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

特許第6571375号
(P6571375)

(45)発行日　令和1年9月4日(2019.9.4)　(24)登録日　令和1年8月16日(2019.8.16)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675Z
G06Q 50/10	(2012.01)	G06Q	50/10	
G06F 21/16	(2013.01)	G06F	21/16	

請求項の数 6　(全 17 頁)

(21)出願番号　特願2015-89317(P2015-89317)
(22)出願日　平成27年4月24日(2015.4.24)
(65)公開番号　特開2016-208347(P2016-208347A)
(43)公開日　平成28年12月8日(2016.12.8)
審査請求日　平成30年4月12日(2018.4.12)

特許法第３０条第２項適用　平成２６年１１月　５日
国立大学法人筑波大学において開催された知能機能システム専攻　大学院セミナーで発表

(73)特許権者　504171134
国立大学法人　筑波大学
茨城県つくば市天王台一丁目１番１
(74)代理人　100106909
弁理士　棚井　澄雄
(74)代理人　100188558
弁理士　飯田　雅人
(72)発明者　延原　肇
茨城県つくば市天王台一丁目１番１　国立大学法人筑波大学内
(72)発明者　張　丘平
茨城県つくば市天王台一丁目１番１　国立大学法人筑波大学内

最終頁に続く

(54)【発明の名称】著作物保護支援装置

(57)【特許請求の範囲】
【請求項１】
通信部と、
前記通信部を用いて、時刻認証を要求する旨の情報が付された著作物を取得する取得部と、
前記取得部により取得された、時刻認証を要求する旨の情報が付された著作物に基づく情報を、送受信された情報が時刻情報と共に保持される分散型ネットワークに対して発信するように、前記通信部を制御する処理部と、
を備える著作物保護支援装置。
【請求項２】
利用者の端末装置に、著作物の投稿を受け付けるウェブサイトを提供する提供部を備え、
前記取得部は、前記ウェブサイトに対する前記利用者の操作に基づいて前記時刻認証を要求する旨の情報が付与された、前記投稿される著作物を取得する、
請求項１記載の著作物保護支援装置。
【請求項３】
前記分散型ネットワークは、所定のフォーマットを有する情報を送受信するネットワークであり、
前記処理部は、前記取得部により取得された、前記時刻認証を要求する旨の情報が付された著作物を前記所定のフォーマットに合致する形式に変換し、前記変換した情報を含む

情報を、前記分散型ネットワークに対して発信するように、前記通信部を制御する、
請求項１または２記載の著作物保護支援装置。
【請求項４】
前記分散型ネットワークは、クリプトカレンシーによる決済ネットワークであり、
前記処理部は、疑似的な取引データに、前記時刻認証を要求する旨の情報が付された著作物を変換した情報を埋め込み、前記分散型ネットワークに対して発信するように、前記通信部を制御する、
請求項３記載の著作物保護支援装置。
【請求項５】
前記処理部は、前記時刻認証を要求する旨の情報が付された少なくとも著作物、または前記著作物および関連情報を、不可逆性の符号化処理を含む変換処理によって前記所定のフォーマットに合致する形式に変換する、
請求項３または４記載の著作物保護支援装置。
【請求項６】
前記処理部は、前記時刻認証を要求する旨の情報が付された少なくとも著作物の発信元の識別情報、または前記著作物および関連情報の発信元の識別情報を含む情報を、不可逆性の符号化処理によって前記所定のフォーマットに合致する形式に変換し、前記変換した情報を、前記時刻認証を要求する旨の情報が付された著作物に基づく情報と共に前記分散型ネットワークに対して発信するように、前記通信部を制御する、
請求項３から５のうちいずれか１項記載の著作物保護支援装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、著作物保護支援装置に関する。
【背景技術】
【０００２】
近年、動画共有サイトやイラスト投稿ＳＮＳ（Social Networking Service）などＣＧＭ（Consumer Generated Media）において、一般ユーザのコンテンツ創作活動が活発に行われるようになってきている。
【０００３】
ＣＧＭに投稿されたコンテンツは電子データであり、他のユーザによる編集が容易なため、無断転載や改変等著作権の侵害が多発している。著作権侵害が発覚した場合には、自身の著作権を主張しなければならないが、そのための帰属証明や侵害の証拠保全が必要である。これらの証明等の手段に関して、従来は、著作権登録制度や第三者機関のタイムスタンプサービス等を利用している。
【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, (2008).
【非特許文献２】後藤真孝, “初音ミク, ニコニコ動画, ピアプロの切り拓いたCGM現象”, 情報処理学会誌, Vol.53, No.5, pp.466-471, (2012).
【非特許文献３】野口祐子, “コモンズに関わる法的課題”, 情報知識学会誌, Vol. 21, No.1, pp.94-102, (2011)
【非特許文献４】Christian Decker, “Information propagation in the Bitcoin network”, IEEE Thirteenth. International Conference on Peer-to-Peer Computing, pp.1-10, (2013)
【発明の概要】
【発明が解決しようとする課題】
【０００５】

しかしながら、従来の技術では、時刻認証を行うための手続きが煩雑であり、さらに費用が高額である傾向があるため、多くの一般のユーザが利用するＣＧＭのコンテンツへの適用は難しかった。この結果、コンテンツ等の著作物に対して時刻認証を実施できない場合があった。

【０００６】

本発明は、このような事情を考慮してなされたものであり、所望の著作物に対して、簡易かつ安価に時刻認証を行うことができる著作物保護支援装置を提供することを目的の一つとする。

【課題を解決するための手段】

【０００７】

本発明の一態様は、通信部と、前記通信部を用いて、時刻認証を要求する旨の情報が付された著作物を取得する取得部と、前記取得部により取得された、時刻認証を要求する旨の情報が付された著作物に基づく情報を、送受信された情報が時刻情報と共に保持される分散型ネットワークに対して発信するように、前記通信部を制御する処理部と、を備える著作物保護支援装置である。

【０００８】

また、本発明の他の態様は、通信部と、時刻認証を要求する旨の情報が付された著作物に基づく情報を、送受信された情報が時刻情報と共に保持される分散型ネットワークに対して発信するように、前記通信部を制御する処理部と、を備える著作物保護支援装置である。

【発明の効果】

【０００９】

本発明によれば、所望の著作物に対して、簡易かつ安価に時刻認証を行うことができる著作物保護支援装置を提供することができる。

【図面の簡単な説明】

【００１０】

【図１】一実施形態における著作物保護支援装置１００を含む分散ネットワークシステム１の一例を示す構成図である。

【図２】一実施形態における著作物保護支援装置１００の構成の一例を示す図である。

【図３】一実施形態における著作物保護支援装置１００を含む分散ネットワークシステム１の処理の流れの一例を示すシーケンス図である。

【図４】著作物の投稿を受け付けるウェブページの一概略例を示す図である。

【図５】各ＣＣライセンスの種別に対するＣＣコードの一例を示す図である。

【図６】検証用ハッシュＨｖに変換可能な著作物データの種類の一例を示す図である。

【図７】対分散ネットワーク処理部１２０のハッシュ化処理部１２６により行われるハッシュ化処理の様子を示す図である。

【図８】所定のフィールドに埋め込むデータの一例を示す図である。

【図９】時刻認証の対象となる著作物データの一例を示す図である。

【図１０】トランザクションに埋め込まれるデータの一例を示す図である。

【図１１】著作物データが埋め込まれたトランザクションＴＸをブロードキャストする様子を示す図である。

【図１２】データ量ごとに著作物の内容を示すデータをハッシュ化する際に要する時間を導出した結果の一例を示す図である。

【図１３】分散ネットワークに支払う手数料に応じた遅延時間の変化の一例を示す図である。

【図１４】図１３に示す実験結果を得るために用いた手数料の一例を示す図である。

【図１５】ブロックチェーンに著作物データを格納した後に著作物データを変更した際に行われる時刻認証の場面を概略的に示す図である。

【図１６】ブロックチェーンを用いて時刻認証を行った著作物の著作権が侵害された場合において、侵害行為の証明を説明するための図である。

【図１７】一実施形態における著作物保護支援装置１００の処理の流れの一例を示すフローチャートである。
【図１８】端末装置１０によって著作物データが埋め込まれたトランザクションＴＸがブロードキャストされる様子を示す図である。
【発明を実施するための形態】
【００１１】
以下、図面を参照し、本発明の著作物保護支援装置の実施形態について説明する。
図１は、一実施形態における著作物保護支援装置１００を含む分散ネットワークシステム１の一例を示す構成図である。分散ネットワークシステム１において、著作物保護支援装置１００は、端末装置１０－１から１０－ｎ、および端末装置２０－１から２０－ｋとネットワークＮＷを介して接続される。ネットワークＮＷは、ＬＡＮ（Local Area Network）やＷＡＮ（Wide Area Network）等である。上述した装置のうち、端末装置１０－１から１０－ｎは、著作物保護支援装置１００が提供するウェブサイトにアクセス可能な端末装置である。
【００１２】
また、著作物保護支援装置１００と端末装置２０－１から２０－ｋとは、Ｐ２Ｐ（Peer to Peer）等の分散型のネットワークを構築している。なお、端末装置１０－１から１０－ｎのうちの一部または全部は、分散型のネットワークを構築する端末であってもよいし、端末装置２０－１から２０－ｋのうちの一部または全部は、著作物保護支援装置１００が提供するウェブサイトにアクセス可能な端末装置であってよい。
【００１３】
本実施形態において、分散型のネットワークを構築する装置には、「ビットコイン」のクリプトカレンシー（Cryptocurrency）の決済網に参加するためのアプリケーションプログラムがインストールされているものとして説明する。クリプトカレンシーとは、暗号化技術に基づく仮想通貨である。このような装置は、「ビットコイン」のクリプトカレンシーの決済網に参加する場合、ビットコイン用のアプリケーションプログラムを実行し、自身内部のコンピュータリソースの一部を使用して、参加装置の全てにおいて共通のブロックチェーンを保持する。
【００１４】
ブロックチェーンとは、ビットコインの全取引履歴が記録された公共台帳である。ビットコインのブロックチェーンに書き込まれたデータは、偽造、改竄、または削除が困難である特性を有していると共に、偽造、改竄、または削除がされていないことを公的に検証可能な特性を有している。また、ブロックチェーンを構成するブロック（複数のトランザクションにより構成されるもの）、すなわち公共元帳の各ブロックは、ビットコインのクリプトカレンシーの決済網に参加する装置のいずれかによって、一定の時間間隔Ｔ（例えば１０分程度）ごとに生成される。例えば、最新のブロックは、過去に生成されたブロックが時系列に連なって構成されているチェーンの最後尾に追加される。すなわち、最新のブロックは、過去に生成されたブロックのうち、生成時刻が現在に最も近いブロックの後ろに追加される。
【００１５】
ブロックには、例えば、ブロックの識別子が格納される領域、ブロックの生成間隔Ｔの間に生じたビットコインの取引件数（トランザクション数）が格納される領域、ブロックの生成時刻が格納される領域、当該ブロックのハッシュ値が格納される領域、前回生成されたブロックのハッシュ値が格納される領域、ブロックのサイズが格納される領域、トランザクションそのものが格納される領域等が含まれる。上述したブロックの識別子は、ブロックチェーンに新しいブロックが追加される度に、１ずつ加算される一連番号である。従って、ブロック内の識別子を参照することにより、「いつ生成されたブロックなのか」、また「どの程度の取引が行われたのか」等の情報を得ることができる。また、ブロックチェーンの最新のブロックのハッシュ値を参照することにより、ブロックチェーンが「改竄されているか否か」を公的に検証することができる。従って、ブロックチェーンに格納

されたデータの存在性（Existence）および完全性（Integrity）は守られることになる。
【００１６】
端末装置１０－１から１０－ｎおよび端末装置２０－１から２０－ｋは、ユーザによって操作される端末であり、例えば、スマートフォンやタブレット端末、パーソナルコンピュータ、業務用コンピュータ等である。以下、端末装置１０－１から１０－ｎを特段区別しない場合、単に「端末装置１０」と記載し、端末装置２０－１から２０－ｋを特段区別しない場合、単に「端末装置２０」と記載する。
【００１７】
著作物保護支援装置１００は、ブロックチェーンを含むビットコインの流通インフラストラクチャーを利用して、ＣＧＭ（Consumer Generated Media）ウェブサイトに投稿される著作物（ディジタルコンテンツ）の時刻認証を行う。ＣＧＭウェブサイトとは、例えば、動画共有サイトやイラスト投稿ＳＮＳ（Social Networking Service）等の情報共有を目的としたウェブサイトである。
【００１８】
著作物保護支援装置１００は、通信インターフェース１０２と、ウェブサイト提供部１１０と、対分散ネットワーク処理部１２０とを備える。通信インターフェース１０２は、ネットワークＮＷに接続するための通信インターフェースであり、例えば、ネットワークカード等を含む。ウェブサイト提供部１１０は、集中型のネットワークに接続される端末装置１０に対して、所定のＣＧＭウェブサイトを提供する。また、対分散ネットワーク処理部１２０は、ＣＧＭウェブサイトに投稿されたコンテンツの著作物に時刻認証を行うために、当該著作物を上述したブロックチェーンに追加される最新のブロックを生成する際に用いるトランザクションに格納する。
【００１９】
以下、著作物保護支援装置１００の具体的な構成について説明する。
図２は、一実施形態における著作物保護支援装置１００の構成の一例を示す図である。著作物保護支援装置１００は、上述した通信インターフェース１０２、ウェブサイト提供部１１０、および対分散ネットワーク処理部１２０と、記憶部１４０とを備える。対分散ネットワーク処理部１２０は、通信制御部１２２と、符号化処理部１２４と、ハッシュ化処理部１２６と、格納処理部１２８とを備える。なお、通信インターフェース１０２は、「通信部」の一例であり、通信インターフェース１０２および通信制御部１２２は、「取得部」の一例である。また、対分散ネットワーク処理部１２０は、「処理部」の一例である。
【００２０】
ウェブサイト提供部１１０および対分散ネットワーク処理部１２０は、例えば、ＣＰＵ（Central Processing Unit）等のプロセッサが記憶部１４０に記憶されたプログラムを実行することにより機能するソフトウェア機能部である。また、ウェブサイト提供部１１０および対分散ネットワーク処理部１２０のうち一部または全部は、ＬＳＩ（Large Scale Integration）、ＡＳＩＣ（Application Specific Integrated Circuit）等のハードウェアを含んでもよい。
【００２１】
記憶部１４０は、例えば、ＲＯＭ（Read Only Memory）、フラッシュメモリ、ＨＤＤ（Hard Disk Drive）等の不揮発性の記憶媒体と、ＲＡＭ（Random Access Memory）、レジスタ等の揮発性の記憶媒体とを有する。記憶部１４０に記憶される情報は、プロセッサが実行するプログラムの他、後述するビットコイン用アプリケーションプログラム、ＣＧＭウェブサイトを表示させるテキスト文書（画像、音声、映像データ等を含む）、各種ラジオボタンの状態を示す情報、ＣＣコードおよびＣＣライセンス、アカウントＩＤ、著作物のタイトル、著作物データ、検証用ハッシュＨｖ、検索用ハッシュＨｓ、ブロックチェーン（複数のトランザクションから構成されるもの）等の情報を含む。
【００２２】
以下、図３に示すシーケンス図を参照して著作物保護支援装置１００における機能部の

説明を行う。図３は、一実施形態における著作物保護支援装置１００を含む分散ネットワークシステム１の処理の流れの一例を示すシーケンス図である。

【００２３】

著作物保護支援装置１００の通信制御部１２２は、記憶部１４０に予め記憶させておいたビットコイン用のアプリケーションプログラムを実行し、分散ネットワーク内の端末装置２０と同期を行うように通信インターフェースを制御する（ステップＳ１００）。通信制御部１２２は、同期した端末装置２０内の図示しない記憶部からブロックチェーンを取得するように通信インターフェースを制御する（ステップＳ１０２）。次に、通信制御部１２２は、通信インターフェースに取得させたブロックチェーンを記憶部１４０に記憶させる（ステップＳ１０４）。なお、通信制御部１２２は、端末装置２０に同期させる前の段階で、既にブロックチェーンが記憶部１４０に記憶されている場合、端末装置２０が記憶するブロックチェーンと記憶部１４０に記憶されているブロックチェーンとの差分を示すブロックを導出し、導出したブロックのみを更新するようにしてもよい。上述した処理を行うことで、著作物保護支援装置１００は、ビットコインの流通インフラストラクチャーの構成要素の一つであるブロックチェーンを利用することが可能な状態に移行する。

【００２４】

一方、端末装置１０を操作するユーザは、自身が創作した著作物を著作物保護支援装置１００が提供するＣＧＭウェブサイトに投稿して、不特定多数の人と共有することを所望する場合がある。著作物とは、小説等の文書（テキストデータ）、写真等の画像データ、音楽等の音声データ、または映画等の映像データ等である。このような場合、著作物を創作したユーザは、端末装置１０を操作して、著作物保護支援装置１００が提供するＣＧＭウェブサイトにアクセスする。より具体的には、ユーザは、端末装置１０において所定のウェブブラウザを立ち上げ、上述したＣＧＭウェブサイトのアドレスのＵＲＬ（Uniform Resource Locator）を、マウスやキーボード等のユーザインターフェースを用いて入力する。ウェブブラウザ上でＵＲＬが入力された端末装置１０は、当該ＵＲＬが示すウェブサーバ（本実施形態では著作物保護支援装置１００）に、アクセス要求を送信する（ステップＳ１０６）。

【００２５】

ウェブサイト提供部１１０は、端末装置１０からアクセス要求が送信された場合、送信元の端末装置１０の端末ＩＤを取得し、取得した端末ＩＤを記憶部１４０に記憶させる（ステップＳ１０８）。ウェブサイト提供部１１０は、記憶部１４０に記憶させた端末ＩＤによって示される端末装置１０に対して、著作物の投稿を受け付けるウェブページをウェブブラウザ上で表示させるためのテキスト文書等を送信する（ステップＳ１１０）。テキスト文書は、例えば、ＨＴＭＬ（HyperText Markup Language）等のマークアップ言語で記述された文書である。

【００２６】

端末装置１０は、ウェブサイト提供部１１０から送信されたテキスト文書等を受信し、受信したテキスト文書に基づいて、ウェブブラウザ上において著作物の投稿を受け付けるウェブページを表示する（ステップＳ１１２）。

【００２７】

図４は、著作物の投稿を受け付けるウェブページの一概略例を示す図である。当該ウェブページでは、著作物の投稿を選択させるための投稿ボタンＢ１と、投稿に対する利用規約に同意するか否かを選択させるラジオボタンＢ２と、投稿する著作物に対して時刻認証を行うか否かを選択させるラジオボタンＢ３と、投稿した著作物の利用条件を１つ選択させるラジオボタン群Ｂ４とが表示される。利用条件とは、投稿した著作物が他者に使用する際に制限を設ける条件である。利用条件は、例えば、ＣＣ（Creative Commons）ライセンスによって表される。

【００２８】

本実施形態におけるＣＣライセンスは、例えば、ＢＹ、ＢＹ－ＳＡ、ＢＹ－ＮＤ、ＢＹ－ＮＣ、ＢＹ－ＮＣ－ＳＡ、およびＢＹ－ＮＣ－ＮＤの６種類に分類される。ＢＹは、著

作権者の表示を要する条件であり、ＢＹ－ＳＡは、著作権者の表示を要求し、投稿した著作物に改変、変形、または加工を行って創作した著作物に対して、元となる著作物の著作権を継承させた上で頒布を認める条件である。また、ＢＹ－ＮＤは、著作権者の表示を要求し、投稿した著作物を複製、頒布、展示、実演を行うにあたり、いかなる改変も禁止する条件であり、ＢＹ－ＮＣは、著作権者の表示を要求し、投稿した著作物に対する複製、頒布、展示、実演を非営利目的での利用に限定する条件である。ＢＹ－ＮＣ－ＳＡは、著作権者の表示を要求し、投稿した著作物に対する複製、頒布、展示、実演を非営利目的での利用に限定し、元となる著作物の著作権を継承させた上で頒布を認める条件である。ＢＹ－ＮＣ－ＮＤは、著作権者の表示を要求し、投稿した著作物に対する複製、頒布、展示、実演を非営利目的での利用に限定し、投稿した著作物を複製、頒布、展示、実演を行うにあたり、いかなる改変も禁止する条件である。

【００２９】

なお、図４に示すようなウェブページにおいて、ラジオボタンＢ２の初期状態は、投稿に対する利用規約に同意しないことを示す状態に設定されており、また、ラジオボタンＢ３の初期状態は、投稿する著作物に対して時刻認証を行わないことを示す状態に設定されている。また、ラジオボタン群Ｂ４の初期状態は、いずれかの利用条件も選択されていない状態に設定されている。

【００３０】

ユーザは、著作物をＣＧＭウェブサイトに投稿する場合、端末装置１０を操作し、投稿ボタンＢ１をウェブブラウザ上で押下する。この結果、端末装置１０は、例えば、ＯＳ（Operating System）のファイルシステムを立ち上げ、自装置内の記憶部（不図示）に記憶された著作物の電子データ（以下、「著作物データ」と称する）から投稿を行うデータをユーザに選択させる。端末装置１０は、投稿を行う著作物データが選択された状態で、ラジオボタンＢ２が利用規約に同意することを示す状態に選択されている場合、すなわちユーザの確定操作が行われたときに、著作物データを著作物保護支援装置１００に送信する（ステップＳ１１４）。この結果、端末装置１０は、著作物データをアップロードする。

【００３１】

著作物データには、著作物の内容を電子化（バイナリ変換）したデータと、著作物のタイトルと、各種ラジオボタンの状態を示す情報と、ＣＧＭウェブサイトを利用するユーザのアカウントＩＤとが含まれる。著作物データが送信される段階において、ラジオボタンＢ３の状態は、時刻認証を行うことを示す状態である場合も存在し、時刻認証を行わないことを示す状態（初期状態）である場合も存在する。また、ラジオボタン群Ｂ４の状態は、初期状態である場合も存在し、６種類の条件のうちいずれか１つが選択されている状態である場合も存在する。端末装置１０は、これらの各種ラジオボタンの状態に基づく要求情報とユーザのアカウントＩＤを示す情報とを、著作物データと共に著作物保護支援装置１００に送信する。

【００３２】

ウェブサイト提供部１１０は、端末装置１０から送信された著作物データを記憶部１４０に記憶させ、当該著作物データを埋め込んだウェブページを表示させるためのテキスト文書等を生成する（ステップＳ１１６）。これによって、著作物保護支援装置１００は、ネットワークＮＷを介して、アップロード（投稿）された著作物データを埋め込んだウェブページを不特定多数の端末装置１０に対して表示させることができる。この結果、ユーザが投稿した著作物は、著作物保護支援装置１００が管理するウェブサイト上で共有される。

【００３３】

対分散ネットワーク処理部１２０は、端末装置１０から著作物データがアップロードされる際に、同時に時刻認証を求める要求情報が送信されているか否かを判定する（ステップＳ１１８）。そして、対分散ネットワーク処理部１２０は、時刻認証を求める要求情報が送信されている場合、アップロードされた電子データに対して時刻認証処理を実施する。

【００３４】
以下、対分散ネットワーク処理部１２０による時刻認証処理を説明する。
符号化処理部１２４は、受信した要求情報に基づいて、ユーザにより選択されたＣＣライセンスを抽出し、抽出したＣＣライセンスを２進数のコードに変換（符号化）する。以下、ＣＣライセンスをコード化したものを、「ＣＣコード」と記載する。なお、符号化処理部１２４において、ＣＣライセンスをＣＣコードに変換する際に参照される符号化のプロトコル（手順）は、実施形態によって適宜変更される場合がある。そのため、本実施形態では、過去に参照された符号化のプロトコルと、現在に参照される符号化のプロトコルとを区別するため、符号化のプロトコルには、更新の度に変更されるバージョン番号（２進数）が付与されるものとする。
【００３５】
図５は、各ＣＣライセンスの種別に対するＣＣコードの一例を示す図である。符号化処理部１２４は、例えば、ラジオボタン群Ｂ４の状態からＣＣライセンスを抽出した後、図５に示すＣＣライセンスとＣＣコードとの対応テーブルを参照して、コード化を行う。
【００３６】
ハッシュ化処理部１２６は、著作物データに含まれる著作物の内容を示すデータに対して、不可逆的な一方向の関数としてハッシュ関数を用いて、固定長のハッシュ値を生成する。ハッシュ化処理部１２６は、例えば、暗号学的ハッシュ関数の一つであるＲＩＰＥＭＤ－１６０を用いて、著作物の内容データをハッシュ値に変換する。以下、著作物の内容データがハッシュ値に変換されたものを、「検証用ハッシュＨｖ」と記載する。なお、ハッシュ化処理部１２６は、ＲＩＰＥＭＤ－１６０に代えて、ＳＨＡ－２５６等のアルゴリズムを用いてデータをハッシュ値に変換してもよい。
【００３７】
図６は、検証用ハッシュＨｖに変換可能な著作物データの種類の一例を示す図である。図６に示すように、ハッシュ化処理部１２６は、例えば、拡張子が「ｔｘｔ、ｄｏｃ、ｐｐｔ、ｘｌｓ、ｐｄｆ」等のテキストデータを検証用ハッシュＨｖに変換することができる。また、同様に、ハッシュ化処理部１２６は、拡張子が「ｂｍｐ、ｐｎｇ、ｊｐｇ、ｇｉｆ」等の画像データや、拡張子が「ｍｐ３、ｗｍａ、ｗａｖ」等の音声データ、拡張子が「ａｖｉ、ｍｐ４」等の映像データ等を検証用ハッシュＨｖに変換することができる。
【００３８】
また、ハッシュ化処理部１２６は、著作物データに含まれる著作物のタイトルと、端末装置１０に対してウェブサイト提供部１１０により提供されたＣＧＭウェブサイトのＩＤと、当該ＣＧＭウェブサイト利用するユーザのアカウントＩＤとを組み合わせ、組み合わせた情報を、ＲＩＰＥＭＤ－１６０を用いてハッシュ値に変換する。以下、著作物のタイトル、ＣＧＭウェブサイトのＩＤ、およびアカウントＩＤを組み合わせた情報がハッシュ値に変換されたものを、「検索用ハッシュＨｓ」と記載する。
【００３９】
図７は、対分散ネットワーク処理部１２０のハッシュ化処理部１２６により行われるハッシュ化処理の様子を示す図である。図７の例では、ハッシュ化処理部１２６は、ＲＩＰＥＭＤ－１６０を用いて、検索用ハッシュＨｓと検証用ハッシュＨｖとを生成する。
【００４０】
格納処理部１２８は、著作物データに対して時刻認証を行うために、著作物データを上述したトランザクションに格納する（ステップＳ１２０）。具体的には、格納処理部１２８は、符号化処理部１２４により符号化されたＣＣコードと、符号化処理部１２４により参照される符号化のプロトコルのバージョン番号と、ハッシュ化処理部１２６により変換された検証用ハッシュＨｖと、ハッシュ化処理部１２６により変換された検索用ハッシュＨｓと、識別子とを、トランザクション内の所定のフィールドに埋め込む。識別子とは、トランザクションに格納する全データの冒頭に追加される情報である。例えば、格納処理部１２８は、ブロックチェーンに格納した著作物データを容易に検索できるように識別子を所定のフィールドに埋め込む。これによって、著作物保護支援装置１００は、ブロック

チェーンから抽出したブロック内から、著作物データが埋め込まれたトランザクションを容易に抽出することができる。また、所定のフィールドとは、ビットコインの出金額や、送金先にビットコインを送信する際に必要になる送金先の公開鍵のハッシュ値等が埋め込まれる場所（例えば“scriptPubKey”）である。

【００４１】

なお、格納処理部１２８は、所定のフィールドに埋め込むデータ量に制限が設けられている場合、検証用ハッシュＨｖおよび検索用ハッシュＨｓにおける一部のデータを埋め込むようにしてもよい。例えば、所定のフィールドに埋め込むデータ量が４０バイトに制限されている場合、格納処理部１２８は、検証用ハッシュＨｖの冒頭から２０バイトのデータと、検索用ハッシュＨｓの冒頭から１０バイトのデータとを埋め込むようにすると好適である。

【００４２】

図８は、所定のフィールドに埋め込むデータの一例を示す図である。図８の例の場合、所定のフィールドには４０バイトの容量制限が設けられている。従って、著作物保護支援装置１００は、埋め込むデータ量が４０バイト以内になるように、例えば、識別子を５バイト、バージョン番号を１バイト、ＣＣコードを１バイト、検索用ハッシュＨｓを１０バイト、検証用ハッシュＨｖを２０バイトとする。なお、著作物保護支援装置１００は、図８に示す拡張ビット（３バイト）のような領域を設け、埋め込むデータ容量に余裕を持たせてもよい。

【００４３】

図９は、時刻認証の対象となる著作物データの一例を示す図である。図９に示す著作物データは、テキストデータである。また、当該テキストデータには、ＢＹ－ＮＣ－ＮＤのＣＣライセンスを示す情報が付与されている。図１０は、トランザクションに埋め込まれるデータの一例を示す図である。図１０に示すデータは、図９に示す著作物データを元に生成したデータである。図１０に示すように、トランザクションには、１０進数の数値、あるいはアルファベット等で構成される４０バイトのデータが埋め込まれる。

【００４４】

通信制御部１２２は、トランザクション内の所定のフィールドに対して、変換された著作物データが格納処理部１２８によって埋め込まれた場合、著作物データが埋め込まれたトランザクションを、端末装置２０の全ての装置に送信する。すなわち、通信制御部１２２は、著作物データが埋め込まれたトランザクションをブロードキャストする（ステップＳ１２２）。

【００４５】

図１１は、著作物データが埋め込まれたトランザクションＴＸをブロードキャストする様子を示す図である。図１１に示すように、トランザクションＴＸが分散ネットワーク内にブロードキャストされた後、分散ネットワーク内の端末装置２０のうちいずれかの装置は、直近のブロックの生成時刻から現ブロックの生成を開始する時刻までの間に蓄積したトランザクションＴＸをまとめて１つのブロックに生成する。これによって、分散ネットワーク内の端末装置２０が記憶するブロックチェーンが更新される。なお、トランザクションＴＸからブロックを生成する処理に時間を要するため、ブロックチェーンの更新には、ある程度（例えば１０分程度）の遅延が生じる。すなわち、著作物保護支援装置１００は、ユーザから時刻認証の要求を受けてから、時刻認証が完了するまで遅延時間を要する。

【００４６】

従って、本願の出願人は、以下の実験を行い、ブロックチェーンの更新に要する時間を導出した。実験では、Ｕｂｕｎｔｕ１４．０４ＬＴＳのＯＳを使用し、Ｎｏｄｅ．ｊｓというプラットフォームと、ビットコインのクライアント（ビットコイン；Ｃｏｒｅｖ０．９．３．０）とを用いて実験を行った。サーバーサイドの言語は、Ｊａｖａｓｃｒｉｐｔ（登録商標）を使用し、フロントエンドの言語は、Ｊａｄｅを使用した。

【００４７】

図１２は、データ量ごとに著作物の内容を示すデータをハッシュ化する際に要する時間を導出した結果の一例を示す図である。図１２の例では、１１個の異なるサイズの映像データを利用し、各映像データのハッシュ化が完了するまでの時間を示している。いずれのデータも、１分以内にハッシュ化処理が完了している。

【００４８】

図１３は、分散ネットワークに支払う手数料に応じた遅延時間の変化の一例を示す図である。また、図１４は、図１３に示す実験結果を得るために用いた手数料の一例を示す図である。ビットコインのブロックチェーンの更新タイミングは、ビットコイン用のアプリケーションプログラムを実行して分散ネットワークに支払われる手数料に応じて決められる。例えば、手数料が多額である場合、トランザクションをブロックにする処理を端末装置２０に速く実施してもらえる。すなわち、ブロックチェーンの更新時に生じる遅延時間が短くなる。

【００４９】

図１３の例では、手数料の金額に対する遅延時間の影響は少なく、ビットコインのプロトコルに決められた最低金額の手数料０．０００００１ＢＴＣ（０．３８円相当）であっても、平均遅延は１２分程度であった。従って、現行著作権登録制度において，登録の所要費用は１件につき３０００円以上，所要時間は通常６ヶ月となっていることから、本実験からビットコインのブロックチェーンを用いて時刻認証を行うことは、社会的効率向上とコスト削減に繋がることが示唆される。

【００５０】

図１５は、ブロックチェーンに著作物データを格納した後に著作物データを変更した際に行われる時刻認証の場面を概略的に示す図である。図１５の例の場合、ユーザが時刻Ａの時点で創作したコンテンツ（著作物）を、時刻Ｂにおいて端末装置１０を操作してＣＧＭウェブサイトに投稿すると共に、ＣＣライセンスを選択した場合、著作物保護支援装置１００は、時刻Ｂにおいて投稿されたコンテンツ（著作物）をトランザクションに埋め込み、ブロックチェーン上に格納させる。これによって、ブロックチェーン上に格納されたコンテンツ（著作物）には、時刻情報が付与されることになる。

【００５１】

ユーザは、例えば、時刻Ｃの時点で、ブロックチェーン上に格納されたコンテンツ（著作物）のＣＣライセンスを変更した場合、著作物保護支援装置１００は、ＣＣライセンスが変更されたことを示すために、ＣＣライセンスを変更したデータを、時刻Ｂ時点でトランザクションに埋め込んだデータとは異なるデータとして新たにトランザクションに埋め込み、新しいブロックを端末装置２０に生成させる。これによって、著作物保護支援装置１００は、ブロックチェーン上には、時刻Ｂ時点に時刻認証を依頼された著作物データと、時刻Ｃ時点に時刻認証を依頼された著作物データとを格納させることができる。これによって、ユーザは、ＣＣライセンスの変更前後で、著作物に対して時刻認証を行うことができる。

【００５２】

図１６は、ブロックチェーンを用いて時刻認証を行った著作物の著作権が侵害された場合において、侵害行為の証明を説明するための図である。図１６の例では、時刻Ｔ１において、ユーザＡは、創作した著作物$Ｃ_{0}$を、著作物保護支援装置１００から提供されるＣＧＭウェブサイトに投稿する。このとき、ユーザＡは、複製を許可しない旨（All rights reserved）のＣＣライセンスを選択する。時刻Ｔ２において、ユーザＢは、ユーザＡにより投稿された著作物$Ｃ_{0}$を元に改変した著作物Ｃ’を当該ＣＧＭウェブサイトに投稿する。

【００５３】

時刻Ｔ３において，ユーザＡは、時刻Ｔ１において投稿した著作物$Ｃ_{0}$を改変した著作物$Ｃ_{1}$を、ＢＹ－ＮＣライセンス設定で投稿するともに著作物$Ｃ_{0}$の投稿を削除する。時刻Ｔ４において、ユーザＡは、ユーザＢの侵害行為を発見し、侵害行為が行われているウェブページのテキスト文書（ＨＴＭＬデータ）を、ＣＧＭウェブサイトに投稿する。著作

物保護支援装置１００は、侵害行為が行われているウェブページのテキスト文書データに対してハッシュ化を行い、トランザクションに埋め込む。著作物保護支援装置１００は、侵害行為が行われているウェブページのテキスト文書データが埋め込まれたトランザクションをブロードキャストする。この結果、分散ネットワーク上のブロックチェーンに侵害行為が行われているウェブページのテキスト文書データが格納される。すなわち、著作物保護支援装置１００は、侵害行為が行われているウェブページのテキスト文書データに対して、時刻認証を行う。

【００５４】

その後、ユーザＡは、ユーザＢに侵害行為の停止を要求する。これに対して、ユーザＢは、ユーザＡの要求を拒否する。従って、ユーザＡは、ユーザＢを損害賠償の訴訟に持ち込む。このような場合、ユーザＢは、著作物Ｃ’の投稿を削除し、侵害行為を否認する可能性がある。そこで、ユーザＡは、時刻認証を行った証拠、すなわちブロックチェーン上に格納されているウェブページのテキスト文書データを裁判所に提出し、ユーザＢが時刻Ｔ４において侵害行為を行ったと訴える。

【００５５】

このような場合、ユーザＢは、ユーザＡが最初に投稿した著作物C_0の投稿を削除したということに付け込み、投稿した著作物Ｃ’を自分が創作したオリジナルの著作物だと弁解する可能性がある。しかしながら、著作物C_0の投稿先は著作物保護支援装置１００が提供するＣＧＭウェブサイトであることから、ユーザＡは容易に著作物C_0が確かに時刻Ｔ１に存在していたことを証明することができる。このような場合、さらにユーザＢは、現存する著作物C_1がＢＹ－ＮＣライセンスであることに付け込み、著作物C_0も同じＣＣライセンスであると主張し、著作物C_0の改変は許されるものであると弁解する可能性がある。

【００５６】

しかしながら、ユーザＡは、ブロックチェーンを使用して、容易に時刻Ｔ１から時刻Ｔ３までの期間において、確かに著作物C_0は、「All rights reserved」に設定されていたことを証明することができる。このような場合であっても、ユーザＢは、さらに著作物Ｃ’が時刻Ｔ３以降に制作されたものだと弁解する可能性がある。しかしながら、著作物Ｃ’を著作物保護支援装置１００が提供するＣＧＭウェブサイトに投稿し、著作物Ｃ’に対して時刻認証を行っていることから、ユーザＡは、容易に著作物Ｃ’が確かに時刻Ｔ２時点で存在していたことを証明することができる。この結果、ユーザＢは、弁解の余地がなくなり、ユーザＡは、侵害行為の停止要求をユーザＢに受け入れさせることができる。

【００５７】

図１７は、一実施形態における著作物保護支援装置１００の処理の流れの一例を示すフローチャートである。著作物保護支援装置１００は、例えば、所定周期で、本フローチャートの処理を実行する。

【００５８】

まず、通信制御部１２２は、記憶部１４０に予め記憶させておいたビットコイン用のアプリケーションプログラムを実行する（ステップＳ２００）。次に、通信制御部１２２は、分散ネットワーク内の端末装置２０と同期を行うように通信インターフェースを制御する（ステップＳ２０２）。次に、ウェブサイト提供部１１０は、端末装置１０からアクセス要求を受信したか否かを判定する（ステップＳ２０４）。次に、著作物保護支援装置１００は、端末装置１０からアクセス要求を受信していない場合（ステップＳ２０４；Ｎｏ）、ステップＳ２００の処理に戻る。

【００５９】

ウェブサイト提供部１１０は、端末装置１０からアクセス要求を受信した場合（ステップＳ２０４；Ｙｅｓ）、端末装置１０から端末ＩＤを取得し（ステップＳ２０６）、取得した端末ＩＤを記憶部１４０に記憶させる。次に、ウェブサイト提供部１１０は、記憶部１４０に記憶させた端末ＩＤによって示される端末装置１０に対して、著作物の投稿を受け付けるウェブページをウェブブラウザ上で表示させるためのテキスト文書等を送信する

（ステップＳ２０８）。
【００６０】
次に、著作物保護支援装置１００は、ユーザの確定操作が行われた端末装置１０から著作物データを受信したか否かを判定する（ステップＳ２１０）。著作物保護支援装置１００は、端末装置１０から著作物データを受信しない場合（ステップＳ２１０；Ｎｏ）、本フローチャートの処理を終了する。ウェブサイト提供部１１０は、端末装置１０から著作物データを受信した場合（ステップＳ２１０；Ｙｅｓ）、著作物データを記憶部１４０に記憶させると共に、当該著作物データと共に端末装置１０から送信された各種ラジオボタンの状態に基づく要求情報とユーザのアカウントＩＤを示す情報とを記憶部１４０に記憶させる（ステップＳ２１２）。
【００６１】
次に、著作物保護支援装置１００は、記憶部１４０に記憶させた著作物データを埋め込んだウェブページを表示させるためのテキスト文書等を生成する（ステップＳ２１４）。次に、対分散ネットワーク処理部１２０は、端末装置１０から著作物データがアップロードされる際に、同時に時刻認証を求める要求情報が受信したか否かを判定する（ステップＳ２１６）。著作物保護支援装置１００は、端末装置１０から時刻認証を求める要求情報が受信していない場合（ステップＳ２１６；Ｎｏ）、本フローチャートの処理を終了する。
【００６２】
符号化処理部１２４は、端末装置１０から時刻認証を求める要求情報が受信した場合（ステップＳ２１６；Ｙｅｓ）、受信した要求情報に基づいて、ユーザにより選択されたＣＣライセンスを抽出し、抽出したＣＣライセンスをＣＣコードに変換する（ステップＳ２１８）。次に、ハッシュ化処理部１２６は、著作物データに含まれる著作物の内容データに対してハッシュ化を行い、検証用ハッシュＨｖを生成する（ステップＳ２２０）。
【００６３】
次に、ハッシュ化処理部１２６は、著作物のタイトルと、ＣＧＭウェブサイトのＩＤと、ユーザのアカウントＩＤとを組み合わせ、組み合わせた情報に対してハッシュ化を行い、検索用ハッシュＨｓを生成する（ステップＳ２２２）。次に、格納処理部１２８は、符号化処理部１２４により符号化されたＣＣコードと、符号化処理部１２４により参照される符号化のプロトコルのバージョン番号と、ハッシュ化処理部１２６により変換された検証用ハッシュＨｖと、ハッシュ化処理部１２６により変換された検索用ハッシュＨｓと、識別子とを、トランザクション内の所定のフィールドに埋め込む（ステップＳ２２４）。
【００６４】
次に、通信制御部１２２は、著作物データが埋め込まれたトランザクションをブロードキャストする（ステップＳ２２６）。これによって本フローチャートの処理が終了する。
【００６５】
以上、一実施形態における著作物保護支援装置１００によれば、通信インターフェースを用いて、時刻認証の要求情報が付された著作物データを取得し、時刻認証の要求情報が付された著作物データに基づく情報を、ブロックチューンを共有する分散ネットワークに対して発信するように、通信インターフェースを制御することにより、所望の著作物に対して、簡易かつ安価に時刻認証を行うことができる。
【００６６】
また、一実施形態における著作物保護支援装置１００によれば、ＣＣライセンスの要求情報が付された著作物データを取得することにより、ＣＧＭウェブサイトを利用するユーザの著作権帰属の証明および侵害の証拠保全、さらにＣＣライセンスの証拠能力向上を行うことができる。
【００６７】
なお、上述した端末装置１０または端末装置２０は、著作物保護支援装置１００の対分散ネットワーク処理部１２０に相当する機能を有していてもよい。図１８は、端末装置１０によって著作物データが埋め込まれたトランザクションＴＸがブロードキャストされる

様子を示す図である。例えば、端末装置１０または端末装置２０は、自身内部に記憶された著作物データをブロックチェーンのフォーマットに格納するために、当該著作物データに対してハッシュ化および符号化の対分散ネットワーク処理を行い、対分散ネットワーク処理を実施したデータをトランザクションＴＸに埋め込み、当該トランザクションＴＸを分散ネットワークに送信する。これによって、例えば、ユーザが、ＣＧＭウェブサイトに著作物を投稿する前に、予め投稿対象の著作物データに時刻認証をしておきたい場合、端末装置１０または端末装置２０は、著作物データに基づく情報をトランザクションＴＸに埋め込みことで、ブロックチェーン上に著作物を示すデータを格納する、この結果、端末装置１０または端末装置２０は、著作物に対して時刻認証を行うことができる。

【００６８】

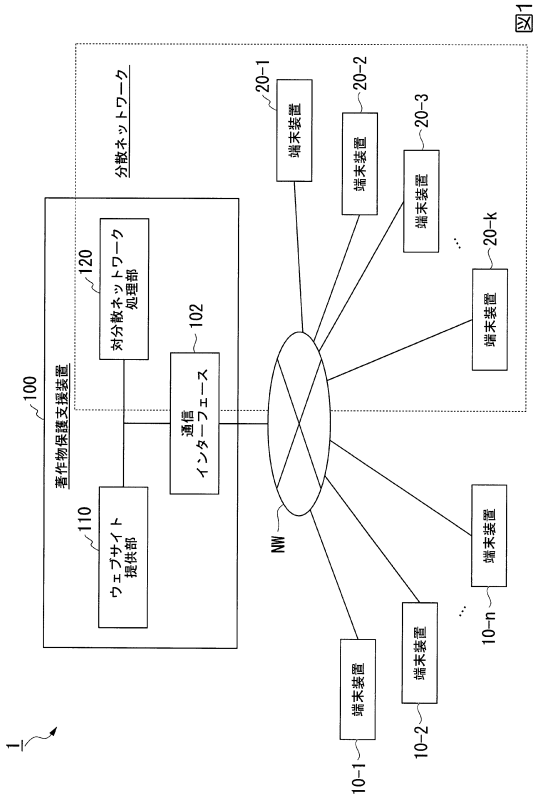
以上、本発明を実施するための形態について実施形態を用いて説明したが、本発明はこうした実施形態に何等限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々の変形及び置換を加えることができる。

【符号の説明】

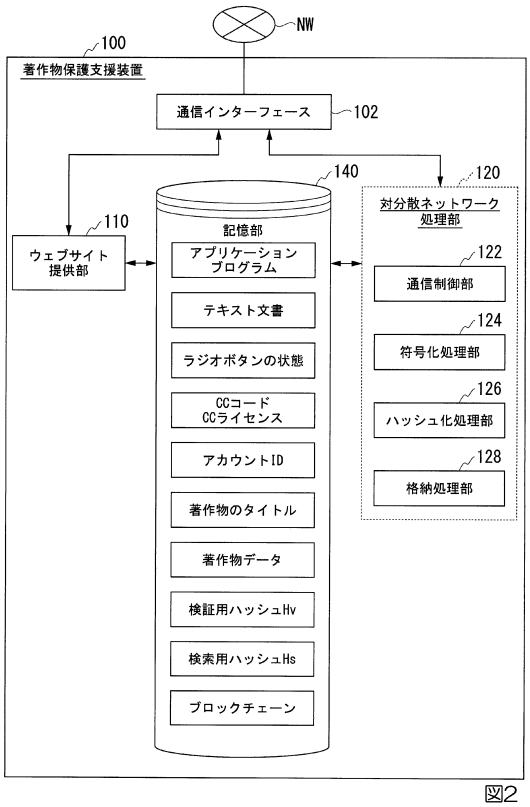
【００６９】

１‥分散ネットワークシステム、１０、２０…端末装置、１００…著作物保護支援装置、１０２…通信インターフェース、１１０…ウェブサイト提供部、１２０…対分散ネットワーク処理部

【図１】



【図２】



【図３】

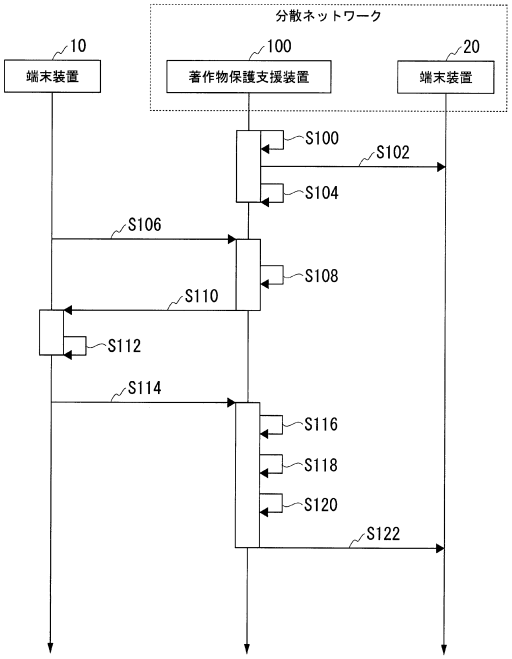


図3

【図４】

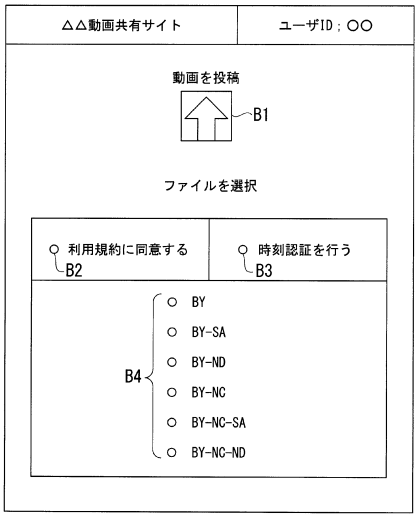


図4

【図５】

CCライセンス	CCコード
BY	00000001
BY-SA	00000010
BY-ND	00000011
BY-NC	00000100
BY-NC-SA	00000101
BY-NC-ND	00000110

図5

【図６】

著作物データの種類	拡張子	検証用ハッシュHv
テキストデータ	txt, doc, ppt, xls, pdf…	…
画像データ	bmp, png, jpg, gif…	…
音声データ	mp3, wma, wav…	…
映像データ	mp4, avi…	…

図6

【図７】

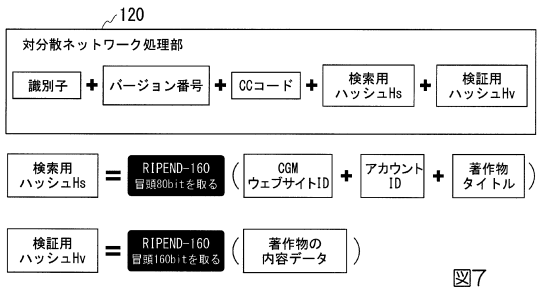


図7

【図８】

格納情報	内容	データ量 (byte)
識別子	BITCC	5
バージョン番号	00000001	1
CCコード	BY-NC-ND	1
検索用ハッシュHs	ハッシュ値 (ウェブサイトID+アカウントID+タイトル)	10
検証用ハッシュHv	ハッシュ値 (著作物の内容データ)	20
拡張ビット	-	3

図8

【図９】

BITCC 00 CC BY NC ND John Doe 分散型時刻認証方法を使...ｾﾐﾅｰﾚｼﾞｭﾒ_chou-1016.docx

4249544343O006f985854h5254k23247478i95261k1144e65788322181157i156j55h,10000000

図9

【図１０】

OP_RETURN 42533652221798322f7fd335863aa36824111a64889631744174aaa8bb5740000000
(decoded)j(BIYMUsspp<nmnslgpwuybvvawYUKD

図10

【図１１】

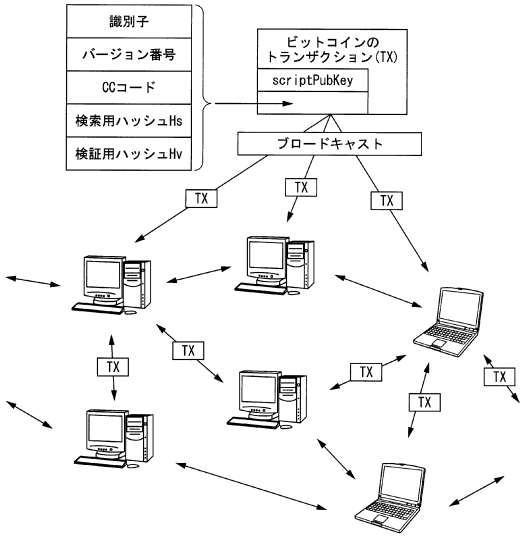


図11

【図１２】

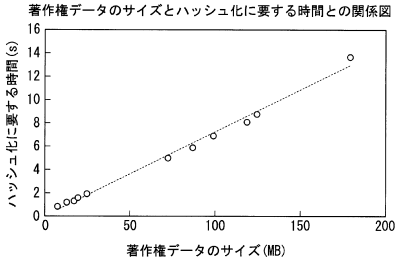


図12

【図１３】

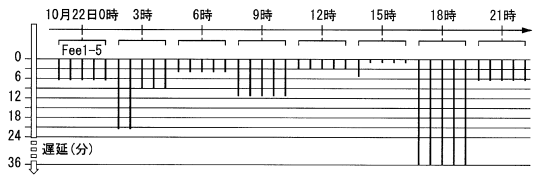


図13

【図１４】

手数料	ビットコイン	日本円
Fee 1	0.00001	0.38
Fee 2	0.00005	1.9
Fee 3	0.0001	3.8
Fee 4	0.0005	19
Fee 5	0.001	38

図14

【図１５】

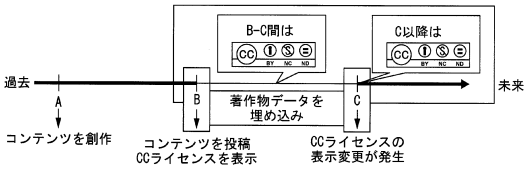


図15

【図１６】

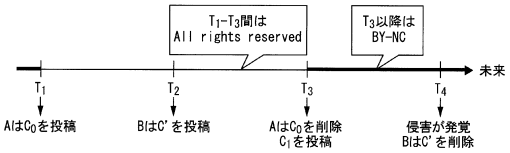


図16

【図１７】

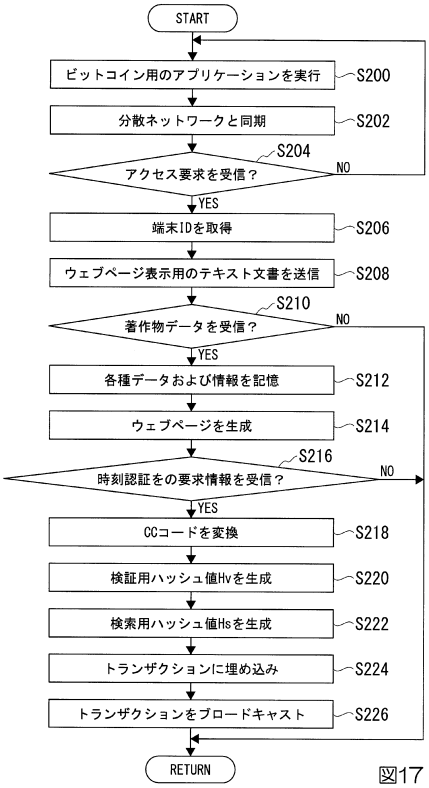


図17

【図１８】

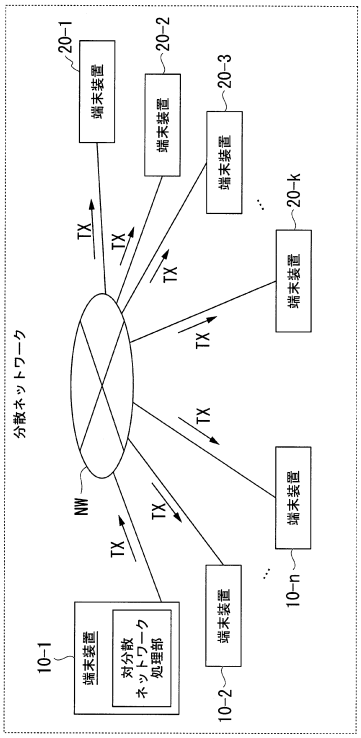


図18

フロントページの続き

(72)発明者　高　月菲
茨城県つくば市天王台一丁目１番１　国立大学法人筑波大学内

審査官　青木　重徳

(56)参考文献　特開２００７－２４９５６９（ＪＰ，Ａ）
特開２００８－２１７０４８（ＪＰ，Ａ）
特開２００９－２０５１９７（ＪＰ，Ａ）
特表２０１５－５０９２３６（ＪＰ，Ａ）
米国特許出願公開第２０１０／０１８５５０２（ＵＳ，Ａ１）
山崎　重一郎，仮想通貨の技術的イノベーションと課題，電子情報通信学会２０１４年基礎・境界ソサイエティ大会講演論文集，日本，一般社団法人　電子情報通信学会，２０１４年　９月９日，ＡＫ－２－１，ｐｐ．SS-5～SS-6

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／１６
Ｇ０６Ｑ　５０／１０