XY ऑरेकल नेटवर्क: उत्पत्ति के साक्ष्य पर आधारित क्रिप्टोग्राफ़िक लोकेशन नेटवर्क

एरी ट्रौ [1] , मार्कस लेविन [2], स्कॉट स्कीपर [3]

जनवरी 2018

आभासी प्रस्तुति

कनेक्टेड, स्थान-आधारित प्रौद्योगिकियों की बढ़ती मौजूदगी में, हमारी निजता और सुरक्षा के लिए स्थान संबंधी जानकारियों की सटीकता और वैधता काफी महत्वपूर्ण है। स्थान संबंधी डेटा के प्रवाह को नियंत्रित करने वाले केंद्रीकृत निकायों की आवश्यकता खत्म करने के लिए विभिन्न प्रयास किए गए हैं, लेकिन प्रत्येक प्रयास ने भौतिक दुनिया में इस डेटा को नियंत्रित करने वाले डिवाइस के सत्यता पर भरोसा किया है। हम स्थान संबंधी जानकारी के संदर्भ में डेटा की उच्चस्तरीय सुनिश्चितता स्थापित करने के लिए शून्य-जानकारी वाले साक्ष्यों की श्रृंखला पर आधारित नई संरचना का उपयोग करके एक गैर-भरोसा आधारित, कूटबद्ध (क्रिप्टोग्राफ़िक) स्थान का नेटवर्क प्रस्तावित करते हैं। **XYO नेटवर्क (XY ऑरेकल नेटवर्क)** एक आभासी प्रस्तुतिकरण है, जो कई डिवाइस श्रेणियों और प्रोटोकॉल में लेयर्ड, स्थान सत्यापन को सक्षम करता है। इसके केंद्र में **उद्भव के प्रमाण** और **प्रतिबद्धतापूर्ण साक्ष्य** नाम की नई कूटबद्ध पद्धतियों का सेट होता है, जो आज प्रत्यक्ष अनुप्रयोगों द्वारा ब्लॉकचेन प्रौद्योगकी और वास्तविक दुनिया की डेटा संग्रहण की शक्ति को एक सिस्टम में संयोजित करती हैं।

1 परिचय

ब्लॉकचेन-आधारित, गैर-भरोसा आधारित स्मार्ट कॉन्ट्रैक्ट की शुरुआत के साथ ही अनुबंध के परिणामों की विवेचना करने वाली ऑरेकल सेवाओं की आवश्यकता उल्लेखनीय रूप से बढ़ी है। स्मार्ट कॉन्ट्रैक्ट की नवीनतम कार्यान्वय पद्धति अनुबंध के परिणामों के निर्धारण के लिए प्राधिकृत ऑरेकल के एकल या एकीकृत सेट पर भरोसा करती है। जिन मामलों में दोनों पक्ष निर्दिष्ट ऑरेकल के प्राधिकार और अदूषणीयता पर सहमत होते हैं, उनके लिए यह पर्याप्त है। फिर भी, कई मामलों में, या तो कोई उपयुक्त ऑरेकल मौजूद नहीं होता या किसी त्रुटि अथवा दूषण की संभावना के कारण ऑरेकल को प्राधिकृत नहीं माना जा सकता है।

स्थान संबंधी ऑरेकल इस श्रेणी में आते हैं। भौतक दुनिया की चीज़ों के स्थान का अनुमान दिए गए ऑरेकल की रिपोर्टिंग, प्रसारण, संग्रहण और त्रुटि का परिचय देने व दूषित किए जा सकने वाले प्रसंस्करण अवयवों के आधार पर लगाया जाता है। जोखिमों में डेटा कौशल, डेटा प्रदूषण, डेटा क्षति और दुरभि संधि शामिल हैं।

[1] XYO Network, arie.trouw@xyo.network

[2] XYO Network, markus.levin@xyo.network

[3] XYO Network, scott.scheper@xyo.network

इसलिए, निम्नलिखित समस्याएँ होती हैं: **स्थान की सुनिश्चितता और सटीकता पर गैर-भरोसा आधारित, विकेंद्रीकृत स्थान ऑरेकल की कमी के चलते नकारात्मक प्रभाव पड़ता है।** ICOs के रूप में निधि की व्यवस्था करने वाले निलंब लेख के लिए निलंब लेख वाले प्राथमिक उपयोग के मामलों में ऑनलाइन सुरक्षित रूप से पारस्परिक क्रियाओं की मध्यस्थता करने की अपनी शक्ति के चलते इथीरियम और EOS जैसे प्लेटफ़ॉर्म का अत्यधिक उपयोग किया जाता है। फिर भी, भौतिक दुनिया में वर्तमान सूचना माध्यमों में बाधायुक्त, दूषणयोग्य डेटा सत्यता होने के कारण, अब तक प्रत्येक प्लेटफ़ॉर्म ने ऑनलाइन दुनिया पर पूरी तरह फ़ोकस कर लिया है।

XYO नेटवर्क डेवलपर को API की तरह भौतिक दुनिया से पारस्परिक क्रिया करने में सक्षम बनाने की अवधारणा के लिए काम करता रहा है। XYO नेटवर्क दुनिया का पहला ऑरेकल प्रोटोकॉल है, जो किसी केंद्रीकृत तृतीय पक्ष के बिना वास्तविक दुनिया में दो निकायों के बीच लेनदेन को संभव बना देता है। हमारा आभासी प्रस्तुतिकरण नए उपयोग के मामलों वाले ऐसे प्रोटोकॉल बनाकर हमें स्थान के सत्यापन को गैर-भरोसा आधारित बनाने की अनुमति देता है, जो आज तक संभव नहीं था।

XYO नेटवर्क दुनिया में संचरित होते 1,000,000 ऐसे डिवाइस के मौजूदा अवसंरचना पर बनाया जाएगा, जो अपने उपभोक्ता आधारित प्राप्य व्यवसाय को वितरित किए गए थे। XY के ब्लूटूथ और GPS डिवाइस की मदद से नियमित उपभोक्ता जिन चीज़ों पर निगरानी रखना चाहते हैं (जैसे चाबियाँ, सामान, दोपहिया वाहन और यहाँ तक कि पालतू जानवर), उन पर संकेतक (फ़िजिकल ट्रैकिंग बीकॉन) लगा सकते हैं। अगर उनसे ये चीजें खो जाएँ तो वे एक स्मार्टफ़ोन ऐप्लिकेशन के जरिए देख सकते हैं कि असल में ये चीजें किस स्थान पर हैं। मात्र छः वर्षों में XYO नेटवर्क ने दुनिया के सबसे बड़े उपभोक्ता ब्लूटूथ और GPS नेटवर्क में से एक तैयार कर लिया है।

2 ऐतिहासिक पृष्ठभूमि और पिछली पद्धतियाँ

2.1 स्थान का प्रमाण

प्रमाणन-योग्य स्थान की अवधारणा 1960 के दशक में आई और इससे पहले 1940 के दशक में भूतल-स्थित रेडियो-नेविगेशन सिस्टम, जैसे LORAN [1] से इसकी शुरुआत मानी जा सकती है। आज, ऐसी स्थान संबंधी सेवाएँ हैं, जिनमें ट्राएंगुलराइज़ेशन (त्रिकोणीकरण) और GPS सेवाओं के जरिए स्थान के साक्ष्य तैयार करने के लिए एक के बाद एक, कई माध्यम से सत्यापन होते हैं। फिर भी, ये पद्धतियाँ स्थान संबंधी आधुनिक प्रौद्योगिकी के संदर्भ में रोज़ाना हमारे सामने आने वाले सबसे महत्वपूर्ण घटक का समाधान अब तक नहीं उपलब्ध करा सकी हैं: ऐसा सिस्टम तैयार करना, जो जालसाजीपूर्ण सिग्नल की पहचान कर सके और स्थान संबंधी डेटा के स्पूफिंग को हतोत्साहित कर सके। इस कारण से, हम प्रस्तावित करते हैं कि आज सबसे महत्वपूर्ण क्रिप्टो-लोकेशन (कूट-स्थान) प्लेटफ़ॉर्म वह होगा, जो स्थान संबंधी भौतिक संकेतों की उत्पत्ति को प्रमाणित करने पर सबसे ज्यादा ध्यान दे।

आश्चर्यजनक रूप से, ब्लॉकचेन प्रौद्योगिकी पर स्थान सत्यापन लागू करने की अवधारणा पहली बार सितंबर 2016 में इथीरियम के DevCon 2 पर देखी गई। इसे बर्लिन के एक इथीरियम डेवलपर लेफ्टेरिस कारापेटसास ने शुरू किया। कारापेटसास के प्रोजेक्ट, *सिकोर्का* ने स्मार्ट कॉन्ट्रैक्ट को "मौजूदगी के साक्ष्य" का उपयोग कर वास्तविक दुनिया के स्थान पर नियोजन हेतु सक्षम बनाया। उसके स्थान के बीच सेतु बनाने वाले ऐप्लिकेशन और ब्लॉकचेन की दुनिया ने प्राथमिक रूप से संवर्धित वास्तविक उपयोग वाले मामलों पर फ़ोकस किया और उसने नई अवधारणाएँ प्रस्तावित किया, जैसे किसी का स्थान प्रमाणित करने के लिए चुनौति प्रश्न [2]।

17 सितंबर 2016 में, "स्थान का साक्ष्य" शब्द इथीरियम समुदाय में औपचारिक रूप से सामने आया [3]। इसके बाद यह पुनः इथीरियम फाउंडेशन के डेवलपर मैट डी फेरान्टे द्वारा प्रतिपादित किया गया:

> "*स्थान के जिस साक्ष्य पर आप भरोसा कर सकते हैं, सच कहें तो वह कार्यान्वित करने में सबसे कठिन चीज़ों में से एक है। यहाँ तक कि अगर आपके पास ऐसे कई प्रतिभागी हैं, जो एक-दूसरे के स्थान को अभिप्रमाणित कर सकते हैं, फिर भी इस बात की कोई गारंटी नहीं है कि भविष्य में कभी वे गलत न हों, और चूंकि आप हमेशा से केवल बहुसंख्यक सूत्रों से प्राप्त सूचनाओं पर यकीन करते आए हैं, इसलिए यह एक बहुत बड़ी*

कमजोरी है। अगर आपको कुछ विशिष्ट प्रकार के हार्डवेयर डिवाइस चाहिए, जिसमें छेड़छाड़ से बचाने वाली तकनीक का उपयोग हुआ हो, जैसे कि खोलने का एक प्रयास किए जाने पर व्यक्तिगत कुंजी को नष्ट किया जाता है या इस पर मौजूद फर्मवेयर को बदल दिया जाता है, तो संभवतः आपको बेहतर सुरक्षा मिल सकती है, लेकिन इसका मतलब यह नहीं है कि किसी GPS *सिग्नल को स्पूफ करना असंभव है। इसके सही कार्यान्वयन के लिए बहुत तैयारी और कई अग-अलग डेटा स्रोतों की आवश्यकता होती है, जिससे कि सटीकता का आश्वासन मिल सके, इसके लिए बहुत अधिक निधि की आवश्यकता होती।*" []

—मैट. डी. फेरान्टे, डेवलपर, इथीरियम फ़ाउंडेशन

2.2 स्थान संबंधी साक्ष्य: कमियाँ

संक्षेप में, स्थान संबंधी साक्ष्य को ब्लॉकचेन के कुछ शक्तिशाली गुणों का फायदा उठाना समझा जा सकता है, जैसे टाइम-स्टाम्पिंग और विकेंद्रीकरण तथा उन्हें ऑफ़-चेन, स्थान की जानकारी रखने वाले ऐसे डिवाइस से संयोजित करना, जिनके बारे में आशा की जाती है कि वे स्पूफिंग से सुरक्षित होंगे। हम क्रिप्टोग्राफ़िक स्थान के अधिकार क्षेत्र को "क्रिप्टो-लोकेशन (कूट-स्थान)" कहते हैं। इसके अतिरिक्त, जैसे सत्य के एकल स्रोत का उपयोग करने वाले ऑरेकल के इर्द-गिर्द स्मार्ट कॉन्ट्रैक्ट में कमजोरी होती है (और इसलिए विफलता का अकेला स्रोत होता है), उसी तरह से क्रिप्टो-लोकेशन सिस्टम में भी वही समस्या होती है। वर्तमान क्रिप्टो-लोकेशन प्रौद्योगिकी की कमजोरी ऐसे ऑफ़-चेन डिवाइस से संबंधित है, जो किसी वस्तु के स्थान की सूचना देते हैं। स्मार्ट कॉन्ट्रैक्ट में, ऑफ़-चेन डेटा का स्रोत ऑरेकल है। XYO नेटवर्क में, ऑफ़-चेन डेटा स्रोत वास्तविक दुनिया में एक विशिष्ट प्रकार के ऑरेकल के रूप में काम करते हैं, जिन्हें हम सेंटिनेल कहते हैं। XYO नेटवर्क सेंटर में मुख्य नवप्रवर्तन पहचानहीन, स्थान आधारित साक्ष्य से संबंधित हैं, जो गैर-भरोसा आधारित, क्रिप्टो-लोकेशन प्रोटोकॉल बनाने के लिए हमारे सिस्टम के घटकों में अंतर्निहित होते हैं।

3 XY ऑरेकल नेटवर्क

"GPS *का पूरक बनने के लिए ऐसे सिस्टम की ज़रूरत वर्षों से महसूस की जा रही है, जिसे आसानी से विघटित न किया जा सके।* GPS *अत्यधिक सटीक और विश्वसनीय है, फिर भी, जामिंग, स्पूफिंग, साइबर हमले और दूसरी तरह की बाधाओं की आवृत्ति और गंभीरता बढ़ती जा रही है। ये हमारे जीवन और आर्थिक गतिविधि पर अत्यंत घातक प्रभाव डाल सकते हैं।*" [5]

—दाना गोवार्ड, अध्यक्ष, RNT फाउंडेशन

3.1 परिचय

XYO नेटवर्क का लक्ष्य स्थान संबंधी ऑरेकल का एक गैर-भरोसा आधारित, विकेंद्रीकृत सिस्टम बनाना है, जो हमले से सुरक्षित हो और उपलब्ध डेटा की पूछताछ करने पर यथासंभव अधिकतम सटीकता दे सके। हम ऐसा आभासी प्रस्तुतिकरण के सेट के द्वारा कर पाते हैं, जिससे सिस्टम के घटकों के साथ ज़ीरो-नॉलेज (जानकारी रहित) साक्ष्यों की शृंखला के जरिए स्पूफिंग का जोखिम काफी हद तक कम हो जाता है।

3.2 नेटवर्क का अवलोकन

हमारा सिस्टम कनेक्टेड डिवाइस के प्रोटोकॉल में एक प्रवेश बिंदु प्रदान करता है, जिससे क्रिप्टोग्राफ़िक साक्ष्यों

की श्रृंखला के माध्यम से स्थान संबंधी डेटा के संबंध में उच्च स्तरीय सटीकता प्राप्त होती है। उपयोगकर्ता स्मार्ट कॉन्ट्रैक्ट सुविधा वाले किसी ब्लॉकचेन प्लेटफ़ॉर्म पर स्थान संबंधी कोई डेटा पुनर्प्राप्त करने के लिए "पूछताछ" कर सकते हैं।[4] इसके बाद XYO नेटवर्क के एकत्रणकर्ता अनुबंध के लिए जारी किए गए पूछताछ को सुनते हैं और डिवाइस के ऐसे विकेंद्रीकृत समूह से उच्चतम शुद्धता वाले उत्तर खोजते हैं, जो इन एकत्रणकर्ताओं को क्रिप्टोग्राफ़िक साक्ष्यों के बैक अप प्रदान करते हैं। इसके बाद ये एकत्रणकर्ता इन उत्तरों में से सर्वश्रेष्ठ उत्तर चुनने के बाद इनको फिर से स्मार्ट कॉन्ट्रैक्ट में फ़ीड करते हैं। घटकों के इस नेटवर्क से इस बात का सबसे प्रामाणिक, गैर-भरोसा आधारित यथासाध्य सटीकता के साथ निर्धारण करना संभव हो जाता है कि क्या कोई वस्तु दिए गए समय पर किसी विशिष्ट XY-निर्देशांक पर मौजूद है।

XYO नेटवर्क में चार प्राथमिक घटक होते हैं: **सेंटिनेल** (डेटा एकत्रक), **ब्रिज** (डेटा प्रसारक), **आर्किविस्ट** (डेटा संग्राहक), और **डिवाइनर** (उत्तर एकत्रक)। सेंटिनेल स्थान संबंधी जानकारी सेंसर, रेडियो और दूसरे माध्यमों से देते हैं। ब्रिज इस डेटा को सेंटिनेल से प्राप्त करके आर्किविस्ट को देते हैं। आर्किविस्ट इस जानकारी को डिवाइनर द्वारा विश्लेषण के लिए संग्रहित करते हैं। डिवाइनर पूछताछ में पूछे गए प्रश्नों का उत्तर तैयार करने के लिए आर्किविस्ट के अनुभव के आधार पर विश्लेषण करते हैं और उन्हें शुद्धता का स्कोर देते हैं। डिवाइनर इसके बाद इन उत्तरों को स्मार्ट कॉन्ट्रैक्ट के लिए प्रसारित करते हैं (इसलिए, डिवाइनर ऑरेकल की तरह काम करते हैं)। शुद्धता के स्कोर को **ऑरिजिन चेन स्कोर** (उत्पत्ति श्रृंखला अंक) कहा जाता है, और इसे **उत्पत्ति श्रृंखला के प्रमाण** कहलाने वाले शून्य-जानकारी वाले प्रमाणों के समूह के माध्यम से निर्धारित किया जाता है। यह श्रृंखला किसी अंतर्निहित जानकारी का खुलासा किए बिना, एक ही स्रोत से उत्पन्न दो या अधिक डेटा की गारंटी देती है। पूछताछ के पथ के साथ प्रत्येक घटक अपनी उत्पत्ति का साक्ष्य तैयार करता है, जिसे ऐसे प्रत्यक घटक से श्रृंखलाबद्ध किया जाता है, जिसके लिए यह डेटा प्रसारित करता है। उत्पत्ति का साक्ष्य एक नई संरचना है, जो वास्तविक दुनिया के डेटा को उच्च विश्वसनीयता प्रदान करने के लिए नेटवर्क में प्रसारणकर्ता के पथ के साथ क्रिप्टोग्राफ़िक गारंटी की एक श्रृंखला तैयार करता है। इस **उत्पत्ति श्रृंखला के प्रमाण** के कारण डेटा जनरेट करने वाले पहले डिवाइस से प्राप्त स्थान संबंधी डेटा पर हम विश्वास कर सकते हैं। अगले खंडों में हम विस्तार से पता लगाएँगे कि उत्पत्ति के साक्ष्य किस प्रकार काम करते हैं।

डिवाइनर के बीच विकेंद्रीकृत सहमति पद्धति स्थापित करने के लिए, XYO नेटवर्क **XYOMainChain** नाम के सार्वजनिक, अपरिवर्तनीय ब्लॉकचेन पर भरोसा करेगा, जो डिवाइनर और उनके संबद्ध उत्पत्ति स्कोर से प्राप्त डेटा के साथ ही पूछताछ ट्रांजेक्शन को संग्रहित करता है। हम पूरे सिस्टम की कार्यात्मकता पर विस्तृत चर्चा करें, इससे पहले हम अपने नेटवर्क के प्रत्येक घटक की जिम्मेदारियों को स्पष्ट रूप से परिभाषित करेंगे।

3.2.1 सेंटिनेल

सेंटिनेल स्थान संबंधी साक्ष्य होते हैं। वे अनुभव पर आधारित डेटा का अवलोकन करते हैं और अस्थायी खाता-बही बनाकर अनुभव आधारित डेटा की सुनिश्चितता और शुद्धता प्रमाणित करते हैं। सेंटिनेल का सबसे महत्वपूर्ण पक्ष ये है कि वे इस बात की खाता-बही तैयार करते हैं कि दूसरे घटक निश्चित रूप से उसी स्रोत से आए हो सकते हैं। वे इसके लिए क्रिप्टोग्राफ़िक प्रमाणों की प्रसारण श्रृंखला में उत्पत्ति का साक्ष्य जोड़ते हैं। जैसा कि बताया गया है, XYO नेटवर्क एक गैर भरोसा-आधारित सिस्टम है, इसलिए सेंटिनेल को ईमानदारी से स्थान संबंधी जानकारी देने के लिए प्रोत्साहित किया जाना चाहिए। ऐसा भुगतान घटक के साथ प्रतिष्ठा घटक का संयोजन करके किया जाता है। जब सेंटिनेल से प्राप्त जानकारी का उपयोग किसी पूछताछ का उत्तर देने में किया जाता है तो इसके पुरस्कार स्वरूप सेंटिनेल को XYO नेटवर्क टोकन (XYO) मिलते हैं। उनकी पुरस्कार प्राप्त करने की संभावना बढ़ाने के लिए, उन्हें इस बात की खाता-बही बनानी चाहिए कि वे अपने साथियों के अनुरूप चल रहे हैं और स्थान संबंधी जानकारी के स्रोत के रूप में स्वयं की पहचान के लिए उत्पत्ति का साक्ष्य प्रदान करना चाहिए।

[4] Ethereum, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counter- party, Monax and others

3.2.2 ब्रिज

ब्रिज स्थान संबंधी डेटा को प्रतिलिपित करते हैं। वे सुरक्षित रूप से स्थान संबंधी खाता बही को को सेंटिनेल से लेकर आर्किविस्ट को जारी कर सकते हैं। ब्रिज का सबसे महत्वपूर्ण पहलु ये है कि आर्किविस्ट इस बात के प्रति निश्चिंत हो सकते हैं कि ब्रिज से प्राप्त अनुभव आधारित खाता बही में किसी प्रकार की कोई छेड़छाड़ नहीं की गई है। ब्रिज का दूसरा महत्वपूर्ण पक्ष ये है कि वे उत्पत्ति का एक अतिरिक्त साक्ष्य जोड़ते हैं।बताया गया है कि XYO नेटवर्क एक गैर भरोसा-आधारित सिस्टम है, इसलिए ब्रिज को अनुभव आधारित डेटा का ईमानदारी से प्रसारण करने के लिए प्रोत्साहित किया जाना चाहिए। इसके लिए प्रतिष्ठा घटक का भुगतान घटक से संयोजन किया जाता है। जब ब्रिज से जारी की गई जानकारी का उपयोग किसी पूछताछ का उत्तर देने में किया जाता है तो इसके पुरस्कार स्वरूप ब्रिज को XYO नेटवर्क टोकन (XYO) मिलते हैं। उनकी पुरस्कार प्राप्त करने की संभावना बढ़ाने के लिए, उन्हें इस बात की खाता-बही बनानी चाहिए कि वे अपने साथियों के अनुरूप चल रहे हैं और अनुभव आधारित डेटा जारी कर्ता के रूप में स्वयं की पहचान के लिए उत्पत्ति का साक्ष्य प्रदान करना चाहिए।

3.2.3 आर्किविस्ट

आर्किविस्ट ब्रिज से प्राप्त स्थान संबंधी जानकारी को एक विकेंद्रीकृत स्वरूप में संग्रहित करते हैं, जिसका लक्ष्य सभी पुरानी खाता-बहियों को संग्रहित करना होता है। यहाँ तक कि अगर कुछ डेटा की क्षति भी हो जाती है या यह अस्थायी रूप से अनुपलब्ध भी हो जाती है, तो सिस्टम काम करता रहता है, बस थोड़ी कम सटीक जानकारी देती है। आर्किविस्ट खाता-बही की भी सूची बनाते हैं, ताकि जरूरत पड़ने पर वह खाता बही का डेटा आसानी से उपलब्ध करा सकें। आर्किविस्ट केवल अपरिष्कृत डेटा एकत्र करते हैं और डेटा की पुनर्प्राप्ति तथा इसके अनुवर्ती उपयोग के लिए मात्र इन्हें ही XYO नेटवर्क टोकन का भुगतान किया जाता है। संग्रहण हमेशा निःशुल्क होता है।

आर्किविस्ट का अपना नेटवर्क होता है, तो एक आर्किविस्ट को पूछने पर उस आर्किविस्ट के पास जो डेटा नहीं होता, वह उसे दूसरे आर्किविस्ट को मांगेगा। कोई आर्किविस्ट वैकल्पिक रूप से किसी भी ऐसी खाता बही सूचना को संग्रहित कर सकता है, जो इसे दी गई हो। इसके परिणामस्वरूप दो प्रकार के आर्किविस्ट की संभावना अधिक होती है: एक वह, जो “क्लाउड” के डेटा के जनक होते हैं और दूसरे, जो “क्लाउड” के डेट का उपयोग करते हैं। बीच के आर्किविस्ट हाइब्रिड (संकर या मिश्रित किस्म) होंगे। डेटा संग्रहित करने के विकल्प पर बल नहीं दिया जाता, लेकिन IPFS या अन्य किसी विकेंद्रीकृत संग्रहण समाधान के जरिए ऐसा आसानी से किया जा सकता है। हर बार डेटा एक आर्किविस्ट द्वारा दूसरे को सौंपा जाता है, तो भुगतान का पता लगाने के लिए उत्पत्ति के अतिरिक्त प्रमाण लगाने पड़ते हैं, क्योंकि सभी आर्किविस्ट को भुगतान करना होता है। पुनर्प्राप्ति के लिए, वैधता बढ़ाने हेतु उत्पत्ति के साक्ष्य का न्यूनतम स्तर सेट किया जा सकता है। डेटा अवरोध से बचने के लिए सेंटिनेल, ब्रिज और आर्किविस्ट को हितों को संरेखित होना चाहिए।

3.2.4 डिवाइनर

डिवाइनर XYO नेटवर्क का सबसे जटिल हिस्सा हैं। डिवाइनर का समग्र लक्ष्य XYO नेटवर्क के पूछताछ के लिए सबसे सटीक डेटा खोजना और उस डेटा को पूछताछ करने वाले को प्रत्युत्तर के रूप में देना है। डिवाइनर, XYO स्मार्ट कॉन्ट्रैक्ट को जारी पूछताछ के लिए उपयुक्त ब्लॉकचेन प्लेटफॉर्म (अर्थात इथीरियम, स्टेलर, कारडैनो, IOTA, आदि) का चुनाव करते हैं। इसके बाद, आर्किविस्ट नेटवर्क से सीधा संवाद करके वे पूछताछ का सबसे सटीक/विश्वसनीय उत्तर प्राप्त करते हैं। वे उत्पत्ति के साक्ष्य की सबसे अच्छी श्रृंखला वाले प्रमाण पर निर्णय लेकर ऐसा करते हैं। सबसे कम समय में सबसे सटीक उत्तर खोजने वाले डिवाइनर कार्य के साक्ष्य के द्वारा मुख्य XYO ब्लॉकचेन (XYOMainChain) में एक ब्लॉक बना सकेंगे। पूछताछ को मिलने वाले पुरस्कार के परिमाण और जटिलता के अनुसार प्राथमिकता दी जाती है, इसलिए किसी उत्तर के लिए अधिक XYO प्रस्तावित होने पर पूछताछ को अधिक प्राथमिकता दी जाएगी।

दूसरे डिवाइनर किसी ब्लॉक की वैधता के आधार पर सहमति पर पहुँचते हैं और ब्लॉक पर डिजिटल हस्ताक्षर करते हैं। उस ब्लॉक पर कॉइनबेस पता वाला डिवाइनर स्मार्ट कॉन्ट्रैक्ट को उत्तर और उसकी सटीकता के स्कोर वाला ट्रांजेक्शन भेजेगा। यह दूसरे डिवाइनर के हस्ताक्षर की सूची भी भेजता है, जिससे हमला करने वाले को डिवाइनर होने का बहाना करके ब्लॉकचेन में गलत जानकारी जारी करने से रोका जा सके।

इसके बाद स्मार्ट कॉन्ट्रैक्ट पेलोड के हस्ताक्षर की सूची को जाँचकर इस सूचना की सत्यता को सत्यापित कर सकता है।

3.3 एक छोर से दूसरे छोर तक की कार्यात्मकता

अब, प्रत्येक घटक की जिम्मेदारियों को विस्तार से बताया जा रहा है, यहाँ सिस्टम के प्रत्येक घटक के काम का एक उदाहरण दिया गया है।

1. **सेंटिनेल डेटा एकत्र करते हैं**

• सेंटिनेल वास्तविक दुनिया के स्थान संबंधी अनुभव आधारित डेटा एकत्र करते हैं और अपने ऊपर के नोड से श्रृंखलाबद्ध करने के लिए अपनी उत्पत्ति का साक्ष्य तैयार करते हैं

2. **ब्रिज सेंटिनेल से डेटा एकत्र करते हैं**

• ब्रिज ऑनलाइन सेंटिनेल से जरूरी डेटा एकत्र करते हैं और उनकी श्रृंखला में उत्पत्ति का साक्ष्य जोड़ते हैं। इसके बाद ब्रिज स्वयं को नेटवर्क के आर्किविस्ट के लिए उपलब्ध कराते हैं।

3. **आर्किविस्ट ब्रिज से प्राप्त डेटा को सूचीबद्ध/असेम्बल करते हैं**

• ब्रिज लगातार आर्किविस्ट को सूचनाएँ भेजते रहते हैं, जिन्हें स्थान संबंधी अनुभव आधारित डेटा की सूची के साथ विकेंद्रीकृत स्टोर में रखा जाता है।

4. **डिवाइनर उपयोगकर्ता की पूछताछ के उत्तर खोजते हैं**

• डिवाइनर इथीरियम स्मार्ट कॉन्ट्रैक्ट को भेजे गए प्रश्न का उत्तर चुनते हैं और उत्तर तैयार करने की प्रक्रिया शुरू करने का निर्णय लेते हैं।

5. **डिवाइनर आर्किविस्ट से डेटा एकत्र करते हैं**

• इसके बाद डिवाइनर आर्किविस्ट के नेटवर्क से आवश्यक उपयुक्त जानकारी लेकर पूछताछ का उत्तर देने का निर्णय लेते हैं।

6. **डिवाइनर उत्तर तैयार करते हैं**

• डिवाइनर आर्किविस्ट के नेटवर्क से पूछताछ का सर्वश्रेष्ठ उत्तर चुनते हैं, जिसकी उत्पत्ति श्रृंखला का स्कोर सबसे अधिक होता है।

7. **डिवाइनर ब्लॉक प्रस्तावित करता है**

• इसके बाद डिवाइनर XYOMainChain पर ब्लॉक प्रस्तावित करते हैं, जिसमें उत्तर सामग्रियाँ, पूछताछ के प्रश्न और कार्य के साक्ष्य के जरिए भुगतान किए गए XYO टोकन (XYO) होते हैं। नेटवर्क के दूसरे डिवाइनर ब्लॉक की सामग्री पर डिजिटल हस्ताक्षर करते हैं, इसके बाद कॉइनबेस Di- viner के खाते की जानकारी अद्यतित हो जाती है, जिससे किसी वैध ब्लॉक पर सहमति होने पर सिस्टम में इसके कार्य का साक्ष्य दिखाई दे सके।

8. **डिवाइनर पूछताछ करने वाले को परिणाम प्रदान करते हैं**

• डिवाइनर उत्तर, उसकी उत्पत्ति श्रृंखला के स्कोर और इसके डिजिटल हस्ताक्षर के सेट को पैकेज करते हैं और इन्हें XYO स्मार्ट कॉन्ट्रैक्ट से सुरक्षित रूप से कनेक्ट करने वाले अडैप्टर घटक को भेजते हैं। अडैप्टर की जिम्मेदारी यह सुनिश्चित करना होता है कि डिवाइनर से कोई समझौता नहीं किया गया है और यह स्मार्ट कॉन्ट्रैक्ट को डिजिटल रूप से हस्ताक्षरित उत्तरों का सेट भेजता है।
ऐसा ब्लॉक बनाने की प्रक्रिया के तुरंत बाद होता है। इसके बाद कॉइनबेस डिवाइनर को इसमें योगदान के लिए भुगतान किया जाता है।

9. **XYO नेटवर्क के घटकों को अपने काम के लिए पुरस्कार मिलते हैं**

• उत्पत्ति श्रृंखला का साक्ष्य के साथ घटकों को पूछताछ के प्रश्न का उत्तर खोजने में उनके योगदान के

लिए भुगतान किया जाता है। सेंटिनेल, ब्रिज, आर्किविस्ट और डिवाइनर, सभी को उनके काम के लिए पुरस्कृत किया जाता है।

ऐसे मामले में, जहाँ एक ही प्रश्न कई बार किया जाता है, एक से अधिक उत्तर आ सकते हैं, क्योंकि उत्तर उस समय सिस्टम द्वारा प्रदान किए जा रहे उपलब्ध अनुभव आधारित डेटा पर आधारित होते हैं। ब्लॉकचेन को उत्तर सबमिट करने के दो चरण होते हैं। पहला, पूछताछ के सर्वश्रेष्ठ उत्तर के निर्धारण के लिए विश्लेषण किया जाना चाहिए। अगर सिस्टम द्वारा एक से अधिक उत्तर तैयार किए जाते हैं तो नोड उत्तरों की तुलना करेगा और हमेशा बेहतर उत्तर को चुनेगा। किसी सामान्य पूछताछ का एक उदाहरण इस प्रकार है: "भूतकाल में किसी खास समय पर नेटवर्क पर नोड कहाँ था "

3.4 सत्यता के एकल स्रोत के रूप में ब्लॉकचेन

मुख्यतः, डिवाइनर सापेक्ष डेटा को निरपेक्ष डेटा में बदलते हैं। वे XYO नेटवर्क के पूछताछ के लिए एक निरपेक्ष उत्तर को वास्तविक रूप देने के लिए पूरे आर्किविस्ट नेटवर्क का पता लगा सकते हैं। डिवाइनर भी ऐसे नोड हैं, जो XYOMainChain के लिए ब्लॉक प्रस्तावित करते और जोड़ते हैं और अपने कार्य के साक्ष्य के लिए पुरस्कार पाते हैं। चूंकि आर्किविस्ट नेटवर्क संसाधित न किए गए डेटा का स्टोर है और ब्लॉकचेन निरपेक्ष, संसाधित डेटा का स्टोर है, इसलिए नेटवर्क भविष्य के पूछताछ का उत्तर देने के लिए XYOMainChain पर आर्कविस्ट नेटवर्क के जरिए मंहगे परिकलन पर विश्वास करने के बजाय आकस्मिक रूप से नवीनतम जानकारी का उपयोग कर सकता है।

चूंकि XYOMainChain पर ब्लॉक उत्पत्ति श्रृंखला का साक्ष्य और घटकों के ग्राफ़ संग्रहित करता है, जिनका उपयोग पूछताछ का उत्तर देने के लिए किया जाता था, भविष्य के डिवाइनर कम बैंडविड्थ के उपयोग से सटीक परिणाम प्राप्त करने के लिए इस निरपेक्ष डेटा का उपयोग कर सकते हैं। जैसे कि, XYOMainChain धीरे-धीरे सिस्टम की सत्यता का सबसे महत्वपूर्ण स्रोत बन जाएगा। फिर भी, सेंटिनेल द्वारा प्राप्त स्थान संबंधी अनुभव आधारित डेटा के बारे में नवीनतम जानकारी बनाए रखने के लिए आर्किविस्ट नेटवर्क अभी भी आवश्यक होगा।

3.5 सर्वश्रेष्ठ उत्तर की उम्मीदवारी के चयन के लिए XYO नेटवर्क का फ्रेमवर्क

हम उत्तरों की एक सूची में से सर्वश्रेष्ठ उत्तर को एकल उत्तर के रूप में परिभाषित करते हैं, जिसका वैधता स्कोर सबसे अधिक होता है और सटीकता का परिमाण न्यूनतम आवश्यक सटीकता से अधिक होता है। वैधता स्कोर उत्पत्ति श्रृंखला के स्कोर पर आधारित होता है। सिस्टम जानता है कि उच्चतम रिकॉर्ड उत्पत्ति स्कोर क्या है, यह 100 प्रतिशत रहेगा या इससे अधिक स्कोर प्राप्त होने पर उसे नया 100 प्रतिशत माना जाएगा। XYO नेटवर्क सर्वश्रेष्ठ उत्तर का निर्धारण करने के लिए सर्वश्रेष्ठ उत्तर अल्गोरिद्म के चयन की अनुमति देता है। इससे वैकल्पिक अल्गोरिद्म में भविष्य के शोध के लिए विस्तार किया जाता है।

जब डेटा को खराब या गलत माना जाने के कारण उत्तर से हटाया जाता है तो इसे आर्किविस्ट को भेजा जाएगा, ताकि वे इस डेटा को अपने विकेंद्रीकृत स्टोर से निकाल सकें।

3.6 पब्लिक ब्लॉकचेन से आरंभिक एकीकरण

XYO नेटवर्क को ऐसे आभासी प्रस्तुतिकरण के लिए तैयार किया गया है, जो किसी भी स्मार्ट कॉन्ट्रैक्ट सक्षम, पब्लिक ब्लॉकचेन, जैसे इथीरियम, बिटकॉइन + RSK, EOS, NEO, स्टेलर, कार्डैनो और अन्य से इंटरैक्ट कर सकता है। उदाहरण के लिए, इथीरियम के उपयोगकर्ता XYO नेटवर्क से इंटरैक्ट करने के लिए, हमारे XYO स्मार्ट कॉन्ट्रैक्ट पर अपनी पूछताछ कर सकते हैं और XYO टोकन (ERC20) से भुगतान कर सकते हैं। हमारे XYO ब्लॉकचेन में डिवाइनर कहे जाने वाले नोड इन पूछताछ के लिए हमेशा इथीरियम को चुनेंगे और हमारे XYO ब्लॉकचेन की अपनी मुद्रा (XYO टोकन) से पुरस्कृत किए जाएँगे। भविष्य में, हम अपने ERC20 टोकन धारकों से अपने ब्लॉकचेन की मुद्रा में सीधा रुपांतरण करेंगे, जिससे कि हम लेनदेन का शुल्क लेकर अपना प्लेटफॉर्म प्रदान कर सकें, जिससे बड़े पैमाने पर IoT उपयोग के मामले में जरूरी सूक्ष्म भुगतान आवश्यकताओं की पूर्ति हो सके। इन मामलों मं, हम उपयोगकर्ताओं को पब्लिक स्मार्ट कॉन्ट्रैक्ट के जरिए संवाद करने की जगह

सीधे अपने ब्लॉकचेन में पूछताछ की अनुमति देंगे।

4 उत्पत्ति के साक्ष्य

भरोसारहित नोड से बने भौतिक नेटवर्क में ऐसे डेटा की सुनिश्चितता निर्धारित करना संभव है, शून्य-जानकारी वाले साक्ष्य पर आधारित एज नोड द्वारा प्रदान किया गया हो, कि एक ही स्रोत से दो या अधिक डेटा तैयार किए गए हैं। इन डेटा सेट के साथ विभिन्न समान डेटा सेट के संयोजन और कम से कम एक नोड के निरपेक्ष स्थान, की जानकारी का उपयोग करके दूसरे नोड के निरपेक्ष स्थान का पता लगाया जा सकता है।

4.1 उत्पत्ति के साक्ष्य का परिचय

पारंपरिक गैर भरोसा आधारित सिस्टम किसी सिस्टम में लेनदेन या अनुबंधों पर हस्ताक्षर के ए निजी कुंजी पर भरोसा करते हैं। यह इस धारणा पर अच्छी तरह काम करता है कि किसी नेटवर्क का वह नोड, जो संदिग्ध प्रश्न पर हस्ताक्षर करता है, भौतिक औऱ आभासी रूप से सुरक्षित होता है। फिर भी, अगर निजी कुंजी से छेड़छाड़ की गई है तो उत्पत्ति का प्रमाणित करने की क्षमता में कमी आ सकती है।

चीजों के अंतर्जाल के लिए गैर भरोसा आधारित अवधारणाएँ लागू करने पर, यह माना जाना चाहिए कि नेटवर्क पर मौजूद एज नोड भौतिक या आभासी रूप से सुरक्षित नहीं हैं। इससे अद्वितीय ID के उपयोग के बिना और नेटवर्क से बाहर की कोई जानकारी के बिना, एज नोड के ईमानदार और वैध होने के चलते इनके द्वारा तैयार डेटा पर निर्णय देने की जगह एज नोड के पहचान की आवश्यकता सामने आती है।

4.2 उत्पत्ति के साक्ष्य का मुख्य भाग: बाध्य साक्षी

उत्पत्ति का साक्ष्य बाध्य साक्षी की अवधारणा पर भरोसा करता है। बताया गया है कि डिजिटल अनुबंध (ऑरेकल) के समाधान के लिए गैर-भरोसेमंद स्रोत उपयोगी नहीं है, तो हम स्थान के द्विआयामी साक्ष्य की मौजूदगी के द्वारा डेटा की सुनिश्चितता में उल्लेखनीय बढ़ोतरी कर सकते हैं। प्राथमिक द्विआयामी स्थान संबंधी अनुभव आधारित डेटा है निकटता, क्योंकि दोनों पक्ष इंटरैक्शन को सह-हस्ताक्षरित करके विभिन्न प्रकार के इंटरैक्शन होने का सत्यापन कर सकते हैं। इससे इस शून्य-जानकारी साक्ष्य को अनुमति मिलती है कि दोनों नोड एक-दूसरे के निकट थे।

इसके बाद हमें यह सुनिश्चित करना होता है कि एक गैर भरोसा-आधारित सिस्टम में ऑरेकल साक्षी नोड ने डेटा एकत्र किया है कि इसे साझा किया जा रहा है। किसी गैर भरोसा आधारित सिस्टम में, साक्षी नोड या तो त्रुटि या दूषण के कारण गलत डेटा तैयार कर सकते हैं। अगर उस अनुभव आधारित डेटा के लिए अनुमत सीमा से बाहर का कोई डेटा मिलता है तो इसकी अमान्य डेटा के रूप में पहचान करके, इसे निकाला जा सकता है। वैध, लेकिन गलत डेटा को पहचानना कहीं अधिक कठिन है।

4.3 एकल आयामी बनाम द्विआयामी स्थान संबंधी अनुभव आधारित डेटा

भौतिक दुनिया से संबंधित अधिकांश डेटा (अनुभव आधारित डेटा) एकल आयामी होते हैं। इसका अर्थ है कि मापा जाने वाला पदार्थ दोबारा माप नहीं करता, एकल आयामी अनुभव आधारित डेटा का सत्यापन बहुत कठिन होता है।

द्विआयामी अनुभव आधारित डेटा ऐसा डेटा है, जहाँ मापा गया पदार्थ अपनी माप की सूचना दूसरे पक्ष को देता है, जिसके चलते सत्यापन संभव है। स्थान एक ऐसा दुर्लभ अनुभव आधारित डेटा है, जिसके अंतर्गत यह द्विआयामी हो सकता है, जिसमें दो एज नोड एक-दूसरे को सूचना देते **हैं। वास्तविक दुनिया में इसका उदाहरण वैसे दो आदमी होंगे, जो एक दूसरे के पास होकर सेल्फी लेते हैं, प्रत्येक पार्टी की एक प्रति मुद्रित करते हैं और इसके बाद दोनों, सेल्फ़ी पर हस्ताक्षर करते हैं। यह प्रक्रिया दोनों पक्षों को निकटता का साक्ष्य प्रदान करेगी। इन दो लोगों के लिए इस "डेटा" को पाने का केवल एक तरीका होगा कि वे दोनों एक ही जगह पर एक साथ बने रहें।**

आगे, चलिए हम नेटवर्क क प्रभावों पर चर्चा करते हैं: मान लें कि एक ऐसा सिस्टम है, जिसमें प्रत्येक एज नोड से ये "सेल्फी" लगातार तैयार करने की अपेक्षा की जाती है, क्योंकि वे साथ-साथ यात्रा कर रहे हैं और उन्हें बाइंडर में रखते जा रहे हैं। उनसे यह अपेक्षा भी की जाती है कि वे बाइंडर को समयानुसार रखेंगे और उन्हें किसी को हटाने की कभी अनुमति नहीं। यह प्रत्येक एज नोड के लिए निकटता रिकॉर्डर स्थापित करता है, जिसका दूसरे एज नोड के रिकॉर्डर से क्रॉस संदर्भ दिया जा सकता है।

4.4 नॉन-एज नोड

सभी नोड को साक्षी माना जाता है, जिसमें ब्रिज, रिले (प्रसारण), संग्रहण और विश्लेषण नोड होते हैं। इसकी मदद से एक नोड से दूसरे बाउंड होने वाले नोड के लिए डेटा प्रसारित किया जा सकता है। यह **बाउंड विटनेस** (बाध्य साक्षी) की अवधारणा है।

4.5 क्रॉस संदर्भ

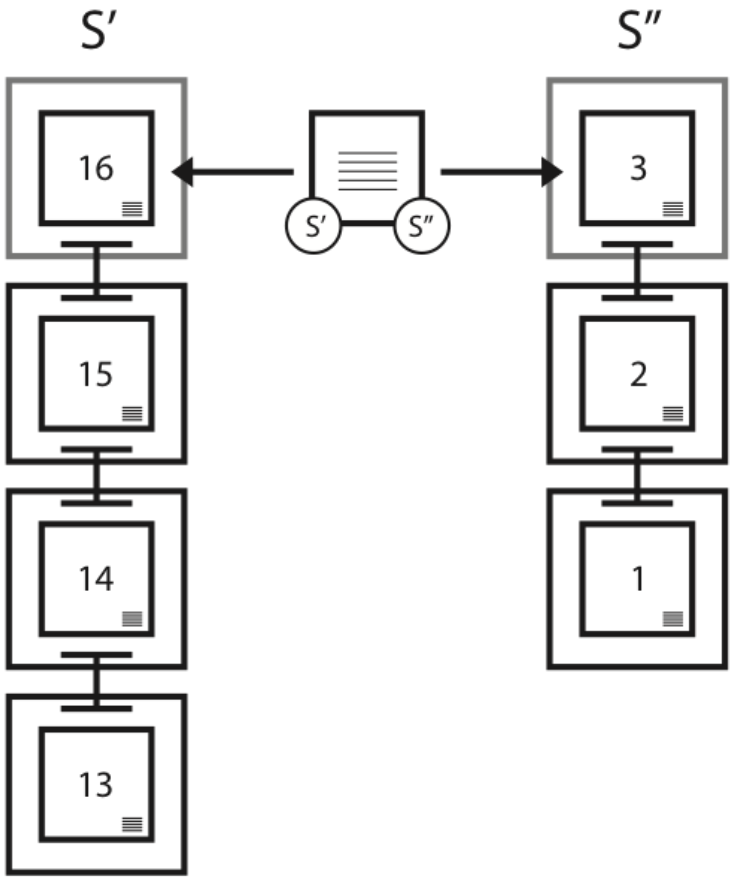
प्रत्येक एज नोड द्वारा तैयार और एक साथ श्रृंखलाबद्ध सेल्फी के प्रत्येक सेट का विश्लेषण करने से सिस्टम नेटवर्क में मौजूद सभी नोड की सापेक्ष निकटता से सबसे अच्छा उत्तर तैयार कर लेता है। अगर प्रत्येक नोड ईमानदारी से और सटीक सूचना देता है तो एज नोड की सभी सापेक्ष स्थितियों के मापन से अधिकतम संभव सुनिश्चितता और शुद्धता हासिल होगी: 100 प्रतिशत। इसके विपरीत, अगर प्रत्येक नोड बेईमान या दोषपूर्ण है तो सुनिश्चितता और सटीकता, दोनों 0 पर पहुँच सकती है।

बताया गया है कि रिपोर्ट किए गए डेटा और किसी एज नोट की सापेक्ष स्थिति के लिए पूछताछ, स्थिति के लगभग निर्धारण को सुनिश्चितता और सटीकता के गुणांक के साथ तैयार किया जा सकता है।

दिए हुए डेटा के इसी सेट और इसी विश्लेषण अल्गोरिद्म के लिए, प्रत्येक परिकलन से एक ही स्थिति का निर्धारण और सुनिश्चितता व सटीकता के लिए एक ही गुणांक होना चाहिए।

4.6 आरेख

S' और *S"* (चित्र 1.) में से प्रत्येक, एक सेंटिनेल (एज नोड) हैं, जो अनुभव आधारित डेटा एकत्र करते हैं। जब एक-दूसरे के संपर्क में होते हैं तो वे अनुभव आधारित डेटा और सार्वजनिक कुंजियों का आदान-प्रदान करते हैं। दोनों इंटरैक्शन का पूरा रिकॉर्ड तैयार करते हैं और परिणामी इंटरैक्शन पर हस्ताक्षर करते हैं। रिकॉर्ड पर हस्ताक्षर करने के बाद उनकी दोनों स्थानीय खाता बही (S' के लिए 16 और S" के लिए 3) में अगली प्रविष्टि की जाती है। इस कार्रवाई से ये दो साक्षी एक-दूसरे के संपर्क में ला दिए जाते हैं।



चित्र 1. दो सेंटिनेल के बीच साक्ष्य की बाइंडिंग का उदाहरण

4.7 उत्पत्ति श्रृंखलाएँ

प्रत्येक उत्पत्ति की अपनी खाता-बही होती है और यह उत्पत्ति श्रृंखला का साक्ष्य बनाने के लिए इस पर हस्ताक्षर करता है। जब उत्पत्ति के साक्ष्य की श्रृंखला संबंधी जानकारी साझा की जाती है तो यह हमेशा प्रभावी रहती है। क्योंकि साझा करने के बाद के विभाजन से श्रृंखला खत्म हो जाती है और भविष्य का सभी डेटा साक्ष्य से बनता है, जिसे इस तरह लिया जाता है, मानो यह कोई नया साक्ष्य हो। किसी उत्पत्ति के साक्ष्य की श्रृंखला में कोई लिंक तैयार करने के लिए, उत्पत्ति कोई सार्वजनिक/निजी कुंजी युग्म तैयार करती है। इसके बाद, दोनों ब्लॉक में सार्वजनिक कुंजी शामिल करने के बाद, इसी युग्म के पिछले और अगले, दोनों ब्लॉक पर हस्ताक्षर करता है। हस्ताक्षर करने के तुरंत बाद, सार्वजनिक कुंजी हटा दी जाती है। सार्वजनिक कुंजी के तुरंत हटाते ही, कुंजी चोरी हो जाने या दोबारा उपयोग में आने का जोखिम काफी घट जाता है।

उत्पत्ति श्रृंखलाओं के साक्ष्य इस बात के सत्यापन की कुंजी हैं कि XYO नेटवर्क के प्रवाह की खाता-बहियाँ मान्य हैं। डेटा के स्रोत के लिए एक अद्वितीय ID का होना व्यावहारिक नहीं है, क्योंकि इसके साथ जालसाजी की जा सकती है। निजी कुंजी हस्ताक्षर व्यावहारिक नहीं है, क्योंकि XYO नेटवर्क के अधिकतर हिस्से को भौतिक रूप से सुरक्षित करना कठिन या असंभव है, इसलिए किसी दुर्भावनापूर्ण व्यक्ति द्वारा निजी कुंजी को चुरा लेना भी संभव है। इसके समाधान के लिए, XYO नेटवर्क अस्थायी कुंजी श्रृंखलाओं का उपयोग करता है।

उनके उपयोग से लाभ यह है कि श्रृंखला टूटने पर, यह हमेशा के लिए टूट जाता है और इसे आगे उपयोग में नहीं लाया जा सकता।

जब भी XYO नेटवर्क में अनुभव आधारित खाता बही सौंपी जाती है, हर बार प्राप्तकर्ता उसमें अपनी उत्पत्ति के साक्ष्य भी जोड़ता है, जिससे उत्पत्ति के साक्ष्य की श्रृंखला लंबी होती चली जाती है और उत्पत्ति के साक्ष्य का विभाजन होता है। उत्पत्ति के साक्ष्य की श्रृंखलाएँ और उत्पत्ति के साक्ष्य के विभाजन डिवाइनर द्वारा खाता-बही की वैधता के सत्यापन हेतु प्राथमिक संकेतक हैं। खाता-बही की प्रतिष्ठा का समीकरण बताता है कि XYO नेटवर्क का कितना प्रतिशत इससे संबंधित उत्पत्ति के साक्ष्य का बॉल बनाने में शामिल था। सैद्धांतिक रूप से, अगर XYO नेटवर्क के रिकॉर्ड का100 प्रतिशत हिस्सा उत्पत्ति के साक्ष्य से जुड़ा है और उसका पूरा विश्लेषण किया गया है तो इसके वैध होने की संभावना भी 100 प्रतिशत है। अगर XYO नेटवर्क के रिकॉर्ड का 0 प्रतिशत विश्लेषण के लिए उपलब्ध है, तो वैधता घटकर 0 प्रतिशत पर आ जाती है।

संवर्धित सुरक्षा के लिए, किसी श्रृंखला लिंक के लिए सार्वजनिक कुंजी तब तक प्रदान नहीं की जाती, जब तक इसके लिए दूसरी प्रविष्टि उपलब्ध नहीं हो जाती। यह प्रविष्टियों के बीच समय अंतराल या पिछले अथवा अगले लिंक में दूसरे डेटा के संग्रहण की भी अनुमति देता है।

4.8 उत्पत्ति श्रृंखला स्कोर

उत्पत्ति श्रृंखला स्कोर का निम्नलिखित तरीके से परिकलन किया जाता है (डिफ़ॉल्ट अल्गोरिद्म):

- *PcL* = उत्पत्ति के साक्ष्य की श्रृंखला की लंबाई
- *PcD* = उत्पत्ति के साक्ष्य की श्रृंखला की जटिलता
- *Pc' Pc" O* = *Pc'* और *Pc"* के लिए उत्पत्ति के साक्ष्य की श्रृंखलाएँ ओवरलैप करती हैं

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

4.9 उत्पत्ति वृक्ष

उत्पत्ति वृक्ष (ऑरिजिन ट्री) का उपयोग किसी उत्तर की वैधता के करीब करीब परिकलन के लिए किया जाता है। इसमें आदर्श वृक्ष बनाने के लिए एकत्रित डेटा का उपयोग किया जाता है, जो कि कथित उत्तर के लिए सबसे उपयुक्त वृक्ष होता है। नोड *N* अगर X,Y,Z,T स्थान पर है, तो सेट में सभी डेटा के बीच त्रुटि का कोई नियत मान होना चाहिए। इस त्रुटि का परिकलन करने के लिए, हम न्यूनतम, अधिकतम, माध्य, औसत और माध्य से औसत दूरी का परिकलन करेंगे।

S का एक सेट दिया गया है, जिसमें s के सभी स्कोर, उत्पत्ति के साक्ष्य की श्रृंखला की जटिलता PcD और त्रुटि का कोई कारक या त्रुटि है तो सर्वश्रेष्ठ उत्तर का निर्धारण निम्नलिखित तरीके से किया जाता है:

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

दूसरे शब्दों में, कथित उत्तर, जिसे सर्वाधिक स्कोर मिला है, सर्वश्रेष्ठ उत्तर है। उत्पत्ति के साक्ष्य वृक्ष का उपयोग करके, हम असंभव शाखाओं (बाहरी) की पहचान कर और उसे हटा सकते हैं।

4.10 अस्थायी कुंजी श्रृंखला

दो अनुवर्ती पैकेट पर हस्ताक्षर करने के लिए अस्थायी निजी कुंजियों का उपयोग करके डेटा पैकेट की श्रृंखलाओं को आपस में जोड़ा जा सकता है। जब डेटा पैकेट में सार्वजनिक कुंजी का निजी कुंजी के साथ युग्मन किया जाता

है तो प्राप्तकर्ता सत्यापित कर सकता है कि दोनों पैकेट पर एक ही निजी कुंजी का हस्ताक्षर किया गया था या नहीं। हस्ताक्षर को विघटित किए बिना पैकेट का डेटा बदला नहीं जा सकता, जिससे इस बात का आश्वासन मिलता है कि हस्ताक्षरित पैकेट को किसी तृतीय पक्ष, जैसे ब्रिज या संग्रहण नोड के द्वारा नहीं बदला गया था।

4.11 लिंक की व्यापकता

कम से कम, नोड उत्पत्ति के साक्ष्य की श्रृंखला में प्रत्येक लिंक के लिए एक नई सार्वजनिक/निजी कुंजी युग्म तैयार करता है, जिसके लिंक की व्यापकता 1 है। हो सकता है कि किसी दिए गए खाता बही प्रविष्टि के लिए लिंक तालिका में N प्रविष्टियाँ हो, जिसमें से प्रत्येक प्रविष्टि लिंक का भाग दो जोड़े जाने पर भविष्य की दूरी निर्दिष्ट करती हो। किसी दो लिंक के परिमाण बेस 2 के पैमाने पर एक ही क्रम में नहीं हो सकते। उदाहरण के लिए, प्रविष्टि [1,3,7,12,39] की अनुमति होगी, लेकिन [1,3,7,12,15] की नहीं होगी।

व्यापकता 1 वाला लिंक बनाया, उपयोग किया और पिछले ब्लॉक के प्रकाशित होने पर उसे हटाया जाता है। फिर भी, 1 से अधिक व्यापकता वाले लिंक का युग्म तैयार किया जाता है, क्योंकि पिछला ब्लॉक हस्ताक्षरित किया जा रहा है और दूसरा हस्ताक्षर तब तक नहीं होता, जब तक कि N ब्लॉक न आ जाए, जिसके बाद निजी कुंजी हटा दी जाती है। इस कारण से, 1 से अधिक की व्यापकता वाले लिंक को हमेशा 1 की व्यापकता वाले लिंक से कम सुरक्षित माना जाता है, लेकिन सुरक्षा से समझौता करके कार्यप्रदर्शन में सुधार लाने और डेटा क्षति में कमी लाने के लिए उनका उपयोग किया जा सकता है।

4.12 नियत क्रम

खाता-बही के क्रम निर्धारण के लिए मुख्य घटक वह क्रम है, जिसमें उनकी रिपोर्ट की गई थी। बताया गया है कि किसी डिवाइस के लिए उत्पत्ति के साक्ष्य द्वारा हस्ताक्षरित खाता-बही का क्रम बदलना संभव नहीं है, सभी खाता-बही को सामूहिक रूप से देखने पर एक निरपेक्ष क्रम स्थापित किया जा सकता है।

4.13 अंतिम से पहले का प्रकाशन

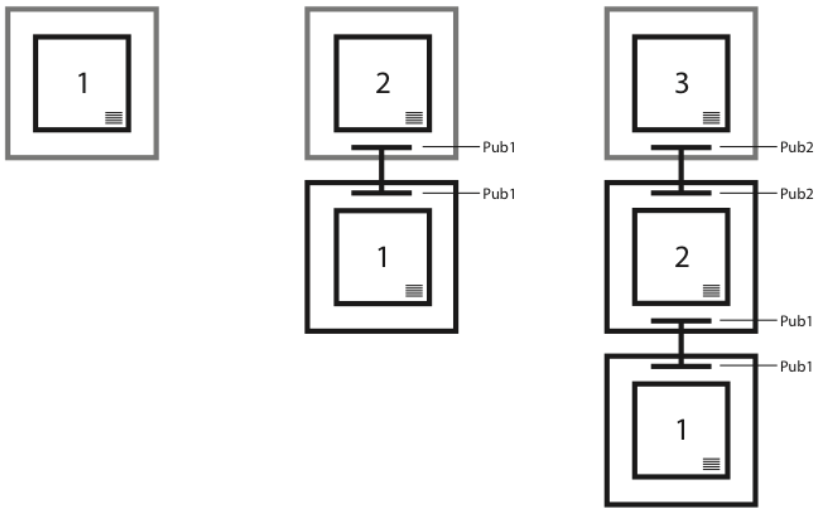
उत्पत्ति का साक्ष्य तैयार करने की प्राथमिक पद्धति इस तथ्य पर आधारित है कि सेंटिनेल अंतिम ब्लॉक की रिपोर्ट न करके, हमेशा इसके अंतिम से पहले वाले ब्लॉक की रिपोर्ट करता है। इसके कारण अंतिम ब्लॉक इससे पहले वाले के लिए लिंक के साक्ष्य के रूप में लिंक हस्ताक्षरित कर सकता है।

4.14 खाली लिंक

उत्पत्ति के साक्ष्य की श्रृंखला को और अधिक सुरक्षित बनाने के लिए, जरूरी है कि श्रृंखला को प्रत्येक दस सेकंड में एक बार से अधिक और साठ मिनट में एक बार से कम अद्यतित न किया गया हो। जिस मामले में कोई नया डेटा उपलब्ध नहीं है, उसमें श्रृंखला में एक खाली ब्लॉक जोड़ा जाएगा।

4.15 आरेख

जैसे ही घड़ी की सूइयाँ बाएँ से दाएँ जाती हैं (चित्र 2.), उत्पत्ति के साक्ष्य की श्रृंखला लंबी होती जाती है। किसी समय श्रृंखला के निर्माता, इसे उपलब्ध कराने से पहले दूसरे हस्ताक्षर की प्रतीक्षा करते हुए कॉलर को केवल गहरे रंग के बॉर्डर वाली प्रविष्टियाँ ही प्रदान करेंगे। उदाहरण के लिए, तीसरे कॉलम में केवल प्रविष्टि 2 और 1 को श्रृंखला के भाग के रूप में वापस किया जाएगा।



चित्र 2. उत्पत्ति के साक्ष्य की श्रृंखला में लिंक शामिल करने का उदाहरण

4.16 सारांश

डेटा पैकेट की श्रृंखला, जिन्हें अस्थायी निजी कुंजियों के साथ क्रमिक युग्म में हस्ताक्षरित किया गया है और युग्मित सार्वजनिक कुंजियों को शामिल करते हैं, निरपेक्ष सुनिश्चितता के साथ माने जा सकते हैं कि पैकेट एक ही स्रोत से आए हैं।

5 सुरक्षा को ध्यान में रखना

5.1 नकली डिवाइनर का हमला

डिजिटल हस्ताक्षरों के सेट को XYO स्मार्ट कॉन्ट्रैक्ट को भेजा जाता है, क्योंकि कॉन्ट्रैक्ट को उत्तर भेजने वाले डिवाइनर की सत्यता का सत्यापन करना होता है। इसके बाद कॉन्ट्रैक्ट उच्च विश्वसनीयता अंतराल में इस सूची पर हस्ताक्षर करने वाले दूसरे डिवाइनर को सत्यापित कर सकता है। इसके बिना, प्रसारणकर्ता ऑरेकल विफलता का अकेला स्रोत होंगे और सिस्टम में जोखिम होगा।

5.2 सेंटिनेल DDoS के हमले

जिस हमले पर विचार करना है, उसमें से दूसरा है किसी खास क्षेत्र में सेंटिनेल नोड के बीच सेवा वितरण से इन्कार (डिस्ट्रीब्यूटेड डिनायल ऑफ़ सर्विस या DDoS)। हमला करने वाला सेंटिनेल से बहुत से कनेक्शन स्थापित करने का प्रयास कर सकता ह।

ताकि उन्हें सही जानकारी या कोई भी जानकारी ब्रिज को प्रसारित करने से रोका जा सके। हम सेंटिनेल से कनेक्ट करने का प्रयास करने वालों से एक छोटी सी क्रिप्टोग्राफिक पहेली का समाधान मांगकर इस समस्या से बच सकते हैं। चूंकि पूछताछ में सेंटिनेल से बहुत से कनेक्शन शामिल नहीं होंगे, इसलिए यह XYO रिले सिस्टम पर कोई भारी बोझ नहीं डालेगा और हमलावर को हमारे नेटवर्क पर सफल DDoS निष्पादित करने के लिए बहुत से संसाधनों की आवश्यकता होगी। किसी निश्चित समय पर कोई उत्पत्ति के साक्ष्य की श्रृंखला का सत्यापन XYOMainChain पर संग्रहित डेटा के रूप में कर सकता है। यह सुनिश्चित करता है कि श्रृंखला के साथ अगर कोई एकल प्रविष्टि की गई है तो पूछताछ के उत्तर की सटीकता (उत्पत्ति श्रृंखला का स्कोर) गिरकर 0 हो जाएगी।

6 XYO टोकन अर्थव्यवस्था

ऑरेकल विकेंद्रीकृत ऐप्लिकेशन के लिए जरूरी शक्ति और अवसंरचना का उल्लेखनीय भाग होता है, जिसमें सबसे अधिक ध्यान प्राधिकृत ऑरेकल की कनेक्टिविटी और एकीकरण पर होता है। हम मानते हैं कि ऑरेकल के पूरी तरह विकेंद्रीकृत और गैर भरोसा आधारित सिस्टम की आवश्यकता अधिकतम क्षमता पाने के लिए विकेंद्रीकृत ऐप्लिकेशन को पड़ती है।

6.1 XYO नेटवर्क क्रिप्टोइकोनॉमिक्स

हम सटीक, विश्वसनीय स्थान संबंधी अनुभव आधारित डेटा प्रदान करने के लिए वांछित व्यवहार को प्रोत्साहित करने हेतु XYO टोकन का उपयोग करते हैं। XYO टोकन को इस प्रकार माना जा सकता है, जैसे वास्तविक दुनिया में किसी निर्दिष्ट वस्तु के XY-गुणांक को सत्यापित करने के लिए इंटरफेस हेतु "गैस" की आवश्यकता हो।

प्रक्रिया इस प्रकार काम करती है: टोकन धारक पहले XYO नेटवर्क से कोई पूछताछ करता है (उदा. *"मेरा XYO पता 0x123456789 वाला ई-कॉमर्स ऑर्डर पैकेज कहाँ है...?"*)। इसके बाद पूछताछ को कतार में भेजा जाता है, जहाँ यह संसाधित किए जाने और उत्तर पाने का इंतजार करता है। उपयोगकर्ता पूछताछ करते समय अपने वांछित विश्वास के स्तर और XYO गैस के मूल्य को सेट कर सकता है। पूछताछ की लागत (XYO टोकन में), उस पूछताछ का उत्तर देने के लिए आवश्यक डेटा के परिमाण और बाजार की सक्रियता द्वारा निर्धारित किया जाता है। जितने डेटा की आवश्यकता होती है, पूछताछ उतना ही मंहगा होता जाता है और XYO गैस का मूल्य बढ़ता जाता है। XYO नेटवर्क से पूछे जाने वाले प्रश्न बहुत बड़े और मंहगे हो सकते हैं। उदाहरण के लिए, एक ट्रकिंग और लॉजिस्टिक्स की कंपनी XYO नेटवर्क से पूछ सकती है, "हमारे कारों के काफिले में से प्रत्येक कार की जगह क्या है*?*

XYO टोकन धारक द्वारा XYO नेटवर्क से पूछताछ करने और अनुरोधित गैस के लिए भुगतान करने पर, इस कार्य में लगे सभी डिवाइनर संबंधित आर्किविस्ट से पूछताछ का उत्तर देने के लिए जरूरी डेटा पुनर्प्राप्त करने हेतु उसे कॉल करते हैं। वापस किया गया डेटा ब्रिज से व्युत्पन्न होता है, जिसने मूल रूप से सेंटिनेल से डेटा एकत्र किया है। सेंटिनेल अनिवार्य से वे डिवाइस या सिग्नल होते हैं, जो वस्तुओं के स्थान को सत्यापित करते हैं। इनमें IoT डिवाइस में निहित ब्लूटूथ ट्रैकर, GPS ट्रैकर, जियो-लोकेशन ट्रैकिंग, सैटेलाइट ट्रैकिंग प्रौद्योगिकी, QR कोड स्कैनर, RFID स्कैनिंग और कई अन्य निकाय शामिल होते हैं। XY फाइंडेबल वस्तुओं ने अपने उपभोक्ता ब्लूटूथ और GPS व्यवसाय के क्षेत्र में शुरुआत किया है, जिसके चलते यह यह वास्तविक दुनिया के स्थान संबंधी अनुभव आधारित डेटा की जाँच और इनका संसाधन कर सकता है। XY फाइंडेबल उपभोक्ता व्यवसाय को विकसित करने के सभी प्रयासों से XYO नेटवर्क ब्लॉकचेन प्रोटोकॉल डिजाइन करने में उल्लेखनीय सहायता मिली है।

अगर सेंटिनेल डिवाइस (जैसे ब्लूटूथ बीकॉन) द्वारा प्रदत्त डेटा का उपयोग पूछताछ का उत्तर देने के लिए किया जाता है तो ट्रांजेक्शन में शामिल सभी चारों घटकों को टोकन धारक द्वारा भुगतान किए गए XYO गैस में से हिस्सा मिलता है: डिवाइनर (जिसने उत्तर खोजा है), आर्काइवर (जिसने डेटा संग्रहित किया), ब्रिज (जिसने डेटा ट्रांसमिट किया) और सेंटिनेल (जिसने स्थान संबंधी डेटा रिकॉर्ड किया)। XYO नेटवर्क के 4 में से 3 घटकों के बीच गैस का वितरण

हमेशा बराबर अनुपात में किया जाता है। अपवाद है डिवाइनर का हिस्सा, जिसकी उत्तर देने की प्रक्रिया

में संलिप्तता अधिक मंहगी होती है। प्रत्येक घटक में, गैस समान रूप से वितरित किया जाता है।

6.2 स्वतंत्रता हेतु पुरस्कार

स्थान संबंधी डेटा एकत्र करने वाले डिवाइस अपने नेटवर्क के एटॉमिक ब्लॉक होते हैं और एक डिवाइस सिस्टम के चार में से एक या अधिक घटकों का काम कर सकता है। फिर भी, खासकर बड़े XYO नेटवर्क में यह विरले ही होगा कि कोई डिवाइस इनमें से दो से अधिक घटकों का काम करे। इसके अतिरिक्त, ब्लॉकचेन की खाता-बही, जिसकी उत्पत्ति के साक्ष्य अधिक स्वतंत्र होते हैं, को अधिक बड़ा पुरस्कार मिलेगा, इसलिए एकाधिक घटक के रूप में काम करने वाले डिवाइस के लिए एक क्रिप्टोइकोनॉमिक आर्थिक दंड होता है।

6.3 स्थिर समग्रता के लिए पुरस्कार

XYO नेटवर्क में सेंटिनेल को पूरे जीवनचक्र में उनकी गति के परिमाण के लिए एक स्थिरता गुणांक निर्दिष्ट किया जाता है। किसी समयावधि में सेंटिनेल जितना कम घूमता है, इसके डेटा उतने अधिक विश्वसनीय होते हैं। आर्किविस्ट ट्रैक रखते हैं और पूछताछ को किस सेंटिनेल की ओर रूट किया जाए, इस पर विचार करते समय इन स्थिरता गुणांकों का विश्लेषण करते हैं।

6.4 टोकन के उपयोग को प्रोत्साहित करना

जिस सिस्टम में टोकन धारकों को उनके टोकन का उपयोग नहीं करने के लिए प्रोत्साहित किया जाता है, उसमें अंतर्निहित अर्थव्यवस्था के लिए दीर्घकालिक समस्या उत्पन्न हो जाती है। इसके चलते ऐसा परिवेश बनता है, जिसमें स्टोर के मूल्य बहुत कम होते हैं और वह उपयोगिता तथा तरलता बढ़ाने की जगह टोकन का उपयोग नहीं करने का कारण खोजने के लिए स्वाभाविक संवेग उत्पन्न करता है।

अधिकतर क्रिप्टोग्राफ़िक प्रोत्साहनों में समस्या ये रहती है कि टोकन माइनर (उदा, सेंटिनेल, ब्रिज, आर्किविस्ट, डिवाइनर) पर बहुत अधिक फोकस रहता है और बाकि टोकन उपयोगकर्ताओं पर नहीं रहता। XYO टोकन दोनों को खाता में रखता है।

XYO टोकन मॉडल माइनर को न सिर्फ सटीक डेटा देने के लिए, बल्कि ये जानने के लिए भी प्रोत्साहित करता है कि कब डेटा प्रदान नहीं करना है। नेटवर्क की तरलता अधिक होने की तुलना में कम होने पर अधिक ट्रांज़ेक्शन करने पर अंतिम उपभोक्ता को पुरस्कृत किया जाता है। इसलिए XYO टोकन के परिवेश में संतुलित, तरल और विशाल बने रहने की क्षमता होती है।

6.5 XYO टोकन संबंधी विशिष्टताएँ

सार्वजनिक टोकन सेल में एक श्रेणीबद्ध मूल्य संरचना होती है, जो 1 ETH: 100,000 XYO से शुरू होकर अधिकतम 1 ETH: 33,333 XYO तक जाती है। हमारे परिमाण और समय आधारित मूल्य संरचना को जल्दी ही घोषित किया जाएगा।

- स्मार्ट क्रॉन्ट्रैक्ट प्लेटफॉर्म: इथीरियम
- क्रॉन्ट्रैक्ट का प्रकार: ERC20
- टोकन: XYO
- टोकन का नाम: XYO नेटवर्क यूटिलिटी टोकन
- टोकन का पता: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- कुल निर्गमन: राशि के टोकन मैन सेल पर पहुँचने के बाद निश्चित और सर्वोच्च स्तर पर
- लक्षित XYO टोकन कैप: 4 करोड़ 80 लाख डॉलर

- न बिके और आवंटित न किए गए टोकन: टोकन सेल ईवेंट के बाद जला दिए जाते हैं। मेन सेल खत्म होने पर फिर से XYO टोकन नहीं तैयार किए जाएँगे।

7 XYO नेटवर्क के उपयोग संबंधी मामले

XYO नेटवर्क का उपयोग बड़ा अनुप्रयोग है, जिसका विस्तार बहुत से उद्योगों तक है। उदाहरण के लिए, एक ई-कॉमर्स कंपनी, जो अपने प्रीमियम ग्राहकों को वितरण सेवाओं के समय भुगतान करना प्रस्तावित करती है। यह सेवा देने के लिए, ई-कॉमर्स कंपनी स्मार्ट कॉन्ट्रैक्ट (अर्थात इथीरियम के प्लेटफॉर्म पर) तैयार करने के लिए XYO नेटवर्क (जो XYO टोकन उपयोग करता है) का उपयोग करेगी। इसके बाद XYO नेटवर्क उपभोक्ता को भेजे जा रहे पैकेज का स्थान ट्रैक करेगा, जिसके लिए हर चरण को सही तरीके से पूरा किया गया होगा, जिसमें भंडारस्थल की आलमारी से लेकर शिपिंग कुरियर तक और उपभोक्ता का घर और बीच का हर स्थान शामिल है। यह ई-कॉमर्स रीटेलर और वेबसाइट को एक गैर-भरोसा आधारित तरीके का सत्यापन करने में सक्षम बनाता है, कि पैकेज न सिर्फ ग्राहक के घर तक पहुँच गया है, बल्कि सुरक्षित रूप से उनके घर के भीतर जा चुका है। ग्राहक के घर में पैकेज पहुँच जाने पर (XY-गुणांक द्वारा परिभाषित और सत्यापित), शिपमेंट पूर्ण माना जाता है और विक्रेता का भुगतान कर दिया जाता है। इस तरह से XYO नेटवर्क का ई-कॉमर्स एकीकरण व्यापारियों को धोखाधड़ी से बचाता है और सुनिश्चित करता है कि उपभोक्ता केवल उन्हीं सामानों की कीमत दें, जो उनके घर पहुँच चुका है।

होटल रिव्यू साइट पर XYO नेटवर्क के एक बिल्कुल अलग तरह के एकीकरण पर विचार करें, जिसकी वर्तमान समस्या ये है कि उनकी समीक्षाएँ अक्सर विश्वसनीय नहीं होती हैं। स्वाभाविक है कि होटल के स्वामियों को उनकी समीक्षा हर हाल में सुधारने के लिए प्रोत्साहित किया जाता है। अगर कोई पूरे दावे के साथ कहे कि कोई सैन डिएगो का कोई व्यक्ति बाली के एक होटल में दो सप्ताह तक ठहरा और फिर सैन डिएगो लौटकर उसने बाली के उस होटल में ठहराव के बारे में समीक्षा लिखा? उस समीक्षा को बहुत महत्व मिलेगा, खासकर अगर इसे किसी ऐसे समीक्षक ने लिखा हो, जिसने स्थान संबंधी सत्यापित डेटा के साथ कई समीक्षाएँ लिखी हो।

8 XYO नेटवर्क विस्तार

हम भाग्यशाली हैं कि हमारा ऐसा उपभोक्ता व्यवसाय है, जिसने वास्तविक दुनिया में एक सफल नेटवर्क बना लिया है, जिससे दुनिया के दस लाख ब्लूटूथ और GPS डिवाइस जुड़े हैं। स्थान संबंधी अधिकांश नेटवर्क इस अवस्था तक नहीं पहुँच पाते और विस्तृत नेटवर्क बनाने के लिए आवश्यक निर्णायक परिमाण नहीं प्राप्त कर पाते। हमारे द्वारा बनाया गया सेंटिनेल नेटवर्क केवल आरंभिक बिंदु है। XYO नेटवर्क एक खुला सिस्टम है, जिसमें स्थान संबंधी डिवाइस का कोई भी ऑपरेटर प्रवेश कर सकता है और XYO टोकन कमाना प्रारंभ कर सकता है।

सामान्य रूप से, XYO नेटवर्क में सेंटिनेल की जितनी प्रमुखता होगी, इसकी विश्वसनीयता उतनी ही अधिक होगी। इसका नेटवर्क और अधिक विस्तृत करने के लिए, XYO नेटवर्क, अपने XY फाइन्डेबल बीकॉन के नेटवर्क से आगे बढ़कर दूसरे व्यवसायों से मिलकर इसके सेंटिनेल के नेटवर्क को विस्तारित कर रहा है।

9 अभिस्वीकृतियाँ

यह श्वेत पत्र टीम की कोशिशों को प्रेरित करने का प्रतिफल है, जो निम्नलिखित लोगों के ध्येय पर विश्वास करने के चलते संभव हो पाया: रॉउल जॉर्डन (हार्वर्ड कॉलेज, थिएल फेलो और XYO नेटवर्क के परामर्शदाता); हमारा श्वेत पत्र को अधिक संक्षिप्त बनाने में अपने योगदान और दुनिया को इसका तकनीकी विवरण देने हेतु शानदार संचार में हमारी मदद करने के लिए हम इन्हें धन्यवाद देते हैं। हम क्रिस्टाइन सैको को उनकी असाधारण कार्य नैतिकता और हमारे कार्य की समीक्षा में पूरी सावधानी बरतने के लिए धन्यवाद देते हैं। हमारे श्वेत पत्र में संरचना में संगतता और सही पद्धति देखी गई, जो कि क्रिस्टाइन के प्रयासों का परिणाम है। हम जॉनी

कौलासिंस्की को उनके शोध और लागू उपयोग के मामलों के संकलन के लिए धन्यवाद देते हैं। अंत में, हम जॉन एरेना को उनकी समीक्षा और रचनात्मक इनपुट के लिए धन्यवाद देते हैं।

संदर्भ

[1] ब्लैंचर्ड, वाल्टर. *हाइड्रोबोलिक वायुजनित रेडियो नेविगेशन* सहायक उपकरण। जर्नल ऑफ़ नेविगेशन, 44(3), सितंबर 1991.

[2] कारापेटसास, लेफ्टेरिस। *Sikorka.io*.
http://sikorka.io/files/devcon2.pdf. शंघाई, 29 सितंबर 2016.

[3] डी फेरान्टे, मैट. स्थान का साक्ष्य।
https://www.reddit.com/r/ethereum/comments/539o9c/proof of location/. September 17, 2016.

[4] गोवार्ड, डाना। RNT *फाउंडेशन कांग्रेस के सामने जाँच करता है।* US हाउस ऑफ़ रिप्रेजेंटेटिव की सुनवाई: "अपनी राह खोजना: नेविगेशन के लिए संघीय सहायता उपकरण का भविष्य," वाशिंगटन, DC, 4 फरवरी 2014.

शब्दावली

सटीकता विश्वास की माप, कि डेटा पॉइंट या अनुभव आधारित डेटा एक विशिष्ट त्रुटि सीमा के भीतर आते हैं।

आर्किविस्ट आर्किविस्ट विकेंद्रीकृत डेटा सेट के भाग के रूप में अनुभव आधारित डेटा संग्रहित करते हैं, जिसका लक्ष्य सभी ऐतिहासिक खाता-बही को संग्रहित करना होता है, लेकिन इसकी कोई आवश्यकता नहीं होती। यहाँ तक कि कुछ डेटा के खो जाने या अस्थायी रूप से अनुपलब्ध होने पर, सिस्टम काम करना जारी रखता है, बस सटीकता में कमी आ जाती है। आर्किविस्ट खाता-बही की सूची भी बनाते हैं, ताकि जरूरी होने पर वे खाता-बही का डेटा उपलब्ध करा सकें। आर्किविस्ट केवल असंसाधित डेटा संग्रहित करते हैं और डेटा की पुनर्प्राप्ति के लिए अकेले भुगतान प्राप्त करते हैं। संग्रहण हमेशा निःशुल्क होता है।

सर्वश्रेष्ठ उत्तर हम उत्तरों की एक सूची में से सर्वश्रेष्ठ उत्तर को एकल उत्तर के रूप में परिभाषित करते हैं, जिसका वैधता स्कोर सबसे अधिक होता है और सटीकता का परिमाण न्यूनतम आवश्यक सटीकता से अधिक होता है।

सर्वश्रेष्ठ उत्तर का अल्गोरिद्म: डी-विनर द्वारा उत्तर चुने जाने पर सर्वश्रेष्ठ उत्तर तैयार करने के लिए एक अल्गोरिद्म का उपयोग किया जाता है। XYO नेटवर्क विशिष्ट अल्गोरिद्म जोड़ने की अनुमति देता है ग्राहकों को यह चयन करने देता है कि किस अल्गोरिद्म का उपयोग करना है। दिए गए डेटा सेट के लिए किसी डिवाइनर पर रन करते समय जरूरी है कि इस अल्गोरिद्म के परिणामस्वरूप उतने ही स्कोर आएँ।

बाध्य साक्षी (बाध्य साक्षी) बाध्य साक्षी द्विआयामी अनुभव आधारित डेटा की मौजूदगी द्वारा हासिल अवधारणा है। बताया गया है कि डिजिटल कॉन्ट्रैक्ट रिज़ॉल्यूशन (ऑरेकल) के उपयोग के लिए गैर-भरोसेमंद डेटा स्रोत उपयोगी नहीं होता, ऐसे अनुभव आधारित डेटा केंद्र की स्थापना से प्राप्त डेटा की सुनिश्चितता में काफी बढ़ोतरी होती है। प्राथमिक द्विआयामीय अनुभव आधारित स्रोत है निकटता, क्योंकि इंटरैक्शन पर सह-हस्ताक्षर होने के चलते, दोनों पक्ष इंटरैक्शन और इसकी सीमा को सत्यापित कर सकते हैं। यह दो नोड के एक दूसरे के निकट होने की स्थिति के लिए शून्य-जानकारी के साक्ष्य को अनुमति देता है.

ब्रिज: ब्रिज अनुभव आधारित डेटा को प्रतिलिपित करते हैं। वे सुरक्षित रूप से अनुभव आधारित खाता बही को को सेंटिनेल से लेकर आर्किविस्ट को जारी कर सकते हैं। ब्रिज का सबसे महत्वपूर्ण पहलु ये है कि आर्किविस्ट इस बात के प्रति

निश्चिंत हो सकते हैं कि ब्रिज से प्राप्त अनुभव आधारित खाता बही में किसी प्रकार की कोई छेड़छाड़ नहीं की गई है। ब्रिज का दूसरा महत्वपूर्ण पक्ष ये है कि वे उत्पत्ति मेटाडेटा का एक अतिरिक्त साक्ष्य जोड़ते हैं।

सुनिश्चितता: संभावना की एक माप कि एक डेटा पॉइंट या अनुभव आधारित डेटा से छेड़छाड़ या उसे दूषित नहीं किया गया है।

क्रिप्टो-लोकेशन: क्रिप्टोग्राफ़िक स्थान संबंधी प्रौद्योगिकी का क्षेत्र।

क्रिप्टोइकोनॉमिक्स: औपचारिक क्षेत्र, जिसमें एक विकेंद्रीकृत डिजिटल अर्थव्यवस्था में उत्पादन, वितरण और सामान तथा सेवाओं की खपत को नियंत्रित करने वाले प्रोटोकॉल का अध्ययन किया जाता है। क्रिप्टोइकोनॉमिक्स एक व्यावहारिक विज्ञान है, जिसका फोकस इन प्रोटोकॉल के डिजाइन और विशेषता बताने पर होता है।

डिवाइनर: डिवाइनर XYO नेटवर्क पर संग्रहित पुराने डेटा का विश्लेषण करके, किसी पूछताछ का उत्तर देता है। XYO नेटवर्क पर संग्रहित अनुभव आधारित डेटा का उत्पत्ति का साक्ष्य उच्च स्तरीय होना चाहिए, जिससे अनुभव आधारित डेटा की वैधता और शुद्धता निर्धारित हो। डिवाइनर उत्पत्ति के साक्ष्य के आधार पर साक्ष्यों पर निर्णय लेते हुए उत्तर प्राप्त और वितरित करता है। बताया गया है कि XYO नेटवर्क एक गैर भरोसा आधारित सिस्टम है, तो डिवाइनर को अनुभव आधारित डेटा के ईमानदार विश्लेषण के लिए प्रोत्साहित किया जाना चाहिए। सेंटिनेल और ब्रिज से अलग, डिवाइनर ब्लॉकचेन में उत्तर जोड़ने के लिए कार्य के साक्ष्य का उपयोग करते हैं।

अनुभव आधारित डेटा: वास्तविक दुनिया से संबंधित डेटा, जो सेंटिनेल (निकटता, तापमान, प्रकाश, गति आदि...) की स्थिति के सापेक्ष होता है।

ऑरेकल DApp (विकेंद्रीकृत ऐप्लिकेशन) सिस्टम का एक भाग, जो शुद्धता और सुनिश्चितता के साथ उत्तर देकर डिजिटल कॉन्ट्रैक्ट का समाधान करने के लिए जिम्मेदार है। "ऑरेकल" शब्द क्रिप्टोग्राफ़ी से संबंध रखता है, जहाँ यह वाकई यादृच्छिक स्रोतों (उदा., यादृच्छिक संख्या) का उल्लेख करता है। यह बाहर की दुनिया को क्रिप्टो समीकरण के माध्यम से एक द्वार उपलब्ध कराता है। ऑरेकल श्रृंखला से बाहर (वास्तविक दुनिया या ऑफ़-चेन) की जानकारियाँ स्मार्ट कॉन्ट्रैक्ट को देता है।ऑरेकल डिजिटल दुनिया में वास्तविक दुनिया का इंटरफेस है।बीमार व्यक्ति का उदाहरण लेने पर, अंतिम इच्छा और वसीयत पर विचार करें। वसीयत की शर्तें इस बात की पुष्टि के बाद निष्पादित की जाती हैं कि वसीयतकर्ता की मृत्यु हो गई है। ऑरेकल सेवा आधिकारिक स्रोतों से संबंधित डेटा के संकलन और एकीकरण द्वारा वसीयत को लागू करने के लिए तैयार की जा सकती है। ऑरेकल का उपयोग स्मार्ट कॉन्ट्रैक्ट को कॉल करने के लिए फीड या अंतिम बिंदु के रूप में उपयोग किया जाता है, ताकि यह देखा जा सके कि व्यक्ति की मृत्यु हुई है या नहीं।

उत्पत्ति श्रृंखला का स्कोर: उत्पत्ति श्रृंखला की साख के निर्धारण के लिए इसे स्कोर असाइन किया जाता है।इस आंकलन में लंबाई, उलझन, ओवरलैप और पुनरावृत्ति पर विचार किया जाता है।

उत्पत्ति वृक्ष: विभिन उत्पत्ति श्रृंखलाओं से ली गई खाता-बही प्रविष्टियों का एक डेटा सेट, जिससे एक विशिष्ट स्तर की सुनिश्चितता वाले अनुभव आधारित खाता बही की उत्पत्ति प्रमाणित की जा सके।

उत्पत्ति के साक्ष्य: उत्पत्ति का साक्ष्य XYO नेटवर्क में होने वाले प्रवाह की खाता-बही की वैधता के सत्यापन की कुंजी है। डेटा के स्रोत के लिए एक अद्वितीय ID व्यावहारिक नहीं है, क्योंकि इसमें जालसाजी की जा सकती है। सार्वजनिक कुंजी हस्ताक्षर व्यावहारिक नहीं है, क्योंकि XYO नेटवर्क के अधिकांश भाग को भौतिक रूप से सुरक्षित बनाना कठिन या असंभव है, इसलिए दुर्भावनापूर्ण व्यक्ति के द्वारा सार्वजनिक कुंजी चुरा लिया जाना भी संभव है। इसके समाधान के लिए, XYO नेटवर्क अस्थायी कुंजी श्रृंखला का उपयोग करता है। इसका लाभ यह है कि डेटा के लिए उत्पत्ति की श्रृंखला का जालसाजीकरण असंभव हो जाता है। फिर भी, यह श्रृंखला एक बार टूटने पर हमेशा के लिए टूट जाता है और फिर जारी नहीं रखा जा सकता।

उत्पत्ति के साक्ष्य की श्रृंखला: अस्थायी कुंजी श्रृंखला, जिसमें बाध्य साक्षी अनुभव आधारित खाता बही प्रविष्टियाँ एक साथ जुड़ी होती हैं।

कार्य के साक्ष्य: कार्य का साक्ष्य ऐसा डेटा होता है, जो कुछ नियत अपेक्षाओं को पूरी करता है, इसे तैयार करना कठिन होता है (अर्थात, मंहगा होता है, बनने में समय लेता है), लेकिन दूसरे इसे आसानी से सत्यापित कर सकते हैं। कार्य का साक्ष्य तैयार करना ऐसी यादृच्छिक प्रक्रिया हो सकती है, जिसमें इसे तैयार करने की संभावना कम होती है, इसलिए कार्य का वैध साक्ष्य बनाने के लिए अक्सर उससे पहले कठिन परीक्षण से गुजरना और त्रुटियों का सामना करना पड़ता है।

सेंटिनेल: सेंटिनेल अनुभव-आधारित साक्ष्य होते हैं। वे अनुभव पर आधारित डेटा का अवलोकन करते हैं और अस्थायी

खाता-बही बनाकर अनुभव आधारित डेटा की सुनिश्चितता और शुद्धता प्रमाणित करते हैं। सेंटिनेल का सबसे महत्वपूर्ण पक्ष ये है कि वे उत्पत्ति का साक्ष्य जोड़कर इस बात की खाता-बही तैयार करते हैं कि डिवाइनर निश्चित रूप से किसी खास निर्दिष्ट स्रोत से ही आए हैं।

स्मार्ट कॉन्ट्रैक्ट: निक जैबो द्वारा बिटकॉइन से पहले खोजा गया प्रोटोकॉल, इसे कथित रूप से 1994 में खोजा गया (इसीलिए कुछ लोग मानते हैं कि वे ही बिटकॉइन के रहस्यमयी और गुमनाम आविष्कारक सातोषी नाकामोटो हैं) स्मार्ट कॉन्ट्रैक्ट के पीछे किसी प्रोग्राम में कानूनी समझौते को कूटबद्ध करने और इसकी शर्तों का पालन करने के लिए विकेंद्रीकृत कम्प्यूटर बनाने का उद्देश्य था, जिससे लोग समझौते को समझ न सकें। स्मार्ट कॉन्ट्रैक्ट में मुद्रा (उदा., ईथर) और अनुबंध का इसी अवधारणा के अंतर्गत विघटन हो जाता है। स्मार्ट कॉन्ट्रैक्ट होने का अर्थ है कि यह निर्णायक (जैसे कि कंप्यूटर प्रोग्राम) और पूरी तरह पारदर्शक तथा पठनीय है, वे मध्यस्थों और दलालों (ब्रोकर) को हटाकर एक शक्तिशाली माध्यम के रूप में काम करते हैं। 17, 13, 16

अस्थायी कुंजी श्रृंखला: अस्थायी कुंजी श्रृंखला अस्थायी कुंजी क्रिप्टोग्राफ़ी का उपयोग करके डेटा पैकेट की श्रृंखला को लिंक करता है। 11

गैर भरोसा आधारित: ऐसी विशेषता, जहाँ किसी सिस्टम के सभी पक्ष वैधानिक सत्यता के संदर्भ में एक सहमति पर पहुँच सकें। शक्ति और विश्वास किसी एक व्यक्ति या निकाय (उदा, बैंक, सरकार और वित्तीय संस्थाएँ) पर संकेद्रित रहने के बजाय नेटवर्क के साझेदारों (उदा., डेवलपर, माइनर और उपभोक्ता) के बीच वितरित (या साझा) किए जाते हैं। यह एक ऐसा शब्द है, जिसका गलत अर्थ लगाया जाना आम है। ब्लॉकचेन में भरोसा हो ही नहीं, ऐसा नहीं है। इसमें असल में, सिस्टम के किसी एक घटक के लिए जरूरी भरोसा का परिमाण कम होता है। वे एक आर्थिक गेम के जरिए भरोसे को सिस्टम के विभिन्न घटकों के बीच वितरित कर देते हैं, जो घटकों को प्रोटोकॉल द्वारा परिभाषित नियमों के अनुरूप सहभागिता के लिए प्रोत्साहित करता है। 1, 3–5, 8, 14, 16

XY ऑरेकल नेटवर्क XYO नेटवर्क। 1

XYO नेटवर्क XYO नेटवर्क का अभिप्राय है "XY ऑरेकल नेटवर्क।" यह XYO सक्षम घटकों/नोड के पूरे सिस्टम से बना होता है, जिसमें सेंटिनेल, ब्रिज, आर्किविस्ट और डिवाइनर होते हैं। XYO का प्राथमिक कार्य एक ऐसे पोर्टल के रूप मे काम करना है, जिसके द्वारा डिजिटल स्मार्ट कॉन्ट्रैक्ट को वास्तविक दुनिया के जियो-लोकेशन की पुष्टि के जरिए निष्पादित किया जाता है। 2–5, 7, 11, 14–17

XYOMainChain: XYO नेटवर्क में अपरिवर्तनीय ब्लॉकचेन, जो डिवाइनर के द्वारा एकत्र किए गए डेटा और उनसे संबंधित उत्पत्ति के स्कोर के साथ पूछताछ के ट्रांज़ेक्शन को संग्रहित करता है। 4–7, 14