明　細　書

発明の名称 ： 情報処理装置、プログラム、情報処理方法

技術分野

[0001]　本開示は、情報処理装置、プログラム、情報処理方法に関する。

背景技術

[0002]　ブロックチェーン上で管理するトークンの発行方法及び制御方法に関して、電子的かつ中央集権的な仕組みを持たずに価値を表現・移転させることができるビットコインが登場し、これを実現しているブロックチェーン技術が広く広まっている。ビットコインの概念やブロックチェーン技術の理解が進むと共にビットコイン以外に電子的に価値を表現する様々なコインが登場している。これらの価値を持つコインのことを、以下ではトークンと呼ぶ。ブロックチェーン技術の特徴から、発行されたトークンは改ざんすることが非常に困難という特徴を持つ。この特徴を活かし、画像、動画、音声などの様々な電子データの保有者をブロックチェーンに記録して保有者であることを保証・証明するという使い方が広まっている。このような用途で利用されるトークンをＮｏｎ－Ｆｕｎｇｉｂｌｅ　Ｔｏｋｅｎ（ＮＦＴ）と呼ぶ。ＮＦＴのコンセプト自体は古くからあるが、２０１７年頃から少しずつ認知され始め、２０２１年には高額で取引されるものも出てきたこともあり、注目されている。ＮＦＴの具体的な利用方法として、無形資産の管理（特許文献１）や契約・ライセンス管理（特許文献２）などが検討されている。従来、権利保有者が中央管理していたシステムからブロックチェーンを活用した分散システムにすることで耐障害性を高めると共に、中央管理者が業務を遂行できなくなっても、問題なく記録済みの情報が利用できるという特徴を提供することができる。

先行技術文献

特許文献

[0003] 特許文献1：特許第６６４０３２０号

特許文献2：特開２０２０－６８３８８号公報

発明の概要

発明が解決しようとする課題

[0004] 現時点ではＮＦＴという技術自体が新しいものであり、その作成には専門家の知見が必要であると共に、利用者もブロックチェーンにおける取引方法を理解しないとＮＦＴのようなトークンを取得すること自体が難しいという課題がある。

[0005] そこで、本開示は、利用者によるトークンの取得や管理を効果的に支援することを目的とする。

課題を解決するための手段

[0006] 本開示の一局面によれば、複数の計算機で構成されるブロックチェーンネットワーク上で流通可能な一のトークンを取得するための取得要求が、利用者端末により生成されることに基づいて、前記一のトークンの取得又は管理を可能とする所定情報を生成するとともに、生成した前記所定情報を前記利用者端末又はサーバ装置に係る所定記憶領域に記憶させる第１処理を実行する、情報処理装置が提供される。

発明の効果

[0007] 本開示によれば、利用者によるトークンの取得や管理を効果的に支援することが可能となる。

図面の簡単な説明

[0008] [図1]本実施形態の基本構成を示す図である。

[図2]ブロックチェーンネットワークを構成する各ノード及び利用者端末、トークン制御処理受付部の構成を示す図である。

[図3]トークン生成処理を示す図である。

[図4]配信手段に設定するトークン制御情報を示す図である。

[図5]受信データ格納部を示す図である。

[図6]スマートコントラクトのトークン管理情報を示す図である。

[図7]トークン配布数管理を示す図である。

[図8]実施形態３に係るトークン受け取り処理の説明用のフローチャートである。

[図9]実施形態３に係るトークン受け取り処理の説明用の画面イメージを示す図（その１）である。

[図10]実施形態３に係るトークン受け取り処理の説明用の画面イメージを示す図（その２）である。

[図11]実施形態３に係るトークン受け取り処理の説明用の画面イメージを示す図（その３）である。

[図12]保持しているトークンの保管場所変更を指示する場合の画面イメージを示す図である。

[図13]トークンの保管方法の選択肢の説明用の画面イメージを示す図である。

発明を実施するための形態

[0009] 以下、添付図面を参照しながら各実施例について詳細に説明する。

[0010] ［実施形態１］

図１は実施形態を実現するシステムの全体構成図である。

[0011] ブロックチェーンネットワーク１００は多数のコンピュータがお互いに接続されたネットワークであり、接続されている各コンピュータをノードと呼ぶ。各ノードは外部からブロックチェーンネットワーク１００に通知された処理依頼を記録すると共に、利用者からの処理依頼に応じた処理を実行し、その結果をノードが管理しているストレージに記録する。処理依頼は各ノードに伝達され、それぞれのノードがその処理依頼に対して同じ処理を実行して出力を記録することにより、分散環境下においても各ノードが全く同じ情報を保持することを実現する。このブロックチェーン上で実行する処理のことをスマートコントラクトと言う。

[0012] スマートコントラクトは各ノードで実行されるコンピュータプログラムであり、処理依頼と同様、ブロックチェーンネットワーク１００がプログラム

の登録依頼を受けた後、それを各ノードに配布して登録する。トークン処理部２００はスマートコントラクトであり、利用者からのリクエストに応じてトークンを制御する。本実施形態ではトークンの発行を例として説明する。

[0013] トークン制御処理受付部３００はブロックチェーンネットワーク１００とのやり取りを実施するサーバであり、利用者端末４００からの要求を受けてトークン処理部２００に依頼をし、その応答を利用者端末４００に返す。利用者端末４００は利用者が利用する情報処理装置であり、スマートフォンやＰＣなどがこれにあたる。配信手段Ａ～配信手段Ｃ（５００Ａ～５００Ｃ）は利用者に対してトークンに関する情報（例えば後述するトークン制御情報の一部又は全部）を提供するものである。具体的には、ＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）、ＱＲコード、ＮＦＣ（Ｎｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、音声、画像、ビーコン情報、位置情報、外部サーバの挙動（例えば、ＳＮＳ（Ｓｏｃｉａｌ Ｎｅｔｗｏｒｋｉｎｇ Ｓｅｒｖｉｃｅ）のＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）情報）など利用者端末４００と連携して各種データを提供するものである。なお、利用者がブロックチェーンネットワーク１００と直接やり取りする場合、利用者の端末にはウォレットと呼ばれるブロックチェーンで利用する秘密鍵を管理するソフトウェアやハードウェアが利用される。利用者端末４００にこれらがインストール済みであれば、トークン制御処理受付部３００を介さずに直接利用者端末４００からトークン処理部２００に処理依頼を投げてもよい。本実施形態においては、多くの利用者がウォレットを保持していないことを想定し、トークン制御処理受付部３００を使う例で説明する。

[0014] 図２はブロックチェーンネットワーク１００を構築する各ノードの構成図である。ノード端末１１０は通常のコンピュータであってよく、ＣＰＵ１２０、メモリ１３０、ストレージ１４０、ストレージを接続するためのインタフェースであるストレージＩ／Ｆ１５０、外部のキーボードやマウス、ディ

スプレイと接続するための入出力Ｉ／Ｆ１６０、外部のコンピュータと接続してネットワークを構築するためのネットワークＩ／Ｆ１７０で構成されてよい。図示していないが、その他の演算処理部としてＧＰＵやＦＰＧＡを持つものもあり、これらの機能部にマイニングなどのブロックチェーン運用に必要な処理をオフロードしているものもある。ノード端末１１０のストレージ１４０にブロックチェーンネットワークの情報が格納され、スマートコントラクトの処理はストレージ１４０からメモリ１３０に読みだされてＣＰＵ１２０（場合によってはＧＰＵやＦＰＧＡ）で実行される。なお、トークン制御処理受付部３００、利用者端末４００も通常のコンピュータであり、ノード端末１１０と同様の構成である。

[0015] 利用者にＮＦＴなどのトークンを配信する際には、事前にトークンを作成する、またはリクエストに応じてトークンを作成する仕組みを準備する必要がある。その準備部分と実際に利用者がトークンを受け取るまでの処理を示したものが図３である。以下「ＮＦＴを新規に配布する」ものとして、この処理手順について説明する。

[0016] まず、ＮＦＴを配布するにあたり、ＮＦＴを管理・運用するためのスマートコントラクトを開発する必要がある（ステップＳ１０００）。開発したものにバグなどがないことが確認できたら、ブロックチェーンネットワーク１００に、作成したスマートコントラクトを登録する（ステップＳ１０１０。ブロックチェーンネットワーク１００、スマートコントラクトはこのフローに図示していない）。これと並行してＮＦＴとして参照するコンテンツを作成し、スマートコントラクトに登録すべき情報を用意する（ステップＳ１０２０）。スマートコントラクトとコンテンツが準備できたら、その情報をスマートコントラクトに設定し、開発作業としては終了になる（ステップＳ１０３０）。なお、本実施形態ではスマートコントラクトをブロックチェーンネットワーク１００に登録した後でコンテンツ情報を登録する形で説明したが、スマートコントラクト登録後にコンテンツ情報を設定するのではなく、全ての情報を用意してスマートコントラクトとしてコンテンツ情報も確定し

た上で登録する、という手順で進める場合もありうる。

[0017] 本実施形態においては、スマートコントラクトやコンテンツの開発・作成と並行して配信手段の準備が可能とされる。これを実現するのが設定情報生成処理（ステップＳ１１００）である。ここでは、設定情報として十分な範囲を持った乱数を利用する。例えば、２の２５６乗の範囲の数値を乱数で割り振る、などである。設定できる空間が広ければ広いほど生成した乱数が一致する可能性は低くなる。配信手段によっては、印刷や専用デバイスにデータ書き込みなどの作業が必要になる。ＱＲコードなどの配信手段で提供する情報とＮＦＴで管理するＩＤ情報を１対１に対応させようとすると、ＮＦＴ側の開発完了を待つ必要があるが、アクセスすべきサイトのＵＲＬなど一定の準備やルールが確定できれば、その後は乱数を使って自由に配信手段を生成することができる。こうして開発と独立で作業を進めることができるとともに、配信手段側の作業も機械的に実施することができる。または、乱数ではなく各配信手段に対して利用する数値範囲を割り当てて通番を振るというルールを定義してもよい。

[0018] 例えば、ＱＲコードは１から１００００、ＮＦＣは１０００１から２００００、という形で全て一意となるように番号を割り当てる。こうして生成した情報を配信手段に設定し（ステップＳ１１１０）、利用者に配布する（ステップＳ１１２０）。開発と配布を分離できることにより、事前販売も実現することができ、他の製品とのコラボレーションなどもやりやすくなる。配信手段から利用者端末に提供される情報が図４のトークン制御情報６００である。ここでは、制御情報としてＮＦＴの発行または配布で利用する乱数または事前定義した通番が設定され、付加情報としてＮＦＴ取得用のアクセス先ＵＲＬなどが格納されることを想定している。付加情報はアクセス先ＵＲＬ以外のものが含まれてもよい。例えば、配信手段の種類や管理番号、販売開始日時、提供会社のＵＲＬなどである。

[0019] こうして、例えば配信手段として印刷されたＱＲコードを利用者が受け取り、これをスマートフォンなどで読み込んでアクセス先の情報とＮＦＴ引き

換え用として設定された乱数を取得する（ステップＳ１２００）。次に利用者は取得したアクセス先に読み込んだ乱数を通知して、ＮＦＴの取得を要求する（ステップＳ１２１０）。なお、利用者がアクセス先に情報を通知する際は、利用者がＮＦＴを受け取るための情報（パブリックブロックチェーンの場合、利用者のアドレスが相当する。以降、この情報をアドレスとして説明する。）なども送信する。

[0020] 本実施形態ではアクセス先としてトークン制御処理受付部３００が設定されるため、ここが利用者からのリクエストを受け付ける（ステップＳ１３００）。図５はトークン制御処理受付部が受信した情報を格納する受信データ格納部７００である。なお、送信者欄にはブロックチェーンネットワーク１００で利用者のアドレスが格納されるが、必要であれば利用者のＩＰアドレスなどを格納して確実に個人または個人の利用者端末４００を特定する情報を格納してもよい。また、トークン制御情報の付加情報の全体または一部が不要であればこれらを削除した上で受信データ格納部７００のトークン制御情報欄に格納してもよい。

[0021] トークン制御処理受付部３００は受信データの格納時に同じトークン制御情報を持つものがないかを確認し、既に登録済みであった場合はその配信手段の内容が利用済みであったことを利用者に伝え、処理を終了する。あるいは、「一人３個まで」というように同じ利用者が複数個持つことを許容する場合は、その数を超えていないかどうかをチェックして超えていれば処理を終了する。一利用者あたりの上限数のチェックはトークン制御処理受付部３００でなく、スマートコントラクトでチェックしても構わない。チェックを実施して問題がなければそのまま受け取った情報を格納し、受信した情報を使ってＮＦＴの発行または設定をスマートコントラクトに依頼する（ステップＳ１３１０）（スマートコントラクトはこのフローに図示していない）。発行または設定のリクエストを受け取ったスマートコントラクトは、通知に不備がないことを確認した上で対象のＮＦＴの保有者を利用者に変更する。または新規にＮＦＴを発行して保有者を利用者に設定する。なお、ＮＦＴを

管理・運用するスマートコントラクトはＮＦＴのＩＤと保有者の情報を保持している。これがトークン管理情報８００である。図６は、スマートコントラクトのトークン管理情報８００の一例を示す図である。一番シンプルなやり方は、通知された乱数や通番をそのままＩＤとして設定し、そのＩＤに通知された利用者のアドレスを関連付けてトークン管理情報８００に格納する方法である。スマートコントラクトの実装上の制約からとりうるＩＤの上限値はあるが、乱数や通番を割り当てる際にそのことを考慮して送信情報に設定する情報を定義すれば、この制約は回避できる。また、多くの場合、ＮＦＴは１００個、１００００個などの上限を設けている。この場合に対応する一例として、受け取った乱数の剰余を求めて対応する方法がある。例えば配布するＮＦＴが１００個なのであれば、受け取った乱数を１００で割って、その余りをＩＤとして利用する。剰余を使うことで、どのような値が通知されても、一定範囲に収めることができる。しかし、この場合は後から通知された乱数の剰余を算出すると、利用済みのＩＤと同じ値になることが考えられる。この場合、算出した値の次の値をＩＤにするクローズドハッシュ法を使うなどの工夫で対応することができる。通番を割り振る際に個数上限を想定済みであれば、そのままその値をＩＤとして使えばよい。

[0022] さらに、ＮＦＴの発行数に制約をつけて流通数を少なくして希少性を出すという取り組みも行われている。本実施形態であれば、配信手段で提供する個数を制限することで実現できる。

[0023] 別の実現方法として、ＩＤの範囲により希少性を表現する場合も考えられる。例えば１００個のＮＦＴがあるが、１から１０までのＮＦＴの価値が高い（特別なコンテンツと関連付けるなど）という場合である。これも剰余で実現できるが、クローズドハッシュ法を使ったときに「剰余は１０なのにずれて１１になり価値の高いＮＦＴがもらえない」ということが発生しうる。このような場合は単純にクローズドハッシュ法を使うのではなく、剰余が１から１０になったものはこの範囲でクローズドハッシュ法を使う、とすれば対応できる。

[0024] ただ、本実施形態では複数の配信手段の利用を想定しているため、ある配信手段で価値の高いＮＦＴを大量に配布してしまう可能性がある。配信手段によっては受信できる利用者が限られる場合もありえるため、配布の公平性も担保する必要がある。それを管理するのが、例えば図７に示すようなトークン配布数管理９００であってよい。これは利用を想定している配信手段において、どのＩＤをどのくらい割り当てるかを管理する情報であり、最大割り当て数と配布開始後は実際に割り当てた数を管理するために利用する。スマートコントラクトで利用者を割り当てる際に、この情報も参照して、ＩＤを割り当てる。ある配信手段で最大数を割り当てた後に通知された送信情報の剰余がその範囲となった場合にどのＩＤを割り当てるかは、開発者がそのＮＦＴのコンセプトや運用ルールなどからスマートコントラクトに実装するものとする。ここでは単純にＩＤ範囲だけを定義したが、販売を開始してから１ヶ月以内、３ヶ月以内などの時間的な制約や、総受信数に対する統計値などを使ってもよいし、これらを組み合わせたルールを作成してもよい。

[0025] 本実施形態では、「いずれかの配信手段から入手した情報を使ってＮＦＴを取得する」場合についての説明であった。実際には同じ場所でＮＦＴ配布情報がＱＲコードと放送音声で提供されるなど複数の配信手段が利用される場合がある。この時、複数の配信手段によるトークン配布情報を送信した場合のみＮＦＴを配布する、複数の配信手段を利用すると特別なＮＦＴを配布するといった応用も考えることができる。このように複数の配信手段を組み合わせることで、送信情報や付加情報に追加情報を加えることなく、場所や時間に応じたＮＦＴ配布を実現できる。また、「ＱＲコードを持っているだけでは配布しない」といった、ある程度のセキュリティ対策にもなりうる。

[0026] また、本例は「ＮＦＴの発行」処理を想定して説明したが、発行だけでなくＮＦＴを含めたブロックチェーンネットワーク１００上のトークンに対する処理の実施をこの仕組みで実現することができる。例えば、ゲームに利用されるＮＦＴが「ある特定の日時にある場所に行けばパラメータが向上する」など、現実世界とＮＦＴ情報とを連携させるサービスを構築する際にも活

用できる。

[0027] 本実施形態では、利用者がトークン制御処理受付部３００経由でトークン処理部２００に処理を依頼する構成を例として説明しているが、利用者端末４００にウォレットが搭載されるのが当たり前になった場合、利用者は直接トークン処理部２００にトークン制御情報６００を通知して処理を依頼する形になることが多いと考えられる。この場合、トークン制御処理受付部３００にて管理している受信データ格納部７００はスマートコントラクトであるトークン処理部２００で管理することで本実施形態を実現できる。

[0028] ［実施形態２］

上述した実施形態１の方法により、コンテンツ作成と独立して配布用情報を作成でき、様々な配布手段で事前に利用者にＮＦＴなどのトークンを配布することができる。しかし、個数制限や高価値のトークン配布に配布手段を単純に利用すると悪用される恐れがある。例えばＱＲコードを利用する場合について考えると、ＱＲコードの情報自体は誰でも受け取ることができて、その内容を簡単に確認することができる。つまり、アクセス先のＵＲＬなどの情報とＩＤ割り当てに利用する乱数や通番を利用者が簡単に知ることができる。また、ＱＲコード作成ツールもＷｅｂなどで公開されているため、ＱＲコードを受け取ると利用者側でオリジナルの情報を加工した上でトークン制御処理受付部３００に処理を依頼することができてしまう。このため、「利用者が望むＩＤを持つトークンが取得できてしまう」「配布手段から情報を入手することなくいくらでもトークンが取得できてしまう」という大きく２つの課題がある。

[0029] 「任意のＩＤのトークンが取得可能」については、受信側で乱数を加工することで対応できる。トークン制御処理受付部３００が利用者からのリクエストを受け付けた（ステップＳ１３００）際に、乱数を生成してこれと合成（ＸＯＲするなど）して新しい情報を作成し、これをＩＤ割り当ての情報として利用する。乱数生成でなく、ソルト（任意の可変情報）と通知された情報からハッシュ値を求めてそれを割り当て情報として使ってもよい。利用者

から通知された情報をそのまま使わないことで、この問題は対応できる。なお、ここではトークン制御処理受付部３００で乱数作成＆合成またはハッシュ値作成する例を説明したが、同様の処理をスマートコントラクトで実施してもよい。通常、スマートコントラクトでは乱数を生成することはできないが、外部から信頼できる情報を提供するオラクルという仕組みがある。これを使って乱数を取得することでスマートコントラクトでも乱数を利用することができる。トークン制御処理受付部３００はトークン提供者の管理下にあることが多いため、利用者から見える場所であるブロックチェーンネットワーク１００上に情報を公開して公平性を提示するためにスマートコントラクトで実装するということはありえる。

[0030] 後者の「利用者が任意個のトークンを取得できてしまう」ことはより大きな問題である。一利用者が複数個を発行または設定することを許容している場合でも、送信者情報としてブロックチェーンネットワーク１００のアドレス情報しか保持していない場合、利用者はアドレスを自由に複数個作成することができるため、個数制限は制約として機能できない。この問題に対する１つの方法として、配布手段からトークン制御情報を受領する際に名前や住所、メールアドレスなどの利用者情報を収集し、利用者がトークン制御情報を利用する際に利用者情報も入力してもらうという形にすればこの問題に対応はできる。しかし、ＱＲコードやＮＦＣなどの配信手段だけでは利用者の詳細情報を取得することが実現できず、別のシステムが必要になるため運用も手間がかかる。また、利用者にとっても手間を強いられ、人によっては不必要に個人情報を提供するように感じる人も出てくるため、トークンを受け取ってもらえないという課題が生じる。

[0031] そこで、本実施形態ではこの問題に対応するために配信手段で伝達するトークン制御情報を暗号化して提供することで対応する。手順自体は図３と同じであるが、一部処理が追加になる。その内容について、以下説明する。

[0032] まず、トークン制御情報６００に格納する制御情報を暗号化するために、暗号鍵を用意する。ここでは公開鍵暗号を使う場合について説明するが、Ａ

ＥＳなどの共通鍵暗号を使う場合でも同様である。まずトークン提供者がトークン作成を実施する前に公開鍵ペアを作成する。秘密鍵はトークン提供者が管理すると共に安全に利用できる形でトークン制御処理受付部３００に設定し、公開鍵を配信手段向けに情報設定作業を行う人に提供する。配信手段では乱数または通番生成に受け取った公開鍵を使って制御情報を暗号化する（ステップＳ１１００）。なお、トークン制御情報６００の付加情報はアクセス先のＵＲＬなどの情報を格納する。処理上、他に秘匿したい情報があれば、その部分も暗号化して格納してもよい。また、情報生成に利用する公開鍵は配信手段にトークン制御情報６００を設定する設定者だけが利用し、他の作業者や外部に公開してはいけない。以降の処理は図３の通りだが、ステップＳ１３００で利用者からトークン制御情報６００を受け取ったトークン制御処理受付部３００は、設定された秘密鍵を使って送信情報を復号して設定された乱数などを取得して以降の処理を実施する処理が追加になる。

[0033] このようにして、トークン制御情報６００における制御情報を暗号化し、利用者には暗号に必要な鍵情報を公開しない仕組みを構築する。

[0034] 上記ではトークン制御処理受付部３００にて秘密鍵を管理する方法について説明した。しかし、内部犯まで考慮すると秘密鍵を持ち続けることがリスクになる可能性もある。そこで、鍵をスマートコントラクトに持たせることで管理自体を容易にする方法について説明する。

[0035] 鍵もデータなのでスマートコントラクトに鍵を持たせること自体は簡単である。しかし、スマートコントラクトはブロックチェーンネットワーク１００にアクセスする者全員に公開される情報であるため、そのまま鍵を持たせるわけにはいかない。そこで、公開鍵暗号を利用する。公開鍵暗号の技術的特徴から、秘密鍵から公開鍵の導出は容易だが、公開鍵から秘密鍵の導出は莫大な計算時間がかかるため、現実的に不可能という特徴がある。この特徴を活かし「公開鍵」をスマートコントラクトに登録する。トークン制御情報６００の暗号化処理は先ほどと同様である。トークン提供者が公開鍵ペアを生成し、「秘密鍵」を配信手段向けに情報設定作業を行う人に提供し、生成

するトークン制御情報６００をこの鍵で暗号化する。なお先ほどと同様、秘密鍵が漏洩することないよう作業しなければならない。全てのトークン制御情報６００が作成できれば秘密鍵は不要になるため、破棄してもよい。将来的にコンテンツ追加などで同じ秘密鍵を利用する可能性がある場合は、トークン提供者がこれを厳密に管理しておく。また、この場合はトークン制御処理受付部３００で復号できないので、暗号化されたデータと送信者の情報を受信データ格納部７００に格納して管理する。トークン制御処理受付部３００がスマートコントラクトに発行または設定を依頼（ステップＳ１３１０）した後、これを受け取ったスマートコントラクトは自身が持つ公開鍵で通知された情報を復号して利用する。このように、通常の公開鍵ペアの持ち方と逆の持たせ方をすることで、スマートコントラクトに登録した鍵情報で復号はできても暗号化できないことが担保できる。こうして、スマートコントラクトに鍵情報を登録しても安全にトークン制御情報６００を利用することができる。

[0036] ［実施形態３］

利用者がＮＦＴなどのトークンを受け取る際には、ブロックチェーンネットワーク１００で利用者を一意に特定する情報が必要になる。Ｅｔｈｅｒｅｕｍなどのパブリックブロックチェーンでは利用者が管理している公開鍵ペアの公開鍵から生成したアドレスがこれに相当する。しかし、アドレスを持つためにはその元となる公開鍵ペアを管理するためのウォレットなどのアプリまたはハードウェアが必要になり、一般の利用者からは利用しづらいものになる。そこで、本例ではこの問題を解決する方法について説明する。

[0037] 図８は、実施形態３に係るトークン受け取り処理の説明図である。図８に示すトークン受け取り処理は、図３のステップＳ１２００の処理としてステップＳ１２１０の前に実行されてよい。

[0038] 図３のステップＳ１２００では、上述したように、利用者は配信手段から情報を取得する。具体的にＱＲコードの場合で説明すると、配信手段はＱＲコードを利用者に提供する。この提供方法は人が紙を渡すのでも、会社など

の入り口にＱＲコードを掲示しておくのでも、インターネット経由で配信するのでも、どのような形でもよい。利用者はスマートフォンのカメラアプリやスキャナアプリを使ってＱＲコードを読み取る（ステップＳ２１００）。なお、配布手段から提供される方法により、起動するアプリが変更になってもよい。アプリがこれを読み取るとＵＲＬを提示してアクセスするかどうかを確認し、「アクセスする」と指示した後、スマートフォンはブラウザを立ち上げて（ステップＳ２１１０）、トークン制御情報６００で指定されたＵＲＬ先にアクセスする（ステップＳ２２００）。なお、「アクセスする」との指示は、自動的に発生されてもよい。すなわち、アプリがＱＲコードを読み取ると、トークン制御情報６００で指定されたＵＲＬ先へのアクセスが自動的に実現されてもよい。

[0039] この時に、アクセス先である配布サイトに係るトークン制御処理受付部３００がユーザ側処理送信を実行し（ステップＳ２３００）、トークン制御処理受付部３００が用意しているページ内のＪａｖａＳｃｒｉｐｔ（登録商標）などのプログラムが利用者用のアドレス作成の元になる公開鍵ペアを生成して（ステップＳ２２１０）、公開鍵ペア及び／又はアドレス情報をブラウザのローカルストレージに格納する処理を実行する（ステップＳ２２２０）。こうして利用者は自身が意識することなくブロックチェーンネットワーク１００で一意であるアドレス情報を取得することができる。また、ローカルストレージはそのスマートフォンの利用者しか利用できないため、比較的安全であるといえる。なお、変形例では、公開鍵ペアは、ブラウザのローカルストレージに代えて、ブラウザのセッションストレージ、及びブラウザのクッキー等のような他のブラウザのストレージに記憶されてもよいし、ブラウザのストレージ以外の記憶領域（例えば利用者端末４００内の記憶領域や、トークン制御処理受付部３００等によりアクセス可能なサーバ装置の記憶領域等）に記憶されてもよい。

[0040] ただし、ローカルストレージは利用者操作により削除できてしまう。公開鍵ペア（特に秘密鍵）が削除されてしまうと、利用者に付与されたトークン

の移動が永久に利用できなくなってしまう。それを回避するために公開鍵ペアの作成後にそれら、またはそれらの生成に利用した情報をＱＲコード化して利用者に表示する（ステップＳ２２３０）。すなわち、ブラウザのローカルストレージから公開鍵ペア（特に秘密鍵）が削除された場合でも復元可能とできる復元手段（復元情報）を利用者に通知する。これにより、利用者は表示された画面をキャプチャするなどしてブラウザのローカルストレージ以外の場所（例えばスマートフォン内の記憶装置や他のクラウドストレージ）に保存しておく（ステップＳ２１２０）ことができる。この情報があれば、利用者はアクセス時に生成された公開鍵ペアをいつでも生成でき、付与されたトークンを無駄にすることがなくなる。図９には、復元手段の保存をユーザに促すＵＩ９９０の一例が示されている。この場合、ＵＩ９９０は、ＱＲコードＣ１２や、復元手段の保存をユーザに促すメッセージを含む。なお、ＱＲコードでなく、複数の単語など、生成した公開鍵ペアを復元できるものであればどのようなものでもよい。ブラウザのローカルストレージに格納する公開鍵ペアは、受け取り用の暫定情報ともいえる。このため、利用者が恒常的に利用するアドレスを入手した後、対象のトークンと恒常利用アドレスと復元情報、または対象のトークンと恒常利用アドレスとローカルストレージに格納した秘密鍵の情報とをトークン制御処理受付部３００に提供することで、利用者のローカルストレージに格納したアドレスから恒常利用アドレスに対象トークンを送信する機能も提供する。この機能のＵＩイメージが図１２である。「Ｆｒｏｍ」はローカルストレージに格納したアドレスであるため、自動的に設定されるが、手動で設定（入力）されてもよい。「Ｔｏ」は、恒常利用アドレス又はその類（例えば、代理処理を経る場合は、代理処理用のアドレス等）のような、対応するウォレットを特定可能なウォレット情報を入力する欄であり、利用者自身に入力してもらう。「Ｔｏ」はＱＲコードなどから読み取って設定してもよい。復元情報はここでは別ファイルとして保持されているものとしている。

[0041] ついで、ユーザからの指示に応じて、ブラウザにおける生成用情報を通知

する処理（ステップＳ２２４０）を介して、ＮＦＴの取得を要求する（図３のステップＳ１２１０）処理が実行される。なお、配布手段からはトークン制御情報６００が通知され、ここから必要な情報を取得・暗号化などの処理は、生成用情報通知に係る処理（Ｓ２２４０）において実行されてよい。なお、トークン制御情報６００の一部又は全部は、対応するＵＲＬ内に組み込まれもよいし、対応するＵＲＬに基づき展開されるＷＥＢページ内に含まれてもよい。

[0042] 例えば、図９に示す例では、「保存したので進む」と付されたボタンＢＴ９９０をユーザがスマートフォン上で操作すると、ステップＳ２２４０を介して図３のステップＳ１２１０以降の処理が実行される。この場合、ユーザのスマートフォン上では、図１０に示す画面９９０を介して、図１０に示すＵＩ９９１が出力されてよい。図１０に示す例では、取得対象のトークン（ＮＦＴ）を表す画像Ｇ１０やその説明Ｇ１１、取得中であることを視覚的に示す処理中表示Ｇ１２等を含む画面９９０が表示されている。ユーザは、画面９９０を見ることで、取得中のＮＦＴについての情報を得ることができる。なお、説明Ｇ１１には、配布元に係る広告情報が含められてもよい。また、図１１に示すＵＩ９９２は、取得完了時の画面であり、「ＮＦＴ保存完了！」なるメッセージを含む。なお、ここでいう「保存」は、上述したように、ブラウザのローカルストレージへの保存である。図１１に示すＵＩ９９２は、保存完了したトークン（ＮＦＴ）を表す画像Ｇ１０やその説明Ｇ１３等を含む画面９９０が表示されている。説明Ｇ１３は、より詳細な説明画面へのリンクや、広告情報に係るサイトへのリンク等を含んでもよい。

[0043] なお、図８に示す例では、復元手段の保存を促す処理（ステップＳ２２３０）が実行されるが、本処理は、省略されてもよいし、後から通知する態様で事後的に実行されてもよい。また、図８では、パブリックブロックチェーン用のアドレス作成処理は明示していないが、アドレスは公開鍵から生成されるため、公開鍵ペア作成に係る処理（Ｓ２２１０）にて作成されることとしてよい。

[0044] また、本実施例において、トークン制御情報６００で指定されたＵＲＬ先に基づく表示情報（この場合、ＷＥＢ画面）は、取得対象のトークン（ＮＦＴ）の保存先を選択可能なＵＩを有してもよい。例えば、図１３に示す例では、ウォレットを所有しているユーザが選択可能なボタンＢ２１と、ウォレットを所有していないユーザによる選択が好適なボタンＢ２２とを含む。ユーザがボタンＢ２１を操作した場合は、恒常利用アドレスへの対象トークンの対応付けが実行され、図１２を参照して上述した処理を不要とすることができる。他方、ユーザがボタンＢ２２を操作した場合は、図８を参照して上述した各種処理が実行され、ウォレットを所有しているユーザに対しても対象トークンの付与が可能となる。このようにして、取得対象のトークン（ＮＦＴ）の保存先を選択可能なＵＩを提供することで、幅広いユーザに対して利便性の高いサービスを提供できる。

[0045] また、ブロックチェーンネットワーク１００に処理を依頼する場合は多くのブロックチェーンではガス代と呼ばれる手数料が発生する。このガス代は各ブロックチェーンにおいて基本となるトークンを使って支払う必要があるが、一般の利用者はガス代用のトークンを確保すること自体が難しい。そこで、利用者の公開鍵ペアを使ってブロックチェーンネットワーク１００向けの処理を作成するが、依頼に必要なガス代はトークン制御処理受付部３００が負担する方法を提供して対応する。利用者端末４００はローカルストレージに格納した公開鍵ペアの秘密鍵を使い、自身が配信手段から受け取ったトークン制御情報６００に署名して確実に使う旨をトークン制御処理受付部３００通知することで、ガス代負担を依頼する。トークン制御処理受付部３００では送信者情報と署名から確実に送信者を確認することができ、その確認によりガス代負担を許可する。また、この代理依頼を実行できるスマートコントラクトをブロックチェーンネットワーク１００に準備しておき、トークン制御処理受付部３００からはそのスマートコントラクトに処理を依頼することで、代理処理を実現する。このように、ブロックチェーンネットワーク１００に対する処理をトークン制御処理受付部３００に代理してもらうこと

により、利用者はガス代を意識せずにブロックチェーンネットワーク１００に処理を依頼することができる。上記で恒常的なアドレスに保有トークンを送信する方法についても説明したが、秘密鍵情報などを提供せず代理手段でも実現できる。大きく２通りあり、一つは利用者がローカルストレージに格納した公開鍵ペアのアドレスから自身が用意した恒常利用アドレスに対象トークンを送信する処理依頼を作成し、ローカルストレージの秘密鍵で署名してその実行をトークン制御処理受付部３００に依頼する。もう一つは、トークン制御処理受付部３００に対象トークンを操作する権限を付与する処理依頼を作成してローカルストレージ等に格納した秘密鍵で署名して、その実行をトークン制御処理受付部３００に依頼する。いずれの場合も、リクエストを受け取ったトークン制御処理受付部３００はガス代を設定した上で代理処理を実現するスマートコントラクトに処理を依頼して処理を完了させる。なお、トークン保管場所の変更をこれらの手段で実現する場合は、図１２のＵＩ１０００には復元情報の項目は不要であり、２通りの方法を提示して選択してもらう、システムとして２通りのうち片方を利用するよう実装し、ＵＩ上は選択肢をなくす、といった方法が考えられる。実際に代理処理をする場合、図５の受信データ格納部７００を参照して、要求者が正しいかどうかを確認した上でブロックチェーンネットワーク１００に代理処理を依頼する。また、受信データ格納部７００の情報を参照して代理実行の可否を決定してもよい。例えば、ＱＲコードは配布数が多いのでガス代は補助しないが音声経由でＮＦＴを取得した人は許可する、ＮＦＣで取得した人で３日以内の実施であればガス代負担と将来ガス代として利用できる少額をプレゼントし、１ヶ月以内であればガス代負担のみ、それ以上は許可しないなどの制御をしてもよい。このような制御をすることで、特定の配信手段を重みづけることができ、ＮＦＴの配布方法のバリエーションを増やすことができる。

[0046] ［その他の実施形態］

以上、各実施例について詳述したが、特定の実施例に限定されるものではなく、特許請求の範囲に記載された範囲内において、種々の変形及び変更が

可能である。また、前述した実施例の構成要素を全部又は複数を組み合わせることも可能である。

[0047] 以上の各実施形態に関して、更に以下の付記を開示する。

[0048] ［付記１］

複数の計算機で構成されるブロックチェーンネットワーク上で流通するトークンを制御するシステムであって、

前記トークンを管理し処理するトークン処理部と、

利用者端末からの指示によって前記トークン処理部にトークン制御情報を通知するとともに、前記トークン処理部からの結果を利用者端末に送信するトークン制御処理受付部と、

前記利用者端末に情報を配信する配信手段と、を有し、

前記配信手段は、前記利用者端末に配信する前記トークン制御情報の一部に乱数または所定のルールで設定された情報を設定し、

前記利用者端末は、前記トークン制御情報を、前記トークン制御処理受付部を介してまたは介さずに前記トークン処理部に通知し、

前記トークン制御処理受付部または前記トークン処理部は、利用者端末から受け取った前記トークン制御情報を、該トークン制御情報を送信した前記利用者端末に関する利用者情報と共に格納し、

前記トークン処理部は、前記配信手段によって前記トークン制御情報に設定された前記乱数または前記ルールで設定された情報を参照して、前記乱数または前記ルールで設定された情報を前記トークン処理部が管理するトークンの特定情報として利用することを特徴とするトークン制御システム。

[0049] ［付記２］

前記トークン処理部は、前記トークン制御情報に格納された前記乱数または前記ルールによって設定された情報を加工することで該情報を一定の範囲に収める情報加工処理部を有し、

前記加工処理部は、前記乱数または所定のルールによって設定された情報を加工した第１の加工情報が前記トークン制御情報に格納された既存の情報と

同じ情報であった場合、前記第１の加工情報をさらに加工して第２の加工情報にすることで、前記トークン制御情報を一定の範囲内に収めるとともに、前記第１の加工情報または前記第２の加工情報を、前記トークン処理部が管理するトークンを特定するための情報として利用し、前記特定されたトークンに対して制御を実施することを特徴とする付記１に記載のトークン制御システム。

[0050] ［付記３］

前記トークン処理部は、前記加工処理部において情報を一定の範囲に収めると共に、前記範囲をさらに分割して重みづけし、前記加工処理部において既存の情報と同じ情報になった場合において、前記加工処理部において前記分割範囲に収まるように再加工し、前記分割範囲に収まった情報をトークンを特定するための情報として利用し、前記特定されたトークンに対して制御を実施することを特徴とする付記２に記載のトークン制御システム。

[0051] ［付記４］

前記トークン処理部は、前記加工処理部において情報を一定の範囲に収める際に、前記トークン制御情報に格納される付加情報を踏まえて情報を加工することを特徴とする付記２または付記３に記載のトークン制御システム。

[0052] ［付記５］

前記トークン処理部は、前記加工処理部において、前記配信手段に応じて割り当て範囲および割り当て数を制御することを特徴とする付記２から付記４に記載のトークン制御システム。

[0053] ［付記６］

前記トークン制御処理部または前記トークン処理部は、前記利用者端末が前記トークン制御情報を送信する際に、送信された日時および／または前記配信手段の組み合わせに応じて処理の受付可否、前記加工処理部の加工処理方法、前記範囲の分割範囲の重みづけを変更した上で、前記特定されたトークンに対して制御を実施することを特徴とする付記３から付記５に記載のトークン制御システム。

[0054] ［付記７］

前記情報加工処理部は、情報を一定の範囲に収める際に、前記トークン処理受付部、または前記トークン処理部が前記ブロックチェーンネットワーク上で稼働する乱数生成機能を呼び出して乱数を生成し、前記乱数または所定のルールで設定された情報と前記乱数を組み合わせて第３の加工情報を生成し、前記第３の加工情報を該情報加工処理部の入力として利用することを特徴とする付記２から付記６に記載のトークン制御システム。

[0055] ［付記８］

前記配信手段は、前記トークン制御情報のうち、前記トークン処理部が利用する情報を暗号化して情報を作成し、前記トークン制御処理受付部または前記トークン処理部は復号用暗号鍵を保持し、前記復号用暗号鍵を使って復号して利用し、前記トークン処理部が復号する場合は公開鍵ペアの公開鍵を前記トークン処理部に登録することを特徴とする付記１から付記７に記載のトークン制御システム。

[0056] ［付記９］

前記利用者端末は、前記トークン制御情報を前記トークン制御処理受付部または前記トークン処理部に送信する際に、前記利用者端末のみが利用することができる記憶部に前記ブロックチェーンネットワークで利用者を一意に特定するために必要な情報を自動で生成し、または前記記憶部に前記一意に特定する情報が格納されている場合はその情報を読み出し、前記生成した一意に特定する情報を設定した上で前記トークン制御情報を送信することを特徴とする付記１から付記８に記載のトークン制御システム。

[0057] ［付記１０］

前記利用者端末は、前記生成した一意に特定する情報を生成した時に、前記一意に生成した一意に特定する情報を復元するための情報を生成するとともに、利用者に提示して保管を指示する通知を行うことを特徴とする付記９に記載のトークン制御システム。

[0058] ［付記１１］

前記利用者端末は、利用者が恒常的に利用する前記ブロックチェーンネットワークにおいて一意に特定する情報を入手した際に、前記利用者端末だけが利用することができる記憶部で管理している前記生成した一意に特定する情報を読み出し、前記トークン処理部で管理されている利用者に利用権限があるトークンを前記生成した一意に特定する情報から、前記恒常的に利用する一意に特定する情報に利用者情報の更新を指示するためのＵＩを提供し、前記ＵＩの指示に応じて前記利用者情報を更新することを特徴とする付記９または付記１０に記載のトークン制御システム。

[0059] ［付記１２］

前記利用者端末は、前記ブロックチェーンネットワークに対する処理要求を前記利用者端末で保持する秘密鍵で署名し、前記トークン制御処理受付部に代理処理を依頼し、前記トークン制御処理受付部は前記ブロックチェーンネットワークに処理要求する際に必要となる手数料を利用者に代わって負担し、前記ブロックチェーンネットワークに処理を依頼することを特徴とする付記９から付記１１に記載のトークン制御システム。

[0060] ［付記１３］

前記利用者端末は、前記トークン制御処理受付部が代理処理を実施する際に、前記トークン制御情報処理受付部に格納された前記トークン制御情報を参照し、前記トークン制御情報の内容に応じて代理処理の実施可否の判断、または代理処理実施時において追加処理すべき作業を確定したうえで前記ブロックチェーンネットワークに処理を依頼し、追加処理も含めて代理処理を実行または代理処理を実行しないことを特徴とする付記１２に記載のトークン制御システム。

符号の説明

[0061] １００…ブロックチェーンネットワーク、６００…トークン制御情報、７００…受信データ格納部、８００…トークン管理情報、９００…トークン配布数管理、１０００…トークン保管場所変更ＵＩ

請求の範囲

[請求項1] ブロックチェーンネットワーク上で流通可能な一のトークンを取得するための取得要求が、利用者端末により生成されることに基づいて、前記一のトークンの取得又は管理を可能とする所定情報を生成するとともに、生成した前記所定情報を前記利用者端末又はサーバ装置に係る所定記憶領域に記憶させる第１処理を実行する、情報処理装置。

[請求項2] 前記所定記憶領域は、ブラウザのストレージを含む、請求項１に記載の情報処理装置。

[請求項3] 前記所定情報は、秘密鍵に係る情報を含む、請求項１に記載の情報処理装置。

[請求項4] 前記一のトークンに係る状態を、ブロックチェーンネットワーク上で前記所定情報を介して管理される第１状態から、利用者によりアクセス可能なウォレットを介して管理される第２状態へと移行させる第２処理を更に実行する、請求項１に記載の情報処理装置。

[請求項5] 前記第２処理は、前記所定情報と、前記ウォレットを特定可能なウォレット情報とに基づいて、実行される、請求項４に記載の情報処理装置。

[請求項6] 前記所定情報を復元可能とする復元情報を前記利用者端末に向けて通知する第３処理を更に実行する、請求項１に記載の情報処理装置。

[請求項7] 前記取得要求は、前記一のトークンに係るトークン制御情報に基づいて生成され、

前記トークン制御情報は、乱数または所定のルールで設定された、前記一のトークンの特定情報を含む、請求項１に記載の情報処理装置。

[請求項8] 前記トークン制御情報は、所定のＵＲＬにアクセスするための情報を含み、

前記取得要求は、前記所定のＵＲＬへのアクセスに基づいて生成される、請求項７に記載の情報処理装置。

[請求項9] 前記取得要求は、前記所定のＵＲＬにおける第１所定入力に更に基づいて生成される、請求項８に記載の情報処理装置。

[請求項10] 前記所定のＵＲＬに基づく表示情報は、前記第１所定入力、及び、前記第１所定入力とは異なる第２所定入力のいずれかを利用者が選択的に入力可能とするＵＩを含み、

前記第２所定入力に基づいて、利用者によりアクセス可能なウォレットを介して前記一のトークンが管理される状態を形成する、請求項９に記載の情報処理装置。

[請求項11] 前記第１処理は、前記所定のＵＲＬに対応付けて用意されたプログラムによりブラウザ上で実行される、請求項８又は９に記載の情報処理装置。

[請求項12] 前記利用者端末は、前記ブロックチェーンネットワークに対する処理要求を前記利用者端末又はブラウザのストレージ上で保持する秘密鍵で署名し、

前記第２処理は、前記所定情報に係るアドレス情報と前記署名された処理要求とに更に基づいて実行され、

前記アドレス情報は、ブラウザにおけるＵＩ上で入力される、請求項５に記載の情報処理装置。

[請求項13] 前記第３処理は、前記通知とともに、前記復元情報を保存するように利用者に促す情報を出力することを含む、請求項６に記載の情報処理装置。

[請求項14] ブロックチェーンネットワーク上で流通可能な一のトークンを取得するための取得要求が、利用者端末により生成されることに基づいて、前記一のトークンの取得又は管理を可能とする所定情報を生成するとともに、生成した前記所定情報を前記利用者端末に係る所定記憶領域に記憶させる第１処理を、コンピュータに実行させるプログラム。

[請求項15] ブロックチェーンネットワーク上で流通可能な一のトークンを取得するための取得要求が、利用者端末により生成されることに基づいて

、前記一のトークンの取得又は管理を可能とする所定情報を生成するとともに、生成した前記所定情報を前記利用者端末に係る所定記憶領域に記憶させる第１処理を、コンピュータにより実行する情報処理方法。