【書類名】明細書
【発明の名称】デジタルはがき、デジタル郵便システム、情報処理システム
【技術分野】
【０００１】
本願は、分散型台帳システム用いたデジタルはがきの提供に関するコンピュータ・コンピュータシステム・コンピュータネットワークシステム・情報処理システム・プログラム等に関する。また分散型ＳＮＳシステムに関連する。
【背景技術】
【０００２】
例えば紙の郵便物は火災により消失したり、雨などで濡れて破損するなどして差出人から宛名のユーザにメールが届かないこともあるかもしれない。その対策としてデジタルのはがきの提供が考えられるが、デジタルはがきをユーザ端末と中央サーバを用いた場合にはデータの管理ミスによる消去・改ざんが起きうるかもしれない。
【０００３】
そこで分散型台帳技術ＤＬＴ・分散型台帳システムを用いた本願提案のはがきシステムを提案する。例えば前記デジタルはがきは代替不可能なトークン（ＮＦＴ）の形ではがきデータ一枚ごと・トランザクション一件ごとに個別のトークンＩＤを割り当ててデジタルはがきの差出人Ｂがその受取人Ａに対しトークンを発行してはがきデータを送付・割り当てしてよい。
【０００４】
（非特許文献１のようなブロックチェーン技術・ブロックチェーンネットワークが公知であり、ブロックチェーンのデータブロック内にスマートコントラクト・プログラムを格納し。例えばＮＦＴをユーザに割り当てたり動的コードの生成などの処理を行わせることができる。）
【０００５】
＜デジタルはがき＞分散型台帳システム・ブロックチェーン上に非代替性トークンＮＦＴを特定のユーザ識別子に発行・送付できることは公知であるが、本願で分散型ＳＮＳの１つの形態として前記ＮＦＴにメッセージデータ（短文でもよい）を持たせ発行する情報処理システムを（デジタルはがきシステムとして）提案する。
【０００６】
＜デジタルはがきの差出人ユーザの実在確認・ユーザ認証＞分散型台帳技術では秘密鍵からユーザ識別子・公開鍵アカウント・ウォレットを作成する。しかしそのユーザ識別子・ウォレットは実在するユーザの物か否か確かめる必要があるかもしれない。例えば秘密鍵はランダムに生成できるが、それは人の手ではなくボットプログラムによっても出来てしまい、機械のユーザーがヒトに成りすましてデジタルはがきやシステムのＳＮＳ上での投稿が行えてしまうかもしれない。
【０００７】
ＳＮＳユーザーがＡＩ・ボットであることを防ぎ、ＳＮＳの話題が意図時に作られた話題であるなどする事を防ぐときに、（あるいはユーザがボットでないかどうか判断するデータを提供する為に）ユーザの認証が必要になる。
本提案では秘密鍵を有するユーザ端末に対するユーザ識別子・公開鍵アカウント・ウォレットを対面のコード認証により認証することが可能なシステムを提案する。
【０００８】
具体的には秘密鍵を有することで生成可能な認証コードを秘密鍵を有する（秘密鍵にアクセスできる）被認証者ユーザ端末の表示装置・出力装置に動的コード生成認証部３０ＡＰＰ－ＯＴＰ－ＡＵＴＨに基づいて生成させた認証コード出力させ、認証用ユーザ端末に前記認証コードを読み取らせる二次元コード認証（ストアスキャン方式の二次元コード認証、図２のＤ１、図６のシークエンス部、図３）により、被認証者ユーザ端末のユーザ識別子（及び秘密鍵を用いて動的コード認証用のコードをユーザ端末が生成できている事、秘密鍵を保有・利用出来る事）を認証する。

【先行技術文献】
【非特許文献】
【０００９】
【非特許文献１】イーサリアムホワイトペーパー、ｈｔｔｐｓ：／／ｅｔｈｅｒｅｕｍ．ｏｒｇ／ｅｎ／ｗｈｉｔｅｐａｐｅｒ／
【発明の概要】
【発明が解決しようとする課題】
【００１０】
本願にて解決しようとする問題点は、デジタルはがきＥＭを提供する際に、ＥＭ内の暗号化されたメッセージＭを復号し開封する際にユーザ認証されているいるか確認しやすくすることである。前記はがきの差出人情報・署名部が付与されたはがきシステムを構築したいときにユーザーの認証が必要であって、好ましくは対面でのユーザ認証（郵便局等施設窓口でのユーザ認証）を行いやすくすること。また短文・はがき風でもよいＳＮＳを提供する。
デジタル郵便物の改ざん・紛失を防ぐことも課題である。例えば火災により消失したり、雨などで濡れて破損するなどして差出人から宛名のユーザにメールが届かないことを防ぐ。またデジタルの分野ではデータの管理ミスによる消去・改ざんから郵便物を守る事も必要かもしれない。
【課題を解決するための手段】
【００１１】
対面でのユーザ認証・郵便局等施設窓口でのユーザ認証を行いやすくするために、図６に記載のシーケンスによるユーザ認証とホワイトリストを作成を行う。また前記ユーザ認証部（プログラム・スマートコントラクト）や認証結果及び前記結果３０ＤＬＲ－ＬＩＳＴ－ＡＰによるホワイトリスト部３０ＡＰＰＥＭ－ＷＬはブロックチェーン部に格納されており改ざん耐性・耐障害性を有している。
＊図１はデジタルはがきＥＭの説明図である。図１にはデジタルはがきを構成するデータ記憶部の記憶部ＥＭが記載されている。
＊前記デジタルはがきの記憶部ＥＭに含まれるメッセージデータＭは暗号化されてもよい。データＭは平文と暗号文を混合したものでもよい。（封筒に紙の信書を格納し封じた信書郵便をデジタルはがきＥＭにて再現する場合、暗号文の含まれるＭを必要とする）
＊前記デジタルはがきの記憶部に含まれる差出人デジタル署名・電子署名部ＣＡＳは次の（１）（２）を備えてよい。（１）ユーザ識別子ＥＯＡの基になる秘密鍵による署名ＥＴＨＣＡＳ（２）公的・民間の電子証明書による電子署名・デジタル署名ＣＡＰＣＡＳを含んでよい。署名ＣＡＳが含まれることでメッセージの送信者とメッセージ受信者の間で紛争が生じた場合であっても送信者・署名者を識別・判別・検知することができる。
【００１２】
＊図３には登録された送信者・署名者を識別・判別・検知する為のＥＭの選択部・仕訳部・セレクタ部３０ＡＰＰＥＭ－ＳＥＬＥＣＴＯＲ－ＷＬ－ＡＣＣＯＵＮＴが記載されている。前記セレクタ部３０ＡＰＰＥＭ－ＳＥＬＥＣＴＯＲ－ＷＬ－ＡＣＣＯＵＮＴはホワイトリスト３０ＡＰＰＥＭ－ＵＬ・３０ＡＰＰＥＭ－ＷＬを用いて前記リストに登録されたユーザの識別子・ＥＯＡによるデジタル署名ＥＴＨＡＣＡＳが付与されたはがきＥＭ又ははがきＥＭのトランザクションであるかどうかを判定し、登録されているＥＯＡが差し出したはがきＥＭを選別・仕訳し、宛名のユーザ識別子にはがきＥＭが来ていることを通知したりはがきＥＭの閲覧ダウンロードを仲介したりしてよい。
（また前記セレクタ部３０ＡＰＰＥＭ－ＳＥＬＥＣＴＯＲ－ＷＬ－ＡＣＣＯＵＮＴはノード３Ａに配置してもよいしユーザ端末１に配置してもよい。）
＊前記セレクタ部３０ＡＰＰＥＭ－ＳＥＬＥＣＴＯＲ－ＷＬ－ＡＣＣＯＵＮＴは認証されたホワイトリストに追加されている署名部がＥＭに記録されているか否かを検知してよい。
＊また署名ＣＡＳが含まれていないデジタルはがきデータＥＭ・データ記憶部ＥＭについ

てはブロックチェーン部のブロックチェーン記憶部３０ＤＬＲに格納しないブロックチェーンのノード部がコンピュータネットワークシステムに含まれていてよい。
差出人デジタル署名の前記（２）の公的・民間の電子証明書による電子署名・デジタル署名部は暗号化されていない・可読性のある差出人の電子証明書に基づく電子署名が付与された記憶部・データ部を有してもよい。
【００１３】
ＣＡＰＣＡＳが例えば暗号化されておらず平文又は読み取れる公的な電子証明書による署名データである場合、差出人の署名ＣＡＰＣＡＳを受取人は認知・検知できる。
差出人が問題のあるメッセージＥＶＩＬＭを暗号化しＭに記憶させ受取人に送付し、受取人はＭを鍵を用いて復号し、ＥＶＩＬＭを見て抗議したいと考え、捜査機関に願い出る場合に、前記署名ＣＡＰＣＡＳを捜査機関に提示することで、差出人を識別・検知・認知し差出人に対して紛争解決のための行動をとりやすくすることを期待する。
またＣＡＰＣＡＳを付与したメッセージをデジタルはがきＥＭに含めることで、メッセージ送信時に責任が生じ、メッセージを送るときにそのメッセージを本当に送るべきか考える時間を与えるかもしれない。
【００１４】
前記（２）の公的・民間の電子証明書による電子署名・デジタル署名部を備えていない場合であっても、（１）のＥＯＡによる署名を備えている場合には、ブロックチェーン部にデータを格納してよい。そして一定時間経過後に（数日、数週間、数か月、数年）ブロックチェーンデータ部からデータを削除してもよい。
【００１５】
＜はがき・通信に付随する機能、決済機能、デジタルＩＤ・アカウントの応用＞
スマートコントラクト部による認証部（３０ＡＰＰ－ＳＴＯＲＥＳＣＡＮ、３０ＡＰＰ－ＯＴＰ－ＡＵＴＨ）を用いた二次元コード認証機能により対面での認証機能・電子決済機能・新規ユーザ招待機能を提供してよい。
【００１６】
ＣＡＰＣＡＳ・ＥＴＨＡＣＡＳを付与したデジタルはがきＥＭに、決済の指図データを含ませてよい。たとえば、農家が生産した米穀・農産物を路地販売等で販売するときに、購入者が自身の持つ口座の残高を販売農家の口座に振り替える指図データＭＮＹＤ（例えば口座を振り返る権限をあたえるパスワード、ワンタイムパスワードデータ）をデータＭ備えさせ、購入者を差出人、販売者を受取人として、（さらには購入のお礼に関するはがき・メッセージをデータＭに含ませ、）送付し、受取人は受け取ったＥＭのＭのＭＮＹＤから口座残高の移動を指図し決済してよい。
【００１７】
＜ＳＮＳや通信分野での、決済機能、デジタルＩＤ・アカウントの応用＞
本提案ではブロックチェーンベース（秘密鍵式のアカウント）の為、ユーザがＳＮＳ内で用いるＮＦＴ・デジタルグッズの交換可能である。ＳＮＳで相手にはがき用でもよいスタンプを与える・投げ銭チップする等にコミュニケーションを取るため秘密鍵を用いたＳＮＳが用いられてよい。
【００１８】
＜ブロックチェーンアカウント認証とアカウントによる署名＞
＊ＣＡＰＣＡＳは公的・民間団体発行の電子証明書が好ましいが、ＣＡＰＣＡＳは民間発行の場合、維持するコストがかかり、また公的な（実印に相当するような認証レベルの）公的・民間身分証の秘密鍵で日常の友人間の通信に署名が常に必要になる事を避けたい場合（日常遣いの場合）、簡易の電子証明書・秘密鍵が欲しくなるかもしれない。
そこでＥＴＨＣＡＳを実在のユーザ間あるいは認証を行う箇所（ＣＶＳ・荷物受取場面・本人確認郵便・郵便局・学校など教育現場・学生証や社員証へのＥＴＨＣＡＳ用鍵の紐づけ箇所）でＥＴＨＣＡＳとユーザを紐づけてよい。（ＥＴＨＣＡＳの持ち主がボットでないこと、ＥＴＨＣＡＳは少なくともある人物が認証したＥＯＡによるものであることを紐づけにより把握する。）

対面でのコード認証・ストアスキャン方式のコード認証を用いて互いのＥＯＡ・ＥＯＡ用秘密鍵が実在することを調べ認証済みのＥＯＡとユーザのホワイトリストを作成し、そのリストにあるＥＯＡの鍵で署名されたはがきＥＭを優先して表示するデジタルはがきシステムを構成してよい。

【００１９】

本願では、ＰＧＰにおける信頼の輪方式（公開鍵が正当な持ち主であることを保証する署名をお互いに付け合う。初めて受け取る公開鍵でも、自分が信頼するユーザーの署名が含まれていれば、その公開鍵が正当だとする）を、ブロックチェーンのＥＯＡ・秘密鍵とブロックチェーンベースのコード認証部・ストアスキャン方式の対面コード認証部・認証スマートコントラクト、対面認証したという結果（Ａ－ｗｉｔｈ－Ｂ）のリストを用いて行おうとする。

＊ＥＴＨＣＡＳはＰＧＰの信頼の輪方式、ＣＡＰＣＡＳは別途第三者による証明書を用いたＳ／ＭＩＭＥ方式で提供されてよい。

【００２０】

＊信頼の輪方式をブロックチェーンで行う場合にブロックチェーンベースの動的コード認証を行いストアスキャン方式でユーザ間で秘密鍵を格納し秘密鍵により駆動される動的認証コードのスマートコントラクトから読みだされた認証コードを読み込み認証させ、ユーザが持っている端末とユーザとＥＯＡをユーザー間で認証しあってよい。

【００２１】

例えばユーザ識別子Ａとユーザ識別子Ｂのユーザ同士で互いの端末に表示されたコードを読取ＯＴＰ認証してその際の互いのＥＯＡ（Ａ・Ｂ）が互いに対面認証したという結果（Ａ－ｗｉｔｈ－Ｂ）を認証コントラクトに保管する。

はがきアプリＡＰＰ－ＥＭは前記認証コントラクトに記録された前記結果（Ａ－ｗｉｔｈ－Ｂ）を読取記録しており、その後Ａ宛てにＢからはがきＥＭがユーザ識別子Ｂの秘密鍵で署名されたＥＴＨＣＡＳを付与された形で届けられたとき、ユーザＡのアプリＡＰＰ－ＥＭは前記結果（Ａ－ｗｉｔｈ－Ｂ）からＢのＥＴＨＣＡＳを付与されたはがきＥＭはホワイトリスト内（簡易に対面認証済みの）のはがきであるとして、仮にＥＭ内部に暗号化文章があってもそれを復号しＡに閲覧できるように表示する。

【００２２】

＊特願２０２１－００４７８８に記載のＯＴＰ生成コントラクトと認証コントラクトを用いて、ストアスキャン方式の認証コードを２つのスマホまたは端末間で表示・読み取りさせ、ＯＴＰ認証させ、ボットでなく自然人・ユーザーであることを確認させ、対面認証済みのユーザのＥＯＡリストをストアスキャン式コード認証で形成し、そのリストを参照してユーザのホワイトリストを作成してよい。

（特願２０２１－００４７８８に記載のように、秘密鍵を有することで生成可能な動的認証コードの生成部は例えばデジタルはがきシステムで用いられるブロックチェーン部にあると、コード生成認証部・コード計算部・計算アルゴリズム部が改ざんされず、計算アルゴリズムの更新が可能であり、別途動的認証コードを生成認証する外部サーバを設置しなくてすむかもしれない。）

【００２３】

たとえば、対面ＯＴＰ認証を招待者からゲストに招待するときに行わせ、認証されたユーザのＥＯＡをＯＴＰ認証コントラクト３０ＡＰＰ－ＯＴＰ－ＡＵＴＨ（３０ＡＰＰ－ＳＴＯＲＥＳＣＡＮ）に記録する。対面認証済みＥＯＡリストをストアスキャン式コード認証で形成し、そのリストを参照してユーザのホワイトリストを作成する。（図６、図２のＤ１）

その後前記認証されたユーザについてはデジタルはがきアプリ１０ＡＰＰＥＭ・３０ＡＰＰＥＭや、短文型で誰からも閲覧できるメッセージMが平文で暗号されていないはがきを用いたメッセージＳＮＳ３０ＡＰＰＥＭやパブリック型の台帳３０ＤＬＲにて優先的に表示させる。

【００２４】

〇ＮＦＴ応用はがきの記憶部と前記記憶部を有する情報処理システム・コンピュータシステムを提案する。
郵便において信書・はがきには切手が貼られ郵送される。本提案スーパーアプリも暗号化されたメッセージを切手の代わりにブロックチェーン内部トークン（ＥＴＨ同等品）を消費することで送付できてもよい。
〇公開されたＮＦＴはがきによる短文公開分散型ＳＮＳを構成してよい。
暗号化しないＮＦＴはがきは、ブロックチェーン上へのコメント・つぶやきのように用いられるかもしれない。ブロックチェーンに古くなったＮＦＴはがきデータを除去する機能がない場合には、ＮＦＴはがきの内容は改ざんできず残り続けるため、はがきの書き手には注意が求められる。
＊ＮＦＴはがきを暗号化し、一部の参加者に復号鍵を渡して閲覧してもよい。
＊ＳＮＳ特化型チェーンはプライベート・コンソーシアムチェーンとパブリックチェーンに分けてよいし、パブリックチェーン内部メッセージを暗号化させてプライベート部を構築してよい。
＊実在の郵便はがきでは差出人の住所記載が必要であり、郵便物には筆跡や指紋等が記録される利点がある。本願尾はがきシステムにおいて、署名ＣＡＰＣＡＳ・ＥＴＨＣＡＳがない場合に犯罪へのコミュニケーションツールとなることを防ぐため、ユーザに収集するデータについて開示し同意を得たうえで１０ＡＰＰＥＭ・３０ＡＰＰＥＭはユーザ識別子ＥＯＡやユーザ端末のセンサ値・デバイスＩＤ・ＩＰアドレス等のデータを収集し追跡等できる構成でもよい。
＊本願提案のはがきシステムは、犯罪に使われることを防ぐため、好ましくは署名ＣＡＰＣＡＳやホワイトリスト化されたＥＴＨＣＡＳがＥＭに付与されているかを調べ、前記署名ＣＡＰＣＡＳ・ホワイトリストに含まれる署名ＥＴＨＣＡＳ付与されている場合には、はがき閲覧アプリ１０ＡＰＰＥＭはＥＭを優先的に閲覧できるよう処理を行う。（例えば新着のＥＭである場合には新着で未開封であるので開封閲覧するように促し、内部にＡＫＴＢによる暗号化データがある場合には別途ＡＫＴＢの入力を求め復号処理を行い閲覧させる。）
若しくは犯罪への利用を防ぐためホワイトリストに記載・登録されたＥＯＡによる署名の無いＥＭは台帳部３０ＤＬＲに格納記録しない恒星もとることができる。その際は３０ＡＰＰＥＭ－ＳＥＬＥＣＴＯＲ－ＷＬ－ＡＣＣＯＵＮＴが台帳に記録できるＥＭ（すなわちホワイトリスト登録された正味ユーザによるＥＭか否か検知し、仕訳選択して台帳に格納するか判断し、正味ユーザであれば格納する。
＊本願のはがきシステムでは図１から図４のようなカメラとスキャナを用いたコード認証によりユーザ間でユーザ端末を認証し信頼の輪・ホワイトリストを構成し、前記ホワイトリストに基づく署名のあるはがきを優先してユーザに閲覧させる。
＊差出人情報の無いＮＦＴを消去・ミュート・優先してユーザに閲覧させない制御部をブロックチェーンノードのアプリ３０ＡＰＰＥＭあるいはブラウザ部・フロントエンドアプリ部１０ＡＰＰＥＭをユーザ端末１は備えてよい。
【００２５】
さて、災害時においてＳＮＳ・テキストメッセージによる情報の通信は音声動画よりもデータトラフィックを低減されうる。そのため被災者間での情報伝達を行うときにＳＮＳは有用かもしれない。本願のはがきシステムは短文テキストベース且つ分散型・ブロックチェーンベースのコミュニケーション手段となる事も意図するが実証が必要である。
【００２６】
例えば地上の災害時に地上間の電力・通信網が停止する虞がある。それに対抗する為、通信網についてはＨＡＰＳ高高度プラットフォーム、あるいは人工衛星コンステレーションとユーザ端末間の通信手段の提供（通信網の提供）が有効かもしれない。
また電力確保についてユーザ端末は非常時においても太陽電池や電気自動車・自動車エンジン発電機による充電ができると好ましい。災害時においても前記電力・通信が確保でき本提案のはがきシステムを利用出来る場合、コミュニケーションが取れるかもしれない。

【発明の効果】
【００２７】
本願デジタルはがきＥＭについて、差出人が匿名でなく身元をたどれるホワイトリストに登録された認証されたユーザであってメッセージに認証されたユーザの署名が含まれていれば、後日問題が起きても署名やＥＭのユーザ識別子から差出人をたどり紛争解決が可能になる。
また差出人は署名部が必要の為メッセージの内容に責任を持つ効果が生まれる。他方、本システムは匿名であってもメッセージは送る事ができるが、開封時に前記署名部がないのでユーザは未開封でＥＭを復号開封しない事もできる。匿名性と安全性を兼ね備えるためにはがきＥＭに署名部を付与し・署名を行ったユーザはホワイトリスト登録を行う構成であって、前記ＥＭ・署名部・ホワイトリスト・ユーザ認証プログラム・デジタルＩＤ記憶部はブロックチェーン部（ノード部３Ａ）に格納でき、中央管理型でなく複数団体ので分散管理が行え、はがきＥＭ・デジタルＩＤ記憶部・コンピュータネットワークシステムを管理する際の１社・１ユーザ当たりのコスト低減を狙いつつ、改ざん耐性や耐障害性をもたせる効果が生まれうる。
本願システムでは分散型台帳システム・ブロックチェーンを用い、デジタルはがきＥＭやユーザ認証用プログラム、認証されたユーザのホワイトリスト等改ざんを防ぎたいデータをブロックチェーンに格納し保管できる。またブロックチェーン内のユーザ識別子を前記認証プログラム部にて認証し、ホワイトリストを作成し、デジタルＩＤ・ウォレットして利用できる。（具体的な例として、切手トークンの販売とユーザ確認を運輸系企業・通信系企業・郵便局などのＰＯＳレジや職員のスマホカメラ・スキャナで行える効果も生じる）
本願デジタルはがきシステムは、紙の郵便物では火災により消失したり、雨などで濡れて破損するなどはせず、ブロックチェーンにより改ざん耐性・耐障害性があって、ＥＭの送信時にブロックチェーン内部のタイムスタンプ（送信時のブロック番号の記録）が自動的に付与がされる（そして切手は切手トークンとして用いられ、切手の消印がデジタルシステム内で自動でできる）、デジタルはがき・信書を提供できるかもしれない。
（なお本願で紙の信書郵便による通信を用いてユーザ間１Ａ・１Ｂでの鍵ＡＫＴＢの共有を行ってもよい。紙により封書できる既存郵便を本願ではメッセージの暗号化の鍵共有時に利用されてよい。
＊紙の郵便には信書を封書・封印・封緘できるメリットがある。同様に秘匿化できるのであれば量子鍵配送による鍵や公開鍵暗号によるメッセージを暗号化する鍵を生成・用意してよい。）
〇本願システムは郵便局・郵便インフラ利用は確定していない。郵便インフラの利用を限定しているわけではない。本提案のシステムは郵便をイメージして考案された電気通信システムであり、実物の郵便物・紙書類を扱う郵便はがきとは異なる面がある。
＊例えばストアスキャン方式のユーザ認証（Ｄ１）は郵便局窓口などが既存のはがき郵送の延長で想定されるが、宅配・配達事業者の拠点であったりＣＶＳや駅・商業施設・公的施設に設置のＡＴＭ・改札装置・チケット利用関連装置・窓口であってもよい。
＊例えば鍵ＡＫＴＢは封書に格納し信書便に相当する配達・宅配手段を用いて送付してよい。
【図面の簡単な説明】
【００２８】
【図１】はがきデータＥＭの説明図。左図（Ａ）は外部電子証明書によるデジタル署名（ＨＭＡＣ等でもよい）部分ＣＡＰＣＡＳをＥＭは有しており、右図（Ｂ）はブロックチェーン部・分散台帳システムに用いる鍵・電子証明書による署名ＥＴＨＣＡＳやユーザ識別子をＥＭは有している。
【図２】ユーザとコンピュータの説明図。
【図３】アプリ３０ＡＰＰＥＭ、１０ＡＰＰＥＭの説明図。
【図４】正味使用可能なユーザーリストの算出に用いるリストの記憶部の説明図。

【図５】ノード端末３Ａとブロックチェーン型データ記憶部３０ＤＬＲの説明図。

【図６】ブロックチェーン型記憶部に記録されてもよいＯＴＰ／動的コード認証部とホワイトリスト記憶部３０ＡＰＰＥＭ－ＷＬを有する認証サーバ３Ａを介して、差出人端末１Ａから宛名受取人１Ｂをユーザ認証しホワイトリストを作成するシークエンスの説明図。

【図７】ブロックチェーン型記憶部を含むはがきサーバ３Ａを介して、差出人端末１Ａから宛名受取人１Ｂまでデジタルはがきｅｍが伝達されるシークエンスの説明図。（はがきサーバ３Ａはユーザ認証サーバとＥＯＡ／アカウント／デジタルＩＤのホワイトリスト保管サーバを兼ねる）

【発明を実施するための形態】

【００２９】

図１にはがきＥＭが含む情報を記載する。はがきにはユーザの秘密鍵による署名部ＣＡＰＣＡＳ・ＥＴＨＣＡＳを設けることで送付するユーザは署名を付与し明確にメッセージを送ろうとする意思を表明させ（責任をもって）はがきＥＭを送付したことを見分けることに用いる。前記署名はホワイトリストに登録された署名か否かをはがきアプリ内で検証する。

この他、既存の紙のはがきと同じく宛名の名前・宛名の住所・宛名のユーザ識別子と、差出人の名前・差出人の住所・差出人のユーザ識別子と、トランザクションＩＤとトランザクションに費やしたコスト・ネットワークのガス代金・切手トークンの量・トランザクションがブロックチェーンに送付された時の差出日を記載できる。

図２はユーザとコンピュータの説明図である。差出人ユーザ１Ａと受取人ユーザ１Ｂとそれを仲介するブロックチェーンノード３Ａ（３Ａはブロックチェーン以外にも個別のサービス例えばオンライン動画配信サイト等も含んでよい）が記載されている。

図２の右図Ｄ１には対面コード認証の説明例が記載されており、対面コード認証ではブロックチェーンベーススマートコントラクトによりＯＴＰ・認証コードを生成させストアスキャン方式によりそのコードを表示させ読み取らせる。例えば図６のシークエンス図に従ってユーザ１Ａはユーザ１Ｂに認証されたコードを読み取ることで１Ａは１Ｂを認証する（Ａ－＞ａｕｔｈ－＞Ｂ）。そして認証済みのユーザをリスト（３０ＤＬＲ－ＬＩＳＴ－ＡＰ、３０ＡＰＰＥＭ－ＷＬ、３０ＡＰＰＥＭ－ＵＬ）に記録し、図１におけるＥＴＨＣＡＳが認証されたユーザ識別子であるか調べるときに用いる。

図３はＥＭを含む台帳部３０ＤＬＲとそれに含まれるＥＭの説明図である。また前記ＥＭがホワイトリスト３０ＡＰＰＥＭ－ＷＬ・３０ＡＰＰＥＭ－ＵＬと３０ＡＰＰＥＭ－ＳＥＬＥＣＴＯＲ－ＷＬ－ＡＣＣＯＵＮＴによって選別仕訳されユーザに届けられる説明図である。またアプリ３０ＡＰＰＥＭ、１０ＡＰＰＥＭの説明図である。明示していない場合があるが、アプリを動作させる為の処理部と記憶部を３０ＡＰＰＥＭ、１０ＡＰＰＥＭは備える。

図４はユーザリストの作成の仕方に関する説明図である。認証済みのユーザをリスト３０ＤＬＲ－ＬＩＳＴ－ＡＰから３０ＡＰＰＥＭ－ＷＬそして３０ＡＰＰＥＭ－ＵＬへと転記していく。その途中で失効済みのユーザーリスト３０ＡＰＰＥＭ－ＲＬやＣＡＰＣＡＳによる署名が無いと失効指示できないＥＴＨＣＡＳのリスト・保護リスト３０ＤＬＲ－ＬＩＳＴ－ＣＡ－ＥＴに記憶された情報も組合せて正味の現在のユーザーリスト３０ＡＰＰＥＭ－ＵＬを作成する。３０ＡＰＰＥＭ－ＵＬは選択部３０ＡＰＰＥＭ－ＳＥＬＥＣＴＯＲ－ＷＬ－ＡＣＣＯＵＮＴに伝達される。

またＣＡＰＣＡＳに関する登録されたユーザーリスト或いは失効リストについては外部サーバよりリストを得く、こちらも正味現在のＣＡＰＣＡＳ用ユーザリスト３０ＣＡＰＣＡＳ－ＬＩＳＴが端末３Ａやユーザ端末１に記憶され選択部３０ＡＰＰＥＭ－ＳＥＬＥＣＴＯＲ－ＷＬ－ＡＣＣＯＵＮＴに伝達される。

図５はノード端末３Ａとブロックチェーン型データ記憶部３０ＤＬＲの説明図である。

図６はユーザ認証をストアスキャン方式で行うときのシークエンス図である。

図７はデジタルはがきＥＭを差出人から宛先受取人に伝達する際のシークエンス図である

。
【実施例１】
【００３０】
＜＜ユーザ認証＞＞
図６にブロックチェーン型記憶部に記録されてもよいＯＴＰ／動的コード認証部とホワイトリスト記憶部３０ＡＰＰＥＭ－ＷＬを有する認証サーバ３Ａを介して、差出人端末１Ａから宛名受取人１Ｂをユーザ認証しホワイトリストを作成するシークエンスの説明図を記載する。
図６において、Ｓ－ＰＡ１のステップでは、ユーザ端末１Ｂが１Ｂの持つ秘密鍵１０ＫＥＹと秘密鍵に基づくユーザ識別子Ｂを用いており、前記秘密鍵・識別子を用いてブロックチェーンのノード３Ａにアクセスし、３Ａの台帳部３０ＤＬＲに格納された動的コード認証プログラム３０ＡＰＰ－ＯＴＰ－ＡＵＴＨを用いて認証コード（ワンタイムパスワード）を生成・呼び出しする。
Ｓ－ＰＡ２のステップでは、Ｓ－ＰＡ１の後、例えばスマートコントラクトに記憶された動的コード生成認証プログラムである３０ＡＰＰ－ＯＴＰ－ＡＵＴＨにて動的コード（ＯＴＰ）を生成する。例えば認証コード：認証コード１４２８４５。
Ｓ－ＰＡ３のステップでは、Ｓ－ＰＡ２の後、端末１Ｂが取得した前記認証コードと、１Ｂや３Ａ等でストアスキャンを行う一連のソフトウェア３０ＡＰＰ－ＳＴＯＲＥＳＣＡＮを用いてユーザ端末１Ｂは出力装置から前記認証コードを出力する（例えば１Ｂのディスプレイに二次元コード・バーコードの形で出力する。）例として、ストアスキャン時にユーザ１Ａに読み取らせるデータとして、前記認証コードを含むＤ１－ＢＲＣＤ－ＤＡＴＡを生成して表示・出力させる。例えばＳ－ＰＡ３では端末１Ｂのディスプレイに認証コード・認証データＤ１－ＢＲＣＤ－ＤＡＴＡ＝「ＥＯＡユーザ識別子：Ｂ。認証コード１４２８４５。」という情報を含む二次元バーコードを表示させる。この場面で名刺交換やユーザ名・ユーザＩＤの認証を行う場合は、例えばユーザ名：Ｂｏｂ＠３８９１．．．をコードに含めたり、ユーザ情報（ユーザ名、ユーザＩＤ・ドメイン、ユーザ識別子、ユーザの現実の氏名住所、電話番号、メールアドレス、所属団体、個人のＰＲ部分コメント、顔写真、名刺の任意画像・任意テキスト）又は名刺情報を含めてよい。
Ｓ－ＰＡ４のステップではストアスキャンにてコードを読み取る端末１Ａは入力装置例えばカメラやバーコードスキャナを用いて前記認証コード・認証データＤ１－ＢＲＣＤ－ＤＡＴＡを読み取る。（このときユーザＡとユーザ端末１Ａは認証されるユーザ端末１Ｂとユーザ Ｂを視認したりその風貌を視認・撮影吸うこともできるかもしれない。防犯用に端末１Ｂのコードを撮影する時のデータが利用されうる。）
Ｓ－ＰＡ５のステップでは、読み取られたコードＤ１－ＢＲＣＤ－ＤＡＴＡに含まれる認証コード（例：認証コード１４２８４５）をノード３Ａに含まれるコード真贋判定部・コードの検証部３０ＡＰＰ－ＯＴＰ－ＡＵＴＨに入力し、検証させその結果を戻り値又は応答として得る。
Ｓ－ＰＡ６のステップでは３０ＡＰＰ－ＳＴＯＲＥＳＣＡＮ・３０ＡＰＰ－ＯＴＰ－ＡＵＴＨの動作後に、認証結果が正しい場合、結果（Ａ－＞Ａｕｔｈ－＞Ｂ）を
３０ＤＬＲ－ＬＩＳＴ－ＡＰに記憶する。
Ｓ－ＰＡ７のステップでは３０ＤＬＲ－ＬＩＳＴ－ＡＰを用いて３０ＡＰＰＥＭ－ＷＬ／ＵＬを作成する。
【００３１】
＜＜はがき＞＞
図７にブロックチェーン型記憶部を含むはがきサーバ３Ａを介して、差出人端末１Ａから宛名受取人１Ｂまでデジタルはがきｅｍが伝達されるシークエンスの説明図を記載する。
図７において、Ｓ－ＰＯＳＴ１はＥＭのメッセージＭを暗号化する場合に必要である。共有鍵暗号又は非対称鍵暗号の鍵をユーザＡとＢの間で共有・保有する。
＜１．はがきＥＭの送信＞
Ｓ－ＰＯＳＴ２では宛先・署名に用いるＥＴＨＣＡＳ・ＣＡＰＣＡＳ、メッセージＭ、添

付ファイル又は添付ファイルの保存先（例えばＩＰＦＳやクラウドストレージのような保存先のＵＲＬリンクやそのファイルのパスワード等）メッセージに必要な切手トークンの確保、はがきソフト１０ＡＰＰＥＭの起動等を行う。
Ｓ－ＰＯＳＴ３でははがきＥＭのトランザクションを作成する。ユーザＡの鍵ＥＴＨＣＡＳＫを用いてＥＭのＥＴＨＣＡＳ部にデジタル署名を行ったり、差出人部を記述したり、宛名部、宛先のユーザ識別子Ｂを記述する。＊また通常ブロックチェーンシステム（イーサリアム等）ではトランザクションの送付先と送信元のＥＯＡユーザ識別子が自動でトランザクションに付与されるので、その部分も宛名と差出人の情報部分と考えてもよい。
Ｓ－ＰＯＳＴ４では１Ａからネットワークを介してブロックチェーンネットワークのノード３Ａにトランザクションが送付され、コンセンサスアルゴリズムに基づいてブロックチェーン型記憶部３０ＤＲＬに格納される。
＜２．はがきＥＭの受信＞
Ｓ－ＰＯＳＴ５では、Ｓ－ＰＯＳＴ４で送付されたＥＭについてユーザＢとユーザ端末１Ｂが（紙の郵便物が自身の管理する私書箱・ポストに郵便物が来ているか巡回して郵便物を回収するように）自身のアカウント・ＥＯＡにＥＭが届いているか３Ａにアクセスして検索・探索する。又は新着のＥＭがあるか３Ａに問い合わせ・リクエストする。
＊図７では開示していないが、端末３Ａ内部にはがきの新着等をモニタリングしユーザ１ＢのメールアドレスやＳＭＳあるいはスマートフォンに通知を送るアプリ（メールのダイモン部、メーラーソフト、ウェブメール）のようなものがあって、新着メールの有無をリアルタイムに通知してもよい。ブロックチェーンエクスプローラーであるサーバやサイトに自身のＥＯＡについて新たなＥＭ到着に関するトランザクションが来たかどうか監視させる形でメールの新着通知を行わせてもよい。図７では私書箱に対しユーザが郵便物の有無を問い合わせしたり、届いた郵便物を回収していくイメージで記載されている。
Ｓ－ＰＯＳＴ６ではユーザの問い合わせに応じて３０ＤＬＲ内のはがきＥＭをユーザ側はがきアプリ１０ＡＰＰＥＭ又はサーバー側はがきアプリ３０ＡＰＰＥＭが選択・読取する。
そしてＳ－ＰＯＳＴ７では前記１０ＡＰＰＥＭ・３０ＡＰＰＥＭは、ＥＭに付与されたデジタル署名ＣＡＰＣＡＳ・ＥＴＨＣＡＳや送信元のユーザ識別子がホワイトリスト３０ＡＰＰＥＭ－ＷＬ・３０ＡＰＰＥＭ－ＵＬに記録・登録されているか確認し、登録されていれば（このときＥＭの送信者は責任をもってメッセージＭに署名しておりいたずらなＥＭ・ボットのＥＭではないと期待して）ユーザ１Ｂに恐らく開封してよい署名済みＥＭであると表示しメールの開封・メッセージ復号を待つ。
Ｓ－ＰＯＳＴ８ではメッセージＭが暗号化されている場合鍵ＡＫＴＢを用いて復号する。（メッセージを開封する）
Ｓ－ＰＯＳＴ９ではＥＭのコンテンツ・メッセージＭをユーザに出力する（ユーザの入出力装置１２に出力する）。テキストや画像をディスプレイで表示したり、メッセージを音声で読み上げたり、ＥＭに添付又はリンク貼り付けされた画像・動画・音声・コンテンツデータを利用できるように処理する。
＊例えばホームビデオの動画ファイルが記録されたクラウドストレージへのリンクとファイルのハッシュ値・ダイジェストとファイルの復号又はクラウドストレージへのログインパスワードを表示したり自動でリンクさせ前記動画ファイルを再生させてもよい。
【００３２】
＜＊他の利用例＞
本願のはがきシステムとそのＥＯＡの対面でもよいコード認証に用いるデジタルＩＤシステムは、郵便・通信に用いるとともに身分証としても動作する効果があるかもしれない。例えばパーティ・交流会で相手の身分証を相手の連絡先をストアスキャン風にユーザが互いに認証コードを読み取り確認しつつ伝え合うことができ、交流・名刺交換のようなＩＤ交換に利用できるかもしれない。
＊本願でははがきをやり取りするユーザ情報（ユーザ名、ユーザＩＤ・ドメイン、ユーザ識別子、ユーザの現実の氏名住所、電話番号、メールアドレス、所属団体、個人のＰＲ部

分コメント、顔写真、名刺の任意画像・任意テキスト）又は名刺情報　について、ＩＤ交換・名刺交換を図６にシークエンスに従って行ってよい。名刺情報はユーザ端末１，（１Ａと１Ｂ）の間でそれぞれの１の記憶部１０に１０ＥＯＡ－ＵＳＥＲＮＡＭＥ－ＬＩＳＴ・１０ＥＯＡ－ＮＡＭＥＣＡＲＤ－ＬＩＳＴとして記憶してもよい。
＊また図６の構成で、名刺の他に身分証と身分証を読み取る端末として利用されてもよい。身分証データとして（ＥＯＡの秘密鍵ＥＴＨＣＡＳＫは身分証データ内では秘匿されており、例えば耐タンパ領域に鍵・ＥＴＨＣＡＳＫは格納されておりＰＩＮ等でロックされており）そのＥＯＡ識別子と氏名、住所、生年月日、性別や顔写真（流通可能な生体的特徴）情報１０ＥＯＡ－ＩＤＣＡＲＤがユーザ端末１に記憶されてもよい。そして１０ＥＯＡ－ＩＤＣＡＲＤを読み取りリスト化し１０ＥＯＡ－ＩＤＣＡＲＤ－ＬＩＳＴ・３０ＥＯＡ－ＩＤＣＡＲＤ－ＬＩＳＴに記憶する、本人確認やＩＤ管理に用いるユーザ端末１やサーバ３Ａであってもよい。
【００３３】
＜本システムのサーバと通信網・ソフトウェアの維持＞
本発明は通信網（有線インフラと無線インフラ・周波数帯域）とサーバとユーザ端末からなるものでネットワークを維持し計算機端末・保守要員・電力など投入し稼働させ続ける必要があり、それを（例えば災害戦災などでインフレする中で）経済的に維持するには本ネットワークのノード群とそのネットワークを複数法人が維持する事が妥当であると考える。
＊例えば前記法人が郵便局・運輸業・情報通信業（他に認証された個人・個人団体経営の簡易郵便局）の事業者連合体であってよく、前記連合体を構成する各団体がそれぞれノード３Ａを分担してネットワーク２０を維持して本願はがき用コンピュータネットワークシステム２０ＥＭを構成してよいかもしれない。
＊本願ではブロックチェーンを用いるがそのデータブロックの連結コンセンサスアルゴリズムとしてＰｏＳやＰｏＡ（Ｐｒｏｏｆ－ｏｆ－Ａｕｔｈｏｒｉｔｙ）、ｉｓｔａｎｂｕｌ　ＢＦＴ、Ｒａｆｔ等公知の方式を用いてよい。コンセンサスアルゴリズムにＰｏＡを用いた場合内部トークンは前記各団体が最初の保有者となり、その後はがき代の法定通貨を払い込みしたユーザへの対価としてユーザに内部トークンを付与する形態が想定される。（各団体のＥＯＡ・ウォレットからユーザのユーザ識別子ＥＯＡ・ウォレットに内部トークンが信書用の支払い手段・トークン・コインとして付与されると想定する。）
【００３４】
＜切手に該当する内部トークンの流通・消費＞
＊本提案のはがきシステムも紙の郵便と同じくＥＭ１通を送付するごとに料金・トークン・デジタル切手を消費するよう設計してよい。＊はがきＥＭのトランザクションを送付するには内部トークンを手に入れて消費する必要がある。内部トークンは例えばユーザ識別子間で所謂ファンジブルトークンのように譲渡したり、トークンを新規に発行する部分・箇所から調達してよい。
＊ＰｏＷや内部トークンを提供するＰｏＳ方式にてノードの担い手にトークンを付与してもよいしＰｏＡ方式で管理してもよい。
＊本提案のシステムは、ユーザが内部トークンを第三者（システムからのマイニング・第三者ユーザ等）から調達しなければはがきＥＭを送ることができない特徴を持つ。内部トークンは例えば郵便局・ＣＶＳ・古物商のユーザから購入する事が想定される。クレジットカード等による切手トークン販売をしてもよい。
（この時トークン販売においても対面でのコード認証・コード決済の形でユーザ端末を販売店のＰＯＳレジのスキャナなどで読取ストアスキャンし、代金支払いの対価としてスキャン先のＥＯＡにトークンを付与してよい。所謂コード決済により郵便局窓口などで顧客を確認しつつ切手トークン販売してよい。ホワイトリストに登録のＥＯＡにはクレジットカードで切手トークン販売・付与してよい）
【００３５】
＊ユーザはボット・匿名・ホワイトリストユーザーであってもＥＭの送付には内部トーク

ン（或いは例えばイーサリアム等既存のブロックチェーンネットワークの内部にそのようなトークンを作る場合はＥＲＣ２０等のトークン）の消費を要する。
＊３０ＡＰＰＥＭや分散型台帳システムの設計によっては既存の紙郵便と同じく宛名など郵便配達に必要な事項が記載され切手・切手トークンが消費されれば匿名（差出人不明郵便）であっても宛名ユーザにはがき・信書封筒が伝達されうる。しかしその封筒を開封するか否かはユーザに任される事になる。ＥＭに署名部ＣＡＰＣＡＳ・ＥＴＨＣＡＳがあるか確認したうえで、それがない匿名のＥＭを開封するかどうかはユーザの意思による。本願ではＯＴＰ方式でもよいストアスキャン式コード認証部を含めたことでユーザ間での対面でのホワイトリストに登録しやすくしており、かつホワイトリストに登録されたＥＯＡのＥＴＨＣＡＳの署名を確認し匿名のＥＭを見づらくする又は匿名であるとアプリ３０ＡＰＰＥＭで警告する処理を行うときに処理しやすくする意図を持っている。署名があるＥＭか否かを見分ける事に役立てようという意図がある。
【００３６】
＜本発明のハードウェアの構成＞
コンピュータの構成を図２に示す。コンピュータ・ユーザ端末・ノード端末は制御処理部（１１，３１）、記憶部（１０、３０）、入出力装置又は通信装置（１２、３２）を有しており通信経路２０・通信ネットワークと接続されている。Ｄ１に記載の様に例えばカメラ（入力装置１４の例）とディスプレイ（出力装置１５の例）を搭載したユーザ端末同士（ユーザ端末を手に持ったユーザ同士で）ストアスキャン方式の図６に記載のシークエンスによるユーザの認証を行える。
各端末はコンピュータとしての五大装置を含み電源や電気回路・バスを有している。本出願における一般的なスマートフォン端末のハードウェアでは制御処理部はＣＰＵ、グラフィック処理用のＧＰＵないしはＡＩ用の処理を行うプロセッサ、ＩＯや通信などのコントローラ部を含んでもよいシステムオンチップＳｏＣが用いられうる。記憶部においてはＲＡＭやＲＯＭが用いられる。ＲＯＭ又は不揮発メモリとしてＮＡＮＤフラッシュメモリ・ＳＳＤが用いられる。通信装置には無線モデム・無線用チップが用いられ、サーバ端末の場合は有線接続も用いられる。
＜ストアスキャン用のハードウェア構成＞
Ｄ１において、カメラ又はディスプレイが用いられているが、Ｄ１の例と同等のユーザ認証ができる場合は別の装置でもよい。たとえばカメラの代わりにスキャナ・ハンディスキャナ・ＰＯＳレジのスキャナが利用されうる。Ｄ１においてユーザＡはヒトでもよいしカメラ・スキャナとディスプレイを搭載した本人確認機能を持つＡＴＭ装置でもよい。
公的な身分証とその鍵ＣＡＰＣＡＳＫとブロックチェーン上の鍵ＥＴＨＣＡＳＫやＥＯＡの対応リストを作れるように、公的な身分証のデジタル証明書や公的な身分証とデータ通信可能なＡＴＭ装置・ＡＴＭユーザ端末でもよい。
前記ＡＴＭ装置はコンビニエンスストアＣＶＳや郵便局、駅、役場など施設に配置され、市中のユーザが無人のＡＴＭ装置を用いてユーザ登録・ホワイトリストへの登録を行うときに用いる想定である。
【産業上の利用可能性】
【００３７】
本願のはがきシステムと、はがきシステムに用いるユーザ識別子・ＥＯＡの対面でもよいコード認証・ホワイトリスト登録システムを用いたデジタルＩＤシステムは、郵便・通信に用いるとともに身分証としても動作する効果があるかもしれない。
【符号の説明】
【００３８】
＜図１＞
ＥＭ：はがきデータ。
本願では、はがきデータ　ＥＭは、分散型台帳システム・ブロックチェーンネットワークのノードサーバ３Ａ内部の記憶装置３０のブロックチェーン式記録部３０・記憶部３０に複数のＥＭｓとしてデータブロックに格納され記録されている。

宛名情報ＲＥＳＵ：ＥＯＡユーザ識別子Ａ、（住所、氏名Ａ）。郵便はがきの宛名部
メッセージＭ：メッセージデータＭまたはコンテンツデータＭ。Ｍは平文データと暗号文データとを混合可能。メッセージには任意のタイプのデータが含まれていてよい。例えば音声や画像・動画データが含まれていてよい。音声や動画等のコンテンツデータを別途異なるストレージに保存させ、前記ストレージへリンクまたはアクセス手段が記録されていてもよいし、前記コンテンツデータのハッシュ値がＭに含まれていてよい。例えばメッセージＭは絵はがき・動画音声付デジタルはがきでもよく、動画データについてはそのハッシュ値と動画データのリンク先（あるいはＩＰＦＳのようなファイル流通サービスにおける識別子）が保存されていてもよい。暗号データはＡＫＴＢ等の鍵により復号され又は暗号化により生成される。
差出人情報ＴＲＡＵ：ＥＯＡユーザ識別子Ｂ、（住所、氏名Ｂ）、デジタル署名部。郵便はがきの差出人部
差出人デジタル署名・電子署名ＣＡＳ：例（１）ＥＯＡの秘密鍵による署名ＥＴＨＣＡＳ（２）公的・民間の電子証明書ＣＡＰＣＡＳ、個人にいては個人番号カードの電子証明者や公的・民間団体発行する任意の証明書を用いる想定であり、法人においては商業登記に基づく電子証明書等を用いてよい。
トランザクションコスト、切手トークン部：必要に応じてトランザクションにかかった金額・ガス量・手数料を記憶してよい（郵便物の切手を張る部分・切手貼付部に該当）
トランザクションＩＤ、特定記録追跡ラベル部：ＥＭをはがき信書便１通１トランザクションとした場合の管理ＩＤでありブロックチェーンにおけるユーザ端末がノード３Ａブロックチェーンシステムへトランザクションを送る場合のトランザクションＩＤ。（郵便物の特定記録・書留用の管理ＩＤ部・ラベル部に相当）
図１（Ａ）：電子署名付きデジタルはがき、デジタル信書ＥＭ、信頼されたはがき用＊公的・民間の電子証明書による電子署名があり、防犯の為発信者たどれる。暗号文も搭載可能
図１（Ｂ）：電子署名無しデジタルはがき、やや匿名性のあるＳＮＳ用
（＊ＥＯＡの秘密鍵はランダム生成可能の場合、匿名性のあるＥＯＡからのＥＭ送信を行う。他方、匿名であり証明書の無いメッセージの為、ＥＭの差出人が実在する人物か否かは不透明である。またボットの可能性もある。ただし、証明書をつけるわけにはいかない用途、例えば匿名でメッセージを送りたい用途（匿名での口コミ・内部告発など）のために、（Ｂ）の構成も必要かもしれないので本願では（Ｂ）の構成を持つＥＭも利用されうる。）
＊図１の（Ａ）ではＣＡＰＣＡＳを用いており暗号化データをメッセージＭに含む形（紙の郵便物における手紙を封書に入れて受取人以外は読めないようにした状態）と同等にしたことで、ＥＭが受取人Ａへの暗号化された脅迫などを含む場合であっても、差出人ＢのＣＡＰＣＡＳがＥＭに含まれている事で受取人Ａは差出人ＢのＣＡＰＣＡＳでどのような脅迫文が届けられたかを連絡できる。
＊本発明では、ＣＡＰＣＡＳを付与したはがき信書はブロックチェーン中で改ざんされず時刻情報・タイムスタンプを付与されながら台帳部に保存・保管される利点を持つ。
＊そしてＣＡＰＣＡＳ・ＥＴＨＣＡＳ署名をＥＭが含む場合、ＥＭはブロックチェーに記憶されており改ざん困難でタイムスタンプもついており、捜査機関などへの証拠等として提出されうるから、差出人Ｂは脅迫文等を書きにくくなる・発言メッセージにに責任を持つこと事を期待する。他方、図１の（Ｂ）のようにＣＡＰＣＡＳを持たず匿名ではがきＥＭをブロックチェーン位格納してもよいが、その場合、はがき閲覧アプリなどで、ＥＭに署名がなく発信元が不明でありリスクがあるとユーザに警告してよい。
＊また該署名無しＥＭについては匿名であり署名もなく重要度が低いデータであるからノード３Ａの台帳部３０ＤＬＲに記録保管する期間を短くする・削除する・アクセスできなくするようにしてもよい。
＜図２＞
１　ユーザ端末、ユーザコンピュータ

１Ａ　ＥＭとＭのデータを伝えたいユーザ端末、はがき受取人ユーザ端末
１Ｂ　ＥＭとＭのデータを作成・ＣＡＰＣＡＳ等による署名・３Ａへ送信するユーザ端末、はがき差出人ユーザ端末
１０記憶装置　（基本ソフト、ブラウザ等、動作用ソフトウェア含む）
１０ＫＥＹ　秘密鍵情報記録手段（３Ａの３０ＤＬＲアクセス用）
１１処理装置
１０ＣＶＭ　ユーザ端末における実行環境（メッセージＭの暗号化部、復号部を含む）
１６外部記憶装置、外部記録手段
２０　ネットワーク、通信経路、情報の伝達（配布）経路
３　サーバ（ユーザ端末１がサーバになってもよい）
＊１や１Ａ、３や３Ａコンピュータであって、記憶装置１０・３０、処理装置１１・３１、通信装置・入出力装置１２・３２は電気回路・通信経路・バス等で接続されている
３Ａ　分散型台帳システムのノード端末　、　３Ｂ３Ａと同等の他のノード
３０　記憶部
３１　制御部・処理部
３Ｃ　サーバ　、３Ｄ　サーバ（オフラインになりうる）
３０ＫＥＹ　暗号化・復号用鍵情報記録手段　※耐タンパ性有する物可
３０ＣＶＭ・３０ＣＶＭＵ　メッセージＭ内部の暗号データを復号可能な実行環境（鍵ＥＴＨＡＣＡＳＫ、１０ＫＥＹ、３０ＫＥＹやや外部の鍵ＡＫＴＢ等を暗号化又は復号の鍵に用いる）
３０ＵＩユーザ端末インターフェース（ブラウザ等）
３０ＰＶＭ　平文データ読み取り用の第１実行環境
３０ＤＬＲ　分散型台帳システムＤＬＳの記録部・台帳部。具体的にはブロックチェーン部
ＣＡ：デジタル署名・電子署名用鍵又は証明書
ＣＡＰＣＡＳＫ：公的・民間の電子証明書・秘密鍵（公的・民間の電子証明書・秘密鍵ＣＡＰＫＥＹ）
ＣＡＰＣＡＳ：ＣＡＰＣＡＳＫによるデジタル署名
ＥＣＡ：ＥＯＡ又は或るユーザ識別子の電子署名用鍵又は証明書
ＥＴＨＣＡＳＫ：ＥＯＡ又は或るユーザ識別子の秘密鍵（ＥＯＡ又は或るユーザ識別子の秘密鍵：ＥＴＨＫＥＹ）
ＥＴＨＣＡＳ：ＥＴＨＣＡＳＫによるデジタル署名
ＡＫＴＢ：オプションのパスワード・鍵（ネットワーク２０以外の通信経路、量子暗号通信や電話・口頭・封書・信書郵便等で伝達されてもよいパスワードであってＥＭに含まれる暗号化メッセージの復号鍵ＡＫＴＢでもよい。）
Ｄ１：対面コード認証の説明例
＜図３＞
３０ＡＰＰ－ＳＴＯＲＥＳＣＡＮ：ストアスキャン形式の動的コード認証用プログラム（ユーザ端末１やサーバ３、３Ａに含まれる）
３０ＡＰＰ－ＯＴＰ－ＡＵＴＨ：動的コード認証用プログラム（特願２０２１－００４７８８に開示のブロックチェーンのスマートコントラクトを用いた　動的コード認証用プログラムでもよい。）
３０ＤＬＲ：ブロックチェーン方式の記憶部。台帳部。３０ＤＬＲはパブリック型でよい。例えばサーバ３Ａに含まれる３０ＤＬＲはネットワークを介してユーザ端末１に閲覧・データ複製されてもよい。またパブリック型であるため、ユーザはＥＭを３０ＤＬＲに格納するときにＥＭのメッセージの一部を暗号化しなければはがきの内容を秘匿化する事ができない。
＊暗号化されたデータについて常にブロックチェーン上で保管していると将来計算力が高く暗号化を突破できる計算機が現れた場合に復号されてしまう虞が無いとは言えないので、ブロックチェーン上のデータについて例えば１０年を過ぎたデータＥＭについては削除

するブロックチェーン基盤等を用いると好ましいかもしれない。＊好ましくは、３０ＤＬＲの内容を需要やユーザの求めに応じて一部削除・忘却させることができると好ましい。不要である３０ＤＬＲのデータを削除する機構を本願のはがきＥＭを利用するシステムに備えさせて良い。
＊ブロックチェーン型であり、３０ＤＬＲにＥＭを記録させるときに内部トークンＫＩＴＴ（郵便切手型トークンＫＩＴＴ）を消費する。
ブロックチェーンシステム・ノード３Ａは、署名ＣＡＰＣＡＳやＥＴＨＣＡＳの有無、メッセージMの暗号化の有無（信書メッセージか？ＳＮＳのつぶやきメッセージか？）に関わらず、ユーザ・ユーザ識別子が保有する前記トークンＫＩＴＴを消費することでブロックチェーン部３０ＤＬＲにＥＭを組み込むトランザクションを送り、組み込まれる。
＊いたずらなＥＭやＤＯＳ攻撃を防止するため、経済的価値のある本願デジタルはがきを行うための内部トークンを購入又は入手したユーザ識別子でないとＥＭを含むトランザクションをブロックチェーンに送付する事ができない。
（内部トークンはブロックチェーンでの付与・交換・譲渡の履歴をさかのぼることで追跡することができる特徴がある。匿名のユーザ識別子ＸがメッセージMを暗号化しＥＭを送付しようとしても内部トークンの残高がなければ送ることはできず、Ｘは何らかの手段で内部トークン・ガスを手に入れる必要があり、それを手に入れるときにＸはトークンの持ち手と接点を持たねばならない特徴を有する。トークンについては特定のユーザに権限を与えて生成させる場合とＰｏＷやＰｏＳのようにノードを維持することで報酬として内部トークンを得る形があるかもしれない。）
＊内部トークン（内部切手トークン）の他にＥＲＣ２０型の様なファンジブルトークンでもよいし、紙の切手の様に個別の絵柄と額面価格データを有するノンファンジブルトークンでもよい。
３０ＤＬＲ－ＰＬＯＰＡＬ：暗号化されたメッセージMを含んでよい、はがきやレター等デジタルはがきＥＭを格納した３０ＤＬＲの記憶部。（はがきや手紙のブロックチェーン公開台帳　Ｂｌｏｃｋｃｈａｉｎ　ｐｕｂｌｉｃ　ｌｅｄｇｅｒ　ｏｆ　ｐｏｓｔｃａｒｄｓ　ａｎｄ　ｌｅｔｔｅｒｓ）
３０ＤＬＲ－ＰＬＯＰＡＬや３０ＤＬＲのデータブロックに格納されたトランザクションやそれに含まれるはがきＥＭやメッセージMについては、Mが一部または全部暗号化されていない場合、その内容は外部ユーザが読み取れ、その読み取られることをＳＮＳにおける他の全ユーザが閲覧できるつぶやき・コメントとすることもできる。他方、メッセージMにＡＫＴＢ等鍵で暗号化することではがきＥＭを封筒で封書にするように内容を秘匿化できる。
３０ＤＬＲ－ＬＩＳＴ－ＡＰ：　動的コード認証用プログラムで認証した側と認証された側の対応関係のリスト記憶部。（該記憶部はブロックチェーンのデータブロックやスマートコントラクト内部のリストデータとして記憶されていてよい。）
３０ＡＰＰＥＭ－ＷＬ：３０ＤＬＲ－ＬＩＳＴ－ＡＰより作成したホワイトリスト。この場合失効したＥＯＡ・ユーザ識別子はカウントできないので以下失効リスト３０ＡＰＰＥＭ－ＲＬも併せて必要。
３０ＡＰＰＥＭ－ＲＬ：ユーザ識別子の失効リスト。ＣＡＰＣＡＳで署名されたトランザクションの有無によりユーザ識別子を失効する。予めＥＴＨＣＡＳＫとＣＡＰＣＡＳＫの対応関係を台帳３０ＤＬＲに記憶している事が好ましい。
（例えばＫＡＺという名前のユーザの公的な証明書の秘密鍵ＣＡＰＣＡＳＫ－ＫＡＺがある場合、その公開鍵ＣＡＰＣＡＰ－ＫＡＺ又はその識別子と、ブロックチェーン用秘密鍵ＥＴＨＣＡＳＫ－ＫＡＺの公開鍵ＥＴＨＣＡＰ－ＫＡＺ又は識別子の対応関係を記憶することが好ましい。そして鍵ＥＴＨＣＡＳＫ－ＫＡＺが第三者に漏洩したりあるいは定期的に更新したい場合には、公開鍵ＣＡＰＣＡＰ－ＫＡＺと公開鍵ＥＴＨＣＡＰ－ＫＡＺ又は識別子間の対応関係を失効させるトランザクションを台帳に記憶させ、３０ＡＰＰＥＭに失効結果が読み取られるようにする）
＊公開鍵ＥＴＨＣＡＰの失効について、他には複数のＥＯＡ・識別子から失効の指定を集

める・失効の投票を求める形で失効をさせてもよい。
３０ＡＰＰＥＭ－ＵＬ：正味のホワイトリスト、正味のユーザーリスト。該リストは３０ＡＰＰ－ＯＴＰ－ＡＵＴＨや３０ＤＬＲ－ＬＩＳＴ－ＡＰと同一のブロックチェーンに記録されていてもよい。また別のブロックチェーンネットワークに記録されてもよいし或るサーバ３Ａやユーザ端末１に記録されてもよい。１や３Ａに記録される場合該ホワイトリストには改ざんされないようデジタル署名やタイムスタンプが付与されていると好ましい。
３０ＡＰＰＥＭ、１０ＡＰＰＥＭ：ユーザ端末１やサーバ３、３Ａ等のデジタルはがきのダイモンソフト（守護ソフト）、常駐プログラム。
３０ＡＰＰＥＭ－ＳＥＬＥＣＴＯＲ－ＷＬ－ＡＣＣＯＵＮＴ：はがきＥＭの送信者についてホワイトリストに記載の送信者のはがきか否かを選別する部分、または、ホワイトリストに該当するＥＭをユーザ端末に閲覧させる選別・選択を行う部分。（受取人Ａが受取人Ａ宛てのはがきを検索又ははがきデータ取得をリクエストした際に、３０ＡＰＰＥＭ－ＵＬのようなホワイトリスト・ユーザーリストに記載のユーザの識別子が送信者であるデジタルはがきＥＭを優先してユーザに伝達する部分）
３０ＣＶＭ：実行環境仮想機械・ソフトウェア。暗号化メッセージMの復号部を含んでよい。Mの復号には鍵ＡＫＴＢを用いてよい。
３０ＡＰＰＥＭ一ＭＡＩＮ：はがき閲覧ソフト、ブラウザソフト。はがき閲覧の為の基本プログラム・メインプログラム。
３０－ＵＩ：ユーザーインターフェース。ブラウザソフトのＵＩでもよい。
３０ＡＰＰＥＭ一ＥＴＣ：その他ソフトウェア、変数・関数・鍵等。
ＥＸ－ＣＯＮＴＥＮＴＳ：ＥＭに含まれる外部リンクコンテンツ・添付ファイル
３０ＥＯＡ－ＵＳＥＲＮＡＭＥ－ＬＩＳＴ：ユーザ名・ユーザーネーム・ドメインネームとユーザ識別子の対応リスト部。ドメインネームシステムのドメイン名とＩＰアドレスの対応リストに類似するリスト。
該リストはＤ１：対面コード認証の説明例のようにユーザＡがユーザＢとユーザＢの端末をスキャンしてコード認証するときにユーザＢの端末に表示されたユーザ識別子とユーザー名を読取してその対応関係を記録する。なおリスト内に同一のユーザ名が登録済みである場合にはユーザ識別子の末尾等を付与して登録するなどしてよい。
公知のドメインネームサービスシステムの様に利用者同士でユーザ名・ドメインを譲渡付与しあってもよい。
Ｄ１－ＢＲＣＤ－ＤＡＴＡ：Ｄ１のシーンにてコード認証Ａ－＞ａｕｔｈ－＞Ｂを行うときにユーザ間でやり取りする認証コードに含まれる情報（例、ＥＯＡユーザ識別子：Ｂ、ユーザ名：Ｂｏｂ＠３８９、認証コード１４２８４５）
＜図４＞
３０ＤＬＲ－ＬＩＳＴ－ＡＰ：動的コード認証用プログラムで認証した側と認証された側の対応関係のリスト記憶部。
３０ＡＰＰＥＭ－ＷＬ：ホワイトリスト。３０ＡＰＰＥＭのホワイトリストＷＬあるいはトラストリストＴＬ、認証されたユーザのリスト、ユーザＡがユーザＢをストアスキャンで認証したなどのＬＩＳＴ－ＡＵＴＨ－ＰＡＩＲ。これは３０ＤＬＲに記録されてよいし、３０ＤＬＲより３０ＡＰＰＥＭが参照してアプリ動作時に利用してよい。また前記リストを３０ＡＰＰＥＭに転記・複製してよい。
＊ホワイトリストはユーザ間の交流で作成してもよいし、団体や公的窓口が確認してもよい。例えば郵便や宅配を行う団体の識別子Ｐがあって団体に属する職員のユーザＰがユーザＡＡＡからＦＦＦまで各住所の玄関に赴いてユーザ端末のストアスキャンを行いＷＬを作成してもよい。あるいは住所変更時に役所でストアスキャンしてユーザを認証しつつＷＬに記載してよい。或いは役所・会社・団体のユーザＰがその窓口にてユーザを認証しＷＬに加えてもよい。
＊なお説明例＜ＷＬ＞ではＸの端末はストアスキャンされていないので、（Ｘは＜ＬＩＳＴ－ＡＵＴＨ－ＰＡＩＲ＞には記録されているが、Ｘの端末をスキャンした端末による記

録はないので）ＸはホワイトリストＷＬに入っていない。
３０ＡＰＰＥＭ－ＲＬ：失効リスト。失効を指示したユーザ識別子と失効されるべきユーザ識別子の指示のリスト。失効には公的又は民間の第三者が発行した証明書による署名ＣＡＰＣＡＳを付与し、失効したいユーザが失効を希望する識別子に対し失効希望するトランザクションを送付し失効させる。もしくはノード３Ａのはがきシステムを提供するサービス提供者・団体の管理するユーザ識別子（図では識別子Ｃ）が失効させたいユーザの識別子（図ではＢ，Ｄ）を失効させる。）
＊または、３０ＡＰＰＥＭ－ＲＬは３０ＡＰＰＥＭ－ＷＬに登録されたユーザ識別子が指定時間（数か月、数年、５年）経過した場合失効するようにプログラムされ時間経過とともに実行すべきユーザ識別子を自動的に追加してよい。前記自動で失効する場合、ユーザは失効する前に新たなユーザ識別子と鍵を生成しＤ１に記載のコード認証を行って再度鍵とＥＯＡを３０ＤＬＲ－ＬＩＳＴ－ＡＰと３０ＡＰＰＥＭ－ＷＬに登録する事を求めてもよい。＊自動で失効する場合においても３０ＤＬＲ－ＬＩＳＴ－ＣＡ－ＥＴを用い、ＣＡＰＣＡＳ署名付きの指示がなければＥＯＡを失効させないこともできる。
３０ＤＬＲ－ＬＩＳＴ－ＣＡ－ＥＴ：ＣＡＰＣＡＳとＥＴＨＣＡＳの利用者を対応付けたリスト。またはＥＴＨＡＣＡＳとＣＡＰＣＡＳが該リストで結びついておりそのＣＡＰＣＡＳによる署名つきの失効指示がなければ失効されないＥＴＨＣＡＳのリスト・保護リスト。該リストに記載のＣＡＰＣＡＳはそれに対応するＥＴＨＣＡＳを失効する際に用いる。（このリストに記載がないＥＴＨＣＡＳを失効させる場合はノード３Ａのはがきシステムを提供するサービス提供者・団体の管理するユーザ識別子Ｃが失効させたいユーザの識別子（図ではＢ，Ｃ）を失効させる。（図では例えば識別子Ｃとその秘密鍵は郵便の団体や公的役所等で管理者として利用されうるアカウント。）
３０ＡＰＰＥＭ－ＵＬ：現在、正味使用可能なユーザーリスト。３０ＡＰＰＥＭ－ＷＬ、３０ＡＰＰＥＭ－ＲＬ、３０ＤＬＲ－ＬＩＳＴ－ＣＡ－ＥＴから算出する。ユーザの要求に応じて毎回前記３つのリストを検索し算出してもよいが、計算資源・通信資源を節約する目的で、定期的に（例えば毎日１時に算出、月１、年１回算出するなどして）算出し３０ＡＰＰＥＭ－ＵＬとして３Ａや３０ＤＬＲに記録させてもよい。その算出部３０ＡＰＰＥＭ－ＵＬにユーザからのアクセスをうけるようにしてよい。
＜図５＞
３０Ａ・３１Ａ：分散台帳システムのノード端末の記憶部・処理部
３０ＤＬＲ：分散型台帳システムの記録部、３１ＤＬＲ：分散型台帳システムの制御部・処理部
ａ１，ａ２，ａ３，ａ４，，，ａｎ：ブロックデータａ１，ａ２，ａ３，，，ａｎ
ａ１ｈ，ａ２ｈ，ａ３ｈ，ａ４ｈ，，，ａｎｈ：データブロックａ１，ａ２，ａ３，ａ４，，，，，ａｎのハッシュ値・ダイジェストデータ
ａ１：ジェネシスブロック（ａ０ｈ：ジェネシスブロックのデータ）
ＥＭ：はがきデータＥＭ。ブロックチェーンにおけるユーザ端末からノード３Ａに送信される１つのトランザクションに相当するデータのまとまりでもよい。
ＥＭｓ：複数のはがきデータＥＭを含む記憶部
３０ＤＬＳＣ・３１ＤＬＳＣ：ノードクライアントのプログラム記憶部・制御部管理部
３０ＰＶＭ・３１ＰＶＭ：実行環境のプログラム記憶部・実行環境制御部
３０ＥＴＣ・３１ＥＴＣ：　その他制御部のソフトウェア・その他制御部
＜図６＞＜図７＞は実施例１にて説明。
【００３９】
＜書類名＞要約書
＜要約＞デジタルはがきシステムにおいて、防犯性を持たせるためデジタル署名を有する記憶部を備えさせ、前記記憶部がないはがきデータＥＭについてブロックチェーン部・台帳部３０ＤＬＲに取り込まない処理部・制御部や取り込み後であってもユーザの目に触れない閲覧部を備えさせ、はがきデータを閲覧する受信者ユーザを保護する。
＜課題＞ブロックチェーン部に記録したはがきデータＥＭ（はがきトークン、トランザク

ション）について、匿名性を重視する場合と防犯の為発信者特定に役立つ場合の両方を共存させたい。
＜解決手段＞ノード３Ａのブロックチェーン部のブロックデータに格納するはがきデータＥＭについて、ＥＭをブロックチェーン部３０ＤＬＲに格納する。データＥＭにはブロックチェーンにて持ちいるユーザ秘密鍵由来の証明書によるデジタル署名部ＥＴＨＣＡＳ又は外部による証明書（例：身分証の証明書・秘密鍵）による署名部ＣＡＰＣＡＳを記録させる・含ませる。ＥＴＨＡＣＡＳは例えばブロックチェーンベースの二次元コード認証を用いたユーザ間の認証を通じ登録ユーザをリストに登録する形で信頼の輪を形成してよい。
＜＜請求の範囲＞＞
＜請求項１＞通信経路と、差出人・送信者ユーザー端末と、受取人・受信者ユーザー端末と、ブロックチェーンノード端末と、メッセージデータ・トランザクションに付与された差出人・送信者ユーザ署名の有無を検知する検知部、若しくは、前記検知部を有するノード端末と、前記差出人・送信者ユーザ署名つきのメッセージデータ・トランザクションを選択する選択部、若しくは、前記選択部を有するノード端末とを含む、コンピュータネットワークシステムであって、
前記メッセージデータ又は前記データのトランザクションは、ブロックチェーンノード端末のブロックチェーン部のブロックデータに記憶されており、前記メッセージデータ又は前記データのトランザクションは、公的な証明書・第三者による電子証明書の秘密鍵、
又は、ブロックチェーンにトランザクションを送付する秘密鍵・ブロックチェーンのユーザ識別子の基になる秘密鍵・ブロックチェーンのユーザ識別子による、署名部を含んでおり、
前記選択部又は前記選択部を有するノード端末は、前記秘密鍵に対応する認証されたユーザ識別子・電子証明書のリストを記憶しており、前記記憶されたリストに記憶されたユーザ識別子・電子証明書による署名が付与されたメッセージデータ・トランザクションを、前記選択部を用いて選択し、受取人・受信者ユーザー端末ユーザに伝達・閲覧させるコンピュータネットワークシステム。
＜請求項２＞前記秘密鍵に対応する認証されたユーザ識別子・電子証明書のリストは、差出人・送信者ユーザー端末と、受取人・受信者ユーザー端末との間でストアスキャンを行うことにより作成される特徴を持ち、前記ストアスキャンのための認証コードはブロックチェーンノード端末に記憶されたブロックチェーン部のスマートコントラクトにより生成される特徴を持つ請求項１に記載のコンピュータネットワークシステム。
＜請求項３＞メッセージデータ・トランザクションは暗号化されたメッセージＭを含む請求項２に記載のコンピュータネットワークシステム。
＜請求項４＞暗号化されたメッセージＭを復号・暗号する為の鍵ＡＫＴＢは、信書郵便・封書配達による通信経路を用い、受取人・受信者ユーザー端末に伝達する、請求項３に記載のコンピュータネットワークシステム。
【００４０】
本発明の実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行なうことができる。