【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1年7月18日(2019.7.18)

【公開番号】特開2019-50480(P2019-50480A)
【公開日】平成31年3月28日(2019.3.28)
【年通号数】公開・登録公報2019-012
【出願番号】特願2017-173060(P2017-173060)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ａ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】令和1年6月14日(2019.6.14)
【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】
コンピュータによって実行される方法であって、
交換される情報の処理に使用する秘密情報に基づいて、ｎ個の秘密情報復元可能値を生成するステップであって、前記秘密情報は、前記生成したｎ個の秘密情報復元可能値のうちの少なくともｋ個の秘密情報復元可能値を使用して復元可能であり、ｎ＞＝ｋ＞＝２である、ステップと、
前記生成したｎ個の秘密情報復元可能値を、対応するｎ個の物理的記憶装置に記憶するステップであって、前記ｎ個の物理的記憶装置のうちの少なくとも１つは、第１の取外可能記憶装置であり、前記ｎ個の物理的記憶装置のうちの少なくともう１つは、第２の取外可能記憶装置であり、前記第１の取外可能記憶装置および前記第２の取外可能記憶装置は、同一の種別の取外可能記憶装置であり、
前記生成したｎ個の秘密情報復元可能値のうちの第１の秘密情報復元可能値を前記第１の取外可能記憶装置に記憶するステップと、
前記第２の取外可能記憶装置が前記コンピュータに接続されているか否かを判定するステップと、
前記第２の取外可能記憶装置が前記第１の取外可能記憶装置と物理的に異なる取外可能記憶装置であるかを判定するステップと、
前記第２の取外可能記憶装置が前記第１の取外可能記憶装置と物理的に異なる取外可能記憶装置であると判定したことに応答して、前記生成したｎ個の秘密情報復元可能値のうちの第２の秘密情報復元可能値を前記第２の取外可能記憶装置に記憶するステップと
を含む、ステップと、
前記生成した秘密情報を削除するステップと
を備えたことを特徴とする方法。
【請求項２】
コンピュータによって実行される方法であって、
複数のアプリケーションプログラムを実行することによって、交換される情報の処理に使用する秘密情報を生成するステップと、
前記秘密情報に基づいて、ｎ個の秘密情報復元可能値を生成するステップであって、前

記秘密情報は、前記生成したｎ個の秘密情報復元可能値のうちの少なくともｋ個の秘密情報復元可能値を使用して復元可能であり、ｎ＞＝ｋ＞＝２である、ステップと、
前記生成したｎ個の秘密情報復元可能値を、対応するｎ個の物理的記憶装置に記憶するステップであって、前記ｎ個の物理的記憶装置のうちの少なくとも１つは、前記コンピュータに内蔵された記憶装置であり、前記記憶装置は、前記複数のアプリケーションプログラムのそれぞれに対して独立した複数の論理的記憶領域を含み、前記生成したｎ個の秘密情報復元可能値のうちの１つを、前記複数の論理的記憶領域のうちのいずれか１つに記憶するステップを含む、ステップと、
前記生成した秘密情報を削除するステップと
を備えたことを特徴とする方法。
【請求項３】
前記ｎ個の物理的記憶装置のうちのｋ個の物理的記憶装置から、対応するｋ個の秘密情報復元可能値を読み出すステップと、
前記読み出したｋ個の秘密情報復元可能値を使用して、前記秘密情報を復元するステップと、
前記ｋ個の秘密情報復元可能値を削除するステップと
をさらに備えたことを特徴とする請求項１または２に記載の方法。
【請求項４】
前記ｎ個の物理的記憶装置のうちの少なくともｎ－（ｋ－１）個は、取外可能記憶装置であり、
前記方法は、前記取外可能記憶装置が前記コンピュータに接続されているか否かを判定するステップをさらに備えたことを特徴とする請求項１乃至３のいずれか一項に記載の方法。
【請求項５】
前記秘密情報を生成し、または前記秘密情報を受信するステップをさらに備えたことを特徴とする請求項１乃至４のいずれか一項に記載の方法。
【請求項６】
前記ｎ個の秘密情報復元可能値を生成するステップは、（ｋ，ｎ）閾値法を使用して実行されることを特徴とする請求項１乃至５のいずれか一項に記載の方法。
【請求項７】
前記秘密情報は、秘密鍵であることを特徴とする請求項１乃至６のいずれか一項に記載の方法。
【請求項８】
前記処理は、署名であることを特徴とする請求項１乃至７のいずれか一項に記載の方法。
【請求項９】
前記交換される情報は、仮想通貨のトランザクション履歴情報であることを特徴とする請求項１乃至８のいずれか一項に記載の方法。
【請求項１０】
コンピュータデバイスであって、
制御装置と、
前記制御装置に結合され、コンピュータ実行可能命令を記憶したメモリと
を備え、
前記コンピュータ実行可能命令は、前記制御装置によって実行されると、前記コンピュータデバイスに、請求項１乃至９のいずれか一項に記載の方法を実行させることを特徴とするコンピュータデバイス。
【請求項１１】
コンピュータ実行可能命令を含むコンピュータプログラムであって、前記コンピュータ実行可能命令は、コンピュータによって実行されると、前記コンピュータに請求項１乃至９のいずれか一項に記載の方法を実行させることを特徴とするコンピュータプログラム。