(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2020-502864
(P2020-502864A)
(43)公表日　令和2年1月23日(2020.1.23)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675Z	
G09C	1/00	(2006.01)	H04L	9/00	675B	
			G09C	1/00	640D	

審査請求 有　予備審査請求 未請求　（全 24 頁）

(21)出願番号　特願2019-521681 (P2019-521681)
(86)(22)出願日　平成30年11月7日 (2018.11.7)
(85)翻訳文提出日　令和1年6月18日 (2019.6.18)
(86)国際出願番号　PCT/CN2018/114344
(87)国際公開番号　WO2019/072264
(87)国際公開日　平成31年4月18日 (2019.4.18)

(71)出願人　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(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】準同型暗号を使用したブロックチェーンデータ保護

(57)【要約】
本開示の実装形態は、第1のアカウントから、第1の乱数に基づいて生成されるトランザクション量の第1の量のコミットメント値のデジタル署名されたコピー、第1のアカウントの公開鍵を使用して暗号化される残高移動の第1の量および第1の乱数、第2のアカウントの公開鍵を使用して暗号化される残高移動の第2の量および第2の乱数、ならびに1つまたは複数の選択された乱数に基づいて生成される値のセットを受信することを含む。第1のアカウントは、値のセットに基づいて、第1の量と第2の量が同じであるかどうか、および第1の乱数と第2の乱数が同じであるかどうかを決定し、残高移動の第1の量に基づいて、第1のアカウントの残高および第2のアカウントの残高を更新する。

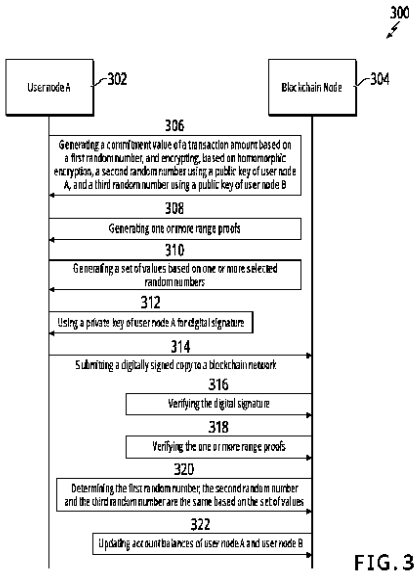


FIG.3

【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のコンセンサスノードによって実施されるコンピュータ実装方法であって、
第1のアカウントから、第1の乱数に基づいて生成される第1のアカウントから第2のアカウントへ移されるべきトランザクション量の第1の量のコミットメント値のデジタル署名されたコピー、前記第1のアカウントの公開鍵を使用して暗号化される前記残高移動の前記第1の量および前記第1の乱数、前記第2のアカウントの公開鍵を使用して暗号化される前記残高移動の第2の量および第2の乱数、1つまたは複数のレンジプルーフ、ならびに1つまたは複数の選択された乱数に基づいて生成される値のセットを受信するステップと、
前記デジタル署名されたコピーに対応するデジタル署名を、前記デジタル署名を生成するために使用される秘密鍵に対応する前記第1のアカウントの公開鍵を使用して検証するステップと、
前記残高移動の前記量が0より大きく、かつ前記第1のアカウントの残高以下であることを、前記1つまたは複数のレンジプルーフが証明すると決定するステップと、
値の前記セットに基づいて、前記第1の量と前記第2の量が同じであるかどうか、および、前記第1の乱数と前記第2の乱数が同じであるかどうかを決定するステップと、
前記第1の量と前記第2の量が同じであり、前記第1の乱数と前記第2の乱数が同じである場合、前記残高移動の前記第1の量に基づいて前記第1のアカウントの前記残高および前記第2のアカウントの残高を更新するステップとを備える、コンピュータ実装方法。
【請求項２】
前記コミットメント値が、準同型であるコミットメントスキームを使用して生成される、請求項1に記載のコンピュータ実装方法。
【請求項３】
前記コミットメントスキームがペダーセンコミットメントスキームである、請求項2に記載のコンピュータ実装方法。
【請求項４】
前記残高移動の前記第1の量および前記第1の乱数が、確率論的準同型暗号(HE)アルゴリズムに基づいて前記第1のアカウントの前記公開鍵を使用して暗号化され、前記残高移動の前記第2の量および第2の乱数が、前記確率論的HEアルゴリズムに基づいて前記第2のアカウントの前記公開鍵を使用して暗号化される、請求項1に記載のコンピュータ実装方法。
【請求項５】
前記確率論的HEアルゴリズムが、岡本-内山HEアルゴリズムである、請求項4に記載のコンピュータ実装方法。
【請求項６】
前記選択された乱数がr*、t*、z1*、およびz2*によって表され、前記選択された乱数がa、b、c、およびdを生成するために使用され、a=r*+xr、b=t*+xt、c=z1*+xz1、かつd=z2*+xz2であり、rが前記第1の乱数であり、tが前記残高移動の前記第1の量であり、xがハッシュ値である、請求項4に記載のコンピュータ実装方法コンピュータ実装方法。
【請求項７】
値の前記セットがC、D、およびEに基づいてさらに生成され、$C=g^{r*}h^{t*}$、$D=u2^{r*}v2^{z1*}$、$E=u2^{t*}v2^{z2*}$であり、g、h、u2、およびv2が楕円曲線のジェネレータであり、xがC、D、およびEをハッシュすることに基づいて生成される、請求項6に記載のコンピュータ実装方法。
【請求項８】
確率論的HEの性質に基づいて、前記第1の量および前記第2の量が同じであると決定され、前記第1の乱数および前記第2の乱数が同じであると決定される、請求項7に記載のコンピュータ実装方法。
【請求項９】

$g^a h^b = CT^x$、$u2^a v2^c = DZ\_B1^x$、かつ$u2^b v2^d = EZ_B2^x$である場合、前記第1の量と前記第2の量が同じであると決定され、前記第1の乱数と前記第2の乱数が同じであると決定され、$T = g^r h^t$が前記残高移動の前記量の前記コミットメント値であり、$Z\_B1 = u2^r v2^{z1}$、$Z_B2 = u2^t v2^{z2}$であり、z1およびz2が、前記確率論的HEスキームに基づいて前記残高移動の前記第2の量および前記第2の乱数を暗号化するために使用される乱数である、請求項8に記載のコンピュータ実装方法。

【請求項１０】

前記第1のアカウントの前記残高および前記第2のアカウントの残高を更新することがHEに基づいて実行される、請求項1に記載のコンピュータ実装方法。

【請求項１１】

1つまたは複数のプロセッサによって実行されると、請求項1から10のうちの1つまたは複数の方法に従う動作を前記1つまたは複数のプロセッサに実行させる命令が記憶された、前記1つまたは複数のプロセッサに結合される、非一時的コンピュータ可読記憶媒体。

【請求項１２】

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よって実行されると、請求項1から10のうちの1つまたは複数の方法に従う動作を前記1つまたは複数のプロセッサに実行させる命令が記憶された、前記コンピューティングデバイスに結合される、コンピュータ可読記憶デバイスとを備える、システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、準同型暗号を使用したブロックチェーンデータ保護に関する。

【背景技術】

【０００２】

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得るブロックチェーンネットワークは、参加するエンティティが安全にかつ変更不可能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トランザクションの台帳システムとして記述されることが可能であり、台帳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。例示的なタイプのブロックチェーンには、パブリックブロックチェーン、パーミッションドブロックチェーン、およびプライベートブロックチェーンがあり得る。パブリックブロックチェーンは、その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ことがすべてのエンティティに開かれている。パーミッションドブロックチェーンは、パブリックブロックチェーンに似ているが、加わるための許可を得たエンティティだけに開かれている。プライベートブロックチェーンは、読取りパーミッションおよび書込みパーミッションを集中的に制御する特定のエンティティだけに提供される。

【０００３】

ブロックチェーンは、参加者が暗号通貨を使用して商品および/またはサービスを購入/販売するために取引を行うことを可能にする、暗号通貨ネットワークにおいて使用される。一般的な暗号通貨にはビットコインがある。暗号通貨ネットワークでは、ユーザ間の取引を記録するために記録管理モデルが使用される。例示的な記録管理モデルには、未使用トランザクションアウトプット(UTXO: Unspent Transaction Output)モデルおよびアカウント残高(Account Balance)モデルがある。UTXOモデルでは、各トランザクションは、前のトランザクションからのアウトプットを使用し、後のトランザクションにおいて使用され得る新しいアウトプットを生成する。ユーザの未使用のトランザクションが追跡され、ユーザの保有する残高がユーザのすべての未使用のトランザクションの合計として計算される。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追跡される。各トランザクションに対して、使用するアカウントの残高がトランザクションの量以上であることを確実にするために、その残高が確認される。これは従来の銀行業と

同等である。

【０００４】

ブロックチェーン台帳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。各ブロックは台帳のページに類似していることがあるが、ブロックチェーン自体が台帳の完全なコピーである。個々のトランザクションが確認されてブロックに追加され、ブロックはブロックチェーンに追加される。ブロックチェーン台帳のコピーは、ネットワークの複数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ついてグローバルな合意ができる。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には、すべてのノードが閲覧のために公開されている。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、暗号化技術が実装され得る。

【０００５】

アカウントモデルのもとでは、トランザクションの双方の関係者がコミットする対象の値を隠すために、コミットメントスキームが使用され得る。コミットメントスキームは、関係者が選択または値をコミットし、関与する他の関係者にその値を後で伝えることの必要性から生じ得る。たとえば、対話型のペダーセンコミットメントでは、関係者Aは、乱数rに基づいて生成されるコミットメント値(Commitment Value)PC(r,t)を送信することによって、トランザクション量tをコミットすることができる。コミットメント値が生成され、関係者Bは乱数rを得ることによってのみトランザクション量tを明らかにすることができる。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

本開示の実装形態は、ユーザによる確認、対話、およびトランザクション量またはアカウント残高の暴露を伴わない、ブロックチェーントランザクションのプライバシーが保護された検証のための、コンピュータ実装方法を含む。より具体的には、本開示の実装形態は、トランザクション量、アカウント残高、または他のブロックチェーンノードへのコミットメントを生成するための乱数を明らかにすることなく、コミットメントスキームおよび準同型暗号(Homomorphic Encryption)に基づいて、ブロックチェーンユーザ間のトランザクションを承認することを対象とする。

【課題を解決するための手段】

【０００７】

いくつかの実装形態では、活動は、第1のアカウントから、第1の乱数に基づいて生成される第1のアカウントから第2のアカウントへ移されるべきトランザクション量の第1の量のコミットメント値のデジタル署名されたコピー、第1のアカウントの公開鍵を使用して暗号化される残高移動の第1の量および第1の乱数、第2のアカウントの公開鍵を使用して暗号化される残高移動の第2の量および第2の乱数、1つまたは複数のレンジプルーフ、ならびに1つまたは複数の選択された乱数に基づいて生成される値のセットを受信することと、デジタル署名されたコピーに対応するデジタル署名を、デジタル署名を生成するために使用される秘密鍵に対応する第1のアカウントの公開鍵を使用して検証することと、残高移動の量が0より大きく第1のアカウントの残高以下であることを1つまたは複数のレンジプルーフが証明すると決定することと、値のセットに基づいて、第1の量と第2の量が同じであるかどうか、および第1の乱数と第2の乱数が同じであるかどうかを決定することと、第1の量と第2の量が同じであり、第1の乱数と第2の乱数が同じである場合、残高移動の第1の量に基づいて第1のアカウントの残高および第2のアカウントの残高を更新することとを含む。他の実装形態は、対応するシステムと、装置と、コンピュータ記憶デバイスに符号化される、方法の活動を実行するように構成されるコンピュータプログラムとを含む。

【０００８】

これらのおよび他の実装形態は各々、以下の特徴のうちの1つまたは複数を任意選択で

含み得る。コミットメント値が、準同型であるコミットメントスキームを使用して生成される。コミットメントスキームが、ペダーセンコミットメントスキームである。残高移動の第1の量および第1の乱数が、確率論的準同型暗号(HE)アルゴリズム(Probabilistic Homomorphic Encryption (HE) Algorithm)に基づいて第1のアカウントの公開鍵を使用して暗号化され、残高移動の第2の量および第2の乱数が、確率論的HEアルゴリズムに基づいて第2のアカウントの公開鍵を使用して暗号化される。確率論的HEアルゴリズムが、岡本-内山HEアルゴリズム(Okamoto-Uchiyama HE Algorithm)である。選択された乱数が、r*、t*、z1*、およびz2*によって表され、選択された乱数が、a、b、c、およびdを生成するために使用され、a=r*+xr、b=t*+xt、c=z1*+xz1、かつd=z2*+xz2であり、rが第1の乱数であり、tが残高移動の第1の量であり、xがハッシュ値である。値のセットがさらに、C、D、およびEに基づいて生成され、$C=g^{r^*}h^{t^*}$、$D=u2^{r^*}v2^{z1^*}$、$E=u2^{t^*}v2^{z2^*}$であり、g、h、u2、およびv2が楕円曲線のジェネレータであり、xがC、D、およびEをハッシュすることに基づいて生成される。確率論的HEの性質に基づいて、第1の量および第2の量が同じであると決定され、第1の乱数および第2の乱数が同じであると決定される。$g^ah^b=CT^x$、$u2^av2^c=DZ\_B1^x$、かつ$u2^bv2^d=EZ_B2^x$である場合、第1の量および第2の量が同じであると決定され、第1の乱数および第2の乱数が同じであると決定され、$T=g^rh^t$が残高移動の量のコミットメント値であり、$Z\_B1=u2^rv2^{z1}$、$Z_B2=u2^tv2^{z2}$であり、z1およびz2が、確率論的HEスキームに基づいて、残高移動の第2の量および第2の乱数を暗号化するために使用される乱数である。第1のアカウントの残高および第2のアカウントの残高を更新することが、HEに基づいて実行される。

【０００９】

本開示はまた、1つまたは複数のプロセッサによって実行されると、本明細書で提供される方法の実装形態に従って1つまたは複数のプロセッサに動作を実行さ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る1つまたは複数の非一時的コンピュータ可読記憶媒体を提供する。

【００１０】

本開示はさらに、本明細書で提供される方法を実施するためのシステムを提供する。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って動作を実行さ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るコンピュータ可読記憶媒体とを含む。

【００１１】

本開示による方法は、本明細書で説明される態様および特徴の任意の組合せを含み得ることを理解されたい。すなわち、本開示による方法は、本明細書で特に説明される態様および特徴の組合せに限定されず、提供される態様および特徴の任意の組合せも含む。

【００１２】

本開示の1つまたは複数の実装形態の詳細は、添付の図面および以下の説明に記載される。本開示の他の特徴および利点が、説明および図面から、ならびに特許請求の範囲から明らかになるであろう。

【図面の簡単な説明】

【００１３】

【図１】本開示の実装形態を実行するために使用され得る例示的な環境の図である。

【図２】本開示の実装形態による例示的な概念のアーキテクチャの図である。

【図３】本開示の実装形態による、準同型暗号に基づくブロックチェーントランザクションのプライバシーが保護された承認の例示的な方法の図である。

【図４】本開示の実装形態による、準同型暗号に基づく例示的なブロックチェーントランザクションの図である。

【図５】本開示の実装形態による、準同型暗号に基づくブロックチェーントランザクションのプライバシーが保護された承認の別の例示的な方法の図である。

【図６】本開示の実装形態による、準同型暗号に基づく別の例示的なブロックチェーント

ランザクションの図である。
【図７】本開示の実装形態に従って実行され得る例示的なプロセスの図である。
【図８】本開示の実装形態に従って実行され得る別の例示的なプロセスの図である。
【発明を実施するための形態】
【００１４】
様々な図における同様の参照記号は同様の要素を示す。
【００１５】
本開示の実装形態は、ユーザによる確認、対話、およびトランザクション量またはアカウント残高の暴露を伴わない、ブロックチェーントランザクションのプライバシーが保護された検証のための、コンピュータ実装方法を含む。より具体的には、本開示の実装形態は、トランザクション量、アカウント残高、または他のブロックチェーンノードへのコミットメントを生成するための乱数を明らかにすることなく、コミットメントスキームおよび準同型暗号(HE)に基づいて、ブロックチェーンユーザ間のトランザクションを承認することを対象とする。
【００１６】
本開示の、および上で紹介された実装形態のさらなる背景を提供すると、コンセンサスネットワーク(たとえば、ピアツーピアノードからなる)、分散型台帳システム、または単にブロックチェーンとも呼ばれ得る、ブロックチェーンネットワークは、参加するエンティティが安全かつ変更不可能にトランザクション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、パブリックブロックチェーン、プライベートブロックチェーン、またはコンソーシアムブロックチェーンとして提供され得る。本開示の実装形態は、参加するエンティティの間で公開されているパブリックブロックチェーンに関して、本明細書でさらに詳細に説明される。しかしながら、本開示の実装形態はあらゆる適切なタイプのブロックチェーンにおいて実現され得ることが企図される。
【００１７】
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。たとえば、数百、数千、さらには数百万ものエンティティがパブリックブロックチェーンに参加することができ、それらの各々がパブリックブロックチェーンの中の少なくとも1つのノードを運用する。したがって、パブリックブロックチェーンは、参加するエンティティに関して公開のネットワークであると見なされ得る。いくつかの例では、ブロックが有効となりブロックチェーンに追加されるには、過半数のエンティティ(ノード)がそれぞれのブロックに署名しなければならない。例示的なパブリックブロックチェーンには、ピアツーピア支払ネットワーク(暗号通貨ネットワーク)であるビットコインネットワークにおいて使用されるブロックチェーンがある。ブロックチェーンという用語は一般にビットコインネットワークに関して言及されるが、本明細書では、ブロックチェーンは、ビットコインネットワークに特に言及することなく分散型台帳を全般的に指す。
【００１８】
一般に、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すべてと共有され、ブロックチェーン台帳はすべてのノードにわたって複製される。すなわち、すべてのノードがブロックチェーンに関して完全にコンセンサスのとれた状態にある。コンセンサス(たとえば、ブロックチェーンへのブロックの追加に対する合意)を達成するために、ブロックチェーンネットワーク内でコンセンサスプロトコルが実装される。例示的なコンセンサスプロトコルには、限定はされないが、ビットコインネットワークにおいて実装されるプルーフオブワーク(POW)がある。
【００１９】
本開示の実装形態は、上記の背景に鑑みてここでさらに詳細に説明される。より具体的には、上で紹介されたように、本開示の実装形態は、トランザクション量、アカウント残高、または他のブロックチェーンノードへのコミットメントを生成するための乱数を明ら

かにすることなく、コミットメントスキームおよびHEに基づいて、ブロックチェーンユーザ間のトランザクションを承認することを対象とする。

【００２０】

本開示の実装形態によれば、ブロックチェーントランザクションは、トランザクションアカウント残高、トランザクション量、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承認されブロックチェーン(台帳)に記録され得る。乱数を使用してトランザクション量のコミットメントを生成するために、ペダーセンコミットメント(PC)などのコミットメントスキームが使用され得る。トランザクション量および乱数は、確率的(probabilistic)または決定論的(deterministic)HEを使用して暗号化され得る。トランザクション量および乱数はまた、HEの性質に基づいてトランザクションを承認するためのプルーフとしての値のセットを生成するために使用され得る。トランザクションのコミットメント、暗号化されたトランザクション量、暗号化された乱数、およびプルーフは、アカウント残高、トランザクション量、または乱数が明らかにされることなくトランザクション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され得る。

【００２１】

図1は、本開示の実装形態を実行するために使用され得る例示的な環境100を図示する。いくつかの例では、例示的な環境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。例示的な環境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。いくつかの例では、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、またはこれらの組合せを含み、ウェブサイト、ユーザデバイス(たとえば、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。いくつかの例では、ネットワーク110は有線および/またはワイヤレス通信リンクを通じてアクセスされ得る。

【００２２】

図示される例では、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の中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み得る。例示的なコンピューティングデバイスには、限定はされないが、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ある。いくつかの例では、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で実施されるサービスをホストする。たとえば、コンピューティングシステム106は、第1のエンティティ(たとえば、ユーザA)が1つまたは複数の他のエンティティ(たとえば、他のユーザ)とのトランザクションを管理するために使用するトランザクション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で実施されるサービスをホストすることができる。コンピューティングシステム108は、第2のエンティティ(たとえば、ユーザB)が1つまたは複数の他のエンティティ(たとえば、他のユーザ)とのトランザクションを管理するために使用するトランザクション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で実施されるサービスをホストすることができる。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され、コンピューティングシステム106、108はそれぞれ、パブリックブロックチェーン102に参加する第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する。

【００２３】

図2は、本開示の実装形態による例示的な概念のアーキテクチャ200を図示する。例示的な概念のアーキテクチャ200は、エンティティレイヤ202、ホストされたサービスレイヤ204、およびパブリックブロックチェーンレイヤ206を含む。図示される例では、エンティティレイヤ202は、Entity_1(E1)、Entity_2(E2)、およびEntity_3(E3)という3つのエンティティを含み、各エンティティがそれぞれのトランザクション管理システム208をもつ。

【００２４】

図示される例では、ホストされるサービスレイヤ204は、各トランザクション管理シス

テム208のためのブロックチェーンインターフェース210を含む。いくつかの例では、それぞれのトランザクション管理システム208は、通信プロトコル(たとえば、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(たとえば、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ーフェース210と通信する。いくつかの例では、各ブロックチェーンインターフェース210は、それぞれのトランザクション管理システム208とブロックチェーンレイヤ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ーフェース210は、それぞれのエンティティがブロックチェーンレイヤ206のブロックチェーンネットワーク212に記録されるトランザクションを行うことを可能にする。いくつかの例では、ブロックチェーンインターフェース210とブロックチェーンレイヤ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。いくつかの例では、ブロックチェーンインターフェース210は、それぞれのトランザクション管理システム208のためのブロックチェーンノードを「ホスト」する。たとえば、ブロックチェーンインターフェース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にアプリケーションプログラミングインターフェース(API)を提供する。

【００２５】

本明細書で説明されるように、ブロックチェーンネットワーク212は、ブロックチェーン216に情報を変更不可能に記録する複数のノード214を含む、ピアツーピアネットワークとして提供される。単一のブロックチェーン216が概略的に図示されるが、ブロックチェーン216の複数のコピーが提供され、ブロックチェーン212にわたって維持される。たとえば、各ノード214はブロックチェーン216のコピーを記憶する。いくつかの実装形態では、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の間で実行されるトランザクションと関連付けられる情報を記憶する。

【００２６】

図3は、本開示の実装形態による、HEに基づくブロックチェーントランザクションのプライバシーが保護された承認の例示的な方法300を図示する。高水準において、例示的な方法300が、ユーザノードA302、ユーザノードB(図3に示されない)、およびコンセンサスノード(Consensus Node)とも呼ばれるブロックチェーンノード304によって実行される。価値の移動などのトランザクションが、ユーザノードA302からユーザノードBへ行われ得る。アカウントのプライバシーを保護するために、ユーザノードA302は、乱数rに基づいて、PCなどのコミットメントスキームを使用してトランザクション量tのコミットメントを生成することができる。PCを使用して生成されるコミットメントは、PC(r,t)として表現され得る。ユーザノードA302はまた、ユーザノードBの公開鍵に基づくHEを使用して乱数を暗号化することができる。これはHE(r)として表現され得る。(PC(r,t),HE(r))として表現される、トランザクション量tの暗号文がユーザノードBに送信され得る。暗号文を受信した後で、ユーザノードBは秘密鍵を使用して乱数rを復号することができる。ユーザノードBは、トランザクション量tを復号するために乱数rを使用することができる。トランザクションの有効性を証明するために、ブロックチェーンノード304は、コミットメントの中の乱数を、HEを使用して暗号化された乱数と比較することができる。これらの乱数が一致する場合、トランザクションは、トランザクションデータの知識なしでブロックチェーンノード304によって有効であると決定される。例示的な方法300のさらなる詳細が図3の以下の説明において論じられる。

【００２７】

306において、ユーザノードA302は、第1の乱数に基づいてトランザクション量のコミットメント値を生成し、HEに基づいてユーザノードA302の公開鍵を使用して第2の乱数を暗号化し、ユーザノードBの公開鍵を使用して第3の乱数を暗号化する。第1の乱数、第2の乱数、および第3の乱数は、コミットメントスキームを使用してトランザクション量tのコミットメントを生成するために使用されるのと同じ乱数rであり得る。いくつかの実装形態では、コミットメントスキームは、PCなどの二重指数形式を有し得る。非限定的な例としてPCを使用すると、第1の乱数rによって生成されるコミットメント値を$PC(r,t)=g^r h^t$として表現することができ、ここでgおよびhは楕円曲線のジェネレータであってよく、PC(r,t

)は曲線点のスカラー乗算であり、tはコミットされるトランザクション量である。岡本-内山(OU)HEおよびBoneh-Goh-Nissim HEなどのHEに基づく他のコミットメントスキームも、コミットメント値を生成するために使用され得ることを理解されたい。

【００２８】

ユーザノードA302の公開鍵を使用して暗号化される第2の乱数rの暗号化は、HE_A(r)と表現され得る。ユーザノードBの公開鍵を使用して暗号化される第3の乱数rの暗号化は、HE_B(r)と表現され得る。

【００２９】

いくつかの実装形態では、公開鍵HE暗号は、乱数をある一定の値に設定することによって、Paillier HE、Benaloh HE、OU HE、Naccache-Stern HE、Damgard-Jurik HE、またはBoneh-Goh-Nissim HEなどの確率論的HEスキームから得ることができる決定論的HEであり得る。いくつかの実装形態では、HE(a+b)=HE(a)+HE(b)かつHE(ab)=HE(b)^{a}という線形の性質を満たし、aおよびbがHEのために使用されるプレーンテキストである決定論的HEスキームが、本開示のために使用され得る。

【００３０】

いくつかの例では、T=PC(r,t)、T'=HE_A(r)、かつT''=HE_B(r)であり、トランザクション量の暗号文は(T,T',およびT'')として表現され得る。例示的な条件が満たされる場合、トランザクションは有効であると決定され得る。第1に、トランザクション量tが0以上であり、ユーザノードA302のアカウント残高s_A以下である。第2に、トランザクションがユーザノードA302によって認可されることを証明するために、トランザクションがユーザノードA302の秘密鍵によってデジタル署名される。第3に、コミットメントPC(r,t)の中の乱数rが、それぞれユーザノードA302およびユーザノードBの公開鍵を使用して暗号文HE_A(r)およびHE_B(r)において暗号化されるrと同じである。

【００３１】

いくつかの実装形態では、暗号文はまた、(PC(r',t'),HE_A(r'))として表現され得る送信される量(t')の暗号文、および(PC(r'',t''),HE_B(r''))として表現され得る受信される量(t'')の暗号文として分離され得る。そのような場合、送信される量t'はまた、トランザクションを承認するために、受信される量t'と同じであると決定される必要がある。

【００３２】

308において、ユーザノードA302は、1つまたは複数のレンジプルーフを生成する。いくつかの実装形態では、レンジプルーフは、トランザクション量tが0以上であることを示すためのレンジプルーフRP1と、トランザクション量tがユーザノードAのアカウント残高以下であることを示すためにレンジプルーフRP2とを含み得る。

【００３３】

310において、ユーザノードA302は、1つまたは複数の選択された乱数に基づいてHEを使用して値のセットを生成する。Pfと表記される値のセットは、コミットメントPC(r,t)の中の乱数rが、それぞれユーザノードA302およびユーザノードBの公開鍵を使用して暗号文HE_A(r)およびHE_B(r)において暗号化されるrと同じであることを証明するために使用される、プルーフを含み得る。いくつかの実装形態では、2つの乱数r1およびt1を、(T1,T1',T1'')として表記されるt1の暗号文の別のセットを計算するために選択することができ、ここでT1=$g^{r1}h^{t1}$、T1'=HE_A(r1)、T1''=HE_B(r1)である。2つの追加のプルーフr2およびt2を、r2=r1+xr、t2=t1+xtとして計算することができ、ここでxはT1、T1'、およびT1''のハッシュである。値のセットはPf=(T1,T1',T1'',r2,t2)と表記され得る。

【００３４】

312において、ユーザノードA302は、暗号文(T,T',T'')、暗号文(T1,T1',T1'')、r2、t2、レンジプルーフRP1およびRP2、ならびにユーザノードA302およびユーザノードBの公開鍵をデジタル署名するために、その秘密鍵を使用する。ユーザノードA302によって追加されるデジタル署名は、ユーザノードA302によってトランザクションが認可されることを示すために使用され得る。デジタル署名されるコピーは、314においてブロックチェーンネットワークに提出される。

【００３５】
316において、ブロックチェーンノード304は、ユーザノードA302の公開鍵を使用してデジタル署名を検証する。ブロックチェーンノード304は、ブロックチェーンネットワークにおけるトランザクションの有効性を証明できるコンセンサスノードであり得る。ブロックチェーンノード304が公開鍵を使用してユーザノードA302のデジタル署名を検証できない場合、デジタル署名は正しくないと決定することができ、トランザクションを拒否することができる。いくつかの実装形態では、ブロックチェーンノード304は、二重使用防止機構も含み得る。ブロックチェーンノード304は、トランザクションがすでに実行または記録されているかどうかを検証することができる。トランザクションがすでに実行されている場合、トランザクションは拒絶され得る。それ以外の場合、トランザクションの承認は進行することができる。

【００３６】
318において、ブロックチェーンノード304は、1つまたは複数のレンジプルーフを検証する。たとえば、レンジプルーフRP1を、トランザクション量tが0以上であることを証明するために使用することができ、レンジプルーフRP2を、トランザクション量tがユーザノードA302のアカウント残高以下であることを証明するために使用することができる。

【００３７】
320において、ブロックチェーンノード304は、値のセットに基づいて、第1の乱数、第2の乱数、および第3の乱数が同じであると決定する。いくつかの実装形態では、この決定は、上で論じられたように、例示的な条件$g^{r_2}h^{t_2}=T^{x}T1$、HE_A(r2)=T'^{x}T1'、およびHE_B(r2)=T''^{x}T1''が真であるかどうかを、決定論的HEの性質に基づいて決定することを含む。真である場合、コミットメントの中の乱数は、ユーザノードA302およびユーザノードBの公開鍵を使用して準同型暗号化される乱数と同じであり、トランザクションが有効であることが示され得る。

【００３８】
322において、ブロックチェーンノード304は、ユーザノードA302およびユーザノードBのアカウント残高を更新する。残高更新は、ユーザノードA302またはユーザノードBのいずれのアカウント残高も明らかにすることなく、HEの性質に基づいて実行され得る。アカウント残高の更新は、図4に関して本明細書でさらに詳細に説明される。

【００３９】
図4は、本開示の実装形態による、HEに基づく例示的なブロックチェーントランザクション400を図示する。例示的なブロックチェーントランザクション400において示されるように、ユーザノードA402はトランザクション量tをユーザノードB406に移す。トランザクションの前、ユーザノードA402はs_Aというアカウント残高を有し、ユーザノードB406はs_Bというアカウント残高を有する。

【００４０】
例として図3を参照して本明細書で説明される暗号化スキームおよびトランザクションプロセスを使用すると、PCに基づく乱数r_Aを使用してアカウント残高s_Aを暗号化することができ、HEに基づいて乱数r_Aを暗号化することができる。アカウント残高s_Aの暗号文を、$(S_A,S'_A)=(g^{r-A}h^{s-A},HE_A(r_A))$として表現することができ、ここでgおよびhはアカウント残高s_AのPCを生成するための楕円曲線のジェネレータであり得る。同様に、ユーザノードB406のアカウント残高s_Bは、PCに基づく乱数r_Bを使用して暗号化され得る。アカウント残高s_Bの暗号文は、$(S_B,S'_B)=(g^{r-B}h^{s-B},HE_A(r_B))$として表現され得る。

【００４１】
404において、ユーザノードA402は、トランザクションを承認するために使用されるプルーフにデジタル署名を追加し、ブロックチェーンネットワーク408にデジタル署名されたコピーを提出することができる。図3を参照して上で説明されたように、プルーフは、トランザクション量の暗号文(T,T',T'')、1つまたは複数のレンジプルーフ(RP1,RP2)、および他のプルーフ(T1,T1',T1'',r2,t2)を含み得る。

【００４２】

トランザクションの後、ユーザノードA402のアカウント残高をs_A-t'として表現することができ、ユーザノードB406のアカウント残高をs_B+t''として表現することができ、ここでt'はユーザノードA402によって送信される量であり、t''はユーザノードBによって受信される量である。トランザクションの後のユーザノードA402のアカウント残高の暗号文を(S_A/T,S'_A/T')として表現することができ、トランザクションの後のユーザノードB406のアカウント残高の暗号文を(S_B*T,S'_B*T'')として表現することができる。S_A、S'_A、S_B、S'_B、T、T'、T''は各々、二重指数形式のHEを使用して暗号化され、加算および減算はプレーンテキスト値に対する復号を伴わずに、暗号化された形式で実行され得る。

【００４３】

図5は、本開示の実装形態による、HEに基づくブロックチェーントランザクションのプライバシーが保護された承認の別の例示的な方法500を図示する。高水準において、例示的な方法500は、ユーザノードA502、ユーザノードB(図5に示されない)、およびコンセンサスノードと呼ばれ得るブロックチェーンノード504によって実行される。価値の移動などのトランザクションが、ユーザノードA502からユーザノードBへ行われ得る。アカウントのプライバシーを保護するために、ユーザノードA502は、乱数rに基づくPCなどのコミットメントスキームを使用して、トランザクション量tのコミットメントを生成することができる。PCを使用して生成されるコミットメントは、PC(r,t)として表現され得る。ユーザノードA502はまた、OUなどの二重指数形式を有するHEを使用して、トランザクション量tおよび乱数rを暗号化することができる。

【００４４】

トランザクション量tの暗号文は、ブロックチェーンネットワークに提出され得る。暗号文を受信した後で、ブロックチェーンノード504は、PCに秘匿されている乱数rがOUにおいて暗号化される乱数rと一致するかどうかを、ユーザノードA502およびユーザノードBのそれぞれの公開鍵を使用して決定することができる。さらに、ブロックチェーンノード504は、PCに秘匿されているトランザクション量tがOUにおいて暗号化されるトランザクション量tと一致するかどうかを、ユーザノードA502およびユーザノードBのそれぞれの公開鍵を使用して決定することができる。乱数とトランザクション量の両方が一致する場合、トランザクションデータの知識なしで、トランザクションは有効であるとブロックチェーンノード504によって決定され得る。

【００４５】

506において、ユーザノードA502は、第1の乱数に基づいて第1のトランザクション量のコミットメント値を生成し、第1のトランザクション量および第1の乱数はユーザノードA502の公開鍵を使用して暗号化される。第2のトランザクション量および第2の乱数は、ユーザノードBの公開鍵を使用して暗号化される。第1のトランザクション量および第2のトランザクション量は同じ量tであり得る。第1の乱数および第2の乱数は、コミットメントスキームを使用してトランザクション量tのコミットメントを生成するために使用されるのと同じ乱数rであり得る。いくつかの実装形態では、コミットメントスキームは、PCなどの二重指数形式を有し得る。例としてPCを使用すると、第1の乱数rによって生成されるコミットメント値を$PC(r,t)=g^{r}h^{t}$として表現することができ、ここでgおよびhは楕円曲線のジェネレータであってよく、PC(r,t)は曲線点のスカラー乗算であり、tはコミットされるトランザクション量である。OU HEおよびBoneh-Goh-Nissim HEなどのHEに基づく他のコミットメントスキームも、コミットメント値を生成するために使用され得ることを理解されたい。

【００４６】

ユーザノードA502はまた、ユーザノードA502の公開鍵を使用して第1の乱数および第1のトランザクション量を暗号化し、ユーザノードBの公開鍵を使用して第2の乱数および第2のトランザクション量を暗号化することができる。いくつかの実装形態では、乱数およびトランザクション量の暗号化は、OUなどの確率論的HEに基づき得る。例としてOUを使用すると、ユーザノードA502の公開鍵を使用した第1の乱数および第1のトランザクション量の暗号化を、それぞれ$OU_A(r)=u1^{r}v1^{y1}$、$OU_A(t)=u1^{t}v1^{y2}$として表現することができ、ここ

でu1およびv1は楕円曲線のジェネレータであり、y1およびy2はOU_A(r)およびOU_A(t)を生成するために使用される乱数である。暗号化された第2の乱数および第2のトランザクション量を、それぞれOU_B(r)=u2^{r}v2^{z1}、OU_B(t)=u2^{t}v2^{z2}として表現することができ、ここでu2およびv2は楕円曲線のジェネレータであり、z1およびz2はそれぞれOU_B(r)およびOU_B(t)を生成するために使用される乱数である。確率論的OUはOU(a+b)=OU(a)*OU(b)という性質を満たし、ここでaおよびbはOUに使用されるプレーンテキストである。

【００４７】

トランザクション量tの暗号文は、(PC(r,t),OU_A(r),OU_A(t),OU_B(r),OU_B(t))として表現され得る。以下の例示的な条件が満たされる場合、トランザクションは有効であると決定され得る。第1に、トランザクション量tが0以上であり、ユーザノードA502のアカウント残高s_A以下である。第2に、トランザクションがユーザノードA502によって認可されることを証明するために、トランザクションがユーザノードA502の秘密鍵を使用してデジタル署名される。第3に、コミットメントPC(r,t)の中の乱数rが、それぞれユーザノードA502およびユーザノードBの公開鍵を使用して暗号文OU_A(r)およびOU_B(r)において暗号化されるrと同じである。第4に、コミットメントPC(r,t)の中のトランザクション量tが、それぞれユーザノードA502およびユーザノードBの公開鍵を使用して暗号文OU_A(r)およびOU_B(r)において暗号化されるtと同じである。

【００４８】

いくつかの実装形態では、暗号文はまた、(PC(r',t'),OU_A(r'),OU_A(t'))として表現され得る送信される量(t')の暗号文、および(PC(r'',t''),OU_B(r''),OU_B(t''))として表現され得る受信される量(t'')の暗号文として分離され得る。そのような場合、送信される量t'はまた、トランザクションを承認するために、受信される量t'に等しいと決定される必要がある。

【００４９】

508において、ユーザノードA502は、1つまたは複数のレンジプルーフを生成する。いくつかの実装形態では、レンジプルーフは、トランザクション量tが0以上であることを示すためのレンジプルーフRP1と、トランザクション量tがユーザノードAのアカウント残高以下であることを示すためにレンジプルーフRP2とを含み得る。

【００５０】

510において、ユーザノードA502は、1つまたは複数の選択された乱数に基づいてHEを使用して値のセットを生成する。Pfと表記される値のセットは、コミットメントPC(r,t)の中の乱数rが暗号文OU_A(r)およびOU_B(r)において暗号化されるrと同じであり、コミットメントPC(r,t)の中のトランザクション量tが暗号文OU_A(r)およびOU_B(r)において暗号化されるtと同じであることを証明するために使用される、プルーフを含み得る。いくつかの実装形態では、4つの乱数r*、t*、z1*、およびz2*を、(C,D,E)と表記される暗号文の別のセットを計算するために選択することができ、ここでC=g^{r*}h^{t*}、D=u2^{r*}v2^{z1*}およびE=u2^{t*}v2^{z2*}であり、g、h、u2、およびv2は楕円曲線のジェネレータである。4つの追加のプルーフa、b、c、およびdをa=r*+xr、b=t*+xt、c=z1*+xz1、およびd=z2*+xz2として計算することができ、xはg、h、u2、v2、C、D、およびEのハッシュ関数である。そうすると値のセットは、Pf=(C,D,E,a,b,c,d)と表記され得る。

【００５１】

512において、ユーザノードA502は、暗号文(PC(r,t),OU_A(r),OU_A(t),OU_B(r),OU_B(t))、レンジプルーフRP1およびRP2、ならびに値Pfのセットをデジタル署名するために、その秘密鍵を使用する。ユーザノードA502によって追加されるデジタル署名は、トランザクションがユーザノードA502によって認可されることを示すために使用され得る。デジタル署名されるコピーは、514においてブロックチェーンネットワークに提出される。

【００５２】

516において、ブロックチェーンノード504は、ユーザノードA502の公開鍵を使用してデジタル署名を検証する。ブロックチェーンノード504は、ブロックチェーンネットワーク上でトランザクションの有効性を証明できるコンセンサスノードであり得る。ブロックチ

ェーンノード504がユーザノードAの公開鍵を使用してデジタル署名を検証できない場合、デジタル署名は正しくないと決定することができ、トランザクションを拒否することができる。いくつかの実装形態では、ブロックチェーンノード504は、二重使用防止機構も含み得る。ブロックチェーンノード504は、トランザクションがすでに実行または記録されているかどうかを検証することができる。トランザクションがすでに実行されている場合、トランザクションは拒絶され得る。それ以外の場合、トランザクションの承認は進行することができる。

【００５３】

518において、ブロックチェーンノード504は、1つまたは複数のレンジプルーフを検証する。たとえば、レンジプルーフRP1を、トランザクション量tが0以上であることを証明するために使用することができ、レンジプルーフRP2を、トランザクション量tがユーザノードA502のアカウント残高以下であることを証明するために使用することができる。

【００５４】

520において、ブロックチェーンノード504は、第1のトランザクション量が第2のトランザクション量と同じであるかどうか、および第1の乱数が第2の乱数と同じであるかを、値のセットに基づいて決定する。いくつかの実装形態では、この決定は、$g^a h^b = CT^x$、$u2^a v2^c = DZ\_B1^x$、かつ$u2^b v2^d = EZ_B2^x$であるかどうかを決定することを含み、$T = g^r h^t$は第1のトランザクション量tのコミットメント値であり、$Z\_B1 = u2^r v2^{z1}$、$Z_B2 = u2^t v2^{z2}$であり、z1およびz2は確率論的HEスキームに基づいて第2のトランザクション量および第2の乱数を暗号化するために使用される乱数である。真である場合、コミットメントの中の乱数およびトランザクション量は、それぞれユーザノードA502およびユーザノードBの公開鍵を使用して準同型暗号化される乱数およびトランザクション量と同じであり、トランザクションが有効であることが示され得る。

【００５５】

522において、ブロックチェーンノード504は、ユーザノードA502およびユーザノードBのアカウント残高を更新する。アカウント残高更新は、ユーザノードA502および/またはユーザノードBのアカウント残高を明らかにすることなく、HEの性質に基づいて実行され得る。

【００５６】

図6は、本開示の実装形態による、HEに基づく別の例示的なブロックチェーントランザクション600を図示する。例示的なトランザクション600において示されるように、ユーザノードA602はトランザクション量tをユーザノードB606に移す。トランザクションの前、ユーザノードA602はs_Aというアカウント残高を有し、ユーザノードB606はs_Bというアカウント残高を有する。

【００５７】

いくつかの例では、アカウント残高s_Aは、図5を参照して本明細書で説明される暗号化スキームおよびトランザクションプロセスを使用して、PCに基づく乱数r_Aを使用して秘匿され得る。乱数r_Aおよびアカウント残高は、OUに基づいて暗号化され得る。アカウント残高s_Aの暗号文を、$(S_A, R_A, Q_A) = (g^{r_A} h^{s_A}, OU_A(r_A), OU_A(s_A))$として表現することができ、ここでgおよびhはアカウント残高s_AのPCを生成するための楕円曲線のジェネレータであり得る。同様に、ユーザノードB606のアカウント残高s_Bは、PCに基づく乱数r_Bを使用して暗号化され得る。アカウント残高s_Bの暗号文は、$(S_B, S'_B) = (g^{r_B} h^{s_B}, OU_B(r_B), OU_B(s_B))$として表現され得る。

【００５８】

604において、ユーザノードA602は、トランザクションを承認するために使用されるプルーフにデジタル署名を追加し、ブロックチェーンネットワーク608にデジタル署名されたコピーを提出することができる。図5を参照して本明細書で説明されたように、プルーフは、トランザクション量の暗号文$(PC(r,t), OU_A(r), OU_A(t), OU_B(r), OU_B(t))$、1つまたは複数のレンジプルーフ(RP1,RP2)、および他のプルーフ(C,D,E,a,b,c,d)を含み得る。

【００５９】

トランザクションの後、ユーザノードA602のアカウント残高をs_A-tとして表現することができ、ユーザノードB606のアカウント残高をs_B+tとして表現することができる。トランザクションの後のユーザノードA602のアカウント残高の暗号文を(S_A/T,R_A/Y_A1,Q_A/Y_A2)として表現することができ、ここでY_A1=OU_A(r)かつY_A2=OU_A(t)である。トランザクションの後のユーザノードB606のアカウント残高の暗号文を(S_B*T,R_B*Z_B1,Q_B*Z_B2)として表現することができ、ここでZ_B1=OU_B(r)かつZ_B2=OU_B(t)である。S_A、S_B、R_A、R_B、Q_A、Q_B、Y_A1、Y_A2、Z_B1、Z_B2、およびTは、二重指数形式のHEを使用して暗号化されるので、加算および減算はプレーンテキスト値を復号することなく、暗号化された形式で実行され得る。

【００６０】

図7は、本開示の実装形態に従って実行され得る例示的なプロセス700を図示する。提示を明確にするために、以下の説明は全般に、この説明では他の図面の文脈で方法700を説明する。しかしながら、例示的なプロセス700は、たとえば、任意のシステム、環境、ソフトウェア、およびハードウェア、またはシステム、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、適宜実行され得る。いくつかの実装形態では、例示的なプロセス700のステップは、並列に、組合せで、ループで、または任意の順序で行われ得る。

【００６１】

702において、コンセンサスノードは、第1のアカウントから、第1の乱数に基づいて生成される第1のアカウントから第2のアカウントへ移されるべきトランザクション量のコミットメント値のデジタル署名されたコピーを受信する。コンセンサスノードはまた、第1のアカウントから、第1のアカウントの公開鍵を使用して暗号化される第2の乱数、第2のアカウントの公開鍵を使用して暗号化される第3の乱数、1つまたは複数のレンジプルーフ、および1つまたは複数の選択された乱数に基づくHEを使用して生成される値のセットを受信することができる。いくつかの実装形態では、コミットメント値は、コミットメントスキームに基づくHEを使用して生成される。いくつかの実装形態では、第2の乱数および第3の乱数は、決定論的HEスキームに基づいて暗号化される。

【００６２】

いくつかの実装形態では、値のセットは(T1,T1',T1'',r2,t2)によって表現され、ここでr2=r1+xr、t2=t1+xtであり、r1およびt1は1つまたは複数の選択された乱数を表し、rは第1の乱数を表し、tは残高移動の量を表す。いくつかの例では、$T1=g^{r1}h^{t1}$、T1'=HE_A(r1)、T1''=HE_B(r1)であり、ここでgおよびhは楕円曲線のジェネレータであり、HE_A(r1)は第1のアカウントの公開鍵を使用してr1のHEに基づいて生成され、HE_B(r1)は第2のアカウントの公開鍵を使用してr1のHEに基づいて生成される。いくつかの例では、xはT1、T1'、およびT1''をハッシュ化することに基づいて生成される。

【００６３】

704において、コンセンサスノードは、デジタル署名されたコピーに対応するデジタル署名を、デジタル署名を生成するために使用される秘密鍵に対応する第1のアカウントの公開鍵を使用して検証する。

【００６４】

706において、コンセンサスノードは、残高移動の量が0より大きく、かつ第1のアカウントの残高以下であることを、1つまたは複数のレンジプルーフが証明するかどうかを決定する。

【００６５】

708において、コンセンサスノードは、値のセットに基づいて、第1の乱数、第2の乱数、および第3の乱数が同じであるかどうかを決定する。いくつかの実装形態では、第1の乱数、第2の乱数、および第3の乱数は、$g^{r2}h^{t2}=T^{x}T1$、$HE\_A(r2)=T'^{x}T1'$、かつ$HE_B(r2)=T''^{x}T1'$である場合同じであると決定され、ここで$T=g^{r}h^{t}$は残高移動の量のコミットメント値であり、T'=HE_A(r)であり、かつT''=HE_B(r)であり、HE_A(r)は第1のアカウントの公開鍵を使用してrのHEに基づいて生成され、HE_B(r)は第2のアカウントの公開鍵を使用してrのHEに基づいて生成され、HE_A(r2)は第1のアカウントの公開鍵を使用してr2のHEに基づ

いて生成され、HE_B(r2)は第2のアカウントの公開鍵を使用してr2のHEに基づいて生成され、xはg、h、T1、T1'、およびT1''をハッシュ化することに基づいて生成される。いくつかの実装形態では、T、T'、およびT''は、トランザクション量tの量の暗号文を形成する。

【００６６】

710において、コンセンサスノードは、第1の乱数、第2の乱数、および第3の乱数が同じである場合、トランザクション量に基づいて第1のアカウントの残高および第2のアカウントの残高を更新する。いくつかの実装形態では、第1のアカウントの残高および第2のアカウントの残高を更新することはHEに基づいて実行される。

【００６７】

図8は、本開示の実装形態に従って実行され得る別の例示的なプロセス800を図示する。提示を明確にするために、以下の説明は全般に、この説明では他の図面の文脈で例示的なプロセス800を説明する。しかしながら、例示的なプロセス800は、たとえば、任意のシステム、環境、ソフトウェア、およびハードウェア、またはシステム、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、適宜実行され得る。いくつかの実装形態では、例示的なプロセス800のステップは、並列に、組合せで、ループで、または任意の順序で行われ得る。

【００６８】

802において、コンセンサスノードは、第1のアカウントから、第1のアカウントから第2のアカウントへ移動する第1のトランザクション量のコミットメント値のデジタル署名されたコピーを受信する。いくつかの例では、コミットメント値のデジタル署名されたコピーは、第1の乱数に基づいて生成される。コンセンサスノードはまた、第1のアカウントの公開鍵を使用して暗号化される第1のトランザクション量および第1の乱数、第2のアカウントの公開鍵を使用して暗号化される残高移動の第2の量および第2の乱数、1つまたは複数のレンジプルーフ、ならびに1つまたは複数の選択された乱数に基づくHEを使用して生成される値のセットを受信する。いくつかの実装形態では、コミットメント値はPCスキームを使用して生成される。いくつかの実装形態では、残高移動の第1の量および第1の乱数は、確率論的HEアルゴリズムに基づいて第1のアカウントの公開鍵を使用して暗号化される。いくつかの例では、残高移動の第2の量および第2の乱数は、確率論的HEアルゴリズムに基づいて第2のアカウントの公開鍵を使用して暗号化される。いくつかの実装形態では、確率論的HEアルゴリズムは岡本-内山HEアルゴリズムである。

【００６９】

いくつかの実装形態では、値のセットは(C,D,E,a,b,c,d)によって表現され、ここでa=r*+xr、b=t*+xt、c=z1*+xz1、かつd=z2*+xz2であり、r*、t*、z1*、およびz2*は1つまたは複数の選択された乱数を表し、rは第1の乱数を表し、tは残高移動の第1の量を表し、$C=g^{r^*}h^{t^*}$、$D=u2^{r^*}v2^{z1^*}$、$E=u2^{t^*}v2^{z2^*}$であり、g、h、u2、およびv2は楕円曲線のジェネレータであり、xはC、D、およびEをハッシュ化することに基づいて生成される。

【００７０】

804において、コンセンサスノードは、デジタル署名されたコピーに対応するデジタル署名を、デジタル署名を生成するために使用される秘密鍵に対応する第1のアカウントの公開鍵を使用して検証する。

【００７１】

806において、コンセンサスノードは、残高移動の量が0より大きく、かつ第1のアカウントの残高以下であることを、1つまたは複数のレンジプルーフが証明するかどうかを決定する。

【００７２】

808において、コンセンサスノードは、第1の量が第2の量と同じであるかどうか、および第1の乱数および第2の乱数が同じであるかを、値のセットに基づいて決定する。いくつかの実装形態では、$g^ah^b=CT^x$、$u2^av2^c=DZ\_B1^x$、かつ$u2^bv2^d=EZ_B2^x$である場合、第1の量および第2の量は同じであると決定され、第1の乱数および第2の乱数は同じであると決定

され、ここでT=$g^r h^t$は残高移動の量のコミットメント値であり、Z_B1=$u2^r v2^{z1}$、Z_B2=$u2^t v2^{z2}$である。いくつかの例では、z1およびz2は、第2のトランザクション量を暗号化するために使用される乱数および確率論的HEスキームに基づく第2の乱数である。

【００７３】

810において、コンセンサスノードは、第1の量および第2の量が同じであり、第1の乱数および第2の乱数が同じである場合、残高移動の第1の量に基づいて第1のアカウントの残高および第2のアカウントの残高を更新する。いくつかの実装形態では、第1のアカウントの残高および第2のアカウントの残高を更新することはHEに基づいて実行される。

【００７４】

本明細書で説明される主題の実装形態は、特定の利点または技術的な効果を実現するように実装され得る。たとえば、本開示の実装形態は、アカウント残高およびブロックチェーンノードのトランザクション量がトランザクションの間に非公開であることを可能にする。資金移動の受領者は、トランザクションを確認すること、またはコミットメントを検証するために乱数を使用することが必要ではなく、トランザクションの承認は非相互的であり得る。ブロックチェーンノードは、HEおよびコミットメントスキームに基づいてトランザクションを承認して、知識なしのプルーフを可能にできる。

【００７５】

説明される方法は、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向上を可能にする。アカウントの残高およびトランザクション量は、HEに基づいて暗号化され、コミットメントスキームによって秘匿され得る。したがって、コンセンサスノードは、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の性質に基づいてトランザクションの後の台帳のアカウント残高を更新することができる。トランザクションを確認するために乱数を受領者に送信する必要がないので、データ漏洩のリスクを減らすことができ、乱数を管理するために使用することが必要なコンピューティングリソースおよびメモリリソースがより少なくなる。

【００７６】

本明細書で説明される実装形態および動作は、本明細書で説明される構造もしくはそれらのうちの1つまたは複数の組合せを含めて、デジタル電子回路で、または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実装され得る。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る、または他のソースから受信されるデータに対して、データ処理装置によって実行される動作として実施され得る。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、前述の1つのプログラマブルプロセッサ、1つのコンピュータ、1つのシステムオンチップ、またはこれらの複数、または組合せを例として含む、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得る。装置は、専用論理回路、たとえば、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)を含み得る。装置はまた、対象のコンピュータプログラムのための実行環境を作り出すコード、たとえば、プロセッサファームウェア、プロトロルスタック、データベース管理システム、オペレーティングシステム(たとえば、1つのオペレーティングシステムまた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ランタイム環境、仮想マシン、またはこれらの1つまたは複数の組合せを構成するコードを含み得る。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することができる。

【００７７】

コンピュータプログラム(たとえば、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、コンパイル型またはインタプリタ型言語、宣言型または手続き型言語を含む、任意の形式のプログラミング言語で書かれてよく、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において使用するのに適した他のユニットを含む、任意の形式で展開されてよい。プログラムは、他のプログラムもしくはデータ(たとえば、マークアップ言語ドキュメントに記憶される1つまたは複数のスクリプト)を保持するファイルの一部分、対象のプログラムに専用の単一のファイル、または複数の協調的なファイル(たとえば、1つまたは複数のモジュール、サブプログラム、またはコードの部分を記憶するファイル)に記憶され得る。コンピュータプログラムは、1つの場所に位置する、または、複数の場所に分散され通信ネットワークによって相互接続される、1つのコンピュータまたは複数のコンピュータ上で実行され得る。

【００７８】

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、汎用マイクロプロセッサと専用マイクロプロセッサの両方、および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、読取り専用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信する。コンピュータの不可欠な要素は、命令に従って活動を実行するためのプロセッサ、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、データを記憶するための1つまたは複数のマスストレージデバイスも含み、または、そのマスストレージデバイスからデータを受信し、もしくはそこへデータを移し、もしくはその両方を行うように、動作可能に結合される。コンピュータは、別のデバイス、たとえば、モバイルデバイス、携帯情報端末(PDA)、ゲームコンソール、全地球測位システム(GPS)受信機、またはポータブル記憶デバイスに埋め込まれ得る。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したデバイスは、例として、半導体メモリデバイス、磁気ディスク、および磁気光学ディスクを含む、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、専用の論理回路によって補完されても、またはそれに組み込まれてもよい。

【００７９】

モバイルデバイスは、ハンドセット、ユーザ機器(UE)、携帯電話(たとえば、スマートフォン)、タブレット、ウェアラブルデバイス(たとえば、スマートウォッチおよびスマート眼鏡)、人体に埋め込まれたデバイス(たとえば、バイオセンサ、人工内耳)、または他のタイプのモバイルデバイスを含み得る。モバイルデバイスは、様々な通信ネットワーク(以下で説明される)にワイヤレスに(たとえば、高周波(RF)信号を使用して)通信することができる。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決定するためのセンサを含み得る。センサは、カメラ、マイクロフォン、近接センサ、GPSセンサ、モーションセンサ、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(たとえば、Wi-Fiおよびセルラー無線)、温度センサ、または他のタイプのセンサを含み得る。たとえば、カメラは、可動レンズまたは固定レンズ、フラッシュ、イメージセンサ、およびイメージプロセッサを伴う、前面カメラまたは後面カメラを含み得る。カメラは、顔認識および/または虹彩認識のための詳細を捉えることが可能なメガピクセルカメラであり得る。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リモートでアクセスされる認証情報とともに、顔認識システムを形成することができる。顔認識システムまたは1つまたは複数のセンサ、たとえば、マイクロフォン、モーションセンサ、加速度計、GPSセンサ、またはRFセンサは、ユーザ認証のために使用され得る。

【００８０】

ユーザとの対話を提供するために、実装形態は、ディスプレイデバイスおよび入力デバイス、たとえば、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、ユーザがそれによって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、コンピュータ上で実装され得る。他の種類のデバイスも、ユーザとの対話を提供するために使用され得る。たとえば、ユーザに提供されるフィードバックは任意の種類の感覚的なフィードバック、たとえば視覚的なフィードバック、聴覚的な

フィードバック、または触覚的なフィードバックであってよく、ユーザからの入力は、音響入力、発話入力、または触覚入力を含む、任意の形式で受け取られ得る。加えて、コンピュータは、ドキュメントを送信してユーザによって使用されるデバイスからドキュメントを受信することによって、たとえば、ウェブブラウザから受信された要求に応答してユーザのクライアントデバイス上の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、ユーザと対話することができる。

【００８１】

実装形態は、有線またはワイヤレスデジタルデータ通信(またはそれらの組合せ)の任意の形式もしくは媒体、たと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され得る。相互接続されたデバイスの例は、一般に互いから離れており典型的には通信ネットワークを介して対話する、クライアントおよびサーバである。クライアント、たとえばモバイルデバイスは、たとえば、購入、売却、支払、贈与、送付、もしくは貸付のトランザクションの実行、またはこれらの認可を行うサーバと、またはサーバを通じて、自身でトランザクションを実行することができる。そのようなトランザクションは、活動と応答が時間的に近くなるようにリアルタイムであり得る。たとえば、ある個人は、活動および応答が実質的に同時に発生することを知覚し、その個人の活動に続く応答の時間差が1ミリ秒(ms)未満もしくは1秒(s)未満であり、または応答にシステムの処理制約を考慮した意図的な遅延がない。

【００８２】

通信ネットワークの例は、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)を含む。通信ネットワークは、インターネット、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の、すべてもしくは一部分を含み得る。情報は、Long Term Evolution(LTE)、5G、IEEE 802、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む、様々なプロトコルおよび規格に従って通信ネットワーク上で送信され得る。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、音声データ、ビデオデータ、バイオメトリックデータ、または認証データ、または他の情報を送信することができる。

【００８３】

別個の実装形態として説明される特徴は、組合せで、単一の実装形態で実装され得るが、単一の実装形態として説明される特徴は、複数の実装形態で、別々に、または任意の適切な部分組合せで実装され得る。特定の順序で説明され特許請求される動作は、特定の順序が実行されなければならないこと、またはすべての図示される動作が実行されなければならないことを要求するものとして理解されるべきではない(いくつかの動作は任意選択であり得る)。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と並列処理の組合せ)が実行され得る。

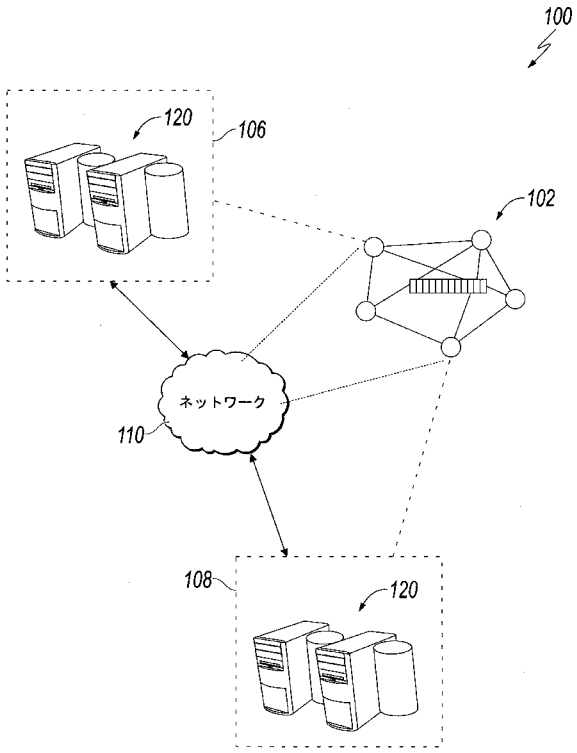
【符号の説明】

【００８４】

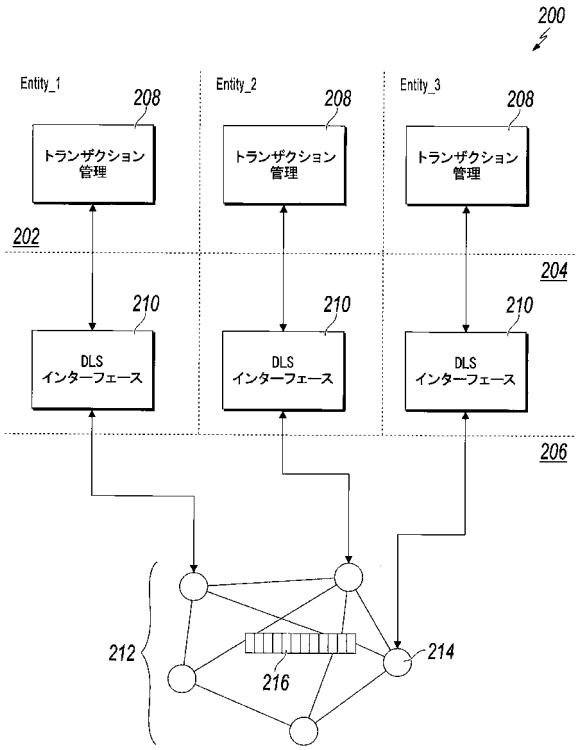
100 例示的な環境
102 パブリックブロックチェーン
106 コンピューティングシステム
108 コンピューティングシステム
110 ネットワーク
202 エンティティレイヤ
204 ホストされたサービスレイヤ
206 パブリックブロックチェーンレイヤ
208 トランザクション管理システム
210 ブロックチェーンインターフェース
212 ブロックチェーンネットワーク
214 ノード

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
406　ユーザノードB
408　ブロックチェーンネットワーク
502　ユーザノードA
504　ブロックチェーンノード
608　ブロックチェーンネットワーク

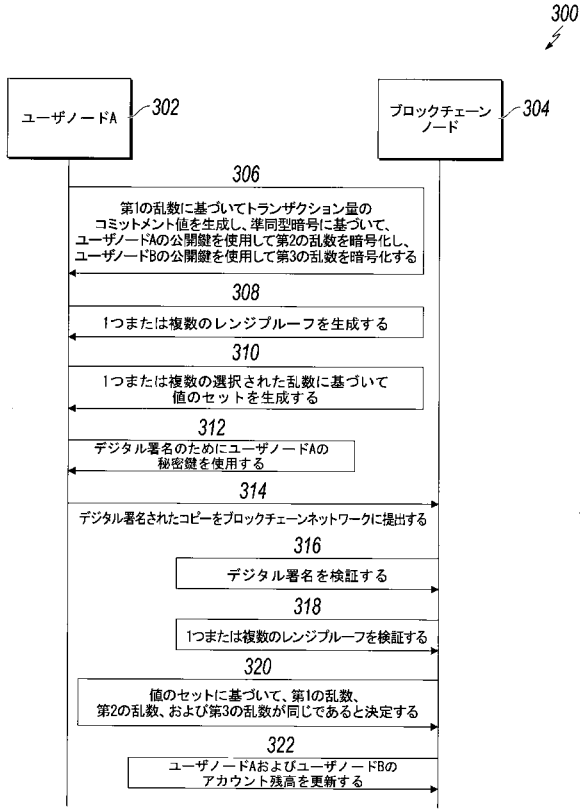
【図１】



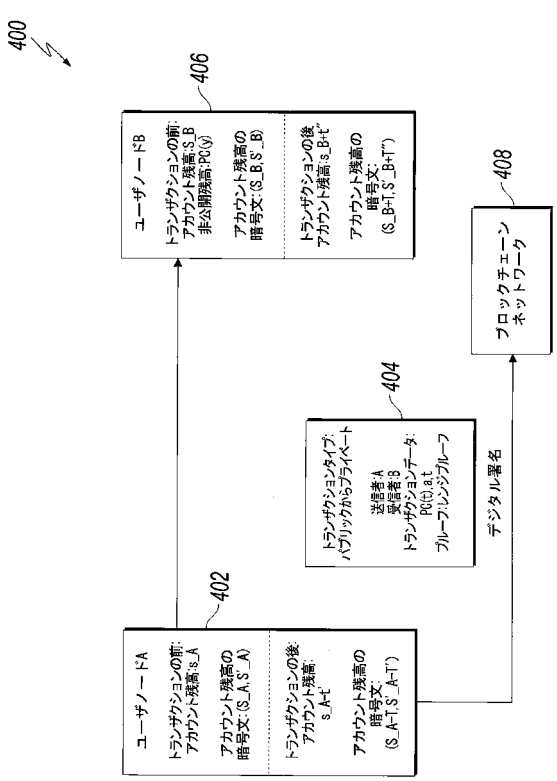
【図２】



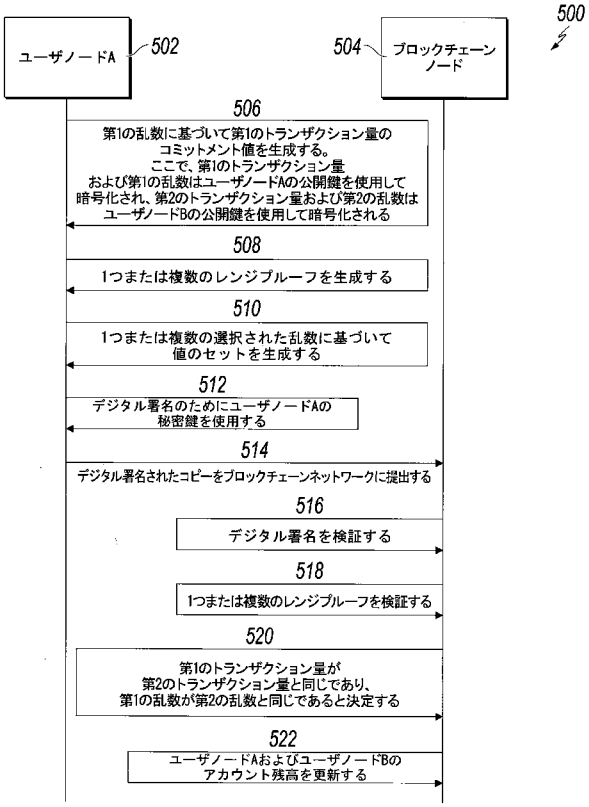
【図３】


300
ユーザノードA
302
ブロックチェーンノード
304
306
第1の乱数に基づいてトランザクション量のコミットメント値を生成し、準同型暗号に基づいて、ユーザノードAの公開鍵を使用して第2の乱数を暗号化し、ユーザノードBの公開鍵を使用して第3の乱数を暗号化する
308
1つまたは複数のレンジプルーフを生成する
310
1つまたは複数の選択された乱数に基づいて値のセットを生成する
312
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
314
デジタル署名されたコピーをブロックチェーンネットワークに提出する
316
デジタル署名を検証する
318
1つまたは複数のレンジプルーフを検証する
320
値のセットに基づいて、第1の乱数、第2の乱数、および第3の乱数が同じであると決定する
322
ユーザノードAおよびユーザノードBのアカウント残高を更新する

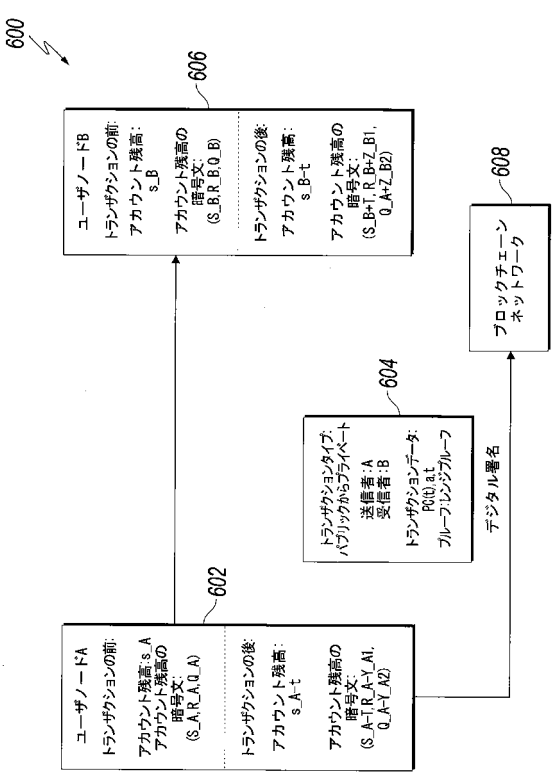
【図４】


400
406
ユーザノードB
トランザクションの前:
アカウント残高:s_B
非公開残高:PC(y)
アカウント残高の暗号文:(S_B,S'_B)
トランザクションの後
アカウント残高:s_B+t''
アカウント残高の暗号文:
(S_B+T,S''_B+T'')
408
ブロックチェーンネットワーク
404
トランザクションタイプ:
パブリックからプライベート
送信者:A
受信者:B
トランザクションデータ:
PC(t), a, t,
ブループレンジプルーフ
デジタル署名
402
ユーザノードA
トランザクションの前:
アカウント残高:s_A
アカウント残高の暗号文:(S_A,S'_A)
トランザクションの後:
アカウント残高
s_A-t''
アカウント残高の暗号文:
(S_A-T,S''_A-T')

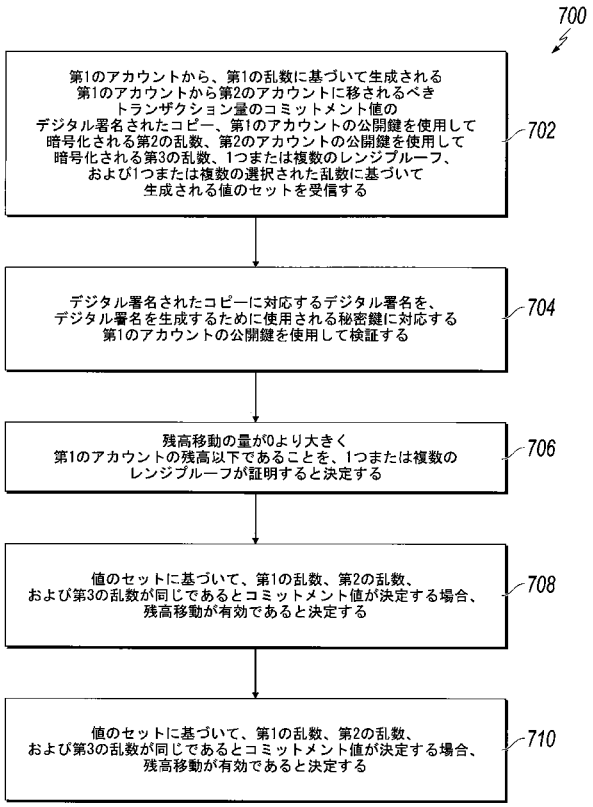
【図５】


500
ユーザノードA
502
504
ブロックチェーンノード
506
第1の乱数に基づいて第1のトランザクション量のコミットメント値を生成する。
ここで、第1のトランザクション量および第1の乱数はユーザノードAの公開鍵を使用して暗号化され、第2のトランザクション量および第2の乱数はユーザノードBの公開鍵を使用して暗号化される
508
1つまたは複数のレンジプルーフを生成する
510
1つまたは複数の選択された乱数に基づいて値のセットを生成する
512
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
514
デジタル署名されたコピーをブロックチェーンネットワークに提出する
516
デジタル署名を検証する
518
1つまたは複数のレンジプルーフを検証する
520
第1のトランザクション量が第2のトランザクション量と同じであり、第1の乱数が第2の乱数と同じであると決定する
522
ユーザノードAおよびユーザノードBのアカウント残高を更新する

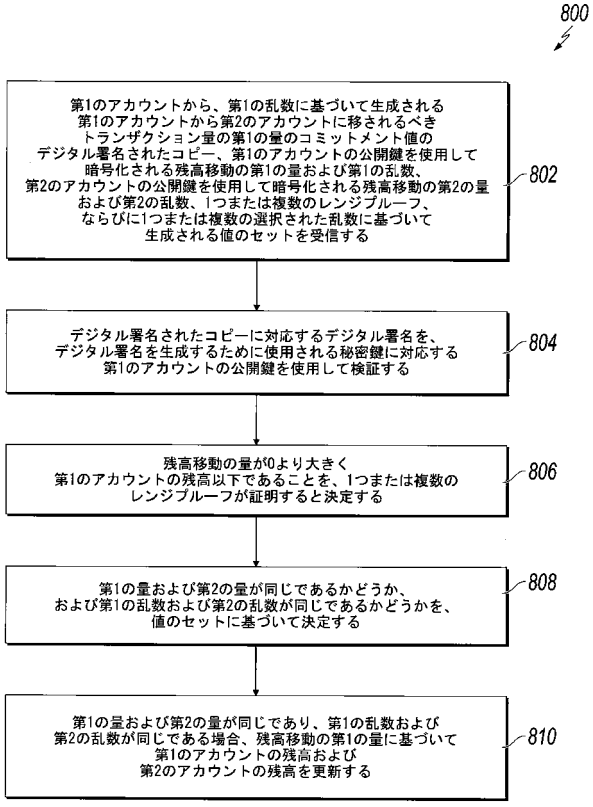
【図６】


600
606
ユーザノードB
トランザクションの前:
アカウント残高:
s_B
アカウント残高の暗号文:
(S_B,R_B,Q_B)
トランザクションの後:
アカウント残高:
s_B-t
アカウント残高の暗号文:
(S_B+T,R_B+Z_B1,
Q_A+Z_B2)
608
ブロックチェーンネットワーク
604
トランザクションタイプ:
パブリックからプライベート
送信者:A
受信者:B
トランザクションデータ:
PC(t), a, t,
ブループレンジプルーフ
デジタル署名
602
ユーザノードA
トランザクションの前:
アカウント残高:s_A
アカウント残高の暗号文:
(S_A,R_A,Q_A)
トランザクションの後:
アカウント残高:
s_A-t
アカウント残高の暗号文:
(S_A-T,R_A-Y_A1,
Q_A-Y_A2)

【図７】


700
第1のアカウントから、第1の乱数に基づいて生成される
第1のアカウントから第2のアカウントに移されるべき
トランザクション量のコミットメント値の
デジタル署名されたコピー、第1のアカウントの公開鍵を使用して
暗号化される第2の乱数、第2のアカウントの公開鍵を使用して
暗号化される第3の乱数、1つまたは複数のレンジプルーフ、
および1つまたは複数の選択された乱数に基づいて
生成される値のセットを受信する
702
デジタル署名されたコピーに対応するデジタル署名を、
デジタル署名を生成するために使用される秘密鍵に対応する
第1のアカウントの公開鍵を使用して検証する
704
残高移動の量が0より大きく
第1のアカウントの残高以下であることを、1つまたは複数の
レンジプルーフが証明すると決定する
706
値のセットに基づいて、第1の乱数、第2の乱数、
および第3の乱数が同じであるとコミットメント値が決定する場合、
残高移動が有効であると決定する
708
値のセットに基づいて、第1の乱数、第2の乱数、
および第3の乱数が同じであるとコミットメント値が決定する場合、
残高移動が有効であると決定する
710

【図８】


800
第1のアカウントから、第1の乱数に基づいて生成される
第1のアカウントから第2のアカウントに移されるべき
トランザクション量の第1の量のコミットメント値の
デジタル署名されたコピー、第1のアカウントの公開鍵を使用して
暗号化される残高移動の第1の量および第1の乱数、
第2のアカウントの公開鍵を使用して暗号化される残高移動の第2の量
および第2の乱数、1つまたは複数のレンジプルーフ、
ならびに1つまたは複数の選択された乱数に基づいて
生成される値のセットを受信する
802
デジタル署名されたコピーに対応するデジタル署名を、
デジタル署名を生成するために使用される秘密鍵に対応する
第1のアカウントの公開鍵を使用して検証する
804
残高移動の量が0より大きく
第1のアカウントの残高以下であることを、1つまたは複数の
レンジプルーフが証明すると決定する
806
第1の量および第2の量が同じであるかどうか、
および第1の乱数および第2の乱数が同じであるかどうかを、
値のセットに基づいて決定する
808
第1の量および第2の量が同じであり、第1の乱数および
第2の乱数が同じである場合、残高移動の第1の量に基づいて
第1のアカウントの残高および
第2のアカウントの残高を更新する
810

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/114344

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/10(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, EPODOC, WPI, GOOGLE: block, chain, account, model, consensus, node, verify, commitment, random, value, signature, public, private, key, balance, less, transfer, proof, range

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 108764874 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 06 November 2018 (2018-11-06) abstract, description, paragraphs [0006]-[0021]	1-12
A	CN 108632293 A (UNIV. SHANDONG JIANZHU) 09 October 2018 (2018-10-09) the whole document	1-12
A	CN 107240018 A (CHENGDU LEEREY ENTERPRISE MANAGEMENT LTD.) 10 October 2017 (2017-10-10) the whole document	1-12
A	US 7434726 B2 (PITNEY BOWES INC.) 14 October 2008 (2008-10-14) the whole document	1-12
A	CN 108377189 A (SHENZHEN ONECONNECT INTELLIGENT TECHNOLOGY) 07 August 2018 (2018-08-07) the whole document	1-12
A	CN 106910072 A (GIESECKE&DEVRIENT GMBH CHINA) 30 June 2017 (2017-06-30) the whole document	1-12

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 July 2019	**29 July 2019**
Name and mailing address of the ISA/CN **National Intellectual Property Administration, PRC** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing** **100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer **SHU,Qi** Telephone No. **86-(10)-53961220**

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/114344

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	108764874	A	06 November 2018	None			
CN	108632293	A	09 October 2018	None			
CN	107240018	A	10 October 2017	WO	2019019490	A1	31 January 2019
US	7434726	B2	14 October 2008	US	2007262135	A1	15 November 2007
CN	108377189	A	07 August 2018	None			
CN	106910072	A	30 June 2017	None			

Form PCT/ISA/210 (patent family annex) (January 2015)

フロントページの続き

(81)指定国・地域 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT

(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 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