(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)公開番号
特開2022-89542
(P2022-89542A)
(43)公開日　令和4年6月16日(2022.6.16)

(51)国際特許分類	FI			テーマコード（参考）
G06Q 20/38 (2012.01)	G06Q	20/38	310	5L055

審査請求　有　請求項の数　11　OL　（全35頁）

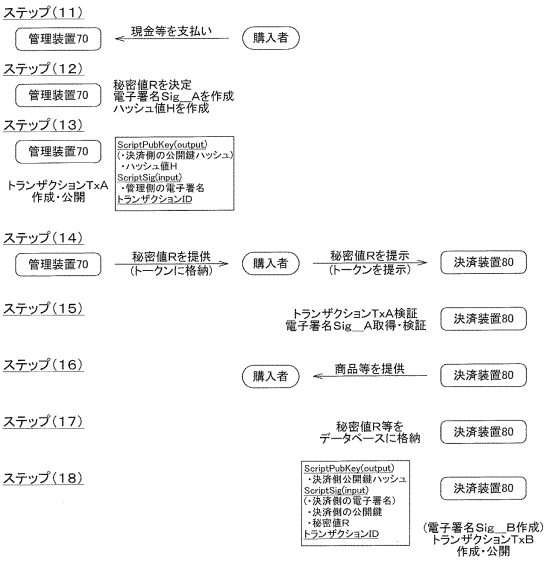
(21)出願番号　特願2020-202004(P2020-202004)
(22)出願日　令和2年12月4日(2020.12.4)

(71)出願人　398034168
株式会社アクセル
東京都千代田区外神田四丁目１４番１号
(74)代理人　100085660
弁理士　鈴木 均
(74)代理人　100149892
弁理士　小川 弥生
(74)代理人　100185672
弁理士　池田 雅人
(72)発明者　星月 優佑
東京都千代田区外神田四丁目１４番１号
株式会社アクセル内

Ｆターム（参考）　5L055　AA73

(54)【発明の名称】　処理システム、処理装置、処理方法及び処理プログラム

(57)【要約】　（修正有）
【課題】ブロックチェーンを用いたロック解除機構によって、プリペイド決済やロック解除のシステムにおける管理用のデータベースサーバの障害に関する問題を解決する処理システム、処理装置、処理方法及び処理プログラムを提供する。
【解決手段】分散型台帳上のＩＤ情報を用いたロック解除システムにおいて、管理装置７０は、決済装置８０が所定動作を行う契機となる所定の秘密情報を決定し、所定動作を行う条件となる特定情報を含む第１トランザクションＴｘＡがネットワークに公開する。決済装置８０は、特定情報が所定の条件を満たす場合には、第１トランザクションＴｘＡをアンロックするための第２トランザクションＴｘＢを作成をネットワークに公開する。
【選択図】図４



【特許請求の範囲】
【請求項１】
第１装置と、第２装置と、を備え、
前記第１装置は、
秘密情報を決定する決定部と、
前記秘密情報を出力する出力部と、
前記第２装置は、
前記秘密情報を譲渡されたユーザから前記秘密情報を受け取る受取部と、
秘密情報を用いてアンロックすることにより取り出し可能な出力情報と、識別情報とを含む第１トランザクションが分散型台帳に公開されたとき、前記受取部により受け取った秘密情報を用いて前記第１トランザクションがアンロック可能な場合、前記第１トランザクションに含まれる前記識別情報を取得する取得部と、
前記取得部により取得した前記識別情報が決められた情報であるとき、指定の処理を実行する実行部と、
を備えることを特徴とする処理システム。
【請求項２】
請求項１に記載の処理システムにおいて、
前記取得部は、
前記第１トランザクションが分散型台帳に公開されたとき、前記受取部により受け取った秘密情報を用いて前記第１トランザクションがアンロック可能な場合、前記受取部により受け取った秘密情報を含む第２トランザクションを分散型台帳に公開し、前記第１トランザクションをアンロックする
ことを特徴とする処理システム。
【請求項３】
請求項１に記載の処理システムにおいて、
前記第１トランザクションは、
前記第２装置の電子署名をさらに用いてアンロック可能である、
ことを特徴とする処理システム。
【請求項４】
請求項３に記載の処理システムにおいて、
前記取得部は、
前記第１トランザクションが分散型台帳に公開されたとき、前記受取部により受け取った秘密情報と、前記第２装置の電子署名とを用いて前記第１トランザクションがアンロック可能な場合、前記受取部により受け取った秘密情報と、前記第２装置の電子署名とを含む第２トランザクションを分散型台帳に公開し、前記第１トランザクションをアンロックする、
ことを特徴とする処理システム。
【請求項５】
請求項１乃至４の何れか一つに記載の処理システムにおいて、
前記識別情報は、
暗号資産の量であり、
前記実行部は、
前記取得部により取得した暗号資産の量が指定の条件を満たすとき、指定の処理を実行する
ことを特徴とする処理システム。
【請求項６】
請求項１乃至５の何れか一つに記載の処理システムにおいて、
前記秘密情報は、
記憶媒体に格納されてユーザに譲渡され、
前記受取部は、

前記記憶媒体を介して前記秘密情報を取得する
ことを特徴とする処理システム。
【請求項７】
請求項１乃至６の何れか一項に記載の処理システムにおいて、
前記第２装置は、
利用履歴を記憶する記憶部
を備えることを特徴とする処理システム。
【請求項８】
請求項２又は４に記載の処理システムにおいて、
前記取得部は、
前記第１トランザクションの改ざん成功確率が十分に低くなったとき、第２トランザクションを分散型台帳に公開する
ことを特徴とする処理システム。
【請求項９】
秘密情報を受け取る受取部と、
秘密情報を用いてアンロックすることにより取り出し可能な出力情報と、識別情報とを含む第１トランザクションが分散型台帳に公開されたとき、前記受取部により受け取った秘密情報を用いて前記第１トランザクションがアンロック可能な場合、前記第１トランザクションに含まれる前記識別情報を取得する取得部と、
前記取得部により取得した前記識別情報が決められた情報であるとき、指定の処理を実行する実行部と、
を備えることを特徴とする処理装置。
【請求項１０】
プロセッサによって実行される処理方法であって、
秘密情報を受け取り、
秘密情報を用いてアンロックすることにより取り出し可能な出力情報と、識別情報とを含む第１トランザクションが分散型台帳に公開されたとき、前記受取部により受け取った秘密情報を用いて前記第１トランザクションがアンロック可能な場合、前記第１トランザクションに含まれる前記識別情報を取得し、
前記取得部により取得した前記識別情報が決められた情報であるとき、指定の処理を実行する、
ことを特徴とする処理方法。
【請求項１１】
プロセッサに実行させる処理プログラムであって、
秘密情報を受け取り、
秘密情報を用いてアンロックすることにより取り出し可能な出力情報と、識別情報とを含む第１トランザクションが分散型台帳に公開されたとき、前記受取部により受け取った秘密情報を用いて前記第１トランザクションがアンロック可能な場合、前記第１トランザクションに含まれる前記識別情報を取得し、
前記取得部により取得した前記識別情報が決められた情報であるとき、指定の処理を実行する、
ことを特徴とする処理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、処理システム、処理装置、処理方法及び処理プログラムに関する。
【背景技術】
【０００２】
スマートフォンの画面に表示させたバーコード等を、店頭のＰＯＳレジに読ませることによって決済を行うコード決済が知られている（例えば、特許文献１参照）。このようなコ

ード決済は、一般にプリペイド型のものが知られており、オンラインでのクレジットカード払いや店頭での現金払いなどによってアカウントにチャージを行い、バーコード等を用いた支払い時には、チャージ金額から必要な金額を引き落とす。
このように支払時にスマートフォンに表示するバーコード等は、アカウントに紐付くＩＤ情報であり、購入者が現金等を事前に支払ったことを証明するものである。
すなわち、プリペイド決済は、金銭の事前支払いによって得られた商品やサービスを受け取る権利に対するロックをＩＤ情報の提示を条件に解除する決済方法であると言える。
プリペイド決済のシステムは、本質的にＩＤ情報に基づくロック解除システムである。
このようなロック解除システムとして、スマートロックのシステムも知られている。作業員等はＩＤ情報を格納したスマートキーを携行し、スマートキーを自動販売機の扉や建物のオートロックにかざしたり、差し込んだりする。管理装置は、データベースサーバに問い合わせ、ＩＤ情報が許可対象であれば、自動販売機や建物の施錠を解除する。
プリペイド残高の不正使用や不正解錠を防ぐために、ＩＤ情報は二度以上使用できないことが望ましい。実際、上記したコード決済では、一度決済に用いたバーコードは再度使えず、バーコードを更新しないと次回の決済を行えないことが知られている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０２０－１７０４４２公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
上記したようなプリペイド決済やロック解除のシステムを構築するためには、ＩＤ情報や、使用状態を管理するためのデータベースサーバが必要となる。
従って、データベースサーバに障害が発生したときには、ＩＤ情報の管理ができず、正常に決済や施錠の解除を行うことが困難である、という問題がある。
本発明は、一側面として、ＩＤ情報に基づくロック解除機構において、ＩＤ情報を管理するデータベースサーバに由来する問題点を解決するものである。
【課題を解決するための手段】
【０００５】
本発明は、上記の課題を解決するためになされたものであり、以下の形態により実現することができる。
本発明に係る第１の形態は、第１装置と、第２装置と、を備え、前記第１装置は、秘密情報を決定する決定部と、前記秘密情報を出力する出力部と、前記第２装置は、前記秘密情報を譲渡されたユーザから前記秘密情報を受け取る受取部と、秘密情報を用いてアンロックすることにより取り出し可能な出力情報と、識別情報とを含む第１トランザクションが分散型台帳に公開されたとき、前記受取部により受け取った秘密情報を用いて前記第１トランザクションがアンロック可能な場合、前記第１トランザクションに含まれる前記識別情報を取得する取得部と、前記取得部により取得した前記識別情報が決められた情報であるとき、指定の処理を実行する実行部と、を備える処理システムを特徴とする。
【発明の効果】
【０００６】
一実施態様によれば、ＩＤ情報に基づくロック解除機構において、ＩＤ情報を管理するデータベースサーバに由来する問題点を解決することができる。
【図面の簡単な説明】
【０００７】
【図１】本実施形態に係るネットワーク構造の一例を示す図である。
【図２】暗号資産の取引情報の一例を示す図である。
【図３】アトミックスワップの処理の一例を示す図である。
【図４】第１実施例のロック解除処理の流れを説明する図である。

【図５】図４で説明したロック解除処理を説明するフローチャートである。
【図６】第２実施例のロック解除処理の流れを説明する図である。
【図７】図６で説明したロック解除処理を説明するフローチャートである。
【図８】第３実施例のロック解除処理の流れを説明する図である。
【図９】図８で説明した解錠処理を説明するフローチャートである。
【図１０】管理装置が有する機能を示すブロック図である。
【図１１】決済装置が有する機能を示すブロック図である。
【図１２】利用者装置が有する機能を示すブロック図である。
【図１３】コンピュータ装置の一実施例を示すブロック図である。
【発明を実施するための形態】
【０００８】
以下に、図面を参照して、本発明の実施の形態を詳細に説明する。
本実施形態のシステムは分散型台帳上のＩＤ情報を用いたロック解除システムである。
後述するように、分散型台帳技術を用いた本実施形態のロック解除システムの一例として、プリペイド決済のシステムやスマートロックのシステムがある。
分散型台帳は分散型台帳技術（Distributed Ledger Technology）に基づくものであり、電子署名とハッシュポインタとを使用して改ざんを検出可能な構造のデータを、ネットワーク上に分散する複数のノードに保持させるという構成を有する。分散型台帳としては、例えば、ブロックチェーンやＤＡＧ（Directed acyclic graph）などが知られている。本明細書では、分散型台帳技術としてブロックチェーンを例に挙げて説明する。
なお、ＤＡＧでは、ユーザがトランザクションを作成したとき、先に公開されている未承認のトランザクションを承認する。ユーザが作成したトランザクションも、後から公開される未承認のトランザクションに承認される。閾値以上の未承認のトランザクションから直接または間接的に承認されたとき、ユーザが作成したトランザクションは、ネットワークで合意されたものとみなされる、というコンセンサスアルゴリズムを採用している。
上記のようにＤＡＧは、以下で説明するブロックチェーンと、コンセンサスアルゴリズムに違いがあるものの、トランザクションの構造はブロックチェーンと同様のものを採用することができる。
したがって、分散型台帳としてブロックチェーンを利用する処理と、分散型台帳としてＤＡＧを利用する処理とは、同様の構成のトランザクションを用いて実行することができる。このため、以下で説明する分散型台帳としてブロックチェーンを利用する処理は、分散型台帳としてＤＡＧを利用して実行することも可能である。
まず、本実施形態のロック解除システムを実現する要素技術として、分散型台帳の一例としてのブロックチェーンと暗号資産の送金について概説する。
【０００９】
［ブロックチェーン］
ブロックチェーンとは、複数の取引情報を含むブロックを生成し、生成したブロックを連結することにより、分散型ネットワークにデータを記録するデータベースである。
ブロックには、複数の取引情報に加えて、１つ前に生成されたブロックの内容を示すハッシュ値を含むので、ブロックチェーンは、生成されたブロックが時系列に沿ってつながっていくデータ構造を有する。ビットコインやモナコイン、イーサリアム等に代表される暗号資産（仮想通貨）の基礎技術である。
【００１０】
資産の取引をトランザクションというデータ形式で表現し、それをＰ２Ｐネットワークで共有する。トランザクション全体をマークルツリーでまとめあげ、マークルツリーのルートノード（マークルルート）と前ブロックのハッシュ値、Ｎｏｎｃｅと呼ばれる任意の値などをまとめたハッシュ値が一定値以下になるようなＮｏｎｃｅを探し当てる作業を、マイニングと呼ぶ。
マイニングに成功するとマイニング報酬が得られる。そのマイニング報酬を目当てにマイニングに投入される計算資源の多さによって、古いデータほど改ざんが難しくなる仕組み

を、ＰｏＷ（Ｐｒｏｏｆ　ｏｆ　Ｗｏｒｋ）型のブロックチェーンシステムと呼ぶ。
このように、何らかの報酬を与えることで、データベースへの信頼性を担保するための資源を提供させる仕組みのことをブロックチェーンと呼ぶ。
ＰｏＷ型ブロックチェーン以外にもＰｏＳ型、ＰｏＩ型のブロックチェーンも適用が可能だが説明は割愛する。
【００１１】
［暗号資産の送金の仕組み］
現在主流となっている暗号資産には大きく分けて２種類がある。ビットコインから派生して開発されているライトコインやモナコインなどと、イーサリアムから派生して開発されているルートストックなどである。
前者の場合、暗号資産の実体は未使用のトランザクションの出力（Ｕｎｓｐｅｎｔ　Ｔｒａｎｓａｃｔｉｏｎ　Ｏｕｔｐｕｔ、ＵＴＸＯ）である。
ＵＴＸＯは通常、ＥＣＤＳＡという楕円曲線暗号を用いた電子署名によってのみアンロック可能なようにロックされている。また、特定の秘密鍵を持つ「所有者」にのみアンロックが可能とするため、通常ＵＴＸＯには秘密鍵に対応する公開鍵が記述されている。
【００１２】
ＵＴＸＯに記述されている公開鍵に対応するＥＣＤＳＡ電子署名を与えることでアンロックし、新たなトランザクションの入力に接続し、その新たなトランザクションのＵＴＸＯに送金先の所有者の公開鍵を記述することで、暗号資産の送金を実現している。
実際には、ＵＴＸＯにはＳｃｒｉｐｔＰｕｂＫｅｙと呼ばれる領域があり、そこにはＳｃｒｉｐｔと呼ばれるプログラミング言語で記述されたプログラムが書いてある。そのＵＴＸＯに接続しようとするトランザクションの入力には、ＳｃｒｉｐｔＳｉｇと呼ばれる領域があり、この２つがちょうど対応づいている場合に、ＵＴＸＯはアンロックされる。
イーサリアムやそこから派生した暗号資産については、スマートコントラクトを用いることで同様の仕組みを実現することが出来る。
【００１３】
図１は、本実施形態に係るネットワーク構造の一例を示す図である。
ネットワークは、管理装置７０と、決済装置８０と、利用者装置９０と、ネットワーク３０と、ネットワーク４０と、ネットワーク２００、とを含む。そして、管理装置７０と、決済装置８０と、利用者装置９０と、ネットワーク３０と、ネットワーク４０とはネットワーク２００を介して互いに通信可能に接続されている。
管理装置７０、決済装置８０、及び利用者装置９０は、例えば、後述するコンピュータ装置である。
図１に示すネットワークには取引装置１０と取引装置２０が含まれるが、これらは、本実施形態が参考にしているアトミックスワップを説明するために参照される。以下の説明において、取引装置１０と取引装置２０とを特に区別しないときは、単に取引装置ともいう。
【００１４】
ネットワーク３０及びネットワーク４０は、Ｐ２Ｐネットワークなどの分散型ネットワークであり、ブロックチェーン上に取引情報を記録する。
以下の説明では、一例として、ネットワーク３０は、例えば、ビットコインのコンセンサスアルゴリズムであるプルーフオブワーク（ＰｏＷ）を採用しているものとして説明する。また、ネットワーク４０は、例えば、ライトコインのコンセンサスアルゴリズムであるプルーフオブワークを採用しているものとして説明する。
【００１５】
また、ネットワーク３０内で発生した取引を記録するブロックチェーンのことをビットコインのブロックチェーンともいう。さらに、ネットワーク４０内で発生した取引を記録するブロックチェーンのことをライトコインのブロックチェーンともいう。なお、ネットワーク３０及びネットワーク４０は、それぞれプルーフオブステーク（ＰｏＳ）、プルーフオブインポータンス（ＰｏＩ）、及びプルーフオブコンセンサス（ＰｏＣ）などの他のコ

ンセンサスアルゴリズムを採用してもよい。
【００１６】
ネットワーク３０は、マイニングを実行する複数のノード装置３０１から３０ｎが通信可能に接続されている。また、ネットワーク４０は、マイニングを実行する複数のノード装置４０１から４０ｎが通信可能に接続されている。以下の説明では、ノード装置３０１から３０ｎを特に区別しないときは、ノード装置３００ともいう。また、ノード装置４０１から４０ｎを特に区別しないときは、ノード装置４００ともいう。
【００１７】
プルーフオブワークにおいて、マイニングとは、ブロックに含まれるＮａｎｃｅを変化させながら、ブロックのデータにハッシュ関数を適用したとき、決められた数以上の０が上位に並ぶハッシュ値が得られるＮａｎｃｅ（以下、正しいＮａｎｃｅともいう）を探す作業のことである。ブロックのデータには、ブロックに連結される前ブロックのデータのハッシュ値と、Ｎａｎｃｅと、取引情報とを含む。
【００１８】
ノード装置は、ブロックを生成するとき、ブロックに含むトランザクションを検証する。そして、ノード装置は、正しいトランザクションを承認し、承認したトランザクションをブロックに含ませて、Ｎａｎｃｅを探す作業を実行する。ノード装置は、正しいＮａｎｃｅを発見すると、正しいＮａｎｃｅを含むブロックを生成し、ノード装置が保持するブロックチェーンに新たに生成したブロックを連結する。また、ノード装置は、ブロックチェーンのネットワーク上に新たに生成したブロックを送信する。そして、新たに生成したブロックは、ネットワークに接続された他のノード装置が保持するブロックチェーンにも連結される。これにより、トランザクションは、ブロックチェーン上に記録される。以下の説明では、トランザクションを含んだブロックがブロックチェーンに連結されることを、トランザクションがブロックチェーンに記録されるともいう。
ネットワーク２００は、ネットワーク３０及びネットワーク４０に限らず、さらに他のネットワークと接続されてもよい。また、ネットワーク２００は、取引装置１０、取引装置２０、管理装置７０、及び決済装置８０に加えて、さらに他の取引装置と接続されてもよい。
【００１９】
図２は、暗号資産の取引情報の一例を示す図である。
図２（ａ）は、取引情報の構成を説明する図である。図２（ｂ）は、取引情報を接続する処理を説明する図である。取引情報とは、暗号資産の引き渡しと、受け取りとを実行し、暗号資産の所有権を移転する処理に用いられるトランザクションのことである。
以下の説明では、トランザクションスクリプトとして、Ｐ２ＰＫＨ（Ｐａｙ ｔｏ Ｐｕｂｌｉｃ Ｋｅｙ Ｈａｓｈ）を用いるものとして説明する。なお、トランザクションスクリプトとして、Ｐ２ＰＫ（Ｐａｙ ｔｏ Ｐｕｂｌｉｃ Ｋｅｙ）を用いる場合には、ＵＴＸＯをロックするＳｃｒｉｐｔＰｕｂＫｅｙは、ＵＴＸＯの受領者である送信先の利用者の公開鍵を含む。また、Ｐ２ＰＫにおいて、ＵＴＸＯをアンロックするＳｃｒｉｐｔＳｉｇは、ＵＴＸＯの授与者であるトランザクションを作成する送信元の利用者の秘密鍵を用いて生成した電子署名を含む。
【００２０】
ＵＴＸＯは、トランザクションのインプットとして使われていない、未使用のトランザクションのアウトプットのことである。ＵＴＸＯは、暗号資産の所有権であり、次のトランザクションのインプットとして使用される。したがって、暗号資産の送金とは、送金者によりＵＴＸＯが使用され、着金者によってのみ使用可能なＵＴＸＯが作成されることである。トランザクションのインプットとは、暗号資産の使用を処理する情報である。また、トランザクションのアウトプットとは、暗号資産の使途を処理する情報である。ＵＴＸＯとは、Ｕｎｓｐｅｎｔ Ｔｒａｎｓａｃｔｉｏｎ Ｏｕｔｐｕｔの略である。
【００２１】
電子署名は、例えば、トランザクションのＳｃｒｉｐｔＳｉｇを除くデータと、前トラン

ザクションのＳｃｒｉｐｔＰｕｂＫｅｙとを用いて得られる電子署名用の値を、トランザクションを作成する送信元の利用者の秘密鍵で暗号化した値である。前トランザクションとは、送信元の利用者が送金時に作成するトランザクションのインプットと接続される、送信元の利用者への送金情報が記述されたアウトプットを含むトランザクションのことである。電子署名用の値とは、例えば、トランザクションのＳｃｒｉｐｔＳｉｇを除くデータと、前トランザクションのＳｃｒｉｐｔＰｕｂＫｅｙとを含むデータにハッシュ関数を適用して得られる値である。

【００２２】

図２（ａ）を参照してトランザクションの構成を説明する。

トランザクションは、暗号資産の所有の移転をまとめた取引情報である。トランザクションは、インプット（ｉｎｐｕｔ）と、アウトプット（ｏｕｔｐｕｔ）とを含む。

インプットは、トランザクションを作成する送信元の利用者が所有する前トランザクションのＵＴＸＯをアンロックするための情報である。そして、インプットは、ＳｃｒｉｐｔＳｉｇを含む。

ＳｃｒｉｐｔＳｉｇは、送信元の利用者が所有するＵＴＸＯをアンロックするためのスクリプトである。ＳｃｒｉｐｔＳｉｇは、送信元の利用者の電子署名と公開鍵とを含む。ＳｃｒｉｐｔＳｉｇに含まれる電子署名及び公開鍵は、送信元の利用者の秘密鍵を用いて生成された値である。

【００２３】

アウトプットは、暗号資産の所有権の移転を示す情報である。アウトプットは、送金額と、ＳｃｉｒｐｔＰｕｂＫｅｙとを含む。

ＳｃｒｉｐｔＰｕｂＫｅｙは、トランザクションのアウトプットをアンロックするための条件を定義したスクリプトである。ＳｃｒｉｐｔＰｕｂＫｅｙは、送信先の利用者の秘密鍵を用いて生成された公開鍵のハッシュ値（以下、公開鍵ハッシュともいう）を含む。

【００２４】

図２（ｂ）を参照してトランザクションを接続する処理を説明する。以下の説明では、一例として、接続対象の前トランザクションのアウトプット０が、新規トランザクションに接続される処理を説明する。また、各トランザクションは、ネットワーク３０内で処理されるものとする。

前トランザクションのアウトプットは、送金額とＳｃｉｒｐｔＰｕｂＫｅｙ０とを含むアウトプット０（ｏｕｔｐｕｔ０）と、送金額とＳｃｉｒｐｔＰｕｂＫｅｙ１とを含むアウトプット１（ｏｕｔｐｕｔ１）と、を含む。アウトプット０とアウトプット１とは、それぞれＩｎｄｅｘ０とＩｎｄｅｘ１と関連付けられている。Ｉｎｄｅｘ０とＩｎｄｅｘ１とは、それぞれアウトプット０とアウトプット１とを識別する識別子である。

【００２５】

前トランザクションのアウトプット０に、新規トランザクションのインプット０が接続される。新規トランザクションのインプット０が接続されるまでは、前トランザクションのアウトプット０は、ＵＴＸＯの状態である。前トランザクションのアウトプット１には、新規トランザクション及び他のトランザクションのインプットが接続されていないので、ＵＴＸＯの状態である。

新規トランザクションのインプット０は、ＳｃｒｉｐｔＳｉｇと、前トランザクションのトランザクションハッシュと、前トランザクションのアウトプットの識別子であるＩｎｄｅｘ０とを含む。

【００２６】

ＳｃｒｉｐｔＳｉｇ０は、前トランザクションのアウトプット０をアンロックする処理に用いられる電子署名と公開鍵とを含む。電子署名は、例えば、新規トランザクションのＳｃｒｉｐｔＳｉｇ０を除くデータと、前トランザクションのアプトプット０に含まれるＳｃｒｉｐｔＰｕｂＫｅｙ０とを用いて得られる電子署名用の値を、秘密鍵を用いて暗号化することにより生成される。このとき、秘密鍵には、新規トランザクションを作成する利用者の秘密鍵が用いられる。

トランザクションハッシュは、前トランザクション全体のハッシュ値である。そして、トランザクションハッシュは、前トランザクションを識別するためのトランザクションＩＤとして用いられる。Ｉｎｄｅｘ０は、前トランザクションにおける接続先のアウトプット０を識別する識別子である。
上記の前トランザクションに含まれるアウトプット０と、新規トランザクションに含まれるインプット０とが接続される処理を説明する。以下の説明では、前トランザクションがビットコインのブロックチェーンに記録された状態であるものとする。
【００２７】
取引装置は、新規トランザクションを作成し、ネットワーク３０に送信することにより、各ノード装置３００が備える未検証のトランザクションを格納するトランザクションプールに新規トランザクションを格納する。ノード装置３００は、新規トランザクションを検証の対象として選択すると、新規トランザクションのトランザクションＩＤとＩｎｄｅｘ０とを参照し、ブロックチェーン上のトランザクションを検索する。ノード装置３００は、トランザクションＩＤに対応する前トランザクションを発見し、さらに、Ｉｎｄｅｘ０に対応するアウトプット０を発見する。
【００２８】
そして、ノード装置３００は、インプット０に含まれるＳｃｒｉｐｔＳｉｇ０と、アウトプット０に含まれるＳｃｒｉｐｔＰｕｂＫｅｙ０とを連結する。これにより、ノード装置３００は、ＳｃｒｉｐｔＳｉｇ０に含まれる公開鍵のハッシュ値と、ＳｃｒｉｐｔＰｕｂＫｅｙ０に含まれる公開鍵ハッシュとの一致を検証する第１検証を実行する。さらに、ノード装置３００は、ＳｃｒｉｐｔＳｉｇ０に含まれる電子署名と公開鍵とを用いて電子署名を検証する第２検証を実行する。ノード装置３００は、第１検証と第２検証とが承認されると、前トランザクションのアウトプット０と新規トランザクションのインプット０とを接続する。
そして、ノード装置３００は、承認した新規トランザクションをブロックに含ませて、Ｎａｎｃｅを探す作業を実行する。ノード装置３００は、正しいＮａｎｃｅを発見すると、正しいＮａｎｃｅが含まれるブロックを生成し、ノード装置３００が保持するブロックチェーンに新たに生成したブロックを連結する。また、ノード装置３００は、ブロックチェーンのネットワーク上に新たに生成したブロックを送信する。これにより、新たに生成したブロックは、ネットワークに接続された他のノード装置が保持するブロックチェーンにも連結され、新規トランザクションがブロックチェーンに記録される。
【００２９】
図３は、アトミックスワップの処理の一例を示す図である。
図４以降で説明する本実施形態のロック解除方法は、このアトミックスワップ及びその変形といえるトランザクションパズルの仕組みを応用したものである。
従って、本実施形態のロック解除方法を説明する前に、図３を用いてアトミックスワップの処理を説明する。
前提として、暗号資産には、異なる特徴を有する複数の種類の暗号資産がある。このため、利用者は、暗号資産を使用するとき、用途に適した暗号資産を選択して利用する。暗号資産の種類には、例えば、ビットコイン（ＢＴＣ：登録商標）、イーサリアム（ＥＴＨ：登録商標）、ライトコイン（ＬＴＣ）、及びモナコイン（ＭＯＮＡ：登録商標）などがある。暗号資産の用途には、例えば、価値の保存、商品の購入、及び契約内容の管理の手数料などがある。
上記のように、複数の種類の暗号資産を用途に応じて使い分けるため、異なる暗号資産を交換する取引が行われている。異なる暗号資産を交換する取引には、利用者間の直接の取引である直接取引と、利用者間に取引所などの第三者を介する取引である仲介取引とがある。
【００３０】
暗号資産の直接取引について説明する。
例えば利用者Ａは、自身が所有するビットコインと、利用者Ｂが所有するライトコインと

の交換取引を行うとき、ビットコインを利用者Ｂに送金する。そして、利用者Ｂは、ビットコインが利用者Ａから届いたことを確認すると、利用者Ａにライトコインを送金する。直接取引において、利用者Ｂは、利用者Ａからビットコインが届いたことを確認したあと、利用者Ａにライトコインを送金しないでビットコインを持ち逃げすることが可能である。したがって、利用者Ａは、取引相手が信用できることを前提として、ビットコインを取引相手に送金しなければならない。

【００３１】

暗号資産の仲介取引について説明する。

例えば利用者Ａは、自身が所有するビットコインを取引所に預ける。また、利用者Ｂは、自身が所有するライトコインを取引所に預ける。そして、取引所は、利用者Ａに利用者Ｂが預けたライトコインを送金し、利用者Ｂに利用者Ａが預けたビットコインを送金する。仲介取引において、利用者Ａと利用者Ｂとは取引所に暗号資産を預けているので、取引所の不正及び取引所のハッキングなどにより、暗号資産が盗難される恐れがある。また、仲介取引では、取引所を利用するので、手数料が直接取引と比較して割高になることがある。したがって、利用者Ａは、取引所が信用できること及び手数料が割高になることを前提として、ビットコインを取引所に預けなければならない。

【００３２】

このような問題を解決するために、信用のない個人間での取引においても暗号資産を持ち逃げされることなく直接取引することができるアトミックスワップが用いられている。

二者間で異なるブロックチェーンを用いた暗号資産同士の交換を行うとき、単純に利用者Ａと利用者Ｂとの間でお互いの暗号資産を送りあうと、利用者Ａから利用者Ｂへの送金及び利用者Ｂから利用者Ａへの送金が同時に行われることは保証できない。これは、ブロックチェーンによって承認までの期間が異なること、及びお互いの暗号資産を送信するタイミングが異なること、などに起因する。

また、承認前の送金トランザクションは取り下げが可能であるため、言い換えれば、先に承認された取引のみを有効とし、残った取引を取り下げることで、片方が暗号資産を持ち逃げすることができてしまう。

ビットコイン及びそこから派生したブロックチェーンシステムにおいて、Ａｔｏｍｉｃ Ｓｗａｐ（アトミックスワップ）は、ＵＴＸＯのアンロックの条件を記述したＳｃｒｉｐｔと呼ばれるプログラミング言語を用いる。そして、アトミックスワップは、Ｓｃｒｉｐｔの命令セットに、一方向ハッシュ関数であるＳＨＡ２５６を求める命令と、値の比較を行う命令があることを利用している。

【００３３】

具体的には、利用者Ａと利用者Ｂの間での暗号資産の交換を以下の手順で行う。

以下の説明では、一例として、取引相手が所有するビットコインと、利用者が所有するライトコインとを交換する処理について説明する。取引装置１０が秘密値Ｒを生成する処理を説明するが、利用者Ｂの取引装置が秘密値Ｒを生成してもよい。すなわち、以下で説明する利用者Ａの取引装置の実行する処理を利用者Ｂの取引装置が実行し、利用者Ｂの取引装置が実行する処理を利用者Ａの取引装置が実行してもよい。また、説明の簡単化のため、各トランザクションのアウトプットには、１つのアウトプットが含まれるものとし、アウトプットをＩｎｄｅｘに応じて参照する処理の説明を省略する。なお、交換する暗号資産の数量（交換数量）は、アトミックスワップの処理の前に利用者と取引相手との間で為替レートなどに基づいて決定してもよい。また、利用者と取引相手とは、アトミックスワップの処理の前にそれぞれお互いのアドレス及び公開鍵を交換してもよい。利用者Ａと利用者Ｂとは、暗号資産の交換数量の決定、並びにアドレス及び公開鍵の交換を、メール及び記録媒体の提供などの任意の通信手段により行ってもよい。

【００３４】

ステップ（１）

利用者Ａは乱数によって秘密値Ｒを定め、秘密値Ｒのハッシュ値Ｈを計算する。

利用者Ａは、「引数の１つが利用者Ｂの公開鍵に対応する電子署名であること（すなわち

受取人が利用者Ｂであること）及び、もう１つの引数のＳＨＡ２５６ハッシュ値がハッシュ値Ｈであること」をアンロック条件としたトランザクションＴｘ１を発行し、承認を待つ。
利用者Ｂは、承認されたトランザクションＴｘ１がブロックチェーンに公開されるため、ハッシュ値Ｈを知ることができる。
すなわち、利用者Ａの取引装置１０は、秘密値Ｒをランダムに生成する。また、利用者Ａの取引装置は、秘密値Ｒにハッシュ関数を適用し、ハッシュ値Ｈを生成する。利用者Ａの取引装置が秘密値Ｒをハッシュ化するときに用いられるハッシュ関数は、例えば、ＳＨＡ－２、ＭＤ５、及びＳＨＡ－１などの一方向ハッシュ関数である。
ハッシュ関数にＳＨＡ－２を用いる場合、ＳＨＡ２５６を２度適用してハッシュ値Ｈを計算する。ハッシュ値Ｈの計算に際してＳＨＡ２５６を２度適用するのは、上記Ｓｃｒｉｐｔにそのような命令があるためであり、ＳＨＡ２５６の適用は１度であってもよい。
【００３５】
さらに、利用者Ａの取引装置１０は、ビットコインを利用者Ｂに送金するためのトランザクションＴｘ１を作成する。そして、利用者Ａの取引装置は、作成したトランザクションＴｘ１をネットワーク３０に送信する。これにより、トランザクションＴｘ１は、ネットワーク３０に公開される。
トランザクションＴｘ１のインプットは、利用者Ａの電子署名及び利用者Ａの公開鍵を含むＳｃｒｉｐｔＳｉｇと、アンロックするＵＴＸＯを含む前トランザクションのトランザクションＩＤとを含む。トランザクションＴｘ１のＳｃｒｉｐｔＳｉｇによってアンロックするＵＴＸＯは、利用者Ａが所有するＵＴＸＯである。利用者Ａの電子署名及び利用者Ａの公開鍵は、利用者Ａが所有する秘密鍵を用いて生成される。
トランザクションＴｘ１のアウトプットは、ハッシュ値Ｈ及び利用者Ｂの公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙを含む。利用者Ｂの公開鍵ハッシュは、利用者Ｂの公開鍵を用いて生成される。利用者Ｂの公開鍵ハッシュとは、利用者Ｂの公開鍵にハッシュ関数を適用して得られるハッシュ値のことである。
【００３６】
ステップ（２）
利用者Ｂも同様に「引数の１つが利用者Ａの公開鍵に対応する電子署名であること（すなわち受取人が利用者Ａであること）及び、もう１つの引数のＳＨＡ２５６ハッシュ値がＨであること」をアンロック条件としたトランザクションＴｘ２を発行し、承認を待つ。
すなわち、利用者Ｂの取引装置２０は、ライトコインを利用者Ａに送金するためのトランザクションＴｘ２を作成する。そして、利用者Ｂの取引装置は、作成したトランザクションＴｘ２をネットワーク４０に送信する。これにより、トランザクションＴｘ２は、ネットワーク４０に公開される。
【００３７】
トランザクションＴｘ２のインプットは、利用者Ｂの電子署名及び利用者Ｂの公開鍵を含むＳｃｒｉｐｔＳｉｇと、アンロックするＵＴＸＯを含む前トランザクションのトランザクションＩＤとを含む。トランザクションＴｘ２のＳｃｒｉｐｔＳｉｇによってアンロックするＵＴＸＯは、利用者Ｂが所有するＵＴＸＯである。利用者Ｂの電子署名及び利用者Ｂの公開鍵は、利用者Ｂが所有する秘密鍵を用いて生成される。
トランザクションＴｘ２のアウトプットは、ハッシュ値Ｈ及び利用者Ａの公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙを含む。利用者Ａの公開鍵ハッシュは、利用者Ａの公開鍵を用いて生成される。利用者Ａの公開鍵ハッシュとは、利用者Ａの公開鍵にハッシュ関数を適用して得られるハッシュ値のことである。ハッシュ値Ｈは、トランザクションＴｘ１がネットワーク３０に公開されると、利用者Ｂの取引装置によりトランザクションＴｘ１から取得され、トランザクションＴｘ２のアウトプットに記述される。
【００３８】
ステップ（３）
利用者Ａは、利用者Ｂが発行したトランザクションＴｘ２が承認され、取り下げや改ざん

ができなくなったことを確認する。
利用者Ａ自身の秘密鍵による電子署名を作成し、秘密値Ｒと共にアンロックのための引数として、利用者Ｂが発行したトランザクションＴｘ２のＵＴＸＯを利用して自分自身に送金を行う。
上記のトランザクションが承認され改ざんができなくなると共に、秘密値Ｒはトランザクション内のデータとしてブロックチェーンに公開されるため、利用者Ｂは秘密値Ｒを知ることができる。
すなわち、利用者Ａの取引装置１０は、ライトコインを利用者Ｂの取引装置から受け取るためのトランザクションＴｘ３を作成する。そして、利用者Ａの取引装置は、作成したトランザクションＴｘ３をネットワーク４０に送信する。これにより、トランザクションＴｘ３は、ネットワーク４０に公開される。
トランザクションＴｘ３のインプットは、秘密値Ｒ、利用者Ａの公開鍵、及び利用者Ａの電子署名を含むＳｃｒｉｐｔＳｉｇと、アンロックするＵＴＸＯを含むトランザクションＴｘ２を識別するトランザクションＩＤとを含む。
トランザクションＴｘ３のアウトプットは、利用者Ａの公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙを含む。
【００３９】
利用者Ｂが送金したライトコインの所有を利用者Ａに移転する処理について、一例として、トランザクションＴｘ３を用いてトランザクションＴｘ２のＵＴＸＯをアンロックし、アンロックしたＵＴＸＯを利用者Ａのアドレスにロックする処理を説明する。利用者Ａのアドレスとは、例えば、利用者Ａの公開鍵ハッシュを変換した値である。
ノード装置４００は、トランザクションＴｘ３がネットワーク４０に送信されると、トランザクションＴｘ３に含まれるトランザクションＩＤに対応するトランザクションＴｘ２のＵＴＸＯ（アウトプット）を参照する。また、ノード装置４００は、トランザクションＴｘ３のＳｃｒｉｐｔＳｉｇに含まれる秘密鍵Ｒにハッシュ関数を適用して、ハッシュ値を求める。そして、ノード装置４００は、求めたハッシュ値と、トランザクションＴｘ２のＳｃｒｉｐｔＰｕｂＫｅｙに含まれるハッシュ値Ｈとが一致するか否かの第１検証を実行する。ノード装置４００が秘密値Ｒのハッシュ値を求めるときに用いるハッシュ関数は、利用者Ａの取引装置が秘密値Ｒをハッシュ化するときに用いるハッシュ関数と同じハッシュ関数である。
【００４０】
また、ノード装置４００は、トランザクションＴｘ３のＳｃｒｉｐｔＳｉｇに含まれる利用者Ａの公開鍵にハッシュ関数を適用して得られるハッシュ値を求める。そして、ノード装置４００は、求めたハッシュ値と、トランザクションＴｘ２のＳｃｒｉｐｔＰｕｂＫｅｙに含まれる利用者Ａの公開鍵ハッシュとが一致するか否かの第２検証を実行する。さらに、ノード装置４００は、トランザクションＴｘ３のＳｃｒｉｐｔＳｉｇに含まれる利用者Ａの電子署名と利用者Ａの公開鍵とを用いて電子署名の検証をする第３検証を実行する。
ノード装置４００は、上記の第１検証、第２検証及び第３検証が成功すると、トランザクションＴｘ２のＵＴＸＯを利用者Ａのアドレスにロックする。すなわち、ノード装置４００は、利用者Ａがライトコインを受け取ったことを示すアウトプットを作成し、作成したアウトプットをトランザクションＴｘ３に含まれる、利用者Ａが所有するＵＴＸＯとしてロックする。これにより、ライトコインの所有は、利用者Ｂから利用者Ａに移転する。
【００４１】
トランザクションＴｘ１のＳｃｒｉｐｔＰｕｂＫｅｙには、所定の時間経過後にトランザクションＴｘ１のアウトプットがＵＴＸＯのままであった場合、利用者Ａの公開鍵を用いて、利用者Ａにビットコインを戻す処理を実行するスクリプトを含んでもよい。これにより、利用者Ａの取引装置は、取引が成立しないとき、所定の時間経過後に利用者Ａのアドレスにビットコインを戻すことができる。以下の説明では、暗号資産が戻される処理を実行するスクリプトをタイムロックともいう。

【００４２】
ステップ（４）
利用者Ｂ自身の秘密鍵による電子署名と秘密値Ｒによって、トランザクションＴｘ１のＵＴＸＯをアンロックし、利用者Ｂ自身に送金する。
すなわち、利用者Ｂの取引装置は、利用者Ａによってネットワーク４０に公開されたトランザクションＴｘ３に含まれる秘密値Ｒを取得し、ビットコインを利用者Ａの取引装置から受け取るためのトランザクションＴｘ４を作成する。そして、利用者Ｂの取引装置は、作成したトランザクションＴｘ４をネットワーク３０に送信する。これにより、トランザクションＴｘ４は、ネットワーク３０に公開される。
トランザクションＴｘ４のインプットは、秘密値Ｒ、利用者Ｂの公開鍵、及び利用者Ｂの電子署名を含むＳｃｒｉｐｔＳｉｇと、アンロックするＵＴＸＯを含むトランザクションＴｘ１を識別するトランザクションＩＤとを含む。
トランザクションＴｘ４のアウトプットは、利用者Ｂの公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙを含む。
【００４３】
利用者Ａが送金したビットコインの所有を利用者Ｂに移転する処理について、一例として、トランザクションＴｘ４を用いてトランザクションＴｘ１のＵＴＸＯをアンロックし、アンロックしたＵＴＸＯを利用者Ｂのアドレスにロックする処理を説明する。利用者Ｂのアドレスとは、例えば、利用者Ｂの公開鍵ハッシュを変換した値である。
ノード装置３００は、トランザクションＴｘ４がネットワーク３０に送信されると、トランザクションＴｘ４に含まれるトランザクションＩＤに対応するトランザクションＴｘ１のＵＴＸＯ（アウトプット）を参照する。また、ノード装置３００は、トランザクションＴｘ４のＳｃｒｉｐｔＳｉｇに含まれる秘密鍵Ｒにハッシュ関数を適用して、ハッシュ値を求める。そして、ノード装置３００は、求めたハッシュ値と、トランザクションＴｘ１のＳｃｒｉｐｔＰｕｂＫｅｙに含まれるハッシュ値Ｈとが一致するか否かの第４検証を実行する。ノード装置３００が秘密値Ｒのハッシュ値を求めるときに用いるハッシュ関数は、利用者Ａの取引装置が秘密値Ｒをハッシュ化するときに用いるハッシュ関数と同じハッシュ関数である。
【００４４】
また、ノード装置３００は、トランザクションＴｘ４のＳｃｒｉｐｔＳｉｇに含まれる利用者Ｂの公開鍵にハッシュ関数を適用して得られるハッシュ値を求める。そして、ノード装置３００は、求めたハッシュ値と、トランザクションＴｘ１のＳｃｒｉｐｔＰｕｂＫｅｙに含まれる利用者Ｂの公開鍵ハッシュとが一致するか否かの第５検証を実行する。さらに、ノード装置３００は、トランザクションＴｘ４のＳｃｒｉｐｔＳｉｇに含まれる利用者Ｂの電子署名と利用者Ｂの公開鍵とを用いて電子署名の検証をする第６検証を実行する。
【００４５】
ノード装置３００は、上記の第４検証、第５検証及び第６検証が成功すると、トランザクションＴｘ１のＵＴＸＯを利用者Ｂのアドレスにロックする。すなわち、ノード装置３００は、利用者Ｂがビットコインを受け取ったことを示すアウトプットを作成し、作成したアウトプットをトランザクションＴｘ４に含まれる、利用者Ｂが所有するＵＴＸＯとしてロックする。これにより、ビットコインの所有は、利用者Ａから利用者Ｂに移転する。
【００４６】
トランザクションＴｘ２のＳｃｒｉｐｔＰｕｂＫｅｙには、所定の時間経過後にトランザクションＴｘ２のアウトプットがＵＴＸＯのままであった場合、利用者Ｂの公開鍵を用いて、利用者Ｂにライトコインを戻す処理を実行するスクリプトを含んでもよい。これにより、利用者Ｂの取引装置は、取引が成立しないとき、所定の時間経過後に利用者Ｂのアドレスにライトコインを戻すことができる。
【００４７】
利用者Ａ、利用者Ｂの取引装置が夫々作成するトランザクションＴｘ１、Ｔｘ２のＵＴＸ

Ｏのアンロック条件を示すＳｃｒｉｐｔＰｕｂＫｅｙは、以下のようなプログラムとなる。
１．ＯＰ＿ＨＡＳＨ２５６
２．ＯＰ＿ＰＵＳＨ　Ｈ
３．ＯＰ＿ＥＱＵＡＬＶＥＲＩＦＹ
４．ＯＰ＿ＰＵＳＨ　公開鍵
５．ＯＰ＿ＣＨＥＣＫＳＩＧ
１．～３．の命令群では、引数のハッシュ値を計算してハッシュ値Ｈと比較している。４．、５．は、最もシンプルな送金手法であるＰ２ＰＫ（ｐａｙ－ｔｏ－ｐｕｂｋｅｙ）形式であるが、Ｐ２ＰＫＨ（ｐａｙ－ｔｏ－ｐｕｂｋｅｙ－ｈａｓｈ）形式のものでも良い。

【００４８】
このＵＴＸＯをアンロックするための、対応するＳｃｒｉｐｔＳｉｇは以下の通りとなる。
１．ＯＰ＿ＰＵＳＨ　電子署名
２．ＯＰ＿ＰＵＳＨ　Ｒ
このＳｃｒｉｐｔＳｉｇがなければトランザクションＴｘ２のＵＴＸＯをアンロックできないことからも、利用者Ａが受け取った時点で秘密値Ｒが公開される。
また、何らかの事情で利用者Ａが秘密値Ｒを公開しなかった場合、利用者Ａも利用者Ｂも双方の暗号資産を取り出すことができなくなり、暗号資産の所有権が宙に浮いてしまう。
そのため、実用上は「もしくは、一定期間が過ぎた場合、送金主の公開鍵に対応する電子署名によって取り戻すことができる」という条件を追加する。具体的には、ＳｃｒｉｐｔＰｕｂＫｅｙを以下のようにする。
１．ＯＰ＿ＩＦ
２．ＯＰ＿ＨＡＳＨ２５６
３．ＯＰ＿ＰＵＳＨ　Ｈ
４．ＯＰ＿ＥＱＵＡＬＶＥＲＩＦＹ
５．ＯＰ＿ＰＵＳＨ　宛先公開鍵
６．ＯＰ＿ＣＨＥＣＫＳＩＧ
７．ＯＰ＿ＥＬＳＥ
８．ＯＰ＿ＣＨＥＣＫＬＯＣＫＴＩＭＥＶＥＲＩＦＹ
９．ＯＰ＿ＰＵＳＨ　送金主公開鍵
１０．ＯＰ＿ＣＨＥＣＫＳＩＧ
１１．ＯＰ＿ＥＮＤＩＦ
ＩＦ命令で分岐して、２種類のＳｃｒｉｐｔＳｉｇを受け付ける。

【００４９】
通常通り取引が進んだ場合は、以下のＳｃｒｉｐｔＳｉｇでアンロックが可能である。
１．ＯＰ＿ＰＵＳＨ　宛先秘密鍵の電子署名
２．ＯＰ＿ＰＵＳＨ　Ｒ
３．ＯＰ＿ＰＵＳＨ　１
このスクリプトは、ｒｅｄｅｅｍ　ｓｃｒｉｐｔと呼ばれる。
最後の１をＯＰ＿ＩＦが読み取り、前半のプログラムが実行される。
何らかの理由で秘密値Ｒが公開されなかった場合は、以下のＳｃｒｉｐｔＳｉｇで暗号資産を取り戻せる。
１．ＯＰ＿ＰＵＳＨ　送信主秘密鍵の電子署名
２．ＯＰ＿ＰＵＳＨ　０
このスクリプトは、ｒｅｆｕｎｄ　ｓｃｒｉｐｔと呼ばれる。
最後の０をＯＰ＿ＩＦが読み取り、ＯＰ＿ＥＬＳＥ以降のプログラムが実行され、取り戻しが行われる。ただし、ＯＰ＿ＣＨＥＣＫＬＯＣＫＴＩＭＥＶＥＲＩＦＹが含まれているため、一定期間経過後である必要がある。なお、この期間の指定は、トランザクションＴ

ｘ１、トランザクションＴｘ２の夫々に含まれている。
【００５０】
なお、この例ではＯＰ＿ＨＡＳＨ２５６を利用しているためハッシュ値ＨはＳＨＡ２５６（ＳＨＡ２５６（Ｒ））とするが、ＯＰ＿ＳＨＡ２５６を利用する場合ハッシュ値ＨはＳＨＡ２５６（Ｒ）とする。
他にもいくつかハッシュ関数を計算する命令が存在するため、ハッシュ値Ｈの計算方法はそれに合わせたものにする必要がある。
以上の手順に従えば、利用者Ａが暗号資産を受け取るためには秘密値Ｒを公開せざるを得ず、秘密値Ｒが公開されると同時に利用者Ｂも暗号資産を受け取ることができることとなる。
利用者Ａが秘密値Ｒを公開しない場合、利用者Ａは利用者Ｂの暗号資産を受け取ることができないので、秘密値Ｒの公開が強制されている、と見ることもできる。
【００５１】
このようなアトミックスワップは、本来は異なるブロックチェーンの間でトラストレス（信用する第三者を置かない）にて暗号資産を交換する技術であるが、一旦仮の送金を確定してから秘密情報の受け渡しによって送金を確定する点にその本質があると言える。
【００５２】
なお、bitcoin wiki（https://en.bitcoin.it/wiki/Script#Transaction_puzzle）には、アトミックスワップと類似する仕組みとして、Ｔｒａｎｓａｃｔｉｏｎ　Ｐｕｚｚｌｅ（トランザクションパズル）が紹介されている。
アトミックスワップとの相違点として、トランザクションパズルでは、ＳｃｒｉｐｔＰｕｂＫｅｙに
１．ＯＰ＿ＨＡＳＨ２５６
２．ＯＰ＿ＰＵＳＨ　Ｈ
３．ＯＰ＿ＥＱＵＡＬ
と記載する。
【００５３】
これに対するＳｃｒｉｐｔＳｉｇには、Ｈ＝ＳＨＡ２５６（ＳＨＡ２５６（Ｒ））を満たすＲを用いて
１．ＯＰ＿ＰＵＳＨ　Ｒ
と記載することによりアンロックが可能である。
すなわち、トランザクションパズルでは、アトミックスワップで必要であった「ＯＰ＿ＰＵＳＨ　宛先秘密鍵の電子署名」を記載する必要が無い。
トランザクションパズルは、宛先秘密鍵の公開鍵を限定しない（受領者を限定しない）、アトミックスワップの変形例と考えることが出来る。
【００５４】
以下に、アトミックスワップ、トランザクションパズルを応用した本実施形態のロック解除システムを説明する。
アトミックスワップ、トランザクションパズルにおいて、秘密値Ｒを再利用することができないので、秘密値Ｒをワンタイムパスワード又は使い捨てのＩＤ情報として用いることが出来る。
本実施形態のロック解除システムは、ブロックチェーン上で異なる暗号資産を交換するアトミックスワップ、トランザクションパズルを応用し、あるいはこれらに準拠して、秘密値ＲをＩＤ情報として用いる。
ブロックチェーンはＰ２Ｐシステムで構築されているため、ＩＤ情報を管理するための管理用データベースサーバが不要である。ＩＤ情報を管理するデータベースサーバの立ち上げ、保守運用管理のコストがかからないという利点がある。
なお、暗号資産の交換取引の場合とは異なり、図１に示すネットワークのうち、決済装置８０への送金に用いる暗号資産のネットワークのみ（ここでは、ネットワーク３０）が用いられる。

【００５５】
本実施形態のロック解除システムの一例に、プリペイドシステムがある。
図１に示すシステムにおいて、管理装置７０は、商品やサービスを提供する自動販売機ベンダが管理運用し、購入者からの事前支払い等を管理する等する。
決済装置８０は、現金等の事前支払いに基づくＩＤ情報と引き替えに商品等を購入者に提供する飲料等の自動販売機である。
管理装置７０は、購入者が管理装置７０に対して現金等による事前支払いを行ったことに応じて、例えば管理装置７０によって秘密値Ｒが決定され、アンロックに秘密値Ｒを必要とする第１トランザクションＴｘＡが公開される。
利用者装置９０は、購入者等の利用者が利用する端末装置である。
第１トランザクションＴｘＡは、一例として購入者が事前支払いした現金と同等価値の暗号資産を決済装置８０に送金するためのトランザクションである。アウトプットに送金額を記載し、管理装置７０の電子署名を含んでいる。
【００５６】
また、第１トランザクションＴｘＡは、トランザクション手数料として必要な暗号資産の最小額をアウトプットに記載して、トランザクション手数料を送金するのみのトランザクションであってもよい。この場合、決済装置８０が価値を認める管理装置７０の電子署名を含むことが出来る。管理装置７０と決済装置８０とはともに同じ販売ベンダに属し金銭的に一の関係にあり、購入者が販売ベンダに対して現金等を事前支払いしたことを決済装置８０に証明できれば十分である。
例えば、秘密値Ｒ、あるいはそれと対応する第１トランザクションＴｘＡ一つに付き、固定で１００円の価値などを認めるなどとすることが出来る。
【００５７】
自動販売機としての決済装置８０は、第１トランザクションＴｘＡに含まれる電子署名が、管理装置７０の電子署名であることを確認できれば、購入者が販売ベンダに対して現金等を事前支払いしたと認める。すなわち、管理装置７０の電子署名は、購入者が販売ベンダに対して現金等を事前支払いしており、そのことに基づいて商品等を受け取る資格があることを管理装置７０に証明するものである。
本来は、暗号資産において、ＵＴＸＯが資産である。Ｂｉｔｃｏｉｎや、そこから派生した各種アルトコインにおける「資産の所有」とは、ブロックチェーンのデータベースに記録されているトランザクションの出力のうち、「未使用」かつ「自分でアンロックできる」ものの合計である。これをＵＴＸＯ（Ｕｎｓｐｅｎｔ　ＴＸ　Ｏｕｔｐｕｔ）と呼ぶ。
ＵＴＸＯのアンロックの条件はＳｃｒｉｐｔＰｕｂＫｅｙという領域に書き込まれており、通常は所有者による電子署名でアンロックし別のトランザクション入力へ接続できるようになっている。
【００５８】
それに対して、本実施形態では、購入者が事前支払いをしたことに応じて管理装置７０が作成した電子署名に金銭的価値がある。電子署名は金銭的価値を有するトークンと考えることが出来る。
管理装置７０の電子署名は、第１トランザクションＴｘＡのインプット（ＳｃｒｉｐｔＳｉｇ）に記載してもいいし、ＯＰ＿ＲＥＴＵＲＮに付加情報として記載してもよい。また、管理装置７０の電子署名は、ＴｘＡのインプットから参照されるトランザクションのＳｃｒｉｐｔＰｕｂＫｅｙに記載されていてもよい。
決済装置８０は、秘密値Ｒを提示され、第１トランザクションＴｘＡが、管理装置７０の電子署名を含むことを確認すると、商品やサービス等を購入者に提供する。
そして、決済装置８０は、秘密値Ｒを含む第１トランザクションＴｘＡに対応する第２トランザクションＴｘＢを公開する。
【００５９】
以下、本実施形態のプリペイドシステムを詳細に説明する。
［第１実施例］

第１実施例では、第１トランザクションＴｘＡを管理装置７０が公開する。
説明の簡単化のため、ブロックチェーンを介した送金処理における各トランザクションのアウトプットには、１つのアウトプットが含まれるものとし、アウトプットをＩｎｄｅｘに応じて参照する処理の説明を省略する。
【００６０】
本実施形態では、秘密値ＲをＩＤ情報として用いるプリペイドシステムのロック解除方法として、以下の４つのパターンが考えられる。
（パターン１）管理装置７０は、購入者が事前に支払った現金と同等価値の暗号資産を決済装置８０に送金するトランザクションパズルに準じた第１トランザクションＴｘＡを作成する。そのトランザクションのアンロック条件は秘密値Ｒだけであり、決済装置８０の電子署名を要求しない（受領者は限定されない）。
（パターン２）管理装置７０は、購入者が事前に支払った現金と同等価値の暗号資産を決済装置８０に送金する、アトミックスワップに準じた第１トランザクションＴｘＡを作成する。そのトランザクションのアンロック条件は秘密値Ｒと決済装置８０の電子署名である（受領者が決済装置８０に限定される）。
（パターン３）管理装置７０は、トランザクション手数料として必要な最小額の暗号資産を送金するとともに決済装置８０が価値を認める電子署名を含むトランザクションパズルに準じた第１トランザクションＴｘＡを作成する。そのトランザクションのアンロック条件は秘密値Ｒだけで受領者としての決済装置８０の電子署名を要求しない（受領者は限定されない）。
（パターン４）管理装置７０は、トランザクション手数料として必要な最小額の暗号資産を送金するとともに決済装置８０が価値を認める電子署名を含むアトミックスワップに準じた第１トランザクションＴｘＡを作成する。そのトランザクションのアンロック条件は秘密値Ｒと決済装置８０の電子署名である（受領者が決済装置８０に限定される）。
【００６１】
これらの４つのパターンのうち、（パターン１）は二重使用を阻止できないため実用できない。以下、二重使用について説明する。
ブロックチェーンを用いた暗号資産の送金はブロックチェーンにおけるトランザクションの承認を待つ必要がある。
送金のトランザクションが公開されなかった歴史（新たなブロックチェーン）を作り、十分なハッシュレートでマイニングを進める。これにより、一旦承認されブロックチェーンに取り込まれた送金トランザクションをなかったことにして暗号資産を再利用することが理論上可能である。これを二重使用と呼ぶ。
なお、送金のトランザクションがブロックチェーンに取り込まれた後に、マイニングが進んだブロック数（承認数）が増えるほどトランザクションの取り消しに成功する確率が急速に低くなる。従って十分な承認数だけ待てばトランザクションの取り消しは不可能と考えることも出来る。
【００６２】
トランザクションパズルを応用した処理を行う場合では、第１トランザクションＴｘＡを秘密値Ｒだけでアンロックでき、決済装置８０が公開した第２トランザクションＴｘＢを取り消して第１トランザクションＴｘＡを受け取る二重使用は理論上可能である。しかし、（パターン３）の場合、第１トランザクションＴｘＡに含まれる管理装置７０の電子署名は決済装置８０にとってのみ価値がありそれ以外の者にはＵＴＸＯのトランザクション手数料分の価値しかない。購入者や第三者が自身に対して送金する二重使用を行う動機づけがなく、二重使用が行われることは想定しにくい。
【００６３】
ただし（パターン１）の場合では、決済装置８０が公開した第２トランザクションＴｘＢを取り消し、第１トランザクションＴｘＡを受け取って事前支払い分の暗号資産を手に入れようとする動機がうまれるため、実用するべきではないと言える。
（パターン２）、（パターン４）のアトミックスワップを応用した処理を行う場合は、決

済装置８０の電子署名がないと第１トランザクションＴｘＡを受け取れないので暗号資産の二重使用は不可能である。

【００６４】

図４は、第１実施例のロック解除処理の流れを説明する図である。

以下の説明では、トランザクションスクリプトとして、Ｐ２ＰＫＨを用いるものとして説明する。

ステップ（１１）において、システムの利用者である商品の購入者は、管理装置７０を管理する商品の販売者（販売ベンダ）に対して現金等を支払う。

現金等の支払いは、管理装置７０に対して直接行われるのではなく、例えばコンビニエンスストアの収納代行サービスなどを介して販売者に行うことになる。現金等の支払いは、販売者の銀行口座への振り込みや、クレジットカード払い、暗号資産の送金であってもよい。なお、現金等の支払いは販売者に対して直接行ってもよい。

ステップ（１２）において、管理装置７０は、現金等の支払いに応じて秘密値Ｒをランダムに決定する。また管理装置７０は、管理装置７０の秘密鍵Ｐｒｋ＿Ａから電子署名Ｓｉｇ＿Ａを作成する。また管理装置７０は、決定した秘密値Ｒにハッシュ関数を適用してハッシュ値Ｈを生成する。

【００６５】

なお、例えば現金の事前支払い時などに、購入者自らが秘密値Ｒを作成し、あるいは購入者の端末装置（利用者装置９０）を用いて秘密値Ｒをランダムに決定し、管理装置７０に提供してもよい。その場合、管理装置７０は、提供された秘密値Ｒに対してハッシュ関数を適用してハッシュ値Ｈを生成する。管理装置７０は秘密値Ｒの生成には関与せず、ハッシュ値Ｈの生成、電子署名Ｓｉｇ＿Ａの生成を行う。

また、購入者自らがハッシュ値Ｈをも作成し、あるいは利用者装置９０を用いて秘密値Ｒにハッシュ関数を適用してハッシュ値Ｈを生成し、管理装置７０に提供してもよい。この場合、管理装置７０は、電子署名Ｓｉｇ＿Ａの生成のみを行う。

【００６６】

ステップ（１３）において、管理装置７０は第１トランザクションＴｘＡを作成する。

アトミックスワップを応用した処理を行う場合、第１トランザクションＴｘＡは、決済装置８０の電子署名Ｓｉｇ＿Ｂ、秘密値Ｒを、対応する第２トランザクションＴｘＢのＳｃｒｉｐｔＳｉｇに記載することを条件にアンロック可能なトランザクションである。第１トランザクションＴｘＡの受領者は決済装置８０に限定される。

第１トランザクションＴｘＡのＳｃｒｉｐｔＰｕｂＫｅｙに、決済装置８０の公開鍵、ハッシュ値Ｈを記載し、ＳｃｒｉｐｔＳｉｇに電子署名Ｓｉｇ＿Ａを記載する。

トランザクションパズルを応用した処理を行う場合、第１トランザクションＴｘＡは、秘密値Ｒを対応する第２トランザクションＴｘＢのＳｃｒｉｐｔＳｉｇに記載することを条件にアンロック可能なトランザクションである。

第１トランザクションＴｘＡのＳｃｒｉｐｔＰｕｂＫｅｙに、秘密値Ｒのハッシュ値Ｈを記載し、決済装置８０の公開鍵は記載しない。第１トランザクションＴｘＡは受領者を限定しないトランザクションである。

さらに、管理装置７０は、第１トランザクションＴｘＡのＳｃｒｉｐｔＳｉｇに電子署名Ｓｉｇ＿Ａを記載する。

なお、後述する第２トランザクションＴｘＢを使用しない構成の場合は、第１トランザクションＴｘＡの付加情報として、直接上記の情報を記載してもよい。

管理装置７０は、作成した第１トランザクションＴｘＡをブロックチェーン（ネットワーク３０）に公開する。

【００６７】

ステップ（１４）において、管理装置７０は秘密値Ｒを購入者に提供する。秘密値Ｒの提供は、例えば、上記したようにコンビニエンスストアの収納代行サービスなどを介して、秘密値Ｒの内容を含むＱＲコード（登録商標）やバーコードを印刷した紙を発行する。あるいは、コンビニエンスストアのサービス端末等を介して秘密値Ｒを購入者が所持するＵ

ＳＢメモリやトークン等に格納してもよい。あるいは、購入者が所持する携帯端末（購入者装置９０）にＥ－ＭＡＩＬその他の手段で秘密値Ｒを送信し、同携帯端末の画面にＱＲコード（登録商標）やバーコードとして表示可能としてもよい。この時、第１トランザクションＴｘＡのトランザクションＩＤも同時に提供すると、決済装置８０の処理負荷が軽減される。
秘密値Ｒを受け取った購入者は、管理装置７０が第１トランザクションＴｘＡを公開したブロックチェーンの改ざん成功確率が十分に低くなるまで待ってから、秘密値Ｒを決済装置８０に対して提示する。
【００６８】
決済装置８０は、ＵＳＢメモリ等のトークンを差し込む差し込み口（ポート）を備える。購入者が差し込み口に、秘密値Ｒを格納したトークンを差し込むと、決済装置８０は、秘密値Ｒをトークンから読み込むことが出来る。
あるいは、決済装置８０は、紙に印字され、あるいは、利用者装置９０としての携帯端末の表示画面に表示されたＱＲコード（登録商標）やバーコードをスキャンして、秘密値Ｒを読み取ることが出来るカメラ等の読み取り装置を備える。購入者が、紙に印字されたＱＲコード（登録商標）やバーコード、あるいは、利用者装置９０の表示画面に表示されたＱＲコード（登録商標）やバーコードを読み取り装置にかざすと、決済装置８０は、ＱＲコード（登録商標）やバーコードから秘密値Ｒを読みとることが出来る。
【００６９】
ステップ（１５）において、決済装置８０は、公開されている第１トランザクションＴｘＡを検証する。
秘密値Ｒにハッシュ値を適用して得たハッシュ値が第１トランザクションＴｘＡに含まれるハッシュ値Ｈと一致する場合には、第１トランザクションＴｘＡが秘密値Ｒを用いてアンロック可能である。この場合、決済装置８０は、第１トランザクションＴｘＡに記載される電子署名を取得する。
決済装置８０は、第１トランザクションＴｘＡに記載の電子署名を検証して、第１トランザクションＴｘＡに管理装置７０の電子署名Ｓｉｇ＿Ａが付与されていることを確認する。第１トランザクションＴｘＡの暗号資産の送金額が指定の条件を満たすか（商品の値段以上であるか、トランザクション手数料以上の値段であるか）を確認してもよい。
ステップ（１６）において、電子署名Ｓｉｇ＿Ａが付与されている場合、さらに送金額が上記の条件を満たす場合に商品やサービスを購入者に提供する。例えば自動販売機である決済装置８０は、図示しない払出機構によって購入者が所望する飲料などの商品を購入者に払い出す。
ステップ（１７）において、決済装置８０は、秘密値Ｒ、秘密値Ｒのハッシュ値Ｈ、第１トランザクションＴｘＡのトランザクションＩＤ、電子署名Ｓｉｇ＿Ａのうち、少なくとも一つを、決済装置８０が備えるデータベースに記憶する。
【００７０】
これは、本実施形態の場合において、同じ秘密値Ｒや第１トランザクションＴｘＡが二重使用され得る問題があるからである。このような二重使用は、決済装置８０が公開した第２トランザクションＴｘＢが取り消されることで行われる。二重使用をしようとする者は、第２トランザクションＴｘＢが取り消されたあと同じ秘密値Ｒを用いて決済装置８０から商品やサービスを得ようとする。
それに対し決済装置８０は、使用済みの秘密値Ｒ、使用済みの電子署名、第１トランザクションＴｘＡのトランザクションＩＤ、ハッシュ値Ｈのリスト（履歴情報）を、ローカルなデータベース等に記憶する。そして決済装置８０は、データベースに記憶するものと同じ秘密値Ｒを提示されたときには、第２トランザクションＴｘＢが取り消されたと判断することが出来る。
【００７１】
決済装置８０は、第２トランザクションＴｘＢが取り消されたと判断したとき、ステップ（１６）において商品やサービスの提供を行わず、データベースに記憶される情報に基づ

いて第２トランザクションＴｘＢを公開しなおす。
このようにすることで、第２トランザクションＴｘＢの取り消しと、秘密値Ｒ、電子署名の二重使用に対抗することが出来る。
本実施形態では、決済装置８０は、グローバルなパブリックチェーンにおいても、ブロックチェーン全体のコピーを保持するのではなく、ローカルなデータベースに保持する秘密値Ｒ、電子署名を確認するだけで、二重使用を阻止することが出来る。
【００７２】
図４の説明に戻り、決済装置８０は、ステップ（１７）の後で、第１トランザクションＴｘＡをアンロックするための第２トランザクションＴｘＢを公開してもよい。
アトミックスワップを応用した処理を行っている場合、決済装置８０は、ステップ（１８）において、決済装置８０の秘密鍵Ｐｒｋ＿Ｂで電子署名Ｓｉｇ＿Ｂを作成する。トランザクションパズルを応用した処理を行っている場合、電子署名Ｓｉｇ＿Ｂの作成は不要である。
そして決済装置８０は、第１トランザクションＴｘＡをアンロックするための第２トランザクションＴｘＢを作成する。
アトミックスワップを応用した処理を行っている場合、第２トランザクションＴｘＢのＳｃｒｉｐｔＰｕｂＫｅｙに、決済装置８０の公開鍵を記載し、第２トランザクションＴｘＢのＳｃｒｉｐｔＳｉｇに、電子署名Ｓｉｇ＿Ｂ、決済装置８０の公開鍵、秘密値Ｒを記載する。
トランザクションパズルを応用した処理を行っている場合、第２トランザクションＴｘＢは、第２トランザクションＴｘＢのＳｃｒｉｐｔＰｕｂＫｅｙに、決済装置８０の公開鍵を記載し、第１トランザクションＴｘＡのＳｃｒｉｐｔＳｉｇに、決済装置８０の公開鍵、秘密値Ｒを記載する。電子署名Ｓｉｇ＿Ｂは記載しない。
【００７３】
そして、決済装置８０は、作成した第２トランザクションＴｘＢをブロックチェーン（ネットワーク３０）に公開する。
上記のように、秘密値Ｒを受け取った購入者は、管理装置７０が第１トランザクションＴｘＡを公開したブロックチェーンの改ざん成功確率が十分に低くなるまで待ってから、秘密値Ｒを決済装置８０に対して提示していた。決済装置８０は、第１トランザクションＴｘＡの改ざん成功確率が十分に低くなったときに第２トランザクションＴｘＢをブロックチェーンに公開するとも言える。
決済装置８０は、購入者による管理装置７０に対する現金の支払いと第１トランザクションＴｘＡの公開には関与しない。
【００７４】
本実施形態のロック解除システムにおいて、第１トランザクションＴｘＡをアンロックできる秘密値Ｒを購入者が所持していることが重要である。従って、購入者が決済装置８０に提示したことに応じて、決済装置８０は、指定の処理（商品の販売）を実行する。
商品の販売後、第２トランザクションＴｘＢをブロックチェーンに公開すると、履歴情報（秘密値Ｒ、ハッシュ値Ｈ、秘密鍵、トランザクションＩＤ）がブロックチェーンに記録されるため、決済装置８０における販売記録を外部から確認することが出来る。そのような効果を望まないのであれば、第２トランザクションＴｘＢの公開は、必須ではない。
【００７５】
第２トランザクションＴｘＢをブロックチェーンに公開したあとで、指定の処理（商品の販売等）を実行してもよい。すなわち、ステップ（１５）とステップ（１６）の間に、ステップ（１８）を実行してもよい。
上記のように、購入者は、第１トランザクションＴｘＡが承認され、第１トランザクションＴｘＡ取り消される確率が十分に低くなった時点以降に秘密値Ｒを決済装置８０に提示するので、決済装置８０は、購入者に商品やサービスを提供した後に秘密値Ｒ（第２トランザクションＴｘＢ）を公開してもよいし、秘密値Ｒ（第２トランザクションＴｘＢ）を公開してから商品等を提供してもよい。

【００７６】
いずれにしても、本実施形態では、購入者による事前支払い時の第１トランザクションＴｘＡと決済装置８０による決済時の第２トランザクションＴｘＢと、の２段階のトランザクションを発行している。
第１トランザクションＴｘＡについては、承認数が十分に増えるまでの時間を待つ必要があるが、第２トランザクションＴｘＢについて承認数が増えるのを待つ必要がなく、データベースに記憶した秘密値Ｒと同じ秘密値Ｒが提示されてないことを条件に商品やサービスを即時提供することが出来る。
第２トランザクションＴｘＢが取り消されてデータベースに記憶した秘密値Ｒと同じ秘密値Ｒが提示された場合でも、商品やサービスを提供せず、データベースに記憶する秘密値Ｒ、秘密値Ｒのハッシュ値Ｈ、第１トランザクションＴｘＡのトランザクションＩＤ、電子署名Ｓｉｇ＿Ａによって第２トランザクションＴｘＢを公開しなおせばよい。
購入者は、商品の提供前に第２トランザクションＴｘＢの十分な数の承認を待機する必要がなく、利便性を高めることが出来る。
【００７７】
また上記したように、トランザクションパズルを応用した処理を行っており、電子署名に金銭的価値を持たせた場合には二重使用が行われことは想定しにくいので、第２トランザクションＴｘＢの十分な数の承認を待機する必要がなく利便性を高め得る。
アトミックスワップを応用した処理を行っている場合は、秘密値Ｒに加えて決済装置８０の電子署名がないと第１トランザクションＴｘＡを受け取れず二重使用は不可能である。
よって、購入者が商品提供前に第２トランザクションＴｘＢの十分な数の承認を待機する必要がなく、利便性を高め得る。
【００７８】
図５は、図４で説明したロック解除処理を説明するフローチャートである。
ステップＳ１０１において、購入者は販売者に対して現金を支払い、管理装置７０が入金を確認すると、ステップＳ１０２において、管理装置７０は秘密値Ｒをランダムに決定する。
ステップＳ１０３において、管理装置７０は、販売者側の秘密鍵で電子署名Ｓｉｇ＿Ａを作成する。
ステップＳ１０４において、管理装置７０は、電子署名Ｓｉｇ＿Ａを記載した第１トランザクションＴｘＡを作成し、ステップ１０５において、管理装置７０は、第１トランザクションＴｘＡをネットワーク３０に公開する。
【００７９】
ステップＳ１０６において、管理装置７０は、秘密値Ｒを購入者に提供する。
ステップＳ１０７において、購入者は決済装置８０に秘密値Ｒを提示する。
ステップＳ１０８において、決済装置８０は第１トランザクションＴｘＡを検証する。
ステップＳ１０９において、決済装置８０は、商品又はサービスを購入者に提供する。
ステップＳ１１０において、決済装置８０は秘密値Ｒ等をデータベースに記憶する。
アトミックスワップを応用した処理を行う場合、ステップＳ１１１において、決済装置８０は、決裁装置８０の秘密鍵で電子署名Ｓｉｇ＿Ｂを作成する。トランザクションパズルを応用した処理を行う場合、決済装置８０はステップＳ１１１の処理を行わない。
【００８０】
アトミックスワップを応用した処理を行う場合、ステップＳ１１２において、決済装置８０は、ステップＳ１１１で作成した電子署名Ｓｉｇ＿Ｂと、ステップＳ１０６で提示された秘密値Ｒを用いて第２トランザクションＴｘＢを作成する。トランザクションパズルを応用した処理を行う場合、決済装置８０は、電子署名Ｓｉｇ＿Ｂを用いずに第２トランザクションＴｘＢを作成する。
ステップＳ１１３において、決済装置８０は、第２トランザクションＴｘＢをネットワーク３０に公開する。
【００８１】

［第２実施例］
第２実施例は、第１実施例の変形であり、管理装置７０が第１トランザクションＴｘＡを公開するのではなく、商品やサービスの購入者が、自身の端末装置を用いて第１トランザクションＴｘＡを公開する
第２実施例でも、第１実施例と同様に、第１トランザクションＴｘＡのアンロックには秘密値Ｒが必要である。第１トランザクションＴｘＡは、購入者が支払った現金と同等価値の暗号資産を決済装置８０に送金するトランザクションである。あるいは、第１トランザクションＴｘＡは、トランザクション手数料として必要な最小額の暗号資産を送金するとともに、決済装置８０が認める管理装置７０の電子署名を含むことが出来る。
後者の場合、管理装置７０の電子署名をトランザクションのＳｃｒｉｐｔＳｉｇに記載するパターンと、ＯＰ＿ＲＥＴＵＲＮ領域の付加情報として記載するパターンが考えられる。第１トランザクションＴｘＡのインプットにより参照されるトランザクションのＳｃｒｉｐｔＰｕｂＫｅｙに、管理装置７０の電子署名を記載するパターンも考えられる。
また、第１トランザクションＴｘＡのアンロック条件として、秘密値Ｒだけを求める場合（トランザクションパズルを応用する場合）、秘密値Ｒを求めるとともに受領者を限定する場合（アトミックスワップを応用する場合）があるのも第１実施例と同じである。
第２実施例においても、第１実施例と同様に、上記（パターン１）～（パターン４）が想定されうる。（パターン１）が二重使用を阻止できないため、実用できないことも同じである。
【００８２】
図６は、第２実施例のロック解除処理の流れを説明する図である。
以下の説明では、トランザクションスクリプトとして、Ｐ２ＰＫＨを用いるものとして説明する。
ステップ（３１）において、システムの利用者である商品の購入者は、管理装置７０を管理する商品の販売者（販売ベンダ）に対して現金等を支払う。
現金等の支払いは、管理装置７０に対して直接行われるのではなく、例えばコンビニエンスストアの収納代行サービスなどを介して販売者に行うことになる。現金等の支払いは、販売者の銀行口座への振り込みや、クレジットカード払い、暗号資産の送金であってもよい。なお、現金等の支払いは販売者に対して直接行ってもよい。
ステップ（３２）において、管理装置７０は、現金等の支払いに応じて秘密値Ｒをランダムに決定する。また管理装置７０は、管理装置７０の秘密鍵Ｐｒｋ＿Ａから電子署名Ｓｉｇ＿Ａを作成する。また管理装置７０は、決定した秘密値Ｒにハッシュ関数を適用してハッシュ値Ｈを生成する。
ステップ（３３）において、管理装置７０は、作成した秘密値Ｒ、電子署名Ｓｉｇ＿Ａ、ハッシュ値Ｈを購入者に提供する。
特に秘密値Ｒの提供は、例えば、上記したコンビニエンスストアの収納代行サービスなどを介して、秘密値Ｒの提供は、例えば、上記したようにコンビニエンスストアの収納代行サービスなどを介して、秘密値Ｒの内容を含むＱＲコード（登録商標）やバーコードを印刷した紙を発行する。あるいは、コンビニエンスストアのサービス端末等を介して秘密値Ｒを購入者が所持するＵＳＢメモリやトークン等に格納してもよい。あるいは、購入者が所持する携帯端末（購入者装置９０）にＥ－ＭＡＩＬその他の手段で秘密値Ｒを送信し、同携帯端末の画面にＱＲコード（登録商標）やバーコードとして表示可能としてもよい。この時、第１トランザクションＴｘＡのトランザクションＩＤも同時に提供すると、決済装置８０の処理負荷が軽減される。
電子署名Ｓｉｇ＿Ａ、ハッシュ値Ｈについては、購入者が所持する購入者装置９０に送信することが望ましい。
【００８３】
なお、例えば現金の事前支払い時などに、購入者自らが秘密値Ｒを作成し、あるいは購入者の端末装置（利用者装置９０）を用いて秘密値Ｒをランダムに決定し、管理装置７０に提供してもよい。その場合、管理装置７０は、提供された秘密値Ｒに対してハッシュ関数

を適用してハッシュ値Ｈを生成する。管理装置７０は秘密値Ｒの生成には関与せず、ハッシュ値Ｈの生成、電子署名Ｓｉｇ＿Ａの生成を行う。管理装置７０は、ハッシュ値Ｈ、電子署名Ｓｉｇ＿Ａだけを利用者装置９０に提供する。
また、購入者自らがハッシュ値Ｈをも作成し、あるいは利用者装置９０を用いて秘密値Ｒにハッシュ関数を適用してハッシュ値Ｈを生成し、管理装置７０に提供してもよい。この場合、管理装置７０は、電子署名Ｓｉｇ＿Ａの生成のみを行う。管理装置７０は、電子署名Ｓｉｇ＿Ａだけを利用者装置９０に提供する。
【００８４】
利用者装置９０は、第１トランザクションＴｘＡを作成する。
アトミックスワップを応用した処理を行う場合、第１トランザクションＴｘＡは、決済装置８０の電子署名Ｓｉｇ＿Ｂ、秘密値Ｒを、対応する第２トランザクションＴｘＢのＳｃｒｉｐｔＳｉｇに記載することを条件にアンロック可能なトランザクションである。受領者は決済装置８０に限定される。
第１トランザクションＴｘＡのＳｃｒｉｐｔＰｕｂＫｅｙに、決済装置８０の公開鍵、秘密値Ｒのハッシュ値Ｈを記載する。
第１トランザクションＴｘＡのＳｃｒｉｐｔＳｉｇに、電子署名Ｓｉｇ＿Ａを記載する。
トランザクションパズルを応用した処理を行う場合、第１トランザクションＴｘＡは、秘密値Ｒを対応する第２トランザクションＴｘＢのＳｃｒｉｐｔＳｉｇに記載することを条件にアンロック可能なトランザクションである。
第１トランザクションＴｘＡのＳｃｒｉｐｔＰｕｂＫｅｙに、秘密値Ｒのハッシュ値Ｈに記載し、決済装置８０の公開鍵は記載しない。第１トランザクションＴｘＡは受領者を限定しないトランザクションである。
さらに、管理装置７０は、第１トランザクションＴｘＡのＳｃｒｉｐｔＳｉｇに電子署名Ｓｉｇ＿Ａを記載する。
なお、第２トランザクションを使用しない構成の場合は、第１トランザクションＴｘＡの付加情報として、直接上記の情報を記載してもよい。
管理装置７０は、作成した第１トランザクションＴｘＡをブロックチェーン（ネットワーク３０）に公開する。
【００８５】
ステップ（３４）において、購入者は、管理装置７０が第１トランザクションＴｘＡを公開したブロックチェーンの改ざん成功確率が十分に低くなるまで待ってから、秘密値Ｒを決済装置８０に対して提示する。
決済装置８０は、ＵＳＢメモリ等のトークンを差し込む差し込み口（ポート）を備える。購入者が差し込み口に、秘密値Ｒを格納したトークンを差し込むと、決済装置８０は、秘密値Ｒをトークンから読み込むことが出来る。
あるいは、決済装置８０は、紙に印字され、あるいは、利用者装置９０としての携帯端末の表示画面に表示されたＱＲコード（登録商標）やバーコードをスキャンして、秘密値Ｒを読み取ることが出来るカメラ等の読み取り装置を備える。購入者が、コンビニエンスストア等で発行された紙に印字されたＱＲコード（登録商標）やバーコード、あるいは、自身の携帯端末（利用者装置９０）の表示画面に表示されたＱＲコード（登録商標）やバーコードを読み取り装置にかざすと、決済装置８０は、秘密値ＲをＱＲコード（登録商標）やバーコードから読みとることが出来る。
【００８６】
秘密値Ｒを受け取った後の、決済装置８０による以下のステップ（３５）～（３８）の処理は、上記のステップ（１５）～（１８）と同じであるので説明を省略する。
【００８７】
図７は、図６で説明したロック解除処理を説明するフローチャートである。
以下の説明では、トランザクションスクリプトとして、Ｐ２ＰＫＨを用いるものとして説明する。
ステップＳ２０１において、購入者は販売者に対して現金を支払い、管理装置７０が入金

を確認すると、ステップＳ２０２において、管理装置７０は秘密値Ｒをランダムに決定する。
ステップＳ２０３において、管理装置７０は、管理装置７０の秘密鍵で電子署名Ｓｉｇ＿Ａを作成する。
ステップＳ２０４において、管理装置７０は、秘密値Ｒと電子署名Ｓｉｇ＿Ａを提供する。
ステップＳ２０５において、利用者装置９０は、電子署名Ｓｉｇ＿Ａを記載した第１トランザクションＴｘＡを作成する。
ステップＳ２０６において、利用者装置９０は、第１トランザクションＴｘＡをネットワーク３０に公開する。
ステップＳ２０７において、利用者装置９０は、秘密値Ｒを決済装置８０に提示する。
【００８８】
ステップＳ２０８において、決済装置８０は第１トランザクションＴｘＡを検証する。
ステップＳ２０９において、決済装置８０は、商品又はサービスを購入者に提供する。
ステップＳ２１０において、決済装置８０は、秘密値Ｒ等をデータベースに記憶する。
アトミックスワップを応用した処理を行う場合、ステップＳ２１１において、決済装置８０は、決裁装置８０の秘密鍵で電子署名Ｓｉｇ＿Ｂを作成する。トランザクションパズルを応用した処理を行う場合、決済装置８０はステップＳ２１１の処理を行わない。
アトミックスワップを応用した処理を行う場合、ステップＳ２１２において、決済装置８０は、ステップＳ２１１で作成した電子署名Ｓｉｇ＿Ｂと、ステップＳ２０７で提示された秘密値Ｒを用いて第２トランザクションＴｘＢを作成する。トランザクションパズルを応用した処理を行う場合、決済装置８０は、電子署名Ｓｉｇ＿Ｂを用いず秘密値Ｒを用いて第２トランザクションＴｘＢを作成する。
ステップＳ２１３において、決済装置８０は、第２トランザクションＴｘＢをネットワーク３０に公開する。
【００８９】
［第３実施例］
本実施形態のロック解除システムは、プリペイドシステムのみならず、スマートキーにも適用することが出来る。
例えば、同じ自動販売機ベンダの例を考えると、自動販売機（決済装置８０）に商品を補充するには、システムの利用者である作業員（作業者）等が自動販売機の扉の施錠を解除して扉を開放し、自動販売機の内部に商品を補充する。
通常は物理的な鍵を携行する作業者が自動販売機の扉を解錠して商品を補充している。
この方法では、第三者であっても鍵を入手すれば扉を解錠でき、自動販売機内の商品や売上金を持ち出される恐れがある。
そこで、物理的な鍵を利用せず、使い捨てのＩＤ情報を使って自動販売機を解錠できるようにすることで、このような不正を防止することが出来る。
自動販売機ベンダの管理者は、自動販売機に商品の補充に向かう作業者に秘密値Ｒを渡す。このとき、秘密値Ｒは、ＵＳＢメモリなど自動販売機に対して着脱可能な記憶媒体に格納された状態で作業者に渡される。
【００９０】
現場に到着した作業者は、秘密値Ｒを使って自動販売機を解錠する。秘密値Ｒを格納したＵＳＢメモリ等の記憶媒体は、スマートキーとして用いることが出来る。
秘密値Ｒを用いたスマートキーを実現する場合でも、アトミックスワップ、トランザクションパズルの何れをも利用可能であり、上記４つのパターンを適用することが出来るが、特に受領者の電子署名を求めることで受領者を限定するアトミックスワップを好適に採用することが出来る。
複数の自動販売機（決済装置８０）夫々に秘密鍵Ｐｒｋ＿Ｂを与えてもよい。秘密値Ｒと自動販売機（決済装置８０）が一対一対応するため、秘密値Ｒは個々の自動販売機専用の鍵になる。ある自動販売機のために発行した秘密値Ｒを別の自動販売機に読み込ませても

解錠することができないからである。
秘密値Ｒは、一度ブロックチェーンに公開されると二度は使用できないので、使い捨てのＩＤ情報として用いることが出来る。
第１トランザクションＴｘＡに記載される電子署名に基づいて、第１トランザクションＴｘＡの発行元が管理会社であることを確認できる。電子署名に限らず、その他のトークンによって第１トランザクションＴｘＡの発行元を特定可能としてもよい。
【００９１】
図８は、第３実施例のロック解除処理の流れを説明する図である。
以下の説明では、トランザクションスクリプトとして、Ｐ２ＰＫＨを用いるものとして説明する。
ステップ（５１）において、管理装置７０は、秘密値Ｒをランダムに決定し、管理装置７０の秘密鍵Ｐｒｋ＿Ａから電子署名Ｓｉｇ＿Ａを作成する。また管理装置７０は、決定した秘密値Ｒにハッシュ関数を適用してハッシュ値Ｈを生成する。
【００９２】
なお、作業者（利用者）自らが秘密値Ｒを作成し、あるいは作業者の端末装置（利用者装置９０）を用いて秘密値Ｒをランダムに決定し、管理装置７０に提供してもよい。その場合、管理装置７０は、提供された秘密値Ｒに対してハッシュ関数を適用してハッシュ値Ｈを生成する。管理装置７０は秘密値Ｒの生成には関与せず、ハッシュ値Ｈの生成、電子署名Ｓｉｇ＿Ａの生成を行う。
また、作業者自らがハッシュ値Ｈも作成し、あるいは利用者装置９０を用いて秘密値Ｒにハッシュ関数を適用してハッシュ値Ｈを生成し、管理装置７０に提供してもよい。この場合、管理装置７０は、電子署名Ｓｉｇ＿Ａの生成のみを行う。
秘密値Ｒを利用者が決定する場合は、例えば秘密値Ｒの提示を条件としたＰＣの起動やログオン許可等に適用することが考えられる。この場合管理装置７０は、例えば会社等に属するＰＣに対する社員ユーザのログオン許可を管理する管理サーバなどが相当する。
【００９３】
ステップ（５２）において、管理装置７０は、第１トランザクションＴｘＡを作成する。
アトミックスワップを応用した処理を行う場合、第１トランザクションＴｘＡは、決済装置８０の電子署名Ｓｉｇ＿Ｂ、秘密値Ｒを、対応する第２トランザクションＴｘＢのＳｃｒｉｐｔＳｉｇに記載することを条件にアンロック可能なトランザクションである。受領者は決済装置８０に限定される。
第１トランザクションＴｘＡのＳｃｒｉｐｔＰｕｂＫｅｙに、決済装置８０の公開鍵、秘密値Ｒのハッシュ値Ｈを記載する。
第１トランザクションＴｘＡのＳｃｒｉｐｔＳｉｇに電子署名Ｓｉｇ＿Ａを記載する。
【００９４】
トランザクションパズルを応用した処理を行う場合、第１トランザクションＴｘＡは、秘密値Ｒを対応する第２トランザクションＴｘＢのＳｃｒｉｐｔＳｉｇに記載することを条件にアンロック可能なトランザクションである。
第１トランザクションＴｘＡのＳｃｒｉｐｔＰｕｂＫｅｙに、秘密値Ｒのハッシュ値Ｈに記載し、決済装置８０の公開鍵は記載しない。第１トランザクションＴｘＡは受領者を限定しないトランザクションである。
第１トランザクションＴｘＡのＳｃｒｉｐｔＳｉｇに電子署名Ｓｉｇ＿Ａを記載する。
管理装置７０は、作成した第１トランザクションＴｘＡをブロックチェーン（ネットワーク３０）に公開する。
【００９５】
ステップ（５３）において、管理装置７０は、秘密値Ｒを作業者に提供する。秘密値Ｒの提供は、秘密値Ｒを作業者が所持するＵＳＢメモリやトークン等に格納してもよい。あるいは、作業者が所持する携帯端末（利用者装置９０）にＥ－ＭＡＩＬその他の手段で秘密値Ｒを送信し、同携帯端末の画面にＱＲコード（登録商標）やバーコードとして表示可能としてもよい。

この時、第１トランザクションＴｘＡのトランザクションＩＤも同時に提供すると、決済装置８０の処理負荷が軽減される。
秘密値Ｒを受け取った作業者は、管理装置７０が第１トランザクションＴｘＡを公開したブロックチェーンの改ざん成功確率が十分に低くなるまで待ってから、秘密値Ｒを決済装置８０に対して提示する。
決済装置８０は、ＵＳＢメモリ等のトークンを差し込む差し込み口（ポート）を備える。作業者が差し込み口に、秘密値Ｒを格納したトークンを差し込むと、決済装置８０は、秘密値Ｒをトークンから読み込むことが出来る。
あるいは、決済装置８０は、紙に印字され、あるいは、利用者装置９０としての携帯端末の表示画面に表示されたＱＲコード（登録商標）やバーコードをスキャンして、秘密値Ｒを読み取ることが出来るカメラ等の読み取り装置を備える。作業者が、紙に印字されたＱＲコード（登録商標）やバーコード、あるいは、利用者装置９０の表示画面に表示されたＱＲコード（登録商標）やバーコードを読み取り装置にかざすと、決済装置８０は、ＱＲコード（登録商標）やバーコードから秘密値Ｒを読みとることが出来る。
【００９６】
ステップ（５４）において、決済装置８０は、公開されている第１トランザクションＴｘＡを検証する。
秘密値Ｒにハッシュ値を適用して得たハッシュ値が第１トランザクションＴｘＡに含まれるハッシュ値Ｈと一致する場合には、第１トランザクションＴｘＡが秘密値Ｒを用いてアンロック可能である。この場合、決済装置８０は、第１トランザクションＴｘＡに記載される電子署名を取得する。
決済装置８０は、第１トランザクションＴｘＡに記載の電子署名を検証して、第１トランザクションＴｘＡに管理装置７０の電子署名Ｓｉｇ＿Ａが付与されていることを確認する。
ステップ（５５）において、電子署名Ｓｉｇ＿Ａが付与されている場合、例えば自動販売機である決済装置８０は、図示しない解錠機構によって扉の施錠を解除する。
ステップ（５６）において、決済装置８０は、秘密値Ｒ、秘密値Ｒのハッシュ値Ｈ、第１トランザクションＴｘＡのトランザクションＩＤ、電子署名Ｓｉｇ＿Ａうち、少なくとも一つを、決済装置８０が備えるデータベースに記憶する。
【００９７】
その後、決済装置８０は、第１トランザクションＴｘＡをアンロックするための第２トランザクションＴｘＢを公開することが出来る。
ステップ（５７）において、アトミックスワップを応用した処理を行う場合には、決済装置８０は、決済装置８０の秘密鍵Ｐｒｋ＿Ｂで電子署名Ｓｉｇ＿Ｂを作成する。トランザクションパズルを応用した処理を行う場合は電子署名Ｓｉｇ＿Ｂの作成は不要である。
そして決済装置８０は、第１トランザクションＴｘＡをアンロックするための第２トランザクションＴｘＢを作成する。
【００９８】
アトミックスワップを応用した処理を行う場合は、第２トランザクションＴｘＢのＳｃｒｉｐｔＰｕｂＫｅｙに、決済装置８０の公開鍵を記載し、第２トランザクションＴｘＢのＳｃｒｉｐｔＳｉｇに、電子署名Ｓｉｇ＿Ｂ、決済装置８０の公開鍵、秘密値Ｒを記載する。
トランザクションパズルを応用した処理を行う場合は、第２トランザクションＴｘＢは、第２トランザクションＴｘＢのＳｃｒｉｐｔＰｕｂＫｅｙに、決済装置８０の公開鍵を記載し、第１トランザクションＴｘＡのＳｃｒｉｐｔＳｉｇに、決済装置８０の公開鍵、秘密値Ｒを記載する。電子署名Ｓｉｇ＿Ｂは記載しない。
そして、決済装置８０は、作成した第２トランザクションＴｘＢをブロックチェーン（ネットワーク３０）に公開する。
【００９９】
本実施形態のロック解除システムにおいて、第１トランザクションＴｘＡをアンロックで

きる秘密値Ｒを作業者が所持していることが重要である。従って、作業者が決済装置８０に提示したことに応じて、決済装置８０は、指定の処理（施錠を解除）を実行する。
施錠の解除後、第２トランザクションＴｘＢをブロックチェーンに公開すると、履歴情報（秘密値Ｒ、ハッシュ値Ｈ、秘密鍵、トランザクションＩＤ）がブロックチェーンに記録されるため、決済装置８０における解錠記録を外部から確認することが出来る。
ただし、これに限らず、第２トランザクションＴｘＢをブロックチェーンに公開したあとで、指定の処理（施錠の解除）を実行してもよい。ステップ（５４）とステップ（５５）の間に、ステップ（５７）を実行してもよい。
上記のように、作業者は、第１トランザクションＴｘＡ取り消される確率が十分に低くなった時点以降に秘密値Ｒを決済装置８０に提示する。よって、決済装置８０は、施錠を解除した後に秘密値Ｒ（第２トランザクションＴｘＢ）を公開してもよいし、秘密値Ｒ（第２トランザクションＴｘＢ）を公開してから施錠を解除してもよい。
なお、本実施形態では、第１トランザクションＴｘＡと決済装置８０による施錠解除時の第２トランザクションＴｘＢと、の２段階のトランザクションを発行している。第１トランザクションＴｘＡについては、承認数が十分に増えるまでの時間を待つ必要があるが、第２トランザクションＴｘＢについて承認数が増えるのを待つ必要がなく、データベースに記憶した秘密値Ｒと同じ秘密値Ｒが提示されてないことを条件に即時施錠を解除することが出来る。
第２トランザクションＴｘＢが取り消されデータベースに記憶した秘密値Ｒと同じ秘密値Ｒが提示された場合でも、施錠を解除しなければよい。
また、データベースに記憶する秘密値Ｒ、秘密値Ｒのハッシュ値Ｈ、第１トランザクションＴｘＡのトランザクションＩＤ、電子署名Ｓｉｇ＿Ａによって第２トランザクションＴｘＢを公開しなおせばよい。
作業者は、施錠の解除前に第２トランザクションＴｘＢの十分な数の承認を待機する必要がなく、作業の効率性を高めることが出来る。
【０１００】
また上記したように、トランザクションパズルを応用し、決済装置８０にとってのみ電子署名の価値がある場合には、二重使用が行われことは想定しにくいので、第２トランザクションＴｘＢの十分な数の承認を待機する必要がなく、利便性を高めることが出来る。
アトミックスワップでは、秘密値Ｒに加えて決済装置８０の電子署名がないと第１トランザクションＴｘＡを受け取れないので、暗号資産の二重使用は不可能である。よって、購入者が、施錠の解除前に第２トランザクションＴｘＢの十分な数の承認を待機する必要がない。
【０１０１】
図９は、図８で説明した解錠処理を説明するフローチャートである。
以下の説明では、トランザクションスクリプトとして、Ｐ２ＰＫＨを用いるものとして説明する。
ステップＳ３０１において、管理装置７０は、秘密値Ｒをランダムに決定する。
ステップＳ３０２において、管理装置７０は、管理装置７０の秘密鍵で電子署名Ｓｉｇ＿Ａを作成する。
ステップＳ３０３において、管理装置７０は、秘密値Ｒと電子署名Ｓｉｇ＿Ａを用いた第１トランザクションＴｘＡを作成する。
ステップＳ３０４において、管理装置７０は、第１トランザクションＴｘＡをネットワーク３０に公開する。
ステップＳ３０５において、管理装置７０は、秘密値Ｒを作業者に提供する。
ステップＳ３０６において、作業者は、秘密値Ｒを決済装置８０に提示する。
ステップＳ３０７において、決済装置８０は第１トランザクションＴｘＡを検証する。
ステップＳ３０８において、決済装置８０は、扉の施錠を解除する。
ステップＳ３０９において、決済装置８０は、秘密値Ｒ等をデータベースに記憶する。
【０１０２】

アトミックスワップを応用した処理を行う場合、ステップＳ３１０において、決済装置８０は、決裁装置８０の秘密鍵で電子署名Ｓｉｇ＿Ｂを作成する。トランザクションパズルを応用した処理を行う場合、決済装置８０はステップＳ３１０の処理を行わない。
ステップＳ３１１において、決済装置８０は第２トランザクションＴｘＢを作成する。
アトミックスワップを応用した処理を行う場合、決済装置８０は、電子署名Ｓｉｇ＿Ｂと秘密値Ｒを用いて第２トランザクションＴｘＢを作成する。トランザクションパズルを応用した処理を行う場合、決済装置８０は、電子署名Ｓｉｇ＿Ｂを用いず、秘密値Ｒを用いて第２トランザクションＴｘＢを作成する。
ステップＳ３１０において、決済装置８０は、第２トランザクションＴｘＢをネットワーク３０に公開する。

【０１０３】
なお、図８、図９に示すスマートロックの場合も、上記のプリペイドシステムと同様に、トランザクションＡを利用者装置９０が公開してもよい。
その場合も、管理装置７０は、秘密値Ｒをランダムに決定し、管理装置７０の秘密鍵Ｐｒｋ＿Ａから電子署名Ｓｉｇ＿Ａを作成し、秘密値Ｒにハッシュ関数を適用してハッシュ値Ｈを生成する。管理装置７０は、秘密値Ｒ、電子署名Ｓｉｇ＿Ａ、ハッシュ値Ｈを、作業者に提供する。
また、作業者（利用者）自らが秘密値Ｒを作成し、あるいは作業者の端末装置（利用者装置９０）を用いて秘密値Ｒをランダムに決定し、管理装置７０に提供してもよい。その場合、管理装置７０は、提供された秘密値Ｒに対してハッシュ関数を適用してハッシュ値Ｈを生成する。管理装置７０は秘密値Ｒの生成には関与せず、ハッシュ値Ｈの生成、電子署名Ｓｉｇ＿Ａの生成を行い、電子署名Ｓｉｇ＿Ａ、ハッシュ値Ｈを作業者に提供する。
また、作業者自らがハッシュ値Ｈをも作成し、あるいは利用者装置９０を用いて秘密値Ｒにハッシュ関数を適用してハッシュ値Ｈを生成し、作業者に提供してもよい。この場合、管理装置７０は、電子署名Ｓｉｇ＿Ａの生成のみを行い、生成した電子署名Ｓｉｇ＿Ａを作業者に提供する。

【０１０４】
装置管理装置、決済装置、利用者装置について説明する。
図１０乃至図１３は、各装置の一実施例を示す機能ブロック図である。
管理装置７０、決済装置８０、利用者装置９０は夫々、他の装置が有する機能の少なくとも１つ以上の機能を有してもよい。
図１０は管理装置７０が有する機能を示すブロック図である。
図１０を参照して、管理装置７０の機能を説明する。
管理装置７０は、制御部６０と、通信部９１と、記憶部９２とを含む。
制御部６０は、確認部６１と、決定部６２と、生成部６３と、出力部６４と、作成部６５と、公開部６６と、取得部６７と、を含む。通信部９１は、管理装置７０をネットワークに接続する。記憶部９２は、各種情報を記憶する。

【０１０５】
確認部６１は、例えば、外部の収納代行サービスなどを介して、購入者よりの事前入金を確認する。
決定部６２は、秘密値Ｒをランダムに決定する。
生成部６３は、管理装置７０の秘密鍵から電子署名を生成し、秘密値ＲからハッシュＨを生成する。
出力部６４は、決定した秘密値Ｒ、生成した電子署名、ハッシュ値Ｈを、購入者に向けて出力する。具体的には、秘密値Ｒを紙出力させるために収納代行サービスに向けて出力したり、電子署名、ハッシュ値ＨをＥ－ＭＡＩＬなどで利用者装置９０に向けて送信したりする。
作成部６５は、第１トランザクションＴｘＡを作成する。
公開部６６は、作成部６５が作成した第１トランザクションＴｘＡをネットワーク３０に公開する。

取得部６７は、例えば、外部の収納代行サービスなどを介して、利用者装置９０から秘密値Ｒ、ハッシュ値Ｈを取得する。
【０１０６】
図１１は、決済装置８０が有する機能を示すブロック図である。
図１１を参照して、決済装置８０の機能を説明する。
決済装置８０は、制御部１００と、通信部１１１と、記憶部１１２とを含む。
制御部１００は、受取部１０１と、取得部１０２、生成部１０３と、作成部１０４と、公開部１０５と、格納部１０６と、実行部１０７を含む。
記憶部１１２は、各種情報を記憶する。記憶部１１２は、例えば、秘密値Ｒ、管理装置７０の電子署名、ハッシュ値Ｈ等のデータベースを記憶する。
受取部１０１は、購入者や作業者から提示されたＱＲコード（登録商標）やトークン（ＵＳＢメモリ）から、秘密値Ｒを取得する。
取得部１０２は、受取部１０１により受け取った秘密値を用いて第１トランザクションＴｘＡがアンロック可能な場合、第１トランザクションＴｘＡに含まれる識別情報（電子署名）を取得する。
生成部１０３は、決済装置８０の秘密鍵から電子署名を生成する。
作成部１０４は、第２トランザクションＴｘＢを作成する。
公開部１０５は、作成部１０３が作成した第２トランザクションＴｘＢをネットワーク３０に公開する。
格納部１０６は、秘密値Ｒ、管理装置７０の電子署名、ハッシュ値Ｈ等を記憶部１１２のデータベースに格納する。
実行部１０７は、所定の払出機構を制御して商品の払出を行い、所定の解錠機構を制御して施錠する、などの処理を実行する。
【０１０７】
図１２は、利用者装置９０が有する機能を示すブロック図である。
図１２を参照して、利用者装置９０の機能を説明する。
決済装置８０は、制御部１２０と、通信部１３１と、記憶部１３２と、表示部１３３とを含む。
制御部１２０は、取得部１２１と、決定部１２２と、生成部１２３と、作成部１２４と、公開部１２５と、出力部１２６と、を含む。
取得部１２１は、管理装置７０から、秘密値Ｒ、ハッシュ値Ｈ、管理装置７０の電子署名を取得する。
決定部１２２は、秘密値Ｒをランダムに決定する。
生成部１２３は、秘密値Ｒからハッシュ値Ｈを生成し、秘密値Ｒに基づくコード情報（ＱＲコード（登録商標）、バーコード）を生成する。
作成部１２４は、第１トランザクションＴｘＡを作成する。
公開部１２５は、作成部１２４が作成した第１トランザクションＴｘＡをネットワーク３０に公開する。
受渡部１２６は、生成部１２３が生成したコード情報を表示部１３３に表示して秘密値Ｒを決済装置８０に受け渡す。
【０１０８】
図１３は、コンピュータ装置の一実施例を示すブロック図である。
図１３を参照して、コンピュータ装置５０の構成について説明する。
図１３において、コンピュータ装置５０は、制御回路５１と、記憶装置５２と、読書装置５３と、記録媒体５４、通信インターフェイス５５と、入出力インターフェイス５６と、入力装置５７と、表示装置５８とを含む。また、通信インターフェイス５５は、ネットワーク６００と接続される。そして各構成要素は、バス５９により接続される。取引装置１０、取引装置２０、管理装置７０、決済装置８０及び利用者装置９０は、コンピュータ装置５０に記載の構成要素の一部または全てを適宜選択して構成することができる。
【０１０９】

制御回路５１は、コンピュータ装置５０全体の制御をする。制御回路５１は、例えば、Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ（ＣＰＵ）、Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ（ＦＰＧＡ）、Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ（ＡＳＩＣ）及びＰｒｏｇｒａｍｍａｂｌｅ Ｌｏｇｉｃ Ｄｅｖｉｃｅ（ＰＬＤ）などのプロセッサである。制御回路５１は、例えば、図１０において、制御部６０として機能する。また制御回路５１は、図１１において、制御部１００として機能する。制御回路５１は、例えば、図１２において、制御部１２０として機能する。

記憶装置５２は、各種データを記憶する。そして、記憶装置５２は、例えば、Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ（ＲＯＭ）及びＲａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ（ＲＡＭ）などのメモリや、Ｈａｒｄ Ｄｉｓｋ（ＨＤ）などである。記憶装置５２は、制御回路５１を、制御部６０として機能させるロック解除プログラムを記憶してもよい。記憶装置５２は、例えば、図１０において、記憶部９２として機能する。また記憶部５２は、図１１において、記憶部１１２として機能する。また記憶部５２は、図１２において記憶部１３２として機能する。

【０１１０】

管理装置７０、決済装置８０及び利用者装置９０は、ロック解除処理をするとき、記憶装置５２に記憶されたロック解除プログラムをＲＡＭに読み出す。

ＲＡＭに読み出されたロック解除プログラムを制御回路５１で実行することにより、管理装置７０は、確認処理と、決定処理と、生成処理と、出力処理と、作成処理と、公開処理と、のいずれか１以上を含むロック解除処理を実行する。

また決済装置８０は、ＲＡＭに読み出されたロック解除プログラムを制御回路５１で実行することにより、取得処理と、生成処理と、作成処理と、公開処理と、格納処理と、のいずれか１以上を含むロック解除処理を実行する。

また決済装置９０は、ＲＡＭに読み出されたロック解除プログラムを制御回路５１で実行することにより、取得処理と、決定処理と、生成処理と、作成処理と、公開処理と、受渡処理と、のいずれか１以上を含むロック解除処理を実行する。

なお、ロック解除プログラムは、制御回路５１が通信インターフェイス５５を介してアクセス可能であれば、ネットワーク６００上のサーバが有する記憶装置に記憶されていても良い。

【０１１１】

読書装置５３は、制御回路５１に制御され、着脱可能な記録媒体５４のデータのリード／ライトを行なう。

記録媒体５４は、各種データを保存する。記録媒体５４は、例えば、ロック解除処理プログラムを記憶する。記録媒体５４は、例えば、Ｓｅｃｕｒｅ Ｄｉｇｉｔａｌ（ＳＤ）メモリーカード、Ｆｌｏｐｐｙ Ｄｉｓｋ（ＦＤ）、Ｃｏｍｐａｃｔ Ｄｉｓｃ（ＣＤ）、Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ（ＤＶＤ）、Ｂｌｕ－ｒａｙ（登録商標） Ｄｉｓｋ（ＢＤ）、及びフラッシュメモリなどの不揮発性メモリ（非一時的記録媒体）である。

【０１１２】

通信インターフェイス５５は、ネットワーク６００を介してコンピュータ装置５０と他の装置とを通信可能に接続する。通信インターフェイス５５は、例えば、図１０において、通信部９１として機能する。

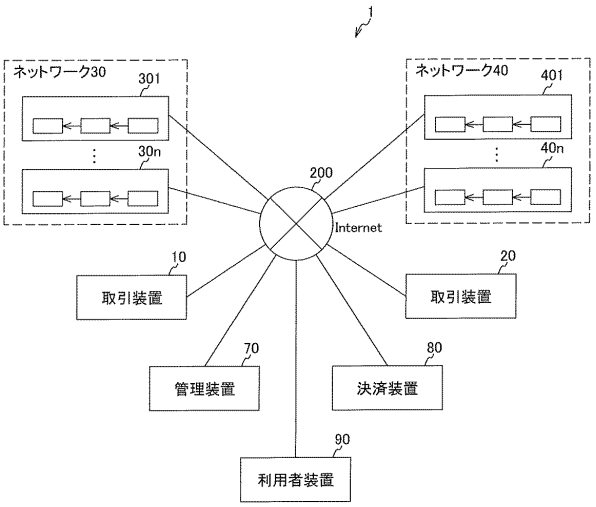
通信インターフェイス５５は、例えば、図１０において、通信部９１として機能する。また通信インターフェイス５５は、図１１において、通信部１１１として機能する。また通信インターフェイス５５は、図１２において、通信部１３２として機能する。

入出力インターフェイス５６は、例えば、各種入力装置と着脱可能に接続するインターフェイスである。入出力インターフェイス５６は、接続された各種入力装置とコンピュータ装置５０とを通信可能に接続する。そして、入出力インターフェイス５６は、接続された各種入力装置から入力された信号を、バス５９を介して制御回路５１に出力する。また、入出力インターフェイス４０６は、制御回路５１から出力された信号を、バス５９を介し

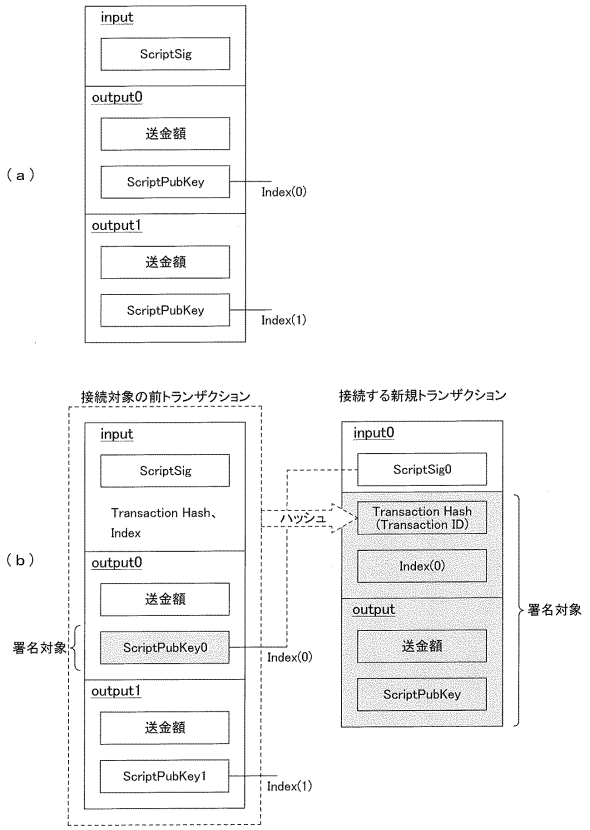
て入出力装置に出力する。
入力装置５７は、例えば、タッチパネル、コード読み取り装置、キーボード及びマウスなどである。特に入出力インターフェイス５６に接続された入力装置５７としてのコード読み取り装置は、例えば、紙や利用者装置に表示される秘密値ＲのＱＲコード（登録商標）やバーコードを介した秘密値Ｒの入力を受け付けてもよい。
表示装置５８は、各種情報を表示する。表示装置５８は、例えば、図１２の表示部１３３として機能し、秘密値ＲのＱＲコード（登録商標）やバーコードを表示してもよい。
ネットワーク６００は、例えば、ＬＡＮ、無線通信、Ｐ２Ｐネットワーク、またはインターネットなどであり、コンピュータ装置５０と他の装置を通信接続する。
なお、本実施形態は、以上に述べた実施形態に限定されるものではなく、本実施形態の要旨を逸脱しない範囲内で種々の構成または実施形態を取ることができる。
【符号の説明】
【０１１３】
５０　コンピュータ装置
５１　制御回路
５２　記憶装置
５３　読書装置
５４　記録媒体
５５　通信Ｉ／Ｆ
５６　入出力Ｉ／Ｆ
５７　入力装置
５８　表示装置
５９　バス
６０、１００　制御部
７０　管理装置
８０　決済装置
９０　利用者装置
９１、１１１、１３１　通信部
９２、１１２、１３２　記憶部
１３３　表示部

【図面】

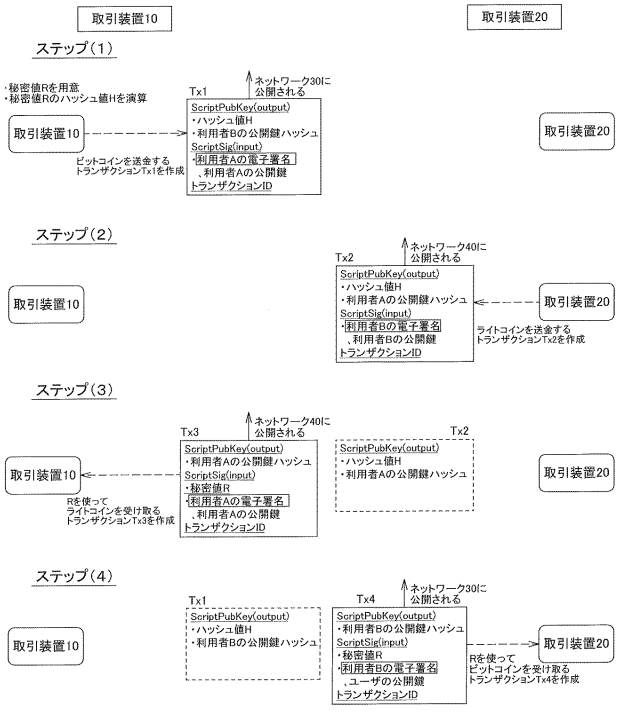
【図１】


1
ネットワーク30
301
30n
ネットワーク40
401
40n
200
Internet
10
取引装置
20
取引装置
70
管理装置
80
決済装置
90
利用者装置

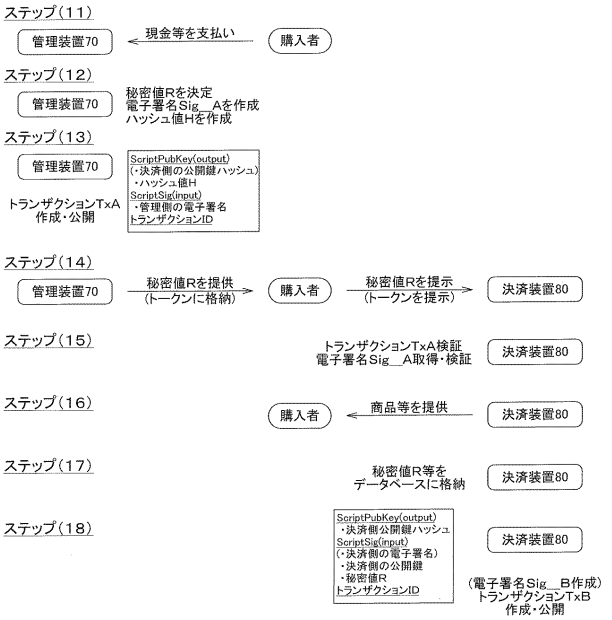
【図２】


(a)
input
ScriptSig
output0
送金額
ScriptPubKey
Index(0)
output1
送金額
ScriptPubKey
Index(1)
(b)
接続対象の前トランザクション
接続する新規トランザクション
input
ScriptSig
Transaction Hash、
Index
output0
送金額
ScriptPubKey0
Index(0)
output1
送金額
ScriptPubKey1
Index(1)
署名対象
ハッシュ
input0
ScriptSig0
Transaction Hash
(Transaction ID)
Index(0)
output
送金額
ScriptPubKey
署名対象

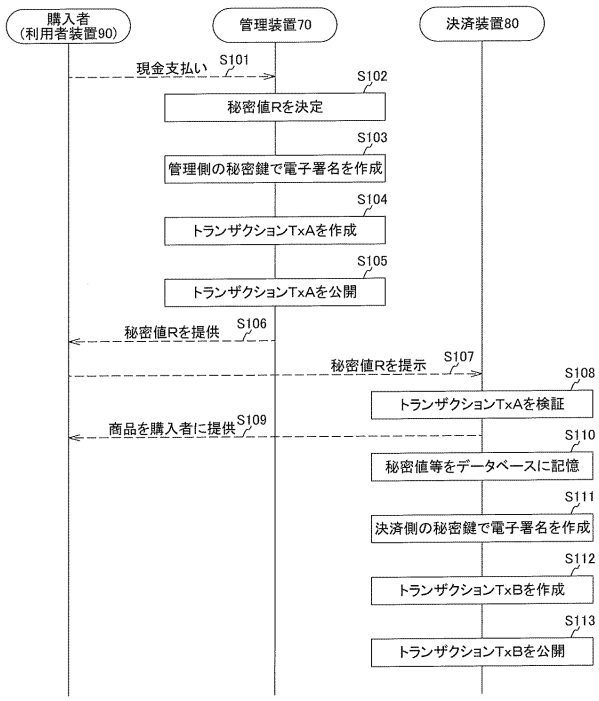
【図３】


取引装置10
取引装置20
ステップ(1)
・秘密値Rを用意
・秘密値Rのハッシュ値Hを演算
Tx1
ネットワーク30に公開される
ScriptPubKey(output)
・ハッシュ値H
・利用者Bの公開鍵ハッシュ
ScriptSig(input)
・利用者Aの電子署名
、利用者Aの公開鍵
トランザクションID
ビットコインを送金する
トランザクションTx1を作成
ステップ(2)
Tx2
ネットワーク40に公開される
ScriptPubKey(output)
・ハッシュ値H
・利用者Aの公開鍵ハッシュ
ScriptSig(input)
・利用者Bの電子署名
、利用者Bの公開鍵
トランザクションID
ライトコインを送金する
トランザクションTx2を作成
ステップ(3)
Tx3
ネットワーク40に公開される
ScriptPubKey(output)
・利用者Aの公開鍵ハッシュ
ScriptSig(input)
・秘密値R
・利用者Aの電子署名
、利用者Aの公開鍵
トランザクションID
Tx2
ScriptPubKey(output)
・ハッシュ値H
・利用者Aの公開鍵ハッシュ
Rを使って
ライトコインを受け取る
トランザクションTx3を作成
ステップ(4)
Tx1
ScriptPubKey(output)
・ハッシュ値H
・利用者Bの公開鍵ハッシュ
Tx4
ネットワーク30に公開される
ScriptPubKey(output)
・利用者Bの公開鍵ハッシュ
ScriptSig(input)
・秘密値R
・利用者Bの電子署名
、ユーザの公開鍵
トランザクションID
Rを使って
ビットコインを受け取る
トランザクションTx4を作成

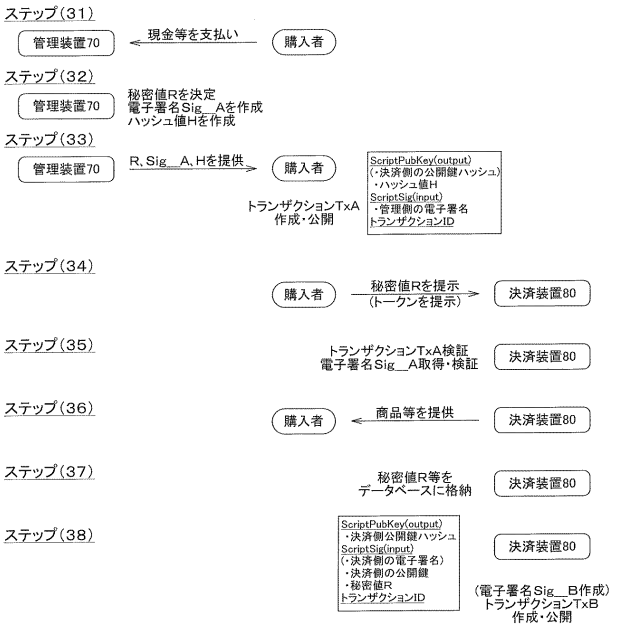
【図４】


ステップ(11)
管理装置70
現金等を支払い
購入者
ステップ(12)
管理装置70
秘密値Rを決定
電子署名Sig__Aを作成
ハッシュ値Hを作成
ステップ(13)
管理装置70
ScriptPubKey(output)
(・決済側の公開鍵ハッシュ)
・ハッシュ値H
ScriptSig(input)
・管理側の電子署名
トランザクションID
トランザクションTxA
作成・公開
ステップ(14)
管理装置70
秘密値Rを提供
(トークンに格納)
購入者
秘密値Rを提示
(トークンを提示)
決済装置80
ステップ(15)
トランザクションTxA検証
電子署名Sig__A取得・検証
決済装置80
ステップ(16)
購入者
商品等を提供
決済装置80
ステップ(17)
秘密値R等を
データベースに格納
決済装置80
ステップ(18)
ScriptPubKey(output)
・決済側公開鍵ハッシュ
ScriptSig(input)
(・決済側の電子署名)
・決済側の公開鍵
・秘密値R
トランザクションID
決済装置80
(電子署名Sig__B作成)
トランザクションTxB
作成・公開

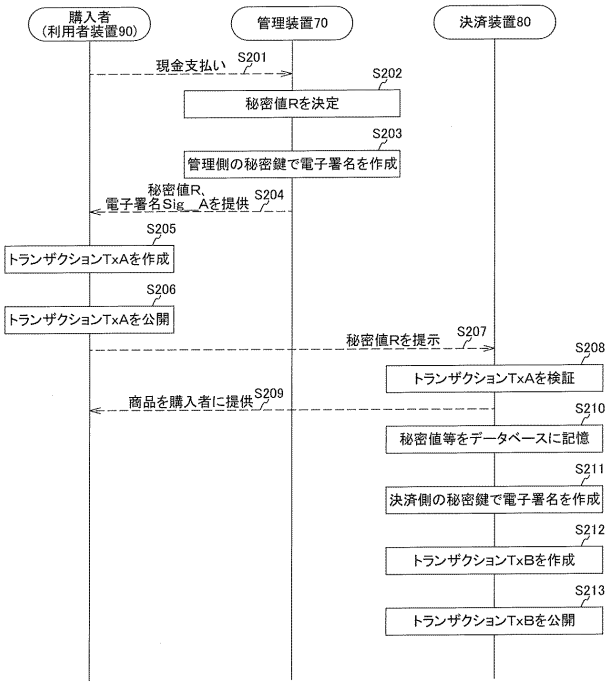
【図５】


購入者
(利用者装置90)
管理装置70
決済装置80
現金支払い
S101
S102
秘密値Rを決定
S103
管理側の秘密鍵で電子署名を作成
S104
トランザクションTxAを作成
S105
トランザクションTxAを公開
秘密値Rを提供
S106
秘密値Rを提示
S107
S108
トランザクションTxAを検証
商品を購入者に提供
S109
S110
秘密値等をデータベースに記憶
S111
決済側の秘密鍵で電子署名を作成
S112
トランザクションTxBを作成
S113
トランザクションTxBを公開

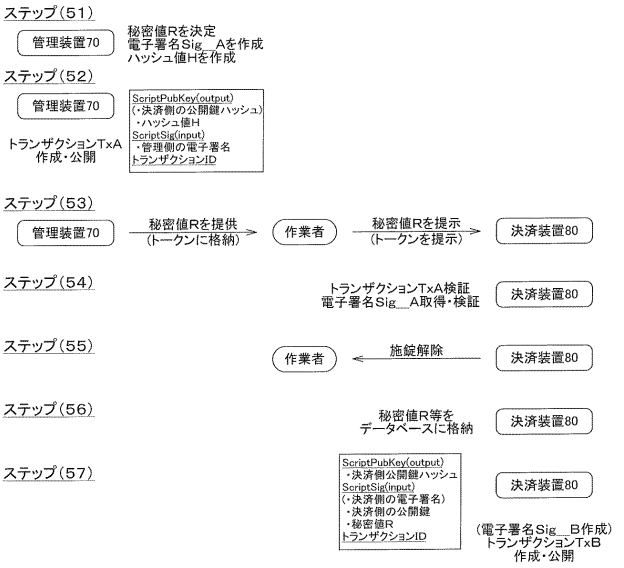
【図６】


ステップ(31)
管理装置70
現金等を支払い
購入者
ステップ(32)
管理装置70
秘密値Rを決定
電子署名Sig__Aを作成
ハッシュ値Hを作成
ステップ(33)
管理装置70
R, Sig__A, Hを提供
購入者
ScriptPubKey(output)
(・決済側の公開鍵ハッシュ)
・ハッシュ値H
ScriptSig(input)
・管理側の電子署名
トランザクションID
トランザクションTxA
作成・公開
ステップ(34)
購入者
秘密値Rを提示
(トークンを提示)
決済装置80
ステップ(35)
トランザクションTxA検証
電子署名Sig__A取得・検証
決済装置80
ステップ(36)
購入者
商品等を提供
決済装置80
ステップ(37)
秘密値R等を
データベースに格納
決済装置80
ステップ(38)
ScriptPubKey(output)
・決済側公開鍵ハッシュ
ScriptSig(input)
(・決済側の電子署名)
・決済側の公開鍵
・秘密値R
トランザクションID
決済装置80
(電子署名Sig__B作成)
トランザクションTxB
作成・公開

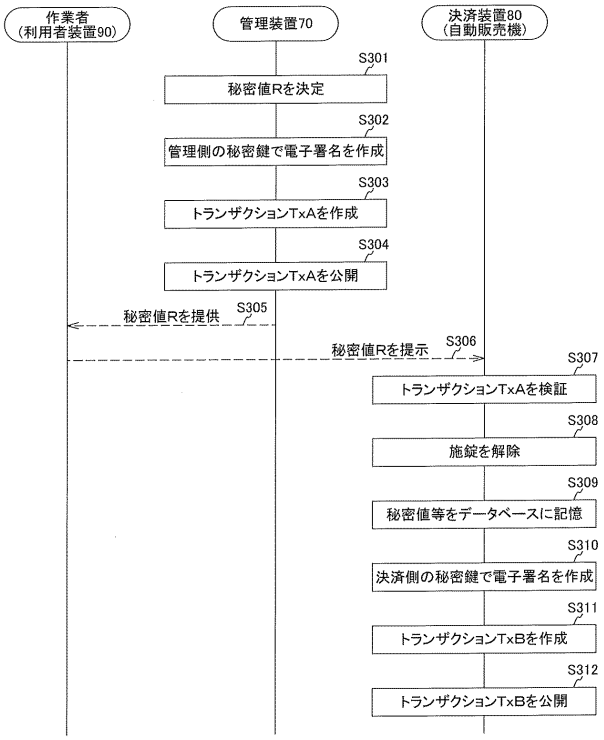
【図７】


購入者
(利用者装置90)
管理装置70
決済装置80
現金支払い
S201
S202
秘密値Rを決定
S203
管理側の秘密鍵で電子署名を作成
秘密値R、
電子署名Sig__Aを提供
S204
S205
トランザクションTxAを作成
S206
トランザクションTxAを公開
秘密値Rを提示
S207
S208
トランザクションTxAを検証
商品を購入者に提供
S209
S210
秘密値等をデータベースに記憶
S211
決済側の秘密鍵で電子署名を作成
S212
トランザクションTxBを作成
S213
トランザクションTxBを公開

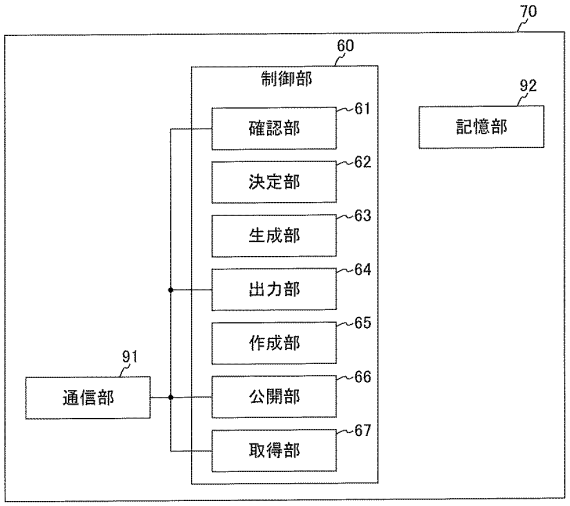
【図８】


ステップ(51)
管理装置70
秘密値Rを決定
電子署名Sig__Aを作成
ハッシュ値Hを作成
ステップ(52)
管理装置70
ScriptPubKey(output)
(・決済側の公開鍵ハッシュ)
・ハッシュ値H
ScriptSig(input)
・管理側の電子署名
トランザクションID
トランザクションTxA
作成・公開
ステップ(53)
管理装置70
秘密値Rを提供
(トークンに格納)
作業者
秘密値Rを提示
(トークンを提示)
決済装置80
ステップ(54)
トランザクションTxA検証
電子署名Sig__A取得・検証
決済装置80
ステップ(55)
作業者
施錠解除
決済装置80
ステップ(56)
秘密値R等を
データベースに格納
決済装置80
ステップ(57)
ScriptPubKey(output)
・決済側公開鍵ハッシュ
ScriptSig(input)
(・決済側の電子署名)
・決済側の公開鍵
・秘密値R
トランザクションID
決済装置80
(電子署名Sig__B作成)
トランザクションTxB
作成・公開

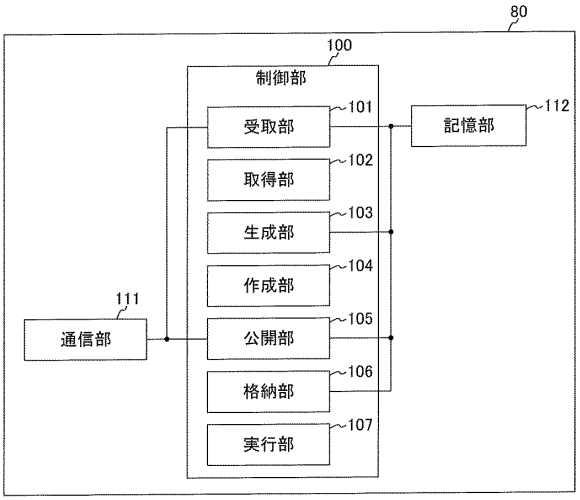
【図９】



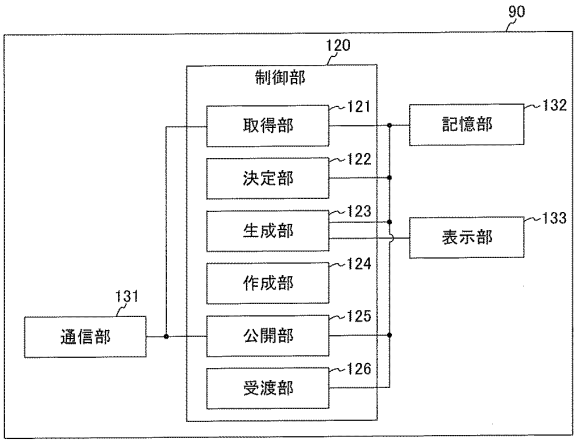
【図１０】



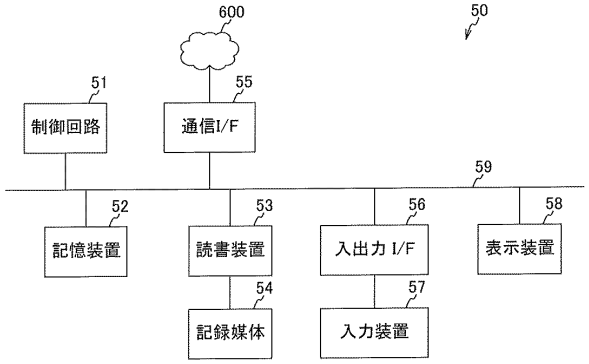
【図１１】



【図１２】



【図１３】


600
50
51
55
制御回路
通信I/F
59
52
53
56
58
記憶装置
読書装置
入出力 I/F
表示装置
54
57
記録媒体
入力装置