(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2023-501152
(P2023-501152A)
(43)公表日　令和5年1月18日(2023.1.18)

(51)国際特許分類　FI
H04L 9/32 (2006.01)　H04L 9/32 200Z
G06F 21/62 (2013.01)　G06F 21/62 318

審査請求　未請求　予備審査請求　未請求　（全49頁）

(21)出願番号　特願2022-524730(P2022-524730)
(86)(22)出願日　令和2年10月22日(2020.10.22)
(85)翻訳文提出日　令和4年4月26日(2022.4.26)
(86)国際出願番号　PCT/IB2020/059927
(87)国際公開番号　WO2021/090100
(87)国際公開日　令和3年5月14日(2021.5.14)
(31)優先権主張番号　16/673,911
(32)優先日　令和1年11月4日(2019.11.4)
(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】　許可型ブロックチェーンのためのランダムなノード選択

(57)【要約】
例示的な動作は、ブロックチェーンに格納されたデータ・ブロックのブロック・ハッシュを取り出すことと、ブロック・ハッシュの値に基づいて、署名者になるべきピア組織のサブセットをブロックチェーンのブロックチェーン・ネットワークからランダムに決定することと、ブロックチェーン格納要求を、クライアントから、ランダムに決定された署名者ピア組織のサブセットに送信することと、ランダムに決定された署名者ピア組織のサブセットからのシミュレートされた応答を、格納要求提案に収集することとのうちの１つまたは複数を含んでよい。

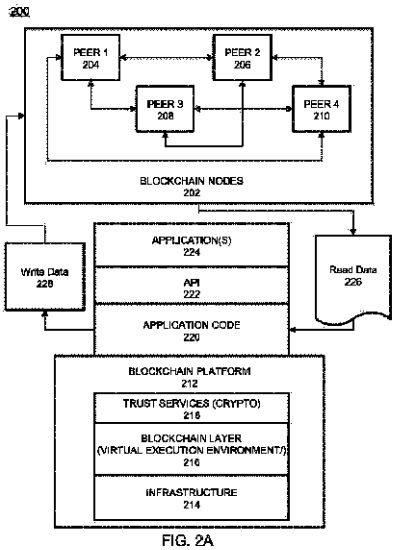


FIG. 2A

【特許請求の範囲】
【請求項１】
ブロックチェーンに格納されたデータ・ブロックのブロック・ハッシュを取り出すことと、前記ブロック・ハッシュの値に基づいて、ピア組織のサブセットを前記ブロックチェーンのブロックチェーン・ネットワークからランダムに決定することと、ブロックチェーン格納要求を、クライアントから、前記ランダムに決定された署名者ピア組織のサブセットに送信することとを実行するように構成されたプロセッサと、
前記ランダムに決定された署名者ピア組織のサブセットからのシミュレートされた応答を、格納要求提案に収集するように構成されたネットワーク・インターフェイスとを備える、装置。
【請求項２】
前記プロセッサが、前記ブロック・ハッシュを乱数に変換することと、前記乱数を複数のビット・セグメントに分割することと、前記複数のビット・セグメントに基づいて前記ピア組織のサブセットを識別することとを実行するように構成される、請求項１に記載の装置。
【請求項３】
前記プロセッサが、前記ブロックチェーン・ネットワークに含まれているピア組織の数に基づいて、前記複数のピア組織のうちの各ピア組織に一意の識別子を割り当てることと、前記複数のビット・セグメントからのビット・セグメントを１０進数値に変換することと、前記ビット・セグメントの前記１０進数値を前記ピア組織のうちの１つの一意の識別子にマッピングすることとを実行するように構成される、請求項２に記載の装置。
【請求項４】
前記プロセッサが、前記ブロックチェーン・ネットワークに含まれているピア組織の数に基づいて前記ビット・セグメントのサイズを選択するようにさらに構成される、請求項２に記載の装置。
【請求項５】
前記プロセッサが、前記ブロックチェーン上の最新のブロックのサブセットを識別するブロック間隔値を決定するようにさらに構成され、前記サブセットから前記ブロック・ハッシュが取り出され得る、請求項１に記載の装置。
【請求項６】
前記プロセッサが、前記ブロック間隔値によって識別された前記最新のブロックのサブセット内のブロックを選択することと、前記ブロック間隔値によって識別された前記最新のブロックのサブセット内の前記選択されたブロックから前記ブロック・ハッシュを取り出すこととを実行するように構成される、請求項５に記載の装置。
【請求項７】
前記プロセッサが、前記ブロックチェーンの現在の高さおよび前記ブロック間隔値に基づいて完全性値を生成することと、前記完全性値を前記格納要求提案内に格納することとを実行するようにさらに構成される、請求項６に記載の装置。
【請求項８】
前記ネットワーク・インターフェイスが、前記ランダムに決定された署名者ピア組織のサブセットから前記収集された、シミュレートされた応答を含んでいる前記格納要求提案を、前記ブロックチェーンの順序付けノード・サービスに送信するようにさらに構成される、請求項１に記載の装置。
【請求項９】
ブロックチェーンに格納されたデータ・ブロックのブロック・ハッシュを取り出すことと、
前記ブロック・ハッシュの値に基づいて、署名者になるべきピア組織のサブセットを前記ブロックチェーンのブロックチェーン・ネットワークからランダムに決定することと、
ブロックチェーン格納要求を、クライアントから前記ランダムに決定された署名者ピア組織のサブセットに送信することと、

前記ランダムに決定された署名者ピア組織のサブセットからのシミュレートされた応答を、格納要求提案に収集することとを含む、方法。
【請求項１０】
前記ランダムに決定することが、前記ブロック・ハッシュを乱数に変換することと、前記乱数を複数のビット・セグメントに分割することと、前記複数のビット・セグメントのうちの１つまたは複数に基づいて前記ピア組織のサブセットを識別することとを含む、請求項９に記載の方法。
【請求項１１】
前記識別することが、前記ブロックチェーン・ネットワークに含まれているピア・ノードの数に基づいて、前記複数のピア・ノードのうちの各ピア組織に一意の識別子を割り当てることと、前記複数のビット・セグメントからのビット・セグメントを１０進数値に変換することと、前記ビット・セグメントの前記１０進数値を前記ピア組織のうちの１つの一意の識別子にマッピングすることとを含む、請求項１０に記載の方法。
【請求項１２】
前記ブロックチェーン・ネットワークに含まれているピア組織の数に基づいて前記ビット・セグメントのサイズを選択することをさらに含む、請求項１０に記載の方法。
【請求項１３】
前記ブロックチェーン上の最新のブロックのサブセットを識別するブロック間隔値を決定することをさらに含み、前記サブセットから前記ブロック・ハッシュが取り出され得る、請求項９に記載の方法。
【請求項１４】
前記ブロック間隔値によって識別された前記最新のブロックのサブセット内のブロックを選択することと、前記ブロック間隔値によって識別された前記ブロックのサブセット内の前記選択されたブロックから前記ブロック・ハッシュを取り出すこととをさらに含む、請求項１３に記載の方法。
【請求項１５】
前記ブロックチェーンの現在の高さおよび前記ブロック間隔値に基づいて完全性値を生成することと、前記完全性値を前記格納要求提案内に格納することとをさらに含む、請求項１４に記載の方法。
【請求項１６】
前記ランダムに決定された署名者ピア・ノードのサブセットから前記収集された、シミュレートされた応答を含んでいる前記格納要求提案を、前記ブロックチェーンの順序付けノード・サービスに送信することをさらに含む、請求項９に記載の方法。
【請求項１７】
命令を含んでいる非一過性コンピュータ可読媒体であって、前記命令が、プロセッサによって読み取られたときに、前記プロセッサに、
ブロックチェーンに格納されたデータ・ブロックのブロック・ハッシュを取り出すことと、
前記ブロック・ハッシュの値に基づいて、署名者になるべきピア組織のサブセットを前記ブロックチェーンのブロックチェーン・ネットワークからランダムに決定することと、
ブロックチェーン格納要求を、クライアントから前記ランダムに決定された署名者ピア組織のサブセットに送信することと、
前記ランダムに決定された署名者ピア組織のサブセットからのシミュレートされた応答を、格納要求提案に収集することとを含む方法を実行させる、非一過性コンピュータ可読媒体。
【請求項１８】
前記ランダムに決定することが、前記ブロック・ハッシュを乱数に変換することと、前記乱数を複数のビット・セグメントに分割することと、前記複数のビット・セグメントのうちの１つまたは複数に基づいて前記ピア組織のサブセットを識別することとを含む、請求項１７に記載の非一過性コンピュータ可読媒体。

【請求項１９】
前記識別することが、前記ブロックチェーン・ネットワークに含まれているピア組織の数に基づいて、前記複数のピア・ノードのうちの各ピア組織に一意の識別子を割り当てることと、前記複数のビット・セグメントからのビット・セグメントを１０進数値に変換することと、前記ビット・セグメントの前記１０進数値を前記ピア組織のうちの１つの一意の識別子にマッピングすることとを含む、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】
前記ブロックチェーン・ネットワークに含まれているピア組織の数に基づいて前記ビット・セグメントのサイズを選択することをさらに含む、請求項１８に記載の非一過性コンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、一般に、データをブロックチェーンに格納することに関連しており、より詳細には、ブロックチェーン・データに基づいて署名を実行するために、許可型ブロックチェーンからピア・ノードのサブセットをランダムに選択するプロセスに関連している。
【背景技術】
【０００２】
集中データベースは、データを単一のデータベース（例えば、データベース・サーバ）に格納して一か所で維持する。この位置は、多くの場合、中央コンピュータであり、例えば、デスクトップの中央処理装置（ＣＰＵ：central processing unit）、サーバＣＰＵ、またはメインフレーム・コンピュータである。集中データベースに格納された情報は、通常、複数の異なる位置からアクセス可能である。複数のユーザまたはクライアント・ワークステーションが、例えばクライアント／サーバ構成に基づいて、集中データベースを使用して同時に作業することができる。集中データベースは、単一の位置のため、特にセキュリティの目的で、管理、維持、および制御するのが容易である。集中データベース内では、すべてのデータの単一の格納場所が、特定のデータのセットのみが１つの一次記録を含むということも意味するため、データの冗長性が最小限に抑えられる。
【０００３】
しかし、集中データベースは重大な欠点を抱えている。例えば、集中データベースには、単一障害点が存在する。特に、耐故障性が考慮されておらず、ハードウェア故障（例えば、ハードウェア、ファームウェア、またはソフトウェア、あるいはその組み合わせの故障）が発生した場合、データベース内のすべてのデータが失われ、すべてのユーザの作業が中断される。加えて、集中データベースは、ネットワークの接続性に大きく依存している。その結果、接続の速度が低下すると、各データベース・アクセスに必要な時間が増加する。別の欠点は、単一の位置に起因する、集中データベースの通信量が増えた場合のボトルネックの発生である。さらに、集中データベースは、データの１つのコピーのみがデータベースによって維持されるため、データへの制限されたアクセスを提供する。その結果、格納されたデータを上書きする重大な問題またはリスクを引き起こさずに、複数のデバイスが同時にデータの同じ部分にアクセスすることができない。さらに、データベース・ストレージ・システムがデータの冗長性を最小限しか持たないか、または全く持たないため、突然失われたデータを、手動の操作によってバックアップ・ストレージから取り出す以外に、取り出すことが非常に困難である。
【０００４】
ブロックチェーンの一種は、実行、順序、および妥当性確認の枠組みに従う許可型ブロックチェーンである。この環境では、クライアントのトランザクションが、ピア（署名者ノード）のサブセットによって投機的に実行され、これらのピアが、シミュレートされた実行の結果をクライアントに返送し、クライアントはこの結果を、ブロックチェーン上の格納ためのトランザクション提案への入力として使用する。トランザクションは、順序付

けられてからブロックに追加されてよく、このブロックが、ピア・ノードによってブロックチェーン台帳にコミットされる。ここで、コミット・ノードは、署名者ノードの署名を検証し、トランザクションを再度実行してもよい。ブロックチェーン・ネットワークが拡大するにつれて、トランザクションに署名するために必要なノードの数も同様に増大することがある。その結果、セキュリティの向上に対する性能におけるトレードオフが存在する。特に、署名するのに必要なノード／署名の数が多いほど、トランザクションのセキュリティが高いということを意味する。しかしそれは、コミット時に検証するべき、より多くの署名が存在するということも意味する。そのため、これらの欠点および制限を克服する解決策が必要とされている。

【発明の概要】

【０００５】

１つの実施形態例は、ブロックチェーンに格納されたデータ・ブロックのブロック・ハッシュを取り出すことと、ブロック・ハッシュの値に基づいて、署名者になるべきピア組織のサブセットをブロックチェーンのブロックチェーン・ネットワークからランダムに決定することと、ブロックチェーン格納要求を、クライアントから、ランダムに決定された署名者組織のサブセットに送信することとのうちの１つまたは複数を実行するように構成されたプロセッサと、ランダムに決定された署名者組織のサブセットからのシミュレートされた応答を、格納要求提案（storage request proposal）に収集するように構成されたネットワーク・インターフェイスとのうちの１つまたは複数を含むシステムを提供する。

【０００６】

別の実施形態例は、ブロックチェーンに格納されたデータ・ブロックのブロック・ハッシュを取り出すことと、ブロック・ハッシュの値に基づいて、署名者になるべきピア組織のサブセットをブロックチェーンのブロックチェーン・ネットワークからランダムに決定することと、ブロックチェーン格納要求を、クライアントから、ランダムに決定された署名者ピア組織のサブセットに送信することと、ランダムに決定された署名者ピア組織のサブセットからのシミュレートされた応答を、格納要求提案に収集することとのうちの１つまたは複数を含む方法を提供する。

【０００７】

さらに別の実施形態例は、命令を含んでいる非一過性コンピュータ可読媒体を提供し、これらの命令は、プロセッサによって読み取られたときに、プロセッサに、ブロックチェーンに格納されたデータ・ブロックのブロック・ハッシュを取り出すことと、ブロック・ハッシュの値に基づいて、署名者になるべきピア組織のサブセットをブロックチェーンのブロックチェーン・ネットワークからランダムに決定することと、ブロックチェーン格納要求を、クライアントから、ランダムに決定された署名者ピア組織のサブセットに送信することと、ランダムに決定された署名者ピア組織のサブセットからのシミュレートされた応答を、格納要求提案に収集することとのうちの１つまたは複数を実行させる。

【図面の簡単な説明】

【０００８】

【図１】実施形態例に従って、署名のためのピア組織をランダムに選択するためのコンピューティング環境を示す図である。

【図２Ａ】実施形態例に従って、ブロックチェーン・アーキテクチャ構成を示す図である。

【図２Ｂ】実施形態例に従って、ブロックチェーン・トランザクション・フローを示す図である。

【図３Ａ】実施形態例に従って、許可型ブロックチェーン・ネットワークを示す図である。

【図３Ｂ】実施形態例に従って、別の許可型ブロックチェーン・ネットワークを示す図である。

【図３Ｃ】実施形態例に従って、許可なしブロックチェーン・ネットワークを示す図であ

る。
【図４Ａ】実施形態例に従って、署名者組織をランダムに選択することにおいて使用するために、ブロックチェーンからハッシュを取り出すプロセスを示す図である。
【図４Ｂ】実施形態例に従って、一意の識別子をブロックチェーン・ネットワーク内の組織に割り当てるプロセスを示す図である。
【図４Ｃ】実施形態例に従って、ハッシュをセグメントに分割し、セグメントに基づいて署名者組織を識別するプロセスを示す図である。
【図５】実施形態例に従って、署名者になるべきピア組織をランダムに選択する方法を示す図である。
【図６Ａ】実施形態例に従って、本明細書に記載された１つまたは複数の動作を実行するように構成された例示的なシステムを示す図である。
【図６Ｂ】実施形態例に従って、本明細書に記載された１つまたは複数の動作を実行するように構成された別の例示的なシステムを示す図である。
【図６Ｃ】実施形態例に従って、スマート・コントラクトを利用するように構成された、さらに別の例示的なシステムを示す図である。
【図６Ｄ】実施形態例に従って、ブロックチェーンを利用するように構成された、さらに別の例示的なシステムを示す図である。
【図７Ａ】実施形態例に従って、分散型台帳に追加されている新しいブロックのプロセスを示す図である。
【図７Ｂ】実施形態例に従って、新しいデータ・ブロックのデータの内容を示す図である。
【図７Ｃ】実施形態例に従って、デジタル・コンテンツのためのブロックチェーンを示す図である。
【図７Ｄ】実施形態例に従って、ブロックチェーン内のブロックの構造を表すことができるブロックを示す図である。
【図８Ａ】実施形態例に従って、機械学習（人工知能）データを格納する例示的なブロックチェーンを示す図である。
【図８Ｂ】実施形態例に従って、例示的な量子セキュアなブロックチェーンを示す図である。
【図９】実施形態例のうちの１つまたは複数をサポートする例示的なシステムを示す図である。

【発明を実施するための形態】
【０００９】
本明細書の図において一般的に説明され、示されているように、本明細書のコンポーネントが、多種多様な異なる構成で配置および設計されてよいということが、容易に理解されるであろう。したがって、添付の図において表された方法、装置、非一過性コンピュータ可読媒体、およびシステムのうちの少なくとも１つの実施形態に関する以下の詳細な説明は、請求されている本出願の範囲を制限するよう意図されておらず、単に選択された実施形態を代表している。
【００１０】
本明細書全体を通して説明された特徴、構造、または特性は、１つまたは複数の実施形態において、任意の適切な方法で組み合わせられるか、または削除されてよい。例えば、語句「実施形態例」、「一部の実施形態」、またはその他の同様の言葉の使用は、本明細書全体を通じて、実施形態に関連して説明された特定の特徴、構造、または特性が少なくとも１つの実施形態に含まれてよいということを指している。したがって、語句「実施形態例」、「一部の実施形態において」、「その他の実施形態において」、またはその他の同様の言葉の出現は、本明細書全体を通じて、必ずしもすべてが実施形態の同じグループを指しておらず、説明された特徴、構造、または特性は、１つまたは複数の実施形態において、任意の適切な方法で組み合わせられるか、または削除されてよい。さらに、各図では、要素間の任意の接続は、示された接続が一方向または双方向の矢印である場合でも、

一方向通信または双方向通信あるいはその両方を許可することができる。また、図面に示された任意のデバイスは、異なるデバイスであることができる。例えば、情報を送信しているモバイル・デバイスが示された場合、その情報を送信するために、有線デバイスも使用され得る。

【００１１】

加えて、「メッセージ」という用語が実施形態の説明において使用されていることがあるが、本出願は、多くの種類のネットワークおよびデータに適用されてよい。さらに、特定の種類の接続、メッセージ、および信号伝達が実施形態例において示されることがあるが、本出願は、特定の種類の接続、メッセージ、および信号伝達に限定されない。

【００１２】

実施形態例は、ランダム化された選択プロセスを対象にする方法、システム、コンポーネント、非一過性コンピュータ可読媒体、デバイス、またはネットワーク、あるいはその組み合わせを、許可型ブロックチェーン内の署名者ノードに提供する。

【００１３】

１つの実施形態では、本出願は、互いに通信する複数のノードを含んでいる分散ストレージ・システムである分散型データベース（ブロックチェーンなど）を利用する。分散型データベースは、相互に信頼できない関係者間でレコードを維持することができる分散型台帳に似ている、追加専用の変更不可能なデータ構造を含む。信頼できない関係者は、本明細書ではピアまたはピア・ノードと呼ばれる。各ピアは、データベース・レコードのコピーを維持し、単一のピアは、分散されたピア間で合意に達することなく、データベース・レコードを変更することができない。例えば、ピアは、ブロックチェーン格納トランザクションの妥当性を確認し、それらの格納トランザクションをブロックにグループ化し、ブロック上にハッシュ・チェーンを構築するために、合意プロトコルを実行してよい。このプロセスは、一貫性のために、必要に応じて、格納トランザクションを順序付けることによって台帳を形成する。さまざまな実施形態では、許可型ブロックチェーンまたは許可なしブロックチェーンあるいはその両方が使用され得る。パブリック・ブロックチェーンまたは許可なしブロックチェーンには、特定の識別情報なしで、誰でも参加することができる。パブリック・ブロックチェーンは、ネイティブ暗号通貨を含み、プルーフ・オブ・ワーク（ＰｏＷ：Proof of Work）などのさまざまなプロトコルに基づいて、合意を使用することができる。一方、許可型ブロックチェーン・データベースは、資金、商品、情報などを交換する企業などの、共通の目標を共有しているが、互いに完全には信用していない実体のグループ内で、安全な相互作用を提供する。

【００１４】

本出願は、分散型ストレージ方式に合わせてある、「スマート・コントラクト」または「チェーンコード」と呼ばれる、任意のプログラム可能な論理を操作するブロックチェーンを利用することができる。場合によっては、システム・チェーンコードと呼ばれる、管理機能およびパラメータのための特殊なチェーンコードが存在することがある。アプリケーションは、ブロックチェーン・データベースの改ざん防止の特性、および署名または署名ポリシーと呼ばれるノード間の基礎になる合意を活用する、信頼できる分散されたアプリケーションであるスマート・コントラクトをさらに利用することができる。このアプリケーションに関連付けられたブロックチェーン・トランザクションは、ブロックチェーンにコミットされる前に「署名される」ことができ、一方、署名されていないトランザクションは無視される。署名ポリシーは、チェーンコードが、トランザクションの署名者を、署名に必要なピア・ノードのセットの形態で指定できるようにする。クライアントが、トランザクションを、署名ポリシーで指定されたピアに送信するときに、トランザクションの妥当性を確認するためのトランザクションが実行される。妥当性確認の後に、トランザクションが順序付けフェーズに移行し、順序付け段階では、合意プロトコルが使用され、ブロックにグループ化された、署名されたトランザクションの順序付けられたシーケンスを生成する。

【００１５】

本出願は、ブロックチェーン・システムの通信実体であるノードを利用することができる。「ノード」は、異なる種類の複数のノードが同じ物理サーバ上で実行され得るという意味で、論理機能を実行してよい。ノードは、信頼できるドメイン内でグループ化され、さまざまな方法でそれらのノードを制御する論理的実体に関連付けられる。ノードは、トランザクション呼び出しを署名者（例えば、ピア）にサブミットし、トランザクション提案を順序付けサービス（例えば、順序付けノード）にブロードキャストするクライアントまたはサブミット・クライアント・ノードなどの、さまざまな種類を含んでよい。別の種類のノードは、クライアントがサブミットしたトランザクションを受信し、トランザクションをコミットし、ブロックチェーン・トランザクションの台帳の状態およびコピーを維持することができるピア・ノードである。ピアは署名者の役割を持つこともできるが、これは必須要件ではない。順序付けサービス・ノードまたは順序付けノードは、すべてのノードのための通信サービスを実行するノードであり、トランザクションをコミットするとき、およびブロックチェーンの世界状態（world state）（通常は制御情報および設定情報を含んでいる初期ブロックチェーン・トランザクションの別名）を変更するときの、システム内のピア・ノードの各々へのブロードキャストなどの、配信保証を実施する。

【００１６】

本出願は、ブロックチェーンのすべての状態遷移の順序付けられた改ざん防止機能付きレコードである台帳を利用することができる。状態遷移は、参加している関係者（例えば、クライアント・ノード、順序付けノード、署名者ノード、ピア・ノードなど）によってサブミットされたチェーンコード呼び出し（すなわち、トランザクション）から生じてよい。各参加している関係者（ピア・ノードなど）は、台帳のコピーを維持することができる。トランザクションは、１つまたは複数のオペランド（作成、更新、削除など）として台帳にコミットされているアセットのキーと値のペアのセットをもたらしてよい。台帳は、変更不可能な順序付けられたレコードをブロックに格納するために使用されるブロックチェーン（チェーンとも呼ばれる）を含む。台帳は、ブロックチェーンの現在の状態を維持する状態データベースも含む。

【００１７】

本出願は、ハッシュ・リンク・ブロックとして構造化されたトランザクション・ログであるチェーンを利用することができ、各ブロックはＮ個のトランザクションのシーケンスを含んでおり、Ｎは１以上である。ブロック・ヘッダーは、ブロックのトランザクションのハッシュ、および前のブロックのヘッダーのハッシュを含んでいる。このようにして、台帳のすべてのトランザクションが順序付けられ、暗号によって一緒にリンクされてよい。したがって、ハッシュ・リンクを壊さずに台帳データを改ざんすることはできない。直前に追加されたブロックチェーンのブロックのハッシュは、それ以前に発生したチェーン上のすべてのトランザクションを表し、すべてのピア・ノードが一貫性のある信頼できる状態にあることを保証できるようにする。チェーンは、ブロックチェーンのワークロードの追加専用という性質を効率的にサポートするピア・ノードのファイル・システム（すなわち、ローカル、取り付けられたストレージ、クラウドなど）に格納されてよい。

【００１８】

変更不可能な台帳の現在の状態は、チェーンのトランザクション・ログに含まれているすべてのキーの最新の値を表す。現在の状態は、チャネルに知られている最新のキーの値を表すため、世界状態と呼ばれることもある。チェーンコード呼び出しは、台帳の現在の状態のデータに対してトランザクションを実行する。それらのチェーンコードの相互作用を効率的にするために、最新のキーの値が状態データベースに格納されてよい。状態データベースは、単にチェーンのトランザクション・ログへのインデックス付きビューであってよく、したがって、いつでもチェーンから再生成され得る。状態データベースは、ピア・ノードの起動時に、トランザクションが受け取られる前に、自動的に回復されて（必要な場合は、生成されて）よい。

【００１９】

さまざまな実施形態によれば、（例えば、ブロックチェーン・ピア・ノードを含んでい

る）署名者組織は、例えばクライアント、ピア・ノードなどによって、ブロックチェーン台帳にすでに格納されているデータ（例えば、データ・ブロックのハッシュ値など）に基づいてランダムに選択されてよい。組織のランダム化された選択は、ブロックチェーンのメンバーによって知られているプロセスを使用して実行され得る。残りのメンバー・ノードは、データの同じハッシュを使用して同じプロセスを実行することによって、署名者組織の選択のランダム化を検証することができ、このようにして、署名者組織の選択のランダム化の完全性を保証する。

【００２０】

本明細書において説明され、示された解決策の利点は、実行順序型であるより大きい許可型ブロックチェーン・ネットワーク内のトランザクションで格納される必要があるデータの量を減らすことを含む。特に、ピア組織のランダムなサブセットを選択することによって、それらのランダムに選択された組織に対して攻撃者が前もって攻撃を開始する可能性が非常に低くなる。したがって、安全な署名ポリシーに必要な組織が少なくなる。加えて、ピアをハッキングする攻撃者が、ランダムなピア選択プロセスの発生前に、そのプロセスを見つけ出さなければならず、これは非常に困難であるため、本明細書の解決策は、ピアのセキュリティを改善する。

【００２１】

一部の許可型ブロックチェーンは、実行順序の妥当性確認の枠組みに従い、この枠組みは、ブロックの妥当性確認時に、すべてのピアがトランザクションを実行する代わりに、トランザクションが、ネットワーク内のピア（例えば、署名者ノード）のサブセット上で投機的に実行され、データ内の予想される変更などの計算結果が、実行しているピアによって署名され、その後、それらの計算結果が順序付けノードに送信され、順序付けノードがトランザクションをブロックにまとめる。コミット時に、ブロックがピア・ノードに送信され、各ピア・ノードが、実行結果が適切に署名されている限り、それらの実行結果が正しいということを検証する。

【００２２】

そのような許可型ブロックチェーンの例はＨｙｐｅｒｌｅｄｇｅｒ　Ｆａｂｒｉｃであり、Ｈｙｐｅｒｌｅｄｇｅｒ　Ｆａｂｒｉｃでは、クライアントがソフトウェア開発キット（ＳＤＫ：software development kit）を使用し、ソフトウェア開発キットが、スマート・コントラクトの名前およびスマート・コントラクト・トランザクションへの入力を含んでいるトランザクション提案を、署名者ピア・ノードに送信する。署名者は、トランザクションを投機的に実行し、読み取り／書き込みセット（「署名」とも呼ばれる）に署名し、署名をクライアントに返送し、クライアントは、これらの署名を使用してトランザクションを構築する。次に、クライアントによって、トランザクションが順序付けサービスに送信され、順序付けサービスがトランザクションをブロックにまとめる。ブロックがピアに配布され、ピアは、実行結果がピアの許容できるサブセットによって署名されているかどうか、およびトランザクションの読み取りセットが投機的実行以降に変化していないかどうかを含む、トランザクション実行の側面の妥当性を確認する。前者は、「署名ポリシー」と呼ばれ、その役割は、ネットワークのセキュリティの前提に従って、場合によっては、トランザクションが拘束される取引関係も考慮して、トランザクションが十分なピア上で正しく実行されていることを強制することである。

【００２３】

すべての署名を実行する組織／ピア・ノードの信頼できるコアをブロックチェーン・ネットワークに含めることは、すべてのトランザクション実行の健全性を保証することができるが、他者に完全な信用が存在しないというブロックチェーン・ネットワークの極めて核心的な部分と矛盾する不合理な信用の前提を必要とする。

【００２４】

非限定的な例として、ブロックチェーン・ネットワークは、複数の管理領域内のピアによって取引相手間のトランザクションが署名されることを必要としてよい。会社Ａが会社Ｂに送金する契約では、会社Ａのピアおよび会社Ｂのピアだけでなく、会社Ｃなどの監査

組織のピアよってシミュレートされ、署名されるトランザクションを含むことが標準的である。この例では、会社ＡおよびＢは、これらの会社の残高が商取引に応じて確実に更新されるようにしたいであろう。監査人のピアは、多くの場合、システム内で循環する通貨の合計金額が同じままになるように含まれ、通貨の合計金額が同じでない場合、通貨が会社Ａの口座から引き落とされないが、会社Ｂの口座が増えるというように、ピアＡおよびＢが悪意をもって合意した可能性がある。したがって、ネットワーク内のすべてのピアによってトランザクションが有効であると見なされるようにするために、したがってトランザクションの実行結果がコミット時に適用されるようにするために、対応する組織（Ａ、Ｂ、およびＣ）の各々からのピアがトランザクションに署名することが、必要とされてよい。

【００２５】

この署名ポリシーは、取引プロセスに十分に結び付けられているが、一部の脅威モデル（特に、他の組織によってハッキングされる組織を考慮する脅威モデル）に適していないことがある。この例において、組織ＡまたはＢが監査組織Ｃをハッキングする場合、ハッキング側が共謀し、Ａの口座残高が変化しないまま、Ｂの口座残高が増えるようなトランザクション実行結果を構築し、組織Ｃの（セキュリティを侵害された）ピアに、この実行結果に署名させ、その後、このトランザクションが、ネットワーク内のすべてのピアによって有効と見なされるであろう。そのような目的で、トランザクションに署名する必要があるさまざまな組織を増やし、そうすることによって、不正なトランザクション実行に署名するために十分な（セキュリティを侵害された悪意のある）組織を獲得することをますます困難にするのが一般的である。

【００２６】

ブロックチェーン・ネットワークが拡大し、さらに多くの組織が参加するにつれて、セキュリティと性能の間のトレードオフが発生する。例えば、トランザクションが有効と見なされるために、異なる組織からのより多くの署名が必要になるほど、署名ポリシーがより安全になる。しかしそれは、コミット時に検証するべきより多くの署名が存在するということも意味し、より多くの署名は、公開鍵（およびＨｙｐｅｒｌｅｄｇｅｒ　Ｆａｂｒｉｃでは、ｘ５０９証明書全体）がトランザクションに存在する必要もあるということも意味し、これによってトランザクションのサイズが増え、署名者ピア上の全体的実行負荷が増大する。これら３つの要因（より多くの署名検証、より大きいトランザクション、追加のトランザクション実行および署名）の各々は、システム性能に対する悪影響を引き起こす。さらに、ネットワーク内の組織が多いほど、攻撃者が組織をハッキングするか、または共謀するように組織に影響を与えるのがより容易になり（より多くの機会が存在し）、異なる組織からの必要な署名が少ないほど、攻撃者が攻撃を開始するのがより容易になる。

【００２７】

別の説得力のある使用事例は、互いに完全には信用していないが、それでも実行順序の枠組み内で正しいスマート・コントラクトの実行を保証したい多数の（数十個または１００個にさえなる）組織を含むブロックチェーン・ネットワークを伴う事例である。この例の場合は、組織の大部分を含んでいる署名ポリシー、または実際には、組織の数においてやや線形である任意の署名ポリシーが、性能および拡張性の観点から、非実用的である。その結果、署名するために一定の数の組織（例えば、１００個のうちの１０個の組織）を必要とする署名ポリシーは、唯一の実行可能な解決策であるが、おそらく比較的少数の組織が、ハッキングされる可能性があるか、または共謀して、相互利益を促進するためにスマート・コントラクトのビジネス・ルールに従って実行されなかったトランザクションを偽造することができ、したがって、ネットワークのデータの完全性を損なう。

【００２８】

そのような攻撃の重要なイネーブラは、トランザクション提案を（署名のために）ピアにサブミットするクライアントが、署名者の選択において完全な自由を有しており、したがってクライアントは、概要が示された攻撃の共犯者として積極的役割を果たすことがで

きるという事実である。コミット・ピアが、署名ピアのランダムなサブセットを選択することをクライアントに強制することができれば、この懸念は軽減され得る。さらに、ブロックチェーンは、クライアント自身によって選択されるランダム性に依存することができず、そうでなければ、クライアントは、選択が望ましい破損したピアを生み出すまで、単に（ランダムな）選択を繰り返すことができる。代わりにランダム性は、クライアントが完全には制御しない（その後、検証されることができる）ソースから生じなければならない。

【００２９】

実施形態例は、ブロックチェーンにすでに格納されている既知／検証可能なデータに対して実行する既知のアルゴリズムに基づいてネットワークからピア組織をランダムに選択することをクライアント（またはピア・ノードなどのその他の実体）に要求することによって、ランダム性を署名者ピア組織の選択プロセスに導入する。ブロックチェーン・ネットワーク内の組織の数に基づいて、一意の識別子（数値）が組織の各々に割り当てられ得る。ブロックチェーン・ネットワークから署名者組織のサブセットを選択するために、クライアントは、以前のブロックのグループからのブロック・ハッシュ値を使用することを要求されてよい。ブロック・ハッシュは、乱数（例えば、２進数）を生成するために使用され得る。２進乱数が、ビット値のセグメントにセグメント化されてよい。第１のビット値が、２進乱数からスライスされ、１０進値に変換されてよく、この１０進値が、組織の一意の識別子に直接的または間接的にマッピングされてよい。十分な署名者組織がランダムに決定されるまで、このプロセスが繰り返され得る（別のスライスが２進乱数から取得される）。次に、クライアントは、トランザクションの署名を実行するために、これらの署名者ノードに依存してよい。

【００３０】

本明細書の解決策において説明される別の利点は、基本的に、ブロック・ハッシュとして使用され得るブロックチェーン上のブロック（直前に格納されたブロック）のサブセットを指定する、ブロック間隔の使用である。クライアントは、ブロックチェーン台帳の現在の高さを取り出し、ブロックチェーン台帳の現在の高さをブロック間隔値で割ることに基づいて、完全性値を生成する。得られた完全性値は、トランザクションと共に格納されてよく、クライアントが、ブロックチェーン台帳に直前に格納されたブロックのうちから、ブロック間隔によって示されたブロックを選択したということを検証するために使用されてよい。

【００３１】

図１は、実施形態例に従って、トランザクションの署名のためのピア・ノードをランダムに選択するためのコンピューティング環境１００を示している。図１を参照すると、コンピューティング環境１００は、Ｎ個のピア・ノード１１０を含む許可型ブロックチェーンを含んでいる。この例では、Ｎ個のピア・ノード１１０のいずれかが、トランザクションの署名者として機能することができる。各ピアは、それ自身の組織（図に示されていない）に参加し、例えば、ピア１が組織１であり、ピア２が組織２である、などとなる。さまざまな実施形態によれば、クライアント１２０は、ピア組織のサブセットをランダムに選択するように強制されてよく、その後、Ｎ個のピア・ノード１１０のグループからのピア・ノードが、署名を実行する。さらに、どのピア組織を選択するべきかをランダムに決定するプロセスは、ブロック・ハッシュ値、または図４Ａ～４Ｃの例で説明されるような複数のブロック・ハッシュ値などの、ブロックチェーンにすでに格納されている検証可能なデータに基づいてよい。図１の例では、クライアント１２０が、Ｎ個のピア・ノード１１０のうちからピア２、３、５、および８をランダムに選択している。

【００３２】

一部の実施形態では、ランダムな選択を実行するための論理は、クライアント１２０のソフトウェア開発キット（ＳＤＫ）に構築されてよく、ピア・ノードまたは順序付けノードから最新のブロック（または直前に格納されたブロックのサブセットのうちのブロック）を取得し、その後、この情報を使用して、組織のランダム化された選択を計算する。別

の例として、ランダムな選択を実行するための論理が、ＳＤＫが問い合わせることができる信頼できるピアに構築されてよく、クライアントのために選択を計算するサービスとして機能する。さらに、トランザクション（およびそれに対応するブロック）をブロックチェーンにコミットするときに、Ｎ個のピア・ノード１１０もランダムな選択プロセスの妥当性を確認できるように、Ｎ個のピア・ノード１１０の各々が、ノード内に構築されたランダムな選択プロセスを含んでよい。

【００３３】

例えば、ＳＨＡ－２５６、ＭＤ５などのハッシュ関数によって、ブロック・ハッシュが生成されてよい。得られたハッシュ値は、１２８ビット、２５６ビット、５１２ビットなどの特定のサイズを有する文字列である。さまざまな実施形態によれば、疑似乱数発生器（ＰＲＮＧ：pseudo-random number generator）などによって２進乱数を生成するために、ハッシュ値が使用されてよい。得られた２進乱数は、ブロック・ハッシュと同じ数のビットを含んでよいが、文字と数字の組み合わせの代わりに、乱数は２進数１および０のみを含んでよい。６４ビットのハッシュ値の例を以下に示す。

Hash =as7r430pohvb21msw98210pplhnmbn30431trewq9820pksgreder084321abyx09

【００３４】

ここで、ブロック・ハッシュは、ハッシュ値を２進乱数に変換するＰＲＮＧへのシード値の役割を果たしてよい。例えば、ＰＲＮＧは、一連の２進乱数の特性に近い特性を有する一連の２進数を生成するためのアルゴリズムを含んでよい。ＰＲＮＧによって生成されるシーケンスは、（真にランダムな値を含んでよい）ＰＲＮＧのシードと呼ばれる初期値（ブロック・ハッシュ）によって完全に決定されるため、真にランダムではない。上記のハッシュから作成された２進数のＰＲＮＧの例を以下に示す。

PRNG =1100101000101111010001011010100101100101001001001010 1001010001

【００３５】

ブロック・ハッシュから作成されたＰＲＮＧの値に基づいて、ランダムなピア選択プロセスが実行されてよい。例えば、ネットワークに含まれているピア組織の数に基づいて、Ｎ個のピア組織１１０のうちの各ピア組織に一意の識別子が割り当てられてよい。一意の識別子は、数値（１０進数など）であってよい。例えば、Ｎ個の組織の各々に、０～Ｎ－１の一意の識別子が割り当てられ得る。一方、データ・セグメント／チャンクが、２進数形式であるＰＲＮＧから除去され、１０進数の形態に変換され得る。データ・セグメントのサイズは、ｌｏｇ２（Ｎ）ビット、またはｆ（ｘ）＝2^{x}の逆関数に対応する２の基数での対数であってよい。例えば、ピア組織の数が２０（すなわち、Ｎ＝２０）である場合、各ピア組織に、０～１９の一意の値が割り当てられてよく、データ・セグメントのサイズはｌｏｇ２（２０）＝４．３２であってよく、この値が５ビットに切り上げられる。

【００３６】

したがって、この例では１０００１である最初の５ビットが、ＰＲＮＧから除去され、１７である１０進数に変換されてよい。この値は、ピア組織の一意の識別子１８に対応する。システムが５つの署名者組織を選択する必要がある場合、追加のビット・セグメントを２進乱数から取得し、このプロセスをビット・セグメントに対して実行することによって、５つの異なる一意の識別子が決定されるまで、このプロセスが繰り返され得る。十分な組織がランダムに識別される前に、２進乱数がビットを使い果たした場合、ブロック・ハッシュが再びハッシュされてプロセスが繰り返されてよく、または別のブロック・ハッシュが選択されてプロセスが繰り返されてよい。

【００３７】

強制されたランダムなピア選択が、多数の組織を含むブロックチェーン・ネットワークなどのブロックチェーン・ネットワークの署名ポリシーに含まれてよい。その結果、署名ポリシーが満たされるための十分な組織をハッキングすることが、実現困難になる。署名ポリシーは、組織のいずれかの特定のセットに制限されず、代わりに、署名ポリシーによ

って許容できると見なされる、同じトランザクション実行に署名する組織の任意の十分に大きいサブセットを含んでよい。本明細書に記載された技術およびメカニズムが、組織の選択がより狭い他のモデルに適用され得るということも、理解されるべきである。

【００３８】

さらに、Ｎ個のピア組織の各々は、ランダムな署名者ノード選択プロセスの妥当性を確認することができる。言い換えると、コミット・ピアは、署名者ノードが実際にランダムであるということを検証してよい。乱数を生成するためのシードとして使用されるハッシュが、ブロックチェーンに格納されたブロック・ハッシュから決定されるため、ブロックチェーン・ネットワーク内のピア・ノードは、同じブロック・ハッシュを取り出し、同じ２進乱数の生成を実行することができる。次に、ピアの各々は、ブロック・ハッシュをセグメント化し、セグメントを一意の組織ＩＤにマッピングし、同じ組織ＩＤがクライアントによって選択されることを保証することができ、それによって、２進乱数から得られた対応する組織に基づいて正しい署名者ノードが選択されたということの妥当性を確認する。

【００３９】

例えば、Ｎが組織の数であり、Ｋ＜Ｎが、署名ポリシーが満たされるためにトランザクションに署名しなければならない組織の数であるとする。ネットワーク・ピアによって妥当性が確認され得るトランザクションを偽造するために、攻撃者は、Ｎ個の組織のうちのＫ個をハッキング／説得する必要があり、つまり攻撃者は、任意のＫ個の組織を選択し、それらをターゲットにすることができる。しかし、ランダムに選択されたＫ個の組織を急にハッキングすることは、攻撃者にとって明らかに極めて困難である。本明細書に記載された署名ポリシーは、（選択されたｎ個の組織のうちの任意のｋ個を選択するのとは対照的に）ランダムに選択されたＫ個の組織の制限された組み合わせのみを選択することを攻撃者に強制し、下でさらに説明されるように、組織の組み合わせは、Ｔ個ごとのブロックの後に、ブロックチェーン自体の内容に従って絶えず（ランダムに）変化する。例えば、すべての連続するＴ個のブロックのシーケンスは、Ｎ個の組織のうちのＫ個の選択に対して、少数の組み合わせを定義するために使用されてよく、トランザクションが有効であると見なされるためには、Ｋ個の組織の組み合わせが、最後のＴ個のブロック内で検出されるように、それらの組み合わせによって、トランザクションが署名される必要がある。

【００４０】

「最後のＴ個のブロック」は、本明細書では、ターゲット間隔制約（target interval constraint）と呼ばれてよく、Ｔはブロック間隔値である。例えば、署名ポリシーは、トランザクションが有効に署名されるために、ブロックチェーンに格納された最後のＴ個のブロックからのブロック・ハッシュに基づいて、ランダムなピア選択プロセスが実行されなければならないという制約を含んでよい。これを検証するために、クライアントまたはピアは、台帳の現在の高さ（Ｈ）をブロック間隔（Ｔ）で割った値などの完全性値をトランザクションに含めてよい。次に、妥当性確認時に、コミット・ピアが、現在の高さ（Ｈ）をＴで割った（最も近い最小の整数に切り上げた）値がその数値に等しいかどうかをチェックし、等しくない場合、トランザクションが無効であると見なされる。この制約は、長過ぎるトランザクションが、未来のブロックに含めるためにサブミットされる前に、クライアントによって保持されることができないということを指示し、基本的に、トランザクションが、ブロックチェーンがＴ個のブロックよりさらに進んだ後のブロックに入った場合、高さＨでシミュレートされたトランザクションを無効にする。この制約の使用は、セキュリティの保証を大幅に向上させることができる。

【００４１】

さまざまな実施形態によれば、本明細書で提供された変更に基づいて、攻撃者がトランザクションを偽造しようとした場合、攻撃者は、ランダムに選択された組織を引き継ぐことを強制され、この引継ぎは、それに要する時間のため、達成不可能であることがある。ここで、新しいＴ個のブロックが、すでに形成されていてよく、偽造されたトランザクションが古い（Ｔ個のブロックが形成される前の）組織の署名から形成された場合、トラン

ザクションの署名者のセットが、最後のＴ個のブロックによって生じた組織のいずれかの組み合わせにおいて検出されないため、そのトランザクションは、コミット時に無効化される。別の選択肢として、攻撃者は、前もって選択された組織を引き継ぎ、その有効として事前に準備された署名者のセットからの署名を宣言するＴ個のブロックが形成されるのを待機する必要があってよい。しかしこれは、発生するのに長い時間を要するか、または全く発生しないことがある。これは、ブロックチェーンの高さをブロック間隔値Ｔで割った値に対応するトランザクションの完全性値をブロックに記録することによっても妨げられる。これによって、攻撃者は、事前に準備された署名者のセットを引き起こすＴ個のブロックの正しい間隔を推測することが必要になる。しかし、他の（悪意のない）関係者がトランザクションをブロックチェーンにサブミットしている場合、Ｔ個のブロックの間隔を事前に予測することは、ランダムな入力（本物の関係者によって選択され、ランダム性を含んでいるトランザクション）に依存するため、不可能である。

【００４２】

実施形態例は、２５６ビットを出力する安全なハッシュ関数を使用してブロック・ハッシュを生成し（この技術は、さまざまな長さのハッシュ関数に適合するように変更され得る）、最後のＴ個の連続するブロックのハッシュをH_0、H_1、H_2、．．．H_{T-1}として示し、署名者の組織をO_0、O_1、O_2、．．．、O_{N-1}として示してよい。一意の組織ＩＤをエンコードするために、システムはｌｏｇ２（Ｎ）ビットを使用してよく、Ｋ個の組織をエンコードするために、システムはｌｏｇ２（Ｎ）ビットのうちの少なくともＫ個の数値を取得してよい。最後のＴ個の連続するブロックのハッシュが、次の方法でＫ個の組織の第１の組み合わせを定義する。システムは、組織のＩＤを表すために、数値の空のセットＳを初期化し、ブロック・ハッシュ（H_{T-1}など）の最下位のｌｏｇ２（Ｎ）ビットを受け取り、それをＢ０として示し、Ｂ０の数値表現をＳに追加する。次にシステムは、ブロック・ハッシュの次のｌｏｇ２（Ｎ）ビットを受け取り、それをＢ１として示し、Ｂ１がＳに存在する場合、システムはＢ１を破棄することができ、そうでない場合、システムはＢ１をＳに追加することができる。その後システムは、プロセスを続行し、Ｋ個の異なるＩＤを検出するか、またはブロック・ハッシュH_{T-1}内のビットを使い果たすまで、ブロック・ハッシュの次のｌｏｇ２（Ｎ）ビットに移動してよい。システムが十分な異なるＩＤを保有していない場合、システムは、ブロック・ハッシュを再びハッシュするか、または以前のブロック・ハッシュを取り出し、さらに多くの一意のＩＤの取り出しを開始することができる。

【００４３】

ブロックチェーン・ネットワークが１００個のピア組織をネットワークに含み、１０個の組織からの署名が必要とされる例では、Ｎ＝１００およびＫ＝１０である。さらに、ターゲット間隔制約が、ブロック・ハッシュを最後の１２個のブロックからであるように制限し、ブロック間隔値がＴ＝１２である。この例では、最後の１２個のブロックは、組織の選択を指示し、つまりトランザクションごとに、署名用のＫ個の組織の識別に使用するために、最大でＴ個のブロック・ハッシュが存在する。例えば、ブロックチェーンは、毎秒２０００トランザクションのスループットを維持してよい。この例では、アプリケーションは、トランザクションに署名するために約３秒を有し、このトランザクションを次のブロックに含めるために送信する。選択するための１００個の識別子および８ビットの３２個の間隔が存在するため、単一のブロック・ハッシュが１０個の異なる数値を含んでいない（つまり、２５６ビットのハッシュ・サイズを使用する場合、３２個の８ビットのシーケンスすべてが、全体で１０個未満の数値を含む）確率は極めて小さい。さらに、ブロック・ハッシュがＫ個未満の識別子を生み出す場合（これは、前述したように低い確率で発生する）、システムは、ブロックのハッシュにもう一度ハッシュを適用してから、このハッシュを使用し続けてよい。代替として、ブロック・ハッシュをシードとして疑似乱数発生器（ＰＲＮＧ）を使用して、数値の導出が実行され得る。

【００４４】

図２Ａは、実施形態例に従って、ブロックチェーン・アーキテクチャの構成２００を示

している。図２Ａを参照すると、ブロックチェーン・アーキテクチャ２００は、特定のブロックチェーン要素（例えば、ブロックチェーン・ノードのグループ２０２）を含んでよい。ブロックチェーン・ノード２０２は、１つまたは複数のノード２０４～２１０を含んでよい（単に例として、これらの４つのノードが示されている）。これらのノードは、ブロックチェーン・トランザクションの追加および妥当性確認プロセス（合意）などの、複数の活動に参加する。ブロックチェーン・ノード２０４～２１０のうちの１つまたは複数は、署名ポリシーに基づいてトランザクションに署名してよく、アーキテクチャ２００内のすべてのブロックチェーン・ノードのための順序付けサービスを提供してよい。ブロックチェーン・ノードは、ブロックチェーン認証を開始し、ブロックチェーン層２１６に格納されたブロックチェーンの変更不可能な台帳に書き込もうとしてよく、この書き込みのコピーが、基盤になる物理的インフラストラクチャ２１４にも格納されてよい。ブロックチェーンの構成は、格納されたプログラム／アプリケーション・コード２２０（例えば、チェーンコード、スマート・コントラクトなど）にアクセスして実行するためにアプリケーション・プログラミング・インターフェイス（ＡＰＩ：application programming interfaces）２２２にリンクされた１つまたは複数のアプリケーション２２４を含んでよく、プログラム／アプリケーション・コード２２０は、参加者によって要求されてカスタマイズされた構成に従って作成することができ、それら自身の状態を維持し、それら自身のアセットを制御し、外部の情報を受信することができる。ブロックチェーンの構成は、トランザクションとしてデプロイし、分散型台帳に追加することによって、すべてのブロックチェーン・ノード２０４～２１０にインストールすることができる。

【００４５】

ブロックチェーン・ベースまたはプラットフォーム２１２は、ブロックチェーン・データのさまざまな層と、サービス（例えば、暗号信用サービス、仮想実行環境など）と、新しいトランザクションを受信して格納し、データ・エントリにアクセスしようとしている監査人にアクセスを提供するために使用されてよい、基盤になる物理的コンピュータ・インフラストラクチャとを含んでよい。ブロックチェーン層２１６は、プログラム・コードを処理し、物理的インフラストラクチャ２１４に参加させるために必要な仮想実行環境へのアクセスを提供するインターフェイスを公開してよい。暗号信用サービス２１８は、アセット交換トランザクションなどのトランザクションを検証し、情報をプライベートに保つために使用されてよい。

【００４６】

図２Ａのブロックチェーン・アーキテクチャの構成は、ブロックチェーン・プラットフォーム２１２によって公開された１つまたは複数のインターフェイスおよび提供されたサービスを介して、プログラム／アプリケーション・コード２２０を処理および実行してよい。コード２２０は、ブロックチェーンのアセットを制御してよい。例えば、コード２２０は、データを格納および転送することができ、スマート・コントラクトおよび条件を含む関連するチェーンコードまたは実行の対象になるその他のコード要素の形態で、ノード２０４～２１０によって実行されてよい。非限定的な例として、リマインダ、更新、または変更、更新の対象になるその他の通知、あるいはその組み合わせなどを実行するために、スマート・コントラクトが作成されてよい。スマート・コントラクト自体は、権限付与およびアクセスの要件ならびに台帳の使用に関連付けられたルールを識別するために使用され得る。例えば、書き込みデータ２２８を含んでいるブロックチェーンに書き込まれる処理結果を作成するために、読み取りデータ２２６が、ブロックチェーン層２１６に含まれている１つまたは複数の処理実体（例えば、仮想マシン）によって処理されてよい。物理的インフラストラクチャ２１４は、本明細書に記載されたデータまたは情報のいずれかを取り出すために利用されてよい。

【００４７】

高水準のアプリケーションおよびプログラミング言語を使用して、スマート・コントラクトが作成され、その後、ブロックチェーン内のブロックに書き込まれてよい。スマート・コントラクトは、ブロックチェーン（例えば、ブロックチェーン・ピアの分散ネットワ

ーク）への登録、格納、または複製、あるいはその組み合わせが実行される実行可能コードを含んでよい。トランザクションは、スマート・コントラクトが満たされていることに関連付けられた条件に応答して実行され得る、スマート・コントラクト・コードの実行である。スマート・コントラクトの実行は、デジタル・ブロックチェーン台帳の状態に対する信頼できる変更をトリガーしてよい。スマート・コントラクトの実行によって引き起こされるブロックチェーン台帳に対する変更は、１つまたは複数の合意プロトコルを介して、ブロックチェーン・ピアの分散ネットワーク全体に自動的に複製されてよい。

【００４８】

スマート・コントラクトは、データをキーと値のペアの形式でブロックチェーンに書き込んでよい。さらに、スマート・コントラクト・コードは、ブロックチェーンに格納された値を読み取り、それらをアプリケーションの動作において使用することができる。スマート・コントラクト・コードは、さまざまな論理演算の出力をブロックチェーンに書き込むことができる。このコードは、仮想マシンまたはその他のコンピューティング・プラットフォーム内の一時的データ構造を作成するために使用されてよい。ブロックチェーンに書き込まれたデータは、パブリックになること、またはプライベートとして暗号化されて維持されること、あるいはその両方が行われ得る。スマート・コントラクトによって使用／生成される一時的データは、提供された実行環境によってメモリ内に保持され、ブロックチェーンに必要なデータが識別された後に削除される。

【００４９】

チェーンコードは、追加機能と共に、スマート・コントラクトのコード解釈を含んでよい。本明細書に記載されているように、チェーンコードは、コンピューティング・ネットワーク上にデプロイされるプログラム・コードであってよく、合意プロセス中に、チェーン・バリデータによって一緒に実行されて妥当性を確認される。チェーンコードは、ハッシュを受信し、以前に格納された特徴抽出機能の使用によって作成されたデータ・テンプレートに関連付けられたハッシュをブロックチェーンから取り出す。ハッシュ識別子のハッシュと、格納された識別子テンプレート・データから作成されたハッシュが一致する場合、チェーンコードは、権限付与キーを、要求されたサービスに送信する。チェーンコードは、暗号の詳細に関連付けられたデータをブロックチェーンに書き込んでよい。

【００５０】

図２Ｂは、実施形態例に従って、ブロックチェーンのノード間のブロックチェーン・トランザクション・フロー２５０の例を示している。図２Ｂを参照すると、トランザクション・フローは、アプリケーション・クライアント・ノード２６０によって１つまたは複数の署名ピア・ノード（例えば、ピア・ノード２８１および２８３）に送信されるトランザクション提案２９１を含んでよい。さまざまな実施形態によれば、アプリケーション・クライアント・ノード２６０は、本明細書の例で説明されたように、（例えば、ピア・ノードなどを介して）ブロックチェーンのブロックから取り出されたハッシュ値に基づいて、署名ピア組織をランダムに選択してよい。例えば、ブロック・ハッシュが２進乱数に変換され得る。２進数は、２進乱数からスライスされ、署名ピア・ノードを識別するために使用される、ビット・セグメントに分割され得る。アプリケーション・クライアント・ノード２６０は、Ｋ個の署名者ノードを識別し、トランザクション提案２９１を署名ピア・ノードに送信してよい。署名ピア・ノードは、クライアントの署名を検証し、チェーンコード関数を実行してトランザクションを開始してよい。出力は、チェーンコードの結果、チェーンコードに読み取られたキー／値のバージョンのセット（読み取りセット）、およびチェーンコードに書き込まれたキー／値のセット（書き込みセット）を含んでよい。提案応答２９２が、承認されている場合は署名と共に、クライアント２６０に返送される。クライアント２６０は、署名をトランザクションのペイロード２９３にまとめ、合意のために順序付けサービス・ノード２８４にブロードキャストする。その後、順序付けサービス・ノード２８４は、トランザクションをブロックに順序付け、それらのブロックをチャネル上のすべてのピア２８１～２８３に配布する。ブロックチェーンへのコミットの前に、各ピア２８１～２８３は、署名者ピア・ノード選択プロセスが実際にランダムであるとい

うことを検証し、トランザクションの妥当性を確認してよい。例えば、ピアは、同じブロック・ハッシュに基づいてそれら自身のランダムな選択プロセスを実行し、正しい署名者ノードが選択されたことを検証し、署名ポリシーもチェックして、指定されたピアの正しい割り当てが結果に署名し、トランザクションのペイロード２９３に対する署名を認証したことを確認してよい。

【００５１】

図２Ｂを再び参照すると、２９０で、クライアント・ノード２６０が、ブロックチェーンに格納されたブロックのブロック・ハッシュに基づいて、Ｋ個の署名者ピア組織（例えば、ピア・ノード２８１およびピア・ノード２８３）をランダムに選択する。クライアント・ノード２６０は、要求を構築し、２９０で署名者としてランダムに選択された署名者ピア・ノード２８１および２８３に送信することによって、トランザクション２９１を開始する。クライアント２６０は、サポートされているソフトウェア開発キット（ＳＤＫ：software development kit）を利用するアプリケーションを含んでよく、このアプリケーションは、使用可能なＡＰＩを利用してトランザクション提案を生成する。提案は、データが台帳から読み取られること、または台帳に書き込まれること（すなわち、アセットの新しいキーと値のペアを書き込むこと）、あるいはその両方を実行できるように、チェーンコード関数を呼び出すことの要求である。ＳＤＫは、トランザクション提案を、適切に設計された形式（例えば、遠隔手続き呼び出し（ＲＰＣ：remote procedure call）を経由するプロトコル・バッファ）にパッケージ化するためのシムとして機能し、クライアントの暗号認証情報を受け取って、トランザクション提案の一意の署名を生成してよい。

【００５２】

それに応じて、署名ピア・ノード２８１および２８３は、（ａ）トランザクション提案が適切に形成されていること、（ｂ）トランザクションが過去にすでにサブミットされていないこと（リプレイアタック保護）、（ｃ）署名が有効であること、および（ｄ）そのチャネルに対する提案された操作を実行するための適切な権限がサブミッター（例では、クライアント２６０）に与えられていることを検証してよい。署名ピア・ノード２８１および２８３は、トランザクション提案の入力を、呼び出されるチェーンコード関数への引数として受け取ってよい。その後、チェーンコードが、現在の状態データベースに対して実行され、応答値、読み取りセット、および書き込みセットを含んでいるトランザクション結果を生成する。ただしこの時点では、台帳に対する更新は行われない。２９２で、値のセットが、署名ピア・ノード２８１および２８３それぞれの署名と共に、提案応答２９２としてクライアント２６０のＳＤＫに返され、このＳＤＫが、アプリケーションが使用するためのペイロードを構文解析する。

【００５３】

それに応じて、クライアント２６０のアプリケーションが、署名ピアの署名を検査／検証し、提案応答を比較して、提案応答が同じであるかどうかを判定する。チェーンコードが単に台帳に問い合わせた場合、アプリケーションは問い合わせ応答を検査し、通常は、トランザクションを順序付けノード・サービス２８４にサブミットしない。クライアント・アプリケーションが、台帳を更新するためにトランザクションを順序付けノード・サービス２８４にサブミットしようとしている場合、アプリケーションは、サブミットする前に、指定された署名ポリシーが満たされているかどうか（すなわち、トランザクションに必要なすべてのピア・ノードがトランザクションに署名したかどうか）を判定する。ここで、クライアントは、トランザクションの複数の関係者のうちの１つのみを含んでよい。アーキテクチャは、アプリケーションが応答を検査しないことを選択するか、またはその他の方法で署名されていないトランザクションを転送する場合でも、署名ポリシーが、ピアによってまだ実施され、コミット妥当性確認フェーズで維持されるようにする。

【００５４】

検査に成功した後に、ステップ２９３で、クライアント２６０が、署名をトランザクションにまとめ、順序付けノード２８４へのトランザクション・メッセージ内でトランザク

ション提案およびトランザクション応答をブロードキャストする。トランザクションは、読み取り／書き込みセット、ランダムに選択された署名ピアの署名、およびチャネルＩＤを含んでよい。順序付けノード２８４は、その動作を実行するために、トランザクションの内容全体を検査する必要はなく、代わりに順序付けノード２８４は、単に、トランザクションをネットワーク内のすべてのチャネルから受信して、チャネル別に経時的に順序付けし、チャネルごとにトランザクションのブロックを作成してよい。

【００５５】

トランザクションのブロックは、順序付けノード２８４からチャネル上のすべてのピア・ノード２８１～２８３に配信される。いずれかの署名ポリシーが満たされていることを保証するため、および読み取りセットがトランザクションの実行によって生成されて以来、読み取りセットの変数に関して台帳の状態に対する変更がないことを保証するために、ブロック内のトランザクション２９４の妥当性が確認される。ブロック内のトランザクションは、有効または無効であるとしてタグ付けされる。

【００５６】

さまざまな実施形態によれば、ステップ２９５で、ピア・ノード２８１～２８３の各々が、クライアント・ノード２６０によって実行されたランダムな署名者組織選択プロセスを検証することができる。例えば、ピア・ノード２８１～２８３の各々は、ブロックに含まれているトランザクションが、２９０からのランダムな選択に従ってピアによってシミュレートされ、署名されたかどうかをチェックすることができる。さらに、ランダムな選択の検証が成功した場合、ステップ２９６で、各ピア・ノード２８１～２８３は、ブロックをチャネルのチェーンに追加し、有効なトランザクションごとに、書き込みセットが現在の状態データベースにコミットされる。トランザクション（呼び出し）が変更不可能なようにチェーンに追加されたことをクライアント・アプリケーションに通知するため、およびトランザクションの妥当性が確認されたか、または無効にされたかを通知するために、イベントが発行される。

【００５７】

図３Ａは許可型ブロックチェーン・ネットワーク３００の例を示しており、許可型ブロックチェーン・ネットワーク３００は、分散型の非集中的ピアツーピア・アーキテクチャを特徴とする。この例では、ブロックチェーン・ユーザ３０２は、許可型ブロックチェーン３０４に対するトランザクションを開始してよい。この例では、トランザクションは、デプロイ、呼び出し、または問い合わせであることができ、ＳＤＫを利用するクライアント側のアプリケーションを介して、ＡＰＩを介して直接的に、などによって、発行されてよい。ネットワークは、監査人などのレギュレータ３０６へのアクセスを提供してよい。ブロックチェーン・ネットワーク・オペレータ３０８は、レギュレータ３０６を「監査人」として登録し、ブロックチェーン・ユーザ３０２を「クライアント」として登録するなど、メンバーの許可を管理する。監査人を、台帳への問い合わせのみに制限することができ、一方、特定の種類のチェーンコードのデプロイ、呼び出し、および問い合わせを行うための権限をクライアントに与えることができる。

【００５８】

ブロックチェーン開発者３１０は、チェーンコードおよびクライアント側のアプリケーションを書き込むことができる。ブロックチェーン開発者３１０は、インターフェイスを介して、チェーンコードをネットワークに直接デプロイすることができる。従来のデータ・ソース３１２からの認証情報をチェーンコードに含めるために、開発者３１０は、帯域外接続を使用してデータにアクセスすることができる。この例では、ブロックチェーン・ユーザ３０２は、ピア・ノード３１４を介して許可型ブロックチェーン３０４に接続する。ピア・ノード３１４は、いずれかのトランザクションを開始する前に、ユーザの登録およびトランザクションの証明書を、ユーザの役割および許可を管理する認証機関３１６から取得する。場合によっては、ブロックチェーン・ユーザは、許可型ブロックチェーン３０４上でトランザクションを実行するために、それらのデジタル証明書を所有しなければならない。一方、チェーンコードを利用しようとしているユーザは、従来のデータ・ソー

ス３１２上のそれらのユーザの認証情報を検証することが必要になることがある。ユーザの権限付与を確認するために、チェーンコードは、従来の処理プラットフォーム３１８を介して、このデータへの帯域外接続を使用することができる。

【００５９】

図３Ｂは許可型ブロックチェーン・ネットワーク３２０の別の例を示しており、許可型ブロックチェーン・ネットワーク３２０は、分散型の非集中的ピアツーピア・アーキテクチャを特徴とする。この例では、ブロックチェーン・ユーザ３２２は、トランザクションを許可型ブロックチェーン３２４にサブミットしてよい。この例では、トランザクションは、デプロイ、呼び出し、または問い合わせであることができ、ＳＤＫを利用するクライアント側のアプリケーションを介して、ＡＰＩを介して直接的に、などによって、発行されてよい。ネットワークは、監査人などのレギュレータ３２６へのアクセスを提供してよい。ブロックチェーン・ネットワーク・オペレータ３２８は、レギュレータ３２６を「監査人」として登録し、ブロックチェーン・ユーザ３２２を「クライアント」として登録するなど、メンバーの許可を管理する。監査人を、台帳への問い合わせのみに制限することができ、一方、特定の種類のチェーンコードのデプロイ、呼び出し、および問い合わせを行うための権限をクライアントに与えることができる。

【００６０】

ブロックチェーン開発者３３０は、チェーンコードおよびクライアント側のアプリケーションを書き込む。ブロックチェーン開発者３３０は、インターフェイスを介して、チェーンコードをネットワークに直接デプロイすることができる。従来のデータ・ソース３３２からの認証情報をチェーンコードに含めるために、開発者３３０は、帯域外接続を使用してデータにアクセスすることができる。この例では、ブロックチェーン・ユーザ３２２は、ピア・ノード３３４を介してネットワークに接続する。ピア・ノード３３４は、いずれかのトランザクションを開始する前に、ユーザの登録およびトランザクションの証明書を認証機関３３６から取得する。場合によっては、ブロックチェーン・ユーザは、許可型ブロックチェーン３２４上でトランザクションを実行するために、それらのデジタル証明書を所有しなければならない。一方、チェーンコードを利用しようとしているユーザは、従来のデータ・ソース３３２上のそれらのユーザの認証情報を検証することが必要になることがある。ユーザの権限付与を確認するために、チェーンコードは、従来の処理プラットフォーム３３８を介して、このデータへの帯域外接続を使用することができる。

【００６１】

一部の実施形態では、本明細書におけるブロックチェーンは、許可なしブロックチェーンであってよい。参加するために許可を必要とする許可型ブロックチェーンとは対照的に、誰でも許可なしブロックチェーンに参加することができる。例えばユーザは、許可なしブロックチェーンに参加するために、個人のアドレスを作成し、トランザクションをサブミットすることによって、したがってエントリを台帳に追加することによって、ネットワークとの情報のやりとりを開始してよい。さらに、すべての関係者が、ノードをシステム上で実行すること、およびトランザクションの検証に役立つようにマイニング・プロトコルを採用することを選択できる。

【００６２】

図３Ｃは、複数のノード３５４を含んでいる許可なしブロックチェーン３５２によって処理されているトランザクションのプロセス３５０を示している。送信側３５６は、許可なしブロックチェーン３５２を介して、支払いまたはその他の形態の値（例えば、証書、医療記録、契約、商品、サービス、またはデジタル・レコードにカプセル化され得る任意のその他のアセット）を受信側３５８に送信することを望んでいる。１つの実施形態では、送信側デバイス３５６および受信側デバイス３５８の各々は、トランザクション・パラメータのユーザ・インターフェイス制御および表示を提供する（ブロックチェーン３５２に関連付けられた）デジタル・ウォレットを有してよい。それに応じて、トランザクションがブロックチェーン３５２全体のノード３５４にブロードキャストされる。ブロックチェーン３５２のネットワーク・パラメータに応じて、ノードが、許可なしブロックチェー

ン３５２の作成者によって確立されたルール（事前に定義されるか、または動的に割り当てられてよい）に基づいてトランザクションを検証する（３６０）。例えば、この検証は、関わっている関係者の識別情報を検証することなどを含んでよい。トランザクションは、直ちに検証されてよく、またはトランザクションは、他のトランザクションと共にキューに配置されてよく、ノード３５４は、ネットワーク・ルールのセットに基づいてトランザクションが有効であるかどうかを判定する。

【００６３】

構造３６２内で、有効なトランザクションがブロック内に形成され、ロック（ハッシュ）を使用して封印される。このプロセスは、マイニング・ノードによって、ノード３５４間で実行されてよい。マイニング・ノードは、特に、許可なしブロックチェーン３５２のブロックをマイニングして作成するために、追加のソフトウェアを利用してよい。各ブロックは、ネットワークによって合意されたアルゴリズムを使用して作成されたハッシュ（例えば、２５６ビットの数値など）によって識別されてよい。各ブロックは、ヘッダー、チェーン内の前のブロックのヘッダーのハッシュへのポインタまたは参照、および有効なトランザクションのグループを含んでよい。前のブロックのハッシュへの参照は、ブロックの安全な独立したチェーンの作成に関連付けられる。

【００６４】

ブロックをブロックチェーンに追加できるようになる前に、ブロックの妥当性が確認されなければならない。許可なしブロックチェーン３５２の妥当性確認は、ブロックのヘッダーから得られたパズルに対する解であるプルーフ・オブ・ワーク（ＰｏＷ）を含んでよい。図３Ｃの例には示されていないが、ブロックの妥当性確認ための別のプロセスは、プルーフ・オブ・ステークである。アルゴリズムが、数学問題を解くマイナーに報酬を与えるプルーフ・オブ・ワークとは異なり、プルーフ・オブ・ステークでは、ウェルス（「ステーク」としても定義される）に応じて、新しいブロックの作成者が確定的方法で選択される。その後、選択されたノードによって、同様の証明が実行される。

【００６５】

マイニング３６４で、ノードは、解がネットワーク全体にわたるターゲットを満たすまで、１つの変数に対して漸進的な変更を行うことによって、ブロックを解こうとする。これによってＰｏＷを作成し、それによって、正しい答えを保証する。言い換えると、可能性のある解は、計算リソースが問題を解くことにおいて消耗されたということを証明しなければならない。一部の種類の許可なしブロックチェーンでは、マイナーに、ブロックを正しくマイニングしたことに対する報酬として価値（例えば、コインなど）が与えられることがある。

【００６６】

ここで、攻撃者が、１つのブロックの変更を受け入れるために、その後のすべてのブロックを変更しなければならないため、ＰｏＷプロセスは、ブロックの変更と共に、ブロックチェーンの変更を極めて困難にする。さらに、新しいブロックがマイニングされるにつれて、ブロックを変更することの困難さが増大し、その後のブロックの数が増加する。配布３６６で、正常に妥当性が確認されたブロックが、許可なしブロックチェーン３５２全体に配布され、すべてのノード３５４が、そのブロックを、許可なしブロックチェーン３５２の監査可能な台帳であるマジョリティ・チェーン（ｍａｊｏｒｉｔｙ ｃｈａｉｎ）に追加する。さらに、送信側３５６によってサブミットされたトランザクションにおける価値が、受信側デバイス３５８のデジタル・ウォレットに預け入れられるか、またはその他の方法で転送される。

【００６７】

図４Ａは、実施形態例に従って、署名者組織をランダムに選択することにおいて使用するために、ブロックチェーン４１０からハッシュを取り出すプロセス４００Ａを示している。図４Ａを参照すると、ブロックチェーン４１０上の格納のためにトランザクションをサブミットしたいクライアント４２０によって、ランダムなピア選択プロセスが実行される。クライアント４２０の代わりに、ピア・ノードまたはその他のサービスによってラン

ダムな組織選択プロセスが実行されてよいということも、理解されるべきである。ここで、クライアント４２０は、１つまたは複数のブロック（およびブロック・ハッシュ）を、ブロックチェーン４１０を管理するブロックチェーン・ネットワークのピア・ノード（図示されていない）または順序付けサービス（図示されていない）から取り出してよい。ランダムなピア選択プロセスは、ブロックチェーン４１０上のブロックのサブセットを指定する制約を含んでよく、このサブセットからブロック・ハッシュが取り出されてよい。言い換えると、この制約（本明細書では、ターゲット間隔制約とも呼ばれる）は、ブロックチェーンに直前に追加された既定の数のブロック（ブロック間隔値４１２）を指定してよい。この例では、ブロック間隔値４１２は５に等しい（例えば、Ｔ＝５）。したがって、ブロック・ハッシュは、ブロックチェーン台帳に追加された最後の５個のブロック内を含む１つまたは複数のブロックから取り出されなければならない。

【００６８】

この例では、クライアント４２０は、ブロック間隔４１２に含まれているブロックのいずれかからブロック・ハッシュを選択してよい。場合によっては、クライアント４２０は、ブロックチェーン４１０に直前に追加されたブロックを自動的に選択してよいが、実施形態はこれに限定されない。クライアント４２０が、ブロック間隔４１２内からブロックを選択したことを検証するために、クライアント４２０は、ブロックチェーン台帳の現在の高さ（ｉ）をブロック間隔値４１２（Ｔ）で割った値に等しい完全性値をサブミットしてよい。ブロックチェーン台帳の高さが５０であり（例えば、Ｈ＝５０）、ブロック間隔値が５である（例えば、Ｔ＝５）場合、完全性値は（Ｈ／Ｔ）＝（５０／５）＝１０になる。図４Ｂは、図４Ａのクライアント４２０によって選択されたブロックのブロック・ハッシュ４３０を示している。ここで、ブロック・ハッシュ４３０は、ＳＨＡ２５６ハッシュなどの文字および数字の２５６ビットを含んでいる。このハッシュ値４３０は、ブロック・ハッシュ４３０の値に基づいてハッシュ値４３０を疑似２進乱数４４０に変換する２進乱数発生器のシードであってよい。２進乱数は、図４Ｃの例でさらに説明されるように、署名者ピアを識別するために使用され得る。

【００６９】

図４Ｂを参照すると、一意の識別子をピア組織に割り当てるプロセスが示されている。この例では、ブロックチェーン・ネットワークが１６（例えば、Ｎ＝１６）個のピア組織を含んでいる。各ピアに、一意の識別子が割り当てられてよい。したがって、一意のＩＤ４５０の表に示されているように、１６個の組織に、０～Ｎ－１の値が割り当てられてよい。この例では、一意のＩＤ４５０の各々が、１０進数値として表されているが、２進数値として表されてもよい。

【００７０】

図４Ｃは、実施形態例に従って、２進乱数４４０を、ブロックチェーン内の組織の数に基づくサイズを有する２進ビット・セグメント（binary bit segments）４４１に分割し、２進ビット・セグメント４４１に基づいて署名者ノードを識別する、プロセス４００Ｃを示している。この例では、乱数４４０は（シードとして使用されるハッシュ値４３０と同じ）２５６ビットを有している。組織を識別するために、クライアント４２０は、ブロックチェーン・ネットワーク内の組織の数に基づいて、２進乱数４４０をより小さいチャンクまたはサイズのビットにセグメント化してよい。例えば、対数関数ｌｏｇ２（Ｎ）ビットが２進ビット・セグメント４４１のサイズを決定してよい。この例では、ビット・セグメント４４１に、ｌｏｇ２（１６）＝４ビットのサイズが与えられる。

【００７１】

ビット・セグメント４４１の２進数は、ピア組織の一意のＩＤ４５０のうちの１つにマッピングされ得る１０進数値に変換されてよい。例えば、最初のビット・セグメントが「１０１１」の乱数を含み、この乱数が、ピア組織１２の一意のＩＤにマッピングされる１１の１０進数値に変換され得る。２進セグメントを１０進数値に変換し、ピア組織の一意のＩＤにマッピングするこのプロセスは、署名ポリシーを満たすための十分な一意のＩＤ（および対応する組織）が識別されるまで、繰り返され得る。この例では、必要な署名者

の数はＫ＝４である。その結果、組織１２、組織９、組織１１、および組織６が、２進乱数４４０の最初の４つのセグメントから識別される。したがって、プロセスが終了してよく、クライアント４２０は、トランザクション提案を、ランダムな選択プロセスから識別された４つの組織（１２、９、１１、および６）の各々のノードにサブミットすることができる。

【００７２】

１０進数値への２進ビット・セグメントの変換が、以前のビット・セグメントの重複する一意のＩＤへのマッピングを引き起こす場合、ビット・セグメントが破棄され得る。システムは、取得され得る最初の４つの異なる一意のＩＤを探し続ける。クライアント４２０が２進ビット・セグメントを使い果たした場合（これは、必要なノード／署名者の数の方がより大きい場合に起こることが多い）、クライアント４２０は、ブロック間隔４１２から別のブロック・ハッシュを取得するか、または現在のハッシュを再びハッシュし、新しい乱数を生成して、必要な残りの数の署名者ノードを識別するためのプロセスを再開してよい。

【００７３】

図５は、実施形態例に従って、署名者になるべきピア組織をランダムに選択する方法５００を示している。図５を参照すると、５１０で、この方法は、ブロックチェーンに格納されたデータ・ブロックのブロック・ハッシュを取り出すことを含んでよい。例えば、この方法を実行しているクライアント、スマート・コントラクト、ブロックチェーン・ピア・ノードなどのシステムは、直前に格納された既定の量のブロックからブロック・ハッシュを選択することに制限されてよい。これらのブロックの間隔は、ブロック間隔値と呼ばれてよい。例えば、ブロック間隔値が１０である場合、この方法は、ブロックチェーンに格納された最後の１０個のブロックのうちの１つまたは複数のブロックのみからブロック・ハッシュを選択してよい。そうすることで、セキュリティは、古いハッシュを使用している攻撃者から保護する。

【００７４】

５２０で、この方法は、ブロック・ハッシュの値に基づいて、署名者になるべきピア組織のサブセットをブロックチェーンのブロックチェーン・ネットワークからランダムに決定することを含んでよい。例えば、ランダムに決定することは、ブロック・ハッシュを２進乱数に変換することと、２進乱数を複数のビット・セグメントに分割することと、複数のビット・セグメントのうちの１つまたは複数に基づいて、ピア組織のサブセットを識別することとを含んでよい。

【００７５】

５３０で、この方法は、ブロックチェーン格納要求を、クライアントからランダムに決定された署名者ピア・ノードのサブセットに送信することを含んでよい。さらに、５４０で、この方法は、ランダムに決定された署名者ピア・ノードのサブセットからのシミュレートされた応答を、格納要求提案に収集することを含んでよい。図５に示されていないが、一部の実施形態では、この方法は、ランダムに決定された署名者ピア・ノードのサブセットから収集された、シミュレートされた応答を含んでいる格納要求提案を、ブロックチェーンの順序付けノード・サービスに送信することをさらに含んでよい。

【００７６】

さまざまな実施形態によれば、識別することは、ブロックチェーン・ネットワークに含まれているピア・ノードの数に基づいて、複数のピア・ノードのうちの各ピア・ノードに一意の識別子を割り当てることと、複数のビット・セグメントからのビット・セグメントを１０進数値に変換することと、ビット・セグメントの１０進数値をピア・ノードのうちの１つの一意の識別子にマッピングすることとを含んでよい。ビット・セグメントは、２進乱数シーケンスからスライスされた特定のサイズのビットであってよい。次に、システムは、どの組織が一意の識別子に対応するかを識別し、その組織からのピアをトランザクションの署名者ノードとして選択してよい。一部の実施形態では、ブロックチェーン・ネットワークに含まれている組織の数に基づいて、ビット・セグメントのサイズが選択され

てよい。

【００７７】

一部の実施形態では、この方法は、ブロックチェーン上の最新のブロックのサブセットを識別するブロック間隔値を決定することをさらに含んでよく、このサブセットからブロック・ハッシュが取り出され得る。一部の実施形態では、この方法は、ブロック間隔値によって識別された最新のブロックのサブセット内のブロックを選択することと、ブロック間隔値によって識別されたブロックのサブセット内の選択されたブロックからブロック・ハッシュを取り出すこととをさらに含んでよい。一部の実施形態では、この方法は、ブロックチェーンの現在の高さおよびブロック間隔値に基づいて完全性値を生成することと、完全性値を格納要求提案内に格納することとをさらに含んでよい。格納要求提案は、順序付けノードに送信されてよく、順序付けノードは、格納要求提案をデータ・ブロックに含め、このデータ・ブロックを、ブロックチェーンのコミット・ノードに配布し、コミット・ノードでは、データ・ブロックがブロックチェーン台帳に格納され得る。

【００７８】

さまざまな実施形態によれば、方法５００は、図５に明示的に示されていない追加のステップを含んでよい。例えば、クライアントは、応答をトランザクション提案にまとめ、トランザクション提案をブロックチェーンの順序付けサービスに送信してよい。順序付けサービスは、トランザクション提案をブロックに追加し、このブロックをブロックチェーン・ネットワーク内のすべてのコミット・ピア・ノードに送信してよい。それに応じて、コミット・ピアの各々は、ブロックに含まれているトランザクションが、ランダムな選択プロセスに従ってピアによってシミュレートされ、署名されたかどうかを検証してよい。チェックが成功した場合、コミット・ピアによってトランザクションが台帳に追加され、そうでない場合、トランザクションが追加されない。

【００７９】

図６Ａは、実施形態例に従ってさまざまな動作を実行するように構成された物理的インフラストラクチャ６１０を含んでいる例示的なシステム６００を示している。図６Ａを参照すると、物理的インフラストラクチャ６１０は、モジュール６１２およびモジュール６１４を含んでいる。モジュール６１４は、実施形態例のいずれかに含まれる（モジュール６１２内の）動作ステップ６０８のいずれかを実行してよい、ブロックチェーン６２０およびスマート・コントラクト６３０（ブロックチェーン６２０に存在してよい）を含んでいる。ステップ／動作６０８は、説明されたか、または図に示された実施形態のうちの１つまたは複数を含んでよく、１つまたは複数のスマート・コントラクト６３０またはブロックチェーン６２０あるいはその両方から書き込まれるか、または読み取られる、出力されたか、または書き込まれた情報を表してよい。物理的インフラストラクチャ６１０、モジュール６１２、およびモジュール６１４は、１つまたは複数のコンピュータ、サーバ、プロセッサ、メモリ、または無線通信デバイス、あるいはその組み合わせを含んでよい。さらに、モジュール６１２およびモジュール６１４は同じモジュールであってよい。

【００８０】

図６Ｂは、実施形態例に従ってさまざまな動作を実行するように構成された別の例示的なシステム６４０を示している。図６Ｂ参照すると、システム６４０はモジュール６１２および６１４を含んでいる。モジュール６１４は、実施形態例のいずれかに含まれる（モジュール６１２内の）動作ステップ６０８のいずれかを実行してよい、ブロックチェーン６２０およびスマート・コントラクト６３０（ブロックチェーン６２０に存在してよい）を含んでいる。ステップ／動作６０８は、説明されたか、または図に示された実施形態のうちの１つまたは複数を含んでよく、１つまたは複数のスマート・コントラクト６３０またはブロックチェーン６２０あるいはその両方から書き込まれるか、または読み取られる、出力されたか、または書き込まれた情報を表してよい。物理的インフラストラクチャ６１０、モジュール６１２、およびモジュール６１４は、１つまたは複数のコンピュータ、サーバ、プロセッサ、メモリ、または無線通信デバイス、あるいはその組み合わせを含んでよい。さらに、モジュール６１２およびモジュール６１４は同じモジュールであってよ

い。

【００８１】

図６Ｃは、実施形態例に従って、契約当事者間でのスマート・コントラクトの構成、およびブロックチェーンに対してスマート・コントラクトの条件を実施するように構成された仲介サーバを利用するように構成された例示的なシステムを示している。図６Ｃを参照すると、構成６５０は、通信セッション、アセット転送セッション、あるいはプロセスまたは手順を表してよく、これらは、１つまたは複数のユーザ・デバイス６５２または６５６あるいはその両方を明示的に識別するスマート・コントラクト６３０によって動作させられる。スマート・コントラクトの実行の、実行、動作、および結果は、サーバ６５４によって管理されてよい。スマート・コントラクト６３０の内容は、スマート・コントラクト・トランザクションの関係者である実体６５２および６５６のうちの１つまたは複数によるデジタル署名を要求してよい。スマート・コントラクトの実行結果は、ブロックチェーン・トランザクションとしてブロックチェーン６２０に書き込まれてよい。スマート・コントラクト６３０は、１つまたは複数のコンピュータ、サーバ、プロセッサ、メモリ、または無線通信デバイス、あるいはその組み合わせに存在してよい、ブロックチェーン６２０に存在する。

【００８２】

図６Ｄは、実施形態例に従って、ブロックチェーンを含んでいるシステム６６０を示している。図６Ｄの例を参照すると、アプリケーション・プログラミング・インターフェイス（ＡＰＩ）ゲートウェイ６６２が、ブロックチェーンの論理（例えば、スマート・コントラクト６３０またはその他のチェーンコード）およびデータ（例えば、分散型台帳など）にアクセスするための共通インターフェイスを提供する。この例では、ＡＰＩゲートウェイ６６２は、１つまたは複数の実体６５２および６５６をブロックチェーン・ピア（すなわち、サーバ６５４）に接続することによってブロックチェーンに対してトランザクション（呼び出し、問い合わせなど）を実行するための共通インターフェイスである。ここで、サーバ６５４は、世界状態および分散型台帳のコピーを保持するブロックチェーン・ネットワークのピア・コンポーネントであり、これらのコピーは、クライアント６５２および６５６が世界状態に関するデータを問い合わせること、およびトランザクションをブロックチェーン・ネットワークにサブミットすることを可能にし、スマート・コントラクト６３０および署名ポリシーに応じて、署名ピアがスマート・コントラクト６３０を実行する。

【００８３】

前述の実施形態は、ハードウェアにおいて、プロセッサによって実行されるコンピュータ・プログラムにおいて、ファームウェアにおいて、またはこれらの組み合わせにおいて実装されてよい。コンピュータ・プログラムは、ストレージ媒体などのコンピュータ可読媒体に具現化されてよい。例えば、コンピュータ・プログラムは、ランダム・アクセス・メモリ（ＲＡＭ：random access memory）、フラッシュ・メモリ、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）、電子的消去可能プログラマブル読み取り専用メモリ（ＥＥＰＲＯＭ：electrically erasable programmable read-only memory）、レジスタ、ハード・ディスク、取り外し可能なディスク、コンパクト・ディスク読み取り専用メモリ（ＣＤ－ＲＯＭ：compact disk read-only memory）、または従来技術において知られた任意のその他の形態のストレージ媒体に存在してよい。

【００８４】

例示的なストレージ媒体は、プロセッサがストレージ媒体から情報を読み取り、ストレージ媒体に情報を書き込むことができるように、プロセッサに結合されてよい。代替方法では、ストレージ媒体はプロセッサと一体であってよい。プロセッサおよびストレージ媒体は、特定用途向け集積回路（ＡＳＩＣ：application specific integrated circuit）に存在してよい。代替方法では、プロセッサおよびストレージ媒体は、個別のコンポ

ーネントとして存在してよい。

【００８５】

図７Ａは、実施形態例に従って、分散型台帳７２０に追加されている新しいブロックのプロセス７００を示しており、図７Ｂは、実施形態例に従って、ブロックチェーンの新しいデータ・ブロック構造７３０の内容を示している。図７Ａを参照すると、クライアント（図示されていない）は、トランザクションをブロックチェーン・ノード７１１、７１２、または７１３、あるいはその組み合わせにサブミットしてよい。クライアントは、ブロックチェーン７２０に対する活動を規定するための、いずれかのソースから受信された命令であってよい。一例として、クライアントは、ブロックチェーンのトランザクションを提案するデバイス、人、または実体などの要求者の代わりに動作するアプリケーションであってよい。複数のブロックチェーン・ピア（例えば、ブロックチェーン・ノード７１１、７１２、および７１３）が、ブロックチェーン・ネットワークの状態および分散型台帳７２０のコピーを維持してよい。クライアントによって提案されたトランザクションをシミュレートして署名する署名ピア、および署名を検証し、トランザクションの妥当性を確認し、トランザクションを分散型台帳７２０にコミットするコミット・ピアを含む、さまざまな種類のブロックチェーン・ノード／ピアが、ブロックチェーン・ネットワーク内に存在してよい。この例では、ブロックチェーン・ノード７１１、７１２、および７１３は、署名者ノード、コミッター・ノード（committer node）、あるいはその両方の役割を実行してよい。

【００８６】

分散型台帳７２０は、ブロック内の変更不可能な順序付けられたレコードを格納するブロックチェーン、およびブロックチェーン７２２の現在の状態を維持する状態データベース７２４（現在の世界状態）を含む。１つのチャネルにつき１つの分散型台帳７２０が存在してよく、各ピアが、そのピアがメンバーであるチャネルごとに、分散型台帳７２０のそれ自身のコピーを維持する。ブロックチェーン７２２は、ハッシュ・リンク・ブロックとして構造化されたトランザクション・ログであり、各ブロックがＮ個のトランザクションのシーケンスを含む。ブロックは、図７Ｂに示されているコンポーネントなどの、さまざまなコンポーネントを含んでよい。ブロックのリンク（図７Ａの矢印によって示されている）は、前のブロックのヘッダーのハッシュを、現在のブロックのブロック・ヘッダー内に追加することによって生成されてよい。このようにして、ブロックチェーン７２２上のすべてのトランザクションが、順序付けられ、暗号によって一緒にリンクされ、ハッシュ・リンクを壊さずにブロックチェーン・データを改ざんすることを防ぐ。さらに、これらのリンクのため、ブロックチェーン７２２内の最新のブロックが、その前に来たすべてのトランザクションを表す。ブロックチェーン７２２は、追加専用のブロックチェーンのワークロードをサポートするピアのファイル・システム（ローカルまたは取り付けられたストレージ）に格納されてよい。

【００８７】

ブロックチェーン７２２および分散型台帳７２０の現在の状態が、状態データベース７２４に格納されてよい。ここで、現在の状態データは、ブロックチェーン７２２のチェーン・トランザクション・ログにこれまで含まれたすべてのキーの最新の値を表す。チェーンコード呼び出しは、状態データベース７２４内の現在の状態に対してトランザクションを実行する。それらのチェーンコードの相互作用を極めて効率的にするために、すべてのキーの最新の値が状態データベース７２４に格納される。状態データベース７２４は、ブロックチェーン７２２のトランザクション・ログへのインデックス付きビューを含んでよく、したがって、いつでもチェーンから再生成され得る。状態データベース７２４は、ピアの起動時に、トランザクションが受け取られる前に、自動的に回復されてよい（または必要な場合に生成されてよい）。

【００８８】

署名ノードは、トランザクションをクライアントから受信し、シミュレーション結果に基づいてトランザクションに署名する。署名ノードは、トランザクション提案をシミュレ

ートするスマート・コントラクトを保持する。署名ノードがトランザクションに署名するときに、署名ノードは、シミュレートされたトランザクションの署名を示す署名ノードからクライアント・アプリケーションへの署名された応答である、トランザクションの署名を生成する。トランザクションに署名する方法は、チェーンコード内で指定されることがある署名ポリシーによって決まる。署名ポリシーの例は、「署名ピアの大部分がトランザクションに署名しなければならない」である。異なるチャネルは、異なる署名ポリシーを有してよい。署名されたトランザクションは、クライアント・アプリケーションによって順序付けサービス７１０に転送される。

【００８９】

順序付けサービス７１０は、署名されたトランザクションを受け取り、それらをブロック内に順序付けし、ブロックをコミット・ピアに配信する。例えば、順序付けサービス７１０は、トランザクションのしきい値に達したか、タイマーがタイムアウトするか、または別の条件の場合に、新しいブロックを開始してよい。図７Ａの例では、ブロックチェーン・ノード７１２は、ブロックチェーン７２０に格納するための新しいデータの新しいデータ・ブロック７３０を受信したコミット・ピアである。ブロックチェーン内の第１のブロックは、ブロックチェーン、ブロックチェーンのメンバー、格納されたデータなどに関する情報を含んでいるジェネシス・ブロックと呼ばれてよい。

【００９０】

順序付けサービス７１０は、順序付けノードのクラスタで構成されてよい。順序付けサービス７１０は、トランザクション、スマート・コントラクトを処理することも、共有台帳を維持することもない。むしろ、順序付けサービス７１０は、署名されたトランザクションを受け取ってよく、それらのトランザクションが分散型台帳７２０にコミットされる順序を指定する。ブロックチェーン・ネットワークのアーキテクチャは、「順序付け」の特定の実装（例えば、Ｓｏｌｏ、Ｋａｆｋａ、ＢＦＴなど）が着脱可能なコンポーネントになるように設計されてよい。

【００９１】

トランザクションは、一貫性のある順序で分散型台帳７２０に書き込まれる。トランザクションの順序は、トランザクションがネットワークにコミットされるとき状態データベース７２４に対する更新が有効であることを保証するように確立される。暗号パズルを解くことまたはマイニングによって順序付けが発生する暗号通貨ブロックチェーン・システム（例えば、ビットコインなど）とは異なり、この例では、分散型台帳７２０の関係者が、そのネットワークに最も適した順序付けメカニズムを選択してよい。

【００９２】

順序付けサービス７１０は、新しいデータ・ブロック７３０を初期化し、新しいデータ・ブロック７３０がコミット・ピア（例えば、ブロックチェーン・ノード７１１、７１２、および７１３）にブロードキャストされてよい。それに応じて、各コミット・ピアは、読み取りセットおよび書き込みセットが状態データベース７２４内の現在の世界状態にまだ一致することをチェックして確認することによって、新しいデータ・ブロック７３０内のトランザクションの妥当性を確認する。特に、コミット・ピアは、署名者がトランザクションをシミュレートしたときに存在していた読み取られたデータが、状態データベース７２４内の現在の世界状態と同一であるかどうかを判定することができる。コミット・ピアがトランザクションの妥当性を確認した場合、トランザクションが分散型台帳７２０のブロックチェーン７２２に書き込まれ、状態データベース７２４が、読み取り／書き込みセットからの書き込みデータに更新される。トランザクションが失敗した場合、すなわち、コミット・ピアが、読み取り／書き込みセットが状態データベース７２４内の現在の世界状態に一致しないということを検出した場合、ブロック内に順序付けられたトランザクションは、そのブロックにまだ含まれるが、無効としてマーク付けされ、状態データベース７２４が更新されない。

【００９３】

図７Ｂを参照すると、分散型台帳７２０のブロックチェーン７２２に格納された新しい

データ・ブロック７３０（データ・ブロックとも呼ばれる）が、ブロック・ヘッダー７４０、ブロック・データ７５０、およびブロック・メタデータ７６０などの、複数のデータ・セグメントを含んでよい。図７Ｂに示された新しいデータ・ブロック７３０およびその内容などの、さまざまな示されたブロックおよびそれらの内容が、例にすぎず、実施形態例の範囲を制限するよう意図されていないということが、理解されるべきである。新しいデータ・ブロック７３０は、ブロック・データ７５０内のＮ個（例えば、１、１０、１００、５００、１０００、２０００、３０００など）のトランザクションのトランザクション情報を格納してよい。新しいデータ・ブロック７３０は、（例えば、図７Ａのブロックチェーン７２２上の）前のブロックへのリンクをブロック・ヘッダー７４０内に含んでもよい。特に、ブロック・ヘッダー７４０は、前のブロックのヘッダーのハッシュを含んでよい。ブロック・ヘッダー７４０は、新しいデータ・ブロック７３０の一意のブロック番号、ブロック・データ７５０のハッシュなどを含んでもよい。新しいデータ・ブロック７３０のブロック番号は、一意であり、０から開始する漸進的／連続的順序などのさまざまな順序で割り当てられてよい。

【００９４】

ブロック・データ７５０は、新しいデータ・ブロック７３０内に記録された各トランザクションのトランザクション情報を格納してよい。例えば、トランザクション・データは、トランザクションの種類、バージョン、タイムスタンプ、分散型台帳７２０のチャネルＩＤ、トランザクションＩＤ、エポック、ペイロードの可視性、チェーンコード・パス（トランザクションのデプロイ）、チェーンコード名、チェーンコードのバージョン、入力（チェーンコードおよび関数）、公開鍵および証明書などのクライアント（作成者）の識別、クライアントの署名、署名者の識別情報、署名者の署名、提案のハッシュ、チェーンコード・イベント、応答の状態、名前空間、書き込みセット（トランザクションによって読み取られたキーおよびバージョンのリストなど）、書き込みセット（キーと値のリストなど）、開始キー、終了キー、キーのリスト、マークル・ツリー・クエリ・サマリー（Merkle tree query summary）などのうちの１つまたは複数を含んでよい。トランザクション・データは、Ｎ個のトランザクションの各々に格納されてよい。

【００９５】

一部の実施形態では、ブロック・データ７５０に含まれている各トランザクションが、トランザクションをサブミットしたピア・ノードのブロック高さをブロックチェーンのブロック間隔値で割った値に等しいブロック間隔値７５２を格納してもよい。ブロック間隔値７５２は、ブロック間隔値７５２内にあるブロックからのブロック・ハッシュ値を使用して、ランダム化された署名者ノード選択プロセスが実行されたことを検証するために、使用され得る。ブロック間隔値７５２は、本明細書で説明されたか、または示された、ステップ、特徴、プロセス、または動作、あるいはその組み合わせのうちの１つまたは複数を含む。それに応じて、ブロック間隔値７５２が、分散型台帳７２０上のブロックの変更不可能なログに格納され得る。ブロック間隔値７５２をブロックチェーンに格納する利点の一部は、本明細書で開示されて示されたさまざまな実施形態に反映され、ランダムなピア選択プロセスの完全性を保証することを含む。

【００９６】

ブロック・メタデータ７６０は、メタデータの複数のフィールドを（例えば、バイト配列などとして）格納してよい。メタデータ・フィールドは、ブロック作成時の署名、最後の構成ブロックへの参照、ブロック内の有効なトランザクションと無効なトランザクションを識別するトランザクション・フィルタ、ブロックを順序付けた順序付けサービスの永続的な最後のオフセットなどを含んでよい。順序付けサービス７１０によって署名、最後の構成ブロック、および順序付けノードのメタデータが追加されてよい。一方、ブロックのコミッター（ブロックチェーン・ノード７１２など）は、署名ポリシー、読み取り／書き込みセットの検証などに基づいて、有効／無効情報を追加してよい。トランザクション・フィルタは、ブロック・データ７５０内のトランザクションの数に等しいサイズのバイト配列、およびトランザクションが有効／無効だったかどうかを識別する妥当性確認コー

ドを含んでよい。

【００９７】

図７Ｃは、本明細書に記載された実施形態に従って、デジタル・コンテンツのためのブロックチェーン７７０の実施形態を示している。デジタル・コンテンツは、１つまたは複数のファイルおよび関連する情報を含んでよい。これらのファイルは、媒体、画像、ビデオ、音声、テキスト、リンク、グラフィックス、アニメーション、Ｗｅｂページ、文書、またはデジタル・コンテンツのその他の形態を含んでよい。ブロックチェーンの変更不可能な追加専用の特徴は、デジタル・コンテンツの完全性、有効性、および信頼性を保護するための予防手段として役立ち、認容性ルールが適用される法的手続きにおいて、あるいは証拠が考慮されるか、またはデジタル情報の提示および使用がその他の方法で対象になる、その他の設定において、ブロックチェーンの使用を適切にする。この場合、デジタル・コンテンツはデジタル証拠と呼ばれることがある。

【００９８】

ブロックチェーンは、さまざまな方法で形成されてよい。１つの実施形態では、デジタル・コンテンツは、ブロックチェーン自体に含まれ、ブロックチェーン自体からアクセスされてよい。例えば、ブロックチェーンの各ブロックは、参照情報（例えば、ヘッダー、値など）のハッシュ値を、関連するデジタル・コンテンツと共に格納してよい。その後、ハッシュ値および関連するデジタル・コンテンツは、一緒に暗号化されてよい。したがって、各ブロックのデジタル・コンテンツは、ブロックチェーン内の各ブロックを復号することによってアクセスされてよく、各ブロックのハッシュ値は、前のブロックを参照するための基礎として使用されてよい。これは、次のように示されてよい。

ブロック１　ブロック２・・・・ブロックＮ
ハッシュ値１　ハッシュ値２　ハッシュ値Ｎ
デジタル・コンテンツ１　デジタル・コンテンツ２　デジタル・コンテンツＮ

【００９９】

１つの実施形態では、デジタル・コンテンツがブロックチェーンに含まれなくてよい。例えば、ブロックチェーンは、デジタル・コンテンツを含んでいない各ブロックの内容の暗号化されたハッシュを格納してよい。デジタル・コンテンツは、元のファイルのハッシュ値に関連して、別のストレージ領域またはメモリ・アドレスに格納されてよい。他のストレージ領域は、ブロックチェーンを格納するために使用されるストレージ・デバイスと同じストレージ・デバイスであってよく、または異なるストレージ領域もしくは分離したリレーショナル・データベースであってもよい。各ブロックのデジタル・コンテンツは、対象のブロックのハッシュ値を取得するか、または問い合わせ、次に、実際のデジタル・コンテンツに対応して格納されているハッシュ値をストレージ領域内で検索することによって、参照またはアクセスされてよい。この動作は、例えば、データベース・ゲートキーパーによって実行されてよい。これは、次のように示されてよい。

ブロックチェーン　ストレージ領域
ブロック１のハッシュ値　ブロック１のハッシュ値・・・内容
・　・
・　・
・　・
ブロックＮのハッシュ値　ブロックＮのハッシュ値・・・内容

【０１００】

図７Ｃの実施形態例では、ブロックチェーン７７０は、順序付けられたシーケンスで暗号によってリンクされた複数のブロック778_1、778_2、．．．778_Nを含んでおり、Ｎ≧１である。ブロック778_1、778_2、．．．778_Nをリンクするための使用される暗号化は、複数の鍵付きハッシュ関数または鍵なしハッシュ関数のいずれかであってよい。１つの実施形態では、ブロック778_1、778_2、．．．778_Nは、ブロック内の情報に基づいて入力からｎビットの英数字出力を生成するハッシュ関数の対象になる（ｎは２５６または別の数である）。そのようなハッシュ関数の例としては、ＳＨＡ

型（ＳＨＡは、セキュア・ハッシュ・アルゴリズム（Secured Hash Algorithm）を表す）アルゴリズム、マークル・ダンガード・アルゴリズム、ＨＡＩＦＡアルゴリズム、マークル・ツリー・アルゴリズム、ノンスに基づくアルゴリズム、および非衝突耐性ＰＲＦアルゴリズムが挙げられるが、これらに限定されない。別の実施形態では、ブロック７７８$_1$、７７８$_2$、．．．７７８$_N$は、ハッシュ関数とは異なる関数によって、暗号によってリンクされてよい。例示の目的で、以下では、ハッシュ関数（例えば、ＳＨＡ－２）を参照して説明が行われる。

【０１０１】

ブロックチェーン内のブロック７７８$_1$、７７８$_2$、．．．７７８$_N$の各々は、ヘッダー、ファイルのバージョン、および値を含む。ヘッダーおよび値は、ブロックチェーン内のハッシュ処理の結果として、ブロックごとに異なる。１つの実施形態では、値がヘッダーに含まれてよい。以下でさらに詳細に説明されるように、ファイルのバージョンは、元のファイルであるか、または元のファイルの異なるバージョンであってよい。

【０１０２】

ブロックチェーン内の最初のブロック７７８$_1$は、ジェネシス・ブロックと呼ばれ、ヘッダー７７２$_1$、元のファイル７７４$_1$、および初期値７７６$_1$を含んでいる。ジェネシス・ブロックに使用される（実際には、その後のすべてのブロックにおいて使用される）ハッシュ処理方式は、変化してよい。例えば、最初のブロック７７８$_1$内のすべての情報が一緒に同時にハッシュされてよく、または最初のブロック７７８$_1$内の情報の各々または一部が別々にハッシュされ、その後、別々にハッシュされた部分のハッシュが実行されてよい。

【０１０３】

ヘッダー７７２$_1$は、１つまたは複数の初期パラメータを含んでよく、初期パラメータは、例えば、バージョン番号、タイムスタンプ、ノンス、ルート情報、難易度、合意プロトコル、期間、媒体形式、ソース、記述的キーワード、あるいは元のファイル７７４$_1$もしくはブロックチェーンまたはその両方に関連付けられたその他の情報、あるいはその組み合わせを含んでよい。ヘッダー７７２$_1$は、自動的に（例えば、ブロックチェーン・ネットワーク管理ソフトウェアによって）生成されるか、またはブロックチェーンの参加者によって手動で生成されてよい。ブロックチェーン内の他のブロック７７８$_2$～７７８$_N$内のヘッダーとは異なり、ジェネシス・ブロック内のヘッダー７７２$_1$は、単に前のブロックが存在しないため、前のブロックを参照しない。

【０１０４】

ジェネシス・ブロック内の元のファイル７７４$_1$は、例えば、ブロックチェーンに含まれる前の処理を伴うか、または伴わずに、デバイスによって捕捉されたデータであってよい。元のファイル７７４$_1$は、システムのインターフェイスを介して、デバイス、媒体ソース、またはノードから受信される。元のファイル７７４$_1$はメタデータに関連付けられ、メタデータは、例えば、ユーザ、デバイス、またはシステム・プロセッサあるいはその組み合わせによって、手動または自動のいずれかで、生成されてよい。メタデータは、元のファイル７７４$_1$に関連して、最初のブロック７７８$_1$に含まれてよい。

【０１０５】

ジェネシス・ブロック内の値７７６$_1$は、元のファイル７７４$_1$の１つまたは複数の一意の属性に基づいて生成された初期値である。１つの実施形態では、１つまたは複数の一意の属性は、元のファイル７７４$_1$のハッシュ値、元のファイル７７４$_1$のメタデータ、およびファイルに関連付けられたその他の情報を含んでよい。１つの実装では、初期値７７６$_1$は、以下の一意の属性に基づいてよい。

１）ＳＨＡ－２によって元のファイルに対して計算されたハッシュ値
２）発信デバイスＩＤ
３）元のファイルの開始タイムスタンプ
４）元のファイルの初期ストレージ位置
５）元のファイルおよび関連するメタデータを現在制御するためのソフトウェアのブロ

ックチェーン・ネットワーク・メンバーＩＤ

【０１０６】

ブロックチェーン内の他のブロック７７８$_2$～７７８$_N$も、ヘッダー、ファイル、および値を含む。しかし、最初のブロック７７２$_1$とは異なり、他のブロック内のヘッダー７７２$_2$～７７２$_N$の各々は、直前のブロックのハッシュ値を含む。直前のブロックのハッシュ値は、単に前のブロックのヘッダーのハッシュであってよく、または前のブロック全体のハッシュ値であってよい。先行するブロックのハッシュ値を残りのブロックの各々に含めることによって、矢印７８０によって示されているように、Ｎ番目のブロックからジェネシス・ブロック（および関連する元のファイル）まで戻りブロックごとのトレースを実行することができ、監査可能かつ変更不可能な証拠保全を確立する。

【０１０７】

他のブロック内のヘッダー７７２$_2$～７７２$_N$の各々は、一般に、他の情報（例えば、バージョン番号、タイムスタンプ、ノンス、ルート情報、難易度、合意プロトコル、あるいは対応するファイルもしくはブロックチェーンまたはその両方に関連付けられたその他のパラメータまたは情報、あるいはその組み合わせ）を含んでもよい。

【０１０８】

他のブロック内のファイル７７４$_2$～７７４$_N$は、例えば実行される処理の種類に応じて、ジェネシス・ブロック内の元のファイルと同じであってよく、または元のファイルの変更されたバージョンであってよい。実行される処理の種類は、ブロックごとに変化してよい。処理は、例えば、情報を編集するか、またはその他の方法で情報の内容を変更するか、情報をファイルから取り除くか、または情報をファイルに追加するなどの、先行するブロック内のファイルの任意の変更を含んでよい。

【０１０９】

追加的または代替的に、処理は、先行するブロックからファイルを単にコピーすること、ファイルのストレージ位置を変更すること、１つまたは複数の先行するブロックからのファイルを分析すること、ファイルをあるストレージまたはメモリ位置から別のストレージまたはメモリ位置に移動すること、あるいはブロックチェーンのファイルもしくは関連するメタデータまたはその両方に対して動作を実行することを含んでよい。ファイルを分析することを含んでいる処理は、例えば、さまざまな分析、統計値、またはファイルに関連付けられたその他の情報を追加すること、含めること、またはその他の方法で関連付けることを含んでよい。

【０１１０】

他のブロック内の他のブロック７７６$_2$～７７６$_N$の各々に含まれる値は、実行された処理の結果として、一意の値であり、すべて異なっている。例えば、いずれか１つのブロック内の値は、前のブロック内の値の更新されたバージョンに対応する。この更新は、値が割り当てられたブロックのハッシュに反映される。したがって、ブロックの値は、ブロック内で何の処理が実行されたかの指示を提供し、ブロックチェーンを元のファイルまで戻りトレースすることも可能にする。このトレースは、ブロックチェーン全体を通じて、ファイルの証拠保全を確認する。

【０１１１】

例えば、ファイル内で示されている人の識別情報を保護するために、前のブロック内のファイルの一部が編集されるか、遮断されるか、または画素化される場合について考える。この場合、編集されたファイルを含んでいるブロックは、例えば、編集がどのように実行されたか、誰が編集を実行したか、編集が発生したタイムスタンプなどの、編集されたファイルに関連付けられたメタデータを含むであろう。このメタデータがハッシュされ、値を形成してよい。ブロックのメタデータが、前のブロック内の値を形成するためにハッシュされた情報と異なっているため、値は、互いに異なっており、復号されたときに回復されてよい。

【０１１２】

１つの実施形態では、次のうちのいずれか１つまたは複数が発生した場合に、現在のブ

ロックの値を形成するように、前のブロックの値が更新されてよい（例えば、新しいハッシュ値が計算されてよい）。新しいハッシュ値は、この実施形態例では、以下に示された情報のすべてまたは一部をハッシュすることによって計算されてよい。

ａ）ファイルがいずれかの方法で処理された場合（例えば、ファイルが編集されたか、コピーされたか、変更されたか、アクセスされたか、またはその他の動作が実行された場合）に、新しいＳＨＡ－２によって計算されたハッシュ値

ｂ）ファイルの新しいストレージ位置

ｃ）ファイルに関連付けられている識別された新しいメタデータ

ｄ）あるブロックチェーンの参加者から別のブロックチェーンの参加者へのファイルのアクセスまたは制御の移動

【０１１３】

図７Ｄは、１つの実施形態例に従って、ブロックチェーン７９０内のブロックの構造を表すことができるブロックの実施形態を示している。ブロック（ブロック$_i$）は、ヘッダー７７２$_i$、ファイル７７４$_i$、および値７７６$_i$を含んでいる。

【０１１４】

ヘッダー７７２$_i$は、本明細書において説明された、前のブロック（ブロック$_{i-1}$）のハッシュ値、および例えば情報の種類のいずれかであってよい、追加の参照情報（例えば、参照、特性、パラメータなどを含んでいるヘッダー情報）を含む。すべてのブロックは、当然ながらジェネシス・ブロックを除いて、前のブロックのハッシュを参照する。前のブロックのハッシュ値は、単に前のブロック内のヘッダーのハッシュであるか、またはファイルおよびメタデータを含む、前のブロック内の情報のすべてもしくは一部のハッシュであってよい。

【０１１５】

ファイル７７４$_i$は、データ１、データ２、．．．、データＮなどの複数のデータを順に含んでいる。データは、データに関連付けられた内容または特性あるいはその両方を記述するメタデータ（メタデータ１、メタデータ２、．．．、メタデータＮ）でタグ付けされる。例えば、データごとのメタデータは、データのタイムスタンプ、データのプロセス、データに示された人またはその他の内容を示しているキーワード、またはファイルの有効性および内容を全体として確立し、特に、例えば以下で説明される実施形態に関連して説明されるように、デジタル証拠を使用するのに役立つことができるその他の特徴、あるいはその組み合わせを示すための情報を含んでよい。メタデータに加えて、各データは、改ざん、ファイル内のギャップ、およびファイル全体の連続的な参照を防ぐために、前のデータへの参照（参照$_1$、参照$_2$、．．．、参照$_N$）でタグ付けされてよい。

【０１１６】

メタデータが（例えば、スマート・コントラクトを介して）データに割り当てられた後に、ハッシュを変更せずにメタデータを変更することはできず、ハッシュの変更は、無効であると容易に識別され得る。したがって、メタデータは、ブロックチェーン内の参加者による使用のためにアクセスされてよい、情報のデータ・ログを作成する。

【０１１７】

値７７６$_i$は、前に説明された情報の種類のいずれかに基づいて計算されたハッシュ値またはその他の値である。例えば、いずれかの特定のブロック（ブロック$_i$）の場合、そのブロックの値は、そのブロックに対して実行された処理（例えば、新しいハッシュ値、新しいストレージ位置、関連するファイルの新しいメタデータ、制御もしくはアクセスの移動、識別子、またはその他の動作もしくは追加される情報）を反映するように更新されてよい。各ブロック内の値が、ファイルおよびヘッダーのデータのメタデータから分離しているように示されているが、別の実施形態では、値は、このメタデータに部分的または全体的に基づいてよい。

【０１１８】

ブロックチェーン７７０が形成された後に、いずれかの時点で、ブロック全体にわたる値のトランザクション履歴に関してブロックチェーンに問い合わせることによって、ファ

イルの変更不可能な証拠保全が取得されてよい。この問い合わせ手順または追跡手順は、最後に含まれたブロック（例えば、最後の（Ｎ番目の）ブロック）の値を復号することから開始してよく、その後、ジェネシス・ブロックに達し、元のファイルが回復されるまで、他のブロックの値を復号し続ける。復号は、さらに各ブロックでヘッダーおよびファイルならびに関連するメタデータを復号することを含んでもよい。

【０１１９】

復号は、各ブロックで行われた暗号化の種類に基づいて実行される。この復号は、秘密鍵、公開鍵、または公開鍵と秘密鍵のペアの使用を含んでよい。例えば、非対称暗号化が使用される場合、ブロックチェーンの参加者またはネットワーク内のプロセッサが、既定のアルゴリズムを使用して公開鍵および秘密鍵のペアを生成してよい。公開鍵および秘密鍵は、何らかの数学的関係によって互いに関連付けられる。公開鍵は、他のユーザからメッセージを受信するためのアドレス（例えば、ＩＰアドレスまたは自宅住所）として機能するように、パブリックに配布されてよい。秘密鍵は、秘密に保たれ、他のブロックチェーンの参加者に送信されるメッセージにデジタル署名するために使用される。署名は、受信者が送信者の公開鍵を使用して検証することができるように、メッセージに含まれる。このようにして、受信者は、送信者のみがこのメッセージを送信できたということを確信することができる。

【０１２０】

鍵のペアを生成することは、ブロックチェーンにアカウントを作成することに類似しているが、実際は、どこにも登録する必要はない。また、ブロックチェーンに対して実行されたすべてのトランザクションが、秘密鍵を使用して送信者によってデジタル署名される。この署名は、アカウントの所有者のみが（スマート・コントラクトによって決定された許可の範囲内である場合に）ブロックチェーンのファイルを追跡して処理することができるということを保証する。

【０１２１】

図８Ａおよび８Ｂは、本明細書に組み込まれて使用されてよい、ブロックチェーンの追加の使用事例を示している。特に、図８Ａは、機械学習（人工知能）データを格納するブロックチェーン８１０の例８００を示している。機械学習は、新しいデータに対する正確な予測のための予測モデルを構築するために、大量の履歴データ（またはトレーニング・データ）に依存する。機械学習ソフトウェア（例えば、ニューラル・ネットワークなど）は、多くの場合、非直感的パターンを発見するために、数百万レコードを取捨選択することができる。

【０１２２】

図８Ａの例では、ホスト・プラットフォーム８２０が、アセット８３０の予測監視のための機械学習モデルを構築してデプロイする。ここで、ホスト・プラットフォーム８２０は、クラウド・プラットフォーム、工業用サーバ、Ｗｅｂサーバ、パーソナル・コンピュータ、ユーザ・デバイスなどであってよい。アセット８３０は、航空機、機関車、タービン、医療機器、石油ガス機器、ボート、船、車両などの、任意の種類のアセット（例えば、機械または機器など）であることができる。別の例として、アセット８３０は、株式、通貨、デジタル・コイン、保険などの、無形のアセットであってよい。

【０１２３】

ブロックチェーン８１０は、機械学習モデルのトレーニング・プロセス８０２およびトレーニング済み機械学習モデルに基づく予測プロセス８０４の両方を大幅に改善するために使用され得る。例えば、８０２では、データを収集するためにデータ科学者／技術者またはその他のユーザを必要とするのではなく、アセット８３０自体によって（または、図示されていない中間物を介して）、ブロックチェーン８１０に関する履歴データが格納されてよい。これによって、予測モデルのトレーニングを実行するときにホスト・プラットフォーム８２０によって必要とされる収集時間を大幅に減らすことができる。例えば、スマート・コントラクトを使用して、データを、元の場所からブロックチェーン８１０に真っすぐに、直接かつ確実に転送することができる。スマート・コントラクトは、ブロック

チェーン８１０を使用して、収集されたデータのセキュリティおよび所有権を保証することによって、アセットから、機械学習モデルを構築するためにデータを使用する個人に、データを直接送信することができる。これによって、アセット８３０間のデータの共有を可能にする。

【０１２４】

収集されたデータは、合意メカニズムに基づいてブロックチェーン８１０に格納されてよい。合意メカニズムは、記録されているデータが検証されており、正確であることを保証するために、（許可されたノードを）制御する。記録されたデータは、タイムスタンプが付与され、暗号によって署名されており、変更不可能である。したがって、記録されたデータは、監査可能、透過的、かつ安全である。ブロックチェーンに直接書き込むＩｏＴデバイスを追加することによって、特定の場合（すなわち、サプライ・チェーン、医療、物流などの場合）に、データが記録される頻度を増やし、その精度を向上させることができる。

【０１２５】

さらに、収集されたデータに対する機械学習モデルのトレーニングは、ホスト・プラットフォーム８２０による一連の改良およびテストを必要とし得る。各改良およびテストは、機械学習モデルの知識を拡張するのに役立つように、追加データまたは以前に考慮されなかったデータに基づいてよい。８０２では、ホスト・プラットフォーム８２０によって、異なるトレーニング・ステップおよびテスト・ステップ（および関連するデータ）がブロックチェーン８１０に格納されてよい。機械学習モデルの各改良（例えば、変数、重みなどにおける変更）は、ブロックチェーン８１０に格納されてよい。これによって、モデルがどのようにトレーニングされたか、およびモデルをトレーニングするためにどのデータが使用されたかの検証可能な証明を提供する。さらに、ホスト・プラットフォーム８２０が最終的なトレーニング済みモデルを実現した場合、得られたモデルがブロックチェーン８１０に格納されてよい。

【０１２６】

モデルがトレーニングされた後に、そのモデルは、活動中の環境にデプロイされてよく、最終的なトレーニング済み機械学習モデルの実行に基づく予測／決定を行うことができる。例えば、８０４で、機械学習モデルは、航空機、風力タービン、医療機械などのアセットのための状態監視保全（ＣＢＭ：condition-based maintenance）に使用されてよい。この例では、アセット８３０からフィードバックされたデータが機械学習モデルに入力され、故障イベント、エラー・コードなどのイベント予測を行うために使用されてよい。ホスト・プラットフォーム８２０で機械学習モデルの実行によって行われた決定は、監査可能／検証可能な証明を提供するために、ブロックチェーン８１０に格納されてよい。１つの非限定的な例として、機械学習モデルは、アセット８３０の部品での将来の停止／故障を予測し、その部品を交換するように警告または通知を作成してよい。この決定の背後にあるデータが、ホスト・プラットフォーム８２０によってブロックチェーン８１０に格納されてよい。１つの実施形態では、本明細書において説明されたか、または示されたか、あるいはその両方である特徴または動作あるいはその両方が、ブロックチェーン８１０で、またはブロックチェーン８１０に関して発生することができる。

【０１２７】

ブロックチェーンの新しいトランザクションが新しいブロックに一緒に集められ、既存のハッシュ値に追加されることができる。次に、このハッシュ値が暗号化されて、新しいブロックの新しいハッシュを生成する。この新しいハッシュが、トランザクションが暗号化されるときなどに、トランザクションの次のリストに追加される。この結果は、先行するすべてのブロックのハッシュ値をそれぞれ含んでいるブロックのチェーンである。これらのブロックを格納するコンピュータは、ブロックのハッシュ値を定期的に比較し、それらのコンピュータがすべて合意していることを確認する。合意していないすべてのコンピュータは、問題を引き起こしているレコードを破棄する。この方法は、ブロックチェーンの改ざん防止を保証することに適しているが、完璧ではない。

【０１２８】
このシステムを不正に操作する１つの方法は、不正なユーザが、ハッシュを変更しないような方法で、トランザクションのリストを自分の都合の良いように変更することである。これは、総当たり攻撃によって実行されることができ、言い換えると、レコードを変更し、結果を暗号化し、ハッシュ値が同じであるかどうかを確認することによって、実行されることができる。ハッシュ値が同じでない場合、一致するハッシュを見つけるまで、何度も繰り返して試みる。ブロックチェーンのセキュリティは、通常のコンピュータが、宇宙の年齢などの、全く非実用的な時間的尺度にわたってしかこの種の総当たり攻撃を実行できないという考えに基づく。それに対して、量子コンピュータは非常に高速（数千倍高速）であり、したがって、非常に大きい脅威をもたらす。

【０１２９】
図８Ｂは、量子コンピューティング攻撃に対して保護するために量子鍵配送（ＱＫＤ：quantum key distribution）を実装する量子セキュアなブロックチェーン８５２の例８５０を示している。この例では、ブロックチェーン・ユーザは、ＱＫＤを使用して互いの識別情報を検証することができる。この検証では、光子などの量子的粒子を使用して情報を送信し、この情報は、破壊することなく盗聴者によってコピーされることが不可能である。このようにして、送信者および受信者が、ブロックチェーンを介して、互いの識別情報を確認することができる。

【０１３０】
図８Ｂの例では、４人のユーザ（８５４、８５６、８５８、および８６０）が存在している。ユーザのペアの各々は、ユーザ自身の間で秘密鍵８６２（すなわち、ＱＫＤ）を共有することができる。この例には４つのノードが存在するため、ノードの６つのペアが存在し、したがって、QKD_{AB}、QKD_{AC}、QKD_{AD}、QKD_{BC}、QKD_{BD}、およびQKD_{CD}を含む６つの異なる秘密鍵８６２が使用される。各ペアは、光子などの量子的粒子を使用して情報を送信することによってＱＫＤを作成することができ、この情報は、破壊することなく盗聴者によってコピーされることが不可能である。このようにして、ユーザのペアが互いの識別情報を確認することができる。

【０１３１】
ブロックチェーン８５２の動作は、（ｉ）トランザクションの作成、および（ｉｉ）新しいトランザクションを集めるブロックの構築という２つの手順に基づく。新しいトランザクションは、従来のブロックチェーン・ネットワークと同様に作成されてよい。各トランザクションは、送信者、受信者、作成時間、転送される量（または値）、送信者が操作のための資金を持っていることを正当化する参照トランザクションのリストに関する情報などを含んでよい。次に、このトランザクション・レコードは、すべての他のノードに送信され、未確認トランザクションのプールに入力される。ここで、２人の関係者（すなわち、８５４～８６０のうちのユーザのペア）が、共有秘密鍵８６２（ＱＫＤ）を提供することによって、トランザクションを認証する。この量子署名は、すべてのトランザクションに添付され、改ざんを極めて困難にすることができる。各ノードは、ブロックチェーン８５２のローカル・コピーに関してトランザクションのエントリをチェックし、各トランザクションが十分な資金を持っていることを検証する。しかし、トランザクションはまだ確認されていない。

【０１３２】
ブロックに対して従来のマイニング・プロセスを実行するのではなく、ブロードキャスト・プロトコルを使用して、分散された方法でブロックが作成されてよい。既定の期間（例えば、数秒、数分、数時間など）に、ネットワークがブロードキャスト・プロトコルをいずれかの未確認トランザクションに適用してよく、それによって、トランザクションの正しいバージョンに関してビザンチン合意（合意）を達成する。例えば、各ノードは、プライベートな値（その特定のノードのトランザクション・データ）を所有してよい。１回目に、ノードは、プライベートな値を互いに送信する。その後、ノードは、前回他のノードから受信した情報を伝達する。ここで、本物のノードが、新しいブロック内のトランザ

クションの完全なセットを作成することができる。この新しいブロックは、ブロックチェーン８５２に追加されることができる。１つの実施形態では、本明細書において説明されたか、または示されたか、あるいはその両方である特徴または動作あるいはその両方が、ブロックチェーン８５２で、またはブロックチェーン８５２に関して発生することができる。

【０１３３】

図９は、本明細書において説明されたか、または示されたか、あるいはその両方である実施形態例のうちの１つまたは複数をサポートする例示的なシステム９００を示している。システム９００は、他の多数の汎用または特殊用途のコンピューティング・システム環境または構成で運用できるコンピュータ・システム／サーバ９０２を備えている。コンピュータ・システム／サーバ９０２と共に使用するのに適し得る周知のコンピューティング・システム、環境、または構成、あるいはその組み合わせの例としては、パーソナル・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、ハンドヘルドまたはラップトップ・デバイス、マルチプロセッサ・システム、マイクロプロセッサベース・システム、セット・トップ・ボックス、プログラマブル・コンシューマ・エレクトロニクス、ネットワークＰＣ、ミニコンピュータ・システム、メインフレーム・コンピュータ・システム、およびこれらの任意のシステムまたはデバイスを含む分散クラウド・コンピューティング環境などが挙げられるが、これらに限定されない。

【０１３４】

コンピュータ・システム／サーバ９０２は、コンピュータ・システムによって実行されているプログラム・モジュールなどの、コンピュータ・システムによって実行可能な命令との一般的な関連において説明されてよい。通常、プログラム・モジュールは、特定のタスクを実行するか、または特定の抽象データ型を実装するルーチン、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んでよい。コンピュータ・システム／サーバ９０２は、通信ネットワークを介してリンクされたリモート処理デバイスによってタスクが実行される、分散クラウド・コンピューティング環境で実行されてよい。分散クラウド・コンピューティング環境において、プログラム・モジュールは、メモリ・ストレージ・デバイスを含む、ローカルおよびリモートの両方のコンピュータ・システム・ストレージ媒体に配置されてよい。

【０１３５】

図９に示すように、クラウド・コンピューティング・ノード９００内のコンピュータ・システム／サーバ９０２は、汎用コンピューティング・デバイスの形態で示されている。コンピュータ・システム／サーバ９０２のコンポーネントは、１つまたは複数のプロセッサまたはプロセッシング・ユニット９０４、システム・メモリ９０６、およびシステム・メモリ９０６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９０４に結合するバスを含んでよいが、これらに限定されない。

【０１３６】

バスは、メモリ・バスまたはメモリ・コントローラ、ペリフェラル・バス、アクセラレーテッド・グラフィックス・ポート、および任意のさまざまなバス・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、任意の複数の種類のバス構造のうちの１つまたは複数を表す。例として、そのようなアーキテクチャは、ＩＳＡ（Industry Standard Architecture）バス、ＭＣＡ（Micro Channel Architecture）バス、ＥＩＳＡ（Enhanced ISA）バス、ＶＥＳＡ（Video Electronics Standards Association）ローカル・バス、およびＰＣＩ（Peripheral Component Interconnects）バスを含むが、これらに限定されない。

【０１３７】

コンピュータ・システム／サーバ９０２は、通常、さまざまなコンピュータ・システム可読媒体を含む。そのような媒体は、コンピュータ・システム／サーバ９０２によってアクセスできる任意の使用可能な媒体であってよく、揮発性および不揮発性媒体、取り外し

可能および取り外し不可の媒体を含む。システム・メモリ９０６は、１つの実施形態では、他の図のフロー図を実装する。システム・メモリ９０６は、ランダム・アクセス・メモリ（ＲＡＭ：random access memory）９１０またはキャッシュ・メモリ９１２あるいはその両方などの、揮発性メモリの形態でのコンピュータ・システム可読媒体を含むことができる。コンピュータ・システム／サーバ９０２は、その他の取り外し可能／取り外し不可、揮発性／不揮発性のコンピュータ・システム・ストレージ媒体をさらに含んでよい。単に例として、取り外し不可、不揮発性の磁気媒体（図示されておらず、通常は「ハード・ドライブ」と呼ばれる）に対する読み取りと書き込みを行うために、ストレージ・システム９１４を提供することができる。図示されていないが、取り外し可能、不揮発性の磁気ディスク（例えば、「フロッピー（Ｒ）・ディスク」）に対する読み取りと書き込みを行うための磁気ディスク・ドライブ、およびＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、またはその他の光媒体などの取り外し可能、不揮発性の光ディスクに対する読み取りと書き込みを行うための光ディスク・ドライブを提供することができる。そのような例では、それぞれを、１つまたは複数のデータ媒体インターフェイスによってバスに接続することができる。下で詳細に示され、説明されるように、メモリ９０６は、本出願のさまざまな実施形態の機能を実行するように構成された一連の（例えば、少なくとも１つの）プログラム・モジュールを備える少なくとも１つのプログラム製品を含んでよい。

【０１３８】

例えば、一連の（少なくとも１つの）プログラム・モジュール９１８を含んでいるプログラム／ユーティリティ９１６がメモリ９０６に格納されてよいが、これに限定されず、オペレーティング・システム、１つまたは複数のアプリケーション・プログラム、その他のプログラム・モジュール、およびプログラム・データも格納されてよい。オペレーティング・システム、１つまたは複数のアプリケーション・プログラム、その他のプログラム・モジュール、およびプログラム・データまたはこれらの組み合わせの各々は、ネットワーク環境の実装を含んでよい。プログラム・モジュール９１８は、通常、本明細書に記載された本出願のさまざまな実施形態の機能または方法あるいはその両方を実行する。

【０１３９】

当業者によって理解されるように、本出願の態様は、システム、方法、またはコンピュータ・プログラム製品として具現化されてよい。したがって、本出願の態様は、完全にハードウェアの実施形態、完全にソフトウェアの実施形態（ファームウェア、常駐ソフトウェア、マイクロコードなどを含む）、またはソフトウェアの態様とハードウェアの態様を組み合わせる実施形態の形態を取ってよく、これらはすべて、本明細書では、一般に「回路」、「モジュール」、または「システム」と呼ばれてよい。さらに、本出願の形態は、コンピュータ可読プログラム・コードが具現化されている１つまたは複数のコンピュータ可読媒体において具現化されたコンピュータ・プログラム製品の形態を取ってよい。

【０１４０】

また、コンピュータ・システム／サーバ９０２は、キーボード、ポインティング・デバイス、ディスプレイ９２２などの１つまたは複数の外部デバイス９２０、ユーザがコンピュータ・システム／サーバ９０２と情報をやりとりできるようにする１つまたは複数のデバイス、またはコンピュータ・システム／サーバ９０２が１つまたは複数の他のコンピューティング・デバイスと通信できるよう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）、あるいはその組み合わせと通信することもできる。このような通信は、Ｉ／Ｏインターフェイス９２４を介して行うことができる。さらに、コンピュータ・システム／サーバ９０２は、ローカル・エリア・ネットワーク（ＬＡＮ：local area network）、一般的な広域ネットワーク（ＷＡＮ：wide area network）、またはパブリック・ネットワーク（例えば、インターネット）、あるいはその組み合わせなどの１つまたは複数のネットワークと、ネットワーク・アダプタ９２６を介して通信することができる。図示されているように、ネットワーク・アダプタ９２６は、バスを介してコンピュータ・システム／サーバ９０２の他のコンポーネントと通信する。図示されていないが、その他のハードウェア・コンポーネントまたはソフトウェア・コンポーネントあるいは

その両方を、コンピュータ・システム／サーバ９０２と併用できるということが理解されるべきである。その例として、マイクロコード、デバイス・ドライバ、冗長プロセッシング・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・アーカイブ・ストレージ・システムなどが挙げられるが、これらに限定されない。

【０１４１】

システム、方法、および非一過性コンピュータ可読媒体のうちの少なくとも１つの実施形態例が添付の図面において示され、前述の詳細な説明において説明されたが、本出願が、開示された実施形態に限定されず、以下の特許請求の範囲によって示され、定義されているように、多数の再配置、変更、および置き換えを行うことができるということが理解されるであろう。例えば、さまざまな図のシステムの機能は、本明細書に記載されたモジュールまたはコンポーネントのうちの１つまたは複数によって、あるいは分散アーキテクチャにおいて実行することができ、送信器、受信器、またはその両方のペアを含んでよい。例えば、個々のモジュールによって実行される機能の全部または一部は、それらのモジュールのうちの１つまたは複数によって実行されてよい。さらに、本明細書に記載された機能は、さまざまな時間に、さまざまなイベントに関して、モジュールまたはコンポーネントの内部または外部で、実行されてよい。また、さまざまなモジュールの間で送信される情報は、データ・ネットワーク、インターネット、音声ネットワーク、インターネット・プロトコル・ネットワーク、無線デバイス、有線デバイスのうちの少なくとも１つを介して、または複数のプロトコルを介して、あるいはその組み合わせを介して、モジュール間で送信され得る。また、モジュールのいずれかによって送信または受信されるメッセージは、直接的に、または他のモジュールのうちの１つまたは複数を介して、あるいはその両方によって、送信または受信されてよい。

【０１４２】

当業者は、「システム」を、パーソナル・コンピュータ、サーバ、コンソール、ＰＤＡ（personal digital assistant）、携帯電話、タブレット・コンピューティング・デバイス、スマートフォン、または任意のその他の適切なコンピューティング・デバイス、あるいはデバイスの組み合わせとして具現化できるということを、理解するであろう。「システム」によって実行されている前述の機能を提示することは、本出願の範囲を限定するように全く意図されておらず、多くの実施形態のうちの１つの例を提供するよう意図されている。実際に、本明細書で開示された方法、システム、および装置は、計算技術に一致する局所的な分散された形態で実装されてよい。

【０１４３】

本明細書において説明されたシステムの特徴の一部が、それらの実装の独立性を特により強調するために、モジュールとして提示されていることに、注意するべきである。例えば、モジュールは、カスタム超大規模集積（ＶＬＳＩ：very large-scale integration）回路またはゲート・アレイ、論理チップなどの市販の半導体、トランジスタ、またはその他の個別のコンポーネントを備えているハードウェア回路として実装されてよい。モジュールは、フィールド・プログラマブル・ゲート・アレイ、プログラマブル・アレイ論理、プログラマブル論理デバイス、グラフィックス・プロセッシング・ユニットなどの、プログラム可能なハードウェア・デバイスにおいて実装されてもよい。

【０１４４】

モジュールは、さまざまな種類のプロセッサによって実行するために、ソフトウェアにおいて少なくとも部分的に実装されてもよい。例えば、実行可能コードの識別されたユニットは、例えばオブジェクト、プロシージャ、または関数として編成されてよいコンピュータ命令の１つまたは複数の物理的または論理的ブロックを備えてよい。それにもかかわらず、識別されたモジュールの実行可能によって、物理的に一緒に配置される必要はなく、異なる位置に格納された異種の命令を含んでよく、それらの命令は、論理的に一緒に結合された場合にモジュールを備え、モジュールの規定された目的を達成する。さらに、モジュールはコンピュータ可読媒体に格納されてよく、このコンピュータ可読媒体は、例え

ば、ハード・ディスク・ドライブ、フラッシュ・デバイス、ランダム・アクセス・メモリ（ＲＡＭ）、テープ、またはデータの格納に使用される任意のその他の媒体であってよい。

【０１４５】

実際に、実行可能コードのモジュールは、単一の命令であるか、または多くの命令であることができ、複数の異なるコード・セグメントにわたって、異なるプログラム間および複数のメモリ・デバイスにまたがって、分散されてもよい。同様に、操作可能なデータが、識別され、本明細書ではモジュール内で示されてよく、任意の適切な形態で具現化され、任意の適切な種類のデータ構造内で編成されてよい。操作可能なデータは、単一のデータ・セットとして収集されてよく、または異なるストレージ・デバイスを含む、異なる位置にわたって分散されてよく、システムまたはネットワーク上の単なる電子信号として、少なくとも部分的に存在してよい。

【０１４６】

本明細書の図において概略的に説明され、示されているように、本出願のコンポーネントが、多種多様な異なる構成で配置および設計されてよいということが、容易に理解されるであろう。したがって、実施形態の詳細な説明は、請求される本出願の範囲を限定するよう意図されておらず、単に、本出願の選択された実施形態を表している。

【０１４７】

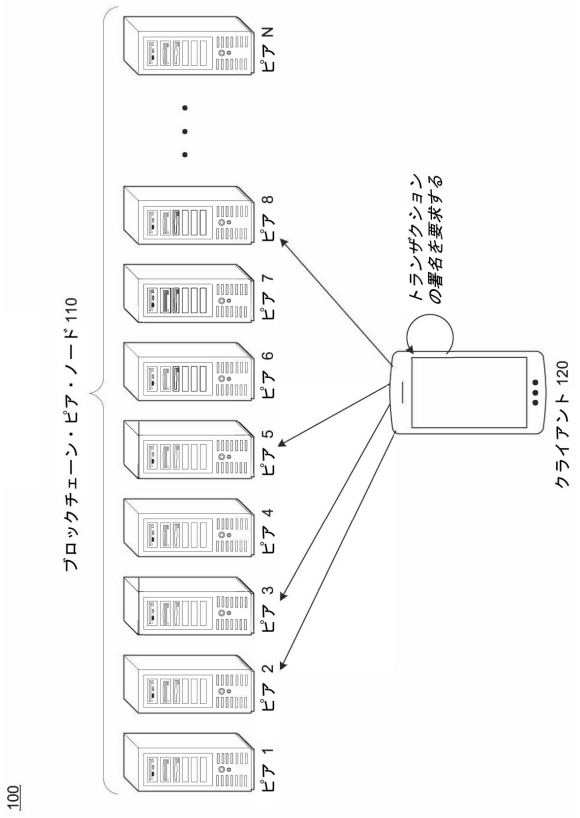
当業者は、開示された順序とは異なる順序でステップを使用して、または開示された構成におけるハードウェア要素とは異なるハードウェア要素を使用して、あるいはその両方を使用して、前述の内容を実践できるということを、容易に理解するであろう。したがって、本出願は、これらの好ましい実施形態に基づいて説明されたが、特定の変更、変形、および代替の構造が明白であるということは、当業者にとって明らかであろう。

【０１４８】

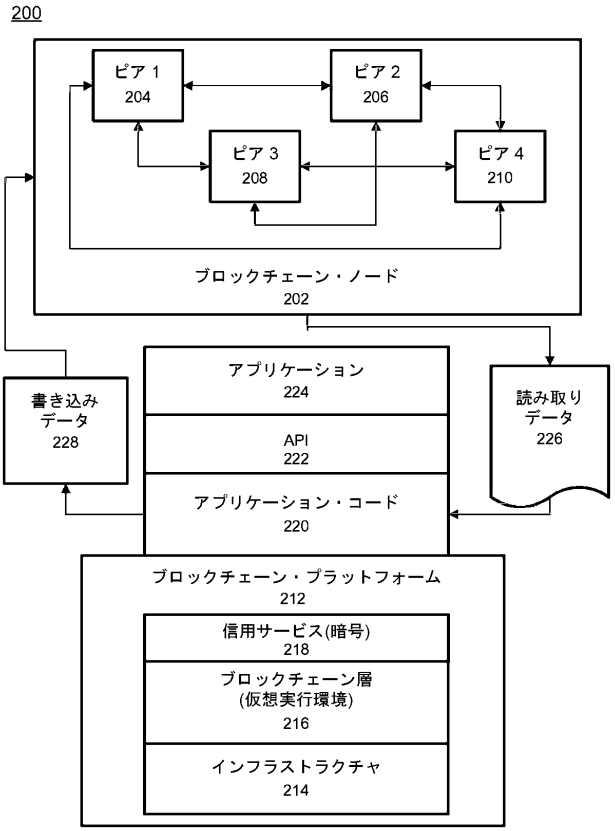
本出願の好ましい実施形態が説明されたが、説明された実施形態が単なる例であり、それらの実施形態と同等のものおよびそれらの実施形態に対する変更の完全な範囲（例えば、プロトコル、ハードウェア・デバイス、ソフトウェア・プラットフォームなど）で考えた場合、本出願の範囲が添付の特許請求の範囲のみによって定義されるべきであるということが、理解されるべきである。

【図面】

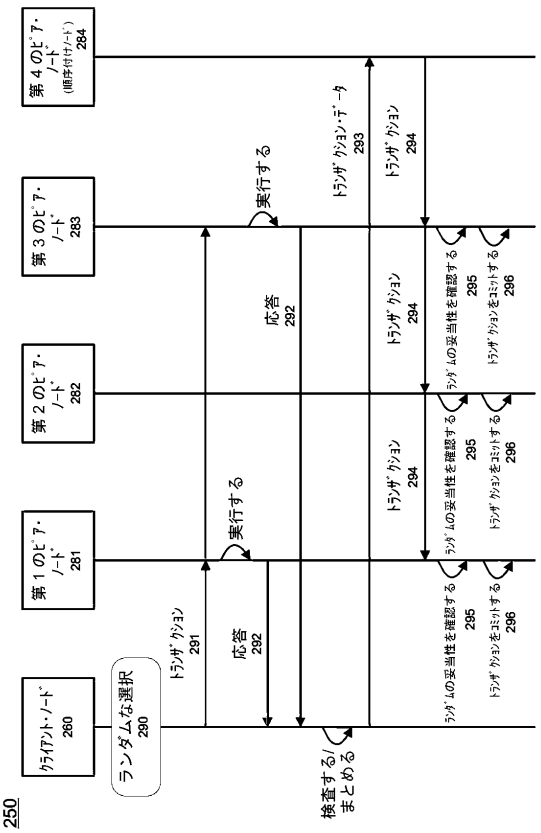
【図１】



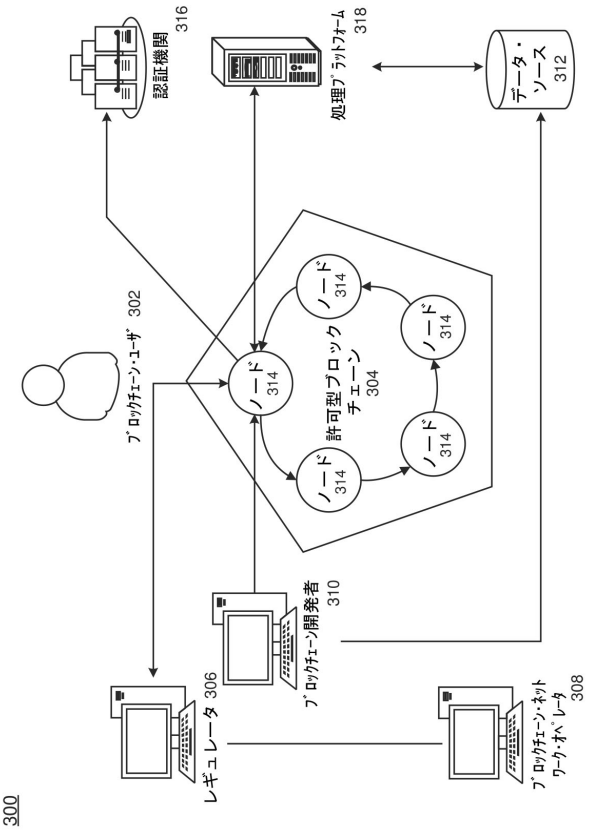
【図２Ａ】



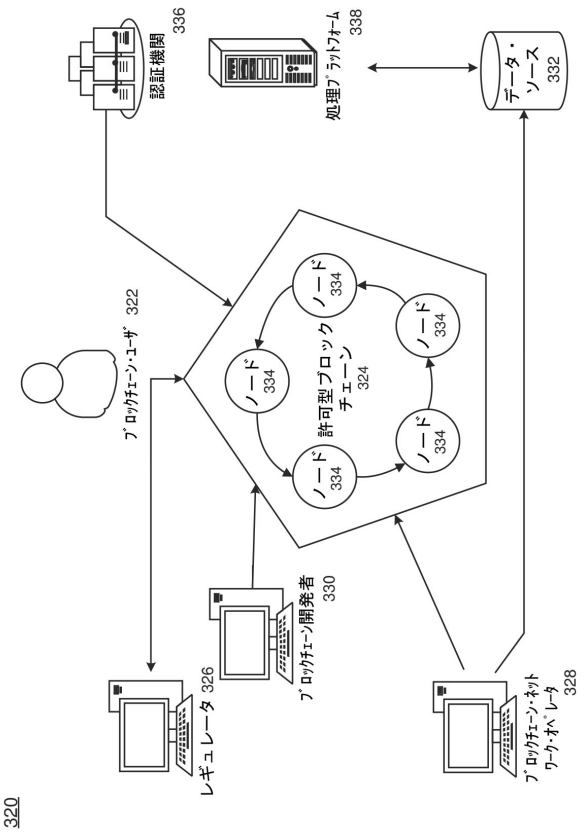
【図２Ｂ】



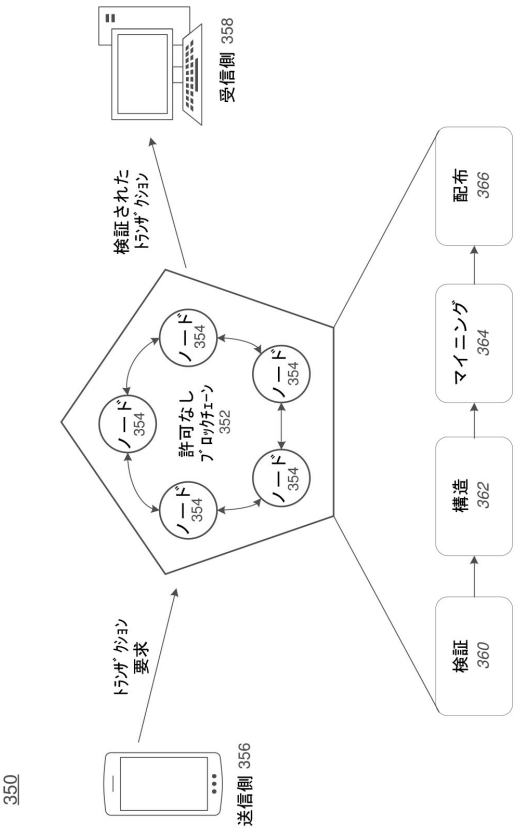
【図３Ａ】



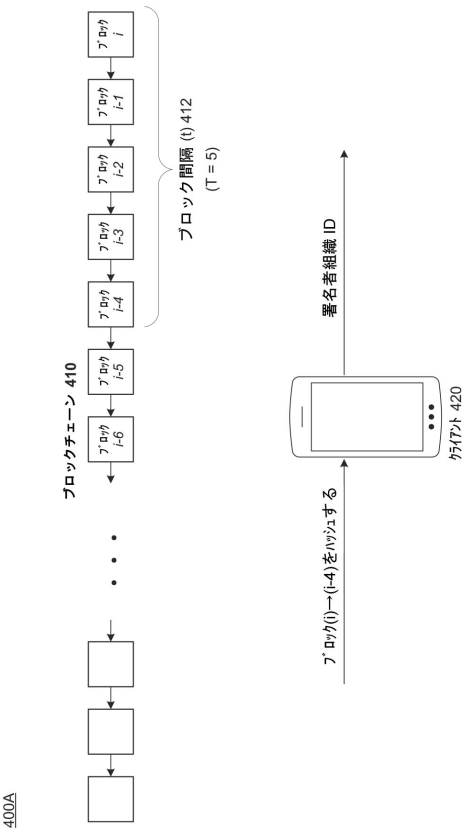
【図３Ｂ】



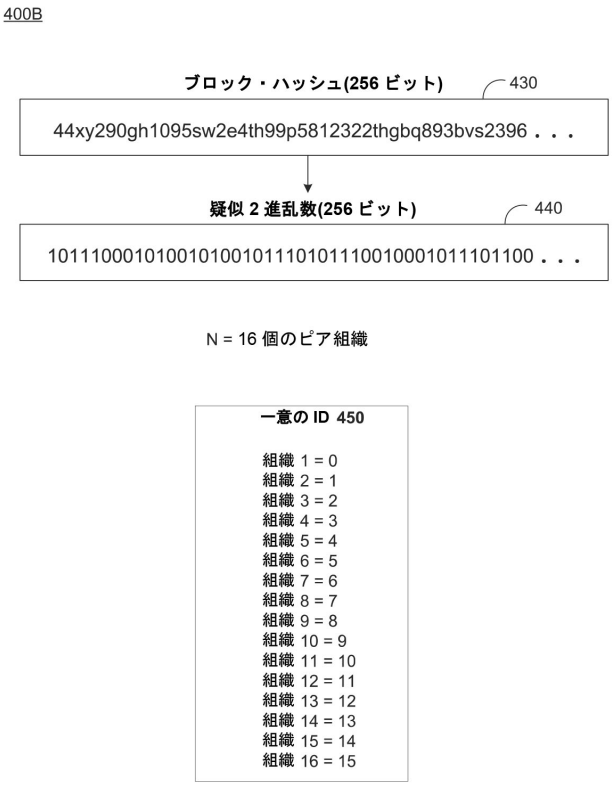
【図３Ｃ】



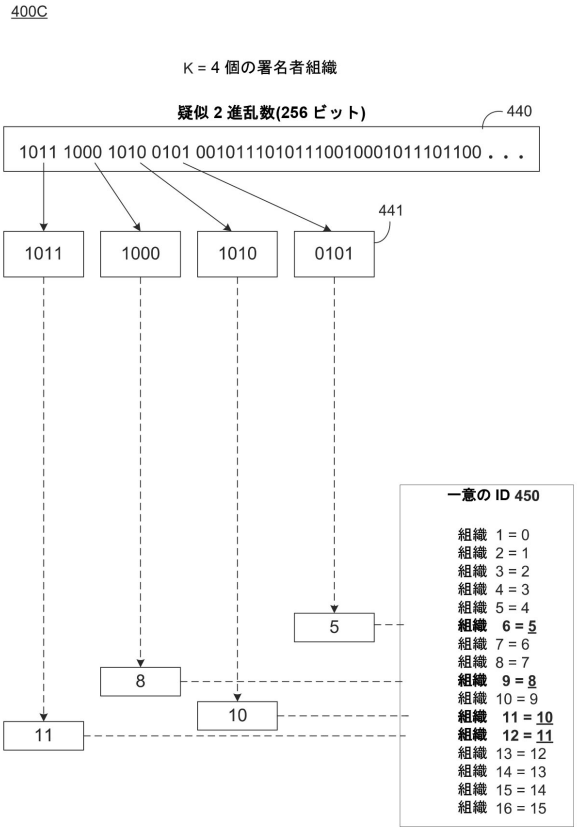
【図４Ａ】



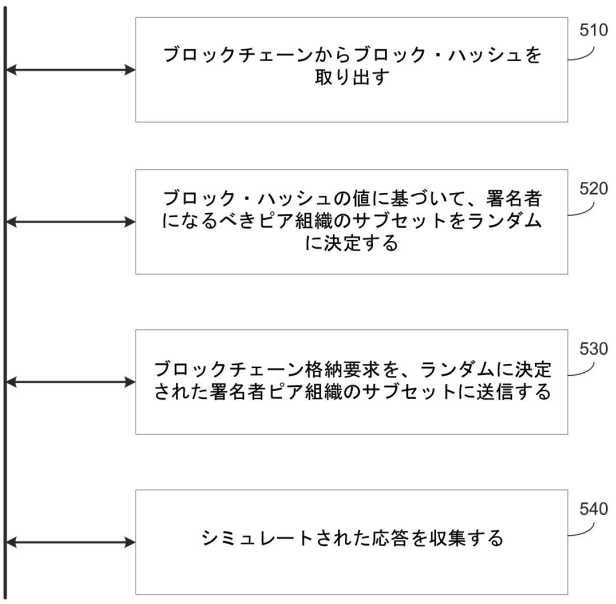
【図４Ｂ】



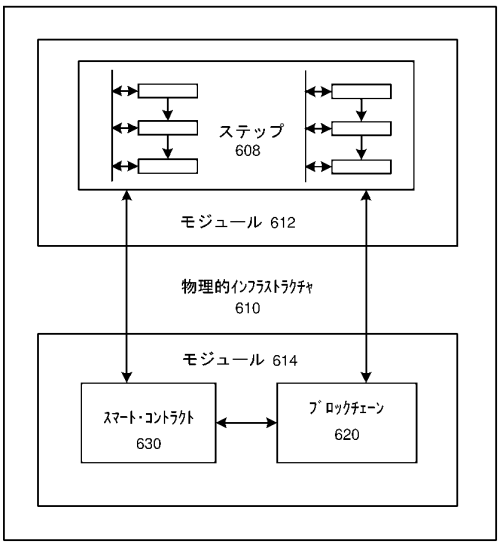
【図４Ｃ】



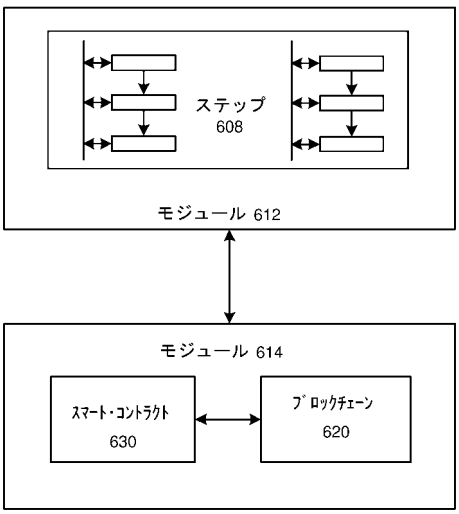
【図５】



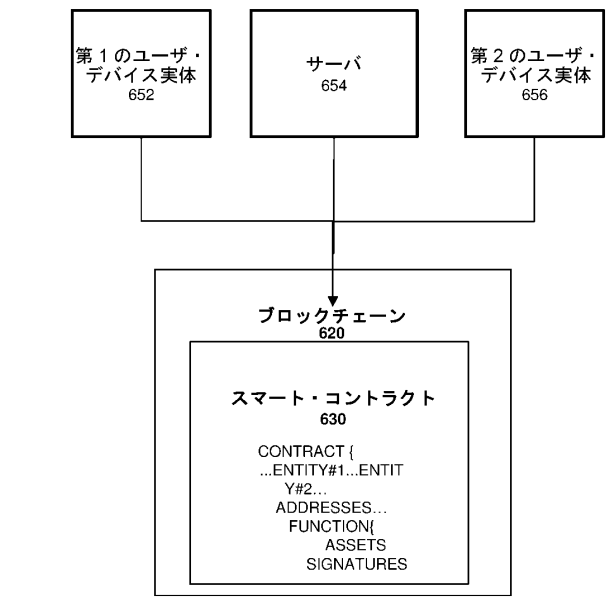
【図６Ａ】



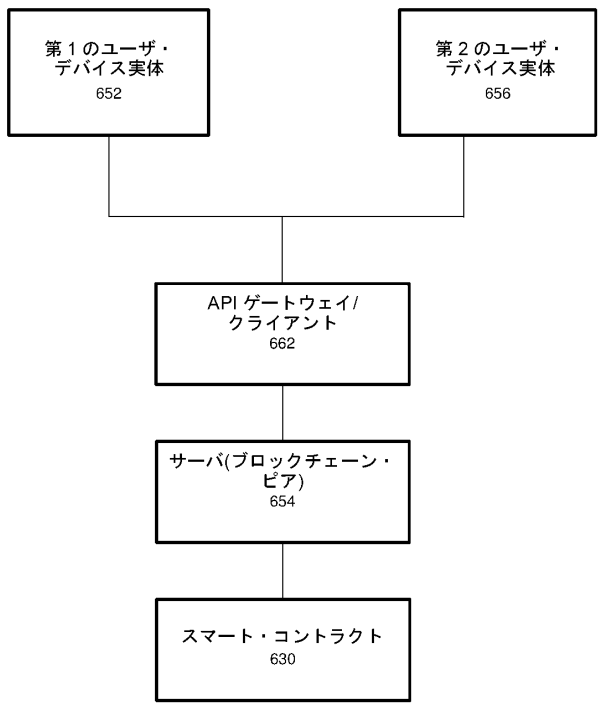
【図６Ｂ】



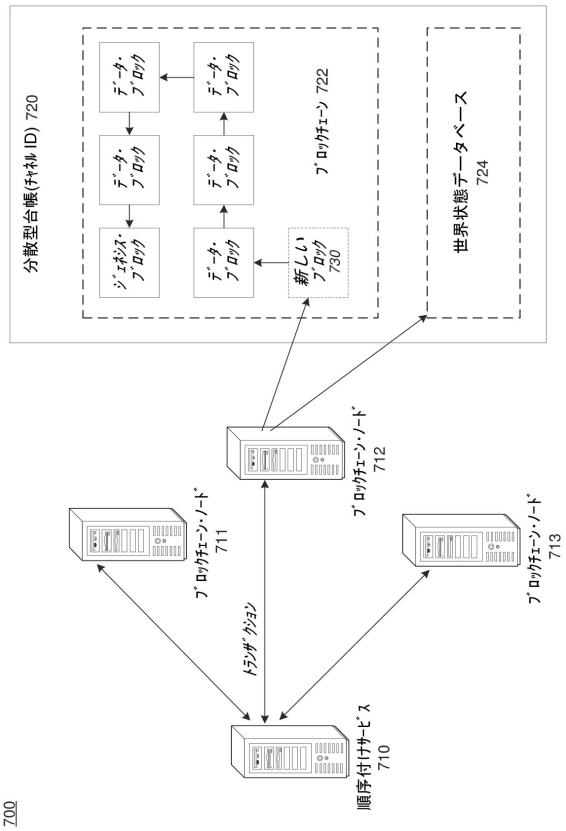
【図６Ｃ】



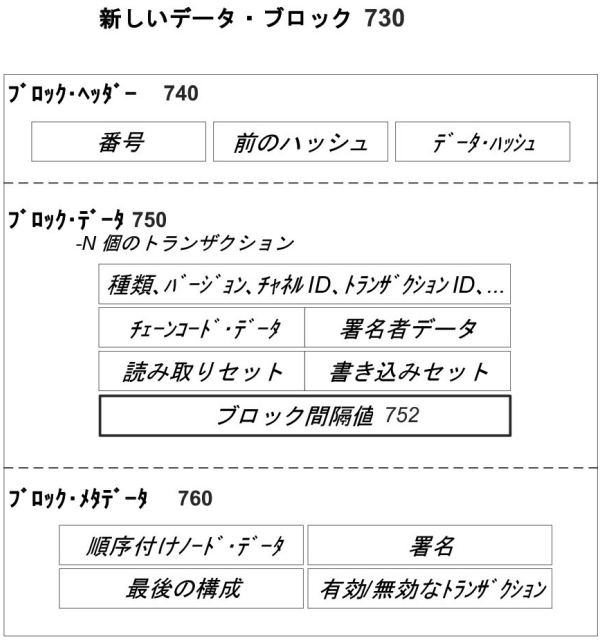
【図６Ｄ】



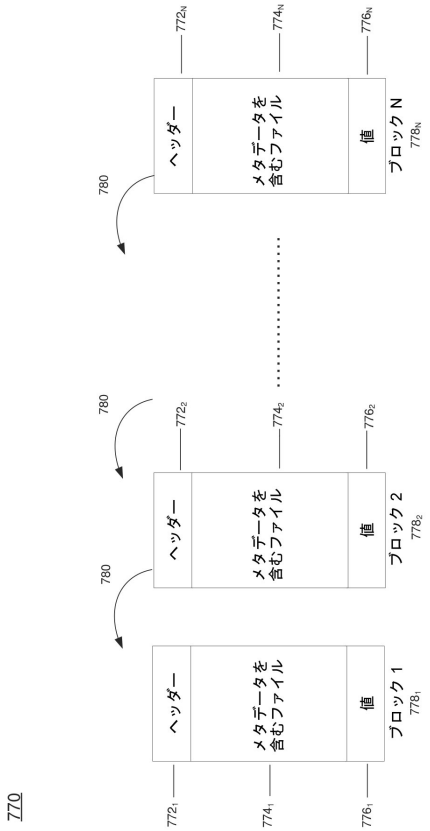
【図７Ａ】



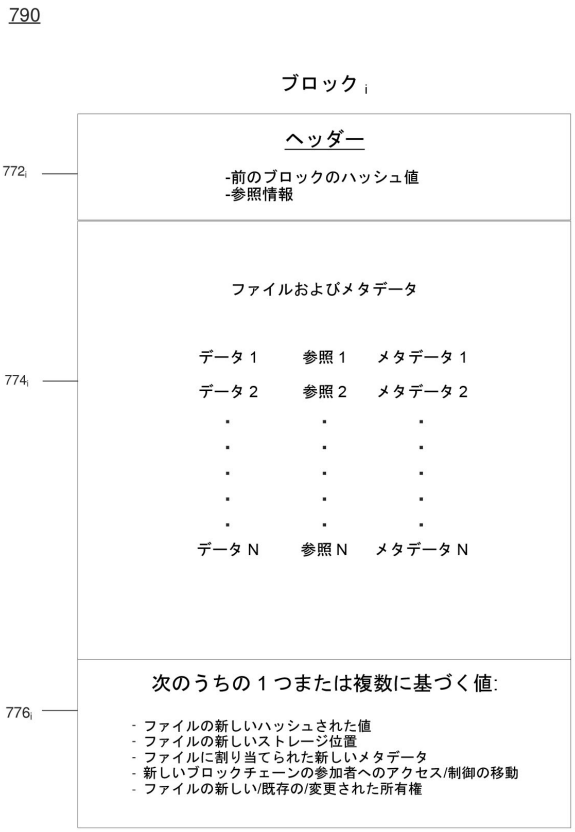
【図７Ｂ】



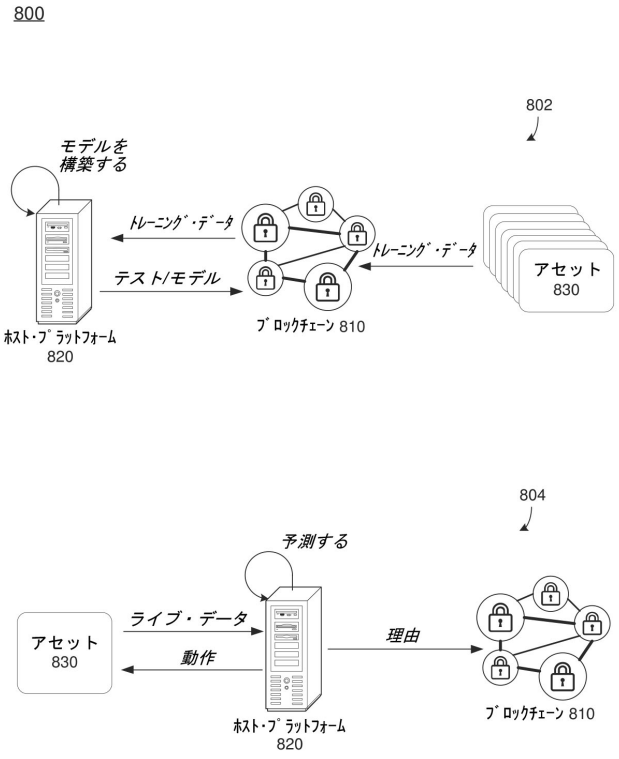
【図７Ｃ】



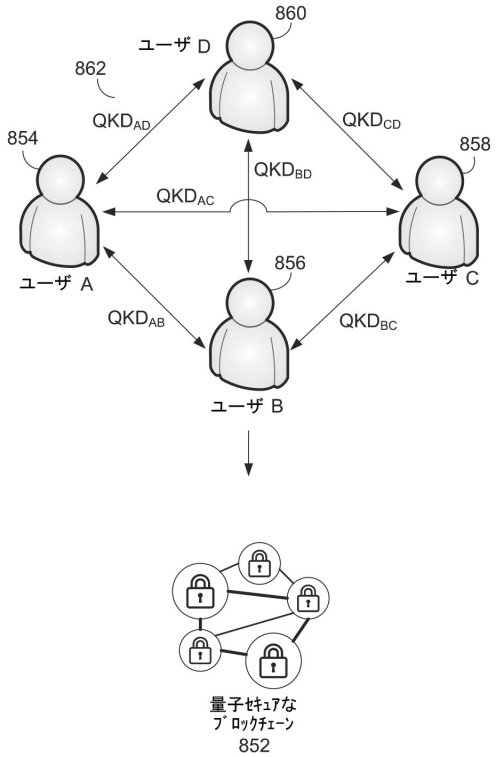
【図７Ｄ】



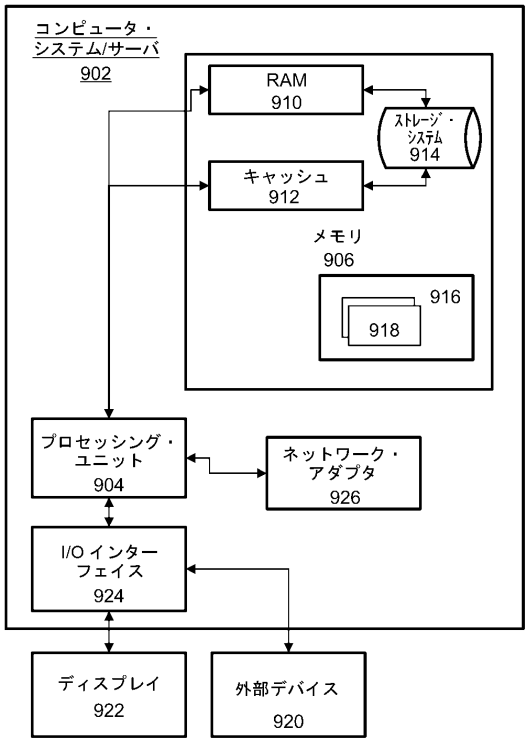
【図８Ａ】



【図８Ｂ】



【図９】


900
コンピュータ・システム/サーバ
902
RAM
910
ストレージ・システム
914
キャッシュ
912
メモリ
906
916
918
プロセッシング・ユニット
904
ネットワーク・アダプタ
926
I/O インターフェイス
924
ディスプレイ
922
外部デバイス
920

【手続補正書】
【提出日】令和4年12月14日(2022.12.14)
【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】
ブロックチェーンに格納されたデータ・ブロックのブロック・ハッシュを取り出すことと、前記ブロック・ハッシュの値に基づいて、ピア組織のサブセットを前記ブロックチェーンのブロックチェーン・ネットワークからランダムに決定することと、ブロックチェーン格納要求を、クライアントから、前記ランダムに決定された署名者ピア組織のサブセットに送信することとを実行するように構成されたプロセッサと、
前記ランダムに決定された署名者ピア組織のサブセットからのシミュレートされた応答を、格納要求提案に収集するように構成されたネットワーク・インターフェイスとを備える、装置。
【請求項２】
前記プロセッサが、前記ブロック・ハッシュを乱数に変換することと、前記乱数を複数のビット・セグメントに分割することと、前記複数のビット・セグメントに基づいて前記ピア組織のサブセットを識別することとを実行するように構成される、請求項１に記載の装置。
【請求項３】
前記プロセッサが、前記ブロックチェーン・ネットワークに含まれているピア組織の数に基づいて、前記複数のピア組織のうちの各ピア組織に一意の識別子を割り当てることと、前記複数のビット・セグメントからのビット・セグメントを１０進数値に変換することと、前記ビット・セグメントの前記１０進数値を前記ピア組織のうちの１つの一意の識別子にマッピングすることとを実行するように構成される、請求項２に記載の装置。
【請求項４】
前記プロセッサが、前記ブロックチェーン・ネットワークに含まれているピア組織の数に基づいて前記ビット・セグメントのサイズを選択するようにさらに構成される、請求項２に記載の装置。
【請求項５】
前記プロセッサが、前記ブロックチェーン上の最新のブロックのサブセットを識別するブロック間隔値を決定するようにさらに構成され、前記サブセットから前記ブロック・ハッシュが取り出され得る、請求項１に記載の装置。
【請求項６】
前記プロセッサが、前記ブロック間隔値によって識別された前記最新のブロックのサブセット内のブロックを選択することと、前記ブロック間隔値によって識別された前記最新のブロックのサブセット内の前記選択されたブロックから前記ブロック・ハッシュを取り出すこととを実行するように構成される、請求項５に記載の装置。
【請求項７】
前記プロセッサが、前記ブロックチェーンの現在の高さおよび前記ブロック間隔値に基づいて完全性値を生成することと、前記完全性値を前記格納要求提案内に格納することとを実行するようにさらに構成される、請求項６に記載の装置。
【請求項８】
前記ネットワーク・インターフェイスが、前記ランダムに決定された署名者ピア組織のサブセットから前記収集された、シミュレートされた応答を含んでいる前記格納要求提案を、前記ブロックチェーンの順序付けノード・サービスに送信するようにさらに構成される、請求項１に記載の装置。

【請求項９】
ブロックチェーンに格納されたデータ・ブロックのブロック・ハッシュを取り出すことと、
前記ブロック・ハッシュの値に基づいて、署名者になるべきピア組織のサブセットを前記ブロックチェーンのブロックチェーン・ネットワークからランダムに決定することと、
ブロックチェーン格納要求を、クライアントから前記ランダムに決定された署名者ピア組織のサブセットに送信することと、
前記ランダムに決定された署名者ピア組織のサブセットからのシミュレートされた応答を、格納要求提案に収集することとを含む、方法。
【請求項１０】
前記ランダムに決定することが、前記ブロック・ハッシュを乱数に変換することと、前記乱数を複数のビット・セグメントに分割することと、前記複数のビット・セグメントのうちの１つまたは複数に基づいて前記ピア組織のサブセットを識別することとを含む、請求項９に記載の方法。
【請求項１１】
前記識別することが、前記ブロックチェーン・ネットワークに含まれているピア・ノードの数に基づいて、前記複数のピア・ノードのうちの各ピア組織に一意の識別子を割り当てることと、前記複数のビット・セグメントからのビット・セグメントを１０進数値に変換することと、前記ビット・セグメントの前記１０進数値を前記ピア組織のうちの１つの一意の識別子にマッピングすることとを含む、請求項１０に記載の方法。
【請求項１２】
前記ブロックチェーン・ネットワークに含まれているピア組織の数に基づいて前記ビット・セグメントのサイズを選択することをさらに含む、請求項１０に記載の方法。
【請求項１３】
前記ブロックチェーン上の最新のブロックのサブセットを識別するブロック間隔値を決定することをさらに含み、前記サブセットから前記ブロック・ハッシュが取り出され得る、請求項９に記載の方法。
【請求項１４】
前記ブロック間隔値によって識別された前記最新のブロックのサブセット内のブロックを選択することと、前記ブロック間隔値によって識別された前記ブロックのサブセット内の前記選択されたブロックから前記ブロック・ハッシュを取り出すこととをさらに含む、請求項１３に記載の方法。
【請求項１５】
前記ブロックチェーンの現在の高さおよび前記ブロック間隔値に基づいて完全性値を生成することと、前記完全性値を前記格納要求提案内に格納することとをさらに含む、請求項１４に記載の方法。
【請求項１６】
前記ランダムに決定された署名者ピア・ノードのサブセットから前記収集された、シミュレートされた応答を含んでいる前記格納要求提案を、前記ブロックチェーンの順序付けノード・サービスに送信することをさらに含む、請求項９に記載の方法。
【請求項１７】
コンピュータ・プログラムであって、請求項１ないし１６のいずれか１項に記載の方法の各ステップ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１８】
請求項１７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。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2020/059927

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/64(2013.01)i; H04L 29/06(2006.01)i; H04L 9/06(2006.01)i

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 G06Q 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)

CNPAT,CNKI,WPI,EPODOC:hash, endors+, chain block, blockchain, peer, node

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2019303621 A1 (IBM CORP.) 03 October 2019 (2019-10-03) description, paragraphs 28-60, figures 1, 2B	1-20
A	US 10425230 B1 (CAPITAL ONE SERVICES, LLC) 24 September 2019 (2019-09-24) the whole document	1-20
A	CN 108833081 A (NATIONAL DEFENSE UNIVERSITY OF SCIENCE AND TECHNOLOGY OF PLA) 16 November 2018 (2018-11-16) the whole document	1-20
A	CN 108737370 A (XI'AN UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY) 02 November 2018 (2018-11-02) the whole document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ 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
13 January 2021	**27 January 2021**
Name and mailing address of the ISA/CN **National Intellectual Property Administration, PRC** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing** **100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer **JIANG,Li** Telephone No. **(86-10) 53961751**

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2020/059927

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2019303621 A1	03 October 2019	US 10754989 B2	25 August 2020
		WO 2019185329 A1	03 October 2019
US 10425230 B1	24 September 2019	US 2020280444 A1	03 September 2020
CN 108833081 A	16 November 2018	None	
CN 108737370 A	02 November 2018	None	

Form PCT/ISA/210 (patent family annex) (January 2015)

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,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

(72)発明者　マネヴィッチ、ヤコブ
イスラエル ハイファ３１９０５ マウント・カーメル ハイファ・ユニバーシティ・キャンパス アイ・ビー・エム イスラエル
(72)発明者　バーガー、アーテム
イスラエル ハイファ３１９０５ マウント・カーメル ハイファ・ユニバーシティ・キャンパス アイ・ビー・エム イスラエル
(72)発明者　メール、ヘイガー
イスラエル ハイファ３１９０５ マウント・カーメル ハイファ・ユニバーシティ・キャンパス アイ・ビー・エム イスラエル