

【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4年11月8日(2022.11.8)

【国際公開番号】WO2020/110025
 【公表番号】特表2022-509104(P2022-509104A)
 【公表日】令和4年1月20日(2022.1.20)
 【年通号数】公開公報(特許)2022-010
 【出願番号】特願2021-527844(P2021-527844)
 【国際特許分類】

H 0 4 L 9/32(2006.01)
 G 0 6 F 21/64(2013.01)
 G 0 6 F 16/182(2019.01)

【F I】

H 0 4 L 9/00 6 7 5 Z
 G 0 6 F 21/64
 G 0 6 F 16/182

10

【手続補正書】

【提出日】令和4年10月28日(2022.10.28)

20

【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】

コンピュータにより実施される方法であって、
 階層構造の複数のブロックチェーンランザクションを提供し又は使用するステップであって、前記階層構造のより低いレベルにある少なくとも1つの更なるブロックチェーンランザクションの中で提供された又は参照されたデータ部分が、前記階層構造のより高いレベルにある第1ブロックチェーンランザクションに署名するために使用される暗号鍵との比較によりアクセス又は識別可能になる、ステップを含む方法。

30

【請求項2】

コンピュータにより実施される方法であって、
 第1ブロックチェーンランザクションを使用して、前記第1ブロックチェーンランザクションに署名するために使用される暗号鍵に基づき、ブロックチェーンランザクションの階層構造の中のより低いレベルにある少なくとも1つの更なるブロックチェーンランザクションの中で提供される又は参照されるデータ部分へのアクセスを提供する又は禁止するステップを含む方法。

40

【請求項3】

前記第1ブロックチェーンランザクションに署名するために使用される鍵と前記階層構造のより低いレベルにある少なくとも1つの更なるブロックチェーンランザクションとの間のマッピングを格納し及び/又は維持するステップ、を更に含む請求項1又は2に記載の方法。

【請求項4】

前記第1ブロックチェーンランザクション及び/又は前記階層構造のより低いレベルにある少なくとも1つの更なるブロックチェーンランザクションは、
 トランザクションID(TxID)、
 プロトコルフラグ、

50

任意公開鍵 (DPK)、及び
任意トランザクションID (DTxID)、
を含む、請求項 1 ~ 3 のいずれかに記載の方法。

【請求項 5】

前記データ部分又は前記データ部分への参照、前記プロトコルフラグ、前記任意公開鍵 (DPK)、及び/又は前記任意トランザクションID (DTxID) は、前記第 1 又は少なくとも 1 つの更なるブロックチェーントランザクションのアウトプット (UTXO) の中で、前記アウトプット (UTXO) に関連付けられたロックスクリプトの中で提供される、請求項 4 に記載の方法。

【請求項 6】

前記データ部分、前記データ部分への参照、前記プロトコルフラグ、前記任意公開鍵 (DPK) 及び/又は前記任意トランザクションID (DTxID) は、後のブロックチェーントランザクションへのインプットとしての後の使用に対してアウトプットを無効であるとマークするスクリプトオペコードに続く位置において、前記ブロックチェーントランザクション (Tx) 内で提供される、請求項 4 又は 5 に記載の方法。

【請求項 7】

前記第 1 ブロックチェーントランザクション及び/又は少なくとも 1 つの更なるブロックチェーントランザクションは 1 つ以上の属性を含む、請求項 1 ~ 6 のいずれかに記載の方法。

【請求項 8】

前記 1 つ以上の属性は、以下：

i) 前記第 1 ブロックチェーントランザクション及び/又は少なくとも 1 つの更なるブロックチェーントランザクションの中で提供される又は参照されるデータ部分、及び/又は、

ii) 前記第 1 ブロックチェーントランザクション及び/又は少なくとも 1 つの更なるブロックチェーントランザクション、
_ に関連付けられたキーワード、タグ、又は識別子を含む、請求項 7 に記載の方法。

【請求項 9】

前記第 1 ブロックチェーントランザクション及び/又は少なくとも 1 つの更なるブロックチェーントランザクションは、以下：

論理的親トランザクション (LPTx) に関連付けられた親公開鍵 (PPK) であって、前記論理的親トランザクション (LPTx) は、前記任意トランザクションID (DTxID) により識別される、論理的親トランザクション (LPTx) と、

前記親公開鍵 (PPK) を使用して生成された署名と、

を含むインプットを更に含む、請求項 1 ~ 8 のいずれかに記載の方法。

【請求項 10】

前記任意公開鍵 (DPK) 及び前記トランザクションID (TxID) を使用して、ブロックチェーンの中の前記第 1 ブロックチェーントランザクション、前記少なくとも 1 つの更なるブロックチェーントランザクション、及び/又は前記論理的親トランザクションを識別するステップ、を更に含む請求項 9 に記載の方法。

【請求項 11】

コンピュータにより実装されるシステムであって、

プロセッサと、

前記プロセッサによる実行の結果として、前記システムに請求項 1 ~ 10 のいずれか一項に記載のコンピュータにより実施される方法を実行させる実行可能命令を含むメモリと、

を含むシステム。

【請求項 12】

実行可能命令を記憶した非一時的コンピュータ可読記憶媒体であって、前記実行可能命令は、コンピュータシステムのプロセッサにより実行された結果として、少なくとも、前記コンピュータシステムに、請求項 1 ~ 10 のいずれか一項に記載の方法を実行させる、

10

20

30

40

50

非一時的コンピュータ可読記憶媒体。

10

20

30

40

50