(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2020-72307
(P2020-72307A)
(43)公開日　令和2年5月7日(2020.5.7)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675Z	5J104

審査請求 未請求　請求項の数 11　ＯＬ　（全 18 頁）

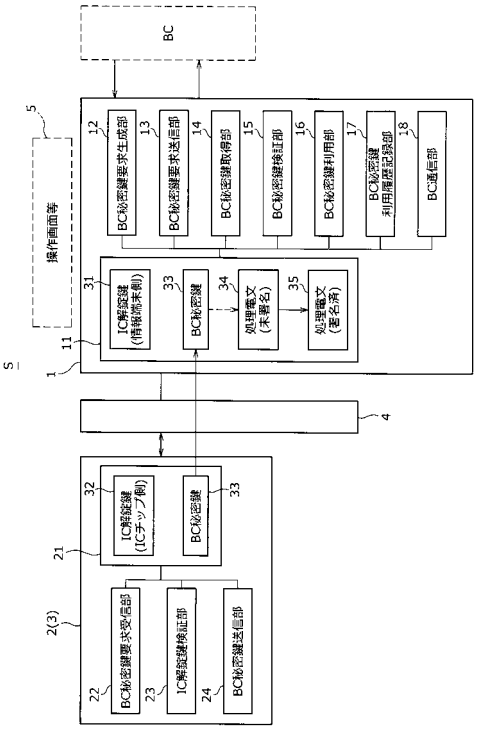
(21)出願番号　特願2018-203180 (P2018-203180)
(22)出願日　平成30年10月29日 (2018.10.29)

(71)出願人　518117599
合同会社玉木栄三郎事務所
神奈川県鎌倉市山ノ内１９７番地９
(71)出願人　510250032
フェリカポケットマーケティング株式会社
東京都港区西新橋三丁目２番１号
(74)代理人　100088580
弁理士　秋山　敦
(74)代理人　100111109
弁理士　城田　百合子
(72)発明者　玉木　栄三郎
神奈川県鎌倉市山ノ内１９７番地９　合同会社玉木栄三郎事務所内

Ｆターム(参考)　5J104 AA09 AA16 EA04 EA19 JA21 LA03 NA35 NA37 NA40 PA12

(54)【発明の名称】分散型ネットワークにおける秘密鍵管理システム及び秘密鍵管理方法

(57)【要約】
【課題】利用時の利便性を損なうことなく、安全且つ簡便な方法で秘密鍵を保持及び利用することができ、さらに、正当な秘密鍵の保有者による不正をも防止することができる分散型ネットワークにおける秘密鍵管理システム及び秘密鍵管理方法を提供する。
【解決手段】秘密鍵管理システムＳは、ブロックチェーンと通信可能に接続された情報端末１と、ＢＣ秘密鍵３３を保持するＩＣチップ２を組み込んだＩＣカード３と、ＩＣリーダー４と、から主に構成されている。ＢＣ秘密鍵３３は、ネットワークとは完全に遮断されたＩＣチップ２側の暗号化されたメモリ内に保持している。情報端末１とＩＣチップ２とはＩＣ解錠鍵３１，３２による認証を行い、情報端末１は、ＩＣリーダー４を介してＩＣチップ２にＢＣ秘密鍵３３の利用を要求し、ＩＣチップ２から読み取ったＢＣ秘密鍵３３を利用して処理電文３４に署名し、署名済の処理電文３５をブロックチェーンに送信する。
【選択図】図２



【特許請求の範囲】
【請求項１】
分散型ネットワークを構成するノードと通信可能に接続され、前記ノードとの間で処理情報を送受信する情報端末と、
ネットワークから遮断され、専用リーダーを介して前記情報端末と接触型又は非接触型の通信手段により通信可能なＩＣチップを組み込んだ媒体と、から構成される秘密鍵管理システムであって、
前記ＩＣチップは、前記分散型ネットワーク上の所有者情報に関連する情報であって前記処理情報に署名をするための秘密鍵情報と、該秘密鍵情報に対して外部からのアクセスの可否を判断するための第１解錠鍵情報とを記憶し、
前記情報端末は、前記ＩＣチップ内に記憶された前記秘密鍵情報にアクセスするための第２解錠鍵情報を記憶し、
前記秘密鍵管理システムは、
前記第１解錠鍵情報と前記第２解錠鍵情報との整合性を検証する解錠鍵検証手段と、
前記秘密鍵情報の利用可否を検証し、前記秘密鍵情報を利用可能と判断した場合に前記秘密鍵情報を利用して前記処理情報に署名する秘密鍵利用手段と、を備えることを特徴とする分散型ネットワークにおける秘密鍵管理システム。
【請求項２】
前記秘密鍵管理システムは、前記秘密鍵利用手段を前記情報端末側に備え、
前記情報端末は、
前記ＩＣチップに対して前記秘密鍵情報の送信を要求する秘密鍵要求手段と、
前記ＩＣチップから送信された前記秘密鍵情報を取得する秘密鍵取得手段と、をさらに備えることを特徴とする請求項１に記載の分散型ネットワークにおける秘密鍵管理システム。
【請求項３】
前記秘密鍵管理システムは、前記秘密鍵利用手段を前記ＩＣチップ側に備え、
前記ＩＣチップは、
前記秘密鍵利用手段により前記処理情報に署名した署名済処理情報を前記情報端末に送信する署名済処理情報送信手段を、さらに備え、
前記情報端末は、
前記ＩＣチップに対して前記処理情報を送信する未署名処理情報送信手段と、
前記ＩＣチップから送信された前記署名済処理情報を取得して該署名済処理情報を検証する署名済処理情報検証手段と、をさらに備えることを特徴とする請求項１に記載の分散型ネットワークにおける秘密鍵管理システム。
【請求項４】
前記情報端末は、前記秘密鍵情報の利用履歴を記録する利用履歴記録手段をさらに備えることを特徴とする請求項１乃至３のいずれか１項に記載の分散型ネットワークにおける秘密鍵管理システム。
【請求項５】
前記秘密鍵情報は、前記秘密鍵利用手段により前記秘密鍵情報を利用して前記処理情報に署名した後に破棄されることを特徴とする請求項１乃至４のいずれか１項に記載の分散型ネットワークにおける秘密鍵管理システム。
【請求項６】
前記秘密鍵情報は、他の媒体に複製不可とすることを特徴とする請求項１乃至５のいずれか１項に記載の分散型ネットワークにおける秘密鍵管理システム。
【請求項７】
前記媒体は、前記秘密鍵情報により生成される情報であって、前記分散型ネットワーク上の前記所有者情報を移転させるための情報を表示することを特徴とする請求項１乃至６のいずれか１項に記載の分散型ネットワークにおける秘密鍵管理システム。
【請求項８】

前記媒体は、非接触型ＩＣカードであることを特徴とする請求項１乃至７のいずれか１項に記載の分散型ネットワークにおける秘密鍵管理システム。
【請求項９】
分散型ネットワークを構成するノードと通信可能に接続され、前記ノードとの間で処理情報を送受信する情報端末と、
ネットワークから遮断され、専用リーダーを介して前記情報端末と接触型又は非接触型の通信手段により通信可能なＩＣチップを組み込んだ媒体と、を用いる秘密鍵管理方法であって、
前記ＩＣチップは、前記分散型ネットワーク上の所有者情報に関連する情報であって前記処理情報に署名をするための秘密鍵情報と、該秘密鍵情報に対して外部からのアクセスの可否を判断するための第１解錠鍵情報とを記憶し、
前記情報端末は、前記ＩＣチップ内に記憶された前記秘密鍵情報にアクセスするための第２解錠鍵情報を記憶し、
前記情報端末又は前記ＩＣチップが、
前記第１解錠鍵情報と前記第２解錠鍵情報との整合性を検証する解錠鍵検証工程と、
前記秘密鍵情報の利用可否を検証し、前記秘密鍵情報を利用可能と判断した場合に前記秘密鍵情報を利用して前記処理情報に署名する秘密鍵利用工程と、を実行することを特徴とする分散型ネットワークにおける秘密鍵管理方法。
【請求項１０】
前記情報端末は、前記秘密鍵利用工程を実行すると共に、
前記ＩＣチップに対して前記秘密鍵情報の送信を要求する秘密鍵要求工程と、
前記ＩＣチップから送信された前記秘密鍵情報を取得する秘密鍵取得工程と、をさらに実行することを特徴とする請求項９に記載の分散型ネットワークにおける秘密鍵管理方法。
【請求項１１】
前記ＩＣチップは、前記秘密鍵利用工程を実行すると共に、
前記秘密鍵利用工程により前記処理情報に署名してその署名済処理情報を前記情報端末に送信する署名済処理情報送信工程をさらに実行し、
前記情報端末は、
前記ＩＣチップに対して前記処理情報を送信する未署名処理情報送信工程と、
前記ＩＣチップから送信された前記署名済処理情報を取得して該署名済処理情報を検証する署名済処理情報検証工程と、をさらに実行することを特徴とする請求項９に記載の分散型ネットワークにおける秘密鍵管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、分散型ネットワークにおける秘密鍵管理システム及び秘密鍵管理方法に係り、特に、分散型ネットワークで稼働する取引における所有者確認のための秘密鍵情報を保持及び利用する分散型ネットワークにおける秘密鍵管理システム及び秘密鍵管理方法に関する。
【背景技術】
【０００２】
近年、分散型ネットワークの一つとして分散型台帳技術であるブロックチェーンと呼ばれる技術が開発され、暗号通貨等の金融分野やその他幅広い分野において注目されている（例えば、特許文献１、２）。
このブロックチェーンは公開鍵暗号技術を基盤としており、ブロックチェーン上で稼働する暗号通貨では、ブロックチェーン上の資産の所有者確認のために秘密鍵情報が利用されている。つまり、秘密鍵を保有している者がブロックチェーン上の資産の所有者となる仕組みとなっている。
【先行技術文献】

【特許文献】
【０００３】
【特許文献１】特許第５８５８５０６号公報
【特許文献２】特開２０１８－１１７２８７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、この秘密鍵が盗難等により本来の所有者以外に入手された場合、ブロックチェーン上に記録された資産が不正に操作されてしまうという問題が生じる。したがって、ブロックチェーンやブロックチェーンを利用したシステムにおいては、秘密鍵をいかに安全に保管するかということが非常に重要な課題となっている。一方、秘密鍵の管理を厳重にした場合、秘密鍵を利用する際の利便性（主に即時性）が失われる場合が多く、秘密鍵を安全に保管しつつ、利用時の利便性が損なわれない方法が必要とされている。さらに、暗号通貨には正当な秘密鍵保有者による二重払という不正リスクも存在しており、このような不正リスクを解決する方法も必要とされている。
【０００５】
最も利便性が高い方法はブロックチェーンネットワークを構成するサーバ（ノード）上に秘密鍵を保持する方法である。
この秘密鍵の保持方法は一般にホットウォレットと呼ばれており、秘密鍵と、その秘密鍵を利用するプログラムとが同一のサーバ上に存在するため、秘密鍵の利用要求から利用までの手順や物理的障害が少なく、利便性が損なわれないという利点を有する。なお、ここでいう利便性とは、例えば、暗号通貨の送金処理要求に対して、実際に送金処理が完了するまでに要する手順や時間の少なさを意味する。しかし、このホットウォレットは、ネットワーク上に存在するサーバに秘密鍵を保持するため、いわゆるハッキングによる盗難リスクが相対的に高い方法と言える。
【０００６】
一方、上記のホットウォレットと比べ、相対的に安全性が高い方法としてコールドウォレットと呼ばれる秘密鍵の保持方法が存在する。この方法は、例えば、秘密鍵情報を紙に印刷して物理的な金庫等で保管する等、秘密鍵を完全にネットワークから遮断する保持方法である。
この方法では、少なくともネットワークを経由した秘密鍵の盗難は完全に防ぐことができる。しかし、コールドウォレットの場合、秘密鍵情報を利用する際には、金庫の解錠、秘密鍵情報の再デジタル化、利用という手順を必要とするため、利便性が失われるという欠点がある。つまり、処理要求が発生してから、処理が完了するまでに一定の時間を要するため、処理の即時性が要求される利用状況には適さない方法と言える。
【０００７】
紙に秘密鍵を印刷して金庫に保管するという方法は、多くの利用状況において非現実的な管理手法であるため、例えば、暗号通貨取引事業者等のようにブロックチェーンが商用利用されている現場においては、ホットウォレットとコールドウォレットの中間的な手法が利用されている。
具体的には、外部ネットワークからはファイヤーウオールで遮断された内部ネットワーク上に設置されたＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）と呼ばれる電子鍵管理に特化した専用機器にて秘密鍵を保持する方法である。
この方法では、外部からのハッキングを防ぐと同時に、金庫から秘密鍵情報が印刷された紙を取り出し、再デジタル化する、といった人手を介することなく一定の安全性と利便性が確保されたバランスの取れた方法となっている。
【０００８】
しかし、ホットウォレットであれ、コールドウォレットであれ、それらの中間手法であれ、１つの場所や事業者により秘密鍵情報が集中管理されている場合、盗難が発生した際には、その管理下にある全ての利用者の秘密鍵情報が盗まれてしまうというリスクが存在

している。実際、多くの暗号通貨取引事業者において集中管理されている秘密鍵情報が盗まれ、利用者の暗号通貨資産が失われるという被害がしばしば発生している。

【０００９】

秘密鍵の集中管理によるリスクを低減するためには、分散管理、すなわち、秘密鍵の保有者が個別に秘密鍵を管理することが基本となる。

分散管理には大きく２つの方法が存在している。１つは、利用者が保有するパソコンやスマートフォンなどの情報端末にインストールされた一般に「ウォレットアプリ」と呼ばれる専用アプリケーションソフトで秘密鍵を管理する方法である。もう１つは秘密鍵管理専用に設計された一般に「ハードウエアウォレット」と呼ばれる専用ハードウエアを利用する方法である。

しかしながら、従来の分散管理の方法では、前者は日常的に使い慣れたスマートフォンアプリ等として利用できるため利便性が高い一方、ネットワークを経由した盗難やコンピューターウイルス感染による秘密鍵漏洩のリスクを否定できない。また、後者は、安全性は高いものの、日常的に利用する装置ではなく、操作に一定の知識を要するため、利便性が高いとは言えない。

【００１０】

さらに、ブロックチェーンを利用したシステムには、暗号通貨の二重払問題に代表されるような、正当な秘密鍵保有者による不正という課題も存在する。

これは、ブロックチェーンが分散システムであることから生じるデータ同期のタイムラグを利用した不正である。この不正の根源は、複数の箇所で暗号通貨を移動可能であること、つまり、複数の箇所で秘密鍵をコピーして利用できることに起因している。例えば、ある利用者が、１００単位の仮想通貨を保有しているとする。この利用者が、自分が管理しているアドレスに１００単位を送金後、直ちに店舗で買物をした場合、店舗が利用しているノードに利用者の送金履歴が反映されておらず、その利用者に１００単位の残高があると判断して商品を渡してしまうようなケースである。

【００１１】

そこで、本発明は、上記の課題を鑑みてなされたものであり、その目的は、利用時の利便性を損なうことなく、安全且つ簡便な方法で秘密鍵を保持及び利用することができ、さらに、正当な秘密鍵の保有者による不正をも防止することができる分散型ネットワークにおける秘密鍵管理システム及び秘密鍵管理方法を提供することにある。

【課題を解決するための手段】

【００１２】

前記課題は、本発明の分散型ネットワークにおける秘密鍵管理システムによれば、分散型ネットワークを構成するノードと通信可能に接続され、前記ノードとの間で処理情報を送受信する情報端末と、ネットワークから遮断され、専用リーダーを介して前記情報端末と接触型又は非接触型の通信手段により通信可能なＩＣチップを組み込んだ媒体と、から構成される秘密鍵管理システムであって、前記ＩＣチップは、前記分散型ネットワーク上の所有者情報に関連する情報であって前記処理情報に署名をするための秘密鍵情報と、該秘密鍵情報に対して外部からのアクセスの可否を判断するための第１解錠鍵情報とを記憶し、前記情報端末は、前記ＩＣチップ内に記憶された前記秘密鍵情報にアクセスするための第２解錠鍵情報を記憶し、前記秘密鍵管理システムは、前記第１解錠鍵情報と前記第２解錠鍵情報との整合性を検証する解錠鍵検証手段と、前記秘密鍵情報の利用可否を検証し、前記秘密鍵情報を利用可能と判断した場合に前記秘密鍵情報を利用して前記処理情報に署名する秘密鍵利用手段と、を備えること、により解決される。

【００１３】

また、本発明の分散型ネットワークにおける秘密鍵管理方法によれば、分散型ネットワークを構成するノードと通信可能に接続され、前記ノードとの間で処理情報を送受信する情報端末と、ネットワークから遮断され、専用リーダーを介して前記情報端末と接触型又は非接触型の通信手段により通信可能なＩＣチップを組み込んだ媒体と、を用いる秘密鍵管理方法であって、前記ＩＣチップは、前記分散型ネットワーク上の所有者情報に関連す

る情報であって前記処理情報に署名をするための秘密鍵情報と、該秘密鍵情報に対して外部からのアクセスの可否を判断するための第１解錠鍵情報とを記憶し、前記情報端末は、前記ＩＣチップ内に記憶された前記秘密鍵情報にアクセスするための第２解錠鍵情報を記憶し、前記情報端末又は前記ＩＣチップが、前記第１解錠鍵情報と前記第２解錠鍵情報との整合性を検証する解錠鍵検証工程と、前記秘密鍵情報の利用可否を検証し、前記秘密鍵情報を利用可能と判断した場合に前記秘密鍵情報を利用して前記処理情報に署名する秘密鍵利用工程と、を実行すること、により解決される。

【００１４】

以上のように構成された本発明の分散型ネットワークにおける秘密鍵管理システム及び秘密鍵管理方法では、分散型ネットワーク、すなわち、ブロックチェーン等の分散型台帳技術におけるネットワーク上の情報の所有者証明と直接結びつく秘密鍵情報を、ブロックチェーン等のネットワークから完全に遮断されたＩＣチップに記憶しておき、その秘密鍵情報を利用する際にのみ、ＩＣチップと情報端末とを専用のリーダーを介して通信可能とする。そして、その秘密鍵情報を利用してブロックチェーン（厳密にはブロックチェーンを構成するノード）との間で送受信される処理情報に署名を行う。また、ＩＣチップ内に記憶されている秘密鍵情報にアクセスするために、ＩＣチップと情報端末とは、互いに保持する解錠鍵情報により認証を行い、その解錠鍵情報の整合性が取れた場合にのみ、情報端末はＩＣチップ内の秘密鍵情報にアクセスできることとする。

これにより、安全性や利便性を犠牲にすること無く、利用者が操作習得に努力を必要としない簡便な方法で、ブロックチェーンで利用される秘密鍵を保持及び利用することができる。すなわち、秘密鍵情報の保存場所としてＩＣチップのメモリ領域を利用することにより、安全性の向上という観点からは、ネットワークから完全に遮断された環境で秘密鍵を安全に保持することができるうえ、利便性の向上という観点からは、秘密鍵の利用の際に、そのＩＣチップを読取装置である専用リーダーにかざすだけで簡単に秘密鍵を利用することができる。また、秘密鍵の利用時には、ＩＣチップと情報端末側とで相互に認証を行う事により、許可の無い第三者による秘密鍵の利用を防止することができる。

なお、本発明は、ＩＣチップにおいて、ブロックチェーン上の情報の所有者証明と直接結びつく秘密鍵情報を保持することを特徴とするため、電子マネーやクレジットカード等で既に行われているように、ＩＣチップに金融情報等、すなわち、残高そのものや利用者や利用企業の認証情報を保持するものとは、大きく異なるものである。

【００１５】

特に、上記の分散型ネットワークにおける秘密鍵管理システム及び秘密鍵管理方法について好適な構成を述べると、前記秘密鍵管理システムは、前記秘密鍵利用手段を前記情報端末側に備え、前記情報端末は、前記ＩＣチップに対して前記秘密鍵情報の送信を要求する秘密鍵要求手段と、前記ＩＣチップから送信された前記秘密鍵情報を取得する秘密鍵取得手段と、をさらに備える、とよい。

また、前記情報端末は、前記秘密鍵利用工程を実行すると共に、前記ＩＣチップに対して前記秘密鍵情報の送信を要求する秘密鍵要求工程と、前記ＩＣチップから送信された前記秘密鍵情報を取得する秘密鍵取得工程と、をさらに実行する、とよい。

【００１６】

このように、ＩＣチップ側から情報端末側に秘密鍵情報を送信し、情報端末側でその秘密鍵情報を利用して処理情報に署名することにより、ＩＣチップ側の処理負担を軽減しつつ、利用時の利便性を損なうことなく、安全且つ簡便な方法で秘密鍵を保持及び利用することができる。

【００１７】

また、特に、上記の分散型ネットワークにおける秘密鍵管理システム及び秘密鍵管理方法について好適な構成を述べると、前記秘密鍵管理システムは、前記秘密鍵利用手段を前記ＩＣチップ側に備え、前記ＩＣチップは、前記秘密鍵利用手段により前記処理情報に署名した署名済処理情報を前記情報端末に送信する署名済処理情報送信手段を、さらに備え、前記情報端末は、前記ＩＣチップに対して前記処理情報を送信する未署名処理情報送信

手段と、前記ＩＣチップから送信された前記署名済処理情報を取得して該署名済処理情報を検証する署名済処理情報検証手段と、をさらに備える、とよい。
また、前記ＩＣチップは、前記秘密鍵利用工程を実行すると共に、前記秘密鍵利用工程により前記処理情報に署名してその署名済処理情報を前記情報端末に送信する署名済処理情報送信工程をさらに実行し、前記情報端末は、前記ＩＣチップに対して前記処理情報を送信する未署名処理情報送信工程と、前記ＩＣチップから送信された前記署名済処理情報を取得して該署名済処理情報を検証する署名済処理情報検証工程と、をさらに実行する、とよい。
【００１８】
このように、情報端末側からＩＣチップ側に未署名の処理情報を送信し、ＩＣチップ側で秘密鍵情報を利用して処理情報に署名し、その署名済の処理情報を情報端末側に送信することにより、秘密鍵情報をＩＣチップ側から情報端末側に送信して展開する必要がなくなるので、より安全性が向上する。故に、利用時の利便性を損なうことなく、安全且つ簡便な方法で秘密鍵を保持及び利用することができる。
【００１９】
また、上記の分散型ネットワークにおける秘密鍵管理システムについて好適な構成を述べると、前記情報端末は、前記秘密鍵情報の利用履歴を記録する利用履歴記録手段をさらに備える、とよい。
【００２０】
このように、秘密鍵情報の利用履歴を記録することにより、同一の秘密鍵情報が複数回利用されることを防止することができるので、二重払処理が発生することを防止することができる。故に、利用時の利便性を損なうことなく、安全且つ簡便な方法で秘密鍵を保持及び利用することができるうえ、正当な秘密鍵の保有者による不正をも防止することができる。
【００２１】
また、上記の分散型ネットワークにおける秘密鍵管理システムについて好適な構成を述べると、前記秘密鍵情報は、前記秘密鍵利用手段により前記秘密鍵情報を利用して前記処理情報に署名した後に破棄される、とよい。
【００２２】
このように、秘密鍵情報は、利用した後速やかに再現不可能な状態で破棄することにより、同一の秘密鍵情報が複数回利用されることを防止することができるので、より安全性が向上するうえ、二重払処理が発生することを防止することができる。故に、利用時の利便性を損なうことなく、安全且つ簡便な方法で秘密鍵を保持及び利用することができるうえ、正当な秘密鍵の保有者による不正をも防止することができる。
【００２３】
また、上記の分散型ネットワークにおける秘密鍵管理システムについて好適な構成を述べると、前記秘密鍵情報は、他の媒体に複製不可とする、とよい。
【００２４】
このように、秘密鍵情報は、他のＩＣチップ等の媒体への複製を不可とすることにより、より安全性が向上するうえ、二重払処理が発生することを防止することができる。故に、利用時の利便性を損なうことなく、安全且つ簡便な方法で秘密鍵を保持及び利用することができるうえ、正当な秘密鍵の保有者による不正をも防止することができる。
【００２５】
また、上記の分散型ネットワークにおける秘密鍵管理システムについて好適な構成を述べると、前記媒体は、前記秘密鍵情報により生成される情報であって、前記分散型ネットワーク上の前記所有者情報を移転させるための情報を表示する、とよい。
【００２６】
このように、ＩＣチップを組み込んだＩＣカード等の媒体に、秘密鍵情報より生成したアドレス情報等を表示することにより、そのアドレスに容易にブロックチェーン上の情報の所有権を移転させることができ、安全性を確保したうえで、より利便性が向上する。故

に、利用時の利便性を損なうことなく、安全且つ簡便な方法で秘密鍵を保持及び利用することができる。

【００２７】

また、上記の分散型ネットワークにおける秘密鍵管理システムについて好適な構成を述べると、前記媒体は、非接触型ＩＣカードである、とよい。

【００２８】

このように、ＩＣチップを組み込む媒体として、広く普及している非接触型のＩＣカードを利用することにより、実施コストを抑えることができるうえ、利用者もそのＩＣカードを専用のＩＣリーダーにかざすだけという簡単な操作で済むので、安全性を確保したうえで、より利便性が向上する。故に、利用時の利便性を損なうことなく、安全且つ簡便な方法で秘密鍵を保持及び利用することができる。

【発明の効果】

【００２９】

本発明の分散型ネットワークにおける秘密鍵管理システム及び秘密鍵管理方法によれば、利用時の利便性を損なうことなく、安全且つ簡便な方法で秘密鍵を保持及び利用することができ、さらに、正当な秘密鍵の保有者による不正をも防止することができる。

【図面の簡単な説明】

【００３０】

【図１】秘密鍵管理システムの概要を示すイメージ図である。

【図２】秘密鍵管理システムの詳細構成を説明するための図である。

【図３】秘密鍵の一例を示す図である。

【図４】秘密鍵管理処理の一連の流れを示すフローチャートである。

【図５】他の実施形態における秘密鍵管理システムの詳細構成を説明するための図である。

【図６】他の実施形態における秘密鍵管理処理の一連の流れを示すフローチャートである。

【発明を実施するための形態】

【００３１】

以下、本発明の一実施形態（以下「本実施形態」という。）について説明する。

本実施形態は、分散型ネットワーク、すなわち、ブロックチェーン等の分散型台帳技術におけるネットワーク上の資産の所有者確認のために利用される秘密鍵情報について、利用時の利便性を損なうことなく、安全且つ簡便な方法で管理（保持及び利用）することができ、さらに、正当な保有者による不正をも防止することができる、分散型ネットワークにおける秘密鍵管理システム及び秘密鍵管理方法の発明に関するものである。

なお、以下、本明細書において、ＢＣと表記した場合はブロックチェーンの略称を示すものとする。また、ブロックチェーンに関する技術、及び、秘密鍵と共通鍵を用いた暗号技術については、従来から既知の技術を利用するので、ここでの詳細な説明は省略する。

【００３２】

＜秘密鍵管理システムの概要について＞

先ず、本発明にかかる秘密鍵管理システムＳの概要について説明する。

図１は、秘密鍵管理システムＳの概要を示すイメージ図である。図２は、秘密鍵管理システムＳの詳細構成を説明するための図である。図３は、秘密鍵の一例を示す図である。

【００３３】

図１及び図２に示すように、本実施形態の秘密鍵管理システムＳは、ブロックチェーン（厳密にはブロックチェーンを構成するノード）と通信可能に接続された情報端末１と、秘密鍵情報を保持するＩＣチップ２を組み込んだ媒体であるＩＣカード３と、ＩＣチップ２内の秘密鍵情報を読み取る専用リーダーであるＩＣリーダー４と、から主に構成されている。

【００３４】

情報端末１は、ブロックチェーン用の制御プログラムがインストールされており、ＩＣ

リーダー４を介してＩＣチップ２から読み取ったＢＣ秘密鍵３３を利用して、ブロックチェーンに対して各種処理要求を行う。

具体的には、図１に示すように、ＩＣチップ２から読み取ったＢＣ秘密鍵３３の検証を行い、そのＢＣ秘密鍵３３を利用して未署名のトランザクション（未署名の処理電文３４）に対して署名処理を行う。そして、その署名済トランザクション（署名済の処理電文３５）をブロックチェーンに送信し、ブロックチェーンにおいて各種取引が実行される。

【００３５】

ブロックチェーンで特定の情報を変更する処理を行う場合、ブロックチェーン上の資産の所有者情報に関連する情報であってその所有者証明と直接結びつくＢＣ秘密鍵３３を利用し、その情報の持ち主により署名された命令文が要求される。

本実施形態においては、ブロックチェーンで利用されるそのＢＣ秘密鍵３３を情報端末１側ではなく、ネットワークとは完全に遮断されたＩＣチップ２側の暗号化されたメモリ内に保持している。そして、情報端末１は、上記のようにブロックチェーンに対してＢＣ秘密鍵３３を必要とする処理を行う際に、ＩＣリーダー４を介してＩＣチップ２にＢＣ秘密鍵３３の利用を要求する。

なお、情報の保管場所としてのＩＣチップ２の安全性については既に公知であるように、ＩＣチップ２は、ＢＣ秘密鍵３３の保管場所としても十分に安全性が高く、最適であるといえる。

【００３６】

また、許可の無い第三者によるＢＣ秘密鍵３３の不正利用を防止するために、情報端末１とＩＣチップ２とは互いに共通鍵であるＩＣ解錠鍵３１，３２による認証を行う。具体的には、情報端末１は、ＢＣ秘密鍵３３を要求する際に自身が保有する認証用の鍵情報であって第２解錠鍵情報に該当するＩＣ解錠鍵３１を一緒に添付する。要求命令を受け取ったＩＣチップ２は、先ず、情報端末１から送信されてきたＩＣ解錠鍵３１を、ＩＣチップ２側で保有する認証用の鍵情報であって第１解錠鍵情報に該当するＩＣ解錠鍵３２と突き合わせを行い、両ＩＣ解錠鍵３１，３２が一致した場合にのみ交信が許可され、その後の処理を継続する。なお、ＩＣチップ２側も情報端末１側への返信情報に自身の保有するＩＣ解錠鍵３２を添付することにより、情報端末１側でも同様の認証を行うこととしてもよい。

【００３７】

さらに、許可の無い第三者によるＢＣ秘密鍵３３の不正利用を防止するために、ＩＣチップ２に保持されているＢＣ秘密鍵３３は、他のＩＣチップやその他の媒体等への複製を不可とする。

【００３８】

なお、図３に示すように、所定のアルゴリズムにより、ＢＣ秘密鍵３３より生成させた、ブロックチェーン上の資産の所有者の情報を示すアドレスが表示される。

【００３９】

＜秘密鍵管理システムの詳細構成について＞

次に、秘密鍵管理システムＳを構成する情報端末１及びＩＣチップ２それぞれの詳細構成について説明する。

【００４０】

（情報端末）

先ず、情報端末１について説明する。

情報端末１は、少なくとも、制御やデータの計算・加工を行う演算部としてのＣＰＵ、読み出し専用の記憶装置としてのＲＯＭ、メインメモリ（主記憶装置）としてのＲＡＭ、通信回線Ｎを通じて通信可能な外部の機器等とデータの送受信を行う通信用インタフェース、及び、補助記憶装置としてのハードディスクドライブ等を構成要素として有するコンピュータである。また、入力装置と出力装置の機能を兼ね備えた操作画面等５も有する。

【００４１】

また、情報端末１には、秘密鍵管理システムＳの一構成要素として、その機能を発揮さ

せるための制御プログラム（以下、秘密鍵管理プログラム）が予めインストールされている。この秘密鍵管理プログラムがＣＰＵに読み取られて実行されることにより、秘密鍵管理システムＳの一構成要素を担う装置としての機能が発揮される。

なお、情報端末１の機能は、ユーザによって享受されることになるが、当該機能のユーザへの提供方式としては、例えば、クラウドサービスやＡＳＰサービス等の方式であっても利用可能である。

【００４２】

情報端末１のハードウェア構成については上述の通りであるが、以下、情報端末１の構成を機能面から改めて説明する。

図２に示すように、情報端末１は、記憶部１１、ＢＣ秘密鍵要求生成部１２、ＢＣ秘密鍵要求送信部１３、ＢＣ秘密鍵取得部１４、ＢＣ秘密鍵検証部１５、ＢＣ秘密鍵利用部１６、ＢＣ秘密鍵利用履歴記録部１７、ＢＣ通信部１８と、を主な構成要素として有している。

これらの機能部は、情報端末１が実行する各種処理を担うものであり、情報端末１を構成する上述のハードウェア構成機器と上述の秘密鍵管理プログラムとが協働することによって構成されている。以下、上述した情報端末１の機能部の各々について説明する。

【００４３】

（記憶部）

記憶部１１は、ハードディスクドライブ、ＲＯＭ又はＲＡＭ等により構成されており、予め記憶されている秘密鍵管理プログラムや情報端末１の各種機能を制御するための他のプログラム、さらに、その他の各種データが記憶されている。また、第２解錠鍵情報に該当するＩＣ解錠鍵３１と、処理情報に該当する未署名の状態の処理電文３４が生成された際にはその処理電文３４が記憶される。

【００４４】

（ＢＣ秘密鍵要求生成部）

ＢＣ秘密鍵要求生成部１２は、秘密鍵要求手段として機能し、ユーザが操作する操作画面等５を要求起点として、処理電文３４に署名するためのＢＣ秘密鍵３３をＩＣチップ２に対して要求するための秘密鍵要求命令を生成する処理を行うものである。

【００４５】

（ＢＣ秘密鍵要求送信部）

ＢＣ秘密鍵要求送信部１３は、秘密鍵要求手段として機能し、ＢＣ秘密鍵要求生成部１２により生成された秘密鍵要求命令をＩＣチップ２に送信する処理を行うものである。このとき、秘密鍵要求命令には情報端末１が保持するＩＣ解錠鍵３１を添付して、秘密鍵要求命令と共に、ＩＣチップ２に送信する。なお、ＩＣチップ２との通信は、ＩＣリーダー４を中継して行う。

【００４６】

（ＢＣ秘密鍵取得部）

ＢＣ秘密鍵取得部１４は、秘密鍵取得手段として機能し、ＩＣチップ２から送信されたＢＣ秘密鍵３３をＩＣリーダー４を中継して受信する処理を行うものである。

【００４７】

（ＢＣ秘密鍵検証部）

ＢＣ秘密鍵検証部１５は、秘密鍵利用手段として機能し、ＢＣ秘密鍵取得部１４により受信したＢＣ秘密鍵３３を展開してその正当性等を検証し、ＢＣ秘密鍵３３の利用の可否を確認する処理を行うものである。

【００４８】

（ＢＣ秘密鍵利用部）

ＢＣ秘密鍵利用部１６は、秘密鍵利用手段として機能し、ＢＣ秘密鍵検証部１５により利用可能と判断されたＢＣ秘密鍵３３を利用して、処理電文３４に署名する処理を行うものである。また、ＢＣ秘密鍵３３の利用後、すなわち、処理電文３４への署名後は、速やかに再現不可能な状態でＢＣ秘密鍵３３を破棄する処理を行う。

【００４９】
（ＢＣ秘密鍵利用履歴記録部）
ＢＣ秘密鍵利用履歴記録部１７は、秘密鍵利用履歴記録手段として機能し、ＢＣ秘密鍵３３の全ての利用履歴をチェックする処理を行うものである。ここでの利用履歴には、ＢＣ秘密鍵３３を利用して処理電文３４へ署名したか否かのみならず、そのＢＣ秘密鍵３３を利用して署名した処理電文３５がブロックチェーンにより承認されているか否か、及び、その承認の回数等も含むものである。
【００５０】
（ＢＣ通信部）
ＢＣ通信部１８は、通信用インタフェースにより構成されており、インターネットや３Ｇ、４Ｇ、ＬＴＥ等のネットワークにより、情報端末１の外部、すなわち、ブロックチェーンと相互にデータのやりとりをするものである。なお、ここでのデータとは、ブロックチェーンに対する処理情報に該当する署名済みの処理電文３５等を含むものである。
【００５１】
（ＩＣチップ）
次に、ＩＣチップ２について説明する。
本実施形態のＩＣチップ２は、情報の記録や演算をするために、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ等の半導体メモリに集積回路を作り込んだものであって、複雑な演算処理をするためのＣＰＵ等は内蔵していないタイプのものである。
また、本実施形態では、非接触型で通信可能なＩＣチップ２を媒体としてのＩＣカード３に組み込んでいる。このように、非接触型のＩＣカード３を利用することにより、ＩＣチップ２を搭載したＩＣカード３をＩＣリーダー４にかざすだけで秘密鍵情報を利用した処理依頼をブロックチェーンに対して行うことができる。
【００５２】
また、ＩＣカード３の券面には、ＢＣ秘密鍵３３より生成したブロックチェーン上の資産の所有者の情報を示すアドレス情報を示す不図示の二次元コードが印刷されている。その二次元コードを読み込むことにより、ＩＣチップ２に紐付いたアドレスに容易にブロックチェーン上の情報の所有権を移転させることができる。
【００５３】
なお、本実施形態では、ＩＣチップ２を組み込んだ媒体として、内蔵されたアンテナを介して専用リーダーであるＩＣリーダー４と無線で交信する非接触型のＩＣカード３を利用することとしたが、カード表面に形成された外部装置接続端子と外部装置の接点を直接接触させて交信する接触型のＩＣカードであっても適用可能である。また、ＩＣチップ２を組み込む媒体は、カード形状に限らず、ＩＣタグや携帯情報端末等であってもよい。媒体が携帯情報端末等の場合は、上記の二次元コードは画面に表示することもできる。
【００５４】
以下、図２を参照して、ＩＣチップ２の構成を機能面から改めて説明する。
ＩＣチップ２は、記憶部２１、ＢＣ秘密鍵要求受信部２２、ＩＣ解錠鍵検証部２３、ＢＣ秘密鍵送信部２４と、を主な構成要素として有している。
【００５５】
（記憶部）
記憶部２１は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ等により構成されており、ブロックチェーン上の情報の所有者証明と直接結びつく情報であって処理電文３４に署名するための秘密鍵情報に該当するＢＣ秘密鍵３３と、そのＢＣ秘密鍵３３等の情報に対して外部からのアクセスの可否を判断するための第１解錠鍵情報に該当するＩＣ解錠鍵３２と、が記憶されている。
【００５６】
（ＢＣ秘密鍵要求受信部）
ＢＣ秘密鍵要求受信部２２は、情報端末１から送信された秘密鍵要求命令をＩＣリーダー４を中継して受信する処理を行うものである。

【００５７】
（ＩＣ解錠鍵検証部）
ＩＣ解錠鍵検証部２３は、解錠鍵検証手段として機能し、ＢＣ秘密鍵要求受信部２２により情報端末１から送信された秘密鍵要求命令を受信した際に、記憶部２１からＩＣ解錠鍵３２を取り出し、そのＩＣ解錠鍵３２と情報端末１から送信されたＩＣ解錠鍵３１との整合性を検証する処理を行うものである。そして、検証の結果、両ＩＣ解錠鍵３１，３２が一致した場合に、ＩＣチップ２内、厳密にはＩＣチップ２の記憶部２１へのアクセスを許可する処理を行う。
【００５８】
（ＢＣ秘密鍵送信部）
ＢＣ秘密鍵送信部２４は、情報端末１からの秘密鍵要求命令に基づいて、記憶部２１からＢＣ秘密鍵３３を取り出し、そのＢＣ秘密鍵３３を情報端末１に送信する処理を行うものである。なお、ＩＣチップ２との通信は、ＩＣリーダー４を中継して行う。
【００５９】
＜秘密鍵管理方法について＞
以下、本実施形態に係る秘密鍵管理方法の説明として、上記構成の秘密鍵管理システムＳにおける一連の動作の流れについて説明する。
なお、本実施形態に係る秘密鍵管理方法は、秘密鍵管理プログラムが稼働するコンピュータである情報端末１を含む秘密鍵管理システムＳ全体で行われる。換言すると、秘密鍵管理システムＳが実行する秘密鍵管理処理では、本実施形態に係る秘密鍵管理方法が適用されていることになる。
図４は、秘密鍵管理処理の一連の流れを示すフローチャートである。
【００６０】
先ず、情報端末１は、要求起点となる操作画面等５のユーザの操作に起因して、ＢＣ秘密鍵要求処理が発生し（Ｓ１０１）、情報端末１側に保持するＩＣ解錠鍵３１を添付して（Ｓ１０２）、ＢＣ秘密鍵要求命令を生成する（Ｓ１０３）。生成されたＢＣ秘密鍵要求命令は、ＩＣリーダー４の処理中継（Ｓ１０４）を経て、ＩＣリーダー４にかざされたＩＣチップ２側に受領される（Ｓ１０５）。
ＩＣチップ２は、ＩＣチップ２側に保持するＩＣ解錠鍵３２を取り出し（Ｓ１０６）、そのＩＣ解錠鍵３２と受領したＩＣ解錠鍵３１との整合性を検証する（Ｓ１０７）。検証の結果、一致していると判断した場合（Ｓ１０８：Ｙｅｓ）、記憶部２１からＢＣ秘密鍵３３を取り出して情報端末１に送信する（Ｓ１０９）。
情報端末１は、ＩＣリーダー４の処理中継（Ｓ１１０）を経て、そのＢＣ秘密鍵３３を受け取り（Ｓ１１１）、ＢＣ秘密鍵３３の利用可否を確認する（Ｓ１１２）。そして、未署名の処理電文３４を生成し（Ｓ１１３）、その処理電文３４に対してＢＣ秘密鍵３３を利用して署名処理を行う（Ｓ１１４）。また、ＢＣ秘密鍵３３の利用後は、速やかにそのＢＣ秘密鍵を破棄する（Ｓ１１５）。そして、その署名済の処理電文３５をブロックチェーンに送信する（Ｓ１１６、Ｓ１１７）。
ブロックチェーン側では、その署名済の処理電文３５を受け取り、検証した後（Ｓ１１８）、その処理電文３５に基づき各種処理を実行する（Ｓ１１９）。
情報端末１は、ブロックチェーンで実行された処理結果を受領し（Ｓ１２０）、秘密鍵管理処理を終了する。なお、ＩＣ解錠鍵３１，３２が一致していないと判断した場合は（Ｓ１０８：Ｎｏ）、そのまま秘密鍵管理処理を終了する。
【００６１】
＜他の実施形態における秘密鍵管理システムの概要について＞
上記の実施形態（第１実施形態）では、ＩＣチップ２側の処理負担を軽減することに重点を置き、ＢＣ秘密鍵３３を保持するＩＣチップ２を比較的簡易な構成として、単なるメモリ媒体として利用する場合の例について説明した。
以下、他の実施形態（第２実施形態）として、ＩＣチップ１０２上でＣＰＵ等の計算機能が利用可能な場合について説明する。なお、以下の説明において、第１実施形態と同一

部材・同一機能部については、符号を１００番台として援用する。
【００６２】
第２実施形態においては、情報端末１０１は、ＩＣリーダー１０４を介してＩＣチップ１０２に対してＢＣ秘密鍵１３３そのものの送信を要求せずに、ＩＣチップ１０２側に対してＩＣチップ１０２上に実装されたＢＣ秘密鍵１３３を利用する処理を要求する点において、第１実施形態と相違する。
具体的には、情報端末１０１は、ＩＣチップ１０２に対して未署名の状態の処理電文１３４を送信し、ＢＣ秘密鍵１３３を情報端末１０１側で受信せずにＩＣチップ１０２側でそのままＢＣ秘密鍵１３３を利用して処理電文１３４に署名した後、その署名済の処理電文１３５を受け取ることになる。
【００６３】
＜他の実施形態における秘密鍵管理システムの詳細構成について＞
次に、第２実施形態における秘密鍵管理システムＳを構成する情報端末１０１及びＩＣチップ１０２それぞれの詳細構成について、第１実施形態との相違点を中心に説明する。
図５は、他の実施形態（第２実施形態）における秘密鍵管理システムＳの詳細構成を説明するための図である。
【００６４】
（情報端末）
先ず、情報端末１０１について説明する。
情報端末１０１のハードウェア構成については第１実施形態と同様であるが、情報端末１０１の機能面について、相違点を有する。
すなわち、図５に示すように、情報端末１０１は、記憶部１１１、ＢＣ秘密鍵要求生成部１１２、ＢＣ秘密鍵要求送信部１１３、未署名処理電文送信部１１４、署名済処理電文取得部１１５、署名済処理電文検証部１１６、ＢＣ秘密鍵利用履歴記録部１１７、ＢＣ通信部１１８と、を主な構成要素として有している。
【００６５】
（ＢＣ秘密鍵要求生成部）
ＢＣ秘密鍵要求生成部１１２は、秘密鍵要求手段として機能し、ユーザが操作する操作画面等５を要求起点として、処理電文１３４に署名するためにＢＣ秘密鍵１３３を利用することをＩＣチップ１０２に対して要求するための秘密鍵要求命令を生成する処理を行うものである。
【００６６】
（未署名処理電文送信部）
未署名処理電文送信部１１４は、未署名処理電文送信手段として機能し、生成された未署名の処理電文１３４をＩＣチップ１０２に送信する処理を行うものである。このとき、未署名の処理電文１３４は、ＢＣ秘密鍵要求送信部１１３により送信される、秘密鍵要求命令とＩＣ解錠鍵１３１と共に、ＩＣチップ１０２に送信する。なお、ＩＣチップ１０２との通信は、ＩＣリーダー１０４を中継して行う。
【００６７】
（署名済処理電文取得部）
署名済処理電文取得部１１５は、署名済処理電文検証手段として機能し、ＩＣチップ１０２から送信された署名済の処理電文１３５を、ＩＣリーダー１０４を中継して受信する処理を行うものである。
【００６８】
（署名済処理電文検証部）
署名済処理電文検証部１１６は、署名済処理電文検証手段として機能し、署名済処理電文取得部１１５により取得した署名済の処理電文を検証する処理を行うものである。
【００６９】
なお、その他の機能部、すなわち、記憶部１１１、ＢＣ秘密鍵要求送信部１１３、ＢＣ秘密鍵利用履歴記録部１１７、ＢＣ通信部１１８の各機能については、上述の第１実施形

態と同様であるので、ここでの説明は省略する。
【００７０】
（ＩＣチップ）
次に、ＩＣチップ１０２について説明する。
第２実施形態にかかるＩＣチップ１０２は、ＣＰＵやコプロセッサ等を内蔵することにより演算処理機能を持たせ、ＩＣチップ１０２内で複雑な情報処理が可能になる点において、第１実施形態と相違する。
その他、非接触型、接触型を問わない点、媒体がカード形状に限定されない点等は、第１実施形態と同様である。
【００７１】
以下、図５を参照して、ＩＣチップ１０２の構成を機能面から説明する。
ＩＣチップ１０２は、記憶部１２１、ＢＣ秘密鍵要求受信部１２２、ＩＣ解錠鍵検証部１２３、ＢＣ秘密鍵利用部１２４、署名済処理電文送信部１２５と、を主な構成要素として有している。
【００７２】
（ＢＣ秘密鍵要求受信部）
ＢＣ秘密鍵要求受信部１２２は、情報端末１０１から送信された秘密鍵要求命令と未署名の処理電文１３４とをＩＣリーダー１０４を中継して受信する処理を行うものである。なお、第２実施形態における秘密鍵要求命令とは、ＢＣ秘密鍵１３３の送信を要求することではなく、ＢＣ秘密鍵１３３の利用を要求することを意味する。
【００７３】
（ＢＣ秘密鍵利用部）
ＢＣ秘密鍵利用部１２４は、秘密鍵利用手段として機能し、記憶部１２１から取り出したＢＣ秘密鍵１３３を利用して、情報端末１０１から受信した処理電文１３４に署名する処理を行うものである。
【００７４】
（署名済処理電文送信部）
署名済処理電文送信部１２５は、署名済処理電文送信手段として機能し、ＢＣ秘密鍵利用部２４により署名した署名済の処理電文１３５を情報端末１０１に送信する処理を行うものである。なお、ＩＣチップ１０２との通信は、ＩＣリーダー１０４を中継して行う。
【００７５】
なお、記憶部１２１、ＩＣ解錠鍵検証部１２３については、上述の第１実施形態と同様であるので、ここでの説明は省略する。
【００７６】
＜他の実施形態における秘密鍵管理方法について＞
以下、第２実施形態に係る秘密鍵管理方法の説明として、上記構成の秘密鍵管理システムＳにおける一連の動作の流れについて説明する。
図６は、他の実施形態（第２実施形態）における秘密鍵管理処理の一連の流れを示すフローチャートである。
【００７７】
先ず、情報端末１０１は、要求起点となる操作画面等１０５のユーザの操作に起因して、ＢＣ秘密鍵要求処理が発生し（Ｓ２０１）、情報端末１０１側に保持するＩＣ解錠鍵１３１と未署名の処理電文１３４を添付して（Ｓ２０２、Ｓ２０３）、ＢＣ秘密鍵要求命令を生成する（Ｓ２０４）。生成されたＢＣ秘密鍵要求命令は、ＩＣリーダー１０４の処理中継（Ｓ２０５）を経て、ＩＣリーダー１０４にかざされたＩＣチップ１０２側に受領される（Ｓ２０６）。
ＩＣチップ１０２は、ＩＣチップ１０２側に保持するＩＣ解錠鍵１３２を取り出し（Ｓ２０７）、そのＩＣ解錠鍵１３２と受領したＩＣ解錠鍵１３１との整合性を検証する（Ｓ２０８）。検証の結果、一致していると判断した場合（Ｓ２０９：Ｙｅｓ）、記憶部１２１からＢＣ秘密鍵１３３を取り出し（Ｓ２１０）、未署名の処理電文１３４に対して、Ｂ

Ｃ秘密鍵１３３を利用して署名処理を行い（Ｓ２１１）、その署名済の処理電文１３５を情報端末１０１に送信する（Ｓ２１２）。
情報端末１０１は、ＩＣリーダー１０４の処理中継（Ｓ２１３）を経て、その署名済の処理電文１３５を受け取り（Ｓ２１４）、その署名済の処理電文１３５の内容を検証する（Ｓ２１５）。そして、その署名済の処理電文１３５をブロックチェーンに送信する（Ｓ２１６、Ｓ２１７）。
ブロックチェーン側では、その署名済の処理電文１３５を受け取り、検証した後（Ｓ２１８）、その処理電文１３５に基づき各種処理を実行する（Ｓ２１９）。
情報端末１は、ブロックチェーンで実行された処理結果を受領し（Ｓ２２０）、秘密鍵管理処理を終了する。なお、ＩＣ解錠鍵１３１，１３２が一致していないと判断した場合は（Ｓ２０９：Ｎｏ）、そのまま秘密鍵管理処理を終了する。

【００７８】

＜まとめ＞

以上説明してきたように、ブロックチェーンで特定の情報を変更する処理を行う場合、その情報の持ち主により署名された命令文（処理電文）が要求されることとなるが、その署名の際に利用される秘密鍵の利用要求は、保存先のＩＣチップの状態に応じて、２つの方法を利用することができる。すなわち、秘密鍵自体を要求する方法と、秘密鍵自体は要求せず、秘密鍵を利用した電子署名等の処理をＩＣチップに要求する方法であり、どちらの場合でも、署名済の命令文がブロックチェーンに送信されることになる。

【００７９】

１つ目の方法（第１実施形態）は、ブロックチェーンに通信可能に接続された情報端末が、ＩＣチップから秘密鍵を受け取り、情報端末側にて命令文に署名を行うものであり、ＩＣチップを安全なメモリ媒体として利用する場合に採用する。
この方法では、ＩＣチップ内に保持された秘密鍵を、ＩＣリーダーを介して情報端末が取得し利用する。なお、この際、情報端末のメモリ上に秘密鍵が展開されることになるが、難読化技術や情報端末自体に搭載されたメモリ空間分離機能等を利用して秘密鍵の漏洩リスクの低減をはかる。また、秘密鍵の利用後、その秘密鍵は速やかに再現不可能な状態で破棄される。

【００８０】

２つ目の方法（第２実施形態）は、ブロックチェーンに通信可能に接続された情報端末が、ＩＣチップに未署名の命令文を送り、ＩＣチップで秘密鍵を利用して署名された署名済の命令文を受け取るものであり、ＩＣチップ上でＣＰＵ等の演算処理機能が利用可能な場合に採用する。
この方法では、情報端末は、ＩＣリーダーを介してＩＣチップに対して秘密鍵そのものではなく、ＩＣチップ上に実装された秘密鍵を利用する処理を要求する。具体的には、ＩＣチップに対して未署名の処理電文を送付し、ＩＣチップ内の秘密鍵で電子署名をした署名済の処理電文を受け取る。この方法では、ブロックチェーンに通信可能に接続された情報端末のメモリ上に秘密鍵が展開されることが無いため、１つ目の方法と比較すると、より安全性を重視した方法となる。

【００８１】

また、ブロックチェーンに命令文を送信する際、情報端末はどの秘密鍵（若しくは秘密鍵に紐づくアドレス等であってもよい。）が利用されたかについて、全て把握可能な状態となる。特に、秘密鍵はコピーされることはないため、情報端末が把握した利用履歴が、その秘密鍵の全ての利用履歴となる。
さらに、情報端末によって、最新（前回）のその秘密鍵を利用した処理がブロックチェーンにより承認されているか否かや、その承認の回数等をチェックすることにより、前回の処理が既に他のノードにも同期されているか否かを確認することができるので、未承認の処理や承認回数の少ない場合には次の処理要求をブロックすることにより、二重払処理が発生することを防止することができる。

【００８２】

また、ＩＣチップやＩＣチップを搭載した媒体を紛失したり、盗まれたりすることにより、秘密鍵に紐付いたブロックチェーン上の情報が本来の所有者以外の者に利用されるリスクがあるが、本機能は二重払チェックだけでなく、利用停止等の登録をすることで、紛失や盗難の報告を受け、特定の秘密鍵の利用を停止することもできる。

【００８３】

暗号通貨の秘密鍵保存場所として非接触ＩＣチップのメモリ領域を利用することにより、安全性の向上という観点からは、ネットワークから完全に遮断された環境で秘密鍵を安全に保持することができるうえ、利便性の向上という観点からは、秘密鍵の利用の際に、そのＩＣチップを読取装置である専用リーダーにかざすだけで簡単に秘密鍵を利用することができる。

また、秘密鍵の利用時には、ＩＣチップと情報端末側とで相互に認証を行う事により、許可の無い第三者による秘密鍵の利用を防止することができる。

さらに、ＩＣチップ以外への秘密鍵のコピーを防止することにより、正当な情報端末以外での支払処理発生を防ぐことが可能となり、暗号通貨利用で課題となっている二重払という不正を防止することもできる。

【００８４】

以上説明したように、本発明によれば、ブロックチェーン等の分散型台帳技術におけるネットワーク上の資産の所有者情報に関連する情報であってその所有者証明と直接結びつく秘密鍵を、所有者自身が安全且つ利便性を損なうことなく管理（保持及び利用）することができるので、取引の安全性及び利便性を向上させることができる。

また、正当な秘密鍵保有者による不正（故意・不故意によらず）も防止することができる。

さらに、例えば、日本において日常的に利用される非接触ＩＣカードや、非接触ＩＣチップ搭載のスマートフォン内に秘密鍵を保持することにより、従来の同技術を利用した電子マネーと同様に誰もが安全且つ簡単に暗号通貨による支払等を行うことができるようになったり、ブロックチェーンを利用したシステムにおいて本人認証等を行ったりできるようになる。

【００８５】

上記の実施形態（第１実施形態及び第２実施形態）では、主として、分散型ネットワークの一例として代表的な分散型台帳技術であるブロックチェーンを挙げて説明した。

ただし、上記の実施形態は、本発明の理解を容易にするための一例に過ぎず、本発明を限定するものではない。すなわち、本発明は、その趣旨を逸脱することなく、変更、改良され得ると共に、本発明にはその等価物が含まれることは勿論である。

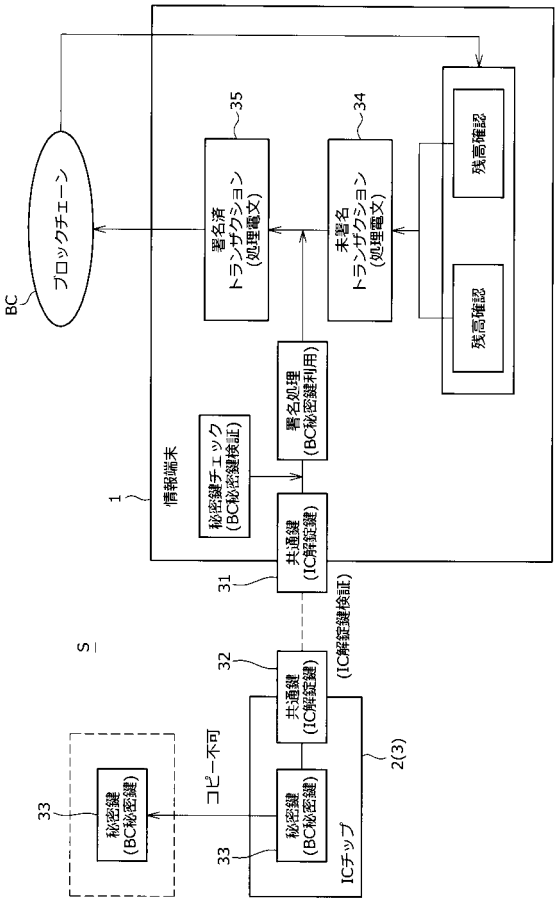
【符号の説明】

【００８６】

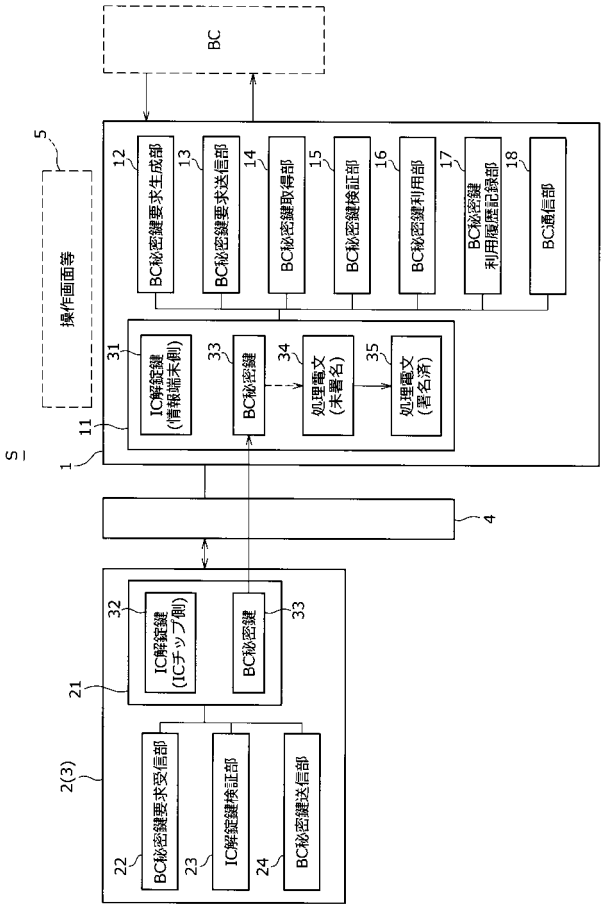
１　情報端末
２　ＩＣチップ
３　ＩＣカード
４　ＩＣリーダー
５　操作画面等
１１　記憶部
１２　ＢＣ秘密鍵要求生成部
１３　ＢＣ秘密鍵要求送信部
１４　ＢＣ秘密鍵取得部
１５　ＢＣ秘密鍵検証部
１６　ＢＣ秘密鍵利用部
１７　ＢＣ秘密鍵利用履歴記録部
１８　ＢＣ通信部
２１　記憶部
２２　ＢＣ秘密鍵要求受信部

２３　　ＩＣ解錠鍵検証部
２４　　ＢＣ秘密鍵送信部
３１　　ＩＣ解錠鍵
３２　　ＩＣ解錠鍵
３３　　ＢＣ秘密鍵
３４　　処理電文（未署名）
３５　　処理電文（署名済）
１１４　未署名処理電文送信部
１１５　署名済処理電文取得部
１１６　署名済処理電文検証部
１２４　ＢＣ秘密鍵利用部
１２５　署名済処理電文送信部
Ｓ　　秘密鍵管理システム
ＢＣ　　ブロックチェーン

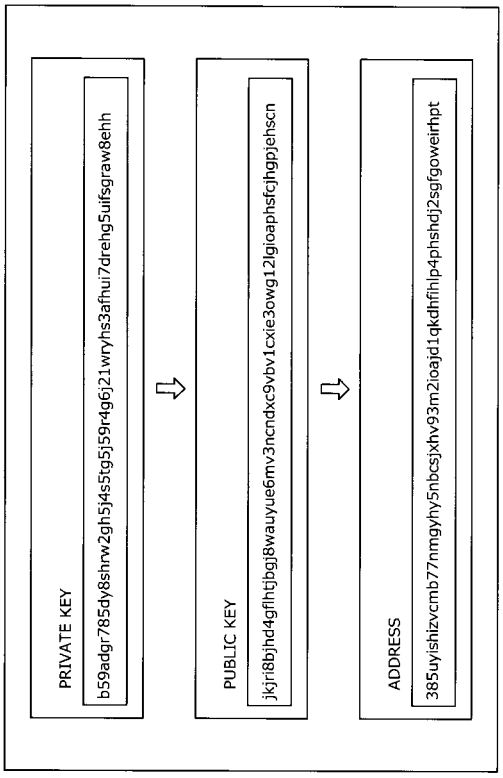
【図１】



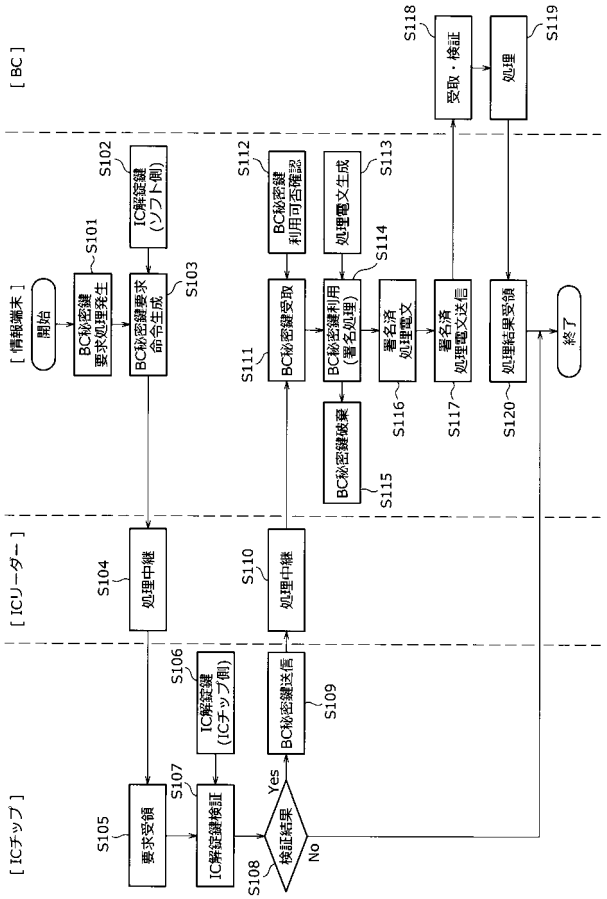
【図２】



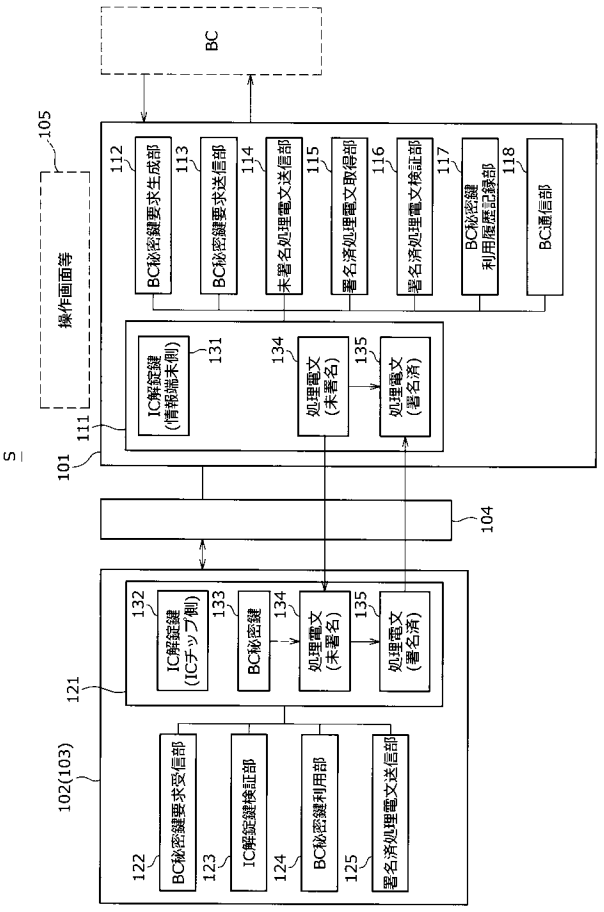
【図３】


PRIVATE KEY
b59adgr785dy8shrw2gh5j4s5tg5j59r4g6j21wryhs3afhui7dreng5uifsgraw8ehh
PUBLIC KEY
jkjri8bjhd4gflhtjbgj8wauyue6mv3ncndxc9vbv1cxie3owg12lgioaphsfcjhgpjehscn
ADDRESS
385uyishizvcmb77nmgyhy5nbcsjxhv93m2ioajd1qkdhfihlp4phshdj2sgfgoweirhpt

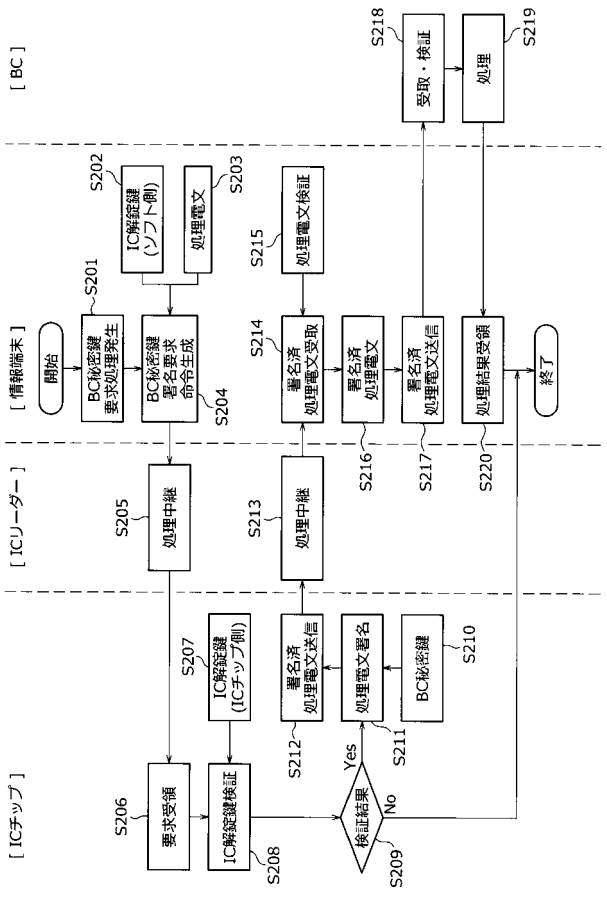
【図４】


[情報端末]
[ICリーダー]
[ICチップ]
[BC]
開始
BC秘密鍵要求処理発生
IC解錠鍵(ソフト側)
BC秘密鍵要求命令生成
処理中継
要求受領
IC解錠鍵(ICチップ側)
IC解錠鍵検証
検証結果
Yes
No
BC秘密鍵送信
処理中継
BC秘密鍵受取
BC秘密鍵利用可否確認
処理電文生成
BC秘密鍵利用(署名処理)
BC秘密鍵破棄
署名済処理電文
署名済処理電文送信
処理結果受領
受取・検証
処理
終了
S101
S102
S103
S104
S105
S106
S107
S108
S109
S110
S111
S112
S113
S114
S115
S116
S117
S118
S119
S120

【図５】


S
BC
操作画面等
105
101
111
IC解錠鍵(情報端末側)
131
112
BC秘密鍵要求生成部
113
BC秘密鍵要求送信部
114
未署名処理電文送信部
115
署名済処理電文取得部
116
署名済処理電文検証部
117
BC秘密鍵利用履歴記録部
118
BC通信部
134
処理電文(未署名)
135
処理電文(署名済)
104
121
102(103)
132
IC解錠鍵(ICチップ側)
133
BC秘密鍵
122
BC秘密鍵要求受信部
123
IC解錠鍵検証部
124
BC秘密鍵利用部
125
署名済処理電文送信部

【図６】


[情報端末]
[ICリーダー]
[ICチップ]
[BC]
開始
BC秘密鍵要求処理発生
IC解錠鍵(ソフト側)
処理電文
BC秘密鍵署名要求命令生成
処理中継
要求受領
IC解錠鍵(ICチップ側)
IC解錠鍵検証
検証結果
Yes
No
署名済処理電文送信
処理電文署名
BC秘密鍵
処理中継
署名済処理電文受取
署名済処理電文
署名済処理電文送信
処理結果受領
処理電文検証
受取・検証
処理
終了
S201
S202
S203
S204
S205
S206
S207
S208
S209
S210
S211
S212
S213
S214
S215
S216
S217
S218
S219
S220