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

特許第6533771号
(P6533771)

(45)発行日　令和1年6月19日(2019.6.19)　(24)登録日　令和1年5月31日(2019.5.31)

(51)Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F	21/62	318
G06F 13/00	(2006.01)	G06F	13/00	520D
G06F 16/14	(2019.01)	G06F	16/14	
G06F 21/64	(2013.01)	G06F	21/64	
G06F 21/44	(2013.01)	G06F	21/44	

請求項の数 7　(全 31 頁)　最終頁に続く

(21)出願番号　特願2016-222778(P2016-222778)
(22)出願日　平成28年11月15日(2016.11.15)
(65)公開番号　特開2018-81464(P2018-81464A)
(43)公開日　平成30年5月24日(2018.5.24)
審査請求日　平成30年7月6日(2018.7.6)

早期審査対象出願

(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　100074099
弁理士　大菅　義之
(74)復代理人　100157967
弁理士　菅田　洋明
(74)復代理人　100150315
弁理士　松林　出
(74)復代理人　100196656
弁理士　佐藤　康平
(74)代理人　100133570
弁理士　▲徳▼永　民雄

最終頁に続く

(54)【発明の名称】通信方法、装置、及びプログラム

(57)【特許請求の範囲】
【請求項１】
分散ファイル共有ネットワークに含まれるノード装置が通信プログラムを実行することによって、
端末が有するデータに関する情報を前記分散ファイル共有ネットワークに保持させ、
前記データを指定したブロックチェーンのトランザクションをファイル閲覧トランザクションとして発行し、
前記ファイル閲覧トランザクションの発行を契機に、前記データに関する情報に基づいて前記データを取得する、
ことを特徴とする通信プログラム。
【請求項２】
前記データに関する情報は、ブロックチェーンネットワークでの承認結果を用いて前記分散ファイル共有ネットワークに保持されることを特徴とする請求項１に記載の通信プログラム。
【請求項３】
前記データに関する情報は、前記データのアドレス情報を含み、
前記データのアドレス情報に前記データに対応するサービス内容を含む情報を紐付けた情報は、前記データに関する情報として前記分散ファイル共有ネットワークに保持される、ことを特徴とする請求項１または２に記載の通信プログラム。
【請求項４】

前記データのアドレス情報が前記分散ファイル共有ネットワークに保持される時のデータ履歴を、前記ブロックチェーンによって管理する、ことを特徴とする請求項３に記載の通信プログラム。

【請求項５】

前記ノード装置が、前記分散ファイル共有ネットワークへのアクセス時のアクセス履歴を、前記ブロックチェーンによって管理する、ことを特徴とする請求項１乃至４のいずれかに記載の通信プログラム。

【請求項６】

分散ファイル共有ネットワークに含まれるノード装置であって、

端末が有するデータに関する情報を前記分散ファイル共有ネットワークに保持させるための処理を行う処理部と、

前記データを指定したブロックチェーンのトランザクションをファイル閲覧トランザクションとして発行する発行部と、

前記ファイル閲覧トランザクションの発行を契機に、前記データに関する情報に基づいて前記データを取得する取得部

を有することを特徴とするノード装置。

【請求項７】

分散ファイル共有ネットワークに含まれるノード装置が実行する通信方法であって、

端末が有するデータに関する情報を前記分散ファイル共有ネットワークに保持させ、

前記データを指定したブロックチェーンのトランザクションをファイル閲覧トランザクションとして発行し、

前記ファイル閲覧トランザクションの発行を契機に、前記データに関する情報に基づいて前記データを取得する、

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】

分散ファイル共有ネットワークにおいてファイルを通信する通信方法、装置、及びプログラムに関する。

【背景技術】

【０００２】

クライアント端末やＩｏＴ（Ｉｎｔｅｒｎｅｔ ｏｆ Ｔｈｉｎｇｓ）デバイス間のピアツーピア通信により、電子ファイルの情報を共有する分散ファイル共有技術が提案されている。電子ファイルのフォーマットとしては、ＨＴＭＬ（Ｈｙｐｅｒ Ｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）やＰＤＦ（Ｐｏｒｔａｂｌｅ Ｄｏｃｕｍｅｎｔ Ｆｏｒｍａｔ）等が使用される。

【０００３】

分散ファイル共有技術の具体的な実装例として、インタープラネタリーファイルシステム（ＩＰＦＳ：Ｉｎｔｅｒｐｌａｎｅｔａｒｙ Ｆｉｌｅ Ｓｙｓｔｅｍ）が知られている。ＩＰＦＳは、ピアツーピア通信による分散ファイル共有システムを、ＷＷＷ（Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂ）サービスとして拡張した分散ＷＥＢ技術で、Ｊｕａｎ Ｂｅｎｅｔが２０１５年に発表し、オープンソース化されているソフトウェア技術である。ＩＰＦＳは、分散された環境下でＨＴＴＰ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）通信方式によるファイルアクセスを可能にする。更に、ＩＰＦＳでは、ＨＴＴＰのサーバアドレスではなく、コンテンツに対して一意のハッシュ値アドレスが割り当てられ、以下の例のようなハッシュ値を指定したＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）の形式でアドレス指定が行われる。

コンテンツアドレス例：QmRvPJi7GmNAFbJnVeEEhMCGtJsDEaJYVa4a52J9bqn1AN

アドレス指定方法：

http://localhost:8080/ipfs/QmRvPJi7GmNAFbJnVeEEhMCGtJsDEaJYVa4a52J9bqn1AN/

【０００４】
これにより、ＩＰＦＳでは、高速なコンテンツファイルの検索と取得が可能になる。ＩＰＦＳは、従来のクラウド等に配備されたサーバによるコンテンツ配信やネットワークリソース浪費や耐障害性の問題を解決することが可能であり、サーバレスのコンテンツ配信技術として、分散されたクライアントだけで永続的にコンテンツを提供できる。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１１－７０５５７号公報
【特許文献２】特開２０１３－１０５２２７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかし、上述した従来の分散ファイル共有システムでは、ファイル発行やアクセスに関するユーザに紐づいた認証の仕組みがなく、アプリケーションさえインストールすれば、分散ファイル共有ネットワークにアクセスできてしまうという課題があった。
【０００７】
そこで、本発明の１つの側面では、分散ファイル共有システムにおいて、高セキュアなファイル共有空間を構築することを目的とする。
【課題を解決するための手段】
【０００８】
態様の一例では、分散ファイル共有ネットワークに含まれるノード装置が実行する通信方法であって、端末で発生したイベントに関する情報をブロックチェーンを用いて前記分散ファイル共有ネットワークに含まれるノード装置間で共有し、イベントに関する情報を含むファイルを生成し、生成されたファイルを分散ファイル共有ネットワークに含まれるいずれかのノード装置で保持する。
【発明の効果】
【０００９】
分散ファイル共有システムにおいて、高セキュアなファイル共有空間を構築することが可能となる。
【図面の簡単な説明】
【００１０】
【図１】本実施形態が対象とするユースケースの例を示す図である。
【図２】ＩＰＦＳ等の分散ファイル共有システムにおいて高セキュアな情報共有サービスをクラウドサービスによって実現する構成例を示す図である。
【図３】本実施形態の基本概念の説明図である。
【図４】ブロックチェーンの説明図である。
【図５】本実施形態における通信システムの構成例を示す図である。
【図６】ファイル発行の処理例を示すシーケンス図である。
【図７】ファイル発行の処理例で使用されるトランザクションのデータフォーマット例を示す図である。
【図８】ポータルファイルのデータフォーマット例を示す図である。
【図９】ファイル発行の他の処理例を示すシーケンス図である。
【図１０】ファイルアクセスの処理例を示すシーケンス図である。
【図１１】ファイルアクセスの処理例で使用されるトランザクションのデータフォーマット例を示す図である。
【図１２】本実施形態のハードウェア構成例を示す図である。
【図１３】ファイル発行の処理例を示すフローチャートである。
【図１４】ファイル発行の他の処理例を示すフローチャートである。
【図１５】ファイルアクセスの処理例を示すフローチャートである。

【発明を実施するための形態】
【００１１】
以下、本発明を実施するための形態（以下、「本実施形態」と記載）について図面を参照しながら詳細に説明する。図１は、本実施形態が対象とするユースケースの例を示す図である。本実施形態は、ノード装置の一つであるクライアント端末やＩｏＴデバイスのピアツーピア通信により、ＨＴＭＬ、ＰＤＦやテキスト等の電子ファイル情報を共有する分散ファイル共有技術を用いて、次のようなサービスを実現するものである。例えば図１（ａ）のように、各ＩｏＴデバイスから収集される情報ＡからＥが、各ＩｏＴデバイス１０３と一体の又は分離した各ＩｏＴゲートウェイで形成される分散ファイル共有ネットワーク１０１上で自律的にＷＥＢサービス化され、共有される。或いは図１（ｂ）のように、サプライチェーン上の原材料・部品の調達から、製造、在庫管理、販売、配送までの製品の工程情報ＡからＥが、流通に関わる組織のクライアント端末１０４で形成される分散ファイル共有ネットワーク１０１上で共有される。分散ファイル共有ネットワーク上で共有される情報は、ユーザの端末から任意に状況確認１０２を行うことができる。
【００１２】
本実施形態における分散ファイル共有ネットワーク１０１は例えば、前述したＩＰＦＳによって実現される。しかし、ＩＰＦＳでは、以下のような課題がある。
【００１３】
１．ファイル発行やアクセスに関するユーザに紐づいた認証の仕組みがなく、アプリケーションさえインストールすれば、分散ファイル共有ネットワークにアクセスできてしまう。
【００１４】
２．ハッシュ値によるアドレッシングとアドレス指定によるファイル検索機能はあるものの、サービスとアドレスの関係を一元管理するリポジトリ機能やＷＥＢアクセスやデータ履歴（ログ）等を管理できる機能はない。
【００１５】
３．誰でも、また、どこでもＷＥＢファイルを登録でき、コンテンツの一意性を保証できる機能はない。
【００１６】
上述のＩＰＦＳなどは、例えばインターネット上で、あらゆるＩｏＴゲートウェイ又はクライアント端末によってファイルを共有することを主眼として開発された分散ファイル共有システムである。このような分散ファイル共有システム上で、ユーザ認証と、ファイル登録やファイルアクセスの証跡（ログ）が管理された高セキュアな情報共有サービスを実現するためには、次のような機能が必要となる。まず、ユーザによるファイル発行やファイルアクセスに関するユーザ認証の機能が必要となる。また、ファイル発行者であるコンテンツの一意性を保証する機能が必要となる。更に、ファイル登録やアクセスログを管理する機能が必要となる。加えて、ファイルによって提供するサービス情報とアドレスの関係を一元管理する機能が必要となる。
【００１７】
図２は、ＩＰＦＳ等の分散ファイル共有システムにおいて高セキュアな情報共有サービスをクラウドサービスによって実現する構成例を示す図である。この構成例では、クライアント端末２２２やＩｏＴゲートウェイ２２１によって構成されるＩＰＦＳによる閉域ネットワークである分散ＷＥＢネットワーク２０１に対して、インターネット又はキャリアネットワーク２０３を介して、クラウドサービスが提供される。このクラウドサービス２０２は、以下のような機能のサービスを提供する。
【００１８】
１．認証機能：アクセスやデータ履歴（ログ）管理を提供するサービスである。例えば、ＲＡＤＩＵＳ（Ｒｅｍｏｔｅ Ａｕｔｈｅｎｔｉｆｉｃａｔｉｏｎ Ｄｉａｌ Ｉｎ Ｕｓｅｒ Ｓｅｒｖｉｃｅ）サーバ２０１によって、ネットワーク利用可否（認証）と利用事実の記録（アカウンティング）を実行するサービスが提供される。

【００１９】
２．サービスリポジトリ機能：ＷＥＢポータルサイトのようなポータルサーバ２１２によって、サービスとＵＲＬの関係を管理するサービスが提供される。
【００２０】
３．コンテンツの一意性の保証機能：コンテンツが登録される際に、サーバ２１３によって、ライセンスコードやコンテンツＩＤ（識別子）を発行すると共に、コンテンツファイルに記載することで、該当ファイルの一意性を保証するサービスが提供される。
【００２１】
４．ログ管理機能：サーバ２１４によって、ファイル登録やファイルアクセスのログを記録するサービスが提供される。
【００２２】
しかし、図２に示されるように、ＩＰＦＳのような分散ファイル共有システムに対して上述の１から４の機能をクラウドサービス２０２で実現した場合、次のような課題が生じる。分散ＷＥＢネットワーク２０１とクラウドサービス２０２とを結ぶインターネット又はキャリアネットワーク２０３内でやり取りされるトラフィック量が増大する。この結果、クライアント端末２２２やＩｏＴゲートウェイ２２１などのエッジノードで実現するサーバレスの処理、即時ファイル共有といった分散ファイル共有システムの利点が享受されないという課題が生じる。
【００２３】
そこで、以下に説明する本実施形態では、分散ファイル共有システムを維持したまま、アクセス認証やファイルのコンテンツの一意性の保証、アクセスログやファイル登録の証跡情報の管理をサポートし、高セキュアなファイル共有システムを実現する。図３は、本実施形態の基本概念の説明図である。
【００２４】
本実施形態はまず、ＩＰＦＳに代表されるピアツーピア型通信で実現する分散ファイル共有ネットワーク上で、前述した４つの機能が分散環境のもとで実現される。そのため本実施形態では、ブロックチェーンと呼ばれる通信方法が利用される。本実施形態では、端末で発生したイベントに関する情報が、ブロックチェーンを用いて分散ファイル共有ネットワークに含まれるノード装置間で共有される。そして、そのイベントに関する情報を含むファイルが生成され、このファイルを分散ファイル共有ネットワークのいずれかのノード装置で保持する。これにより、分散環境でのトランザクション(取引)の認証と正当性保証、及び改ざん不能な取引履歴管理の機能が応用され拡張される。概念的には本実施形態では、図３（ａ）に示されるように、各ノード３０７は、分散ファイル共有ネットワーク３０１と通信を行うときに、まず、ブロックチェーンの拡張により実現される分散型の認証／証跡管理ネットワーク３０２にアクセスする。その後、認証／証跡管理ネットワーク３０２に包含されるように構成される分散ファイル共有ネットワーク３０１へのアクセスが行われる。
【００２５】
より具体的には、本実施形態は、図３（ｂ）に示される構成を有する。図３（ｂ）の構成では、ＩｏＴゲートウェイ３０５又はクライアント端末３０６に、ブロックチェーンアプリケーション３０３（図中「ＢＣ」）がインストールされる。このブロックチェーンアプリケーション３０３は、ブロックチェーンによるトランザクションを処理するソフトウェアである。ＩｏＴゲートウェイ３０５又はクライアント端末３０６で動作するブロックチェーンアプリケーション３０３により、認証／証跡管理ネットワーク３０２が形成される。また、ＩｏＴゲートウェイ３０５又はクライアント端末３０６には、ＩＰＦＳアプリケーション３０４（図中「ＩＰＦＳ」）がインストールされる。このＩＰＦＳアプリケーション３０４は、分散ファイル共有ネットワーク３０１に対するファイルの登録（保持）又はアクセスの機能を提供するソフトウェアである。ＩｏＴゲートウェイ３０５又はクライアント端末３０６で動作するＩＰＦＳアプリケーション３０４により、分散ファイル共有ネットワーク３０１が形成される。以下、クライアント端末とは、クライアントが操作

する端末あるいはクライアントそのものを指すものとする。

【００２６】

本実施形態において、ＩｏＴゲートウェイ３０５でセンサ検知等のイベントが発生し又は受信され、それに対応するイベント情報（イベントに関する情報）のファイル登録要求が発生すると、まず、ＩｏＴゲートウェイ３０５でブロックチェーンアプリケーション３０３が実行される。このブロックチェーンアプリケーション３０３は、ＩＰＦＳアプリケーション３０４を実行することにより、ＩＰＦＳアプリケーション３０４に、分散ファイル共有ネットワーク３０１へのイベント情報ファイルの登録を実行させる。このとき、ＩｏＴゲートウェイ３０５で動作するブロックチェーンアプリケーション３０３は、ＩｏＴゲートウェイ３０５のユーザに対する認証や、コンテンツの一意性の保証、サービスリポジトリ、データ履歴（ログ）管理（証跡管理）等の機能を実行する。これにより、イベント情報ファイルの分散ファイル共有ネットワーク３０１への登録が、高セキュアに実行される。

【００２７】

また、本実施形態において、クライアント端末３０６からファイル閲覧要求が発生すると、そのクライアント端末３０６でブロックチェーンアプリケーション３０３が実行される。このブロックチェーンアプリケーション３０３は、ＩＰＦＳアプリケーション３０４を実行することにより、ＩＰＦＳアプリケーション３０４に、分散ファイル共有ネットワーク１０１へのファイル要求処理を実行させる。このとき、クライアント端末３０６で動作するブロックチェーンアプリケーション３０３は、クライアント端末３０６のユーザ又はユーザが属するグループに対する認証や、ファイルのアクセス制御、アクセスログ管理（証跡管理）等の機能を実行する。これにより、分散ファイル共有ネットワーク３０１上のファイル閲覧が、高セキュアに実行される。

【００２８】

以上の図３（ｂ）に関する説明のように、本実施形態では、ブロックチェーンアプリケーション３０３が、ＩＰＦＳアプリケーション３０４を介して分散ファイル共有ネットワーク３０１にアクセスするためのプロキシとして動作する。これにより、高セキュアな分散ファイル共有の閉域ネットワーク空間が構築される。

【００２９】

ここで、ブロックチェーンとは、ユーザ間で 『情報(台帳)』 を共有する技術であり、様々な取引情報(トランザクション)を記した台帳を公開し、ユーザ全員でその正当性をチェックすることで、不正の無い契約を遂行する分散台帳システムである。

【００３０】

図４は、ブロックチェーンの説明図である。ブロックチェーンでは、電子証明書の技術を使ってユーザ認証が行われる。ユーザが最初にブロックチェーンにアカウント登録した時点で、図４（ａ）に示されるように、まず秘密鍵とその秘密鍵に対応する公開鍵が生成され、更にユーザＩＤが生成されて、ユーザに対して発行される。更に、これらの秘密鍵及び公開鍵に基づいて、電子証明書がユーザに対して発行される。ブロックチェーンは、この電子証明書を持っているユーザがブロックチェーンを使うことができるという認証の機能を有している。本実施形態では、この認証の機能を活用する。

【００３１】

ユーザは、秘密鍵、公開鍵、ユーザＩＤという３つの情報を用いて、トランザクションを発行する。今、発行元の自分がＢだとすると、ＢからＣにトランザクションＴｘ２が発行されるケースを考える。この場合に、ブロックチェーンは、自分宛てに送られているトランザクションＴｘ１を入力として新しいトランザクションを発行する機能を有する。このように、ブロックチェーンでは、承認済みのトランザクションをもとにして新しいトランザクションが発行されることにより、トランザクションの信頼性を向上させることができる。

【００３２】

図４（ｂ）に示されるように、送信先のユーザＣの公開鍵が、トランザクションＴｘ２

の宛先の情報として指定される。また、承認済みのトランザクションＴｘ１のハッシュ値を含む未署名のトランザクションＴｘ２に対して、ハッシュ値が計算され、そのハッシュ値に対しユーザＢ自身の秘密鍵を用いて電子署名が計算され、その電子署名がトランザクションＴｘ２の発行元の情報として付加される。

【００３３】

このようなトランザクションＴｘ２がブロックチェーンネットワークにブロードキャストされると、ブロックチェーンネットワークに属する他のユーザがトランザクションＴｘ２の署名を次のようにして検証する。図４（ｂ）のように、トランザクションＴｘ２の未署名部分からハッシュ値が計算される。また、トランザクションＴｘ２の発行元として添付されているユーザＢの電子署名を生成させたハッシュ値が、ユーザＢの公開鍵を使って計算される。そして、これらの２つのハッシュ値が比較され、２つのハッシュ値が一致すれば、トランザクションＴｘ２は、正しいユーザＢが発行したものであるとの検証結果が得られる。

【００３４】

このように、ブロックチェーンは、過去の承認済トランザクションに対して、電子署名による検証を行いながら、そのハッシュ値を入力として新たなトランザクションを発行していくことで、トランザクションそのものの信頼性を向上させる仕組みを有する。ブロックチェーンを構成するそれぞれのブロックは、「そのブロックの一つ前のブロックに関する情報」と、「ある時間内に行われたすべての取引のリスト（＝個々のトランザクションをまとめたもの）」を記録したトランザクションで構成される。これにより、各ブロックのトランザクションには、ある時間内に行われたすべての取引が記録されることになる。

【００３５】

ブロックチェーンでは更に、ブロックチェーンネットワーク内でマイナーと呼ばれる特定の検査ノードが、任意のノードから新規に発行されたトランザクションのブロックを確定する処理を実行する。この確定処理によって、高セキュアな台帳管理を実現することが可能であり、それらのトランザクション発行のすべての履歴情報が分散台帳上で共有・管理されるという特徴を有する。

【００３６】

図４（ｃ）は、上記確定処理の説明図である。マイナーは、直前ブロックのハッシュ値と、取引リストをまとめたマークルツリーのルートのハッシュ値とに、自身がランダムに生成するナンス（ｎｏｎｃｅ）値と呼ばれる情報を加えた３つの情報からなる未承認ブロックに対して、ハッシュ値を計算する。マイナーは、ナンス値をランダムに変更しながら、このハッシュ値が特定の条件を満たす（例えば先頭に一定数以上の０が並ぶような値となる）ようなナンス値を発見する。この結果、マイナーは、上記発見したナンス値を含む上記３つの情報によって、未承認ブロックを改ざん不能な形で確定（承認）する。この確定処理を実行したマイナーは報酬を獲得できる。マイナーは、上記確定したブロックを、ブロックチェーンネットワーク内のユーザ全員にブロードキャストする。上記ブロックの確定の仕組みにより、ブロックチェーンネットワークにおいて、上記特定の条件（例えば先頭に一定数以上の０が並ぶ値となっている状態）が満たされないハッシュ値となるブロックは、確定された（承認された）ブロックとは見なされない。確定されていない未承認のブロックは、次のブロックへの入力として採用することはできない。

【００３７】

ブロックのナンス値を受け取った他のユーザは、ブロックに含まれる各トランザクションの電子署名が正しいか否かをまず検証する。更に、上記ユーザは、そのブロックから算出されるハッシュ値が前述した特定の条件（例えば先頭に一定数以上の０が並ぶ値となっている状態）が満たされているか否かを検証する。そして、上記ユーザは、上記２つの検証に問題がなければ、図４（ｂ）で説明した手順で、自身のブロックチェーンの末尾に承認済みのブロックを追加する。

【００３８】

このブロック内の情報を改ざんしようとした場合、ブロック内の３つの情報とブロック

チェーン全体に矛盾が生じるようにデータ構造を作ることで、実質改ざん不能なデータベースを構築することができる。ネットワーク全体で「唯一のブロックの鎖」を持つようにされることによって、一貫した取引履歴を全体が共有することができる。

【００３９】

本実施形態では、以上の仕組みのブロックチェーンネットワークで動作する図３（ｂ）のブロックチェーンアプリケーション３０３が、ＩＰＦＳアプリケーション３０４を介して分散ファイル共有ネットワーク３０１にアクセスするためのプロキシとして動作する。このように、本実施形態では、端末で発生したイベントに関する情報が、ブロックチェーンを用いて分散ファイル共有ネットワークに含まれるノード装置間で共有される。

【００４０】

図５は、本実施形態における通信システム５００の構成例を示す図である。通信システム５００は、トランザクション発行アプリケーション（以下「トランザクション発行アプリ」）５１０を備えるセンサデバイス又はクライアント端末（以下「センサデバイス／クライアント端末」）５０１を備える。通信システム５００は、ブロックチェーンアプリケーション（以下「ブロックチェーンアプリ」）５１１と分散ファイル共有アプリケーション（以下「分散ファイル共有アプリ」）５１２を備えるセンサエッジノード又はクライアント端末（以下、「センサエッジノード／クライアント端末」）５０２を備える。センサデバイス５０１とセンサエッジノード５０２の組合せは、図１（ａ）のＩｏＴサービス例のセンサネットワークのユースケースで使用される。クライアント端末５０１とクライアント端末５０２の組合せは、図１（ｂ）のサプライチェーン例のユースケースで使用される。センサデバイス／クライアント端末５０１とセンサエッジノード／クライアント端末５０２は、一体のノード装置であるＩｏＴゲートウェイ又はクライアント端末（以下「ＩｏＴゲートウェイ／クライアント端末」）５０３であってもよい。即ち、ＩｏＴゲートウェイ／クライアント端末５０３は、トランザクション発行アプリ５１０と、ブロックチェーンアプリ５１１と、分散ファイル共有アプリ５１２とを備える。これらのアプリは、ＩｏＴゲートウェイまたはクライアント端末からなるノード装置以外のノード装置に配備されても良い。以下の説明では、センサデバイス／クライアント端末５０１とセンサエッジノード／クライアント端末５０２とを合わせてＩｏＴゲートウェイ／クライアント端末５０３として説明する。

【００４１】

また、通信システム５００は、トランザクション発行アプリ５１０とブロックチェーンアプリ５１１と分散ファイル共有アプリ５１２とを備えるクライアント端末５０４を備える。例えば、クライアント端末５０４がトランザクション発行アプリ５１０のみを有するようにし、クライアント端末５０４内のブロックチェーンアプリ５１１と分散ファイル共有アプリ５１２が別のノード装置に実装されるような構成であってもよい。

【００４２】

そのほか、通信システム５００は、ブロックチェーン認証ノード５０５及びブロックチェーンノード５０６を備える。この認証部は、認証証跡管理ブロックネットワーク５２１へのユーザまたはグループのログインと、ブロックチェーンの初期トランザクションであるサービス許可トランザクションの発行を行う。

【００４３】

トランザクション発行アプリ５１０は、ブロックチェーン認証ノード５０５と通信を行って、ＩｏＴゲートウェイ／クライアント端末５０３又はクライアント端末５０４を操作するユーザ又はグループを認証する認証部を備える。

【００４４】

ＩｏＴゲートウェイ／クライアント端末５０３は、図１のＩｏＴゲートウェイ１０３又はクライアント端末１０４、或いは図３のＩｏＴゲートウェイ３０５に対応する。即ち、ＩｏＴゲートウェイ／クライアント端末５０３は、センサ情報を出力し、又は端末操作者によって入力される原材料・部品の調達から、製造、在庫管理、販売、配送までの製品の工程情報等を出力する。

【００４５】
ＩｏＴゲートウェイ／クライアント端末５０３、クライアント端末５０４、ブロックチェーン認証ノード５０５、及びブロックチェーンノード５０６は、認証／証跡管理プロキシネットワーク５２１を形成する。認証／証跡管理プロキシネットワーク５２１は、ブロックチェーンネットワークに含まれる。また、ＩｏＴゲートウェイ／クライアント端末５０３及びクライアント端末５０４は、分散ファイル共有ネットワーク５２２を形成する。
【００４６】
図５の構成を有する本実施形態における通信システム５００の動作の詳細について、以下に説明する。図６は、図５の通信システム５００におけるファイル発行の処理例を示すシーケンス図、図７は、図６のファイル発行の処理例で使用される各トランザクションのデータフォーマット例を示す図である。
【００４７】
まず、ファイル発行の処理例について概説する。
＜ＳＴＥＰ１：ユーザ認証の実行＞
最初に、ＩｏＴゲートウェイ／クライアント端末５０３内のセンサデバイス／クライアント端末５０１に対するユーザ認証を、既存のブロックチェーンソフトウェアで利用される電子証明書を用いて行う。
【００４８】
＜ＳＴＥＰ２：ファイル登録の証跡管理の実行＞
センサデバイス／クライアント端末５０１がイベントを検知した際、図６のトランザクション発行アプリ５１０が、次の処理を実行する。トランザクション発行アプリ５１０は、センサデバイス／クライアント端末５０１（ｕｓｅｒＩＤ　＃Ｘ）から、特定ユーザ（ｕｓｅｒＩＤ　＃Ｙ）あるいは共有サービス（ｇｒｏｕｐＩＤ　＃Ｚ）宛てに、イベントトランザクション（イベントに関するトランザクション）を発行する。このイベントトランザクションは、サービス認可トランザクションのハッシュ値を入力し、イベント情報を含む。
【００４９】
＜ＳＴＥＰ３：イベント情報ファイルの生成／登録とコンテンツの一意性の保証＞
イベントトランザクションを含むブロックが検査ノードにより確定された後、ブロックチェーンアプリ５１１は、イベントトランザクションに含まれるイベント情報を含むファイルを生成するためのファイル生成トランザクション（ファイルを生成するトランザクション）を新たに発行する。ブロックチェーンアプリ５１１は、ファイル生成トランザクションの発行を契機に、イベントトランザクションのハッシュ値の情報をコンテンツの一意性を保証するＩＤとして埋め込み、上記イベント情報を含んだイベント情報ファイルを自動生成する。ブロックチェーンアプリ５１１は、上記イベント情報ファイルを、分散ファイル共有アプリ５１２を介してＩＰＦＳ等の分散ファイル共有ネットワーク５２２に登録する。このとき、イベント情報ファイルには、イベントトランザクションを発行したタイムスタンプ情報が付与されても良い。
【００５０】
＜ＳＴＥＰ４：ポータルファイルの更新によるリポジトリ機能の提供＞
ブロックチェーンアプリ５１１は、イベント情報ファイルが分散ファイル共有ネットワーク５２２に登録された際に発行されるファイルアドレス情報（ＩＰＦＳの場合はハッシュ値のアドレス）を、分散ファイル共有アプリ５１２を介して取得する。ブロックチェーンアプリ５１１は、ファイル生成トランザクションのハッシュ値を入力とし、前記ファイルアドレスを記載したセンサデバイス／クライアント端末５０１（ｕｓｅｒＩＤ　＃Ｘ）から、特定ユーザ（ｕｓｅｒＩＤ　＃Ｙ）あるいは共有サービス（ｇｒｏｕｐＩＤ　＃Ｚ）宛てのサービス登録トランザクションを発行する。このサービス登録トランザクションは、ファイル生成トランザクションのハッシュ値と、イベント情報ファイルのアドレス情報と、サービス情報とを含む。ブロックチェーンアプリ５１１は、サービス登録トランザクションの発行を契機に、コンテンツ例えばサービス名とファイルアドレスとを紐づけた

情報を、分散ファイル共有ネットワーク５２２で公開されるポータルサイトを示すポータルファイルに追加・更新し、再登録する。

【００５１】

上記手続きにより、分散ファイル共有ネットワーク５２２へのファイル登録に関する認証と証跡情報、およびコンテンツの一意性の保証をブロックチェーンで管理することが可能になる。同時に、ファイルアドレスとコンテンツ例えばサービス情報の関係を紐づけ、分散ファイル共有ネットワーク５２２上のポータルファイルとして一元管理するリポジトリ機能を提供することが可能となる。

【００５２】

次に、図６のファイル発行の処理例の詳細について説明する。

まず、ＩｏＴゲートウェイ／クライアント端末５０３は、自装置内のセンサからのセンサ出力又は端末入力等のイベントが発生すると、自装置内のトランザクション発行アプリ５１０を起動する。トランザクション発行アプリ５１０は、自装置に予め割り当てられているユーザアカウントを用いて、自装置で実行されるブロックチェーンアプリ５１１内の既存の認証部にアクセスし、ログインを実行する（Ｓ６０１）。

【００５３】

ＩｏＴゲートウェイ／クライアント端末５０３内のブロックチェーンアプリ５１１の認証部は、認証／証跡管理プロキシネットワーク５２１内のブロックチェーン認証ノード５０５と通信をしながら、上記ログインのアクセスに対して認証を実行する（Ｓ６０２）。

【００５４】

上記認証部は、認証が成立したら、トランザクション発行アプリ５１０に、所定のサービス認可トランザクションのハッシュ値を通知して、ユーザが認証／証跡ネットワーク（ブロックチェーン）３０２に対してログインすることを認可する（Ｓ６０３）。

【００５５】

続いて、ＩｏＴゲートウェイ／クライアント端末５０３内のトランザクション発行アプリ５１０は、自装置内で発生したイベントに対応するイベント情報（センサ出力情報又は工程情報等）と、上記サービス認可トランザクションのハッシュ値とを含むイベントトランザクションを発行する（Ｓ６０４）。このとき、トランザクション発行アプリ５１０は、イベントトランザクションに、発行元の情報として、自装置のユーザＩＤと、それに対応する公開鍵情報を設定する。また、トランザクション発行アプリ５１０は、イベントトランザクションに、宛先の情報として、ファイル登録処理のサービスに予め割り当てられたユーザＩＤ又はグループＩＤと、それに対応する公開鍵情報を併せて設定する。

【００５６】

このイベントトランザクションは、ブロックチェーンである認証／証跡管理プロキシネットワーク５２１を形成している全てのブロックチェーンノード５０６に通知される（Ｓ６０５）。ブロックチェーンノード５０６のうちの１つ以上のノードは、図４（ｃ）で説明した検査ノード（マイナー）として動作しており、通知されたトランザクションに記載された電子署名を検証し、ブロックを確定する処理を実行している。この結果、何れかの検査ノードは、上記イベントトランザクションのブロックに対して確定処理を実行し、確定通知を発行する（Ｓ６０６）。

【００５７】

ＩｏＴゲートウェイ／クライアント端末５０３で実行中のブロックチェーンアプリ５１１は、イベントトランザクションの発行通知（Ｓ６０４）とそれに対応する確定通知（Ｓ６０６）を受信すると、次の処理を実行する。上記ブロックチェーンアプリ５１１は、ファイル生成トランザクションを発行する（Ｓ６０７）。このファイル生成トランザクションは、確定したブロックに対応するイベントトランザクションのハッシュ値とイベントトランザクションに含まれていたイベント情報とを含み、ファイル生成処理を実行する。このとき、上記ブロックチェーンアプリ５１１は、ファイル生成トランザクションに、イベントトランザクションに設定されているセンサデバイス／クライアント端末５０１（図５参照）のユーザＩＤを設定する。このユーザＩＤは発行元の情報である。また、ブロック

チェーンアプリ５１１は、ファイル生成トランザクションに、宛先の情報として、イベントトランザクションに設定されているファイル登録処理のサービスに予め割り当てられたユーザＩＤ又はグループＩＤを設定する。

【００５８】

このファイル生成トランザクションは、ブロックチェーンである認証／証跡管理プロキシネットワーク５２１を形成している全てのブロックチェーンノード５０６に通知される（Ｓ６０８）。ブロックチェーンノード５０６のうちの１つの検査ノードは、通知された上記ファイル生成トランザクションのブロックに対して確定処理を実行し、確定通知を発行する（Ｓ６０６）。

【００５９】

ＩｏＴゲートウェイ／クライアント端末５０３で実行中のブロックチェーンアプリ５１１は、ファイル生成トランザクションの発行通知（Ｓ６０７）とそのブロックに対応する確定通知（Ｓ６０９）を受信すると、次の処理を実行する。

【００６０】

上記ブロックチェーンアプリ５１１は、受信したイベントトランザクション内のイベント情報を含むイベント情報ファイルを生成するファイル生成処理（Ｓ６１０）を実行する。上記ブロックチェーンアプリ５１１は、このとき同時に、確定したブロックに対応するファイル生成トランザクションに設定されているイベントトランザクションのハッシュ値を、コンテンツの一意性を保証するＩＤとして、イベント情報ファイルに埋め込む。また、イベント情報ファイルには、イベントトランザクションが発行されたときのタイムスタンプ情報が付与されてもよい。更に、ファイルそのものの秘匿性を向上させるため、上記ブロックチェーンアプリ５１１は、ファイル生成トランザクションに設定されている宛先のユーザＩＤ又はグループＩＤに対応した公開鍵で、分散ファイルシステムに登録するイベント情報ファイルを暗号化してもよい。この場合、上記ユーザＩＤ又はグループＩＤの公開鍵に対応した秘密鍵を持つユーザやグループのみが、分散ファイル共有システムに登録された該当するイベント情報ファイルの情報を閲覧することが可能になる。その後、上記ブロックチェーンアプリ５１１は、自装置内の分散ファイル共有アプリ５１２を起動する（以上、Ｓ６１０）。

【００６１】

上記分散ファイル共有アプリ５１２は、生成されたイベント情報ファイルに対して、以下のＳ６１１及びＳ６１２からなるファイル登録処理を実行する。上記分散ファイル共有アプリ５１２は、このファイル登録処理において、まず、分散ファイル共有ネットワーク５２２に対して、上記イベント情報ファイルを登録する（Ｓ６１１）。そして、上記分散ファイル共有アプリ５１２は、登録先のノードから登録したイベント情報ファイルのハッシュ値をアドレス情報として取得し、そのアドレス情報を自装置内のブロックチェーンアプリ５１１に通知する（Ｓ６１２）」。

【００６２】

上記ブロックチェーンアプリ５１１は、イベント情報ファイルに対応するアドレス情報を取得すると、ファイル生成トランザクションのハッシュ値を入力とするサービス登録トランザクションを発行する（Ｓ６１３）。このとき、上記ブロックチェーンアプリ５１１は、サービス登録トランザクションに、Ｓ６１２で取得したイベント情報ファイルのハッシュ値（アドレス情報）と、このイベント情報ファイルに対応するイベントのサービスの情報とを設定する。また、上記ブロックチェーンアプリ５１１は、サービス登録トランザクションに、発行元の情報として、ファイル生成トランザクションに設定されているセンサデバイス／クライアント端末５０１（図５参照）のユーザＩＤを設定する。また、ブロックチェーンアプリ５１１は、サービス登録トランザクションに、宛先の情報として、ファイル生成トランザクションに設定されているファイル登録処理のサービスに予め割り当てられたユーザＩＤ又はグループＩＤを設定する。

【００６３】

このサービス登録トランザクションは、ブロックチェーンである認証／証跡管理プロキ

シネットワーク５２１を形成している全てのブロックチェーンノード５０６に通知される（Ｓ６１４）。ブロックチェーンノード５０６のうちの１つの検査ノードは、通知された上記サービス登録トランザクションのブロックに対して確定処理を実行し、確定通知を発行する（Ｓ６１５）。

【００６４】

ＩｏＴゲートウェイ／クライアント端末５０３で実行中のブロックチェーンアプリ５１１は、サービス登録トランザクションの発行通知（Ｓ６１３）とそのブロックに対応する確定通知（Ｓ６１５）を受信すると、以下のサービス登録処理を実行する。上記ブロックチェーンアプリ５１１は、まず、自装置の分散ファイル共有アプリ５１２にアクセスして、分散ファイル共有ネットワーク５２２からポータルファイルを取得する（Ｓ６１６）。続いて、上記ブロックチェーンアプリ５１１は、Ｓ６１２で取得したイベント情報ファイルに対応するハッシュ値（アドレス情報）に、イベント情報ファイルに対応するサービス内容を含む情報を紐付けた情報を、上記取得したポータルファイルに追加して更新する。そして、上記ブロックチェーンアプリ５１１は、その更新したポータルファイルを、自装置の分散ファイル共有アプリ５１２にアクセスして、分散ファイル共有ネットワーク５２２に再登録させる（以上、Ｓ６１７）。

【００６５】

上記ポータルファイルの更新処理で、他のＩｏＴゲートウェイ／クライアント端末５０３からのポータルファイルの同時更新を避けるために、ＩｏＴゲートウェイ／クライアント端末５０３内の上記分散ファイル共有アプリ５１２は、排他制御を実行してもよい。この場合、上記分散ファイル共有アプリ５１２では、ポータルファイルの同時更新が許容されず、１ユーザのみに更新権限が与えられ、他ユーザはロックされるような制御が実行される。また、ポータルファイル管理者にコンテンツとファイルアドレスの関係を通知するＡＰＩを設け、ＩｏＴゲートウェイ／クライアント端末５０３内の上記分散ファイル共有アプリ５１２がポータルファイル管理者にポータルファイルの更新を一任する制御が実行されてもよい。

【００６６】

上記制御処理により、分散ファイル共有ネットワーク５２２へのファイル登録に関する認証と証跡情報、およびコンテンツの一意性の保証を、ブロックチェーンである認証／証跡管理プロキシネットワーク５２１で管理することが可能になる。

【００６７】

また、コンテンツとファイルアドレスの関係が紐づけられ、分散ファイル共有システム上のポータルファイルとして、ブロックチェーンで一元管理することも可能となる。図８は、Ｓ６１６及びＳ６１７で処理されるポータルファイルのデータフォーマット例を示す図である。ポータルファイルには、イベント情報ファイルに対応するハッシュ値（アドレス情報）に、イベント情報ファイルに対応するサービス内容と、イベント情報ファイルのファイル名とが紐付けられる。

【００６８】

次に、図７に示される、図６で説明したファイル発行の処理で使用される各トランザクションのデータフォーマット例の詳細について説明する。

【００６９】

図６のＳ６０４でＩｏＴゲートウェイ／クライアント端末５０３のトランザクション発行アプリ５１０により発行されるイベントトランザクションは、図７（ａ）に例示されるデータフォーマットを有する。図７（ａ）に示されるように、イベントトランザクションには、ブロックチェーンの入力トランザクションとして、Ｓ６０３で通知されたサービス認可トランザクションのハッシュ値が設定される。また、イベントトランザクションには、自装置内で発生したセンサイベントに対応するイベント情報が設定される。更に、イベントトランザクションには、発行元の情報として、センサデバイス／クライアント端末５０１（図５参照）のユーザＩＤ（図７（ａ）中の「ｕｓｅｒＩＤ　＃Ｘ」）とそれに対応する公開鍵情報が設定される。また、イベントトランザクションには、宛先の情報として

、ファイル登録処理のサービスに予め割り当てられたユーザＩＤ（図７（ａ）中の「ｕｓｅｒＩＤ　＃Ｙ」）又はグループＩＤ（図７（ａ）中の「ｇｒｏｕｐＩＤ　＃Ｚ」）とそれに対応する公開鍵情報が設定される。

【００７０】

図６のＳ６０７でＩｏＴゲートウェイ／クライアント端末５０３のブロックチェーンアプリ５１１により発行されるファイル生成トランザクションは、図７（ｂ）に例示されるデータフォーマットを有する。図７（ｂ）に示されるように、ファイル生成トランザクションには、ブロックチェーンの入力トランザクションとして、Ｓ６０６の確定通知で確定されたブロックに対応するイベントトランザクションのハッシュ値が設定される。また、ファイル生成トランザクションには、イベントトランザクションに設定されているイベント情報が設定される。更に、ファイル生成トランザクションには、発行元の情報として、イベントトランザクションに設定されているセンサデバイス／クライアント端末５０１（図５参照）のユーザＩＤ（図７（ｂ）中の「ｕｓｅｒＩＤ　＃Ｘ」）とそれに対応する公開鍵情報が設定される。また、ファイル生成トランザクションには、宛先の情報として、ファイル登録処理のサービスに予め割り当てられたユーザＩＤ（図７（ｂ）中の「ｕｓｅｒＩＤ　＃Ｙ」）又はグループＩＤ（図７（ｂ）中の「ｇｒｏｕｐＩＤ　＃Ｚ」）とそれに対応する公開鍵情報が設定される。

【００７１】

図６のＳ６１３でＩｏＴゲートウェイ／クライアント端末５０３のブロックチェーンアプリ５１１により発行されるサービス登録トランザクションは、図７（ｃ）に例示されるデータフォーマットを有する。図７（ｃ）に示されるように、サービス登録トランザクションには、ブロックチェーンの入力トランザクションとして、Ｓ６０９の確定通知で確定されたブロックに対応するファイル生成トランザクションのハッシュ値が設定される。また、サービス登録トランザクションには、Ｓ６１２で取得したイベント情報ファイルに対応するハッシュ値（アドレス情報）と、このイベント情報ファイルに対応するイベントのサービスの情報とが設定される。更に、サービス登録トランザクションには、発行元の情報として、ファイル生成トランザクションに設定されているセンサデバイス／クライアント端末５０１（図５参照）のユーザＩＤ（図７（ｃ）中の「ｕｓｅｒＩＤ　＃Ｘ」）が設定される。加えて、サービス登録トランザクションには、宛先の情報として、ファイル登録処理のサービスに予め割り当てられたユーザＩＤ（図７（ｃ）中の「ｕｓｅｒＩＤ　＃Ｙ」）又はグループＩＤ（図７（ｃ）中の「ｇｒｏｕｐＩＤ　＃Ｚ」）が設定される。

【００７２】

図７（ｄ）の統合トランザクションのデータフォーマットについては、後述する。

図９は、図５の通信システム５００におけるファイル発行の他の処理例を示すシーケンス図である。前述した図６では、ファイル生成処理（Ｓ６１０）及びファイル登録処理（Ｓ６１１、Ｓ６１２）を実行するためのファイル生成トランザクションと、サービス登録処理（Ｓ６１６、Ｓ６１７）を実行するためのサービス登録トランザクションが、２つに分かれていた。これに対して、図９では、ファイル生成処理（Ｓ６１０）、ファイル登録処理（Ｓ６１１、Ｓ６１２）、及びサービス登録処理（Ｓ６１６、Ｓ６１７）が、１つのトランザクションのブロックの確定を契機として、連続して実行される点が異なる。

【００７３】

具体的には、図９において、図６と同じ参照番号が付されたシーケンスは、図６の場合と同じ処理である。図９のシーケンスが図６のシーケンスと異なる部分についてのみ、以下に説明する。

【００７４】

ＩｏＴゲートウェイ／クライアント端末５０３で実行中のブロックチェーンアプリ５１１は、図６のシーケンスと同様にして、イベントトランザクションの発行通知（Ｓ６０４）とそれに対応する確定通知（Ｓ６０６）を受信すると、次の処理を実行する。上記ブロックチェーンアプリ５１１は、図７（ｄ）のデータフォーマット例に示される統合トランザクションを発行する。この統合トランザクションには、Ｓ６０６の確定通知により確定

されたブロックに対応するイベントトランザクションのハッシュ値が設定される。また、統合トランザクションには、イベントトランザクションに含まれていたイベント情報が設定される。また、統合トランザクションには、上記イベント情報に対応するサービスの情報が設定される。更に、統合トランザクションには、発行元の情報として、イベントトランザクションに設定されているユーザＩＤ（図７（ｄ）中の「ｕｓｅｒＩＤ　＃Ｘ」）が設定される。加えて、統合トランザクションには、宛先の情報として、イベントトランザクションに設定されているユーザＩＤ（図７（ｄ）中の「ｕｓｅｒＩＤ　＃Ｙ」）又はグループＩＤ（図７（ｄ）中の「ｇｒｏｕｐＩＤ　＃Ｚ」）が設定される。

【００７５】

この統合トランザクションは、ブロックチェーンである認証／証跡管理プロキシネットワーク５２１を形成している全てのブロックチェーンノード５０６に通知される（Ｓ９０２）。ブロックチェーンノード５０６のうちの１つの検査ノードは、通知された上記ファイル生成トランザクションのブロックに対して確定処理を実行し、確定通知を発行する（Ｓ９０３）。

【００７６】

ＩｏＴゲートウェイ／クライアント端末５０３で実行中のブロックチェーンアプリ５１１は、統合トランザクションの発行通知（Ｓ９０１）とそれに対応する確定通知（Ｓ９０３）を受信すると、次の処理を実行する。上記ブロックチェーンアプリ５１１は、図６のシーケンスで説明したファイル生成処理（Ｓ６１０）、ファイル登録処理（Ｓ６１１、Ｓ６１２）、及びサービス登録処理（Ｓ６１６、Ｓ６１７）を、連続して実行する。

【００７７】

図１０は、図５の通信システム５００におけるファイルアクセスの処理例を示すシーケンス図、図１１は、図１０のファイルアクセスの処理例で使用されるトランザクションのデータフォーマット例を示す図である。

【００７８】

まず、ファイルアクセスの処理例について概説する。

＜ＳＴＥＰ１：ユーザ認証の実行＞

最初に、クライアント端末５０４からファイルアクセスを行うユーザの認証を、既存のブロックチェーンで発行される電子証明書を用いて行う。

【００７９】

＜ＳＴＥＰ２：ファイルアクセスの証跡管理の実行＞

ユーザがファイルにアクセスするため、クライアント端末５０４内のトランザクション発行アプリ５１０が、サービス認可トランザクションのハッシュ値を入力とし、ポータルサイトのポータルファイルのアドレスを含むファイル閲覧トランザクションを発行する。このファイル閲覧トランザクションの発行元はクライアント端末５０４のユーザ（ｕｓｅｒＩＤ　＃Ｗ）、宛先は特定ユーザ（ｕｓｅｒＩＤ　＃Ｙ）あるいは共有サービス（ｇｒｏｕｐＩＤ　＃Ｚ）とそられに対応する公開鍵情報である。トランザクション発行アプリ５１０は、クライアント端末５０４内のブロックチェーンアプリ５１１及び分散ファイル共有アプリ５１２を介して、分散ファイル共有ネットワーク５２２から、共有空間を管理するサービスのポータルファイルの情報を取得する。これによってユーザはポータルサイトの情報を閲覧する。

【００８０】

＜ＳＴＥＰ３：ファイルアクセスの実行とファイルアクセスの証跡管理の実行＞

クライアント端末５０４において、ユーザがポータルサイトに記載されているファイルを選択する。この結果、クライアント端末５０４内のトランザクション発行アプリ５１０が、サービス認可トランザクションのハッシュ値を入力とし、ユーザが選択したファイルのアドレスを含むファイル閲覧トランザクションを発行する。このファイル閲覧トランザクションの発行元はクライアント端末５０４のユーザ（ｕｓｅｒＩＤ　＃Ｗ）、宛先は特定ユーザ（ｕｓｅｒＩＤ　＃Ｙ）あるいは共有サービス（ｇｒｏｕｐＩＤ　＃Ｚ）とそらに対応する公開鍵情報である。トランザクション発行アプリ５１０は、クライアント端

末５０４内のブロックチェーンアプリ５１１及び分散ファイル共有アプリ５１２を介して、分散ファイル共有ネットワーク５２２から該当するファイルを取得する。この結果、ユーザは、該当ファイルを閲覧することが可能になる。

【００８１】

以上の処理により、分散ファイル共有ネットワーク５２２上でのファイルアクセスの認証と証跡情報をブロックチェーンの機能を活用し実現することが可能になる。この情報をサービス課金に利用してもよい。また、要求したファイル情報をユーザが取得するまでは、ファイルアクセスのファイル閲覧トランザクションの発行を待機し、ファイル取得確認後に該当トランザクションを発行するようにしてもよい。なお、各トランザクションはブロックチェーンにおけるブロック確定の処理が完了するまでは実行されないものとし、ブロック確定を実行するノードは、自身のノードでも他のノードでも良い。

【００８２】

次に、図１０のファイルアクセスの処理例の詳細について説明する。

まず、クライアント端末５０４は、ファイル閲覧要求のイベントが発生すると、自装置内のトランザクション発行アプリ５１０を起動する。トランザクション発行アプリ５１０は、クライアント端末５０４に予め割り当てられているユーザアカウントを用いて、クライアント端末５０４のブロックチェーンアプリ５１１内の既存の認証部にアクセスし、ログインを実行する（Ｓ１００１）。

【００８３】

クライアント端末５０４内のブロックチェーンアプリ５１１の認証部は、認証／証跡管理プロキシネットワーク５２１内のブロックチェーン認証ノード５０５と通信をしながら上記ログインのアクセスに対して認証を実行する（Ｓ１００２）。

【００８４】

上記認証部は、認証が成立したら、トランザクション発行アプリ５１０に、所定のサービス認可トランザクションのハッシュ値を通知して、ログインを認可する（Ｓ１００３）。

【００８５】

続いて、クライアント端末５０４内のトランザクション発行アプリ５１０は、自装置内で発生したファイル閲覧要求で指定されているポータルファイルのハッシュ値（アドレス情報）と、上記サービス認可トランザクションのハッシュ値とを含む第１のファイル閲覧トランザクションを発行する（Ｓ１００４）。このとき、トランザクション発行アプリ５１０は、第１のファイル閲覧トランザクションに、発行元の情報として、クライアント端末５０４のユーザＩＤを設定する。また、トランザクション発行アプリ５１０は、第１のファイル閲覧トランザクションに、宛先の情報として、ファイル登録処理のサービスに予め割り当てられたユーザＩＤ又はグループＩＤを設定する。

【００８６】

この第１のファイル閲覧トランザクションは、ブロックチェーンである認証／証跡管理プロキシネットワーク５２１を形成している全てのブロックチェーンノード５０６に通知される（Ｓ１００５）。ブロックチェーンノード５０６のうちの１つの検査ノードは、通知された上記第１のファイル閲覧トランザクションのブロックに対して確定処理を実行し、確定通知を発行する（Ｓ１００６）。

【００８７】

クライアント端末５０４で実行中のブロックチェーンアプリ５１１は、第１のファイル閲覧トランザクションの発行通知（Ｓ１００４）とそれに対応する確定通知（Ｓ１００６）を受信すると、次の処理を実行する。上記ブロックチェーンアプリ５１１は、クライアント端末５０４内の分散ファイル共有アプリ５１２に、第１のファイル閲覧トランザクションに含まれるポータルファイルのハッシュ値（アドレス情報）を指定したポータルファイル要求を発行する（Ｓ１００７）。

【００８８】

この結果、クライアント端末５０４内の分散ファイル共有アプリ５１２は、上記ハッシ

ュ値によって分散ファイル共有ネットワーク５２２にアクセスし、ポータルファイルを取得し、クライアント端末５０４内のブロックチェーンアプリ５１１に送信する。上記ブロックチェーンアプリ５１１は、このポータルファイルの内容を、クライアント端末５０４内のトランザクション発行アプリ５１０に送信する（以上、Ｓ１００８）。この結果、クライアント端末５０４の特には図示しないディスプレイ等に、図８に例示した、各サービス名、イベント情報ファイル名、及びイベント情報ファイルのハッシュ値（アドレス情報）の一覧が表示され、ユーザが閲覧可能となる。

【００８９】

続いて、クライアント端末５０４のユーザが、ディスプレイ上の上記一覧を見ながら、何れかのサービス名に対応するイベント情報ファイルのハッシュ値を指定する。この結果、クライアント端末５０４内のトランザクション発行アプリ５１０は、自装置内で発生したファイル閲覧要求で指定されているイベント情報ファイルのハッシュ値（アドレス情報）と、Ｓ１００３で取得されているサービス認可トランザクションのハッシュ値とを含む第２のファイル閲覧トランザクションを発行する（Ｓ１００９）。このとき、トランザクション発行アプリ５１０は、第２のファイル閲覧トランザクションに、発行元の情報として、クライアント端末５０４のユーザＩＤとそれに対する公開鍵情報を設定する。また、トランザクション発行アプリ５１０は、第２のファイル閲覧トランザクションに、宛先の情報として、ファイル登録処理のサービスに予め割り当てられたユーザＩＤ又はグループＩＤとそられに対する公開鍵情報を設定する。

【００９０】

この第２のファイル閲覧トランザクションは、ブロックチェーンである認証／証跡管理プロキシネットワーク５２１を形成している全てのブロックチェーンノード５０６に通知される（Ｓ１０１０）。ブロックチェーンノード５０６のうちの１つの検査ノードは、通知された上記第２のファイル閲覧トランザクションのブロックに対して確定処理を実行し、確定通知を発行する（Ｓ１０１１）。

【００９１】

クライアント端末５０４で実行中のブロックチェーンアプリ５１１は、第２のファイル閲覧トランザクションの発行通知（Ｓ１００９）とそれに対応する確定通知（Ｓ１０１１）を受信すると、次の処理を実行する。上記ブロックチェーンアプリ５１１は、クライアント端末５０４内の分散ファイル共有アプリ５１２に、第２のファイル閲覧トランザクションに含まれるイベント情報ファイルのハッシュ値（アドレス情報）を指定したファイル要求を発行する（Ｓ１０１２）。

【００９２】

この結果、クライアント端末５０４内の分散ファイル共有アプリ５１２は、上記ハッシュ値によって分散ファイル共有ネットワーク５２２にアクセスし、イベント情報ファイルを取得し、クライアント端末５０４内のブロックチェーンアプリ５１１に送信する。上記ブロックチェーンアプリ５１１は、このイベント情報ファイルの内容を、クライアント端末５０４内のトランザクション発行アプリ５１０に送信する（以上、Ｓ１０１３）。この結果、クライアント端末５０４の特には図示しないディスプレイ等に、イベント情報ファイルの内容が表示され、ユーザが閲覧可能となる。

【００９３】

次に、図１１に示される、図１０で説明したファイルアクセスの処理例で使用されるトランザクションのデータフォーマット例の詳細について説明する。

【００９４】

図１０のＳ１００４又はＳ１００９でクライアント端末５０４のトランザクション発行アプリ５１０により発行される第１又は第２のファイル閲覧トランザクションは、図１１に例示されるデータフォーマットを有する。図１１に示されるように、ファイル閲覧トランザクションには、ブロックチェーンの入力トランザクションとして、Ｓ１００３で通知されたサービス認可トランザクションのハッシュ値が設定される。また、ファイル閲覧トランザクションには、自装置内で発生したポータルファイル又はイベント情報ファイルの

閲覧要求に対応するポータルファイル又はイベント情報ファイルのハッシュ値（アドレス情報）が設定される。更に、イベントトランザクションには、発行元の情報として、クライアント端末５０４のユーザＩＤ（図１１中の「ｕｓｅｒＩＤ　＃Ｗ」）とそれに対応する公開鍵情報が設定される。また、ファイル閲覧トランザクションには、宛先の情報として、前述したファイル閲覧処理のサービスに予め割り当てられたユーザＩＤ（図１１中の「ｕｓｅｒＩＤ　＃Ｙ」）又はグループＩＤ（図１１中の「ｇｒｏｕｐＩＤ　＃Ｚ」）とそれらに対応する公開鍵情報が設定される。このユーザＩＤ又はグループＩＤは、前述したファイル登録処理のサービスに予め割り当てられた図７に示される宛先のユーザＩＤ又はグループＩＤと同じである。

【００９５】

以上のファイルアクセス処理により、分散ファイル共有ネットワーク５２２上の分散ファイルシステムでのファイルアクセスの認証と証跡情報を、ブロックチェーンの機能を活用し実現することが可能になる。この情報は、サービス課金等に利用してもよい。

【００９６】

また、要求したファイル情報をユーザが取得するまでは、ファイル閲覧トランザクションの発行を待機し、ファイル取得確認後に該当トランザクションが発行されるようにしてもよい。

【００９７】

図１２は、図５のＩｏＴゲートウェイ／クライアント端末５０３又はクライアント端末５０４の機能をソフトウェア処理として実現でき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。

【００９８】

図１２に示されるコンピュータは、ＣＰＵ（中央演算処理装置）１２０１、メモリ１２０２、入力装置１２０３、出力装置１２０４、外部記憶装置１２０５、可搬記録媒体１２０９が挿入される可搬記録媒体駆動装置１２０６、及び通信インタフェース１２０７を有し、これらがバス１２０８によって相互に接続された構成を有する。図１２に示される構成はＩｏＴゲートウェイ／クライアント端末５０３又はクライアント端末５０４の機能を実現できるコンピュータの一例であり、そのようなコンピュータはこの構成に限定されるものではない。

【００９９】

ＣＰＵ１２０１は、当該コンピュータ全体の制御を行う。メモリ１２０２は、プログラムの実行、データ更新等の際に、外部記憶装置１２０５（或いは可搬記録媒体１２０９）に記憶されているプログラム又はデータを一時的に格納するＲＡＭ等のメモリである。ＣＵＰ１２０１は、プログラムをメモリ１２０２に読み出して実行することにより、全体の制御を行う。

【０１００】

入力装置１２０３は、ユーザによるキーボードやマウス等による入力操作を検出し、その検出結果をＣＰＵ１２０１に通知する。

【０１０１】

出力装置１２０４は、ＣＰＵ１２０１の制御によって送られてくるデータを表示装置や印刷装置に出力する。

【０１０２】

外部記憶装置１２０５は、例えばハードディスク記憶装置である。主に各種データやプログラムの保存に用いられる。

【０１０３】

可搬記録媒体駆動装置１２０６は、ＳＤカード、コンパクトフラッシュ（登録商標）や、ＣＤ－ＲＯＭ、ＤＶＤ、光ディスク等の可搬記録媒体１２０９を収容するもので、外部記憶装置１２０５の補助の役割を有する。

【０１０４】

通信インターフェース１２０７は、例えばＬＡＮ（ローカルエリアネットワーク）又は

ＷＡＮ（ワイドエリアネットワーク）の通信回線を接続するための装置である。

【０１０５】

図５のＩｏＴゲートウェイ／クライアント端末５０３又はクライアント端末５０４の機能は、以下に説明する図１３から図１５のフローチャート等で実現される機能を搭載したプログラムをＣＰＵ１２０１が実行することで実現される。そのプログラムは、例えば外部記憶装置１２０５や可搬記録媒体１２０９に記録して配布してもよく、或いは通信インタフェース１２０７によりネットワークから取得できるようにしてもよい。

【０１０６】

図１３は、図５のＩｏＴゲートウェイ／クライアント端末５０３が図１２のハードウェア構成例を有するコンピュータとして実装される場合において実行されるファイル発行処理例、及びそれに対応する検査ノードの処理例を示すフローチャートである。この処理は、前述した図６のシーケンス例で示されるＩｏＴゲートウェイ／クライアント端末５０３のファイル発行処理を、図１２のハードウェア構成例のコンピュータで実行する場合の処理を示した図である。この処理は、図１２のＣＰＵ１２０１が、外部記憶装置１２０５等からメモリ１２０２にロードされたファイル発行処理プログラムを実行する処理である。

【０１０７】

図１３において、ステップＳ１３０１及びＳ１３０２は、図５のＩｏＴゲートウェイ／クライアント端末５０３が実装するトランザクション発行アプリ５１０が実行する処理である。ステップＳ１３０５、Ｓ１３０８からＳ１３１０、及びＳ１３１３及びＳ１３１４の処理は、図５のＩｏＴゲートウェイ／クライアント端末５０３が実装するブロックチェーンアプリ５１１が実行する処理である。また、ステップＳ１３１１とＳ１３１２、及びＳ１３１９とＳ１３２０の処理は、図５のＩｏＴゲートウェイ／クライアント端末５０３が実装する分散ファイル共有アプリ５１２が実行する処理である。更に、ステップＳ１３０３とＳ１３０４、Ｓ１３０６とＳ１３０７、及びＳ１３１５とＳ１３１６の処理は、検査ノードの特には図示しないＣＰＵが実行する処理である。

【０１０８】

ＣＰＵ１２０１はまず、自装置に対するユーザ認証処理を実行する（ステップＳ１３０１）。この処理は、ブロックチェーンの既存の認証処理であり、図６のＳ６０１から Ｓ６０３のシーケンスを実行する処理である。

【０１０９】

次に、ＣＰＵ１２０１は、イベントトランザクション発行処理を実行する（ステップＳ１３０２）。この処理は、図６のＳ６０４のシーケンスを実行する処理である。

【０１１０】

ステップＳ１３０２の処理の結果、ＣＰＵ１２０１から通信インタフェース１２０７を介してＬＡＮ上の認証／証跡管理プロキシネットワーク５２１（図５参照）上の検査ノードに、トランザクション通知（図６のＳ６０５）が送信される。この結果、検査ノードのＣＰＵは、イベントトランザクションを取得し（ステップＳ１３０３）、そのイベントトランザクションを含むブロックを確定させ、そのブロックの確定通知を、ＩｏＴゲートウェイ／クライアント端末５０３に返す（ステップＳ１３０４）。この処理は、図６のＳ６０６のシーケンスを実行する処理である。

【０１１１】

ＩｏＴゲートウェイ／クライアント端末５０３のＣＰＵ１２０１は、通信インタフェース１２０７を介して上記確定通知を受信すると、ファイル生成トランザクション発行処理を実行する（ステップＳ１３０５）。この処理は、図６のＳ６０７のシーケンスを実行する処理である。

【０１１２】

ステップＳ１３０５の処理の結果、ＣＰＵ１２０１から通信インタフェース１２０７を介して認証／証跡管理プロキシネットワーク５２１（図５参照）上の検査ノードに、トランザクション通知（図６のＳ６０８）が送信される。この結果、検査ノードのＣＰＵは、ファイル生成トランザクションを取得し（ステップＳ１３０６）、そのファイル生成トラ

ンザクションを含むブロックを確定させ、そのブロックの確定通知を、ＩｏＴゲートウェイ／クライアント端末５０３に返す（ステップＳ１３０７）。この処理は、図６のＳ６０９のシーケンスを実行する処理である。

【０１１３】

ＩｏＴゲートウェイ／クライアント端末５０３のＣＰＵ１２０１は、通信インタフェース１２０７を介して上記確定通知を受信すると、その確定通知されたブロックに対応するファイル生成トランザクションに対応して実行される処理ロジックの実行を開始する（ステップＳ１３０８）。

【０１１４】

この処理ロジックにおいて、ＣＰＵ１２０１はまず、ファイル生成処理を実行する（ステップＳ１３０９）。この処理は、図６のＳ６１０のシーケンスを実行する処理である。

【０１１５】

上記処理ロジックにおいて、ＣＰＵ１２０１は次に、ファイル登録処理を実行する（ステップＳ１３１０）。この処理は、図６のＳ６１１のシーケンスを実行する処理である。

【０１１６】

この結果、ＣＰＵ１２０１は、通信インタフェース１２０７を介してＬＡＮ上の分散ファイル共有ネットワーク５２２に対して、イベント情報ファイルの登録処理を実行する（ステップＳ１３１１）。この処理は、図６のＳ６１１のシーケンスを実行する処理である。

【０１１７】

ステップＳ１３１１のファイル登録処理の結果、ＣＰＵ１２０１は、イベント情報ファイルのハッシュ値をアドレス情報として発行する（ステップＳ１３１２）。この結果、ＣＰＵ１２０１は、発行されたアドレス情報を取得してメモリ１２０２に記憶する等の処理を実行する（ステップＳ１３１３）。ステップＳ１３１２とＳ１３１３の処理は、図６のＳ６１２のシーケンスを実行する処理である。

【０１１８】

続いて、ＣＰＵ１２０１は、サービス登録トランザクション発行処理を実行する（ステップＳ１３１４）。この処理は、図６のＳ６１３のシーケンスを実行する処理である。

【０１１９】

ステップＳ１３１４の処理の結果、ＣＰＵ１２０１から通信インタフェース１２０７を介して認証／証跡管理プロキシネットワーク５２１（図５参照）上の検査ノードに、トランザクション通知（図６のＳ６１４）が送信される。この結果、検査ノードのＣＰＵは、サービス登録トランザクションを取得し（ステップＳ１３１５）、そのサービス登録トランザクションを含むブロックを確定させ、そのサービス登録トランザクションのブロックの確定通知を、ＩｏＴゲートウェイ／クライアント端末５０３に返す（ステップＳ１３１６）。この処理は、図６のＳ６１５のシーケンスを実行する処理である。

【０１２０】

ＩｏＴゲートウェイ／クライアント端末５０３のＣＰＵ１２０１は、通信インタフェース１２０７を介して上記確定通知を受信すると、その確定通知されたブロックに対応するサービス登録トランザクションに対応して実行される処理ロジックの実行を開始する（ステップＳ１３１７）。

【０１２１】

この処理ロジックにおいて、ＣＰＵ１２０１はまず、ブロックチェーンアプリ５１１上で、ポータルファイルの取得処理を実行する（ステップＳ１３１８）。この結果、ＣＰＵ１２０１は、分散ファイル共有アプリ５１２を実行することにより、分散ファイル共有ネットワーク５２２上のポータルファイルにアクセスし、それを取得する（ステップＳ１３１９）。ステップＳ１３１８及びＳ１３１９の処理は、図６のＳ６１６のシーケンスを実行する処理である。

【０１２２】

上記処理ロジックにおいて、ＣＰＵ１２０１は次に、ポータルファイルの更新処理を実

行する（ステップＳ１３２０）。ここでは、ＣＰＵ１２０１は、ブロックチェーンアプリ５１１を実行する。これにより、ＣＰＵ１２０１は、ステップＳ１３１３で取得したイベント情報ファイルに対応するハッシュ値（アドレス情報）に、イベント情報ファイルに対応するサービス内容を含む情報を紐付けた情報を、上記取得したポータルファイルに追加して更新する。その後、ＣＰＵ１２０１は、ブロックチェーンアプリ５１１から分散ファイル共有アプリ５１２に実行を移す。ＣＰＵ１２０１は、ステップＳ１３２０で更新したポータルファイルを、分散ファイル共有ネットワーク５２２に再登録する（ステップＳ１３２１）。ステップＳ１３２０とＳ１３２１の処理は、図６のＳ６１７のシーケンスを実行する処理である。

【０１２３】

以上の図１３のフローチャートで例示されるファイル発行処理を図１２のハードウェア構成例のコンピュータが実行することにより、ＩｏＴゲートウェイ／クライアント端末５０３による図６に例示されるシーケンスのファイル発行処理が実現される。

【０１２４】

図１４は、図５のＩｏＴゲートウェイ／クライアント端末５０３が図１２のハードウェア構成例を有するコンピュータとして実装される場合において実行される他のファイル発行処理例、及びそれに対応する検査ノードの処理例を示すフローチャートである。この処理は、前述した図９のシーケンス例で示されるＩｏＴゲートウェイ／クライアント端末５０３の他のファイル発行処理を、図１２のハードウェア構成例のコンピュータで実行する場合の処理を示した図である。この処理は、図１２のＣＰＵ１２０１が、外部記憶装置１２０５等からメモリ１２０２にロードされた他のＷＥＢ発行処理プログラムを実行する処理である。

【０１２５】

前述した図１３では、図６で説明したシーケンス例に対応して、イベントトランザクションの発行（Ｓ１３０２）に加えて、２つのトランザクションが発行されていた。そのうちの１つは、ファイル生成処理（Ｓ１３０９）及びファイル登録処理（Ｓ１３１０、Ｓ１３１１）を実行するための、ファイル生成トランザクション発行（Ｓ１３０５）である。他の１つは、サービス登録処理（Ｓ１３１８～Ｓ１３２１）を実行するための、サービス登録トランザクション発行（Ｓ１３１４）である。これに対して、図１４では、図９で前述したシーケンス例に対応して、上記一連の処理（Ｓ１３０９～Ｓ１３１１、Ｓ１３１８～Ｓ１３２１）が、１つのトランザクションのブロックの確定を契機として、連続して実行される点が異なる。

【０１２６】

具体的には、図１４において、図１３と同じ参照番号が付されたステップは、図１３の場合と同じ処理である。図１４のステップが図１３のステップと異なる部分についてのみ、以下に説明する。

【０１２７】

ＣＰＵ１２０１は、ブロックチェーンアプリ５１１の実行において、図１３の場合と同様にして、イベントトランザクションに対応するブロックの確定通知（Ｓ１３０４）を受信すると、次の処理を実行する。ＣＰＵ１２０１は、統合トランザクションの発行処理を実行する（ステップＳ１４０１）。この処理は、図９のＳ９０１のシーケンスを実行する処理である。

【０１２８】

ステップＳ１４０１の処理の結果、ＣＰＵ１２０１から通信インタフェース１２０７を介して認証／証跡管理プロキシネットワーク５２１（図５参照）上の検査ノードに、トランザクション通知（図９のＳ９０２）が送信される。この結果、検査ノードのＣＰＵは、統合トランザクションを取得し（ステップＳ１４０２）、その統合トランザクションを含むブロックを確定させ、その統合トランザクションに対応するブロックの確定通知を、ＩｏＴゲートウェイ／クライアント端末５０３に返す（ステップＳ１４０３）。この処理は、図９のＳ９０３のシーケンスを実行する処理である。

【０１２９】
ＩｏＴゲートウェイ／クライアント端末５０３のＣＰＵ１２０１は、通信インタフェース１２０７を介して上記確定通知を受信すると、その確定通知されたブロックに対応する統合トランザクションに対応して実行される処理ロジックの実行を開始する（ステップＳ１４０１）。
【０１３０】
この処理ロジックにおいて、ＣＰＵ１２０１は、図１３の場合と同様の、ステップＳ１３０９からＳ１３１３の一連の処理を実行し、更に、ステップＳ１３１８からＳ１３２１の一連の処理を連続して実行する。これらの処理は、図９のＳ６１０からＳ６１２の一連のシーケンスを実行し、更にＳ６１６とＳ６１７の一連のシーケンスを連続して実行する処理である。
【０１３１】
以上の図１４のフローチャートで例示される他のファイル発行処理を図１２のハードウェア構成例のコンピュータが実行することにより、ＩｏＴゲートウェイ／クライアント端末５０３による図９に例示されるシーケンスの他のＷＥＢ発行処理が実現される。
【０１３２】
図１５は、図５のクライアント端末５０４が図１２のハードウェア構成例を有するコンピュータとして実装される場合において実行されるファイルアクセス処理例、及びそれに対応する検査ノードの処理例を示すフローチャートである。この処理は、前述した図１０のシーケンス例で示されるクライアント端末５０４のファイルアクセス処理を、図１２のハードウェア構成例のコンピュータで実行する場合の処理を示した図である。この処理は、図１２のＣＰＵ１２０１が、外部記憶装置１２０５等からメモリ１２０２にロードされたファイルアクセス処理プログラムを実行する処理である。
【０１３３】
図１５において、ステップＳ１５０１とＳ１５０２、及びＳ１５０８は、図５のクライアント端末５０４が実装するトランザクション発行アプリ５１０が実行する処理である。ステップＳ１５０５とＳ１５０６、Ｓ１５１１とＳ１５１２は、図５のクライアント端末５０４が実装するブロックチェーンアプリ５１１が実行する処理である。また、ステップＳ１５０７とＳ１５１３の処理は、図５のクライアント端末５０４が実装する分散ファイル共有アプリ５１２が実行する処理である。更に、ステップＳ１５０３とＳ１５０４、及びＳ１５０９とＳ１５１０の処理は、検査ノードの特には図示しないＣＰＵが実行する処理である。
【０１３４】
ＣＰＵ１２０１はまず、クライアント端末５０４に対するユーザ認証処理を実行する（ステップＳ１５０１）。この処理は、ブロックチェーンの既存の認証処理であり、図１０のＳ１００１から Ｓ１００３のシーケンスを実行する処理である。
【０１３５】
次に、ＣＰＵ１２０１は、第１のファイル閲覧トランザクション発行処理を実行する（ステップＳ１５０２）。この処理は、図１０のＳ１００４のシーケンスを実行する処理である。
【０１３６】
ステップＳ１５０２の処理の結果、ＣＰＵ１２０１から通信インタフェース１２０７を介してＬＡＮ上の認証／証跡管理プロキシネットワーク５２１（図５参照）上の検査ノードに、トランザクション通知（図１０のＳ１００５）が送信される。この結果、検査ノードのＣＰＵは、第１のファイル閲覧トランザクションを取得し（ステップＳ１５０３）、その第１のファイル閲覧トランザクションを含むブロックを確定させ、そのブロックの確定通知を、クライアント端末５０４に返す（ステップＳ１５０４）。この処理は、図１０のＳ１００６のシーケンスを実行する処理である。
【０１３７】
クライアント端末５０４のＣＰＵ１２０１は、通信インタフェース１２０７を介して上

記確定通知を受信すると、その確定通知されたブロックに対応する第１のファイル閲覧トランザクションに対して実行される処理ロジックの実行を開始する（ステップＳ１５０５）。

【０１３８】

この処理ロジックで、ＣＰＵ１２０１はまず、クライアント端末５０４内でブロックチェーンアプリ５１１から分散ファイル共有アプリ５１２に、ポータルファイルのハッシュ値（アドレス情報）を用いたポータルファイル要求処理を実行する（ステップＳ１５０６）。ポータルファイルのハッシュ値（アドレス情報）は、第１のファイル閲覧トランザクションで指定されているものが使用される。この処理は、図１０のＳ１００７のシーケンスを実行する処理である。

【０１３９】

この結果、ＣＰＵ１２０１は、分散ファイル共有アプリ５１２上で、上記ハッシュ値によって分散ファイル共有ネットワーク５２２にアクセスし、ポータルファイルを取得し、ブロックチェーンアプリ５１１を介してトランザクション発行アプリ５１０に送信する。この結果、ＣＰＵ１２０１は、クライアント端末５０４の特には図示しないディスプレイ等に、図８に例示した、各サービス名、イベント情報ファイル名、及びイベント情報ファイルのハッシュ値（アドレス情報）の一覧を表示し、ユーザが閲覧可能となる。この処理は、図１０のＳ１００８のシーケンスを実行する処理である。

【０１４０】

続いて、クライアント端末５０４のユーザが、ディスプレイ上の上記一覧を見ながら、何れかのサービス名に対応するイベント情報ファイルのハッシュ値を指定する。この結果、ＣＰＵ１２０１は、トランザクション発行アプリ５１０上で、自装置内で発生したファイル閲覧要求で指定されているイベント情報ファイルのハッシュ値（アドレス情報）を含む第２のファイル閲覧トランザクション発行処理を実行する（Ｓ１５０８）。この処理は、図１０のＳ１００９のシーケンスを実行する処理である。

【０１４１】

ステップＳ１５０８の処理の結果、ＣＰＵ１２０１から通信インタフェース１２０７を介してＬＡＮ上の認証／証跡管理プロキシネットワーク５２１（図５参照）上の検査ノードに、トランザクション通知（図１０のＳ１０１０）が送信される。この結果、検査ノードのＣＰＵは、第２のファイル閲覧トランザクションを取得し（ステップＳ１５０９）、その第２のファイル閲覧トランザクションを含むブロックを確定させ、そのブロックの確定通知を、クライアント端末５０４に返す（ステップＳ１５１０）。この処理は、図１０のＳ１０１１のシーケンスを実行する処理である。

【０１４２】

クライアント端末５０４のＣＰＵ１２０１は、通信インタフェース１２０７を介して上記確定通知を受信すると、その確定通知されたブロックに対応する第２のファイル閲覧トランザクションに対応して実行される処理ロジックの実行を開始する（ステップＳ１５１１）。

【０１４３】

この処理ロジックで、ＣＰＵ１２０１はまず、クライアント端末５０４内でブロックチェーンアプリ５１１から分散ファイル共有アプリ５１２に、イベント情報ファイルのハッシュ値（アドレス情報）を用いたファイル要求処理を実行する（ステップＳ１５１２）。イベント情報ファイルファイルのハッシュ値（アドレス情報）は、第２のファイル閲覧トランザクションで指定されているものが使用される。この処理は、図１０のＳ１０１２のシーケンスを実行する処理である。

【０１４４】

この結果、ＣＰＵ１２０１は、分散ファイル共有アプリ５１２上で、上記ハッシュ値によって分散ファイル共有ネットワーク５２２にアクセスし、イベント情報ファイルを取得し、ブロックチェーンアプリ５１１を介してトランザクション発行アプリ５１０に送信する。この結果、クライアント端末５０４の特には図示しないディスプレイ等に、イベント

情報ファイルの内容が表示され、ユーザが閲覧可能となる。この処理は、図１０のＳ１０１３のシーケンスを実行する処理である。

【０１４５】

以上説明したように、本実施形態では、端末で発生したイベントに関する情報が、ブロックチェーンを用いて分散ファイル共有ネットワークに含まれるノード装置間で共有される。そして、そのイベントに関する情報を含むファイルが生成され、このファイルを分散ファイル共有ネットワークのいずれかのノード装置で保持する。これにより、分散ファイル共有システムにおいて、閉域ネットワーク空間である高セキュアなファイル共有空間を構築することが可能となる。本実施形態では、ＩｏＴゲートウェイ／クライアント端末５０３でセンサ検知や端末入力等に基づくイベント情報のファイル登録要求が発生したり、クライアント端末５０４からファイル閲覧要求が発生したりした場合に、次のような制御が実行される。この場合、ＩｏＴゲートウェイ／クライアント端末５０３やクライアント端末５０４でブロックチェーンアプリ５１１が実行され、このブロックチェーンアプリケーション５１１が分散ファイル共有アプリ５１２を実行（キック）する。これにより、分散ファイル共有アプリ５１２が、分散ファイル共有ネットワーク５２２に対するイベント情報ファイルの登録やアクセスを実行する。この場合、ＩｏＴゲートウェイ／クライアント端末５０３やクライアント端末５０４のブロックチェーンアプリ５１１は、ユーザ／グループ認証や、コンテンツの一意性の保証、サービスリポジトリ、ファイルのデータ／アクセスログ管理、ファイルのアクセス制御を実行する。これにより、分散ファイル共有ネットワーク５２２に対するイベント情報ファイルの登録／アクセスや、ポータルファイルのアクセスが、高セキュアに実行される。

【０１４６】

具体的には、本実施形態では、ブロックチェーンが備える認証機能により、分散ファイル共有ネットワークにおけるユーザやグループを単位とする認証機能を提供することが可能となる。

【０１４７】

また、本実施形態では、ファイル生成処理において、イベントトランザクションのハッシュ値が、コンテンツの一意性を保証する識別情報としてイベント情報ファイルに埋め込まれる。これにより、本実施形態によれば、分散ファイル共有ネットワーク上のイベント情報ファイルのコンテンツの一意性を保証する機能を提供することが可能となる。

【０１４８】

更に、本実施形態では、分散ファイル共有ネットワークに登録されたイベント情報ファイルのアドレス情報にサービス内容を含む情報を紐付けた情報が、分散ファイル共有ネットワーク上のポータルファイルに登録される。これにより、本実施形態によれば、サービスと分散ファイル共有ネットワーク上のイベント情報ファイルのアドレスとの関係を一元管理するリポジトリ機能を提供することが可能となる。

【０１４９】

加えて、本実施形態では、イベント情報ファイルの登録やアクセスの過程がブロックチェーンに記録される。これにより、本実施形態によれば、分散ファイル共有ネットワークにおけるファイル登録時のデータ履歴（ログ）の記録やファイルアクセス時のアクセス履歴（ログ）の記録等の証跡管理機能を提供することが可能となる。

【０１５０】

以上説明したように、本実施形態では、ブロックチェーンでつくる堅牢なネットワーク空間に、例えばＩＰＦＳによる分散ＷＥＢシステム等の分散ファイル共有ネットワークを統合することが可能となる。これにより、例えば膨大なセンサ情報出力やクライアント端末入力のファイルサービス化を行うことのできるＩｏＴゲートウェイ／クライアント端末を簡単かつセキュアに実現することが可能となる。

【０１５１】

本実施形態が適用されるユースケースとしては、物流における「モノ」の状態をセンシングし、異常発生等の「コト」の情報を記録して公開するようなシステムが考えられる。

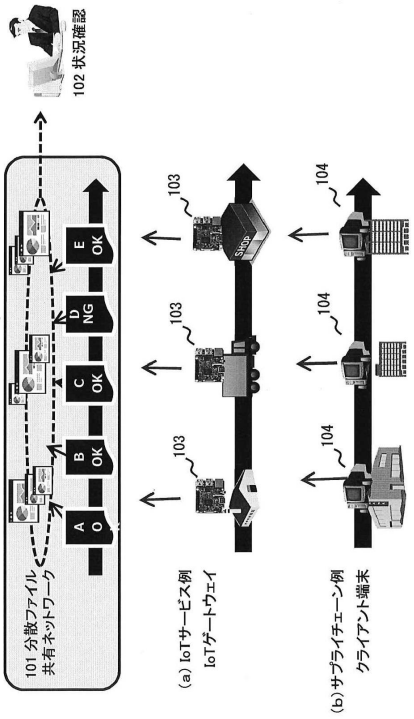
【０１５２】
より具体的には、本実施形態によれば、ＩｏＴゲートウェイ／クライアント端末間のピアツーピア通信のみで、センサ情報出力やクライアント端末入力のファイルサービス化を創る自己組織型ネットワークが実現される。
【０１５３】
また、本実施形態によれば、ユーザ認証、データ著作権を含むコンテンツの一意性の保証、アクセス証跡等のセキュリティ機能をブロックチェーン技術を応用・拡張して実現でき、堅牢な閉空間を創る分散型セキュリティプラットホームが実現される。
【０１５４】
更に、本実施形態による通信システムを、特定の業種／組織のスモールスタートから、複数の業種／組織を繋ぐサービス共創の場に発展させることが可能となり、スモールスタートから拡げるＩｏＴ情報の共創空間が実現される。
【０１５５】
以上の実施形態に関して、更に以下の付記を開示する。
（付記１）
分散ファイル共有ネットワークに含まれるノード装置が実行する通信方法であって、
端末で発生したイベントに関する情報をブロックチェーンを用いて前記分散ファイル共有ネットワークに含まれるノード装置間で共有し、
前記イベントに関する情報を含むファイルを生成し、
前記生成されたファイルを前記分散ファイル共有ネットワークに含まれるいずれかのノード装置で保持する、
ことを特徴とする通信方法。
（付記２）
前記ノード装置が、前記ファイルの保持を行った後に、前記分散ファイル共有ネットワークに保持された前記ファイルのアドレス情報に前記ファイルに対応するサービス内容を含む情報を紐付けた情報をポータルファイルに追加し、前記ポータルファイルを前記分散ファイル共有ネットワークに保持する、
ことを特徴とする付記１に記載の通信方法。
（付記３）
前記ノード装置が、
前記イベントに関する情報を含むトランザクションに対応するブロックの確定後に前記ファイルを生成するトランザクションを発行することにより、前記確定したトランザクションのハッシュ値を、コンテンツの一意性を保証する識別情報として前記ファイルに埋め込む、
ことを特徴とする付記１又は２に記載の通信方法。
（付記４）
前記ノード装置が、前記ファイルを前記分散ファイル共有ネットワークに保持した時のデータ履歴を、前記ブロックチェーンによって管理する、
ことを特徴とする付記１乃至３の何れかに記載の通信方法。
（付記５）
少なくとも１つの前記ノード装置が、
前記ポータルファイルのアドレス情報を指定したブロックチェーンのトランザクションを第１のファイル閲覧トランザクションとして認証及び発行し、
前記第１のファイル閲覧トランザクションの発行を契機に、前記ポータルファイルのアドレス情報に基づいて前記分散ファイル共有ネットワークから前記ポータルファイルを取得し、
前記取得したポータルファイル上で選択された前記サービス内容に対応する前記イベントに関する情報のファイルのアドレス情報を指定したブロックチェーンのトランザクションを第２のファイル閲覧トランザクションとして発行し、
前記第２のファイル閲覧トランザクションの発行を契機に、前記イベントに関する情報

のファイルのアドレス情報に基づいて前記分散ファイル共有ネットワークから前記イベントに関する情報のファイルを取得する、
ことを特徴とする付記２に記載の通信方法。
（付記６）
前記ノード装置が、
前記イベント情報に関するファイルのアドレス情報を指定したブロックチェーンのトランザクションをファイル閲覧トランザクションとして発行し、
前記ファイル閲覧トランザクションの発行を契機に、前記イベントに関する情報のファイルのアドレス情報に基づいて前記分散ファイル共有ネットワークから前記イベントに関する情報のファイルを取得する、
ことを特徴とする付記１に記載の通信方法。
（付記７）
前記ノード装置が、前記分散ファイル共有ネットワークへのアクセス時のアクセス履歴を、前記ブロックチェーンによって管理する、
ことを特徴とする付記５又は６に記載の通信方法。
（付記８）
前記ノード装置が、
前記ノード装置を操作するユーザ毎にユーザ公開鍵とユーザ秘密鍵の組を含むユーザアカウント情報を設定し、
複数のユーザが属するグループ毎に前記グループに属する前記複数のユーザ間で共有されるグループ公開鍵とグループ秘密鍵の組を含むグループアカウント情報を設定し、
前記ファイルを生成するとき、前記ブロックチェーン中のトランザクションに設定されている宛先のユーザ又はグループに対応するユーザ公開鍵又はグループ公開鍵で、前記ファイルを暗号化する、
ことを特徴とする付記１乃至７の何れかに記載の通信方法。
（付記９）
前記ノード装置が、前記ユーザ公開鍵及び前記ユーザ秘密鍵の組の各値、又は前記グループ公開鍵及び前記グループ秘密鍵の組の各値に、利用期限を設けて定期的に更新する、
ことを特徴とする付記８に記載の通信方法。
（付記１０）
前記イベントに関する情報を前記ブロックチェーンのトランザクションとして発行し、前記トランザクションの発行を契機として前記イベントに関する情報を含むファイルを生成する、
ことを特徴とする付記１乃至９の何れかに記載の通信方法。
（付記１１）
前記ファイルの生成、前記ファイルの保持、又は前記ポータルファイルの保持の少なくとも１つは、異なる前記ノード装置によって実行される、
ことを特徴とする付記１乃至１０の何れかに記載の通信方法。
（付記１２）
前記分散ファイル共有ネットワークは、分散ファイルシステムとしてインタープラネタリーファイルシステムを構成し、前記アドレス情報を、前記保持が行われたファイルのハッシュ値を内容アドレスとして含むハイパーリンクとして指定する、
ことを特徴とする付記１乃至１１の何れかに記載の通信方法。
（付記１３）
分散ファイル共有ネットワークに含まれる通信装置であって、
端末で発生したイベントに関する情報を、ブロックチェーン用いて前記分散ファイル共有ネットワークに含まれるノード装置間で共有する手段と、
前記イベントに関する情報を含むファイルを生成する手段と、
前記生成されたファイルを前記分散ファイル共有ネットワークに含まれるいずれかのノード装置で保持する手段と、

を備えることを特徴とする通信装置。
（付記１４）
分散ファイル共有ネットワークに含まれるノード装置のコンピュータに、
端末で発生したイベントに関する情報を、ブロックチェーンを用いて前記分散ファイル共有ネットワークに含まれるノード装置間で共有し、
前記イベントに関する情報を含むファイルを生成し、
前記生成されたファイルを前記分散ファイル共有ネットワークに含まれるいずれかのノード装置で保持する、
ことを実行させるためのプログラム。
【符号の説明】
【０１５６】
１０１、３０１、５２２　分散ファイル共有ネットワーク
１０３　ＩｏＴデバイス
１０４、２２２、３０６、５０４　クライアント端末
２０１　分散ＷＥＢネットワーク
２０２　クラウドサービス
２０３　インターネット又はキャリアネットワーク
２２１、３０５　ＩｏＴゲートウェイ
３０２　認証／証跡管理ネットワーク
３０３　ブロックチェーンアプリケーション
３０４　ＩＰＦＳアプリケーション
３０７　ノード
５００　通信システム
５０１　センサデバイス／クライアント端末
５０２　センサエッジノード／クライアント端末
５０３　ＩｏＴゲートウェイ／クライアント端末
５０５　ブロックチェーン認証ノード
５０６　ブロックチェーンノード
５１０　トランザクション発行アプリ
５１１　ブロックチェーンアプリ
５１２　分散ファイル共有アプリ
５２１　認証／証跡管理プロキシネットワーク
１２０１　ＣＰＵ
１２０２　メモリ
１２０３　入力装置
１２０４　出力装置
１２０５　外部記憶装置
１２０６　可搬記録媒体駆動装置
１２０７　通信インタフェース
１２０８　バス
１２０９　可搬記録媒体

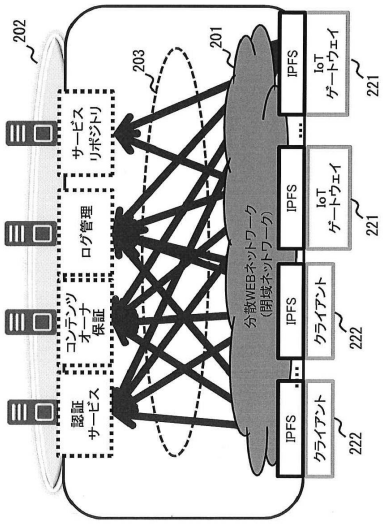
【図１】

本実施形態が対象とする
ユースケースの例を示す図



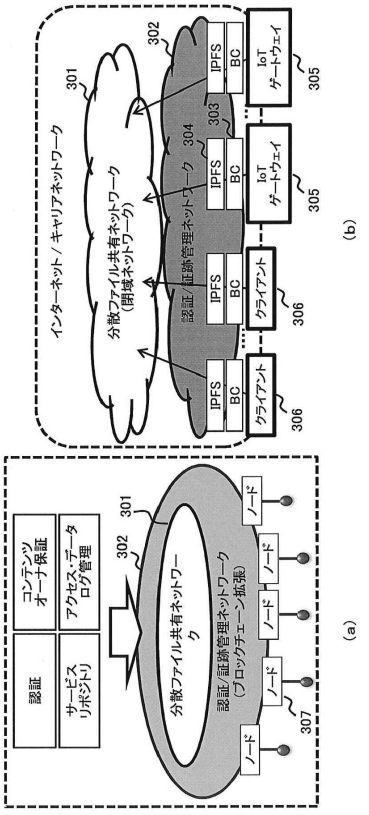
【図２】

IPFS等の分散ファイル共有システムにおいて
高セキュアな情報共有サービスをクラウドサービスに
よって実現する構成例を示す図



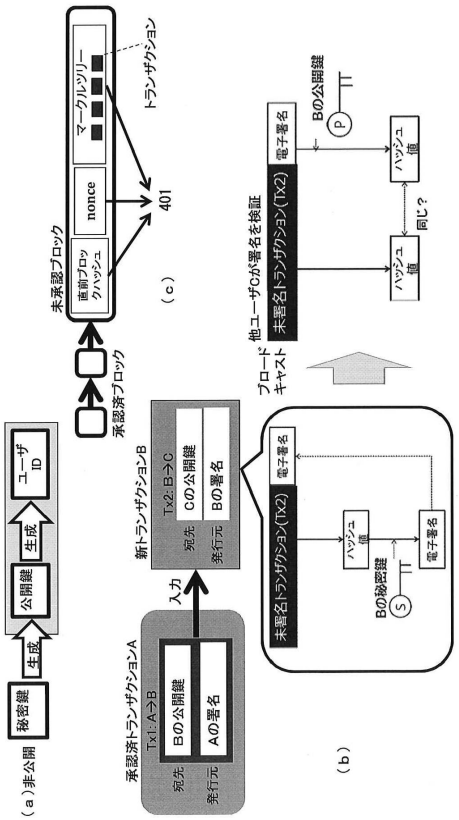
【図３】

本実施形態の基本概念の説明図



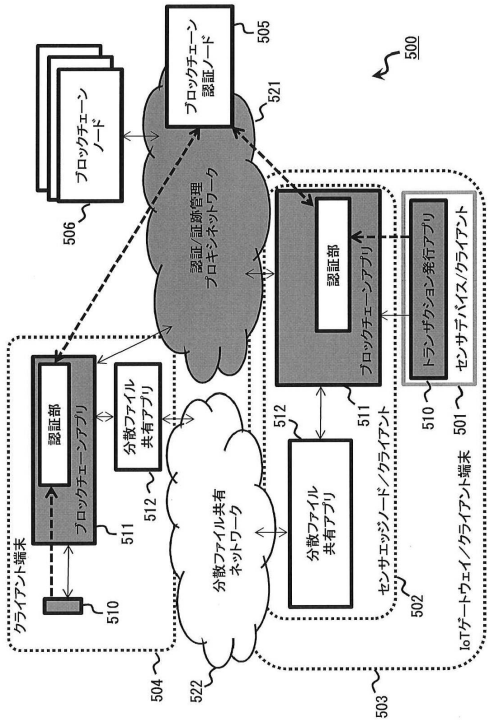
【図４】

ブロックチェーンの説明図



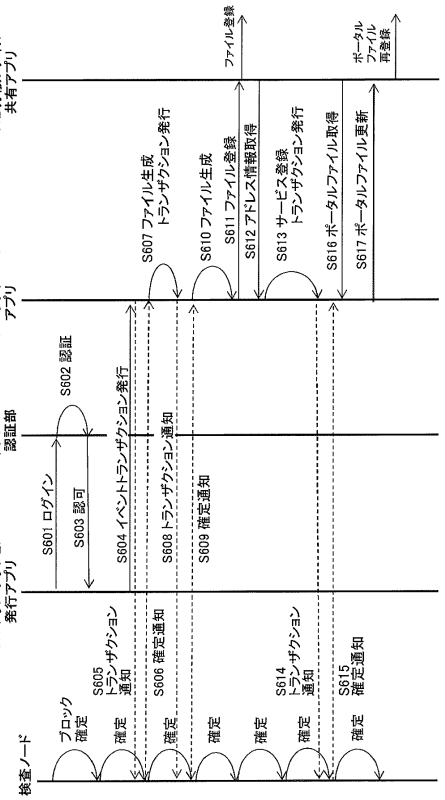
【図５】

本実施形態における通信システムの構成例を示す図



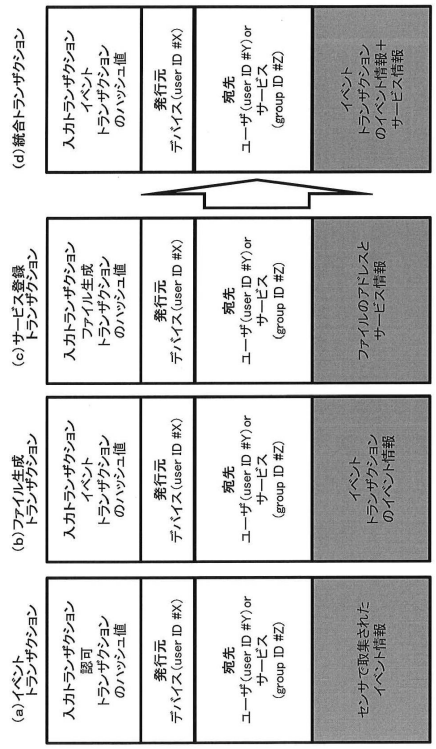
【図６】

ファイル発行の処理例を示すシーケンス図



【図７】

ファイル発行の処理例で使用される
トランザクションのデータフォーマット例を示す図



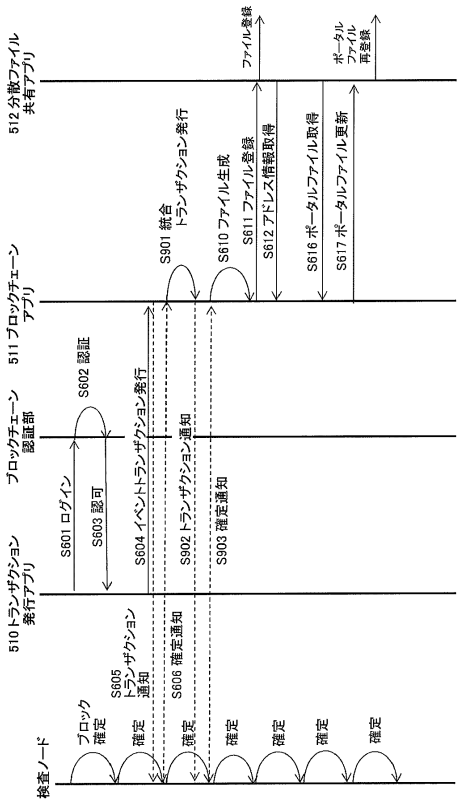
【図８】

ポータルファイルのデータフォーマット例を示す図

サービス内容	ファイル名	イベント情報ファイルのハッシュ値(アドレス情報)
sample1	sample1.csv	QmaZuSmfT9bxj3nN4USDCTW9FG6xgzj73rZBQ3oAEQnWq
sample2	sample2.html	QmRvPJI7GmNAFbJnVeEhMCGtJsDEaJYVa4a52J9bqn1AN
sample3	sample3.pdf	QmPw7VyqirNpx2N2fcT7B8nBFbe1Pq7fd3P1uyK6gKSYv7
.....		
New_sample	New_sample.txt	QmYkwheqFpZE1LozCFYLsAWp2g8pf5dD1aVTrtMTTEPEQ9

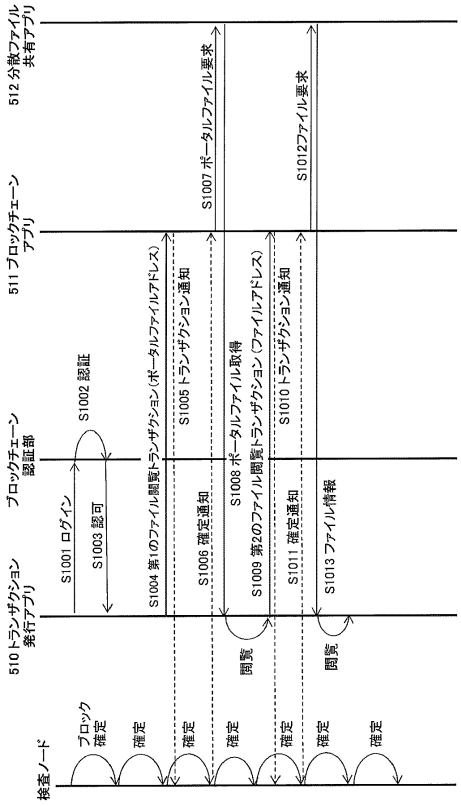
【図９】

ファイル発行の他の処理例を示すシーケンス図



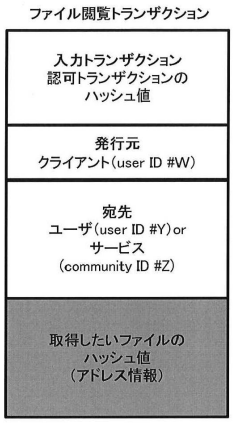
【図１０】

ファイルアクセスの処理例を示すシーケンス図



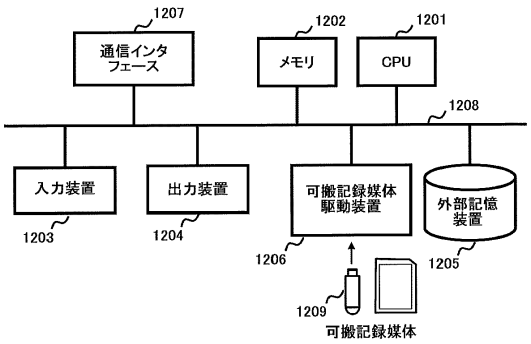
【図１１】

ファイルアクセスの処理例で使用される
トランザクションのデータフォーマット例を示す図



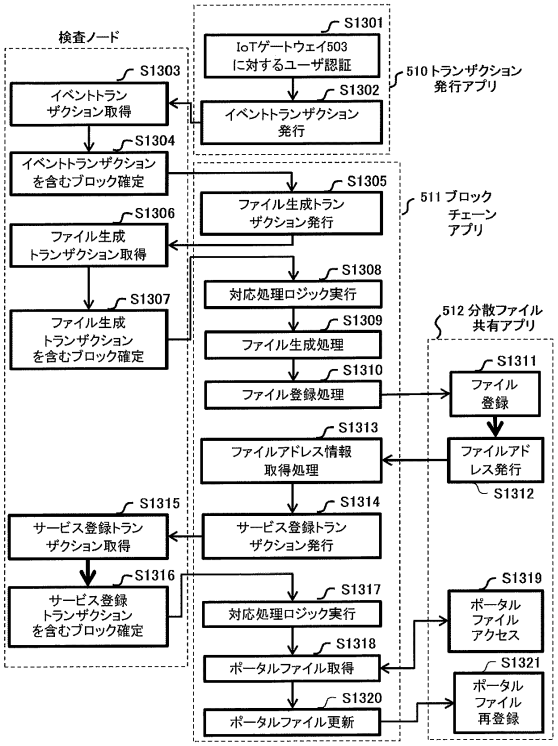
【図１２】

本実施形態のハードウェア構成例を示す図



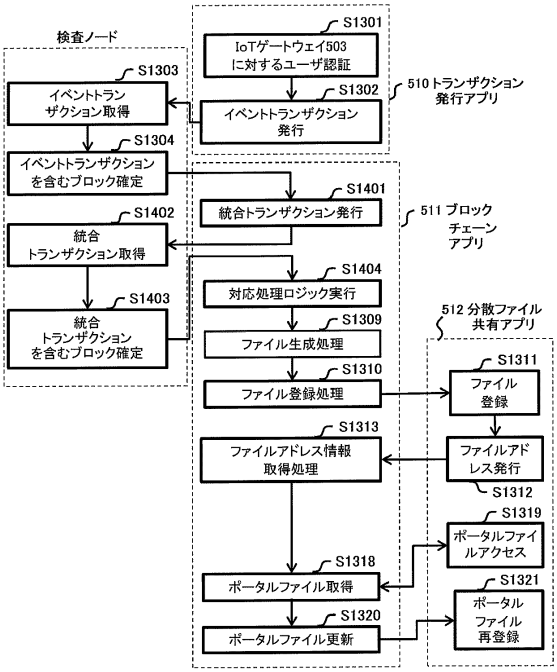
【図１３】

ファイル発行の処理例を示すフローチャート



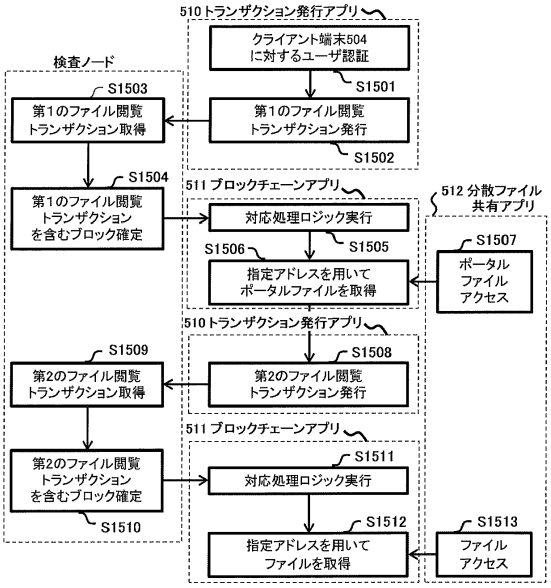
【図１４】

ファイル発行の他の処理例を示すフローチャート



【図１５】

ファイルアクセスの処理例を示すフローチャート



フロントページの続き

(51)Int.Cl. F I
H04L 9/08 (2006.01) H04L 9/00 601A

(72)発明者 今井 悟史
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
(72)発明者 片桐 徹
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
(72)発明者 関屋 元義
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

審査官 宮司 卓佳

(56)参考文献 特開２０１６－１７０５３０（ＪＰ，Ａ）
米国特許出願公開第２０１６／０２０３５７２（ＵＳ，Ａ１）
米国特許出願公開第２０１６／０２８３９２０（ＵＳ，Ａ１）
米国特許出願公開第２０１６／０２８４０３３（ＵＳ，Ａ１）
三浦広平,稲葉宏幸，プライバシーを考慮したディジタルコンテンツ転々流通システムのＢｉｔｃｏｉｎ ２．０による実現，電子情報通信学会技術研究報告 Ｖｏｌ．１１６ Ｎｏ．７１，日本，一般社団法人電子情報通信学会，２０１６年 ５月２６日，第116巻,第71号，p.29-p.32
Melanie Swan, Blockchain Thinking:The Brain as a Decentralized Autonomous Corporation, IEEE Technology and Society Magazine, ２０１５年１２月, Vol.34, p.41-p.52

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｆ １３／００
Ｇ０６Ｆ １６／１４
Ｇ０６Ｆ ２１／４４
Ｇ０６Ｆ ２１／６４
Ｈ０４Ｌ ９／０８