【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６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2020-525875(P2020-525875A)
【公表日】令和2年8月27日(2020.8.27)
【年通号数】公開・登録公報2020-034
【出願番号】特願2019-559278(P2019-559278)
【国際特許分類】
Ｇ０６Ｆ　21/12　(2013.01)
Ｇ０６Ｆ　21/62　(2013.01)
Ｈ０４Ｌ　 9/32　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　21/12　３１０
Ｇ０６Ｆ　21/62
Ｈ０４Ｌ　 9/00　６７５Ｚ

【手続補正書】
【提出日】令和2年10月23日(2020.10.23)
【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】
ブロックチェーンデータを信頼できる実行環境(TEE)下で処理するためのコンピュータが実行する方法であって、
ブロックチェーンノードにより、前記ブロックチェーンノード上で実行するTEEにおいて1つまたは複数のソフトウェア命令を実行する要求を受信するステップと、
前記TEEにおける仮想マシンにより、前記1つまたは複数のソフトウェア命令の実行に関する1つまたは複数のブロックチェーンアカウントに関連するデータを前記要求に基づいて識別するステップと、
前記1つまたは複数のブロックチェーンアカウントに関連するデータの識別に応じて、前記仮想マシンにより、前記TEEに保存されているブロックチェーンのグローバルステートを走査して、前記1つまたは複数のブロックチェーンアカウントに関連するデータを見つけるステップと、
前記仮想マシンにより、前記データに基づいて前記1つまたは複数のソフトウェア命令を実行するステップであって、前記TEEに保存されているブロックチェーンのグローバルステートが、前記1つまたは複数のソフトウェア命令の実行中に更新されて、更新されたグローバルステートを生成する、ステップと、
前記1つまたは複数のソフトウェア命令の実行に応じて、前記ブロックチェーンノードにより、前記更新されたグローバルステートの暗号化表現を生成するステップと、
前記ブロックチェーンノードにより、前記TEEから分離している保存場所に前記更新されたグローバルステートの暗号化表現を保存するステップと、
を含む、コンピュータが実行する方法。
【請求項２】
前記要求は、1つまたは複数の入力パラメータを含み、前記TEEのインターフェース関数に対して行われる、請求項1に記載のコンピュータが実行する方法。
【請求項３】

前記グローバルステートは、前記TEEにマークルパトリシアツリー(MPT)として保存されている、請求項1に記載のコンピュータが実行する方法。
【請求項４】
前記グローバルステートは、前記ブロックチェーンの複数のブロックチェーンアカウントのアドレスと状態との間のマッピングを含み、前記複数のブロックチェーンアカウントは、1つまたは複数の外部所有アカウントまたはコントラクトアカウントを含み、前記コントラクトアカウントのそれぞれがストレージルートを含む、請求項1に記載のコンピュータが実行する方法。
【請求項５】
前記ストレージルートはマークルパトリシアツリー(MPT)のルートノードのハッシュを含み、前記MPTは、対応するコントラクトアカウントのストレージ内容のハッシュをエンコードする、請求項4に記載のコンピュータが実行する方法。
【請求項６】
更新されたグローバルステートは、前記対応するコントラクトアカウントのストレージ内容のハッシュをエンコードする前記MPTを更新することによって生成される、請求項5に記載のコンピュータが実行する方法。
【請求項７】
前記TEEから分離している保存場所は、キャッシュまたはデータベースに関連している、請求項1に記載のコンピュータが実行する方法。
【請求項８】
前記要求は、前記TEEに関連するアプリケーションプログラミングインターフェースを介して受信される、請求項1に記載のコンピュータが実行する方法。
【請求項９】
請求項1から8のいずれか一項に記載の方法を1つまたは複数のコンピュータに実行させる1つまたは複数の命令を記憶した非一時的コンピュータ可読記憶媒体。
【請求項１０】
コンピュータが実装されたシステムであって、
1つまたは複数のコンピュータと、
前記1つまたは複数のコンピュータによって実行されるとき、ブロックチェーンデータを信頼できる実行環境(TEE)下で処理するための1つまたは複数の動作を実行する1つまたは複数の命令を記憶した有形の非一時的機械可読媒体を有し、前記1つまたは複数のコンピュータと相互作用可能に結合された1つまたは複数のコンピュータメモリデバイスと、
を含み、前記動作は、
ブロックチェーンノードにより、前記ブロックチェーンノード上で実行するTEEにおいて1つまたは複数のソフトウェア命令を実行する要求を受信するステップと、
前記TEEにおける仮想マシンにより、前記1つまたは複数のソフトウェア命令の実行に関する1つまたは複数のブロックチェーンアカウントに関連するデータを前記要求に基づいて識別するステップと、
前記1つまたは複数のブロックチェーンアカウントに関連するデータの識別に応じて、前記仮想マシンにより、前記TEEに保存されているブロックチェーンのグローバルステートを走査して、前記1つまたは複数のブロックチェーンアカウントに関連するデータを見つけるステップと、
前記仮想マシンにより、前記データに基づいて前記1つまたは複数のソフトウェア命令を実行するステップであって、前記TEEに保存されているブロックチェーンのグローバルステートが、前記1つまたは複数のソフトウェア命令の実行中に更新されて、更新されたグローバルステートを生成する、ステップと、
前記1つまたは複数のソフトウェア命令の実行に応じて、前記ブロックチェーンノードにより、前記更新されたグローバルステートの暗号化表現を生成するステップと、
前記ブロックチェーンノードにより、前記TEEから分離している保存場所に前記更新されたグローバルステートの暗号化表現を保存するステップと、

を含む、システム。
【請求項１１】
前記要求は、1つまたは複数の入力パラメータを含み、前記TEEのインターフェース関数に対して行われる、請求項10に記載のシステム。
【請求項１２】
前記グローバルステートは、前記TEEにマークルパトリシアツリー(MPT)として保存されている、請求項10に記載のシステム。
【請求項１３】
前記グローバルステートは、前記ブロックチェーンの複数のブロックチェーンアカウントのアドレスと状態との間のマッピングを含み、前記複数のブロックチェーンアカウントは、1つまたは複数の外部所有アカウントまたはコントラクトアカウントを含み、前記コントラクトアカウントのそれぞれがストレージルートを含む、請求項10に記載のシステム。
【請求項１４】
前記ストレージルートはマークルパトリシアツリー(MPT)のルートノードのハッシュを含み、前記MPTは、対応するコントラクトアカウントのストレージ内容のハッシュをエンコードする、請求項13に記載のシステム。
【請求項１５】
更新されたグローバルステートは、前記対応するコントラクトアカウントのストレージ内容のハッシュをエンコードする前記MPTを更新することによって生成される、請求項14に記載のシステム。
【請求項１６】
前記TEEから分離している保存場所は、キャッシュまたはデータベースに関連している、請求項10に記載のシステム。
【請求項１７】
前記要求は、前記TEEに関連するアプリケーションプログラミングインターフェースを介して受信される、請求項10に記載のシステム。