(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-195627
(P2017-195627A)
(43)公開日　平成29年10月26日(2017.10.26)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
H04L 9/32	(2006.01)	H04L	9/00	601E	5L055
G09C 1/00	(2006.01)	H04L	9/00	675B	
G06Q 20/38	(2012.01)	G09C	1/00	640D	
G06F 21/60	(2013.01)	G06Q	20/38	310	

審査請求 有　請求項の数 6　ＯＬ　公開請求　（全 21 頁）　最終頁に続く

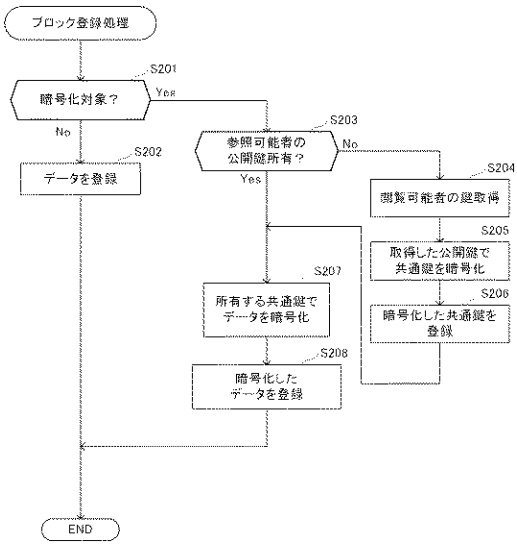
(21)出願番号　特願2017-123622 (P2017-123622)
(22)出願日　平成29年6月23日 (2017.6.23)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(74)代理人　100095407
弁理士　木村　満
(74)代理人　100132883
弁理士　森川　泰司
(74)代理人　100166442
弁理士　鈴木　洋雅
(74)代理人　100174067
弁理士　湯浅　夏樹
(74)代理人　100208410
弁理士　岩瀬　寛司

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理方法およびプログラム

(57)【要約】
【課題】特定の情報に対する秘匿性を担保することができる情報処理装置、情報処理方法およびプログラムを提供する。
【解決手段】情報処理装置は、ネットワーク内に構築されるブロックチェーンで連結されるブロックに、生成されたデータを共通鍵で暗号化して格納する。また、予め記憶している第１公開鍵とは異なる第２公開鍵を、ブロックチェーンで連結されたブロックから取得する。そして、第２公開鍵で共通鍵を暗号化し、暗号化した共通鍵をブロックチェーンで連結されるブロックに格納する。
【選択図】図６



【特許請求の範囲】
【請求項１】
ネットワーク内に構築されるブロックチェーンで連結されるブロックに、生成されたデータを共通鍵で暗号化して格納するデータ格納手段と、
予め記憶している第１公開鍵とは異なる第２公開鍵を、前記ブロックチェーンで連結されたブロックから取得する公開鍵取得手段と、
前記公開鍵取得手段で取得した前記第２公開鍵で前記共通鍵を暗号化し、前記暗号化した前記共通鍵を前記ブロックチェーンで連結されるブロックに格納する共通鍵格納手段と、
を備えることを特徴とする情報処理装置。
【請求項２】
ネットワーク内に構築されるブロックチェーンで連結されたブロックから、共通鍵で暗号化されたデータを取得するデータ取得手段と、
前記共通鍵を記憶していない場合、前記ブロックチェーンで連結されたブロックから、予め記憶している公開鍵で暗号化された前記共通鍵を取得する暗号化共通鍵取得手段と、
前記暗号化共通鍵取得手段で取得した前記共通鍵を、前記公開鍵に対応する秘密鍵で復号化する共通鍵復号化手段と、
前記データ取得手段で取得した前記データを、前記共通鍵で復号化するデータ復号化手段と、
前記データ復号化手段により復号化したデータを表示する表示手段と、
を備えることを特徴とする情報処理装置。
【請求項３】
前記共通鍵格納手段は、前記第１公開鍵で前記共通鍵を暗号化し、前記暗号化した前記共通鍵を前記ブロックチェーンで連結されるブロックに格納する、
ことを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記共通鍵とは異なる新たな共通鍵を生成する共通鍵生成手段をさらに備え、
前記共通鍵格納手段は、前記第１公開鍵で前記新たな共通鍵を暗号化し、前記暗号化した前記新たな共通鍵を前記ブロックチェーンで連結されるブロックに格納し、
前記データ格納手段は、前記ブロックチェーンで連結されるブロックに、生成されたデータを前記新たな共通鍵で暗号化して格納する、
ことを特徴とする請求項１または３に記載の情報処理装置。
【請求項５】
情報処理装置における情報処理方法であって、
ネットワーク内に構築されるブロックチェーンで連結されるブロックに、生成されたデータを共通鍵で暗号化して格納するデータ格納ステップと、
予め記憶している第１公開鍵とは異なる第２公開鍵を、前記ブロックチェーンで連結されたブロックから取得する公開鍵取得ステップと、
前記公開鍵取得ステップで取得した前記第２公開鍵で前記共通鍵を暗号化し、前記暗号化した前記共通鍵を前記ブロックチェーンで連結されるブロックに格納する共通鍵格納ステップと、
を備えることを特徴とする情報処理方法。
【請求項６】
コンピュータを、
ネットワーク内に構築されるブロックチェーンで連結されるブロックに、生成されたデータを共通鍵で暗号化して格納するデータ格納手段、
予め記憶している第１公開鍵とは異なる第２公開鍵を、前記ブロックチェーンで連結されたブロックから取得する公開鍵取得手段、
前記公開鍵取得手段で取得した前記第２公開鍵で前記共通鍵を暗号化し、前記暗号化した前記共通鍵を前記ブロックチェーンで連結されるブロックに格納する共通鍵格納手段、

として機能させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報処理方法およびプログラムに関する。
【背景技術】
【０００２】
近年、ビットコイン（登録商標）等の仮想通貨を用いた商取引が行われている。当該仮想通貨を用いた商取引では、中央集権的な管理を必要とせずに不正を防止するため、ブロックチェーンと呼ばれる技術が用いられている。ブロックチェーンでは、複数のトランザクション、直前のハッシュ値及びその他の情報を「ブロック」として定義し、参加者全体で形成されるネットワーク内での合意形成のプロセスによって当該「ブロック」内の情報の信頼性を担保している。
【０００３】
例えば特許文献１には、このようなブロックチェーン技術により仮想通貨を用いた商取引を実現する技術が開示されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１６－２１８６３３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ここで、ブロックチェーンは参加者全ての取引の内容を示すものであるから、ビットコイン（登録商標）等の仮想通貨の取引に限られず、様々な取引に応用することが考えられる。例えば、複数者間で契約書を交わす際の証跡としてブロックチェーンを用いる方法が考えられる。しかしながら、契約といった性質上、当該契約書の内容を特定の参加者にのみ参照可能とし、他の者には秘匿しておきたいといった問題が生じる。このような場合に、特許文献１に記載の技術をそのまま適用しただけでは、当該問題を解決することはできず、特定の情報に対する秘匿性を担保するといった面からすると未だ十分ではなかった。
【０００６】
本発明は、上述のような事情に鑑みてなされたものであり、特定の情報に対する秘匿性を担保することができる情報処理装置、情報処理方法およびプログラムを提供することを目的としている。
【課題を解決するための手段】
【０００７】
上記目的を達成するため、本発明の第１の観点に係る情報処理装置は、
ネットワーク内に構築されるブロックチェーンで連結されるブロックに、生成されたデータを共通鍵で暗号化して格納するデータ格納手段（例えばステップＳ２０７およびステップＳ２０８の処理を実行する暗号化復号化部１２４およびデータ登録部１２１）と、
予め記憶している第１公開鍵とは異なる第２公開鍵を、前記ブロックチェーンで連結されたブロックから取得する公開鍵取得手段（例えばステップＳ２０４の処理を実行する他公開鍵取得部１２６）と、
前記公開鍵取得手段で取得した前記第２公開鍵で前記共通鍵を暗号化し、前記暗号化した前記共通鍵を前記ブロックチェーンで連結されるブロックに格納する共通鍵格納手段（例えばステップＳ２０５およびステップＳ２０６の処理を実行する暗号化復号化部１２４およびデータ登録部１２１）と、
を備えることを特徴とする。
【０００８】
上記目的を達成するため、本発明の第２の観点に係る情報処理装置は、

ネットワーク内に構築されるブロックチェーンで連結されたブロックから、共通鍵で暗号化されたデータを取得するデータ取得手段（例えばステップＳ３０１の処理を実行するブロック統合部１２５）と、
前記共通鍵を記憶していない場合、前記ブロックチェーンで連結されたブロックから、予め記憶している公開鍵で暗号化された前記共通鍵を取得する暗号化共通鍵取得手段（例えばステップＳ３０１の処理を実行するブロック統合部１２５）と、
前記暗号化共通鍵取得手段で取得した前記共通鍵を、前記公開鍵に対応する秘密鍵で復号化する共通鍵復号化手段（例えばステップＳ３０５の処理を実行する暗号化復号化部１２４）と、
前記データ取得手段で取得した前記データを、前記共通鍵で復号化するデータ復号化手段（例えばステップＳ３０６の処理を実行する暗号化復号化部１２４）と、
前記データ復号化手段により復号化したデータを表示する表示手段（例えばステップＳ３０７の処理を実行するブロック統合部１２５）と、
を備えることを特徴とする。
【０００９】
前記共通鍵格納手段は、前記第１公開鍵で前記共通鍵を暗号化し、前記暗号化した前記共通鍵を前記ブロックチェーンで連結されるブロックに格納する（例えばステップＳ１０３およびステップＳ１０４の処理を実行する暗号化復号化部１２４およびデータ登録部１２１）、
ようにしてもよい。
【００１０】
前記共通鍵とは異なる新たな共通鍵を生成する共通鍵生成手段（例えばステップＳ１０２の処理により、第１共通鍵１１３とは異なる新たな共通鍵を生成する共通鍵生成部１２３）をさらに備え、
前記共通鍵格納手段は、前記第１公開鍵で前記新たな共通鍵を暗号化し、前記暗号化した前記新たな共通鍵を前記ブロックチェーンで連結されるブロックに格納し（例えばステップＳ１０３およびステップＳ１０４の処理を実行する暗号化復号化部１２４およびデータ登録部１２１）、
前記データ格納手段は、前記ブロックチェーンで連結されるブロックに、生成されたデータを前記新たな共通鍵で暗号化して格納する（例えばステップＳ２０７およびステップＳ２０８の処理を実行する暗号化復号化部１２４およびデータ登録部１２１）、
ようにしてもよい。
【００１１】
上記目的を達成するため、本発明の第３の観点に係る情報処理方法は、
情報処理装置における情報処理方法であって、
ネットワーク内に構築されるブロックチェーンで連結されるブロックに、生成されたデータを共通鍵で暗号化して格納するデータ格納ステップ（例えばステップＳ２０７およびステップＳ２０８の処理を実行するステップ）と、
予め記憶している第１公開鍵とは異なる第２公開鍵を、前記ブロックチェーンで連結されたブロックから取得する公開鍵取得ステップ（例えばステップＳ２０４の処理を実行するステップ）と、
前記公開鍵取得ステップで取得した前記第２公開鍵で前記共通鍵を暗号化し、前記暗号化した前記共通鍵を前記ブロックチェーンで連結されるブロックに格納する共通鍵格納ステップ（例えばステップＳ２０５およびステップＳ２０６の処理を実行するステップ）と、
を備えることを特徴とする。
【００１２】
上記目的を達成するため、本発明の第４の観点に係るプログラムは、
コンピュータを、
ネットワーク内に構築されるブロックチェーンで連結されるブロックに、生成されたデ

ータを共通鍵で暗号化して格納するデータ格納手段（例えばステップＳ２０７およびステップＳ２０８の処理を実行する暗号化復号化部１２４およびデータ登録部１２１）、
予め記憶している第１公開鍵とは異なる第２公開鍵を、前記ブロックチェーンで連結されたブロックから取得する公開鍵取得手段（例えばステップＳ２０４の処理を実行する他公開鍵取得部１２６）、
前記公開鍵取得手段で取得した前記第２公開鍵で前記共通鍵を暗号化し、前記暗号化した前記共通鍵を前記ブロックチェーンで連結されるブロックに格納する共通鍵格納手段（例えばステップＳ２０５およびステップＳ２０６の処理を実行する暗号化復号化部１２４およびデータ登録部１２１）、
として機能させることを特徴とする。

【発明の効果】
【００１３】
本発明によれば、特定の情報に対する秘匿性を担保することができる。

【図面の簡単な説明】
【００１４】
【図１】本発明の実施形態に係る情報処理システムの一例を示すブロック図である。
【図２】本発明の実施形態に係る情報処理装置の一例を示すブロック図である。
【図３】作成する契約書の一例を示す図である。
【図４】事前登録処理の一例を示すフローチャートである。
【図５】事前登録処理にて登録される具体的内容の一例を示す図である。
【図６】ブロック登録処理の一例を示すフローチャートである。
【図７】参照処理の一例を示すフローチャートである。
【図８】パターン１におけるブロック登録処理の具体的な登録内容の一例を示す図である。
【図９】ブロックチェーンの内容が図８に示す状態である場合の具体的な参照内容の例を示す図である。
【図１０】パターン２におけるブロック登録処理の具体的な登録内容の一例を示す図である。
【図１１】ブロックチェーンの内容が図１０に示す状態である場合の具体的な参照内容の例を示す図である。
【図１２】パターン３におけるブロック登録処理の具体的な登録内容の一例を示す図である。
【図１３】ブロックチェーンの内容が図１２に示す状態である場合の具体的な参照内容の例を示す図である。
【図１４】変形例におけるブロックチェーンの具体的内容を示す図である。
【図１５】変形例における情報処理システムの一例を示すブロック図である。

【発明を実施するための形態】
【００１５】
まず、図１に示す情報処理システム１を例に、ブロックチェーンの概要について説明する。情報処理システム１では、図１に示すように、情報処理装置１００Ａ～１００Ｃ（情報処理装置１００Ａ～１００Ｃを単に情報処理装置１００ともいう）のそれぞれがネットワーク２１０を介して通信可能に接続されている。
【００１６】
情報処理装置１００は、携帯電話やスマートフォン、タブレットやＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）等の情報端末であり、Ｐ２Ｐ（Ｐｅｅｒ　ｔｏ　Ｐｅｅｒ）等の分散型のネットワーク２１０を構築している。なお、情報処理システム１は、Ｐ２Ｐ型のシステムに限られず、例えばクラウドコンピューティング型であってもよい。
【００１７】
情報処理装置１００は、ユーザによる操作により契約に関するデータなどを生成し、ネットワーク２１０へ配信する機能を有するトランザクション生成装置として機能する。ま

た、情報処理装置１００は、トランザクション生成装置により配信されたトランザクションの正当性を検証し、新たなブロックを生成して既存のブロックチェーンを連結するブロックチェーン生成装置としても機能する。ブロックチェーン生成装置が検証した結果は、ネットワーク２１０を介して、各情報処理装置１００で共有される。なお、図示する例では、理解を容易にするために、トランザクション生成装置の機能とブロックチェーン生成装置の機能とを当該情報処理装置１００が併せ持つ例を示しているが、それぞれ別の端末が備え持っていてもよい。また、通常、一定数のトランザクションにて扱われるデータが一つのブロックに格納される（ブロックチェーン生成装置は、一定数のトランザクションをひとまとめにして当該トランザクションにて扱われる複数のデータを一つのブロックに格納する）が、この実施の形態では、理解を容易にするため、一つのトランザクションによって扱われるデータが一つのブロックに格納されるものとする。

【００１８】

この実施の形態において、トランザクション生成装置としての機能により生成されたトランザクションにて扱われる契約に関するデータ（単にデータという）は、ブロックと呼ばれる一つの単位に格納され、当該ブロックを時系列に連結したブロックチェーンによって管理される。具体的に、データは、ブロックチェーン生成装置としての機能により新たに生成されたブロックに格納された後、既存のブロックチェーンに連結され、各情報処理装置１００で共有される。例えば、ブロックチェーンに含まれていないトランザクションが配信されると、ブロックチェーン生成装置の機能により、当該トランザクションについての検証を行い、新たなブロック（第ｎのブロック）を生成する。そして、当該データに、現在のブロックチェーンの末尾のブロック（第ｎ－１のブロック）のハッシュ値（２５６ビット）を含めて新たなブロック（第ｎのブロック）に格納する。これにより、データがブロックに格納され、ブロックチェーンにより時系列に管理されることとなる。すなわち、ブロックチェーンは、契約に関するデータ（契約内容）を記録した台帳としての役割を有している。なお、以下では、ユーザＡ、ユーザＢ、ユーザＣの三者にて行われる契約を例に説明する。

【００１９】

次に、図２を参照し、この実施の形態における情報処理装置１００の構成について説明する。なお、図示する例では、ユーザＡの端末である情報処理装置１００Ａを例としているが、ユーザＢの端末である情報処理装置１００ＢおよびユーザＣの端末である情報処理装置１００Ｃについても同様であるため、説明は省略する。

【００２０】

図２に示すように、情報処理装置１００Ａ（以下、情報処理装置１００）は、記憶部１１０と、制御部１２０と、入出力部１３０と、通信部１４０と、これらを相互に接続するシステムバス（図示省略）と、を備えている。

【００２１】

記憶部１１０は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ)やＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等を備える。ＲＯＭは制御部１２０のＣＰＵが実行するプログラム及び、プログラムを実行する上で予め必要なデータを記憶する。具体的に、この実施の形態では、当該情報処理装置１００を、トランザクション生成装置として機能させるためのプログラム、ブロックチェーン生成装置として機能させるためのプログラム、各種鍵を生成するプログラム等が、予めインストールされている。ＲＡＭは、プログラム実行中に作成されたり変更されたりするデータを記憶する。記憶部１１０は、制御部１２０が実行するプログラムが用いる主要な情報として、ユーザＡの秘密鍵１１１、ユーザＡの公開鍵１１２、第１共通鍵１１３、ブロック統合データ１１４、他ユーザの公開鍵１１５、を記憶する。

【００２２】

ユーザＡの秘密鍵１１１、ユーザＡの公開鍵１１２は、後述するペア鍵生成部１２２により生成される、暗号化および復号化に用いられる鍵である。ユーザＡの公開鍵１１２にて暗号化されたデータは、ユーザＡの秘密鍵１１１でのみ復号可能である。なお、図示す

る例では、ユーザＡの公開鍵１１２およびユーザＡの秘密鍵１１１が記憶されているが、当該公開鍵１１２および秘密鍵１１１は、ペア鍵生成部１２２によりユーザ毎に生成され記憶される。

【００２３】

第１共通鍵１１３は、後述する共通鍵生成部１２３により生成される鍵であり、暗号化および復号化の両方で共通して用いられる鍵である。図示する例では、第１共通鍵１１３が記憶されている例を示しているが、共通鍵は記憶されていなくてもよく、また、第１共通鍵１１３とは異なる新たな共通鍵が生成され記憶されてもよい（詳しくは後述する）。ブロック統合データ１１４は、後述するブロック統合部１２５にて統合された各ブロックの内容を示すデータである。他ユーザの公開鍵１１５は、後述する他公開鍵取得部１２６により取得される他のユーザの公開鍵である。

【００２４】

ブロック情報ＤＢ１１６は、生成されたブロックに関する情報が格納されるデータベースである。

【００２５】

制御部１２０は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）やＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）等から構成される。制御部１２０は、記憶部１１０に記憶されたプログラムに従って動作し、当該プログラムに従った処理を実行する。制御部１２０は、記憶部１１０に記憶されたプログラムにより提供される主要な機能部として、データ登録部１２１と、ペア鍵生成部１２２と、共通鍵生成部１２３と、暗号化復号化部１２４と、ブロック統合部１２５と、他公開鍵取得部１２６と、を備える。

【００２６】

データ登録部１２１は、上述したトランザクション生成装置としての機能およびブロックチェーン生成装置としての機能を実現する機能部である。データ登録部１２１は、ユーザの入出力部１３０に対する操作の基づいて新たなトランザクションを生成する機能（トランザクション生成装置の機能）、当該新たなトランザクションが正当なものであることを検証する機能、および新たなブロックを生成して検証済みのトランザクションにて扱われるデータを格納してブロックチェーンを生成する機能（ブロックチェーン生成装置の機能）、を有する。すなわち、データ登録部１２１は、ブロックチェーンのデータ登録に関する一般的な機能を有している。なお、上述したように、この実施の形態では、理解を容易にするため、当該情報処理装置１００（ユーザＡの端末）がデータ登録部１２１としてトランザクション生成装置としての機能およびブロックチェーン生成装置としての機能を有するものとして説明しているが、例えば、ユーザＡの端末におけるデータ登録部１２１がトランザクション生成装置としての機能を有し、ユーザＢの端末におけるデータ登録部１２１がブロックチェーン生成装置としての機能を有していてもよい。すなわち、データ登録部１２１は必ずしも両方の機能を有していなくてもよく、条件（状況）に応じて異なる機能を有していてもよい。

【００２７】

ペア鍵生成部１２２は、当該ユーザの公開鍵および秘密鍵を生成する機能を有する。具体的にペア鍵生成部１２２は、記憶部１１０に記憶されたペア鍵生成プログラムに従って、当該ユーザの公開鍵および秘密鍵を生成する（図２に示す例では、ユーザＡの公開鍵１１２およびユーザＡの秘密鍵１１１を生成する）。なお、この実施の形態では、予めユーザ毎の公開鍵および秘密鍵が、当該ペア鍵生成部１２２により生成され記憶部１１０に記憶されている。

【００２８】

共通鍵生成部１２３は、記憶部１１０に記憶された共通鍵生成プログラムに従って、共通鍵を生成する機能を有する（図２に示す例では、第１共通鍵１１３を生成する）。なお、この実施の形態では、共通鍵生成プログラムにより共通鍵を生成する例を示しているが、共通鍵については、ネットワーク２１０を介して外部から取得してもよい。

【００２９】
暗号化復号化部１２４は、各種暗号化および復号化を行う機能を有する。詳しくは後述するが、この実施の形態における暗号化復号化部１２４は、共通鍵を自己または他者の公開鍵により暗号化する機能、データを共通鍵により暗号化する機能、暗号化された共通鍵を自己の秘密鍵により復号化する機能、暗号化されたデータを共通鍵により復号化する機能、を有する。
【００３０】
ブロック統合部１２５は、ブロックチェーンとして連結されている各ブロックの内容（各データ）を統合してブロック統合データ１１４を生成する機能を有している。
【００３１】
他公開鍵取得部１２６は、他のユーザの公開鍵を取得する機能を有する。他公開鍵取得部１２６は、他のユーザの端末にて生成されブロックチェーンに登録された公開鍵を取得する。
【００３２】
入出力部１３０は、キーボード、マウス、カメラ、マイク、液晶ディスプレイ、有機ＥＬ（Ｅｌｅｃｔｏｒｏ－Ｌｕｍｉｎｅｓｃｅｎｃｅ）ディスプレイ等から構成され、データの入出力を行うための装置である。
【００３３】
通信部１４０は、他の情報処理装置１００とネットワーク２１０を介して通信を行うためのデバイスである。
【００３４】
以上が、情報処理装置１００の構成である。続いて情報処理装置１００の動作について、図３～図７を参照して説明する。なお、この実施の形態では、図３に示す「書類Ａ」をユーザＡ、ユーザＢ、ユーザＣ間の契約書として作成する場合を例に説明する。また、この実施の形態では、書類の種類（書類名）によって一意に識別可能なグループ情報が予め定められており、グループ毎にブロックチェーンが生成される（図示する例では、書類Ａがグループ Ａのグループ情報に相当し、書類Ａのブロックチェーンが生成されることとなる）。なお、図３に示す項目１～３の内容がそれぞれ一つのデータに相当するものである。また、この実施の形態では、理解を容易にするため、項目１～３のそれぞれの内容（すなわち、データ１～３）が、ブロック１～３にそれぞれ順に格納され、ブロックチェーンとして管理されるものとする（一つのトランザクションにて一つのデータが扱われ、当該一つのデータが一つのブロックに順次格納される）。
【００３５】
まず、ユーザによる操作に基づいて、図４に示す事前登録処理が行われる。事前登録処理は、ブロックチェーンとして図３に示すグループの書類のデータを、ブロックチェーンにより管理するための設定を行う処理である。なお、ユーザＡ、ユーザＢ、ユーザＣそれぞれの情報端末（情報処理装置１００）には、各ユーザの公開鍵１１２および秘密鍵１１１が予めペア鍵生成部１２２の機能により生成され、記憶部１１０に格納されているものとする。この実施の形態では、ユーザＡの操作により当該事前登録処理が実行されるものとする。事前登録処理を行うユーザは予め定められており、ユーザＡ以外のユーザにより行われてもよい。
【００３６】
図４に示す事前登録処理において、まず、情報処理装置１００は、データ登録部１２１の機能により、グループ情報を作成する（ステップＳ１０１）。具体的にステップＳ１０１の処理では、ブロックチェーンで管理するグループが「書類Ａ」（グループＡ）であり、当該グループには項目１～項目Ｎ（Ｎは整数で当該書類Ａの最終項目）が含まれることを、ブロック１を生成して定義する（登録する）。なお、ブロック１は、ブロックチェーンにおける先頭のブロックである。このように、ステップＳ１０１の処理が行われることにより、図５に示すように、ブロック１に、作成対象のグループ情報として、書類Ａを示すグループＡの内容が定義されることとなる。なお、ステップＳ１０１の処理では、予め

記憶部１１０に記憶された複数のグループ情報の中から作成対象のグループ情報をユーザが選択することにより行われてもよい。また、当該ステップＳ１０１の処理は、情報処理装置１００ではなく、当該情報処理装置１００にネットワークを介して接続された専用のサーバにて行われてもよい。そして、当該専用サーバでは、後述する参照可能者の管理が行われるとともに、当該専用サーバが、ペア鍵生成部１２２の機能および共通鍵生成部１２３の機能を有していてもよい。すなわち、専用サーバにて生成された公開鍵や秘密鍵が各ユーザの識別情報に対応付けて管理され、各ユーザに配布されてもよい。そして、共通鍵については、必要とされるユーザに当該専用サーバから配布されるようにしてもよい。

【００３７】

続いて、情報処理装置１００は、共通鍵生成部１２３の機能により、第１共通鍵１１３を生成し（ステップＳ１０２）、暗号化復号化部１２４の機能により、当該生成した第１共通鍵１１３をユーザＡの公開鍵１１２で暗号化する（ステップＳ１０３）。そして、データ登録部１２１の機能により、暗号化した第１共通鍵１１３Ａを当該ブロック１に登録し（ステップＳ１０４）、事前登録処理を終了する。なお、ステップＳ１０４の処理では、図５に示すように、ユーザＡの公開鍵１１２についても、第１共通鍵１１３Ａと同様にブロック１へ登録する。図４および図５に示す例では、ユーザＡの公開鍵１１２および第１共通鍵１１３Ａをブロックへ登録する例を示しているが、これは、ユーザＡが当該秘密鍵１１１さえ管理すれば、第１共通鍵１１３を管理しなくとも、ブロックから取得可能となるためであり、鍵の管理負担を軽減することができるためである。鍵の管理負担を考慮しない場合には、当該、ユーザＡの公開鍵１１２および第１共通鍵１１３Ａをブロックへ登録しなくてもよい。

【００３８】

なお、この実施の形態では、一般的なブロックチェーンの技術と同様に、ブロックへ登録される全てのトランザクションについて、ブロックチェーン生成装置の機能により定期的なタイミングにて内容の検証が行われる。そして、正当であると認定されると、当該トランザクションにて扱われたデータがブロックへ登録されるとともに、既存のブロックチェーンに連結され、ネットワーク２１０を介して各情報処理装置１００で共有されることとなる。以下、ブロックへの登録については同様であるため、当該事項については説明を省略する。

【００３９】

続いて、ユーザの操作により生成されたトランザクションにて扱われるデータ（生成されたデータ、または単にデータという）をブロックへ登録するブロック登録処理について説明する。当該ブロック登録処理は、ユーザによる操作（トランザクションを生成してデータを登録する旨の操作）により実行される。なお、この実施の形態では、上述したように、一つの項目（一つのデータ）につき一つのブロックが作成され登録されることから、当該ブロック登録処理は、登録すべき項目の数（トランザクションの数）、繰り返し実行されればよい。

【００４０】

図６は、当該ブロック登録処理の一例を示すフローチャートである。なお、ここでは、実行ユーザを指定せずに説明する。ブロック登録処理において、まず、情報処理装置１００は、データ登録部１２１の機能により、発生したトランザクションにて扱われるデータ（登録対象のデータ）が暗号化対象であるか否かを判定する（ステップＳ２０１）。なお、暗号化対象であるか否かは、事前登録処理にてグループ情報が登録（定義）される際に、後述する参照可能者とともに予め定められていればよく（暗号化対象の項目および参照可能者が予め定められている）、暗号化対象のデータであるか否かを示す情報が、参照可能者に関する情報とともに記憶部１１０に記憶されていればよい。

【００４１】

登録対象のデータが暗号化対象でない場合（ステップＳ２０１；Ｎｏ）、情報処理装置１００は、データ登録部１２１の機能により、当該データを対象のブロックへ登録し（ステップＳ２０２）、ブロック登録処理を終了する。

【００４２】
一方、登録対象のデータが暗号化対象である場合（ステップＳ２０１；Ｙｅｓ）、当該データを参照可能なユーザ（参照可能者）の公開鍵を所有しているか否かを判定する（ステップＳ２０３）。上述したように、参照可能者に関する情報は、事前登録処理にてグループ情報が登録（定義）される際に予め定められ記憶部１１０に記憶されているため、ステップＳ２０３の処理では、記憶部１１０に記憶された情報に基づいて参照可能者を特定し、当該特定した参照可能者全員の公開鍵を所有しているか否かを判定すればよい。なお、公開鍵にはユーザを識別する識別情報が付加されていればよく、当該識別情報によりいずれのユーザの公開鍵であるかを判定すればよい。

【００４３】
参照可能者の公開鍵を所有していないと判定した場合（ステップＳ２０３；Ｎｏ）、情報処理装置１００は、他公開鍵取得部１２６の機能により、参照可能者の公開鍵を取得する（ステップＳ２０４）。詳しくは後述するが、ステップＳ２０４の処理では、ブロックに登録された参照可能者の公開鍵を取得する。ステップＳ２０４の処理を実行した後、情報処理装置１００は、暗号化復号化部１２４の機能により、取得した公開鍵で共通鍵（当該共通鍵は図４のステップＳ１０２の処理にて生成されている）を暗号化し（ステップＳ２０５）、ブロックに登録する（ステップＳ２０６）。当該ステップＳ２０６の処理が行われることにより、参照可能者が、ステップＳ２０５の処理にて暗号化された共通鍵を取得可能となる。そして、参照可能者は、当該取得した暗号化された共通鍵を、自己の所有する秘密鍵で復号化すればよい（後述するステップＳ３０５）。なお、当該ステップＳ２０４～ステップＳ２０６の処理は、後述するステップＳ２０８の処理の後に行ってもよい。

【００４４】
ステップＳ２０６の処理を実行した後、またはステップＳ２０３にて参照可能者の公開鍵を所有していると判定した場合（ステップＳ２０３；Ｙｅｓ）、情報処理装置１００は、暗号化復号化部１２４の機能により、所有する共通鍵にてデータを暗号化する（ステップＳ２０７）。そして、暗号化したデータを対象のブロックへ登録し（ステップＳ２０８）、ブロック登録処理を終了する。当該ブロック登録処理が行われることで、登録対象のデータ（発生したトランザクションにて扱われるデータ）がブロックチェーンにより管理されることとなる。

【００４５】
次に、図６のブロック登録処理によりブロックチェーンに連結されたブロックの内容を参照する場合の参照処理について、図７を参照して説明する。当該参照処理は、ユーザによる操作により実行される。より具体的には、参照したいグループを指定する操作が行われることにより実行される。なお、当該参照処理は、ユーザ毎に実行可能である。

【００４６】
参照処理が開始されると、情報処理装置１００は、ブロック統合部１２５の機能により、当該指定されたグループに対応するブロックチェーンで連結されたブロックの内容（各データおよび鍵情報）を全て取得する（ステップＳ３０１）。そして、当該取得したブロックの内容に、暗号化されたデータが含まれているか否かを判定する（ステップＳ３０２）。暗号化されているデータが含まれている場合（ステップＳ３０２；Ｙｅｓ）、対応する共通鍵を所有しているか否かを判定する（ステップＳ３０３）。この実施の形態では、データの暗号化が行われる場合には、図６のステップＳ２０７の処理により共通鍵にて暗号化されるため、ステップＳ３０３の処理では、復号化可能な共通鍵を所有しているか否かの判定を行う。

【００４７】
対応する共通鍵を所有していないと判定した場合（ステップＳ３０３；Ｎｏ）、情報処理装置１００は、ブロック統合部１２５の機能により、取得した内容に暗号化された共通鍵が含まれているか否かを判定する（ステップＳ３０４）。具体的に、ステップＳ３０４の処理では、当該暗号化された共通鍵が自己の所有する秘密鍵で復号化可能であるか否か

を判定する。自己の所有する秘密鍵にて当該暗号化された共通鍵が復号化可能である場合（ステップＳ３０４；Ｙｅｓ）、情報処理装置１００は、暗号化復号化部１２４の機能により、当該暗号化された共通鍵を、自己の秘密鍵で復号化する（ステップＳ３０５）。

【００４８】

ステップＳ３０５の処理を実行した後、またはステップＳ３０３の処理にて対応する共通鍵を所有していると判定した場合（ステップＳ３０３；Ｙｅｓ）、情報処理装置１００は、暗号化復号化部１２４の機能により、当該暗号化されたデータを、共通鍵にて復号化する（ステップＳ３０６）。ステップＳ３０６の処理を実行した後、情報処理装置１００は、ブロック統合部１２５の機能により、当該復号化したデータを出力し（ステップＳ３０７）、参照処理を終了する。

【００４９】

一方、ステップＳ３０４にて、暗号化された共通鍵が自己の所有する秘密鍵では復号化不可能であると判定した場合（ステップＳ３０４；Ｎｏ）、暗号化されたデータを、暗号化された状態のまま出力し（ステップＳ３０７）、参照処理を終了する。また、ステップＳ３０２にて暗号化されたデータが含まれていないと判定した場合（ステップＳ３０２；Ｎｏ）、情報処理装置１００は、ブロック統合部１２５の機能により、当該データを出力して（ステップＳ３０７）参照処理を終了する。

【００５０】

以上が、情報処理装置１００の動作である。続いて、より具体的な動作について、パターン１～パターン３に分けて説明する。

【００５１】

まず、図３に示す「書類Ａ」のグループにおける項目３に相当するデータが、ユーザＡにのみ参照可能である場合（パターン１）について説明する。図８は、パターン１におけるブロック登録処理の具体的な登録内容の一例を示す図である。なお、以下では、ユーザＡにより図４に示す事前登録処理が行われていることを前提に説明する（すなわち、図８に示すように、ユーザＡの公開鍵およびユーザＡの公開鍵で暗号化した第１共通鍵がブロック１に登録されていることを前提に説明する）。また、ユーザＡによりブロック登録処理が行われ、項目１～項目３に相当するデータが対象のブロックへ登録されるものとする（パターン２についても同様）。

【００５２】

ユーザＡはまず、図６に示すブロック登録処理を開始すると、項目１に相当するデータが暗号化対象ではないため、図６のステップＳ２０１にてＮｏと判定され、ステップＳ２０２の処理にて項目１の内容がブロック１に登録される（図８のブロック１参照）。項目２についても項目１と同様に、ステップＳ２０２の処理にて項目２の内容がブロック２に登録される（図８のブロック２参照）。

【００５３】

一方、項目３に相当するデータについては暗号化対象であるため、図６のステップＳ２０１にてＹｅｓと判定され、ステップＳ２０３の処理に移行する。ステップＳ２０３では、参照可能者がユーザＡ本人であることから、参照可能者の公開鍵を所有していると判定される（Ｙｅｓと判定される）。そして、ステップＳ２０７により第１共通鍵１１３にて当該項目３に相当するデータが暗号化され（図８に示すように、９９９９９９９９をＭｚＹＷｄＵ０Ｍとするなど）、ステップＳ２０８にて当該暗号化したデータが、ブロック３に登録される。

【００５４】

以上がパターン１におけるブロック登録処理の具体的な登録内容である。なお、いずれのユーザについても参照可能なデータのみを登録する場合については、図８に示すブロック１およびブロック２への登録と同様である。続いて、当該パターン１における参照処理の具体的な参照内容について説明する。図９は、ブロックチェーンの内容が図８に示す状態である場合の具体的な参照内容の例を示している。

【００５５】

まず、ユーザＡが図７に示す参照処理を行った場合について説明する。参照処理を開始すると、ステップＳ３０１の処理により、図８に示すブロック１～ブロック３の内容が取得される。そのうち、項目３に相当するデータが暗号化されていることから、ステップＳ３０２にてＹｅｓと判定され、ステップＳ３０３の処理に移行する。ステップＳ３０３の処理では、当該暗号化されたデータに対応する第１共通鍵１１３を所有しているため、Ｙｅｓと判定され、ステップＳ３０６の処理に移行する。そして、ステップＳ３０６の処理にて項目３に相当するデータが第１共通鍵１１３により復号化される。続けてステップＳ３０７の処理が実行されることで、図９（Ａ）に示すように、項目３に相当するデータが、復号化された状態で表示される（項目１および２は暗号化されていないためそのまま表示される）。

【００５６】

これに対し、ユーザＢまたはユーザＣが図７に示す参照処理を行った場合、ユーザＡの場合と同様に、ステップＳ３０１の処理により、図８に示すブロック１～ブロック３の内容が取得され、図７のステップＳ３０２にてＹｅｓと判定されるものの、ユーザＢおよびユーザＣは第１共通鍵１１３を所有していないため、ステップＳ３０３の処理にてＮｏと判定される。そして、ステップＳ３０４の処理に移行するが、取得したブロック１～３の内容には、暗号化された共通鍵が含まれていないため、ステップＳ３０４にてＮｏと判定される。そして、ステップＳ３０７の処理が実行され、図９（Ｂ）に示すように、項目３に相当するデータが暗号化された状態のまま表示される（項目１および２は暗号化されていないためそのまま表示される）。

【００５７】

このように、ユーザＡにて項目３に相当するデータを、第１共通鍵１１３にて暗号化してブロックへ登録することにより、項目３に相当するデータをユーザＡにのみ参照可能とすることができる。したがって、特定の情報に対する秘匿性を担保することができる。また、生成した第１共通鍵１１３をユーザＡの公開鍵１１２にて暗号化してブロックへ登録することで、ユーザＡは第１共通鍵１１３を所有せずとも、当該ブロックから取得可能となる。したがって、ユーザＡは秘密鍵１１１を管理すればよく、第１共通鍵１１３の管理負担を軽減することができる。

【００５８】

次に、図３に示す「書類Ａ」のグループにおける項目３に相当するデータが、ユーザＡおよびユーザＢにのみ参照可能である場合（パターン２）について説明する。図１０は、パターン２におけるブロック登録処理の具体的な登録内容の一例を示す図である。なお、パターン１と同様の部分については説明を省略する。なお、図１０にて図示を省略したブロック１にも、パターン１と同様（図８のブロック１と同様）に、ユーザＡの公開鍵で暗号化された第１共通鍵が登録されているものとする。

【００５９】

ユーザＡは、図６に示すブロック登録処理を開始すると、項目１に相当するデータおよび項目２に相当するデータを、パターン１と同様に各ブロックへ登録する（図１０のブロック２参照）。そして、項目３に相当するデータについては暗号化対象であるため、図６のステップＳ２０１にてＹｅｓと判定され、ステップＳ２０３に移行する。

【００６０】

ステップＳ２０３では、参照可能者であるユーザＢの公開鍵を所有していないため、Ｎｏと判定されることとなる。そして、ユーザＡは、ステップＳ２０４の処理により、参照可能者であるユーザＢの公開鍵を取得する。なお、図１０に示すように、ユーザＢの公開鍵は、予めブロック（図示する例ではブロック３）に登録されている。例えば、ユーザＡによりブロック２が登録され各ユーザ間で共有されたことに基づいて、ユーザＢの操作により当該ユーザＢの公開鍵が対象のブロックへ登録されればよい。また、ユーザＡによりユーザＢに対して公開鍵を対象ブロックへ登録する指示を送信し、当該指示に基づいてユーザＢが公開鍵を登録してもよい。図６に示すステップＳ２０４の処理では、このようにユーザＢにより登録されたユーザＢの公開鍵を取得する。

【００６１】
ステップＳ２０４の処理に続いて、ユーザＡは、ステップＳ２０５の処理により、取得したユーザＢの公開鍵で第１共通鍵１１３が暗号化され、ステップＳ２０６の処理により、当該暗号化した第１共通鍵１１３が、図１０に示すように、ブロック４へ登録される。その後、上記パターン１と同様に、項目３に相当するデータが、第１共通鍵で暗号化され、ブロック５へ登録される（図６のステップＳ２０７、Ｓ２０８、図１０のブロック５参照）。
【００６２】
以上がパターン２におけるブロック登録処理の具体的な登録内容である。続いて、当該パターン２における参照処理の具体的な参照内容について説明する。図１１は、ブロックチェーンの内容が図１０に示す状態である場合の具体的な参照内容の例を示している。なお、参照可能者であるユーザＡが参照処理を行った場合についてはパターン１で説明した処理（パターン１の第１共通鍵１１３を所有している場合の処理）と同様の処理により（図７のステップＳ３０３にてＹｅｓと判定され、ステップＳ３０６の処理にて復号化されることにより）、図１１（Ａ）に示すように、項目３に相当するデータが復号化された状態で表示される。また、参照可能者ではないユーザＣが参照処理を行った場合についても、パターン１で説明した処理（パターン１の第１共通鍵１１３を所有していない場合の処理）と同様の処理により（図７のステップＳ３０４にてＮｏと判定され）、図１１（Ｂ）に示すように、項目３に相当するデータが暗号化された状態で表示される。したがって、ここでは、ユーザＢにより参照処理が行われた場合を例に説明する。
【００６３】
ユーザＢが参照処理を開始すると、ステップＳ３０１の処理により、図１０に示すブロック１～ブロック５の内容が取得される（なお、図１０に示す例ではブロック１を省略している）。そのうち、項目３に相当するデータが暗号化されていることから、ステップＳ３０２にてＹｅｓと判定され、ステップＳ３０３の処理に移行する。ステップＳ３０３の処理では、当該暗号化されたデータに対応する第１共通鍵１１３を所有していないため、Ｎｏと判定され、ステップ３０４の処理に移行する。ここで、図１０に示すブロック４にユーザＢの公開鍵で暗号化された第１共通鍵１１３が登録されており、当該ブロックの内容は、図７のステップＳ３０１の処理にて取得されているため、当該ステップＳ３０４の処理では、自己の所有する秘密鍵（ユーザＢの所有する秘密鍵）で当該第１共通鍵１１３を復号化可能であると判定される（すなわち、Ｙｅｓ）と判定される。
【００６４】
続いてステップＳ３０５の処理により、ユーザＢの秘密鍵で、当該暗号化された第１共通鍵１１３が復号化され、ユーザＢは第１共通鍵１１３を取得することとなる。そして、ステップＳ３０６の処理にて、項目３に相当するデータが第１共通鍵１１３により復号化され、続けてステップＳ３０７の処理が実行されることで、図１１（Ａ）に示すように、項目３に相当するデータが、復号化された状態で表示される（項目１および２は暗号化されていないためそのまま表示される）。
【００６５】
このように、ユーザＢの公開鍵をユーザＡが取得し、第１共通鍵１１３を取得したユーザＢの公開鍵にて暗号化してブロックへ登録することにより、項目３に相当するデータを、ユーザＡおよびユーザＢが参照可能とすることができる。したがって、参照可能者以外のユーザに対し、特定の情報に対する秘匿性を適切に担保することができる。
【００６６】
次に、図３に示す「書類Ａ」のグループにおける項目３にデータが、ユーザＢにのみ参照可能である場合（パターン３）について説明する。なお、パターン３は、パターン１およびパターン２とは異なり、参照可能者がユーザＢのみであるため、当該項目３に相当するデータについては、項目１および項目２とは異なり（項目１および項目２はユーザＡが登録）、ユーザＢが対象のブロックへ登録する。図１２は、パターン３におけるブロック登録処理の具体的な登録内容の一例を示す図である。なお、パターン１と同様の部分につ

いては説明を省略する。なお、図１２にて図示を省略したブロック１にも、パターン１と同様（図８のブロック１と同様）に、ユーザＡの公開鍵で暗号化された第１共通鍵が登録されているものとする。

【００６７】

ユーザＡは、図６に示すブロック登録処理を開始すると、項目１に相当するデータおよび項目２に相当するデータを、パターン１と同様に各ブロックへ登録する（図１２のブロック２参照）。続いて項目３に相当するデータを対象のブロックへ登録することとなるが、項目３に相当するデータは、ユーザＢにのみ参照可能であるため、ユーザＢにより登録されるべきデータである。なお、データの登録者については、事前登録処理にてグループ情報が登録（定義）される際に予め定められていればよい。

【００６８】

項目２に相当するデータが対象のブロック（この例ではブロック２）に登録され各ユーザ間で共有されると、ユーザＢはこのことに基づいて、図４のステップＳ１０２～ステップＳ１０４の処理を実行する。なお、ユーザＡによりユーザＢへ、項目３に相当するデータの登録を促す信号を送信してもよい。具体的に、ユーザＢの情報処理装置１００は、共通鍵生成部１２３の機能により、第１共通鍵１１３とは異なる新たな共通鍵として第２共通鍵を生成し（ステップＳ１０２）、暗号化復号化部１２４の機能により、当該生成した第２共通鍵をユーザＢの公開鍵１１２で暗号化する（ステップＳ１０３）。そして、データ登録部１２１の機能により、暗号化した第２共通鍵を対象のブロック（図１２に示す例ではブロック３）に登録する（ステップＳ１０４）。ここで、第２共通鍵は、第１共通鍵１１３とは異なる鍵であるため、当該第２共通鍵で暗号化した内容を復号化できるのは、当該第２共通鍵の所有者のみとなる。また、当該第２共通鍵は、ユーザＢの公開鍵により暗号化されているため、ユーザＢの秘密鍵でなければ復号化することができないこととなる。

【００６９】

暗号化した第２共通鍵を対象のブロックへ登録した後、ユーザＢは、パターン１と同様に、参照可能者がユーザＢ本人であることから、図６のステップＳ２０３にて参照可能者の公開鍵を所有していると判定され（Ｙｅｓと判定され）、ステップＳ２０７にて第２共通鍵にて当該項目３に相当するデータの内容が暗号化される（図１２に示すように、９９９９９９９をＸＩ０ｔａｇＢａｇとする）。そして、ステップＳ２０８にて当該暗号化した内容が、ブロック４に登録される（図１２のブロック４参照）。

【００７０】

以上がパターン３におけるブロック登録処理の具体的な登録内容である。なお、その後、ユーザＢのみでなくユーザＣも参照可能とする場合には、パターン２と同様に、ユーザＢがユーザＣの公開鍵を取得し、当該ユーザＣの公開鍵により第２共通鍵を暗号化して、対象のブロックに登録すればよい。また、パターン２において項目３に相当するデータを対象のブロックへ登録した後、例えば、ユーザＡにのみ参照可能な項目４に相当するデータを、対象のブロックへ登録するような場合においても、当該パターン３と同様に、登録者であるユーザＡが新たな共通鍵を生成し、当該生成した新たな共通鍵により項目４に相当するデータを暗号化してブロックへ登録すればよい。すなわち、登録対象のデータに対する参照可能者を追加する場合には、パターン２で説明したように、追加された参加者の公開鍵を取得し、取得した公開鍵にて共通鍵を暗号化してブロック登録を行う一方で、登録対象のデータに対する参照可能者を減少させる場合や、全く異なる参照可能者とする場合には、パターン３で説明したように、新たな共通鍵を生成すればよい。

【００７１】

なお、パターン３における参照処理の具体的な参照内容については、第１共通鍵１１３が第２共通鍵であり、第２共通鍵所有者がユーザＢである他は、パターン１と同様であるため、詳細な説明は省略する。図１３は、ブロックチェーンの内容が図１２に示す状態である場合の具体的な参照内容の例を示している。

【００７２】

参照可能者であるユーザＢが参照処理を行った場合、パターン１で説明した処理（パターン１の第１共通鍵１１３を所有している場合の処理）と同様の処理により（図７のステップＳ３０３にてＹｅｓと判定され、ステップＳ３０６の処理にて復号化されることにより）、図１３（Ａ）に示すように項目３に相当するデータが、復号化された状態で表示される。一方、参照可能者ではないユーザＡおよびユーザＣが参照処理を行った場合については、パターン１で説明した処理（パターン１の第１共通鍵１１３を所有していない場合の処理）と同様の処理により（ステップＳ３０４にてＮｏと判定され）、図１３（Ｂ）に示すように項目３に相当するデータが暗号化された状態で表示されることとなる。

【００７３】

このように、先に共通鍵をブロックに登録したユーザＡ以外のユーザＢにのみ参照可能とする場合、当該参照可能者（ユーザＢ）が新たに第２共通鍵を生成し、当該第２共通鍵にて暗号化したデータをブロックへ登録すればよい。したがって、参照可能者以外のユーザに対し、特定の情報に対する秘匿性を適切に担保することができる。また、当該生成した第２共通鍵を自己の所有する公開鍵で暗号化してブロックへ登録しておけば、第２共通鍵の管理負担を軽減することができる。

【００７４】

（変形例）

なお、この発明は、上記実施の形態に限定されず、様々な変形及び応用が可能である。例えば、情報処理装置１００では、上記実施の形態で示した全ての技術的特徴を備えるものでなくてもよく、従来技術における少なくとも１つの課題を解決できるように、上記実施の形態で説明した一部の構成を備えたものであってもよい。また、下記の変形例それぞれについて、少なくとも一部を組み合わせても良い。

【００７５】

上記実施の形態では、理解を容易にするため、同一グループ内の一つのトランザクションにて扱われるデータが一つのブロックに登録され、グループ毎にブロックチェーンが生成される例を示したが、これは一例である。例えば、図１４に示すように、一つのブロックには、異なるグループの契約書に関するトランザクションにて扱われるデータがそれぞれ登録されてもよい。図示する例では、グループＡについては、ユーザＡ、ユーザＢ、ユーザＣ間における契約書を示し、グループＢについては、ユーザＡ、ユーザＤ間における契約書を示している。なお、図示は省略しているが、同一グループ内の複数のトランザクションにて扱われるデータが一つのブロックに登録されてもよい。この場合についても、上記実施の形態と同様の処理により、参照可能者に対し適切に復号化可能となり、参照可能者以外のユーザに対し、特定の情報に対する秘匿性を適切に担保することができる。

【００７６】

また、上記実施の形態では、図１に示す情報処理システム１において、当該トランザクションにて扱われるデータを全てブロックチェーンにて管理する例を示したが、これは一例である。例えば、将来に亘って機密性の高い情報については、例えば図１５に示す情報処理システム２により管理してもよい。図２に示す情報処理システム２は、図１に示す情報処理システム１と比較して、データベース１９９を備えるセンターサーバ９９９を備えている。図２に示す情報処理システム２では、例えば、機密性の極めて高い情報（機密情報）については、センターサーバ９９９のデータベース１９９にて管理されている。そして、ブロックチェーンで連結されたブロックに、機密情報の格納先であるアドレス情報（センターサーバ９９９のデータベース１９９のアドレス）と、当該機密情報のハッシュ値と、当該機密情報を特定するユニークキーが暗号化されて（上記実施の形態と同様に暗号化されればよい）登録される。参照可能者は、参照処理を行うことで各ブロックの情報を取得し、機密情報の格納先アドレス情報、ハッシュ値、およびユニークキーを復号化する。

【００７７】

そして、復号化したアドレス情報に基づいてセンターサーバ９９９のデータベース１９９にアクセスし、当該ハッシュ値およびユニークキーが一致するか否かが検証され、一致

する場合にアクセスを許可して参照可能者に情報を参照させればよい。これによれば、機密情報をセンターサーバ９９９にて管理し、機密情報そのものをブロックチェーンでは管理せず、機密情報のハッシュ値をブロックチェーンにて管理する。したがって、万が一鍵に関する情報が漏洩した場合でも安全性を確保することができる。また、ハッシュ値に基づいて機密情報を復元することは不可能であるため、機密性を担保することができる。

【００７８】

また、上記実施の形態では、契約書を作成する場合を例として説明したが、この発明は、契約書を作成する場合に限られず、特定の情報についての秘匿性を担保することが必要な様々な取引が行われる場合において適用可能である。

【００７９】

なお、上述の機能を、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）とアプリケーションとの分担、またはＯＳとアプリケーションとの協同により実現する場合等には、ＯＳ以外の部分のみを媒体に格納してもよい。

【００８０】

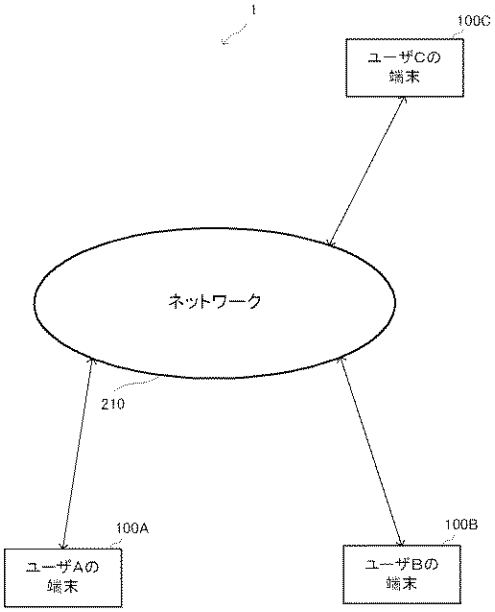
また、搬送波にプログラムを重畳し、通信ネットワークを介して配信することも可能である。例えば、通信ネットワーク上の掲示板（ＢＢＳ、Ｂｕｌｌｅｔｉｎ　Ｂｏａｒｄ　Ｓｙｓｔｅｍ）に当該プログラムを掲示し、ネットワークを介して当該プログラムを配信してもよい。そして、これらのプログラムを起動し、オペレーティングシステムの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行できるように構成してもよい。

【符号の説明】

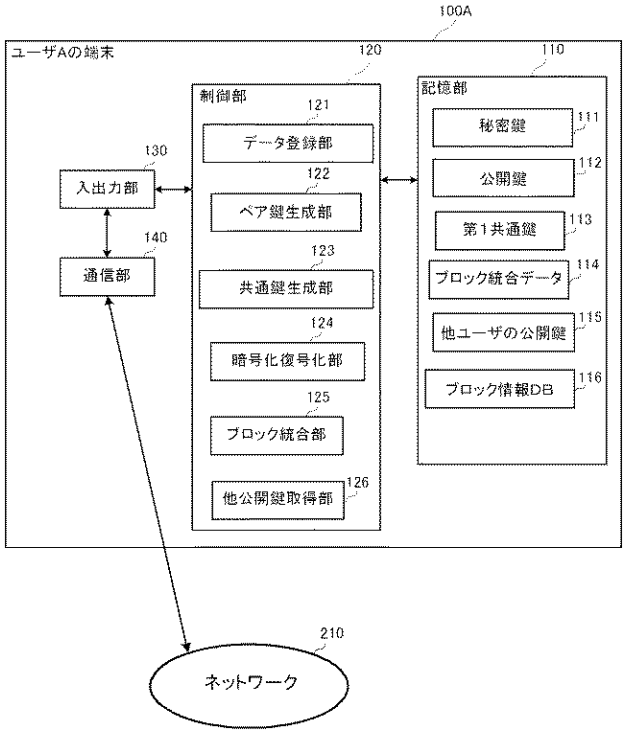
【００８１】

１　情報処理システム、２　情報処理システム、　１００Ａ～Ｃ　情報処理装置、１１０　記憶部、１１１　秘密鍵、１１２　公開鍵、１１３　第１共通鍵、１１３Ａ　暗号化した第１共通鍵、１１４　ブロック統合データ、１１５　他ユーザの公開鍵、１１６　ブロック情報ＤＢ、１２０　制御部、１２１　データ登録部、１２２　ペア鍵生成部、１２３　共通鍵生成部、１２４　暗号化復号化部、１２５　ブロック統合部、１２６　他公開鍵取得部、１３０　入出力部、１４０　通信部、１９９　データベース、２１０　ネットワーク、９９９　センターセーバ

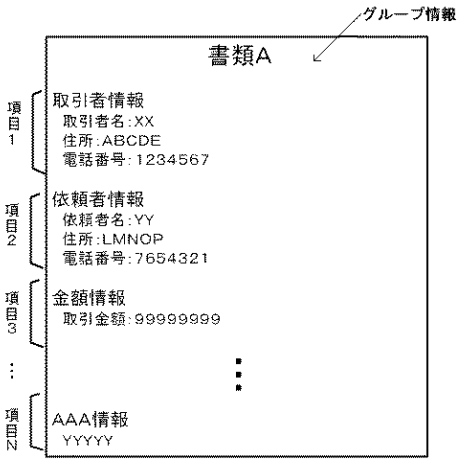
【図１】


1
100C
ユーザCの端末
ネットワーク
210
100A
ユーザAの端末
100B
ユーザBの端末

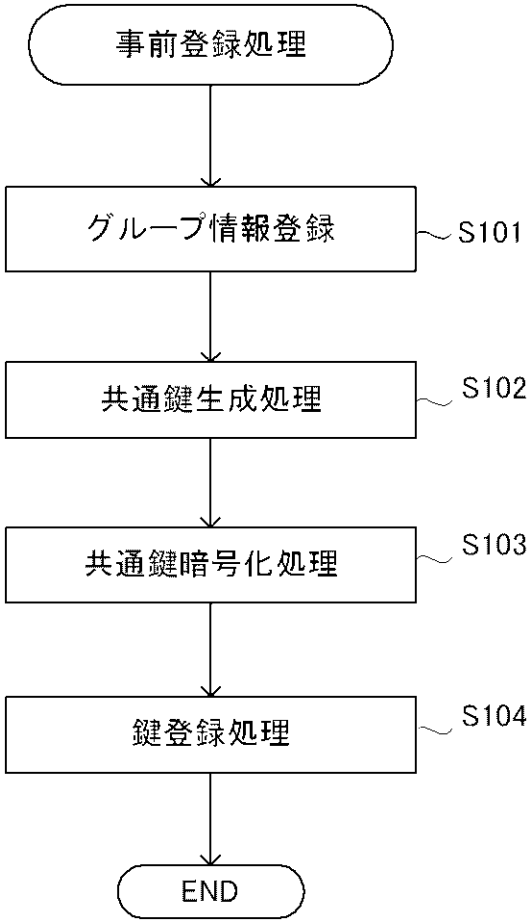
【図２】


100A
ユーザAの端末
120
制御部
121
データ登録部
122
ペア鍵生成部
123
共通鍵生成部
124
暗号化復号化部
125
ブロック統合部
126
他公開鍵取得部
110
記憶部
111
秘密鍵
112
公開鍵
113
第1共通鍵
114
ブロック統合データ
115
他ユーザの公開鍵
116
ブロック情報DB
130
入出力部
140
通信部
210
ネットワーク

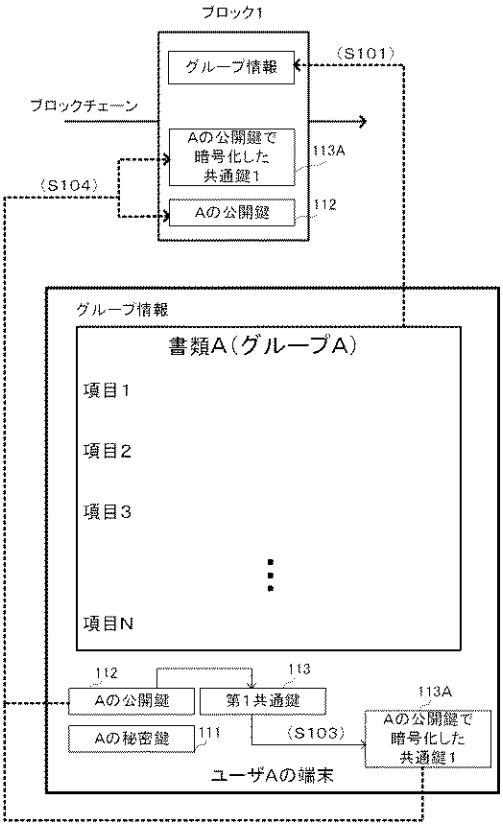
【図３】


グループ情報
書類A
項目1
取引者情報
取引者名:XX
住所:ABCDE
電話番号:1234567
項目2
依頼者情報
依頼者名:YY
住所:LMNOP
電話番号:7654321
項目3
金額情報
取引金額:99999999
項目N
AAA情報
YYYYY

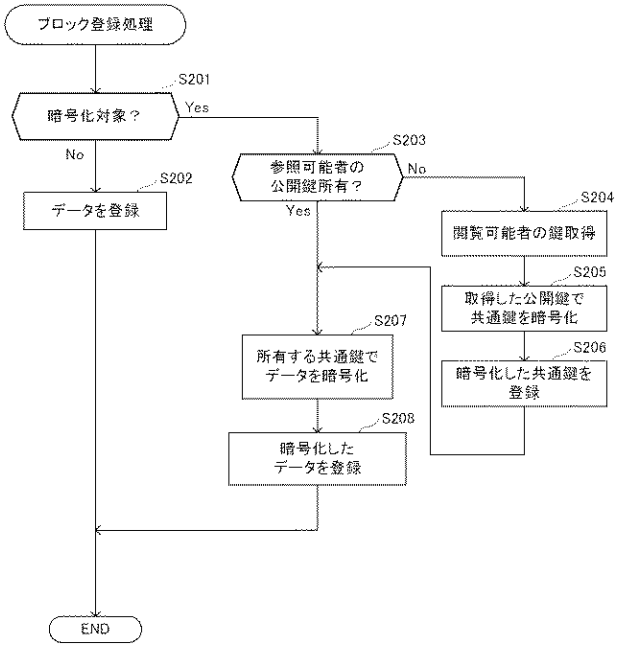
【図４】


事前登録処理
グループ情報登録
S101
共通鍵生成処理
S102
共通鍵暗号化処理
S103
鍵登録処理
S104
END

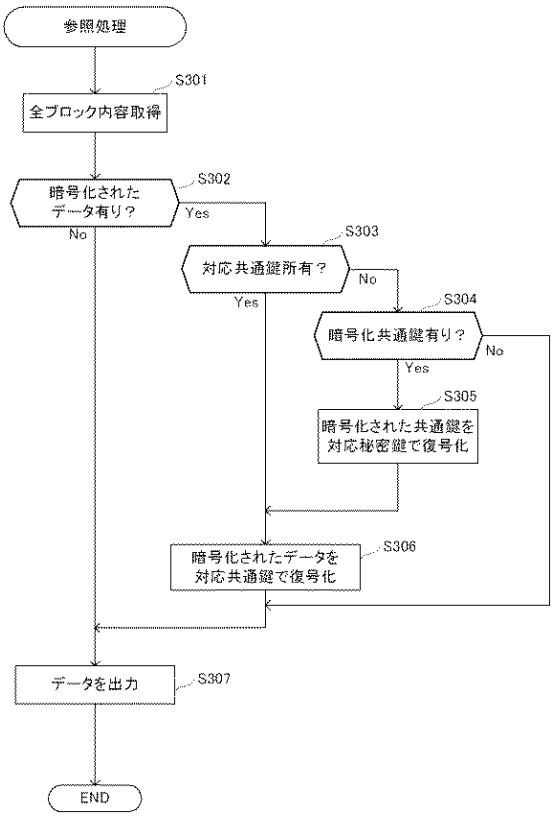
【図５】



【図６】

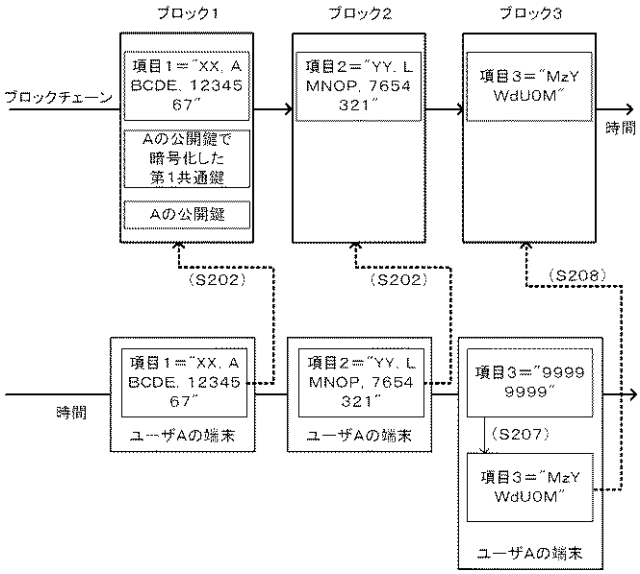


【図７】



【図８】

＊項目3について、ユーザAのみ参照可能な場合（パターン1）におけるブロック登録



【図９】

(A)ユーザAが参照した場合

書類A

取引者情報
取引者名:XX
住所:ABCDE
電話番号:1234567

依頼者情報
依頼者名:YY
住所:LMNOP
電話番号:7654321

金額情報(S306にて復号化)
取引金額:99999999

(B)ユーザB、Cが参照した場合

書類A

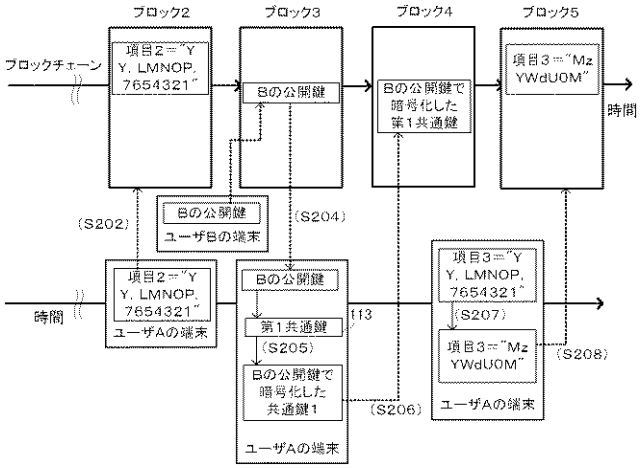
取引者情報
取引者名:XX
住所:ABCDE
電話番号:1234567

依頼者情報
依頼者名:YY
住所:LMNOP
電話番号:7654321

金額情報(S304でNoと判断)
取引金額:MzYWdUOM

【図１０】

＊項目3について、ユーザAおよびBが参照可能な場合(パターン2)におけるブロック登録



【図１１】

(A)ユーザA、Bが参照した場合

書類A

取引者情報
取引者名:XX
住所:ABCDE
電話番号:1234567

依頼者情報
依頼者名:YY
住所:LMNOP
電話番号:7654321

金額情報(ユーザBはS305,S306により復号化)
取引金額:99999999

(B)ユーザCが参照した場合

書類A

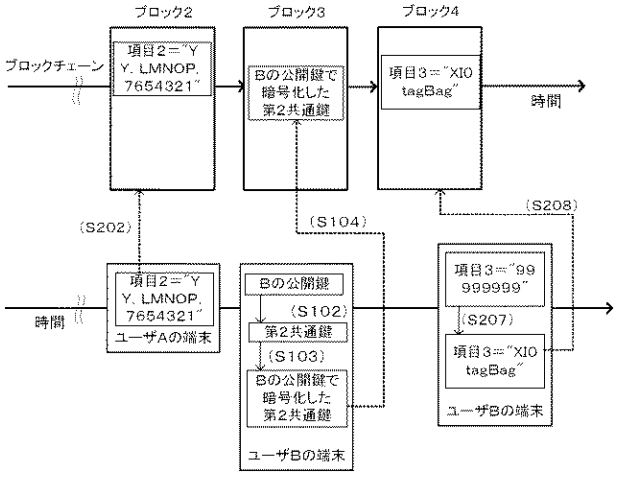
取引者情報
取引者名:XX
住所:ABCDE
電話番号:1234567

依頼者情報
依頼者名:YY
住所:LMNOP
電話番号:7654321

金額情報(S304でNoと判断)
取引金額:MzYWdUOM

【図１２】

＊項目3について、ユーザBのみが参照可能な場合(パターン3)におけるブロック登録



【図１３】

(A)ユーザBが参照した場合

書類A

取引者情報
取引者名:XX
住所:ABCDE
電話番号:1234567

依頼者情報
依頼者名:YY
住所:LMNOP
電話番号:7654321

金額情報(S306にて復号化)
取引金額:99999999

(B)ユーザA、Cが参照した場合

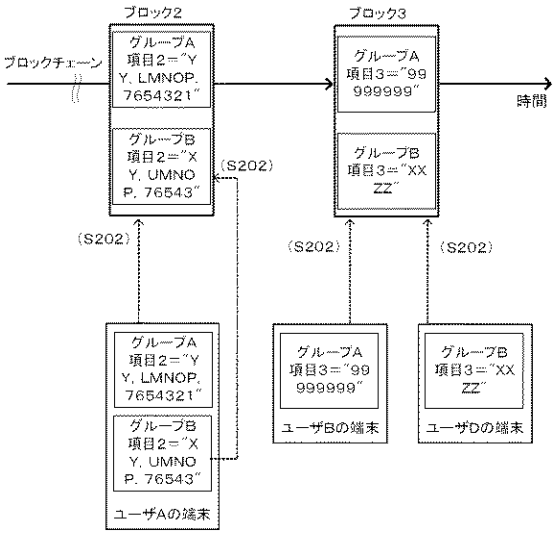
書類A

取引者情報
取引者名:XX
住所:ABCDE
電話番号:1234567

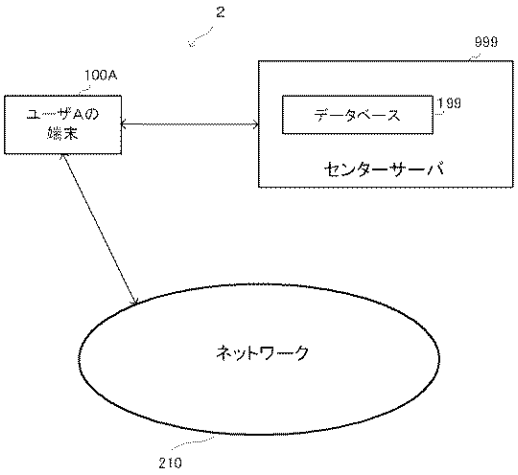
依頼者情報
依頼者名:YY
住所:LMNOP
電話番号:7654321

金額情報(S304でNoと判断)
取引金額:XIOtagBag

【図１４】



【図１５】



フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
	G06F 21/60 320	

(72)発明者 愛敬 真生
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72)発明者 赤羽 喜治
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72)発明者 世取山 進二
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72)発明者 稲葉 高洋
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72)発明者 成清 義博
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72)発明者 富田 京志
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72)発明者 大網 恵一
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内

Ｆターム(参考) 5J104 AA08 AA16 EA04 EA19 LA03 NA02 NA37 PA07
5L055 AA71