XYオラクルネットワーク：源泉証明 （Proof-of-Origin）に基づく暗号化位置ネットワーク

アーリー・トゥロウ（Arie Trouw)*、マルクス・レーヴィン（Markus Levin)†、
スコット・シェーパー（Scott Scheper)‡
2018年1月

要約

位置情報に依存する技術の時代が徐々に到来するに伴い、私たちのプライバシーと安全は位置情報の正確性と合法性に大きく依存するようになりました。　位置データの流れを制御する中央集中化した主体の必要性を排除するためにさまざまな試みが行われてきたが、それらの試みは実世界でこれらのデータを収集するデバイスの完全性に依存してきました。　位置情報に関する高度なデータの確実性を確立するために、私たちはゼロ知識証明(zero-knowledge proof) チェーンを基盤にする革新的な形態を用いるトラストレス（trustless：信用の必要がない）暗号化位置ネットワークを提案します。 XYOネットワーク（XYオラクルネットワーク）は、さまざまなデバイスのレベルやプロトコルにわたって階層化された位置検証を可能にする存在です。　　その中心には、ブロックチェーン技術の力と現実世界のデータ収集を直接アプリケーションでシステムに接続する源泉証明（Proof of Origin）とバウンド・ウィットネス（Bound Witness）と呼ばれる一連の暗号メカニズムが位置を占めています。

1　序論

ブロックチェーン基盤のトラストレススマートコントラクトの到来とともに契約の結果を調整するオラクルサービスの必要性もそれに伴って増加します。今日のほとんどのスマートコントラクトの実行は、単一または蓄積された一連の権威あるオラクルに依存して契約の結果に対して精算をします。当事者双方がそのような具体的なオラクルの権威との整合性について合意する場合、これは十分な条件になります。このような多くの場合、適切なオラクルが存在しないか、またはそのオラクルがエラーや欠点の可能性により権威のあるものとみなされずにいます。

ロケーションオラクルは、次のカテゴリに属する。実世界の対象の位置は、一定のオラクルの報告、伝達、保管、および処理の要素を通じて処理され、これらのものはすべてエラーを生じさせる可能性がある上、汚染される可能性があります。このようなリスクの要因には、データの改ざん、データの汚染、データの損失や結託があります。

*XYOネットワーク, **arie.trouw@xyo.network**
†XYOネットワーク, **markus.levin@xyo.network**
‡XYOネットワーク, **scott.scheper@xyo.network**

これにより、位置情報の確実性と正確性がトラストレスの分散化されたロケーションオラクルの不在により否定的に影響を受ける可能性があるという問題点が存在します。イーサリアム（Ethereum）やEOSのようなプラットフォームは、ICO形式の資金調達エスクローと関係した主な利用事例と関連して、オンラインで安全に相互活動を仲裁することができる機能として幅広く使用されてきました。しかし、現在までプラットフォームはすべて現在の情報チャンネルのデータ完全性に汚染の可能性があったため、実世界の代わりに完全にオンラインの世界だけに集中してきました。

XYOネットワークは、ブロックチェーンプラットフォームを作る者を含める開発者によって、まるでAPIのように現実の世界と相互作用できるようにする概念のために努力を傾けてきました。XYOネットワークは、2つの主体が集中化された、第三者なしに実際の世界で取引できるようにする世界初のオラクルプロトコルです。これらの概念によって位置検証が開発者にトラストレス(trustless)　に対応することによって、これまで不可能だった革新的なユースケースのためのプロトコルが提供されます。

XYO ネットワークは、私たちの対顧客ビジネスのXY Findablesを通じて、世界中に配布された100万個のデバイスで構成された既存のインフラストラクチャに基づいて構築されます。XYのBluetoothとGPSデバイスを通じて日常的な顧客は、自分たちが継続的に追跡する物（キー、バッグ、自転車、さらにはペットなど）に物理的な追跡ビーコンを付与することができます。もし、物が他の所に置かれたり紛失した場合は、スマートフォンのアプリケーションで位置を確認することによって、その正確な位置を知ることができます。XYはわずか6年のうちに世界で最も膨大なレベルの顧客のBluetoothとGPSネットワークを備えました。

2　歴史的背景と以前の接近法

2.1　位置証明

証明可能な位置の概念は1960年代から提示されてきました。LORAN[1]など、1940年代の地上電波航法システムまでさかのぼることができます。現在は、いくつかの検証媒体を互いに積み重ね三角化（triangularization）とGPSサービスを通じて位置情報を作り出す位置情報サービスがあります。しかし、これらの接近法は、今日の位置の技術において、私たちが直面している最も重要な要素、すなわち詐欺信号を検出し、位置データのなりすまし（spoofing）を無力化させるシステムを構築する問題を適切に解決できないでいます。こういう理由から、今日の暗号化 – 位置プラットフォームは、物理的な位置信号の発端を証明することに集中するものでなければならなりません。

驚くことに、位置検証の概念をブロックチェーンの技術に適用する概念は2016年9月に開催されたイーサリアムのDevCon 2で初めて提示されたという事実です。ベルリン出身のイーサリアム開発者であるLefteris Karapetsasが提起しました。彼のプロジェクトであるSikorkaは彼が称するいわゆる実在証明（Proof　of　Presence）を使用して、スマートコントラクトが現実の世界の現場に配置されるようにしました。彼が位置とブロックチェーンの世界を接続した試みは、主に拡張現実の使用事例に焦点を当てており、位置の証明において、彼は把握質問のような新しい概念を発表しました[2]。

2016年9月17日には、「位置情報」という用語がイーサリアムのコミュニティに正式に登場し[3]、その後、Ethereum Foundationの開発者Matt Di Ferranteが次のように加えて語りました。

> *「皆さんが信頼できる位置証明とは、率直に言って最も実行が難しいことの一つです。多数の参加者のそれぞれの位置を検証できたとしても、今後いつ困難にならないという保証はない上、多数者の報告にのみ依存するのは、大きな弱点といえます。もし誰かが機器を開けたり、またはそのファームウェアを変えようとする場合、秘密鍵が破壊されるような改ざんを防止する技術を備えた特殊な種類のハードウェア機器を備えるなら安全性が強化されるが、にもかかわらず、GPS信号*

を欺くのは不可能ではないでしょう。これをしっかり行って正確性を期するなら、多くの対策とともにさまざまなデータソースが多量に必要なため、莫大な資金のプロジェクトにならなければならないだろう。」

—Matt Di Ferrante, (Ethereum Foundation開発者)

2.2 位置証明：短所

位置証明は、要約するとタイムスタンピング(time-stamping）や分散化などのブロックチェーンの強力な特性を活用し、それらを改ざんに耐えられるオフチェーンの位置認識デバイスと組み合わせるものとして理解できるでしょう。暗号化位置技術の領域を私たちは「暗号化位置(crypto-location)」という。さらに、スマートコントラクトの弱点が単一のデータソースを使用して（よって単一の問題発生源を持つ）オラクルと関連としているのと同様に、暗号化ロ位置システムもやはり同じ問題に直面しています。現在の暗号化位置技術の弱点は、個体の位置を報告するオフチェーンデバイスと関連がある。スマートコントラクトにおけるオフチェーンのデータソースはオラクルです。 XYOネットワークでは、オフチェーンのデータソースは、Sentinel（センチネル）と呼ばれる特別な形態のオラクルとして実世界を移動します。 XYOネットワークを取り巻く中心的な革新は、安全な暗号化位置プロトコルを生成するために、システムの構成要素の基礎となるアイデンティティレスの位置情報証明を基盤にします。

---

3 XYオラクルネットワーク

「GPSを補完する充分なシステムの必要性は以前から知られてきました。 GPSは非常に正確で信頼性があるが、妨害(jamming)、スプーフィング（spoofing）、サイバー攻撃、また、その他の形態の干渉行為がその頻度と強度を徐々に増しています。 これによって私たちの生活と経済活動は大きな打撃を受ける可能性があります。」

—Dana Goward (RNT Foundation理事長)

3.1 序論

XYOネットワークの目標は、攻撃に耐えて可能なデータのクエリがある場合は、最高レベルの確実性を提供する信頼の必要がない分散化された位置オラクルシステムを構築します。私たちは、これらの目標をゼロ知識証明チェーンを介してシステムの構成要素から位置偽装のリスクを大幅に軽減させる一連の抽象化を通じて達成します。

3.2 ネットワークの概観

このシステムは、暗号化証明のチェーンを介して位置データの高い確実性を提供する接続機器のプロトコルのエントリポイントを提供します。ユーザーは「クエリ（query）」と呼ばれる取引の発行を通じて、スマートコントラクト機能[1]を保有するブロックチェーンプラットフォーム上で一連の位置データを取得できます。その後、XYOネット

[1] Ethereum, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counter- party, Monax その他,

ワークからのアグリゲータ（aggregator）は、契約に対して発行されたこれらのクエリに着目し、暗号化証明をアグリゲータ—に再び伝達する分散化されたデバイスの集合体から最も高い正確性を持った回答を導き出す。これらのアグリゲータ—は、以後、最も高いスコアの回答について合意に達した後、そのスマートコントラクトに回答を提供する。このような構成要素のネットワークにより、どのような個体が特定の時間に特定のXY座標にいるのか、最も可能性が高いトラストレスの確実性により確認することができます。

XYOネットワークは4つの主な構成要素、つまり、センチネル（Sentinel：データ収集者）、ブリッジ（Bridge：データ伝達者）、アーキビスト（Archivist：データ保管者）、ディバイナー（Diviner：回答収集者）で構成されます。センチネルはセンサー、無線機器、その他の手段で位置情報を収集します。ブリッジは、センチネルから、これらのデータを受け取りアーキビストに提供します。アーキビストはディバイナーが、これらの情報を分析できるように情報を保管します。ディバイナーはアーキビストからの位置ヒューリスティック（heuristic）を分析して、クエリに対する回答を生成して正確性スコアを与えます。その後ディバイナーは、これらの回答をもう一度スマートコントラクトに伝達します（つまりディバイナーがオラクルの役割をします）。正確性スコア（「源泉チェーンスコア（Origin Chain Score）」とする）は、一連のゼロ知識証明（「源泉証明チェーン（Proof of Origin Chain）」とする）によって決定されます。

これらのチェーンを通じてそのどんな基本的な情報の公開せずに、同じソースから出てきた二つの以上のデータが保証されます。クエリ経路上の各構成要素は、それ自体の源泉証明（Proof of Origin）を生成し、データを伝達する各構成要素に接続されます。源泉証明は現実世界のデータに対して高いレベルの信頼性を提供するために、ネットワーク上で伝達者の経路に従って暗号化の保証を構築する独自の情報です。これらの源泉証明チェーンは、データを収集した最も初期の機器までの位置データから、私たちが持てる信頼性を含みます。源泉証明の機能方式については、次のセクションで見てみることにします。

ディバイナー間に分散化した合意メカニズムを構築するために、XYOネットワークはディバイナーから収集したデータとその関連源泉スコアに応じてクエリの取引を保管する、XYOメインチェーンという名前の公開的で変更不可能なブロックチェーンに依存しなければなりません。システム全体の機能の詳細内容を見る前に、まずネットワークの各構成要素の役割に対して定義することにします。

3.2.1 センチネル（Sentinel）

センチネルは位置証明です。これらはデータヒューリスティックを観察して一時的に台帳を生成することにより、ヒューリスティックの確実性と正確性を保証します。センチネルの最も重要な側面は、同じソースから来たものだという点を他の構成要素が確信できる台帳をセンチネルが生成するという点です。　センチネルは源泉証明を暗号化証明のリレーチェーンに追加することによって、これらの機能を実行します。　XYOネットワークは信頼の必要がないシステムなので、センチネルは正しい位置情報を提供するように導かれなければなりません。これは評判要素を支払要素と結合することによって実行されます。センチネルは、その情報がクエリの回答に使用されるとき、XYOネットワークトークン（XYO）で報酬を受ける。報酬を受ける可能性を高めるために、センチネルはそれと同等の存在のものと合致する台帳を作成して源泉証明を提供し、自分たちの位置情報のソースであることを確認させなければなりません。

3.2.2 ブリッジ（Bridge)

ブリッジは、位置データトランスクライバー（transcriber）です。センチネルからディバイナーに安全に位置台帳を伝達する役割をします。ブリッジの最も重要な部分は、アーキビストはブリッジから受け取ったヒューリスティックの台帳がどんな形にも変わらなかったと安心できる点です。ブリッジの2番目の重要な部分は、オリジン・メタデータ(metadata)の追加的な証明もしてくれる点である。　XYOネットワークは信頼の必要がないシステムであるため、ブリッジが正しいヒューリスティックを伝達できるように導びかれなければなりません。この機能は、評判要素を支払要素と結合させることによって実行されます。ブリッジは自分が伝達した情報がクエリの回答に使うとき、XYOネットワークトークンで報酬を受けます。報酬を受ける可能性を高めるために、ブリッジはそれと同等の存在のものと合致する台帳を生成して源泉証明を提供して、自分たちをヒューリスティックの伝達者であることを確認させてあげなければなりません。

3.2.3 アーキビスト（Archivist)

アーキビストは、すべての履歴台帳を保管するために、ブリッジからの位置情報を分散化形式で保管する。　一部のデータが失われたり、または一時的に利用できなくなってもシステムは正確性が多少低下するだけで機能は維持されます。アーキビストはまた、必要に応じて台帳データの文字列を簡単に返すことができるように台帳を索引付けします。アーキビストは生データ(raw　data)だけ保管し、データの検索や関連の利用に対してだけXYOネットワークトークンで支払いを受けます。 保管はいつも無料です。

アーキビストはネットワーク化されているので、1人のアーキビストに質問をすると、該当するデータを含んでいない他のアーキビストにも質問をする結果になります。アーキビストは自分に戻ってきたすべての台帳情報を選択して保管することができます。　これによって2つのタイプのアーキビストが現れるが、1つは“クラウド(cloud)”のデータ生産側にあるものと、もう1つのタイプは“クラウド”のデータ消費側にあるタイプです。　中間のアーキビストはハイブリッドタイプです。　データ保管の選択は強制されないが、IPFSまたは他の分散化された保管ソリューションを通じて容易に行うことができます。データがあるアーキビストから他のアーキビストに移動する度に源泉証明が追加され、支払いに対する追跡が行われる(すべてのアーキビストに支払われるため)。 検索の場合、有効性を高めるために最小源泉証明のレベルを設定することができます。データの誇張を防ぐためにセンチネル、ブリッジ、アーキビストの割合が調節されなければなりません。

3.2.4 ディバイナー（Diviner)

ディバイナーはXYO ネットワークの中でも最も複雑な部分です。 ディバイナーの全般的な目的は、クエリに対する最も正確なデータをXYO　ネットワークから導き出し、そのデータをクエリの発行人に再び伝達することです。ディバイナーはXYOスマートコントラクトに提起されたクエリに対して適切なブロックチェーンプラットフォーム（Ethereum、Stellar、Cardano、IOTAなど）を探し、その後、アーキビストのネットワークと直接相互作用を行ってクエリの最も高い精度と信頼性スコアを持つ回答を探します。こういった作業は、証人を最適の源泉証明チェーンと判断することによって行われます。最も短い時間で最高スコアの回答を導き出したディバイナーはプルーフオブワーク（Proof of Work）を通じて主なXYOブロックチェーン（XYOメインチェーン）上にブロックを生成することができるようになります。クエリは、報酬の大きさと複雑さに応じて優先順位が決まる関係で、回答に対して提供されたXYOが多ければ多いほど、クエリの優先順位は高くなります。

それ以外のディバイナーはブロックの有効性について合意に達したら、ブロックにデジタル署名をします。そのブロックのコインベース（coinbase）アドレスであったディバイナーは、その後、取引をその精度スコアと一緒に回答を含むスマートコントラクトに送ります。また、攻撃者がディバイナーのふりをして、偽の情報をブロックチェーンに発行することを防ぐために、他のディバイナーの署名リストを送ります。その後、スマートコントラクトはペイロード（payload）の署名リストを確認することによって、この情報の完全性を検証します。

3.3　エンドツーエンド （End-to-End）機能

各構成要素の役割について説明したので、今度はシステムがどのように動作するかについてのエンドツーエンドの例をあげてみることにします。：

1. **センチネルのデータ収集**
    - センチネルは現実世界のロケーションヒューリスティックを収集して、自分の源泉証明(Proof　of Origin)がその上のノードに接続されるように準備します。
2. **ブリッジのセンチネルからのデータ収集**
    - ブリッジは、オンラインのセンチネルから必要なデータを収集して源泉証明をチェーンに追加する。 その後、ブリッジはネットワーク上でアーキビストが自分を利用するようにします。
3. **アーキビストのブリッジからのデータのインデックス化/組み合わせ**
    - ブリッジはアーキビストに情報を絶えず送信し、その後アーキビストはロケーションヒューリスティックのインデックスとともに分散化したストアに保たれます。
4. **ディバイナーのユーザーのクエリの導出**
    - ディバイナーは、スマートコントラクトに送られたクエリを探して回答の作成手順を開始することを決定します。

5. **ディバイナーのアーキビストからのデータ収集**
    - ディバイナーは、その後アーキビストのネットワークから必要で適切な情報を取得してクエリを実行します。
6. **ディバイナーの回答構成**
    - ディバイナーは、　アーキビストのネットワークから最適のオリジンチェーンスコアをもつクエリの最適な回答を選択します
7. **ディバイナーのブロック提示**
    - Divinerはその後の回答の内容、クエリ、プルーフオブワーク（Proof of Work）を通じて支払われたXYOトークン（XYO）を含むXYOメインチェーンでブロックを提案する。 ネットワーク上の他のディバイナーはブロックのコンテンツにデジタル署名し、その後コインベースのディバイナーのアカウントが更新され、有効なブロックの合意に達するとシステムでプルーフオブワークが示されます。
8. **ディバイナーのクエリ開始者へ結果の返信**
    - ディバイナーは、回答、オリジンチェーンスコア、そのデジタル署名のセットをパッケージ化し、XYOスマートコントラクトに安全に接続するアダプターの構成要素に送信します。　アダプターはディバイナーの完全性が損なわれないように役割を行って、デジタル署名された回答のセットをスマートコントラクトにもう一度送信します。このプロセスは、ブロックを生産するプロセスの直後に行われます。 コインベースのディバイナーは、その努力に対する報酬を受け取ります。
9. **XYOネットワークの構想要素の作業に対する報酬**
    - 源泉証明チェーン(Proof of Origin Chain)上の構成要素は、クエリの回答を導き出したその参加に対する報酬を受けます。センチネル、ブリッジ、アーキビスト、ディバイナー全員が作業の報酬を受けます。

同じクエリが数回質問される場合は、特定の時点に生成された回答がその時点でシステムが提供できるヒューリスティックに基づいているので、複数の回答が生成されることがあります。ブロックチェーンへの回答の提出は2段階で行われます。 まず、クエリに対するベストアンサー（最適な回答）を決定するために分析を行う必要があります。 2番目に、システムによって複数の回答が生成された場合、ノードは回答を比較して常により良い回答を選択します。　簡単なクエリの例としては、「過去、特定の時間にネットワーク上のノードの位置は？」を例に挙げることができます。

3.4　単一データソースとしてのブロックチェーン

ディバイナーは、その中心から相対データ(relative data)を絶対データ(absolute data)に単純に変換させる。アーキビストのネットワーク全体を探索して、XYOネットワーク上でクエリの絶対的な回答を具体化させます。　ディバイナーは、XYOメインチェーンにブロックを提示して追加するノードで、プルーフオブワーク（Proof of Work）に対する報酬を得ます。　アーキビスト・ネットワークは未処理データのストアで、ブロックチェーンは絶対処理されたデータのストアなので、ネットワークは XYOメインチェーンで 最新情報を使用することによって、アーキビスト・ネットワークによる高価な電算処理に依存するかわりに、今後のクエリに肯定的に回答することができます。

XYOメインチェーン上のブロックは、クエリの回答に使用された源泉証明チェーン(Proof of Origin Chain)と構成要素のグラフを保管するため、今後のディバイナーはこの絶対データを検索して、より低い帯域幅を使用しても正確な結果を導き出すことができます。　これによって、XYOメインチェーンは徐々にシステムの最も重要なデータソースになります。　しかし、センチネルによって収集されたロケーションヒューリスティックに関する最新情報を維持するためには、アーキビストのネットワークが依然として必要です。

3.5　最適の回答候補を選択するための　XYOネットワークのフレームワーク

私たちは、ベストアンサー(Best　Answer)を一連の回答候補の中から最高レベルの有効性スコアを提供し、最低限必要な正確性よりも高い正確性をもつ妥当性スコアを提供して、最低必要正確性よりも高い正確性をもつ1つの回答と定義します。有効性スコアは源泉チェーンスコア（Origin Chain Score）を基にします。 システムは、最も高いスコアの源泉スコアがどういうものなのか、より高いスコアが達成されるまではどれが100%なのか、そしてどれが新しく100%になるのか知っています。　XYOネットワークは、ベストアンサーを決定するベストアンサーアルゴリズム

(Best Answer Algorithm)の選択を許可します。 これによって代替アルゴリズムへの今後の調査のための拡張が行われます。

データが不適切だったり正確でないと見なされて回答から除外される場合、データはアーキビストに送られて分散化されたストアから除外される。

3.6　パブリックブロックチェーンとの最初の統合

XYO ネットワークはイーサリアム、ビットコイン + RSK、EOS、NEO、Stellar、Cardanoなどのスマートコントラクトの能力を持つパブリックブロックチェーンとの相互作用をするように設計されました。XYOネットワークと相互作用するために、いわばイーサリアムのユーザーは、私たちのXYOスマートコントラクトにクエリを提起してXYOトークン（ERC20）で支払うことができます。私たちのXYOブロックチェーンであるディバイナーのノードは、これらのクエリのに対して継続的にイーサリアムをポーリング（polling）して、私たち自身のXYOブロックチェーン（XYOトークンとも呼ばれる）固有の通貨で報酬を受けます。今後、私たちはERC20の保有者から、私たちのブロックチェーンの固有の通貨に1：1で切り替えることによって、拡張可能なIoTの用途に必要な小額の支払い要求基準をサポートしている取引手数料を当社のプラットフォームに提供します。これらの用途では、私たちはユーザーによってパブリックスマートコントラクトを通じて相互作用をする代わりに、私たちのブロックチェーンに直接クエリを提起するように許可します。

4　源泉証明（Proof of Origin）

非信頼ノードで構成された物理的ネットワークでは、二つ以上のデータが同じソースから出たゼロ知識証明（zero-knowledge proof）に基づいて、エッジノード（edge node）によって提供されたデータの確実性を決定することができます。これらのデータセットの使用および多数の類似するデータセットと、少なくとも一つのノードの絶対位置についての知識との結合を通じて、その相手ノードの絶対位置を確認することができます。

4.1　源泉証明　序論

従来のトラストレス（非信頼性）システムは、システム内の取引や契約の際に署名するために秘密鍵（private key）に依存してきました。　これはそのデータに署名するネットワーク上のノードが物理的かつ仮想的に安全であるという仮定で非常にうまく機能する。しかし、万が一秘密鍵が侵害された場合は、起源証明の能力は損なわれます。

モノのインターネットにトラストレスの概念を適用する場合、ネットワーク上のエッジノードは物理的または仮想的に安全ではないと仮定しなければならなりません。これによって、固有のIDを使用せずにエッジノードを識別し、代わりにネットワークの外部からの知識もいらずに、それによって生成されたデータを正当で有効なものとして判断する必要性が増えます。

4.2　源泉証明の核心The Core of Proof of Origin: バウンド・ウィットネス（Bound Witnesses）

源泉証明は、バウンド・ウィットネス(Bound　Witness)の概念に依存します。デジタルコントラクトを解決するために使用されるトラストレス（信用の必要がない）データソース（オラクル）が有用ではないので、最初に双方向の位置証明の存在を構築することによって提供されるデータの確実性を大幅に高めることができます。　第1の双方向ロ

ケーションヒューリスティックは近接性です。これは、双方の当事者が相互作用に共同で署名することによって相互作用の発生と範囲を検証することができるからです。これによって、両方のノードが互いに近接したというゼロ知識証明が成立します。

次に、トラストレスシステム内のオラクル証人ノードが、それが共有しているデータを収集したという確実性を判断しなければなりません。　トラストレスシステムでは、証人ノードが欠陥や汚染によって偽のデータを生成する可能性があります。無効なデータは、そのヒューリスティックの許容範囲外になった場合、容易に検出して削除できます。 有効でも不正確なデータ（偽データなど）は検出するのがもっと難しい。

4.3　単方向 vs. 双方向ロケーションヒューリスティック

実世界に関連するほとんどのデータ（ヒューリスティック）は一方向です。これは、測定された要素をもう一度測定することが不可能であることを意味し、一方向ヒューリスティックデータの検証を非常に難しくする。双方向ヒューリスティックは、測定された要素が自分の測定値を他の当事者に報告することができるヒューリスティックで、これによって検証が可能となります。位置は、2つのエッジノードが相互に報告することができる双方向という点で珍しいヒューリスティックです。

これに対する現実の世界の例として、二人がお互いに近距離からセルフカメラで写真を撮って、相手にあげるために印刷した後、各自がセルフカメラに署名をする場合を挙げることができます。このような過程を経て、両者には接近性証明（Proof of Proximity）が付与される。この二人がこれらの「データ」を得る唯一の方法は、両者が同じ位置に一緒にいることです。

では、ネットワークの効果について調べてみましょう。すべてのエッジノードが歩き回りながら、これらの「セルフカメラ」を続けて生産し、これらをバインダーで保存するシステムを想定してみましょう。これらはまた、そのバインダーを時間の順序で保管すると予想でき、そのどれも削除が許されない。これにより、相手のエッジノードのレコーダーと相互参照できる各エッジノードのための接近性レコーダーが構築されます。

4.4　ノンエッジノード（Non-Edge Nodes)

ノードはすべて、ブリッジ、リレー、ストレージ、そして分析ノードを含めて「証人（witness）」とみなされます。これにより、あるノードから次のノードに転送されたすべてのデータが接続される。これがバウンド・ウィットネス（Bound Witness）の概念です。

4.5　相互参照（Cross Reference）

各エッジノードによって生産とともに束ねられたすべての「セルフカメラ」セットを分析すると、システムは、ネットワーク内のすべてのノードの相対的な接近性から最も満足できる回答（Best Answer）を得ます。もし、すべてのノードが正しくと正確に報告をするなら、エッジノードのすべての相対ポジションのマッピングは最大限の確実性と正確性（つまり、100%）を達成するようになります。

これとは逆に、もし、すべてのノードに正直でなかったり欠陥がある場合は、確実性と正確性の両方が最小値の0%となります。

報告されたデータセットとエッジノードのどちらか1つの相手ポジションのクエリに基づいて確実性と正確性係数とともに、そのポジションの近似値が生成されます。

同じデータセットと同じ解析アルゴリズムに基づいて、すべての計算は同じポジション近似値、確実性、正確性の同じ係数に到着しなければならなりません。

4.6　ダイアグラム

S　'とS"（図1参照）は、ヒューリスティックを収集する各々1つのセンチネル（エッジノード）です。これらは互いに接触すると、ヒューリスティックデータとパブリックキーを交換します。両者は相互作用の記録を完全に構築した後、その結果の相互作用に署名します。これらの署名された記録は、その後すべてのローカル台帳で次のエントリされます（S　'に対して16、S"に対して3）。これらのアクションは、2人の証人がお互いに近接した存在のように結びつきます。

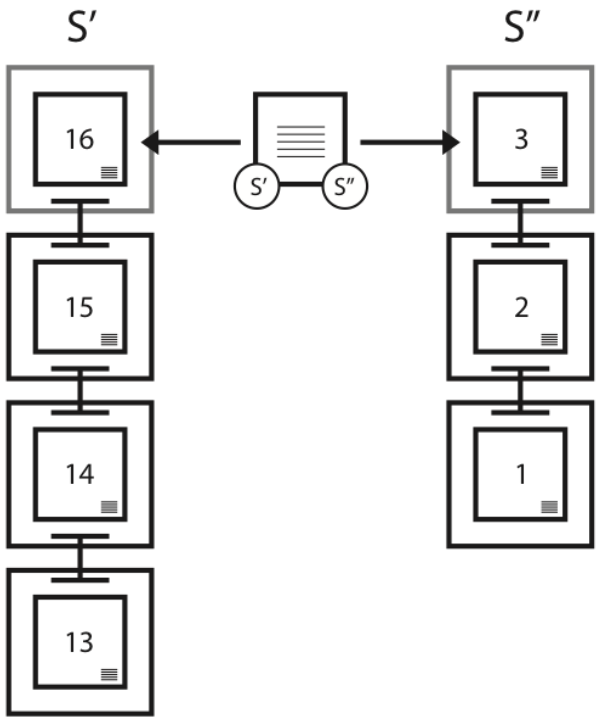

図1.　2つのセンチネル間のウィットネスバインディングの例

4.7　源泉チェーン（Origin Chains）

各源泉（origin）は、それ自体の台帳を保って、それに署名して1つの源泉証明チェーン（Proof of Origin Chain）を作ります。この源泉証明チェーンに関する情報が共有されると、それは事実上恒久的に保たれます。これは、共有した後に発生するフォーク（fork）がチェーンを終了させ、証人からの将来のすべてのデータが新しい証人から来たかのように処理されるようにするためです。

源泉証明チェーンでリンクを作成するため、源泉はパブリック/プライベートキーのペアを生成する。その次に、両ブロックのすべてにパブリックキーを含めた後、同じペアで前と次のブロックの両方に署名をします。署名が完了したら、すぐにプライベートキーは削除されます。プライベートキーがすぐに削除されるので、キーが盗難や再利用されるリスクが大幅に減ります。

源泉証明チェーンは、XYOネットワークに流れ込む台帳が有効であることを確認するための鍵となります。データソースの固有IDは偽造される可能性があるため実効性に欠けます。プライベートキー署名はXYOネット

ワークのほとんどが物理的なセキュリティの確保が難しかったり不可能であるため、悪意を持った者がプライベートキーを盗む可能性があるので、これもまた実質的でありません。これを解決するためにXYOネットワークは一時的なキーチェーン（Transient Key Chain）を使用します。この効用性は、データの源泉チェーンを改ざんすることは不可能だという点です。しかし、一度チェーンが破損すると永久に破損した状態になり、したがって1つの孤立した存在になってしまいます 。

ヒューリスティック台帳がXYOネットワークから送られると受信機（receiver）は、それ自体の源泉証明を追加し、これにより源泉証明が長くなって源泉証明インターセクション（Proof of Origin Intersection）を生成します。源泉証明チェーン（Proof of Origin Chain）と源泉証明インターセクション（Proof of Origin Intersection）はディバイナーが台帳の妥当性を検証するために使用する基本的な指標です。

台帳の評判（Ledger Reputation）のための式は実質的に何パーセントのXYOネットワークがそれと連携した源泉証明ボール（Proof of Origin Ball）の作成に参加したのかにあります。理論的に、もしXYOネットワークの記録の100パーセントが源泉証明とリンクし、その後完全に分析されれば、それが有効になる可能性は100パーセントになります。もしXYOネットワークの記録の0%が分析に利用されれば有効性は0%に落ちます。

追加のセキュリティのためにチェーンリンク（Chain Link）のパブリックキーは、2次のエントリーが利用できるときまで提供されません。これにより、エントリーと、前または次のリンクで保管されるその他のデータ間の時間に間隔が生じます。

4.8 源泉チェーンスコア（Origin Chain Score）

源泉チェーンスコアは次のように計算する。（ディフォルトアルゴリズム ）：

- PcL = 源泉証明チェーンの長さ
- PcD = 源泉証明チェーンの難易度
- Pc’ Pc” O = Pc’および Pc”の源泉証明チェーンオーバーラップ

$$Score = \prod_{i=0}^{i=n} \frac{PcL * PcD}{Pc' Pc'' O}$$

4.9 源泉ツリー（Origin Tree）

源泉ツリーは、回答の概略的な有効性を計算するために使用されます。これは、特定の断言的な回答のためのデータに最も適したツリーである理想的なツリー（Ideal Tree）を生成するために収集されたデータを使用します。もしノードNが、X、Y、Z、Tの位置に位置する場合、データセット内の全データにわたる誤差は一定の価値を持ちます。これらの誤差を計算するために、私たちはMIN、MAX、MEAN、MEDIANとAVERAGE DISTANCE FROM THE MEANを計算します。

すべてのスコアsのセットS、源泉証明チェーンの難易度PcDおよび誤差率errorを基準として決定されたベストアンサー（Best Answer）は、以下の通りである：

$$BestAnswerScore = \max_{\forall s \in S_j} [PcD * (1 - error)]$$

つまり、最も高いベストアンサースコア（Best Answer Score）を獲得した断言的な回答がベストアンサーとなります。私たちは、源泉証明ツリーを利用して、不可能な枝（異常値）を確認して削除することができます。

4.10 一時的キーの変更（ Transient Key Chaining）

一時的なプライベートキーを使用して一連のデータパケットをチェーン化し、二つの連続したパケットに署名をすることができます。プライベートキーとペアを組んだパブリックキーがデータパケットに含まれる場合、受信機は、両パケットが同一のプライベートキーによって署名されたことを確認することができます。パケット内のデータは署名を破棄せずには修正が不可能なため、署名されたパケットがブリッジや保存ノードのような第三者によって変更されていないことを確認することができます。

4.11 リンクの深さ

最小限の場合、ノードは源泉証明チェーン（Proof of Origin Chain）内のすべてのリンクに新しいパブリック/プライベートキーのペアを生成します。このリンクは、1のリンクの深さ（Link Depth）をもちます。一つのLedger Entryのリンクテーブル内にはNエントリーがある可能性があり、各エントリーはリンクのパート2が追加されたときの距離を表します。2つのどんなリンクもベース2尺度で同じ評価の順序を持ちません。例えば、エントリー[1,3,7,12,39]は許容されるが[1,3,7,12,15]は許可されません。

以前のブロックが発行される場合、深さ1のリンクが生成、使用、削除されます。しかし、1よりも大きい深さのリンクは、以前のブロックが署名されることによってそのペアが生成がされ2番目の署名は、今後nブロックの後になってようやく発生し、この後プライベートキーは削除されます。これらの理由から、深さが1よりも大きいリンクは、深さが1のリンクより常に安全性の低いとみなされますが、そのようなリンクは、安全性が低い代わりに機能の改善やデータの損失を減らすのに使用することができます。

4.12 固定した順序

台帳の順序を決定する際の重要な要素は、報告された順序です。　デバイスが源泉証明の署名入り台帳の順序を変更することはできないので、すべての台帳を一括して検討することにより絶対的な順序を確立することができます。

4.13 最後から2番目の発行

源泉証明を確立するための主な方法は、センチネル（Sentinel）が最終ブロックを報告することなく、常に最後から2番目のブロックを報告するという事実に基づいている。 これにより、最終ブロックは以前のブロックへの署名付きリンクをリンクの証拠として持つことができます。

4.14 空のリンク

源泉証明チェーンをより安全に作るためには、チェーンが最大10秒毎に1回、最小6秒毎に1回更新されるようにする必要があります。 新しいデータがない場合、空のブロックがチェーンに追加されます。

4.15 ダイアグラム,

時間が左から右に進むにつれて（図2）、構築される源泉証明チェーンも長くなります。そのどの時点でも、チェーンの生産者は濃い境界をもつエントリーを訪問者に提供することによって使用可能になる前にエントリーの2番目の署名を待つようになります。たとえば、3番目の列でエントリー2と1だけチェーンの一部として返されます。

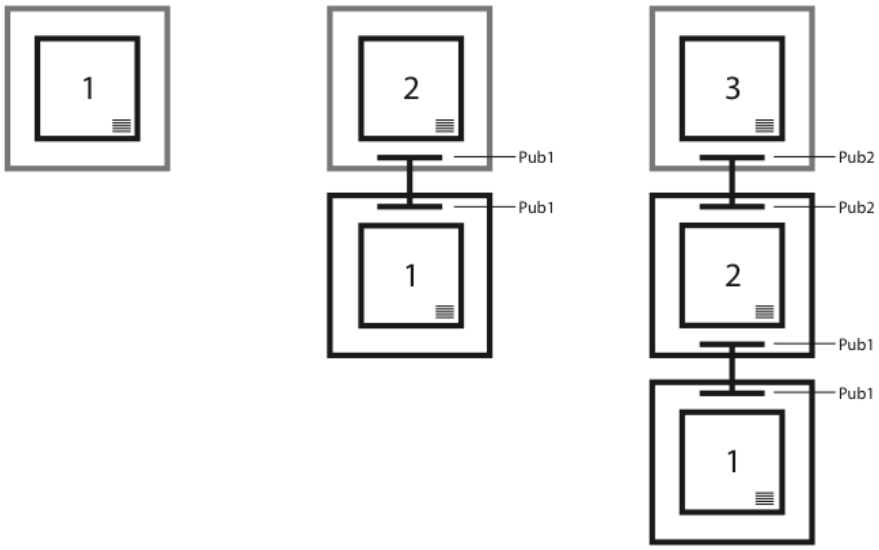

図2. 源泉証明チェーンでのリンクの例

4.16 要約

一時的なプライベートキー（秘密鍵）と順次ペアで署名され、ペアになったパブリックキー（公開鍵）を含む一連のデータパケットを基に、パケットが同じ源泉から来たものであることが絶対的に確かであると決定することができます。

---

5 セキュリティ関連事項

5.1 偽のディバイナー攻撃

デジタル署名のセットは、XYOスマートコントラクトに送られますが、これは契約が回答を送信したディバイナーの完全性を確認する必要があるからです。その後、契約は高い信頼性の間隔でこのリストに署名した他のディバイ

ナーを確認することができます。これがなければ伝達オロクルがシステム内で唯一の異常および危険源となるでしょう。

5.2　センチネルのDDoS攻撃

考えるべきまた別の攻撃に、特定区域内でのセンチネルノード間における「分散サービス拒否攻撃」（Distributed Denial of Service：DDoS）があります。攻撃者は、センチネルに多くの接続をしようとして、センチネンタルが正確な情報を伝えたり、どんな情報もブリッジに伝達することを妨害しようとします。私たちは、センチネルに接続しようとするすべての妨害に対して、小さな暗号化されたパズルを要求することによって解決することができます。

クエリは、センチネルに多数の接続をしないので、XYOリレーシステムに大きな負担を与えない上、攻撃者が私たちのネットワークのDDoS攻撃を成功させるためには多くのリソースを使用しなければいけないように要求をする。いかなる時点でも源泉証明チェーンはXYOメインチェーン上に保存されているすべてのものを通じて、誰でも確認することができます。これにより、もしチェーン上の単一の主体が侵害された場、クエリの回答の正確性（源泉チェーンスコア）は0に落ちます。

6　XYOトークンの経済

オラクルは、分散化したアプリケーションのための力とインフラストラクチャのニーズの重要な部分であす。主な焦点は、信頼できるオーケーの接続性と集約性を中心にしています。　分散化されたアプリケーションが最大の可能性を達成するためには、完全に分散されたトラストレス（信頼性の必要がない）オラクルのシステムが必要であると考えています。

6.1　XYOネットワークの暗号経済学

XYOトークンを使用して、正確で信頼性の高いロケーション（位置）ヒューリスティックを提供するという望ましい動作を導きます。 XYOトークンは、特定の事物のXY座標を検証するために現実世界との接続に必要な「 Gas（ガス）」と考えることができます。

このプロセスは次のように行われます：まず、トークン保有者がクエリ(query)をもってXYOネットワークに質問をします。

（例：「XYOアドレス0x123456789の電子商取引注文パッケージの位置は？」）。　その後、クエリはキュー(queue)に送られ、処理と返答を待ちます。 ユーザーは、クエリを作成する時に希望する信頼性レベルとXYO Gasの価格を設定することができます。クエリのコスト（XYOトークンの単位）は、そのクエリに対する回答を提供するためのデータの量と市場の状況をもとに決定されます。　データがたくさん必要になればなるほど、クエリが高価になり、XYO Gasの価格が高くなる。 XYOネットワークに対するクエリは、非常に広範囲なうえ高価になる可能性があります。 たとえば、運送会社や物流会社は、XYOネットワークに質問して、「各車両の位置は？ 」と質問できるでしょう。

XYOトークン保有者がXYOネットワークに質問をして要求されたGasを支払うと、タスクに取り組んでいるすべてのディバイナー（データを分析してクエリに回答する）は、関連するアーキビストを呼び出して、クエリに答えるために必要な関連データを検索する。　返されたデータは、もともとセンチネルからデータを収集したブリッジから得られたものです。　センチネルは、基本的に個体の位置を確認するデバイスまたは信号です。　これらには、Bluetoothトラッカー、GPSトラッカー、IoTデバイスに組み込まれたジオロケーション追跡(geo-location tracking)、衛星追跡技術、QRコードスキャナー、RFIDスキャニングなどの多くの機能が含まれます。 XY Findablesは、消費者のブルートゥースとGPSビジネスを先駆けて立ち上げ、現実世界の位置ヒューリスティックをテスト、処理するこ

とを可能にしました。 XY Findablesの消費者ビジネスを構築するためのあらゆる努力は、XYOネットワークブロックチェーンプロトコルの設計に大きく貢献しました。

センチネルデバイス（Bluetoothビーコンなど）が提供するデータを使用してクエリに回答する場合、取引に関連する4つのすべての構成要素がトークン所有者が支払ったXYO Gasの一部を受け取ります。その4つの構成要素は次の通りである：ディバイナー（回答を検索）、アーカイバー（データを保存）、ブリッジ（データを送信）、センチネル（位置データを記録）。XYO ネットワークの4つの構成要素のうち、3つの間にGasは常に同じ割合で分配されます。

ディバイナーの例外として、回答を提供するプロセスでの参加がより広範囲です。 各構成要素内でGasは均等に分配されます。

6.2 独立性に対する報償

位置収集デバイスは、ネットワークのアトミックブロックであり、単一のデバイスは、システムの4つの構成要素のうちの1つまたは複数として機能することができます。 しかし、特に大きなXYOネットワークでは、デバイスがこれらの構成要素の2つ以上の役割を行うことはまれです。 さらに、より独立した源泉証明を有するブロックチェーンの台帳は、より高く評価されるため、複数の構成要素に機能するデバイスには暗号経済的なペナルティが付与される。

6.3 定常性・完全性に対する報酬

XYOネットワーク内のセンチネルには、そのライフサイクル全体にわたる移動量に応じて定常性の係数が割り当てられます。センチネルがある期間に移動が少ないほど、データの信頼性が上がります。 アーキビストは、どのセンチネルにクエリをルーティングするのか検討する際に、これらの定常性の係数を追跡して分析します。

6.4 トークン使用のインセンティブを提供

トークン所有者がトークンを使用するように奨励しないシステムでは、基礎経済の長期的な問題を招く。 これは、価値の保存が非常にまれな生態系を生み出し、有用性と流動性を高める代わりにトークンを使用しない理由を生み出します。

今日の多くの暗号化通貨は、トークン・マイナー（例：センチネル、ブリッジ、アーキビスト、ディバイナーなど）にあまりにも焦点を置き、トークン・ユーザーには全く集中していない。 XYOトークンは両方どちらにも集中する。

XYOトークンモデルは、正確なデータを提供するだけでなく、データを提供する時点を把握するために、マイナー（採掘者）にインセンティブを与える。 ネットワークの流動性が高いときに比べて、ネットワークの流動性が低いときは、エンドユーザーが多く取引するほど報酬を受ける。 したがって、XYOトークンの生態系は、バランスが良く流動的で丈夫です。

6.5 XYOトークンの詳細スペック

パブリックトークンの販売は、1ETH：100,000XYOで開始し、1ETH：33,333XYOで始まる階層構造の価格設定をしています。量と時間に基づく価格設定の詳細は、間もなく発表される予定です。

- スマートコントラクトプラットフォーム：イーサリアム
- コントラクトのタイプ：ERC20

- トークン：XYO
- トークン名： XYOネットワークユーティリティトークン
- トークンアドレス：0x55296f69f40ea6d20e478533c15a6b08b654e758
- 発行総額： トークン・メインセールの後に到達した金額で上限
- XYOトークン見込資本額: 4,800万ドル
- 売れ残りおよび未割り当てトークン：トークン販売イベントの後でバーン(burn)される。
  メインセール終了後は、それ以上XYOトークンは生成されない。

7　XYOネットワークの ユースケース

XYOネットワークは、多数の産業にわたる広範囲で活用することができます。たとえば、主な消費者に代金引換サービスを提供する電子商取引会社を挙げることができます。電子商取引会社がXYOネットワークや XYOプラットフォーム（XYOトークンを使用）を活用してスマートコントラクト（イーサリアムのプラットフォームなど）を作成することによって、こういったサービスを提供することができます。 XYOネットワークはその後、消費者に送られる商品の位置をはじめ、倉庫の棚から出荷の際の宅配業者、そして消費者の家と中間のすべてのフルフィルメントを追跡できるようになります。これにより、電子商取引の小売業者やウェブサイトは、信頼できる方法（トラストレス）で、商品が消費者の玄関だけでなく、自宅の中に安全に届けられたことを確認することができます。商品が消費者の家に到着したことが確認されると（特定のXY座標で定義・確認）、配送は完了したものとみなされ、ベンダーに支払われる。 XYOネットワークの電子商取引の統合により、販売業者を不正行為から守り、消費者も商品が自宅に到着した後に代金を支払うことができます。

上記の例とは別に、ホテルレビューサイトに XYOネットワークを結合するケースを考えてみます。このサイトの現在の問題は、レビューの内容が信頼性に欠ける場合が多いという点です。 当然ホテルのオーナーは、どんなに費用がかかったとしてもレビューを改善しようとするでしょう。 例えば、米国サンディエゴに住んでいるある人がインドネシアのバリ島に行き、ホテルに2週間滞在した後に自宅のあるサンディエゴに戻ってバリ島のホテルのレビューを書いたとしたらどうでしょうか？ このレビューは非常に信頼されたでしょう。特に、レビューの投稿者が確認した位置データをもとに多くのレビューを書いたとしたら、なおさらでしょう。

8　XYOネットワークの拡張

私たちは幸運にも、世界中の100万（1,000,000）台以上のBluetoothとGPSデバイスを備えた実世界のネットワークを構築しました。ほとんどの位置情報ネットワークはこの段階まで達しておらず、広範囲なネットワークを構築するのに必要な最小必要量を確保できていません。私たちが作成したセンチネルネットワークは出発点にすぎません。XYOネットワークは、位置デバイスの運営者がアクセスしてXYOトークンの獲得を開始することができるオープンシステムです。

一般的に、XYOネットワークのセンチネルの数が大きければ大きいほど、その信頼性は高くなる。 さらにネットワークを拡大するため、XYOネットワークは他の企業と協力して、独自のXY Findablesビーコンを超えるセンチネルネットワークを拡張しています。

---

9 謝辞

本ホワイトペーパーは、以下の方々と 私たちのビジョンの信念によって可能になった勇敢なチームの努力の産物です。：ホワイトペーパーをより簡潔に整理して、技術的な詳細を世界に伝えるのに貢献してくださったラウル・ジョーダン（ハーバード大学、 ティール・フェロー、XYOネットワークアドバイザー）：卓越した検討作業を詳細に行ったクリスティン・サコ（特に、構成と模範的なケースに関してサポートを提供）：
関連したユースケースの調査 と編集をしてくださったジョニー・コラシンスキー：そして 、慎重なレビューとクリエイティブな意見をくださったジョン・アラーナに感謝します。

参考文献

[1] Blanchard, Walter. Hyperbolic Airborne Radio Navigation Aids. Journal of Navigation, 44(3), September 1991.

[２] Karapetsas, Lefteris. Sikorka.io.
http://sikorka.io/files/devcon2.pdf. Shanghai, September 29, 2016.

[3] Di Ferrante, Matt. Proof of Location. https://www.reddit.com/r/ethereum/comments/539o9c/proof of location/. September 17, 2016.

[４] Goward, Dana. RNT Foundation Testifies Before Congress. US House of Representatives Hearing: “Finding Your Way: The Future of Federal Aids to Navigation,” Washington, DC, February 4, 2014.

用語解説

正確度（accuracy）
あるデータポイントまたはヒューリスティック(heuristic)が特定の誤差範囲内にあるという信頼性の尺度

アーキビスト（Archivist）
アーキビストは、すべての履歴台帳を保存するために、分散型データセットの一部としてヒューリスティックを保存します。一部のデータが失われたり一時的に利用できなくなっても、システムは正確度がやや低下するものの機能し

続けます。 また、アーキビストは台帳をインデックス化して必要なときに台帳データの文字列を返すことができます。アーキビストはローデータだけを保存し、データの検索に対してのみを支払いを受けます。保管は常に無料です。

ベストアンサー（Best Answer）
回答の候補(Answer Candidate) のリストの中で最高の妥当性スコアを提示して最小限に必要な正確性より高い正確度スコアを提供する1つの答え。

ベストアンサーアルゴリズム（Best Answer Algorithm）
ディバイナーが回答を選択するとき、ベストアンサースコアを生成するために使用されるアルゴリズム。XYOネットワークは特化されたアルゴリズムの追加を許容し、ユーザーはどのアルゴリズムを使用するのか指定することができます。同じデータセットを与えられたディバイナー上で実行するとき、アルゴリズムは同じスコアにならなければなりません。

バウンド・ウィットネス（Bound Witness）
バウンド・ウィットネスは、双方向ヒューリスティックの存在によって実現される概念です。 デジタルコントラクトの解決（オラクル）のためのトラストレス（信頼の必要がない）データソースが有用ではないため、ヒューリスティックを構築して提供されるデータの確実性は大幅に向上します。第1の双方向ヒューリスティックは接近性(proximity)ですが、これは、双方の関係者が相互作用に共同署名することによって相互作用の発生と範囲を検証できるためです。これによって、2つのノードが互いに近接しているというゼロ知識証明(zero-knowledge proof)が可能です。

ブリッジ（Bridge）
ブリッジはヒューリスティックトランスクライバー(transcriber)です。センチネルからディバイナーにヒューリスティック台帳を安全に伝達します。ブリッジの最も重要な側面は、ブリッジから受け取ったヒューリスティックの台帳がどんな形にも変更されていないことをディバイナーが安心できる点です。ブリッジの2番目に重要な側面は、オリジンメタデータ(metadata)の証明も加えてしてくれる点です。

確実性（certainty）
データポイントまたはヒューリスティックに破損または改ざんがない可能性の尺度。

暗号化された位置情報（crypto-location）
暗号の位置情報技術の領域

暗号経済学（cryptoeconomics）
分散化されたデジタル経済における通貨やサービスの生産、流通、消費を運営するプロトコルを研究する正式な規律。暗号経済学は、これらのプロトコルの設計と特徴付けに焦点を当てた実用的な科学です。

ディバイナー（Diviner）
Divinerは、XYOネットワークによって保存された履歴データを分析することによって、クエリに対して回答します。XYOネットワークに格納されているヒューリスティックは、ヒューリスティックの妥当性と正確さを判断するために、高いレベルの源泉証明を持っていなければなりません。ディバイナーはその源泉証明に基づいて証人を判断することによって、回答を得て伝達します。 XYOネットワークはトラストレス（信頼の必要がない）システムなため、ディバイナーは正当なヒューリスティック分析を提供するよう導かれなければならない。ディバイナーはセンチネルやブリッジとは異なり、プルーフオブワーク（Proof of Work）を使用してブロックチェーンに対する回答を追加します。

ヒューリスティック（heuristic）
センチネルの位置（接近性、気温、光、動きなど）と関連する実世界のデータポイント。

オラクル（oracle）

正確かつ確実な回答を提供することによってデジタルコントラクト（契約）を解決するDApp（分散型アプリケーション）システムの一部。暗号学から由来する「オラクル」という用語は、真のランダムソース（例：乱数のこと）を意味する。オラクルは、暗号化の等式からそれ以上の世界へ必要なゲート(gate)を提供します。オラクルは、チェーン（実際の世界またはオフチェーン）を超えたスマートコントラクト情報を提供します。オラクルは、デジタルの世界から現実世界へのインターフェースです。Last Will＆Testament（遺言と遺言状）を例に挙げてみましょう。 遺言は遺言者が死亡したことを確認した条件のもとで実行されます。 オラクル・サービスは、公式のソースから関連データを編集・集約することによって、遺言を実行するためのオラクルサービスが構築されます。 オラクルは、該当者の死亡を確認するために、スマートコントラクトのためのフィード(feed) またはエンドポイントとして使用することができます

源泉チェーンスコア（Origin Chain Score）
源泉チェーンに対して、その信頼性を決定するために割り当てられたスコア。この評価は、長さ、絡み合い、重なり、冗長性が考慮されます。

源泉ツリー（Origin Tree）
ヒューリスティックの台帳の源泉を確実性のレベルで構築するために、さまざまな源泉チェーンから得た台帳エントリーデータセット。

源泉証明（Proof of Origin）
源泉証明（Proof of Origin）は、XYOネットワークに流れ込む台帳が有効なものなのか検証するための鍵(key)です。データソースに対する固有のIDは偽造される可能性があるため実用的ではありません。XYOネットワークのほとんどが物理的に安全であることが困難または不可能なため、やはり実用的ではなく、悪意をもつ何者かによって秘密鍵が盗まれれる可能性が非常に高い。これを解決するために、XYOネットワークは一時的キーの変更（Transient Key Chaining）機能を使用します。この機能の利点は、データの源泉チェーンを改ざんすることは不可能な点です。しかし、一度チェーンが壊れると永久に破損した状態になって維持できないため、孤立した状態になります。

源泉証明チェーン（Proof of Origin Chain）
一連のバウンド・ウィットネスのヒューリスティック台帳エントリーを一緒にリンクする一時的キーチェーン

プルーフオブワーク（Proof of Work）
プルーフオブワーク（PoW）は、特定の要件を満たし、生産するのが難しい（つまり、コストがかかり時間がかかる）が、他のモノによって容易に検証できるデータです。プルーフオブワークは、発生確率の低いランダムなプロセスであるため、有効なプルーフオブワークを生成するまで、厳密な試行錯誤が必要です。

センチネル（Sentinel）
センチネルはヒューリスティックな証人です。 一時的な台帳を作成することによって、それらの確実性と正確性を保証します。センチネルの最も重要な側面は、ディバイナーがオリジンに源泉証明（Proof of Origin）を追加することで同じソースから来たものであることを確信することができる台帳をセンチネルが作成する点です。

スマートコントラクト（smart contract）
ビットコイン以前のおよそ1994年頃にNick Szaboが作ったプロトコルです（ビットコインの伝説的な開発者である中村聡氏であると信じている人もいる）。スマートコントラクトの基本的な概念は、法的な契約をプログラムをコード化し、人間が契約を解釈して実行する代わりに、分散化したコンピュータによってその条件を実行するように作ることです。 スマートコントラクトは、通貨（例：イーサ）や契約を同じ概念として分類します。そのスマートコントラクトは決定論的であり（コンピュータプログラムのように）、完全に透過的で確認が可能なため、仲介者やブローカーに代わる強力な手段になります。

一時的なキーチェーン （Transient Key Chain）
一時的キーの暗号学を使用して一連のデータパケットをリンクする一時的なキーチェーン。

トラストレス（trustless：無信頼性）
システム内のすべての関係者が標準的な真実が合意に達することができる特性。 単一の個人または団体（銀行、政府、金融機関など）に集中するのではなく、ネットワークの利害関係者（開発者、採掘者、消費者など）に力と信頼が分配されます。 この概念は非常に誤解されやすい一般用語です。ブロックチェーンは事実上、信頼を失わずにシステム内の1人のアクター（利用者。人間に限らずマシンや別のシステムも含まれる）から要求される信頼の量を最小限に抑えます。これは、アクターがプロトコルで定義されたルールに協力するようにインセンティブする経済ゲームを通じて、システム内の複数のアクター間で信頼を分配することによって行われます。

XY オラクルネットワーク
XYOネットワーク.

XYOネットワーク
XYOネットワークは、「XYオラクルネットワーク」を意味します。このネットワークは、センチネル、ブリッジ、アーキビスト、ディバイナーを含むXYOを実行する構成要素/ノードのシステム全体で構成されています。XYOネットワークの主な機能は、現実の世界の地理的位置(geo-location)の検証によってデジタルスマートコントラクトを実行できるポータルとして機能することです

XYOメインチェーン（XYO MainChain）
クエリの取引やディバイナーから収集したデータと関連する源泉証明スコアを保存するXYOネットワークの変更不可能なブロックチェーン。