドラインを取り出す。すなわち、一実施形態では、９１５で、メイン・マイナーが、そのプラグイン４０のキーバリュー・データベース６０内のデッドライン・データベース６２からデッドラインを取り出す。このデッドラインは、プルーフ・オブ・キャパシティ・コンセンサスを解くことに参加するように選択されたマイナー（例えばノード）の１つが、ノンスに対する解を見つけるためのマイナー（ノード）として選択されるまでに経過する時間、例えば秒で表された時間である。ノンス（ナンバー・オンリー・ユーズド・ワンス（number only used once））は、マイナーが、例えば推測のために、暗号問題に対する解として解を見つけている数である。この暗号問題は、（キーバリュー・データベース６０内のノンス採掘難易度データベース６４に格納された）ノンス解である。

【００４７】

９２０で、プルーフ・オブ・キャパシティ暗号コンセンサス問題を解くことに参加する

全てのノードが、ノンスに対する可能な全ての解をノンス解ストア６６に格納する。すなわち、９２０では、プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択されたそれぞれのノードが、そのノンス解ストア６２に、ノンスに対する可能な全ての解を格納する。９２５で、プルーフ・オブ・キャパシティ・コンセンサスに参加するマイナーとして選択されたそれぞれのノードが、プルーフ・オブ・キャパシティ・コンセンサス・アルゴリズム計算を開始する。一実施形態では、ノンス解ストア６６からの可能なそれぞれの解が、ノンスに対する解を生成するためのブロックチェーン・プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択されたそれぞれのノード（例えばマイナー）のそれぞれのノンス解生成器４４によって使用される。９３０で、サーティフィケート・オブ・オーソリティを発行するために、デッドライン内のノンスに対する解を含む最初のノードが選択される。すなわち、９３０では、ノンスを解くノードが、新たなサーティフィケート・オブ・オーソリティを発行する。規定されたデッドライン時間内にノードがノンスの解を見つけなかった場合、９４０で、メイン・マイナーが、サーティフィケート・オブ・オーソリティを発行するノードとして選択される。１つまたは複数の実施形態では、実施中に、メイン・マイナーまたは他のノードによってノンスの解を見つける（推測する）必要はない。

【００４８】

図１０は、ネットワーク、例えばクローズド・ネットワーク３０のノード、例えばノード２５にわたってデータを同期させる方法１０００を説明する。例示的なフローチャートである方法１０００は、便宜上、本開示を限定する意図なしに、一連のステップもしくはいくつかのステップまたは一連のいくつかのステップを含むものとして説明されるが、プロセスが一連のステップとして実行される必要はなく、もしくはステップが、図１０に関して示し説明する順序で実行される必要はなく、またはその両方であるが、プロセスを統合すること、または１つもしくは複数のステップを一緒に同時に実行すること、あるいはその両方を実行することができること、あるいは開示された順序でもしくは代替の順序でステップを実行することができることが理解される。

【００４９】

１００５で、ＲＡＦＴプロトコル・モジュールに、ログもしくはデータベースまたはその両方がタイムスタンプとともに格納される。ＲＡＦＴ（リライアブル、リプリケーテッド、リダンダント、アンド　フォールトトレラント（Reliable, Replicated, Redundant, and Fault-tolerant））は、コンピューティング・ノードまたはシステムのクラスタ／ネットワークの全体にわたって状態機械を分散させる手段を提供するコンセンサス・アルゴリズムである。一態様では、ノード２５のプラグイン４０のＲＡＦＴプロトコル・モジュール４６内のログもしくはデータベースまたはその両方が、タイムスタンプとともに格納される。１０１０で、いずれかのノード上で事象が起こったことに応答して、もしくは事象が起こったときに、またはその両方で、その事象に関するデータがＲＡＦＴプロトコル・モジュール４６に記録される。１０１５で、１つのノードがＲＡＦＴリーダーとして選択される。一実施形態では、それぞれのノードが交替で、好ましくはラウンド・ロビン方式でＲＡＦＴリーダーになるが、他の選択プロセスも企図される。１０２０で、ＲＡＦＴリーダー・ノード内のデータベースが残りのノードと共有される。固定された期間もしくは動的期間においてノード上で事象が起こったことに応答して、またはノード上で事象が起こったときに、あるいは他の判定基準に従って、ＲＡＦＴリーダー内のデータベースを共有することができる。ＲＡＦＴプロトコルは当技術分野で知られており、ネットワークのノードにわたって状態機械を分散させる他の手段も企図される。

【００５０】

本発明は、統合化の可能な技術的詳細レベルにある、システム、方法もしくはコンピュータ・プログラム製品、またはこれらの組合せであることがある。このコンピュータ・プログラム製品は、本発明の態様をプロセッサに実行させるためのコンピュータ可読プログラム命令をその上に有するコンピュータ可読ストレージ媒体を含むことがある。

【００５１】

このコンピュータ可読ストレージ媒体は、命令実行デバイスが使用するための命令を保持および格納することができる有形のデバイスとすることができる。このコンピュータ可読ストレージ媒体は例えば、限定はされないが、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適当な組合せとすることができる。コンピュータ可読ストレージ媒体のより具体的な例の非網羅的なリストは、ポータブル・コンピュータ・ディスケット、ハード・ディスク、ランダム・アクセス・メモリ（ＲＡＭ）、リード・オンリー・メモリ（ＲＯＭ）、消去可能なプログラマブル・リード・オンリー・メモリ（ＥＰＲＯＭ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）、ポータブル・コンパクト・ディスク・リード・オンリー・メモリ（ＣＤ－ＲＯＭ）、デジタル・バーサタイル・ディスク（ＤＶＤ）、メモリ・スティック、フロッピー（Ｒ）・ディスク、機械的にコード化されたデバイス、例えばパンチカードまたはその上に命令が記録された溝の中の一段高くなった構造体、およびこれらの適当な組合せを含む。本明細書で使用されるコンピュータ可読ストレージ媒体を、それ自体が一過性の信号、例えば電波もしくは他の自由に伝搬する電磁波、ウェーブガイドもしくは他の伝送体内を伝搬する電磁波（例えば光ファイバ・ケーブル内を通る光パルス）、または電線を通して伝送される電気信号であると解釈すべきではない。

【００５２】

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、コンピュータ可読ストレージ媒体から対応するそれぞれのコンピューティング／処理デバイスにダウンロードすることができ、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、ワイド・エリア・ネットワークもしくは無線ネットワークまたはこれらの組合せを介して外部コンピュータもしくは外部ストレージ・デバイスにダウンロードすることができる。このネットワークは、銅伝送ケーブル、光伝送ファイバ、無線伝送、ルータ、ファイアウォール、スイッチ、ゲートウェイ・コンピュータもしくはエッジ・サーバ、またはこれらの組合せを含むことができる。それぞれのコンピューティング／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・インターフェースは、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、対応するそれぞれのコンピューティング／処理デバイス内のコンピュータ可読ストレージ媒体に格納するために転送する。

【００５３】

本発明の動作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）命令、機械命令、機械依存命令、マイクロコード、ファームウェア命令、状態設定データ、もしくは集積回路用のコンフィギュレーション・データであってもよく、またはＳｍａｌｌｔａｌｋ（Ｒ）、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種のプログラミング言語など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合せで書かれた、ソース・コードもしくはオブジェクト・コードであってもよい。このコンピュータ可読プログラム命令は、全体がユーザのコンピュータ上で実行されてもよく、一部がユーザのコンピュータ上で実行されてもよく、独立型ソフトウェア・パッケージとして実行されてもよく、一部がユーザのコンピュータ上で、一部がリモート・コンピュータ上で実行されてもよく、または全体がリモート・コンピュータもしくはリモート・サーバ上で実行されてもよい。上記の最後のシナリオでは、リモート・コンピュータが、ローカル・エリア・ネットワーク（ＬＡＮ）もしくはワイド・エリア・ネットワーク（ＷＡＮ）を含む任意のタイプ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もよく、またはこの接続が、外部コンピュータに対して（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）実施されてもよい。いくつかの実施形態では、本発明の態様を実行するために、例えばプログラム可能論理回路、フィールドプログラマブル・ゲート・アレイ（ＦＰＧＡ）またはプログラム可能論理アレイ（ＰＬＡ）を含む電子回路が、このコンピュータ可読プログラム命令の状態情報を利用してその

電子回路をパーソナライズすることにより、このコンピュータ可読プログラム命令を実行してもよい。

【００５４】

本明細書では、本発明の態様が、本発明の実施形態による方法、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もしくはブロック図またはその両方の図を参照して説明される。それらのフローチャート図もしくはブロック図またはその両方の図のそれぞれのブロック、およびそれらのフローチャート図もしくはブロック図またはその両方の図のブロックの組合せは、コンピュータ可読プログラム命令によって実施することができることが理解される。

【００５５】

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他のプログラム可能データ処理装置のプロセッサによって実行されるこれらの命令が、フローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックに指定された機能／操作を実施する手段を作り出すべく、コンピュータまたは他のプログラム可能データ処理装置のプロセッサに提供されて機械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さらに、その中に命令が格納されたコンピュータ可読ストレージ媒体が、フローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックに指定された機能／操作の態様を実施する命令を含む製品を含むように、コンピュータ可読ストレージ媒体に格納され、コンピュータ、プログラム可能データ処理装置もしくは他のデバイスまたはこれらの組合せに特定の方式で機能するように指示するものであってもよい。

【００５６】

これらのコンピュータ可読プログラム命令はさらに、コンピュータ、他のプログラム可能装置または他のデバイス上で実行されるこれらの命令が、フローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックに指定された機能／操作を実施するように、コンピュータによって実施されるプロセスを生み出すために、このコンピュータ、他のプログラム可能データ処理装置または他のデバイスにロードされ、コンピュータ、他のプログラム可能装置または他のデバイス上で一連の動作ステップを実行させるものであってもよい。

【００５７】

添付図中のフローチャートおよびブロック図は、本発明のさまざまな実施形態によるシステム、方法およびコンピュータ・プログラム製品の可能な実施態様のアーキテクチャ、機能および動作を示す。この点に関して、それらのフローチャートまたはブロック図のそれぞれのブロックは、指定された論理機能を実施する１つまたは複数の実行可能命令を含む、命令のモジュール、セグメントまたは部分を表すことがある。いくつかの代替実施態様では、ブロックに示された機能を、図に示された順序とは異なる順序で実行することができる。例えば、例えば、連続して示された２つのブロックが実際は実質的に同時に実行されること、または含まれる機能によってはそれらのブロックが時に逆の順序で実行されることもある。それらのブロック図もしくはフローチャート図またはその両方の図のそれぞれのブロック、ならびにそれらのブロック図もしくはフローチャート図またはその両方の図のブロックの組合せを、指定された機能もしくは操作を実行しまたは専用ハードウェアとコンピュータ命令の組合せを実行するハードウェアベースの専用システムによって実施することができることにも留意すべきである。

【００５８】

さらに、さまざまな実施形態によるシステムは、プロセッサ、プロセッサの機能ユニットまたはコンピュータ実施システム、およびこのシステム、プロセッサもしくは機能ユニットと統合された、またはこのシステム、プロセッサもしくは機能ユニットによって実行可能な、あるいはその両方である論地を含むことができ、この論理は、本明細書に記載されたプロセス・ステップのうちの１つまたは複数を実行するように構成されている。～と統合されているとは、一実施形態において、機能ユニットまたはプロセッサが、特定用途向け集積回路（ＡＳＩＣ）、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）

などのハードウェア論理として実装された論理を有することを意味する。機能ユニットまたはプロセッサによって実行可能は、一実施形態において、その論理が、ハードウェア論理；ファームウェア、オペレーティング・システムの部分、アプリケーション・プログラムの部分などのソフトウェア論理；などであること、または機能ユニットもしくはプロセッサによってアクセス可能であり、機能ユニットもしくはプロセッサによる実行時に機能ユニットもしくはプロセッサにある機能実行させるように構成された、ハードウェアもしくはソフトウェア論理のある組合せであることを意味する。ソフトウェア論理は、当技術分野で知られている任意のメモリ・タイプのローカル・メモリもしくはリモート・メモリまたはその両方に格納することができる。ソフトウェア・プロセッサ・モジュール、もしくはＡＳＩＣ、ＦＰＧＡ、中央処理ユニット（ＣＰＵ）、集積回路（ＩＣ）、グラフィクス処理ユニット（ＧＰＵ）などのハードウェア・プロセッサ、またはその両方など、当技術分野で知られている任意のプロセッサを使用することができる。

【００５９】

上記のシステムもしくは方法またはその両方のさまざまな特徴をさまざまに組み合わせて、以上の説明から、複数の組合せを生み出すことができることは明白である。サービスをオンデマンドで提供するために顧客のために展開されるサービスの形態で本発明の実施形態を提供することができることも理解される。

【００６０】

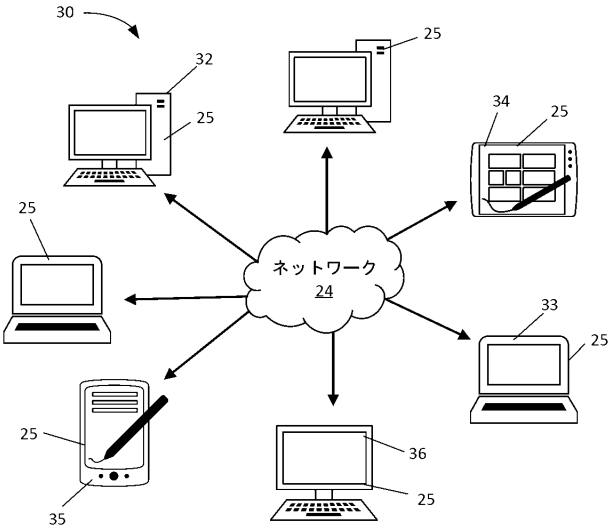
本明細書で使用されている用語は、特定の実施形態を記述することだけを目的としており、本発明を限定することを意図していない。本明細書において特に定義されていない限り、全ての用語には、本明細書から暗示される意味、ならびに当業者によって理解される意味もしくは辞書、学術論文などに定義された意味またはその両方を含む、その可能な最も幅広い解釈が与えられる。本明細書で使用されるとき、単数形「ａ」、「ａｎ」および「ｔｈｅ」は、文脈からそうでないことが明らかでない限り、複数形も含むことが意図されている。本明細書で使用されるとき、用語「備える（comprises）」もしくは「備える（comprising）」またはその両方は、明示された特徴、完全体（integer）、ステップ、動作、要素もしくは構成要素またはこれらの組合せの存在を指定するが、他の１つもしくは複数の特徴、完全体、ステップ、動作、要素、構成要素もしくはこれらのグループ、またはこれらの組合せの存在または追加を排除しないことも理解される。特許請求の範囲に記載された全ての要素の対応する構造体、材料、動作および等価物は、特許請求の範囲に記載された他の請求の要素と組み合わせて機能を実行するための一切の構造体、材料または動作を含むことが意図されている。本発明の説明は例示および説明のために示したものであり、それらの説明が網羅的であること、または開示された形態に限定されることは意図されていない。当業者には、本発明の範囲を逸脱しない多くの変更および変形が明らかとなろう。実施形態および用語は、本発明の原理および実際的用途を最もうまく説明するため、ならびに企図された特定の使用に適したさまざまな変更を有するさまざまな実施形態に関して他の当業者が本発明を理解することを可能にするために選択し、説明した。

【図面】

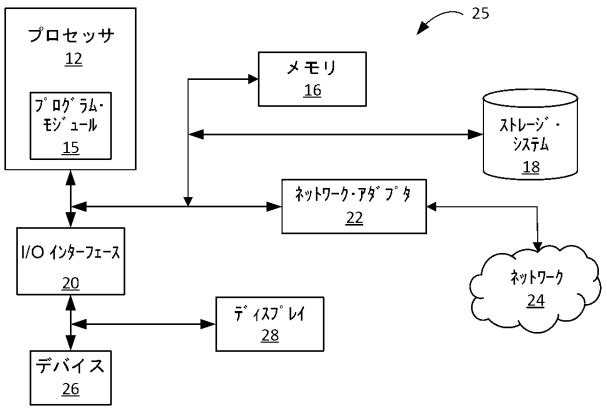
【図１】


ネットワーク
24
ノード 25
ノード 25

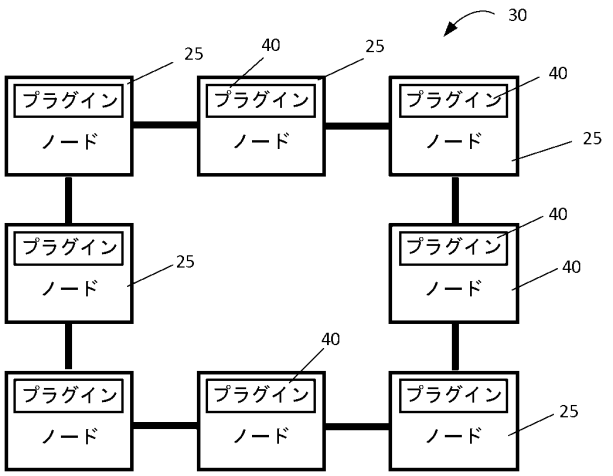
【図２】


30
32
25
25
34
25
25
ネットワーク
24
33
25
25
36
25
35

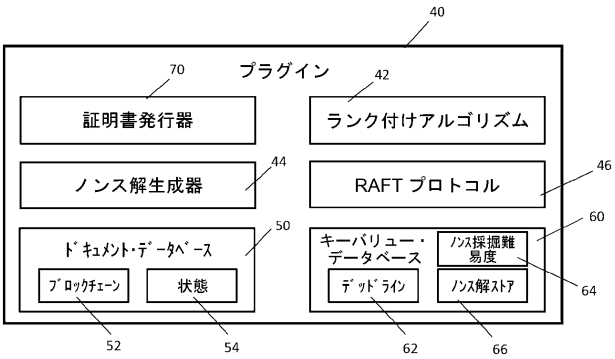
【図３】


25
プロセッサ
12
ﾌﾟﾛｸﾞﾗﾑ・ﾓｼﾞｭｰﾙ
15
メモリ
16
ｽﾄﾚｰｼﾞ・ｼｽﾃﾑ
18
ﾈｯﾄﾜｰｸ･ｱﾀﾞﾌﾟﾀ
22
I/O ｲﾝﾀｰﾌｪｰｽ
20
ﾈｯﾄﾜｰｸ
24
ﾃﾞｨｽﾌﾟﾚｲ
28
デバイス
26

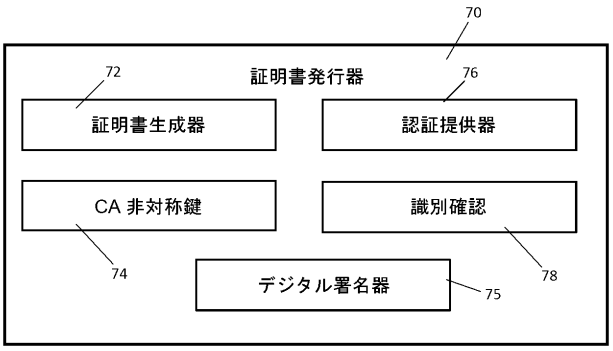
【図４】


30
25
40
25
プラグイン
ノード
プラグイン
ノード
プラグイン
ノード
40
25
プラグイン
ノード
25
プラグイン
ノード
40
40
40
プラグイン
ノード
プラグイン
ノード
プラグイン
ノード
25

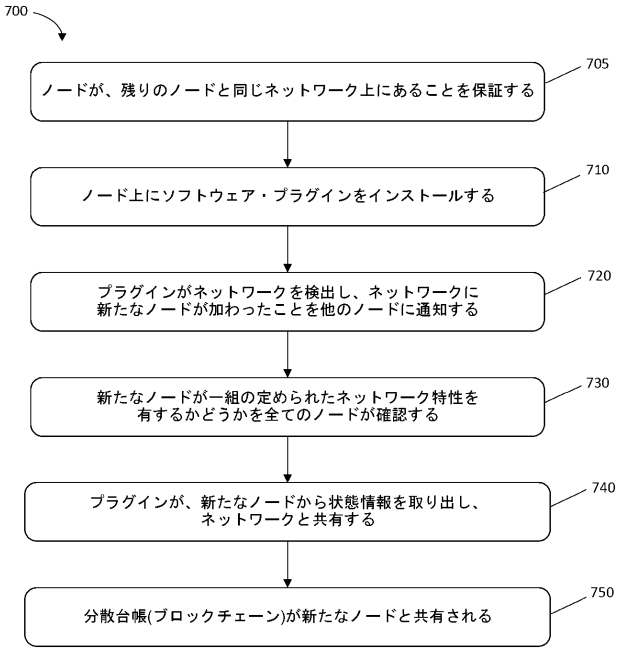
【図５】


40
プラグイン
70
証明書発行器
42
ランク付けアルゴリズム
44
ノンス解生成器
46
RAFT プロトコル
50
ﾄﾞｷｭﾒﾝﾄ･ﾃﾞｰﾀﾍﾞｰｽ
ﾌﾞﾛｯｸﾁｪｰﾝ
状態
60
キーバリュー・データベース
ﾉﾝｽ採掘難易度
ﾃﾞｯﾄﾞﾗｲﾝ
ﾉﾝｽ解ｽﾄｱ
64
52
54
62
66

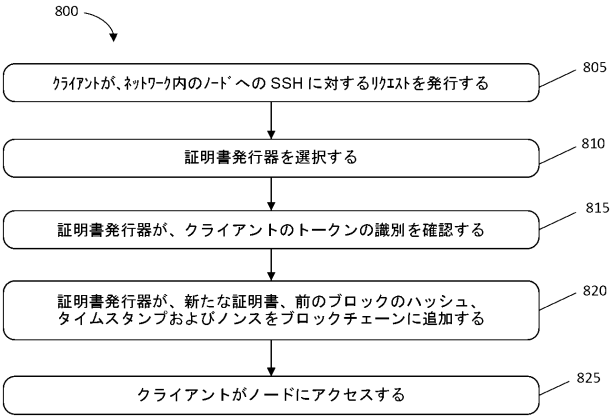
【図６】


70
証明書発行器
72
証明書生成器
76
認証提供器
CA 非対称鍵
識別確認
74
78
デジタル署名器
75

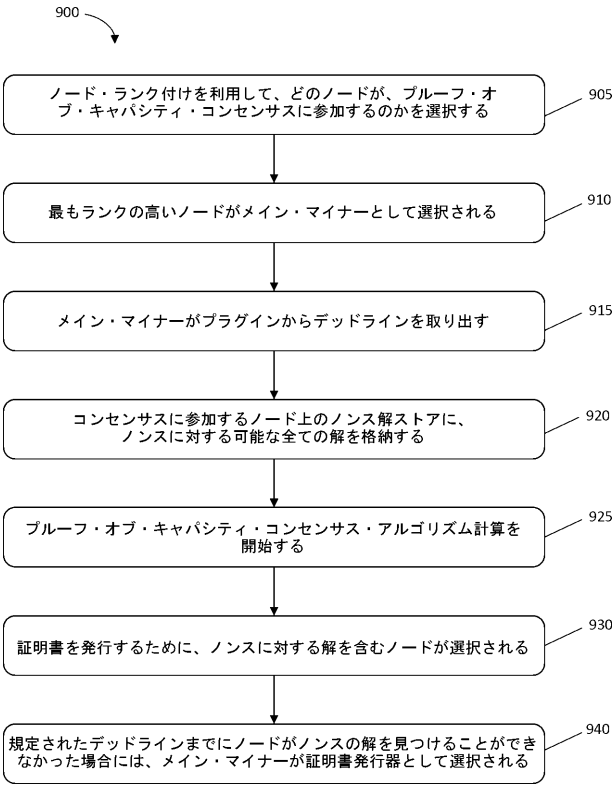
【図７】


700
ノードが、残りのノードと同じネットワーク上にあることを保証する
705
ノード上にソフトウェア・プラグインをインストールする
710
プラグインがネットワークを検出し、ネットワークに新たなノードが加わったことを他のノードに通知する
720
新たなノードが一組の定められたネットワーク特性を有するかどうかを全てのノードが確認する
730
プラグインが、新たなノードから状態情報を取り出し、ネットワークと共有する
740
分散台帳(ブロックチェーン)が新たなノードと共有される
750

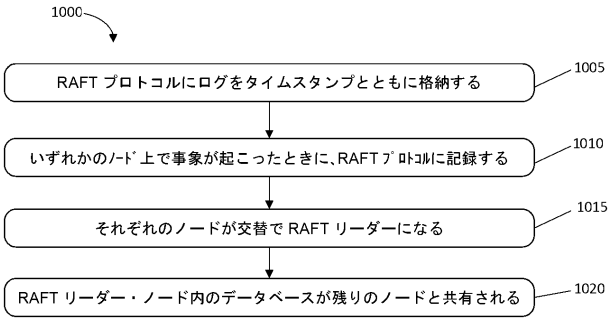
【図８】


800
ｸﾗｲｱﾝﾄが、ﾈｯﾄﾜｰｸ内のﾉｰﾄﾞへの SSH に対するﾘｸｴｽﾄを発行する
805
証明書発行器を選択する
810
証明書発行器が、クライアントのトークンの識別を確認する
815
証明書発行器が、新たな証明書、前のブロックのハッシュ、タイムスタンプおよびノンスをブロックチェーンに追加する
820
クライアントがノードにアクセスする
825

【図９】


900
ノード・ランク付けを利用して、どのノードが、プルーフ・オブ・キャパシティ・コンセンサスに参加するのかを選択する
905
最もランクの高いノードがメイン・マイナーとして選択される
910
メイン・マイナーがプラグインからデッドラインを取り出す
915
コンセンサスに参加するノード上のノンス解ストアに、ノンスに対する可能な全ての解を格納する
920
プルーフ・オブ・キャパシティ・コンセンサス・アルゴリズム計算を開始する
925
証明書を発行するために、ノンスに対する解を含むノードが選択される
930
規定されたデッドラインまでにノードがノンスの解を見つけることができなかった場合には、メイン・マイナーが証明書発行器として選択される
940

【図１０】


1000
RAFT プロトコルにログをタイムスタンプとともに格納する
1005
いずれかのﾉｰﾄﾞ上で事象が起こったときに、RAFTﾌﾟﾛﾄｺﾙに記録する
1010
それぞれのノードが交替で RAFT リーダーになる
1015
RAFT リーダー・ノード内のデータベースが残りのノードと共有される
1020

【手続補正書】
【提出日】令和5年12月27日(2023.12.27)
【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】
コンピューティング・ノードのネットワークへのアクセスを提供するコンピュータ実施方法であって、前記方法が、
クライアントによって、前記ネットワーク内のホスト・ノードへのアクセスをリクエストすること、
デジタル証明書発行器を選択すること、
前記デジタル証明書発行器によって、クライアントのトークンの識別を確認すること、
前記デジタル証明書発行器によって、分散台帳にノンスを追加すること、および
前記ネットワーク内の前記ホスト・ノードへのアクセスを前記クライアントに許可すること
を含むコンピュータ実施方法。
【請求項２】
前記ネットワーク内の前記コンピューティング・ノードをランク付けすること、および前記ネットワーク内の前記コンピューティング・ノードのランクに従って、前記ノンスに対する解を見つけるプルーフ・オブ・キャパシティ・コンセンサスに参加する１つまたは複数のコンピューティング・ノードを選択することをさらに含む、請求項１に記載のコンピュータ実施方法。
【請求項３】
前記ネットワーク内の前記コンピューティング・ノードをランク付けすることが、前記コンピューティング・ノードの使用されていないＣＰＵ容量に基づく、請求項２に記載のコンピュータ実施方法。
【請求項４】
最も高いランクを有する前記コンピューティング・ノードをメイン・マイナーとして選択すること、および前記メイン・マイナーによって、前記メイン・マイナー上にインストールされたプラグインからデッドラインを取り出すことをさらに含む、請求項２に記載のコンピュータ実施方法。
【請求項５】
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノード上のノンス解ストアに、前記ノンスに対する可能な全ての解を格納することをさらに含む、請求項４に記載のコンピュータ実施方法。
【請求項６】
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノードによって、前記ノンスに対する解を見つける前記プルーフ・オブ・キャパシティ・コンセンサスを計算することをさらに含む、請求項５に記載のコンピュータ実施方法。
【請求項７】
前記ノンスに対する前記解を含む前記ノードを、前記デジタル証明書発行器であるとして選択することをさらに含む、請求項６に記載のコンピュータ実施方法。
【請求項８】
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノードによって、前記ノンスに対する解を見つける前記プルーフ・オブ・キャパシティ・コンセンサスを計算すること、および

前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された前記コンピューティング・ノードがいずれも、前記デッドラインまでに前記ノンスに対する解を見つけなかったことに応答して、前記メイン・マイナーを前記デジタル証明書発行器として選択すること
をさらに含む、請求項５に記載のコンピュータ実施方法。
【請求項９】
前記ネットワークに新たなホスト・ノードを追加することをさらに含み、前記ネットワークに新たなホスト・ノードを追加することが、
前記ネットワーク上の全ての前記コンピューティング・ノードによって、前記新たなホスト・ノードが一組の定められたネットワーク特性を有するかどうかを判定すること、
前記新たなホスト・ノードが一組の定められたネットワーク特性を有すると判定したことに応答して、前記新たなホスト・ノードから状態情報を取り出すこと、および
前記状態情報を、前記ネットワーク上の全ての前記コンピューティング・ノードと共有すること
を含む、請求項１に記載のコンピュータ実施方法。
【請求項１０】
前記ネットワークに新たなホスト・ノードを追加することが、前記分散台帳を前記新たなホスト・ノードと共有することをさらに含む、請求項９に記載のコンピュータ実施方法。
【請求項１１】
前記ネットワークに新たなホスト・ノードを追加することが、
前記新たなホスト・ノードが、前記コンピューティング・ノードと同じネットワークに追加されることを保証すること、
前記新たなホスト・ノード上にプラグインをインストールすること、
前記プラグインによって前記ネットワークを検出すること、および
前記ネットワークに新たなホスト・ノードが加わったことを、前記ネットワーク上の全ての前記コンピューティング・ノードに通知すること
をさらに含む、請求項１０に記載のコンピュータ実施方法。
【請求項１２】
前記分散台帳を前記新たなホスト・ノードと共有することが、ＲＡＦＴプロトコルを利用することを含み、ＲＡＦＴリーダー・ノード内の前記分散台帳を含むデータベースが、前記新たなホスト・ノードと共有される、請求項１０に記載のコンピュータ実施方法。
【請求項１３】
コンピュータ・プログラムであって、請求項１ないし１２のいずれか１項に記載の方法をコンピュータに実行させるための、コンピュータ・プログラム。
【請求項１４】
請求項１３に記載のコンピュータ・プログラムを記録した、非一過性コンピュータ可読媒体。
【請求項１５】
コンピューティング・ノードのネットワークを構成するためのコンピュータ実施システムであって、
プログラム命令を格納したメモリ・ストレージ・デバイスと、
前記コンピューティング・ノードのネットワークを構成するための前記プログラム命令を実行するための回路および論理を有するハードウェア・プロセッサと
を備え、前記ハードウェア・プロセッサが、前記メモリ・ストレージ・デバイスに結合されており、前記プログラム命令を実行したことに応答して、
クライアントによって、前記コンピューティング・ノードのネットワーク内のホスト・ノードへのリモート・アクセスをリクエストすること、
デジタル証明書発行器としてコンピューティング・ノードを選択すること、
前記デジタル証明書発行器によって、クライアントのトークンの識別を確認すること、

前記証明書発行器によって、分散台帳にノンスを追加すること、および
前記ネットワーク内の前記ホスト・ノードへのアクセスを前記クライアントに許可すること
を実行するように構成されている、コンピュータ実施システム。
【請求項１６】
使用されていないＣＰＵ容量の量に従って、前記ネットワーク内の前記コンピューティング・ノードをランク付けすること、
前記使用されていないＣＰＵ容量の量の前記ランク付けに基づいて、前記ノンスに対する解を見つけるプルーフ・オブ・キャパシティ・コンセンサスに参加する複数のコンピューティング・ノードを選択すること、
前記ノンスに対する解を見つける前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記複数のコンピューティング・ノードによって、前記プルーフ・オブ・キャパシティ・コンセンサスを計算すること、および
前記ノンスに対する前記解を含む前記ノードを、前記デジタル証明書発行器であるとして選択すること
を実行するようにさらに構成されている、請求項１５に記載のコンピュータ実施システム。
【請求項１７】
最も高いランクを有する前記コンピューティング・ノードをメイン・マイナーとして選択すること、
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された全ての前記コンピューティング・ノードによって、前記ノンスに対する解を見つける前記プルーフ・オブ・キャパシティ・コンセンサスを計算すること、および
前記プルーフ・オブ・キャパシティ・コンセンサスに参加するように選択された前記コンピューティング・ノードがいずれも、デッドラインまでに前記ノンスに対する解を見つけなかったことに応答して、前記メイン・マイナーを前記デジタル証明書発行器として選択すること
を実行するようにさらに構成されている、請求項１６に記載のコンピュータ実施システム。
【請求項１８】
前記ネットワークに新たなホスト・ノードを追加するようにさらに構成されており、前記ネットワークに新たなホスト・ノードを追加することが、
前記ネットワーク上の全ての前記コンピューティング・ノードによって、前記新たなホスト・ノードが一組の定められたネットワーク特性を有するかどうかを判定すること、および
前記新たなホスト・ノードが一組の定められたネットワーク特性を有すると判定したことに応答して、前記新たなホスト・ノードから状態情報を取り出すこと、および
前記状態情報を、前記ネットワーク上の全ての前記コンピューティング・ノードと共有すること
を実行するように前記システムを構成することを含む、請求項１５に記載のコンピュータ実施システム。
【請求項１９】
前記ネットワークに新たなホスト・ノードを追加することがさらに、
前記新たなホスト・ノードが他のコンピューティング・ノードと同じネットワークに追加されるかどうかを判定すること、
前記新たなホスト・ノードが他のコンピューティング・ノードと同じネットワークに追加されると判定したことに応答して、前記新たなホスト・ノード上にプラグインをインストールすること、
前記プラグインによって前記ネットワークを検出すること、
前記ネットワークに新たなホスト・ノードが加わったことを、前記ネットワーク上の全

ての前記コンピューティング・ノードに通知すること、および
前記分散台帳を前記新たなホスト・ノードと共有すること
を実行するように前記システムを構成することを含み、前記プラグインが、証明書発行器モジュール、ランク付けアルゴリズム・モジュール、ノンス生成器、前記分散台帳および状態情報を含むドキュメント・データベース、ならびにキーバリュー・データベースを含む、
請求項１８に記載のコンピュータ実施システム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/060366

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/40 G06Q20/38 G06Q20/40 H04L9/32 H04L9/00
H04L67/1097 G06F21/31 G06F21/33 G06F21/41
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)
H04L G07G G06Q G06F

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.
Y	US 2021/083882 A1 (VENABLE SR JEFFREY C [US]) 18 March 2021 (2021-03-18) paragraph [0001] - paragraph [0004] paragraph [0014] - paragraph [0086]; figures 1,3,5	1-25
Y	US 2019/036906 A1 (BIYANI AMIT [US] ET AL) 31 January 2019 (2019-01-31) paragraph [0049] paragraph [0059] - paragraph [0061]	1-25

-/--

[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 August 2022	10/08/2022

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

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/060366

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Hasib Anwar: "Consensus Algorithms: The Root Of The Blockchain Technology", , 25 August 2018 (2018-08-25), XP055598924, Retrieved from the Internet: URL:https://101blockchains.com/consensus-algorithms-blockchain [retrieved on 2019-06-24] page 19 - page 21	2-12, 14-20, 22-25
Y	US 2021/073285 A1 (HUNTER EDWARD [US]) 11 March 2021 (2021-03-11) paragraph [0079] paragraph [0196] paragraph [0267]	2-20, 22-25

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2022/060366

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2021083882 A1	18-03-2021	NONE	
US 2019036906 A1	31-01-2019	US 2019036906 A1	31-01-2019
		US 2021160233 A1	27-05-2021
US 2021073285 A1	11-03-2021	BR 112022003950 A2	24-05-2022
		CA 3150253 A1	11-03-2021
		CA 3150262 A1	11-03-2021
		CA 3150320 A1	11-03-2021
		CA 3150324 A1	11-03-2021
		EP 4010814 A1	15-06-2022
		EP 4010815 A1	15-06-2022
		EP 4010816 A1	15-06-2022
		EP 4010817 A1	15-06-2022
		US 2021073282 A1	11-03-2021
		US 2021073284 A1	11-03-2021
		US 2021073285 A1	11-03-2021
		WO 2021046540 A1	11-03-2021
		WO 2021046541 A1	11-03-2021
		WO 2021046551 A1	11-03-2021
		WO 2021046552 A1	11-03-2021

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

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,IT,JM,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,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

(74)代理人　100120710
弁理士　片岡 忠彦

(72)発明者　オルイェミ、オルワニフェミ
カナダ エル３アール ９ゼット７ オンタリオ州マークハム スティールス・アベニュー・イースト３６００

(72)発明者　ラン、チュアン
アメリカ合衆国２７７０９－２１９５ ノースカロライナ州 リサーチ・トライアングル・パーク イースト・コーンウォリス・ロード３０３９

(72)発明者　モッヴァ、ヴァムシー
アメリカ合衆国２７７０９－２１９５ ノースカロライナ州 リサーチ・トライアングル・パーク イースト・コーンウォリス・ロード３０３９

(72)発明者　シャリフ、エー ジャイラニ
アメリカ合衆国１３７６０ ニューヨーク州エンディコット ビルディング０４０－３ デパートメントアイキュー０エイ