

(19) 日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2021-529397

(P2021-529397A)

(43) 公表日 令和3年10月28日 (2021. 10. 28)

(51) Int.Cl.	F I	テーマコード (参考)
G 0 6 F 21/64 (2013.01)	G O 6 F 21/64	5 L O 5 5
G 0 6 Q 20/38 (2012.01)	G O 6 Q 20/38 3 1 0	

審査請求 未請求 予備審査請求 未請求 (全 22 頁)

(21) 出願番号 特願2020-573204 (P2020-573204) (86) (22) 出願日 令和1年7月3日 (2019. 7. 3) (85) 翻訳文提出日 令和3年2月10日 (2021. 2. 10) (86) 国際出願番号 PCT/US2019/040646 (87) 国際公開番号 W02020/010279 (87) 国際公開日 令和2年1月9日 (2020. 1. 9) (31) 優先権主張番号 62/693, 713 (32) 優先日 平成30年7月3日 (2018. 7. 3) (33) 優先権主張国・地域又は機関 米国 (US) (31) 優先権主張番号 62/768, 049 (32) 優先日 平成30年11月15日 (2018. 11. 15) (33) 優先権主張国・地域又は機関 米国 (US)	(71) 出願人 519010617 ジーエムオーグローバルサイン ピーティ ーイー リミテッド シンガポール国 ワリック ストリート 1 グオコタワー # 2 5 - 0 1 A (74) 代理人 100114890 弁理士 アインゼル・フェリックス＝ライ ンハルト (74) 代理人 100098501 弁理士 森田 拓 (74) 代理人 100116403 弁理士 前川 純一 (74) 代理人 100134315 弁理士 永島 秀郎
--	---

最終頁に続く

(54) 【発明の名称】 ブロックチェーンアドレスおよび所有者の検証のためのシステムおよび方法

(57) 【要約】

安全なブロックチェーントランザクションのためのシステムおよび方法であって、1つまたは複数のコンピューティングデバイスによって、複数のノードを有するブロックチェーンを形成することを含んでいる。各ノードはブロックチェーンアドレスを有している。認証サーバから、認証証明書が要求される。認証証明書は、トランザクションに関連付けられたエンティティの同一性を検証するための1つまたは複数のフィールドと、複数のブロックチェーンノードのうちの1つのブロックチェーンノードの認証されたアドレスを含むアドレスフィールドとを含んでいる、信用される証明書である。エントリが信用される証明書によって認証されていること、および認証されたアドレスが第1のブロックチェーンアドレスと一致することを決定することによって、トランザクションが検証される。

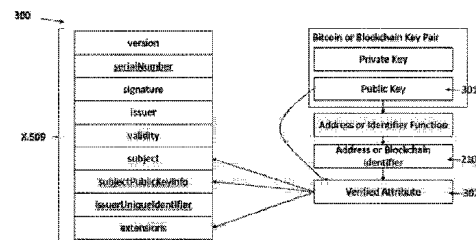


FIG. 3

【特許請求の範囲】

【請求項 1】

ブロックチェーンを維持する 1 つまたは複数のコンピューティングデバイスとサーバとを含み、

前記ブロックチェーンは、それぞれがブロックチェーンアドレスを含む 1 つまたは複数のノードを有し、前記 1 つまたは複数のコンピューティングデバイスは、ネットワークを介して相互に通信することができ、

前記サーバは、前記ネットワーク上で通信し、エンティティに関連付けられた認証証明書を提供するように構成されており、前記認証証明書は、前記ブロックチェーンアドレスが前記エンティティに関連付けられていることを検証するための、複数の前記ブロックチェーンアドレスのうちの少なくとも 1 つのブロックチェーンアドレスを含むアドレスフィールドを含む、システム。

10

【請求項 2】

前記ブロックチェーンは、ビットコインブロックチェーンを含む、請求項 1 記載のシステム。

【請求項 3】

前記ブロックチェーンアドレスは、ビットコインアドレスである、請求項 2 記載のシステム。

【請求項 4】

前記認証証明書は、X. 509 証明書である、請求項 1 記載のシステム。

20

【請求項 5】

前記アドレスフィールドは、前記 X. 509 証明書の拡張子フィールドである、請求項 4 記載のシステム。

【請求項 6】

前記サーバは、認証サービスに関連付けられている、請求項 1 記載のシステム。

【請求項 7】

前記 1 つまたは複数のコンピューティングデバイスは、前記サーバからの前記認証証明書の要求によって、各エンティティの同一性を検証するように構成されている、請求項 1 記載のシステム。

30

【請求項 8】

前記 1 つまたは複数のコンピューティングデバイスは、前記各エンティティの同一性を検証した後、前記各エンティティとの金融トランザクションを行うように構成されている、請求項 7 記載のシステム。

【請求項 9】

前記認証証明書は、暗号化公開鍵に関連付けられている、請求項 1 記載のシステム。

【請求項 10】

前記認証証明書に含まれる前記ブロックチェーンアドレスに対応するブロックチェーンノードは、前記暗号化公開鍵に関連付けられている、請求項 9 記載のシステム。

【請求項 11】

安全なトランザクションのための方法であって、

1 つまたは複数のコンピューティングデバイスによって、複数のノードを有するブロックチェーンを形成するステップであって、各ノードはブロックチェーンアドレスを有し、前記複数のノードの第 1 のノードは、トランザクションに関連付けられた第 1 のブロックチェーンアドレスを有する、ステップと、

認証サーバから認証証明書を要求するステップであって、前記認証証明書は、前記トランザクションに関連付けられたエンティティの同一性を検証するための 1 つまたは複数のフィールドを含み、かつ認証されたアドレスを含むアドレスフィールドを有する、ステップと、

前記認証されたアドレスが前記第 1 のブロックチェーンアドレスと一致することを決定

40

50

することによって、前記エンティティが前記トランザクションに関連付けられていることを検証するステップと、
を含む、方法。

【請求項 1 2】

前記エンティティが前記トランザクションに関連付けられていることを検証するステップの後に、資金を前記第 1 のブロックチェーンアドレスとの間で転送するステップをさらに含む、請求項 1 1 記載の方法。

【請求項 1 3】

前記ブロックチェーンは、ビットコインブロックチェーンを含む、請求項 1 1 記載の方法。

【請求項 1 4】

前記ブロックチェーンアドレスは、ビットコインアドレスである、請求項 1 3 記載の方法。

【請求項 1 5】

前記認証証明書は、X. 509 証明書である、請求項 1 1 記載の方法。

【請求項 1 6】

前記アドレスフィールドは、前記 X. 509 証明書の拡張子フィールドである、請求項 1 5 記載の方法。

【請求項 1 7】

前記サーバを、認証サービスに関連付ける、請求項 1 1 記載の方法。

【請求項 1 8】

前記 1 つまたは複数のコンピューティングデバイスは、前記サーバからの前記認証証明書の要求によって、各エンティティの同一性を検証するように構成されている、請求項 1 1 記載の方法。

【請求項 1 9】

前記 1 つまたは複数のコンピューティングデバイスは、前記各エンティティの同一性を検証した後、前記各エンティティとの金融トランザクションを行うように構成されている、請求項 1 8 記載の方法。

【請求項 2 0】

前記認証証明書を、暗号化公開鍵に関連付ける、請求項 1 1 記載の方法。

【請求項 2 1】

前記認証証明書に含まれる前記ブロックチェーンアドレスに対応するブロックチェーンノードを、前記暗号化公開鍵に関連付ける、請求項 2 0 記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、ブロックチェーン、より具体的には、同一性の検証を伴うブロックチェーンに関する。

【0002】

背景

ブロックチェーンは、暗号化ハッシュを含む暗号化を使用して共にリンクされている、ブロックと称される記録の増大するリストである。ブロックチェーンの各ブロックは、先行するブロックの暗号化ハッシュ、タイムスタンプおよびトランザクションデータを含むことが可能である。ブロックがチェーンに記録されると、後続のすべてのブロックを変更することなく、任意の所与のブロックにおけるデータをさかのぼって変更することはできない。したがって、ブロックチェーンは変更に対して比較的耐性があり、設計上安全である。

【0003】

いくつかのブロックチェーンには、システムと密接に絡み合っている「コイン」または「トークン」等の価値の単位が根付いていることがある。単なる元帳は価値の会計を提供

10

20

30

40

50

するが、ブロックチェーンは価値を保存することもできる。ビットコインブロックチェーンは、価値を保存する新世代のインターネットプロトコルの最初の、かつ最長の実行を表している。

【0004】

ビットコインはプルーフオブワークシステムに基づいており、プルーフオブワークシステムは、エネルギーと、新しいブロックを作成し、ブロック報酬を請求するための計算リソース、より一般的には労力とを必要とする。各ビットコインを生成するために必要なこれらの計算リソースは、各ビットコインが犠牲の尺度であるため、価値を表すために必要なトラストを最小化する。

【0005】

取引の各当事者は、特定のユニットが、システムを維持および保護する作業によって作成されたものであり、命令または恣意的な法令または投機的債務によって作成されたものではないことを確認することができる。この意味で、少なくとも、ビットコインの偽造不可能な性質とそれを生成するために必要なリソースとは、ビットコインに価値を与える。言い換えれば、ビットコインブロックのマイニング作業は、ブロックチェーンを偽造不可能にすることによってブロックチェーンを保護することになる。

【0006】

具体的には、マイニング作業は、セキュリティの侵害およびネットワークの障害に直面した際に、その完全性を維持するデータ構造を作成することに向けられている。ビットコインネットワーク内のすべてのコンピュータがオフラインになり、すべての秘密鍵が危険にさらされた場合でも、攻撃者は、最初に、ブロックチェーンデータ構造を作成するために必要なすべての作業を再作成することによってのみ、ブロックチェーンデータ構造を偽造することができる。ほとんどの攻撃者にとって、それは時間をかけても実行可能ではない。

【0007】

さらに、マイニングによってブロックチェーンを保護するコストは、システムから得られる効率によって、時間にわたって回収される。

【0008】

偽りなく高価な商品には有益富の転送を可能にすることによって繰り返し、価値を加算する。トランザクションが可能になるか、より安価になるたびに、ビットコインを生成するためのコストはより多く回収される。このコストは多くのトランザクションにわたって償却される。貴金属の金銭的価値はこの原則に基づいている。それは収集品にも当てはまる。収集品は、それらが希少であるほどより評価され、さらに偽造可能性が低いほどこれは希少である。また、芸術のように、確実に熟練した人的労働または特有の人的労働が製品に追加される場合にも、これは当てはまる。

【0009】

したがって、ビットコインのマイニング作業はブロックチェーンを保護し、マイニング作業は、得られる効率によってこれを相殺する多くのトランザクションにわたって償却される。

【0010】

そのすべての長所について、ブロックチェーンは、集中型のシステムおよびトラストベースのシステムと比較して、必ずしも計算上効率的であるとは限らない。これは主に、その最下層で、ブロックチェーンが計算効率およびスケーラビリティを社会的スケーラビリティ、セキュリティおよび偽造不可能性とトレードするためである。つまり、ブロックチェーンは、管理性が高く、柔軟性の高いコンピューティングプラットフォームを、オープンで冗長性があり、かつ堅牢なコンピューティングプラットフォームとトレードする。

【0011】

概要

一実施形態では、システムは、ブロックチェーンを維持する1つまたは複数のコンピューティングデバイス、それぞれがブロックチェーンアドレスを含む1つまたは複数のノー

10

20

30

40

50

ド（たとえばトランザクション）を有するブロックチェーン、ネットワークを介して相互に通信することができる1つまたは複数のコンピューティングデバイスを含んでいる。ネットワーク上で通信するサーバは、エンティティに関連付けられた認証証明書を提供するように構成されており、ここで認証証明書は、ブロックチェーンアドレスがエンティティに関連付けられていることを検証するための、複数のブロックチェーンアドレスのうちの少なくとも1つのブロックチェーンアドレスを含むアドレスフィールドを含んでいる。

【0012】

以下の特徴のうちの1つまたは複数が含まれ得る。

【0013】

ブロックチェーンは、ビットコインブロックチェーンであり得る。

10

【0014】

ブロックチェーンアドレスは、ビットコインアドレスであり得る。

【0015】

認証証明書は、X. 509証明書であり得る。

【0016】

アドレスフィールドは、X. 509証明書の拡張子フィールドであり得る。

【0017】

サーバを、認証サービスに関連付けてよい。

【0018】

1つまたは複数のコンピューティングデバイスは、サーバからの認証証明書の要求によって、各エンティティの同一性を検証するように構成され得る。

20

【0019】

1つまたは複数のコンピューティングデバイスは、各エンティティの同一性を検証した後、各エンティティとの金融トランザクションを行うように構成され得る。

【0020】

認証証明書を、暗号化公開鍵に関連付けてよい。

【0021】

認証証明書に含まれるブロックチェーンアドレスに対応するブロックチェーンノードを、暗号化公開鍵に関連付けてもよい。

【0022】

別の実施形態では、安全なトランザクションのための方法は、1つまたは複数のコンピューティングデバイスによって、複数のノードを有するブロックチェーンを形成することを含んでおり、各ノードはブロックチェーンアドレスを有しており、複数のノードの第1のノードは、トランザクションに関連付けられた第1のブロックチェーンアドレスを有している。認証サーバから、認証証明書が要求される。認証証明書は、トランザクションに関連付けられたエンティティの同一性を検証するための1つまたは複数のフィールドを含んでおり、認証されたアドレスを含むアドレスフィールドを有している。トランザクションに関連付けられたエンティティは、認証されたアドレスが第1のブロックチェーンアドレスと一致することを決定することによって検証される。

30

【0023】

以下の特徴のうちの1つまたは複数が含まれ得る。

【0024】

エンティティがトランザクションに関連付けられていることを検証した後、資金が第1のブロックチェーンアドレスとの間で転送されてよい。

40

【0025】

ブロックチェーンは、ビットコインブロックチェーンを含み得る。

【0026】

ブロックチェーンアドレスは、ビットコインアドレスであり得る。

【0027】

認証証明書は、X. 509証明書であり得る。

50

【0028】

アドレスフィールドは、X. 509 証明書の拡張子フィールドであり得る。

【0029】

サーバを、認証サービスに関連付けてよい。

【0030】

1つまたは複数のコンピューティングデバイスは、サーバからの認証証明書の要求によって、各エンティティの同一性を検証するように構成され得る。

【0031】

1つまたは複数のコンピューティングデバイスは、各エンティティの同一性を検証した後、各エンティティとの金融トランザクションを行うように構成され得る。

10

【0032】

認証証明書を、暗号化公開鍵に関連付けてよい。

【0033】

認証証明書に含まれるブロックチェーンアドレスに対応するブロックチェーンノードを、暗号化公開鍵に関連付けてもよい。

【0034】

前述の特徴は、以下の図面の説明からより完全に理解され得る。図面は、開示された技術を説明および理解するのに役立つ。すべての可能な実施形態を例示および説明することはしばしば非現実的または不可能であるため、提供される図は、1つまたは複数の例示的な実施形態を示す。したがって、これらの図は、本発明の範囲を制限することを意図するものではない。図中の同様の数字は、同様の要素を示している。

20

【図面の簡単な説明】

【0035】

【図1】 認証サーバを含むコンピューティングシステムのブロック図である。

【図2】 ブロックチェーンのブロック図である。

【図3】 認証証明書のブロック図である。

【図3A】 QRコードを含むシステムの図である。

【図4】 ブロックチェーントランザクションに関連付けられたエンティティの同一性を検証するためのプロセスのフローチャートである。

【図5】 ブロックチェーン転送に関連付けられたエンティティの同一性を検証するためのプロセスのフローチャートである。

30

【図6】 ブロックチェーン引き出しに関連付けられたエンティティの同一性を検証するためのプロセスのフローチャートである。

【図7】 ライトニングネットワークに関連付けられたエンティティの同一性を検証するためのプロセスのフローチャートである。

【図8】 コンピューティングデバイスのブロック図である。

【0036】

詳細な説明

本明細書で論じられる方法およびシステムの例は、以下の説明に記載されるか、または添付の図面に示される構成要素の構造の詳細および配置に適用されることに限定されない。方法およびシステムは、他の実施形態で実装することができ、かつ様々な様式で実施可能または実行可能であることが当業者に理解されるであろう。特定の実装の例は、説明のみを目的として本明細書に提供されており、制限することを意図するものではない。また、本明細書において使用される表現および用語は、説明を目的とするものであり、制限をするものと見なされるべきではない。本明細書において単数形で参照される、システムおよび方法の例、実施形態、構成要素、要素または作用へのあらゆる参照は、複数形を含んでいる実施形態も包含してよく、本明細書における任意の実施形態、構成要素、要素または作用への複数形でのあらゆる参照は、単数形のみを含む実施形態も包含してよい。単数形または複数形での参照は、現在開示されているシステムまたは方法、それらの構成要素、作用または要素を制限することを意図するものではない。本明細書における「inc l

40

50

uding (含んでいる)」、「comprising (含んでいる)」、「having (有している)」、「containing (含んでいる)」、「involving (含んでいる)」およびそれらの変形の使用は、その後に挙げられる項目およびそれらの同等物ならびに付加的な項目を包含することを意味する。「or (または)」の参照は、「or (または)」を使用して説明される任意の用語が、説明される用語の1つ、複数およびすべてのいずれかを示すことができるように、包括的であると解釈され得る。

【0037】

当業者は、ブロックチェーンの説明の際に、用語「ブロック」が、典型的に、ブロックチェーン内のブロックを指すために使用され、用語「ノード」が、典型的に、ライトニングネットワーク内のノードを指すために使用されることを認識するであろう。しかし、本開示では、用語「ブロック」および「ノード」は、ブロックチェーン内のブロック、ライトニングネットワーク内のノード、またはその両方を指すために交換可能に使用される。用語「ブロック」および「ノード」は、本開示の文脈において適切に任意のブロックまたはノードを意味すると解釈されてもよい。

【0038】

図1を参照すると、コンピューティングシステム100は、ネットワーク106上で通信するコンピューティングデバイス102および104を含んでいる。コンピューティングデバイス102および104は、ソフトウェア命令を実行することができる任意のタイプのコンピューティングデバイスであってよく、これに制限されないが、デスクトップコンピュータ、ラップトップコンピュータ、携帯電話、サーバ、internet of things (IoT) センサー、組み込みデバイス等のデバイスを含んでいる。ネットワーク106は、コンピューティングデバイスが互いに通信することを可能にする任意のタイプのネットワークであってよく、これに制限されないが、WAN、LAN、インターネット等を含んでいる。

【0039】

システム100は、認証サービスに関連付けられ得る1つまたは複数のサーバ108も含み得る。認証サービスは、アドレス、同一性、トランザクション、署名等の安全な認証を提供するデジタル証明書を発行または提供するサービスであってよい（たとえば、公開鍵基盤（PKI）に対応する認証局（CA））。認証サービスは、（たとえば、デジタル署名またはトランザクションを立証または承認することによって）データまたはトランザクションのソース、またはデータまたはトランザクションとエンティティとの関連付けを確立するために、非対称暗号化（たとえば、公開鍵／秘密鍵のペアを使用した公開鍵暗号化）を使用した認証を提供してもよい。

【0040】

システム100は、エンティティ112に関連付けられたサーバ110も含み得る。エンティティ112は、会社、個人、またはサーバ108によって認証され得る同一性を有する任意の他の法的なエンティティであり得る。たとえば、CAは、エンティティの名前、メールアドレス、インターネットドメイン名およびビットコインアドレスを検証することができる。任意選択で、またたとえば、CAは、ブロックチェーン識別子に対応する秘密鍵の所有権を証明するようにエンティティに要求することによって（たとえば、ビットコインアドレスに対応する秘密鍵を使用して構築されたデジタル署名を提供することによって）、ブロックチェーン識別子（たとえばビットコインアドレス）の所有権を確立することができる。

【0041】

システム100は、比較的最小限のシステムとして示されており、これは2つのコンピューティングデバイス102および104と、認証サービスに関連付けられたサーバ108と、ネットワーク106を介して通信するエンティティ112に関連付けられたサーバ110とを有している。しかし、付加的なデバイスが、ネットワーク106を介して通信を行ってもよく、さらにシステム100と相互作用してよい、またはシステム100の一部であってよい。これらのデバイスは、見やすくするために示されていない。

【0042】

図2を参照すると、ブロックチェーン200が、システム100に関連付けられていてよい。ブロックチェーン200は、コンピューティングデバイス102および104によってならびにサーバ110によって、全体的または部分的に格納され得る。示されていない他のデバイスも、ブロックチェーン200の全体または一部を格納し得る。実施形態では、ブロックチェーン200は、ビットコインブロックチェーン、ライトニングネットワーク等であり得る（ライトニングネットワークは必ずしもブロックチェーンではないが、本開示に記載されるシステムおよび技術は、ライトニングネットワーク上で動作し得る、またはライトニングネットワークと関連して動作し得るということに留意されたい）。ブロックチェーン200は、任意のエンティティによる参加を許可するパブリックブロックチェーンまたはビットコインブロックチェーンやイーサリアムブロックチェーン等の個人的なブロックチェーンであってよい。他の実施形態では、ブロックチェーン200は、ユーザーの閉じられたグループおよびプライベートトランザクションを伴うプライベートブロックチェーン、またはグループまたはコンソーシアムによって管理され得るハイブリッドブロックチェーンであってよい。

10

【0043】

ブロックチェーン200のタイプに関係なく、様々なエンティティをブロックチェーン内のトランザクションに関連付けてよい。たとえば、ブロックチェーン200は、あるエンティティから別のエンティティに資金を転送するビットコイントランザクションを含み得る。任意選択で、トランザクションを、（トランザクションへの入力を許可するエンティティに関連付けられている）1つまたは複数の送信元アドレスおよび／または（トランザクションの出力に対して潜在的に権利を行使することができるエンティティに関連付けられている）宛先アドレスに関連付けてよい。金融（およびその他の）トランザクションの安全な性質のため、トランザクションの当事者が、このトランザクションの他の当事者の同一性を認証できるのは有益であり得る。たとえば、受取人が銀行である場合、譲渡人にとって、適切な銀行に関連付けられている受取人のアドレスを認証することは有益であり得る。

20

【0044】

ブロックチェーン200は、デバイス102および104等のコンピューティングデバイスによって作成され、維持され、実行されてよい。ブロックチェーン200は、オリジナルのブロック202のような（本開示においてノードとも称される）ブロックのシリーズを含み得る。用語「ブロックチェーン」は、ブロックチェーン200構造全体を指す場合もあれば、構造内で最も長く中断されないチェーン（たとえばブロック204）を指す場合もある。ブロックチェーン200は、メインブロックチェーンから分岐するノード（ブロック206等）も含み得る。

30

【0045】

各ブロックは、ブロックに関連付けられ、ブロックチェーントランザクションを受け入れて、送るために使用されるアドレス210と、データトランザクションのハッシュ木212とを含み得る。実施形態では、ブロックを特定のエンティティに関連付けてよい。したがって、ブロックのアドレス210を、特定のエンティティに関連付けてもよい。たとえば、資金がアドレス210に転送される場合、それらの資金は、ブロック214に関連付けられたエンティティに利用可能になり得る。

40

【0046】

ライトニングネットワークは、基礎となるブロックチェーン（たとえばビットコイン）の頂上に構築されたレイヤ2プロトコルである。ユーザーのペアは、担保によって保護された誠意を持って交渉するための契約を締結する。チャネルと称されるこれらの契約を、ブロックチェーン200内に記録することができる（たとえば「資金調達」トランザクションとして）。

【0047】

各ペアは、進行中の交渉および部分的に署名されているが記録されていない契約（すな

50

わち「オフチェーン」) を使用することによってチャンネルを更新し、チャンネルの担保の割り当てを調整し、ブロックチェーンでの解決 (settlement) を延期する。

【0048】

資金を転送するために、送信者は、別の当事者との記録されていない契約を更新し、次に、別の当事者との自身の契約の1つを更新し、以下同様に続いて、プロセスが受取人に到達する。その結果、一連の契約更新が生じ得る。

【0049】

当事者は、誠意を持って交渉しなければならない(過去の取り消されたまたは更新された契約を否認することを含む)、またはライトニングネットワークにおける担保を失うリスクを冒さなければならない。交渉が決裂し、紛争または違反がない場合は、最新の契約更新において、合意された割り当てに従って担保を返却することができる。

10

【0050】

ブロックチェーンへの記録を延期することによって、ライトニングネットワークは、より高いトランザクション量およびほぼ即時の確認を可能にする。

【0051】

ブロックチェーン自体の速度および容量の制限は、ライトニングトランザクションを直接制限しない。自動化されたほぼ瞬時の交渉および契約更新は、ブロックチェーンにすぐに記録する必要がない場合がある。すなわち、これらは、オフチェーンで発生する可能性がある。しかし、場合によっては、ブロックチェーンによって紛争解消および解決の速度および量が制限される。紛争および解決が日常のトランザクションよりも格段に稀である場合、ライトニングネットワークは極めて高度なトランザクションのスケーラビリティを得ることができる。

20

【0052】

標準的なビットコイントランザクションは通常、それがブロックチェーンに含まれるまで、すなわち、それが、その後いくつかの付加的なブロックが連結されるブロックに含まれるまで、最終的または取消不能(たとえば「確認済み」)として受け入れられない。トランザクションがブロックになる前は、まだブロックチェーンの一部ではなく、まだ二重支払いの影響を受けやすい場合がある。ブロックチェーンのプルーフオブワークは、未確認のトランザクションを保護しない。

【0053】

ライトニングネットワークでは、ブロックチェーンへの解決は延期されるが、これは、トラスト最小化の様式で延期される。ライトニングペイメントが完了すると、これは、ライトニングネットワークトランザクションに伴う、トラスト最小化された保護をすぐに受け取ってよい。すなわち、相手方当事者が、記録されていない契約に違反した場合、相手方当事者は自身の担保を失う。その結果、ライトニングペイメントは、オフチェーンで、技術的には確認されていないが、効率的に、ほぼ瞬時に最終的なものになる。

30

【0054】

ライトニングネットワークでは、ビットコインは、各個々のチャンネル内で前後に行ったり来たりする可能性がある。ライトニングトランザクションでは、1つのビットコインが1つのトランザクションにおいて、最初の送信者から最終的な受信者まで移動しない場合がある。代わりに、ライトニングネットワークは、行き来するビットコインの広大なネットワークを形成してよく、各個々のビットコインは1つのチャンネル内でのみ前後に移動する。

40

【0055】

交流用の変圧器のように、ライトニングネットワーク内のノードは、異なる値のチャンネルを維持し、他の「高電力」ノードを伴う大きなチャンネルを作成し、他方で、他のユーザーとの任意の小さなチャンネルを直接維持する。そうすることで、そのようなノードは変圧器として機能することができ、非常に大きい容量のフローを、日常の消費者トランザクションに適した、管理可能な小さいフローに変換する。同様に、このようなノードは、同じ方向に移動する小さいフローを集約して、より大きい容量のチャンネルを介した、束化され

50

た移送を実現することができる。エンドポイントノードがネットワークの接続性または計算リソースを制限している場合、そのような大きい容量のノードは、一部のルーティングタスクおよびチャンネルモニタリングタスクを処理することができてよい。たとえば、容量の小さいノードは、ルート決定を、信用される、認証された、容量の大きいノードまたは十分に接続されたノードに、潜在的に安全に外部委託することができる。

【0056】

付加的に、ライトニングチャンネルは資金供給されなければならないので、ノードは大量の利用可能な資金を有してよく、より多くの（そしてより価値の高い）チャンネルを維持してよい。

【0057】

高度に接続されたハブがライトニングネットワーク内に出現するとき、それらは依然として、トラスト最小化されるだろう。チャンネルはライトニングネットワークの規則によって保護されており、ノードは一方的にチャンネルを閉じることができる。

【0058】

ライトニングネットワーク上の同一性は大部分が静的であり、かつ公開されているが、トランザクションは相手方当事者だけに知られている場合がある。たとえば、一部の情報は、トランザクションにおける中間ノードで利用可能であり、一部の要約情報はパブリックブロックチェーン上で利用可能である。ライトニングネットワーク上のノードの同一性を、任意選択で公開鍵に関連付けることが可能である。

【0059】

したがって、ライトニングネットワークでは、同一性および評判がトランザクションにとって重要である場合がある。たとえば、評判は、契約および相手方当事者を探す上で重要である。評判によって、当事者は、潜在的な相手方当事者が可用性、接続性および料金に関する表明を尊重するか否かをより効率的に評価することができる。評判は、稼働時間、チャンネルの数および容量、違反および非相互解決の数等、客観的に観察可能なネットワークメトリックに基づくことができる。このような情報は、認証証明書によって認証された信用されるエンティティを使用して配布可能である。

【0060】

公開同一性は、払受人および商人の認証を可能にする。たとえば、購入を行う際に、認証された同一性（たとえば、エンティティおよび公開鍵に関連付けられた認証証明書を使用する）によって、ユーザーは、支払いが、目的の商人に送られることを検証し、請求書および領収書を有効化することができる。検証および認証された同一性は特に重要である。なぜなら、これは、既存の信用を有していない、匿名化されたデジタルコンテキストにおいて防止が難しい、中間者攻撃に対する効率的な保護を提供するからである。

【0061】

効率的かつ封じ込められた信用のポイントを提供することができる公開鍵基盤（PKI）は、ブロックチェーンのトラスト最小化の性質を損なうことなく、これらのニーズ、すなわち評判および同一性の両方に対処することができる。

【0062】

たとえば、ライトニングネットワークでは、ノードを、その公開鍵およびネットワーク識別子（たとえば、IPアドレスまたは他のエンドポイント識別子）によって表すことができる。その公開鍵は、公的に信用されているX. 509デジタル証明書における公開鍵（または別のフィールド、たとえば、サブジェクト属性またはX. 509拡張子における対応する情報）に対応することができる。たとえば、再び図1を参照すると、認証証明書を提供するサーバ108が、それらの認証証明書を（たとえばX. 509証明書として）提供してよい。次に、このデジタル証明書を使用して、認証局（CA）または登録局（RA）によって検証または確認されたノードの同一性を（会社名またはドメイン名等によって）認証することができる。認証されたライトニングノードを使用して、ユーザーは、たとえば、支払いが実際に目的の商人に送られることを確認することができる。

【0063】

10

20

30

40

50

いくつかの実施形態では、レイヤ2ブロックチェーンプロトコル（たとえば、ライトニングネットワーク）トランザクションにおける認証のために発行された証明書（たとえばX. 509証明書）は、潜在的なトランザクションに関連するデータ（たとえば、目的地、金額、時間、目的地または承認された当事者の署名または1人または複数の参加者の地理的位置）を含む請求書フィールドを含み得る。たとえば、商人が、商品またはサービスの販売に対するトランザクションにおいてカスタマーからの支払いを要求している場合、X. 509証明書は、潜在的なトランザクションに関連する情報を含んでいる請求書フィールドを（たとえば、サブジェクト属性としてまたはX. 509拡張子において）含むことができる（たとえば、標準のライトニングネットワーク請求書）。

【0064】

図3を参照すると、エンティティに関連付けられた特定の同一性情報の検証を可能にする認証証明書300が、サーバ108によって発行されてよい。任意選択で、認証証明書300は、X. 509フォーマットに準拠してよく、X. 509証明書であってよい。任意選択で、認証証明書300は、第3の当事者によって承認または検証されてよく、たとえば、そのような証明書のデータの一部または全部は、認証局（CA）の秘密鍵（たとえば、信用される、またはその他の方法で承認されたデジタル証明書に対応する秘密鍵）で署名され得る。実施形態では、アドレス210および／または公開鍵301は、検証された属性302を含んでいてよく、検証された属性302として使用されてよく、または検証された属性302を導出するために使用されてよく、任意選択で、たとえば、認証局（CA）によって署名された、またはその他の方法で検証された（たとえば、認証証明書300の発行中にCAの秘密鍵によって署名された）認証証明書300の一部内に含まれ得る。認証局が認証証明書300に署名するのに使用する秘密鍵は、公的な認証サービスに関連付けられ得るサーバ108等の信用されるソースによって提供され得る。

【0065】

認証証明書300は、たとえば、検証された属性302を含む、検証された属性302として使用される、または検証された属性302を導出するために使用されるフィールドを含んでいる、様々なフィールドを含み得る。たとえば、認証証明書300は、検証されたビットコインアドレスまたはブロックチェーン識別子が導出され得る公開鍵を含むことができる。任意選択で、証明書における1つまたは複数のフィールドは、1つまたは複数の検証されたブロックチェーンアドレス（たとえばビットコインアドレス）を含むことができる。このアドレスは、ブロックチェーンブロック214において見られるのと同じアドレス210であり得る。認証証明書300は、シリアルナンバー、発行者名、有効性、公開鍵、特有のID、およびそれに限定されないが、認証証明書300の一部として示されるフィールドに含まれる情報を含んでいる他の情報等の、エンティティを識別する情報も含み得る。任意選択で、そのような情報の一部または全部は、1つまたは複数の検証された属性を含んでいてよい、1つまたは複数の検証された属性として使用されてよい、または1つまたは複数の検証された属性を導出するために使用されてよい（たとえば公開鍵は、エンティティに対する検証された属性を含むことができ、ここでこのエンティティは対応する秘密鍵の所有を検証する）。したがって、認証証明書300は、アドレス210および／または公開鍵301を、信用されるエンティティに関連付け、認証してよい。

【0066】

認証証明書300に含まれている検証された属性302は、ブロックチェーンアドレスまたは公開鍵に制限されない。たとえば、検証された属性は、IPアドレス、別のタイプのネットワークアドレス、ブロックチェーン200内のトランザクションに関連付けられた別の特有の識別子、ブロックチェーン200内のトランザクションに転送された量、またはブロックチェーントランザクションに関連付けることができる任意の他のデータおよび／またはブロックチェーントランザクションに含まれているエンティティであり得る。実施形態では、検証された属性は、アドレス参照であり得る。たとえば、検証された属性302は、X. 509証明書の公開鍵を介して間接的にアドレスを参照してよい。したがって、認証証明書300は、認証証明書300において挙げられたエンティティが、実際

に、検証された属性 302 に関連付けられたブロックチェーントランザクションに含まれているエンティティであるという保証を提供することができる。

【0067】

X. 509 証明書内の別個のフィールドとして示されているが、検証された属性 302 は、X. 509 証明書内のどこにでも格納され得る。また、実施形態では、検証された属性 302 を、X. 509 証明書とは別に格納してよいが、X. 509 証明書に関連付けてよい。

【0068】

図 3A を参照すると、認証証明書 300 を、QR コード 350 において符号化することができる。一例として、QR コードは、たとえば、DER または PEM 形式で証明書を符号化することができる。次に、QR コード 350 は、ハードウェアウォレットまたはソフトウェアウォレットを含み得る、352 等のコンピューティングデバイスによってスキャンされ得る。コンピューティングデバイスは、トランザクションにおける相手方当事者の同一性（たとえば、ビットコイントランザクションにおける譲受人の同一性）を確立するために、認証証明書を検証することができる。コンピューティングデバイスは、認証証明書を検証した後に、たとえば、証明書が有効であることの表示とともに、認証証明書に含まれている同一性情報を表示することによって、ユーザーに通知をすることができる。

10

【0069】

QR コード内の認証証明書は、QR コード、または認証証明書、または 1 つまたは複数の潜在的なまたは既存の暗号通貨アドレスまたはブロックチェーンアドレス、または 1 つまたは複数の潜在的なまたは既存の暗号通貨トランザクションまたはブロックチェーントランザクション（たとえば、ビットコインアドレスを参照するまたは含むオンチェーンビットコイントランザクション）に関連付けられたエンティティの検証された同一性をウォレットに提供し得る。これは、たとえば、暗号通貨アドレスまたはブロックチェーンアドレス、またはそのようなアドレスに対応する公開鍵を含めることによって行われる。

20

【0070】

次に、任意選択で、ウォレットは、認証証明書に基づいて情報の信憑性を検証することができる。また、任意選択で、ウォレットは、たとえば、サーバ 108 が QR コードに含まれる認証証明書等を認証することを要求することによって、QR コード内の証明書を検証することもできる。その後、ウォレットは、検証されたエンティティでトランザクションを実行していることを確信して、このアドレスでのトランザクションに従事することができる。

30

【0071】

QR コード 350 は、たとえば、認証証明書と請求書との両方を符号化してよい。場合によっては、請求書が認証証明書に含まれていることがある。付加的または択一的に、QR コード 350 は、暗号通貨アドレスまたは識別子以外の情報、または暗号通貨アドレスまたは識別子に対して付加的な情報を含む証明書を符号化してよい。たとえば、QR コードは、URL、アカウント識別子、ユーザー識別子、または転々と変化する識別子または定期的に変わる識別子（たとえば Ali Pay（登録商標）、Line（登録商標）または WeChat Pay（登録商標）の支払い URL またはアカウント番号）を含む認証証明書を含み得る。

40

【0072】

したがって、たとえば、エンティティが QR コードをスキャンするとき、エンティティは、認証証明書およびこの証明書または QR コードに含まれている情報を検証して、この QR コード（およびこの QR コード内の情報）が正しいソースに関連付けられていることの保証を得ることができる。

【0073】

任意選択で、QR コードは、認証証明書を回収することができるオンラインの場所（たとえば URL）またはインターフェース（たとえばインターネットアクセス可能な API）を符号化することができる。次に、ハードウェアデバイスまたはソフトウェアプログラ

50

ム（たとえばハードウェアビットコインウォレット）は、（たとえば、指定されたURLからダウンロードすることによって）認証証明書を回収し、この証明書を検証することができる。たとえば、ユーザーは、モバイルデバイス上のビットコインウォレットを使用することができ、これによって、URLを符号化するまたはその他の方法で参照するQRコードをスキャンし、このURLからの認証証明書を回収し、回収したこの認証証明書を検証する。これはたとえば、証明書内に含まれる同一性情報およびビットコインアドレスまたは証明書から導出される同一性情報およびビットコインアドレスを検証することを含んでいる。

【0074】

任意選択で、QRは、証明書を回収することができる場所に対して付加的な情報を含むことができる、または符号化することができる。たとえば、QRコードは、認証証明書を回収することができるURLとともに、宛先ブロックチェーンアドレスまたは暗号通貨アドレスを含むことができる。任意選択で、暗号通貨アドレスまたはブロックチェーンアドレスに対応する同一性を確立し、そのような暗号通貨アドレスまたはブロックチェーンアドレスが、QRコード内の符号化されているアドレスまたは含まれているアドレスと一致することを確認するために、証明書を使用することができる。任意選択で、（たとえば、QRコードに含まれているデータが、証明書に対応する秘密鍵によって有効に署名されていることを確認することによって）QRコードに含まれている情報に含まれている、QRコードに含まれている情報に添付される、またはその他の方法でQRコードに含まれている情報に関連するデジタル署名を確認するために、回収した証明書を使用することができる。

【0075】

図4を参照すると、フローチャートは、ブロックチェーントランザクションの当事者を認証するための一般的なプロセス400を記載している。プロセス400は、トランザクションの他の当事者に自身の同一性を証明することを望んでいるエンティティによって、またはトランザクションの他の当事者の同一性の保証を得ることを望んでいるエンティティによって使用されてよい。

【0076】

ステップ402において、当事者は、エンティティ（要求している当事者自体またはこのトランザクションに関連付けられている別の当事者のいずれか）が詐欺師ではないことの証明書をサーバ108に要求する。任意選択で、この要求は、これに限定されないが、デバイス指紋、ドメイン認証、生体認証データ、2FAトークン検証ビデオ、課題となる質問および／または答え、住所、電話番号、ネットワークアドレス、特有の識別子、暗号化鍵等を含んでいる、エンティティに関する識別情報を含むことができる。この識別情報が、エンティティの同一性を検証するために、コンタクトを取ることによって、認証サービスによって、電話またはテキストメッセージを介して、確立されてもよい。

【0077】

ステップ404において、証明書を要求している当事者は、アドレス（すなわちアドレス210）をサーバ108に送る。アドレスは、ブロックチェーン識別子、たとえば公開鍵またはブロックチェーンアドレスまたは暗号通貨アドレス（たとえばビットコインアドレス）を含み得る。また、たとえば、ブロックチェーン内のトランザクション、またはエンティティが従事している任意の他のタイプのブロックチェーンアクティビティである。

【0078】

ステップ406において、サーバ108は、エンティティの同一性を認証する。場合によっては、たとえば、アドレスが静的である場合、サーバ108は、提供されたアドレスがエンティティに関連付けられていることを認証してもよい。これは、アドレスを解読すること、データベースに対してアドレスを確認すること、または幾つかの他の方法でデータの関連付けを介してアドレスをエンティティにリンク付けすることによって行われてよい。たとえば、サーバ108は、アドレスまたはアドレスに対応する公開鍵（たとえば、そこから暗号通貨アドレスが導出されている、またはそこから暗号通貨アドレスを導出す

ることができる公開鍵)のいずれかに対応する秘密鍵の所持を検証することができる。また、たとえば、公開鍵またはアドレスとエンティティとの関連付けを、全体的または部分的に、以下の1つまたは複数に基づいて、確立または想定することができる。すなわち、

(1) 公開鍵またはアドレスに対応する秘密鍵によって、サーバ108への要求に応じて、署名を要求すること、(2) 公開鍵またはアドレスに対応する秘密鍵によって、その対応する公開鍵に応じて、署名を要求すること、(3) 公開鍵またはアドレスに対応する秘密鍵によって、その公開鍵に対応するアドレスに応じて、署名を要求すること、または(4) 公開鍵またはアドレスに対応する秘密鍵によって、たとえば、ノンス値を提供し、署名を要求することによって、ノンス値に応じて、要求しているエンティティに、対話型署名プロトコルに参加することを要求すること、である。

10

【0079】

エンティティおよびアドレスが認証されると、サーバ108は、認証証明書(認証証明書300等)を発行し、エンティティを提供されたアドレスに関連付ける要求者に送ってよい。次に、トランザクションに含まれているエンティティが実際に、認証証明書において挙げられているエンティティであるという保証を提供するために、証明書がトランザクションの他の当事者に提供されてよい。

【0080】

図5を参照すると、フローチャートは、ブロックチェーントランザクションを介して資金を要求するおよび／または受け取るためのプロセス500を示している。ステップ502において、ある当事者は、別の第2の当事者に資金を要求することによって資金の転送を開始する。ステップ504において、第1の当事者は、資金が転送され得る受け取りアドレス(たとえばアドレス210)を作成する。

20

【0081】

ステップ506において、第1の当事者(または別の当事者)は、第1の当事者の同一性を認証する認証証明書を求める要求をサーバ108に送る。この要求は、ステップ504において作成された受け取りアドレスと同様に、第1の当事者に関する識別情報を含んでいる。ステップ510において、サーバ108は、(たとえば、上記の技術のうちの1つまたは複数を使用して)第1の当事者の同一性を認証する。

【0082】

サーバ108が第1の当事者の同一性を認証することができる場合、サーバ108は認証証明書を作成し、受け取りアドレスを認証証明書に関連付ける。次に、認証証明書を資金の譲渡人に送ることができ、譲渡人はステップ514において、認証証明書を介して、提供されたアドレスが実際に第1の当事者に関連付けられたアドレスであることを検証することができる。ステップ516において、資金の転送を開始することができる。

30

【0083】

図6を参照すると、フローチャートは、ブロックチェーントランザクションを通じて資金を引き出すためのプロセス600を示している。ステップ602において、引き出し当事者は、引き出しを開始し、ステップ604において、資金が転送されるべきアドレスを作成する。ステップ606において、引き出し当事者(または別の当事者)は、サーバ108に、引き出し当事者の同一性の認証のための要求を送る。認証の要求は、ステップ604において作成された受け取りアドレスを含んでいる。

40

【0084】

ステップ608において、サーバ108は、たとえば、上述された識別方法の1つによって、引き出し当事者の同一性を検証する。サーバ108が引き出し当事者の同一性を識別できる場合、サーバ108は、ステップ610において認証証明書を作成してよい。認証証明書は、ステップ604において作成された受け取りアドレスを含んでいてよい。したがって、認証証明書は、受け取りアドレスが正しい引き出し当事者に関連付けられていることの検証を提供することができる。

【0085】

次に、認証証明書を譲渡人に提供することができ、譲渡人は、ステップ612において

50

、受け取りアドレスが正しい引き出し当事者に関連付けられていることを検証することができる。検証後、譲渡人は、ステップ614において、引き出しを承認および／または開始してよい。

【0086】

図7を参照すると、フローチャートは、ライトニングネットワークにおいてチャンネルを確立するためのプロセス700を示している。ステップ702において、ライトニングIDを有する新しいライトニングノードが作成される。新しいライトニングノードのエンティティは、サーバ108がステップ704において、認証証明書を作成することを要求することができる。この要求は、新しいノードIDを含み得る。

【0087】

ステップ706において、サーバ108は、たとえば、上述された技術の1つを使用することによって、検証を要求するエンティティの同一性を検証することができる。同一性が検証されると、ステップ708において、サーバ108は、認証証明書を作成することができ、これは、新しいライトニングノードに関連付けられたエンティティの同一性を検証し、新しいライトニングノードIDを検証されたエンティティに関連付ける。

【0088】

ステップ710において、認証証明書を他のライトニングノードに提供することができ、これは次にステップ712において、新しいライトニングノードの同一性を検証してよい。ステップ714において、他のライトニングノードは、新しいライトニングノードでチャンネルを開いてよく、ステップ716において、このチャンネルを介して新しいライトニングノードでのトランザクションを開始してよい。

【0089】

図8を参照すると、例示的なコンピューティングシステム800が、上述のプロセスおよび方法の幾つか、全部または一部を実施するために使用されてよい。たとえば、コンピューティングデバイス102および104およびサーバ108は、コンピューティングシステム800の変形を含んでいてよい。これらのデバイスは、ブロックチェーンを維持および作成し、ブロックチェーントランザクションを実行し、たとえば、上述のように、同一性およびアドレスを検証する方法を実施してよい。

【0090】

コンピューティングシステム800は、プロセッサ802（プロセッサ110と同じであってよい、または類似していてよい）、ランダムアクセスメモリ（RAM）804および記憶装置806を含んでおり、記憶装置806は、ハードドライブ、CD、DVD、フラッシュドライブまたは任意の他の種類の不揮発性メモリであってよい。ソフトウェア命令は、RAM804および／または記憶装置806に格納されてよい。プロセッサ802は、プロセッサ802がソフトウェア命令を読み取ることができるように、記憶装置806および／またはRAM804に結合されていてよい。プロセッサ802がソフトウェア命令を読み取るとき、ソフトウェア命令は、プロセッサ802に、磁気ターゲットの位置を計算するために、上記のような操作を実行させてよい。図示されていないが、プロセッサ802および／またはシステム800は、センシング要素からの信号を受け取るための入力、GPIO、電力入力等の他の入力および出力、またはUSB、SATA、HDMI等の他のインターフェースを含んでいてよい。

【0091】

上記のシステムおよび技術は、任意のブロックチェーントランザクションに含まれているエンティティの検証のためのものであり得る。たとえば、公的に信用されているX.509デジタル証明書によって、ユーザー（およびソフトウェアウォレットおよびハードウェアウォレット）は、特定のブロックチェーンアドレスが、中間者ではなく目的の受取人によって実際にコントロールされていることを検証することができる。ソフトウェアウォレットまたはハードウェアウォレットは、受取人の同一性を検証するために、X.509デジタル証明書を使用することもできる。

【0092】

10

20

30

40

50

上記のシステム、デバイスおよび方法は、理解および例示を目的として示されている例示的なシステム、デバイスおよび方法である。これらのシステム、デバイスおよび方法の変形は、本開示の範囲内である。同等のシステム、デバイスおよび方法も、本開示の範囲内にある。図示され、本開示に記載されているフローチャートは、必ずしも、ステップの特定の順序を必要としない。また、同じ結果または同様の結果をもたらす、本開示の範囲内にとどまるために、必要に応じて、様々なステップを追加、削除、再配置および並べ替えることができる。

【0093】

本特許明細書において、様々な実施形態を記載した。しかし本特許請求の範囲は、記載された実施形態に制限されるべきではなく、むしろ、後続の特許請求の範囲の主旨および範囲によってのみ制限されるべきである。本特許明細書において挙げられたすべての参照は、その全体において、参照によって組み込まれている。

10

【図 1】

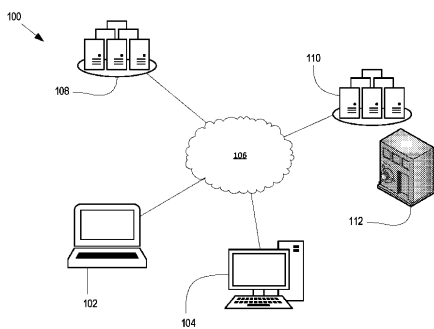
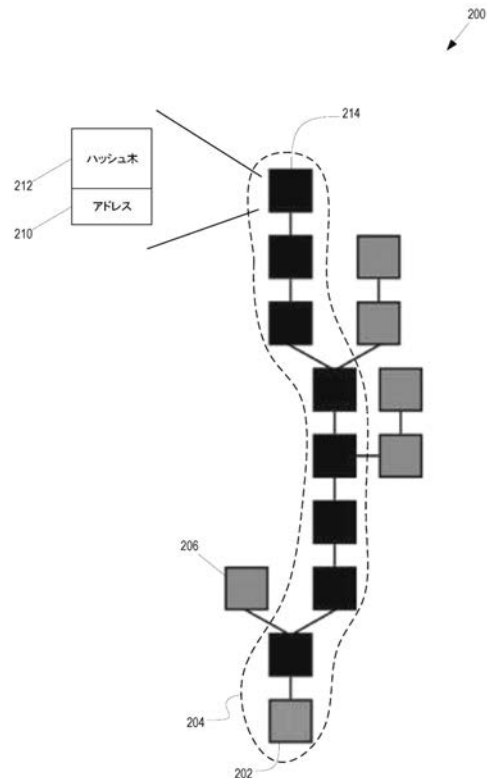
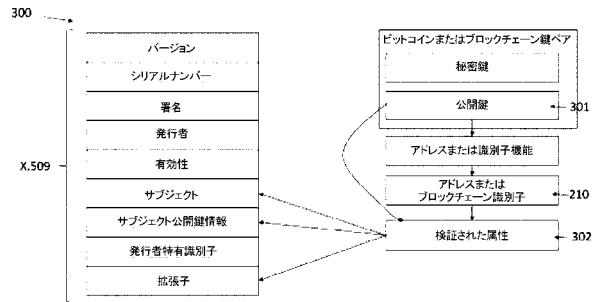


FIG. 1

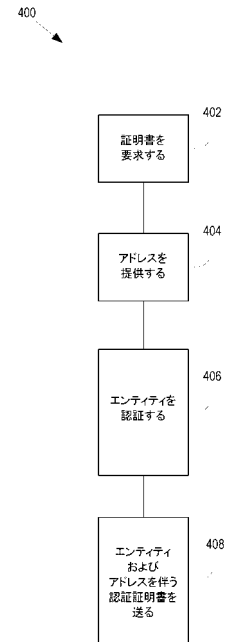
【図 2】



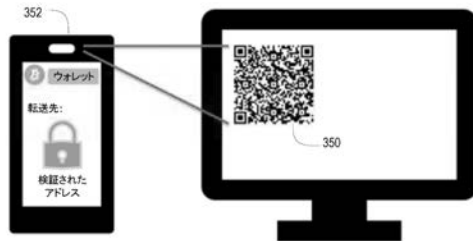
【図 3】



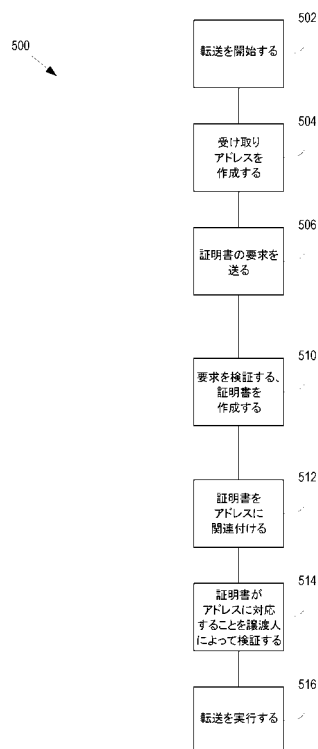
【図 4】



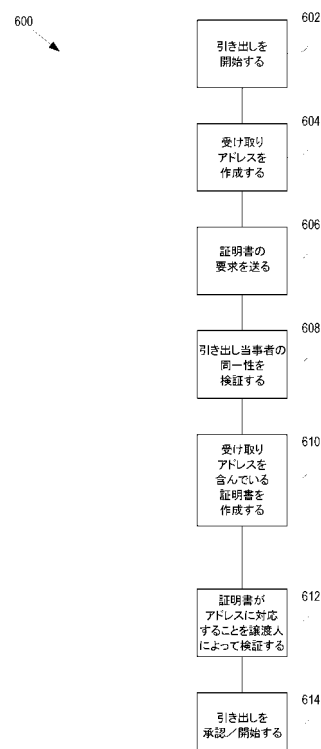
【図 3 A】



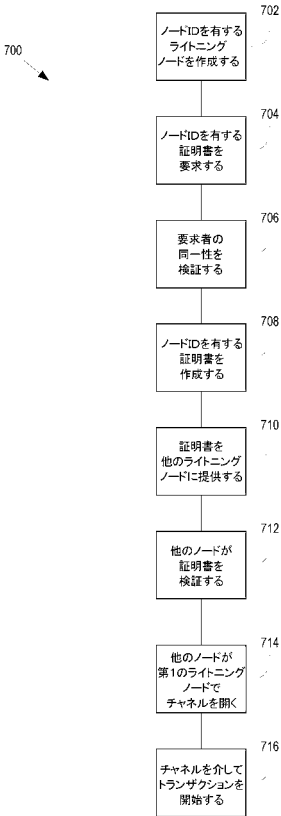
【図 5】



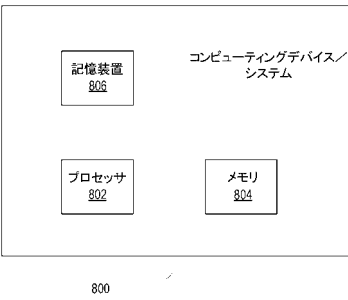
【図 6】



【図 7】



【図 8】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2019/040646

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06Q20/38
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q

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)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TANAS CRISTIAN ET AL: "An Integrated Reward and Reputation Mechanism for MCS Preserving Users' Privacy", 21 September 2015 (2015-09-21), INTERNATIONAL CONFERENCE ON COMPUTER ANALYSIS OF IMAGES AND PATTERNS. CAIP 2017: COMPUTER ANALYSIS OF IMAGES AND PATTERNS; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER, BERLIN, HEIDELBERG, PAGE(S) 83 - 99, XP047358358, ISBN: 978-3-642-17318-9 abstract PaySense: An Integrated Privacy Preserving Solution for Reward and Reputation; paragraph ["4."] ----- -/-	1-21

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"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

"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

"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

"Z" document member of the same patent family

Date of the actual completion of the international search

17 September 2019

Date of mailing of the international search report

26/09/2019

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel: (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Bruegelmans, Jan

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2019/040646

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Duane Wilson ET AL: "From Pretty Good To Great: Enhancing PGP using Bitcoin and the Blockchain (FULL VERSION)", 21 August 2015 (2015-08-21), XP055594712, Retrieved from the Internet: URL:https://arxiv.org/pdf/1508.04868.pdf [retrieved on 2019-06-06] abstract Bitcoin-Based PGP Certificates; paragraph ["2.2"] -----	1-21
A	US 2015/220917 A1 (AABYE CHRISTIAN [US] ET AL) 6 August 2015 (2015-08-06) abstract; figures -----	1-21
A	US 2015/371224 A1 (LINGAPPA PHANEENDRA RAMASESHU [US]) 24 December 2015 (2015-12-24) abstract; figures -----	1-21

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2019/040646

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015220917 A1	06-08-2015	AU 2015214271 A1	21-07-2016
		CA 2936985 A1	13-08-2015
		CN 105960776 A	21-09-2016
		EP 3103084 A1	14-12-2016
		US 2015220917 A1	06-08-2015
		WO 2015120082 A1	13-08-2015

US 2015371224 A1	24-12-2015	NONE	

フロントページの続き

(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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT

(特許庁注：以下のものは登録商標)

1. QRコード
2. HDM I
3. ビットコイン

(74)代理人 100135633

弁理士 二宮 浩康

(74)代理人 100162880

弁理士 上島 類

(72)発明者 ウィロウ ヌーナン

アメリカ合衆国 ニューハンプシャー ポーツマス インターナショナル ドライヴ 2 スイート 150

(72)発明者 ランセン ラチャンス

アメリカ合衆国 ニューハンプシャー ポーツマス インターナショナル ドライヴ 2 スイート 150

(72)発明者 ルーク ファン デン ブルーク

アメリカ合衆国 ニューハンプシャー ポーツマス インターナショナル ドライヴ 2 スイート 150

Fターム(参考) 5L055 AA71