【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9月10日(2020.9.10)

【公表番号】特表2020-522904(P2020-522904A)
【公表日】令和2年7月30日(2020.7.30)
【年通号数】公開・登録公報2020-030
【出願番号】特願2019-540398(P2019-540398)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｚ

【手続補正書】
【提出日】令和2年6月23日(2020.6.23)
【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】
デジタル証明書管理のための方法であって、前記方法は、
有効なデジタル証明書をノードに割り当てるための要求を受信するステップであって、前記要求は、ブロックチェーン内の前記ノードによって送信され、前記要求は、前記ノードのための前記有効なデジタル証明書についての申請であり、前記有効なデジタル証明書は、前記ノードが前記ブロックチェーン内で通信することを認可し、前記要求は、前記ノードの固有秘密鍵を使用して前記ノードによって署名された検証用デジタル証明書を含み、前記要求は、前記ブロックチェーン内の前記ノードのための前記有効なデジタル証明書を記憶するためのものである、ステップ(S101)と、
前記ブロックチェーン内のノードのうちの各ノードによって前記検証用デジタル証明書についての複数のコンセンサス検証を行うことによって、前記ノードの前記検証用デジタル証明書のコンセンサス検証結果を決定するステップ(S103)と、
前記コンセンサス検証結果に基づいて、前記検証用デジタル証明書を前記ブロックチェーンに記憶するかどうかを決定するステップ(S105)と、
前記コンセンサス検証結果が前記ブロックチェーンにおいて前記検証用デジタル証明書を認可するための承認を含む場合には、前記ブロックチェーンの通信のために前記ノードを認可するために前記有効なデジタル証明書を記憶するステップであって、前記有効なデジタル証明書は、前記ブロックチェーンの複数のノードに記憶され、前記有効なデジタル証明書を前記ノードに割り当てる、ステップとを含む、方法。
【請求項２】
前記ノードの前記検証用デジタル証明書の前記コンセンサス検証結果を決定するステップは、
前記ブロックチェーン内の前記コンセンサス検証に関与している前記ノードの各々の検証結果を決定するステップ(S301)と、
前記コンセンサス検証に関与している前記ブロックチェーンの前記ノードに由来する第1のノードの数および第2のノードの数を決定するステップであって、前記第1のノードの数に由来する第1のノードの各々の検証結果は、前記コンセンサス検証についての承認を含み、前記第2のノードの数に由来する第2のノードの各々の検証結果は、前記コンセンサス検証についての拒否を含む、ステップ(S303)と、

前記第1のノードの数および前記第2のノードの数に基づいて前記コンセンサス検証結果を決定するステップ(S305)とを含む、請求項1に記載の方法。
【請求項３】
前記ノードの前記検証用デジタル証明書の前記コンセンサス検証結果を決定するステップは、
前記ブロックチェーン内の前記コンセンサス検証に関与している前記ノードの各々の検証結果を決定するステップ(S301)と、
前記コンセンサス検証に関与している前記ブロックチェーンの前記ノードに由来する第1のノードの数を決定するステップであって、前記第1のノードの数に由来する第1のノードの各々の検証結果は、前記コンセンサス検証の承認を含む、ステップ(S303)と、
前記第1のノードの数に基づいて前記コンセンサス検証結果を決定するステップ(S305)とを含む、請求項1に記載の方法。
【請求項４】
前記ノードの前記検証用デジタル証明書の前記コンセンサス検証結果を決定するステップは、
前記ブロックチェーン内の前記コンセンサス検証に関与している前記ノードの各々の検証結果を決定するステップ(S301)と、
前記コンセンサス検証に関与している前記ブロックチェーンの前記ノードに由来する第2のノードの数を決定するステップであって、前記第2のノードの数に由来する第2のノードの各々の検証結果は、前記コンセンサス検証の拒否を含む、ステップ(S303)と、
前記第2のノードの数に基づいて前記コンセンサス検証結果を決定するステップ(S305)とを含む、請求項1に記載の方法。
【請求項５】
前記第1のノードの数に基づいて前記コンセンサス検証結果を決定するステップは、
前記第1のノードの数が第1の所定の条件を満足する場合には、前記コンセンサス検証結果が前記コンセンサス検証をパスしているであると決定するステップを含み、
前記第1の所定の条件は、
前記第1のノードの数が第1の所定の閾値に達することと、
前記コンセンサス検証に関与している前記ノードの数に対する前記第1のノードの数の比が第2の所定の閾値に達することと、
前記ブロックチェーン内の前記ノードの数に対する前記第1のノードの数の比が第3の所定の閾値に達することとのうちの1つまたは複数を含む、請求項2に記載の方法。
【請求項６】
前記ブロックチェーン内の前記ノードによって送信されたデジタル証明書の取り消しのための要求を受信するステップであって、前記取り消しのための要求は、取り消すように要求されているターゲットノードのデジタル証明書を含む、ステップ(S201)と、
前記ターゲットノードの前記デジタル証明書のコンセンサス検証結果を決定するステップ(S203)と、
前記コンセンサス検証結果に基づいて、前記ターゲットノードの前記デジタル証明書を取り消すかどうかを決定するステップ(S205)とをさらに含む、請求項1から3のいずれか一項に記載の方法。
【請求項７】
前記コンセンサス検証結果に基づいて、前記ブロックチェーン内の前記ターゲットノードの前記デジタル証明書を取り消すかどうかを決定するステップは、
前記コンセンサス検証結果が前記コンセンサス検証をパスしているである場合には、前記ブロックチェーン内の前記ターゲットノードの前記デジタル証明書を取り消すステップを含む、請求項1に記載の方法。
【請求項８】
前記ブロックチェーン内の前記ノードによって、前記ブロックチェーンが、前記ノードの検証用デジタル証明書のコンセンサス検証結果を決定するように、前記要求を前記ブロ

ックチェーンに送信するステップをさらに含む、請求項1から5のいずれか一項に記載の方法。
【請求項９】
ブロックチェーン内のノードによって、前記ブロックチェーンが、ターゲットノードのデジタル証明書のコンセンサス検証結果を決定し、前記コンセンサス検証結果に基づいて、前記ブロックチェーン内の前記ターゲットノードの前記デジタル証明書を取り消すかどうかを決定するように、デジタル証明書の取り消しのための要求を前記ブロックチェーンに送信するステップであって、前記取り消しのための要求は、前記取り消すように要求されているターゲットノードの前記デジタル証明書を含む、ステップをさらに含む、請求項1から6のいずれか一項に記載の方法。
【請求項１０】
前記デジタル証明書は、バージョン、シリアルナンバー、発行者情報、有効期間、および発行者のシグニチャのうちの少なくとも1つを含む、請求項1から7のいずれか一項に記載の方法。
【請求項１１】
前記ブロックチェーンにおいて前記ノードに割り当てられる前は、前記デジタル証明書は無認可である、請求項1から8のいずれか一項に記載の方法。
【請求項１２】
電子デバイスであって、前記電子デバイスは、ブロックチェーンに適用され、
プロセッサと、
コンピュータ実行可能命令を記憶するように構成される、ストレージであって、前記実行可能命令が実行されると、前記プロセッサは、請求項1から11のいずれか一項に記載の方法を行う、ストレージとを含む、電子デバイス。