(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2019-514089
(P2019-514089A)
(43)公表日　令和1年5月30日(2019.5.30)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 20/40	(2012.01)	G06Q	20/40		5J104
G06Q 30/06	(2012.01)	G06Q	30/06		5L049
H04L 9/32	(2006.01)	H04L	9/00	675Z	5L055

審査請求 有　予備審査請求 未請求　（全 54 頁）

(21)出願番号　特願2018-539915 (P2018-539915)
(86)(22)出願日　平成29年2月16日 (2017.2.16)
(11)特許番号　特許第6511201号 (P6511201)
(45)特許公報発行日　令和1年5月15日 (2019.5.15)
(85)翻訳文提出日　平成30年8月29日 (2018.8.29)
(86)国際出願番号　PCT/IB2017/050865
(87)国際公開番号　WO2017/145019
(87)国際公開日　平成29年8月31日 (2017.8.31)
(31)優先権主張番号　1603123.9
(32)優先日　平成28年2月23日 (2016.2.23)
(33)優先権主張国　英国 (GB)
(31)優先権主張番号　1603125.4
(32)優先日　平成28年2月23日 (2016.2.23)
(33)優先権主張国　英国 (GB)

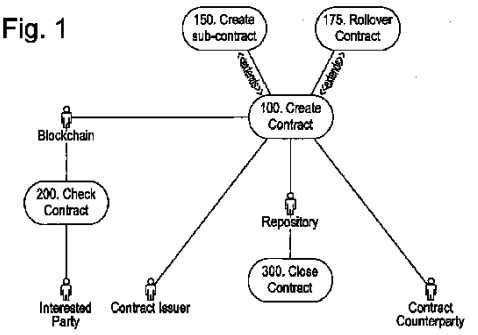
(71)出願人　318001991
エヌチェーン　ホールディングス　リミテッド
NCHAIN HOLDINGS LIMITED
アンティグア・バーブーダ、　セントジョンズ、　４４　チャーチ　ストリート、　フィッツジェラルド　ハウス
Fitzgerald House, 44 Church Street, St. John's, Antigua and Barbuda (AG)
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】ブロックチェーンにより施行される洗練された取引のためのレジストリ及び自動管理方法

(57)【要約】
本発明は、トークン化、ブロックチェーン、及びスマートコントラクト（smart contract）技術の分野に関する。本発明は、取引の自動管理を簡易化する技術的構成を提供する。本発明は、取引の記憶のためのコンピュータに基づくレポジトリを用いる方法及びシステムを含む。取引は、次に、ブロックチェーン上のトランザクションにより表現される。トランザクションのスクリプトの中のメタデータは、取引のハッシュ、及びレポジトリ内の場所を識別する手段を含む。トランザクションは、自身の状態をオープン（つまり、終了していない）取引として示す未使用アウトプット（ＵＴＸＯ）も含む。取引は、後の時点で、例えばｎＬｏｃｋＴｉｍｅ＋ＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ（ＣＬＴＶ）を用いてアウトプットを使用することにより終了される。この概念を他の技術及び計算コンポーネントと組み合わせることにより、本発明は、取引の更新又はロールオーバ、又は取引をサブ取引若しくは条件に分割するような種々のタスクを実施する強力なメカニズムを提供できる。さらに、取引の状態及び存在はブロックチェーンによる証

Fig. 1



【特許請求の範囲】
【請求項１】
取引の可視性及び／又は実行を制御するコンピュータにより実施される方法であって、前記方法は、
（ａ）コンピュータに基づくレポジトリ上に又はその中に取引を格納するステップと、
（ｂ）ブロックチェーンにトランザクションをブロードキャストするステップであって、前記トランザクションは、
ｉ）少なくとも１つの未使用アウトプット（ＵＴＸＯ）、及び、
ｉｉ）前記取引の格納された場所を示す識別子を有するメタデータ、を有する、ステップと、
（ｃ）前記取引を、
前記取引に関連付けられた前のキーに関連するデータを用いて、新しいキーを生成し、
前記新しいキー、前記取引の前記場所、前記取引のハッシュを有するスクリプトを生成し、
前記スクリプトに通貨額を支払う、
ことにより、更新する又はロールオンするステップと、
を含む方法。
【請求項２】
前記トランザクションは、決定性ＲｅｄｅｅｍＳｃｒｉｐｔアドレスを更に有し、望ましくは、前記ＲｅｄｅｅｍＳｃｒｉｐｔアドレスはＰ２ＳＨ（pay－to－script－hash）アドレスである、請求項１に記載の方法。
【請求項３】
前記アウトプット（ＵＴＸＯ）を使用するために前記ブロックチェーンに更なるトランザクションをブロードキャストすることにより、前記取引を終了するステップ、を更に含む請求項２に記載の方法。
【請求項４】
前記更なるトランザクションは、
前記アウトプット（ＵＴＸＯ）であるインプット、及び、
署名と前記メタデータと公開鍵とを含むアンロックスクリプト、を有する、請求項１乃至３のいずれか一項に記載の方法。
【請求項５】
前記取引は、
ｉ）少なくとも１つの条件、及び、
ｉｉ）前記条件の評価に実行が依存する少なくとも１つのアクション、を定める、請求項１乃至４のいずれか一項に記載の方法。
【請求項６】
前記メタデータは、
ｉ）前記取引が前記コンピュータに基づくレポジトリに格納された場所のアドレス又はアドレスの提示、及び／又は、
ｉｉ）前記取引のハッシュ、を有する、請求項１乃至５のいずれか一項に記載の方法。
【請求項７】
前記未使用トランザクションＵＴＸＯが前記ブロックチェーンの未使用トランザクションアウトプットのリストの中にあるか否かを決定することにより、前記取引が終了しているか否かを調べるステップ、を含む請求項１乃至６のいずれか一項に記載の方法。
【請求項８】
前記取引は分散ハッシュテーブル（ＨＤＴ）に格納される、請求項１乃至７のいずれか一項に記載の方法。
【請求項９】
指定日及び／又は時間に前記アウトプットを使用する指示を有するトランザクションを

前記ブロックチェーンにブロードキャストするステップであって、望ましくは前記指示はＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ指示である、ステップ、を含む請求項１乃至８のいずれか一項に記載の方法。

【請求項１０】

前記取引の内容のうちの一部又は全部へのアクセスは、少なくとも１つの指定認定パーティに制限される、請求項１乃至９のいずれか一項に記載の方法。

【請求項１１】

前記取引は、前記取引を実施する決定性有限オートマンを有する、請求項１乃至１０のいずれか一項に記載の方法。

【請求項１２】

前記決定性有限オートマンは、コード化スキームを用いて定められる、請求項１１に記載の方法。

【請求項１３】

前記決定性有限オートマンは、

ｉ）望ましくはスクリプト言語を用いる少なくとも１つのブロックチェーントランザクション、

ｉｉ）前記ブロックチェーンの状態を監視するよう構成された計算エージェント、及び／又は、

ｉｉｉ）デジタルウォレットのための指示セット、

を用いて実施される、請求項１１又は１２に記載の方法。

【請求項１４】

取引の可視性及び／又は実行を制御するコンピュータにより実施される方法であって、前記方法は、

（ａ）コンピュータに基づくレポジトリ上に又はその中に取引を格納するステップと、

（ｂ）ブロックチェーンにトランザクションをブロードキャストするステップであって、前記トランザクションは、

ｉ）少なくとも１つの未使用アウトプット（ＵＴＸＯ）、及び、

ｉｉ）前記取引の格納された場所を示す識別子を有するメタデータ、を有する、ステップと、

（ｃ）前記取引から導出されるサブ取引を生成するステップであって、前記サブ取引は、決定性アドレスに関連付けられ、

ｉｉｉ）シードを用いて導出された新しい公開鍵を用いて、

ｉｖ）前記取引への参照と共に前記レポジトリ上に又はその中に前記サブ取引を格納し、前記参照を含むスクリプトを有するトランザクションを前記ブロックチェーンにブロードキャストし、及び／又は、

ｖ）既存の取引のメタデータに前記サブ取引への参照を追加する、

ことにより生成される、ステップと、

を含む方法。

【請求項１５】

前記トランザクションは、決定性ＲｅｄｅｅｍＳｃｒｉｐｔアドレスを更に有し、望ましくは、前記ＲｅｄｅｅｍＳｃｒｉｐｔアドレスはＰ２ＳＨ（pay－to－script－hash）アドレスである、請求項１４に記載の方法。

【請求項１６】

前記アウトプット（ＵＴＸＯ）を使用するために前記ブロックチェーンに更なるトランザクションをブロードキャストすることにより、前記取引を完了するステップ、を更に含む請求項１５に記載の方法。

【請求項１７】

前記更なるトランザクションは、

前記アウトプット（ＵＴＸＯ）であるインプット、及び、

署名と前記メタデータと公開鍵とを含むアンロックスクリプト、を有する、請求項１４

乃至１６のいずれか一項に記載の方法。
【請求項１８】
前記取引は、
ｉ）少なくとも１つの条件、及び、
ｉｉ）前記条件の評価に実行が依存する少なくとも１つのアクション、を定める、請求項１４乃至１７のいずれか一項に記載の方法。
【請求項１９】
前記メタデータは、
ｉ）前記取引が前記コンピュータに基づくレポジトリに格納された場所のアドレス又はアドレスの提示、及び／又は、
ｉｉ）前記取引のハッシュ、を有する、請求項１４乃至１８のいずれか一項に記載の方法。
【請求項２０】
前記未使用アウトプットＵＴＸＯが前記ブロックチェーンの未使用トランザクションアウトプットのリストの中にあるか否かを決定することにより、前記取引が終了しているか否かを調べるステップ、を含む請求項１４乃至１９のいずれか一項に記載の方法。
【請求項２１】
前記取引は分散ハッシュテーブル（ＨＤＴ）に格納される、請求項１４乃至２０のいずれか一項に記載の方法。
【請求項２２】
指定日及び／又は時間に前記アウトプットを使用する指示を有するトランザクションを前記ブロックチェーンにブロードキャストするステップであって、望ましくは前記指示はＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ指示である、ステップ、を含む請求項１４乃至２１のいずれか一項に記載の方法。
【請求項２３】
前記取引の内容のうちの一部又は全部へのアクセスは、少なくとも１つの指定認定パーティに制限される、請求項１４乃至２２のいずれか一項に記載の方法。
【請求項２４】
前記取引は、前記取引を実施する決定性有限オートマンを有する、請求項１４乃至２３のいずれか一項に記載の方法。
【請求項２５】
前記決定性有限オートマンは、コード化スキームを用いて定められる、請求項２４に記載の方法。
【請求項２６】
前記決定性有限オートマンは、
ｉ）望ましくはスクリプト言語を用いる少なくとも１つのブロックチェーントランザクション、
ｉｉ）前記ブロックチェーンの状態を監視するよう構成された計算エージェント、及び／又は、
ｉｉｉ）デジタルウォレットのための指示セット、
を用いて実施される、請求項２４又は２５に記載の方法。
【請求項２７】
請求項１乃至２６のいずれか一項に記載の方法を実行するよう構成されたシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概して、コンピュータプロトコルに関し、より詳細には、例えば取引に関するような条件制御されたプロセスの検証、施行、及び／又は実行に関する。本発明は、特に、ブロックチェーンネットワークと共に使用することに適し、洗練された取引を促進するために使用できる。

【背景技術】
【０００２】
ブロックチェーンは、不変ブロックにより構成される、非集中型の、分散型コンピュータシステムである。また、不変ブロックはトランザクションにより構成される。各ブロックは前のブロックのハッシュを含み、ブロックは共にチェーンになって、その発端からブロックチェーンに書き込まれている全てのトランザクションのレコードを生成する。トランザクションは、そのインプット及びアウトプットに組み込まれるスクリプトとして知られる小さなプログラムを含む。スクリプトは、トランザクションのアウトプットがどのように及び誰によりアクセス可能かを指定する。各未使用トランザクション（ＵＴＸＯとして参照される）は、新トランザクションへのインプットとして使用可能である。
【０００３】
最も広く知られているブロックチェーン技術の用途はビットコイン台帳であるが、他のブロックチェーンの実装が提案され開発されている。ビットコインは便宜上及び説明を目的として本願明細書において言及されるが、本発明はビットコインのブロックチェーンと共に使用することに限定されず、代替のブロックチェーンの実装が本発明の範囲に含まれることに留意すべきである。
【０００４】
ブロックチェーン技術は、暗号通貨の実装の使用のために知られている。しかしながら、更に近年は、デジタル起業家が、新しいシステムを実装するために、ビットコインの基づく暗号通貨セキュリティシステムの使用、及びブロックチェーンに格納可能なデータの両者を探索し始めている。これらは、限定ではないが、以下を含む：
・メタデータを格納する。
・デジタルトークンを実施する。
・取引を実施する及び管理する。
【０００５】
近年の取引管理に伴う主な問題のうちの１つは、アドホックである傾向があり、手動で維持されている取引のローカルストア及びコピーを伴うことである。結果として、「スマートコントラクト（smart contracts）」として知られるコンピュータプロトコルは、それらが部分的に又は全体的に取引の自動施行又は実行を可能にできるので、注目を集め始めている。スマートコントラクトは、セキュリティ向上及びトランザクションコスト低減のような利益を提供できる。しかしながら、これらの取引が変更できないことを保証することを目的とする既知の技術的ソリューションが存在する一方で、取引の有効性、つまり依然としてオープンか又は終了しているか、を調べるために一般に認められた公の登録所は存在しない。
【０００６】
したがって、取引の存在の公の可視性を制御できるコンピュータにより実施されるメカニズムを提供し、及び自動化方法で（つまり、人間による管理ではなく機械により）取引のような実行に基づく処理を管理し、施行し、及び維持する関連パーティの能力を実現することが望ましい。重要なことに、このメカニズムは、取引の中で定められた動作についての制御条件及びトリガを指定する技術的能力を提供し得る。
【発明の概要】
【０００７】
留意すべきことに、本願明細書に定められ及び記載される本発明は、言葉の正当な意味で、取引と共に使用することに限定されない。取引は、文書、ファイル、又は指定条件下でトリガされ得る動作セットを定める他のメカニズムであって良い。制御条件は、公然と満たされて良い。本発明は、法的又は商業的指向の状況における使用に限定されると考えられるべきではない。用語「取引」は、このような限定的意味に解釈されるべきではない。例えば、取引は、鉄道若しくは航空機又はコンサート会場のチケットであって良く、チケットには、バリアのアンロックを提供するための機械可読バーコードのようなアクセスコードが印刷される。

【０００８】
したがって、添付の請求項に定められるように、本願明細書において発明が提供される。
【０００９】
本発明の態様によると、取引の可視性及び／又は実行を制御するコンピュータにより実施される方法であって、前記方法は、
（ａ）コンピュータに基づくレポジトリ上に又はその中に取引を格納するステップと、
（ｂ）ブロックチェーンにトランザクションをブロードキャストするステップであって、前記トランザクションは、
ｉ）少なくとも１つの未使用アウトプット（ＵＴＸＯ）、及び、
ｉｉ）前記取引の格納された場所を示す識別子を有するメタデータ、を有する、ステップと、
（ｃ）前記取引を、
前記取引に関連付けられた前のキーに関連するデータを用いて、新しいキーを生成し、
前記新しいキー、前記取引の前記場所、前記取引のハッシュを有するスクリプトを生成し、
前記スクリプトに通貨額を支払う、
ことにより、更新する又はロールオンするステップと、
を含む方法が提供される。
【００１０】
取引に関連付けられた前のキーに関連するデータを用いて新しいキーを生成し、新しいキーと取引の場所と取引のハッシュとを含むスクリプトを生成し、及びスクリプトに通貨額を支払うことにより、取引を更新し又はロールオンすることにより、これは、新しいキーが前のキーに関連するので、許可されたパーティが更新又はロールオンされる取引との自身の接続により、確実性又はプライバシの損失を伴わずに、元の取引を閲覧できるという利益をもたらす。更新又はロールオンされる取引に関連付けられたキーは元の取引のキーに関連付けられるので、コンピュータに基づくオフチェーン（つまり、ブロックチェーンの部分を形成しない）レポジトリに取引を格納することにより、確実性又はプライバシの損失を伴わずに、メモリ及び処理容量が削減できるという更なる利益がもたらされる。
【００１１】
「ロールオーバ」の状況では、ＵＴＸＯが使用されて、それを「新しい」ロールオンされる取引に送る。しかしながら、ロック時間の前にアウトプットを使用することにより、したがって取引全体を取り消すことにより、既存の取引を取り消すことが可能であって良い。
【００１２】
本発明は、取引の可視性及び／又は実行を制御するコンピュータにより実施される方法及びシステムを提供できる。「可視性」は、取引の存在及び／又は内容がどのように及び誰に利用可能か又はアクセス可能かを意味し得る。取引は「スマートコントラクト（smart contract）」であって良い。方法は自動スマートコントラクト方法であって良い。これは、取引の存在、有効性、及び／又は実行を監視する処理を自動化する方法であって良い。取引はブロックチェーントランザクションの少なくとも部分の形式で表現できるので、本発明は、トークン化方法／システムとして参照されて良い。トランザクションの中のメタデータは、取引を表現し及び／又はアクセスするために使用される、ブロックチェーンにより実施されるトークンを提供して良い。
【００１３】
本発明は、レポジトリ（記録簿）への取引の記憶を可能にする方法／システムを提供し得る。ここで、取引のハッシュは、取引を見付けるための検索キーとして使用できる。
【００１４】
方法は、

コンピュータに基づくレポジトリ上に又はその中に取引を格納するステップと、
ブロックチェーンへトランザクションをブロードキャストするステップであって、前記トランザクションは、
ｉ）少なくとも１つの未使用アウトプット（ＵＴＸＯ）、及び、
ｉｉ）前記取引の格納された場所を示す識別子を有するメタデータ、を含む、ステップと、
を含んで良い。
【００１５】
取引は、ＵＴＸＯがブロックチェーン上で使用されるまで、公開され又は有効であると解釈されて良い。ブロックチェーンは、ビットコインブロックチェーンであって良く、又はそうでなくて良い。これは、ＵＴＸＯにより表現されるようなブロックチェーン上の取引の状態又は有効性を表現する新規なメカニズムの利益をもたらす。
【００１６】
方法は、オフチェーンのコンピュータにより実施される処理、エージェント、又は他のエンティティを用いて、ブロックチェーンの状態を観察し、及びアウトプットが現在未使用か否かに基づき特定の方法で振る舞うステップを含んで良い。処理は、未使用アウトプットを、取引の状態の指示子として解釈するよう構成されて良い。言い換えると、アウトプットがブロックチェーン上のＵＴＸＯリスト内に残る、つまりトランザクションが未使用のままである間、これは、メタデータにより指される又は参照される取引の有効性又は「公開」状態を示すために使用されて良い。取引は、ＵＴＸＯが使用されると、完了された（終了された）と考えられて良い。この条件は、取引の中で記述されて良い。しかしながら、ＵＴＸＯが使用されると、メタデータは、取引へのポインタ又は参照及び取引のハッシュを含み続けることが可能であるので、取引はその機能を保持できる。
【００１７】
方法は、取引の存在を公表するステップを含んで良い。これは、以下のステップにより達成できる。
・取引発行人は、新しい取引文書を作成し、これをレポジトリに公表する。該文書の格納場所及びセキュアなハッシュが、後の使用のために格納されて良い。
・ｎ人のうちのｍ人のマルチシグネチャ構造で、取引文書がセキュアであることを保証するＲｅｄｅｅｍＳｃｒｉｐｔを生成する。ここで、
－　ｍは少なくとも１であり、
－　ｎはｍとメタデータブロック数の和である。
・少なくとも１つの公開鍵をスクリプトに含める。これは、取引発行人の公開鍵であって良い。しかしながら、他の署名も要求されて良い。
・望ましくはＰ２ＳＨトランザクションを通じて、通貨額、例えばビットコインをスクリプトに支払う。
・トランザクションがブロックチェーンに公表されるまで待機し、公表されたトランザクションのトランザクションＩＤを抽出する。
・ロック時間を取引の有効期限に設定して新しいトランザクションを生成し、トランザクションから公開鍵ハッシュへアウトプットを払い戻す。又は、
ローリング期間取引について、自動計算エージェントを用いて、ブロックチェーン上のトランザクションを検出し、それを新しい取引にローリングするためのコードをトリガする前に取引有効期限まで待機する。又は、
完了に基づく取引について（ここで、ｙ個のエンティティのうちのｘ個のエンティティが、取引が満たされたことに合意する）、ｎ人のうちのｍ人のマルチシグネチャトランザクションを生成し、完了すると共同署名するために、それをこれらのエンティティに発行する。
【００１８】
レポジトリは、オフブロック記憶リソースであって良い。言い換えると、レポジトリは、ブロックチェーン自体の部分を形成しなくて良い。コンピュータに基づくレポジトリは

、サーバであって良く又はそれを含んで良い。レポジトリは、データベース又はコンピュータに基づくリソース上に設けられた他の記憶設備であって良い。レポジトリは、インデックス付けされて良く、検索可能である。レポジトリは、分散ハッシュテーブルを含んで良い。取引は、分散ハッシュテーブル（Distributed Hash Table：ＤＨＴ）の中に又はそれに関連付けられて格納されて良い。

【００１９】

トランザクションは、決定性Ｒｅｄｅｅｍ又はロッキングスクリプトアドレスを更に含んで良い。アドレスは、Ｐ２ＳＨ（pay－to－script－hash）アドレスであって良い。したがって、取引の存在（又は取引の中の定められた要素）は、取引の発行人により決定され又は提供され得るｐａｙ－ｔｏ－ｓｃｒｉｐｔ－ｈａｓｈアドレス、及び／又は取引のメタデータを用いて、ブロックチェーンに公表されるトランザクションを用いて公衆に利用可能にされて良い。

【００２０】

方法は、アウトプット（ＵＴＸＯ）を使用するためにブロックチェーンに（更なる）トランザクションをブロードキャストすることにより、取引を終了するステップ、を更に含んで良い。更なるトランザクションは、アウトプット（ＵＴＸＯ）であるインプット、及び、署名と前記メタデータと公開鍵とを含むアンロックスクリプト、を有して良い。

【００２１】

これは、アウトプットを使用するために、ブロックチェーントランザクションの使用により、取引の自動終了の利益をもたらし得る。

【００２２】

取引は、ｉ）少なくとも１つの条件、ｉｉ）条件の評価に実行が依存する少なくとも１つのアクション、を定めて良い。条件は、真又は偽に評価可能なテストであって良い。条件は、取引（例えば、条項（clause））の部分であって良い。条件の完了又は実行は、取引の達成のために要求されて良い。条件は、真と評価された場合に、完了されて良い。

【００２３】

メタデータは、ｉ）取引がコンピュータに基づくレポジトリに格納された場所のアドレス又はアドレスの提示、及び／又は、ｉｉ）取引のハッシュ、を有して良い。

【００２４】

方法は、ブロックチェーン状態を観察するステップを含んで良い。これは、ＵＴＸＯを含むトランザクションを見付けるためにブロックチェーンを検索するステップを含んで良い。これは、未使用トランザクションＵＴＸＯがブロックチェーンの未使用トランザクションアウトプットのリストの中にあるか否かを決定することにより、取引が終了しているか否かを調べるステップ、を含んで良い。この監視する又は調べる処理は、自動化されて良い。これは、適切にプログラムされたコンピューティングエージェント又はリソースにより実行されて良い。これは、実質的に以下に「本発明と共に使用するための説明のための計算エージェント」と題される章に記載される通りであり得る。エージェントは、ＵＴＸＯの使用又は未使用状態に基づきアクションを実行して良い。したがって、ＵＴＸＯの状態は、オフブロック計算エージェントの振る舞いを制御し又はそれに影響して良い。

【００２５】

方法は、指定日及び／又は時間にアウトプットを使用する指示を含むトランザクションをブロックチェーンにブロードキャストするステップを含んで良い。指示はＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ指示であって良い。

【００２６】

取引の内容の一部又は全部へのアクセスは、少なくとも１つの指定された許可パーティに制限されて良い。言い換えると、取引の一部又は全部にアクセスする又はそれを閲覧するために、許可が必要とされて良い。幾つかの実施形態では、保護メカニズムが取引自体に適用されて良い。例えば、ファイルの１又は複数の部分が保護されて良いが、全体的な内容は公開されて良い。この部分的保護は、取引の中の情報の暗号化、並びに、取引の内容に対する変更を検出するハッシュ、の両方に適用されて良い。

【００２７】
取引は、取引を実施するために決定性有限オートマン（Deterministic Finite Automaton：ＤＦＡ）を有して良い。決定性有限オートマンは、コード化スキームを用いて定められて良い。決定性有限オートマンは、
ｉ）望ましくはスクリプト言語を用いる、少なくとも１つのブロックチェーントランザクション、
ｉｉ）ブロックチェーンの状態を監視するよう構成された計算エージェント（これは、以下の「本発明と共に使用するための説明のための計算エージェント」と題される章に記載され得る）、及び／又は、
ｉｉｉ）デジタルウォレットに対する指示セット、を用いて実施されて良い。
【００２８】
本発明の別の態様によると、取引の可視性及び／又は実行を制御するコンピュータにより実施される方法であって、前記方法は、
（ａ）コンピュータに基づくレポジトリ上に又はその中に取引を格納するステップと、
（ｂ）ブロックチェーンにトランザクションをブロードキャストするステップであって、前記トランザクションは、
ｉ）少なくとも１つの未使用アウトプット（ＵＴＸＯ）、及び、
ｉｉ）前記取引の格納された場所を示す識別子を有するメタデータ、を有する、ステップと、
（ｃ）前記取引から導出されるサブ取引を生成するステップであって、前記サブ取引は、決定性アドレスに関連付けられ、
ｉｉｉ）シードを用いて導出された新しい公開鍵を用いて、
ｉｖ）前記取引への参照と共に前記レポジトリ上に又はその中に前記サブ取引を格納し、前記参照を含むスクリプトを有するトランザクションを前記ブロックチェーンにブロードキャストし、及び／又は、
ｖ）既存の取引のメタデータに前記サブ取引への参照を追加する、
ことにより生成される、ステップと、
を含む方法が提供される。
【００２９】
取引から導出されるサブ取引を生成するステップであって、サブ取引は決定性アドレスに関連付けられ、シードを用いて導出された新しい公開鍵を用いて、取引への参照と共にレポジトリ上に又はその中にサブ取引を格納し、参照を含むスクリプトを有するトランザクションをブロックチェーンにブロードキャストし、及び／又は、既存の取引のメタデータにサブ取引への参照を追加する、ことにより生成される、ステップにより、これは、サブ取引が元の取引に暗号によって結合されるので、確実性又はプライバシの損失を伴わずに、サブ取引が独立に管理可能であるという利点を提供する。さらに、サブ取引をオフブロックレポジトリに格納することにより、メモリ及び処理リソースが最小化できる。
【００３０】
方法は、ブロックチェーンを監視するために及び／又は取引内容に基づきアクションを実行するために、コンピュータに基づくエージェントの使用を含み得る。このようなエージェントは、実質的に以下に「本発明と共に使用するための説明のための計算エージェント」と題される章に記載される通りであり得る。
【００３１】
本発明は、上述の方法ステップのうちのいずれか又は本願明細書に記載の方法の任意の実施形態を実行するよう構成された、コンピュータにより実施されるシステムを更に提供し得る。本発明は、取引の可視性及び／又は実行を制御するコンピュータにより実施されるシステムであって、前記システムは、
取引を格納するよう構成されたコンピュータに基づくレポジトリと、
トランザクションを有するブロックチェーンであって、前記トランザクションは、
ｉ）少なくとも１つのアウトプット（ＵＴＸＯ）、及び、

ｉｉ）前記取引の格納された場所を表す識別子を有するメタデータ、
を有する、ブロックチェーンと、
を含むシステムを提供し得る。
【００３２】
メタデータは、取引のハッシュを更に格納して良い。取引はスマートコントラクト（smart contract）であって良い。
【００３３】
レポジトリは、データベースを有して良い。これは、ＤＨＴを有して良い。これは、インデックス付けされ、検索可能であって良い。これは、取引へのアクセスを制御するために少なくとも１つのセキュリティメカニズムを有して良い。
【００３４】
システムは、的セルに構成された計算に基づくエンティティ又はエージェントを更に有して良い。エージェントは、ブロックチェーンを監視し及び／又は検索するよう構成されて良い。これは、ブロックチェーンの状態に基づき、少なくとも１つのアクションを実行するよう構成されて良い。これは、ＵＴＸＯが使用されたか否かを決定するよう構成されて良い。これは、ＵＴＸＯが使用されたか否かに基づき１又は複数のアクションを実行するよう構成されて良い。
【００３５】
ある実施形態又は態様に関連して本願明細書に記載された任意の特徴は、任意の他の実施形態又は態様に関連して使用されても良い。例えば、方法に関連して記載されて任意の特徴は、システムに関連して使用されて良く、逆も同様である。
【００３６】
本発明により提供され得る利益のうちの幾つかの非限定的リストがここで提供される。
【００３７】
本発明は、ここでは「取引（contracts）」として参照される場合のある構造化制御条件の自動管理を簡略化する技術的構成を提供し得る。これは、また、疑義の生じた場合に、取引の状態に合意することを容易にする。本発明は、取引の有効性のコンピュータによる自動決定を可能にする方法で、取引のセキュアな公開されたレコードを保持し、及び検証により許可エンティティに取引の詳細を公開するメカニズムも提供し得る。したがって、本発明は、知的な方法でリソースへのアクセスを許可し又は禁止する、セキュリティの向上した制御メカニズムを提供し得る。
【００３８】
本発明は、コンピュータシステムを介して聴衆に取引を公表する能力も提供し、取引の詳細が認定エンティティだけに制限可能であるが、取引の存在の知識が公衆に知られるようにする。言い換えると、ＡとＢとの間に取引が存在することを誰もが知ることができ、これは公に検証可能であるが、その存在以外の全ては認定パーティ（標準的にＡ及びＢだけ）に制限される。
【００３９】
これは、取引が時間で制限される（つまり、特定時間後に又は所与の日付で取引が終了する）、条件で制限される（つまり、取引の中で指定された成果物が満たされると、取引が終了する）、又は制限のない（つまり、取引を終了すべき通知期間と共に取引がロールオンし続ける）ことを可能にする、コンピュータにより実施されるメカニズムも提供する。
【００４０】
これは、該取引を公に終了するための通知を提供するメカニズムを提供し得る。例えば、期間終了を「制定する」ために、使用されるトランザクションの中でｎＬｏｃｋＴｉｍｅ＋ＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ（ＣＬＴＶ）を用いる。
【００４１】
これは、区分化されるべき取引の異なる側面に渡る制御を可能にする決定性の方法で、サブ取引の階層を構造化するメカニズムを提供し得る。例えば、技術の発展過程において

、要求段階は、発展段階と異なる制御トリガセットを有することがある。
【００４２】
本発明がブロックチェーンプラットフォーム上で実施され、ブロックチェーンの機能を拡張して、技術的に異なる方法で使用可能になるとき、本発明は改良されたブロックチェーンシステム又はプラットフォームを提供し得る。
【００４３】
本発明は、例えばデジタルアクセスのために、任意の未使用トランザクション（ＵＴＸＯ）をスマートコントラクトにするために使用できる。例えば、消費者がある期間中にサービスにアクセスするために商人に支払うシナリオを考える。商人の支払アドレスがスマートコントラクトとして実施される場合、本発明は、サービスのためのアクセス制御メカニズムを実装するために使用できる。金銭が支払われたこと、及び期間の終了時に商人のアカウントに価値を運び去るために自動化処理が使用されることを保証するために、チェックが行われ得る。
【図面の簡単な説明】
【００４４】
本発明の上述の及び他の態様は、本願明細書に記載される実施形態から明らかであり、それらの実施形態を参照して教示される。本発明の実施形態は、単なる例として添付の図面を参照して以下に説明される。
【図１】種々の取引関連タスクを実施するために、ブロックチェーントランザクションが本発明の実施形態によりどのように使用できるかの概要を示す。
【図２Ａ】２つの状態：（ｉ）取引が開かれている、及び（ｉｉ）取引が閉じられている、を有する単純な状態機械を示す。
【図２Ｂ】図２Ａのシナリオのためのメタデータ定義を示す。メタデータは、（ビットコイン）トランザクションアウトプット上で伝達され、取引場所及び（ハッシュにより）有効性の証明を指定する。
【図２Ｃ】図２Ａ及び２Ｂのシナリオに関連する、最初にブロックチェーン上に取引（のハッシュ）を格納する「発行（issuance）」トランザクションを示す。
【図２Ｄ】ビットコインを使用することにより、図２Ａ～２Ｃの取引を取り消す。
【図３Ａ】隠された所有権を有する資産が生成されブロックチェーンに公表されるシナリオのための説明のためのメタデータを示す。
【図３Ｂ】図３Ａの資産に「資金を供給する」説明のためのトランザクションを示す。つまり、幾つかのビットコインを資産の公開鍵に入れて、資産が（図３Ｃに示す公表トランザクションのような）自身のトランザクションに資金供給するようにする
【図３Ｃ】図３Ａ及び３Ｂの資産の公表のための説明のためのブロックチェーントランザクションを示す。
【図３Ｄ】図３Ａ、Ｂ、及びＣに関連する取引を閉鎖するための説明のためのトランザクションを示す。取引の取り消しが要求されると、ＵＴＸＯが使用される。このシナリオでは、要件は、資産及び署名すべき資産の隠された所有者の両者のためである。
【図４Ａ】賃貸借取引を含むシナリオのための説明のための状態機械モデルを示す。
【図４Ｂ】図４Ａのシナリオのための説明のためのメタデータを示す。
【図４Ｃ】図４Ａ及び４Ｂの資産の所有権をブロックチェーンに公表するための説明のためのトランザクションを示す。
【図５Ａ】取引がロールオンされるシナリオのための説明のための状態機械モデルを示す。
【図５Ｂ】図５Ａのシナリオのための説明のためのメタデータを示す。
【図５Ｃ－１】図５Ａ及び５Ｂの初期取引及び取引の初期ロールオーバをブロックチェーンに公表するために使用され得る説明のためのトランザクションを示す。
【図５Ｃ－２】図５Ａ及び５Ｂの初期取引及び取引の初期ロールオーバをブロックチェーンに公表するために使用され得る説明のためのトランザクションを示す。
【図５Ｄ】図５Ａ～５Ｄの取引の終了のための説明のためのトランザクションを示す。

【図６Ａ】取引条件付けを含むシナリオのための説明のための状態機械モデルである。
【図６Ｂ】図６Ａのシナリオのための説明のためのメタデータを示す。
【図６Ｃ－１】初期取引及び２つのサブ取引を生成し、それらを公表するために使用され得る、説明のためのトランザクションを示す。
【図６Ｃ－２】初期取引及び２つのサブ取引を生成し、それらを公表するために使用され得る、説明のためのトランザクションを示す。
【図６Ｃ－３】初期取引及び２つのサブ取引を生成し、それらを公表するために使用され得る、説明のためのトランザクションを示す。
【図６Ｄ】図６Ａ～６Ｃのシナリオに関連して使用するための説明のためのトランザクションを示す。
【図７】親キーからサブキーを導出する技術の種々の態様を示す。本技術は、本発明の態様と関連して使用することに適する。
【図８】親キーからサブキーを導出する技術の種々の態様を示す。本技術は、本発明の態様と関連して使用することに適する。
【図９】親キーからサブキーを導出する技術の種々の態様を示す。本技術は、本発明の態様と関連して使用することに適する。
【図１０】親キーからサブキーを導出する技術の種々の態様を示す。本技術は、本発明の態様と関連して使用することに適する。
【図１１】親キーからサブキーを導出する技術の種々の態様を示す。本技術は、本発明の態様と関連して使用することに適する。
【図１２】親キーからサブキーを導出する技術の種々の態様を示す。本技術は、本発明の態様と関連して使用することに適する。
【図１３】親キーからサブキーを導出する技術の種々の態様を示す。本技術は、本発明の態様と関連して使用することに適する。
【発明を実施するための形態】
【００４５】
ブロックチェーンに構築されるスマートコントラクトは、ビットコイントランザクションに（つまり、ロック／アンロックスクリプトの中に）直接埋め込まれるロジックを通じて、及び／又は外部のコンピュータに基づくアプリケーションを通じて、施行できる。このような外部のコンピュータに基づくアプリケーションは、「エージェント」、「オラクル」、又は「ボット」として参照される場合がある。さらに、幾つかの取引条件は、ｎＬｏｃｋＴｉｍｅフィールドのような他のビットコイントランザクション要素を通じて施行可能である。
【００４６】
本願明細書に記載される発明では、取引は、取引を表すブロックチェーン上に有効な未使用トランザクションアウトプットＵＴＸＯが存在する限り、事実上残っていると解釈される。この未使用状態は、取引自体の中の条件又は諸規定により振る舞いが制御される種々のメカニズム（例えば、プログラムされた計算エージェント）の結果として影響を受け変更され得ることが理解される。例えば、取引は、該取引が特定日に終了すること、又は該取引が特定値が指定閾に達すると終了することを規定する。
【００４７】
取引を表現するために未使用トランザクションアウトプットを使用するこの原理は、暗号化技術のような他の特徴と組み合わせて使用できる。これは、複雑なシナリオ及び活動の実施を可能にする。事実上、未署名トランザクションアウトプットＵＴＸＯに関するコンテキスト、及び自身を使用可能にするスクリプト内の関連メタデータは、該トランザクションが、取引の正式な詳細を含むオフチェーンレポジトリへのポインタ又は参照として作用することを可能にする。ここで、「オフチェーン」は、ブロックチェーン自体の部分ではないことを意味する。これは、ブロックチェーンを検査することにより取引が終了しているか又は未だ有効／公開されているかを決定するために、誰もがソフトウェアに基づくコンポーネント又はツールを使用できるようにするメカニズムを提供する。取引が終了

すると、これは、トランザクション内の使用済みアウトプットとしてブロックチェーンに記録され、これは公開検査のために利用可能である。ブロックチェーントランザクションは、取引の存在及び現在状態の恒久的、変更不可能、且つ公開されたレコードになる。

【００４８】

レポジトリ（「レジストリ」又は「レジスタ」とも呼ばれる）は、例えば分散ハッシュテーブル（distributed hash table：ＤＨＴ）を含む種々の方法で実装されて良い。取引のハッシュが生成され、メタデータとしてブロックチェーントランザクション内に格納され、ブロックチェーンから取引を参照するための検索キーとして機能できる。取引の場所への参照も、トランザクションメタデータ内で提供される。例えば、レポジトリのＵＲＬが提供されて良い。メタデータが公衆の閲覧に付されている間、取引自体は、部分的に保護されなくて良く又はされて良い。

【００４９】

ＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ（ＣＬＴＶ）のような標準的なビットコインの特徴は、取引が、将来のある時点での正式な自動終了を有することを可能にする。ブロックチェーンの使用は、この終了日をセキュアな（変更不可能な）公開レコードの問題にすることを可能にする。この概念は、以下に記載する複数の暗号鍵の使用と組み合わせて、明示的に取り消されない限り、ＣＬＴＶモデルが取引を自動的にロールオンする又は更新することを可能にする。

【００５０】

決定性サブキーの使用は、本願明細書に記載のトークン化メカニズムと組み合わせて、取引に対してサブ取引又はスケジュールが生成されることを可能にする。

【００５１】

さらに、オフブロック計算エージェント（オラクル）の使用は、取引条件付けが信頼できる第三者により構築され及び偏光されることを可能にする。これは、エージェントのアクションが、取引定義の中で提供される条件（例えば「ＩＦ」ステートメント）により影響され得ることを意味する。

【００５２】

＜主な用語＞

以下の用語が本願明細書で使用され得る。

・取引発行人：

このエンティティは、取引のブロックチェーンへの公表を担う主体を表す。

・関心パーティ：

このエンティティは、特定の取引が未だ場にあるか否かを決定する必要があり得る又は取引の細目を決定する必要があり得る主体を表す。

・レポジトリ：

このエンティティは、ブロックチェーンのスマートコントラクトが参照する取引の構造化表現を安全に保管する／格納する場所を表す。

・取引相手：

このエンティティは、特定取引の相手を表す。多くの場合、このエンティティは存在しないことに留意する。

・取引：

これは、レポジトリ内に格納された構造化文書又はファイルであり、ブロックチェーンから参照される。取引は、任意の種類の取引又は合意であり得る。これは、例えば、金融取引、権利証書、サービス取引、等を含み得る。取引は、その内容の観点で公開又は秘密であり得る。取引は、コード化スキームを用いる構造化方法で表現されるという点で、形式化される。

【００５３】

＜取引モデル＞

取引モデルの基本要素は以下の通りである：

・コード化スキームは、任意の種類の取引の完全な記述を可能にする。スキームは、新し

い構成であって良く、又はＸＢＲＬ、ＸＭＬ、ＪＳＯＮ（等）のような既存の設備を使用して良い。
・取引を実施するためのＤＦＡ（決定性有限オートマン、Deterministic Finite Automaton）は、コード化スキームの中で完全に定義できる。これは、以下から構成される。
－　パラメータのセット、これのパラメータを供給すべき場所、
－　状態定義のセット、
－　遷移のトリガ及び遷移中に従うルールを含む、状態間の遷移のセット、
－　ルール定義テーブル。
・取引のこのインスタンスのための特定パラメータの定義。
・取引を安全に保管し保護するためのメカニズム。
・取引を、正式な法律の言語で人間に可読にする「ブラウザ」。
・コード化スキームをオラクルコード及び／又はビットコインスクリプトのようなスクリプトに変換する「コンパイラ」。
【００５４】
＜取引の実施＞
取引がレポジトリに登録されると、関連アドレス、例えばＵＲＬ及びハッシュは、チェーン上のトランザクションを制御トランザクション自体に関連付けるために、ブロックチェーントランザクション内のメタデータとして使用可能である。これは、種々の形式で実施できるが、適切なコード化スキームは、完全のために以下の「コード化スキーム」と題された章で提供される。
【００５５】
取引定義に含まれるＤＦＡがどのように実施できるかに関する多数の異なる方法が存在する。
・ブロックチェーントランザクション又はトランザクションシーケンスとして。種々の形式のＤＦＡが、ビットコインスクリプト言語の中で直接実施されて良い。当業者はこれを理解し、本発明はＤＦＡがブロックチェーントランザクションにより実施される方法に関して限定されない。
・エージェントに基づく（例えば、オラクル）プロセス又はプロセスシーケンスとして。以下の「本発明と共に使用するための説明のための計算エージェント」と題された章は、ブロックチェーン及び可能な他の外部ソースを監視するために適切なエージェントを定義し及び実行する基本処理を記載する。
・スマートウォレットに対する指示セットとして。この内容では、スマートウォレットは、トランザクションインプットのブロックチェーントランザクションへの割り当てのような特定取引条件を処理可能なローカルなオラクル処理を事実上簡略化する。
【００５６】
所与の取引定義は、上述の３つのメカニズムの混合として実施でき、各取引状態トランザクションは事実上別個の実施であることに留意する。
【００５７】
関連トランザクション／コードを手作業で作ることを含む、取引定義から実施を生成する多数の方法が存在する。
【００５８】
＜取引の存在の公表＞
取引の存在（又は取引の中の定義された要素）を公表するために、トランザクションＴｘは、ｐａｙ－ｔｏ－ｓｃｒｉｐｔ－ｈａｓｈ（Ｐ２ＳＨ）アドレスを用いてブロックチェーンに公表される。Ｐ２ＳＨトランザクションは、トランザクションが送信されるために、受け手が、スクリプトハッシュに適合するスクリプト、及びスクリプト評価を真にマークするデータを提供しなければならないものである。本発明の実施形態に関連して、ｐａｙ－ｔｏ－ｓｃｒｉｐｔ－ｈａｓｈ（Ｐ２ＳＨ）は、直ちに以下から決定できる。
－　取引の発行人、及び、
－　取引のメタデータ。

【００５９】
本発明の幾つかの実施形態に従い、未使用トランザクションは、取引状態の指示子として解釈できる。オフチェーン処理は、ブロックチェーンを監視し、アウトプットが未使用か否かに基づき特定方法で振る舞うよう構成され得る。言い換えると、このアウトプットがブロックチェーン上のＵＴＸＯリスト内に残る（つまりトランザクションが未使用のままである）間、これは、メタデータにより指される又は参照される取引の有効性を示す。取引は、このアウトプットが使用されると、完了されたと考えられる。ＵＴＸＯが存在する限り（取引が有効／公開されたままである）この状態は、取引自体の状態であり得る。しかしながら、他の実施形態では代替の終了条件が適切な場合があるので、これはプロトコルの必須規定ではない。トランザクションが使用された後でも（したがって、ＵＴＸＯリストの中にもはや存在しない）、該トランザクションは永久にブロックチェーン上に存在したままであり、取引へのポインタ又は参照、及び取引のハッシュを保持したままである。したがって、使用された後でもトランザクションはその機能を保持し得る。
【００６０】
＜サブ取引／条件＞
サブ取引は、既存取引に直接関連する取引である。条件は、取引条件に適合するために満たされなければならない、既存取引の中の条項（clause）である。
【００６１】
本発明の実施形態に従い、サブ取引及び条件の両者は、同じ方法で、つまり決定性ｒｅｄｅｅｍスクリプトアドレスを有するＵＴＸＯとして実装される取引として、実施できる。両方の場合に、エンティティは、ＵＴＸＯが使用されるとき完了すると解釈できる（ある条件の場合には、これは、該条件が満足されていることを示す）。上述のように、メタデータは、レポジトリ内のエンティティの場所へのポインタ又は参照、及びそのハッシュも依然として含む。したがって、他の実施形態では、取引上指定された条件に依存して、アウトプットが使用された後でも、サブ取引又は条件は存在したままであり、及び機能を保持したままであって良い。
【００６２】
条件又はサブ取引の決定性アドレスを生成するために使用可能な多数のメカニズムが存在する。
－　シード情報を用いて新しい公開鍵を導出する。
－　レポジトリ内にあるマスタ取引への参照と有し、これをメタデータ参照として使用する、サブ取引を生成し公表する。
－　既存取引のメタデータへの参照を条件／サブ取引に追加する。
【００６３】
＜取引の安全な保管＞
取引の正式表現（つまり、取引内容を指定する文書又はファイル）は、特定取引の正式な必要に依存して種々の方法で安全に保管され得る。しかしながら、全ての場合に、取引の存在の公開レコードが、メタデータレコードに含まれるブロックチェーンに公表される（特定のメタデータ構造の詳細については「コード化スキーム」と題された章を参照する）。
【００６４】
このブロックチェーンレコードから、認定エンティティは、トランザクションが公表されてから正式表現が変更されていないことを決定するためのハッシュと一緒に、正式表現の場所を知ることができる。
【００６５】
しかしながら、多数の方法を通じて正式表現自体を更に安全に保管することが可能である。
－　文書レポジトリ自体が、アクセス制御メカニズムを提示可能である。
－　取引自体が、関連復号鍵へのアクセスを有するこれらのエンティティへのアクセスを制限する標準的な暗号化技術を通じて安全に保管できる。

【００６６】
多くの場合、取引自体は、取引について部分的保護を有する。例えば、ファイル内の幾つかのセクションは保護されて良く、一方で、全体的内容は公開される。例えば、固定利率ローンをどのように実施するかの詳細は公開されるが、そのローンを誰が、いくら、及びどんな率で組んだかという知識は取引パーティにだけ知られる。
【００６７】
この部分的保護は、取引の中の情報の暗号化、並びに、取引の内容に対する変更を検出するハッシュ、の両方に適用される。
【００６８】
多数の取引について、取引の詳細はその寿命に渡り変更され得る。これは、取引自体の再発行を要求すべきではない。これは、取引のサブセットに渡るハッシュの範囲を決定することにより達成できる。これが有用であり得る一例は、契約型投資信託の実施においてである。契約型投資信託を支える取引は変化してはならないが、構成単位の受益者は取引の売りを通じて変更され得る。一実施形態では、変化の記録は、サブ取引を用いて達成できる。
【００６９】
＜取引の終了＞
ブロックチェーンは永久的な変更不可能なトランザクションのレコードを提供するので、取引は、単に関連する取引文書を削除することにより終了できない。これは、セキュアな取引レポジトリが、多数の標準的メカニズムを通じてサポートされるブロックチェーン自体と同じ記憶装置及び維持ルールを有しなければならないことを意味する。これは、ソリューションが、ブロックチェーンレコードを通じて直接に取引の終了を検出するメカニズムを提示しなければならないことを意味する。
【００７０】
終了の方法は、取引の中の条件として定められ、様々な方法で施行できる。これらの方法の全部は、本発明により概念的にカバーされる。本発明の好適な実施形態では、終了は、取引を表すＵＴＸＯの使用を通じて取り扱われる。
【００７１】
多数の取引種類について、取引の終了は、取引自体の公開と同時に公表され得る。実際上、２つのトランザクションが生成される。第１トランザクションは、取引を公表し、取引を表すトランザクションアウトプットを得るためである。第２トランザクションは、該アウトプットを使用するためである。この第２トランザクションは、所与の将来の日（取引の終わりを表す）にアウトプットを使用するために該トランザクションに設定されたＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙを有する。
【００７２】
上述のように、これは私達の標準的方法であるが、唯一の方法ではない。
【００７３】
この自動使用は、取引のロールリングオンをサポートするために拡張できる（例えば、取引が取り消されない場合、該取引は更に１２ヶ月の間、自動的に延長される）。この状況では、ＵＴＸＯが使用されて、それを「新しい」ロールオンされる取引に送る。しかしながら、ロック時間の前にアウトプットを使用することにより、したがって取引全体を取り消すことにより、古い取引を取り消すことが可能である。
【００７４】
＜使用例モデル＞
図１は、本発明の実施形態による使用例モデルの概観を示す。この説明のための使用例モデルは、ビットコインスクリプト内のＤＦＡの要素を直接実施するために、標準的なビットコイントランザクションがどのように使用できるかを示す。主要な使用例の例が、説明を目的としてここに提供される。
【００７５】
＜取引の生成＞

取引発行人（本例では１次主体である）は、一般的可視性のためにブロックチェーンに取引を公表したいと望む。この処理は、表１に概略を示される。

【表１】

ｽﾃｯﾌﾟ	詳細
100.10	取引発行人は、新しい取引文書を生成し、これをレポジトリに公表して、将来の使用のために該文書の格納場所及びセキュアなハッシュを格納する。このレポジトリは、取引文書自体の特性に依存して、公開、秘密、又は半秘密であり得ることに留意する。レポジトリは、様々な属性により検索できるように、インデックス付けされる。
100.20	取引発行人は、ｎ人のうちのｍ人のマルチシグネチャ構造で、セキュアである取引文書をカバーするＲｅｄｅｅｍＳｃｒｉｐｔを生成する。 ・ｍは少なくとも１であり、 ・ｎはｍとメタデータブロック数の和である（これは少なくとも２である） このスクリプトに常に供給されなければならない１つの公開鍵は、取引発行人の公開鍵である。しかしながら、取引の条項に依存して、他の署名も要求されて良い。
100.30	取引発行人は、標準的なＰ２ＳＨトランザクションを通じて、正規通貨額、例えばビットコインを、ステップ１００．２０で計算したＲｅｄｅｅｍＳｃｒｉｐｔに支払う。
100.40	取引発行人は、トランザクションがブロックチェーン上に公表されるまで待機し、公表されたトランザクションのトランザクションＩＤを抽出する。
100.50	固定期間取引では、取引発行人は、次に、ロック時間が取引の終了時間に設定された新しいトランザクションを生成し、ステップ１００．４０からのアウトプットを取引発行人の公開鍵ハッシュに払い戻す。 ローリング期間取引では、コンピュータに基づくエージェントは、トランザクションを取り上げ、該トランザクションを取引にローリングするために以下の表３の「ロールオーバ」使用例をトリガする前に、取引終了時間まで待機する。 完了に基づく取引では（ｙ個のうちのｘ個のエンティティが、取引が満たされていることに合意する）、ｎ人のうちのｍ人のマルチシグネチャトランザクションが生成され、完了により共同署名するために、これらのエンティティに発行される。

以下に詳述される、２つの主要な実施形態又は本シナリオの変形が存在する。

・既存取引からサブ取引を生成する。

・既存取引を新しい取引へロールオーバする（既存取引を更新する）。

【００７６】

＜サブ取引の生成＞

この状況では、取引発行人は、既存取引からサブ取引を生成したいと望む。この処理は、表２に概略を示される。

【表２】

ステップ	詳細
150.10	取引発行人は、親取引からのサブキー情報の導出において、シード値を用いて親取引を生成するために使用した彼らの公開鍵から新しいサブキーを生成する。これは、取引発行人が望む（及び取り組んでいた）任意の導出であり得るが、適切なシードの例は以下を含み得る。 ・トランザクションＩＤ／ステップ１００．４０で生成された取引ＵＴＸＯのインデックス、又は、 ・ステップ１００．２０で生成されたＲｅｄｅｅｍＳｃｒｉｐｔ。 留意すべきことに、本例は上述の公開鍵が取引発行人の公開鍵であることを想定しているが、当業者は、これが導出されるサブキー（つまり、サブ取引のサブ取引）であることを妨げないことを理解する。
150.20	生成されているサブ取引の特性に依存して、取引発行人は、以下の何れかを行う： ・マスタ取引文書の場所及びハッシュを使用する、又は、 ・マスタへのリンクを埋め込まれた新しい取引文書を生成し、後の使用のために該文書の場所及び該文書のセキュアなハッシュを格納するする、又は、 ・マスタへのリンク及びカバーされる元の取引文書からのフィールドのリストを埋め込まれた新しい取引文書を生成する。事実上、これは、元の情報を複製するのではなく、このサブ取引が別の文書の特定セクションをカバーすることを指定する文書である。 このレポジトリは、取引文書自体の特性に依存して、公開、秘密、又は半秘密であり得ることに留意する。
150.30	取引発行人は、ｎ人のうちのｍ人のマルチシグネチャ構造で、取引文書がセキュアであることをカバーするＲｅｄｅｅｍＳｃｒｉｐｔを生成し、 ・ｍは少なくとも１であり、及び、 ・ｎはｍとメタデータブロック数の和である（これは少なくとも２である）。 このスクリプトに常に供給されなければならない１つの公開鍵は、取引発行人の公開鍵である。しかし、取引の条項に依存して、他の署名も要求されて良い。
150.40	取引発行人は、名目上通貨額、例えばビットコインを、標準的なＰ２ＳＨ（pay-to-script-hash）トランザクションを通じて、ステップ１５０．３０で計算されたＲｅｄｅｅｍＳｃｒｉｐｔに支払う。
150.50	取引発行人は、トランザクションがブロックチェーン上に公表されるまで待機し、公表されたトランザクションのトランザクションＩＤを抽出する。
150.60	固定期間サブ取引では、取引発行人は、次に、ロック時間が取引の終了時間に設定された新しいトランザクションを生成し、ステップ１５０．５０からのアウトプットを取引発行人の公開鍵ハッシュに払い戻す。

１又は複数の実施形態によると、サブ取引は独立に監視されて良い。例えば、測量士からの承認の要求される不動産建造取引を検討する。取引は「subject to sign－off by <x>」と記載する。これを実施するために、ステップ１５０．６０が生成され、署名すべき＜ｘ＞へ巡回させられる。ＲｅｐａｙＳｃｒｉｐｔは、時間制限されていないが、要求される署名者が＜ｘ＞であるｎ人のうちのｍ人のマルチシグネチャ要素として生成される。幾つかの実施形態では、トランザクションは、２つのアウトプット：＜ｘ＞への手数料、及びステップ１５０．５０で生成されたＵＴＸＯの支払、を有する。

【００７７】

＜例示的な使用例：既存取引のロールオーバ＞

本使用例では、取引発行人は、既存取引を新しい取引にロールオーバしたいと望む。表３に説明のための処理が提供される。

【表３】

ステップ	詳細
175.10	取引発行人は、ブロックチェーンを調べ、前のＵＴＸＯが使用されているか否かを検証することにより、取引が取り消されているか否かを決定する。使用されている場合、処理は終了する。
175.20	取引発行人は、親取引を生成するために使用した彼らの公開鍵から新しいサブキーを生成し、親取引シーケンスからのサブキー情報の導出において新しいサブキーをシード値として使用する。これは、取引発行人の望む（及び取り組んでいた）任意の決定性導出であるが、以下であり得る： ・シーケンス番号（例えば、ロールオーバされたインスタンス「１」）、又は、 ・ロールオーバされた取引のデータ範囲。 以上は、上述の公開鍵が取引発行人の公開鍵であることを想定しているが、実際には、これが導出されたサブキー（つまりサブ取引のサブ取引）であることを妨げない。 サブキーをどのように生成するかの例については、「サブキー生成の方法」と題された章を参照する。
175.30	取引発行人は、既存取引文書の場所及びハッシュを取り入れる。 このレポジトリは、取引文書自体の特性に依存して、公開、秘密、又は半秘密であり得る。
175.40	取引発行人は、ｎ人のうちのｍ人のマルチシグネチャ構造で、セキュアである取引文書をカバーするＲｅｄｅｅｍＳｃｒｉｐｔを生成する。ここで、 ・ｍは少なくとも１であり、及び、 ・ｎはｍとメタデータブロック数の和である（これは少なくとも２である）。 本スクリプトに常に供給されなければならない２つの公開鍵は、取引発行人及び顧客のものである。しかしながら、取引の条項に依存して、他の署名も要求されて良い。
175.50	取引発行人は、名目上ビットコイン額を、標準的なＰ２ＳＨトランザクションを通じてステップ１７５．４０で計算されたＲｅｄｅｅｍＳｃｒｉｐｔに支払う。
175.60	取引発行人は、トランザクションがブロックチェーン上に公表されるまで待機し、公表されたトランザクションのトランザクションＩＤを抽出する。
175.70	（ボット又はオラクルに基づく実施のような）処理は、トランザクションを取り上げ、トランザクションが取り消されていない場合に、トランザクションを再びロールオンするために表３の「ロールオーバ」処理を再トリガする前に、取引終了時間まで待機する。

＜例：取引のチェック＞

本使用例では、関心パーティが、彼（彼女）の問い合わせている活動をカバーする取引が存在することを確認したいと望む。このような処理は、表４に示される。

【表４】

ステップ	詳細
200.10	関心パーティは、ブロックチェーンを調べて、彼らの関心のある取引に関連するＵＴＸＯが使用されたか否かを確認する。ＵＴＸＯが未だ未使用である場合、取引は有効のままである。ＵＴＸＯが未だ未使用であるが、保留中のロック時間トランザクションが存在する場合、これは、取引の終了時間を決定する。ＵＴＸＯが使用された場合、ある面では取引は完了している。

上述の主な変化は、関心パーティが、何らかのルートを通じて取引を支配するトランザクションに気付いていることを想定している（通常、関心パーティが取引発行人又は取引相手である場合である）。しかしながら、取引文書及び取引発行人の知識へのアクセスを有する任意のエンティティは、以下によりチェックできる：

・ＵＴＸＯトランザクションのＲｅｄｅｅｍＳｃｒｉｐｔを導出する、及び、
・ＲｅｄｅｅｍＳｃｒｉｐｔハッシュに適合するＵＴＸＯを見付けるためにブロックチェーンをスキャンする。

【００７８】

＜例：取引の終了＞

この使用例では、取引発行人又は取引相手は、既存取引を閉じたいと望む。この処理は、表５に概略を示される。

【表５】

ｽﾃｯﾌﾟ	詳細
300.10	閉鎖の扇動者は、ブロックチェーンを調べて、前のＵＴＸＯが使用されたか否かを検証することにより、取引がキャンセルされているか否かを決定する。使用されている場合、取引は既に閉じられているので、処理は終了する。
300.20	既存の閉鎖トランザクションが存在する場合、扇動者は単にこのトランザクションに署名して、ブロックチェーンに提出するだけである。
300.30	既存の閉鎖トランザクションが存在しない場合、扇動者は、最後の取引のＵＴＸＯであるトランザクションインプット、及び彼らの署名であるアンロックスクリプトを有するトランザクション、取引に関連付けられたメタデータ、及び彼らの公開鍵を生成する。
300.40	トランザクションがブロックチェーンに受け付けられた時点で、取引が閉じられたことが一般に知られる（しかしながら、参加者だけが特定の理由を知っている）。

＜取引条件＞

上述と同じメカニズムが、チェックポイントのような所与の取引の中の条件を監視するために使用できる。例えば、取引が１００ＢＴＣの価値であると決定され、２０ＢＴＣがチェックポイント１～５で支払われるべきである場合、上述のサブ取引モデルは、マスタ取引及び５個のサブ取引を導出するために使用できる。これらのサブ取引の各々は、（例えば公証人、又は同様の者のような）同じ又は異なる署名者を用いて完了としてマークできる。この方法では、公開レコードが維持でき、取引に付属する条件が満たされたことを示す。次に、この概念を、処理、又は取引が完了としてマークされると２０ＢＴＣの支払をトリガするために使用可能なアプリケーション（「ボット」）と組み合わせることが可能である。

【００７９】

説明を目的として、本発明が使用され得るアプリケーションのうちの幾つかを示す幾つかの例示的なシナリオが以下に提供される。これらのシナリオの全てで、取引自体の内容は、無関係且つ非限定的であると考えられる。

【００８０】

＜例示的シナリオ１：資産の公開レジストリ＞

本シナリオでは、ボブは、彼の資産（例えば、彼の家）所有権をブロックチェーンに公表することを決定する。この段階で他に行うことはない。次に後続のトランザクションで使用され得るものは単に資産である。この状況では、取引について終了日は存在しない。図２Ａは、２つの状態：（ｉ）取引が開かれている、及び（ｉｉ）取引が閉じられている、を有する単純な状態機械を示す。図２Ｂは、ビットコイントランザクションアウトプット上で伝達され、取引場所及び（ハッシュにより）有効性の証明を指定する、メタデータ定義を示す。図２Ｃは、ブロックチェーンに取引を最初に格納した「発行」トランザクションを示す（しかしながら、これは実際には、実際の取引ではなく、ハッシュを格納するだけである）。図２Ｄは、ビットコインを使用することにより取引を取り消す。

【００８１】

＜例示的シナリオ２：隠された所有権を有する資産の生成及びレジストリ＞

これは、シナリオ１の僅かに拡張されたバージョンであり、ボブは、ブロックチェーン

に資産を公表したいと望むが、彼の所有権を直接明かすことを望まない。
【００８２】
この状況では、ボブは、先ず、資産を表現するために、彼の公開鍵からサブキーを生成する。このサブキーは、次に、資産の詳細の部分としてブロックチェーン上で公開される。ここでも、この状況では、資産について終了日は存在しない。（詳細な例は、サブキーが生成され得る１つの方法について以下に提供される。「サブキー生成の方法」と題された以下の章を参照する。）
本シナリオの状態機械は、図２Ａに示すようなシナリオ１の状態機械と同じである。図３Ａは、本シナリオのためのメタデータ定義を示す。メタデータは、ビットコイントランザクションアウトプット上で伝達され、取引場所及び（ハッシュにより）有効性の証明を指定する。図３Ｂは、アセットに「資金を供給する」ためのトランザクションを示す。つまり、幾つかのビットコインを資産の公開鍵に入れて、資産が（図３Ｃに示す公開トランザクションのような）自身のトランザクションに資金供給できるようにする。図３Ｂは、ビットコイントランザクションではないので、ボブによる資産サブキーの生成を示さない。
【００８３】
図３Ｃは、資産の公開のためのブロックチェーントランザクションを示す。図３Ｄは、取引の閉鎖のためのトランザクションを示す。取引の取り消しが要求されると、ＵＴＸＯが使用される。この状況では、要件は、資産及び署名すべき資産の隠された所有者の両者のためである。
【００８４】
＜例示的シナリオ３：賃貸借取引＞
この説明のための状況では、ボブは、３年間の固定期間の間、イブと賃貸借取引を組む。取引の条項は、支払数を指定する。支払の詳細は、本発明に関して関係ない。しかしながら、取引は破棄条項を有しない固定条項を有する。
【００８５】
これは、図４Ａに示すような単純な状態機械モデルを有する。図４Ｂは、本シナリオのためのメタデータを示す。図４Ｃは、資産の所有権をブロックチェーン上で公表するためのトランザクションを示す。先ず、ボブが資産に何らかの資金を供給し、次に、資産が自身を公表する。
【００８６】
＜例示的シナリオ４：取引のローリング＞
この説明のための状況では、ボブは、ローリング年率ベースでイブから家を借りることを決定する。ここで、彼は、更新日に賃貸借を取り消すために２ヶ月前に通知を提供する必要がある。その他の場合には、自動継続される。これは、図５Ａに示すような単純な状態機械モデルを有する。図５Ｂは、本シナリオのためのメタデータを示す。図５Ｃは、初期取引及び取引の初期ロールオーバをブロックチェーン上に公表するためのトランザクションを示す。
【００８７】
最初の年の後に、ボブは、賃貸借を継続し、終了しない。ＥＶＥ－Ｓ３－Ｔ２は公表された直後に、自動計算エージェントにより取り上げられ、もう１年継続される。留意すべきことに、これはイブ自身の内部ロジックを用いてイブにより行われることも可能である。
【００８８】
２年目の後に、ボブは、賃貸借を終了することを選択し、ＥＶＥ－Ｓ３－Ｔ３と同じインプットを用いてトランザクションを提出する。しかしながら、このトランザクションは未だ提出されていないので、インプットは未使用であり、ボブのトランザクションが最初にブロックチェーン上に公表された場合、ＥＶＥ－Ｓ３－Ｔ３を無効にしてしまう。含まれる額は些細であるが、ボットは、アウトプットがイブの公開鍵ハッシュに向けられない限り（又は取引が実際に何を記載しても）、トランザクションに連署しない。ボブの取引

の終了のためのトランザクションは図５Ｄに示される。
【００８９】
＜例示的シナリオ５：取引条件付き＞
この説明のための状況では、ボブは、新しい不動産を供給するために建築業者のプールと契約に入り、独立した承認を必要とする取引の中の多数の条件を指定する（第１条件は、ローカルの計画当局からの計画の認可である）。これは、図６Ａに示すような単純な状態機械モデルを有する。図６Ｂは、本シナリオのためのメタデータを示す。図６Ｃは、ボブが、（場合によっては後述するサブキー生成技術を用いて、間ｒねんサブキーを導出した後に）初期取引及び２つのサブ取引を生成し、それらを公表するトランザクションを示す。図６Ｄは、計画許可が承認されるときのためのトランザクションを示す。
【００９０】
＜コード化スキーム＞
取引を参照するために使用されるメタデータは、様々な方法でフォーマット化できる。しかしながら、適切なコード化スキームがここに記載される。
【００９１】
取引の定める権利が取引の保持者又は所有者に贈与される場合、取引は転送可能である。非転送可能取引の一例は、参加者が指名される取引である。つまり、権利が、取引の保持者ではなく特定の指名されたエンティティに贈与される。転送可能取引だけが、このコード化スキームで議論される。
【００９２】
トークンは、取引により贈与される権利を詳述する又は定める特定取引を表す。本発明に従い、トークンは、ビットコイントランザクションの形式の取引の表現である。
【００９３】
このコード化方法は、３つのパラメータ又はデータアイテムを有するメタデータを使用する。このデータは、以下を示し得る：
ｉ）取引の下で利用可能な株（share、持分）の量
（これは、本願明細書で「ＮｕｍＳｈａｒｅｓ」と呼ばれることがある）、
ｉｉ）送り手から少なくとも１つの受け手へ転送されるべき転送単位の量（これは、「ＳｈａｒｅＶａｌ」と呼ばれることがある）、
ｉｉｉ）転送単位の量の値を計算するための因子（これは、「ペギングレート（pegging rate）」と呼ばれることがある）。
【００９４】
このコード化スキームの利点は、上述の３つのパラメータだけを用いて、ブロックチェーン上のトークンとして取引をカプセル化又は表現するために使用できることである。実際に、取引は、これらの３つのデータアイテムのうちの最小限を用いて指定できる。このコード化スキームは任意の種類の転送可能取引のために使用可能なので、共通アルゴリズムが考案され適用され得る。これらのメタデータアイテムの更なる詳細は、以下に提供される。
【００９５】
分割可能トークンは、トランザクションアウトプット上の値が、複数のトークンに渡り（つまり、複数のトランザクションに渡り）割り当てられるより小さな量に細分化され得るものである。典型は、トークン化されたフィアット通貨である。分割可能取引は、非ゼロペギングレート（PeggingRate）を指定する取引として定められる。分割可能取引では、トランザクションアウトプットの中で転送されるトークン化された値は、ペギングレートにより基礎ビットコイン（bitcoin：ＢＴＣ）値に結び付けられる。つまり、取引ａｈ、ペギングレートの観点で、保持者の権利を指定する。非分割可能トークンでは、ペギングレートが存在せず、取引は、固定値の観点で、保持者の権利を指定する（例えば、「この取引は、正確に＄１０００で換金できる」という無記名債券、又は「この取引は１ヘアカットと交換可能である」という商品引換券のように）。非」分割可能取引では、基礎トランザクションＢＴＣ値は取引値と無関係である。

【００９６】
表現「基礎ＢＴＣ値」は、トランザクションアウトプットに付加されるビットコイン額（ＢＴＣ）を表す。ビットコインプロトコルでは、各トランザクションアウトプットは、有効と考えられる非ゼロＢＴＣ額を有しなければならない。実際には、ＢＴＣ額は、記述時に現在５４６サトシに設定される設定最小値（「ダスト（dust）」）より大きくなければならい。１ビットコインは、１００百万サトシに等しいと定められる。ビットコイントランザクションは本願明細書では所有権の交換を助ける手段としてのみ使用されるので、実際の基礎ＢＴＣ額は任意である。真の値は、取引仕様の中にある。理論上、全てのトークンは、ダストにより伝達され得る。

【００９７】
本発明のコード化スキームに従い、具体的に、分割可能トークンでは、基礎ＢＴＣ値は次の意味：ペギングレートにより取引値との関係を運ぶ、を有する。ペギングレートは、それ自体任意であり、基礎ＢＴＣ額を小さく保つために選択される。単にダストを有する基礎となる各トークントランザクションではなく、ペギングレートを使用する理由は、本発明のプロトコルが可視性を実現するからである。トークンが幾つかの小さな額のトランザクションアウトプットに分けられるとき、元の取引を調整する必要がない。むしろ、各細分化トークンの取引値は、単に、ペギングレート及び基礎ＢＴＣ値の細分化された額に基づき計算される。

【００９８】
限定トークンは、ＮｕｍＳｈａｒｅｓと呼ばれる量により定められる固定非ゼロの株数により合計発行値が固定された（又は「限定された」）トークンである。したがって、限定取引の下では更なる株は発行されない。例えば、競走馬の共同所有権のための取引は、競走馬の１００％に限定される（例えば、それぞれ１％で１００個の株、又はそれぞれ１０％で１０個の株、等）。非限定取引は、例えば要求額のフィアット通貨を彼らの引当金（Reserve Account）に追加することにより、発行人が株の更なる発行を引き受け可能であることを意味する。ＮｕｍＳｈａｒｅｓは、全ての取引に明示的に記載されなければならない。限定取引は、ＮｕｍＳｈａｒｅｓ＞０を有しなければならない。非限定取引は、ＮｕｍＳｈａｒｅｓ＝０を設定することにより示される。

【００９９】
典型的な例は、準備預金口座に保持される合計値が存在する約束手形（つまり未償還トークン）の合計値に一致するようにする、通貨準備（金準備と類似する）である。この概念は、通貨準備を超えて、在庫ストックにまで拡大する。例えば、認可印刷Ｔシャツトークンの発行人は、１０，０００枚のＴシャツの在庫で開始して良く、これらの１０，０００枚のＴシャツを表す分割可能トークンを発行して良い（ここで、各株＝１枚のＴシャツを表す）。元のトークンは細分化でき、各細分化トークンは、ペギングレートにより定められるトランザクションアウトプットの基礎ＢＴＣ値に従い、Ｔシャツの枚数に償還可能である。しかしながら、需要が増大する場合、発行人は更なる株を発行することを決定して良い（つまり、更に１０，０００枚だけ流通株数を増大する）。このような場合には、更なる発行を引き受けるために、発行人の準備口座（つまり、在庫倉庫）に更に１０，０００枚のＴシャツを預けることが、発行人の義務である。したがって、在庫にあるＴシャツの合計枚数は、常に、合計未償還株数である（ここで、在庫は「準備口座」として作用する）。

【０１００】
ペギングレートは、分割可能取引にのみ適用される。ここで、（ＳｈａｒｅＶａｌと呼ばれる量により表される）株の値は、基礎ＢＴＣ額に固定される。例えば、取引は、発行人が基礎１ＢＴＣ毎に＄１０，０００のレートでトークンを償還することを約束すると指定して良い。これは、（例えば）１５，４００サトシのトークン化された基礎アウトプット値を有するトランザクションが＄１．５４で償還可能であることを意味し得る。ペギングレートについて０の値は、取引が非分割可能であることを示す（つまり、無記名債券のように、全体のみが転送可能である）。ペギングレートが０に設定されると（非分割可能

トークンを意味する）、基礎ＢＴＣ値は、取引値と無関係であり、任意の額に設定可能である。通常、この場合には、運用コストを最小化するために、基礎ＢＴＣ額を可能な限り小さく保つ（つまり、ダストに設定する）ことが望ましい。

【０１０１】

ＮｕｍＳｈａｒｅｓは、（限定）取引の下で利用可能な合計（固定）株数である。限定取引では、ＮｕｍＳｈａｒｅｓは、ゼロより大きい全体数でなければならない。非限定取引では、いつでも（引き受けられるならば）より多くの株が発行可能なので、ＮｕｍＳｈａｒｅｓは固定されない。これは、値を０に設定することにより示される。

【０１０２】

株は、転送単位として定められ、ＳｈａｒｅＶａｌはその単位の値である。例えば、フィアット通貨では、転送単位は１セントに設定されて良い。あるいは、例えば、転送単位は５０セントに設定されて良く、この場合には、転送は５０セントの「ロット」でのみ実行できる。ＳｈａｒｅＶａｌは、パーセンテージとしても表現できる。例えば、ブリーダが競走馬を１０個の等しい株で売りたいと望む場合、ＳｈａｒｅＶａｌ＝０を設定１０％である。ＳｈａｒｅＶａｌは０より大きくなければならず、且つ取引において定められなければならない。

【０１０３】

ＴｏｔａｌＩｓｓｕａｎｃｅは、発行された株の合計値を表す。この値は限定取引にのみ関連する。非限定取引については、発行は固定されず、より多くの株が発行されて良い。株がパーセンテージとして表現される場合、定義によりＴｏｔａｌＩｓｓｕａｎｃｅ＝０を設定１００％である。

【０１０４】

限定取引では、ＮｕｍＳｈａｒｅｓ、ＳｈａｒｅＶａｌ、及びＴｏｔａｌＩｓｓｕａｎｃｅは、以下のように関連する。

【０１０５】

ＮｕｍＳｈａｒｅｓ×ＳｈａｒｅＶａｌ＝ＴｏｔａｌＩｓｓｕａｎｃｅ

ＴｏｔａｌＩｓｓｕａｎｃｅの０の値は、非限定取引であることを意味する。非限定取引の一例は、フィアット通貨である（したがって、ＴｏｔａｌＩｓｓｕａｎｃｅは０に設定される）。限定取引の例は、（ｉ）限定版記念硬貨（１０００個鋳造され、１株＝１硬貨である）、ＴｏｔａｌＩｓｓｕａｎｃｅ＝１０００×１＝１０００個の硬貨、（ｉｉ）入場券のある会場の席、ＴｏｔａｌＩｓｓｕａｎｃｅ＝利用可能な合計席数、である。

【０１０６】

流通は、未使用トークンの合計値として定められる（つまり、ＵＴＸＯ（未使用トランザクションアウトプット）の中のトランザクションにより決定される）。全部の未使用トランザクションの完全な集合は、全てのビットコインノードに利用可能なリストの中に保持される。例えば、発行人が最初に＄１０，０００をフィアット通貨型のトークンとして発行し、時間を経て＄５５００の価値のトークンが償還された場合、流通＝＄４５００である（未償還トークンの値である）。この値は、関連する準備口座の差引残高に調整されるべきである。

【０１０７】

＜サブキー生成の方法＞

以上では、表３及び例示的なシナリオは、元の（マスタ）キーからサブキーを生成することが有利である状況を参照した。これが実行され得る１つの方法を説明するために、これを達成する方法が以下に提供される。

【０１０８】

図７は、通信ネットワーク５を介して第２ノード７と通信する第１ノード３を含むシステム１を示す。第１ノード３は関連する第１処理装置２３を有し、及び第２ノード５は関連する第２処理装置２７を有する。第１及び第２ノード３、７は、コンピュータ、電話機、タブレットコンピュータ、モバイル通信装置、コンピュータサーバ、等のような電子装置を含んで良い。一例では、第１ノード３はクライアント（ユーザ）装置であって良く、

第２ノード７はサーバであって良い。サーバは、デジタルウォレットプロバイダのサーバであって良い。

【０１０９】

第１ノード３は、第１ノードマスタ秘密鍵（V_{1C}）及び第１ノードマスタ公開鍵（P_{1C}）を有する第１非対称暗号対に関連付けられる。第２ノード７は、第２ノードマスタ秘密鍵（V_{1S}）及び第２ノードマスタ公開鍵（P_{1S}）を有する第２非対称暗号対に関連付けられる。言い換えると、第１及び第２ノードは、それぞれ、個々の公開－秘密鍵対を保有する。

【０１１０】

個々の第１及び第２ノード３、７の第１及び第２非対称暗号対は、ウォレットの登録のような登録処理中に生成されて良い。各ノードの公開鍵は、通信ネットワーク５に渡るように、公に共有されて良い。

【０１１１】

第１ノード３及び第２ノード７の両者において共通シークレット（common secret：ＳＣ）を決定するために、ノード３、７は、通信ネットワーク５を介して秘密鍵を通信することなく、それぞれ方法３００、４００のステップを実行する。

【０１１２】

第１ノード３により実行される方法３００は、少なくとも第１ノードマスタ秘密鍵（V_{1C}）及び生成器値（Generator Value：ＧＶ）に基づき、第１ノード第２秘密鍵（V_{2C}）を決定するステップ３３０を含む。生成器値は、第１ノードと第２ノードとの間で共有されるメッセージ（Ｍ）に基づいて良い。これは、以下に詳述するように、通信ネットワーク５を介してメッセージを共有するステップを含んで良い。方法３００は、少なくとも第２ノードマスタ公開鍵（P_{1S}）及び生成器値（Generator Value：ＧＶ）に基づき、第２ノード第２公開鍵（P_{2S}）を決定するステップ３７０を更に含む。方法３００は、第１ノード第２秘密鍵（V_{2C}）及び第２ノード第２公開鍵（P_{2S}）に基づき、共通シークレット（common secret：ＣＳ）を決定するステップ３８０を含む。

【０１１３】

重要なことに、同じ共通シークレット（ＣＳ）が、方法４００により第２ノード７においても決定できる。方法４００は、第１ノードマスタ公開鍵（P_{1C}）及び生成器値（Generator Value：ＧＶ）に基づき、第１ノード第２公開鍵（P_{2C}）を決定するステップ４３０を含む。方法４００は、第２ノードマスタ秘密鍵（V_{1S}）及び生成器値（Generator Value：ＧＶ）に基づき、第２ノード第２秘密鍵（V_{2S}）を決定するステップ４７０を更に含む。方法４００は、第２ノード第２秘密鍵（V_{2S}）及び第１ノード第２公開鍵（P_{2C}）に基づき、共通シークレット（common secret：ＣＳ）を決定するステップ４８０を含む。

【０１１４】

通信ネットワーク５は、ローカルエリアネットワーク、ワイドエリアネットワーク、セルラネットワーク、無線通信ネットワーク、インターネット、等を含んで良い。これらのネットワークでは、データは電気線、光ファイバ、又は無線のような通信媒体を介して送信されて良く、登頂者１１による様な盗聴を受けやすい場合がある。方法３００、４００は、通信ネットワーク５を介して共通シークレットを送信することなく、第１ノード３及び第２ノード７が共通シークレットを両方とも独立して決定できるようにする。

【０１１５】

したがって、１つの利点は、安全でない可能性のある通信ネットワーク５を介して秘密鍵を送信する必要を有しないで、共通シークレット（ＣＳ）が安全に且つ各ノードにより独立して決定できることである。また、共通シークレットは、秘密鍵として（又は秘密鍵の基礎として）使用されて良い。

【０１１６】

方法３００、４００は、追加ステップを含んで良い。図１１を参照する。方法３００は、第１ノード３において、メッセージ（Ｍ）及び第１ノード第２秘密鍵（V_{2C}）に基づ

き、署名メッセージ（ＳＭ１）を生成するステップを含んで良い。方法３００は、第１署名メッセージ（ＳＭ１）を通信ネットワークを介して第２ノード７へ送信するステップ３６０を更に含む。一方、第２ノード７は、第１署名メッセージ（ＳＭ１）を受信するステップ４４０を実行して良い。方法４００は、第１署名メッセージ（ＳＭ２）を第１ノード第２公開鍵（Ｐ２Ｃ）により検証するステップ４５０、及び第１署名メッセージ（ＳＭ１）を検証するステップの結果に基づき第１ノード３を認証するステップ４６０を更に含む。有利なことに、これは、第２ノード７が、（第１署名メッセージが生成された場所である）意図された第１ノードが第１ノード３であることを認証することを可能にする。これは、第１ノード３だけが、第１ノードマスタ秘密鍵（V_{1C}）へのアクセスを有する、したがって、第１ノード３だけが、第１署名メッセージ（ＳＭ１）を生成するための第１ノード第２秘密鍵（V_{2C}）を決定できるという仮定に基づく。理解されるべきことに、同様に、第２署名メッセージ（ＳＭ２）は、第２ノード７において生成され、第１ノード３へ送信され得る。したがって、ピアツーピアシナリオにおけるように、第１ノード３は、第２ノード７を認証できる。

【０１１７】

第１ノードと第２ノードの間のメッセージ（Ｍ）の共有は、様々な方法で達成されて良い。一例では、メッセージは、第１ノード３において生成されて良く、次に通信ネットワーク５を介して第２ノード７へ送信される。代替として、メッセージは、第２ノード７において生成されて良く、次に通信ネットワーク５を介して第１ノード３へ送信される。幾つかの例では、メッセージ（Ｍ）は公開されて良く、したがってセキュアでないネットワーク５を介して送信されて良い。１又は複数のメッセージ（Ｍ）は、データストア１３、１７、１９に格納されて良い。当業者は、メッセージの共有が様々な方法で達成できることを理解する。

【０１１８】

有利なことに、共通シークレット（ＣＳ）の再生成を可能にするレコードは、そのレコード自体が秘密に格納され又はセキュアに送信される必要がなく、保持され得る。

【０１１９】

＜登録の方法１００、２００＞

登録の方法１００、２００の一例は、図９を参照して記載される。図９では、方法１００は第１ノード３により実行され、方法２００は第２ノード７により実行される。これは、それぞれ第１ノード３及び第２ノード７のために第１及び第２非対称暗号対を確立するステップを含む。

【０１２０】

非対称暗号対は、公開鍵暗号化で使用されるような、関連付けられた秘密鍵及び公開鍵を含む。本例では、非対称暗号対は、楕円曲線暗号システム（Elliptic Curve Cryptography：ＥＣＣ）及び楕円曲線演算の特性を用いて生成される。

【０１２１】

方法１００、２００では、これは、共通ＥＣＣシステムに合意している１１０、２１０、且つ基点（Ｇ）を用いる、第１ノード及び第２ノードを含む（注：基点は、共通生成器として参照され得るが、用語「基点」は、生成器値ＧＶとの混同を避けるために使用される）。一例では、共通ＥＣＣシステムは、ビットコインにより使用されるＥＣＣシステムであるｓｅｃｐ２５６Ｋ１に基づいて良い。基点（Ｇ）は、選択され、ランダムに生成され、又は割り当てられて良い。

【０１２２】

ここで第１ノード３について考えると、方法１００は、共通ＥＣＣシステム及び基点（Ｇ）を解決するステップ１１０を含む。これは、第２ノード７又は第３ノード９から、共通ＥＣＣシステム及び基点を受信するステップを含んで良い。代替として、ユーザインタフェース１５は、第１ノード３に関連付けられる。これにより、ユーザは、共通ＥＣＣシステム及び／又は基点（Ｇ）を選択的に提供できる。更に別の代替案では、共通ＥＣＣシステム及び／又は基点（Ｇ）の一方又は両方が、第１ノード３によりランダムに選択され

て良い。第１ノード３は、通信ネットワーク５を介して、基点（Ｇ）と共に共通ＥＣＣシステムを使用することを示す通知を、第２ノード７へ送信して良い。また、第２ノード７は、共通ＥＣＣシステム及び基点（Ｇ）の使用に対する肯定応答を示す通知を送信することにより、解決して良い２１０。

【０１２３】

方法１００は、第１ノード３が、第１ノードマスタ秘密鍵（V_{1C}）及び第１ノードマスタ公開鍵（P_{1C}）を有する第１非対称暗号対を生成するステップ１２０を更に含む。これは、共通ＥＣＣシステムの中で指定された許容範囲の中のランダム整数に少なくとも部分的に基づき、第１ノードマスタ秘密鍵（V_{1C}）を生成するステップを含む。これは、次式に従い第１ノードマスタ秘密鍵（V_{1C}）及び基点（Ｇ）の楕円曲線点乗算に基づき、第１ノードマスタ公開鍵（P_{1C}）を決定するステップを更に含む。

$$P_{1C}=V_{1C}\times G \quad （式１）$$

したがって、第１非対称暗号対は、以下を含む：

V_{1C}：第１ノードにより秘密に保持される第１ノードマスタ秘密鍵。

P_{1C}：公に知らされる第１ノードマスタ公開鍵。

【０１２４】

第１ノード３は、第１ノードマスタ秘密鍵（V_{1C}）及び第１ノードマスタ公開鍵（P_{1C}）を、第１ノード３に関連付けられた第１データストア１３に格納して良い。セキュリティのために、第１ノードマスタ秘密鍵（V_{1C}）は、鍵が秘密のままであることを保証するために、第１データストア１３のセキュアな部分に格納されて良い。

【０１２５】

方法１００は、図９に示すように、第１ノードマスタ公開鍵（P_{1C}）を通信ネットワーク５を介して第２ノード７へ送信するステップ１３０を更に含む。第２ノード７は、第１ノードマスタ公開鍵（P_{1C}）を受信すると２２０、第１ノードマスタ公開鍵（P_{1C}）を第２ノード７に関連付けられた第２データストア１７に格納して良い２３０。

【０１２６】

第１ノード３と同様に、第２ノード７の方法２００は、第２ノードマスタ秘密鍵（V_{1S}）及び第２ノードマスタ公開鍵（P_{1S}）を有する第２非対称暗号対を生成するステップ２４０を含む。第２ノードマスタ秘密鍵（V_{1S}）も、許容範囲内のランダム整数である。また、第２ノードマスタ公開鍵（P_{1S}）は、次式により決定される。

$$P_{1S}=V_{1S}\times G \quad （式２）$$

したがって、第２非対称暗号対は、以下を含む：

V_{1S}：第２ノードにより秘密に保持される第２ノードマスタ秘密鍵。

P_{1S}：公に知らされる第２ノードマスタ公開鍵。

【０１２７】

第２ノード７は、第２非対称暗号対を第２データストア１７に格納して良い。方法２００は、第２ノードマスタ公開鍵（P_{1S}）を第１ノード３へ送信するステップ２５０を更に含む。また、第１ノード３は、第２ノードマスタ公開鍵（P_{1S}）を受信し１４０、格納して良い１５０。

【０１２８】

理解されるべきことに、幾つかの代案では、それぞれの公開マスタ鍵は、受信され、（信頼できる第三者のような）第３ノード９に関連付けられた第３データストア１９に格納されて良い。これは、認証機関のような、公開ディレクトリとして動作する第三者を含んで良い。したがって、幾つかの例では、第１ノードマスタ公開鍵（P_{1C}）は、共通シークレット（ＣＳ）が要求されるときだけ、第２ノード７により要求され受信されて良い（逆も同様である）。

【０１２９】

登録ステップは、初期設定として１度生じるだけで良い。

【０１３０】

＜セッション開始及び第１ノード３による共通シークレットの決定＞

共通シークレット（ＣＳ）を決定する一例は、図１０を参照してここに記載される。共通シークレット（ＣＳ）は、第１ノード３と第２ノード７との間の特定のセッション、時間、トランザクション、又は他の目的のために使用されて良く、同じ共通シークレット（ＣＳ）を使用することが望ましい又はセキュアでなくて良い。したがって、共通シークレット（ＣＳ）は、異なるセッション、時間、トランザクション、等の間で変更されて良い。

【０１３１】

以下は、上述したセキュアな送信技術の説明のために提供される。

【０１３２】

［メッセージ（Ｍ）を生成する３１０］

本例では、第１ノード３により実行される方法３００は、メッセージ（Ｍ）を生成するステップ３１０を含む。メッセージ（Ｍ）は、ランダム、疑似ランダム、又はユーザ定義であって良い。一例では、メッセージ（Ｍ）は、Ｕｎｉｘ時間又はノンス（及び任意の値）に基づく。例えば、メッセージ（Ｍ）は次のように与えられ得る。

メッセージ（Ｍ）＝Ｕｎｉｘ時間＋ノンス　（式３）

幾つかの例では、メッセージ（Ｍ）は任意である。しかしながら、理解されるべきことに、メッセージ（Ｍ）は、幾つかのアプリケーションで有用であり得る（Ｕｎｉｘ時間、等のような）選択的値を有して良い。

【０１３３】

方法３００は、メッセージ（Ｍ）を通信ネットワーク５を介して第２ノード７へ送信するステップ３１５を含む。メッセージ（Ｍ）は秘密鍵についての情報を含まないので、メッセージ（Ｍ）は、セキュアでないネットワークを介して送信されて良い。

【０１３４】

［生成器値（ＧＶ）を決定する３２０］

方法３００は、メッセージ（Ｍ）に基づき生成器値（Generator Value：ＧＶ）を決定するステップ３２０を更に含む。本例では、これは、メッセージの暗号ハッシュを決定するステップを含む。暗号ハッシュアルゴリズムの一例は、２５６ビット発生器値（ＧＶ）を生成するためにＳＨＡ－２５６を含む。つまり、

ＧＶ＝ＳＨＡ－２５６（Ｍ）　（式４）

理解されるべきことに、他のハッシュアルゴリズムが使用されて良い。これは、セキュアなハッシュアルゴリズム（Secure Hash Algorithm：ＳＨＡ）ファミリの中の他のハッシュアルゴリズムを含んで良い。幾つかの特定の例は、ＳＨＡ３－２２４、ＳＨＡ３－２５６、ＳＨＡ３－３８４、ＳＨＡ３－５１２、ＳＨＡＫＥ１２８、ＳＨＡＫＥ２５６を含むＳＨＡ－３サブセットの中のインスタンスを含む。他のハッシュアルゴリズムは、ＲＩＰＥＭＤ（RACE Integrity Primitives Evaluation Message Digest）ファミリの中のアルゴリズムを含んで良い。特定の例は、ＲＩＰＥＭＤ－１６０を含んで良い。他のハッシュ関数は、Ｚｅｍｏｒ－Ｔｉｌｌｉｃｈハッシュ関数及びナップサック・ハッシュ関数に基づくファミリを含んで良い。

【０１３５】

［第１ノード第２秘密鍵を決定する３３０］

方法３００は、次に、第２ノードマスタ秘密鍵（V_{1C}）及び生成器値（ＧＶ）に基づき、第１ノード第２秘密鍵（V_{2C}）を決定するステップ３３０を含む。これは、次式に従い第１ノードマスタ秘密鍵（V_{1C}）及び生成器値（ＧＶ）のスカラ加算に基づき得る。

$V_{2C}=V_{1C}+GV$　（式５）

【０１３６】

したがって、第１ノード第２秘密鍵（V_{2C}）は、ランダム値ではないが、代わりに第１ノードマスタ秘密鍵から確定的に導出される。暗号対の中の対応する公開鍵、つまり第１ノード第２公開鍵（P_{2C}）は、以下の関係を有する。

$P_{2C}=V_{2C}\times G$　（式６）

【０１３７】
式５から式６にV_{2C}を代入すると、次式を得る。
$P_{2C}=(V_{1C}+GV)\times G$　（式７）
ここで、「＋」演算子はスカラ加算を表し、「×」演算子は楕円曲線点乗算を表す。楕円曲線暗号代数は、分配的であり、式７は次式のように表すことができる。
$P_{2C}=V_{1C}\times G+GV\times G$　（式８）
【０１３８】
最後に、（式１）は（式７）に代入され、次式を得る。
$P_{2C}=P_{1C}+GV\times G$　（式９．１）
$P_{2C}=P_{1C}+SHA-256(M)\times G$　（式９．２）
式８～９．２において、「＋」演算子は楕円曲線点加算を表す。したがって、対応する第１ノード第２公開鍵（P_{2C}）は、第１ノードマスタ公開鍵（P_{1C}）及びメッセージ（Ｍ）の導出可能な所与の知識であり得る。方法４００に関して以下に更に詳述するように、第２ノード７は、第１ノード第２公開鍵（P_{2C}）を独立に決定するために、このような知識を有して良い。
【０１３９】
［メッセージ及び第１ノード第２秘密鍵に基づき、第１署名メッセージ（ＳＭ１）を生成する３５０］
方法３００は、メッセージ（Ｍ）及び決定した第１ノード第２秘密鍵（V_{2C}）に基づき、第１署名メッセージ（ＳＭ１）を生成するステップ３５０を更に含む。署名メッセージを生成するステップは、メッセージ（Ｍ）にデジタル方式で署名するために、デジタル署名アルゴリズムを適用するステップを含む。一例では、これは、第１署名メッセージ（ＳＭ１）を得るために、楕円曲線デジタル署名アルゴリズム（Elliptic Curve Digital Signature Algorithm：ＥＣＤＳＡ）の中でメッセージに第１ノード第２秘密鍵（V_{2C}）を適用するステップを含む。ＥＣＤＳＡの例は、ｓｅｃｐ２５６ｋ１、ｓｅｃｐ２５６ｒ１、ｓｅｃｐ３８４ｒ１、ｓｅ３ｃｐ５２１ｒ１を有するＥＣＣシステムに基づくものを含む。
【０１４０】
第１署名メッセージ（ＳＭ１）は、第２ノード７において対応する第１ノード第２公開鍵（P_{2C}）により検証できる。第１署名メッセージ（ＳＭ１）のこの検証は、第１ノード３を認証するために第２ノード７により使用されて良い。これは、方法４００において以下に議論される。
【０１４１】
［第２ノード第２公開鍵を決定する３７０’］
第１ノード３は、次に、第２ノード第２公開鍵（P_{2S}）を決定して良い３７０。上述のように、第２ノード第２公開鍵（P_{2S}）は、少なくとも第２ノードマスタ公開鍵（P_{1S}）及び生成器値（ＧＶ）に基づいて良い。本例では、公開鍵は、基点（Ｇ）との楕円曲線点乗算により秘密鍵として決定されるので３７０’、第２ノード第２公開鍵（P_{2S}）は、式６と同様に次のように表すことができる。
$P_{2S}=V_{2S}\times G$　（式１０．１）
$P_{2S}=P_{1S}+GV\times G$　（式１０．２）
式１０．２の数学的証明は、第１ノード第２公開鍵（P_{2C}）について式９．１を導出するために上述したものと同じである。理解されるべきことに、第１ノード３は、第２ノード７と独立に第２ノード第２公開鍵を決定できる３７０。
【０１４２】
［第１ノード３において共通シークレットを決定する３８０］
第１ノード３は、次に、第１ノード第２秘密鍵（V_{2C}）及び決定した第２ノード第２公開鍵（P_{2S}）に基づき、共通シークレット（ＣＳ）を決定して良い３８０。共通シークレット（ＣＳ）は、第１ノード３により次式により決定されて良い。
$S=V_{2C}\times P_{2S}$　（式１１）

【０１４３】
＜第２ノード７において実行される方法４００＞
第２ノード７において実行される対応する方法４００が、ここで説明される。理解されるべきことに、これらのステップのうちの幾つかは、第１ノード３により実行された上述のステップと同様である。
【０１４４】
方法４００は、メッセージ（Ｍ）を通信ネットワーク５を介して第１ノード３から受信するステップ４１０を含む。これは、ステップ３１５において第１ノード３により送信されたメッセージ（Ｍ）を含んで良い。第２ノード７は、次に、メッセージ（Ｍ）に基づき生成器値（ＧＶ）を決定する４２０。第２ノード７により生成器値（ＧＶ）を決定するステップ４２０は、上述の第１ノードにより実行されるステップ３２０と同様である。本例では、第２ノード７は、第１ノード３と独立の、この決定するステップ４２０を実行する。
【０１４５】
次のステップは、第１ノードマスタ公開鍵（P_{1C}）及び生成器値（ＧＶ）に基づき、第１ノード第２公開鍵（P_{2C}）を決定するステップ４３０を含む。本例では、公開鍵は、基点（Ｇ）との楕円曲線点乗算により秘密鍵として決定されるので４３０’、第１ノード第２公開鍵（P_{2C}）は、式９と同様に次のように表すことができる。
$P_{2C}=V_{2C}\times G$　（式１２．１）
$P_{2C}=P_{1C}+GV\times G$　（式１２．２）
【０１４６】
式１２．１及び１２．２の数学的証明は、式１０．１及び１０．２について上述したものと同じである。
【０１４７】
［第２ノード７が第１ノード３を認証する］
方法４００は、未確認第１ノード３が第１ノード３であることを認証するために、第２ノード７により実行されるステップを含んで良い。上述のように、これは、第１ノード３から第１署名メッセージ（ＳＭ１）を受信するステップ４４０を含む。第２ノード７は、次に、ステップ４３０で決定された第１ノード第２公開鍵（P_{2C}）により第１署名メッセージ（ＳＭ１）の署名を検証して良い４５０。
【０１４８】
デジタル署名の検証は、上述の楕円曲線デジタル署名アルゴリズム（Elliptic Curve Digital Signature Algorithm：ＥＣＤＳＡ）に従い行われて良い。重要なことに、第１ノード第２秘密鍵（V_{2C}）により署名された第１署名メッセージ（ＳＭ１）は、V_{2C}及びP_{2C}が暗号対を形成するので、対応する第１ノード第２公開鍵（P_{2C}）によってのみ正しく検証されるべきである。これらの鍵は、第１ノード３の登録で生成された第１ノードマスタ秘密鍵（V_{1C}）及び第１ノードマスタ公開鍵（P_{1C}）において確定するので、第１署名メッセージ（ＳＭ１）の検証は、第１署名メッセージ（ＳＭ１）を送信する未確認第１ノードが登録中と同じ第１ノード３であることを認証する基礎として使用できる。したがって、第２ノード７は、第１署名メッセージを検証するステップ（４５０）の結果に基づき、第１ノード３を認証するステップ（４６０）を更に実行して良い。
【０１４９】
［第２ノード７が共通シークレットを決定する］
方法４００は、第２ノード７が、第２ノードマスタ秘密鍵（V_{1S}）及び生成器値（ＧＶ）に基づき、第２ノード第２秘密鍵（V_{2S}）を決定するステップ４７０を更に含んで良い。第１ノード３により実行されるステップ３３０と同様に、第２ノード第２秘密鍵（V_{2S}）は、次式に従い、第２ノードマスタ秘密鍵（V_{1S}）及び生成器値（ＧＶ）のスカラ加算に基づき得る。
$V_{2S}=V_{1S}+GV$　（式１３．１）
$V_{2S}=V_{1S}+SHA-256(M)$　（式１３．２）

【０１５０】
第２ノード７は、次に、第１ノード３と独立して、次式に基づき、第２ノード第２秘密鍵（V_{2S}）及び第１ノード第２公開鍵（P_{2C}）に基づき、共通シークレット（ＣＳ）を決定して良い４８０。
$S = V_{2S} \times P_{2C}$　（式１４）
【０１５１】
［第１ノード３及び第２ノード７により決定された共通シークレット（ＣＳ）の証明］
第１ノード３により決定された共通シークレット（ＣＳ）は、第２ノード７において決定された共通シークレット（ＣＳ）と同じである。式１１及び式１４が同じ共通シークレット（ＣＳ）を提供することの数学的証明が、ここで記載される。
【０１５２】
第１ノード３により決定された共通シークレット（ＣＳ）を考えると、次のように式１０．１は式１１に代入できる。
$S = V_{2C} \times P_{2S}$　（式１１）
$S = V_{2C} \times (V_{2S} \times G)$
$S = (V_{2C} \times V_{2S}) \times G$　（式１５）
【０１５３】
第２ノード７により決定された共通シークレット（ＣＳ）を考えると、次のように式１２．１は式１４に代入できる。
$S = V_{2S} \times P_{2C}$　（式１４）
$S = V_{2S} \times (V_{2C} \times G)$
$S = (V_{2S} \times V_{2C}) \times G$　（式１６）
【０１５４】
ＥＣＣ代数学は可換性なので、次の通り式１５及び式１６は等価である。
$S = (V_{2C} \times V_{2S}) \times G = (V_{2S} \times V_{2C}) \times G$　（式１７）
【０１５５】
［共通シークレット（ＣＳ）及び秘密鍵］
共通シークレット（ＣＳ）は、ここで、第１ノード３と第２ノード７との間のセキュアな通信のために、対称鍵アルゴリズムにおいて、秘密鍵として又は秘密鍵の基礎として、使用できる。
【０１５６】
共通シークレット（ＣＳ）は、楕円曲線点（x_S，y_S）の形式であって良い。これは、ノード３、７により合意された標準的な公に知られた演算を用いて、標準的な鍵フォーマットに変換されて良い。例えば、x_S値は、AES_{256}暗号鍵として使用され得る２５６ビットの整数であって良い。これは、更に、１６０ビットの長さの鍵を必要とする任意のアプリケーションのために、ＲＩＰＥＭＤ１６０を用いて１６０ビットの整数に変換され得る。
【０１５７】
共通シークレット（ＣＳ）は、必要に応じて決定されて良い。重要なことに、共通シークレット（ＣＳ）はメッセージ（Ｍ）に基づき再決定できるので、第１ノード３は共通シークレット（ＣＳ）を格納する必要がない。幾つかの例では、使用されるメッセージ（Ｍ）は、マスタ秘密鍵のために要求されるのと同レベルのセキュリティを有しないデータストア１３、１７、１９（又は他のデータストア）に格納されて良い。幾つかの例では、メッセージ（Ｍ）は公に利用可能であって良い。
【０１５８】
しかしながら、幾つかのアプリケーションに依存して、共通シークレット（ＣＳ）が第１ノードマスタ秘密鍵（V_{1C}）と同じくらいセキュアに保たれるならば、共通シークレット（ＣＳ）は、第１ノードに関連付けられた第１データストア（Ｘ）に格納され得る。
【０１５９】
有利なことに、この技術は、単一のマスタキー暗号対に基づき、複数のセキュアな秘密

鍵に対応し得る複数の共通シークレットを決定するために使用できる。

【０１６０】

＜生成器値（鍵）の階層構造＞

例えば、一連の連続する生成器値（ＧＶ）が決定されて良い。ここで、各連続ＧＶは、前の生成器値（ＧＶ）に基づき決定されて良い。例えば、連続する専用鍵を生成するためにステップ３１０～３７０、４１０～４７０を繰り返す代わりに、ノード間の事前合意により、生成器値の階層構造を確立するために、前に使用された生成器値（ＧＶ）が両方のパーティにより繰り返し再ハッシュされ得る。実際に、メッセージ（Ｍ）のハッシュに基づく生成器値は、次世代生成器値（ＧＶ’）のための次世代メッセージ（Ｍ’）になり得る。これを行うことは、計算されるべき共有シークレットの連続生成を可能にし、更なるプロトコルにより確立される送信、特に共通シークレットを生成する毎に複数のメッセージの送信の必要がない。次世代共通シークレット（ＣＳ’）は、以下のように計算できる。

【０１６１】

先ず、第１ノード３及び第２ノード７の両者が、次世代生成器値（ＧＶ’）を独立して決定する。これは、ステップ３２０及び４２０と同様であるが、次式により適応される。

【０１６２】

Ｍ’＝ＳＨＡ－２５６（Ｍ）　（式１８）

ＧＶ’＝ＳＨＡ－２５６（Ｍ’）　（式１９．１）

ＧＶ’＝ＳＨＡ－２５６（ＳＨＡ－２５６（Ｍ））　（式１９．２）

【０１６３】

第１ノード３は、次に、次世代の第２ノード第２公開鍵（P_{2S}’）及び第１ノード第２秘密鍵（V_{2C}’）を上述のステップ３７０及び３３０と同様であるが次式により適応され、決定して良い。

P_{2S}’＝P_{1S}＋ＧＶ’×Ｇ　（式２０．１）

V_{2C}’＝V_{1C}＋ＧＶ’　（式２０．２）

【０１６４】

第２ノード７は、次に、次世代の第１ノード第２公開鍵（P_{2C}’）及び第２ノード第２秘密鍵（V_{2S}’）を上述のステップ４３０及び４７０と同様であるが次式により適応され、決定して良い。

P_{2C}’＝P_{1C}＋ＧＶ’×Ｇ　（式２１．１）

V_{2S}’＝V_{1S}＋ＧＶ’　（式２１．２）

【０１６５】

第１ノード３及び第２ノード７は、次に、それぞれ、次世代共通シークレット（ＣＳ’）を決定して良い。特に、第１ノード３は、次式により次世代共通シークレット（ＣＳ’）を決定する。

ＣＳ’＝V_{2C}’×P_{2S}’　（式２２）

【０１６６】

第２ノード７は、次式により次世代共通シークレット（ＣＳ’）を決定する。

ＣＳ’＝V_{2S}’×P_{2C}’　（式２３）

更なる世代（ＣＳ’’、ＣＳ’’’、等）は、チェーン階層構造を生成するために同じ方法で計算できる。この技術は、第１ノード３及び第２ノード７の両者が元のメッセージ（Ｍ）又は最初に計算された生成器値（ＧＶ）、及びそれがどのノードに関連するか、を見失わないことを要求する。これは公に知られた情報なので、この情報の保有に関してセキュリティ問題は存在しない。したがって、この情報は、（ハッシュ値を公開鍵にリンクする）「ハッシュテーブル」に保持され、（例えばＴｏｒｒｅｎｔを用いて）ネットワーク５に渡り自由に配布されて良い。さらに、階層構造内の任意の個々の共通シークレット（ＣＳ）が今までに解決されていない場合、これは、秘密鍵V_{1C}、V_{1S}がセキュアなままであるならば、階層構造の中の任意の他の共通シークレットのセキュリティに影響しない。

【０１６７】
＜鍵の木構造＞
上述のようなチェーン（線形）階層構造と同様に、木構造の形式の階層構造が生成できる。木構造によると、認証鍵、暗号鍵、署名鍵、支払鍵、等のような異なる目的の様々な鍵が決定されて良い。それにより、これらの鍵は、全て単一のセキュアに維持されるマスタキーにリンクされる。これは、種々の異なる鍵を有する木構造９０１を示す図１２に図示される。これらの各々は、別のパーティと共有されるシークレットを生成するために使用できる。枝分かれする木は、幾つかの方法で達成でき、それらのうちの３つが以下に記載される。
【０１６８】
（ｉ）マスタキー・スポーニング
チェーン階層構造では、乗算した再ハッシュしたメッセージを元のマスタキーに加算することにより、各々の新しい「リンク」（公開／秘密鍵ペア）が生成される。例えば（明確性のため、第１ノード３の秘密鍵のみを示す）、
$V_{2C}=V_{1C}+SHA-256(M)$　（式２４）
$V_{2C}'=V_{1C}+SHA-256(SHA-256(M))$　（式２５）
$V_{2C}''=V_{1C}+SHA-256(SHA-256(SHA-256(M)))$　（式２６）
等である。
【０１６９】
枝を生成するために、任意の鍵がサブマスタキーとして使用できる。例えば、V_{2C}'は、正規のマスタキーに対して行われるように、ハッシュを加算することにより、サブマスタキー（V_{3C}）として使用できる。
$V_{3C}=V_{2C}'+SHA-256(M)$　（式２７）
【０１７０】
サブマスタキー（V_{3C}）は、それ自体が、次世代鍵（V_{3C}'）を有して良い。例えば次式の通りである。
$V_{3C}'=V_{2C}'+SHA-256(SHA-256(M))$　（式２８）
【０１７１】
これは、図１３に示すマスタキー・スポーニング（spawning）方法を用いて、木構造９０３を提供する。
【０１７２】
（ｉｉ）論理的関連付け
この方法では、木の中の全てのノード（公開／秘密鍵ペア）は、チェーンとして（又は任意の他の方法で）生成され、木の中のノード間の論理的関係は、ポインタを用いて木の中の各ノードが木の中の自身の親ノードに単純に関連付けられるテーブルにより維持される。したがって、ポインタは、セッションの共通シークレットキー（ＣＳ）を決定するために、関連する公開／秘密鍵ペアを決定するために使用できる。
【０１７３】
（ｉｉｉ）メッセージ多様性
新しい公開／秘密鍵ペアは、チェーン又は木の任意のポイントに新しいメッセージを導入することにより、生成できる。メッセージ自体は、任意であって良く、又は何らかの意味若しくは関数を伝達して良い（例えば、それは、「現実の」銀行口座番号に関連して良い、等である）。新しい公開／秘密鍵ペアを形成するためのこのような新しいメッセージがセキュアに保持されることが望ましい場合がある。
【０１７４】
＜本発明と共に使用するための説明のための計算エージェント＞
本発明は、取引処理の自動化された態様を実行するために、計算リソース又はエージェントを利用できる。適切なエージェントの一例が以下に提供されるが、他の実装が使用されて良い。

【０１７５】
エージェントは、チューリング（Turing）機械の実装において非消去可能テープとしてブロックチェーンを使用して、ブロックチェーンと連携して動作して良い。このエージェントは、ブロックチェーンネットワークと並列に実行し、（ループ）処理の実行を監督し及び扱う。ループ処理は、例えば装置又はシステムの処理又は制御の自動化のような所与のタスクを実行するよう設計される。この並列リソースは、ブロックチェーンの状態を監視し、トランザクションをブロックチェーンに書き込ませることができる。ある意味で、これは、ブロックチェーンをチューリング機械の非消去可能テープとして利用し、以下の定義及び特徴を有する。
１．ブロックチェーンは、チューリング機械のテープとして作用する。ブロックチェーンの中の各トランザクションは、テープ上のセルを表す。このセルは、有限なアルファベットからの記号を含み得る。
２．テープヘッドは、ブロックチェーン上に既に書き込まれているブロックから情報を読み出すことができる。
３．テープヘッドは、多くのトランザクションを含む新しいブロックを、ブロックチェーンの終わりに書き込むことができる。しかしながら、それらは、既に存在するブロックに書き込むことができない、このように、ブロックチェーンテープは非消去可能である。
４．各トランザクションのマルチシグネチャのＰ２ＳＨ（pay－to－script－hash）トランザクションの部分として格納され得る。
【０１７６】
エージェントに重要な機能は、ブロックチェーンの現在状態を監視する自動エンティティとして作用することである。これは更に、任意のオフブロックソースから、信号又は入力を受信できる。ブロックチェーン状態及び／又は受信した入力に依存して、エージェントは特定動作を実行して良い。エージェントは、どの動作が実行されるべきかを決定する。これらは、「現実世界」（つまり、オフブロック）の中の作用、及び／又（新しいトランザクションを生成する及びブロードキャストするような）はブロックチェーンに対する作用を含んで良く又は含まなくて良い。エージェントが取る作用は、ブロックチェーン状態によりトリガされて良い。エージェントは、更に、ビットコインネットワークにブロードキャストされるべき次のトランザクションセットについて決定し、後にブロックチェーンに書き込んで良い。
【０１７７】
エージェントの作用は、並列に且つ同時にブロックチェーン（例えば、ビットコイン）ネットワークに対して実行する。ある意味で、これは、ブロックチェーン（例えば、ビットコイン）スクリプトの機能を格納する。この連続監視は、結合されたエージェント及びブロックチェーンシステムチューリング完全（Turing Complete）を作成する「ループ」制御フロー構成を実施する。
【０１７８】
チューリング機械は、以下の２つのスタックを含む。
・データスタック：これは、上述のようにブロックチェーンにより表される。
・制御スタック：これは、エージェント機能により表される。これは、繰り返し制御フロー機能に関連する情報を格納する。
【０１７９】
制御スタックのデータスタックからの分離は、無限ループがビットコイン中核で生じることを防ぎ、サービス拒否攻撃を軽減するという利点を提供する。
【０１８０】
エージェントは、任意の種類のループ構成（例えば、ＦＯＲ－ＮＥＸＴ、ＲＥＰＥＡＴ ＵＮＴＩＬ、等）によりループ可能なサブルーチンを管理し及び実行する。本願明細書に記載の説明のための実施形態は、「繰り返し（ｒｅｐｅａｔ）」構成の一例を用いる処理を含む。ユーザは、インデックス（ｉ）及び限界（Ｊ）を指定して良い。これらはそれぞれ、現在の反復番号（標準的に０から開始してカウントされる）、及び繰り返しループ

の合計反復数、を表す。
【０１８１】
各反復について、
１．インデックスが１だけ増大する。終了条件については、インデックスが限界に達すると、反復は停止する。
２．「if condition then action（［条件］ならば［動作］する）」（ＩＣＴＡ）文を含むコードブロックが実行される。動作は、ブロックチェーン上の又は外の任意の動作であって良い。
３．このサブルーチンの暗号ハッシュが計算される。これは、トランザクションの部分としてブロックチェーンに格納できる。ハッシュは各コードにユニークなので、どのコードが使用されているかの検証を可能にする。
【０１８２】
ループ本体は、コードブロックを含む。各コードブロックは、「if condition then action（［条件］ならば［動作］する）」（ＩＣＴＡ）文を含む。これは、以下に一致するトランザクションについて、ブロックチェーンの現在状態を監視する。
・開始又はトリガ条件（例えば、特定日に達したとき）、
・繰り返し条件（つまり、前の反復に関連付けられたメタデータ又はハッシュ）、
・停止条件（つまり、ループの最後の反復）。
【０１８３】
ＩＣＴＡ文は、エージェントが、ブロックチェーンの現在状態に基づき、次のトランザクションについて決定することを可能にする。次のトランザクションを生成することは、トランザクションをビットコインネットワークにブロードキャストすること、及び新しいトランザクションをブロックチェーンに書き込むことを含む。これは、この反復が実行されたことの記録として作用する。トランザクションがブロックチェーンに書き込まれると、マネジャは、続いて、前の反復が実行されブロックチェーンに書き込まれたことを知り、次の反復を実行するだろう。後者は、インデックス（ｉ）がコードブロックの中で指定された限度（Ｊ）に達するとき、繰り返しループが存在するまで継続する。
【０１８４】
各トランザクションは、再利用可能な方法で、ブロックチェーンに保存される。ビットコイン実装では、トランザクションの中の各署名は、ＳＩＧＨＡＳＨフラグを付加される。このフラグは、異なる値を取ることができる。これらの値の各々は、この署名の所有者の関与無しに、トランザクションの他の部分が変更され得るか否かを示す。再利用可能トランザクションは、トランザクションインプットのうちの１つの中にＳＩＧＨＡＳＨフラグ「ＳｉｇＨａｓｈ＿ＡｎｙｏｎｅＣａｎＰａｙ」を有する。これは、誰もがトランザクションのインプットに貢献することを許容する。このパラメータは、エージェントのＩＣＴＡ関数が、複数回、異なるインプットで、実行され且つ繰り返されることを可能にする。この関数の使用は、例えば再利用トランザクションの複製により、認可パーティに制限できる。
【０１８５】
ＩＣＴＡコードブロックの「If condition」部分は、任意の種類の条件を監視できる。これは、他のプログラミング言語（例えば、Ｃ、Ｃ＋＋、Ｊａｖｅ）と同様であり、ブロックチェーンに格納された情報に限定されない。例えば、これは、日付及び時間（つまり、特定の日時に達したとき）を監視し、又は天気（つまり、気温が１０℃より低く且つ雨が降っているとき）を監視し、取引又は信用の条件（つまり、企業Ａが企業Ｂを買うとき）を監視し得る。
【０１８６】
ＩＣＴＡコードブロックの「Then action」部分は、多数の動作を実行できる。本発明は、取り得る動作の数又は種類に関して限定されない。動作は、ブロックチェーン上のトランザクションに限定されないが、動作に関連するメタデータを含むトランザクションは、ブロックチェーンに書き込まれて良い。

【０１８７】
メタデータは、任意の形式であり得る。しかしながら、一実施形態では、メタデータは、動作に関連するより多くのデータ又は指示を含むファイルへのハイパーリンクを格納して良い。メタデータは、動作に関連するより多くのデータ又は指示を含むハッシュテーブルへのハイパーリンク、及びハッシュテーブルに対する検索キーとして作用する動作のハッシュの両方を格納して良い。
【０１８８】
エージェントの制御スタックは、各ユーザの必要に特化した多数の方法で実装できる。例えば、制御スタックの繰り返しループは、任意のチューリング完全言語に基づき得る。言語の１つの可能な選択は、Ｆｏｒｔｈ型スタックに基づく言語である。この言語を使用する利点は、制御スタックを、既知であり且つ広く使用されているビットコインスクリプトとプログラミング型において一貫性を保つことである。
【０１８９】
＜ビットコインスクリプトの交互形式スタック（Alternate Stack）をデータ記憶空間として使用する＞
ビットコインスクリプトは、コマンド、更に呼び出されるオペコード、を含む。これらは、ユーザが、データを「ａｌｔ ｓｔａｃｋ」として知られる交互形式スタックに移動させることを可能にする。
【０１９０】
オペコードは、次の通りである。
・ＯＰ＿ＴＯＡＬＴＳＴＡＣＫ。これは、データを主スタックの最上部からａｌｔ ｓｔａｃｋの最上部に移動させる。
・ＯＰ＿ＦＲＯＭＡＬＴＳＴＡＣＫ。これは、データをａｌｔ ｓｔａｃｋの最上部から主スタックの最上部に移動させる。
【０１９１】
これは、計算機にデータを格納させる「記憶（memory）」機能と同様に、中間計算ステップからのデータをａｌｔ ｓｔａｃｋに格納させる。一実施形態では、ａｌｔ ｓｔａｃｋは、小さな計算タスクを解決するようビットコインスクリプトを構成するために、及び結果を計算に返すために、使用される。
【０１９２】
＜エージェントを管理するためにコードレジスタを使用する＞
エージェントは、また、自身の所有し且つ実行する全てのコードのレジストリを管理する。このレジストリは、特定キーを特定値にマッピングするルックアップテーブル又は辞書のように構造化される。キー及び値ペアは、それぞれ、コードブロックのハッシュ（H_1）及びコードが格納された場所のＩＰｖ６アドレスにより表される。キーH_1を用いてコードブロックを読み出すために、ルックアップテーブルが使用されて、関連する値（これは、コードの格納されている場所である）を読み出し、及びそれに応じてソースコードを読み出す。コードレジストリの実装は変化し得る。
【０１９３】
＜エージェントのコードのトランザクションメタデータ、及びループの再スポーニング＞
特定の反復でエージェントのループを再スポーニングするために必要な情報は、ブロックチェーンに記録されたトランザクションの中にメタデータとして格納される。
【０１９４】
このように、ブロックチェーン上のトランザクションは、エージェント上で実行されているループの所与の反復に関する情報を格納し、又はそれへのアクセスを提供する。この情報は、ループに関連付けられた任意の変数の値、例えばインデックスｉ、及び任意の他の必要な情報、例えばコードブロック内で使用されるパラメータの値又は更に要求される情報がアクセス可能な場所の位置関連データ、を含み得る。
【０１９５】

メタデータ自体は、トランザクションの中のマルチシグネチャのＰ２ＳＨ（pay－to－script－hash）スクリプトの部分として格納される。トランザクションと共に記録されたメタデータは、コードが過去にどのように実行されたかのオーディットトレイルを記録する能力も与える。

【０１９６】

エージェントが各反復で繰り返しループコードブロックを再スポーニングできる幾つかの方法が存在する。コードブロックは、エージェント自体にハードコードされて良く、又は秘密に若しくは公に利用可能なファイルに格納でき、又は、秘密若しくは公開ハッシュテーブルファイル上のエントリとして格納され得る、又はこれらの組み合わせである。コードブロックは、ハードコードされた変数に固定され、又は固定であるが、移植可能なパラメータを含み得る。パラメータは、任意のデータフォーマットの単一値であって良く、又は小さなコードチャンクであって良く、又はそれらの組み合わせであって良い。パラメータは、トランザクション（例えば、ビットコイントランザクション）の中のメタデータから、又は内部データベース又は秘密／公開ファイル又はハッシュテーブル又はこれらの任意の組み合わせのような外部ソースから、直接に該パラメータを読み出すことにより移植され得る。パラメータ値の外部ソースへのポインタは、トランザクションの中のメタデータに格納されて良い。

【０１９７】

以下のステップは、エージェントがｉ番目の反復で繰り返しループコードブロックをどのように再スポーニングできるかの一例を提供する。本例では、コードレジストリは、ハッシュテーブルである。これにより、ハッシュ値がテーブルの検索キーとして作用し、トランザクション上のメタデータに格納される。

１．エージェントは、コードレジストリ内のエントリに一致するコードブロックのハッシュを含むトランザクションについて、ブロックチェーンを監視する。

２．エージェントは、対応するハッシュ（H_1）を含むトランザクションを見付ける。

３．エージェントは、「メタデーターＣｏｄｅＨａｓｈ」を読み出し、H_1を得るためにＣｏｄｅＨａｓｈフィールドを得て、H_1を用いてコード（C_1）を読み出す。ＲＩＰＥＭＤ－１６０（ＳＨＡ２５６（C_1））がH_1に等しい場合、コードは変化しておらず、安全に次のステップに進める。

４．エージェントは、インデックスＩを格納する「メタデーターＣｏｄｅＨａｓｈ」を読み出し、ｉ番目の反復でコードを再スポーニングする。言い換えると、ループが、適切な反復で「リロード」される。

５．メタデータの発生元を検証するために、ユーザの署名がＰ２ＳＨコマンドに含まれる。

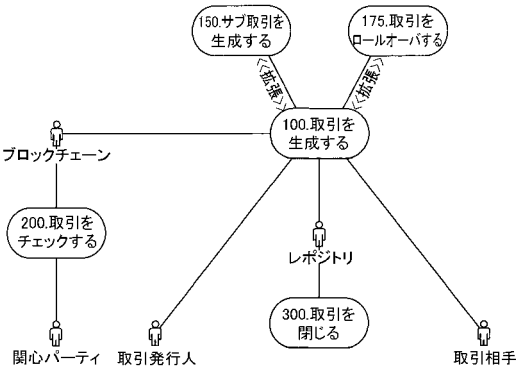
６．これらのデータがループのこの反復のために必要な場合、エージェントは、「メタデーターＯｕｔｐｕｔＨａｓｈ」及び「メタデーターＯｕｔｐｕｔＰｏｉｎｔｅｒ」を読み出し、前のステップのアウトプットを検索する。

【０１９８】

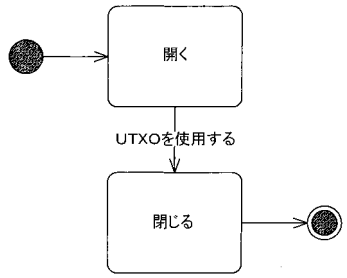
留意すべきことに、上述の実施形態は、本発明を限定するのではなく、当業者は添付の請求項により定められる本発明の範囲から逸脱することなく多数の代替の実施形態を考案できる。請求項中、括弧内に記載された如何なる参照符号も、請求項を制限すると見なされるべきではない。用語「有する（comprising又はcomprises）」等は、全体としていかなる請求項中に及び明細書に列挙された以外の要素又はステップの存在を排除するものではない。本願明細書において、「有する（comprises）」は「含む（includes）又は構成される（consists of）」を意味し、「有する（comprising）」は「含む（including）又は構成される（including of）」を意味する。要素の単数の参照は、該要素の複数の存在を排除するものではなく、逆も同様である。本発明は、複数の別個の要素を有するハードウェアにより又は適切にプログラムされたコンピュータにより、実施され得る。複数の手段を列挙している装置の請求項では、これらの複数の手段は、１つの同一のハードウェア要素により実装することができる。特定の量が相互に異なる従属請求項に記載される

という事実は、これらの量の組合せが有利に用いることが出来ないことを示すものではない。

【図１】



【図２Ａ】



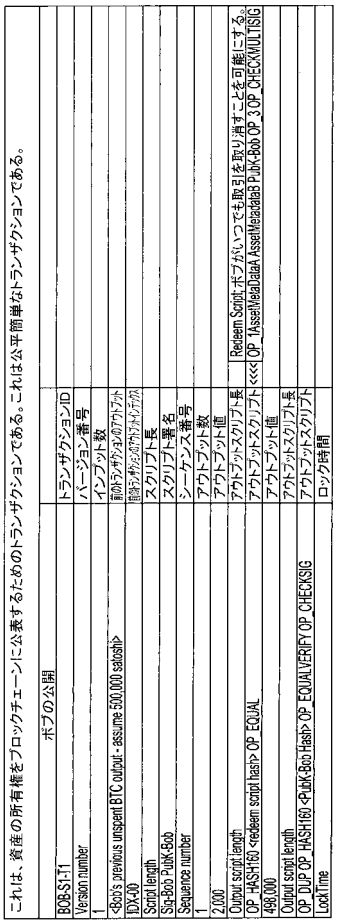
【図２Ｂ】

シナリオ定義
ボブ：自宅をブロックチェーンに登録したい

住宅ベースメタデータ

フィールド	サブフィールド	バイト	値	コメント
Asset Metadata A	ContractType	4	0x0000FF04	単位を示す
	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxxx	資産定義（Asset Definition）ファイルのアドレス
	Padding	12		予備
Asset Metadata B	ContractHash	20	################...	資産定義（Asset Definition）ファイルのハッシュ（トークン化ではない）
	Jurisdiction	2	EN	資産が英法によりカバーされることを指定する
	Options	2	0x0000	オプション指定なし
	Padding	8		予備

【図２Ｃ】



これは、資産の所有権をブロックチェーンに公表するためのトランザクションである。これは公平簡単なトランザクションである。

ボブの公開	
BOB-S1-T1	トランザクションID
Version number	バージョン番号
1	インプット数
<Bob's previous unspent BTC output - assume 500,000 satoshi>	前のトランザクションのアウトプット
IDX-00	前のトランザクションのアウトプットのインデックス
Script length	スクリプト長
Sig-Bob PubK-Bob	スクリプト署名
Sequence number	シーケンス番号
1	アウトプット数
2,000	アウトプット値
Output script length	アウトプットスクリプト長
OP_HASH160 <redeem script hash> OP_EQUAL	アウトプットスクリプト
498,000	アウトプット値
Output script length	アウトプットスクリプト長
OP_DUP OP_HASH160 <PubK-Bob Hash> OP_EQUALVERIFY OP_CHECKSIG	アウトプットスクリプト
Lock time	ロック時間

Redeem Script: ボブがいつでも取引を取り消すことを可能にする。
<<< OP_1AssetMetadataA AssetMetadataB PubK-Bob OP_3 OP_CHECKMULTISIG

【図２Ｄ】

ボブが資産を除去する、又はもはや資産を公表（又は準公表）することを望まないとき、彼は単にトランザクションアウトプットを使用する

ボブの取引取り消し	
BOB-S1-T2	トランザクションID
Version number	バージョン番号
1	インプット数
BOB-S1-T1	前のトランザクションアウトプット
IDX-00	前のトランザクションアウトプットのインデックス
Script length	スクリプト長
Sig-Bob OP_1AssetMetadataA AssetMetadataB PubK-Bob OP_3 OP_CHECKMULTISIG	スクリプト署名
Sequence number	シーケンス番号
1	アウトプット数
1,000	アウトプット値
Output script length	アウトプットスクリプト長
OP_DUP OP_HASH160<PubK-Bob Hash>OP_EQUALVERIFY OP_CHECKSIG	アウトプットスクリプト
LockTime	ロック時間

【図３Ａ】

シナリオ定義
ボブ：隠された所有権を有する資産を生成し、ブロックチェーン上で公表したい

住宅ベースメタデータ

フィールド	サブフィールド	バイト	値	コメント
Asset Metadata A	ContractType	4	0x0000FF04	単位を示す
	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) xxxx	資産定義（Asset Definition）ファイルのアドレス
	Padding	12		予備
Asset Metadata B	ContractHash	20	################...	資産定義（Asset Definition）ファイルのハッシュ（トークン化ではない）
	Juristiction	2	EN	資産が英法によりカバーされることを指定する
	Options	2	0x0000	オプション指定なし
	Padding	8		予備

【図３Ｂ】

ボブによる資産の提供	
BOB-S2-T1	
1	
<Bob's previous unspent BTC output - assume 500,000 satoshi>	
IDX-00	
Sig-Bob PubK-Bob	
2	
4,000	アウトプット値
OP_DUP OP_HASH160<PubK-Asset Hash>OP_EQUALVERIFY OP_CHECKSIG	
496,000	
Output script length	アウトプットスクリプト長
OP_DUP OP_HASH160 <PubK-Bob Hash> OP_EQUALVERIFY OP_CHECKSIG	

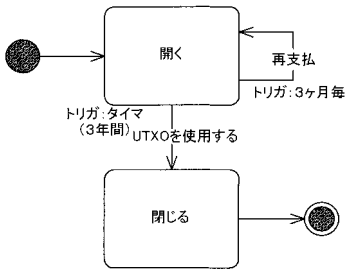
【図３Ｃ】

資産の公表	
ASSET-S2-T1	バージョン番号
Version number	
1	
BOB-S2-T1	
IDX-00	
Sig-Asset PubK-Asset	
2	
1,000	
Redeem Script: ボブ及び資産の両方に取り消しを要求する。	
OP_2AssetMetaDataA AssetMetadataB PubK-Asset PubK-Bob OP_4 OP_CHECKMULTISIG >>>	OP_HASH160<Redeem script hash>OP_EQUAL
	2,000
	OP_DUPOP HASH160 <PubK-AssetHash> OP EQUALVERIFY OP_CHECKSIG

【図３Ｄ】

取引閉鎖	
ASSET-S2-T2	トランザクションID
Version number	バージョン番号
1	インプット数
ASSET-S2-T1	前のトランザクションアウトプット
IDX-00	前のトランザクションアウトプットのインデックス
Script length	スクリプト長
Sig-Asset Sig-Bob OP_2 AssetMetaDataA AssetMetadataB PubK-Asset PubK-Bob OP_4 OP_CHECKMULTISIG	スクリプト署名
Sequence number	シーケンス番号
1	アウトプット数
1,000	アウトプット値
Output script length	アウトプットスクリプト長
OP_DUP OP_HASH160<PubK-Bob Hash>OP_EQUALVERIFY OP_CHECKSIG	アウトプットスクリプト
LockTime	ロック時間

【図４Ａ】



【図４Ｂ】

シナリオ定義
ボブ：３年間の期間、イブから車を借りている

賃貸借ベースメタデータ

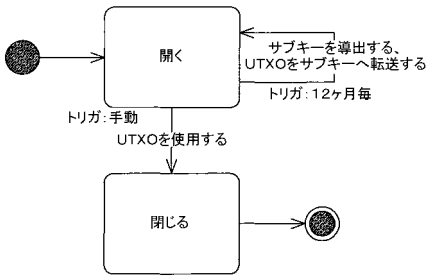
フィールド	サブフィールド	バイト	値	コメント
Asset Metadata A	ContractType	4	0x0000FF04	単位を示す
	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) xxxx	資産定義（Asset Definition）ファイルのアドレス
	Padding	12		予備
Asset Metadata B	ContractHash	20	################...	資産定義（Asset Definition）ファイルのハッシュ（トークン化ではない）
	Juristiction	2	EN	資産が英法によりカバーされることを指定する
	Options	2	0x0000	オプション指定なし
	Padding	8		予備

【図４Ｃ】

イブによる賃貸借取引の生成		
	EVE-S4-T1	トランザクションID
	Version number	バージョン番号
	1	インプット数
	<Eve's previous unspent BTC output - assume 500,000 satoshi>	前のトランザクションアウトプット
	IDX-00	前のアウトプットのインデックス
	Script length	スクリプト長
	Sig-Eve PubK-Eve	スクリプト署名
	Sequence number	シーケンス番号
	2	アウトプット数
	1,000	アウトプット値
Redeem Script: ボブ、イブ、独立計算エージェントのうち2つに解除を要求する	Output script length	アウトプットスクリプト長
OP_2AssetMetaDataA AssetMetadataB PubK-Eve PubK-Oracle OP_5 OP_CHECKMULTISIG	>>> OP_HASH160<Redeem script hash>OP_EQUAL	
	498,000	アウトプットスクリプト値
	Output script length	アウトプットスクリプト長
	OP_DUP OP_HASH160 <PubK-Eve Hash> OP_EQUALVERIFY OP_CHECKSIG	アウトプットスクリプト
	LockTime	ロック時間
	Eve's TimelockedRollon of the Contract	
	EVE-S4-T2	トランザクションID
	Version number	バージョン番号
	2	インプット数
	<Eve's mining fee of 1000 satoshi (note that no change can be given from this transaction because of the effect of the timelock) which means that she'll probably generate a previous transaction to get an input of the exact value>	前のトランザクションアウトプット
	IDX-00	前のアウトプットのインデックス
	Script length	スクリプト長
	Sig-Eve Sig-Bob OP_2AssetMetaDataA AssetMetadataB PubK-Bob PubK-Eve	スクリプト署名
	OP_5 OP_CHECKMULTISIG	
	Sequence number	シーケンス番号
	1	アウトプット数
	1,000	アウトプット値
Redeem Script: ボブ、イブの第2契約ロールオンサブキー、独立計算エージェントのうち2つに要求する	Output script length	アウトプットスクリプト長
OP_2AssetMetaDataA AssetMetadataB PubK-Bob PubK-Eve SKI PubK-Oracle OP_5 OP_CHECKMULTISIG	OP_HASH160 <redeem script hash> OP_EQUAL	アウトプットスクリプト
注：トランザクションは3年の期間の終了前の時間に提出される。	>>> Date when EVE-S4-T1 was transmitted plus 3 years	ロック時間

イブによる賃貸借取引の生成		
	EVE-S4-T1	トランザクションID
	Version number	バージョン番号
	1	インプット数
	<Eve's previous unspent BTC output - assume 500,000 satoshi>	前のトランザクションアウトプット
	IDX-00	前のアウトプットのインデックス
	Script length	スクリプト長
	Sig-Eve PubK-Eve	スクリプト署名
	Sequence number	シーケンス番号
	2	アウトプット数
	2,000	アウトプット値
Redeem Script: 単にイブが取引の閉鎖を要求する（ボブとイブの両者に要求するソリューションも可能であることに留意）	Output script length	アウトプットスクリプト長
OP_2AssetMetaDataA AssetMetadataB PubK-Eve OP_3 OP_CHECKMULTISIG	>>> OP_HASH160<Redeem script hash>OP_EQUAL	
	498,000	アウトプットスクリプト値
	Output script length	アウトプットスクリプト長
	OP_DUP OP_HASH160 <PubK-Eve Hash> OP_EQUALVERIFY OP_CHECKSIG	アウトプットスクリプト
	LockTime	ロック時間
	Eve's Timelocked Termination of the Contract	
	EVE-3-T2	トランザクションID
	Version number	バージョン番号
	1	インプット数
	EVE-3-T1	前のトランザクションアウトプット
	IDX-00	前のアウトプットのインデックス
	Script length	スクリプト長
	Sig-Eve OP_2AssetMetaDataA AssetMetadataB PubK-Eve OP_3 OP_CHECKMULTISIG	スクリプト署名
	Sequence number	シーケンス番号
	1	アウトプット数
	2,000	アウトプット値
	Output script length	アウトプットスクリプト長
	OP_DUP OP_HASH160<PubK-Eve Hash>OP_EQUALVERIFY OP_CHECKSIG	アウトプットスクリプト
注：トランザクションは3年の期間の終了前の時間に提出される。	>>> Date when EVE-S3-T1 was transmitted plus 3 years	ロック時間

【図５Ａ】



【図５Ｂ】

シナリオ定義
ボブ：年単位でイブから家を借りているが、契約応当日の2ヶ月以内に取り消し可能である

賃貸借ベースメタデータ

フィールド	サブフィールド	バイト	値	コメント
Asset Metadata A	ContractType	4	0x0000FF04	単位を示す
	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxxx	資産定義（Asset Definition）ファイルのアドレス
	Padding	12		予備
Asset Metadata B	ContractHash	20	################...	資産定義（Asset Definition）ファイルのハッシュ（トークン化ではない）
	Jurisdiction	2	EN	資産が英法によりカバーされることを指定する
	Options	2	0x0000	オプション指定なし
	Padding	8		予備

【図５Ｃ－１】

イブによる賃貸借取引の生成		
	EVE-S4-T1	トランザクションID
	Version number	バージョン番号
	1	インプット数
	<Eve's previous unspent BTC output - assume 500,000 satoshi>	前のトランザクションアウトプット
	IDX-00	前のアウトプットのインデックス
	Script length	スクリプト長
	Sig-Eve PubK-Eve	スクリプト署名
	Sequence number	シーケンス番号
	2	アウトプット数
	1,000	アウトプット値
Redeem Script: ボブ、イブ、独立計算エージェントのうち2つに解除を要求する	Output script length	アウトプットスクリプト長
OP_2AssetMetaDataA AssetMetadataB PubK-Bob PubK-Eve PubK-Oracle OP_5 OP_CHECKMULTISIG	>>> OP_HASH160<Redeem script hash>OP_EQUAL	
	498,000	アウトプットスクリプト値
	Output script length	アウトプットスクリプト長
	OP_DUP OP_HASH160 <PubK-Bob Hash> OP_EQUALVERIFY OP_CHECKSIG	アウトプットスクリプト
	LockTime	ロック時間
	Eve's TimelockedRollon of the Contract	
	EVE-S4-T2	トランザクションID
	Version number	バージョン番号
	2	インプット数
	<Eve's mining fee of 1000 satoshi (note that no change can be given from this transaction because of the effect of the timelock) which means that she'll probably generate a previous transaction to get an input of the exact value>	前のトランザクションアウトプット
	IDX-00	前のアウトプットのインデックス
	Script length	スクリプト長
	Sig-Eve Sig-Bob OP_2AssetMetaDataA AssetMetadataB PubK-Bob PubK-Eve	スクリプト署名
	OP_5 OP_CHECKMULTISIG	
	Sequence number	シーケンス番号
	1	アウトプット数
	1,000	アウトプット値
Redeem Script: ボブ、イブの第2契約ロールオンサブキー、独立計算エージェントのうち2つに要求する	Output script length	アウトプットスクリプト長
OP_2AssetMetaDataA AssetMetadataB PubK-Bob PubK-Eve SKI PubK-Oracle OP_5 OP_CHECKMULTISIG	OP_HASH160 <redeem script hash> OP_EQUAL	アウトプットスクリプト
注：トランザクションは3年の期間の終了前の時間に提出される。	>>> Date when EVE-S4-T1 was transmitted plus 1 year	ロック時間

【図５Ｃ－２】

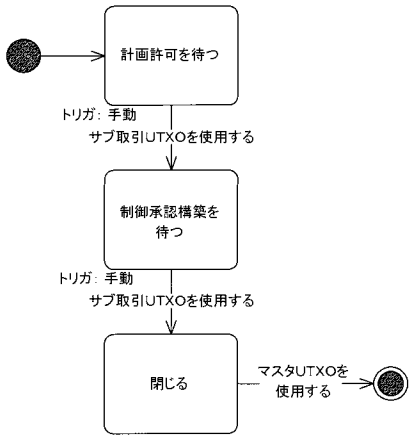
第1年の後、ボブは賃貸借を継続し終了しない。EVE-S3-T2の公表直後に、エージェント（oracle）により取り上げられ、もう1年ロールオンされる（これはイブ自身の内部ロジックを用いてイブにより行われることも可能であることに留意）

イブによる取引の時限付きロールオン		
	EVE-S4-T3	トランザクションID
	Version number	バージョン番号
	2	インプット数
	<Eve's mining fee of 1000 satoshi (note that no change can be given from this transaction) because of the effect of the timelock) which means that she'll probably generate a previous transaction to get an input of the exact value>	前のトランザクションアウトプット
	IDX-00	前のアウトプットのインデックス
	Script length	スクリプト長
	Sig-Eve PubK-Eve	スクリプト署名
	EVE-S4-T2	シーケンス番号
	IDX-00	前のアウトプットのインデックス
	Script length	スクリプト長
	Sig-EveSK1 Sig-Oracle OP_2AssetMetaDataA AssetMetadataB PubK-Bob PubK-EveSK1 PubK-Eve OP_5 OP_CHECKMULTISIG	スクリプト署名
	Sequence number	シーケンス番号
	1	アウトプット数
	1,000	アウトプット値
Redeem Script: ボブ、イブの第2契約ロールオンサブキー、独立エージェントのうち2つに解除を要求する	Output script length	アウトプットスクリプト長
OP_2AssetMetaDataA AssetMetadataB PubK-Bob PubK-EveSK1 PubK-Oracle OP_5 OP_CHECKMULTISIG	OP_HASH160 <redeem script hash> OP_EQUAL	アウトプットスクリプト
注：トランザクションは3年の期間の終了前の時間に提出される。	>>> Date when EVE-S4-T2 was transmitted plus 1 year	ロック時間

【図５Ｄ】

ボブによる取引閉鎖	
BOB-S4-T1	トランザクションID
Version number	バージョン番号
2	インプット数
<Bob's mining fee of 1000 satoshi (note that no change can be given from this transaction) because of the effect of the timelock) which means that she'll probably generate a previous transaction to get an input of the exact value>	前のトランザクション アウトプット
IDX-00	前のトランザクションアウトプットのインデックス
Script length	スクリプト長
Sig-Bob PubK-Bob	スクリプト署名
EVE-S4-T2	シーケンス番号
IDX-00	前のトランザクションアウトプットのインデックス
Script length	スクリプト長
Sig-Bob Sig-Oracle OP_2AssetMetaDataA AssetMetadataB PubK-Bob PubK-EveSK1 PubK-Eve OP_3 OP_CHECKMULTISIG	スクリプト署名
Sequence number	シーケンス番号
1	アウトプット数
1,000	アウトプット値
Output script length	アウトプットスクリプト長
OP_DUP OP_HASH160 <PubK-Eve Hash>OP_EQUALVERIFY OP_CHECKSIG	アウトプットスクリプト
LockTime	ロック時間

【図６Ａ】



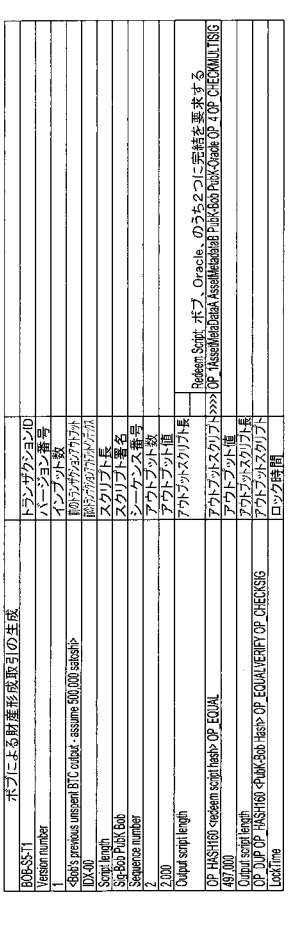
【図６Ｂ】

シナリオ定義
ボブ：　財産を形成しており、取引が満たされる前の過程の異なる時間に2つの独立した評価を必要とする（計画許可、及び認定構築）

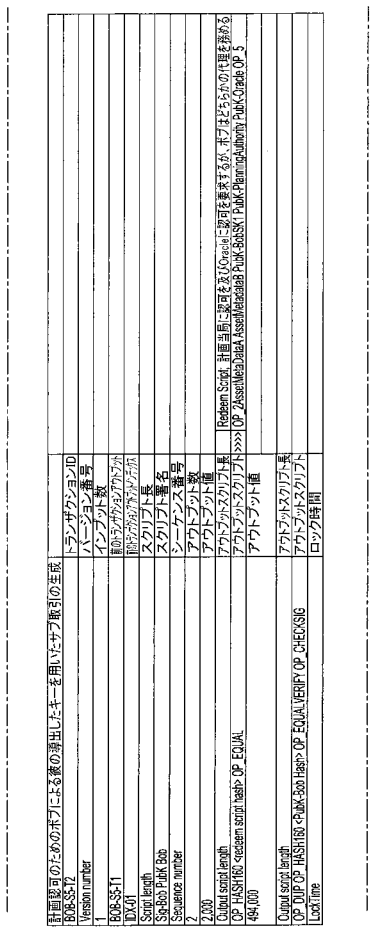
住宅ベースメタデータ

フィールド	サブフィールド	バイト	値	コメント
Asset Metadata A	ContractType	4	0x0000FF04	単位を示す
	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxxx	資産定義（Asset Definition）ファイルのアドレス
	Padding	12		予備
Asset Metadata B	ContractHash	20	##################...	資産定義（Asset Definition）ファイルのハッシュ（トークン化ではない）
	Jurisdiction	2	EN	資産が英法によりカバーされることを指定する
	Options	2	0x0000	オプション指定なし
	Padding	8		予備

【図６Ｃ－１】



【図６Ｃ－２】



【図６Ｃ－３】

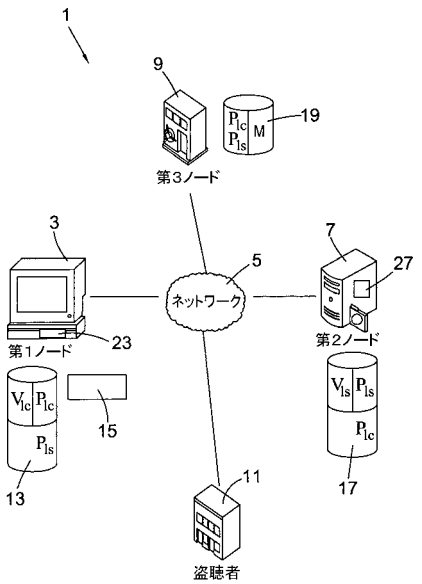
構築記号構築を確認するための秘匿による後の導出したキーを用いたサブ取引の生成	トランザクションID
BOB-SS-T3	バージョン番号
Version number	インプット数
1	前のトランザクションアウトプット
BOB-SS-T2	前のスクリプトアウトプットインデックス
IDX-01	スクリプト長
Script length	スクリプト署名
Sig-Bob PubK Bob	シーケンス番号
Sequence number	アウトプット数
2	アウトプット値
2,000	アウトプットスクリプト長
Output script length	アウトプットスクリプト
OP_HASH160 <redeem script hash> OP_EQUAL	アウトプットスクリプト数
491,000	アウトプット値
Output script length	アウトプットスクリプト長
OP_DUP OP_HASH160 <PubK-Bob Hash> OP_EQUALVERIFY OP_CHECKSIG	アウトプットスクリプト
LockTime	ロック時間

【図６Ｄ】

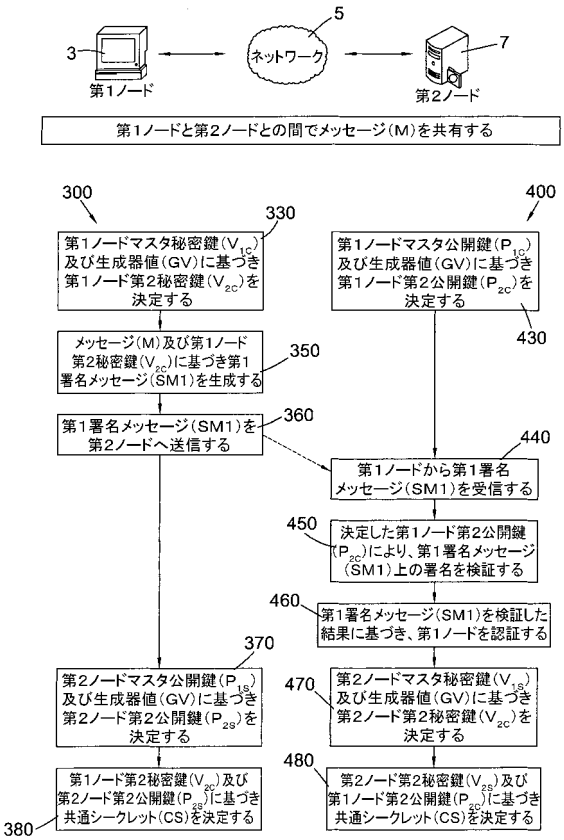
計画当局が承認する	トランザクションID
BOB-SS-T4	バージョン番号
Version number	インプット数
1	前のトランザクションアウトプット
BOB-SS-T2	前のスクリプトアウトプットインデックス
IDX-00	スクリプト長
Script length	スクリプト署名
Sig-PlanningAuthority Sig-Oracle OP_2AssetMetaDataA AssetMetadateB PubK-BobSK1 PubK-PlanningAuthority PubK-Oracle OP_5 OP_CHECKMULTISIG	シーケンス番号
Sequence number	アウトプット数
1	アウトプット値
1,000	アウトプットスクリプト長
Output script length	アウトプットスクリプト
OP_DUP OP_HASH160<PubK-PlanningAuthority Hash>OP_EQUALVERIFY OP_CHECKSIG	<<<<
LockTime	ロック時間

注：
ナトシは計画当局に手数料を支払う（Oracleと計画当局の両者に2つのアウトプットモデルが存在し得ることに留意）

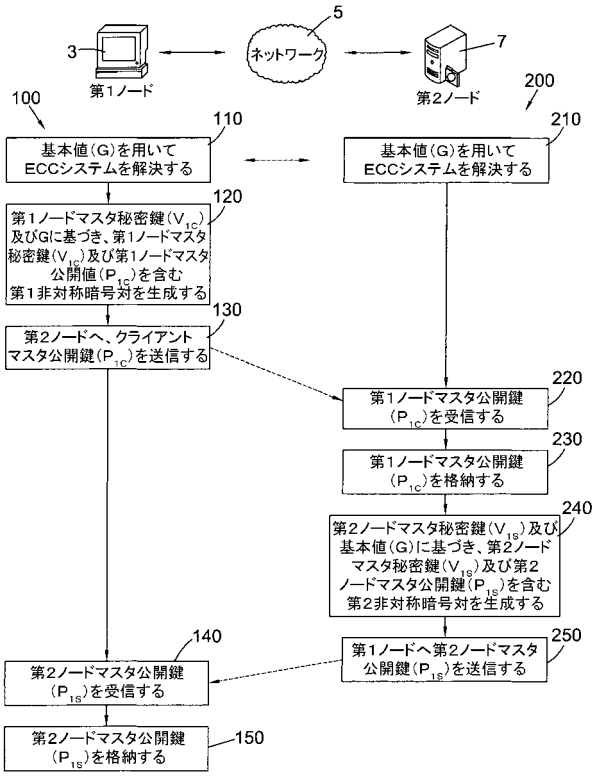
【図７】



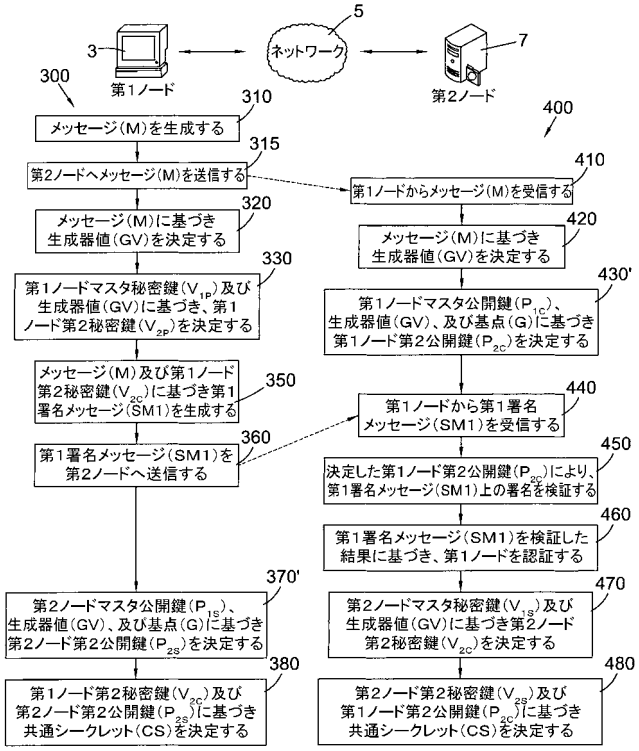
【図８】



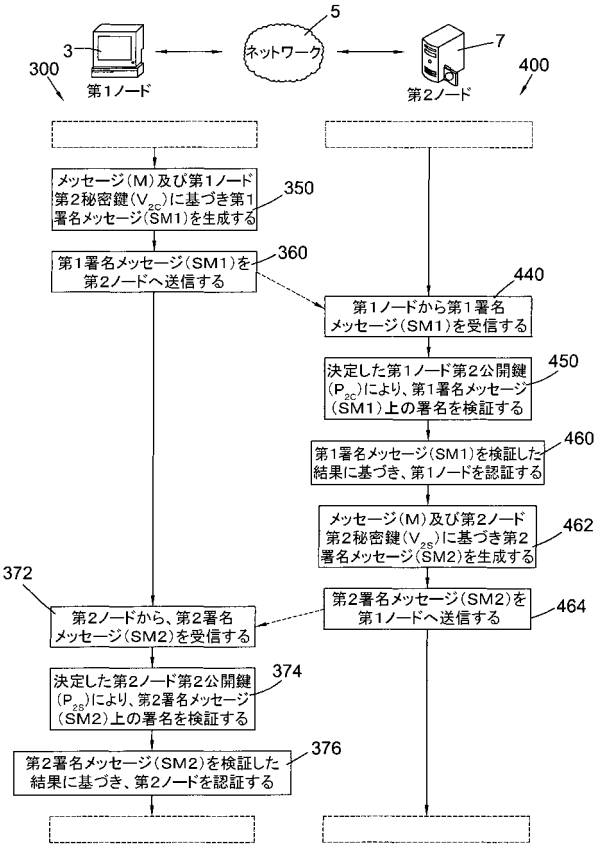
【図９】



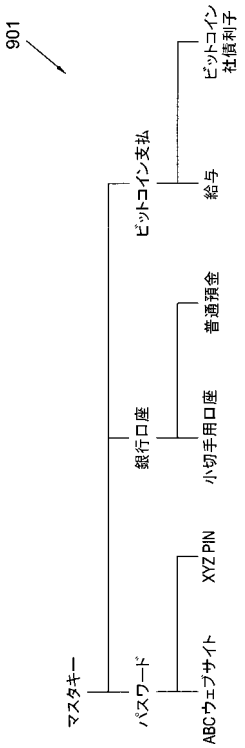
【図１０】



【図１１】



【図１２】



【図１３】

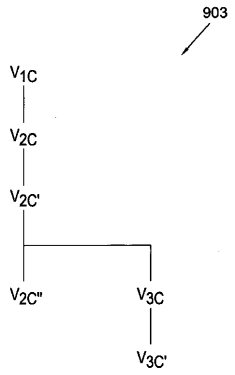


Fig. 13

【誤訳訂正書】
【提出日】平成31年3月20日(2019.3.20)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
取引の可視性及び／又は実行を制御するコンピュータにより実施される方法であって、前記方法は、
（ａ）コンピュータに基づくレポジトリ上に又はその中に取引を格納するステップと、
（ｂ）ブロックチェーンにトランザクションをブロードキャストするステップであって、前記トランザクションは、
ｉ）少なくとも１つの未使用アウトプット（ＵＴＸＯ）、及び、
ｉｉ）前記取引の格納された場所を示す識別子を有するメタデータ、を有する、ステップと、
（ｃ）前記未使用アウトプット（ＵＴＸＯ）が前記ブロックチェーン上で使用されるまで、前記取引を公開又は有効として解釈するステップと、
（ｄ）前記取引を、
前記取引に関連付けられた前のキーに関連するデータを用いて、新しいキーを生成し、
前記新しいキー、前記取引の前記場所、前記取引のハッシュを有するスクリプトを生成し、
前記スクリプトに通貨額を支払う、

ことにより、更新する又はロールオンするステップと、
を含む方法。
【請求項２】
前記トランザクションは、決定性ＲｅｄｅｅｍＳｃｒｉｐｔアドレスを更に有し、望ましくは、前記決定性ＲｅｄｅｅｍＳｃｒｉｐｔアドレスはＰ２ＳＨ（pay－to－script－hash）アドレスである、請求項１に記載の方法。
【請求項３】
前記未使用アウトプット（ＵＴＸＯ）を使用するために前記ブロックチェーンに更なるトランザクションをブロードキャストすることにより、前記取引を終了するステップ、を更に含む請求項２に記載の方法。
【請求項４】
前記更なるトランザクションは、
前記未使用アウトプット（ＵＴＸＯ）であるインプット、及び、
署名と前記メタデータと公開鍵とを含むアンロックスクリプト、を有する、請求項３に記載の方法。
【請求項５】
前記取引は、
ｉ）少なくとも１つの条件、及び、
ｉｉ）前記条件の評価に実行が依存する少なくとも１つのアクション、を定め、
前記メタデータは、
ｉ）前記取引が前記コンピュータに基づくレポジトリに格納された場所のアドレス又はアドレスの提示、及び／又は、
ｉｉ）前記取引のハッシュ、を有する、
請求項１乃至４のいずれか一項に記載の方法。
【請求項６】
前記未使用アウトプット（ＵＴＸＯ）が前記ブロックチェーンの未使用トランザクションアウトプットのリストの中にあるか否かを決定することにより、前記取引が終了しているか否かを調べるステップ、を含む請求項１乃至５のいずれか一項に記載の方法。
【請求項７】
ｉ）前記取引は分散ハッシュテーブル（ＨＤＴ）に格納され、及び／又は、
ｉｉ）前記方法は、
指定日及び／又は時間に前記未使用アウトプット（ＵＴＸＯ）を使用する指示を有するトランザクションを前記ブロックチェーンにブロードキャストするステップであって、望ましくは前記指示はＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ指示である、ステップ、を含む、
請求項１乃至６のいずれか一項に記載の方法。
【請求項８】
ｉ）前記取引の内容のうちの一部又は全部へのアクセスは、少なくとも１つの指定認定パーティに制限され、
ｉｉ）前記取引は、前記取引を実施する決定性有限オートマトン（ＤＦＡ）を有し、
望ましくは、前記決定性有限オートマトンは、コード化スキームを用いて定められる、
請求項１乃至７のいずれか一項に記載の方法。
【請求項９】
前記決定性有限オートマトンは、
ｉ）望ましくはスクリプト言語を用いる少なくとも１つのブロックチェーントランザクション、
ｉｉ）前記ブロックチェーンの状態を監視するよう構成された計算エージェント、及び／又は、
ｉｉｉ）デジタルウォレットのための指示セット、
を用いて実施される、請求項８に記載の方法。

【請求項１０】
取引の可視性及び／又は実行を制御するコンピュータにより実施される方法であって、前記方法は、
（ａ）コンピュータに基づくレポジトリ上に又はその中に取引を格納するステップと、
（ｂ）ブロックチェーンにトランザクションをブロードキャストするステップであって、前記トランザクションは、
ｉ）少なくとも１つの未使用アウトプット（ＵＴＸＯ）、及び、
ｉｉ）前記取引の格納された場所を示す識別子を有するメタデータ、を有する、ステップと、
（ｃ）前記未使用アウトプット（ＵＴＸＯ）が前記ブロックチェーン上で使用されるまで、前記取引を公開又は有効として解釈するステップと、
（ｄ）前記取引から導出されるサブ取引を生成するステップであって、前記サブ取引は、決定性アドレスに関連付けられ、
ｉｉｉ）シードを用いて導出された新しい公開鍵を用いて、
ｉｖ）前記取引への参照と共に前記レポジトリ上に又はその中に前記サブ取引を格納し、前記参照を含むスクリプトを有するトランザクションを前記ブロックチェーンにブロードキャストし、及び／又は、
ｖ）既存の取引のメタデータに前記サブ取引への参照を追加する、
ことにより生成される、ステップと、
を含む方法。
【請求項１１】
前記トランザクションは、決定性ＲｅｄｅｅｍＳｃｒｉｐｔアドレスを更に有し、望ましくは、前記決定性ＲｅｄｅｅｍＳｃｒｉｐｔアドレスはＰ２ＳＨ（pay－to－script－hash）アドレスである、請求項１０に記載の方法。
【請求項１２】
前記未使用アウトプット（ＵＴＸＯ）を使用するために前記ブロックチェーンに更なるトランザクションをブロードキャストすることにより、前記取引を完了するステップ、を更に含み、
望ましくは、前記更なるトランザクションは、
前記未使用アウトプット（ＵＴＸＯ）であるインプット、及び、
署名と前記メタデータと公開鍵とを含むアンロックスクリプト、を有する、
請求項１１に記載の方法。
【請求項１３】
ｉ）前記取引は、
ａ）少なくとも１つの条件、及び、
ｂ）前記条件の評価に実行が依存する少なくとも１つのアクション、を定め、及び／又は、
ｉｉ）前記メタデータは、
ａ）前記取引が前記コンピュータに基づくレポジトリに格納された場所のアドレス又はアドレスの提示、及び／又は、
ｂ）前記取引のハッシュ、を有する、
請求項１０乃至１２のいずれか一項に記載の方法。
【請求項１４】
前記未使用アウトプット（ＵＴＸＯ）が前記ブロックチェーンの未使用トランザクションアウトプットのリストの中にあるか否かを決定することにより、前記取引が終了しているか否かを調べるステップ、を含む請求項１０乃至１３のいずれか一項に記載の方法。
【請求項１５】
前記取引は分散ハッシュテーブル（ＨＤＴ）に格納される、請求項１０乃至１４のいずれか一項に記載の方法。
【請求項１６】

指定日及び／又は時間に前記未使用アウトプット（ＵＴＸＯ）を使用する指示を有するトランザクションを前記ブロックチェーンにブロードキャストするステップであって、望ましくは前記指示はＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ指示である、ステップ、を含む請求項１０乃至１５のいずれか一項に記載の方法。

【請求項１７】

ｉ）前記取引の内容のうちの一部又は全部へのアクセスは、少なくとも１つの指定認定パーティに制限され、及び／又は、

ｉｉ）前記取引は、前記取引を実施する決定性有限オートマトン（ＤＦＡ）を有し、

望ましくは、

前記決定性有限オートマトンは、コード化スキームを用いて定められる、及び／又は、

前記決定性有限オートマトンは、

ｉ）望ましくはスクリプト言語を用いる少なくとも１つのブロックチェーントランザクション、

ｉｉ）前記ブロックチェーンの状態を監視するよう構成された計算エージェント、及び／又は、

ｉｉｉ）デジタルウォレットのための指示セット、

を用いて実施される、

請求項１０乃至１６のいずれか一項に記載の方法。

【請求項１８】

請求項１乃至１７のいずれか一項に記載の方法を実行するよう構成されたシステム。

【誤訳訂正２】

【訂正対象書類名】明細書

【訂正対象項目名】００２７

【訂正方法】変更

【訂正の内容】

【００２７】

取引は、取引を実施するために決定性有限オートマトン（Deterministic Finite Automaton：ＤＦＡ）を有して良い。決定性有限オートマトンは、コード化スキームを用いて定められて良い。決定性有限オートマトンは、

ｉ）望ましくはスクリプト言語を用いる、少なくとも１つのブロックチェーントランザクション、

ｉｉ）ブロックチェーンの状態を監視するよう構成された計算エージェント（これは、以下の「本発明と共に使用するための説明のための計算エージェント」と題される章に記載され得る）、及び／又は、

ｉｉｉ）デジタルウォレットに対する指示セット、を用いて実施されて良い。

【誤訳訂正３】

【訂正対象書類名】明細書

【訂正対象項目名】００５３

【訂正方法】変更

【訂正の内容】

【００５３】

＜取引モデル＞

取引モデルの基本要素は以下の通りである：

・コード化スキームは、任意の種類の取引の完全な記述を可能にする。スキームは、新しい構成であって良く、又はＸＢＲＬ、ＸＭＬ、ＪＳＯＮ（等）のような既存の設備を使用して良い。

・取引を実施するためのＤＦＡ（決定性有限オートマトン、Deterministic Finite Automaton）は、コード化スキームの中で完全に定義できる。これは、以下から構成される。

－　パラメータのセット、これのパラメータを供給すべき場所、

－　状態定義のセット、

－　遷移のトリガ及び遷移中に従うルールを含む、状態間の遷移のセット、
－　ルール定義テーブル。
・取引のこのインスタンスのための特定パラメータの定義。
・取引を安全に保管し保護するためのメカニズム。
・取引を、正式な法律の言語で人間に可読にする「ブラウザ」。
・コード化スキームをオラクルコード及び／又はビットコインスクリプトのようなスクリプトに変換する「コンパイラ」。
【手続補正書】
【提出日】平成30年9月11日(2018.9.11)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
取引の可視性及び／又は実行を制御するコンピュータにより実施される方法であって、前記方法は、
（ａ）コンピュータに基づくレポジトリ上に又はその中に取引を格納するステップと、
（ｂ）ブロックチェーンにトランザクションをブロードキャストするステップであって、前記トランザクションは、
ｉ）少なくとも１つの未使用アウトプット（ＵＴＸＯ）、及び、
ｉｉ）前記取引の格納された場所を示す識別子を有するメタデータ、を有する、ステップと、
（ｃ）前記未使用アウトプット（ＵＴＸＯ）が前記ブロックチェーン上で使用されるまで、前記取引を公開又は有効として解釈するステップと、
（ｄ）前記取引を、
前記取引に関連付けられた前のキーに関連するデータを用いて、新しいキーを生成し、
前記新しいキー、前記取引の前記場所、前記取引のハッシュを有するスクリプトを生成し、
前記スクリプトに通貨額を支払う、
ことにより、更新する又はロールオンするステップと、
を含む方法。
【請求項２】
前記トランザクションは、決定性ＲｅｄｅｅｍＳｃｒｉｐｔアドレスを更に有し、望ましくは、前記ＲｅｄｅｅｍＳｃｒｉｐｔアドレスはＰ２ＳＨ（pay－to－script－hash）アドレスである、請求項１に記載の方法。
【請求項３】
前記アウトプット（ＵＴＸＯ）を使用するために前記ブロックチェーンに更なるトランザクションをブロードキャストすることにより、前記取引を終了するステップ、を更に含む請求項２に記載の方法。
【請求項４】
前記更なるトランザクションは、
前記アウトプット（ＵＴＸＯ）であるインプット、及び、
署名と前記メタデータと公開鍵とを含むアンロックスクリプト、を有する、請求項３に記載の方法。
【請求項５】
前記取引は、
ｉ）少なくとも１つの条件、及び、

ｉｉ）前記条件の評価に実行が依存する少なくとも１つのアクション、を定め、
前記メタデータは、
ｉ）前記取引が前記コンピュータに基づくレポジトリに格納された場所のアドレス又はアドレスの提示、及び／又は、
ｉｉ）前記取引のハッシュ、を有する、
請求項１乃至４のいずれか一項に記載の方法。
【請求項６】
前記未使用トランザクションＵＴＸＯが前記ブロックチェーンの未使用トランザクションアウトプットのリストの中にあるか否かを決定することにより、前記取引が終了しているか否かを調べるステップ、を含む請求項１乃至５のいずれか一項に記載の方法。
【請求項７】
ｉ）前記取引は分散ハッシュテーブル（ＨＤＴ）に格納され、及び／又は、
ｉｉ）前記方法は、
指定日及び／又は時間に前記アウトプットを使用する指示を有するトランザクションを前記ブロックチェーンにブロードキャストするステップであって、望ましくは前記指示はＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ指示である、ステップ、を含む、
請求項１乃至６のいずれか一項に記載の方法。
【請求項８】
ｉ）前記取引の内容のうちの一部又は全部へのアクセスは、少なくとも１つの指定認定パーティに制限され、
ｉｉ）前記取引は、前記取引を実施する決定性有限オートマン（ＤＦＡ）を有し、
望ましくは、前記決定性有限オートマンは、コード化スキームを用いて定められる、
請求項１乃至７のいずれか一項に記載の方法。
【請求項９】
前記決定性有限オートマンは、
ｉ）望ましくはスクリプト言語を用いる少なくとも１つのブロックチェーントランザクション、
ｉｉ）前記ブロックチェーンの状態を監視するよう構成された計算エージェント、及び／又は、
ｉｉｉ）デジタルウォレットのための指示セット、
を用いて実施される、請求項８に記載の方法。
【請求項１０】
取引の可視性及び／又は実行を制御するコンピュータにより実施される方法であって、前記方法は、
（ａ）コンピュータに基づくレポジトリ上に又はその中に取引を格納するステップと、
（ｂ）ブロックチェーンにトランザクションをブロードキャストするステップであって、前記トランザクションは、
ｉ）少なくとも１つの未使用アウトプット（ＵＴＸＯ）、及び、
ｉｉ）前記取引の格納された場所を示す識別子を有するメタデータ、を有する、ステップと、
（ｃ）前記未使用アウトプット（ＵＴＸＯ）が前記ブロックチェーン上で使用されるまで、前記取引を公開又は有効として解釈するステップと、
（ｄ）前記取引から導出されるサブ取引を生成するステップであって、前記サブ取引は、決定性アドレスに関連付けられ、
ｉｉｉ）シードを用いて導出された新しい公開鍵を用いて、
ｉｖ）前記取引への参照と共に前記レポジトリ上に又はその中に前記サブ取引を格納し、前記参照を含むスクリプトを有するトランザクションを前記ブロックチェーンにブロードキャストし、及び／又は、
ｖ）既存の取引のメタデータに前記サブ取引への参照を追加する、
ことにより生成される、ステップと、

を含む方法。
【請求項１１】
前記トランザクションは、決定性ＲｅｄｅｅｍＳｃｒｉｐｔアドレスを更に有し、望ましくは、前記ＲｅｄｅｅｍＳｃｒｉｐｔアドレスはＰ２ＳＨ（pay－to－script－hash）アドレスである、請求項１０に記載の方法。
【請求項１２】
前記アウトプット（ＵＴＸＯ）を使用するために前記ブロックチェーンに更なるトランザクションをブロードキャストすることにより、前記取引を完了するステップ、を更に含み、
望ましくは、前記更なるトランザクションは、
前記アウトプット（ＵＴＸＯ）であるインプット、及び、
署名と前記メタデータと公開鍵とを含むアンロックスクリプト、を有する、
請求項１１に記載の方法。
【請求項１３】
ｉ）前記取引は、
ａ）少なくとも１つの条件、及び、
ｂ）前記条件の評価に実行が依存する少なくとも１つのアクション、を定め、及び／又は、
ｉｉ）前記メタデータは、
ａ）前記取引が前記コンピュータに基づくレポジトリに格納された場所のアドレス又はアドレスの提示、及び／又は、
ｂ）前記取引のハッシュ、を有する、
請求項１０乃至１２のいずれか一項に記載の方法。
【請求項１４】
前記未使用アウトプットＵＴＸＯが前記ブロックチェーンの未使用トランザクションアウトプットのリストの中にあるか否かを決定することにより、前記取引が終了しているか否かを調べるステップ、を含む請求項１０乃至１３のいずれか一項に記載の方法。
【請求項１５】
前記取引は分散ハッシュテーブル（ＨＤＴ）に格納される、請求項１０乃至１４のいずれか一項に記載の方法。
【請求項１６】
指定日及び／又は時間に前記アウトプットを使用する指示を有するトランザクションを前記ブロックチェーンにブロードキャストするステップであって、望ましくは前記指示はＣｈｅｃｋＬｏｃｋＴｉｍｅＶｅｒｉｆｙ指示である、ステップ、を含む請求項１０乃至１５のいずれか一項に記載の方法。
【請求項１７】
ｉ）前記取引の内容のうちの一部又は全部へのアクセスは、少なくとも１つの指定認定パーティに制限され、及び／又は、
ｉｉ）前記取引は、前記取引を実施する決定性有限オートマン（ＤＦＡ）を有し、
望ましくは、
前記決定性有限オートマンは、コード化スキームを用いて定められる、及び／又は、
前記決定性有限オートマンは、
ｉ）望ましくはスクリプト言語を用いる少なくとも１つのブロックチェーントランザクション、
ｉｉ）前記ブロックチェーンの状態を監視するよう構成された計算エージェント、及び／又は、
ｉｉｉ）デジタルウォレットのための指示セット、
を用いて実施される、
請求項１０乃至１６のいずれか一項に記載の方法。
【請求項１８】

請求項１乃至１７のいずれか一項に記載の方法を実行するよう構成されたシステム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2017/050865

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00 G06Q30/06 G06Q20/36
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2015/206106 A1 (YAGO YARON EDAN [US]) 23 July 2015 (2015-07-23) paragraphs [0007], [0042], [0047], [0051], [0066], [0069], [0070] figures 5, 7 -----	1-27
A	Andreas M. Antonopoulos: "Mastering Bitcoin - Unlocking Digital Cryptocurrencies" In: "Mastering bitcoin : [unlocking digital cryptocurrencies]", 20 December 2014 (2014-12-20), O'Reilly Media, Beijing Cambridge Farnham Köln Sebastopol Tokyo, XP055306939, ISBN: 978-1-4493-7404-4 page 22 - page 25 page 113 - page 117 -----	1-27

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 April 2017	26/04/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Volpato, Gian Luca

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2017/050865

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015206106 A1	23-07-2015	US 2015206106 A1	23-07-2015
		WO 2015106285 A1	16-07-2015

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(31)優先権主張番号 1603117.1
(32)優先日 平成28年2月23日(2016.2.23)
(33)優先権主張国 英国(GB)
(31)優先権主張番号 1603114.8
(32)優先日 平成28年2月23日(2016.2.23)
(33)優先権主張国 英国(GB)
(31)優先権主張番号 1605571.7
(32)優先日 平成28年4月1日(2016.4.1)
(33)優先権主張国 英国(GB)
(31)優先権主張番号 1619301.3
(32)優先日 平成28年11月15日(2016.11.15)
(33)優先権主張国 英国(GB)

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ

（特許庁注：以下のものは登録商標）
１．ＵＮＩＸ

(74)代理人 100070150
弁理士 伊東 忠彦
(74)代理人 100091214
弁理士 大貫 進介
(72)発明者 ライト, クレイグ スティーヴン
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー 内
(72)発明者 サヴァナ, ステファヌ
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー 内

Ｆターム(参考) 5J104 AA07 AA08 AA16 EA23 JA25 KA02 KA05 LA01 LA03 NA02
NA12 NA37 PA07 PA10
5L049 BB21
5L055 AA12

【要約の続き】
明なので、これは、永久的に、公に可視の且つ変更不可能な、取引のレコードを提供する。