(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7190336号
(P7190336)

(45)発行日　令和4年12月15日(2022.12.15)

(24)登録日　令和4年12月7日(2022.12.7)

(51)国際特許分類			FI		
H04L	*9/08*	*(2006.01)*	H04L	9/08	A
H04L	*9/32*	*(2006.01)*	H04L	9/08	C
G06F	*21/62*	*(2013.01)*	H04L	9/32	200Z
			G06F	21/62	309
			G06F	21/62	318

請求項の数　7　（全20頁）

(21)出願番号　特願2018-215054(P2018-215054)
(22)出願日　平成30年11月15日(2018.11.15)
(65)公開番号　特開2020-88421(P2020-88421A)
(43)公開日　令和2年6月4日(2020.6.4)
審査請求日　令和3年8月10日(2021.8.10)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100121083
弁理士　青木 宏義
(74)代理人　100138391
弁理士　天田 昌行
(74)代理人　100074099
弁理士　大菅 義之
(74)代理人　100133570
弁理士　▲徳▼永 民雄
(72)発明者　鈴木 大
神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内

最終頁に続く

(54)【発明の名称】　通信装置、通信方法、および通信プログラム

(57)【特許請求の範囲】
【請求項１】
データ提供ノード、データ取得ノード、および複数の参加ノードが接続されるネットワークにおいて使用される通信方法であって、
前記データ提供ノードは、
　データをＮ（Ｎは、２以上の整数）個のデータ部品に分割し、
　　前記Ｎ個のデータ部品を異なる記憶領域に保存し、
　　各データ部品が保存された記憶領域のアドレスを、前記複数の参加ノードの中の異なるＮ個の参加ノードの公開鍵でそれぞれ暗号化し、
　　前記データ取得ノードが前記データにアクセスする権利を有することを表すアクセス権情報および暗号化されたＮ個のアドレスを前記複数の参加ノードに送信し、
各参加ノードは、前記データの取得を要求するデータ取得要求を前記データ取得ノードから受信したときに、
前記アクセス権情報を用いて前記データ取得ノードが前記データにアクセスする権利を有することを確認し、
暗号化された前記Ｎ個のアドレスを自分の秘密鍵で復号し、
復号により得られたアドレスを前記データ取得ノードに送信する
　ことを特徴とする通信方法。
【請求項２】
　前記データ取得ノードは、２以上の参加ノードから受信するアドレスを用いて、前記記

憶領域から対応するデータ部品を取得する
　ことを特徴とする請求項１に記載の通信方法。
【請求項３】
　前記Ｎ個のデータ部品のうちのＫ個のデータ部品から前記データを再生可能なように、シャミアの秘密分散法を用いて前記データがＮ個のデータ部品に分割されたとき、前記データ取得ノードは、Ｋ個以上の参加ノードから受信するアドレスを用いて、前記記憶領域からＫ個以上のデータ部品を取得して前記データを再生する
　ことを特徴とする請求項２に記載の通信方法。
【請求項４】
　前記データは、Ｎ個のデータ部品に分割される前に、前記データ取得ノードの公開鍵で暗号化される
　ことを特徴とする請求項１に記載の通信方法。
【請求項５】
　前記データは、Ｎ個のデータ部品に分割される前に、共通鍵で暗号化され、
　前記共通鍵は、前記データ取得ノードの公開鍵で暗号化されて前記データ取得ノードに送信される
　ことを特徴とする請求項１に記載の通信方法。
【請求項６】
データ提供ノード、データ取得ノード、および複数の参加ノードが接続されるネットワークにおいて使用される通信方法であって、
　前記データ提供ノードは、
　データをＮ（Ｎは、２以上の整数）個のデータ部品に分割し、
　　前記データ取得ノードが前記データにアクセスする権利を有することを表すアクセス権情報を前記複数の参加ノードに送信し、
　　各データ部品を、前記複数の参加ノードの中の異なるＮ個の参加ノードに送信し、
　前記Ｎ個の参加ノードは、それぞれ、
　　前記データの取得を要求するデータ取得要求を前記データ取得ノードから受信し、且つ、前記アクセス権情報を用いて前記データ取得ノードが前記データにアクセスする権利を有することを確認したときに、前記データ提供ノードから受信したデータ部品を前記データ取得ノードに送信する
　ことを特徴とする通信方法。
【請求項７】
データ提供ノード、データ取得ノード、および複数の参加ノードが接続されるネットワークにおいて使用される通信方法であって、
　前記データ提供ノードは、
　データをＮ（Ｎは、２以上の整数）個のデータ部品に分割し、
　　各データ部品を、前記複数の参加ノードの中の異なるＮ個の参加ノードの公開鍵でそれぞれ暗号化し、
　　前記データ取得ノードが前記データにアクセスする権利を有することを表すアクセス権情報および暗号化された前記Ｎ個のデータ部品を前記複数の参加ノードに送信し、
　前記Ｎ個の参加ノードは、それぞれ、
　　前記データの取得を要求するデータ取得要求を前記データ取得ノードから受信し、且つ、前記アクセス権情報を用いて前記データ取得ノードが前記データにアクセスする権利を有することを確認したときに、暗号化された前記Ｎ個のデータ部品を自分の秘密鍵で復号し、
　　復号により得られたデータ部品を前記データ取得ノードに送信する
　ことを特徴とする通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、通信装置、通信方法、および通信プログラムに係わる。
【背景技術】
【０００２】
近年、データを売買するサービスを提供するデータ流通市場が普及し始めている。データ流通市場の参加者は、自分が保有するデータを市場に提供することができる。また、参加者は、市場に提供されているデータを取得または購入することができる。
【０００３】
他方、管理者が存在しない分散環境下で、改ざん不能な状態でデータを管理するブロックチェーン技術が注目されている。ブロックチェーン技術は、複数の参加者または全参加者がトランザクションを検証することで改ざん不能な分散台帳を実現する。そして、データ流通市場をサポートするためにブロックチェーンを利用する方法が提案されている。
【０００４】
ここで、ブロックチェーンのような複数の分散されたノードが協調して処理を実行するシステムでは、各ノードにおける処理結果を同期させるため、合意形成アルゴリズムが使用される。合意形成アルゴリズムは、複数の参加ノードが処理内容および処理結果を検証した後に処理を確定させる。
【０００５】
また、データ流通システムにおいては、データの登録およびデータの取得が行われる。データ登録手続においては、登録するデータに関連する情報（例えば、メタデータ）が使用される。メタデータは、登録するデータをどのユーザに公開するのかを表すアクセスポリシ情報を含む。データ取得手続においては、データ提供者は、アクセスポリシの検証を行い、データの取得を要求するユーザがアクセス権を有することを確認できたときにデータを送信する。
【０００６】
なお、秘匿性の高いデータを少ないハードウェア資源で安全に保管する方法が提案されている（例えば、特許文献１）。また、クラウドコンピューティングリソースに確実にデータを記憶する方法が提案されている（例えば、特許文献２）。さらに、ネットワークを介して行われる通信の匿名性を向上する方法が提案されている（例えば、特許文献３）。
【先行技術文献】
【特許文献】
【０００７】
【文献】特開２００６－３１１３８３号公報
特表２０１２－５２７８３８号公報
特開２０１７－０７９３５０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００８】
ブロックチェーンにおいては、上述したように、複数の参加者によりトランザクションが検証される。そして、複数の検証結果に基づいて全参加者の合意が形成される。
【０００９】
合意形成アルゴリズムの１つとして、ＰｏＷ（Proof of Work）が普及している。ＰｏＷは、厳格な承認処理を行うので、不特定多数の参加者によるネットワークで合意を形成するケースに適している。したがって、データ流通サービスにおいて不特定多数の参加者から要求されるトランザクションを処理する場合、ＰｏＷで合意形成を行うことが考えられる。ただし、ＰｏＷで合意形成を行う場合、要求されたトランザクションが実行されるまでに要する時間が長くなることがある。
【００１０】
本発明の１つの側面に係わる目的は、管理者が存在しない分散環境下で、改ざん困難なデータの送信に要する時間を削減することである。
【課題を解決するための手段】

【００１１】
本発明の１つの態様の通信方法は、複数の参加ノードの合意に基づいてデータ取得ノードにデータを提供する。この通信方法は、前記データをＮ（Ｎは、２以上の整数）個のデータ部品に分割し、前記Ｎ個のデータ部品を異なる記憶領域に保存し、各データ部品が保存された記憶領域のアドレスを、前記複数の参加ノードの中の異なるＮ個の参加ノードの公開鍵でそれぞれ暗号化し、前記データ取得ノードが前記データにアクセスする権利を有することを表すアクセス権情報および暗号化されたＮ個のアドレスを前記複数の参加ノードに送信する。
【発明の効果】
【００１２】
上述の態様によれば、管理者が存在しない分散環境下で、改ざん困難なデータの送信に要する時間が削減される。
【図面の簡単な説明】
【００１３】
【図１】本発明の実施形態に係わる通信システムの一例を示す図である。
【図２】ブロックの検証および確定について説明する図である。
【図３】ＰｏＷで合意形成が行われるケースにおけるデータ送信のシーケンスの一例を示す図である。
【図４】データ登録手続の一例を示す図である。
【図５】シャミアの秘密分散法について説明する図である。
【図６】アドレスリストの一例を示す図である。
【図７】データ部品および暗号化アドレスを生成する手順の一例を示す図である。
【図８】データ取得手続の一例を示す図（その１）である。
【図９】データ取得手続の一例を示す図（その２）である。
【図１０】データ取得手続の一例を示す図（その３）である。
【図１１】データ取得手続の一例を示す図（その４）である。
【図１２】暗号化アドレスの復号およびデータ部品の取得の一例を示す図である。
【図１３】データ取得手続のシーケンスの一例を示す図である。
【図１４】データ登録手続の一例を示すフローチャートである。
【図１５】データ取得手続における参加ノードの処理の一例を示すフローチャートである。
【図１６】データ取得者の処理の一例を示すフローチャートである。
【図１７】各ノードに実装されるコンピュータのハードウェア構成の一例を示す図である。
【図１８】第２の実施形態におけるデータ登録手続の一例を示す図である。
【図１９】第３の実施形態におけるデータ登録手続の一例を示す図である。
【図２０】データ部品リストの一例を示す図である。
【発明を実施するための形態】
【００１４】
図１は、本発明の実施形態に係わる通信システムの一例を示す。この実施例では、通信システム１００において、ブロックチェーン技術を利用してデータ流通サービスが提供される。
【００１５】
以下の記載では、データ流通サービスに参加するユーザにより使用されるコンピュータを「参加ノード（又は、参加者）」と呼ぶことがある。データ流通サービスにデータを提供するユーザまたはそのユーザにより使用されるコンピュータを「データ提供者（又は、データ提供ノード）」と呼ぶことがある。データ流通サービスを利用してデータを取得するユーザまたはそのユーザにより使用されるコンピュータを「データ取得者（又は、データ取得ノード）」と呼ぶことがある。データ処理トランザクションを検証するコンピュータを「マイナー」と呼ぶことがある。なお、データ提供者、データ取得者、マイナーは、それぞれデータ流通サービスに参加する参加ノードである。すなわち、各参加ノードは、データ提供ノード、データ取得ノード、またはマイナーとして機能することができる。

【００１６】
ブロックチェーンネットワーク２００には、図１に示すように、複数の参加ノード（図１では、参加ノード１～４）、データ提供者１１、参加ノード（データ取得者）１２、マイナー１３が接続されている。なお、ブロックチェーンネットワーク２００には、不特定多数の参加ノードが接続され得る。また、ブロックチェーンネットワーク２００には、複数のマイナーが接続される。
【００１７】
各参加ノード１～４は、暗号通信を実行する機能を備える。すなわち、各参加ノード１～４は、公開鍵および秘密鍵のペアを生成し、その公開鍵を公開する。よって、例えば、データ提供者１１は、各参加ノード１～４の公開鍵を取得している。
【００１８】
データ提供者１１は、データ流通サービスにデータＤを提供する。ただし、この実施例では、データ提供者１１は、データ提供者１１が許可する参加ノードのみに対してデータＤを提供する。図１に示す例では、データ提供者１１は、参加ノード（データ取得者）１２に対してデータＤへのアクセスを許可するものとする。
【００１９】
参加ノード（データ取得者）１２は、データＤを取得したいときは、データＤの取得を要求するデータ取得要求トランザクションを生成する。このデータ取得要求トランザクションは、ブロックチェーンネットワーク２００を介して各参加ノードに送信される。
【００２０】
マイナー１３は、各参加ノードにより生成されるトランザクションを検証する。たとえば、データ取得者１２によりデータ取得要求トランザクションが生成されたときは、マイナー１３は、そのデータ取得要求トランザクションを検証する。但し、マイナー１３は、複数のトランザクションを含む「ブロック」を検証する。
【００２１】
図２は、ＰｏＷによるブロックの検証および確定について説明する図である。この実施例では、マイナー＃１～＃３がそれぞれブロックを検証する。検証結果は、ブロックチェーンネットワークに接続する全参加ノードに送信される。なお、図２に示す例では、ブロックＡの検証が終了しているものとする。
【００２２】
マイナー＃１は、トランザクションＴｘ１、Ｔｘ２、Ｔｘ３を含むブロックＢを検証し、さらにトランザクションＴｘ４、Ｔｘ５、Ｔｘ６を含むブロックＣを検証する。これらの検証結果は、全参加ノードに送信される。また、マイナー＃２は、トランザクションＴｘ１、Ｔｘ２、Ｔｘ３を含むブロックＢを検証し、さらにトランザクションＴｘ４、Ｔｘ６、Ｔｘ７を含むブロックＤを検証する。これらの検証結果も、全参加ノードに送信される。
【００２３】
各参加ノードにおいて、受信順に検証結果が結合される。すなわち、チェーンが形成される。たとえば、参加ノードＸにおいては、マイナー＃１から受信する検証結果に基づいて、ブロックＡ、Ｂ、Ｃが順番に結合される。続いて、マイナー＃２の検証結果が参加ノードＸに到着する。マイナー＃２から受信する検証結果においては、ブロックＢの次にブロックＤが続いている。この場合、参加ノードＸにおいて、ブロックＢの次にブロックＤも結合される。この後、マイナー＃３の検証結果が参加ノードＸに到着する。マイナー＃３から受信する検証結果においては、ブロックＣの次にブロックＥが続いている。この場合、参加ノードＸにおいて、ブロックＣの次にブロックＥが結合される。
【００２４】
参加ノードは、あるブロック（以下、対象ブロック）の後ろに所定数のブロックが結合されたときに、対象ブロックを確定させる。ＰｏＷにおいては、例えば、対象ブロックの後ろに６個のブロックが結合されたときに、対象ブロックが確定したと判定される。そして、参加ノードは、確定したブロック内のトランザクションを実行できる。例えば、デー

タ送信要求トランザクションが参加ノードＸに与えられたときは、そのデータ送信要求トランザクションを含むブロックの後ろに６個のブロックが結合された後に、参加ノードＸは、そのデータ送信要求トランザクションに従ってデータ送信を行うことができる。

【００２５】

図３は、ＰｏＷで合意形成が行われるケースにおけるデータ送信のシーケンスの一例を示す。この実施例では、データ取得者がデータ取得要求トランザクションを生成して全ノードに送信するものとする。なお、データ取得者がデータ取得要求トランザクションを生成したとき、データ提供者のブロックチェーンには、ブロック０が記録されているものとする。

【００２６】

マイナーは、データ取得要求トランザクションを含むブロック１を検証し、その検証結果を全ノードに送信する。これにより、データ提供者のブロックチェーンにおいて、ブロック０の次にブロック１が結合される。

【００２７】

この後、ネットワーク上の参加ノードが次々とトランザクションを生成する。また、マイナーは、生成される複数のトランザクションを含むブロックを検証し、その検証結果を全ノードに送信する。この結果、各ノードのブロックチェーンにブロックが追加されてゆく。そして、データ提供者のブロックチェーンにおいて、ブロック１の後ろに６個のブロック（すなわち、ブロック２～７）が結合すると、データ提供者は、ブロック１に含まれているデータ取得要求トランザクションを実行する。これにより、データ提供者からデータ取得者にデータが送信される。

【００２８】

このように、ＰｏＷで合意形成が行われるケースでは、処理すべきトランザクションを受け取ったノードは、所定数のブロックの検証が終了するまでそのトランザクションを実行できない。このため、要求された処理（図３に示す例では、データ送信）が実行されるまでの待ち時間が長くなることがある。

【００２９】

＜第１の実施形態＞

図４は、データ登録手続の一例を示す。この実施例では、データ提供者１１がデータ流通サービスにデータＤを提供するものとする。

【００３０】

データ提供者１１は、シャミアの秘密分散法で、データＤをＮ（Ｎは、２以上の整数）個のデータ部品に分割する。図４に示す例では、データＤは、４個のデータ部品Ｄ１～Ｄ４に分割されている。

【００３１】

なお、データ提供者１１は、データＤを分割する前に、データＤを暗号化してもよい。例えば、データＤは、データＤへのアクセスが許可されている参加ノードの公開鍵で暗号化される。或いは、データＤは、共通鍵で暗号化される。この場合、この共通鍵は、データＤへのアクセスが許可されている参加ノードの公開鍵で暗号化される。

【００３２】

シャミアの秘密分散法においては、図５に示すように、入力データは、Ｎ個のデータ部品に分割される。このとき、各データ部品は、入力データの内容が分からないように生成される。また、復号装置は、Ｎ個のデータ部品のうちのＫ（Ｋは、Ｎ以下の整数）個のデータ部品から入力データを再生できる。Ｎの値およびＫの値は、予め設定することが可能である。例えば、ＮおよびＫの値は、それぞれ参加ノードの総数であってもよい。また、ＮおよびＫの値は、それぞれデータの重要度に応じて決定してもよい。この場合、データが重要であるときに、ＮおよびＫの値を大きくしてもよい。

【００３３】

データ提供者１１は、シャミアの秘密分散法以外の方法でデータＤをＮ個のデータ部品に分割してもよい。ただし、各データ部品は、元データの内容が分からないように生成さ

れることが好ましい。また、Ｎ個のデータ部品のうちのＫ個のデータ部品から元データを再生できることが好ましい。

【００３４】

データ提供者１１は、データ部品Ｄ１～Ｄ４を所定の記憶領域に保存する。この実施例では、データ部品Ｄ１～Ｄ４は、ＩＰＦＳ（Inter Planetary File System）上の異なる領域に保存される。このとき、データ部品Ｄ１～Ｄ４は、各参加ノードからアクセス可能な状態でＩＰＦＳに保存される。ただし、データ部品Ｄ１～Ｄ４が保存された記憶領域のアドレスは公開されない。よって、この時点では、各参加ノードは、実質的にデータ部品Ｄ１～Ｄ４にアクセスできない。

【００３５】

データ提供者１１は、データ部品Ｄ１～Ｄ４が保存された記憶領域のアドレスを取得する。例えば、ＩＰＦＳにデータ部品Ｄ１～Ｄ４が保存されたときには、各データ部品Ｄ１～Ｄ４が保存された記憶領域のアドレスが出力される。この例では、データ部品Ｄ１、Ｄ２、Ｄ３、Ｄ４がそれぞれアドレスＡＤＤ１、ＡＤＤ２、ＡＤＤ３、ＡＤＤ４に保存されるものとする。

【００３６】

なお、図４に示す例では、データ部品Ｄ１～Ｄ４はＩＰＦＳに保存されるが、第１の実施形態はこの構成に限定されるものではない。すなわち、データ提供者１１は、任意の記憶領域にデータ部品Ｄ１～Ｄ４を保存することができる。

【００３７】

データ提供者１１は、データ部品Ｄ１～Ｄ４が保存された記憶領域のアドレスＡＤＤ１～ＡＤＤ４をそれぞれ暗号化する。このとき、データ提供者１１は、データ流通サービスに参加する全参加ノードの中から、後述する復号処理を実行する参加ノードとして、ＩＰＦＳに保存したデータ部品の個数と同数の参加ノードを選択する。この実施例では、後述する復号処理を実行する参加ノードとして、データ部品Ｄ１～Ｄ４に対してそれぞれ参加ノード１～４が選択されるものとする。そして、データ提供者１１は、データ部品Ｄ１～Ｄ４が保存された記憶領域のアドレスＡＤＤ１～ＡＤＤ４を、それぞれ参加ノード１～４の公開鍵で暗号化する。即ち、アドレスＡＤＤ１は参加ノード１の公開鍵で暗号化され、アドレスＡＤＤ２は参加ノード２の公開鍵で暗号化され、アドレスＡＤＤ３は参加ノード３の公開鍵で暗号化され、アドレスＡＤＤ４は参加ノード４の公開鍵で暗号化される。この結果、暗号化アドレスＡＤＤ１～ＡＤＤ４が得られる。

【００３８】

データ提供者１１は、データＤの登録に係わるアドレスリストを生成する。このアドレスリストは、図６に示すように、アクセス権情報、復号ノードリスト、暗号化アドレスを含む。アクセス権情報は、データＤへのアクセスが許可された参加ノードを表す。この例では、データ提供者１１は、参加ノード（データ取得者）１２に対してデータＤへのアクセスを許可している。復号ノードリストは、暗号化アドレスＡＤＤ１～ＡＤＤ４のいずれか１つを復号する参加ノードを表す。この例では、参加ノード１～４の公開鍵でアドレスＡＤＤ１～ＡＤＤ４をそれぞれ暗号化することで、暗号化アドレスＡＤＤ１～ＡＤＤ４が得られている。よって、復号ノードリストには、参加ノード１～４が設定されている。さらに、暗号化アドレスとして、上述のようにして生成された暗号化アドレスＡＤＤ１～ＡＤＤ４がアドレスリストに設定される。

【００３９】

アドレスリストは、全参加ノードに公開される。すなわち、データ提供者１１は、図４に示すように、このアドレスリストを全参加ノードに送信する。アドレスリストは、例えば、データ登録コントラストの実行結果として、ブロックチェーン上に記録されるようにしてもよい。そして、各参加ノードは、データ提供者１１から受信するアドレスリストを保存する。これにより、データ登録手続が完了する。

【００４０】

図７は、データ部品および暗号化アドレスを生成する手順の一例を示す。データ登録手

続においては、データ提供者１１は、データＤをシャミアの秘密分散法でデータ部品Ｄ１～Ｄ４に分割してＩＰＦＳに登録する。また、データ提供者１１は、データ部品Ｄ１～Ｄ４が保存された記憶領域のアドレスＡＤＤ１～ＡＤＤ４を取得する。さらに、データ提供者１１は、参加ノード１～４の公開鍵ＰＫ１～ＰＫ４でアドレスＡＤＤ１～ＡＤＤ４を暗号化して暗号化アドレスＡＤＤ１～ＡＤＤ４を生成する。そして、暗号化アドレスＡＤＤ１～ＡＤＤ４を含むアドレスリストは、ブロックチェーン上で公開される。

【００４１】

図８～図１１は、データ取得手続の一例を示す。この例では、参加ノード（データ取得者）１２がデータＤを取得するものとする。よって、データ取得手続の説明においては、参加ノード（データ取得者）１２を単に「データ取得者１２」と呼ぶことがある。なお、図８～図１１に示すデータ取得手続が開始される前に、図４に示すデータ登録手続が完了しているものとする。すなわち、データＤを分割することにより得られるデータ部品Ｄ１～Ｄ４がＩＰＦＳに保存されている。また、各参加ノード１～４は、データ提供者１１から図６に示すアドレスリストを受信している。

【００４２】

図８において、データ取得者１２は、データ取得要求トランザクションを生成する。このとき、データ取得者１２は、データ取得コントラストにトランザクションを送信してもよい。また、このデータ取得要求トランザクションは、データＤの取得を要求するメッセージを含む。そして、このデータ取得要求トランザクションは、全参加ノードに送信される。すなわち、各参加ノード１～４は、データ取得者１２から送信されるデータ取得要求トランザクションを受信する。なお、データ取得要求トランザクションは、その送信元を表す情報を含む。

【００４３】

図９において、マイナー１３は、データ取得者１２から送信されたデータ取得要求トランザクションを含むブロックを検証する。そして、マイナー１３は、このブロックの検証結果を全参加ノードに送信する。すなわち、各参加ノード１～４は、マイナー１３から検証結果を受信する。

【００４４】

図１０において、各参加ノード１～４は、データ取得要求トランザクションを含むブロックについての検証結果をマイナー１３から受信すると、データ取得者１２から送信されたデータ取得要求トランザクションが要求するデータへのアクセス権を確認する。このとき、各参加ノード１～４は、データ提供者１１から先に受信しているアドレスリストを参照する。この実施例では、図６に示すように、参加ノード（データ取得者）１２に対してデータＤへのアクセス権が与えられている。したがって、各参加ノード１～４は、受信したデータ取得要求トランザクションに対応する処理を実行する。

【００４５】

まず、各参加ノード１～４は、自ノードが暗号化アドレスを復号する復号ノードであるか否かを判定する。具体的には、データ提供者１１から先に受信しているアドレスリストにおいて、復号ノードとして自ノードが登録されているか否が判定される。図６に示す例では、復号ノードとして参加ノード１～４が登録されている。よって、各参加ノード１～４は、復号処理を実行する。

【００４６】

参加ノード１は、参加ノード１の秘密鍵を用いて４個の暗号化アドレスＡＤＤ１～ＡＤＤ４に対して復号処理を行う。ここで、暗号化アドレスＡＤＤ１～ＡＤＤ４は、それぞれ参加ノード１～４の公開鍵で暗号化されている。したがって、参加ノード１の秘密鍵で復号処理を実行すると、暗号化アドレスＡＤＤ１に対する復号は成功するが、暗号化アドレスＡＤＤ２～ＡＤＤ４に対する復号は失敗する。すなわち、参加ノード１は、アドレスＡＤＤ１を取得できるが、アドレスＡＤＤ２～ＡＤＤ４を取得できない。

【００４７】

同様に、参加ノード２は、参加ノード２の秘密鍵を用いて暗号化アドレスＡＤＤ１～Ａ

ＤＤ４に対して復号処理を行い、アドレスＡＤＤ２を取得する。参加ノード３は、参加ノード３の秘密鍵を用いて暗号化アドレスＡＤＤ１～ＡＤＤ４に対して復号処理を行い、アドレスＡＤＤ３を取得する。参加ノード４は、参加ノード４の秘密鍵を用いて暗号化アドレスＡＤＤ１～ＡＤＤ４に対して復号処理を行い、アドレスＡＤＤ４を取得する。この後、参加ノード１～４は、それぞれアドレスＡＤＤ１～ＡＤＤ４をデータ取得者１２に送信する。

【００４８】

図１１において、データ取得者１２は、参加ノード１～４から受信したアドレスにアクセスして、ＩＰＦＳからデータ部品Ｄ１～Ｄ４を取得する。具体的には、データ取得者１２は、アドレスＡＤＤ１からデータ部品Ｄ１を取得し、アドレスＡＤＤ２からデータ部品Ｄ２を取得し、アドレスＡＤＤ３からデータ部品Ｄ３を取得し、アドレスＡＤＤ４からデータ部品Ｄ４を取得する。そして、データ取得者１２は、取得したデータ部品Ｄ１～Ｄ４からデータＤを再生する。

【００４９】

なお、図１１に示す例では、データ取得者１２は全てのデータ部品Ｄ１～Ｄ４を取得しているが、第１の実施形態はこのようなケースに限定されるものではない。例えば、データ部品Ｄ１～Ｄ４のうちの任意の３つからデータＤを再生可能なときは、データ取得者１２は、データ部品Ｄ１～Ｄ４のうちの任意の３つを取得してデータＤを再生してもよい。例えば、参加ノード４による復号が失敗した場合、データ取得者１２は、アドレスＡＤＤ１～ＡＤＤ３を受信する。この場合、データ取得者１２は、ＩＰＦＳからデータ部品Ｄ１～Ｄ３を取得してデータＤを再生する。

【００５０】

図１２は、暗号化アドレスの復号およびデータ部品の取得の一例を示す。この例では、各参加ノード１～４によりデータ取得者１２のアクセス権の確認が終了しているものとする。

【００５１】

参加ノード１～４は、アドレスリストに設定されている暗号化アドレスＡＤＤ１～ＡＤＤ４をそれぞれ参加ノード１～４の秘密鍵ＳＫ１～ＳＫ４で復号してアドレスＡＤＤ１～ＡＤＤ４を得る。アドレスＡＤＤ１～ＡＤＤ４は、それぞれデータ取得者１２に送信される。そうすると、データ取得者１２は、アドレスＡＤＤ１～ＡＤＤ４を用いてＩＰＦＳにアクセスしてデータ部品Ｄ１～Ｄ４を取得する。そして、データ取得者１２は、データ部品Ｄ１～Ｄ４からデータＤを再生する。

【００５２】

図１３は、データ取得手続のシーケンスの一例を示す。この例では、図４に示すデータ登録手続が完了しているものとする。すなわち、データＤを分割することにより得られるデータ部品Ｄ１～Ｄ４がＩＰＦＳに保存されている。また、各参加ノード１～４は、データ提供者１１から図６に示すアドレスリストを受信している。

【００５３】

データ取得者１２がデータ取得要求トランザクションを生成すると、マイナー１３は、そのトランザクションを含むブロックに対してマイニングを実行する。このマイニングによりデータ取得要求トランザクションが検証される。そして、検証結果は各参加ノードに送信される。

【００５４】

参加ノード１～４は、データ取得者１２のアクセス権を確認すると、自分の秘密鍵を用いた復号処理によりアドレスを取得してデータ取得者１２に送信する。データ取得者１２は、参加ノード１～４から受信したアドレスからデータ部品Ｄ１～Ｄ４を取得し、データＤを再生する。

【００５５】

ここで、図３に示す通信方法と第１の実施形態の通信方法とを比較する。図３に示す通信方法では、対象トランザクションを含むブロックの後ろに所定数（実施例では、６個）

のブロックが結合されたときに合意が形成され、対象トランザクションの実行が可能になる。このため、対象トランザクションが生成されたときからそのトランザクションが実行されるまでの時間が長くなることがある。

【００５６】

これに対して、第１の実施形態の通信方法においては、複数の参加ノードが暗号化アドレスの復号を行い、所定数以上のアドレスが得られたときに、データ取得者１２はデータを取得できる。この方式においては、ブロックチェーンの合意は、実施的に、所定数の参加ノードにより形成されることになる。ここで、シャミアの秘密分散法でＮ個のデータ部品に分割されたデータが、Ｋ個のデータ部品から再生可能であるときは、上記所定数はＫである。この場合、データ取得者により生成されるデータ取得要求トランザクションに対する合意は、そのトランザクションがマイナーにより検証された後、Ｋ個の参加ノードがデータ取得者のアクセス権を確認することで実現される。また、複数の参加ノードによる復号処理は、実質的に並列に実行される。よって、図３に示す通信方法と比較すると、第１の実施形態の通信方法においては、対象トランザクションが生成されたときからそのトランザクションが実行されるまでの時間が短縮される。

【００５７】

図１４は、データ登録手続の一例を示すフローチャートである。このフローチャートの処理は、データ提供者１１により実行される。

【００５８】

Ｓ１において、データ提供者１１は、シャミアの秘密分散法でデータを分割して複数のデータ部品を生成する。Ｓ２において、データ提供者１１は、複数のデータ部品をＩＰＦＳに登録する。Ｓ３において、データ提供者１１は、複数のデータ部品が保存された記憶領域のアドレスを取得する。Ｓ４において、データ提供者１１は、復号処理を実行すべき複数の参加ノードを選択する。図４～図１３に示す例では、参加ノード１～４が選択される。Ｓ５において、データ提供者１１は、Ｓ４で選択した複数の参加ノードの公開鍵でそれぞれ対応するアドレスを暗号化する。図４～図１３に示す例では、参加ノード１～４の公開鍵でそれぞれアドレスＡＤＤ１～ＡＤＤ４が暗号化される。

【００５９】

Ｓ６において、データ提供者１１は、Ｓ５で得られた複数の暗号化アドレスを含むアドレスリストを作成する。なお、アドレスリストは、図６に示すように、データにアクセスする権利を有する参加ノードを表すアクセス権情報、および暗号化アドレスを復号する参加ノードを表す復号ノードリストを含む。そして、Ｓ７において、データ提供者１１は、アドレスリストを各参加ノードに送信する。すなわち、アドレスリストがブロックチェーン上に公開される。

【００６０】

図１５は、データ取得手続における参加ノードの処理の一例を示すフローチャートである。なお、各参加ノードは、図１４に示すデータ登録手続で生成されるアドレスリストを受信しているものとする。

【００６１】

Ｓ１１において、参加ノードは、データ取得者からデータ取得要求トランザクションを受信する。Ｓ１２において、参加ノードは、アドレスリストのアクセス権情報を参照し、データ取得要求トランザクションの送信元ノードがアクセス権を有しているか否かを判定する。なお、参加ノードは、データ取得要求トランザクションを含むブロックがマイナーにより検証された後にＳ１２の処理を実行するようにしてもよい。

【００６２】

データ取得要求トランザクションの送信元ノードがアクセス権を有しているときは、参加ノードは、Ｓ１３において、自ノードがアドレスリストにより復号ノードとして指定されているか否かを判定する。自ノードが復号ノードとして指定されているときは、参加ノードは、Ｓ１４において、アドレスリストに設定されている暗号化アドレスを、自分の秘密鍵で復号する。そして、Ｓ１５において、参加ノードは、復号により得られたアドレス

をデータ取得要求トランザクションの送信元ノードに送信する。

【００６３】

図１６は、データ取得者の処理の一例を示すフローチャートである。なお、図１４に示すデータ登録手続は、先に完了しているものとする。

【００６４】

Ｓ２１において、データ取得者１２は、データ取得要求トランザクションを各参加ノードに送信する。この後、データ取得者１２は、データ取得要求トランザクションに対する応答を待ち受ける。すなわち、データ取得者１２は、取得しようとするデータが格納されている記憶領域のアドレスの送信を待ち受ける。

【００６５】

Ｓ２２において、データ取得者１２は、所定数の参加ノードからアドレスを受信したか否かを判定する。なお、シャミアの秘密分散法でＮ個のデータ部品に分割されたデータがＫ個のデータ部品から再生可能であるときは、所定数はＫである。所定数の参加ノードからアドレスを受信すると、データ取得者１２は、Ｓ２３において、各アドレスからデータ部品を取得する。そして、Ｓ２４において、データ取得者１２は、所定数のデータ部品からデータを再生する。

【００６６】

なお、図１４～図１６に示すフローチャートは、１つの実施例であり、本発明はこの手順に限定されるものではない。例えば、データ提供者１１は、データＤを分割する前に、データＤを参加ノード（データ取得者）１２の公開鍵で暗号化してもよい。この場合、暗号化されたデータＤがシャミアの秘密分散法で分割されてＩＰＦＳに登録される。データ取得者１２は、データ部品Ｄ１～Ｄ４から暗号化されたデータＤを再生した後、データ取得者１２の秘密鍵でデータＤの暗号を解除する。これにより、データ取得者１２はデータＤを取得する。

【００６７】

或いは、データ提供者１１は、データＤを分割する前に、データ提供者１１およびデータ取得者１２が使用する共通鍵でデータＤを暗号化してもよい。この場合、データ提供者１１は、その共通鍵をデータ取得者１２の公開鍵で暗号化してデータ取得者１２に送信する。データ取得者１２は、暗号化された共通鍵を受信し、データ取得者１２の秘密鍵でその共通鍵を復号する。そして、データ取得者１２は、データ部品Ｄ１～Ｄ４から暗号化されたデータＤを再生した後、復号後の共通鍵でデータＤの暗号を解除する。これにより、データ取得者１２はデータＤを取得する。

【００６８】

図１７は、各ノードに実装されるコンピュータのハードウェア構成の一例を示す。このコンピュータ３００は、プロセッサ３０１、メモリ３０２、記憶装置３０３、Ｉ／Ｏデバイス３０４、記録媒体デバイス３０５、通信インタフェース３０６を備える。なお、参加ノード、データ提供者、データ取得者、マイナーは、それぞれ図１７に示すコンピュータにより実現され得る。

【００６９】

プロセッサ３０１は、記憶装置３０３に格納されている通信プログラムを実行することにより、データ登録手続およびデータ取得手続を実現することができる。なお、コンピュータ３００がデータ提供者として動作するときは、プロセッサ３０１は、図１４に示すフローチャートの処理を記述した通信プログラムを実行する。コンピュータ３００が参加ノードとして動作するときは、プロセッサ３０１は、図１５に示すフローチャートの処理を記述した通信プログラムを実行する。コンピュータ３００がデータ取得者として動作するときは、プロセッサ３０１は、図１６に示すフローチャートの処理を記述した通信プログラムを実行する。

【００７０】

メモリ３０２は、例えば半導体メモリであり、プロセッサ３０１の作業領域として使用される。記憶装置３０３は、コンピュータ３００内に実装されていてもよいし、コンピュ

ータ３００に接続されていてもよい。Ｉ／Ｏデバイス３０４は、ユーザまたはネットワーク管理者の指示を受け付ける。また、Ｉ／Ｏデバイス３０４は、プロセッサ３０１による処理結果を出力する。記録媒体デバイス３０５は、可搬型記録媒体３０７に記録されている信号を読み取る。なお、上述した通信プログラムは、可搬型記録媒体３０７に記録されていてもよい。通信インタフェース３０６は、ネットワークとの間のインタフェースを提供する。

【００７１】

＜第２の実施形態＞

図１８は、第２の実施形態におけるデータ登録手続の一例を示す。なお、通信システム１００の構成は、第１の実施形態および第２の実施形態において実質的に同じであるものとする。

【００７２】

第１の実施形態と同様に、第２の実施形態においても、データ提供者１１は、データＤをシャミアの秘密分散法でデータ部品Ｄ１～Ｄ４に分割する。ただし、第２の実施形態においては、データ提供者１１は、データ部品Ｄ１～Ｄ４をそれぞれ参加ノード１～４に送信する。すなわち、参加ノード１はデータ部品Ｄ１を受信し、参加ノード２はデータ部品Ｄ２を受信し、参加ノード３はデータ部品Ｄ３を受信し、参加ノード４はデータ部品Ｄ４を受信する。また、データ提供者１１は、データＤのアクセス権を表すアクセス権情報を各参加ノードに送信する。この実施例では、アクセス権情報は、参加ノード（データ取得者）１２に対してデータＤへのアクセスを許可する。

【００７３】

データ取得手続において、データ取得者１２は、第１の実施形態と同様に、データ取得要求トランザクションを生成する。このデータ取得要求トランザクションは、データＤの取得を要求するメッセージを含む。そして、このデータ取得要求トランザクションは、全参加ノードに送信される。

【００７４】

マイナー１３は、第１の実施形態と同様に、データ取得者１２から送信されたデータ取得要求トランザクションを含むブロックを検証する。そして、マイナー１３は、このブロックの検証結果を全参加ノードに送信する。すなわち、各参加ノード１～４は、マイナー１３から検証結果を受信する。

【００７５】

各参加ノード１～４は、データ取得要求トランザクションを含むブロックについての検証結果をマイナー１３から受信すると、第１の実施形態と同様に、データ取得者１２から送信されたデータ取得要求トランザクションのアクセス権を確認する。このとき、各参加ノード１～４は、データ提供者１１から先に受信しているアクセス権情報を参照する。この実施例では、参加ノード（データ取得者）１２に対してデータＤへのアクセス権が与えられている。したがって、各参加ノード１～４は、受信したデータ取得要求トランザクションに対応する処理を実行する。

【００７６】

具体的には、各参加ノード１～４は、データ提供者１１から先に受信しているデータ部品をデータ取得者１２に送信する。すなわち、参加ノード１～４は、データ部品Ｄ１～Ｄ４をデータ取得者１２に送信する。そして、データ取得者１２は、参加ノード１～４から受信するデータ部品Ｄ１～Ｄ４からデータＤを再生する。

【００７７】

＜第３の実施形態＞

図１９は、第３の実施形態におけるデータ登録手続の一例を示す。なお、通信システム１００の構成は、第１の実施形態および第３の実施形態において実質的に同じであるものとする。

【００７８】

第１の実施形態と同様に、第３の実施形態においても、データ提供者１１は、データＤ

をシャミアの秘密分散法でデータ部品Ｄ１～Ｄ４に分割する。ただし、第３の実施形態においては、データ提供者１１は、データ部品Ｄ１～Ｄ４をそれぞれ参加ノード１～４の公開鍵で暗号化する。すなわち、データ部品Ｄ１は参加ノード１の公開鍵で暗号化され、データ部品Ｄ２は参加ノード２の公開鍵で暗号化され、データ部品Ｄ３は参加ノード３の公開鍵で暗号化され、データ部品Ｄ４は参加ノード４の公開鍵で暗号化される。そして、データ提供者１１は、暗号化されたデータ部品Ｄ１～Ｄ４を含むデータ部品リストを生成する。

【００７９】

データ部品リストは、図２０に示すように、アクセス権情報、復号ノードリスト、暗号化データ部品を含む。なお、アクセス権情報および復号ノードリストは、第１の実施形態および第３の実施形態において実質的に同じなので説明を省略する。

【００８０】

データ提供者１１は、データ部品リストをブロックチェーン上で公開する。すなわち、データ提供者１１は、データ部品リストを全参加ノードに送信する。したがって、各参加ノード１～４はデータ部品リストを受信する。

【００８１】

データ取得手続において、データ取得者１２は、第１の実施形態と同様に、データ取得要求トランザクションを生成する。このデータ取得要求トランザクションは、データＤの取得を要求するメッセージを含む。そして、このデータ取得要求トランザクションは、全参加ノードに送信される。

【００８２】

マイナー１３は、第１の実施形態と同様に、データ取得者１２から送信されたデータ取得要求トランザクションを含むブロックを検証する。そして、マイナー１３は、このブロックの検証結果を全参加ノードに送信する。すなわち、各参加ノード１～４は、マイナー１３から検証結果を受信する。

【００８３】

各参加ノード１～４は、データ取得要求トランザクションを含むブロックについての検証結果をマイナー１３から受信すると、第１の実施形態と同様に、データ取得者１２から送信されたデータ取得要求トランザクションのアクセス権を確認する。このとき、各参加ノード１～４は、データ提供者１１から先に受信しているデータ部品リスト内のアクセス権情報を参照する。この実施例では、参加ノード（データ取得者）１２に対してデータＤへのアクセス権が与えられている。したがって、各参加ノード１～４は、受信したデータ取得要求トランザクションに対応する処理を実行する。

【００８４】

参加ノード１は、参加ノード１の秘密鍵を用いて４個の暗号化データ部品Ｄ１～Ｄ４に対して復号処理を行う。ここで、暗号化データ部品Ｄ１～Ｄ４は、それぞれ参加ノード１～４の公開鍵で暗号化されている。したがって、参加ノード１の秘密鍵で復号処理を実行すると、暗号化データ部品Ｄ１に対する復号は成功するが、暗号化データ部品Ｄ２～Ｄ４に対する復号は失敗する。すなわち、参加ノード１は、データ部品Ｄ１を取得できるが、データ部品Ｄ２～Ｄ４を取得できない。

【００８５】

同様に、参加ノード２は、参加ノード２の秘密鍵を用いて暗号化データ部品Ｄ１～Ｄ４に対して復号処理を行い、データ部品Ｄ２を取得する。参加ノード３は、参加ノード３の秘密鍵を用いて暗号化データ部品Ｄ１～Ｄ４に対して復号処理を行い、データ部品Ｄ３を取得する。参加ノード４は、参加ノード４の秘密鍵を用いて暗号化データ部品Ｄ１～Ｄ４に対して復号処理を行い、データ部品Ｄ４を取得する。この後、参加ノード１～４は、それぞれデータ部品Ｄ１～Ｄ４をデータ取得者１２に送信する。そして、データ取得者１２は、参加ノード１～４から受信するデータ部品Ｄ１～Ｄ４からデータＤを再生する。

【符号の説明】

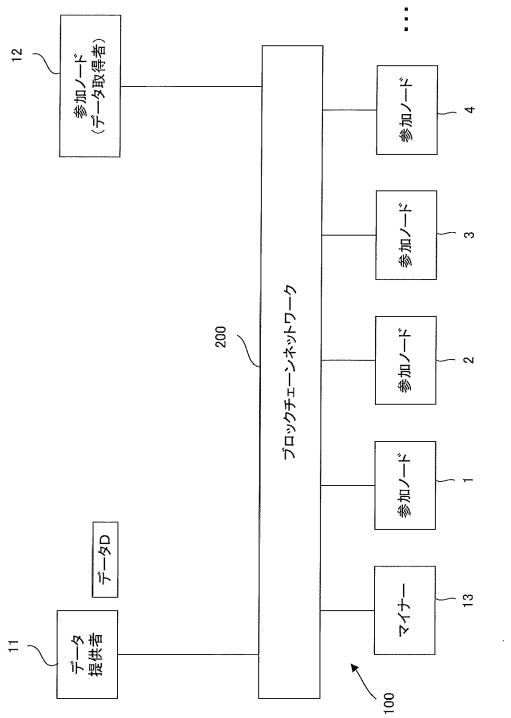
【００８６】

１～４　参加ノード
１１　データ提供者
１２　参加ノード（データ取得者）
１３　マイナー
１００　通信システム
２００　ブロックチェーンネットワーク
３０１　プロセッサ

【図面】

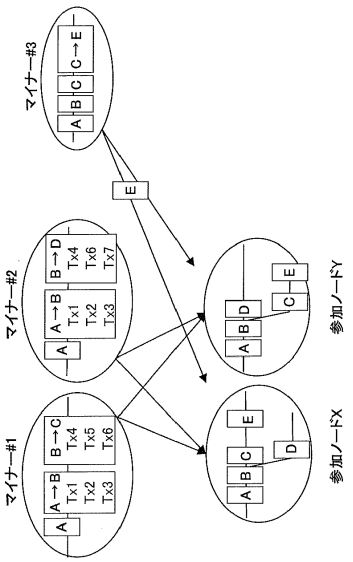
【図１】

本発明の実施形態に係わる通信システムの一例を示す図



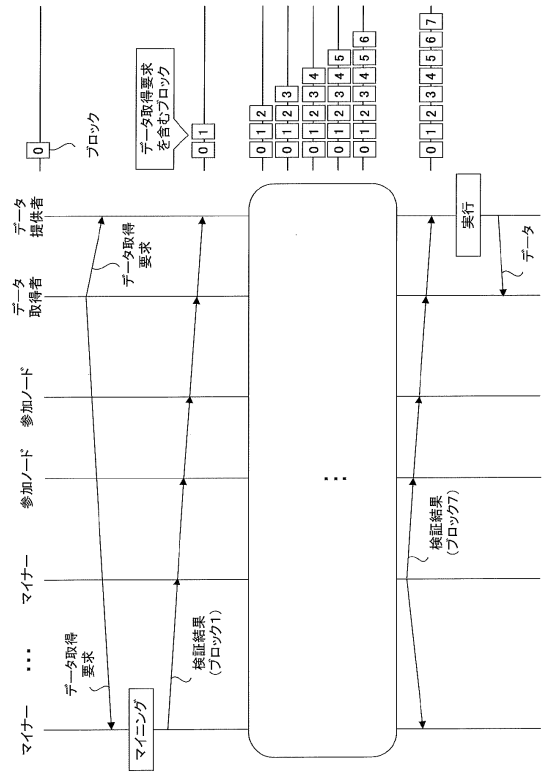
【図２】

ブロックの検証および確定について説明する図



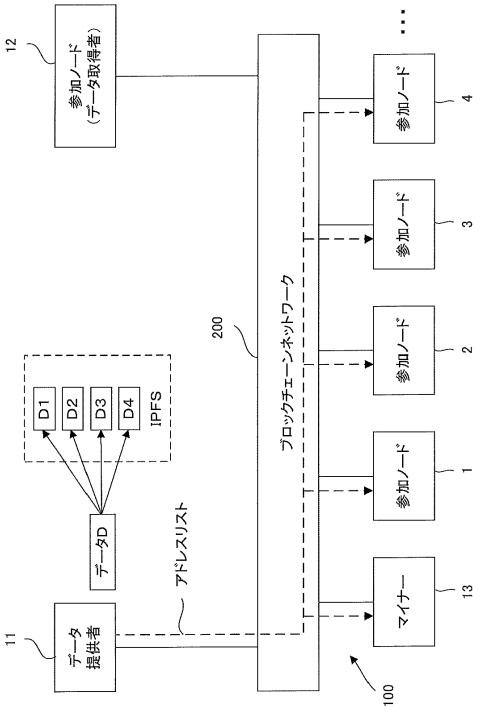
【図３】

PoWで合意形成が行われるケースにおける
データ送信のシーケンスの一例を示す図



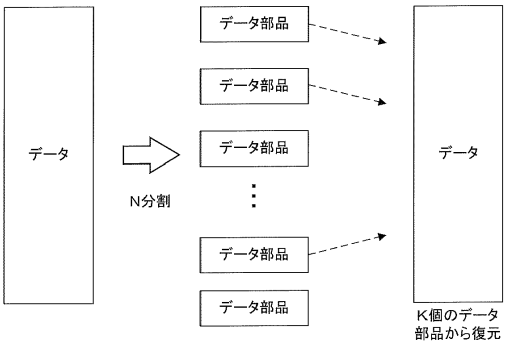
【図４】

データ登録手続の一例を示す図



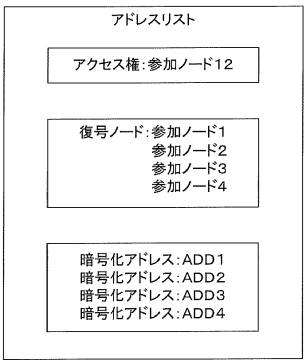
【図５】

シャミアの秘密分散法について説明する図



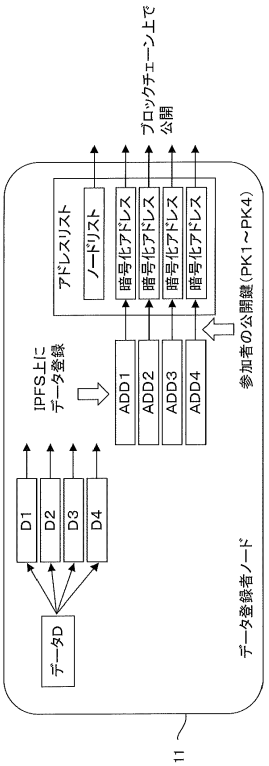
【図６】

アドレスリストの一例を示す図



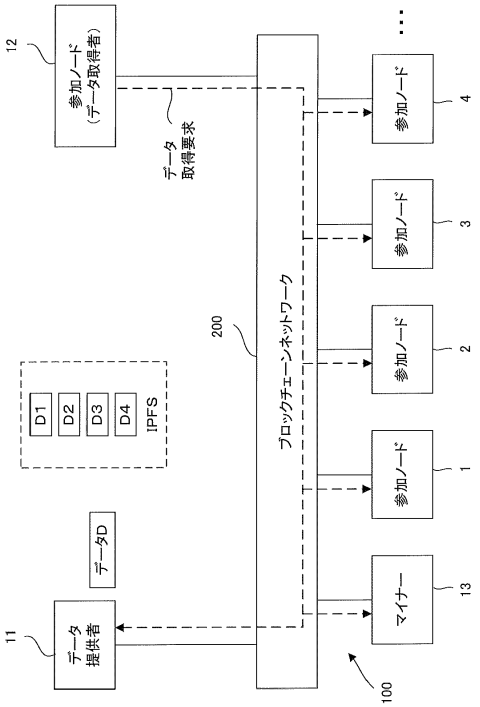
【図７】

データ部品および暗号化アドレスを
生成する手順の一例を示す図



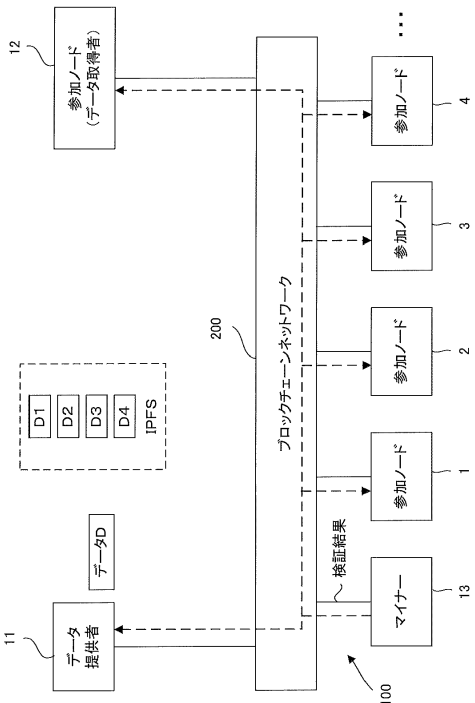
【図８】

データ取得手続の一例を示す図（その1）



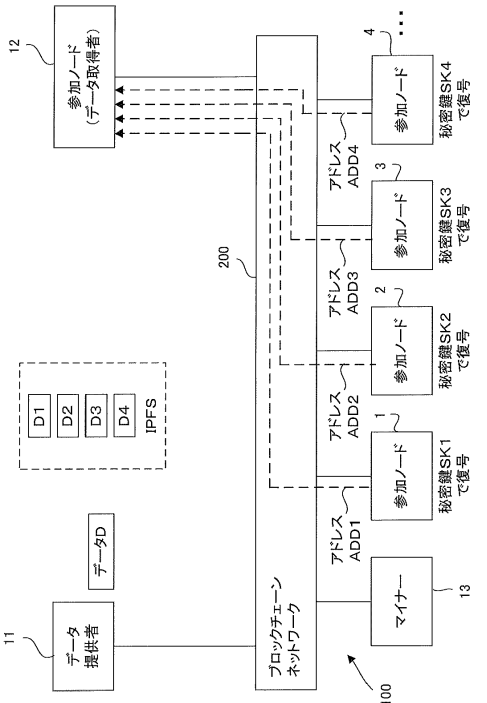
【図９】

データ取得手続の一例を示す図（その2）



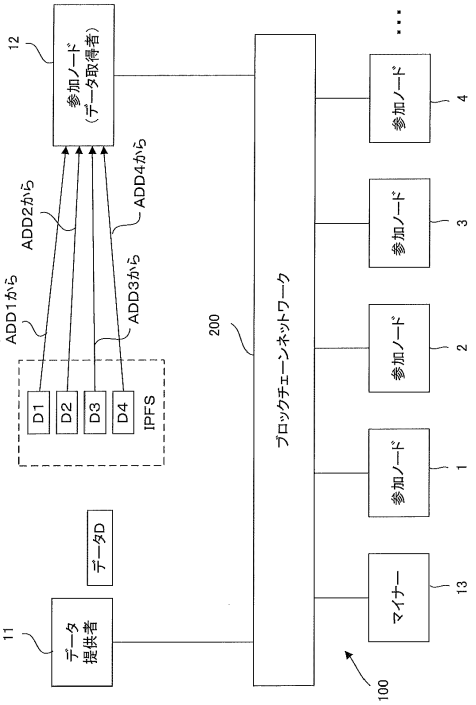
【図１０】

データ取得手続の一例を示す図（その3）



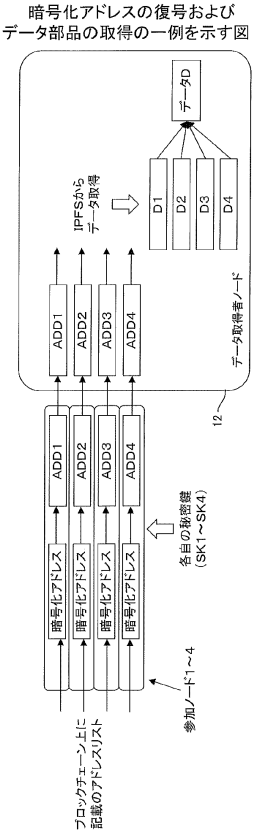
【図１１】

データ取得手続の一例を示す図（その4）



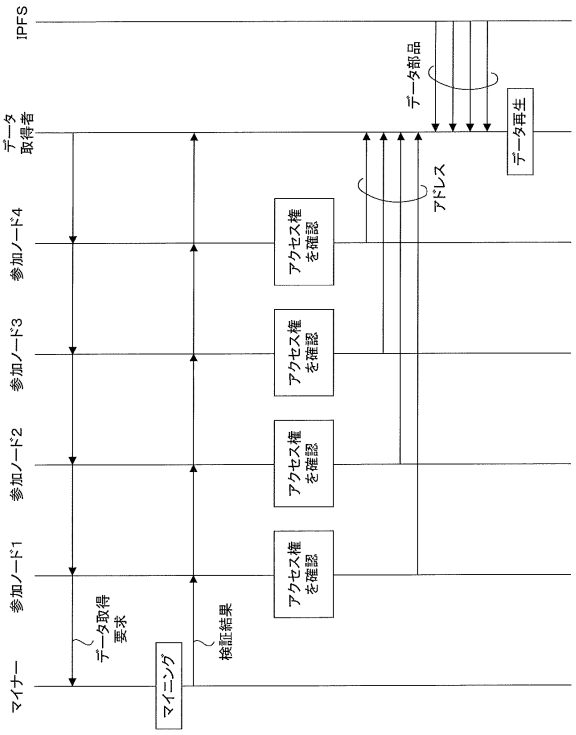
【図１２】

暗号化アドレスの復号および
データ部品の取得の一例を示す図



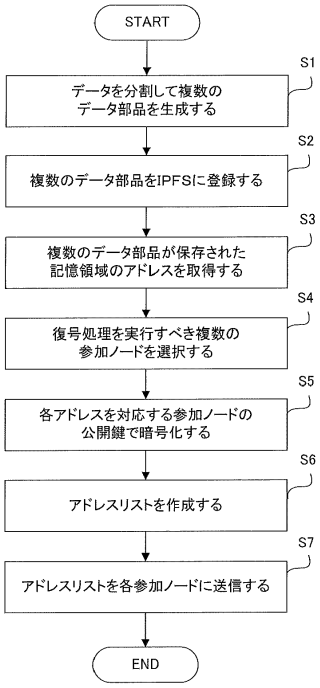
【図１３】

データ取得手続のシーケンスの一例を示す図



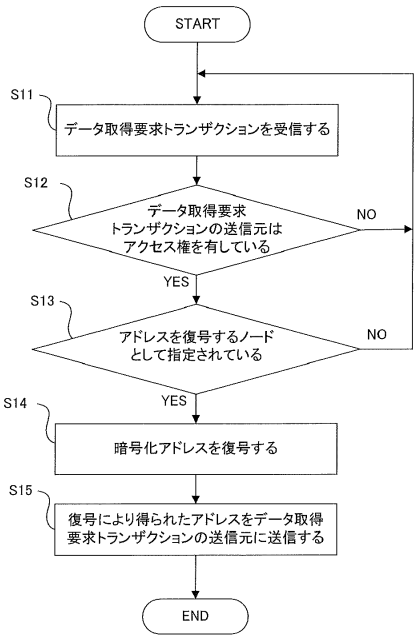
【図１４】

データ登録手続の一例を示すフローチャート



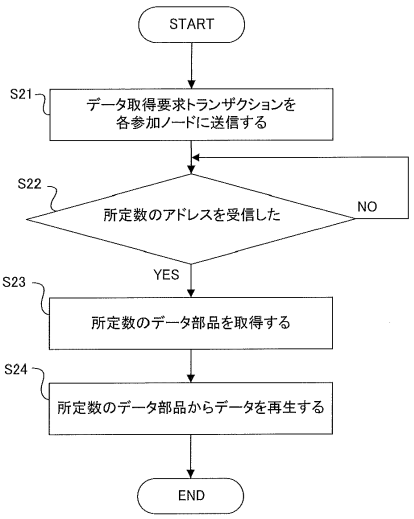
【図１５】

データ取得手続における参加ノードの
処理の一例を示すフローチャート



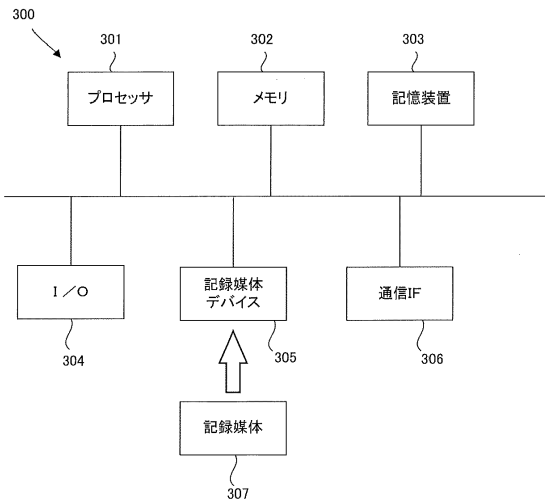
【図１６】

データ取得者の処理の一例を示すフローチャート



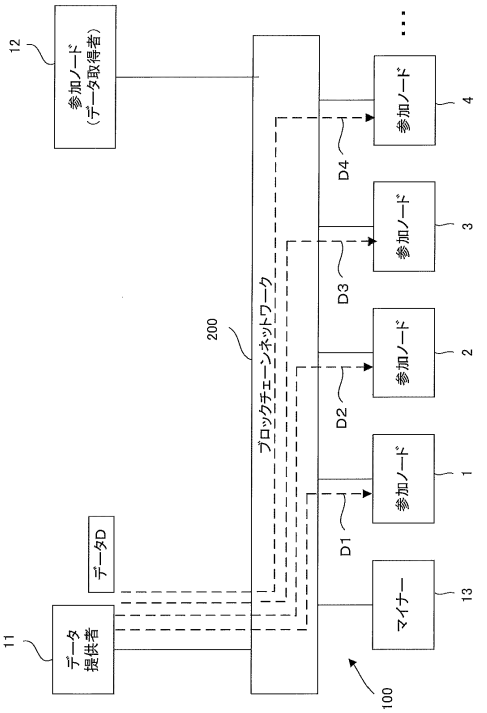
【図１７】

各ノードに実装されるコンピュータの
ハードウェア構成の一例を示す図



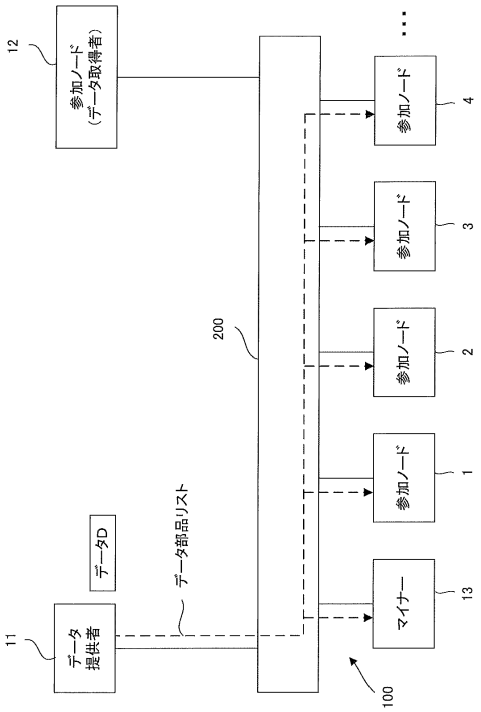
【図１８】

第2の実施形態におけるデータ登録手続の一例を示す図



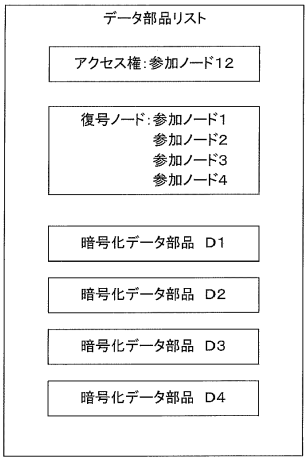
【図１９】

第3の実施形態におけるデータ登録手続の一例を示す図



【図２０】

データ部品リストの一例を示す図



フロントページの続き

審査官　金沢 史明

(56)参考文献　特開２００９－１０３７７４（ＪＰ，Ａ）
特開２０１５－０７９３４６（ＪＰ，Ａ）
特開２００８－１０３９３６（ＪＰ，Ａ）
特開２０１６－２１２２９３（ＪＰ，Ａ）
福光 正幸，他，秘密分散法と匿名通信による秘匿性に優れたP2P型ストレージ技術の提案，情報処理学会研究報告，情報処理学会，2016年02月25日，Vol. 2016-CSEC-72，No. 6，pp. 1-8

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／０８
Ｈ０４Ｌ　９／３２
Ｇ０９Ｃ　１／００
Ｇ０６Ｆ　２１／６０－２１／６２