(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6806924号
(P6806924)
(45)発行日　令和3年1月6日(2021.1.6)　(24)登録日　令和2年12月8日(2020.12.8)

(51)Int.Cl.　F I
G06Q 20/38 (2012.01)　G06Q 20/38　３１０
G06Q 20/40 (2012.01)　G06Q 20/40

請求項の数 16　(全 20 頁)

(21)出願番号　特願2019-552922(P2019-552922)
(86)(22)出願日　平成31年3月4日(2019.3.4)
(65)公表番号　特表2020-526804(P2020-526804A)
(43)公表日　令和2年8月31日(2020.8.31)
(86)国際出願番号　PCT/CN2019/076866
(87)国際公開番号　WO2019/101231
(87)国際公開日　令和1年5月31日(2019.5.31)
審査請求日　令和2年1月27日(2020.1.27)

早期審査対象出願

(73)特許権者　511050697
アリババ　グループ　ホウルディング　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ジョージ　タウン　ピーオーボックス　８４７　ワン　キャピタル　プレイス　フォース　フロア
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(74)代理人　100117189
弁理士　江口　昭彦
(74)代理人　100134120
弁理士　内藤　和彦

最終頁に続く

(54)【発明の名称】ブロックチェーンシステムにおいて証明書を処理するための方法及び装置

(57)【特許請求の範囲】
【請求項１】
ブロックチェーンシステムにおいて証明書を処理するためのコンピュータ実行方法であって、
前記ブロックチェーンシステムにおいてスマートコントラクトを生成させることであって、前記スマートコントラクトが、証明書を処理するためのコンピュータ可読命令を含むことと、
前記スマートコントラクトが生成された後で、第１の取引用の第１の要求を前記ブロックチェーンシステムに送信することであって、前記第１の取引が、前記第１の要求に基づいて証明書明細を生成するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させることと、
前記証明書明細を前記ブロックチェーンシステムから受信することと、
複数の第２の取引用の第２の要求を前記ブロックチェーンシステムに送信することであって、前記複数の第２の取引が、複数の証明書を生成するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させ、前記複数の証明書が、クーポン、チケット、又はバウチャーの少なくとも１つを含むことと、
第３の取引用の第３の要求を前記ブロックチェーンシステムに送信することであって、前記第３の取引が、前記複数の証明書のうちの対象証明書を消去するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させることと、
前記対象証明書が消去されたことを示す結果を前記ブロックチェーンシステムから受信

することと、
を含む方法。
【請求項２】
前記証明書明細に基づいて、前記複数の第２の取引用の前記第２の要求を生成することを更に含む、請求項１に記載の方法。
【請求項３】
前記証明書明細が、証明書タイプ、各証明書タイプの証明書の数、前記証明書の総数、又は各証明書の有効期間の少なくとも１つを示す、請求項１に記載の方法。
【請求項４】
前記複数の証明書が前記証明書明細を満たすかどうかを判定するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させることと、
前記複数の証明書が前記証明書明細を満たすと判定された後で、前記複数の証明書が成功裏に生成されたことを示すメッセージを受信することと、
を更に含む、請求項３に記載の方法。
【請求項５】
前記複数の証明書をユーザに配送することを更に含む、請求項１に記載の方法。
【請求項６】
複数の第３の取引用の複数の第３の要求を前記ブロックチェーンシステムに非同期的に送信することであって、前記複数の第３の取引のそれぞれが、前記複数の証明書のうちの対応する対象証明書を消去するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させることを更に含む、請求項１に記載の方法。
【請求項７】
前記証明書明細が、前記第１の取引の実行を表すハッシュ値を含み、前記複数の証明書のそれぞれが、対応する第２の取引の実行を表すハッシュ値を含む、請求項１に記載の方法。
【請求項８】
前記ブロックチェーンシステムが、コンソーシアムブロックチェーンを実現する、請求項１に記載の方法。
【請求項９】
ブロックチェーンシステムにおいて証明書を処理するための装置であって、
１つ又は複数のプロセッサと、
前記１つ又は複数のプロセッサに結合され、前記１つ又は複数のプロセッサによって実行可能な命令を記憶した１つ又は複数のコンピュータ可読メモリと、
を含み、前記１つ又は複数のプロセッサが、
前記ブロックチェーンシステムにおいてスマートコントラクトを生成させることであって、前記スマートコントラクトが、証明書を処理するためのコンピュータ可読命令を含むことと、
前記スマートコントラクトが生成された後で、第１の取引用の第１の要求を前記ブロックチェーンシステムに送信することであって、前記第１の取引が、前記第１の要求に基づいて証明書明細を生成するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させることと、
前記証明書明細を前記ブロックチェーンシステムから受信することと、
複数の第２の取引用の第２の要求を前記ブロックチェーンシステムに送信することであって、前記複数の第２の取引が、複数の証明書を生成するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させ、前記複数の証明書が、クーポン、チケット、又はバウチャーの少なくとも１つを含むことと、
第３の取引用の第３の要求を前記ブロックチェーンシステムに送信することであって、前記第３の取引が、前記複数の証明書のうちの対象証明書を消去するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させることと、
前記対象証明書が消去されたことを示す結果を前記ブロックチェーンシステムから受信

することと、
を行うように構成される、装置。
【請求項１０】
装置のプロセッサによって実行された場合に、ブロックチェーンシステムにおいて証明書を処理するための方法を前記装置に実行させる命令を記憶した非一時的なコンピュータ可読媒体であって、前記方法が、
前記ブロックチェーンシステムにおいてスマートコントラクトを生成させることであって、前記スマートコントラクトが、証明書を処理するためのコンピュータ可読命令を含むことと、
前記スマートコントラクトが生成された後で、第１の取引用の第１の要求を前記ブロックチェーンシステムに送信することであって、前記第１の取引が、前記第１の要求に基づいて証明書明細を生成するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させることと、
前記証明書明細を前記ブロックチェーンシステムから受信することと、
複数の第２の取引用の第２の要求を前記ブロックチェーンシステムに送信することであって、前記複数の第２の取引が、複数の証明書を生成するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させ、前記複数の証明書が、クーポン、チケット、又はバウチャーの少なくとも１つを含むことと、
第３の取引用の第３の要求を前記ブロックチェーンシステムに送信することであって、前記第３の取引が、前記複数の証明書のうちの対象証明書を消去するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させることと、
前記対象証明書が消去されたことを示す結果を前記ブロックチェーンシステムから受信することと、
を含む、非一時的なコンピュータ可読媒体。
【請求項１１】
前記１つ又は複数のプロセッサが、前記証明書明細に基づいて、前記複数の第２の取引用の前記第２の要求を生成することを行うように更に構成される、請求項９に記載の装置。
【請求項１２】
前記証明書明細が、証明書タイプ、各証明書タイプの証明書の数、前記証明書の総数、又は各証明書の有効期間の少なくとも１つを示す、請求項９に記載の装置。
【請求項１３】
前記１つ又は複数のプロセッサが、
前記複数の証明書が前記証明書明細を満たすかどうかを判定するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させることと、
前記複数の証明書が前記証明書明細を満たすと判定された後で、前記複数の証明書が成功裏に生成されたことを示すメッセージを受信することと、
を行うように更に構成される、請求項１２に記載の装置。
【請求項１４】
前記１つ又は複数のプロセッサが、前記複数の証明書をユーザに配送することを行うように更に構成される、請求項９に記載の装置。
【請求項１５】
前記１つ又は複数のプロセッサが、
複数の第３の取引用の複数の第３の要求を前記ブロックチェーンシステムに非同期的に送信することであって、前記複数の第３の取引のそれぞれが、前記複数の証明書のうちの対応する対象証明書を消去するために、前記ブロックチェーンシステムに前記スマートコントラクトを実行させることを行うように更に構成される、請求項９に記載の装置。
【請求項１６】
前記証明書明細が、前記第１の取引の実行を表すハッシュ値を含み、前記複数の証明書のそれぞれが、対応する第２の取引の実行を表すハッシュ値を含む、請求項９に記載の装

置。

【発明の詳細な説明】
【技術分野】
【０００１】
技術分野
[0001] 本明細書は、一般にコンピュータ技術に関し、特にブロックチェーンシステムにおいて証明書（certificate）を処理するための方法及び装置に関する。
【背景技術】
【０００２】
背景
[0002] 分散台帳システム（ＤＬＳ）又はコンセンサスシステムとしても知られているブロックチェーンシステムは、参加エンティティが、データを安全且つ不変に記憶できるようにし得る。ブロックチェーンシステムは、どんな特定の使用事例も参照せずに、任意のＤＬＳを含んでもよく、且つパブリック、プライベート、及びコンソーシアムブロックチェーンネットワーク用に使用されてもよい。パブリックブロックチェーンネットワークは、システムを使用する、且つコンセンサスプロセスに参加する全てのエンティティ用に公開されている。プライベートブロックチェーンネットワークは、特定のエンティティ用に提供され、特定のエンティティは、読み出し及び書き込み許可を中央で制御する。コンソーシアムブロックチェーンネットワークは、エンティティの選抜グループ用に提供され、選抜グループは、コンセンサスプロセスを制御し、且つアクセス制御層を含む。
【０００３】
[0003] ブロックチェーンシステムは、１つ又は複数のブロックチェーンを維持する。ブロックチェーンは、悪意のある者たちによるデータの改竄及び操作を防ぎ得る、取引などのデータを記憶するためのデータ構造である。
【０００４】
[0004] 透明性の要件ゆえに、証明書（例えばクーポン、チケットなど）の処理は、ブロックチェーンシステムにおいて実行されてもよい。従来的に、証明書は、ブロックチェーンシステムで実行されるスマートコントラクトの契約アカウントに基づいて作成される。例えば、証明書が、作成されるか、配送されるか、又は消去される場合に、それに応じて、スマートコントラクトのアカウントは、アカウントの正確さ及びバランスを維持するために、更新される必要がある。しかしながら、１つの証明書用のアカウントの更新は、数秒から数分かかる可能性がある。従って、システムの繁忙期中に、従来方式で多数の証明書を処理することは、ブロックチェーンシステムの性能に影響を与える可能性がある。
【発明の概要】
【課題を解決するための手段】
【０００５】
概要
[0005] 一態様において、ブロックチェーンシステムにおいて証明書を処理するためのコンピュータ実行方法は、ブロックチェーンシステムにおいてスマートコントラクトを生成させることであって、スマートコントラクトが、証明書を処理するためのコンピュータ可読命令を含むことと、スマートコントラクトが生成された後で、第１の取引用の第１の要求をブロックチェーンシステムに送信することであって、第１の取引が、第１の要求に基づいて証明書明細を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させることと、証明書明細をブロックチェーンシステムから受信することと、複数の第２の取引用の第２の要求をブロックチェーンシステムに送信することであって、複数の第２の取引が、複数の証明書を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させることと、を含む。
【０００６】
[0006] 別の態様において、ブロックチェーンシステムにおいて証明書を処理するため

の装置は、１つ又は複数のプロセッサと、１つ又は複数のプロセッサに結合された１つ又は複数のコンピュータ可読メモリであって、ブロックチェーンシステムにおいてスマートコントラクトを生成させ、スマートコントラクトが、証明書を処理するためのコンピュータ可読命令を含むように、スマートコントラクトが生成された後で、第１の取引用の第１の要求をブロックチェーンシステムに送信し、第１の取引が、第１の要求に基づいて証明書明細を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させるように、証明書明細をブロックチェーンシステムから受信するように、且つ複数の第２の取引用の第２の要求をブロックチェーンシステムに送信し、複数の第２の取引が、複数の証明書を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させるように、１つ又は複数のプロセッサによって実行可能な命令を記憶した１つ又は複数のコンピュータ可読メモリと、を含む。

【０００７】

[0007] 更に別の態様において、非一時的なコンピュータ可読媒体は、装置のプロセッサによって実行された場合に、ブロックチェーンにおいて証明書を処理するための方法を装置に実行させる命令を記憶している。方法は、ブロックチェーンシステムにおいてスマートコントラクトを生成させることであって、スマートコントラクトが、証明書を処理するためのコンピュータ可読命令を含むことと、スマートコントラクトが生成された後で、第１の取引用の第１の要求をブロックチェーンシステムに送信することであって、第１の取引が、第１の要求に基づいて証明書明細を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させることと、証明書明細をブロックチェーンシステムから受信することと、複数の第２の取引用の第２の要求をブロックチェーンシステムに送信することであって、複数の第２の取引が、複数の証明書を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させることと、を含む。

【０００８】

[0008] 本明細書に組み込まれ、且つその一部を構成する添付の図面は、実施形態を示す。図面を参照する以下の説明において、相異なる図面における同じ番号は、別段の表現がない限り、同じ又は同様の要素を表す。

【図面の簡単な説明】

【０００９】

図面の簡単な説明

【図１】[0009]実施形態によるブロックチェーンシステムの概略図である。

【図２】[0010]実施形態による、ブロックチェーンシステムにおいてノードを実現するためのコンピューティング装置の概略図である。

【図３】[0011]実施形態による、ブロックチェーンシステムにおいて証明書を処理するための方法の流れ図である。

【図４】[0012]実施形態による、ブロックチェーンシステムにおいて証明書を処理するための方法の流れ図である。

【図５】[0013]実施形態による、ブロックチェーンシステムにおいて証明書を処理するためのコンピュータ実行方法の流れ図である。

【図６】[0014]実施形態による、ブロックチェーンシステムにおいて証明書を処理するコンピュータ実行方法の流れ図である。

【図７】[0015]実施形態による、ブロックチェーンシステムにおいて証明書を処理するための機器のブロック図である。

【発明を実施するための形態】

【００１０】

詳細な説明

[0016] 本明細書の実施形態は、ブロックチェーンシステムにおいて証明書を処理するための方法及び装置を提供する。方法及び装置は、ブロックチェーンシステムにおいてスマートコントラクトを生成させてもよい。スマートコントラクトは、証明書を処理するためのコンピュータ可読命令を含む。スマートコントラクトが生成された後で、方法及び装

置は、第１の取引用の第１の要求をブロックチェーンシステムに送信してもよく、第１の取引は、第１の要求に基づいて証明書明細を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させる。方法及び装置は、ブロックチェーンシステムから証明書明細を受信してもよい。方法及び装置は、複数の第２の取引の第２の要求をブロックチェーンシステムに更に送信してもよい。複数の第２の取引は、複数の証明書を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させる。

【００１１】

[0017] 本明細書において開示される実施形態は、１つ又は複数の技術的効果を有する。幾つかの実施形態において、方法及び装置は、証明書明細を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させる。これは、証明書明細が、ブロックチェーンシステム上で公にアクセス可能であるようにすることができ、取引活動の透明性を保証する。幾つかの実施形態において、方法及び装置は、更に、証明書明細に基づいた証明書を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させる。これは、証明書明細において指定された情報を備えた正確な証明書の生成を可能にし、それによって、システム性能を改善し、且つブロックチェーンシステムにおいて契約アカウントを実行するコンピューティングコストを低減する。他の実施形態において、方法及び装置は、証明書を用いるための要求を受信する前に複数の証明書を生成するために、ブロックチェーンシステムに複数の第２の取引を実行させる。これは、証明書の生成を証明書の配送及び消去から分離できるようにし、その結果、ブロックチェーンの性能に対する証明書の処理の影響が低減される。ブロックチェーンシステム上の証明書の生成はまた、取引活動の追加の透明性を提供する。例えばブロックチェーンシステムのノードは、証明書明細に基づいて証明書を検証してもよい。

【００１２】

[0018] 以下の説明は、実施形態の詳細を提供する。実施形態において、ブロックチェーンは、取引が不変であり、且つ、後に検証され得る方法で、データ、例えば取引を記憶するデータ構造である。ブロックチェーンは、１つ又は複数のブロックを含む。各ブロックは、前のブロックの暗号ハッシュを含むことによって、ブロックチェーンにおいて、各ブロックの直前のブロックにリンクされる。各ブロックはまた、タイムスタンプ、それ自体の暗号ハッシュ、及び１つ又は複数の取引を含んでもよい。取引は、一般に、ブロックチェーンシステムのノードによって既に検証されているが、マークルツリーなどのデータ構造にハッシュされコード化されてもよい。マークルツリーにおいて、ツリーのリーフノードにおけるデータは、ハッシュされ、ツリーの各ブランチにおける全てのハッシュは、ブランチのルートにおいて連結されてもよい。このプロセスは、ツリー全体のルートまでツリーの上方へ継続し、ツリー全体は、ツリーにおける全てのデータを表すハッシュを記憶する。ツリーに記憶された取引であることを意味するハッシュは、それが、ツリーの構造と一致しているかどうかを判定することによって、素早く検証することができる。

【００１３】

[0019] ブロックチェーンシステムは、１つ又は複数のブロックチェーンを管理し、更新し、且つ維持するコンピューティングノードのネットワークを含む。そのネットワークは、パブリックブロックチェーンネットワーク、プライベートブロックチェーンネットワーク、又はコンソーシアムブロックチェーンネットワークであってもよい。例えば、数百、数千、又は数百万ものエンティティなどの非常に多数のエンティティが、パブリックブロックチェーンネットワークにおいて動作することが可能であり、エンティティのそれぞれは、パブリックブロックチェーンネットワークにおける少なくとも１つのノードを操作する。従って、パブリックブロックチェーンネットワークは、参加するエンティティに関してはパブリックネットワークと見なすことができる。時には、エンティティ（ノード）の大多数は、ブロックが有効にされ、且つブロックチェーンネットワークのブロックチェーンに追加されるために、全てのブロックに署名しなければならない。パブリックブロックチェーンネットワークの例には、ブロックチェーンと呼ばれる分散台帳を活用する特定のピアツーピア決済ネットワークを含む。

【００１４】
[0020] 一般に、パブリックブロックチェーンネットワークは、公開取引を支援し得る。公開取引は、パブリックブロックチェーンネットワークにおける全てのノードと共有され、且つグローバルブロックチェーンに記憶される。グローバルブロックチェーンは、全てのノードにわたって複写されるブロックチェーンであり、全てのノードは、グローバルブロックチェーンに対して合意している。コンセンサス（例えばブロックチェーンへのブロックの追加に対する同意）を達成するために、コンセンサスプロトコルが、パブリックブロックチェーンネットワークにおいて実行される。コンセンサスプロトコルの例には、プルーフオブワーク（ＰＯＷ）（例えば幾つかの暗号通貨ネットワークにおいて実行される）、プルーフオブステーク（ＰＯＳ）、及びプルーフオブオーソリティ（ＰＯＡ）を含む。

【００１５】
[0021] 一般に、プライベートブロックチェーンネットワークは、特定のエンティティ用に提供されてもよく、プライベートブロックチェーンネットワークは、読み出し及び書き込み許可を中央で制御する。エンティティは、どのノードが、ブロックチェーンネットワークに参加できるかを制御する。結果として、プライベートブロックチェーンネットワークは、一般に、誰がネットワークに参加できるか、及びその参加レベル（例えば一定の取引においてのみ）に対して制限をする許可制ネットワークと呼ばれる。様々なタイプのアクセス制御機構を用いることができる（例えば既存の参加者は、新しいエンティティの追加について投票し、規制機関は、承認を制御することができる）。

【００１６】
[0022] 一般に、コンソーシアムブロックチェーンネットワークは、参加するエンティティ間でプライベートであってもよい。コンソーシアムブロックチェーンネットワークにおいて、コンセンサスプロセスは、認定されたノードセットによって制御され、１つ又は複数のノードは、それぞれのエンティティ（例えば金融機関、保険会社）によって操作される。例えば１０個のエンティティ（例えば金融機関、保険会社）のコンソーシアムは、コンソーシアムブロックチェーンネットワークを操作することができ、エンティティのそれぞれは、コンソーシアムブロックチェーンネットワークにおける少なくとも１つのノードを操作する。従って、コンソーシアムブロックチェーンネットワークは、参加するエンティティに関してはプライベートネットワークと見なすことができる。幾つかの例において、各エンティティ（ノード）は、ブロックが有効にされ、且つブロックチェーンに追加されるために、全てのブロックに署名しなければならない。幾つかの例において、エンティティ（ノード）の少なくともサブセット（例えば少なくとも７つのエンティティ）は、ブロックが有効にされ、且つブロックチェーンに追加されるために、全てのブロックに署名しなければならない。

【００１７】
[0023] 図１は、実施形態に従って、ブロックチェーンシステム１００の概略図である。図１を参照すると、ブロックチェーンシステム１００は、ブロックチェーン１２０上で動作するように構成された複数のノード、例えばノード１０２－１１０を含んでもよい。ノード１０２－１１０は、ピアツーピア（Ｐ２Ｐ）ネットワークなどのネットワーク１１２を形成してもよい。ノード１０２－１１０のそれぞれは、ブロックチェーン１２０のコピーを記憶するように構成された、コンピュータ若しくはコンピュータシステムなどのコンピューティング装置であってもよく、又はプロセス若しくはアプリケーションなど、コンピューティング装置上で実行されるソフトウェアであってもよい。ノード１０２－１１０のそれぞれは、一意の識別子を有してもよい。

【００１８】
[0024] ブロックチェーン１２０は、図１におけるブロックＢ１－Ｂ５など、データブロックの形における増え続ける記録リストを含んでもよい。ブロックＢ１－Ｂ５のそれぞれは、タイムスタンプ、前のブロックの暗号ハッシュ、及び現在のブロックのデータを含んでもよく、それらは、金融取引などの取引であってもよい。例えば、図１に示されてい

るように、ブロックＢ５は、タイムスタンプ、ブロックＢ４の暗号ハッシュ、及びブロックＢ５の取引データを含んでもよい。また、例えば、ハッシュ演算は、前のブロックの暗号ハッシュを生成するために、前のブロック上で実行されてもよい。ハッシュ演算は、ＳＨＡ－２５６などのハッシュアルゴリズムを通して、様々な長さの入力を固定長の暗号出力に変換してもよい。

【００１９】

[0025] ノード１０２－１１０は、ブロックチェーン１２０上で操作を実行するように構成されてもよい。例えば、ノード、例えばノード１０２が、ブロックチェーン１２０上に新しいデータを記憶したい場合に、そのノードは、ブロックチェーン１２０に追加される新しいブロックを生成し、且つ新しいブロックをネットワーク１１２における他のノード、例えばノード１０４－１１０にブロードキャストしてもよい。新しいブロックの合法性、例えばその署名及び取引の有効性に基づいて、他のノードは、新しいブロックを受け入れることを決定してもよく、その結果、ノード１０２及び他のノードは、ブロックチェーン１２０のそれらのそれぞれのコピーに新しいブロックを追加してもよい。このプロセスが繰り返されるので、ますます多くのデータブロックが、ブロックチェーン１２０に追加され得る。

【００２０】

[0026] ブロックチェーンシステム１００は、１つ又は複数のスマートコントラクトに従って動作してもよい。各スマートコントラクトは、契約の交渉又は遂行を促進、検証、又は執行するために、ブロックチェーン１２０に組み込まれるコンピュータコードの形のコンピュータプロトコルであってもよい。例えば、ブロックチェーンシステム１００のユーザは、C++、Java（登録商標）（ジャバ）、Solidity（ソリディティ）、Python（パイソン）などのプログラミング言語を用いて、スマートコントラクトに同意条件をプログラムしてもよく、条件が満たされた場合に、スマートコントラクトは、例えば取引を実行するために、ブロックチェーンシステム１００によって自動的に実行されてもよい。また例えばスマートコントラクトは、複数のサブルーチン又は関数を含んでもよく、サブルーチン又は関数のそれぞれは、特定のタスクを実行するプログラム命令のシーケンスであってもよい。スマートコントラクトは、人とのインタラクションなしに完全に又は部分的に実行される操作コードであってもよい。

【００２１】

[0027] ノード１０２－１１０のそれぞれが、ブロックチェーン１２０のコピーを記憶してもよいので、ノード１０２－１１０のそれぞれはまた、ブロックチェーン１２０に含まれるスマートコントラクトのコピーへのアクセスを有してもよい。実施形態において、スマートコントラクトは、例えばスマートコントラクトが操作コードにコンパイルされた後で、ブロックチェーン１２０上のアドレスを割り当てられてもよい。スマートコントラクトのアドレスは、ブロックチェーン１２０上でスマートコントラクトの位置を特定するように構成又は使用される。

【００２２】

[0028] 実施形態において、ブロックチェーンシステム１００におけるノード（例えばノード１０２）は、スマートコントラクトのコピーに基づいて取引を実行してもよい。取引を含む新しいブロックがブロックチェーンシステム１００にブロードキャストされた後で、ブロックチェーンシステム１００における他のノードは、新しいブロックを検証してもよい。新しいブロックがブロックチェーンシステム１００における大多数又は全てのノードによって検証された後で、新しいブロックは、それらのノード上におけるブロックチェーン１２０のそれぞれのコピーに追加されてもよく、取引は完了する。

【００２３】

[0029] 図２は、本明細書の実施形態に従って、ブロックチェーンシステムにおけるノード、例えばノード１０２（図１）を実現するためのコンピューティング装置２００の概略図である。図２を参照すると、コンピューティング装置２００は、通信インターフェース２０２、プロセッサ２０４、及びメモリ２０６を含んでもよい。

【００２４】
[0030] 通信インターフェース２０２は、ネットワークにおいて、コンピューティング装置２００と、他のノード、例えばノード１０４－１１０（図１）を実現する装置との間の通信を容易にし得る。幾つかの実施形態において、通信インターフェース２０２は、インターネット標準又はプロトコル、統合サービスデジタルネットワーク（ＩＳＤＮ）標準などの、１つ又は複数の通信標準をサポートし得る。幾つかの実施形態において、通信インターフェース２０２は、ローカルエリアネットワーク（ＬＡＮ）カード、ケーブルモデム、衛星モデム、データバス、ケーブル、無線通信チャネル、無線ベースの通信チャネル、セルラー通信チャネル、インターネットプロトコル（ＩＰ）ベースの通信装置、又は有線及び／若しくは無線通信用の他の通信装置における、１つ又は複数を含んでもよい。幾つかの実施形態において、通信インターフェース２０２は、パブリック・クラウド・インフラストラクチャ、プライベート・クラウド・インフラストラクチャ、ハイブリッド・パブリック／プライベート・クラウド・インフラストラクチャに基づいてもよい。
【００２５】
[0031] プロセッサ２０４は、１つ又は複数の専用処理ユニット、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、又は様々な他のタイプのプロセッサ若しくは処理ユニットを含んでもよい。プロセッサ２０４は、メモリ２０６と結合され、且つメモリ２０６に記憶された命令を実行する。
【００２６】
[0032] メモリ２０６は、ブロックチェーン１２０（図１）のコピーなど、プロセッサ実行命令及びデータを記憶してもよい。メモリ２０６は、スタティックランダムアクセスメモリ（ＳＲＡＭ）、電気的消去可能プログラマブル読み出し専用メモリ（ＥＥＰＲＯＭ）、消去可能プログラマブル読み出し専用メモリ（ＥＰＲＯＭ）、プログラマブル読み出し専用メモリ（ＰＲＯＭ）、読み出し専用メモリ（ＲＯＭ）、磁気メモリ、フラッシュメモリ、又は磁気若しくは光ディスクなど、任意のタイプの揮発性若しくは不揮発性メモリ装置、又はそれらの組み合わせを含んでもよい。メモリ２０６における命令が、プロセッサ２０４によって実行される場合に、コンピューティング装置２００は、ブロックチェーン１２０上で操作を実行してもよい。
【００２７】
[0033] 図１を参照すると、ブロックチェーンシステム１００は、販売促進活動、マーケティング活動など、公開データ及び透明性のある条項を含む取引活動において用いられてもよい。例えば商人は、かかる製品を購入しなかった顧客に、クーポンなどの証明書を発行してもよい。ブロックチェーンシステム１００を用いることによって、クーポンの発行は、スマートコントラクトを用いて執行されてもよい。例えば顧客が、スマートコントラクトにおいて指定された条項（例えば「消費者は、この製品を購入しなかった」）を満たす場合に、対応するイベントが行われるようにされてもよい（例えば「その消費者クーポンを発行する」）。スマートコントラクトの使用は、契約条項及び条件を透明にし得る。何故なら、スマートコントラクトが、ブロックチェーンに記憶され、ユーザに開放されているからである。
【００２８】
[0034] 証明書は、クーポン、チケット、バウチャーなどを含んでもよい。例えばクーポンは、販売促進活動において用いられ、オンラインプラットホームのユーザに割引を提供してもよい。また例えば、チケットは、イベント（例えばコンサート）又は興味のある場所（例えば観光地、博物館など）において用いられ、イベント又は興味のある場所へのアクセスを提供してもよい。別の例として、休日に、興味対象の場所は、訪問者の往来を管理するために、限られた数のチケットを提供してもよい。これらの例において、証明書は、ユーザの間で人気になり得、証明書を処理するための透明性を更に要求してもよい。ブロックチェーンシステムが、悪意のある者たちによる記憶データの改竄及び操作を防ぎ得、且つブロックチェーンシステムの各ノードが、コピーを含んでもよいので、ブロックチェーンシステムにおける証明書の処理は、信頼できるように且つ検証可能にすることが

できる。

【００２９】

[0035] 実施形態において、図１における装置１３０は、ブロックチェーンシステム１００とインタラクションするために、ユーザ、例えば商人によって用いられてもよい。装置１３０は、コンピューティング装置２００（図２）に似たコンピューティング装置であってもよく、それは、通信インターフェース、プロセッサ、及びメモリを含んでもよい。幾つかの実施形態において、装置１３０は、ブロックチェーンシステム１００のノードとして動作する。他の実施形態において、装置１３０は、ノードとして動作せず、ブロックチェーンシステム１００の１つ又は複数のノード、例えばノード１０２－１１０で確立された接続を通して、ブロックチェーンシステム１００とインタラクションしてもよい。接続は、１つ又は複数のアプリケーションプログラミングインターフェース（ＡＰＩ）を通して確立されてもよい。ソフト開発キット（ＳＤＫ）もまた、かかる接続の確立を容易にするために提供されてもよい。

【００３０】

[0036] 図３は、実施形態１による、ブロックチェーンシステム１００（図１）などのブロックチェーンシステムにおいて証明書を処理するための方法３００の流れ図である。例えば方法３００は、証明書を生成するために用いられる。また例えば、方法３００は、装置１３０（図１）の１つ又は複数のプロセッサによって実行されてもよく、１つ又は複数のプロセッサは、ユーザインターフェースシステム及び活動管理システムを実現してもよい。ユーザインターフェースシステムは、データを入力及び出力するために、ユーザ、例えば商人とインタラクションし、且つ証明書を生成するための要求を活動管理システムに送信してもよい。活動管理システムは、実行用にブロックチェーンシステム１００への命令又は要求を生成してもよい。幾つかの実施形態において、ブロックチェーンシステムは、コンソーシアムブロックチェーンを実現してもよい。

【００３１】

[0037] 図３を参照すると、ステップ３０２において、活動管理システムは、スマートコントラクトを生成するための要求をブロックチェーンシステムに送信してもよい。幾つかの実施形態において、スマートコントラクトは、ユーザによって（例えばユーザ生成プログラムコードをブロックチェーンに提示することによって）提供されるか、又はブロックチェーンサービスプロバイダによって提供されるテンプレートスマートコントラクトからユーザによって選択及び構成されてもよい。例えばユーザは、メニューからスマートコントラクトを選択し、且つカスタマイズされたパラメータを提供してもよい。スマートコントラクトは、ユーザによって設定された取引活動の戦略及び規則を表してもよい。例えばクーポンに基づいた販売促進活動において、規則は、顧客ごとに受信されるクーポンの許可される合計値、顧客ごとに受信されるクーポンの許可される総数、クーポンの額面金額、クーポンのタイプ、指定の地理的地域における対象顧客のパーセンテージ、顧客がクーポンを受け取るための方法、顧客がクーポンを用いるための条件及び制約などに対する制限を含んでもよい。

【００３２】

[0038] それに応じて、ステップ３０４において、ブロックチェーンシステム１００は、スマートコントラクトを生成し、且つ生成されたスマートコントラクトのアドレスを返してもよい。スマートコントラクトのアドレスは、複数の数字（例えば１６０の２進数字）を含んでもよい。幾つかの実施形態において、スマートコントラクトのアドレスは、アドレスに対応するハッシュ値を用いて、記憶され伝送されてもよい。取引が、スマートコントラクトのアドレスに送信される場合に、取引は、スマートコントラクトの対応する機能によって実行されてもよい。スマートコントラクトは、証明書明細生成機能、証明書生成機能、証明書検証機能、又は消去機能などの複数の機能を含んでもよい。生成されたスマートコントラクトが、相異なる要求に従って、クーポンの発行、チケットの発行などの相異なる取引活動用に使用されてもよいことが分かる。

【００３３】

[0039] ステップ３０６において、活動管理システムは、証明書を生成するための要求をユーザインターフェースシステムから受信してもよい。例えば、ユーザインターフェースシステムは、ユーザ入力に基づいて要求を生成してもよい。証明書を生成するための要求は、生成される証明書に関する情報を含んでもよい。幾つかの実施形態において、証明書に関する情報は、証明書タイプ、各証明書タイプの証明書の数、証明書の総数、又は各証明書の有効期間の少なくとも１つを含んでもよい。例えば、クーポンを生成するための要求は、３ドルの割引用の１，０００個のクーポン及び５ドルの割引用の５００個のクーポンを生成すること、及びこれらのクーポンが３日間有効であることを要求してもよい。

【００３４】

[0040] ユーザインターフェースシステムから受信された、証明書を生成するための要求に基づいて、活動管理システムは、第１の取引用の第１の要求を生成してもよく、第１の取引は、第１の要求に基づいて証明書明細を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させるために用いられる。ステップ３０８において、活動管理システムは、第１の取引用の第１の要求をブロックチェーンシステム１００に更に送信してもよい。例えば第１の取引用の第１の要求は、ステップ３０４においてブロックチェーンシステムから受信されたスマートコントラクトのアドレスに送信されてもよい。

【００３５】

[0041] ステップ３１０において、第１の取引用の第１の要求に応じて、ブロックチェーンシステム１００は、証明書を生成するための要求からの情報に基づいて証明書明細を生成するために、スマートコントラクトを実行する。例えば、ブロックチェーンシステム１００は、第１の取引を実行するために、スマートコントラクトの証明書明細生成機能を実行する。第１の取引の実行の結果として、証明書明細は、例えばハッシュ値として生成され記憶されてもよい。生成された証明書明細は、生成される証明書の証明書タイプ、各証明書タイプの証明書の数、証明書の総数、又は各証明書の有効期間の少なくとも１つを含んでもよい。証明書明細は、取引の実行の結果として、ブロックチェーン上に記録され、且つブロックチェーンシステム１００のノードによってアクセス可能であってもよい。従って、証明書明細は、取引活動の透明性を保証するために、ブロックチェーン上で公開される。

【００３６】

[0042] ステップ３１２において、活動管理システムは、ブロックチェーンシステム１００から証明書明細を受信してもよい。ステップ３１４において、活動管理システムは、証明書明細に基づいて証明書を生成するための第２の要求を生成してもよい。例えば証明書明細は、３ドルの割引用の１，０００個のクーポン及び５ドルの割引用の５００個のクーポンを指定してもよく、それに応じて、活動管理システムは、証明書明細に基づいて、３ドルの割引用の１，０００個のクーポン及び５ドルの割引用の５００個のクーポンを生成するための第２の要求を生成してもよい。第２の要求は、証明書に対応する複数の第２の取引を含んでもよい。幾つかの実施形態において、複数の第２の取引のそれぞれは、１つの証明書に対応する。例えば、第２の取引は、３ドルの割引用のクーポンを生成することに向けられもよく、別の第２の取引は、５ドルの割引用のクーポンを生成することに向けられもよい。１つの第２の取引がまた、多数の証明書を生成することに向けられもよいことが分かる。

【００３７】

[0043] ステップ３１６において、活動管理システムは、第２の取引用の第２の要求をブロックチェーンシステム１００に送信してもよい。例えば、第２の取引は、スマートコントラクトのアドレスに送信されてもよい。

【００３８】

[0044] ステップ３１８において、第２の取引用の第２の要求に応じて、ブロックチェーンシステム１００は、第２の取引に対応する証明書を生成するために、スマートコントラクトを実行してもよい。第２の取引の実行の結果として、証明書は、例えばハッシュ値として生成され記憶されてもよい。生成された証明書のそれぞれは、証明書と関係する情

報を含んでもよい。例えば、証明書がクーポンである場合に、証明書は、クーポンのコード、クーポンのタイプ、クーポンによって提供される割引、クーポンの適用可能なカテゴリ、クーポンの有効期間などを含んでもよい。生成された証明書は、ブロックチェーンシステム１００に記憶されてもよい。

【００３９】

[0045] 幾つかの実施形態において、ステップ３１８で、ブロックチェーンシステム１００はまた、生成された証明書が、証明書明細を満たすかどうかを判定するために、スマートコントラクトの検証機能を実行してもよい。検証機能は、生成された証明書のタイプ及び数を監視し、生成された証明書のタイプ及び数が証明書明細の要件を満たすかどうかを判定してもよい。例えば、証明書明細が、３ドルの割引用の１，０００個のクーポン及び５ドルの割引用の５００個のクーポンを指定した場合に、検証機能は、３ドルの割引用の１，０００個のクーポン及び５ドルの割引用の５００個のクーポンが生成されたと充足判定機能が判定したときに、生成された証明書が証明書明細を満たすと判定してもよい。生成された証明書が証明書明細を満たすという判定に応じて、スマートコントラクトは、証明書の生成を停止する。検証機能がまた、各生成された証明書の有効期間を検証してもよいことが分かる。

【００４０】

[0046] ステップ３２０において、ブロックチェーンシステム１００は、生成された証明書を活動管理システムに送信してもよい。従って、ステップ３２２において、活動管理システムは、証明書の生成の成功を示すメッセージをユーザインターフェースシステムに送信してもよい。

【００４１】

[0047] 図４は、実施形態による、ブロックチェーンシステムにおいて証明書を処理するための方法４００の流れ図である。例えば、方法４００は、ユーザに証明書を配送し、また配送された証明書をブロックチェーンシステム上で消去するために用いられる。また例えば、方法４００は、装置１３０（図１）によって実行されてもよく、装置１３０は、ユーザインターフェースシステム及び活動管理システムを含んでもよい。

【００４２】

[0048] 図４を参照すると、ステップ４０２において、ユーザインターフェースシステムは、ユーザから対象証明書用のユーザ要求を受信してもよい。ユーザ要求は、対象証明書の情報、ユーザの身分証明（ＩＤ）などを含んでもよい。対象証明書の情報は、対象証明書のタイプを含んでもよい。ＩＤは、対象証明書がユーザに配送される場合に、ユーザを識別するために用いられてもよい。ユーザが、インターネットなどの任意のタイプのネットワークを通して対象証明書を要求してもよいことが分かる。

【００４３】

[0049] ステップ４０４において、ユーザインターフェースシステムは、ユーザ要求に基づいて、証明書配送要求を生成し、証明書配送要求を活動管理システムに送信してもよい。証明書を要求するユーザのＩＤは、証明書配送要求と一緒に活動管理システムに送信されてもよい。

【００４４】

[0050] 受信された証明書配送要求に基づいて、ステップ４０６において、活動管理システムは、配送されるべき対象証明書としての証明書を判定してもよい。上記のように、ステップ３２０（図３）において、生成された証明書は、活動管理システムに送信される。従って、活動管理システムは、証明書配送要求に基づいて、受信された証明書のなかで対象証明書を判定してもよい。例えば、活動管理システムは、対象証明書のタイプを判定し、受信された証明書に、判定されたタイプの有効な証明書が含まれるかどうかを判定してもよい。幾つかの実施形態において、活動管理システムは、有効な証明書のリストを有してもよい。有効な証明書のリストに、判定されたタイプの有効な証明書が含まれる場合に、活動管理システムは、ユーザ用の対象証明書として当該有効な証明書を判定してもよい。

【００４５】
[0051] 対象証明書が判定された後で、ステップ４０８において、活動管理システムは、消去取引用の要求をブロックチェーンシステム１００に送信してもよい。例えば、消去は、アカウントからの項目のキャンセル又は削除である。実施形態において、証明書がユーザに配送された場合に、その証明書は、別のユーザによって使用されてはならず、従って消去されてもよい。幾つかの実施形態において、証明書の配送は、証明書が消去される前に検証されてもよい。また例えば、消去取引は、対象証明書が配送される前に、スマートコントラクトのアドレスに送信されてもよい。ブロックチェーンシステム１００が、要求を受信し、且つ対象証明書を消去した場合に、証明書は、別のユーザによって用いられてはならない。幾つかの実施形態において、活動管理システムは、複数の消去取引用の複数の要求をブロックチェーンシステムに非同期的に送信してもよく、複数の消去取引のそれぞれは、複数の証明書における対応する対象証明書を消去するために、ブロックチェーンシステムにスマートコントラクトを実行させてもよい。これは、特定の時刻にブロックチェーンシステムに負荷をかけ過ぎることを回避する。
【００４６】
[0052] ステップ４１０において、消去取引用の要求に応じて、ブロックチェーンシステム１００は、対象証明書を消去するために、スマートコントラクトを実行する。例えば、ブロックチェーンシステム１００は、消去取引を実行するために、スマートコントラクトの消去機能を実行する。例えば、スマートコントラクトの消去機能は、対象証明書が有効かどうかを判定してもよい。対象証明書が消去されることになる場合に、当該対象証明書が有効であることが分かる。ブロックチェーンシステム１００のコンセンサスは、達成までに幾らかの時間、例えば数秒掛かり得るので、対象証明書用の別の要求は、コンセンサスが達成される前に受信され得る。スマートコントラクトの消去機能は、証明書を配送した後で、対象証明書を消去する。従って、消去機能は、証明書が、今、無効であると別の要求に応答してもよく、応答はまた、証明書が配送されるユーザの情報（例えばユーザのＩＤ）を含んでもよい。
【００４７】
[0053] ステップ４１２において、ブロックチェーンシステム１００は、証明書の消去の成功を示すメッセージを活動管理システムに送信してもよい。他方で、消去取引用の要求が受信された場合に、証明書は、配送され得るが、もはや有効ではない。この状況で、ブロックチェーン１００は、消去失敗を示すメッセージを活動管理システムに送信してもよい。活動管理システムは、配送用の別の証明書を要求するために、ステップ４０６を再実行してもよい。
【００４８】
[0054] ステップ４１４において、証明書の消去の成功を示すメッセージを受信すると、活動管理システムは、対象証明書の配送の成功の結果をユーザインターフェースシステムに送信してもよい。
【００４９】
[0055] 方法３００（図３）及び方法４００（図４）において、証明書の配送及び消去は、証明書の生成から分離される。従って、ブロックチェーンシステム１００に対する計算負担は、ある期間にわたって広げることが可能であり、ブロックチェーンシステム１００の性能への影響が低減され得る。
【００５０】
[0056] 図５は、実施形態による、ブロックチェーンシステムにおいて証明書を処理するためのコンピュータ実行方法５００の流れ図である。方法５００は、コンピュータシステムによって実行されてもよい。コンピュータシステムは、命令セットを記憶するメモリと、コンピュータシステムに方法５００を行わせるために当該命令セットを実行する少なくとも１つのプロセッサと、を含んでもよい。例えばコンピュータシステムは、装置１３０（図１）であってもよく、装置１３０は、ユーザインターフェースシステム並びに活動管理システム（図３及び４）を含んでもよい。図５を参照すると、方法５００は、以下

のステップを含んでもよい。

【００５１】

[0057] ステップ５０２において、コンピュータシステムは、ブロックチェーンシステム、例えばブロックチェーンシステム１００（図１）において、スマートコントラクトを生成させてもよい。上記のように、スマートコントラクトは、証明書を処理するためのコンピュータ可読命令を含んでもよい。証明書は、クーポン、チケット、バウチャー等であってもよい。

【００５２】

[0058] ステップ５０４において、コンピュータシステムは、スマートコントラクトが生成された後で、第１の取引用の第１の要求をブロックチェーンシステムに送信してもよい。第１の取引は、実行のためにスマートコントラクトのアドレスに送信されてもよい。例えば、第１の取引は、第１の要求に基づいて証明書明細を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させてもよい。証明書明細は、第１の取引の実行を表すハッシュ値を含んでもよい。証明書明細はまた、証明書タイプ、各証明書タイプの証明書の数、証明書の総数、又は各証明書の有効期間の少なくとも１つを含んでもよい。幾つかの実施形態において、証明書は、クーポン、チケット、バウチャーなどの少なくとも１つを含む。

【００５３】

[0059] ステップ５０６において、コンピュータシステムは、ブロックチェーンシステムから証明書明細を受信してもよい。証明書明細に基づいて、コンピュータシステムは、複数の第２の取引用の第２の要求を生成してもよい。

【００５４】

[0060] ステップ５０８において、コンピュータシステムは、複数の第２の取引用の第２の要求をブロックチェーンシステムに送信してもよい。複数の第２の取引は、スマートコントラクトのアドレスに送信されてもよい。複数の第２の取引は、複数の証明書を生成及び検証するために、ブロックチェーンシステムにスマートコントラクトを実行させる。幾つかの実施形態において、複数の証明書を検証する際に、ブロックチェーンシステムは、複数の証明書が証明書明細を満たすかどうかを判定するために、スマートコントラクトを実行させてもよい。例えば、ブロックチェーンシステムは、生成された証明書が、要求された証明書タイプの証明書かどうか、生成された証明書の数が、当該証明書タイプの要求された数を満たすかどうか、全ての生成された証明書の数が、証明書の要求された総数を満たすかどうか、又は生成された証明書の有効期間が、要求された有効期間を満たすかどうかを判定してもよい。幾つかの実施形態において、証明書明細の全ての条件が満たされる場合に、ブロックチェーンシステムは、複数の証明書が証明書明細を満たすと判定し、複数の証明書が成功裏に生成されたことを示すメッセージをコンピュータシステムに送信する。

【００５５】

[0061] コンピュータシステムはまた、複数の証明書をユーザに配送してもよい。例えばコンピュータシステムは、対象証明書用の要求を受信してもよい。対象証明書用の要求は、ユーザ入力に基づいて生成されてもよい。例えば、コンピュータシステムのユーザインターフェースシステムは、証明書用のユーザ入力の要求を受信し、且つそれに応じて要求を生成してもよい。

【００５６】

[0062] 図６は、実施形態による、ブロックチェーンシステムにおいて証明書を処理するためのコンピュータ実行方法６００の流れ図である。方法６００はまた、図５に関連して説明されたコンピュータシステムによって実行されてもよい。方法６００が、方法５００の一部として又は別個の方法として実行されてもよいことが分かる。図６を参照すると、方法６００は、以下のステップを含んでもよい。

【００５７】

[0063] ステップ６０２において、コンピュータシステムは、第３の取引用の第３の要

求をブロックチェーンシステムに送信してもよい。第３の取引は、ブロックチェーンシステムから受領される複数の証明書における対象証明書が配送される前に、ブロックチェーンシステム上で実行されるスマートコントラクトのアドレスに送信されてもよい。ブロックチェーンシステムは、対象証明書を消去するために、第３の取引によってスマートコントラクトを実行させられてもよい。上記のように、複数の証明書は、クーポン、チケット、バウチャー等であってもよい。幾つかの実施形態において、対象証明書が、対象クーポンである場合に、ブロックチェーンシステムは、対象クーポンを消去するために、スマートコントラクトを実行させられる。幾つかの実施形態において、コンピュータシステムは、複数の第３の取引用の複数の第３の要求をブロックチェーンシステムに非同期に送信してもよく、複数の第３の取引のそれぞれは、複数の証明書の対応する対象証明書を消去するために、ブロックチェーンシステムにスマートコントラクトを実行させる。これは、特定の時刻にブロックチェーンシステムに負荷をかけ過ぎることを回避する。

【００５８】

[0064] 対象証明書が実施されたことを示す結果が、生成され、且つコンピュータシステムに送信されてもよい。従って、ステップ６０４において、コンピュータシステムは、対象証明書が実施されたことを示す結果をブロックチェーンシステムから受信してもよい。

【００５９】

[0065] 図７は、実施形態による、ブロックチェーンシステムにおいて証明書を処理するための機器７００のブロック図である。例えば、機器７００は、装置１３０（図１）を実現してもよい。また例えば、機器７００は、方法５００（図５）及び方法６００（図６）を実行してもよい。図７を参照すると、機器７００は、スマートコントラクト生成モジュール７０２及び証明書生成モジュール７０４を含んでもよい。

【００６０】

[0066] スマートコントラクト生成モジュール７０２は、ブロックチェーンシステムにおいてスマートコントラクトを生成させてもよい。スマートコントラクトは、証明書を処理するためのコンピュータ可読命令を含んでもよい。証明書生成モジュール７０４は、第１の取引用の第１の要求をブロックチェーンシステムに送信し、第１の取引は、第１の要求に基づいて証明書明細を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させてもよい。証明書生成モジュール７０４は、証明書明細をブロックチェーンシステムから受信してもよい。証明書生成モジュール７０４は、複数の第２の取引用の第２の要求をブロックチェーンシステムに更に送信し、複数の第２の取引は、複数の証明書を生成するために、ブロックチェーンシステムにスマートコントラクトを実行させてもよい。

【００６１】

[0067] 幾つかの実施形態において、機器７００はまた、証明書配送モジュール７０６を含んでもよい。証明書配送モジュール７０６は、第３の取引用の第３の要求をブロックチェーンシステムに送信し、第３の取引は、対象証明書が配送される前に、複数の証明書のうちの対象証明書を消去するために、ブロックチェーンシステムにスマートコントラクトを実行させてもよい。証明書配送モジュール７０６は、対象証明書が消去されたことを示す結果を　ブロックチェーンシステムから受信してもよい。

【００６２】

[0068] 上記のモジュールのそれぞれは、ソフトウェア、ハードウェア、又はソフトウェア及びハードウェアの組み合わせとして実現されてもよい。例えば、上記のモジュールのそれぞれは、メモリに記憶された命令を実行するプロセッサを用いて実現されてもよい。また、例えば、上記のモジュールのそれぞれは、上記の方法を実行するための１つ又は複数の特定用途向け集積回路（ＡＳＩＣ）、デジタル信号プロセッサ（ＤＳＰ）、デジタル信号処理装置（ＤＳＰＤ）、プログラマブル論理装置（ＰＬＤ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、コントローラ、マイクロコントローラ、マイクロプロセッサ、又は他の電子コンポーネントで実現されてもよい。更に、例えば、上記のモジュ

ールのそれぞれは、コンピュータチップ若しくはエンティティを用いることによって実現されてもよく、又は或る機能を有する製品を用いることによって実現されてもよい。一実施形態において、機器７００は、コンピュータであってもよく、コンピュータは、パーソナルコンピュータ、ラップトップコンピュータ、携帯電話、カメラ付き携帯電話、スマートフォン、携帯情報端末、メディアプレーヤ、ナビゲーション装置、電子メール受信及び送信装置、ゲーム機、タブレットコンピュータ、ウェアラブル装置、又はこれらの装置の任意の組み合わせであってもよい。

【００６３】

[0069] 機器７００における各モジュールの機能及び役割の実現プロセス用に、上記の方法における対応するステップを参照することができる。詳細は、簡潔にするためにここでは省略される。

【００６４】

[0070] 幾つかの実施形態において、コンピュータプログラムプロダクトは、上記の方法をプロセッサに実行させるためのコンピュータ可読プログラム命令を有する非一時的なコンピュータ可読記憶媒体を含んでもよい。

【００６５】

[0071] コンピュータ可読記憶媒体は、命令実行装置による使用のための命令を記憶できる有形装置であってもよい。コンピュータ可読記憶媒体は、例えば、限定するわけではないが、電子記憶装置、磁気記憶装置、光記憶装置、電磁気記憶装置、半導体記憶装置、又は前述のものの任意の適切な組み合わせであってもよい。コンピュータ可読記憶媒体のより具体的な例の非包括的リストは、次のもの、即ち、ポータブルコンピュータディスケットと、ハードディスクと、ランダムアクセスメモリ（ＲＡＭ）と、読み出し専用メモリ（ＲＯＭ）と、消去可能プログラマブル読み出し専用メモリ（ＥＰＲＯＭ）と、スタティックランダムアクセスメモリ（ＳＲＡＭ）と、ポータブルコンパクトディスク読み出し専用メモリ（ＣＤ－ＲＯＭ）と、デジタル多用途ディスク（ＤＶＤ）と、メモリスティックと、フロッピーディスクと、パンチカードか又は命令を自らに記録した溝における凸構造など、機械的にコード化された装置と、前述のものの任意の適切な組み合わせと、を含む。

【００６６】

[0072] 上記の方法を実行するためのコンピュータ可読プログラム命令は、アセンブラ命令か、命令セットアーキテクチャ（ＩＳＡ）命令か、機械語命令か、機械依存命令か、マイクロコードか、ファームウェア命令か、状態設定データか、又はオブジェクト指向プログラミング言語を含む１つ若しくは複数のプログラミング言語及び従来の手続き型プログラミング言語の任意の組み合わせで書かれたソースコード若しくはオブジェクトコードであってもよい。コンピュータ可読プログラム命令は、スタンドアロンのパッケージソフトとしてコンピューティング装置上で完全に、又は第１のコンピューティング装置上で部分的に且つ第１のコンピューティング装置から遠隔の第２のコンピューティング装置上で部分的に実行されてもよい。後のシナリオにおいて、第２の遠隔コンピューティング装置は、ローカルエリアネットワーク（ＬＡＮ）又はワイドエリアネットワーク（ＷＡＮ）を含む任意のタイプのネットワークを通して、第１のコンピューティング装置に接続されてもよい。

【００６７】

[0073] コンピュータ可読プログラム命令は、機械を作製するために、汎用若しくは専用コンピュータ又は他のプログラマブルデータ処理機器のプロセッサに提供されてもよく、その結果、命令は、コンピュータ又は他のプログラマブルデータ処理機器のプロセッサを介して実行されるが、上記の方法を実行するための手段を生成する。

【００６８】

[0074] 図における流れ図及び図形は、本明細書の様々な実施形態に従って、装置、方法及びコンピュータプログラムプロダクトの可能な実装形態のアーキテクチャ、機能、及び動作を示す。この点において、流れ図又は図形におけるブロックは、ソフトウェアプロ

グラム、セグメント、又はコードの一部を表してもよく、それは、特定の機能を実行するための１つ又は複数の実行可能命令を含む。幾つかの代替実装形態において、ブロックに書かれた機能が、図に書かれた順序から外れて行われてもよいことに留意されたい。例えば連続して示されている２つのブロックは、実際にはほぼ同時に実行されてもよく、又はブロックは、含まれる機能性に依存して、時には逆順に実行されてもよい。図形及び／又は流れ図の各ブロック、並びに図形及び流れ図におけるブロックの組み合わせが、特定の機能若しくは行動を実行する専用ハードウェアベースシステム、又は専用ハードウェア及びコンピュータ命令の組み合わせによって実行されてもよいこともまた注目される。

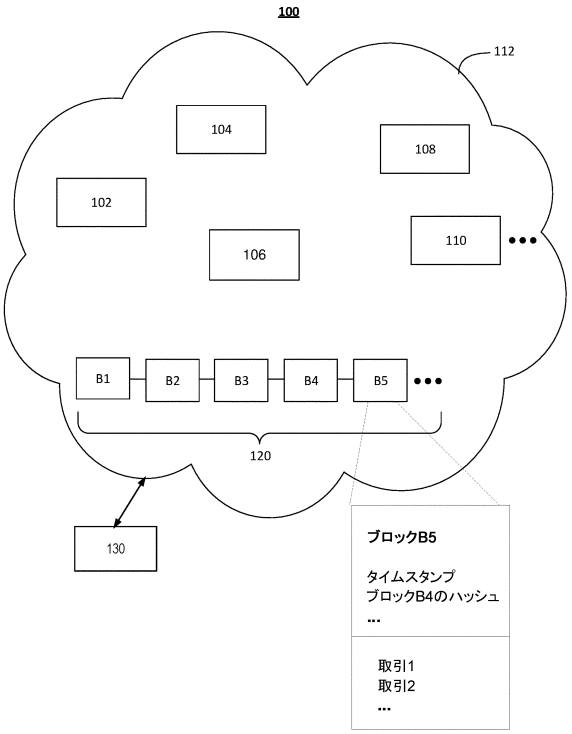
【００６９】

[0075] 簡潔にするために別個の実施形態の文脈で説明される本明細書の或る特徴はまた、単一の実施形態における組み合わせで提供されてもよいことが認識される。反対に、簡潔にするために単一の実施形態の文脈で説明される本明細書の様々な特徴もまた、別々に、又は任意の適切なサブ組み合わせで、若しくは本明細書の任意の他の説明される実施形態において適切なように提供されてもよい。様々な実施形態の文脈で説明される或る特徴は、別段の記載がない限り、それらの実施形態の不可欠な特徴ではない。

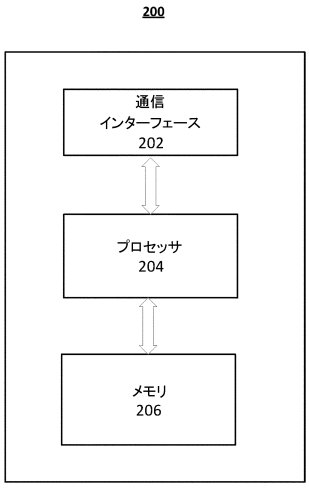
【００７０】

[0076] 本明細書が、特定の実施形態に関連して説明されたが、多くの代替、修正、及び変形が、当業者には明らかであろう。従って、次の特許請求の範囲は、請求項の条項内に入る全てのかかる代替、修正、及び変形を包含する。

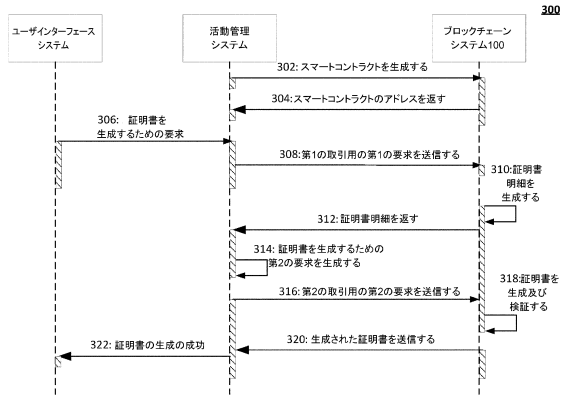
【図１】



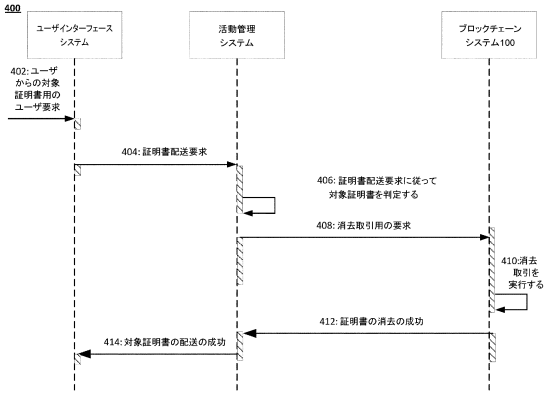
【図２】



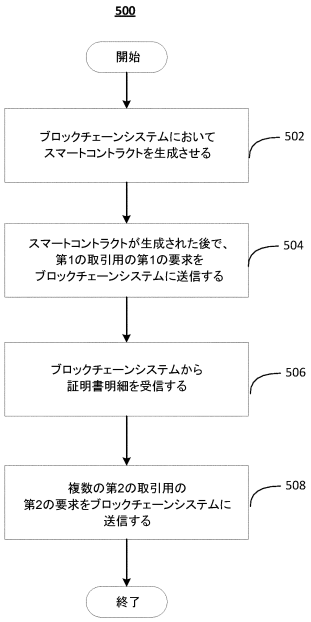
【図３】


300
ユーザインターフェース システム
活動管理 システム
ブロックチェーン システム100
302: スマートコントラクトを生成する
304: スマートコントラクトのアドレスを返す
306: 証明書を 生成するための要求
308: 第1の取引用の第1の要求を送信する
310: 証明書 明細を 生成する
312: 証明書明細を返す
314: 証明書を生成するための 第2の要求を生成する
316: 第2の取引用の第2の要求を送信する
318: 証明書を 生成及び 検証する
320: 生成された証明書を送信する
322: 証明書の生成の成功

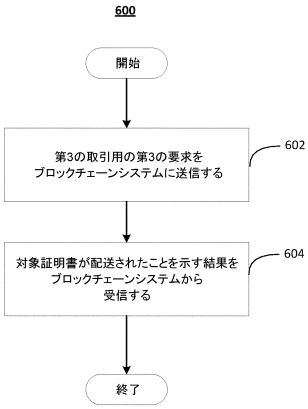
【図４】


400
ユーザインターフェース システム
活動管理 システム
ブロックチェーン システム100
402: ユーザ からの対象 証明書用の ユーザ要求
404: 証明書配送要求
406: 証明書配送要求に従って 対象証明書を判定する
408: 消去取引用の要求
410: 消去 取引を 実行する
412: 証明書の消去の成功
414: 対象証明書の配送の成功

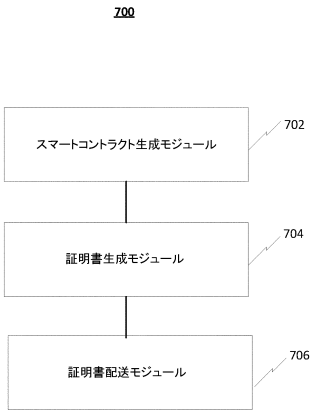
【図５】


500
開始
ブロックチェーンシステムにおいて スマートコントラクトを生成させる
502
スマートコントラクトが生成された後で、 第1の取引用の第1の要求を ブロックチェーンシステムに送信する
504
ブロックチェーンシステムから 証明書明細を受信する
506
複数の第2の取引用の 第2の要求をブロックチェーンシステムに 送信する
508
終了

【図６】


600
開始
第3の取引用の第3の要求を ブロックチェーンシステムに送信する
602
対象証明書が配送されたことを示す結果を ブロックチェーンシステムから 受信する
604
終了

【図７】



フロントページの続き

(72)発明者　チェン，ロン
中華人民共和国，ジャージャン　３１１１２１，ハンチョウ，ユ　ハン　ディストリクト，ウェスト　ウェン　イ　ロード　ナンバー９６９，ビルディング　３，５／エフ　アリババ　グループ　リーガル　デパートメント
(72)発明者　リ，ヤンペン
中華人民共和国，ジャージャン　３１１１２１，ハンチョウ，ユ　ハン　ディストリクト，ウェスト　ウェン　イ　ロード　ナンバー９６９，ビルディング　３，５／エフ　アリババ　グループ　リーガル　デパートメント

審査官　大野　朋也

(56)参考文献　特開２０１９－００８７９１（ＪＰ，Ａ）
特開２０１８－０２８７６２（ＪＰ，Ａ）
米国特許第１０１０２２６５（ＵＳ，Ｂ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９９／００