(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第6671617号
(P6671617)
(45)発行日　令和2年3月25日(2020.3.25)　(24)登録日　令和2年3月6日(2020.3.6)

(51)Int.Cl.　F I
G06F 16/182 (2019.01)　G06F 16/182

請求項の数 12　(全 36 頁)

(21)出願番号　特願2019-223803(P2019-223803)
(22)出願日　令和1年12月11日(2019.12.11)
審査請求日　令和1年12月11日(2019.12.11)

早期審査対象出願

(73)特許権者　519442829
株式会社ブルーキャッスル
東京都港区新橋６－５－３　山田屋ビル４Ｆ
(74)代理人　100134430
弁理士　加藤　卓士
(72)発明者　李　晨
東京都港区新橋６－５－３　山田屋ビル４Ｆ　株式会社ブルーキャッスル内
(72)発明者　曲　衛東
東京都港区新橋６－５－３　山田屋ビル４Ｆ　株式会社ブルーキャッスル内

審査官　鹿野　博嗣

最終頁に続く

(54)【発明の名称】ブロックチェーン技術と分散ストレージ技術とにより実現した分散型ストレージプラットフォームおよびアプリケーションプログラム

(57)【特許請求の範囲】
【請求項１】
ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、
前記複数の保存用ノードの識別情報を含むロケーションリストをブロックチェーン化しつつ保存する検索用ノードを複数含む検索用ネットワークと、
前記ファイルを複数の部分データに分割し、前記複数の部分データのそれぞれを前記複数の保存用ノードに含まれる少なくとも２つの保存用ノードに送信して保存させる保存処理部と、
を備え、
前記検索用ノードは、前記部分データを保存した前記保存用ノードの識別情報を用いて、前記ロケーションリストを更新する更新処理部を備えた情報処理システム。
【請求項２】
前記更新処理部は、さらに、分散保存したファイルを識別するファイル識別情報と、前記部分データを識別する部分データ識別情報とを用いて、前記ロケーションリストを更新する請求項１に記載の情報処理システム。
【請求項３】
前記保存処理部は、前記複数の保存用ノードから、各々の保存用ノードの信頼性を考慮して前記少なくとも２つの保存用ノードを選択する請求項１または２に記載の情報処理システム。
【請求項４】

前記検索用ノードは、前記ロケーションリストに基づいて、前記複数の部分データのそれぞれが保存されている前記少なくとも２つの保存用ノードを検索する検索処理部をさらに備え、
前記少なくとも２つの保存用ノードから前記複数の部分データのそれぞれを取得し、前記複数の部分データを合成して前記ファイルを復元する復元処理部をさらに備えた請求項１乃至３のいずれか１項に記載の情報処理システム。
【請求項５】
前記保存処理部は、前記ファイルを暗号化して得られた暗号化ファイルを前記複数の部分データに分割し、前記複数の部分データのそれぞれを前記少なくとも２つの保存用ノードに保存させる請求項４に記載の情報処理システム。
【請求項６】
前記複数の保存用ノードに対して報酬を提供する報酬提供部をさらに備え、
前記報酬提供部は、
前記部分データを保存した前記少なくとも２つの保存用ノードに対して第１報酬を提供する第１報酬提供部と、
前記復元処理部が前記ファイルを復元した場合に、前記ファイルの一部である前記部分データを保存していた前記少なくとも２つの保存用ノードに対して、第２報酬を提供する第２報酬提供部と、
を有する請求項４または５に記載の情報処理システム。
【請求項７】
前記第２報酬は前記第１報酬より多い請求項６に記載の情報処理システム。
【請求項８】
前記保存処理部および前記復元処理部の少なくともいずれか１つを実現するクライアント端末をさらに備えた請求項４に記載の情報処理システム。
【請求項９】
ファイルの分割により生成された複数の部分データを保存するための複数の保存用ノードを含む保存用ネットワークと、
前記複数の保存用ノードの識別情報を含むロケーションリストをブロックチェーン化しつつ保存する検索用ノードを複数含む検索用ネットワークと、
前記複数の部分データを前記保存用ノードから取得し、前記複数の部分データを合成して前記ファイルを復元する復元処理部と、
を備え、
前記保存用ネットワークは、ファイルの分割により生成された前記複数の部分データを、前記複数の保存用ノードに保存すると共に、前記ファイルの分割により生成された前記複数の部分データのそれぞれを、少なくとも２つの保存用ノードに分けて保存し、
前記検索用ノードは、前記ロケーションリストに基づいて、前記複数の部分データが保存されている前記保存用ノードを検索する検索処理部を備えた情報処理システム。
【請求項１０】
ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、
前記複数の保存用ノードの識別情報を含むロケーションリストをブロックチェーン化しつつ保存する検索用ノードを複数含む検索用ネットワークと、
を備える情報処理システムの情報処理方法であって、
前記ファイルを複数の部分データに分割し、前記複数の部分データのそれぞれを前記複数の保存用ノードに含まれる少なくとも２つの保存用ノードに送信して保存させる保存処理ステップと、
前記部分データを保存した前記保存用ノードの識別情報を用いて、前記ロケーションリストを更新する更新処理ステップと、
を含む情報処理方法。
【請求項１１】
ファイルの分割により生成された複数の部分データを保存するための複数の保存用ノー

ドを含む保存用ネットワークと、
前記複数の保存用ノードの識別情報を含むロケーションリストをブロックチェーン化しつつ保存する検索用ノードを複数含む検索用ネットワークと、
を備える情報処理システムの情報処理方法であって、
前記保存用ネットワークは、ファイルの分割により生成された前記複数の部分データを、前記複数の保存用ノードに保存すると共に、前記ファイルの分割により生成された前記複数の部分データのそれぞれを、少なくとも２つの保存用ノードに分けて保存し、
前記ロケーションリストに基づいて、前記複数の部分データが保存されている前記保存用ノードを検索する検索処理ステップと、
前記複数の部分データを前記保存用ノードから取得し、前記複数の部分データを合成して前記ファイルを復元する復元処理ステップと、
を含む情報処理方法。
【請求項１２】
ファイルの分割により生成された複数の部分データのそれぞれを保存する、少なくとも２つの保存用ノードから、前記複数の部分データを取得して合成するためのアプリケーションプログラムであって、
ファイルのハッシュ値であるファイルハッシュを取得するハッシュ取得ステップと、
前記ファイルハッシュを検索用ノードに送信し、対応するファイルリストを検索させるファイルハッシュ送信ステップと、
受信した前記ファイルハッシュに対応する前記ファイルリストを、前記検索用ノードから取得するファイルリスト取得ステップと、
前記ファイルリストが示す前記複数の部分データを、前記ファイルリストに指定される、前記保存用ノードから取得する部分データ取得ステップと、
前記保存用ノードから取得した前記複数の部分データを合成して、前記ファイルを復元する復元処理ステップと、
をコンピュータに実行させるアプリケーションプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ブロックチェーン技術と分散ストレージ技術とにより実現した分散型ストレージプラットフォームおよびアプリケーションプログラムに関する。
【背景技術】
【０００２】
上記技術分野において、特許文献１には、データの分散保存における冗長性の技術が開示されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】米国特許第１０１２７１０８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、上記文献に記載の技術では、中央集中型のデータセンタを前提としており、安全性が十分とは言えなかった。複数のデータセンタが同時にダウンしてしまうと、データが消えてしまうことがあった。
【０００５】
本発明の目的は、上述の課題を解決する技術を提供することにある。
【課題を解決するための手段】
【０００６】
上記目的を達成するため、本発明に係る情報処理システムは、

ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、
前記複数の保存用ノードの識別情報を含むロケーションリストをブロックチェーン化しつつ保存する検索用ノードを複数含む検索用ネットワークと、
前記ファイルを複数の部分データに分割し、前記複数の部分データのそれぞれを前記複数の保存用ノードに含まれる少なくとも２つの保存用ノードに送信して保存させる保存処理部と、
を備え、
前記検索用ノードは、前記部分データを保存した前記保存用ノードの識別情報を用いて、前記ロケーションリストを更新する更新処理部を備えた。

【０００７】

上記目的を達成するため、本発明に係る情報処理システムは、
ファイルの分割により生成された複数の部分データを保存するための複数の保存用ノードを含む保存用ネットワークと、
前記複数の保存用ノードの識別情報を含むロケーションリストをブロックチェーン化しつつ保存する検索用ノードを複数含む検索用ネットワークと、
前記複数の部分データを前記保存用ノードから取得し、前記複数の部分データを合成して前記ファイルを復元する復元処理部と、
を備え、
前記保存用ネットワークは、ファイルの分割により生成された前記複数の部分データを、前記複数の保存用ノードに保存すると共に、前記ファイルの分割により生成された前記複数の部分データのそれぞれを、少なくとも２つの保存用ノードに分けて保存し、
前記検索用ノードは、前記ロケーションリストに基づいて、前記複数の部分データが保存されている前記保存用ノードを検索する検索処理部を備えた。

【０００８】

上記目的を達成するため、本発明に係る情報処理方法は、
ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、
前記複数の保存用ノードの識別情報を含むロケーションリストをブロックチェーン化しつつ保存する検索用ノードを複数含む検索用ネットワークと、
を備える情報処理システムの情報処理方法であって、
前記ファイルを複数の部分データに分割し、前記複数の部分データのそれぞれを前記複数の保存用ノードに含まれる少なくとも２つの保存用ノードに送信して保存させる保存処理ステップと、
前記部分データを保存した前記保存用ノードの識別情報を用いて、前記ロケーションリストを更新する更新処理ステップと、
を含む。

【０００９】

上記目的を達成するため、本発明に係る情報処理方法は、
ファイルの分割により生成された複数の部分データを保存するための複数の保存用ノードを含む保存用ネットワークと、
前記複数の保存用ノードの識別情報を含むロケーションリストをブロックチェーン化しつつ保存する検索用ノードを複数含む検索用ネットワークと、
を備える情報処理システムの情報処理方法であって、
前記保存用ネットワークは、ファイルの分割により生成された前記複数の部分データを、前記複数の保存用ノードに保存すると共に、前記ファイルの分割により生成された前記複数の部分データのそれぞれを、少なくとも２つの保存用ノードに分けて保存し、
前記ロケーションリストに基づいて、前記複数の部分データが保存されている前記保存用ノードを検索する検索処理ステップと、
前記複数の部分データを前記保存用ノードから取得し、前記複数の部分データを合成して前記ファイルを復元する復元処理ステップと、
を含む。

【００１１】
上記目的を達成するため、本発明に係るアプリケーションプログラムは、
ファイルの分割により生成された複数の部分データのそれぞれを保存する、少なくとも２つの保存用ノードから、前記複数の部分データを取得して合成するためのアプリケーションプログラムであって、
ファイルのハッシュ値であるファイルハッシュを取得するハッシュ取得ステップと、
前記ファイルハッシュを検索用ノードに送信し、対応するファイルリストを検索させるファイルハッシュ送信ステップと、
受信した前記ファイルハッシュに対応する前記ファイルリストを、前記検索用ノードから取得するファイルリスト取得ステップと、
前記ファイルリストが示す前記複数の部分データを、前記ファイルリストに指定される、前記保存用ノードから取得する部分データ取得ステップと、
前記保存用ノードから取得した前記複数の部分データを合成して、前記ファイルを復元する復元処理ステップと、
をコンピュータに実行させる。
【発明の効果】
【００１２】
本願発明によれば、高い安全性を担保しつつ、小規模ストレージの集合により大規模データサーバと同様の機能を実現することができる。
【図面の簡単な説明】
【００１３】
【図１Ａ】本発明の第１実施形態に係る情報処理システムの構成を示すブロック図である。
【図１Ｂ】本発明の第２実施形態に係る情報処理システムの構成を示すブロック図である。
【図２】本発明の第３実施形態に係る情報処理システムの構成を示すブロック図である。
【図３Ａ】本発明の第３実施形態に係る情報処理システムの、ファイルを分散して保存する動作手順を示す図である。
【図３Ｂ】本発明の第３実施形態に係る情報処理システムの、ファイルを合成して再現する動作手順を示す図である。
【図４】本発明の第３実施形態に係る情報処理システムの、保存用ノードまたは検索用ノードに参加する動作手順を示す図である。
【図５】本発明の第３実施形態に係るクライアントアプリケーションの構成を示す図である。
【図６】本発明の第３実施形態に係るクライアントアプリケーションを含むクライアント端末のハードウェア構成を示すブロック図である。
【図７】本発明の第３実施形態に係るクライアントアプリケーションの処理手順を示すフローチャートである。
【図８】本発明の第３実施形態に係るファイル保存処理部の機能構成を示すブロック図である。
【図９】本発明の第３実施形態に係るファイル保存処理部で使用するデータの構成を示す図である。
【図１０】本発明の第３実施形態に係るファイル保存処理部の処理手順を示すフローチャートである。
【図１１Ａ】本発明の第３実施形態に係るデータの分割処理の手順を示すフローチャートである。
【図１１Ｂ】本発明の第３実施形態に係る保存先ノードの選定処理の手順を示すフローチャートである。
【図１２】本発明の第３実施形態に係るリスト検索処理部の機能構成を示すブロック図である。

【図１３】本発明の第３実施形態に係るリスト検索処理部で使用するデータの構成を示す図である。
【図１４】本発明の第３実施形態に係るリスト検索処理部の処理手順を示すフローチャートである。
【図１５】本発明の第３実施形態に係るファイル取得処理部の機能構成を示すブロック図である。
【図１６】本発明の第３実施形態に係るファイル取得処理部で使用するデータの構成を示す図である。
【図１７】本発明の第３実施形態に係るデータ取得処理部の処理手順を示すフローチャートである。
【図１８】本発明の第３実施形態に係る報酬処理部の機能構成を示すブロック図である。
【図１９】本発明の第３実施形態に係る報酬処理部で使用するデータの構成を示す図である。
【図２０】本発明の第３実施形態に係る報酬処理部の処理手順を示すフローチャートである。
【図２１】本発明の第３実施形態に係る保存用ノードの機能構成を示すブロック図である。
【図２２】本発明の第３実施形態に係る保存用ノードの処理手順を示すフローチャートである。
【図２３】本発明の第３実施形態に係る検索用ノードの機能構成を示すブロック図である。
【図２４】本発明の第３実施形態に係る検索用ノードの処理手順を示すフローチャートである。
【図２５】本発明の第３実施形態に係る保存用ノードまたは検索用ノードとなるクライアント装置のハードウェア構成を示すブロック図である。
【図２６】本発明の第４実施形態に係る情報処理システムの構成を示すブロック図である。
【図２７】本発明の第５実施形態に係る情報処理システムの構成を示すブロック図である。

【発明を実施するための形態】

【００１４】
以下に、図面を参照して、本発明の実施の形態について例示的に詳しく説明する。ただし、以下の実施の形態に記載されている構成要素は単なる例示であり、本発明の技術範囲をそれらのみに限定する趣旨のものではない。

【００１５】
［第１実施形態］
本発明の第１実施形態としての情報処理システム１１０について、図１Ａを用いて説明する。

【００１６】
図１Ａに示すように、情報処理システム１１０は、保存用ネットワーク１０１と、検索用ネットワーク１０２と、保存処理部１０３と、を含む。保存用ネットワーク１０１は、ファイル１３０を分散保存するための複数の保存用ノード１１１を含む。検索用ネットワーク１０２は、複数の保存用ノード１１１のロケーションを含むロケーションリスト１２２をブロックチェーン化しつつ保存する検索用ノード１２１を複数含む。保存処理部１０３は、ファイル１３０を複数の部分データ１３１～１３ｎに分割し、複数の部分データ１３１～１３ｎのそれぞれを複数の保存用ノード１１１に含まれる少なくとも２つの保存用ノードに送信して保存させる。更新処理部１２３は、検索用ノード１２１に含まれ、部分データを保存した保存用ノード１１１の識別情報を用いて、ロケーションリスト１２２を更新する。

【００１７】

本実施形態によれば、高い安全性を担保しつつ、小規模ストレージの集合により大規模データサーバと同様の機能を実現することができる。

【００１８】

［第２実施形態］

本発明の第２実施形態に係る情報処理システム１２０について図１Ｂを用いて説明する。

【００１９】

図１Ｂに示すように、情報処理システム１２０は、保存用ネットワーク１０１と、検索用ネットワーク１０５と、復元処理部１０４とを含む。検索用ネットワーク１０５は、複数の保存用ノードのロケーションを含むロケーションリスト１５２をブロックチェーン化しつつ保存する検索用ノード１５１を複数含む。また、各検索用ノード１５１は、検索処理部１５３を含む。検索処理部１５３は、ロケーションリスト１２２に基づいて、複数の部分データ１４１～１４ｎが保存されている保存用ノード１１１を検索する。復元処理部１０４は、保存用ノード１１１から複数の部分データ１４１～１４ｎを取得し、複数の部分データ１４１～１４ｎを合成してファイル１４０を復元する。

【００２０】

本実施形態によれば、高い安全性を担保しつつ、小規模ストレージの集合により大規模データサーバと同様の機能を実現することができる。

【００２１】

［第３実施形態］

本発明の第３実施形態に係る情報処理システム２００について図２以降を用いて説明する。

本実施形態の情報処理システム２００は、ファイルおよびその分割された部分データがハッシュ化（以下、ハッシュをHash、ハッシュ値をHash値と表す）されて、検索用ネットワークと保存用ネットワークとの独立した二層構造で管理される。そして、ファイルのアップロードでは、ファイルから分割した複数の部分データを、複数の保存用ノードから複数の部分データのそれぞれの保存先として選定した保存用ノードに保存させる。そして、複数の部分データをそれぞれ保存する選定された保存用ノードを示すロケーションリストをブロックチェーン化しつつ生成し、複数の検索用ノードに共有させる。一方、ファイルのダウンロードでは、複数の検索用ノードに共有されたロケーションリストをいずれか１つの検索用ノードから取得して、ファイルに対応するロケーションリストを検索する。そして、検索したロケーションリストに従って、ファイルから分割された複数の部分データをそれぞれ保存する複数の保存用ノードから取得し、複数の部分データを合成して取得対象のファイルを生成する。

【００２２】

ファイルをアップロードする際には、ファイルを暗号化し、暗号化されたファイルから分割した複数の部分データを保存先として選定した保存用ノードに保存させる。また、ファイルをダウンロードする際には、暗号化ファイルから分割された複数の部分データをそれぞれ保存する複数の保存用ノードから取得し、暗号化ファイルを構成する。そして、暗号化ファイルからファイルを復号する。なお、検索用ノードおよび保存用ノードは、ノードを識別するノード識別情報のHash値により識別されることが望ましい。

【００２３】

《情報処理システム》

以下、図２～図４に従って、本実施形態の情報処理システム２００の構成および動作について説明する。

【００２４】

（ブロック構成）

図２は、本実施形態に係る情報処理システム２００の構成を示すブロック図である。

【００２５】

情報処理システム２００は、保存用ネットワーク２０１と、検索用ネットワーク２０２

と、クライアント端末２０３とを有する。クライアント端末２０３は、ファイル保存処理、リスト検索処理およびファイル取得処理を実現するクライアントアプリケーション２３２を実行するよう構成されている。

【００２６】

保存用ネットワーク２０１は、Ｐ２Ｐ通信を行う複数の保存用ノード２１１を含む。複数の保存用ノード２１１のそれぞれは、クライアントアプリケーション２３２からのファイルの保存要求において、ファイルから分割された部分データを、ファイルHash（ファイルハッシュ）と部分Hash（部分ハッシュ）を検索キーとして保存する。また、複数の保存用ノード２１１は、クライアントアプリケーション２３２からのファイルの取得要求において、検索用ノード２２１がロケーションリストからファイルのHash値によって検索したファイルリストを含まれる部分Hashを用いて、部分データを検索して読出し、クライアント端末２０３に送信する。

【００２７】

検索用ネットワーク２０２は、Ｐ２Ｐ通信を行う複数の検索用ノード２２１を含む。検索用ノード２２１は、ファイルが複数の保存用ノード２１１に保存された場合に、そのファイルのHash値によって特定されたファイルリストを含むロケーションリストを生成して複数の検索用ノード２２１で共有する。また、検索用ノード２２１は、クライアント端末２０３からのファイルの取得要求において、最新のロケーションリストから、取得要求されたファイルに対応するファイルHashと部分Hashと保存用ノードＩＤとから構成されるファイルリストを検索して、クライアント端末２０３に提供する。

【００２８】

クライアントアプリケーション２３２は、ファイルの保存要求に対しては、ファイルを分割して部分データを部分Hashを検索キーとして、複数の保存用ノード２１１から選択された保存用ノードに保存する。部分データの保存が完了すると、保存用ノード２１１は、ファイルHashと部分Hashと部分データを保存した保存用ノードＩＤとを検索用ノード２２１に通知する。そして、検索用ノード２２１が、ファイルHashと、部分Hash値と、保存用ノードＩＤと、から構成されたファイルリストを生成して、ロケーションリストを更新する。更新されたロケーションリストは、全ての検索用ノード２２１で共有される。

【００２９】

クライアントアプリケーション２３２は、ファイルの取得要求に対しては、ファイルashを検索キーとして、近傍の検索用ノード２２１に送り、最新のロケーションリストに含まれるファイルのファイルリストを取得する。取得したファイルリストには、ファイルHashと、部分Hashと、保存用ノードＩＤと、が含まれている。クライアントアプリケーション２３２は、ファイルリストから抽出した部分Hashと保存用ノードＩＤとの組合せを用いて、部分データを保存用ノードから読出す。

【００３０】

以下、図３Ａ、図３Ｂおよび図４を参照して、情報処理システム２００の動作手順を示す。

【００３１】

（ファイルの保存手順）

図３Ａは、実施形態に係る情報処理システム２００の、ファイルを分散して保存する動作手順を示す図である。

【００３２】

ファイルの保存を要求するクライアント３０１は、クライアント端末２０３にファイル名によりファイルデータの保存を指示する。ファイルデータ３１１は、クライアント端末２０３のクライアントアプリケーション２３２に渡される。

【００３３】

クライアントアプリケーション２３２は、ファイルデータ３１１を暗号化し、暗号化ファイルデータ３１２を生成する。そして、クライアントアプリケーション２３２は、ファイルハッシュ生成処理として、暗号化ファイルデータ３１２からファイルHash３１３を算

出する。クライアントアプリケーション２３２は、ファイルHash３１３を検索用ノード２２１に送信する。なお、送信先の検索用ノード２２１は、ロケーションリスト３１７の検索用ノードリスト３２４を参照して、例えば、ＫＡＤ(Kademlia)ネットワークにおけるノード検索の再帰アルゴリズムを用いて、最も近い検索用ノードを見付けることが望ましい。また、本実施形態においては、ファイルの暗号化後にファイルHashを算出したが、ファイルHashを算出した後にファイルHashを含んでファイルを暗号化してもよい。

【００３４】

検索用ノード２２１は、保持するロケーションリスト３１７に、ファイルHash３１３を検索キーとして有する空のファイルリストを生成して追加する。そして、検索用ネットワーク２０２に含まれる全ての検索用ノードは、Ｐ２Ｐ通信により空のファイルリストが追加された最新のロケーションリストを保持することができる。なお、ファイル名と検索キーとなるファイルHash３１３との対応データ３１４を生成してアプリケーションに保持しておくことによって、ファイルの取得を行う場合のクライアントからの要求を簡易にすることができる。

【００３５】

一方、クライアントアプリケーション２３２は、暗号化ファイルデータ３１２を、クライアントやファイルの重要性、さらに、復元可能な冗長性を考慮して複数の部分データ３１５に分割する。そして、クライアントアプリケーション２３２は、部分ハッシュ生成処理として、複数の部分データ３１５のそれぞれのHash値を算出して、部分Hash３１６を生成する。部分Hash３１６は、部分データ３１５の先頭から順に、前の部分Hash３１６に次の部分データ３１５を加えてHash値を算出することによりブロックチェーン化する。ブロックチェーン化してHash値を算出するので、ファイルリストに保持された部分Hashや保存用ノードから読み出した部分Hashから部分データの合成順を知ることができる。なお、部分Hash３１６は、各部分データ３１５に対して独立して算出してもよい。独立して部分Hashを算出する場合には、ファイルの読み出し時に部分データを合成する順序を保持する必要がある。例えば、ロケーションリストのファイルリスト３２２に保持する、あるいは、保存用ノードに保存された部分データや部分Hash内に保持することができる。

【００３６】

クライアントアプリケーション２３２は、検索用ノード２２１のロケーションリスト３１７から保存用ネットワーク２０１に参加する保存用ノードリスト３１８を取得する。なお、クライアントアプリケーション２３２から検索用ノード２２１へのファイルHash３１３の送信と、検索用ノード２２１からクライアントアプリケーション２３２への保存用ノードリスト３１８の送信とは、一緒に行われてもよい。また、検索用ノード２２１のロケーションリスト３１７には検索用ノードリスト３２４も保持されており、クライアントアプリケーション２３２からアクセスする検索用ノードを選定する場合に参照され、クライアント端末の検索用ノードとしての参加や離脱時には、最新データに更新される。

【００３７】

クライアントアプリケーション２３２は、受信した保存用ノードリスト３１８から、分割された複数の部分データ３１５の数に相当する保存ノードを識別する保存用ノードＩＤ３１９を選定する。なお、保存用ノードＩＤ３１９は、保存用ノードに関連する属性から算出されたHash値であるのが望ましい。また、選定される保存用ノードＩＤ３１９の数は、保存時のエラーを考慮して分割された複数の部分データ３１５の数より多く選定する。

【００３８】

クライアントアプリケーション２３２は、ファイルHash３１３と部分データ３１５と部分Hash３１６との組合せと、選定された保存用ノードＩＤ３１９とを組み合わせて、選定された保存用ノードに対して保存を指示する保存用メッセージ３２０を生成する。ここで、ファイルHash３１３と部分データ３１５と部分Hash３１６との組合せ、あるいは、少なくとも部分データ３１５は各データごとに暗号鍵で暗号化される。そして、クライアントアプリケーション２３２は、各保存用メッセージ３２０を各保存用ノードに送信する。なお、保存用メッセージ３２０の送信は、保存相手の複数の保存用ノードに一斉送信するの

が高速化の面で望ましい。

【００３９】

保存相手の保存用ノード２１１では、保存用ノードＩＤ３１９を確認して、ファイルHashと部分Hashとを検索キーとした部分データ３２１を保存する。そして、保存がエラーなく完了すると、保存用ノード２１１は検索用ノードに保存完了報告を行う。この保存完了報告には、ファイルHashと部分Hashと保存用ノードＩＤとの組合せが含まれる。なお、保存完了報告は、全検索用ノードに一斉送信されても、先にクライアントアプリケーション２３２がアクセスした検索用ノードであってもよい。なお、検索用ネットワーク２０２では、全検索用ノードがＰ２Ｐ通信により空のファイルリストを含む最新のロケーションリストを保持している。図示されていないが、保存完了報告を行った保存用ノードには、保存対価の報酬が支払われる。

【００４０】

エラーなしに保存完了した保存用ノードからの保存完了報告を受信した検索用ノードは、保存完了報告に含まれる部分Hashと保存用ノードＩＤとの組合せを、ファイルHashを検索キーとする空のファイルリストに順次に記憶する。冗長を含む保存対象のファイルが再生可能な数の部分データが保存されると、新たなファイルリスト３２２が追加された最新のロケーションリストが完成する。

【００４１】

図示されていないが、ファイルの保存用ネットワーク２０１の保存用ノードへの保存が完了すると、ファイルの保存を要求したクライアント３０１から通常は保存料金が徴収される。

【００４２】

（ファイルの再現手順）

図３Ｂは、本実施形態に係る情報処理システム２００の、ファイルを合成して復元する動作手順を示す図である。なお、図３Ｂにおいては、図３Ａで保存したファイルを読み出す例を説明するが、他のファイルであっても動作手順は同様である。

【００４３】

ファイルの取得を要求するクライアント３０３からのクライアント端末２０３に対して入力されたファイル名は、クライアントアプリケーション２３２に渡される。クライアントアプリケーション２３２は、ファイルハッシュ取得処理として、対応データ３１４を参照してファイル名に対応付けて保持されているファイルHash３１３を取得する。そして、取得したファイルHash３１３を検索用ノードに送信する。なお、ファイルの保存時と同様に、送信先の検索用ノードは、ロケーションリスト３１７の検索用ノードリストを参照して、例えば、ＫＡＤ(Kademlia)ネットワークにおけるノード検索の再帰アルゴリズムを用いて、最も近い検索用ノードを見付けることが望ましい。

【００４４】

検索用ノードは、受信したファイルHash３１３を検索キーとして、ファイルのファイルリスト３２２を検索する。そして、ファイルHash３１３を有するファイルリスト３２５を見つける。そして、検索用ノードは、見つけたファイルリスト３２５をクライアントアプリケーション２３２に送信する。

【００４５】

クライアントアプリケーション２３２は、保存用ノード情報取得処理として、受信したファイルリスト３２５に含まれる、ファイルの分割数だけの部分Hashと保存用ノードＩＤとの組合せ３２６をそれぞれ抽出する。そして、クライアントアプリケーション２３２は、保存用ノードＩＤが示す保存用ノードに対してファイルHashと部分Hashとを送信する。なお、保存用ノードＩＤとファイルHashと部分Hashとは、保存用ネットワーク２０１の保存用ノードに対してＰ２Ｐ送信される。

【００４６】

送信された各保存用ノードＩＤを有する保存用ノード２１１は、受信したファイルHashと部分Hashとを検索キーとして部分データを検索する。そして、保存用ノード２１１は、

見つかった部分データを、ファイルHashと部分Hashと共にクライアントアプリケーション２３２に送信する。図示されていないが、本実施形態においては、部分データを読み出してクライアントアプリケーション２３２に送信した保存用ノード２１１には、保存時の報酬よりも高い読出の報酬が支払われる。

【００４７】

クライアントアプリケーション２３２は、それぞれの保存用ノード２１１からファイルHashと部分Hashと部分データとの組合せ３２１を受信して、その数がファイルを復元できる数を超えた場合、保存用ネットワーク２０１からのファイルの読み出しが成功したとする。クライアントアプリケーション２３２は、受信したデータを部分データを暗号化した暗号鍵に対応する復号鍵で復号し、部分Hashと部分データとの組合せ３２１に含まれる各部分Hashを照合して、部分データ３１５を分割した順序で合成して、暗号化ファイルデータ３１２を復元する。なお、複数の部分データの合成については、先にファイルの保存処理で説明したように、部分データを分割順にブロックチェーン化して部分Hashを算出しているので、合成順序を持つ必要はない。ただし、各部分データから独立に部分Hashを算出する場合は、部分データの合成順序を保持する必要がある。

【００４８】

クライアントアプリケーション２３２は、復元された暗号化ファイルデータからファイルを暗号化した暗号鍵に対応する復号鍵でファイルデータを復号して、クライアント端末２０３によりクライアント３０３に提供する。なお、図示していないが、クライアント３０３にファイルが提供されると、普通はクライアント３０３からファイルを提供した料金が徴収される。

【００４９】

（保存用ノードまたは検索用ノードの動作手順）

図４は、本実施形態に係る情報処理システム２００の、保存用ノードまたは検索用ノードの動作手順を示す図である。

【００５０】

（保存用ノード）

クライアント端末が保存用ネットワーク２０１の保存用ノード２１１として参加する場合、クライアント端末は、ステップＳ４５１において、保存用ノードアプリケーション４１１をダウンロードして駆動する。保存用ノードアプリケーション４１１は、ステップＳ４５２において、電子キャッシュ保存部を設定する。

【００５１】

クライアント端末は、ステップＳ４５３において、保存用ノードへの参加を申し込み、ステップＳ４５４において、クライアント情報としてストレージサイズやクライアント属性などを保存用ノードアプリケーション４１１に送出する。保存用ノードアプリケーション４１１は、ステップＳ４５５において、クライアント情報に基づいて保存用ノード２１１の選定時に考慮されるノードの信頼性を示すノードランクが初期設定され、保存用ノード２１１を識別するHashＩＤが設定される。そして、保存用ノードの登録は、検索用ノードに伝えられて検索用ノードに保持されたロケーションリスト内の保存用ノードリストが最新状態に更新される。

【００５２】

保存用ノード２１１が部分ファイルを保存する場合、保存用ノードアプリケーション４１１は、ステップＳ４５６において、クライアントアプリケーション２３２から保存用ノードＩＤを送信先として（ファイルHash、部分Hash、部分データ）の組合せを取得して保存する。そして、保存用ノードアプリケーション４１１は、ステップＳ４５７において、保存報酬を取得する。

【００５３】

保存用ノード２１１が部分データを読出す場合、保存用ノードアプリケーション４１１は、ステップＳ４５８において、クライアントアプリケーション２３２から保存用ノードＩＤを送信先としてファイルHasnと部分Hashとを取得する。そして、保存用ノードアプリ

ケーション４１１は、ファイルHasnと部分Hashとを検索キーとして部分データを検索して読み出し、クライアントアプリケーション２３２に送る。保存用ノードアプリケーション４１１は、ステップＳ４５９において、保存報酬より多い読出報酬を取得する。

【００５４】

（検索用ノード）

クライアント端末が検索用ネットワーク２０２の検索用ノード２２１として参加する場合、クライアント端末は、ステップＳ４６１において、検索用ノードアプリケーション４２１をダウンロードして駆動する。検索用ノードアプリケーション４２１は、ステップＳ４６２において、電子キャッシュ保存部を設定する。

【００５５】

クライアント端末は、ステップＳ４６３において、検索用ノードへの参加を申し込み、ステップＳ４６４において、クライアント情報としてクライアント属性や参加料金などを検索用ノードアプリケーション４２１に送出する。検索用ノードアプリケーション４２１は、ステップＳ４６５において、検索用ノードから選ばれた管理グループに対して、参加可否の判定要求をして、判定結果を取得する。なお、参加可否の判定は、検索用ネットワーク２０２に参加する検索用ノードの投票で行われる。そして、検索用ノードアプリケーション４２１は、ステップＳ４６６において、クライアント情報に基づいて検索用ノード２２１の投票時に考慮されるノードの信頼性を示すノードランクが設定され、検索用ノード２２１を識別するHashＩＤが設定される。そして、検索用ノードの登録は、検索用ノードが保持するロケーションリスト内の検索用ノードリストを最新状態に更新する。

【００５６】

検索用ノード２２１がロケーションリストを保存して共有する場合、検索用ノードアプリケーション４２１は、ステップＳ４６７において、クライアント端末からファイルHashを受信すると、ファイルHashを検索キーとする空のファイルリストをロケーションリストに追加する。そして、各保存用ノードから部分データの保存完了報告を受信すると、検索用ノードアプリケーション４２１は、ステップＳ４６８において、空のファイルリストに、部分Hashと、部分データを保存した保存用ノードＩＤとの組合せを書き込む。また、ファイルの取得要求として、クライアント端末からファイルHashを受信すると、検索用ノードアプリケーション４２１は、ステップＳ４６９において、ロケーションリストからファイルHashを含むファイルリストを読出して、クライアントアプリケーション２３２に送信する。

【００５７】

検索用ノード２２１が検索用ネットワーク２０２における投票に参加する場合、検索用ノードアプリケーション４２１は、ステップＳ４７０において、各投票に参加すると、ステップＳ４７１において、参加に対する報酬を取得する。

【００５８】

《クライアントアプリケーション》

以下、図５～図７に従って、クライアントアプリケーション２３２の構成および動作について説明する。

【００５９】

図５は、本実施形態に係るクライアントアプリケーション２３２の構成を示す図である。

【００６０】

クライアントアプリケーション２３２は、通信制御部５００～５０２と、ファイル保存処理部５０３と、リスト検索処理部５０５と、ファイル取得処理部５０６と、を備える。

【００６１】

通信制御部５００は、クライアント端末２０３との通信を制御する。通信制御部５０１は、保存用ネットワーク２０１との間でＰ２Ｐトンネルによる（ファイルHash、部分Hash、部分データ）の組合せや報酬などの通信を制御する。通信制御部５０２は、検索用ネットワーク２０２との間で保存用ノードリストまたはファイルリストをやり取りする独立し

たＰ２Ｐネットワークを制御する。

【００６２】

ファイル保存処理部５０３は、クライアント端末２０３から通信制御部５００を介して取得したファイルを暗号化してHash値であるファイルHashを生成する。また、ファイル保存処理部５０３は、暗号化したファイルを部分データに分割して、各部分データのHash値である部分Hashを生成する。さらに、ファイル保存処理部５０３は、検索用ノードから取得した保存用ノードリストに記載された複数の保存用ノードから、部分データの分割数と冗長数を加えたブロック数の保存用ノードを選定する。そして、ファイル保存処理部５０３は、通信制御部５０１を介して、選定された保存用ノードに（ファイルHash、部分Hash、部分データ）の組合せを送信して、ファイルHashと部分Hashとを検索キーとして部分データを保存させる。

【００６３】

リスト検索処理部５０５は、クライアント端末２０３から取得を望むファイルを表す取得対象情報、例えば、文書名、ファイル名、動画タイトルなどを取得し、取得対象情報をファイルに対応付けられた検索キーとしてのファイルHashを生成する。リスト検索処理部５０５は、通信制御部５０２を介して、検索用ネットワーク２０２内の近傍にある検索用ノードから、ファイルHashを検索キーとして検索された、最新のロケーションリスト内のファイルリストを取得する。

【００６４】

ファイル取得処理部５０６は、リスト検索処理部５０５から取得したファイルリストから各部分データの（部分Hash、保存用ノードＩＤ）の組合せを抽出する。そして、ファイル取得処理部５０６は、通信制御部５０１を介して、（ファイルHash、部分Hash、保存用ノードＩＤ）の組合せを用いて、各部分データを対応する保存用ノードから検索して読み出す。ファイル取得処理部５０６は、各部分データを復号して、正しく読み出された部分データのブロック数が所定数以上の場合には、部分データを合成して暗号化ファイルを再生する。ファイル取得処理部５０６は、再生された暗号化ファイルを暗号化鍵に対応する復号鍵で復号してクライアント端末２０３に送出する。

【００６５】

図６は、本実施形態に係るクライアントアプリケーション２３２を含むクライアント端末２０３のハードウェア構成を示すブロック図である。

【００６６】

図６で、ＣＰＵ６１０は演算制御用のプロセッサであり、プログラムを実行することで図５の構成を実現する。ＣＰＵ(Central Processing Unit)６１０は１つであっても複数であってもよい。ＲＯＭ(Read Only Memory)６２０は、初期データおよびプログラムなどの固定データおよびプログラムを記憶する。ネットワークインタフェース６３０は、保存用ネットワーク２０１や検索用ネットワーク２０２との通信を制御する。

【００６７】

ＲＡＭ(Random Access Memory)６４０は、ＣＰＵ６１０が一時記憶のワークエリアとして使用するランダムアクセスメモリである。ＲＡＭ６４０には、本実施形態の実現に必要なデータを記憶する領域が確保されている。保存すべきファイル６４１は、保存用ネットワーク２０１の保存用ノード２１１に部分データとして分散保存するためのファイルである。取得したファイル６４２は、保存用ネットワーク２０１の保存用ノード２１１に分散保存された部分データを合成して復元されたファイルである。ロケーションリスト６４３は、検索用ネットワーク２０２の全ての検索用ノードに共有された分散保存の構成を示すリストである。ファイルHash６４４は、保存すべきファイル６４１あるいは取得したファイル６４２のHash値である。検索用ノードＩＤ６４５は、クライアント端末２０３がアクセスしているロケーションリストを保持する検索用ノードを識別するためのＩＤである。部分Hashと部分データと保存用ノードＩＤ６４６は、分割されて各保存用ノードに保存される部分データと、その部分データのHash値と、保存先ノードのＩＤである。なお、保存用ノードＩＤは保存用ノードを識別する識別情報のHash値であることが望ましい。電子キ

ャッシュデータ６４７は、ファイル保存や取得に対応する料金の支払い、あるいは、ファイル保存や読出しの報酬の受取りのためのブロックチェーンされたデータである。送受信データ６４８は、ネットワークインタフェース６３０を介して送受信されるデータである。入出力データ６４９は、入出力インタフェース６６０を介して入出力機器と入出力するデータである。

【００６８】

ストレージ６５０は、ＣＰＵ６１０が使用する、本実施形態の実現に必要な以下のデータまたはプログラムが記憶されている。データベース６５１は、本実施形態の実現に必要な基本データを保持する。各種アルゴリズム６５２は、本実施形態の実現に必要なアルゴリズムを保持する。各種パラメータ６５３は、各種アルゴリズム６５２が用いる本実施形態の実現に必要なアルゴリズムを保持する。電子キャッシュ保持部６５４は、電子サイフとして、本実施形態の処理に必要な料金の支払い、あるいは、処理により得られる報酬をブロックチェーンされた電子キャッシュで保持する。

【００６９】

ストレージ６５０には、以下のプログラムが格納される。クライアント端末制御プログラム６５５は、クライアント端末２０３の全体を制御するプログラムである。クライアントアプリケーション２３２は、クライアント端末２０３にダウンロードされて、あるいは、ブラウザ機能を伴ってクライアント端末２０３で実行されるアプリケーションである。クライアントアプリケーション２３２は、以下のモジュールを有する。

【００７０】

ファイル保存処理部５０３として機能するファイル保存処理モジュールは、図５に図示された、保存すべきファイル６４１を分割した部分データを保存用ノードに分散保存させるモジュールである。リスト検索処理部５０５として機能するリスト検索処理モジュールは、図５に図示された、１つの検索用ノードが保持するロケーションリストからファイルHashを検索キーとして検索したファイルリストを受信モジュールである。ファイル取得処理部５０６として機能するファイル取得処理モジュールは、図５に図示された、リスト検索処理モジュールにより受信したファイルリストが保持するファイルHashと部分Hashと保存用ノードＩＤとの組合せを用いて部分データを読出して合成して、取得したファイル６４２を復元するモジュールである。報酬処理部として機能する報酬処理モジュールは、ファイル保存完了通知や、ファイル取得完了通知に応答して、参加ノード特に保存用ノードに対する報酬を提供するためのモジュールである。各種通信制御部５００、５０１、５０２として機能する通信制御モジュールは、図５に図示された、各通信制御を行うモジュールである。

【００７１】

入出力インタフェース６６０は、入出力デバイスとのデータ入出力を制御するためのインタフェースを行なう。本実施形態においては、入出力インタフェース６６０には、表示部６６１、操作部６６２、音声入出力部６６３、記憶媒体６６４などが接続される。

【００７２】

なお、図６のＲＡＭ６４０やストレージ６５０には、クライアント端末２０３が有する汎用の機能や他の実現可能な機能に関連するプログラムやデータは図示されていない。

【００７３】

図７は、本実施形態に係るクライアントアプリケーション２３２の処理手順を示すフローチャートである。このフローチャートは、図６のＣＰＵ６１０がＲＡＭ６４０を用いて実行し、図５の機能構成を実現する。

【００７４】

クライアント端末２０３は、ステップＳ７１１において、ファイルの保存であるか否かを判定する。ファイルの保存であれば、クライアント端末２０３は、ステップＳ７１３において、ファイルを分割して、分割された部分データを保存用ノード２１１に保存するデータ保存処理を実行する。

【００７５】

ファイルの保存でないと判定された場合、クライアント端末２０３は、ステップＳ７２１において、ファイルの取得（または閲覧）であるか否かを判定する。ファイルの取得であれば、クライアント端末２０３は、ステップＳ７２３において、１つの検索用ノードが保持するロケーションリストから、ファイルを識別するファイルHashに一致するファイルリストを受信するリスト検索処理を実行する。そして、クライアント端末２０３は、ステップＳ７２５において、ファイルから分割された部分データを、ファイルリストに含まれる部分Hashと保存用ノードＩＤとに基づいて読出し、部分データからファイルを合成して復元するファイル取得処理を実行する。

【００７６】

（ファイル保存処理部）

図８は、本実施形態に係るファイル保存処理部５０３の機能構成を示すブロック図である。

【００７７】

ファイル保存処理部５０３は、ファイル暗号化部８３１と、ファイルHash生成部８３２と、部分データ生成部８３３と、部分Hash生成部８３４と、保存用ノード選定部８３５と、分散保存指示部８３６と、を備える。

【００７８】

ファイル暗号化部８３１は、暗号化アルゴリズムと暗号化鍵とを有し、クライアントから保存を指示されたファイルを暗号化する。なお、使用される暗号化アルゴリズムや暗号化鍵は限定されないが、クライアントに対応する暗号化鍵が配布されているとする。ファイルHash生成部８３２は、ファイル暗号化部８３１において暗号化されたファイルのHash値を算出する。なお、Hash値の算出方法は、その認証方法と対応していれば限定されない。部分データ生成部８３３は、分割アルゴリズムと分割アルゴリズムで算出された分割数とを有し、データ分割部として、ファイル暗号化部８３１において暗号化されたファイルを算出された分割数に基づいて分割する。なお、部分データ生成部８３３の分割アルゴリズムは、ファイルに対応して部分データの数を制御すると共に、保存時や取得時のエラーによってもデータ復元が可能なように、分割における冗長のための処理が含まれる。部分Hash生成部８３４は、部分データ生成部８３３で分割された部分データのHash値を算出する。なお、Hash値の算出方法は、その認証方法と対応していれば限定されない。保存用ノード選定部８３５は、選定アルゴリズムと選定アルゴリズムで選定された保存先ノードＩＤとを有し、部分データ生成部８３３で冗長を含めて分割された分割数の部分データを保存する保存用ノードを、各々の保存用ノードの信頼性も考慮して選定する。なお、保存用ノードの識別は、保存用ノードに関連する情報のHash値であるのが望ましい。かかる保存用ノードを識別するHash値は、保存用ノードとして保存用ネットワーク２０１に参加する時に付与される。

【００７９】

分散保存指示部８３６は、保存データテーブル８３７を有し、ファイルHashと、部分Hash生成部８３４で生成された部分Hashを部分データを識別する識別子として部分データと組み合わせ、保存用ノード選定部８３５が選定した各保存用ノードへ保存を指示する。なお、図示しないが、部分データは暗号化鍵により暗号化される。

【００８０】

図９は、本実施形態に係るファイル保存処理部５０３で使用する保存データテーブル８３７の構成を示す図である。保存データテーブル８３７には、分散保存指示部８３６で保存用ノードに部分データを保存するための情報が保持される。

【００８１】

保存データテーブル８３７は、ファイルHash９２１に対応付けて、分割数９１２の各々の部分データ９２３について、部分Hash９２２と、対応する部分データ９２３と、選定された保存用ノードＩＤ９２４とを記憶する。

【００８２】

図１０は、実施形態に係るファイル保存処理部５０３の処理手順を示すフローチャート

である。このフローチャートは、図６のＣＰＵ６１０がＲＡＭ６４０を用いて実行し、図８のファイル保存処理部５０３の機能構成部を実現する。

【００８３】

ファイル保存処理部５０３は、ステップＳ１００１において、保存すべきファイルを取得したか否かを判定する。ファイルを取得した場合、ファイル保存処理部５０３は、ステップＳ１００３において、ファイルの暗号化処理を実行する。ファイル保存処理部５０３は、ステップＳ１００５において、暗号化されたファイルのHash値を算出する。

【００８４】

ファイル保存処理部５０３は、ステップＳ１００７において、暗号化されたファイルの部分データへの分割処理を実行する。ファイル保存処理部５０３は、ステップＳ１００９において、分割された部分データを保存する保存先の保存用ノードを選定する。

【００８５】

ファイル保存処理部５０３は、ステップＳ１０１１において、選定された各保存用ノードに（ファイルHash、部分Hash、部分データ）により保存を指示する。

【００８６】

図１１Ａは、本実施形態に係るファイル分割処理Ｓ１００７の手順を示すフローチャートである。

【００８７】

ファイル保存処理部５０３は、ステップＳ１１７１において、ファイルのサイズを取得する。ファイル保存処理部５０３は、ステップＳ１１７３において、データブロック数を、（データブロック数＝サイズ／部分データサイズ）の式により算出する。次に、ファイル保存処理部５０３は、ステップＳ１１７５において、冗長ブロック数を、（冗長ブロック数＝データブロック数／所定数）の式により算出する。所定数は、本実施形態では例えば、３が用いられる。次に、ファイル保存処理部５０３は、ステップＳ１１７７において、分割数を、（分割数＝データブロック数＋冗長ブロック数）の式により算出する。そして、ファイル保存処理部５０３は、ステップＳＳ１１７９において、ステップＳ１００３で暗号化されたファイルを算出された分割数に分割する。

【００８８】

図１１Ｂは、本実施形態に係る保存先ノードの選定処理Ｓ１００９の手順を示すフローチャートである。

【００８９】

ファイル保存処理部５０３は、ステップＳ１１９１において、ステップＳ１１７７で算出された分割数を取得する。次に、ファイル保存処理部５０３は、ステップＳ１１９３において、保存用ネットワーク２０１に参加する保存用ノードのリストを１つの検索用ノードから取得する。そして、ファイル保存処理部５０３は、ステップＳ１１９５において、ファイルの重要度や保存要求クライアントの重要度などを取得する。ファイル保存処理部５０３は、ステップＳ１１９７において、取得したファイルの重要度、および／または、保存要求クライアントの重要度を考慮して、クライアント端末により近い分割数に相当する保存用ノードを選定する。

【００９０】

図１１Ｂには、ステップＳ１１９５およびＳ１１９７における処理で用いられる保存用ノードのテーブル１１１０が図示されている。保存用ノードのテーブル１１１０は、各保存用ノードＩＤ（Hash値）１１１１に対応付けて、保存用ノードの属性１１１２、保存用ノードの信頼度（レベル）１１１３、保存用ノードの位置１１１４を記憶する。そして、各保存用ノードＩＤ（Hash値）１１１１に対応付けて、選択結果１１１５を記憶する。

【００９１】

（リスト検索処理部）

図１２は、本実施形態に係るリスト検索処理部５０５の機能構成を示すブロック図である。

【００９２】

リスト検索処理部５０５は、ファイルHash取得部１２５１と、ファイルHash送信部（ファイルハッシュ送信部）１２５２と、ファイルリスト取得部１２５３と、ファイルリスト通知部１２５５と、を備える。ファイルHash取得部１２５１は、取得対象情報、例えば、取得対象のファイル名や文書名、動画題名などから、ファイルの保存時にあらかじめ保持された対応するファイルHashを取得する。ファイルHash送信部１２５２は、検索用ネットワーク２０２中の近接する１つの検索用ノードから、ファイルのHash値を検索キーとして最新のロケーションリストから検索したファイルリストを取得する。ファイルリスト通知部１２５５は、ファイルリスト１２５６を有し、ファイルリスト取得部１２５３が取得したファイルリストをファイル取得処理部５０６に通知する。

【００９３】

図１３は、本実施形態に係るリスト検索処理部５０５で使用するファイルリスト１２５６の構成を示す図である。図１３には、ファイルリスト通知部１２５５がファイル取得処理部５０６に通知するファイルリスト１２５６の構成を図示する。

【００９４】

図１４は、本実施形態に係るリスト検索処理部５０５の処理手順を示すフローチャートである。このフローチャートは、図６のＣＰＵ６１０がＲＡＭ６４０を用いて実行し、図１２の機能構成を実現する。

【００９５】

リスト検索処理部５０５は、ステップＳ１４０１において、クライアント端末２０３からファイルを示す取得対象情報を取得する。リスト検索処理部５０５は、ステップＳ１４０３において、取得した取得対象情報に対応して保持されたファイルHashを取得する。

【００９６】

リスト検索処理部５０５は、ステップＳ１４０５において、検索用ネットワーク２０２中の近くの検索用ノードにファイルHashを送信する。そして、リスト検索処理部５０５は、ステップＳ１４０７において、検索用ノードから返信される、ファイルHashを探索キーとして最新のロケーションリストを検索して得られたファイルリストの受信を待つ。ファイルリストが受信されれば、リスト検索処理部５０５は、ステップＳ１４１１において、ファイルリストをファイル取得処理部５０６に通知する。

【００９７】

（ファイル取得処理部）

図１５は、本実施形態に係るファイル取得処理部５０６の機能構成を示すブロック図である。

【００９８】

ファイル取得処理部５０６は、ファイルリスト取得部１５６１と、部分データ情報抽出部１５６２と、部分データ取得部１５６３と、部分データ合成部１５６４と、を備える。さらに、ファイル取得処理部５０６は、ファイル復号部１５６６と、ファイル送出部１５６７と、を備える。

【００９９】

ファイルリスト取得部１５６１は、リスト検索処理部５０５からファイルリストを取得する。部分データ情報抽出部１５６２は、ファイルリストに含まれる分割された部分データのロケーションを示す部分データ情報である保存用ノードＩＤと部分hashとを抽出する。部分データ取得部１５６３は、保存用ノードＩＤとファイルHashと各部分データの部分Hashとを用いて、保存用ノードＩＤが示す保存用ノードから一斉に部分データを取得する。

【０１００】

部分データ合成部１５６４は、データ合成テーブル１５６５を有し、部分データ取得部１５６３が取得した部分データの数が所定数以上になれば、部分データを合成して暗号化ファイルを復元する。すなわち、部分データの取得にエラーが生じた場合であっても、所定数以上の部分データの取得があればファイルを復元可能である。なお、部分データ合成部１５６４では、保存用ノードから取得した部分データを保存時に暗号鍵に対応する復号

鍵で復号する処理も行う。

【０１０１】

ファイル復号部１５６６は、復元された暗号化ファイルを保存時に暗号化した暗号鍵に対応する復号鍵で復号する。なお、かかる復号鍵は、クライアントに対応して配布された暗号化鍵に対応するものである。このように構成することにより、クライアント以外の人は復号鍵をいずれかの方法で取得しない限り、ファイルを復号して復元することができない。ファイル送出部１５６７は、復号されたファイルをクライアント端末２０３に送出する。ファイルの取得完了通知を報酬処理部に通知して、読出報酬を取得してもよい。

【０１０２】

図１６は、本実施形態に係るファイル取得処理部５０６で使用するデータ合成テーブル１５６５の構成を示す図である。データ合成テーブル１５６５は、部分データ合成部１５６４が取得した部分データから暗号化されたファイルを合成するために使用される。

【０１０３】

データ合成テーブル１５６５は、部分Hash１６０１と、読出された部分データ１６０２と、部分データ１６０２の所定数以上から合成された、暗号化されたファイルである合成ファイル１６０３と、復号されたファイルである復号ファイル１６０４とを記憶する。なお、部分データ１６０２の合成順序は、ブロックチェーン化された部分Hash１６０１から知ることができる。ブロックチェーン化されない部分Hash１６０１においては、合成順序を別途保存しておく必要がある。

【０１０４】

図１７は、本実施形態に係るファイル取得処理部５０６の処理手順を示すフローチャートである。このフローチャートは、図６のＣＰＵ６１０がＲＡＭ６４０を用いて実行し、図１５のファイル取得処理部５０６の機能構成を実現する。

【０１０５】

ファイル取得処理部５０６は、ステップＳ１７０１において、リスト検索処理部５０５からファイルリストを取得する。ファイル取得処理部５０６は、ステップＳ１７０３において、ファイルリストから分割されて保存された部分データを取得するための（部分Hash、保存用ノードＩＤ）の組合せを抽出する。ファイル取得処理部５０６は、ステップＳ１７０５において、（ファイルHash、部分Hash、保存用ノードＩＤ）の組合せを用いて、保存用ネットワーク２０１の保存用ノードから分割数の部分データを取得する。

【０１０６】

ファイル取得処理部５０６は、ステップＳ１７０７において、正しく取得した部分データの取得数を数える。例えば、保存用ノードの故障、保存用ノードの部分データの削除、改ざんやエラー、通信状況によるエラーなど、その一部は部分Hashにより検証可能である。ファイル取得処理部５０６は、ステップＳ１７０９において、正しく取得した部分データの取得数が所定数α以上である、復元可能な数であるか否かを判定する。

【０１０７】

部分データの取得数が所定数α以上である場合、ファイル取得処理部５０６は、ステップＳ１７１１において、正しく取得した部分データを合成する。ファイル取得処理部５０６は、ステップＳ１７１３において、合成ファイルを復号する。ファイル取得処理部５０６は、ステップＳ１７１５において、部分データから合成され復号されたファイルをクライアント端末２０３から送出する。

【０１０８】

部分データの取得数が所定数α未満である場合、ファイル取得処理部５０６は、ステップＳ１７１９において、データ取得エラーをクライアント端末２０３に通知する。

【０１０９】

（報酬処理部）

図１８は、本実施形態に係る報酬処理部１８００の機能構成を示すブロック図である。なお、報酬処理部１８００は、検索用サーバに搭載されていても、クライアントアプリケーション２３２に組み込まれていても、あるいは、検索用ノードアプリケーションや保存

用ノードアプリケーションなどに分散されていてもよい。また、報酬処理部１８００を含む管理サーバを別途設ける構成であってもよい。

【０１１０】

報酬処理部１８００は、保存完了通知取得部１８７１と、取得完了通知取得部１８７２と、報酬算出アルゴリズム取得部１８７３と、報酬算出部１８７４と、報酬提供部１８７６と、を備える。

【０１１１】

保存完了通知取得部１８７１は、保存完了した各保存用ノードから部分データの保存完了通知を取得する。取得完了通知取得部１８７２は、ファイル取得処理部５０６からファイルの取得完了通知を取得する。

【０１１２】

報酬算出アルゴリズム取得部１８７３は、情報処理システム２００における、保存用ネットワーク２０１に保存用ノードとして参加したクライアント、あるいは、検索用ネットワーク２０２に検索用ノードとして参加したクライアントに、どのように報酬を提供するかのアルゴリズムを取得する。本実施形態においては、例えば、ファイルの保存時に徴収する料金の内から総額２割程度の比較的少ない初期報酬を保存用ノードに提供し、その後は、所定期間でゼロとなる下降曲線で残りの８割をファイルの読み出し時に還元する報酬提供アルゴリズムを採用している。このようなアルゴリズムを用いることにより、保存用ノードの参加者が保存された部分データを削除しないように誘導している。しかしながら、報酬の提供アルゴリズムはこれに限定されない。

【０１１３】

報酬算出部１８７４は、報酬テーブル１８７５を有し、報酬提供アルゴリズムに従って、部分データの保存完了時および部分データの読出し完了時に保存用ノードに対して提供する報酬を算出する。報酬提供部１８７６は、報酬算出部１８７４が算出した報酬を、部分データを保存あるいは読出した保存用ノードに提供する。

【０１１４】

なお、図１８には、検索用ネットワーク２０２の検索用ノードへの報酬については図示されてない。本実施形態においては、例えば、検索用ネットワーク２０２への新規参加時、あるいは、保存用ノードに対して提供する報酬の算出アルゴリズムなどの決定あるいは変更時などに行われる保存用ノードによる投票への参加に対して、報酬を提供する。

【０１１５】

図１９は、本実施形態に係る報酬処理部１８００で使用する報酬テーブル１８７５の構成を示す図である。報酬テーブル１８７５は、報酬算出部１８７４が本実施形態のアルゴリズムで保存用ノードに報酬を提供する場合に用いる。

【０１１６】

報酬テーブル１８７５は、保存対象あるいは取得対象のファイルHashによるファイルＩＤ１９１０に対応付けて、保存料金１９０２と取得または閲覧料金×回数１９０３とを考慮して算出された、データ保存時の報酬１９０４とデータ読出時の報酬１９０５とを記憶する。なお、データ読出時の報酬１９０５の変化は、初期値と減少する変化曲線とを含む。

【０１１７】

図２０は、本実施形態に係る報酬処理部１８００の処理手順を示すフローチャートである。このフローチャートは、報酬処理部１８００のＣＰＵがＲＡＭを用いて実行し、図１８の報酬処理部１８００の機能構成部を実現する。

【０１１８】

報酬処理部１８００は、ステップＳ２００１において、各保存用ノードからの保存完了通知、または、ファイル取得処理部５０６からの取得完了通知を待つ。保存完了通知、または、取得完了通知があれば、報酬処理部１８００は、ステップＳ２００３において、部分データの保存であるかファイルの取得であるかを判定する。

【０１１９】

部分データの保存完了であれば、報酬処理部１８００は、ステップＳ２００５において、保存料金から各保存用ノードへの報酬Ｘを算出する。そして、報酬処理部１８００は、ステップＳ２００７において、部分データを保存した保存用ノードに報酬Ｘを提供する。

【０１２０】

一方、ファイルを取得した場合、報酬処理部１８００は、ステップＳ２００９において、保存料金（＋取得料金）から各保存用ノードへの報酬Ｙを算出する。ここで、報酬Ｙは報酬Ｘよりも多い。そして、報酬処理部１８００は、ステップＳ２０１１において、ファイルの部分データを正しく読出した保存用ノードに報酬Ｙを提供する。

【０１２１】

《保存用ノード》

図２１は、本実施形態に係る保存用ノード２１１の機能構成を示すブロック図である。

【０１２２】

保存用ノード２１１は、Ｐ２Ｐの通信制御部２１０１と、入出力インタフェース２１０２と、保存用ノードアプリケーションダウンロード部２１０３と、保存用ノードアプリケーション実行部２１０４と、を備える。

【０１２３】

Ｐ２Ｐの通信制御部２１０１は、クライアント端末２０３や保存用ネットワーク２０１の他の保存用ノードとのＰ２Ｐ通信を制御する。入出力インタフェース２１０２は、保存用ノード２１１に接続する入出力機器である、表示部２１２１、操作部２１２２、音声入出力部２１２３、記憶媒体２１２４などとの入出力を制御する。保存用ノードアプリケーションダウンロード部２１０３は、種々のクライアント端末が保存用ノードとして保存用ネットワーク２０１に参入するために保存用ノードアプリケーションをダウンリードする。保存用ノードアプリケーション実行部２１０４は、保存用ノードアプリケーションダウンロード部２１０３がダウンロードした保存用ノードアプリケーションを実行し、保存用ノードとして機能する。

【０１２４】

保存用ノードアプリケーション実行部２１０４は、HashＩＤ記憶部２１４１と、保存用部分データ受信部２１４２と、ストレージ２１４３と、部分データ保存完了通知部２１４４と、を有する。さらに、保存用ノードアプリケーション実行部２１０４は、部分データ要求受信部２１４５と、部分データ送信部２１４６と、電子キャッシュ保存部２１４７と、料金送信部２１４８と、報酬受信部２１４９と、を有する。

【０１２５】

HashＩＤ記憶部２１４１は、保存用ノードとして保存用ネットワーク２０１に参入した時に付与される保存用ノード情報のHash値であるＩＤを記憶する。この保存用ノードHashＩＤは、保存用ノードＩＤとして使用される。保存用部分データ受信部２１４２は、ファイル保存処理部５０３からの保存用の部分データをファイルHashおよび部分Hashと共に受信する。ストレージ２１４３は、保存用部分データ受信部２１４２が受信した（ファイルHash、部分Hash、部分データ）を、ファイルHashと部分Hashとを検索キーとして保存する。部分データ保存完了通知部２１４４は、ストレージ２１４３へのファイルHashと部分Hashとを検索キーとした部分データの保存が完了した場合に、その旨を（ファイルHash、部分Hash、保存用ノードＩＤ）の組合せと共に検索用ノードに通知する。部分データ要求受信部２１４５は、ファイル取得処理部５０６からのファイルhashと部分Hashとを検索キーとする部分データの読み出し要求を受信する。部分データ送信部２１４６は、ファイルHashと部分Hashとの検索キーにより検索された部分データをストレージ２１４３から読出して、ファイル取得処理部５０６に送信する。

【０１２６】

電子キャッシュ保存部２１４７は、保存用ノードとして保存用ネットワーク２０１に参入する場合に、設定される電子キャッシュの記憶部である。料金送信部２１４８は、保存用ノードとして参入する場合、あるいは、他の料金支払いが必要な場合に、電子キャッシュ保存部２１４７から電子キャッシュを送金する。報酬受信部２１４９は、報酬処理部１

８００からの報酬を受信して、電子キャッシュ保存部２１４７に保存する。
【０１２７】
図２２は、本実施形態に係る保存用ノード２１１の動作手順を示すフローチャートである。このフローチャートは、保存用ノード２１１となるクライアント端末のＣＰＵがＲＡＭを用いて実行し、図２１の機能構成を実現する。
【０１２８】
保存用ノード２１１は、ステップＳ２２１１において、保存用の部分データの受信か否かを判定する。保存用の部分データの受信であると判定する場合、保存用ノード２１１は、ステップＳ２２１３において、取得した（ファイルhash、部分Hash、部分データ）の組合せをストレージ２１４３に保存する。そして、ストレージ２１４３への保存が完了すると、保存用ノード２１１は、ステップＳ２２１５において、保存完了を（ファイルhash、部分Hash、保存用ノードＩＤ）の組合せと共に、検索用ノードに通知する。
【０１２９】
保存用の部分データの受信でないと判定する場合、保存用ノード２１１は、ステップＳ２２２１において、部分データの読み出し要求か否かを判定する。部分データの読み出し要求であると判定された場合、保存用ノード２１１は、ステップＳ２２２３において、読出し要求に伴うファイルHashと部分Hashとを受け取り、ファイルHashと部分Hashとを検索キーとしてストレージ２１４３に保存された部分データを検索する。保存用ノード２１１は、ステップＳ２２２５において、部分データがストレージ２１４３内に有るか否かを判定する。部分データが見つかった場合、保存用ノード２１１は、ステップＳ２２２７において、部分データをファイルHashおよび部分Hashと共にファイル取得処理部５０６に送信する。部分データが見つからなかった場合、保存用ノード２１１は、ステップＳ２２２９において、エラー処理を行う。
【０１３０】
保存用の部分データの受信でもなく、部分データの要求でもないと判定する場合、保存用ノード２１１は、ステップＳ２２３１において、料金の送信か否かを判定する。料金の送信と判定された場合、保存用ノード２１１は、ステップＳ２２３３において、電子キャッシュ保存部２１４７から電子キャッシュを取得し、ステップＳ２２３５において、取得した電子キャッシュを送信する。保存用の部分データの受信でもなく、部分データの要求でもなく、料金の送信でもないと判定する場合、保存用ノード２１１は、ステップＳ２２４１において、報酬の受信か否かを判定する。報酬の受信と判定された場合、保存用ノード２１１は、ステップＳ２２４３において、報酬処理部１８００からの報酬を受信し、ステップＳ２２４５において、受信した報酬を電子キャッシュ保存部２１４７に保存する。
【０１３１】
《検索用ノード》
図２３は、本実施形態に係る検索用ノード２２１の機能構成を示すブロック図である。なお、図２３には、検索用ノード２２１が行う、ロケーションリスト３１７内の検索用ノードリストや保存用ノードリストを作成あるいは更新するための機能構成については、図面が煩雑となるため図示していない。
【０１３２】
検索用ノード２２１は、Ｐ２Ｐの通信制御部２３０１と、入出力インタフェース２３０２と、検索用ノードアプリケーションダウンロード部２３０３と、検索用ノードアプリケーション実行部２３０４と、を備える。
【０１３３】
Ｐ２Ｐの通信制御部２３０１は、クライアント端末２０３や検索用ネットワーク２０２の他の検索用ノードとのＰ２Ｐ通信を制御する。入出力インタフェース２３０２は、検索用ノード２２１に接続する入出力機器である、表示部２３２１、操作部２３２２、音声入出力部２３２３、記憶媒体２３２４などとの入出力を制御する。検索用ノードアプリケーションダウンロード部２３０３は、種々のクライアント端末が検索用ノードとして検索用ネットワーク２０２に参入するために検索用ノードアプリケーションをダウンリードする

。検索用ノードアプリケーション実行部２３０４は、検索用ノードアプリケーションダウンロード部２３０３がダウンロードした検索用ノードアプリケーションを実行し、検索用ノードとして機能する。

【０１３４】

検索用ノードアプリケーション実行部２３０４は、検索用ノードHashＩＤ記憶部２３４１と、ロケーションリスト更新指示受信部２３４２と、ロケーションリスト保存ストレージ２３４３と、部分データ保存完了通知受信部２３４４と、を有する。さらに、検索用ノードアプリケーション実行部２３０４は、ファイルリスト要求受信部２３４５と、ファイルリスト送信部２３４６と、電子キャッシュ保存部２３４７と、料金送信部２３４８と、報酬受信部２３４９と、を有する。

【０１３５】

検索用ノードHashＩＤ記憶部２３４１は、検索用ノードとして検索用ネットワーク２０２に参入した時に付与される検索用ノード情報のHash値であるＩＤを記憶する。この検索用ノードHashＩＤは、検索用ノードを特定するＩＤとして使用される。ロケーションリスト更新指示受信部２３４２は、ファイル保存要求の場合に、クライアント端末２０３からファイルHashを受信して、ロケーションリストにファイルHashを検索キーとする空のファイルリストを追加する。ロケーションリスト保存ストレージ２３４３は、ロケーションリスト更新指示受信部２３４２により更新された最新のロケーションリストを保存し、他の検索用ノードと共有する。部分データ保存完了通知受信部２３４４は、部分データの保存が完了した保存用ノードから保存完了通知を、（ファイルHash、部分Hash、保存用ノードＩＤ）の組合せと共に受信して、ロケーションリスト保存ストレージ２３４３内の空のファイルリストに挿入する。ファイルリスト要求受信部２３４５は、ファイル取得要求の場合に、クライアント端末２０３のリスト検索処理部５０５から、ファイルHashを検索キーとする最新ロケーションリストからのファイルリストの読み出し要求を受信する。ファイルリスト送信部２３４６は、ロケーションリスト保存ストレージ２３４３に保持されたロケーションリストを、ファイルHashを検索キーとして検索し、見つけたファイルリストをリスト検索処理部５０５に送信する。

【０１３６】

電子キャッシュ保存部２３４７は、検索用ノードとして検索用ネットワーク２０２に参入する場合に、設定される電子キャッシュの記憶部である。料金送信部２３４８は、検索用ノードとして参入する場合、あるいは、投票の参加するなどによる他の料金支払いが必要な場合に、電子キャッシュ保存部２３４７から電子キャッシュを送金する。報酬受信部２３４９は、報酬処理部１８００からの報酬を受信して、電子キャッシュ保存部２３４７に保存する。

【０１３７】

図２４は、本実施形態に係る検索用ノード２２１の動作手順を示すフローチャートである。このフローチャートは、検索用ノード２２１となるクライアント端末のＣＰＵがＲＡＭを用いて実行し、図２３の機能構成を実現する。なお、図２４においても、検索用ノード２２１が行う、ロケーションリスト３１７の検索用ノードリストや保存用ノードリストを作成あるいは更新するための動作手順については、図面が煩雑となるため図示していない。

【０１３８】

検索用ノード２２１は、ステップＳ２４１１において、ロケーションリスト更新指示の受信か否かを判定する。ロケーションリスト更新指示の受信であると判定する場合、検索用ノード２２１は、ステップＳ２４１３において、ロケーションリスト更新指示に付随して送信されたファイルHashを取得する。そして、検索用ノード２２１は、ステップＳ２４１３において、取得したファイルHashを検索キーとする空のファイルリストをロケーションリストに追加し、最新のロケーションリストをロケーションリスト保存ストレージ２３４３に保存する。

【０１３９】

ロケーションリスト更新指示の受信でないと判定する場合、検索用ノード２２１は、ステップＳ２４２１において、部分データの保存完了通知か否かを判定する。部分データの保存完了通知であると判定された場合、検索用ノード２２１は、ステップＳ２４２３において、保存完了通知に付随するファイルHashによりロケーションリスト内の空の（あるいは未完の）ファイルリストを検索する。そして、検索用ノード２２１は、ステップＳ２４２５において、空の（あるいは未完の）ファイルリストに保存完了通知と共に受信した（部分Hash、保存用ノードＩＤ）の組合せを挿入する。

【０１４０】

ロケーションリストの受信でなく、部分データの保存完了通知でもないと判定する場合、検索用ノード２２１は、ステップＳ２４３１において、ファイルリストの読み出し要求か否かを判定する。ファイルリストの読み出し要求であると判定された場合、検索用ノード２２１は、ステップＳ２４３３において、ロケーションリスト保存ストレージ２３４３に保持された最新のロケーションリストから、読み出し要求と共に受信したファイルHashを検索キーとしてファイルリストを検索する。そして、検索用ノード２２１は、ステップＳ２４３５において、ファイルリストを読み出し要求元のリスト検索処理部５０５に送信する。

【０１４１】

ロケーションリストの受信でもなく、部分データの保存完了通知でもなく、ロケーションリストの要求でもないと判定する場合、検索用ノード２２１は、ステップＳ２４４１において、料金の送信か否かを判定する。料金の送信と判定された場合、検索用ノード２２１は、ステップＳ２４３３において、電子キャッシュ保存部２３４７から電子キャッシュを取得し、ステップＳ２４４５において、取得した電子キャッシュを送信する。

【０１４２】

ロケーションリストの受信でもなく、部分データの保存完了通知でもなく、ロケーションリストの要求でもなく、料金の送信でもないと判定する場合、検索用ノード２２１は、ステップＳ２４５１において、報酬の受信か否かを判定する。報酬の受信と判定された場合、検索用ノード２２１は、ステップＳ２４５３において、報酬処理部１８００からの報酬を受信し、ステップＳ２４５５において、受信した報酬を電子キャッシュ保存部２３４７に保存する。

【０１４３】

（クライアント端末のハードウェア構成）

図２５は、本実施形態に係る保存用ノード２１１または検索用ノード２２１となるクライアント端末のハードウェア構成を示すブロック図である。

【０１４４】

図２５で、ＣＰＵ２５１０は演算制御用のプロセッサであり、プログラムを実行することで図２１または図２３の機能構成部を実現する。ＣＰＵ(Central Processing Unit)２５１０は１つであっても複数であってもよい。ＲＯＭ(Read Only Memory)２５２０は、初期データおよびプログラムなどの固定データおよびプログラムを記憶する。ネットワークインタフェース２５３０は、クライアント端末２０３や、保存用ネットワーク２０１や検索用ネットワーク２０２の他の保存用ノードや検索用ノードとの通信を制御する。

【０１４５】

ＲＡＭ(Random Access Memory)２５４０は、ＣＰＵ２５１０が一時記憶のワークエリアとして使用するランダムアクセスメモリである。ＲＡＭ２５４０には、本実施形態の実現に必要なデータを記憶する領域が確保されている。保存用ノードのデータ２５４１は、保存用ノードとして動作する場合のデータである。保存用ノードのデータ２５４１には、部分Hashや部分データが含まれる。検索用ノードのデータ２５４２は、検索用ノードとして動作する場合のデータである。検索用ノードのデータ２５４２には、ファイルHashや、ファイルHashを検索キーとするファイルリストや、登録されている保存用ノードの一覧である保存用ノードリストが含まれる。電子キャッシュデータ２５４３は、送金あるいは報酬受信されるデータである。送受信データ２５４４は、ネットワークインタフェース２５３

０を介して送受信されるデータである。入出力データ２５４５は、入出力インタフェース２１０２や２３０２を介して入出力機器と入出力するデータである。

【０１４６】

ストレージ２５５０は、ＣＰＵ２５１０が使用する、本実施形態の実現に必要な以下のデータまたはプログラムが記憶されている。データベース２５５１は、本実施形態の実現に必要な基本データを保持する。保存用ノードまたは検索用ノードのHashＩＤ記憶部２１４１／２３４１は、ノード参入時に配布されるノードＩＤである。ストレージ２１４３／２３４３は、部分データやロケーションリストを保存するストレージである。電子キャッシュ保存部２１４７／２３４７は、電子キャッシュを保存するストレージである。

【０１４７】

ストレージ２５５０には、以下のプログラムが格納される。クライアント端末制御プログラム２５５２は、保存用ノードや検索用ノードに参入したクライアント端末の全体を制御するプログラムである。保存用ノードアプリケーションプログラム２５５３は、保存用ノードとして機能する場合のアプリケーションプログラムである。検索用ノードアプリケーションプログラム２５５４は、検索用ノードとして機能する場合のアプリケーションプログラムである。

【０１４８】

入出力インタフェース２１０２／２３０２は、入出力デバイスとのデータ入出力を制御するためのインタフェースを行なう。本実施形態においては、入出力インタフェース２１０２／２３０２には、表示部２１２１／２３２１、操作部２１２２／２３２２、音声入出力部２１２３／２３２３、記憶媒体２１２４／２３２４などが接続される。

【０１４９】

なお、図２５のＲＡＭ２５４０やストレージ２５５０には、保存用ノードや検索用ノードとして機能するクライアント端末が有する汎用の機能や他の実現可能な機能に関連するプログラムやデータは図示されていない。

【０１５０】

本実施形態によれば、データおよびその分割された部分データがHash化されて、検索用ネットワークと保存用ネットワークとの独立した二層構造で管理されるため、高い安全性を担保しつつ、小規模ストレージの集合により大規模データサーバと同様の機能を実現することができる。

【０１５１】

また、本実施形態によれば、ファイルは暗号化されて部分データに分割され、ファイルは部分データから合成されて復号されるので、機密性を高めることができる。また、保存するブロック数に冗長性を持たせて保存するので、所定数以上の正常なブロックがあればデータを再現できる。また、保存時の報酬と読出時の報酬とを制御することにより、保存用ノードでの部分データの喪失を防ぐことができる。

【０１５２】

また、本実施形態によれば、インターネット上で第三者がストレージ容量を提供し、それに対して報酬を支払うことによって、効率的なインセンティブシステムによりシステム全体を維持および管理することができる。したがって、ユーザはハードディスクの空きスペースを十分に活用し、収益を得ることができる。すなわち、膨大なデータ量が発生し、これらのデータをどのように保存して、よりよいデータをどのように利用していくという問題がある中で、世界中に存在するハードディスクの大半が使用されておらず、価値のある資源が知らない間に消費されている。本実施形態においては、ユーザがソフトウェア（保存用ノードアプリケーションや検索用ノードアプリケーション）を、パソコンやスマートフォンにダウンロードあるいはインストールした後、ネットワークノード（保存用ノードおよび／または検索用ノード）になれる。したがって、ユーザは、専用のマイニングマシーンを自宅に設置することで報酬を得られることになる。

【０１５３】

また、本実施形態によれば、システムは２層の保存用ネットワークと検索用ネットワー

クとに分離されて構成され、ネットワーク効率を高める同時に、マイニング閾値を下げる。マイニングマシーンはストレージと検索の要求にとって異なり、検索には、高価なコンピューティングパワーとエネルギー消費が必要だが、ストレージには、空きストレージリソースと帯域幅資源とが必要である。ストレージと検索との分離は、低コストのマイニングマシーンを使ってススステムの運営に貢献するのに役に立つ。さらに、２層ネットワークの保存と検索とが分離されることによって、ネットワークの効率を向上させる。なお、実施形態では言及されていないが、検索用ノードは、Ｐ２Ｐネットワーク全体の中で最も見つけられ攻撃され易い部分であるので、検索ノード用に対する保護を強化する必要があり、検索用ノードのＩＰアドレスを暗号化して保護している。

【０１５４】

本実施形態によれば、ユーザのファイルデータを一定数に分割して保存し、分割された部分データが異なるノードに保存されていることを保証する。あるノードの部分データが異常な状況で消えても、他のノードのバックアップを通じて、ユーザのファイルデータを完全に復元することができる。また、保存されたデータのセキュリティを保証することができる。分散型ストレージは、戦争、自然災害、あるいは人為的な原因で発生するデータの損失を減らし、価値のあるデータを永久に保存できるように有利になる。すなわち、ファイルデータは破片に分割し、異なったノードに分布するので、データの安全性はより高く、同時に覗きされたりコピーされたりはしない。さらに、データの冗長技術を加えることによって、分割された破片データが失われた場合や、ノードがオフラインになってもとしても、完全にファイルを復元することができる。同時にある破片が復元されても、?部のデータだけなのでファイルデータ全体は保護される。なお、ノードに障害が発生してアクセス不能な場合、システムはネットワークの既存の副本を新しいノードに転送することによって、ネットワーク複製プロセスを開始して、ファイルデータを復元する。

【０１５５】

また、本実施形態によれば、保存されたデータは、デバイスによってブロックされ、暗号化されるなどの過程を経て、さらに分散型ストレージに配布され、これにより、安全性は非常に高いレベルにまで向上させて、ユーザのファイルデータはネットワーク内の他のいかなる人も覗くことができない。また、各ノードが実際に保存しているデータは、ファイルの一部分であり、その上で暗号化された方法で保存されているので、データはより安全に保護できる。ストレージノードを提供したユーザが、ファイルデータの一部分を見る機会があったとしても、意味のないデータだけであり、秘密キーを得るユーザのみが、正常にダウンロードを行うことができる。

【０１５６】

本実施形態によれば、ファイルデータをダウンロード中に、分割された破片データが再編成されるので、速度が集中型ストレージよりもはるかに速くなる。すなわち、１つのファイルが多くの破片に分散されて世界各地のストレージノードに保存されており、ユーザがファイルをダウンロードしようとすると、該当するアドレス（ハッシュ値）のみ検索するだけで、各ストレージノードから同時にデータを取得することができる。そのため、集中型ストレージよりスピードが速くなります。また、データ伝送速度に関しても、ユーザがデータを読み取る必要がある場合、全ての保存者が同時にユーザのために自分の保存したデータを送信し、アプリケーションが受信した後自動的に合成を行う。したがって、ユーザのダウンロード速度は、主にネットワークのダウンロード帯域幅により決まる。そのため、今後急激な成長を遂げる５Ｇ技術などにより更なるデータ伝送速度が達成される。

【０１５７】

また、本実施形態によれば、基準化された基盤技術のプラットフォームの提供を通じて、サポート基準ツールを、分散式資源を必要としているユーザに提供できる。このプラットフォームにより自分のＤＡＰＰ（decentralized application：分散型アプリケーション）を開発することができる。そして、サーバやＰＣ、モバイルストレージなどの集中型ストレージと比較して、本実施例のＰ２Ｐ分散型ストレージは、ストレージとインターネットの効率を向上させ、分散型技術を通じてストレージの容量とネットワークリソースの

浪費を解決した。すなわち、データの自動分配、柔軟な拡張の実現、運営コストの低減、資源浪費を避けることができた。例えば、それに対するコストは従来のクラウドストレージだと１０ＴＭ（Translation Memory）あたり月間コストは１００ドルですが、本実施形態のＰ２Ｐ分散型ストレージに以降することによって月間コストを１／５に抑えることができた。

【０１５８】

さらに詳細には、例えば、ＤＨＴ（Distributed Hash Table：分散型ハッシュテーブル）を用いることで、Hashキー値によってユニークと識別することできる情報を、ある条件/プロトコルに従って複数のノードに保存される。これにより中央集権型サーバなどの単一故障状態でネットワーク全体が麻痺することを効果的に避けることができる。中央ノードサーバと違って、ＤＨＴによるネットワーク内の各ノードはネットワーク全体の情報を維持する必要がなく、隣接する後続ノード情報を保存するだけなので、帯域幅の占有および資源消費を大幅に減少する。また、ＤＨＴによるネットワークはキーワードの最も近いノードに冗長データもバックアップし、単一ノードの障害を回避できる。

【０１５９】

［第４実施形態］

次に、本発明の第４実施形態に係る情報処理システムについて説明する。本実施形態に係る情報処理システムは、上記第３実施形態と比べると、それぞれ独立したクライアント端末とクライアントアプリケーションを有するアプリケーションサーバとを有する点で異なる。その他の構成および動作は、第２実施形態と同様であるため、同じ構成および動作については同じ符号を付してその詳しい説明を省略する。

【０１６０】

《情報処理システムの構成》

図２６は、本実施形態に係る情報処理システム２６００の構成を示すブロック図である。図２６においては、情報処理システム２６００がアプリケーションサーバ２６３３を備え、アプリケーションサーバ２６３３が、データ保存処理、リスト保存処理、リスト検索処理およびデータ取得処理を含む処理を実行する。

【０１６１】

図２６においては、クライアントアプリケーション２３２がアプリケーションサーバ２６３３に変更されている。

【０１６２】

なお、図２や図２６においては、クライアントアプリケーション２３２やアプリケーションサーバ２６３３のそれぞれがファイルの保存や取得の全機能を果たすように図示しているが、これらの機能をクライアント端末２０３の処理能力に応じて振り分けるよう構成してもよい。

【０１６３】

本実施形態によれば、処理能力の比較的低いクライアント端末であっても、あるいは、通信能力が比較的低いシステムであっても、ファイルの分散保存とその読み出し再生を行う情報処理システムが実現できる。

【０１６４】

［第５実施形態］

次に、本発明の第５実施形態に係る情報処理システムについて説明する。本実施形態に係る情報処理システムは、上記第３実施形態および第４実施形態と比べると、クライアント端末、保存用ノードおよび検索用ノードが既存のＩＰアドレスを用いたＨＴＴＰに代わるＨａｓｈアドレスを用いたプロトコルで通信する点で異なる。その他の構成および動作は、第３実施形態または第４実施形態と同様であるため、同じ構成および動作については同じ符号を付してその詳しい説明を省略する。

【０１６５】

《情報処理システムの構成》

図２７は、本実施形態に係る情報処理システム２７００の構成を示すブロック図である

。図２７においては、Ｈａｓｈアドレスを用いたプロトコルをＩＰＷＢで示している。すなわち、プロトコルとしてIPWB://…を用いている。

【０１６６】

図２７の情報処理システム２７００においては、保存用ネットワーク２７０１と、検索用ネットワーク２７０２と、クライアントアプリケーション２７３２との間において、IPWB://…で表現されるHashアドレスによるＰ２Ｐ通信が可能となっている。

【０１６７】

本実施形態によれば、非集権分散ネットワークによる分散型ストレージが実現される。すなわち、本実施形態は、多数のＰ２Ｐ接続を同時に転送することができる。このような動的な柔軟性と展延性により、システムのスケーラビリティが拡張上限なしに実現する。そして、将来的に、本実施形態のシステムは、Ｐ２Ｐ分散型クラウドストレージのみの提供だけではなく、そのストレージを利用したWebページを開設することも可能になる。すなわち、本実施形態が提供するプラットフォームにおいては、ユーザ自らがＰ２Ｐ分散ストレージのサービス事業者になることができる。サービス事業者は、本実施形態のブロックチェーンを利用し、独自サービスの決済で利用するトークンを発行することができる。そして、トークンの発行者は、ストレージの利用料金体系や、ストレージ容量提供者への報酬体系を自由に設定することにより、サービスにオリジナリティを出すこともできる。

【０１６８】

［他の実施形態］

以上、実施形態を参照して本願発明を説明したが、本願発明は上記実施形態に限定されるものではない。本願発明の構成や詳細には、本願発明の技術的範囲で当業者が理解し得る様々な変更をすることができる。また、それぞれの実施形態に含まれる別々の特徴を如何様に組み合わせたシステムまたは装置も、本発明の技術的範囲に含まれる。

【０１６９】

また、本発明は、複数の機器から構成されるシステムに適用されてもよいし、単体の装置に適用されてもよい。さらに、本発明は、実施形態の機能を実現する情報処理プログラムが、システムあるいは装置に供給され、内蔵されたプロセッサによって実行される場合にも適用可能である。したがって、本発明の機能をコンピュータで実現するために、コンピュータにインストールされるプログラム、あるいはそのプログラムを格納した媒体、そのプログラムをダウンロードさせるＷＷＷ(World Wide Web)サーバも、プログラムを実行するプロセッサも本発明の技術的範囲に含まれる。特に、少なくとも、上述した実施形態に含まれる処理ステップをコンピュータに実行させるプログラムを格納した非一時的コンピュータ可読媒体（non-transitory computer readable medium）は本発明の技術的範囲に含まれる。

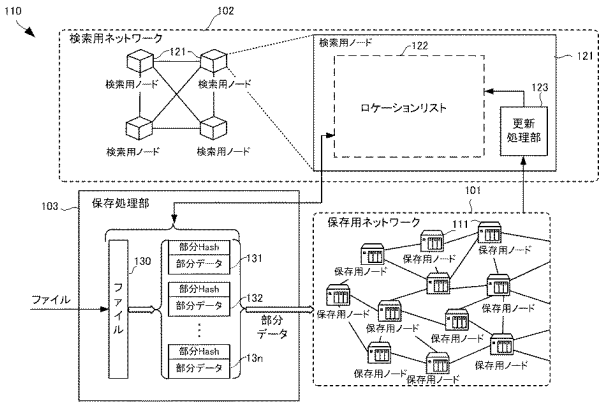
【要約】

【課題】高い安全性を担保しつつ、小規模ストレージの集合により大規模データサーバと同様の機能を実現すること。

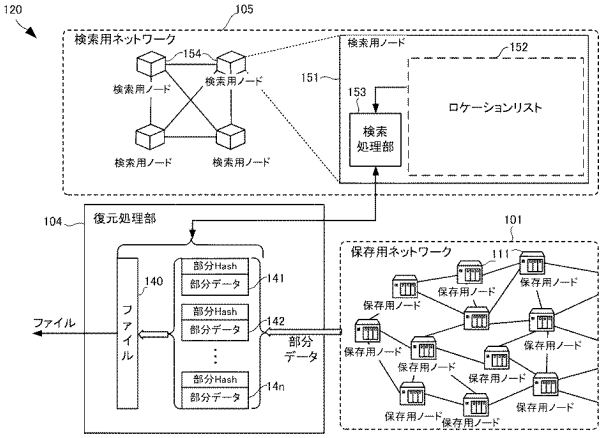
【解決手段】ファイルを分散保存するための複数の保存用ノードを含む保存用ネットワークと、複数の保存用ノードのロケーションを含むロケーションリストをブロックチェーン化しつつ保存する検索用ノードを複数含む検索用ネットワークと、ファイルを複数の部分データに分割し、複数の部分データのそれぞれを複数の保存用ノードに含まれる少なくとも２つの保存用ノードに送信して保存させる保存処理部と、を備え、検索用ノードは、前記部分データを保存した前記保存用ノードの識別情報を用いて、ロケーションリストを更新する更新処理部を備えた。

【選択図】　図１Ａ

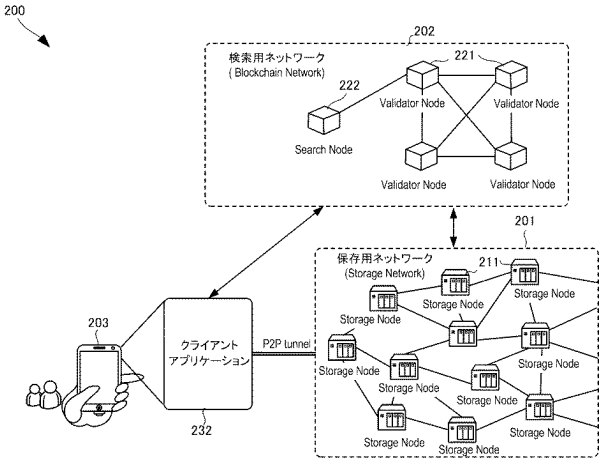
【図１Ａ】



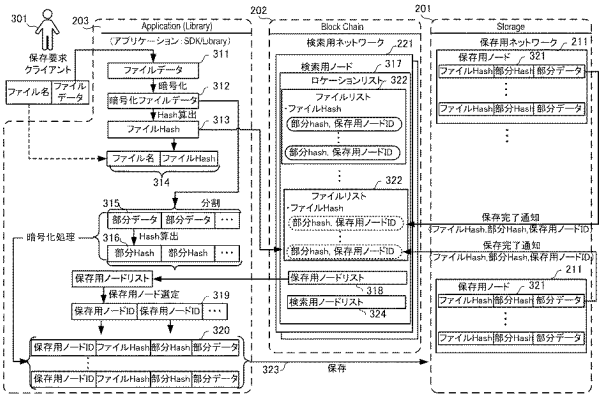
【図１Ｂ】



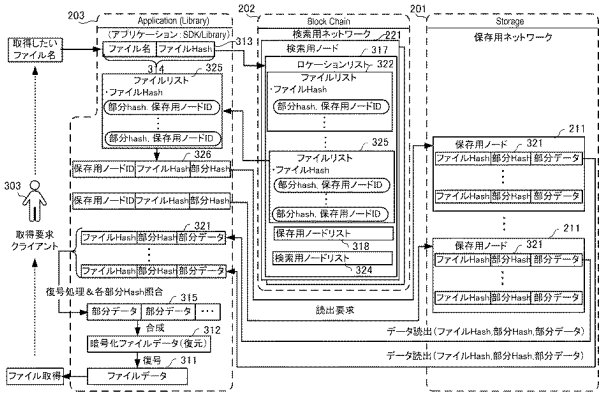
【図２】



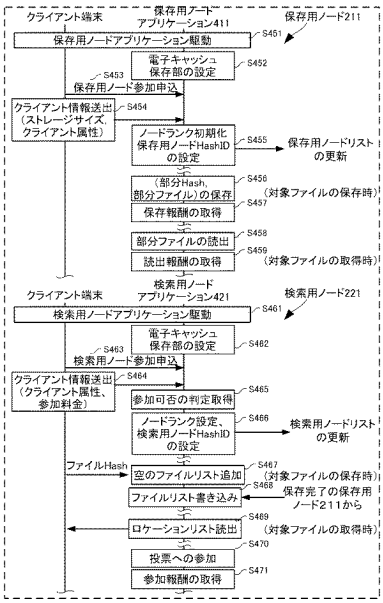
【図３Ａ】



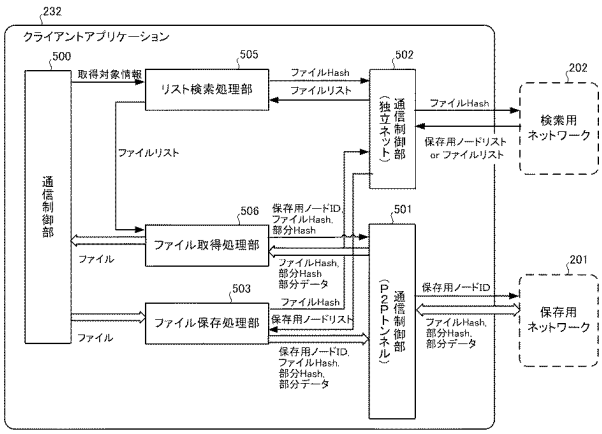
【図３Ｂ】


Application (Library)
Block Chain
Storage
検索用ネットワーク
保存用ネットワーク
取得したい
ファイル名
ファイル名
ファイルHash
検索用ノード
ロケーションリスト
ファイルリスト
・ファイルHash
部分hash, 保存用ノードID
保存用ノードリスト
検索用ノードリスト
保存用ノード
ファイルHash
部分Hash
部分データ
取得要求
クライアント
復号処理＆各部分Hash照合
部分データ
合成
暗号化ファイルデータ（復元）
復号
ファイルデータ
ファイル取得
読出要求
データ読出（ファイルHash,部分Hash,部分データ）
データ読出（ファイルHash,部分Hash,部分データ）

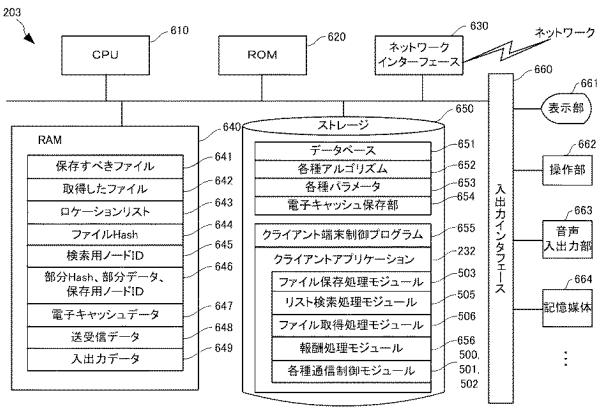
【図４】


クライアント端末
保存用ノード
アプリケーション411
保存用ノード211
保存用ノードアプリケーション駆動
電子キャッシュ
保存部の設定
保存用ノード参加申込
クライアント情報送出
（ストレージサイズ、
クライアント属性）
ノードランク初期化
保存用ノードHashIDの設定
保存用ノードリストの更新
（部分Hash、
部分ファイル）の保存
（対象ファイルの保存時）
保存報酬の取得
部分ファイルの読出
読出報酬の取得
（対象ファイルの取得時）
検索用ノード
アプリケーション421
検索用ノード221
検索用ノードアプリケーション駆動
検索用ノード参加申込
クライアント情報送出
（クライアント属性、
参加料金）
参加可否の判定取得
ノードランク設定、
検索用ノードHashIDの設定
検索用ノードリストの更新
ファイルHash
空のファイルリスト追加
（対象ファイルの保存時）
ファイルリスト書き込み
保存完了の保存用
ノード211から
ロケーションリスト読出
（対象ファイルの取得時）
投票への参加
参加報酬の取得

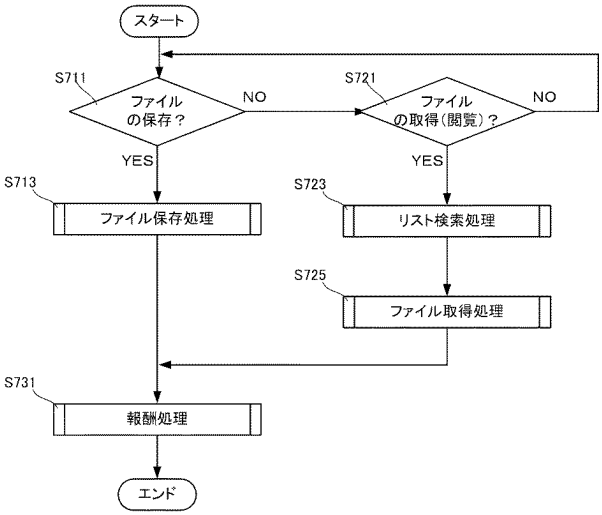
【図５】


クライアントアプリケーション
通信制御部
取得対象情報
リスト検索処理部
ファイルHash
ファイルリスト
通信制御部
（独立ネット）
検索用
ネットワーク
保存用ノードリスト
or ファイルリスト
ファイル取得処理部
保存用ノードID,
ファイルHash,
部分Hash
ファイル
ファイル保存処理部
保存用ノードリスト
通信制御部
（P2Pトンネル）
保存用
ネットワーク
保存用ノードID
ファイルHash,
部分Hash,
部分データ

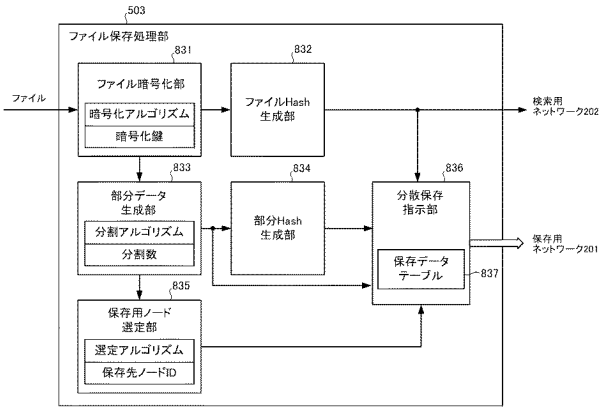
【図６】


CPU
ROM
ネットワーク
インターフェース
ネットワーク
RAM
保存すべきファイル
取得したファイル
ロケーションリスト
ファイルHash
検索用ノードID
部分Hash、部分データ、
保存用ノードID
電子キャッシュデータ
送受信データ
入出力データ
ストレージ
データベース
各種アルゴリズム
各種パラメータ
電子キャッシュ保存部
クライアント端末制御プログラム
クライアントアプリケーション
ファイル保存処理モジュール
リスト検索処理モジュール
ファイル取得処理モジュール
報酬処理モジュール
各種通信制御モジュール
入出力インタフェース
表示部
操作部
音声
入出力部
記憶媒体

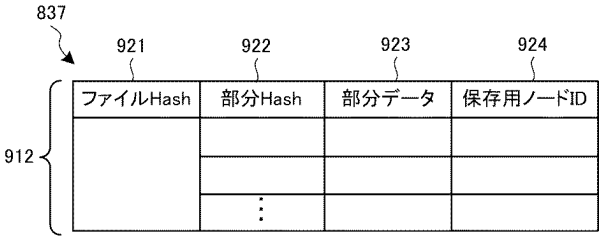
【図７】


スタート
S711
ファイル
の保存？
NO
S721
ファイル
の取得（閲覧）？
NO
YES
YES
S713
ファイル保存処理
S723
リスト検索処理
S725
ファイル取得処理
S731
報酬処理
エンド

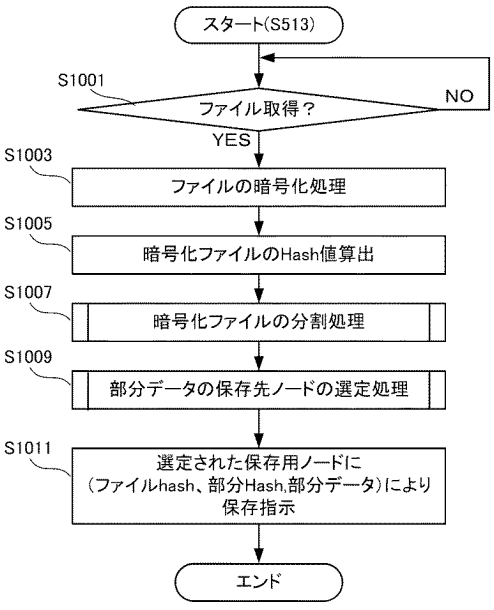
【図８】


503
ファイル保存処理部
831
ファイル暗号化部
暗号化アルゴリズム
暗号化鍵
832
ファイルHash
生成部
ファイル
検索用
ネットワーク202
833
部分データ
生成部
分割アルゴリズム
分割数
834
部分Hash
生成部
836
分散保存
指示部
保存データ
テーブル
837
保存用
ネットワーク201
835
保存用ノード
選定部
選定アルゴリズム
保存先ノードID

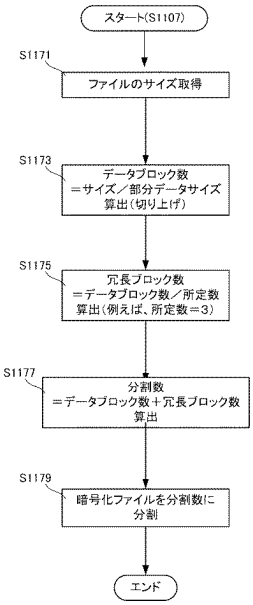
【図９】


837
921
922
923
924
912
ファイルHash
部分Hash
部分データ
保存用ノードID

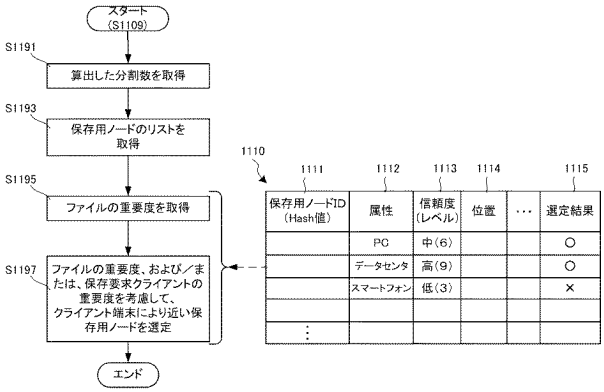
【図１０】


スタート(S513)
S1001
ファイル取得？
NO
YES
S1003
ファイルの暗号化処理
S1005
暗号化ファイルのHash値算出
S1007
暗号化ファイルの分割処理
S1009
部分データの保存先ノードの選定処理
S1011
選定された保存用ノードに
（ファイルhash、部分Hash,部分データ）により
保存指示
エンド

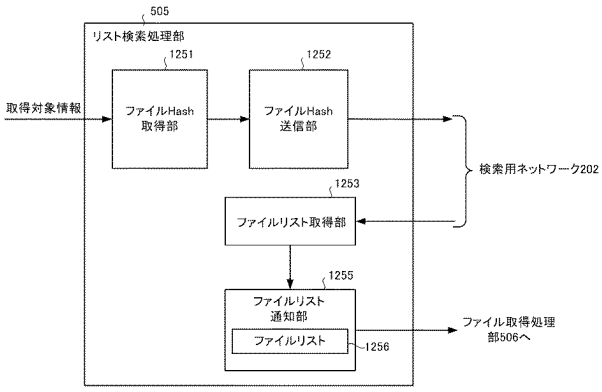
【図１１Ａ】



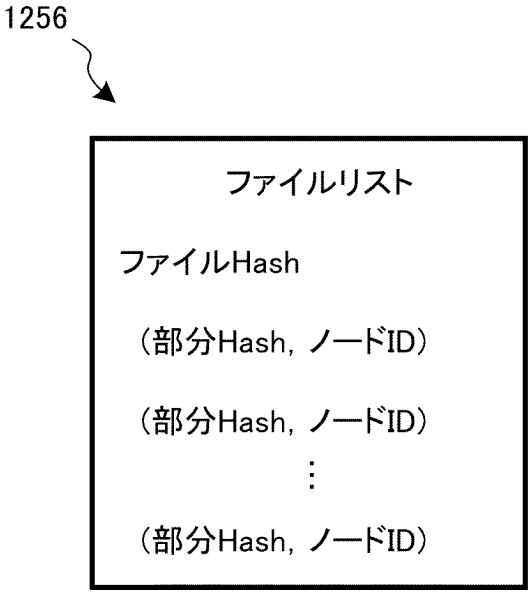
【図１１Ｂ】



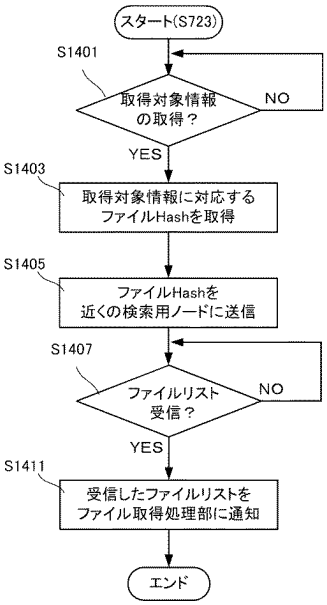
【図１２】



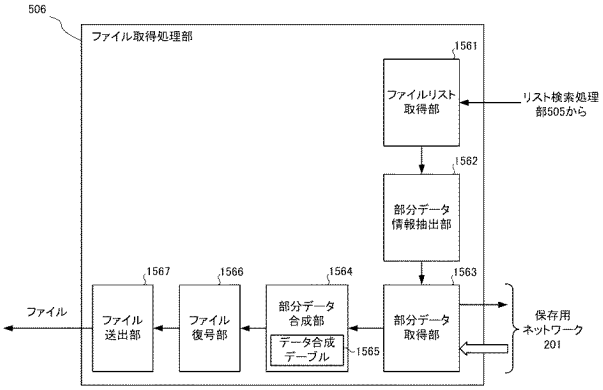
【図１３】



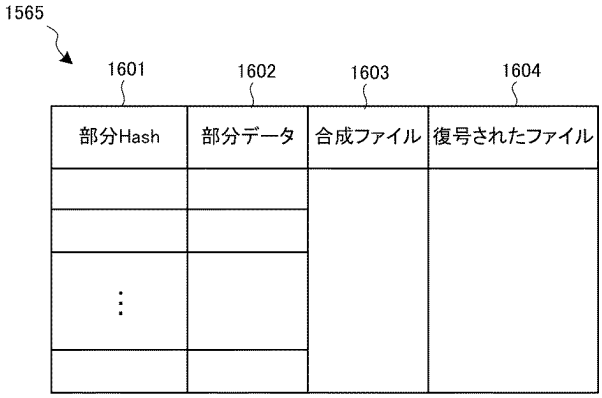
【図１４】



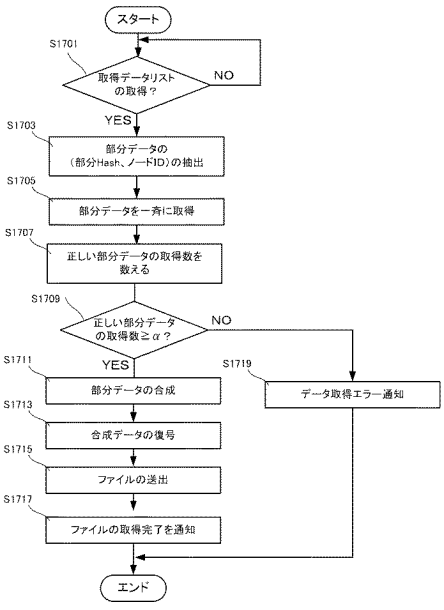
【図１５】



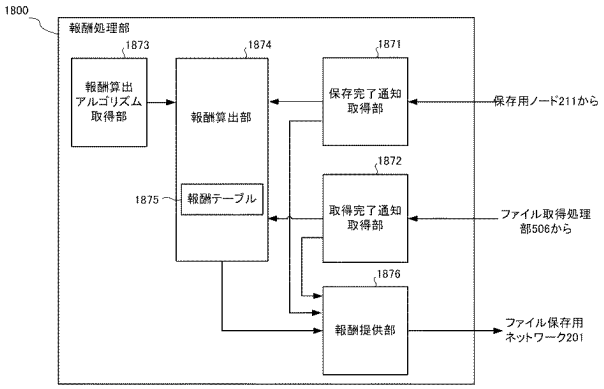
【図１６】



【図１７】



【図１８】

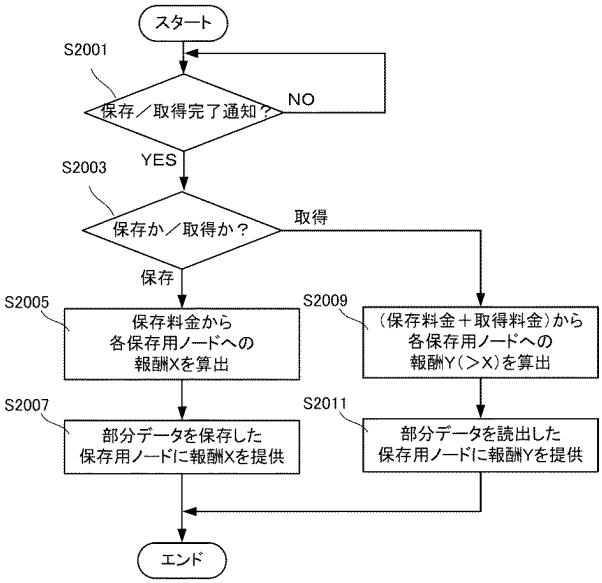


【図１９】

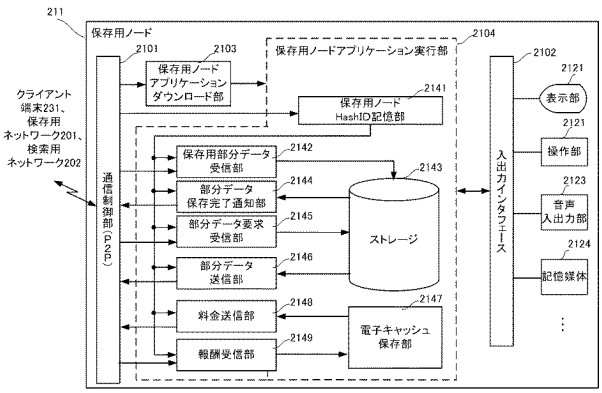
1875

1901 データID（Hash）	1902 保存料金	1903 （取得（閲覧）料金×回数）	1904 データ保存時報酬	1905 データ読出時報酬 初期値	1905 データ読出時報酬 変化曲線	…
⋮						

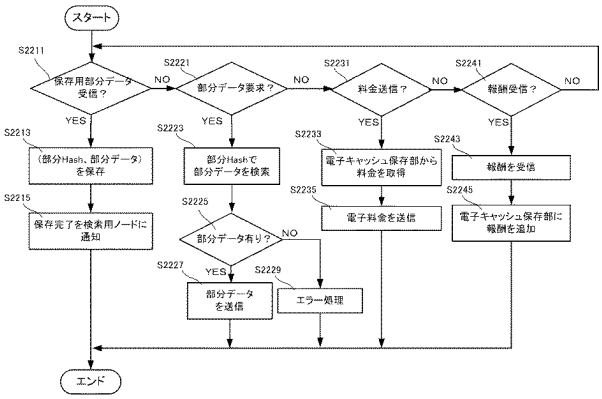
【図２０】



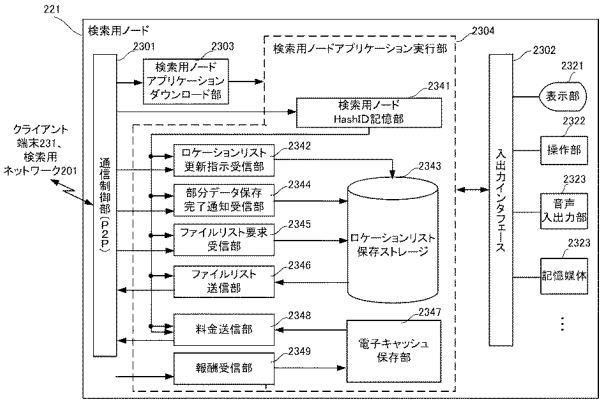
【図２１】



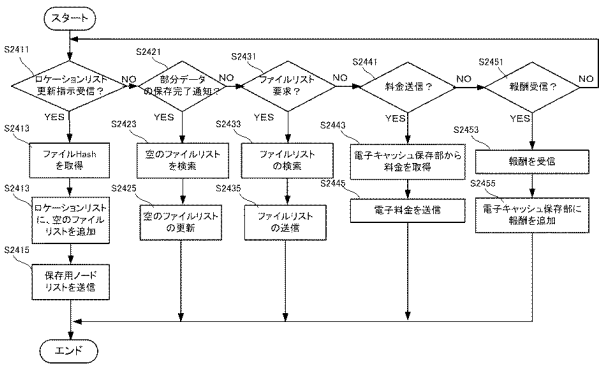
【図２２】



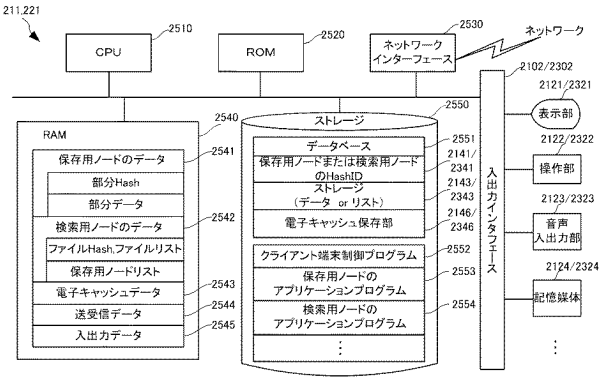
【図２３】



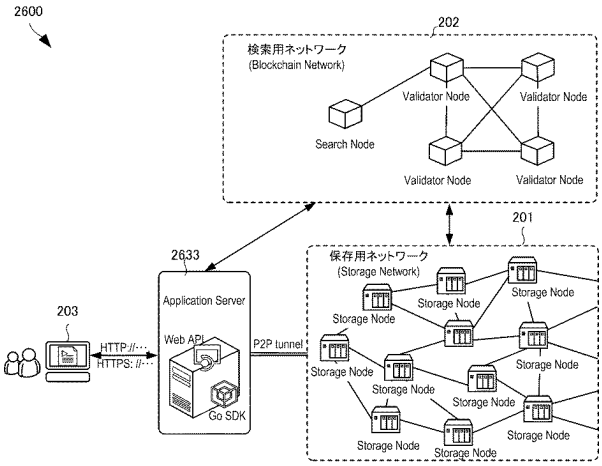
【図２４】



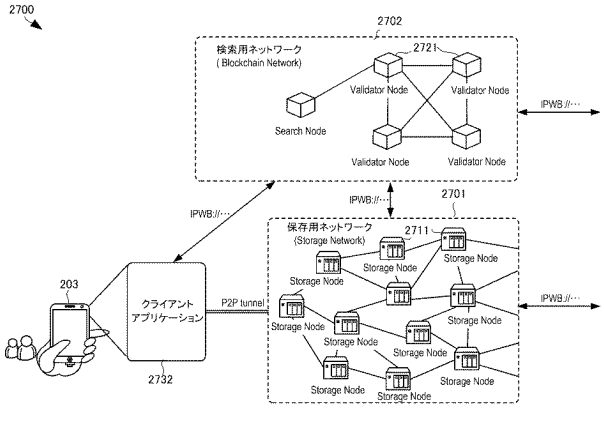
【図２５】



【図２６】


2600
202
検索用ネットワーク
(Blockchain Network)
Validator Node
Validator Node
Search Node
Validator Node
Validator Node
201
2633
保存用ネットワーク
(Storage Network)
Application Server
Storage Node
203
Web API
HTTP://…
HTTPS://…
P2P tunnel
Go SDK

【図２７】


2700
2702
検索用ネットワーク
(Blockchain Network)
2721
Validator Node
Validator Node
Search Node
Validator Node
Validator Node
IPWB://…
2701
保存用ネットワーク
(Storage Network)
2711
Storage Node
203
クライアント
アプリケーション
2732
P2P tunnel

フロントページの続き

(56)参考文献　特開２０１８－１９０２２７（ＪＰ，Ａ）
米国特許出願公開第２０１９／０１７９８０１（ＵＳ，Ａ１）
木下　学，ブロックチェーンと連携する「Ｐ２Ｐストレージ」　イーサリアムの「Ｓｗａｒｍ」を使ってみよう，日経ソフトウエア　第２１巻　第５号，日本，日経ＢＰ社，２０１８年　７月２４日，p.040～049

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　１６／１８２