(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6811317号
(P6811317)
(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	675Z
H04L 9/08	(2006.01)	H04L	9/00	601A
G06F 21/62	(2013.01)	G06F	21/62	318
G06F 21/64	(2013.01)	G06F	21/64	
G09C 1/00	(2006.01)	G09C	1/00	650Z

請求項の数 22　(全 25 頁)

(21)出願番号　特願2019-521791 (P2019-521791)
(86)(22)出願日　平成30年11月7日 (2018.11.7)
(65)公表番号　特表2020-515087 (P2020-515087A)
(43)公表日　令和2年5月21日 (2020.5.21)
(86)国際出願番号　PCT/CN2018/114322
(87)国際公開番号　WO2019/072262
(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6月19日 (2019.6.19)

早期審査対象出願

(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】ブロックチェーン機密トランザクション内の暗号化されたトランザクション情報の復元

(57)【特許請求の範囲】
【請求項１】
ブロックチェーン機密トランザクションに参加するクライアントノードのコンピュータ実施方法であって、前記方法は、
クライアントノードによって、複数のクライアントノードによって合意された閾値秘密分散法に従って、秘密鍵を取得するステップと、
暗号コミットメントスキームをトランザクションデータに適用することによって前記クライアントノードのブロックチェーン機密トランザクションの1つまたは複数のコミットメント値を生成するステップであって、前記ブロックチェーン機密トランザクションの内容は、前記ブロックチェーン機密トランザクションの参加者によってのみアクセス可能であり、ブロックチェーン機密トランザクションの任意の他のノードによってアクセス可能ではなく、前記1つまたは複数のコミットメント値は、
前記クライアントノードのトランザクション前のアカウント残高に基づいて生成される第1のコミットメント値と、
前記ブロックチェーン機密トランザクションのトランザクション金額に基づいて生成される第2のコミットメント値と、
前記第1のコミットメント値と前記第2のコミットメント値とに基づいて生成されるとともに前記クライアントノードのトランザクション後のアカウント残高に対応する第3のコミットメント値と
を含む、ステップと、

前記秘密鍵を使用して前記トランザクションデータを暗号化することによって前記ブロックチェーン機密トランザクションの暗号化されたトランザクション情報を生成するステップと、

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、実行のために前記ブロックチェーン機密トランザクションの前記内容を送信するステップであって、前記ブロックチェーン機密トランザクションの前記内容は、

前記1つまたは複数のコミットメント値と、

前記暗号化されたトランザクション情報と、

前記トランザクションデータの1つまたは複数のゼロ知識証明と

を含み、前記暗号化されたトランザクション情報は、前記ブロックチェーンネットワークのブロックチェーン上に記憶される、ステップと

を含む、方法。

【請求項２】

前記ブロックチェーン機密トランザクションの前記トランザクションデータは、前記ブロックチェーン機密トランザクションの前の前記クライアントノードのアカウント残高または前記ブロックチェーン機密トランザクションのトランザクション金額の一方または両方を含む、請求項1に記載の方法。

【請求項３】

前記トランザクションデータの前記1つまたは複数のゼロ知識証明は、前記トランザクションデータの値がそれぞれの範囲内にあるという1つまたは複数のゼロ知識範囲証明を含む、請求項1に記載の方法。

【請求項４】

前記暗号コミットメントスキームは、Pedersenコミットメントスキームを含み、

暗号コミットメントスキームをトランザクションデータに適用することによって前記クライアントノードのブロックチェーン機密トランザクションの1つまたは複数のコミットメント値を生成するステップは、前記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に対応する乱数に基づいて前記クライアントノードの前記ブロックチェーン機密トランザクションの前記1つまたは複数のコミットメント値を生成するステップを含み、

前記ブロックチェーン機密トランザクションの暗号化されたトランザクション情報を生成するステップは、前記秘密鍵を使用して前記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に対応する乱数を暗号化することによって前記ブロックチェーン機密トランザクションの暗号化されたトランザクション情報を生成するステップを含む、請求項1に記載の方法。

【請求項５】

前記閾値秘密分散法は、Shamirの秘密分散法を含む、請求項1に記載の方法。

【請求項６】

ブロックチェーンネットワークのコンセンサスノードのコンピュータ実施方法であって、前記方法は、

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、クライアントノードのブロックチェーン機密トランザクションの内容を受信するステップであって、前記ブロックチェーン機密トランザクションの前記内容は、前記ブロックチェーン機密トランザクションの参加者によってのみアクセス可能であり、前記ブロックチェーン機密トランザクションの任意の他のノードによってアクセス可能ではなく、前記ブロックチェーン機密トランザクションの前記内容は、

前記ブロックチェーン機密トランザクションのトランザクションデータに暗号コミットメントスキームを適用することによって前記クライアントノードによって生成された前記ブロックチェーン機密トランザクションの1つまたは複数のコミットメント値であって、前記1つまたは複数のコミットメント値は、

前記クライアントノードのトランザクション前のアカウント残高に基づいて生成される第1のコミットメント値と、

前記ブロックチェーン機密トランザクションのトランザクション金額に基づいて生成される第2のコミットメント値と、
前記第1のコミットメント値と前記第2のコミットメント値とに基づいて生成されるとともに前記クライアントノードのトランザクション後のアカウント残高に対応する第3のコミットメント値と
を含む、1つまたは複数のコミットメント値と、
前記クライアント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暗号化することによって生成される暗号化されたトランザクション情報であって、秘密鍵は、複数のクライアントノードとの閾値秘密分散法に従って前記クライアントノードによって取得される、暗号化されたトランザクション情報と、
前記トランザクションデータの1つまたは複数のゼロ知識証明と
を含む、ステップと、
前記ブロックチェーンネットワークの前記コンセンサスノードによって、前記ブロックチェーン機密トランザクションの前記内容に基づいて前記ブロックチェーン機密トランザクションが正当なものであることを検証するステップと、
前記ブロックチェーンネットワークの前記コンセンサスノードによって、前記ブロックチェーンネットワークのブロックチェーン上に前記暗号化されたトランザクション情報を記憶するステップと
を含む、方法。
【請求項７】
前記ブロックチェーン機密トランザクションの前記トランザクションデータは、前記ブロックチェーン機密トランザクションの前の前記クライアントノードのアカウント残高または前記ブロックチェーン機密トランザクションのトランザクション金額のうちの1つまたは複数を含む、請求項6に記載の方法。
【請求項８】
前記トランザクションデータの前記1つまたは複数のゼロ知識証明は、前記トランザクションデータの値がそれぞれの範囲内にあるという1つまたは複数のゼロ知識範囲証明を含む、請求項6に記載の方法。
【請求項９】
前記ブロックチェーン機密トランザクションの前記内容に基づいて前記ブロックチェーン機密トランザクションが正当なものであることを検証するステップは、
前記コミットメントスキームに基づいて前記1つまたは複数のコミットメント値が正しいと決定するステップと、
前記トランザクションデータの前記1つまたは複数のゼロ知識証明を検証するステップと
を含む、請求項6に記載の方法。
【請求項１０】
前記トランザクションデータの前記1つまたは複数のゼロ知識証明を検証するステップは、
前記ブロックチェーン機密トランザクションの前の前記クライアントノードのアカウント残高がゼロより大きいと決定するステップと、
前記ブロックチェーン機密トランザクションのトランザクション金額が前記ブロックチェーン機密トランザクションの前の前記クライアントノードのアカウント残高以下であると決定するステップと
を含む、請求項9に記載の方法。
【請求項１１】
前記暗号コミットメントスキームは、準同型であり、前記方法は、前記コミットメントスキームの準同型に基づいて前記ブロックチェーン機密トランザクションの後の前記クライアントノードのアカウント残高を更新するステップをさらに含む、請求項6に記載の方法。

【請求項１２】
前記閾値秘密分散法は、Shamirの秘密分散法を含む、請求項6に記載の方法。
【請求項１３】
ブロックチェーン機密トランザクション内の暗号化されたトランザクション情報を復元するためのコンピュータ実施方法であって、前記方法は、
特定のクライアントノードによって、ブロックチェーンネットワークのコンセンサスノードから、前記特定のクライアントノードのブロックチェーン機密トランザクションの暗号化されたトランザクション情報を受信するステップであって、前記ブロックチェーン機密トランザクションの内容は、前記ブロックチェーン機密トランザクションの参加者によってのみアクセス可能であり、前記ブロックチェーン機密トランザクションの任意の他のノードによってアクセス可能ではなく、前記ブロックチェーン機密トランザクションの前記内容は、トランザクションデータの1つまたは複数のコミットメント値と、前記暗号化されたトランザクション情報と、前記トランザクションデータの1つまたは複数のゼロ知識証明とを含み、前記1つまたは複数のコミットメント値は、前記特定のクライアントノードのトランザクション前のアカウント残高に基づいて生成される第1のコミットメント値と、前記ブロックチェーン機密トランザクションのトランザクション金額に基づいて生成される第2のコミットメント値と、前記第1のコミットメント値と前記第2のコミットメント値とに基づいて生成されるとともに前記特定のクライアントノードのトランザクション後のアカウント残高に対応する第3のコミットメント値とを含み、前記暗号化されたトランザクション情報は、前記ブロックチェーンネットワーク内の少なくとも1つのブロックチェーンに記憶されており、前記特定のクライアントノードは、前記暗号化されたトランザクション情報を復号するように構成される秘密鍵へのアクセスを有しておらず、前記特定のクライアントノードは、前記秘密鍵を以前発行されていた、ステップと、
前記特定のクライアントノードによって、複数のクライアントノードによって合意された閾値秘密分散法に従って、前記ブロックチェーンネットワーク上の前記複数のクライアントノードのうちの少なくとも閾値の数のクライアントノードから前記秘密鍵を復元するステップと、
前記特定のクライアントノードによって、前記復元した秘密鍵を使用して前記暗号化されたトランザクション情報から前記特定のクライアントノードの前記ブロックチェーン機密トランザクションの前記トランザクションデータを復号するステップと
を含む、方法。
【請求項１４】
前記特定のクライアントノードは、ローカルデータストレージに障害が発生したことに基づいて、前記秘密鍵および前記暗号化されたトランザクション情報が失われたことに起因して、前記暗号化されたトランザクション情報を復号するように構成される秘密鍵へのアクセスを有しておらず、前記秘密鍵および前記暗号化されたトランザクション情報は、前記ローカルデータストレージにおいて前記特定のクライアントノードによって保存されていた、請求項13に記載の方法。
【請求項１５】
前記秘密鍵を使用して前記暗号化されたトランザクション情報から前記特定のクライアントノードの前記ブロックチェーン機密トランザクションのトランザクションデータを復号するステップは、前記秘密鍵を使用して前記ブロックチェーン機密トランザクションの送金金額を復元するステップを含む、請求項13に記載の方法。
【請求項１６】
前記秘密鍵を使用して前記暗号化されたトランザクション情報から前記特定のクライアントノードの前記ブロックチェーン機密トランザクションのトランザクションデータを復号するステップは、前記秘密鍵を使用して前記ブロックチェーン機密トランザクションの送金金額および前記送金金額に対応する乱数の両方を復元するステップであって、前記送金金額および前記乱数は、前記特定のクライアントノードの前記ブロックチェーン機密トランザクションのトランザクション情報を秘匿するためにPedersenコミットメントスキー

ムにおいて使用される、ステップを含む、請求項13に記載の方法。
【請求項１７】
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、前記命令は、前記1つまたは複数のプロセッサに、請求項1から5のいずれか一項に記載の方法に従って動作を行わせる、非一時的コンピュータ可読記憶媒体。
【請求項１８】
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、前記命令は、前記1つまたは複数のプロセッサに、請求項6から12のいずれか一項に記載の方法に従って動作を行わせる、非一時的コンピュータ可読記憶媒体。
【請求項１９】
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、前記命令は、前記1つまたは複数のプロセッサに、請求項13から16のいずれか一項に記載の方法に従って動作を行わせる、非一時的コンピュータ可読記憶媒体。
【請求項２０】
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ストレージデバイスであって、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、前記命令は、前記コンピューティングデバイスに、請求項1から5のいずれか一項に記載の方法に従って動作を行わせる、コンピュータ可読ストレージデバイスと
を含む、トランザクション管理システム。
【請求項２１】
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ストレージデバイスであって、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、前記命令は、前記コンピューティングデバイスに、請求項6から12のいずれか一項に記載の方法に従って動作を行わせる、コンピュータ可読ストレージデバイスと
を含む、トランザクション管理システム。
【請求項２２】
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ストレージデバイスであって、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、前記命令は、前記コンピューティングデバイスに、請求項13から16のいずれか一項に記載の方法に従って動作を行わせる、コンピュータ可読ストレージデバイスと
を含む、トランザクション管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
ブロックチェーン機密トランザクション内の暗号化されたトランザクション情報の復元に関する。
【背景技術】
【０００２】
コンセンサスネットワークおよび/またはブロックチェーンネットワークとも称することができる分散型台帳システム(DLS)は、参加エンティティが安全かつ変更不可能な形でデータを記憶することを可能にする。DLSは、いかなる特定のユーザケース(例えば、暗号通貨)を指すわけではなく、ブロックチェーンネットワークと一般には称される。例示的なタイプの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、およびコンソーシアムブロックチェーン

ネットワークを含み得る。パブリックブロックチェーンネットワークは、DLSを使用し、コンセンサスプロセスに参加するように、すべてのエンティティに対してオープンとなっている。プライベートブロックチェーンネットワークは、特定のエンティティに提供されており、読込みおよび書込みの許可を中央集権的に制御する。コンソーシアムブロックチェーンネットワークは、エンティティの選抜グループに提供されており、コンセンサスプロセスを制御し、アクセス制御レイヤを含む。

【０００３】

ブロックチェーンは、暗号通貨ネットワークにおいて使用されており、物品を売買するための取引および/または暗号通貨を使用したサービスを参加者が実施することを可能にする。共通の暗号通貨は、Bitcoinを含む。暗号通貨ネットワークにおいては、レコードキーピングモデルは、ユーザ間のトランザクションを記録するために使用される。例示的なレコードキーピングモデルは、未使用トランザクションアウトプット(UTXO)モデル、およびアカウントモデル(アカウントベースモデルまたはアカウント/残高モデルとも称する)を含む。

【０００４】

UTXOモデルにおいては、チェーン上のアセットは、トランザクションの形式となっている。各トランザクションは、以前のトランザクションからのアウトプットを使用し、以後のトランザクションにおいて使用され得る新規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はトラッキングされ、ユーザが使用する必要がある残高は未使用トランザクションの合計として算出される。各トランザクションは、インプットとして1つまたは複数の未使用アウトプット(且つ未使用アウトプットのみ)を取り込み、1つまたは複数のアウトプットを有することができる。未使用アウトプットのみがさらなるトランザクションにおいて使用され得るという要件は、二重支払および不正行為を防ぐために必要である。UTXOモデルは、トランザクションの検証および証明機能をサポートするが、スマートコントラクトに関するサポートは不得手である。

【０００５】

アカウントモデルは、Ethereumによって採用されている。アカウントモデルは、レコードキーピングを行い、従来の銀行のようにアカウント残高を管理する。このモデルの下では、アカウントは、アドレスおよび対応するアカウント残高を有し得る。チェーン上のアセットは、アカウントの残高として表される。各送金トランザクションは、送金されたアセットのアカウントアドレスおよび着金したアセットのアカウントアドレスを有し得る。トランザクション金額は、アカウントの残高に関して直接更新される。送金アカウントがトランザクションに対する支払いをするのに十分な残高を有していることを各トランザクションが確認するだけでよいため、アカウントモデルは効率的である。トランザクションの検証および証明機能をサポートすることに加えて、アカウントモデルは、スマートコントラクト、特に、状態情報を必要とするまたは複数の関係者が関与するスマートコントラクトを完全にサポートし得る。

【発明の概要】

【課題を解決するための手段】

【０００６】

本開示の実施形態は、ブロックチェーン技術(ブロックチェーン機密トランザクション、または単に、機密トランザクションと称する)に基づいた機密トランザクションのためのコンピュータ実施方法を含む。より詳細には、本開示の実施形態は、ブロックチェーン機密トランザクション内の暗号化されたトランザクション情報を復元することを目的としている。

【０００７】

いくつかの実施形態においては、アクションは、クライアントノードによって、ある数のクライアントノードによって合意された閾値秘密分散法に従って、秘密鍵を取得するステップと、暗号コミットメントスキームをトランザクションデータに適用することによってクライアントノードの機密トランザクションの1つまたは複数のコミットメント値を生

成するステップと、秘密鍵を使用してトランザクションデータを暗号化することによって機密トランザクションの暗号化されたトランザクション情報を生成するステップと、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、実行のために機密トランザクションの内容を送信するステップであって、機密トランザクションの内容は、1つまたは複数のコミットメント値と、暗号化されたトランザクション情報と、トランザクションデータの1つまたは複数のゼロ知識証明とを含む、ステップとを含む。

【０００８】

いくつかの実施形態においては、動作は、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、クライアントノードの機密トランザクションの内容を受信するステップであって、機密トランザクションの内容は、機密トランザクションのトランザクションデータに暗号コミットメントスキームを適用することによってクライアントノードによって生成された機密トランザクションの1つまたは複数のコミットメント値と、クライアントノードの秘密鍵を使用してトランザクションデータを暗号化することによって生成される暗号化されたトランザクション情報であって、秘密鍵は、ある数のクライアントノードとの閾値秘密分散法に従ってクライアントノードによって取得される、暗号化されたトランザクション情報と、トランザクションデータの1つまたは複数のゼロ知識証明とを含む、ステップと、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、機密トランザクションの内容に基づいて機密トランザクションが正当なものであることを検証するステップと、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、ブロックチェーンネットワークのブロックチェーン上に暗号化されたトランザクション情報を記憶するステップとを含む。

【０００９】

いくつかの実施形態においては、動作は、特定のクライアントノードによって、ブロックチェーンネットワークのコンセンサスノードから、特定のクライアントノードの機密トランザクションの暗号化されたトランザクション情報を受信するステップであって、暗号化されたトランザクション情報は、ブロックチェーンネットワーク内の少なくとも1つのブロックチェーンに記憶されており、特定のクライアントノードは、暗号化されたトランザクション情報を復号するように構成される秘密鍵へのアクセスを有しておらず、特定のクライアントノードは、秘密鍵を以前発行されていた、ステップと、特定のクライアントノードによって、ある数のクライアントノードによって合意された閾値秘密分散法に従って、ブロックチェーンネットワーク上のある数のクライアントノードのうちの少なくとも閾値の数のクライアントノードから秘密鍵を復元するステップと、特定のクライアントノードによって、復元した秘密鍵を使用して暗号化されたトランザクション情報から特定のクライアントノードの機密トランザクションのトランザクションデータを復号するステップとを含む。

【００１０】

他の実施形態は、対応する、システムと、装置と、コンピュータストレージデバイス上に符号化された、方法のアクションを行うように構成される、コンピュータプログラムとを含む。

【００１１】

これらおよび他の実施形態の各々は、以下の特徴の1つまたは複数を必要に応じて含み得る。

【００１２】

下記の特徴のいずれかと組み合わせることが可能な第1の特徴としては、機密トランザクションのトランザクションデータは、機密トランザクションの前のクライアントノードのアカウント残高または機密トランザクションのトランザクション金額の一方または両方を含む。

【００１３】

上記または下記の特徴のいずれかと組み合わせることが可能な第2の特徴としては、トランザクションデータの1つまたは複数のゼロ知識証明は、トランザクションデータの値

がそれぞれの範囲内にあるという1つまたは複数のゼロ知識範囲証明を含む。
【００１４】
上記または下記の特徴のいずれかと組み合わせることが可能な第3の特徴としては、暗号コミットメントスキームは、Pedersenコミットメントスキームを含み、暗号コミットメントスキームをトランザクションデータに適用することによってクライアントノードの機密トランザクションの1つまたは複数のコミットメント値を生成するステップは、トランザクションデータおよびトランザクションデータに対応する乱数に基づいてクライアントノードの機密トランザクションの1つまたは複数のコミットメント値を生成するステップを含み、機密トランザクションの暗号化されたトランザクション情報を生成するステップは、秘密鍵を使用してトランザクションデータおよびトランザクションデータに対応する乱数を暗号化することによって機密トランザクションの暗号化されたトランザクション情報を生成するステップを含む。
【００１５】
上記または下記の特徴のいずれかと組み合わせることが可能な第4の特徴としては、閾値秘密分散法は、Shamirの秘密分散法を含む。
【００１６】
上記または下記の特徴のいずれかと組み合わせることが可能な第5の特徴としては、機密トランザクションの内容に基づいて機密トランザクションが正当なものであることを検証するステップは、コミットメントスキームに基づいて1つまたは複数のコミットメント値が正しいと決定するステップと、トランザクションデータの1つまたは複数のゼロ知識証明を検証するステップとを含む。
【００１７】
上記または下記の特徴のいずれかと組み合わせることが可能な第6の特徴としては、トランザクションデータの1つまたは複数のゼロ知識証明を検証するステップは、機密トランザクションの前のクライアントノードのアカウント残高がゼロより大きいと決定するステップと、機密トランザクションのトランザクション金額が機密トランザクションの前のクライアントノードのアカウント残高以下であると決定するステップとを含む。
【００１８】
上記または下記の特徴のいずれかと組み合わせることが可能な第7の特徴としては、暗号コミットメントスキームは、準同型であり、方法は、コミットメントスキームの準同型に基づいて機密トランザクションの後のクライアントノードのアカウント残高を更新するステップをさらに含む。
【００１９】
上記または下記の特徴のいずれかと組み合わせることが可能な第8の特徴としては、秘密鍵を使用して暗号化されたトランザクション情報から特定のクライアントノードの機密トランザクションのトランザクションデータを復号するステップは、秘密鍵を使用して機密トランザクションの送金金額を復元するステップを含む。
【００２０】
上記または下記の特徴のいずれかと組み合わせることが可能な第9の特徴としては、秘密鍵を使用して暗号化されたトランザクション情報から特定のクライアントノードの機密トランザクションのトランザクションデータを復号するステップは、秘密鍵を使用して機密トランザクションの送金金額および送金金額に対応する乱数の両方を復元するステップであって、送金金額および乱数は、特定のクライアントノードの機密トランザクションのトランザクション情報を秘匿するためにPedersenコミットメントスキームにおいて使用される、ステップを含む。
【００２１】
本開示はまた、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1つまたは複数の非一時的コンピュータ可読記憶媒体であって、1つまたは複数のプロセッサによって実行されると、命令は、1つまたは複数のプロセッサに、本明細書で提供した方法の実施形態に従って動作を行わせる、非一時的コンピュータ可読記憶媒体を提供している

。
【００２２】
本開示は、本明細書で提供した方法を実施するためのシステムをさらに提供している。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ると、命令は、1つまたは複数のプロセッサに、本明細書で提供した方法の実施形態に従って動作を行わせる、コンピュータ可読記憶媒体とを含む。
【００２３】
本開示による方法が本明細書に記載の態様と特徴との任意の組合せを含み得ることは諒解されよう。すなわち、本開示による方法は、特に本明細書に記載の態様と特徴との組合せに限定されるわけではなく、提供した態様と特徴との任意の組合せも含む。
【００２４】
本開示についての1つまたは複数の実施形態の詳細を添付の図面および以下の説明に記載している。本開示についての他の特徴および利点が、説明および図面から、および特許請求の範囲から明らかとなるであろう。
【図面の簡単な説明】
【００２５】
【図１】本開示の実施形態を実行するために使用され得る例示的な環境を示す図である。
【図２】本開示の実施形態による、例示的な概念的機構を示す図である。
【図３】本開示の実施形態による、機密トランザクションを準備するための例示的なプロセス300を示す図である。
【図４】本開示の実施形態による、機密トランザクションのトランザクション情報の例示的な復元プロセス400を示す図である。
【図５】本開示の実施形態による、実行され得る例示的なプロセスを示す図である。
【発明を実施するための形態】
【００２６】
様々な図面における類似の参照記号は類似の要素を示す。
【００２７】
本開示の実施形態は、ブロックチェーン技術に基づいた機密トランザクションのためのコンピュータ実施方法を含む。より詳細には、本開示の実施形態は、ブロックチェーン機密トランザクション内の暗号化されたトランザクション情報を復元することを目的としている。
【００２８】
いくつかの実施形態においては、アクションは、クライアントノードによって、ある数のクライアントノードによって合意された閾値秘密分散法に従って、秘密鍵を取得するステップと、暗号コミットメントスキームをトランザクションデータに適用することによってクライアントノードの機密トランザクションの1つまたは複数のコミットメント値を生成するステップと、秘密鍵を使用してトランザクションデータを暗号化することによって機密トランザクションの暗号化されたトランザクション情報を生成するステップと、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、実行のために機密トランザクションの内容を送信するステップであって、機密トランザクションの内容は、1つまたは複数のコミットメント値と、暗号化されたトランザクション情報と、トランザクションデータの1つまたは複数のゼロ知識証明とを含む、ステップとを含む。
【００２９】
いくつかの実施形態においては、動作は、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、クライアントノードの機密トランザクションの内容を受信するステップであって、機密トランザクションの内容は、機密トランザクションのトランザクションデータに暗号コミットメントスキームを適用することによってクライアントノードによって生成された機密トランザクションの1つまたは複数のコミットメント値と、クライアントノードの秘密鍵を使用してトランザクションデータを暗号化することによって生成され

る暗号化されたトランザクション情報であって、秘密鍵は、ある数のクライアントノードとの閾値秘密分散法に従ってクライアントノードによって取得される、暗号化されたトランザクション情報と、トランザクションデータの1つまたは複数のゼロ知識証明とを含む、ステップと、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、機密トランザクションの内容に基づいて機密トランザクションが正当なものであることを検証するステップと、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、ブロックチェーンネットワークのブロックチェーン上に暗号化されたトランザクション情報を記憶するステップとを含む。

【００３０】

いくつかの実施形態においては、動作は、特定のクライアントノードによって、ブロックチェーンネットワークのコンセンサスノードから、特定のクライアントノードの機密トランザクションの暗号化されたトランザクション情報を受信するステップであって、暗号化されたトランザクション情報は、ブロックチェーンネットワーク内の少なくとも1つのブロックチェーンに記憶されており、特定のクライアントノードは、暗号化されたトランザクション情報を復号するように構成される秘密鍵へのアクセスを有しておらず、特定のクライアントノードは、秘密鍵を以前発行されていた、ステップと、特定のクライアントノードによって、ある数のクライアントノードによって合意された閾値秘密分散法に従って、ブロックチェーンネットワーク上のある数のクライアントノードのうちの少なくとも閾値の数のクライアントノードから秘密鍵を復元するステップと、特定のクライアントノードによって、復元した秘密鍵を使用して暗号化されたトランザクション情報から特定のクライアントノードの機密トランザクションのトランザクションデータを復号するステップとを含む。

【００３１】

本開示の実施形態についてのさらなる状況をあげるとすれば、および上述したように、コンセンサスネットワーク(例えば、ピア・ツー・ピアノードで構成される)およびブロックチェーンネットワークとも称することができる分散型台帳システム(DLS)は、参加エンティティが安全かつ変更不可能な形で取引を実施しデータを記憶することを可能にする。ブロックチェーンという用語は、Bitcoinといった暗号通貨ネットワークと一般的に関連深いが、本明細書では、いかなる特定のユースケースを指すわけではなく一般的にDLSを指すために、ブロックチェーンを使用している。上述したように、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され得る。

【００３２】

パブリックブロックチェーンネットワークにおいては、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、数百、数千、さらには数百万のエンティティがパブリックブロックチェーンネットワークに協力し得るし、その各々がパブリックブロックチェーンネットワーク内の少なくとも1つのノードを管理する。それゆえ、パブリックブロックチェーンネットワークを、参加エンティティに対するパブリックネットワークとみなすことができる。いくつかの例においては、ブロックを有効とするためにおよびブロックチェーンネットワークのブロックチェーン(分散型台帳)に追加するために、大部分のエンティティ(ノード)はブロックごとに記帳する必要がある。例示的なパブリックブロックチェーンネットワークは、ピア・ツー・ピア決済ネットワークであるBitcoinネットワークを含む。Bitcoinネットワークは、ブロックチェーンと称する分散型台帳を活用する。しかしながら、上述したように、ブロックチェーンという用語は、Bitcoinネットワークを特に指すわけではなく分散型台帳を一般的に指すために使用される。

【００３３】

一般に、パブリックブロックチェーンネットワークは、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、パブリックブロックチェーンネットワー

ク内のノードのすべてと共有され、グローバルブロックチェーンに記憶されている。グローバルブロックチェーンは、すべてのノードにわたって複製されるブロックチェーンである。すなわち、すべてのノードは、グローバルブロックチェーンに関して完全ステータスコンセンサスとなる。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に対する合意)を得るために、コンセンサスプロトコルがパブリックブロックチェーンネットワークにおいて実施される。例示的なコンセンサスプロトコルは、限定を意図したものではないが、Bitcoinネットワークにおいて実施されるプルーフ・オブ・ワーク(POW)を含む。

【００３４】

一般に、プライベートブロックチェーンネットワークは、特定のエンティティに提供されており、読込みおよび書込みの許可を中央集権的に制御する。エンティティは、どのノードがブロックチェーンネットワークに参加することができるかを制御する。それゆえ、プライベートブロックチェーンネットワークは、誰がネットワークに参加することができるかについての制約、およびそれらの参加のレベル(例えば、あるトランザクションに限定)についての制約を設定している、許可型ネットワークと一般的には称される。(例えば、既存の参加者が新規エンティティの追加について表決する、監督機関が許可を制御することができるといった)様々なタイプのアクセス制御機構を使用することができる。

【００３５】

一般に、コンソーシアムブロックチェーンネットワークは、参加エンティティの間でプライベートなものとなっている。コンソーシアムブロックチェーンネットワークにおいては、コンセンサスプロセスは権限を与えられたノードのセットによって制御され、1つまたは複数のノードがそれぞれのエンティティ(例えば、金融機関、保険会社)によって管理される。例えば、十(10)のコンソーシアムエンティティ(例えば、金融機関、保険会社)がコンソーシアムブロックチェーンネットワークを管理してもよく、その各々がコンソーシアムブロックチェーンネットワーク内の少なくとも1つのノードを管理する。それゆえ、コンソーシアムブロックチェーンネットワークを、参加エンティティに対するプライベートネットワークとみなすことができる。いくつかの例においては、ブロックを有効とするためにおよびブロックチェーンに追加するために、各エンティティ(ノード)はブロックごとに記帳する必要がある。いくつかの例においては、ブロックを有効とするためにおよびブロックチェーンに追加するために、少なくともエンティティ(ノード)のサブセット(例えば、少なくとも7つのエンティティ)はブロックごとに記帳する必要がある。

【００３６】

本開示の実施形態を、コンソーシアムブロックチェーンネットワークを参照して本明細書ではさらに詳細に説明する。しかしながら、本開示の実施形態を任意の適切なタイプのブロックチェーンネットワークにおいて実現することができることは念頭に置かれたい。

【００３７】

本開示の実施形態は、上記の事情を考慮して本明細書ではさらに詳細に説明する。より詳細には、および上述したように、本開示の実施形態は、ブロックチェーン機密トランザクションを管理することを目的としている。

【００３８】

ブロックチェーンは、パブリックまたはプライベートピア・ツー・ピアネットワーク内のトランザクションを記録する、改竄耐性のある、共有デジタル台帳である。台帳はネットワーク内のすべてのメンバノードに分散されており、ネットワークにおいて生じるアセットトランザクションの履歴はブロックに恒久的に記録される。台帳が参加エンティティに対して完全に公になっているため、ブロックチェーン台帳自体は、プライバシー保護機能を有しておらず、アセットトランザクションの内容のプライバシーを保護する追加の技術を必要とする。

【００３９】

ブロックチェーンのためのプライバシー保護のための技法は、機密トランザクションを実現してトランザクションの内容のプライバシーを保護するための技法を含み得る。機密

トランザクションにおいては、トランザクションの内容は、いかなる他の部外者も対象外であり、トランザクションの参加者によってのみアクセス可能または知るところとなる。例えば、機密トランザクションは、トランザクションに参加する2人の関係者のみが取引される金額に関与することができ、外部の監視者がこの情報を知ることを防ぐ。機密トランザクションを実現するためのそのような技法が、例えば、MONEROおよびZCASHにおいて、使用されている。

【００４０】

ブロックチェーンのためのプライバシー保護のための技法はまた、あるトランザクションに対する関係者の識別情報を保護するための技法を含んでいてもよく、例えば、ステルスアドレスまたはリングシグニチャ機構を使用して実現され得る。

【００４１】

プライバシー保護が(例えば、機密トランザクションとの関連で)ブロックチェーンに追加されている場合には、Pedersenコミットメントスキームなどのコミットメントスキームが、クライアントノードのあるトランザクション情報を秘匿または暗号化するために使用され得る。トランザクション情報は、例えば、トランザクションの前のユーザのアカウント残高、トランザクション金額、および/または他の情報を含み得る。例えば、クライアントノード(クライアント、ユーザ、関係者、またはトランザクションの参加者とも称する)は、Pedersenコミットメントスキームに従ってトランザクション前のアカウント残高aおよび対応する乱数rを裏付けまたはコミットし得る。クライアントノードは、値aおよび乱数rを保存し得る。コミットメントに対応するaまたはrが失われると、アカウント内の残高はクライアントノードによって使用することができなくなる。例えば、aおよびrの両方が失われるケースにおいては、クライアントノードは、残高aも残高に対応する乱数rも分からなくなる。aではなくrのみが失われるケースにおいては、クライアントノードは、残高tを把握することはできるが、残高の使用にはrの操作が関与するためその残高を使用することはできない。aが失われるケースにおいては、クライアントは、彼または彼女の残高が分からなくなる。クライアントノードは、クライアントノードの演算能力が限られている場合には、平文金額を修復または復元することができない。

【００４２】

トランザクションの情報を秘匿または暗号化するためにコミットメントスキーム(例えば、Pedersenコミットメント)を使用する際における上述した問題を解決するために例示的な技法を説明する。説明した技法は、そのようなトランザクション情報が失われるケースにおいてクライアントノードが元の平文トランザクション情報(例えば、コミットされた値aおよび/または乱数r)を復元することを可能およびより容易にし得る。

【００４３】

説明した技法は、ブロックチェーン機密トランザクションにおいて秘匿されたトランザクション情報(例えば、失われてしまったコミットされたトランザクション値a)を復元するための復元スキームを含む。いくつかの実施形態においては、説明した技法は、ブロックチェーンネットワーク内の1つまたは複数のブロックチェーンに秘匿されたトランザクション情報を記憶することを含む。いくつかの実施形態においては、ブロックチェーンに記憶されている機密トランザクションの秘匿されたトランザクション情報を暗号化することはできない。暗号化の前の情報を平文情報と称し得る。暗号化の後にその結果として生じる情報を暗号化情報または暗号文情報と称し得る。

【００４４】

いくつかの実施形態においては、クライアントノードは、秘密鍵を使用して暗号化トランザクションデータまたは暗号文トランザクションデータにあるトランザクションデータ(すなわち、平文トランザクションデータ)を暗号化し得る。例えば、クライアントノードは、秘密鍵を使用してPedersenコミットメントに従って平文値(例えば、アカウント情報)および平文値に対応する乱数の両方を暗号化し得る。その結果として生じる機密トランザクションの暗号化されたトランザクション情報(例えば、暗号化された乱数および暗号化された平文値)は、トランザクションの内容の一部として含まれ、ブロックチェーンネッ

トワークによって実行のために送信され得る。1つまたは複数のブロックチェーンノードは、例えばブロックチェーンネットワーク内の1つまたは複数のブロックチェーンに、暗号化されたトランザクション情報を記憶し得る。クライアントノードは、1つまたは複数のブロックチェーンノードからクライアントノードに対応する暗号化されたトランザクション情報を読み出し、秘密鍵を使用して暗号化されたトランザクション情報から平文トランザクションデータを復号し得る。

【００４５】

いくつかの実施形態においては、クライアントノードは、平文トランザクションデータおよび/または秘密鍵を失う場合がある。例えば、クライアントノードがクライアントノードのデータストレージ上にローカルに平文トランザクションデータおよび/または秘密鍵を保存している場合には、クライアントノードは、データストレージが占有されるとまたは損傷すると、平文トランザクションデータおよび/または秘密鍵を失う可能性がある。説明した技法は、平文トランザクションデータおよび/または秘密鍵を復元することに役立ち得る。

【００４６】

いくつかの実施形態においては、セキュアなマルチパーティ計算(MPC)のために閾値秘密分散法(例えば、Shamirの秘密分散法)に従ってクライアントノードの秘密鍵を保証することができる。例えば、クライアントノードの暗号化コミットメントに対応するプライベート秘密鍵が、すべての数の参加者(例えば、Shamirの秘密分散法のn個の参加者)間で取り決めおよび生成され得る。秘密鍵は、複数のパーツに分割し、それぞれ、すべての数の参加者によって保存され得る、それによって、クライアントノードの秘密鍵の漏洩を回避している。クライアントノードが秘密鍵を失ったケースにおいては、クライアントノードは、n個のうちの少なくともk個の参加者から秘密鍵の少なくとも閾値の数のパーツ(例えば、k個のパーツ)を受信することによって、Shamirの秘密分散法に従って秘密鍵を復元することができる。それゆえ、クライアントノードは、秘密鍵を使用して暗号化されたトランザクション情報から平文トランザクションデータを復号するために、秘密鍵を復元し、秘密鍵を使用することができる。

【００４７】

説明した技法は、秘密鍵および機密トランザクションの平文トランザクションデータを復元することに役立ち得る。説明した技法は、クライアントノードがそれらのハードウェアを使用して(例えば、ハードウェアベースのウォレットに)それらの秘密鍵をバックアップする、ハードウェアベースのバックアップスキームに依存するものではない。説明した技法は、トランザクションデータがブロックチェーンネットワーク内の1つまたは複数のブロックチェーン上に記憶されるときの強化されたセキュリティおよびトランザクションデータのロバスト性を提供し得る。説明した技法は、ハードウェアベースのウォレットまたはソフトウェアベースのウォレットの実施形態にかかわらず、その秘密鍵へのクライアントノードアクセスを提供し得る。説明した技法は、追加のまたは異なる利点を達成し得る。

【００４８】

図1は、本開示の実施形態を実行するために使用され得る例示的な環境100を図示している。いくつかの例においては、例示的な環境100は、エンティティがコンソーシアムブロックチェーンネットワーク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デバイスまたはシステム106、108、およびネットワーク110を含む。いくつかの例においては、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、クライアントデバイス(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。いくつかの例においては、ネットワーク110は、有線および/または無線通信リンクを介してアクセスされ得る。

【００４９】

図示した例においては、コンピューティングシステム106、108の各々は、コンソーシア

ムブロックチェーンネットワーク102内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は、限定を意図したものではないが、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を含む。いくつかの例においては、コンピューティングシステム106、108は、コンソーシアムブロックチェーンネットワーク102とやりとりするための1つまたは複数のコンピュータ実施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のエンティティが1つまたは複数の他のエンティティ(例えば、他のクライアント)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といった、第1のエンティティ(例えば、クライアントA)のコンピュータ実施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のエンティティが1つまたは複数の他のエンティティ(例えば、他のクライアント)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といった、第2のエンティティ(例えば、クライアントB)のホストコンピュータ実施サービスをホストすることができる。図1の例においては、コンソーシアムブロックチェーンネットワーク102を、ノードからなるピア・ツー・ピアネットワークとして表しており、コンピューティングシステム106、108は、コンソーシアムブロックチェーンネットワーク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それぞれ提供する。

【００５０】

図2は、本開示の実施形態による、例示的な概念的機構200を図示している。例示的な概念的機構200は、エンティティレイヤ202、ホステッドサービスレイヤ204、およびブロックチェーンネットワークレイヤ206を含む。図示した例においては、エンティティレイヤ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、各エンティティは、それぞれのトランザクション管理システム208を有する。

【００５１】

図示した例においては、ホステッドサービスレイヤ204は、各トランザクション管理システム208のためのインターフェース210を含む。いくつかの例においては、それぞれのトランザクション管理システム208は、プロトコル(例えば、ハイパーテキスト・トランスファー・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)を介してそれぞれのインターフェース210と通信する。いくつかの例においては、各インターフェース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ネットワークレイヤ206との間の通信接続を提供する。より詳細には、インターフェース210は、ブロックチェーンネットワークレイヤ206のブロックチェーンネットワーク212と通信する。いくつかの例においては、インターフェース210とブロックチェーンネットワークレイヤ206との間の通信は、リモートプロシージャコール(RPC)を使用して実施される。いくつかの例においては、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ネットワークノードを「ホスト」する。例えば、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の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。

【００５２】

本明細書に記載しているように、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内の情報を変更不可能な形で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を概略的に図示しているが、ブロックチェーン216の複数のコピーが、提供され、ブロックチェーンネットワーク212にわたって保持される。例えば、各ノード214は、ブロックチェーンのコピーを記憶する。いくつかの実施形態においては、ブロックチェーン216は、コンソーシアムブロックチェーンネットワークに参加する2つ以上のエンティティの間で行われるトランザクションに関連付けられた情報を記憶する。

【００５３】

図3は、本開示の実施形態による、機密トランザクションを準備するための例示的なプ

ロセス300を示す図である。クライアントノードA302、B304、C306、およびD308は、閾値秘密分散法(閾値鍵分散法とも称する)の参加者を表している。閾値秘密分散法は、複数の関係者による鍵のセキュリティ管理の問題を解決する。例示的な秘密分散法としては、Shamirの秘密分散法(Shamir(k,n)と表される)は、秘密鍵をn個のパーツに分割し、それぞれ、n個のパーツをn個の参加者に割り当てる。各参加者は、秘密鍵についての一意な割り当てを有する。元の秘密鍵を再構築するためには、最小または閾値の数のパーツが必要となる。閾値スキームにおいては、この最小の数kは、パーツの総数n未満である。換言すれば、秘密鍵の少なくともk個のパーツを収集すれば、元の秘密鍵を復元することができる。Shamirアルゴリズムは、例えばLagrangian差分アルゴリズムまたは他の方法を使用して、秘密鍵を復元することができる。

【００５４】

ここで、Shamir(k,n)は、平文mが暗号化されn個のパーツに分割されており、平文mを復元するために少なくともk個のパーツが必要となることを意味する。図3に示しているように、クライアントノードA302は、鍵Akeyを生成し、Akeyを4個のパーツに分解し得る。クライアントノードA302は、1個のパーツを保持し、それぞれのパーツをクライアントノードB304、C306、およびD308の各々に与え得る。

【００５５】

いくつかの実施形態においては、クライアントノードA302の観点からすれば、310において、クライアントノードA302が、上述したようにShamir(k,n)と表されるShamirの秘密分散法に従って、秘密鍵Akeyを取り決めおよび取得し得る。kおよびnの値は、セキュリティおよび複雑度の検討に基づいて例えばクライアントノードA302または別の関係者によって、決定され得る。図3に示した例においては、クライアントノードA302、B304、C306、およびD308のすべてがShamirの秘密分散法の参加者であるように、nは4となり得る。この場合には、クライアントノードA302がすべての参加者クライアントノードA302、B304、C306、およびD308のうちの少なくとも2または3個の参加者から秘密鍵Akeyを復元することができるように、kは2または3となり得る。別の例としては、クライアントノードA302がShamirの秘密分散法のすべての参加者のうちの少なくとも4個の参加者から秘密鍵Akeyを復元できるように、kは4となり得るしnは4より大きくなり得る。

【００５６】

いくつかの実施形態においては、クライアントノードA302は、図1および図2において説明したように、第1のクライアントまたはエンティティに対応するコンピューティングシステム106、108の一例である。クライアントノードA302は、ブロックチェーンネットワーク350を介したトランザクションのための対応するアカウント(例えば、パブリックアカウントまたはプライベートアカウント)を有する。ブロックチェーンネットワーク350は、複数のコンセンサスノード(図3中のブロックチェーンノード312など)を含み得る。いくつかの実施形態においては、クライアントノードB304、C306、およびD308は、ブロックチェーンネットワーク350のクライアントノードであってもなくてもよい。換言すれば、クライアントノードA302は、ブロックチェーンネットワーク350から独立した形で秘密鍵を取得し得る。例えば、クライアントノードA302は、ブロックチェーンネットワーク350以外の通信を介してクライアントノードB304、C306、およびD308から秘密鍵を取得し得る。

【００５７】

いくつかの実施形態においては、クライアントノードA302は、トランザクション情報がクライアントノードA302およびクライアントノードB304によってのみ閲覧可能またさもなければ知るところとなるが他の関係者(例えば、クライアントノードC306もしくはD308、またはブロックチェーンネットワーク350内のブロックチェーンノード312)によっては閲覧可能またさもなければ知るところとならないように、別のクライアントノード(例えば、クライアントノードB304)との機密トランザクションを行い得る。

【００５８】

320において、クライアントノードA302が、金額tをクライアントノードB304に送金する機密トランザクションを作成する。いくつかの実施形態においては、クライアントノード

A302は、ローカルで機密トランザクションの内容を構築し、機密トランザクションの内容をブロックチェーンネットワーク350(例えば、ブロックチェーンネットワーク350内の1つまたは複数のブロックチェーンノード312)に送信し得る。

【００５９】

いくつかの実施形態においては、機密トランザクションは、トランザクションデータ(例えば、トランザクションの前のアカウント残高、およびトランザクション金額)を秘匿するために、コミットメントスキームに基づいて構築され得る。例示的なコミットメントスキームは、限定を意図したものではないが、Pedersenコミットメント(PC)を含む。例えば、クライアントノードA302は、PCを使用してトランザクション金額tおよび乱数rに基づいてコミットメント値を生成する。例えば、コミットメント値は、PC(t)=rG+tHに従って取得することができる暗号文を含む、ここで、GおよびHは楕円曲線の生成元であり得るし、PC(t)は曲線の点についてのスカラ乗算であり、tはコミットされることになる値である。PCコミットメントスキームは準同型を有し、すなわち、$PC(t_1)+PC(t_2)=PC(t_1+t_2)$である。暗号文PC(t)の所持者は、乱数rを使用することによってトランザクション金額tを検証することができる。PCを参照して、本開示の実施形態を本明細書ではさらに詳細に説明しているが、本開示の実施形態が任意の適切なコミットメントスキームを使用して実現することができることは念頭に置かれたい。

【００６０】

例示的な機密トランザクションにおいて、クライアントノードA302は、トランザクション前のアカウント残高aおよび送金金額tをコミットし得る。いくつかの実施形態においては、クライアントノードA302は、トランザクション前のアカウント残高aおよび対応する乱数raに基づいてPCを使用してコミットメント値PC(a)を生成し得る。同様に、クライアントノードA302は、トランザクション前のアカウント残高tおよび対応する乱数rtに基づいてPCを使用してコミットメント値PC(t)を生成し得る。いくつかの実施形態においては、クライアントノードA302はまた、トランザクション後の残高a-tが0以上となるような十分な資金をそれが有していることをコミットし得る。例えば、クライアントノードA302は、例えば、PCの準同型の特性を前提としたコミットメント値PC(a)およびPC(t)に基づいて、コミットメント値PC(a-t)を生成し得る。コミットメント値は、機密トランザクションの内容に含まれ得る。

【００６１】

いくつかの実施形態においては、機密トランザクションの内容は、送信関係者が送信している情報が正当なものであることを受信関係者が確認することができるように、1つまたは複数のゼロ知識証明を含み得る。ゼロ知識証明は、確認される情報についての実際の知識がなくとも受信関係者がこれを行うことを可能にする。ゼロ知識証明は、Proof(a-t>0)、Proof(t>0)、およびProof(a>0)などといった範囲証明、または他のタイプの証明を含み得る。ゼロ知識証明は、受信関係者(例えば、クライアントノードB)が、金額が送金される元となる残高aを知らずともまたは送金金額tさえ知らずとも、送信関係者(例えば、クライアントノードA)が送金するのに十分な資金を有している(すなわち、a-t>0)ことおよび送金金額がゼロより大きいことを確認することを可能にする。

【００６２】

いくつかの実施形態においては、各Pedersenコミットメントに関して、乱数rおよび金額tは、暗号化されたトランザクション情報M=Akey(r,t)を得るために、秘密鍵Akeyを使用して暗号化され得る。暗号化されたトランザクション情報Mは、機密トランザクションの内容の一部として含まれ得る。

【００６３】

いくつかの実施形態においては、例示的な機密トランザクションの内容は、トランザクション上のAのデジタルシグニチャなどといった他のトランザクション関連情報を含み得る。

【００６４】

トランザクションの内容を生成した後に、クライアントノードA302は、機密トランザク

ションの内容をブロックチェーンネットワーク350(例えば、ブロックチェーンネットワーク350内の1つまたは複数のブロックチェーンノード312)に送信し得る。330において、ブロックチェーンネットワーク350が、機密トランザクションを実行し得る。いくつかの実施形態においては、機密トランザクションは、ブロックチェーンネットワーク350内のブロックチェーンノード312の各々によって実行され得る。例えば、ブロックチェーンノード312の各々は、例えば、機密トランザクションの内容に含まれるコミットメント値およびゼロ知識証明のうちの1つまたは複数を検証することによって、機密トランザクションの内容が正規のものであるかどうかを決定し得る。例えば、ブロックチェーンノード312の各々は、PC(a)=PC(t)+PC(a-t)、すなわち、インプットされたトランザクション値がアウトプットされたトランザクション値に等しいことを検証することによって、コミットメント値を検証し得る。ブロックチェーンノード312の各々は、例えば、Bulletproof、MoneroのRingCTアルゴリズム、または任意の他の適切なアルゴリズムに基づいて、ゼロ知識証明を検証し得る。

【００６５】

いくつかの実施形態においては、コミットメント値およびゼロ知識証明の検証が済んだ後に、ブロックチェーンノード312の各々は、トランザクションを記録し、クライアントノードA302およびクライアントノードB304のアカウントを更新することができる。例えば、トランザクション後には、クライアントノードA302はアカウント残高a-tを有し、クライアントノードB304はアカウント残高b+tを有する。いくつかの実施形態においては、クライアントノードA302とクライアントノードB304とのトランザクション後の残高は、コミットメントスキームの準同型に起因してコミットメント値の直接的な操作によって反映され得る。例えば、クライアントノードA302は、この時点では、トランザクション後のアカウント残高のコミットメント値PC(a-t)=PC(a)-PC(t)を有し得る。クライアントノードB304は、この時点では、トランザクション後のアカウント残高のコミットメント値PC(b+t)=PC(b)+PC(t)を有し得る。

【００６６】

いくつかの実施形態においては、ブロックチェーンノード312の各々は、暗号化されたトランザクション情報を記録または記憶し得る。例えば、コミットメントPC(a)、Ma=Akey(ra,a)に対応する暗号化されたトランザクション情報と、コミットメントPC(t)、Mt=Akey(rt,t)に対応する暗号化されたトランザクション情報とを、各ブロックチェーンノード312によってブロックチェーンに記録し得る、ここで、raおよびrtは、それぞれ、金額aおよびtに対応する乱数を表す。

【００６７】

図4は、本開示の実施形態による、機密トランザクションのトランザクション情報の例示的な復元プロセス400を示す図である。例えば、クライアントノードA302がその鍵Akeyを失ったケースにおいては、その結果、その対応するブロックチェーンアカウント上の金額が分からなくなる。クライアントノードA302は、例示的な復元プロセス400を使用してクライアントノードA302のアカウント金額を復元することができる。

【００６８】

410において、クライアントノードA302が、例えばブロックチェーンノード312からダウンロードすることによってまたはブロックチェーンノード312と同期することによって、Pedersenコミットメント(例えば、Ma=Akey(ra,a)およびMt=Akey(rt,t))の下で暗号化されたトランザクション情報を取得する。いくつかの実施形態においては、クライアントノードA302は、Pedersenコミットメントの下で暗号化されたトランザクション情報のローカルコピーを保存し得る。

【００６９】

420において、クライアントノードA302が、例えば、Shamir秘密分散法に従って、例えばブロックチェーンネットワーク350の鍵Akeyを復元するために、クライアントノードB304、C306、およびD308と通信し得る。

【００７０】

復元した鍵Akeyを用いて、430において、クライアントノードA302が、クライアントノードA302のアカウントの各Pedersenコミットメントに対応する暗号化されたトランザクション情報(例えば、Ma=Akey(ra,a)およびMt=Akey(rt,t))を復号し得る。その後、クライアントノードA302は、復元した鍵Akeyを使用して暗号化されたトランザクション情報(例えば、Ma=Akey(ra,a)およびMt=Akey(rt,t))を復号し、平文トランザクション情報ra、a、rt、およびtを取得し得る。

【００７１】

図5は、本開示の実施形態による、実行され得る例示的なプロセス500を図示している。いくつかの実施形態においては、例示的なプロセス500は、1つまたは複数のコンピューティングデバイスを使用して実行される1つまたは複数のコンピュータ実行可能プログラムを使用して行われ得る。概要説明を明確にするために、以下の説明では、本説明においては他の図に則して方法500を一般的に説明している。例えば、図3および図4を参照して説明したように、クライアントノード510はクライアントノードC306およびクライアントノードD312を含み得るし、ブロックチェーンノード520はブロックチェーンノード312であり得るし、クライアントノードA530はクライアントノードA302であり得るし、クライアントノードB540はクライアントノードB304であり得る。しかしながら、必要に応じて、例えば、任意の適切なシステム、環境、ソフトウェア、およびハードウェア、またはシステムと、環境と、ソフトウェアと、ハードウェアとの組合せによって、方法500を行い得ることを理解されよう。いくつかの実施形態においては、方法500の様々なステップは、並行して、組み合わせて、繰り返して、または任意の順序で実行され得る。

【００７２】

512において、ある数の(例えば、n個の)クライアントノード510が、ブロックチェーンネットワークのクライアントノード(例えば、クライアントノードA530)のための秘密鍵を生成する。いくつかの実施形態においては、秘密鍵は、すべての数のクライアントノード510によって合意された閾値秘密分散法に従ってすべての数の(例えば、n個の)クライアントノード510によって取り決めまたさもなければ生成され得る。いくつかの実施形態においては、閾値秘密分散法は、Shamirの秘密分散法を含む。

【００７３】

514において、ある数のクライアントノード510が、秘密鍵をクライアントノードA530に発行し得る。秘密鍵は、クライアントノードA530の機密トランザクションのトランザクション情報を暗号化および復号するためにクライアントノードA530によって使用され得る。

【００７４】

532において、クライアントノードA530が、すべての数のクライアントノード510(例えば、秘密分散法のすべての数の参加者)によって合意された閾値秘密分散法に従って秘密鍵を取得する。クライアントノードA530は、クライアントノードA530の秘密鍵を使用してクライアントノードA530の機密トランザクションのトランザクションデータを暗号化し得る。クライアントノードA530の機密トランザクションは、例えば、クライアントノードA530のアカウントからクライアントノードB540のアカウントへの資金の金額の送金などといった、機密トランザクション535であり得る。クライアントノードA530は、トランザクションの参加者(すなわち、本例においてはクライアントノードA530およびクライアントノードB540)を除く他のエンティティによる調査からトランザクションデータのプライバシーを保護するとともにトランザクションデータを秘匿するように、機密トランザクションの内容を構築し得る。いくつかの実施形態においては、クライアントノードA530は、閾値秘密分散法に従って取得した秘密鍵を使用してコミットメントスキームに基づいて機密トランザクションのトランザクションデータを秘匿し得る。

【００７５】

いくつかの実施形態においては、機密トランザクションのトランザクションデータは、機密トランザクションの前のクライアントノードA530のアカウント残高または機密トランザクションのトランザクション金額の一方または両方を含む。いくつかの実施形態においては、機密トランザクションのトランザクションデータは、追加のトランザクション情報

(例えば、トランザクションの時間、トランザクションの関係者、アセットタイプ(例えば、株式証券または他のタイプ))を含み得る。

【００７６】

534において、クライアントノードA530が、機密トランザクションのトランザクションデータに暗号コミットメントスキームを適用することによってクライアントノードA530の機密トランザクションの1つまたは複数のコミットメント値を生成する。いくつかの実施形態においては、暗号コミットメントスキームは、Pedersenコミットメントスキームまたは別のタイプのコミットメントスキームなどといった準同型暗号コミットメントスキームを含む。

【００７７】

536において、クライアントノードA530が、クライアントノードA530の秘密鍵を使用してトランザクションデータを暗号化することによって機密トランザクションの暗号化されたトランザクション情報を生成する、ここで、暗号化されたトランザクション情報は、秘密鍵を使用したクライアントノードA530による復号を可能にするように構成される。

【００７８】

いくつかの実施形態においては、暗号コミットメントスキームは、Pedersenコミットメントスキームを含む。この場合には、暗号コミットメントスキームをトランザクションデータに適用することによってクライアントノードの機密トランザクションの1つまたは複数のコミットメント値を生成するステップは、トランザクションデータおよびトランザクションデータに対応する乱数に基づいてクライアントノードの機密トランザクションの1つまたは複数のコミットメント値を生成するステップを含み、機密トランザクションの暗号化されたトランザクション情報を生成するステップは、クライアントノードA530の秘密鍵を使用してトランザクションデータおよびトランザクションデータに対応する乱数を暗号化することによって機密トランザクションの暗号化されたトランザクション情報を生成するステップを含む。

【００７９】

538において、クライアントノードA530が、例えば機密トランザクションの内容をブロックチェーンノード520(例えば、ブロックチェーンネットワークのコンセンサスノード)に送信することによって、実行のためにブロックチェーンネットワークに機密トランザクションの内容を送信する。いくつかの実施形態においては、機密トランザクションの内容は、暗号コミットメントスキームを機密トランザクションのトランザクションデータに適用することによってクライアントノードA530によって生成された機密トランザクションの1つまたは複数のコミットメント値と、秘密鍵を使用してトランザクションデータを暗号化することによってクライアントノードA530によって生成された暗号化されたトランザクション情報と、トランザクションデータの1つまたは複数のゼロ知識証明とを含み得る。

【００８０】

いくつかの実施形態においては、トランザクションデータの1つまたは複数のゼロ知識証明は、トランザクションデータの値がそれぞれの範囲内にあるという1つまたは複数のゼロ知識範囲証明を含む。例えば、1つまたは複数のゼロ知識範囲証明は、機密トランザクションの前のクライアントノードA530のアカウント残高がゼロより大きいというゼロ知識範囲証明と、機密トランザクションのトランザクション金額がゼロより大きいというゼロ知識範囲証明と、トランザクション金額が機密トランザクションの前のクライアントノードA530のアカウント残高以下であるというゼロ知識範囲証明とを含み得る。

【００８１】

いくつかの実施形態においては、機密トランザクションの内容は、クライアントノードA530のデジタルシグニチャをさらに含む。いくつかの実施形態においては、機密トランザクションの内容は、追加のまたは異なる情報を含み得る。

【００８２】

522において、機密トランザクションの内容を受信する際に、ブロックチェーンノード520が、例えば機密トランザクションの内容に基づいて機密トランザクションが正当なもの

であることを検証することによって、機密トランザクションを実行し得る。いくつかの実施形態においては、機密トランザクションの内容に基づいて機密トランザクションが正当なものであることを検証することは、コミットメントスキームおよび/または1つまたは複数のゼロ知識証明に基づいて1つまたは複数のコミットメント値が正しいと決定すること、または、例えば図3を参照して説明したようなアルゴリズムに従ってトランザクションデータの1つまたは複数のゼロ知識証明を検証することのうちの1つまたは複数を含み得る。

【００８３】

524において、機密トランザクションが正当なものであることを検証した後に、ブロックチェーンノード520が、機密トランザクションによってもたらされるアカウント情報(例えば、クライアントノードA530およびクライアントノードB540のアカウント残高)を更新し得る。いくつかの実施形態においては、暗号コミットメントスキームは、準同型であり、ブロックチェーンノード520は、例えば図3を参照して説明した技法または他の技法に従って、コミットメントスキームの準同型に基づいてアカウント情報を更新し得る。

【００８４】

526において、ブロックチェーンノード520が、ブロックチェーンネットワークのブロックチェーン上に暗号化されたトランザクション情報を記憶し得る。いくつかの実施形態においては、暗号化されたトランザクション情報は、ブロックチェーンネットワークの2個以上/すべてのコンセンサスノードに記憶され得る、そのため、クライアントノードA530が秘密鍵を失うケースにおけるクライアントノードA530の暗号化されたトランザクション情報についてのロバストなバックアップを提供している。加えて、ブロックチェーンネットワークのブロックチェーンに暗号化されたトランザクション情報を記憶することは、ローカルまたはシングルポイントストレージスキームに対するクライアントノードA530の依存を低減または排除することができ、暗号化されたトランザクション情報へのクライアントノードA530のアクセスについてのセキュリティおよび信頼性を改善している。

【００８５】

528において、クライアントノードA530が、ブロックチェーンノード520(例えば、ブロックチェーンネットワークのコンセンサスノード)から暗号化されたトランザクション情報を読み出しまたさもなければ取得し得る。暗号化されたトランザクション情報は、ブロックチェーンネットワーク内の少なくとも1つのブロックチェーンに記憶されている。クライアントノードA530は、秘密鍵を使用して暗号化されたトランザクション情報から平文トランザクション情報を復号し得る。

【００８６】

542において、クライアントノードA530が、暗号化されたトランザクション情報を復号するように構成される秘密鍵へのアクセスをそれが失っているまたさもなければ有しておらず、秘密鍵がクライアントノードA530に以前発行されていたと決定する。

【００８７】

544において、いくつかの実施形態においては、そのような決定に応答して、クライアントノードA530が、例えばブロックチェーンネットワーク内のすべての数のクライアントノードのうちの少なくとも閾値の数のクライアントノードから秘密鍵の少なくとも閾値の数のパーツを復元することによって、複数のクライアントノードによって合意された閾値秘密分散法(例えばShamirの秘密分散法)に従って、ブロックチェーンネットワーク内のすべての数の(例えば、n個の)クライアントノードのうちの少なくとも閾値の数の(例えば、k個の)クライアントノードから秘密鍵を復元する。

【００８８】

546において、クライアントノードA530が、復元した秘密鍵を使用して暗号化されたトランザクション情報からクライアントノードA530の機密トランザクションのトランザクションデータ(例えば、平文トランザクションデータ)を復号する。いくつかの実施形態においては、秘密鍵を使用して暗号化されたトランザクション情報から特定のクライアントノードの機密トランザクションのトランザクションデータを復号するステップは、秘密鍵を

使用して機密トランザクションの送金金額を復元するステップを含む。いくつかの実施形態においては、秘密鍵を使用して暗号化されたトランザクション情報から特定のクライアントノードの機密トランザクションのトランザクションデータを復号するステップは、秘密鍵を使用して機密トランザクションの送金金額および送金金額に対応する乱数の両方を復元するステップであって、送金金額および乱数は、特定のクライアントノードの機密トランザクションのトランザクション情報を秘匿するためにPedersenコミットメントスキームにおいて使用される、ステップを含む。

【００８９】

説明した特徴は、デジタル電子回路の形式で、またはコンピュータハードウェア、ファームウェア、ソフトウェアの形式で、またはそれらの組合せで実装され得る。装置は、プログラマブルプロセッサによる実行のために情報媒体に有形に具現化されたコンピュータプログラム製品の形式で(例えば、機械可読ストレージデバイスの形式で)実装されてもよく、方法のステップは、入力データに対する処理をして出力を生成することによって説明した実施形態の機能を行う命令についてのプログラムを実行するプログラマブルプロセッサによって行われ得る。説明した特徴は、データストレージシステムからデータおよび命令を受信するとともにデータストレージシステムにデータおよび命令を送信するために結合された少なくとも1つのプログラマブルプロセッサ、少なくとも1つの入力デバイス、および少なくとも1つの出力デバイスを含むプログラマブルシステム上で実行可能な1つまたは複数のコンピュータプログラムの形式で有利に実装され得る。コンピュータプログラムは、あるアクティビティを行うためにコンピュータにおいて直接的または間接的に使用され得る、または、ある結果をもたらし得る、命令のセットである。コンピュータプログラムは、コンパイル型またはインタプリタ型言語を含むプログラミング言語の任意の形式で書かれてもよく、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、もしくはコンピューティング環境における使用に適した他のユニットとして、ということを含む任意の形式で、デプロイされ得る。

【００９０】

命令についてのプログラムの実行に適したプロセッサは、例として、汎用および特殊用途マイクロプロセッサの両方、および任意の種類のコンピュータの単一プロセッサまたはマルチプルプロセッサの1つを含む。一般的に、プロセッサは、リードオンリーメモリまたはランダムアクセスメモリまたはその両方から命令およびデータを受信することになる。コンピュータの要素は、命令を実行するためのプロセッサと、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とを含み得る。一般的に、コンピュータはまた、データファイルを記憶するための1つまたは複数のマスストレージデバイスを含み得る、またはそのようなデバイスと通信するように動作可能なように結合されてもよく、そのようなデバイスは、内蔵型ハードディスクおよびリムーバブルディスクなどの磁気ディスク、光磁気ディスク、および光ディスクを含む。コンピュータプログラム命令およびデータを有形に具現化するのに適したストレージデバイスは、例として、EPROM、EEPROM、およびフラッシュメモリデバイスなどの半導体メモリデバイス、内蔵型ハードディスクおよびリムーバブルディスクなどの磁気ディスク、光磁気ディスク、ならびにCD-ROMおよびDVD-ROMディスクを含む、すべての形式の不揮発性メモリを含む。プロセッサおよびメモリは、特定用途向け集積回路(ASIC)によって補完または組み込まれていてもよい。

【００９１】

クライアントとのインタラクションを提供するために、前記特徴は、クライアントノードA302に情報を表示するための陰極線管(CRT)または液晶ディスプレイ(LCD)モニタなどの表示デバイスと、クライアントがコンピュータに入力を提供し得るキーボードおよびマウスまたはトラックボールなどのポインティングデバイスとを有するコンピュータ上で実装され得る。

【００９２】

前記特徴は、データサーバなどのバックエンドコンポーネントを含む、または、アプリケーションサーバもしくはインターネットサーバなどのミドルウェアコンポーネントを含

む、または、グラフィッククライアントインターフェースを有するクライアントコンピュータもしくはインターネットブラウザなどのフロントエンドコンポーネントを含む、または、それらの任意の組合せを含む、コンピュータシステムの形式で実装され得る。システムのコンポーネントは、通信ネットワークなどのデジタルデータ通信の任意の形式または媒体によって接続され得る。通信ネットワークの例としては、例えば、ローカルエリアネットワーク(LAN)と、ワイドエリアネットワーク(WAN)とを含み、コンピュータとネットワークとがインターネットを形成する。

【００９３】

コンピュータシステムは、クライアントとサーバとを含み得る。クライアントノードA302とサーバとは、一般的に互いにリモートにあり、通常は上述したようなネットワークを介してやりとりする。クライアントノードA302とサーバとの関係は、それぞれのコンピュータ上で動作し互いにクライアントサーバ関係を有するコンピュータプログラムによって生まれる。

【００９４】

加えて、図に示したロジックフローは、望ましい結果を得るために図示した特定の順序または一連の順序を必要としていない。加えて、他のステップが提供されてもよいし、またはステップが説明したフローから除去されてもよいし、他のコンポーネントが説明したシステムに追加されても削除されてもよい。それゆえ、他の実施形態も特許請求の範囲の範囲内にある。

【００９５】

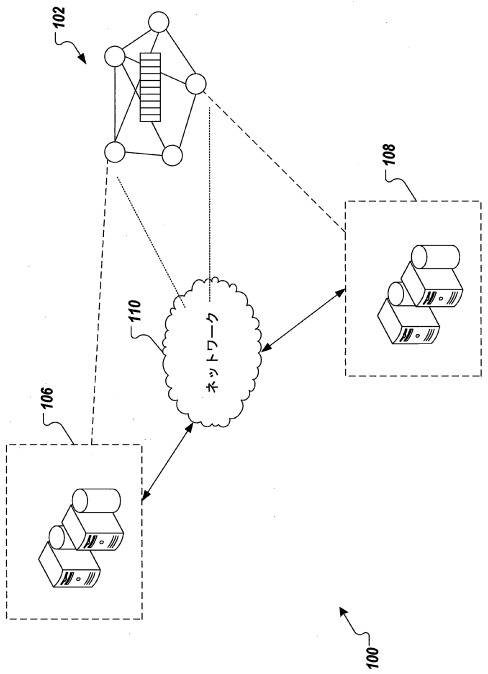
多くの本開示の実施形態を説明してきた。しかしながら、本開示の精神および範囲から逸脱しない限り様々な変更をしてもよいことは理解されよう。それゆえ、他の実施形態も特許請求の範囲の範囲内にある。

【符号の説明】

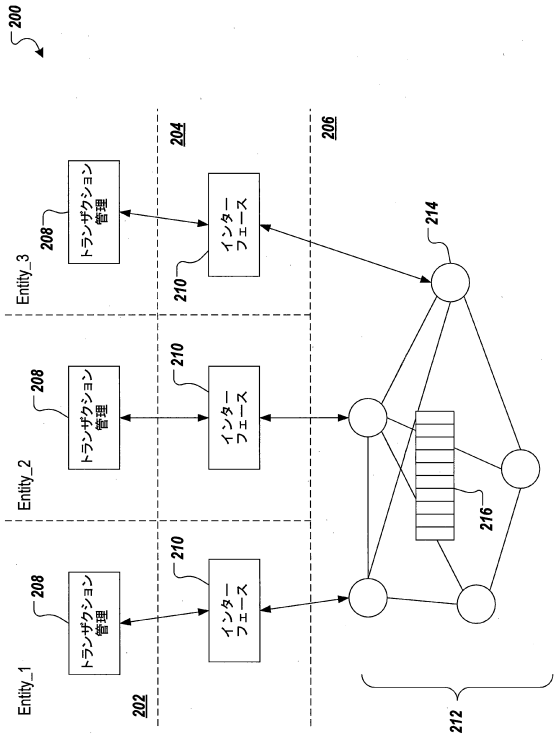
【００９６】

102　コンソーシアムブロックチェーンネットワーク
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　ホステッドサービスレイヤ
206　ブロックチェーンネットワークレイヤ
208　トランザクション管理システム
210　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　クライアントノードA
304　クライアントノードB
306　クライアントノードC
308　クライアントノードD
312　ブロックチェーンノード
350　ブロックチェーンネットワーク
510　クライアントノード
520　ブロックチェーンノード
530　クライアントノードA
540　クライアントノードB

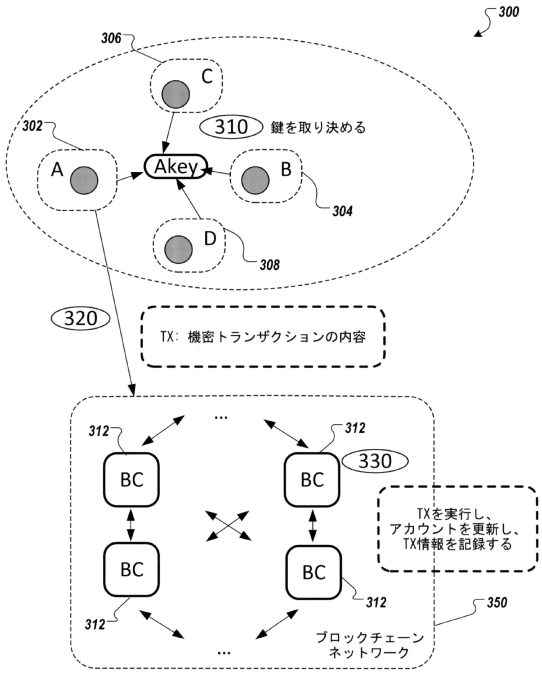
【図１】


102
108
110
ネットワーク
106
100

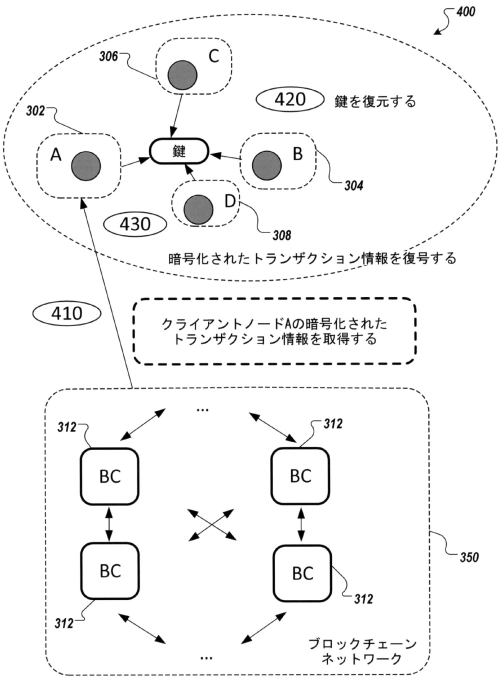
【図２】


200
204
206
トランザクション管理
インターフェース
208
210
214
Entity_3
Entity_2
Entity_1
216
202
212

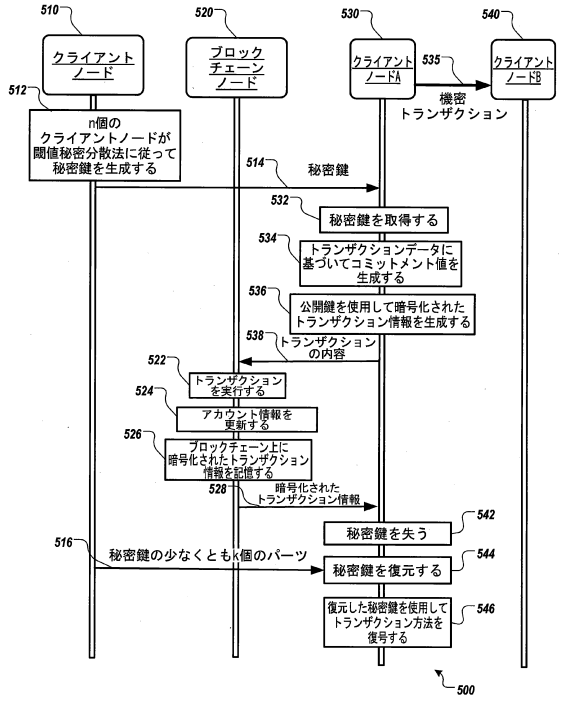
【図３】


300
306
C
310 鍵を取り決める
302
A
Akey
B
304
D
308
320
TX: 機密トランザクションの内容
312
BC
330
TXを実行し、
アカウントを更新し、
TX情報を記録する
350
ブロックチェーン
ネットワーク

【図４】


400
306
C
420 鍵を復元する
302
A
鍵
B
304
D
308
430
暗号化されたトランザクション情報を復号する
410
クライアントノードAの暗号化された
トランザクション情報を取得する
312
BC
350
ブロックチェーン
ネットワーク

【図５】


510
520
530
540
クライアントノード
ブロックチェーンノード
クライアントノードA
535
クライアントノードB
機密トランザクション
512
n個のクライアントノードが閾値秘密分散法に従って秘密鍵を生成する
514
秘密鍵
532
秘密鍵を取得する
534
トランザクションデータに基づいてコミットメント値を生成する
536
公開鍵を使用して暗号化されたトランザクション情報を生成する
538
トランザクションの内容
522
トランザクションを実行する
524
アカウント情報を更新する
526
ブロックチェーン上に暗号化されたトランザクション情報を記憶する
528
暗号化されたトランザクション情報
542
秘密鍵を失う
516
秘密鍵の少なくともk個のパーツ
544
秘密鍵を復元する
546
復元した秘密鍵を使用してトランザクション方法を復号する
500

フロントページの続き

(72)発明者　ジェン・リュウ
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　リチュン・リ
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　シャン・イン
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

審査官　児玉　崇晶

(56)参考文献　米国特許出願公開第２０１６／０３５８１６５（ＵＳ，Ａ１）
国際公開第２０１８／１０９０１０（ＷＯ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　２１／６４
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／０８