(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2020-48161
(P2020-48161A)
(43)公開日　令和2年3月26日(2020.3.26)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
G09C	1/00	(2006.01)	H04L	9/00	675Z	
			G09C	1/00	640D	

審査請求 有　請求項の数 8　ＯＬ　（全 25 頁）

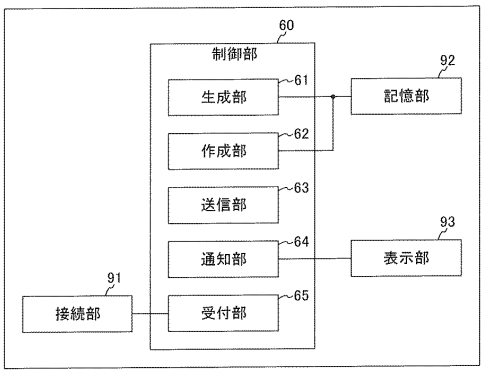
(21)出願番号　特願2018-177386 (P2018-177386)
(22)出願日　平成30年9月21日 (2018.9.21)

(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)　5J104 AA09　AA12　LA03　LA06　NA12
PA07　PA10

(54)【発明の名称】取引装置、取引方法及び取引プログラム

(57)【要約】
【課題】ハードウェアウォレットを用いたアトミックスワップにおいて、ユーザの作業を簡略にする技術を提供する。
【解決手段】取引装置は、生成部と、記憶部と、作成部と、送信部とを備える。生成部は、秘密情報を用いて算出された特定情報を含む第１取引情報が第１ネットワークに公開されたあと、特定情報を含む第２取引情報に含ませる第１電子署名を生成する。また、生成部は、第１取引情報に含まれる情報を用いて、第４取引情報に含ませる第２電子署名を生成する。記憶部は、第２電子署名を記憶する。作成部は、特定情報と第１電子署名とを含む第２取引情報を作成する。また、作成部は、秘密情報を含む第３取引情報が第２ネットワークに公開されたあと、記憶部に記憶されている第２電子署名を用いて、秘密情報と第２電子署名とを含む第４取引情報を作成する。送信部は、取引情報を送信する。
【選択図】図６



【特許請求の範囲】
【請求項１】
取引相手からユーザに第１データを引き渡しする取引に用いる第１取引情報であって、秘密情報を用いて算出された特定情報を含む前記第１取引情報が第１ネットワークに公開されたあと、前記ユーザから前記取引相手に第２データを引き渡しする取引に用いる第２取引情報であって、前記特定情報を含む前記第２取引情報に含ませる第１電子署名の生成と、前記第１取引情報に含まれる情報を用いて、前記ユーザが前記取引相手から前記第１データを受け取る取引に用いる第４取引情報に含ませる前記第２電子署名の生成と、をする生成部と、
前記第２電子署名を記憶する記憶部と、
前記特定情報と前記第１電子署名とを含む前記第２取引情報の作成と、前記取引相手が前記ユーザから第２データを受け取る取引に用いる第３取引情報であって、前記秘密情報を含む前記第３取引情報が第２ネットワークに公開されたあと、前記記憶部に記憶されている前記第２電子署名を用いて、前記秘密情報と前記第２電子署名とを含む前記第４取引情報の作成と、をする作成部と、
前記第１ネットワークに前記第４取引情報を送信する処理と、前記第２ネットワークに前記第２取引情報を送信する処理と、をする送信部と、
を備えることを特徴とする取引装置。
【請求項２】
前記作成部は、
前記第２電子署名を含む前記第４取引情報を作成して前記記憶部に記憶させ、前記秘密情報を含む前記第３取引情報が第２ネットワークに公開されたあと、前記記憶部に記憶されている前記第２電子署名を含む前記第４取引情報を用いて、前記秘密情報と前記第２電子署名とを含む前記第４取引情報を作成する
ことを特徴とする請求項１に記載の取引装置。
【請求項３】
前記取引装置は、さらに、
前記第１取引情報が前記第１ネットワークに公開されたあと、前記第１取引情報が公開されたことを通知する通知部
を備えることを特徴とする請求項１または２に記載の取引装置。
【請求項４】
前記取引装置は、さらに、
前記第１電子署名と前記第２電子署名とを生成するときに用いられる秘密鍵を格納する記憶装置と着脱可能に接続される接続部と、
前記記憶装置が前記接続部に接続されたとき、前記秘密鍵の入力を受け付ける受付部と、
を備えることを特徴とする請求項１から３のいずれか一つに記載の取引装置。
【請求項５】
前記記憶部は、さらに、
前記第１電子署名を記憶し、
前記作成部は、
前記第１取引情報が前記第１ネットワークに公開されたあと、前記記憶部に記憶されている前記第１電子署名を用いて、前記特定情報と前記第１電子署名とを含む前記第２取引情報を作成する
ことを特徴とする請求項１から４のいずれか一つに記載の取引装置。
【請求項６】
前記記憶部は、さらに、
前記第２取引情報を記憶し、
前記送信部は、
前記第１ネットワーク内で発生した取引を記録するブロックチェーンに前記第１取引情

報が記録されたあと、前記記憶部に記憶されている前記第２取引情報を前記第２ネットワークに送信する
ことを特徴とする請求項１から５のいずれか一つに記載の取引装置。
【請求項７】
コンピュータによって実行される取引方法であって、
取引相手からユーザに第１データを引き渡しする取引に用いる第１取引情報であって、秘密情報を用いて算出された特定情報を含む前記第１取引情報が第１ネットワークに公開されたあと、前記ユーザから前記取引相手に第２データを引き渡しする取引に用いる第２取引情報であって、前記特定情報を含む前記第２取引情報に含ませる第１電子署名の生成と、前記第１取引情報に含まれる情報を用いて、前記ユーザが前記取引相手から前記第１データを受け取る取引に用いる第４取引情報に含ませる前記第２電子署名の生成と、をし、
前記第２電子署名を記憶し、
前記特定情報と前記第１電子署名とを含む前記第２取引情報の作成と、前記取引相手が前記ユーザから第２データを受け取る取引に用いる第３取引情報であって、前記秘密情報を含む前記第３取引情報が第２ネットワークに公開されたあと、前記記憶部に記憶されている前記第２電子署名を用いて、前記秘密情報と前記第２電子署名とを含む前記第４取引情報の作成と、をし、
前記第１ネットワークに前記第４取引情報を送信する処理と、前記第２ネットワークに前記第２取引情報を送信する処理と、をする
ことを特徴とする取引方法。
【請求項８】
取引相手からユーザに第１データを引き渡しする取引に用いる第１取引情報であって、秘密情報を用いて算出された特定情報を含む前記第１取引情報が第１ネットワークに公開されたあと、前記ユーザから前記取引相手に第２データを引き渡しする取引に用いる第２取引情報であって、前記特定情報を含む前記第２取引情報に含ませる第１電子署名の生成と、前記第１取引情報に含まれる情報を用いて、前記ユーザが前記取引相手から前記第１データを受け取る取引に用いる第４取引情報に含ませる前記第２電子署名の生成と、をし、
前記第２電子署名を記憶し、
前記特定情報と前記第１電子署名とを含む前記第２取引情報の作成と、前記取引相手が前記ユーザから第２データを受け取る取引に用いる第３取引情報であって、前記秘密情報を含む前記第３取引情報が第２ネットワークに公開されたあと、前記記憶部に記憶されている前記第２電子署名を用いて、前記秘密情報と前記第２電子署名とを含む前記第４取引情報の作成と、をし、
前記第１ネットワークに前記第４取引情報を送信する処理と、前記第２ネットワークに前記第２取引情報を送信する処理と、をする
処理をコンピュータに実行させることを特徴とする取引プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、取引装置、取引方法及び取引プログラムに関する。
【背景技術】
【０００２】
ブロックチェーン上に取引情報を記録する暗号通貨（仮想通貨）が用いられている。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のことである。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。

【０００３】
暗号通貨には、異なる特徴を有する複数の種類の暗号通貨がある。このため、ユーザは、暗号通貨を使用するとき、用途に適した暗号通貨を選択して利用する。暗号通貨の種類には、例えば、ビットコイン（ＢＴＣ：登録商標）、イーサリアム（ＥＴＨ：商標登録）、ライトコイン（ＬＴＣ）、及びモナコイン（ＭＯＮＡ：登録商標）などがある。暗号通貨の用途には、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。
【０００４】
上記のように、複数の種類の暗号通貨を用途に応じて使い分けるため、異なる暗号通貨を交換する取引が行われている。異なる暗号通貨を交換する取引には、ユーザと取引相手のユーザとの間の直接の取引である直接取引と、ユーザと取引相手のユーザとの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。以下の説明では、取引相手のユーザのことを単に取引相手ともいう。
【０００５】
暗号通貨の直接取引について説明する。
例えば、ユーザは、自身が所有するビットコインと、取引相手が所有するライトコインとの交換取引を行うとき、ビットコインを取引相手に送金する。そして、取引相手は、ビットコインがユーザから届いたことを確認すると、ユーザにライトコインを送金する。
【０００６】
直接取引において、取引相手は、ユーザからビットコインが届いたことを確認したあと、ユーザ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、ユーザは、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。
【０００７】
暗号通貨の仲介取引について説明する。
例えば、ユーザは、自身が所有するビットコインを取引所に預ける。また、取引相手は、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、ユーザに取引相手が預けたライトコインを送金し、取引相手にユーザが預けたビットコインを送金する。
【０００８】
仲介取引において、ユーザと取引相手とは取引所に暗号通貨を預けているので、取引所の不正及び取引所のハッキングなどにより、暗号通貨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、ユーザは、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。
【０００９】
上記の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通貨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（Ａｔｏｍｉｃ　Ｓｗａｐ）という取引手法が用いられている。
【００１０】
関連する技術として、トランザクションに記された取引内容の信頼性を確保しつつ、１つのトランザクションで複合的な取引形態を扱うことを可能にする技術がある。関連する技術において、資産の移動元（保持元）ａ、ｂは、自己の管理するアドレスの秘密鍵による署名「ａ」、「ｂ」を付することを条件に、複合的な取引に関する取引情報を一つのトランザクション（複合トランザクション）に記すことを許容する。そして、複合トランザクションをデータベースに記録する場合、なりすまし（取引主体となる当事者を含む）を防止すべく、資産の移動元の全署名「ａ」、「ｂ」が正当であることを記録の条件の一つとする（例えば、特許文献１及び非特許文献１参照）。
【先行技術文献】
【特許文献】
【００１１】

【特許文献１】国際公開第２０１７／１７０９１２号
【非特許文献】
【００１２】
【非特許文献１】ｂｉｔｃｏｉｎ　ｗｉｋｉ、［２０１８年3月1日検索］、ネットワーク、＜ＵＲＬ：ｈｔｔｐｓ：／／ｅｎ．ｂｉｔｃｏｉｎ．ｉｔ／ｗｉｋｉ／Ａｔｏｍｉｃ＿ｃｒｏｓｓ－ｃｈａｉｎ＿ｔｒａｄｉｎｇ＞
【発明の概要】
【発明が解決しようとする課題】
【００１３】
アトミックスワップでは、ブロッチェーンの承認時間以上の間隔を空けて、各ユーザはブロックチェーンのネットワークに２回ずつ取引情報を送信する。ハードウェアウォレットを用いる場合、秘密鍵の盗難を防止するために、ユーザは電子署名の生成処理以外のときに取引装置からハードウェアウォレットを取り外すことにより、ハードウェアウォレットをオフライン状態にする。このように、ハードウェアウォレットを用いたアトミックスワップでは、ハードウェアウォレットを取引装置に抜き差しするため、ユーザの作業が煩雑になる。
本発明は、一側面として、ハードウェアウォレットを用いたアトミックスワップにおいて、ユーザの作業を簡略にする技術を提供する。
【課題を解決するための手段】
【００１４】
本明細書で開示する取引装置のひとつに、生成部と、記憶部と、作成部と、送信部とを備える取引装置がある。生成部は、秘密情報を用いて算出された特定情報を含む第１取引情報が第１ネットワークに公開されたあと、特定情報を含む第２取引情報に含ませる第１電子署名の生成をする。また、生成部は、第１取引情報に含まれる情報を用いて、第４取引情報に含ませる第２電子署名の生成をする。記憶部は、第２電子署名を記憶する。作成部は、特定情報と第１電子署名とを含む第２取引情報の作成をする。また、作成部は、秘密情報を含む第３取引情報が第２ネットワークに公開されたあと、記憶部に記憶されている第２電子署名を用いて、秘密情報と第２電子署名とを含む第４取引情報の作成をする。送信部は、第１ネットワークに第４取引情報を送信する処理と、第２ネットワークに第２取引情報を送信する処理とをする。第１取引情報は、取引相手からユーザに第１データを引き渡しする取引に用いる情報である。第２取引情報は、ユーザから取引相手に第２データを引き渡しする取引に用いる情報である。第３取引情報は、取引相手がユーザから第２データを受け取る取引に用いる情報である。第４取引情報は、ユーザが取引相手から第１データを受け取る取引に用いる情報である。
【発明の効果】
【００１５】
１実施態様によれば、ハードウェアウォレットを用いたアトミックスワップにおいて、ユーザの作業を簡略にすることができる。
【図面の簡単な説明】
【００１６】
【図１】アトミックスワップに用いられるネットワーク構造の一例を示す図である。
【図２】暗号通貨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】ハードウェアウォレットを用いたアトミックスワップの処理の一例を示すシーケンス図である。
【図５】実施形態のハードウェアウォレットを用いたアトミックスワップの処理の一例を示すシーケンス図である。
【図６】取引装置の一実施例を示す機能ブロック図である。
【図７】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】

【００１７】
実施形態の取引装置について説明する。
以下の説明では、取引装置がアトミックスワップを用いて、異なる種類の暗号通貨を交換する処理について説明する。なお、実施形態の取引装置が実行するアトミックスワップは、暗号通貨の交換に限らず、メッセージの送信及び契約内容の管理などで用いるデータの交換にも用いることができる。
【００１８】
図１は、アトミックスワップに用いられるネットワーク構造の一例を示す図である。
図１を参照して、アトミックスワップに用いられるネットワーク構造を説明する。
アトミックスワップに用いられるネットワークは、取引装置１０と、取引装置２０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、取引装置１０と、取引装置２０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。
【００１９】
取引装置１０及び取引装置２０は、例えば、後述するコンピュータ装置である。以下の説明では、一例として、取引装置１０を取引相手が操作する取引装置として説明する。また、取引装置２０をユーザが操作する取引装置として説明する。
【００２０】
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、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、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。
【００２１】
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。
【００２２】
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。
【００２３】
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ナンスを変化させながら、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が並ぶハッシュ値が得られるナンス（以下、正しいナンスともいう。）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、ナンスと、取引情報とを含む。
【００２４】
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、ナンスを探す作業を実行する。ノード装置は、正しいナンスを発見すると、正しいナンス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。

【００２５】

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及び取引装置２０に加えて、さらに他の取引装置と接続されてもよい。

【００２６】

図２は、暗号通貨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、暗号通貨の引き渡しと、受け取りとを実行し、暗号通貨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。

【００２７】

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ユーザの公開鍵を含む。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ユーザの秘密鍵を用いて生成した電子署名を含む。

【００２８】

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、暗号通貨の所有権であり、次のトランザクションのインプットとしてＵＴＸＯが使用される。したがって、暗号通貨の送金とは、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、暗号通貨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、暗号通貨の使途を処理する情報である。ＵＴＸＯとは、Ｕｎｓｐｅｎｔ Ｔｒａｎｓａｃｔｉｏｎ Ｏｕｔｐｕｔの略である。

【００２９】

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ユーザ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、送信元のユーザ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、送信元のユーザ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。

【００３０】

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、暗号通貨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。

【００３１】

インプットは、トランザクションを作成する送信元のユーザ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、送信元のユーザが所有するＵＴＸＯをアンロックするためのスクリプトである。ＳｃｒｉｐｔＳｉｇは、送信元のユーザ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、送信元のユーザの秘密鍵を用いて

生成された値である。

【００３２】

アウトプットは、暗号通貨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、送信先のユーザ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。

【００３３】

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。

【００３４】

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。

【００３５】

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。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。

【００３６】

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ユーザの秘密鍵が用いられる。

【００３７】

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。

【００３８】

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。

【００３９】

取引装置１０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。

【００４０】
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。
【００４１】
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、ナンスを探す作業を実行する。ノード装置３００は、正しいナンスを発見すると、正しいナンス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。
【００４２】
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３を参照して、アトミックスワップの処理を説明する。
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、ユーザ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、取引装置２０が秘密値Ｒを生成してもよい。すなわち、以下で説明する取引装置１０の実行する処理を取引装置２０が実行し、取引装置２０が実行する処理を取引装置１０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、交換する暗号通貨の数量（交換数量）は、アトミックスワップの処理の前にユーザ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、ユーザと取引相手とは、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。ユーザと取引相手とは、暗号通貨の交換数量の決定、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。
【００４３】
ステップ（１）において、取引相手の取引装置１０は、秘密値Ｒをランダムに生成する。また、取引装置１０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。取引装置１０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。
【００４４】
さらに、取引装置１０は、ビットコインをユーザ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、取引装置１０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。
【００４５】
トランザクションＴｘ１のインプットは、取引相手の電子署名及び取引相手の公開鍵を含む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、取引相手が所有するＵＴＸＯである。取引相手の電子署名及び取引相手の公開鍵は、取引相手が所有する秘密鍵を用いて生成される。
【００４６】
トランザクションＴｘ１のアウトプットは、ハッシュ値Ｈ及びユーザの公開鍵ハッシュ

を含むＳｃｒｉｐｔＰｕｂＫｅｙを含む。ユーザの公開鍵ハッシュは、ユーザの公開鍵を用いて生成される。ユーザの公開鍵ハッシュとは、ユーザ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。

【００４７】

ステップ（２）において、ユーザの取引装置２０は、ライトコインを取引相手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、取引装置２０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。

【００４８】

トランザクションＴｘ２のインプットは、ユーザの電子署名及びユーザの公開鍵を含む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、ユーザが所有するＵＴＸＯである。ユーザの電子署名及びユーザの公開鍵は、ユーザが所有する秘密鍵を用いて生成される。

【００４９】

トランザクションＴｘ２のアウトプットは、ハッシュ値Ｈ及び取引相手の公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙを含む。取引相手の公開鍵ハッシュは、取引相手の公開鍵を用いて生成される。取引相手の公開鍵ハッシュとは、取引相手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、取引装置２０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。

【００５０】

ステップ（３）において、取引装置１０は、ライトコインを取引装置２０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、取引装置１０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。

【００５１】

トランザクションＴｘ３のインプットは、秘密値Ｒ、取引相手の公開鍵、及び取引相手の電子署名を含む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、取引相手の公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙを含む。

【００５２】

ユーザが送金したライトコインの所有を取引相手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を取引相手のアドレスにロックする処理を説明する。取引相手のアドレスとは、例えば、取引相手の公開鍵ハッシュを変換した値である。

【００５３】

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、取引装置１０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。

【００５４】

また、ノード装置４００は、トランザクションＴｘ３のＳｃｒｉｐｔＳｉｇに含まれる取引相手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に含まれる取引相手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に含まれる取引相手の電子署名と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。

【００５５】

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を取引相手のアドレスにロックする。すなわち、ノード装置４００は、取引相手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、取引相手が所有するＵＴＸＯとしてロックする。これにより、ライトコインの所有は、ユーザから取引相手に移転する。

【００５６】

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、取引相手の公開鍵を用いて、取引相手にビットコインを戻す処理を実行するスクリプトを含む。これにより、取引装置１０は、取引が成立しないとき、所定の時間経過後に取引相手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、暗号通貨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。

【００５７】

ステップ（４）において、取引装置２０は、取引相手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、ビットコインを取引装置１０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、取引装置２０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。

【００５８】

トランザクションＴｘ４のインプットは、秘密値Ｒ、ユーザの公開鍵、及びユーザの電子署名を含む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、ユーザの公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙを含む。

【００５９】

取引相手が送金したビットコインの所有をユーザ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をユーザのアドレスにロックする処理を説明する。ユーザのアドレスとは、例えば、ユーザの公開鍵ハッシュを変換した値である。

【００６０】

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、取引装置１０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。

【００６１】

また、ノード装置３００は、トランザクションＴｘ４のＳｃｒｉｐｔＳｉｇに含まれるユーザ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に含まれるユーザ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に含まれるユーザ

の電子署名と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。
【００６２】
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をユーザのアドレスにロックする。すなわち、ノード装置３００は、ユーザ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、ユーザが所有するＵＴＸＯとしてロックする。これにより、ビットコインの所有は、取引相手からユーザに移転する。
【００６３】
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、ユーザの公開鍵を用いて、ユーザにライトコインを戻す処理を実行するスクリプトを含む。これにより、取引装置２０は、取引が成立しないとき、所定の時間経過後にユーザのアドレスにライトコインを戻すことができる。
【００６４】
図４は、ハードウェアウォレットを用いたアトミックスワップの処理の一例を示す図（その１）である。
図４を参照して、ハードウェアウォレットを用いたアトミックスワップについて説明する。図３を参照して説明した処理については、説明を省略する。以下の説明では、ハードウェアウォレットＡは、取引相手の秘密鍵ａを格納しているものとして説明する。また、ハードウェアウォレットＢは、ユーザの秘密鍵ｂを格納しているものとして説明する。なお、以下で説明する取引装置１０の実行する処理を取引装置２０が実行し、取引装置２０が実行する処理を取引装置１０が実行してもよい。
【００６５】
取引装置１０は、ハードウェアウォレットＡが取引相手により接続されると、取引相手の電子署名Ａ１を生成する。そして、取引相手は、秘密鍵ａを用いて電子署名Ａ１が生成されると、ハードウェアウォレットＡを取引装置１０から取り外す（Ｓ１）。ハードウェアウォレットＡは、例えば、取引装置１０から電子署名用の値が入力されると、記憶している秘密鍵ａを用いて電子署名Ａ１を生成する署名生成回路を含んでもよい。
【００６６】
取引装置１０は、ビットコインをユーザ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、取引装置１０は、ネットワーク３０にトランザクションＴｘ１を送信する（Ｓ２）。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。
【００６７】
トランザクションＴｘ１のインプットは、電子署名Ａ１及び取引相手の公開鍵を含むＳｃｒｉｐｔＳｉｇＡ１（ＳＳｉｇＡ１）と、ＳｃｒｉｐｔＳｉｇＡ１を用いてアンロックされる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。また、トランザクションＴｘ１のアウトプットは、取引装置１０がランダムに生成した秘密値Ｒのハッシュ値Ｈ及びユーザの公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙＢ１（ＳＰｕｂＫｅｙＢ１）を含む。したがって、Ｓ２において、トランザクションＴｘ１がネットワーク３０に送信されることにより、ハッシュ値Ｈはネットワーク３０に公開される。
【００６８】
取引装置２０は、ハードウェアウォレットＢがユーザにより接続されると、ユーザの電子署名Ｂ１を生成する。そして、ユーザは、秘密鍵ｂを用いて電子署名Ｂ１が生成されると、ハードウェアウォレットＢを取引装置２０から取り外す（Ｓ３）。ハードウェアウォレットＢは、例えば、取引装置２０から電子署名用の値が入力されると、記憶している秘密鍵ｂを用いて電子署名Ｂ１を生成する署名生成回路を含んでもよい。Ｓ３において、例えば、ユーザは、トランザクションＴｘ１がビットコインのブロックチェーンに記録されて送金完了とみなされてから、ハードウェアウォレットＢを取引装置２０に接続する。
【００６９】
取引装置２０は、ライトコインを取引相手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、取引装置２０は、ネットワーク４０にトランザクションＴｘ２を送信する（Ｓ４）。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。

【００７０】

トランザクションＴｘ２のインプットは、電子署名Ｂ１及びユーザの公開鍵を含むＳｃｒｉｐｔＳｉｇ（ＳＳｉｇＢ１）と、ＳｃｒｉｐｔＳｉｇＢ１を用いてアンロックされる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。また、トランザクションＴｘ２のアウトプットは、Ｓ２においてネットワーク３０に公開されたハッシュ値Ｈ及び取引相手の公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙＡ１（ＳＰｕｂＫｅｙＡ１）を含む。

【００７１】

トランザクションＴｘ１及びトランザクションＴｘ２が承認され、それぞれが対応するブロックチェーンのブロックに記録されたあと、取引相手により取引装置１０にハードウェアウォレットＡが接続される。取引装置１０は、ハードウェアウォレットＡが取引相手により接続されると、トランザクションＴｘ２に含まれる情報を用いて生成した電子署名用の値と、ハードウェアウォレットＡに格納されている秘密鍵ａとを用いて、取引相手の電子署名Ａ２を生成する。そして、取引相手は、ハードウェアウォレットＡを取引装置１０から取り外す（Ｓ５）。Ｓ５において、例えば、取引相手は、トランザクションＴｘ２がライトコインのブロックチェーンに記録されて送金完了とみなされてから、ハードウェアウォレットＡを取引装置１０に接続する。

【００７２】

取引装置１０は、ライトコインを取引装置２０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、取引装置１０は、ネットワーク４０にトランザクションＴｘ３を送信する（Ｓ６）。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。

【００７３】

トランザクションＴｘ３のインプットは、秘密値Ｒ、取引相手の公開鍵、及び電子署名Ａ２を含むＳｃｒｉｐｔＳｉｇＡ２（ＳＳｉｇＡ２）と、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、取引相手の公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙＡ２（ＳＰｕｂＫｅｙＡ２）を含む。したがって、Ｓ６において、トランザクションＴｘ３がネットワーク４０に送信されることにより、秘密値Ｒはネットワーク４０に公開される。

【００７４】

そして、ノード装置４００がトランザクションＴｘ３のインプットと、トランザクションＴｘ２のアウトプットとを接続し、承認する。これにより、トランザクションＴｘ３がライトコインのブロックチェーンに記録され、ユーザから取引相手にライトコインを送金する処理が完了する。

【００７５】

なお、トランザクションＴｘ２に含まれるタイムロックの指定時間は、トランザクションＴｘ３がライトコインのブロックチェーンに記録されるよりも十分に長く設定される。すなわち、Ｓ５とＳ６との処理が、タイムロックを用いた返金処理よりも優先的に実行できるように設定されている。これにより、取引相手からビットコインを受け取ったユーザが、取引相手がライトコインを受け取るよりも先に自身のアドレスにライトコインを戻す処理をできなくすることで、取引の安全を確保している。

【００７６】

取引装置２０は、トランザクションＴｘ３がネットワーク４０に公開され、ハードウェアウォレットＢがユーザにより接続されると、ユーザの電子署名Ｂ２を生成する。そして、ユーザは、ハードウェアウォレットＢを取引装置２０から取り外す（Ｓ７）。

【００７７】

取引装置２０は、ビットコインを取引装置１０から受け取るためのトランザクションＴ

ｘ４を作成する。そして、取引装置２０は、ネットワーク３０にトランザクションＴｘ４を送信する（Ｓ８）。

【００７８】

トランザクションＴｘ４のインプットは、Ｓ６においてネットワーク４０に公開された秘密値Ｒ、ユーザの公開鍵、及び電子署名Ｂ２を含むＳｃｒｉｐｔＳｉｇＢ２（ＳＳｉｇＢ２）と、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、ユーザの公開鍵ハッシュを含むＳｃｒｉｐｔＰｕｂＫｅｙＢ２（ＳＰｕｂＫｅｙＢ２）を含む。そして、ノード装置３００がトランザクションＴｘ４のインプットと、トランザクションＴｘ１のアウトプットとを接続し、承認する。これにより、トランザクションＴｘ４がビットコインのブロックチェーンに記録され、取引相手からユーザにビットコインを送金する処理が完了する。

【００７９】

なお、トランザクションＴｘ１に含まれるタイムロックの指定時間は、トランザクションＴｘ４がビットコインのブロックチェーンに記録されるよりも十分に長く設定される。すなわち、Ｓ７とＳ８との処理が、タイムロックを用いた返金処理よりも優先的に実行できるように設定されている。これにより、ユーザからライトコインを受け取った取引相手が、ユーザがビットコインを受け取るよりも先に自身のアドレスにビットコインを戻す処理をできなくすることで、取引の安全を確保している。

【００８０】

アトミックスワップの処理では、上記のように、トランザクションＴｘ１及びトランザクションＴｘ２がブロックチェーンに記録されたあとに、トランザクションＴｘ３及びトランザクションＴｘ４の生成を実行する。

【００８１】

ビットコインのブロックチェーンは、１つのブロックを承認し、ブロックチェーンに連結するのに約１０分の時間を要する。そして、トランザクションＴｘ１を含むブロックがブロックチェーンに記録されてから、トランザクションＴｘ１を含むブロックの後ろに複数のブロックが連結されると送金完了とみなされる。複数のブロックの数は、新たに連結したブロックの改ざんができなくなると考えられる、十分に安全な数として決められる。

【００８２】

したがって、例えば、複数のブロックの数が５つである場合、トランザクションＴｘ１を作成したあと、トランザクションＴｘ１がブロックに記録されて、トランザクションＴｘ３を作成するまでに、少なくとも約６０分以上の時間がかかることになる。すると、取引相手は、アトミックスワップの処理をするとき、できる限りハードウェアウォレットＡをオフライン状態にしておくために、少なくとも約６０分以上の時間をおいて、ハードウェアウォレットＡを取引装置１０に抜き差しする作業をしなければならない。なお、トランザクションＴｘ１の送金手数料が低く設定されていると、ノード装置３００によるトランザクションの承認の優先順位も低くなるので、結果として時間間隔が６０分よりもさらに長くかかることもある。

【００８３】

また、ライトコインのブロックチェーンは、１つのブロックを承認し、ブロックチェーンに連結するのに約２．５分の時間を要する。そして、トランザクションＴｘ２を含むブロックがブロックチェーンに記録されてから、トランザクションＴｘ２を含むブロックの後ろに複数のブロックが連結されると送金完了とみなされる。複数のブロックの数は、新たに連結したブロックの改ざんができなくなると考えられる、十分に安全な数として決められる。

【００８４】

したがって、例えば、複数のブロックの数が５つである場合、トランザクションＴｘ２を作成したあと、トランザクションＴｘ２がブロックに記録されて、トランザクションＴｘ４を作成するまでに、少なくとも約１２．５分以上の時間がかかることになる。すると、ユーザは、アトミックスワップの処理をするとき、できる限りハードウェアウォレット

Ｂをオフライン状態にしておくために、少なくとも約１２．５分以上の時間をおいて、ハードウェアウォレットＢを抜き差しする作業をしなければならない。なお、トランザクションＴｘ２の送金手数料が低く設定されていると、ノード装置４００によるトランザクションの承認の優先順位も低くなるので、結果として時間間隔が１２．５分よりもさらに長くかかることもある。

【００８５】

以上のように、ハードウェアウォレットを用いたアトミックスワップでは、安全性を確保するために、電子署名の生成処理を実行するタイミング以外において、ハードウェアウォレットを取引装置から取り外しておき、オフライン状態にしておく作業が発生する。したがって、ハードウェアウォレットを用いたアトミックスワップでは、安全性を確保するために、ハードウェアウォレットを取引装置に抜き差ししなければならないので、ユーザの作業が煩雑になる。

【００８６】

図５は、実施形態のハードウェアウォレットを用いたアトミックスワップの処理の一例を示すシーケンス図である。

図５を参照して、ハードウェアウォレットを用いたアトミックスワップの処理の一例を説明する。

アトミックスワップに用いられるネットワークは、図１に示すように、取引装置７０と、取引装置８０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、取引装置７０と、取引装置８０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。

図３及び図４を参照して説明した処理については、説明を省略する。以下の説明では、図５に記載の実施形態の電子署名に含まれるデータ及びトランザクションの記述と、図４を用いて説明した電子署名に含まれるデータ及びトランザクションの記述とは、同じ内容であるので同じ符号を付し説明を省略する。なお、以下で説明する取引装置７０の実行する処理を取引装置８０が実行し、取引装置８０が実行する処理を取引装置７０が実行してもよい。

【００８７】

取引装置７０及び取引装置８０は、例えば、後述するコンピュータ装置である。以下の説明では、一例として、取引装置７０を取引相手が操作する取引装置として説明する。また、取引装置８０をユーザが操作する取引装置として説明する。

【００８８】

取引装置７０は、ハードウェアウォレットＡが取引相手により接続されると、取引相手の秘密鍵ａを用いて電子署名Ａ１を生成する。そして、取引相手は、秘密鍵ａを用いて電子署名Ａ１が生成されると、ハードウェアウォレットＡを取引装置７０から取り外す（Ｓ１１）。また、取引装置７０は、秘密値Ｒをランダムに生成する。さらに、取引装置７０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。取引装置７０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。

【００８９】

そして、取引装置７０は、ビットコインをユーザ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、取引装置７０は、ネットワーク３０にトランザクションＴｘ１を送信する（Ｓ１２）。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。したがって、トランザクションＴｘ１のＳｃｒｉｐｔＰｕｂＫｅｙＢ１（ＳＰｕｂＫｅｙＢ１）に含まれるハッシュ値Ｈもネットワーク３０に公開されることになる。

【００９０】

取引装置８０は、トランザクションＴｘ１がネットワーク３０に公開されたあと、ハードウェアウォレットＢがユーザにより接続されると、ユーザの秘密鍵ｂを用いて電子署名Ｂ１を生成する（Ｓ１３）。さらに、取引装置８０は、ユーザの電子署名Ｂ２を生成する。そして、ユーザは、秘密鍵ｂを用いて電子署名Ｂ１及び電子署名Ｂ２が生成されると、

ハードウェアウォレットＢを取引装置８０から取り外す（Ｓ１４）。

【００９１】

取引装置８０は、例えば、下記の方法でトランザクションＴｘ１がネットワーク３０に公開されたか否かを監視し、トランザクションＴｘ１がネットワーク３０に公開されたと判定すると、Ｓ１３及びＳ１４の処理を実行する。

取引装置８０は、例えば、取引相手のアドレスを用いて、取引装置７０から送信されたトランザクションを監視することにより、トランザクションＴｘ１がネットワーク３０に公開されたか否かを判定してもよい。また、取引装置８０は、取引装置７０からトランザクションＴｘ１のトランザクションＩＤを受け取り、ビットコインのブロックチェーンを監視することにより、トランザクションＴｘ１がネットワーク３０に公開されたことを判定してもよい。

【００９２】

そして、取引装置８０は、トランザクションＴｘ１がネットワーク３０に公開されたとき、取引装置８０の音声、表示、及び振動などの機能の少なくとも一つを利用してユーザに通知してもよい。また、取引装置８０は、トランザクションＴｘ１がネットワーク３０に公開されたとき、ユーザが携帯する携帯端末に情報を出力することにより、携帯端末の音声、表示、または振動などの機能を利用してユーザに通知してもよい。図５を用いた説明においては、取引装置８０による通知のタイミングは、トランザクションＴｘ１がネットワーク３０に公開されたときであるものとして説明する。これに限らず、取引装置８０による通知のタイミングは、トランザクションＴｘ１がネットワーク３０に公開されたあと、であれば他のタイミングであってもよい。

【００９３】

取引装置８０は、Ｓ１２において公開されたトランザクションＴｘ１のＳｃｒｉｐｔＰｕｂＫｅｙＢ１に含まれるハッシュ値Ｈを用いて、ライトコインを取引装置７０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、取引装置８０は、トランザクションＴｘ１がビットコインのブロックチェーンに記録されたあと、ネットワーク４０にトランザクションＴｘ２を送信する（Ｓ１５）。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。

【００９４】

取引装置８０は、Ｓ１２において公開されたトランザクションＴｘ１に含まれる情報を用いて、ビットコインを取引装置７０から受け取るための仮のトランザクションＴｘ４を作成する。そして、取引装置８０は、仮のトランザクションＴｘ４を記憶する（Ｓ１６）。仮のトランザクションＴｘ４とは、トランザクションＴｘ４から秘密値Ｒを除いた情報である。すなわち、仮のトランザクションＴｘ４は、秘密値Ｒがネットワーク４０に公開される前に得られる情報を用いて作成された、秘密値Ｒを含まないトランザクションＴｘ４である。なお、Ｓ１３のあとに Ｓ１５、Ｓ１４のあとにＳ１６、という処理の順番を守る限り、Ｓ１３からＳ１６の処理は順不同に実行されてもよい。

【００９５】

取引装置７０は、トランザクションＴｘ２がネットワーク４０に公開されたあと、ハードウェアウォレットＡが取引相手により接続されると、トランザクションＴｘ２に記述された情報を用いて電子署名用の値を生成する。そして、取引装置７０は、電子署名用の値と、ハードウェアウォレットＡに格納されている秘密鍵ａとを用いて、ユーザの電子署名Ａ２を生成する。そして、取引相手は、秘密鍵ａを用いて電子署名Ａ２が生成されると、ハードウェアウォレットＡを取引装置７０から取り外す（Ｓ１７）。

【００９６】

取引装置７０は、例えば、下記の方法でトランザクションＴｘ２がネットワーク４０に公開されたか否かを監視し、トランザクションＴｘ２がネットワーク４０に公開されたと判定すると、Ｓ１７の処理を実行する。

取引装置７０は、例えば、ユーザのアドレスを用いて、取引装置８０から送信されたトランザクションを監視することにより、トランザクションＴｘ２がネットワーク４０に公

開されたか否かを判定してもよい。また、取引装置７０は、取引装置８０からトランザクションＴｘ２のトランザクションＩＤを受け取り、ライトコインのブロックチェーンを監視することにより、トランザクションＴｘ２がネットワーク４０に公開されたことを判定してもよい。

【００９７】

そして、取引装置７０は、トランザクションＴｘ２がネットワーク４０に公開されると、取引装置７０の音声、表示、及び振動などの機能の少なくとも一つを利用して取引相手に通知してもよい。また、取引装置７０は、トランザクションＴｘ２がネットワーク４０に公開されると、取引相手が携帯する携帯端末に情報を出力することにより、携帯端末の音声、表示、または振動などの機能を利用して取引相手に通知してもよい。図５を用いた説明においては、取引装置７０による通知のタイミングは、トランザクションＴｘ２がネットワーク４０に公開されたときであるものとして説明する。これに限らず、取引装置７０による通知のタイミングは、トランザクションＴｘ２がネットワーク４０に公開されたあと、であれば他のタイミングであってもよい。

【００９８】

取引装置７０は、電子署名Ａ２を生成すると、ライトコインを取引装置８０から受け取るための電子署名Ａ２を含むトランザクションＴｘ３を作成する。そして、取引装置７０は、トランザクションＴｘ２がライトコインのブロックチェーンに記録されたあと、ネットワーク４０にトランザクションＴｘ３を送信する（Ｓ１８）。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。したがって、トランザクションＴｘ３のＳｃｒｉｐｔＳｉｇＡ２（ＳＳｉｇＡ２）に含まれる秘密値Ｒもネットワーク４０に公開されることになる。そして、トランザクションＴｘ３は、ノード装置４００により承認されることにより、ライトコインのブロックチェーンに記録される。なお、Ｓ１４のあとにＳ１６、Ｓ１５のあとにＳ１７、Ｓ１７のあとにＳ１８、という処理の順番を守る限り、Ｓ１４、Ｓ１６、Ｓ１７、Ｓ１８の処理は順不同に実行されてもよい。

【００９９】

取引装置８０は、Ｓ１８において公開されたトランザクションＴｘ３のＳｃｒｉｐｔＳｉｇＡ２に含まれる秘密値Ｒと、記憶している仮のトランザクションＴｘ４とを用いて、ビットコインを取引装置７０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、取引装置８０は、ネットワーク３０にトランザクションＴｘ４を送信する（Ｓ１９）。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。そして、トランザクションＴｘ４は、ノード装置３００により承認されることにより、ビットコインのブロックチェーンに記録される。

【０１００】

上記の説明では、取引装置８０は、Ｓ１６において、仮のトランザクションＴｘ４を作成したが、Ｓ１４において、電子署名Ｂ２を記憶することにより、Ｓ１６の処理を省略してもよい。この場合には、取引装置８０は、Ｓ１４において生成した電子署名Ｂ２を記憶し、Ｓ１９において、ネットワーク４０に公開されたトランザクションＴｘ３のＳｃｒｉｐｔＳｉｇＡ２に含まれる秘密値Ｒと、記憶している電子署名Ｂ２とを用いてトランザクションＴｘ４を作成する。

【０１０１】

なお、ノード装置が、トランザクションから秘密値Ｒ及びハッシュ値Ｈの値を取得し、秘密値Ｒにハッシュ関数を適用したハッシュ値と、ハッシュ値Ｈとが一致するか否かの検証を、上記した第４検証に代えて実行する場合、下記の構成を採用してもよい。上記の説明では、ハッシュ値ＨをＳｃｒｉｐｔＰｕｂＫｅｙＡ１及びＳｃｒｉｐｔＰｕｂＫｅｙＢ１に含むものとして説明したが、ハッシュ値Ｈは、数値としてトランザクションＴｘ１及びトランザクションＴｘ２に含まれてもよい。また、秘密値ＲをＳｃｒｉｐｔＳｉｇＡ２及びＳｃｒｉｐｔＳｉｇＢ２に含むものとして説明したが、秘密値Ｒは、数値としてトランザクションＴｘ３及びトランザクションＴｘ４に含まれてもよい。

【０１０２】

図６は、取引装置の一実施例を示す機能ブロック図である。
図６は、取引装置７０及び取引装置８０が有する機能を示すブロック図である。
図６を参照して、取引装置８０の機能について説明する。なお、取引装置７０は、取引装置８０の機能の少なくとも１つ以上の機能を有してもよい。以下の説明では、図５で説明した構成に関しては、同じ符号を付し、説明を省略する。また、ビットコインを引き渡しする処理と、受け取る処理とは、ビットコインの所有権を移転する処理のことである。また、ライトコインを引き渡しする処理と、受け取る処理とは、ライトコインの所有権を移転する処理のことである。ビットコインは、第１データの一例である。ライトコインは、第２データの一例である。

【０１０３】

取引装置８０は、制御部６０と、接続部９１と、記憶部９２と、表示部９３とを含む。制御部６０は、生成部６１と、作成部６２と、送信部６３と、通知部６４と、受付部６５と、を含む。接続部９１は、電子署名Ｂ１と電子署名Ｂ２とを生成するときに用いられる秘密鍵ｂを格納するハードウェアウォレットＢ（記憶装置）と着脱可能に接続される。記憶部９２は、各種情報を記憶する。表示部９３は、各種情報を表示する。

【０１０４】

記憶部９２は、生成部６１により生成される電子署名Ｂ２、並びに作成部６２により作成される仮のトランザクションＴｘ４の少なくとも一方を記憶する。また、記憶部９２は、作成部６２により作成されるトランザクションＴｘ２を記憶してもよい。さらに、記憶部９２は、電子署名Ｂ１を記憶してもよい。トランザクションＴｘ２は、ユーザから取引相手にライトコインを引き渡しする取引に用いる情報である。トランザクションＴｘ２は、第２取引情報の一例である。トランザクションＴｘ４は、ユーザが取引相手からビットコインを受け取る取引に用いる情報である。トランザクションＴｘ４は、第４取引情報の一例である。

【０１０５】

生成部６１は、秘密値Ｒを用いて算出されたハッシュ値Ｈを含むトランザクションＴｘ１がネットワーク３０に公開されたあと、ハッシュ値Ｈを含むトランザクションＴｘ２に含ませる電子署名Ｂ１を生成する。すなわち、生成部６１は、トランザクションＴｘ１に含まれるハッシュ値Ｈを用いて、ハッシュ値を含むトランザクションＴｘ２を生成する。このとき、生成部６１は、ユーザにより接続部９１に接続されるハードウェアウォレットＢに格納されている秘密鍵ｂを用いて、電子署名Ｂ１を生成する。秘密値Ｒは、秘密情報の一例である。ハッシュ値Ｈは、特定情報の一例である。トランザクションＴｘ１は、取引相手からユーザにビットコインを引き渡しする取引に用いる情報である。トランザクションＴｘ１は、第１取引情報の一例である。電子署名Ｂ１は、第１電子署名の一例である。ネットワーク３０は、第１ネットワークの一例である。

【０１０６】

また、生成部６１は、トランザクションＴｘ１がネットワーク３０に公開されたあと、トランザクションＴｘ１に含まれる情報を用いて、トランザクションＴｘ４に含ませる電子署名Ｂ２を生成する。このとき、生成部６１は、ユーザにより接続部９１に接続されるハードウェアウォレットＢに格納されている秘密鍵ｂを用いて、電子署名Ｂ２を生成する。そして、生成部６１は、生成した電子署名Ｂ２を記憶部９２に記憶させてもよい。電子署名Ｂ２は、第２電子署名の一例である。トランザクションＴｘ１に含まれる情報とは、例えば、トランザクションＴｘ４のＳｃｒｉｐｔＳｉｇＢ２と接続される、トランザクションＴｘ１のＳｃｒｉｐｔＰｕｂＫｅｙＢ１である。

【０１０７】

作成部６２は、ハッシュ値と電子署名Ｂ１とを含むトランザクションＴｘ２を作成する。そして、作成部６２は、作成したトランザクションＴｘ２を記憶部９２に記憶させてもよい。作成部６２は、記憶部９２に電子署名Ｂ２が記憶されているとき、秘密値Ｒを含むトランザクションＴｘ３がネットワーク４０に公開されたあと、記憶部９２に記憶されている電子署名Ｂ２を用いて秘密値Ｒと電子署名Ｂ２とを含むトランザクションＴｘ４を作

成する。なお、作成部６２は、トランザクションＴｘ４を作成したあと、安全性を確保するために、記憶部９２から電子署名Ｂ２を消去してもよい。トランザクションＴｘ３は、取引相手がユーザからライトコインを受け取る取引に用いるトランザクションである。トランザクションＴｘ３は、第３取引情報の一例である。ネットワーク４０は、第２ネットワークの一例である。

【０１０８】

作成部６２は、仮のトランザクションＴｘ４を作成して記憶部９２に記憶させてもよい。すなわち、作成部６２は、電子署名Ｂ２を仮のトランザクションＴｘ４に含ませた状態で記憶部９２に記憶させる。作成部６２は、記憶部９２に仮のトランザクションＴｘ４が記憶されているとき、秘密値Ｒを含む第３トランザクションがネットワーク４０に公開されたあと、記憶部９２に記憶されている仮のトランザクションＴｘ４を用いて、トランザクションＴｘ４を作成する。なお、作成部６２は、トランザクションＴｘ４を作成したあと、安全性を確保するために、記憶部９２から電子署名Ｂ２を消去してもよい。また、作成部６２は、記憶部９２に電子署名Ｂ２及び仮のトランザクションＴｘ４が記憶されているとき、電子署名Ｂ２及び仮のトランザクションＴｘ４のいずれか一方を用いてトランザクションＴｘ４を作成してもよい。

【０１０９】

作成部６２は、記憶部９２に電子署名Ｂ１が記憶されているとき、トランザクションＴｘ１がネットワーク３０に公開されたあと、記憶部９２に記憶されている電子署名Ｂ１を用いて、ハッシュ値Ｈと電子署名Ｂ１とを含むトランザクションＴｘ２を作成してもよい。この場合には、作成部６２は、ビットコインのブロックチェーンにトランザクションＴｘ１が記録されたあと、記憶部９２に記憶されている電子署名Ｂ１を用いて、ハッシュ値と電子署名Ｂ１とを含むトランザクションＴｘ２を作成してもよい。

【０１１０】

送信部６３は、ネットワーク３０にトランザクションＴｘ４を送信する。また、送信部６３は、ネットワーク４０にトランザクションＴｘ２を送信する。すなわち、送信部６３は、ビットコインの取引が実行されるネットワーク３０に、トランザクションＴｘ４を送信する。さらに、送信部６３は、ライトコインの取引が実行されるネットワーク４０に、トランザクションＴｘ２を送信する。

【０１１１】

送信部６３は、記憶部９２にトランザクションＴｘ２が記憶されているとき、ビットコインのブロックチェーンにトランザクションＴｘ１が記録されたか否かを判定する。そして、送信部６３は、ビットコインのブロックチェーンにトランザクションＴｘ１が記録されたあと、記憶部９２に記憶されているトランザクションＴｘ２をネットワーク４０に送信する。

【０１１２】

通知部６４は、トランザクションＴｘ１がネットワーク３０に公開されたあと、トランザクションＴｘ１が公開されたことを通知する。通知部６４は、例えば、ネットワーク３０上でユーザのアドレス宛に送信されたトランザクションを監視することにより、トランザクションＴｘ１が公開されたか否かを判定してもよい。また、通知部６４は、例えば、トランザクションＴｘ１が公開されたとき、表示部９３にトランザクションＴｘ１が公開されたことを示す情報を表示することにより、トランザクションＴｘ１が公開されたことをユーザに通知してもよい。

【０１１３】

通知部６４は、トランザクションＴｘ１がビットコインのブロックチェーンに記録されたあと、トランザクションＴｘ１がビットコインのブロックチェーンに記録されたことを通知してもよい。通知部６４は、例えば、ネットワーク４０上で取引相手のアドレス宛に送信されたトランザクションを監視することにより、トランザクションＴｘ１がビットコインのブロックチェーンに記録されたか否かを判定してもよい。また、通知部６４は、例えば、トランザクションＴｘ１がビットコインのブロックチェーンに記録されたあと、表

示部９３にトランザクションＴｘ１が記録されたことを示す情報を表示してもよい。これにより、通知部６４は、トランザクションＴｘ１がビットコインのブロックチェーンに記録されたことを取引相手に通知してもよい。

【０１１４】

受付部６５は、ハードウェアウォレットＢが接続部９１に接続されたとき、ユーザによる秘密鍵ｂの入力を受け付ける。受付部６５は、例えば、ハードウェアウォレットＢが接続部９１に接続されたとき、自動的に秘密鍵ｂを取得してもよい。

【０１１５】

図６を参照して、取引装置７０の機能を説明する。なお、取引装置８０は、取引装置７０の機能の少なくとも１つ以上の機能を有してもよい。

取引装置７０は、制御部６０と、接続部９１と、記憶部９２と、表示部９３とを含む。制御部６０は、生成部６１と、作成部６２と、送信部６３と、通知部６４と、受付部６５と、を含む。接続部９１は、電子署名Ａ１と電子署名Ａ２とを生成するときに用いられる秘密鍵ａを格納するハードウェアウォレットＡ（記憶装置）と着脱可能に接続される。記憶部９２は、各種情報を記憶する。表示部９３は、各種情報を表示する。

【０１１６】

生成部６１は、ユーザにより接続部９１に接続されるハードウェアウォレットＡに格納されている秘密鍵ａを用いて、電子署名Ａ１を生成する。また、生成部６１は、トランザクションＴｘ２がネットワーク４０に公開されたあと、ユーザにより接続部９１に接続されるハードウェアウォレットＡに格納されている秘密鍵ａと、トランザクションＴｘ２に含まれる情報とを用いて、電子署名Ａ２を生成する。

作成部６２は、ハッシュ値Ｈと電子署名Ａ１とを用いて、トランザクションＴｘ１を作成する。また、作成部６２は、秘密値Ｒと電子署名Ａ２とを用いて、トランザクションＴｘ３を作成する。

送信部６３は、トランザクションＴｘ１をネットワーク３０に送信する。また、送信部６３は、トランザクションＴｘ３をネットワーク４０に送信する。すなわち、送信部６３は、ビットコインの取引が実行されるネットワーク３０に、トランザクションＴｘ１を送信する。さらに、送信部６３は、ライトコインの取引が実行されるネットワーク４０に、トランザクションＴｘ３を送信する。

【０１１７】

通知部６４は、トランザクションＴｘ２がネットワーク４０に公開されたとき、トランザクションＴｘ２が公開されたことを通知する。通知部６４は、例えば、ネットワーク４０上で取引相手のアドレス宛に送信されたトランザクションを監視することにより、トランザクションＴｘ２が公開されたか否かを判定してもよい。また、通知部６４は、例えば、トランザクションＴｘ２が公開されたとき、表示部９３にトランザクションＴｘ２が公開されたことを示す情報を表示することにより、トランザクションＴｘ２が公開されたことを取引相手に通知してもよい。

【０１１８】

通知部６４は、トランザクションＴｘ２がライトコインのブロックチェーンに記録されたあと、トランザクションＴｘ２がライトコインのブロックチェーンに記録されたことを通知してもよい。通知部６４は、例えば、ネットワーク４０上で取引相手のアドレス宛に送信されたトランザクションを監視することにより、トランザクションＴｘ２がライトコインのブロックチェーンに記録されたか否かを判定してもよい。また、通知部６４は、例えば、トランザクションＴｘ２がライトコインのブロックチェーンに記録されたあと、表示部９３にトランザクションＴｘ２が記録されたことを示す情報を表示してもよい。これにより、通知部６４は、トランザクションＴｘ２がライトコインのブロックチェーンに記録されたことを取引相手に通知してもよい。

【０１１９】

受付部６５は、ハードウェアウォレットＡが接続部９１に接続されたとき、ユーザによる秘密鍵ａの入力を受け付ける。受付部６５は、例えば、ハードウェアウォレットＡが接

続部９１に接続されたとき、自動的に秘密鍵ａを取得してもよい。

【０１２０】

図７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７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７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４００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、取引装置７０、及び取引装置８０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。

【０１２１】

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）などのプロセッサである。制御回路５１は、例えば、図６において、制御部６０として機能する。

【０１２２】

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として機能させる取引プログラムを記憶してもよい。記憶装置５２は、例えば、図６において、記憶部９２として機能する。

【０１２３】

取引装置７０及び取引装置８０は、取引処理をするとき、記憶装置５２に記憶された取引プログラムをＲＡＭに読み出す。ＲＡＭに読み出された取引プログラムを制御回路５１で実行することにより、取引装置７０及び取引装置８０は、生成処理と、作成処理と、送信処理と、通知処理と、接続処理と、受付処理とのいずれか１以上を含む取引処理を実行する。なお、取引プログラムは、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４００上のサーバが有する記憶装置に記憶されていても良い。

【０１２４】

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、取引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。

【０１２５】

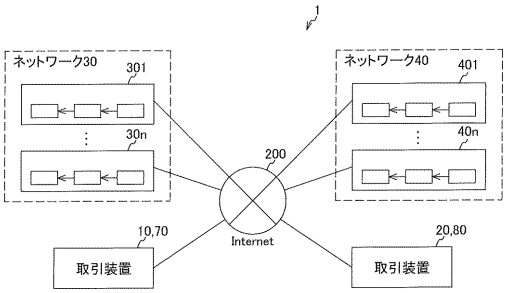
通信インターフェイス５５は、ネットワーク４００を介してコンピュータ装置５０と他の装置とを通信可能に接続する。

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と接続される入力装置には、例えば、ハードウェアウォレットＨＷ、キーボード、及びマウスなどがある。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。ハードウェアウォレットＨＷは、例えば、ハードウェアウォレットＡ及びハードウェアウォレットＢである。入出力インターフェイス５６は、例えば、図６において、接続部９１として機能する。

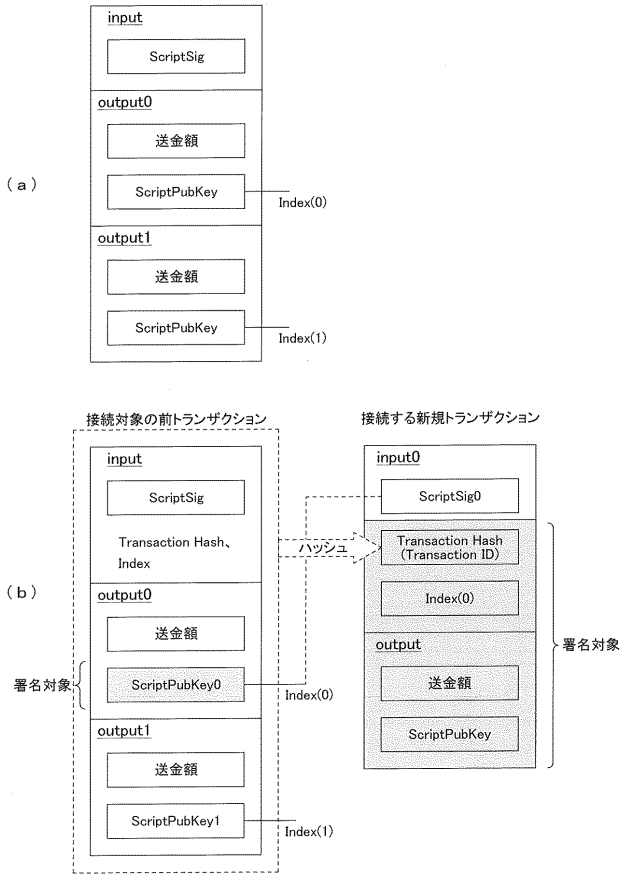
【０１２６】
入力装置５７は、例えば、タッチパネル、コード読み取り装置及びキーボードなどである。入出力インターフェイス５６に接続された各種入力装置及び入力装置５７は、例えば、ユーザ及び取引相手から秘密鍵、公開鍵、トランザクションＩＤ、及び秘密値Ｒなどの入力を受け付けてもよい。
【０１２７】
表示装置５８は、各種情報を表示する。表示装置５８は、例えば、及びトランザクションＴｘ１が公開されたとき、トランザクションＴｘ１が公開されたことを示す画像を表示してもよい。また、表示装置５８は、例えば、及びトランザクションＴｘ２が公開されたとき、トランザクションＴｘ２が公開されたことを示す画像を表示してもよい。さらに、表示装置５８は、タッチパネルでの入力を受け付けるための情報を表示しても良い。表示装置５８は、例えば、図６の表示部９３として機能する。
ネットワーク４００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。
【０１２８】
以上のように、実施形態の取引装置８０は、トランザクションＴｘ１がネットワーク３０に公開されたあと、電子署名Ｂ１及び電子署名Ｂ２を生成し、記憶装置５２に電子署名Ｂ２を記憶させる。そして、取引装置８０は、トランザクションＴｘ３がネットワー４０に公開されたあと、トランザクションＴｘ３に含まれる秘密値Ｒと、記憶装置５２に記憶している電子署名Ｂ２とを用いてトランザクションＴｘ４を作成する。したがって、取引装置７０は、ハードウェアウォレットが一度接続されるだけでアトミックスワップの処理を実行できるので、ユーザの作業を簡略にすることができる。
【０１２９】
実施形態の取引装置８０は、トランザクションＴｘ１がネットワーク３０に公開されたあと、電子署名Ｂ１及び電子署名Ｂ２を生成する。さらに、取引装置８０は、秘密値Ｒを含まない仮のトランザクションＴｘ４を作成し、記憶装置５２に記憶させる。そして、取引装置８０は、トランザクションＴｘ３がネットワー４０に公開されたあと、トランザクションＴｘ３に含まれる秘密値Ｒと、記憶装置５２に記憶している仮のトランザクションＴｘ４とを用いてトランザクションＴｘ４を作成する。したがって、取引装置８０は、ハードウェアウォレットが一度接続されるだけでアトミックスワップの処理を実行できるので、ユーザの作業を簡略にすることができる。
【０１３０】
実施形態の取引装置８０は、取引装置７０によりトランザクションＴｘ１がネットワーク３０に公開されたあと、トランザクションＴｘ１が公開されたことをユーザに通知する。これにより、取引装置８０は、トランザクションＴｘ１が公開されたあと、ユーザにハードウェアウォレットＢを接続するタイミングを知らせることができる。なお、取引装置８０は、トランザクションＴｘ１がビットコインのブロックチェーンに記録されたあと、トランザクションＴｘ１がビットコインのブロックチェーンに記録されたことをユーザに通知してもよい。これにより、取引装置８０は、トランザクションＴｘ１がビットコインのブロックチェーンに記録されたあと、ユーザにハードウェアウォレットＢを接続するタイミングを知らせることができる。この場合には、取引装置８０は、トランザクションＴｘ１がビットコインのブロックチェーンに記録される前にハードウェアウォレットＢが接続部９１に接続される場合と比較して、電子署名Ｂ１及び電子署名Ｂ２を記憶部９２に記憶しておく時間を短くできる。したがって、取引装置８０は、より安全性の高い取引を実行することができる。
【０１３１】
実施形態の取引装置８０は、ハードウェアウォレットＢと着脱可能に接続される接続部９１を有するので、電子署名Ｂ１及び電子署名Ｂ２の生成処理の実行のとき以外において、ハードウェアウォレットＢをオフラインにすることが可能である。したがって、取引装置８０は、アトミックスワップ実行時の安全性を向上することができる。

【０１３２】
実施形態の取引装置８０は、電子署名Ｂ１及び電子署名Ｂ２を記憶装置５２に記憶する。そして、取引装置８０は、取引装置７０によりトランザクションＴｘ１がネットワーク３０に公開されたあと、記憶装置５２に記憶されている電子署名Ｂ１を用いて、ハッシュ値Ｈと電子署名Ｂ１とを含むトランザクションＴｘ２を作成する。この場合には、取引装置８０は、ビットコインのブロックチェーンにトランザクションＴｘ１が記録されたあと、記憶部９２に記憶されている電子署名Ｂ１を用いて、ハッシュ値と電子署名Ｂ１とを含むトランザクションＴｘ２を作成してもよい。これにより、取引装置８０は、トランザクションＴｘ１がネットワーク３０に公開されたあと、ユーザの任意のタイミングでハードウェアウォレットＢの接続を受け付け、電子署名Ｂ１及び電子署名Ｂ２を同じタイミングで生成することが可能になる。したがって、取引装置８０は、ユーザの作業を簡略にすることができる。
【０１３３】
実施形態の取引装置８０は、トランザクションＴｘ２を記憶装置５２に記憶する。そして、取引装置８０は、ビットコインのブロックチェーンにトランザクションＴｘ１が記録されたあと、記憶装置５２に記憶されているトランザクションＴｘ２をネットワーク４０に送信する。これにより、取引装置８０は、二重払いのリスクを抑制することができる。
【０１３４】
上記の説明においては、ビットコインのブロックチェーン及びライトコインのブロックチェーンを用いて説明したが、例えば、モナコインのブロックチェーン及びイーサリアムのブロックチェーンなど他の種類のブロックチェーンを利用してもよい。他のブロックチェーンを用いる場合でも、取引装置８０は、電子署名Ｂ１及び電子署名Ｂ２を同じタイミングで生成し、電子署名Ｂ２を記憶装置５２に記憶することより、ハードウェアウォレットＢが一度接続されるだけでアトミックスワップを実行することができる。
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】
【０１３５】
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　制御部
７０、８０　取引装置
９１　接続部
９２　記憶部
９３　表示部

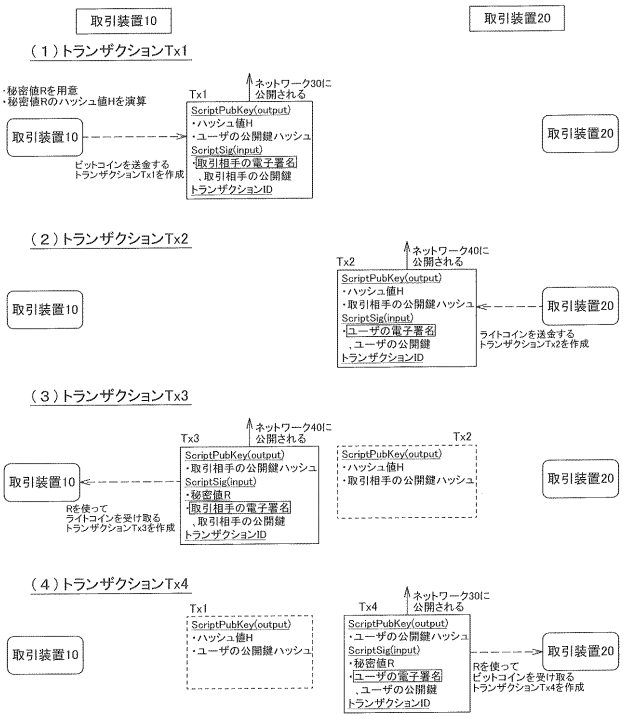
【図１】


1
ネットワーク30
301
30n
ネットワーク40
401
40n
200
Internet
10,70
取引装置
20,80
取引装置

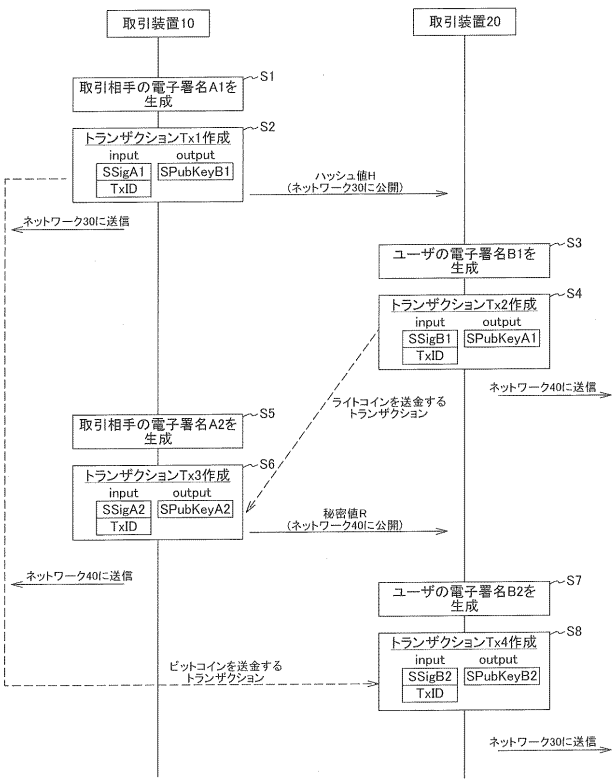
【図２】


（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

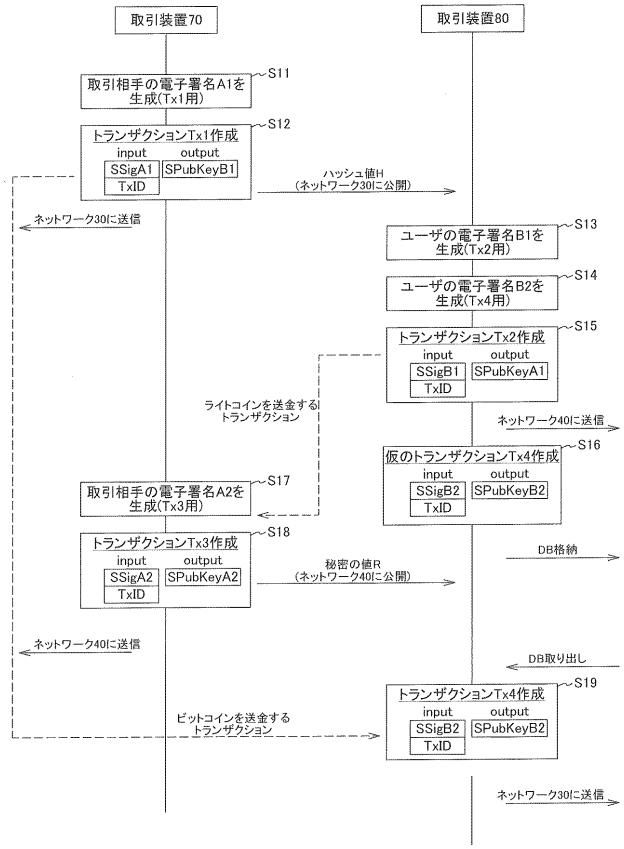
【図３】


取引装置10
取引装置20
（１）トランザクションTx1
・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
・ユーザの公開鍵ハッシュ
ScriptSig(input)
・取引相手の電子署名
、取引相手の公開鍵
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
（２）トランザクションTx2
Tx2
ネットワーク40に公開される
ScriptPubKey(output)
・ハッシュ値H
・取引相手の公開鍵ハッシュ
ScriptSig(input)
・ユーザの電子署名
、ユーザの公開鍵
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
（３）トランザクションTx3
Tx3
ネットワーク40に公開される
ScriptPubKey(output)
・取引相手の公開鍵ハッシュ
ScriptSig(input)
・秘密値R
・取引相手の電子署名
、取引相手の公開鍵
トランザクションID
Tx2
ScriptPubKey(output)
・ハッシュ値H
・取引相手の公開鍵ハッシュ
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
（４）トランザクションTx4
Tx1
ScriptPubKey(output)
・ハッシュ値H
・ユーザの公開鍵ハッシュ
Tx4
ネットワーク30に公開される
ScriptPubKey(output)
・ユーザの公開鍵ハッシュ
ScriptSig(input)
・秘密値R
・ユーザの電子署名
、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

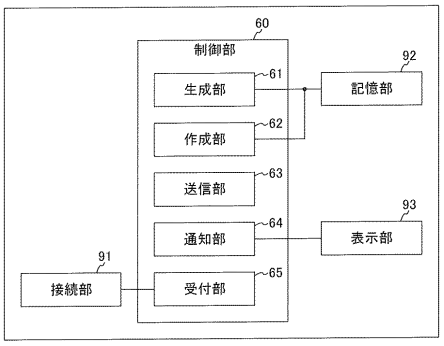
【図４】


取引装置10
取引装置20
取引相手の電子署名A1を生成
S1
トランザクションTx1作成
input output
SSigA1 SPubKeyB1
TxID
S2
ハッシュ値H
(ネットワーク30に公開)
ネットワーク30に送信
ユーザの電子署名B1を生成
S3
トランザクションTx2作成
input output
SSigB1 SPubKeyA1
TxID
S4
ネットワーク40に送信
ライトコインを送金する
トランザクション
取引相手の電子署名A2を生成
S5
トランザクションTx3作成
input output
SSigA2 SPubKeyA2
TxID
S6
秘密値R
(ネットワーク40に公開)
ネットワーク40に送信
ユーザの電子署名B2を生成
S7
トランザクションTx4作成
input output
SSigB2 SPubKeyB2
TxID
S8
ビットコインを送金する
トランザクション
ネットワーク30に送信

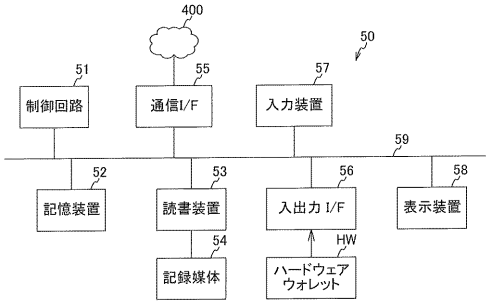
【図５】


取引装置70
取引装置80
取引相手の電子署名A1を生成(Tx1用)
S11
トランザクションTx1作成
input output
SSigA1 SPubKeyB1
TxID
S12
ハッシュ値H
(ネットワーク30に公開)
ネットワーク30に送信
ユーザの電子署名B1を生成(Tx2用)
S13
ユーザの電子署名B2を生成(Tx4用)
S14
トランザクションTx2作成
input output
SSigB1 SPubKeyA1
TxID
S15
ライトコインを送金するトランザクション
ネットワーク40に送信
仮のトランザクションTx4作成
input output
SSigB2 SPubKeyB2
TxID
S16
取引相手の電子署名A2を生成(Tx3用)
S17
トランザクションTx3作成
input output
SSigA2 SPubKeyA2
TxID
S18
秘密の値R
(ネットワーク40に公開)
DB格納
ネットワーク40に送信
DB取り出し
トランザクションTx4作成
input output
SSigB2 SPubKeyB2
TxID
S19
ビットコインを送金するトランザクション
ネットワーク30に送信

【図６】


60
制御部
92
生成部
61
記憶部
作成部
62
送信部
63
93
通知部
64
表示部
91
接続部
受付部
65

【図７】


400
50
51
55
57
制御回路
通信I/F
入力装置
59
52
53
56
58
記憶装置
読書装置
入出力 I/F
表示装置
54
HW
記録媒体
ハードウェアウォレット