Apostille

アポスティーユ

ブロックチェーンの公証・タイムスタンプサービス
追跡・アップデートが可能で、タイムスタンプの押された共同所有の公証を行うことができます。

著者
J・マクドナルド（啓明大学助教授）E-mail: jeff@ournem.com
J・オリベリオ（ナノウォレット開発者）E-mail: oliverio.j@outlook.com

2016年11月1日
初版（v.1.0）

概要：ブロックチェーンの世界には多くのタイムスタンプサービスが様々な形で存在しています。しかしそうしたサービスのほとんどが、単純な第一世代のシステムを使いドキュメントをハッシュ化してフィンガープリント値を得て、その後にトランザクションを行いブロックチェーン上でそのフィンガープリントにタイムスタンプを押すというようなものです。

それらは一度限りの固定されたトランザクションであり、そのため最終的には後に監査できるようにブロックの中に収容されるにすぎません。こうした1.0のタイムスタンプはアップデートできませんし、あるオーナーから別のオーナーへと送ることもできません。そのタイムスタンプに付加価値や利点はないのです。アポスティーユは最初の2.0ブロックチェーンの公証サービスなので、こうした問題を解決して、新しい機能とビジネスチャンスを提供することができます。

目次

1.はじめに

その存在を証明し、それを誰かが所有しているということを証明するためにドキュメントにタイムスタンプを押すという考えは、ブロックチェーン登場のはるかに以前から存在しました。しかしビットコインの発明により、多くの人々がブロックチェーンはタイムスタンプサービスに非常に適していると考えるようになりました。

あるドキュメントについてのハッシュ化したフィンガープリントにタイムスタンプを刻印してブロックチェーンに記録するという方法は、Proof-of-existence(PoE)として知られています。もっとも初期のもので有名なサービスは、proofofexistence.comであり、2012年に開始したオープンソースのウェブサイトです。

ユーザーは自分のドキュメントをドラッグ・アンド・ドロップして、そのドキュメントのフィンガープリント値を示すハッシュを入手し、それにビットコインのブロックチェーン上でタイムスタンプを押してもらうことができます。PoEの開始以来、他の多くのサービスが登場しました。多少の改善が加わっていたり、安価な手数料のものもありましたが、それらはおおよそ同じ計算式に依拠しています。それらは一度限りのタイムスタンプであり、その過程でユーザーはドキュメントをアップロードしてそれをチェーン上に刻印します。それらのサービスにはそうした使用方法しかありません。

ブロックチェーン外の公証においては伝統的に、公証人は紙の書類を検証してそれに刻印をすることで、その内容に偽りがないことを公に証明してきました。それらの公証人が権限を持つのは、彼らが世界の政府に公証人として登録されており、それにより根拠を与えられているからです。しかしブロックチェーンの発明により、ブロックチェーン上でドキュメントのフィンガープリントにタイムスタンプを押す作業を、「ブロックチェーンによる公証」の一種として考えることが可能となりました。つまり政治的な意思により裏付けされているのではなく、ブロックチェーンの分散型ネットワークにより支えられた公証制度です。

現存の法的認証と公証の制度は、世界中の政府や伝統的な機関により支援されており、ある対象の状態を検証するという作業には様々な使用用途があります。財産所有の証明、例えば自動車の所有証明、業績の証明、例えば卒業証書、証人の検証、例えば公証人の認定、商品の品質の検証、例えばA級品として認証することなどです。

こうした既存のシステムは、その証明に以下のような質を与えます。それは検証可能であり、証明されていて、第二者・第三者により品質の管理が行われていて、公的な機関に登録されており、譲渡と更新が可能であるということです。

アポスティーユはこのような以前はブロックチェーンの外部にだけ存在していた性質を、ブロックチェーンのエコシステムの内部に導入しようと試みています。これはブロックチェーンの技術における理にかなった進歩と言えます。こうした技術の中で、暗号通貨のような譲渡可能な財産という概念と、ドキュメントにタイムスタンプを刻印するという行為が組み合わされて、一つのシステムの中でそれぞれの最高の機能を発揮します。

アポスティーユはそれを、ネーミングサービス、マルチシグネイチャーのアカウントとメッセージ、そしてブロックチェーンの特性を利用して行おうとしています。それらはビットコインのようなブロックチェーン上で行うことができますが、様々なプロジェクトの様々なAPIを組み込む必要があります(その中には中央集権型のものもあります)。例えば以下のようなものです。ネーミングサービスのためのOnename、マルチシグのためのBitpay、通貨のためのカウンターパーティーとカラードコイン、そしてメッセージングのためのビットコインのトランザクションに使われるOP_RETURNの変数です。

代わりに、イーサリアムの採用を検討して、これらの機能の代わりになるスマートコントラクトを書くこともできます。しかし、NEMという2.0のブロックチェーンはこれらのサービスを、一つの普遍的なAPIを使ってデフォルトで提供することができます。そのため私たちは、それを実例として使いながら議論を進めていくことになります。

アポスティーユ(Apostille)という名前は、「証明する」「認証する」「完成させる」という意味を持つ同じ綴りのフランス語の単語に由来します。postの箇所はafterを意味するラテン語で、illaはtheseを意味し、そしてverbaはwordsを意味します。つまり語源を辿れば、アポスティーユはafter these wordsという意味を持っていると言えます。

この語は1961年のハーグ条約基づく、112カ国が署名した国際的な公証制度を創るための
アポスティーユ条約の登場により一般的に使われるようになりました。NEMは国際的な分散型の技術であり、そのためアポスティーユのアイディアに一つの工夫を加えることができます。NEMアポスティーユのトランザクションは、政治的な機関や条約に支えられて施行されている伝統的な法的公証ではありません。そうではなく、ブロックチェーンの公証は国際的に支援されたブロックチェーン上で、コンピューターのコードと暗号化技術により安全性を確保された上で施行されます。

2.NEMの機能

NEMのブロックチェーンはゼロから作り上げられた2.0プラットフォームです。理想的なブロックチェーンのあるべき姿を再現するために、企業レベルの開発者によって設計されました。そのため、どのようにNEMやアポスティーユが作動するかを十分に理解するためには、NEMの技術を紹介することが重要になります。それは多くの点で他のブロックチェーンとは異なるからです。さらに詳細なNEMテクノロジーの技術的な説明はTechnical Reportで読むことができます。

2.1.ネームスペース

NEMシステムのネームスペースはドメインを命名するものですが、インターネットのそれとは異なります。固有のルートレベルのドメインとそうではないサブドメインがあり、一般的にネーミングシステムや、完全に要件を満たした固有のアセットを分類することに使われます。このことにより、固有のルートドメインを持つ人が、様々なプロジェクトのためであったりビジネスアカウントの外部で、様々な多くのサブドメインを作ることが可能になります。また登録された名前で作ったサービスに対する評価システムを作り、維持することも容易になります。その一例がブロックチェーンより支えられている、モザイクと名付けられたNEMのアセット機能です。また他の例としてはアプリケーション開発者が作りたいと考える第三者の分散型ネーミングシステムも考えられます。

これはアポスティーユのシステムにおいて非常に有用です。というのは、それによりユーザーは法に則った法人企業が発行したブロックチェーン公証を信頼することができるからです。例えばNEMのネームスペースにより、“foo company”というネームスペースを所有することが可能になり、そうなれば他人がそのルートドメインを名乗ることはできません。ネームスペースにより発行されたブロックチェーン公証は、“foo company”からのものであると信用することができます。このようなことは例えば、高級品を作っている会社が、その商品に対する信頼性をブロックチェーン上で認証する際などに便利です。そうした証明書は信頼に足るものと言えます。なぜなら会社が自身のネームスペースをウェブサイトやパッケージの情報に記載することなどによって、証明書の発行者を誰でも明確に知ることができるからです。

2.2.モザイク—NEMブロックチェーン上のアセット

NEMのモザイクは基本的にはNEMに内在する命名されたアセットであり、第二者のレイヤー上にはありません。それらはある会社、例えば“foo company”が発行したいと考えるいかなる種類のアセットをも表すことができます。名前、説明、可分性、量などがカスタム可能であり、固定することも変更可能にしておくこともできます。

また必要であれば譲渡の制限もすることができます。それらに税金を適用したり、それ自体が他のモザイクに対する税となることもできます。

“foo company”は公証を行えるだけでなく、いかなる種類のアセットをもブロックチェーンの公証に付随させることができます。政府は「税金が支払われた」、「今年度に登録されたモザイクのアセットを作りたいと考えるかもしれません。企業は「換金可能な資金に役立つ」もしくは「会社の株式」のアセットを作り、それと公証のコントラクトとセットにしたいと考えるかもしれません。

こうした作業はアポスティーユで行うのが非常に便利です。なぜなら、多くの様々な第三者がモザイクのアセットをカスタムして、刻印し、それをブロックチェーンの公証に付随させることができるからです。

2.3.メッセージ

NEMのメッセージには三つの特徴があります。オープンであること、暗号化されていること、16進法を採用していることです。320文字(暗号化されたものは272文字)までの長さを送ることができ、必要であれば複数のメッセージを一つにまとめることもできます。

ブロックチェーンの公証が済んだのち、アップデートを記録したり、追加の情報をファイルへ保存することができるので、この機能は非常に有効です。それらは公開するか、プライベートである必要があるかもしれませんし、ひょっとすると16進法でアプリケーションのバックエンドの一部として書く必要があるかもしれません。

2.4.マルチシグ

マルチシグネイチャーとマルチユーザーのアカウントは、アポスティーユのシステムにおいて、重要で決定的な役割を果たします。他のブロックチェーンのマルチシグネイチャーのシステムは、表面上はNEMのマルチシグネイチャーのアカウントに似ています。しかし、NEMを他とは区別させるわずかな違いがあります。そうした違いのおかげで、アポスティーユのシステムをNEMに作ることが可能になるのです。

NEMのマルチシグはチェーン上のコントラクトにより作動します。他のブロックチェーンのシステムとは異なり、他のアカウントのパブリックキーを組み合わせることでは新しいアカウントは作ることができません。そうではなく、すでに存在し出資されたアドレスがマルチシグネイチャーのアカウントに変換され、連署人がそこに割り当てられるのです。連署人はm-of-nの組合せで割り当てることができ、その際mとnはそれぞれ1から32までの数字です。ここにはアポスティーユにとって非常に重要な1-of-1のマルチシグネイチャーのコントラクトも含まれます。

NEMにおいては1-of-1のマルチシグネイチャーのアカウントが可能となります。なぜならマルチシグアカウントへと変換されているアカウントは、そのプライベートキーが無効化されており、そのことは該当アカウントがもはやトランザクションを行う権限がないことを意味しているからです。連署人のプライベートキーだけが、マルチシグ化されたアカウントを代表してトランザクションを始めることができます。したがって、NEMのマルチシグで実装されたアカウントは、親/子アカウントのようなものとして考えることができます。つまり、親アカウントが連署人であり、彼らが子アカウントに対してトランザクションを行うように指示するのです。

このことは非常に有用です。というのはブロックチェーン公証を代表する専用アカウントが、ブロックチェーン公証をアップデートするためにメッセージを受け取ることができるからです。また、専用アカウントに送られた、重要性があったりブロックチェーン公証にステータスを付与するアセット/モザイクを受信することもできます。NEMのマルチシグネイチャーのわずかでありながら決定的な利点は、専用のブロックチェーン公証が人から人へ譲渡可能だということです。

マルチシグのコントラクトの作成

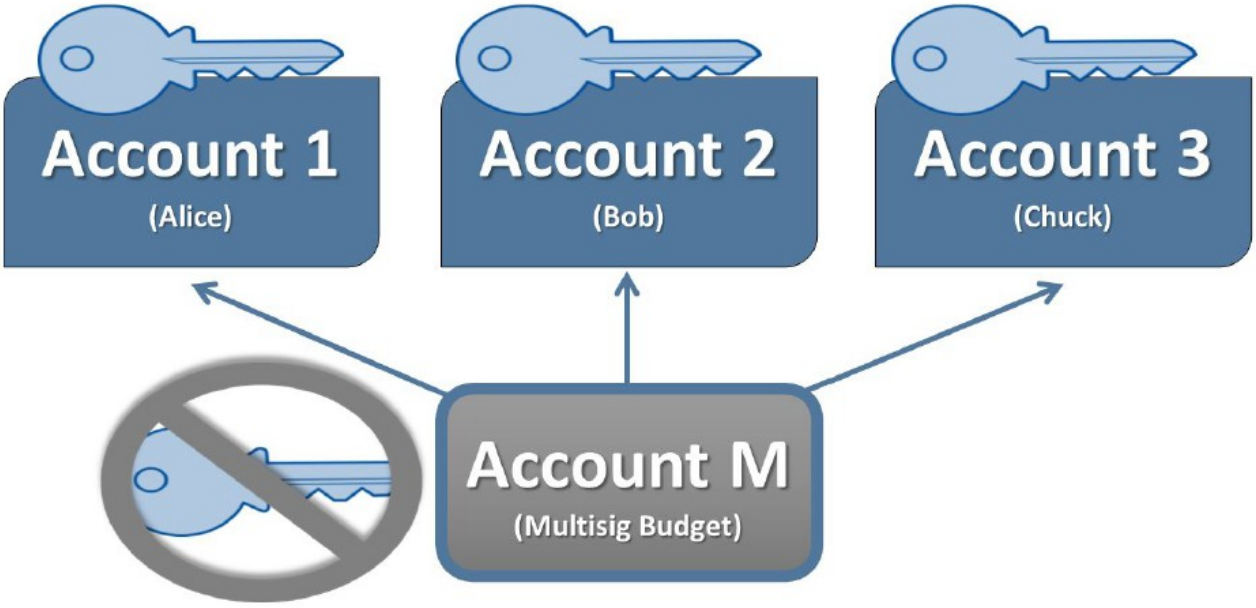

図1 マルチシグのコントラクトの作成。マルチシグアカウントMのプライベートキーはもはや重要ではなく、使用されません。一方で、Alice、BobそしてChuckはアカウントMに対して管理者としての権限を持ちます。

マルチシグのコントラクトの編集

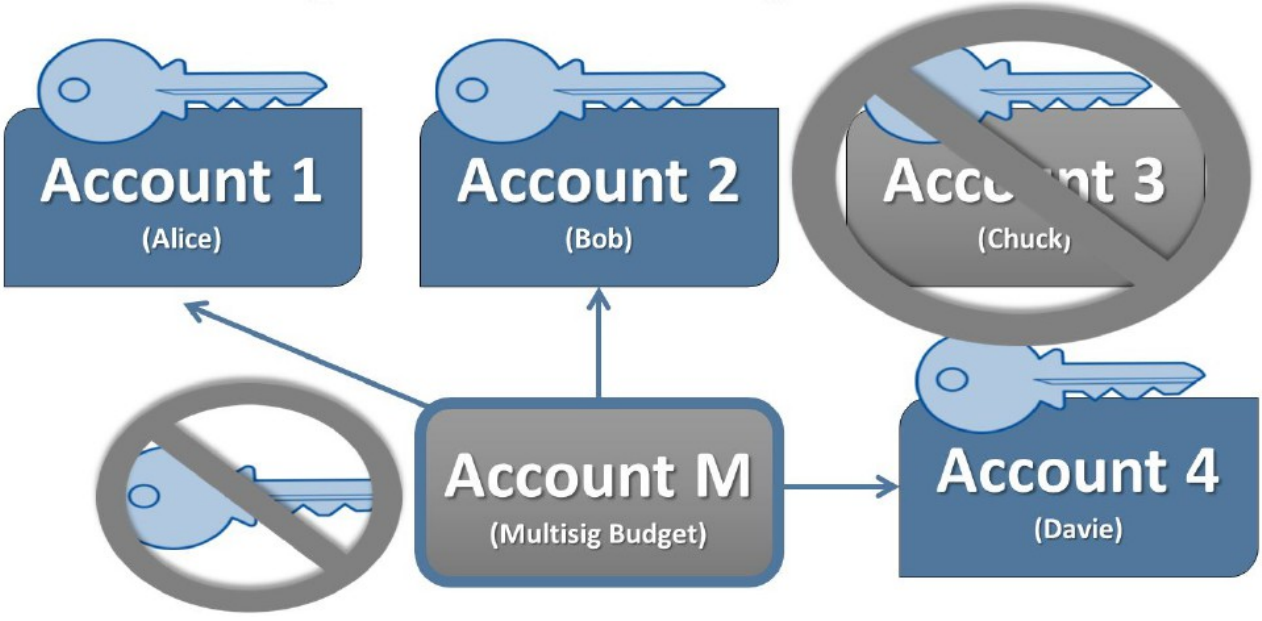

図2 マルチシグのアカウントの編集。数クリックするだけで、Chuckのアカウントを削除し、Davieのアカウントを追加することができます。

3.アポスティーユのシステム

このホワイトペーパーを読めば分かるように、これまでのところアポスティーユは多くの様々な機能を使って総体的なブロックチェーン公証のシステムを作り上げようとしています。そのシステムでは公証は静的な一度限りのタイムスタンプではなく、動的で、移動し、変化するものであり、ブロックチェーン上で更新可能な価値を持つ存在なのです。

もしビットコインのカラードコインのシステムに詳しいのであれば、アポスティーユのシステムを理解することは容易となります。ビットコインにおいてはカラードコインは、1Satoshiを使いそれを自動車所有証明といった要素にタグ付けし、その後にそのSatoshiをブロックチェーン上に送信し、それを追跡し色づけされた時刻とリンクさせることができるようにすることで作られます。この場合、自動車所有証明という指定で、Satoshiを色づけしようとしていることになります、そしてそれは先見の明あるコンセプトではありますが、不運なことに、第二のレイヤーとして作られており、ビットコインの組織とウォレットがそれを実装するのは大変骨の折れる作業なのです。

NEMのアポスティーユは同じコンセプトを提示しますが、それをSatoshiではなく、アカウントへ適用します。**それらのアカウントはカラードアカウントとして考えることすら可能であり、データ値のまとまりをトークン化することにはるかに適していて有用なものです。そして作り手が表したり、送信したり、アップデートしたいと考えるものを、何でも表現することができます。そもそもコインを情報で色づけすることは意図されていません。**ビットコインはピアツーピアの電子マネーのシステムとして設計されましたが、その場合に重視されているのは「マネー」であり、ピアツーピアのメッセージ交換システムではないのです。

一方でNEMブロックチェーンのアカウントはデフォルトでメッセージ機能とモザイク(アセット)が内蔵されており、マルチシグのコントラクトを経由して人から人へ譲渡できるように設計されています。それらは最初から、ただのアドレスよりもはるかに優れたものを意図して作られました。そしてこれらはすべてNEMのブロックチェーンのサーバーにより支えられたAPIsを使って行われるので、NEMブロックチェーンのエコシステムとすべてのNEM Walletにおいて普遍的なものとなります。いかなる第三者のAPIsも必要とはなりません。さらに、未使用出力(ビットコインに内蔵のUXTO)がないことによって、それが可能になります。

3.1.ブロックチェーン公証のアカウント開始の準備

いかなるアカウントもブロックチェーン公証を開始することができますが、ネームスペースを持ち、それを自社のウェブサイト、冊子、パッケージ情報などに記載しているアカウントであることが望ましいです。これは選択自由であり必須の条件ではありませんが、ブロックチェーン公証に妥当性を与える手助けとなります。特に消費者が「私はこの会社を信頼することができる。そしてこの会社だけがこのネームスペースを使用することができる。したがって、このネームスペースにより発行されたブロックチェーン公証はこの種の製品の公式の公証だと信用することができる」と考える場合に有効です。

3.2.アポスティーユ公証の種類

アポスティーユのシステムでは、ビジネスでの使用用途や個人的なニーズに応じて二つの異なる種類の公証から選ぶことができます。

- パブリック：平易なハッシュがパブリックなシンクのアドレスに送られます。これはフィンガープリントが取られタイムスタンプが押されたドキュメントを自由に共有したいときに有効です。

- プライベート：ハッシュは所有者のプライベートキーを使って署名され、ファイル専用のプライベートキーから作られたカラードHDアカウントへ送られます。これは公証されたドキュメントの内容を私的なものに留めておきたい場合、またはそれを更新や譲渡が可能な状態にしたり、共同で所有できるブロックチェーン公証を作りたい際に有効です。

3.3.ファイル専用のプライベートキーの作成―HDアカウントの色付け

階層的決定性のアカウント(HDアカウント)はファイル名から作られ、SHA-256を使ってハッシュ化され、その後にユーザーのプライベートキーで署名されます。

最後の署名されたハッシュは切り捨てられ、ファイル専用のプライベートキーに割り当てられた最初の64文字が維持されます。ファイル専用のプライベートキーはハッシュ化されたファイル名から作られるため、常に送信者ごとに固有のものであり、ただランダムなアカウントのプライベートキーというだけでなく、そのファイル特有のものであると考えることができます。ファイル専用のプライベートキーを使って、HDアカウントを作る場合、そのアカウントが色付けされたものとみなすことができます。例えば、自動車所有証明のためのブロックチェーン公証を発行したい場合、その場合のHDアカウントの色付けは「自動車所有証明」となります。

作業を開始しているアカウントとファイルのオーナーだけが、カラードHDアカウントを作るファイル専用のプライベートキーを回収することができます。そしてそれは常にあるファイル名に対して同じアカウントを生成します。

名前の決定方法は以下の通りです。

HDprivateKey =
truncate(userKeyPair.sign(SHA256(fileName)));

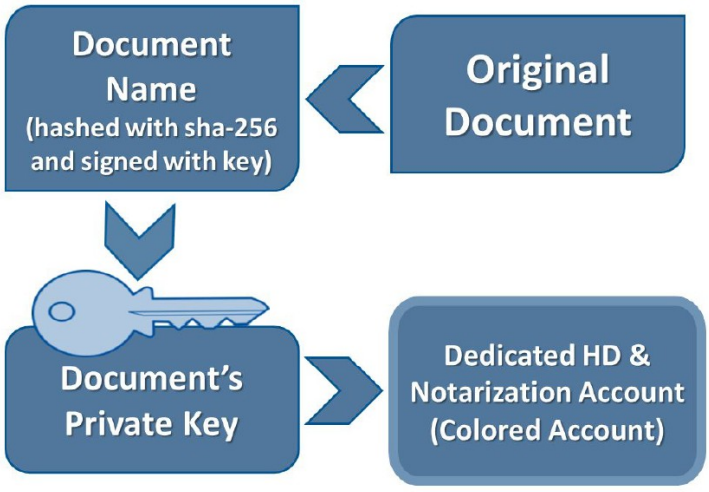

図3 後に専用のプライベートキーを作るドキュメントの名前やアカウント情報から、カラードHDアカウントを作る過程。

3.4.アポスティーユのハッシュ―タイムスタンプやフィンガープリントの用意―ブロックチェーン公証の実行

アポスティーユのトランザクションにおける、アポスティーユのトランザクションのメッセージは、チェックサムがプリペンドされたファイルデータ(ドキュメントのフィンガープリント)のハッシュです。チェックサムにより検証の最中に、使用されているハッシュのアルゴリズムを判別し、そのハッシュが署名されているかどうかも判断することができます。その過程は以下の通りです。

ApostilleHash = checksum + fileContentHash;

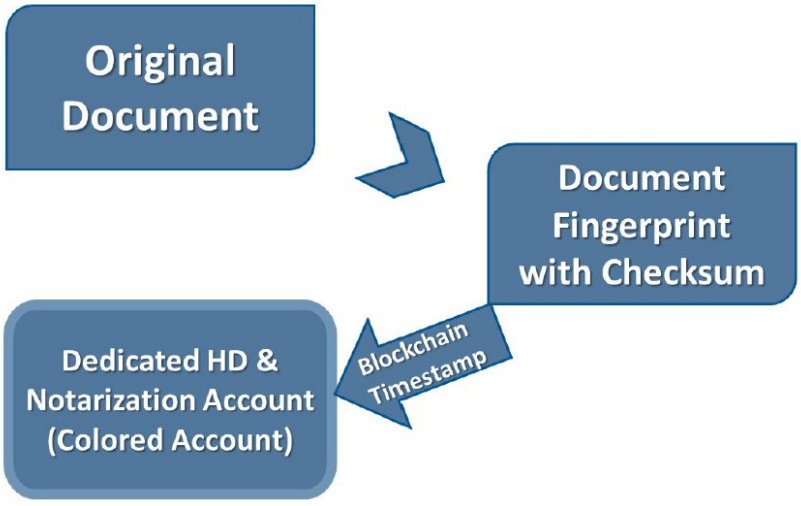

図4 アポスティーユのトランザクションのメッセージを作るプロセス。ドキュメントのフィンガープリントとチェックサムがメッセージを介して専用のHDアカウントへ送られます。

プライベートなアポスティーユのブロックチェーン公証を実行する、全プロセスは以下のようになります。

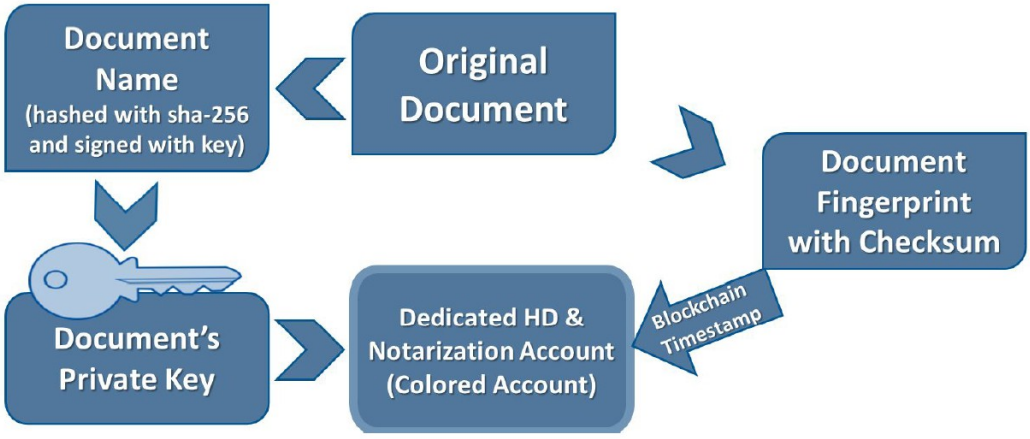

図5 ドキュメントのプライベートキー、またそのキーから専用のHDアカウントを作り、さらに元のドキュメントのフィンガープリントを生成するプロセス。そのアカウントはブロックチェーン上でタイムスタンプを押されたので、その後はブロックチェーン公証のアカウントとなります。

3.5.ハッシュの違い

アポスティーユではユーザーはブロックチェーン公証を行う際に、二つの異なる選択肢から選ぶことができます。パブリックとプライベートです。さらに、ハッシュ化のアルゴリズムのリストからも選択をすることができます。ユーザーの選択により以下のような様々なハッシュが生まれることになります。

- Non-signed (public):
  xFE 'N' 'T' 'Y' 0x01 + md5(data)
  0xFE 'N' 'T' 'Y' 0x02 + sha-1(data)
  0xFE 'N' 'T' 'Y' 0x03 + sha-256(data)
  0xFE 'N' 'T' 'Y' 0x08 + sha3-256(data)
  0xFE 'N' 'T' 'Y' 0x09 + sha3-512(data)

- Signed (private):
  0xFE 'N' 'T' 'Y' 0x81 + sign(md5(data))
  0xFE 'N' 'T' 'Y' 0x82 + sign(sha-1(data))
  0xFE 'N' 'T' 'Y' 0x83 + sign(sha-256(data))
  0xFE 'N' 'T' 'Y' 0x88 + sign(sha3-256(data))
  0xFE 'N' 'T' 'Y' 0x89 + sign(sha3-512(data))

NEMのハッシュは十六進法でメッセージを解釈するために、oxFEという文字列で始まります。

N、TそしてYはNotary(公証人)を表し、以下のように十六進法に則って変換されます。

- N: 0x4E
- T: 0x54
- Y: 0x59

両方の公証に共通するチェックサムはFE4E5459です。チェックサムの末尾二つの16進法の数字はユーザーにより決定されます(ハッシュ化の方法や、署名されているかいないかなど)。

例えば、

- SHA-256を使ってハッシュ化した署名されていないファイルのチェックサムはFE4E545903となります。
- MD5を使ってハッシュ化した署名されたファイルのチェックサムはFE4E545981となります。

署名されたSHA-256方式のファイルのハッシュ例：
79952024fa6fd302abda4dfef63b1499b786c4269305bbf08d4058
b417a528421d4f877c5a00d34e2addeba650b23812777448f22265
15c801e4a424eefa6e04

また別のハッシュの例：
Now with added checksum example:
fe4e54598379952024fa6fd302abda4dfef63b1499b786c4269305
bbf08d4058b417a528421d4f877c5a00d34e2addeba650b2381277
7448f2226515c801e4a424eefa6e04

3.6.ブロックチェーン公証の監査

あるファイルを監査するためには、公証済みドキュメントのファイルを特定のフォーマットに従って命名しておく必要があります。アポスティーユの公証を受けるドキュメントはファイル名を編集され、そのまま編集せずに安全に保管できるようにZipフォルダーでユーザーに返送されます。専用のネーミングフォーマットは以下の通りです。

> *<Filename> - Apostille TX <transaction hash> -- Date YYYY-MM-DD.pdf*

元のドキュメントファイル名の例：MyProject2016.pdf

ハッシュ化されたドキュメントファイル名の例：MyProject2016 - Apostille
TX 0e94da29910ae64bb544e9de0e6a5c6440bd75e6bedafd81b5b
4cf729ca25ef -- Date 2016-09-12.pdf

ユーザーがこのファイルを監査に送った場合、そのファイル名は分解されて、トランザクションのハッシュを使ってブロックチェーン公証が取り出されます。

私たちはそのトランザクション内のメッセージを取りだし、チェックサムをカットしてそれを分析します。

チェックサムから読み取った情報を使い、ユーザーがアポスティーユの公証の際にどのアルゴリズムを選択したかを知ることができます。そのため監査済みのファイルをハッシュ化する際にも、適切な方法を使用し、もし(チェックサムなしの)トランザクションのメッセージのハッシュと一致するのであればブロックチェーンを固定することができます。

パブリックな公証のように、ハッシュが署名されていないのであれば、単にアップロードされたファイルのハッシュが、トランザクションのメッセージのもの一致しているか認証します。

プライベートな公証のように、ハッシュが署名されているのであれば、署名者のプライベートキー、(トランザクションのメッセージ内の)署名されたファイルのハッシュそしてアップロードされたファイルのハッシュを使用し、その署名を認証します。

3.7.ブロックチェーン公証のカラードHDアカウントの管理権譲渡

カラードHDアカウントに対する公証済みファイルの専用プライベートキーは、そのブロックチェーン公証を行った人だけが知っているので、所有者は自由にそのアカウントを1-of-1のマルチシグネイチャーのアカウントもしくは任意のm-of-nの組み合わせに変更することができます。

1-of-1のマルチシグネイチャーのコントラクトは、ブロックチェーン公証を行う人がその専有を希望し、それを単独の第三者へと渡したい場合にもっとも有効な手段となります。n-of-nのマルチシグネイチャーアカウント(nが2以上)は、共同で所有したり共有したいコントラクトを作る場合、また複数の関係者間で拘束力のある合意を行う場合に適しています。

NEMのマルチシグネイチャーのコントラクトは数クリックで制作・編集が可能です。そのコントラクトはすべてNEMブロックチェーンサーバーの同じコアAPIを使用しているため、NEMシステム内部のすべてのウォレットにより支援されます。同様にアカウントを削除したり、カラードHDアカウントの親/子アカウントとして追加で作成を行うことも数クリックで可能です。自分たちのアカウントアドレス以外は、いかなる情報も新しいブロックチェーン公証のアカウントの所有者と交換する必要はありません。スマートコントラクトを書いたり、特定の第三者のウォレットを使う必要もありません。

ステップ1：マルチシグネイチャーコントラクト制作以前の公証アカウント

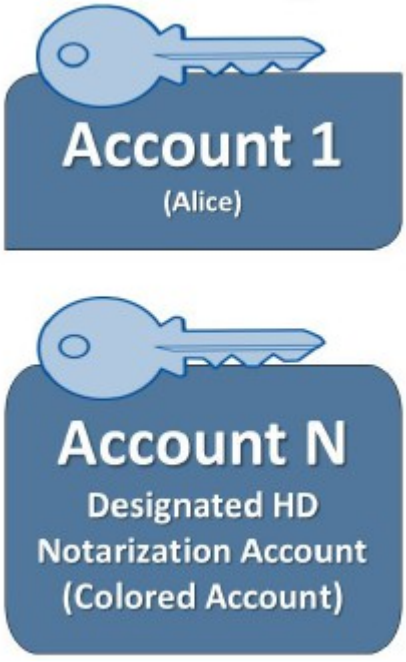

図6：この図は、公証アカウントが既に作られ、ファイルのフィンガープリントのハッシュでスタンプが押された状態です。このファイルの専用プライベートキーはアカウントNを作成するために使用されますが、この時点ではそのアカウントに対するマルチシグネイチャーのコントラクトはありません。

ステップ2：マルチシグネイチャーコントラクト制作後の公証アカウント

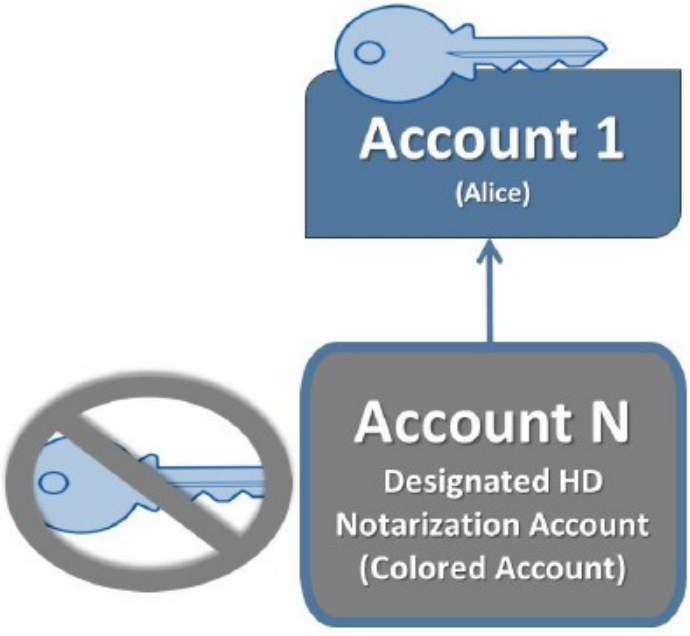

図7：この図ではアカウントNが1-of-1のマルチシグネイチャーのアカウント下に置かれています。ここではAliceはその公証アカウントの完全な管理権限を持っています。アカウントNのプライベートキーではもうトランザクションを始めることはできません。

ステップ3：第三者に譲渡された公証アカウント

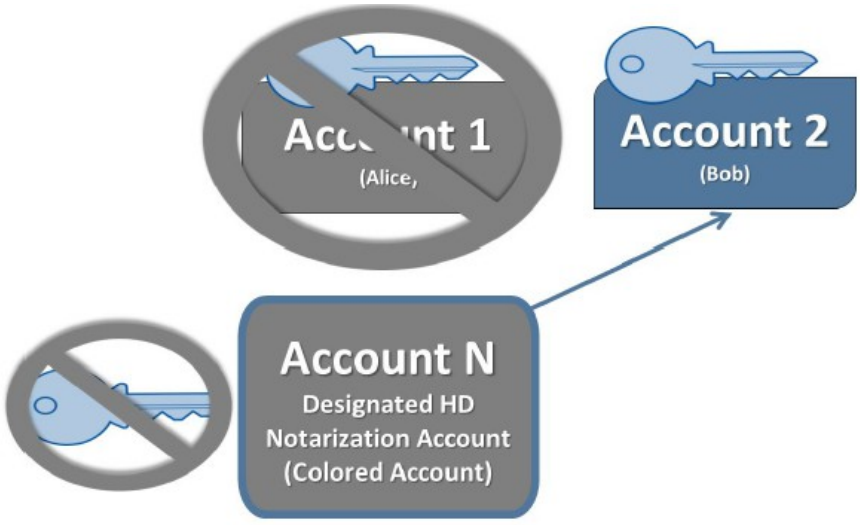

図8：この図では、AliceはアカウントNの管理権をBobに譲渡しようと決定しました。数クリックで行える一度のトランザクションで、Aliceは自身のアカウントを削除してBobを追加することができます。この状態ではBobがアカウントNの完全な管理権限を持っています。

3.8.ブロックチェーン公証のアップデート

ブロックチェーンをアップデートする方法は二つあります。ひとつは、完全に新しいバージョンのドキュメントを公証することです。もうひとつは、HDのカラードアカウントにメッセージを送り、元の公証の修正をすることです。後者の方法は、公証済みの製品について継続的に注釈を追加する必要がある場合にも便利です。

しばしばドキュメントや製品は認証後に変化することがあります。公証済みのアイテムが拡張された場合、変更を反映するメッセージをブロックチェーン公証のカラードHDアカウントへ送ることができます。

ブロックチェーン公証のカラードHDアカウントが第三者に譲渡されているケースでは、その製品に対する拡張を行った第三者が、その製品に対する変更を示すメッセージを、ブロックチェーン公証のカラードHDアカウントからそのアカウント自身に対して送信することができます。

そのアカウントの所有者でも作成者でもない登録・認証済みの第三者が、ある製品に変更を加えてそれを記録したい場合もあるでしょう。その場合には、彼らの個人アカウントからブロックチェーン公証のカラードHDアカウントへ、加えた変更を書いたメッセージを送ることができます。理想的にはその第三者のアカウントをネームスペースに登録し、評価システムに役立ててほしいところですが、それはあくまで任意です

3.9.多者間のコントラクト認証―多者により開始され、署名され、アップデートされ、管理され、そして譲渡される公証―

ブロックチェーン公証が明確に有効なケースとして、多者間でコントラクトを作成して、それに共同で署名をし、そのフィンガープリントをブロックチェーン上にアップロードするというものが考えられます。これらの行為は、署名時にすべての当事者がそのコントラクトに同意していたことの証明になります。

アポスティーユでは、それもまた可能です。もっともスマートな方法は、登録済みのアカウントでコントラクトに署名ができるように、それぞれの当事者が自分たちのネームスペースを所有することです。しかしこれは必須の条件ではありません。

ネームスペースが使用されているかに関係なく、そのプロセスは同じです。コントラクトに同意するすべての当事者は、アポスティーユのトランザクションを開始するのに使われるアカウントに対するマルチシグのコントラクトを作成します。そのアカウントはn-of-nのコントラクトの管理下に置かれ、そのアカウントが発行するブロックチェーン公証はすべて、全当事者によって署名されていなければなりません。NEMではこの作業は、ブロックチェーンのネットワークを通じプッシュ通知をライトクライアントに送り、署名する意思があるかどうか確認するという方法で行われます。

アポスティーユのトランザクションから作られたブロックチェーン公証のカラードHDカウントは、最初は他の普通のアカウントのようなものにすぎません。しかし、公証済みのファイルの専用プライベートキーを知った後には、ブロックチェーン公証のカラードHDアカウントをマルチシグに加え、その適切な所有者を連署人として設定することができます。

これらの連署人はその手続きの後、チェンーン上でそのアカウントへのトランザクションにすべての連署人に署名をしてもらうことで、コントラクトのアップデート、拡張そして期間の延長などを行うことができます。

3.10.プライベートおよびパブリックなブロックチェーン—Mijinのためのアポスティーユ

これまでのところ、このホワイトペーパーでは主にNEMのパブリックなチェーン上でアポスティーユを使用することについて論じてきました。しかしNEMにはその姉妹にあたるブロックチェーン技術があります。それはテックビューロ社により運営されているMijinというプライベートなブロックチェーンです。MijinとNEMはそれぞれ異なるニーズに応えるように設計されているものの、基本となるコードの大部分と同じAPIsのすべてを共有しています。そのためNEMのアポスティーユで稼働するアプリケーションはすべて、コードを僅かに修正するだけでMijin上でも稼働させることができます。

このペーパーが書かれた時点では、現行のMijinは100's tx/sで稼働しています。次世代のMijinとNEMのコアのアップデートバーションは"Catapult（カタパルト）"というコードネームが付けられ、プライベートなチェーンのテストネット上で1000's tx/sで現在稼働しています。これは初の三層構造のブロックチェーン技術で、その三つの層はそれぞれ、ブロックチェーン、APIサーバー、ライトクライアントに充てられ、他のブロックチェーンのプロジェクトをはるかに上回る規模の成長を可能にします。

アポスティーユの公証に使用されるMijinのプライベートなチェーンは、NEMのパブリックなチェーンにも備え付けることもできます。このプロセスによって、Mijinのチェーンのハッシュそれ自体が、NEMのパブリックなチェーン上で公証されるのです。これによりMijinチェーンのユーザーと監査者そしてその中でのブロックチェーン公証に、パブリックチェーンを直接使用した時と同じレベルの普遍性が保証されます。

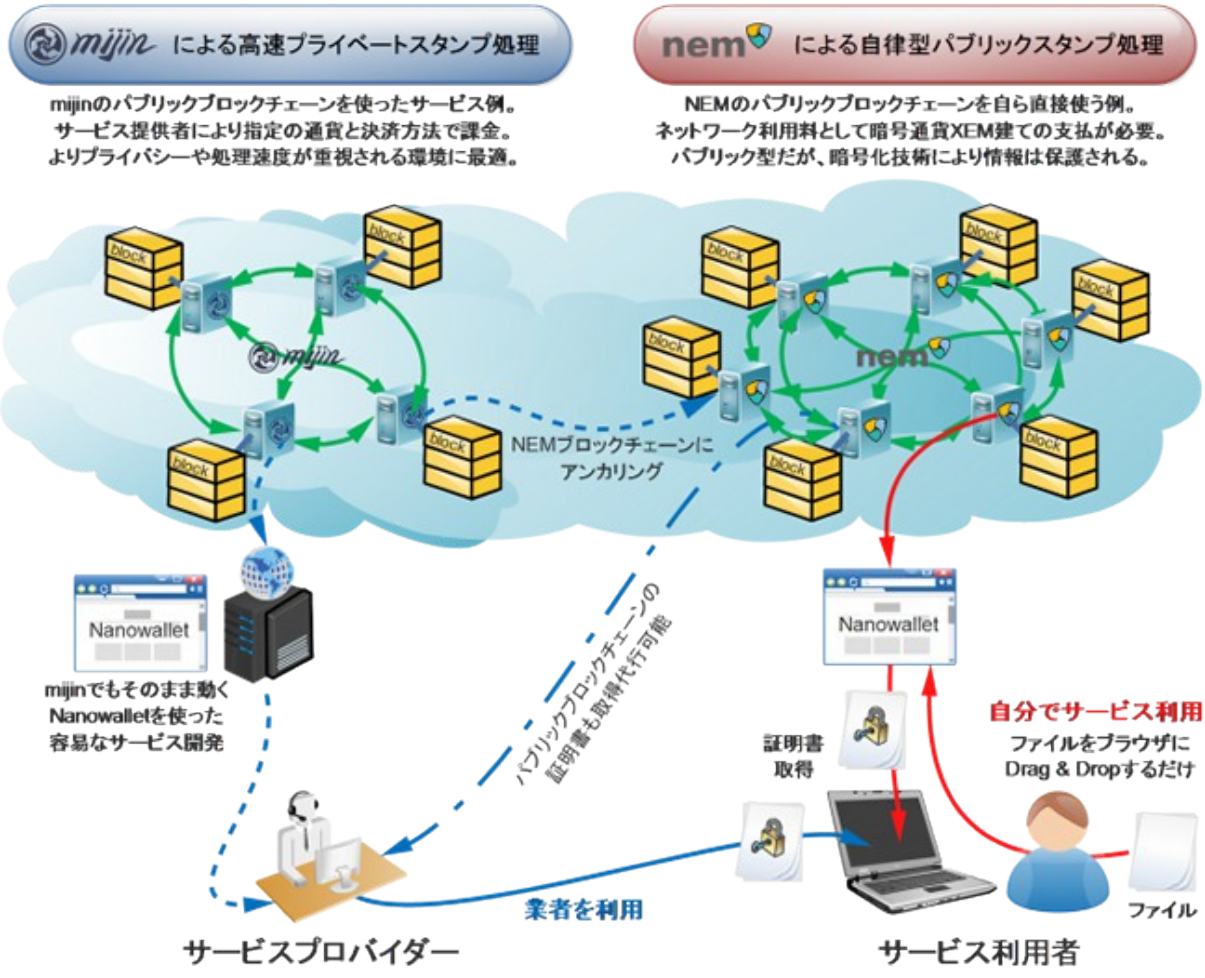

図9：NEMのアポスティーユシステムを使用するMijinとNEMのブロックチェーンネットワーク。
イメージ出典：テックビューロとNEMが、所有権が移転可能な世界初のブロックチェーン証明書発行ツール『アポスティーユ』を無償公開

4.使用用途（ユースケース）

以下の使用用途をご覧いただければ、アポスティーユの公証システムの便利さと応用範囲の広さがお分かり頂けると思います。

4.1.自動車所有証明

所有権の証明がブロックチェーンで公証された自動車については、そのカラードHDアカウントに、修理やメンテナンスの履歴そして走行距離を反映したメッセージが送られます。もしこうしたメッセージが信頼された自動車メンテナンスのネームスペースアカウントからのものであれば、その作業が適切に行われたものと信じることができるでしょう。モザイクをカラードHDアカウントへ送ってもらい、その車が有料の保険に加入している事や、ある基準を満たしていることを証明することもできます。

4.2.政府登録

政府機関はモザイクかメッセージをブロックチェーンのカラードHDアカウントへ送り、自動車が登録済みであり、税金も支払い済みであると示すことができます。そのような場合、NEMシステム上のモザイクが“転送不可能(non-transferable)”なものとして作られます。それはそのカラードHDアカウントの管理者が、公式の政府のモザイクをいかなる第三者へも送信できないことを意味しています。唯一の選択肢は元の送り手、この場合には政府機関、に返送することだけです。

4.3.デジタルメディアのランセンス

デジタルメディアのブロックチェーンライセンスでは、そのメディアに何回その製品がストリーミングされたかを示すメッセージが送られます。また、規約の詳細や、ライセンスに対する制限について詳しく述べたメッセージを送ってもらうこともできます。

4.4.高級品と偽造防止

高級な製品を製造する企業は、その企業だけが管理できるネームスペースを作ることができます。そしてその名前を企業のプロフィールに公開することができます。それぞれの商品について、シリアルナンバーや高精度のスキャン、化学組成などを使うことでブロックチェーン公証を行い、それらを個別に識別し登録をすることができます。それぞれの商品は独自のもので、それぞれがフィンガープリントされており、さらにはそれぞれのブロックチェーン公証は登録済みの広く認知されたソースにより行われたものなので、ブロックチェーン公証なしの偽造品を販売する業者を特定するのは非常に容易です。

登録されライセンスを持ったプロにより維持・修正が行われるため、その公証は商品の状態についての情報を加えて時折アップデートされるかもしれません。

高級製品に関しては、リコールに関するメッセージもブロックチェーン公証のカラードHDカウントへ送ってもらうことも可能です。

これらすべてのケースにおいて、中古品(ブロックチェーン公証のカラードHDアカウントに沿うもの)の購入を希望する第三者はその商品の信頼性とこれまでの歴史をたどって調べることができます。

4.5.二者間の法的なコントラクト

3.9.で述べたように、アポスティーユのシステムは、複数の当事者によって署名され、後に必要であればアップデートや譲渡ができるコントラクトの公証を、チェーン上で行うのに理想的な方法です。

5.最後に

このペーパーではブロックチェーンを利用した、NEMのブロックチェーンプラットフォーム上で可能となった公証システムを提案してきました。アポスティーユのブロックチェーン公証はファイル専用のプライベートキーを使い、HDアカウントに色付けを行います。そしてその後にメッセージ機能、ネームスペース、モザイクそしてマルチシグを組み合わせることによって、公証の刻印・登録・譲渡が可能なダイナミックなブロックチェーン公証のシステムが創られるのです。

以前の公証はブロックチェーン上で一回性のデジタルフィンガープリントを施して、ドキュメントを記録するだけにすぎませんでした。私たちの公証システムはこうした初期のバージョンの拡張と言えます。アポスティーユはその水準を引き上げ、さらなる機能と使用用途が実現できる異なるパラダイムを採用し、商業的な利用にも適したものにしました。このシステムはブロックチェーン公証のサービスにおける、第二世代の技術革新を代表するものといえるでしょう。

6.謝辞

アポスティーユのプロジェクトは、NEMのコミュニティファンドから財政的な支援を受けました。このプロジェクトを支えるために時間を割いてくれたNEMコミュニティのメンバーに感謝を申し上げたいと思います。また、アポスティーユの開発中に私たちを指導し貴重な知恵を授けてくれたLon WongとTakao Asayamaに個人的に感謝を伝えたいです。

私たちはNEMの開発者とNEMのコアチームを賞賛したいと思います。彼らは何年間も熱心に働き、NEMの技術を今日あるような素晴らしいプラットフォームへと昇華させてくれました。そして最後に、私たちをサポートし貢献してくれた素晴らしいNEMのコミュニティへ。本当にありがとうございました。

7.参考文献

アポスティーユ(2014). 『コリンズ英語辞書―完全版　第12版』
2016年10月、以下より引用　http://www.thefreedictionary.com/Apostille

アポスティーユ条約 (2016年10月24日). 『ウィキペデキア』
2016年10月、以下より引用　https://en.wikipedia.org/wiki/Apostille_Convention

アラオス, M. (2012). 『存在証明(Proof of Existence)について』
2016年10月、以下より引用　https://proofofexistence.com/about

ナカモト, S. (2008). 『ビットコイン：ピアツーピアの電子マネーの仕組み』
2014年4月28日、以下より引用　https://bitcoin.org/bitcoin.pdf

NEM コアチーム. (2015). 『NEMの技術的参考文献』
2016年10月、nem.ioより引用　https://www.nem.io/NEM_techRef.pdf

NEM チーム. (2016). 『モザイクとネームスペース』
2016年10月、nem.ioより引用　https://blog.nem.io/mosaics-and-namespaces-2/

ローゼンフェルド, M. (2012). 『カラードコイン概要』
2016年10月、Bitcoilより引用　https://bitcoil.co.il/BitcoinX.pdf

スワン, M. (2014). 『ブロックチェーン：新し経済への展望』
オライリーメディアより。