(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2020-521342
(P2020-521342A)
(43)公表日　令和2年7月16日(2020.7.16)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675Z	
G06F 21/62	(2013.01)	H04L	9/00	675B	
		G06F	21/62	318	

審査請求 有　予備審査請求 未請求　（全 26 頁）

(21)出願番号　特願2019-553421 (P2019-553421)
(86)(22)出願日　平成31年3月29日 (2019.3.29)
(85)翻訳文提出日　令和1年11月25日 (2019.11.25)
(86)国際出願番号　PCT/CN2019/080493
(87)国際公開番号　WO2019/120326
(87)国際公開日　令和1年6月27日 (2019.6.27)

(71)出願人　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　100188558
弁理士　飯田　雅人
(74)代理人　100205785
弁理士　▲高▼橋　史生

最終頁に続く

(54)【発明の名称】ブロックチェーンネットワークにおける機密データ要素の管理

(57)【要約】
ブロックチェーンネットワークに記憶された機密データ要素を管理するための、コンピュータ記憶媒体上に符号化されたコンピュータプログラムを含む方法、システム、および装置を本明細書で開示する。方法の1つは、ブロックチェーンネットワークに記憶されたウォッチリストに変更を行うようにとのクライアントデバイスからの要求を受け取るステップを含む。ウォッチリストは、1つまたは複数の機密データ要素を含む。ブロックチェーンネットワークノードは、要求内のデジタル署名に基づいて、クライアントデバイスがウォッチリストを変更する権限があるかどうかを決定する。クライアントデバイスがウォッチリストを変更する権限があるとの決定に応じて、ブロックチェーンネットワーク内で要求についてコンセンサスプロシージャが行われる。コンセンサスが達成された後、ブロックチェーンネットワークノードは、ウォッチリストの変更に基づいてウォッチリストを更新する。

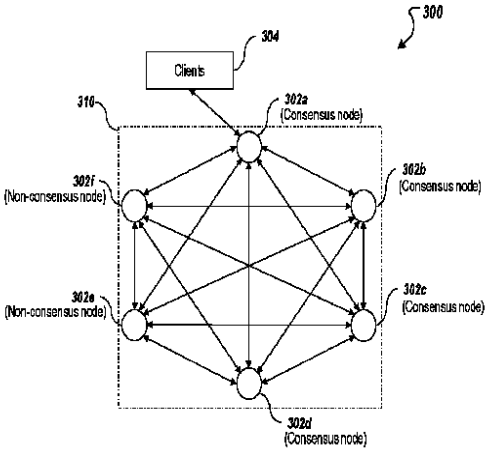


FIG. 3

【特許請求の範囲】
【請求項１】
ブロックチェーンネットワークに記憶された機密データ要素を管理するためのコンピュータ実装方法であって、
ブロックチェーンネットワークのネットワークノードによって、前記ブロックチェーンネットワークに記憶されたウォッチリストの変更を行うようにとのクライアントデバイスからの要求を受け取るステップであって、前記ウォッチリストが、複数の機密データ要素を含み、前記要求が、前記クライアントデバイスのプライベート鍵を使用して生成されたデジタル署名を含む、ステップと、
前記ネットワークノードによって、前記デジタル署名に基づいて、前記クライアントデバイスが前記ウォッチリストを変更する権限があるかどうかを決定するステップと、
前記クライアントデバイスが前記ウォッチリストを変更する権限があるとの決定に応じて、
前記ネットワークノードによって、前記ブロックチェーンネットワーク内で前記要求についてコンセンサスプロシージャを行い、
前記コンセンサスプロシージャを完了した後にコンセンサスが達成されたとの決定に応じて、前記ネットワークノードによって、前記ウォッチリストの前記変更を行うステップ、または
前記クライアントデバイスが前記ウォッチリストを変更する権限がないとの決定に応じて、前記ネットワークノードによって、前記ウォッチリストの前記変更を行うようにとの前記クライアントデバイスからの前記要求を拒否するステップと
を含む、方法。
【請求項２】
前記複数の機密データ要素が、1つまたは複数の権限を与えられた機関によるモニタリング、フィルタリング、または両方を受ける、請求項1に記載の方法。
【請求項３】
前記ウォッチリストの前記変更を行う前記要求が、新しい機密データ要素を前記ウォッチリストに追加する要求、機密データ要素を前記ウォッチリストから取り除く要求、または前記ウォッチリスト内の機密データ要素を編集する要求のうちの1つまたは複数を含む、請求項1または2に記載の方法。
【請求項４】
前記複数の機密データ要素が暗号化される、請求項1から3のいずれか一項に記載の方法。
【請求項５】
前記ネットワークノードによって前記デジタル署名に基づいて前記クライアントデバイスが前記ウォッチリストを変更する権限があるかどうかを前記決定するステップが、前記デジタル署名と、前記ウォッチリストを変更する権限のある権限を与えられた機関の公開鍵とに基づいて、前記クライアントデバイスが前記ウォッチリストを変更する権限があると決定するステップを含む、請求項1から4のいずれか一項に記載の方法。
【請求項６】
前記権限を与えられた機関が、前記ネットワークノードに記憶されたホワイトリストに示され、
前記ホワイトリストが、前記ウォッチリストを変更する権限がある1つまたは複数の権限を与えられた機関を含む、請求項5に記載の方法。
【請求項７】
前記ネットワークノードによって、前記ブロックチェーンネットワークに記憶された前記ウォッチリスト内の機密データ要素を求める第2のクライアントデバイスからの照会要求を受け取るステップであって、前記照会要求が前記第2のクライアントデバイスのプライベート鍵を使用して生成された第2のデジタル署名を含む、ステップと、
前記ネットワークノードによって、前記第2のデジタル署名に基づいて前記第2のクライ

アントデバイスが前記機密データ要素を取得する権限があるかどうかを決定するステップと、
前記第2のクライアントデバイスが前記機密データ要素を取得する権限があるとの決定に応じて、前記ネットワークノードによって、前記第2のクライアントデバイスに応答を送信するステップであって、前記応答が、暗号化された前記機密データ要素を含む、ステップと
をさらに含む、請求項1から6のいずれか一項に記載の方法。
【請求項８】
ブロックチェーンネットワークに記憶された機密データ要素を管理するための装置であって、請求項1から7のいずれか一項に記載の方法を実施するための複数のモジュールを備える、装置。
【請求項９】
ブロックチェーンネットワークに記憶された機密データ要素を管理するためのシステムであって、
1つまたは複数のプロセッサと、
前記1つまたは複数のプロセッサに結合され、前記1つまたは複数のプロセッサに、請求項1から7のいずれか一項に記載の方法を実行させる命令を記憶した1つまたは複数のコンピュータ可読メモリと
を含む、システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書は、ブロックチェーンネットワークに記憶された機密データ要素(sensitive data element)を管理することに関する。
【背景技術】
【０００２】
コンセンサスネットワークおよび/またはブロックチェーンネットワークと呼ばれることもある分散台帳システム(DLS: Distributed ledger system)は、参加するエンティティがデータを安全かつ不変に記憶することを可能にする。DLSは、任意の特定のユーザ事例に関係なく、一般にブロックチェーンネットワークと呼ばれる。ブロックチェーンネットワークのタイプの例は、パブリックブロックチェーンネットワーク、プライベートブロックチェーンネットワーク、およびコンソーシアムブロックチェーンネットワークを含むことができる。コンソーシアムブロックチェーンネットワークは、コンセンサスプロセスを制御するエンティティの選択グループに提供され、アクセス制御層を含む。
【０００３】
ブロックチェーンネットワークを含むコンピュータネットワークで送信されるデータは、個人を突き止めることができ、開示されれば、その個人への害または損失を生じることがある、個人情報などの機密のデータ(たとえば、生体データ、医療情報、および社会保障番号)を含むことができる。機密のデータは、競争相手または一般大衆に発見される場合、企業体に危険をもたらす機密のビジネス情報(たとえば、営業秘密、取得計画、および財務データ)を含むこともできる。機密のデータは、政府機関に関係する極秘扱いの情報を含むことができ、情報セキュリティを保護するために機微のレベル(たとえば、制限付き(restricted)、秘匿(confidential)、秘密(secret)、およびトップシークレット(top secret))に従って制限される。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
コンピュータネットワークにおける機密のデータのデータセキュリティ問題に対処する解決策を提供することが望ましい。
【課題を解決するための手段】

【０００５】
本明細書は、ブロックチェーンネットワークに記憶された機密データ要素を管理するための技術を説明する。これらの技術は、一般的に、ブロックチェーンネットワークにおいてウォッチリスト(ブロックチェーンベースのウォッチリストとも呼ばれる)を実装することを含む。ウォッチリストは、1つまたは複数の、権限を与えられた機関(authorized entity)(たとえば、機構、規制機関、官庁、または政府)によるモニタリングおよび/またはフィルタリングを受ける1つまたは複数の機密データ要素を含む。機密データ要素は、機密の、個人的な、および/または秘匿の情報を含む、またはこれに関係することがある。いくつかの実施形態では、ブロックチェーンベースのウォッチリストは、機密データ要素をブロックチェーンネットワークに分散的に記憶する。いくつかの実施形態では、ブロックチェーンベースのウォッチリストは、ウォッチリストに記憶された機密データ要素の管理を容易にすることができる。いくつかの実施形態では、ブロックチェーンベースのウォッチリストは、機密データ要素の改ざん防止保護を与え、ウォッチリストに対する悪意のあるアクションおよびサイバー攻撃を予防することによって、強化されたデータセキュリティを実現することができる。
【０００６】
本明細書はまた、1つまたは複数のプロセッサに結合され、命令を記憶している1つまたは複数の非一時的コンピュータ可読記憶媒体を提供し、命令は、1つまたは複数のプロセッサによって実行されると、1つまたは複数のプロセッサに、本明細書で提供する方法の実施形態による動作を実行させる。
【０００７】
本明細書は、本明細書で提供する方法を実施するためのシステムをさらに提供する。このシステムは、1つまたは複数のプロセッサと、1つまたは複数のプロセッサに結合され、命令を記憶しているコンピュータ可読記憶媒体とを含み、命令は、1つまたは複数のプロセッサによって実行されると、1つまたは複数のプロセッサに、本明細書で提供する方法の実施形態による動作を実行させる。
【０００８】
本明細書による方法は、本明細書で説明する態様および特徴のいかなる組合せも含み得ることを諒解されたい。すなわち、本明細書による方法は、具体的に本明細書で説明する態様および特徴の組合せに限定されず、与えられる態様および特徴のいかなる組合せもまた含む。
【０００９】
本明細書の1つまたは複数の実施形態の詳細について、添付の図面および以下の説明に示す。本明細書の他の特徴および利点は、説明および図面から、ならびに特許請求の範囲から明らかとなるであろう。
【図面の簡単な説明】
【００１０】
【図１】本明細書の実施形態を実行するために使用できる環境の一例を示す図である。
【図２】本明細書の実施形態によるアーキテクチャの一例を示す図である。
【図３】本明細書の実施態様によるシステムの一例を示す図である。
【図４】本明細書の実施形態により実行できるプロセスの一例を示す図である。
【図５】本明細書の実施形態により実行できるプロセスの一例を示す図である。
【図６】本明細書の実施形態による装置のモジュールの例を示す図である。
【発明を実施するための形態】
【００１１】
様々な図面における同じ参照番号および名称は、同じ要素を示す。
【００１２】
本明細書は、ブロックチェーンネットワークに記憶された機密データ要素を管理するための技術を説明する。これらの技術は、一般的に、ブロックチェーンネットワークにおいてウォッチリスト(ブロックチェーンベースのウォッチリストとも呼ばれる)を実装するこ

とを含む。ウォッチリストは、1つまたは複数の権限を与えられた機関(たとえば、機構、規制機関、官庁、または政府)によるモニタリングおよび/またはフィルタリングを受ける1つまたは複数の機密データ要素を含む。機密データ要素は、機密の、個人的な、および/または秘匿情報を含む、またはそれに関係することがある。いくつかの実施形態では、ブロックチェーンベースのウォッチリストは、機密データ要素をブロックチェーンネットワークに分散的に記憶する。いくつかの実施形態では、ブロックチェーンベースのウォッチリストは、ウォッチリストに記憶された機密データ要素の管理を容易にすることができる。いくつかの実施形態では、ブロックチェーンベースのウォッチリストは、機密データ要素の改ざん防止保護を与え、ウォッチリストに対する悪意のあるアクションおよびサイバー攻撃を予防することによって、強化されたデータセキュリティを実現することができる。

【００１３】

本明細書で説明する技法は、1つまたは複数の技術的効果をもたらす。いくつかの実施形態では、ブロックチェーンネットワークにウォッチリストを実装することができる。ウォッチリストは、1つまたは複数の権限を与えられた機関によるモニタリングおよび/またはフィルタリングを受ける1つまたは複数の機密データ要素を含むことができる。ウォッチリスト内の機密データ要素は、ブロックチェーンネットワークに分散的に記憶される。分散ブロックチェーンネットワークの改ざん防止の性質により、ウォッチリストに対する悪意のあるアクションおよびサイバー攻撃を軽減することができる。いくつかの実施形態では、ブロックチェーンベースのウォッチリストは、ウォッチリストに記憶された機密データ要素の管理を容易にすることができる。たとえば、クライアントデバイスがブロックチェーンネットワークに記憶されたウォッチリストの変更を行う要求を提示するとき、要求を受け取るブロックチェーンネットワークのネットワークノードは、要求内のクライアントデバイスのデジタル署名に基づいてクライアントデバイスを認証することができる。いくつかの実施形態では、認証されるクライアントデバイスは、変更を行うことを許され得るが、認証されないクライアントデバイスは、変更を行うことを拒否されることになる。これは、ブロックチェーンネットワークに記憶された機密のデータが、悪意のある行為者によって損なわれることを防ぎ、それによってウォッチリストのデータセキュリティを向上させることができる。いくつかの実施形態では、ウォッチリスト内の機密データ要素は、たとえば、暗号化アルゴリズムを使用して、暗号化される。いくつかの実施形態では、権限を与えられた当事者のみが、暗号化されたデータ要素を復号し、機密データ要素を取得することができる。これは、悪意のある行為者がブロックチェーンネットワークに潜入し、機密データ要素を取得することを防ぎ、それによってウォッチリストのデータセキュリティを向上させることができる。

【００１４】

本明細書の実施形態のさらなるコンテキストを与えると、上記で紹介したように、(たとえば、ピアツーピアノードから構成される)コンセンサスネットワークと呼ばれることもある分散台帳システム(DLS)、およびブロックチェーンネットワークは、参加するエンティティが安全かつ不変にトランザクションを行い、データを記憶することを可能にする。ブロックチェーンという用語は、一般に特定のネットワーク、および/または使用事例に関連するが、本明細書ではブロックチェーンは、特定の使用事例に関係なく、一般的にDLSを指すように使用される。

【００１５】

ブロックチェーンは、トランザクションが不変であるような方法でトランザクションを記憶するデータ構造である。したがって、ブロックチェーンに記録されたトランザクションは、信頼でき、信用の置けるものである。ブロックチェーンは、1つまたは複数のブロックを含む。チェーン内の各ブロックは、チェーンにおけるその直前の前のブロックに、前のブロックの暗号学的ハッシュを含むことによってリンクされる。各ブロックはまた、タイムスタンプ、それ自体の暗号学的ハッシュ、および1つまたは複数のトランザクションを含む。ブロックチェーンネットワークのノードによってすでに検証されたトランザク

ションは、ハッシュされ、マークルツリー(Merkle tree)に符号化される。マークルツリーは、ツリーのリーフノードのデータがハッシュされ、ツリーの各ブランチのすべてのハッシュがブランチのルートで連結されるデータ構造である。このプロセスは、ツリー内のすべてのデータを表すハッシュを記憶するツリー全体のルートまで、ツリーを上って続く。ツリーに記憶されたトランザクションのものとされるハッシュを、それがツリーの構造に一致するかどうかを決定することによって迅速に検証することができる。

【００１６】

ブロックチェーンは、トランザクションを記憶するための、非集中型または少なくとも部分的に非集中型データ構造であるが、ブロックチェーンネットワークは、トランザクションをブロードキャストすること、検証すること、および確認すること(validating)などによって、1つまたは複数のブロックチェーンを管理し、更新し、維持するコンピューティングノードのネットワークである。上記で紹介したように、ブロックチェーンネットワークは、パブリックブロックチェーンネットワーク、プライベートブロックチェーンネットワーク、またはコンソーシアムブロックチェーンネットワークとして提供されることがある。本明細書ではコンソーシアムブロックチェーンネットワークに関して、本明細書の実施形態をさらに説明する。しかしながら、本明細書の実施形態は、任意の適切なタイプのブロックチェーンネットワークで実現され得ると考えられる。

【００１７】

一般に、コンソーシアムブロックチェーンネットワークは、参加するエンティティの間でプライベートである。コンソーシアムブロックチェーンネットワークでは、コンセンサスプロセスは、コンセンサスノードと呼ばれることがある、権限を与えられたノードのセットによって制御され、1つまたは複数のコンセンサスノードが、それぞれのエンティティ(たとえば、金融機関、保険会社)によって操作される。たとえば、10個の(10)エンティティ(たとえば、金融機関、保険会社)のコンソーシアムが、コンソーシアムブロックチェーンネットワークを操作することができ、その各々が、コンソーシアムブロックチェーンネットワーク内の少なくとも1つのノードを操作する。

【００１８】

いくつかの例では、コンソーシアムブロックチェーンネットワーク内で、グローバルブロックチェーンが、すべてのノードにわたって複製されるブロックチェーンとして与えられる。すなわち、すべてのコンセンサスノードが、グローバルブロックチェーンに関してコンセンサスの完全状態である。コンセンサス(たとえば、ブロックチェーンへのブロックの追加の合意)を実現するために、コンソーシアムブロックチェーンネットワーク内にコンセンサスプロトコルが実装される。たとえば、コンソーシアムブロックチェーンネットワークは、以下でさらに詳細に説明する、実用的ビザンチンフォールトトレランス(PBFT: practical Byzantine fault tolerance)コンセンサスを実装することができる。

【００１９】

図1は、本明細書の実施形態を実行するために使用できる環境100の一例を示す図である。いくつかの例では、環境100は、エンティティがコンソーシアムブロックチェーンネットワーク102に参加することを可能にする。環境100は、コンピューティングデバイス106、108、およびネットワーク110を含む。いくつかの例では、ネットワーク110は、ローカルエリアネットワーク(LAN)、ワイドエリアネットワーク(WAN)、インターネット、またはそれらの組合せを含み、ウェブサイト、ユーザデバイス(たとえば、コンピューティングデバイス)、バックエンドシステムを接続する。いくつかの例では、ネットワーク110は、ワイヤードおよび/またはワイヤレス通信リンクを介してアクセスすることができる。いくつかの例では、ネットワーク110は、コンソーシアムブロックチェーンネットワーク102との通信、およびコンソーシアムブロックチェーンネットワーク102内での通信を可能にする。一般に、ネットワーク110は、1つまたは複数の通信ネットワークを表す。場合によっては、コンピューティングデバイス106、108は、クラウドコンピューティングシステム(図示せず)のノードであることがあり、または各コンピューティングデバイス106、108が、ネットワークによって相互接続された、いくつかのコンピュータを含み、分散処理シス

テムとして機能する、別個のクラウドコンピューティングシステムであることがある。

【００２０】

図示した例では、コンピューティングシステム106、108は各々、コンソーシアムブロックチェーンネットワーク102でのノードとしての参加を可能にする任意の適切なコンピューティングシステムを含むことができる。コンピューティングデバイスの例は、限定はしないが、サーバ、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピューティングデバイス、およびスマートフォンを含む。いくつかの例では、コンピューティングシステム106、108は、コンソーシアムブロックチェーンネットワーク102と対話するための1つまたは複数のコンピュータ実装サービスをホストする。たとえば、コンピューティングシステム106は、第1のエンティティ(たとえば、ユーザA)が1つまたは複数の他のエンティティ(たとえば、他のユーザ)とのそのトランザクションを管理するために使用するトランザクション管理システムなど、第1のエンティティのコンピュータ実装サービスをホストすることができる。コンピューティングシステム108は、第2のエンティティ(たとえば、ユーザB)が1つまたは複数の他のエンティティ(たとえば、他のユーザ)とのトランザクションを管理するために使用するトランザクション管理システムなど、第2のエンティティのコンピュータ実装サービスをホストすることができる。図1の例では、コンソーシアムブロックチェーンネットワーク102は、ノードのピアツーピアネットワークとして表され、コンピューティングシステム106、108は、コンソーシアムブロックチェーンネットワーク102に参加する、それぞれ第1のエンティティのノード、および第2のエンティティのノードを与える。

【００２１】

図2は、本明細書の実施形態によるアーキテクチャ200の一例を示す。例示的な概念アーキテクチャ200は、参加者A、参加者B、および参加者Cにそれぞれ対応する参加者システム202、204、206を含む。各参加者(たとえば、ユーザ、企業)が、複数のノード214を含むピアツーピアネットワークとして与えられるブロックチェーンネットワーク212に参加し、複数のノード214のうちの少なくとも一部が、ブロックチェーン216に情報を不変に記録する。ブロックチェーンネットワーク212内に単一のブロックチェーン216が概略的に示されているが、ブロックチェーン216の複数のコピーが与えられ、本明細書でさらに詳細に説明するように、ブロックチェーンネットワーク212にわたって維持される。

【００２２】

図示した例では、各参加者システム202、204、206が、それぞれ参加者A、参加者B、および参加者Cによって、またはこれらの参加者のために与えられ、ブロックチェーンネットワーク内のそれぞれのノード214として機能する。本明細書で使用するノードは、一般に、ブロックチェーンネットワーク212に接続され、それぞれの参加者がブロックチェーンネットワークに参加できるようにする個々のシステム(たとえば、コンピュータ、サーバ)を指す。図2の例では、参加者が、各ノード214に対応する。しかしながら、参加者がブロックチェーンネットワーク212内の複数のノード214を操作できる、および/または複数の参加者がノード214を共有できることが考えられる。いくつかの例では、参加者システム202、204、206は、プロトコル(たとえば、ハイパーテキスト転送プロトコルセキュア(HTTPS))を使用して、および/またはリモートプロシージャコール(RPC)を使用して、ブロックチェーンネットワーク212と、またはブロックチェーンネットワーク212を介して通信する。

【００２３】

ノード214は、ブロックチェーンネットワーク212内の参加の様々な度合いを有することができる。たとえば、いくつかのノード214は、コンセンサスプロセスに(たとえば、ブロックチェーン216にブロックを追加するマインダーノード(minder node)として)参加することができ、他のノード214は、コンセンサスプロセスに参加しない。別の例として、いくつかのノード214は、ブロックチェーン216の完全なコピーを記憶し、他のノード214は、ブロックチェーン216の一部分のコピーを記憶するにすぎない。たとえば、データアクセス特権が、それぞれの参加者がそのそれぞれのシステム内に記憶するブロックチェーン

データを制限することができる。図2の例では、参加者システム202、204は、ブロックチェーン216のそれぞれの、完全なコピー216'、216''を記憶する。

【００２４】

ブロックチェーン(たとえば、図2のブロックチェーン216)は、各ブロックがデータを記憶したブロックのチェーンから構成される。データの例は、2人以上の参加者間のトランザクションを表すトランザクションデータを含む。本明細書では非限定的な例としてトランザクションが使用されるが、任意の適切なデータをブロックチェーンに記憶することができる(たとえば、文書、画像、映像、音声)と考えられる。トランザクションの例は、限定はしないが、価値のある何か(たとえば、資産、製品、サービス、通貨)の交換を含むことができる。トランザクションデータは、ブロックチェーン内に不変に記憶される。すなわち、トランザクションデータを変えることはできない。

【００２５】

ブロックに記憶する前に、トランザクションデータはハッシュされる。ハッシングは、(文字列データとして提供される)トランザクションデータを(同じく文字列データとして提供される)固定長ハッシュ値に変換するプロセスである。トランザクションデータを取得するために、ハッシュ値をハッシュ解除する(un-hash)ことはできない。ハッシングは、トランザクションデータのわずかな変更でも、完全に異なるハッシュ値が得られることを確実にする。さらに、上述のように、ハッシュ値は固定長である。すなわち、トランザクションデータのサイズにかかわらず、ハッシュ値の長さは固定される。ハッシングは、ハッシュ値を生成するためにハッシュ関数によりトランザクションデータを処理することを含む。ハッシュ関数の例は、限定はしないが、256ビットのハッシュ値を出力する、セキュアハッシュアルゴリズム(SHA)-256を含む。

【００２６】

複数のトランザクションのトランザクションデータがハッシュされ、ブロックに記憶される。たとえば、2つのトランザクションのハッシュ値が与えられ、別のハッシュを与えるためにそれら自体がハッシュされる。このプロセスは、すべてのトランザクションがブロックに記憶されるように、単一のハッシュ値が与えられるまで繰り返される。このハッシュ値は、マークルルートハッシュ(Merkle root hash)と呼ばれ、ブロックのヘッダに記憶される。トランザクションのいずれかの変更が、それのハッシュ値の変更、最終的にはマークルルートハッシュの変更をもたらすことになる。

【００２７】

コンセンサスプロトコルにより、ブロックチェーンにブロックが追加される。ブロックチェーンネットワーク内の複数のノードが、コンセンサスプロトコルに参加し、ブロックチェーンにブロックが追加される作業を行う。そのようなノードは、コンセンサスノードと呼ばれる。上記で紹介したPBFTが、コンセンサスプロトコルの非限定的な例として使用される。コンセンサスノードは、ブロックチェーンにトランザクションを追加し、ブロックチェーンネットワークの全体的な状態を更新するために、コンセンサスプロトコルを実行する。

【００２８】

さらに詳細には、コンセンサスノードは、ブロックヘッダを生成し、ブロック内のトランザクションのすべてをハッシュし、ブロック内のすべてのトランザクションに対する単一のハッシュ値が与えられるまで(マークルルートハッシュ)、さらなるハッシュ値を生成するために、2つ1組にしてハッシュ値を結合する。このハッシュは、ブロックヘッダに追加される。コンセンサスノードはまた、ブロックチェーン内の直近のブロック(すなわち、ブロックチェーンに追加された最後のブロック)のハッシュ値を決定する。コンセンサスノードはまた、ノンス値およびタイムスタンプをブロックヘッダに追加する。

【００２９】

一般に、PBFTが、ビザンチンフォールト(たとえば、誤動作を起こしているノード、悪意のあるノード)に耐性がある実用的ビザンチン状態機械複製(state machine replication)を与える。これは、不具合が発生すると仮定すること(たとえば、独立したノード障害

、および/またはコンセンサスノードによって送られた改ざんされたメッセージの存在を仮定すること)によってPBFTにおいて実現される。PBFTでは、コンセンサスノードは、プライマリコンセンサスノード、およびバックアップコンセンサスノードを含むシーケンスで与えられる。プライマリコンセンサスノードは、定期的に変更される。トランザクションは、ブロックチェーンネットワーク内のすべてのコンセンサスノードがブロックチェーンネットワークのワールド状態に関して合意に達することによってブロックチェーンに追加される。このプロセスでは、メッセージがコンセンサスノード間で送信され、各コンセンサスノードが、指定されたピアノードからメッセージが受信されることを証明し、メッセージが送信中に変更されなかったことを検証する。

【００３０】

PBFTでは、コンセンサスプロトコルは、すべてのコンセンサスノードが同じ状態で開始する複数のフェーズで与えられる。始めるには、クライアントが、サービス動作を呼び出す(たとえば、ブロックチェーンネットワーク内でトランザクションを実行する)ために、プライマリコンセンサスノードに要求を送る。要求を受け取ったことに応答して、プライマリコンセンサスノードが、バックアップコンセンサスノードに要求をマルチキャストする。バックアップコンセンサスノードは要求を実行し、各々がクライアントに返信を送る。クライアントは、しきい値数の返信が受け取られるまで待つ。いくつかの例では、クライアントは、f+1個の返信が受け取られるまで待ち、ここでfは、ブロックチェーンネットワーク内で許容することができる欠陥のあるコンセンサスノードの最大数である。最終結果は、十分な数のコンセンサスノードが、ブロックチェーンに追加される記録の順序に関して合意に達することであり、記録は受け入れられるか、または拒否される。

【００３１】

いくつかのブロックチェーンネットワークでは、トランザクションのプライバシーを維持するために、暗号法が実装される。たとえば、2つのノードが、ブロックチェーン内の他のノードがトランザクションの詳細を認識できないように、トランザクションをプライベートに維持したい場合、ノードはトランザクションデータを暗号化することができる。暗号法の例は、限定はしないが、対称暗号化、および非対称暗号化を含む。対称暗号化は、暗号化(平文から暗号文を生成する)と復号(暗号文から平文を生成する)の両方に単一の鍵を使用する暗号化プロセスを指す。対称暗号化では、同じ鍵が、複数のノードに利用可能であり、したがって各ノードはトランザクションデータを暗号化/復号することができる。

【００３２】

非対称暗号化は、プライベート鍵と、公開鍵とを各々含む鍵ペアを使用し、プライベート鍵は、それぞれのノードにしかわからず、公開鍵はブロックチェーンネットワーク内の他のいずれかまたはすべてのノードにわかっている。ノードは、データを暗号化するために他のノードの公開鍵を使用することができ、暗号化されたデータは、他のノードのプライベート鍵を使用して復号することができる。たとえば、再び図2を参照すると、参加者Aは、データを暗号化するために参加者Bの公開鍵を使用し、暗号化されたデータを参加者Bに送ることができる。参加者Bは、暗号化されたデータ(暗号文)を復号するためにそのプライベート鍵を使用し、元のデータ(平文)を引き出すことができる。あるノードの公開鍵で暗号化されたメッセージは、そのノードのプライベート鍵を使用してのみ復号することができる。

【００３３】

非対称暗号化は、デジタル署名を与えるために使用され、トランザクションの参加者がトラザクションの他の参加者、ならびにトランザクションの妥当性を確認することを可能にする。たとえば、あるノードは、メッセージにデジタルに署名することができ、他のノードは、参加者Aのデジタル署名に基づいてそのノードによってメッセージが送られたことを確認することができる。デジタル署名は、メッセージが伝送中に改ざんされないことを確実にするために使用することもできる。たとえば、再び図2を参照すると、参加者Aが、参加者Bにメッセージを送ろうとしている。参加者Aはメッセージのハッシュを生成し、

次いで、そのプライベート鍵を使用してハッシュを暗号化して、暗号化されたハッシュとしてデジタル署名を与える。参加者Aは、デジタル署名をメッセージに添付し、デジタル署名付きのメッセージを参加者Bに送る。参加者Bは、参加者Aの公開鍵を使用してデジタル署名を復号し、ハッシュを引き出す。参加者Bはメッセージをハッシュし、ハッシュを比較する。ハッシュが同じである場合、参加者Bは、メッセージが実際に参加者Aからのものであって、改ざんされていなかったことを確認することができる。

【００３４】

図3は、ブロックチェーンネットワークに記憶された機密データ要素を管理するシステム300の一例を示す図である。図示のように、システム300は、いくつかのブロックチェーンネットワークノード302a～fを含むブロックチェーンネットワーク310と、1つまたは複数のクライアントデバイス304とを含む。ブロックチェーンネットワーク310は、単に説明のために、6個のブロックチェーンネットワークノード302を含むように示されていることに留意する。ブロックチェーンネットワーク310は、任意の好適な数のブロックチェーンネットワークノード302を含むことができる。クライアントデバイス304は、任意の好適なコンピュータ、モジュール、サーバ、または本明細書で説明する方法を行うようにプログラムされたコンピューティング要素であることがある。

【００３５】

いくつかの実施形態では、ブロックチェーンネットワーク310は、権限を与えられた機関(たとえば、機構、規制機関、官庁、または政府)によるモニタリングおよび/またはフィルタリングを受ける機密データ要素を含むウォッチリストを記憶するように構成される。いくつかの実施形態では、機密データ要素は、プライバシー保護、データセキュリティ、および/または検閲もしくは監視目的で、モニタリングまたはフィルタリングされることがある。いくつかの例では、機密のデータは、個人を突き止めることができ、開示されれば、その個人への害または損失をもたらし得る個人的に識別可能な情報(たとえば、生体データ、医療情報、および社会保障番号)などの個人情報を含むことができる。いくつかの実施形態では、機密のデータは、競争相手または一般大衆に発見される場合、企業体に危険をもたらす機密のビジネス情報(たとえば、営業秘密、取得計画、および財務データ)を含むことができる。いくつかの実施形態では、機密のデータは、政府機関に関係する極秘扱いの情報を含むことができ、情報セキュリティを保護するために機微のレベル(たとえば、制限付き、秘匿、秘密、およびトップシークレット)に従って制限される。いくつかの実施形態では、機密のデータは、たとえば、特にテキスト、音声、映像、または画像のフォーマットを有することができる。いくつかの実施形態では、機密のデータは、潜在的なセキュリティ脅威をもたらす悪意のあるプログラムを含むことができる。

【００３６】

いくつかの実施形態では、ブロックチェーンネットワーク310のネットワークノード302(たとえば、ノード302a)が、クライアントデバイス304から要求を受け取る。要求は、ウォッチリストの変更の要求(たとえば、リストにデータ要素を追加すること、リストからデータ要素を削除すること、またはリストのデータ要素を編集することを求める要求)を含むことができる。ネットワークノード302aは、ブロックチェーンネットワークノード302のサブセット(たとえば、コンセンサスノード302a～d)が提案された変更についてコンセンサスに到達することができる場合、ウォッチリストの要求された変更を行うことができるように、ブロックチェーンネットワーク310内でコンセンサスプロシージャを開始することができる。

【００３７】

いくつかの実施形態では、ブロックチェーンネットワーク310は、コンセンサスプロシージャに参加しないブロックチェーンネットワークノード302のサブセット(たとえば、非コンセンサスノード302e～f)を含む。いくつかの実施形態では、ブロックチェーンネットワーク310のコンセンサスノード302a～dは、ウォッチリストの変更を行うようにとのクライアントデバイス304からの要求を処理することを許され得るが、ブロックチェーンネットワーク310の非コンセンサスノード302e～fは、ウォッチリストの変更を行うようにとの

クライアントデバイス304からの要求を処理することを許されない。たとえば、コンセンサスノード302は、ウォッチリストへのアクセスを制御し、ウォッチリストを定期的に更新する、権限を与えられた機関(たとえば、政府)のサーバに実装されることがあるが、非コンセンサスノード302は、ウォッチリストを変更する許可または権限なしで、コンセンサスノード302からウォッチリストを取得することができる、権限を与えられた機関の従属機関(たとえば、発行プラットフォーム)のサーバに実装されることがある。

【００３８】

図4は、本明細書の実施形態による信号フロー400の一例を示す。信号フロー400は、ブロックチェーンネットワークに記憶された機密データ要素を管理するためのプロセスを表す。便宜上、プロセスは、1つまたは複数の場所にある1つまたは複数のコンピュータのシステムによって行われ、本明細書に従って適切にプログラムされるものとして説明する。たとえば、適切にプログラムされた分散システム(たとえば、図3のシステム300)が、プロセスを行うことができる。

【００３９】

プロセス400は、クライアントデバイス(たとえば、クライアント304a)が、ブロックチェーンネットワークに記憶されたウォッチリストの変更を行うためにブロックチェーンネットワーク310に要求を送る402において始まる。たとえば、クライアント304aは、ブロックチェーンネットワーク310のコンセンサスノード302aに要求を送る。ウォッチリストは、1つまたは複数の権限を与えられた機関によるモニタリング、フィルタリング、または両方を受けるいくつかの機密データ要素(たとえば、キーワード)を含む。いくつかの実施形態では、ウォッチリストの変更は、リストにデータ要素を追加すること、リストからデータ要素を削除すること、またはリストのデータ要素を編集することのうちの1つまた複数を含む。いくつかの実施形態では、ウォッチリスト内の機密データ要素の一部または全部が、一般大衆に閲覧可能でないまたは知られないように、それらを暗号化することができる。

【００４０】

いくつかの実施形態では、要求は、クライアントデバイス304aの識別情報(たとえば、識別子)、およびクライアントデバイス304aのプライベート鍵を使用して生成されたデジタル署名を含む。デジタル署名は、クライアントデバイス304aの識別情報を検証または認証するために使用することができる。

【００４１】

404において、ブロックチェーンネットワークノード302aは、クライアントデバイス304aがブロックチェーンネットワーク310に記憶されたウォッチリストを変更する権限があるかどうかを決定する。いくつかの実施形態では、ブロックチェーンネットワークノード302aは、ウォッチリストを変更する権限があるクライアントデバイスの識別子を含むホワイトリストを記憶する。

【００４２】

いくつかの実施形態では、ブロックチェーンネットワークノード302aは、要求内のクライアントデバイス304aの識別子がホワイトリスト内のクライアントデバイスの識別子に一致するかどうかを決定することができる。追加または代替として、ブロックチェーンネットワークノード302aは、要求内のデジタル署名が、ホワイトリスト内のクライアントデバイスの公開鍵(たとえば、その識別子が要求内のクライアントデバイス304aの識別子に一致する、ホワイトリスト内のクライアントの公開鍵)を使用して復号できるかどうかを決定することができる。いくつかの実施形態では、ホワイトリスト内のクライアントデバイスの公開鍵は、ブロックチェーンネットワークに記憶される。ブロックチェーンネットワークノード302aは、ホワイトリスト内のクライアントデバイスの公開鍵をブロックチェーンネットワークから検索する、またはそれらを別のリソースから取得することができる。

【００４３】

要求内のデジタル署名が、ホワイトリスト内のクライアントデバイスの公開鍵を使用して生成された署名を使用して復号される場合、ブロックチェーンネットワークノード302a

は、要求内のクライアントデバイス304aによって生成されたハッシュを引き出すことができる。ブロックチェーンネットワークノード302aは、受け取った要求をハッシュし、生成されたハッシュを、デジタル署名から引き出されたハッシュと比較することができる。ハッシュが一致する場合、ブロックチェーンネットワークノード302aは、クライアントデバイス304aがウォッチリストを変更する権限があると決定し、プロセスは次のステップへ進む。ハッシュが一致しない、または要求内のデジタル署名が、ホワイトリスト内のどのクライアントデバイスの公開鍵を使用しても復号できない場合、ブロックチェーンネットワークノード302aは、クライアントデバイス304aがウォッチリストを変更する権限がないと決定し、プロセスを終了することができる。たとえば、ブロックチェーンネットワークノード302aはクライアントデバイス304aに、クライアントデバイス304aがウォッチリストを変更する権限がないことを示すエラーメッセージを送ることができ、要求は拒否される。

【００４４】

406において、ブロックチェーンネットワークノード302aは、クライアントデバイス304aからの提案された変更についてブロックチェーンネットワーク310内でコンセンサスプロシージャを開始する。ブロックチェーンネットワークノード302aは、ブロックチェーンネットワーク310内の他のコンセンサスノード302b～dを識別することができる。いくつかの実施形態では、コンセンサスプロシージャは、ブロックチェーンネットワーク310のコンセンサスノード302a～dの間で行われる。本明細書で説明するコンセンサスプロシージャの例は、特に、プルーフオブワーク(proof of work)、プルーフオブステーク(proof of stake)、または実用的ビザンチンフォールトトレランスを含む。たとえば、コンセンサスプロシージャは、コンセンサスノード302aが、他のコンセンサスノード(たとえば、ノード302b～d)に要求を検証するための初期メッセージをマルチキャストするステップと、コンセンサスノード302b～dが、スマートコントラクトを使用して要求を検証し、次いでノード302aに返信メッセージを送るステップと、コンセンサスノード302aが、同じ結果を有する異なるノードからのいくつかの返信メッセージを待つステップとを含むことができる。同じ結果を有する他のノードからの返信メッセージの数が所定のしきい値を超える場合、コンセンサスノード302aは、コンセンサスが達成されたと決定し、要求内の提案された変更を行うことができる。たとえば、変更が新しい機密データ要素をウォッチリストに追加することを含む場合、コンセンサスノード302aは、新しい機密データ要素をウォッチリストに記憶することができる。

【００４５】

408において、ブロックチェーンネットワークノード302aは、ブロックチェーンネットワーク310の他のネットワークノードに通知を送る。いくつかの実施形態では、通知は、クライアントデバイス304aからの要求内の変更、およびコンセンサスプロシージャを実行するよう他のネットワークノードに命令する要求を含む。いくつかの実施形態では、ブロックチェーンネットワークノード302aは、コンセンサスノード302a～dのみがコンセンサスプロシージャに参加するよう通知されるように、コンセンサスノード302b～dに通知を送る。

【００４６】

410において、ブロックチェーンネットワークノード302b～dは、コンセンサスプロシージャを実行する。いくつかの実施形態では、ノード302b～dの各々が、他のコンセンサスノードに要求を検証するための初期メッセージをマルチキャストし、同じ結果を有する異なるノードからのいくつかの返信メッセージを待つ。同じ結果を有する他のノードからの返信メッセージの数が所定のしきい値を超える場合、ブロックチェーンネットワークノード302b～dは、コンセンサスが達成されたと決定し、要求内の提案された変更を行うことができる。たとえば、変更が、ウォッチリストに新しい機密データ要素を追加することを含む場合、コンセンサスノード302a～dの各々が、新しい機密データ要素を含む更新されたウォッチリストを所有できるように、ブロックチェーンネットワークノード302b～dは、新しい機密データ要素をウォッチリストに記憶することができる。

【００４７】

412において、ブロックチェーンネットワークノード302b～dは、コンセンサスプロシージャが各ネットワークノードで実行され、コンセンサスが達成されたことを示す通知をネットワークノード302aに送る。

【００４８】

414において、ブロックチェーンネットワークノード302aは、他のコンセンサスノードからの通知に基づいて、ブロックチェーンネットワーク310のコンセンサスノードによってコンセンサスプロシージャが実行されたと決定する。いくつかの実施形態では、ブロックチェーンネットワークノード302aは、クライアントデバイス304aからの要求に基づいてブロックチェーントランザクションを生成し、ブロックチェーントランザクションに基づくマークルツリーのルートハッシュ値を計算する。マークルツリーのルートハッシュ値は、将来のコンセンサスプロシージャで悪意のあるネットワークノードを識別するためにコンセンサスノード302a～dによって使用され得る。

【００４９】

416において、クライアントデバイス(たとえば、クライアントデバイス304b)が、ブロックチェーンネットワーク310に記憶されたウォッチリスト内の機密データ要素を求めて、ブロックチェーンネットワークノード302aに照会要求を送る。いくつかの実施形態では、照会要求は、クライアントデバイス304bのプライベート鍵を使用して生成されたデジタル署名を含む。

【００５０】

418において、ブロックチェーンネットワークノード302aは、クライアントデバイス304bがウォッチリスト内の機密データ要素を取得する権限があるかどうかを決定する。いくつかの実施形態では、ブロックチェーンネットワークノード302aは、クライアントデバイス304bが、たとえば、要求内のデジタル署名、およびブロックチェーンネットワークノード302aに記憶されたホワイトリストに記載されている権限を与えられた機関の公開鍵に基づいて、404に関して説明した技法により、または別の方法で、ウォッチリスト内の機密データ要素を取得する権限があるかどうかを決定することができる。ブロックチェーンネットワークノード302aが、クライアントデバイス304bはウォッチリスト内の機密データ要素を取得する権限がないと決定する場合、ブロックチェーンネットワークノード302aは要求を拒否することができる。

【００５１】

420において、ブロックチェーンネットワークノード302aは、クライアントデバイス304bが機密データ要素を取得する権限があると決定することに応じて、機密データ要素をクライアントデバイス304bに送る。いくつかの実施形態では、機密データ要素は暗号化され、クライアントデバイス304bは暗号化された機密データ要素を受け取ることができる。いくつかの実施形態では、機密データ要素は、秘密鍵を使用して暗号化され得る。クライアントデバイス304bが秘密鍵を保有する場合、クライアントデバイス304bは、暗号化された機密データ要素を復号することによって機密データ要素を取得することができる。

【００５２】

図5は、ブロックチェーンネットワークに記憶された機密データ要素を管理するためのプロセス500の一例のフローチャートである。便宜上、プロセス500は、1つまたは複数の場所にある1つまたは複数のコンピュータのシステムによって行われ、本明細書に従って適切にプログラムされるものとして説明する。たとえば、適切にプログラムされた分散システム、たとえば、図3の分散システム300が、プロセス500を行うことができる。

【００５３】

502において、ブロックチェーンネットワークノード(たとえば、ブロックチェーンネットワークノード302)が、ブロックチェーンネットワーク(たとえば、ブロックチェーンネットワーク310)に記憶されたウォッチリストの変更を行うためにクライアントデバイス(たとえば、クライアントデバイス304)から要求を受け取る。いくつかの実施形態では、ブロックチェーンネットワークノードは、ブロックチェーンネットワークのコンセンサスノードとすることができる。いくつかの実施形態では、ウォッチリストは、たとえば、ネッ

トワークノード(たとえば、ブロックチェーンネットワークまたはインターネットなどの別のネットワーク)によるモニタリングおよび/またはフィルタリングを受ける(たとえば、キーワードの形式の)いくつかの機密データ要素を含む。いくつかの実施形態では、要求は、クライアントデバイスのプライベート鍵を使用して生成されたデジタル署名を含む。いくつかの実施形態では、要求内の変更は、リストにデータ要素を追加する要求、リストからデータ要素を削除する要求、またはリストのデータ要素を編集する要求のうちの1つまた複数を含む。いくつかの実施形態では、ウォッチリスト内の機密データ要素は、暗号化することができる。

【００５４】

504において、ブロックチェーンネットワークノードは、クライアントデバイスがウォッチリストを変更する権限があるかどうかを決定する。いくつかの実施形態では、ブロックチェーンネットワークノードは、クライアントデバイスからの要求内のデジタル署名に基づいて、クライアントデバイスがウォッチリストを変更する権限があるかどうかを決定する。いくつかの実施形態では、ブロックチェーンネットワークノードは、ウォッチリストを変更する権限がある1つまたは複数のクライアントデバイスの識別子および/または公開鍵を含むホワイトリストを記憶する。いくつかの実施形態では、ネットワークノードによって、デジタル署名に基づいてクライアントデバイスがウォッチリストを変更する権限があるかどうかを決定することは、たとえば、404に関して説明した技法により、または別の方法で、要求内のデジタル署名と、ウォッチリストを変更する権限がある、権限を与えられた機関の公開鍵とに基づいて、クライアントデバイスがウォッチリストを変更する権限があると決定することを含む。

【００５５】

クライアントデバイスが、ウォッチリストを変更する権限があると決定される場合、プロセスはステップ506へ進む。クライアントデバイスが、ウォッチリストを変更する権限がないと決定される場合、プロセスはステップ516へ進み、要求は拒否される。

【００５６】

506において、ブロックチェーンネットワークノードは、クライアントデバイスがウォッチリストを変更する権限があると決定されると決定した後、ブロックチェーンネットワーク内で要求についてコンセンサスプロシージャを行う。本明細書で説明するコンセンサスプロシージャの例は、特に、プルーフオブワーク、プルーフオブステーク、または実用的ビザンチンフォールトトレランスを含む。いくつかの実施形態では、ブロックチェーンネットワークノードは、ブロックチェーンネットワーク内の他のコンセンサスノードを識別することができる。いくつかの実施形態では、コンセンサスプロシージャは、ブロックチェーンネットワークのコンセンサスノードの間で行われる。たとえば、コンセンサスプロシージャは、ブロックチェーンネットワークノードが、他のコンセンサスノードに要求を検証するための初期メッセージをマルチキャストするステップと、他のコンセンサスノードが、スマートコントラクトを使用して要求を検証し、次いでブロックチェーンネットワークノードに返信メッセージを送るステップと、ブロックチェーンネットワークノードが、同じ結果を有する異なるノードからのいくつかの返信メッセージを待つステップとを含むことができる。同じ結果を有する他のコンセンサスノードからの返信メッセージの数が所定のしきい値を超える場合、ブロックチェーンネットワークノードは、コンセンサスが達成されたと決定することができる。

【００５７】

508において、ブロックチェーンネットワークノードは、コンセンサスプロシージャを完了したと決定し、コンセンサスが達成されたと決定した後、要求内の変更を行う。いくつかの例では、変更が新しい機密データ要素をウォッチリストに追加することを含む場合、ブロックチェーンネットワークノードは、新しい機密データ要素をウォッチリストに記憶することができる。いくつかの実施形態では、ブロックチェーンネットワークノードは、新しい機密データ要素をウォッチリストに記憶する前に、新しい機密データ要素を暗号化することができる。

【００５８】
510において、ブロックチェーンネットワークノードは、たとえば、第2のクライアントデバイスから、ブロックチェーンネットワークに記憶されたウォッチリスト内の機密データ要素を求める照会要求を受け取る。いくつかの実施形態では、照会要求は、第2のクライアントデバイスのプライベート鍵を使用して生成された第2のデジタル署名を含む。
【００５９】
512において、ブロックチェーンネットワークノードは、第2のデジタル署名に基づいて、第2のクライアントデバイスが、機密データ要素を調べる、これにアクセスする、または場合によってはこれを取得する権限があるかどうかを決定する。いくつかの実施形態では、ブロックチェーンネットワークノードは、ウォッチリスト内の機密データ要素を調べる、これにアクセスする、または場合によってはこれを取得する(ウォッチリストを照会すると総称される)権限を与えられた1つまたは複数のクライアントデバイスの識別子および/または公開鍵を含むホワイトリストを記憶する。いくつかの実施形態では、ホワイトリストは、ウォッチリストを変更する権限がある1つまたは複数のクライアントデバイスの識別子および/または公開鍵を含むホワイトリストと同じまたはこれとは異なるものであることがある。いくつかの実施形態では、クライアントデバイスは、ウォッチリストの許容される動作に関するさらなるまたは異なる権限レベルを割り当てられることがあり、単一のまたは複数のホワイトリストに示されることがある。
【００６０】
いくつかの実施形態では、ネットワークノードによって、デジタル署名に基づいてクライアントデバイスがウォッチリストを照会する権限があるかどうかを決定することは、たとえば、404に関して説明した技法により、または別の方法で、デジタル署名と、ウォッチリストを照会する権限がある、権限を与えられた機関の公開鍵とに基づいて、クライアントデバイスがウォッチリストを照会する権限があると決定することを含む。
【００６１】
クライアントデバイスが、ウォッチリストを照会する権限があると決定される場合、プロセスはステップ514へ進む。クライアントデバイスが、ウォッチリストを照会する権限がないと決定される場合、プロセスはステップ518へ進み、照会要求は拒否される。
【００６２】
514において、第2のクライアントデバイスが機密データ要素を取得する権限があると決定することに応じて、ブロックチェーンネットワークノードは、第2のクライアントデバイスに応答を送信する。応答は、要求された機密データ要素を含む。いくつかの実施形態では、ウォッチリスト内の機密データ要素は暗号化され、応答は、暗号化された機密データ要素を含む。
【００６３】
図6は、本明細書の実施形態による装置600のモジュールの一例の図である。装置600は、ブロックチェーンネットワークに記憶された機密データ要素を管理するように構成されたブロックチェーンネットワークのノードの実施形態の一例とすることができる。装置600は、上記で説明した実施形態に対応することができ、装置600は、ブロックチェーンネットワークに記憶されているウォッチリストの変更を行うようにとのクライアントデバイスからの要求を受け取る受取モジュール602であって、ウォッチリストが複数の機密データ要素を含み、要求がクライアントデバイスのプライベート鍵を使用して生成されたデジタル署名を含む、受取モジュール602と、デジタル署名に基づいて、クライアントデバイスがウォッチリストを変更する権限があるかどうかを決定する決定モジュール604と、クライアントデバイスがウォッチリストを変更する権限があると決定することに応じて、ブロックチェーンネットワーク内で要求についてコンセンサスプロシージャを行う実行モジュール606と、コンセンサスプロシージャを完了した後にコンセンサスが達成されたと決定することに応じて、ウォッチリストの変更を行う実行モジュール608と、ウォッチリストの変更を行うようにとのクライアントデバイスからの要求を拒否する拒否モジュール610とを含む。

【００６４】
オプションの実施形態では、複数の機密データ要素は、1つまたは複数の権限を与えられた機関によるモニタリング、フィルタリング、または両方を受ける。
【００６５】
オプションの実施形態では、ウォッチリストの変更を行う要求は、新しい機密データ要素をウォッチリストに追加する要求、機密データ要素をウォッチリストから取り除く要求、またはウォッチリスト内の機密データ要素を編集する要求のうちの1つまた複数を含む。
【００６６】
一実施形態では、複数の機密データ要素は暗号化される。
【００６７】
オプションの実施形態では、装置600は、デジタル署名と、ウォッチリストを変更する権限がある、権限を与えられた機関の公開鍵とに基づいて、クライアントデバイスがウォッチリストを変更する権限があると決定する決定サブモジュールをさらに含む。
【００６８】
オプションの実施形態では、権限を与えられた機関は、ネットワークノードに記憶されたホワイトリストに示され、ホワイトリストは、ウォッチリストを変更する権限がある、1つまたは複数の権限を与えられた機関を含む。
【００６９】
オプションの実施形態では、装置600は、ブロックチェーンネットワークに記憶されたウォッチリスト内の機密データ要素を求める第2のクライアントデバイスからの照会要求を受け取る受取モジュールであって、照会要求が、第2のクライアントデバイスのプライベート鍵を使用して生成された第2のデジタル署名を含む、受取モジュールと、第2のデジタル署名に基づいて第2のクライアントデバイスが機密データ要素を取得する権限があるかどうかを決定する決定モジュールと、第2のクライアントデバイスに応答を送信する送信モジュールであって、応答が、暗号化された機密データ要素を含む、送信モジュールとをさらに含む。
【００７０】
先の実施形態で示したシステム、装置、モジュール、またはユニットは、コンピュータチップもしくはエンティティを使用することによって実装されることがあり、またはある機能を有する製品を使用することによって実装されることがある。一般的な実施形態デバイスはコンピュータであり、コンピュータは、パーソナルコンピュータ、ラップトップコンピュータ、携帯電話、カメラ電話、スマートフォン、携帯情報端末、メディアプレーヤ、ナビゲーションデバイス、電子メール受信および送信デバイス、ゲーム機、タブレットコンピュータ、ウェアラブルデバイス、またはこれらのデバイスの任意の組合せであることがある。
【００７１】
装置内の各モジュールの機能および役割の実施形態プロセスについては、先の方法の対応するステップの実施形態プロセスを参照することができる。本明細書では簡単のために詳細を省く。
【００７２】
装置実施形態は基本的に、方法実施形態に対応するので、関連する部分については、方法実施形態での関連する説明を参照することができる。前述の装置実施形態は、一例にすぎない。分かれた部分として説明するモジュールは、物理的に分かれている、または物理的に分かれていないことがあり、モジュールとして表示する部分が、物理モジュールである、もしくは物理モジュールではないことがある、1つの場所に設置されることがある、または複数のネットワークモジュールに分散されることがある。モジュールの一部または全部が、本明細書の解決策の目的を達成するために実際の需要に基づいて選択され得る。当業者は、創造的努力なしに、本出願の実施形態を理解し、実施することができる。
【００７３】

再び図6を参照すると、図6は、ブロックチェーンデータ要素管理装置の内部機能モジュールおよび構造を示すと解釈することができる。ブロックチェーンデータ要素管理装置は、ブロックチェーンネットワークに記憶された機密データ要素を管理するように構成されたブロックチェーンネットワークノードの一例とすることができる。本質的に実行本体は、電子デバイスとすることができ、電子デバイスは、1つまたは複数のプロセッサと、1つまたは複数のプロセッサの実行可能命令を記憶するように構成されたメモリとを含む。

【００７４】

本明細書で説明する技法は、1つまたは複数の技術的効果をもたらす。いくつかの実施形態では、クライアントデバイスがブロックチェーンネットワークに記憶されたウォッチリストへの変更を行う要求を提示するとき、要求を受け取るブロックチェーンネットワークのネットワークノードは、要求中のクライアントデバイスのデジタル署名に基づいてクライアントデバイスを認証する必要がある。いくつかの実施形態では、認証されるクライアントデバイスは、変更を行うことを許され得るが、認証されないクライアントデバイスは、変更を行うことを拒否されることになる。これは、ブロックチェーンネットワークに記憶された機密のデータが、悪意のある行為者によって損なわれることを防ぎ、それによってブロックチェーンネットワークのデータセキュリティを向上させることができる。さらに、いくつかの実施形態では、ウォッチリスト内の機密データ要素は、暗号化される(たとえば、秘密鍵を使用して暗号化する)。秘密鍵を保有するクライアントデバイスのみが、暗号化されたデータ要素を復号し、機密データ要素を取得することができる。これは、悪意のある行為者がブロックチェーンネットワークに潜入し、機密データ要素を取得することを防ぎ、それによってブロックチェーンネットワークのデータセキュリティを向上させることができる。さらに、ウォッチリスト内の機密データ要素は、ブロックチェーンネットワークに分散的に記憶される。分散ブロックチェーンネットワークの改ざん防止の性質により、ウォッチリストに対する悪意のあるアクションおよびサイバー攻撃を軽減することができる。

【００７５】

主題の説明する実施形態は、1つまたは複数の特徴を、単独でまたは組み合わせて含むことができる。たとえば、第1の実施形態では、ブロックチェーンネットワークに記憶された機密データ要素を管理するための方法が、ブロックチェーンネットワークのネットワークノードによって、ブロックチェーンネットワークに記憶されたウォッチリストの変更を行うようにとのクライアントデバイスからの要求を受け取るステップであって、ウォッチリストが、複数の機密データ要素を含み、要求がクライアントデバイスのプライベート鍵を使用して生成されたデジタル署名を含む、受け取るステップと、ネットワークノードによって、デジタル署名に基づいてクライアントデバイスがウォッチリストを変更する権限があるかどうかを決定するステップと、クライアントデバイスがウォッチリストを変更する権限があるとの決定に応じて、ネットワークノードによって、ブロックチェーンネットワーク内で要求についてコンセンサスプロシージャを行うステップと、コンセンサスプロシージャを完了した後、コンセンサスが達成されたとの決定に応じて、ネットワークノードによってウォッチリストの変更を行うステップと、クライアントデバイスがウォッチリストを変更する権限がないとの決定に応じて、ネットワークノードによって、ウォッチリストの変更を行うようにとのクライアントデバイスからの要求を拒否するステップと含む。上記および他の説明した実施形態は各々、場合によっては、以下の特徴のうち1つまたは複数を含むことがある。

【００７６】

第1の特徴は、以下の特徴のいずれかと組合せ可能であるが、複数の機密データ要素が、1つまたは複数の権限を与えられた機関によるモニタリング、フィルタリング、または両方を受けることを指定する。

【００７７】

第2の特徴は、前または以下の特徴のいずれかと組合せ可能であるが、ウォッチリストの変更を行う要求が、新しい機密データ要素をウォッチリストに追加する要求、機密デー

タ要素をウォッチリストから取り除く要求、またはウォッチリスト内の機密データ要素を編集する要求のうちの1つまたは複数を含むことを指定する。

【００７８】

第3の特徴は、前または以下の特徴のいずれかと組合せ可能であるが、複数の機密データ要素が暗号化されることを指定する。

【００７９】

第4の特徴は、前または以下の特徴のいずれかと組合せ可能であるが、ネットワークノードによって、デジタル署名に基づいてクライアントデバイスがウォッチリストを変更する権限があるかどうかを決定することが、デジタル署名と、ウォッチリストを変更する権限がある権限を与えられた機関の公開鍵とに基づいて、クライアントデバイスがウォッチリストを変更する権限があることを決定することを含むと指定する。

【００８０】

第5の特徴は、前または以下の特徴のいずれかと組合せ可能であるが、権限を与えられた機関は、ネットワークノードに記憶されたホワイトリストに示され、ホワイトリストは、ウォッチリストを変更する権限がある、1つまたは複数の権限を与えられた機関を含むことを指定する。

【００８１】

第6の特徴は、前または以下の特徴のいずれかと組合せ可能であるが、方法が、ネットワークノードによって、ブロックチェーンネットワークに記憶されたウォッチリスト内の機密データ要素を求める第2のクライアントデバイスからの照会要求を受け取るステップであって、照会要求が、第2のクライアントデバイスのプライベート鍵を使用して生成された第2のデジタル署名を含む、受け取るステップと、ネットワークノードによって、第2のデジタル署名に基づいて、第2のクライアントデバイスが機密データ要素を取得する権限があるかどうかを決定するステップと、第2のクライアントデバイスが機密データ要素を取得する権限があるとの決定に応じて、ネットワークノードによって、第2のクライアントデバイスへの応答を送信するステップであって、応答が、暗号化された機密データ要素を含む、送信するステップとをさらに含むことを指定する。

【００８２】

本明細書で説明する主題およびアクションおよび動作の実施形態は、デジタル電子回路において、有形に具現化されたコンピュータソフトウェアもしくはファームウェアにおいて、本明細書で開示する構造およびそれらの構造的に同等のものを含む、コンピュータハードウェアにおいて、またはそれらの1つもしくは複数の組合せにおいて、実装されることがある。本明細書で説明する主題の実施形態は、1つまたは複数のコンピュータプログラムとして実装されることがあり、たとえば、データ処理装置によって実行されるように、またはデータ処理装置の動作を制御するために、コンピュータプログラムキャリア上に符号化されたコンピュータプログラム命令の1つまたは複数のモジュールとして実装されることがある。たとえば、コンピュータプログラムキャリアは、命令をその上に符号化されたまたは記憶された、1つまたは複数のコンピュータ可読記憶媒体を含むことができる。キャリアは、磁気、光磁気、もしくは光ディスク、ソリッドステートドライブ、ランダムアクセスメモリ(RAM)、読取り専用メモリ(ROM)、または他のタイプの媒体など、有形の非一時的コンピュータ可読媒体であってよい。代替的に、または追加として、キャリアは、人為的に生成した伝搬信号であってよく、たとえば、データ処理装置による実行のために好適な受信装置に送信するために情報を符号化するために生成される機械生成の電気、光、または電磁信号であってよい。コンピュータ記憶媒体は、機械可読ストレージデバイス、機械可読記憶基板、ランダムもしくはシリアルアクセスメモリデバイス、またはそれらのうちの1つもしくは複数の組合せである、またはその一部であることがある。コンピュータ記憶媒体は伝搬信号ではない。

【００８３】

プログラム、ソフトウェア、ソフトウェアアプリケーション、アプリ、モジュール、ソフトウェアモジュール、エンジン、スクリプト、またはコードと呼ばれる、または説明さ

れる場合もあるコンピュータプログラムは、コンパイラ型もしくはインタープリタ型言語、または宣言型もしくは手続き型言語を含む、プログラム言語の任意の形態で書くことができ、また、コンピュータプログラムは、スタンドアロンプログラムとして、またはモジュール、コンポーネント、エンジン、サブルーチン、もしくはコンピューティング環境で実行するのに適した他のユニットとしてなどの、任意の形態で展開することができる。

【００８４】

コンピュータプログラムは、ファイルシステムのファイルに対応する場合があるが、対応する必要はない。コンピュータプログラムは、他のプログラムまたはデータ、たとえば、マークアップ言語文書に記憶された1つまたは複数のスクリプトを入れたファイルの一部分に、当該プログラムに専用の単一ファイルに、または複数の協調ファイル、たとえば、1つもしくは複数のモジュール、サブプログラム、もしくはコードの一部を記憶するファイルに、記憶することができる。

【００８５】

コンピュータプログラムの実行用のプロセッサは、例として、汎用マイクロプロセッサと専用マイクロプロセッサの両方、および任意の種類のデジタルコンピュータの任意の1つまたは複数のプロセッサを含む。一般に、プロセッサが、プロセッサに結合された非一時的コンピュータ可読媒体から、実行のためのコンピュータプログラムの命令ならびにデータを受け取る。

【００８６】

「データ処理装置」という用語は、例としてプログラマブルプロセッサ、コンピュータ、または複数のプロセッサもしくはコンピュータを含む、データを処理するためのすべての種類の装置、デバイス、および機械を包含する。データ処理装置は、専用論理回路、たとえばFPGA(フィールドプログラマブルゲートアレイ)またはASIC(特定用途向け集積回路)、またはGPU(グラフィカル処理ユニット)を含むことができる。装置はまた、ハードウェアに加えて、コンピュータプログラムのための実行環境を作成するコード、たとえば、プロセッサファームウェアを構成するコード、プロトコルスタック、データベース管理システム、オペレーティングシステム、またはそれらのうちの1つもしくは複数の組合せを含むことができる。

【００８７】

本明細書で説明するプロセスおよび論理フローは、入力データ上で動作し、出力を生成することによって動作を行うために、1つまたは複数のコンピュータまたはプロセッサが1つまたは複数のコンピュータプログラムを実行することによって実施され得る。プロセスおよび論理フローは、専用論理回路、たとえば、FPGA、ASIC、もしくはGPUによって、または専用論理回路および1つもしくは複数のプログラムされたコンピュータの組合せによって実施されることもある。

【００８８】

コンピュータプログラムの実行に好適なコンピュータは、汎用または専用マイクロプロセッサ、または両方、または他の種類の中央処理ユニットに基づくことがある。一般的に中央処理ユニットは、読取り専用メモリ、またはランダムアクセスメモリ、または両方から命令およびデータを受け取ることになる。コンピュータの要素は、命令を実行するための中央処理ユニット、ならびに命令およびデータを記憶するための1つまたは複数のメモリデバイスを含むことができる。中央処理ユニットおよびメモリは、専用論理回路によって補われる、または専用論理回路に組み込まれることがある。

【００８９】

一般にコンピュータはまた、1つまたは複数の大容量ストレージデバイスを含む、またはこれらからデータを受信する、もしくはこれらにデータを転送するために動作可能に結合される。ストレージデバイスは、たとえば、磁気、光磁気、もしくは光ディスク、ソリッドステートドライブ、または任意の他のタイプの非一時的コンピュータ可読媒体であることがある。しかしながら、コンピュータがそのようなデバイスを有する必要はない。したがって、コンピュータが、1つまたは複数のメモリなど、ローカルおよび/またはリモー

トにある1つまたは複数のストレージデバイスに結合されてもよい。たとえば、コンピュータは、コンピュータの一体構成要素である1つまたは複数のローカルメモリを含むことがあり、またはコンピュータは、クラウドネットワークにある1つまたは複数のリモートメモリに結合されることがある。さらに、コンピュータが別のデバイス、たとえば、ほんのいくつかの例を挙げれば、携帯電話、携帯情報端末(PDA)、モバイルオーディオもしくはビデオプレーヤ、ゲーム機、全地球測位システム(GPS)レシーバ、またはポータブルストレージデバイス、たとえば、ユニバーサルシリアルバス(USB)フラッシュドライブに埋め込まれることがある。

【００９０】

構成要素は、直接または1つもしくは複数の中間構成要素を介して、電気的または光学的になど、交換可能に互いに結合されることによって、互いに「結合される」ことがある。構成要素はまた、構成要素の一方が他方に統合される場合、互いに「結合される」ことがある。たとえば、プロセッサに統合されるストレージ構成要素(たとえば、L2キャッシュ構成要素)は、プロセッサに「結合される」。

【００９１】

ユーザとの対話を可能にするために、本明細書で説明する主題の実施形態は、ユーザに情報を表示するためのディスプレイデバイス、たとえばLCD(液晶ディスプレイ)モニタと、ユーザがそれによりコンピュータに入力を与えることができる入力デバイス、たとえばキーボードおよびポインティングデバイス、たとえばマウス、トラックボール、またはタッチパッドとを有するコンピュータ上に実装される、またはコンピュータと通信するように構成されることがある。ユーザとの対話を可能にするために他の種類のデバイスが使用されることもあり、たとえばユーザに提供されるフィードバックは、任意の形態の感覚フィードバック、たとえば視覚フィードバック、聴覚フィードバック、もしくは触覚フィードバックであることが可能であり、ユーザからの入力は、音響入力、音声入力、もしくは触覚入力など、任意の形態で受け取ることができる。加えて、コンピュータが、ユーザによって使用されるデバイスに文書を送信し、そのデバイスから文書を受け取ることによって、たとえば、ウェブブラウザから受け取られる要求に応じてユーザのデバイス上のウェブブラウザにウェブページを送信することによって、またはユーザデバイス、たとえばスマートフォンもしくは電子タブレット上で動作しているアプリと対話することによって、ユーザと対話することができる。また、コンピュータが、パーソナルデバイス、たとえば、メッセージングアプリケーションを実行しているスマートフォンに、テキストメッセージまたは他の形態のメッセージを送信し、返信としてユーザから応答メッセージを受け取ることによってユーザと対話することができる。

【００９２】

本明細書は、システム、装置、およびコンピュータプログラムコンポーネントに関連して「ように構成される」という用語を使用する。1つまたは複数のコンピュータのシステムが特定の動作またはアクションを行うように構成されるとは、動作時にシステムに動作またはアクションを行わせるソフトウェア、ファームウェア、ハードウェア、またはそれらの組合せをシステムがインストールしていることを意味する。1つまたは複数のコンピュータプログラムが特定の動作またはアクションを行うように構成されるとは、1つまたは複数のプログラムが、データ処理装置によって実行されると、装置に動作またはアクションを行わせる命令を含むことを意味する。専用論理回路が特定の動作またはアクションを行うように構成されるとは、回路が動作またはアクションを行う電子論理を有することを意味する。

【００９３】

本明細書は、多くの特定の実施形態の詳細を含むが、これらは、特許請求の範囲自体によって定義される、特許請求されるものの範囲の制限と解釈されるべきではなく、むしろ特定の実施形態に固有であってもよい特徴の説明と解釈されるべきである。本明細書で別個の実施形態の文脈で説明されるいくつかの特徴は、単一の実施形態において組み合わせて実現されることもある。逆に、単一の実施形態の文脈で説明される様々な特徴は、複数

の実施形態において別々に、または任意の適切な部分的組合せで実現されることもある。さらに、特徴は、ある組合せで機能するものとして上記で説明され、さらに当初はそのように特許請求される場合があるが、特許請求される組合せからの1つまたは複数の特徴は、場合によってはその組合せから削除されることがあり、特許請求の範囲は、部分的組合せ、または部分的組合せの変形を対象とすることがある。

【００９４】

同様に、動作は特定の順序で図面に示され、特許請求の範囲に記載されるが、これは、望ましい結果を得るために、このような動作が図示された特定の順序でもしくは逐次的な順序で行われること、または例示したすべての動作が行われることを必要とするものと理解されるべきではない。いくつかの環境では、マルチタスクおよび並列処理が有利である場合がある。さらに、上記で説明した実施形態における様々なシステムモジュールおよび構成要素の分離は、すべての実施形態においてそのような分離を必要とすると理解されるべきではなく、記載するプログラム構成要素およびシステムは、一般的に単一のソフトウェア製品に統合される、または複数のソフトウェア製品にパッケージ化されることがあると理解されるべきである。

【００９５】

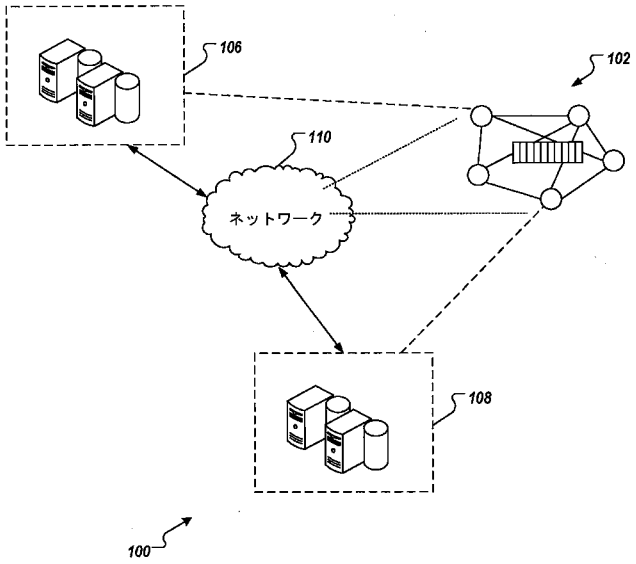
主題の特定の実施形態について説明した。他の実施形態も、特許請求の範囲内である。たとえば、特許請求の範囲に記載するアクションは、異なる順序で行われ、やはり望ましい結果を実現することがある。一例として、添付図に示すプロセスは、望ましい結果を達成するために、示した特定の順序、または逐次的な順序を必ずしも必要としない。場合によっては、マルチタスクおよび並列処理が有利である可能性がある。

【符号の説明】

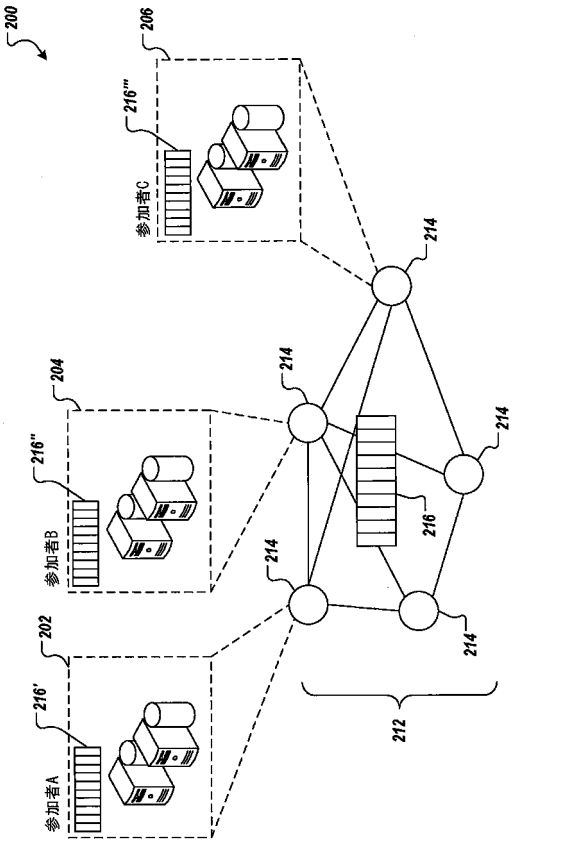
【００９６】

100 環境
102 コンソーシアムブロックチェーンネットワーク
106 コンピューティングデバイス
108 コンピューティングデバイス
110 ネットワーク
200 アーキテクチャ
202 参加者システム
204 参加者システム
206 参加者システム
212 ブロックチェーンネットワーク
214 ノード
216 ブロックチェーン
300 システム
302 ブロックチェーンネットワークノード
304 クライアントデバイス
310 ブロックチェーンネットワーク
600 装置
602 受取モジュール
604 決定モジュール
606 実行モジュール
608 実行モジュール
610 拒否モジュール

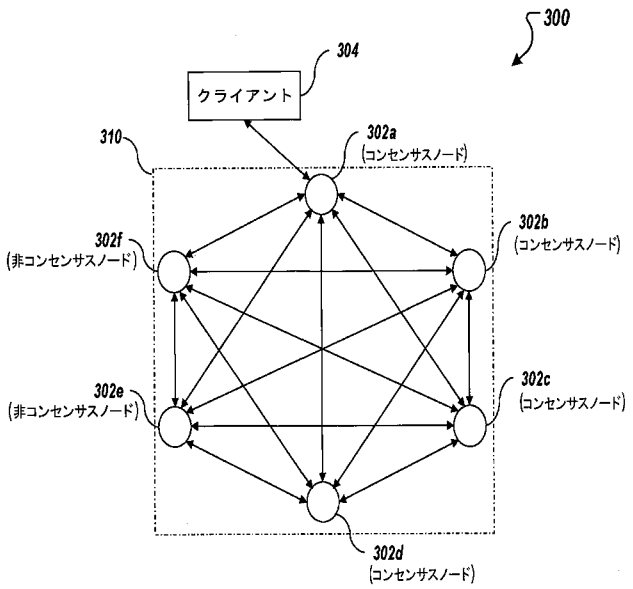
【図１】


106
102
110
ネットワーク
108
100

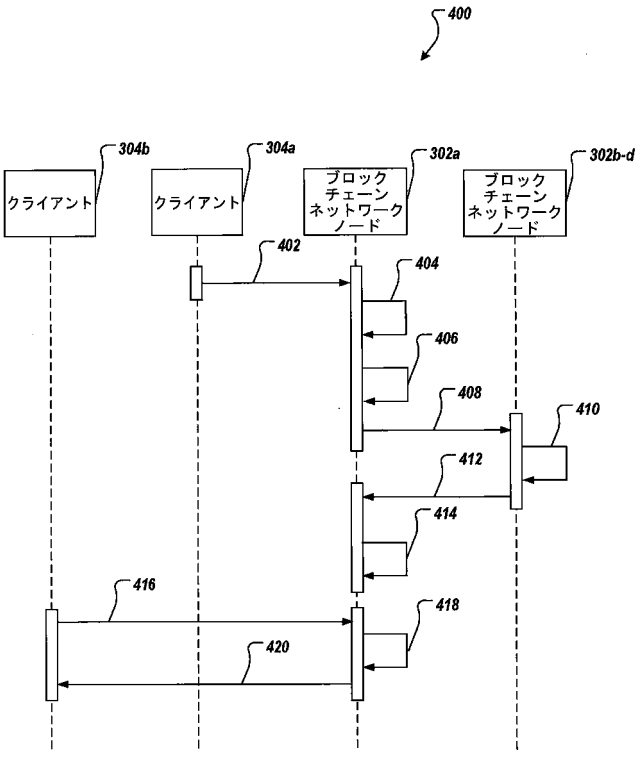
【図２】


200
206
216'''
参加者C
214
204
214
216''
参加者B
216
214
214
202
214
216'
参加者A
212

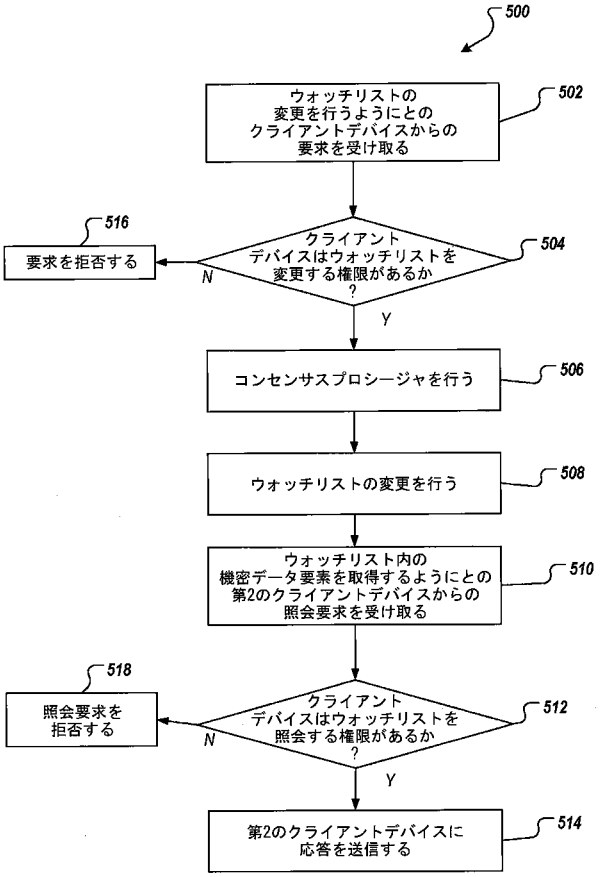
【図３】


300
304
クライアント
310
302a
(コンセンサスノード)
302b
(コンセンサスノード)
302f
(非コンセンサスノード)
302e
(非コンセンサスノード)
302c
(コンセンサスノード)
302d
(コンセンサスノード)

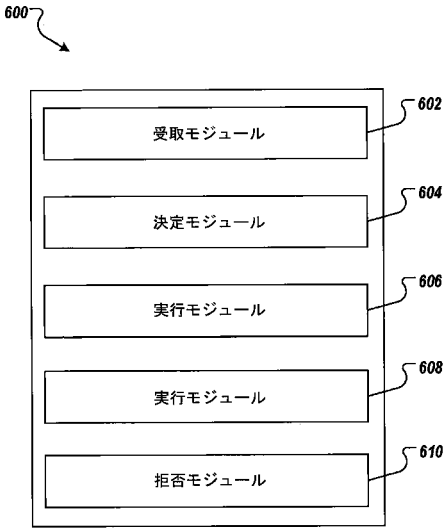
【図４】


400
304b
クライアント
304a
クライアント
302a
ブロックチェーンネットワークノード
302b-d
ブロックチェーンネットワークノード
402
404
406
408
410
412
414
416
418
420

【図５】


500
ウォッチリストの
変更を行うようにとの
クライアントデバイスからの
要求を受け取る
502
クライアント
デバイスはウォッチリストを
変更する権限があるか
?
504
N
516
要求を拒否する
Y
コンセンサスプロシージャを行う
506
ウォッチリストの変更を行う
508
ウォッチリスト内の
機密データ要素を取得するようにとの
第2のクライアントデバイスからの
照会要求を受け取る
510
クライアント
デバイスはウォッチリストを
照会する権限があるか
?
512
N
518
照会要求を
拒否する
Y
第2のクライアントデバイスに
応答を送信する
514

【図６】


600
受取モジュール
602
決定モジュール
604
実行モジュール
606
実行モジュール
608
拒否モジュール
610

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/080493

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(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)

H04L G06Q H04W

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: blockchain, block chain, require, request, distributed ledger system, DLS, security, sensitive, personal, restricted, list, table, consensus, user, client, authorize, modification, vertif+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017222814 A1 (CAMBRIDGE BLOCKCHAIN, LLC) 03 August 2017 (2017-08-03) the whole document	1-9
A	US 2017353311 A1 (THOMSON REUTERS GLOBAL RESOURCES) 07 December 2017 (2017-12-07) the whole document	1-9
A	US 2017213221 A1 (BANK OF AMERICA CORPORATION) 27 July 2017 (2017-07-27) the whole document	1-9
A	US 2018039667 A1 (CHICAGO MERCANTILE EXCHANGE INC.) 08 February 2018 (2018-02-08) the whole document	1-9
A	US 2017149819 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 25 May 2017 (2017-05-25) the whole document	1-9
A	CN 108256858 A (BULL SAS) 06 July 2018 (2018-07-06) the whole document	1-9

☐ 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
03 December 2019	**02 January 2020**
Name and mailing address of the ISA/CN **National Intellectual Property Administration, PRC** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China**	Authorized officer **CHEN,Gang**
Facsimile No. **(86-10)62019451**	Telephone No. **86-(10)-53961690**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/080493

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2017222814	A1	03 August 2017	US	2018234433	A1	16 August 2018
				US	2019207951	A1	04 July 2019
				US	2017111175	A1	20 April 2017
				CA	3002034	A1	20 April 2017
				CN	108701276	A	23 October 2018
				WO	2017066715	A1	20 April 2017
				JP	2018537022	A	13 December 2018
				EP	3234878	A1	25 October 2017
				SG	11201803010U	A	30 May 2018
				KR	20180108566	A	04 October 2018
US	2017353311	A1	07 December 2017	CN	108780390	A	09 November 2018
				EP	3465418	A1	10 April 2019
				CA	3017578	A1	14 December 2017
				SG	11201806653S	A	27 September 2018
				AU	2017277538	A1	16 August 2018
				WO	2017213719	A1	14 December 2017
US	2017213221	A1	27 July 2017	None			
US	2018039667	A1	08 February 2018	WO	2018026883	A1	08 February 2018
				EP	3494535	A1	12 June 2019
				US	2019340170	A1	07 November 2019
US	2017149819	A1	25 May 2017	None			
CN	108256858	A	06 July 2018	BR	102017028033	A2	02 January 2019
				EP	3343425	A1	04 July 2018
				FR	3061330	A1	29 June 2018
				ES	2729312	T3	31 October 2019
				US	2019171830	A1	06 June 2019
				US	2018181768	A1	28 June 2018

フロントページの続き

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

(72)発明者 ジユアン・フェン
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント
(72)発明者 ヤンペン・リ
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント
(72)発明者 ロン・チェン
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント