(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6714156号
(P6714156)

(45)発行日　令和2年6月24日(2020.6.24)　(24)登録日　令和2年6月8日(2020.6.8)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675Z
G06Q 20/38	(2012.01)	G06Q	20/38	310
G06F 21/60	(2013.01)	G06F	21/60	320

請求項の数 23　(全 32 頁)

(21)出願番号	特願2019-520853(P2019-520853)
(86)(22)出願日	平成30年11月27日(2018.11.27)
(65)公表番号	特表2020-507222(P2020-507222A)
(43)公表日	令和2年3月5日(2020.3.5)
(86)国際出願番号	PCT/CN2018/117558
(87)国際公開番号	WO2019/072277
(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7月30日(2019.7.30)
早期審査対象出願	

(73)特許権者　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　100099759
弁理士　青木　篤
(74)代理人　100123582
弁理士　三橋　真二
(74)代理人　100114018
弁理士　南山　知広

最終頁に続く

(54)【発明の名称】情報保護のためのシステム及び方法

(57)【特許請求の範囲】

【請求項１】

情報保護のためのコンピュータで実施される方法であって、

トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームに取引金額ｔの取引をコミットし、チェンジコミットメント値Ｙを取得するために第２のコミットメントスキームにチェンジｙの取引をコミットし、前記第１のコミットメントスキームは、トランザクションブラインディングファクタr_tを備え、前記第２のコミットメントスキームは、チェンジブラインディングファクタr_yを備えることと、

前記チェンジブラインディングファクタr_yと前記チェンジｙの第１の組合せを第１の鍵ＫＡによって暗号化することと、

前記取引の着信者に関連する着信者ノードが前記取引を確認するために、前記トランザクションブラインディングファクタr_t、前記取引金額ｔ及び前記トランザクションコミットメント値Ｔを前記着信者ノードに送信することと、

前記着信者ノードの前記取引の確認の成功に応答して、第２の鍵ＫＢによって暗号化された前記トランザクションブラインディングファクタr_t及び前記取引金額ｔの暗号化された第２の組合せを取得することと、

ブロックチェーンの複数のノードが前記取引を確認するために、暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送信することと、

を備える方法。

【請求項２】
前記第１のコミットメントスキームは、少なくとも前記トランザクションブラインディングファクタr_tに基づくとともに前記取引金額ｔが対応するコミッテッド値であるペダーソンコミットメントを備え、
前記第２のコミットメントスキームは、少なくとも前記チェンジブラインディングファクタr_yに基づくとともに前記チェンジｙが対応するコミッテッド値であるペダーソンコミットメントを備える請求項１に記載の方法。
【請求項３】
前記取引の着信者に関連する着信者ノードが前記取引を確認するために、前記トランザクションブラインディングファクタr_t、前記取引金額ｔ及び前記トランザクションコミットメント値Ｔを前記着信者ノードに送信することは、
前記トランザクションブラインディングファクタr_t、前記取引金額ｔ及び前記トランザクションコミットメント値Ｔを前記着信者ノードに送信することによって、前記着信者ノードは、前記トランザクションコミットメント値Ｔが前記取引金額ｔを前記トランザクションブラインディングファクタr_tにコミットする前記第１のコミットメントスキームに等しいか否かを確認することを備える請求項１に記載の方法。
【請求項４】
暗号化された第２の組合せを取得することは、暗号化された前記第２の組合せと、暗号化された前記第２の組合せ及び前記トランザクションコミットメント値Ｔに関連する署名ＳＩＧＢを前記着信者ノードから受け取ることを備える請求項１に記載の方法。
【請求項５】
前記取引金額ｔは、前記取引の発信者の一つ以上の資産A_1，A_2，．．．，A_kから選ばれ、
前記資産の各々は、（１）少なくとも各資産のブラインディングファクタr_{a_k}及び値に基づくペダーソンコミットメント及び（２）少なくとも各資産の前記ブラインディングファクタr_{a_k}及び値に基づく暗号化に関連し、
前記チェンジｙは、前記取引金額ｔと選ばれた資産の間の差である請求項４に記載の方法。
【請求項６】
暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送信する前に、
前記署名ＳＩＧＢを確認することと、
前記署名ＳＩＧＢの確認の成功に応答して、前記資産A_1，A_2，．．．，A_k、前記第１の組合せ、前記第２の組合せ、前記トランザクションコミットメント値Ｔ、前記チェンジコミットメント値Ｙ及び前記資産A_1，A_2，．．．，A_kに対応するブラインディングファクタの和と前記トランザクションブラインディングファクタr_t及び前記チェンジブラインディングファクタr_yの和との差に関連する署名ＳＩＧＡを生成することと、
を更に備える請求項５に記載の方法。
【請求項７】
暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送信することは、
前記資産A_1，A_2，．．．，A_k、前記第１の組合せ、前記第２の組合せ、前記トランザクションコミットメント値Ｔ、前記チェンジコミットメント値Ｙ及び前記資産A_1，A_2，．．．，A_kに対応するブラインディングファクタの和と前記トランザクションブラインディングファクタr_t、前記チェンジブラインディングファクタr_yの和との差、前記署名ＳＩＧＡ及び前記署名ＳＩＧＢを、前記ブロックチェーンの複数のノードに送信すること備える請求項６に記載の方法。
【請求項８】
ブロックチェーンの複数のノードが前記取引を確認するために、暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送

信することは、
暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送信することによって、前記ブロックチェーンの複数のノードは、前記取引の確認の成功に応答して、前記着信者に前記取引金額ｔを発し、前記資産A_1，A_2，．．．，A_kを削除し、前記発信者に前記チェンジｙを発することを備える請求項７に記載の方法。
【請求項９】
プロセッサによって実行するときに、
トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームに取引金額ｔの取引をコミットし、チェンジコミットメント値Ｙを取得するために第２のコミットメントスキームにチェンジｙの取引をコミットし、前記第１のコミットメントスキームは、トランザクションブラインディングファクタr_tを備え、前記第２のコミットメントスキームは、チェンジブラインディングファクタr_yを備えることと、
前記チェンジブラインディングファクタr_yと前記チェンジｙの第１の組合せを第１の鍵ＫＡによって暗号化することと、
前記取引の着信者に関連する着信者ノードが前記取引を確認するために、前記トランザクションブラインディングファクタr_t、前記取引金額ｔ及び前記トランザクションコミットメント値Ｔを前記着信者ノードに送信することと、
前記着信者ノードの前記取引の確認の成功に応答して、第２の鍵ＫＢによって暗号化された前記トランザクションブラインディングファクタr_t及び前記取引金額ｔの暗号化された第２の組合せを取得することと、
ブロックチェーンの複数のノードが前記取引を確認するために、暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送信することと、
を備える動作を前記プロセッサによって実行させる命令を記憶する非一時的コンピュータ可読記憶媒体。
【請求項１０】
前記第１のコミットメントスキームは、少なくとも前記トランザクションブラインディングファクタr_tに基づくとともに前記取引金額ｔが対応するコミッテッド値であるペダーソンコミットメントを備え、
前記第２のコミットメントスキームは、少なくとも前記チェンジブラインディングファクタr_yに基づくとともに前記チェンジｙが対応するコミッテッド値であるペダーソンコミットメントを備える請求項９に記載の非一時的コンピュータ可読記憶媒体。
【請求項１１】
前記取引の着信者に関連する着信者ノードが前記取引を確認するために、前記トランザクションブラインディングファクタr_t、前記取引金額ｔ及び前記トランザクションコミットメント値Ｔを前記着信者ノードに送信することは、
前記トランザクションブラインディングファクタr_t、前記取引金額ｔ及び前記トランザクションコミットメント値Ｔを前記着信者ノードに送信することによって、前記着信者ノードは、前記トランザクションコミットメント値Ｔが前記取引金額ｔを前記トランザクションブラインディングファクタr_tにコミットする前記第１のコミットメントスキームに等しいか否かを確認することを備える請求項９に記載の非一時的コンピュータ可読記憶媒体。
【請求項１２】
暗号化された第２の組合せを取得することは、暗号化された前記第２の組合せと、暗号化された前記第２の組合せ及び前記トランザクションコミットメント値Ｔに関連する署名ＳＩＧＢを前記着信者ノードから受け取ることを備える請求項９に記載の非一時的コンピュータ可読記憶媒体。
【請求項１３】
前記取引金額ｔは、前記取引の発信者の一つ以上の資産A_1，A_2，．．．，A_kから

選ばれ、
前記資産の各々は、（１）少なくとも各資産のブラインディングファクタr_{a_k}及び値に基づくペダーソンコミットメント及び（２）少なくとも各資産の前記ブラインディングファクタr_{a_k}及び値に基づく暗号化に関連し、
前記チェンジｙは、前記取引金額ｔと選ばれた資産の間の差である請求項１２に記載の非一時的コンピュータ可読記憶媒体。
【請求項１４】
暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送信する前に、
前記署名ＳＩＧＢを確認することと、
前記署名ＳＩＧＢの確認の成功に応答して、前記資産A_1，A_2，．．．，A_k、前記第１の組合せ、前記第２の組合せ、前記トランザクションコミットメント値Ｔ、前記チェンジコミットメント値Ｙ及び前記資産A_1，A_2，．．．，A_kに対応するブラインディングファクタの和と前記トランザクションブラインディングファクタr_t及び前記チェンジブラインディングファクタr_yの和との差に関連する署名ＳＩＧＡを生成することと、
を更に備える請求項１３に記載の非一時的コンピュータ可読記憶媒体。
【請求項１５】
暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送信することは、
前記資産A_1，A_2，．．．，A_k、前記第１の組合せ、前記第２の組合せ、前記トランザクションコミットメント値Ｔ、前記チェンジコミットメント値Ｙ及び前記資産A_1，A_2，．．．，A_kに対応するブラインディングファクタの和と前記トランザクションブラインディングファクタr_t、前記チェンジブラインディングファクタr_yの和との差、前記署名ＳＩＧＡ及び前記署名ＳＩＧＢを、前記ブロックチェーンの複数のノードに送信すること備える請求項１４に記載の非一時的コンピュータ可読記憶媒体。
【請求項１６】
ブロックチェーンの複数のノードが前記取引を確認するために、暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送信することは、
暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送信することによって、前記ブロックチェーンの複数のノードは、前記取引の確認の成功に応答して、前記着信者に前記取引金額ｔを発し、前記資産A_1，A_2，．．．，A_kを削除し、前記発信者に前記チェンジｙを発することを備える請求項１５に記載の非一時的コンピュータ可読記憶媒体。
【請求項１７】
情報保護のためのシステムであって、プロセッサ及び前記プロセッサに結合された非一時的コンピュータ可読記憶媒体を備え、前記非一時的コンピュータ可読記憶媒体は、前記プロセッサによって実行するときに、
トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームに取引金額ｔの取引をコミットし、チェンジコミットメント値Ｙを取得するために第２のコミットメントスキームにチェンジｙの取引をコミットし、前記第１のコミットメントスキームは、トランザクションブラインディングファクタr_tを備え、前記第２のコミットメントスキームは、チェンジブラインディングファクタr_yを備えることと、
前記チェンジブラインディングファクタr_yと前記チェンジｙの第１の組合せを第１の鍵ＫＡによって暗号化することと、
前記取引の着信者に関連する着信者ノードが前記取引を確認するために、前記トランザクションブラインディングファクタr_t、前記取引金額ｔ及び前記トランザクションコミットメント値Ｔを前記着信者ノードに送信することと、
前記着信者ノードの前記取引の確認の成功に応答して、第２の鍵ＫＢによって暗号化された前記トランザクションブラインディングファクタr_t及び前記取引金額ｔの暗号化さ

れた第２の組合せを取得することと、
ブロックチェーンの複数のノードが前記取引を確認するために、暗号化された前記第１の組合せ及び暗号化された前記第２の組合せを前記ブロックチェーンの複数のノードに送信することと、
を備える動作を前記プロセッサによって実行させる命令を記憶するシステム。
【請求項１８】
情報保護のためのコンピュータで実施される方法であって、
トランザクションブラインディングファクタr_t、取引金額ｔの取引及びトランザクションコミットメント値Ｔを取引の発信者に関連する発信者ノードから取得し、前記取引金額ｔは、前記トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームにコミットされ、前記第１のコミットメントスキームは、前記トランザクションブラインディングファクタr_tを備えることと、
取得した前記トランザクションブラインディングファクタr_t、取得した前記取引金額ｔの取引及び取得した前記トランザクションコミットメント値Ｔに基づいて前記取引を確認することと、
前記取引の確認の成功に応答して、前記トランザクションブラインディングファクタr_t及び前記取引金額ｔの第２の組合せを第２の鍵ＫＢによって暗号化することと、
暗号化された前記第２の組合せを前記発信者ノードに送信することと、
を備える方法。
【請求項１９】
取得した前記トランザクションブラインディングファクタr_t、取得した前記取引金額ｔの取引及び取得した前記トランザクションコミットメント値Ｔに基づいて前記取引を確認することは、前記トランザクションコミットメント値Ｔが前記取引金額ｔを取得した前記トランザクションブラインディングファクタr_tにコミットする前記第１のコミットメントスキームに等しいか否かを確認することを備える請求項１８に記載の方法。
【請求項２０】
暗号化された前記第２の組合せを前記発信者ノードに送信する前に、
暗号化された前記第２の組合せ及び前記トランザクションコミットメント値Ｔに関連する署名ＳＩＧＢを生成することを更に備え、
暗号化された前記第２の組合せを前記発信者ノードに送信することは、暗号化された前記第２の組合せ及び前記署名ＳＩＧＢを前記発信者ノードに送信すること備える請求項１８に記載の方法。
【請求項２１】
前記第１のコミットメントスキームは、少なくとも前記トランザクションブラインディングファクタr_tに基づくとともに前記取引金額ｔが対応するコミッテッド値であるペダーソンコミットメントを備える請求項１８に記載の方法。
【請求項２２】
プロセッサによって実行するときに、
トランザクションブラインディングファクタr_t、取引金額ｔの取引及びトランザクションコミットメント値Ｔを取引の発信者に関連する発信者ノードから取得し、前記取引金額ｔは、前記トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームにコミットされ、前記第１のコミットメントスキームは、前記トランザクションブラインディングファクタr_tを備えることと、
取得した前記トランザクションブラインディングファクタr_t、取得した前記取引金額ｔの取引及び取得した前記トランザクションコミットメント値Ｔに基づいて前記取引を確認することと、
前記取引の確認の成功に応答して、前記トランザクションブラインディングファクタr_t及び前記取引金額ｔの第２の組合せを第２の鍵ＫＢによって暗号化することと、
暗号化された前記第２の組合せを前記発信者ノードに送信することと、
を備える動作を前記プロセッサによって実行させる命令を記憶する非一時的コンピュー

タ可読記憶媒体。
【請求項２３】
情報保護のためのシステムであって、プロセッサ及び前記プロセッサに結合された非一時的コンピュータ可読記憶媒体を備え、前記非一時的コンピュータ可読記憶媒体は、前記プロセッサによって実行するときに、
トランザクションブラインディングファクタr_t、取引金額ｔの取引及びトランザクションコミットメント値Ｔを取引の発信者に関連する発信者ノードから取得し、前記取引金額ｔは、前記トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームにコミットされ、前記第１のコミットメントスキームは、前記トランザクションブラインディングファクタr_tを備えることと、
取得した前記トランザクションブラインディングファクタr_t、取得した前記取引金額ｔの取引及び取得した前記トランザクションコミットメント値Ｔに基づいて前記取引を確認することと、
前記取引の確認の成功に応答して、前記トランザクションブラインディングファクタr_t及び前記取引金額ｔの第２の組合せを第２の鍵ＫＢによって暗号化することと、
暗号化された前記第２の組合せを前記発信者ノードに送信することと、
を備える動作を前記プロセッサによって実行させる命令を記憶するシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、一般的には、情報保護のための方法及び装置に関する。
【背景技術】
【０００２】
プライバシーは、種々のユーザの間の通信及びデータ転送に重要である。保護がない場合、ユーザは、なりすまし犯罪、不正転送（ｉｌｌｅｇａｌ　ｔｒａｎｓｆｅｒ）又は他の潜在的損失のリスクにさらされる。リスクは、通信及び転送がオンラインで実現されるときにはオンライン情報のフリーアクセスのために更に高くなる。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
本開示の種々の実施の形態は、情報保護のためのシステム、方法及び非一時的コンピュータ可読媒体を有する。
【課題を解決するための手段】
【０００４】
一態様によれば、情報保護のためのコンピュータで実施される方法であって、トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームに取引金額ｔの取引をコミットし、チェンジコミットメント値Ｙを取得するために第２のコミットメントスキームにチェンジｙの取引をコミットし、第１のコミットメントスキームは、トランザクションブラインディングファクタr_tを備え、第２のコミットメントスキームは、チェンジブラインディングファクタr_yを備えることと、チェンジブラインディングファクタr_yとチェンジｙの第１の組合せを第１の鍵ＫＡによって暗号化することと、取引の着信者に関連する着信者ノードが取引を確認するために、トランザクションブラインディングファクタr_t、取引金額ｔ及びトランザクションコミットメント値Ｔを着信者ノードに送信することと、着信者ノードの取引の確認の成功に応答して、第２の鍵ＫＢによって暗号化されたトランザクションブラインディングファクタr_t及び取引金額ｔの暗号化された第２の組合せを取得することと、ブロックチェーンの複数のノードが取引を確認するために、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信することと、を備える。
【０００５】
一部の実施の形態において、第１のコミットメントスキームは、少なくともトランザク

ションブラインディングファクタr_tに基づくとともに取引金額ｔが対応するコミッテッド値であるペダーソンコミットメントを備え、第２のコミットメントスキームは、少なくともチェンジブラインディングファクタr_yに基づくとともにチェンジｙが対応するコミッテッド値であるペダーソンコミットメントを備える。

【０００６】

一部の実施の形態において、取引の着信者に関連する着信者ノードが取引を確認するために、トランザクションブラインディングファクタr_t、取引金額ｔ及びトランザクションコミットメント値Ｔを着信者ノードに送信することは、トランザクションブラインディングファクタr_t、取引金額ｔ及びトランザクションコミットメント値Ｔを着信者ノードに送信することによって、着信者ノードは、トランザクションコミットメント値Ｔが取引金額ｔをトランザクションブラインディングファクタr_tにコミットする第１のコミットメントスキームに等しいか否かを確認することを備える。

【０００７】

一部の実施の形態において、暗号化された第２の組合せを取得することは、暗号化された第２の組合せと、暗号化された第２の組合せ及びトランザクションコミットメント値Ｔに関連する署名ＳＩＧＢを着信者ノードから受け取ることを備える。

【０００８】

一部の実施の形態において、取引金額ｔは、取引の発信者の一つ以上の資産A_1，A_2，．．．，A_kから選ばれ、資産の各々は、（１）少なくとも各資産のブラインディングファクタr_{a_k}及び値に基づくペダーソンコミットメント及び（２）少なくとも各資産のブラインディングファクタr_{a_k}及び値に基づく暗号化に関連し、チェンジｙは、取引金額ｔと選ばれた資産の間の差である。

【０００９】

一部の実施の形態において、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信する前に、方法は、署名ＳＩＧＢを確認することと、署名ＳＩＧＢの確認の成功に応答して、資産A_1，A_2，．．．，A_k、第１の組合せ、第２の組合せ、トランザクションコミットメント値Ｔ、チェンジコミットメント値Ｙ及び資産A_1，A_2，．．．，A_kに対応するブラインディングファクタの和とトランザクションブラインディングファクタr_t及びチェンジブラインディングファクタr_yの和との差に関連する署名ＳＩＧＡを生成することと、を更に備える。

【００１０】

一部の実施の形態において、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信することは、資産A_1，A_2，．．．，A_k、第１の組合せ、第２の組合せ、トランザクションコミットメント値Ｔ、チェンジコミットメント値Ｙ及び資産A_1，A_2，．．．，A_kに対応するブラインディングファクタの和とトランザクションブラインディングファクタr_t、チェンジブラインディングファクタr_yの和との差、署名ＳＩＧＡ及び署名ＳＩＧＢを、ブロックチェーンの複数のノードに送信すること備える。

【００１１】

一部の実施の形態において、ブロックチェーンの複数のノードが取引を確認するために、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信することは、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信することによって、ブロックチェーンの複数のノードは、取引の確認の成功に応答して、着信者に取引金額ｔを発し、資産A_1，A_2，．．．，A_kを削除し、発信者にチェンジｙを発することを備える。

【００１２】

他の態様によれば、非一時的コンピュータ可読記憶媒体は、プロセッサによって実行するときに、トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームに取引金額ｔの取引をコミットし、チェンジコミットメント値Ｙを取得するために第２のコミットメントスキームにチェンジｙの取引をコミットし、第１のコミットメン

トスキームは、トランザクションブラインディングファクタr_tを備え、第２のコミットメントスキームは、チェンジブラインディングファクタr_yを備えることと、チェンジブラインディングファクタr_yとチェンジｙの第１の組合せを第１の鍵ＫＡによって暗号化することと、取引の着信者に関連する着信者ノードが取引を確認するために、トランザクションブラインディングファクタr_t、取引金額ｔ及びトランザクションコミットメント値Ｔを着信者ノードに送信することと、着信者ノードの取引の確認の成功に応答して、第２の鍵ＫＢによって暗号化されたトランザクションブラインディングファクタr_t及び取引金額ｔの暗号化された第２の組合せを取得することと、ブロックチェーンの複数のノードが取引を確認するために、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信することと、を備える動作をプロセッサによって実行させる命令を記憶する。

【００１３】

他の態様によれば、情報保護のためのシステムは、プロセッサ及びプロセッサに結合された非一時的コンピュータ可読記憶媒体を備え、非一時的コンピュータ可読記憶媒体は、プロセッサによって実行するときに、トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームに取引金額ｔの取引をコミットし、チェンジコミットメント値Ｙを取得するために第２のコミットメントスキームにチェンジｙの取引をコミットし、第１のコミットメントスキームは、トランザクションブラインディングファクタr_tを備え、第２のコミットメントスキームは、チェンジブラインディングファクタr_yを備えることと、チェンジブラインディングファクタr_yとチェンジｙの第１の組合せを第１の鍵ＫＡによって暗号化することと、取引の着信者に関連する着信者ノードが取引を確認するために、トランザクションブラインディングファクタr_t、取引金額ｔ及びトランザクションコミットメント値Ｔを着信者ノードに送信することと、着信者ノードの取引の確認の成功に応答して、第２の鍵ＫＢによって暗号化されたトランザクションブラインディングファクタr_t及び取引金額ｔの暗号化された第２の組合せを取得することと、ブロックチェーンの複数のノードが取引を確認するために、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信することと、を備える動作をプロセッサによって実行させる命令を記憶する。

【００１４】

他の態様によれば、情報保護のためのコンピュータで実施される方法は、トランザクションブラインディングファクタr_t、取引金額ｔの取引及びトランザクションコミットメント値Ｔを取引の発信者に関連する発信者ノードから取得し、取引金額ｔは、トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームにコミットされ、第１のコミットメントスキームは、トランザクションブラインディングファクタr_tを備えることと、取得したトランザクションブラインディングファクタr_t、取得した取引金額ｔの取引及び取得したトランザクションコミットメント値Ｔに基づいて取引を確認することと、取引の確認の成功に応答して、トランザクションブラインディングファクタr_t及び取引金額ｔの第２の組合せを第２の鍵ＫＢによって暗号化することと、暗号化された第２の組合せを発信者ノードに送信することと、を備える。

【００１５】

一部の実施の形態において、取得したトランザクションブラインディングファクタr_t、取得した取引金額ｔの取引及び取得したトランザクションコミットメント値Ｔに基づいて取引を確認することは、トランザクションコミットメント値Ｔが取引金額ｔを取得したトランザクションブラインディングファクタr_tにコミットする第１のコミットメントスキームに等しいか否かを確認することを備える。

【００１６】

一部の実施の形態において、暗号化された第２の組合せを発信者ノードに送信する前に、方法は、暗号化された第２の組合せ及びトランザクションコミットメント値Ｔに関連する署名ＳＩＧＢを生成することを更に備え、暗号化された第２の組合せを発信者ノードに送信することは、暗号化された第２の組合せ及び署名ＳＩＧＢを発信者ノードに送信する

こと備える。

【００１７】

他の態様によれば、非一時的コンピュータ可読記憶媒体は、プロセッサによって実行するときに、トランザクションブラインディングファクタr_t、取引金額ｔの取引及びトランザクションコミットメント値Ｔを取引の発信者に関連する発信者ノードから取得し、取引金額ｔは、トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームにコミットされ、第１のコミットメントスキームは、トランザクションブラインディングファクタr_tを備えることと、取得したトランザクションブラインディングファクタr_t、取得した取引金額ｔの取引及び取得したトランザクションコミットメント値Ｔに基づいて取引を確認することと、取引の確認の成功に応答して、トランザクションブラインディングファクタr_t及び取引金額ｔの第２の組合せを第２の鍵ＫＢによって暗号化することと、暗号化された第２の組合せを発信者ノードに送信することと、を備える動作をプロセッサによって実行させる命令を記憶する。

【００１８】

他の態様によれば、情報保護のためのシステムは、プロセッサ及びプロセッサに結合された非一時的コンピュータ可読記憶媒体を備え、非一時的コンピュータ可読記憶媒体は、プロセッサによって実行するときに、トランザクションブラインディングファクタr_t、取引金額ｔの取引及びトランザクションコミットメント値Ｔを取引の発信者に関連する発信者ノードから取得し、取引金額ｔは、トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームにコミットされ、第１のコミットメントスキームは、トランザクションブラインディングファクタr_tを備えることと、取得したトランザクションブラインディングファクタr_t、取得した取引金額ｔの取引及び取得したトランザクションコミットメント値Ｔに基づいて取引を確認することと、取引の確認の成功に応答して、トランザクションブラインディングファクタr_t及び取引金額ｔの第２の組合せを第２の鍵ＫＢによって暗号化することと、暗号化された第２の組合せを発信者ノードに送信することと、を備える動作をプロセッサによって実行させる命令を記憶する。

【００１９】

ここに開示したススステム、方法及び非一時的コンピュータ可読記憶媒体のこれらの特徴及び他の特徴並びに動作の方法及び構造の関連の素子及び製造のパーツ及び経済性の組合せの機能は、添付図面を参照することにより以下の説明及び添付した特許請求の範囲の考察から更に明らかになり、そのすべては、明細書の一部を形成し、同様な参照願号を種々の図面の対応する部分に付す。しかしながら、図面が図示及び説明のみのためのものであるとともに発明の限定を規定することを意図しないことを明示的に理解すべきである。

【００２０】

本技術の種々の実施の形態の所定の特徴を、特に、添付した特許請求の範囲で説明する。技術の特徴及び利点の更なる理解は、理解を助ける実施の形態を説明する以下の詳細な説明及び図面を参照することによって得られる。

【図面の簡単な説明】

【００２１】

【図１】種々の実施の形態による例示的な情報保護のためのシステムを示す。

【図２】種々の実施の形態による取引開始及び確認のための例示的なステップを示す。

【図３】種々の実施の形態による例示的な情報保護のための方法のフローチャートを示す。

【図４】種々の実施の形態による例示的な情報保護のための方法のフローチャートを示す。

【図５】ここで説明する実施の形態のいずれかを実現することができる例示的なコンピュータシステムのブロック図を示す。

【発明を実施するための形態】

【００２２】

ブロックチェーンを、一般的に分散型台帳と称される分散データベースと見なしてもよ

い。その理由は、動作がネットワークの種々のノード（例えば、コンピュータデバイス）によって実行されるからである。あらゆる情報をブロックチェーンに書き込むとともにブロックチェーンへの保存又はブロックチェーンからの読出しを行ってもよい。誰でもサーバをセットアップするとともにノードになるためにブロックチェーンネットワークに加わってもよい。任意のノードは、現在のブロックチェーンにブロックを追加するためのハッシュ計算のような複雑な計算を行うことによってブロックチェーンを維持するために計算能力を提供してもよく、追加されたブロックは、種々のタイプのデータ又は情報を含んでもよい。追加したブロックに対して計算能力を提供したノードは、トークン（例えば、デジタル通貨単位）を貰ってもよい。ブロックチェーンが中央ノードを有しないので、各ノードは、同等であるとともに全体のブロックチェーンデータベースを保持する。

【００２３】

ノードは、例えば、ブロックチェーンネットワークをサポートするとともにブロックチェーンネットワークの運営を円滑に保つコンピュータデバイス又は大型コンピュータシステムである。二つのタイプのノード：フルノード及び軽量ノードが存在する。フルノードは、ブロックチェーンの完全なコピーを保持する。ブロックチェーンネットワークのフルノードは、取引及びフルノードが受け取るブロックを確認し、これらを、取引の合意確認を提供するために接続ピアに送る。それに対し、軽量ノードは、ブロックチェーンのほんの一部のダウンロードしか行わない。例えば、軽量ノードは、デジタル通貨取引のために用いられる。軽量ノードは、軽量ノードが取引を所望するときにフルノードと通信を行う。

【００２４】

分散特性は、管理センタが制御位置に出現するのを防止するのに有用となることができる。例えば、ビットコイン（登録商標）ブロックチェーンのメンテナンスは、ビットコイン（登録商標）ソフトウェアの通信ノードのネットワークによって実行領域で行われる。本開示は、例としてのビットコイン（登録商標）及びイーサリアムのような一つ以上のブロックチェーン又はデジタル通貨を用いる。当業者は、本開示に開示した技術的解決が他のタイプのブロックチェーン及びデジタル通貨を用いることができる又は適用することができることを理解すべきである。すなわち、従来の意味での銀行、機関又は管理者の代わりに、複数の仲介人がビットコイン（登録商標）ソフトウェアを実行するコンピュータサーバの形態で存在する。これらのコンピュータサーバは、インターネットを介して接続されたネットワークを形成し、誰でも潜在的にネットワークに加わることができる。ネットワークによって適応される取引を、形式「ユーザＡがＺビットコイン（登録商標）をユーザＢに送ることを所望する」としてもよく、この場合、取引は、簡単に手に入るソフトウェアアプリケーションを用いてネットワークに送信される。コンピュータサーバは、これらの金融取引を確認し、これらの記録を台帳のコピーに追加し、かつ、これらの台帳追加をネットワークの他のサーバに送信するように操作可能なビットコイン（登録商標）サーバとして機能する。

【００２５】

ブロックチェーンのメンテナンスを行うことは、「マイニング」と称され、そのようなメンテナンスを行う者は、上述したように、新たに作られたビットコイン（登録商標）及び取引手数料を貰う。例えば、ノードは、ブロックチェーンネットワークが合意した一連の規則に基づいて取引が有効であるか否かを決定してもよい。マイナーは、いずれかの大陸に配置されてもよく、各取引が有効であると確認するとともにそれをブロックチェーンに加えることによって支払処理を行ってもよい。そのような確認は、複数のマイナーによって行われる合意を通じて実現され、組織的な共謀（ｓｙｓｔｅｍａｔｉｃ　ｃｏｌｌｕｓｉｏｎ）が存在しないと仮定する。結局、全てのデータは一貫している。その理由は、計算が有効となるための所定の要求に適合する必要があるとともにブロックチェーンが一貫していることを確実にするために全てのノードが同期されるからである。したがって、データは、ブロックチェーンノードの分散システムに一貫して記憶される。

【００２６】

マイニング処理によって、資産移転のような取引は、ネットワークノードによって確認されるとともにブロックチェーンのブロックの成長するチェーン（ｇｒｏｗｉｎｇ　ｃｈａｉｎ）に加えられる。ブロックチェーン全体を詳しく検討することによって、確認は、例えば、支払人が移転する資産にアクセスする必要があるか否か、資産が以前に使われたか否か、移転料（ｔｒａｎｄｆｅｒｒｉｎｇ　ａｍｏｕｎｔ）が合っているか否か等を含んでもよい。例えば、発信者によって認められた仮想取引（ｈｙｐｏｔｈｅｔｉｃａｌ　ｔｒａｎｓａｃｔｉｏｎ）（例えば、ＵＴＸＯ（未使用トランザクションアウトプット）モデルの下でのビットコイン（登録商標）の取引、勘定残高モデルの下でのイーサリアムコインの取引）において、提案される取引を、マイニングのためにブロックチェーンネットワークに送信してもよい。マイナーは、取引をブロックチェーン履歴に従って行う資格があるか否かをチェックする必要がある。発信者のウォレット残高（ｗａｌｌｅｔ　ｂａｌａｎｃｅ）が既存のブロックチェーン履歴による十分な資金を有する場合、取引は、有効であると見なされるとともにブロックに加えることができる。一旦確認されると、資産移転を、ブロックチェーンに加えるために次のブロックに含めてもよい。

【００２７】

ブロックは、データベース記録によく似ている。データを書き込む度にブロックが作成される。これらのブロックは、互いに接続されたネットワークとなるために暗号を用いてリンクされるとともに保護される。各ブロックは、名称「ブロックチェーン」の発端でもある前のブロックに接続される。各ブロックは、通常、前のブロックの暗号学的ハッシュ、生成時間（ｇｅｎｅｒａｔｉｏｎ　ｔｉｍｅ）及び実データを含む。例えば、各ブロックは、二つのパーツ：現在のブロックの特徴量を記録するブロックヘッダ及び実データ（例えば、取引データ）を記録する主部を含む。ブロックのチェーンは、ブロックヘッダを介してリンクされる。各ブロックヘッダは、バージョン、前のブロックハッシュ、マークルルート、タイムスタンプ、難易度ターゲット（ｄｉｆｆｉｃｕｌｔｙ　ｔａｒｇｅｔ）及びノンスを含んでもよい。前のブロックハッシュは、前のブロックのアドレスだけでなく前のブロックの内部のデータのハッシュも含み、これによって、ブロックチェーンを変更不可能にする。ノンスは、含まれるときに特定の数の先行ゼロのビットによってハッシュを生成する数である。

【００２８】

マイニングのために、新たなブロックのコンテンツのハッシュがノードによって取り出される。ノンス（例えば、ランダムな文字列）は、新たな文字列を取得するためにハッシュに加えられる。新たな文字列は、再びハッシュされる。最終的なハッシュは、難易度ターゲット（例えば、レベル）と比較され、最終的なハッシュが実際に難易度ターゲットより小さいか否かを判断する。否である場合、ノンスを変更するとともに処理を再び繰り返す。是である場合、ブロックがチェーンに加えられ、公開台帳が更新されるとともに加えられたことの注意が喚起される。加えることの成功に貢献するノードは、例えば、（コインベース生成（ｃｏｉｎｂａｓｅ　ｇｅｎｅｒａｔｉｏｎ）として知られている）報酬取引を新たなブロックに加えることによってビットコインを貰う。

【００２９】

すなわち、各出力“Ｙ”に対して、ｋを高い最小エントロピーを有する分布から選択する場合、Ｈ（ｋ｜ｘ）＝Ｙとなるような入力ｘを見つけることができなくなり、この場合、ｋは、ノンスであり、ｘは、ブロックのハッシュであり、Ｙは、難易度ターゲットであり、“｜”は、連結を表す。暗号学的ハッシュが十分にランダムであるという理由で、出力を入力から予測することができないという意味では、例えば、総当たり攻撃として知られている１，２，３等々と整数を次々と試すためにノンスを見つける唯一の既知の方法しか存在しない。先行ゼロ（ｌｅａｄｉｎｇ　ｚｅｒｏｓ）の数が大きくなるにしたがって、必要なノンスを見つけるのに要する時間は、概して長くなる。一例において、ビットコイン（登録商標）システムは、ノンスを見つけるための平均時間が約１０分となるように先行ゼロの数を常に調整する。したがって、計算ハードウェアの処理能力が数年に亘って経時的に上がるので、ビットコイン（登録商標）プロトコルは、マイニングが実現のため

に常に約１０分の持続時間を要するようにするために更に多くの先行ゼロのビットを簡単に要求する。

【００３０】

上述したように、ハッシングは、ブロックチェーンに重要なものである。ハッシュアルゴリズムを、任意の長さのメッセージを固定長のメッセージダイジェストに圧縮する関数と理解することができる。通常はＭＤ５及びＳＨＡが用いられる。一部の実施の形態において、ブロックチェーンのハッシュ長は、２５６ビットであり、それは、元のコンテンツがどのようなものであったとしても、２５６ビットの２進数が最終的に計算される。また、元のコンテンツが互いに異なる限り、対応するハッシュが固有のものであることを保証することができる。例えば、文字列“１２３”のハッシュは、ａ８ｆｄｃ２０５ａ９ｆ１９ｃｃ１ｃ７５０７ａ６０ｃ４ｆ０１ｂ１３ｄ１１ｄ７ｆｄ０（１６進）であり、それは、２進に変換されるときに２５６ビットを有し、“１２３”のみがこのハッシュを有する。ブロックチェーンのハッシュアルゴリズムは不可逆であり、すなわち、（“１２３”からａ８ｆｄｃ２０５ａ９ｆ１９ｃｃ１ｃ７５０７ａ６０ｃ４ｆ０１ｂ１３ｄ１１ｄ７ｆｄ０への）順算は容易であり、全ての計算リソースを使い尽くす場合でも逆算は不可能である。したがって、ブロックチェーンの各ブロックのハッシュは固有のものである。

【００３１】

さらに、ブロックのコンテンツが変更される場合、そのハッシュも変更される。ブロック及びハッシュは１対１の対応であり、各ブロックのハッシュは、ブロックヘッダに対して明確に（ｓｐｅｃｉｆｉｃａｌｌｙ）計算される。すなわち、ブロックヘッダの特徴量は、長い文字列を形成するために接続され、その後、ハッシュが文字列に対して計算される。例えば、“Ｈａｓｈ＝ＳＨＡ２５６（ブロックヘッダ）”は、ブロックハッシュ計算式であり、ＳＨＡ２５６は、ブロックヘッダに適用されるブロックチェーンハッシュアルゴリズムである。ハッシュは、ブロック主部ではなくブロックヘッダによって固有のものとして決定される。上述したように、ブロックヘッダは、現在のブロックのハッシュ及び前のブロックのハッシュを含む多くのコンテンツを含む。これは、現在のブロックのコンテンツが変更される場合又は前のブロックのハッシュが変更される場合に現在のブロックのハッシュが変更されることを意味する。ハッカーがブロックに変更を加える場合、当該ブロックのハッシュも変更される。変更が加えられたブロックに後のブロックを接続するために、ハッカーは、全ての続くブロックに変更を加える必要がある。その理由は、次のブロックが前のブロックのハッシュを含むからである。そうでない場合、変更が加えられたブロックは、ブロックチェーンから切り離される。設計の理由のために、ハッシュ計算は、多大な時間を必要とし、ハッカーがネットワーク全体の計算能力の５１％を超える計算能力を習得していない場合には、短期間で複数のブロックに変更を加えることはほとんど不可能である。したがって、ブロックチェーンは、それ自体の信頼性を保証し、データが書き込まれると、データを改ざんすることができない。

【００３２】

一旦マイナーが新たなブロックのハッシュ（すなわち、適格な署名（ｅｌｉｇｉｂｌｅ　ｓｉｇｎａｔｕｒｅ）又はソリューション）を見つけると、マイナーは、この署名を他の全てのマイナー（ブロックチェーンのノード）に送信する。他のマイナーは、当該ソリューションが発信者のブロックの問題に対応するか否かを確認する（すなわち、ハッシュ入力の実際の結果が当該署名になるか否かを決定する。）。ソリューションが有効である場合、他のマイナーは、ソリューションを承認し、新たなブロックをブロックチェーンに加えることができることに合意する。したがって、新たなブロックの合意に達する。これは、「プルーフオブワーク」としても知られている。合意に達したブロックを、ブロックチェーンに加えることができ、その署名と共にネットワークの全てのノードに送信する。ブロック内の取引が取引の時点で現在のウォレット残高（取引履歴）に正確に対応する限り、ノードは、ブロックを許容するとともにブロックを取引データに保存する。このブロックのトップに新たなブロックが加えられる度に、加える前のブロックの他の「確認」として加えることがカウントされる。例えば、取引がブロック５０２に含まれるとともにブ

ロックチェーンが５０７ブロック長である場合、それは、取引が（ブロック５０７～５０２に対応する）五つの確認を有することを意味する。取引が有する確認が多くなるに従って、攻撃者が変更を加えるのが困難になる。

【００３３】

一部の実施の形態において、例示的なブロックチェーン資産システムは、公開鍵暗号方式を利用し、この場合、二つの暗号鍵：一つの公開鍵及び一つの秘密鍵を生成する。公開鍵を、アカウント番号と考えることができ、秘密鍵を所有権認証情報（ｏｗｎｅｒｓｈｉｐ　ｃｒｅｄｅｎｔｉａｌｓ）と考えることができる。例えば、ビットコイン（登録商標）ウォレットは、公開鍵と秘密鍵の組である。所定の資産アドレス（ａｓｓｅｔ　ａｄｄｒｅｓｓ）に関連する資産（例えば、デジタル通貨、現金資産、株（ｓｔｏｃｋ）、国債（ｅｑｕｉｔｙ）、債権（ｂｏｎｄ））の所有権を、アドレスに属する秘密鍵の知識と共に示すことができる。例えば、「ビットコイン（登録商標）クライアントソフトウェア」と時々称されるビットコイン（登録商標）ウォレットソフトウェアによって、所定のユーザは、ビットコイン（登録商標）取引を行うことができる。ウォレットプログラムは、秘密鍵の生成及び記憶を行うとともにビットコイン（登録商標）ネットワークのピアと通信を行う。

【００３４】

ブロックチェーン取引において、支払人及び受取人は、公開暗号鍵によりブロックチェーンにおいて識別される。例えば、大抵の現在のビットコイン（登録商標）の移動は、ある公開鍵から異なる公開鍵までのものである。実際には、これらの鍵のハッシュは、ブロックチェーンで用いられるとともに「ビットコイン（登録商標）アドレス」と称される。原理的には、仮想的な攻撃者Ｓは、ユーザの名前の代わりのユーザのビットコイン（登録商標）アドレスを用いることによって、「人Ａが人Ｓに１００ビットコイン（登録商標）を支払う」ようにブロックチェーン台帳に取引を加えることによって人Ａから金を盗むことができる。ビットコインプロトコルは、移動の度に支払人の秘密鍵を用いたデジタル署名を要求することによってこの種の窃盗を防止し、署名された移動のみをブロックチェーン台帳に加えることができる。人Ｓは人Ａの署名を偽造することができないので、人Ｓは、「人Ａが人Ｓに１００ビットコイン（登録商標）を支払う」に等しいブロックチェーンへのエントリを加えることによって人Ａに詐欺行為を行うことができない。同時に、誰でも公開鍵を用いて人Ａの署名を確認することができ、したがって、支払人である場合にブロックチェーンのあらゆる取引が許可される。

【００３５】

ビットコイン（登録商標）取引の状況において、一部のビットコイン（登録商標）をユーザＢに移動させるために、ユーザＡは、ノードを通じた取引についての情報を含む記録を構成してもよい。ユーザＡの署名鍵（秘密鍵）によって記録に署名を行ってもよく、記録は、ユーザＡの公開検証鍵及びユーザＢの公開検証鍵を含む。署名は、取引がユーザに起因することを確認するために用いられ、一旦署名が発行されると誰かによる取引の変更を防止する。記録を、同一の時間ウィンドウで新たなブロックで生じた他の記録と共にフルノードに送信してもよい。フルノードは、記録を受け取ると、ブロックチェーンシステムでこれまで生じた全ての取引の台帳に記録を組み込み、上述したマイニング処理によって以前に許容されたブロックチェーンに新たなブロックを加え、かつ、加えられたブロックを、ネットワークの合意規則に対して有効にする。

【００３６】

ＵＴＸＯ（未使用トランザクションアウトプット）モデル及び勘定残高モデルは、ブロックチェーン取引を実現するための二つの例示的なモデルである。ＵＴＸＯは、ブロックチェーンオブジェクトモデルである。ＵＴＸＯの下では、資産は、消費されなかったブロックチェーン取引の出力によって表され、新たな取引の入力として用いることができる。例えば、移動させるユーザＡの資産をＵＴＸＯの形式にしてもよい。資産を使用（取引）するために、ユーザＡは、秘密鍵によって署名を行う必要がある。ビットコイン（登録商標）は、ＵＴＸＯモデルを用いるデジタル通貨の一例である。有効なブロックチェーン取

引の場合、更なる取引を行うために未使用出力を用いてもよい。一部の実施の形態において、二重使用（ｄｏｕｂｌｅ　ｓｐｅｎｄｉｎｇ）及び詐欺を防止するために未使用出力のみを更なる取引に用いてもよい。このために、ブロックチェーンの入力は、取引が生じたときに削除され、同時に、出力がＵＴＸＯの形式で生成される。これらの未使用取引出力を、将来の取引のために（秘密鍵の所有者、例えば、デジタル通貨ウォレットを有する人によって）用いてもよい。

【００３７】

それに対し、（アカウントベース取引モデルとも称される）勘定残高モデルは、大域状態（ｇｌｏｂａｌ　ｓｔａｔｅ）としての各勘定残高を追跡し続ける。勘定残高は、勘定残高が使用される取引金額以上であることを確実にするためにチェックされる。勘定残高モデルがイーサリアムで作動する方法の一例を提供する。

【００３８】

１．アリスは、マイニングによって５イーサを獲得する。アリスが５イーサを有することがシステムに記録される。

【００３９】

２．アリスがボブに１イーサを与えることを所望し、システムは、アリスの預金額から１イーサを差し引き、したがって、アリスは、４イーサを有する。

【００４０】

３．その後、システムは、ボブの預金額を１イーサだけ増やす。システムは、ボブが最初に２イーサを有することを知っており、したがって、ボブの預金額は、３イーサに増える。

【００４１】

イーサリアムの記録管理は、銀行の記録管理に似ていてもよい。似ていることは、ＡＴＭ／デビットカードを用いることである。銀行は、各デビットカードがどれだけの金額を有するかを追跡し、ボブがお金を使う必要があるとき、銀行は、取引を承認する前にボブが十分な残高を有することを確実にするために記録をチェックする。

【００４２】

ブロックチェーン及び他の同様な台帳が完全に公のものであるので、ブロックチェーンそれ自体はプライバシー保護を行わない。Ｐ２Ｐネットワークの公共性は、Ｐ２Ｐを使用する者が名前によって識別されない間に取引を個人及び企業にリンクすることが容易であることを意味する。例えば、国境を超えた送金又はサプライチェーンにおいて、取引金額は、極めて高いレベルのプライバシー保護値を有し、取引金額情報によって、取引関係者の特定の位置及び識別子を推論することができる。取引の内容は、例えば、金銭、トークン、デジタル通貨、契約書、譲渡証書、診察記録、顧客の詳細（ｃｏｓｔｏｍｅｒ　ｄｅｔａｉｌ）、株、債権、国債又はデジタル形式で表現することができる他の任意の資産を備えてもよい。ＵＸＴＯモデルが、例えば、モレノ及びゼロ知識暗号方式ジーキャッシュ（Ｍｏｒｅｎｏ　ａｎｄ　ｚｅｒｏ－ｋｎｏｗｌｅｄｇｅ　ｃｒｙｐｔｏｇｒａｐｈｙ　Ｚｃａｓｈ）のリング署名によって取引金額に対する匿名性を提供するとしても、取引金額は、勘定残高モデルの下では保護されないままである。したがって、本開示によって対処される技術的課題は、取引金額のプライバシーのようなオンライン情報をどのように保護するかである。そのような取引を、勘定残高モデルの下でのものとすることができる。

【００４３】

一部の既存の技術は、取引金額を暗号化するとともに勘定残高モデルを置換するためにペダーソンコミットメントスキームを用いることを提案する。そのようなスキームの下では、発信者は、取引金額及び取引金額のペダーソンコミットメントに対応する乱数をブロックチェーンの安全が保証されたチャネルを介して受取人に送信する。受取人は、乱数がトランザクションコミットメントにマッチするか否かを確認するとともに局所記憶を行う。例えば、勘定残高モデルの下では、預金高を、集約されるが統合されない資産を保持するウォレット（預金高）として取り扱うことができる。各資産は、資産タイプ（例えば、暗号通貨）に対応してもよく、勘定残高は、資産価値の和である。同一タイプの資産さえ

併合されない。取引中、移動する資産の受取人を特定してもよく、対応する資産は、取引に資金を出すためにウォレットから除去される。ブロックチェーンノードは、支払いウォレットが取引をカバーするのに十分な（一つ以上の）資産を有することを確認し、その後、ノードは、移動された資産を支払いウォレットから除去するとともに対応する資産を受取人のウォレットに加える。

【００４４】

しかしながら、そのようなスキームに対する制限が存在する。取引金額及びペダーソンコミットメントによって生成された乱数は、プライバシーセンシティブデータ（ｐｒｉｖａｃｙ－ｓｅｎｓｉｔｉｖｅ　ｄａｔａ）である。取引に関連する関係者以外の関係者は、値を知る機会を有するべきではない。したがって、そのような情報は、暗号化されるとともに保存されるべきであり、使用の際に解読されるべきである。コミッテッド値及び乱数は、取引される資産を将来使うのに必要な要素であるが、消失しやすく、乱数を適切に記憶する安全、安定及び有効方法がないために、復元するのが困難である。例えば、現在の技術のスキームは、乱数と暗号化された勘定残高に対応するプレーンテキスト残高とを管理するための局所的な永続記憶を維持することをユーザに要求し、管理の実現は複雑である。さらに、ブラインディングファクタ（例えば、乱数）と「ペダーソン資産」に対応するプレーンテキスト残高との単一のローカルノードへの記憶は、消失又は破損する傾向があり、それに対し、マルチノードバックアップ記憶は、勘定残高が頻繁に変化するので実現するのが困難である。

【００４５】

本開示のシステム及び方法は、上述した制限を克服するとともにコミットメントスキームの取引金額、資産価値及びブラインディングファクタの強固なプライバシー保護を実現する。そのために、種々の暗号情報交換プロトコルを、乱数及びプレーンテキスト残高の暗号化／解読に用いることができ、したがって、簡便な管理を提供する。さらに、ブロックチェーンの暗号化された情報を格納することは、コミットメントスキームの取引金額、資産価値及びブラインディングファクタが簡単に消失されない又は簡単に改ざんされないことを保証する。

【００４６】

一部の実施の形態において、コミットメントスキーム（例えば、ペダーソンコミットメント）は、次のように所定の値ａ（例えば、取引金額、資産価値、主要パラメータ）を暗号化してもよい。

【００４７】

【数１】

$$PC(a) = r \times G + a \times H$$

【００４８】

この場合、ｒは、隠蔽を提供する（代替的にバインディングファクタとも称する）ランダムブラインディングファクタであり、Ｇ及びＨは、楕円曲線の公的に合意された生成元／ベースポイント（ｐｕｂｌｉｃｌｙ　ａｇｒｅｅｄ　ｇｅｎｅｒａｔｏｒｓ／ｂａｓｅ　ｐｏｉｎｔｓ）であり、ランダムに選択してもよく、ｓｎは、コミットメントの値であり、Ｃ（ｓｎ）は、コミットメントとして用いられるとともに相手方に与えられる曲線の点（ｃｕｒｖｅ　ｐｏｉｎｔ）であり、Ｈは、他の曲線の点である。すなわち、Ｇ及びＨは、ノードに既知のパラメータである。Ｈの“ｎｏｔｈｉｎｇ　ｕｐ　ｍｙ　ｓｌｅｅｖｅ”生成を、ある点から他の点へのマッピングを行うハッシュ関数Ｈ＝Ｈａｓｈ（Ｇ）によりベースポイントＧをハッシュすることによって行ってもよい。Ｈ及びＧは、所定のシステムの公開パラメータ（例えば、楕円曲線のランダムに生成された点）である。上記が楕円曲線形式のペダーソンコミットメントの例を提供するが、ペダーソンコミットメント又は他のコミットメントスキームの他の種々の形式を代替的に用いてもよい。

【００４９】
コミットメントスキームは、データの秘密を保持するが、データがデータの発信者によって後に変更することができないようにするためにデータをコミットする。関係者がコミットメント値（例えば、ＰＣ（ａ））しか知らない場合、どの内在するデータ値（例えば、ａ）がコミットされたかを決定することができない。データ（例えば、ａ）とブラインディングファクタ（例えば、ｒ）の両方を（例えば、開始ノードによって）後に明らかにしてもよく、コミットメントの受取人（例えば、合意ノード）は、コミットメントを実行するとともにコミッテッドデータが明らかにされたデータにマッチすることを確認する。ブラインディングファクタは、１以外で存在し、誰かがデータを推測することを試みることがある。

【００５０】
コミットメントスキームは、コミットされた値を秘密のままにすることができるがコミットする関係者がコミットメント処理の必要なパラメータを暴露するときに後に明らかになることがあるように値（例えば、ａ）をコミットする。強固なコミットメントスキームは、情報隠匿とコンピュータ的なバインディング（ｃｏｍｐｕｔａｔｉｏｎａｌｌｙ　ｂｉｎｄｉｎｇ）の両方であってもよい。隠匿は、所定の値ａ及び値ＰＣ（ａ）のコミットメントを関連付けできないようにすべきであるという概念である。すなわち、ＰＣ（ａ）は、ａについての情報を明らかにすべきでない。既知のＰＣ（ａ）、Ｇ及びＨを用いることによって、乱数ｒのためにａを知るのはほとんど不可能である。コミットメントスキームは、二つの互いに異なる値の結果として同一のコミットメントとなることができる妥当な方法が存在しない場合にはバインディングである。ペダーソンコミットメントは、離散対数仮定の下で完全に隠匿であるとともに計算的にバインディング（ｃｏｍｐｕｔａｔｉｏｎａｌｌｙ　ｂｉｎｄｉｎｇ）である。さらに、既知のＰＣ（ａ）、Ｇ及びＨを用いることにより、ＰＣ（ａ）＝ｒ×Ｇ＋ａ×Ｈであるか否かを判断することによってＰＣ（ａ）を確認することができる。

【００５１】
ペダーソンコミットメントは、追加の特性を有する。コミットメントを追加することができ、コミットメントのセットの和は、（ブラインディングファクタの和のようなブラインディングファクタセットを有する）データの和に対するコミットメントと同一である。ＰＣ（r_1,$data_1$）＋ＰＣ（r_2,$data_2$）＝＝ＰＣ（r_1＋r_2,$data_1$＋$data_2$）；ＰＣ（r_1,$data_1$）-ＰＣ（r_1,$data_1$）＝＝０。換言すれば、コミットメントは、加算を保持し、可換特性を適用する、すなわち、ペダーソンコミットメントは、内在するデータが暗号化されないかのように内在するデータが数学的に取り扱われるという点で加算的に同形（ａｄｄｉｔｉｖｅｌｙ　ｈｏｍｏｍｏｒｐｈｉｃ）である。

【００５２】
一部の実施の形態において、入力値を暗号化するのに用いられるペダーソンコミットメントを、楕円曲線の点を用いて構成してもよい。通常、楕円曲線暗号（ＥＣＣ）公開鍵は、群（Ｇ）の生成元と秘密鍵（ｒ）とを乗算することによって作成される：Ｐｕｂ＝ｒＧ。結果を、３３バイトアレイのようにシリアル化してもよい。ＥＣＣ公開鍵は、ペダーソンコミットメントについて上述したような加算的同形特性に従ってもよい。すなわち、Ｐｕｂ１＋Ｐｕｂ２＝（ｒ１＋ｒ２（ｍｏｄ　ｎ））Ｇである。

【００５３】
入力値に対するペダーソンコミットメントを、ｘＧ＝Ｈとなるようなｘを誰も知らないことを意味する第１の生成元Ｇに対する第２の生成元Ｈの離散対数（逆の場合も同じ）を誰も知らないようにするように群（下の式のＨ）の他の生成元を取り出すことによって作成してもよい。これを、例えば、Ｈ：　Ｈ＝ｔｏ＿ｐｏｉｎｔ（ＳＨＡ２５６（ＥＮＣＯＤＥ（Ｇ））））を取り出すためにＧの暗号化ハッシュを用いることによって成し遂げてもよい。

【００５４】

二つの生成元Ｇ及びＨが与えられた場合、入力値を暗号化するための例示的なコミットメントスキームは、ｃｏｍｍｉｔｍｅｎｔ＝ｒＧ＋ａＨとして規定してもよい。ここで、ｒを、秘密ブラインディングファクタとしてもよく、ａを、コミットされる入力値としてもよい。したがって、ｓｎがコミットされる場合、上述したコミットメントスキームＰＣ（ａ）＝ｒ×Ｇ＋ａ×Ｈを取得することができる。ペダーソンコミットメントは、あらゆるコミットメントに対して理論的に秘密の情報であり、あらゆる量をコミットメントにマッチさせるブラインディングファクタが存在する。ペダーソンコミットメントを、任意マッピングが計算できないように偽りのコミットメントに対して計算的に安全にしてもよい。

【００５５】

値をコミットした関係者（ノード）は、元の値ａとコミットメント式を完成させるファクタｒとを開示することによってコミットメントをオープンにしてもよい。値ＰＣ（ａ）をオープンにすることを所望する関係者は、実際に共有された元の値が最初に受け取ったコミットメントＰＣ（ａ）にマッチすることを再び確認するためにコミットメントを計算する。したがって、資産タイプ情報を、資産タイプ情報を固有のシリアルナンバーにマッピングした後にペダーソンコミットメントにより暗号化することによって保護することができる。コミットメントを生成するときに選択した乱数ｒによって、コミットメント値ＰＣ（ａ）に従ってコミットされたアセットタイプを誰かが推論するのをほとんど不可能にする。

【００５６】

一部の実施の形態において、公衆鍵プロトコル、対称暗号化プロトコル、ディフィーヘルマン（ＤＨ）鍵交換等のような種々の暗号化情報交換プロトコルを用いてもよい。例えば、ＤＨ鍵交換を、公開チャネルを介して暗号鍵を安全に交換する方法として用いてもよい。指数鍵（ｅｘｐｏｎｅｎｔｉａｌ　ｋｅｙ）交換とも称されるＤＨ鍵交換は、直接的に送信されることがない要素に基づいて暗号鍵を生成するために乗となる数を用いるデジタル暗号化の方法であり、これによって、自称コードブレーカー（ｗｏｕｌｄ－ｂｅ　ｃｏｄｅ　ｂｒｅａｋｅｒ）のタスクを数学的に圧倒する。

【００５７】

ディフィーヘルマン（ＤＨ）鍵交換の一例において、二人のエンドユーザであるアリスとボブは、アリスとボブが秘密であると知っているチャネルを通じて通信を行う間に、ｐが素数であるとともにｑがｐの生成元となるような正の整数ｐ及びｑに互いに合意する。生成元ｑは、ｐ未満の正の整数の乗となったときに任意の二つのそのような整数に対して同一の結果を生成することが絶対にない数である。ｐの値を大きくしてもよいが、ｑの値は、通常、小さい。すなわち、ｑは、法ｐの原子根である。

【００５８】

アリスとボブが秘密裏にｐ及びｑに合意すると、アリスとボブは、正の整数の秘密鍵ａ及びｂを選択することができ、ａとｂの両方は、法ｐの原子根より小さく、かつ、ランダムに生成されてもよい。ユーザは、秘密鍵を誰にも漏らさず、理想的には、ユーザは、秘密鍵の番号を覚え、秘密鍵の番号を書き留めない又はどこかに記憶させない。次に、アリスとボブは、次の式に従って秘密鍵に基づいて公開鍵ａ＊及びｂ＊を計算する。

【００５９】

【数２】

$$a^* = q^a \mod p$$

及び

$$b^* = q^b \mod p$$

【００６０】

二人のユーザは、インターネット又は企業のワイドエリアネットワーク（ＷＡＮ）のよ

うな安全でないと仮定される通信媒体を介して公開鍵ａ＊及びｂ＊を共有することができる。これらの公開鍵から、数字ｋ１をユーザの秘密鍵に基づいていずれかのユーザによって生成することができる。

【００６１】

アリスは、式：ｋ１＝（ｂ＊）^{a}　ｍｏｄ　ｐを用いてｋ１を計算する。

【００６２】

ボブは、式：ｋ１＝（ａ＊）^{b}　ｍｏｄ　ｐを用いてｋ１を計算する。

【００６３】

ｋ１の値が上述した二つの式のいずれかに従って同一であるということがわかる。しかしながら、ｋ１の計算に重要な秘密鍵ａ及びｂは、公衆媒体を介して送信されない。ｐ、ｑ、ａ＊及びｂ＊を用いる場合でも、ａ及びｂを計算するのは困難である。ｋ１が非常に大きくて一見したところ乱数であるので、潜在的なハッカーは、何百万の試験を行うために高性能のコンピュータの助けがあるとしてもｋ１を正確に推測するチャンスはほとんどない。したがって、二人のユーザは、理論的には、暗号鍵ｋ１を用いる二人のユーザに最適な暗号化方法によって公衆媒体を介して秘密裏に通信を行うことができる。

【００６４】

ディフィーヘルマン（ＤＨ）鍵交換を実現する他の例において、全ての計算は、十分なサイズの離散群において生じ、ディフィーヘルマン問題は、難しいと考えられ、通常、（例えば、従来のＤＨに対する）大きな素数を法とする乗法群又は（例えば、楕円曲線ディフィーヘルマン）に対する楕円曲線群である。

【００６５】

二人の関係者に対して、各関係者は、秘密鍵ａ又はｂを選択する。各関係者は、対応する公開鍵ａＧ又はｂＧを計算する。各関係者は、公開鍵ａＧ又はｂＧを他の関係者に送る。各関係者は、対称暗号化スキームの鍵のセットを導出するための鍵導出関数と共に用いることができる新たな共有された秘密ａ（ｂＧ）＝ｂ（ａＧ）を計算するために受け取った公開鍵を関係者の秘密鍵と共に用いる。代替的には、他の種々の計算方法を、例えば、公開鍵ｇ^{a}及びｇ^{b}並びに共有鍵ｇ^{ab}又はｇ^{ba}を生成することによって用いることができる。

【００６６】

取引中、情報保護は、ユーザのプライバシーを守るのに重要であり、取引金額は、保護されない一つのタイプの情報である。図１は、種々の実施の形態による情報保護のための例示的なシステム１００を示す。図示したように、ブロックチェーンネットワークは、複数のノード（例えば、サーバ、コンピュータ等において実現されるフルノード）を備えてもよい。一部のブロックチェーンプラットフォーム（例えば、ＮＥＯ）に対して、所定のレベルの議決権を有するフルノードを、取引確認の責任を仮定するコンセンサスノードと称してもよい。本開示において、フルノード、コンセンサスノード又は他の同等のノードは、取引を確認することができる。

【００６７】

また、図１に示すように、ユーザＡ及びユーザＢは、取引を行う軽量ノードとしての役割を果たすラップトップ及び携帯電話のような対応する装置を用いてもよい。例えば、ユーザＡは、ユーザＡの口座の一部の資産をユーザＢの口座に移すことによってユーザＢと取引を行ってもよい。ユーザＡ及びユーザＢは、取引のための適切なブロックチェーンソフトウェアがインストールされた対応する装置を用いてもよい。ユーザＡの装置を、着信者ノードＢと称するユーザＢの装置との取引を開始する開始ノードＡと称してもよい。ノードＡは、ノード１との通信を介してブロックチェーンにアクセスしてもよく、ノードＢは、ノード２との通信を介してブロックチェーンにアクセスしてもよい。例えば、ノードＡ及びノードＢは、取引をブロックチェーンに加えることを要求するためにノード１及びノード２を介してブロックチェーンに提示してもよい。ノードＡ及びノードＢは、オフブロックチェーンで他の通信（例えば、ノード１及び２を経由しない通常のインターネット通信）の他のチャネルを有してもよい。

【００６８】
図１のノードの各々は、プロセッサ及びプロセッサに結合された非一時的コンピュータ可読記憶媒体を備え、非一時的コンピュータ可読記憶媒体は、プロセッサによって実行するときに、ここで説明する情報保護のための種種のステップをプロセッサによって実行させる命令を記憶する。各ノードは、他のノード及び／又は他の装置と通信を行うためにソフトウェア（例えば、取引プログラム）及び／又はハードウェア（例えば、有線、無線接続）がインストールされてもよい。ノードハードウェア及びソフトウェアの更なる詳細を、図５を参照しながら後に説明する。
【００６９】
図２は、種々の実施の形態による発信者ノードＡ、着信者ノードＢ及び一つ以上の確認するノードの間の取引及び確認の例示的なステップを示す。以下に示す動作は、理解を助けるのを意図するものである。実現に応じて、例示的なステップは、種々の順番で又は並列に実行される追加のステップ、更に少ないステップ又は代替的なステップを有してもよい。
【００７０】
種々の実施の形態において、取引金額の関係者（発信者であるユーザＡ及び着信者であるユーザＢ）が勘定残高モデルに対して設定される。ユーザＡ及びユーザＢは、ラップトップ、携帯電話等のような一つ以上の装置を介して取引を行うために以下のステップを実行してもよい。装置は、種々のステップを実行するために適切なソフトウェア及びハードウェアがインストールされてもよい。各口座を、暗号化秘密鍵（秘密鍵）－公開鍵ペアに関連させてもよい。秘密鍵をＳＫで表してもよく、公開鍵をＰＫで表してもよい。秘密鍵を、送信される情報（例えば、取引情報）に署名をするのに用いてもよい。公開鍵を、署名された情報を確認するとともに口座アドレス（ａｃｃｏｕｎｔ　ａｄｄｒｅｓｓ）を生成するのに用いてもよい。各口座は、各々を（Ｖ＝ＰＣ（ｒ,ｖ）,E_K（ｒ,ｖ））で表す種々の資産を含んでもよく、この場合、ｖは、資産の額面通りの価値を表し、Ｖは、額面通りの価値ｖのペダーソンコミットメントを表し、ｒは、ブラインディングファクタ（例えば、乱数）を表し、ＰＣ（）は、ペダーソンコミットメントアルゴリズムであり、Ｅ（）は、暗号化アルゴリズム（例えば、暗号鍵暗号化アルゴリズム）であり、Ｋは、各口座に固有の暗号鍵である。例えば、各資産を、（Ｖ＝ＰＣ（ｒ,ｖ）,E_K（ｒ||ｖ））で表すことができ、この場合、||は、連結を表す。連結を以下の実施の形態で用いるが、ｒ及びｖを含む他の代替的な表現を用いてもよい。暗号鍵Ｋ（例えば、ＫＡ，ＫＢ）を、秘密鍵プロトコル、鍵導出関数等のような種々の方法によって生成することができる。各資産は、資産のソース情報のようなリストした情報以外の情報も有してもよい。
【００７１】
一例において、ユーザＡが、ブロックチェーンで確認される取引においてユーザＢと取引金額ｔの取引が成功する前に、Ａの口座のアドレス及び資産並びにＢの口座は、以下の通りである。
【００７２】
Ａの口座（口座Ａ）に対して、
アドレス：ＡｄｄｒＡ
公開鍵：PK_A
秘密鍵：SK_A
第１の鍵：ＫＡ
価値a_1～a_mのそれぞれの資産A_1～A_mを、以下のように示す。
（A_1＝ＰＣ（r_{a1},a_1）,E_{KA}（r_{a1},a_1））,
（A_2＝ＰＣ（r_{a2},a_2）,E_{KA}（ra_2,a_2））,
・・・
（A_m＝ＰＣ（r_{am},a_m）,ＥＫＡ（r_{am},a_m））
【００７３】
Ｂの口座（口座Ｂ）に対して、

アドレス：ＡｄｄｒＢ
公開鍵：PK_B
秘密鍵：SK_B
第１の鍵：ＫＢ
価値b_1～b_mのそれぞれの資産B_1～B_mを、以下のように示す。
（B_1＝ＰＣ（r_{b1},b_1）,E_{KB}（r_{b1},b_1））,
（B_2＝ＰＣ（r_{b2},b_2）,E_{KB}（r_{b2},b_2））,
・・・
（B_m＝ＰＣ（r_{bm},b_m）, E_{KB}（r_{bm},b_m））

【００７４】

一部の実施の形態では、ステップ２０１において、ノードＡは、ノードＢとの取引を開始してもよい。例えば、ユーザＡ及びユーザＢは、ユーザＡの口座Ａからユーザ Ｂの口座Ｂまでの取引金額ｔの交渉を行う。口座Ａ及び口座Ｂは、ここで説明する「ウォレット」に対応してもよい。口座Ａは、一つ以上の資産を有してもよい。資産は、例えば、金銭、トークン、デジタル通貨、契約書、譲渡証書、診察記録、顧客の詳細、株、債権、国債又はデジタル形式で表現することができる他の任意の資産を備えてもよい。口座Ｂは、一つ以上の資産を有してもよい又は資産を有しなくてもよい。各資産を、ブロックチェーンのブロックに記憶された種々のブロックチェーン情報に関連させてもよく、ブロックチェーン情報は、例えば、資産タイプを表すノートタイプ（ＮｏｔｅＴｙｐｅ）、資産の固有の識別子を表すノートＩＤ（ＮｏｔｅＩＤ）、資産価値のコミットメント（例えば、ペダーソンコミットメント）値を表すコミットメント値、乱数及び資産価値の暗号化等を備えてもよい。

【００７５】

口座Ａに関連して説明するように、一部の実施の形態において、資産A_1～A_mはそれぞれ、資産価値a_1～a_m及び乱数r_{a1}～r_{am}に対応する。乱数r_{a1}～r_{am}に基づいて、ノードＡは、暗号化されたコミットメント値を取得するために口座Ａの資産価値をコミットメントスキーム（例えば、ペダーソンコミットメント）にコミットしてもよい。例えば、口座Ａに対して、暗号化されたコミットメント値をPC_1～PC_mとしてもよく、この場合、PC_i＝ＰＣ（r_{ai},a_i）＝r_{ai}×Ｇ＋a_i×Ｈであり、Ｇ及びＨは、既知であり、ｉは、１とｍの間の変数である。第１のフィールドＰＣ（．．．）に加えて、各資産を、上述した第２のフィールドＥ（．．．．）にも関連させる。第２のフィールドＥ（．．．．）は、鍵ＫＡによって暗号化される対応する乱数及び資産価値の暗号化を表す。例えば、暗号化を、E_{KA}（r_{ai},a_i）としてもよい。各資産に対するＰＣ（．．．）及びＥ（．．．．）を、以前の取引から引き継いでもよい。同一の機構を口座Ｂ及びその資産に適用してもよい。

【００７６】

一部の実施の形態において、ユーザＡは、取引金額ｔを支払うために、口座Ａからの少なくともｔの合意された値の一つ以上の資産を解読するための第１の鍵ＫＡ（例えば、対称暗号鍵）を用いてもよい。例えば、ノードＡは、この取引のために資産A_1，A_2，．．．，A_kを選んでもよく、この場合、ｋは、ｍ以下である。口座Ａの残りの資産A_{k+1}，A_{k+2}，．．．，A_mは選ばれない。したがって、ノードＡは、ノード１から資産ＰＣ（r_{a1},a_1），ＰＣ（r_{a2},a_2），．．．，ＰＣ（r_{ak}，a_k）を読み出してもよい。ノードＡに知られている乱数r_{a1}，r_{a2}，．．．r_{ak}を用いることによって、ノードＡは、和（a_1＋a_2＋，．．．，＋a_k）が取引金額ｔ未満となることを確実にするように資産価値a_1，a_2，．．．，a_kを取得するために、読み出される資産ＰＣ（r_{a1},a_1），ＰＣ（r_{a2},a_2），．．．，ＰＣ（r_{ak}，a_k）を解読することができる。種々の資産を、種々のレートに基づいて口座内で互いに交換してもよい。

【００７７】

一部の実施の形態において、対称暗号鍵は、プレーンテキストの暗号化と暗号文の解読

の両方に対して暗号対称鍵アルゴリズムで用いられる同一の暗号鍵を意味してもよい。鍵は同一であってもよい又は二つの鍵の仲介をする簡単な変換が存在してもよい。鍵は、秘密情報リンクを維持するために用いることができる二人以上の関係者の間の共有された秘密を表してもよい。

【００７８】

一部の実施の形態において、選択した資産価値のｔを超えた量は、存在する場合にチェンジとしてのｙに設定される。例えば、ノードＡは、チェンジｙ＝（a_1＋a_2＋，．．．，＋a_k）－ｔを決定してもよい。ノードＡは、ｔ及びｙに対するペダーソンコミットメント：Ｔ＝ＰＣ（r_t，ｔ），Ｙ＝ＰＣ（r_y，ｙ）を生成するためのブラインディングファクタとして乱数r_t及びr_yを選択してもよい。すなわち、ノードＡは、ｔに対する乱数r_t及びｙに対する乱数r_yを生成してもよい。ノードＡは、コミットメント値Ｔ＝ＰＣ（r_t，ｔ）を取得するためにｔ及びr_iをコミットメントスキーム（例えば、同形暗号化）にコミットするとともにコミットメント値Ｔ＝ＰＣ（r_y，ｙ）を取得するためにｙ及びr_yをコミットメントスキーム（例えば、同形暗号化）にコミットすることができる。さらに、ノードＡは、ｒ’＝（r_1＋r_2．．．＋r_k）－r_t－r_yを決定してもよい。

【００７９】

一部の実施の形態において、ノードＡは、暗号E_{KA}（r_y，ｙ）を取得するために（r_y，ｙ）を暗号化する第１の鍵ＫＡを用いてもよい。ノードＡは、E_{KA}（r_y，ｙ）を局所的に記憶してもよい。

【００８０】

ステップ２０２において、ノードＡは、（例えば、ブロックチェーンを介して、ブロックチェーンの安全なチャネルを介して）取引情報をノードＢに送信してもよい。送信される情報は、例えば、乱数r_t、取引金額ｔ及びコミットメント値Ｔを備えてもよい。取引情報をプレーンテキストで送信してもよい。

【００８１】

ステップ２０３において、ノードＢは、乱数r_t、取引金額ｔ及びコミットメント値Ｔを確認してもよい。一部の実施の形態において、ノードＢは、ユーザＢに送信される金額ｔが正しいか否か及びＴ＝ＰＣ（r_t，ｔ）であるか否かを確認してもよい。ステップ２０３に対して、マッチ／確認が否である場合、ノードＢは、取引を拒否してもよい。マッチ／確認が是である場合、ノードＢは、ステップ２０４でノードＡに応答してもよい。

【００８２】

ステップ２０４において、ノードＢは、暗号E_{KB}（r_t，ｔ）を取得するために第２の鍵ＫＢ（例えば、対称暗号鍵）によってE_{KB}（r_t，ｔ）を暗号化するとともに署名ＳＩＧＢを生成するためにユーザＢの秘密鍵によって取引（E_{KB}（r_t，ｔ），Ｔ）を署名してもよい。署名は、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）のようなデジタル署名アルゴリズム（ＤＳＡ）に従ってもよく、これによって、署名の受取人は、署名されたデータを認証するために署名者の公開鍵によって署名を確認することができる。署名ＳＩＧＢは、着信者ノードＢが取引に合意したことを表す。

【００８３】

ステップ２０５において、ノードＢは、署名された取引E_{KB}（r_t，ｔ）及び署名ＳＩＧＢをノードＡに戻してもよい。

【００８４】

ステップ２０６において、ＳＩＧＢの確認が成功しない場合、ノードＡは、取引を拒否してもよい。ＳＩＧＢの確認が成功した場合、ノードＡは、ＰＣ（r_t，ｔ）の値及びＰＣ（r_y，ｙ）の値がそれぞれ有効範囲内であるか否かをブロックチェーンノードに対して証明するために範囲証明ＰＲを生成してもよい。例えば、ＰＣ（r_t，ｔ）の有効値を有するために、取引金額ｔは、有効範囲［０，2^n－１］内であってもよく、ＰＣ（r_y，ｙ）の有効値を有するために、チェンジｙは、有効範囲［０，2^n－１］内であってもよい。一実施の形態において、ノードＡは、後のステップにおいて取引金額ｔ及びチェン

ジｙが有効範囲内にあるか否かを範囲証明に基づいて確認するために、ブロックチェーンノード（例えば、コンセンサスノード）の（Ｔ，r_t，ｔ，Ｙ，r_y，ｙ）に関連する範囲証明を生成するブロック証明技術（ｂｌｏｃｋ　ｐｒｏｏｆ　ｔｅｃｈｎｉｑｕｅ）を用いることができる。範囲証明は、例えば、Ｂｕｌｌｅｔｐｒｏｏｆｓ、ボロミアンリング署名等を備えてもよい。

【００８５】

さらに、ノードＡは、署名ＳＩＧＡを生成するためにユーザＡの秘密鍵SK_Aによって取引に署名を行ってもよい。同様に、署名は、デジタル署名アルゴリズム（ＤＳＡ）に従ってもよい。一部の実施の形態において、ノードＡは、署名ＳＩＧＡを生成するためにユーザＡの秘密鍵によって（｛ＰＣ（r_{a1},a_1），E_{KA}（r_{a1},a_1）；ＰＣ（r_{a2},a_2），E_{KA}（r_{a2},a_2）；．．．ＰＣ（r_{ak},a_k），E_{KA}（r_{ak},a_k）｝；｛ＰＣ（r_y,ｙ），E_{KA}（r_y，Ｙ）｝；｛ＰＣ（r_t,ｔ），E_{KB}（r_t,ｔ）｝；Ｙ；Ｔ；ｒ’；ＲＰ）を署名してもよく、この場合、｛ＰＣ（r_{a1},a_1），E_{KA}（r_{a1},a_1）；ＰＣ（r_{a2},a_2），E_{KA}（r_{a2},a_2）；．．．ＰＣ（r_{ak},a_k），E_{KA}（r_{ak},a_k）｝は、取引のために口座Ａから選ばれた資産A_1，A_2，．．．，A_kを表す。｛ＰＣ（r_y,ｙ），E_{KA}（r_y，Ｙ）｝は、口座Ａが取引から受け取るチェンジを表す。｛ＰＣ（r_t,ｔ），E_{KB}（r_t,ｔ）｝は、口座Ｂが取引から受け取る移された資産を表す。

【００８６】

ステップ２０７において、ノードＡは、ブロックチェーンに取引を提示し、これによって、ブロックチェーンノードは、取引を確認するとともに取引をブロックチェーンに加えるべきか否かを判断する。一実施の形態において、ノードＡは、取引を実行するためにノード１を介して取引（｛ＰＣ（r_{a1},a_1），E_{KA}（r_{a1},a_1）；ＰＣ（r_{a2},a_2），E_{KA}（r_{a2},a_2）；．．．ＰＣ（r_{ak},a_k），E_{KA}（r_{ak},a_k）｝；｛ＰＣ（r_y,ｙ），E_{KA}（r_y,ｙ）｝；｛ＰＣ（r_t,ｔ），E_{KB}（r_t,ｔ）｝；Ｙ；Ｔ；ｒ’；ＲＰ；ＳＩＧＡ；ＳＩＧＢ）を提示してもよい。取引は、他のパラメータを備えてもよい又はリストされたパラメータの全てを備えなくてもよい。取引を、確認のためにブロックチェーンの一つ以上のノード（例えば、コンセンサスノード）に送信してもよい。確認が成功する場合、取引をブロックチェーンに加える。確認が成功しない場合、取引がフロックチェーンに加えられるのを拒否される。

【００８７】

ステップ２１３～２１８において、一つ以上のノード（例えば、コンセンサスノード）は、提示された取引の署名、範囲証明及び他の情報を確認する。確認が成功しない場合、ノードは、取引を拒否する。確認が成功した場合、ノードは、取引を受け入れ、ユーザＡの口座及びユーザＢの口座を更新する。

【００８８】

一部の実施の形態において、取引を実行するために、取引情報を種々のブロックチェーンノードによって確認してもよい。取引情報は、取引アドレスＴＸＩＤ、（一つ以上の）署名、入力及び出力を備えてもよい。ＴＸＩＤは、取引内容のハッシュを備えてもよい。署名は、発信者及び着信者による暗号鍵署名を備えてもよい。入力は、ブロックチェーンの発信者の口座のアドレス、取引のために発信者のブロックチェーンから選ばれた一つ以上の資産等を備えてもよい。出力は、ブロックチェーンの着信者の口座のアドレス、着信者の（一つ以上の）資産の（一つ以上の）資産タイプ、信者の（一つ以上の）資産の（一つ以上の）コミットメント値等を備えてもよい。入力及び出力は、表形式のインデックス付き情報を備えてもよい。一部の実施の形態において、ノートＩＤ値の値を、「ＴＸＩＤ＋出力の資産のインデックス」とすることができる。

【００８９】

一部の実施の形態において、ブロックチェーンの一つ以上のノードは、提示された取引（｛ＰＣ（r_{a1},a_1），E_{KA}（r_{a1},a_1）；ＰＣ（r_{a2}，a_2），E_{KA}（r_{a2}，a_2）；．．．ＰＣ（r_{ak},a_k），E_{KA}（r_{ak},a_k）｝；｛ＰＣ（r_y，

y），E_{KA}（r_y，y）｝；｛PC（r_t，t），E_{KB}（r_t，t）｝；Y；T；r’；RP；SIGA；SIGB）を確認してもよい。

【００９０】

ステップ２０８において、ノードは、二重払い防止（ａｎｔｉ－ｄｏｕｂｌｅ－ｓｐｅｎｄｉｎｇ）機構又はリプレイアタック防止（ａｎｔｉ－ｒｅｐｌａｙ－ａｔｔａｃｋ）機構を用いて取引が実行されたか否かを確認してもよい。取引が実行された場合、ノードは、取引を拒否してもよい。そうでない場合、方法は、ステップ２０９に進む。

【００９１】

ステップ２０９において、ノードは、（例えば、Ａの公開鍵及びＢの公開鍵に基づいて）署名ＳＩＧＡ及びＳＩＧＢをそれぞれチェックしてもよい。署名のいずれかが正しくない場合、ノードは、取引を拒否してもよい。そうでない場合、方法は、ステップ２１０に進む。

【００９２】

任意のステップ２１０において、ノードは、資産タイプが一致するか否かを確認してもよい。例えば、ノードは、A_1～A_kのノートタイプの資産タイプが取引金額ｔの（一つ以上の）資産タイプに一致するか否かを確認してもよい。資産タイプのいずれかが一致しない場合、ノードは、取引を拒否してもよい。そうでない場合、方法は、ステップ２１１に進む。一部の実施の形態において、ウォレットの元の資産タイプは、為替レートに基づいて他のタイプに変換してもよく、このステップをスキップしてもよい。

【００９３】

ステップ２１１において、ノードは、PC（r_t，t）の値及びPC（r_y，y）の値を認証するために範囲証明ＲＰをチェックしてもよい。一部の実施の形態において、ノードは、取引金額ｔが０以上であるとともにチェンジｙが０以上であるか否かを確認するために範囲証明ＰＲをチェックしてもよい。確認が成功しない場合、ノードは、取引を拒否してもよい。そうでない場合、方法は、ステップ２１２に進む。

【００９４】

ステップ２１２において、ノードは、取引の入力及び出力が一致するか否かをチェックしてもよい。一部の実施の形態において、ｒ’は、同形特性に基づく資産価値ｔ’＝a_1＋a_2．．．＋a_k－ｔ－ｙに対応してもよく、この場合、ｒ’＝（r_1＋r_2．．．＋r_k）－r_t－r_yである。入力する資産がa_1＋a_2．．．＋a_kであるとともに出力がｔ＋ｙであるので、入力と出力が一致する（a_1＋a_2．．．＋a_k＝ｔ＋ｙ）ときにｔ’＝０である。したがって、ｒ’に対応するコミットメント値は、ＰＣ（ｒ’，ｔ’）＝ｒ’×Ｇ＋ｔ’×Ｈ＝ｒ’Ｇである。ｒ’＝（r_1＋r_2．．．＋r_k）－r_t－r_yであるので、ノードは、ｒ’Ｇが（r_1＋r_2．．．＋r_k）－r_t－r_yに対応するPC$_1$＋．．．＋PC$_k$－Ｔ－Ｙに等しいか否かを確認することによって入力と出力が等しいか否かを判断することができる。ｒ’ＧがPC$_1$＋．．．＋PC$_k$－Ｔ－Ｙに等しい場合、ノードは、取引の入力と出力が一致すると判断するとともに次のステップに進むことができる。そうでない場合、ノードは、取引の入力と出力が一致しないと判断するとともに取引を拒否してもよい。

【００９５】

ステップ２１３において、ノードは、ノードＡが取引から選択した（一つ以上の）資産を有するか否かを確認してもよい。一実施の形態において、ノードは、この確認を、口座Ａに対応する情報のようなブロックチェーンに記憶された情報に基づいて行ってもよい。情報は、全ての資産の以前の取引情報を備えてもよい。したがって、ノードは、口座Ａが取引する資産を有するか否かを判断することができる。判断が否である場合、ノードは、取引を拒否してもよい。そうでない場合、方法は、ステップ２１４に進む。

【００９６】

ステップ２１４において、ノードは、口座Ａ及び口座Ｂを更新してもよい。例えば、ノードは、金額ｔで取引する資産を口座Ａから除去するとともにそれを口座Ｂに加えてもよい。同形特性に基づいて、Ｙ＝ＰＣ（r_y，y）であり、ノード１がr_yを既知であると

ともにブロックチェーンからコミットメント値Ｙにアクセスすることができるので、ノード１は、資産価値ｙを取得するとともに口座Ａに戻すためにＹを解読することができる。ノード２は、ステップ２０２で乱数r_tをノード１から取得するとともにブロックチェーンからコミットメント値Ｙを取得することができる。したがって、ノード２は、資産価値ｔを取得するとともの口座Ｂに加えるためにＴを解読することができる。

【００９７】

一例において、口座Ａ及び口座Ｂを更新した後に、口座Ａは、選んだ資産A_1，A_2，．．．，A_kに対するチェンジｙを受け取るとともに選ばない資産A_{ak+1}，．．．，A_mを受け取り、口座Ｂは、取引金額ｔを受け取るとともに元の資産B_1，B_2，．．．，B_nを受け取る。Ａの口座の資産及びＢの口座の資産は、次の通りである。

【００９８】

Ａの口座（口座Ａ）に対して、更新した資産は、次のように表される。

（$Y=PC(r_y,y),E_{KA}(r_y,y)$），

（$A_{ak+1}=PC(r_{ak+1},a_{k+1}),E_{KA}(r_{ak+1},a_{k+1})$）

（$A_{ak+2}=PC(r_{ak+2},a_{k+2}),E_{KA}(ra_{k+2},a_{k+2})$）

．．．

（$A_m=PC(r_{am},a_m),E_{KA}(r_{am},a_m)$）

【００９９】

Ｂの口座（口座Ｂ）に対して、更新した資産は、次のように表される。

（$B_1=PC(r_{b1},b_1),E_{KB}(r_{b1},b_1)$），

（$B_2=PC(rb_2,b_2),E_{KB}(r_{b2},b_2)$），

．．．

（$B_n=PC(r_{bn},b_n),E_{KB}(r_{bn},b_n)$），

（$T=PC(r_t,t),E_{KB}(r_t,t)$）

【０１００】

本開示は、発信者及び着信者をそれぞれ説明するためのノードＡ／ユーザＡ及びノードＢ／ユーザＢを用いるが、発信者及び着信者を同一のノード／ユーザとすることができる。例えば、取引のチェンジｙ（口座Ａの選んだ資産の合計から取引金額を引いたもの）を取引の発信者に戻してもよい。したがって、ここで説明するようなノードＢによって実行される種々のステップを、ノードＡによって代わりに実行してもよい。

【０１０１】

図３は、本開示の種々の実施の形態による情報保護のための例示的な方法３００のフローチャートを示す。方法３００を、図１のシステム１００の一つ以上の構成要素（例えば、ノードＡ、ノード１、ノードＡとノード１の組合せ）によって実施してもよい。方法３００を、プロセッサと命令を記憶する非一時的コンピュータ可読記憶媒体（例えば、メモリ）を備えるシステム又は装置（例えば、コンピュータ、サーバ）によって実施してもよい。命令は、プロセッサによって実行されるときに、システム又は装置（例えば、プロセッサ）によって方法３００を実施させる。後に説明する方法３００の動作は、説明することを意図したものである。実現に応じて、方法３００は、種々の順番で又は並列に実行される追加のステップ、更に少ないステップ又は代替的なステップを有してもよい。

【０１０２】

ブロック３０１は、トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームに取引金額ｔの取引をコミットし、チェンジコミットメント値Ｙを取得するために第２のコミットメントスキームにチェンジｙの取引をコミットし、第１のコミットメントスキームは、トランザクションブラインディングファクタr_tを備え、第２のコミットメントスキームは、チェンジブラインディングファクタr_yを備えることを備える。一部の実施の形態において、第１のコミットメントスキームは、少なくともトランザクションブラインディングファクタr_tに基づくとともに取引金額ｔが対応するコミッテッド値であるペダーソンコミットメントを備える。例えば、Ｔ＝ＰＣ（r_t，ｔ）を参照。一部の実施の形態において、第２のコミットメントスキームは、少なくともチェンジ

ブラインディングファクタr_yに基づくとともにチェンジｙが対応するコミッテッド値であるペダーソンコミットメントを備える。例えば、Ｙ＝ＰＣ（r_y，ｙ）を参照。

【０１０３】

ブロック３０２は、チェンジブラインディングファクタr_yとチェンジｙの第１の組合せを第１の鍵ＫＡによって暗号化することを備える。

【０１０４】

ブロック３０３は、取引の着信者に関連する着信者ノードが取引を確認するために、トランザクションブラインディングファクタr_t、取引金額ｔ及びトランザクションコミットメント値Ｔを着信者ノードに送信することを備える。一部の実施の形態において、取引の着信者に関連する着信者ノードが取引を確認するために、トランザクションブラインディングファクタr_t、取引金額ｔ及びトランザクションコミットメント値Ｔを着信者ノードに送信することは、トランザクションブラインディングファクタr_t、取引金額ｔ及びトランザクションコミットメント値Ｔを着信者ノードに送信することによって、着信者ノードは、トランザクションコミットメント値Ｔが取引金額ｔをトランザクションブラインディングファクタr_tにコミットする第１のコミットメントスキームに等しいか否かを確認することを備える。

【０１０５】

ブロック３０４は、着信者ノードの取引の確認の成功に応答して、第２の鍵ＫＢによって暗号化されたトランザクションブラインディングファクタr_t及び取引金額ｔの暗号化された第２の組合せを取得することを備える。一部の実施の形態において、暗号化された第２の組合せを取得することは、暗号化された第２の組合せと、暗号化された第２の組合せ及びトランザクションコミットメント値Ｔに関連する署名ＳＩＧＢを着信者ノードから受け取ることを備える。

【０１０６】

ブロック３０５は、ブロックチェーンの複数のノードが取引を確認するために、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信することを備える。

【０１０７】

一部の実施の形態において、取引金額ｔは、取引の発信者の一つ以上の資産A_1，A_2，．．．，A_kから選ばれ、資産の各々は、（１）少なくとも各資産のブラインディングファクタr_{a_k}及び値に基づくペダーソンコミットメント及び（２）少なくとも各資産のブラインディングファクタr_{a_k}及び値に基づく暗号化に関連し、チェンジｙは、取引金額ｔと選ばれた資産の間の差である。

【０１０８】

一部の実施の形態において、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信する前に、方法は、署名ＳＩＧＢを確認することと、署名ＳＩＧＢの確認の成功に応答して、資産A_1，A_2，．．．，A_k、第１の組合せ、第２の組合せ、トランザクションコミットメント値Ｔ、チェンジコミットメント値Ｙ及び資産A_1，A_2，．．．，A_kに対応するブラインディングファクタの和とトランザクションブラインディングファクタr_t及びチェンジブラインディングファクタr_yの和との差に関連する署名ＳＩＧＡを生成することと、を更に備える。すなわち、差は、$r' = (r_1 + r_2 . . . + r_k) - (r_t + r_y)$である。

【０１０９】

一部の実施の形態において、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信することは、資産A_1，A_2，．．．，A_k、第１の組合せ、第２の組合せ、トランザクションコミットメント値Ｔ、チェンジコミットメント値Ｙ及び資産A_1，A_2，．．．，A_kに対応するブラインディングファクタの和とトランザクションブラインディングファクタr_t、チェンジブラインディングファクタr_yの和との差、署名ＳＩＧＡ及び署名ＳＩＧＢを、ブロックチェーンの複数のノードに送信すること備える。

【０１１０】
一部の実施の形態において、ブロックチェーンの複数のノードが取引を確認するために、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信することは、暗号化された第１の組合せ及び暗号化された第２の組合せをブロックチェーンの複数のノードに送信することによって、ブロックチェーンの複数のノードは、取引の確認の成功に応答して、着信者に取引金額ｔを発し、資産A_1，A_2，．．．，A_kを削除し、発信者にチェンジｙを発することを備える。
【０１１１】
図４は、種々の実施の形態による例示的な情報保護のための方法４００のフローチャートを示す。方法４００を、図１のシステム１００の一つ以上の構成要素（例えば、ノードＢ、ノード２、ノードＢとノード２の組合せ）によって実施してもよい。方法４００を、プロセッサと命令を記憶する非一時的コンピュータ可読記憶媒体（例えば、メモリ）を備えるシステム又は装置（例えば、コンピュータ、サーバ）によって実施してもよい。命令は、プロセッサによって実行されるときに、システム又は装置（例えば、プロセッサ）によって方法４００を実施させる。後に説明する方法４００の動作は、説明することを意図したものである。実現に応じて、方法４００は、種々の順番で又は並列に実行される追加のステップ、更に少ないステップ又は代替的なステップを有してもよい。
【０１１２】
ブロック４０１は、トランザクションブラインディングファクタr_t、取引金額ｔの取引及びトランザクションコミットメント値Ｔを取引の発信者に関連する発信者ノードから取得し、取引金額ｔは、トランザクションコミットメント値Ｔを取得するために第１のコミットメントスキームにコミットされ、第１のコミットメントスキームは、トランザクションブラインディングファクタr_tを備えることを備える。
【０１１３】
ブロック４０２は、取得したトランザクションブラインディングファクタr_t、取得した取引金額ｔの取引及び取得したトランザクションコミットメント値Ｔに基づいて取引を確認することを備える。一部の実施の形態において、取得したトランザクションブラインディングファクタr_t、取得した取引金額ｔの取引及び取得したトランザクションコミットメント値Ｔに基づいて取引を確認することは、トランザクションコミットメント値Ｔが取引金額ｔを取得したトランザクションブラインディングファクタr_tにコミットする第１のコミットメントスキームに等しいか否かを確認することを備える。
【０１１４】
ブロック４０３は、取引の確認の成功に応答して、トランザクションブラインディングファクタr_t及び取引金額ｔの第２の組合せを第２の鍵ＫＢによって暗号化することを備える。
【０１１５】
ブロック４０４は、暗号化された第２の組合せを発信者ノードに送信することを備える。一部の実施の形態において、暗号化された第２の組合せを発信者ノードに送信する前に、方法は、暗号化された第２の組合せ及びトランザクションコミットメント値Ｔに関連する署名ＳＩＧＢを生成することを更に備え、暗号化された第２の組合せを発信者ノードに送信することは、暗号化された第２の組合せ及び署名ＳＩＧＢを発信者ノードに送信すること備える。
【０１１６】
図示したように、取引金額のプライバシーを、コンピュータ技術の種種の改善によって保護することができる。例えば、取引構造は、資産価値のペダーソンコミットメントに関連する第１のフィールド（例えば、第１のフィールドは、ＰＣ（$r_{a\,i}$，a_i）であり、ｉは、１とｍの間である）及び資産価値のペダーソンコミットメントに関連する第２のフィールド（例えば、第２のフィールドは、E_{KA}（$r_{a\,i}$，a_i）であり、ｉは、１とｍの間である）のような一つ以上のフィールドを備える。第１のフィールド及び第２のフィールドは、取引ステップで用いられるとともにブロックチェーンに記憶される。

【０１１７】
他の例に対して、暗号鍵を、各ペダーソンコミットメントの乱数及び対応する資産価値を暗号化するために用いる。暗号化／解読のための暗号鍵は、資産所有者によって保持され、したがって、資産価値のプライバシーは、暗号鍵を有しないユーザから保護される。さらに、暗号化された乱数及び資産価値を含む取引をブロックチェーンに記憶することができる。この方法は、乱数を管理する際の利便性を提供し、乱数及び資産価値の消失及び変更の機会を最小にし、分配されるとともに一貫したブロックチェーン記憶に基づいてセキュリティを高める。
【０１１８】
取引をブロックチェーンに提示する前のステップを、「オフチェーン」又は「事前取引」動作として取り扱うことができる。その理由は、Ｅ（）関数によって表される暗号化された「試算価値＋対応する乱数」をブロックチェーンが記憶する間に暗号化処理及び解読処理がクライアント側で発生するからである。ペダーソンコミットメントは、資産が中にある金庫と似ていてもよく、「試算価値＋対応する乱数」は、金庫の鍵と似ていてもよい。暗号化された鍵及び関連の金庫をブロックチェーンに記憶することができ、それは、改ざん防止であるとともに消失防止を行う。ユーザが（一つ以上の）資産を使うことを所望する度に、ユーザは、金庫及び暗号鍵をブロックチェーンから検索するとともに鍵をクライアント側で解読することができ、その結果、「事前取引」ステップを、（一つ以上の）資産を使う新たな取引を構築するために実行することができる。
【０１１９】
そのようにして、ペダーソンコミットメントの乱数を、破損のリスクなく、かつ、追加の鍵の管理の負担が生じることなく便利に管理することができる。したがって、取引プライバシーを完全に保護することができ、取引金額を秘密に保持することができる。
【０１２０】
ここで説明した技術は、一つ以上の専用コンピュータデバイスによって実現される。専用コンピュータデバイスを、デスクトップコンピュータシステム、サーバコンピュータシステム、ポータブルコンピュータシステム、携帯装置、ネットワークデバイス又は技術を実現するためのハードワイヤード及び／又はプログラム論理を包含する他の任意の装置又は装置の組合せであってもよい。（一つ以上の）コンピュータデバイスは、一般的には、オペレーティングシステムソフトウェアによって制御及び調整される。通常のオペレーティングシステムは、コンピュータプロセスを実行するための制御及びスケジューリングを行い、メモリ管理を行い、ファイルシステム、ネットワーク及びＩ／Ｏサービスを提供し、かつ、特にグラフィカルユーザインタフェース（ＧＵＩ）のようなユーザインタフェース機能を提供する。
【０１２１】
図５は、ここで説明する実施の形態のいずれかを実現することができる例示的なコンピュータシステム５００のブロック図を示す。システム５００を、ここで説明するノードのいずれかにおいて実現してもよく、情報保護方法の対応するステップを実行するように構成してもよい。コンピュータシステム５００は、情報の通信を行うためのバス５０２又は他の通信機構と、情報を処理するためにバス５０２に結合された一つ以上のハードウェアプロセッサ５０４と、を有する。（一つ以上の）ハードウェアプロセッサ５０４は、例えば、一つ以上の汎用マイクロプロセッサであってもよい。
【０１２２】
コンピュータシステム５００は、情報と（一つ以上の）プロセッサ５０４によって実行される命令とを記憶するためにバス５０２に結合されたランダムアクセスメモリ（ＲＡＭ）、キャッシュ及び／又は他のダイナミック記憶装置のような主記憶装置５０６も有する。主記憶装置５０６を、（一つ以上の）プロセッサ５０４によって実行される命令の実行中に変数又は他の中間情報（ｉｎｔｅｒｍｅｄｉａｔｅ　ｉｎｆｏｒｍａｔｉｏｎ）を一時的に記憶するのに用いてもよい。そのような命令は、（一つ以上の）プロセッサ５０４にアクセス可能な記憶媒体に記憶されるときに、カスタマイズされた専用マシンのコンピ

ュータシステム５００によって、命令で指定された動作を実行する。コンピュータシステム５００は、（一つ以上の）プロセッサ５０４の静的情報及び命令を記憶するためにバス５０２に結合されたリードオンリーメモリ（ＲＯＭ）も有する。磁気ディスク、光ディスク、ＵＳＢサムドライブ（フラッシュドライブ）のような記憶装置５１０を、情報及び命令を記憶するために設けるとともにバス５０２に結合する。

【０１２３】

システム５００は、コンピュータシステムと協働してコンピュータシステム５００を専用マシンにする又は専用マシンにプログラムするカスタマイズされたハードワイヤード論理、一つ以上のＡＳＩＣ又はＦＰＧＡ、ファームウェア及び／又はプログラム論理を用いることによって、ここで説明する技術を実現してもよい。一実施の形態によれば、ここで説明する動作、方法及びプロセスを、主記憶装置５０６に含まれる一つ以上の命令の一つ以上のシーケンスを実行する（一つ以上の）プロセッサ５０４に応答してコンピュータシステム５００によって実行する。そのような命令を、記憶装置５１０のような他の記憶媒体から主記憶装置５０６に読み込んでもよい。主記憶装置５０６に含まれる命令のシーケンスを実行することによって、一つ以上のプロセッサ５０４は、ここで説明する処理工程を実行する。代替的な実施の形態において、ハードワイヤード回路を、ソフトウェア命令の代わりに又はソフトウェア命令と共に用いてもよい。

【０１２４】

主記憶装置５０６、ＲＯＭ５０８及び／又は記憶装置５１０は、非一時的記憶媒体を有してもよい。ここで用いるような用語「非一時的媒体」及び同様な用語は、マシンを特定の方法で動作させるデータ及び／又は命令を記憶する媒体を意味し、当該媒体は、一時的な信号を除外する。そのような非一時的媒体は、不揮発性媒体及び／又は揮発性媒体を備えてもよい。不揮発性媒体は、例えば、記憶装置５１０のような光ディスク又は磁気ディスクを含む。揮発性媒体は、主記憶装置５０６のようなダイナミックメモリを含む。非一時的媒体の一般的形式は、例えば、フロッピーディスク（登録商標）、フレキシブルディスク、ハードディスク、固体ドライブ、磁気テープ又は他の任意の磁気データ記憶媒体、ＣＤ－ＲＯＭ、他の任意の光データ記憶媒体、孔のパターンを有する任意の物理媒体、ＲＡＭ、ＰＲＯＭ、ＥＰＲＯＭ、フラッシュＥＰＲＯＭ、ＮＶＲＡＭ、他の任意のメモリチップ若しくはカートリッジ及びこれらのネットワーク形態を含む。

【０１２５】

コンピュータシステム５００は、バス５０２に結合されたネットワークインタフェース５１８も有する。ネットワークインタフェース５１８は、一つ以上のローカルネットワークに接続された一つ以上のネットワークリンクに結合する双方向データ通信を提供する。例えば、ネットワークインタフェース５１８は、総合デジタル通信網（ＩＳＤＮ）カード、ケーブルモデム、衛星モデム又は対応するタイプの電話線に対するデータ通信を提供するモデムであってもよい。他の例として、ネットワークインタフェース５１８は、互換性のあるＬＡＮ（又はＷＡＮと通信を行うＷＡＮ構成要素）に対するデータ通信接続を提供するローカルエリアネットワーク（ＬＡＮ）カードであってもよい。無線リンクを実現してもよい。そのようないずれかの実現において、ネットワークインタフェース５１８は、種々のタイプの情報を表すデジタルデータストリームを搬送する電気信号、電磁信号又は光信号を送受信する。

【０１２６】

コンピュータシステム５００は、（一つ以上の）ネットワーク、ネットワークリンク及びネットワークインタフェース５１８を介してメッセージを送信するとともにプログラムコードを含むデータを受信することができる。インターネットの例において、サーバは、インターネット、ＩＳＰ，ローカルネットワーク及びネットワークインタフェース５１８を介して、アプリケーションプログラムの要求されるコードを送信する。

【０１２７】

受信したコードを、受信の際に（一つ以上の）プロセッサ５０４によって実行してもよい及び／又は後の実行のために記憶装置５１０又は他の不揮発性記憶装置に記憶してもよ

い。

【０１２８】

前のセクションで説明したプロセス、方法及びアルゴリズムの各々を、コンピュータハードウェアを備える一つ以上のコンピュータシステム又はコンピュータプロセッサによって実行されるコードモジュールで実施するとともに当該コードモジュールによって完全に又は部分的に自動化してもよい。プロセス及びアルゴリズムを、特定用途向け乖離で部分的に又は完全に実現してもよい。

【０１２９】

上述した種々の特徴及びプロセスを互いに独立して用いてもよい又は種々の方法で組み合わせて用いてもよい。全てのあり得る組合せ及び部分的組合せは、本開示の範囲に入ることを意図する。追加的に、所定の方法又は処理ブロックを一部の実現において省略してもよい。ここで説明する方法及びプロセスは、任意の特定の順番に限定されず、それに関連するブロック及び段階（ｓｔａｔｅ）を、適切な他の順番で実行してもよい。例えば、説明したブロック又は段階を特に開示した順番以外の順番で実行してもよい又は複数のブロック又は段階を単一のブロック又は段階で組み合わせてもよい。例示的なブロック又は段階を、シリアルに、並列に又は他の方法で実行してもよい。ブロック又は段階を開示した例示的な実施の形態に加えてもよい又は開示した例示的な実施の形態から除去してもよい。ここで説明する例示的なシステム及び構成要素を、開示したのと異なるように構成してもよい。例えば、素子を、開示した例示的な実施の形態に追加してもよい、開示した例示的な実施の形態から除外してもよい又は開示した例示的な実施の形態において位置を変えてもよい。

【０１３０】

ここで説明する例示的な方法の種種の動作を、アルゴリズムによって少なくとも部分的に実行してもよい。アルゴリズムは、メモリ（例えば、上述した非一時的コンピュータ可読記憶媒体）に記憶されたプログラムコード又は命令に含まれてもよい。そのようなアルゴリズムは、機械学習アルゴリズムを備えてもよい。一部の実施の形態において、機械学習アルゴリズムは、機能を実行するためにコンピュータを明示的にプログラムしなくてもよいが、機能を実行する予測モデルを形成するためにトレーニングデータから学習を行うことができる。

【０１３１】

ここで説明する例示的な方法の種種の動作を、関連の動作を実行するために（例えば、ソフトウェアによって）一時的に構成された又は永久的に構成された一つ以上のプロセッサによって少なくとも部分的に実行してもよい。一時的に構成されているか永久的に構成されているかに関係なく、そのようなプロセッサは、ここで説明する一つ以上の動作又は機能を実行するために動作するプロセッサで実施されるエンジンを構成してもよい。

【０１３２】

同様に、ここで説明する方法を、ハードウェアの例である特定の一つ以上のプロセッサを用いることによって少なくとも部分的にプロセッサで実施してもよい。例えば、方法の動作の少なくとも一部を、一つ以上のプロセッサ又はプロセッサで実施されるエンジンによって実行してもよい。さらに、一つ以上のプロセッサは、「クラウドコンピューティング」環境において又は「サービスとしてのソフトウェア」（ＳａａＳ）として関連の動作の実行をサポートするように動作してもよい。例えば、動作の少なくとも一部を、（プロセッサを有するマシンの例としての）一群のコンピュータによって実行してもよく、これらの動作は、ネットワーク（例えば、インターネット）を介して及び一つ以上の適切なインタフェース（例えば、アプリケーションプログラムインタフェース（ＡＰＩ））を介して利用可能である。

【０１３３】

所定の動作の性能（ｐｅｒｆｏｒｍａｎｃｅ）を、単一のマシン内に存在するプロセッサの間だけでなく複数のマシンに亘って配置されたプロセッサの間に分布させることができる。一部の例示的な実施の形態において、プロセッサ又はプロセッサで実施するエンジ

ンを、（例えば、家庭環境、オフィス環境又はサーバファーム内の）単一の地理的な位置に配置してもよい。他の例示的な実施の形態において、プロセッサ又はプロセッサで実施するエンジンを、複数の地理的な位置にわたって分布させてもよい。

【０１３４】

本明細書を通じて、複数の例は、単一の例として説明した構成要素、動作又は構造を実現してもよい。一つ以上の方法の個別の動作を個別の動作として図示及び説明したが、個別の動作の一つ以上を同時に実行してもよく、説明した順番で動作を実行する必要はない。例示的な形態において個別の構成要素として示した構造及び機能を、組み合わせた構造又は構成要素として実現してもよい。同様に、単一の構成要素として示した構造及び機能を、個別の構成要素として実現してもよい。これらの変形、変更、追加及び改善並びに他の変形、変更、追加及び改善は、ここでの主題の範囲内にある。

【０１３５】

主題の概観を特定の例示的な実施の形態を参照しながら説明したが、種種の変更及び変形が、本開示の実施の形態の広い範囲から逸脱することなくこれらの実施の形態において行ってもよい。主題のそのような実施の形態を、本願の範囲を実際に一つ以上の開示又は概念が存在する場合の任意の一つの開示又は概念に自発的に限定することを意図することなく単なる便宜上の用語「発明」によって個別に又は集合的にここに示す。詳細な説明を限定の意味ととるべきではなく、種々の実施の形態の範囲は、添付した特許請求の範囲によって、そのような特許請求の範囲の権利が与えられる等価物の全範囲と共に規定される。

【図１】

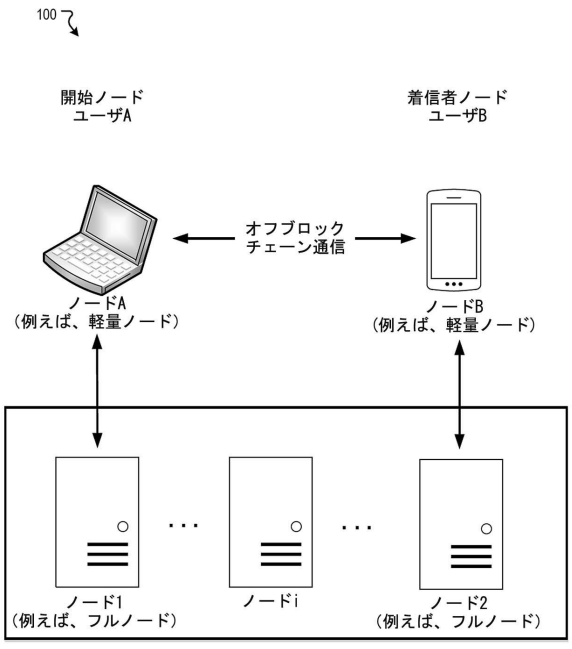

FIG. 1

【図２】

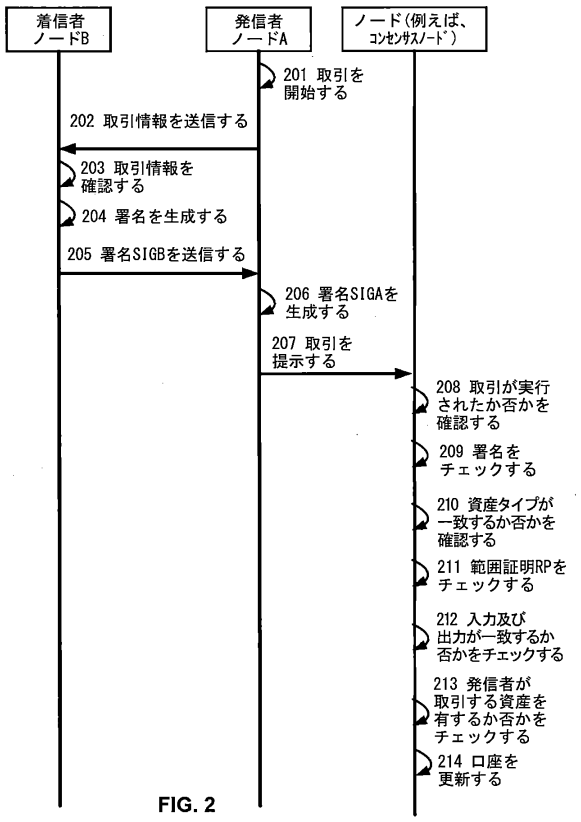

FIG. 2

【図３】

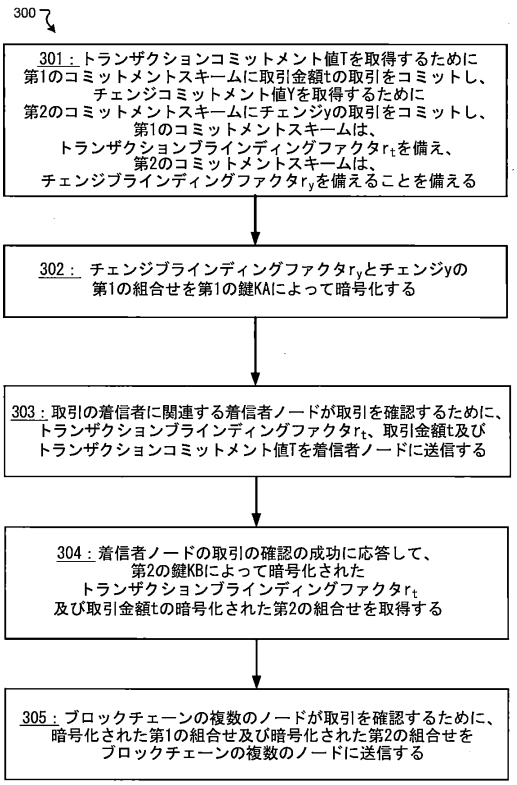

FIG. 3

【図４】

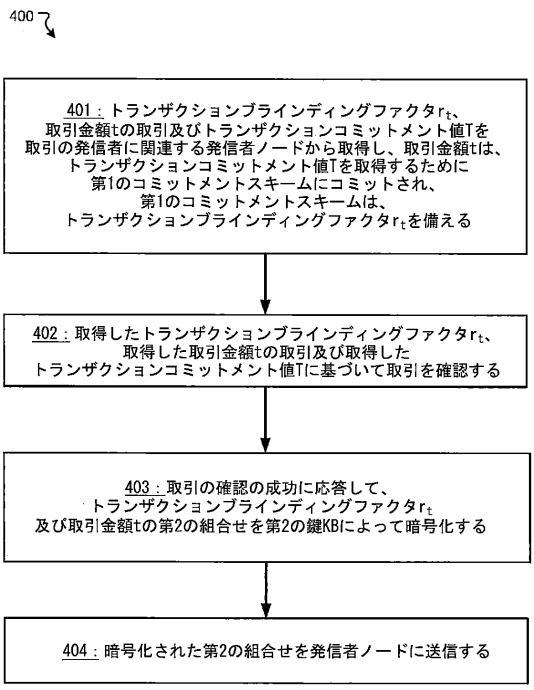

FIG. 4

【図５】

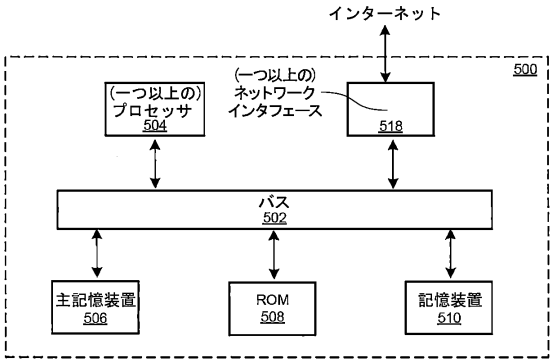

FIG. 5

フロントページの続き

(74)代理人 100165191
弁理士 河合 章
(74)代理人 100133835
弁理士 河野 努
(72)発明者 マー ホアンユイ
中華人民共和国, ジョージアーン ３１１１２１, ハーンジョウ, ユイ ハーン ディストリクト, ウエスト ウエン イー ロード ナンバー９６９, ビルディング ３, ５／フロア, アリババ グループ リーガル ディパートメント
(72)発明者 チャン ウェンピン
中華人民共和国, ジョージアーン ３１１１２１, ハーンジョウ, ユイ ハーン ディストリクト, ウエスト ウエン イー ロード ナンバー９６９, ビルディング ３, ５／フロア, アリババ グループ リーガル ディパートメント
(72)発明者 マー パオリー
中華人民共和国, ジョージアーン ３１１１２１, ハーンジョウ, ユイ ハーン ディストリクト, ウエスト ウエン イー ロード ナンバー９６９, ビルディング ３, ５／フロア, アリババ グループ リーガル ディパートメント
(72)発明者 リウ チョン
中華人民共和国, ジョージアーン ３１１１２１, ハーンジョウ, ユイ ハーン ディストリクト, ウエスト ウエン イー ロード ナンバー９６９, ビルディング ３, ５／フロア, アリババ グループ リーガル ディパートメント
(72)発明者 ツイ チアホイ
中華人民共和国, ジョージアーン ３１１１２１, ハーンジョウ, ユイ ハーン ディストリクト, ウエスト ウエン イー ロード ナンバー９６９, ビルディング ３, ５／フロア, アリババ グループ リーガル ディパートメント

審査官 行田 悦資

(56)参考文献 米国特許出願公開第２０１６／０３５８１６５（ＵＳ，Ａ１）
米国特許出願公開第２０１８／００３４６３４（ＵＳ，Ａ１）
特開２０２０－７１６１７（ＪＰ，Ａ）
PEDERSEN, T. P., Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing, Advances in Cryptology - CRYPTO'91, ドイツ, Springer-Verlag, １９９２年, LNCS 576, pp.129-140, <DOI:https://doi.org/10.1007/3-540-46766-1_9>

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／６０
Ｇ０６Ｑ ２０／３８