【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10日(2020.12.10)

【公表番号】特表2019-519137(P2019-519137A)
【公表日】令和1年7月4日(2019.7.4)
【年通号数】公開・登録公報2019-026
【出願番号】特願2018-557931(P2018-557931)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/64　(2013.01)
Ｇ０６Ｑ　20/38　(2012.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｚ
Ｇ０６Ｆ　21/64
Ｇ０６Ｑ　20/38　３１０
Ｈ０４Ｌ　9/00　６７５Ｂ

【手続補正書】
【提出日】令和2年10月29日(2020.10.29)
【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】
ブロックチェーンシステムの第１のエンティティが、前記第１のエンティティが所与のタスクを実行するために選択されていることを、前記ブロックチェーンシステムに関連付けられた他のエンティティに対して証明することを可能にする方法であって、
第１の暗号化手順に従って、ブロックチェーンの既存のブロックのシーケンスに基づいて最初のストリングを生成することと、
秘密暗号鍵を用いて、前記最初のストリングに一意に関連付けられている証明のストリングを計算することと、
第２の暗号化手順に従って、前記証明のストリングに基づいて数量を決定することと、
前記数量が所与の閾値を満たすかを判定することと、
前記判定に応答して、前記証明のストリングを前記ブロックチェーンに伝播させることと、を含む方法。
【請求項２】
前記第１のエンティティは潜在的なブロック提案者を含み、前記タスクは、前記ブロックチェーンに追加される新しいブロックを提案することを含む、請求項１に記載の方法。
【請求項３】
前記第１のエンティティは、前記ブロックチェーンに追加される前記提案された新しいブロックとともに、前記証明のストリングを伝播させる、請求項２に記載の方法。
【請求項４】
前記第１のエンティティは、潜在的な検証者を含み、前記タスクは、前記ブロックチェーンに投稿される情報の一部が正しいことを検証することを含む、請求項１乃至３のいずれか１項に記載の方法。
【請求項５】
前記ブロックチェーンに投稿される前記情報の一部は、前記ブロックチェーンに追加さ

れる新しいブロックを含む、請求項４に記載の方法。
【請求項６】
前記潜在的な検証者は、前記証明のストリングを、その検証の結果とともに伝播させる、請求項４又は５に記載の方法。
【請求項７】
前記第１のエンティティは潜在的な検証者を含み、前記タスクは、一組のトランザクションを正しく処理すること、を含む、請求項１乃至３のいずれか１項に記載の方法。
【請求項８】
前記トランザクションは、前記ブロックチェーンに投稿される提案されたトランザクションのブロックの一部である、請求項７に記載の方法。
【請求項９】
前記潜在的な検証者は、前記証明のストリングを、その検証の結果とともに伝播させる、請求項７又は８に記載の方法。
【請求項１０】
前記証明のストリングはデジタル署名を含む、請求項１乃至９のいずれか１項に記載の方法。
【請求項１１】
前記証明のストリングは、前記ブロックチェーンに関連付けられた他のエンティティによって検証可能であり、前記秘密暗号鍵は前記他のエンティティには利用できない、請求項１乃至１０のいずれか１項に記載の方法。
【請求項１２】
前記第１の暗号化手順は、前記ブロックチェーンの前記既存のブロックのシーケンスの過去の最初のストリングに基づいて定義されたランダムな数量を決定することを含む、請求項１乃至１１のいずれか１項に記載の方法。
【請求項１３】
前記第２の暗号化手順はランダムオラクルを含む、請求項１乃至１２のいずれか１項に記載の方法。
【請求項１４】
前記第２の暗号化手順は暗号学的ハッシュ関数を含む、請求項１乃至１３のいずれか１項に記載の方法。
【請求項１５】
前記数量が所与の閾値を満たすかを判定することは、前記数量が前記所与の閾値よりも小さいかを判定することを含む、請求項１乃至１４のいずれか１項に記載の方法。
【請求項１６】
請求項１乃至１５のいずれか１項に記載の方法を実施する実行可能コードを含む、コンピュータソフトウェア。
【請求項１７】
ブロックチェーンシステムの第１のエンティティが、前記第１のエンティティが所与のタスクを実行するために選択されていることを、前記ブロックチェーンシステムに関連付けられた他のエンティティに対して証明することを可能にするシステムであって、
第１の暗号化手順に従って、ブロックチェーンの既存のブロックのシーケンスに基づいて最初のストリングを生成する手段と、
秘密暗号鍵を用いて、前記最初のストリングに一意に関連付けられている証明のストリングを計算する手段と、
第２の暗号化手順に従って、前記証明のストリングに基づいて数量を決定する手段と、
前記数量が所与の閾値を満たすかを判定する手段と、
前記判定に応答して、前記証明のストリングを前記ブロックチェーンに伝播させる手段と、を備えるシステム。