

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7532414号
(P7532414)

(45)発行日 令和6年8月13日(2024.8.13)

(24)登録日 令和6年8月2日(2024.8.2)

(51)国際特許分類			F I		
H 0 4 L	9/32	(2006.01)	H 0 4 L	9/32	2 0 0 Z
G 0 6 F	21/10	(2013.01)	G 0 6 F	21/10	
G 0 6 Q	20/38	(2012.01)	G 0 6 Q	20/38	3 1 0
請求項の数 27 (全54頁)					
(21)出願番号 特願2021-568723(P2021-568723)			(73)特許権者 318001991		
(86)(22)出願日 令和2年4月21日(2020.4.21)			エヌチェーン ライセンシング アーゲー		
(65)公表番号 特表2022-533386(P2022-533386 A)			スイス・6 3 0 0・ツーク・グラーフェ		
(43)公表日 令和4年7月22日(2022.7.22)			ナウヴェーク・6		
(86)国際出願番号 PCT/IB2020/053771			(74)代理人 100107766		
(87)国際公開番号 WO2020/240292			弁理士 伊東 忠重		
(87)国際公開日 令和2年12月3日(2020.12.3)			(74)代理人 100070150		
審査請求日 令和5年3月22日(2023.3.22)			弁理士 伊東 忠彦		
(31)優先権主張番号 1907340.2			(74)代理人 100135079		
(32)優先日 令和1年5月24日(2019.5.24)			弁理士 宮崎 修		
(33)優先権主張国・地域又は機関 英国(GB)			(72)発明者 ジャン, ウェイ		
			イギリス ダブリュー1ダブリュー 8エ		
			ービー ロンドン マーケット プレイス		
			3 0 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】 サイドチャネル上でのデータの部分のストリーミング

(57)【特許請求の範囲】

【請求項1】

ノードのネットワークの少なくとも一部の夫々で保持されているブロックチェーンのコピーにターゲットトランザクションを記録する方法であって、

第2パーティのコンピュータ機器によって、

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間に、前記ネットワークとは別のサイドチャネルを形成することと、

連続したデータ部分のシーケンスを、該シーケンス内の最新のデータ部分まで、前記サイドチャネル上で前記第1パーティのコンピュータ機器へストリーミングすることと、

前記データ部分の各々のデータ部分に回答して、前記第1パーティのコンピュータ機器から第1トランザクションの異なった各々のインスタンスを前記サイドチャネル上で受信することであり、前記第1トランザクションは、デジタルアセットの量を指定する第1出力を有し、前記ターゲットトランザクションは、前記第1トランザクションの前記第1出力へのポインタを含む入力を含み、前記ターゲットトランザクションは、前記第1トランザクションの前記第1出力から前記第2パーティのコンピュータ機器へ転送すべき前記デジタルアセットの量を指定する出力を更に有し、前記第1トランザクションの前記第1出力で指定されている前記量は、前記第1トランザクションの連続するインスタンスごとに増大することと、

前記第1トランザクションの最新のインスタンス及び前記ターゲットトランザクションの対応するバージョンが前記ネットワークを通じて伝播されて前記ブロックチェーンに記

録されるようにすることであり、前記ターゲットトランザクションの前記対応するバージョンにおける前記ポインタは、前記シーケンスにおいて前記第1トランザクションの前記最新のインスタンスでの前記第1出力を指す、ことと
を有する方法。

【請求項2】

前記第1トランザクションの前記第1出力で指定されている前記量は、前記第1トランザクションの連続するインスタンスごとに線形に増大する、

請求項1に記載の方法。

【請求項3】

前記第1トランザクションの各インスタンスは、前記第1パーティのコンピュータ機器による前記各々のデータ部分の受信の肯定応答としての機能を果たし、

前記ストリーミングすることは、前記第1トランザクションの各インスタンスの受信に
応答して前記シーケンスにおける次のデータ部分を送信することを有する、

請求項1又は2に記載の方法。

【請求項4】

前記第2パーティのコンピュータ機器で、

前記第1トランザクションのインスタンスのうちのいずれか1つのインスタンスと、その
インスタンスを指す前記ターゲットトランザクションの対応するバージョンとが、前記
シーケンス内の任意の時点で、前記ネットワークにわたって伝播されて前記ブロックチェ
ーンに記録されるようにすることを可能にするアプリケーション機能を提供することを有し、

当該方法は、代わりに前記機能を用いて、前記インスタンスのうちの先行するインスタ
ンスのいずれかの代わりに、前記シーケンスにおける前記第1トランザクションの前記最
最新のインスタンス及び前記シーケンスにおける前記最新のインスタンスを指す前記ターゲ
ットトランザクションの対応するバージョンの伝播及び記録を引き起こすことを有する、
請求項1乃至3のうちいずれか一項に記載の方法。

【請求項5】

前記データ部分の夫々は、メディアコンテンツ片の各々の部分を有する、

請求項1乃至4のうちいずれか一項に記載の方法。

【請求項6】

前記データ部分の夫々は、前記第1パーティのコンピュータ機器がサービスサプライヤ
からのサービスのユニットをアンロックすることを可能にする異なった各々のキーを有す
る、

請求項1乃至4のうちいずれか一項に記載の方法。

【請求項7】

前記サービスは、

電気、ガス、又は水道を含む公共事業の提供、あるいは、

不動産、車、又は他の物理オブジェクトの賃借

のうちの1つを有する、

請求項6に記載の方法。

【請求項8】

前記シーケンスは、有限なシーケンスであり、

前記最新のデータ部分は、前記シーケンス内の最後の部分である、

請求項1乃至7のうちいずれか一項に記載の方法。

【請求項9】

前記第1トランザクションの少なくとも最後のインスタンスの前記第1出力は、少なく
とも第1条件及び第2条件を含む、前記第1トランザクションの前記第1出力をアンロッ
クするための複数の代替条件を指定するロッキングスクリプトを有し、前記ターゲットト
ランザクションの前記入力、アンロッキングスクリプトを有し、

前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるよう送信され

10

20

30

40

50

る前記ターゲットトランザクションの前記対応するバージョンにおいて、前記ロッキングスクリプトは、前記代替条件のうちの第1条件ではなく第2条件を満足することに基づいて前記第1トランザクションの前記第1出力をアンロックするよう構成される、

請求項8に記載の方法。

【請求項10】

前記第1トランザクションの各インスタンスの出力は、前記複数の代替条件を指定する前記ロッキングスクリプトを有し、

前記機能は、前記最後のインスタンスより前の前記第1トランザクションの現在受信されているインスタンスと、該現在のインスタンスを指す前記ターゲットトランザクションの第1バージョンとが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにすることを可能にし、前記第1バージョンにおける前記ロッキングスクリプトは、前記第1条件を満足することに基づいて前記第1トランザクションの前記第1出力をアンロックするよう構成され、前記第2条件を満足する前記ロッキング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バージョンは、第2バージョンである、

10

請求項4に従属する請求項9に記載の方法。

【請求項11】

前記機能は、前記第1トランザクションの前記現在受信されているインスタンス及び前記ターゲットトランザクションの第1バージョンが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにすることを手動で選択するためのオプションを前記シーケンス内の任意の時点で前記第2パーティのコンピュータ機器に提供し、かつ／あるいは、

20

前記機能は、前記第1パーティのコンピュータ機器が前記シーケンスを通じた前記第1トランザクションのインスタンスの送信を止める場合に、自動で前記第1トランザクションの前記現在のインスタンス及び前記ターゲットトランザクションの第1バージョンが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにするよう構成される、

請求項10に記載の方法。

【請求項12】

前記第2条件は、前記アンロッキングスクリプトが、該アンロッキング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1パーティの暗号署名を有することを要求し、

30

伝播されて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第2バージョンは、前記アンロッキングスクリプトにおいて前記第1パーティの前記署名を含む、

請求項10又は11に記載の方法。

【請求項13】

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乃至12のうちいずれか一項に記載の方法。

【請求項14】

少なくとも前記第1条件は、前記アンロッキングスクリプトが、該アンロッキング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する、

40

請求項10乃至13のうちいずれか一項に記載の方法。

【請求項15】

前記第2条件は、前記アンロッキングスクリプトが、該アンロッキング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、

伝播されて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第2バージョンは、前記アンロッキングスクリプトにおいて前記第2パーティの前記署名を含む、

請求項10乃至14のうちいずれか一項に記載の方法。

【請求項16】

50

前記第 2 パーティの前記コンピュータ機器によって、

前記第 1 パーティの前記署名を加えることによって前記第 1 パーティのコンピュータ機器が前記ターゲットトランザクションの前記第 2 バージョンに統合するように前記第 1 バージョンを前記第 1 パーティのコンピュータ機器へ送ることを有する、

請求項 13 又は 14 に記載の方法。

【請求項 17】

前記第 1 条件は、前記データ部分の夫々が前記アンロッキング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、前記データ部分のいずれも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通じて伝播されて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第 2 バージョンは、前記ターゲットトランザクションにおいて前記データ部分のいずれも含まない、

請求項 10 乃至 16 のうちいずれか一項に記載の方法。

【請求項 18】

前記第 1 条件は、前記アンロッキングスクリプトが前記データ部分の夫々と、前記アンロッキング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とを有することを要求するが、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、前記アンロッキング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有することを要求するが、前記データ部分のいずれも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、

伝播されて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第 2 バージョンは、該第 2 バージョンにおいて前記データ部分のいずれも含まないが、前記アンロッキングスクリプトにおいて前記第 1 パーティ及び前記第 2 パーティの前記署名を含む、

請求項 17 に記載の方法。

【請求項 19】

前記データ部分の夫々を含むという要件は、前記ロッキングスクリプトに含まれているハッシュチャレンジによって生成され、該ハッシュチャレンジは、データの各々の部分のハッシュと、前記アンロッキングスクリプトにおける各々のデータ部分のハッシュが前記ロッキングスクリプトに含まれているハッシュと一致することをチェックするハッシュ関数とを有し、

当該方法は、前記ネットワークとは別に、前記第 1 トランザクションのインスタンスの受信より前に、ハッシュセットを前記第 1 パーティのコンピュータ機器に利用可能にすることを有し、前記ハッシュセットは、前記第 1 パーティのコンピュータ機器が各々のデータ部分について前記ハッシュチャレンジを生成することを可能にするためのデータの部分ごとのハッシュ値を有する、

請求項 17 又は 18 に記載の方法。

【請求項 20】

当該方法は、前記第 2 パーティのコンピュータ機器が前記サイドチャンネル上で前記第 1 パーティのコンピュータ機器から前記第 1 トランザクションを受信することを有し、

前記第 1 トランザクションは、入力量を指定する 1 つ以上の第 1 入力を有し、前記第 1 トランザクションの前記第 1 出力は、第 1 ペイメントを指定し、前記第 1 トランザクションは、ペイメントの合計が前記入力量よりも多くなるように 1 つ以上の更なるペイメントを指定する 1 つ以上の更なる出力を更に有し、前記第 1 パーティのコンピュータ機器から前記第 2 パーティのコンピュータ機器によって受信される前記第 1 トランザクションは、差を補うための他の入力を有さず、前記ネットワークの前記ノードは、前記第 1 トランザクションが総入力量よりも多い総ペイメントを指定する場合には無効であるとして前記第 1 トランザクションを拒絶するよう構成され、

当該方法は、前記第 2 パーティのコンピュータ機器が、前記差を補うよう前記第 1 トラ

10

20

30

40

50

ンザクションの最新又は最後のインスタンスに第2入力を加え、該第2入力に加えられた前記第1トランザクションを、前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるよう送信することを有する、

請求項9乃至19のうちいずれか一項に記載の方法。

【請求項21】

前記更なる出力は、前記入力量から前記第1ペイメントをマイナスしたものに等しい前記第1パーティへの第2ペイメントを指定する第2出力と、前記第2ペイメントに等しい前記第2パーティへの第3ペイメントを指定する第3出力とを有する、

請求項20に記載の方法。

【請求項22】

前記ロッキングスクリプトは、前記代替条件のうちの第3条件を含み、該第3条件は、タイムアウト期間が経過していることと、前記第1パーティの暗号署名が前記アンロッキングスクリプトに含まれることを要求して、前記タイムアウト期間内に前記第2パーティのコンピュータ機器によって精算されない場合に前記第1パーティのコンピュータ機器が前記第1トランザクションの前記第1出力におけるペイメントを精算することを可能にする、

請求項9乃至21のうちいずれか一項に記載の方法。

【請求項23】

コンピュータ読み出し可能なストレージにおいて具現され、第2パーティのコンピュータ機器で実行される場合に、請求項1乃至22のうちいずれか一項に記載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。

【請求項24】

1つ以上のメモリユニットを有するメモリと、

1つ以上の処理ユニットを有する処理装置と

を有し、

前記メモリは、前記処理装置で実行されるよう配置されたコードを記憶し、該コードは、前記処理装置で実行される場合に、請求項1乃至22のうちいずれか一項に記載の方法を実行するよう構成される、

コンピュータ機器。

【請求項25】

ノードのネットワークの少なくとも一部の夫々で保持されているブロックチェーンのコピーにターゲットトランザクションを記録することを第2パーティに可能にする方法であって、

第1パーティのコンピュータ機器によって、

前記ネットワークとは別のサイドチャネルを介して、前記第2パーティのコンピュータ機器から連続したデータ部分のシーケンスを受信することと、

前記データ部分の各々のデータ部分に応答して、前記第1パーティのコンピュータ機器から第1トランザクションの異なった各々のインスタンスを前記サイドチャネル上で返送することであり、前記第1トランザクションは、デジタルアセットの量を指定する第1出力を有し、前記ターゲットトランザクションは、前記第1トランザクションの前記第1出力へのポインタを含む入力を有し、前記ターゲットトランザクションは、前記第1トランザクションの前記第1出力から前記第2パーティのコンピュータ機器へ転送すべき前記デジタルアセットの量を指定する出力を更に有し、前記第1トランザクションの前記第1出力で指定されている前記量は、前記第1トランザクションの連続するインスタンスごとに増大する、ことと

を有し、

それによって、前記第2パーティのコンピュータ機器が、前記ターゲットトランザクションのインスタンスのいずれか1つを、前記ネットワークにわたって伝播されて前記ブロックチェーンに記録されるよう送信することを可能にする、

方法。

10

20

30

40

50

【請求項 26】

コンピュータ読み出し可能なストレージにおいて具現され、第1パーティのコンピュータ機器で実行される場合に、請求項25に記載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。

【請求項 27】

1つ以上のメモリユニットを有するメモリと、

1つ以上の処理ユニットを有する処理装置と

を有し、

前記メモリは、前記処理装置で実行されるよう配置されたコードを記憶し、該コードは、前記処理装置で実行される場合に、請求項25に記載の方法を実行するよう構成される、コンピュータ機器。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、ブロックチェーンベースのシステムとの関連において「オフチェーン」サイドチャンネル上でのデータのストリーミング及び交換に関する。

【背景技術】

【0002】

ブロックチェーンは、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コピーが、ピア・ツー・ピア（P2P）ネットワーク内の複数のノードの夫々で保持される。ブロックチェーンは、データのブロックのチェーンを有し、各ブロックは1つ以上のトランザクションを有する。各トランザクションは、順番において前のトランザクションを指し示し得る。トランザクションは、「マイニング」として知られているプロセスによって新しいブロックに含まれるようネットワークにサブミットされ得る。マイニングは、複数のマイニングノードの夫々が「ブルーフ・オブ・ワーク」を実行するよう競争すること、すなわち、ブロックに含まれるよう待機しているペンディング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伴う。

【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、価値の蓄蔵として働くデータ、を運ぶために使用される。しかし、ブロックチェーンは、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も利用されることがある。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出力における追加のユーザデータの保存を可能にすることができる。最新のブロックチェーンは、より複雑なデータが組み込まれることを可能にしながら、単一のトランザクション内に保存され得る最大データ容量を増やしている。例えば、これは、ブロックチェーンに電子文書や、音声又は映像データさえも保存するために使用される可能性がある。

【0004】

ネットワーク内の各ノードは、3つの役割、転送、マイニング及び保存、のうちのいずれか1つ、2つ、又は全てを有することができる。転送ノードは、1つ以上の他のノードへ（有効な）トランザクションを夫々伝播し、よって、それらのノードの間でネットワークのノードにわたってトランザクションを伝播する。マイニングノードは、ブロック内へのトランザクションのマイニングを実行するよう夫々競争する。保存ノードは、ブロックチェーンのマイニングされたブロックのそれら自身のコピーを夫々記憶する。ブロックチェーンにトランザクションを記録するために、パーティは、ネットワークのノードの1つへトランザクションを送信して伝播する。トランザクションを受け取ったマイニングノードは、新しいブロック内にトランザクションをマイニングするために競争することができる。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、ブロック内にマイニングもされない。トランザクションが妥当性確認（validated）され、それによってブロックチェーン上に受け入れられると仮定すると、追加のユーザデータは、よ

10

20

30

40

50

って、不変のパブリックレコードとしてP 2 Pネットワーク内のノードの夫々で保存されたままである。

【0005】

プルーフ・オブ・ワークパズルを解いて最新のブロックを生成することに成功したマイナ(miner)は、通常は、新しい量のデジタルアセット生成する「ジェネレーショントランザクション」と呼ばれるトランザクションを見返りに与えられる。トランザクションは、任意に、成功したマイナに対する余分のマイニングフィーも指定してもよい。マイナは、ブロックをマイニングするために大量の計算リソースを必要とし、かつ、二重支払いの試みを含むブロックは、他のノードによって受け入れられない可能性があるので、プルーフ・オブ・ワークは、二重支払いトランザクションを彼らのブロックに含めることによってシステムをだまさないようにマイナに動機付けする。

10

【0006】

「出力ベース」のモデル(時々、UTXOベースモデルと呼ばれる)では、所与のトランザクションのデータ構造は、1つ以上の入力及び1つ以上の出力を有する。如何なる使用可能な(spendable)出力も、時々UTXO(“Unspent Transaction Output”)と呼ばれる、デジタルアセットの量を指定する要素を有する。出力は、出力を精算(redemption)する条件を指定するロッキングスクリプトを更に有することがある。各入力は、前のトランザクションにおけるかような出力へのポインタを有し、更には、指し示された出力のロッキングスクリプトをアンロックするアンロッキングスクリプトを有することがある。故に、一对のトランザクションを考え、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量を指定するとともに、出力をアンロックする1つ以上の条件を定義するロッキングスクリプトを有する少なくとも1つの出力を有する。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出力へのポインタと、第1トランザクションの出力をアンロックするアンロッキングスクリプトとを有する少なくとも1つの入力を有する。

20

【0007】

かようなモデルにおいて、第2の、ターゲットトランザクションがP 2 Pネットワークへ送られて伝播されて、ブロックチェーンに記録される場合に、各ノードで適用される妥当性のための条件のうちの1つは、第1トランザクションのロッキングスクリプトで定義されている要件をアンロッキングスクリプトが満足することである。ターゲットトランザクションが有効であるための他の条件は、第1トランザクションの出力が他の有効なトランザクションによってまだ精算されていないことである。これらの条件のいずれかに従ってターゲットトランザクションを無効と判断した如何なるノードも、ブロックチェーンに記録するためにそれを伝搬することも、それをブロック内にマイニングするために含めることもない。

30

【0008】

例えば、ターゲットトランザクションは、ある量のデジタルアセットを第1パーティ(「アリス」)から第2パーティ(「ボブ」)へ運ぶことであるとする。先行する第1トランザクションのロッキングスクリプトで定義されている要件のうちの1つは、通常は、ターゲットトランザクションのアンロッキングスクリプトがアリス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一部にアリスが署名することによって生成されるべきである。

40

【0009】

トランザクションがブロックチェーンに記録されるようP 2 Pネットワークへブロードキャストされる前に、「オフチェーン」でパーティ間のトランザクションを交換するために、「ペイメントチャネル」と時々呼ばれるサイドチャネルを形成することも知られている。サイドチャネルは、P 2 Pオーバーレイネットワークとは別であり、従って、サイドチャネル上で送信される如何なるトランザクションも、パーティの1つがそれをネットワークに公開すると選択するまでは、ブロックチェーンでの記録のためにネットワークにわ

50

たって（まだ）伝播されない。典型的なペイメントチャンネルは、「ファンディングトランザクション」（funding transaction）を必要とし、これによって、両方のパーティは、それらのファンドを一緒に有効にエスクローする。ファンディングトランザクションは、チャンネルをセットアップするようブロードキャストされ、それから、問題となっているサービスが提供されると、決算（settlement）トランザクションが、チャンネルを閉じるようブロードキャストされ、ファンディングトランザクションを使用する。

【0010】

「マイクロペイメントチャンネル」のための、つまり、小さいインストールメントで他のパーティ（「ボブ」）に支払うために1つのパーティ（「アリス」）からボブヘトランザクションのシーケンスを送るための、いくつかの既存の提案も存在している。これは、ファンディングトランザクションを必要としない。少なくとも1つの既存の提案は、パケットで映画のデータをストリーミングするためにサイドチャンネルを使用することである。ボブは、データのパケットのシーケンスをアリスに送り、各パケットに応答して、アリスは、各々のトランザクションを返す。それから、ボブは、それをネットワークにブロードキャストして、映画の各々のパケットに対する支払いを得る。

【発明の概要】

【0011】

しかし、マイクロペイメントチャンネルに対する既存の提案に伴う問題は、各々の個別トランザクションが、ボブがアリスとへ送るデータの各々の個別部分（例えば、映画の各パケット）について、P2Pネットワークへブロードキャストされてブロックチェーンに記録されることを必要とする点である。これは、より多くのネットワークトラフィックを生じさせるとともに、多数の小さいトランザクションでブロックチェーンを膨張させることになる。ファンディングトランザクションの必要を回避しながら、多くの小さい個別トランザクションでネットワークをあふれさせチェーンを膨張させることを回避するメカニズムを提供することが望まれる。

【0012】

本開示は、部分単位でデータのストリーミング及びストリーミングされたデータの各部に対する支払いを可能にしながら、シーケンス内のデータ部分の数（例えば、シーケンス内の3つ以上から数百又は数千を超える部分までの任意の数）にかかわらず、一対のトランザクションしか実際にネットワークへ送信されてブロックチェーンに記録されることを必要としないメカニズムを提供する。第1の受信パーティ（「アリス」）は、第2の送信パーティ（「ボブ」）からデータをストリーミングすることをいつでも停止可能であり、ボブは、ただ一対のトランザクションのネットワークへの公開に基づいて、これまでストリーミングされたデータの部分に対する支払いを依然として取得することができる。逆に、ボブは、データの部分を送信することをいつでも停止可能であり、アリスは、これまで送信されたデータの部分に対する支払いを取得することボブに可能にするだけである。

【0013】

これを達成するために、本明細書で開示されている一態様に従って、ノードのネットワークの少なくとも一部の夫々で保持されているブロックチェーンのコピーにターゲットトランザクションを記録する方法であって、第2パーティのコンピュータ機器によって実行される次の動作を有する方法が提供される。方法は、第1パーティと前記第2パーティとの間に、前記ネットワークとは別のサイドチャンネルを形成することと、連続したデータ部分のシーケンスを、該シーケンス内の最新のデータ部分まで、前記サイドチャンネル上で前記第1パーティヘストリーミングすることと、前記データ部分の各々のデータ部分に回答して、前記第1パーティから第1トランザクションの異なった各々のインスタンスを前記サイドチャンネル上で受信することとを有する。ターゲットトランザクションは、前記第1トランザクションの第1出力へのポイントを含む入力を含み、前記ターゲットトランザクションは、前記第1トランザクションの前記第1出力から前記第2パーティヘ転送すべき前記デジタルアセットの量を指定する出力を更に有し、前記量は、前記ターゲットトランザクションの連続するインスタンスごとに増大する。方法は、前記第1トランザクション

10

20

30

40

50

の最新のインスタンス及び前記ターゲットトランザクションの対応するバージョンが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにすることを更に有し、前記ターゲットトランザクションの前記対応するバージョンにおける前記ポインタは、順番において前記第1トランザクションの前記最新のインスタンスでの前記第1出力を指す。

【0014】

2つ（以上）のトランザクションは、両方が同じソーストランザクション（又は「0番目」のトランザクション）の同じ出力（例えば、UTXO）を参照する入力を含む場合には、（実質的に）同じトランザクションのインスタンスであると本明細書では言われることがある。それらは、同じアンロック条件を満足することに基づいてその入力を精算してもよい。それらは、しかし、異なる入力署名を含むことがある（例えば、どちらのインスタンス内の署名されたメッセージも非同一である）。異なるインスタンスは、実質的に同じ機能を提供し得るが、各々のデータ部分が異なっており、量が増大している。後述されるいくつかの実施形態はまた、ターゲットトランザクションの異なる可能なバージョンを可能にし得る。2つのトランザクションは、両方が（インスタンスにかかわらず）第1トランザクションの同じ出力（例えば、同じUTXO）を参照する入力を含む場合には、（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われることがある。異なるバージョンは、その出力の異なるアンロック条件を満足することによって、異なる機能を提供し得る。異なるバージョンはまた、両方が同じ入力署名を含んでもよい（すなわち、どちらのインスタンス内の署名されたメッセージも同一である）。

【0015】

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夫々について、ネットワークの少なくともいくつかのノードは、トランザクションが有効であるという条件で各トランザクションを伝播するよう構成され、少なくともいくつかのノードは、トランザクションが有効であるという条件でそのノードで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る。例えば、ターゲットトランザクションは、通常は、アンロックスクリプトが第1トランザクションの出力をアンロックすることを条件とする。しかし、ネットワーク内の各ノードはまた、インスタンスのうちの1つが任意の所与のノードで妥当性確認されると、それから、他のインスタンスが、そのノードによって無効と見なされるので、ノードによって伝播されることもブロックチェーンに記録されることもないように、構成される。また、ターゲットトランザクションの1バージョンが所与のノードで妥当性確認されると、それから、ターゲットトランザクションの如何なる他のバージョンもそのノードによって無効と見なされるので、ノードによって伝播されることもブロックチェーンに記録されることもない。

【0016】

第1トランザクションのインスタンス（例えば、それらを Tx_1 、 Tx_2 、 Tx_3 、・・・と呼ぶ）は、ネットワークの各ノードによって、実質的に同じトランザクションのインスタンスと見なされる。これは、各インスタンスが、同じ先行ソーストランザクション（又は「0番目」のトランザクションであり、以下の例では Tx_0 と表記される）の同じ出力を指し示す入力を有しているからである。これは、第1トランザクションの1つのインスタンス（例えば、 Tx_1 、 Tx_2 、・・・のうちの1つ）がマイニングされると直ぐに、それから、ソーストランザクション（例えば、 Tx_0 ）の出力が消費され、従って、如何なる他のインスタンスによっても消費され得ないことを意味する。従って、ただ1つのインスタンスしかブロックチェーンに記録され得ない。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、任意の所与のノードで、ターゲットトランザクションの任意のバージョン（例えば、 Tx_p 又は Tx_p' ）によって有効に精算されることが検出されると、それから、第1トランザクションのいずれかのインスタンスを精算しようと試みる如何なる更なるターゲットトランザクションも、そのノードによって無効と見なされ、従って、そのノードによって伝播されることもブロックチェーンに記録されることもない。

【0017】

ターゲットトランザクションの任意のバージョン（例えば、 $T x_p$ 又は $T x_p'$ ）が P 2 P ネットワーク上でブロードキャストされ、所与のノードで、第 1 トランザクションの特定のインスタンス（異なる量を定義する異なるインスタンス）の第 1 出力を有効に指し示すことが検出されると、これは、ただ 1 つのターゲットトランザクションしか出力を有効に精算することができないということで、その出力が如何なる更なるバージョンによっても再びに精算され得ないことを意味する。すなわち、第 1 トランザクションのインスタンス（ $T x_1$ 、 $T x_2$ 、 $T x_3$ 、 $\dots$ ）のうちの 1 つが、所与のノードでターゲットトランザクション（例えば、 $T x_p$ 又は $T x_p'$ ）によって有効に精算されることが検出されると、それから、第 1 トランザクションのいずれかのインスタンスを精算しようと試みる如何なる更なるターゲットトランザクションも、無効に見なされ、従って、そのノードによって伝播されることもブロックチェーンに記録されることもない。それでもなお、各インスタンスでの支払いも、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（「ボブ」）が行うべき全ては、第 1 トランザクションの最後又は最新のインスタンス $T x_n$ を精算するターゲットトランザクションのバージョン（例えば、 $T x_p'$ ）を、伝播されてブロックチェーンに記録されるよう送信される。彼は、次いで、単一のトランザクション対に基づいてその時点までに送られたデータの全部分に対する完全な支払いを受け取る。

【0018】

任意の時点で、アリスが、シーケンスの終了前に、第 1 トランザクションのインスタンス（ $T x_1$ 、 $T x_2$ 、 $T x_3$ 、 $\dots$ ）を送ることを止めた場合に、ボブは、更なるデータ部分をアリスへ送ることを止めて、その時点より前に送られたデータの部分に対する支払いを精算するためにターゲットトランザクションのバージョン（例えば、 $T x_p$ ）をネットワークへ送信するという選択肢を依然として有している（従って、送信された最新のデータ部分のみを失う）。逆に、任意の時点で、ボブがデータ部分を送信することを止めた場合に、アリスは、第 1 トランザクションの更なるインスタンス $T x_i$ を送信することを止めるという選択肢を有しており、ボブは、それまでにアリスが受け取ったデータ部分に対する支払いを精算する能力のみを受け取っていることになる。

【0019】

特定の任意の実施で、方法は、前記第 2 パーティが前記サイドチャネル上で前記第 1 パーティから前記第 1 トランザクションを受信することを有してもよく、前記第 1 トランザクションは、入力量を指定する 1 つ以上の第 1 入力に有してもよく、前記第 1 トランザクションの前記第 1 出力は、第 1 ペイメントを指定し、前記第 1 トランザクションは、支払いの合計が前記入力量よりも多くなるように 1 つ以上の更なる支払いを指定する 1 つ以上の更なる出力を更に有し、前記第 1 パーティから前記第 2 パーティによって受信される前記第 1 トランザクションは、差を補うための他の入力を有さない。例えば、前記更なる出力は、前記入力量から前記第 1 ペイメントをマイナスしたものに等しい前記第 1 パーティへの第 2 ペイメントを指定する第 2 出力と、前記第 2 ペイメントに等しい前記第 2 パーティへの第 3 ペイメントを指定する第 3 出力とを有してもよい。前記ネットワークの前記ノードは、前記第 1 トランザクションが総入力量よりも多い総支払いを指定する場合には無効であるとして前記第 1 トランザクションを拒絶する。かような実施形態で、方法は、前記第 2 パーティが、前記差を補うよう前記第 1 トランザクションの最新又は最後のインスタンスに第 2 入力を加え、該第 2 入力に加えられた前記第 1 トランザクションを、前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるよう送信することを有する。

【0020】

これは、第 1 パーティ（「アリス」）が、彼女自身のターゲットトランザクションを送信して前のインスタンスのうちの 1 つを精算し、このようにして、ボブが後のインスタンスのうちの 1 つ（又は、実際には、インスタンスのうちのいずれか）を精算できないようにすることによって、システムをごまかすことを防ぐ。これは、そうするために、アリスが、彼女のデジタルアセットのより多くを負担することになる余分の入力を追加する必要

があるからである。従って、アリスがシステムをごまかそうとする価値はない。

【0021】

更なる任意の実施形態で、前記第1トランザクションの少なくとも最後のインスタンスの前記第1出力は、少なくとも第1条件及び第2条件を含む、前記第1トランザクションの前記第1出力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キングスクリプトを有してもよく、前記ターゲットトランザクションの前記入力、アンロッキングスクリプトを有してもよい。かような実施形態で、前記ネットワークを通じて伝播されて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対応するバージョンにおいて、前記ロッキングスクリプトは、前記代替条件のうちの第1条件ではなく第2条件を満足することに基づいて前記第1トランザクションの前記第1出力をアンロックするよう構成される。

10

【0022】

前記第1トランザクションの各インスタンスの出力は、前記複数の代替条件を指定する前記ロッキングスクリプトを有してもよい。この場合に、方法は、最後のインスタンスより前の前記第1トランザクションの現在受信されているインスタンスと、該現在のインスタンスを指す前記ターゲットトランザクションの第1バージョンとが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにすることを可能にする機能を提供することを有してもよく、前記第1バージョンにおける前記ロッキングスクリプトは、前記第1条件を満足することに基づいて前記第1トランザクションの前記第1出力をアンロックするよう構成される。

20

【0023】

例えば、前記機能は、前記第1トランザクションの前記現在受信されているインスタンス及び前記ターゲットトランザクションの第1バージョンが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにすることを手動で選択するためのオプションを前記シーケンス内の任意の時点で前記第2パーティに提供してもよい。代替的に、又は追加的に、前記機能は、前記第1パーティが前記シーケンスを通じた前記第1トランザクションのインスタンスの送信を止める場合に、自動で前記第1トランザクションの前記現在のインスタンス及び前記ターゲットトランザクションの第1バージョンが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにするよう構成されてもよい。

30

【0024】

ターゲットトランザクションの有効性は、上記の条件のうちのいずれか1つに従ってアンロッキングスクリプトが第1トランザクションの出力をアンロックすることを条件とする。しかし、バージョンのうちの1つが任意の所与のノードで妥当性確認されると、他のバージョンは、そのノードで無効と見なされることになるので、そのノードによって伝播されることも、そのノードでブロックチェーンに記録されることもない。

【0025】

従って、第2パーティ（「ボブ」）は、両方のバージョンが第1トランザクションを有効に精算することができないということで、両方のバージョンを、伝播されてブロックチェーンに記録されるよう送信しない。彼は、第2条件を満足することに基づいて、第2バージョンを、伝播されて記録されるように送信する。これは、彼の好みである。しかし、第1バージョンが存在したという事実により、第2バージョンに対する必要な条件が満たされない場合には、第1バージョンが記録されたというフォールバックが彼に与えられる。例えば、第1条件は、データペイロードがターゲットトランザクションのアンロッキングスクリプトに含まれることを求めてもよく、これはボブにペナルティを課すことになる（例えば、マイニングフィーがデータサイズに比例するため、及び／又はデータがボブに独自のものであって、それをブロックチェーンに置くことがそれを公にすることになるため）。他方で、第2条件は、アリスの署名を求めてもよく、従って、アリスの承認を必要とする。

40

【0026】

50

本明細書で開示されている更なる態様によれば、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ムされている第2パーティのコンピュータ機器が提供される。

【0027】

本開示の実施形態の理解を助けるために、かつ、どのようにそのような実施形態が具体化され得るかを示すために、単なる例として、添付の図面が参照される。

【図面の簡単な説明】

【0028】

【図1】ブロックチェーンを実装するシステムの略ブロック図である。

【図2】ブロックチェーンに記録され得るトランザクションのいくつかの例を概略的に表す。

【図3】ブロックチェーンを実装する他のシステムの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って提示され得るユーザインターフェースの例の略モックアップである。

【図6】トランザクションの組の模式図である。

【図7】データをストリーミングする方法を示すシグナリングチャートである。

【図8】図7の方法の実施例における第1トランザクションのインスタンスの入力及び出力の値を示すグラフである。

【図9】図7の方法における第1トランザクションのためのトランザクションフォーマットの例である。

【発明を実施するための形態】

【0029】

述べられたように、ペイメントチャネル及びマイクロペイメントチャネルのためのいくつかの既存の提案が存在している。しかし、それらは全て、個々のトランザクションが、ペイメントにおける個々のインクリメントごとに（すなわち、ストリーミングの場合には、送信された個々のデータ部分ごとに）、P2Pネットワーク上で公開されてブロックチェーンに記録されることを必要とする。これは、P2Pネットワーク上でのネットワーク輻輳を消費させ、また、小さいマイクロペイメントのための多くのトランザクションでブロックチェーンを膨張させる。

【0030】

本開示は、代わりに、ボブから受け取られたデータの各部分に応答して、アリスが、サイドチャネル上で、毎回ペイメントが増大する所与のトランザクションの異なるインスタンスをボブへ返送するメカニズムを提供する。ボブは、このトランザクションのインスタンスのうちの1つでのみペイメントを請求することができる。

【0031】

更に、既存のプロトコルのほとんどは、信頼を確立するためにファンディングトランザクションを必要とする。ペイメントチャネルの如何なる時期尚早の閉鎖も、ファンドが一定期間ロックされることを生じさせることになる。代替的に、それらは、コンセンサスルールの変更、つまり、プロトコルの安定性を損なう可能性がある新しいオペコードを導入すること、を必要とする。他のいくつかは、有効期限を有している。しかし、チャネルセットアッププロセスでのオーバーヘッドと相まって、有効期限は望ましくない特性になる。

【0032】

本明細書で開示されている実施形態は、ペイメントチャネルをセットアップするためのファンディングトランザクションを有さないという選択肢を提供する。代わりに、参加者は、彼らが望むようにチャネルに参加したり、チャネルから離れたたりすることができる。開示されている技術はまた、既存のトランザクション及びノードプロトコルで実装され可能である。

【0033】

実施形態は、可鍛性（malleability）の概念を利用し得る。可鍛性は、トランザクシ

10

20

30

40

50

ンを全体として無効にせずに、トランザクションの少なくとも一部を変更する能力を指す。関連する形式の暗号署名（例えば、E C D S A 署名）によって署名されているトランザクション内の如何なる署名も、書き換え（malleation）の可能性を受けない。

【0034】

例えば、ターゲットトランザクションは、ある量のデジタルアセットを第1パーティ（「アリス」）から第2パーティ（「ボブ」）へ運ぶこととする。先行する第1トランザクションのロッキングスクリプトで定義されている条件の1つは、通常は、ターゲットトランザクションのアンロッキングスクリプトがアリスの暗号署名を含むことである。署名は、アリスがターゲットトランザクションの部分に署名することによって生成される必要がある。これがどの部分であるかは、ロッキングスクリプトによって柔軟に定義されてもよく、あるいは、使用されているプロトコルに応じて、ノードプロトコルの固有の特徴であってもよい。それでもなお、署名される部分は、通常は、ターゲットトランザクションのその他の部分、例えば、アンロッキングスクリプト自体の一部又は全部、を除く。

【0035】

これは、「可鍛性」の可能性をもたらす。すなわち、マイニング前に、署名されていないターゲットトランザクションの部分は、トランザクションを無効にせずに変更（“malleated”）され得る。可鍛性は、一般的に暗号化で知られている概念であり、それは、通常、メッセージが悪意を持って変更される可能性がありながら依然として本物として受け入れられるという安全上の懸念と見なされている。ブロックチェーンの概念では、可鍛性は、必ずしも問題ではなく、単に、トランザクションの特定の部分がそれを無効にせずに変更され得る興味をそそるアーチファクトとして知られている。可鍛性に関連した如何なる安全上の懸念も、代わりに、プロトコル自体ではなく不適切な実装によって引き起こされる。

【0036】

本明細書で開示されている実施形態は、高速で、安全で、信頼できるペイメントチャネルを容易にするための有用な特徴として可鍛性を任意に用いる。アイデアは、トランザクション内のどの1つ以上の部分が（例えば、E C D S A 署名によって）署名されていないかまたは署名されるべきではないかを識別することである。開示されているスキームは、トランザクションの各入力のアンロッキングスクリプト（例えば、「scriptSig」フィールド）内の如何なるコンテンツも如何なる署名によっても署名されないという事実を利用する。実施形態はまた、トランザクションをそれを無効にせずに変更するための更なる柔軟性を可能にするためにS I G H A S Hフラグを利用してもよい。

【0037】

例は次の通りである。ブロックチェーン上でデータを交換する場合に、一般的な方法の1つは、ハッシュパズルを使用して、データの公開とペイメントの受け取りとが同時に行われるようにすることである。これを回避するために、トランザクションは、ペイメントが2つの条件：i）「データ+ボブの署名」を提供すること、又はii）「アリスの署名+ボブの署名」を提供することのうちのどちらか一方で請求可能であるように、構成され得る。

【0038】

ボブは、データ及び彼の署名を提供することによってファンドを請求し、それをアリスへ送るようトランザクションを構成する。それから、アリスは、データを彼女の署名で置換し、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。代替的に、ボブがアリスの署名を取得し、それによりデータを置換して、ネットワークへブロードキャストする。いずれにしても、データはボブの署名によって署名されたメッセージの部分ではないので、それをアリスの署名で置換することは、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、入力が条件ii）を満足するという一方で、依然として有効である。アリス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しないか、あるいは、署名を提供しない場合には、ボブは、条件i）に基づいて、ファンドを請求するよう元のトランザクションをブロードキャストするという選択肢を依然として有している（これは、ボ

10

20

30

40

50

ブが、サイズが大きいかつ／あるいは独自仕様である可能性があるデータアップロードする必要があるので、それほど望ましくない)。アリスは、承認の要件や割引のインセンティブによって彼女の署名を提供するよう、あるいは、十分に実行されたサービスに対してボブに報酬を与えるよう、促され得る。

【0039】

〔システム概要〕

図1は、ブロックチェーン150を実装する、例となるシステム100を示す。システム100は、パケット交換ネットワーク101、通常は、インターネットなどのワイドエリアインターネットネットワーク、を有する。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内でピア・ツー・ピア(P2P)オーバーレイネットワーク106を形成するよう配置された複数のノード104を有する。各ノード104は、ピアのコンピュータ設備を有し、ノード104の異なる1つは異なるピアに属している。各ノード104は、1つ以上のプロセッサ、例えば、1つ以上の中央演算処理装置(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)を有する処理装置を有する。各ノード104はまた、メモリ、すなわち、1つ以上の非一時的なコンピュータ可読媒体の形を取るコンピュータ読み出し可能なストレージも有する。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、ソリッド・ステート・ドライブ(SSD)、フラッシュメモリ、若しくは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媒体を用いる1つ以上のメモリユニットを有してもよい。

【0040】

ブロックチェーン150は、データのブロック151のチェーンを有し、ブロックチェーン150の各々のコピーは、P2Pネットワーク106内の複数のノードの夫々で保持される。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を有し、この文脈中のトランザクションは、一種のデータ構造を指す。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部分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、通常は、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つの入力及び少なくとも1つの出力を有する。各出力は、出力が暗号でロックされているユーザ103に属するデジタルアセットの分量を表す量を指定する(アンロックされて精算又は使用されるためにそのユーザの署名を必要とする)。各入力は、前のトランザクション152の出力を指し示して、トランザクションをリンクする。

【0041】

ノード104のうちの少なくともいくつかは、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の役割を果たす。ノード104のうち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104Mの役割を果たす。ノード104のうちの少なくともいくつかは、保存ノード104S(「完全コピー」ノードとも時々呼ばれる)の役割を果たし、それらの夫々は、各々のメモリに同じブロックチェーン150の各々のコピーを記憶する。各マイナノード104Mはまた、ブロック151内にマイニングされるのを待っているトランザクション152のプール154を保持する。所与のノード104は、転送ノード104F、マイナ104M、保存ノード104S、又はそれらのうちの2つ又は全ての任意の組み合わせであってよい。

【0042】

所与の、目下のトランザクション152jで、(各)入力は、トランザクションのシーケンスにおいて前のトランザクション152iの出力を参照し、この出力が目下のトランザクション152jで精算又は“使用”(spent)されるべきであることを指定するポイントを有する。一般に、前の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ってよい。前のトランザクション152iは、必ずしも、目下のトランザクション152jが生成されるか、又はネットワーク106へ送信され

る時点に存在している必要はないが、前のトランザクション152 i は、目下のトランザクション152 j が有効であるために存在し妥当性確認される必要がある。従って、本願での「前の」(preceding)は、ポインタによってリンクされた論理順序において前にあるもの(predecessor)を指し、必ずしも時間順序における生成又は送信の時点ではなく、従って、それは、トランザクション152 i、152 j が順不同で生成又は送信されることを必ずしも排除するわけではない(孤立トランザクションに関する以下の説明を参照)。前のトランザクション152 i は、先行(antecedent又はpredecessor)トランザクションと同様に呼ばれることがある。

【0043】

目下のトランザクション152 j の入力または、前のトランザクション152 i の出力がロックされるユーザ103 a の署名も有する。つまり、目下のトランザクション152 j の出力は、新しいユーザ103 b に暗号でロックされ得る。目下のトランザクション152 j は、このようにして、目下のトランザクション152 j の出力で定義されている新しいユーザ103 b へ、前のトランザクション152 i の入力または定義されている量を転送し得る。いくつかの場合に、トランザクション152 は、複数のユーザ(そのうちの1ユーザが、チェンジ(change)を与えるために元のユーザ103 a であってよい)の間で入力量を分割するために複数の出力を有してもよい。いくつかの場合に、トランザクションはまた、1つ以上の前のトランザクションの複数の出力からの両方をひとまとめにして、現在のトランザクションの1つ以上の出力に再分配するために複数の入力を有することができる。

【0044】

上記は、未使用トランザクション出力(UTXO)タイププロトコル(出力がUTXOと呼ばれる)とも時々呼ばれる「出力ベース」のトランザクションプロトコルと呼ばれることがある。ユーザの総合収支(total balance)は、ブロックチェーンに保存されているいずれか1つの番号では定義されず、代わりに、ユーザは、ブロックチェーン150内の多種多様なトランザクション152にわたって散らばっているそのユーザの全てのUTXOの値を照合するよう特別の“ウォレット”105を必要とする。

【0045】

トランザクションプロトコルの代替のタイプは、アカウントベースのトランザクションモデルの部分として、「アカウントベース」のプロトコルと呼ばれることがある。アカウントベースの場合に、各トランザクションは、過去のトランザクションのシーケンスにおいて前のトランザクションのUTXOを参照することによって、転送されるべき量を定義するのではなく、むしろ、絶対的なアカウント残高を参照することによって定義する。全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のマイナによって保存され、常に更新される。本開示は、アカウントベースではなく、出力ベースのモデルに関係がある。

【0046】

いずれのタイプのトランザクションプロトコルによっても、ユーザ103が新しいトランザクションを成立させたい場合に、彼/彼女は、その新しいトランザクションを彼/彼女のコンピュータ端末102からP2Pネットワーク106のノード104(今日、通常は、サーバ又はデータセンタであるが、原理上、他のユーザ端末であってもよい)の1つへ送る。このノード104は、トランザクションが有効であるかどうかを、ノード104の夫々で適用されるノードプロトコルに従ってチェックする。ノードプロトコルの詳細は、問題となっているブロックチェーン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、一緒にトランザクションモデル全体を形成する。ノードプロトコルは、通常は、新しいトランザクション152 j 内の暗号署名が、トランザクション152の順序づけられたシーケンスにおける前のトランザクション152 i 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ように、ノード104に求める。出力ベースの場合に、これは、新しいトランザクション152 j の入力に含まれているユーザの暗号署名が、新しいトランザクションが使用する前のトランザクション152 i の出力で定義されている条件と一致することをチェックすることを有してもよい。この条件は、通常は、新し

いトランザクション152jの入力における暗号署名が、新しいトランザクションの入力が指し示す前のトランザクション152iの出力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、条件は、入力及び／又は出力に含まれているカスタムスクリプトによって少なくとも部分的に定義されてもよい。代替的に、それは、単に、ノードプロトコルのみによって確定されても、あるいは、これらの組み合わせによってもよい。いずれにしても、新しいトランザクション152jが有効である場合には、現在のノードはそれをP2Pネットワーク106内のノード104のうちの1つ以上の他のノードへ転送する。これらのノード104のうち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ながら、転送ノード104Fとしても働くので、新しいトランザクション152jを1つ以上の更なるノード104へ転送し、以降同様である。このようにして、新しいトランザクションは、ノード104のネットワークにわたって伝播される。

【0047】

出力ベースのモデルでは、所与の出力（例えば、UTXO）が使用されるかどうかの定義は、それがノードプロトコルに従って他の以降のトランザクション152jの入力によってまだ有効に精算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他の条件は、使用又は精算しようと試みている前のトランザクション152iの出力が他の有効なトランザクションによってまだ使用／精算されていないことである。先と同じく、有効でない場合には、トランザクション152jは、ブロックチェーンにおいて伝搬又は記録されない。これは、使用者（spender）が同じトランザクションの出力を1回よりも多く使用しようとする二重支払いを防ぐ。

【0048】

妥当性確認に加えて、ノード104Mの少なくともいくつかはまた、マイニングとして知られているプロセスでトランザクションのブロックを生成する最初のものであるよう競争する。これは「プルーフ・オブ・ワーク」によって裏打ちされる。マイニングノード104Mで、新しいトランザクションは、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加えられる。マイナは、次いで、暗号パズルを解こうと試みることによって、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を組み立てるよう競争する。通常、これは、ノンスがトランザクションのプール154と連結されてハッシュ化される場合に、ハッシュの出力が所定の条件を満足するように、「ノンス」（nonce）値を探すことを有する。例えば、所定の条件は、ハッシュの出力が特定の予め定義された数の先行ゼロ（leading zeros）を有していることであってよい。ハッシュ関数の特性は、それがその入力に関して予測不能な出力を有していることである。従って、この探索は、ブルート・フォース（brute force）によってのみ実行可能であるから、パズルを解こうとしている各ノード104Mでかなりの量の処理リソースを消費する。

【0049】

パズルを解く最初のマイナノード104Mは、このことをネットワーク106にアナウンスし、解をプルーフとして供給する。解は、次いで、ネットワーク内の他のノード104によって容易にチェックされ得る（ハッシュに対する解を与えられると、それがハッシュの出力に条件を満足させることをチェック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、次いで、保存ノード104Sとして動作するノード104のうちの少なくともいくつかによって、各そのようなノードで勝者のアナウンスした解をチェックしたことに基づいて、ブロックチェーン150で新しいブロック151として記録されることになる。ブロックポインタ155も新しいブロック151nに割り当てられ、チェーン内の前に生成されたブロック151n-1を指し示す。プルーフ・オブ・ワークは、新しいブロック151を生成するのに多大な労力を要するので、二重支払いのリスクを減らすのに役立ち、そして、二重支払いを含む如何なるブロックも他のノード104によって拒絶される可能性が高いということで、マイニングノード104Mは、二重支払いが彼らのブロックに含まれることを許さないよう動機付けられる。生成され

10

20

30

40

50

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内の保存ノード104Sの夫々で認識されて保持されるので、変更され得ない。ブロックポインタ155も、ブロック151に順次的な順序を課す。トランザクション152は、P2Pネットワーク106内の各保存ノード104Sで順序づけられたブロックに記録されるので、これは、従って、トランザクションの不変のパブリック台帳を提供する。

【0050】

如何なる所与の時点でもパズルを解くよう競争する異なるマイナ104Mは、いつそれが解を探し始めたかに応じて、如何なる所与の時点での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そうしている可能性がある点に留意されたい。各々のパズルを解く者は誰でも、どのトランザクションが次の新しいブロック151nに含まれるかを最初に定義し、マイニングされていないトランザクションの現在のプール154は更新される。マイナ104Mは次いで、新たに定義された未処理のプール154からブロックを生成するよう競争を続け、以降同様である。プロトコルはまた、発生する可能性がある如何なる「フォーク」(fork)も解決するためにも存在する。フォークは、2つのマイナ104Mが互いに非常に短時間にパズルを解き、それにより、ブロックチェーンの競合する見解が伝播されることになる場合である。要するに、フォークのどちらの先が最も長いとしても、確定的なブロックチェーン150になる。

【0051】

ほとんどのブロックチェーンで、勝者マイナ104Mは、(1ユーザから他のユーザへある量のデジタルアセットを転送する通常のトランザクションとは対照的に)どこからともなく、新しいデジタルアセットを生成する特別な種類の新しいトランザクションを自動的に見返りに与えられる。従って、勝者ノードは、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。この特別なタイプのトランザクションは、時々「ジェネレーション」トランザクションと呼ばれる。それは、自動的に、新しいブロック151nの部分形成する。この見返りは、マイナ104Mがブルーフ・オブ・ワーク競争に参加する動機を与える。しばしば、通常の(非ジェネレーション)トランザクション152も、その出力の1つで追加トランザクションフィーを指定して、そのトランザクションが含まれたブロック151nを生成した勝者マイナ104Mに更に見返りを与える。

【0052】

マイニングに関与する計算リソースにより、通常、マイナノード104Mの少なくとも夫々は、1つ以上の物理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を取る。各転送ノード104F及び／又は保存ノード104Sも、サーバ又はデータセンタの形を取る。しかし、原則として、如何なる所与のノード104も、ユーザ端末又は一緒にネットワーク化されたユーザ端末のグループの形をとってもよい。

【0053】

各ノード104のメモリは、その各々の1つ以上の役割を実行しかつ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の処理装置で実行されるよう構成されたソフトウェアを記憶している。本明細書でノード104に起因する如何なる動作も、各々のコンピュータ設備の処理装置でソフトウェアが実行されることによって実行されてよいことが理解される。また、本明細書で使用されている「ブロックチェーン」という用語は、その種類の技術全般を指す一般名称であり、如何なる特定の独自仕様のブロックチェーン、プロトコル、又はサービスにも限定されない。

【0054】

ネットワーク101には、消費ユーザの役割を担う複数のパーティ103の夫々のコンピュータ機器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プレイヤー及び受取人として働くが、必ずしも、他のパーティに成り代わってトランザクションをマイニング又は伝播することに参加するわけではない。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及びそれらの各々の機器102は、実例の目的で示されている。すなわち、第1パーティ103a及び彼／彼女の各々のコンピュータ機器102a、並びに第2パーティ103及び彼／彼女の各々のコンピュー

タ機器 102b である。多数のより多くのそのようなパーティ 103 及びそれらの各々のコンピュータ機器 102 が存在してシステムに参加してもよいが、便宜上それらは表されていないことが理解されるだろう。各パーティ 103 は、個人又は組織であってよい。純粋に実例として、第 1 パーティ 103a は、本明細書ではアリス (Alice) と呼ばれ、第 2 パーティ 103b は、ボブ (Bob) と呼ばれるが、これは限定ではなく、本明細書でのアリス又はボブへの如何なる言及も、「第 1 パーティ」及び「第 2 パーティ」で夫々置換されてもよいことが理解されるだろう。

【0055】

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、を有する各々の処理装置を有する。各パーティ 103 のコンピュータ機器 102 は、メモリ、すなわち、1 つ以上の非一時的なコンピュータ可読媒体の形を取るコンピュータ読み出し可能なストレージ、を更に有する。このメモリは、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、SSD、フラッシュメモリ、若しくは 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媒体、を用いる 1 つ以上のメモリユニットを有してもよい。各パーティ 103 のコンピュータ機器 102 におけるメモリは、処理装置で実行されるよう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 の各々のインスタンスを有するソフトウェアを記憶している。本明細書で所与のパーティ 103 に起因する如何なる動作も、各々のコンピュータ機器 102 の処理装置で実行されるソフトウェアを用いて実行されてもよいことが理解されるだろう。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、デスクトップ若しく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などのウェアラブルデバイス、を有する。所与のパーティ 103 のコンピュータ機器 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などの、1 つ以上の他のネットワーク化されたリソースを有してもよい。

【0056】

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可読記憶媒体でいずれかの所与のパーティ 103 のコンピュータ機器 102 へ供給されてよく、例えば、サーバからダウンロードされるか、あるいは、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（登録商標）ディスク若しくはテープ、CD 若しくは DVD ROM などの光ディスク、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デバイスで供給される。

【0057】

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」機能を有する。これは、2 つの主な機能性を有している。それらのうちの 1 つは、各々のユーザパーティ 103 が、ノード 104 のネットワークにわたって伝播され、それによってブロックチェーン 150 に含まれるようトランザクション 152 を生成、署名し、送信することを可能にすることである。他は、彼又は彼女が現在所有しているデジタルアセットの量を各々のパーティに折り返し報告することである。出力ベースのシステムでは、この第 2 の機能性は、問題となっているパーティに属するブロックチェーン 150 にわたって散らばった様々なトランザクション 152 の出力で定義されている量を照合することを有する。

【0058】

各コンピュータ機器 102 で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 のうちの少なくとも 1 つに動作可能に結合される。これは、クライアント 105 のウォレット機能がトランザクションをネットワーク 106 へ送ることを可能にする。クライアント 105 は、各々のパーティ 103 が受け手である如何なるトランザクションについてもブロックチェーン 150 にクエリする（あるいは、実施形態において、ブロックチェーン 150 は、その公共の可視性を通じて部分的に取引への信頼を提供する公共施設であるため、実際に、ブロックチェーン 150

10

20

30

40

50

内の他のパーティのトランザクションを検査する) ために、保存ノード 104S のうちの 1 つ、いくつか、又は全てに連絡することもできる。各コンピュータ機器 102 で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プロトコル 152 を定式化して送信するよう構成される。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 をネットワーク 106 にわたって伝播するためにそれらを転送する転送ノード 104F の場合に、トランザクション 152 を妥当性確認するよう構成されたソフトウェアを実行する。トランザクションプロトコル及びノードプロトコルは、互いに対応しており、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同調して、一緒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 における全てのトランザクション 152 に対して使用される (なお、トランザクションプロトコルは、その中で異なったサブタイプのトランザクションを許し得る)。同じノードプロトコルが、ネットワーク 106 内の全てのノード 104 によって使用される (なお、それは、異なったサブタイプのトランザクションを、そのサブタイプに対して定義された規則に従って異なるように扱ってもよく、また、異なるノードは、異なる役割を果たし、従って、プロトコルの異なった対応する態様を実装し得る)。

【0059】

述べられているように、ブロックチェーン 150 は、ブロック 151 のチェーンを有し、各ブロック 151 は、上述されたようにプルーフ・オブ・ワークプロセスによって生成された 1 つ以上のトランザクション 152 の組を有する。各ブロック 151 はまた、ブロック 151 に順次的な順序を定義するために、チェーン内の前に生成されたブロック 151 を指し示すブロックポインタ 155 も有する。ブロックチェーン 150 はまた、プルーフ・オブ・ワークプロセスによって新しいブロックに含まれるのを待っている有効なトランザクションのプール 154 も有する。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に対するポインタを有する (トランザクション 152 のシーケンスは枝分かれすることを許されている点に留意されたい)。ブロック 151 のチェーンは、チェーン内の最初のブロックであったジェネシスブロック (Gb) 153 にまでずっとさかのぼる。チェーン 150 内の初期にある 1 つ以上のオリジナルのトランザクション 152 は、先行するトランザクションよりむしろ、ジェネシスブロック 153 を指し示していた。

【0060】

所与のパーティ 103、例えば、アリスが、新しいトランザクション 152j をブロックチェーン 150 に含まれるよう送信したいと望む場合に、彼女は、関連するトランザクションプロトコルに従って (例えば、彼女の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を用いて) 新しいトランザクションを定式化する。次いで、彼女は、トランザクション 152 をクライアントアプリケーション 105 から、彼女が接続されている 1 つ以上の転送ノード 104F へ送る。例えば、これは、アリスのコンピュータ 102 へ最も近く又は最も良く接続されている転送ノード 104F であってもよい。いずれかの所与のノード 104 が新しいトランザクション 152j を受け取る場合に、それは、その新しいトランザクション 152j をノードプロトコル及びその各々の役割に従って処理する。これは、最初に、新たに受け取ら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足するかどうかをチェックすることを有する。この例は、後で更に詳細に説明される。いくつかのトランザクションプロトコルで、有効性の条件は、トランザクション 152 に含まれているスクリプトによってトランザクションごとに設定可能であってもよい。代替的に、条件は、単に、ノードプロトコルのビルトイン機構であっても、あるいは、スクリプトとノードプロトコルとの組み合わせによって定義されてもよい。

【0061】

新たに受け取られたトランザクション 152j が、有効であると見なされるためのテストを通過する、という条件で (すなわち、それが「妥当性確認」される、という条件で)、トランザクション 152j を受け取る如何なる保存ノード 104S も、新しい妥当性確認されたトランザクション 152 を、そのノード 104S で保持されているブロックチェ

10

20

30

40

50

ーン150のコピーで、プール154に加える。更に、トランザクション152jを受け取った如何なる転送ノード104Fも、妥当性確認されたトランザクション152を、P2Pネットワーク106内の1つ以上の他のノード104へと前方に伝播する。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し、これは、トランザクション152jがP2Pネットワーク106の全体にわたって直ぐに伝播されることになることを意味する。

【0062】

1つ以上の保存ノード104Sで保持されているブロックチェーン150のコピーでプール154に入れられると、次いで、マイナノード104Mは、新しいトランザクション152を含むプール154の最新バージョンに関してプルーフ・オブ・ワークパズルを解くよう競争し始める（他のマイナ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こうとしている可能性があるが、最初にそこに着いた者は、どこで次の新しいブロック151が終了し、新しいプールが開始するかを定義し、最終的に、誰かが、アリスのトランザクション152jを含むプール154の一部についてパズルを解く）。プルーフ・オブ・ワークが、新しいトランザクション152jを含むプール154について行われると、それは不変に、ブロックチェーン150内のブロック151のうちの1つの部分となる。各トランザクション152は、先のトランザクションへのポインタを有するので、トランザクションの順も不変に記録される。

【0063】

図2は、例となるトランザクションプロトコルを表す。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」と略される）は、ブロックチェーン150の基本データ構造である（各ブロック151は1つ以上のトランザクション152を含む）。以下は、出力ベース又は“UTXOベース”のプロトコルを参照することによって記載される。しかし、これは、全ての可能な実施形態に対する限定ではない。

【0064】

UTXOベースのモデルでは、各トランザクション（「Tx」）152は、1つ以上の入力202及び1つ以上の出力203を含むデータ構造を有する。各出力203は、未使用のトランザクション出力（UTXO）を有してもよく、UTXOは、（UTXOがまだ精算されていない場合に）他の新しいトランザクションの入力202のためのソースとして使用可能である。UTXOは、デジタルアセット（価値の蓄蔵）の量を指定する。それはまた、数ある情報の中でもとりわけ、それが伝来したトランザクションのトランザクションIDを含んでもよい。トランザクションデータ構造はまた、ヘッダ201を有してもよく、ヘッダ201は、入力フィールド202及び出力フィールド203のサイズのインジケータを有してもよい。ヘッダ201はまた、トランザクションのIDを含んでもよい。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（トランザクションID自体を除く）のハッシュであり、マイナ104Mにサブミットされた生の（raw）トランザクション152のヘッダ201に格納される。

【0065】

例えば、アリス103aは、問題となっているデジタルアセットのある量をボブ103bに転送するトランザクション152jを生成したいと望む。図2で、アリスの新しいトランザクション152jは、「Tx₁」とラベル付けされている。それは、順番において前のトランザクション152iの出力203でアリスにロックされているデジタルアセットの量を取り、これの少なくともいくらかをボブへ転送する。前のトランザクション152iは、図2では「Tx₀」とラベル付けされている。Tx₀及びTx₁は、単に任意のラベルである。それらは必ずしも、Tx₀がブロックチェーン150内の最初のトランザクションであることも、Tx₁がプール154内の直ぐ次のトランザクションであることも意味しない。Tx₁は、アリスにロックされている未使用出力203を依然として有しているいずれかの前の（すなわち、先行する）トランザクションを指し示し得る。

【0066】

前のトランザクションTx₀は、既に妥当性確認をされて、アリスが新しいトランザク

10

20

30

40

50

ション $T x_1$ を生成する時点には、あるいは、少なくとも、彼女がそれをネットワーク 106 へ送る時点までには、ブロックチェーン 150 に含まれていることができる。それは既に、その時点でブロック 151 のうちの 1 つに含まれていてもよく、あるいは、それは依然としてプール 154 で待機していてもよく、その場合に、それは、新しいブロック 151 に間もなく含まれることになる。代替的に、 $T x_0$ 及び $T x_1$ は生成されて、一緒にネットワーク 106 へ送信されてもよく、あるいは、ノードプロトコルが「孤立」(orphan) トランザクションをバッファすることを有する場合には、 $T x_0$ は $T x_1$ の後に送信されてもよい。トランザクションのシーケンスに関連して本明細書で使用されている「前の」(preceding) 及び「後の」(subsequent) という用語は、トランザクションで指定されたトランザクションポイントによって定義されているシーケンス内のトランザクションの順序を指す(どのトランザクションは、どの他のトランザクションを指し示すか、以降同様)。それらは、同様に、「先行」(predecessor) 及び「後続」(successor)、又は「先祖」(antecedent) 及び「子孫」(descendant)、「親」(parent) 及び「子」(child)、等で置換され得る。それは必ずしも、それらが生成され、ネットワーク 106 へ送信され、あるいは、いずれかの所与のノード 104 に到着する順序を暗示するわけではない。それでもなお、前のトランザクション(先行するトランザクション又は「親」)を指し示す後続のトランザクション(続くトランザクション又は「子」)は、親トランザクションが妥当性確認されない限りは、妥当性確認されない。その親より前にノード 104 に到着する子は、孤立と見なされる。それは、ノードプロトコル及び／又はマイナ挙動に応じて、捨てられるか、あるいは、親を待つ一定の時間の間バッファされ得る。

【0067】

前のトランザクション $T x_0$ の 1 つ以上の出力 203 のうちの 1 つは、ここでは $U T X O_0$ とラベル付けされている特定の $U T X O$ を有する。各 $U T X O$ は、その $U T X O$ によって表されるデジタルアセットの量を指定する値と、後続のトランザクションが妥当性確認されるために、従って、 $U T X O$ が成功裏に精算されるためにその後続のトランザクションの入力 202 内のアンロッキングスクリプトによって満足されるべき条件を定義するロッキングスクリプトとを有する。通常、ロッキングスクリプトは、その量を特定のパーティ(それが含まれるトランザクションの受取人)にロックする。すなわち、ロッキングスクリプトは、アンロッキング条件を定義し、通常は、後続のトランザクションの入力内のアンロッキングスクリプトが、前のトランザクションがロックされているパーティの暗号署名を含む、という条件を有する。

【0068】

ロッキングスクリプト(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言語で記述されたコード片である。そのような言語の特定の例は、「スクリプト」(Script)(大文字 S)と呼ばれる。ロッキングスクリプトは、どのような情報がトランザクション出力 203 を使用するために必要とされるか、例えば、アリスの署名の要件、を指定する。アンロッキングスクリプトは、トランザクションの出力に現れる。アンロッキングスクリプト(別名、`scriptSig`)は、ロッキングスクリプト基準を満足するために必要な情報を供給するドメイン固有言語で記述されたコード片である。例えば、それは、ボブの署名を含んでもよい。アンロッキングスクリプトは、トランザクションの入力 202 に現れる。

【0069】

故に、表されている例では、 $T x_0$ の出力内の $U T X O_0$ は、 $U T X O_0$ が精算されるために(厳密には、 $U T X O_0$ を精算しようと試みる後続のトランザクションが有効であるために)、アリスの署名 $S i g P_A$ を必要とするロッキングスクリプト $[C h e c k s i g P_A]$ を有する。 $[C h e c k s i g P_A]$ は、アリスのパブリック-プライベートキーペアからのパブリックキー P_A を含む。 $T x_1$ の入力 202 は、(例えば、実施形態において、トランザクション $T x_0$ の全体のハッシュであるそのトランザクション $I D T x I D_0$ を用いて) $T x_1$ を指し示すポイントを含む。 $T x_1$ の入力 202 は、 $T x_0$ 内の $U T X O_0$ を識別するインデックスを、 $T x_0$ の如何なる他の起こり得る出力の中から

もそれを識別するために有する。Tx₁の入力202は、アリスがキーペアからの彼女のプライベートキーをデータ（時々、暗号法で「メッセージ」と呼ばれる）の予め定義された部分に適用することによって生成されたアリスの暗号署名を含むアンロックングスクリプト<Sig PA>を更に有する。どのようなデータ（又は「メッセージ」）が有効な署名をもたらすようアリスによって署名される必要があるかは、ロックングスクリプトによって、又はノードプロトコルによって、又はそれらの組み合わせによって定義されてよい。

【0070】

新しいトランザクションTx₁がノード104に到着する場合に、ノードはノードプロトコルを適用する。これは、アンロックングスクリプトが、ロックングスクリプトで定義されている条件（この条件は1つ以上の基準を含んでもよい）を満足するかどうかをチェックするために、ロックングスクリプト及びアンロックングスクリプトを一緒に実行することを含む。実施形態において、これは、2つのスクリプトを連結することを含む：

<Sig PA><PA>||[Checksig PA]

ここで、「||」は、連結を表し、「<...>」は、スタックにデータを置くことを意味し、「[...]」は、アンロックングスクリプトによって構成された関数（本例では、スタックベースの言語）である。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、順々に実行されてもよい。いずれの場合にも、一緒に実行される場合に、スクリプトは、Tx₁の入力内のロックングスクリプトが、データの期待された部分に署名するアリスの署名を含むことを認証するために、Tx₀の出力内のロックングスクリプトに含まれているアリスのパブリックキーPAを使用する。データ自体（「メッセージ」）の期待された部分はまた、この認証を実行するためにTx₀にも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（故に、データの署名された部分を平文で指定する別個の要素は、それが既に本質的に存在するということで、含まれる必要がある）。

【0071】

パブリック-プライベート暗号法による認証の詳細は、当業者によく知られている。基本的に、アリスが、彼女のプライベートキー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ている場合に、アリスのパブリックキー及び平文のメッセージ（暗号化されていないメッセージ）を考えると、ノード104などの他のエンティティは、メッセージの暗号化されたバージョンがアリスによって署名されているべきであることを認証することができる。署名することは、通常は、メッセージをハッシュ化し、ハッシュに署名し、これを署名としてメッセージの平文バージョンにタグ付けすることを有するので、パブリックキーのいずれのホルダも署名を認証することが可能となる。従って、特定のデータ片又はトランザクションの部分に署名すること等への本明細書中の如何なる言及も、実施形態において、その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点に留意されたい。

【0072】

Tx₁におけるアンロックングスクリプトが、Tx₀のロックングスクリプトで指定されている1つ以上の条件を満足する場合に（故に、示されている例では、アリスの署名がTx₁で与えられて、認証される場合に）、ノード104は、Tx₁を有効であると見なす。それが保存ノード104Sである場合には、これは、保存ノード104Sが、Tx₁を、プルーフ・オブ・ワークを待っているトランザクションのプール154に加えることを意味する。それが転送ノード104Fである場合に、転送ノード104Fは、トランザクションTx₁をネットワーク106内の1つ以上のノード104へ転送して、それがネットワークにわたって伝播されるようにする。Tx₁が妥当性確認されて、ブロックチェーン150に含まれると、これにより、Tx₀からのUTXO₀は使用済みとして定義される。Tx₁は、それが未使用トランザクション出力203として使用される場合にのみ有効であることができる点に留意されたい。他のトランザクション152によって既に使用されている出力を使用しようと試みる場合には、Tx₁は、他の全ての条件が満足され

10

20

30

40

50

る場合でさえ無効となる。従って、ノード104はまた、前のトランザクションTx₀における参照されたUTXOが既に使用されているか（他の有効なトランザクションへ有効な入力を既に形成しているか）どうかもチェックする必要がある。これは、ブロックチェーン150が予め定義された順序をトランザクション152に課することが重要である1つの理由である。特に、所与のノード104は、どのトランザクション152内のどのUTXO203が使用されているかをマークする別個のデータベースを保持することができるが、最終的に、UTXOが使用されているかどうかを定義するものは、それがブロックチェーン150内の他の有効なトランザクションへの有効な入力を既に形成しているかどうかである。

【0073】

UTXOベースのトランザクションモデルでは、所与のUTXOは、全体として使用される必要がある点に留意されたい。それは、UTXOで定義されている量の一部分を、他の部分が使用されている間に使用されるものとして「残しておく」ことはできない。しかし、UTXOからの量は、次のトランザクションの複数の出力間で分割可能である。例えば、Tx₀内のUTXO₀で定義されている量は、Tx₁内の複数のUTXOの間で分割され得る。従って、アリスが、UTXO₀で定義されている量の全てをボブに与えたくない場合には、彼女は、残りを使用してTx₁の第2出力で彼女自身にチェンジ（change）を与えるか、あるいは、別のパーティに支払うことができる。

【0074】

実際に、アリスは、通常、勝者マイナのためのフィーを含めることも必要になる。これは、今日、ジェネレーショントランザクションの見返りが、通常、マイニングを動機付けるのに十分でないからである。アリスがマイナのためのフィーを含めない場合には、Tx₀は、マイナノード104Mによって拒絶される可能性があり、従って、技術的に有効だとしても、それは依然として伝播されず、ブロックチェーン150に含まれないことになる（マイナプロトコルは、マイナ104Mが望まない場合にトランザクション152を受け入れるようマイナ104Mに強制しない）。いくつかのプロトコルで、マイニングフィーは、それ自体の別個の出力203を必要としない（すなわち、別個のUTXOは不要である）。代わりに、入力202によって指し示されている総量と、所与のトランザクション152の出力203で指定されている総量との間の如何なる差も、勝者マイナ104Mに自動的に与えられる。例えば、UTXO₀へのポインタは、Tx₁への唯一の入力であり、Tx₁は、ただ1つの出力UTXO₁しか有していない。UTXO₀で指定されているデジタルアセットの量が、UTXO₁で指定されている量よりも多い場合には、差は勝者マイナ104Mに自動的に行く。代替的に、又は追加的に、しかしながら、マイナフィーがトランザクション152のUTXO203のうちのそれ自身の1つで明示的に指定され得ることは必ずしも除外されない。

【0075】

所与のトランザクション152の全ての出力203で指定されている総量が、その全ての入力202によって指し示されている総量よりも多い場合には、これは、ほとんどのトランザクションモデルでの無効性のもう1つの基準である。従って、そのようなトランザクションは、伝播も、ブロック151内にマイニングもされない。

【0076】

アリス及びボブのデジタルアセットは、ブロックチェーン150内のどこでも、どのトランザクション152でも彼らにロックされている未使用UTXOから成る。従って、通常、所与のパーティ103のアセットは、ブロックチェーン150にわたって様々なトランザクション152のUTXOにわたって散らばっている。所与のパーティ103の合計残高を定義する1つの番号は、ブロックチェーン150のどこにも保存されていない。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は、各々のパーティにロックされており、他の以降のトランザクションでまだ使用されていない全ての様々なUTXOの値と一緒に照合することである。それは、保存ノード104Sのいずれか、例えば、各々のパーティのコンピュータ機器102へ最も近く又は最も良く接続されている保

10

20

30

40

50

存ノード104S、で保存されているブロックチェーン150のコピーをクエリすることによって、これを行うことができる。

【0077】

スクリプトコードは、しばしば、概略的に（すなわち、厳密な言語でなく）表現される点に留意されたい。例えば、 $[Checksig\ P_A] = OP_DUP\ OP_HASH\ 160 < H(P_A) > OP_EQUAL\ VERIFY\ OP_CHECKSIG$ を意味するよう $[Checksig\ P_A]$ が記述され得る。「 $OP_...$ 」は、スクリプト言語の特定のオペコードを指す。 $OP_CHECKSIG$ （「 $Checksig$ 」とも呼ばれる）は、2つの入力（署名及びパブリックキー）を取り、楕円曲線デジタル署名アルゴリズム（Elliptic Curve Digital Signature Algorithm, ECDSA）を用いて署名の有効性を検証するスクリプトオペコードである。ランタイム時に、署名（「 sig 」）の如何なる発生も、スクリプトから除かれるが、ハッシュパズルなどの追加の要件は、「 sig 」入力によって検証されたトランザクションにとどまる。他の例として、 OP_RETURN は、トランザクション内のメタデータを保存し、それによって、ブロックチェーン150に不変にメタデータを記録することができるトランザクションの使用不可能な出力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保存することが望まれる文書を有してもよい。

【0078】

署名 P_A 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 $secp256k1$ を用いたECDSAに基づく。デジタル署名は、特定のデータ片に署名する。実施形態において、所与のトランザクションについては、署名は、トランザクション入力の部分と、トランザクション出力の全て又は部分とに署名することになる。それが署名する出力の特定の部分は、 $SIGHASH$ フラグに依存する。 $SIGHASH$ フラグは、どの出力が署名されるかを選択するよう署名の最後に含まれ（て、署名する時点で修正され）る4バイトコードである。

【0079】

ロッキングスクリプトは、各々のトランザクションがロックされるパーティのパブリックキーをそれが有するという事実を参照して、時々「 $scriptPubKey$ 」と呼ばれる。アンロッキングスクリプトは、それが対応する署名を供給するという事実を参照して、時々「 $scriptSig$ 」と呼ばれる。しかし、より一般的に、 $UTXO$ が精算されるための条件が、署名を認証することを有することは、ブロックチェーン150の全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、スクリプト言語は、いずれかの1つ以上の条件を定義するために使用され得る。従って、より一般的な用語「ロッキングスクリプト」及び「アンロッキングスクリプト」が好まれ得る。

【0080】

図3は、ブロックチェーン150を実装するシステム100を示す。システム100は、追加の通信機能性が含まれることを除いて、図1に関して記載されているものと略同じである。アリス及びボブのコンピュータ機器102a、102bの夫々でのクライアントアプリケーションは、追加の通信機能性を夫々有している。すなわち、それは、アリス103aが（どちらかのパーティ又はサードパーティの扇動で）ボブ103bと別個のサイドチャンネル301を確立することを可能にする。サイドチャンネル301は、P2Pネットワークとは別にデータの交換を可能にする。かような通信は、「オフチェーン」と時々呼ばれる。例えば、これは、パーティの1つがトランザクション152をネットワーク106へ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（まだ）P2Pネットワーク106に公開されないか又はチェーン150にたどり着かない状態で、アリスとボブ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得る。そのようなサイドチャンネル301は、例えば、「ペイメントチャンネル」として時々使用される。

【0081】

サイドチャンネル301は、P2Pオーバーレイネットワーク106と同じパケット交換ネットワーク101を介して確立され得る。代替的に、又は追加的に、サイドチャンネル3

10

20

30

40

50

01は、モバイルセルラーネットワーク、又はローカルワイヤレスネットワークなどのローカルエリアネットワーク、又はアリス及びボブのデバイス102a、102bの間の直接的な有線若しくは無線リンクなどの異なるネットワークを介して確立されてもよい。一般に、本明細書中のどこかで言及されているサイドチャンネル301は、「オフチェーン」で、すなわち、P2Pオーバーレイネットワーク106とは別個に、データを交換する1つ以上のネットワーキング技術又は通信媒体を介したいずれかの1つ以上のリンクを有してもよい。1よりも多いリンクが使用される場合に、オフチェーンリンクのバンドル又は集合は全体として、サイドチャンネル301と呼ばれ得る。従って、アリス及びボブがサイドチャンネル301を介して特定の情報又はデータ片などを交換すると言われる場合に、これは必ずしも、これら全てのデータ片が、厳密に同じリンク又は同じタイプのネットワークを介して送られる必要があることを意味しているわけではないことに留意されたい。

10

【0082】

〔定義例〕

以下は、いくつかの実施で採用され得るいくつかの定義の例である。これらは全てが、全ての可能な実施に対する限定であるわけではなく、特定の可能な実施の理解を助けるためにのみ与えられており、例えば、後述される使用ケースの例のいくつかの可能な実施で用いられ得ることに留意されたい。

【0083】

定義1：トランザクション。トランザクションは、入力及び出力を含むメッセージである。それはまた、プロトコルバージョン番号及び／又はロックタイムを有してもよい。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、後に別途説明される。

20

【0084】

定義2：入力。トランザクションの入力は、順序付きリストを形成する。リスト内の各エントリは、アウトポイント（未使用トランザクション出力に対する識別子）及びscriptSig（アンロッキングスクリプト）を有する。それはまた、シーケンス番号を有してもよい。

【0085】

定義3：出力。トランザクションの出力は、順序付きリストを形成する。リスト内の各エントリは、値（その基本単位でのデジタルアセットの量）及びscriptPubKey（ロッキングスクリプト）を有する。

30

【0086】

定義4：アウトポイント。アウトポイントは、トランザクション識別子TxID及びインデックス番号iによって一意に定義される。それは、未使用トランザクション出力（UTXO）の一意の位置を与える、トランザクションTxIDの出力におけるi番目のエントリを参照する。ここで「未使用」（unspent）という用語は、アウトポイントが如何なる有効な後続トランザクションでも決して現れていないことを意味する。

【0087】

定義5：scriptSig。これは、所与のアウトポイントに対応するUTXOをアンロック又は使用するために必要とされる情報である。標準トランザクションでは、この情報は、通常は、ECDSA署名である。従って、スクリプトは「scriptSig」と呼ばれる。しかし、アウトポイントをアンロックするための必要な情報は、UTXOのロッキング条件を満足する如何なるデータであることもできる。

40

【0088】

定義6：scriptPubKey。これは、特定のUTXOに関連したファンドをロックするスクリプトである。scriptSigがscriptPubKeyに付け加えられて、結合されたスクリプトの実行がTRUEを与える場合かつその場合に限り、ファンドはアンロックされて使用され得る。これが当てはまらない場合には、トランザクションは無効であり拒絶されることになる。それは、一般的に、標準トランザクションのためのECDSAパブリックキーのハッシュ値を含むので、「scriptPubKey」と

50

呼ばれる。

【0089】

次の定義では、1つ以上の入力に署名することが参照される場合に、これは、`scriptSig`部分を除く1つ以上の入力に署名することを意味する（定義2を参照）。

【0090】

定義7：`SIGHASH`フラグ。`ECDSA`署名を与える場合に、次の`SIGHASH`フラグのうちの1つを付け加えることも必要である。

【表1】

フラグ	機能的意味
<code>SIGHASH_ALL</code>	全ての入力及び出力に署名する
<code>SIGHASH_SINGLE</code>	全ての入力及び同じインデックスを有する出力に署名する
<code>SIGHASH_NONE</code>	全ての入力に署名し、出力には署名しない
<code>SIGHASH_ALL ANYONECANPAY</code>	自身の入力及び全ての出力に署名する
<code>SIGHASH_SINGLE ANYONECANPAY</code>	自身の入力及び同じインデックスを有する出力に署名する
<code>SIGHASHU_NONE ANYONECANPAY</code>	自身の入力に署名し、出力には署名しない

【0091】

特徴として可鍛性（malleability）について話題にする場合に、`ECDSA`署名によって署名されていないトランザクション内の情報が期待される。署名されるべきメッセージから除かれ得る入力及び出力は別として、`scriptSig`の内容は常に除かれる。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ているからである。

【0092】

定義8：ブロックチェーンタイムロック。一般に、トランザクションで使用可能なタイムロックには、絶対タイムロック及び相対タイムロックの2タイプがある。絶対タイムロックは、特定の時点を指定し、その時点の後で何かが「有効」と見なされ得る。一方、相対タイムロックは、何かが有効と見なされ得る前に経過しなければならない期間を指定する。いずれかの場合にも、ブロックチェーンタイムロックを使用する場合に、時間のプロキシとして、ブロック高さ（マイニングされるブロックの数）又は経過時間（例えば、UNIX（登録商標）時間）のどちらかを使用することができる。

【0093】

ブロックチェーンタイムロックのもう1つの特性は、それらがどこで現れるか、及びそれらがトランザクションのどの側面に適用されるか、である。この意味でタイムロックにはやはり2つの分類がある。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、及び特定の出力をロックするスクリプトレベルである。それらのタイムロックレベルのどちらも、絶対又は相対タイムロックのどちらかを実装するために使用され得る。以下の表は、これらの特性に基づき生成され得るタイムロックを実装するための4つの可能なメカニズムをまとめたものである。

10

20

30

40

50

【表 2】

		タイプ	
		絶対	相対
トランザクションレベル	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

【0094】

10

定義9：nLocktime：ロックタム（nLocktime）は、ブロックの高さ又はUnix時間での特定の時間を表す非負整数である。それは、指定されたブロック又は指定された時間の後にのみトランザクションが加えられ得るという意味で、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未満であるようセットされる場合には、それはブロック高さで見なされる。それが500,000,000以上であるようセットされる場合には、それはUnix時間の表示と見なされる。それは、1970年1月1日の00:00:00より後の秒数である。

【0095】

例えば、現在の最も高いブロックが3,000,000の高さであり、ロックタイムが4,000,000であるようセットされる場合には、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によって考慮されない。

20

【0096】

定義10：nSequence。シーケンス番号（nSequence）は、メッセージとしてトランザクションのバージョンを示す。トランザクションが変更されると、シーケンス番号は大きくなる。nSequenceの最大値は $2^{32}-1$ であり、一般に、シーケンス番号は、トランザクションが終了していることを示すようデフォルトでこの最大値にセットされる。nSequence値は、トランザクションの入力ごとに定義され、入力によって参照されたUTXOが、それが有効な入力として使用され得る前にブロックに含まれた後の期間を指定する。マイナが同じ入力を有する2つのトランザクションを確認する場合に、マイナは、より大きいシーケンス番号を有しているトランザクションを選択する。しかし、この特徴は、一般的には無効にされている。

30

【0097】

定義11：CheckLockTimeVerify（OP_CLTV）。オペコードOP_CHECKLOCKTIMEVERIFY（OP_CLTV）は、トランザクションの特定のブロックを将来のある特定の時間又はブロック高さにロックするために使用され得る絶対的な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で参照されている現在のUnix時間又はブロック高さが、UTXOが生成されたUnix時間又はブロック高さに、OP_CLTVオペコードの前に指定されているパラメータをプラスしたものによって越えられる場合には、使用中のトランザクションのスクリプト実行は失敗する。

40

【0098】

定義12：CheckSequenceVerify（OP_CSV）。オペコードOP_CHECKSEQUENCEVERIFY（OP_CSV）は、将来の特定の期間又はブロック数の間にトランザクションの特定の出力をロックするために使用される相対的な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に与えられるパラメータが相対時間を表す点で相違する。UTXOがトランザクションで参照されている現在のUnix時間又はブロック高さが、OP_CSVオペコードの前に指定されているパラメータによって越えられる場合に、使用中のトランザクションのスクリプト実行は失敗する。

【0099】

50

定義 13：可鍛性（malleability）：一般に、ブロックチェーントランザクションで可能な可鍛性には2つの広いタイプがある。それらのどちらも、入力で与えられている署名を無効にせずにトランザクションの内容が変更されることを可能にする。

【0100】

両方の場合を説明するために、1つの入力と、その入力にある1つの署名と、1つの出力とを有する最初のトランザクションTxを考える。

【0101】

タイプ1：スクリプトレベルの可鍛性。このタイプの可鍛性は、スクリプトオペコードOP_CHECKSIGでチェックされるべき署名がトランザクション内のいずれの入力のスクリプトフィールドにも署名しないという事実を利用する。この事実は、我々がトランザクションTxに対して署名を生成し、トランザクションTx'がTxと非同一であるように入力スクリプトを変更し、ブロックチェーンコンセンサスルールの下で同じ署名によって署名された有効なトランザクションメッセージと見なされるTx及びTx'の両方を依然として有することを可能にする。

【0102】

タイプ2：入力及び出力レベルの可鍛性。このタイプの可鍛性は、トランザクションで用いられている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つの他のSIGHASHフラグの組み合わせのいずれかを使用する入力署名を有している場合に、入力又は出力のどちらかは、署名を変更する必要なしに、両方のトランザクションが、コンセンサスに従って、有効なトランザクションメッセージと見なされるように、非同一のトランザクションTx'を生成するよう加えられ得る。

【0103】

〔特徴としての可鍛性〕

図4は、現在開示されているスキームの実施形態を実装するクライアントアプリケーション105の実施例を表す。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及びユーザインターフェース（UI）レイヤ402を有する。トランザクションエンジン401は、上述されて更に詳細に簡潔に説明されるスキームに従って、トランザクション152を定式化し、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上で受信及び／又は送信し、かつ／あるいは、P2Pネットワーク106を通じて伝播されるようトランザクションを送信するために、クライアント105の基本的なトランザクション関連機能を実装するよう構成される。いくつかの実施形態で、少なくともボブのクライアント105bのトランザクションエンジン401は、任意に、選択機能の形でアプリケーション機能403を有してもよい。選択機能は、2つ以上の異なったバージョンのターゲットトランザクション（「Tx_p」及び「Tx_p'」）のどちらが、妥当性のためにP2Pネットワーク106を通じて伝播でされて、ブロックチェーン150に記録されるよう、ボブの各々のコンピュータ機器102から送信されるべきであるかに関して選択を可能にする（伝播及び記録それら自体は上記のメカニズムによる）。この送信は、ボブ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へ直接にターゲットトランザクションを送信することを、又はネットワーク106のノード1ー4Fのうちの1つへ転送されるようアリスの機器102a若しくはサードパーティ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有してもよいことにやはり留意されたい。

【0104】

UIレイヤ402は、情報を機器102のユーザ出力手段を介して各々のユーザ103へ出力することと、各々のユーザ103から機器102のユーザ入力手段を介して入力を受け取ることを含め、各々のユーザのコンピュータ機器102のユーザ入力／出力（I／O）手段を介してユーザインター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、視覚出力を供給する1つ以上の表示スクリーン（タッチ若しくは非タッチスクリーン）、オーディオ出力を供給する1つ以上のスピーカ、及び／又は触覚出

力を供給する1つ以上の触覚出力デバイス、等を有してもよい。ユーザ入力手段は、例えば、1つ以上のタッチスクリーン（出力手段のために使用されるものと同じ又は異なる）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つ以上のカーソルベースデバイス、スピーチ若しくは音声入力を受け取る1つ以上のマイクロホン及びは発話音声認識アルゴリズム、手若しくは身体ジェスチャの形で入力を受け取る1つ以上のジェスチャベース入力デバイス、又は1つ以上の機械ボタン、スイッチ、若しくはジョイスティック、等を有してもよい。

【0105】

注釈：ここでは、様々な機能性が、同じクライアントアプリケーション105に含まれているものとして記載されることがあるが、これは必ずしも限定ではなく、代わりに、それらは、例えば、一方が他方にプラグインされていたりする、2つ以上の相異なるアプリケーションのスイートで実装されてもよい。例えば、トランザクションエンジン401の機能性は、UIレイヤ402とは別のアプリケーションで実装されてもよく、あるいは、トランザクションエンジン401等の所与のモジュールの機能性は、1よりも多いアプリケーション間で分割されてもよい。また、記載されている機能性の一部又は全てが、例えば、オペレーティングシステムレイヤで実装され得ることも除外されない。本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等を参照する場合に、これは、単なる例示であって、より一般的には、記載されている機能性は、任意の形式のソフトウェアで実装されてもよいことが理解されるだろう。

【0106】

図5は、ボブの機器102bでクライアントアプリケーション105bのUIレイヤ402によってレンダリングされ得るユーザインターフェース(UI)500の例のモックアップを与える。実施形態で、ユーザインターフェース500は、任意に、2つのオンスクリーンボタン又はメニュー内の2つの異なるオプションのような、ユーザ出力手段を介して2つの相異なったUI要素としてレンダリングされ得る少なくとも2つのユーザ選択的なオプション501、502を有してもよい。ユーザ入力手段は、ユーザ103b（この場合に、ボブ）が、例えば、スクリーン上でUI要素をクリック若しくはタッチすること、又は所望のオプションの名称を発声することによって、オプションから1つを選択することを可能にするよう配置される（本明細書で使用される「手動」との用語は、自動と対照をなすことのみを意味し、1つ以上の手の使用に限定しないことに留意されたい）。オプションをレンダリングし選択する特定手段は物質でないことが理解されるだろう。

【0107】

どのような手段を使用する場合でも、オプションの夫々は、第1及び第2のターゲットトランザクション Tx_p 及び Tx_p' 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とインターフェースするように構成される。すなわち、ボブ103bが第1オプション501を選択する場合、これは、トランザクションエンジン403に、第1バージョンのターゲットトランザクション Tx_p を、ネットワーク106を通じて伝播してブロックチェーン150に登録されるよう送信させる。しかし、ボブ103bが第2オプション502を選択した場合、これは、トランザクションエンジン403に、第2バージョンのターゲットトランザクション Tx_p' を、ネットワーク106を通じて伝播してブロックチェーン150に登録されるよう送信させる。図5に示されるUI500は、図式化されたモックアップにすぎず、実際には、1つ以上の更なるUI要素を有してもよい、簡潔にするために図示されていないことが理解されるだろう。

【0108】

UIオプション501、502に代わるものとして、又はそれらに加えて、選択機能403は、ブロックチェーン150での記録の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 及び Tx_p' の送信の自動選択を実行するよう構成されてもよい。これは、所定のイベントに応じて又は所定のタイムアウトの後で自動的にトリガされてもよい。例えば、イベントYがタイムアウト前に起こる場合には、機能403は、第2バー

ジョン $T x_p$ 'を、ネットワーク106を通じて伝播されるよう自動送信する。しかし、イベントYが起こる前にタイムアウトが経過する場合には、機能403は代わりに、第1バージョン $T x_p$ を自動送信する。あるいは、イベントXが起こる場合には、機能402は、第1バージョン $T x_p$ を、ネットワーク106を通じて伝播されるよう自動送信するが、イベントYが起こる場合には、機能403は代わりに、第2バージョン $T x_p$ 'を自動送信する。実際に、第1及び第2バージョンをネットワーク106へ自動的に送信するための状況は、システム設計者によって事実上どうにでも構成され得る。

【0109】

図6は、本明細書で開示されている実施形態に従う仕様のためのトランザクション152の組を表す。組は、0番目のトランザクション $T x_0$ と、第1トランザクション $T x_i$ （その複数のインスタンス $i = 1, 2, 3, \dots$ が存在する）と、第2トランザクション（その1つ以上のバージョン $T x_p$ 又は $T x_p$ 'が存在する）とを有する。「0番目」、「第1」、及び「第2」は、単に便宜上のラベルであることに留意されたい。それらは必ずしも、それらの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で次々に直ぐに配置されることも、0番目の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で最初のトランザクションであることも示しているわけではない。また、それらのラベルは、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必ずしも何かを示しているわけでもない。それらは、1つのトランザクションの出力が次のトランザクションの入力によって指し示されるという点で、論理的な連続を単に指す。いくつかのシステムでは、親をその子の後にネットワーク106へ送ることが可能であることに留意されたい（この場合に、「孤立した」子は、親が到着するのを待つ間、1つ以上のノード104で一定期間バッファリングされる）。

【0110】

0番目のトランザクション $T x_0$ は、アリス103aにロックされているデジタルアセットの量のソースとして働く点で、現在の目的のためにソーストランザクションとも呼ばれ得る。第1トランザクション $T x_i$ は、ソーストランザクション $T x_0$ からのデジタルアセットの量を条件付きで転送する仲介人として働く点で、現在の目的のために仲介トランザクション又は条件付きトランザクションとも呼ばれる。第2トランザクションは、条件の1つをアンロックしてボブ（あるいは、場合により、ボブが代理を務める受益者）のためのペイメントを運ぶトランザクションであるということで、ターゲットトランザクション又はペイメントトランザクション（従って、添え字「p」）とも呼ばれ得る。実施形態で、ターゲットトランザクションは、少なくとも2つの可能なバージョン、第1バージョン $T x_p$ 及び第2バージョン $T x_p$ 'を有する。これらのトランザクションは夫々、少なくともある時点で存在することができ、アリス（第1パーティ）のコンピュータ機器102a、若しくはボブ（第2パーティ）のコンピュータ機器102b、若しくは、サードパーティの機器（図示せず）、又はそれらの任意の組み合わせのどれかで現れる。2つのバージョン $T x_p$ 及び $T x_p$ 'は、同時に一緒に、又は次々に、又は時間において部分的に重なって、一定期間存在することができる。

【0111】

図6に示されるように、ソーストランザクション $T x_0$ は、デジタルアセットの量を指定する少なくとも1つの出力2030（例えば、 $T x_0$ の出力0）を有し、出力は、更に、個の出力をアリスと103aにロックするロッキングスクリプトを有する。これは、ソーストランザクション $T x_0$ のロッキングスクリプトが、少なくとも1つの条件が満足されることを求めていることを意味する。条件は、出力をアンロックしようとしている（従って、デジタルアセットのその量を精算しようとしている）如何なるトランザクションの入力もそのアンロッキングスクリプトでアリスとの暗号署名（すなわち、アリスのパブリックキーを使用する）を含まなければならない、ことである。この意味で、 $T x_0$ の出力で定義されている量は、アリスによって所有されていると言われることがある。どの先行トランザクションのどの出力を $T x_0$ の入力が指し示しているかは、（それらが $T x_0$ の合計出力をカバーするのに十分である限りは）特に重要ではない。

【0112】

この場合に、ソーストランザクション Tx_0 の出力をアンロックするトランザクションは、第1の、すなわち、仲介トランザクション Tx_i のインスタンスである。従って、 Tx_i は、 Tx_0 の関連出力（表されている例では、 Tx_0 の出力0）へのポインタを有する少なくとも1つの入力2021（例えば、 Tx_i の入力0）を有している。入力は更に、アリスの少なくとも署名を必要とする、その出力のロックングスクリプトで定義されている条件に従って、 Tx_0 の指し示されている出力をアンロックするよう構成されたアンロックングスクリプトを有する。 Tx_0 のロックングスクリプトによってアリスに要求された署名は、 Tx_i のある部分に署名するために必要とされる。いくつかのプロトコルで、署名される必要がある Tx_i の部分は、 Tx_i のアンロックングスクリプトで定義されている設定であることができる。例えば、これは、署名に付け加えられている1バイトであるS I G H A S Hフラグによってセットされてもよく、故に、データに関して、アンロックングスクリプトは、 $\langle Sig \ PA \rangle \langle s i g h a s h f l a g \rangle \langle PA \rangle$ と現れる。代替的に、署名される必要がある部分は、単純に、 Tx_i の固定部分であることができる。いずれにしても、署名される部分は、通常は、アンロックングスクリプト自体を除き、そして、 Tx_i の入力の一部又は全てを除いてもよい。これは、 Tx_i の入力が可鍛性であることを意味する。

10

【0113】

第1の又は仲介トランザクション Tx_i は、少なくとも1つの出力2031（例えば、 Tx_i の出力0であり、やはり出力はU T X Oと呼ばれ得る）を有する。仲介トランザクション Tx_i の出力は、どのパーティにも無条件にはロックされない。 Tx_0 のように、それは、前方へ転送されるべきデジタルアセットの量を指定する少なくとも1つの出力（例えば、 Tx_i の出力0）を有し、出力は更に、その出力をアンロックし、従ってこの量を精算するために必要とされるものを定義するロックングスクリプトを有する。しかし、実施形態において、このロックングスクリプトは、その出力が、少なくともi) 第1条件（「条件1」）及びii) 第2条件（「条件2」）を含む複数の異なった可能な条件うちのいずれか1つに基づきアンロックされることを可能にし得る。

20

【0114】

第2の、ターゲットトランザクション Tx_p / Tx_p' は、 Tx_i の上記の出力（示される例では、 Tx_i の出力0）へのポインタを有し、更には、 Tx_i のその出力を、 Tx_i のロックングスクリプトで定義されている1つ以上の条件のうちの1つを満足することに基づいてアンロックするよう構成されたアンロックングスクリプトを有する少なくとも1つの入力202p（例えば、 Tx_p / Tx_p' の入力0）を有する。例えば、ターゲットトランザクションの第1バージョン Tx_p で、アンロックングスクリプトは、第1条件、条件1を満足するよう構成される。ある時点で、ターゲットトランザクションの第2バージョンは、それから、例えば、書き換え（malleation）によって、 Tx_p から生成されることがある。第2バージョンで、アンロックングスクリプトは、第2条件、条件2を満足するよう構成される。

30

【0115】

第2の、ターゲットトランザクション Tx_p / Tx_p' は、いずれのバージョンでも、ボブに転送すべきデジタルアセットの量と、これをボブにロックするロックングスクリプトとを有する少なくとも1つの出力202p（例えば、 Tx_p / Tx_p' の出力0）を有する（すなわち、それは、アンロックングスクリプトでボブの署名を含む更に先のトランザクションを実行する必要がある）。この意味で、ターゲットトランザクション Tx_p / Tx_p' の出力は、ボブによって所有されていると言われる。この出力はやはりU T X Oと呼ばれ得る。

40

【0116】

実施形態で、第1条件は、 Tx_i をアンロックしようとしているどのトランザクション（実施形態では、ターゲットトランザクションの第1バージョン Tx_p ）のアンロックングスクリプトも、そのアンロックングスクリプトにおいてボブの暗号署名、及び／又はボ

50

ブが供給するか若しくは含める必要があるボブのデータであることができるデータペイロードを含む、ことを求める。データペイロードを含むという要件は、 Tx_i のロッキングスクリプトに含まれているハッシュチャレンジによって課され得る。チャレンジは、(アンロッキングスクリプトとともにノード104で実行される場合に)対応するアンロッキングスクリプトで与えられているデータのハッシュがロッキングスクリプトで与えられているハッシュ値に等しいかどうかをテストするように構成されているスクリプト片とともに、データのハッシュ(データ自体ではない)を有する。署名に対する要件は、例えば、上述された $CheckSig$ によって、課され得る。実施形態で、第1条件は、アリスの署名が Tx_p のアンロッキングスクリプトに含まれることを求めない。ボブによって署名される必要がある Tx_p の部分は、 Tx_p のアンロッキングスクリプトの設定であってよく(例えば、 $SIGHASH$ フラグによって指定される)、あるいは、固定であってもよい。いずれにしても、それは、少なくともアンロッキングスクリプトを除く。従って、 Tx_p のアンロッキングスクリプトは可鍛性である。

【0117】

実施形態で、第2条件は、 Tx_i をアンロックしようとしているどのトランザクション(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')のアンロッキングスクリプトも、そのアンロッキングスクリプトにおいてボブの暗号署名及びアリスの暗号署名を含む、ことを求める。やはり、これは、例えば、 $CheckSig$ によって課され得る。実施形態で、第2条件は、データペイロードが Tx_p' のアンロッキングスクリプトに含まれることを求めない。アリス及びボブによって署名される必要がある Tx_p' の部分は、 Tx_i のアンロッキングスクリプトの設定であってよく(例えば、 $SIGHASH$ フラグによって指定される)、あるいは、固定であってもよい。

【0118】

0番目の(すなわち、ソース)トランザクション Tx_0 は、アリス、ボブ、又はサードパーティによって生成され得る。それは、通常は、 Tx_0 の入力で定義されている量をアリスが取得した前のパーティの署名を必要とする。それは、アリス、ボブ、前のパーティ、又は他のサードパーティによってネットワーク106へ送信され得る。

【0119】

第1の(すなわち、仲介、条件付き)トランザクション Tx_i も、アリス、ボブ、又はサードパーティによって生成され得る。実施形態で、それはアリスの署名を必要とするので、アリスによって生成されてもよい。代替的に、それは、テンプレートとしてボブ又はサードパーティによって生成されて、署名すべきアリスへ送信されてもよい(例えば、サイドチャンネル301上で送信される)。アリスは、次いで、署名されたトランザクションをネットワーク106へ彼女自身が送信することも、あるいは、それをボブ又はサードパーティへ、彼らがネットワーク106へ転送するために送信することも、あるいは、単に彼女の署名を、ボブ又はサードパーティが署名された Tx_i に組み込んでネットワーク106へ転送するために送信することもできる。やはり、 Tx_i をネットワーク106へ送る前のオフチェーンでの如何なるやりとりも、サイドチャンネル301上で実行されてよい。

【0120】

第2の(すなわち、ターゲット又はペイメント)トランザクションのどちらのバージョン Tx_p/Tx_p' も、アリス、ボブ、又はサードパーティによって生成され得る。第1バージョンはボブの署名及び/又はデータを必要とするということで、それはボブによって生成されてもよい。代替的に、それは、テンプレートとしてアリス又はサードパーティによって生成され、それからボブへ、署名してデータを加えるために送信されてもよい(例えば、サイドチャンネル301上でボブへ送信される)。ボブは、次いで、署名されたトランザクションをネットワーク106へ彼自身が送信することも、あるいは、それをアリス又はサードパーティへ、彼らがネットワーク106へ転送するために送信することも、あるいは、単に彼の署名及びデータを、アリス又はサードパーティが署名された Tx_p に組み込んでネットワークへ転送するために送信することもできる。実施形態で、第2バージョンはボブ及びアリスの両方の署名を必要とする。従って、それは、テンプレートとして

アリス又はボブによって生成され、他方へ、彼らの署名を加えるために、例えば、やはりサイドチャンネル301上で、テンプレートとして送られてもよい。代替的に、それは、テンプレートとしてサードパーティによって生成され、それからアリスへ送信されてもよく、アリスは、彼女の署名を加え、ボブへ、彼の署名を加えるために転送する。ボブは、次いで、署名されたトランザクションをネットワーク106へ転送するか、あるいは、アリス又はサードパーティへ、彼らがネットワーク106へ転送するために返送する。あるいは、Tx_p'は、サードパーティによってテンプレートとして生成され、それからボブへ送信されてもよく、ボブは、彼の署名を加え、アリスへ、彼女の署名を加えるために転送する。アリスは、次いで、署名されたトランザクションをネットワーク106へ転送するか、あるいは、ボブ又はサードパーティへ、彼らがネットワーク106へ転送するために返送する。更なる変形例では、アリス及び／又はボスは、受け取ったトランザクションテンプレートに署名し、単に彼らの署名を他方のパーティの1つへ、そのパーティがTx_p'に組み込んでネットワーク106へ転送するために、返す。やはり、Tx_p及び／又はTx_p'をネットワーク106へ送る前のオフチェーンでの如何なるやりとりも、サイドチャンネル301上で実行されてもよい。

10

【0121】

トランザクションの異なる要素が生成されて組み込まれ得る様々な場所、及びそれが直接に又は身代わりでP2Pネットワーク106の最終的な送り先へ送信される様々な方法があることが理解されるだろう。開示されている技術の実施の範囲は、これらの点のいずれにおいても限定されない。

20

【0122】

また、「アリスによって」、「ボブによって」及び「サードパーティによって」等の本明細書中の表現は、夫々、「アリス103aのコンピュータ機器102aによって」、「ボブ103bのコンピュータ機器102bによって」及び「サードパーティのコンピュータ機器によって」に対する短縮として使用され得ることも理解されるだろう。また、所与のパーティの機器は、そのパーティによって使用される1つ以上のユーザデバイス、又はそのパーティによって用いられるクラウドリソース等のサーバリソース、又はそれらの任意の組み合わせを有してもよい。それは、必ずしも、動作を、単一のユーザデバイスで実行されることに限定するものではない。

【0123】

ターゲットトランザクションTx_pのアンロッキングスクリプトは可鍛性であるから、実施形態で、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バージョンを書き換えること(malleating)、すなわち、Tx_pの既存データを取り、それを、第2バージョンTx_p'を形成するよう変更することによって、この場合には、ロッキングスクリプトを書き換えることによって、生成され得る。これは、スクリプトレベルの可鍛性の例である。同等の変形例では、しかしながら、Tx_p'は、アンロッキングスクリプトが異なることを除いて同じ構造を有しているターゲットトランザクションの新しいバージョンを作ることによって生成されてもよい。「アップデート」が、既存の構造を書き換えること又は新しい置換バージョンを作ることのどちらかの可能性について記載するための一般的な用語として本明細書では使用されることがある。書き換え(Malleation)は、例として本明細書では様々な実施形態に関連して言及されることがあるが、これは、スクラッチからのターゲットトランザクションの新しいバージョンの生成によって置換されてもよいことが理解されるだろう。いずれの場合にも、書き換え又は新しいバージョンの生成は、アリス及び／又はボブ、かつ／あるいはアリス及び／又はボブの署名を与えられたサードパーティによって、実行されてよい。

30

40

【0124】

述べられているように、実施形態で、Tx_iにおいて、第1条件i)は、ボブの署名及びデータペイロードがTx_pのアンロッキングスクリプトに含まれることを必要とするが、アリスの署名は不要であり、第2条件ii)は、アリス及びボブの両者の署名を必要とするが、データペイロードがTx_p'に含まれることは要しない。

50

【0125】

ターゲットトランザクション $T x_p$ は、よって、アリスの署名を必要とせず、しかし、ボブがアンロックングスクリプトにデータペイロードを含める場合にのみ、ボブ（又はボブの代理）によって一方的に精算可能である。これは、マイニングするのにより費用がかかることになる。マイナ104Mは、マイニングのためにトランザクションにアクセスするためにマイニングフィーを必要とする、フィーが不十分である場合には、彼らは、例えばトランザクションが有効であるとしても、ブロック151に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（有効性及び受任可能性は別の概念である）。マイニングフィーは、データの量（バイト又はキロバイトの数）に関連してトランザクションのサイズと通常は比例する。更に、データペイロードは、ブロックチェーン150自体で公に利用可能にしたいくないボブの独自のデータであることがある。従って、ボブは、アリスを幸せなままとし、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の更新されたバージョン $T x_p'$ を提供してもらうことを望む（あるいは、少なくとも彼女の署名を送ってもらい、ボブ又はサードパーティがターゲットトランザクション $T x_p'$ を組み立てる）。これは、ボブが、ターゲットトランザクション $T x_p'$ にデータペイロードを含める必要なしに $T x_i$ の出力を精算することを可能にする。しかし、アリスが約束を破る場合には、ボブは、データペイロードがターゲットトランザクション $T x_p$ に含まれることを求める、より好ましくない第1条件に基づいて、 $T x_i$ の出力を精算するフォールバックを依然として有している。

【0126】

第1トランザクション $T x_i$ は、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での記録の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、それらが全てある段階で最終的に妥当性確認される限りは、如何なるパーティによってもいつでも行われ得る。

【0127】

$T x_i$ のロックングスクリプトにおける第1条件の要件は、データペイロード自体が $T x_i$ のロックングスクリプトに含まれることも、 $T x_i$ がアリスによって定式化される場合でさえ、アリスによって知られていることも求めないことに留意されたい。むしろ、それは、データペイロードのハッシュが（ノード104でハッシュ化される場合に、アンロックング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よう、 $T x_p$ のアンロックングスクリプトに調整するスクリプトとともに） $T x_i$ のロックングスクリプトに含まれることをしか求めない。従って、たとえアリスと又はサードパーティが $T x_i$ を定式化するとしても、ボブは、彼のデータのハッシュを彼らに与えさえすればよく、データ自体を与える必要はない。データを自体を与えるのは、彼がデータを公開する必要があるチェーンに彼がターゲットトランザクション $T x_p$ の第1バージョンを公開する必要がある場合のみである。

【0128】

いくつかの実施形態で、 $T x_i$ のロックングスクリプトは、第1及び第2の両方の条件に対する代案として、第3のアンロックング条件を含んでもよい。第3条件は、ロックタイムが経過しており、かつ、アリス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 $T x_p''$ のアンロックングスクリプトに含まれていることを求めてもよい。これは、ボブが第1及び第2条件のどちらかに基づいてペイメントを請求していない場合に（例えば、ボブが、時間制限内にそうすることできないか又は処理に全く関わっていないため）、アリスが $T x_i$ の出力から彼女のペイメントを取り戻すことを可能にする。ロックタイムは、絶対的な時点、又は経過すべき時間（例えば、秒で又はマイニングされたブロックの数で測定される）として定義され得る。

【0129】

本開示のために、第1トランザクション及び異なるバージョンのターゲットトランザクションにおける異なる代替条件の使用は、任意の付加的なセキュリティ手段であることが理解されるだろう、それらは、ストリーミング及びマイクロペイメントメカニズムを実装

10

20

30

40

50

するのに有利であるが必須ではない。これらの実施形態について、これより、更に詳細に説明する。

【0130】

〔ストリーミング及びマイクロペイメントチャネル〕

図7を参照すると、例えば、アリスは、ボブからあるデータをストリーミングするために支払いたい。データは、ボブからアリスへ「チャンク・バイ・チャンク」で、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、アリスがボブ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、映画等のビデオトラック、及び／又は楽曲などのオーディオトラックを有する。ビデオは、任意の時間変化する画像又はグラフィクス、例えば、映画、テレビ番組、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、アニメーション化されたベクターグラフィクス、及び／又はゲームコンテンツを有してもよい。オーディオは、スピーチ、音楽、ノイズ及び／又は効果、あるいはそのようなものを含む、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有してもよい。他の例では、次の技術が使用されてもよく、アリスがサービス、例えば、ガス、電気若しくは水道などの公共事業の供給、又は車両、不動産、若しくは他の物理オブジェクトの賃貸に対して「使った分だけ支払う」(pay as she goes) ことを可能にする。サービスに支払う場合に、その場合には、所望のコンテンツ自体の部分であるデータの代わりに、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った各々のキーを有する。例えば、アリスのガス、電気又は水道供給は、彼女のコンピュータ機器102aへ接続されたスマートメーターによって管理されている。受け取られた各キーにより、彼女は、これを彼女のコンピュータ機器102aから彼女のメーターへ供給し、メーターは、各々のキーを検証することに応答して、公共事業の他のユニットをアンロックする。

【0131】

ボブのペイメントがこれまで受け取ら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。これを行うために、アリスは、各データ部分 D_0 、 D_1 、 D_2 等がボブから受け取られたことに応答して、サイドチャネル301上でボブへ各々の署名されたトランザクション T_{x1} 、 T_{x2} 、 T_{x3} 等を返すことができる。つまり、ボブがデータの送信を止める場合に、アリスは単純にペイメントの送信を止めることができ、アリスがペイメントの送信を止める場合に、ボブは単純にデータの送信を止めることができ、アリスが支払っていないデータ D の部分はこれ以上与えない。

【0132】

しかし、ストリーミングされるデータの各個別的な部分 D_0 、 D_1 、 D_2 等について個々のトランザクションがネットワーク106へブロードキャストされてブロックチェーン150に記録される必要がないようにこれを実装することも望ましい。これによりネットワーク輻輳は増大し、ブロックチェーン150は膨張するからである。

【0133】

これに対処するために、アリスがボブから受け取る各データ部分 D_0 、 D_1 、 D_2 等に夫々応答してアリスがボブへ返送する各トランザクション T_{x1} 、 T_{x2} 、 T_{x3} 等は、同じソーストランザクション T_{x0} の同じ出力(例えば、同じ $UTXO$)を指し示す第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毎回増大するので、ボブは単に、ある定義されたシーケンスの終わりに、例えば、オーディオ又はビデオトラックの終わり(例えば、映画の終わり)に、あるいは、指定された期間のサービス(例えば、1時間、1日、1週間、又は1ヶ月に1つ)の終わりに、最後の1つの出力を請求する。これは、更に図7を参照して後で更に詳細に説明される。

【0134】

第1に、ボブが、データを送信しないにもかかわらずアリスからペイメントを得ることによって不正を働くことができないように、第2に、アリスが、データを受け取りながらボブの支払わないことによって不正を働く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。

【0135】

実施形態において、第1トランザクションの各インスタンスは、その入力によって指し示されているよりも多い量のデジタルアセットに合計でなる複数の出力を有する。つまり、トランザクションは、誰か、実際にはボブが、彼自身の他の入力を加えて差を補うまでは有効でない（入力レベルの可鍛性の例）。これにより、アリスはシーケンスにおいて初期のトランザクションを公開するのを止め、ボブが後のトランザクションを公開するのをブロックする。従って、これは、映画全体などのためのデポジットとして機能する初期ファンディングトランザクションなしでストリーミングを可能にする。これは、図8を参照して後で更に詳細に説明される。

【0136】

ストリーミング方法を実装するために、アリス及びボブは、彼らの間にオフチェーンサイドチャンネル301を形成する。すなわち、このチャン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での記録のためにP2Pネットワークへ（まだ）公開されない。これは、本明細書で「マイクロペイメントチャンネル」とも呼ばれる、ペイメントチャンネルの変更された形式として使用される。更に、ボブは、シーケンスにおけるデータ部分D₀、D₁、D₂等のためのハッシュセットをアリスに利用可能にする。例えば、ボブは、ペイメントチャンネル301を介してハッシュセットをアリスに送ってもよく、あるいは、インターネット101等でサーバからアクセスするようそれを公に利用可能にしてもよい。ハッシュセットは、アリスが、実際の生（raw）データ自体を前もって知らなくても、データのハッシュチャレンジを作成することを可能にするハッシュの組を有する。例えば、ハッシュセットは、マークル木（Merkle tree）としても知られているハッシュ木を有してもよい（マークル木という用語は、あらゆるハッシュ木を意味するためにその最も広い意味で本明細書では使用され、必ずしも、例えば、2項枝分かれに限定されるわけではないことに留意されたい）。代替的に、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有してもよい。

【0137】

ボブは、ペイメントチャンネル301を介して第1データ部分D₀をアリスに送ることによって、開始する。この第1部分は、無料で又はつけで送られる。アリスが支払わない場合には、ボブは、第1部分に相当するデータしか失わない。アリスが継続したと望むならば、D₀を受け取ったことに応答して、彼女は、ペイメントチャンネル301を介して第1トランザクションの第1インスタンスTx₁をボブに送る。これに応答して、ボブは、シーケンスにおける次のデータ部分D₁をアリスに送る、次いで、これに応答して、アリスは、第1トランザクションTx₂の第2インスタンスをボブに送り、次いで、ボブはD₂をアリスに送り、アリスはTx₃をボブに送り、以降同様に続くが、全てペイメントチャンネル301を介する。第1トランザクションの各インスタンスTx₁、Tx₂、Tx₃等は、ボブへの増大するペイメント（例えば、これまで受け取ったデータ部分Dの数とともに線形に増大する）を指定する。しかし、第1トランザクションの各インスタンスTx₁、Tx₂、Tx₃等は、アリスの同じUTXOを指し示す。従って、ボブは、それらのうちの1つにペイメントを請求する第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'しか構成することができない（同じUTXOを2回精算しようとする如何なる試みも、無効としてネットワーク106によって拒絶されることになる）。全てが上手くいくと、ボブは、従って、順番において第1トランザクションの最後のインスタンスにペイメント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作成することになる。

【0138】

実施形態において、第1トランザクションの各インスタンスTx₁、Tx₂、Tx₃等又は最後のインスタンスTx_nは、（例えば、図5を参照して）上述されたように、そのトランザクションの出力でアリスからのペイメントを精算するための複数の代替条件を定義する。この場合に、シーケンス内の最後のデータ部分D_nのアリスの確認応答Tx_nとともに、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'も供給し、あるいは、少なくとも、ボブがTx_p'を組み立てることを可能にする彼女の署名を供給する。これ

10

20

30

40

50

により、ボブは、ボブに不利益をもたらす第1条件ではなく、好ましい第2条件に基づいて、完全なシーケンス（例えば、映画全体）に対するペイメントを請求することが可能にある。ボブが部分Dをストリーミングすることを止め、アリスが不満を抱く場合には、彼女は、第2条件を満足するために必要な彼女の署名を提供しなくてもよく、従って、ボブは、第1の、より好ましくない条件に基づいてしかペイメントを請求することができない。他方で、アリスが、途中でそれ以上の部分を要求することを止めたが不満足でない（例えば、彼女が、映画を観るのを止めることを単に選択する）場合には、これまでの第1トランザクションのインスタンスの夫々 Tx_1 、 Tx_2 、 Tx_3 等に複数の代替条件が含まれているとすれば、アリスは、好ましい第2条件に基づいてこれまでのシーケンスに対するペイメントを請求することをボブに可能にするように、 Tx_p ' 又は彼女の署名を提供し得る。

10

【0139】

第1トランザクションのインスタンス Tx_i ($i = 1, 2, 3, \dots$) は、共通のUTXOを使用するが、異なるメッセージで署名を使用する。従って、これに関連して、インスタンスは、トランザクションのインスタンスとして、アリスからのデータに対する各々の「要求」を参照する（後述される）。これは、値及び要求されたデータを変更することが、署名されたメッセージを変更するからである。

【0140】

第2トランザクションのバージョン Tx_p / Tx_p' は、共通のUTXOを使用するが、同じメッセージで署名を使用する。従って、これに関連して、バージョンは、トランザクションの各々のバージョンとして、トランザクションの「書き換えられていない」形式及び「書き換えられた」形式を参照する。これは、スクリプトレベルの書き換えが、署名されたメッセージを変更しないからである。

20

【0141】

注釈：どのパーティが第1トランザクション $Tx_1 \dots$ 並び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 / Tx_p' を生成及び／又はブロードキャストするかに関して上述された変形例のいずれもが、ここで適用されてもよい。例えば、サードパーティは、アリス又はボブの代わりにそれらの一部又は全てを生成及び／又はブロードキャストしてもよく、あるいは、ボブは、 Tx_p / Tx_p' をネットワークへ彼自身が送っても、又は彼の署名をアリスへ、アリスがターゲットトランザクション Tx_p / Tx_p' 等を組み立てるために送ってもよい。便宜上、これらの様々な選択肢は、ここでは完全に再びは繰り返されない。

30

【0142】

例として、映画産業を考える。スクリプトサイズ制限は、書き込みの時点で10キロバイトである。従って、映画ごとに、それは多数の8キロバイト部分に分割され得る。部分のサイズは、他の制約が存在する場合には、より一層小さくてもよく、あるいは、スクリプトサイズ制限が増やされる場合には、より大きくてもよい。部分が定義されると、マークル木が次いで構成され得、ルートハッシュが映画タイトルとともに公にリスト化される。

【0143】

簡単のために、説明は、マイニングフィーが暗黙的に適用されると仮定する。明示的な入力が明示的な出力に暗黙的なトランザクションフィーをプラスしたものをカバーすることができない場合には、他の暗黙的な入力があるとする。

40

【0144】

アリスは、ボブから映画を買おうとしている。映画は、 $n+1$ 個のデータパケット $D_0, \dots, D_n$ と、ルートハッシュ H_{root} を有するそれらのマークル木 T とによって定義される。方法は、アリスからボブへの一連のトランザクション $Tx_1, Tx_2, \dots, Tx_n$ を構成する。各トランザクション Tx_i は、 D_i に対する要求と、 D_{i-1} を受け取ったことの確認応答とに対応する。理想的に、ペイメントチャネル301が適切に選択される場合には、ただ2つのトランザクション Tx_n ' 及び Tx_p ' のみが、アリスからボブへのペイメントを完了するよう公開される。このシナリオは図7に表されている。図7は

50

、アリスとボブとの間のペイメントチャンネル301のシーケンス図である。ボブからアリスへの1つの初期メッセージが存在し、その後、各データパケットのためのn個のメッセージ対と、チャンネルを選択するための2つの最終メッセージとが続くことに留意されたい。

【0145】

第1ラウンドーアリスのターン：最初に、ボブは、アリスに、 D_0 と、期待されるデータパケットを含む完全なマークル木とを送る。アリスは、ルートハッシュが彼女の選択する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。アリスが受け取ったデータに満足すると、彼女は、彼女が D_0 を受け取ったことを承認するよう TX_1 を構成し、 D_1 を要求したいと思う。このトランザクションは、次の形を取ることができる：

TX_1

ロックタイム：0

入力0：

●アリスの未使用アウトポイント ($TXID_0$, $vout=0$)

●アリスの署名及び $SIGHASH_ALL | ANYONECANNPAY$

出力0：

●ロッキング条件

(i) ボブが D_1 及び彼の署名を提供する場合に、彼は出力を請求することができる。

(ii) 他に、アリス及びボブが彼らの署名を提供する場合に、ボブは出力を請求することができる。

(iii) さもなければ、720個のブロックの後（このトランザクションがマイニングされてから後）に、アリスは出力を請求することができる。

●値：デジタルアセットの500ユニット

出力1：

●アリスのチェンジ

出力2：

●出力1と同量をボブに支払う

【0146】

この例となるインスタンス化は、図9に示されている、単一のトランザクション設計は、3つの意図された機能を備える。余分の意味合いをトランザクションのいくつかのフィールドに割り当てることによって、データトレードシナリオで必要とされる複数のメッセージをただ1つの単一トランザクションテンプレートで置換す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け取られて満足していることを認める署名である。 $PP_DUP \quad OP_SHA256 < H(D_1) > OP_EQUAL$ は、データの次のパックを求める要求である。500個のユニットは、データの次のパックに対するペイメントである。

【0147】

TX_1 の入力は、少なくとも入力0を有する。これは、その量が TX_1 の出力0よりも多い（以下を参照）、アリスにロックされている前のトランザクション TX_0 の $UTXO$ へのポインタを有する。 TX_1 の入力0はまた、入力のアンロッキングスクリプトでのアリスの署名と、他のパーティが入力を加えることを可能にするフラグ（「 $ANYONECANNPAY$ 」）とを有する。

【0148】

TX_1 の出力は、少なくとも出力0を有する。これは、 TX_1 の入力0よりも小さい（最初に）小さい量のデジタルアセット（例えば、500個のユニット）を指定する。任意の実施形態では、 TX_1 の出力はまた、条件：

i) 後続のトランザクション TX_p の入力でのアンロッキングスクリプトが D_1 及びボブの署名を含む；

ii) 後続のトランザクション TX_p' の入力でのアンロッキングスクリプトがアリスの

10

20

30

40

50

署名及びボブの署名を含む；又は

i i i) タイムアウト制限が経過しており、後続のトランザクションの入力でのアンロッキングスクリプトがアリスの署名を含む；
のうちのいずれかの下でこれがアンロックされることを可能にするロッキングスクリプトを有する。

【0149】

条件 i) に関して、アリスは、ボブがハッシュ木と呼ばれるマークル木を彼女に送っているので、どのデータ部分を期待すべきかを知っている。これにより、彼女は、彼女がこの条件をハッシュチャレンジによって含めるのに十分である D_1 のハッシュを決定することができる。(TX_1 のロッキングスクリプトは、 TX_p の入力のアンロッキングスクリプトで与えられている値が、ハッシュ化される場合に、ロッキングスクリプト内の値に一致することをチェックする何らかのコードをプラスした D_1 のハッシュを含む)。この条件は、ボブがアリスの署名なしで今すぐペイメントを請求したい場合に、彼が D_1 をブロックチェーン 150 に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、ボブの独自のデータであり、また、 D_1 のサイズは高いマイニングフィーを負うために、ボブは、そうしたくないことがある。この技術はまた、後続のデータ部分 D_2 、 D_3 等に対しても使用され得る。

【0150】

条件 i i) は、ボブが代わりにアリスに彼の署名を与える場合に、ボブがデータをアップロードせずにペイメントを請求することを可能にする。しかし、彼はまだそうしたくないと仮定する。

【0151】

条件 i i i) は任意である。これにより、特定の指定されたタイムアウト期間後にボブが何らかの理由で請求しなかった場合（例えば、ボブは決してプロセスに関与しない場合）に、アリスは TX_1 の出力 0 内の量を取り戻すことができる。720 個の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よう。より一般的には、タイムアウト期間は、ブロック数又は秒などの人間の時間で定義でき、任意の値に設定可能である。これは、絶対的な時点又は経過時間で期限切れになると定義可能である。

【0152】

TX_1 はまた、任意に、1 つ以上の更なる出力を有してもよい。実施形態で、これらは、出力 1 及び出力 2 を有する。出力 1 は、入力量に等しいデジタルアセットの量を定義し、これをアリスにロックする（「アリスのチェンジ」）スクリプトを有する。例えば、これは 2000 - 500 個のユニット = 1500 個のユニットである。

【0153】

出力 2 は、出力 1 に等しいデジタルアセットの量を定義し、これをボブにロックする（「出力 1 でのアリスのチェンジと同量をボブに支払う」）スクリプトを有する。この効果は、他に誰か（実際には、ボブだけである）が自身の他の入力 1 を TX_1 に加えて差を補わない限りは、合計出力（例では、500 + 1500 + 1500 個のユニット = 3500 個のユニット）が常に入力よりも大きいことである。

【0154】

出力 2 は、ボブの肯定応答なしでアリスがトランザクションを公開しないよう設計されたトリックである。支払人として、アリスは、最初に、 TX_1 をブロードキャストするよう動機付けられていない。しかし、数ラウンドの後、アリスがボブにより多く支払う他のトランザクションが存在する場合には、アリスは、ボブが彼のペイメントを請求するよう後のインスタンスを使用する前に、 TX_1 をネットワーク 106 にブロードキャストすることによって、他のトランザクションを無効にするために TX_1 を使用する可能性がある。出力 2 を含めることによって、 TX_1 は、ボブが出力と入力との間の不足をカバーするために自身の入力（入力 1）を TX_1 に加えるまで、有効でない。ボブは、アリスが S I G H A S H フラグ「ALL | ANYONE CAN PAY」を使用するので、余分の入力を加えることができる。結果として、 TX_1 は、ボブによってのみブロードキャストされる

可能性が高くなる。アリスは、 TX_i を有効にするために必要な余分の入力を追加したくない。これは、彼女がシステムをだまさなかった場合よりもコストがかかるためである。

【0155】

アリスのチェンジは、アリスの入力（入力0）の値からボブのペイメント（出力0）の値をマイナスしたものであるよう定義される。図8のグラフが示すとおり、ボブの保険（出力2）は、最後のデータ部分が送られる前に、合計出力（破線）が常に入力よりも大きいことを確かにする。

【0156】

より一般的に、 TX_1 の合計出力値が合計入力値よりも大きい状況が生じるように出力の他の組み合わせが使用されてもよく、よって、ボブに TX_1 の出力を請求するために彼自身の入力を加えるよう求めるとともに、アリスに TX_1 をブロードキャストすることを思いとどまらせる。

【0157】

スクリプト言語において出力0に3つの条件*i*）、*ii*）及び*iii*）を実装する例として、ハッシュパズル及び条件付きオペコードを使用することができる。例えば、次の通りである。

【数1】

OP_DUP OP_HASH256 < D_1 のハッシュ> OP_EQUAL

OP_IF

OP_DROP OP_DUP OP_SHA256 <ボブのパブリックキーのハッシュ>

OP_EQUALVERIFY

OP_CHECKSIGVERIFY

OP_ELSE

2 <アリスのパブリックキーのハッシュ> <ボブのパブリックキーのハッシュ> 2

OP_CHECKMULTISIG

OP_IF

OP_VERIFY

OP_ELSE

<720 個のブロック> OP_CHECKSEQUENCEVERIFY

OP_DUP OP_SHA256 <アリスのパブリックキーのハッシュ>

OP_EQUALVERIFY OP_CHECKSIGVERIFY

OP_ENDIF

OP_ENDIF

【0158】

第1ラウンドーボブのターン：ボブがトランザクション TX_1 を受け取るとき、彼は単純に D_1 をアリスへ送る。ボブは、次のことを行うことによって、アリスからの如何なる助けもなしで彼が TX_1 でペイメントを請求することができるということで、これを安全に行うことに留意されたい。最初に、ボブは、 TX_1 で出力2の値をカバーするよう、アウトポイント（ $TXID_B, vout=0$ ）を用いて、自身の入力を加えることによって、 TX_1' を生成する。第2に、ボブは、ペイメントを請求するよう他のトランザクション TX_p を生成する：

TX_p

ロックタイム：0

入力0：

- TX_1 ' の出力 0 からのアウトポイント
- アンロックングデータ
 - D_1
 - ボブの署名

出力 0 :

- ボブに支払う
- 値 : 500 個のユニット

【0159】

ボブは、次いで、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する。しかし、ボブにとって、これは、理想的な状況ではない。これは、彼がトランザクションで D_1 をさらさなければならぬからである。これは、チャンネルの早期閉鎖 (premature closure) と見なされる。しかし、アリスが、ペイメントチャンネルを閉じるよう適切な手順に従う場合には (後述される)、ボブはこれを行う必要がない。

10

【0160】

第 2 ラウンドーアリスのターン : アリスが D_1 を受け取り、内容に満足する場合に、彼女は、データの次のパックのための続くトランザクションを構成する。このトランザクションも、 D_1 を受け取ったことの確認応答と見なされる :

TX_2

ロックタイム : 0

入力 0 :

- アリスの未使用アウトポイント (TX_1 と同じアウトポイントであるとする)
- アリスの署名及び $SIGHASH_ALL | ANYONECANSPAY$

20

出力 0 :

- ロッキング条件

(i) ボブが D_2 及び彼の署名を提供する場合に、彼は出力を請求することができる。
(ii) 他に、アリス及びボブが彼らの署名を提供する場合に、ボブは出力を請求することができる。

(iii) さもなければ、720 個のブロックの後に、アリスは出力を請求することができる。

- 値 : 1000 ユニット

30

出力 1 :

- アリスのチェンジ

出力 2 :

- 出力 1 と同量をボブに支払う

【0161】

TX_1 と TX_2 とを比較すると、 D_1 が D_2 に変更されており、出力 0 の値がデジタルアセットの 500 ユニットから 1000 ユニットに増加していることに気付く。これら 2 つの変更の結果として、(アリスが同じ未使用アウトポイントを使用していると仮定して) 他の出力は異なる値を有することになる。更に、これらの変更はトランザクションの可鍛部分に行われていないので、アリスは TX_2 に対して新しい署名を生成しなければならない。

40

【0162】

第 2 ラウンドーボブのターン : ボブがトランザクション TX_2 を受け取るとき、彼は単純に D_2 をアリスへ送る。前と同様に、ボブは、第 1 ラウンドと同じように、アリスからの如何なる助けもなしで彼が TX_1 でペイメントを請求することができるということで、これを安全に行う。ボブは、 TX_2 で出力 2 をカバーするよう、やはり ($TXID_B, vout = 0$) から、自身の入力を加えて、 TX_2 ' を生成する。また、ボブは、ペイメントを請求するよう他のトランザクション TX_p を生成する :

TX_p

ロックタイム : 0

50

入力 0 :

- TX_2' の出力 0 からのアウトポイント
- アンロッキングデータ
 - D_2
 - ボブの署名

出力 0 :

- ボブに支払う
- 値 : 1000 個のユニット

【0163】

ボブは、次いで、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する。

10

【0164】

アリス及びボブがチャンネルを閉じるよう協働する場合に、ボブは、第 1 ラウンドで述べられたように、これを行うことを回避することができる。

【0165】

最終ラウンドーアリスのターン：数ラウンドの後、アリスは、データの最後のパック D_n を要求するよう TX_n を構成する：

TX_n

ロックタイム : 0

入力 0 :

- アリスの未使用アウトポイント (TX_1 と同じアウトポイントであるとする)
- アリスの署名及び $SIGHASH_ALL | ANYONECANNPAY$

20

出力 0 :

- ロッキング条件
 - (i) ボブが D_n 及び彼の署名を提供する場合に、彼は出力を請求することができる。
 - (ii) 他に、アリス及びボブが彼らの署名を提供する場合に、ボブは出力を請求することができる。
 - (iii) さもなければ、720 個のブロックの後に、アリスは出力を請求することができる。

- 値 : 500n ユニット

出力 1 :

- アリスのチェンジ

30

出力 2 :

- 出力 1 と同量をボブに支払う

【0166】

最終ラウンドーボブのターン：ボブは、最後のデータパック D_n で応答する。

【0167】

チャンネルの閉鎖：ペイメントチャンネルを閉じるために、アリスとボブとの間には数回のインタラクションが存在する。アリス又はボブのどちらかが、チャンネル 301 を閉じる意志を他方に伝えることができる。一般性を失わずに、ボブからアリスへ送られたデータの最後のパックは D_n であるとする。ボブは、 D_n を要求するトランザクションである TX_n を見つけ、自身の入力を加えて出力 2 をカバーして TX_n' を生成する。ボブは、次のように TX_p を生成する：

40

TX_p

ロックタイム : 0

入力 0 :

- TX_n' の出力 0 からのアウトポイント
- アンロッキングデータ
 - D_n
 - ボブの署名

出力 0 :

50

●ボブに支払う

●値：500n個のユニット

【0168】

ボブは、両方のトランザクション TX_n' 及び TX_p を直接にアリスへペイメントチャンネル301を介して送信する。アリスは、 TX_n' 及び TX_p の入力が、彼女が期待するように実際に関係していることをチェックする。アリスは、 TX_p に署名し、 D_n を彼女の署名で置換して、 TX_p' を生成する。

TX_p'

ロックタイム：0

入力0：

● TX_n' の出力0からのアウトポイント

●アンロックングデータ

○アリスの署名

○ボブの署名

出力0：

●ボブに支払う

●値：500n個のユニット

【0169】

アリスは、 TX_p' をボブへ送る。ボブは TX_n' 及び TX_p' をネットワーク106へブロードキャストする。代替的に、アリスは、 TX_n' 及び／又は TX_p' をブロードキャストしてもよく、あるいは、それらの一方又は両方をサードパーティへおくって、アリス及びボブの代わりにブロードキャストしてもらってもよい。アリスは、いつでもチャンネルを閉じることを選択することができることに留意されたい。

【0170】

図7では、(A)チャンネルがボブによって一対のトランザクションをブロードキャストすることによって一方的に閉じられ得る方法と、(B)対を形成する2つのトランザクションが両方ともチャンネルの閉鎖時にブロードキャストされる方法とを両方に言及しており、チャンネルがネットワーク106と通信しない有効に「開かされた」オフチェーンであることを示す。

【0171】

シーケンスをリキャップするために、 TX_1 に応答して、ボブは D_2 をアリスへ送る。アリスは承認するためにボブに TX_2 を送り、次いで、ボブは D_3 を送り、以降同様に続く。 TX_2 は、 TX_1 と同じであるが、 D_1 が D_2 で置換されており、出力0の量が増えている。 TX_3 では、 D_2 が D_3 で置換されており、出力0の量がやはり増えている。実施形態において、出力0での量は、 i とともに、つまり、確認応答で送られたチャック及び TX ごとに、線形に増大する。代替的に、他の増大関係が使用されること、例えば、シーケンスを完了することを更に奨励するようシーケンスの終わりに向かってより高い重み付けを与えること、は除かれない。

【0172】

ボブは、基準 i に基づき TX_1 、 $\dots$ 、 TX_i のうちのいずれか1つを一方的に請求することができる。これを行うために、ボブは、それを書き換えて TX_i' を生成する。書き換えは、 TX_i を使用するために、差を補うようボブのデジタルアセットの一部の入力を加え、それから、その入力 D_i を含む他のトランザクションを生成することを有する。 TX_p は無条件にボブにロックされた出力を有する。ボブは、彼の入力を加え、前のトランザクション TX_1 又は TX_2 等の1つを使用できたが、それだけの価値はない。彼は、映画を送信し続けて、最後に全量を手に入れたと思っている。また、ボブは、彼がブロックチェーンで彼の映画のチャックのうちの1つを公開する必要があるために、基準 i にのみ依存したくない。

【0173】

夫々の TX_1 、 TX_2 、 TX_3 、 $\dots$ の入力は、 TX_0 の同じUTXOを指定すること

10

20

30

40

50

に留意されたい。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、いずれかの所与のノードで妥当性確認される場合に、インスタンスのうちのその他はもはや、そのノードによって有効と見なされなくなる（有効性の条件は、Txが、他のトランザクションに既に有効に使用されているUTXOを使用しようと試みていないことである）。異なるノード104は、最初の異なるインスタンスを受け取るので、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見解を有しており、その時点で、全てのノード104は、マイニングされたインスタンスが唯一の有効なインスタンスであることに同意する。ノード104が1つのインスタンスを有効として受け入れ、それから、第2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する場合に、そのノード104は、これを受け入れ（るべきであり）、最初に受け入れたマイニングされていないインスタンスを捨てる（すなわち、無効として扱う）。

10

【0174】

ボブが早期にキャッシュインを行って、映画を送るのを止める場合に、アリスは、彼女が受け取っているよりも1つ多いチャックについて支払っただけであるから、500しか失わない。アリスは、いつでも手を引くことができたが、彼女がそうしない場合には、ボブは、アリスが支払わなかった映画の1よりも多いチャック（例えば、500ユニットの価値）を決して彼女に送っていない。

【0175】

量が、最初は小さくて映画の終わりまでに増大しながら、毎回増大し、そして、全てのトランザクションがTx₀で同じUTXOを使用しようと試みるので、メカニズムは機能する。故に、いずれか1つをキャッシュインすると、その他が無効になる。また、実施形態で、出力合計は、ボブが自身の入力を加えるまで、入力よりも本質的に大きい。これは、入力レベルの可鍛性の例である。

20

【0176】

ボブ及びアリスの両方が映画の終わりまで待つ場合には、ボブは、アリスが署名するためにTx_n’をアリスへ送る。それにより、D_nのハッシュはアリスの署名で置換される。これは、ボブが、データの如何なるチャックDも公開せずに完全なペイメント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可鍛性の例である。

【0177】

ブロックチェーンでのデータ輻輳を回避するために、プロセスは、何らかのデータパケット又はデータ受信者の署名のどちらかを使用してアンロックされ得るロッキングスクリプトを使用する。トランザクションの可鍛性を使用することによって、データ受信者は、アンロッキングスクリプト内のデータを彼又は彼女の署名で置換することができる。この動作は、データが受け取られたことを承認したり又はペイメントチャネルの閉鎖を確認したりするのみならず、空間を節約するようトランザクションからデータをプルーニングする。

30

【0178】

ボブが、トランザクションの値の漸進的な増大を考慮して、彼がアリスから受け取る最後のトランザクション以外の如何なるトランザクションも公開する動機はない。アリスが時期尚早にチャネルから去る場合に、ボブは単純に、彼がアリスから受け取る最後のトランザクションを、ペイメントを請求するトランザクションとともに公開する。彼がアリスの書き換えられたトランザクションを受け取らなかった場合には、彼は、ペイメントを請求するために、関連するデータパックをさらさなければならない。実施形態で、データ機密性に関する強い要件が存在する場合には、ボブはアリスへ送られるデータを暗号化し、トランザクションで暗号解読キーを明らかにすることができる（以下を参照）。

40

【0179】

アリスについては、しかしながら、彼女が十分なデータパックを受け取る場合に、最初のトランザクションを公開する動機が存在する可能性がある。最初のトランザクション及び最新のトランザクションの両方が有効である場合に、彼女が最新の通信されたトランザ

50

クションを無事に無効にすることは定かでない。このシナリオを完全に回避するために、実施啓太は、誰かが出力と入力との間の不足をカバーしない限りは、トランザクション自体を無効にする余分の出力を含む。アリスがトランザクションを有効にするために、彼女は余分の入力を供給する必要がある、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無にする。

【0180】

ボブがオフラインになる場合に、アリスは、映画を観続けることができなくなる。しかし、彼女は、彼女が見たものにこれ以上支払うことはない。彼女は、ボブが戻るのを待つか、あるいは、他のサービスプロバイダに移動して、彼女が停止した場所から開始することができる。

【0181】

この形式のペイメントチャネルに必要なファンディングトランザクションはないことに留意されたい。更に、それは、アリスがいつでもストリーミングサービスを再開するよう再接続することができるほどに柔軟である。つまり、ペイメントチャネルを形成するためのオーバーヘッドはない。

【0182】

実施形態は、ペイメントチャネル内の全てのリスクに対処する。アリスはペイメントチャネル外で彼女のUTXOを二重に支払う可能性が依然としてあり得る。実施形態は、これを防ぐために3つの選択肢のうちの1つ以上を阻止することができる。1つは、アリスがUTXOを二重支払いしようとしたときに、デポジットアカウントの秘密鍵を明らかにするように強制する手法を採用することである。この場合、ボブは全てのデポジットを請求可能である。第2の選択肢は、アリスの確認応答を法的拘束力のあるものにすることである。つまり、ボブのペイメント請求トランザクションに対するアリスの署名は、彼女の身元の拘束力のある証拠と見なされ得る。アリスからの如何なる不正行為も、法執行の対象となる。第3の選択肢は、ボブがペイメントを随時、例えば、5分ごとに完了及び再開することである。頻度は、ボブによって、リスクに関する彼自身の評価に従って調整可能である。ファンディングトランザクションは不要であるから、ペイメントチャネルを再開することによるオーバーヘッドがないことに留意されたい。

【0183】

データ暗号化：データ機密性は、データがパブリックネットワーク上で交換される場合に、しばしば必要条件である。前のセクションでは、データ受信者は、何が受け取られると期待されるかを正確に知っている、と仮定した。しかし、データが暗号化される場合に、暗号文が何であるか、又はどのようなハッシュ値を期待すべきかを、如何なる通信もなしで前もって知ることは困難である。これにより、ロッキングスクリプトでハッシュパズルを構成する必要が生じる。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、その暗号文をそうしする前にデータの受け手へ伝えることができる。データの受け手は、与えられたハッシュ値を用いて、ペイメントトランザクションを構成する。暗号化されたデータを受け取る場合に、データの受け手は、データを暗号解読し、データが期待されているかどうかを検証することができる。そうである場合には、全てが大丈夫である。そうでない場合には、最悪のケースは、受け手がお金を失うことである。しかし、受け手が失う可能性がある量は、データパックあたりの価格によって制限される。映画の場合に、それはおそらく約500ユニットである。例えば、映画を合計すると約5ドルになる。経済的価値の規模が小さく、評判への影響はるかに大きいことを考えると、データの売り手には不正を行う動機がない。

【0184】

いくつかの実施形態は、データの売り手とデータの各買い手との間で対称暗号法により共通の秘密キーを形成するメカニズムを実装してもよい。従って、伝送における全てのデータは、暗号化され得る。

【0185】

〔結論〕

上記の実施形態は、単に例として記載されていることが理解されるだろう。

【0186】

より一般的には、本明細書で開示されている一態様に従って、ノードのネットワークの少なくとも一部の夫々で保持されているブロックチェーンのコピーにターゲットトランザクションを記録する方法であって、

第2パーティのコンピュータ機器によって、

第1パーティと前記第2パーティとの間に、前記ネットワークとは別のサイドチャンネルを形成することと、

連続したデータ部分のシーケンスを、該シーケンス内の最新のデータ部分まで、前記サイドチャンネル上で前記第1パーティへストリーミングすることと、

前記データ部分の各々のデータ部分に回答して、前記第1パーティから第1トランザクションの異なった各々のインスタンスを前記サイドチャンネル上で受信することであり、前記第1トランザクションは、デジタルアセットの量を指定する出力を有し、前記ターゲットトランザクションは、前記第1トランザクションの前記第1出力へのポインタを含む入力を含み、前記ターゲットトランザクションは、前記第1トランザクションの前記第1出力から前記第2パーティへ転送すべき前記デジタルアセットの量を指定する出力を更に有し、前記第1トランザクションの前記第1出力で指定されている前記量は、前記第1トランザクションの連続するインスタンスごとに増大する、ことと、

前記第1トランザクションの最新のインスタンス及び前記ターゲットトランザクションの対応するバージョンが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにすることであり、前記ターゲットトランザクションの前記対応するバージョンにおける前記ポインタは、前記シーケンスにおいて前記第1トランザクションの前記最新のインスタンスでの前記第1出力を指す、ことと

を有する方法が提供される。

【0187】

前記第1トランザクションの最新のインスタンス及び前記ターゲットトランザクションの対応するバージョンが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにすることは、第2パーティ自体が（第2パーティのコンピュータ機器によって）第1トランザクションの最新のインスタンス及び／又は対応するターゲットトランザクションを、ネットワークを通じて伝播されてブロックチェーンに記録されるよう送信することを有してもよい（当該送信することは、直接であっても、あるいは、第1又は第3パーティを介してもよい）。代替的に、前記第1トランザクションの最新のインスタンス及び前記ターゲットトランザクションの対応するバージョンが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにすることは、第2パーティが第1トランザクションの最新のインスタンス及び／又は対応するターゲットトランザクションの一方又は両方を、ネットワークを通じて伝播されてブロックチェーンに記録されるように送信することを、第1パーティ又は第3パーティに要求又はトリガすることを有してもよい。例えば、第2パーティは、第1及び／又は第2トランザクションの一方又は両方を第1パーティへ部分的な形式で（例えば、第2パーティの署名を含むが第1パーティの署名は含まない）、第1パーティが完成させてネットワークへ（直接に又は第3パーティを介して）転送するために、送信してもよい。他の例として、第1パーティにトランザクションの1つを送信させることは、第2パーティがトランザクションのコンポーネント（例えば、第2パーティの署名）を第1パーティへ、第1パーティがトランザクションを形成して送信するために、送信することを有してもよい。

【0188】

実施形態において、前記第1トランザクションの前記第1出力で指定されている前記量は、前記第1トランザクションの連続するインスタンスごとに線形に増大してもよい。

【0189】

実施形態において、前記第1トランザクションの各インスタンスは、前記第1パーティによる前記各々のデータ部分の受信の肯定応答としての機能を果たしてもよく、その場合

に、前記ストリーミングすることは、前記第1トランザクションの各インスタンスの受信に
応答して前記シーケンスにおける次のデータ部分を送信することを有する。

【0190】

実施形態において、方法は、前記第2パーティのコンピュータ機器で、前記第1トラン
ザクションのインスタンスのうちのいずれか1つのインスタンスと、そのインスタンスを
指す前記ターゲットトランザクションの対応するバージョンとが、前記シーケンス内の任
意の時点で、前記ネットワークにわたって伝播されて前記ブロックチェーンに記録される
ようにすることを可能にするアプリケーション機能を提供することを有してもよい。この
場合に、方法は、このために前記機能を使用する代わりに、前記機能を用いて、前記イン
スタンスのうちの先行するインスタンスのいずれかの代わりに、前記シーケンスにおける
前記第1トランザクションの前記最新のインスタンス及び前記シーケンスにおける前記最
最新のインスタンスを指す前記ターゲットトランザクションの対応するバージョンの伝播及
び記録を引き起こすことを有する。

10

【0191】

実施形態において。前記データ部分の夫々は、メディアコンテンツ片（例えば、ビデオ
及び／又はオーディオコンテンツ）の各々の部分を有してもよい。

【0192】

代替的に、前記データ部分の夫々は、前記第1パーティがサービスサプライヤからのサ
ービスのユニットをアンロックすることを可能にする異なった各々のキーを有してもよい
。例えば、前記サービスは、電気、ガス、又は水道を含む公共事業の提供、あるいは、不
動産、車、又は他の物理オブジェクトの賃借、のうちの1つを有してよい。

20

【0193】

実施形態において、前記シーケンスは、有限なシーケンスであってよく、前記最新のデ
ータ部分は、前記シーケンス内の最後の部分であってよい。

【0194】

実施形態において、前記第1トランザクションの少なくとも最後のインスタンスの前記
第1出力は、少なくとも第1条件及び第2条件を含む、前記第1トランザクションの前記
第1出力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キングスクリプトを有し
てもよく、前記ターゲットトランザクションの前記入力、アンロッキングスクリプトを
有してもよい。前記ネットワークを通じて伝播されて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対応するバージョンにおいて、前
記ロッキングスクリプトは、前記代替条件のうちの第1条件ではなく第2条件を満足する
ことに基づいて前記第1トランザクションの前記第1出力をアンロックするよう構成され
てもよい。

30

【0195】

実施形態において、前記第1トランザクションの各インスタンスの出力は、前記複数の
代替条件を指定する前記ロッキングスクリプトを有してもよい。前記機能は、前記最後の
インスタンスより前の前記第1トランザクションの現在受信されているインスタンスと、
該現在のインスタンスを指す前記ターゲットトランザクションの第1バージョンとが前記
ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにすることを可
能にすることができ、前記第1バージョンにおける前記ロッキングスクリプトは、前記第
1条件を満足することに基づいて前記第1トランザクションの前記第1出力をアンロック
するよう構成される。

40

【0196】

例えば、前記機能は、前記第1トランザクションの前記現在受信されているインスタ
ンス及び前記ターゲットトランザクションの第1バージョンが前記ネットワークを通じて伝
播されて前記ブロックチェーンに記録されるようにすることを手動で選択するためのオブ
ションを前記シーケンス内の任意の時点で前記第2パーティに提供してもよい。代替的に
、又は追加的に、前記機能は、前記第1パーティが前記シーケンスを通じた前記第1トラ
ンザクションのインスタンスの送信を止める場合に、自動で前記第1トランザクションの

50

前記現在のインスタンス及び前記ターゲットトランザクションの第1バージョンが前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるようにするよう構成されてもよい。

【0197】

実施形態において、前記第2条件は、前記アンロックングスクリプトが、該アンロックング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1パーティの暗号署名を有することを要求してもよく、伝播されて前記ブロックチェーンに記録されるよう送信される第2バージョンは、前記アンロックングスクリプトにおいて前記第1パーティの前記署名を含んでもよい。

【0198】

実施形態において、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くてもよい。

【0199】

実施形態において、少なくとも前記第1条件は、前記アンロックングスクリプトが、該アンロックング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する。

【0200】

実施形態において、前記第2条件は、前記アンロックングスクリプトが、該アンロックング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もよい。この場合に、伝播されて前記ブロックチェーンに記録されるよう送信される第2バージョンは、前記アンロックングスクリプトにおいて前記第2パーティの前記署名を含むことになる。

【0201】

実施形態において、方法は、前記第2パーティの前記コンピュータ機器によって、前記第1パーティの前記署名を加えることによって前記第1パーティが前記ターゲットトランザクションに統合するように前記第1バージョンを前記第1パーティへ送ることを有してもよい。

【0202】

実施形態において、前記第1条件は、前記データ部分の夫々が前記アンロックング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、前記データ部分のいずれも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い。この場合に、前記ネットワークを通じて伝播されて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第2バージョンは、前記ターゲットトランザクションにおいて前記データ部分のいずれも含む必要がない。

【0203】

実施形態において、前記第1条件は、前記アンロックングスクリプトが前記データ部分の夫々と、前記アンロックング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とを有することを要求するが、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、前記アンロックング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有することを要求するが、前記データ部分のいずれも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い。この場合に、伝播されて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第2バージョンは、該第2バージョンにおいて前記データ部分のいずれも含む必要がないが、前記アンロックングスクリプトにおいて前記第1パーティ及び前記第2パーティの前記署名を含む。

【0204】

実施形態において、前記データ部分の夫々を含むという要件は、前記ロックングスクリプトに含まれているハッシュチャレンジによって生成されてもよく、該ハッシュチャレンジは、データの各々の部分のハッシュと、前記アンロックングスクリプトにおける各々のデータ部分のハッシュが前記ロックングスクリプトに含まれているハッシュと一致するこ

10

20

30

40

50

とをチェックするハッシュ関数とを有する。この場合に、方法は、前記ネットワークとは別に、前記第1トランザクションのインスタンスの受信より前に、ハッシュセットを前記第1パーティに利用可能にすることを有し、前記ハッシュセットは、前記第1パーティが各々のデータ部分について前記ハッシュチャレンジを生成することを可能にするためのデータの部分ごとのハッシュ値を有する。

【0205】

実施形態において、方法は、前記第2パーティが前記サイドチャンネル上で前記第1パーティから前記第1トランザクションを受信することを有してもよい。前記第1トランザクションは、入力量を指定する1つ以上の第1入力を含む。前記第1トランザクションの前記第1出力は、第1ペイメントを指定し、前記第1トランザクションは、ペイメントの合計が前記入力量よりも多くなるように1つ以上の更なるペイメントを指定する1つ以上の更なる出力を更に有し、前記第1パーティから前記第2パーティによって受信される前記第1トランザクションは、差を補うための他の入力を有さない。前記ネットワークの前記ノードは、前記第1トランザクションが総入力量よりも多い総ペイメントを指定する場合には無効であるとして前記第1トランザクションを拒絶するよう構成される。可能な実施形態で、方法は、前記第2パーティが、前記差を補うよう前記第1トランザクションの最新又は最後のインスタンスに第2入力を加え、該第2入力が増えられた前記第1トランザクションを、前記ネットワークを通じて伝播されて前記ブロックチェーンに記録されるよう送信することを有する。

【0206】

上記の実施例として、前記更なる出力は、前記入力量から前記第1ペイメントをマイナスしたものに等しい前記第1パーティへの第2ペイメントを指定する第2出力を含む。第3出力は、前記第2ペイメントに等しい前記第2パーティへの第3ペイメントを指定してもよい。

【0207】

実施形態において、前記ロッキングスクリプトは、前記代替条件のうちの第3条件を含んでもよく、該第3条件は、タイムアウト期間が経過していることと、前記第1パーティの暗号署名が前記アンロッキングスクリプトに含まれることを要求して、前記タイムアウト期間内に前記第2パーティによって精算されない場合に前記第1パーティが前記第1トランザクションの前記第1出力におけるペイメントを精算することを可能にする。

【0208】

本明細書で開示されている他の態様に従って、コンピュータ読み出し可能なストレージにおいて具現され、第2パーティのコンピュータ機器で実行される場合に、第2パーティ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。

【0209】

本明細書で開示されている他の態様に従って、1つ以上のメモリユニットを有するメモリと、1つ以上の処理ユニットを有する処理装置とを有し、前記メモリは、前記処理装置で実行されるよう配置されたコードを記憶し、該コードは、前記処理装置で実行される場合に、第2パーティ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。

【0210】

実施形態において、プログラム又はコードは、本明細書で開示されている第2パーティのステップのいずれかを実行するよう更に構成されてもよい。

【0211】

本明細書で開示されている他の態様に従って、ノードのネットワークの少なくとも一部の夫々で保持されているブロックチェーンのコピーにターゲットトランザクションを記録することを第2パーティに可能にする方法であって、

第1パーティのコンピュータ機器によって、

前記ネットワークとは別のサイドチャンネルを介して、前記第2パーティから連続したデータ部分のシーケンスを受信することと、

前記データ部分の各々のデータ部分に回答して、前記第1パーティから第1トランザク

10

20

30

40

50

ションの異なった各々のインスタンスを前記サイドチャネル上で返送することであり、前記第1トランザクションは、デジタルアセットの量を指定する第1出力を有し、前記ターゲットトランザクションは、前記第1トランザクションの前記第1出力へのポインタを含む入力を含み、前記ターゲットトランザクションは、前記第1トランザクションの前記第1出力から前記第2パーティへ転送すべき前記デジタルアセットの量を指定する出力を更に有し、前記第1トランザクションの前記第1出力で指定されている前記量は、前記第1トランザクションの連続するインスタンスごとに増大する、ことと

を有し、

それによって、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インスタンスのいずれか1つを、前記ネットワークにわたって伝播されて前記ブロックチェーンに記録されるよう送信することを可能にする、

方法が提供される。

【0212】

実施形態において、方法は、本明細書で開示されている第2パーティのステップのいずれかに相補的に対応する第1パーティのステップを更に有してもよい。

【0213】

本明細書で開示されている他の態様に従って、コンピュータ読み出し可能なストレージにおいて具現され、第1パーティのコンピュータ機器で実行される場合に、第1パーティ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。

【0214】

本明細書で開示されている他の態様に従って、1つ以上のメモリユニットを有するメモリと、1つ以上の処理ユニットを有する処理装置とを有し、前記メモリは、前記処理装置で実行されるよう配置されたコードを記憶し、該コードは、前記処理装置で実行される場合に、第1パーティ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。

【0215】

実施形態において、プログラム又はコードは、本明細書で開示されている第1パーティのステップのいずれかを実行するよう更に構成されてもよい。

【0216】

本明細書で開示されている他の態様に従って、ブロックチェーンでの記録のためのトランザクションの組であって、当該組は、1以上のコンピュータ可読データ媒体で具現されて、

第1トランザクションのインスタンスのシーケンスを最新のインスタンスまで有し、各インスタンスが、同じソーストランザクションの同じ出力を指す入力を含み、前記ソーストランザクションの前記出力が、第1パーティのデジタルアセットの量を指定し、前記第1トランザクションの各インスタンスが、前記デジタルアセットの量を指定する第1出力を更に有し、

前記第1トランザクションのインスタンスのうちの1つの前記第1出力へのポインタを含む入力を含み、ターゲットトランザクションを有し、該ターゲットトランザクションが、前記第1トランザクションの前記第1出力から第2パーティへ転送すべき前記デジタルアセットの量を指定する出力を更に有し、

前記第1トランザクションの前記第1出力で指定されている前記量は、前記第1トランザクションの連続するインスタンスごとに増大し、前記ターゲットトランザクションの対応するバージョンにおけるポインタは、前記シーケンスにおいて前記第1トランザクションの最新のインスタンスでの前記第1出力を指す、

前記トランザクションの組が提供される。

【0217】

開示されている教示の他の変形又は使用ケースは、本明細書での開示を鑑みて当業者に明らかになる。本開示の範囲は、記載されている実施形態によって限定されず、添付の特許請求の範囲によってのみ限定される。

10

20

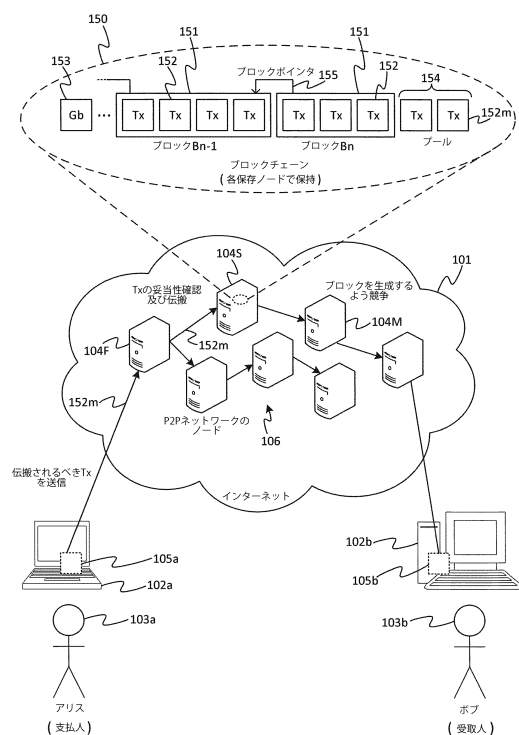
30

40

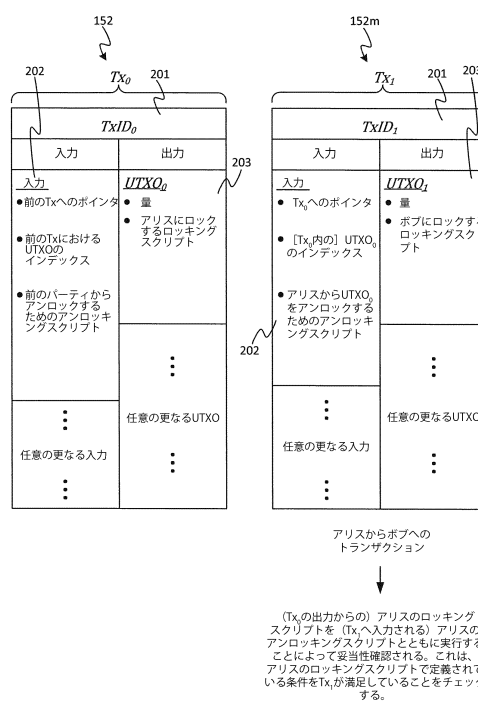
50

【図面】

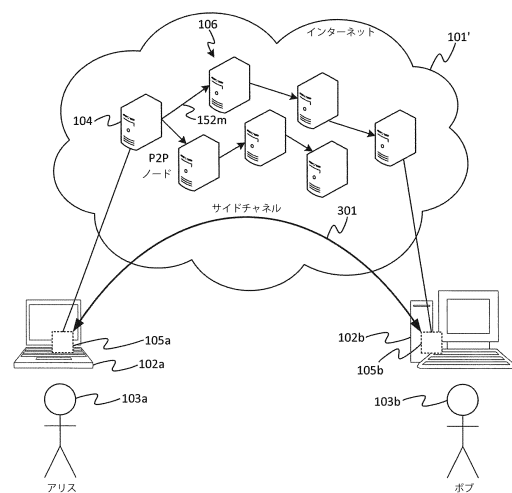
【図 1】



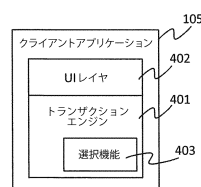
【図 2】



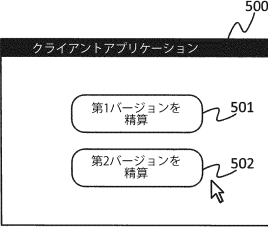
【図 3】



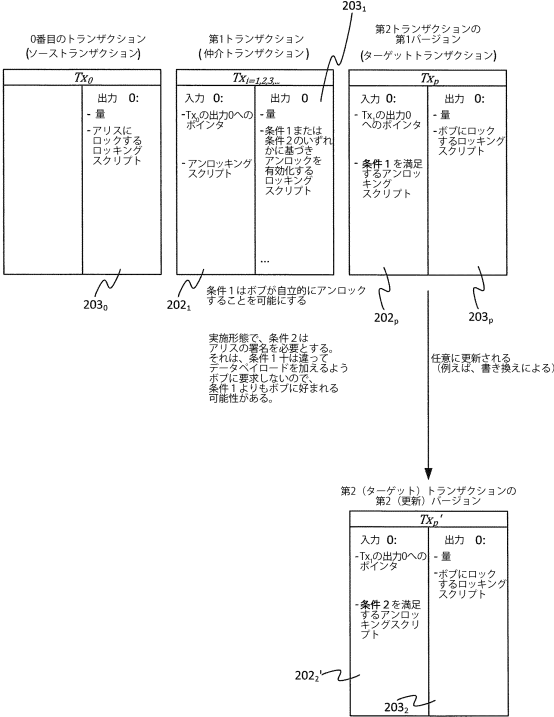
【図 4】



【図 5】



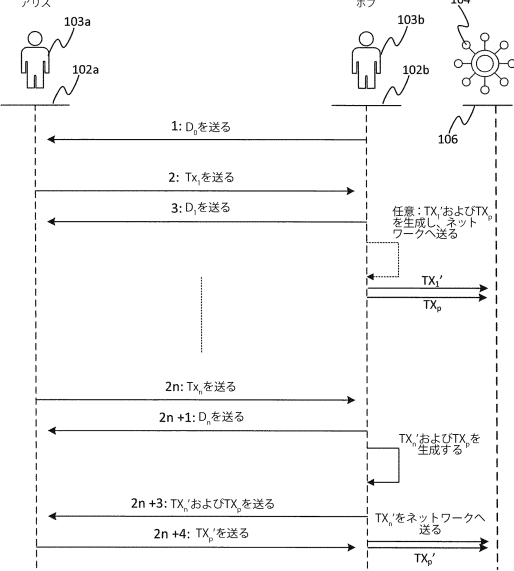
【図 6】



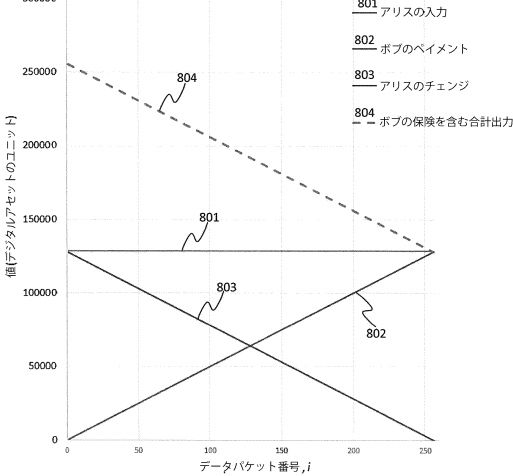
10

20

【図 7】



【図 8】

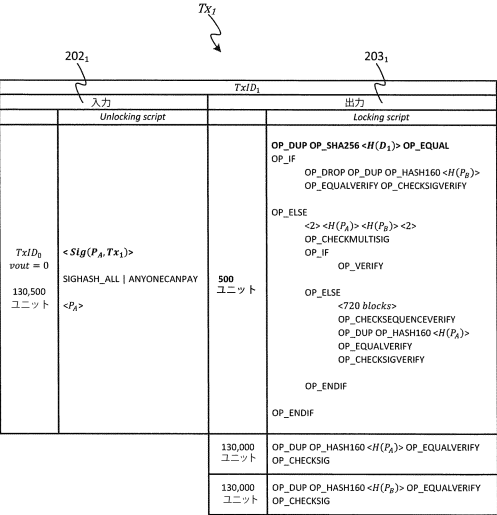


30

40

50

【図 9】



10

20

30

40

50

フロントページの続き

(72)発明者 デーヴィス, 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 中里 裕正

(56)参考文献 特表2019-511147 (JP, A)
 特許第6487091 (JP, B1)
 米国特許出願公開第2019/0028278 (US, A1)
 米国特許出願公開第2019/0058910 (US, A1)
 国際公開第2018/020389 (WO, A2)
 国際公開第2018/092443 (WO, A1)
 SHI, F., QIN, Z. and MCCANN, J. A., OPPay: Design and Implementation of A Payment System for Opportunistic Data Services, 2017 IEEE 37th International Conference on Distributed Computing Systems, 2017年06月, pp.1618-1628

(58)調査した分野 (Int.Cl., DB名)
 H04L 9/32
 G06F 21/10
 G06Q 20/38