التقرير البحثي لـXYO Network :Proof of Origin (سند المصدر) المستند إلى الشبكة التشفيرية لتحديد الموقع

عده أري تراو*، وماركوس ليفين†، وسكوت شيبر‡
يناير 2018

نبذة مختصرة

مع الظهور المتزايد للتقنيات المعتمدة على الموقع، فإن خصوصيتنا وأماننا يعتمدان بشدة على دقة معلومات الموقع وصحتها. تم إجراء العديد من المحاولات التي تهدف إلى إزالة الحاجة إلى الكيانات المتمركزة التي تتحكم في تدفق بيانات الموقع ولكن كل محاولة اعتمدت على نزاهة الأجهزة التي تجمع هذه البيانات في العالم المادي. إننا نقدم شبكة موقع تشفيرية لا تتطلب منح الثقة تستخدم صيغة جديدة تعتمد على سلسلة من الإثباتات صفرية المعرفة لتحقيق درجة عالية من اليقين في بيانات معلومات الموقع. XYO Network (XY Oracle Network) هي خاصية مجردة تتيح التأكد من صحة بيانات الموقع بشكل طبقي من خلال العديد من فئات الأجهزة والبروتوكولات. وجوهرها مجموعة من الآليات التشفيرية التي تعرف بـ Proof of Origin وBound Witness وهي آليات تربط بين قوة تقنية سلسلة الكتل "بلوك تشين" وبين تجميع بيانات العالم الحقيقي داخل نظام واحد مع التطبيقات المباشرة حاليًا.

---

1 مقدمة

مع ظهور العقود الذكية التي لا تتطلب الثقة في طرف آخر المبنية على تقنية سلسلة الكتل، ازدادت بشكل ملحوظ الحاجة إلى خدمات أوراكل التي تمثل حَكَمًا على نتائج العقد. وتعتمد معظم عمليات تنفيذ العقود الذكية الحالية على مجموعة مفردة أو مجمعة من نظم الأوراكل المعتمدة في تسوية نتائج العقد. وفي الحالات التي من الممكن أن يتفق فيها الطرفان على الثقة في أوراكل محددة وأنها غير قابلة للتلف، فهنا تكفي أوراكل واحدة. ولكن في العديد من الحالات، إما لا توجد أوراكل مناسبة أو أنه لا يمكن اعتمادها بسبب إمكانية حدوث خطأ أو تلف بها.

نظم أوراكل المواقع تقع في هذه الفئة. إن التنبؤ بموقع عنصر في العالم المادي يعتمد على مكونات الإبلاغ والنقل والتخزين والمعالجة في نظم أوراكل معينة، وجميعها قابلة للخطأ وللتلف. ومن بين المخاطر المحتملة: تداول البيانات، وتلوث البيانات، وفقدان البيانات، وتزويرها.

XYO Network, arie.trouw@xyo.network
XYO Network, markus.levin@xyo.network
XYO Network, scott.scheper@xyo.network

ولذلك توجد المشكلة التالية: حيث إن التأكد ودقة الموقع تتأثران سلبًا بنقص قواعد بيانات الأوراكل اللامركزية التي لا تحتاج إلى الثقة في طرف ثالث المتعلقة بالموقع. لقد تم استخدام منصات مثل Ethereum وEOS بشكل مكثف نظرًا لقدرتها على التوسط بين التعاملات بشكل آمن عبر الانترنت، وتشتمل حالات الاستخدام الأولية على مستندات تجميع الأموال في صورة ICOs. ولكن، حتى هذه المسألة ركزت كل منصة بالكامل على عالم الانترنت وليس على العالم المادي وذلك لأن قنوات المعلومات الحالية تتسم بالضوضاء وإمكانية تعطل تكامل البيانات.

لقد عملت XYO Network تجاه مفهوم تمكين المطورين -مثل أولئك الذين يكتبون عقودًا ذكية لمنصات سلسلة الكتل- من التفاعل مع العالم المادي كما لو كان واجهة برمجة تطبيقات. تعد XYO Network أول بروتوكول أوراكل في العالم يجعل من الممكن لكيانين أن يتعاملا في العالم الحقيقي بدون طرف ثالث متمركز. إن تجريداتنا تتيح لنا أن نجعل التحقق من صحة بيانات الموقع الذي لا يتطلب منح الثقة من الغير بالنسبة للمطورين، وإنشاء بروتوكولاً بحالات استخدام جديدة لم تكن ممكنة حتى اليوم.

سيتم إنشاء XYO Network على بنية تحتية تتكون من أكثر من مليون جهاز حول العالم تم توزيعها من خلال أعمال تجارية مواجهة للمستهلكين يسهل العثور عليها. تسمح أجهزة نظام تحديد المواقع العالمي وبلوتوث إكس واي للمستهلكين اليوميين أن يضعوا إرشادات تتبع فعلية على الأشياء التي يريدون تتبعها (مثل: المفاتيح، والأمتعة، والدراجات، وحتى الحيوانات الأليفة). وإذا فقدوا عنصرًا ما أو وضعوه في غير مكانه، يمكنهم أن يروا أين هو بالضبط عن طريق رؤية موقعه على تطبيق الهاتف الذكي. في غضون ستة أعوام فقط، أنشأت XYO Network واحدة من أكبر شبكات البلوتوث وتحديد المواقع في العالم من حيث المستهلكين.

---

2 الخلفية التاريخية والمناهج السابقة

2.1 إثبات الموقع Proof of Location

ظهر مفهوم الموقع الذي يمكن إثباته أو التحقق منه منذ الستينيات ويمكن حتى أن يرجع تاريخه إلى الأربعينيات عبر أنظمة الملاحة الراديوية الأرضية مثل LORAN [1]. أما في الوقت الحالي، توجد خدمات للمواقع تجمع عدة وسائل للتحقق من الموقع إلى جانب وسائل أخرى لإنشاء ما يسمى إثبات الموقع من خلال التقسيم الثلاثي للموقع وخدمات النظام العالمي لتحديد المواقع GPS. برغم ذلك فإن هذه النهج يجب حتى الآن أن تتناول الجانب الأكثر أهمية الذي نواجهه في تقنيات الموقع حاليًا: وهو تصميم نظام يرصد الإشارات الاحتيالية ويردع تزوير بيانات الموقع. ولهذا السبب، نقترح أن تكون منصة الموقع المشفر الأكثر أهمية اليوم ستكون هي المنصة التي ينصب تركيزها على إثبات والتحقق من مصدر الإشارات المادية للموقع.

ما يبعث على الدهشة أن فكرة تطبيق التحقق من الموقع على سلسلة الكتل (البلوك تشين) ظهرت لأول مرة في سبتمبر 2016 في المؤتمر السنوي الثاني لمطوري الإيثريوم Ethereum's DevCon 2. وكان من قدم هذه الفكرة ليفتريس كارابيتساس وهو أحد مطوري إيثريوم من برلين. وقد أتاح مشروع كارابيتساس الذي يسمى Sikorka الهادف لتمكين استخدام العقود الذكية فرصة في الموقع بالعالم الواقعي باستخدام المصطلح الذي أطلقه هو باسم "Proof of Presence." وقد ركز تطبيقه الذي يربط الموقع وعالم سلسلة الكتل (البلوك تشين) في المقام الأول على حالات استخدام الواقع المعزز وقدم مفاهيم مبتكرة مثل تحدي الأسئلة في التحقق من موقع المرء[2].

في 17 سبتمبر 2016، ظهر مصطلح "Proof of Location","إثبات الموقع" رسميًا في مجتمع الإيثريوم [3].

وبعد ذلك قام مطور أساس الإيثريوم "مات دي فيرين" بتبسيطه:

"وكان المصطلح حينئذ قد شُرح ونوقش بالتفصيل من قبل مطور مؤسسة الإيثريوم مات دي فيرانتي. حتى لو كان لديك العديد من المشاركين الذين يمكنهم التصديق على موقع كل منهم للآخر، لا يوجد أي ضمان بأنهم لن يذهبوا "سيبيل" في أي لحظة في المستقبل، ولأنك تعتمد دائمًا على إبلاغ الغالبية فقط، فهذا ضعف شديد. إذا كان من الممكن أن تتطلب نوعًا من الأجهزة المادية المتخصصة التي بها تقنية مضادة للتلاعب بحيث يتدمر المفتاح الخاص عندما يحاول أحد أن يفتح أو يغير البرامج الثابتة عليه، في هذه الحالة قد تحصل على أمن أكبر، ولكن في نفس الوقت من غير المحتمل من المستحيل أن تخدع إشارات نظام تحديد المواقع العالمي. إن التطبيق المناسب لهذا الأمر يستلزم الكثير من الاحتياط والعديد من مصادر البيانات المختلفة لضمان الدقة، وعليه يجب أن يمول المشروع بصورة جيدة." [3]
— مات دي فيرانت، مطور أساس الإيثريوم

2.2 إثبات الموقع Proof of Location: أوجه القصور

باختصار، من الممكن فهم "إثبات الموقع" بأنه دعم الخصائص القوية لتقنية سلسلة الكتل مثل ختم التوقيت وعدم المركزية، وجمعها مع جهاز/أجهزة عمليات تحويل خارج السلسلة والأجهزة المحددة للموقع، وهذه الأجهزة لحسن الحظ مقاومة للتلاعب. إننا نشير إلى حيز تكنولوجيا الموقع التشفيرية بأنظمة "crypto-location." على غرار الطريقة التي تتمحور بها نقطة ضعف العقود الذكية حول قواعد بيانات الأوراكل التي تستخدم مصدر ثقة واحد (وبالتالي يصبح لديها مصدر وحيد للعطل)، فإن أنظمة المواقع المشفرة تواجه المشكلة نفسها. تتمركز نقاط ضعف تقنيات المواقع المشفرة الحالية حول الأجهزة التي تمارس عملها بعيداً عن سلسلة الكتل (بلوك تشين) والتي تبلغ عن موقع شيء ما. في العقود الذكية، يكون مصدر البيانات غير المتعلق بسلسلة الكتل (بلوك تشين) عبارة عن أوراكل. في XYO Network, يتنقل مصدر البيانات غير المتعلق بسلسلة الكتل في العالم الحقيقي كنوع متخصص من أوراكل نطلق عليه Sentinel. إن الابتكار الأساسي المحيط بـ XYO Network يتمركز حول الإثبات القائم على الموقع المزود بهوية غير مكشوفة، وهذا الإثبات يوجد ضمنيًا في مكونات نظامنا من أجل إنشاء بروتوكول الموقع المشفر الذي لا يتطلب منح الثقة من الغير.

---

3 شبكة XY Oracle

"اشتهرت منذ سنوات الحاجة إلى نظام يصعب إزعاجه ليتكامل مع نظام تحديد المواقع العالمي. إن نظام تحديد المواقع العالمي نظام ممتاز ودقيق ويعتمد عليه، ومع ذلك فإن التشويش والتلاعب والهجمات الإلكترونية وغيرها من صور التداخل تتزايد في عددها وخطورتها. وهذا يحمل احتمالية حدوث آثار مدمرة على أنشطتنا الحياتية والاقتصادية." [4]
— دانا غووارد، رئيس قاعدة RNT

3.1 مقدمة

الهدف من XYO Network هو إنشاء نظام لا يتطلب منح الثقة من الغير ولامركزي خاص بالموقع وهو أوراكل بحيث يكون نظامًا مقاومًا للهجمات ويخرج معلومات يقينية بأعلى درجة ممكنة عند الاستعلام عن البيانات المتاحة. إننا نحقق ذلك من خلال مجموعة من التجريدات التي تحد بشكل كبير من خطر التلاعب ببيانات الموقع عن طريق سلسلة من إثباتات "صفرية المعرفة" داخل مكونات النظام.

3.2 نظرة عامة عن الشبكة

يوفر نظامنا نقطة دخول إلى بروتوكول من الأجهزة المتصلة التي تقدم بيانات الموقع بدرجة عالية من اليقين من خلال سلسلة من الإثباتات المشفرة . يستطيع المستخدمون أن يقوموا بإجراء المعاملات، التي يطلق عليها اسم "queries," (استعلامات) من أجل استرجاع جزءًا من بيانات الموقع على أي منصة سلسلة كتل تقوم بوظيفة العقد الذكي.[1] ثم تستمع مجمعات من XYO Network إلى هذه الاستعلامات التي يصدرها للعقد ، ويحصل على الإجابات التي تتميز بأعلى دقة من مجموعة أجهزة غير متمركزة تقوم بنقل الإثباتات المشفرة على مراحل إلى تلك المجمعات. ثم تقوم تلك المجمعات بإمداد العقد الذكي بهذه الإجابات بعد الوصول إلى إجماع على الإجابة بأفضل نتيجة. تمكنت شبكة المكونات هذه من تحديد وجود شيء ما في موضع محدد XY ووقت معين بأقصى قدر ممكن من اليقين المحقق الذي لا يتطلب منح ثقة الغير .

XYO Network تتكون من أربعة مكونات أساسية: Sentinels (أجهزة لجمع البيانات), و Bridges (أجهزة لنقل البيانات), و Archivists (أجهزة لتخزين البيانات), و Diviners (أجهزة لجمع الإجابات). Sentinels تجمع معلومات الموقع عن طريق أجهزة استشعار، وأجهزة راديو، وغير ذلك من الوسائل. ثم تأخذ Bridges هذه البيانات من Sentinels وتعطيها لـ . Archivists تخزن Archivists هذه المعلومات لكي تقوم Diviners بتحليلها. Diviners تحلل البيانات الافتراضية للموقع من Archivists لتقديم إجابات للاستعلامات وتعيين درجات دقتها. ثم تقوم Diviners بنقل هذه الإجابات إلى العقد الذكي (ولذلك فإن Diviners تعمل كـأوراكل). درجة الدقة تعرف بـ Origin Chain Score ويتم تحديدها من خلال مجموعة من الإثباتات صفرية المعرفة المعروفة كذلك باسم Proof of Origin Chain. تضمن السلسلة جزأين أو أكثر من البيانات الناشئة من نفس المصدر بدون كشف أي معلومات أساسية. يقوم كل مكون على طول مسار الاستعلام بإنتاج Proof of Origin خاص به وهو ما يتم نقله بعد ذلك إلى المكون الذي تنتقل البيانات إليه. يعد Proof of Origin تركيبًا جديدًا يقوم ببناء سلسلة من الضمانات التشفيرية على طول مسار من مكونات التي ترحل البيانات من بعضها لبعض في الشبكة من أجل تقديم ثقة عالية في بيانات العالم الحقيقي. يقوم Proof of Origin Chain بتغليف الثقة التي يمكننا الحصول عليها في جزء من بيانات موقع تمامًا نزولا إلى الأجهزة الأولى التي جمعت المعلومات. وسوف نكتشف كيف يعمل Proof of Origin بعمق في الفصل التالي.

لتأسيس آلية إجماع غير مركزية بين Diviners، ستعتمد XYO Network على سلسلة كتل (بلوك تشين) عامة غير قابلة للتغيير تعرف بـXYOMainChain تعمل على تخزين معاملات الاستعلام إلى جانب البيانات المجمعة من Diviners ودرجة المنشأ المرتبطة بها. قبل أن نغوص في تفاصيل وظائف النظام بأكمله، سوف نعرّف بوضوح مسئوليات كل مكون من مكونات شبكتنا.

3.2.1 أجهزة Sentinels

Sentinels هي شهود الموقع. إنها ترصد البيانات الافتراضية وتجزم بـحقيقة ودقة البيان الافتراضي عن طريق إنتاج سجلات . الأمر الأكثر أهمية في Sentinels هو أنها تنتج سجلات يمكن للمكونات الأخرى أن تتأكد من أنها آتية من نفس

[1] يتضمن ذلك الإيثريوم، البتكوين+ RSK, EOS, IOTA, NEO, Stellar، وCounterparty، وMonax، وDragonchain، وCardano، وRChain، وLisk وغيرها.

المصدر. إنها تقوم بذلك عن طريق إضافة Proof of Origin إلى سلسلة نقل من الإثباتات المشفرة . علمًا بأن XYO Network هو نظام لا يتطلب الثقة من الغير، يجب أن يتم تحفيز Sentinels لكي تعطي معلومات موقع صادقة. ويتم هذا عن طريق الجمع بين مكون السمعة ومكون الدفع. يكافأ Sentinel بـ XYO) XYO Network Tokens) عندما تُستخدَم معلوماتها في إجابة استعلام ما. ولزيادة فرصها في المكافأة، يجب أن تنشئ سجلات متوافقة مع السجلات التي تنشئها نظرائها وتوفر Proof of Origin لتميّز نفسها بصفتها مصدر معلومات الموقع.

3.2.2 أجهزة Bridges

Bridges هي ناسخات بيانات الموقع. إنها تقوم بنقل السجلات من Sentinels إلى Archivists. الجانب الأكثر أهمية في Bridge هو أن Archivist يمكنه من أن يتأكد أن سجلات البيانات الافتراضية المستلمة من Bridge لم يتم تغييرها بأي طريقة. والجانب الثاني من حيث الأهمية في Bridge هو أنها تزود بـ Proof of Origin إضافيًا. علمًا بأن XYO Network هو نظام لا يتطلب الثقة من الغير، يجب أن يتم تحفيز Bridges لتقدم بيانات افتراضية صادقة. ويتم هذا عن طريق الجمع بين مكون السمعة ومكون الدفع. وتكافأ Bridge بالعملات الرمزية (التوكن) XYO) XYO Network) عندما تُستخدَم المعلومات التي قامت بنقلها في إجابة استعلام ما. ولزيادة فرصها في المكافأة، يجب أن تنشئ دفاتر متوافقة مع السجلات التي تنشئها نظائرها وتوفر Proof of Origin لتميّز نفسها بصفتها ناقل البيانات الافتراضية .

3.2.3 أجهزة Archivists

Archivists تخزن معلومات الموقع من Bridges في صورة غير مركزية بهدف تخزين كافة سجلات الأحداث التاريخية . وحتى إذا فُقِدت بعض البيانات أو أصبحت غير متاحة مؤقتًا، يستمر النظام في العمل، ولكن بدقة أقل. كما أن Archivists تفهرس الدفاتر وبالتالي يمكنها أن تسترجع سلسلة من بيانات الدفتر بسهولة عند الحاجة لذلك. تقوم Archivists بتخزين بيانات أولية فقط وتحصل على توكن (العملات الرمزية) XYO Network تُدفَع لها لمجرد استرجاع البيانات واستخدامها التالي لذلك. التخزين مجاني دائمًا.

أجهزة Archivists متصلة بالشبكة، وبالتالي عند طرح سؤال على Archivist فإنه يسأل الـ Archivists الأخرى عن البيانات التي لا يحتوي هو عليها. يمكن لـ Archivist اختياريًا أن يخزن أي معلومات سجل يرجع إليه. وسينتج عن هذا في الغالب نوعان من Archivists: النوع الأول هو الذي يكون عند حافة إنتاج البيانات في "السحابة"، والنوع الثاني هو الذي يكون عند حافة استهلاك البيانات في "السحابة". Archivists التي تكون في المنتصف ستكون هجائن. لا يُفرَض تخزين البيانات قهرًا لكن إجراء ذلك بسهولة من خلال IPFS أو غيره من حلول التخزين اللامركزية. كل مرة يتم فيها تسليم البيانات من Archivist إلى Archivist آخر، يتم إلحاقه بـ Proof of Origin من أجل تتبع الدفع، وبالتالي يتم الدفع لكل الـ Archivists. ولاسترداد النقود، يمكن تعيين أدنى Proof of Origin من أجل زيادة الصلاحية. يجب تنظيم اهتمامات Sentinels، وBridges، وArchivists من أجل منع تضخم البيانات.

3.2.4 أجهزة Diviners

Diviners هي الجزء الأكثر تعقيدًا في XYO Network. الهدف الكلي لـDiviner هو أن يجلب أكثر البيانات دقة من أجل استعلام ما من XYO Network وينقل تلك البيانات إلى المستعلم . تقوم Diviners باستقصاء منصة سلسلة الكتل القابلة للتطبيق (أي: ايثريوم، أو ستيلار، أو كاردانو، أو IOTA إلخ.) للاستعلامات الصادرة إلى العقود الذكية XYO. بعد ذلك تجد الإجابة عن الاستعلام عن طريق التفاعل مباشرة مع شبكة Archivist من أجل جلب الإجابة بأعلى درجة من الدقة/ الثقة. إنها تقوم بذلك عن طريق الحكم على الشاهد بأفضل Proof of Origin Chain. أجهزة Diviners التي تقدم الإجابة بأعلى درجة وفي أقصر مدة زمنية سيكون لها القدرة على إنشاء كتلة من سلسلة الكتل XYO الأساسية (

XYOMainChain) من خلال Proof-of-Work. تأخذ الاستعلامات مستوى أولوية حسب قدر المكافأة والتعقيد، كلما زاد ما تعرضه XYO مقابل إجابة ما، كلما زادت أولوية الاستعلام.

تحقق الـ Diviners الأخرى الإجماع على صحة الكتلة وتقوم بالتوقيع رقميًا عليها. الـ Diviner الذي كان عنوان أساس العملة في هذه السلسلة سوف يرسل بعد ذلك صفقة للعقد الذكي تحتوي على الإجابة إلى جانب درجة دقتها. ويرسل أيضًا قائمة بتوقيعات بقية الـ Diviners الأخرى من أجل منع المهاجم من إصدار معلومات مزيفة في سلسلة الكتل (بلوك تشين) من خلال التظاهر بكونها Diviner. يمكن للعقد الذكي بعد ذلك أن يتحقق من صحة تكامل هذه المعلومات عن طريق فحص قائمة توقيع الحمولة.

3.3 وظائف شاملة

الآن بعد أن فصّلنا مسئوليات كل مكون، فيما يلي نعرض مثالًا لكيفية عمل النظام بشكل شامل من البداية إلى النهاية:

1. بيانات تجميع Sentinels

- تعمل Sentinels على تجميع بيانات افتراضية الخاصة بالموقع بالعالم الحقيقي وتجهيز Proof of Origin الخاص بها والمراد إرفاقه بالعُقد الموجودة فوقها.

2. بيانات تجميع Bridges من Sentinels

- تجمع Bridges البيانات الضرورية من sentinels عبر الانترنت وتقوم بإلحاق Proof of Origin بسلسلتها. ثم تجعل Bridges نفسها متاحة لـ Archivists في الشبكة.

3. تقوم Archivists بفهرسة/ تجميع البيانات من Bridges

- ترسل Bridges باستمرار معلومات إلى Archivists التي يتم بعد ذلك حفظها في مستودعات غير مركزية مع فهرس البيانات الافتراضي بتحديد موقع.

4. تقدم Diviner إجابة إلى استعلام مستخدِم

- تقوم Diviners باستقصاء على الاستعلامات المرسلة إلى العقد الذكي إيثريوم وتقرر بدء عملية صياغة الإجابة

5. تجمع Diviners البيانات من Archivists

- ثم تقرر Diviners أن تأخذ استعلامًا عن طريق إحصار المعلومات المناسبة التي تحتاجها شبكة Archivist.

6. يقوم Diviner بصياغة الإجابة.

- يختار Diviners الـ Best Answer عن الاستعلام من شبكة Archivist التي تحتوي على أفضل Origin Chain Score.

7. يقدم Diviner كتلة

- ثم تقدم Diviners كتلاً على XYOMainChain بها محتويات إجابة الاستعلام، وعملات XYO الرمزية (XYO) المدفوعة من خلال Proof of Work. يقوم بقية الـ Diviners على الشبكة بالتوقيع رقميًا على محتويات الكتلة، ثم يكون حساب Diviner قاعدة العملة في الوقت الحالي محدثًا لأجل إبراز Proof of Work الخاص بها في النظام بمجرد الوصول إلى إجماع على كتلة صحيحة.

8. يرجع Diviner النتيجة إلى المبادر بالاستعلام

- يقوم Diviners بوضع الإجابة و Origin Chain Score الخاص بها، ومجموعة التوقيعات الرقمية الخاصة بها، ويرسلها إلى مكون محول يقوم بدوره بالاتصال بعقد XYO الذكي. المحول مسئول عن التأكد من سلامة الـ Diviner وأنه لم يتعرض للاختراق، ويرسل مجموعة الإجابات الموقّع عليها رقميًا

إلى العقد الذكي. يحدث هذا بعد عملية إنشاء الكتلة مباشرة. بعد ذلك يتم الدفع للـ Diviner على منصة coinbase مقابل صنيعه .

9. تُكافأ مكونات XYO Network على عملها

- تحصل المكونات المرفقة بـ Proof of Origin Chain على دفع مقابل مشاركتها في جلب إجابة الاستعلام. كل من Sentinels و Bridges و Archivists و Diviners يحصل على مكافأة مقابل عمله.

في حالة طلب نفس الاستعلام أكثر من مرة، قد تنتج أكثر من إجابة لأن الإجابة المنتجة في لحظة معينة مبنية على البيانات الافتراضية المتاحة التي يمكن أن يقدمها النظام في ذلك الوقت. إرسال إجابة إلى سلسلة الكتل يتم في خطوتين. أولاً: يجب عمل تحليل لتحديد Best Answer للاستعلام. إذا أنتج النظام عدة إجابات، ستقوم العقد بمقارنة الإجابات ودائمًا تختار الإجابة الأفضل. مثال على استعلام بسيط: "أين كانت العقدة في الشبكة في زمن معين بالماضي؟"

3.4 سلسلة الكتل (بلوك تشين) كمصدر وحيد للحقيقة

Diviners في صميمها تقوم ببساطة بتحويل البيانات النسبية إلى بيانات مطلقة. إنها قادرة على استكشاف شبكة Archivist حتى تثبت الإجابة المطلقة لاستعلام ما على شبكة XYO Network .Diviners هي أيضًا العقد التي تعرض الكتل وتضيفها إلى XYOMainChain ، وتحصل على مكافآت مقابل Proof-of-Work. نظرًا لكون شبكة Archivist هي مخزن للبيانات غير المعالَجة، وسلسلة الكتل هي مخزن للبيانات المطلقة المعالجة، يمكن في النهاية أن تستخدم الشبكة أحدث معلومات على XYOMainChain من أجل الإجابة عن الاستعلامات المستقبلية بدلاً من الاعتماد على الحسابات باهظة الثمن عبر شبكة Archivist.

ولأن الكتل في XYOMainChain تخزن Proof of Origin Chain ومخطط للمكونات التي استخدِمَت في إجابة الاستعلامات، ويمكن لـ Diviners المستقبلية استكشاف هذه البيانات المطلقة من أجل الوصول إلى نتائج دقيقة مع تقليل استخدام عرض النطاق. ومن ثَم، ستصبح XYOMainChain تدريجيًا أهم مصدر جدير بالثقة في النظام. ومع ذلك ستظل شبكة Archivist مطلوبة من أجل الحفاظ على أحدث المعلومات المتعلقة بالبيانات الافتراضية الموقع التي تجمعها Sentinels.

3.5 إطار XYO Network لاختيار مرشح The Best Answer

إننا نعرّف Best Answer بأنها الإجابة الوحيدة -من بين قائمة الإجابات المرشحة- التي تعطي أعلى درجة صحة، وتعطي درجة دقة أعلى من الدرجة الدنيا للدقة المطلوبة. تتحدد درجة الصحة على أساس Origin Chain Score. إن النظام يعرف ما هو أعلى سجل لـ Origin Score، وهو ما ينبغي أن يكون 100 بالمائة حتى تتحقق درجة أعلى لسجل آخر ويصبح هو صاحب الـ 100 بالمائة الجديدة. تسمح XYO Network باختيار Best Answer Algorithm من أجل تحديد Best Answer. وهذا يؤدي إلى توسعة نطاق البحث في المستقبل عن خوارزميات بديلة.

عندما يتم استبعاد بيانات عن الإجابة بها لأنها سيئة وغير صحيحة، سيتم نقلها إلى archivists حتى يتمكنوا من تنظيف مستودعاتهم غير المركزية من هذه البيانات.

3.6 الدمج الأولي مع سلاسل الكتل العامة

صممت شبكة XYO Network لتكون مجردة يمكنها التفاعل مع أي عقد ذكي وسلسلة كتل عامة صالحة مثل إيثريوم، وبيتكوين، و+Cardano، Stellar، NEO، EOS، RSK وغيرها. للتفاعل مع XYO Network، يمكن أن يطلق المستخدمون على إيثريوم -على سبيل المثال-استعلامات إلى عقد XYO الذكي الخاص بنا ودفع توكن XYO (ERC20).

إن العُقَد في سلسلة كتل XYO والتي تسمّى بـDiviners، وهي التي ستقوم بعمل استقصاء عن إيثريوم باستمرار لهذه الاستعلامات وتكافأ بالعملة الأصلية من سلسلة كتل XYO (والتي تسمى أيضًا توكن (العملات الرمزية) XYO). وفي المستقبل، سنقوم بعمل تحويل واحد-إلى-واحد من حاملي توكن (العملة الرمزية) ERC20 إلى عملتنا الرمزية الأصلية عملة سلسلة الكتل من أجل إمداد منصاتنا بأجور معاملة تدعم متطلبات المدفوعات المصغرة اللازمة للكثير من حالات الاستخدام القابلة للقياس. وفي هذه الحالات، سوف نسمح للمستخدمين بإطلاق استعلامات مباشرة إلى سلسلة الكتل الخاصة بنا بدلاً من التفاعل من خلال عقد ذكي عام.

---

4 Proof of Origin

عند وجود شبكة مادية تشتمل على عُقد غير جديرة بالثقة، من الممكن تحديد دقة البيانات التي توفرها عقد الحواف المستندة على الإثبات صفري المعرفة بأن جزأين أو أكثر من البيانات أتيا من نفس المصدر. وباستخدام مجموعات البيانات هذه، مجتمعة مع عدد من مجموعات البيانات المتشابهة ومعرفة الموقع المطلق لعقدة واحدة على الأقل، من الممكن التحقق من الموقع المطلق للعقدة الأخرى.

4.1 مقدمة عن Proof of Origin

تعتمد الأنظمة التقليدية التي لا تحتاج إلى الثقة في طرف ثالث على مفتاح سري لتوقيع المعاملات أو العقود في النظام. وهذا يعمل بشكل جيد جدًا بافتراض أن العقدة على الشبكة التي توقِّع على البيانات المعنية مؤمنة ماديًا وافتراضيًا. ومع ذلك إذا كُشِف المفتاح الخاص تتعثر القدرة على إثبات الأصل.

وعند تطبيق مفاهيم انعدام الحصول على الثقة من الغير على إتصال الأشياء بالإنترنت، يجب افتراض أن عقد الحواف في الشبكة ليست مؤمنة ماديًا أو افتراضيًا. وهذا يولد الحاجة إلى التعرف على عقد الحواف بدون استخدام معرفات فريدة، وإلى الحكم على البيانات المنتجة منها بأنها صادقة وصحيحة بدون أي معرفة من خارج الشبكة.

4.2 جوهر Proof of Origin: Bound Witnesses

يعتمد Proof of Origin على مفهوم Bound Witness. يعد من غير المفيد استخدام مصدر بيانات غير موثوق به في حل عقد رقمي (أوراكل)، ويمكننا تزويد يقين البيانات المتاحة بشكل كبير من خلال تأسيس وجود إثبات موقع ثنائي الاتجاه. يكون البيانات الافتراضيةلموقع ثنائي الاتجاه الأساسي تقريبيًا، لأن كلا الطرفين يمكنه إثبات حدوث تفاعل ما ونطاقه عن طريق التوقيع على التفاعل. وهذا يسمح بإنشاء إثبات صفري المعرفة أن العقدتين كانتا بالقرب من بعضهما البعض.

ثم نحن نحتاج إلى تحديد حقيقة أن عقدة شاهد أوراكل في نظام لا يتطلب ثقة الغير التي جمعت البيانات التي تشاركها. في النظام الذي لا يتطلب ثقة الغير، يمكن لعقدة الشاهد أن تنتج بيانات خاطئة بسبب عطل أو تلف. ومن الممكن اكتشاف البيانات غير الصالحة وحذفها ببساطة إذا كانت تقع خارج النطاق المسموح به لتلك البيانات الافتراضية . البيانات السارية ولكنها غير صحيحة (أي: البيانات الخاطئة) أصعب بكثير جدًا في اكتشافها.

4.3 مقارنة بين البيانات الافتراضية لتحديد الموقع أحادية الاتجاه وثنائية الاتجاه

معظم البيانات المتعلقة بالعالم الفعلي (بيان افتراضي) هي أحادية الاتجاه. وهذا يعني أن العنصر الذي يتم قياسه لا يستطيع أن يدعم إعادة القياس، مما يجعل البيانات الافتراضية أحادية الاتجاه من الصعب للغاية التحقق من صحتها. في البيانات

الافتراضية ثنائية الاتجاه، يستطيع العنصر المُقاس أن يبلغ الطرف الآخر عن قياساته الخاصة مما يجعل التحقق من صحتها ممكنًا. يعد الموقع بيانًا افتراضيًا نادرًا لأنه يمكن أن يكون ثنائي الاتجاه، بوجود عقدتي حواف تبلغان بعضهما البعض. **مثال على ذلك من العالم الحقيقي: شخصان قريبان من بعضهما البعض يلتقطان صورة ذاتية (سيلفي)، ويطبعان نسخة لكل طرف، ثم يوقع كل منهما على الصورة. هذه العملية تعطي كلا الطرفين "إثبات اقتراب". إن الطريقة الوحيدة التي يحصل بها هذان الشخصان على هذه "البيانات" هي أن يكونا معًا في نفس الموقع.**

لاحقاً، دعونا نناقش آثار الشبكة: تخيل نظامًا يتوقع من كل عقدة حواف فيه أن تنتج باستمرار هذه الصور "السيلفي" لأنهما يسافران، وتخزن الصور في مجلد مغلف. ويتوقع منها أيضًا أن تحتفظ بهذا المجلد في ترتيب زمني تسلسلي ولا يسمح لها أبدًا بحذف أي منها. وهذا ينشئ مسجِلًا للاقتراب لكل عقدة حواف من الممكن أن يكون مرجعًا ترافقيًا مع مسجلات عقد الحواف الأخرى.

4.4 عقد بدون حواف

تعتبر جميع العقد شهود "بما فيها عقد bridge، وعقد النقل والتخزين والتحليل. " وهذا يسمح بتقييد أي بيانات يتم نقلها من عقدة إلى العقدة التي تليها. وهذا هو مفهوم **Bound Witness** (الشهود المقيدة).

4.5 مرجع ترافقي

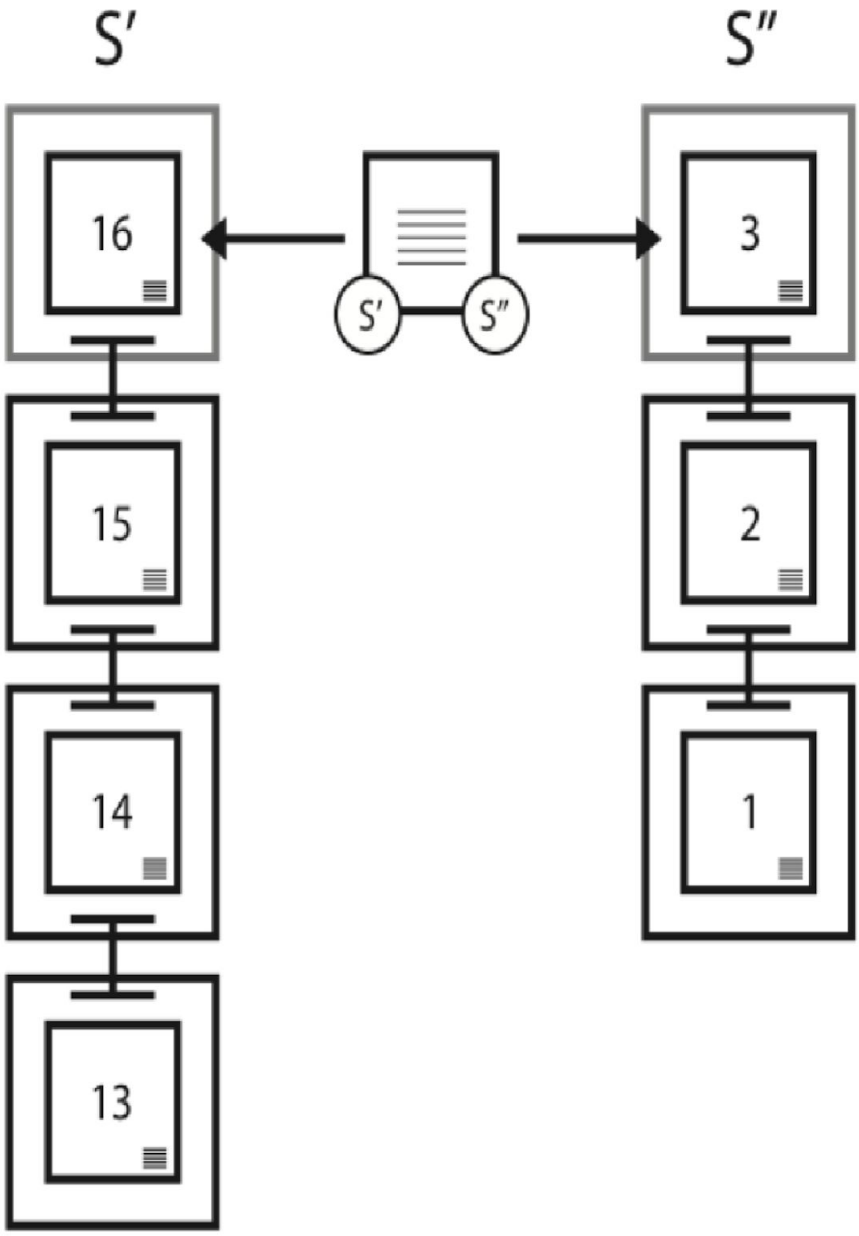
إن تحليل كل مجموعة من صور السيلفي المنتجَة والمقيدة معًا في كل عقدة حواف يسمح للنظام بإنتاج Best Answer من التقارب النسبي لجميع العقد الموجودة في الشبكة. إذا أخبرت كل عقدة بصدق وبدقة، فإن تعيين كل المواضع النسبية لعقد الحواف سوف يحقق أقصى يقين ودقة ممكنة: 100 بالمائة. وعلى العكس، إذا كانت كل عقدة غير صادقة أو مذهولة فقد تقترب درجة اليقين والدقة من الحد الأدنى وهو 0 بالمائة.

بإعطاء مجموعة من البيانات المبلغ عنها والاستعلام عن الوضع النسبي لعقد الحواف، من الممكن إنتاج الموقع بالتقريب إلى جانب معاملات اليقين والدقة.

وبإعطاء نفس المجموعة من البيانات ونفس خوارزمية التحليل، ينبغي أن تصل كل عملية حسابية إلى نفس الوضع التقريبي ونفس معاملات اليقين والدقة.

4.6 الرسم البياني

(الشكل 1) كل من S' و S" عبارة عن (عقدة حواف) Sentinel تقوم بجمع البيانات الافتراضية . وعندما تتصلان ببعضهما البعض، تتبادلان البيانات الافتراضية والمفاتيح العامة. كل منهما تبني سجلاً كاملاً من التفاعل وتوقع على التفاعل الناتج. ثم يصبح هذا السجل الموقع عليه المدخل التالي في كل من دفتريهما المحليين (16 لـ S' و 3 لـ S"). هذا العمل يقيد هذين الشاهدين بكونهما بالقرب من بعضهما البعض.



الشكل 1. مثال على تقييد الشاهد بين اثنين Sentinels

4.7 Origin Chains

كل أصل يحتفظ بسجله ويوقع عليه من أجل عمل Proof of Origin Chain. بمجرد مشاركة معلومة من Proof of Origin، تصبح ثابتة بفعالية. وهذا بسبب التفرع الذي يحدث بعد أن تصل المشاركة لنهاية السلسلة وتجعل كل البيانات المستقبلية من الشاهد تعامل كأنها آتية من شاهد جديد. ومن أجل إنتاج رابط Proof of Origin Chain، يقوم الأصل بإنتاج زوج مفاتيح عام/خاص. ثم يوقع على كل من الكتل السابقة والكتل التالية بنفس زوج المفاتيح بعد اشتمال الكتل على المفتاح العام. وبعد إجراء التوقيع مباشرة، يتم حذف المفتاح الخاص. يؤدي الحذف الفوري للمفتاح الخاص إلى الحد من خطر سرقته أو إعادة استخدامه بشكل كبير.

Proof of Origin Chains عبارة عن المفتاح الذي يعمل على التحقق من أن XYO Network صالحة. يعد تعيين معرف فريد لكل مصدر بيانات شيئًاغير عمليًا لأنه من الممكن أن يُزور. كما أنَّ توقيع المفتاح الخاص لا يُعد عمليًّا نظرًا لصعوبة أو استحالة تأمين أجزاء XYO Network ماديًّا، ومن ثم، فإنَّ احتمالية استيلاء الطرف السيئ على المفتاح الخاص أمر يمكن وقوعه . لحل هذه المشكلة، تستخدم XYO Network خاصية Transient Key Chains. حيث تكمن الفائدة من هذا الإجراء في أنَّه من المحال تزييف سلسة الأصل الخاصة بالبيانات. ومع ذلك، بمجرد تعطل السلسلة، فإنّها تتعطل للأبد ويحال استمرارها مما يجعل منها كتلة رقمية معزولة.

كل مرة يتم فيها تسليم دفتر البيانات الافتراضية في XYO Network، يقوم المستلم بإلحاق Proof of Origin الخاص به، بما يجعل Proof of Origin Chain أكثر طولاً وينتج نقطة تقاطع Proof of Originو Proof of Origin Chains. وتقاطعات Proof of Origin هي المؤشرات الأساسية التي تستخدمها Diviners للتحقق من صحة السجلات . المعادلة التي تبين سمعة السجل بفعالية هي: ما النسبة المئوية من XYO Network التي شاركت في صنع Proof of Origin Ball المرتبطة به. نظريًا إذا كان 100% من سجلات XYO Network مرتبطة بـ Proof of Origin ثم تم تحليلها بالكامل فإن فرصة كونها صحيحة تبلغ 100%. إذا كان 0% من سجلات XYO Network متاح للتحليل فتتراجع نسبة صحتها إلى 0%.

للمزيد من الحماية، لا يتم توفير المفتاح العمومي الخاص بـChain Link حتى يصبح الإدخال الثاني متاحاً. يتيح ذلك أيضاً نظرًا للفاصل الزمني ما بين الإدخالات أو غيرها من البيانات أن يتم تخزينها في الرابط السابق أو التالي.

4.8 Origin Chain Score

Origin Chain Score يتم حسابها كالتالي (الخورزامية الافتراضية):

- PcL = طول Proof of Origin Chain
- PcL = صعوبة Proof of Origin Chain
- O = تراكب Proof of Origin Chain لـPc وPc" Pc' Pc"

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

4.9 Origin Tree

تستخدم Origin Tree لحساب النسبة التقريبية لصحة إجابة ما. إنها تستخدم البيانات المجمعة لإنتاج الشجرة المثالية (Ideal Tree) وهي الشجرة التي توافق تلك البيانات بأفضل درجة ممكنة من أجل إعطاء إجابة مؤكدة. إذا كانت العقدة N موجودة في الموقع Z،T ، X،Y ، فيجب أن يحمل الخطأ عبر كل البيانات في المجموعة قيمة محددة. لحساب هذا الخطأ، يجب عليك احتساب الحد الأدنى، والحد الأقصى، والعادي،و المتوسط والمسافة المتوسطة عن العادي.

إذا كان لدينا مجموعة S من كل الدرجات s، وصعوبة PcD) Proof of Origin Chain)، وعامل خطأ error، فإنه يتم تحديد Best Answer كالتالي:

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

وبمعنى آخر، فإن الإجابة المؤكدة هي التي لها Best Answer Score وبهذا توصف بـ Best Answer. وباستخدام Proof of Origin Tree، يمكننا التعرف على الفروع المستحيلة (المتطرفة) وتهذيبها.

4.10 Transient Key Chaining

من الممكن عمل سلسلة من مجموعات من حزم البيانات عن طريق استخدام مفاتيح خاصة مؤقتة للتوقيع على الحزم المتتالية. عندما تشتمل حزم البيانات على المفتاح العام مقترنًا بالمفتاح الخاص، يمكن أن يتحقق المستلِم من أن كلتا الحزمتين تم توقيعهما بنفس المفتاح الخاص. لا يمكن تغيير البيانات في الحزمة بدون إنتهاك التوقيع، مما يضمن أن الحزم الموقع عليها لم يتم تغييرها بواسطة طرف ثالث مثل Bridge أو عقدة تخزين.

4.11 عمق الرابط

تنتج العقدة على الأقل زوج مفاتيح عام/خاص لك رابط في Proof of Origin Chain، ويكون عمق الرابط 1، ربما يوجد N مدخلات في جدول الرابط الخاص بمدخل سجل معين، كل مدخل يحدد المسافة في المستقبل عندما تتم إضافة الجزء الثاني من الرابط. لا يمكن أن يكون لرابطين نفس درجة المرتبة على مقياس القاعدة 2. على سبيل المثال، المدخل [1، 3، 7، 12، 39] مسموح به، أما المدخل [1، 3، 7، 12، 15] غير مسموح به.

يتم إنشاء رابط العمق 1 واستخدامه وحذفه عندما يتم نشر الكتلة السابقة. ومع ذلك، الروابط التي لها عمقِ أكبر من 1 يتم إنتاج زوج لها كما يتم توقيع الكتلة السابقة، ولا يحدث التوقيع الثاني حتى الكتل N فيما بعد، والتي بعدها يُحذَف المفتاح الخاص. ولهذا السبب، دائمًا ما تعتبر الروابط ذات العمق أكبر من 1 أقل أمنًا من الروابط ذات العمق 1، ولكن يمكن استخدامها لتحسين الأداء وتقليل فقدان البيانات على حساب ذلك الأمن.

4.12 الترتيب الثابت

يعد العنصر الرئيسي في تحديد تسلسل السجلات هو الترتيب الذي تم الإبلاغ عنها. علمًا بأنه من الممكن لجهاز ما أن يغير ترتيب أي سجل موقع عليه بـProof of Origin، ومن الممكن وضع ترتيب مطلق عن طريق النظر إلى السجلات مجتمعة.

4.13 النشر من الثاني-إلى-الأخير

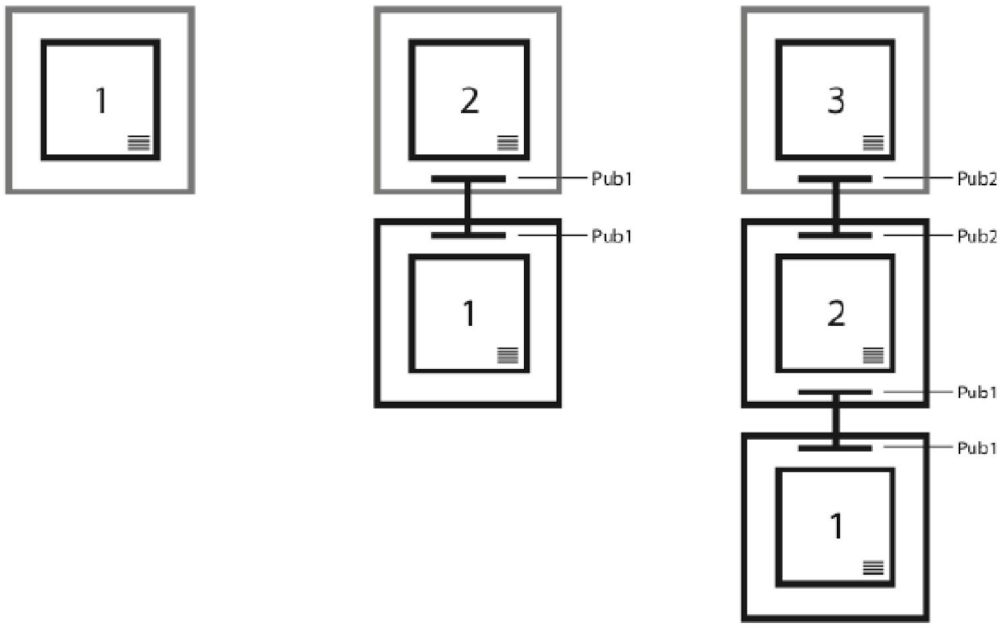
تتبني الطريقة الأولية لإنشاء Proof of Origin على أساس الحقيقة التي تفيد بأن Sentinel دائمًا يبلغ عن كتلة من الكتلة الثانية حتى الأخيرة بدون الإبلاغ عن الكتلة الأخيرة. وهذا يسمح للكتلة الأخيرة أن تجعل الرابط الموقع للكتلة التي تسبقها دليلاً على الرابط.

4.14 الروابط الفارغة

لجعل Proof of Origin Chain أكثر أمنًا، يتطلب الأمر ألا يتم تحديث السلسلة أكثر من مرة واحدة كل عشر ثوانٍ ولا أقل من مرة واحدة كل ستين دقيقة. وفي حالة عدم توفر بيانات جديدة، ستتم إضافة كتلة فارغة إلى السلسلة.

4.15 الرسم البياني

وبمرور الوقت من اليسار إلى اليمين (الشكل 2)، يزداد طول Proof of Origin Chain الذي يتم بناؤه. وفي أي لحظة زمنية سيوفر منتِج السلسلة للمتصل المدخلات ذات الحدود المظلمة فقط، مع انتظار التوقيع الثاني للمدخل قبل جعله متاحًا. على سبيل المثال، في العمود الثالث، فقط المدخلات 2 و 1 هي التي سيتم إرجاعها كجزء من السلسلة.



الشكل 2.مثال عن إدراج الرابط في Proof of Origin Chain

4.16 الملخص

إذا عُلِم أن تسلسلاً من حزم البيانات تم توقيعه في ثنائيات متتالية بمفاتيح خاصة مؤقتة وتتضمن المفاتيح العامة المزدوجة، يمكن القول بيقين مطلق أن الحزم أتت من نفس الأصل.

---

5 الاعتبارات الأمنية

5.1 هجوم Diviner مزيف

يتم إرسال مجموعة من التوقيعات الرقمية إلى العقد الذكي XYO لأن العقد يحتاج إلى التحقق من سلامة Diviner الذي أرسل الإجابة. بعد ذلك يمكن للعقد أن يتحقق من بقية Diviners التي وقّعت هذه القائمة خلال فترة ثقة عالية. وبدون ذلك، سيكون الأوراكل الناقل هو المصدر الوحيد للإخفاق والخطر في النظام.

5.2 هجمات Sentinel DDoS

الهجوم الآخر الذي يؤخذ في الاعتبار هو "الحرمان من الخدمة الموزع " (DDoS) بين عقد Sentinel في منطقة معينة . من الممكن أن يحاول المهاجم وضع عددًا ضخمًا من الاتصالات إلى Sentinels من أجل منعها من نقل المعلومات الصحيحة أو نقل أي معلومات مطلقًا إلى Bridge. ويمكننا إحباط هذه المحاولةعن طريق طلب حل لغز تشفيري صغير من أي شخص يحاول أن يتصل بـ Sentinel. وبما أن الاستعلام لن يشتمل على عدد ضخم جدًا من الاتصالات إلى Sentinels، فهذا لن يفرض حمل ثقيل على نظام ترحيل XYO، وسيتطلب من المهاجم إنفاق كمية ضخمة من الموارد لتنفيذ هجوم الحرمان من الخدمة الموزع DDoS ناجح على شبكتنا. وعند أي نقطة زمنية، يمكن لأي شخص التحقق من Proof of Origin Chain لأنه مُخزن في XYOMainChain. وهذا يضمن أنه إذا تم اختراق كيان واحد إلى جانب السلسلة فإن دقة إجابة الاستعلام (Origin Chain Score) سوف تهوى إلى صفر.

---

6 اقتصاد العملات الرمزية XYO

تعد Oracles جزءًا هامًا من احتياجات الطاقة والبنية التحتية للتطبيقات غير المركزية، مع كون معظم التركيز يدور حول الاتصال وتجميع أوراكل معتمدة. إننا نؤمن بالحاجة لنظام لا يتطلب ثقة الغير وغير مركزي بالكامل من أوراكل لأجل التطبيقات غير المركزية حتى تحقق الحد الأقصى من إمكانياتها.

6.1 الاقتصاد المشفرة XYO Network

إننا نستخدم عملات XYO لتحفيز السلوك المرغوب به وهو إعطاء بيانات افتراضية موقع دقيقة وموثوقة. يمكن أن نعتبر أن العملات الرمزية (التوكن) XYO بمثابة (التسعيرة الداخلية) أي الكلفة اللازمة للتفاعل مع العالم الحقيقي من أجل التحقق من موقع XY لأي شيء محدد.

تتم العملية بالطريقة التالية: أولًا يستفسر صاحب الرمز من XYO Network عن شيء ما (مثلا "أين الطرد المطلوب إلكترونيًا من خلال XYO بعنوان 0x123456789...؟") بعد ذلك يتم إرسال الاستعلام إلى صف ينتظر فيه حتى تتم معالجته وإجابته. يمكن للمستخدم تعيين مستوى الثقة المطلوب وتكلفة السعر الداخلي XYO عند الاستفسار. يتم تحديد كلفة الاستفسار (بتوكن XYO) من خلال كمية البيانات المطلوبة لتقديم إجابة السؤال أو الاستفسار إلى جانب ديناميكية السوق. كلما زادت البيانات المطلوبة، ارتفعت تكلفة السعر الداخلي XYO. إن الاستفسارات المرسلة إلى XYO Network من الممكن أن تكون كثيرة ومكلفة للغاية. فعلى سبيل المثال قد ترسل شركة الشحن والخدمات اللوجستية استفسارًا إلى XYO Network لكي تسأل (ما موقع كل سيارة في أسطول سياراتنا على حدة؟)"

بمجرد أن يستفسر حامل توكن XYO من XYO Network ويدفع التسعير الداخلي المطلوب فإن كافة أجهزة Diviners المسئولة عن تحليل البيانات والتي تتولى المهمة تستدعي الملفات ذات الصلة من Archivists لاسترجاع البيانات ذات الصلة اللازمة لإجابة السؤال أو الاستفسار. البيانات المسترجعة هي جزء مشتق من Bridges الذي جمع البيانات في البداية من Sentinels. Sentinels هي الأجهزة أو الإشارات التي تؤكد موقع الأشياء. ويتضمن ذلك أجهزة مثل أجهزة التتبع بالبلوتوث وأجهزة تحديد المواقع العالمية وأجهزة تتبع الموقع الجغرافي المدمجة في أجهزة إتصال الأشياء بالإنترنت وتكنولوجيا التتبع عبر الأقمار الصناعية وأجهزة مسح وقراءة أكواد الاستجابة السريعة والمسح الضوئي لأجهزة تحديد الهوية بموجات الراديو والعديد من الأجهزة الأخرى. اضطلعت شركة XY Findables بدور رائد وأطلقت مشاريع البلوتوث Bluetooth وGPS للمستهلك مما أتاح لها اختبار ومعالجة البيانات المستخلصة للمواقع في العالم المادي. إن

الجهود التي بذلت في تطوير مشاريع شركة XY Findables قد ساعدت بصورة كبيرة في تصميم برتوكول البلوك تشين لـ XYO Network.

إذا تم استخدام البيانات التي يوفرها جهاز Sentinel (مثل Bluetooth Beacon) المستخدم لإجابة الاستعلام، فإن كافة المكونات الأربعة المشاركة في المعاملة تتلقى جزءًا من التسعير الداخلي XYO الذي يدفعه حامل العملة الرمزية: Diviner (هو الذي بحث عن الإجابة)، وArchiver (هو الذي خزن البيانات)، وBridge (هو الذي أرسل نقل البيانات)، و Sentinel (هو الذي سجل بيانات الموقع). توزيع التسعير الداخلي ما بين 3 مكونات خاصة بـ4 مكونات لـ XYO Network يتم تقديمه دوماً في نفس النسبة والتناسب. الاستثناء هو في أن Diviners، والذي تعتبر مشاركته في عملية توفير الإجابة أكبر حجمًا. ويتم توزيع التسعير الداخلي (الغاز) بالتساوي في نطاق كل مكون.

6.2 مكافآت الاستقلالية

أجهزة تجميع المواقع عبارة عن كتل ذرية خاصة بالشبكة، وقد يعمل جهاز واحد بعمل مكون أو أكثر من مكونات النظام الأربعة. ورغم ذلك، سيكون من النادر خصوصًا في XYO Network الضخمة أن تمثل الأجهزة أكثر من مكونين من تلك المكونات. وبالإضافة إلى ذلك، سيحصل سجل سلسلة الكتل (بلوك تشين) الذي له Proof of Origin أكثر استقلالاً على تقدير أكبر، وبالتالي توجد عقوبة الاقتصاد المشفر للجهاز الذي يعمل بعمل مكونات عديدة.

6.3 مكافآت لتكامل التوقعية

Sentinels في XYO Network تكون مخصصة كمعامل توقعي يعبر عن مقدار حركتها خلال دورة الحياة الخاصة بها. كلما قلت تحركات Sentinel في مدة زمنية ما، كلما زادت الثقة في بياناتها. تقوم Archivists بمتابعة معاملات الثبوتية وتحليلها عند الحاجة لتحديد أي من Sentinels سيتم تمرير الاستعلامات إليه.

6.4 تحفيز استخدام العملات الرمزية (التوكن)

إن النظام الذي يُشجَّع فيه حاملو العملة الرمزية على عدم استخدام عملاتهم يخلق مشكلة طويلة المدى في الاقتصاد الأساسي. إنه يخلق نظام بيئي بمخازن ذات قيمة شحيحة جدًا ويخلق دافعًا طبيعيًا لاختراع أسباب لعدم استخدام العملة الرمزية، بدلاً من تعزيز الاستخدام والسيولة.

المشكلة لدى معظم محفزات الاقتصاد المشفر هو انصباب التركيز بشدة على معدني العملة (مثل: Sentinelsو Bridgesو Archivistsو Diviners) ولا ينصب إطلاقًا على مستخدمي العملة الرمزية. تأخذ عملة XYO الاثنين في اعتبارها.

يُحفز معدنو التوكن XYO ليس فقط لأجل تقديم البيانات الدقيقة وإنما أيضًا من أجل معرفة متى لا يقدمون أي بيانات على الإطلاق. يتم تشجيع المستخدم النهائي الذي يحمل العملات الرمزية (التوكن) XYO على إجراء الصفقات بكثرة في حال انخفاض سيولة الشبكة مقارنة بوقت ارتفاع سيولة العملات في الشبكة. ولذلك فإن النظام البيئي للتوكن (العملات الرمزية) XYO لديه القدرة أن يظل متوازنًا بشكل جيد ومرنًا وقويًا.

6.5 مواصفات العملات المميزة التوكن XYO

مبيعات العملة الرمزية العامة لها بنية تسعير متدرجة تبدأ بـ 1 إيثريوم: 100000 XYO وتصل الحد الأقصى عند 1 إيثريوم: 33,333 XYO. سنعلن قريبًا عن التفاصيل المتعلقة بالكمية وبنية التسعير القائمة على الوقت.

- منصة العقود الذكية: الإيثريوم
- نوع العقد: ERC20
- التوكن: XYO
- اسم التوكن: XYO Network الأداة المساعدة للتوكن
- عنوان التوكن: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- الإصدار الكامل: محدود بالكمية التي يصل إليها بعد عرض البيع الرئيسي لرمز
- رأس مال توكن XYO المتوقع هو 48 مليون دولار
- عملات رمزية غير مباعة وغير مخصصة: تصبح غير قابلة للإنفاق بعد عرض البيع للعملة الرمزية. لن يتم إنشاء المزيد من عملات XYO الرمزية بعد انتهاء المزاد الرئيسي.

---

7 حالات استخدام XYO Network

يمكن استخدام XYO Network في عدد ضخم من التطبيقات التي تغطي العديد من الصناعات. خذ على سبيل المثال إمكانية تقديم شركة تجارة إلكترونية لخدمة الدفع عند التسليم لعملائها. لكي تستطيع شركة التجارة الإلكترونية عرض مثل تلك الخدمة، فإنها سوف تزيد من خدمات XYO Network (والتي تستخدم عملات XYO الرمزية) لكتابة عقد ذكي (وهو عقد يُكتب على منصة إيثريوم). ويمكن لـ XYO Network بعد ذلك تتبع موقع الطرد الذي تم إرساله إلى المستهلك خلال كل خطوة من خطوات تنفيذ العقد؛ بدايةً من وجوده فوق رف المخزن وحتى وصوله لموظف الشحن، ومتابعته طوال الطريق حتى منزل المستهلك وكل موقع يمر عليه خلال تلك العملية . من شأن تلك العملية أن تمكن مواقع التجارة الإلكترونية والبائعين من خلالها التحقق بطريقة لا تتطلب الثقة من طرف آخر تمامًا من وصول الطرد بأمان إلى داخل بيت المستهلك وليس فقط على باب داره. وبمجرد وصول الطرد إلى منزل العميل (الذي يتم تحديده والتحقق منه عن طريق إحداثيات محاور الطول والعرض XY)، تُعتبر عملية الشحن منجزة ويتم تحرير مبلغ الدفع للبائع. وبهذا يتيح استخدام XYO Network في التجارة الإلكترونية القدرة على حماية التاجر من الغش ويضمن للمستهلكين ألّا يدفعون إلا ثمن البضائع التي تصلهم حتى بيوتهم فقط.

وننظر لاستخدام آخر مختلف تمامًا لـXYO Network في موقع تقييمات ومراجعات لفندق، والذي تكمن مشكلته الحالية في عدم الوثوق بأغلب التقييمات والمراجعات التي تصلهم من هذا الموقع. وبالطبع فإن أصحاب الفنادق متحفزون لتحسين التقييمات التي تصلهم بأي ثمن. ماذا لو استطاع المرء أن يقول بأعلى مستويات التأكد أنه كان شخصًا يعيش في سان دييجو، ثم ركب الطائرة وارتاد فندق في بالي ومكث هناك لمدة أسبوعين، وعاد إلى سان دييجو، ثم كتب تقييمًا لإقامته في ذلك الفندق ببالي؟ سيكون لذلك التقييم مكاننته العالية جدًا ، خاصةً إذا صدر عن شخص يعطي تقييمات عديدة بشكل دوري مع بيانات تؤكد زيارته لتلك الأماكن.

---

8 تمديد XYO Network

نحن محظوظون لامتلاكنا شركة تجارية لخدمة المستهلكين وقد نجحت بالفعل في بناء شبكة من مليون (1000000) جهاز في العالم الحقيقي يحتوي على أنظمة مثل البلوتوث ونظام تحديد المواقع GPS على مستوى العالم. تفشل معظم الشبكات المعتمدة على المواقع في الوصول إلى هذه المرحلة وتحقيق الكتلة الحرجة اللازمة لبناء وتطوير شبكة واسعة النطاق. تُعتَبر شبكة Sentinel التي أنشأناها نقطة البداية فقط. XYO Network هي نظام مفتوح يستطيع الدخول إليه أي شخص يقوم بتشغيل جهاز لتحديد الموقع ويبدأ في كسب العملات الرمزية (التوكن) XYO.

وبشكل عام، كلما زادت علاقات واتصالات شبكة Sentinel في XYO Network، كلما زادت فعاليتها وجدارتها بالثقة. وللمزيد من نمو شبكاتها، تقوم XYO Network بالاشتراك مع غيرها من الشركات لتوسيع شبكتها الخاصة من شبكات Sentinel خارج نطاق شبكتها الخاصة من البرامج الملحقة XY Findables.

---

9 كلمة شكر وعرفان بالجميل

هذا البحث التقريري هو نتيجة جهد متواصل من فريق عمل ملهِم، والذي أمكن إنجازه عن طريق الأشخاص التاليين من خلال إيمانهم بوجهة نظرنا: نقدم الشكر لراؤول جوردان (خريج جامعة هارفارد، الحاصل على زمالة ثيل ومستشار XYO Network); على مساهماته في جعل تقريرنا البحثي أكثر إيجازًا ولمساعدته لنا على نقل التفاصيل الفنية إلى العالم بشكل أنيق. ونشكر كريستين ساكو على أخلاقيات عملها الاستثنائية واهتمامها البالغ بالتفاصيل أثناء مراجعتها لعملنا. ويعود الفضل بالاتساق في هيكل وضع تقريرنا البحثي وأفضل الممارسات التي رُصدت فيه إلى جهود كريستين. ونشكر جوني كولاسينسكي على أبحاثه وتصنيفه لحالات الاستخدام القابلة للتطبيق. وأخيرًا، نشكر جون أرانا على مراجعته الدقيقة ومساهماته المبدعة.

مسرد المصطلحات

الدقة وهي مقياس الثقة في وقوع نقطة بيانات أو بيانات إفتراضية ضمن إطار هامش خطأ محدد.

Archivist يخزن جهاز Archivist البيانات الإفتراضية باعتبارها جزء من مجموعة البيانات اللامركزية مع الاحتفاظ بجميع السجلات التاريخية المُخزنة، لكن من دون الحاجة إلى الثقة في طرف ثالث . وحتى إذا فُقِدت بعض البيانات أو أصبحت غير متاحة مؤقتًا، يستمر النظام في العمل، ولكن بدقة أقل. كما تقوم Archivists بفهرسة السجلات بحيث يمكنها استرجاع سلسلة من بيانات السجل إذا لزم الأمر. تُخزّن Archivists بيانات أوّلية فقط وتتقاضى وحدها أجر استرجاع البيانات. التخزين مجاني دائمًا.

نعرّف Best Answer بأنها الإجابة الوحيدة -من بين قائمة الإجابات المرشحة- التي تعطي أعلى درجة صلاحية، وتعطي درجة دقة أعلى من الحد الأدنى المطلوب من الدقة.

Best Answer Algorithm هي إحدى الخوارزميات المستخدمة من أجل استنتاج Best Answer Scores حينما يختار Diviner إحدى الإجابات. تسمح XYO Network بإضافة خوارزميات متخصصة، كما تسمح للعميل بتحديد الخوارزمية المقرر استخدامها. من الضروري أن ينتج عن هذه الخوارزمية الدرجة نفسها حال تطبيقها على أي Diviner يعطي مجموعة البيانات ذاتها.

Bound Witness يُعد Bound Witness مفهومًا ناتجًا عن وجود بيان افتراضي ثنائي الاتجاه. نظرًا لأنَّ مصدر البيانات غير الموثوق فيه لاستخدام تسوية العقد الرقمي (أوراكل) غير مجدي، فإنَّ هناك زيادة ملحوظة في موثوقية البيانات الناتجة عن إنشاء هذا البيان الافتراضي . يكون البيانات الافتراضي لتحديدالموقع ثنائي الاتجاه هو الأساسي تقريبيًا، لأن كلا الطرفين يمكنه إثبات حدوث تفاعل ما ونطاقه عن طريق التوقيع على التفاعل. وهذا يسمح بإثبات صفري المعرفة أن العقدتين كانتا بالقرب من بعضهما البعض.

Bridge يُعد Bridge ناسخًا إرشاديًّا. إنَّه ينقل السجلات من Sentinels إلىArchivists. الأمر الأكثر أهمية في Bridge هو أن Diviner يستطيع أن يتأكد من عدم تغيير سجلات البيانات الإفتراضية المستلمة من Bridge بأي حال . ويتمثل الأمر الثاني من حيث الأهمية في Bridge في إضافة بيانات التعريف مصاحبة بـ Proof of Origin.

اليقين مقياس مدى احتمالية خُلوّ نقطة البيانات أو البيانات الإفتراضية من الفساد أو التلاعب.

تحديد الموقع المشفر وهو نطاق تكنولوجيا تحديد الموقع المشفر .

الاقتصاد المشفر إجراء رسمي يدرس البروتوكولات التي تحكم إنتاج البضائع والخدمات وتوزيعها واستهلاكها ضمن اقتصاد رقمي لامركزي. يُعد الاقتصاد المشفر علم عملي يُركز على تصميم هذه البروتوكولات وتحديد خصائصها.

Diviner يجيب Diviner إلى استفسار محدد من خلال تحليل بيانات الأحداث التاريخية التي خزنتها شبكة XYO Network. كما يجب أن تتضمن البيانات الإفتراضية المخزنة في XYO Network مستوى عالٍ من Proof of Origin لتحديد مدى سلامة البيانات الإفتراضية ودقتها.. يحصل Diviner على إحدى الإجابات ويسلمها من خلال الحكم على الشاهد استنادً إلى Proof of Origin الخاص به. نظرًا لأن XYO Network نظام لا يحتاج للثقة في طرف ثالث ، يجب تحفيز Diviners لتقديم تحليلات نزيهة للبيانات الإفتراضية . على النقيض من Sentinels وBridges، تيستخدم أجهزة Diviners خاصية Proof of Work لإضافة إجابات إلى سلسلة الكتل.

البيانات الإفتراضية وهي نقطة بيانات حول العالم الحقيقي مقارنة بموضع Sentinel (التقارب، ودرجة الحرارة، والضوء، والحركة، وما إلى ذلك).

أوراكل جزء من نظام DApp (التطبيقات اللامركزية) المسؤول عن إبرام عقد رقمي من خلال تقديم إجابة بكل دقة ويقين. يُشتق مصطلح "أوراكل" من التشفير حيث يعني مصدر عشوائي حقًا (على سبيل المثال، لرقم عشوائي). حيث يوفر هذا بوابة ضرورية من معادلة تشفيرية إلى العالم الخارجي. يقوم وسطاء أوراكل بتزويد معلومات العقود الذكية بما يتجاوز من وراء السلسلة (العالم الواقعي، أو عمليات تحويل خارج السلسلة). يمثل وسطاء أوراكل وصلات بينية من العالم الرقمي إلى العالم الحقيقي. خذ على سبيل المثال،أن تفكّر في عقد الشهادة والوصية الأخيرة لتُنفذ بنود الوصية بموجب تأكيد وفاة الموصي. كما يمكن تقديم خدمات أوراكل لبدء تفعيل الوصية من خلال تجميع وتبويب البيانات ذات الصلة من المصادر الرسمية. حينئذٍ،

يمكن استخدام أوراكل باعتبارها قناة تلقيم أو نقطة نهاية لعقد ذكي للاتصال من أجل التحقق مما إذا كان الشخص قد توفى أم لا.

Origin Chain Score الدرجة المحتسبة لإحدى سلاسل الأصل لتحديد مدى مصداقيتها. يأخذ هذا التقييم كلًا من الطول والتشابك والتداخل والتكرار بعين الاعتبار.

Origin Tree وهي مجموعة من بيانات مدخلات السجلات المستمدة من سلاسل أصل متعددة لإنشاء الأصل الخاص بمدخل السجل الاستدلالي بمقدار محدد من اليقين.

Proof of Origin يُعد Proof of Origin المفتاح المنوط التحقق من مدى صلاحية السجلات المتدفقة إلى XYO Network. يعد تعيين معرف فريد لكل مصدر بيانات أمرًا غير عمليًا لأنه من الممكن أن يُزور. كما أنَّ توقيع المفتاح الخاص لا يُعد عمليًّا نظرًا لصعوبة أو استحالة تأمين أجزاء XYO Network ماديًّا، ومن ثم، فإنَّ احتمالية استيلاء الطرف السيئ على المفتاح الخاص أمر قد يحدث . لحل هذه المشكلة، تستخدم XYO Network خاصية Transient Key Chaining. حيث تكمن الفائدة من هذه الخاصية في أنَّه من المحال تزييف سلسة الأصل الخاصة بالبيانات. ومع ذلك، بمجرد تعطل السلسلة، فإنّها تتعطل للأبد ويحال استمرارها مما يجعل منها كتلة رقمية معزولة.

Proof of Origin Chain هو Transient Key Chain التي تربط بين سلسلة إدخالات سجل البيانات الافتراضيات Bound Witness.

Proof of Work يُعد Proof of Work جزءًا من البيانات التي تُلبي بعض المتطلبات المحددة، فضلاً عن أنَّه يصعب تحقيقها (بعبارة أخرى، مكلّفة وتستغرق وقتًا طويلاً)، إلا أنَّه من السهل التحقق منها بالنسبة للآخرين. قد تتسم عملية إنتاج Proof of Work بأنَّها عملية عشوائية مع ضعف احتمالية استحداثها، ومن ثم، فإنَّه من الضروري إجراء التجربة الدقيقة والخطأ في إطار المعدل المتوسط قبل إنشاء Proof of Work صالح.

Sentinel يُعد Sentinelشهودًا على البيانات الإفتراضية. فهي ترصد البيانات الإفتراضية وتضمن دقتها وموثوقيتها من خلال إنتاج سجلات مؤقتة . وتتأكد أجهزة Diviners من أنَّها مستمدة من مصدر واحد وذلك من خلال إضافةProof of Origin إليها هو أحد أهم جوانب Sentinels.

العقد الذكي هو بروتوكول أول من وضعه كان نايك زابو قبل بيتكوين، حيث يُزعم أنَّه كان في عام 1994 (وهذا هو السبب وراء اعتقاد البعض بأنَّه هو سأتوشي ناكاموتو، مبتكر البيتكوين الغامض المجهول). تكمن الفكرة من العقد الذكي في تدوين اتفاق قانوني في برنامج وامتلاك أجهزة حاسوب لا مركزية تتولى مهمة تنفيذ بنوده، بدلاً من الحاجة إلى قيام الأشخاص بتفسير العقود واتخاذ إجراءات بشأنها. تجمع العقود الذكية كلاً من الأموال (على سبيل المثال، الإيثريوم Ether) والعقود في المفهوم نفسه. ونظرًا لأنّ العقود الذكية تتسم بالجبرية (مثل برامج الحاسوب) والشفافية الكاملة وقابلية قراءتها، فإنَّها تُعد بمثابة وسيلة جيدة للاستعاضة بها عن الوسطاء والسماسرة.

Transient Key Chain يربط Transient Key Chain سلسلة من حزم البيانات باستخدام تشفير Transient Key Cryptography.
عدم مطالبة الثقة في طرف آخر وهو إحدى السمات عندما يتوصل أطراف النظام كافة إلى اتفاق جماعي بشأن ماهية الوضع القانوني. يتم توزيع السلطة والثقة (أو مشاركتها) بين الجهات المعنية بالشبكات (على سبيل المثال، المطورين والمنقبين

والمستهلكين)، بدلاً من التمركز في فرد أو كيان واحد (على سبيل المثال، البنوك والحكومات والمؤسسات المالية). يُعد هذا المصطلح واحدًا من المصطلحات الشائعة التي يمكن إساءة فهمها بسهولة. في الحقيقة، لا يمكن أن تقضي سلاسل الكتل على الثقة. فما تقدمه هو تقليص مقدار الثقة المطلوب من أي طرف فردي في النظام. يتحقق هذا من خلال نشر الثقة بين مختلف أطراف النظام عبر لعبة اقتصادية تساعد على تحفيز الأطراف على التعاون مع القواعد المنصوص عليها في البروتوكول.

XYO Network **XY Oracle Network**

شبكة XYO Network ترمز شبكة XYO Network إلى XY Network الخاصة بأوراكل" فهي تتألف من نظام عناصر XYO / عقده التي تتضمن كلًا من Sentinels وBridges وArchivists وDiviners. تتمثل الوظيفة الأساسية لـ XYO Network في العمل بصفتها بوابة تنفذ من خلالها العقود الرقمية الذكية وذلك من خلال تأكيدات المواقع الجغرافية في العالم الحقيقي.

XYOMainChain هي سلسلة الكتل (بلوك تشين) غير القابلة للتغيير في XYO Network التي تخزن معاملات الاستعلام بالتزامن مع البيانات التي تم جمعها من Diviners ودرجة الأصل ذات الصلة.

11 المراجع

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

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

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

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