【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17日(2020.12.17)

【公表番号】特表2020-526053(P2020-526053A)
【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2019-559290(P2019-559290)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｑ　20/38　(2012.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｚ
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｈ０４Ｌ　9/00　６７５Ｃ
Ｇ０６Ｑ　20/38　３１０

【手続補正書】
【提出日】令和2年11月6日(2020.11.6)
【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】
ブロックチェーンネットワークにおけるプライベート資産間取引のためのコンピュータ実装方法であって、1つまたは複数のプロセッサによって実行され、かつ、
前記ブロックチェーンネットワークにおける第1のノードによって、かつボウネイ-ゴー-ニッシム(BGN)暗号化を使用して、第1の値と、第2の値とに基づいて暗号文を生成するステップであって、
前記第2の値は、前記第1の値の準同型乗算と、前記ブロックチェーンネットワークにおける第2のノードによって提供される暗号化された為替レートとに基づいて決定され、
前記暗号文および前記暗号化された為替レートは同一の楕円曲線上にある、ステップと、
前記第1のノードによって前記第2のノードに、前記第1の値および前記暗号文を送信するステップと、
前記第1のノードによって、かつ前記第2のノードから、前記為替レートを明かすことなくゼロ知識証明(ZKP)ルーチンで前記為替レートを検証するために使用できるデータの集合を備える第1の証拠集合を受信するステップと、
前記第1のノードによって、前記暗号文が前記第1のノードのBGN公開鍵によって暗号化されていることを、前記ZKPルーチンを使用して、検証するために使用できるデータの集合を備える第2の証拠集合を生成するステップと、
前記第1のノードによって、前記第1のノードから前記第2のノードへの前記第1の値の移転のための前記第1のノードと前記第2のノードとの間の第1のトランザクション、および前記第2のノードから第3のノードへの前記第2の値の移転のための前記第2のノードと前記第3のノードとの間の第2のトランザクションを備えるトランザクションを定義するステップと、
前記第1のノードによって、前記トランザクションであって、前記第1の証拠集合および前記第2の証拠集合に基づいて検証される、前記トランザクションの検証および実行のた

めに前記ブロックチェーンネットワークの少なくとも1つのコンセンサスノードに前記トランザクションを送信し、そして前記トランザクションの検証に応じて、前記第1のトランザクションおよび前記第2のトランザクションを実行して、前記第1のノードの残高を前記第1の値だけ減少させ、前記第2のノードの第1の残高を前記第1の値だけ増加させ、前記第2のノードの第2の残高を前記第2の値だけ減少させ、そして前記第3のノードの残高を前記第2の値だけ増加させるステップと
を含む、方法。
【請求項２】
前記第1の証拠集合が、前記第1の値、前記第1のノードによって提供される一対の乱数、および前記暗号文に基づいて前記第2のノードによって提供される、請求項1に記載の方法。
【請求項３】
前記少なくとも1つのコンセンサスノードによって前記トランザクションを検証するステップが、前記第1のノードのデジタル署名および前記第2のノードのデジタル署名を検証するステップを含む、請求項1に記載の方法。
【請求項４】
前記少なくとも1つのコンセンサスノードによって前記トランザクションを検証するステップが、前記第1のノードによって提供される第1の範囲証明および前記第2のノードによって提供される第2の範囲証明を検証するステップを含む、請求項1に記載の方法。
【請求項５】
前記第1の範囲証明が、前記第1の値がゼロより大きいこと、および前記第1のノードの前記残高が前記第1の値以上であることを証明するZKPを備える、請求項4に記載の方法。
【請求項６】
前記第2の範囲証明が、前記第2のノードの前記第2の残高が前記第2の値以上であることを証明するZKPを備える、請求項4に記載の方法。
【請求項７】
前記トランザクションが、BGN暗号化を使用して生成される暗号文の集合を備えるデータ集合であって、前記少なくとも1つのコンセンサスノードによって前記トランザクションを検証するために使用される、データ集合をさらに備える、請求項1に記載の方法。
【請求項８】
前記第1のノードによって、前記ブロックチェーンネットワークのサブチェーンチャネルを通じて前記第2のノードから前記為替レートを受信するステップをさらに含む、請求項1に記載の方法。
【請求項９】
前記暗号文のうちの少なくとも1つの暗号文が、ペダーセンコミットメントを使用して提供される、請求項1に記載の方法。
【請求項１０】
前記第1の証拠集合の前記データの集合が、第1のデータ値および第2のデータ値であって、前記第2のノードのBGN公開鍵を生成するために使用されるパラメータに基づいて各々が決定される、第1のデータ値および第2のデータ値を備える、請求項1に記載の方法。
【請求項１１】
前記第2の証拠集合の前記データの集合が、暗号文の集合と、各値が前記暗号文の集合のハッシュに基づく値の集合とを備える、請求項1に記載の方法。
【請求項１２】
ブロックチェーンネットワークにおけるプライベート資産間取引のための命令が符号化された1つまたは複数のコンピュータ可読記憶媒体であって、前記命令が、1つまたは複数のプロセッサによって実行可能であり、かつ前記1つまたは複数のプロセッサに、請求項1乃至11のいずれか1項に記載の方法を実行させる、
1つまたは複数のコンピュータ可読記憶媒体。
【請求項１３】

1つまたは複数のプロセッサと、
前記1つまたは複数のプロセッサに結合され、かつブロックチェーンネットワークにおけるプライベート資産間取引のための命令が記憶された1つまたは複数のコンピュータ可読メモリと
を備え、前記命令が前記1つまたは複数のプロセッサによって実行可能であり、かつ前記1つまたは複数のプロセッサに、請求項1乃至11のいずれか1項に記載の方法を実行させる、
システム。