(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年12月24日(24.12.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/255207 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G06F 21/64* (2013.01)
G06F 21/10 (2013.01)

(21) 国際出願番号： PCT/JP2019/023904

(22) 国際出願日： 2019年6月17日(17.06.2019)

(25) 国際出願の言語： 日本語

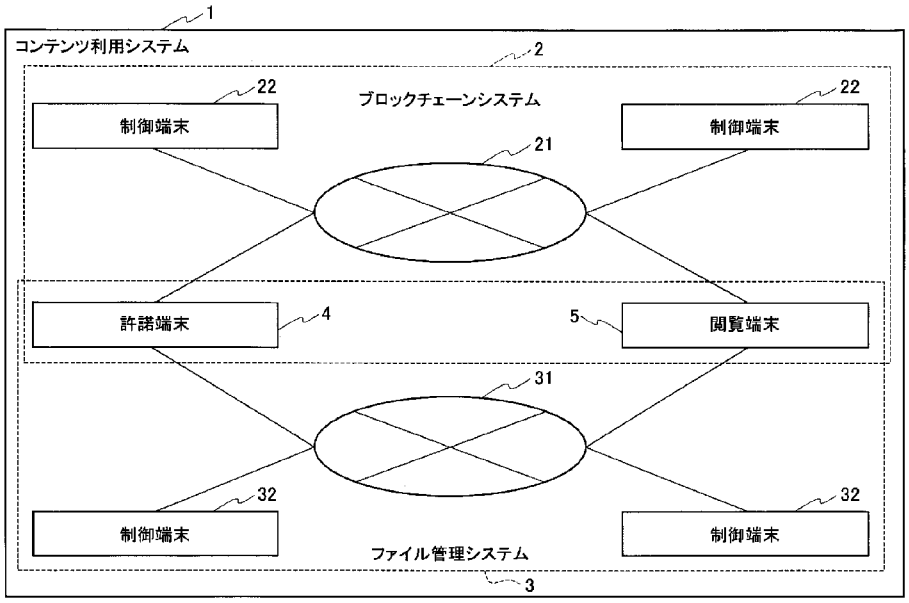
(26) 国際公開の言語： 日本語

(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 渡邊 大喜 (**WATANABE Hiroki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 大橋 盛徳(**OHASHI Shigenori**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 石田 達郎(**ISHIDA Tatsuro**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 藤村 滋 (**FUJIMURA Shigeru**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 中平 篤(**NAKADAIRA Atsushi**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

(54) **Title:** CONTENT USE SYSTEM, ACCEPTANCE TERMINAL, BROWSING TERMINAL, DISTRIBUTION TERMINAL AND CONTENT USE PROGRAM

(54) 発明の名称： コンテンツ利用システム、許諾端末、閲覧端末、配信端末、および、コンテンツ利用プログラム



1 Content use system
2 Block chain system
3 File management system
4 Acceptance terminal
5 Browsing terminal
22, 32 Control terminal

(57) **Abstract:** This acceptance terminal 4 is provided with: a generating unit 423 that uses a content public key for content and a user public key for a person browsing the content to generate access information concerning the content; and a registering unit 424 that registers the access information in a block chain. The access information includes an integrated public key formed by integrating the content public key and the user public key, a message for the content, and a content signature in which the message is signed with a content private key corresponding to the content public key. A browsing terminal 5 is provided with: a confirming unit 523 that acquires the access information of requested content from the block chain and verifies, with the integrated public key for the access information, an integrated signature formed by integrating

WO 2020/255207 A1

[続葉有]

(74) 代理人: 三好 秀和, 外 (MIYOSHI Hidekazu et al.); 〒1050001 東京都港区虎ノ門１丁目２番８号 虎ノ門琴平タワー Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告（条約第21条(3)）

a user signature that is the message of the access information signed with the user private key, and the content signature of the access information; and a requesting unit 524 that transmits a content request that includes the user signature or the integrated signature when the verification is successful.

(57) 要約：許諾端末４は、コンテンツのコンテンツ公開鍵と、コンテンツの閲覧者のユーザ公開鍵とを用いて、前記コンテンツに対するアクセス情報を生成する生成部４２３と、アクセス情報をブロックチェーンに登録する登録部４２４とを備え、アクセス情報は、コンテンツ公開鍵とユーザ公開鍵とを集約した集約公開鍵と、コンテンツ用のメッセージと、メッセージをコンテンツ公開鍵に対応するコンテンツ秘密鍵で署名したコンテンツ署名とを含み、閲覧端末５は、要求するコンテンツのアクセス情報をブロックチェーンから取得し、アクセス情報のメッセージをユーザ秘密鍵で署名したユーザ署名と、アクセス情報のコンテンツ署名とを集約した集約署名を、アクセス情報の集約公開鍵で検証する確認部５２３と、検証に成功した場合、ユーザ署名または前記集約署名を含むコンテンツ要求を送信する要求部５２４とを備える。

明　細　書

発明の名称 ：

コンテンツ利用システム、許諾端末、閲覧端末、配信端末、および、コンテンツ利用プログラム

技術分野

[0001] 本発明は、コンテンツ利用システム、許諾端末、閲覧端末、配信端末、および、コンテンツ利用プログラムに関する。

背景技術

[0002] デジタル仮想通貨の取引において、非中央集権型の分散台帳の一種であるブロックチェーンが用いられる。ブロックチェーンでは、参加者間の仮想通貨の取引の情報がブロックという単位でまとめられ、ブロックチェーンを形成する。ブロックチェーンの構造に関し、ブロックチェーンは、チェーンという言葉のとおり、ブロックが直前のブロックと紐付けが行われる形で記録される。具体的には、直前のブロックのハッシュ値をブロックの中に含むことで、各ブロックが紐付けされる。

[0003] これにより、ある時点のブロックの中に含まれた取引情報を改竄するには、ブロックのハッシュ値が変わることからそれ以降全てのブロックの改竄が必要となる。また、ブロックを追加する際、それを追加することによってブロックのハッシュ値が特定条件と合致するような付加情報（ナンス）を発見する処理（マイニング）が必要である。この処理の計算量が非常に大きなことも相まって、ブロックチェーンは、改竄に対して極めて強固な仕組みにより形成される。

[0004] またEthereum（イーサリアム）において、プログラマブルブロックチェーンが提案されている。コントラクトとも称されるプログラムコードが、予めブロックチェーンに登録される。コントラクトの実行を指定したトランザクションが入力されると、トランザクションがブロックに含まれる際、そのプログラムコードが実行される。実行結果は、ブロックチェーンのステートデ

ータに格納される。

[0005] 一方、特権的なノードを仮定しない分散ファイル管理システムとして、IPFS(InterPlanetary File System)がある（非特許文献１参照）。IPFSにおいて、ファイルは特定サイズのブロックに分割されて、IPFSに属する端末において管理される。ファイルは、ハッシュ値から生成される識別子により認識され、ファイルの改竄はできない。IPFSは、分散性およびID構造により、透明性および信頼性を確保できる。

[0006] またブロックチェーンの改竄に対して極めて強固な仕組みである点に着目し、分散ファイル管理システムと、ブロックチェーンとを融合したシステムがある（非特許文献２参照）。非特許文献２において、ファイルは、チャンクに分割される。各チャンクは、DAG(Directed Acyclic Graph：向非巡回グラフ)でまとめられ、チャンクには、リンク先のチャンクの情報が記載される。非特許文献２においてDAGを形成する全てのチャンクの識別子が、それぞれブロックチェーンに登録される。

先行技術文献

非特許文献

[0007] 非特許文献1：Juan Banet, “IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3)”, ＜https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf＞

非特許文献2：Mathis Steichen, 他、 “Blockchain-Based, Decentralized Access Control for IPFS” ：＜https://www.researchgate.net/publication/327034734_Blockchain-Based_Decentralized_Access_Control_for_IPFS＞

発明の概要

発明が解決しようとする課題

[0008] 非特許文献２では、IPFSで管理されるファイルへアクセス可能なユーザのリストは、ブロックチェーン上のスマートコントラクト内で保持される。リストにおいて、ユーザはEthereum上の識別子、すなわちEthereumアドレスに

よって指定される。アドレスはユーザが生成した楕円曲線暗号による公開鍵から算出され、ユーザが端末で管理する秘密鍵に一意に紐づいている。

[0009] 非特許文献２では、このリストはブロックチェーン上に共有される。このため、ユーザ自身が当該ファイルのアクセス権を確認可能であると同時に、他の第三者からも本ユーザがアクセス可能であることが判別されるといったプライバシー上の懸念がある。匿名性を高めるための一つの方法は、固定のアドレス（公開鍵）を使い回さずに、ファイルごとに異なるアドレスを使用することである。しかし、この方法は、複数のアドレス分の秘密鍵を生成および管理する必要が生じ、ユーザビリティを損ねる。

[0010] 本発明は、上記課題を鑑みてなされたものであり、本発明の目的は、ブロックチェーン上で管理されるアクセス情報の匿名性を確保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

[0011] 上記目的を達成するため、本発明の一態様は、許諾端末と閲覧端末とを備えるコンテンツ利用システムであって、前記許諾端末は、コンテンツのコンテンツ公開鍵と、前記コンテンツの閲覧者のユーザ公開鍵とを用いて、前記コンテンツに対するアクセス情報を生成する生成部と、前記アクセス情報をブロックチェーンに登録する登録部と、を備え、前記アクセス情報は、前記コンテンツ公開鍵と前記ユーザ公開鍵とを集約した集約公開鍵と、前記コンテンツ用のメッセージと、前記メッセージを前記コンテンツ公開鍵に対応するコンテンツ秘密鍵で署名したコンテンツ署名とを含み、前記閲覧端末は、要求するコンテンツのアクセス情報を前記ブロックチェーンから取得し、前記アクセス情報のメッセージをユーザ秘密鍵で署名したユーザ署名と、前記アクセス情報のコンテンツ署名とを集約した集約署名を、前記アクセス情報の集約公開鍵で検証する確認部と、検証に成功した場合、前記ユーザ署名または前記集約署名を含むコンテンツ要求を送信する要求部と、を備える。

[0012] 本発明の一態様の許諾端末は、コンテンツのコンテンツ公開鍵と、前記コンテンツの閲覧者のユーザ公開鍵とを用いて、前記コンテンツに対するアク

セス情報を生成する生成部と、前記アクセス情報をブロックチェーンに登録する登録部と、を備え、前記アクセス情報は、前記コンテンツ公開鍵と前記ユーザ公開鍵とを集約した集約公開鍵と、前記コンテンツ用のメッセージと、前記メッセージを前記コンテンツ公開鍵に対応するコンテンツ秘密鍵で署名したコンテンツ署名とを含む。

[0013] 本発明の一態様の閲覧端末は、要求するコンテンツのアクセス情報をブロックチェーンから取得し、前記アクセス情報のメッセージをユーザ秘密鍵で署名したユーザ署名と、前記アクセス情報のコンテンツ署名とを集約した集約署名を、前記アクセス情報の集約公開鍵で検証する確認部と、検証に成功した場合、前記ユーザ署名または前記集約署名を含むコンテンツ要求を、送信する要求部と、を備える。

[0014] 本発明の一態様の配信端末は、要求するコンテンツのアクセス情報をブロックチェーンから取得し、前記アクセス情報のメッセージをユーザ秘密鍵で署名したユーザ署名と、前記アクセス情報のコンテンツ署名とを集約した集約署名を、前記アクセス情報の集約公開鍵で検証する確認部と、検証に成功した場合、前記ユーザ署名を含むコンテンツ要求を、許諾端末に送信する要求部と、コンテンツ要求に応じて、当該コンテンツに対応するアクセス情報を前記ブロックチェーンから取得し、前記アクセス情報のコンテンツ署名と、前記コンテンツ要求に含まれるユーザ署名とを集約した集約署名を前記アクセス情報の集約公開鍵で検証し、前記コンテンツ要求を許諾するか否かを判定する共有制御部と、を備える。

[0015] 本発明の一態様の配信端末は、要求するコンテンツのアクセス情報をブロックチェーンから取得し、前記アクセス情報のメッセージをユーザ秘密鍵で署名したユーザ署名と、前記アクセス情報のコンテンツ署名とを集約した集約署名を、前記アクセス情報の集約公開鍵で検証する確認部と、検証に成功した場合、前記集約署名を含むコンテンツ要求を、許諾端末に送信する要求部と、コンテンツ要求に応じて、当該コンテンツに対応するアクセス情報を前記ブロックチェーンから取得し、前記コンテンツ要求に含まれる前記集約

署名を前記アクセス情報の集約公開鍵で検証し、前記コンテンツ要求を許諾するか否かを判定する共有制御部と、を備える。

[0016] 本発明の一態様は、上記許諾端末として、コンピュータを機能させることを特徴とするコンテンツ利用プログラムである。

[0017] 本発明の一態様は、上記閲覧端末として、コンピュータを機能させることを特徴とするコンテンツ利用プログラムである。

[0018] 本発明の一態様は、上記配信端末として、コンピュータを機能させることを特徴とするコンテンツ利用プログラムである。

発明の効果

[0019] 本発明によれば、ブロックチェーン上で管理されるアクセス情報の匿名性を確保する技術を提供することができる。

図面の簡単な説明

[0020] [図1]第１の実施形態に係るコンテンツ利用システムの全体構成図である。

[図2A]アクセス情報の一例を示す図である。

[図2B]アクセス情報の他の一例を示す図である。

[図3]許諾端末の構成例を示すブロック図である。

[図4]閲覧端末の構成例を示すブロック図である。

[図5]第１の実施形態の動作を示すシーケンス図である。

[図6]第１の実施形態の動作を示すシーケンス図である。

[図7]第２の実施形態に係るコンテンツ利用システムの全体構成図である。

[図8]配布端末の構成例を示すブロック図である。

[図9]第２の実施形態の動作を示すシーケンス図である。

[図10]第２の実施形態の動作を示すシーケンス図である。

[図11]コンピュータの構成図である。

発明を実施するための形態

[0021] 以下、本発明の実施の形態について、図面を参照して説明する。図面の記載において、同一部分には同一符号を付し説明を省略する。

[0022] ［実施形態の概要］

本実施形態では、通常のブロックチェーン上のアドレスとは別に、匿名化用の公開鍵を定義する。この匿名用公開鍵は、ユーザを識別するための匿名アドレスとしても機能するが、限られた関係者しか知り得ないとする。例えば、アクセス権を与える許諾者は、アクセス権が与えられるユーザから匿名用公開鍵を受け取り、匿名用公開鍵によってユーザを識別する。一方で、この匿名用公開鍵は、関係者以外には配布されないとする。

[0023] この匿名用公開鍵は、暗号学的に集約特性を持つ。例えばｎ個の公開鍵P_1, P_2,P_3,…,P_nが定義されていた場合、その公開鍵は以下のように集約される。

[0024] [数1]

$$P = P_1 + P_2 + P_3 + \cdots + P_n$$

[0025] 各公開鍵と対となる秘密鍵を使用した署名σ_1, σ_2, σ_3,…, σ_nを下記のように集約した場合、集約された署名σは、集約された公開鍵Pによって検証可能である。

[0026] [数2]

$$\sigma = \sigma_1 + \sigma_2 + \sigma_3 + \cdots + \sigma_n$$

[0027] このような署名鍵の集約が可能な署名アルゴリズムとして、Schnorr署名やBLS（Boneh, Lynn, Shacham）署名などが知られている。

[0028] 本実施形態では、この集約特性を利用してユーザの匿名化を実現する。匿名化は、ファイルを登録し、アクセス情報（アクセス制御情報）を生成する許諾者の許諾端末によって行われる。まず許諾端末（許諾者）は、コンテンツファイルとユーザの組合せに対して、集約が可能な１つの公開鍵P_c（以降、「匿名用コンテンツ公開鍵」と呼ぶ）を生成する。その後、許諾端末は、匿名用コンテンツ公開鍵P_cと、ユーザから受け取った匿名用ユーザ公開鍵P_uとを集約し、匿名化された集約公開鍵Pを生成する。

[0029] 許諾端末は、この集約公開鍵Pをアクセス権の許諾先としてアクセス情報を作成し、ブロックチェーンに登録する。この時、許諾端末は、アクセス情報として、集約公開鍵Pと、任意のメッセージmと、匿名用コンテンツ秘密鍵s_c

で署名したメッセージmに対する署名値σ_cとを登録する。

[0030] 集約の元となる匿名用コンテンツ公開鍵P_cとその秘密鍵s_cの鍵ペアは、ファイルとユーザの組合せに対し１つランダムに生成される。そのため、例えユーザが匿名用ユーザ公開鍵P_uを使い回していたとしても、集約される結果である集約公開鍵Pは毎回異なる値となる。これにより、ユーザが固定の匿名用ユーザ公開鍵P_uを用いていたとしても、本実施形態では、匿名性が向上する仕組みを提供できる。

[0031] ［第１の実施形態］

（コンテンツ利用システムの全体構成）

図１は、本発明の第１の本実施形態に係るコンテンツ利用システムの全体構成を示す図である。本実施形態コンテンツ利用システム１は、ブロックチェーンシステム２（分散台帳システム）と、ファイル管理システム３とを備える。

[0032] ブロックチェーンシステム２は、許諾端末４と、閲覧端末５とを備える。これらの端末４、５は、P2P(Peer to Peer)ネットワークであるブロックチェーンのネットワーク２１に自律分散的に接続される。なお、ブロックチェーンシステム２は、許諾端末４および閲覧端末５の他にも、複数の制御端末２２を備えていてもよい。

[0033] ブロックチェーンシステム２に属する各端末４、５、２２は、後述するブロックチェーン（分散台帳）と、ブロックチェーンを同期するためのブロックチェーン制御部とを備える。各端末は、ブロックチェーンに記録されたデータおよびトランザクションを相互に検証し、系を維持している。ブロックチェーンは、当該システム２に属する端末間で共有される。ブロックチェーンは、システムに属する端末が発行したトランザクションを含むブロックが繋がったデータである。

[0034] なお、本実施形態のブロックチェーンは、スマートコントラクト型ブロックチェーンであって、例えばブロックチェーン基盤技術の１つであるEthereumを用いてもよい。Ethereumは、ブロックチェーンを、状態遷移を記録する分

散台帳として用いるためのアプリケーション開発プラットフォームである。ただし、ブロックチェーンは、Ethereumに限定されるものではなく、Ethereum以外を用いてもよい。

[0035] ファイル管理システム３は、許諾端末４と、閲覧端末５とを備える。これらの端末４、５は、ファイル管理システム３のネットワーク３１に接続される。なお、ファイル管理システム３は、許諾端末４および閲覧端末５の他にも、複数の制御端末３２を備えていてもよい。ファイル管理システム３に属する各端末４、５、３２は、ネットワーク３１を介してP2P接続される。

[0036] 本実施形態では、ファイル管理システム３は、例えばIPFS等の非中央集権型の分散ファイル管理システムである場合について説明する。分散ファイル管理システムは、当該システムに属する各端末が分散してファイルを管理するシステムである。ただし、ファイル管理システム３は、分散ファイル管理システムに限らない。例えば、ファイル管理システム３に、通常のクラウド型の中央管理されたストレージを利用しても良い。

[0037] 許諾端末４は、コンテンツへのアクセス（閲覧）を許可する許諾者が利用する端末（ノード）である。許諾端末４は、ブロックチェーンシステム２と、ファイル管理システム３とに接続される。閲覧端末５は、コンテンツの閲覧者が利用する端末であって、ブロックチェーンシステム２と、ファイル管理システム３に接続される。許諾端末４および閲覧端末５は、複数であってもよい。

[0038] ブロックチェーンシステム２の制御端末２２は、当該システム２を利用するユーザのうち、コンテンツの許諾者および閲覧者以外のユーザが利用する端末である。ファイル管理システム３の制御端末３２は、当該システム３を利用するユーザのうち、コンテンツの許諾者および閲覧者以外のユーザが利用する端末である。制御端末２２、３２の数は、図示する例ではそれぞれ２つであるが、その数に限定されるものではない。また、ブロックチェーンシステム２の制御端末２２とファイル管理システム３の制御端末３２とは、互いに異なる端末であっても良いし、１つの端末がブロックチェーンの機能と

、ファイル管理の機能とを実装しても良い。

[0039] （アクセス情報）

本実施形態のブロックチェーンには、コンテンツ利用システム１において利用されるコンテンツデータのアクセス情報（アクセス制御情報）が登録される。アクセス情報は、ファイル管理システム３におけるコンテンツデータの識別子と、閲覧可能なユーザとを紐づける。

[0040] 図２Ａ、図２Ｂを参照して、本実施形態のアクセス情報について説明する。アクセス情報は、ファイル管理システム３に登録するコンテンツデータへのアクセス権を管理するための情報である。アクセス情報は、許諾端末４により作成される。アクセス情報は、ブロックチェーン上に公開され、ブロックチェーンのネットワーク２１に接続された他の端末からも閲覧可能である。アクセス情報は、各コンテンツの識別子に対して、集約公開鍵と、メッセージと、署名とが対応付けて格納されている。

[0041] 図２Ａ、図２Ｂに示すアクセス情報は、コンテンツ識別子と、集約公開鍵と、メッセージと、匿名用コンテンツ秘密鍵によって署名された署名（署名値）とを含む。コンテンツ識別子は、コンテンツデータを一意に特定する。コンテンツ識別子は、例えば、ファイル管理システム３に登録されたコンテンツのハッシュ値などであっても良い。

[0042] 図２Ａに示す例では、コンテンツ識別子C^iが示され、ここでｉ＝1,2,3とし、それぞれ異なるコンテンツを扱うことを示す。このコンテンツ識別子はユーザを認証するための要素セット（P^i，m^i，$\sigma_c{}^i$）と紐づいている。ここでPは集約公開鍵、mは任意のメッセージ、σ_cはメッセージmに対して匿名用コンテンツ秘密鍵を用いて作成した署名である。

[0043] 図２Ｂは、１つのコンテンツ識別子に対して、複数ユーザが紐づいている例を示す。この場合、コンテンツ識別子は、C^iで表現される。このコンテンツ識別子は、ユーザを認証するための要素セット（$P^{i,j}$，$m^{i,j}$，$\sigma_c{}^{i,j}$）と紐づいている。ここでｉ＝1,2,3はそれぞれ異なるコンテンツを扱うことを示し、ｊ＝1,2は異なるユーザを扱うことを示す。

[0044] なお、以降は、複数コンテンツおよび複数のユーザの場合を除き、アクセス情報を、コンテンツ識別子Cと、認証要素セット（P，m，σ_c）とで表記し、上付き添字を省略して記述する。

[0045] 以下、署名の集約について説明する。本実施形態では、署名集約を可能とするために双線形写像（ペアリング）を利用した署名アルゴリズムを用いる。

[0046] G_1, G_2を素数位数ｑの加法巡回群とし、双線形写像ｅを用いて下記が成り立つ位数ｑの乗法巡回群G_Tが存在する。

[0047] [数3]

$$e: G_1 \times G_2 \rightarrow G_T$$

[0048] また任意長の入力Mが写像した先がG_1となるようにハッシュ関数を定める。

[0049] [数4]

$$H : M \rightarrow G_1$$

[0050] 有限体F_qから秘密鍵ｓを以下のように選ぶ。

[0051] [数5]

$$s \in \mathbb{F}_q$$

[0052] 公開パラメータQ ∈G_2を生成元として、公開鍵Pは以下となる。

[0053] [数6]

$$P \leftarrow sQ \in G_2$$

[0054] この時、上記の秘密鍵ｓを用いて、メッセージmのハッシュ値H(m)に対する署名は以下となる。

[0055] [数7]

$$\sigma \leftarrow sH(m) \in G_1$$

[0056] このとき、以下の式が成り立つかを検証する。

[0057]

[数8]

$$e(H(m),P)=e(\sigma,Q)$$

[0058] 上記検証において、ペアリングの双線形性を利用する。ペアリングの双線形性においては、下記の関係式が成り立つ。

[0059] [数9]

$$e(aX,bY)=e(X,Y)^{ab}$$

[0060] したがって、上記の検証過程では、P＝ｓQ、σ＝ｓH(m)であるからσが正しい署名であるならば、下記の式が成り立つ。

[0061] [数10]

$$e(H(m),P)=e(H(m),sQ)=\ e(H(m),Q)^{s}=\ e(sH(m),Q)=\ e(\sigma,Q)$$

[0062] ここでペアリングを用いた署名においては、署名鍵と公開鍵において集約特性が成り立つことを確認する。

[0063] 例えば公開鍵、秘密鍵、署名の組（P_1，s_1，σ_1）に対して異なる組（P_2，s_2，σ_2）を定義し、次のように集約された署名σと公開鍵Pを作るとする。

[0064] [数11]

$$\sigma=\sigma_1+\sigma_2=\ (s_1+s_2)H(m)$$
$$P=P_1+P_2=(s_1+s_2)Q$$

[0065] この集約署名σと集約公開鍵Pに対しても下記の双線形性を利用して、署名の検証が可能である。

[0066] [数12]

$$e(H(m),P)=e(H(m),(s_1+s_2)Q)=\ e(H(m),Q)^{s_1+s_2}$$
$$=\ e((s_1+s_2)H(m),Q)=\ e(\sigma,Q)$$

[0067] ここで、アクセス情報の説明に戻る。アクセス情報における集約公開鍵Pは、匿名用コンテンツ公開鍵P_cと匿名用ユーザ公開鍵P_uとを集約したものである。この時、検証に係る式は下記のようになる。

[0068]

[数13]

$$e(H(m),P) = e(H(m),P_c + P_u) = e(\sigma_c + \sigma_u, Q)$$

[0069] 上記より、ユーザからメッセージmに対する署名値σ_uが提出されれば、集約公開鍵Pを使って集約署名値が検証可能となる。この署名値σ_uは、匿名用ユーザ公開鍵P_uと対になる秘密鍵s_uを所持していないと作ることはできない。

[0070] 従ってアクセス情報を見たユーザは、自身が持つ匿名用ユーザ公開鍵P_uを使って、自身にアクセス権があるか否かをブロックチェーン上で確認できる。

[0071] （許諾端末）

図３を参照して、本実施形態の許諾端末４を説明する。許諾端末４は、記憶装置４１、処理装置４２、通信制御装置４３を備える。

[0072] 記憶装置４１には、処理装置４２が処理を実行するための入力データ、出力データおよび中間データなどの各種データを記憶する。処理装置４２は、記憶装置４１に記録されたデータを読み書きし、通信制御装置４３とデータを入出力して、許諾端末４における処理を実行する。通信制御装置４３は、許諾端末４がブロックチェーンのネットワーク２１またはファイル管理のネットワーク３１に属する端末と通信可能に接続するためのインタフェースである。

[0073] 記憶装置４１は、ブロックチェーン４１１と、許諾端末４が有するコンテンツデータ４１２と、鍵管理データ４１３と、許諾端末４の各機能を実行するための許諾端末用プログラム４１４とを記憶する。

[0074] ブロックチェーンデータ４１１は、例えばブロックチェーン基盤のEthereumでは、ブロックチェーン本体のデータ（ブロックチェーン）と、ステートデータとを含む。ブロックチェーン本体のデータは、複数のブロックがチェーン状に連結して形成される。各ブロックは、複数のトランザクションを含む。トランザクションは、例えば、スマートコントラクトを設定し、また、ス

マートコントラクトの関数を実行する。

[0075] ステートデータは、スマートコントラクト毎にデータ領域が設けられている。スマートコントラクトの実行に伴って、対応するスマートコントラクトのデータ領域が更新される。本実施形態においては、ステートデータとして、上述したアクセス情報を管理するスマートコントラクトと、そのデータとが記憶装置４１に登録される。

[0076] コンテンツデータ４１２は、コンテンツ本体であるコンテンツファイル（コンテンツともいう）と、コンテンツをファイル管理システム３で動作させるために必要な管理データ（ルーティング情報等）と含む。

[0077] 鍵管理データ４１３は、本実施形態で使用する署名用の秘密鍵を保管する。本実施形態では２種類の鍵がある。第１の鍵は、ブロックチェーンのトランザクションを生成するための秘密鍵（ブロックチェーン用秘密鍵）である。この秘密鍵は、ブロックチェーンシステム２のプロトコルに従って、トランザクションに署名を付与するための秘密鍵である。Ethereumでは楕円曲線暗号を使用した秘密鍵を保持している。

[0078] 第２の鍵は、本実施形態特有の匿名化のための秘密鍵（匿名用秘密鍵）である。本実施形態においては、この秘密鍵は、BLS署名を生成するための秘密鍵を用いるものとするが、鍵の集約が可能な署名であればBLS署名に限られない。匿名用秘密鍵には、コンテンツに関する秘密鍵（匿名用コンテンツ秘密鍵）とユーザに関する秘密鍵（匿名用ユーザ秘密鍵）とを含む。

[0079] 処理装置４２は、ブロックチェーン制御部４２１と、ファイル管理部４２２と、生成部４２３と、登録部４２４と、共有制御部４２５とを備える。

[0080] ブロックチェーン制御部４２１は、ネットワーク２１に接続された端末と自律分散的に協調してブロックチェーンの系を維持する。ブロックチェーン制御部４２１は、ブロックチェーン４１１にアクセスし、ブロックチェーン４１１のデータを読み出し、または、更新する。

[0081] ファイル管理部４２２は、許諾者（ユーザ）からの指示に基づいて、任意のコンテンツをファイル管理システム３に登録し、コンテンツ識別子Cを取得

する。本実施形態では、IPFS等の分散型ファイル管理システムを使用しているため、まずは、許諾端末４（ローカル端末）にコンテンツ（コンテンツファイル）が保存される。コンテンツは、共有制御部４２５の制御によって、必要に応じてファイル管理システム３を介して他の端末に共有可能である。従って、他の端末にコンテンツのありかを共有する際に必要な管理データ（ルーティング情報）などは、通信制御装置４３介してファイル管理システム３のネットワーク３１で共有される。

[0082] 生成部４２３は、コンテンツのコンテンツ公開鍵と、コンテンツの閲覧者のユーザ公開鍵とを用いて、コンテンツに対するアクセス情報を生成する。具体的には、生成部４２３は、コンテンツへのアクセスを許諾する閲覧者（ユーザ）の匿名用ユーザ公開鍵P_uと、コンテンツ識別子Cとのペアを入力として、匿名用コンテンツ鍵ペア（P_c, s_c）を生成し、認証要素セット（P,m,σ_c）を出力する。生成部４２３は、匿名用ユーザ公開鍵P_uをあらかじめ取得しているものとする。

[0083] 認証要素セットは、匿名用コンテンツ公開鍵Pcと、ユーザ公開鍵P_uとを集約した集約公開鍵Pと、コンテンツ用のメッセージmと、メッセージmを匿名用コンテンツ公開鍵P_uに対応する匿名用コンテンツ秘密鍵s_cで署名したコンテンツ署名σ_cとを含む。なお、匿名用コンテンツ鍵ペアを生成するときに必要な公開パラメータQは事前に設定され、他のユーザと共有しているものとする（すなわち$P_c = s_c Q$）。

[0084] ここで、生成部４２３は、入力された匿名用ユーザ公開鍵P_uと、生成した匿名用コンテンツ公開鍵P_cとを用いて鍵集約（$P= P_u + P_c$）を行う。σ_cは、メッセージmを匿名用コンテンツ秘密鍵s_cで署名した署名値である。すなわち、$\sigma_c = s_c H(m)$である。

[0085] 署名用のメッセージmは、（P_u,C）のペア毎（つまり、ユーザとコンテンツの組み合わせ毎）に、異なるmが生成できれば良い。例えば、集約署名Pにコンテンツ識別子Cを結合したデータをmとしても良い。その場合、PとCによりmが決定されるため、敢えてmを指定せずに、認証要素セットとして（P, σ_c）

を出力しても良い。生成部４２３が生成した匿名用コンテンツ秘密鍵s_cは、鍵管理データ４１３として記憶装置４１に格納される。

[0086] 登録部４２４は、生成部４２３で生成したアクセス情報を、ブロックチェーン上に登録する。登録部４２４は、通信制御装置４３を介してブロックチェーンネットワーク２１にトランザクションを発行することにアクセス情報をブロックチェーン上に登録する。本実施形態では、登録部４２４は、コンテンツ識別子Cに対して認証要素セット（P, m, σ_c）または（P, σ_c）を対応する値として紐づけて登録するためのトランザクションを発行する。

[0087] 共有制御部４２５は、コンテンツ要求に応じて、当該コンテンツに対応する認証要素セット（P, m, σ_c）（すなわち、アクセス情報）をブロックチェーンから取得し、認証要素セットのコンテンツ署名σ_cと、コンテンツ要求に含まれるユーザ署名σ_uとを集約した集約署名σを認証要素セットの集約公開鍵Pで検証し、コンテンツ要求を許諾するか否かを判定する。

[0088] 具体的には、共有制御部４２５は、許諾者が自端末に登録したコンテンツを、他端末からの共有の要求を受けた際に、要求元にアクセス権があるか否かを判定し、アクセス権がある場合に、共有する。例えばここで、閲覧端末５からファイル管理システム３を介し、コンテンツ識別子を指定してコンテンツ共有の要求があるとする。閲覧端末５は、コンテンツ識別子に対応する、閲覧者の匿名用署名σ_uを添付して要求を行う。要求を受けた共有制御部４２５は、ブロックチェーンからアクセス情報を取得し、閲覧者にアクセス権があるか否かを判定する。

[0089] 判定は以下の手順で行われる。まず、共有制御部４２５は、コンテンツ識別子に対応する認証要素セット（P, m, σ_c）に対して、集約署名$\sigma = \sigma_c + \sigma_u$を算出する。次に，共有制御部４２５は、集約署名$\sigma$を集約公開鍵Pで検証する。即ち、共有制御部４２５は、$e(H(m), P) = e(\sigma, Q)$が成り立つか否かにより、閲覧者の署名$\sigma_u$を検証する。共有制御部４２５は、前記式が成り立つ場合、コンテンツ識別子に対応するコンテンツを共有する。

[0090] （閲覧端末）

図４を参照して、本実施形態の閲覧端末５を説明する。閲覧端末５は、記憶装置５１と、処理装置５２と、通信制御装置５３とを備える。

[0091] 記憶装置５１には、処理装置５２が処理を実行するための入力データ、出力データおよび中間データなどの各種データを記憶する。処理装置５２は、記憶装置５１に記録されたデータを読み書きし、通信制御装置５３とデータを入出力して、閲覧端末５における処理を実行する。通信制御装置５３は、閲覧端末５がブロックチェーンシステム２のネットワーク２１またはファイル管理システムのネットワーク３１に属する端末と通信可能に接続するためのインタフェースである。

[0092] 記憶装置５１は、ブロックチェーン５１１と、コンテンツデータ５１２と、鍵管理データ５１３と、閲覧端末５の各機能を実行するための閲覧端末用プログラム５１４とを記憶する。ブロックチェーン５１１は、許諾装置４のブロックチェーン４１１と同様であるため、ここでは説明を省略する。

[0093] コンテンツデータ５１２は、閲覧端末５が有するコンテンツの本体であるコンテンツファイルと、当該コンテンツをファイル管理システム３で動作させるために必要な管理データ（ルーティング情報等）と含む。

[0094] 鍵管理データ５１３は、本実施形態で使用する署名用の秘密鍵を保管する。第１の鍵は、ブロックチェーンのトランザクションを生成するための秘密鍵（ブロックチェーン用秘密鍵）である。第２の鍵は、匿名用秘密鍵である。匿名用秘密鍵には、ユーザに関する秘密鍵（匿名用ユーザ秘密鍵）を含む。

[0095] 処理装置５２は、ブロックチェーン制御部５２１と、鍵管理部５２２と、確認部５２３と、要求部５２４と、同期部５２５とを備える。ブロックチェーン制御部５２１は、許諾装置４のブロックチェーン制御部４２１と同様であるため、ここでは説明を省略する。

[0096] 鍵管理部５２２は、閲覧者（ユーザ）からの指示に基づいて、匿名用ユーザ鍵ペア（P_u，s_u）を生成する。許諾端末４と共有する公開パラメータQにより、$P_u = s_u Q$が成り立つ。生成した秘密鍵s_uは、鍵管理データ５１３として記

憶装置５１に格納される。

[0097] 確認部５２３は、コンテンツ識別子Cで識別されるコンテンツに対して、ブロックチェーン上でアクセス権が設定されているか否かを確認する。具体的には、確認部５２３は、要求するコンテンツのアクセス情報（認証要素セット（P,m,σ_c））をブロックチェーンから取得し、アクセス情報のメッセージmをユーザ秘密鍵s_uで署名したユーザ署名σ_uと、アクセス情報のコンテンツ署名σ_cとを集約した集約署名σを、アクセス情報の集約公開鍵Pで検証する。

[0098] ここで、閲覧端末５は、事前に許諾端末４に匿名用ユーザ公開鍵P_uを共有し、許諾端末４によってブロックチェーン上に，コンテンツ識別子Cに対する匿名用ユーザ公開鍵P_uに係るアクセス権が設定されているとする。この場合、確認部５２３は、コンテンツ識別子Cをクエリとしてブロックチェーン上のスマートコントラクトに問い合わせ、認証要素セット（P,m,σ_c）を取得する。認証要素セットには、mが明示的に含まれず、PとCを結合して一意に算出される値をmとしても良い。

[0099] 確認部５２３は、メッセージmに対する閲覧者の署名σ_uを生成する。閲覧者の署名σ_uは、$\sigma_u = s_u H(m)$となる。確認部５２３は、集約署名$\sigma = \sigma_c + \sigma_u$を算出する。そして、確認部５２３は、集約公開鍵Pと、算出した集約署名σとを用いて、$e(H(m),P) = e(\sigma,Q)$が成り立つか否かにより、閲覧者の署名σ_uを検証する。確認部５２３は、前記式が成り立つ場合、署名検証に成功したことと、検証に用いた閲覧者の署名σ_uとを出力する。

[0100] 要求部５２４は、検証に成功した場合、ユーザ署名σ_uを含むコンテンツ要求を送信する。具体的には、要求部５２４は、閲覧者（ユーザ）からの指示に基づいて、任意のコンテンツの取得をファイル管理システム３に要求する。要求には、コンテンツ識別子Cおよび閲覧者のユーザ署名σ_uが必要である。要求部５２４は、確認部５２３を用いて、コンテンツのアクセス権を確認し、閲覧者の署名σ_uを取得する。そして、要求部５２４はコンテンツ識別子Cおよび閲覧者の署名σ_uと含むコンテンツ要求をファイル管理システム３に

送信する。ファイル管理システム３は、コンテンツ識別子Cをキーとして、実体となるファイルを所有する許諾端末４にアクセスし、許諾端末４の共有制御部４２５に対してコンテンツ識別子Cおよび閲覧者の署名σ_uを含むコンテンツ要求を送信する。

[0101] 同期部５２５は、コンテンツ要求に対して、許諾端末４からコンテンツの共有が許諾された場合に、ファイル管理システム３を介してコンテンツファイルを閲覧端末５に同期する。同期されたコンテンツファイルは記憶装置５１に格納される。

[0102] （コンテンツ利用システムの動作）

次に、本実施形態のコンテンツ利用システムの動作について説明する。

[0103] 図５および図６は、コンテンツ利用システムの動作を示すシーケンス図である。Ｓ１１からＳ１６は、許諾端末４がコンテンツを登録した際に、ブロックチェーン上に対応する認証要素セット（P, m, σ_c）を登録する処理である。Ｓ２１からＳ２８は、ブロックチェーン上に登録された（P, m, σ_c）を閲覧端末５が取得し、コンテンツファイルの共有を閲覧者の署名σ_uを添えて要求する処理である。Ｓ２９からＳ３４は、要求を受信した許諾端末４が集約署名を検証し、コンテンツファイルを送信する処理である。以下に、図５および図６を参照して具体的に説明する。

[0104] 許諾端末４は、許諾者からの指示に基づいて、任意のコンテンツをファイル管理システム３に登録する（Ｓ１１）。ファイル管理システム３がIPFSなどの分散ファイル管理システムの場合、Ｓ１１でファイル管理システム３に登録されるのは、端末のネットワークアドレス、コンテンツの場所などを示すルーティング情報であり、コンテンツ本体（コンテンツファイル）は許諾者端末４自身が保持する。なお、ファイル管理システム３が中央集権的なクラウドサーバ等の場合は、Ｓ１１でコンテンツ本体がファイル管理システム３に登録される。

[0105] 許諾端末４は、ファイル管理システム３から当該コンテンツに対するコンテンツ識別子Cを取得する（Ｓ１２）。許諾端末４（生成部４２３）は、アク

セス情報を生成する。具体的には、許諾端末４は、コンテンツへのアクセスを許諾する閲覧者（ユーザ）の匿名用ユーザ公開鍵P_uと、コンテンツ識別子Cとのペアを入力として、匿名用コンテンツ鍵ペア（P_c，s_c）を生成する（Ｓ１３）。

[0106] そして、許諾端末４は、匿名用ユーザ公開鍵P_uと、生成した匿名用コンテンツ公開鍵P_cとを用いて鍵集約（$P= P_u+P_c$）を行う（Ｓ１４）。また、許諾端末４は、匿名用コンテンツ鍵ペア（P_c，s_c）の秘密鍵s_cを用いて所定のメッセージmに署名し、署名値$\sigma_c = s_c H(m)$を生成する（Ｓ１５）。

[0107] そして、許諾端末４は、アクセス情報として、コンテンツ識別子Cと、認証要素セット（P,m,σ_c）とを、ブロックチェーン上に登録する（Ｓ１６）。具体的には、許諾端末４は、アクセス情報を登録するトランザクションを生成し、当該トランザクションをブロックチェーンのネットワーク２１に発行する。これにより、コンテンツ識別子Cの認証要素セット（P,m,σ_c）が、ネットワーク２１に接続された端末の記憶装置に、ブロックチェーンデータとして登録される。

[0108] 閲覧端末５は、閲覧者からの指示に基づいて、匿名用ユーザ鍵ペア（P_u，s_u）を生成する（Ｓ２１）。なお、許諾端末４と共有する公開パラメータQにより、$P_u = s_u Q$が成り立つ。

[0109] そして、閲覧端末５は、コンテンツ識別子Cのコンテンツを要求するために、当該コンテンツに対して、ブロックチェーン上でアクセス権が設定されているか否かを確認する。具体的には、閲覧端末５は、コンテンツ識別子Cをクエリとして、自身の閲覧端末５のブロックチェーン５１１上のスマートコントラクトに問い合わせ（Ｓ２２）、コンテンツ識別子Cに対応する認証要素セット（P,m,σ_c）を取得する（Ｓ２３）。

[0110] そして、閲覧端末５は、メッセージmに対する閲覧者の署名$\sigma_u = s_u H(m)$を生成する（Ｓ２４）。また、閲覧端末５は、集約署名$\sigma = \sigma_c + \sigma_u$を算出し、集約公開鍵Pと、算出した集約署名$\sigma$とを用いて、$e(H(m),P) = e(\sigma,Q)$が成り立つか否かにより、閲覧者の署名$\sigma_u$を検証する（Ｓ２５）。閲覧端

末５は、前記式が成り立つ場合、署名検証に成功したことと、検証に用いた閲覧者の署名σ_uとを出力する（Ｓ２６）。

[0111] そして、閲覧端末５は、閲覧者からの指示に基づいて、コンテンツをファイル管理システム３に要求する（Ｓ２７）。すなわち、閲覧端末５は、コンテンツ識別子Cと閲覧者の署名σ_uとを含むコンテンツ要求をファイル管理システム３に送信する。ファイル管理システム３は、コンテンツ識別子Cをキーとして、コンテンツファイルを所有する許諾端末４にアクセスし、許諾端末４に対してコンテンツ識別子Cおよび閲覧者の署名σ_uを含むコンテンツ要求を送信する（Ｓ２８）。

[0112] 許諾端末４は、許諾者が自端末５に登録したコンテンツを、閲覧端末５からの要求を受けた際に、閲覧端末５にアクセス権があるか否かを判定する。具体的には、許諾端末４は、自端末のブロックチェーン５１１にアクセスし、コンテンツ識別子Cに対応する認証要素セット（P, m, σ_c）を、ブロックチェーン５１１から取得する（Ｓ２９、Ｓ３０）。

[0113] 許諾端末４は、取得した認証要素セット（P, m, σ_c）に対して、集約署名$\sigma = \sigma_c + \sigma_u$を算出する（Ｓ３１）。そして、許諾端末４は、集約署名σを集約公開鍵Pで検証する。即ち、許諾端末４は、$e(H(m),P) = e(\sigma,Q)$が成り立つか否かを判定し、成り立つ場合、閲覧者にアクセス権があると判定し、コンテンツ識別子Cに対応するコンテンツを閲覧端末５と共有する（Ｓ３２）。

[0114] 許諾端末４は、コンテンツを共有する場合、Ｓ２８のコンテンツ要求に対して許諾する旨の応答と、コンテンツ識別子Cに対応するコンテンツファイルとを、ファイル管理システム３に送信する（Ｓ３３）。ファイル管理システム３は、Ｓ３３で受信したコンテンツファイルを要求元の閲覧端末５に送信する（Ｓ３４）。閲覧端末５は、コンテンツファイルを受信し、は記憶装置５１に格納する。

[0115] なお、本実施形態において、図２Ｂに示すように、一つのコンテンツ識別子に対し、複数のユーザが設定されている場合について説明する。コンテンツ識別子C^iに対してｉ＝１で、複数のユーザ（ｊ＝1,2,3,・・・,ｎ）に対す

るアクセス権が設定されている場合、許諾端末４および閲覧端末５は、全ての認証要素セット（$P^{1,j}$,$m^{1,j}$,$\sigma_c^{1,j}$）に対して、総当り的に署名検証を行う（図５：Ｓ２４、Ｓ２５、図６：Ｓ３１、Ｓ３２）。後述する、第２の実施形態でも同様である。

[0116] 以上説明した本実施形態では、許諾端末４は、コンテンツ公開鍵P_cとユーザ公開鍵P_uとを集約した集約公開鍵Pと、メッセージmと、メッセージmをコンテンツ公開鍵P_cに対応するコンテンツ秘密鍵s_cで署名したコンテンツ署名σ_cとを含む認証要素セット（アクセス情報）を、ブロックチェーンに登録する。

[0117] これにより、本実施形態では、ブロックチェーンで管理される権限（ここでは、コンテンツへのアクセス権限）を示すアクセス情報の匿名化を確保することができる。したがって、閲覧者（権限を設定される者）が複数のコンテンツに対して固定のユーザ公開鍵を使い回していたとしても、ブロックチェーンに登録されるアクセス情報には、集約公開鍵が設定される。集約公開鍵は、ユーザ公開鍵と、コンテンツ毎に異なるコンテンツ公開鍵とが、許諾者（権限を設定する者）によって集約された公開鍵である。すなわち、本実施形態では、ユーザ公開鍵はブロックチェーンに登録されず、ユーザ公開鍵を匿名化することができる。ブロックチェーンで公開されるアクセス情報（認証要素セット）は、集約公開鍵Pと、メッセージmと、コンテンツ署名σ_cであるため、第三者は匿名用に用いたユーザ公開鍵P_uを取得することができない。

[0118] 本実施形態では、ブロックチェーンに公開されたアクセス情報を用いて、アクセス権を与える許諾者、および、アクセス権を持つ閲覧者は、当該閲覧者がアクセス権を持つことを判別可能であるが、関係者（許諾者、閲覧者）以外の第三者からは、どのユーザがアクセス可能かを容易に判別できない仕組みを提供することができる。

[0119] また、本実施形態では、コンテンツごとに異なるユーザ公開鍵を使用し、ユーザ公開鍵を使い捨てる方式ではなく、固定された特定のユーザ公開鍵を

用いることができる。これにより、本実施形態では、複数のユーザ公開鍵の各々の秘密鍵を生成および管理する必要が生じないため、ユーザビリティの低下を回避することができる。

[0120] ［第２の実施形態］

以下に本発明の第２の実施形態について説明する。本実施形態は、コンテンツの配布が許諾端末以外からも行われる実施形態である。

[0121] （コンテンツ利用システムの全体構成）

図７は、第２の実施形態に係るコンテンツ利用システムの全体構成を示す図である。図示するコンテンツ利用システム１Ａは、配布端末６を備える点において、図１に示す第１の実施形態のコンテンツ利用システム１と異なり、その他は第１の実施形態のコンテンツ利用システム１と同様である。

[0122] 本実施形態において、コンテンツの実体であるコンテンツファイルは、許諾端末４だけでなく配布端末６からも配布される。配布端末６は、コンテンツの共用を閲覧者に許諾する権限を持たないが、コンテンツの実体を保持し、ブロックチェーン上に登録されたアクセス情報に従って、閲覧端末５にコンテンツを共有させる権限を有する。

[0123] 配布端末６の役割は、まず許諾端末４にコンテンツを要求し、取得したコンテンツを閲覧端末５に再配布することである。これにより、許諾端末４がコンテンツを集中管理することなく、分散して緩やかにコンテンツを流通させることができる。コンテンツの再配布については、アクセス情報に従って、限られたユーザのみに配布される。以下に、配布端末６について説明する。

[0124] （配布端末）

図８を参照して、本実施形態の配布端末６を説明する。配布端末６は、記憶装置６１と、処理装置６２と、通信制御装置６３とを備える。

[0125] 記憶装置６１には、処理装置６２が処理を実行するための入力データ、出力データおよび中間データなどの各種データを記憶する。処理装置６２は、記憶装置６１に記録されたデータを読み書きし、通信制御装置６３とデータ

を入出力して、配布端末６における処理を実行する。通信制御装置６３は、配布端末６がブロックチェーンのネットワーク２１またはファイル管理のネットワーク３１に属する端末と通信可能に接続するためのインタフェースである。

[0126] 記憶装置６１は、ブロックチェーン６１１と、コンテンツデータ６１２と、鍵管理データ６１３と、配布端末６の各機能を実行するための配布端末用プログラム６１４とを記憶する。ブロックチェーン６１１は、許諾装置４のブロックチェーン４１１と同様であるため、ここでは説明を省略する。

[0127] コンテンツデータ６１２は、配布端末６が有するコンテンツの本体であるコンテンツファイルと、当該コンテンツをファイル管理システム３で動作させるために必要な管理データ（ルーティング情報等）と含む。

[0128] 鍵管理データ６１３は、本実施形態で使用する署名用の秘密鍵を保管する。第１の鍵は、ブロックチェーンのトランザクションを生成するための秘密鍵（ブロックチェーン用秘密鍵）である。第２の鍵は、匿名用秘密鍵である。匿名用秘密鍵には、配信者の匿名用ユーザ秘密鍵を含む。

[0129] 処理装置６２は、ブロックチェーン制御部６２１と、鍵管理部６２２と、確認部６２３と、要求部６２４と、同期部６２５と、共有制御部６２６とを備える。ブロックチェーン制御部６２１は、図３に示す許諾装置４のブロックチェーン制御部４２１と同様であるため、ここでは説明を省略する。

[0130] 鍵管理部５２２は、配布者（ユーザ）からの指示に基づいて、匿名用ユーザ鍵ペア（P_d，s_d）を生成する。許諾端末４と共有する公開パラメータQにより、$P_d = s_dQ$が成り立つ。生成した秘密鍵s_dは、鍵管理データ６１３として記憶装置６１に格納される。

[0131] 許諾端末４は、配布者の匿名用ユーザ公開鍵P_dと、閲覧者の匿名用ユーザ公開鍵P_uとを、それぞれ事前に取得している（許諾端末４がこれらの公開鍵を取得する方法および経路は問わない）。許諾端末４が、コンテンツ識別子Cのコンテンツのアクセス権を、配布者および閲覧者に対して設定している場合、それぞれ異なる認証要素セット（P, m, σ_c）が生成される。ここでは、配

布者の認証要素セットをE_dとし、閲覧者の認証要素セットをE_uと記載する。本実施形態では、認証要素セットE_dおよびE_uが、ブロックチェーンに登録されている。

[0132] 確認部６２３は、コンテンツ識別子Cで識別されるコンテンツに対して、ブロックチェーン上でアクセス権が設定されているか否かを確認する。具体的には、確認部６２３は、要求するコンテンツのアクセス情報（認証要素セット（P,m,σ_c））をブロックチェーンから取得し、アクセス情報のメッセージmをユーザ秘密鍵で署名したユーザ署名と、アクセス情報のコンテンツ署名σ_cとを集約した集約署名σを、アクセス情報の集約公開鍵Pで検証する。

[0133] ここでは、配布端末６は、事前に許諾端末４に匿名用ユーザ公開鍵P_dを共有し、許諾端末４によって，ブロックチェーン上にコンテンツ識別子Cに対する匿名用ユーザ公開鍵P_dに係るアクセス権が設定されているとする。この場合、確認部６２３は、コンテンツ識別子Cをクエリとしてブロックチェーン上のスマートコントラクトに問い合わせ、全ての認証要素セット（P,m,σ_c）を取得する。認証要素セットには、mが明示的に含まれず、PとCを結合して一意に算出される値をmとしても良い。また、本実施形態では、配布端末６と閲覧端末５の各認証要素セットE_d、E_uが取得されるが、その他のユーザに対する認証要素セットが含まれていても良い。

[0134] 確認部６２３は、E_d、E_uを含む全ての認証要素セットに対して、次の処理を繰り返し、いずれかの認証要素セットで下記の式が成り立つ場合、署名検証に成功したと判定する。例えば、認証要素セットE_dについて、確認部６２３は、メッセージmに対する配布者の署名σ_dを生成する。閲覧者の署名σ_dは、$\sigma_d = s_d H(m)$となる。確認部６２３は、集約署名$\sigma = \sigma_c + \sigma_d$を算出する。そして、確認部６２３は、集約公開鍵Pと、算出した集約署名σとを用いて、$e(H(m),P) = e(\sigma,Q)$が成り立つか否かにより、配布者の署名σ_dを検証する。確認部６２３は、前記式が成り立つ場合、署名検証に成功したことと、検証に用いた配布者の署名σ_dとを出力する。確認部６２３は、認証要素セットE_dの署名検証に成功した場合は、他の認証要素セットE_uの署名検証を行

わず、認証要素セットE_dの署名検証に失敗した場合は、他の認証要素セットE_uについて、同様の処理を繰り返す。

[0135] 要求部６２４は、検証に成功した場合、配布者のユーザ署名σ_dを含むコンテンツ要求を送信する。具体的には、要求部６２４は、配布者からの指示に基づいて、任意のコンテンツをファイル管理システム３に要求する。要求には、コンテンツ識別子Cおよび配布者の署名σ_dが必要である。要求部６２４は、確認部６２３を用いて、コンテンツのアクセス権を確認し、配布者の署名σ_dを取得する。そして、要求部６２４はコンテンツ識別子Cおよび配布者の署名σ_dと含むコンテンツ要求をファイル管理システム３に送信する。

[0136] ファイル管理システム３は、コンテンツ識別子Cをキーとして、コンテンツを所有する許諾端末４にアクセスし、許諾端末４の共有制御部４２５に対してコンテンツ識別子Cおよび配布者の署名σ_dを含むコンテンツ要求を送信する。なお、要求部６２４は、この要求の際にコンテンツ識別子Cと、署名σ_dに加えて、この署名σ_dが、いづれの認証要素セットに対する署名かを示すインデックス情報を追加してもよい。

[0137] 同期部６２５は、コンテンツ要求に対して、許諾端末４からコンテンツの共有が許諾された場合に、ファイル管理システム３を介してコンテンツファイルを配布端末６に同期する。同期されたコンテンツファイルは記憶装置６１に格納される。

[0138] 共有制御部６２６は、配布者が自端末に登録したコンテンツを、他端末からの共有の要求を受けた際に、要求元にアクセス権があるか否かを判定し、アクセス権がある場合に、共有する。具体的には、共有制御部６２６は、コンテンツ要求に応じて、当該コンテンツに対応する閲覧端末５の認証要素セットE_u（P,m,σ_c）（すなわち、アクセス情報）をブロックチェーンから取得し、認証要素セットのコンテンツ署名σ_cと、コンテンツ要求に含まれるユーザ署名σ_uとを集約した集約署名σを認証要素セットの集約公開鍵Pで検証し、コンテンツ要求を許諾するか否かを判定する。

[0139] 例えばここで、閲覧端末５からファイル管理システム３を介し、コンテン

ツ識別子を指定してコンテンツの要求があるとする。閲覧端末５は、コンテンツ識別子に対応する、閲覧者の匿名用署名σ_uを添付してコンテンツを要求する。要求を受けた共有制御部６２６は、ブロックチェーンからアクセス情報を取得し、閲覧者にアクセス権があるか否かを判定する。

[0140] 判定はコンテンツ識別子に対応する全ての認証要素セット（P,m,σ_c）に対して次の署名検証を繰り返し、いずれかの認証要素セットで署名検証に成功した場合、閲覧者にアクセス権があると判定する。まず、共有制御部６２６は、コンテンツ識別子に対応する認証要素セット（P,m,σ_c）に対して、集約署名$\sigma=\sigma_c+\sigma_u$を計算する。次に，共有制御部４２５は、集約署名σを集約公開鍵Pで検証する。即ち、共有制御部６２６は、$e(H(m),P)=e(\sigma,Q)$が成り立つか否かにより、閲覧者の署名σ_uを検証する。共有制御部６２６は、前記式が成り立つ場合、コンテンツ識別子に対応するコンテンツを共有する。

[0141] （コンテンツ利用システムの動作）

次に、本実施形態のコンテンツ利用システムの動作について説明する。

[0142] 図９および図１０は、コンテンツ利用システムの動作を示すシーケンス図である。ここでは、第１の実施形態と異なる点を中心に記載し、第１の実施形態と同じ処理については簡略化して記載する。

[0143] 許諾端末４は、許諾者からの指示に基づいて、任意のコンテンツをファイル管理システム３に登録し、ファイル管理システム３から当該コンテンツに対するコンテンツ識別子Cを取得する（Ｓ４１）。

[0144] 許諾端末４は、アクセス情報を生成する（Ｓ４２）。許諾端末４は、配布者の匿名用ユーザ公開鍵P_dと閲覧者の匿名用ユーザ公開鍵P_uとを、事前に取得済みであるものとする。許諾端末４は、配布者の匿名用ユーザ公開鍵P_dを用いて、コンテンツ識別子Cのコンテンツに対応する配布者への認証要素セットE_d（P,m,σ_c）を生成する。また、許諾端末４は、閲覧者の匿名用ユーザ公開鍵P_uを用いて、コンテンツ識別子Cのコンテンツに対応する閲覧者への認証要素セットE_u（P,m,σ_c）を生成する。なお、認証要素セットの生成について

は、第１の実施形態と同様である。

[0145] そして、許諾端末４は、アクセス情報（コンテンツ識別子Cの認証要素セットE$_d$、E$_u$）を、ブロックチェーン上に登録する（Ｓ４３）。

[0146] 配布端末６は、配布者からの指示に基づいて、匿名用ユーザ鍵ペア（P$_d$，s$_d$）を生成する（Ｓ５１）。なお、許諾端末４と共有する公開パラメータQにより、P$_d$＝s$_d$Qが成り立つ。生成した秘密鍵s$_d$は、記憶装置６１に格納される。

[0147] そして、配布端末６は、コンテンツ識別子Cのコンテンツを要求するために、当該コンテンツに対して、ブロックチェーン上でアクセス権が設定されているか否かを確認する。具体的には、配布端末６は、コンテンツ識別子Cをクエリとして、自身の配布端末６のブロックチェーン６１１上のスマートコントラクトに問い合わせ（Ｓ５２）、コンテンツ識別子Cに対応する認証要素セットE$_d$、E$_u$を取得する（Ｓ５３）。

[0148] そして、配布端末６は、各認証要素セットE（ここでは、認証要素セットE$_d$、E$_u$）について、Ｓ５４～Ｓ５６の処理をそれぞれ行う。例えば認証要素セットE$_d$の場合、配布端末６は、メッセージmに対する閲覧者の署名σ$_d$＝ｓ$_d$Ｈ（m）を生成する（Ｓ５４）。また、閲覧端末５は、集約署名σ＝σ$_c$＋σ$_d$を算出し、集約公開鍵Pと、算出した集約署名σとを用いて、e(H(m),P) ＝e(σ,Q)が成り立つか否かにより、配布者の署名σ$_d$を検証する（Ｓ５５）。配布端末６は、前記式が成り立つ場合、署名検証に成功したことと、検証に用いた配布者の署名σ$_d$とを出力する（Ｓ５６）。

[0149] 配布端末６は、１つの認証要素セットEの署名検証に成功した場合は、残りの認証要素セットEの署名検証を行わない。すなわち、配布端末６は、署名検証に成功するまで、取得した各認証要素セットEの署名検証（Ｓ５４～Ｓ５６）を繰り返し行う。

[0150] そして、配布端末６は、配布者からの指示に基づいて、コンテンツ識別子Cと配布者の署名σ$_d$とを含むコンテンツ要求をファイル管理システム３に送信する（Ｓ５７）。ファイル管理システム３は、コンテンツ識別子Cをキーとし

て、コンテンツファイルを所有する許諾端末４にアクセスし、許諾端末４に対してコンテンツ識別子Cおよび配布者の署名σ_dを含むコンテンツ要求を送信する（Ｓ５８）。

[0151] 許諾端末４は、配布端末６からの要求に応じて、自端末４のコンテンツに対して、配布端末６にアクセス権があるか否かを判定する。具体的には、許諾端末４は、コンテンツ識別子Cに対応する全ての認証要素セットE（P,m,σ_c）をブロックチェーン４１１から取得する（Ｓ５９）。

[0152] 許諾端末４は、取得した各認証要素セットEを用いて配布者の署名σ_dを検証する（Ｓ６０）。例えば認証要素セットE_d（P,m,σ_c）の場合、許諾端末４は、集約署名$\sigma=\sigma_c+\sigma_d$を算出し、集約署名σを集約公開鍵Pで検証する。すなわち、許諾端末４は、$e(H(m),P)=e(\sigma,Q)$が成り立つか否かを判定し、成り立つ場合、コンテンツ識別子Cのコンテンツに対して配布端末６にアクセス権があると判定し、コンテンツを配布端末６と共有する。許諾端末４は、署名検証に成功するまで、取得した各認証要素セットEの署名検証を行う。

[0153] 許諾端末４は、アクセス権がある場合、Ｓ５８のコンテンツ要求に対して許諾する旨の応答と、コンテンツ識別子Cのコンテンツファイルとを、ファイル管理システム３に送信する（Ｓ６１）。ファイル管理システム３は、受信したコンテンツファイルを要求元の配布端末６に送信する（Ｓ６２）。配布端末６は、コンテンツファイルを受信し、記憶装置６１に格納する。

[0154] 閲覧端末５は、閲覧者からの指示に基づいて、匿名用ユーザ鍵ペア（P_u，s_u）を生成する（Ｓ７１）。許諾端末４と共有する公開パラメータQにより、$P_u=s_uQ$が成り立つ。そして、閲覧端末５は、コンテンツ識別子Cで識別されるコンテンツに対して、ブロックチェーン上でアクセス権が設定されているか否かを確認する。具体的には、閲覧端末５は、コンテンツ識別子Cをクエリとして、自身の閲覧端末５のブロックチェーン５１１上のスマートコントラクトに問い合わせ、コンテンツ識別子Cに対応する全ての認証要素セットE（P,m,σ_c）を取得する（Ｓ７２）。

[0155] そして、閲覧端末５は、取得した各認証要素セットEを用いて閲覧者の署名

σ_uを検証する（Ｓ７３）。例えば認証要素セットE_u（P,m,σ_c）の場合、閲覧端末５は、メッセージmに対する閲覧者の署名$\sigma_u = s_u H$（m）を生成すし、集約署名$\sigma = \sigma_c + \sigma_u$を算出する。そして、閲覧端末５は、集約公開鍵Pと、集約署名σとを用いて、e(H(m),P) ＝e(σ,Q)が成り立つか否かにより、閲覧者の署名σ_uを検証する。閲覧端末５は、前記式が成り立つ場合、署名検証に成功したことと、検証に用いた閲覧者の署名σ_uとを出力する。閲覧端末５は、署名検証に成功するまで、取得した各認証要素セットEの署名検証を行う。

[0156] そして、閲覧端末５は、閲覧者からの指示に基づいて、コンテンツ識別子Cと閲覧者の署名σ_uとを含むコンテンツ要求をファイル管理システム３に送信する（Ｓ７４）。ファイル管理システム３は、コンテンツ識別子Cをキーとして、コンテンツファイルを所有する配布端末６にコンテンツ識別子Cおよび閲覧者の署名σ_uを含むコンテンツ要求を送信する（Ｓ７５）。

[0157] 配布端末６は、閲覧端末５からの要求に応じて、自端末６で保持するコンテンツのアクセス権が閲覧端末５にあるか否かを判定する。具体的には、配布端末６は、自端末６のブロックチェーン６１１にアクセスし、コンテンツ識別子Cに対応する全ての認証要素セットE_d、E_uを、ブロックチェーン６１１から取得する（Ｓ７６）。

[0158] 配布端末６は、取得した全ての認証要素セットE_d、E_uを用いて、閲覧者の署名σ_uを検証する（Ｓ７７）。署名σ_uを検証はＳ６０と同様である。配布端末６は、取得した認証要素セットE_d、E_uのいずれかを用いた署名σ_uの検証に成功した場合、コンテンツに対して閲覧端末５にアクセス権があると判定し、コンテンツを閲覧端末５と共有する。

[0159] 配布端末６は、アクセス権がある場合、Ｓ７５のコンテンツ要求に対して許諾する旨の応答と、コンテンツ識別子Cのコンテンツファイルとを、ファイル管理システム３に送信する（Ｓ７８）。ファイル管理システム３は、コンテンツファイルを要求元の閲覧端末５に送信する（Ｓ７９）。閲覧端末５は、コンテンツファイルを受信し、記憶装置５１に格納する。

[0160] 以上説明した本実施形態の配布端末６は、匿名用コンテンツ鍵P_cを保管する必要はなく、コンテンツを要求された際に、要求元の閲覧端末５が送付したユーザ署名σ_uと、ブロックチェーンで公開されている認証要素セット（P, m, σ_c）とを用いて要求元にアクセス権限があるかを判定することができる。

[0161] また、本実施形態の配布端末６は、閲覧端末５に匿名用ユーザ公開鍵P_uを要求しない。配布端末６が知り得る情報は、認証要素セット（P,m, σ_c）およびユーザ署名σ_uのみであり、配布端末６は、これらのデータからは閲覧者の匿名用ユーザ公開鍵P_uを取得することはできない。よって、本実施形態では、コンテンツを中継して配布する配布端末６にも、匿名用ユーザ公開鍵P_uを知られることなく、閲覧端末５はコンテンツを取得することができる。

[0162] なお、上記説明した許諾端末４、閲覧端末５および配布端末６には、例えば、図１１に示すような汎用的なコンピュータシステムを用いることができる。図示するコンピュータシステムは、CPU（Central Processing Unit、プロセッサ）９０１と、メモリ９０２と、ストレージ９０３（HDD：Hard Disk Drive、SSD：Solid State Drive）と、通信装置９０４と、入力装置９０５と、出力装置９０６とを備える。メモリ９０２およびストレージ９０３は、記憶装置である。このコンピュータシステムにおいて、CPU９０１がメモリ９０２上にロードされた所定のプログラムを実行することにより、各装置の各機能が実現される。

[0163] なお、許諾端末４、閲覧端末５および配布端末６は、１つのコンピュータで実装されてもよく、あるいは複数のコンピュータで実装されても良い。また、許諾端末４、閲覧端末５および配布端末６は、コンピュータに実装される仮想マシンであっても良い。

[0164] 許諾端末４用のプログラム、閲覧端末５用のプログラム、および、配布端末６用のプログラムは、HDD、SSD、USB（Universal Serial Bus）メモリ、CD（Compact Disc）、DVD（Digital Versatile Disc)などのコンピュータ読取り可能な記録媒体に記憶することも、ネットワークを介して配信することもできる。

[0165] また、本発明は上記実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。例えば、以下のような変形例がある。

[0166] （変形例１）

BLS署名を使った鍵集約においては、Rouge-key攻撃などの不正な鍵交換の攻撃を防ぐために、署名値や鍵に特定の数を掛けてから集約する対策が行われることがある。本実施形態においても同様の対策を行うことで、より強度の高く匿名性を保つことが可能になる。

[0167] この変形例においては、許諾者と閲覧者の間で決定論的に定められた二つの秘密の値t_c, t_uを用意する。例えば、加法巡回群G_1からそれぞれ一意の数値を出力するハッシュ関数H_0を匿名用コンテンツ公開鍵P_cと匿名用ユーザ公開鍵P_uに適用し、t_c, t_uとしてもよい。ここで、集約公開鍵を下記のように定義する。

[0168] [数14]

$$P' \leftarrow t_c P_c + t_u P_u$$

[0169] その場合、対応する集約署名は、以下のとおりである。

[0170] [数15]

$$\sigma' \leftarrow t_c \sigma_c + t_u \sigma_u$$

[0171] 署名検証では、e(H(m),P'）＝e(σ',Q)が成り立つか否かを検証し、成り立つ場合に正当な署名であることが確認される。この場合、上記実施形態で記載していたコンテンツ署名σ_cは、そのt_c倍してコンテンツ署名$t_c\sigma_c$と置き換えられ、アクセス情報に含まれる認証要素セットは（P',m,$t_c\sigma_c$）となる。また閲覧端末５がコンテンツ要求時に添付する閲覧者の情報はt_u倍して、$t_u\sigma_u$となる。

[0172] （変形例２）

上記実施形態では、閲覧端末５は、コンテンツを要求する際に閲覧者の匿名用ユーザ署名σ_uを添付しているが、閲覧端末５側で集約署名$\sigma = \sigma_c + \sigma_u$を算出し、集約署名σを添付しても良い。すなわち、閲覧端末５の確認部５

２３は、匿名用ユーザ署名σ_uの代わりに、集約署名σを含むコンテンツ要求を送信してもよい。この場合、許諾端末４の共有制御部４２５は、コンテンツ要求に含まれる集約署名σを認証要素セット（アクセス情報）の集約公開鍵で検証し、コンテンツ要求を許諾するか否かを判定する。

[0173] 具体的には、図６のＳ２６においては、「集約署名の検証が成功したら、閲覧者のユーザ署名σ_uを出力」とあるが、この「ユーザ署名σ_u」を既に集約された「集約署名$\sigma=\sigma_c+\sigma_u$」と置き換えても良い。この場合、Ｓ２７およびＳ２８で送信されるコンテンツ要求には、ユーザ署名σ_uの代わりに集約署名σが含まれる。許諾端末４は、コンテンツ要求に含まれる集約署名σを集約公開鍵Pで検証する。したがって、許諾端末４は、Ｓ３１の署名集約を計算する必要はなく、演算負荷を低減することができる。

[0174] 第２の実施形態においても同様である。すなわち、第２の実施形態の閲覧端末５および配布端末６は、匿名用ユーザ署名σ_u、σ_dの代わりに、集約署名σを含むコンテンツ要求を送信してもよい（図９、図１０：Ｓ５６－Ｓ５８、Ｓ７３－Ｓ７５）。この場合、第２の実施形態の許諾端末４および配布端末６は、コンテンツ要求に含まれる集約署名σを認証要素セットの集約公開鍵で検証し、コンテンツ要求を許諾するか否かを判定する（図１０：Ｓ６０、Ｓ７７）。

符号の説明

[0175] １、１Ａ：コンテンツ利用システム

２　：ブロックチェーンシステム

３　：ファイル管理システム

４　：許諾端末

４２１：ブロックチェーン制御部

４２２：ファイル管理部

４２３：生成部

４２４：登録部

４２５：共有制御部

５　：閲覧端末

５２１：ブロックチェーン制御部

５２２：鍵管理部

５２３：確認部

５２４：要求部

５２５：同期部

６　：配布端末

６２１：ブロックチェーン制御部

６２２：鍵管理部

６２３：確認部

６２４：要求部

６２５：同期部

６２６：共有制御部

４１１、５１１、６１１：ブロックチェーン

４１２、５１２、６１２：コンテンツデータ

４１３、５１３、６１３：鍵管理データ

４１４、５１４、６１４：プログラム

請求の範囲

[請求項1] 許諾端末と閲覧端末とを備えるコンテンツ利用システムであって、

前記許諾端末は、

コンテンツのコンテンツ公開鍵と、前記コンテンツの閲覧者のユーザ公開鍵とを用いて、前記コンテンツに対するアクセス情報を生成する生成部と、

前記アクセス情報をブロックチェーンに登録する登録部と、を備え、

前記アクセス情報は、前記コンテンツ公開鍵と前記ユーザ公開鍵とを集約した集約公開鍵と、前記コンテンツ用のメッセージと、前記メッセージを前記コンテンツ公開鍵に対応するコンテンツ秘密鍵で署名したコンテンツ署名とを含み、

前記閲覧端末は、

要求するコンテンツのアクセス情報を前記ブロックチェーンから取得し、前記アクセス情報のメッセージをユーザ秘密鍵で署名したユーザ署名と、前記アクセス情報のコンテンツ署名とを集約した集約署名を、前記アクセス情報の集約公開鍵で検証する確認部と、

検証に成功した場合、前記ユーザ署名または前記集約署名を含むコンテンツ要求を送信する要求部と、を備えるコンテンツ利用システム。

[請求項2] コンテンツのコンテンツ公開鍵と、前記コンテンツの閲覧者のユーザ公開鍵とを用いて、前記コンテンツに対するアクセス情報を生成する生成部と、

前記アクセス情報をブロックチェーンに登録する登録部と、を備え、

前記アクセス情報は、前記コンテンツ公開鍵と前記ユーザ公開鍵とを集約した集約公開鍵と、前記コンテンツ用のメッセージと、前記メッセージを前記コンテンツ公開鍵に対応するコンテンツ秘密鍵で署名

したコンテンツ署名とを含む許諾端末。

[請求項3] コンテンツ要求に応じて、当該コンテンツに対応するアクセス情報を前記ブロックチェーンから取得し、前記アクセス情報のコンテンツ署名と、前記コンテンツ要求に含まれるユーザ署名とを集約した集約署名を前記アクセス情報の集約公開鍵で検証し、前記コンテンツ要求を許諾するか否かを判定する共有制御部を備える

請求項２に記載の許諾端末。

[請求項4] コンテンツ要求に応じて、当該コンテンツに対応するアクセス情報を前記ブロックチェーンから取得し、前記コンテンツ要求に含まれる集約署名を前記アクセス情報の集約公開鍵で検証し、前記コンテンツ要求を許諾するか否かを判定する共有制御部を備える

請求項２に記載の許諾端末。

[請求項5] 要求するコンテンツのアクセス情報をブロックチェーンから取得し、前記アクセス情報のメッセージをユーザ秘密鍵で署名したユーザ署名と、前記アクセス情報のコンテンツ署名とを集約した集約署名を、前記アクセス情報の集約公開鍵で検証する確認部と、

検証に成功した場合、前記ユーザ署名または前記集約署名を含むコンテンツ要求を送信する要求部と、

を備える閲覧端末。

[請求項6] 要求するコンテンツのアクセス情報をブロックチェーンから取得し、前記アクセス情報のメッセージをユーザ秘密鍵で署名したユーザ署名と、前記アクセス情報のコンテンツ署名とを集約した集約署名を、前記アクセス情報の集約公開鍵で検証する確認部と、

検証に成功した場合、前記ユーザ署名を含むコンテンツ要求を、許諾端末に送信する要求部と、

コンテンツ要求に応じて、当該コンテンツに対応するアクセス情報を前記ブロックチェーンから取得し、前記アクセス情報のコンテンツ署名と、前記コンテンツ要求に含まれるユーザ署名とを集約した集約

署名を前記アクセス情報の集約公開鍵で検証し、前記コンテンツ要求を許諾するか否かを判定する共有制御部と、

を備える配信端末。

[請求項7] 要求するコンテンツのアクセス情報をブロックチェーンから取得し、前記アクセス情報のメッセージをユーザ秘密鍵で署名したユーザ署名と、前記アクセス情報のコンテンツ署名とを集約した集約署名を、前記アクセス情報の集約公開鍵で検証する確認部と、

検証に成功した場合、前記集約署名を含むコンテンツ要求を、許諾端末に送信する要求部と、

コンテンツ要求に応じて、当該コンテンツに対応するアクセス情報を前記ブロックチェーンから取得し、前記コンテンツ要求に含まれる前記集約署名を前記アクセス情報の集約公開鍵で検証し、前記コンテンツ要求を許諾するか否かを判定する共有制御部と、

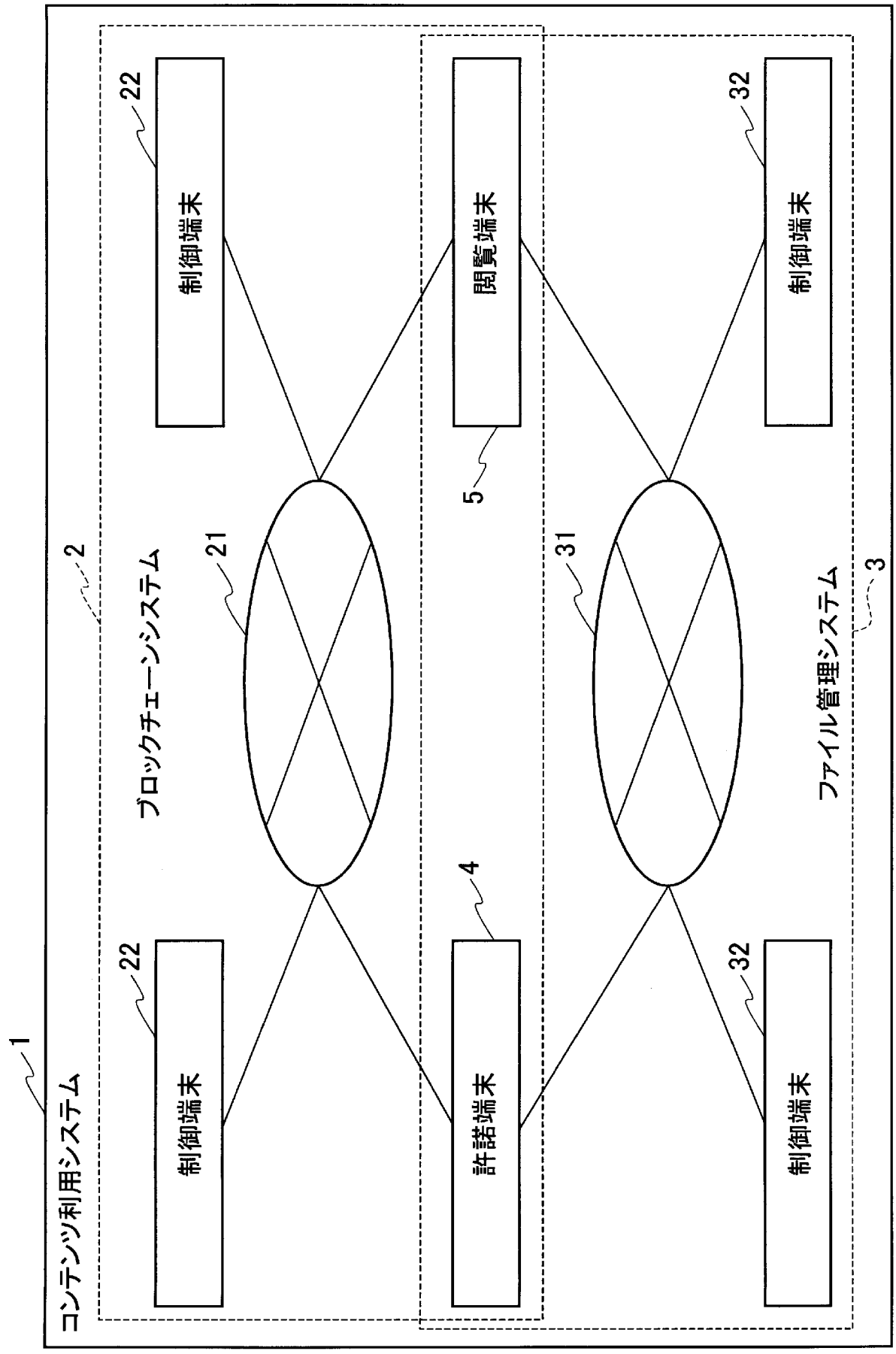
を備える配信端末。

[請求項8] 請求項２から４のいずれか１項に記載の許諾端末として、コンピュータを機能させることを特徴とするコンテンツ利用プログラム。

[請求項9] 請求項５に記載の閲覧端末として、コンピュータを機能させることを特徴とするコンテンツ利用プログラム。

[請求項10] 請求項６または７に記載の配信端末として、コンピュータを機能させることを特徴とするコンテンツ利用プログラム。

[図1]


1
コンテンツ利用システム
2
ブロックチェーンシステム
3
ファイル管理システム
21
22
制御端末
22
制御端末
4
許諾端末
5
閲覧端末
31
32
制御端末
32
制御端末

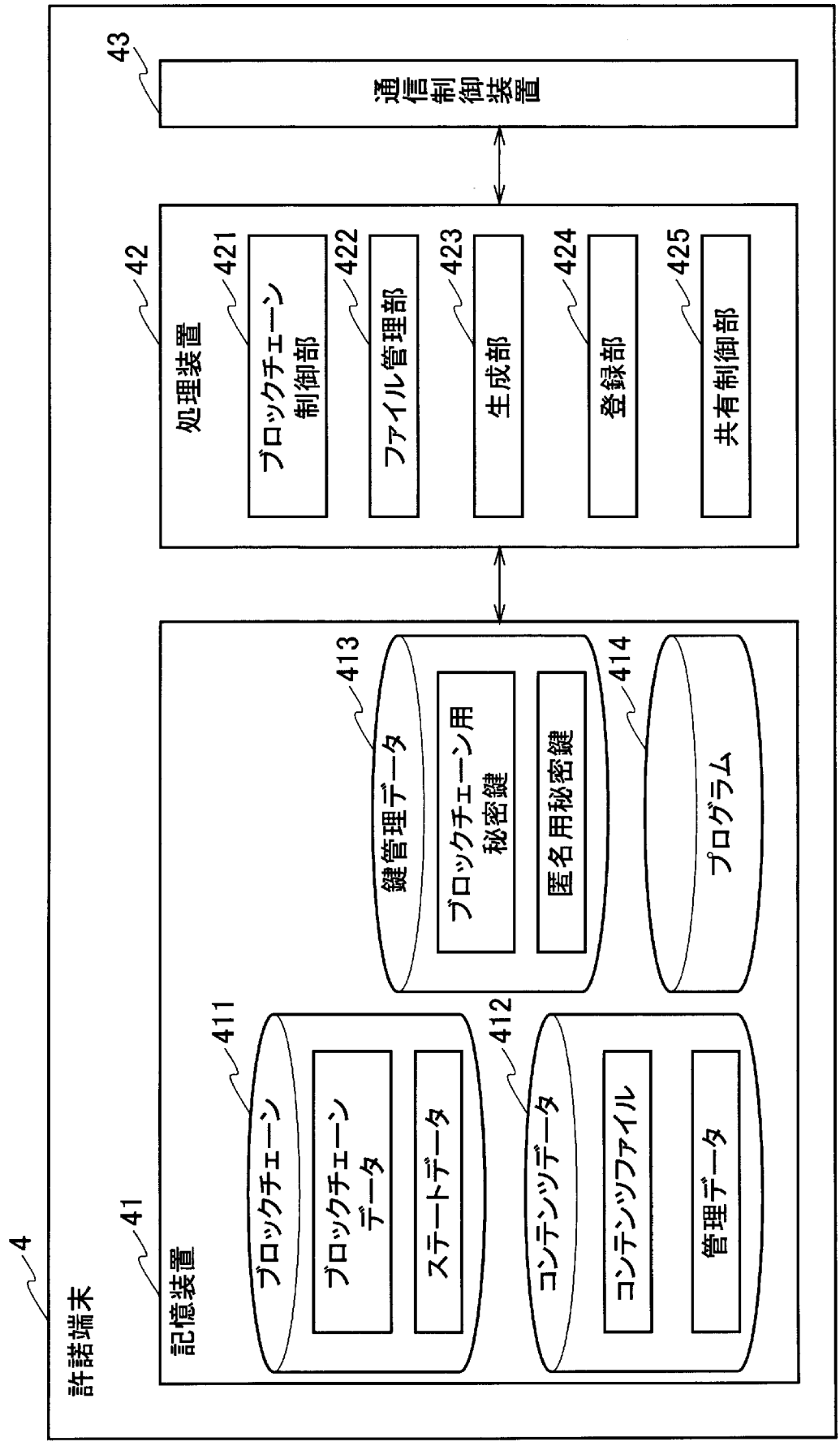
[図2A]

	コンテンツ識別子	集約公開鍵	メッセージ	匿名コンテンツ鍵による署名
コンテンツ1	C^1	P^1	m^1	$\sigma_c{}^1$
コンテンツ2	C^2	P^2	m^2	$\sigma_c{}^2$
コンテンツ3	C^3	P^3	m^3	$\sigma_c{}^3$
⋮	⋮	⋮	⋮	⋮

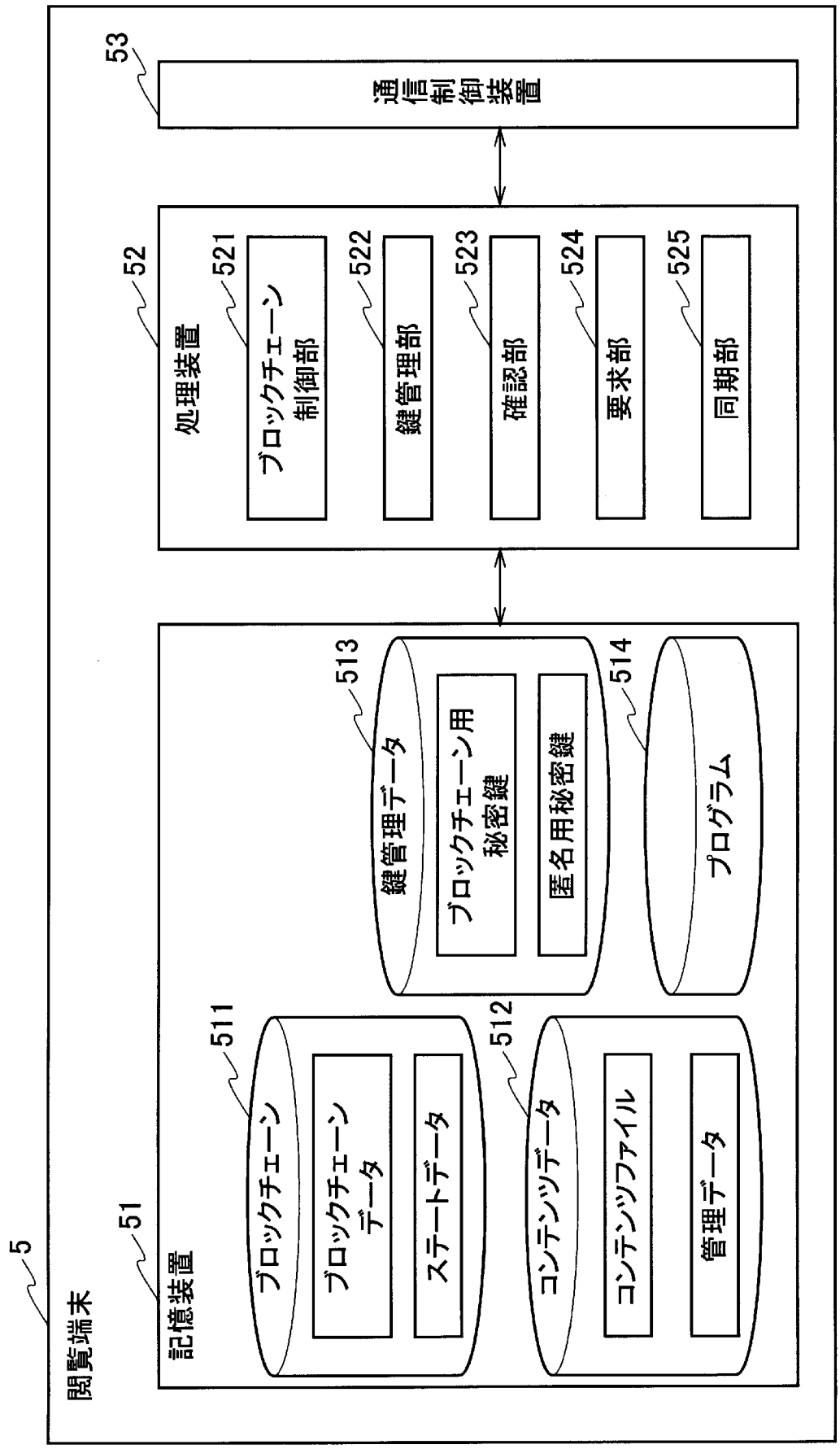
[図2B]

	コンテンツ識別子	集約公開鍵	メッセージ	匿名コンテンツ鍵による署名
コンテンツ1	C^1	$P^{1,1}$	$m^{1,1}$	$\sigma_c{}^{1,1}$
		$P^{1,2}$	$m^{1,2}$	$\sigma_c{}^{1,2}$
コンテンツ2	C^2	$P^{2,1}$	$m^{2,1}$	$\sigma_c{}^{2,1}$
⋮	⋮	⋮	⋮	⋮

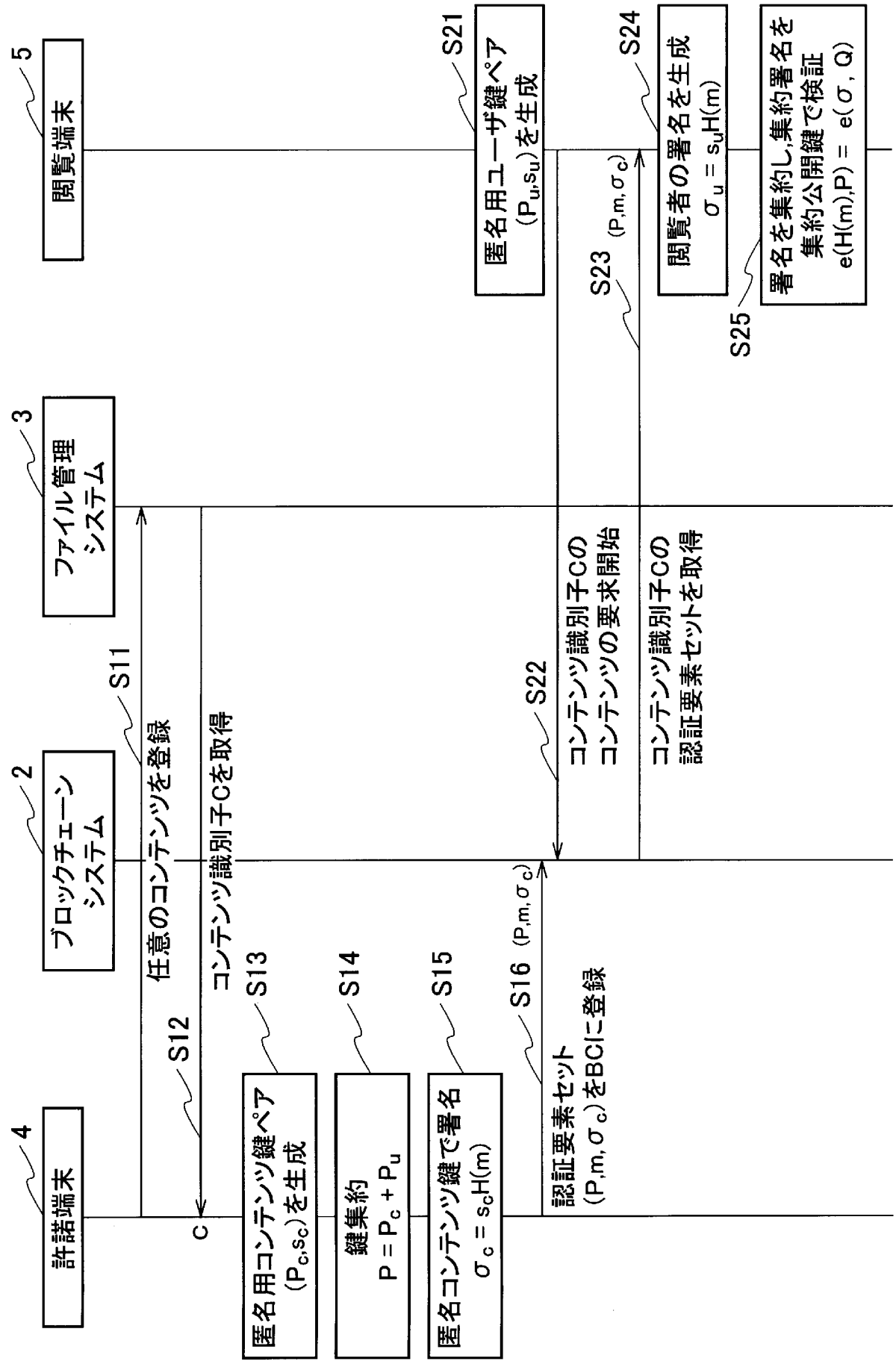
[図3]


4
許諾端末
41
記憶装置
411
ブロックチェーン
ブロックチェーンデータ
ステートデータ
412
コンテンツデータ
コンテンツファイル
管理データ
413
鍵管理データ
ブロックチェーン用秘密鍵
匿名用秘密鍵
414
プログラム
42
処理装置
421
ブロックチェーン制御部
422
ファイル管理部
423
生成部
424
登録部
425
共有制御部
43
通信制御装置

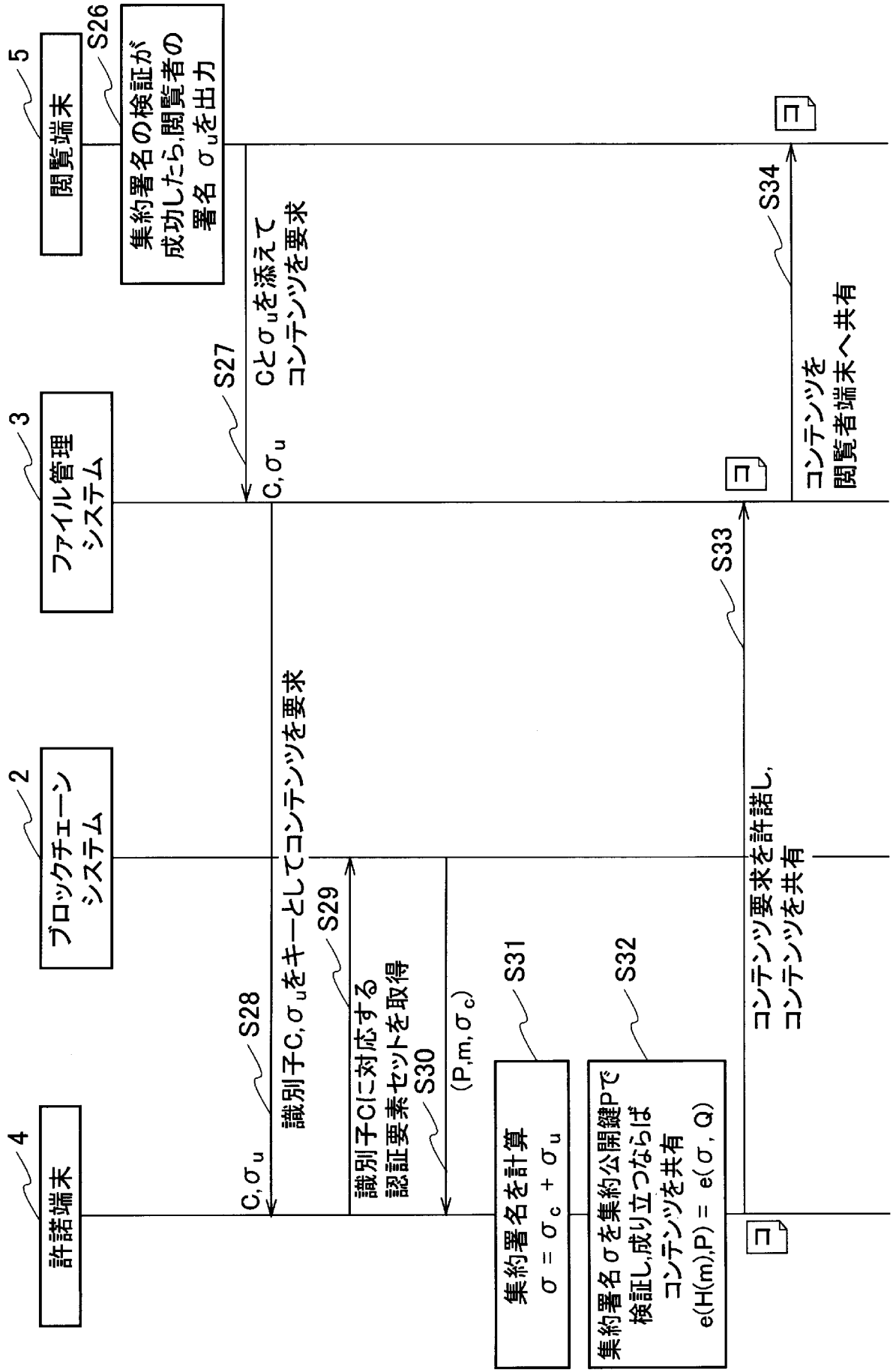
[図4]


5
閲覧端末
51
記憶装置
511
ブロックチェーン
ブロックチェーンデータ
ステートデータ
512
コンテンツデータ
コンテンツファイル
管理データ
513
鍵管理データ
ブロックチェーン用秘密鍵
匿名用秘密鍵
514
プログラム
52
処理装置
521
ブロックチェーン制御部
522
鍵管理部
523
確認部
524
要求部
525
同期部
53
通信制御装置

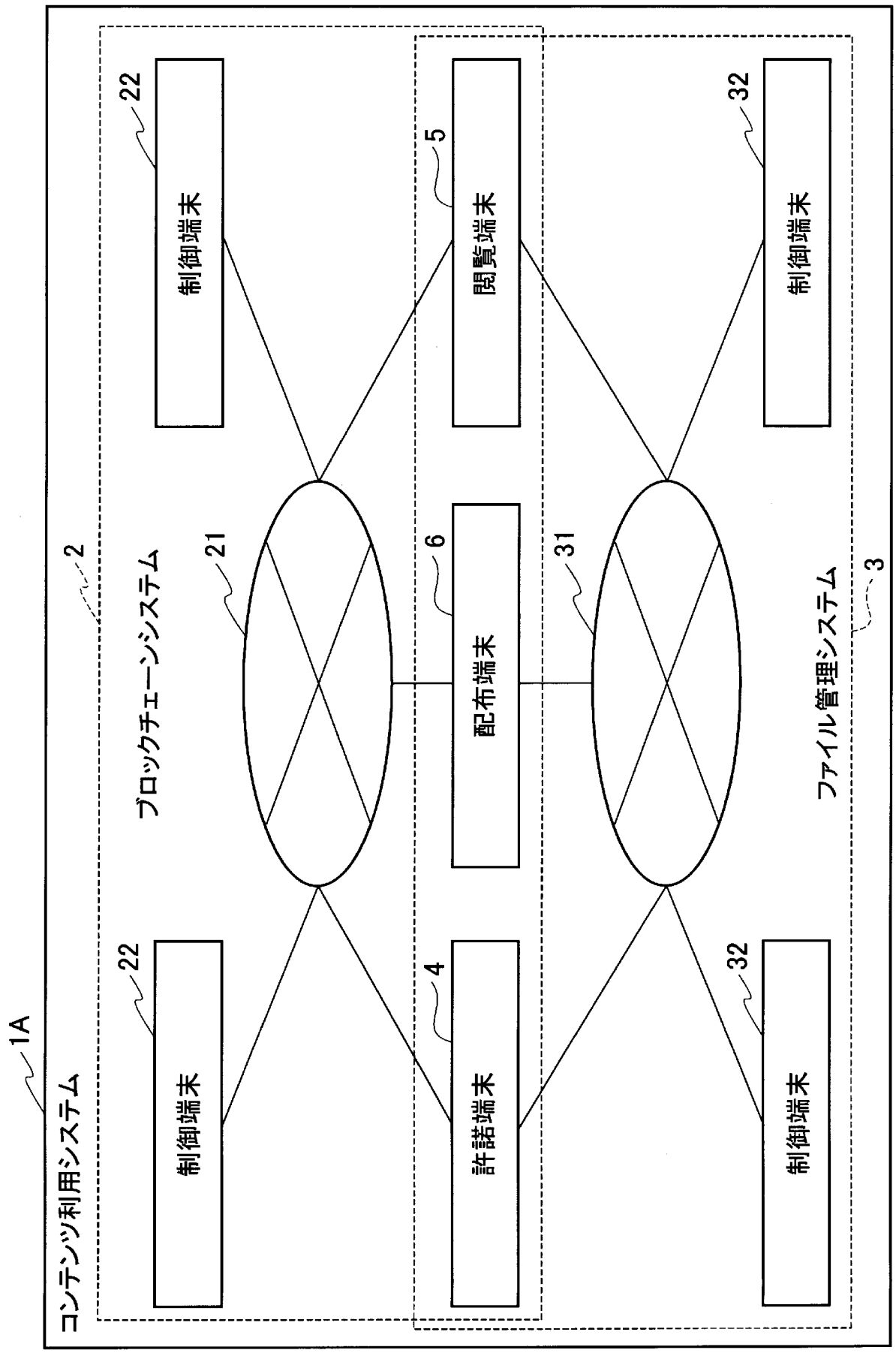
[図5]


5
閲覧端末
S21
匿名用ユーザ鍵ペア
(Pu,su)を生成
S24
閲覧者の署名を生成
σu = suH(m)
S25
署名を集約し,集約署名を
集約公開鍵で検証
e(H(m),P) = e(σ, Q)
3
ファイル管理
システム
S11
任意のコンテンツを登録
S23 (P,m,σc)
コンテンツ識別子Cの
コンテンツの要求開始
コンテンツ識別子Cの
認証要素セットを取得
2
ブロックチェーン
システム
S22
コンテンツ識別子Cを取得
S12
S13
S14
S15
S16 (P,m,σc)
4
許諾端末
c
匿名用コンテンツ鍵ペア
(Pc,sc)を生成
鍵集約
P = Pc + Pu
匿名コンテンツ鍵で署名
σc = scH(m)
認証要素セット
(P,m,σc)をBCに登録

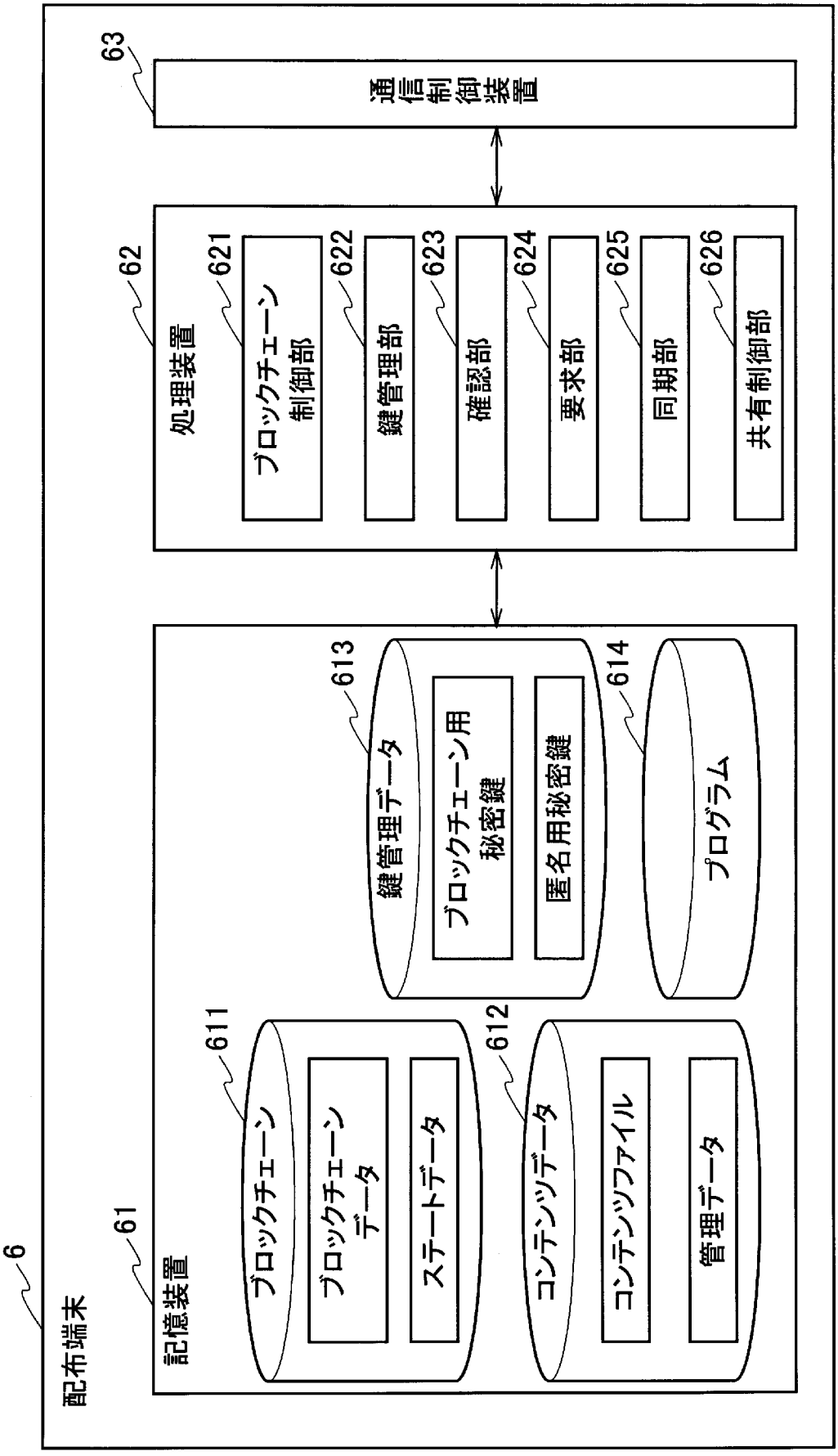
[図6]


5
閲覧端末
S26
集約署名の検証が
成功したら,閲覧者の
署名 σuを出力
3
ファイル管理
システム
S27
C,σu
Cとσuを添えて
コンテンツを要求
ヨ
S34
コンテンツを
閲覧者端末へ共有
ヨ
S33
2
ブロックチェーン
システム
識別子C,σuをキーとしてコンテンツを要求
S28
S29
識別子Cに対応する
認証要素セットを取得
S30
(P,m,σc)
S31
集約署名を計算
σ = σc + σu
S32
集約署名σを集約公開鍵Pで
検証し,成り立つならば
コンテンツを共有
e(H(m),P) = e(σ, Q)
コンテンツ要求を許諾し,
コンテンツを共有
4
許諾端末
C,σu
ヨ

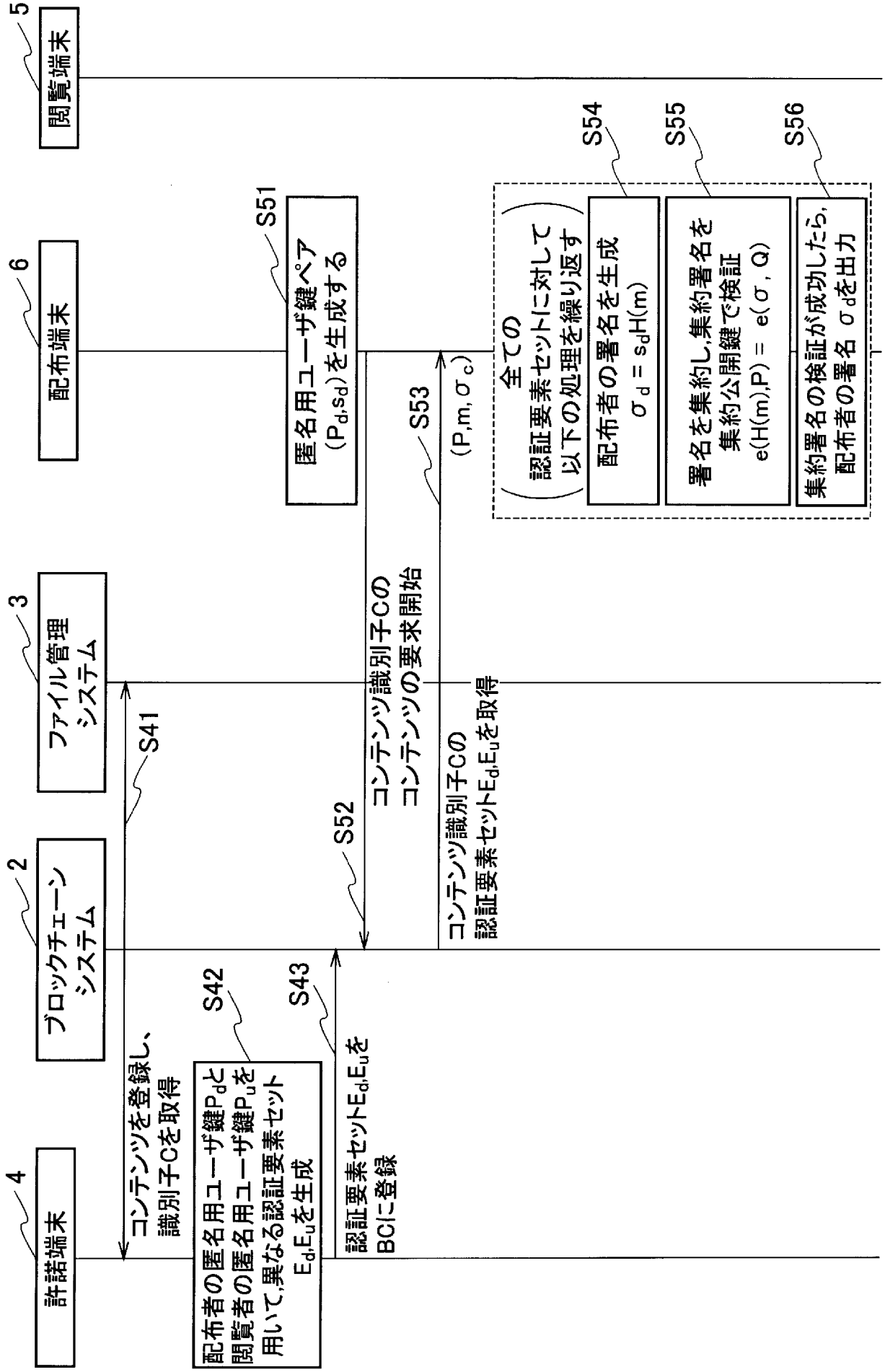
[図7]


1A
コンテンツ利用システム
2
ブロックチェーンシステム
3
ファイル管理システム
21
31
22
制御端末
22
制御端末
4
許諾端末
5
閲覧端末
6
配布端末
32
制御端末
32
制御端末

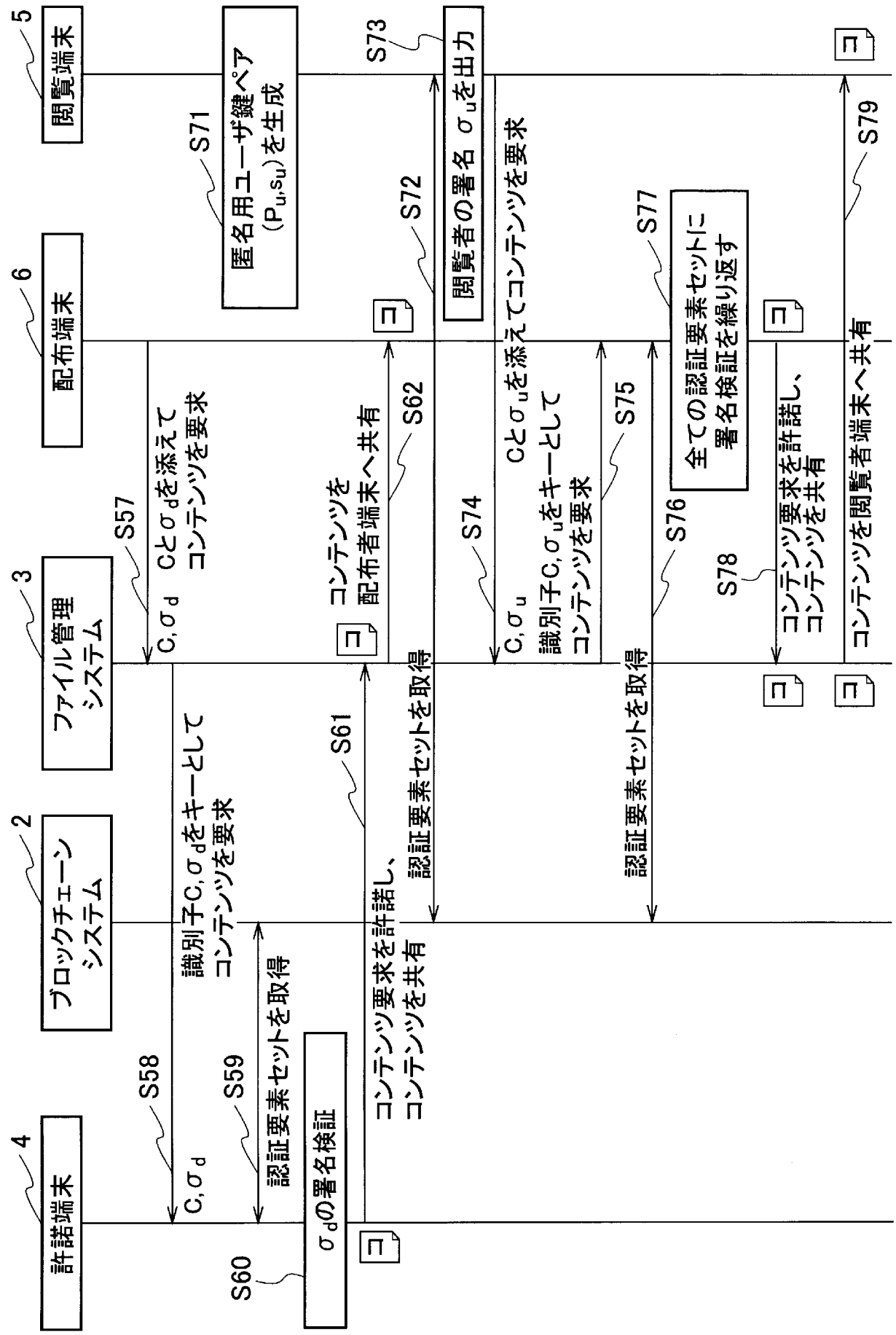
[図8]


6
配布端末
61
記憶装置
611
ブロックチェーン
ブロックチェーンデータ
ステートデータ
612
コンテンツデータ
コンテンツファイル
管理データ
613
鍵管理データ
ブロックチェーン用秘密鍵
匿名用秘密鍵
614
プログラム
62
処理装置
621
ブロックチェーン制御部
622
鍵管理部
623
確認部
624
要求部
625
同期部
626
共有制御部
63
通信制御装置

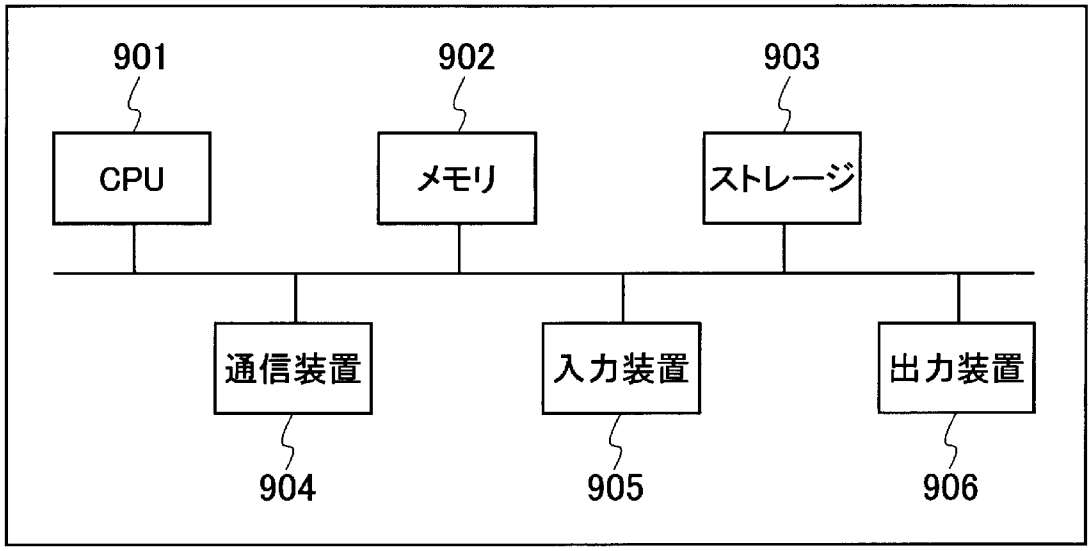
[図9]


5
閲覧端末
6
配布端末
3
ファイル管理システム
2
ブロックチェーンシステム
4
許諾端末
S51
匿名用ユーザ鍵ペア
(P_d,s_d)を生成する
S41
コンテンツを登録し、
識別子Cを取得
S42
配布者の匿名用ユーザ鍵P_dと
閲覧者の匿名用ユーザ鍵P_uを
用いて,異なる認証要素セット
E_d,E_uを生成
S43
認証要素セットE_d,E_uを
BCに登録
S52
コンテンツ識別子Cの
コンテンツの要求開始
S53
(P,m,σ_c)
コンテンツ識別子Cの
認証要素セットE_d,E_uを取得
全ての
認証要素セットに対して
以下の処理を繰り返す
S54
配布者の署名を生成
$\sigma_d = s_d H(m)$
S55
署名を集約し,集約署名を
集約公開鍵で検証
$e(H(m),P) = e(\sigma, Q)$
S56
集約署名の検証が成功したら,
配布者の署名 σ_dを出力

[図10]


5
閲覧端末
6
配布端末
3
ファイル管理システム
2
ブロックチェーンシステム
4
許諾端末
S71
匿名用ユーザ鍵ペア
(P_u,s_u)を生成
S73
閲覧者の署名 σ_uを出力
S72
S57
C,σ_d Cとσ_dを添えて
コンテンツを要求
S62
コンテンツを
配布者端末へ共有
S74
C,σ_u Cとσ_uを添えてコンテンツを要求
S75
識別子C,σ_uをキーとして
コンテンツを要求
S77
全ての認証要素セットに
署名検証を繰り返す
S76
認証要素セットを取得
S78
コンテンツ要求を許諾し、
コンテンツを共有
S79
コンテンツを閲覧者端末へ共有
S61
コンテンツ要求を許諾し、
コンテンツを共有
認証要素セットを取得
S58
C,σ_d
識別子C,σ_dをキーとして
コンテンツを要求
S59
認証要素セットを取得
S60
σ_dの署名検証

[図11]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/023904

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. H04L9/32(2006.01)i, G06F21/10(2013.01)i, G06F21/64(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int. Cl. H04L9/32, G06F21/10, G06F21/64

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2019
Registered utility model specifications of Japan 1996-2019
Published registered utility model applications of Japan 1994-2019

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore, block chain, access controll

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2019-500799 A (SONY CORP.) 10 January 2019, paragraphs [0030]-[0072]	1-10
A	JP 2005-522968 A (DOCOMO COMMUNICATIONS LABORATORIES USA, INC.) 28 July 2005, paragraphs [0034]-[0045]	1-10
A	US 2019/0050854 A1 (INTEL CORPORATION) 14 February 2019, paragraphs [0028]-[0074]	1-10
A	US 2018/0343126 A1 (NXM LABS INC.) 29 November 2018, paragraphs [0033]-[0049], [0059]	1-10
A	US 2018/0294957 A1 (WALMART APOLLO, LLC) 11 October 2018, paragraphs [0017]-[0034]	1-10

☒ Further documents are listed in the continuation of Box C.
☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28.08.2019	10.09.2019
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/023904

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WANG, S., ZHANG, Y. and ZHANG, Y., A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems, IEEE Access, [online], 30 July 2018, vol. 6, pp. 38437-38450, [retrieved on 27 August 2019], retrieved from the Internet: <URL: https://ieeexplore.ieee.org/document/8400511> <DOI:10.1109/ACCESS.2018.2851611 especially III. PRELIMINARIES, IV. SYSTEM MODEL, V. CASE STUDY A. CONCRETE CONSTRUCTION	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2019/023904

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
JP 2019-500799 A	2019.01.10	US 2019/0020661 A1, paragraphs [0046]-[0080] WO 2017/107976 A1 EP 3396576 A1 CN 106911641 A CA 3009567 A AU 2016377729 A KR 10-2018-0095896 A	2019.01.17 2017.06.29 2018.10.31 2017.06.30 2017.06.29 2018.07.26 2018.08.28
JP 2005-522968 A	2005.07.28	US 2005/0022102 A1, paragraphs [0036]-[0049] WO 2003/090429 A1 EP 1497948 A1 CN 1633776 A AU 2003226413 A	2005.01.27 2003.10.30 2005.01.19 2005.06.29 2003.11.03
US 2019/0050854 A1	2019.02.14	Family: none	
US 2018/0343126 A1	2018.11.29	Family: none	
US 2018/0294957 A1	2018.10.11	WO 2018/187408 A1	2018.10.11

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０２３９０４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32(2006.01)i, G06F21/10(2013.01)i, G06F21/64(2013.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32, G06F21/10, G06F21/64

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　　１９２２－１９９６年
日本国公開実用新案公報　　１９７１－２０１９年
日本国実用新案登録公報　　１９９６－２０１９年
日本国登録実用新案公報　　１９９４－２０１９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore
block chain, access controll

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2019-500799 A (ソニー株式会社) 2019.01.10, 段落[0030]-[0072]	1-10
A	JP 2005-522968 A (ドコモ　コミュニケーションズ　ラボラトリーズ　ユー・エス・エー　インコーポレーティッド) 2005.07.28, 段落[0034]-[0045]	1-10
A	US 2019/0050854 A1 (INTEL CORPORATION) 2019.02.14, 段落[0028]-[0074]	1-10

☑　Ｃ欄の続きにも文献が列挙されている。

☑　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２８．０８．２０１９	１０．０９．２０１９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　９３６４
中里　裕正
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	US 2018/0343126 A1 (NXM LABS INC.) 2018.11.29, 段落[0033]-[0049],[0059]	1-10
A	US 2018/0294957 A1 (WALMART APOLLO, LLC) 2018.10.11, 段落[0017]-[0034]	1-10
A	WANG, S., ZHANG, Y. and ZHANG, Y., A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems, IEEE Access, [online], 2018.07.30, Vol.6, p.38437-38450, [retrieved on 2019.08.27], retrieved from the Internet: <URL:https://ieeexplore.ieee.org/document/8400511> <DOI:10.1109/ACCESS.2018.2851611> especially III. PRELIMINARIES, IV. SYSTEM MODEL, V. CASE STUDY A. CONCRETE CONSTRUCTION	1-10

JP 2019-500799 A	2019.01.10	US 2019/0020661 A1, 段落[0046]-[0080]	2019.01.17
		WO 2017/107976 A1	2017.06.29
		EP 3396576 A1	2018.10.31
		CN 106911641 A	2017.06.30
		CA 3009567 A	2017.06.29
		AU 2016377729 A	2018.07.26
		KR 10-2018-0095896 A	2018.08.28
JP 2005-522968 A	2005.07.28	US 2005/0022102 A1, 段落[0036]-[0049]	2005.01.27
		WO 2003/090429 A1	2003.10.30
		EP 1497948 A1	2005.01.19
		CN 1633776 A	2005.06.29
		AU 2003226413 A	2003.11.03
US 2019/0050854 A1	2019.02.14	ファミリーなし	
US 2018/0343126 A1	2018.11.29	ファミリーなし	
US 2018/0294957 A1	2018.10.11	WO 2018/187408 A1	2018.10.11