(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7585524号
(P7585524)

(45)発行日　令和6年11月18日(2024.11.18)

(24)登録日　令和6年11月8日(2024.11.8)

(51)国際特許分類		FI		
H04L 9/32 (2006.01)		H04L	9/32	200Z
G09C 1/00 (2006.01)		G09C	1/00	650Z

請求項の数　20　（全24頁）

(21)出願番号	特願2023-569697(P2023-569697)
(86)(22)出願日	令和4年4月7日(2022.4.7)
(65)公表番号	特表2024-518487(P2024-518487A)
(43)公表日	令和6年5月1日(2024.5.1)
(86)国際出願番号	PCT/US2022/023795
(87)国際公開番号	WO2022/240500
(87)国際公開日	令和4年11月17日(2022.11.17)
審査請求日	令和5年11月13日(2023.11.13)
(31)優先権主張番号	17/317,456
(32)優先日	令和3年5月11日(2021.5.11)
(33)優先権主張国・地域又は機関	米国(US)

(73)特許権者	500041363 マスターカード インターナショナル インコーポレイテツド アメリカ合衆国ニューヨーク州 パーチエイス パーチエイス ストリート ２００
(74)代理人	100147485 弁理士　杉村 憲司
(74)代理人	230118913 弁護士　杉村 光嗣
(74)代理人	100224683 弁理士　齋藤 詩織
(72)発明者	スティーブン シー デイビス アメリカ合衆国 ミズーリ州 ６３３７６ セント ピーターズ グレナレン ドライブ

最終頁に続く

(54)【発明の名称】　量子耐性ハッシュ化スキームについての方法及びシステム

(57)【特許請求の範囲】

【請求項１】

ハッシュ指向型スキームを用いてパーミッション型ブロックチェーンにて調整をなす方法であって、

処理サーバのメモリ内に、最新ブロックを含む複数のブロックを備えるブロックチェーンを記憶するステップであって、前記最新ブロックはブロックヘッダを含む、ステップと、

処理サーバの受信部によって、１つ以上のトランザクションデータ値を受信するステップと、

処理サーバの前記受信部によって、第１の参照値及び第２の参照値を受信するステップと、

前記処理サーバの処理装置によって、前記第１の参照値をハッシュ化することによって第１のハッシュ値を生成するステップと、

前記処理サーバの前記処理装置によって、少なくとも、前記第１のハッシュ値と第２のハッシュ値と第３の参照値とブロック値とを含むブロックプルーフを生成するステップと、

前記処理サーバの前記処理装置によって、前記ブロックプルーフを用いて前記最新ブロック内に含まれる前記ブロックヘッダを検証するステップと、

前記処理サーバの前記受信部によって、新たなブロック値を受信するステップと、

前記処理サーバの前記処理装置によって、少なくとも、前記第１の参照値と前記第２の参照値と第４の参照値と前記新たなブロック値とを含む新たなブロックヘッダを生成するステップと、

前記処理サーバの前記処理装置によって、前記新たなブロックヘッダと前記１つ以上のトランザクションデータ値とを含む、前記ブロックチェーンについての新たなブロックを生成するステップと、
前記処理サーバの送信部によって、前記新たなブロックを、前記ブロックチェーンと関連付けられている１つ以上の追加のノードへと送信するステップとを含む、方法。
【請求項２】
請求項１に記載の方法において、
前記処理サーバの前記処理装置によって、前記１つ以上のトランザクションデータ値を用いてマークルツリーを生成するステップをさらに含み、
前記新たなブロックヘッダは前記マークルツリーのルートをさらに含む、方法。
【請求項３】
請求項２に記載の方法において、前記新たなブロックヘッダはバージョンデータとブロックヘッダ参照値とをさらに含む、方法。
【請求項４】
請求項３に記載の方法において、
前記処理サーバの前記処理装置によって、前記検証されたブロックヘッダをハッシュ化することによって前記ブロックヘッダ参照値を生成するステップをさらに含む、方法。
【請求項５】
請求項１に記載の方法において、
前記処理サーバの前記処理装置によって、前記第１の参照値と、前記第２の参照値と、前記第４の参照値と、１つ以上のデータポイントとについての組合せをハッシュ化することによって前記ブロック値を生成するステップをさらに含む、方法。
【請求項６】
請求項５に記載の方法において、前記１つ以上のデータポイントは、少なくとも、バージョンデータと、ブロックヘッダ参照値と、マークルツリーのルートとを含む、方法。
【請求項７】
請求項１に記載の方法において、
前記処理サーバの前記処理装置によって、前記第４の参照値をハッシュ化することによって前記第２のハッシュ値を生成するステップをさらに含む、方法。
【請求項８】
請求項７に記載の方法において、前記第４の参照値は前記処理サーバの前記メモリ内に記憶される、方法。
【請求項９】
請求項１に記載の方法において、
前記第１の参照値及び第２の参照値は外部のコンピューティングシステムから受信され、また、
前記新たなブロック値は前記外部のコンピューティングシステムから受信される、方法。
【請求項１０】
請求項９に記載の方法において、前記外部のコンピューティングシステムは前記ブロックチェーンと関連付けられている前記１つ以上の追加のノードのうちの１つである、方法。
【請求項１１】
ハッシュ指向型スキームを用いてパーミッション型ブロックチェーンにて調整をなすシステムであって、
ブロックチェーンと関連付けられているノードとしての処理サーバと、
前記ブロックチェーンと関連付けられている１つ以上の追加のノードとを備え、
前記処理サーバは少なくとも、
送信部と、
最新ブロックを含む複数のブロックを備えるブロックチェーンを記憶するメモリであって、前記最新ブロックはブロックヘッダを含む、メモリと、
１つ以上のトランザクションデータ値と第１の参照値と第２の参照値とを受信する受

信部と、
処理装置と、を含み、前記処理装置は、
前記第１の参照値をハッシュ化することによって第１のハッシュ値を生成するステップと、
少なくとも、前記第１のハッシュ値と第２のハッシュ値と第３の参照値とブロック値とを含むブロックプルーフを生成するステップと、
前記ブロックプルーフを用いて前記最新ブロック内に含まれる前記ブロックヘッダを検証するステップと、を実行し、
前記受信部は新たなブロック値をさらに受信し、
前記処理装置はさらに、
少なくとも、前記第１の参照値と前記第２の参照値と第４の参照値と前記新たなブロック値とを含む新たなブロックヘッダを生成するステップと、
前記新たなブロックヘッダと前記１つ以上のトランザクションデータ値とを含む、前記ブロックチェーンについての新たなブロックを生成するステップと、を実行し、また、
前記送信部は、前記新たなブロックを、前記ブロックチェーンと関連付けられている１つ以上の追加のノードへと送信する、システム。
【請求項１２】
請求項１１に記載のシステムにおいて、
前記処理サーバの前記処理装置はさらに、前記１つ以上のトランザクションデータ値を用いてマークルツリーを生成するステップを実行し、また、
前記新たなブロックヘッダは前記マークルツリーのルートをさらに含む、システム。
【請求項１３】
請求項１２に記載のシステムにおいて、前記新たなブロックヘッダはバージョンデータとブロックヘッダ参照値とをさらに含む、システム。
【請求項１４】
請求項１３に記載のシステムにおいて、前記処理サーバの前記処理装置はさらに、前記検証されたブロックヘッダをハッシュ化することによって前記ブロックヘッダ参照値を生成するステップを実行する、システム。
【請求項１５】
請求項１１に記載のシステムにおいて、前記処理サーバの前記処理装置はさらに、前記第１の参照値と、前記第２の参照値と、前記第４の参照値と、１つ以上のデータポイントとについての組合せをハッシュ化することによって前記ブロック値を生成するステップを実行する、システム。
【請求項１６】
請求項１５に記載のシステムにおいて、前記１つ以上のデータポイントは、少なくとも、バージョンデータと、ブロックヘッダ参照値と、マークルツリーのルートとを含む、システム。
【請求項１７】
請求項１１に記載のシステムにおいて、前記処理サーバの前記処理装置はさらに、前記第４の参照値をハッシュ化することによって前記第２のハッシュ値を生成するステップを実行する、システム。
【請求項１８】
請求項１７に記載のシステムにおいて、前記第４の参照値は前記処理サーバの前記メモリ内に記憶される、システム。
【請求項１９】
請求項１１に記載のシステムにおいて、
前記第１の参照値及び第２の参照値は外部のコンピューティングシステムから受信され、また、
前記新たなブロック値は前記外部のコンピューティングシステムから受信される、システム。

【請求項２０】
請求項１９に記載のシステムにおいて、前記外部のコンピューティングシステムは前記ブロックチェーンと関連付けられている前記１つ以上の追加のノードのうちの１つである、システム。
【発明の詳細な説明】
【関連出願の相互参照】
【０００１】
本出願は、2021年5月11日に出願された米国特許出願第17/317,456号の利益を主張するのであり、その全内容は全ての用途に関して参照によって取り込まれる。
【技術分野】
【０００２】
本開示は、量子コンピューティングを含む演算手法を用いての攻撃又は解読に関して耐性を有するハッシュ化スキームを用いることによって、提示される身分(identity)又は契約等のアサーション（assertion）の証明を検証できるようにすることに関する。
【背景技術】
【０００３】
多くの暗号学的手法は、標準的なコンピュータにとっては解くことが殆ど不可能となる数学的問題を含む複雑なアルゴリズムを伴う。例えば、デジタル署名に頼るブロックチェーン及び他の技術は多くの場合、素因数分解に頼るRSA（Rivest-Shamir-Adleman）法又は離散対数問題を用いるECDSA（elliptic curve digital signature algorithm（楕円曲線デジタル署名アルゴリズム））法を活用する。どちらの場合でも、標準的なコンピュータはこれらの数学的問題を解くには遅すぎるのであり且つ非効率すぎるのである故に、関連する諸アルゴリズムを適切に暗号学的に安全なものたらしめる。
【０００４】
もっとも、量子コンピューティングが開発中であり、これが成功すれば上述のような数学的問題が解かれる可能性がある。その結果、根底にある数学的問題が解決可能となる場合にはRSA及びECDSA等のアルゴリズムを介してのデジタル署名の活用は無効となり得るのであり、それによっていくつかの脆弱性及びセキュリティ脅威が生起し得る。また、伝統的なハッシュに基づく署名は実用的な用法にはあまりにも非現実的なデータサイズを伴う。したがって、既存のアルゴリズムから利用可能な身分及びアサーションについての証明を提供しつつ量子コンピューティングをも用いる解決試行に対して耐性を有する暗号学的手法を用い得る技術的なシステムが必要とされる。
【発明の概要】
【０００５】
本開示は、ハッシュ指向型トランザクションスキームを用いる値についてのアサーションについての証明に関するシステム及び方法についての説明を提供する。数学的問題に頼る標準的なアルゴリズムの代わりにハッシュ化を用いることによって、SHA-256等の衝突耐性のある十分なサイズの値を結果としてもたらす十分に複雑なハッシュが用いられた場合には特に、量子コンピューティングに対して耐性がもたらされる。宣言（declaration）を記憶するのにブロックチェーンが用いられるのであり、ブロックチェーンは宣言メッセージ（declaration message）についての不変且つタイムスタンプ付き記録をもたらす。宣言は、身分証、契約、土地の権利証、投票記録等のユーザが後に証明することを望み得る値を含む。宣言はハッシュ値をも含むのであり、これは値とユーザにのみ知られる１つ以上の他のアイテムとをハッシュ化することによって生成される。ユーザがその値について所有を証明する或いはその真正性について他の態様で認証することを望む場合、ユーザはブロックチェーン上で確認メッセージ（confirmation message）を発することができる。確認メッセージは、宣言内に格納されているハッシュ値を作成するのに用いられていた１つ以上の他のアイテムを含む。ユーザに知られるそれらの値が開示されることによって、ユーザのアサーションを監査することを望む任意のエンティティは、認証される値と確認メッセージ内の１つ以上の他のアイテムとを用いてハッシュ値を計算でき、また、

それを宣言内のハッシュ値との関係で検査できる。一致は、ユーザのアサーションについての成功を証明する。その結果として、ユーザがハッシュ化及びブロックチェーンの活用によって値のアサーションについて迅速且つ簡便且つ安全に証明することを可能としつつ、量子コンピューティングに対しての耐性を示すシステムが得られる。

【０００６】

ハッシュ指向型スキームを用いてパーミッション型ブロックチェーンにて調整をなす方法は次のステップを含む：処理サーバのメモリ内に、最新ブロックを含む複数のブロックを備えるブロックチェーンを記憶するステップであって、該最新ブロックはブロックヘッダを含む、ステップと、処理サーバの受信部によって、１つ以上のトランザクションデータ値を受信するステップと、処理サーバの前記受信部によって、第１の参照値及び第２の参照値を受信するステップと、前記処理サーバの処理装置によって、前記第１の参照値をハッシュ化することによって第１のハッシュ値を生成するステップと、前記処理サーバの前記処理装置によって、少なくとも、前記第１のハッシュ値と第２のハッシュ値と第３の参照値とブロック値とを含むブロックプルーフを生成するステップと、前記処理サーバの前記処理装置によって、前記ブロックプルーフを用いて前記最新ブロック内に含まれる前記ブロックヘッダを検証するステップと、前記処理サーバの前記受信部によって、新たなブロック値を受信するステップと、前記処理サーバの前記処理装置によって、少なくとも、前記第１の参照値と前記第２の参照値と第４の参照値と前記新たなブロック値とを含む新たなブロックヘッダを生成するステップと、前記処理サーバの前記処理装置によって、前記新たなブロックヘッダと前記１つ以上のトランザクションデータ値とを含む、前記ブロックチェーンについての新たなブロックを生成するステップと、前記処理サーバの送信部によって、前記新たなブロックを、前記ブロックチェーンと関連付けられている１つ以上の追加のノードへと送信するステップ。

【０００７】

ハッシュ指向型スキームを用いてパーミッション型ブロックチェーンにて調整をなすシステムは：ブロックチェーンと関連付けられているノードとしての処理サーバと、前記ブロックチェーンと関連付けられている１つ以上の追加のノードとを備え、前記処理サーバは少なくとも、送信部と、最新ブロックを含む複数のブロックを備えるブロックチェーンを記憶するメモリであって前記最新ブロックはブロックヘッダを含むメモリと、１つ以上のトランザクションデータ値と第１の参照値と第２の参照値とを受信する受信部と、処理装置とを含み、前記処理装置は、前記第１の参照値をハッシュ化することによって第１のハッシュ値を生成するステップと、少なくとも、前記第１のハッシュ値と第２のハッシュ値と第３の参照値とブロック値とを含むブロックプルーフを生成するステップと、前記ブロックプルーフを用いて前記最新ブロック内に含まれる前記ブロックヘッダを検証するステップとを実行し、前記受信部は新たなブロック値をさらに受信し、前記処理装置はさらに、少なくとも、前記第１の参照値と前記第２の参照値と第４の参照値と前記新たなブロック値とを含む新たなブロックヘッダを生成するステップと、前記新たなブロックヘッダと前記１つ以上のトランザクションデータ値とを含む、前記ブロックチェーンについての新たなブロックを生成するステップとを実行し、また、前記送信部は前記新たなブロックを前記ブロックチェーンと関連付けられている１つ以上の追加のノードへと送信する。

【図面の簡単な説明】

【０００８】

本開示の範囲は、以下の例示的な実施形態の詳細な説明を添付の図面と併せて読むことによって最もよく理解される。図面には、以下の図面が含まれる:

【０００９】

【図１】例示的な実施形態による、ハッシュ指向型トランザクションスキーム及びブロックチェーンを用いて値のアサーションを証明するための高レベルシステムアーキテクチャを示すブロック図である。

【図２】例示的な実施形態による、ハッシュ指向型トランザクションスキーム及びブロックチェーンを用いて値のアサーションを検証するための図１のシステムの処理サーバを示

すブロック図である。
【図３】例示的な実施形態による、図１のブロックチェーン内に格納され得る例示的な宣言及び確認メッセージについて示す図である。
【図４】例示的な実施形態による、図１のブロックチェーン内に格納され得る、ブロックヘッダを通じての所有移転のための例示的なメッセージについて示す図である。
【図５Ａ】例示的な実施形態による、ハッシュ指向型トランザクションスキーム及びブロックチェーンを用いて図１のシステム内においてアサートされた値を検証するための処理について示す流れ図である。
【図５Ｂ】例示的な実施形態による、ハッシュ指向型トランザクションスキーム及びブロックチェーンを用いて図１のシステム内においてアサートされた値を検証するための処理について示す流れ図である。
【図６】例示的な実施形態による、ハッシュ指向型トランザクションスキームを用いて値のアサーションの証明を検証するための例示的な方法について示す流れ図である。
【図７】例示的な実施形態による、ハッシュ指向型スキームを用いてのパーミッション型ブロックチェーンにて調整をなす例示的な方法について示す流れ図である。
【図８】例示的な実施形態による、コンピュータシステムアーキテクチャを示すブロック図である。
【００１０】
本開示の適用可能性のさらなる態様は、以下に提供される詳細な説明から明らかになる。例示的な実施形態の詳細な説明は例示のみを目的としたものであり、したがって、本開示の範囲を必ずしも限定することを意図したものではないことを理解されたい。
【発明を実施するための形態】
【００１１】
用語集
ブロックチェーン：暗号通貨等のブロックチェーンベースのデジタル資産の全てのトランザクションについての共有台帳。１つ以上のコンピューティング装置はブロックチェーンネットワークを備えることができ、ブロックチェーンネットワークはブロックチェーン内のブロックの一部としてトランザクションを処理し記録するように構成することができる。ブロックが完成すると、ブロックはブロックチェーンに追加され、それによってトランザクション記録が更新される。多くの場合、ブロックチェーンは、時系列順のトランザクションの台帳であってもよく、又はブロックチェーンネットワークによる使用に適し得る任意の他の順序で提示されてもよい。いくつかの構成では、どの資産が特定のアドレスに起因するかをブロックチェーンが記録するように、ブロックチェーンに記録されたトランザクションは宛先アドレス及びデジタル資産量を含むことができる。場合によっては、トランザクションは金融であり、他のものは金融ではないか、又はソースアドレス、タイムスタンプ等の追加又は別の情報を含むことができる。いくつかの実施形態では、ブロックチェーンは、追加的に又は代替的に、その操作者によってさえ、改ざん及び改訂に対して強化されたデータレコードの連続的に増大する一覧を維持する分散データベースに配置されるか、又は配置される必要があるトランザクション形態として、ほぼ任意のタイプのデータを含むことができるし、ブロックチェーンネットワークによって、プルーフオブワーク（ＰｏＷ）及び／又はそれに関連する任意の他の適切な検証技術を介して、確認及び検証されることができる。場合によっては、所与のトランザクションに関するデータがトランザクションデータに添付されたトランザクションの直接的な部分ではない追加のデータをさらに含むことができる。場合によっては、ブロックチェーンにおいてそのようなデータを包含することがトランザクションを構成し得る。そのような場合、ブロックチェーンは、特定のデジタル通貨、仮想通貨、不換通貨、又は他のタイプの通貨に直接的に関連付けられなくてもよい。
【００１２】
ハッシュ化及びブロックチェーンを用いるアサーション証明のシステム
図１は、ハッシュ指向型スキーム及びブロックチェーンを用いての、値についてのアサ

ーション証明の検証のためのシステム100について示す。
【００１３】
システム100は、処理サーバ102を含み得る。以下にて詳述される処理サーバ102は、特定の値をアサートするユーザ104によって与えられる証明を検証するように構成され得る。システム100では、ユーザ104によって特定の値を、ブロックチェーンネットワーク106と関連付けられているブロックチェーンに供給できる。特定の値は、ユーザ104によってブロックチェーンネットワーク106へと宣言メッセージとして提出され得るのであり、これについては以下詳述する。
【００１４】
ブロックチェーンネットワーク106は、複数のノードを備え得る。各ノードは、ブロックチェーンの処理及び管理に関する機能をなすように構成されているコンピューティングシステムとされ得るのであり、例えば次の事項が含まれ得る：ブロックチェーン値の生成、提案されたブロックチェーントランザクションの検証、デジタル署名の検証、新たなブロックの生成、新たなブロックの検証、及びブロックチェーンのコピーの保全。ブロックチェーンは、少なくとも複数のブロックを備える分散台帳とされ得る。各ブロックは、少なくとも、ブロックヘッダと１つ以上のデータ値とを含み得る。各ブロックヘッダは、少なくとも、タイムスタンプと、ブロック参照値と、データ参照値とを含み得る。タイムスタンプは、ブロックヘッダが生成された時刻とされ得るのであり、また、任意の適切な方法を用いて表され得る（例えば、ＵＮＩＸタイムスタンプ、DateTime等）。ブロック参照値は、ブロックチェーン内の前のブロックを（例えば、タイムスタンプに基づいて）参照する値とされ得る。いくつかの実施形態では、ブロックヘッダ内のブロック参照値は、各々のブロックに先行する最も新しく追加されたブロックのブロックヘッダへの参照とされ得る。例示的な実施形態では、ブロック参照値は、最も新しく追加されたブロックのブロックヘッダについてのハッシュ化を介して生成されたハッシュ値とされ得る。同様に、データ参照値は、ブロックヘッダを含むブロック内に格納された１つ以上のデータ値への参照とされ得る。例示的な実施形態では、データ参照値は、１つ以上のデータ値についてのハッシュ化を介して生成されたハッシュ値とされ得る。例えば、ブロック参照値は、１つ以上のデータ値を用いて生成されたマークルツリーのルートとされ得る。
【００１５】
ブロック参照値及びデータ参照値を、各ブロックヘッダにて用いることによって、結果としてブロックチェーンが不変なものとされ得る。データ値についての任意の改変試行は、そのブロックについての新たなデータ参照値の生成が必要となるのであり、それにより後続のブロックのブロック参照値が新たに生成されることが必要となり、更にそれにより全ての後続のブロックについて新たなブロック参照値の生成が必要となる。変更を永続的なものとするには、ブロックチェーンに新たなブロックの生成及び追加をすることに先行してこのことに関してブロックチェーンネットワーク106内のあらゆる個々のノードについて実行及び更新されることが必要となる。演算及び通信に関する制約故に、そのような改変は、不可能ではないにしてもかなり困難なものとなり、それによってブロックチェーンが不変性を帯びるに至る。
【００１６】
各ブロックチェーンデータ値は、後述のように、確認メッセージ又は宣言メッセージに対応し得る。デスクトップコンピュータ、ラップトップコンピュータ、ノートブックコンピュータ、タブレットコンピュータ、携帯電話、スマートフォン、スマートウォッチ、スマートテレビ、ウェアラブルコンピューティング装置又は本明細書で述べる機能をなすように具体的に構成された任意の他のタイプのコンピューティング装置等の適切なコンピューティング装置108を用いるユーザ104によって、宣言メッセージをノードに提出できる。宣言メッセージは、値それ自体が真正であることの証明或いは値の所有についての証明をユーザが後に証明することを望み得る特定の値を含み得る。例えば、特定の値は身分証に関する場合があり、説明される方法を用いることによってユーザ104が、身分証にて特定される人物（person）が自己であることを立証することが可能となり得る。別の例では

、特定の値は土地の権利証に関する場合があり、説明される方法を用いることによってユーザ104が、土地の権利証の所有者が自己でありそれ故にそれが適用される土地の所有者が自己であることを立証することが可能となる。

【００１７】

宣言メッセージは、「アイデンティティハッシュ値」とも称されるハッシュ値をも含み得る。ハッシュ値は、特定の値と「チェーン値」とも称される１つ以上の追加の値とをハッシュ化することによって生成し得る。チェーン値は、宣言メッセージ提出時にはユーザ104に知られていることはあり得るが、それ以外について任意の他のエンティティ（特に、ブロックチェーンネットワーク106における任意のノード）に関しては未知とされ得る。ユーザ104は、SHA-256等の任意の適切なハッシュアルゴリズムを用いて特定の値とチェーン値とをハッシュ化してアイデンティティハッシュ値を生成できる。例示的な実施形態では、衝突耐性ハッシュアルゴリズムを用い得る。好適な実施形態では、ハッシュ値の生成では少なくとも２つのチェーン値を用い得る。ユーザ104は、ブロックチェーンネットワーク106内のノードへと宣言メッセージを提出でき、宣言メッセージには少なくとも、特定の値とアイデンティティハッシュ値とが含まれる。そして、宣言メッセージは、新たなブロックに含めることができ、それを検証してブロックチェーンに追加できる。

【００１８】

システム100では、リクエストシステム110は、特定の値についてのアサーションについての証明をユーザ104が提供することを要求できる。例えば、特定の値が身分証に関する例では、リクエストシステム110は、ユーザ104が自己の身分についての証明を提供するように要求できる。このような例では、ユーザ104は、ブロックチェーンとアイデンティティハッシュ値とを用いて、宣言メッセージ内に格納されている身分証にて示されている個人（individual）が自己であることを立証できる。リクエストシステム110は、確認要求を処理サーバ102へと提出できる。確認要求は、リクエストシステム110が検証を得ることを望む宣言メッセージを指定できる。一部の例では、各宣言メッセージは、一意的識別子を含み得るのであり、宣言メッセージの識別のために処理サーバ102が活用するために確認要求に含めることができる。

【００１９】

そして、処理サーバ102は、ユーザ104によって提供されたアサーションの証明を介して宣言メッセージに含まれる値の検証を試みることができる。検証は、ブロックチェーン内に格納されている確認メッセージを用いることによってなされ得る。検証が要求された場合には、ユーザ104によって確認メッセージが（例えば、コンピューティング装置108を介して）ブロックチェーンネットワーク106内のノードへと提出され得る。一部の場合では、処理サーバ102はユーザ104が確認メッセージを提出するように要求できる（例えば、リクエストシステム110から確認要求を受信した後にこれをなし得るのであって、ユーザ104についての連絡先情報が確認要求に含まれていることができる）。一部の場合では、リクエストシステム110は、ユーザ104が確認メッセージをポスト（post）するように要求できる。例えば、上述の例では、リクエストシステム110が、ユーザ104が自己の身分について証明を提供するように要求した場合、ユーザ104は、確認メッセージをブロックチェーンに提出して、また、自己の身分証を含む宣言メッセージについての識別子をリクエストシステム110に提供することによって応答できる。

【００２０】

特定の値についてのアサーションについてのユーザの証明を検証するために、処理サーバ102は先ず、ブロックチェーンに格納されている確認メッセージを識別できる。一部の場合では、各確認メッセージは、それが対応する宣言メッセージ内に見出される識別子を含み得る。他の場合では、各確認メッセージはそれ自体の識別子を含み得るのであって、識別子はブロックチェーン内の全メッセージについてそれによって一意的であり、ユーザ104又はリクエストシステム110はその識別子を、確認メッセージの識別に用いるために、処理サーバ102に提供できる。

【００２１】

確認メッセージは、宣言メッセージに格納されていたアイデンティティハッシュ値を生成する際にユーザ104によって用いられた検査値を少なくとも含み得る。処理サーバ102は、確認メッセージ内の検査値を識別して、また、検査値と、識別された宣言メッセージに含まれる特定の値とを用いて検査ハッシュ値を生成できる。そして、処理サーバ102は、検査ハッシュ値を、宣言メッセージ内に見出されたアイデンティティハッシュ値との関係で検査して、一致があるかを検討できる。一致がある場合には、特定の値の所有をそれがブロックチェーンへ追加された時点において（例えば、宣言メッセージを含むブロックのブロックヘッダ内に見出されるタイムスタンプにて）ユーザ104が有していたに違いないということになる。なぜならば、アイデンティティハッシュ値を生成するのに用いられた検査値をそれらが有していたからである。これは特定の値についてのアサーションについての証明として機能し得るのであり、そしてこの場合、処理サーバ102はリクエストシステム110に対して適宜通知し得る。検査値とアイデンティティハッシュ値との間で一致がない場合、処理サーバ102は、リクエストシステム110に対してユーザの証明試行が失敗したと適宜通知し得る。

【００２２】

よって、説明される方法及びシステムは、所有又は特定の時点にて値が存在したことをユーザ104がアサートすることを可能とするのであり、ブロックチェーンを用いることを介してこれがなされ、そのアサーションの証明はハッシュ指向型トランザクションスキームを用いることを介して検証でき、ブロックチェーンへ後に提出された確認メッセージを用いることを介することとなる。開示のように特に構成された処理サーバ102によって検証を容易になし得るのであり、リクエストシステム110は、それ自体が何らかの複雑な動作をなすことを要さずにして証明を容易に検証させることができる。また、デジタル署名に代えてハッシュを用いることによって、説明される方法は、量子コンピューティングを介した解読試行に対して耐性を有するのであり、他方で十分に複雑なハッシュ化アルゴリズムが衝突の欠如を担保するのであり、それによって、安全でありつつ容易に実装可能なシステムが得られる。

【００２３】

一部の実施形態では、確認メッセージ及び宣言メッセージを連鎖させて、所有及びアサーションについて追加的セキュリティ並びに別のユーザへの特定の値についての所有の移転をもたらすことができる。連鎖化は、追加のチェーン値を用いることによってなし得る。例えば、確認メッセージは、宣言メッセージ内に見出されるアイデンティティハッシュ値を算出するために用いられる２つのチェーン値を含み得る。宣言メッセージは、２つの新たなチェーン値を含み得る。これらの新たなチェーン値は、新たな宣言及び確認メッセージの組合せにて用いられるハッシュチェーンの一部たり得る。

【００２４】

例えば、宣言メッセージは、値Ｘと、Ｘ及びＡ及びＢの組合せをハッシュ化することによって生成されたアイデンティティハッシュ値とを含み得る。したがって、Ａ及びＢは、値Ｘの検証に用いられる確認メッセージ内に見出されるチェーン値であることができる。さらに、宣言メッセージは、２つの新たなチェーン値C_2及びD_2を含み得る。後続の宣言メッセージはユーザ104によって値Ｘについての後の証明ラウンドのために提出できるのであり、宣言メッセージはＸ及びC_1及びD_1の組合せをハッシュ化することによって生成されたアイデンティティハッシュ値を含み得る。C_2及びD_2についての値はC_1及びD_1についての値と関連し得るのであって、例えばC_1及びD_1の値についてのハッシュ等とされ得るのであり、ここで$C_2 = H(C_1)$及び$D_2 = H(D_1)$とし、Ｈはハッシュ化オペレーションを指す。

【００２５】

例を挙げるに、公職選挙の投票に先んじて投票者は選挙管理者に対して自己の身分について証明することを要求され得るのであって、その身分証が値Ｘであるものとする。投票者はC_1の所有を持っていることがあり、適宜ハッシュ化を介してC_2を生成することができる。身分の証明を確立するためには、選挙管理者は投票者にD_1を提供できる。投票

者はD_1のハッシュ化を介してD_2を生成でき、そして、C_2、D_2、身分証、並びにC_1＋D_1＋身分証のハッシュを含む宣言メッセージをポスト（post）できる。この時点にて選挙管理者は宣言をみることができ、提供された値に基づいてD_2を認識できる。そして、選挙管理者は、投票者が、自己のC_1と供給されたD_1とを伴う確認メッセージをポストすることを待つことができ、値を用いて宣言メッセージ内のハッシュを確認することができる。確認されると、身分証の所有が投票者にあることがそれによって証明され、また、それ故に投票者の身分を検証できる。

【００２６】

一部の場合、宣言メッセージ内にて用いられている新たなチェーン値の１つは、新たなハッシュチェーンの一部たり得る。例えば、ユーザ104は値Ｘについての第１の宣言メッセージを提出でき、これはアイデンティティハッシュ値$H(X+A_1+B_1)$を含む（ここで、対応する確認メッセージはチェーン値A_1及びB_1を含む）。第１の宣言メッセージは、新たなチェーン値A_2及びB_2をも含み得る。第２の宣言メッセージについては新たなハッシュチェーンを活用できるのであり、第２の宣言メッセージは値Ｘ及びアイデンティティハッシュ値$H(X+B_3+C_1)$を含むものとされる。第２の宣言メッセージについての確認メッセージは、したがって、チェーン値B_3及びC_1を含み得る。したがって、極悪な行為者は、宣言メッセージ内のチェーン値についてハッシュ化を単に継続していって、後の宣言－確認の組合せの推測を試みることはできない。なぜならば、新たなハッシュチェーンC_1が用いられるからである。同様に、ユーザ104が値Ｘの所有を移転したい場合、新たなユーザからアイデンティティハッシュ値$H(X+B_3+C_1)$を与えられることができ、ここで新たなユーザが値C_1を知っているがこれはユーザ104に知られていない。よって、新たなユーザのみが値Ｘについてのアサーションについての検証可能な証明を提供できることとなる。したがって、宣言メッセージにおいてハッシュチェーン又は他の新たに導入されたチェーン値を用いることによって、システム100にて値についての所有又は他のアサーションを容易に移転するために用いられ得る

【００２７】

一部の場合では、ブロックチェーンはパーミッション型又は他の態様で調整されたブロックチェーンとされ得るのであり、この場合には１つ以上の調整エンティティ112がブロックチェーンネットワーク106に参加して、コンピューティング装置108、処理サーバ102、及び／又はブロックチェーンに関与する他のシステムの参加を調整できる。そのような場合、調整エンティティ112は、自己のデジタル署名を、ブロックチェーンに追加される新たなブロックについて提供するように要求され得る。その結果、ブロックチェーンにて表わされている任意の新たなアクションには３つのエンティティが関与している場合があるのであり、またそれ故に、調整エンティティ112を含めるに際しては宣言及び確認メッセージを用いたのでは不十分となり得る。そのような場合、上述のハッシュチェーンと併せてブロックヘッダを用いることができるのであり、各ブロックヘッダがハッシュチェーン値を含み得る。

【００２８】

そのような実施形態では、ブロックヘッダは、値Ｘと、Ｘ及びチェーン値の組合せをハッシュ化することによって生成したハッシュ値Ｈと、チェーン値それ自体とを格納するために用いられ得る。これらの実施形態では、チェーン値は、移転に関与しているエンティティと関連付けられている値を含み得るのであり（例えば、チェーン値A_1及びB_2）、また、調整エンティティと関連付けられている別のチェーン値をも含み得る（例えば、チェーン値C_2）。図４には、調整型ブロックチェーンにおけるブロックヘッダの例が示されており、以下においてより詳しく説明する。このようなブロックチェーンでは、チェーンの「所有者」が次のブロックを確認する権利を有しているという意味合いで所有移転を実行し得る。一部の場合では、エンティティは、追加される新たなブロック毎に所有を自己に戻すように移転することによって所有者として繰り返すことができる。例えば、調整エンティティ112は、全てのブロックの確認に関して完全な所有を維持でき、他のエンティティは上述のようにそれに参加することとなる。

【００２９】
そのような実施形態では、各ブロックのヘッダに含まれる値Ｘは、ブロックバージョン等のバージョンデータ、ネットワーク識別子、及びスロット番号、前のブロックのブロックヘッダのハッシュ（例えば、ブロック参照値）、及び追加される新たなブロックに含まれる全トランザクションのマークルツリーのルート（例えば、データ参照値）が含まれ得る。この値Ｘは、各ブロックに追加されるハッシュ値に含まれていることができ、ここで、値Ｘは、上述されておりまた図４にて示されているようにチェーン値と組み合わされることができる。
【００３０】
処理サーバ
図2は、システム100における処理サーバ102の一実施形態を示す。図2に示される処理サーバ102の実施形態は例示としてのみ提供され、本明細書で説明されるような機能を実行するのに適した処理サーバ102の考えられるすべての構成を網羅するものではないことが、当業者には明らかであろう。例えば、図8に示され、以下でより詳細に説明されるコンピュータシステム800が、処理サーバ102の好適な構成であってもよい。
【００３１】
処理サーバ102は、受信装置202を含むことができる。受信装置202は、１つ以上のネットワークプロトコルを介して１つ以上のネットワーク上でデータを受信するように構成され得る。いくつかの例では、受信装置202は無線周波数、ローカルエリアネットワーク、無線エリアネットワーク、セルラ通信ネットワーク、Bluetooth、インターネット等の１つ以上の通信方法を介して、ブロックチェーンネットワーク106、コンピューティング装置108、リクエストシステム110、並びに他のシステム及びエンティティからデータを受信するように構成され得る。いくつかの実施形態では、受信装置202が、異なるネットワークを介してデータを受信するための異なる受信装置(ローカルエリアネットワークを介してデータを受信するための第1の受信装置、及びインターネットを介してデータを受信するための第2の受信装置等)等の複数の装置から構成されてもよい。受信装置202は電子的に送信されたデータ信号を受信でき、ここで、データは、データ信号上に重畳されるか、さもなければ符号化され、受信装置202によるデータ信号の受信により復号され、解析され、読み取られ、又はさもなければ取得され得る。いくつかの例では、受信装置202は、受信されたデータ信号を解析してその上に重畳されたデータを取得するための解析モジュールを含んでもよい。例えば、受信装置202は、受信されるデータ信号を受信し、それを処理装置によって実行される機能用に使用可能な入力に変換して、本明細書に記載された方法及びシステムを実行するよう構成された解析プログラムを含んでもよい。
【００３２】
受信装置202は、ブロックチェーンデータと重畳されることができるか又はさもなければ符号化することができるブロックチェーンネットワーク106内のノードによって電子的に送信されるデータ信号を受信するように構成されていることができ、ブロックチェーンデータには確認メッセージ及び宣言メッセージを含み得るブロックチェーンデータ値が含まれる。一部の実施形態では、受信装置202は全ての新たなブロックを含むブロックチェーンの完全コピーを受信し得る。他の実施形態では、受信装置202は要求されたブロックを受信し得る。他の実施形態では、受信装置202はブロックチェーンデータ値を受信し得る。一部の実施形態では、処理サーバ102は、ブロックチェーンネットワーク106内のノードとされ得るのであり、ブロックチェーンネットワーク106の他のノードから検証及び追加のためのブロックを受信し得る。また、受信装置202は、宣言及び／又は確認メッセージについての識別子を含み得る確認要求が重畳又はその他の態様で符号化された電子的に送信されたデータ信号であってコンピューティング装置108及び／又はリクエストシステム110によって送信された信号を受信するように構成されていることもできる。
【００３３】
処理サーバ102はまた、通信モジュール204を含んでもよい。通信モジュール204は、モジュール、エンジン、データベース、メモリ、及び本明細書で説明される機能を実行す

る際に使用するための処理サーバ102の他の構成要素の間でデータを送信するように構成され得る。通信モジュール204は、１つ以上の通信種別から構成され、コンピューティング装置内の通信のために様々な通信方法を利用することができる。例えば、通信モジュール204は、バス、接点ピンコネクタ、配線等から構成されてもよい。いくつかの実施形態では、通信モジュール204はまた、処理サーバ102の内部構成要素と、外部接続データベース、表示装置、入力装置等の処理サーバ102の外部構成要素との間で通信するように構成されてもよい。処理サーバ102はまた、処理装置を含んでもよい。当業者には明らかなように、処理装置は、本明細書で説明する処理サーバ102の機能を実行するように構成することができる。いくつかの実施形態では、処理装置が問い合わせモジュール218、生成モジュール220、検証モジュール222等、処理装置の１つ以上の機能を実行するように特別に構成された複数のエンジン及び／又はモジュールを含むことができ、及び／又はそれらから構成することができる。本明細書で使用される「モジュール」という用語は、入力を受信し、入力を使用して１つ以上の処理を実行し、出力を提供するように特にプログラムされたソフトウェア又はハードウェアとすることができる。様々なモジュールによって実行される入力、出力、及び処理は、本開示に基づいて当業者には明らかであろう。

【００３４】

処理サーバ102は、問い合わせモジュール218を含むことができる。問い合わせモジュール218は、情報を識別するためにデータベース上で照会を実行するように構成することができる。問い合わせモジュール218は１つ以上のデータ値又はクエリ文字列を受信することができ、メモリ226等の指示されたデータベースに基づいてクエリ文字列を実行して、その中に格納された情報を識別することができる。そして、問い合わせモジュール218は、特定した内容を適宜、処理サーバ102の適切なエンジンに出力する。問い合わせモジュール218は、例えば、メモリ226上にてクエリを実行して、識別子を用いる等してブロックチェーン内のブロックにて格納されている宣言メッセージ又は確認メッセージを識別できる。

【００３５】

処理サーバ102はまた、生成モジュール220を含んでもよい。生成モジュール220は、本明細書で説明される機能を実行するに際して処理サーバ102が用いるためのデータを生成するように構成され得る。生成モジュール220は入力として命令を受け取り、命令に基づいてデータを生成し、生成されたデータを処理サーバ102の１つ以上のモジュールに出力できる。例えば、生成モジュール220は、通知及び他のデータメッセージを生成するように構成されていることができ、例えば確認メッセージ及び／又は識別子についてのプロンプト又は試みられた検証の結果等をコンピューティング装置108又はリクエストシステム110へ送信したり、並びに、例えば新たなブロック又はブロックチェーンデータ値等を要求することをブロックチェーンネットワーク106内のノードへと送信したりできる。生成モジュール220は、データをハッシュ化することによって検査ハッシュ値を生成するように構成されていることができる。処理サーバ102がブロックチェーンネットワーク106内のノードである実施形態では、生成モジュール220は、検証するため或いはブロックチェーンへの追加のためにブロックヘッダ及び新しいブロックを生成するようにも構成され得る。

【００３６】

処理サーバ102はまた、検証モジュール222を含んでもよい。検証モジュール222は、説明したように処理サーバ102の機能の一部としてデータを検証するように構成されていることができる。検証モジュール222は、検証されるべきデータを入力として受信することができ、データ検証を試みることができ、また、検証の結果を処理サーバの別のモジュール又はエンジンに出力することができる。場合によっては、入力が検証に使用されるデータを含むことができる。一部の場合では、検証モジュール222は検証に用いられるべきデータを識別するように構成されていることができ、これは生成モジュール220に対して検査ハッシュ値を生成せよと命令することによってでき、この際には検証モジュール222による検査ハッシュ値に用いるための宣言メッセージ内のチェーン値を用いる。検証モジ

ュール222は、例えば、宣言メッセージ内に見出されるアイデンティティハッシュ値を検証するように構成されていることができ、対応する確認メッセージ内に見出されるチェーン値を用いて生成された検査ハッシュ値を用いてこれがなされ得る。

【００３７】

処理サーバ102はまた、送信装置224を含んでもよい。送信装置224は、1つ以上のネットワークプロトコルを介して1つ以上のネットワーク上でデータを送信するように構成されてもよい。いくつかの例では、送信装置224はローカルエリアネットワーク、無線エリアネットワーク、セルラ通信、Bluetooth、無線周波数、インターネット等の１つ以上の通信方法を介して、ブロックチェーンネットワーク106、コンピューティング装置108、リクエストシステム110、並びに他のエンティティへとデータを送信するように構成され得る。いくつかの実施形態では、送信装置224が異なるネットワークを介してデータを送信するための異なる送信装置(ローカルエリアネットワークを介してデータを送信するための第1の送信装置、及びインターネットを介してデータを送信するための第2の送信装置等)等の複数の装置から構成されてもよい。送信装置224は、受信側コンピューティング装置によって解析され得るデータが重畳されたデータ信号を電子的に送信することができる。いくつかの例では、送信装置224は、重畳する、符号化する、又は伝送に適したデータ信号にデータを成形(フォーマット)するための１つ以上のモジュールを含むことができる。

【００３８】

送信装置224は、ブロックチェーンネットワーク106内のノードへとデータ信号を電子的に送信するように構成されていることができ、これらにはブロックチェーンデータ値又はブロックについての要求が重畳されているか又はさもなければ符号化されており、宣言又は確認メッセージ用の識別子が含まれ得る。また、送信装置224は、コンピューティング装置108へとデータ信号を電子的に送信するようにも構成されていることができ、これらには確認メッセージの提出についての要求、確認メッセージの識別子についての要求等が重畳されているか又はさもなければ符号化されていることができる。また、送信装置224は、リクエストシステム110へとデータ信号を電子的に送信するようにも構成されていることができ、これらには検証結果が重畳されているか又はさもなければ符号化されていることができる。

【００３９】

処理サーバ102はまた、メモリ226を含んでもよい。メモリ226は、公開鍵及び秘密鍵、対称鍵等、本明細書で説明される機能を実行する際に処理サーバ102によって使用されるデータを記憶するように構成され得る。メモリ226は、適切なデータ成形方法及びスキーマを使用してデータを記憶するように構成されてもよく、読出し専用メモリ、ランダムアクセスメモリ等の任意の適切なタイプのメモリであってもよい。メモリ226は例えば、暗号鍵及びアルゴリズム、通信プロトコル及び規格、データフォーマット規格及びプロトコル、プロセッシング装置のモジュール及びアプリケーションプログラムのためのプログラムコード、ならびに当業者に明らかであるように、本明細書で開示される機能の性能において処理サーバ102によって使用されるのに適し得る他のデータを含み得る。いくつかの実施形態では、メモリ226がその中に格納された構造化データセットの格納、識別、修正、更新、アクセス等のために構造化クエリ言語を利用するリレーショナルデータベースから構成されてもよく、又はさもなければリレーショナルデータベースを含んでもよい。メモリ226は、例えば、確認メッセージ及び宣言メッセージを含むブロックチェーンデータ、ブロック生成用のハッシュアルゴリズム、検査ハッシュ値生成用のハッシュアルゴリズム、検証用の認証情報、用法規則テンプレート、ブロックチェーンノード用通信データ、コンピューティング装置108及びリクエストシステム110用の通信データ等を格納するように構成されていることができる。

【００４０】

メッセージの宣言及び確認

図3は、図1のシステム100における値のアサーションの証明の検証にて用いるための例示的な宣言及び確認メッセージについて示す。

【００４１】
上述のように、ユーザ104は、検証されてブロックチェーンに追加される新たなブロックに内に含められるために、宣言メッセージ302をブロックチェーンネットワーク106へと提出できる。宣言メッセージは特定の値304を含み得るのであり、ユーザ104は特定の値304の証明をアサートしたいかもしれない（例えば、上述の例における身分証等）。宣言メッセージはアイデンティティハッシュ値308をも含み得るのであり、アイデンティティハッシュ値は特定の値並びに2つのチェーン値312をハッシュ化して生成したハッシュ値である。宣言メッセージ302の提出時においては、チェーン値312はユーザ104に知られているが他の誰にも知られていないものとされ得る。宣言メッセージ302も2つの新たなチェーン値306を含み得るのであり、図3では新たなチェーン値306a及び306bとして示され、これは後の宣言及び確認メッセージのペアに用いられるハッシュチェーンの一部とされ得る。
【００４２】
ユーザ104が特定の値304のアサーションを証明したい場合には、ユーザ104は確認メッセージ310をブロックチェーンに提出できる。確認メッセージはチェーン値312を含み得るのであり、図3においてはチェーン値312a及び312bとして示されており、アイデンティティハッシュ値308を生成するために用いられたのである。一部の実施形態では、チェーン値312は新たなチェーン値306を伴うハッシュチェーンの一部とされ得る。図3に示される例では、新たなチェーン値306aはチェーン値312aのハッシュとされ得るのであり、また、新たなチェーン値306bはチェーン値312bのハッシュとされ得る。示された例では、チェーン値312aは新たなハッシュチェーンの始点である場合があり、チェーン値312bは、宣言及び確認メッセージの以前のセットで用いられたような既存のハッシュチェーンの一部である場合がある。
【００４３】
調整型ブロックチェーンにおけるブロックヘッダ
図4は、図１のシステム100にて用いるためのブロックヘッダの例について示し、ハッシュチェーンを活用する調整型ブロックチェーンのブロックヘッダの確認に関するものである。
【００４４】
システム100では、リクエストシステム110は、ブロックチェーンについての新たなブロックを構築可能とするという意味でのブロックチェーンの所有取得に関して関心が持たれていることがある。リクエストシステム110は、示されている例では「Ｂ」とラベル付けされたチェーン値によって表され得るのであり、リクエストシステム110は、現在は所有を有しておらず、後続ブロック４０４を構築可能としたい故に所有を得たいものとされる。所有を得るために、リクエストシステム110は、現在の所有者から所有を求めるのであり、処理サーバ102については示される例では「Ａ」とラベル付けされたチェーン値によって表され得る。所有の取得の前に、リクエストシステム110は、次に生じることとなる移転について把握していることを要し、そのような後続のエンティティは「Ｃ」とラベル付けされたチェーン値によって表され得る。
【００４５】
所有を受けるためには、リクエストシステム110はチェーン値406b及び406cを処理サーバ102へと送信し、チェーン値406bはＢ２であり、これはＢ１のハッシュであり、リクエストシステム110のみに知られる値である。チェーン値406cはＣ３であり、これはＣ２のハッシュであり、後続のエンティティによってリクエストシステム110であるものと知られており、その基礎となる値はリクエストシステム110には知られていない。そして、処理サーバ102は、特定の値410aとチェーン値406b及び406cとを有していることになる。新たなブロック402を追加できるようにするためには、リクエストシステム110はブロック値412aを供給しなければならず、これはリクエストシステム110には知られているが処理サーバ102には知られていないチェーン値のハッシュである。そして、処理サーバ102は、チェーン値406a，406b及び406cと特定の値410aとハッシュ値412aとから

なる新たなブロック402を生成する。新たなブロック402の追加により、ブロック構築についての所有はリクエストシステム110に移転する。なぜならば、リクエストシステム110が少なくともチェーン値408aについて知っている(knowledge)唯一のエンティティであるからである。そして、リクエストシステム110は、上述に類する態様でリクエストシステム110に関する値2(410b)と408cと412bとを用いて、チェーン値４０８ｂについての基礎となる値を有する後続のエンティティに所有を移転できるようになり得るのであり、以降の新たなブロックについてもそのようになされる。

【００４６】

ハッシュ化及びブロックチェーンを用いてアサーションの証明を検証するプロセス

図５Ａ及び図５Ｂは、ブロックチェーンネットワーク106及びハッシュ指向型トランザクションスキームを用いて、ユーザ104によって提示された特定の値のアサーションの証明を検証するための図１のシステム100におけるプロセスの例について示す。

【００４７】

Ｓ（ステップ）５０２では、ユーザ104は、コンピューティング装置108を用いて、宣言メッセージをブロックチェーンネットワーク106へと提出する。宣言メッセージは少なくとも、識別子（本明細書にてはデータエントリ識別子と称される）と特定の値とアイデンティティハッシュ値とを含む。Ｓ５０４では、ブロックチェーンネットワーク106は宣言メッセージを受信できる。Ｓ５０６では、宣言メッセージは新たなブロックに含めることができ、それを検証してブロックチェーンに追加できる。一部の実施形態では、宣言メッセージのデータエントリ識別子はＳ５０４又はＳ５０６にてブロックチェーンネットワーク106によって識別され得るのであり、これはコンピューティング装置108に戻され得る。

【００４８】

Ｓ５０８では、コンピューティング装置108及びリクエストシステム110は取り決めに加入できる。例えば、上述の例では、リクエストシステム110は、ユーザ104が自己の身分についての証明を提供するように要求し得るのであり、これを達成することに関してユーザ104は、身分証を特定の値として用いるのであり、これはブロックチェーンネットワーク106に提出された宣言メッセージに含まれている。Ｓ５１０では、取り決めの一環として、ユーザ104は宣言メッセージについてのデータエントリ識別子をリクエストシステム110に、コンピューティング装置108を介して、提供できる。Ｓ５１２では、リクエストシステム110は、適切な通信ネットワーク及び方法を用いて確認要求を処理サーバ102に提出できる。確認要求は、少なくともデータエントリ識別子を含み得る。

【００４９】

Ｓ５１４では、処理サーバ102の受信装置202は、リクエストシステム110からの確認要求を受信できる。Ｓ５１６では、処理サーバ102は、要求メッセージ（request message）をコンピューティング装置108へと電子的に送信できるのであり、特定の値（例えば、上述の例の身分証）の証明をアサートするためにユーザ104がブロックチェーンネットワーク106に確認メッセージを提出するように要求する。Ｓ５１８では、コンピューティング装置108は、処理サーバ102から要求メッセージを受信できる。

【００５０】

Ｓ５２０では、コンピューティング装置108は確認メッセージをブロックチェーンネットワーク106に提出できる。確認メッセージは、少なくとも、データエントリ識別子及び１つ以上のチェーン値を含み得る。Ｓ５２２では、ブロックチェーンネットワーク106は確認メッセージを受信できる。Ｓ５２４では、確認メッセージは新たなブロック内に含まれ得るのであり、これは生成され、検証され、ブロックチェーンにポストされる。Ｓ５２６では、処理サーバ102の受信装置202は、ブロックチェーンネットワークの更新を介して確認メッセージを受信できる。Ｓ５２８では、処理サーバ102の生成モジュール220は、確認メッセージ内に見出されるチェーン値と宣言メッセージ内に見出される特定の値とをハッシュ化することによって検査ハッシュ値を生成できる。

【００５１】

Ｓ５３０では、処理サーバ102の検証モジュール222は、検査ハッシュ値の検証を、宣言メッセージ内に見出されるアイデンティティハッシュ値とそれを比較することによって試み得るのであり、ユーザ104によるアサーションの証明の検証とすることができる。Ｓ５３２では、処理サーバ102の送信装置224は、確認通知（confirmation notification）をリクエストシステム110に電子的に送信できる。確認通知は、検証の結果を含み得るのであり、これが成功である場合にはユーザのアサーションを確認することができる（例えば、その者が上述の例の身分証にて識別される人物であること）。Ｓ５３４では、リクエストシステム110は、処理サーバ102から確認通知を受信できる。

【００５２】

値についてのアサーションについての証明を検証するための例示的方法

図６は、ブロックチェーンをハッシュ指向型トランザクションスキームと組み合わせて用いることを介して、値についてのアサーションについての証明を検証する方法６００について示す。

【００５３】

Ｓ６０２では、確認要求が処理サーバ（例えば、処理サーバ102）の受信部（例えば、受信装置202）によって受信され得る。Ｓ６０４では、確認メッセージが処理サーバの処理装置（例えば、問い合わせモジュール218）によって識別され得るのであり、確認メッセージは少なくとも１つ以上のチェーン値を含み且つ次のいずれかである：確認要求に含まれる、或いは、ブロックチェーン内に含まれるブロック内に記憶されており及び確認要求内に含まれる参照識別子を用いて識別される。Ｓ６０６では、宣言メッセージが処理サーバの処理装置によって識別されることができ、該宣言メッセージは少なくとも、アサートされた値とアイデンティティハッシュ値とを含む。

【００５４】

Ｓ６０８では、少なくとも、アサートされた値と１つ以上のチェーン値とをハッシュ化することによって処理サーバの処理装置（例えば、生成モジュール220）によって検査ハッシュ値を生成できる。Ｓ６１０では、アイデンティティハッシュ値を用いて処理サーバの処理装置（例えば、検証モジュール222）によって検査ハッシュ値を検証できる。Ｓ６１２では、検査ハッシュ値の検証の結果を、受信された確認要求に応答して、処理装置の送信部（例えば、送信装置224）によって送信できる。

【００５５】

パーミッション型ブロックチェーンにおける調整についての例示的方法

図７は、ハッシュ指向型トランザクションスキームを用いてなされるパーミッション型ブロックチェーンでの調整についての方法７００について示す。

【００５６】

Ｓ７０２では、ブロックチェーンは処理サーバ（例えば、処理サーバ102）のメモリ（例えば、メモリ226）内に格納されていることができるのであり、ブロックチェーンは最新ブロックを含む複数のブロックを備えるのであり、該最新ブロックはブロックヘッダを含む。Ｓ７０４では、１つ以上のトランザクションデータ値が処理サーバの受信部（例えば、受信装置202）によって受信され得る。Ｓ７０６では、第１の参照値及び第２の参照値が処理サーバの受信部によって受信され得る。Ｓ７０８では、第１の参照値をハッシュ化することによって、処理サーバの処理装置（例えば、生成モジュール220）によって第１のハッシュ値を生成できる。Ｓ７１０では、処理サーバの処理装置によって、少なくとも、第１のハッシュ値と第２のハッシュ値と第３の参照値とブロック値とを含むブロックプルーフを生成することができる。

【００５７】

Ｓ７１２では、最新ブロック内に含まれるブロックヘッダについては、ブロックプルーフを用いて処理装置（例えば、検証モジュール222）によって検証をなし得る。Ｓ７１４では、新たなブロック値を処理サーバの受信部によって受信できる。Ｓ７１６では、処理サーバの処理装置によって、少なくとも、第１の参照値と第２の参照値と第４の参照値と新たなブロック値とを含む新たなブロックヘッダを生成できる。Ｓ７１８では、処理サー

バの処理装置によって、ブロックチェーンについての新たなブロックが生成されることができる。該新たなブロックは、新たなブロックヘッダと１つ以上のトランザクションデータ値とを含む。Ｓ７２０では、新たなブロックはブロックチェーンと関連付けられている１つ以上の追加のノードへと処理サーバの送信部（例えば、送信装置224）によって送信されることができる。

【００５８】

１つの実施形態では、方法７００は、処理サーバの処理装置によって１つ以上のトランザクションデータ値を用いてマークルツリーを生成するステップをさらに含み得るのであり、新たなブロックヘッダはマークルツリーのルートをさらに含む。さらなる実施形態では、新たなブロックヘッダは、バージョンデータとブロックヘッダ参照値とをさらに含む。さらなる実施形態では、方法７００は、処理サーバの処理装置によって検証されたブロックヘッダをハッシュ化することによってブロックヘッダ参照値を生成するステップをさらに含み得る。一部の実施形態では、方法７００は、処理サーバの処理装置によって第１の参照値と、第２の参照値と、第４の参照値と、１つ以上のデータポイントとについての組合せをハッシュ化することによってブロック値を生成するステップをさらに含み得る。さらなる実施形態では、１つ以上のデータポイントは、少なくとも、バージョンデータと、ブロックヘッダ参照値と、マークルツリーのルートとを含み得る。

【００５９】

１つの実施形態では、方法７００は、処理サーバの処理装置によって、第４の参照値をハッシュ化することによって第２のハッシュ値を生成するステップをさらに含み得る。さらなる実施形態では、第４の参照値は処理サーバのメモリ内に記憶されることができる。一部の実施形態では、第１の参照値及び第２の参照値は外部のコンピューティングシステム（例えば、調整エンティティ112）から受信され得るのであり、新たなブロック値は外部のコンピューティングシステムから受信され得る。さらなる実施形態では、外部のコンピューティングシステムはブロックチェーンと関連付けられている１つ以上の追加のノードのうちの１つとされ得る。

【００６０】

コンピュータシステムアーキテクチャ

図8は、本開示の実施形態又はその一部がコンピュータ可読コードとして実装され得るコンピュータシステム800を示す。例えば、図1の処理サーバ102は、ハードウェア、ソフトウェア、ファームウェア、命令が格納された非一時的なのコンピュータ可読媒体、又はそれらの組合せを使用して、コンピュータシステム800内で実装されることができ、１つ又は複数のコンピュータシステム又は他の処理システム内で実装されることができる。ハードウェア、ソフトウェア、又はそれらの任意の組合せは、図3、図4、図5A、図5B、図6及び図7の方法を実施するために使用されるモジュール及び構成要素を具現化することができる。

【００６１】

プログラマブルロジックが使用される場合、そのようなロジックは特定の目的のコンピュータ又は特別の目的の装置(例えば、プログラマブルロジックアレイ、特定用途向け集積回路等)になるように、実行可能なソフトウェアコードによって構成された市販の処理プラットフォーム上で実行されてもよい。当業者は、開示された主題の実施形態がマルチコアのマルチプロセッサシステム、ミニコンピュータ、メインフレームコンピュータ、分散機能とリンクされた又はクラスタ化されたコンピュータ、並びに実質的に任意の装置に埋め込まれ得るパーベイシブ又はミニチュアコンピュータを含む、様々なコンピュータシステム構成で実施され得ることを理解し得る。例えば、少なくとも1つのプロセッサ装置及びメモリを使用して、上記の実施形態を実施することができる。

【００６２】

本明細書で説明するプロセッサユニット又は装置は、単一のプロセッサ、複数のプロセッサ、又はそれらの組み合わせとすることができる。本明細書で論じる「コンピュータプログラム媒体」、「非一時的コンピュータ可読媒体」、及び「コンピュータ使用可能媒体

」という用語は一般に、取外し可能な記憶ユニット818、取外し可能な記憶ユニット822、及びハードディスクドライブ812にインストールされたハードディスク等の有形媒体を指すために使用される。

【００６３】

本開示の様々な実施形態を、この例示的なコンピュータシステム800に関して説明する。この説明を読んだ後、他のコンピュータシステム及び／又はコンピュータアーキテクチャを使用して本開示をどのように実施するかが、当業者には明らかになるであろう。動作は連続的なプロセスとして説明することができるが、動作のいくつかは実際には並列に、同時に、及び／又は分散環境で、及び単一又はマルチプロセッサマシンによるアクセスのためにローカル又はリモートに格納されたプログラムコードを用いて実行することができる。さらに、いくつかの実施形態では、動作の順序は、開示された主題の趣旨から逸脱することなく再構成され得る。

【００６４】

プロセッサ装置804は、本明細書で説明する機能を実行するように特に構成された専用又は汎用プロセッサ装置とすることができる。プロセッサ装置804は、バス、メッセージキュー、ネットワーク、マルチコアメッセージパッシングスキーム等の通信インフラストラクチャ806に接続され得る。ネットワークは本明細書で開示されるような機能を実行するのに適した任意のネットワークとすることができ、ローカルエリアネットワーク(LAN)、ワイドエリアネットワーク(WAN)、ワイヤレスネットワーク(例えば、WiFi)、移動通信ネットワーク、衛星ネットワーク、インターネット、光ファイバ、同軸ケーブル、赤外線、無線周波数(RF)、又はそれらの任意の組合せを含むことができる。他の適切なネットワークのタイプ及び構成は、当業者には明らかであろう。コンピュータシステム800はまた、メインメモリ808(例えば、ランダムアクセスメモリ、読み出し専用メモリ等)を含んでもよく、二次メモリ810を含んでもよい。二次メモリ810は、ハードディスクドライブ812と、フロッピーディスクドライブ、磁気テープドライブ、光ディスクドライブ、フラッシュメモリ等の取り外し可能な記憶ドライブ814とを含むことができる。

【００６５】

取り外し可能な記憶ドライブ814は、公知な方法で、取り外し可能な記憶ユニット818から読み取ることも、及び／又は書き取ることもできる。取り外し可能な記憶ユニット818は、取り外し可能な記憶ドライブ814によって読み書きされ得る取り外し可能な記憶媒体を含み得る。例えば、取り外し可能な記憶ドライブ814がフロッピーディスクドライブ又はユニバーサルシリアルバスポートである場合、取り外し可能な記憶ユニット818は、それぞれフロッピーディスク又はポータブルフラッシュドライブであってもよい。一実施形態では、取り外し可能な記憶ユニットは非一時的なコンピュータ可読記録媒体とすることができる。

【００６６】

いくつかの実施形態では、二次メモリ810がコンピュータプログラム又は他の命令をコンピュータシステム800、例えば、取り外し可能な記憶ユニット822及びインタフェース820にロードすることを可能にする代替手段を含むことができる。このような方法の例はプログラムカートリッジ及びカートリッジインタフェース(例えば、ビデオゲームシステムに見られるようなもの)、取り外し可能なメモリチップ(例えば、EEPROM、PROM等)及び関連するソケット、並びに他の取り外し可能な記憶ユニット822及びインタフェース820を含むことができる。

【００６７】

コンピュータシステム800(例えば、メインメモリ808及び／又は二次メモリ810)に記憶されたデータは光学記憶装置(例えば、コンパクトディスク、デジタルバーサタイルディスク、ブルーレイディスク等)又は磁気テープ記憶装置(例えば、ハードディスクドライブ)のような、任意のタイプの好適なコンピュータ可読媒体に記憶されてもよい。データは、リレーショナルデータベース、SQL(structured query language)データベース、分散データベース、オブジェクトデータベース等、任意のタイプの適切なデータベース構成で構

成することができる。好適な形態及び格納の種別は、当業者には明らかであろう。

【００６８】

コンピュータシステム800は、通信インタフェース824をも含むことができる。通信インタフェース824は、ソフトウェア及びデータがコンピュータシステム800と外部装置との間で転送されることを可能にするように構成されてもよい。例示的な通信インタフェース824はモデム、ネットワークインタフェース(例えば、イーサネットカード)、通信ポート、PCMCIAスロット及びカード等を含むことができる。通信インタフェース824を介して転送されるソフトウェア及びデータは当業者には明らかなように、電子信号、電磁気信号、光学信号、又は他の信号形態とすることができる。信号は、信号を搬送するように構成されてもよく、ワイヤ、ケーブル、光ファイバ、電話回線、携帯電話リンク、無線周波数リンク等を使用して実装されてもよい通信経路826を介して伝搬してもよい。

【００６９】

コンピュータシステム800は、表示インタフェース802をさらに含むことができる。表示インタフェース802は、コンピュータシステム800と外部のディスプレイ830との間でデータが転送されることを可能にするように構成されてもよい。例示的な表示インタフェース802は、高精細マルチメディアインタフェース(HDMI)、デジタルビジュアルインタフェース(DVI)、ビデオグラフィックスアレイ(VGA)等を含むことができる。ディスプレイ830は、陰極線管(CRT)ディスプレイ、液晶表示装置(LCD)、発光ダイオード(LED)ディスプレイ、静電タッチディスプレイ、薄膜トランジスタ(TFT)ディスプレイ等を含む、コンピュータシステム800の表示インタフェース802を介して伝送されるデータを表示するための任意の好適な種類のディスプレイであってもよい。

【００７０】

コンピュータプログラム媒体及びコンピュータ使用可能媒体は、メモリ半導体(例えば、DRAM等)であってもよいメインメモリ808及び二次メモリ810等のメモリを指してもよい。これらのコンピュータプログラム製品は、コンピュータシステム800にソフトウェアを提供するための手段とすることができる。コンピュータプログラム(例えば、コンピュータ制御ロジック)は、メインメモリ808及び/又は二次メモリ810に記憶されてもよい。コンピュータプログラムはまた、通信インタフェース824を介して受信されてもよい。そのようなコンピュータプログラムは、実行されると、コンピュータシステム800が本明細書で論じる本方法を実施することを可能にすることができる。特に、コンピュータプログラムは、実行されると、プロセッサ装置804が本明細書で説明するように、図3、図4、図5A、図5B、図6及び図7に示す方法を実施することを可能にすることができる。したがって、そのようなコンピュータプログラムは、コンピュータシステム800のプロセッサを示すことができる。本発明がソフトウェアを使用して実施される場合、ソフトウェアは、コンピュータプログラムプロダクトに格納され、取り外し可能な記憶ドライブ814、インタフェース820、及びハードディスクドライブ812、又は通信インタフェース824を使用してコンピュータシステム800にロードされてもよい。

【００７１】

プロセッサ装置804は、コンピュータシステム800の機能を実行するように構成された1つ又は複数のモジュール又はエンジンを備えることができる。モジュール又はエンジンのそれぞれはハードウェアを使用して実装することができ、場合によってはメインメモリ808又は二次メモリ810に格納されたプログラムコード及び／又はプログラムに対応するようなソフトウェアを利用することもできる。そのような場合、プログラムコードはコンピュータシステム800のハードウェアによって実行される前に、プロセッサ装置804によって（例えば、コンパイルモジュール又はエンジンによって）コンパイルされてもよい。例えば、プログラムコードはプロセッサ装置804及び／又はコンピュータシステム800の任意の追加のハードウェアコンポーネントによる実行のために、アセンブリ言語又はマシンコード等の低レベル言語に翻訳されるプログラミング言語で書かれたソースコードであってもよい。コンパイル処理は、語彙解析、前処理、構文解析、意味解析、構文指向翻訳、コード生成、コード最適化、及び本明細書で開示される機能を実行するようにコンピュ

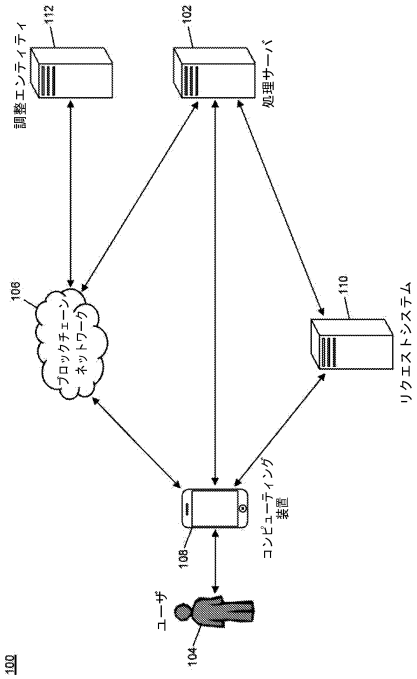
ータシステム800を制御するのに適した低レベル言語へのプログラムコードの翻訳に適し得る任意の他の技術の使用を含み得る。当業者には、このようなプロセスの結果、コンピュータシステム800が上述の機能を実行するように一意にプログラムされた特別に構成されたコンピュータシステム800になることが明らかであろう。

【００７２】

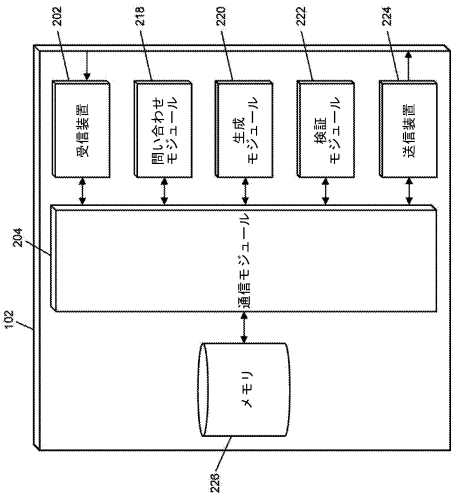
本発明による技術は、とりわけ、ハッシュ指向型スキームを用いてパーミッション型ブロックチェーンにて調整をなすためのシステム及び方法を提供する。開示されたシステム及び方法の様々な例示的な実施形態が上記で説明されるが、それらは限定的なものではなく、単に例示の目的のために提示されることが理解されるべきである。これは網羅的ではなく、開示される厳密な形態に本開示を限定するものではない。上記の教示に照らして修正及び変形が可能であり、或いは、本開示の実施から、その広さ又は範囲から逸脱することなく、修正及び変形を得ることができる。

【図面】

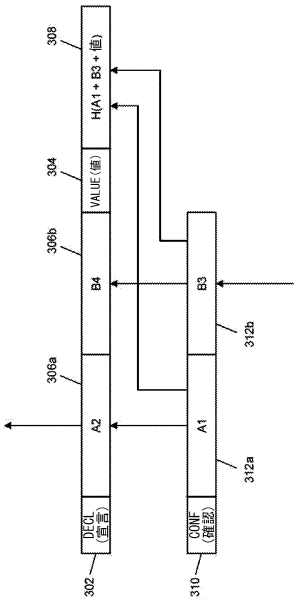
【図１】


調整エンティティ
112
処理サーバ
102
ブロックチェーン
ネットワーク
106
リクエストシステム
110
コンピューティング
装置
108
ユーザ
104
100

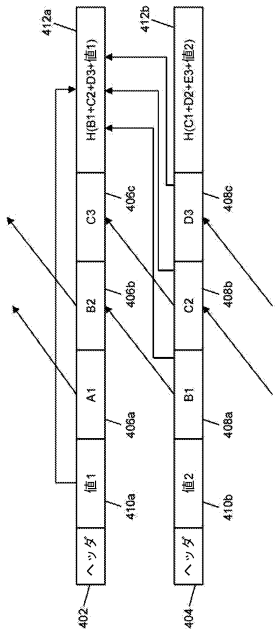
【図２】


202
218
220
222
224
受信装置
問い合わせ
モジュール
生成
モジュール
検証
モジュール
送信装置
204
通信モジュール
102
メモリ
226

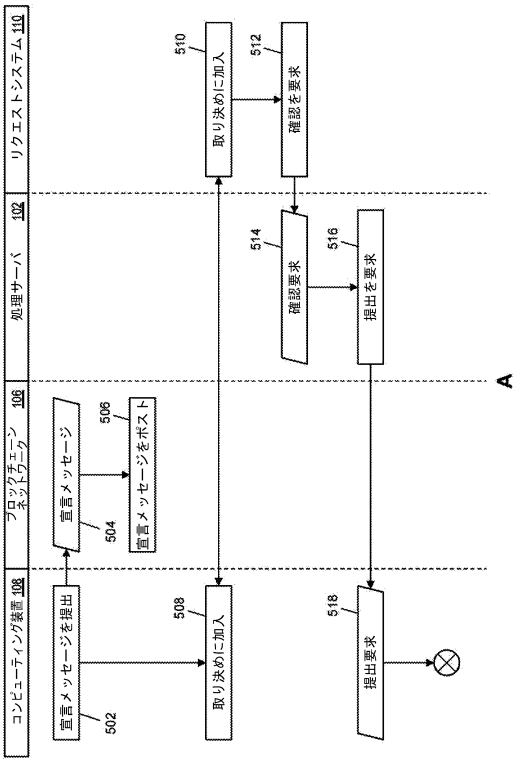
【図３】


308
H(A1 + B3 + 値)
304
VALUE（値）
306b
B4
B3
312b
306a
A2
A1
312a
DECL
（宣言）
CONF
（確認）
302
310

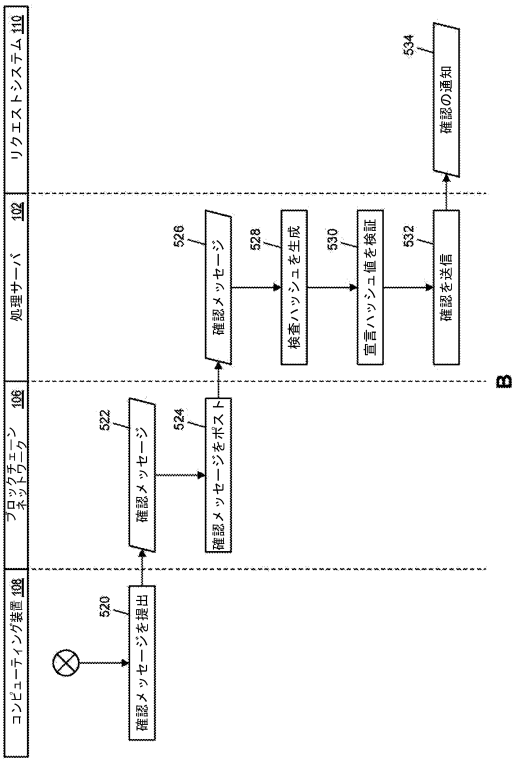
【図４】


412a
412b
H(B1+C2+D3+値1)
H(C1+D2+E3+値2)
C3
D3
408c
406c
B2
C2
406b
408b
A1
B1
406a
408a
値1
値2
410a
410b
ヘッダ
ヘッダ
402
404

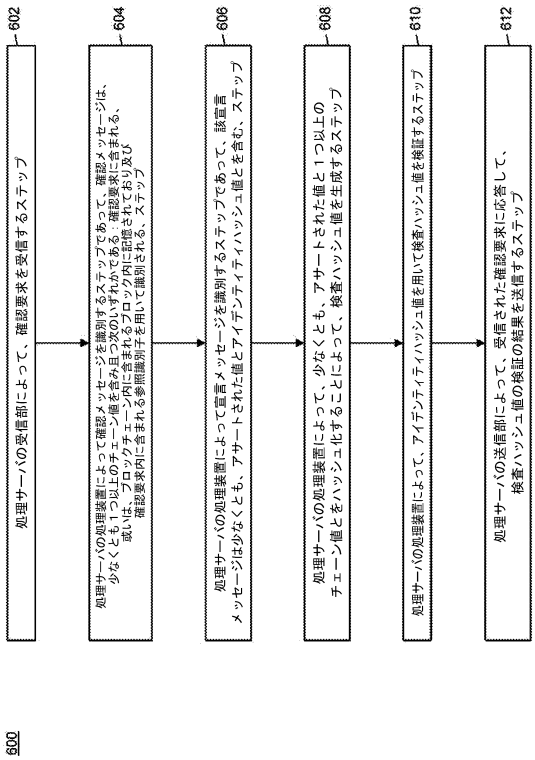
【図５Ａ】


コンピューティング装置 108
ブロックチェーン ネットワーク 106
処理サーバ 102
リクエストシステム 110
宣言メッセージを提出
502
宣言メッセージ
504
宣言メッセージをポスト
506
取り決めに加入
508
確認要求
514
提出を要求
516
提出要求
518
A
取り決めに加入
510
確認を要求
512

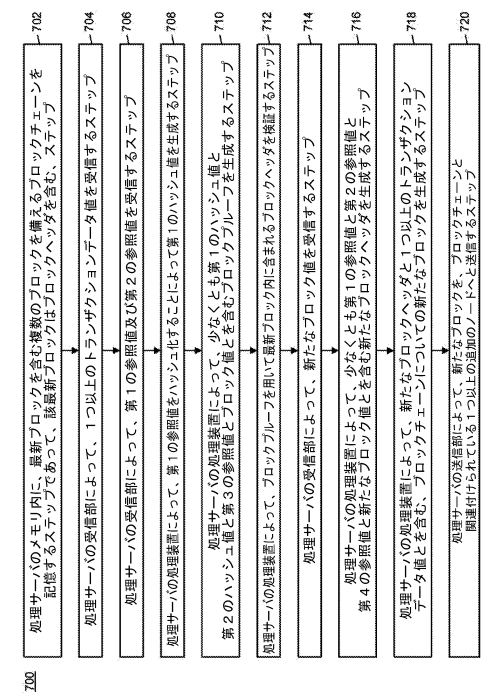
【図５Ｂ】


コンピューティング装置 108
ブロックチェーン ネットワーク 106
処理サーバ 102
リクエストシステム 110
確認要求を提出
520
確認メッセージ
522
確認メッセージをポスト
524
確認メッセージ
526
検査ハッシュを生成
528
宣言ハッシュ値を検証
530
確認を送信
532
B
確認の通知
534

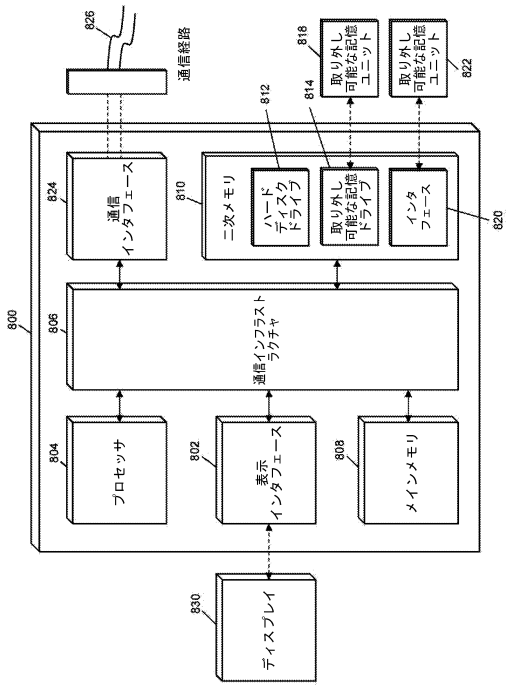
【図６】


600
処理サーバの受信部によって、確認要求を受信するステップ
602
処理サーバの処理装置によって確認メッセージを識別するステップであって、確認メッセージは、少なくとも１つのチェーン値を含み且つ次のいずれかである：確認要求に含まれる、または、ブロックチェーン内に含まれるブロック内に記憶されており及び確認要求内に含まれる参照識別子を用いて識別される、ステップ
604
処理サーバの処理装置によって宣言メッセージを識別するステップであって、該宣言メッセージは少なくとも、アサートされた値とアイデンティティハッシュ値とを含む、ステップ
606
処理サーバの処理装置によって、少なくとも、アサートされた値と１つ以上のチェーン値とをハッシュ化することによって、検査ハッシュ値を生成するステップ
608
処理サーバの処理装置によって、アイデンティティハッシュ値を用いて検査ハッシュ値を検証するステップ
610
処理サーバの送信部によって、受信された確認要求に応答して、検査ハッシュ値の検証の結果を送信するステップ
612

【図７】


700
処理サーバのメモリ内に、最新ブロックを含む複数のブロックを備えるブロックチェーンを記憶するステップであって、該最新ブロックはブロックヘッダを含む、ステップ
702
処理サーバの受信部によって、１つ以上のトランザクションデータ値を受信するステップ
704
処理サーバの受信部によって、第１の参照値及び第２の参照値を受信するステップ
706
処理サーバの処理装置によって、第１の参照値をハッシュ化することによって第１のハッシュ値を生成するステップ
708
処理サーバの処理装置によって、少なくとも第１のハッシュ値と第２のハッシュ値と第３の参照値とブロック値とを含むブロックブルーフを生成するステップ
710
処理サーバの処理装置によって、ブロックブルーフを用いて最新ブロック内に含まれるブロックヘッダを検証するステップ
712
処理サーバの受信部によって、新たなブロック値を受信するステップ
714
処理サーバの処理装置によって、少なくとも第１の参照値と第２の参照値と第４の参照値と新たなブロック値とを含む新たなブロックヘッダを生成するステップ
716
処理サーバの処理装置によって、新たなブロックヘッダと１つ以上のトランザクションデータ値とを含む、ブロックチェーンについての新たなブロックを生成するステップ
718
処理サーバの送信部によって、新たなブロックを、ブロックチェーンと関連付けられている１つ以上の追加のノードへと送信するステップ
720

【図８】


826
通信経路
818
取り外し可能な記憶ユニット
822
取り外し可能な記憶ユニット
812
814
824
通信インタフェース
810
二次メモリ
ハードディスクドライブ
取り外し可能な記憶ドライブ
インタフェース
820
800
806
通信インフラストラクチャ
804
プロセッサ
802
表示インタフェース
808
メインメモリ
830
ディスプレイ

フロントページの続き

１２８
(72)発明者　ポール テイラー
アイルランド国 １６ ダブリン ダンドラム パイン コプス ロード ２９
(72)発明者　エデュアルド フィリペ フェレイラ アンドレイド
アイルランド国 エイ６７ エックスピー０２ ウィックロー ブリタス ベイ コーナゴワー ウェスト バンガロー
審査官　青木 重徳

(56)参考文献　特開２０２０－１７８２４０（ＪＰ，Ａ）
米国特許出願公開第２０１７／０３４４９８７（ＵＳ，Ａ１）
米国特許出願公開第２０２０／０１５３６３０（ＵＳ，Ａ１）
米国特許出願公開第２０２０／００９７９２７（ＵＳ，Ａ１）
国際公開第２０１９／１９４２６７（ＷＯ，Ａ１）
高橋 康 ほか，量子計算機がブロックチェーンの安全性へ及ぼす影響とその対策，２０２１年 暗号と情報セキュリティシンポジウム予稿集 ［ｏｎｌｉｎｅ］，日本，2021年01月19日，2E3-2，pp.1-6

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｇ０９Ｃ　１／００