【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7月2日(2020.7.2)

【公表番号】特表2020-501406(P2020-501406A)
【公表日】令和2年1月16日(2020.1.16)
【年通号数】公開・登録公報2020-002
【出願番号】特願2019-521710(P2019-521710)
【国際特許分類】
Ｈ０４Ｌ　9/30　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｑ　20/38　(2012.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６６３Ｚ
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０６Ｑ　20/38　３１０

【手続補正書】
【提出日】令和2年5月22日(2020.5.22)
【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】
アカウントモデルに基づくブロックチェーントランザクションを検証するためのコンピュータ実装方法であって、
トランザクションデータおよび前記トランザクションデータのデジタル署名を、ブロックチェーンネットワークのコンセンサスノードによって受信するステップであって、前記トランザクションデータは、暗号化されたトランザクション量、乱数、および第1のユーザノードのパブリックアカウントから第2のユーザノードのプライベートアカウントに、または前記第1のユーザノードのプライベートアカウントから前記第2のユーザノードのパブリックアカウントに、移動されるべき暗号化されていないトランザクション量を含み、各パブリックアカウントは残高を含み、各プライベートアカウントは暗号化された残高を含み、前記デジタル署名は、前記第1のユーザノードの秘密鍵を使用して前記トランザクションデータをデジタル署名することによって生成され、前記暗号化されたトランザクション量は、コミットメントスキームを使用して前記乱数および前記暗号化されていないトランザクション量に基づいて生成される、ステップと、
前記第1のユーザノードの公開鍵を使用して前記トランザクションデータの前記デジタル署名を検証するステップと、
前記コミットメントスキームを使用して前記乱数および前記暗号化されていないトランザクション量に基づいて第2の暗号化されたトランザクション量を生成するステップと、
前記第2の暗号化されたトランザクション量が前記受信された暗号化されたトランザクション量に等しいと決定するステップと、
前記トランザクションが前記第1のユーザノードの前記パブリックアカウントから前記第2のユーザノードの前記プライベートアカウントへのものであるとき、前記暗号化されていないトランザクション量が移動前の前記第1のユーザノードの前記パブリックアカウントの残高以下であること、あるいは、前記トランザクションが前記第1のユーザノードの前記プライベートアカウントから前記第2のユーザノードの前記パブリックアカウント

へのものであるとき、前記暗号化されていないトランザクション量が移動前の前記第1のユーザノードの前記プライベートアカウントの暗号化された残高の暗号化されていない値以下であることを決定するステップと、
前記トランザクションが前記第1のユーザノードの前記パブリックアカウントから前記第2のユーザノードの前記プライベートアカウントへのものであるとき、前記第1のユーザノードの前記パブリックアカウントの前記残高から前記暗号化されていないトランザクション量を差し引いて、前記受信した暗号化されたトランザクション量を前記第2のユーザノードの前記プライベートアカウントの暗号化された残高に追加する、あるいは、前記トランザクションが前記第1のユーザノードの前記プライベートアカウントから前記第2のユーザノードの前記パブリックアカウントへのものであるとき、前記第1のユーザノードの前記プライベートアカウントの暗号化された残高から前記受信した暗号化されたトランザクション量を差し引いて、前記暗号化されていないトランザクション量を前記第2のユーザノードの前記パブリックアカウントの残高に追加するステップと
を含むコンピュータ実装方法。
【請求項２】
前記第1のユーザノードまたは前記第2のユーザノードの前記パブリックアカウントの前記残高が、前記コンセンサスノードによって閲覧可能であり、前記第1のユーザノードまたは前記第2のユーザノードの前記プライベートアカウントの前記暗号化された残高の前記暗号化されていない値が、それぞれのユーザノードの秘密鍵を使用して閲覧可能である、請求項1に記載のコンピュータ実装方法。
【請求項３】
前記トランザクションが前記第1のユーザノードの前記プライベートアカウントから前記第2のユーザノードの前記パブリックアカウントへのものであり、前記方法が、
前記暗号化されていないトランザクション量が前記第1のユーザノードの前記プライベートアカウントの前記暗号化された残高の前記暗号化されていない値以下であることを証明する範囲証明を、前記第1のユーザノードから受信するステップをさらに含み、
前記暗号化されていないトランザクション量が前記範囲証明に基づいて前記第1のユーザノードの前記プライベートアカウントの前記暗号化された残高の前記暗号化されていない値以下である場合、前記移動が有効であると決定される、請求項1または2に記載のコンピュータ実装方法。
【請求項４】
前記コミットメントスキームが準同型である、請求項1～3のいずれか一項に記載のコンピュータ実装方法。
【請求項５】
前記第1のユーザノードが、前記第1のユーザノードの前記パブリックアカウントおよび前記第1のユーザノードの前記プライベートアカウントの両方を有し、
前記第1のユーザノードに関連付けられるユーザが、前記第1のユーザノードの前記パブリックアカウントまたは前記第1のユーザノードの前記プライベートアカウントを使用して前記トランザクションを実行するかどうかを選択する、請求項1～4のいずれか一項に記載のコンピュータ実装方法。
【請求項６】
1つまたは複数のプロセッサに結合されるとともに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、前記命令は、前記1つまたは複数のプロセッサによって実行されると、前記1つまたは複数のプロセッサに請求項1から5の1つまたは複数の方法に記載の動作を実行させる、非一時的コンピュータ可読記憶媒体。
【請求項７】
コンピューティングデバイスと、
前記コンピューティングデバイスに結合されるとともに命令を記憶したコンピュータ可読記憶媒体とを備えるシステムであって、前記命令は、前記コンピューティングデバイスによって実行されると、前記コンピューティングデバイスに請求項1から5の1つまたは複

数の方法に記載の動作を実行させる、システム。