

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号

特表2024-540123

(P2024-540123A)

(43)公表日 令和6年10月31日(2024.10.31)

(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 21/64 (2013.01)

G 0 6 F

21/64

審査請求 未請求 予備審査請求 未請求 (全69頁)

(21)出願番号 特願2024-525457(P2024-525457)  
(86)(22)出願日 令和4年10月25日(2022.10.25)  
(85)翻訳文提出日 令和6年6月25日(2024.6.25)  
(86)国際出願番号 PCT/EP2022/079837  
(87)国際公開番号 WO2023/072965  
(87)国際公開日 令和5年5月4日(2023.5.4)  
(31)優先権主張番号 2115511.4  
(32)優先日 令和3年10月28日(2021.10.28)  
(33)優先権主張国・地域又は機関  
英国(GB)  
(31)優先権主張番号 2115512.2  
(32)優先日 令和3年10月28日(2021.10.28)  
(33)優先権主張国・地域又は機関  
英国(GB)  
(31)優先権主張番号 2115516.3

最終頁に続く

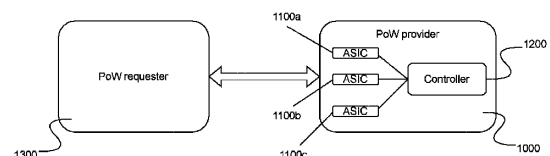
(71)出願人 318001991  
エヌチェーン ライセンシング アーゲー  
スイス・6 3 0 0・ツーク・グラフェ  
ナウヴェーク・6  
(74)代理人 100108453  
弁理士 村山 靖彦  
(74)代理人 100110364  
弁理士 実広 信哉  
(74)代理人 100133400  
弁理士 阿部 達彦  
(72)発明者  
クレイグ・スティーヴン・ライト  
イギリス・ロンドン・マーケット・プレ  
イス・3 0・エヌチェーン・ライセンシ  
ング・アーゲー内

(54)【発明の名称】 分散型ブロックチェーン機能のための方法およびシステム

## (57)【要約】

本開示は、データレコードの分散処理および/または並列処理、特にブロックチェーンブロック内のブロックチェーントランザクションのマイニング、さらになおブロックチェーンブロックに対するプルーフオブワーク(PoW)の生成のための方法およびシステムを提供する。有利には、実施形態は、PoW計算を他のブロックチェーンのマイニング/有効性確認タスクから分離することを可能にする。好ましくは、PoW要求者は、専門家であるPoW提供者に、i) トランザクションのセットを表すマークルツリーのマークルルート、ii) 制御トランザクション(TX<sub>0</sub>)、およびiii) TX<sub>0</sub>がトランザクションのセットに含まれることを確認するマークル証明のうちの1つまたは複数を送信する。TX<sub>0</sub>は、PoW提供者がPoW計算の実行がなされるべきかまたは完了しているかを決定するために使用することができる制御データを提供するか、または含み得る。

Figure 15



## 【特許請求の範囲】

## 【請求項 1】

コンピュータ実装方法であって、

第1のリソースから第2のリソースに、複数のトランザクションを収容するブロックチェーンブロックに対するプルーフオブワーク(PoW)を生成するための要求を送信するステップであって、前記要求は制御トランザクション(TX<sub>0</sub>)が前記複数のトランザクションに含まれることを検証するためのマークル証明を含む、ステップ、および/または

前記第1のリソースから前記第2のリソースにおいて、複数のトランザクションを収容するブロックチェーンブロックに対するプルーフオブワーク(PoW)を生成するための要求を受信するステップであって、前記要求は制御トランザクション(TX<sub>0</sub>)が前記複数のトランザクションに含まれることを検証するためのマークル証明を含む、ステップを含む、コンピュータ実装方法。

10

## 【請求項 2】

前記制御トランザクション(TX<sub>0</sub>)は、前記プルーフオブワークの生成の実行を制御し、許可し、および/または禁止するための制御データを含み、好ましくは前記制御データは、

i) ブロックチェーン移転のデスティネーションに対する所定のアドレスを指定する少なくとも1つの出力であって、

好ましくは、前記アドレスは、前記第2のリソース、または前記第2のリソースに関連付けられたもしくは前記第2のリソースによって認可された当事者に関連付けられる、出力、および/または

20

ii) 少なくとも1つの所定の署名、および/または

iii) 少なくとも1つの秘密値またはデータの秘密部分を含む、請求項1に記載のコンピュータ実装方法。

## 【請求項 3】

前記第1のリソースは、PoW要求リソース、ブロックチェーン有効性確認リソース、またはブロックチェーンマイニングリソースであり、および/または

前記第2のリソースは、プルーフオブワーク提供者であり、および/または

前記第2のリソースは、少なくとも1つのASIC、またはハッシュマシン、または専用暗号通貨マイニングリソースを含む、

30

請求項1または2に記載のコンピュータ実装方法。

## 【請求項 4】

i) 前記第2のリソースから前記第1のリソースにおいて、前記ブロックチェーンブロックに対するプルーフオブワークを受信するステップ、および/または

ii) 前記第2のリソースから前記第1のリソースに、前記ブロックチェーンブロックに対するプルーフオブワークを送信するステップ

をさらに含む、請求項1から3のいずれか一項に記載のコンピュータ実装方法。

## 【請求項 5】

前記プルーフオブワークは、

ブロックチェーンプロトコルによって指定されたターゲット、ルール、または基準のうちの1つもしくは複数を満たす出力を提供するように構成された値(ノンス)、および/または

40

前記ブロックチェーンブロックに対するブロックヘッダ、および/または

ブロックチェーンプロトコルに従って指定されたパズルまたはチャレンジの解を含む、請求項1から4のいずれか一項に記載のコンピュータ実装方法。

## 【請求項 6】

前記プルーフオブワークを生成するステップは、

i) ブロックチェーンプロトコルによって指定されたターゲット、チャレンジ、ルール、または基準を満たす出力を提供するように構成された値(ノンス)を生成するか、もしくは選択するステップ、

50

ii)前記ブロックチェーンブロックに対するブロックメッセージとノンスとを連結するステップ、および/または

iii)前記ブロックチェーンブロックに対するブロックヘッダをダブルハッシュ化するステップ

を含む、請求項1から5のいずれか一項に記載のコンピュータ実装方法。

【請求項7】

事前定義された制御基準に関して前記制御トランザクション(TX<sub>0</sub>)の少なくとも一部を処理するか、もしくは比較し、前記処理もしくは比較の出力に基づき前記プルーフオブワークを生成するか、もしくは生成しないステップを含み、

好ましくは、前記制御基準は、開始、実行もしくは完了、または前記プルーフオブワークの生成を可能にするための閾値、ルール、または基準のうちの少なくとも1つを含む、請求項1から6のいずれか一項に記載のコンピュータ実装方法。

【請求項8】

前記プルーフオブワークの前記生成を許可するか、または禁止することを、

i)前記制御トランザクション(TX<sub>0</sub>)が前記複数のトランザクションに含まれることの確認の成功もしくは失敗、および/または

ii)前記制御トランザクションが、所定のルールもしくは基準を満たすデータの一部を含むか、もしくは含まないことの決定、および/または

iii)前記制御トランザクションもしくはそのの少なくとも一部が前記制御基準を満たすという決定に基づき行うステップ

をさらに含む、請求項7に記載のコンピュータ実装方法。

【請求項9】

前記第1もしくは第2のリソースにおいて、ブロックに対するプルーフオブワークの生成のためにブロックチェーンプロトコルによって必要とされるデータの一部を決定するステップを含み、データの前記一部は

プロトコルバージョン識別子、

ブロックハッシュ、

前記プロトコルによって指定されたプルーフオブワーク難易度ターゲット、および/または

タイムスタンプ

のうちの1つもしくは複数を含む、請求項1から8のいずれか一項に記載のコンピュータ実装方法。

【請求項10】

i)前記マール証明は、前記制御トランザクションが前記複数のトランザクションに含まれるかどうかを決定するためのSPV検証の実行を可能にするように構成されたデータを含み、

ii)前記要求は、前記制御トランザクションを含む、

請求項1から9のいずれか一項に記載のコンピュータ実装方法。

【請求項11】

前記複数のトランザクションを処理してマールツリーを提供するステップを含み、

好ましくは、前記処理は、ハッシュ関数を伴う、

請求項1から10のいずれか一項に記載のコンピュータ実装方法。

【請求項12】

前記制御トランザクション(TX<sub>0</sub>)は、前記第2のリソースが前記第1のリソースを識別することを可能にする識別子を含み、好ましくは、前記識別子は、前記制御トランザクションの入力、出力、スクリプト、またはメタデータ部分で提供される、請求項1から11のいずれか一項に記載のコンピュータ実装方法。

【請求項13】

複数のトランザクションを収容するブロックチェーンブロックに対するプルーフオブワークの前記生成を制御するかまたはそれに影響を及ぼすように動作可能であり、および/

10

20

30

40

50

または請求項1から12のいずれか一項に記載の方法を実装するように動作可能である、システム。

【請求項14】

少なくとも1つのプルーフオブワーク提供リソース(1000)であって、

好ましくは、前記少なくとも1つのプルーフオブワーク提供リソースは、少なくとも1つのASICまたはハッシュマシン(1100aから1100c)を含む、少なくとも1つのプルーフオブワーク提供リソース(1000)、

少なくとも1つのプルーフオブワーク要求リソース(1300)であって、

好ましくは前記少なくとも1つのプルーフオブワーク要求リソースは、本明細書において実質的に開示されている分散有効性確認ノード(700)を含む、少なくとも1つのプルーフオブワーク要求リソース(1300)

のうちの少なくとも一方を備える、請求項13に記載のシステム。

【請求項15】

コンピュータシステムのプロセッサによって実行された結果として、請求項1から13のいずれか一項に記載の前記コンピュータ実装方法を前記コンピュータシステムに実行させるか、または前記コンピュータシステムが実行することを可能にする実行可能命令をその上に記憶した、非一時的コンピュータ可読記憶媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、一般的に、関係するもしくは関連するデータレコードを処理するための改善された方法およびシステム、ならびに/または分散ネットワークの実装に関する。本開示は、限定はしないが、ブロックチェーントランザクションのマイニング前および/またはマイニング後有効性確認(pre and/or post mining validation)、SPVチェックなど、ブロックチェーンネットワーク上で、またはブロックチェーンネットワークを使用して、実施される移転に関する使用に特に適している。利点は、限定はしないが、セキュリティおよびレジリエンスの改善、速度およびリソース要件の効率化または削減、ならびに従来技術の構成では可能でなかった有効性確認への新規性のあるアプローチを含み、したがって、結果として以前には可能でなかったブロックチェーン実装構成が可能になる。

【背景技術】

【0002】

ビットコインプロトコルおよびネットワークは、実装のための例示的なコンテキストを提供することを目的として本明細書において参照されることがあるが、本開示は、ビットコインブロックチェーンとの使用に限定されず、代替的プロトコルおよび実装(アカウントベースのものおよびプルーフオブステークコンセンサスを含むものを含む)もその範囲に入る。以下では、「UTXO」という用語は、純粹に便宜上、トランザクション出力を指し示すために使用されるものとしてよく、本開示の実施形態がUTXOベースのブロックチェーンモデルに関する使用に限定されることを意味するものとして解釈されるべきではない。

【0003】

ブロックチェーンは、コンピュータベースの非集中的な分散型システムとして実装されるピアツーピア電子台帳であり、これはブロックから構成され、さらにブロックはトランザクションから構成される。各トランザクションは、ブロックチェーンシステム内の参加者間でのデジタル資産の制御の移転を符号化したデータ構造であり、少なくとも1つの入力と少なくとも1つの出力とを含む。各ブロックは、前のブロックのハッシュを含み、ブロックが連鎖することで、ブロックチェーンの開始以来、ブロックチェーンに書き込まれたすべてのトランザクションの永久的変更不可能な記録を作成する。

【0004】

トランザクション(Tx)がブロックチェーンに書き込まれるためには、これは、有効性確認がなされなければならない。ネットワークノード(マイナー)は、各トランザクション

10

20

30

40

50

が有効であることを確認する作業を実行し、無効なトランザクションはネットワークから拒絶される。いくつかのプロトコルでは、ノード上にインストールされたソフトウェアクライアントは、ロックスクリプトおよびロック解除スクリプトを実行することによって未消費(unspent)トランザクション(UTXO)に対してこの有効性確認作業を実行する。ロックスクリプトおよびロック解除スクリプトの実行結果がTRUEと評価された場合、トランザクションは有効であり、トランザクションはブロックチェーンに書き込まれる。したがって、トランザクションがブロックチェーンに書き込まれるためには、i)トランザクションを受信した最初のノードによって有効性確認される--トランザクションが有効であると確認された場合、ノードはそのトランザクションをネットワーク内の他のノードに中継する、すなわちトランザクションは伝搬される--こと、ii)マイナーによって構築された新しいブロックに追加されること、iii)マイニングされること、すなわち過去のトランザクションのパブリック台帳に追加されることが、トランザクションに対して行われなければならない。トランザクションがUTXOとしてブロックチェーン内に保管された後、ユーザは関連する暗号通貨の制御を、その後ブロックチェーンに書き込まれる別のトランザクションの入力に関連付けられている別のアドレスに移転することができる。これは、ユーザの暗号通貨に関連付けられた公開鍵と秘密鍵のペアを保管するデジタルウォレットを使用して行われることが多い。知られている暗号通貨ウォレットには、SPVウォレット(Simplified Payment Verification)を含む、様々な形態のものがある。SPV技術は、ユーザおよびマーチャントノードが、特定の送金に関連する部分的情報のみに基づきローカル検証を実行することを可能にする。SPVは、以下でさらに詳しく説明される。

10

20

#### 【0005】

しかしながら、セキュリティ、所与のブロックチェーンに対する関連するプロトコルへの適合性、および二重支払いエクスプロイト(double spends exploit)からの保護を確実にする上で検証が不可欠である一方で、ブロックをダウンロードして保存し、大規模なUTXOプールを維持し、検証に必要な処理タスクを実行する必要があることに起因して、このような有効性確認タスクは著しいリソースおよび時間を必要とし得ることが認識されている。多くのユーザは、そのような要件を満たすことができないか、または場合によっては要件を満たす必要がないのでそうすることを望まない。したがって、セキュリティを侵害すること、既存のプロトコルを適応させることなく、少なくともこれらのチャレンジ(およびその他のもの)に対処する、より高速で効率的な検証モデルが必要とされている。

30

#### 【0006】

そこで、そのような改善されたソリューションが考案された。

#### 【発明の概要】

#### 【課題を解決するための手段】

#### 【0007】

本開示の実施形態は、改善されたブロックチェーン関係の方法、デバイス、およびシステムを提供するものである。一表現形式によれば、そのような実施形態は、ブロックチェーントランザクションおよび/またはブロックチェーンブロックの一部または全体の有効性確認を行うまたはマイニングのためのソリューションを提供する。追加のまたは代替的な表現形式によれば、ブロックチェーントランザクションの処理に対する知られているアプローチの効率、リソース要件、速度、および/またはレジリエンスを制御し、管理し、および/または増強するための安全なソリューションを提供する。実施形態は、また、ブロックチェーン実装ソリューションのスケーラビリティを可能にし、デジタルリソースの電子移転(electronic transfer)のための改善された方法および技術的アーキテクチャを提供する。実施形態は、ブロックチェーンブロックに対するプルーフオブワークの計算/生成を、分散および/または並列方式で可能にし、および/または制御するための方法も含み得る。

40

#### 【0008】

本開示の実施形態は、様々な装置によって部分的にまたは全体的に実装され得る。これらは、1つまたは複数の仮想マシン、サーバ、GPUベースのコンピューティングリソース

50

、またはマルチプロセッサシステムを(限定はしないが)含む、ハードウェアおよび/またはソフトウェアベースの装置であってよい。それに加えて、または代替的に、実施形態は、1つまたは複数のデジタルウォレットを含み得る。しかしながら、重要なことに、実施形態はブロックチェーン関係の有効性確認タスクを分散処理するためのメカニズムを提供する。分散プロセスの協調、管理、および制御は、関わっているハードウェアコンポーネントおよびソフトウェアコンポーネントの間のインタラクションの全体論的な理解を必要とするので、本来、本質的に技術的であることが知られており、そのような分散ソリューションの実装は、技術的些末を超えるものである。

【0009】

実施形態は、複数の処理リソースにわたるマイニングタスクの分散を可能にするか、または円滑にするソリューションを含み得る。

【0010】

本開示の実施形態は、「分散マイニング」と題されたセクションに関して本明細書で説明され、例示され、特許請求されるような方法およびシステムを含み得る。そのような実施形態は、トランザクションの特定の複数の(セット)を含むブロックチェーンブロックに対するプルーフオブワーク(PoW)の生成の要求を認可し、制御し、認可を確立し、または他の方法で定式化するための技術を含み得る。好ましくは、このセットは、プルーフオブワーク提供者(Proof-of-Work provider)が、要求されたPoW労力(PoW effort)が開始されるべきか、実行されるべきか、および/または履行されるべきかどうかを決定するために使用することができる制御データの少なくとも一部分を含むトランザクションを含む。これは「制御トランザクション」(TX<sub>0</sub>)と呼ばれ得る。要求は、また、PoW提供者がTX<sub>0</sub>が複数のトランザクションに含まれることを決定するために使用することができるデータを含み得る。好ましい実施形態において、これは、マークル証明、制御トランザクション(TX<sub>0</sub>)、および/またはトランザクションのセットを表すマークルツリーのルートの中の少なくとも1つもしくは複数を含み得る。PoW提供者は、少なくとも1つの事前指定されたルール、基準、または要件を併用して、a)制御トランザクションがセットに含まれる、および/またはb)使用され得る制御データの少なくとも1つの部分を含むことを確実にするための要求を処理し、要求済みPoW労力の作業が開始されるべきか、実行されるべきか、および/または履行されるべきかどうかを決定することができる。

【0011】

これらを組み合わせて、PoW要求者(PoW requester)およびPoW提供者は、分散ブロックチェーンマイニングノードを提供するものとしてよい。実施形態は、ブロックチェーントランザクションの有効性確認および/またはマイニングに関わる様々な機能およびタスクを分離し、分散させ、並列化する能力を提供する。

【0012】

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、添付の図面が参照される。

【図面の簡単な説明】

【0013】

【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得るトランザクションのいくつかの例の概略を例示する図である。

【図3】当技術分野で知られているような一般的なマークルツリー構造を例示する図である。

【図4】当技術分野で知られているように、ブロックチェーントランザクションのセットからマークルルートがどのように導出され得るかを示す図である。

【図5】本開示の一実施形態によるそれぞれの有効性確認リソースにその後割り当てられ得るサブセット(または「セグメント」)にマークルツリーがどのように分割され得るかを示す例示的な図である。

10

20

30

40

50

【図6】マークルツリーが論理セグメントにどのように分割され得るかを示す図5の代替的例を例示する図である。

【図7】本開示の例示的な一実施形態による分散有効性確認ノードをシステムレベルで例示する図である。

【図8】本開示の例示的な方法に関わるステップを高水準で示すフローチャートである。

【図9】図7の例示的なシステムをより詳細に示す図である。

【図10】本開示の好ましい一実施形態の高水準の概要を提示する図である。

【図11】当該技術分野で知られているように、ブロックチェーンネットワーク上のノードによって実行される有効性確認およびマイニング活動に対する従来のアプローチを例示する図である。

【図12】本開示の好ましい一実施形態による、図2の従来のタスクが異なるエンティティ間にどのように分散され得るかを例示する図である。

【図13】本開示の好ましい一実施形態によるPoW要求者によって実行される典型的なタスクの一例を示す図である。

【図14】本開示の好ましい一実施形態によるPoW提供者によって実行される典型的なタスクの一例を示す図である。

【図15】本開示の例示的な一実施形態による分散マイニングノードを例示する図である。

【発明を実施するための形態】

【0014】

われわれは、次に、限定することなく、例示することを目的とし、添付の図を参照しつつ、本開示の例示的な実施形態を説明する。

【0015】

従来、ブロックチェーンネットワーク内のノードは、ブロックチェーン上のすべてのトランザクションのグローバル台帳を維持する。グローバル台帳は分散型台帳であり、各ノードはグローバル台帳の完全コピーまたは部分的コピーを保存し得る。グローバル台帳に影響を及ぼすノードによるトランザクションは、他のノードによって検証され、それによりグローバル台帳の有効性および完全性は維持される。ビットコインプロトコルを使用するものなどの、ブロックチェーンネットワークの実装、および運用の詳細は、当業者であれば理解するであろう。

【0016】

各トランザクションは、典型的には、1つまたは複数の入力および1つまたは複数の出力を有する。入力および出力に埋め込まれたスクリプトは、トランザクションの出力がどのように誰によってアクセスされ得るかを指定する。トランザクションの出力は、トランザクションの結果として価値の制御が移転される先のアドレスであってよい。その価値は、次いで、未消費トランザクション出力(UTXO)としてその出力アドレスに関連付けられる。次いで、後続のトランザクションは、その価値の制御または所有権を取得するために入力としてそのアドレスを参照し得る。

【0017】

上述のように、ビットコインのネットワークおよびプロトコルを使用するわれわれの例では、マイニングノードは、ブロックチェーン内の次のブロックを作成する競争に参加する。ブロックを組み立てるために、マイナーは、未承認トランザクションのプール(「mempool」)からトランザクションのセットとしてブロックを構築する。次いで、マイナーは、組み立てたブロックに関してプルーフオブワーク(PoW)パズルを完成することを試みる。他のマイナーがそれ自身のブロックを生成しPoWを完成することに成功したという通知を受信するのに先立ちPoWを完成することを管理する場合、マイナーは、そのブロックをネットワーク上のピアノードに送信することによって伝搬する。それらのノードはブロックを有効性確認し、次いでそれをさらにネットワーク上の他のノードに送信する。マイナーが自身のPoWを終了するのに先立ち別のブロックが完了しているという通知を受信した場合、マイナーは、その作業を放棄し、次のブロックを構築する試みを始める

10

20

30

40

50

。

## 【0018】

したがって、ブロックの高速伝搬は、マイナーおよび有効性確認ノードに代わって無駄な労力(および関連するエネルギー)を回避するのに役立つ。ブロックのより高速な有効性確認およびしたがって伝搬を可能にするソリューションを提供することによって、本発明は、増強されたネットワーク性能を提供する。計算時間の量と必要な労力を削減し、したがってネットワークに必要なエネルギーの量を減らす。これはリソースおよび時間に関してより効率的なネットワークを提供する。これは、最終的に、改善された(ブロックチェーン)ネットワークを提供する。

## 【0019】

ビットコインネットワークなどの、現在のブロックチェーンの実装形態において、ブロックを受信した各ノードは、最初に、他のノードに送信する前にブロックを有効性確認する。ブロックの有効性確認に時間がかかると、ネットワークを通るブロックの伝搬が遅くなる。既存のプロトコルの進化を含む、ブロックチェーンのいくつかの実装形態は、ネットワーク内の各ノードではなくむしろ、ノードのサブセットのみによるブロック有効性確認を提供するが、大半のノードにおけるブロック有効性確認は、それでも、無効なブロックがネットワークを通して伝搬するのを防ぐブロックチェーンの実装形態の一特徴である可能性が高いことに留意されたい。

## 【0020】

ブロックを有効性確認することは、適用可能なブロックチェーンプロトコルによって設定されている規定された基準をブロックが満たしていることを確認することを伴う。ビットコインプロトコルに適用可能な例示的な基準は、CheckBlockおよびCheckBlockHeaderなどの関数を含み得る。ブロックそれ自体が規定された基準に適合していることを確認することに加えて、ブロック内の各トランザクションは、トランザクションレベルの基準に適合しているかについて評価され得る。一例として、ビットコインプロトコルで適用されるトランザクションレベルの基準は、関数AcceptToMemoryPool、CheckTransaction、およびCheckInputsを含み得る。

## 【0021】

ビットコインプロトコルに基づくブロックレベルの基準の具体的な例は、以下を含むものとしてよい。

- ・ブロックデータ構造は、構文的に有効である。
- ・ブロックヘッダハッシュは、ターゲット難易度(プルーフオブワークを強制する)未満である。
- ・ブロックのタイムスタンプは、2時間以内の未来である(時間の誤差を許容する)。
- ・ブロックサイズは、許容範囲内にある。
- ・最初のトランザクション(そして最初のトランザクションのみ)がコインベース生成トランザクションである。
- ・ブロック内のすべてのトランザクションは、有効である。

## 【0022】

ビットコインプロトコルに基づくトランザクションレベルの基準の具体的な例は、以下を含むものとしてよい。

- ・トランザクションの構文およびデータ構造は、正しくなければならない。
- ・入力または出力のリストも空ではない。
- ・各出力値 $x$ 、さらにはすべての出力の合計は、 $0 < x < 21 \cdot 10^6$ の範囲内になければならない。
- ・入力はどれもNULLハッシュを有しない。
- ・`nLockTime`は、`INT_MAX`以下である。
- ・バイト単位のトランザクションサイズは、最小値以上、最大値以下である。
- ・署名演算の回数は、署名演算上限数未満である。
- ・ロック解除スクリプト`scriptSig`はスタックに数値のみをプッシュすることができ、

10

20

30

40

50

ロックスクリプトscriptPubkeyはisStandard形式と一致しなければならない。

- ・各入力について、参照される出力がプール内の任意の他のトランザクション内に存在する場合、そのトランザクションは、拒絶されなければならない。

- ・各入力について、参照される出力トランザクションがコインベース出力である場合、少なくともCOINBASE\_MATURITY(100)の確認を有していなければならない。

- ・各入力について、参照される出力は存在していなければならない、すでに消費されていることはあってはならない。

- ・参照される出力トランザクションを使用して入力値を取得し、各入力値、さらには合計が値xの許容される範囲内、すなわち $0 < x < 21 \cdot 10^6$ にあることをチェックする。

- ・プール内または主分岐内のブロック内に一致するトランザクションが存在していなければならない。

- ・入力値の合計は、出力値の合計以上でなければならない。

- ・トランザクション手数料は、空のブロックに入るのに十分でなければならない。

- ・各入力に対するロック解除スクリプトは、対応する出力ロックスクリプトと突き合わせて有効性確認しなければならない。

#### 【0023】

これらの例示的な基準は例示的であり、規定された基準は異なるプロトコルでは異なることがあり、プロトコルに変更が加えられた場合に所与のプロトコルに対して時間の経過とともに変化することがあるのですべての実施形態に対して十分であるまたは必要であると解釈されるべきではない。一般に、トランザクションレベルの有効性確認基準は、適用可能なブロックチェーンプロトコルの下で有効であるとみなされるためにトランザクションが有していなければならない規定された特性である。同様に、ブロックレベルの有効性確認基準は、適用可能なブロックチェーンプロトコルの下で有効であるとみなされるためにブロックが有していなければならない規定された特性である。

#### 【0024】

本出願により、ネットワークにおけるブロックのより高速な伝搬を促進するようにブロック有効性確認をスピードアップする方法およびデバイスが説明される。

#### 【0025】

一態様では、本出願は、個別のトランザクションの少なくともトランザクションレベル有効性確認を並行して、および/または分散方式で実行することによってブロックを有効性確認するように構造化されたノードを説明する。しかしながら、特定のトランザクションレベルの基準は、並列で評価され得ない。たとえば、UTXOの一意性は直列ベースで評価され得る。そのような場合、本開示の分散有効性確認ノードは、残りのトランザクションレベル基準の有効性確認のために2つまたはそれ以上の並列プロセッサのセットの間でトランザクションのセットを割り当てるのに先立ち、トランザクションの参照入力(UTXO)の一意性を確認するように構造化されるかまたは構成され得る。

#### 【0026】

特に、本開示の実施形態は、ツリー構造に保存される関係するまたは関連するデータレコードを処理するための、改善された検証およびセキュリティソリューションを提供する。ツリーは、二分木またはメッシュ構造とすることができる。当技術分野で知られているように、ツリー構造は、より小さなツリー(本明細書では、ツリーの「セグメント」、「サブセット」、または「部分」と称され得る)に分解することができ、各セグメントは、ツリー全体のデータレコードのサブセットを含み、それ自身のルートを持有する。有利には、本開示の実施形態は、この特徴を利用して、複数の処理リソースにわたる関係するデータレコードの処理の分散化および並列化のための方法およびシステムを提供する。

#### 【0027】

われわれの例示的な実施形態では、複数のデータレコードは、マークルツリー内のノードを形成するので関係するブロックチェーントランザクションを含む。マークルツリーは、ブロックチェーンプロトコルに従ってトランザクションのブロックのヘッダに含まれているか、または含まれ得るルートを持有し、ルートはツリー内のすべてのリーフ(すなわち

10

20

30

40

50

トランザクションID(TxID))に辿って到達できる経路を提供する。われわれの例では、ブロックチェーンプロトコルは、ビットコインプロトコルであるか、ビットコインプロトコルから派生したものであるが、他のプロトコルも本開示の範囲に含まれる。

【0028】

われわれの例では、複数のトランザクションの処理は、複数のブロックチェーントランザクションを含むブロックチェーンブロックの少なくとも一部、およびそのブロックに対するマークルツリーのルートを有効性確認することを含む。これらの例は非限定的なものであり、本明細書において開示されている技術は、非ブロックチェーン関係データに関して、および/または有効性確認以外の他のプロセスに関して利用され得る。たとえば、実施形態は、マークルツリーで表され得る任意のタイプのデータレコードを保存し、構造化し、検索し、および/または維持するために使用され得る。ブロックチェーン台帳の代わりに、またはさらにブロックチェーン台帳とともに、データベースおよび他の知られているストレージリソースが利用され得る。

【0029】

別の例示的な実施形態では、複数のトランザクションの処理は、複数のブロックチェーントランザクションを含むブロックチェーンブロックの少なくとも一部、およびそのブロックに対するマークルツリーのルートをダウンロードすることを含む。

【0030】

完全を期するため、図3および図4を参照しつつ、われわれは、マークルツリーおよびブロックチェーントランザクションのブロックを表現する際のマークルツリーの使用についての詳解を提示する。

【0031】

マークルツリー

図3を参照すると、マークルツリーは、データの集まりを安全に検証することを可能にする階層データ構造である。マークルツリーにおいて、ツリー内の各ノードは、インデックスペア(i,j)を与えられており、N(i,j)として表される。インデックスi、jは、ツリー内の特定の位置に関係する単なる数値ラベルである。

【0032】

マークルツリーの特徴は、そのノードの各々の構造が、式

【0033】

【数1】

$$N(i,j) = \begin{cases} H(D_i) & i = j \\ H(N(i,k) \parallel N(k+1,j)) & i \neq j \end{cases}$$

【0034】

で決められることであり、

ここで、そして、Hは暗号学的ハッシュ関数である。

【0035】

これらの式に従って形成されるバイナリマークルツリーの一例が図3に示されている。図示されているように、i=jの場合はリーフノードに対応し、これは単にi番目データパケットD<sub>i</sub>のハッシュであることがわかる。i≠jの場合は内部または親ノードに対応し、これは1つの親(マークルルート)が見つかるまで子ノードを再帰的にハッシュ化して連結することによって生成される。

【0036】

たとえば、ノードN(0,3)は、4つのデータパケットD<sub>0</sub>,...,D<sub>3</sub>から以下のように構築される。

$$\begin{aligned} N(0,3) &= H(N(0,1) \parallel N(2,3)) \\ &= [H(N(0,0) \parallel N(1,1)) \parallel H(N(2,2) \parallel N(3,3))] \\ &= [H(H(D_0) \parallel H(D_1)) \parallel H(H(D_2) \parallel H(D_3))] \end{aligned}$$

10

20

30

40

50

## 【0037】

ツリーの深さ $M$ は、ツリーにおけるノードの最低レベルとして定義され、ノードの深さ $m$ は、そのノードが存在するレベルである。たとえば、 $m_{\text{root}}=0$ および $m_{\text{leaf}}=M$ であり、図3では $M=3$ である。

## 【0038】

ビットコインおよびいくつかの他のブロックチェーンにおけるマークルツリーについては、ハッシュ関数は、ダブルSHA256であり、これは標準ハッシュ関数SHA-256を2回適用するものである。

$$H(x) = \text{SHA256}(\text{SHA256}(x))$$

## 【0039】

マークルツリーの主な機能は、あるデータパケット $D_i$ が $N$ 個のデータパケット $D \in \{D_0, \dots, D_{N-1}\}$ のリストまたはセットのメンバーであることを検証することである。検証に対するメカニズムは、マークル証明として知られており、所与のデータパケット $D_i$ およびマークルルート $R$ に対するマークル経路として知られているハッシュのセットを取得することを伴う。データパケットに対するマークル証明は、単純に、ハッシュ化と連結とを繰り返すことによってルート $R$ を再構成するのに必要なハッシュの最小リストであり、しばしば「認証証明」と称される。

## 【0040】

存在証明は、すべてのパケット $D_0, \dots, D_{N-1}$ およびその順序が証明者に知られている場合、自明に実行される可能性がある。しかしながら、これは、マークル証明よりも非常に大きいストレージオーバーヘッドを要求するが、さらにはデータセット全体が証明者に利用可能であることを要求する。マークル証明を使用することとリスト全体を使用することとの比較は以下の表に示されており、われわれは、バイナリマークルツリーを使用し、データブロックの数 $N$ が2の整数乗に正確に等しいと仮定している。

## 【0041】

次の表は、マークルツリー内のリーフノードの数と、マークル証明に必要なハッシュの数(またはマークル証明)との関係を示している。

## 【0042】

【表1】

|               |    |     |      |         | マークルツリー        |
|---------------|----|-----|------|---------|----------------|
| データパケット数      | 32 | 256 | 1024 | 1048576 | $N = 2^M$      |
| 存在証明に必要なハッシュ数 | 5  | 8   | 10   | 20      | $M = \log_2 N$ |

## 【0043】

この簡略化されたシナリオ--データパケットの数がリーフノードの数に等しい--において、われわれは、マークル証明を計算するのに必要なハッシュ値の数は対数的に増加することを見だした。 $N$ 個のデータハッシュを保存して明示的証明を計算するよりも、 $\log_2 N$ 個のハッシュを伴うマークル証明を計算する方がはるかに効率的であり実用的であることは明らかである。

## 【0044】

マークルルート $R$ が与えられたとして、データブロック $D_0$ が $R$ で表される順序付きリスト $D \in \{D_0, \dots, D_{N-1}\}$ に属することを証明したい場合、次のようにマークル証明を実行することができる。

i. 信頼できるソースからマークルルート $R$ を取得する。

ii. ソースからマークル証明 $\Gamma$ を取得する。この場合、 $\Gamma$ はハッシュのセットである。

$$\Gamma = \{N(1,1), N(2,3), N(4,7)\}$$

iii.  $D_1$ および $\Gamma$ を使用して、次のようにマークル証明を計算する。

a. データブロックをハッシュ化して

$$N(0,0)=H(D_0)$$

を得る。

b.  $N(1,1)$ と連結し、ハッシュ化して

$$N(0,1)=H(N(0,0) \parallel N(1,1))$$

を得る。

c.  $N(2,3)$ と連結し、ハッシュ化して

$$N(0,3)=H(N(0,1) \parallel N(2,3))$$

を得る。

d.  $N(4,7)$ と連結し、ハッシュ化してルート

$$N(0,7)=H(N(0,3) \parallel N(4,7)),$$

$$R'=N(0,7)$$

を得る。

e. 計算されたルート $R'$ と(i)で得られたルート $R$ とを比較する。

1.  $R'=R$ である場合、ツリーにおける $D_0$ の存在、したがってデータセット $D$ は確認される。

2.  $R' \neq R$ である場合、証明は失敗し、 $D_0$ が $D$ のメンバーであることは確認されない。

【0045】

これは、マークルツリーとそのルートで表されるデータセットの一部として、あるデータに対する存在の証明を提供するための効率的なメカニズムである。たとえば、データ $D_0$ がブロックチェーンのトランザクションに対応し、ルート $R$ がブロックヘッダの一部として公に利用可能である場合、そのトランザクションがそのブロックに含まれていたことを迅速に証明することができる。

【0046】

SPV

Simplified Payment Verification (SPV)は、サトシ・ナカモトが2008年に発表したホワイトペーパー「Bitcoin: A Peer-to-Peer Electronic Cash System」の第8節で初めて示されたように、マークルツリーのこれらの特徴をうまく利用している。アリスとボブとの間のSPVベースの暗号通貨交換では、両者は同じタイプのSPVウォレットを使用する。SPVウォレットは、ユーザの秘密鍵および公開鍵、未消費トランザクション、およびブロックを一意に識別するブロックヘッダを保存し、これによりブロックチェーン上に配置され得る。説明されているように、ブロックヘッダは、ブロック全体の内容の一意的な要約またはフィンガープリントを提供するデータのフィールド、さらにはそのブロックに対するマークルルートを提供するフィールドを含む。マークルルートは、ブロックからトランザクションID (TxID) のペアを、最終的に単一のハッシュに到達するまで繰り返しハッシュ化することによって生成される。マークルルートは、トランザクションがブロックの一部であることを検証するための効率的で安全なメカニズムを提供するが、それは、ウォレットおよびマーチャントノードなどのユーザがブロックチェーン全体をダウンロードすることなく特定のトランザクションをローカルで検証することを可能にするからである。これは、フルノードを実行することを必要としない、または実行することを望んでいないが、単純に特定のトランザクションが特定のブロックにあるかどうか局所的チェックを実行する必要があるユーザ、たとえば、マーチャントと顧客との間の送金の実行を望んでいるマーチャントおよび顧客などの当事者にとって有利である。要約すると、SPVは、そのようなユーザが所与のルートに有するマークルツリーを検索し、ブロックチェーン全体をダウンロードして保存する必要なく特定のトランザクションが特定のブロックチェーンブロック内に含まれているかどうかをチェック(すなわち検証)することを可能にする。

【0047】

したがって、SPVウォレットは、他の形式のウォレットのようにブロックチェーンの完全なチェックを実行するのではなく、トランザクションが検証されていることを確認す

10

20

30

40

50

るだけでよいので(したがって「simplified payment verification」という名前がついている)、少なくとも、携帯電話およびラップトップなどの電力およびストレージに制約のあるデバイスがビットコインエコシステム内で動作することができるという利点を提供する。SPVウォレットは、トランザクションのどれも含むことなくブロックヘッダのみをダウンロードするので、これは、検証に必要な記憶域、エネルギー、および処理リソースを著しく削減する。SPVウォレットは、以下で説明されている理由により本開示の実施形態との使用に特に適しており、本明細書において「検証」という用語をSPVチェックを含むように使用する。

【0048】

#### トランザクションのブロック

図4は、ブロックチェーンブロックの一例の概略を例示する。各ブロックは、ブロックヘッダとトランザクションのセットを収容する。ブロックヘッダは、ほかにもあるがとりわけ、前のブロックヘッダのハッシュ、すなわち現在のブロックが構築された際にに基づくブロックのブロックヘッダのハッシュを含む。ブロックヘッダは、また、トランザクションのセットを使用して構築されたマークルツリーのマークルルートも含む。各トランザクションは、まず最初に、ハッシュ化(たとえばダブルハッシュ化)され、そのトランザクションのトランザクション識別子(Txid)を生成する。次いで、トランザクション識別子は、マークルツリーのリーフノードとして使用される。次いで、トランザクション識別子のペアが連結され、ハッシュ化されて、マークルツリーの第1内部レベルのそれぞれの内部ノードを形成する。次いで、第1の内部レベルの内部ノードのペアが連結され、ハッシュ化されて、マークルツリーの第2の内部レベルのそれぞれの内部ノードを形成する。内部ノードのペアを連結してハッシュ化するプロセスは、単一のハッシュ、マークルルートのみが残るまで繰り返される。このマークルルートは、ブロックマークルルートと称されることもある。

【0049】

次に、特に図5、図6、および図7を参照しつつ、本開示の実施形態について説明する。

【0050】

#### ブロックのマークルツリーのセグメントを識別する

特定の当事者、たとえばアリスがいくつかのトランザクションの有効性確認を望んでいると仮定する。本開示の一実施形態によれば、トランザクションの少なくとも1つのサブセットが識別され、サブセットは、そのブロックに対するマークルツリー全体のセグメントを形成し、および/またはセグメントによって表される。したがって、トランザクションのブロックは、ブロックのマークルツリーに基づき論理的に複数のセグメントにセグメント化され得、各セグメントはブロックのトランザクションのサブセットを含み、各セグメントはそれ自身のルートノード(または「ルートハッシュ」)を有する。この共通のルートハッシュは、ときには、ブロック全体のルートハッシュと区別するために、以下では「セグメントハッシュ」と称される。ツリーセグメント内の同じレベル(すなわち、ときには「リーフレベル」または「リーフ層」とも称される最低レベル)のトランザクションは、兄弟姉妹である。所与のセグメント内のすべてのトランザクションは、そのセグメントに対する共通のルートノードを共有する。共通のルートノードは、マークルツリーの隣接レベル、すなわち最低レベルのすぐ上のレベルに属するものとしてよい。代替的に、共通のルートノードは、より高いレベルに属し得る。一般に、共通のルートノードは、最下位レベルとマークルルートとの間のマークルツリーの任意のレベルに属し得る。

【0051】

ブロックをそのマークルツリーに基づきより小さな部分に分割することによって、複数のバリデータの間にトランザクションを迅速に効率的に割り当てることができることを含む、著しい技術的利点をもたらす。たとえば、ビットコインのプロトコルは二分木を使用しているので、複数のマシンにまたがるバイナリ割り当て(binary allocation)を実装することが可能である。セグメントに対するインデキシングシステムとして小さなバイナリマーカを使用することによって、マークルツリー全体における各セグメントの位置は

素早く計算され、これはセグメントが検証完了後に一緒に元に戻されることを可能にし、ブロックに対する完全なマークルツリーを再構成することができる。このバイナリインデキシングアプローチについては後で詳述する。

#### 【0052】

セグメントを識別するために様々な技術が使用され得るが、一アプローチによれば、セグメントの数はシステム内の利用可能なバリデータの数によって決定され得る。たとえば、4つのバリデータを有するシステムにおいて、マークルツリーは、4つのセグメントに分割され、8つのバリデータがある場合には、マークルツリーは、8つのセグメントに分割され、と言うように続き得る。所与のマークルツリーに対するセグメントの識別は、図7のコントローラ702によって例示されている、制御エンティティによって実行されるか、または影響を受け得る。

10

#### 【0053】

上で説明されている点は、図5および図6を参照しつつさらに例示され、図5は、マークルツリーがどのように別々の部分502に分割され得、バリデータに割り当てられるかを示す一例を例示している。図5の例では、各矢印は、それぞれのトランザクション識別子を形成するためにハッシュ化されるそれぞれのトランザクションを表し、これはマークルツリーのそれぞれのリーフノードで使用される。マークルツリーの最上位はブロックマークルルートである。この例では、マークルツリーで表されるトランザクションのブロックは、32個のトランザクションを収容する。しかしながら、これは、単なる例示であり、一般に、マークルツリーは、ブロック内のトランザクション数に応じて、任意の数のトランザクションを収容し得ることは理解されるであろう。示されるように、マークルツリーは、破線のボックスで示される、4つの部分502a~dに分割される。各部分502は、実線の丸で示されている、マークルツリーのそれぞれの共通内部ノード(内部ハッシュ)504によってリンクされる。各部分502は、8個のトランザクションを表す。この例では、共通内部ノード504はマークルツリーの第4のレベルに属す。本明細書において説明される実施形態によれば、各それぞれの部分502(またはむしろ、部分を形成するトランザクションおよび/または部分を表すトランザクション)は、処理のために、たとえばそれぞれの部分502に属すトランザクションの有効性確認のために、それぞれのバリデータに割り当てられる。

20

#### 【0054】

図6は、マークルツリーがどのように部分602に分割され得るかを示す別の例を例示している。図6のマークルツリーは、図5のものと同一である。次に、この例では、マークルツリーは、8個の部分602a~hに分割され、各部分602は4つのトランザクションを表している。この例では、共通内部ノード604はマークルツリーの第3のレベルに属す。図5および図6のマークルツリーは、その代わりに、より多くの(たとえば16個の)またはより少ない(たとえば2個の)部分502、602に分割されることも可能であろう。一般に、ブロックのトランザクションのセットから形成されるマークルツリーは、任意の数の部分502、602に分割されてよく、各部分は、最低2つのトランザクションを含む。

30

#### 【0055】

それぞれの有効性確認リソースへのセグメントの割り当て

40

トランザクションのサブセットは、その識別に続いて、複数の有効性確認リソースに分散され、簡単に参照できるように「バリデータ」とも称され得る。複数のバリデータは、図7および図9においてリソースAからD(704aから704d)として示されている。割り当てプロセスは、限定するものではないが、図9に示されているようにコンポーネント904などの専用ユニットによって指示されるかまたは影響を受け得る。

#### 【0056】

各バリデータ(704aから704d)は、1つまたは複数の処理リソースを含み得る。したがって、複数のバリデータ(704aから704d)のバリデータのうちの少なくとも1つは、1つもしくは複数の仮想マシン、1つもしくは複数のサーバ、1つもしくは複数のGPUベースのコンピューティングリソース、1つもしくは複数のスレッド、および/または1つもし

50

くは複数のマルチプロセッサシステム、などのうちの少なくとも1つであるか、または含み得る。基本的に、複数のバリデータのうちのどれも、任意のタイプまたは組合せの処理リソースから構成され、各々ブロックのマークルツリーのセグメントによって互いに関連付けられている1つまたは複数のトランザクションを有効性確認することができる。複数のバリデータ(704aから704d)および他のシステムコンポーネントは、集合的なリソースまたはエンティティ700を形成し、これを「(分散)有効性確認ノード」と称する。

#### 【0057】

好ましくは、分散は、複数のバリデータ内のそれぞれのバリデータにセグメントの各々を割り当てることを含む。バリデータは、少なくとも、

- ・割り当てられたセグメントを構成する1つまたは複数のトランザクションを操作する

10

・1つまたは複数のトランザクションを有効性確認して、それらがブロックチェーンプロトコルに適合していることを検証する、および/または

・ブロックチェーン台帳もしくは知られている、登録された、あるいは消費済みのトランザクションのデータベースなど、既存のリポジトリにおいて識別され得ることの有効性確認を行う

ように構成され得る。

#### 【0058】

バリデータの活動、および異なるバリデータへのサブセットの割り当ては、コントローラによって指示され得る。図7は、コントローラ702が、それぞれのツリーセグメントに対するトランザクションAからDのサブセットを、それぞれバリデータ704aから704dに割り当てる様子を示している。システムレベルコントローラ702は、分散有効性確認ノード内のシステムまたはデバイス704aから704dの活動を協調させ、ブロックのマークルツリーによるツリーセグメントの識別、識別済みセグメントの各バリデータへの割り当て、ブロックに対する完全なマークルツリーへの有効性確認済みツリーセグメントの再順序付け、および/または再構成されたブロック内のトランザクションの順序付けなどの、タスクを制御するかもしれない。それはそれに影響を及ぼし得る。

20

#### 【0059】

これらのバリデータの1つまたは複数は、バリデータレベルでコントローラとして機能するように構成された少なくとも1つの協調エンティティを含み得る。したがって、バリデータ704aから704dのいずれかまたはすべてが、それ自身の少なくとも1つのコントローラコンポーネントを含み得る。この下位レベルのコントローラは、バリデータ内の1つまたは複数の処理リソースへのタスクまたはサブタスクの割り当て、所与のセグメントに対するマークルツリーの再構成、または他のシステムコンポーネント、たとえば他のバリデータもしくは上位レベルのコントローラ、UTXOプール、ウォレットなどとのインタラクションなどの操作に影響を及ぼすか、または指示するものとしてよい。続いて、処理リソースそれ自体が、より小さなシステムにさらに分解されるものとしてよく、そのうちの1つまたは複数のシステムは、コントローラ、およびそれ自身の1つまたは複数の処理リソースを含み得る。このようにして、システムは、有効性確認タスクを実行するための1つまたは複数の処理リソース、およびプロセッサの活動の協調およびコンポーネント間通信の実行のための1つまたは複数のコントローラを含む有効性確認エンティティによってセグメント有効性確認が実行される階層アーキテクチャを含み得る。

30

40

#### 【0060】

バリデータが複数の処理リソースを含む実施形態では、バリデータは、割り当てられたセグメントをより小さなセグメントに分割し得る。次いで、バリデータのコントローラは、その制御下にあるプロセッサ上にサブセグメントを分散させることができる。このようにして、有効性確認プロセスは、階層方式および分散方式で実装され得る。

#### 【0061】

この階層的分解は、トランザクションレベルにも拡張され、有効性確認は、ツリーセグメントレベルではなくむしろ、トランザクション毎にサブプロセスまたはタスクにさらに

50

分解され得る。このアプローチでは、個別のトランザクションの有効性確認は、異なるマシン、または同一のもしくは異なるマシン上で実行される異なるスレッド上に分散されるサブタスクに分解される。これらのプロセスは、スレッドが利用可能になると、別のトランザクションまたはタスクがそのスレッドに割り当てられるようにキューに入れられ得る。

#### 【0062】

したがって、本開示は、多くのトランザクションが同時に処理されることを可能にし、唯一の制限は従来の技術のようにボトルネックとなる利用可能な処理速度ではなくむしろ、分散有効性確認ノードを形成するために利用可能なハードウェアの数である。これは、ブロックチェーンネットワークの基礎となるプロトコルを改変することを必要とせず、

10

#### 【0063】

したがって、本開示は、「本開示の例示的な実施形態の実装のための例示的な技術環境」と題された以下のセクションにおいて、図1および2を参照しつつより詳細に説明される、有効性確認に対する従来のアプローチからの著しい逸脱を提示している。説明されているように、従来のアプローチは、1つのブロックがエンティティ全体として有効性確認されること、および有効性確認ノード(図1の104を参照)が単一のコンピューティングユニットであるという従来の見解を伴う。対照的に、本開示の実施形態は、マークルツリーを異なるバリデータ(図7および図9の704aから704d)に与えられる複数のセグメントに分割し、セグメントおよびバリデータの各々は関わる分散の程度を高めるためにさらに分割することができる。

20

#### 【0064】

なおもさらに、各ブロックをそのマークルツリーに基づきセグメントに分割することによって、本開示の実施形態は、バリデータがブロック全体ではなくむしろブロックの小部分にアクセスし、ダウンロードし、処理することを可能にする。各セグメント内のトランザクションは(ペアで)単一のルート値までハッシュアップすることを想起されたい。これは、セグメントは、ブロック全体が全体としてダウンロードされる、保存される、および処理されるのではなくむしろ、必要な関連するトランザクションのみを使用して有効性が確認され得ることを意味する。ビットコインSVなどのプロトコルはブロックサイズのスケールアップおよび台帳への大きなブロックの包含を可能にすると、ブロック全体をダウンロードする従来のモデルはボトルネックになる。本開示の実施形態は、個別のバリデータがそれらに関連する(より小さな)部分のみを受信して処理することを可能にすることによってブロックチェーンのスケラビリティに対するこの難題を解消する。この結果、有効性確認全体の時間の短縮、ブロックチェーンネットワークの改善、およびブロックチェーン上で実行されるアプリケーションの改善をもたらす。

30

#### 【0065】

さらに、実施形態は、SPVプロセスおよびリソースの使用をサポートし、円滑にするが、それは、そのようなSPVが、所与の当事者にとって関心のあるマークルツリーの部分のみのローカル有効性確認を伴うからである。したがって、SPV技術の剪定の性質は、本開示の実施形態と組み合わせて使用するのに理想的である。SPVコンテキストでは、バリデータは、これらが必要とするブロックデータの一部のみ、すなわちブロックヘッダまたはセグメントルートノードおよび関連するトランザクションを与えられ得る。

40

#### 【0066】

各バリデータがチェックを実行し、それが処理したセグメントを有効性確認したときに、ツリーを生成するために使用されるハッシュメカニズムに起因してブロックが有効であることが保証され得る。

#### 【0067】

複数のバリデータ間の負荷分散

負荷分散の技術およびシステムは、当技術分野で知られており、複数のリソースの間にタスクを均等に分散させ、効率を高めることを目的として構成される。その目的は、いく

50

つかの処理リソースがアイドル状態になり、他のリソースが過負荷状態になるリスク、およびそれにより性能が低下し、さらには障害が発生するリスクを最小限に抑えることである。したがって、負荷分散は、システム全体のレジリエンス、およびその性能および効率を確実にする上で重要である。本開示の実施形態は、たとえば、静的負荷分散または動的負荷分散などの任意の知られている負荷分散技術を利用するものとしてよい。それに加えて、または代替的に、本明細書において開示されている負荷分散アプローチが有利に使用され得る。

【0068】

上で述べたように、本開示の実施形態は、それぞれのバリデータへのブロックセグメントの割り当ての際にインデキシングシステムを使用することができる。好ましくは、これは、バイナリインデキシングシステムである。この好ましいシステムでは、各バリデータは、バイナリラベルまたは識別子を指定される。各識別子は4桁長であり、最初のバリデータは0000として識別され、次のバリデータは0001として識別され、次のバリデータは0010というように識別される。明らかに、4桁の識別子では256個のバリデータIDが可能であり、最後のバリデータは1111として識別される(すなわちバリデータ番号は10進数で255である)。

【0069】

ツリーセグメントが、バリデータに割り当てられる必要があるときに、そのダブルハッシュの最初の4桁(すなわちツリーセグメントのセグメントハッシュ)が、どのバリデータがそのセグメントを処理するかを決定するために使用され得る。マークルルートは、ブロックからのトランザクションID(TxID)のペアと一緒にハッシュしてマークルツリーのそれぞれの内部ノード(または内部ハッシュ)を生成し、次いで隣接する内部ハッシュを、最終的に単一のハッシュに達するまで繰り返しハッシュすることによって生成される。このダブルハッシュ済みマークルルートは、効率的で迅速、安全な検証メカニズムを提供する。これは、また、現在のコンテキストにおいて、ダブルハッシュがランダム2進数を生成するという利点ももたらす。各セグメントハッシュを含む各内部ハッシュは、それ自体ダブルハッシュである。したがって、われわれは、セグメントハッシュの先行桁の最初のx個を割り当てインデックスとすることができる。4つの先行ゼロを有するハッシュでは、結果として、ツリーセグメントはID 0000を有するバリデータに割り当てられ、先行桁0001を有するハッシュでは、結果として、ID 0001を有するバリデータに割り当てる、というように続く。ダブルハッシュのランダム生成は、バリデータへのツリーセグメントのランダム分配を確実にする。

【0070】

ダブルハッシュ化は、典型的には、マークルツリーを生成するときに使用されるが、すべての例において必須というわけではなく、その代わりに、シングルハッシュ化のみが使用され得る。実際には、ハッシュ演算を何回行っても、ランダム2進数が生成される。負荷分散タスクは、図9において905として示されている、専用システムコンポーネントによって実行され得るか、またはシステム700内の他の場所で提供され得るか、またはシステム700と関連し、通信して提供されてもよい。

【0071】

ブロックの分散ダウンロード

いくつかの実施形態によれば、異なるバリデータへのブロックマークルツリーのセグメントの割り当ては、トランザクションのブロックの一部または全部をダウンロードするための、より高速で効率的なプロセスを提供するために使用されてもよい。

【0072】

各バリデータは、たとえば上で説明されている割り当てインデックスに基づきマークルツリーのセグメントを割り当てられる。次いで、任意の所与のバリデータが、割り当て済みツリーセグメントを形成するトランザクションのセットをダウンロードするように動作する。これは、トランザクションのセットを、ブロックチェーンそれ自体から(たとえばブロックチェーンノードから)またはサードパーティのサービスプロバイダなどの異なる

リソースもしくはエンティティからダウンロードすることを伴い得る。トランザクションのセットは、バリデータの内部メモリに、またはクラウド上の共有ドライブなどの共有ストレージロケーションにダウンロードされ得る。

【0073】

分散ノードは、完全なブロック、すなわちブロックを形成するトランザクションのセット全体を必要とすることがある。その場合、ツリーセグメントを割り当てられた各バリデータは、セグメントを形成するトランザクションのサブセットをダウンロードする。他のシナリオでは、分散ノードは、ブロックの特定の部分のみを必要とし得る。その場合、バリデータのうちのいくつかのみが、望ましいトランザクションを取得するためにトランザクションのそれぞれのサブセットをダウンロードする必要がある得る。

10

【0074】

このような方式でブロック(またはブロックの一部)をダウンロードすると、各バリデータがブロックを形成するトランザクションのセット全体のうち、トランザクションのサブセットを処理するだけで済むので、ダウンロード全体が速くなる。これは従来のブロックダウンロードとは対照的であり、所与のエンティティ(たとえばフルノード)は、たとえばブロック内に出現する順序で各トランザクションをダウンロードすることによって、ブロック全体をダウンロードしなければならない。そこで、ブロックは、複数のバリデータによって並行してダウンロードされる。1つのブロックは、数桁以上とは言わないまでも、数万件のトランザクションを収容し得る。単一のエンティティがこの数のトランザクションをダウンロードすることは、著しいリソースを消費し、かなりの時間を要する。計算負荷はバリデータ間に分散され、それにより各個別のバリデータは処理リソースのほんの一部を消費するだけである。同様に、ブロックをダウンロードするのにかかる全体的な時間も短縮される。

20

【0075】

説明されているように、各バリデータは、トランザクションのサブセットをダウンロードし得る。次いで、サブセットは組み合わされ、ブロックを単一のストレージロケーション内に再構築し得る。(「単一のストレージロケーション」は、自己完結的なエンティティであるストレージリソース、または集合的なエンティティを形成する複数の関連付けられたストレージリソースのいずれかを意味する)。そうするために、個別のバリデータは、それぞれのサブセットを、トランザクションを正しい順序に構成するように構成されている分散ノードの中央コントローラに伝送し得る。この目的のために、セグメントハッシュ(すなわち、ツリーセグメントをリンクするハッシュ)が利用され得る。たとえば、マークルツリー内のその位置への、たとえば、セグメントハッシュがマークルツリー内に出現するときに左から右へ、セグメントハッシュのマッピングが維持され得る。次いで、トランザクションのサブセットは、対応するセグメントハッシュに基づき(たとえば、最初から最後への)順番に配置され得る。

30

【0076】

いくつかの実施形態では、個別のバリデータ(または分散ノード全体)は、マークルツリーを再構築することによって正しいトランザクションがダウンロードされたこと(またはトランザクションが正しくダウンロードされたこと)を確認し得る。トランザクションのサブセットをダウンロードした後、バリデータは、それらのトランザクションに基づき候補セグメントハッシュを生成し得る。候補セグメントハッシュは、TxIDのペアをハッシュ化してそれぞれの内部ハッシュを生成し、候補セグメントハッシュが生成されるまで内部ハッシュのペアを繰り返しハッシュ化することによって構築される。候補セグメントハッシュが属すマークルツリーのレベルは、マークルツリーが分割されるツリーセグメントの数に依存する。バリデータは、候補セグメントハッシュがマークルツリーのハッシュであることを検証し得る。ハッシュが一致しない場合は、ダウンロード中にエラーが発生している。いくつかの例では、各バリデータは、候補セグメントハッシュを生成し、それをコントローラに送信して検証を実行し得る。別の例として、候補ブロックマークルルートは、ダウンロードされたトランザクションのセット全体に基づき生成され得る。ここでも

40

50

また、候補マークルルートは、ブロックが正しくダウンロードされていれば、実際のブロックマークルルート(すなわち、ブロックに保存されているマークルルート)と一致するべきである。

【0077】

いくつかの場合において、バリデータは、上で説明されている技術を使用してダウンロード済みトランザクションの有効性確認し得る。すなわち、各バリデータは、ツリーセグメントを割り当てられ、トランザクションの対応するサブセットをダウンロードし、それらのトランザクションを有効性確認する。他の場合には、バリデータは、必ずしもトランザクションを有効性確認しなくてもよく、後で使用するために、たとえばサードパーティに送信するために、トランザクションを単にダウンロードするだけでよい。

【0078】

分散UTXOプール

好ましくは、分散有効性確認ノードの一部を構成する各バリデータ704は、未消費トランザクション出力(UTXOS)を生成し、保存し、および/または維持するためのそれ自身のリポジトリ(プール)を有する。これは、ブロックチェーントランザクションに関連付けられた未消費すなわち未消費出力の記録を提供するUTXOプールとして機能する。したがって、各バリデータのUTXOプールは、マークルツリーセグメントに関してコントローラによって割り当てられたトランザクションに基づくものであり、それらのトランザクションから構築される。一実施形態において、これは、処理のために所与のバリデータに割り当てられたトランザクションの未消費UTXOに関係するデータを含む(グラフ)データベースであってよい。各UTXOに対して、新しいマークルツリーセグメントが割り当てられると、バリデータが認識することになるデータベース内のレコードが作成される。したがって、分散有効性確認ノードの観点からは、UTXOプールは、1つの単一プールではなく、複数の異なるUTXOプールから構成され、各々異なるバリデータのところでまたは異なるバリデータ上で提供されUTXOの異なるセットを含む。したがって、ノードに対するUTXOプールは、データと、さらにはそれを保存しおよび/または処理するリソースの両方において分散される。

【0079】

これは、ネットワーク内の各フルノードがブロックチェーン上のすべてのUTXOを追跡するUTXOプールのコピーを有する従来のUTXOモデルから著しく逸脱している。対照的に、本開示は、UTXOプールを複数の有効性確認リソースに分散し、各々ブロックチェーンのUTXOセット全体のサブセットであるUTXOプールを有する。各バリデータのUTXOプールは、これに任された有効性確認がなされるマークルツリーのサブ部分を構成するトランザクションのUTXOを含む。

【0080】

そのようなアプローチに従って、新しいブロックが有効性確認される必要がある毎に、データベースに関係するすべてのコマンド、イベント、アイテムがログに記録されるという点で、SQLトランザクションログに類似する方式で実装され得る。「データベースログ」という用語は、本明細書では、ブロックチェーンに関して知られているような「トランザクション」という用語の使用から生じる混同を回避するために使用されるが、われわれは、「トランザクションジャーナル」、「トランザクションログ」などの用語を含むように「データベースログ」という用語を使用する。本質的に、データベースログは、コンピュータベースのデータベースの分野で知られているように、データベースの状態に関して発生したすべての変更の記録を提供する、データベース管理システムによって実行されたアクションの履歴として解釈され得る([https://en.wikipedia.org/wiki/Transaction\\_log](https://en.wikipedia.org/wiki/Transaction_log)を参照)。

【0081】

順序付けられた、履歴データベースログの使用は、UTXOプール全体がログの履歴を元の順序で実行することによって構築され得ることを意味する。有利には、これは、必要ときに常にデータベースのコピーが(再)生成され得、データの別個のコピーが保存される

10

20

30

40

50

必要がないことを確実にする。データ完全性が確実にされ、必要なストレージリソースも少なく済む。各UTXOプールは、個別に保存され、維持され、処理され得る。また、有利には、SPV技術でマークルツリーの剪定済み部分を操作するならば、SPV技術は各バリデータについて個別のUTXOデータベースを作成することを円滑にする。

#### 【0082】

データベース内のトランザクション(TX)は様々な方法で構造化され得るが、特に有利なアプローチは、ブロックIDとトランザクションIDとの連結(block\_ID || TxID)を含む識別子に従って構造化することである。ブロックIDおよびトランザクションIDは両方とも、256ビットハッシュであり、その結果、安全で衝突のない512ビット連結フィールド構造を形成する。

10

#### 【0083】

このようにしてトランザクションを構造化することは、高速で効率的なルックアップメカニズムを提供する。トランザクションは、同じblock\_IDを有するすべてのトランザクションがデータベース内で一緒に配置されるようにblock\_IDでソートされ得る。したがって、バリデータがトランザクションを必要とするとき(たとえばトランザクションのUTXOが消費されたかどうかを確認するため)、バリデータは、最初に対応するblock\_IDを検索し、次いで対応するTxIDを検索することによってデータベース内のトランザクションを特定することができる。これは、検索がデータベースの関連セクションに限定されるという効果を有する。この効率が、検索操作に必要な時間、処理リソース、およびエネルギーを削減し、先行技術に勝る著しい改善をもたらす。

20

#### 【0084】

フラグまたはマーカーは、バリデータのプール内の各UTXOに関連付けられ、UTXOがロックされているかロック解除されているかを示す。われわれは、便宜上、このフラグまたはマーカーを「ロックフラグ」と称することがある。UTXOが「locked」とマークされたときに、これはグループ内の(すなわち分散有効性確認ノード内の他の場所の)バリデータに対する、このUTXOが消費のために利用可能でないことを示す指標として働く。逆に、UTXOが「unlocked」とマークされたときに、これはバリデータに対して、UTXOが消費され得ることを示す指標として働く。したがって、これは、UTXOを消費するトランザクションの検証に割り当てられているバリデータがトランザクションが有効であると証明されたと仮定してUTXOが償還されたこと、したがって、もはや使用可能でないことをピアにシグナリングすることを可能にする。「locked」状態は、消費が許可されていることを意味するが、「unlocked」状態は、消費が禁止されていることを意味する。

30

#### 【0085】

このロック/ロック解除フラグは、「locked」に対して「0」、「unlocked」に対して「1」などの、単純で小さなバイナリマーカーとすることができる。マーカーメカニズムは、分散ノードシステムのバリデータによって内部的に使用され、トランザクションがプロトコルルールに適合するようにブロックチェーンとインタラクティブにやり取りするのに先立ちマーカーはトランザクションから除去される。

#### 【0086】

使用中、バリデータはコントローラによって割り当てられた新規トランザクションの各々における出力を検査する。あらゆる未消費の出力(UTXO)はバリデータのUTXOプールに追加される、すなわち、UTXOデータベース内のエントリとして記録される。各新規UTXOに対する関連データベースレコードでは、ロックフラグは、「unlocked」に設定される。

40

#### 【0087】

バリデータは、UTXOが新規に割り当てられたトランザクションによって消費されているのを確認したときに、複数のバリデータ内の他のすべてのバリデータに、このUTXOもそれぞれのプールでロックされるべきであることを通知するメッセージを送信する。本質的に、バリデータは、特定の時刻に特定のハッシュIDを有するトランザクションを伴う消費を確認したことを示す通信内容をピアに送信する。他のバリデータは、トランザクシ

50

ョンハッシュおよびそれが消費するUTXOのリストが注目するトランザクションをそれらが識別し、それをそれ自身のデータベースにおいてロック済みであるというマークを付けるのに十分であるので、トランザクション全体に対する完全なデータを受信する必要がない。メッセージを受信すると、各受信バリデータは、注目するUTXOがそれらのUTXOプールにあるかどうかチェックする。そうであれば、ロックフラグの状態は「locked」に変更される。したがって、ロックは、同じUTXOが後続のトランザクションにおいて消費されるのをバリデータが許すのを妨げる。新しいトランザクションが同じUTXOを消費することを試みた場合、ロックフラグのチェックは、2回目の消費の試みが無視されるべきであることを示す。メッセージを送信したバリデータが、有効性確認が失敗し、したがってUTXOが消費されていないと決定した場合、バリデータのピアに対して、UTXOに対するロックフラグが「unlocked」状態に変更されるべきであることを示す、その旨のさらなるメッセージが送信され得る。有効な消費が完了した後、その旨のメッセージが送信され、ロック済みUTXOが関連するUTXOプールから削除され得る。

10

【0088】

上で説明されている実施形態において、各バリデータは、単一のUTXOプールを有し、これは、それに割り当てられているツリーセグメントのすべてにおけるすべてのトランザクションのUTXOを含む。しかしながら、代替的アプローチにおいて、各バリデータによって維持されるUTXOプールは、ブロック毎に1つずつ、複数のサブプールに、分けられ/分割され/区画化され/形成され得る。このようにして、単一のUTXOプールは、論理階層に編成され得る。さらに別のアプローチでは、1つまたは複数のバリデータは、それぞれの複数のUTXOプールに関連して構成されるものとしてよく、各複数のプールは1つまたは複数のツリーセグメントのセットに対してUTXOに関係する。したがって、いくつかの実施形態において、バリデータは、異なる個別のツリーセグメントについて、またはツリーセグメントのタイプ、または所与の範囲内にあるツリーセグメントなどの事前定義された基準に従って、UTXOを別々のUTXOプールに編成し得る。そのような実施形態では、識別子は、関連するUTXOプールに対する検索を絞り込むために使用され得るブロックIDを含むものとしてよく、次いで、検索はそのプール内で進行し、そのTxIDによって関連するトランザクションを識別する(ことを試みる)ことができる。当事者であれば、いくつかの実施形態において、これらのアプローチの混合したものが使用できる、すなわち、分散ノード内の1つまたは複数のバリデータが単一UTXOプールアプローチを採用し得るが、他のものは複数の、別個のUTXOプール、および/またはサブプールに編成されたUTXOプール、またはそれらの任意の組合せを使用するように構成されることを理解するであろう。

20

30

【0089】

これは、当事者が同じUTXOを2回使用しようとする「二重支払い」状況に対する保護を提供する。これは、システム内のバリデータの数またはロケーションに関係なく、効率的に、また迅速に動作し、ブロックチェーン上で実装される送金のセキュリティおよび完全性を維持する、シンプルで安全なロックメカニズムを提供する。

【0090】

分散マイニング

40

次に、われわれは、マイニングタスクおよび機能が、ブロックチェーンネットワーク上の「フルノード」に典型的に関連付けられているか、または「フルノード」によって実行される他の操作から分離される、本開示の一態様の詳細な説明を提示する。これは、マイニングタスクが異なるリソース間に分散され並列化されることを可能にする。これは、従来技術と比べて異なる技術的アーキテクチャおよびシステム構成を提供し、リソースの配置または提供に関してより柔軟に対応することができる。たとえば、再生可能エネルギーの供給が利用可能である地理的地域にマイニングリソースが用意され、それにより高価な、または環境コストの高いエネルギー源にあまり頼らないネットワークを構築することが可能であろう。

【0091】

50

当技術分野で知られ、図11に例示されているように、トランザクションは、ブロックチェーンに書き込まれ得る前に有効性確認されなければならない。ネットワークノード(マイナー)は、各トランザクションが有効であることを確認する作業を実行し、無効なトランザクションはネットワークから拒絶される。ノード上にインストールされたソフトウェアクライアントは、ロックスクリプトおよびロック解除スクリプトを実行することによって未消費トランザクション(UTXO)に対してこの有効性確認作業を実行する。ロックスクリプトおよびロック解除スクリプトの実行結果がTRUEと評価された場合、トランザクションは有効であり、トランザクションはブロックチェーンに書き込まれる。したがって、トランザクションがブロックチェーン台帳に追記されるためには、これはi)トランザクションを受信した最初のノードによって有効性確認なされ--トランザクションが有効性確認された場合、ノードはそれをネットワーク内の他のノードに中継し、ii)マイナーによって構築された新しいブロックに追加され、iii)マイニングされることを行わなければならない。

10

#### 【0092】

従来、ブロックをマイニングするために、マイニングノードは、未確認のトランザクションをmempoolから選択し、そのブロックに対するコインベーストランザクションを生成し、すべてのトランザクションをペアでハッシュ化することによって候補ブロックを形成し、マークル(ハッシュ)ルートを持つマークルツリー構造を形成する。マークルツリーは、候補ブロック内のすべてのトランザクションを表す。マイナーはまた、バージョン番号および現在のエポック時間を決定し、台帳の最長チェーン上の最新ブロックのハッシュを取得する。マークルルートおよび他の値は、連結され、ブロックメッセージBMを形成する。

20

#### 【0093】

次いで、マイナーは、ブロックメッセージに付加され完全なブロックヘッダを生成するときに、指定された数の先行ゼロを含むハッシュを生成する整数値(ノンス(nonce))を見つけることによって、PoWチャレンジを解決することを試みる。この試みが適格なハッシュを生成するのに失敗した場合、マイナーは、別のノンスを使用して計算を繰り返す。これは、必要な数の先行ゼロを生成することに成功したノンスを見つけた場合、候補ブロックをその完全なヘッダを含めてブロックチェーンネットワークに送信し、他のノードによって検証される。したがって、ノンスは、マイナーがチャレンジの解を見つける際にエネルギー、労力、および時間を費やしたことの証明を提供する。

30

#### 【0094】

したがって、従来のアプローチでは、マイナーは、トランザクションを選択し、候補ブロックを生成し、PoWおよび完全なブロックヘッダを生成する。これらの機能が同じエンティティによって実行される従来のアプローチとは対照的に、現在開示されているアプローチでは、これらの機能は、異なる処理エンティティ間に分散され、並列化されている。これは、PoW計算を実行し、および/または完了するのに先立ち事前指定された認可基準の検証および実施を可能にする。

#### 【0095】

好ましい一実施形態において、ブロックのマークル構造は、有効性確認およびマイニングプロセスの様々な機能が分離され、異なるコンピューティングリソースによって独立して取り扱われることを可能にする。これらのリソースは、世界中のどこにでも配置され得、分離して、または互いに組み合わせて、動作し得る。これらのリソースは、集合的に「分散ノード」を形成することができ、異なるノードコンポーネントは、ブロックチェーントランザクションおよびブロックの有効性確認および/またはマイニングに関係する1つまたは複数の機能に特化している。

40

#### 【0096】

本開示のアプローチは、プルーフオブワーク(PoW)計算を、従来のフルノードによるマイニングに典型的に関連する有効性確認労力、トランザクション処理、および他のタスクから分離することに関連している。これは、PoW提供者はどんな検証タスクをも実行

50

する必要がなく、逆に有効性確認ノードはPoW計算を世界中のどこにでも配置され得る専門家、専用リソースに任せることができることを意味する。

【0097】

したがって、本開示は、「本開示の例示的な実施形態の実装のための例示的な技術的環境」と題された本明細書のセクションにおいて、図1および図2を参照しつつより詳細に説明される、有効性確認に対する従来のアプローチからの著しい逸脱を提示している。

【0098】

われわれは、次に、この態様の実施形態を例示する図10および図12から図15を参照する。このアプローチでは、図15に示されているように、分散マイニングノード1000が提供される。代替的に、これは「PoW提供者」と称され得る。PoW提供者1000は、「ハッシュマシン」またはASICとも称され得る少なくとも1つの専用PoW計算機を含む。PoW計算機は、関連付けられたプロトコルに従って暗号通貨をマイニングするように構成された1つまたは複数の集積回路チップ(図では1100a、1100b、1100cとして示されている)を備える。計算機1100aから1100cは、SHA-256アルゴリズムを使用してビットコインをマイニングするように構成され得る。たとえばイーサリアムをマイニングするためのETHASHなど、他の暗号通貨には、他のアルゴリズムが採用されてもよい。

【0099】

図10および図15に示されているように、PoW提供者1000は、所与の複数のトランザクションに対して有効なノンス(または、好ましくは、完全なブロックヘッダ)の生成を要求するための要求をPoW提供者に送信するように構成されたPoW要求リソース1300と通信する。本明細書において使用されるような「要求(する)」という用語は、「指示(する)」および/または「開始(する)」を含むことを意図されている。したがって、要求は、PoW生成の指示または開始を含むか、または指示または開始であってよい。われわれは、簡単にするため、「要求」という用語を使用することにする。

【0100】

代替的な表現では、PoW要求リソース1300は、有効性確認および/もしくはマイニングリソースもしくはノード、または単に「PoW要求者」と称され得る。好ましい一実施形態において、要求リソース1300は、分散されてよく、有効性確認および/またはマイニング動作の並列化を円滑にし得る。要求者1300は、実質的に、本明細書において説明され、有効性確認ノード700を参照しつつ図7において例示されるとおりであってよい。しかし、他の実施形態では、要求エンティティは、任意の好適な代替的形態をとるものとしてよく、PoW(ノンスまたはブロックヘッダ)の生成を必要とする任意のエンティティであってよい。

【0101】

PoWを要求するために、PoW要求者1300は、トランザクションの候補ブロックのブロックヘッダの構築に必要な情報の少なくとも一部をPoW提供者1000に送信する。PoW要求者から送信される情報は、「ブロックテンプレート」または「ブロックメッセージ」と称されることがあり、少なくとも、ブロック内のすべてのトランザクションを表すマークルツリーに対するルートを含み得る。ブロックテンプレートは、また、バージョン番号、前のブロックハッシュ、難易度ターゲットおよび/またはタイムスタンプなど、トランザクションに対するブロックヘッダを生成するためにPoW提供者によって使用される他の情報を含み得るか、またはこれらのデータ項目の1つまたは複数が、PoW提供者によって計算されるか、または取得され得る。たとえば、PoW提供者は、バージョン番号を取得するか、取り出すか、もしくは選択するか、またはネットワークから前のブロックハッシュを取得するものとしてよい。PoW提供者は、PoW要求者からブロック全体を受信する必要はなく、単に、選択済みノンスと組み合わせてPoWチャレンジを解くことを試みるために、プロトコルによって指定される十分な、最小限の情報を必要とするだけであることに留意されたい。これは、しかしながら、PoW要求者がブロックに含めることを望むトランザクションに対するマークルルートを受信しなければならないが、それは、これがPoW提供者1000によって決定できないからである。

## 【0102】

いくつかの実施形態において、PoW提供者は、PoW計算機の活動を協調するように構成されているコントローラ1200を備え得る。いくつかの実施形態において、PoW提供者1000および/またはコントローラ1200の機能は、ASICまたはハッシュマシン1100に実装され得る。図15は、コントローラをPoW計算機と同じエンティティの一部として示しているが、これは、コントローラとASICsが同じハードウェアまたはデバイス内に実装されていることを必ず意味するものとして解釈されるべきではない。これらは、物理的に別個のデバイスとして提供され得るが、互いに論理的または電子的に関連付けられること、および/または互いに通信することによって、PoW提供者1000を形成し得る。

## 【0103】

コントローラ1200は、所与の計算機(1100aから1100c)が動作するためのノンスまたはノンスの範囲を選択する、要求者から提供されていないPoW計算に必要な任意の情報を取得する、および/または以下で説明されるように認可基準をチェックするなどの動作を実行し得る。計算機1100a、1100b、および1100cは、同じ候補ブロックに対して異なるノンス範囲で動作するように構成され得る。しかしながら、いくつかの実施形態において、PoW要求リソースは、ノンス範囲を割り当てるものとしてよく、PoW提供者1000および/またはコントローラ1200の機能は、ASIC1100に実装され得る。さらに他の実施形態では、PoW要求者は、ノンス範囲を割り当てるものとしてよい。

## 【0104】

ブロックテンプレートに加えて、PoW要求者は、PoW提供者にさらなるデータを提供することができる。これは、PoW提供者が少なくとも1つの前提条件のルールまたは基準の達成またはそうでないことを確認するために必要とする任意の種類のデータとすることも可能であろう。この少なくとも1つの事前指定されたルールまたは基準は、参照しやすいように、以下では制御基準と称される。制御基準は、PoW提供者がそのPoW計算作業を開始し、継続し、および/または完了する前に満たされていなければならない。PoW提供者に提供された(制御)データが制御基準を満たす場合、PoW生成に対する要求は、認可された、合法的な、および/または許可されたものとPoW提供者によってみなされ得る。制御基準は、PoW提供者において、PoW提供者によって、またはPoW提供者に代わって、事前決定され得る。それは、PoW要求者とPoW提供者、またはそれぞれの関連エンティティの間で合意されてもよい。

## 【0105】

好ましい一実装形態において、制御データは、PoWが計算されるブロックの一部を形成するトランザクションに含まれる。制御データは、当事者間の事前認可もしくは合意、または認可された要求者からの要求の合法性を保証するために、制御基準と突き合わせてPoW提供者によって評価されるか、またはチェックされ得る。たとえば、PoW提供者は、ブロックが暗号通貨の一部を特定のアドレスに移転するトランザクション(TX<sub>0</sub>)を含むことを必要とし得る。この基準が満たされていない場合、PoW要求は、許可されていないとみなされ、必要なPoWを計算することを試みない。チェックプロセスを支援するために、PoW要求者は、PoW提供者に送信するデータの一部として、PoW提供者が、ブロックが正常にマイニングされブロックチェーンに追加された場合に、事前指定されたアドレスへの移転が行われることを確認するために使用することができるSPV形式の証明を提供し得る。

## 【0106】

別の例では、TX<sub>0</sub>が認可当事者によって署名されていることが前提条件となることもあり得る。

## 【0107】

他の例では、制御基準は、PoW提供者がチェックし確認することができるメタデータをTX<sub>0</sub>が収容することであり得る。たとえば、メタデータは、暗号鍵、またはパスワード/コード、またはPoW提供者が要求者のために、または要求者に代わってPoWを生成することを認可されるかまたは許可されていることを確認するために使用することができ

10

20

30

40

50

る他の何らかのデータなどの秘密情報を含み得る。

【0108】

いくつかの実装形態において、TX<sub>0</sub>は、PoWがどこに送信されるべきかに関する指示も含むことが可能である。たとえば、デフォルトで、PoW要求者に送り返され得るか、またはメタデータもしくはトランザクションの他の何らかの部分で指定されるような別のエンティティに送信され得る。メタデータは、PoWがどのデスティネーションに送信されるべきか、またはどの当事者がPoW要求を認可しているかを指令するためのフラグまたは他の識別子を含むことも可能である。フラグまたは識別子またはパスワードなどは、PoW提供者および/または要求者にのみ知られるものとしてよい。これは、PoW提供者が複数の無関係な要求者からの要求を受信することができるシナリオにおいて有利であり得る。

10

【0109】

いくつかの場合において、TX<sub>0</sub>の検査は、PoW提供者によるイベントをトリガーする可能性もある。たとえば、PoW提供者が、PoW提供者のアカウントを有している特定の認可された要求者から受信されるような要求を識別することができるので、トランザクション内のデータは、残高またはアカウントが更新されることを引き起こす可能性がある。それに加えて、または代替的に、PoW提供者は、場合によっては所与の期間内に、所与の要求者に対して指定された数より多いPoWを提供することを望まないこともあり、また閾値の条件が満たされたかどうかを決定するためにTX<sub>0</sub>を使用し得る。それに加えて、または代替的に、アラーム、アラート、または他の通信は、TX<sub>0</sub>において提供されるデータに基づきPoW提供者によって開始され得る。

20

【0110】

さらに他の例では、制御基準は、TX<sub>0</sub>が十分な量の暗号通貨を、場合によっては事前指定されたアドレスに対して消費することであり得、PoWは、制御基準が満たされていることを確実にするためにTX<sub>0</sub>の出力をチェックすることも可能であろう。

【0111】

さらに他のいくつかの例では、TX<sub>0</sub>の入力は、非合法または非承認ソースからの資金の移転および受け取りがなされないことを確実にするために検査されることも可能であろう。たとえば、PoW提供者が、たとえば違法行為に関連していることが知られているか、または疑われているなどの理由で、特定の当事者からの要求を受け取ることを望まない場合、PoWは、要求済みPoWの生成を断ることができる。したがって、本開示は、法律または規制要件の順守を確実にするためのソリューションを提供でき、詐欺/犯罪行為を防止するための対策を提供することができる。

30

【0112】

要するに、本発明は、効率的であり参加当事者間の信頼を必要としない方式で、PoW計算を並列化し分散するための認可メカニズムを提供する。制御基準は、PoW計算とは別に、場合によってはそれと並行してチェックされ得る。言い換えれば、PoW要求者から要求が受信されたときに、PoW提供者は、受信済みデータを制御基準と突き合わせてチェックし始めるのと実質的に同時に、PoW計算に関する作業を開始し得る。受信済みデータが制御基準を満たせない場合、PoW提供者は、PoW計算に関する作業を停止することができるか、または基準を満たしている場合、作業を続けさせることができる。これには、要求が合法的であり認可されているという仮定の下で利点があり、PoWは、要求者/指定済みデスティネーションにできるだけ速やかに返され得る。ブロックチェーンマイニングは、最初の有効なブロックをネットワークにサブミットする競争を伴うので、これは、厳しい時間制約がある場合の利点を提供することができる。

40

【0113】

使用例において：

次に、図13および図14を特に参照しつつ、われわれは、例示的な一実施形態により、本開示がどのように実践され得るかを説明する。

図13のPoW要求者の視点から：

50

・ステップS1300:PoW要求者1300は、そのmempoolから未確認トランザクション(TX)を選択し、コインベーストランザクションを生成する(関連プロトコルが要求または許可している場合)。他の場合には、PoW要求者にトランザクションを提供する別のソースからトランザクションのセットを受け取ることもある。PoW要求者は、また、PoW提供者またはPoW提供者の活動を認可しおよび/または指示する関連エンティティによって指定された認可要件を満たすように構成された少なくとも1つのトランザクションTX<sub>0</sub>を生成するかまたは入手する。われわれの例示的な例では、要件は、TX<sub>0</sub>が少なくとも1つの指定されたアドレスに資産を移転する少なくとも1つの出力を含むことである。

・ステップS1320:PoW要求者(または関連リソース)は、トランザクションのセットに対するマークルツリーを生成するためにすべてのトランザクションをペアでハッシュ化する。マークルツリーはルートRを有する。

・ステップS1330:いくつかの実施形態において、PoW要求者は、ルートRを、ブロックヘッダの生成に必要な他の情報、たとえばバージョン番号、前のブロックハッシュ、難易度ターゲットおよび/またはタイムスタンプと連結することによって、ブロックメッセージBM(テンプレート)を生成し得る。別の実施形態では、これらの値の少なくとも1つ、いくつか、またはすべては、PoW要求者によって提供される代わりにPoW提供者によって取得され、取り出され、または生成され得る。

・ステップ1340:PoW要求者は、ルートRを(潜在的にブロックメッセージBMの一部として)PoW提供者に送信する。バリデータは、また、Rがルートであるツリーによって表されるトランザクションのブロックにTX<sub>0</sub>が含まれることを証明するためにPoWが使用することができるマークル証明も送信する。このマークル証明は、TX<sub>0</sub>とともにペアと一緒にハッシュ化されたときに、証明者がルートに戻ることに可能にするツリーの部分を含む。この方法で、PoW要求者は、ルートR、認可トランザクションTX<sub>0</sub>、およびTX<sub>0</sub>からRへの経路を生成するために使用することができるトランザクションの最小セットをPoW提供者に送信するだけでよい。PoW提供者は、PoW要求者が認可基準を満たしていることをチェックするためにSPVスタイルの検証を実行することができる(図15)。

【0114】

図14のPoW提供者の観点から:

・ステップS1400:PoW提供者1000は、PoW要求者からトランザクションのセットに対するマークルルートを受信する。これらのトランザクションは、PoWがPoW要求者に代わってPoWを生成するべきブロックの本体を形成する。上で説明されているように、トランザクションのセットは、mempool、少なくとも1つの認可トランザクションTX<sub>0</sub>、および関連する場合はコインベーストランザクションから選択された1つまたは複数のトランザクションを含み得る。マークルルートRは、完全または不完全なブロックメッセージの一部としてPoW要求者から受信され得る。PoW提供者は、また、少なくとも1つの認可要件を満たすように構成された少なくとも1つのトランザクションTX<sub>0</sub>、およびTX<sub>0</sub>がセットに含まれていることを確認するためのマークル証明として働くトランザクションのセットの一部を受信する。

・ステップS1410:PoW提供者は、マークル証明を使用してSPVスタイルのローカル検証を実行しTX<sub>0</sub>がセットに含まれていることを確認し、PoW要求者が認可要件を満たしていることをチェックする。

・ステップS1420:検証が失敗した場合、PoWはPoW計算を続けることを認可されていない。これは、有効なノンスの発見に関する作業を開始することをPoW計算機に指示しないか、またはそうすることをすでに開始している場合には、停止することを指示することによってプロセスを終了する。PoW要求者には送信されるブロックヘッダはない。しかしながら、PoW生成に対する認可が失敗したことを示す警告、信号、またはメッセージが、PoW要求者または別のデスティネーションに送信され得る。

【0115】

代替的に、検証が成功した場合、PoW生成を続けることを認可される。

・ステップS1430:PoWを生成するために、計算機(1100a、1100bまたは1100c)

はノンスを選択するかまたは受信する。これはランダムに生成され得るか、またはコントローラ1200によって計算機に指定された、許可されたノンスの範囲から選択されてもよい。

・ステップS1440:計算機は、ブロックメッセージと選択済みノンスとを連結する。上で説明されているように、PoW要求者が完全なブロックメッセージを提供していない場合、PoW提供者は、関連するブロックチェーンプロトコルに従って、ブロックヘッダの生成に必要な任意の追加データを取り出すか、取得するか、または生成し得ることに留意されたい。ブロックメッセージとノンスとの連結は、ブロックヘッダBHを提供する。

・ステップS1450:ブロックヘッダBHは、次いで、ダブルハッシュ化される。

・ステップS1460:次いで、ステップS1450の結果は、プロトコルによって設定された難易度ターゲットと突き合わせて比較される。前提条件となる数の先行ゼロを提供しない場合、ブロックは台帳に追加できないので、別のノンスが選択され、プロセスはステップS1430に戻る。

・ステップS1470:しかしながら、選択されたノンスが必要とされる数のゼロを生成する場合、ブロックは、有効にマイニングされ、したがって有効なノンスを含むブロックヘッダは、PoW要求者または別の指定されたデスティネーションに送信される。

【0116】

図示されていないが、PoW要求者または別のエンティティは、次いで、オンチェーンで包含するためにブロックをネットワークにサブミットすることができる。重要なのは、PoWの生成は専門家、PoW提供者にアウトソーシングされているので、PoW要求者は、PoW計算と並行して有効性確認作業などの他のタスクを処理するか、委任するか、協調することができるということである。これは、トランザクションの処理速度およびリソースの効率性の点で技術的な改善を提供する。

【0117】

利点:

本開示の態様は、限定はしないが、以下を含む、多数の利点を提供する。

1. PoWを計算する労力およびコストは、PoW要求者によってそれらの選択の任意のPoW提供サービスに委任され、アウトソーシングされ得る。

2. これらは、バリデータが既存の関係を持たない提供者ですらあってもよい。その代わりに、PoW要求者とPoW提供者との関係は、PoW作業を行う事前認可として働く少なくとも1つの事前指定基準を満たすことによって支配される。いくつかの実装形態において、PoW要求者は、PoW提供者がPoW計算作業を開始する前に、必要な基準が満たされていることを確実にするために使用することができるマークル証明を送信する。

3. これは、PoW要求者およびPoW提供者は両方とも候補ブロックが事前指定されたまたは合意された条件を満たすトランザクションを収容することを証明できるので、PoWプロセスに事前認可の追加の層が組み込まれることを可能にする。ブロックが首尾よくマイニングされ、トランザクションがブロックチェーンに含まれる場合、トランザクションおよび資産のその移転は不変的に記録される。認可基準が指定済みアドレスへの移転を要求する場合、PoW提供者は、ブロックが台帳に書き込まれた場合に望む移転が行われることを確実にされ得る。

4. したがって、事前指定された基準を満たすことは、PoW提供者によって処理されるべきデータ中に証明可能に埋め込まれる。これは、PoW要求者からPoW提供者に別々に送信されることはない。これは、別個の通信を伴うアプローチと比較してより効率的なソリューションを提供する。

5. このソリューションはマイニングおよび有効性確認タスクの分散を可能にするので、トランザクション処理機能は、ブロックヘッダの処理から分離される。したがって、ハッシュマシン/ASICコンポーネントは1つまたは複数のロケーションに置くことができ、一方でトランザクション処理は他のロケーションで実行され得る。異なる機能に対するロケーションは、エネルギー資源またはネットワークインフラストラクチャなどの異なるニーズに従って選択され得る。たとえば、PoW提供者はPoW要求者に小さな(80バイトの)

10

20

30

40

50

ブロックヘッダを返すだけでよいので、インターネットへのアクセスが制限されていても再生可能エネルギー源の使用を可能にする孤立したロケーションに置くことができる。ブロックヘッダは、低帯域幅の携帯電話を使用して送信され得る。他方、トランザクション処理は、主要都市など、インターネットへのアクセスが良好なロケーションで実行され得る。同時に、これは、持続可能な、環境に優しいエネルギー供給源の使用を含む、タスクのより用途の広い効率的な分散を可能にする。

6.  $TX_0$ が制御基準と突き合わせて比較され、合法的な要求者からの要求のみが処理されることを確実にするという点で、追加のセキュリティが提供され得る。これは、無認可当事者、攻撃者などの悪意のある当事者による搾取、および/または望ましくないもしくは違法行為に潜在的に関連する当事者に対するPoW作業の提供、ひいては犯罪行為への参加を回避することができる。

7.  $TX_0$ を介して供給される制御データを介して要求者が様々な方法で自己を識別することができるので、ブロックチェーンマイニングに対する認可および制御技術が改善される。

【0118】

可能な実施形態の例示的なシステム

図7および図9は、説明された実施形態のうちの少なくともいくつかを実装するための例示的なシステム700を例示している。図8は、本開示の方法(の高水準ビュー)において取り得る例示的なステップのフローチャートを例示している。

【0119】

システム700は、組織に関連付けられ、より大きな専有システムの一部を形成し得るという意味で閉鎖システムであり得る。そのような場合、そのデータ、たとえばトランザクションは、組織のより広いシステム内の他のコンポーネントから受信され、その結果および出力は内部のデスティネーションに送信され得る。それに加えて、または代替的に、システム700は、組織の外部にその一部または全部が配置され得る様々なエンティティとインターフェースするように構成され得る。そのような場合、システム700は、有効性確認機能をサービスとして提供するように構成され得る。たとえば、システム700は、必要とするデータを取得するためにブロックチェーンネットワークとインタラクティブにやり取りするように構成され得る。それに加えて、または代替的に、システム700は、その有効性確認サービスを使用することを望んでいるエンティティとインタラクティブにやり取りすることも可能である。したがって、システム700の活動は、特定の組織またはエンティティに関してもっぱら内部的であり得るか、または他の当事者に有効性確認サービスを提供するために外部のエンティティとのインタラクションに開かれているか、またはその2つの組合せであってもよい。他の内部エンティティまたは外部エンティティの間の通信は、図9に902として示されている1つもしくは複数のインターフェースまたは通信コンポーネントによって協調させられ得る。

【0120】

図7および図9に示されているように、システム700は、制御エンティティ702(または単に「コントローラ」)および本明細書では単に「バリデータ」とも称される複数の有効性確認リソース704を含む。図7には4つのバリデータ701a~dのみが示されているが、一般に、システム700は任意の数のバリデータを含み得る。さらに、コントローラ702は、バリデータ704とは別個のものとして図7および図9に示されているが、コントローラ702がバリデータ704のうちの1つを含むか、またはバリデータ704によって構成され得ることは排除されない。上で説明されているように、各バリデータは、1つまたは複数の処理リソースを含み、それ自身の内部活動を協調させるためのそれ自身のコントローラを含み得る。このようにして実装できる階層レベルに対する、技術的または論理的な制限はない。しかしながら、図7は、理解するのに単純で容易であるように、そのような階層の1つ(最上位)のレベルのみを示している。

【0121】

図7に示されているように、コントローラ702は、トランザクションのセットを取得す

る。トランザクションは、送信リソースから電子チャネルまたはネットワークにまたがって受信され得る。送信者は、上で説明されているように、システムの組織の内部または外部で、ある種の有効性確認チェックを実行することを望んでいる任意のエンティティであり得る。たとえば、これは、図1のノード104などの、ブロックチェーンネットワーク上のフルノード、またはデジタルウォレット、または当事者間で行われるブロックチェーン実装送金に関係するローカルチェックを実行することを望んでいるマーチャント/SPVノードであり得る。インターフェース902は、システム700とシステム外部のソースとの間のデータの伝送を円滑にし得る。

#### 【0122】

トランザクションは、トランザクションのブロックを形成するか、または形成し得る。トランザクションは、単一のリソースから(たとえばブロックチェーンのブロックから)、または異なるリソースから(たとえば1つまたは複数のユーザ、1つまたは複数のブロックチェーンノードなどから)取得されてもよい。トランザクションは、それらがブロックチェーン上で公開されるのに先立ち、すなわちブロックに記録される前に取得され得る。代替的に、トランザクションは、ブロックチェーンに記録された後に取得され得る。

#### 【0123】

コントローラ702は、本明細書で説明するように、トランザクションのそれぞれのサブセットを各バリデータ704に割り当てる。トランザクションの各サブセットは、トランザクションのフルセットに基づき生成されたマークルツリーのそれぞれの部分の少なくとも一部を形成し、マークルツリーのそれぞれの共通の内部ノードによってリンクされる。図7の例では、トランザクションのサブセットAがバリデータAに割り当てられ、トランザクションのサブセットBがバリデータBに割り当てられ、トランザクションのサブセットCがバリデータCに割り当てられ、トランザクションのサブセットDがバリデータDに割り当てられている。トランザクションのサブセットが割り当てられると、バリデータ704はそれらのそれぞれのサブセットを処理する。いくつかの実施形態において、これは、各バリデータ704がトランザクションのそれぞれのサブセットを有効性確認することを伴う。これを行うために、コントローラ702は、関連するトランザクションをそれぞれのバリデータ704に伝送し得る。バリデータ704は、トランザクションのそれらのそれぞれのサブセットの各々が有効であること、または少なくとも1つのトランザクションが有効でないことを示すためにコントローラ704に通信内容を送り返すものとしてよい。

#### 【0124】

バリデータ704aから704dのうちの少なくとも1つ、ただし好ましくはいくつかもしくはすべてが、図9において901aから901dとして示されているそれ自身のUTXOプールへのアクセス権を有する。このプールは、上で説明されているデータベースなどのストレージファシリティを含み、潜在的に、有利なインデックス付け構造はブロックIDとトランザクションIDとの連結を含む。図9では、プールは各バリデータ内に含まれるものとして示されているが、当業者であれば、これらがさらに/代替的にバリデータの外部にあるものとして設けられるがそれらと通信するものであってもよいことを容易に理解するであろう。

#### 【0125】

1つまたは複数の実施形態において、開示されているプロセスは、ブロックレベル有効性確認段階を含むことができ、この段階で、入ってくる新しいブロックは、ブロックレベル基準と突き合わせて検査される。例示的なブロックレベル基準は上で説明されており、一般的に、規定された形式要件およびブロック内のトランザクションとは反対に、ブロックそれ自体に適用可能な特性または制限に関係する。例は、ブロックサイズ、ブロックヘッダ構造、またはコンテンツ、および類似の基準を含む。そのような動作は、コントローラ、またはコントローラのコンポーネント、または別のシステムコンポーネントによって実行され得る。

#### 【0126】

いくつかの実施形態において、この方法は、新しいブロック内のトランザクションへの

入力の各々、すなわち各UTXOが一意であるかどうかを評価するように動作可能であるUTXO一意性確認モジュールをさらに含み得る。同じUTXOが新しいブロック内の入力として複数回出現した場合、それは潜在的な二重支払いの問題があることを示し、UTXO一意性基準に違反する。UTXO一意性確認モジュールが、新しいブロック内のトランザクション入力の中で複数回参照されているUTXOを識別した場合、そのブロックが拒絶されるべきであることを示す誤り信号または他の割り込みを出力し得る。

#### 【0127】

新しいブロックが拒絶されない、すなわちすべてのUTXO入力が一意であると仮定すると、マークルツリーセグメントは、次いで、識別され、その関連付けられたトランザクションがバリデータのセットの間に割り当てられ得る。識別プロセスは、図9に示されている、セグメント識別ユニット903などのコンポーネントによって実行され得る。割り当てプロセスは、図9に904として示されているセグメント割り当てユニットによって実行され得る。割り当てユニット904は、個別のバリデータ間にブロックセグメントを分散させるために多数の可能な割り当てスキームのいずれか1つを採用し得るが、有利なアプローチでは、割り当てスキームは、上で説明されているように負荷分散を目的とするものとしてよい。割り当てユニット904は、負荷分散ユニット905を含む(またはそれと通信する)ものとしてよい。これは、図9では、システムの別個の関連付けられているコンポーネントとして示されているが、他の実施形態では、負荷分散ユニットは、割り当てユニット904の一部であり得るか、またはコントローラ702に関して別になってもよい。コンポーネントの任意の組合せは、容易に採用され得る。

#### 【0128】

個別のバリデータは、これらが受信するセグメントに関連付けられているトランザクションの有効性を、トランザクションレベル有効性確認基準と突き合わせて確認する。バリデータは、割り当てられたトランザクションが有効であることを検証することに対して各々独立して働きかけるときにバリデータ間の同期パラダイムを必要としない。各バリデータは、その割り当て済みトランザクションを有効性確認する結果を出力する。これらの結果は、セグメント内のすべてのトランザクションが有効であることを確認するために加えられるかまたは蓄積される。これらのバリデータのうちの1つが非準拠トランザクション、すなわち無効なトランザクションを識別した場合、バリデータは、無効なトランザクションがあることを示すために、割り込みまたは他の信号などの出力を発するものとしてよい。その割り込みまたは信号は、他のバリデータに、またはコントローラもしくは別のシステムコンポーネントに送信され、それぞれのトランザクションの検査を直ちに中止し、拒絶されるべきブロック内のトランザクションを有効性確認することに対してさらなるリソースを浪費しないようにすることができる。

#### 【0129】

いくつかの例において、システムは、ブロックレベル基準をチェックするように構成され得る。これは、セグメントをバリデータに割り当てることに先立ち実行され得るが、ブロックレベル有効性確認段階は、バリデータによるトランザクションレベル有効性確認検査の後に、またはいくつかの場合において、トランザクションレベル有効性確認検査と並行して、起こり得ることは理解されるであろう。

#### 【0130】

次に、ブロックの有効性の確認する方法の一例をフローチャートの形で示す図8を参照する。ブロックは、複数のトランザクションを収容し、各トランザクションは1つまたは複数の入力を参照し、各入力はUTXOである(コインベース生成トランザクションの場合を除く)。方法は、ブロックチェーンネットワーク上のノード内で好適なハードウェアおよびプロセッサ実行可能命令を使用して実装される。

#### 【0131】

動作時、分散有効性確認ノード700は、ステップS801で新しいブロックデータを受信する。これは、ブロック全体であり得るか、またはSPV関係有効性確認の場合には、SPVチェックを実行するために必要な部分的データのみを含み得る。われわれは、便宜上、

10

20

30

40

50

これを「ブロック」としてのデータと称する。有効性確認されるべき新しいブロックは、新しいブロックを生成してプルーフオブワークを完了したブロックチェーンネットワーク上のマイニングノードから受信され得るか、または(SPV)チェックを実行することを望んでいるマーチャントノードから受信され得るか、またはSPVウォレットなどのウォレットから受信され得る。新しいブロックは、ネットワーク内の別の(非マイニング)ノードから受信され得る。いくつかの例において、分散有効性確認ノード700は、ネットワーク内の任意の他のノードに転送する前にブロックを有効性確認する。上で説明されているように、新しいブロックの有効性確認は、ブロックが特定のプロトコルベースの基準、および/または所与の実装形態内で指定され要求され得る他の基準を満たすことを確認することを含み得る。

10

#### 【0132】

ステップS802において、システム700は、ブロックのマークルツリーのチャンクを識別する。S803で、セグメントは、複数のバリデータに分配され、S804で、バリデータは、実質的に並行して、互いに独立してトランザクションのそれぞれのサブセットを処理する。S805で、バリデータは、有効性確認が成功したか失敗したかをコントローラにシグナリングする。

#### 【0133】

本明細書における並列プロセッサの説明に関して使用されたときに、「プロセッサ」という用語は、必ずしも物理的に異なるマイクロプロセッサを意味するものではなく、プロセッサ機能を独立して並列に実行することができる並列処理リソースを可能にする任意のハードウェアまたはソフトウェア実装形態を含み得ることに留意すべきである。並列プロセッサは、複数のコアを有する1つのプロセッサを含み得る。いくつかの場合において、並列プロセッサは、複数の別々の処理ユニットを備え得る。並列プロセッサは、物理メモリを共有することも共有しないこともある。各並列プロセッサは、どのように実装されるにせよ、無効なトランザクションを識別したことに応答して信号を出力するなど、シグナリングのためのソフトウェアまたはハードウェアメカニズムを有する。並列プロセッサの実装形態は、また、割り当てられたトランザクションデータをローカル処理のためにそれぞれのプロセッサにルーティングする、必要なデータ転送メカニズムをソフトウェアおよび/またはハードウェアで提供することを含む。

20

#### 【0134】

列挙された条項

本開示の実施形態は、例示を目的として、限定することなく、以下の列挙された条項において提示される。

30

#### 【0135】

本開示の列挙された条項または態様の1つのセットに関して以下で言及される特徴は、そのような点で限定されることを意図されるのではなく、条項の1つのセットに関して言及される任意の特徴は、条項の他のセットのうちの1つまたは複数に組み込まれ得る。

#### 【0136】

条項セット1:

条項1.1:複数のブロックチェーントランザクションを含むブロックチェーンブロックの少なくとも一部およびブロックに対するマークルツリーのルートを処理する(たとえば、有効性確認する)コンピュータ実装方法。

40

この方法は

ブロックチェーントランザクションのそれぞれのサブセットを複数の処理(たとえば、有効性確認リソース)に割り当てることであって、各それぞれのサブセットは、マークルツリーのそれぞれの部分を提供し、マークルツリーのそれぞれの内部ノードによって表される、割り当てること、および/または

複数の処理(たとえば有効性確認)リソースを使用して、ブロックチェーントランザクションのそれぞれのサブセットを処理(たとえば有効性確認)することを含み得る。

50

## 【0137】

それに加えて、または代替的に、この方法は、

複数のブロックチェーントランザクションを含むブロックチェーンブロックの少なくとも一部およびそのブロックに対するマークルツリーのルートを送信するか、または受信することを含み得る。ブロックチェーンブロックの一部分は、送信リソースから受信リソースに送信され得る。これはインターネットなどのネットワークを介して送信され得る。この方法は、受信リソースにおいてブロックチェーンブロックの一部を処理するステップを含み得る。受信リソースは、処理リソースまたは有効性確認リソースと称され得る。ブロックチェーンブロックの一部分は、IPv6マルチキャスト伝送を使用して送信されてもよい。複数の処理リソースの少なくとも1つ、いくつか、またはすべては、IPv6マルチキャストグループのメンバーであってよい。送信リソースは、ネットワークデバイスを備え得る。ネットワークデバイスは、IPv6マルチキャスト通信をマルチキャストアドレスに送信するように動作可能であり得る。MLDスヌーピングがネットワークデバイスにおいて有効化され得る。これは、送信リソースがブロックチェーンブロックの一部分を特定の受信リソース(たとえば、複数の処理リソース内のリソース)に選択的に送信することができるので、ネットワーク上のトラフィックに関する効率を提供する。データの受信を必要とすることまたはデータを受信することを望むことがないものを含む、ネットワーク上のすべてのリソースにデータパケットを送信することによってネットワークトラフィックが削減され、エネルギーおよび処理リソースが浪費されない。また、これはサービス拒否(DOS)攻撃の可能性を回避するのでセキュリティを改善し、また、ネットワーク輻輳のレベルが低いことによりトランザクションの処理速度を速めることによってブロックチェーンネットワークのスケラビリティを促す。

## 【0138】

「バリデータ」という用語は、「有効性確認リソース」という用語と交換可能に使用され得る。本明細書において、便宜上、「プロセッサ/処理」の代わりに「バリデータ/有効性確認」が使用され得る。複数の有効性確認リソースは、分散有効性確認ノードを形成し得る。複数の有効性確認リソースのうちの少なくとも1つは、1つまたは複数の処理リソースを含み得る。それに加えて、または代替的に、複数の有効性確認リソースのうちの1つまたは複数の、実質的に本明細書において説明されているようなバリデータコントローラコンポーネントを含み得る。分散有効性確認ノード内の有効性確認リソースの少なくとも1つまたはいくつかは、共通のIPv6マルチキャストアドレスを共有する、すなわちサブスクライブし得る。

## 【0139】

それぞれの内部ノードは、セグメントルートであってもよい。言い換えると、「内部ノード」とは、ツリー全体のルートノードでもリーフノードでもない、マークルツリーのノードのことである。各サブセット内のトランザクションは、それぞれ共通内部ノードを共有し得る。

## 【0140】

代替的な表現では、各サブセットは、サブセットがマークルツリーの(サブ)部分を提供する、および/またはマークルツリーの(サブ)部分によって表現されるように、マークルツリー内の共通ノードに関連付けられている少なくとも2つのトランザクションを含み得る。共通(内部)ノードは、実質的に本明細書において説明されているようにセグメントノードまたはルートであってよい。マークルツリーの一部分は、実質的に本明細書において説明されているような「セグメント」であってよい。

## 【0141】

条項1.2。条項1.1に記載の方法であって、ブロックチェーンブロックおよび/またはブロックチェーントランザクションのサブセットを有効性確認することは、

i) 少なくとも1つのブロックチェーントランザクションを有効性確認しおよび/または検証すること、および/または

ii) Simplified Payment Verification (SPV) プロセスを実行すること、および/ま

10

20

30

40

50

たは

iii) 所与のブロックチェーントランザクション(Tx)がブロックチェーンブロック内に収容されるかどうかを確認すること、および/または

iii) ブロックチェーントランザクションの少なくとも1つのハッシュを生成し、そのハッシュを使用してマークル経路を構築し、および/またはそのハッシュがブロックチェーンブロックのヘッダ内のトランザクション識別子(Txid)と一致するかどうかをチェックすること

を含む、方法。

【0142】

条項1.3。条項1.1または1.2に記載の方法であって、

10

ブロックチェーントランザクションのサブセットのうちの少なくとも1つは、サブセットに関連付けられている、サブセットを識別しおよび/または表す、識別子を含む方法。

【0143】

条項1.4。条項1.3に記載の方法であって、

識別子は、マークルツリー内の少なくとも1つのサブセットの位置の計算を円滑にする、方法。

【0144】

条項1.5。条項1.3または1.4に記載の方法であって、

識別子は、ブロックチェーントランザクションの少なくとも1つのサブセット内のブロックチェーントランザクションのハッシュの一部を含む、方法。

20

【0145】

条項1.6。条項1.1から1.5のいずれか一項に記載の方法であって、

ブロックチェーントランザクションのそれぞれのサブセットを複数の有効性確認リソースに割り当てるステップは、トランザクションのサブセットに関連付けられているそれぞれの識別子に基づきそれぞれのサブセットをそれぞれの有効性確認リソースと照合することを含む、方法。

【0146】

条項1.7。条項1.1から1.6のいずれか一項に記載の方法であって、

i) ブロックチェーントランザクションの少なくとも1つのサブセットを複数の有効性確認リソースのうちの少なくとも1つにダウンロードするステップ、および/または

30

ii) ブロックチェーントランザクションの少なくとも1つのサブセットを複数の有効性確認リソースのうちの少なくとも1つに送信するステップをさらに含む、方法。

【0147】

条項1.8。条項1.1から1.7のいずれか一項に記載の方法であって、

マークルツリーは、二分木または複数のブロックチェーントランザクションのハッシュのメッシュを含む、方法。

【0148】

条項1.9。条項1.1から1.8のいずれか一項に記載の方法であって、

複数のブロックチェーントランザクション内のブロックチェーントランザクションのサブセットを識別しおよび/または決定するステップをさらに含む、方法。

40

【0149】

条項1.10。条項1.1から1.9のいずれか一項に記載の方法であって、

複数の有効性確認リソースのうちの少なくとも1つは、

仮想マシン、サーバ、GPUベースコンピューティングリソース、処理スレッド、および/またはマルチプロセッサシステムのうちの1つまたは複数であるか、またはこれらのうちの1つまたは複数を備える、方法。

【0150】

条項1.11。条項1.1から1.10のいずれか一項に記載の方法であって、

i) 少なくとも2つのトランザクションは、マークルツリーにおいて兄弟姉妹であり、および/または

50

ii) 共通ノードは、少なくとも2つのトランザクションの親または先祖である、方法。

【0151】

条項1.12。複数のブロックチェーントランザクションを含むブロックチェーンブロックの少なくとも一部およびそのブロックに対するマークルツリーのルートの有効性確認するように動作可能であるブロックチェーン有効性確認システムであって、

システムは、複数の有効性確認リソースを備え、複数の有効性確認リソースは、プロセッサと、

プロセッサによる実行の結果として、条項1.1から1.11のいずれか一項に記載のコンピュータ実装方法をシステムに実行させる実行可能命令を含むメモリとを各々備える、ブロックチェーン有効性確認システム。

【0152】

条項1.13。コンピュータシステムのプロセッサによって実行された結果として、条項1.1から1.11のいずれか一項に記載のコンピュータ実装方法をコンピュータシステムに実行させる実行可能命令をその上に記憶した非一時的コンピュータ可読記憶媒体。

【0153】

本開示の別の態様によれば、本明細書において説明されるかまたは請求されている任意の方法ステップまたは方法ステップの組合せを実行するように構成されたコンピュータ実装システムが提供される。

【0154】

複数のコンピュータ実装ノードを含むブロックチェーンシステム(ネットワーク)も提供され、ブロックチェーンネットワーク内の各ノードは、

プロセッサと、

プロセッサによる実行の結果として、本明細書において請求されるか、または説明されているコンピュータ実装方法の任意の変更形態をシステムに実行させる実行可能命令を含むメモリとを備える。

ネットワークは、本明細書において説明されているようなブロックチェーンプロトコルを使用して動作するように構成され得る。

【0155】

それに加えて、または代替的に、本開示は、ブロックチェーンブロックの少なくとも一部をダウンロードするコンピュータ実装方法を含み得る。ブロックは、複数のブロックチェーントランザクションと、ブロックに対するマークルツリーのルートとを含み得る。方法は、次の条項の1つまたは複数において規定されるステップを含み得る。

【0156】

条項セット2:

条項2.1。複数のブロックチェーントランザクションを含むブロックチェーンブロックの少なくとも一部およびブロックに対するマークルツリーのルートを受信する、たとえば、ダウンロードするコンピュータ実装方法であって、

ブロックチェーントランザクションのそれぞれのサブセットを複数の処理リソースに割り当てることであって、各それぞれのサブセットは、マークルツリーのそれぞれの部分を提供し、マークルツリーのそれぞれの内部ノードによって表される、割り当てることと、

複数の処理リソースの1つ、いくつか、またはすべてを使用してブロックチェーントランザクションのそれぞれのサブセットを受信する、たとえば、ダウンロードすることを含む、コンピュータ実装方法。

【0157】

1つまたは複数の実施形態によれば、処理リソースの1つ、いくつか、またはすべては、提供(送信)リソースからブロックチェーントランザクションのそれぞれのサブセットを受信し得る。これはインターネットなどのネットワークを介して送信され得る。ブロックチェーントランザクションのそれぞれのサブセットは、IPv6マルチキャスト伝送を使用して送信されてもよい。複数の処理リソースの少なくとも1つ、いくつか、またはすべては、IPv6マルチキャストグループのメンバーであってよい。送信リソースは、ネットワ

10

20

30

40

50

ークデバイスを備え得る。ネットワークデバイスは、IPv6マルチキャスト通信をマルチキャストアドレスに送信するように動作可能であり得る。MLDスヌーピングがネットワークデバイスにおいて有効化され得る。これは、送信リソースがブロックチェーントランザクションのサブセットを特定の受信リソース(たとえば、複数の処理リソース内のリソース)に選択的に送信することができるので、ネットワーク上のトラフィックに関する効率を提供する。データの受信を必要とすることまたはデータを受信することを望むことがないものを含む、ネットワーク上のすべてのリソースにデータパケットを送信することによってネットワークトラフィックが削減され、エネルギーおよび処理リソースが浪費されない。また、これはサービス拒否(DOS)攻撃の可能性を回避するのでセキュリティを改善し、また、ネットワーク輻輳のレベルが低いことによりトランザクションの処理速度を速めることによってブロックチェーンネットワークのスケーラビリティを促す。

10

【0158】

各それぞれのサブセットは、それぞれの内部ノードがそれぞれのサブセットを符号化し得るという意味で、それぞれの内部ノードによって表され得る。すなわち、それぞれの内部ノードは、それぞれのサブセットに基づき(すなわち、それぞれのサブセットの関数として)生成され得る。それぞれのサブセット内の各トランザクションは、1つまたは複数のハッシュ演算によってそれぞれの内部ノードにリンクされる。

【0159】

条項2.2。条項2.1に記載の方法であって、

複数の処理リソースの1つ、いくつか、またはすべてがブロックチェーントランザクションのそれぞれのサブセットを中央ストレージロケーションに送信することを含む、方法。

20

【0160】

条項2.3。条項2.2に記載の方法であって、

マークルツリーのそれぞれの内部ノードは、マークルツリーにおけるそれぞれの位置を有し、この方法は

ブロックチェーントランザクションのそれぞれのサブセットを、マークルツリーのそれぞれの内部ノードのそれぞれの位置に基づき構成することを含む、方法。

【0161】

条項2.4。条項2.1から2.3のいずれか一項に記載の方法であって、

処理リソースの1つ、いくつか、またはすべてが、ブロックチェーントランザクションのそれぞれのダウンロード済みサブセットに基づきマークルツリーのそれぞれの候補内部ノードを生成することを含み、

30

それぞれの候補内部ノードが、マークルツリーのそれぞれの内部ノードと一致することを確認すること、および/または

それぞれの候補内部ノードがマークルツリーのノードであることを、マークルツリーのルートに基づきマークル証明を実行することによって、確認すること、および/または

マークルツリーのそれぞれの候補内部ノードを、1つまたは複数の他の処理リソースに送信することのうちの少なくとも1つをさらに含む、方法。

【0162】

40

条項2.5。条項2.1から2.4のいずれか一項に記載の方法であって、

複数の処理リソースの1つ、いくつか、またはすべてを使用してブロックチェーントランザクションのそれぞれのサブセットを有効性確認することを含む、方法。

【0163】

条項2.6。条項2.1に記載の方法であって、

ブロックチェーントランザクションのそれぞれのサブセットを有効性確認することは、

i) 少なくとも1つのブロックチェーントランザクションを有効性確認しおよび/または確認すること、および/または

ii) Simplified Payment Verificationプロセスを実行すること、および/または

iii) 所与のブロックチェーントランザクションがブロックチェーンブロック内に収容さ

50

れるかどうかを確認すること、および/または

iii) ブロックチェーンランザクションの少なくとも1つのハッシュを生成し、そのハッシュを使用してマークル経路を構築し、および/またはそのハッシュがブロックチェーンブロックのヘッダ内のランザクション識別子と一致するかどうかをチェックすることを含む、方法。

【0164】

条項2.7。条項2.1から2.6のいずれか一項に記載の方法であって、

ブロックチェーンランザクションのそれぞれのサブセットのうちの少なくとも1つは、それぞれのサブセットに関連付けられる、識別する、および/または表すそれぞれの識別子を含む、方法。

【0165】

条項2.8。条項2.7に記載の方法であって、

それぞれの識別子は、マークルツリー内の少なくとも1つのそれぞれのサブセットのそれぞれの位置の計算を円滑にする、方法。

【0166】

条項2.9。条項2.7または2.8に記載の方法であって、

それぞれの識別子は、マークルツリーのそれぞれの内部ノードに基づく、方法。

【0167】

条項2.10。条項2.9に記載の方法であって、

それぞれの識別子は、マークルツリーのそれぞれの内部ノードの一部を含む、方法。

【0168】

条項2.11。条項2.1から2.10のいずれか一項に記載の方法であって、

ブロックチェーンランザクションのそれぞれのサブセットを複数のそれぞれの処理リソースに割り当てるステップは、ランザクションのそれぞれのサブセットに関連付けられるそれぞれの識別子に基づきそれぞれのサブセットをそれぞれの処理リソースと照合することを含む、方法。

【0169】

条項2.12。条項2.1から2.11のいずれか一項に記載の方法であって、

マークルツリーは、二分木または複数のブロックチェーンランザクションのハッシュのメッシュ構造を含む、方法。

【0170】

条項2.13。条項2.1から2.12のいずれか一項に記載の方法であって、

複数のブロックチェーンランザクション内のブロックチェーンランザクションのサブセットを識別しおよび/または決定するステップを含む、方法。

【0171】

条項2.14。条項2.1から2.13のいずれか一項に記載の方法であって、

複数の処理リソースのうちの少なくとも1つは、仮想マシン、サーバ、GPUベースのコンピューティングリソース、またはマルチプロセッサシステムであるか、またはそれらを含む、方法。

【0172】

条項2.15。複数のブロックチェーンランザクションを含むブロックチェーンブロックの少なくとも一部およびそのブロックに対するマークルツリーのルートをダウンロードするように動作可能であるブロックチェーン処理システムであって、システムは、複数の処理リソースを備え、複数の処理リソースは、

プロセッサと、

プロセッサによる実行の結果として、条項2.1から2.14のいずれか一項に記載のコンピュータ実装方法をシステムに実行させるか、またはシステムが実行することを可能にする実行可能命令を含むメモリとを各々備える、ブロックチェーン処理システム。

【0173】

条項2.16。コンピュータシステムのプロセッサによって実行された結果として、条項2.

10

20

30

40

50

1から2.14のいずれか一項に記載のコンピュータ実装方法をコンピュータシステムに実行させるか、またはコンピュータシステムが実行することを可能にする実行可能命令をその上に記憶した非一時的コンピュータ可読記憶媒体。

【0174】

別の態様によれば、コンピュータシステムのプロセッサによって実行された結果として、本明細書において請求されているか、または説明されているコンピュータ実装方法の任意のバージョンをコンピュータシステムに実行させる実行可能命令をその上に記憶した非一時的コンピュータ可読記憶媒体が提供される。

【0175】

条項セット3:

10

条項3.1。コンピュータ実装方法であって、

ブロックチェーンブロックの複数のブロックチェーントランザクション(TX)におけるトランザクション(Tx)に各々関連付けられている、複数の未消費トランザクション出力(たとえば、UTXO)を記録し、検索し、および/または処理するための第1の出力リポジトリを生成し、保存し、および/または維持するステップを含み、

複数のブロックチェーントランザクションは、ブロックチェーンブロックに対するマークルツリーの一部を提供する、および/またはマークルツリーの一部によって表される、コンピュータ実装方法。

【0176】

条項3.2。条項3.1に記載の方法であって、

20

少なくとも1つのさらなる出力リポジトリを生成し、保存し、および/または維持することを含む、方法。

【0177】

条項3.3。条項3.1または3.2に記載の方法であって、

出力リポジトリに関係するアクション、変更、およびイベントの履歴を含むデータベースログを生成し、および/または維持することをさらに含む、方法。

【0178】

条項3.4。条項3.1から3.3のいずれか一項に記載の方法であって、

第1および/またはさらなる出力リポジトリは、

i)未消費トランザクション出力、および/または

30

ii) a)未消費トランザクション出力および/またはb)複数のブロックチェーントランザクションにおけるトランザクション(Tx)に関連付けられたものに関連付けられている少なくとも1つのレコードを含む、方法。

【0179】

条項3.5。条項3.4に記載の方法であって、

少なくとも1つのレコードは、

i)ブロックチェーンブロックに関連付けられているブロック識別子(block\_ID)、および/または

ii)複数のブロックチェーントランザクションにおけるトランザクション(Tx)に関連付けられたトランザクション識別子(TxID)を有するレコード識別子を含む、方法。

40

【0180】

条項3.6。条項3.5に記載の方法であって、

i)レコード識別子は、ブロック識別子(block\_ID)とトランザクション識別子(TxID)の関数を含み、および/または

ii)ブロック識別子(block\_ID)とトランザクション識別子(TxID)の連結があり、および/または

iii)複数のブロックチェーントランザクションのトランザクションは、未消費トランザクション出力に関連付けられる、方法。

【0181】

条項3.7。条項3.5または3.6に記載の方法であって、

50

レコード識別子を使用して、出力リポジトリ内の少なくとも1つのレコードを検索するか、識別するか、アクセスするか、または挿入するステップをさらに含む、方法。

【0182】

条項3.8。条項3.1から3.7のいずれか一項に記載の方法であって、

複数の未消費トランザクション出力のうちの少なくとも1つの未消費トランザクション出力(UTXO)は、出力リポジトリにおいて、

i)未消費トランザクション出力が消費のために利用可能であるかもしくは利用不可能であるかを示し、および/または

ii)未消費トランザクション出力の消費が許可されていることを示す第1の状態と、未消費トランザクション出力の消費が禁止されていることを示す第2の状態との間で構成可能であるロックフラグと関連付けられる、方法。

10

【0183】

条項3.9。条項3.8に記載の方法であって、

i)未消費トランザクション出力をロックフラグと関連付けるステップ、および/または

ii)ロックフラグの状態を第1の状態から第2の状態に、または第2の状態から第1の状態に、変更するステップを含む、方法。

【0184】

条項3.10。条項3.8または3.9に記載の方法であって、

第1の処理リソースから少なくとも1つのさらなる処理リソースに通信内容を送信して、少なくとも1つのさらなる処理リソースに、未消費トランザクション出力に関連付けられているロックフラグの状態を第1の状態から第2の状態に、または第2の状態から第1の状態に変更させるステップを含む、方法。

20

【0185】

条項3.11。条項3.10に記載の方法であって、通信内容は、

i)トランザクション(TX)、トランザクション識別子(TxID)、および/またはトランザクション(Tx)のハッシュと、

ii)1つまたは複数の未消費トランザクション出力のリストとを含む、方法。

【0186】

条項3.12。条項3.10または3.11に記載の方法であって、

少なくとも1つのさらなる処理リソースにおいて通信内容を受信するステップと、

ロックフラグの状態を第1の状態から第2の状態に、または第2の状態から第1の状態に変更するステップとを含む、方法。

30

【0187】

条項3.13。条項3.1から3.12のいずれか一項に記載の方法であって、

i)マークルツリーの一部は、ブロックチェーンブロックに対するマークルツリーのサブ部分またはセグメントであり、および/または

ii)複数のブロックチェーントランザクションは、マークルツリーの内部ノードによって表される、方法。

【0188】

条項3.14。複数の処理リソースを含むブロックチェーン実装システムであって、複数の処理リソースは、

プロセッサと、

プロセッサによる実行の結果として、条項3.1から3.13のいずれか一項に記載のコンピュータ実装方法をシステムに実行させるか、またはシステムが実行することを可能にする実行可能命令を含むメモリとを各々備える、ブロックチェーン実装システム。

40

【0189】

条項3.15。コンピュータシステムのプロセッサによって実行された結果として、条項3.1から3.13のいずれか一項に記載のコンピュータ実装方法をコンピュータシステムに実行させるか、またはコンピュータシステムが実行することを可能にする実行可能命令をその上に記憶した非一時的コンピュータ可読記憶媒体。

50

## 【0190】

## 条項セット4

条項セット4内の任意の条項または条項の組合せで定義される任意の実施形態は、条項セット1から3内の任意の条項を実装するか、または組み合わせるように構成され得る。

## 【0191】

条項4.1。複数のブロックチェーントランザクションを含むブロックチェーンブロックの少なくとも一部およびそのブロックに対するマークルツリーのルートを有効性確認するように動作可能であるシステムであって、

複数の処理(たとえば、有効性確認)リソースであって、

実行可能命令を記憶するメモリの少なくとも一部分に関連付けられた少なくとも1つのプロセッサであって、実行可能な命令は、少なくとも1つのプロセッサによる実行の結果として、有効性確認リソースが

複数のブロックチェーントランザクションの少なくとも1つのサブセットを処理する(たとえば、有効性確認する)ことを引き起こすか、または可能にし、少なくとも1つのサブセットは、マークルツリーの一部を提供し、マークルツリーの内部ノードによって表される、

少なくとも1つのプロセッサ

を各々備える、複数の有効性確認リソース

を備える、システム。

## 【0192】

条項4.2。条項4.1に記載のシステムであって、システムは、

i) 複数の有効性確認リソース間への複数のブロックチェーントランザクションの複数のサブセットの分配の負荷分散を円滑にするように構成された負荷分散コンポーネント、および/または

ii) 複数のブロックチェーントランザクションの少なくとも1つのサブセットの識別を円滑にするように構成されたセグメント識別コンポーネント、および/または

iii) 割り当てユニット、および/または

iv) システムと1つもしくは複数のデータソースまたはデスティネーションとの間で通信内容を送信するかまたは受信するための1つもしくは複数のインターフェースをさらに備える、システム。

## 【0193】

条項4.3。条項4.1または4.2に記載のシステムであって、

システムは、少なくとも1つのコントローラコンポーネントを備え、コントローラコンポーネントは、

少なくとも1つの有効性確認リソース、

少なくとも1つの有効性確認リソースの少なくとも1つのプロセッサ、

1つまたは複数のインターフェース、

1つまたは複数の負荷分散コンポーネント、および/または

複数のブロックチェーントランザクションの少なくとも1つのサブセットの識別を円滑にするように構成された1つもしくは複数のセグメント識別コンポーネントのうちの少なくとも1つの動作に影響を及ぼし、および/または制御するように構成される、システム。

## 【0194】

条項4.4。条項4.1から4.3のいずれか一項に記載のシステムであって、

i) 複数のブロックチェーントランザクションの少なくとも2つのトランザクションは、マークルツリー内の兄弟姉妹であり、および/または

ii) 内部ノードは、ブロックチェーントランザクションのサブセットの親または先祖である、システム。

## 【0195】

条項4.5。条項4.1から4.4のいずれか一項に記載のシステムであって、

複数の出力リポジトリであって、複数のリポジトリのうちの各リポジトリはそれぞれの有効性確認リソースに関連付けられ、複数の未消費トランザクション出力(たとえば、UTXO)の記録、検索、および/または処理を円滑にするように構成される、複数のUTXOリポジトリをさらに含み、

好ましくは、複数の未消費トランザクション出力は各々、複数のブロックチェーントランザクション内の少なくとも1つのトランザクション(Tx)に関連付けられる、システム。

【0196】

条項4.6。条項4.5に記載のシステムであって、システムは、

複数の出力リポジトリのうちの少なくとも1つに関係するアクション、変更、およびイベントの履歴を含むデータベースログを作成し、および/または維持するように動作可能である、システム。

【0197】

条項4.7。条項4.1から4.6のいずれか一項に記載のシステムであって、

複数の出力リポジトリのうちの少なくとも1つは、

i) 未消費トランザクション出力、および/または

ii) a) 未消費トランザクション出力および/またはb) 複数のブロックチェーントランザクションにおけるトランザクション(Tx)に関連付けられている識別子に関連付けられている少なくとも1つのレコードを含む、システム。

【0198】

条項4.8。条項4.7に記載のシステムであって、

少なくとも1つのレコードは、

i) ブロックチェーンブロックに関連付けられているブロック識別子(block\_ID)、および/または

ii) 複数のブロックチェーントランザクションにおけるトランザクション(Tx)に関連付けられたトランザクション識別子(TxID)を有するレコード識別子を含む、システム。

【0199】

条項4.9。条項4.7または4.8に記載のシステムであって、レコード識別子は、

i) ブロック識別子(block\_ID)とトランザクション識別子(TxID)の関数、および/または

ii) ブロック識別子(block\_ID)とトランザクション識別子(TxID)の連結を含む、システム。

【0200】

条項4.10。条項4.8または4.9に記載のシステムであって、システムは、

レコード識別子を使用して、複数の出力リポジトリ内の少なくとも1つの出力リポジトリ内の少なくとも1つのレコードを検索するか、識別するか、アクセスするか、または挿入するように動作可能である、システム。

【0201】

条項4.11。条項4.5から4.10のいずれか一項に記載のシステムであって、

複数のトランザクション出力(UTXO)のうちの少なくとも1つの未消費トランザクション出力(UTXO)は、

i) 未消費トランザクション出力(UTXO)が消費のために利用可能であるか利用不可能であることを示し、および/または

ii) 未消費トランザクション出力の消費が許可されていることを示す第1の状態と、未消費トランザクション出力の消費が禁止されていることを示す第2の状態との間で構成可能であるロックフラグと関連付けられる、システム。

【0202】

条項4.12。条項4.11に記載のシステムであって、システムは、

ロックフラグの状態を第1の状態から第2の状態に、または第2の状態から第1の状態に変更するように動作可能である、システム。

【0203】

10

20

30

40

50

条項4.13。条項4.1から4.12に記載のシステムであって、システムは、

i) ブロックチェーンランザクションのそれぞれのサブセットを複数の有効性確認リソースに割り当てることと、

ii) 複数の有効性確認リソースの1つ、いくつか、またはすべてを使用してブロックチェーンランザクションのそれぞれのサブセットをダウンロードし、および/または受信することと

をできるように動作可能である、システム。

【0204】

条項4.14。条項4.1から4.13のいずれか一項に記載のシステムであって、

有効性確認リソースの1つ、いくつか、またはすべてを使用してブロックチェーンランザクションのそれぞれのダウンロード済みサブセットに基づきマークルツリーのそれぞれの候補内部ノードを生成するように動作可能であり、さらに、

それぞれの候補内部ノードが、マークルツリーのそれぞれの内部ノードと一致することを確認すること、および/または

それぞれの候補内部ノードがマークルツリーのノードであることを、マークルツリーのルートに基づきマークル証明を実行することによって、確認すること、および/または

マークルツリーのそれぞれの候補内部ノードを、1つまたは複数の他の処理リソースに送信すること、のうちの少なくとも1つを実行するように動作可能である、システム。

【0205】

条項4.15。条項4.1から4.14に記載のシステムであって、システムは、

i) 少なくとも1つのブロックチェーンランザクションを有効性確認しおよび/または確認すること、および/または

ii) Simplified Payment Verificationプロセスを実行すること、および/または

iii) 所与のブロックチェーンランザクションがブロックチェーンブロック内に収容されるかどうかを確認すること、および/または

iii) ブロックチェーンランザクションの少なくとも1つのハッシュを生成し、そのハッシュを使用してマークル経路を構築し、および/またはそのハッシュがブロックチェーンブロックのヘッダ内のランザクション識別子と一致するかどうかをチェックすることをするように動作可能である、システム。

【0206】

条項4.16。条項4.1から4.15のいずれか一項に記載のシステムであって、

複数の有効性確認リソースのうちの少なくとも1つは、仮想マシン、サーバ、GPUベースコンピューティングリソース、スレッド、および/またはマルチプロセッサシステムのうちの少なくとも1つであるか、または少なくとも1つを含む、システム。

【0207】

条項セット5:

本特許請求される開示の実施形態は、次の列挙された条項で提示され得る。次の条項セットで提供される特徴はいずれも、先行する列挙された条項セットのいずれか1つまたは複数の中の特徴の1つまたは複数と組み合わせられ得る。

【0208】

本開示は、データレコードの分散および/または並列処理のための方法およびシステムを提供するものとしてよい。ブロックチェーンブロック内のブロックチェーンランザクションのマイニングのため、および/またはブロックチェーンブロックに対するプルーフオブワーク(PoW)もしくはプルーフオブステーク(PoS)の生成のための、そのような方法/システムを提供してもよい。有利には、実施形態は、PoWまたはプルーフオブステーク計算を他のブロックチェーンのマイニング/有効性確認タスクから分離することを可能にし得る。ここでは、われわれは、単に、便宜上プルーフオブワークに言及するが、これはプルーフオブステークを除外するものとして解釈されるべきではない。本開示は、改善されたブロックチェーンマイニング技術および/または改善されたPoW生成技術のための認可および/または制御メカニズムを提供するものとして説明され得る。また、改善され

10

20

30

40

50

たセキュリティ技術として説明され得る。

【0209】

好ましくは、PoW要求者(第1の当事者/エンティティ)は、専門家であるPoW提供者(第2の当事者/エンティティ)に、i)トランザクションのセットを表すマークルツリーに対するマークルルート、ii)制御トランザクション(TX<sub>0</sub>)、およびiii)TX<sub>0</sub>がトランザクションのセットに含まれることを確認するマークル証明のうちの1つまたは複数を送信し得る。TX<sub>0</sub>は、PoW提供者がPoW計算の実行がなされるべきかまたは完了しているかを決定するために使用することができる制御データを提供するか、または含み得る。

【0210】

好ましい一実施形態は、以下のように説明され得る。

条項5.1. コンピュータ実装方法であって、

第1のリソースから第2のリソースに、複数のトランザクションを収容するブロックチェーンブロックに対するプルーフオブワーク(PoW)を生成するための要求を送信することであって、要求は制御トランザクション(TX<sub>0</sub>)が複数のトランザクションに含まれることを検証するためのマークル証明を含む、送信すること、および/または第1のリソースから第2のリソースにおいて、複数のトランザクションを収容するブロックチェーンブロックに対するプルーフオブワーク(PoW)を生成するための要求を受信することであって、要求は制御トランザクション(TX<sub>0</sub>)が複数のトランザクションに含まれることを検証するためのマークル証明を含む、受信すること

を含む、コンピュータ実装方法。

第1のリソースはPoW要求者であり、第2のリソースはPoW提供者であってよい。PoWは、ブロックチェーンプロトコルによって指定される任意のPoWであってもよい。マークル証明は、所与のブロックチェーントランザクションがトランザクションの特定のセットに含まれることを証明し、逆にトランザクションのセットに含まれることを反証するのに十分なデータを含み得る。トランザクションのセットは、マークルルートRを有するマークルツリーTによって表現され得る。

【0211】

条項5.2. 条項5.1に記載の方法であって、

制御トランザクション(TX<sub>0</sub>)は、プルーフオブワーク生成の実行を制御し、許可し、および/または禁止するための制御データを含み、好ましくは、制御データは、

i)ブロックチェーン移転のデスティネーションに対する所定のアドレスを指定する少なくとも1つの出力であって、

好ましくは、アドレスは、第2のリソースまたは第2のリソースに関連付けられたもしくは第2のリソースによって認可された当事者に関連付けられる、出力、および/または

ii)少なくとも1つの所定の署名、および/または

iii)少なくとも1つの秘密値またはデータの秘密部分を含む、方法。

【0212】

条項5.3. 条項5.1または5.2に記載の方法であって、

第1のリソースは、PoW要求リソース、ブロックチェーン有効性確認リソース、またはブロックチェーンマイニングリソースであり、および/または

第2のリソースは、プルーフオブワーク提供者であり、および/または

第2のリソースは、少なくとも1つのASIC、またはハッシュマシン、または専用暗号通貨マイニングリソースを含む、方法。

【0213】

条項5.4. 条項5.1から5.3のいずれか一項に記載の方法であって、

i)第2のリソースから第1のリソースにおいて、ブロックチェーンブロックに対するプルーフオブワークを受信すること、および/または

ii)第2のリソースから第1のリソースに、ブロックチェーンブロックに対するプルーフオブワークを送信することをさらに含む、方法。

【0214】

条項5.5。条項5.1から5.4のいずれか一項に記載の方法であって、プルーフオブワークは、

ブロックチェーンプロトコルによって指定されたターゲット、ルール、または基準のうちの1つもしくは複数を満たす出力を提供するように構成された値(ノンス)、および/または

ブロックチェーンブロックに対するブロックヘッダ、および/または

ブロックチェーンプロトコルに従って指定されたパズルまたはチャレンジの解を含む、方法。

【0215】

条項5.6。条項5.1から5.5のいずれか一項に記載の方法であって、プルーフオブワークを生成することは、

i) ブロックチェーンプロトコルによって指定されたターゲット、チャレンジ、ルール、または基準を満たす出力を提供するように構成された値(ノンス)を生成するか、もしくは選択すること、

ii) ブロックチェーンブロックに対するブロックメッセージとノンスとを連結すること、および/または

iii) ブロックチェーンブロックに対するブロックヘッダをダブルハッシュ化することを含む、方法。

【0216】

条項5.7。条項5.1から5.6のいずれか一項に記載の方法であって、

事前定義された制御基準に関して制御トランザクション(TX<sub>0</sub>)の少なくとも一部を処理するか、もしくは比較し、処理もしくは比較の出力に基づきプルーフオブワークを生成するか、もしくは生成しないことを含み、

好ましくは、制御基準は、開始、実行もしくは完了、またはプルーフオブワーク生成を可能にするための閾値、ルール、または基準のうちの少なくとも1つを含む、方法。

【0217】

条項5.8。条項5.7に記載の方法であって、

プルーフオブワークの生成を許可するかもしれない禁止することを、

i) 制御トランザクション(TX<sub>0</sub>)が複数のトランザクションに含まれることの確認の成功もしくは失敗、および/または

ii) 制御トランザクションが、所定のルールもしくは基準を満たすデータの一部を含むか、もしくは含まないという決定、および/または

iii) 制御トランザクションもしくはその少なくとも一部が制御基準を満たすという決定に基づき行うことをさらに含む、方法。

【0218】

条項5.9。条項5.1から5.8のいずれか一項に記載の方法であって、

第1もしくは第2のリソースにおいて、ブロックに対するプルーフオブワークの生成のためにブロックチェーンプロトコルによって必要とされるデータの一部を決定するステップを含み、データのその一部は

プロトコルバージョン識別子、

ブロックハッシュ、

プロトコルによって指定されたプルーフオブワーク難易度ターゲット、および/またはタイムスタンプのうちの1つもしくは複数をさらに含む、方法。

【0219】

条項5.10。条項5.1から5.9のいずれか一項に記載の方法であって、

i) マークル証明は、制御トランザクションが複数のトランザクションに含まれるかどうかを決定するためのSPV検証の実行を可能にするように構成されたデータを含み、

ii) 要求は、制御トランザクションを含む、方法。

【0220】

条項5.11。条項5.1から5.10のいずれか一項に記載の方法であって、

10

20

30

40

50

複数のトランザクションを処理してマークルツリーを形成するステップをさらに含み、好ましくは、処理は、ハッシュ関数を伴う、方法。

【0221】

条項5.12。条項5.1から5.11のいずれか一項に記載の方法であって、

制御トランザクション(TX<sub>0</sub>)は、第2のリソースが第1のリソースを識別することを可能にする識別子を含み、好ましくは、識別子は、制御トランザクションの入力、出力、スクリプト、またはメタデータ部分で提供される、方法。

【0222】

条項5.13。複数のトランザクションを収容するブロックチェーンブロックに対するプルーフオブワークの生成を制御するかまたはそれに影響を及ぼすように動作可能であり、および/または条項5.1から5.12のいずれか一項に記載の方法を実装するように動作可能である、システム。

【0223】

条項5.14。条項5.13に記載のシステムであって、

少なくとも1つのプルーフオブワーク提供リソース(1000)であって、

好ましくは、少なくとも1つのプルーフオブワーク提供リソースは、少なくとも1つのASICまたはハッシュマシン(1100aから1100c)を含む、少なくとも1つのプルーフオブワーク要求リソース(1000)、

少なくとも1つのプルーフオブワーク要求リソース(1300)であって、

好ましくは少なくとも1つのプルーフオブワーク要求リソースは、本明細書において実質的に開示されている分散有効性確認ノード(700)を含む、少なくとも1つのプルーフオブワーク要求リソース(1300)、のうちの少なくとも一方を備える、システム。

【0224】

条項5.15。コンピュータシステムのプロセッサによって実行された結果として、条項5.1から5.13のいずれか一項に記載のコンピュータ実装方法をコンピュータシステムに実行させるか、またはコンピュータシステムが実行することを可能にする実行可能命令をその上に記憶した、非一時的コンピュータ可読記憶媒体。

【0225】

本開示の例示的な実施形態を実装するための例示的な技術的環境

われわれは、次に、本開示の1つまたは複数の実施形態が実践され得るコンピューティング環境の概要を説明する。しかしながら、上述したように、この文脈は、限定を意図するものではなく、実施形態は、ブロックチェーンを介して実装されないデータレコードおよび構造の処理のために実施され得る。非ブロックチェーン実施形態は、たとえば、分散台帳の代わりにデータベースを使用して考案されてもよい。

【0226】

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を示している。システム100は、パケット交換ネットワーク101、典型的に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備え得る。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内にピアツーピア(P2P)ネットワーク106を形成するように構成され得る複数のブロックチェーンノード104を含む。例示されていないが、ブロックチェーンノード104は、ほぼ完全なグラフとして構成され得る。したがって、各ブロックチェーンノード104は、他のブロックチェーンノード104と高度に接続されている。

【0227】

各ブロックチェーンノード104は、ピアのコンピュータ機器を含み、ノード104のうちの異なるノードは異なるピアに属す。各ブロックチェーンノード104は、1つまたは複数のプロセッサ、たとえば1つまたは複数の中央演算処理装置(CPU)、アクセラレータプロセッサ、特定用途プロセッサおよび/またはフィールドプログラマブルゲートアレイ(FPGA)、ならびに特定用途集積回路(ASIC)などの他の機器を含む処理装置を含む。各ノードは、また、メモリ、すなわち、非一時的コンピュータ可読媒体の形態のコンピュータ可読記憶装置を含む。メモリは、1つまたは複数のメモリ媒体、たとえば、ハードディスク

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、もしくはEEPROMなどの電子媒体、および/または光ディスクドライブなどの光学媒体を採用する1つまたは複数のメモリユニットを含み得る。

#### 【0228】

ブロックチェーン150は、データのブロック151のチェーンを含み、ブロックチェーン150のそれぞれのコピーは、分散型またはブロックチェーンネットワーク106内の複数のブロックチェーンノード104の各々において維持される。上述のように、ブロックチェーン150のコピーを維持することは、必ずしもブロックチェーン150を完全に記憶することを意味しない。その代わりに、各ブロックチェーンノード150が各ブロック151のブロックヘッダ(後述)を記憶する限りブロックチェーン150はデータを剪定され得る。チェーン内の各ブロック151は、1つまたは複数のトランザクション152を含み、この文脈で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また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、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。トランザクションプロトコルの1つの共通のタイプにおいて、各トランザクション152のデータ構造は、少なくとも1つの入力と少なくとも1つの出力とを含む。各出力は、財産としてのデジタル資産の数量を表す額を指定し、その一例は、出力が暗号的にロックされている(ロックを解除し、それによって償還または消費されるためにそのユーザの署名または他の解を必要とする)ユーザ103である。各入力は、先行するトランザクション152の出力を指し示し、それによってトランザクションをリンクする。

10

20

#### 【0229】

各ブロック151は、また、ブロック151に順序を定義するように、チェーン内の以前に作成されたブロック151を指すブロックポインタ155を含んでいる。各トランザクション152(コインベーストランザクション以外の)は、トランザクションのシーケンスに順序を定義するように、前のトランザクションを指すポインタを含む(注:トランザクションのシーケンス152は分岐することが許されている)。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にまで遡る。チェーン150内の初期の1つまたは複数の元のトランザクション152は、先行するトランザクションではなくむしろジェネシスブロック153を指していた。

30

#### 【0230】

ブロックチェーンノード104の各々は、トランザクション152を他のブロックチェーンノード104に転送し、それによってトランザクション152をネットワーク106全体に伝搬するように構成される。各ブロックチェーンノード104は、ブロック151を作成し、同じブロックチェーン150のそれぞれのコピーをそれぞれのメモリに記憶するように構成される。各ブロックチェーンノード104は、また、ブロック151内に組み込まれるのを待っているトランザクション152の順序付けられたセット(または「プール」)154を維持する。順序付けられたプール154は、「mempool」と称されることが多い。本明細書のこの用語は、任意の特定のブロックチェーン、プロトコル、またはモデルに限定することを意図されていない。それは、ノード104が有効であるとして受け入れたトランザクションの順序付けられたセットを指し、それに対してノード104は、同じ出力を消費することを試みる任意の他のトランザクションを受け入れないようにする義務がある。

40

#### 【0231】

所与の現在のトランザクション152jにおいて、その(または各)入力は、トランザクションのシーケンス内の先行するトランザクション152iの出力を参照するポインタを含み、この出力が現在のトランザクション152jにおいて償還されるかまたは「消費」されるべきであることを指定する。一般に、先行するトランザクションは、順序付きセット154または任意のブロック151内の任意のトランザクションである可能性がある。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152jが作成されるか、またはさらにはネットワーク106に送信された時点では必ずしも存在している必要はないが、現在

50

のトランザクションが有効であるためには先行するトランザクション152iが存在し、有効性確認される必要がある。したがって、本明細書における「先行する」は、必ずしも時間的シーケンスにおける作成または送信の時点ではない、ポインタによってリンクされた論理的シーケンス内の先行要素を指し、したがって、トランザクション152i、152jが順序から外れて作成されるか、または送信されることを必ずしも除外しない(オーファントランザクションに関する以下の説明を参照)。先行するトランザクション152iは、等しく前のトランザクションまたは先行トランザクションと呼ばれることも可能である。

#### 【0232】

本トランザクション152jの入力は、また、入力認可、たとえば先行するトランザクション152iの出力がロックされているユーザ103aの署名も含む。次に、本トランザクション152jの出力は、新規ユーザまたはエンティティ103bに暗号的にロックされ得る。本トランザクション152jは、したがって、本トランザクション152jの出力で定義されるように先行するトランザクション152iの入力で定義された額を新規ユーザまたはエンティティ103bに転送することができる。いくつかの場合において、トランザクション152は、複数のユーザまたはエンティティ(そのうちの1つは、釣り銭を渡すために元のユーザまたはエンティティ103aである可能性もある)の間で入力額を分割するために複数の出力を有し得る。いくつかの場合において、トランザクションは、1つまたは複数の先行するトランザクションの複数の出力から金額を集め、現在のトランザクションの1つまたは複数の出力に再分配するための複数の入力を有することもできる。

#### 【0233】

ビットコインなどの出力ベースのトランザクションプロトコルによれば、個人ユーザまたは組織などの当事者103が、(手動または当事者によって採用される自動化プロセスによって)新規のトランザクション152jを制定することを望むときに、実施当事者は、そのコンピュータ端末102から受信者に新しいトランザクションを送信する。実施当事者または受信者は、最終的にこのトランザクションをネットワーク106のブロックチェーンノード104の1つまたは複数に送信する(現在では典型的にはサーバまたはデータセンターであるが、原理上、他のユーザ端末とすることも可能である)。また、新しいトランザクション152jを制定する当事者103が、このトランザクションをブロックチェーンノード104の1つまたは複数に直接的に送信し、いくつかの例では、受信者に送信しないことも除外されない。トランザクションを受信したブロックチェーンノード104は、ブロックチェーンノード104の各々で適用されるブロックチェーン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。ブロックチェーンノードプロトコルは、典型的には、ブロックチェーンノード104が、新規トランザクション152jにおける暗号署名が、トランザクション152の順序付けられたシーケンス内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必要とする。そのような出力ベースのトランザクションプロトコルにおいて、これは、新規トランザクション152jの入力に含まれる当事者103の暗号署名または他の認可が、新規トランザクションが割り当てる先行するトランザクション152iの出力において定義された条件に一致することをチェックすることを含むものとしてよく、この条件は、典型的には、新規トランザクション152jの入力における暗号署名または他の認可が、新規トランザクションの入力がリンクされている前のトランザクション152iの出力をロック解除するかを少なくともチェックすることを含む。この条件は、前のトランザクション152iの出力に含まれるスクリプトによって少なくとも部分的に定義され得る。代替的に、単純にブロックチェーンノードプロトコルだけで修正されるか、またはこれらの組合せに起因することもあり得る。いずれにせよ、新規トランザクション152jが有効である場合、ブロックチェーンノード104は、それをブロックチェーンネットワーク106内の1つまたは複数の他のブロックチェーンノード104に転送する。これらの他のブロックチェーンノード104は、同じブロックチェーンノードプロトコルに従って同じテストを適用するので、新規トランザクション152jを1つまたは複数のさらなるノード104に転送する、というように続く。このようにして、新規トランザクションは、ブロックチェーンノード104のネ

10

20

30

40

50

ットワーク全体に伝搬される。

【0234】

出力ベースモデルでは、所与の出力(たとえばUTXO)が割り当てられた(たとえば消費された)かどうかの定義は、ブロックチェーンノードプロトコルに従って、別の、前方のトランザクション152jの入力によってまだ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、償還を試みる先行するトランザクション152iの出力が、別のトランザクションによってまだ償還されていないことである。ここでもまた有効でない場合、トランザクション152jは伝搬されないか(警告のために無効であるとフラグが立てられ伝搬されない限り)、またはブロックチェーン150に記録されない。これは、トランザクション実行者が同じトランザクションの出力を複数回割り当てようとする二重支払いから保護するものである。その一方で、アカウントベースモデルは、勘定残高を維持することによって二重支払いを防止する。ここでもまたトランザクションの定められた順序があるので、勘定残高はどの時点においても単一の定義済み状態を有する。

【0235】

トランザクションを有効性確認することに加えて、ブロックチェーンノード104は、「ブルーフオブワーク」によってサポートされる、マイニングと一般的に称さ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ものとなる競争を行う。ブロックチェーンノード104では、新規トランザクションが、ブロックチェーン150上に記録されたブロック151内にまだ出現していない有効なトランザクションの順序付けられたプール154に追加される。次いで、ブロックチェーンノードは、暗号パズルを解くことを試みることによってトランザクション152の新しい有効なブロック151を、トランザクション154の順序付けられたセットから組み立てる競争をする。典型的には、これは、「ノンス」値を探索することであって、ノンスが保留トランザクション154の順序付けられたプールの表現と連結されハッシュ化されたときにハッシュの出力が所定の条件を満たすような、探索をすることを含む。たとえば、所定の条件は、ハッシュの出力が特定の事前定義済みの数の先行ゼロを有することであり得る。これは1つの特定のタイプのブルーフオブワークパズルに過ぎず、他のタイプは除外されない。ハッシュ関数の特性は、入力に対して予測不可能な出力を有するという性質である。したがって、この探索は総当りによってのみ実行することができ、したがって、パズルを解こうとしている各ブロックチェーンノード104において処理リソースのかなりの量が消費される。

【0236】

パズルを解いた最初のブロックチェーンノード104は、これをネットワーク106に発表し、ネットワーク内の他のブロックチェーンノード104が容易にチェックできる証明として解を提供する(ハッシュの解が与えられれば、それがハッシュの出力を条件に合致させることをチェックするのは容易である)。最初のブロックチェーンノード104は、ブロックを受け入れる他のノードの閾値コンセンサスにブロックを伝搬し、したがって、プロトコルルールを強制する。次いで、トランザクション154の順序付けられたセットは、ブロックチェーンノード104の各々によってブロックチェーン150内に新しいブロック151として記録されるようになる。ブロックポイント155も、チェーン内の以前に作成されたブロック151n-1を指す新しいブロック151nに割り当てられる。ブルーフオブワークの解を作成するために必要な、たとえばハッシュの形態の、著しい量の労力は、ブロックチェーンプロトコルのルールに従う第1のノード104の意向をシグナリングする。そのようなルールは、以前に有効性確認されたトランザクションと同じ出力を割り当てる場合にトランザクションを有効なものとして受け入れないことを含むが、これは他の場合には二重支払いとしても知られている。作成された後、ブロック151は、ブロックチェーンネットワーク106内のブロックチェーンノード104の各々で認識され維持されるので、修正できない。ブロックポイント155は、また、ブロック151に順序を課す。トランザクション152は、ネットワーク106内の各ブロックチェーンノード104において順序付けられたブロックに記録されるので、これはしたがって、トランザクションの不変の

10

20

30

40

50

公開台帳を提供する。

【0237】

任意の所与の時点でパズルを解く競争をしている異なるブロックチェーンノード104は、解を探し始めた時期またはトランザクションが受信された順序に応じて、任意の所与の時点でまだ公開されていないトランザクション154のプールの異なるスナップショットに基づきそうするものとしてよいことに留意されたい。それぞれのパズルを最初に解いた者は、どのトランザクション152が次の新しいブロック151nに含まれ、どの順序で含まれるかを定義し、未公開トランザクションの現在のプール154は更新される。次いで、ブロックチェーンノード104は、未公開トランザクション154の新規に定義された順序付きプールからブロックを作成する競争をする、というように続ける。また、2つのブロックチェーンノード104がブロックチェーンの対立する見解がノード104間で伝搬されるような互いの非常に短い時間内にパズルを解く場合である、発生し得る任意の「フォーク」を解決するためのプロトコルも存在する。要するに、フォークのどの分岐が最も長く成長しても、決定的なブロックチェーン150になる。これは同じトランザクションが両方のフォークに出現するときにネットワークのユーザまたはエージェントに影響を及ぼしてはならないことに留意されたい。

10

【0238】

ビットコインブロックチェーン(およびほとんどの他のブロックチェーン)によれば、新しいブロック104を首尾よく構成したノードは、デジタル資産の追加の定められた量を分配する新しい特殊な種類のトランザクションにおいてデジタル資産の追加の受け入れられた額を新しく割り当てる能力を付与される(あるエージェントまたはユーザから他方へデジタル資産を送金するエージェント間またはユーザ間トランザクションとは対照的に)。この特別なタイプのトランザクションは通常「コインベーストランザクション」と称されるが、「開始トランザクション」または「生成トランザクション」と呼ばれることもある。これは、典型的には、新しいブロック151nの最初のトランザクションを形成する。プルーフオブワークは、新しいブロックを構築するノードが、この特別なトランザクションが後で償還されることを可能にするプロトコルルールに従うという意向をシグナリングする。ブロックチェーンプロトコルルールでは、この特別なトランザクションが償還され得る前に償還期限、たとえば100ブロック分を必要とし得る。多くの場合に、正規の(非生成)トランザクション152は、また、そのトランザクションが公開されたブロック151nを作成したブロックチェーンノード104にさらに報酬を払うために出力の1つで追加のトランザクション手数料を指定する。この手数料は、通常、「トランザクション手数料」と称され、以下で説明する。

20

30

【0239】

トランザクションの有効性確認および公開に関与するリソースに起因して、典型的には、ブロックチェーンノード104の少なくとも各々は、1つまたは複数の物理的サーバユニットを含むサーバ、またはさらにはデータセンター全体の形態をとる。しかしながら、原理上、任意の所与のブロックチェーンノード104は、ユーザ端末またはネットワーク接続されたユーザ端末のグループの形態をとることも可能である。

【0240】

40

各ブロックチェーンノード104のメモリは、ブロックチェーンノードプロトコルに従ってそれぞれの1つまたは複数の役割を遂行し、トランザクション152を処理するためにブロックチェーンノード104の処理装置上で実行するように構成されているソフトウェアを記憶する。本明細書においてブロックチェーンノード104に帰される任意の活動は、それぞれのコンピュータ機器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は理解されるであろう。ノードソフトウェアは、アプリケーション層、またはオペレーティングシステム層もしくはプロトコル層などの下位層、またはこれらの任意の組合せにおける1つまたは複数のアプリケーションで実装され得る。

【0241】

また、ネットワーク101に接続されているのは、消費ユーザの役割を担う複数の当事

50

者103の各々のコンピュータ機器102である。これらのユーザは、ブロックチェーンネットワーク106とインタラクティブにやり取りし得るが、トランザクションを有効性確認することまたはブロックを構築することに参加することはない。これらのユーザまたはエージェント103のいくつかは、トランザクションにおける送信者および受信者として働き得る。他のユーザは、必ずしも送信者または受信者として活動することなくブロックチェーン150とインタラクティブにやり取りし得る。たとえば、いくつかの当事者は、ブロックチェーン150のコピーを記憶する(たとえば、ブロックチェーンノード104からブロックチェーンのコピーを取得している)ストレージエンティティとして働き得る。

#### 【0242】

当事者103の何人かまたは全員は、異なるネットワーク、たとえばブロックチェーンネットワーク106の上に重ねられたネットワークの一部として接続され得る。ブロックチェーンネットワークのユーザ(多くの場合に「クライアント」と称される)は、ブロックチェーンネットワーク106を含むシステムの一部であると言われ得るが、これらのユーザは、ブロックチェーンノードの必要な役割を実行しないのでブロックチェーンノード104ではない。その代わりに、各当事者103は、ブロックチェーンノード106に接続する(すなわち、通信する)ことによってブロックチェーンネットワーク106とインタラクティブにやり取りし、それによってブロックチェーン150を利用し得る。2つの当事者103およびそれぞれの機器102、すなわち第1の当事者103aおよびそのそれぞれのコンピュータ機器102a、ならびに第2の当事者103bおよびそのそれぞれのコンピュータ機器102bが例示を目的として示されている。さらに多くのそのような当事者103およびそのそれぞれのコンピュータ機器102が存在し、システム100に参加し得るが、便宜上、それらは例示されていないことは理解されるであろう。各当事者103は、個人であっても組織であってもよい。純粋に例示を用いて、第1の当事者103aは本明細書ではアリスと称され、第2の当事者103bはボブと称されるが、これは限定するものではなく、本明細書におけるアリスまたはボブへの参照は、それぞれ「第1の当事者」および「第2の当事者」と置き換えてもよいことは理解されるであろう。

#### 【0243】

各当事者103のコンピュータ機器102は、1つまたは複数のプロセッサ、たとえば1つまたは複数の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、および/またはFPGAを含むそれぞれの処理装置を備える。各当事者103のコンピュータ機器102は、メモリ、すなわち、非一時的コンピュータ可読媒体の形態のコンピュータ可読記憶装置をさらに含む。このメモリは、1つまたは複数のメモリ媒体、たとえば、ハードディスクなどの磁気媒体、SSD、フラッシュメモリ、もしくはEEPROMなどの電子媒体、および/または光ディスクドライブなどの光学媒体を採用する1つまたは複数のメモリユニットを含み得る。各当事者103のコンピュータ機器102上のメモリは、処理装置上で実行するように構成されている少なくとも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。本明細書において所与の当事者103に帰される任意の活動は、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して実行され得ることは理解されるであろう。各当事者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、たとえば、デスクトップも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、またはスマートウォッチなどのウェアラブルデバイスを含む。所与の当事者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つまたは複数の他のネットワーク接続リソースも備え得る。

#### 【0244】

クライアントアプリケーション105は、たとえばサーバからダウンロードされた、好適なコンピュータ可読記憶媒体上で任意の所与の当事者103のコンピュータ機器102に最初に提供され得るか、または取り外し可能SSD、フラッシュメモリキー、取り外し可能EEPROM、取り外し可能磁気ディスクドライブ、磁気フロッピーディスクもしくはテープなどの取り外し可能記憶デバイス、CDまたはDVD ROMなどの光ディスク、または取

り外し可能光学式ドライブなど、で提供され得る。

【0245】

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。これは、主に2つの機能性を有する。これらのうちの1つは、それぞれの当事者103が、トランザクション152を作成し、認可し(たとえば署名し)、1つまたは複数のビットコインノード104に送信して、次いでブロックチェーンノード104のネットワーク全体に伝搬させ、それによってブロックチェーン150に含まれることを可能にすることである。他は、それぞれの当事者に、現在所有しているデジタル資産の額を報告することである。出力ベースシステムでは、この第2の機能は、ブロックチェーン150全体に散らばる様々なトランザクション152の出力において定められた、注目する当事者に属する金額を照合することを含む。

10

【0246】

注:様々なクライアント機能が所与のクライアントアプリケーション105に統合されていると説明され得るが、これは必ずしも限定するものではなく、その代わりに本明細書において説明されている任意のクライアント機能が、代わりに、2つまたはそれ以上の異なるアプリケーションの組、たとえば、APIを介してインターフェースされるか、または一方が他方へのプラグインされるもので実装され得る。より一般的には、クライアント機能は、アプリケーション層、またはオペレーティングシステムなどの下位層、またはこれらの任意の組合せで実装されることも可能である。次に、クライアントアプリケーション105に関して説明されるが、これは限定的なものではないことは理解されるであろう。

20

【0247】

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またはソフトウェア105のインスタンスは、ネットワーク106のブロックチェーンノード104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ネットワーク106にトランザクション152を送信することを可能にする。クライアント105は、また、それぞれの当事者103が受信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を問い合わせる(または実施形態ではブロックチェーン150は、一部はその公共の可視性を通してトランザクションに信頼を提供する公共の施設であるので、実際にブロックチェーン150内の他の当事者のトランザクションを検査する)ためにブロックチェーンノード104と連絡を取ることができる。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を定式化し送信するように構成される。上で述べたように、各ブロックチェーンノード104は、ブロックチェーンノードプロトコルに従ってトランザクション152を有効性確認し、ブロックチェーンネットワーク106全体に伝搬させるためにトランザクション152を転送するように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および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一緒に、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は、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。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。

30

【0248】

所与の当事者103、たとえばアリスは、ブロックチェーン150に含まれるべき新しいトランザクション152jを送信することを望むときに、アリスは、関連するトランザクションプロトコルに従って(アリス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)新しいトランザクションを定式化する。次いで、アリスは、クライアントアプリケーション105から、自分が接続されている1つまたは複数のブロックチェーンノード104にトランザクション152を送信する。たとえば、これはアリスのコンピュータ102に最もよく接続されているブロックチェーンノード104である可能性もある。任意の所与のブロックチェーンノード104が新規トランザクション152jを受信したときに、これは、ブロックチェーンノードプロトコルおよびそのそれぞれの役割に従ってそれを処理する。これは、新しく受信されたトランザクション152jが「有効」であるためのある条件

40

50

を満たすかどうかを最初にチェックすることを含むが、その例は、まもなくより詳細に説明される。いくつかのトランザクションプロトコルでは、有効性確認のための条件は、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毎に構成可能であり得る。代替的に、この条件は、単純にノードプロトコルの組み込み機能であるか、またはスクリプトとノードプロトコルとの組合せによって定義されることも可能である。

【0249】

新たに受信されたトランザクション152jが有効とみなされることについてのテストに合格するという条件で(すなわち、それが「有効性確認される」という条件で)、トランザクション152jを受信する任意のブロックチェーンノード104は、そのブロックチェーンノード104で維持されているトランザクション154の順序付けられたセットに新しい有効性確認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を受信した任意のブロックチェーンノード104は、有効性確認されたトランザクション152をネットワーク106内の1つまたは複数の他のブロックチェーンノード104に前方伝搬される。各ブロックチェーンノード104は同じプロトコルを適用するので、次いで、トランザクション152jが有効であると仮定すると、これは、それがすぐにネットワーク106全体にわたって伝搬されることを意味する。

【0250】

所与のブロックチェーンノード104で維持されている保留トランザクション154の順序付けられたプールに入るのを許された後、そのブロックチェーンノード104は、新しいトランザクション152を含むそれぞれのプール154の最新バージョンでプルーフオブワークパズルを解く競争を開始する(他のブロックチェーンノード104はトランザクション154の異なるプールに基づきパズルを解こうとしている可能性があるが、最初にそこに辿り着いた者が最新のブロック151に含まれるトランザクションのセットを定義するということを想起されたい。最終的にブロックチェーンノード104は、アリスのトランザクション152jを含む順序付けられたプール154の一部に対するパズルを解くことになる)。新規トランザクション152jを含むプール154に対してプルーフオブワークが行われた後、それは、不変的に、ブロックチェーン150内のブロック151のうちの1つのブロックの一部となる。各トランザクション152は、以前のトランザクションを指すポインタを含み、したがってトランザクションの順序もまた、不変的に記録される。

【0251】

異なるブロックチェーンノード104は、所与のトランザクションの異なるインスタンスを最初に受信し、したがって、インスタンスが新しいブロック151において公開される、すべてのブロックチェーンノード104が公開されたインスタンスが唯一の有効インスタンスであると合意する時点より前に、どのインスタンスが「有効」であるかについて対立する見解を有することがある。ブロックチェーンノード104が1つのインスタンスを有効なものとして受け入れ、次いで第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、そのブロックチェーンノード104はこれを受け入れなければならない、最初に受け入れたインスタンス(すなわち、ブロック151で公開されていないもの)を破棄する(すなわち、無効として扱う)ことになる。

【0252】

いくつかのブロックチェーンネットワークによって運用されるトランザクションプロトコルの代替的タイプは、アカウントベーストランザクションモデルの一部として、「アカウントベース」プロトコルと称され得る。アカウントベースのケースでは、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内において先行するトランザクションのUTXOを参照することによって振替金額を定義するのではなく、むしろ絶対的な口座残高を参照することによって振替金額を定義する。すべての口座の現在の状態は、ブロックチェーンとは別の、そのネットワークのノードによって記憶され、常に更新される。そのようなシステムでは、トランザクションは、口座の実行中トランザクション集計(「ポジション」とも呼ばれる)を使用して順序付けられる。この値は、暗号署名の一部として送信者によって署名され、トランザクション参照計算の一部としてハッシュ化される。それに

10

20

30

40

50

加えて、任意選択のデータフィールドもトランザクションにおいて署名され得る。このデータフィールドは、たとえば以前のトランザクションIDがデータフィールドに含まれる場合に、以前のトランザクションを指してもよい。

【0253】

UTXOベースのモデル

図2は、トランザクションプロトコルの例を例示している。これは、UTXOベースプロトコルの一例である。トランザクション152(「Tx」と略記)は、ブロックチェーン150の基本的なデータ構造である(各ブロック151は1つまたは複数のトランザクション152を含む)。以下は、出力ベースまたは「UTXO」ベースプロトコルを参照して説明される。しかしながら、これは、すべての可能な実施形態に限定されない。例示的なUTXOベースプロトコルは、ビットコインを参照しつつ説明されるが、他の例示的なブロックチェーンネットワーク上で等しく実装され得ることに留意されたい。

10

【0254】

UTXOベースモデルでは、各トランザクション(「Tx」)152は、1つまたは複数の入力202、および1つまたは複数の出力203を含むデータ構造を備える。各出力203は、(UTXOがまだ償還されていない場合に)別の新しいトランザクションの入力202のソースとして使用され得る、未消費トランザクション出力(UTXO)を含み得る。UTXOは、デジタル資産の額を指定する値を含む。これは、分散台帳上のトークンの設定された数を表す。UTXOは、また、他の情報の中で、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も含み得る。トランザクションデータ構造は、また、入力フィールド202および出力フィールド203のサイズのインジケータを含み得る、ヘッダ201を備え得る。ヘッダ201は、また、トランザクションのIDを含むものとしてよい。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それ自体を除く)であり、ノード104に提出された生のトランザクション152のヘッダ201に記憶される。

20

【0255】

たとえば、アリス103aが、注目しているデジタル資産の額をボブ103bに転送するトランザクション152jを作成することを望んでいる。図2において、アリスの新規トランザクション152jは「Tx<sub>1</sub>」とラベル付けされている。これは、シーケンス内の先行するトランザクション152iの出力203においてアリスにロックされているデジタル資産の額を取り、これの少なくとも一部をボブに転送する。先行するトランザクション152iは、図2において「Tx<sub>0</sub>」とラベル付けされている。Tx<sub>0</sub>およびTx<sub>1</sub>は、任意のラベルにすぎない。これらは、必ずしも、Tx<sub>0</sub>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も、Tx<sub>1</sub>がプール154内のすぐ次のトランザクションであることも意味しない。Tx<sub>1</sub>は、アリスにロックされた未消費の出力203を依然として有する任意の先行する(すなわち前の)トランザクションを指すことも可能である。

30

【0256】

先行するトランザクションTx<sub>0</sub>は、アリスが新規トランザクションTx<sub>1</sub>を作成する時点、または少なくともネットワーク106に送信する時点までに、すでに有効性確認され、ブロックチェーン150のブロック151に含まれているものとしてよい。それは、その時点でブロック151のうちの1つにすでに含まれているか、または順序付けられたセット154においてまだ待機しているものとしてよく、その場合、それはすぐに新しいブロック151に含まれることになる。代替的に、Tx<sub>0</sub>およびTx<sub>1</sub>は、一緒に作成されてネットワーク106と一緒に送信される可能性があるか、またはTx<sub>0</sub>は、ノードプロトコルが「オープン」トランザクションのバッファリングを可能にする場合にTx<sub>1</sub>の後に送信され得ることすら可能である。トランザクションのシーケンスの文脈で本明細書において使用されている「先行する」および「後続の」という言い回しは、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しているか、など)によって定義されるようなシーケンス内のトランザクションの順序を指している。これらは、等しく、「先行要素」および「後続要素」、または「前要素」および「

40

50

子孫」、「親」および「子」、またはそのようなものと置き換えられることも可能である。これは、必ずしも、それらが作成され、ネットワーク106に送信され、または任意の所与のブロックチェーンノード104に到着する順序を暗示するものではない。それでもなお、先行するトランザクション(前のトランザクションまたは「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または「子」)は、親トランザクションが有効性確認されるまで、また有効性確認がなされない限り、有効性確認されない。親よりも先にブロックチェーンノード104に到着した子は、オーファンとみなされる。それは、ノードプロトコルおよび/またはノードの挙動に応じて、親を待つために廃棄されるか、または一定時間バッファリングされ得る。

【0257】

先行するトランザクションTx<sub>0</sub>の1つまたは複数の出力203のうちの1つは、ここではUTXO<sub>0</sub>とラベル付けされている、特定のUTXOを含む。各UTXOは、UTXOによって表されるデジタル資産の額を指定する値と、後続のトランザクションが有効性確認され、したがってUTXOが首尾良く償還されるために後続のトランザクションの入力202のロック解除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を含む。典型的には、ロックスクリプトは、金額を特定の当事者(それが含まれるトランザクションの受益者)にロックする。すなわち、ロックスクリプトは、典型的には、後続のトランザクションの入力におけるロック解除スクリプトが、先行するトランザクションがロックされている当事者の暗号署名を含む条件を含む、ロック解除条件を定義する。

【0258】

ロックスクリプト(scriptPubKeyとも呼ばれる)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書かれたコードの断片である。このような言語の特定の例は、ブロックチェーンネットワークで使用される「Script」(大文字のS)と呼ばれる。ロックスクリプトは、たとえばアリスの署名の要件など、トランザクション出力203を消費するために必要な情報を指定する。ロック解除スクリプトは、トランザクションの出力内に出現する。ロック解除スクリプト(scriptSigとも呼ばれる)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言語で書かれたコードの断片である。たとえば、これはボブの署名を含み得る。ロック解除スクリプトは、トランザクションの入力202内に出現する。

【0259】

したがって、例示されている例では、Tx<sub>0</sub>の出力203のUTXO<sub>0</sub>は、UTXO<sub>0</sub>が償還されるために(厳密には、UTXO<sub>0</sub>を償還することを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Sig P<sub>A</sub>を必要とするロックスクリプト[Checksig P<sub>A</sub>]を備えている。[Checksig P<sub>A</sub>]は、アリスの公開鍵-秘密鍵ペアからの公開鍵P<sub>A</sub>の表現(すなわち、ハッシュ)を含む。Tx<sub>1</sub>の入力202は、Tx<sub>1</sub>を指すポインタ(たとえば、実施形態ではトランザクションTx<sub>0</sub>全体のハッシュである、そのトランザクションID、TxID<sub>0</sub>を用いて)を含む。Tx<sub>1</sub>の入力202は、Tx<sub>0</sub>の任意の他の可能な出力のうちからそれを識別するために、Tx<sub>0</sub>内でUTXO<sub>0</sub>を識別するインデックスを含む。Tx<sub>1</sub>の入力202は、アリスが鍵ペアから秘密鍵をデータ(暗号では「メッセージ」と呼ばれることもある)の事前定義済み部分に適用することによって作成された、アリスの暗号署名を含むロック解除スクリプト<Sig P<sub>A</sub>>をさらに含む。有効な署名を提供するためにアリスによって署名される必要があるデータ(または「メッセージ」)は、ロックスクリプトによって、またはノードプロトコルによって、またはこれらの組合せによって定義され得る。

【0260】

新規トランザクションTx<sub>1</sub>がブロックチェーンノード104に到着すると、そのノードは、ノードプロトコルを適用する。これは、ロックスクリプトおよびロック解除スクリプトと一緒に実行して、ロック解除スクリプトがロックスクリプトで定義されている条件(ここで、この条件は1つまたは複数の基準を含み得る)を満たす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つのスクリプトを次のように連結することを含む。

<Sig P<sub>A</sub>> <P<sub>A</sub>> | | [Checksig P<sub>A</sub>]

10

20

30

40

50

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、「[...]」はロックスクリプト(この例ではスタックベースの言語)によって構成される関数である。同等に、スクリプトは、スクリプトを連結するのではなくむしろ、共通のスタックにより、他方の後にスクリプトを次々に実行され得る。いずれにせよ、一緒に実行したときに、スクリプトは、 $T_{x_0}$ の出力内にあるロックスクリプトに含まれるような、アリスの公開鍵 $P_A$ を使用して、 $T_{x_1}$ の入力内にあるロック解除スクリプトが、データの期待される部分に署名するアリスの署名を含むことを認証する。この認証を実行するために、データそれ自体の期待される部分(「メッセージ」)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、 $T_{x_1}$ の全体を含む(したがって、すでに本質的に存在しているので、データの署名された部分を平文で指定する別の要素が含まれる必要はない)。

10

#### 【0261】

公開秘密暗号による認証の詳細は、当業者には馴染み深いものであろう。基本的に、アリスが自分の秘密鍵を使用してメッセージに署名している場合、アリスの公開鍵および平文のメッセージが与えられれば、ノード104などの別のエンティティは、メッセージがアリスによって署名されたに違いないと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化し、ハッシュに署名し、これを署名としてメッセージにタグ付けすることを含み、したがって公開鍵の保有者は誰でも署名を認証することができる。したがって、特定のデータ部分またはトランザクションの一部などに署名するという本明細書の言及は、実施形態において、そのデータ部分またはトランザクションの一部のハッシュに署名することを意味し得ることに留意されたい。

20

#### 【0262】

$T_{x_1}$ のロック解除スクリプトが $T_{x_0}$ のロックスクリプトで指定された1つまたは複数の条件を満たす場合(したがって、図示されている例では、アリスの署名が $T_{x_1}$ で提供され認証された場合)、ブロックチェーンノード104は $T_{x_1}$ を有効とみなす。これは、ブロックチェーンノード104が、 $T_{x_1}$ を保留トランザクション154の順序付きプールに追加することを意味する。ブロックチェーンノード104は、また、トランザクション $T_{x_1}$ をネットワーク106内の1つまたは複数の他のブロックチェーンノード104に転送し、それによりネットワーク106全体にわたって伝搬される。 $T_{x_1}$ が有効性確認され、ブロックチェーン150に入れられた後、これは、 $T_{x_0}$ から $UTXO_0$ を消費済みとして定義する。 $T_{x_1}$ は、それが未消費トランザクション出力203を消費する場合にのみ有効であり得ることに留意されたい。それが別のトランザクション152によってすでに消費されてしまっている出力を消費することを試みた場合、 $T_{x_1}$ は、他のすべての条件が満たされている場合であっても無効となる。したがって、ブロックチェーンノード104は、先行するトランザクション $T_{x_0}$ において参照されている $UTXO$ がすでに消費されているかどうか(すなわち、それがすでに別の有効なトランザクションへの有効な入力を形成しているかどうか)をチェックする必要もある。これは、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ることが重要である理由の1つである。実際に、所与のブロックチェーンノード104は、どのトランザクション152においてどの $UTXO$ 203が消費されたかをマークする別のデータベースを維持するものとしてよいが、 $UTXO$ が消費されたかどうかを定義するのは最終的にはそれがブロックチェーン150内の別の有効なトランザクションへの有効な入力をすでに形成しているかどうかである。

30

40

#### 【0263】

所与のトランザクション152のすべての出力203で指定された総額が、そのすべての入力202によって指されている総額よりも大きい場合、これはほとんどのトランザクションモデルにおいて無効であることに対する別の基準である。したがって、そのようなトランザクションは伝搬されず、ブロック151に含まれることもない。

#### 【0264】

$UTXO$ ベーストランザクションモデルでは、所与の $UTXO$ は全体として消費される必要があることに留意されたい。 $UTXO$ において定義された金額の一部を、別の部分が消費されている間に、消費済みとして「残す」ことはできない。しかしながら、 $UTXO$ からの金

50

額は、次のトランザクションの複数の出力の間に分割され得る。たとえば、 $Tx_0$ において  $UTXO_0$  で定義されている金額は、 $Tx_1$  における複数の  $UTXO$  の間に分割され得る。したがって、アリスがボブに  $UTXO_0$  で定義された金額のすべてを与えたくない場合、アリスは、残りを  $Tx_1$  の第2の出力で自分自身に釣り銭を渡すか、または他の当事者に支払うために使用することができる。

【0265】

実際には、アリスは、通常、自分のトランザクション104をブロック151に正常に入るビットコインノード104に対する手数料を含める必要もある。アリスがそのような手数料を含めない場合、 $Tx_0$  は、ブロックチェーンノード104によって拒絶され、したがって技術的には有効であるが、伝搬されずブロックチェーン150に含まれ得ない(ノードプロトコルは、ブロックチェーンノード104にトランザクション152を受け入れることを、そうするのを望まない場合には強制しない)。いくつかのプロトコルでは、トランザクション手数料は、それ自身の別個の出力203を必要としない(すなわち、別個の  $UTXO$  を必要としない)。その代わりに、入力202によって指される総額と、所与のトランザクション152の出力203において指定される総額との間の任意の差額が、トランザクションを公開するブロックチェーンノード104に自動的に与えられる。たとえば、 $UTXO_0$  へのポイントは  $Tx_1$  への入力のみであり、 $Tx_1$  は1つの出力  $UTXO_1$  のみを有する。 $UTXO_0$  で指定されたデジタル資産の額が  $UTXO_1$  で指定された額よりも大きい場合、その差額は、 $UTXO_1$  を含むブロックを作成するためにプルーフオブワークの競争に勝ったノード104によって割り当てられ得る。しかしながら、代替的に、またはそれに加えて、トランザクション手数料がトランザクション152の  $UTXO_203$  のうちのそれ自身の1つにおいて明示的に指定されることが可能であることは、必ずしも除外されない。

【0266】

アリスおよびボブのデジタル資産は、ブロックチェーン150内のどこかにある任意のトランザクション152において彼らにロックされた  $UTXO$  からなる。したがって、典型的には、所与の当事者103の資産は、ブロックチェーン150全体における様々なトランザクション152の  $UTXO$  全体を通して散らばっている。所与の当事者103の総残高を定義する1つの数がブロックチェーン150内のどこかに記憶されているわけではない。それぞれの当事者にロックされ、別の前方のトランザクションでまだ消費されていないすべての様々な  $UTXO$  の値をまとめて照合するのはクライアントアプリケーション105内のウォレット機能の役割である。ビットコインノード104のいずれかに記憶されているようなブロックチェーン150のコピーに問い合わせることによってこれを行うことができる。

【0267】

スクリプトコードは、多くの場合に概略として表現される(すなわち、正確な言語を使用しない)ことに留意されたい。たとえば、特定の機能を表現するためにオペレーションコード(opcode)を使用してもよい。「OP\_...」は、Script言語の特定のオペコードを指す。一例として、OP\_RETURNは、ロックスクリプトの始めにOP\_FALSEが先行するときに、トランザクション内にデータを記憶することができるトランザクションの消費不可能な出力を作成し、それによってデータをブロックチェーン150内に不変的に記録する、Script言語のオペコードである。たとえば、データは、ブロックチェーンに記憶することが望まれる文書を含み得る。

【0268】

典型的には、トランザクションの入力は、公開鍵  $P_A$  に対応するデジタル署名を含む。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ものである。いくつかの実施形態において、所与のトランザクションについて、署名は、トランザクション入力の一部と、トランザクション出力の一部または全部に署名する。こ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、通常、どの出力が署名される(したがって、署名の時点で固定される)かを選択する署名の最後に含まれる4バイトコードである。

【0269】

10

20

30

40

50

ロックスクリプトは、これが典型的にはそれぞれのトランザクションがロックされる当事者の公開鍵を含むという事実を指して、「scriptPubKey」と呼ばれることがある。ロック解除スクリプトは、典型的には対応する署名を提供するという事実を指す「scriptSig」と呼ばれることがある。しかしながら、より一般的に、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、UTXOが償還されるための条件が署名を認証することを含むことは不可欠でない。より一般的には、スクリプト言語は、任意の1つまたは複数の条件を定義するために使用されることが可能である。したがって、より一般的な用語である「ロックスクリプト」および「ロック解除スクリプト」が好まれ得る。

【0270】

サイドチャネル

図1に示されているように、アリスおよびボブのコンピュータ機器102a、102bの各々の上のクライアントアプリケーションは、それぞれ、追加の通信機能を備え得る。この追加の機能は、アリス103aが、ボブ103bと(いずれかの当事者または第三者の扇動で)別個のサイドチャネル107を確立することを可能にする。サイドチャネル107は、ブロックチェーンネットワークから離れてデータを交換することを可能にする。そのような通信は、ときには「オフチェーン」通信と称される。たとえば、これは、当事者の一方がネットワーク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(まだ)ブロックチェーンネットワーク106に登録されることなく、またはチェーン150上を進むことなく、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。このようにトランザクションを共有することは、ときには、「トランザクションテンプレート」を共有すると称される。トランザクションテンプレートは、完全なトランザクションを形成するために必要な1つまたは複数のインプットおよび/またはアウトプットを欠いている場合がある。代替的に、またはそれに加えて、サイドチャネル107は、鍵、交渉された金額または条件、データコンテンツなどの任意の他のトランザクション関係データを交換するために使用され得る。

【0271】

サイドチャネル107は、ブロックチェーンネットワーク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、またはそれに加えて、サイドチャネル301は、モバイルセルラーネットワークなどの異なるネットワーク、また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、またはアリスのデバイス102aとボブのデバイス102bとの間の直接的な有線またはワイヤレスリンクを介してであっても確立され得る。一般的に、本明細書のどこかで参照されているサイドチャネル107は、「オフチェーン」で、すなわちブロックチェーンネットワーク106とは別に、データを交換するための1つまたは複数のネットワーク技術または通信媒体を介した任意の1つまたは複数のリンクを含み得る。複数のリンクが使用される場合、オフチェーンリンクのバンドルまたはコレクションは全体としてサイドチャネル107と称され得る。したがって、アリスおよびボブが、サイドチャネル107上で、いくつかの情報またはデータまたは類似のものを交換すると言われる場合に、これは必ずしもこれらのデータのすべての部分が全く同じリンクまたは同じタイプのネットワーク上で送信されなければならないことを暗示するものではないことに留意されたい。

【0272】

さらなる備考

開示された技術の他の変更形態またはユースケースは、本明細書において開示を示した後に当業者にとって明らかになるであろう。本開示の範囲は、説明されている実施形態によって限定されず、付属の請求項によってのみ限定される。たとえば、上記のいくつかの実施形態は、ビットコインネットワーク106、ビットコインブロックチェーン150、およびビットコインノード104に関して説明されてきた。しかしながら、ビットコインブロックチェーンはブロックチェーン150の特定の一例であり、上記の説明は、任意のブロックチェーンに一般的に適用され得ることは理解されるであろう。すなわち、本発明は、決してビットコインブロックチェーンに限定されるものではない。より一般的には、ビ

10

20

30

40

50

ットコインネットワーク106、ビットコインブロックチェーン150、およびビットコインノード104への上記の任意の参照は、それぞれ、ブロックチェーンネットワーク106、ブロックチェーン150、およびブロックチェーンノード104への参照で置き換えられ得る。ブロックチェーン、ブロックチェーンネットワーク、および/またはブロックチェーンノードは、上で説明されているビットコインブロックチェーン150、ビットコインネットワーク106、およびビットコインノード104の説明されている特性のいくつかまたはすべてを共有し得る。

【0273】

本開示の好ましい実施形態では、ブロックチェーンネットワーク106はビットコインネットワークであり、ビットコインノード104は、ブロックチェーン150のブロック151を作成し、公開し、伝搬し、および記憶する説明されている機能の少なくとも一部または全部を実行する。これらの機能のうちの1つまたはいくつかだけを実行し、すべてを実行することはない他のネットワークエンティティ(またはネットワーク要素)があり得ることは除外されない。すなわち、ネットワークエンティティは、ブロックを作成し公開することなく、ブロックを伝搬し、および/または記憶する機能を実行し得る(これらのエンティティは、好ましいビットコインネットワーク106のノードとは考えられないことを想起されたい)。

【0274】

本開示の他の実施形態では、ブロックチェーンネットワーク106は、ビットコインネットワークでなくてもよい。これらの実施形態において、ノードがブロックチェーン150のブロック151を作成し、公開し、伝搬し、記憶する機能の少なくとも1つまたはいくつかを実行し得るが、すべてを実行するわけではないことは除外されない。たとえば、これらの他のブロックチェーンネットワークにおいて、「ノード」は、ブロック151を作成し、公開するように構成されているが、それらのブロック151を他のノードに記憶しおよび/または伝播することをしないネットワークエンティティを参照するために使用され得る。

【0275】

さらに一般的には、上記の用語「ビットコインノード」104への任意の参照は、用語「ネットワークエンティティ」または「ネットワーク要素」で置き換えられてもよく、そのようなエンティティ/要素は、ブロックを作成し、公開し、伝搬し、記憶する役割のいくつかまたはすべてを実行するように構成される。そのようなネットワークエンティティ/要素の機能は、ブロックチェーンノード104を参照しつつ上で説明されているのと同じ方法を用いてハードウェアで実装され得る。

【0276】

用語「ユーザ」は、本明細書では、人間またはマシンベースのエンティティを含むように使用され得る。

【0277】

上述の実施形態は、本開示を制限するのではなくむしろ本発明を例示するものであり、当業者であれば、付属の請求項によって定義されているような本開示の範囲から逸脱することなく多くの代替的实施形態を設計することができることに留意されたい。請求項において、括弧内に記載されている参照記号は、請求項を制限するものとして解釈されないものとする。また、「備える」および「含む」および同様の言い回しは、任意の請求項または本明細書全体に記載されている以外の要素またはステップの存在を排除するものではない。本明細書では、「含む」、「備える」は、「～を含むまたは～からなる」を意味し、「含むこと」、「備えること」は、「～を含むこと、または～からなること」を意味する。本明細書全体を通して、「含む」、「備える」、または「含んでいる」など活用形は、述べられている要素、整数、もしくはステップ、または要素、整数もしくはステップのグループの包含を暗示し、任意の他の要素、整数、もしくはステップ、または要素、整数、もしくはステップのグループの除外を暗示しないと理解される。要素の単数形での参照は、そのような要素の複数形での参照を除外するものではなく、またその逆もまた同様であ

10

20

30

40

50

る。本開示は、いくつかの異なる要素を含むハードウェアを用いて、および適切にプログラムされているコンピュータを用いて実装されてもよい。いくつかの手段を列挙しているデバイス請求項において、これらの手段のうちのいくつかは、ハードウェアの1つおよび同じ項目によって具現化されてよい。特定の手段が、相互に異なる従属請求項において引用されているという単なる事実は、これらの手段の組合せが有利に使用され得ないことを示すものではない。

【符号の説明】

【0278】

|            |                       |    |
|------------|-----------------------|----|
| 100        | システム                  |    |
| 101        | パケット交換ネットワーク          | 10 |
| 102        | コンピュータ機器              |    |
| 102a       | コンピュータ機器              |    |
| 102b       | コンピュータ機器              |    |
| 103        | ユーザ、当事者               |    |
| 103a       | ユーザ                   |    |
| 103a       | 第1の当事者                |    |
| 103b       | 新規ユーザまたはエンティティ        |    |
| 103b       | 第2の当事者                |    |
| 104        | ブロックチェーンノード           |    |
| 105        | クライアントアプリケーション        | 20 |
| 106        | 分散型またはブロックチェーンネットワーク  |    |
| 107        | サイドチャネル               |    |
| 120b       | コンピュータ機器              |    |
| 150        | ブロックチェーン              |    |
| 151        | データのブロック              |    |
| 151n       | ブロック                  |    |
| 151n-1     | ブロック                  |    |
| 152        | トランザクション              |    |
| 152i       | トランザクション              |    |
| 152j       | トランザクション              | 30 |
| 153        | ジェネシスブロック (Gb)        |    |
| 154        | 順序付けられたセット (または「プール」) |    |
| 155        | ブロックポインタ              |    |
| 201        | ヘッダ                   |    |
| 202        | 入力                    |    |
| 203        | 出力                    |    |
| 301        | サイドチャネル               |    |
| 502        | 部分                    |    |
| 504        | 共通内部ノード (内部ハッシュ)      |    |
| 602        | 部分                    | 40 |
| 602a~h     | 部分                    |    |
| 604        | 共通内部ノード               |    |
| 700        | システム、有効性確認ノード         |    |
| 702        | システムレベルコントローラ         |    |
| 704        | バリデータ                 |    |
| 704aから704d | リソース                  |    |
| 902        | インターフェース              |    |
| 903        | セグメント識別ユニット           |    |
| 904        | コンポーネント               |    |
| 904        | 割り当てユニット              | 50 |

## 905 負荷分散ユニット

## 1000 分散マイニングノード、PoW提供者

## 1100 ASICまたはハッシュマシン

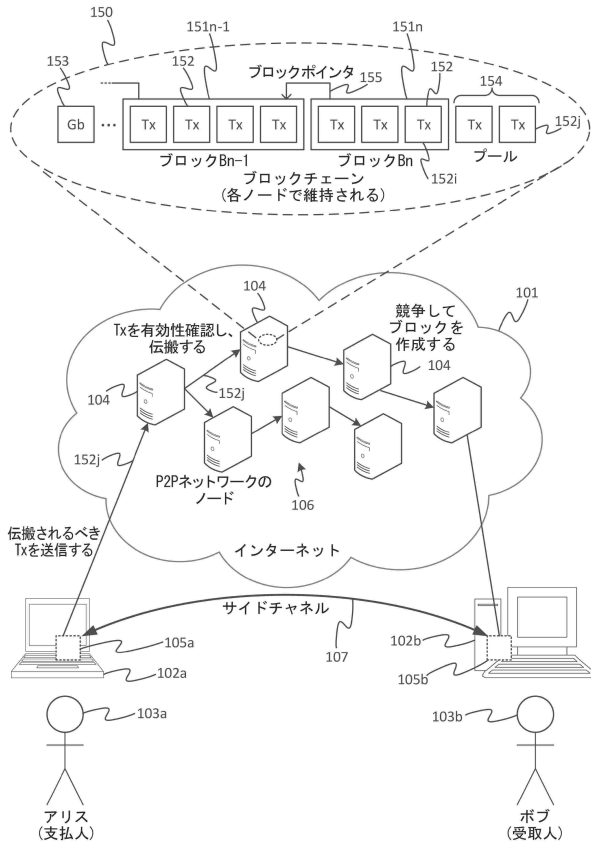
1100a、1100bまたは1100c 計算機

## 1200 コントローラ

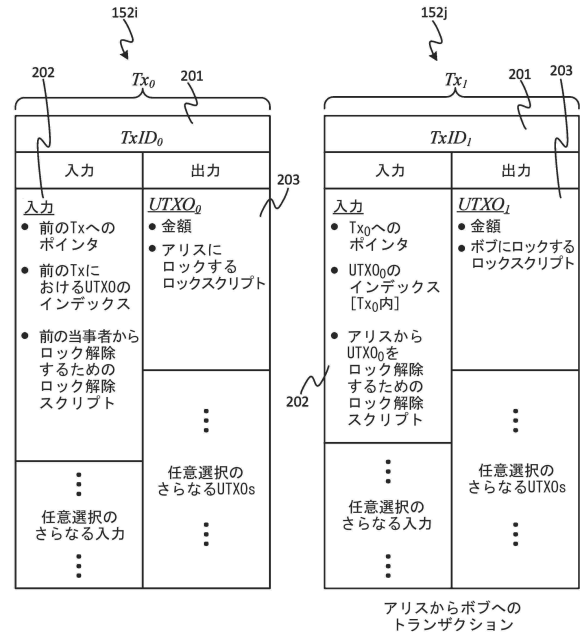
### 1300 PoW 要求リソース、PoW 要求者

【図面】

【図 1】

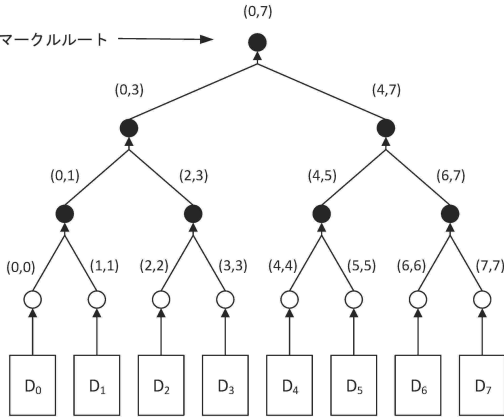


【図 2】

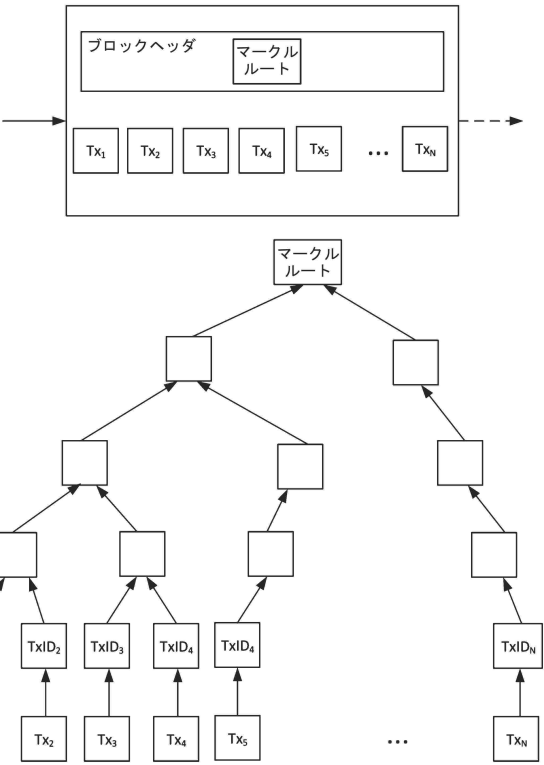


次を実行することによって有効性確認される：  
 $\text{Tx}_1$ の入ット202からのアリスの  
 ロック解除スクリプトとアリスの  
 $\text{Tx}_0$ のアウトット203からのロックスクリプト。  
 これは、 $\text{Tx}_1$ におけるアリスの  
 ロック解除スクリプトが  
 前のトランザクション $\text{Tx}_0$ の  
 ロックスクリプトにおいて  
 定義された条件に合致している。

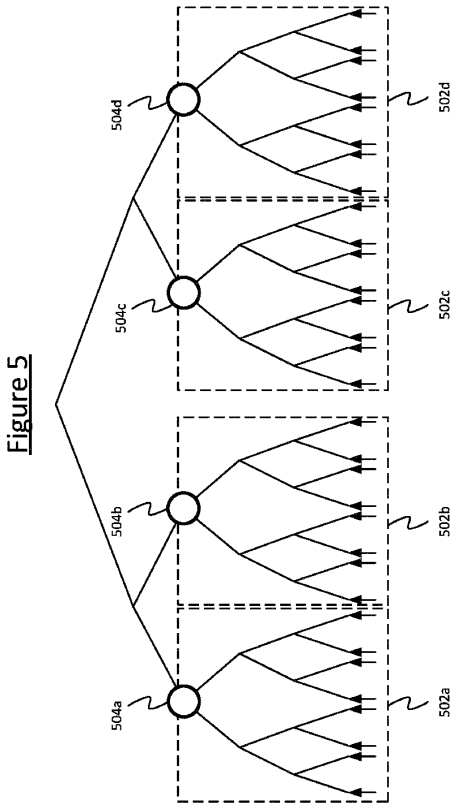
【図 3】



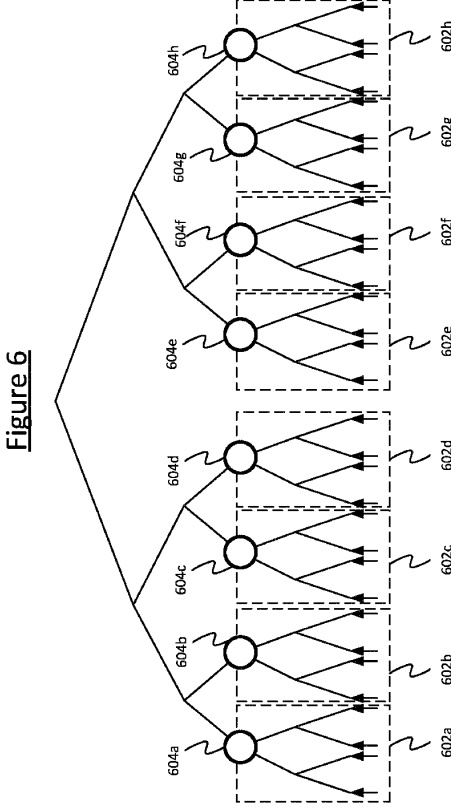
【図 4】



【図 5】



【図 6】



10

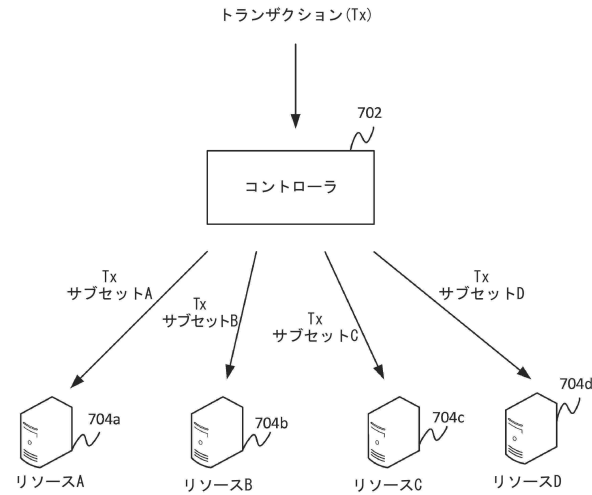
20

30

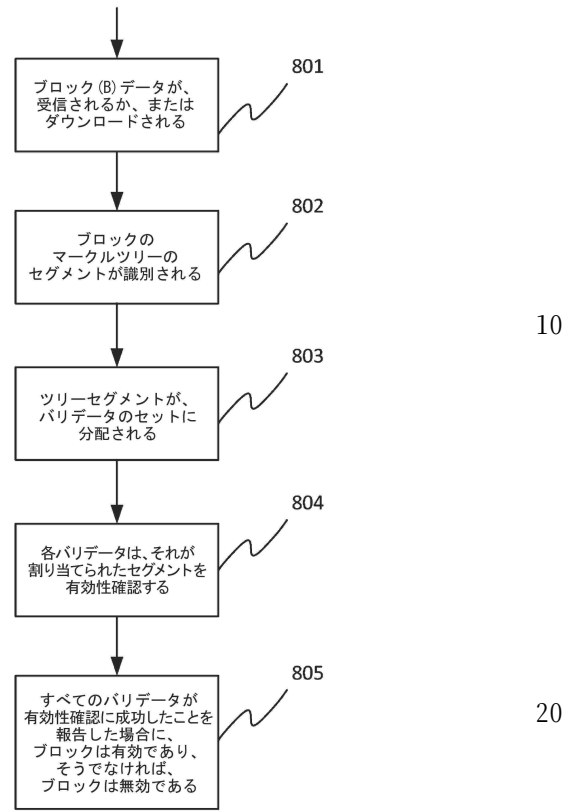
40

50

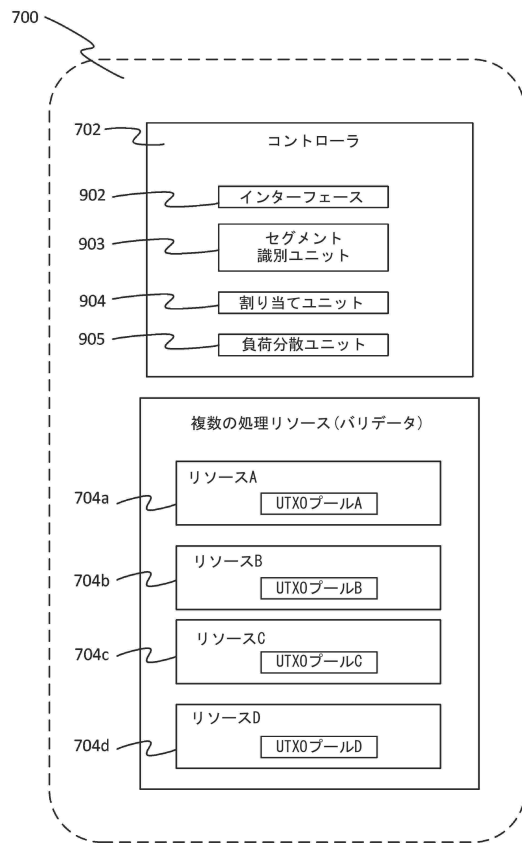
【図 7】



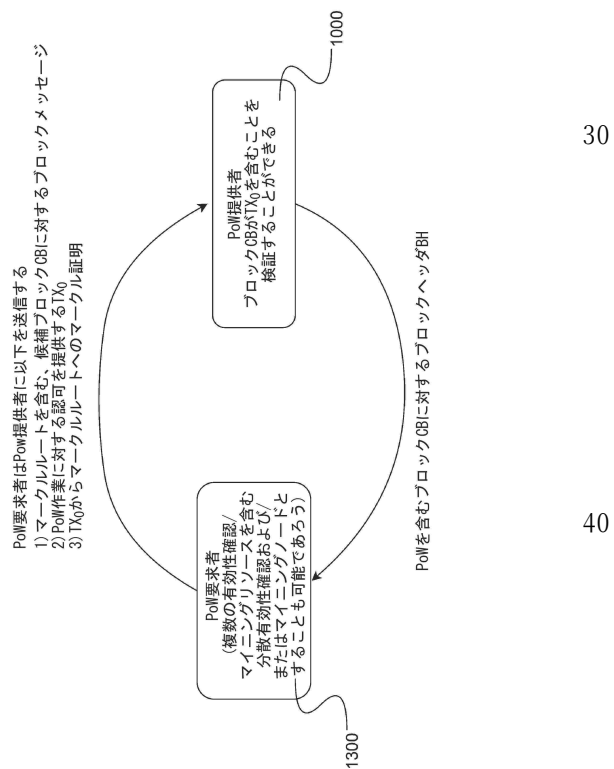
【図 8】



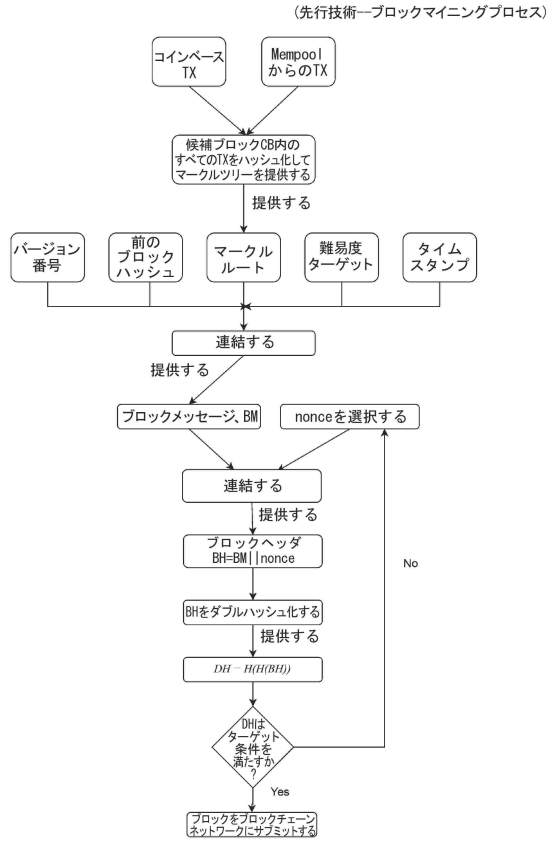
【図 9】



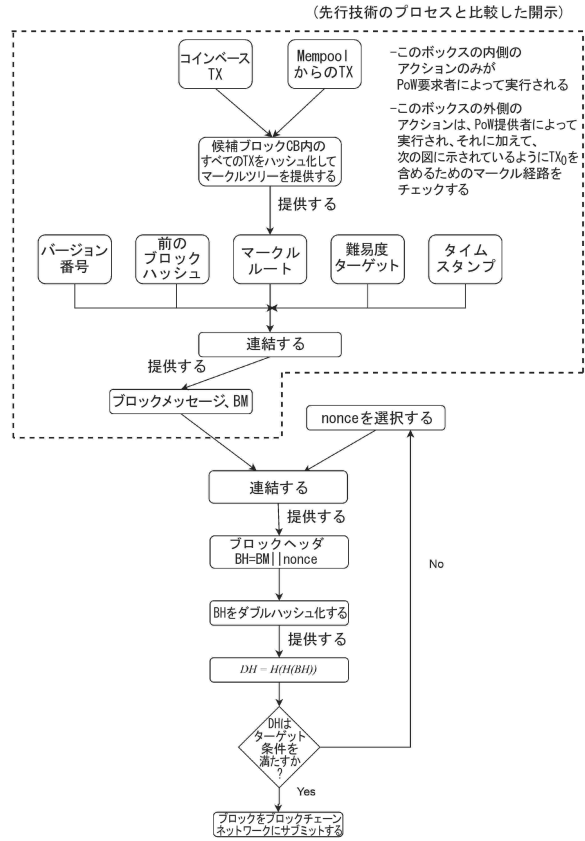
【図 10】



【図 1 1】



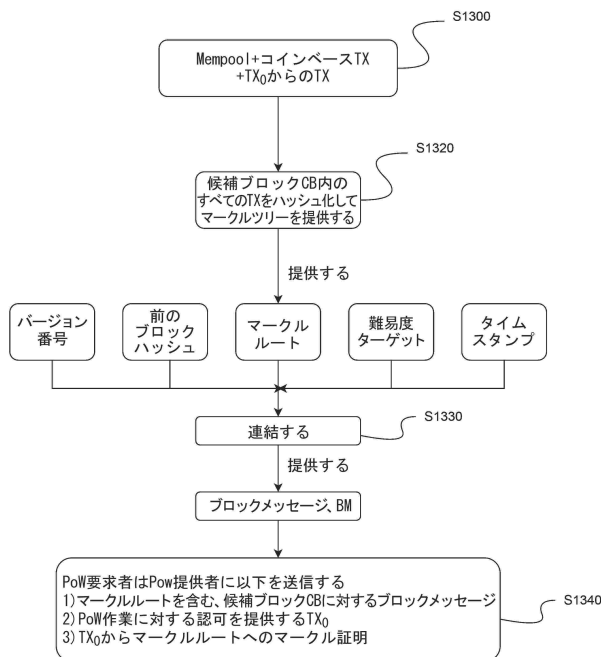
【図 1 2】



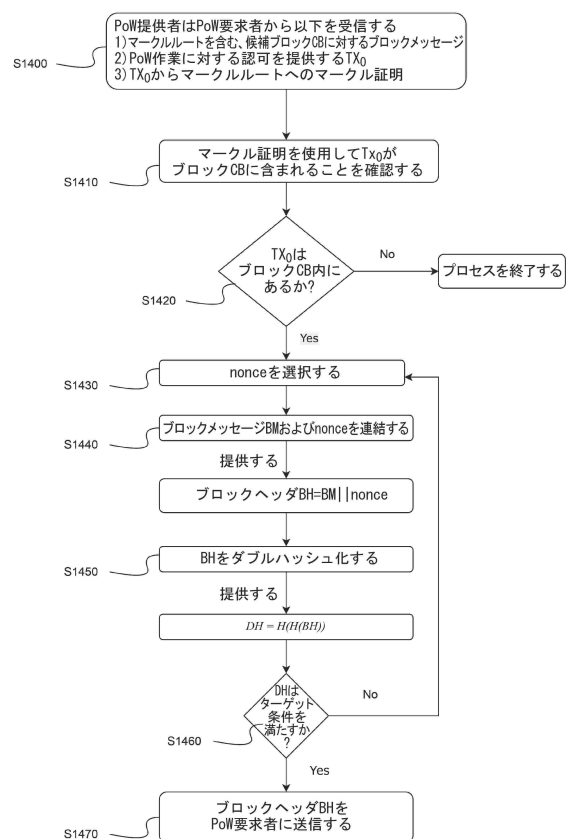
10

20

【図 1 3】



【図 1 4】

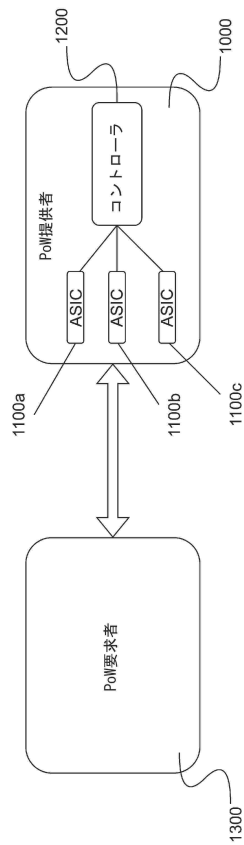


30

40

50

【図 15】



10

20

30

40

50

【手続補正書】

【提出日】令和6年6月27日(2024.6.27)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

コンピュータ実装方法であって、

第1のリソースから第2のリソースに、複数のトランザクションを収容するブロックチェーンブロックに対するプルーフオブワーク(PoW)を生成するための要求を送信するステップであって、前記要求は制御トランザクション(TX<sub>0</sub>)が前記複数のトランザクションに含まれることを検証するためのマークル証明を含む、ステップ、および/または

前記第1のリソースから前記第2のリソースにおいて、複数のトランザクションを収容するブロックチェーンブロックに対するプルーフオブワーク(PoW)を生成するための要求を受信するステップであって、前記要求は制御トランザクション(TX<sub>0</sub>)が前記複数のトランザクションに含まれることを検証するためのマークル証明を含む、ステップを含む、コンピュータ実装方法。

【請求項2】

前記制御トランザクション(TX<sub>0</sub>)は、前記プルーフオブワークの生成の実行を制御し、許可し、および/または禁止するための制御データを含み、前記制御データは、

i)ブロックチェーン移転のデスティネーションに対する所定のアドレスを指定する少なくとも1つの出力であって、

前記アドレスは、前記第2のリソース、または前記第2のリソースに関連付けられたもしくは前記第2のリソースによって認可された当事者に関連付けられる、出力、および/または

ii)少なくとも1つの所定の署名、および/または

iii)少なくとも1つの秘密値またはデータの秘密部分

を含む、請求項1に記載のコンピュータ実装方法。

【請求項3】

前記第1のリソースは、PoW要求リソース、ブロックチェーン有効性確認リソース、またはブロックチェーンマイニングリソースであり、および/または

前記第2のリソースは、プルーフオブワーク提供者であり、および/または

前記第2のリソースは、少なくとも1つのASIC、またはハッシュマシン、または専用暗号通貨マイニングリソースを含む、

請求項1に記載のコンピュータ実装方法。

【請求項4】

i)前記第2のリソースから前記第1のリソースにおいて、前記ブロックチェーンブロックに対するプルーフオブワークを受信するステップ、および/または

ii)前記第2のリソースから前記第1のリソースに、前記ブロックチェーンブロックに対するプルーフオブワークを送信するステップ

をさらに含む、請求項1に記載のコンピュータ実装方法。

【請求項5】

前記プルーフオブワークは、

ブロックチェーンプロトコルによって指定されたターゲット、ルール、または基準のうちの1つもしくは複数を満たす出力を提供するように構成された値(ノンス)、および/または

前記ブロックチェーンブロックに対するブロックヘッダ、および/または

ブロックチェーンプロトコルに従って指定されたパズルまたはチャレンジの解

を含む、請求項1に記載のコンピュータ実装方法。

【請求項6】

前記プルーフオブワークを生成するステップは、

i) ブロックチェーンプロトコルによって指定されたターゲット、チャレンジ、ルール、または基準を満たす出力を提供するように構成された値(ノンス)を生成するか、もしくは選択するステップ、

ii) 前記ブロックチェーンブロックに対するブロックメッセージとノンスとを連結するステップ、および/または

iii) 前記ブロックチェーンブロックに対するブロックヘッダをダブルハッシュ化するステップ

10

を含む、請求項1に記載のコンピュータ実装方法。

【請求項7】

事前定義された制御基準に関して前記制御トランザクション(TX<sub>0</sub>)の少なくとも一部を処理するか、もしくは比較し、前記処理もしくは比較の出力に基づき前記プルーフオブワークを生成するか、もしくは生成しないステップを含み、

前記制御基準は、開始、実行もしくは完了、または前記プルーフオブワークの生成を可能にするための閾値、ルール、または基準のうちの少なくとも1つを含む、請求項1に記載のコンピュータ実装方法。

【請求項8】

前記プルーフオブワークの前記生成を許可するか、または禁止することを、

20

i) 前記制御トランザクション(TX<sub>0</sub>)が前記複数のトランザクションに含まれることの確認の成功もしくは失敗、および/または

ii) 前記制御トランザクションが、所定のルールもしくは基準を満たすデータの一部を含むか、もしくは含まないことの決定、および/または

iii) 前記制御トランザクションもしくはそのの少なくとも一部が前記制御基準を満たすという決定に基づき行うステップ

をさらに含む、請求項7に記載のコンピュータ実装方法。

【請求項9】

前記第1もしくは第2のリソースにおいて、ブロックに対するプルーフオブワークの生成のためにブロックチェーンプロトコルによって必要とされるデータの一部を決定するステップを含み、データの前記一部は

30

プロトコルバージョン識別子、

ブロックハッシュ、

前記プロトコルによって指定されたプルーフオブワーク難易度ターゲット、および/または

タイムスタンプ

のうちの1つもしくは複数を含む、請求項1に記載のコンピュータ実装方法。

【請求項10】

i) 前記マール証明は、前記制御トランザクションが前記複数のトランザクションに含まれるかどうかを決定するためのSPV検証の実行を可能にするように構成されたデータを含み、

40

ii) 前記要求は、前記制御トランザクションを含む、請求項1に記載のコンピュータ実装方法。

【請求項11】

前記複数のトランザクションを処理してマールツリーを提供するステップを含み、

前記処理は、ハッシュ関数を伴う、

請求項1に記載のコンピュータ実装方法。

【請求項12】

前記制御トランザクション(TX<sub>0</sub>)は、前記第2のリソースが前記第1のリソースを識別することを可能にする識別子を含み、前記識別子は、前記制御トランザクションの入力、

50

出力、スクリプト、またはメタデータ部分で提供される、請求項1に記載のコンピュータ実装方法。

【請求項13】

複数のトランザクションを収容するブロックチェーンブロックに対するプルーフオブワークの前記生成を制御するかまたはそれに影響を及ぼすように動作可能であり、および/または請求項1から12のいずれか一項に記載の方法を実装するように動作可能である、システム。

【請求項14】

少なくとも1つのプルーフオブワーク提供リソースであって、  
前記少なくとも1つのプルーフオブワーク提供リソースは、少なくとも1つのASICまたはハッシュマシンを含む、少なくとも1つのプルーフオブワーク提供リソース、

少なくとも1つのプルーフオブワーク要求リソースであって、  
前記少なくとも1つのプルーフオブワーク要求リソースは、本明細書において実質的に開示されている分散有効性確認ノードを含む、少なくとも1つのプルーフオブワーク要求リソース

のうちの少なくとも一方を備える、請求項13に記載のシステム。

【請求項15】

コンピュータシステムのプロセッサによって実行された結果として、請求項1から12のいずれか一項に記載のコンピュータ実装方法を前記コンピュータシステムに実行させるか、または前記コンピュータシステムが実行することを可能にする実行可能命令を含むコンピュータプログラム。

30

40

50

## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No  
**PCT/EP2022/079837**

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>A. CLASSIFICATION OF SUBJECT MATTER</b><br>INV. <b>H04L9/00 G06F21/64</b><br>ADD.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                         |
| According to International Patent Classification (IPC) or to both national classification and IPC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                         |
| <b>B. FIELDS SEARCHED</b><br>Minimum documentation searched (classification system followed by classification symbols)<br><b>H04L G06F</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                         |
| Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                         |
| Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)<br><b>EPO-Internal, WPI Data</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                         |
| <b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                         |
| Category*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                                                                                                                                                                                                                                                                                                                | Relevant to claim No.                                                   |
| <b>X</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>Anonymous: "Stratum Protocol",</b><br><b>/</b><br><b>25 July 2021 (2021-07-25), XP093018969,</b><br><b>Retrieved from the Internet:</b><br><b>URL:https://web.archive.org/web/2021072501</b><br><b>5731/https://reference.cash/mining/stratum</b><br><b>-protocol</b><br><b>[retrieved on 2023-01-30]</b><br><b>page 2, last paragraph</b><br><b>page 3, paragraph 2</b><br><b>page 3, paragraph 3</b><br><b>page 3, paragraph 1</b><br><b>Figure;</b><br><b>page 3</b><br><br><b>-----</b><br><br><b>-/--</b> | <b>1-15</b>                                                             |
| <input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                         |
| * Special categories of cited documents :<br>"A" document defining the general state of the art which is not considered to be of particular relevance<br>"E" earlier application or patent but published on or after the international filing date<br>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)<br>"O" document referring to an oral disclosure, use, exhibition or other means<br>"P" document published prior to the international filing date but later than the priority date claimed<br>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention<br>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone<br>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art<br>"&" document member of the same patent family |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                         |
| Date of the actual completion of the international search<br><b>31 January 2023</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Date of mailing of the international search report<br><b>10/02/2023</b> |
| Name and mailing address of the ISA/<br>European Patent Office, P.B. 5618 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Authorized officer<br><b>Dobre, Dan</b>                                 |

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

INTERNATIONAL SEARCH REPORT

International application No  
PCT/EP2022/079837

| C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT |                                                                                                                                                                                                                                                                                                                                                                                                                     |                       |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Category*                                            | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                                                                                                                                                                                                                  | Relevant to claim No. |
| X                                                    | <p>RUBEN RECABARREN ET AL: "Hardening Stratum, the Bitcoin Pool Mining Protocol",<br/>ARKIV.ORG, CORNELL UNIVERSITY LIBRARY, 201<br/>OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY<br/>14853,<br/>20 March 2017 (2017-03-20), XP080758131,<br/>DOI: 10.1515/POPETS-2017-0028<br/>Sections 2.2, 2.3 and 2.4<br/>page 3, right-hand column - page 5,<br/>right-hand column<br/>figures 2,3<br/>abstract</p> <p>-----</p> | 1-15                  |

1

10

20

30

40

50

## フロントページの続き

(32)優先日 令和3年10月28日(2021.10.28)

(33)優先権主張国・地域又は機関  
英国(GB)

(31)優先権主張番号 2115520.5

(32)優先日 令和3年10月28日(2021.10.28)

(33)優先権主張国・地域又は機関  
英国(GB)

(31)優先権主張番号 2206634.4

(32)優先日 令和4年5月6日(2022.5.6)

(33)優先権主張国・地域又は機関  
英国(GB)

(31)優先権主張番号 2206639.3

(32)優先日 令和4年5月6日(2022.5.6)

(33)優先権主張国・地域又は機関  
英国(GB)

(31)優先権主張番号 2208799.3

(32)優先日 令和4年6月15日(2022.6.15)

(33)優先権主張国・地域又は機関  
英国(GB)

(31)優先権主張番号 2209533.5

(32)優先日 令和4年6月29日(2022.6.29)

(33)優先権主張国・地域又は機関  
英国(GB)

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