(19)日本国特許庁(JP)　　(12)公開特許公報(A)　　(11)特許出願公開番号
特開2024-59549
(P2024-59549A)
(43)公開日　令和6年5月1日(2024.5.1)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 9/32	*(2006.01)*	H04L 9/32	200B	
G06F 21/60	*(2013.01)*	G06F 21/60	320	

審査請求 未請求　請求項の数 2　OL　（全 31 頁）

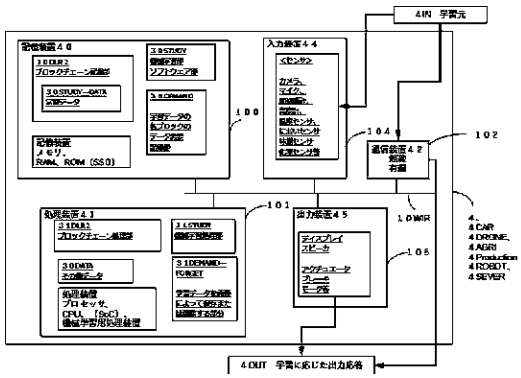
(21)出願番号　特願2023-91772(P2023-91772)
(22)出願日　令和5年6月2日(2023.6.2)
(62)分割の表示　特願2022-167241(P2022-167241)の分割
原出願日　令和4年10月18日(2022.10.18)

（特許庁注：以下のものは登録商標）
１．ＰＹＴＨＯＮ

(71)出願人　714009083
西沢　克弥
長野県上田市吉田５１５番地２
(71)出願人　722014745
株式会社ＳＩＮＧＵＬＩＯＮ
東京都千代田区神田和泉町１番地６－１６
ヤマトビル４０５
(72)発明者　西沢　克弥
長野県上田市吉田５１５番地２

(54)【発明の名称】人工知能システム、人工知能システムの学習方法

(57)【要約】　（修正有）
【課題】人工知能の学習の過程を外部から解析・検証可能な、ブロックチェーンを用いたコンピュータネットワークシステム並びに人工知能の機械学習方法を提供する。機械学習データを忘却・消去しコンピュータ端末の記憶装置の記憶領域を節約するコンピュータネットワークシステムを提供する。
【解決手段】ブロックチェーン部のブロックデータを一部取り除いた場合（データを忘れさせた場合）においてもブロックデータの連続性を検証する方法であって、ブロックチェーン記録部３０ＤＬＲ２の、第１のブロックチェーン部と第１のブロックチェーンのハッシュ値・ダイジェストデータを含む第２のブロックチェーン部を共に記憶装置に記憶させる。
【選択図】図９



【特許請求の範囲】
【請求項１】
ノード端末としてユーザ端末（１Ａ）と、ブロックチェーンを用いた分散型台帳システムのノード端末（３Ａ）とを、ネットワーク（２０）を介して接続したコンピュータネットワークシステムにおいて、
前記ユーザ端末（１Ａ）は、前記ノード端末（３Ａ）のブロックチェーン部（３０ＤＬＲ）のブロックデータに記憶されたデータを読み取り前記データをプログラムとして実行可能な、実行部（３０ＣＶＭ）を含んでおり、前記ユーザ端末（１Ａ）は、前記ブロックデータに記憶された前記データは、暗号化された暗号化データを含み、前記実行部（３０ＣＶＭ）は、前記暗号化データを復号する鍵を備え、前記ユーザ端末（１Ａ）は、前記実行部（３０ＣＶＭ）を用いて前記暗号化データを復号し、前記暗号化データを復号して得られたデータを用いるプログラムを実行可能な実行部を備えている、コンピュータネットワークシステムであって、
前記ノード端末（３Ａ）は、前記ノード端末（３Ａ）の記憶装置に、第１のブロックチェーン部と、第２のブロックチェーン部とを共に記録・記憶しており、前記第２のブロックチェーン部の或るブロックデータに、前記第１のブロックチェーン部の指定個数のブロックデータの其々のハッシュ値が含まれている特徴を持つ、コンピュータネットワークシステムを用いた人工知能システムであって、
機械学習に必要な学習データを、前記コンピュータネットワークシステムの前記ノード端末（３Ａ）の前記第１のブロックチェーン部のブロックデータ、又は、前記第２のブロックチェーン部のブロックデータに記憶する特徴を持つ人工知能システムを用いた機械学習方法。
【請求項２】
第１のブロックチェーンに記録された内容を削除する行程を含む、請求項１に記載の機械学習方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本願（実用新案登録願、又は、特許願）は、分散型台帳システムの台帳記録部３０ＤＬＲ（図面では図１等の３０ＤＬＲ）において、プログラム単位（スマートコントラクト）を実行・記憶するコンピュータシステム、プログラム実行部、データ構造、方法に関する。
【０００２】
本願は台帳３０ＤＬＲに暗号化データが含まれ、前記暗号化データを復号し、復号後のデータに含まれるプログラムを実行する環境や方法に関する。
図４Ａ・図４Ｂ・図４Ｃに本願の主張する方法を用いてワンタイムパスワード認証を行う場合の説明図・概念図を記載する。
【０００３】
また本願は、第１のブロックチェーン（３０ＤＬＲ２－１ＳＴ）と第２のブロックチェーン（３０ＤＬＲ２－２ＮＤ）を含む台帳記録部３０ＤＬＲ２を提案する。
図５に本願で提案する台帳記録部３０ＤＬＲ２の説明図・概念図を記載する。
【背景技術】
【０００４】
＜提案の経緯＞
非特許文献１の発明により、分散型台帳システムＤＬＳで変数関数を備えたスマートコントラクト（以下コントラクト、又はスマコンとも呼称する）と、スマートコントラクトをプログラムとして実行する実行環境・仮想機械（非特許文献２のＥＶＭ）を用いて、前記ＤＬＳ上で用いられるトークン・ＮＦＴの発行や各種サービスの提供が行われるようになった。（例えば動的パスワードに用いられうる動的コードを生成するスマートコントラクトについては、米国特許明細書２００２４４４５７や、特許文献１の明細書部分及び特開

２０２１－００４７８８にて開示されている。）
【０００５】
●しかし公知の分散型台帳システムは（取引の透明性のため、防犯のため）台帳データがパブリックであって（世界中の人に丸見え状態であり）、スマートコントラクト内部の命令コード・関数・変数は外部から解読される恐れがあった。
●そこで本願では特開２０２２－０９１１５８で主張されるワンタイムパスワード（ＯＴＰ）認証プログラムのうち秘匿化・暗号化したいＯＴＰ計算用キー変数や関数・手続き、データ群を暗号化して３０ＤＬＲに記録した後、記録された暗号化データをユーザ端末やサーバでの暗号化データを復号可能な実行環境３０ＣＶＭＵ・３０ＣＶＭ（仮想機械３０ＣＶＭ）にて復号し復号データに含まれるプログラム（特にＯＴＰの計算、ＯＴＰの生成プログラム、ＯＴＰの検証・認証プログラム）を実行させる方法やコンピュータシステムに関して提案を行う。
【０００６】
●また分散型台帳システム上で割当・購入・取引・譲渡・流通するトークン（或いはデジタル資産・デジタル通貨）はユーザ識別子（あるいは或るユーザの公開鍵や識別子の情報）に対し或るトークン番号のトークンが対応する形でスマートコントラクトに記録されており、ユーザの持つトークンの保有状況が外部から見られてしまう。（※そのため、現状ではユーザー識別子と現実世界でのユーザの対応関係は他者に公開しないほうがプライバシーを保つことができる。）（また証券会社や取引所等が仲介することで対応関係を秘匿する）
●個人ユーザ間でのトークンの授受のためにはユーザ識別子を互いに提示する事が必要なことがあって、台帳上に例えばユーザ識別子ＡからＢへの取引があったことが残り、透明性は保てる一方で、プライバシー性が低下する場合がある。
●そこで、本願では台帳上に記録されたユーザ識別子Ａに関する情報や、スマートコントラクトを駆動する際に一部隠したい変数・関数について、平文としてブロックチェーン上の平文・暗号文が混合したデータを読み取る実行部と、読み取られた前記平文・暗号文が混合したデータに含まれるデータのうち、（暗号化データの部分を認識・識別・選択等をして選び取って、）暗号化データを復号鍵を用いて復号することを提案し、前記復号する方法を用いた動的パスワード認証方法についても開示する。
【０００７】
●本提案によれば、平文としてブロックチェーン上の平文・暗号文が混合したデータを読み取る実行部３０ＰＶＭ（例えばイーサリアムのＥＶＭ、イーサリアム仮想機械）を備えた公知の分散型台帳システムに対し、平文に含まれる暗号化データの読み取りと復号を行う実行環境３０ＣＶＭ・３０ＣＶＭＵ（※３０ＣＶＭＵは特にユーザ端末内の実行環境）又は仮想機械３０ＣＶＭをブロックチェーンのノード部やユーザ端末ソフトウェア・記憶部・処理部に備えさせることにより、本願の提案する方法を実施することができ、既存の稼働実績の多いシステムをそのまま利用できる効果を主張する。（既存のブロックチェーン・分散型台帳システムと互換性があるメリットを主張する。）
【０００８】
＜既存の秘匿化方法＞
トランザクションを秘匿化する公知の分散型台帳システムとしてＱｕｏｒｕｍという企業向け分散型台帳システム基盤がある。プライベート及びパブリック型のトランザクションを用いる機構が搭載されている。ＱｕｏｒｕｍではＴｅｓｓｅｒａという暗号化に対応したマネージャ部（実行部）によりトランザクション共有したい相手に共有する。Ｑｕｏｒｕｍの系は暗号化機能をもつＴｅｓｓｅｒａのＡＰＩより暗号化したトランザクションを送付する。
【０００９】
●本願では上記Ｑｕｏｒｕｍとは別の解決方法を模索し、既存のパブリックで誰からも見ることのできる台帳データ部に、一部暗号データを記録させ（又は暗号データの開始部や終了部を表す暗号化データ読み取り用符号を備えさせ、（遺伝子の開始コドンと終止コド

ンのように）データを実行する部分（実行環境、実行部、実行機械、実行用仮想機械）が暗号化データ読み取りできる構成とする。
●なお暗号データと平文データを格納するスマートコントラクトに、暗号化データの呼び出し部又はゲッターとなる関数を設けさせ、暗号化データをブロックチェーンから呼び出して、サーバ３Ｃの第２実行部３０ＣＶＭやユーザ端末１Ａの第２実行環境３０ＣＶＭＵに暗号化データを入力し、復号鍵にて復号し、他の又は次の処理に用いてもよい。
【００１０】
●Ｑｕｏｒｕｍの系は、（発明者からみて）暗号化機能付き実行環境を１つ用いている。対して本願では平文のみの実行環境・第１実行環境により読み取ったデータを、暗号データ復号機能付き実行環境・第２実行環境で必要に応じて復号処理後に実行することで、普及した第１実行環境のみを備える分散型台帳システムにウェブアプリ等の形で第２実行環境を設けて、平文と暗号文交じりのブロックチェーンデータの読み取りに対応させる意図がある。
【００１１】
本願では前記第２実行環境としてウェブページに含まれたＥＣＭＡＳｃｒｉｐｔの処理に従い、１ブロックチェーン上から暗号文と平文の混合したデータを読取又はブロックチェーン上から暗号文を含むデータを選択・区別・識別して読取する処理と、２前記読取した暗号データを復号する処理部と、３復号したデータに従って次の処理（各種サービスのための処理等）を行う処理部があってもよい。
本願では図４Ｂと図４Ｃに、前記第２実行環境として（ユーザー端末にダウンロード若しくは配布され読み込まれた）ウェブページに含まれるＥＣＭＡＳｃｒｉｐｔの処理に従い、（ウェブブラウザやウェブページ・ウェブアプリを前記第２実行環境３０ＣＶＭＵ として）、ＯＴＰ認証時のＯＴＰ生成処理（図４Ｂ）とＯＴＰ認証処理（図４Ｃ）を行う処理の流れ図の例を記載している。
【先行技術文献】
【特許文献】
【００１２】
【特許文献１】特開２０２２－０９１１５８号公報
【非特許文献】
【００１３】
【非特許文献１】Ｖｉｔａｌｉｋ Ｂｕｔｅｒｉｎ、「Ｅｔｈｅｒｅｕｍ Ｗｈｉｔｅ Ｐａｐｅｒ Ａ ＮＥＸＴ ＧＥＮＥＲＡＴＩＯＮ ＳＭＡＲＴ ＣＯＮＴＲＡＣＴ ＆ ＤＥＣＥＮＴＲＡＬＩＺＥＤ ＡＰＰＬＩＣＡＴＩＯＮ ＰＬＡＴＦＯＲＭ」、［ｏｎｌｉｎｅ］、［西暦２０２０年、令和２年１１月１６日検索］、インターネット〈ＵＲＬ：ｈｔｔｐｓ：／／ｃｒｙｐｔｏｒａｔｉｎｇ．ｅｕ／ｗｈｉｔｅｐａｐｅｒｓ／Ｅｔｈｅｒｅｕｍ／Ｅｔｈｅｒｅｕｍ＿ｗｈｉｔｅ＿ｐａｐｅｒ．ｐｄｆ〉
【非特許文献２】Ｅｔｈｅｒｅｕｍ ＥＶＭ ｉｌｌｕｓｔｒａｔｅｄ［西暦２０２２年、令和４年９月３日検索］、インターネット〈ＵＲＬ：ｈｔｔｐｓ：／／ｔａｋｅｎｏｂｕ－ｈｓ．ｇｉｔｈｕｂ．ｉｏ／ｄｏｗｎｌｏａｄｓ／ｅｔｈｅｒｅｕｍ＿ｅｖｍ＿ｉｌｌｕｓｔｒａｔｅｄ．ｐｄｆ
【発明の概要】
【発明が解決しようとする課題】
【００１４】
本願にて解決しようとする問題点を以下に記載する。
１：スマートラクト内部変数や内部の処理手続・関数を秘匿・暗号化する方法を探すこと。
１－Ａ：スマートコントラクト式のＯＴＰ認証システムにおいて、計算に用いる変数関数等を秘匿化する事。
１－Ｂ：ユーザの取引履歴やユーザの保有するトークンの対応関係の秘匿化する手段を探

すこと。
【００１５】
ここで、発明者の考えとして、前記暗号化・秘匿化することにより、第三者から見てトランザクションの中身がＤＯＳ攻撃のデータか通常のユーザの利用データか判別できない事が想定される。（通常、トランザクションに手数料・トークン・ガスを消費させる場合、ＤＯＳ攻撃を経済的に防止するが、ここでは仮に攻撃できるとして）ＤＯＳ攻撃による無意味な暗号化トランザクションが台帳に蓄積しサーバの記憶域を圧迫する事が懸念される。そこで、次の問題を別途設定し、その課題に対応するブロックチェーンのデータ構造（３０ＤＬＲ２等）を提案する。
２：ブロックチェーンにおいて或る設定時間後の過去のデータブロックを削除しつつブロックチェーンの連続性を検証できるデータ構造を探すこと。（一部データブロックを忘れる事の出来るブロックチェーンの方式を検討する事。）
２－Ａ：ブロックチェーンにおいてデータブロックの一部が無くとも、ブロックチェーンのつながりを検証できるデータ構造を見つけること。
※過去のブロックデータを忘れられる事は台帳部のデータ容量の増大を防止できる。
【００１６】
発明者は保管期限が設定された公文書のように、過去のデータブロックを忘れられるブロックチェーンシステム・分散型台帳システム・改竄耐性のあるデータ台帳システムを実現したいと考えた。
データブロックが保管期限切れ（又は需要がなくなった場合）にはブロックチェーンから切り離しできるデータ構造を実現できれば、公文書データや、日常コミュニケーションデータ等含むＳＮＳ等ウェブサービス、証券の取引、物流サービスの記録等、（データ量が多く）データ保管期限が有限な分野でブロックチェーンを利用しやすくなると考え、本願の主張するブロックチェーンのデータ構造を開示する。
【課題を解決するための手段】
【００１７】
＜課題１：スマートラクト内部変数や内部の処理手続・関数を秘匿・暗号化する方法＞
１．スマートコントラクト実行を行う２種のプログラム実行部（仮想機械、プログラム実行部・実行用仮想機械、実施例ではＥＣＭＡＳｃｒｉｐｔ実行部をもつウェブアプリ・ウェブページ）を用いる。
一つはブロックチェーン部に書き込まれたコードをそのまま平文としてスマートコントラクトを実行する仮想機械３０ＰＶＭ（図１等、図４Ｂ等）であり、
他方はブロックチェーン部に書き込まれた暗号化されたコードを読み込み、復号し、スマートコントラクトを実行する仮想機械３０ＣＶＭ又は実行環境３０ＣＶＭ・３０ＣＶＭＵ（図１等、図４Ｂ等）である。
・前記ブロックチェーン部３０ＤＬＲに書き込まれた暗号化されたコードを読み込み、復号し、スマートコントラクトを実行する仮想機械に相当する機能部３０ＣＶＭＵ（図４Ｂ等）がユーザ端末にプログラム・記憶部・処理部の形で含まれていてもよい。
【００１８】
図１はブロックチェーンのノード端末３Ａと、（ＯＴＰ認証やＯＴＰ認証後のサービス提供を行う）サービス提供サーバ端末３Ｃと、ユーザ端末１Ａを通信経路２０を介して接続させ、
ユーザの秘密鍵１０ＡＫＥＹ（秘密鍵１０ＡＫＥＹは必要な場合）、台帳記録部３０ＤＬＲ、平文の実行環境３０ＰＶＭ（実行部３０ＰＶＭ）、復号鍵３０ＣＫＥＹ、暗号化データ復号用実行環境３０ＣＶＭ（実行部３０ＣＶＭ）を用い、
改竄耐性を有する暗号文・平文混合のデータ３０ＤＬＲ―ＤＡＴＡの暗号化データ本体３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹを復号し実行させる系を説明図として開示する。
●台帳記録部３０ＤＬＲに含まれる暗号化データ本体３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹは、図３Ａ・図３Ｂのように、３０ＤＬＲの中から暗号データと平文データを区別・識別・認識できる部分・手段を備えさせ、鍵により暗号化処理・復号処理を行えると好ましい

。
●図３Ｂはサーバ３Ｃがユーザ端末となり３０ＣＶＭや３０ＣＶＭＵを備え、ユーザ端末に暗号化データを用いたサービスを提供する場合の説明図であって、
図４Ａ、図４Ｂ、図４Ｃは暗号データと平文データを含む分散型台帳の記録部３０ＤＬＲ（ブロックチェーン式記録部３０ＤＬＲ）と第２の実行部３０ＣＶＭＵにてワンタイムパスワード認証を行う場合の説明図である。
（ユーザ端末１Ａと、インターネットがオフラインでも動作するサーバ端末３Ｄとを直接接続する経路２０―１Ａ３Ｄで接続されてもよい。前記経路２０―１Ａ３Ｄは有線式・接触式でも無線式・非接触式でもよい）
【００１９】
＜図１から図２＞
図１には、（１）ユーザ端末１Ａ内の３０ＣＶＭ、３０ＣＶＭＵにてＤＬＲ３０から読み取った暗号化データを復号する場合（図１Ａの左側ユーザ端末内の３０ＣＶＭＵ、ユーザインターフェース３０ＵＩ）と、（２）サーバ３Ｃ、３Ｄ内の０ＣＶＭ、３０ＣＶＭＵにてＤＬＲ３０から読み取った暗号化データを復号する場合（図１Ａの中央、サーバ部）と、が記載されている。
図１Ａはノード３Ａに平文対応の第１実行部ＰＶＭと暗号化対応の第２実行部３０ＣＶＭが含まれる例である。
図１Ｂはユーザ端末１Ａに第２実行部３０ＣＶＭＵが含まれる例である。
図２は本願で用いるコンピュータの説明図とコンピュータの接続図である。
【００２０】
＜図３Ａと図３Ｂ＞
図３Ａはブロックチェーン式記録部３０ＤＬＲに記録された、データ３０ＤＬＲ―ＤＡＴＡから、暗号化データ３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹを識別する部分３０ＤＬＲ－ＣＤＡＴＡ－ＰＳ（暗号化データの開始部）や３０ＤＬＲ－ＣＤＡＴＡ－ＰＥ（暗号化データの終了部）についての説明図である。
図３Ａと図３Ｂは前記識別する部分を用いて、平文と暗号文の混合したデータ３０ＤＬＲ―ＤＡＴＡから暗号化データを読み取り、第２実行部３０ＣＶＭ・３０ＣＶＭＵに復号させ、復号後のデータを利用又はプログラム実行させる説明図である。本願のコンピュータシステムは暗号化データに前記識別する部分が付与されていてもよい。
図３Ｂの３０ＤＬＲ－ＤＡＴＡ復号部Ｆ３Ｂ３は、ＤＬＳの台帳記録部３０ＤＬＲの暗号化データでも平文データでもよい（暗号化データと平文データの混合したデータ）３０ＤＬＲ―ＤＡＴＡを、データ入力処理部Ｆ３Ｂ１にて入力し、続いて入力データ解析部Ｆ３Ｂ２　（暗号データの識別部・選択部・認識部Ｆ３Ｂ２　）にて暗号データ本体３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹを検出するための識別部分３０ＤＬＲ－ＣＤＡＴＡ－ＰＳや３０ＤＬＲ－ＣＤＡＴＡ－ＰＥ検出し、前記暗号データ本体のデータ部分・範囲を検出する。
【００２１】
※この方法のほかに、予めスマートコントラクトで３０ＤＬＲに順次暗号化データを格納記録する配列・マッピング型・構造体などを形成し、それを暗号化データの記録場所として設定し、ＥＣＭＡＳｃｒｉｐｔとＤＬＳアクセス用ＡＰＩ（３０ＣＶＭＵ－Ｗ３Ｊ）にて前記暗号データの格納された配列・マッピング型・構造体等から暗号データを呼び出してもよく、その場合でも、暗号化データの配列・マッピングなど型や変数を定義している部分が平文データと暗号化データを区別・認識・識別する部分３０ＤＬＲ－ＣＤＡＴＡ－ＰＳ・３０ＤＬＲ－ＣＤＡＴＡ－ＰＥと同等である。
・本願では暗号化データ本体３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹを平文データ（或いは復号鍵Ｂによる暗号化データ）と暗号化データ（或いは復号鍵Ａによる暗号化データ）の混合した３０ＤＬＲから区別・認識・識別する手段を備えさせる事が好ましい。
・平文または暗号化鍵の鍵データの異なる暗号化データ間で復号したい暗号化データを識別できる部分があると好ましい。

※平文データがなく、格納された暗号化データがいくつかの復号鍵で暗号化されている３０ＤＬＲであっても、暗号化鍵が異なるデータ同士を区別する識別子３０ＤＬＲ－ＣＤＡＴＡ－ＰＳ等があると好ましい。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【００２２】

●※発明者としてはスマートコントラクトをデプロイしたユーザ識別子（３０ＤＬＲ―ＣＤＡＴＡ－ＡＤＤＲＥＳＳ）の形で３０ＤＬＲの或るブロックデータのコントラクトに記録し、ブロックチェーンエクスプローラーなどでコントラクトを検索できると好ましいと考えている。

●例えば３０ＤＬＲを用いてＳＮＳサービスを提供したい法人Ｓがあって、その企業が公的機関などへ登録したコントラクトアドレス３０ＤＬＲ―ＣＤＡＴＡ－ＡＤＤＲＥＳＳがあって、そのコントラクトアドレスで暗号化データを格納する配列等を記録するようにし、３０ＤＬＲのコントラクト内部で記録されるユーザ識別子等やユーザのコミュニケーション内容・コンテンツは前記法人Ｓが管理する暗号化鍵・復号鍵とウェブアプリ型実行部３０ＣＶＭＵで暗号化・復号されユーザにＳＮＳのコンテンツとして提供されうる。

（ＳＮＳアプリのデータ処理の動作図は図３Ｂや図３Ｃ、図１，図１Ｂ、ＯＴＰ認証サービスのＯＴＰ計算部など処理部をＳＮＳサービス用の処理部とした図４Ａ、図４Ｂ、図４ＣをSNS用の処理部記憶部にした形で説明される。ブロックチェーン部には図５等に示すブロックデータを削除できる台帳記録部３０ＤＬＲ２を用いてもよい。）

該コントラクトアドレスのコントラクトに含まれるデータやＳＮＳサービスで事件・紛争等があった場合には、コントラクトアドレス３０ＤＬＲ―ＣＤＡＴＡ－ＡＤＤＲＥＳＳをデプロイした法人Ｓは管理する暗号化鍵・復号鍵とウェブアプリ型実行部３０ＣＶＭＵを捜査当局等に開示し、暗号化データを復号して捜査当局等に開示して、事件・紛争の解決に取り組む事ができうる。

●前記ＳＮＳを捜査当局等への開示の例で述べたが、銀行サービス・証券系サービス、金融サービスや、コントラクトを利用するゲームサービス等においても、事件・紛争等には同様に開示して対応する事が考えられる。（コントラクトデプロイをした法人が鍵やアプリを管理する。）

【００２３】

●防犯のため、実行部３０ＣＶＭＵと後述の図５のブロックチェーン記録部３０ＤＬＲ２と併用して、認証された個人や法人のユーザ識別子による暗号化データを含むコントラクトアドレスであるときは台帳にデータを保持し残すようにして、

認証されていないユーザ識別子による暗号化データを含むコントラクトは、ノードのクライアントソフトウェア・仮想機械部がデプロイを受け付けないようにし、（若しくはデプロイされた暗号化データブロックを削除し、）暗号化データの利用を制限するブロックチェーンシステムも利用されうる。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【００２４】

※暗号化する場合でも、その代表者のアドレス（例えばＮＦＴの発行・送信・取引が行われる取引所の取引データを含むコントラクトアドレス）などがトランザクションに添付されていると好ましい。すべてのトランザクションデータを暗号文にて送信されると記録部３０ＤＬＲの透明性（又は外部から台帳の内容を把握・調査・監査ができる性質）がゼロになる恐れがある。

※送信者ユーザ識別子情報の後に暗号化データを配置し、誰が秘密にしたデータか指定するなどし、発行者が例えば認証された会社のアドレスならそのあとに続く暗号データは実行してもウイルスなどでないかもしれない。

※ブロックチェーン上のデータを、異なるプログラム言語に基づいて条件分けして実行するためにデータに識別子を付与する事に関する特許はＵＳ２０２１００４２１３７があり、スマコンの実行コードの先頭に０１や０３の形でＥＶＭやＣ言語実行環境を示す、米国特許例がある。本願では暗号化データ本体の前部分等に暗号データと区別するための識別

子・データを付与している。
－－－－－－－－－－－－－－－－－－－－－－－－－
【００２５】
●データ実行部Ｆ３Ｂ１３は、復号されたデータＦ３Ｂ９を記憶部Ｆ３Ｂ１０に記憶し、処理部Ｆ３Ｂ１１にて処理し処理後の情報を前記記憶部に記憶し若しくは処理結果・応答Ｆ３Ｂ１２として出力する。出力処理部Ｆ３Ｂ１４を介して外部へ出力される。出力先はユーザ端末１Ａやサーバ３Ｃ等、あるいはブロックチェーンノード端末の記録部３０ＤＬＲである。
●データ実行部Ｆ３Ｂ１３は、暗号化データの復号とプログラムの実行時に、サンドボックス等復号後のデータに含まれうるウイルスの動作に対応し、ウイルスを隔離・停止などできる対策部分を含む耐ウイルス型実行部Ｆ３Ｂ８に含まれていると好ましい。（３０ＤＬＲ－ＣＤＡＴＡ復号部Ｆ３Ｂ３等もＦ３Ｂ８に含まれていてよい。３０ＣＶＭや３０ＣＶＭＵが耐ウイルス型実行部Ｆ３Ｂ８に含まれていてもよい。）
●処理結果・応答Ｆ３Ｂ１２の例は、１．戻り値を返す（例：復号化された実行データに含まれる、スマートコントラクトに従い計算した動的コードを端末１Ａに出力）、２．処理に関連する関数や変数を、他のブロック番号の３０ＤＬＲーＣＤＡＴＡから呼出・計算に使用、３．３０ＤＬＲへトランザクション送信、分散型台帳システム／ブロックチェーンにトランザクションを送信、ブロックに平文／暗号文データを連結、４．その他仮想機械・実行環境での実行後処理、である。
●実行部３０CVM・３０CVMUに暗号化する暗号化部分Ｆ３Ｂ１５を備えさせ、処理結果・応答Ｆ３Ｂ１２を、Ｆ３Ｂ１５にて暗号化し、前記暗号化データをユーザ端末１Ａ、サーバ３Ｃ等、ノード３Ａの３０ＤＬＲへ出力してもよい。
【００２６】
図３Ｃは図３Ｂの構成で、サービス（ＯＴＰ認証等）を行うサーバ端末３Ｃの説明図である。（ユーザ端末に実行部３０ＣＶＭ・３０ＣＶＭＵは無く、ユーザ端末と通信可能なサーバ３Ｃに実行部３０ＣＶＭが含まれる構成である。）（若しくはユーザ端末はサービス用サーバである場合。）
●実行環境３０ＰＶＭがバックエンド部（ウェブサーバ端末３Ｃや端末３Ｄ）に含まれており、ユーザ端末１Ａは端末３Ｃや３Ｄにアクセスし、ユーザ端末１Ａは前記３Ｃや３Ｄの送信するウェブページやＥＣＭＡＳｃｒｉｐｔの手続きに従うか、又はサーバ３Ｃ・３Ｄの内部で実行される実行部３０ＣＶＭＵ・３０ＣＶＭに対し、ユーザ端末１Ａが入力や要求を行い、３Ｃ・３Ｄが処理をし、その結果をユーザ端末１Ａ上に表示・利用させる例が図３Ｃである。
●スマートコントラクト提供部フロントエンドＦ３Ｃ１。［例：スマコン式ＯＴＰ認証と認証後サービスのウェブアプリフロントエンド部と実行部３０ＣＶＭ（実行部をユーザにダウンロードさせる場合実行部３０ＣＶＭＵ）］、
前記Ｆ３Ｃ１はウェブページ・ウェブアプリのフロントエンド部、ＨＴＭＬ５＋ＥＣＭＡＳｃｒｉｐｔ部でよい。（所謂ウェブページの部分）
ユーザのインターフェースとなり、ユーザ要求に従いブロックチェーン部３０ＤＬＲやノード３Ａとの通信の要求を受け付ける。例えばＯＴＰコードの生成要求や、ＯＴＰコードの入力を受け認証を行う要求を受ける。
●３０ＣＶＭ管理部Ｆ３Ｃ３（端末１Ａの指示に応じて３０ＤＬＲを書換・読取する部分。バックエンド部）はユーザー端末１Ａにはアクセス手段が無く（又は一般ユーザからのアクセスを防ぐため意図的にＡＰＩ等が公開されていない等、アクセス者を指定・限定している等で）、通常はアクセスできないDLSやブロックチェーン３０ＤＬＲに、アクセスできるサーバー３Ｃサイドの処理部であり、３Ｃがアクセスできるノード３Ａが設置されている時、前記３Ａの３０ＤＬＲへ３Ｃはアクセスし暗号データを含むデータを読取し、又は３０ＤＬＲへデータを書き込みする。
●３０１Ｃは３Ｃの実施するサービス用プログラム及び記録部、３１１Ｃは３Ｃのサービス処理部である。３０ＤＬＲ—Ｃは３０ＤＬＲから３Ｃが読取し記憶したデータである。

Ｆ３Ｃ５はブロックチェーンとアクセスを可能にするプログラム部である。（クライアントソフトウェア（ノード通信部）も可能）３CがノードＳAと同じくDLSの一部となってもよい。
●Ｆ３Ｃ４　は鍵データ・鍵管理部（耐タンパ性を持つ記憶域可）である。
【００２７】
図１Ａにおいては、サーバ３Ａ内の３０ＣＶＭにてＤＬＲ３０から読み取った暗号化データを復号する構成が記載されている。（サーバ３Ａは３０ＰＶＭを備えてもよい。）
図１Ｂにおいては、ユーザ端末に備えさせた実行環境３０ＣＶＭＵ（仮想機械３０ＣＶＭＵ）と平文読み取り仮想機械ＰＶＭによる暗号データを含むブロックデータからの暗号データの読み取り・復号・データ実行・戻り値生成・データの台帳への書き込みの説明する。
【００２８】
図１Ｂの発展形・実施例として、本願図４Ｂの説明図では、ユーザ端末にウェブアプリ実行部３０ＣＶＭＵ－ＡＰＰ（ウェブブラウザの処理部・記憶部）が記憶され、３０ＣＶＭＵ－ＡＰＰによる処理部３１ＣＶＭＵ－ＡＰＰがユーザ端末に備えられているときに、該処理部３０ＣＶＭＵ－ＡＰＰが３０ＤＬＲからデータを読み取り、暗号化データについては復号鍵Ｆ４Ｂ－９を用いて復号を行い復号後のデータＦ４Ｂ－１１を得て、平文データＦ４Ｂ－１２と、復号後のデータＦ４Ｂ－１１をＯＴＰ計算部Ｆ４Ｂ－１５に入力し、ＯＴＰ計算をさせる事を主張する。
図４ＢではＯＴＰを計算後生成し記録手段や記憶装置に記憶・記録させ、図４Ｃでは入力されたＯＴＰを検証し認証する処理の実行部を開示する。
【００２９】
＜課題２：ブロックチェーンにおいて或る設定時間後の過去のデータブロックを削除しつつブロックチェーンの連続性を検証できるデータ構造＞
第１（３０ＤＬＲ２－１ＳＴ）と第２（３０ＤＬＲ２－２ＮＤ）のブロックチェーンについて、第２のブロックチェーンに第１のブロックチェーンのブロックのハッシュ値が含まれていることで、第１のブロックチェーンのブロックが削除されていても、前記ハッシュ値を含む第２のブロックチェーンによって、ブロックチェーンの連続性を検証可能にする事も提案する。
【００３０】
図５の（ａ）と（ｂ）は、第１（３０ＤＬＲ２－１ＳＴ）と第２（３０ＤＬＲ２－２ＮＤ）のブロックチェーンについて、第２のブロックチェーンに第１のブロックチェーンのブロックのハッシュ値が含まれていることで、第１のブロックチェーンのブロックが削除されていても、前記ハッシュ値を含む第２のブロックチェーンによって、ブロックチェーンの連続性を検証可能にする事の説明図。
図５の（ｃ）は前記第１と第２のブロックチェーンに加え第３のブロックチェーンを備え（あるいは第３、第４、第５、・・・第ｎのブロックチェーンを備え）互いにハッシュ値共有部（３０ＤＬＲーＳＨＡ、３０ＤＬＲーＳＨＡーｎ・・・等）を有するときの説明図である。
【００３１】
※前記台帳記録部３０ＤＬＲ２は図５の（ｂ）のように、ブロックを連結する間隔の短い（例：５秒毎）第１のブロックチェーン（３０ＤＬＲ２－１ＳＴ）と、ブロックを連結する間隔の長い（例：５０分毎）第２のブロックチェーン（３０ＤＬＲ２－２ＮＤ）を含む台帳記録部３０ＤＬＲ２があるとき、
第１のブロックチェーンにおいて設定された個数（例：５０分÷５秒＝３００個、ｍ＝３００）のデータブロック群（例えばデータブロックａｎがａ３０１からａ６００までの時）について、
第２のブロックチェーンのデータブロックｓＡｎ（ここでは例としてｓＡ２）を形成し前記第２のブロックチェーンのデータブロックに設定された個数（例：３００個）の各データブロックのハッシュ値をｓＡｎ（ここではｓＡ２）に格納し、

前記データブロックｓＡｎのハッシュ値ｓＡｎｈ（ここではｓＡ２ｈ）を次のデータブロックｓＡ（ｎ＋１）（ここではｓＡ３）に格納しつつ、
第１のブロックチェーンにおいてデータブロックに設定された個数（例：３００個、ａ６０１からａ９００までの個数）を連結してを繰り返す。
（第１と第２のブロックチェーン其々のブロックを紙のページブロックで表現したときに、契約書の契印（実際はハッシュ値、ダイジェスト、フィンガープリント、特徴データ）を其々のブロックの境目に押印した形式をとる。）
【００３２】
＜第２ブロックチェーンのブロックハッシュ値の第１ブロックチェーンのブロックへの格納［第ｎブロックチェーンのブロックハッシュ値の第（ｎ－１）ブロックチェーンのブロックへの格納］＞
図５の（ｂ）のデータブロックａ４では、前の第１のブロックチェーンのデータブロックａ３のハッシュ値ａ３ｈに加え、第２チェーンの前のブロックｓＡ１のハッシュ値ｓＡ１ｈをデータブロックａ４に格納・組込・取り入れてよい、又は取り入れることができる。

（第ｎブロックチェーンのブロックハッシュ値の第（ｎ－１）ブロックチェーンのブロックへの格納してよい。）
第１のブロックチェーンのデータブロックａ４に第２のブロックチェーンのハッシュ値ｓＡ１ｈを組み込むことで、第１のブロックチェーンのデータブロックは第２のブロックチェーン内のデータを反映（又はデータがリンク）できる。
若しくはハッシュ値を組み込むことで第１と第２のハッシュ値の出方が相互に変わり、データが絡み合うようにできる。第１と第２のブロックチェーンの要素が相互結びつく。
・（第１のチェーンの用いるハッシュ関数と、取り込ませたデータブロックと、連結順序がわかるとき、ブロックチェーンの各ブロックに現れるハッシュ値は推測されうる。
しかし、第２のチェーンのブロックのハッシュ値を第１のチェーンに組み込むと（フィードバックするように組み込むと）第１のチェーンに新規の要素（第２のチェーン要素）が追加され、ブロックチェーンの各ブロックに現れるハッシュ値は推測しにくくなるかもしれない。）
【発明の効果】
【００３３】
＜図１、図４Ｂ等に記載の暗号化データの実行環境３０ＣＶＭ＞
１－１．スマートコントラクト内部に平文データと暗号化データを混在して記録させ、読取・実行・書込ができる。その結果ＯＴＰ計算用キー変数やユーザ識別子など秘匿化したい情報を秘匿化できる。
１－２．例えばトークン、ＮＦＴを異なるユーザ識別子の間で取引する際に暗号化して取引できる。（但し復号鍵を利用可能な実行環境３０ＣＶＭ・３０ＣＶＭＵを持つサーバ３Ｃ、ユーザ端末１Ａが必要）
或るユーザの或るトークンを、ユーザ識別子から除去し別のユーザ識別子に付与する管理者（振替機関）が存在する場合のトークンの保管振替をする場合にもユーザ識別子の秘匿化ができる。
１－３．ソーシャルネットワーキングサービス等に用いる場合、ユーザ間でのコメントに秘匿すべきデータがある場合は隠せる。
【００３４】
＜図５等に記載のブロックチェーンのデータ構造３０ＤＬＲ２＞
２－１．第１のブロックチェーンに含まれる需要のあるブロックのみを残して、需要が少ない又はデータブロックに個人情報が平文のまま含まれるなどして削除要請のある場合に該当するデータブロックを削除又は磁気テープなど外部記憶装置にアーカイブしてノード端末３Ａから取り除きつつ、第２のブロックチェーンの存在により第１および第２のジェネシスブロックからのデータブロック間の連続性を検証できる効果が生じるかもしれない。

２－２．　図５等に記載の第１・第２のブロックチェーンを持つデータ構造３０ＤＬＲ２は、コンテンツの記録に用いられるかもしれない。
例えば、ソーシャルネットワーキングサービス等で、ユーザ間でのコメントなどのやり取りを台帳に記録させていく際に、既存の台帳記録部３０ＤＬＲでは一部ブロックデータを忘れさせるとチェーンの連続性が検証できなくなるかしれないが、
本願図５の３０ＤＬＲ２では一部データを削除したり忘れさせてもチェーンの連続性を検証できシステムは動作を継続できる。
ソーシャルネットワーキングサービスＳＮＳ等で、事情によりユーザ間でのコメントの削除が必要な場合、ノード端末３Ａの３０ＤＬＲ２のクライアントソフトウェアに削除すべきコメントの含まれるデータブロックを削除可能になる。
２－３．図５等に記載の第１・第２のブロックチェーンを持つデータ構造は、分散型台帳システムのほかに、学習データを最新のデータブロックに格納し学習しつつ、指定した条件に該当するデータブロックを忘れることのできる、機械学習を行う人工知能システム・人工知能の学習データの記録部・データベース部に利用できうる。図９はその説明図である。
【００３５】
・図９の例ではデータセット・学習方法・処理部が改竄耐性や透明さをもったＡＩにつながる。
・また過去に学習したことを忘れたり、過去に学習したことと同じことであると判定する記憶部・処理部・コンピュータシステムの構築につながる。（機械学習のプロセス／データ／モデル作成方法などを透明化する必要性がある場合にブロックチェーンの利用が提案される。
・そしてブロックチェーンを利用する場合に、人工知能システムが稼働する限り、学習データを（シングルチェーン式である）従来のブロックチェーン部３０ＤＬＲに取り込み続けてデータ量が増加し続けてしまうが、本願提案の３０ＤＬＲ２であれば重複するデータや時間経過したデータ、需要のないデータのブロックは削除でき、人工知能ＡＩを搭載したコンピュータ・装置、ロボット、家電等、生産機械等、輸送機器等の記憶域・記憶量低減に役立つかもしれない）
・ブロックチェーンのジェネシスブロックから次々にデータブロックに学習データを学んでいったＡＩは、その学びの工程を、ブロックチェーンのデータブロックから第三者が解析できる。どのように学習させれば再現性のあるＡＩになるかのＡＩの学習・成長・動作の解析に役立つかもしれない。
【００３６】
＜図９の説明＞
●図９の３０ＤＬＲ２には人工知能システム４である自動車４ＣＡＲの入力装置１０４により入力元４ＩＮをセンシングあるいは取得したデータ（若しくは、通信装置１０２により得たデータ。前記装置１０２がネットワーク２０に接続されているときインターネットを介して他の電子計算機端末と通信を行い得たデータを含む）が３０ＤＬＲ２のデータブロックに図５（図５から図８）のように記録される。
その後、記憶部と処理部は入力元４ＩＮやその他設定されたデータ・学習データ等に基づき、人工知能としての応答を出力結果４ＯＵＴとして、出力装置１０５や通信装置１０２を用いて行う。
【００３７】
●機械学習ソフトウェア部３０ＳＴＵＤＹと、機械学習処理部３１ＳＴＵＤＹに従って機械学習を行う。学習データは３０ＤＬＲ２に記録する。
●学習データの各ブロックのデータ需要記録部３０ＤＥＭＡＮＤに各データブロックの利用頻度を記録する。例：データブロックやデータブロック内のコントラクトアドレスに帰属する関数等トランザクションが呼ばれた数等。（需要記録部に改竄耐性が必要な場合、需要記録部３０ＤＥＭＡＮＤはブロックチェーン構造を持つ記録部に記録してもよい）
※前記部分（図９の機械学習ソフトウェア部３０ＳＴＵＤＹと、機械学習処理部３１ＳＴ

ＵＤＹ、３０ＤＥＭＡＮＤ、３１ＤＥＭＡＮＤ－ＦＯＲＧＥＴ等）は例えばヒトの頭脳で刺激を受け記憶した情報に関連する部分（生物の特徴を機械にて模倣しようとする部分）である。ヒトやサルなど生物がよく覚えるように回数を重ねトレーニングしたとき（或いは恐怖を覚え強い刺激を受け記憶したとき、欲求に従い強い刺激を受け記憶した等のとき）に脳が刺激を得てその事柄を強く記憶させるような処理部を、コンピュータで再現しようとする処理部・記憶部・ソフトウェア部である。（また需要がない・時間経過したがデータ利用のないデータブロックを忘れようとする部分である。）

●学習データを需要によって保存または削除する処理部３１ＤＥＭＡＮＤーＦＯＲＧＥＴは、需要記録部３０ＤＥＭＡＮＤ又は削除すべき・忘れるべきデータの記録部３０ＤＥＭＡＮＤを用い、削除又は忘れるべきデータブロックを記憶装置から削除する。

●前記データの記録部３０ＤＥＭＡＮＤは、データブロックの利用頻度情報の他に、例えば人工知能システム４の管理者が削除すべきであると判断する情報（例：個人情報、プライバシー情報）や管理者が指定する年数・時間を経過した情報でもよい。

（本願では古くなったデータブロックの削除を行い、ヒトが時間経過により記憶したことを忘れる現象や、睡眠時に記憶の整理をする現象をコンピュータにて再現しようとする。）

【００３８】

●図９の用例ではブロックの連結はシステムの制御部で行われる。分散型台帳システムの複数サーバ群が投票等の工程を得て合意形成する図１や図２の場合とは異なる。

・１個体のロボットや無人機、ドローン、自動車・飛行機・輸送機器の記憶装置に３０ＤＬＲ２を含む場合を図９に記載している。

・例えばオフラインになるかもしれない自動車の人工知能システム４ＣＡＲがあって、４ＣＡＲには機械学習のための処理部と記憶部、入出力装置、通信装置があって、記憶部に３０ＤＬＲ２を備えさせる場合は、ＤＬＳのようなネットワーク２０を介した合意形成は無くてもよい。（但し複数のノード４ＳＥＶＥＲからなるコンピュータネットワークシステムを人工知能システム４とする場合、ブロックチェーン部３０ＤＬＲ２においてブロックデータの連結のための合意形成・コンセンサスに関する処理部・機能部は必要である。）

【００３９】

＜第１・第２（第ｎ）のブロックチェーンに記録されるハッシュ値ａｎｈ、ｓＡｎｈとデータブロックを要約する値ａｎｈ、ｓＡｎｈについて＞

●図５（ｂ）の例では３０ＤＬＲ２－１ＳＴの３つ分のブロックハッシュを３０ＤＬＲ２－２ＮＤの１ブロックに格納する。前記３つ（整数ｍ＝３）に限定せず、所定の整数ｍを（ブロックチェーンのクライアントソフト、ノード用ソフト３０ＤＬＳＣ）に設定し、又はノード端末間の投票により前記整数ｍを決定し、３０ＤＬＲ２－１ＳＴの前記ｍ個のブロックハッシュを３０ＤＬＲ２－２ＮＤの１ブロックに格納してよい。

※例えばｍ＝１００とし、ｍを１つ増やすための時間（Ａｎが１ブロック増加するための時間）が５秒であれば、ｍ＝１００の条件は、５００秒分の時間にａｎに連結された時に、計１００個の各ブロックデータのハッシュ値をｓＡｎの１つのデータブロックに格納し第２のブロックチェーンに連結する。

※Ａｎについて前記ｍを１つ増やすための時間が５秒のとき、１０時間ごとにｓＡｎを増やす場合はｍ＝７２００で、後述の図１０の用途において１０時間ごとに残高の控えをｓＡｎに取る系では１ブロックに７２００個の各ブロックハッシュ値と、その区間でのユーザーの残高の終値を記憶する。（トランザクションのあった全ユーザの最新の残高を記憶してよい）

【００４０】

●図５（ｂ）のブロックチェーンに記録されるハッシュ値ａｎｈ・ｓＡｎｈはデータブロックａｎ・ｓＡｎを基にしてハッシュ関数に入力して得る。

前記ハッシュ値ａｎｈ・ｓＡｎｈはデータブロックａｎ・ｓＡｎを要約したものであり、ａｎｈ・ｓＡｎｈはデータブロックａｎ・ｓＡｎを要約したデータである。

●図５（ｂ）のａｎｈ・ｓＡｎｈはデータブロックａｎ・ｓＡｎの特徴を表す（特徴を要約した）フィンガープリントデータ又は要約データ又は特徴データａｎｄ・ｓＡｎｄを含んでよく、特徴抽出プログラムを用いて、対象となるコンテンツから前記特徴データを抽出しａｎｈ・ｓＡｎｈとともにデータブロックに保存・記録してもよい。（例えば図５（ｂ）のａ４に記録されたａ３のハッシュ値ａ３ｈとａ３の特徴データａ３ｄ。）
［※特徴抽出プログラムを用いて、対象となるコンテンツから前記特徴データを抽出し、前記特徴データを用いて動画サイト・動画閲覧サービスで提供とする動画データ内に違法なコンテンツを検出する事は公知である。（例：ＮＴＴデータ社のサービスｈｔｔｐｓ：／／ｗｗｗ．ｎｔｔｄａｔａ．ｃｏｍ／ｊｐ／ｊａ／ｎｅｗｓ／ｒｅｌｅａｓｅ／２０１０／０８１６００／　２０２２年１０月１６日閲覧、インターネット）］
（ａｎｄ・ｓＡｎｄがハッシュ値と同等に改ざん検知に利用可能なデータならばそれをハッシュ値ａｎｈ・ｓＡｎｈの代わりに用いることも考えられる。）

【００４１】

●データブロックには機械学習に必要なデータが格納されうる。
・教師あり学習における学習データと学習データに対応する人間が付けた正解のラベルデータ・アノテーションが含まれていてもよい。
・教師なし学習で用いる学習データと、学習データに正解を与えず特徴量や規則性や相関性、特徴、特異性、傾向等を解析させる処理手続き・プログラムが含まれていてよい。該処理手続き・学習データには自然界の法則（物理法則、自然科学の法則）を記憶させていてもよい。ヒトや社会に関する内容、例えば各国の法令、法令を守るための処理手続き等、機械が人間の社会であっても守るべきデータを記憶させていてもよい。（例えば取り扱えない画像については黒塗りにする処理手続き等）

【００４２】

●コンテンツは音声データと映像データが含まれうる。センサにより学習元４ＩＮをセンシングしたデータも含まれうる。
特に図９の利用例で自動車４ＣＡＲや無人機４ＤＲＯＮＥ、ロボット４ＲＯＢＯＴが３０ＤＬＲ２を用いる場合、特徴データＡｎｄ・ｓＡｎｄを特徴抽出プログラムを用いて、４ＣＡＲ等の移動時に外界（道路上を歩く人々の振る舞い、自動車や自転車の走行状況、道路上の音声）をカメラ又はセンサで撮影・センシングした動画データ・センシングデータから前記特徴データを抽出しａｎｈ・ｓＡｎｈとともにデータブロックに保存・記録してもよい。
そして前記記録したデータを３０ＳＴＵＤＹ、３１ＳＴＵＤＹを用いて機械学習を行い、学習後に保存すべきデータが生じた場合は３０ＤＬＲ２に記憶する。
人工知能システム４でもある自動車４ＣＡＲ等は機械学習を行いながら、４の外部の系である学習先４ＩＮをセンシングし、３０ＤＬＲ２に記憶された情報をもとに、応答４ＯＵＴを行う。

【００４３】

＜図１０の説明＞
※トランザクションデータ、アドレス型データ、未使用トランザクションアウトプットＵＴＸＯデータ（インプットデータ・アウトプットデータ）を第１のブロックチェーンデータに格納し、前記第１のブロックチェーンデータと第２のブロックチェーンの最新ブロック時点でのアカウント・口座型データを第２のブロックチェーンの最新のブロックｓＡｎ（図ではｓＡ２）に格納する場合を図１０に示す。第２のブロックチェーンのハッシュ値を格納する第３（第ｎ）のブロックチェーンを備えてもよい。

【００４４】

＜ブロックチェーン以外の３０ＤＬＲ＞
●本願で主張する図１や図４Ｂや図４Ｃ等で主張する実行環境３０ＣＶＵを用い、分散型台帳の記録部３０ＤＬＲの記録内容の一部を暗号化し復号して利用する場合、３０ＤＬＲはブロックチェーンによる方式のほか、非対称暗号と暗号的にリンクされたデータブロックを用いてもよい。有向非巡回グラフ等のデータブロック・データのまとまりが連結され

ている有向グラフであってもよい。
●図５の（ｂ）に記載の、第１のブロックチェーンと第２のブロックチェーン（及び必要によっては第３、第ｎのブロックチェーンを持つデータ構造・データ構造体）の概念を考慮すると、３０ＤＬＲ２の第１のブロックチェーンがブロックチェーンでないデータ構造体の場合（例えば非対称暗号と暗号的にリンクされたデータブロック、有向グラフ、有向非巡回グラフであるデータ構造体ａｎの場合）、３０ＤＬＲ２がある時間にｍ個連結されたデータブロックのハッシュ値・要約値・フィンガープリント・特徴データを格納する別途形成される別のデータ構造体ｓＡｎを含みうる。
【００４５】
＜図面説明＞
＜図１＞分散型台帳の記録部の暗号データについて復号を行いプログラムを実行するプログラム実行部３０ＣＶＭ・３０ＣＶＭＵの説明図
＜図１Ａ＞ユーザー端末アクセスを受けて、実行環境３０ＣＶＭ（仮想機械３０ＣＶＭ）と平文読み取り仮想機械ＰＶＭが台帳データ部３０ＤＬＲにアクセス可能であって、前記３０ＣＶＭが暗号化データを含むブロックデータの暗号化データを復号しスマートコントラクトとして実行することを示す説明図（前記平文読み取り仮想機械ＰＶＭはイーサリアムにおけるＥＶＭが実現されている例）
（もしくは、図１Ａは２つのスマートコントラクトを実行するための仮想機械を含むシステムの説明図。前記２つの仮想機械のうち、片方は平文をブロックチェーン部に書き込みする仮想機械ＰＶＭであり、他方は暗号化されたデータをブロックチェーン部に書き込む仮想機械ＣＶＭである。）（図１Ａのシステムはブロックチェーン部について通常は仮想機械ＰＶＭにより他社からも平文や暗号化されたデータを読みだせる。暗号化データを復号して読み取るには仮想機械ＣＶＭに暗号データの復号鍵を入力等して閲覧する）
図中のＢＤＣｎ：暗号化・符号化・秘匿化されたデータを含むデータ、データブロック、トランザクション（ｎは整数）、ＢＤＰｎ：平文データを含むデータ等（ｎは整数）
＜図１Ｂ＞実行環境３０ＣＶＭＵ（仮想機械３０ＣＶＭＵ）と平文読み取り仮想機械ＰＶＭによる暗号データを含むブロックデータからの暗号データの読み取り・復号・データ実行・戻り値生成・データの台帳への書き込みの説明図
（または、図１Ｂは図１Ａの場面でユーザ端末に仮想機械ＣＶＭ類似機能を含む場合の説明図。図１Ａのシステムで仮想機械ＰＶＭにて暗号化したデータをブロックチェーンに書き込み、その後利用したいときに仮想機械ＰＶＭにて暗号化データをブロックチェーンからそのまま読み取り、ユーザ端末に暗号化されたスマートコントラクトを含む暗号データを一時記録させたのち、ユーザ端末に搭載された暗号化データ復号部とスマートコントラクト実行部を用いてスマートコントラクトを実行してもよい。）
＜図２＞本願で用いるコンピュータとコンピュータネットワークの例
＜図３Ａ＞暗号化データを含むデータ３０ＤＬＲ―ＤＡＴＡ内の、暗号化データ本体３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹ及びその付属データと暗号化の開始部分３０ＤＬＲ―ＣＤＡＴＡ―ＰＳと終了部分３０ＤＬＲ―ＣＤＡＴＡ―ＰＥの説明図（暗号化データ３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹを３０ＤＬＲから選択・識別・区別し選び取るための部分の説明図）
＜図３Ｂ＞暗号化データ３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹを３０ＤＬＲから選択・識別・区別し選び取るための部分の説明図
＜図３Ｃ＞サービス提供サーバ３Ｃ（例えばＯＴＰ認証のＯＴＰ生成・認証や認証後のサービスを提供するサーバ３Ｃ）とユーザ端末１Ａとノード端末３Ａ（３Ａの３０ＤＬＲ）は、ユーザ端末１Ａの要求によって、３Ｃが３Ａから得た暗号化データを復号し、ＯＴＰ認証などのサービスを提供する場合の説明図
＜図４Ａ＞ウェブアプリ式実行部３０ＣＶＭＵによるＯＴＰ認証時の電子計算機接続図
※２０―１Ａ３Ｄはインターネットのような通信経路２０が使えず、ユーザ端末１Ａがオフライン対応型認証端末３Ｄと通信したいときの通信経路２０―１Ａ３Ｄ（有線式・無線式の通信経路）

＜図４Ｂ＞ウェブアプリ式実行部３０ＣＶＭＵによるＯＴＰ認証時のＯＴＰ生成・計算に関する本願の実施例
１．ウェブページ・ウェブアプリのサービスを行うサーバ端末３Ｃ・３Ｄが、
ユーザ端末１ＡにＯＴＰ計算アルゴリズムを含むＯＴＰ生成ソフトウェアつきウェブページ・アプリ３０ＣＶＭＵ－ＡＰＰを送付し、
２．ユーザ端末は３０ＣＶＭＵ－ＡＰＰを受け取り、記憶し、実行し、
３．３０ＣＶＭＵ－ＡＰＰはユーザの３０ＤＬＲにアクセスする秘密鍵情報Ｆ４Ｂ－２や、秘密鍵を用いた署名処理と、ユーザの持つトークン番号（ＯＴＰトークンの個体番号）及びその他引数の入力や処理を受け、３０ＣＶＭＵ－Ｗ３Ｊを用いて３０ＤＬＲより暗号化データを含む情報３０ＤＬＲ－ＤＡＴＡ、（これには次が含まれる・・・Ｆ４Ｂ－２４：暗号化されたキー値ＣＫＣ・暗号化された関数Ｃｆｐ等、及び、Ｆ４Ｂ－２５：平文データ、ＴＩＤＡ、Ｂｎ、等）をユーザ端末にダウンロード・記憶する。
４．暗号データ復号部Ｆ４Ｂ－１０にて暗号化データを復号化する。Ｆ４Ｂ－１０に関連して平文データと暗号化データ間、或いは暗号化鍵の異なる暗号化データ間を区別する識別情報が３０ＤＬＲ内に備えられ、前記識別情報を用いＦ４Ｂ－１０やＦ４Ｂ－２６の機能部で識別・検知し、Ｆ４Ｂ－２６のように平文データ・暗号データの振り分けを行ってよい。
５．暗号化データを復号鍵Ｆ４Ｂ－９にて復号し、復号データＦ４Ｂ－１１を得る。
６．復号後データＦ４Ｂ－１１（ＣＫＣを復号して得たＫＣ、Ｃｆｐを復号して得た関数ｆｐ等）、平文データＦ４Ｂ－１２（ブロック番号Ｂｎ、トークン番号ＴＩＤＡ等）をＯＴＰ計算部Ｆ４Ｂ－１５　に入力し、ＯＴＰ計算をさせ、ＯＴＰを出力・生成させる（Ｆ４Ｂ－１６）。その後、ＯＴＰを印刷物や表示装置に記録させ（Ｆ４Ｂ－６）、若しくはユーザ端末の記憶装置に記憶する（Ｆ４Ｂ－５）。　Ｆ４Ｂ－６にて、コンピュータが出力するＯＴＰをユーザが手書きや撮影などして別の記録手段にＯＴＰを記録した場合も本願の記録手段Ｆ４Ｂ－６とする。
※アプリデータは改ざん検知手段やデジタル署名がなされていると好ましい。または改ざんされにくい媒体に記録されていると好ましい。例えば前記ウェブアプリ・アプリデータ３０ＣＶＭＵ－ＡＰＰはブロックチェーンのスマートコントラクトに記録されていてもよい。（ＥＣＭＡＳｃｒｉｐｔ部が改ざんされた場合、正しいＯＴＰの計算・生成、ウェブアプリ動作が困難になるため。またアプリなりすましを防ぐにはアプリデータへの電子証明書等が必要。）アプリデータはＳＳＬ・ＴＬＳ等により暗号化された経路で伝達されてもよい。
・前記ウェブアプリ・アプリデータは証明書・電子署名・ＨＭＡＣ・ハッシュ値などの等改ざん検知できる手段を備えてよい。
＜＜特願２０２１－００４７８８との関連＞＞
※特願２０２１－００４７８８で主張された内容を本願で行ってもよい。特願２０２１－００４７８８ではスマートコントラクトの実行部は本願で定義する平文の実行部３０ＰＶＭ（特にイーサリアム仮想機械）であったが、本願では暗号文の含まれるデータに対応する実行部３０ＣＶＭ、実行部３０ＣＶＭＵを利用することを提案している。
●特願２０２１－００４７８８ではＯＴＰの計算時にＯＴＰの表示期間・入力待ち受け時間を変える処理と、ＯＴＰの桁数・データ量を増減する処理が開示されているが本願でも例えば３０ＣＶＭＵのＯＴＰ計算部Ｆ４Ｂ－１５に前記処理を行う部分を備えさせてよい。公知のＯＴＰを利用するための処理を含んでよい。
※図４Ｃや図４Ｂの場合、変数ＫＣのみシークレットであるが（暗号化データＣＫＣの形で隠されているが）、トークンＩＤやユーザ識別子Ａはオープンにできるので、外部の人が例えばＮＦＴの譲渡が起きたことは察知できる。ユーザ識別子Ａを追加で隠す場合もある。
＜図４Ｃ＞ウェブアプリ式実行部３０ＣＶＭＵによるＯＴＰ認証時のＯＴＰ比較・検証・認証に関する本願の実施例
●図４Ｂと同様である。

・図４Ｃでアプリは認証端末３Ｃ、３Ｄに備えられ、ＯＴＰの記録手段を用いてＦ４Ｃ－９に入力されたＯＴＰについて
・図４Ｂではユーザ端末がＯＴＰを生成するアプリをダウンロードし保有する秘密鍵を用いて３０ＤＬＲにアクセスし変数関数を呼び出してＯＴＰを計算させる。
＜図５＞図５の（ａ）と（ｂ）は、第１（３０ＤＬＲ２－１ＳＴ）と第２（３０ＤＬＲ２－２ＮＤ）のブロックチェーンについて、第２のブロックチェーンに第１のブロックチェーンのブロックのハッシュ値が含まれていることで、第１のブロックチェーンのブロックが削除されていても、前記ハッシュ値を含む第２のブロックチェーンによって、ブロックチェーンの連続性を検証可能にする事の説明図。
・第２のブロックチェーンのブロックハッシュを第１のブロックチェーンのブロックに組み込んで第１と第２を相互に関連付け（リンク付け）てもよい。
図５の（ｃ）は前記第１と第２のブロックチェーンに加え第３のブロックチェーンを備え（あるいは第３、第４、第５、・・・第ｎのブロックチェーンを備え）互いにハッシュ値共有部（３０ＤＬＲ－ＳＨＡ、３０ＤＬＲ－ＳＨＡ－ｎ）を有するときの説明図。
＜図６＞図６は図５のブロックチェーンデータにおいて、第１（３０ＤＬＲ２－１ＳＴ）と第２（３０ＤＬＲ２－２ＮＤ）のブロックチェーンについて、第２のブロックチェーン（３０ＤＬＲ２－２ＮＤ）にＡ２・Ａ４のハッシュ値Ａ３ｈ・Ａ４ｈが含まれていることで、Ａ２・Ａ４のデータが削除されていても、Ａ３ｈ・Ａ４ｈを含む第２のブロックチェーンによって、第２のブロックチェーンと第１ブロックチェーンの残されたブロック間での連続性を検証可能にする事の説明図。
＜図７＞図７は図５の端末３Ａの説明部。３０ＤＬＲ２を用いる分散型台帳システムのノード端末３Ａの制御部・処理部と記憶部の説明部。
＜図８＞図８は図５の第１および第２のブロックチェーンを連結する手順の一つの説明図。
＜図９＞図９は図５のブロックチェーン記録部３０ＤＬＲ２を有するコンピュータ４又は人工知能システム４、又はサーバ４ＳＥＲＶＥＲ、ロボット４ＲＯＢＯＴ、輸送機器（４ＣＡＲ）、無人機（４ＤＲＯＮＥ）、農業機械（４ＡＧＲＩ）、生産用機械（４Ｐｒｏｄｕｃｔｉｏｎ）等の例。（必ずしもネットワーク２０を利用しない装置の例）
※図９に記載のコンピュータは入力元情報４ＩＮから学習用データを取得し、改竄耐性を持つブロックチェーン型記録部３０ＤＬＲ２に学習用データ３０ＳＴＵＤＹ－ＤＡＴＡを記録させ、機械学習部（３１ＳＴＵＤＹ）を用いた機械学習に利用する。
（機械学習には深層学習等公知の方法を用いてよく、学習データについても教師ありデータなど公知の方法を用いてよい。）
※学習後の学習データは、利用した頻度や新しさのデータ（需要データ３０ＤＥＭＡＮＤ）が学習データと対応するように付与され記憶装置に記憶される。
※学習データは学習データを需要によって保存または削除する部分（３１ＤＥＭＡＮＤ－ＦＯＲＧＥＴ）と需要データによって３０ＤＬＲ２の第１のブロックチェーン部から削除される。
※データブロックを忘れさせる事により人工知能システム４が一度記録したことを忘れさせるようにする。またシステムがデータを忘れたとしても、過去のハッシュ値又はデータを要約する部分（ａ１ｈ，ａ２ｈ，ａ３ｈ，，，，ａｎｈ）が第２のブロックチェーンのデータブロック（ｓＡ１，ｓＡ２，ｓＡ３，，，，ｓＡｎ）に残ることにより、改竄の心配なく、既に一度学習していたデータであることがわかる効果もある。）
＜図１０＞ＵＴＸＯ型トランザクションデータやアカウント型のトランザクションデータを第１・第２・・・第ｎのブロックチェーンを含むデータ記録部３０ＤＬＲ２に記憶させる場合の説明図。
※ここで第２（第３、第ｎ）のブロックチェーンの最新のブロックｓＡｎには第１のブロックチェーンの各アカウント毎の残高リスト又はユーザーのＵＴＸＯによる残高リストが第２のブロックチェーンの最新のブロックｓＡｎに記録される場合の説明図。
【図面の簡単な説明】

【００４６】
【図１】分散型台帳の記録部の暗号データについて復号を行いプログラムを実行するプログラム実行部３０ＣＶＭ・３０ＣＶＭＵの説明図
【図１Ａ】ノード端末３Ａの暗号化データ復号機能付き実行環境３０ＣＶＭ（仮想機械３０ＣＶＭ）と平文読み取り型仮想機械３０ＰＶＭの動作説明図
【図１Ｂ】ユーザ端末内実行環境３０ＣＶＭＵと平文読み取り仮想機械３０ＰＶＭによる３０ＤＬＲからの暗号データの読み取り・復号・データ実行、及び３０ＤＬＲへの書き込み説明図
【図２】本願で用いるコンピュータとコンピュータネットワークの例
【図３Ａ】暗号化データ３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹを３０ＤＬＲから選択・識別・区別し選び取るための部分の説明図
【図３Ｂ】暗号化データ３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹを３０ＤＬＲから選択・識別・区別し選び取り、暗号化・復号するための処理説明図
【図３Ｃ】サービス提供サーバ３Ｃが３Ａから得た暗号化データを復号し、ＯＴＰ認証などのサービスを提供する場合の説明図
【図４Ａ】ウェブアプリ式実行部３０ＣＶＭＵによるＯＴＰ認証時の電子計算機接続図
【図４Ｂ】ウェブアプリ式実行部３０ＣＶＭＵによるＯＴＰ認証時のＯＴＰ生成・計算に関する本願の実施例
【図４Ｃ】ウェブアプリ式実行部３０ＣＶＭＵによるＯＴＰ認証時のＯＴＰ比較・検証・認証に関する本願の実施例
【図５】第２と第１のブロックチェーンを備える記録部３０ＤＬＲ２の説明図。
【図６】図５の３０ＤＬＲ２において、第１ブロックチェーンの一部が削除されている場合に、第２のブロックチェーンと第１ブロックチェーンの残されたブロック間での連続性を検証可能にする事の説明図。
【図７】図７は図５の処理をするノード端末３Ａやコンピュータ又はサーバ３Ｃ・３Ｄ、人工知能システム４等の処理部・記憶部の説明部。
【図８】図８は図５の第１および第２のブロックチェーンを連結する場合の手順の例の説明図。
【図９】図９は図５のブロックチェーン記録部３０ＤＬＲ２を有するコンピュータ４又は人工知能システム４等の例。
【図１０】ＵＴＸＯ型トランザクションデータやアカウント型のトランザクションデータを記録部３０ＤＬＲ２に記憶させる場合の説明図。
【発明を実施するための形態】
【００４７】
本願で実行部３０ＣＶＭ・３０ＣＶＭＵを実施する場合には、図１、図１Ａ、図１Ｂ、図２や図４Ａ、図４Ｂ、図４Ｃに記載のコンピュータ、コンピュータネットワーク・システム、コンピュータ処理部と記憶部を用いる。
また、本願主張の記録部３０ＤＬＲ２については図５の（ｂ）や（ｃ）の構成を用いる。
【実施例１】
【００４８】
本願は、実行部３０ＣＶＭＵ・３０ＣＶＭＵをユーザ端末１Ａ、サーバ３Ｃ・３Ｄ、ノード３Ａに備えさせることにより、分散型台帳部の記録部に記録された平文データと暗号化データ混合したデータから暗号化データを復号可能にする。
実行部３０ＣＶＭＵ・３０ＣＶＭＵに関しては代表的な説明図は図１、図１Ａ、図１Ｂ、図３Ａ、図３Ｂ、図４Ａ、図４Ｂ、図４Ｃである。
【００４９】
＜平文と暗号化データ（及び暗号化データ同士）を区別し復号・実行する部分＞
本願は、前記データ台帳の記録部３０ＤＬＲと、
３０ＤＬＲに記録されたデータ３０ＤＬＲ―ＤＡＴＡを読み取る３０ＰＶＭと、
図３Ａに記載の前記３０ＤＬＲ―ＤＡＴＡに含まれる、

暗号化の開始部分３０ＤＬＲ―ＣＤＡＴＡ―ＰＳと、
終了部分３０ＤＬＲ―ＣＤＡＴＡ―ＰＥを表現する、
暗号化区間識別子を検出する検出手段、
又は暗号化部分を指定する部分（３０ＤＬＲ―ＣＤＡＴＡ―ＰＳ・ＰＥ、
３０ＤＬＲ―ＣＤＡＴＡ－ＡＤＤＲＥＳＳ、
３０ＤＬＲ―ＣＤＡＴＡ－ＡＮＮＯＴＡＴＩＯＮ）と、
図３Ｂ等に記載の前記検出手段により暗号化部分を解析・認識し、
暗号化部分を選び取る処理Ｆ３Ｂ２と、
前記暗号化区間に記録された
暗号化データ３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹを復号する手段、
又は前記手段として処理部Ｆ３Ｂ３、処理用の鍵Ｆ３Ｂ４、鍵計算手段Ｆ３Ｂ５　と、
前記復号する手段により、
暗号化データを復号して得られた復号データＦ３Ｂ９を得て、
前記復号データを命令として実行する、
実行部３０ＣＶＭ・３０ＣＶＭＵ・Ｆ３Ｂ１３と、を備えているコンピュータ（前記コンピュータはノード３Ａでもよく、好ましくはユーザ端末やサーバ３Ｃ・３Ｄ）に、
分散型台帳システムの台帳データ部に含まれる、暗号化データを復号し実行させる、仮想機械又は実行環境又は実行部３０ＣＶＭ・ＣＶＭＵを提案する。
前記実行部３０ＣＶＭＵ・３０ＣＶＭのサービス例としてＯＴＰ認証サービスがあり、図４Ｂ、図４Ｃに記載のＯＴＰの生成や認証サービスを行う。

【００５０】

●前記３０ＣＶＭはユーザ端末の記憶部・処理部を用いて形成される実行用ソフトウェア３０ＣＶＭＵ（アプリ・ブラウザ・ウェブページ・ウェブアプリ、３０ＣＶＭＵ－ＡＰＰ）でもよい。
●３０ＰＶＭとは具体的にはイーサリアムにおけるイーサリアム仮想機械ＥＶＭであり、本願では前記ＥＶＭとの互換性持ちつつ、暗号化データを扱うために、３０ＰＶＭで３０ＤＬＲのデータを読み取らせた後に引き続き３０ＣＶＭ、３０ＣＶＭというプログラム実行部に前記データを入力させ、入力されたデータに暗号化データがある場合には復号し復号されたデータを実行または利用する。

【００５１】

＜＜ウェブブラウザベースの暗号化データ復号機能付き実行環境＞＞
●３０ＣＶＭＵの一つとしてウェブブラウザでの実行環境３０ＣＶＭＵ－ＨＴＭＬＪＳでもよい。
●図４Ａ・図４Ｂ・図４Ｃにウェブブラウザのウェブアプリ実行部３０ＣＶＭＵ－ＨＴＭＬＪＳを用いる場合の電子計算機の接続図や、動作例としてワンタイムパスワードＯＴＰを計算し生成・出力する実行環境と、入力されたＯＴＰを比較検証し認証する実行環境の動作の流れ図を記載する。
●図４Ａ・図４Ｂ・図４Ｃの構成では前記ＥＶＭをブロックチェーンの記録部の暗号化データ交じりであってもよい平文読み取り用実行環境（第１のプログラム実行環境）として用い、暗号化データ解読部を持つウェブブラウザのウェブアプリ実行部３０ＣＶＭＵ－ＨＴＭＬＪＳを第２のプログラム実行環境に用いている。

【００５２】

●図４Ｂ・図４Ｃでは３０ＣＶＭＵの具体的な形態として、ウェブブラウザでの実行環境３０ＣＶＭＵ－ＨＴＭＬＪＳ（３０ＣＶＭＵ－ＡＰＰ）内部にＥＣＭＡＳｃｒｉｐｔの形でブロックチェーンからＯＴＰ計算用の変数ＫＣの暗号データＣＫＣやトークン番号ＴＩＤＡ、ブロック番号Ｂｎを呼び出す処理部を持ち、
前記ＣＫＣは復号鍵にて非対称鍵暗号又は対象鍵暗号にて復号されデータＫＣを得て、前記３０ＣＶＭＵ－ＨＴＭＬＪＳ内部ＥＣＭＡＳｃｒｉｐｔのＯＴＰ計算手続き・アルゴリズムに従い、前記変数の群ＫＣ、ＴＩＤＡ、Ｂｎをハッシュ関数或いはＯＴＰ計算用関数に入力する。

図では、ＯＴＰを計算しＯＴＰを生成出力する場合（図４Ｂ）と、
入力されたＯＴＰを検証認証する場合（図４Ｃ）が実施例１として提案される。
（図４Ｂ、図４Ｃでは、ハッシュ関数ｆｈに変数ＣＫＣを復号鍵により復号して得た変数ＫＣやトークン番号ＴＩＤＡ、ブロック番号Ｂｎを入力し、ハッシュ値を求める等の処理を経て、ＯＴＰ計算する。）
【００５３】
●本提案では、ウェブアプリ３０ＣＶＭＵ－ＡＰＰ（或いはダウンロードされたオフライン駆動するローカルなＨＴＭＬ・ＪＳファイル・ＥＸＥファイル等実行可能形式）等の形で用いてもよいが、３０ＣＶＭＵ－ＡＰＰのハッシュ値や作成者の電子署名情報３０ＣＶＭＵ－ＡＰＰ－ＳＩＧＮを含んでよい。３０ＣＶＭＵ－ＡＰＰと３０ＣＶＭＵ－ＡＰＰ－ＳＩＧＮが別のブロックチェーン（或いは改竄検知できる媒体、リポジトリ）に記憶され、ユーザがダウンロードするなどしてユーザ端末にて利用してもよい。第２実行環境のソフトウェアデータは改ざんされていないことが好ましく、ファイル作成者の身元（ファイルの出所）が分かる手段が付与されていてもよく、電子署名、デジタル署名、ＨＭＡＣ、ハッシュ値などでウェブアプリ・第２実行環境３０ＣＶＭ・３０ＣＶＭＵやその作成者の正しさ・真正性を検証できると好ましい。
【００５４】
●第２実行環境はユーザの秘密鍵を管理してもよい。例えば第２実行環境はウォレットソフトウェアの形態でもよい。
●第２実行環境３０ＣＶＭ・３０ＣＶＭＵは復号鍵を備えてもよい。第２実行環境は復号鍵の入力・出力ができてもよい。秘密鍵や復号鍵を耐タンパ性のある記憶装置に記憶していてもよい。
●可能ならば秘密鍵や復号鍵は耐タンパ性のある記憶域に記憶・記録されていると好ましい。
【実施例２】
【００５５】
本願は、ブロックチェーン記録部３０ＤＬＲ２を用いて、第１のブロックチェーンのブロックデータが消去又は忘れられていても、第２のブロックチェーンに第１のブロックチェーンのハッシュ値・特徴データが記憶されていることにより、３０ＤＬＲ２のデータの連続性を検証する事を可能にする。ブロックチェーン記録部３０ＤＬＲ２の説明図は図５、図６，図７、図８であり、３０ＤＬＲ２を利用するシステムの説明図は図９である。
【００５６】
＜一部ブロックを消去する機能＞
暗号化されたデータを含むブロックはその中身が秘密になり、その中身が誰かにとって必要なデータか、ＤｏＳ攻撃で蓄積したデータかを区別できない。そこで本願ではブロックチェーンの古いブロックを忘れる機能が必要であると考え考案する。本願のブロックチェーンデータ構造はデータブロックの一部を消去する（忘れられる機能を持つ）分散型台帳技術用に提案しているが、その用途に限らず改ざん検知可能なコンテンツデータや人工知能の記憶域にもちいてもよい。
【００５７】
＜３０ＤＬＲ２の人工知能システム４への利用（図９）＞
・人工知能が学習していく際にその記憶した内容がブロックチェーンのように過去から未来にわたり連結され学習していくことで、人工知能が学習していく際のデータの蓄積が第三者から追えるようにできる。
（例えば人工知能の学習の過程を外部から解析する際にブロックチェーンのブロック連結にしたがって学習データをため込んでいくので、どのデータブロックの学習結果が処理改善に寄与しているかを検証できるかもしれない。）
・また本願のブロックチェーンのデータ構造３０ＤＬＲ２では第１のブロックチェーン上のデータをノード端末３Ａ・システム４から忘れてもよい。
・記憶領域や外部との通信に制限のある輸送機器や家電に搭載されたコンピュータノード

３Ａに基づくＡＩであっても、その処理系はデータを忘れることができ、忘れることで記憶領域を再度確保し、再度学習に用いることができる。
【実施例３】
【００５８】
＜実施例３＞図１０は３０ＤＬＲ２において、第２のブロックチェーン部に第１のブロックチェーンの指定ブロック数毎のＮＦＴ・ＦＴやデジタル資産、証券データ、デジタル通貨、分散型台帳の手数料トークンの各ユーザの残高リストを記録できる部分を備えさせた実施例である。例えば１分ごとにデータブロックが蓄積する第１のブロックチェーン内のブロックデータが失われていても、例えば１時間・１日・１年毎にデータブロックの蓄積する第２のブロックチェーンには前記時間毎に残高データが記録されており、取引残高がバックアップされる。
【００５９】
＜トランザクションタイプ＞
●本願の実施においてトランザクションタイプは、ＵＴＸＯベーストランザクションやアドレス・アカウントベーストランザクションでもよい。
＜アドレス・アカウントベーストランザクションとアカウント暗号化利用＞
●ＮＦＴ、ＯＴＰ機能付きなどのＮＦＴ、ＦＴ、ユーティリティトークン、ガバナンストークン、セキュリティトークンの保管、流通時に、前記３０ＣＶＭＵ－ＨＴＭＬＪＳのような暗号化に対応する実行環境を用いることで、トークンの内部プログラムを秘匿化し、スマートコントラクト内に記録されたユーザ識別子とトークン番号・トークン保有関係を暗号化して秘匿化する。
【００６０】
●例えば代替不可能なユニークであるＮＦＴを誰が購入し、誰に譲渡されていったか追跡することを管理者以外には把握しづらくする必要があるかもしれない。
・或るスマートコントラクトがトークン持ち主の名簿（又は株式名簿）のようなユーザ識別子（名義）とトークン番号の対応を記録し、株式の数はユーザ識別子に帰属するトークン番号の数を数え上げ調べる、株式名簿型スマートコントラクトがある場合、あるトークン番号に対し割り当てられているユーザ識別子が暗号化されたデータＡ－ＣＲＰＴがブロックチェーンのブロックデータに記録されており、
前記３０ＣＶＭＵ－ＨＴＭＬＪＳのような暗号化に対応する実行環境と復号鍵／暗号化鍵と、前記データＡ－ＣＲＰＴを用いて、ブロックチェーンの記録されたブロックデータに対し読取と復号を行いユーザ識別子Aを得て、ユーザ識別子Aがどのトークン番号・IDのトークンを保有しており、それを誰に送信するかを処理させ、処理結果を暗号化しブロックチェーンの（最新の）ブロックデータに書込を行い、暗号化されたデータを取り扱う事を提案する。
【００６１】
＜ＵＴＸＯトランザクションと暗号化利用＞
本願において、前記３０ＣＶＭ・３０ＣＶＭＵ、３０ＤＬＲや３０ＤＬＲ２を用いる系では、３０ＤＬＲ、３０ＤＬＲ２に格納されるトランザクションタイプは、ＵＴＸＯ型、アカウント型どちらも可能であり、制限されない。（※ＵＴＸＯ：未使用トランザクションアウトプット）データ構造はブロックチェーン型、ＤＡＧ型の分散型台帳でもよい。前記３０ＣＶＭＵ等暗号化データ実行環境を用いる系は、ブロックチェーン型のほかにＤＡＧ型を用いてもよい。
【００６２】
＜匿名性＞データの匿名性を保つために本願実施例１の方法を用いて、情報の一部を暗号化し秘匿化してよい。（例：トークンの保有者のユーザ識別子、トークンＩＤ、残高等）トークンの保有主となるユーザ識別子を暗号化して記録する事により、ユーザのプライバシーを守る。トークンの異なるユーザ間での交換や、トークンの割り当て時にユーザ情報を秘匿化する。
【００６３】

＜保管・振替＞コントラクトを管理するユーザ端末からコントラクトを操作し、或るトークン番号のトークンを或るユーザ識別子Ａから除去し、別のユーザ識別子Ｂに付与するというトークンの振替（保管振替）を、ユーザ識別子を隠しながら行うこともできる。
※実施例３は実施例１と実施例２を組み合わせた例でもよい。
【００６４】
＜＜実施例１のその他事項＞＞
＜秘匿化・暗号化・符号化＞本願はブロックチェーン部又は分散型台帳システムの台帳データ部を部分的に暗号化・符号化・秘匿する方法に関連する。具体的には暗号化されたブロックチェーン上のデータを読み取って実行する実行環境３０ＣＶＭ・３０ＣＶＭＵを提案する。
●実行環境３０ＣＶＭは暗号化されたデータを復号する手段と復号する鍵又は鍵の入力部を備えてよい。鍵はユーザ端末１Ａから入力されてもよいし、実行環境３０ＰＶＭに備えていてもよい。
【００６５】
●図３Ｃでは、例えば実行環境（３０ＣＶＭＵ）がユーザ端末１Ａのフロントエンド部・ウェブブラウザで表示利用されるＨＴＭＬ、ＥＣＭＡＳｃｒｉｐｔ）に含まれる場合に、バックエンド部Ｆ３Ｃ３（ＰＨＰ言語、Ｐｙｔｈｏｎ言語、Ｒｕｂｙ言語等により記述されたプログラムが動く環境・各サービス提供会社システム・分散型台帳システムによる環境）は、サーバ端末３Ｃ又はサーバ端末３Ｃと接続された他のサーバ３Ａ・３Ｄに接続されていてよい。（図では３Ｃは３Ａと接続されており、３Ｃは３０ＤＬＲのデータを呼び出す。）
【００６６】
●図４Ｂ、図４Ｃが本願で主張する具体例である。
例えば、特願２０２１－００４７８８等に記載のスマートコントラクトをハッシュ関数とその引数となるキー変数を用いてＯＴＰを計算させる手法が考案されており、キー値として、変数ＫＣと、時間により変わる変数としてブロック番号Ｂｎ、ＯＴＰを生成する生成器の製造番号に相当するトークンＩＤ変数ＴＩＤＡをハッシュ関数ｆｈに代入し、ｆｈ（Ｂｎ、ＴＩＤＡ、ＫＣ）を計算し、ＯＴＰを計算する。
・本願では暗号化（後述の耐量子暗号の暗号化でもよい）を行う事でＯＴＰ計算時のキー値を秘匿化できる。
・また既存のＥＶＭ等でスマートコントラクト実行・変数・データ読取処理の後に３０ＣＶＭ・３０ＣＶＭＵにて処理をするので、既存システムに対し互換性を有する。
【００６７】
●前記変数ＫＣを暗号化してＣＫＣとし、ブロックチェーン部にＣＫＣ記録させた後、
前記暗号化データを読み取り、３０ＣＶＭ・３０ＣＶＭＵにてＯＴＰを計算させる方法として、以下の手順を考案する。
（１）ブロックチェーン部から３０ＣＶＭ・３０ＣＶＭＵに、次の３つの変数を読み取る。
１．変数Ｂｎ、２．変数ＴＩＤＡ、３．暗号化された変数ＣＫＣ（鍵ＫＣを暗号化して得た鍵ＣＫＣ）
（２）実行部３０ＣＶＭ・３０ＣＶＭＵで復号する。
暗号化されたデータ３０ＤＬＲ－ＣＤＡＴＡである変数ＫＣ（鍵ＣＫＣ、）を、
復号鍵（フロントエンド部に記憶された復号鍵、記録手段または端末３Ａ、端末３Ｃ、端末３Ｄ等に記憶された復号鍵）によって、復号し、鍵ＫＣ（変数ＫＣ、データＫＣ）を得る
（３）ＯＴＰ計算部に入力し計算する
変数Ｂｎ、変数ＴＩＤＡ、復号された鍵ＫＣ・変数ＫＣを、ＥＣＭＡＳｃｒｉｐｔの処理手続き内のハッシュ関数、ＯＴＰ計算部に入力し、ＯＴＰを計算させ、計算結果・処理結果（計算されたＯＴＰ）を、ユーザ端末１Ａの記憶装置に出力を行う。●計算結果（ＯＴＰ）をユーザ端末１Ａと通信可能な端末、サーバ端末３Ｃに送信し出力してもよい。出力

装置を用いて紙などに印刷し、ディスプレイに表示し、（音声出力・点字出力・画像出力等、人に伝える為の出力方法で）出力したＯＴＰをユーザが確認し記録媒体に筆記して記録し、又はＮＦＣタグなどに記録させ、若しくは通信により別の装置に伝達してもよい。

【００６８】

●暗号化に関して対称鍵・共通鍵暗号化と非対称鍵・公開鍵暗号化のいずれを用いてもよい。復号鍵３０ＣＫＥＹ（Ｆ３Ｂ５、Ｆ４Ｂ－９）は耐量子暗号技術で用いられる暗号化鍵／復号鍵でもよく、非対称鍵・公開鍵暗号化でもよい。また対称鍵・共通鍵暗号化でもよい。共通鍵方式ではＡＥＳ、公開鍵方式ではＥＣＤＳＡ、ＲＳＡ等がある。

【００６９】

●本願では、非対称鍵暗号・公開鍵暗号のうち耐量子性のある耐量子公開鍵暗号技術を用いてよい。（耐量子公開鍵暗号技術：公開鍵暗号技術の中でも、量子コンピュータが苦手とすると考えられている問題を基に暗号アルゴリズムが設計されているもの。）

・前記耐量子公開鍵暗号技術のうち格子問題を用いる方式（ＣＲＹＳＴＡＬＳ等）がある。（ＣＲＹＳＴＡＬＳ：Ｃｒｙｐｔｏｇｒａｐｈｉｃ　Ｓｕｉｔｅ　ｆｏｒ　Ａｌｇｅｂｒａｉｃ　Ｌａｔｔｉｃｅｓ）

・本願でも格子問題を用いた（ラティスベースの）非対称鍵・公開鍵暗号化を用いて、ブロックチェーンのブロック内に記録されたデータが暗号化されていてもよい。ハッシュベースの非対称鍵・公開鍵暗号化でもよい。（ＮＩＳＴはラティスベースのＣＲＹＳＴＡＬＳ－ＫＹＢＥＲ、ＣＲＹＳＴＡＬＳ－Ｄｉｌｉｔｈｉｕｍ、ＦＡＬＣＯＮ、ハッシュベースＳＰＨＩＮＣＳ＋方式を候補として発表している。）

【００７０】

●本願でＯＴＰ認証用のキーとなる変数・データのＫＣやそれを暗号化したＣＫＣは、データサイズが大きくないことを期待しており（例えば３２バイトの数倍の量）、先のキー値においてはデータ量が少ないことから耐量子暗号により暗号化・復号するための処理時間が短い事を期待する。

【００７１】

＜＜実施例２のその他事項＞＞

＜所定期間経過後のデータブロックの破棄＞取引履歴などの秘匿化・台帳データの削減のため、或る指定時刻を経過した時に過去の一部のデータブロックが削除されていても、ブロックチェーンの連続性を示すことのできるブロックチェーン構造を提案する。所定期間経過後のデータブロックの削除　・消去・忘却可能な方式を提案する。

例えば最新のブロックに対して７年経過後のブロックチェーン内データブロックを削除可能（及び平文では参照不可能）にしつつ、ジェネシスブロックから最新のブロックまでの連続性を検証できるブロックチェーン構造を提案する。

【００７２】

＜所定期間経過後のデータブロックの検索＞所定期間経過後のデータブロックを検索しない仮想機械・実行部を提案する。所定期間経過後のデータブロック内のアカウントのトランザクション頻度・利用頻度に応じて、データブロックを検索する／しない仮想機械・実行部を提案する。所定期間経過後の暗号化されたデータブロックを検索する／しない仮想機械・実行部を提案する。

【００７３】

＜＜実施例３のその他事項＞＞秘匿化データの発信者を知るための策（１）と、暗号化データが蓄積し台帳部データが増大した場合の策（２）を提案する。

【００７４】

（１）暗号化データへのアドレス等データ付与

アドレス情報・識別子情報３０ＤＬＲ―ＣＤＡＴＡ－ＡＤＤＲＥＳＳや、暗号化データの取り扱いのための情報３０ＤＬＲ―ＣＤＡＴＡ－ＡＮＮＯＴＡＴＩＯＮを、暗号化データ３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹにタグ付けして配置・記録してもよい。３０ＤＬＲ―ＣＤＡＴＡ－ＡＮＮＯＴＡＴＩＯＮは電子署名やハッシュ値、ＭＡＣ等、秘匿化・暗号化されたデータ３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹの証明書データ・検証用データにまつわ

るものでもよい。
※本願は特願２０２１－００４７８８におけるＯＴＰ認証用のＯＴＰ生成コントラクトとＯＴＰ認証部の内部変数・関数を秘匿化したい意図がある。しかし発明者としてはコントラクト作成者の情報まで暗号化して隠す想定はしていない。
例えばＯＴＰ生成トークンのスマートコントラクトのコントラクトアドレスやそれをデプロイしたユーザー識別子（コントラクトオーナーのユーザ識別子）を、暗号化データとともに記憶し、暗号化データの作成者や暗号化データそのものの識別子を記憶できれば好ましいと考える。
【００７５】
●例えばコントラクトアドレスやコントラクトデプロイユーザのアドレス３０ＤＬＲ―ＣＤＡＴＡ－ＡＤＤＲＥＳＳや、その他暗号化データの取り扱いのための情報３０ＤＬＲ―ＣＤＡＴＡ－ＡＮＮＯＴＡＴＩＯＮを、暗号化データ３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹの開始部分識別子３０ＤＬＲ－ＣＤＡＴＡ－ＰＳの直前や、３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹの終了部分識別子３０ＤＬＲ－ＣＤＡＴＡ－ＰＥの直後に配置してよい。
・台帳記録部（３０ＤＬＲ等）内で検索をかける場合に、検索キーワードとして３０ＤＬＲ―ＣＤＡＴＡ－ＡＤＤＲＥＳＳや、その他暗号化データの取り扱いのための情報３０ＤＬＲ―ＣＤＡＴＡ－ＡＮＮＯＴＡＴＩＯＮを利用できるように（検索により望みの暗号化データを含むブロックやコントラクトが見つかるように）、３０ＤＬＲ２のデータにユーザ識別子、コントラクトアドレス、ハッシュタグ、トークンなどを扱う場合トークンの名前等を記憶させていてもよい。
【００７６】
（２）第１のブロックチェーン（メインチェーン）と第二のブロックチェーン（ブロックチェーンを指定されたブロック番号の区間ごとに要約するブロックチェーン）を用いて、ブロックチェーンの連続性を検証しようとする方法
●図面の図５ではデータブロックの連結間隔がＴ１の第一のブロックチェーン３０ＤＬＲ２－１ＳＴがあって、前記３０ＤＬＲ２－１ＳＴの各ブロックデータのハッシュ値を保有する、連結間隔がＴ２の第二のブロックチェーン３０ＤＬＲ２－２ＮＤがあって、前記Ｔ１とＴ２の時間の大小関係はＴ１＜Ｔ２である。
●前記３０ＤＬＲ２－２ＮＤは或るＴ２の時間時刻に含まれる３０ＤＬＲ２－１ＳＴのデータブロック群（ｍ個のデータブロック）の其々のハッシュ値・特徴データを格納する特徴を持つ。
●第３のブロックチェーン３０ＤＬＲ２－３ＲＤがＴ３連結間隔の時間を持ち、さらに高次の第ｍのブロックチェーン３０ＤＬＲ２－ｎの連結間隔がＴｎであるとき、時間の大小関係はＴ１＜Ｔ２＜Ｔ３＜・・・＜Ｔｎである。
【００７７】
＜＜請求の範囲＞＞
請求項１：ブロックチェーンを用いた分散型台帳システムのノード３Ａと、ユーザ端末Ｕと、ネットワーク２０を含む、コンピュータネットワークシステムにおいて、
前記コンピュータネットワークシステムは、ブロックチェーン３０ＤＬＲのブロックデータに記憶されたデータの読み取り、又は前記データを読み取り後に、前記データをプログラムとして実行可能な、仮想機械３０ＰＶＭ又は実行部３０ＰＶＭと、
前記暗号化データを復号し、前記暗号化データを復号して得られたデータを用いる、スマートコントラクト又はプログラムを実行可能な、プログラム実行部３０ＣＶＭ、又はユーザ端末のプログラム実行部３０ＣＶＭＵと、
を備えているコンピュータネットワークシステム。
請求項２：前記ブロックチェーンのデータ構造に、第１のブロックチェーンと第２のブロックチェーンの構造が含まれており、前記第２のブロックチェーンのブロックに、前記第１のブロックチェーンの指定個数のブロックの其々のハッシュ値が含まれている、ブロックチェーンデータ構造３０ＤＬＲ２を用いる、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：前記第２のブロックチェーンのブロックに、前記第１のブロックチェーンのトランザクションデータを基にする情報、又は前記トランザクションデータを基にした資産の残高情報を記録する特徴を持ち、ブロックチェーン内のデータ暗号化を可能する特徴と、前記第１のブロックチェーンのデータを削除可能にする特徴を持つ、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：請求項１に記載のコンピュータネットワークシステムを用いた動的パスワードの認証システム。
請求項A：ブロックチェーン部分に、第１のブロックチェーンと、第２のブロックチェーンの構造が含まれており、前記第２のブロックチェーンのデータブロックに、前記第１のブロックチェーンの指定個数のデータブロックの其々のハッシュ値が含まれている、ブロックチェーンのデータ構造。
請求項B：請求項Aに記載のブロックチェーンのデータ構造に、機械学習における学習データを記憶する特徴を持つ、人工知能システム。
【産業上の利用可能性】
【００７８】
＜実施例１＞パブリックな分散型台帳システムのデータ記録部を利用する場合に、改竄困難かつ動作内容を秘匿化したプログラム・ソフトウェアを提供する。
分散型台帳システムに改竄困難な形で記憶した暗号化データ・変数・関数を用いてサービス用のプログラムが実行できるようなり、ユーザのプライバシーを保護するとともにプログラム動作を秘匿化し保護する。
・分散型台帳システムを用いたＯＴＰ認証サービスにおいてプログラムを秘匿化し保護する。
＜実施例２＞ブロックチェーンから需要に応じてデータブロックを削除できる。
既存のトークンの類をやり取りする分散型台帳システムのほかに、取引履歴、何かの商品荷物追跡データ、ＳＮＳ用途など、記憶すべき量が多い一方で保存期限が限られるサービスへの利用を想定する。
・人工知能が学習していく際に、需要のある若しくは指定されたデータブロックについては、改竄されず忘れないようにしつつ、需要のないデータを忘れることのできる人工知能が実現できる。
・機械学習のための学習データを記憶していく内容がブロックチェーン式で記憶され、過去から未来にわたり連結され学習していくことで、人工知能が学習していく際のデータの蓄積が第三者から追えるようにできるかもしれない。
＜実施例３＞動作内容を秘匿化したプログラム・ソフトウェアを提供する。その際に記録媒体であるブロックチェーン部はデータブロックを削除する機能を備え、例えば何らかの資産や商品の取引データの容量の増大を抑制する。
・またユーザに過去の或る期限の第１のブロックチェーンのデータブロック群での取引の推移や残高をまとめた残高証明書・取引履歴のサマリーを第２のブロックチェーンに記憶でき、ユーザが自身の資産やその推移を確認する事に役立つ。
・前記残高証明書・取引履歴のサマリーを第２のブロックチェーンに改竄困難な状態で記憶することにより、ユーザの財産の記録を守る。
【符号の説明】
【００７９】
＜図１から図２＞
１Ａ　ユーザ端末、ユーザコンピュータ
１０Ａ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）
１０ＡＫＥＹ　秘密鍵情報記録手段（３Ａの３０ＤＬＲアクセス用）
１１Ａ処理装置
１６Ａ外部記憶装置、外部記録手段
１００記憶装置、１０１処理装置、１０ＷＩＲ　内部配線、バス
１０２通信装置、１０４入力装置、１０５出力装置

２０　ネットワーク、通信経路、情報の伝達（配布）経路
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）
３０ＣＫＥＹ　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　ユーザ端末用暗号データ復号可能な第２実行環境
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
３０ＤＬＲ－ＤＡＴＡ　３０ＤＬＲに含まれる暗号化データを含むデータ
３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹ　暗号化データ本体
＜図３Ａから図３Ｃ＞
３０ＤＬＲ－ＣＤＡＴＡ－ＡＤＤＲＥＳＳ（３０ＤＬＲ－ＣＤＡＴＡ－ＡＮＮＯＴＡＴＩＯＮ）　暗号化データを含むデータに付与された識別子（ユーザ識別子、コントラクトアドレス等。ブロックチェーンエクスプローラー等でデータ検索される時の識別子）
３０ＤＬＲ－ＣＤＡＴＡ－ＰＳ　暗号データの開始部、暗号データを他のデータと区別する部分
３０ＤＬＲ－ＣＤＡＴＡ－ＢＯＤＹ　暗号データ本体
３０ＤＬＲ－ＣＤＡＴＡ－ＰＥ　暗号データの終了部、前記区別する部分
３０ＤＬＲ－ＰＤＡＴＡ　平文データ（或いはその他データ）
Ｆ３Ｂ１データ入力処理部、Ｆ３Ｂ２　入力データ解析部　（暗号データを他のデータと区別する部分の識別部、検出部、解析部。３０ＤＬＲ－ＣＤＡＴＡ－ＰＳ・ＰＥ検出部）
Ｆ３Ｂ３復号部分、Ｆ３Ｂ４暗号化鍵／復号鍵管理部分、Ｆ３Ｂ５　鍵・鍵計算方法記憶部
Ｆ３Ｂ６復号鍵入力手段（例：１Ａ、１６Ａ、３Ａ、３Ｃ、３０ＤＬＲ等から鍵を得る）
Ｆ３Ｂ７秘密鍵等３０ＤＬＲアクセス手段
Ｆ３Ｂ８　耐ウイルス型実行部、Ｆ３Ｂ９復号されたデータ、Ｆ３Ｂ１０記憶部、Ｆ３Ｂ１１処理部、Ｆ３Ｂ１２処理結果応答、Ｆ３Ｂ１４　出力処理部、Ｆ３Ｂ１５暗号化部分
Ｆ３Ｃ１スマートコントラクト提供部（ウェブアプリフロントエンド）
Ｆ３Ｃ２暗号処理機能付き仮想機械実行部ＣＶＭ
Ｆ３Ｃ３　３０ＣＶＭ管理部（バックエンド、サーバー３Ｃ・３Ｄ・３Ａの側）
Ｆ３Ｃ４　　鍵データ・鍵管理部（耐タンパ性を持つ記憶域可）
Ｆ３Ｃ５　ブロックチェーンクライアント部ソフトウェア（ノード通信部）
３０ＤＬＲ－Ｃ　ブロックチェーンデータ記録部（又は暗号化データ含む読み出した台帳データ）
＜図４Ｂ、図４Ｃの説明＞
＜＜図４Ｂ＞＞
Ｆ４Ｂ－１ウェブアプリへの入力用データ群、ＤＬＳへのアクセス用データ
Ｆ４Ｂ－２ユーザ秘密鍵
Ｆ４Ｂ－３アプリ入力用復号鍵等
Ｆ４Ｂ－４ウェブアプリ実行用ソフトウェアデータ部ブラウザ、３０ＣＶＭＵ－Ｗ３Ｊ含んでもよい
Ｆ４Ｂ－５計算されたＯＴＰ
Ｆ４Ｂ－６　　記録手段（含む印刷物、表示面）
Ｆ４Ｂ－７計算されたＯＴＰ
Ｆ４Ｂ－８　ウェブアプリ実行部３０ＣＶＭＵ－ＨＴＭＬＪＳ（ウェブブラウザの処理部・記憶部）
配信されたウェブアプリデータ、３０ＣＶＭＵ－ＡＰＰ（ＥＣＭＡＳｃｒｉｐｔ式、ＯＴ

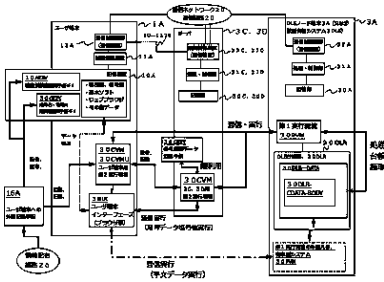
Ｐ生成部）
Ｆ４Ｂ－９　復号鍵（例：ＣＫＣの復号鍵）
Ｆ４Ｂ－１０　暗号データ復号部（暗号化データと平文データを区別・識別・選択し選び取る処理部と、暗号化データを復号する処理部を含んでよい。）
※
Ｆ４Ｂ－１１復号済データ　例：ＣＫＣ復号により得たデータＫＣ、Ｃｆｐ復号により得た関数ｆｐ
Ｆ４Ｂ－１２平文データ例：Ｂｎ、ＴＩＤＡ
Ｆ４Ｂ－１３　ハッシュ関数ｆｈ（或いは、一方向関数ｆｈ、若しくはＯＴＰ計算のための処理手続き関数）、ｆｈの引数例：ｆｈ（ＫＣ、Ｂｎ、ＴＩＤＡ）
Ｆ４Ｂ－１４関数ｆｐ
Ｆ４Ｂ－１５　　ＯＴＰ計算部
Ｆ４Ｂ－１６＜ＯＴＰを生成する処理＞計算されたＯＴＰを戻り値として返す
Ｆ４Ｂ－１７　　３０ＣＶＭＵ－ＡＰＰ‐ＳＩＧＮ（証明書、電子署名、ハッシュ値）、ウェブアプリデータの正しさを検知・検証する手段にかかわるデータ。デジタル署名、ＨＭＡＣ等、タイムスタンプ等（例：３０ＣＶＭＵ－ＡＰＰのハッシュ値等。）、３０ＣＶＭＵ－ＡＰＰは必要によっては３０ＣＶＭＵ－ＡＰＰ－ＳＩＧＮ備える。
※３０ＣＶＭＵ－ＡＰＰを配布若しくは通信によりユーザ端末やサーバに伝達するときは、通信内容を暗号化・秘匿化してよい。（通信のうち、電気通信では、例えばＳＳＬ／ＴＬＳ通信により暗号化通信を行ってもよい。通信のうち郵送による信書郵便で、光学メディア・磁気記録装置・半導体メモリによる記録手段に、３０ＣＶＭＵ－ＡＰＰ（及び３０ＣＶＭＵ－ＡＰＰ‐ＳＩＧＮ）を記録させユーザ端末及びユーザへ送付してもよい。）前記伝達時に３０ＣＶＭＵ－ＡＰＰ‐ＳＩＧＮを３０ＣＶＭＵ－ＡＰＰに添付してよい。
Ｆ４Ｂ－１８　　ユーザ端末１Ａ
Ｆ４Ｂ－１９　　サーバ３Ｃ、３Ｄ
Ｆ４Ｂ－２０　　ＤＬＳノード３Ａ
Ｆ４Ｂ－２１　　３０ＤＬＲ
データブロック又はスマートコントラクトに、暗号化された変数ＣＫＣ、Ａ－ＣＲＰＴや暗号化された関数Ｃｆｐ、トークン番号（ＮＦＴのＩＤ）ＴＩＤＡ、ユーザ識別子Ａ、ブロック番号Ｂｎを含む。（　トークン番号（ＮＦＴのＩＤ）ＴＩＤＡが暗号化し変数ＣＴＩＤＡとして記録してもよい）
Ｆ４Ｂ－２２　　３０ＰＶＭ平文読み取り仮想機械ＰＶＭ。例：イーサリアム仮想機械ＥＶＭ
Ｆ４Ｂ－２３　　３０ＣＶＭＵ－Ｗ３Ｊ、分散型台帳システムへのアクセス手段。例：ブロックチェーンアクセス用ＡＰＩ（Ｗｅｂ３．ｊｓ等）
※３０ＣＶＭＵ－ＡＰＰと、３０ＣＶＭＵ－ＡＰＰ－ＳＩＧＮはブロックチェーンのブロックデータとハッシュ値の対応関係と同様でもよく、前記３０ＣＶＭＵ－ＡＰＰと３０ＣＶＭＵ－ＡＰＰ‐ＳＩＧＮはブロックチェーンのデータブロックでもある３０ＣＶＭＵ－ＡＰＰと、そのハッシュ値３０ＣＶＭＵ－ＡＰＰ－ＳＩＧＮをユーザ１Ａがノード３Ａ（３Ｃ）のブロックチェーン記録部３０ＤＬＲから読み取ることで１Ａの記憶装置、処理部に配置してもよい。
※＜関数ｆｐ＞例：ハッシュ値からＯＴＰを算出する残り手続き
＜＜図４Ｃ＞＞
Ｆ４Ｃ－１　復号鍵（例：ＣＫＣの復号鍵）
Ｆ４Ｃ－２暗号データ復号部
Ｆ４Ｃ－３復号済データＫＣ。例：ＣＫＣを復号化したデータＫＣ
Ｆ４Ｃ－４平文データ。例：Ｂｎ、ＴＩＤＡ等
Ｆ４Ｃ－５　ハッシュ関数ｆｈ。ｆｈ（ＫＣ、Ｂｎ、ＴＩＤＡ）
Ｆ４Ｃ－６　ＯＴＰ計算部、ＯＴＰ比較検証認証部
Ｆ４Ｃ－７　記憶された認証用の変数、関数

Ｆ４Ｃ－８　ＯＴＰ比較・検証、認証部
Ｆ４Ｃ－９　ＯＴＰ認証用入力部
Ｆ４Ｃ－１０認証実行時入力データ（トークン番号ＴＩＤＡ等）
Ｆ４Ｃ－１１　　３０ＤＬＲ－ＰＤＡＴＡ　例：平文のトークン番号変数ＴＩＤＡ、平文のブロック番号Ｂｎ等
Ｆ４Ｃ－１２　３０ＤＬＲ－ＣＤＡＴＡ例：暗号化されたキー値ＣＫＣ、暗号化されたユーザ識別子Ａのデータ Ａ－ＣＲＰＴ等
Ｆ４Ｃ－１３　　「ブロックチェーンアクセス用ＡＰＩ（Ｗｅｂ３．ｊｓ等）」、若しくは、「Ｆ４Ｃ－７記憶された認証用の変数、関数」を端末へ導入若しくは変更・更新する手段
※図４ＣのＦ４Ｃ－１５（認証端末）は、オンラインなサーバ３Ｃとオフラインなサーバ３Ｄのどちらも可能であって、３Ｃ場合、ＡＰＩを用いてネットワーク経由で認証用変数関数を呼び出すことができる。（３Ｄの場合、Ｆ４Ｃ－７を外部から導入し記録させ更新変更させる手段があってもよい。）
Ｆ４Ｃ－１４　　ウェブアプリ実行部３０ＣＶＭＵ－ＨＴＭＬＪＳ（ウェブブラウザの処理部・記憶部）
Ｆ４Ｃ－１５　　認証端末　例：端末１Ａ、３Ｄ、３Ｃ。※３Ｄは予めＯＴＰ計算用キーや、計算手続きを記憶していてよい。（オフライン時でも認証可能とする目的で）
Ｆ４Ｃ－１６　　ユーザ端末１Ｃ、サーバ３Ｃ
Ｆ４Ｃ－１７　アプリデータ　例：ＥＣＭＡＳｃｒｉｐｔ式ＯＴＰ認証部を含むアプリ
Ｆ４Ｃ－１８　　ＤＬＳ、ノード３Ａ（Ｆ４Ｂ－２１　　３０ＤＬＲと同様の暗号化されたデータを含む）
Ｆ４Ｃ－１９　ユーザ端末
Ｆ４Ｃ－２０計算されたＯＴＰ
Ｆ４Ｃ－２１　記録手段
Ｆ４Ｃ－２２計算されたＯＴＰ（その他認証に必要な情報を含んでもよい）
Ｆ４Ｃ－２３認証結果に応じた応答又は戻り値を出力
＜図５＞
３０ＤＬＲ　分散型台帳システムの改竄耐性を持つ記録部
３０ＤＬＲ１　１つのブロックチェーン部から構成されるブロックチェーン部
３０ＤＬＲ２　本願主張の２つ（２つ以上）のブロックチェーンから構成されるブロックチェーン部
３０ＤＬＲ２－１ＳＴ第１のブロックチェーン（ａ１，ａ２，ａ３，，，ａｎ、例：ブロック生成時間５秒毎）
３０ＤＬＲ２－２ＮＤ第２のブロックチェーン（ｓＡ１，ｓＡ２，ｓＡ３，，，ｓＡｎ、例：ブロック生成５分、５時間毎）※第１のブロックチェーンの、指定ブロック数毎に含まれる、各ブロックのハッシュ値をブロックに含む、第２のブロックチェーン
３０ＤＬＲ２－３ＲＤ（ｎ）　第３［又は第ｎ］のブロックチェーン（ｓｓＡ１，ｓｓＡ２，ｓｓＡ３，，，ｓｓＡｎ　　［ｎｓＡ１　，　ｎｓＡ２，ｎｓＡ３，，，ｎｓＡｎ］、例：ブロック生成５時間毎、５年毎）
ａｎｈ　第１のブロックチェーンのブロックａ１，ａ２，ａ３，，，ａｎのハッシュ値ａｎｈ（図中ａ１ｈからａ６ｈ）
ａｎｄ　第１のブロックチェーンのブロックデータの特徴データやフィンガープリント（図中ａ３ｄ）
ｓＡｎｈ　第２のブロックチェーンのブロック　ｓＡ１，ｓＡ２，，，ｓＡｎのハッシュ値ｓＡｎｈ（図中ｓＡ１ｈからｓＡ２ｈ）
ｓＡｎｄ　　第２のブロックチェーンのブロックデータの特徴データ等
ｓｓＡｎｈ　　第３のブロックチェーンのブロックのハッシュ値ｓｓＡｎｈ
３０ＤＬＲ２－ＳＨＡ　第１のブロックチェーンと第２のブロックチェーンにおいてハッシュ値を共有する部分（１ＳＴと２ＮＤ間でのハッシュ値等を互いに記録し合っている部

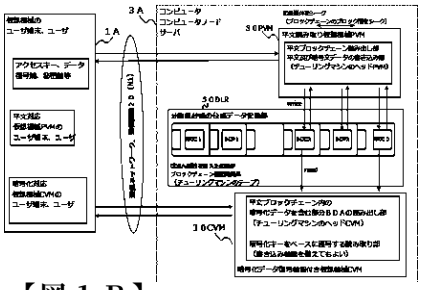
分）
３０ＤＬＲ２－ＳＨＡ－ｎ　第２のブロックチェーンと第３のブロックチェーンにおいてハッシュ値を共有する部分（第ｎと第ｎ＋１のブロックチェーン間でハッシュ値を共有する部分）
３０ＤＬＲ２－Ｆ　（Ｆｏｒｇｅｔ－ｏｌｄ－Ｂｌｏｃｋ－Ｄａｔａ）　第１のブロックチェーンのブロックデータが削除された場合
３１ＤＬＳＣノードクライアント制御部・管理部
３１ＰＶＭ実行環境制御部
３１ＥＴＣその他制御部
３１ＤＬＲ２
３１ＤＬＲ２－ＬＩＮＫデータブロック連結部
３１ＤＬＲ２－１ＳＴ２ＮＤ－ＬＩＮＫデータブロック連結部（第１及び第２のブロックチェーンのデータブロック連結処理部。３０ＤＬＲ２－１ＳＴと、３０ＤＬＲ２－２ＮＤの２つのチェーンを１つのチェーンとしてブロックデータ連結やブロックへハッシュ値の記憶を行う部分３０ＤＬＲ２－ＳＨＡに関する処理含む）
３１ＤＬＲ２－ＳＨＡ　３０ＤＬＲ２－ＳＨＡを計算３０ＤＬＲ２に記憶する部分
３１ＤＬＲ２－ＥＴＣ　その他制御部（ハッシュ値計算部、連続性検証部、合意形成部など）
３１ＤＬＲ２－１ＳＴ第１のブロックチェーン制御部３０ＤＬＲ２－１ＳＴ制御部（ａ１，ａ２，２３，．．．ａｎ）
３１ＤＬＲ２－２ＮＤ第２のブロックチェーン制御部３０ＤＬＲ２－２ＮＤ制御部（ｓＡ１，ｓＡ２，ｓＡ３，．．．ｓＡｎ）
３１ＤＬＲ２－Ｎ（必要時）第ｎのブロックチェーン制御部
＜＜消去条件部分＞＞
＜需要部＞
３０ＢｄＦＧ－ＤＥＭＡＮＤブロックチェーンのブロックデータの需要記憶部（必要時）（消去リクエスト・ネガティブな需要のあるデータブロック指定も含む）
＜消去部＞
３１ＢｄＦＧ　一定期間経過後、ブロックデータを（需要や指定データに応じて）消去可能にする部分（３０ＢｄＦＧ等データ利用）●人工知能システム４においては利用頻度の高いデータやブロックデータを記憶するための部分
３０ＢｄＦＧ　一定期間経過後ブロックデータを消去可能にするプログラム
３０ＢｄＦＧ－ＶＡＲ　消去のための変数・閾値・データ、若しくは消去までの一定期間を設定するデータ
３０ＢｄＦＧ－ＥＸＣＶＡＲ消去の例外となる変数・閾値・データ（あるブロック番号の、データブロックについて、トランザクション数が閾値以上（需要がある）である等。若しくはユーザ投票やアクセス数が閾値以上等）●人工知能システム４においてはヒトの頭脳におけるよく利用するデータを記憶する部分。（該部分はヒトの脳において神経細胞がよく利用されて記憶が強く残っている部分を再現するかもしれない。）
※上記消去条件部分３１ＢｄＦＧ、３０ＢｄＦＧ－ＶＡＲ、３０ＢｄＦＧ－ＥＸＣＶＡＲや需要部３０ＢｄＦＧ－ＤＥＭＡＮＤ、３０ＢｄＦＧ－ＶＡＲ等についても、ブロックチェーンなど改竄困難（あるいは改竄困難だが長期には時間経過により忘れられる）記録部に記録することが好ましいかもしれない。
３０ＤＬＳＣノードクライアントソフトウェア
＜図９＞
４人工知能システム
４ＣＡＲ　４を備える自動車
４ＤＲＯＮＥ　４を備える無人機
４ＡＧＲＩ　４を備える農業機械
４Ｐｒｏｄｕｃｔｉｏｎ　４を備える生産用機械

４ＲＯＢＯＴ　４を備えるロボット
４ＳＥＶＥＲ　４を備えるサーバ
４ＩＮ　学習元、学習対象、又は学習先のインターネットなど通信先
４２　通信装置
４４　４の入力装置（主にセンサ）
４ＯＵＴ　機械学習を行う人工知能システム４が出力する結果。出力応答
４５　４の出力装置
４１　４の処理装置
４０　４の記憶装置
３０ＤＬＲ２　ブロックチェーン記録部（ここでは記憶装置４０内部データ）
３０ＳＴＵＤＹーＤＡＴＡ　４の記憶装置のデータ部３０ＤＬＲ２に記憶された学習データ
３０ＳＴＵＤＹ機械学習部、ソフトウェア部
３０ＤＥＭＡＮＤ学習データの各ブロックのデータ需要記録部
３１ＳＴＵＤＹ機械学習処理部
３１ＤＥＭＡＮＤーＦＯＲＧＥＴ学習データを需要によって保存または削除する部分
３１ＤＬＲ２ブロックチェーン処理部
３０ＤＡＴＡその他データ
＜図１０＞
Ｔｘｎ　トランザクションデータ（整数ｎ＝１，２，３，，，）
ＴｘｎＣ　暗号化されたトランザクションデータ（整数ｎ）
ＵＴＸＯｎ　ＵＴＸＯデータ（整数ｎ）
ＵＴＸＯｎＣ　暗号化されたＵＴＸＯデータ（整数ｎ）
ＮＦＴＬＩＳＴ　ユーザのＮＦＴの残高（ｓＡ２を形成する時点での最新の残高証明データ）
ＵＳＥＲＢａｌａｎｃｅＬＩＳＴ
ＵＴＸＯ　ＡＬＬ　ＵＳＥＲ　ＢａｌａｎｃｅＬＩＳＴ　ＵＴＸＯ残高（最新の残高証明データ）
Ａｃｃｏｕｎｔ　ＡＬＬ　ＵＳＥＲ　ＢａｌａｎｃｅＬＩＳＴ　残高（最新の残高証明データ）

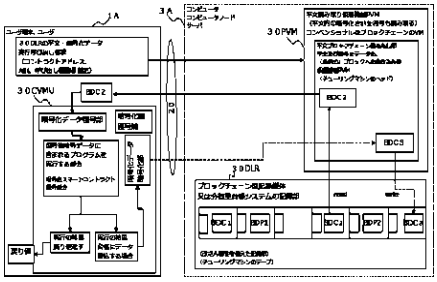
【図１】



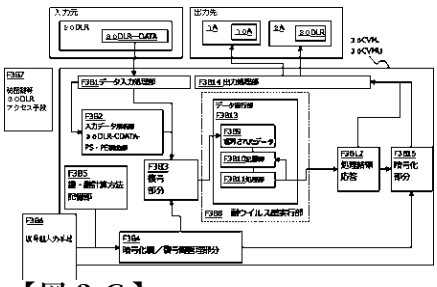
【図１Ａ】



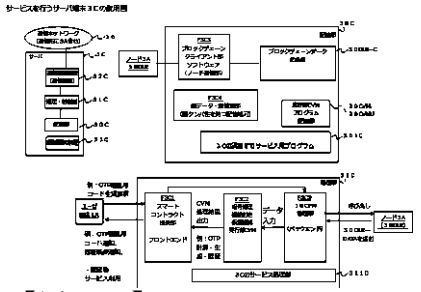
【図１Ｂ】



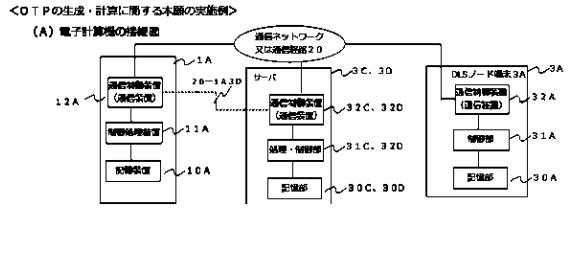
【図３Ｂ】



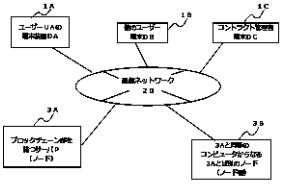
【図３Ｃ】

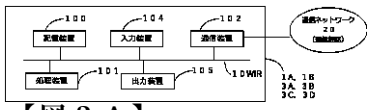


【図４Ａ】

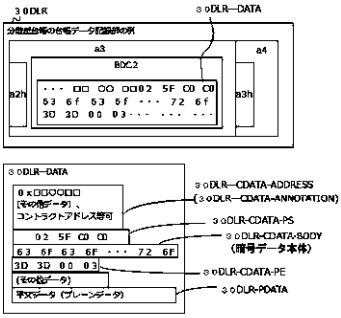


【図２】

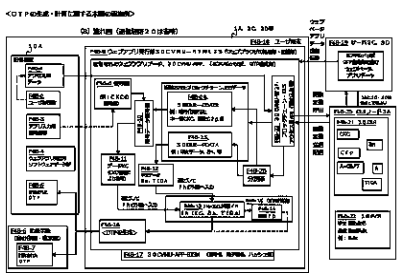




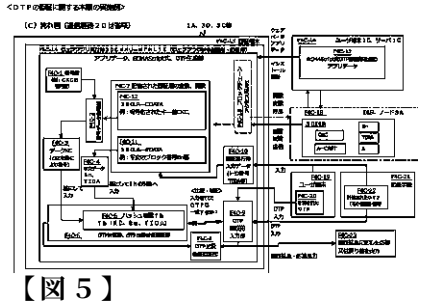
【図３Ａ】



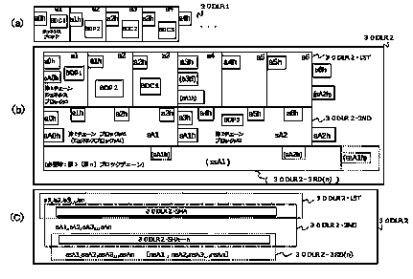
【図４Ｂ】



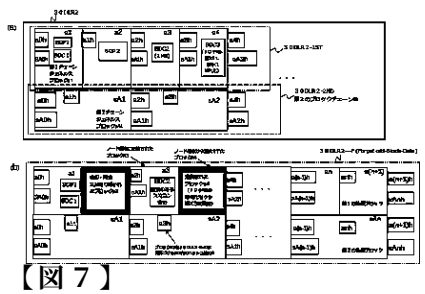
【図４Ｃ】



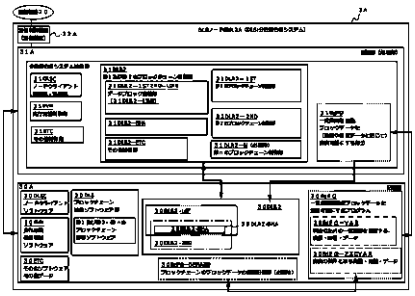
【図５】



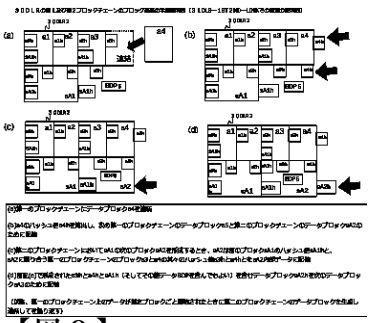
【図６】



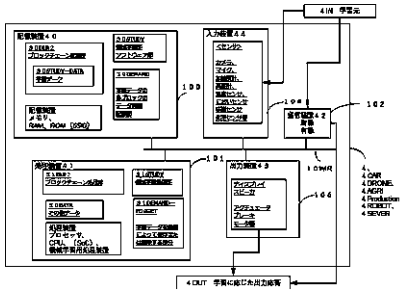
【図７】



【図８】



【図９】



【図１０】