(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6811334号
(P6811334)
(45)発行日　令和3年1月13日(2021.1.13)　(24)登録日　令和2年12月16日(2020.12.16)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675C
G06Q 20/06 (2012.01)　H04L 9/00 675Z
G06Q 20/06 300

請求項の数 12　(全 25 頁)

(21)出願番号　特願2019-542677(P2019-542677)
(86)(22)出願日　平成30年12月21日(2018.12.21)
(65)公表番号　特表2020-515885(P2020-515885A)
(43)公表日　令和2年5月28日(2020.5.28)
(86)国際出願番号　PCT/CN2018/122539
(87)国際公開番号　WO2019/072300
(87)国際公開日　平成31年4月18日(2019.4.18)
審査請求日　令和1年10月4日(2019.10.4)

(73)特許権者　520015461
アドバンスド　ニュー　テクノロジーズ　カンパニー　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ケーワイ１－９００８　ジョージ　タウン　ホスピタル　ロード　２７　ケイマン　コーポレート　センター
(74)代理人　100188558
弁理士　飯田　雅人
(74)代理人　100205785
弁理士　▲高▼橋　史生

最終頁に続く

(54)【発明の名称】汎用アカウントモデルおよび準同型暗号に基づくブロックチェーンデータ保護

(57)【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内の第1のノードと第2のノードとの間の取引を確認するための、コンセンサスノードによって行われるコンピュータ実装方法であって、
前記取引と関連する取引データを受信するステップであり、前記取引データが、複数の資産を表すデータ、第1の乱数および前記取引の取引金額を秘匿した第1のコミットメント、第2の乱数および前記複数の資産の合計値から前記取引金額を差し引くことに基づいて計算されたおつりを秘匿した第2のコミットメント、確率的準同型暗号(HE)方式に基づいて前記第2のノードの公開鍵によって共に暗号化された前記取引金額および第3の乱数、前記確率的HE方式に基づいて前記第1のノードの公開鍵によって共に暗号化された前記おつりおよび第4の乱数、1つまたは複数の範囲証明、ゼロ知識証明(ZKP)、ならびに前記第1のノードの前記公開鍵に対応する秘密鍵に基づいて生成されたデジタル署名を備える、ステップと、
前記第1のノードの前記公開鍵に基づいて前記デジタル署名を検証するステップと、
前記取引金額および前記おつりが各々ゼロ以上であることを前記1つまたは複数の範囲証明が証明すると判定するステップと、
前記複数の資産の前記合計値が前記取引金額と前記おつりの和に等しいと判定するステップと、
前記第1の乱数が前記第3の乱数に等しく、前記第2の乱数が前記第4の乱数に等しく、前記第1のコミットメントに秘匿された前記取引金額が前記第2のノードの前記公開鍵によっ

て暗号化された前記取引金額に等しいと判定することによって、前記ZKPに基づいて、前記取引が有効であると判定するステップと
を含むコンピュータ実装方法。
【請求項２】
前記取引が、前記第1のノードと関連するアカウントと前記第2のノードと関連するアカウントとの間で行われ、前記方法が、前記取引が有効であると判定した後に、前記取引金額および前記おつりに基づいて前記第1のノードと関連する前記アカウントおよび前記第2のノードと関連する前記アカウントを更新するステップをさらに含む、請求項1に記載のコンピュータ実装方法。
【請求項３】
前記複数の資産の各々が、資産型、コミットメントに秘匿される資産価値、および前記コミットメントを生成するために使用される乱数のうちの1つまたは複数と関連付けられる、請求項1に記載のコンピュータ実装方法。
【請求項４】
前記複数の資産の各々が同じ資産型と関連付けられると判定するステップをさらに含む、請求項3に記載のコンピュータ実装方法。
【請求項５】
前記第1のコミットメント、前記第2のコミットメント、および前記資産価値を秘匿した前記コミットメントが、準同型であるコミットメント方式に基づいて生成され、前記複数の資産の前記合計値が前記取引金額と前記おつりの前記和に等しいと判定する前記ステップが、前記コミットメント方式の準同型性に基づいて行われる、請求項3に記載のコンピュータ実装方法。
【請求項６】
前記第3の乱数が、前記取引金額を乱数として扱うことによって前記確率的HE方式に基づいて暗号化され、前記第4の乱数が、前記おつりを乱数として扱うことによって前記確率的HE方式に基づいて暗号化される、請求項1に記載のコンピュータ実装方法。
【請求項７】
前記第1のコミットメントおよび前記第2のコミットメントがペダーセンコミットメント方式に基づいて生成され、前記確率的HE方式が岡本-内山(OU)暗号方式である、請求項1に記載のコンピュータ実装方法。
【請求項８】
前記ZKPが、第5の乱数および第6の乱数を秘匿したペダーセンコミットメント、前記OU暗号方式に基づいて第2のアカウントの前記公開鍵によって暗号化された前記第5の乱数および前記第6の乱数の暗号文、ならびに前記OU暗号方式に基づいて第1のアカウントの前記公開鍵によって暗号化された前記第5の乱数および前記第6の乱数の暗号文を備える、請求項7に記載のコンピュータ実装方法。
【請求項９】
前記ZKPが、前記確率的HEの性質に基づいて前記取引が有効であると判定するために生成および使用される、請求項1に記載のコンピュータ実装方法。
【請求項１０】
前記取引が有効であると判定する前記ステップが、前記ブロックチェーンネットワークの外部を通じた前記第1のノードと前記第2のノードとの間の対話なしに前記ZKPに基づいて行われる、請求項1に記載のコンピュータ実装方法。
【請求項１１】
1つまたは複数のコンピュータに結合され、請求項1から10の1つまたは複数に記載の方法に従う動作を行うように前記1つまたは複数のコンピュータによって実行可能な命令で構成された非一時的コンピュータ可読記憶媒体。
【請求項１２】
1つまたは複数のコンピュータと、
前記1つまたは複数のコンピュータに結合され、請求項1から10の1つまたは複数に記載

の方法に従う動作を行うように前記1つまたは複数のコンピュータによって実行可能な命令で構成された1つまたは複数のコンピュータ可読メモリと
を備えるシステム。
【発明の詳細な説明】
【背景技術】
【０００１】
ブロックチェーンシステム、コンセンサスネットワーク、分散型台帳システムネットワークまたはブロックチェーンとも呼ばれることがあるブロックチェーンネットワークは、参加エンティティが安全かつ不変にデータを記憶することを可能にする。ブロックチェーンは取引の台帳として説明可能であり、ブロックチェーンの複数のコピーがブロックチェーンネットワークにわたって記憶される。ブロックチェーンの種類例には、パブリックブロックチェーン、コンソーシアムブロックチェーンおよびプライベートブロックチェーンが含まれ得る。パブリックブロックチェーンは、全てのエンティティがブロックチェーンを使用してコンセンサスプロセスに参加するように公開されている。コンソーシアムブロックチェーンは、コンセンサスプロセスが或る組織または機関などの予め選択されたノードの集合によって制御されるブロックチェーンである。プライベートブロックチェーンは、読出しおよび書込み許可を中央で制御する特定のエンティティに提供される。
【０００２】
ブロックチェーンは、異なる記録保持モデルを使用してユーザ間の取引を記録できる。記録保持モデル例には、未使用トランザクションアウトプット(UTXO)モデルおよびアカウント残高モデルが含まれる。UTXOモデルでは、各トランザクションが、以前のトランザクションからのアウトプットを費やし、以降のトランザクションで費やされ得る新たなアウトプットを生成する。ユーザの未使用トランザクションがトラッキングされ、費やすことが可能である残高が未使用トランザクションの和として計算される。アカウント残高モデルでは、各ユーザのアカウント残高がグローバル状態としてトラッキングされる。各取引に対して、支出アカウントの残高は、それが取引金額以上であると確かめるためにチェックされる。これは従来の銀行取引に相当する。
【０００３】
ブロックチェーンは一連のブロックを含み、その各々がネットワークにおいて実行される1つまたは複数のトランザクションを含む。各ブロックが台帳のページになぞらえられ得る一方、ブロックチェーン自体は台帳の完全なコピーである。個々のトランザクションは確かめられブロックに追加され、このブロックは、ブロックチェーンに追加される。ブロックチェーンのコピーがネットワークのノードにわたって複製される。このようにして、ブロックチェーンの状態に関するグローバルコンセンサスがある。さらに、ブロックチェーンは、少なくともパブリックネットワークの場合、全てのノードに見えるように公開されている。ブロックチェーンユーザのプライバシーを保護するために、暗号技術が実装される。
【０００４】
アカウント残高モデル下では、取引の両当事者がコミットする値を秘匿する(hide)ためにコミットメント方式が使用可能である。コミットメント方式は、当事者が選択肢または値をコミットし、後に関与する相手方当事者にその値を伝達する必要性から生じ得る。例えば、対話型ペダーセンコミットメント(PC)方式では、第1のユーザが、乱数値rに基づいて生成されるコミットメント値PC(t，r)を送信することによって取引金額tをコミットできる。コミットメント値が生成され、第2のユーザが、乱数rを得ることによって取引金額tを明らかにできるだけである。取引金額が有効であることを保証するために、範囲証明が作成されて、取引金額がゼロ以上アカウント残高以下であることを証明できる。
【０００５】
場合により、ユーザから複数の取引がなされ得る。範囲証明がアカウントの残余残高と関連付けられるので、複数の取引はブロックチェーンにおいて順次検証される必要がある。そのため、対応する範囲証明は各取引後のアカウントの残余残高と正しく関連付け可能

である。しかしながら、順次複数の取引を検証することは時間を浪費し得る。取引の並列検証を許容する記録保持モデルが、特に時間に敏感なタスクに対して有利であろう。

【発明の概要】

【課題を解決するための手段】

【０００６】

本明細書の実装形態は、ブロックチェーン取引の非対話型プライバシー保持検証のためのコンピュータ実装方法を含む。より具体的には、本明細書の実装形態は、他のブロックチェーンノードに、取引金額、アカウント残高、またはコミットメントを生成するための乱数などのプライバシー情報を明らかにすることなくコミットメント方式および準同型暗号に基づいて、ブロックチェーンノードのアカウントと関連する複数の取引を並列に確認する(validate)ことが可能なコンピュータ実装方法を対象とする。

【０００７】

一部の実装形態では、動作は、取引と関連する取引データを受信するステップであって、取引データが:複数の資産を表すデータ、第1の乱数および取引の取引金額を秘匿した第1のコミットメント、第2の乱数および複数の資産の合計値から取引金額を差し引くことに基づいて計算されたおつり(change)を秘匿した第2のコミットメント、確率的準同型暗号(HE)方式に基づいて第2のノードの公開鍵によって共に暗号化された取引金額および第3の乱数、確率的HE方式に基づいて第1のノードの公開鍵によって共に暗号化されたおつりおよび第4の乱数、1つまたは複数の範囲証明、ゼロ知識証明(ZKP)、ならびに第1のノードの公開鍵に対応する秘密鍵に基づいて生成されたデジタル署名を備える、ステップと、第1のノードの公開鍵に基づいてデジタル署名を検証するステップと、取引金額およびおつりが各々ゼロ以上であることを1つまたは複数の範囲証明が証明すると判定するステップと、複数の資産の合計値が取引金額とおつりの和に等しいと判定するステップと、第1の乱数が第3の乱数に等しく、第2の乱数が第4の乱数に等しく、第1のコミットメントに秘匿された取引金額が第2のノードの公開鍵によって暗号化された取引金額に等しいと判定することによって、ZKPに基づいて、取引が有効であると判定するステップとを含む。他の実装形態は、対応するシステム、装置、およびコンピュータ記憶デバイスに符号化される、本方法の動作を行うように構成された、コンピュータプログラムを含む。

【０００８】

これらおよび他の実装形態は各々以下の特徴の1つまたは複数を任意選択で含んでよい。取引が第1のノードと関連するアカウントと第2のノードと関連するアカウントとの間で行われ、本方法が、取引が有効であると判定した後に、取引金額およびおつりに基づいて第1のノードのアカウントおよび第2のノードのアカウントを更新するステップをさらに含む;複数の資産の各々が、資産型、コミットメントに秘匿される資産価値、およびコミットメントを生成するために使用される乱数のうちの1つまたは複数と関連付けられる;複数の資産の各々が同じ資産型と関連付けられると判定する;第1のコミットメント、第2のコミットメント、および資産価値を秘匿したコミットメントが、準同型であるコミットメント方式に基づいて生成され、複数の資産の合計値が取引金額とおつりの和に等しいと判定するステップがコミットメント方式の準同型性に基づいて行われる;第3の乱数が、取引金額を乱数として扱うことによって確率的HE方式に基づいて暗号化され、第4の乱数が、おつりを乱数として扱うことによって確率的HE方式に基づいて暗号化される;第1のコミットメントおよび第2のコミットメントがペダーセンコミットメント方式に基づいて生成され、確率的HE方式が岡本-内山(OU)暗号方式である;ZKPが、第5の乱数および第6の乱数を秘匿したペダーセンコミットメント、OU暗号方式に基づいて第2のアカウントの公開鍵によって暗号化された第5の乱数および第6の乱数の暗号文、ならびにOU暗号方式に基づいて第1のアカウントの公開鍵によって暗号化された第5の乱数および第6の乱数の暗号文を備える;ZKPが、確率的HEの性質に基づいて取引が有効であると判定するために生成および使用される;取引が有効であると判定するステップが、ブロックチェーンネットワークの外部を通じた第1のノードと第2のノードとの間の対話なしにZKPに基づいて行われる。

【０００９】

本明細書は、1つまたは複数のプロセッサに結合され、かつ1つまたは複数のプロセッサによって実行されると、1つまたは複数のプロセッサに本明細書で提供される方法の実装形態に従う動作を行わせる命令が記憶された1つまたは複数の非一時的コンピュータ可読記憶媒体も提供する。

【００１０】

本明細書は、本明細書で提供される方法を実装するためのシステムをさらに提供する。本システムは、1つまたは複数のプロセッサと、1つまたは複数のプロセッサによって実行されると、1つまたは複数のプロセッサに本明細書で提供される方法の実装形態に従う動作を行わせる命令が記憶された、1つまたは複数のプロセッサに結合されたコンピュータ可読記憶媒体とを含む。

【００１１】

本明細書に記載される主題の実装形態は、特定の利点または技術的効果を実現するように実装可能である。例えば、本明細書の実装形態は、ブロックチェーンノードのアカウント残高および取引金額が取引の間プライベートであることを許す。資金移動の受取人は取引を確かめる、または乱数を使用してコミットメントを検証する必要はなく、取引確認は非対話型であることができる。ブロックチェーンノードは、HEおよびコミットメント方式に基づいて取引を確認してゼロ知識証明を許容できる。

【００１２】

記載される方法論は、様々なモバイルコンピューティングデバイスのアカウント/データセキュリティの強化を可能にする。アカウントの残高および取引金額はHEに基づいて暗号化可能で、かつコミットメント方式によって秘匿可能である。そのため、コンセンサスノードが、アカウントの実際のアカウント残高を明らかにすることなくHEの性質に基づいて取引後の台帳におけるアカウント残高を更新できる。取引を確かめるために受取人に乱数が送信される必要がないので、データ漏洩のリスクが低減可能であり、乱数を管理するために使用される必要があるコンピューティングおよびメモリリソースが少なくなる。

【００１３】

本明細書に従う方法が本明細書に記載される態様および特徴のいかなる組合せも含んでよいことが認識される。すなわち、本明細書に従う方法は、本明細書に具体的に記載される態様および特徴の組合せに限定されるのではなく、提供される態様および特徴のいかなる組合せも含む。

【００１４】

本明細書の1つまたは複数の実装形態の詳細が添付図面および以下の説明に明らかにされる。本明細書の他の特徴および利点は同説明および図面から、ならびに請求項から明らかであろう。

【図面の簡単な説明】

【００１５】

【図１】本明細書の実装形態を実行するために使用可能である環境の一例を示す図である。

【図２】本明細書の実装形態に従う概念アーキテクチャの一例を示す図である。

【図３】準同型暗号に基づくブロックチェーン取引のプライバシー保護確認のプロセスの一例を示す図である。

【図４】本明細書の実装形態に従うブロックチェーン取引の一例を示す図である。

【図５】準同型暗号に基づくブロックチェーン取引のプライバシー保護確認のプロセスの別の例を示す図である。

【図６】本明細書の実装形態に従って実行可能である方法の一例を示す図である。

【図７】本明細書の実装形態に従って実行可能である方法の別の例を示す図である。

【図８】本明細書の実装形態に従うプロセスを行うことができるブロックチェーンノードの一例を示す図である。

【発明を実施するための形態】

【００１６】

様々な図面における同様の参照記号は同様の要素を示す。

【００１７】

本明細書の実装形態は、ブロックチェーン取引の非対話型プライバシー保持検証のためのコンピュータ実装方法を含む。より具体的には、本明細書の実装形態は、他のブロックチェーンノードに、取引金額、アカウント残高、またはコミットメントを生成するための乱数などのプライバシー情報を明らかにすることなくコミットメント方式および準同型暗号に基づいて、ブロックチェーンノードのアカウントと関連する複数の取引を並列に確認することが可能なコンピュータ実装方法を対象とする。一部の実装形態では、動作は、取引と関連する取引データを受信するステップであって、取引データが:複数の資産を表すデータ、第1の乱数および取引の取引金額を秘匿した第1のコミットメント、第2の乱数および複数の資産の合計値から取引金額を差し引くことに基づいて計算されたおつりを秘匿した第2のコミットメント、確率的準同型暗号(HE)方式に基づいて第2のノードの公開鍵によって共に暗号化された取引金額および第3の乱数、確率的HE方式に基づいて第1のノードの公開鍵によって共に暗号化されたおつりおよび第4の乱数、1つまたは複数の範囲証明、ゼロ知識証明(ZKP)、ならびに第1のノードの公開鍵に対応する秘密鍵に基づいて生成されたデジタル署名を備える、ステップと、第1のノードの公開鍵に基づいてデジタル署名を検証するステップと、取引金額およびおつりが各々ゼロ以上であることを1つまたは複数の範囲証明が証明すると判定するステップと、複数の資産の合計値が取引金額とおつりの和に等しいと判定するステップと、第1の乱数が第3の乱数に等しく、第2の乱数が第4の乱数に等しく、第1のコミットメントに秘匿された取引金額が第2のノードの公開鍵によって暗号化された取引金額に等しいと判定することによって、ZKPに基づいて、取引が有効であると判定するステップとを含む。他の実装形態は、対応するシステム、装置、およびコンピュータ記憶デバイスに符号化される、本方法の動作を行うように構成された、コンピュータプログラムを含む。

【００１８】

本明細書の実装形態のための更なる文脈を提供するため、上記提示したように、分散型台帳システム(DLS)は、コンセンサスネットワーク(例えば、ピアツーピアノードから構成される)、およびブロックチェーンネットワークとも呼ばれることがあり、参加エンティティが安全かつ不変に取引を行い、データを記憶することを可能にする。ブロックチェーンは本明細書では、いかなる特定のユースケースにも関係なくDLS一般を指すために使用される。

【００１９】

ブロックチェーンは、トランザクションが不変であり、かつ後に検証可能であるようにトランザクションを記憶するデータ構造である。ブロックチェーンは1つまたは複数のブロックを含む。チェーン内の各ブロックは、チェーン内のそれの直前の以前のブロックの暗号学的ハッシュを含むことによって以前のブロックにリンクされる。各ブロックは、タイムスタンプ、それ自身の暗号学的ハッシュ、および1つまたは複数のトランザクションも含む。トランザクションは、ブロックチェーンネットワークのノードによって既に検証されており、マークルツリーへハッシュおよびエンコードされる。マークルツリーは、ツリーのリーフノードにおけるデータがハッシュされ、ツリーの各ブランチにおける全てのハッシュがブランチのルートで連結されるデータ構造である。このプロセスはツリー全体のルートまでツリーを上がり続け、次いで、ツリーにおける全てのデータを表すハッシュを記憶する。ツリーに記憶されたトランザクションのものであるように見せかけるハッシュは、それがツリーの構造と一致しているかどうかを判定することによって迅速に検証可能である。

【００２０】

ブロックチェーンがトランザクションを記憶するためのデータ構造であるのに対して、ブロックチェーンネットワークは、1つまたは複数のブロックチェーンを管理、更新および維持するコンピューティングノードのネットワークである。上記提示したように、ブロックチェーンネットワークは、パブリックブロックチェーンネットワーク、プライベート

ブロックチェーンネットワークまたはコンソーシアムブロックチェーンネットワークとして提供可能である。

【００２１】

パブリックブロックチェーンでは、コンセンサスプロセスはコンセンサスネットワークのノードによって制御される。例えば、何百、何千、何百万ものエンティティさえパブリックブロックチェーンに参加でき、その各々がパブリックブロックチェーンにおいて少なくとも1つのノードを動作させる。したがって、パブリックブロックチェーンは、参加エンティティに関するパブリックネットワークと考えられ得る。一部の例では、ブロックが有効でありブロックチェーンに追加されるためには、大多数のエンティティ(ノード)がブロックごとに署名しなければならない。パブリックブロックチェーンネットワーク例には、ブロックチェーンと称される分散型台帳を活用する特定のピアツーピア決済ネットワークが含まれる。しかしながら、上記で留意したように、用語ブロックチェーンは、特定のブロックチェーンネットワークを特に言及することなしに、分散型台帳を全般的に指すために使用される。

【００２２】

概して、パブリックブロックチェーンはパブリックトランザクションをサポートする。パブリックトランザクションはブロックチェーン内のノードの全てと共有され、ブロックチェーンは全てのノードにわたって複製される。すなわち、全てのノードがブロックチェーンに関してコンセンサスの完全状態にある。コンセンサス(例えば、ブロックチェーンへのブロックの追加への同意)を達成するために、ブロックチェーンネットワーク内にコンセンサスプロトコルが実装される。コンセンサスプロトコル例には、限定することなく、プルーフオブワーク(POW)、プルーフオブステーク(POS)およびプルーフオブオーソリティ(POA)が含まれる。非限定例としてPOWが本明細書でさらに参照される。

【００２３】

本明細書の実装形態は、ブロックチェーン取引の非対話型プライバシー保持検証のためのコンピュータ実装方法を含む。より具体的には、本明細書の実装形態は、他のブロックチェーンノードに、取引金額、アカウント残高、またはコミットメントを生成するための乱数などのプライバシー情報を明らかにすることなくコミットメント方式および準同型暗号に基づいて、ブロックチェーンノードのアカウントと関連する複数の取引を並列に確認することが可能なコンピュータ実装方法を対象とする。

【００２４】

本明細書の実装形態によれば、ブロックチェーンノードは、記録保持方法として並列取引検証をサポートできる汎用アカウントモデルを使用できる。アカウント残高モデルと比較して、汎用アカウントモデルを採用するブロックチェーンノードは、アカウント残高の代わりに複数の資産の記録を保持できる。複数の資産の各々は、資産型、資産IDまたは資産価値の少なくとも1つと関連付け可能である。汎用アカウントモデル下の資産は、貨幣または固定などのいかなる形態または種類でもあることができる。貨幣資産は現実の通貨または暗号通貨を含むことができる。一部の実装形態では、固定資産は、貨幣金額と関連する貨幣資産に変換可能である。貨幣金額は次いで、ブロックチェーンネットワークのアカウント間の取引を行うために使用可能である。例示目的で、本明細書の実装形態に記載される資産が汎用アカウントモデル下で同じ種類の通貨に変換されてブロックチェーンアカウントに保存されると仮定される。

【００２５】

データプライバシーを保護するために、取引は、ブロックチェーンユーザアカウントと関連する取引金額または貨幣金額情報を明らかにすることなくコミットメントに基づいてブロックチェーン(台帳)に記録可能である。乱数を使用して取引金額のコミットメントを生成するためにコミットメント方式が使用可能である。コミットメント方式例には、限定することなく、PC方式が含まれる。取引金額がコミットメントに秘匿されるので、取引金額がブロックチェーンユーザアカウントの価値を超えないことを証明するために1つまたは複数の範囲証明が使用可能である。

【００２６】
アカウント残高モデル下では、範囲証明はアカウント残高と関連付けられる。2つ以上の取引がなされる場合、しかし、全ての取引が確認されてブロックチェーンに記録されるわけではなく、範囲証明は誤ったアカウント残高と関連付けられる場合があり、それゆえに無効である場合がある。比較して、汎用アカウントモデル下では、アカウント価値は複数の資産の和として計算可能である。ブロックチェーンユーザアカウント間で取引金額が移動されることになるとき、取引金額をカバーするために、取引金額以上の総価値を持つ複数の資産の少なくとも一部分が使用可能である。残余資産が移動されることになる金額より大きい総価値を有するという条件下で追加の移動がなされ得る。たとえ取引が確認されてブロックチェーンに記録されなくても、残余資産の総価値が取引金額以上であることを示す範囲証明は依然として有効であることができる。したがって、2つ以上の取引検証が汎用アカウントモデル下で並列に行われ得る。
【００２７】
本明細書の実装形態によれば、ブロックチェーン取引は、取引アカウント残高、取引金額、またはコミットメントを生成するために使用される乱数を明らかにすることなくコミットメントに基づいて確認されてブロックチェーン(台帳)に記録可能である。乱数に基づいて取引金額のコミットメントを生成するために、PC方式などのコミットメント方式が使用可能である。取引金額および乱数は確率的または線形決定性HEを使用して暗号化可能である。取引金額および乱数は、使用されるHE方式の性質に基づいて取引を確認するためのZKPとしての一組の値を生成するためにも使用可能である。取引金額のコミットメント、暗号化された取引金額および乱数、ならびにZKPは、アカウント残高、取引金額または乱数が明らかにされることなく取引が有効であるかどうかを検証するためにブロックチェーンノードによって使用可能である。
【００２８】
図1は、本明細書の実装形態を実行するために使用可能である環境100の一例を描く。一部の例では、環境例100は、エンティティがパブリックブロックチェーン102に参加することを可能にする。環境例100は、コンピューティングシステム106、108およびネットワーク110を含む。一部の例では、ネットワーク110は、ローカルエリアネットワーク(LAN)、ワイドエリアネットワーク(WAN)、インターネットまたはその組合せを含み、ウェブサイト、ユーザデバイス(例えば、コンピューティングデバイス)およびバックエンドシステムを接続する。一部の例では、ネットワーク110は有線および/または無線通信リンクを通じてアクセス可能である。
【００２９】
図示の例では、コンピューティングシステム106、108は各々、パブリックブロックチェーン102へのノードとしての参加を可能にする任意の適切なコンピューティングシステムを含むことができる。コンピューティングデバイス例には、限定することなく、サーバ、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピューティングデバイスおよびスマートフォンが含まれる。一部の例では、コンピューティングシステム106、108は、パブリックブロックチェーン102と対話するための1つまたは複数のコンピュータ実装サービスをホストする。例えば、コンピューティングシステム106は、第1のエンティティ(例えば、ユーザA)が1つまたは複数の他のエンティティ(例えば、他のユーザ)とのその取引を管理するために使用する取引管理システムなどの、第1のエンティティのコンピュータ実装サービスをホストできる。コンピューティングシステム108は、第2のエンティティ(例えば、ユーザB)が1つまたは複数の他のエンティティ(例えば、他のユーザ)とのその取引を管理するために使用する取引管理システムなどの、第2のエンティティのコンピュータ実装サービスをホストできる。図1の例では、パブリックブロックチェーン102はノードのピアツーピアネットワークとして表現され、コンピューティングシステム106、108はそれぞれ第1のエンティティおよび第2のエンティティのノードを提供し、それらがパブリックブロックチェーン102に参加する。
【００３０】

図2は、本明細書の実装形態に従う概念アーキテクチャ200の一例を描く。概念アーキテクチャ例200は、エンティティ層202、ホストサービス層204およびパブリックブロックチェーン層206を含む。図示の例では、エンティティ層202は3つのエンティティEntity_1(E1)、Entity_2(E2)およびEntity_3(E3)を含み、各エンティティがそれぞれの取引管理システム208を有する。

【００３１】

図示の例では、ホストサービス層204は、各取引管理システム208に対するブロックチェーンインタフェース210を含む。一部の例では、それぞれの取引管理システム208は、通信プロトコル(例えば、ハイパーテキスト転送プロトコルセキュア(HTTPS))を使用してネットワーク(例えば、図1のネットワーク110)を通じてそれぞれのブロックチェーンインタフェース210と通信する。一部の例では、各ブロックチェーンインタフェース210は、それぞれの取引管理システム208とブロックチェーン層206との間の通信接続を提供する。より具体的には、各ブロックチェーンインタフェース210は、それぞれのエンティティがブロックチェーン層206のブロックチェーンネットワーク212に記録される取引を行うことを可能にする。一部の例では、ブロックチェーンインタフェース210とブロックチェーン層206との間の通信はリモートプロシージャコール(RPC)を使用して行われる。一部の例では、ブロックチェーンインタフェース210は、それぞれの取引管理システム208に対するブロックチェーンノードを「ホストする」。例えば、ブロックチェーンインタフェース210は、ブロックチェーンネットワーク212へのアクセスのためのアプリケーションプログラミングインタフェース(API)を提供する。

【００３２】

本明細書に記載されるように、ブロックチェーンネットワーク212はピアツーピアネットワークとして設けられ、ブロックチェーン216に不変に情報を記録する複数のノード214を含む。単一のブロックチェーン216が概略的に描かれるが、ブロックチェーン216の複数のコピーが設けられて、ブロックチェーンネットワーク212にわたって維持される。例えば、各ノード214がブロックチェーン216のコピーを記憶する。一部の実装形態では、ブロックチェーン216は、パブリックブロックチェーンに参加する2つ以上のエンティティ間で行われる取引と関連する情報を記憶する。

【００３３】

図3は、HEに基づくブロックチェーン取引のプライバシー保護確認のプロセス300の一例を描く。高レベルでは、プロセス300は、ユーザノードA302、ユーザノードB(図3に図示せず)、およびコンセンサスノードとも称されるブロックチェーンノード304によって行われる。ユーザノードA302のアカウントもユーザノードBのアカウントも汎用アカウントモデルに基づく記録保持モデルを有することができる。すなわち、ユーザノードA302およびユーザノードBのアカウント記録は複数の資産として保持される。価値の移動などの取引がユーザノードA302からユーザノードBになされ得る。ユーザノードA302は、取引金額以上の合計値を有する1つまたは複数のアカウント資産を、取引をカバーするように選択できる。1つまたは複数の資産の合計値と取引金額との間の差は、ユーザノードA302に残される取引のおつりと考えられ得る。

【００３４】

アカウントプライバシーを保護するために、ユーザノードA302は、取引をカバーするために使用される資産の価値のコミットメントを生成できる。ユーザノードA302は、取引の取引金額のコミットメントも生成できる。ユーザノードA302はHEも使用して、取引金額、おつりおよびコミットメントを生成するために使用される乱数を暗号化できる。取引の妥当性を検証するために、ブロックチェーンノード304は、コミットメントに秘匿された、およびZKPに基づいてHEによって暗号化された取引金額、おつりおよび乱数を比較できる。取引金額、おつりおよび乱数が一致すれば、取引は、ブロックチェーンノード304によって有効であると判定される。プロセス300の一層の詳細が図3の以下の説明に述べられる。

【００３５】

306では、ユーザノードA302が、ユーザノードBに取引金額を移動するための複数の資産を選択する。ユーザノードA302およびユーザノードBは、ブロックチェーンコンセンサスノードまたはコンセンサスプロセスに参加することなくブロックチェーンネットワークを使用するユーザノードであることができる。前述したように、ユーザノードA302は汎用アカウントモデルを使用して記録を保持できる。アカウント残高をアカウント残高モデル下の記録のために保持する代わりに、ユーザノードA302のアカウント価値は、それが所有する資産の合計値によって測定される。ユーザノードA302は、取引金額をカバーするのに十分な価値を有する複数の資産を選択できる。例えば、取引金額が7.5米ドルである場合、ユーザノードA302は、それぞれ5、2および1米ドルの価値がある3つの資産を、取引金額をカバーするように選択できる。

【００３６】

一部の実装形態では、各資産は、取引アドレスまたは対応する資産を識別する資産IDと関連付け可能である。資産IDは資産情報のハッシングであることができる。k個の選択された資産の資産IDはID_1、...、ID_kとして表現可能である。

【００３７】

308では、ユーザノードA302が複数の資産の合計値および取引金額に基づいておつりを計算する。資産が取引金額より大きい合計値を有するように選択されるので、おつりは、取引金額が差し引かれた選択された資産の合計値として計算可能である。取引金額を表現するためにtを、およびおつりを表現するためにt_0を使用して、おつりの計算は$t_0 = a_1 + ... + a_k - t$として表され得、式中$a_1$、...、$a_k$は、それぞれ、取引金額tをカバーするようにユーザノードA302によって選択されたk個の資産の資産価値である。

【００３８】

310では、ユーザノードA302が、取引金額に対応する乱数およびおつりに対応する乱数を生成する。取引金額tに対応する乱数はrとして表示可能である。おつりt_0に対応する乱数はr_0として表示可能である。一部の実装形態では、資産価値のコミットメントを作成するために複数の乱数が生成可能である。例えば、a_1、...、a_kが資産価値であると仮定すると、資産価値に対応する乱数はr_{a1}、...、r_{ak}として表され得る。

【００３９】

一部の実装形態では、乱数r_0は、ランダムに生成される代わりに計算可能である。計算は$r_0 = r_{a1} + ... + r_{ak} - r$として表され得、式中rは取引金額tに対するコミットメントを作成するために生成される乱数である。計算された乱数r_0を使用することによって、ユーザノードA302は、追加のZKPを生成して、移動される資産の合計値が受け取られる資産の合計値に等しいことを証明する必要はない。一部の実装形態では、ZKPを支援するために別の乱数r'が$r' = r_1 + ... + r_k - r - r_0$として計算可能である。

【００４０】

312では、ユーザノードA302が取引金額およびおつりのコミットメントを生成し、確率的HEに基づいて対応する乱数を暗号化する。一部の実装形態では、コミットメントを生成するために、PCなどの準同型コミットメント方式が使用可能である。非限定例としてPCを使用して、取引金額tのPCは乱数rを使用することによって生成可能であり、これは$PC(r, t) = g^r h^t$として表され得、式中gおよびhは楕円曲線の母線であることができ、$PC(r, t)$は曲線点のスカラ乗算である。同様に、おつりt_0のPCは$PC(r_0, t_0) = g^{r0} h^{t0}$として表され得る。

【００４１】

乱数rは、岡本-内山(OU)暗号方式などの確率的HE方式に基づいてユーザノードBの公開鍵を使用して暗号化可能である。Boneh-Goh-Nissimなどの他のHE方式も使用可能であることが理解されるはずである。非限定例としてOUを使用して、乱数は、取引金額tを乱数として扱うことによってOUに基づいて暗号化可能であり、これは$OU_B(r, t) = u^r v^t$、または単に$OU_B(t)$として表され得、式中uは、$v = u^n \bmod n$ならびに$n = p \times q$、式中pおよびqは2つの素数である、という条件を満たす$(Z/nZ)^*$の母線である。確率的OUは$OU(a + b) = OU(a) \times OU(b)$という性質を満たすことができ、式中aおよびbはOUのために使用される平文で

ある。

【００４２】

乱数r_0はユーザノードA302の公開鍵を使用して暗号化可能である。乱数は、おつりt_0を乱数として扱うことによってOUに基づいて暗号化可能であり、これは$OU_A(r_0, t_0)$として表され得る。

【００４３】

取引金額の暗号文は、次いで$T = (PC(t, r), OU_B(r, t))$として表され得、おつりの暗号文は$T_0 = (PC(t_0, r_0), OU_A(r_0, t_0))$として表され得る。同様に、k個の選択された資産の暗号文は$T_i = (PC(t_i, r_i), OU_A(r_i, t_i))$として表され得、式中、$i = 1、..., k$である。

【００４４】

314では、ユーザノードA302が1つまたは複数の範囲証明を生成する。一部の実装形態では、取引金額$t \geqq 0$を示すために第1の範囲証明RP_1が生成可能である。おつり$t_0 \geqq 0$、または言い換えれば、複数の資産の合計値が取引金額以上であることを示すために第2の範囲証明RP_2が生成可能である。

【００４５】

316では、ユーザノードA302がZKPを生成する。ZKPは、PC(r, t)に秘匿された乱数および取引金額が$OU_B(r, t)$に暗号化された乱数および取引金額と同じであり、かつ$PC(r_0, t_0)$に秘匿された乱数および取引金額が$OU_A(r_0, t_0)$に暗号化された乱数および取引金額と同じであることを示すために使用可能である。ZKPを生成するために、2つの乱数t'_1およびr'_1が選択可能である。2つの乱数は3つの値を生成するために使用可能であり、それらは$P = PC(t'_1, r'_1)$、$P' = OU_B(r'_1, t'_1)$,$P'' = OU_A(r'_1, t'_1)$。3つの値は次いで、$x = Hash(P, P', P'')$として表されるハッシュを生成するために使用可能である。ハッシュ値xは、$t'_2 = t'_1 + xt$、$r'_2 = r'_1 + xr$、$t'_3 = t'_1 + xt$および$r'_3 = r'_1 + xr_0$を計算するために使用可能である。ZKPはそこで$(P, P', t'_2, r'_2, P'', t'_3, r'_3)$として表され得る。

【００４６】

318では、ユーザノードA302が秘密鍵を使用して、取引データに署名するデジタル署名を生成する。一部の実装形態では、取引データは、k個の選択された資産の資産ID(ID_1、...、ID_k)、取引金額の暗号文(T)、おつりの暗号文(T_0)、範囲証明(RP_1およびRP_2)、乱数r'ならびにZKPを含むことができる。

【００４７】

320では、ユーザノードA302が、ブロックチェーンネットワークに取引データのデジタル署名されたコピーを提出する。

【００４８】

322では、ブロックチェーンノード304がデジタル署名を検証する。デジタル署名の検証は、取引データがユーザノードA302によって送信されることを保証するために行われ得る。一部の実装形態では、ブロックチェーンノード304は、取引が既に行われたかどうかを検証できる反二重支出機構を含む。もしそうであれば、ブロックチェーンノード304は取引を拒否できる。

【００４９】

324では、ブロックチェーンノード304が、選択された資産がユーザノードAのアカウントと関連付けられているかどうかを検証する。検証は資産の資産IDに基づくことができる。

【００５０】

326では、ブロックチェーンノード304が、選択された複数の資産の合計値が取引金額とおつりの和に等しいことを検証する。言い換えれば、ブロックチェーンは$a_1 + ... + a_k = t + t_0$を検証する。前述したように、汎用アカウントモデル下では、資産は、PCとしてブロックチェーンに保持されてデータプライバシーを保護できる。PCの準同型性に基づいて、$PC(r_{a1}, a_1) \times ... \times PC(r_{ak}, a_k) = PC(r_{a1} + ... + r_{ak}, a_1 + ... + a_k)$、および$PC(r, t) \times PC(r_0, t_0) = PC(r + r_0, t + t_0)$。したがって、$PC(r_{a1}, a_1) \times ... \times PC(r_{ak}, a$

$_k$) = PC(r, t)×PC(r_0, t_0)×$g^{r'}$を示すことによって、a_1 + ... + a_k = t + t_0が証明可能である。

【００５１】

328では、ブロックチェーンノード304が1つまたは複数の範囲証明を検証する。

【００５２】

330では、ブロックチェーンノード304がZKPを検証する。上述したように、ZKPは、ユーザノードBの公開鍵を使用して暗号化された取引金額に対応する乱数がPCによって秘匿された対応する乱数と同じであるかどうか、およびユーザノードA302の公開鍵を使用して暗号化されたおつりに対応する乱数がPCによって秘匿された対応する乱数と同じであるかどうかを検証するために生成可能である。一部の実装形態では、ZKPを検証するために、ブロックチェーンノード304は最初に、ハッシュ値xをx = Hash(P, P', P")として計算できる。ブロックチェーンノード304は次いで、PC(t'$_2$, r'$_2$) = P×PC(t, r)^x、OU_B(r'$_2$, t'$_2$) = P'×OU_B(r, t)^x、PC(t'$_3$, r'$_3$) = P×PC(t_0, r_0)^x、およびOU_A(r'$_3$, t'$_3$) = P"×OU_A(r_0, t_0)^{x}が全て真であるかどうかを検証できる。全てが真であれば、プロセス例300は332に進む。そうでなければ、ブロックチェーンノード304は取引を拒否できる。

【００５３】

332では、ブロックチェーンノード304がユーザノードA302およびユーザノードBのアカウントを更新する。ユーザノードA302およびユーザノードBのアカウントが汎用アカウントモデル下の記録として資産を保持するので、取引後に、ユーザノードA302から移動された複数の資産はユーザノードA302のアカウントから削除可能である。おつりはユーザノードA302のアカウントに戻して追加可能である。取引金額および対応する資産IDはユーザノードBのアカウントに新たな資産として追加可能である。一部の実装形態では、更新は、ユーザノードA302およびユーザノードBの対応するアカウントによって維持される資産リストを更新することに基づいて行われ得る。一部の実装形態では、更新は、ユーザノードA302およびユーザノードBによって維持される暗号化された資産価値に取引金額およびおつりの暗号文を追加することに基づいて行われ得る。アカウントの更新は図4を参照しつつ本明細書にさらに詳細に記載される。

【００５４】

図4は、本明細書の実装形態に従うブロックチェーン取引400の一例を描く。ブロックチェーン取引例400に図示されるように、ユーザノードA402がユーザノードB404に取引金額tを移動する。取引前に、ユーザノードA402は、(ID_1, T_1)、(ID_2, T_2)、(ID_n, T_n)を含むn個の資産を有する。

【００５５】

一例として図3を参照しつつ本明細書に記載されるコミットメント方式、暗号方式および取引プロセスを使用して、ユーザノードA402は取引データ408を生成でき、これはk個の選択された資産の資産ID、ID、ID_2、...、ID_kを含むことができる。取引データ408はT_0、T、RP_1、RP_2、r'およびZKPをさらに含むことができる。取引データ408が生成された後に、ユーザノードA402はそのデジタル署名を追加し、デジタル署名された取引データをコンセンサスのためのブロックチェーンネットワーク406に提出できる。

【００５６】

取引後に、k個の選択された資産はユーザノードA402のアカウントから削除可能である。おつりはユーザノードA402に戻して追加可能である。したがって、ユーザノードA402は、以下の(ID_{k+1}, T_{k+1})、(ID_{k+2}, T_{k+2})、...、(ID_n, T_n)、(ID_0, T_0)として表される資産を有することができ、ここでID_0はおつりt_0の資産IDを表現する。

【００５７】

取引前に、ユーザノードB404はm個の資産を有し、それらは($ID_{1'}$, $T_{1'}$)、($ID_{2'}$, $T_{2'}$)、($ID_{m'}$, $T_{m'}$)として表され得る。取引後に、取引金額はユーザノードB404に追加可能である。ユーザノードB404は、以下の($ID_{1'}$, $T_{1'}$)、($ID_{2'}$, $T_{2'}$)、($ID_{m'}$, $T_{m'}$)、(ID_t、T)として表される資産を有することができ、ここでID_tは取引金額tの資産IDを表現する。

【００５８】

図5は、HEに基づくブロックチェーン取引のプライバシー保護確認のプロセス500の一例を描く。高レベルでは、プロセス例500は、ユーザノードA502、ユーザノードB(図5に図示せず)、およびコンセンサスノードとも称されるブロックチェーンノード504によって行われる。ユーザノードA502のアカウントもユーザノードBのアカウントも汎用アカウントモデルに基づくことができる。価値の移動などの取引がユーザノードA502からユーザノードBになされ得る。ユーザノードA502は、取引金額以上の合計値を有する1つまたは複数のアカウント資産を、取引をカバーするように選択できる。1つまたは複数の資産の合計値と取引金額との間の差は、ユーザノードA502に残される取引のおつりと考えられ得る。

【００５９】

アカウントプライバシーを保護するために、ユーザノードA502は、PCなどのコミットメント方式を使用して、取引をカバーするために使用される資産の価値および取引の金額のコミットメントを生成できる。ユーザノードA502は線形決定性HEも使用して、コミットメントを生成するために使用される乱数を暗号化できる。線形決定性HEは、以下の性質を有することができる:$HE(s + t) = HE(s) \times HE(t)$および$HE(kt) = HE(t)^k$。取引の妥当性を検証するために、ブロックチェーンノード504は、コミットメントに秘匿された、およびZKPに基づいてHEによって暗号化された乱数を比較できる。乱数が一致すれば、取引は、ブロックチェーンノード504によって有効であると判定可能である。プロセス例500の一層の詳細が図5の以下の説明に述べられる。

【００６０】

506では、ユーザノードA502が、ユーザノードBに取引金額を移動するための複数の資産を選択する。ユーザノードA502およびユーザノードBは、ブロックチェーンコンセンサスノードまたはコンセンサスプロセスに参加することなくブロックチェーンネットワークを使用するユーザノードであることができる。ユーザノードA502は、取引金額をカバーするのに十分な価値を有する複数の資産を選択できる。

【００６１】

一部の実装形態では、各資産は、取引アドレスまたは対応する資産を識別する資産IDと関連付け可能である。資産IDは資産情報のハッシングであることができる。k個の選択された資産の資産IDはID_1、...、ID_kとして表現可能である。

【００６２】

508では、ユーザノードA502が複数の資産の合計値および取引金額に基づいておつりを計算する。資産が取引金額より大きい合計値を有するように選択されるので、おつりは、取引金額が差し引かれた選択された資産の合計値として計算可能である。取引金額を表現するためにtを、およびおつりを表現するためにt_0を使用して、おつりの計算は$t_0 = a_1 + ... + a_k - t$として表され得、式中$a_1$、...、$a_k$は、それぞれ、取引金額tをカバーするようにユーザノードA502によって選択されたk個の資産の資産価値である。

【００６３】

510では、ユーザノードA502が、取引金額に対応する乱数およびおつりに対応する乱数を生成する。取引金額tに対応する乱数はrとして表示可能である。おつりt_0に対応する乱数はr_0として表示可能である。一部の実装形態では、資産価値のコミットメントを作成するために複数の乱数が生成可能である。例えば、a_1、...、a_kが資産価値であると仮定すると、資産価値に対応する乱数はr_{a1}、...、r_{ak}として表され得る。

【００６４】

一部の実装形態では、乱数r_0は、ランダムに生成される代わりに計算可能である。計算は$r_0 = r_{a1} + ... + r_{ak} - r$として表され得、式中rは取引金額tに対するコミットメントを作成するために生成される乱数である。r_0を計算することによって、ユーザノードA502は、追加のZKPを生成して、移動される資産の合計値が受け取られる資産の合計値に等しいことを示す必要はない。一部の実装形態では、乱数r'がr' $= r_1 + ... + r_k - r - r_0$として計算可能である。

【００６５】

512では、ユーザノードA502が取引金額およびおつりのコミットメントを生成し、決定

性HEに基づいて対応する乱数を暗号化する。一部の実装形態では、コミットメントを生成するために、PCなどの準同型コミットメント方式が使用可能である。非限定例としてPCを使用して、取引金額tのPCは乱数rを使用することによって生成可能であり、これはPC(r, t) = $g^r h^t$として表され得、式中gおよびhは楕円曲線の母線であることができ、PC(r, t)は曲線点のスカラ乗算である。同様に、おつりt_0のPCはPC(r_0, t_0) = $g^{r0} h^{t0}$として表され得る。

【００６６】

乱数rは、線形決定性HEに基づいてユーザノードBの公開鍵を使用して暗号化可能である。線形決定性HEは、HE方式における乱数を0または1または他の適切な数に固定することによって、Paillier、Benaloh、OU、Naccache-Stern、Boneh-Goh-Nissim、Damgard-Jurikまたは等確率HEなどの確率的HEから得られ得る。暗号化された乱数はHE(r)として表され得る。

【００６７】

乱数r_0はユーザノードAの公開鍵を使用して暗号化可能である。乱数は線形決定性HEに基づいて暗号化可能である。暗号化された乱数はHE(r^0)として表され得る。

【００６８】

取引金額tの暗号文は、次いでT = ($g^r h^t$, $HE_B(r)$)として表され得、おつりの暗号文はT_0 = ($g^{r0} h^{t0}$, $HE_A(r_0)$)として表され得る。同様に、k個の選択された資産の暗号文はTi = ($g^{ri} h^{ti}$, HE(r_i))として表され得、式中、i = 1、...、kである。

【００６９】

514では、ユーザノードA502が1つまたは複数の範囲証明を生成する。一部の実装形態では、取引金額t≧0を示すために第1の範囲証明RP_1が生成可能である。おつりt_0≧0、または言い換えれば、複数の資産の合計値が取引金額以上であることを示すために第2の範囲証明RP_2が生成可能である。

【００７０】

516では、ユーザノードA502がZKPを生成する。ZKPは、PC(r, t)に秘匿された乱数がHE(r)に暗号化された乱数と同じであり、かつPC(r_0, t_0)に秘匿された乱数がHE(r_0)に暗号化された乱数と同じであることを示すために使用可能である。ZKPを生成するために、2つの乱数t'_1およびr'_1が選択可能である。2つの乱数は3つの値を生成するために使用可能であり、それらはP = $g^{r'1} h^{t'1}$、P' = $HE_B(r'_1)$,P" = $HE_A(r'_1)$。3つの値は次いで、x = Hash(P, P', P")として表されるハッシュを生成するために使用可能である。ハッシュ値xは、t'_2 = t'_1 + xt、r'_2 = r'_1 + xr、t'_3 = t'_1 + xtおよびr'_3 = r'_1 + xr_0を計算するために使用可能である。ZKPはそこで(P, P', t'_2, r'_2, P", t'_3, r'_3)として表され得る。

【００７１】

518では、ユーザノードA502が秘密鍵を使用して、取引データに署名するデジタル署名を生成する。一部の実装形態では、取引データは、k個の選択された資産の資産ID(ID_1、...、ID_k)、取引金額の暗号文(T)、おつりの暗号文(T_0)、範囲証明(RP_1およびRP_2)、乱数r'ならびにZKPを含むことができる。

【００７２】

520では、ユーザノードA502が、ブロックチェーンネットワークに取引データのデジタル署名されたコピーを提出する。

【００７３】

522では、ブロックチェーンノード504がデジタル署名を検証する。デジタル署名の検証は、取引データがユーザノードA502によって送信されることを保証するために行われ得る。一部の実装形態では、ブロックチェーンノード504は、取引が既に行われたかどうかを検証できる反二重支出機構を含む。もしそうであれば、ブロックチェーンノード504は取引を拒否できる。

【００７４】

524では、ブロックチェーンノード504が、選択された資産がユーザノードAのアカウントと関連付けられているかどうかを検証する。検証は資産の資産IDに基づくことができる

。

【００７５】

526では、ブロックチェーンノード504が、選択された複数の資産の合計値が取引金額およびおつりの和に等しいことを検証する。言い換えれば、ブロックチェーンノード504は$a_1 + ... + a_k = t + t_0$を検証する。前述したように、汎用アカウントモデル下では、資産は、PCとしてブロックチェーンに保持されてデータプライバシーを保護できる。PCの準同型性に基づいて、$PC(r_{a1}, a_1) \times ... \times PC(r_{ak}, a_k) = PC(r_{a1} + ... + r_{ak}, a_1 + ... + a_k)$、および$PC(r, t) \times PC(r_0, t_0) = PC(r + r_0, t + t_0)$。したがって、$PC(r_{a1}, a_1) \times ... \times PC(r_{ak}, a_k) = PC(r, t) \times PC(r_0, t_0) \times g^{r'}$を示すことによって、$a_1 + ... + a_k = t + t_0$が証明可能である。

【００７６】

528では、ブロックチェーンノード504が1つまたは複数の範囲証明を検証する。

【００７７】

530では、ブロックチェーンノード504がZKPを検証する。前述したように、ZKPは、ユーザノードBの公開鍵を使用して暗号化された取引金額に対応する乱数がPCによって秘匿された対応する乱数と同じであるかどうか、およびユーザノードA502の公開鍵を使用して暗号化されたおつりに対応する乱数がPCによって秘匿された対応する乱数と同じであるかどうかを検証するために生成可能である。一部の実装形態では、ZKPを検証するために、ブロックチェーンノード504は最初に、ハッシュ値xを$x = Hash(P, P', P'')$として計算できる。ブロックチェーンノード504は次いで、$g^{r'_2}h^{t'_2} = P \times (g^r h^t)^x$、$HE_B(r') = P' \times HE(r)^x$、$g^{r'_3}h^{t'_3} = P \times (g^{r_0}h^{t_0})^x$、および$HE_A(r'_3) = P'' \times HE_A(r_0)^x$が全て真であるかどうかを検証できる。各々が真であれば、プロセス例500は532に進む。そうでなければ、ブロックチェーンノード504は取引を拒否できる。

【００７８】

532では、ブロックチェーンノード504がユーザノードA502およびユーザノードBのアカウントを更新する。ユーザノードA502およびユーザノードBのアカウントが汎用アカウントモデル下の記録として資産を保持するので、取引後に、ユーザノードA502から移動された複数の資産はユーザノードA502のアカウントから削除可能である。おつりはユーザノードA502のアカウントに戻して追加可能である。取引金額および対応する資産IDはユーザノードBのアカウントに新たな資産として追加可能である。一部の実装形態では、更新は、ユーザノードA502およびユーザノードBの対応するアカウントによって維持される資産リストを更新することに基づいて行われ得る。一部の実装形態では、更新は、ユーザノードA502およびユーザノードBによって維持される暗号化された資産価値に取引金額およびおつりの暗号文を追加することに基づいて行われ得る。ブロックチェーン取引例400および対応するアカウント更新が図4の説明に記載される。

【００７９】

図6は、本明細書の実装形態に従って実行可能であるプロセス600の一例を描く。提示を明確にするため、以降の説明は、本説明におけるその他の図との関連で方法600について全体的に記載する。しかしながら、プロセス例600が、例えば、任意のシステム、環境、ソフトウェア、ならびにハードウェア、または適宜、システム、環境、ソフトウェアおよびハードウェアの組合せによって行われ得ることが理解されるであろう。一部の実装形態では、プロセス例600のステップが並列に、組み合わせて、ループして、または任意の順序で実行され得る。

【００８０】

602では、コンセンサスノードが取引と関連する取引データを受信する。一部の例では、取引データは、複数の資産を表すデータ、第1の乱数および取引の取引金額を秘匿した第1のコミットメント、第2の乱数および複数の資産の合計値から取引金額を差し引くことに基づいて計算されたおつりを秘匿した第2のコミットメント、確率的HE方式に基づいて第2のノードの公開鍵によって共に暗号化された取引金額および第3の乱数、確率的HE方式に基づいて第1のノードの公開鍵によって共に暗号化されたおつりおよび第4の乱数、1つ

または複数の範囲証明、ZKP、ならびに第1のノードの公開鍵に対応する秘密鍵に基づいて生成されたデジタル署名を備える。

【００８１】

一部の実装形態では、複数の資産の各々が、資産型、コミットメントに秘匿される資産価値、およびコミットメントを生成するために使用される乱数のうちの1つまたは複数と関連付けられる。一部の実装形態では、コンセンサスノードは、複数の資産の各々が同じ資産型と関連付けられると判定する。一部の実装形態では、第1のコミットメント、第2のコミットメント、および資産価値を秘匿したコミットメントは、準同型であるコミットメント方式に基づいて生成される。

【００８２】

一部の実装形態では、第3の乱数は、取引金額を乱数として扱うことによって確率的HE方式に基づいて暗号化され、そして第4の乱数は、おつりを乱数として扱うことによって確率的HE方式に基づいて暗号化される。一部の実装形態では、第1のコミットメントおよび第2のコミットメントはペダーセンコミットメント方式に基づいて生成され、そして確率的HE方式はOU暗号方式である。

【００８３】

一部の実装形態では、ZKPは、第5の乱数および第6の乱数を秘匿したペダーセンコミットメント、OU暗号方式に基づいて第2のアカウントの公開鍵によって暗号化された第5の乱数および第6の乱数の暗号文、ならびにOU暗号方式に基づいて第1のアカウントの公開鍵によって暗号化された第5の乱数および第6の乱数の暗号文を備える。

【００８４】

604では、コンセンサスノードが第1のノードの公開鍵に基づいてデジタル署名を検証する。

【００８５】

606では、コンセンサスノードが、取引金額およびおつりが各々ゼロ以上であることを1つまたは複数の範囲証明が証明すると判定する。

【００８６】

608では、コンセンサスノードが、複数の資産の合計値が取引金額およびおつりの和に等しいと判定する。一部の実装形態では、複数の資産の合計値が取引金額およびおつりの和に等しいと判定することは、コミットメント方式の準同型性に基づいて行われる。

【００８７】

610では、コンセンサスノードが、第1の乱数が第3の乱数に等しく、第2の乱数が第4の乱数に等しく、第1のコミットメントに秘匿された取引金額が第2のノードの公開鍵によって暗号化された取引金額に等しいと判定することによって、ZKPに基づいて、取引が有効であると判定する。

【００８８】

一部の実装形態では、取引は、第1のノードと関連するアカウントと第2のノードと関連するアカウントとの間で行われ、そして本方法は、取引が有効であると判定した後に、取引金額およびおつりに基づいて第1のノードと関連するアカウントおよび第2のノードと関連するアカウントを更新することをさらに含む。一部の実装形態では、ZKPは、確率的HEの性質に基づいて取引が有効であると判定するために生成および使用される。一部の実装形態では、取引が有効であると判定することは、ブロックチェーンネットワークの外部を通じた第1のノードと第2のノードとの間の対話なしにZKPに基づいて行われる。

【００８９】

図7は、本明細書の実装形態に従って実行可能であるプロセス例700を描く。提示を明確にするため、以降の説明は、本説明におけるその他の図との関連で方法700について全体的に記載する。しかしながら、プロセス例700が、例えば、任意のシステム、環境、ソフトウェア、ならびにハードウェア、または適宜、システム、環境、ソフトウェアおよびハードウェアの組合せによって行われ得ることが理解されるであろう。一部の実装形態では、プロセス例700のステップが並列に、組み合わせて、ループして、または任意の順序で

実行され得る。

【００９０】

702では、コンセンサスノードが取引と関連する取引データを受信する。一部の例では、取引データは、複数の資産を表すデータ、第1の乱数および取引の取引金額を秘匿した第1のコミットメント、第2の乱数および複数の資産の合計値から取引金額を差し引くことに基づいて計算されたおつりを秘匿した第2のコミットメント、線形決定性HE方式に基づいて第2のノードの公開鍵によって共に暗号化された取引金額および第3の乱数、線形決定性HE方式に基づいて第1のノードの公開鍵によって共に暗号化されたおつりおよび第4の乱数、1つまたは複数の範囲証明、ZKP、ならびに第1のノードの公開鍵に対応する秘密鍵に基づいて生成されたデジタル署名を備える。

【００９１】

一部の実装形態では、複数の資産の各々が、資産型、コミットメントに秘匿される資産価値、およびコミットメントを生成するために使用される乱数のうちの1つまたは複数と関連付けられる。一部の実装形態では、コンセンサスノードは、複数の資産の各々が同じ資産型と関連付けられると判定する。一部の実装形態では、第1のコミットメント、第2のコミットメント、および資産価値を秘匿したコミットメントは、準同型であるコミットメント方式に基づいて生成される。

【００９２】

一部の実装形態では、線形決定性HE方式は、確率的HE方式と関連する乱数を定数に変更することに基づいて確率的HE方式から導出される。

【００９３】

一部の実装形態では、ZKPは、第5の乱数および第6の乱数を秘匿したコミットメント、線形決定性HE方式に基づいて第2のアカウントの公開鍵によって暗号化された第5の乱数および第6の乱数の暗号文、ならびに線形決定性HE方式に基づいて第1のアカウントの公開鍵によって暗号化された第5の乱数および第6の乱数の暗号文を備える。

【００９４】

704では、コンセンサスノードが第1のノードの公開鍵に基づいてデジタル署名を検証する。

【００９５】

706では、コンセンサスノードが、取引金額およびおつりが各々ゼロ以上であることを1つまたは複数の範囲証明が証明すると判定する。

【００９６】

708では、コンセンサスノードが、複数の資産の合計値が取引金額およびおつりの和に等しいと判定する。一部の実装形態では、複数の資産の合計値が取引金額およびおつりの和に等しいと判定することは、コミットメント方式の準同型性に基づいて行われる。

【００９７】

710では、コンセンサスノードが、第1の乱数が第3の乱数に等しく、第2の乱数が第4の乱数に等しく、第1のコミットメントに秘匿された取引金額が第2のノードの公開鍵によって暗号化された取引金額に等しいと判定することによって、ZKPに基づいて、取引が有効であると判定する。

【００９８】

一部の実装形態では、取引は、第1のノードと関連するアカウントと第2のノードと関連するアカウントとの間で行われ、そして本方法は、取引が有効であると判定した後に、取引金額およびおつりに基づいて第1のノードと関連するアカウントおよび第2のノードと関連するアカウントを更新することをさらに含む。一部の実装形態では、ZKPは、線形決定性HEの性質に基づいて取引が有効であると判定するために生成および使用される。一部の実装形態では、取引が有効であると判定することは、ブロックチェーンネットワークの外部を通じた第1のノードと第2のノードとの間の対話なしにZKPに基づいて行われる。

【００９９】

図8は、本明細書の実装形態に従うプロセスを行うことができるブロックチェーンノー

ド800の一例を描く。高レベルでは、ブロックチェーンノード800は、受信ユニット802、検証ユニット804、第1の判定ユニット806、第2の判定ユニット808および第3の判定ユニット810を含む。

【０１００】

一部の実装形態では、受信ユニット802は、取引と関連する取引データを受信するように動作可能である。一部の例では、取引データは、複数の資産を表すデータ、第1の乱数および取引の取引金額を秘匿した第1のコミットメント、第2の乱数および複数の資産の合計値から取引金額を差し引くことに基づいて計算されたおつりを秘匿した第2のコミットメント、確率的HE方式に基づいて第2のノードの公開鍵によって共に暗号化された取引金額および第3の乱数、確率的HE方式に基づいて第1のノードの公開鍵によって共に暗号化されたおつりおよび第4の乱数、1つまたは複数の範囲証明、ZKP、ならびに第1のノードの公開鍵に対応する秘密鍵に基づいて生成されたデジタル署名を備える。

【０１０１】

一部の実装形態では、受信ユニット802は、取引と関連する取引データを受信するように動作可能であり、取引データが:複数の資産を表すデータ、第1の乱数および取引の取引金額を秘匿した第1のコミットメント、第2の乱数および複数の資産の合計値から取引金額を差し引くことに基づいて計算されたおつりを秘匿した第2のコミットメント、線形決定性HE方式に基づいて第2のノードの公開鍵によって共に暗号化された取引金額および第3の乱数、線形決定性HE方式に基づいて第1のノードの公開鍵によって共に暗号化されたおつりおよび第4の乱数、1つまたは複数の範囲証明、ZKP、ならびに第1のノードの公開鍵に対応する秘密鍵に基づいて生成されたデジタル署名を備える。

【０１０２】

一部の実装形態では、複数の資産の各々が、資産型、コミットメントに秘匿される資産価値、およびコミットメントを生成するために使用される乱数のうちの1つまたは複数と関連付けられる。一部の実装形態では、ブロックチェーンノード800は、複数の資産の各々が同じ資産型と関連付けられると判定する。一部の実装形態では、第1のコミットメント、第2のコミットメント、および資産価値を秘匿したコミットメントは、準同型であるコミットメント方式に基づいて生成される。一部の実装形態では、線形決定性HE方式は、確率的HE方式と関連する乱数を定数に変更することに基づいて確率的HE方式から導出される。

【０１０３】

一部の実装形態では、第3の乱数は、取引金額を乱数として扱うことによって確率的HE方式に基づいて暗号化され、そして第4の乱数は、おつりを乱数として扱うことによって確率的HE方式に基づいて暗号化される。一部の実装形態では、第1のコミットメントおよび第2のコミットメントはペダーセンコミットメント方式に基づいて生成され、そして確率的HE方式はOU暗号方式である。

【０１０４】

一部の実装形態では、ZKPは、第5の乱数および第6の乱数を秘匿したペダーセンコミットメント、OU暗号方式に基づいて第2のアカウントの公開鍵によって暗号化された第5の乱数および第6の乱数の暗号文、ならびにOU暗号方式に基づいて第1のアカウントの公開鍵によって暗号化された第5の乱数および第6の乱数の暗号文を備える。一部の実装形態では、ZKPは、第5の乱数および第6の乱数を秘匿したコミットメント、線形決定性HE方式に基づいて第2のアカウントの公開鍵によって暗号化された第5の乱数および第6の乱数の暗号文、ならびに線形決定性HE方式に基づいて第1のアカウントの公開鍵によって暗号化された第5の乱数および第6の乱数の暗号文を備える。

【０１０５】

検証ユニット804は、第1のノードの公開鍵に基づいてデジタル署名を検証するように動作可能である。

【０１０６】

第1の判定ユニット806は、取引金額およびおつりが各々ゼロ以上であることを1つまた

は複数の範囲証明が証明すると判定するように動作可能である。

【０１０７】

第2の判定ユニット808は、複数の資産の合計値が取引金額およびおつりの和に等しいと判定するように動作可能である。一部の実装形態では、複数の資産の合計値が取引金額およびおつりの和に等しいと判定することは、コミットメント方式の準同型性に基づいて行われる。

【０１０８】

第3の判定ユニット810は、第1の乱数が第3の乱数に等しく、第2の乱数が第4の乱数に等しく、第1のコミットメントに秘匿された取引金額が第2のノードの公開鍵によって暗号化された取引金額に等しいと判定することによって、ZKPに基づいて、取引が有効であると判定するように動作可能である。

【０１０９】

一部の実装形態では、取引は、第1のノードと関連するアカウントと第2のノードと関連するアカウントとの間で行われ、そしてブロックチェーンノード800は、第3の判定ユニット810が取引が有効であると判定した後に、取引金額およびおつりに基づいて第1のノードと関連するアカウントおよび第2のノードと関連するアカウントを更新するように動作可能な更新ユニットを含むことができる。一部の実装形態では、ZKPは、確率的HEの性質に基づいて取引が有効であると判定するために生成および使用される。一部の実装形態では、ZKPは、線形決定性HEの性質に基づいて取引が有効であると判定するために生成および使用される。一部の実装形態では、取引が有効であると判定することは、ブロックチェーンネットワークの外部を通じた第1のノードと第2のノードとの間の対話なしにZKPに基づいて行われる。

【０１１０】

本明細書に記載される発明の対象の実装形態は、特定の利点または技術的効果を実現するように実装可能である。例えば、本明細書の実装形態は、ブロックチェーンノードのアカウント残高および取引金額が取引の間プライベートであることを許す。資金移動の受取人は取引を確かめる、または乱数を使用してコミットメントを検証する必要はなく、取引確認は非対話型であることができる。ブロックチェーンノードは、HEおよびコミットメント方式に基づいて取引を確認してゼロ知識証明を許容できる。

【０１１１】

記載される方法論は、様々なモバイルコンピューティングデバイスのアカウント/データセキュリティの強化を可能にする。アカウントの残高および取引金額はHEに基づいて暗号化可能で、かつコミットメント方式によって秘匿可能である。そのため、コンセンサスノードが、アカウントの実際のアカウント残高を明らかにすることなくHEの性質に基づいて取引後の台帳におけるアカウント残高を更新できる。取引を確かめるために受取人に乱数が送信される必要がないので、データ漏洩のリスクが低減可能であり、そして乱数を管理するために使用される必要があるコンピューティングおよびメモリリソースが少なくなる。

【０１１２】

本明細書に記載される実装形態および動作は、デジタル電子回路網で、または本明細書に開示される構造を含め、コンピュータソフトウェア、ファームウェアもしくはハードウェアで、またはそれらの1つもしくは複数の組合せで実装可能である。同動作は、1つまたは複数のコンピュータ可読記憶デバイスに記憶されたまたは他の供給源から受信されたデータに対してデータ処理装置によって行われる動作として実装可能である。データ処理装置、コンピュータまたはコンピューティングデバイスは、例としてプログラマブルプロセッサ、コンピュータ、システムオンチップもしくはその複数、または以上の組合せを含め、データを処理するための装置、デバイスおよび機械を包含してよい。同装置は、専用論理回路網、例えば、中央処理装置(CPU)、フィールドプログラマブルゲートアレイ(FPGA)または特定用途向け集積回路(ASIC)を含むことができる。同装置は、当該コンピュータプログラムのための実行環境を作成するコード、例えば、プロセッサファームウェア、プロ

トコルスタック、データベース管理システム、オペレーティングシステム(例えばオペレーティングシステムもしくはオペレーティングシステムの組合せ)、クロスプラットフォーム実行時環境、仮想マシン、またはそれらの1つもしくは複数の組合せを構成するコードも含むことができる。同装置および実行環境は、ウェブサービス、分散コンピューティングおよびグリッドコンピューティングインフラストラクチャなどの様々な異なるコンピューティングモデルインフラストラクチャを実現できる。

【０１１３】

コンピュータプログラム(例えば、プログラム、ソフトウェア、ソフトウェアアプリケーション、ソフトウェアモジュール、ソフトウェアユニット、スクリプトまたはコードとしても知られている)は、コンパイラ型またはインタープリタ型言語、宣言型または手続き型言語を含め、任意の形式のプログラミング言語で書かれ得、そしてそれは、スタンドアロンプログラムとして、またはモジュール、コンポーネント、サブルーチン、オブジェクトもしくはコンピューティング環境での使用に適する他のユニットとしてを含め、任意の形式に展開可能である。プログラムは、他のプログラムもしくはデータ(例えば、マークアップ言語文書に記憶される1つもしくは複数のスクリプト)を保持するファイルの一部分に、当該プログラムに専用の単一のファイルに、または複数の連係ファイル(例えば、1つもしくは複数のモジュール、サブプログラムもしくはコードの一部分を記憶するファイル)に記憶可能である。コンピュータプログラムは、1つのコンピュータ上で、または1つのサイトに設けられるもしくは複数のサイトにわたって分散されて通信ネットワークによって相互接続される複数のコンピュータ上で実行可能である。

【０１１４】

コンピュータプログラムの実行のためのプロセッサは、例として、汎用および専用の両マイクロプロセッサ、ならびに任意の種類のデジタルコンピュータの任意の1つまたは複数のプロセッサを含む。一般に、プロセッサは、リードオンリメモリまたはランダムアクセスメモリまたは両方から命令およびデータを受けることになる。コンピュータの必須要素は、命令に従って動作を行うためのプロセッサ、ならびに命令およびデータを記憶するための1つまたは複数のメモリデバイスである。一般に、コンピュータはさらに、データを記憶するための1つまたは複数の大容量記憶デバイスを含む、または作動的に結合されて、それからデータを受けるまたはそれにデータを転送するまたは両方行うことになる。コンピュータは、別のデバイス、例えば、モバイルデバイス、携帯情報端末(PDA)、ゲーム機、全地球測位システム(GPS)受信器、またはポータブル記憶デバイスに埋め込み可能である。コンピュータプログラム命令およびデータを記憶するのに適するデバイスには、例として、半導体メモリデバイス、磁気ディスクおよび光磁気ディスクを含め、不揮発性メモリ、媒体およびメモリデバイスを含む。プロセッサおよびメモリは、専用論理回路網によって補足可能、またはそれに組み込み可能である。

【０１１５】

モバイルデバイスには、ハンドセット、ユーザ機器(UE)、移動電話(例えば、スマートフォン)、タブレット、ウェアラブルデバイス(例えば、スマートウォッチおよびスマートグラス)、人体内の埋込みデバイス(例えば、バイオセンサ、人工内耳)、または他の種類のモバイルデバイスを含むことができる。モバイルデバイスは、様々な通信ネットワーク(下記される)に無線で(例えば、無線周波数(RF)信号を使用して)通信できる。モバイルデバイスは、モバイルデバイスの現在の環境の特性を測定するためのセンサを含むことができる。センサには、カメラ、マイクロホン、近接センサ、GPSセンサ、運動センサ、加速度計、周辺光センサ、水分センサ、ジャイロスコープ、コンパス、気圧計、指紋センサ、顔認識システム、RFセンサ(例えば、Wi-Fiおよびセル無線)、温度センサ、または他の種類のセンサを含むことができる。例えば、カメラには、可動または固定レンズ、フラッシュ、イメージセンサおよび画像プロセッサを持つ前方または後方カメラを含むことができる。カメラは、顔および/または虹彩認識のための詳細を取得することが可能なメガピクセルカメラであることができる。カメラは、データプロセッサおよびメモリに記憶されるまたは遠隔でアクセスされる認証情報と共に、顔認識システムを形成できる。顔認識シス

テムまたは1つもしくは複数のセンサ、例えば、マイクロホン、運動センサ、加速度計、GPSセンサもしくはRFセンサはユーザ認証のために使用可能である。

【０１１６】

ユーザとの対話を提供するために、実装形態は、表示デバイスおよび入力デバイス、例えば、ユーザに情報を表示するための液晶ディスプレイ(LCD)または有機発光ダイオード(OLED)/仮想現実(VR)/拡張現実(AR)ディスプレイならびにユーザがコンピュータに入力を提供できるタッチスクリーン、キーボードおよびポインティングデバイス、を有するコンピュータに実装可能である。ユーザとの対話を提供するために他の種類のデバイスも使用可能であり、例えば、ユーザに提供されるフィードバックは任意の形態の感覚フィードバック、例えば、視覚フィードバック、聴覚フィードバックまたは触覚フィードバックであることができ、そしてユーザからの入力は、音響、音声または触覚入力を含め、任意の形態で受け取り可能である。加えて、コンピュータは、ユーザによって使用されるデバイスに文書を送信し、それから文書を受信することによって、例えば、ユーザのクライアントデバイス上のウェブブラウザから受信される要求に応じてウェブブラウザにウェブページを送信することによって、ユーザと対話できる。

【０１１７】

実装形態は、有線または無線デジタルデータ通信(またはその組合せ)の任意の形態または媒体、例えば、通信ネットワークによって相互接続されるコンピューティングデバイスを使用して実装可能である。相互接続されるデバイスの例は、典型的に通信ネットワークを通じて対話する、一般に互いから離れたクライアントおよびサーバである。クライアント、例えば、モバイルデバイスは、サーバと、またはサーバを通じて取引自体を実施、例えば、購入、売却、支払、譲渡、送付もしくは貸付取引を行う、またはそれを許可できる。そのような取引は、動作および応答が時間的に近いように、例えば、動作および応答が実質的に同時に発生していると個人が認める、個人の動作に続く応答に対する時間差が1ミリ秒(ms)未満もしくは1秒(s)未満である、またはシステムの処理限界を考慮に入れて応答には意図的な遅延がないように、リアルタイムであってよい

【０１１８】

通信ネットワークの例には、ローカルエリアネットワーク(LAN)、無線アクセスネットワーク(RAN)、メトロポリタンエリアネットワーク(MAN)およびワイドエリアネットワーク(WAN)が含まれる。通信ネットワークは、インターネットの全てもしくは一部分、別の通信ネットワーク、または通信ネットワークの組合せを含むことができる。情報は、ロングタームエボリューション(LTE)、5G、IEEE802、インターネットプロトコル(IP)、または他のプロトコルもしくはプロトコルの組合せを含め、様々なプロトコルおよび標準に従って通信ネットワーク上で伝送可能である。通信ネットワークは、接続されたコンピューティングデバイス間で音声、ビデオ、生体もしくは認証データまたは他の情報を伝送できる。

【０１１９】

別々の実装形態として記載される特徴が、組み合わせて単一の実装形態で実装されてよい一方、単一の実装形態として記載される特徴が、別々に複数の実装形態で、または任意の適切な部分組合せで実装されてよい。特定の順序で記載および特許請求される動作が、その特定の順序も、全ての例示される動作が行われなければならない(一部の動作は任意選択であり得る)ことも必要とすると理解されるべきでない。適宜、マルチタスキングまたは並列処理(またはマルチタスキングおよび並列処理の組合せ)が行われ得る。

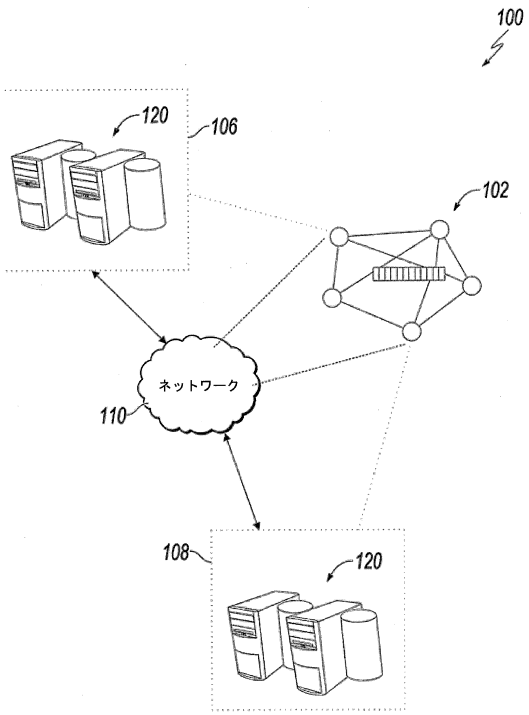
【符号の説明】

【０１２０】

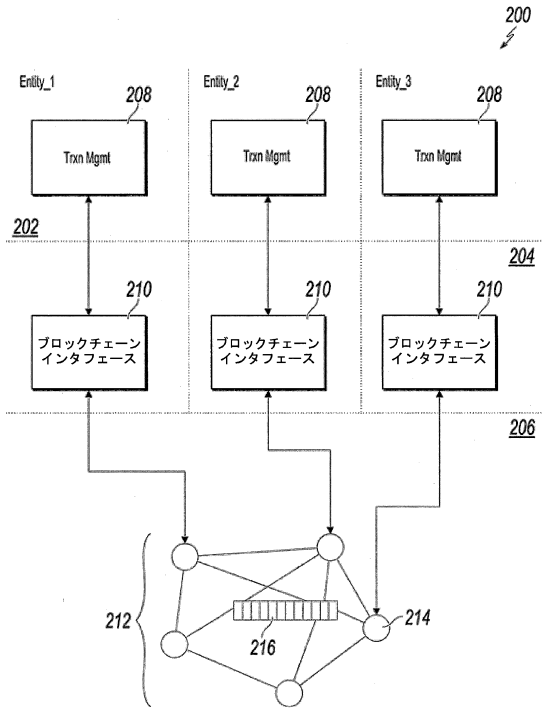
100　環境
102　パブリックブロックチェーン
106　コンピューティングシステム
108　コンピューティングシステム
110　ネットワーク
200　概念アーキテクチャ

202　エンティティ層
204　ホストサービス層
206　パブリックブロックチェーン層
208　取引管理システム
210　ブロックチェーンインタフェース
212　ブロックチェーンネットワーク
214　ノード
216　ブロックチェーン
302　ユーザノードA
304　ブロックチェーンノード
402　ユーザノードA
404　ユーザノードB
406　ブロックチェーンネットワーク
408　取引データ
502　ユーザノードA
504　ブロックチェーンノード
800　ブロックチェーンノード
802　受信ユニット
804　検証ユニット
806　第1の判定ユニット
808　第2の判定ユニット
810　第3の判定ユニット

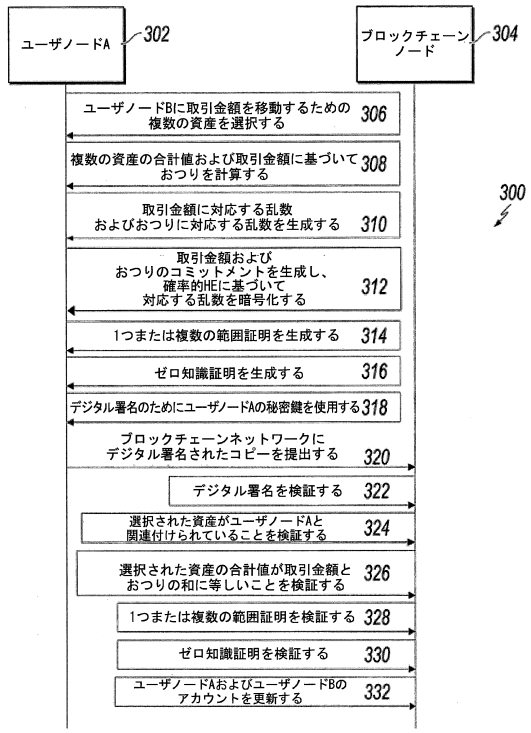
【図１】



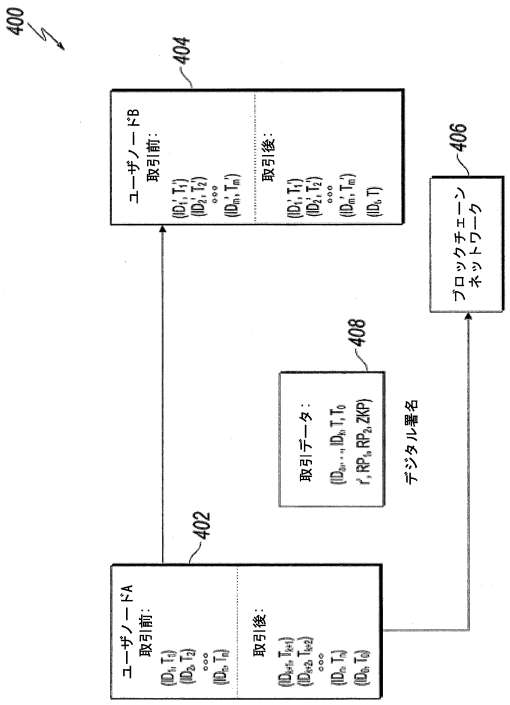
【図２】



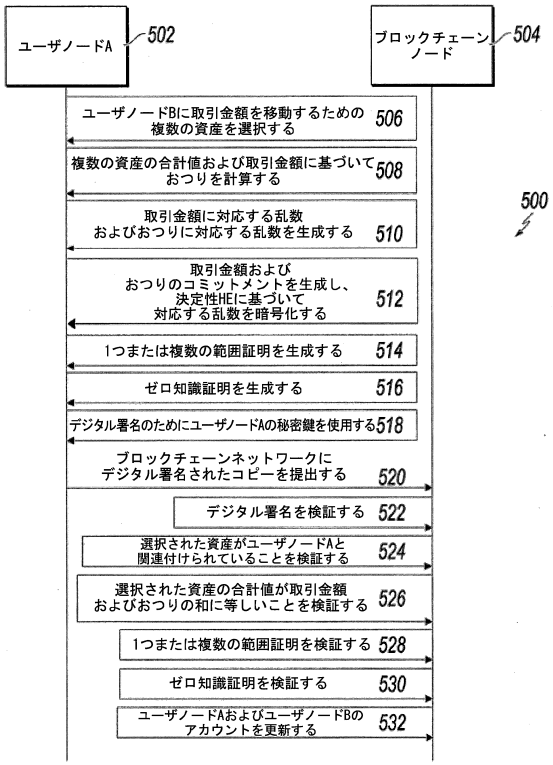
【図３】


ユーザノードA
302
ブロックチェーンノード
304
300
ユーザノードBに取引金額を移動するための複数の資産を選択する 306
複数の資産の合計値および取引金額に基づいておつりを計算する 308
取引金額に対応する乱数およびおつりに対応する乱数を生成する 310
取引金額およびおつりのコミットメントを生成し、確率的HEに基づいて対応する乱数を暗号化する 312
1つまたは複数の範囲証明を生成する 314
ゼロ知識証明を生成する 316
デジタル署名のためにユーザノードAの秘密鍵を使用する 318
ブロックチェーンネットワークにデジタル署名されたコピーを提出する 320
デジタル署名を検証する 322
選択された資産がユーザノードAと関連付けられていることを検証する 324
選択された資産の合計値が取引金額とおつりの和に等しいことを検証する 326
1つまたは複数の範囲証明を検証する 328
ゼロ知識証明を検証する 330
ユーザノードAおよびユーザノードBのアカウントを更新する 332

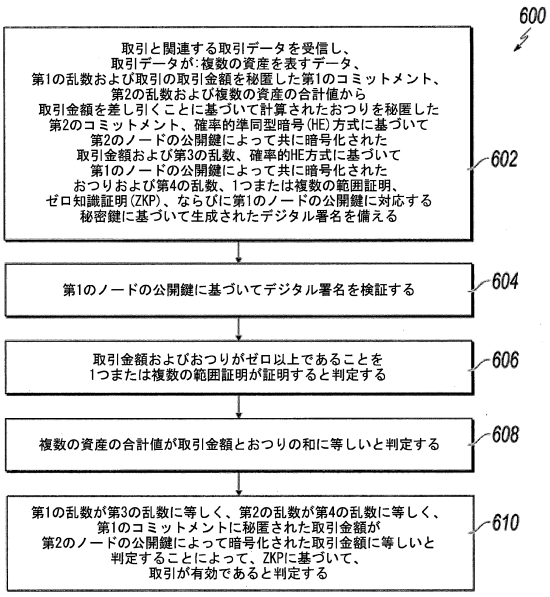
【図４】


400
404
ユーザノードB
取引前:
取引後:
406
ブロックチェーンネットワーク
408
取引データ:
デジタル署名
402
ユーザノードA
取引前:
取引後:

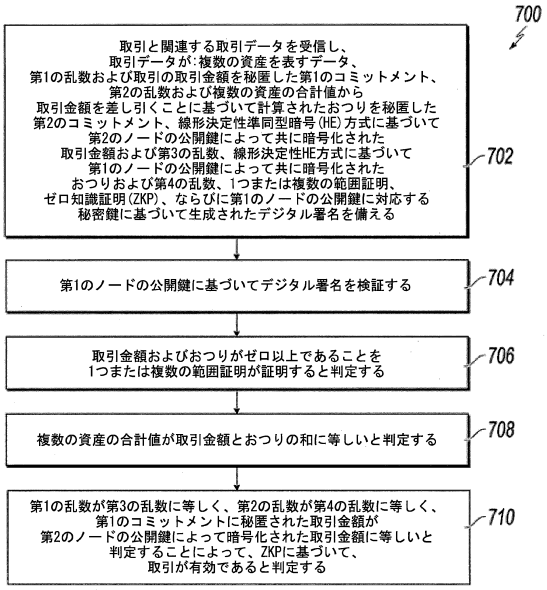
【図５】


ユーザノードA
502
ブロックチェーンノード
504
500
ユーザノードBに取引金額を移動するための複数の資産を選択する 506
複数の資産の合計値および取引金額に基づいておつりを計算する 508
取引金額に対応する乱数およびおつりに対応する乱数を生成する 510
取引金額およびおつりのコミットメントを生成し、決定性HEに基づいて対応する乱数を暗号化する 512
1つまたは複数の範囲証明を生成する 514
ゼロ知識証明を生成する 516
デジタル署名のためにユーザノードAの秘密鍵を使用する 518
ブロックチェーンネットワークにデジタル署名されたコピーを提出する 520
デジタル署名を検証する 522
選択された資産がユーザノードAと関連付けられていることを検証する 524
選択された資産の合計値が取引金額およびおつりの和に等しいことを検証する 526
1つまたは複数の範囲証明を検証する 528
ゼロ知識証明を検証する 530
ユーザノードAおよびユーザノードBのアカウントを更新する 532

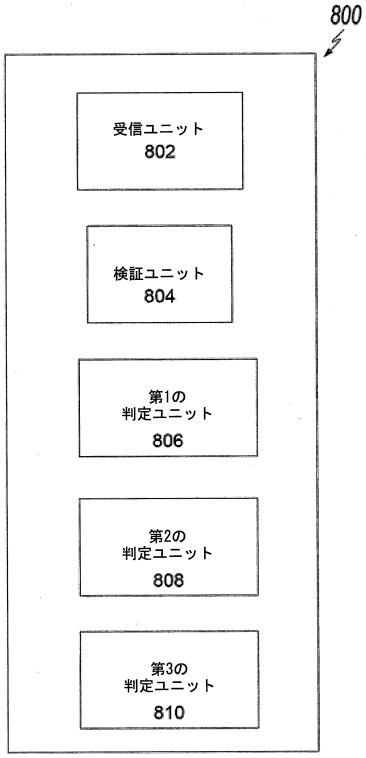
【図６】


600
取引と関連する取引データを受信し、
取引データが:複数の資産を表すデータ、
第1の乱数および取引の取引金額を秘匿した第1のコミットメント、
第2の乱数および複数の資産の合計値から
取引金額を差し引くことに基づいて計算されたおつりを秘匿した
第2のコミットメント、確率的準同型暗号(HE)方式に基づいて
第2のノードの公開鍵によって共に暗号化された
取引金額および第3の乱数、確率的HE方式に基づいて
第1のノードの公開鍵によって共に暗号化された
おつりおよび第4の乱数、1つまたは複数の範囲証明、
ゼロ知識証明(ZKP)、ならびに第1のノードの公開鍵に対応する
秘密鍵に基づいて生成されたデジタル署名を備える 602
第1のノードの公開鍵に基づいてデジタル署名を検証する 604
取引金額およびおつりがゼロ以上であることを
1つまたは複数の範囲証明が証明すると判定する 606
複数の資産の合計値が取引金額とおつりの和に等しいと判定する 608
第1の乱数が第3の乱数に等しく、第2の乱数が第4の乱数に等しく、
第1のコミットメントに秘匿された取引金額が
第2のノードの公開鍵によって暗号化された取引金額に等しいと
判定することによって、ZKPに基づいて、
取引が有効であると判定する 610

【図７】


700
取引と関連する取引データを受信し、
取引データが:複数の資産を表すデータ、
第1の乱数および取引の取引金額を秘匿した第1のコミットメント、
第2の乱数および複数の資産の合計値から
取引金額を差し引くことに基づいて計算されたおつりを秘匿した
第2のコミットメント、線形決定性準同型暗号(HE)方式に基づいて
第2のノードの公開鍵によって共に暗号化された
取引金額および第3の乱数、線形決定性HE方式に基づいて
第1のノードの公開鍵によって共に暗号化された
おつりおよび第4の乱数、1つまたは複数の範囲証明、
ゼロ知識証明(ZKP)、ならびに第1のノードの公開鍵に対応する
秘密鍵に基づいて生成されたデジタル署名を備える
702
第1のノードの公開鍵に基づいてデジタル署名を検証する
704
取引金額およびおつりがゼロ以上であることを
1つまたは複数の範囲証明が証明すると判定する
706
複数の資産の合計値が取引金額とおつりの和に等しいと判定する
708
第1の乱数が第3の乱数に等しく、第2の乱数が第4の乱数に等しく、
第1のコミットメントに秘匿された取引金額が
第2のノードの公開鍵によって暗号化された取引金額に等しいと
判定することによって、ZKPに基づいて、
取引が有効であると判定する
710

【図８】


800
受信ユニット
802
検証ユニット
804
第1の
判定ユニット
806
第2の
判定ユニット
808
第3の
判定ユニット
810

フロントページの続き

(72)発明者　ウェンビン・ジャン
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント
(72)発明者　バオリ・マ
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント
(72)発明者　フアンユ・マ
中華人民共和国・３１１１２１・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・ウェン・イ・ロード・ナンバー・９６９・ビルディング・３・５／エフ・アリババ・グループ・リーガル・デパートメント

審査官　中里　裕正

(56)参考文献　特開２０１８－００７１６８（ＪＰ，Ａ）
米国特許出願公開第２０１６／０３５８１６５（ＵＳ，Ａ１）
国際公開第２０１６／０４９４０６（ＷＯ，Ａ１）
中国特許出願公開第１０８４１８７８３（ＣＮ，Ａ）
長沼 健、鈴木 貴之、吉野 雅之、佐藤 尚宜、高橋 健太，Hyperledger Fabricを用いた非中央集権型ネッティングプロトコル，SCIS2018，日本，電子情報通信学会，２０１８年　1月２６日
安坂 祐紀、渡辺 知恵美、天笠 俊之、北川 博之，プライバシーを考慮したブロックチェーンの取引者間事前合意プロトコル，CSS2018，日本，情報処理学会，２０１８年１０月１５日，P850-856

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｑ　２０／０６