

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】令和2年12月17日(2020.12.17)

【公表番号】特表2020-521342(P2020-521342A)

【公表日】令和2年7月16日(2020.7.16)

【年通号数】公開・登録公報2020-028

【出願番号】特願2019-553421(P2019-553421)

【国際特許分類】

H 04 L 9/32 (2006.01)

G 06 F 21/62 (2013.01)

【F I】

H 04 L 9/00 6 7 5 Z

H 04 L 9/00 6 7 5 B

G 06 F 21/62 3 1 8

【手続補正書】

【提出日】令和2年10月28日(2020.10.28)

【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ч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うステップであって、

前記コンセンサスプロシージャは、

前記ブロックチェーンネットワークの複数のコンセンサスノードに、要求検証メッセージを送信するステップと、

前記複数のコンセンサスノードから応答メッセージを受信するステップとを含む、ステップと、

前記応答メッセージに基づいて、コンセンサスが達成されたと決定するステップと、

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】

前記複数のコンセンサスノードのそれぞれが、前記ウォッチリストへのアクセスを制御する権限を与えられた機関のサーバにある、請求項1に記載の方法。

【請求項9】

前記ブロックチェーンネットワークが、非コンセンサスノードを含み、  
前記非コンセンサスノードが、前記権限を与えられた機関の従属機関のサーバにあり、  
前記従属機関が、前記ウォッチリストを変更する権限なしで、前記複数のコンセンサスノードから前記ウォッチリストを取得することができる、請求項8に記載の方法。

【請求項10】

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9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11】

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9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。