(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7646570号
(P7646570)

(45)発行日　令和7年3月17日(2025.3.17)

(24)登録日　令和7年3月7日(2025.3.7)

(51)国際特許分類		FI		
H04L	*9/32 (2006.01)*	H04L	9/32	200Z
G06Q	*30/0645(2023.01)*	G06Q	30/0645	
G06Q	*50/06 (2024.01)*	G06Q	50/06	
G06Q	*50/26 (2024.01)*	G06Q	50/26	

請求項の数　35　（全63頁）

(21)出願番号　特願2021-567834(P2021-567834)
(86)(22)出願日　令和2年4月22日(2020.4.22)
(65)公表番号　特表2022-532886(P2022-532886A)
(43)公表日　令和4年7月20日(2022.7.20)
(86)国際出願番号　PCT/IB2020/053815
(87)国際公開番号　WO2020/240297
(87)国際公開日　令和2年12月3日(2020.12.3)
審査請求日　令和5年3月24日(2023.3.24)
(31)優先権主張番号　1907339.4
(32)優先日　令和1年5月24日(2019.5.24)
(33)優先権主張国・地域又は機関
英国(GB)

(73)特許権者　318001991
エヌチェーン ライセンシング アーゲー
スイス・６３００・ツーク・グラーフェナウヴェーク・６
(74)代理人　100107766
弁理士　伊東 忠重
(74)代理人　100070150
弁理士　伊東 忠彦
(74)代理人　100135079
弁理士　宮崎 修
(72)発明者　ジャーン，ウエイ
イギリス ダブリュー１ダブリュー ８エーピー ロンドン マーケット プレイス ３０ エヌチェーン ホールディングズ リミテッド 内

最終頁に続く

(54)【発明の名称】　ブロックチェーンへの包含のためのトランザクションの適応性

(57)【特許請求の範囲】

【請求項１】

第１パーティと第２パーティとの間のターゲットトランザクションをブロックチェーンに送信する方法であって、前記方法は、前記第１パーティ及び前記第２パーティのコンピュータ機器により、

前記ターゲットトランザクションの既存の第１バージョンに対して更新されている、前記ターゲットトランザクションの第２の更新バージョンを取得するステップと、

ノードのネットワークを通じて伝播されるように、前記第１バージョンの代わりに、前記ターゲットトランザクションの前記更新バージョンを送信するステップであって、それにより、前記ターゲットトランザクションを、前記ノードのうちの少なくとも幾つかの各々において維持されるブロックチェーンのコピーに記録させる、ステップと、

を含み、

前記ターゲットトランザクションは、アンロックスクリプトと、第１トランザクションの第１アウトプットへのポインタと、を含むインプットを含み、前記第１アウトプットは、前記第１トランザクションの前記第１アウトプットをアンロックするための複数の代替条件を指定するロックスクリプトを含み、

前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記代替条件のうちの第１条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成され、前記更新バージョンの前記アンロックスクリプトは、前記第１条件の代わりに、前記代替条件のうちの第２条件を満たすこと

に基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成される、方法。
【請求項２】
前記第２パーティのコンピュータ機器により、前記ネットワークを通じて伝播され前記第１条件を満たすことに基づき前記ブロックチェーンに記録されるよう、前記第２パーティが前記ターゲットトランザクションの前記第１バージョンを送信できるようにする機能を提供するステップ、を含む請求項１に記載の方法。
【請求項３】
前記機能は、前記第２パーティに、前記第１バージョンの送信を実行することを手動で選択するためのオプションを提供し、及び／又は、
前記機能は、所定の時間の終了後に又は所定のイベントにより、前記ターゲットトランザクションの前記第１バージョンの送信を自動的にトリガするよう構成される、
請求項２に記載の方法。
【請求項４】
前記ターゲットトランザクションの前記更新バージョンを取得すること、及び伝播され前記ブロックチェーンに記録されるよう該更新バージョンを送信することは、前記第２パーティのコンピュータ機器により実行される、請求項１～３のいずれかに記載の方法。
【請求項５】
前記第２の更新バージョンを取得するステップは、第１パーティから前記第２の更新バージョンの少なくとも部分を受信するステップを含む、請求項４に記載の方法。
【請求項６】
前記第２パーティのコンピュータ機器により、
前記ターゲットトランザクションの前記第１バージョンを取得するステップであって、前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記第２パーティが、前記第１条件を満たすことに基づき前記第１トランザクションの前記第１アウトプットを自動的にアンロックできるように構成される、ステップ、を含む請求項１～５のいずれかに記載の方法。
【請求項７】
前記ターゲットトランザクションの前記第２の更新バージョンは、前記第１バージョンの後に取得される、請求項６に記載の方法。
【請求項８】
前記第１バージョンを取得するステップは、前記第１パーティから前記第１バージョンの少なくとも部分を受信するステップを含む、請求項６又は７に記載の方法。
【請求項９】
前記第１バージョンを取得するステップは、前記第２パーティが前記第１トランザクションを生成するステップを含む、請求項６、７又は８に記載の方法。
【請求項１０】
前記第２条件は、前記アンロックスクリプトが、前記アンロックスクリプト以外の前記ターゲットトランザクションの部分に署名する前記第１パーティの暗号署名を含むこと、前記ターゲットトランザクションの前記更新バージョンを取得するステップが前記第１パーティの前記署名を取得することを含むこと、及び伝播され前記ブロックチェーンに記録されるよう送信される前記更新バージョンが、前記アンロックスクリプト内に前記第１パーティの前記署名を含むこと、を要求する、請求項１～９のいずれかに記載の方法。
【請求項１１】
前記第１条件は、前記第１パーティの暗号署名を要求しない、請求項１０に記載の方法。
【請求項１２】
少なくとも前記第１条件は、前記アンロックスクリプトが、前記アンロックスクリプト以外の前記ターゲットトランザクションの部分に署名する前記第２パーティの暗号署名を含むことを要求する、請求項１０又は１１に記載の方法。
【請求項１３】

前記第２条件は、前記アンロックスクリプトが、前記アンロックスクリプト以外の前記ターゲットトランザクションの部分に署名する前記第２パーティの暗号署名を含むことを更に要求し、
伝播され前記ブロックチェーンに記録されるよう送信される前記更新バージョンは、前記アンロックスクリプト内に前記第２パーティの前記暗号署名を含む、請求項１２に記載の方法。
【請求項１４】
前記更新バージョンを取得するステップは、
前記第２パーティが前記第１バージョンを前記第１パーティへ送信するステップであって、前記第１パーティが前記第１パーティの署名を追加することにより、前記更新バージョンに統合できるようにする、ステップを含み、
前記第１条件及び前記第２条件は、前記第２パーティの同じ署名が前記ターゲットトランザクションの同じ部分に署名することを要求し、前記第２パーティが前記更新バージョンに再び署名する必要がない、請求項６に従属する請求項１２又は１３に記載の方法。
【請求項１５】
前記第１条件は、データペイロードがアンロックスクリプトに含まれることを要求するが、前記第２条件は、前記データペイロードが前記ターゲットトランザクションに含まれることを要求せず、
前記ネットワークを介して伝播され前記ブロックチェーンに記録されるよう送信される前記更新バージョンは、前記データペイロードを含まない、請求項１～１３のいずれかに記載の方法。
【請求項１６】
前記第１条件は、前記アンロックスクリプトが、前記データペイロードと、前記アンロックスクリプト以外の前記ターゲットトランザクションの部分に署名する前記第２パーティの暗号署名と、を含むことを要求するが、前記第１パーティの暗号署名が前記ターゲットトランザクションに含まれることを要求せず、
前記第２条件は、前記アンロックスクリプトが、前記第１パーティ及び前記第２パーティの両者の暗号署名を含むことを要求するが、前記データペイロードが前記ターゲットトランザクションに含まれることを要求せず、
前記ターゲットトランザクションの前記更新バージョンを取得するステップは、前記第１パーティの前記署名を取得するステップを含み、
伝播され前記ブロックチェーンに記録されるよう送信される前記ターゲットトランザクションの前記更新バージョンは、前記データペイロードを含まないが、前記アンロックスクリプト内の前記第１パーティ及び前記第２パーティの署名を含む、請求項１５に記載の方法。
【請求項１７】
前記第１トランザクションの前記第１アウトプットは、前記第１条件又は前記第２条件に従い前記第１アウトプットをアンロックすることにより償還される、前記第２パーティへの支払いを指定し、
前記ターゲットトランザクションは、前記支払いの少なくとも一部を前記第２パーティへ移転するアウトプットを含む、請求項１～１５のいずれかに記載の方法。
【請求項１８】
前記第２パーティの前記コンピュータ機器により、
前記第１パーティへデータ部分のシーケンスをストリーミングするステップであって、前記シーケンスの中の最終部分により終了する、ステップと、
前記データ部分のうちのそれぞれの部分に応答して、前記第１パーティから前記第１トランザクションのそれぞれのインスタンスを受信するステップであって、各インスタンスの第１アウトプットは、前記それぞれの部分についての前記第２パーティへの支払いを指定する、ステップと、
を含み

前記支払いは各データ部分と共に増大し、
前記ターゲットトランザクションの前記更新バージョンを取得するステップは、前記シーケンスの中の前記最終部分に続き、前記第１パーティから前記更新バージョンを受信するステップを含む、請求項１７に記載の方法。
【請求項１９】
前記増大は、それまでに送信されたデータ部分の数に線形に比例する、請求項１８に記載の方法。
【請求項２０】
各データ部分は、メディアコンテンツのアイテムの異なる部分である、請求項１８又は１９に記載の方法。
【請求項２１】
各データ部分はサービスのユニットにアクセスするための異なる鍵である、請求項１８又は１９に記載の方法。
【請求項２２】
前記サービスは、
電気、ガス、又は水道を含む生活必需サービスの提供、又は、
不動産、車両、又は別の物理アイテムのレンタル、
のうちの１つを含む、請求項２１に記載の方法。
【請求項２３】
前記機能は、前記第２パーティに、前記シーケンスの中の任意のポイントにおいて、それまでに前記第１パーティから受信した前記シーケンスの中の前記第１トランザクションの最新のインスタンスを償還するために、前記ネットワークを通じて伝播されブロックチェーンに記録されるよう前記ターゲットトランザクションの前記第１バージョンの送信を実行することを手動で選択するオプションを提供し、及び／又は、
前記機能は、前記第１パーティが前記シーケンスの途中で前記第１トランザクションのインスタンスを送信することを停止した場合に、前記第１トランザクションの最新のインスタンスを償還するために、前記ネットワークを通じて伝播されブロックチェーンに記録されるよう前記第１バージョンの送信を自動的に実行するよう構成される、請求項２に従属する請求項１８～２２のいずれか一項に記載の方法。
【請求項２４】
前記第１トランザクションは、インプット額を指定する１つ以上の第１インプットを含み、前記第１トランザクションの前記第１アウトプットは第１支払いを指定し、前記第１トランザクションは、１つ以上の更なる支払いを指定する１つ以上の更なるアウトプットを含み、前記支払いの合計は前記インプット額より大きく、前記第１パーティから前記第２パーティにより受信された前記第１トランザクションは、差を構成する他のインプットを含まず、前記ネットワークのノードは、合計インプット額より大きい合計支払いを指定する場合に、前記第１トランザクションを無効であるとして拒否するよう構成され、
前記方法は、前記第２パーティが、前記差を構成するために前記第１トランザクションの最終的な又は最新のインスタンスに第２インプットを追加し、前記ネットワークを通じて伝播されブロックチェーンに記録されるよう、追加された前記第２インプットを有する前記第１トランザクションを送信するステップ、を含む請求項１８～２３のいずれかに記載の方法。
【請求項２５】
前記更なるアウトプットは、前記インプット額から前記第１支払いを差し引いたものに等しい、前記第１パーティへの第２支払いを指定する第２アウトプットと、前記第２支払いに等しい、前記第２パーティへの第３支払いを指定する第３アウトプットと、を更に含む、請求項２４に記載の方法。
【請求項２６】
前記ロックスクリプトは、前記代替条件のうちの第３条件を含み、これは、ロックタイムが終了すること、及び前記第１パーティの暗号署名が前記アンロックスクリプトに含ま

れることを要求し、従って、前記第２パーティにより前記ロックタイムの範囲内で償還されなかった場合、前記第１パーティが、前記第１トランザクションの前記第１アウトプットの中の支払いを償還することを可能にする、請求項１７～２５のいずれかに記載の方法。
【請求項２７】
前記代替条件のうちの少なくとも幾つかの各々は、投票のための異なる選択肢に対応し、
前記方法は、前記ターゲットトランザクションの前記更新バージョンを取得するステップの前に、前記第１バージョンの中の前記アンロックスクリプトを、投票意向の拘束力のない指示として、アクセス又は第３パーティによりアクセス可能であるとマークするステップを含む、請求項１～９のいずれかに記載の方法。
【請求項２８】
所定の時点の後になるまで前記ネットワークが前記ブロックチェーンに前記第１バージョンを記録するのを防ぐために、前記第１トランザクション及び前記ターゲットトランザクションの前記第１バージョンのうちの少なくとも１つにロックタイムが含まれる、請求項２７に記載の方法。
【請求項２９】
前記第１トランザクションの前記第１アウトプットは、前記ロックスクリプト内で指定された前記代替条件のうちのいずれか１つに従い前記第１アウトプットをアンロックすることにより償還される支払いを指定し、前記ターゲットトランザクションは、前記支払いのうちの少なくとも一部を前記第１パーティへ移転するアウトプットを含む、請求項２７又は２８に記載の方法。
【請求項３０】
前記代替条件は、
第１選択肢の世論調査指示に対応する第１条件、
第２選択肢の世論調査指示に対応する第２条件、
第１選択肢の投票選択に対応する第３条件、及び、
第２選択肢の投票選択に対応する第４条件、
を含み、
前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記第１又は前記第２条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成され、
前記ターゲットトランザクションの前記第２の更新バージョンの前記アンロックスクリプトは、前記第１条件の代わりに前記第３条件を又は前記第２条件の代わりに前記第４条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成されることにより、前記世論調査指示を投票へと変換するよう構成される、請求項２７～２９のいずれかに記載の方法。
【請求項３１】
第１パーティのコンピュータ機器を含むコンピュータシステム上で実行されると前記コンピュータシステムに請求項１に記載の方法を実行させるコンピュータプログラム。
【請求項３２】
第２パーティのコンピュータ機器を含むコンピュータシステム上で実行されると前記コンピュータシステムに請求項１～３０のいずれか一項に記載の方法を実行させるコンピュータプログラム。
【請求項３３】
第１パーティのコンピュータ機器を含むコンピュータシステムであって、前記コンピュータシステムは、前記第１パーティのコンピュータ機器に実装され、前記コンピュータシステムは、
１つ以上のメモリユニットを含むメモリと、
１つ以上の処理ユニットを含む処理機器と、
を含み、
前記メモリはコードを格納し、前記コードは前記処理機器により実行されると前記処理

機器に請求項１に記載の方法を実行させるよう構成される、コンピュータシステム。
【請求項３４】
第２パーティのコンピュータ機器を含むコンピュータシステムであって、前記コンピュータシステムは、前記第２パーティのコンピュータ機器に実装され、前記コンピュータシステムは、
１つ以上のメモリユニットを含むメモリと、
１つ以上の処理ユニットを含む処理機器と、
を含み、
前記メモリはコードを格納し、前記コードは前記処理機器により実行されると前記処理機器に請求項１～３０のうちの一項に記載の方法を実行させるよう構成される、コンピュータシステム。
【請求項３５】
第１パーティのコンピュータ機器及び第２パーティのコンピュータ機器を含むコンピュータシステムであって、前記コンピュータシステムは、前記第１パーティのコンピュータ機器と前記第２パーティのコンピュータ機器との組み合わせの間に分散され、前記コンピュータシステムは、
１つ以上のメモリユニットを含むメモリと、
１つ以上の処理ユニットを含む処理機器と、
を含み、
前記メモリはコードを格納し、前記コードは前記処理機器により実行されると前記処理機器に請求項１～３０のうちの一項に記載の方法を実行させるよう構成される、コンピュータシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、ブロックチェーンの文脈における適応性（malleability）の現象、つまりトランザクションを無効にすることなくトランザクションの特定の未署名部分を変更する能力に関連する。
【背景技術】
【０００２】
ブロックチェーンとは、分散型データ構造の形式を指し、ブロックチェーンの複製のコピーは、ピアツーピア(peer-to-peer （Ｐ２Ｐ))ネットワーク内の複数のノードのそれぞれにおいて維持される。ブロックチェーンは、データのブロックのチェーンを含み、各ブロックは１つ以上のトランザクションを含む。各トランザクションは、シーケンスの中の先行するトランザクションを指してよい。トランザクションは、ネットワークに提供されて、「マイニング」として知られる処理により、新しいブロックに含まれることができる。「マイニング」は、複数のマイニングノードの各々が「proof-of-work」を実行するために競争する、つまりブロックに含まれることを待っている保留中のトランザクションのプールに基づき、暗号パズルを解くことを含む。
【０００３】
従来、ブロックチェーン内のトランザクションは、デジタルアセット、すなわち、価値のストアとして機能するデータを伝達するために使用される。しかし、ブロックチェーンの上に追加の機能を積み重ねるために、ブロックチェーンを利用することもできる。例えば、ブロックチェーンプロトコルは、トランザクションのアウトプットに追加のユーザデータを格納することを可能にしてよい。現代のブロックチェーンは、単一トランザクション内に格納できる最大データ容量を増加させ、より複雑なデータを組み込むことを可能にしている。例えば、これは、ブロックチェーン内に電子ドキュメント（electronic document）、或いはオーディオ若しくはビデオデータを格納するために使用され得る。
【０００４】
ネットワーク内の各ノードは、転送、マイニング、及び記憶のうちの任意の１、２、又

は３つ全部の役割を有することができる。転送ノードは、それぞれ、（有効な）トランザクションを１つ以上の他のノードへ伝播させる。従って、それらの間でネットワークのノードを通じてトランザクションを伝播させる。マイニングノードは、それぞれ、トランザクションのマイニングを実行してブロックにするために競争する。記憶ノードは、それぞれ、ブロックチェーンのマイニングされたブロックの彼ら自身のコピーを格納する。トランザクションをブロックチェーンに記録させるために、パーティは、該トランザクションを、伝播させるようにネットワークのノードのうちの１つへ送信する。トランザクションを受信したマイニングノードは、トランザクションをマイニングして新しいブロックにするよう競争してよい。各ノードは、トランザクションが有効であるための１つ以上の条件を含む同じノードプロトコルを尊重するよう構成される。無効なトランザクションは、伝播されず、マイニングされてブロックにされることもない。トランザクションが検証され、それによってブロックチェーンに受け入れられたと仮定すると、追加のユーザデータは、従って、不変の公開レコードとしてＰ２Ｐネットワークの各ノードに格納されたままである。

【０００５】

最新のブロックを生成するためにproof-of-workパズルを解くことに成功したマイナーは、標準的に、デジタルアセットの新しい額を生成する「生成トランザクション（generation transaction）」と呼ばれるトランザクションにより報酬を受ける。トランザクションは、任意で、成功したマイナーのための追加マイニング手数料も指定してよい。proof-of-workは、ブロックをマイニングするために膨大な量の計算リソースを必要とするので、及び二重支払いの企てを含むブロックは他のノードにより受け入れられない可能性があるので、マイナーが、彼らのブロックに二重支払いトランザクションを含めることによりシステムを騙さないことを奨励し、

「アウトプットに基づく」モデル（UTXOに基づくモデルと呼ばれることもある）では、所与のトランザクションのデータ構造は、１つ以上のインプット及び１つ以上のアウトプットを含む。任意の使用可能アウトプットは、時にUTXO（「unspent transaction output（未使用トランザクションアウトプット）」）と呼ばれる、デジタルアセットの額を指定する要素を含む。アウトプットは、アウトプットを償還（redeem）するための条件を指定するロックスクリプトを更に含んでよい。各インプットは、先行するトランザクション内のそのようなアウトプットへのポインタを含み、ポイントされたアウトプットのロックスクリプトをアンロックするためのアンロックスクリプトを更に含んでよい。従って、トランザクションのペアを考えるとき、それらを、第１トランザクション及び第２トランザクション（又は「ターゲット」トランザクション）と呼ぶ。第１トランザクションは、デジタルアセットの額を指定する、及びアウトプットをアンロックする１つ以上の条件を定義するロックスクリプトを含む、少なくとも１つのアウトプットを含む。第２のターゲットトランザクションは、第１トランザクションのアウトプットへのポインタと、第１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アンロックスクリプトと、を含む少なくとも１つのインプットを含む。

【０００６】

このようなモデルでは、第２のターゲットトランザクションが、伝播されてブロックチェーンに記録されるようＰ２Ｐネットワークへ送信されると、各ノードにおいて適用される有効性のための条件のうちの１つは、アンロックスクリプトが第１トランザクションのロックスクリプト内で定義された要件を満たすことである。ターゲットトランザクションが有効であるための別の条件は、第１トランザクションのアウトプットが、別の有効なトランザクションによって未だ償還されていないことである。これらの条件のうちのいずれかに従いターゲットトランザクションが無効であると分かった任意のノードは、該トランザクションを伝播させず、ブロックチェーンに記録させるためにマイニングしてブロックに含めることもしない。

【０００７】

例えば、ターゲットトランザクションは、第１パーティ（「Alice」）から第２パーティ

（「Bob」）へのデジタルアセット額を運ぶためのものである。先行する第１トランザクションのロックスクリプト内で定義された要件のうちの１つは、標準的に、ターゲットトランザクションのアンロックスクリプトがAliceの暗号署名を含むことである。署名は、ターゲットトランザクションの部分に署名するAliceにより生成されなければならない。これがどの部分であるかは、アンロックスクリプトにより柔軟に定義されてよく、又は使用されるプロトコルに依存して、ノードプロトコルの本来の特徴であってよい。しかしながら、署名されるべき部分は、標準的に、ターゲットトランザクションの特定の他の部分、例えばアンロックスクリプト自体の一部又は全部を除く。

【０００８】

これは、「適応性（malleability）」の可能性を生成する。つまり、マイニングの前に、署名されていないターゲットトランザクションの部分が、トランザクションを無効にすることなく、変更（「malleated」）可能である。適応性は、暗号法において知られている概念である。これは、通常、セキュリティ関心事として知られており、それによりメッセージが悪意を持って変更され得るが、依然として真正であるととして受け入れられる。ブロックチェーンの文脈では、適応性は、必ずしも関心事ではないが、単に奇妙なアーチファクトとして知られており、それにより、トランザクションの特定の部分が該トランザクションを無効にすることなく変更可能である。

【０００９】

近年、トランザクションをメディアデータのキャリアとして使用するために、適応性を慎重に利用する提案が行われた。データコンテンツをトランザクションのアンロックスクリプトに含むことができ、このトランザクションは、次に、「支払い（payment）チャネル」と呼ばれるサイドチャネルを介してパーティ間で送信される。パーティのうちの１つは、次に、トランザクションを変更して（malleate）データを除去し、変更したバージョンをマイニングされるようにＰ２Ｐネットワークへ向けて送信する（一方、データが除去されなかった場合、トランザクションは、ブロックチェーンを膨大にし、トランザクションを受け入れるためにマイナーにより要求される報酬は、トランザクションのデータサイズと共に標準的にスケーリングするので、標準的にはより高いマイニング手数料も要求する）。

【発明の概要】

【００１０】

本開示は、適応性、又はより一般的には更新可能性が肯定的な特徴として利用できる更なる方法を認識する。特に、トランザクションのペアのうちの第１トランザクションは、そのロックスクリプト内に複数の異なるアンロック条件を含み得ることが知られている。従来、１つの条件又は他のものに基づき、第１トランザクションのアウトプットを償還するために、ターゲットトランザクションの１つのバージョンのみがこれまでに生成された。しかしながら、ここで、実際に２つのバージョン：条件のうちの第１条件に基づき第１トランザクションを償還するアンロックスクリプトを有する、ターゲットトランザクションの第１バージョン、及び条件のうちの第２条件に基づき第１トランザクションを償還する第２バージョン、が存在することが有用であると認識される。第２の更新バージョンは、第１バージョンを変更することにより、又はスクラッチから新鮮なバージョンを生成することにより、生成され得る。それらは、並列に又は１つずつ存在し得る。両方のバージョンは第１トランザクションを有効に償還できないが、第１バージョンの存在は、第２条件を満たすために必要な環境が満たされていない場合に、Bobにとっての「バックアップ」として機能し得る。

【００１１】

本願明細書に開示される一態様によると、ブロックチェーンに第１パーティと第２パーティとの間のターゲットトランザクションを記録する方法が提供される。当該方法は、第１パーティ又は第２パーティのコンピュータ機器により、

ターゲットトランザクションの既存の第１バージョンに対して更新されている、前記ターゲットトランザクションの第２の更新バージョンを取得するステップと、

前記第１バージョンの代わりに、ノードのネットワークを通じて伝播され、前記ノードのうちの少なくとも幾つかの各々において維持されているブロックチェーンのコピーに記録されるように、前記ターゲットトランザクションの前記更新バージョンを送信するステップと、を含む。
前記ターゲットトランザクションは、アンロックスクリプトと、第１トランザクションの第１アウトプットへのポインタと、を含み、前記第１アウトプットは、前記第１トランザクションの前記第１アウトプットをアンロックするための複数の代替条件を指定するロックスクリプトを含む。前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記代替条件のうちの第１条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成され、前記更新バージョンの前記アンロックスクリプトは、前記第１条件の代わりに、前記代替条件のうちの第２条件を満たすことに基づき前記第１トランザクションの前記第１アウトプットをアンロックするよう構成される。

【００１２】

前記ターゲットトランザクションを含む複数のトランザクションの各々について、前記ネットワークの少なくとも幾つかのノードは、トランザクションが有効であることを条件として各トランザクションを伝播させ、少なくとも幾つかのノードは、トランザクションが有効であることを条件として、該ノードにおけるブロックチェーンのコピーに各トランザクションを記録するよう構成され、前記ターゲットトランザクションの有効性は、前記アンロックスクリプトが前記条件のうちのいずれか１つに従い前記第１トランザクションの前記アウトプットをアンロックすることを条件とするが、前記バージョンのうちの一方が任意の所与のノードにおいて検証されると、他方のバージョンが該ノードにおいて無効であると見なされる。

【００１３】

従って、両方のバージョンは第１トランザクションを有効に償還できないので、第２パーティ（「Bob」）は、伝播されブロックチェーンに記録されるよう両方のバージョンを送信しない。彼は、彼の好みで伝播され記録されるように第２バージョンを送信するが、第１バージョンが存在したという事実は、第２バージョンのための必要な環境が満たされなかった場合に、第１バージョンを記録させたというフォールバック（fall-back）を彼に与える。

【００１４】

例えば、第１の例示的な使用例では、第１トランザクション（「Tx_1」）は、第２パーティ（「Bob」）により提供されるべきサービスに対する、第１パーティ（「Alice」）からの支払いを含む。第１トランザクションは、Alice、Bob、又は第三者により生成され得る。それは既にオンチェーンにあり、又はそこへ後に記録されるよう送信され得る。いずれの方法も、第１トランザクションのアウトプット内のロックスクリプトが、該アウトプット内で定義された支払いをアンロックするための少なくとも２つの代替条件、第１条件及び第２条件を指定する。第１条件は、Aliceの署名がターゲットトランザクションのアンロックスクリプトに含まれることを必要としないが、幾つかの他の煩わしい要件、例えばアンロックスクリプトが大きな所定のデータ片（これは、高いマイニング手数料を招き得る）又はBobの機密若しくは秘密データ片（これは、Bobがブロックチェーン上で公開したくない）を含むことをBobに課す。第２条件は、Aliceの署名がターゲットトランザクションのアンロックスクリプトに含まれることを要求するが、第１条件の煩わしい要件を課さない。

【００１５】

AliceがBobにターゲットトランザクションの第１バージョン（「Tx_p」）も提供するか、又はBobが彼自身でそれを生成する（若しくは、それは第三者により生成される）。第１バージョンは、第１条件に基づき第１トランザクションTx_1のアウトプットをアンロックするよう構成される。一方、第２バージョン（「Tx_p’」）は、第２条件に基づき、それをアンロックするよう構成される。次に、Bobは、サービスを提供する。Aliceが満足し誠

実であるならば、それに応答して、彼女は、Bobに、彼女の署名を含む、ターゲットトランザクションの第２バージョンTx_p’を提供する（又は第２バージョンを構成するために少なくとも彼女の署名をBob又は第三者に提供する）。しかしながら、Aliceが合意を破った場合には、Bobは、あまり好ましくない第１条件に基づき第１トランザクションのアウトプットを償還するために、既存の、あまり好ましくない第１バージョンTx_pを送信するというオプションを有している。

【００１６】

第２の例示的な使用例では、当該方法は、前記第２パーティの前記コンピュータ機器により、

前記第１パーティへデータ部分のシーケンスをストリーミングするステップであって、前記シーケンスの中の最終部分により終了する、ステップと、

前記データ部分のうちのそれぞれの部分に応答して、前記第１パーティから前記第１トランザクションのそれぞれのインスタンスを受信するステップであって、各インスタンスの第１アウトプットは、前記それぞれの部分についての前記第２パーティへの支払いを指定する、ステップと、

を含んでよく

前記支払いは各データ部分と共に増大する。このような実施形態では、前記ターゲットトランザクションの前記更新バージョンを取得するステップは、前記シーケンスの中の最終部分に続いて、第１パーティから更新バージョンを受信するステップを含む。

【００１７】

例えば、各データ部分は、メディアコンテンツ（例えば、オーディオ及び／又はビデオコンテンツ）のアイテムの異なる部分であってよい。代替として、各データ部分は、サービスのユニット（例えば、ガス、水道、電気のような生活必需サービス、又は車両、不動産、又は他の物理的オブジェクトのレンタル）にアクセスするための異なる鍵である。

【００１８】

例えば、第１アウトプットが各インスタンスの中に同じアウトプット識別子（例えば、UTXO識別子）を有するので、第１トランザクションのインスタンス（Tx_1,Tx_2,Tx_3,…）は、ネットワークの各ノードにより、実質的に同じトランザクションのインスタンスとして認識されてよい。従って、１つのインスタンスのみが、ブロックチェーンに記録できる。１つのインスタンスが任意の所与のノードにより有効であるとして受け入れられると、更なるバージョンを記録しようとする任意の試みは、無効であると見なされ、従って該ノードにより拒否される。更に、第１トランザクションのインスタンスのうちの１つがターゲットトランザクションのバージョンのうちの１つ（Tx_p又はTx_p’）により有効に償還されることが、任意の所与のノードにより分かると、第１トランザクションの任意のインスタンスを償還しようとする任意の更なるターゲットトランザクションは、該ノードにより無効であると見なされ、従って、該ノードにより伝播されず、ブロックチェーンに記録されることもない。

【００１９】

ターゲットトランザクションの任意のバージョン（Tx_p又はTx_p’）は実質的に同じ第１トランザクションのインスタンス（単に異なる額を定義する）の同じアウトプットIDを指すので、１つのターゲットトランザクションのみが、該アウトプットを有効に償還できる。第１トランザクションのインスタンスのうちの１つ（Tx_1,Tx_2,Tx_3,…）がターゲットトランザクションのバージョンのうちの１つ（Tx_p又はTxp’）により有効に償還されることが、任意の所与のノードにおいて分かると、第１トランザクションの任意のインスタンスを償還しようとする任意の更なるターゲットトランザクションは、無効であると見なされ、従って、該ノードにより伝播されず、ブロックチェーンに記録されることもない。しかしながら、各インスタンスの中の支払いも、データの各部分と引き換えに増大するので、第２パーティ（「Bob」）が行わなければならないことは、第１トランザクションの最後の又は最近のインスタンスTx_nを償還するターゲットトランザクションのバージョンTx_p’を送信して、伝播させブロックチェーンに記録することである。彼は、次に、トランザク

ションの単一のペアに基づき、その時点前に送信されたデータの全部の部分についての完全な支払いを受け取る。代わりに、第１パーティ（「Alice」）がデータの各個別部分（例えば、オーディオ又はビデオコンテンツの各パケット又はチャンク）についての別個の個別支払いを送信する場合、Bobは各データ部文意ついて別個のトランザクションを送信しなければならないので、これは、ブロックチェーンを膨大にし、より多くのネットワークトラフィックをもたらすだろう。

【００２０】

任意の時点で、シーケンスの終了の前に、Aliceが第１トランザクションのインスタンス（Tx_1,Tx_2,Tx_3,…）の送信を停止した場合、その時点より前に送信されたデータ部分についての支払いを償還するために（従って、送信された最新のデータ部分のみを失う）、Bobは、Aliceへの更なるデータ部分の送信を停止し、ターゲットトランザクションの第１バージョンTx_pをネットワークへ送信するオプションを依然として有する。反対に、任意の時点で、Bobがデータ部分の送信を停止した場合、Aliceは、第１トランザクションの更なるインスタンスTx_1の送信を停止するオプションを有し、Bobは、それまでにAliceにより受信されたデータ部分に対する支払いを償還する能力のみを受けるだろう。

【００２１】

特に任意的な実装では、第１トランザクションは、インプット額を指定する１つ以上の第１インプットを含んでよく、第１トランザクションの第１アウトプットは第１支払いを指定してよく、第１トランザクションは、１つ以上の更なる支払いを指定する１つ以上の更なるアウトプットを更に含んでよい。その結果、支払いの合計はインプット額より高く、第１パーティから第２パーティにより受信される第１トランザクションは、差分を生成する他のインプットを有しない。ネットワークのノードは、第１トランザクションが合計インプット額より多くの合計支払いを指定する場合、第１トランザクションを無効であるとして拒否する。このような実施形態では、当該方法は、差分を構成する（make up）ために、第２パーティが第２インプットを第１トランザクションの最終又は最近のインスタンスに追加するステップと、追加された第２インプットを有する第１トランザクションを、ネットワークを通じて伝播されブロックチェーンに記録されるよう送信するステップと、を含む。

【００２２】

この例示的な実装として、更なるアウトプットは、インプット額から第１支払いを差し引いたものに等しい、第１パーティへの第２支払いを指定する第２アウトプットと、第２支払いに等しい、第２パーティへの第３支払いを指定する第３アウトプットと、を含む。

【００２３】

このような実施形態は、第１パーティ（「Alice」）が、先のインスタンスのうちの１つを償還するために彼女自身のターゲットトランザクションを送り出すことによりシステムを騙すことを防止し、従って、Bobが後のインスタンスのうちの１つ（又は実際にインスタンスのうちのいずれか）を償還することを防止する。そうすることにより、Aliceは、彼女のデジタルアセットの多くを負担する余分なインプットを追加しなければならないからである。従って、Aliceがシステムを騙そうとすることに価値がない。

【００２４】

別の例示的な使用例では、前記代替条件のうちの少なくとも幾つかの各々は、投票のための異なる選択肢に対応してよく、

前記方法は、前記ターゲットトランザクションの前記更新バージョンを取得するステップの前に、前記第１バージョンの中の前記アンロックスクリプトを、投票意向の拘束力のない指示として、アクセスする又は第三者によりアクセス可能であるとマークするステップを含んでよい。投票の指示が実際に投票に変換されなかった場合、第１バージョンは、投票が最終的な投票結果とどれくらい異なったかの公開された指示として残る。

【００２５】

本願明細書に開示される更なる態様によると、方法を実行するためのプログラム、及び／又は方法を実行するようプログラミングされた第２パーティのコンピュータ機器が提供

される。プログラム又はコンピュータ機器は、第２パーティが、いずれかのバージョンを選択する手動オプションを提供することにより、及び／又は第１イベントにより第１バージョンを自動的に送信するよう構成され及び第２イベントにより第２バージョンの代わりに伝播され記録されるように第２バージョンを自動的に送信するよう更に構成される自動機能により、ネットワークを通じて伝播されブロックチェーンに記録されるように、第１バージョン又は第２バージョンのいずれかを選択的に送信できるように構成されてよい。

【図面の簡単な説明】

【００２６】

本開示の実施形態の理解を助け、そのような実施形態がどのように実施され得るかを示すために、例としてのみ、以下の添付の図面を参照する。

【図１】ブロックチェーンを実装するためのシステムの概略ブロック図である。

【図２】ブロックチェーンに記録されるトランザクションのいくつかの例を概略的に示している。

【図３】ブロックチェーンを実装するための別のシステムの概略ブロック図である。

【図４】クライアントアプリケーションの概略ブロック図である。

【図５】図４のクライアントアプリケーションにより提示される例示的なユーザインタフェースの概略的模擬表示である。

【図６】トランザクションのセットの概略図である。

【図７】データをストリーミングする方法のフローチャートである。

【図８】図７の方法の例示的な実装における第１トランザクションのインスタンスのインプット及びアウトプットの値を示すグラフである。

【図９】投票方法を示すシグナリング図である。

【図１０】投票方法を示すシグナリング図である。

【図１１】図１０の方法を実施するトランザクションの例示的なセットを示す。

【発明を実施するための形態】

【００２７】

適応性は、暗号法において既存の概念である。これは、通常、セキュリティ関心事を支え、それによりメッセージが悪意を持って変更され得るが、依然として真正であるとして受け入れられる。デジタル署名方式は、この関心事を解決するために設計される。ブロックチェーンでは、しかしながら、適応性は、トランザクションを全体として無効にすることなく、トランザクションの少なくとも部分を変更する能力を表す。関連する形式の暗号署名（例えば、ECDSA署名）により署名されるトランザクション内の任意の情報は、適応（malleation）の可能性の影響を受けない。適応性に関連する任意の請求リティ関心事は、代わりに、プロトコル自体ではなく、不適切な実装により引き起こされる。

【００２８】

以下は、速くセキュアな信頼不要の（trustless）支払いチャネルを実現するための有用な特徴として利用する。思想は、（例えば、ECDSA署名により）署名されない又はされる必要のないトランザクション内の１つ又は複数の部分を識別することである。開示の方式は、トランザクションの各インプットのアンロックスクリプト内の任意のコンテンツ（例えば「scriptSig」フィールド）が任意の署名により署名されていないという事実を利用する。実施形態は、トランザクションを無効にすることなく該トランザクションを柔軟に変更することを可能にするために、SIGHASHフラグも利用してよい。

【００２９】

例は以下の通りである。ブロックチェーン上でデータを交換するとき、１つの一般的な方法は、データの開示及び支払いの受け入れが同時に生じることを強制するために、ハッシュパズルを使用することである。これを回避するために、トランザクションは、支払いが２つの条件：（ｉ）「データ＋Bobの署名」を提供すること、又は（ｉｉ）「Aliceの署名＋Bobの署名」を提供すること、のうちのいずれかにより請求できるように、構成できる。

【００３０】

Bobは、データ及び彼の署名を提供することにより資金を請求するためのトランザクションを構成し、それをAliceへ送信する。Aliceは、次に、データを彼女の署名で置き換え、トランザクションをネットワークへブロードキャストする。代替として、BobはAliceの署名を取得し、それでデータを置き換え、ネットワークにブロードキャストする。いずれの方法でも、データはBobの署名により署名されたメッセージの部分ではないので、それをAliceの署名で置き換えることは、トランザクションを無効にしない。更に、トランザクションは、インプットが条件（ｉｉ）を満たすとき、有効のままである。Aliceがトランザクションをネットワークへブロードキャストせず、彼女の署名を提供しない場合、Bobは、条件（ｉ）（これは、彼が相当量の及び／又は独自のデータをアップロードしなければならないので、あまり好ましくない）に基づき資金を請求するために、元のトランザクションをブロードキャストするオプションを依然として有する。Aliceは、肯定すべき要件、割引の動機付け、又はサービスが良好に実行されたことに対してBobに報酬を与えることにより、彼女の署名を提供することを奨励されてよい。

【００３１】

＜システム概要＞

図１は、ブロックチェーン１５０を実装するための例示的なシステム１００を示す。システム１００は、典型的にはインターネットのような広域インターネットワークであるパケット交換ネットワーク１０１を含む。パケット交換ネットワーク１０１は、パケット交換ネットワーク１０１内にピアツーピア(Ｐ２Ｐ)オーバレイネットワーク１０６を形成するように配置された複数のノード１０４を含む。各ノード１０４は、異なるピアに属する異なるノード１０４を有するピアのコンピュータ装置を含む。各ノード１０４は、１つ以上のプロセッサ、例えば、１つ以上の中央処理装置（ＣＰＵ）、アクセラレータプロセッサ、特定用途向けプロセッサ、及び/又はフィールドプログラマブルゲートアレイ（ＦＰＧＡ）を含む処理装置を含む。各ノードはまた、メモリ、すなわち、１つ以上の非一時的コンピュータ読取可能媒体の形態のコンピュータ読取可能記憶装置を備える。メモリは、１つ以上のメモリ媒体、例えば、ハードディスクなどの磁気媒体、固体ドライブ（solid-state drive（SSD））、フラッシュメモリ又はEEPROMなどの電子媒体、及び/又は光ディスクドライブなどの光学的媒体を使用する１つ以上のメモリユニットを含んでもよい。

【００３２】

ブロックチェーン１５０は、データのブロック１５１のチェーンを指し、ブロックチェーン１５０のそれぞれのコピーは、ピアツーピア(peer-to-peer（Ｐ２Ｐ))ネットワーク１６０内の複数のノードのそれぞれにおいて維持される。チェーン内の各ブロック１５１は、１つ以上のトランザクション１５２を含み、この文脈ではトランザクションは、一種のデータ構造を参照する。データ構造の性質は、トランザクションモデル又はスキームの一部として使用されるトランザクションプロトコルのタイプに依存する。所与のブロックチェーンは、典型的には、全体を通して、１つの特定のトランザクションプロトコルを使用する。１つの一般的なタイプのトランザクションプロトコルでは、各トランザクション１５２のデータ構造は、少なくとも１つのインプット及び少なくとも１つのアウトプットを含む。各アウトプットは、そのアウトプットが暗号的にロックされている(アンロックされ、それによって償還又は使用されるために、そのユーザ１０３の署名を必要とする)ユーザに属するデジタルアセットの数量を表す額（amount）を指定する。各インプットは、先行するトランザクション１５２のアウトプットを逆にポイントし、それによってトランザクションをリンクする。

【００３３】

ノード１０４の少なくとも幾つかは、トランザクション１５２を転送し、それによって伝播する転送ノード１０４Ｆの役割を引き受ける。ノード１０４の少なくともいくつかは、ブロック１５１をマイニングするマイナー１０４Ｍの役割を担う。ノード１０４の少なくとも幾つかは、記憶ノード１０４Ｓ（「フル（full-copy）」ノードとも呼ばれる）の役割を引き受け、各ノードは、それぞれのメモリに同じブロックチェーン１５０のそれぞれのコピーを格納する。各マイナーノード１０４Ｍは、マイニングされてブロック１５１にさ

れることを待ってるトランザクション１５２のプール１５４も維持する。所与のノード１０４は、転送ノード１０４、マイナー１０４Ｍ、記憶ノード１０４Ｓ、又はこれらの２つ若しくは全部の任意の組み合わせであり得る。

【００３４】

所与の現在のトランザクション１５２jにおいて、インプット（又はそのそれぞれ）は、トランザクションのシーケンスの中の先行トランザクション１５２iのアウトプットを参照するポインタを含み、このアウトプットが現在のトランザクション１５２jにおいて償還されるか又は「消費される（spent）」ことを指定する。一般に、先行するトランザクションは、プール１５４又は任意のブロック１５１内の任意のトランザクションであり得る。先行するトランザクション１５２iは、必ずしも、現在のトランザクション１５２jが生成された又はネットワーク１０６へ送信されたときに存在する必要はないが、先行するトランザクション１５２iは、現在のトランザクションが結う意向であるために存在し検証されている必要がある。従って、本願明細書で「先行する」は、ポインタによりリンクされた論理的シーケンスの中で先行するものを表し、必ずしも時系列の中での生成又は送信の時間を表さない。従って、それは、必ずしも、トランザクション１５２i,１５２jが順不同で生成され又は送信されることを排除しない（以下の親のない（orphan）トランザクションに関する議論を参照する）。先行するトランザクション１５２iは、等しく、祖先（antecedent）又は先行（predecessor）トランザクションと呼ばれ得る。

【００３５】

現在のトランザクション１５２jのインプットは、先行するトランザクション１５２iのアウトプットがロックされているユーザ１０３aの署名も含む。また、現在のトランザクション１５２jのアウトプットは、新しいユーザ１０３bに暗号的にロックできる。従って、現在のトランザクション１５２jは、先行するトランザクション１５２iのインプットで定義された量を、現在のトランザクション１５２jのアウトプットで定義された新しいユーザ１０３bに移転することができる。幾つかの場合には、トランザクション１５２が複数のアウトプットを有し、複数のユーザ間でインプット量を分割してよい(変更を行うために、そのうちの１人がオリジナルユーザとなる)。場合によっては、トランザクションが複数のインプットを有し、１つ以上の先行するトランザクションの複数のアウトプットから量をまとめ、現在のトランザクションの１つ以上のアウトプットに再分配することもできる。

【００３６】

上記は「アウトプットベースの」トランザクションプロトコルと呼ばれることがあり、時には「未使用のトランザクションアウトプット(unspent transaction output (UTXO))タイプのプロトコル」(アウトプットはUTXOと呼ばれる)とも呼ばれる。ユーザの合計残高は、ブロックチェーンに格納されている１つの数値で定義されるのではなく、代わりに、ユーザは、ブロックチェーン１５１内の多くの異なるトランザクション１５２に分散されている該ユーザのすべてのUTXOの値を照合するために、特別な「ウォレット」アプリケーション１０５を必要とする。

【００３７】

アカウントベースのトランザクションモデルの一部として、別のタイプのトランザクションプロトコルを「アカウントベース」のプロトコルと呼ぶことがある。アカウントベースの場合、各トランザクションは、過去の一連のトランザクションにおいて、先行するトランザクションのUTXOに戻って参照することによって移転される量を定義するのではなく、絶対的な口座（アカウント）残高を参照することによって移転される。すべてのアカウントの現在の状態は、ブロックチェーンとは別個のマイナーによって格納され、絶えず更新される。本開示は、アカウントに基づくのではなくアウトプットに基づくモデルに関する。

【００３８】

どちらのタイプのトランザクションプロトコルでも、ユーザ１０３が新しいトランザクション１５２jを実行したい場合、ユーザは、自分のコンピュータ端末１０２からＰ２Ｐネットワーク１０６のノードの１つ１０４(現在は、通常、サーバ又はデータセンタであるが

、原則として、他のユーザ端末でもよい)に新しいトランザクションを送信する。このノード１０４は、各ノード１０４に適用されるノードプロトコルに従って、トランザクションが有効であるかどうかをチェックする。ノードプロトコルの詳細は、問題のブロックチェーン１５０で使用されているトランザクションプロトコルのタイプに対応し、全体のトランザクションモデルを一緒に形成する。ノードプロトコルは、典型的には、ノード１０４に、新しいトランザクション１５２j内の暗号署名が、トランザクション１５２の順序付けされたシーケンスの中の前のトランザクション１５２iに依存する、期待される署名と一致することをチェックすることを要求する。アウトプットベースの場合、これは、新しいトランザクション１５２jのインプットに含まれるユーザの暗号署名が、新しいトランザクションが消費する先行するトランザクション１５２jのアウトプットに定義された条件と一致することをチェックすることを含んでよく、この条件は、典型的には、新しいトランザクション１５２jのインプット内の暗号署名が、新しいトランザクションのインプットがポイントする前のトランザクション１５２iのアウトプットをアンロックすることを少なくともチェックすることを含む。いくつかのトランザクションプロトコルでは、条件は、少なくとも部分的に、インプット及び/又はアウトプットに含まれるカスタムスクリプトによって定義されてもよい。あるいは、単にノードプロトコルだけで固定することもできるし、あるいは、これらの組み合わせによることもある。いずれにせよ、新しいトランザクション１５２jが有効であれば、現在のノードは新しいトランザクションをＰ２Ｐネットワーク１０６内のノード１０４の１つ以上の他のノードに転送する。これらのノード１０４の少なくともいくつかは、同じノードプロトコルに従って同じテストを適用し、新しいトランザクション１５２jを１つ以上のさらなるノード１０４に転送するなど、転送ノード１０４Ｆとしても機能する。このようにして、新しいトランザクションは、ノード１０４のネットワーク全体に伝播される。

【００３９】

アウトプットベースのモデルでは、与えられたアウトプット(例えば、UTXO)が消費されるかどうかの定義は、ノードプロトコルに従って別の今後の（onward）トランザクション１５２jのインプットによって既に有効に償還されているかどうかである。トランザクションが有効であるための別の条件は、それが消費又は償還を試みる先行するトランザクション１５２iのアウトプットが、別の有効なトランザクションによって未だ消費/償還されていないことである。ここでも、有効でない場合、トランザクション１５２jは、ブロックチェーンに伝播又は記録されない。これは、支払者が同じトランザクションのアウトプットを複数回消費しようとする二重支出を防ぐ。

【００４０】

検証に加えて、ノード１０４Ｍのうちの少なくともいくつかは、「proof of work」に支えられているマイニングと呼ばれるプロセスで、トランザクションのブロックを最初に作成するために競合する。マイニングノード１０４Ｍでは、まだブロックに現れていない有効なトランザクションのプールに新しいトランザクションが追加される。そして、マイナーは、暗号パズルを解決しようと試みることにより、トランザクションのプール１５４からトランザクション１５２の新しい有効なブロック１５１を組み立てるために競争する。これは、典型的には、ノンスがトランザクションのプール１５４と連結され、ハッシュされるときに、ハッシュのアウトプットが所定の条件を満たすような「ノンス」値を探すことを含む。例えば、所定の条件は、ハッシュのアウトプットが、所定の数の先行ゼロを有することであってもよい。ハッシュ関数の特性は、インプットに関して予測不可能なアウトプットを持つことである。従って、この探索は、ブルートフォースによってのみ実行することができ、従って、パズルを解決しようとしている各ノード１０４Ｍにおいて、相当量の処理リソースを消費する。

【００４１】

パズルを解く最初のマイナーノード１０４Ｍは、これをネットワーク１０６に通知し、その解を証明として提供する。この解は、ネットワーク内の他のノード１０４によって簡単にチェックすることができる(ハッシュが対する解が与えられれば、ハッシュのアウトプ

ットが条件を満たすことを確認することは簡単である)。勝者がパズルを解いたトランザクションのプール１５４は、各ノードで勝者が発表した解をチェックしたことに基づいて、記憶ノード１０４Sとして機能するノード１０４のうちの少なくともいくつかによってブロックチェーン１５０の新しいブロック１５１として記録される。また、新しいブロック１５１nにはブロックポインタ１５５が割り当てられ、チェーン内で前に作成されたブロック１５１n-1を指すようになっている。proof-of-workは、新しいブロックを１５１作成するのに多大な労力を要し、二重の支出を含むブロックは他のノード１０４によって拒否される可能性が高く、従ってマイニングノード１０４Mが二重支払いを彼らのブロックに含まないようにするインセンティブが働くので、二重の支出のリスクを減じるのを助ける。一旦生成されると、ブロック１５１は、同じプロトコルに従ってP２Pネットワーク１０６内の各格納ノード１０４Siで認識され、維持されるため、変更することはできない。また、ブロックポインタ１５５は、ブロック１５１に順序を課す。トランザクション１５２は、P２Pネットワーク１０６内の各記憶ノード１０４Sで順序付けられたブロックに記録されるので、これはトランザクションの不変の公開台帳を提供する。

【００４２】

パズルを解決するために常に競争している異なるマイナー１０４Mは、いつ解を探し始めたかによって、いつでもマイニングされていないトランザクションプール１５４の異なるスナップショットに基づいてパズルを解いているかもしれないことに留意する。パズルを解く者は誰でも、最初に次の新しいブロック１５１nに含まれるトランザクション１５２を定義し、現在のマイニングされていないトランザクションのプール１５４が更新される。そして、マイナー１０４Mは、新たに定義された未解決のプール１５４からブロックを作り出すために、競争を続ける。また、生じ得る「分岐（フォーク、fork）」を解決するためのプロトコルも存在する。これは、２人のマイナー１０４Mが互いに非常に短い時間内にパズルを解決し、ブロックチェーンの矛盾したビューが伝播する場合である。要するに、分岐の枝が伸びるときは常に、最長のものが最終的なブロックチェーン１５０になる。

【００４３】

ほとんどのブロックチェーンでは、勝ったマイナー１０４Mは、何も無いものから新しい量のデジタルアセットを生み出す特別な種類の新しいトランザクションによって自動的に報酬を受けている(通常のトランザクションでは、あるユーザから別のユーザにデジタルアセットの額を移転する)。したがって、勝ったノードは、ある量のデジタルアセットを「マイニング」したと言われる。この特殊なタイプのトランザクションは「生成（generation）」トランザクションと呼ばれることもある。それは自動的に新しいブロック１５１nの一部を形成する。この報酬は、マイナー１０４Mがproof-of-work競争に参加するインセンティブを与える。多くの場合、通常の（非生成）トランザクションは、そのトランザクションが含まれたブロック１５１nを生成した勝ったマイナー１０４Mにさらに報酬を与えるために、追加のトランザクション手数料をそのアウトプットの１つにおいて指定する。

【００４４】

マイニングに含まれる計算リソースのために、典型的には、少なくともマイナーノード１０４Mの各々は、１つ以上の物理的サーバユニットを含むサーバ、又はデータセンタ全体の形態をとる。各転送ノード１０４M及び/又は記憶ノード１０４Sは、サーバ又はデータセンタの形態をとることもできる。しかしながら、原則として、任意の所与のノード１０４は、ユーザ端末又は互いにネットワーク接続されたユーザ端末のグループを含むことができる。

【００４５】

各ノード１０４のメモリは、それぞれの１つ以上の役割を実行し、ノードプロトコルに従ってトランザクション１５２を処理するために、ノード１０４の処理装置上で動作するように構成されたソフトウェアを記憶する。ノード１０４に属するいずれの動作も、それぞれのコンピュータ装置の処理装置上で実行されるソフトウェアによって実行され得ることが理解されよう。また、本明細書で使用される「ブロックチェーン」という用語は、一

般的な技術の種類を指す一般的な用語であり、任意の特定の専有のブロックチェーン、プロトコル又はサービスに限定されない。

【００４６】

また、ネットワーク１０１には、消費者ユーザの役割を果たす複数のパーティ１０３の各々のコンピュータ装置１０２も接続されている。これらは、トランザクションにおける支払人及び被支払人の役割を果たすが、他のパーティの代わりにトランザクションをマイニングし又は伝播することに必ずしも参加しない。それらは必ずしもマイニングプロトコルを実行するわけではない。２つのパーティ１０３及びそれぞれの機器１０２は、説明のために示されており、第１パーティ１０３ａ及びそのそれぞれのコンピュータ機器１０２ａ、ならびに第２パーティ１０３ｂ及びそのそれぞれのコンピュータ機器１０２ｂである。より多くのこのようなパーティ１０３及びそれらのそれぞれのコンピュータ機器１０２がシステムに存在し、参加することができるが、便宜上、それらは図示されていないことが理解されよう。各パーティ１０３は、個人又は組織であってもよい。純粋に例示として、第１パーティ１０３ａは、本明細書においてAliceと称され、第２パーティ１０３ｂは、Bobと称されるが、これは限定的なものではなく、本明細書においてAlice又はBobという言及は、それぞれ「第１パーティ」及び「第２パーティ」と置き換えることができることは理解されるであろう。

【００４７】

各パーティ１０３のコンピュータ機器１０２は、１つ以上のプロセッサ、例えば１つ以上のCPU、GPU、他のアクセラレータプロセッサ、特定用途向けプロセッサ、及び/又はFPGAを備えるそれぞれの処理装置を備える。各パーティ１０３のコンピュータ機器１０２は、さらに、メモリ、すなわち、非一時的コンピュータ読取可能媒体又は媒体の形態のコンピュータ読取可能記憶装置を備える。このメモリは、例えば、ハードディスクなどの磁気媒体、ＳＳＤ、フラッシュメモリ又はEEPROMなどの電子媒体、及び/又は光ディスクドライブなどの光学的媒体を使用する１つ以上のメモリユニットを含んでもよい。各パーティ１０３のコンピュータ機器１０２上のメモリは、処理装置上で動作するように配置された少なくとも１つのクライアントアプリケーション１０５のそれぞれのインスタンスを含むソフトウェアを記憶する。所与のノード１０４に属するいずれの動作も、それぞれのコンピュータ機器１０２の処理装置上で実行されるソフトウェアを使用することにより実行され得ることが理解されよう。各パーティ１０３のコンピュータ機器１０２は、少なくとも１つのユーザ端末、例えばデスクトップ又はラップトップコンピュータ、タブレット、スマートフォン、又はスマートウォッチのようなウェアラブルデバイスを備えている。所与のパーティ１０３のコンピュータ装置１０２は、ユーザ端末を介してアクセスされるクラウドコンピューティングリソースのような、１つ以上の他のネットワーク接続されたリソースを含んでもよい。

【００４８】

クライアントアプリケーション又はソフトウェア１０５は、最初に、１つ以上の適切なコンピュータ読取可能な記憶媒体、例えばサーバからダウンロードされたもの、又はリムーバブルSSD、フラッシュメモリキー、リムーバブルEEPROM、リムーバブル磁気ディスクドライブ、磁気フロッピーディスク又はテープ、光ディスク、例えばCD又はDVD ROM、又はリムーバブル光学ドライブなどのリムーバブル記憶装置上で、任意の所与のパーティ１０３のコンピュータ機器１０２に提供され得る。

【００４９】

クライアントアプリケーション１０５は、少なくとも「ウォレット」機能を備える。これには主に２つの機能を有する。これらのうちの１つは、それぞれのユーザパーティ１０３が、ノード１０４のネットワーク全体にわたって伝播され、それによってブロックチェーン１５０に含まれるトランザクション１５２を作成し、署名し、送信することを可能にすることである。もう１つは、現在所有しているデジタルアセットの額をそれぞれのパーティに報告することである。アウトプットベースのシステムでは、この第２の機能は、当該パーティに属するブロックチェーン１５０全体に散在する様々なトランザクション１５

２のアウトプットの中で定義される量を照合することを含む。
【００５０】
各コンピュータ機器１０２上のクライアントアプリケーション１０５のインスタンスは、Ｐ２Ｐネットワーク１０６の転送ノード１０４Ｆの少なくとも１つに動作可能に結合される。これにより、クライアント１０５のウォレット機能は、トランザクション１５２をネットワーク１０６に送信することができる。クライアント１０５は、また、記憶ノード１０４のうちの１つ、一部、又は全部にコンタクトして、それぞれのパーティ１０３が受領者である任意のトランザクションについてブロックチェーン１５０に問い合わせることができる(又は、実施形態では、ブロックチェーン１５０は、部分的にその公開視認性を通じてトランザクションの信頼を提供する公開的設備であるため、実際には、ブロックチェーン１５０内の他のパーティのトランザクションを検査する)。各コンピュータ機器１０２上のウォレット機能は、トランザクションプロトコルに従ってトランザクション１５２を形成し、送信するように構成される。各ノード１０４は、ノードプロトコルに従ってトランザクション１５２を検証するように構成されたソフトウェアを実行し、転送ノード１０４Ｆの場合は、ネットワーク１０６全体にトランザクション１５２を伝播させるためにトランザクション１５２を転送する。トランザクションプロトコルとノードプロトコルは互いに対応し、所与のトランザクションプロトコルは所与のノードプロトコルと共に所与のトランザクションモデルを実装する。同じトランザクションプロトコルが、ブロックチェーン１５０内のすべてのトランザクション１５２に使用される(ただし、トランザクションプロトコルは、トランザクションの異なるサブタイプを許可することができる)。同じノードプロトコルは、ネットワーク１０６内のすべてのノード１０４によって使用される(ただし、多くのノードは、そのサブタイプに対して定義されたルールに従って異なるトランザクションのサブタイプを異なるように処理し、また、異なるノードは異なる役割を引き受け、従って、プロトコルの異なる対応する側面を実装することができる)。
【００５１】
上述のように、ブロックチェーン１５０は、ブロック１５１のチェーンを含み、各ブロック１５１は、前述のように、proof-of-workプロセスによって作成された１つ以上のトランザクション１５２のセットを含む。各ブロック１５１は、また、ブロック１５１への逐次的順序を定義するように、チェーン内の先に生成されたブロック１５１を遡ってポイントするブロックポインタ１５５を含む。ブロックチェーン１５０はまた、proof-of-workプロセスによって新しいブロックに含まれることを待つ有効なトランザクション１５４のプールを含む。各トランザクション１５２は、トランザクションのシーケンスに順序を定義するために、前のトランザクションへのポインタを含む(注：トランザクション１５２のシーケンスは、分岐することが許される)。ブロック１５１のチェーンは、チェーンの最初のブロックであったジェネシスブロック（genesis block (Gb)）１５３にまで戻る。チェーン１５０の初期に１つ以上のオリジナルトランザクション１５２は、先行するトランザクションではなくジェネシスブロック１５３を指し示した。
【００５２】
所与のパーティ１０３、例えばAliceがブロックチェーン１５０に含まれる新たなトランザクション１５２jを送信したいと望む場合、彼女は関連するトランザクションプロトコルに従って(彼女のクライアントアプリケーション１０５のウォレット機能を使用して)新たなトランザクションを定式化する（formulate）。次に、クライアントアプリケーション１０５からトランザクション１５２を、彼女が接続されている１つ以上の転送ノード１０４Ｆの１つに送信する。例えば、これは、Aliceのコンピュータ１０２に最も近いか又は最も良好に接続されている転送ノード１０４Ｆであってもよい。任意の所与のノード１０４が新しいトランザクション１５２jを受信すると、ノードプロトコル及びそのそれぞれの役割に従って、それを処理する。これは、最初に、新たに受信されたトランザクション１５２jが「有効」であるための特定の条件を満たしているかどうかをチェックすることを含み、その例については、簡単に詳述する。いくつかのトランザクションプロトコルでは、検証のための条件は、トランザクション１５２に含まれるスクリプトによってトランザクショ

ンごとに構成可能であってよい。あるいは、条件は単にノードプロトコルの組み込み機能であってもよく、あるいはスクリプトとノードプロトコルの組み合わせによって定義されてもよい。

【００５３】

新たに受信されたトランザクション１５２jが、有効であると見なされるテストに合格したという条件で(すなわち、「有効である」という条件で)、トランザクション１５２jを受信した任意の記憶ノード１０４Sは、そのノード１０４Sに維持されているブロックチェーン１５０のコピー内のプール１５４に、新たに有効とされたトランザクション１５２を追加する。さらに、トランザクション１５２jを受信する任意の転送ノード１０４Fは、検証済みトランザクション１５２をP２Pネットワーク１０６内の１つ以上の他のノード１０４に伝播する。各転送ノード１０４Fは同じプロトコルを適用するので、トランザクション１５２jが有効であると仮定すると、これは、P２Pネットワーク１０６全体に間もなく伝播されることを意味する。

【００５４】

ひとたび１つ以上の記憶ノード１０４で維持されるブロックチェーン１５０のコピー内のプール１５４に入ると、マイナーノード１０４Mは、新しいトランザクション１５２を含むプール１５４の最新バージョンのproof-of-workパズルを解決するために競争を開始する(他のマイナー１０４Mは、依然として、プール１５４の古いビューに基づいてパズルを解決しようとしているが、そこに到達した者は誰でも、最初に、次の新しいブロック１５１が終了し、新しいプール１５４が開始する場所を定義し、最終的には、誰かが、Aliceのトランザクション１５２jを含むプール１５４の一部のパズルを解決する)。一旦、新しいトランザクション１５２jを含むプール１５４についてproof-of-workが行われると、ブロックチェーン１５０内のブロック１５１の１つの一部となる。各トランザクション１５２は、以前のトランザクションへのポインタを含むので、トランザクションの順序もまた、不変的に記録される。

【００５５】

図２は、トランザクションプロトコルの例を示している。これは、UTXOベースのプロトコルの例である。トランザクション１５２(「Tx」と略す)は、ブロックチェーン１５０(各ブロック１５１は１つ以上のトランザクション１５２を含む)の基本的なデータ構造である。以下は、アウトプットベース又は「UTXO」ベースのプロトコルを参照して説明される。しかし、これは、全ての可能な実施形態に限定されるものではない。

【００５６】

UTXOベースのモデルでは、各トランザクション(「Tx」)１５２は、１つ以上のインプット２０２及び１つ以上のアウトプット２０３を含むデータ構造を含む。各アウトプット２０３は、未使用トランザクションアウトプット(UTXO)を含んでもよく、これは、別の新しいトランザクションのインプット２０２のソースとして使用することができる(UTXOがまだ償還されていない場合)。UTXOは、デジタルアセット（値のストア）の量を指定する。それは、情報の中でも特にその元となったトランザクションのトランザクションIDを含む。トランザクションデータ構造はまた、ヘッダ２０１も含んでよく、ヘッダ２０１は、インプットフィールド２０２及びアウトプットフィールド２０３のサイズの指示子を含んでもよいヘッダ２０１を含んでよい。ヘッダ２０１は、トランザクションのIDも含んでもよい。実施形態において、トランザクションIDは、トランザクションデータのハッシュ(トランザクションID自体を除く)であり、マイナー１０４Mに提出された未処理トランザクション１５２のヘッダ２０１に格納される。

【００５７】

例えばAlice１０３aは、問題のデジタルアセットの額をBob１０３bに移転するトランザクション１５２jを作成したいと考えているとする。図２において、Aliceの新しいトランザクション１５２jは「Tx_1」とラベル付けされている。これは、Aliceへのロックされているデジタルアセットの額を、シーケンス内の先行するトランザクション１５２iのアウトプット２０３に取り入れ、その少なくとも一部をBobに移転する。先行するトランザク

ション１５２iは、図２において「Tx_0」とラベル付けされている。Ｔｘ０とＴｘ１は、単なる任意のラベルである。これらは、必ずしも、Ｔｘ０がブロックチェーン１５１の最初のトランザクションであること、又は、Ｔｘ１がプール１５４の直ぐ次のトランザクションであることを意味しない。Tx_1は、まだAliceへのロックされた未使用アウトプット２０３を有する任意の先行する（つまり祖先）トランザクションのいずれかを指し示すことができる。

【００５８】

先行するトランザクションＴｘ０は、Aliceがその新しいトランザクションＴｘ１を作成するとき、又は少なくとも彼女がそれをネットワーク１０６に送信するときまでに、既に検証され、ブロックチェーン１５０に含まれていてもよい。それは、その時点で既にブロック１５１のうちの１つに含まれていてもよく、あるいは、プール１５４内でまだ待機していてもよく、その場合、新しいブロック１５１にすぐに含まれることになる。あるいは、Ｔｘ０及びＴｘ１が生成されネットワーク１０２に送信されることができ、あるいは、ノードプロトコルが「孤児（orphan）」トランザクションのバッファリングを許容する場合にはＴｘ１の後にＴｘ０が送信されることもできる。ここでトランザクションのシーケンスの文脈で使用される「先行する」及び「後の」という用語は、トランザクション内で指定されたトランザクションポインタ(どのトランザクションがどの他のトランザクションを指すかなど)によって定義されるシーケンス内のトランザクションの順序を指す。それらは、「先行者」及び「相続者」又は「祖先」及び「子孫」、「親」及び「子」、等により、等しく置き換えられ得る。これは、必ずしも、それらが作成され、ネットワーク１０６に送られ、又は任意の所与のノード１０４に到達する順序を意味しない。それにもかかわらず、先行するトランザクション(祖先トランザクション又は「親」)を指す後続のトランザクション(子孫トランザクション又は「子」)は、親トランザクションが検証されない限り、検証されない。親の前にノード１０４に到着した子は孤児とみなされる。それは、ノードプロトコル及び/又はマイナーの行動に応じて、親を待つために特定の時間、破棄又はバッファリングされることがある。

【００５９】

先行するトランザクションＴｘ０の１つ以上のアウトプット２０３のうちの１つは、本明細書でＵＴＸＯ０とラベル付けされた特定のＵＴＸＯを含む。各ＵＴＸＯは、ＵＴＸＯによって表されるデジタルアセットの額を指定する値と、後続のトランザクションが検証されるために、従ってＵＴＸＯが正常に償還されるために、後続のトランザクションのインプット２０２の中のアンロックスクリプトによって満たされなければならない条件を定義するロックスクリプトとを含む。典型的には、ロックスクリプトは、特定のパーティ(それが含まれているトランザクションの受益者)に量をロックする。すなわち、ロックスクリプトは、標準的に以下のようなアンロック条件を定義する：後続のトランザクションのインプット内のアンロックスクリプトは、先行するトランザクションがロックされたパーティの暗号署名を含む。

【００６０】

ロックスクリプト(別名scriptPubKey)は、ノードプロトコルによって認識されるドメイン固有の言語で書かれたコードの一部である。そのような言語の特定の例は、「スクリプト」(Script，capital S)と呼ばれる。ロックスクリプトは、トランザクションアウトプット２０３を消費するために必要な情報、例えば、Aliceの署名の必要条件を指定する。トランザクションのアウトプットには、アンロックスクリプトが現れる。アンロックスクリプト(別名：scriptSig)は、ロックスクリプトの基準を満たすために必要な情報を提供するドメイン固有の言語で書かれたコードの一部である。例えば、Bobの署名を含んでもよい。アンロックスクリプトは、トランザクションのインプット２０２に現れる。

【００６１】

図示の例では、Tx_0のアウトプット２０３の$UTXO_0$は、ロックスクリプト[$ChecksigP_A$]を含み、これは、$UTXO_0$が償還されるために(厳密には、$UTXO_0$を償還しようとする後続のトランザクションが有効であるために)、Aliceの署名$SigP_A$を必要とする。[Check

sigPA]は、Aliceの公開鍵と秘密鍵のペアからの公開鍵PAを含む。Tx_1のインプット２０２は、Tx_1を指すポインタ(例えば、そのトランザクションID、実施形態ではトランザクションTx_0全体のハッシュである$TxID_0$による)を含む。Tx_1のインプット２０２は、Tx_0の任意の他の可能なアウトプットの中でそれを識別するために、Tx_0内の$UTXO_0$を識別するインデックスを含む。Tx１のインプット２０２は、さらに、Aliceが鍵ペアからのAliceの秘密鍵をデータの所定の部分(暗号において「メッセージ」と呼ばれることもある)に適用することによって作成された、Aliceの暗号署名を含むアンロックスクリプト〈Sig PA〉を含む。有効な署名を提供するためにAliceが署名する必要があるデータ(又は「メッセージ」)は、ロックスクリプトにより、又はノードプロトコルにより、又はこれらの組み合わせによって定義され得る。

【００６２】

新しいトランザクションTx１がノード１０４に到着すると、ノードはノードプロトコルを適用する。これは、ロックスクリプトとアンロックスクリプトを一緒に実行して、アンロックスクリプトがロックスクリプトで定義されている条件(この条件は１つ以上の基準を含むことができる)を満たしているかどうかをチェックすることを含む。実施形態では、これは、２つのスクリプトの連結を含む。

【数１】

$$<\text{Sig } P_A> <P_A> \,||\, [\text{Checksig } P_A]$$

ここで、「¦¦」は連結を表し、「〈...〉」はスタックにデータを配置することを意味し、「[...]」はアンロックスクリプトに含まれる機能である（本例では、スタックベースの言語）。同等に、スクリプトは。、スクリプトを連結するのではなく共通のスタックにより１つずつ実行されてよい。いずれの方法でも、一緒に実行する場合、スクリプトは、Tx_0のアウトプット内のロックスクリプトに含まれるAliceの公開鍵P_Aを使用して、Tx_1のインプット内のロックスクリプトが、データの期待部分に署名するAliceの署名を含むことを認証する。また、データの期待部分(「メッセージ」)も、この認証を実行するためにTx０に含まれる必要がある。実施形態において、署名されたデータは、Tx０の全体を含む(従って、別個の要素は、データの署名された部分がすでに本質的に存在するので、データの署名された部分の指定にクリアに含まれる必要がある)。

【００６３】

公開－秘密暗号法による認証の詳細は、当業者には周知であろう。基本的に、Aliceが彼女の秘密鍵によりメッセージを暗号化することによってメッセージに署名した場合、Aliceの公開鍵とそのメッセージが明らか(暗号化されていないメッセージ)ならば、ノード１０４のような別のエンティティは、そのメッセージの暗号化されたバージョンがAliceによって署名されていなければならないことを認証することができる。署名は、典型的には、メッセージをハッシュし、ハッシュに署名し、署名としてメッセージのクリアなバージョンにこれをタグ付けすることによって、公開鍵の所有者が署名を認証することを可能にする。従って、実施形態では、特定のデータ片又はトランザクションの部分等に署名するという言及は、データ片又はトランザクションの部分のハッシュに署名することを意味し得る。

【００６４】

Tx１内のアンロックスクリプトが、Tx０のロックスクリプトで指定された１つ以上の条件を満たす場合(示される例では、Aliceの署名がTx１内で提供され、認証されている場合)、ノード１０４は、Tx１が有効であるとみなす。それが記憶ノード１０４Sである場合、これは、proof-of-workを待つトランザクションのプール１５４にそれを追加することを意味する。それが転送ノード１０４Fである場合、それはトランザクションTx１をネットワーク１０６内の１つ以上の他のノード１０４に転送し、それによって、それがネットワーク全体に伝播されることになる。一旦、Tx１が検証され、ブロックチェーン１５０に含まれると、これは、Tx０からのUTXO０を消費したものとして定義する。Tx１は、未使用トランザクションアウトプット２０３を使用する場合にのみ有効であることに留意された

い。別のトランザクション１５２によってすでに消費されたアウトプットを消費しようとする場合、Tx１は、たとえ他のすべての条件が満たされていても無効となる。従って、ノード１０４は、先行するトランザクションTx０において参照されたUTXOが既に使用されているかどうか(既に別の有効なトランザクションへの有効なインプットを形成しているかどうか)もチェックする必要がある。これが、ブロックチェーン１５０がトランザクション１５２に定義された順序を課すことが重要である理由の１つである。実際には、所与のノード１０４は、トランザクション１５２が消費されたUTXO２０３をマークする別個のデータベースを維持することができるが、最終的には、UTXOが消費されたかどうかを定義するのは、ブロックチェーン１５０内の別の有効なトランザクションへの有効なインプットを既に形成しているかどうかである。

【００６５】

UTXOベースのトランザクションモデルでは、所定のUTXOを全体として使用する必要があることに注意する。UTXOで定義されている量のうち、別の分量が消費されている一方で、分量を「残しておく」ことはできない。ただし、UTXOからの量は、次のトランザクションの複数のアウトプットに分割できる。例えば、Tx０のUTXO０で定義された量は、Tx１の複数のUTXOに分割できる。したがって、AliceがBobにUTXO０で定義された量のすべてを与えることを望まない場合、彼女は残りの量を使って、Tx１の第２のアウトプットの中で自分自身にお釣りを与えるか、又は別のパーティに支払うことができる。

【００６６】

実際には、Aliceは通常、勝ったマイナーのための手数料も含める必要がある。なぜなら、今日では、生成トランザクションの報酬だけでは、マイニングを動機づけるには通常十分ではないからである。Aliceがマイナーのための手数料を含まない場合、Tx０はマイナーのノード１０４Mによって拒否される可能性が高く、したがって、技術的には有効であるが、それは依然として伝播されず、ブロックチェーン１５０に含まれない（マイナーのプロトコルは、マイナーが望まない場合には、マイナー１０４Mにトランザクション１５２を受け入れるよう強制しない)。一部のプロトコルでは、マイニング料金は、独自の別個のアウトプット２０３を必要としない(すなわち、別個のUTXOを必要としない)。代わりに、インプット２０２によって指される総量と、所与のトランザクション１５２のアウトプット２０３の中で指定される総量との間の差は、勝ったマイナー１０４に自動的に与えられる。例えば、UTXO０へのポインタがTx１への唯一のインプットであり、Tx１は１つのアウトプットUTXO１しか持っていないとする。UTXO０で指定されたデジタルアセットの額がUTXO１で指定された量より多い場合、その差は自動的に勝ったマイナー１０４Mへ行く。しかし、代替的又は追加的に、必ずしも、トランザクション１５２のUTXO２０３のうちの独自のものにおいて、マイナー手数料を明示的に指定できることは除外されない。

【００６７】

所与のトランザクション１５２の全部のアウトプット２０３の中で指定された総量が全部のそのインプット２０２により指される総量より大きい場合、これは、殆どのトランザクションモデルにおいて無効の別の基礎であることに留意する。従って、このようなトランザクションは、伝播されず、マイニングされてブロック１５１にされることもない。

【００６８】

Alice及びBobのデジタルアセットは、ブロックチェーン１５０内の任意のトランザクション１５２の中で彼らへのロックされた未使用UTXOで構成されている。従って、典型的には、所与のパーティ１０３のアセットは、ブロックチェーン１５０を通して、様々なトランザクション１５２のUTXO全体に分散される。ブロックチェーン１５０内のどこにも、所与のパーティ１０３の総残高を定義する１つの数値は記憶されていない。各パーティへのロックされた、別の将来の（onward）トランザクションにまだ消費されていないすべての様々なUTXOの値をまとめることは、クライアントアプリケーション１０５におけるウォレット機能の役割である。これは、記憶ノード１０４Sのいずれかに記憶されたブロックチェーン１５０のコピーを、例えば、各パーティのコンピュータ機器０２に最も近い

か、又は最も良好に接続されている記憶ノード１０４Ｓに問い合わせることによって行うことができる。

【００６９】

スクリプトコードは、概略的に表現されることが多い(すなわち、正確な言語ではない)ことに注意する。例えば、[Checksig P_A]を[ChecksigP_A]=OP_DUPOP_HASH１６０〈H(P_A)〉OP_EQUALVERIFYOP_CHECKSIGを意味するように記述し得る。「OP_....」は、スクリプト言語の特定のオペコードを表す。OP_CHECKSIG(「Checksig」とも呼ばれる)は、２つのインプット(署名と公開鍵)を取り込み、楕円曲線デジタル署名アルゴリズム(Elliptic Curve Digital Signature Algorithm (ECDSA))を使用して署名の妥当性を検証するスクリプトオペコードである。ランタイムでは、署名(「si」')の発生はすべてスクリプトから削除されるが、ハッシュパズルなどの追加要件は、「sig」インプットによって検証されるトランザクションに残る。別の例として、OP_RETURNは、トランザクション内にメタデータを格納することができ、それによってメタデータをブロックチェーン１５０に不変に記録することができるトランザクションの使用不可能アウトプットを生成するためのスクリプト言語のオペコードである。例えば、メタデータは、ブロックチェーンに格納することが望ましいドキュメントを含むことができる。

【００７０】

署名PAは、デジタル署名である。実施形態において、これは楕円曲線secp２５６ｋ１を使用するECDSAに基づく。デジタル署名は、特定のデータに署名する。実施形態では、所与のトランザクションについて、署名はトランザクションインプットの一部、及びトランザクションアウトプットの全部又は一部に署名する。署名するアウトプットの特定の部分はSIGHASHフラグに依存する。SIGHASHフラグは、署名の最後に含まれる４バイトのコードであり、どのアウトプットが署名されるかを選択する(従って、署名の時点で固定される)。

【００７１】

ロックスクリプトは、それぞれのトランザクションがロックされているパーティの公開鍵を含んでいることを表す「scriptPubKey」と呼ばれることがある。アンロックスクリプトは、対応する署名を提供することを表す「scriptSig」と呼ばれることがある。しかし、より一般的には、UTXOが償還される条件が署名を認証することを含むことは、ブロックチェーン１５０のすべてのアプリケーションにおいて必須ではない。より一般的には、スクリプト言語は、１つ以上の条件を定義するために使用され得る。したがって、より一般的な用語「ロックスクリプト」及び「アンロックスクリプト」が好ましい。

【００７２】

図３は、ブロックチェーン１５０を実装するためのシステム１００を示す。システム１００は、追加の通信機能が含まれることを除いて、図１に関連して説明したものと実質的に同じである。Alice及びBobのコンピュータ機器１０２ａ、１０２ｂの各々に存在するクライアントアプリケーションは、それぞれ、追加通信機能を含む。つまり、それは、Alice１０３ａが、(いずれかのパーティ又は第３者の勧誘で)Bob１０３ｂとの別個のサイドチャネル３０１を確立することを可能にする。サイドチャネル３０１は、Ｐ２Ｐネットワークと別個にデータの交換を可能にする。このような通信は、時に「オフチェーン」と呼ばれる。例えば、これは、パーティのうちの一方がトランザクションをネットワーク１０６にブロードキャストすることを選択するまで、トランザクションがネットワークＰ２Ｐ１０６に（まだ）発行されることなく、又はチェーン１５０乗でそのようにすることなく、AliceとBobとの間でトランザクション１５２を交換するために使用されてよい。このようなサイドチャネル３０１は、時に、例えば「支払いチャネル」として使用される。

【００７３】

サイドチャネル３０１は、Ｐ２Ｐオーバレイネットワーク１０６と同じパケット交換ネットワーク１０１を介して確立されてもよい。代替又は追加で、サイドチャネル３０１は、モバイルセルラネットワーク、又はローカル無線ネットワークのようなローカルエリアネットワーク、又はAliceとBobの装置１０２ａ、１０２ｂの間の直接有線若しくは無線リン

クのような異なるネットワークを介して確立されてよい。一般に、本願明細書のどこかで言及されるサイドチャネル３０１は、「オフチェーン」で、つまりＰ２Ｐオーバレイネットワーク１０６と別個にデータを交換するための１つ以上のネットワーキング技術又は通信媒体を介する任意の１つ以上のリンクを含んでよい。１つより多くのリンクが使用されるとき、全体としてのオフチェーンリンクのバンドル又は集合がサイドチャネル３０１と呼ばれてよい。従って、Alice及びBobが特定の情報又はデータ片等をサイドチャネル３０１を介して交換すると表される場合、これは、必ずしも全部のこれらのデータ片が正確に同じリンクまたは同じ種類のネットワークを介して送信される必要があることを意味しないことに留意する。

【００７４】

＜例示的な定義＞

以下は、幾つかの実装において採用得る幾つかの例示的な定義である。これらは、全部の可能な実装を限定するものではなく、後述する例示的な使用例の幾つかの可能な実装において利用され得る特定の可能な実装の理解を助けるためだけに提供されることに留意する。

【００７５】

定義１：トランザクション。トランザクションは、インプットとアウトプットとを含むメッセージである。それは、プロトコルバージョン番号及び／又はロックタイム（locktime）も含んでよい。プロトコルバージョンは、トランザクションプロトコルのバージョンを示す。ロックタイムは、後に個別に説明される。

【００７６】

定義２：インプットトランザクションのインプットは、順序付きリストを形成する。リスト内の各エントリは、アウトプット（未使用トランザクションアウトプットの識別子）、及びscriptSig（アンロックスクリプト）を含む。それは、シーケンス番号も含んでよい。

【００７７】

定義３：アウトプット：トランザクションのアウトプットは、順序付きリストを形成する。リスト内の各エントリは、値（その基本単位におけるデジタルアセットの額）、及びscriptPubKey（ロックスクリプト）を含む。

【００７８】

定義４：アウトポイント。アウトポイントは、トランザクションID　TxID、及びインデックス番号iによりユニークに定義される。トランザクションアウトプットTxIDのアウトプットの中のi番目のエントリを表し、未使用トランザクションアウトプット（UTXO）のユニークな位置を与える。用語「未使用（unspent）」は、本願明細書で、アウトポイントが任意の有効な後続のトランザクションの中に現れていないことを意味する。

【００７９】

定義５：scriptSig。これは、所与のアウトポイントに対応するUTXOをアンロックする又は使用するために要求される情報である。標準的なトランザクションでは、この情報は通常ECDSA署名である。従って、スクリプトは「scriptSig」と呼ばれる。しかしながら、アウトポイントをアンロックするために必要な情報は、UTXOのロック条件を満たす任意のデータであり得る。

【００８０】

定義６：scriptPubKey。これは、特定のUTXOに関連付けられた資金をロックするスクリプトである。scriptSigがscriptPubKeyに付加され、結合されたスクリプトの実行が真を与える場合に及びその場合にのみ、資金がアンロックされ、使用できる。そうでない場合には、トランザクションは無効であり、拒否される。これは、通常、標準的なトランザクションではECDSA公開鍵のハッシュ値を含むので、「scriptPubKey」と呼ばれる。

【００８１】

次の定義では、インプット又はアウトプットへの署名が参照され、これは、scriptSig部分（定義２を参照）を除く１つ又は複数のインプットへの署名を意味する。

【００８２】
定義７：SIGHASHフラグ。ECDSA署名を提供するとき、以下のSIGHASHフラグのうちの１つも付加する必要がある。
【表１】

フラグ	関数の意味
SIGHASH_ALL	全部のインプット及びアウトプットに署名する
SIGHASH_SINGLE	全部のインプット及び同じインデックスを有するアウトプットに署名する
SIGHASH_NONE	全部のインプットに署名し、アウトプットに署名しない
SIGHASH_ALL | ANYONECANPAY	自身のインプット及び全部のアウトプットに署名する
SIGHASH_SINGLE | ANYONECANPAY	自身のインプット及び同じインデックスを有するアウトプットに署名する
SIGHASH_NONE | ANYONECANPAY	自身のインプットに署名し、アウトプットに署名しない

【００８３】
適応性を機能として議論するとき、トランザクション内で、ECDSA署名により署名されていない情報を探す。署名されるべきメッセージから除外され得るインプット及びアウトプットとは別に、scriptSigのコンテンツは常に除外される。これは、scriptSigが署名のプレースホルダーであるよう設計されるからである。
【００８４】
定義８：ブロックチェーンタイムロック。一般に、トランザクション内で使用可能な２つのタイプのタイムロック：絶対的タイムロック及び相対的タイムロックがある。絶対的タイムロックは、その後に何かが「有効」であると考えられる特定の時点を指定する。一方で、相対的タイムロックは、何かが有効であると考えられる前に経過しなければならない期間を指定する。両方の場合に、ブロックチェーンタイムロックを使用するときの時間の代わりとして、ブロック高（マイニングされたブロックの数）又は経過時間（例えば、UNIX（登録商標）時間）を使用できる。
【００８５】
ブロックチェーンタイムロックの別の特性は、それらが表れる場所であり、それらが適用されるトランザクションの態様である。ここでも、この意味でタイムロックの２つの分類：トランザクション全体をロックするトランザクションレベル、及び特定のアウトプットをロックするスクリプトレベルがある。これらのタイムロックは両方とも、絶対的タイムロック又は相対的タイムロックのいずれかを実装するために使用できる。以下の表は、これらの特性に基づき生成可能なタイムロックを実装する４つの可能なメカニズムを纏めたものである。

【表２】

		タイプ	
		Absolute（絶対的）	*Relative*（相対的）
レベル	トランザクション レベル	nLocktime	nSequence
	スクリプト レベル	OP_CLTV	OP_CSV

【００８６】
定義９：nLocktime。ロックタイム（nLocktime）は、ブロック高又はUNIX時間で特定の時間を表す負ではない整数である。それは、トランザクションが指定されたブロック又は指定された時間の後にのみブロックチェーンに追加できるという意味で、トランザクションレベルのタイムロックである。nLocktimeが５００，０００，０００より小さく設定される場合、それはブロック高と考えられる。それが５００，０００，０００以上に設定された場合、それはUNIX時間の表現と考えられる。それは、１９７０年１月１日の００：００：００の後の秒数である。
【００８７】
例えば、現在のブロック高が３，０００，０００の高さであり、ロックタイムは４，０００，０００に設定される場合、トランザクションは、４百万番目のブロックがマイニングされるまで、マイナーにより検討されない。
【００８８】
定義１０：nSequence。シーケンス番号（nSequence）は、トランザクションのバージョンをメッセージとして示す。トランザクションに対する任意の変更は、シーケンス番号を１つ大きくインクリメントする。nSequenceの最大値は$2^{32}-1$であり、通常、シーケンス番号は、デフォルトでこの最大値に設定されてトランザクションが完了していることを示す。nSequence値は、トランザクションの各インプットについて定義され、インプットにより参照されるUTXOがブロックに含まれた後、有効なインプットとして使用可能になる前の時間期間を指定する。マイナーが同じインプットを有する２つのトランザクションを認識した場合、マイナーは、より大きなシーケンス番号を有するトランザクションを選択する。しかしながら、この特徴は、一般的に無効にされている。
【００８９】
定義１１：CheckLockTimeVerify （OP_CLTV)。オペコードOP_CHECKLOCKTIMEVERIFY （OP_CLTV)は、将来の何らかの特定の時間又はブロック高にトランザクションの特定のアウトプットをロックするために使用可能な絶対的スクリプトレベルのタイムロックである。UTXOがトランザクション内で参照される現在のUNIX時間又はブロック高が、UTXOが生成されたUNIX時間又はブロック高にOP_CLTVオペコードの前に指定されたパラメータを足したものを超える場合、支払いトランザクションについてのスクリプト実行は失敗する。
【００９０】
定義１２：CheckSequenceVerify （OP_CSV)。オペコードOP_CHECKSEQUENCEVERIFY （OP_CSV)は、将来の特定の時間期間又はブロック数についてトランザクションの特定のアウトプットをロックするために使用可能な相対的スクリプトレベルのタイムロックである。これはOP_CLTVと同様に動作するが、OP_CSVに提供されるパラメータが相

対的時間を表すことが異なる。UTXOがトランザクション内で参照される現在のUNIX時間又はブロック高が、UTXOが生成されたUNIX時間又はブロック高にOP_CSVオペコードの前に指定されたパラメータを足したものを超える場合、支払いトランザクションについてのスクリプト実行は失敗する。

【００９１】

定義１３：適応性（Malleability）。一般に、ブロックチェーントランザクションにおいて可能な２つの広義の適応性がある。それらは両方とも、インプットの中で提供される署名を無効にすることなく、トランザクションの内容を変更できるようにする。

【００９２】

両方の場合を説明するために、１つのインプットと、該インプットの中の１つの署名と、１つのアウトプットと、を有する初期トランザクションTxを考える。

【００９３】

タイプ１：スクリプトレベルの適応性。このタイプの適応性は、スクリプトオペコードOP_CHECKSIGによりチェックされるべき署名が、トランザクション内の任意のインプットのスクリプトフィールドに署名しないという事実を利用する。この事実は、トランザクションTxに対する署名を生成し、インプットスクリプトを変更して、トランザクションTx'がTxと同一ではないが、依然としてTx’及びTxが両方とも、ブロックチェーン合意ルールの下で同じ署名により署名された有効なトランザクションメッセージと考えられることを可能にする。

【００９４】

タイプ２：インプット及びアウトプットレベルの適応性。このタイプの適応性は、トランザクション内で利用されているSIGHASH ALL以外のSIGHASHフラグの使用に依存する。トランザクションTxが、５個の他のSIGHASHフラグの組合せのうちのいずれかを使用するインプット署名を有する場合、（１又は複数の）インプット又は（１又は複数の）アウトプットのいずれかが追加されて、同一ではないトランザクションTx'を生成できる。その結果、両者は、署名を変更する必要を伴わずに、合意に従い有効なトランザクションメッセージと考えられる。

【００９５】

特徴としての適応性

【００９６】

図４は、本開示の方式の実施形態を実装するためのクライアントアプリケーション１０５の例示的な実装を示す。クライアントアプリケーション１０５は、トランザクションエンジン４０１と、ユーザインタフェース（UI）レイヤ４０２と、を含む。トランザクションエンジン４０１は、上述の方式に従い、及び以下に詳細に議論するように、トランザクション１５２を形成する、トランザクション及び／又は他のデータをサイドチャネル３０１を介して受信及び／又は送信する、及び／又はP２Pネットワーク１０６を通じて伝播されるようにトランザクションを送信するような、クライアント１０５の基礎にあるトランザクション関連機能を実装するよう構成される。本願明細書に開示される実施形態によると、少なくともBobのクライアント１０５bのトランザクションエンジン４０１は、選択関数の形式のアプリケーション機能４０３を含む。これは、ターゲットトランザクション（「Tx_p」及び「Tx_p’」）の２つ以上の異なるバージョンのうちのどれが、検証のためにP２Pネットワーク１０６と通じて伝播され、従ってブロックチェーン１５０に記録されるように（伝播及び記録それら自体は、前述のメカニズムにより行われる）、Bobのそれぞれのコンピュータ機器１０２から送信されるべきかに関する選択を可能にする。ここでも、この送信は、Bobのコンピュータ機器１０２bからネットワーク１０６の転送ノード１０４Fのうちの１つへターゲットトランザクションを直接送信すること、又はAliceの機器１０２bへ若しくはネットワーク１０６のノード１０４Fのうちの１つへ転送されるように第三者の機器へターゲットトランザクションを送信すること、を含み得る。

【００９７】

UIレイヤ４０２は、それぞれのユーザコンピュータ機器１０２のユーザ入力／出力（I/

０）手段を介して、機器１０２のユーザ出力手段によりそれぞれのユーザ１０３へ情報を出力すること及び機器１０２のユーザ入力手段によりそれぞれのユーザ１０３から入力を受信することを含む、ユーザインタフェースをレンダリングするよう構成される。例えば、ユーザ出力手段は、視覚出力を提供する１つ以上のディスプレイスクリーン（タッチ又は非タッチスクリーン）、オーディオ出力を提供する１つ以上のスピーカ、及び／又は触覚出力を提供する１つ以上の触覚出力装置、等を含み得る。ユーザ入力手段は、例えば、（出力手段のために使用されるものと同じ又は異なる）１つ以上のタッチスクリーンの入力アレイ、マウス、トラックパッド、若しくはトラックボールのような１つ以上のカーソルに基づく装置、会話若しくは音声入力を受信する１つ以上のマイクロフォン及び会話若しくは音声認識アルゴリズム、手動若しくは身体ジェスチャの形式で入力を受信する１つ以上のジェスチャに基づく入力装置、又は１つ以上の機械的ボタン、スイッチ、若しくはジョイスティック、等を含み得る。

【００９８】

注：本願明細書において種々の機能が同じクライアントアプリケーション１０５に統合されるとして説明されることがあるが、これは、必ずしも限定的ではなく、代わりに、それらは２つ以上の異なるアプリケーションのスーツに実装されてよく、例えば一方が他方へのプラグインである。例えば、トランザクションエンジン４０１の機能は、UIレイヤ４０２と別個のアプリケーション、又は所与のモジュールの機能に実装されてよく、トランザクションエンジン４０１が１つより多くのアプリケーションの間で分割されてよい。また、記載の機能の一部又は全部が、例えばオペレーティングシステムレイヤに実装されることを除外しない。本願明細書のどこかで、単一の又は所与のアプリケーション１０５等を参照する場合、これが単に例であること、より一般的には、記載の機能が任意の形式のソフトウェアで実装され得ることが理解される。

【００９９】

図５は、Bobの機器１０２b上のクライアントアプリケーション１０５のUIレイヤ４０２によりレンダリングされてよいユーザインタフェース（UI）５００の例の模擬表示を与える。ユーザインタフェース５００は、少なくとも２つのユーザ選択可能オプション５０１、５０２を含む。これらは、２つのスクリーン上のボタン又はメニューの中の２つの異なるオプションのように、ユーザ出力手段により２つの異なるUI要素としてレンダリングされてよい。ユーザ入力手段は、スクリーン上のUI要素をクリック若しくはタッチすることにより、又は所望のオプションの名称を発話することにより、ユーザ１０３b（この場合にはBob）がオプションのうちの１つを選択できるよう構成される（注：ここで使用される「手動（manual）」は単に自動の反対を意味し、手の使用に限定されない）。オプションをレンダリング及び選択する特定の手段は重要でないことが理解される。

【０１００】

どんな手段が使用されても、オプションの各々は第１及び第２ターゲットトランザクションTx_p及びTx_p’の異なる１つに対応する。選択機能４０３は、以下を可能にするためにUIレイヤ４０２とインタフェースするよう構成される。つまり、Bob１０３bが第１オプション５０１を選択した場合、これは、トランザクションエンジン４０３に、ネットワーク１０６を通じて伝播させブロックチェーン１５０に記録されるように、ターゲットトランザクションの第１バージョンTx_pを送信させる。しかし、Bob１０３bが第２オプション４０３を選択した場合、これは、トランザクションエンジン４０３に、ネットワーク１０６を通じて伝播させブロックチェーン１５０に記録されるように、ターゲットトランザクションの第１バージョンTx_p’を送信させる。

【０１０１】

図５に示されるUI５００は、単なる概略的な模擬表示であり、実際には、それは、簡潔さのために図示されない１つ以上の更なるUI要素を含んでよいことが理解される。

【０１０２】

UIオプション５０１、５０２の代替又は追加として、選択機能４０３は、ブロックチェーン１５０に記録するために、ターゲットトランザクションの第１及び第２バージョンTx_p

又はTx_p’の送信の間で自動選択を実行するよう構成されてよい。これは、所定のイベントに依存して又は所定のタイムアウトの後に、自動的にトリガされてよい。例えば、イベントYがタイムアウトの前に生じた場合、機能４０３は、ネットワーク１５０を通じて伝播されるよう第２バージョンTx_p’を自動的に送信する。しかし、イベントYが生じる前に、タイムアウトが経過した場合、機能４０３は、代わりに、第１バージョンTx_pを自動的に送信する。或いは、イベントXが生じた場合、機能４０３は、ネットワーク１５０を通じて伝播されるよう第１バージョンTx_pを自動的に送信する。しかし、イベントYが生じた場合、機能４０３は代わりに、第２バージョンTx_p'を自動的に送信する。原則では、ネットワーク１５０へ第１バージョン及び第２バージョンを自動的に送り出すための環境は、システム設計者により事実上何でも構成され得る。

【０１０３】

図６は、本願明細書に開示される実施形態に従い使用するためのトランザクション１５２のセットを示す。セットは、第０トランザクションTx_0、第１トランザクションTx_1、及び第２トランザクションTx_p/Tx_p’を含む。これらの名称は単に便宜上のラベルであることに留意する。それらは、必ずしも、これらのトランザクションが直ちに１つずつブロック１５１又はブロックチェーン１５０内に置かれること、又は第０トランザクションがブロック１５１又はブロックチェーン１５０内の最初のトランザクションであることを意味しない。また、これらのラベルは、それらのトランザクションがネットワーク１０６へ送信される順序に関して何も示唆しない。それらは、単に、１つのトランザクションのアウトプットが次のトランザクションのインプットによりポイントされる論理的シリーズを表す。幾つかのシステムでは、親をその子の後にネットワーク１０６へ送信することが可能であることを思い出してほしい（この場合、「親のない」子がある期間の間、１つ以上のノード１０４においてバッファされ、その間、親が到着するのを待っている）。

【０１０４】

２つのトランザクションTx_p又はTx_p’は、両者が第１トランザクションの同じアウトプット（例えば、同じUTXO）を参照するインプットを含む場合、（実質的に）同じトランザクションのバージョンであると言える。異なるバージョンは、そのアウトプットの異なるアンロック条件を満たすことにより、異なる機能を提供し得る。異なるバージョンは、両方とも、同一のインプット署名も含んでよい（つまり、いずれのインスタンスの中の署名済みメッセージが同一である）。後述する幾つかの実施形態は、第１トランザクションの異なるインスタンスTx_i(ここで、i=１,２,３,…)も含んでよい。２つ（以上）のトランザクションは、ここでは、両者が同じソーストランザクション（又は「第０」トランザクション）の同じアウトプット（例えばUTXO）Tx_0を参照するインプットを含む場合、（実質的に）同じ第１トランザクションのインスタンスであると言える。それらは、同じアンロック条件を満たすことに基づき、該インプットを償還してよい。それらは、しかしながら、異なるインプット署名を含んでよい（つまり、いずれのインスタンスの中の署名済みメッセージが同一ではない）。異なるインスタンスは、異なるそれぞれのデータ部分に対する支払い、及びデジタルアセットの増分量を指定するが、実質的に同じ機能を提供してよい。これは、図７～９、及び例示的な使用例２を参照して後に詳述する。

【０１０５】

第０トランザクションTx_0は、本発明の目的のためにソーストランザクションと呼ばれてもよく、Alice１０３aへのロックされたデジタルアセットの額のソースとして機能する。第１トランザクションTx_1は、本発明の目的のために、中間トランザクション又は条件付きトランザクションと呼ばれてもよく、ソーストランザクションTx_0からデジタルアセットの額を条件付きで移転する仲介として機能する。第２トランザクションTx_p/Tx_p’はターゲットトランザクション又は支払いトランザクション（ここでは添え字「P」）と呼ばれてもよく、条件のうちの１つをアンロックし、Bob（又は場合によっては、Bobが代表を務める受益者）への支払いを提供するトランザクションである。上述のように、ターゲットトランザクションは、２つのバージョン、第１バージョンTx_p及び第２バージョンTx_p’を有する。これらのトランザクションは、それぞれ、Alice（第１パーティ）のコンピュ

ータ機器１０２a又はBob（第２パーティ）のコンピュータ機器１０２b、或いは第三者のコンピュータ機器（図示しない）、又はこれらの任意の組合せ、のいずれかにおいて少なくともある時点で存在し、明示される。２つのバージョンTx_p及びTx_p'は、並列に一緒にある期間の間、又は１つずつ、又は部分的に時間において重複して、存在してよい。

【０１０６】

図６に示すように、ソーストランザクションTx_0は、デジタルアセットの額を指定する少なくとも１つのアウトプット２０３$_0$（例えば、Tx_0のアウトプット０）、及びAlice１０３aへのこのアウトプットをロックするロックスクリプトを更に含む。これは、ソーストランザクションTx_0のロックスクリプトが、少なくとも１つの条件が満たされることを要求することを意味する。この条件は、アウトプットをアンロックしようとする（従って、デジタルアセットの額を償還する）任意のトランザクションのインプットが、そのアンロックスクリプト内にAliceの暗号署名（つまり、Aliceの公開鍵を使用する）を含まなければならないことである。この意味で、Tx_0のアウトプット内で定義される量は、Aliceにより所有されると言える。アウトプットは、UTXOと呼ばれてよい。どの先行するトランザクションのアウトプットがTx_0のインプットをポイントするかは（それらが、Tx_0の合計アウトプットをカバーするのに十分である限り）、本発明の目的のために特に重要ではない。

【０１０７】

本発明の場合には、ソーストランザクションTx_0のアウトプットをアンロックするトランザクションは、第１又は中間トランザクションTx_1である。従って、Tx_1は、Tx_0の関連するアウトプット（図示の例ではTx_0のアウトプット０）へのポインタを含み及び該アウトプットのロックスクリプト内で定義された条件に従いTx_0のポイントされたアウトプットをアンロックするよう構成される、少なくともAliceの署名を要求するアンロックスクリプトを更に含む、少なくとも１つのインプット２０２$_1$（例えばTx_1のインプット０）を有する。Tx_0のロックスクリプトにより要求されるAliceからの署名は、Tx_1の特定の部分に署名することが要求される。幾つかのプロトコルでは、署名される必要のあるTx_1の部分は、Tx_1のアンロックスクリプト内で定義された設定であり得る。例えば、これは、署名に付加される１バイトであるSIGHASHフラグにより設定されてよい。従って、データの観点では、アンロックスクリプトは次の通りである：〈Sig P_A〉〈sighashflag〉〈P_A〉代替として、署名される必要のあるの部分は、単にTx_1.の固定部分であってよい。いずれの方法も、署名されるべき部分は、標準的に、アンロックスクリプト自体を除き、及びTx_1のインプットの一部又は全部を除いてよい。これは、Tx_1のインプットが適応性があることを意味する。

【０１０８】

第１又は中間トランザクションTx_1は、少なくとも１つのアウトプット２０３$_1$（例えば、ここでもアウトプットがUTXOと呼ばれてよいTx_1のアウトプット０）を有する。中間トランザクションTx_1のアウトプットは、無条件には任意の１つのパーティにロックされない。Tx_0と同様に、それは、転送されるべきデジタルアセットの額を指定する少なくとも１つのアウトプット（例えば、Tx_1のアウトプット０）を有する。該アウトプットは、該アウトプットをアンロックする、従って該量を償還するために何が必要かを定義するロックスクリプトを更に含む。しかしながら、このロックスクリプトは、少なくとも（ｉ）第１条件（「条件１」）及び（ｉｉ）第２条件（「条件２」）を含む複数の異なる可能な条件のうちの任意の１つに基づき、そのアウトプットがアンロックされること可能にする。

【０１０９】

第２の、ターゲットトランザクションTx_p/Tx_p'は、少なくとも１つのインプット２０２p（例えば、Tx_p/Tx_p'のインプット０）を有し、該インプットは、Tx_1の上述のアウトプット（図示の例ではTx_1のアウトプット０）へのポインタを含み、Tx_1のロックスクリプトの中で定義された複数の代替条件のうちの１つを満たすことに基づきTx_1の該アウトプットをアンロックするよう構成されるアンロックスクリプトも更に含む。ターゲットトラ

ンザクションの第１バージョンTx_pでは、ロックスクリプトは、第１条件、条件１を満たすよう構成される。幾つかのポイントで、ターゲットトランザクションの第２バージョンTx_p’も生成される。第２バージョンでは、アンロックスクリプトは、第２条件、条件２を満たすよう構成される。

【０１１０】

第２の、ターゲットトランザクションTx_p/Tx_p’は、少なくとも１つのアウトプット２０２ｐ（例えば、Tx_p/Tx_p’のアウトプット０）を有し、該アウトプットは、いずれのバージョンでも、Bobへ移転すべきデジタルアセットの額、及びこれをBobに対してロックするロックスクリプトを指定する（つまり、これは、更なる、今後のトランザクションが、使用するためにアンロックスクリプトの中にBobの署名を含むことが要求される）。この意味で、ターゲットトランザクションTx_p/Tx_p’のアウトプットは、Bobにより所有されると言える。このアウトプットは、ここでもUTXOと呼ばれてよい。

【０１１１】

実施形態では、第１条件は、Tx_1、この場合にはターゲットトランザクションの第１バージョンTx_p、をアンロックしようとするトランザクションのアンロックスクリプトが、自身のアンロックスクリプト内に、Bobの暗号署名、及び／又はBobが提供又は含めなければならないBobのデータであってよいデータペイロード、を含むことを要求する。データペイロードを含むという要件は、Tx_1のロックスクリプトに含まれるハッシュチャレンジにより課されることができる。チャレンジは、データのハッシュ（データ自体ではない）、及び（アンロックスクリプトと一緒にノード１０４上で実行すると）対応するアンロックスクリプト内で提供されるデータのハッシュがロックスクリプト内で提供されるハッシュ値と等しいかどうかをテストするよう構成されるスクリプト片を含む。署名に対する要件は、例えば上述のCheckSigにより課される。実施形態では、第１条件が、Aliceの署名がTx_pのアンロックスクリプトに含まれることを要求しない.Bobにより署名される必要のあるTx_pの部分は、Tx_pのアンロックスクリプトの設定であってよく（例えば、SIGHASHフラグにより指定される）、又は固定されてよい。いずれの方法も、少なくともアンロックスクリプトを除く。従って、Tx_pのアンロックスクリプトは適応性がある。

【０１１２】

実施形態では、第２条件は、Tx_1、この場合にはターゲットトランザクションの第２バージョンTx_p’、をアンロックしようとするトランザクションのアンロックスクリプトが、自身のアンロックスクリプト内にBobの暗号署名及びAliceの暗号署名の両方を含むことを要求する。ここでも、これは例えばCheckSigにより課される。実施形態では、第１条件が、データペイロードがTx_p’のアンロックスクリプトに含まれることを要求しない。Alice及びBobにより署名される必要のあるTx_p’の部分は、Tx_p’のアンロックスクリプトの設定であってよく（例えば、SIGHASHフラグにより指定される）、又は固定されてよい。

【０１１３】

第０（つまりソース）トランザクションTx_0は、Alice、Bob、又は第三者により生成されてよい。それは、標準的に、AliceがTx_0のインプット内に定義された量を取得した先行するパーティの署名を要求する。それは、Alice、Bob、先行するパーティ、又は別の第三者によりネットワーク１０６へ送信されてよい。

【０１１４】

第１（つまり中間、条件付き）トランザクションTx_1も、Alice、Bob、又は第三者により生成されてよい。実施形態では、それはAliceの署名を要求するので、それはAliceにより生成されてよい。代替として、それは、Bob又は第三者によりテンプレートとして生成され、次に署名のためにAliceへ送信されてよく、例えばサイドチャネル３０１を介して送信される。Aliceは、次に、署名付きトランザクションをネットワーク１０６へ彼女自身で送信し、又はそれをBob若しくは第三者へ送信してそれらをネットワーク１０６へ転送し、又は単に彼女の署名をBob若しくは第三者へ送信して、署名付きTx_1に構成してネットワーク１０６へ転送できる。ここでも、Tx_1をネットワーク１０６へ送信する前の任意のオフチェーン交換は、サイドチャネル３０１を介して実行されてよい。

【０１１５】
第２の（つまり、ターゲット又は支払い）トランザクションTx_p/Tx_p’のいずれのバージョンも、Alice、Bob、又は第三者により生成されてよい。第１バージョンはBobの署名及び／又はデータを要求するので、Bobにより生成されてよい。代替として、それは、Alice又は第三者によりテンプレートとして生成され、次に、署名し及びデータを追加するためにBobへ送信されてよく、例えば、サイドチャネル３０１を介してBobへ送信される。Bobは、次に、署名付きトランザクションをネットワーク１０６へ彼自身で送信し、又はそれをAlice若しくは第三者へ送信してそれらをネットワーク１０６へ転送し、又は単に彼の署名をAlice若しくは第三者へ送信して、署名付きTx_pに構成してネットワークへ転送できる。実施形態では、第２バージョンは、Bob及びAliceの両方の署名を必要とする。従って、それは、Alice又はBobによりテンプレートとして生成され、彼らの署名を追加するためにテンプレートとして他方へ、例えばここでもサイドチャネル３０１を介して送信されてよい。代替として、それは、第三者によるテンプレートとして生成され、次にAliceへ送信され得る。ここで、Aliceは、彼女の署名を追加し、Bobの署名を追加するためにBobへ転送得る。Bobは、次に、署名付きトランザクションをネットワーク１０６へ転送するか、又はAlice若しくは第三者がネットワーク１０６へ転送するように、彼らへ返送する。或いは、Tx_p’は、第三者によりテンプレートとして生成され、次にBobへ送信され得る。ここで、Bobは、彼の署名を追加し、Aliceの署名を追加するためにAliceへ転送する。Aliceは、次に、署名付きトランザクションをネットワーク１０６へ転送するか、又はBob若しくは第三者がネットワーク１０６へ転送するように、彼らへ返送する。更なる変形では、Alice及び／又はBobは、受信したトランザクションテンプレートに署名し、彼らの署名を他のパーティのうちの１つへ返し、該パーティがTx_p’へと構成して、ネットワーク１０６へ転送する。ここでも、Tx_p及び／又はTx_p’をネットワーク１０６へ送信する前の任意のオフチェーン交換は、サイドチャネル３０１を介して実行されてよい。

【０１１６】
トランザクションの異なる要素が生成され構成され得る種々の位置があり、それが直接に又は間接的にＰ２Ｐネットワーク１０６の最終的な宛先へと送信される種々の方法があることが理解される。開示の技術の実装の範囲は、これらのいずれに関しても限定されない。

【０１１７】
「Aliceにより」、「Bobにより」、及び「第三者により」のような語句は、本願明細書では、それぞれ「Aliceのコンピュータ機器１０２aにより」、「Bobのコンピュータ機器１０２bにより」、及び「第三者のコンピュータ機器１０２により」の短縮表現として使用されることがある。また、所与のパーティの機器は、該パーティにより使用される１つ以上のユーザ装置、又は該パーティにより利用されるクラウドリソースのような幾つかのサーバリソース、又はそれらの任意の組合せを含み得ることに留意する。それは、必ずしも動作が単一のユーザ装置上で実行されることに限定しない。

【０１１８】
ターゲットトランザクションTx_pのアンロックスクリプトは適応性があるので、実施形態では、ターゲットトランザクションの第２バージョンTx_p’は第１バージョンTx_pを適応することにより、つまりTx_pの既存のデータ構造を取り入れ、及びそれを変更して第２バージョンTx_p’を形成することにより、この場合にはロックスクリプトを適応することにより、生成されてよい。これは、スクリプトレベルの適応性の例である。等価な変形ではしかしながら、Tx_p’は、アンロックスクリプトが異なることを除き同じ構造を有するターゲットトランザクションの新しいバージョンを生成することにより、生成されてよい。「更新する」は、本願明細書では、既存の構造を適応する又は新しい置換バージョンを生成する可能性を記述するために一般的な用語として使用されてよい。適応は、種々の実施形態に関連して、本願明細書において例として言及され得るが、これはターゲットトランザクションおｎ新しいバージョンをスクラッチから生成することにより置き換えることができることが理解される。いずれの方法も、新しいバージョンの適応又は生成は、Alice及び／又はBobにより、及び／又はAlice及び／又はBobの署名が与えられれば第三者により、実

行されてよい。

【０１１９】

幾つかの実施形態では、Tx_1のロックスクリプトは、第１及び第２条件の両方に対する代替として、第３アンロック条件を含んでよい。第３条件は、ロックタイムが終了すること、及びAliceの署名がターゲットトランザクションの第３バージョンTx_p’’のアンロックスクリプトに含まれることを要求してよい。これは、（例えば、Bobが処理に全く従事しないため又は時間制限内にそうすることに失敗したために）Bobが第１及び第２条件のいずれかに基づき請求しない場合に、AliceがTx_1のアウトプットからの彼女の支払いの返金を請求することを可能にする。ロックタイムは、絶対的時点、又は例えば秒で計測される経過すべき時間期間、又はマイニングされるブロック数として定義されてよい。

【０１２０】

例示的な使用例１－Bobのためのセキュリティ

上述のように、実施形態では、Tx_1で、第１条件（ｉ）は、Bobの署名及びデータペイロードがTx_pのアンロックスクリプトに含まれることを要求するが、Aliceの署名を要求しない。第２条件（ｉｉ）は、Alice及びBobの両方の署名を要求するが、データペイロードがTx_p’のアンロックスクリプトに含まれることを要求しない。

【０１２１】

つまり、Aliceが、彼女に何らかのサービスを提供する、例えば彼女のために何らかのDIYを行う、何らかの商品を提供する、何らかの相談サービスを提供する、等のためにBobに支払いたいとする。Aliceは、アウトプット（上述の例を参照するとTx_1のアウトプット０）内にサービスに対する支払いを含む第１（中間）トランザクションTx_1を生成する。彼女はこれをサイドチャネル３０１を介してBobへ送信する。代替として第１トランザクションは、Bob、又は第三者により生成され得る。それは、この段階で、Alice、Bob、又は第三者により、ブロックチェーン１５０に記録されるためにネットワーク１０６を介して伝播されるよう、送信され得る。或いは、それは、それら３つのパーティのうちのいずれかにより、後に、第２のターゲットトランザクションTx_p/Tx_p’と同時に、又はターゲットトランザクションの後に、ネットワーク１０６へ送信され得る。

【０１２２】

Aliceは、サイドチャネル３０１を介してBobへ、ターゲットトランザクションの第１バージョンTx_pも、Bobのためのテンプレートとして署名し及びデータペイロードを追加するために送信する（又はペイロードはAliceにより含まれ得る）。代替として、ターゲットトランザクションの第１バージョンは、Bobにより、又は第三者によりBobが署名し彼のデータペイロードを追加するためのテンプレートとして生成され得る（又は第三者がペイロードを含め得る）。Bobは、ターゲットトランザクションの第１バージョンTx_pのコピーを、少なくとも第２バージョンTx_p’が取得されるまで、保持する。或いは、代替として、第１バージョンTx_pは、Bobの署名及びデータが与えられれば、Bobの代わりに第三者により保持され得る。

【０１２３】

ターゲットトランザクションTxpは、最初に、データペイロードを含み、従って、Aliceの署名を必要としないが、データペイロードがアンロックスクリプトに含まれている場合にのみ、Bobにより（又はBobを代表して）一方的に償還可能である。これは、マイニングされるのにより費用がかかり、及び／又はBobのプライベートな又は独自のデータを危うくする可能性がある。従って、Bobは、Aliceを幸せに保ち、彼女に、彼女の署名を含むターゲットトランザクションの第２の、更新バージョンTx_p’を提供すること（又はBob又は第三者がターゲットトランザクションTx_p’へと構成する彼女の署名を送信する）を望む。これは、ターゲットトランザクションTx_p’にデータペイロードを含む必要を伴わずに、BobがTx_1のアウトプットを償還することを可能にする。しかしながら、Bobがサービスを提供するが、Aliceが合意を破った、又はサービスの満足のいく提供に論争がある場合、Bobは、データペイロードがターゲットトランザクションTx_pに含まれることを要求するあまり好ましくない第１条件に基づき、Tx_1のアウトプットを償還するというフォールバ

ックを依然として有する。

【０１２４】

BobがAliceのためにサービスを達成すると、Aliceが誠実でありサービスに満足するならば、彼女は彼女の署名を提供する。ターゲットトランザクションの第２バージョンTx_p’は、Alice及びBobの両方の署名を要求する。Bobは、Aliceが彼女の署名により署名することにより（及び依然として存在する場合にはデータを除去することにより）適応するために、データペイロードと共に又はそれを有しないで第１バージョンTx_pをAliceへサイドチャネル３０１を介して送信してよい。或いは、Bobは、Aliceが第２バージョンTx_p’に構成するために、単に彼の署名をAliceへサイドチャネル３０１を介して送信してよい。Aliceは、次に、Ｐ２Ｐネットワーク１０６を通じて伝播されブロックチェーン１５０に記録されるように、このバージョンを送信してよい（時に、ネットワーク１０６へトランザクションを「ブロードキャストする」又は「発行する」として表される）。代替として、Aliceは、ターゲットトランザクションの完全な第２バージョンTx_p’を、サイドチャネル３０１を介してBobに返して、Bobがネットワーク１０６へブロードキャストするように、又はそれを第三者へサイドチャネルを介して送信して第三者がブロードキャストするようにしてよい。別の例として、Aliceは、第１又は第２バージョンに基づき彼女の署名を生成し（それらの間の唯一の差分は、適応可能な部分にある）、単に彼女の署名をBobへサイドチャネル３０１を介して送信する。Bobは、彼の署名と共にAliceの署名を、ターゲットトランザクションの完全な第２バージョンTx_p’へと構成し、ネットワーク１０６へブロードキャストするか、又は第三者へサイドチャネルを介して送信して第三者がブロードキャストする。或いは別の代替では、Alice及びBobの両者は、彼らの署名を第三者へサイドチャネルを介して送信し、第三者がターゲットトランザクションの完全な第２バージョンTx_p’へと構成し、ネットワーク１０６へブロードキャストする。

【０１２５】

第１トランザクションTx_1及び実際にはソーストランザクションも、ブロックチェーン１５０に記録するために、ネットワーク１０６へブロードキャストされる必要がある。これは、それらが何らかの段階で最終的に検証される限り、任意のパーティにより任意の時点で行われ得る。

【０１２６】

第１条件がAliceの署名を要求しないという事実は、Aliceが彼女の署名により彼女の認可を提供しない場合でも、Bobが、Tx_1のアウトプットの中で定義された量を、ターゲットトランザクションの第１バージョンTx_pを用いて第１条件に基づき自動的に償還できることを意味する。しかしながら、データペイロードを含むという要件は煩わしい。マイナー１０４Ｍは、マイニングのためにトランザクションを受け入れるためにマイニング手数料を要求する。手数料が十分ではない場合、トランザクションが有効であっても（有効性及び受け入れ可能性は、別個の概念である）、彼らはブロック１５１へとマイニングするためにトランザクションを受け入れない。代替又は追加で、対象となるデータは、Bobにとって秘密、機密、又は独自であってよい。その結果、データをブロックチェーン１５０に発行することは、Bobに別の形式のペナルティを提示し得る。従って、Bobは、Aliceの署名を取得しようとするために、及びターゲットトランザクションの第２バージョンTx_p’を用いて好ましい第２条件に基づきTx_1を償還するために、良好なサービスを提供することを動機付けられる。しかしながら、Aliceが違反した場合、Bobは、ターゲットトランザクションの第１バージョンTx_pを用いて、あまり好ましくない第１条件に基づき、依然としてTx_1を償還できる。従って、第１バージョンTx_pは、Bobにとって一種の抵当又はデポジットとして機能する。

【０１２７】

Tx_1がAliceにより形成された場合でも、Tx_1のロックスクリプト内の第１条件の中の要件は、データペイロード自体がTx_1のロックスクリプトに含まれること又はAliceに知られることを要求しないことに留意する。むしろ、それは、（ノード１０４においてハッシングされるとアンロックスクリプト内のハッシュ値と一致するデータを提供するために

、Tx_pのアンロックスクリプトをチャレンジするスクリプトと一緒に）データペイロードのハッシュがTx_1のロックスクリプトに含まれることを要求するだけである。従って、Alice又は第三者がTx_1を形成する場合でも、Bobは、彼らに彼のデータのハッシュを与えればよく、データ自体を与える必要がない。彼がデータを発行しなければならないのは、彼がターゲットトランザクションの第１バージョンTx_pをチェーンに発行した場合のみである。

【０１２８】

例示的な使用例２－ストリーミング

図７を参照すると、例えばAliceはBobからの何らかのデータをストリーミングするために支払いたいと望む。データは、BobからAliceへ「チャンク毎に」、つまり部分D_0,D_1,D_2,等のシーケンスで、転送される。これらは、例えば、AliceがBobからストリーミングしているメディアコンテンツのアイテムの部分であってよく、例えば映画のようなビデオトラック及び／又は音楽のようなオーディオトラックを含む。ビデオは、任意の時間と共に変化する画像又はグラフィック、例えば映画、TV番組、スライドショー、又は他のそのようなシーケンス若しくは静止画像、アニメーションベクトルグラフィック、及び／又はゲームコンテンツを含んでよい。オーディオは、サンプリングされたオーディオ及び／又は合成されたオーディオを含み、会話、音楽、ノイズ、及び／又は効果、等を含み得る。別の例では、以下の技術は、「彼女が支払う限り（pay as she goes）」Aliceにサービス、例えば、ガス、電気、又は水道のような生活必需サービスの提供、又は車両、不動産、又は他の物理的オブジェクトのレンタル、を可能にするために使用され得る。サービスに対する支払いの場合には、データ部分が所望のコンテンツ自体の部分である代わりに、各データ部分D_0,D_1,D_2等は、サービスのユニットをアンロックするために必要な異なるそれぞれの鍵を含む。例えば、Aliceのガス、電気、又は水道供給は、彼女のコンピュータ機器１０２aに接続されるスマートメータにより支配される。それぞれの受信した鍵により、彼女は、これを彼女のコンピュータ機器１０２aから彼女のメータへと供給する。これは、それぞれの鍵を検証することに応答して、生活必需サービスの別のユニットをアンロックする。

【０１２９】

Bobの支払いがそれまでに受信されたデータ部分の数に比例するように、データの部分をストリーミングすることが望ましいことがある。これを行うために、各データ部分D_0,D_1,D_2…がBobから受信されることに応答して、Aliceは、それぞれの署名付きトランザクションTx_1,Tx_2,Tx_3…をBobへ、サイドチャネル３０１を介して返すことができる。これは、Bobがデータの送信を停止した場合、Aliceは単に支払いの送信を停止できること、及びAliceが支払いの送信を停止した場合、Bobは単にデータの送信を停止でき、Aliceが支払っていないデータDの１つより多くの部分を提供しないことを意味する。

【０１３０】

しかしながら、ストリーミングされているそれぞれの個別のデータ部分D_0,D_1,D_2等について個別のトランザクションをネットワーク１０６にブロードキャストしブロックチェーン１５０に記録することはネットワーク輻輳を増大しブロックチェーン１５０を膨大にし得るので、そうする必要がない方法でこれを行うことも望ましい。

【０１３１】

これを解決するために、AliceがBobからそれぞれ受信する各データ部分D_0,D_1,D_2…に応答して、AliceがBobへ返送する各トランザクションTx_1,Tx_2,Tx_3…は、同じソーストランザクションTx_0の同じアウトプット（例えば、同じUTXO）を指す第１トランザクションの異なるインスタンスである。第１トランザクションの量はその都度増大するので、Bobは、特定の定義されたシーケンスの終わりにある最後のもの、例えばオーディオまたはビデオトラックの終わり（例えば、映画の終わり）、又はサービスの指定された期間（例えば、１時間、１日、１週間、又は１月に１回）のアウトプットを請求するだけである。これは、以下に更に図７を参照して更に詳細に説明される。

【０１３２】

第１に、BobがAliceからの支払いを得たままデータを送信しないことにより騙すことができないように、第２に、Aliceがデータを受信してBobに支払わないことにより騙すことができないように、部分をストリーミングすることも望ましい。

【０１３３】

実施形態では、第１トランザクションの各インスタンスは、そのインプットによりポイントされるより多くの合計デジタルアセット量を有する複数のアウトプットを有する。これは、トランザクションが、誰かが、実際にはBobが彼自身の別のインプットを追加して差分を補うまで、有効ではないことを意味する（インプットレベルの適応性の例）。これは、Aliceがシーケンスの中で前のトランザクションを発行するのを止め、これはBobが後のトランザクションを発行するのを阻止する。これは、従って、映画全体等に対してデポジットとして機能する初期資金（funding）トランザクションを有しないでストリーミングを可能にする。これは、以下に図８を参照して更に詳細に議論される。

【０１３４】

ストリーミング方法を実施するために、Alice及びBobは、彼らの間にオフチェーンサイドチャネル３０１を確立する。つまり、このチャネルを介して送信されるトランザクションは、ブロックチェーン１５０に記録するために（未だ）Ｐ２Ｐネットワークに発行されていない。これは、本願明細書で「微細支払いチャネル」とも呼ばれる支払いチャネルの変更された形式として使用される。更に、Bobは、Aliceにシーケンス内のデータ部分D_0,D_1,D_2…のハッシュセットを利用可能にする。例えば、Bobは、Aliceにハッシュセットを支払いチャネル３０１を介して送信してよく、又はインターネット１０１等のサーバからアクセスするためにそれを公に利用可能にしてよい。ハッシュセットは、Alice自身がデータ自体を予め知る必要がなく、Aliceがデータのハッシュチャレンジを生成することを可能にするハッシュのセットを含む。例えば、ハッシュセットは、マークル（Merkle）ツリーとしても知られるハッシュツリーを含んでよい（用語「マークルツリー」は、本願明細書で、その最も広義の意味で使用され、任意のハッシュツリーを意味し、例えば必ずしもバイナリブランチに限定されないことに留意する）。代替として、ハッシュセットはハッシュチェーン又はハッシュリストを含み得る。

【０１３５】

Bobは、Aliceに第１データ部分D_0を支払いチャネル３０１を介して送信することにより開始する。この第１部分は無料で又は信頼して送信される。Aliceが支払わない場合、Bobは第１部分のデータ価値より多くを失わない。Aliceが継続を望むとすると、D_0を受信することに応答して、彼女は、Bobに第１トランザクションの第１インスタンスTx_1を支払いチャネル３０１を介して送信する。これに応答して、Bobは、Aliceにシーケンスの中で次のデータ部分を送信し、次に、これに応答して、AliceはBobに第１トランザクションの第２インスタンスTx_2を送信し、次に、BobはAliceにD_2を送信し、AliceはBobにTx_2を送信し、以下同様であり、全ては支払いチャネル３０１を介する。第１トランザクションの各インスタンスTx_1,Tx_2,Tx_3…は、Bobへの増大する、例えばそれまでに受信したデータ部分Dの数と共に線形に増大する支払いを指定する。しかしながら、第１トランザクションの各インスタンスTx_1,Tx_2,Tx_3…は、Aliceの同じUTXOを指す。従って、Bobは、第２の、ターゲットトランザクションの有効なインスタンスTx_p/Tx_p’を構成し、それらのうちの１つからの支払いを請求するだけでよい（同じUTXOを２回償還しようとする試みは、無効であるとしてネットワーク１０６により拒否されるだろう）。全てが上手く行くとすると、Bobは、従って、シーケンスの中の第１トランザクションの最後のインスタンスからの支払いを請求する、ターゲットトランザクションのバージョンを生成する。

【０１３６】

実施形態では、第１トランザクションの各インスタンスTx_1,Tx_2,Tx_3…又は最後のインスタンスTx_nは、（例えば図５を参照して）上述したように、該トランザクションのアウトプットの中で、Aliceからの支払いを償還するための複数の代替条件を定義する。この場合、シーケンスの中の最後のデータ部分D_nのAliceの肯定応答と共に、彼女は、ターゲットトランザクションの第２バージョンTx_p’も提供するか、又は少なくとも彼女の署名を

提供して、BobがTx_p’を構成できるようにする。これは、Bobが、Bobにペナルティを課す第１条件ではなく、好ましい第２条件に基づき、完全なシーケンス（例えば、映画全体）に対する支払いを請求することを可能にする。Bobが部分Dのストリーミングを停止し、Aliceが不満である場合、彼女は、必要に応じて第２条件を満たすために彼女の署名を提供しなくてよい。従って、Bobは、第１のあまり好ましくない条件に基づき支払いを請求できるだけである。他方で、Aliceが、不満ではないが、途中で更なる部分を要求することを止めた場合（例えば、彼女が単に映画を観るのを止めることを選んだ）、第１トランザクションのインスタンスの各々Tx_1,Tx_2,Tx_3…がそれまでに複数の代替条件を含んでいるとすると、Aliceは、Tx_p’又は彼女の署名を提供してよく、Bobが、好ましい第２条件に基づき、それまでのシーケンスに対する支払いを請求できるようにする。

【０１３７】

第１トランザクションのインスタンスTx_i、i=１,２,３…は、異なるメッセージに対して共通のUTXOを使用するが、複数の署名を使用する。従って、この文脈におけるインスタンスは、（以下に議論する）トランザクションのインスタンスとしての、Aliceからのデータに対するそれぞれの「要求」を表す。これは、値及び要求されたデータを変えることが署名済みメッセージを変えるからである。

【０１３８】

第２トランザクションのバージョンTx_p/Tx_p’は、同一のメッセージに対して、共通のUTXOを使用するが、複数の署名を使用する。従って、この文脈では、バージョンは、「適応されていない」及び「適応された」形式のトランザクションを、トランザクションのそれぞれのバージョンとして表す。これは、スクリプトレベルの適応が署名済みメッセージを変更しないからである。

【０１３９】

注：どのパーティが第１トランザクションTx_1…を生成し及び／又はブロードキャストするかに関して先に議論した変形、及びターゲットトランザクションの第１及び第２バージョンTx_p/Tx_p’のいずれかもここで適用されてよい。例えば、第三者は、Alice又はBobの代わりにこれらのうちの一部又は全部を生成し及び／又はブロードキャストし得る。或いは、Bobが、ブロードキャストするためにTx_p/Tx_p’をネットワークへ彼自身で送信するか又はAliceへ送信するか、彼の署名をAliceへ送信してAliceがターゲットトランザクションTx_p/Tx_p’を構成するようにしてよい、等である。簡潔さのために、これらの種々のオプションは、ここで再び完全に繰り返されない。

【０１４０】

例として、映画産業を考える。スクリプトサイズ限度は、執筆時点で１０キロバイトである。従って、映画毎に、多数の８キロバイト部分に分割できる。他の制約がある場合、部分のサイズは更に小さくてよく、或いは、スクリプトサイズの限度が増大される場合、更に大きくてよい。部分が定義されると、次に、マークルツリーが構成でき、ルートハッシュが、映画タイトルと一緒に公にリストされる。

【０１４１】

簡単のために、議論は、マイニング手数料が暗示的に適用されるとする。明示的インプットが明示的アウトプット及び暗示的トランザクション手数料をカバーしない場合、別の暗示的インプットが存在得るとする。

【０１４２】

Aliceは、Bobから映画を購入しようとしている。映画は、n+１個の小さなデータパックD_0,...,D_n、及びルートハッシュH_{root}を有するそれらのマークルツリーTにより定義される。方法は、AliceからBobへの一連のトランザクションTX_1,TX_2,...,TX_nを構成する。各トランザクションTX_iは、D_iに対する要求、及びD_{i-1}の受信の肯定応答に対する。理想的には、支払いチャネル３０１が正しく閉じられるとき、AliceからBobへの支払いを達成するために、２つのトランザクションTX'_n及びTX'_pのみが発行される。このシナリオは、図７に示される。図７は、使用例２におけるAliceとBobとの間の支払いチャネル３０１のシーケンス図である。BobからAliceへの１つの初期メッセージがあり、次に各データパ

ケットについてn個のメッセージペアが続き、チャネルを閉じるための２つの最終メッセージがある。

【０１４３】

第１ラウンド－Aliceの番：

最初に、Bobは、Aliceに、D_0、及び期待されるデータパックを含む完全なマークルツリーを送信する。Aliceは、ルートハッシュが実際に彼女の選択した映画タイトルに属することをチェックし、D_0のマークルパスを検証する。Aliceが受信したデータに満足すると、彼女は、彼女がTX１を受信したことの肯定応答をするために、及びD_1を要求したいと思い、TX_1を構成し得る。このトランザクションは以下の形式をとり得る：

【数２】

TX_1

Locktime: 0

Input 0:

- Alice の未使用アウトポイント(outpoint) $(TxID_0, vout = 0)$
- Alice の署名、及び SIGHASH_ALL | ANYONECANPAY

Output 0:

- ロック条件:

  (i) Bob がD_1及び彼の署名を提供する場合、彼はアウトプットを請求できる。

  (ii)その他の場合、Alice 及び Bob の両者が彼らの署名を提供するならば、Bob はアウトプットを請求できる。

  (iii) その他の場合、(このトランザクションがマイニングされてから)720 ブロックの後に、Alice はアウトプットを請求できる。

- 値: 500 ユニットのデジタルアセット

Output 1:

- Alice のお釣り

Output 2:

- Output 1 におけるものと同じ額を Bob に支払う

【０１４４】

このインスタンスの例は図９に示される。この単一のトランザクション設計は、３つの

意図される機能を有する。トランザクション内の幾つかのフィールドに追加の含意を割り当てることにより、データトレードシナリオにおいて必要な複数のメッセージを、たった１つのトランザクションテンプレートにより置き換えることが可能である。$Sig(P_A,Tx_1)$は、前のデータパックが受信され及び満足のいくものであることを肯定応答する署名である。OP_DUP OP_SHA２５６ 〈$H(D_1)$〉 OP_EQUALは、次のデータパックを求める要求である。５００ユニットが、次のデータパックのために支払われる。

【０１４５】

Tx_1の（１又は複数の）インプットは、少なくともインプット０を含む。これは、Aliceに対してロックされた前のトランザクションTx_0のUTXOへのポインタを含む。該UTXOは、Tx_1のアウトプット０より大きい（例えば２０００ユニット）額である（以下を参照）。Tx_1のインプット０は、インプットのアンロックスクリプトの中にAliceの署名、及び他のパーティがインプットを追加できるようにするフラグも（「ANYONECANPAY」）含む。

【０１４６】

Tx_1の（１又は複数の）アウトプットは、少なくともアウトプット０を含む。これは、Tx_1のインプット０より少ない、（最初の）少額の（例えば５００ユニットの）デジタルアセットを指定する。Tx_1のアウトプット０は、以下の条件のうちのいずれかによりこれをアンロック可能にするロックスクリプトも含む；

（ｉ）後続のトランザクションTx_pのインプット内のアンロックスクリプトが、D_1及びBobの署名を含む；

（ｉｉ）後続のトランザクションTx_p’のインプット内のアンロックスクリプトが、Aliceの署名及びBobの署名を含む；或いは、

（ｉｉｉ）タイムアウト限度が経過し、後続のトランザクションのインプット内のアンロックスクリプトがAliceの署名を含む。

【０１４７】

条件（ｉ）に関し、BobがAliceにハッシュツリーとも呼ばれるマークルツリーを送信しているので、Aliceは、どんなデータ部分が期待されるかを知っている。これは、彼女に、D_1のハッシュを決定させる。これは、彼女がハッシュチャレンジによりこの条件を含めるのに十分である（Tx_1のロックスクリプトは、D_1のハッシュと、ハッシングされるとTx_p,のインプットのアンロックスクリプト内で提示された値がロックスクリプト内の値と一致することをチェックする何らかのコードを足したものを含む）。この条件は、BobがAliceの署名を有しないで支払いを請求したい場合、彼がブロックチェーン１５０にD_1をアップロードしなければならないことを意味する。D_1は彼独自のデータであるので、更にD_1のサイズは高いマイニング手数料を生じるので、彼はそうすることを好まない。この同じ技術は、後続のデータ部分D_2,D_3等にも使用できる。

【０１４８】

条件（ｉｉ）は、代わりにBobがAliceに彼女の署名を与えさせる場合には、彼はデータをアップロードする必要なく、支払いを請求できる。しかしながら、彼は未だそうすることを望まないとする。

【０１４９】

条件（ｉｉｉ）は任意である。それは、Bobが特定の指定されたタイムアウト期間の後に何らかの理由で請求しない場合に（例えば、Bobが処理に関与しない）、Aliceに、Tx１のアウトプット０内の量の返還を請求する能力を与える。７２０ブロックの特定のタイムアウト値は単なる例であることが理解される。より一般的には、タイムアウト期間は、ブロック数、又は秒のような人間の時間で定義されてよく、任意の値に設定されてよい。絶対的な時間点で終了する、又は経過時間量として定義され得る。

【０１５０】

Tx_1も、任意的に、１つ以上の更なるアウトプットを含んでよい。実施形態では、これらは、アウトプット１及びアウトプット２を含む。アウトプット１は、インプット量に等しく、Alice（Aliceの変更）に対してロックしているデジタルアセットの額を定義するス

クリプトを含む。例えば、これは、２０００-５００ユニット=１５００ユニットである。
【０１５１】
アウトプット２はアウトプット１に等しく、Bob（「アウトプット１内のAliceのお釣り（change）と同じようにBobに支払う」）に対してロックしているデジタルアセットの額を定義するスクリプトを含む。この効果は、差分を構成するために誰か他の者が（実際にはBobしかいないだろう）彼自身の別のインプット１をTx_1に追加しない限り、合計出力（例えば５００+１５００+１５００ユニット=３５００ユニット）が、常に入力より大きいことである。
【０１５２】
アウトプット２は、AliceがBobの承認なしにトランザクションを公開することを防ぐために設計されたトリックである。支払人として、Aliceは、最初にTX_1をブロードキャストする動機がない。しかしながら、数ラウンドの後、AliceがBobにより多くを支払う他のトランザクションが存在するとき、Aliceは、Bobが彼の支払いを請求するために後のインスタンスを使用する前に、TX_1を用いてそれをネットワーク１０６へブロードキャストすることにより、それらを無効にし得る。アウトプット２を含むことにより、Bobがアウトプットとインプットとの間の不足額をカバーするために彼自身のインプット（インプット１）をTX_1に追加するまで、TX_1は、有効にならない。AliceがSIGHASHフラグ「ALL¦ANYONECANPAY」を使用するので、Bobは追加のインプットを追加できる。結果として、TX_1は、Bobによってのみブロードキャストされる可能性がある。Aliceは、Tx_1を有効にするために必要な追加インプットを追加したくない。何故なら、これは、彼女がシステムを騙さない場合には、彼女により多くの費用がかかるからである。
【０１５３】
Aliceのお釣りは、Aliceのインプット（インプット０）の値から、Bobの支払い（アウトプット０）の値を差し引いたものでると定義される。図８のグラフが示すように、Bobの保険金（アウトプット２）は、最後のデータ部分が送信される前は、合計アウトプット（破線）が常にインプットより大きいことを保証する。
【０１５４】
より一般的には、Tx_1の合計アウトプット値が合計インプット値より大きい、従って、Tx_1のアウトプット０を請求するためにBob自身のインプットを追加するようBobに要求し、及びAliceがTx_1をブロードキャストする動機をなくす状況を作り出すために、アウトプットの他の組合せが使用され得る。
【０１５５】
スクリプト言語でアウトプット０において３つの条件（ｉ）、（ｉｉ）、（ｉｉｉ）を実施する例として、例えば以下のようにハッシュパズル及び条件付きオペコードを使用できる。
【数３】

```
OP_DUP OP_HASH256 < hash of D1 > OP_EQUAL
OP_IF
      OP_DROP     OP_DUP     OP_SHA256     < hash of Bob's public key >
OP_EQUALVERIFY
    OP_CHECKSIGVERIFY
OP_ELSE
     2     < hash of Alice's public key >     < hash of Bob's public key >     2
    OP_CHECKMULTISIG
    OP_IF
                OP_VERIFY
    OP_ELSE
      < 720 blocks > OP_CHECKSEQUENCEVERIFY
                OP_DUP     OP_SHA256     < hash of Alice's public key >
                OP_EQUALVERIFY OP_CHECKSIGVERIFY
      OP_ENDIF
OP_ENDIF
```

【０１５６】

第１ラウンド－Bobの番：

Bobは、トランザクションTX_1を受信すると、単にAliceへD_1を送信する。Bobは、TX_1内の支払いを請求し得るので、Aliceからの支援を有しないで、以下を行うことにより、これを安全に行うことに留意する。先ず、Bobは、TX_1内のアウトプット２の値をカバーするためにアウトポイント（$TxID_B$,vout=０）を使用して、彼自身のインプットを追加することにより、TX_1'を生成する。次に、Bobは、支払いを請求するために別のトランザクションTX_pを生成する。

【数４】

TX_p

Locktime: 0

Input 0:

- TX_1' Output 0 からのアウトポイント
- アンロックデータ
  - D_1
  - Bob の署名

Output 0:

- Bob に支払う
- 値: 500 ユニット

【０１５７】
Bobは、次に、両方のトランザクションをネットワーク１０６へブロードキャストしてよい。しかしながら、Bobはトランザクション内でD_1を開示しなければならないので、Bobにとってこれは理想的な状況ではない。これは、チャネルの想起閉鎖であると考えられる。しかしながら、Aliceが正しい手順に従い支払いチャネルを閉じる場合（後述する）、Bobはこれを行う必要がない。
【０１５８】
第２ラウンド－Aliceの番：AliceがD_1を受信しコンテンツに満足すると、彼女は、次のデータパックのために以下のトランザクション内を構築する。このトランザクションは、D_1を受信したことの肯定応答とも考えられる。
【数５】
TX_2

Locktime: 0

Input 0:

- Alice の未使用アウトポイント(TX_1内のものと同じアウトポイントであるとする)
- Alice の署名、及び SIGHASH_ALL|ANYONECANPAY

Output 0:

- ロック条件:
  - Bob がD_2及び彼の署名を提供する場合、彼はアウトプットを請求できる。
  - その他の場合、Alice 及び Bob の両者が彼らの署名を提供するならば、Bob はアウトプットを請求できる
  - その他の場合、720 ブロックの後に、Alice はアウトプットを請求できる。
- 値: 1000 ユニット

Output 1:

- Alice のお釣り

Output 2:

- Bob に Output 1 内のものと同じ額を支払う。

【０１５９】

TX$_1$及びTX$_2$を比較すると、D$_1$がD$_2$に変更され、アウトプット０の値が５００ユニットのデジタルアセットから１０００ユニットへと増大されている。これらの２つの変更の結果として、他のアウトプットは異なる値を有する（Aliceが同じ未使用アウトポイントを使用しているとする）。更に、これらの変更はトランザクションの適応性のある部分には行われないので、AliceはTX$_2$のための新しい署名を生成しなければならない。

【０１６０】

第２ラウンド－Bobの番：

BobはTX$_2$を受信すると、単にAliceへD$_2$を送信する。

【０１６１】

Bobは、第１ラウンドと同じ方法でAliceの支援を有しないで支払いを請求できるので、前の同じように、これを安全に行う。Bobは、ここでも、TX$_2$内のアウトプット２をカバーするために、ここでも（TxID$_B$,vout=０）から彼自身のインプットを追加し、TX$_2$'内を生成する。Bobは、支払いを請求するために別のトランザクションTX$_p$も生成する。

【数６】

TX_p

Locktime: 0

Input 0:

- TX_2' Output 0 からのアウトポイント
- アンロックデータ
  - D_2
  - Bob の署名

Output 0:

- Bob に支払う
- 値: 1000 ユニット

【０１６２】

Bobは、次に、両方のトランザクションをネットワークへブロードキャストしてよい。

【０１６３】

AliceとBobが協力してチャネルを閉じる場合、Bobは、第１ラウンドで説明したようにこれを行うことを回避できる。

【０１６４】

最終ラウンド－Aliceの番：

数ラウンドの後に、Aliceは、最後のデータパックD$_n$を要求するためにTX$_n$を構築する。

【数７】

TX_n

Locktime: 0

Input 0:

- Alice の未使用アウトポイント(TX_1内のものと同じアウトポイントであるとする)
- Alice の署名、及び SIGHASH_ALL | ANYONECANPAY

Output 0:

- ロック条件:
  - Bob がD_n 及び彼の署名を提供する場合、彼はアウトプットを請求できる。
  - その他の場合、Alice 及び Bob の両者が彼らの署名を提供するならば、Bob はアウトプットを請求できる。
  - その他の場合、720 ブロックの後に Alice はアウトプットを請求できる。
- 値: $500n$ ユニット

Output 1:

- Alice のお釣り

Output 2:

- Output 1 内のものと同じ額を Bob に支払う。

【０１６５】
最終ラウンド－Bobの番：
Bobは、最終データパックD_nにより応答する。
【０１６６】
チャネルの閉鎖：支払いチャネルを閉じるために、AliceとBobとの間に幾つかの相互作用がある。Alice又はBobのいずれかは、チャネル３０１を閉じる彼らの意図を、他方へシグナリングできる。一般性を失わずに、BobからAliceへ送信される最後のデータパックがD_nであるとする。Bobは、D_nを要求するトランザクションTX_nを見付け、アウトプット２をカバーするために彼自身のインプットを追加して、TX_n'を生成する。Bobは、以下のようにTX_pを生成する。
【数８】

TX_p

Locktime: 0

Input 0:

- TX'_n Output 0 からのアウトポイント
- アンロックデータ
  - D_n
  - Bob の署名

Output 0:

- Bob に支払う。
- 値: $500n$ ユニット

【０１６７】
Bobは、両方のトランザクションTXn’及びTXpを、支払いチャネル３０１を介してAliceへ直接送信する。Aliceは、TXn’及びTXpのインプットが彼女の期待通り実際に関連するかをチェックする。Aliceは、TXpに署名し、Dnを彼女の署名で置き換えて、TXp'を生成する。
【数９】
TX_p'

Locktime: 0

Input 0:

- TX'_n Output 0 からのアウトポイント
- アンロックデータ
  - Alice の署名
  - Bob の署名

Output 0:

- Bob に支払う
- 値: $500n$ ユニット

【０１６８】
AliceはBobにTXp'を送信する。Bobは、TXn’及びTXp'をネットワーク１０６へブロー

ドキャストする。代替として、Aliceは、TX_n'及び／又はTx_p'をブロードキャストするか、又はAlice及びBobの代わりにブロードキャストするようそれらの一方又は両方を第三者へ送信し得る。Aliceは、いつでもチャネルを閉じることを選択できることに留意する。

【０１６９】

図７に、以下の２つの方法を示す：（Ａ）チャネルが、トランザクションのペアをブロードキャストすることによりBobにより一方的に閉じられる；及び（Ｂ）ペアを形成する２つのトランザクションが、チャネルの閉鎖のときに両方ともブロードキャストされ、チャネルがネットワーク１０６と通信することなく実質的に「開放された（opened）」オフチェーンであることを示す。

【０１７０】

シーケンスを再生するために、Tx_1に応答して、Bobは、D_2をAliceに送信する。Aliceが Bobに肯定応答するためにTx_2を送信し、次に、BobはD_3等を送信する。Tx_2は、Tx_1と同じであるが、D_1がD_2で置き換えられ、アウトプット０の量が増大されている。Tx_3では、D_2はD_3で置き換えられ、ここでもアウトプット０の量が増大される。実施形態では、アウトプット０の量は、iと共に、つまり各チャンク及び肯定応答で送信されるTxと共に、線形に増大する。代替として、例えば、シーケンスを完了する更なる動機を与えるようシーケンスの終わりに向けてより高い重みを与えるために、別の増大する関係が使用されることは排除されない。

【０１７１】

Bobは、基準（ｉｉ）に基づき、Tx_1…Tx_iのうちのいずれか１つを一方的に請求できる。これを行うために、Bobは、それを適応してTx_i'を生成する。適応は、Bobのデジタルアセットの一部のインプットを追加して、差分を構成し、次に、Tx_i.を使用するために自身のインプットの中にD_iを含む別のトランザクションTx_pを生成することを含む。Tx_pは、Bobに対して条件付きでロックされている。Bobは、彼のインプットを追加し、先のトランザクションTx_1又はTx_2、等のうちの１つを使用し得るが、そうする価値はない。彼は、映画を送信し続け、最後には全額を得ることを望む。また、Bobは、彼の映画のチャンクのうちの１つをブロックチェーンに発行しなければならないので、基準（ｉｉ）に依存しないことを望む。

【０１７２】

各Tx_1,Tx_2,Tx_3…のインプットはTx_0の同じUTXOを指定することに留意する。従って、それらのうちのいずれか１つがネットワークへブロードキャストされ、任意の所与のノード１０４で検証される場合、それらのうちの任意の他のものは、該ノードにおいて有効であるとは考えない（有効の条件は、Txが別のトランザクションにより既に有効に使用されたUTXOを使用しようとしないことである）。異なるノード１０４は、最初に異なるインスタンスを受信する可能性があり、従って、１つのインスタンスがマイニングされる前に、どのインスタンスが「有効」であるかについて矛盾するビューを有することがあり、その時点で、全部のノード１０４は、マイニングされたインスタンスのみが有効なインスタンスであることに合意する。ノード１０４が１つのインスタンスを有効であるとして受け入れ、次に第２のインスタンスがブロックチェーン１５０に記録されていることを発見した場合、該ノード１０４は、これを受け入れ（なければならず）、最初に受け入れた未だマイニングされていないインスタンスを破棄する（つまり、無効であるとして扱う）。

【０１７３】

Bobが早い段階で現金に換え、映画の送信を停止した場合、Aliceは、彼女が受信したより１つ多くのチャンクに支払うだけであり、５００しか失わない。Aliceは、任意の時点で保釈金を払うことができるが、彼女がそうする場合、Bobは、Aliceが支払わなかった映画の１つより多くのチャンク（例えば、５００ユニットの価値）を彼女に送信しない。

【０１７４】

少額から開始して、映画の終わりに向かってその都度、額が増大し、全部のトランザクションがTx_0内の同じUTXOを使用しようとするので、いずれか１つにおける換金は任意の他のものを無効にする。また、実施形態では、アウトプットの合計は、Bobが彼自身の

インプットを追加するまで、必ずしもインプットより大きくない。これは、インプットレベルの適応性の例である。

【０１７５】

Bob及びAliceの両者が映画の終わりまで待つ場合、Bobは、Aliceが署名するように、Tx_n'をAliceへ送信する。その結果、p_2のハッシュが彼女の署名により置き換えられる。これは、Bobが、データの任意のチャンクＤを発行することなく、完全な支払いを請求することを可能にする。これは、スクリプトレベルの適応性の例である。

【０１７６】

ブロックチェーン上のデータ輻輳を回避するために、処理は、何らかのデータパッケージ又はデータ受信者の署名を使用してアンロック可能なロックスクリプトを使用する。トランザクションの適応性を使用することにより、データ受信者は、アンロックスクリプト内のデータを彼女又は彼の署名で置き換えることができる。この動作は、データが受信されたことに肯定応答する又は支払いチャネルの閉鎖を確認するだけではなく、トランザクションからデータを削除して空間を節約する。

【０１７７】

Bobには、トランザクションの値の増分的増加を考えると、彼がAliceから受信する最後のトランザクション以外のトランザクションを発行する動機がない。Aliceが途中でチャネルを離れた場合、Bobは、単に、彼がAliceから受信した最後のトランザクションを、支払いを請求するトランザクションと一緒に発行する。彼がAliceの適応されたトランザクションを受信しなかった場合、彼は、支払いを請求するために関連するデータパックを開示しなければならない。実施形態では、データ信頼性に対する強い要求がある場合、BobはAliceへ送信するデータを暗号化し、トランザクション内で復号鍵を開示できる（後述する）。

【０１７８】

Aliceにとっては、しかしながら、彼女が十分なデータパックを受信すると、第１トランザクションを発行する動機がある。最初のトランザクション及び最後のトランザクションが両方とも有効であるとき、彼女が最後に通信されたトランザクションを無効にすることに成功するかどうかは確かではない。このシナリオを完全に回避するために、実施形態は、誰かがアウトプットとインプットとの間の差分をカバーしない限り、トランザクション自体を無効にする追加のアウトプットを含む。Aliceがトランザクションを有効にするために、彼女は、追加インプットを提供し、それはトランザクションをブロードキャストするという彼女の目的を覆す。

【０１７９】

Bobがオフラインになる場合、Aliceは、映画を鑑賞し続けることができない。しかしながら、彼女は、彼女が観たよりも多くを支払わない。彼女は、Bobが戻ってくるのを待つか、又は単に別のサービスプロバイダへと移動し、彼女が停止したところから開始する。

【０１８０】

このために必要な資金供給トランザクションは、支払いチャネルを形成しないことに留意する。更に、Aliceは、任意のポイントでストリーミングサービスを再開するために再接続できるという柔軟性がある。つまり、支払いチャネルを確立するためのオーバヘッドがない。

【０１８１】

実施形態は、支払いチャネル内の全てのリスクを解決する。依然として、Aliceは、支払いチャネルの外部で彼女のUTXOを二重支払いすることが可能な場合がある。実施形態は、これを防ぐために、３つのオプションのうちの任意の１つ以上を防ぐことができる。AliceがUTXOを二重支払いしようとするとき、Aliceに銀行預金のためのシークレット鍵を強制的に開示させるための技術が採用されるべきである。この場合、Bobは、全部の預金を請求することができる。第２のオプションも、Aliceの肯定応答を法的に拘束する。つまり、Bobの支払い請求トランザクションに対するAliceの署名は、彼女のアイデンティティの拘束力のある証明として考えられる。Aliceのいかなる不正行為も、法執行の対象になる。

第３のオプションは、Bobが、時間に渡り、例えば５分毎に、支払いチャネルを終了し再開することである。頻度は、リスクに対するBob自身の評価に従い、Bobにより割り当てることができる。資金供給トランザクションが必要ないので、支払いチャネルを再開することによるオーバヘッドがないことに留意する。

【０１８２】

データ暗号化：データ信頼性は、データが公衆ネットワークを介して交換されるときに、要件である場合が多い。前の章では、データ受信側が受信されるものが何かを正確に知っていると仮定した。しかしながら、データが暗号化されるとき、なんら通信をしないで、どんな暗号文であるか又はどんなハッシュ値が予想されるかは予め知ることが困難である。これは、ロックスクリプト内のハッシュパズルを構成する要件を引き起こす。これを軽減するために、実施形態では、データの売り手は、暗号文のハッシュ値を、送信する前にデータの受信側へ通信できる。データの受信側は、与えられたハッシュ値を用いて支払いトランザクションを構成する。暗号データを受信すると、データ受信側は、データを復号し、データが期待されているかどうかを検証できる。期待されたものである場合、全てが良好である。そうでない場合、最悪の場合は、受信側が金銭を失う。しかしながら、受信側が失う額は、データパケット当たりの価格で区切られる。映画の場合、それはおそらく約５００ユニットであり、例えば映画での合計は５ドルになる。経済的価値が小さく、評判への影響が遙かに大きいことを考えると、データの売り手が不正行為をする動機付けがない。

【０１８３】

幾つかの実施形態は、データの売り手とそれぞれのデータの買い手との間の対称暗号からの共有シークレット鍵を確立するメカニズムを実装してよい。従って、送信中の全部のデータは暗号化できる。

【０１８４】

例示的な使用例３－世論調査及び投票

別の例示的な使用例では、第１トランザクションTx_1の異なる代替条件は、例えば図５に示され、投票を記録する手段としてブロックチェーン１５０を使用するために、異なる投票の選択肢を表すために使用されてよい。Tx_p’がブロック１５１へとマイニングされる前に、Tx_p内のAliceにより表された選択肢は、投票意図を示す投票として考えられる。以下の例では、第１トランザクションは、Tx_{Slip}と表され、第２の（ターゲット）トランザクションの第１バージョンはTx_{Poll}と表され、ターゲットトランザクションの第２バージョンはTx_{Vote}と表される。

【０１８５】

以下の例示的なシナリオを考える。選挙が差し迫っている。行政体（「Bob」１０３b）は、ブロックチェーンに基づく投票システムを用いて、参加する有権者に報酬を与えることができる世論調査（polling）及び投票（vote）自体に参加を奨励したい。説明を簡単にするために、これは「労働党」と「保守党」の２大政党制であるとする。行政体P_{Gov}は、（ａ）有権者の登録、（ｂ）投票票の発行、及び（ｃ）世論調査及び投票の計数、に責任がある。行政体は、第２パーティ１０３bであり、このシナリオでは「Bob」とも呼ばれる。選挙民は、N人の有権者を含む。各投票者（「Alice」１０３a）は、登録するとき、投票者にのみ知られる秘密の「投票トークン（Vote Token）」T_Vを選択する。Bobの行政体は、各登録した投票者のハッシュ値$H(T_V)$を知っている。

【０１８６】

以下の定義は、世論調査及び投票システムのために利用されてよい。

・登録（Registration）:=投票者は、有権者として登録するために何らかのオフ又はオンブロック処理を使用する。投票者は、非公開でT_Vを選択し、Bobの行政体に$H(T_V)$を与える。

・投票票（Vote slip）（Tx_{Slip}）:=投票者が世論調査及び／又は投票に参加する場合に、投票者に支払うロックスクリプトを含むトランザクション。

・世論調査（Poll）（Tx_{Poll}）:=投票票アウトプットをアンロックするためにアンロック

条件（ｉ）又は（ｉｉ）を使用する署名付きトランザクション。ここで、（ｉ）及び（ｉｉ）は、２つのそれぞれのオプション、例えば一般投票又は政党（以下の例を参照）についての投票選択肢を表す。
・投票（Vote）（Tx_{Vote}）:=投票票アウトプットをアンロックするためにアンロック条件（ｉｉｉ）又は（ｉｖ）を使用する署名付きトランザクション。ここで、（ｉｉｉ）及び（ｉｖ）は、２つのそれぞれのオプション（ここでも以下の例示的な条件を参照）についての投票選択肢を表す。
【０１８７】
全ての投票者は、また、彼ら自身の公開鍵P_Vを有し、彼らの選択した政党に投票（poll又はvote）するために、それぞれ、彼らの選択肢を反映する公開鍵を用いて署名しなければならない。
【０１８８】
説明のための２大政党制の例では、２つのみの政党のうちの一方が選択されてよく、投票者が彼らの選択を表すために２つの可能な公開鍵があり、以下であってよい：
【数１０】

$$P_{V,L} = P_V + SHA256("Labour") \cdot G ,$$

$$P_{V,C} = P_V + SHA256("Conservative") \cdot G ,$$

ここで、". . . "は、「スカラーによるEC点乗算」のための演算子として定義される。
【０１８９】
アンロック条件に関して、ロックスクリプトは、４つの異なるアンロック条件のうちのいずれか１つを満たすことによりアンロック可能なように、構成される。条件（ｉ）及び（ｉｉｉ）は、両方とも、「労働党」に関連し、それぞれ世論調査及び投票を表す。条件（ｉｉ）及び（ｉｖ）は、両方とも、「保守党」に関連し、それぞれ世論調査及び投票を表す。条件は、以下のように完全に記述される。
【数１１】

(I) $<SigP_{V,L}>$ $<P_{V,L}>$ <”Labour”>

(II) $<SigP_{V,C}>$ $<P_{V,C}>$ <”Conservative”>

(III) $<SigP_{Gov}><P_{Gov}>$ $<T_V>$ $<SigP_{V,L}>$ $<P_{V,L}>$ <”Labour”>

(IV) $<SigP_{Gov}>$ $<P_{Gov}>$ $<T_V>$ $<SigP_{V,C}>$ $<P_{V,C}>$ <”Conservative”>

実施形態は、以下から切り換えるために、スクリプトレベルの適応性により切り換え条件の概念を使用する。
【数１２】

- (I) → (III)　　労働党への世論調査を労働党への投票に変換する、

  又は、

- (II) → (IV)　　保守党への世論調査を保守党への投票に変換する

これらの切り換えは、同じ政党について、世論調査を（”→”）投票へ変換することを表

す。これらの変換は、適応性を用いて達成できる。何故なら、使用された公開鍵、従って署名は、切り換えに跨がり一貫しているからである。インプットスクリプトデータの残りの部分のみが、適応され（malleated）、従って、投票者の署名は変更される必要がない。

【０１９０】

しかしながら、有権者が条件を以下から切り換えたい場合：

【数１３】

- (I) → (II)　[世論調査選択肢を労働党から保守党へ切り換える];

又は、

- (III) → (IV)　[投票選択肢を労働党から保守党へ切り換える]

実施形態では、これは、適応性及び切り換え条件を用いて行うことができない。代替として、しかしながら、これは、代わりに、それぞれ世論調査又は投票トランザクションのシーケンス番号を増加させることにより、達成できる。ここで、Alice（投票者）により署名されたメッセージがシーケンス番号を含む。これは、Aliceの世論調査選択についてのAliceの署名が、彼女の後の投票選択を偽造する目的でAliceの署名を再生するために悪意ある第三者により使用できないことを意味する。

【０１９１】

アンロック条件は、特定のロックスクリプトをアンロックするために使用される。それにより、各アンロック条件は、ロックスクリプト内の別個のロック条件を満たす。問題のロックスクリプトは、ここでは「投票スクリプト（Vote script）」と呼ばれ、以下に示される。

【数１４】

OP_DUP OP_HASH256 <$H("Labour")$> OP_EQUAL

OP_IF

OP_DROP OP_DUP OP_HASH160 <$H(P_{V,L})$> OP_EQUALVERIFY OP_CHECKSIGVERIFY

OP_HASH256 <$H(T_V)$> OP_EQUAL

OP_IF

OP_DUP OP_HASH160 <$H(P_{Gov})$> OP_EQUALVERIFY OP_CHECKSIGVERIFY

OP_ELSE

OP_1

OP_ENDIF

OP_ELSE

OP_HASH256 <$H("Conservative")$> OP_EQUAL

OP_IF

OP_DROP OP_DUP OP_HASH160 <$H(P_{V,C})$> OP_EQUALVERIFY OP_CHECKSIGVERIFY

OP_HASH256 <$H(T_V)$> OP_EQUAL

OP_IF

OP_DUP OP_HASH160 <$H(P_{Gov})$> OP_EQUALVERIFY OP_CHECKSIGVERIFY

OP_ELSE

OP_1

OP_ENDIF

OP_ELSE

OP_0

OP_ENDIF

OP_ENDIF

【０１９２】

世論調査及び投票手順は図１０に示される。これは、t_0における選挙の公示からt_3における投票期間の終了までの完全な世論調査及び投票処理を示すシーケンス図である。

【０１９３】

この手順は、以下のステップに分けられる。

【０１９４】

ステップ１：Bobの行政体P_{Gov}は、後の時間t_2において行われる投票のために、時間t_0で投票者登録を開始する。投票者は、投票処理の部分として彼らのハッシングされたトークン$H(T_V)$を自由に登録し与える。

【０１９５】

ステップ２：Bobの行政体P_{Gov}は、N個の投票票トランザクションTx_{Poll}を発行する。各票支払い、個々の有権者は、ロックスクリプト［投票スクリプト］により、前述のよう

に、該投票者の公開鍵P_Vに調整される。各トランザクションは、後の時間t_2にタイムロックされる。

【０１９６】

ステップ３：投票者Aliceは、公開鍵P_Vを有し、世論調査フェーズに参加したいと望む。世論調査フェーズは、全ての時間ｔ：$t_0<t<t_2$として定義される。投票者は、彼女の選択「労働党」を行い、及びアンロックスクリプト条件（ｉ）を用いて世論調査トランザクションTx_{Poll}（図１１）を構成することにより、世論調査に参加する。

【０１９７】

このトランザクションは、投票者、行政、又は第三者により公開できるが、t_2までマイニングできない。

【０１９８】

投票者が彼女の世論調査選択を「保守党」に変更したい場合、彼女は代わりにスクリプト条件（ｉｉ）を用いて、新しい世論調査トランザクションを生成し、シーケンス番号を増加させなければならない。

【０１９９】

ステップ４：投票者Aliceは、何らかの時間t_1で、彼女が彼女の「労働党」の世論調査選択肢を投票選択肢に変換したいと決定する。これは、世論調査トランザクションのアンロックスクリプトを適応して、投票トランザクションを生成することを含む。適応は、アンロック条件をスクリプト条件（ｉｉｉ）［（ｉ）→（ｉｉｉ）］に変更する。

【０２００】

適応を実行するために、ステップ４で、投票者Aliceは、彼女の投票トークンT_VをBobの行政体へ送信する。ステップ５で、Bobの行政体は、世論調査トークンを投票トークンへ切り換えて、世論調査トランザクションを投票トランザクションに変え、$Sig(P_{Gov},Tx_{Vote})$により投票トランザクションに署名して、それが有効な投票であることを確認する。変形として、投票者は、投票トークンをトランザクションに入れ、それを署名するために行政へと送信し得る。

【０２０１】

世論調査トランザクション及び後に生成される対応する投票トランザクションの両方は、両方のトランザクションに配置されたロックタイムt_2のために、全ての時間$t<t_2$において無効である。

【０２０２】

ステップ６：Bobの行政体は、t_2で、全部の有効な投票トランザクションをブロードキャストする。Bobの行政体は、時間ｔ：$t_2<t<t_3$、で確定する任意の他の投票トランザクションをブロードキャストし続ける。ここで、t_2は投票期間の開始を定義し、t_3は投票期間の終了を定義する。

【０２０３】

実施形態では、行政体は世論調査トランザクションをブロードキャストしない。これをブロードキャストし報酬を請求することは、調査の対象になる人（Alice）に委ねられる。

【０２０４】

Tx_{slip}は、Tx_{poll}/Tx_{vote}内で使用されるUTXOが実際に存在するように、処理の中の何らかの時点でマイニングされる必要もあることに留意する。簡単のために、このステップは図１０に示されない。トランザクションを時間制限（lock-time）するために使用される実際の方法は、Tx_{slip}がネットワーク１０６へ送信される図１０のシグナリング図の中のどの時点でも僅かに影響する。各Tx_{slip}に「nLocktime」（定義８）を入れる場合、Tx_{slip}も、図の段階６（及び／又は最終的な任意的段階）でマイニングされるためにブロードキャストされる必要がある。代わりに、Tx_{slip}のロックスクリプト内にOP_CLTV又はOP_CSV（定義１０及び１１）を入れることを選択した場合、Tx_{slip}は、上述のステップ２と同じ時間にマイニングできる。

【０２０５】

図１１は、処理を実装するために使用できる幾つかの例示的なトランザクションを示す

。上段のトランザクションTx_{slip}は、選挙民の構成員に世論調査及び／又は投票を行うことにより資金を請求することを可能にする投票票トランザクションである。アウトプットは、投票期間がt_2で開始した後にのみ請求できる。中段のトランザクションは、投票者が世論調査の部分としての選択肢を選択したことを意味する世論調査トランザクションTx_{Poll}である。ロックタイムがOP_CSV又はOP_CLTVを用いて実装され、Tx_{slip}が投票者へ送信されたのと同じ時間にネットワークへ送信された（ステップ２）例を仮定すると、このトランザクションは、自身のインプットの中で参照するTx_{slip}のアウトプットに設定されたタイムロックにより、t_2まで無効である。下段のトランザクションは、投票者が投票の部分としての選択肢を選択したことを意味する投票トランザクションTx_{vote}である。このトランザクションは、Tx_{Poll}と同じであるが、スクリプトレベルの適応性を用いてアンロック条件を切り換えられている。このトランザクションは、同様に、t_2まで無効である。

【０２０６】

実施形態では、タイムロックは、第１トランザクションのアウトプットの部分として含まれる（Tx_{Slip}）。代替的なメカニズムでは、しかしながら、ほぼ同じ効果を得るために、Tx_{Slip}ではなく、Tx_{Poll}をタイムロックする。

【０２０７】

＜結論＞

上記の実施形態は、単なる例示として説明したものであることが理解されるであろう。

【０２０８】

更に一般的には、本願明細書に開示される一態様によると、第１パーティと第２パーティとの間のターゲットトランザクションをブロックチェーンに記録する方法であって、前記方法は、前記第１パーティ及び前記第２パーティのコンピュータ機器により、

前記ターゲットトランザクションの既存の第１バージョンに対して更新されている、前記ターゲットトランザクションの第２の更新バージョンを取得するステップと、

ノードのネットワークを通じて伝播され前記ノードのうちの少なくとも幾つかの各々において維持されるブロックチェーンのコピーに記録されるように、前記第１バージョンの代わりに、前記ターゲットトランザクションの前記更新バージョンを送信するステップと、

を含み、

前記ターゲットトランザクションは、アンロックスクリプトと、第１トランザクションの第１アウトプットへのポインタと、を含むインプットを含み、前記第１アウトプットは、前記第１トランザクションの前記第１アウトプットをアンロックするための複数の代替条件を指定するロックスクリプトを含み、

前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記代替条件のうちの第１条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成され、前記更新バージョンの前記アンロックスクリプトは、前記第１条件の代わりに、前記代替条件のうちの第２条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成される、方法が提供される。

【０２０９】

実施形態では、当該方法は、前記第２パーティのコンピュータ機器により、前記ネットワークを通じて伝播され前記第１条件を満たすことに基づき前記ブロックチェーンに記録されるよう、前記第２パーティが前記ターゲットトランザクションの前記第１バージョンを送信できるようにする機能を提供するステップ、を含んでよい。

【０２１０】

機能は、前記第２パーティが、前記ネットワークを通じて伝播され前記第１又は第２条件をそれぞれ満たすことに基づきブロックチェーンに記録されるよう、前記ターゲットトランザクションの前記第１又は更新バージョンを選択的に送信することを可能にしてよく、当該方法は、前記第２パーティが前記機能を用いて、前記第１バージョンの代わりに、前記更新バージョンをブロックチェーンに記録されるよう前記の送信を実行するステップを含む。

【０２１１】
実施形態では、前記機能は、前記第２パーティに、前記第１バージョンの送信を実行することを手動で選択するためのオプションを提供してよく、及び／又は、
前記機能は、所定の時間の終了後に又は所定のイベントにより、前記ターゲットトランザクションの前記第１バージョンの送信を自動的にトリガするよう構成されてよい。
【０２１２】
実施形態では、前記ターゲットトランザクションの前記更新バージョンを取得すること、及び伝播され前記ブロックチェーンに記録されるよう該更新バージョンを送信することは、前記第２パーティのコンピュータ機器により実行されてよい。
【０２１３】
実施形態では、前記第２バージョンを取得するステップは、前記第２パーティが第１パーティから前記第２バージョンの少なくとも部分を受信するステップを含んでよい。
【０２１４】
実施形態では、前記方法は、前記第２パーティのコンピュータ機器により、
前記ターゲットトランザクションの前記第１バージョンを取得するステップであって、前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記第２パーティが、前記第１条件を満たすことに基づき前記第１トランザクションの前記第１アウトプットを自動的にアンロックできるように構成されてよい、ステップ、を含んでよい。
【０２１５】
実施形態では、前記ターゲットトランザクションの前記第２バージョンは、前記第１バージョンの後に取得されてよい。
【０２１６】
実施形態では、前記第１バージョンを取得するステップは、前記第２パーティが第１パーティから前記第１バージョンの少なくとも部分を受信するステップを含んでよい。
【０２１７】
実施形態では、前記第１バージョンを取得するステップは、前記第２パーティが前記第１トランザクションを生成するステップを含んでよい。
【０２１８】
実施形態では、前記第２条件は、前記アンロックスクリプトが、前記アンロックスクリプト以外の前記ターゲットトランザクションの部分に署名する前記第１パーティの暗号署名を含むことを要求してよい。この場合、前記ターゲットトランザクションの前記更新バージョンを取得するステップは、前記第１パーティの署名を取得するステップを含み、伝播されブロックチェーンに記録されるよう送信される前記更新バージョンは、アンロックスクリプト内に前記第１パーティの署名を含む。
【０２１９】
実施形態では、前記第１条件は、前記第１パーティの暗号書名を要求しなくてよい。
【０２２０】
実施形態では、少なくとも前記第１条件は、前記アンロックスクリプトが、前記アンロックスクリプト以外の前記ターゲットトランザクションの部分に署名する前記第２パーティの暗号署名を含むことを要求してよい。
【０２２１】
実施形態では、前記第２条件は、前記アンロックスクリプトが、前記アンロックスクリプト以外の前記ターゲットトランザクションの部分に署名する前記第２パーティの暗号署名を含むことを要求してよい。この場合、伝播されブロックチェーンに記録されるよう送信される前記更新バージョンは、前記アンロックスクリプト内に前記第２パーティの暗号署名を含む。
【０２２２】
実施形態では、前記更新バージョンを取得するステップは、前記第２パーティが、前記第１バージョンを前記第１パーティへ送信して、前記第１パーティが前記第１パーティの

署名を追加することにより前記更新バージョンへと適応する、ステップを含んでよい。前記第１及び第２条件は、前記第２パーティの同じ署名が前記ターゲットトランザクションの同じ部分に署名することを要求してよく、従って、前記第２パーティは前記更新バージョンに再び署名する必要がない。

【０２２３】

実施形態では、前記第１条件は、データペイロードがアンロックスクリプトに含まれることを要求してよいが、前記第２条件は、前記データペイロードが前記ターゲットトランザクションに含まれることを要求しなくてよい。この場合、ネットワークを介して伝播されブロックチェーンに記録されるよう送信される前記更新バージョンは、前記データペイロードを含む必要がない。

【０２２４】

実施形態では、前記第１条件は、前記アンロックスクリプトが前記データペイロード及び前記アンロックスクリプトを除く前記ターゲットトランザクションの部分に署名する前記第２パーティの暗号署名を含むことを要求してよいが、前記第１パーティの暗号書名がターゲットトランザクションに含まれることを要求せず、前記第２条件は、前記アンロックスクリプトが前記第１パーティ及び前記第２パーティの両方の暗号署名を含むことを要求してよいが、前記データペイロードが前記ターゲットトランザクションに含まれることを要求しなくてよい。このような実施形態では、前記ターゲットトランザクションの前記更新バージョンを取得するステップは、前記第１パーティの署名を取得するステップを含み、伝播されブロックチェーンに記録されるよう送信される前記ターゲットトランザクションの前記更新バージョンは、前記データペイロードを含む必要がないが、前記アンロックスクリプト内に前記第１パーティ及び第２パーティの署名を含む。

【０２２５】

実施形態では、前記要件は、前記それぞれのデータ部分が前記ロックスクリプトに含まれるハッシュチャレンジにより生成されることを含み、前記ハッシュチャレンジは、前記それぞれのデータ部分のハッシュと、前記アンロックスクリプト内の前記それぞれのデータ部分のハッシュが前記ロックスクリプトに含まれるハッシュと一致することをチェックするためのハッシュ関数と、を含む。前記方法は、前記ネットワークと別に、前記第１トランザクションのインスタンスを受信する前に、ハッシュセット（例えば、ハッシュツリー）を前記第１パーティに利用可能にするステップを含んでよく、前記ハッシュセットは、第２第１パーティが前記それぞれのデータ部分の前記ハッシュチャレンジを生成できるようにするために、前記データ部分の各々のハッシュ値を含む。

【０２２６】

実施形態では、前記第１トランザクションの前記第１アウトプットは、前記第１条件又は前記第２条件に従い前記第１アウトプットをアンロックすることにより償還される、前記第２パーティへの支払いを指定してよく、

前記ターゲットトランザクションは、前記支払いの少なくとも一部を前記第２パーティへ移転するアウトプットを含んでよい。

【０２２７】

実施形態では、前記方法は、前記第２パーティの前記コンピュータ機器により、

前記第１パーティへデータ部分のシーケンスをストリーミングするステップであって、前記シーケンスの中の最終部分により終了する、ステップと、

前記データ部分のうちのそれぞれの部分に応答して、前記第１パーティから前記第１トランザクションのそれぞれのインスタンスを受信するステップであって、各インスタンスの第１アウトプットは、前記それぞれの部分についての前記第２パーティへの支払いを指定する、ステップと、

を含んでよく

前記支払いは各データ部分と共に増大し、

前記ターゲットトランザクションの前記更新バージョンを取得するステップは、前記シーケンスの中の前記最終部分に続き、前記第１パーティから前記更新バージョンを受信す

るステップを含む。
【０２２８】
実施形態では、前記増大は、それまでに送信されたデータ部分の数に線形に比例してよい。
【０２２９】
実施形態では、各データ部分は、メディアコンテンツ（例えば、オーディオ及び／又はビデオコンテンツ）のアイテムの異なる部分であってよい。
【０２３０】
代替として、各データ部分は、サービスのユニット（例えば、ガス、水道、電気を含む生活必需サービスの供給、又は車両、不動産、又は他の物理的アイテムのレンタル）にアクセスするための異なる鍵であってよい。
【０２３１】
実施形態では、前記関数は、前記第１パーティからそれまでに受信したシーケンスの中の前記第１トランザクションの最新のインスタンスを償還するために、シーケンスの中の任意の時点で、前記ネットワークを通じて伝播されブロックチェーンに記録されるよう前記ターゲットトランザクションの前記第１バージョンの送信を実行することを手動で選択するオプションを、前記第２パーティに提供してよい。代替又は追加として、前記関数は、前記第１パーティが前記第１トランザクションのインスタンスを送信するのをシーケンスの途中で止めた場合に、前記第１トランザクションの最新のインスタンスを償還するために、ネットワークを通じて伝播されブロックチェーンに記録されるよう前記第１バージョンの送信を自動的に実行するよう構成されてよい。
【０２３２】
実施形態では、前記第１トランザクションは、インプット額を指定する１つ以上の第１インプットを含んでよく、前記第１トランザクションの前記第１アウトプットは第１支払いを指定してよく、前記第１トランザクションは、１つ以上の更なる支払いを指定する１つ以上の更なるアウトプットを更に含んでよい。その結果、支払いの合計は前記インプット額より高く、前記第１パーティから前記第２パーティにより受信される前記第１トランザクションは、差分を生成する他のインプットを有しない。ネットワークのノードは、前記第１トランザクションが合計インプット額より多くの合計支払いを指定する場合、前記第１トランザクションを無効であるとして拒否するよう構成されてよい。このような実施形態では、当該方法は、前記差分を構成する（make up）ために、前記第２パーティが第２インプットを前記第１トランザクションの最終又は最近のインスタンスに追加するステップと、追加された前記第２インプットを有する前記第１トランザクションを、ネットワークを通じて伝播されブロックチェーンに記録されるよう送信するステップと、を含んでよい。
【０２３３】
実施形態では、更なるアウトプットは、前記インプット額から前記第１支払いを差し引いたものに等しい、前記第１パーティへの第２支払いを指定する第２アウトプットと、前記第２支払いに等しい、前記第２パーティへの第３支払いを指定する第３アウトプットと、を含んでよい。
【０２３４】
実施形態では、前記ロックスクリプトは、前記代替条件のうちの第３条件を含み、これは、ロックタイムが終了すること、及び前記第１パーティの暗号署名が前記アンロックスクリプトに含まれることを要求し、従って、前記第２パーティにより前記ロックタイムの範囲内で償還されなかった場合、前記第１パーティが、前記第１トランザクションの前記第１アウトプットの中の支払いを償還することを可能にする。
【０２３５】
実施形態では、前記代替条件のうちの少なくとも幾つかの各々は、投票のための異なる選択肢に対応してよく、
前記方法は、前記ターゲットトランザクションの前記更新バージョンを取得するステッ

プの前に、前記第１バージョンの中の前記アンロックスクリプトを、投票意向の拘束力のない指示として、アクセスする又は第三者によりアクセス可能であるとマークするステップを含んでよい。

【０２３６】

実施形態では、ロックタイムは所定の時点の後になるまで前記ネットワークが前記ブロックチェーンに前記第１バージョンを記録するのを防ぐために、前記第１トランザクション及び前記ターゲットトランザクションの前記第１バージョンのうちの少なくとも１つに含まれてよい。

【０２３７】

実施形態では、前記第１トランザクションの前記アウトプットは、前記ロックスクリプト内で指定された前記条件のうちのいずれか１つに従い前記第１アウトプットをアンロックすることにより償還される支払いを指定し、前記ターゲットトランザクションは、前記支払いのうちの少なくとも一部を前記第１パーティへ移転するアウトプットを含んでよい。

【０２３８】

実施形態では、前記代替条件は、前記第１選択肢の世論調査指示に対応する第１条件、前記第２選択肢の世論調査指示に対応する第２条件、前記第１選択肢の投票選択に対応する第３条件、及び前記第２選択肢の投票選択に対応する第４条件、を含んでよく、前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記第１又は前記第２条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成されてよく、前記ターゲットトランザクションの前記第２バージョンの前記アンロックスクリプトは、前記第１条件の代わりに前記第３条件を又は前記第２条件の代わりに前記第４条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成されることにより、前記世論調査指示を投票へと変換するよう構成されてよい。

【０２３９】

投票の場合には、前記第１条件は、前記ターゲットトランザクションの前記アンロックスクリプトが、前記ロックスクリプト以外の前記ターゲットトランザクションの部分に署名する前記第２パーティの暗号署名を含むことを要求してよい。前記第１条件は、前記第１パーティの前記署名が個人の投票トークンに署名することを要求してよい。前記第２条件は、前記ターゲットトランザクションの前記アンロックスクリプトが、前記第１パーティの前記署名と前記第２パーティの暗号署名とを含み、それぞれが前記ロックスクリプトを除く前記ターゲットトランザクションの部分に署名することを要求してよい。

【０２４０】

本願明細書に開示される別の態様によると、コンピュータ可読記憶装置上に具現化され、第１パーティ及び／又は第２パーティのコンピュータ機器上で実行すると本願明細書に開示されたいずれかの実施形態の方法を実行するよう構成される、コンピュータプログラムが提供される。

【０２４１】

別の態様によると、第１パーティ及び／又は第２パーティのコンピュータ機器であって、

１つ以上のメモリユニットを含むメモリと、

１つ以上の処理ユニットを含む処理機器と、

を含み、

前記メモリは、前記処理機器上で実行するよう構成されるコードを格納し、前記コードは本願明細書に開示されたに任意の実施形態の方法を実行するよう構成される、コンピュータ機器が提供される。

【０２４２】

本願明細書に開示される別の態様によると、コンピュータ可読記憶装置上に具現化され第２パーティのコンピュータで実行されると動作を実行するよう構成されるコンピュータプログラムであって、前記動作は、

前記ターゲットトランザクションの第１バージョンを取得するステップと、

前記ターゲットトランザクションの第２バージョンを取得するステップと、
ノードのネットワークを通じて伝播され前記ノードのうちの少なくとも幾つかの各々において維持されるブロックチェーンのコピーに記録されるように、前記第２パーティに前記第１及び第２バージョンいずれかを選択的に送信させるステップと、
を含み、
前記ターゲットトランザクションは、アンロックスクリプトと、第１トランザクションの第１アウトプットへのポインタと、を含むインプットを含み、前記第１アウトプットは、前記第１パーティのデジタルアセットの額を指定し、前記第１トランザクションの前記第１アウトプットをアンロックするための複数の代替条件を指定するロックスクリプトを含み、
前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記代替条件のうちの第１条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成され、前記アンロックスクリプトは、前記第１条件の代わりに、前記代替条件のうちの第２条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成される、コンピュータプログラムが提供される。

【０２４３】

本願明細書に開示される別の態様によると、コンピュータ可読記憶装置上に具現化され第２パーティのコンピュータ機器で実行されると動作を実行するよう構成されるコンピュータプログラムであって、前記動作は、
前記ターゲットトランザクションの第１バージョンを取得するステップと、
前記ターゲットトランザクションの第２バージョンを取得するステップと、
ノードのネットワークを通じて伝播され前記ノードのうちの少なくとも幾つかにおいて維持されるブロックチェーンのコピーに記録されるように、前記第２パーティに前記第１及び第２バージョンのいずれかを選択的に送信させるステップと、
を含み、
前記ターゲットトランザクションは、アンロックスクリプトと、第１トランザクションの第１アウトプットへのポインタと、を含むインプットを含み、前記第１アウトプットは、第１パーティのデジタルアセットの額を指定し、前記第１トランザクションの前記第１アウトプットをアンロックするための複数の代替条件を指定するロックスクリプトを含み、
前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記代替条件のうちの第１条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成され、前記アンロックスクリプトは、前記第１条件の代わりに、前記代替条件のうちの第２条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成される、コンピュータプログラムが提供される。

【０２４４】

本願明細書に開示される別の態様によると、第２パーティのコンピュータ機器であって、１つ以上のメモリユニットを含むメモリと、１つ以上の処理ユニットを含む処理機器と、を含み、前記メモリは前記処理機器上で実行するよう構成されるコードを格納し、前記コードは、前記処理機器上で動作を実行するよう構成され、前記動作は、
前記ターゲットトランザクションの第１バージョンを取得するステップと、
前記ターゲットトランザクションの第２のバージョンを取得するステップと、
ノードのネットワークを通じて伝播され前記ノードのうちの少なくとも幾つかにおいて維持されるブロックチェーンのコピーに記録されるように、前記第２パーティに前記第１及び第２バージョンいずれかを選択的に送信させるステップと、
を含み、
前記ターゲットトランザクションは、アンロックスクリプトと、第１トランザクションの第１アウトプットへのポインタと、を含むインプットを含み、前記第１アウトプットは、第１パーティのデジタルアセットの額を指定し、前記第１トランザクションの前記第１

アウトプットをアンロックするための複数の代替条件を指定するロックスクリプトを含み、
前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記代替条件のうちの第１条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成され、前記アンロックスクリプトは、前記第１条件の代わりに、前記代替条件のうちの第２条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成される、コンピュータ機器が提供される。

【０２４５】

本願明細書に開示される別態様によると、第２パーティにブロックチェーンにターゲットトランザクションを記録させる方法であって、前記方法は、第１パーティのコンピュータ機器により、
前記ターゲットトランザクションの既存の第１バージョンに対して更新されている、前記ターゲットトランザクションの更新バージョンを送信するステップと、
前記第１バージョンの代わりに、前記ターゲットトランザクションの前記更新バージョンを送信するステップであって、それにより、前記第２パーティが、ノードのネットワークを通じて伝播され前記ノードのうちの少なくとも幾つかにおいて維持されるブロックチェーンのコピーに記録されるように、前記更新バージョンを送信させる、ステップと、
を含み、
前記ターゲットトランザクションは、アンロックスクリプトと、第１トランザクションの第１アウトプットへのポインタと、を含むインプットを含み、前記第１アウトプットは、前記第１トランザクションの前記第１アウトプットをアンロックするための複数の代替条件を指定するロックスクリプトを含み、
前記ターゲットトランザクションの前記第１バージョンの前記アンロックスクリプトは、前記代替条件のうちの第１条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成され、前記アンロックスクリプトは、前記第１条件の代わりに、前記代替条件のうちの第２条件を満たすことに基づき、前記第１トランザクションの前記第１アウトプットをアンロックするよう構成される、方法が提供される。

【０２４６】

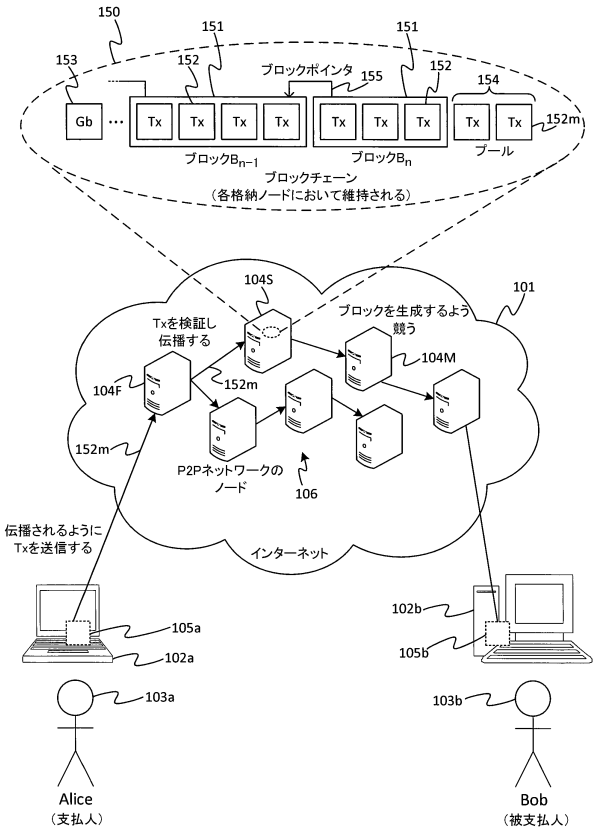
本願明細書に開示された別の態様によると、ブロックチェーンに記録するためのトランザクションのセットであって、前記セットは、コンピュータ可読データ媒体上に具現化され、
第１トランザクションのアウトプットをアンロックするための複数の代替条件を指定するロックスクリプトを含むアウトプットを有する第１トランザクションと、
アンロックスクリプトを含むインプット及び前記第１トランザクションのアウトプットへのポインタを有する第２トランザクションの第１バージョンと、
を含み、前記ターゲットトランザクションのz年期第１バージョンの前記アンロックスクリプトは、前記代替条件のうちの第１条件を満たすことに基づき、前記第１トランザクションの前記アウトプットをアンロックするよう構成され、
前記第２トランザクションの第２バージョンは、アンロックスクリプトを含むインプット、及び前記第１トランザクションの前記アウトプットへのポインタを含み、前記アンロックスクリプトは、前記第１条件の代わりに、前記代替条件のうちの第２条件を満たすことに基づき、前記第１トランザクションの前記アウトプットをアンロックするよう構成される、トランザクションのセットが提供される。

【０２４７】

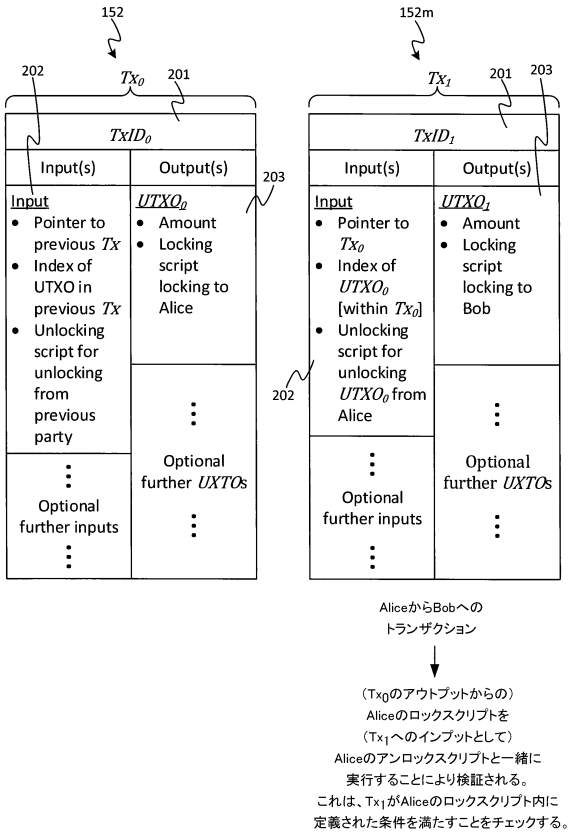
開示された技術の他の変形例又は使用事例は、本明細書で開示されると、当業者に明らかになり得る。本開示の範囲は、記載された実施形態によって限定されるものではなく、添付の特許請求の範囲によってのみ限定される。

【図面】

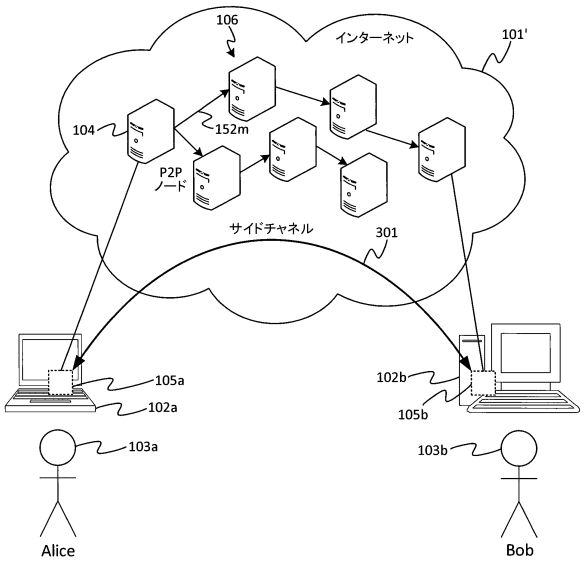
【図１】


150
151
151
153
152
ブロックポインタ
155
152
154
Gb
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
152m
ブロックB$_{n-1}$
ブロックB$_n$
プール
ブロックチェーン
（各格納ノードにおいて維持される）
104S
101
Txを検証し
伝播する
ブロックを生成するよう
競う
104M
104F
152m
152m
P2Pネットワークの
ノード
106
伝播されるように
Txを送信する
インターネット
105a
102a
103a
102b
105b
103b
Alice
（支払人）
Bob
（被支払人）

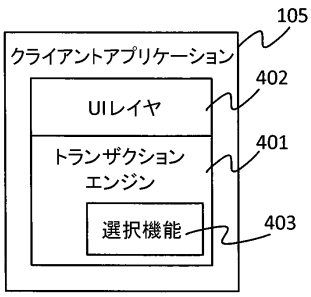
【図２】


152
202
Tx_0
201
$TxID_0$
Input(s)
Output(s)
203
Input
• Pointer to previous Tx
• Index of UTXO in previous Tx
• Unlocking script for unlocking from previous party
$UTXO_0$
• Amount
• Locking script locking to Alice
Optional further inputs
Optional further $UXTO$s
152m
Tx_1
201
203
$TxID_1$
Input(s)
Output(s)
202
Input
• Pointer to Tx_0
• Index of $UTXO_0$ [within Tx_0]
• Unlocking script for unlocking $UTXO_0$ from Alice
$UTXO_1$
• Amount
• Locking script locking to Bob
Optional further inputs
Optional further $UXTO$s
AliceからBobへの
トランザクション
（Tx_0のアウトプットからの）
Aliceのロックスクリプトを
（Tx_1へのインプットとして）
Aliceのアンロックスクリプトと一緒に
実行することにより検証される。
これは、Tx_1がAliceのロックスクリプト内に
定義された条件を満たすことをチェックする。

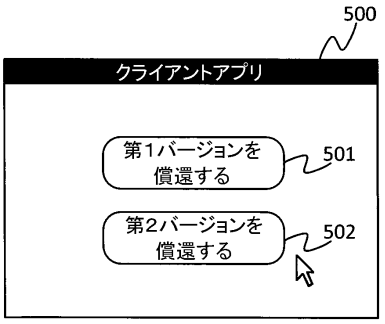
【図３】


106
インターネット
101'
104
152m
P2P
ノード
サイドチャネル
301
105a
102a
103a
102b
105b
103b
Alice
Bob

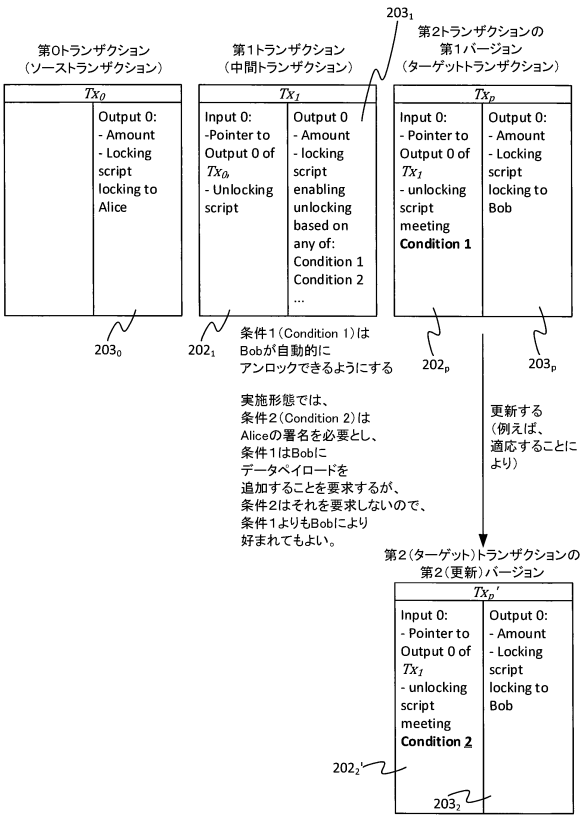
【図４】


105
クライアントアプリケーション
402
UIレイヤ
401
トランザクション
エンジン
403
選択機能

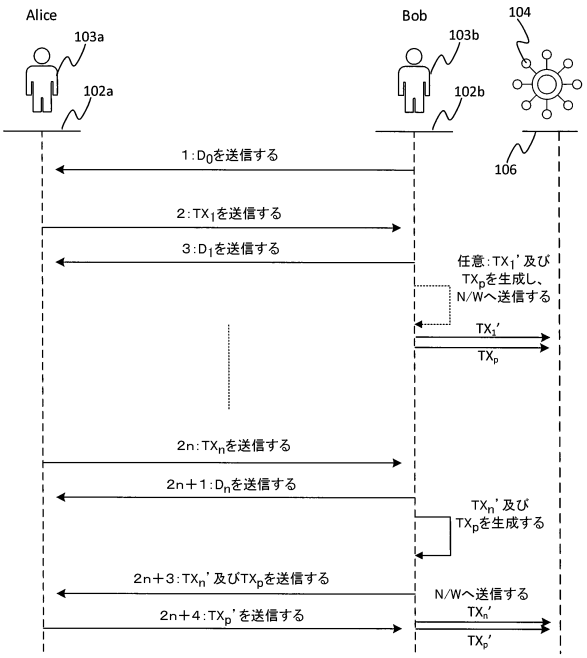
【図５】


500
クライアントアプリ
第1バージョンを償還する
501
第2バージョンを償還する
502

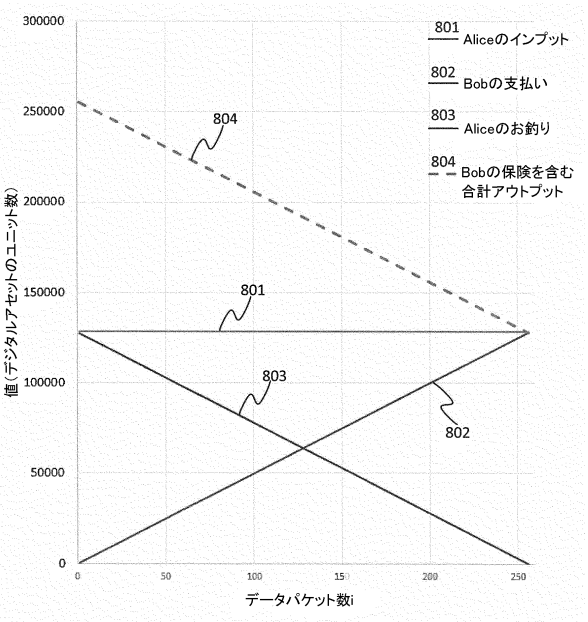
【図６】


第0トランザクション（ソーストランザクション）
第1トランザクション（中間トランザクション）
第2トランザクションの第1バージョン（ターゲットトランザクション）
Output 0: - Amount - Locking script locking to Alice
Input 0: -Pointer to Output 0 of Tx0, - Unlocking script
Output 0 - Amount - locking script enabling unlocking based on any of: Condition 1 Condition 2 ...
Input 0: - Pointer to Output 0 of Tx1 - unlocking script meeting Condition 1
Output 0: - Amount - Locking script locking to Bob
条件1（Condition 1）はBobが自動的にアンロックできるようにする
実施形態では、条件2（Condition 2）はAliceの署名を必要とし、条件1はBobにデータペイロードを追加することを要求するが、条件2はそれを要求しないので、条件1よりもBobにより好まれてもよい。
更新する（例えば、適応することにより）
第2（ターゲット）トランザクションの第2（更新）バージョン
Input 0: - Pointer to Output 0 of Tx1 - unlocking script meeting Condition 2
Output 0: - Amount - Locking script locking to Bob

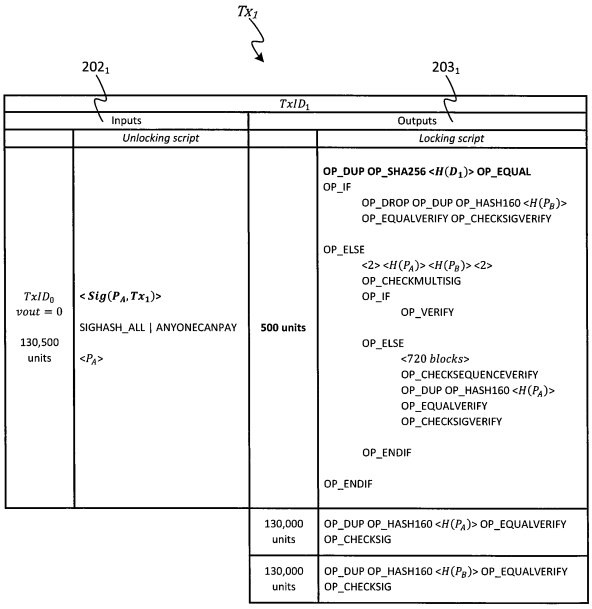
【図７】


Alice
Bob
103a
102a
103b
102b
104
106
1：D0を送信する
2：TX1を送信する
3：D1を送信する
任意：TX1'及びTXpを生成し、N/Wへ送信する
TX1'
TXp
2n：TXnを送信する
2n＋1：Dnを送信する
TXn'及びTXpを生成する
2n＋3：TXn'及びTXpを送信する
N/Wへ送信する
TXn'
2n＋4：TXp'を送信する
TXp'

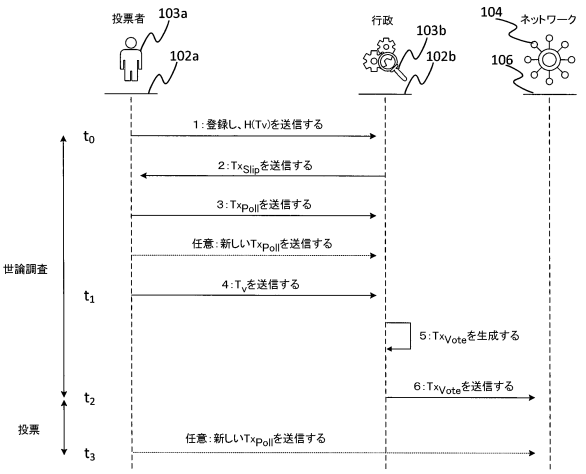
【図８】


801 Aliceのインプット
802 Bobの支払い
803 Aliceのお釣り
804 Bobの保険を含む合計アウトプット
値（デジタルアセットのユニット数）
データパケット数i
300000
250000
200000
150000
100000
50000
0
50
100
150
200
250

【図９】



【図１０】



【図１１】

$TxID_{Slip}$			
Inputs		Outputs	
	Unlocking script		*Locking script*
x BSV	< $Sig(P_{Gov}, Tx_{Slip})$ > <P_{Gov}>	x BSV	<t_2> OP_CHECKSEQUENCEVERIFY **[Vote script]**

$TxID_{Poll}$			
Inputs		Outputs	
	Unlocking script		*Locking script*
$TxID_{Slip}$ $vout = 0$ x BSV	< $Sig(P_{V,L}, Tx_{Poll})$ > <$P_{V,L}$> <"Lab"> ***OR*** < $Sig(P_{V,C}, Tx_{Poll})$ > <$P_{V,C}$> <"Cons">	x BSV	OP_DUP OP_HASH160 <$H(P_V)$> OP_EQUALVERIFY OP_CHECKSIG

$TxID_{Vote}$			
Inputs		Outputs	
	Unlocking script		*Locking script*
$TxID_{Slip}$ $vout = 0$ x BSV	< $Sig(P_{Gov}, Tx_{Vote})$ > <P_{Gov}> <T_V> < $Sig(P_{V,L}, Tx_{Poll})$ > <$P_{V,L}$> <"Lab"> ***OR*** < $Sig(P_{Gov}, Tx_{Vote})$ > <P_{Gov}> <T_V> < $Sig(P_{V,C}, Tx_{Poll})$ > <$P_{V,C}$> <"Cons">	x BSV	OP_DUP OP_HASH160 <$H(P_V)$> OP_EQUALVERIFY OP_CHECKSIG

フロントページの続き

(72)発明者　デイヴィーズ，ジャック
イギリス ダブリュー１ダブリュー ８エーピー ロンドン マーケット プレイス ３０ エヌチェーン ホールディングズ リミテッド 内
(72)発明者　ライト，クレイグ
イギリス ダブリュー１ダブリュー ８エーピー ロンドン マーケット プレイス ３０ エヌチェーン ホールディングズ リミテッド 内

審査官　青木 重徳

(56)参考文献
特開２００９－２７７２１７（ＪＰ，Ａ）
特表２０１９－５０７４４６（ＪＰ，Ａ）
国際公開第２０１８／０２０３８９（WO，Ａ２）
国際公開第２０１８／０７８５２０（WO，Ａ１）
淵田 康之，特集：イノベーションと金融 ブロックチェーンと金融取引の革新，野村資本市場クォータリー，日本，株式会社野村資本市場研究所，2015年11月01日，第１９巻第２号（通巻７４号），ｐ．１１－３５

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｇ０６Ｑ　３０／０６４５
Ｇ０６Ｑ　５０／０６
Ｇ０６Ｑ　５０／２６