XY Oracle Network: Proof-of-Origin Tabanlı Kriptografik Konum Ağı

Arie Trouw *, Markus Levin †, Scott Scheper ‡

Ocak 2018

Özet

Bağlı ve konuma dayalı teknolojilerin büyümekte olan mevcudiyetiyle özel yaşamımız ve güvenliğimiz ciddi şekilde konum bilgisinin doğruluğuna geçerliliğine bağlı hale gelmektedir. Konum verisinin akışını kontrol eden merkezi kuruluşlara olan ihtiyacın ortadan kaldırılması için çeşitli girişimlerde bulunulmuştur ancak her girişim, fiziksel dünyada bu veriyi toplayan cihazların bütünlüğüne dayanmıştır. Biz, konum bilgisinde yüksek dereceli veri kesinliği oluşturmak için sıfır bilgi ispatları zincirine dayanan yeni bir formülasyon kullanarak güvene ihtiyaç duymayan kriptografik konum ağı öneriyoruz. **XYO Network (XY Oracle Network)** birçok cihaz sınıfı ve prokotoller boyunca katmanlı konum doğrulamayı sağlayan bir soyutlamadır. Özünde, bugün blok zinciri teknoloji ve gerçek dünya verisi koleksiyonunu doğrudan uygulamalarla bir sistem içinde birleştiren **Proof of Origin** ve **Bound Witness** olarak bilinen yeni kriptografik mekanizmalar yer almaktadır.

1 Giriş

Blok zinciri tabanlı, güvene ihtiyaç duymayan akıllı kontratların gelmesiyle kontratın sonucuna hakemlik eden oracle servislerine olan ihtiyaç orantılı olarak artmaktadır. Akıllı kontratların mevcut uygulamaları, kontratın sonucunu belirleyen tekli veya kümelenmiş yetkili oracle setlerine dayanır. Her iki tarafın belirtilen oracle'ın yetkisine ve dürüstlüğüne güvenebildiği durumlarda bu yeterlidir. Ancak, birçok durumda ya yeterli oracle mevcut değildir ya da oracle, hata veya bozulma ihtimali nedeniyle yetkili olarak kabul edilememektedir.

Konum oracle'ları bu kategoride yer almaktadır. Fiziksel dünya nesnesinin lokasyonunun tahmini, belirli oracle'ın raporlama, iletme, depolama ve işleme bileşenlerine dayalıdır ve bunların hepsi hata üretebilir veya bozulabilir. Riskler; veri manipülasyonu, veri kirliliği, veri kaybı ve hileli anlaşmayı içerir.

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

Bu nedenle şu sorun mevcuttur; **konumunun kesinliği ve doğruluğu güvene ihtiyaç duymayan ve merkezi olmayan bir oracle'ın eksikliğinden negatif olarak etkilenir.** Ethereum ve EOS gibi platformlar, emanetçileri için emanetleri içeren ana kullanım senaryolarında karşılıklı etkileşimlerde çevrim içi olarak güvenli şekilde aracılık etme karşılığında ICO biçiminde para kazanmak için geniş ölçüde kullanılmaktadır. Ancak, şimdiye kadar her platform, mevcut bilgi kanallarının gürültülü ve bozulabilir veri bütünlüğü nedeniyle fiziksel dünyaya değil, tamamen çevrim içi dünyaya odaklanmıştır.

XYO Network, blok zinciri platformlarında akıllı kontrat yazanlar gibi geliştiricilerin, gerçek dünya ile sanki bir API imiş gibi etkileşimde bulunmalarını sağlama konsepti üzerine çalışıyor. XYO Network, merkezi bir üçüncü taraf ihtiyacı olmadan iki oluşumun gerçek dünyada işlem yapmasını mümkün kılan dünyanın ilk oracle protokolüdür. Soyutlamalarımız, bugüne kadar mümkün olmayan yeni kullanım durumlarıyla bir protokol oluşturarak konum doğrulamayı, geliştiriciler için güvene ihtiyaç duymayacak şekilde yapmamızı sağlamaktadır.

XYO Network, müşteriye dönük findables işi vasıtasıyla bütün dünyaya dağıtılmış olan 1.000.000 cihazlık mevcut bir altyapı üzerine kurulacaktır. XY'nin Bluetooth ve GPS cihazları; günlük tüketicilerin, fiziksel izleme istasyonlarını, takip etmek istedikleri şeylerin (anahtarlar, bagaj, bisikletler ve hatta evcil hayvanlar) üzerine yerleştirmelerini sağlar. Bu tür nesneleri yanlış yerleştirirlerse veya kaybederlerse bir akıllı telefon uygulamasıyla konum görüntüleyerek tam olarak nerede olduklarını görebilirler. Yalnızca altı yıl içinde XY Network, dünyadaki en geniş tüketici Bluetooth ve GPS ağlarından birisini oluşturdu.

2 Tarihsel Arka Plan ve Önceki Yaklaşımlar

2.1 Proof of Location

İspat edilebilir konum konsepti, 1960'lardan beri gündemdedir ve hatta LORAN [1] gibi yerde konuşlu telsiz seyrüsefere sistemleriyle 1940'lara kadar dayanmaktadır. Günümüzde, üçgenleştirme ve GPS servisleri aracılığıyla Proof of Location oluşturmak için doğrulama araçlarını üst üste istif eden konum servisleri vardır. Ancak bu yaklaşımlar, bugün konum teknolojilerinde karşılaştığımız en kritik bileşeni henüz ele alamadı; bu bileşen, hileli sinyalleri tespit eden ve konum verilerinin yanıltılmasını caydıran bir sistemin tasarlanmasıdır. Bu nedenle günümüzde en önemli kripto konum platformunun, fiziksel konum sinyallerinin kökeninin ispat edilmesine en fazla odaklanan platform olacağını ileri sürüyoruz.

Şaşırtıcı şekilde, konum doğrulamanın blok zinciri teknolojisine uygulanması konsepti ilk olarak Eylül 2016'da Ethereum's DevCon 2'da ortaya çıktı. Berlin'de bir Ethereum geliştiricisi olan Lefteris Karapetsas tarafından tanıtıldı. Karapetsas'ın projesi *Sikorka*, "*Proof of Presence*" olarak isimlendirdiği öğeyi kullanarak akıllı kontratların gerçek zamandaki bir noktaya uygulanmasını sağladı. Onun konumu blok zinciri dünyası ile birleştirme uygulaması, esasen artırılmış gerçeklik kullanım durumlarına odaklandı ve o, birisinin konumunun ispat edilmesine yönelik zorlu sorular sorulması gibi yeni konseptleri tanıttı [2].

17 Eylül 2016'da, "*Proof of Location*" terimi resmen Ethereum topluluğunda ortaya çıktı [3]. Ardından, bu konu Ethereum Vakfı geliştiricisi Matt Di Ferrante tarafından bu daha fazla açıklandı:

> *"Güvenebileceğiniz Proof of Location, doğruyu söylemek gerekirse gerçekleştirmesi en zor şeylerden birisidir. Birbirlerinin konumunu açıklayan birçok katılımcıya sahip*

olsanız bile onların gelecekte herhangi bir noktada sabit duracaklarının bir garantisi yoktur ve siz yalnızca çoğunluk bildirimine güvendiğiniz için bu büyük bir zafiyettir. Özel anahtarın, birisi onu açmaya çalıştığında veya üzerindeki donanım yazılımını değiştirmeye çalıştığında imha edilmesi gibi hileyi önleyici teknolojiye sahip birkaç özelleştirilmiş donanım cihazına gerek duyarsanız o zaman belki daha güvenli bir sisteme sahip olabilirsiniz, ancak bu, GPS sinyallerinin yanıltılmasının imkansız olduğu gibi bir şey değildir. Bunun uygun şekilde gerçekleştirilmesi, birçok geri çekilme noktasını ve doğruluğun güvencesi için birçok farklı veri kaynağını gerektirir ve de çok iyi finanse edilmiş bir proje olması gerekecektir." [3]

—Matt Di Ferrante, Geliştirici, Ethereum Vakfı

2.2 Proof of Location: Eksik Yönleri

Özetle, Proof of Location, zaman damgalaması, merkezi olmama gibi blok zincirinin güçlü özelliklerinin kullanılması ve onların, *ümitle* aldatması zor zincir dışı ve konum duyarlı cihazlarla birleştirilmesi olarak anlaşılabilir. Biz, kriptografik konum teknolojisini "*kripto konum*" olarak adlandırıyoruz. Ayrıca, akıllı kontratların zayıflığının tek bir doğruluk kaynağını kullanan (ve bu nedenle de tek bir hata kaynağına sahip olan) oracle'larla ilgili olmasına benzer şekilde kripto konum sistemleri de aynı sorunla karşılaşmaktadır. Mevcut kripto konum teknolojilerindeki zafiyet, bir nesnenin lokasyonunu geri bildirimde bulunan zincir dışı cihazlarla ilgilidir. Akıllı kontratlarda bu zincir dışı veri kaynağı, oracle'dır. XYO Network'te, zincir dışı veri kaynağı, Sentinel olarak adlandırdığımız özel bir oracle tipi olarak gerçek dünyada gezinmektedir. XYO Network'ün özündeki gerçek inovasyon, güvene ihtiyaç duymayan kripto konum protokolü oluşturmak için sistemimizin bileşenlerinin temelini teşkil eden kimliksiz, konum tabanlı ispat ile ilgilidir.

---

3 XY Oracle Network

"GPS'i tamamlamak için bozulması zor bir sistem ihtiyacı yıllardır iyi bilinmektedir. GPS, olağanüstü doğru ve güvenilirdir ancak karıştırma, yanıltma, siber saldırılar ve diğer karıştırma şekilleri, sıklık ve ciddiyet açısından artıyor gibi görünmektedir. Bu durumun, hayatlarımıza ve ekonomik faaliyetimize yıkıcı etkileri olma ihtimali vardır. [4]

—Dana Goward, Başkan, RNT Vakfı

3.1 Giriş

XYO Network'ün amacı, saldırıya dayanıklı ve mevcut veri için sorgulandığında mümkün olan en yüksek kesinliği üreten, konum oracle'larının güvene ihtiyaç duymayan ve merkezi olmayan bir sistemini oluşturmaktır. Bunu, sistemin bileşenleri boyunca sıfır bilgi ispatları zinciri aracılığıyla konum yanıltma riskini geniş ölçüdeazaltan soyutlama setleri vasıtasıyla başarıyoruz.

3.2 Network'e Genel Bakış

Sistemimiz, kriptografik ispatlar zinciri aracılığıyla konum verilerinde yüksek kesinlik sağlayan bağlı cihazlar protokolüne bir giriş noktası sağlar. Kullanıcılar,

akıllı kontrat işlevselliğine sahip herhangi bir blok zinciri teknolojisinde [1] bir parça konum verisini bulup getirmek için "*sorgular*" adı verilen işlemleri yapabilir. Daha sonra XYO Network toplayıcıları, kontrata yayımlanan bu sorguları dinleyebilir ve kriptografik ispatları geri bu toplayıcılara aktaran merkezi olmayan birtakım cihazlardan alınan en yüksek kesinliğe sahip cevapları getirebilirler. Daha sonra bu toplayıcılar, en iyi puana sahip cevap üzerinde fikir birliğine varılmasından sonra bu cevapları geri akıllı kontrata geri yollar. Bu bileşenler ağı, mümkün olan en ispatlanabilir ve güvene ihtiyaç duymayan kesinlikle, bir nesnenin belirli bir zamanda belirli bir XY koordinatında olup olmadığının belirlenmesini mümkün kılar.

XYONetwork, dört ana bileşene sahiptir: **Sentinel'ler** (Veri Toplayıcıları), **Bridge'ler** (Veri Aktarıcıları), **Archivist'ler** (Veri Depolayıcıları), ve **Diviner'lar** (Cevap Toplayıcıları). Sentinel'ler, sensörler, telsizler ve diğer araçlar vasıtasıyla konum bilgisini toplar. Bridge'ler, Sentinel'lerden bu konum verisini alır ve Archivist'lere aktarır. Archivist'ler, bu bilgiyi Diviner'ların analiz etmesi için depolar. Diviner'lar, sorgulara cevap üretmek ve onlara puan vermek için Archivist'lerden alınan konum sezgisel veri noktalarını analiz eder. Diviner'lar daha sonra bu cevapları akıllı kontrata aktarır (bu nedenle, Diviner'lar, oracle'lar olarak işlev görür). **Origin Chain Score** olarak adlandırılan doğruluk puanı, **Proof of Origin Chain** olarak bilinen bir takım sıfır bilgi ispatları aracılığıyla belirlenir. Bu zincir, temel herhangi bir veriyi açığa vurmadan aynı kaynaktan gelen iki veya daha fazla veri parçasını garanti eder. Sorug yolu boyunca her bileşen, veriyi aktardığı her bileşene zincirlenen kendi Proof of Origin'ini üretir. Proof of Origin, yüksek güvene sahip gerçek dünya verisini sağlamak için aktarıcıların yol boyunca kriptografik zincir garantilerini oluşturan yeni bir formülasyondur. Bu **Proof of Origin Chain,** veriyi toplayan ilk cihazlara kadar bir parça konum verisinde sahip olabileceğimiz güveni kapsar. Proof of Origin'in nasıl çalıştığı sonraki bölümde detaylı olarak inceleyeceğiz.

Diviner'lar arasında merkezi olmayan bir fikir birliği tesis etmek için, XYO Network, Diviner'lar ve onların ilişkili köken puanından toplanan veriyle birlikte sorgu işlemlerini depolayan ve **XYOMainChain** olarak bilinen halka açık ve değişmez bir blok zincirine dayanmaktadır. Bütün sistemin işlevselliğinin detaylarına geçmeden önce ağımızdaki her bileşenin sorumluluklarını açık bir biçimde tanımlayacağız.

3.2.1 Sentinel'ler

Sentinel'ler, konum şahitleridir. Sezgisel veri noktalarını gözlemlerler ve geçici kayıt defterleri üreterek sezgisel veri noktalarının kesinliğini ve doğruluğunu teyit ederler. Sentinel'lerin en önemli özelliği, diğer bileşenlerin kayıt defterlerinin aynı kaynaktan geldiğinden emin olabilmelerini sağlayacak şekilde kayıt defterleri üretmeleridir. Bunu, kriptografik ispatların aktarma zincirine Köken İspatı ekleyerek yaparlar. XYO Network'ün, güvene ihtiyaç duymayan bir sistem olduğu göz önüne alındığında Sentinel'ler, sezgisel veri noktaların güvenilir analizini sağlayacak şekilde teşvik edilmelidir. Bu, ün bileşeninin ödeme bileşeni ile birleştirilmesiyle yapılır. Sentinel, bir sorguya cevap vermek için bilgileri kullanıldığında XYO Network Token'leri (XYO) ile ödüllendirilir. Ödüllendirilme ihtimalini artırmak için, kendilerini konum bilgisinin kaynağı olarak tanıtmak için Proof of Origin sağlayan ve akranlarınınkiler ile tutarlı kayıt defterleri oluşturmalıdırlar.

[1] Ethereum, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counterparty, Monax ve diğerleri

3.2.2 Bridge'ler

Bridge'ler, konum veri kopya edicileridir. Konum kayıt defterlerini, güvenli şekilde Sentinel'lerden Archivist'lere aktarırlar. Bridge'in en önemli özelliği Archivist'in, Bridge'den alınan sezgisel veri noktası kayıt defterlerinin herhangi bir şekilde değiştirilmediğinden emin olabilmesinin sağlanmasıdır. Bridge'in ikinci en önemli özelliği ise ilave Proof of Origin eklemeleridir. XYO Network'ün, güvene ihtiyaç duymayan bir sistem olduğu gözönüne alındığında Bridge'ler, sezgisel veri noktalarının güvenilir analizini sağlayacak şekilde teşvik edilmelidir. Bu, ün bileşeninin ödeme bileşeni ile birleştirilmesiyle yapılır. Bridge, bir sorguya cevap vermek için aktardıkları bilgi kullanıldığında XYO Network Token'leri (XYO) ile ödüllendirilir. Ödüllendirilme ihtimalini artırmak için, kendilerini sezgisel veri noktasının aktarıcısı olarak tanıtmak için Proof of Origin sağlayan ve akranlarınınkiler ile tutarlı kayıt defterleri oluşturmalıdırlar.

3.2.3 Archivist'ler

Archivist'ler, tüm geçmiş kayıt defterlerinin depolanması amacıyla merkezi olmayan bir biçimde Bridge'lerden alınan konum bilgisini depolar. Bazı veriler kaybolsa veya geçici olarak kullanılamaz hale gelse bile sistem yalnızca azaltılmış doğrulukla işlev görmeye devam eder. Archivist'ler ayrıca gerektiği takdirde kolaylıkla kayıt defteri veri dizesini döndürebilmeleri için kayıt defterlerini indeksler. Archivist'ler yalnızca ham veriyi depolar ve sadece veri çekme ve sonraki kullanımı için XYO Network Token ödemesi alırlar. Depolama her zaman ücretsizdir.

Archivist'ler ağ bağlantılıdır ve bu nedenle bir Archivist'e talepte bulunulduğunda, o Archivist'in kendisinde bulunmayan veriler için diğer Archivist'lere talepte bulunmasına neden olacaktır. Archivist, isteğe bağlı olarak kendisine döndürülen herhangi bir kayıt defteri verisini depolayabilir. Bu durum, büyük ihtimalle iki tür Archivist'e neden olacaktır; "bulut"un veri üretim kenarında olanlar ve "bulut"un veri tüketim tarafında olanlar. Ortadaki Archivist'ler, hibrit olacaktır. Veriyi depolama seçeneği zorunlu değildir ancak, IPFS veya diğer merkezi olmayan depolama çözümleri vasıtasıyla kolaylıkla yapılabilir. Tüm Archivist'ler ödeme aldığından dolayı veri, bir Archivist'ten diğerine her devredildiğinde, ödemeyi izlemek için ilave Proof of Origin eklenir. Bilgi çekme için, geçerliliği artırmak için minimum Proof of Origin seviyesi ayarlanabilir. Verinin şişmesini önlemek için Sentinel'lerin, Bridge'lerin, ve Archivist'lerin çıkarları aynı seviyede olmalıdır.

3.2.4 Diviner'lar

Diviner'lar, XYO Network'ün en kompleks kısmıdır. Bir Diviner'in bütün amacı, bir sorgu için XYO Network'den en doğru veriyi almak ve o veriyi sorguyu yapana aktarmaktır. Diviner'lar, XYO akıllı kontrata yapılan sorgular için, uygulanabilir blok zinciri platformunu (örn. Ethereum, Stellar, Cardano, IOTA, vb.) sorgular. Ardından cevabı en yüksek doğruluk/güven puanıyla getirmek için doğrudan Archivist ağıyla etkileşimde bulunarak sorgunun cevabını bulur. Bunu, şahiti en iyi Proof of Origin zinciriyle değerlendirerek yapar. En kısa zamanda en iyi puanla cevabı getiren Diviner'lar, Proof of Work aracılığıyla ana XYO blok zincirinde (XYO Main Chain) blok oluşturma yeteneğine sahip olur. Sorgular, ödül boyutuna ve karmaşıklığına göre önceliklendirilir, yani bir cevap için ne kadar fazla XYO sunulursa sorgu öncelik açısından o kadar yüksek olacaktır.

Diğer Diviner'lar, bloğun geçerliliği konusunda fikir birliğine varır ve bloğu dijital olarak imzalar. O blokta coinbase adresi olan Diviner, daha sonra akıllı kontrata cevabı doğruluk puanı ile birlikte içeren bir işlem gönderecektir. Ayrıca bir saldırganın, Diviner

gibi görünerek blok zincirinde sahte bilgi oluşturmasını önlemek için diğer Diviner'ların imzaların bir listesini de gönderir. Daha sonra akıllı kontrat, faydalı yüklerin imza listesini kontrol ederek bu bilginin doğruluğunu onaylayabilir.

3.3 Uçtan Uca İşlevsellik

Her bir bileşenin sorumlulukları ayrıntılı olarak anlatıldığına göre sistemin nasıl çalışacağına dair uçtan uca bir örnek şu şekildedir:

1. **Sentinel'ler Veri Toplar**
   - Sentinel'ler, gerçek dünya konum sezgisel veri noktasını toplar ve kendilerinden üstteki düğümlere zincirlenmesi için kendi Proof of Origin'lerini hazırlar
2. **Bridge'ler, Sentinel'lerden Veriyi Toplar**
   - Bridge'ler, çevrim içi Sentinel'lerden gerekli veriyi toplar ve zincirlerine Proof of Origin ekler. Bridge'ler, Network'teki Archivist'lerin istifadesine sunar.
3. **Archivist'ler, Bridge'lerden Veriyi İndeksler/Toplar**
   - Bridge'ler sürekli olarak Archivist'lere bilgi gönderir ve bu bilgiler merkezi olmayan depolarda bir konum sezgisel veri noktası indeksi ile muhafaza edilir.
4. **Diviner'lar Kullanıcının Sorgusunu Getirir**
   - Diviner'lar, Ethereum akıllı kontratına gönderilen sorguları sorgular ve cevap formülasyon sürecini başlatmaya karar verir
5. **Diviner, Archivist'lerden Veri Toplar**
   - Daha sonra Diviner'lar daha gerekli olan uygun bilgiyi Archivist ağından getirerek sorguyu kabul etmeye karar verir.
6. **Diviner, Cevabı Formülleştirir**
   - Diviner'lar, en iyi Origin Chain Score'u içeren Archivist Network'ten sorgunun En İyi Cevabı'nı seçer
7. **Diviner Blok Önerir**
   - Daha sonra Diviner'lar, cevap içerikleri, sorgu ve Proof of Work aracılığıyla ödenen XYO Token'leri (XYO) içerecek şekilde XYOMainChain'de bloklar önerir. Ağdaki diğer Diviner'lar bloğun içeriğini dijital olarak imzalar ve ardından geçerli blok üzerinde fikir birliğine varıldığında coinbase Diviner'in mevcut hesabı sistem üzerinde Proof of Work'ünü sergilemek için güncellenir.
8. **Diviner, Sorguyu Başlatana Sonucu Gönderir**
   - Diviner'lar, cevabı, cevabın Origin Chain Score'u ve dijital imza setini paketler ve onları, güvenli şekilde XYO akıllı kontrata bağlanan uyarlayıcı bileşene gönderir. Uyarlayıcı, Diviner'in bütünlüğünün riske atılmadığında emin olunmasından sorumludur ve dijital olarak imzalanan cevap setini akıllı kontrata gönderir. Bu, blok oluşturma sürecinden hemen sonra gerçekleşir. Daha sonra coinbase Diviner'a, çabası karşılığında ödeme yapılır.

9. XYO Network Bileşenleri Yaptıkları İş Karşılığında Ödüllendirilir

- Proof of Origin Chain boyunca bileşenlere, sorgunun cevabını getirmeye katılmalara karşılığında ödeme yapılır. Sentinel'ler, Bridge'ler, Archivist'ler ve Diviner'ların hepsi yaptıkları iş karşılığında ödüllendirilir.

Aynı sorgunun birden fazla sorulduğu durumda, belirli bir anda üretilen cevabın, sistemin o anda sunabileceği mevcut sezgisel veri noktasına bağlı olması nedeniyle birden fazla cevap üretilebilir. Blok zincirine cevap gönderilmesi iki adımdan oluşur. Önce sorgunun Best Answer'a karar vermek için analiz yapılmalıdır. Sistem tarafından birden çok cevap üretilirse o zaman düğümler cevapları karşılaştıracak ve daima en iyi cevabı seçecektir. Basit bir sorgu örneği şu şekildedir: "*Geçmişte belli bir zamanda ağ üzerindeki bir düğüm neredeydi?*"

3.4 Tek Doğruluk Kaynağı Olarak Blok Zinciri

Özünde, Diviner'lar basitçe göreceli veriyi mutlak veriye dönüştürür. Bir sorgunun mutlak cevabını XYO Network'te kesinleştirmek için bütün Archivist ağını araştırabilirler. Diviner'lar aynı zamanda XYOMainChain'e bloklar öneren ve ekleyen düğümlerdir ve Proof of Work'leri için ödüllendirilirler. Archivist ağının işlenmemiş verilerin deposu olması ve blok zincirinin de mutlak, işlenmiş verilerin deposu olmasından dolayı ağ, Archivist Network aracılığıyla pahalı hesaplamaya güvenmek yerine gelecek sorguları cevaplamak için XYOMainChain'deki en güncel bilgileri kullanabilir.

XYOMainChain'deki bloklar, Proof of Origin Chain'i ve sorgulara cevap vermek için kullanılan bileşenlerin grafiğini depolandığından dolayı gelecek Diviner'lar, daha düşük bant genişliği kullanımıyla doğru sonuçlar elde etmek için bu mutlak veriyi inceleyebilir. Böylece XYOMainChain, gitgide sistemin en önemli gerçeklik kaynağı haline gelir. Ancak, Sentinel'ler tarafından toplanan sezgisel veri noktası ile ilgili en güncel bilgiyi sağlamak için hala Archivist ağı gerekli olacaktır.

3.5 En İyi Aday Seçmek İçin XYO Network Çerçevesi

Biz *En İyi Cevabı,* Cevap Adayları listesi arasında minimum gerekli kesinlikten daha yüksek kesinliğe sahip ve en yüksek geçerlilik puanını döndüren tek cevap olarak tanımlıyoruz. Geçerlilik puanı, Origin Chain Score'a bağlıdır. Sistem, daha yüksek bir puan elde edilene kadar yüzde 100 olan en yüksek Origin Score'unun ne olduğunu bilir ve daha yüksek bir puan elde edildiğinde yeni yüzde 100 o olur. XYO Network, En İyi Cevaba karar vermek için Best Answer Algorithm'ın seçimine izin verir. Bu, gelecek araştırmalar için alternatif algoritmalara genişleme sağlar.

Veri bir cevaptan kötü veya hatalı olarak değerlendirilmesi nedeniyle çıkarılırsa Archivist'lere döndürülür ve onlar da, merkezi olmayan depolarından o veriyi temizleyebilir.

3.6 Herkese Açık Blok Zincirleri İle İlk Entegrasyon

XYO Network, Ethereum, Bitcoin + RSK, EOS, NEO, Stellar, Cardano ve diğerleri gibi akıllı kontrat yeteneğine sahip herhangi bir herkese açık blok zinciri ile etkileşimde bulunabilen bir soyutlama olacak şekilde tasarlanmıştır. XYO Network ile iletişimde bulunmak için Ethereum'daki kullanıcılar, örneğin,

sorgulamalarını XYO akıllı kontratımıza yapabilir ve XYO Token (ERC20) olarak ödeyebilir. XYO Blok Zincirimizde Diviner'lar olarak adlandırılan düğümler, Ethereum'u bu tür sorgular için sürekli olarak sorgulayacak ve kendi yerli para birimimiz olan XYO Blok Zinciri (aynı zamanda XYO Token olarak da adlandırılır) cinsinden ödüllendirilecektir. Gelecekte, platformlarımıza ölçeklenebilir IoT kullanım senaryoları için gerekli olan mikro ödeme gereksinimlerini destekleyen işlem ücretlerini sağlamak için ERC20 token'lerimizin sahiplerinden blok zincirimizin yerli para birimine bire bir dönüştürme işlemini yapacağız. Bu durumlarda; kullanıcılarımızın, herkese açık akıllı kontrat aracılığıyla etkileşimde bulunmaları yerine sorgulamalarını, doğrudan blok zincirimize yapmalarını sağlayacağız.

---

4 Proof of Origin

Güvenilmeyen düğümlerden oluşan fiziksel bir ağ ile aynı kaynaktan çıkan iki veya daha fazla bilgi parçasının çıktığı sıfır bilgi ispatına bağlı uç düğümden sağlanan verilerin kesinliğine karar vermek mümkündür. Birkaç benzer veri kaynağı ve en az bir düğümün mutlak konum bilgisiyle birleştirilmiş olan bu veri setlerini kullanarak diğer düğümün mutlak konumu belirlenebilir.

4.1 Proof of Origin'in Tanıtımı

Geleneksel güvene ihtiyaç duymayan sistemler, bir sistemde işlemleri veya kontratları imzalamak için özel bir anahtara dayanırlar. Bu, ağ üzerinde söz konusu veriyi imzalayan düğümün fiziksel ve sanal olarak güvenli olduğu varsayımıyla çok iyi çalışır. Ancak, özel anahtar riske atılırsa o zaman kökeni ispatlama yeteneği bocalar.

Güvene ihtiyaç duymayan konseptleri Nesnelerin İnterneti'ne uygularken ağ üzerindeki uç düğümlerin fiziksel olarak veya sanal olarak güvenli olmadığı varsayılmalıdır. Bu, uç düğümleri benzersiz kimlik kullanmadan tanımlama ve ağın dışından herhangi bir bilgi olmadan onlardan alınan verilerin güvenilir ve geçerli olduğuna karar verme ihtiyacına neden olur.

4.2 Proof of Origin'in Özü: Bound Witness'ler

Proof of Origin, *Bound Witness* konseptine dayanır. Dijital bir kontrata (veya bir oracle) karar vermek için güvenilmeyen bir veri kaynağının kullanışlı olmadığı göz önüne alırsak ilk önce çift yönlü konum ispatının mevcudiyetinin oluşturulması kaydıyla verinin kesinliğini önemli derecede artırabiliriz. Birincil çift yönlü konum sezgisel veri noktası, yakınlıktır çünkü her iki taraf da etkileşimi birlikte imzalayarak etkileşiminin oluşumunu ve aralığını doğrulayabilir. Bu, iki düğümün birbirinin yakınında olduğunda dair sıfır bilgi ispatını sağlar.

Daha sonra güvene ihtiyaç duymayan bir sistemdeki bir oracle şahit düğümünün paylaştığı veriyi toplama kesinliğini belirlemeliyiz. Güvene ihtiyaç duymayan bir sistemde bir şahit düğümü, kusurla veya bozuklukla yanlış veri üretebilir. Geçersiz veri, o sezgisel veri noktası için izin verilen aralığın dışına düşerse tespit edilebilir ve basit şekilde çıkarılabilir. Geçerli ancak hatalı verinin (ör. yanlış veri) tespit edilmesi çok daha zordur.

4.3 Tek Yönlü ve Çift Yönlü Konum Sezgisel Veri Noktaları

Fiziksel dünya ile ilgili birçok veri (sezgisel veri noktası), tek yönlüdür. Bu, ölçülen bir elemanın geri ölçememesi manasına gelir ve tek yönlü sezgisel veri noktası verisinin doğrulanmasını çok zor yapar. Çift yönlü sezgisel veri noktası, ölçülen elemanın kendi ölçümünü diğer tarafa bildirebildiği noktadır ve bu, doğrulamayı mümkün kılar. Konum, çift yönlü olabilecek ve içinde iki uç düğümün birbirlerine bildirimde bulunduğu nadir bir sezgisel veri noktasıdır. **Bu durumun bir gerçek dünya örneği, birbirine yakın iki kişinin özçekim yapması, her bir taraf için bir kopya basılması ve sonra her ikisinin de özçekimi imzalamasıdır. Bu işlem, her iki tarafın Proof of Proximity'sini verecektir. Bu iki kişinin bu "veri"yi elde etmesinin tek yolu, aynı konumda beraber olmaları iledir.**

Bundan sonra ağ etkilerini tartışalım: Her uç düğümden etrafta dolanırken sürekli olarak bu özçekimleri üretip onları bir klasörde depolamalarının beklendiğini hayal edin. Ayrıca o klasörü zaman sıralı bir düzende tutmaları beklenmekte ve hiçbirisini silmesine izin verilmemektedir. Bu, her bir uç düğüm için diğer düğüm noktalarının kayıt edicileri ile çapraz referanslandırılabilen bir yakınlık kayıt edicisi oluşturur.

4.4 Uç Olmayan Düğümler

Köprü, röle, depo ve analiz düğümleri dahil tüm düğümler "şahit" olarak kabul edilir. Bu, bir düğümden diğer düğüme aktarılan herhangi bir verinin bağımlı olmasını sağlar. Bu, **Bound Witness** konseptidir.

4.5 Çapraz Referans

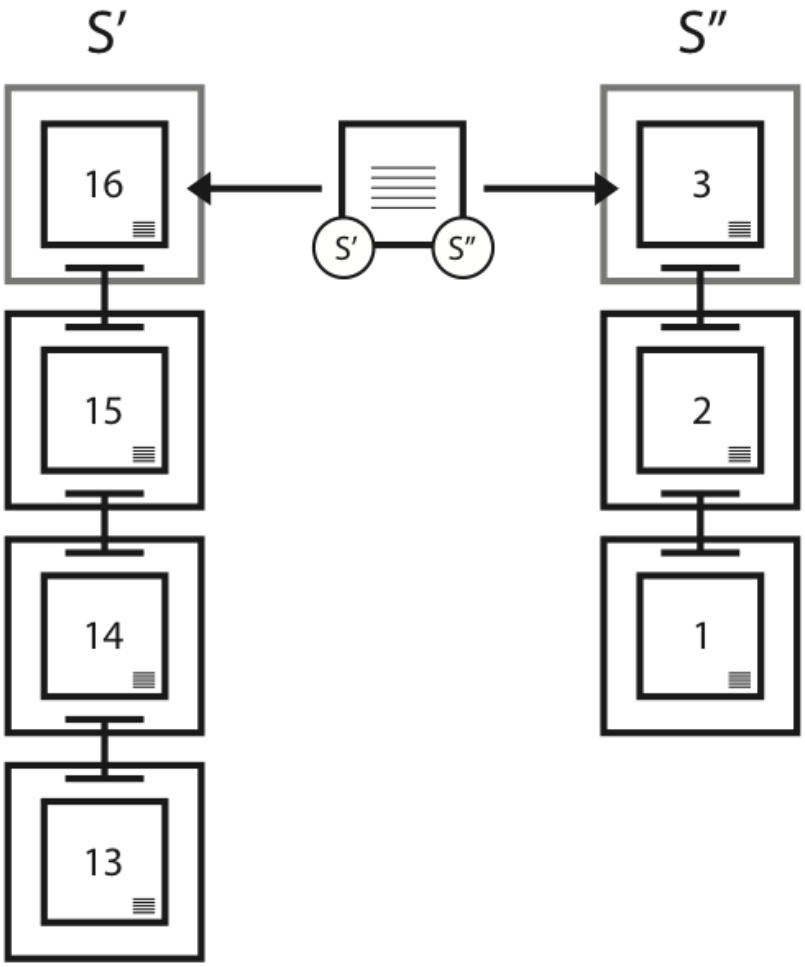
Üretilen her özçekim setinin analiz edilmesi ve her uç düğümü tarafından birlikte zincirlenmesi, sistemin, ağdaki tüm düğümlerin göreceli yakınlığından En İyi Cevabı üretmesini sağlar. Her düğüm güvenli ve doğru şekilde bildirimde bulunursa uç düğümlerin tüm göreceli konumlarının eşleştirilmesi, mümkün olan maksimum kesinliği ve doğruluğu elde edecektir; bu da yüzde 100'dür. Tersine, her düğüm güvenilmez veya kusurluysa kesinlik ve doğruluğun her ikisi de minimum değer olan yüzde 0'a yaklaşacaktır.

Rapor edilen bir veri seti ve uç noktalarından birisinin göreceli konumu için bir sorgu göz önüne alındığında tahmini konum, kesinlik ve doğruluk katsayıları ile üretilebilir.

Aynı veri seti ve aynı analiz algoritması göz önüne alındığında her hesaplama, aynı konum tahmine ve kesinlik ve doğruluk için aynı katsayılara ulaşmalıdır.

4.6 Şema

S′ ve *S″*, (Şekil 1.) sezgisel veri noktasını toplayan Sentinel'lerdir (uç düğüm). Birbirleriyle irtibat kurduklarında sezgisel veri noktası verisini ve açık anahtarları değiş tokuş ederler. Her ikisi de etkileşimin tüm kaydını oluşturur ve ortaya çıkan etkileşimi imzalar. İmzalanan kayıt daha sonra her ikisinin yerel kayıt defterlerine sonraki girdi haline gelir (*S′* için 16 ve *S″* için 3). Bu eylem, birbirlerinin yakınından olmalarından dolayı bu iki şahidi birleştirir.



Şekil 1. İki Sentinel Arasında Şahit Birleştirme Örneği

4.7 Köken Zincirleri

Her köken, kendi kayıt defterini muhafaza eder ve Proof of Origin Chain yapmak için onu imzalar. Proof of Origin Chain üzerindeki bilgi bir kez paylaşıldıktan sonra etkin olarak süreklidir. Bunun nedeni, paylaşmadan sonra meydana gelen çatalın zinciri sonlandırması ve şahitten gelen tüm gelecekteki verilerin sanki yeni bir şahitten geliyor gibi muamele edilmesini sağlamasıdır. Proof of Origin Chain içinde bir bağlantı üretmek için kaynak, açık/özel anahtar çifti üretir. Ardından açık anahtarı her iki bloğa dahil ettikten sonra hem önceki hem de sonraki blokları aynı çiftle imzalar. İmza yapıldıktan hemen sonra özel anahtar silinir. Özel anahtarın anlık olarak silinmesiyle anahtarın çalınma veya tekrar kullanılma riski geniş ölçüde minimize edilir.

Proof of Origin Chain'ler, XYO Network'e akan kayıt defterlerinin geçerli olup olmadığını doğrulamanın anahtarıdır. Veri kaynağı için benzersiz bir kimlik kullanışlı değildir çünkü sahtesi yapılabilir. XYO Network'ün birçok bölümünün fiziksel olarak güvenceye alınmasının zor veya imkansız olması nedeniyle özel anahtar imzalaması kullanışlı değildir ve bu nedenle kötü niyetli bir kişinin özel anahtarı çalma potansiyeli kolaylıkla gerçekleştirilebilir. Bunu çözmek için XYO Network, Transient Key Chain'leri kullanır. Kullanımlarının faydası, veri için köken zincirinin sahtesinin yapılmasının imkansız oluşudur. Ancak zincir bir kez kırıldığında sonsuza kadar kırılır ve devam ettirilemez.

Bir sezgisel veri noktası kayıt defteri, XYO Network'te her aktarıldığında alıcı, Proof of Origin Chain'i daha uzun yapacak ve Proof of Origin Intersection üretecek şekilde kendi Proof of Origin'ini ekler. Proof of Origin Chain'ler ve Proof of Origin Intersection'lar, kayıt defterlerinin geçerliliğini onaylamak için Diviner'lar tarafından kullanılan ana göstergelerdir. Kayı Defteri Ünü'nün denklemi, etkin bir şekilde XYO Network'ün, onunla ilişkilendirilmiş Proof of Origin Ball yapılmasına hangi yüzdeyle katıldığıdır. Teoride, XYO Network kayıtlarının yüzde 100'ü Proof of Origin ile bağlantılıysa ve ardından tamamen analiz edilirse geçerli olma ihtimali yüzde 100'dür. Analiz için XYO Network kayıtlarının yüzde 0'ı mevcutsa o zaman geçerlilik yüzde 0'a düşer.

İlave güvenlik için Chain Link'in açık anahtarı, onun için ikinci giriş mevcut hale getiriline kadar sağlanmaz. Bu aynı zamanda önceki ve sonraki bağlantıda depolanacak girişler veya diğer veriler arasında zaman aralığı sağlar.

4.8 Origin Chain Score

Origin Chain Score, aşağıdaki gibi hesaplanır (varsayılan algoritma):

- PcL = Proof of Origin Chain'in Boyu
- PcD = Proof of Origin Chain'in Zorluğu
- $Pc'\ Pc''\ O$ = Proof of Origin Chain'in Pc' ve Pc'' için Örtüşmesi

$$Score = \prod_{i=0}^{i=n} \frac{PcL * PcD}{Pc'Pc''O} \tag{1}$$

4.9 Origin Tree

Origin Tree, bir cevabın tahminin geçerliliğini hesaplamak için kullanılır. Belirli bir ileri sürülen cevap için o veriye en iyi şekilde uyan ağaç olan Ideal Tree'yi üretmek için toplanan veriyi kullanır. N düğümü, X,Y,Z,T konumunda bulunuyorsa setteki tüm veriler boyunca hata, belli bir değere sahip olmalıdır. Bu hatayı hesaplamak için, MİN, MAKS, ORTALAMA, MEDYAN ve ORTALAMADAN ORTALAMA MESAFEYİ hesaplayacağız.

Tüm puanları s, Proof of Origin Chain'in Zorluğu *PcD* ve hata faktörü *hata* olarak bir S seti göz önüne alındığında BEST ANSWER aşağıda şekilde belirlenir:

$$BestAnswerScore = \max_{\forall s \in S_j} [PcD * (1 - error)] \quad (2)$$

Diğer bir deyişle en yüksek Best Answer Puanı'na sahip ileri sürülen cevap, En İyi Cevap'tır. Proof of Origin Tree kullanarak, budaması imkansız dalları (aykırı değerler) tanımlayabilir ve budayabiliriz.

4.10 Transient Key Chaining

Veri paket serileri, iki ardışık paketi imzalamak için geçici özel anahtarlar kullanarak birbirlerine zincirlenebilir. Özel anahtarla eşleştirilen açık anahtar veri paketlerine dahil edildiğinde alıcı, her iki paketin aynı özel anahtarla imzalanıp imzalanmadığını doğrulayabilir. Paketteki veri, imza bozulmadan değiştirilemez ve böylece imzalanan paketlerin Bridge ve depo düğümü gibi üçüncü bir taraf tarafından değiştirilmemesi garanti edilir.

4.11 Link Depth

Bir düğüm, asgari seviyede, Proof of Origin Chain'deki her bağlantı için Link Depth'i 1 olan yeni genel/özel anahtar çifti üretir. Belirli bir *Kayıt Defteri Girişi* için bağlantı tablosunda N adet giriş olabilir ve her giriş, bağlantının ikinci kısmının gelecekte ekleneceği mesafeyi belirler. Hiçbir iki bağlantı, ikili sayı skalasında aynı büyüklük derecesine sahip olamaz. Örneğin, giriş [1,3,7,12,39]'ye izin verilir ancak [1,3,7,12,15]'ye izin verilmez.

Önceki blok yayınlandığında derinlik 1 bağlantısı oluşturulur, kullanılır ve silinir. Ancak, derinliği 1'den büyük olan bağlantılar, önceki blok imzalanırken kendi çiftini ürettirirler ve sonrasında özel anahtarın silindiği N blok sonrasına kadar ikinci imzalama meydana gelmez. Derinliği 1'den büyük olan bağlantılar, derinliği 1 olan bağlantılardan daima daha az güvenli kabul edilir ancak o güvenlik pahasına performansı iyileştirmek ve veri kaybını azaltmak için kullanılabilirler.

4.12 Sabit Sıra

Kayıt defterlerinin sırasını belirlemede ana unsur, rapor edildikleri sıradır. Bir cihazın Proof of Origin imzalı herhangi bir kayıt defterinin sırasını değiştirmesinin mümkün olmadığı göz önüne alındığında mutlak sıra, tüm kayıt defterlerine toplu olarak bakarak oluşturulabilir.

4.13 Sondan Bir Önceki Yayın

Proof of Origin oluşturmak için ana yöntem, Sentinel'in son bloğu rapor etmeden önce her zaman sondan bir önceki bloğunu rapor etmesi gerçeğine dayalıdır. Bu, bağlantının 12

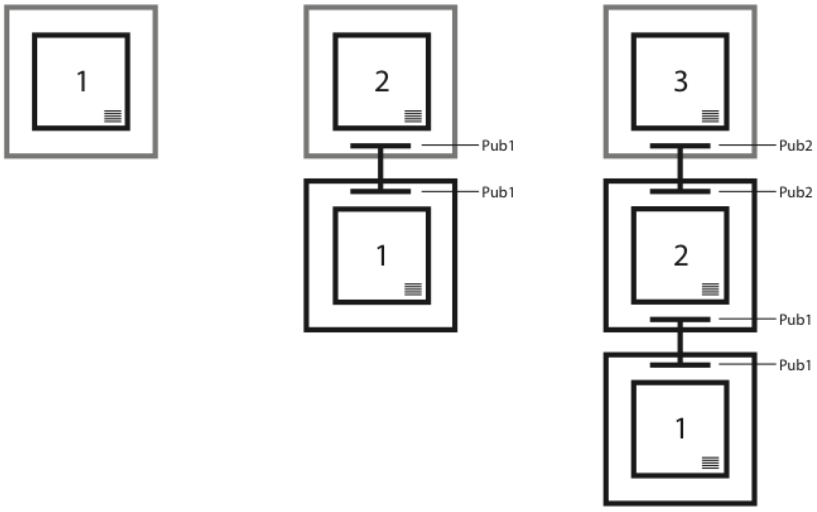
kanıtı olarak son bloğun, önce gelen bloğun imzalı bağlantısına sahip olmasını sağlar.

4.14 Boş Bağlantılar

Proof of Origin Chain'i daha güvenli yapmak için zincirin, her on saniyede birden fazla ve her altmış dakikada birden az güncellenmemesi gereklidir. Hiçbir verisinin mevcut olmadığı durumda boş blok zincire eklenecektir.

4.15 Şema

Zaman, soldan sağa doğru ilerlediğinde (Şekil 2.), oluşturulan Proof of Origin Chain daha uzun olur. Herhangi bir zamanda zincirin üreticisi, onu kullanıma sunmadan önce girişin ikinci imzalanmasını bekleyerek, arayana karartılmış sınırlı girişleri sağlayacaktır. Örneğin, üçüncü sütunda yalnızca girişler 2 ve 1, zincirin bir parçası olarak geri döndürülecektir.



Şekil 2. Proof of Origin Chain'de bağlantı dahil etme örneği

4.16 Özet

Geçici özel anahtarlarla sıralı çiftler olarak imzalanan ve çift açık anahtarları içeren bir dizi veri paketleri verildiğinde paketlerin aynı kökenden geldiği mutlak kesinlikle belirlenebilir.

---

5 Güvenlik Hususları

5.1 Sahte Diviner Saldırısı

Kontratın, cevabı gönderen Diviner'ın doğruluğunu onaylaması için XYO akıllı kontrata bir dijital imza seti gönderilir Daha sonra kontrat, bu listeyi imzalayan diğer Diviner'ları yüksek güven aralığında doğrulayabilir. Bu olmazsa aktarma yapan oracle, sistem içinde tek hata ve risk kaynağı olacaktır.

5.2 Sentinel DDoS Saldırıları

Dikkate alınacak diğer saldırı, özel bir bölgede Sentinel düğümler arasındaki Dağıtık Hizmet Engelleme'dir (DDoS). Saldırgan, Sentinel'lerin Bridge'lere doğru bilgileri veya hiçbir şekilde herhangi bir bilgiyi

aktarmasını engellemek için Sentinel'lere çok sayıda bağlantı kurmaya teşebbüs edebilir. Sentinel'e bağlanmaya teşebbüs eden herhangi birisinin küçük bir kriptografik bulmacayı çözmesini şart koyarak bu sorunun üstesinden gelebiliriz. Bir sorgu, Sentinel'lere çok sayıda bağlantı kurmayı kapsamadığından dolayı bu, XYO röle sisteminde ağır bir yüke neden olmayacaktır ve saldırganın, ağımıza başarılı bir DDoS saldırısı yapabilmesi için çok büyük miktarda kaynak harcamasını gerektirecektir. Zamanda belli bir noktada, XYOMainChain'de depolanması nedeniyle Proof of Origin Chain doğrulanabilir. Bu, zincir boyunca tek bir oluşumda anlaşmaya varılmışsa sorgu cevabının doğruluğunun (Origin Chain Score) o'a d üşmesini sağlar.

---

6 XYO Token Ekonomisi

Oracle'lar, en çok yetkili otoritelerin bağlanabilirlik ve kümelenmesine odaklanan dağıtık uygulamalar için güç ve altyapı ihtiyacının önemli bir bölümünü teşkil ederler. Biz, merkezi olmayan uygulamaların en yüksek potansiyellerine erişebilmeleri için tamamen merkezsiz ve güvene ihtiyaç duymayan oracle sistemi ihtiyaç olduğuna inanıyoruz.

6.1 XYO Network Kripto Ekonomisi

Doğru ve güvenilir konum sezgisel veri noktalarını sağlama istenen davranışını teşvik etmek için XYO Token'leri kullanıyoruz. XYO Token'ler, belirli bir nesnenin XY-koordinatını doğrulamak için gerçek dünya ile arayüz sağlamak amacıyla gerekli olan "benzin" olarak düşünülebilir.

Süreç şu şekilde çalışır: Bir token sahibi, önce bir sorguyla XYO Network'ü sorgular (örn. "0x123456789 XYO adresindeki e-Ticaret sipariş paketim nerede..."). Daha sonra sorgu, sıraya gönderilir ve orada işlenmek ve cevaplandırılmak üzere bekler. Kullanıcı, sorgu oluşturma sırasında istediği güven seviyesini ve XYO benzin fiyatını ayarlayabilir. Sorgunun ücreti (XYO Token cinsinden), sorguya bir cevap vermek için gerekli olan veri miktarının yanı sıra piyasa dinamikleri ile belirlenir. Ne kadar çok veriye ihtiyaç duyulursa sorgu o kadar pahalı ve XYO benzin fiyatı da o kadar yüksek olur. XYO Network'e yapılan sorgular, çok büyük ve pahalı olma potansiyeli taşırlar. Örneğin, bir kamyonculuk ve lojistik firması, "*Filomuzdaki her bir aracın konumu nedir?*" sorusunu sormak için XYO Network'e sorgulama yapabilir.

XYO Token sahibi, XYO Network'ü sorgulayıp gerekli benzin için ödeme yaptığında, görev üzerinde çalışan tüm Diviner'lar, sorguyu cevaplamak için gereken ilgili veriyi çekmek için ilgili Archivist'lere başvurur. Geri döndürülen veri; veriyi aslen Sentinel'lerden toplayan Bridge'ler tarafından elde edilir. Sentinel'ler özünde nesnelerin lokasyonunu doğrulayan cihazlar veya sinyallerdir. Bunlar, Bluetooth takip cihazları, GPS takip cihazları, IoT cihazılarına entegre coğrafi konum izleme, uydu takip teknolojisi, QR-kod tarayıcıları, RFID tarama ve birçok diğer sistemi kapsar. XY Findables, gerçek dünya konum sezgisel veri noktasını işlemesini ve test etmesini sağlayan tüketici Bluetooth ve GPS işine öncülük etti ve bu işi kurdu. XY Findables tüketici işinin geliştirilmesi için yapılan tüm çabalar, XYO Network Blok Zinciri Protokolünün tasarlanmasına önemli oranda yardım etmeyi sağladı.

Bir Sentinel cihazından (Bluetooth İstasyonu gibi) sağlanan veri, sorguyu cevaplandırmak için kullanılırsa o zaman işleme dahil olan tüm dört bileşen, token sahibi

tarafından ödenen XYO benzininin bir kısmını alır: Diviner (cevabı arayan), Archiver (veriyi depolayan), Bridge (veriyi ileten) ve Sentinel (konum verisini kaydeden). XY Network'ün 4 bileşeninden 3'ü arasındaki benzin dağılımı daima aynı oranda verilir. İstisna, cevap verme sürecine katılımı daha kapsamlı olan Diviner'ların oranındadır. Benzin, her bir bileşenin içinde eşit şekilde dağıtılır.

6.2 Bağımsızlık Ödülleri

Konum toplama cihazları, ağın atomik bloklarıdır ve tek bir cihaz, sistemin dört bileşeninden biri veya daha fazlası olarak işlev görebilir.Ancak, özellikle büyük bir XYO Network'te cihazların bu bileşenlerden ikisinden fazlası olması durumu nadirdir. Ayrıca, daha bağımsız Proof of Origin'e sahip olan bir blok zinciri kayıt defteri daha yüksek takdir görecektir, yani çoklu bileşen olarak işlev görencihazlar için kripto ekonomik bir ceza vardır.

6.3 Durağanlık Bütünlüğü Ödülleri

XYO Network içindeki Sentinel'lere, yaşam döngüleriboyunca hareket miktarları için durağanlık katsayısı tahsis edilir. Sentinel, bir zaman diliminde ne kadar az hareket ederse verisine o kadar çok güvenilir. Archivist'ler, hangi Sentinel'lere sorgulara sevk edeceklerini dikkate alırken bu durağanlık katsayıları takip eder ve analiz eder.

6.4 Token Kullanımının Teşvik Edilmesi

Token sahiplerinin, token'lerini *kullanmamaları* yönündeteşvik edilmeleri, temelindeki ekonomi için uzun vadeli bir sorun oluşturur. Bu durum, değerin çok seyrek depolandığı bir ekosistem oluşturur ve faydayı ve likitideyi desteklemek yerine token'i *kullanmamak* için sebepler icat etmek için doğal bir dürtüyü tetikler.

Birçok kripto ekonomi teşvikinin sahip olduğu sorun, odağın aşırı fazla şekilde token madencilerine (örneğin, Sentinel'ler, Bridge'ler, Archivist'ler, Diviner'lar) yönlendirilmesi ve asla token kullanıcılarına yönlendirilmemesidir. XYO Token her ikisini de hesaba katar.

XYO Token modeli, sadece doğru veriyi sağlama konusunda değil aynı zamanda veriyi ne zaman hiçbir şekilde sağlamayacaklarını bilme konusunda da madencileri teşvik eder. Son kullanıcı, ağ likitidesi düşük olduğunda, ağ likitidesinin yüksek olduğu zamana nazaran daha fazla işlem yapmak için teşvik edilir. Bu nedenle, XYO Token ekosistemi; dengeli, akıcı ve sağlam kalma kabiliyetine sahiptir.

6.5 XYO Token'in Özellikleri

Halka açık token satışı, 1 ETH: ve 1 ETH:33,333 XYO'de maksimuma ulaşan bir fiyatlandırma yapısına sahiptir. Hacmimiz ve zamana dayalı fiyatlandırma yapımızla ilgili detaylar kısa bir süre içinde duyurulacaktır.

- Akıllı kontrat platformu: Ethereum
- Kontrat Tipi: ERC20
- Token: XYO
- Token Adı: XYO Network Fayda Tokeni
- Token Adresi: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- Toplam çıkarılma: Sınırlıdır ve Token Ana Satışı'ndan sonra ulaşılan miktarda tamamlanır

- Öngörülen XYO Token Üst Limiti: 48 Milyon $
- Satılmamış ve Tahsis Edilmemiş token'ler: Token satış etkinliğinden sonra yakılır. XYO Ana Satışı bittikten sonra başka XYO Token üretilmeyecektir.

---

7 XYO Network Kullanım Senaryoları

XYO Network'ün kullanımı çok sayıda endüstriyi kapsayan geniş uygulamalara sahiptir. Örneğin, seçkin müşterilerine teslimatta ödeme yapma hizmeti sağlayabilen bir e-Ticaret firmasını ele alın. E- Ticaret firması, bu hizmeti sunabilmek için bir akıllı kontrat yazmak amacıyla (yani Ethereum platformunda) XYO Network'ü (XYO Token kullanan) kullanacaktır. Daha sonra XYONetwork, işin yerine getirilmesi sırasındaki her bir adımda tüketiciye gönderilen paketin konumunu, depo rafından nakliye kuryesine, oradan da tüketicinin evine kadar tüm yol boyunca ve aradaki her konumda izleyebilir. Bu, e-Ticaret bayilerini ve web sitelerini, güvene ihtiyaç duymayacak şekilde paketin yalnızca müşterilerin kapısında değil aynı zamanda güvenli bir şekilde evlerinin içinde olduğunu doğrulamalarını sağlar. Paketin, müşterinin evinde olduğu doğrulandıktan sonra (özel bir XY Koordinatı ile tanımlanıp doğrulanır) sevkıyat, tamamlandı olarak değerlendirilir ve satıcının ödemesi serbest bırakılır. Böylece XYO Network'ün e-Ticaret ile bütünleşmesi, satıcıyı dolandırıcılıktan korumanın yanı sıra müşterilerin de yalnızca evine ulaşan ürün için ödeme yapmasını sağlar.

XYO Network'ün tamamen farklı bir entegrasyonunu, mevcut sorununun değerlendirmelerine çoğu defa güvenilmemesi olan bir otel değerlendirme sitesiyle entegrasyonunu göz önüne alın. Doğal olarak, otel sahipleri, bedeli ne olursa olsun incelemelerini iyileştirmek için teşvik olurlar. Birisinin, San Diego'da olan bir kişinin Bali'ye giderek orada bir otelde iki hafta kaldığını ve sonra San Diego'ya geri dönerek Bali'de kaldıkları otel hakkında değerlendirme yazdığını yüksek kesinlikle söyleyebildiğini farz edelim. Değerlendirme, özellikle onaylı konum verisiyle birçok değerlendirme yazmış olan bir seri eleştirmen tarafından yazılırsa çok yüksek oranda bir üne sahip olacaktır.

---

8 XYO Network'ün Genişlemesi

Dünyada bir milyonun (1.000.000) üzerinde Bluetooth ve GPS cihazıyla başarılı bir şekilde gerçek dünya ağı kuran bir tüketici işine sahip olduğumuz için şanslıyız. Birçok konum ağı, bu aşamaya ulaşamadı ve kapsamlı bir ağ oluşturmak için gerekli kritik kitleyi elde edemedi. Oluşturduğumuz Sentinel ağı sadece bir başlangıç noktasıdır. XYO Network, konum cihazlarının herhangi bir operatörünün bağlanıp XYO Token kazanmaya başlayabileceği açık bir sistemdir.

Genel olarak, XYONetwork'ü içinde Sentinel'in kardinalitesi ne kadar büyükse ağ o kadar güvenilirdir. Ağını daha fazla büyütmek için XYO Network,kendi XY Findables ağının ötesinde Sentinel ağını genişletmek için diğer işletmelerle yakın ilişki kuruyor.

9 Teşekkür

Bu beyaz rapor, aşağıdaki bireylerin vizyonumuza olan inançları sayesinde münkün olan ilham verici bir takım gayretinin bir ürünüdür: Raul Jordan (Harvard Üniversitesi, Thiel Öğretim Üyesi ve XYO Network Danışmanı); beyaz raporun teknik detaylarının dünyaya şık bir şekilde iletilmesi hususunda bize yardımcı olması nedeniyle ve beyaz raporumuzun daha kısa olması konusundaki katkıları için. Christine Sako'ya olağanüstü iş etiği ve çalışmamızın incelemesinde detaylara dikkat etmesi nedeniyle teşekkür ederiz. Beyaz raporumuzda gözlemlenen yapısal tutarlılık ve en iyi uygulamalar, Christine'in gayretlerinin sonucudur. Johnny Kolasinski'ye kullanım durumu uygulamalarını araştırması ve derlemesi için teşekkür ederiz. Son olarak, John Arana'ya dikkatli incelemesi ve yaratıcı girdileri için teşekkür ederiz.

Referanslar

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

[2] Karapetsas, Lefteris. *Sikorka.io*. http://sikorka.io/files/devcon2.pdf. Şangay, 29 Eylül 2016.

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

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

Terimler Sözlüğü

akıllı kontrat Söylendiğine göre 1994'te Bitcoin'den önce Nick Szabo tarafından türetilen bir protokoldür (Bu nedenle bazıları onun Bitcoin'in gizemli ve bilinmeyen mucidi olduğuna inanır). Akıllı kontratların arkasındaki düşünce, bir yasal anlaşmanın bir programa kodlanması ve insanların kontratları yorumlaması ve onlara göre hareket etmesi yerine merkezi olmayan bilgisayarların anlaşmanın koşullarını uygulamasıdır. Akıllı kontratlar parayı (örn. Ether) ve kontratları aynı konseptte birleştirir. Akıllı kontratlar deterministik (bilgisayar programları gibi), tamamen şeffaf ve okunabilir olduklarından dolayı aracıları ve simsarların yerine geçmek için güçlü bir yöntem olarak işlev görürler.

Archivist Archivist, tüm geçmiş kayıt defterlerinin depolanması amacıyla ancak o gereksinim olmadan, merkezi olmayan veri setinin bir parçası olarak sezgisel veri noktalarını depolar. Bazı veriler kaybolsa veya geçici olarak kullanılamaz hale gelse bile sistem yalnızca azaltılmış doğrulukla işlev görmeye devam eder. Archivist'ler ayrıca gerektiği takdirde kayıt defteri veri dizesini döndürebilmeleri için kayıt defterlerini indeksler. Archivist'ler yalnızca ham veriyi depolar ve sadece veri çekme için ödeme alırlar. Depolama her zaman ücretsizdir.

Best Answer Biz, Best Answer'ı, Cevap Adayları listesi arasında minimum gerekli kesinlikten daha yüksek kesinliğe sahip ve en yüksek geçerlilik puanını döndüren tek cevap olarak tanımlıyoruz.

Best Answer Algorithm Diviner, bir cevap seçtiğinde Best Answer Score'ları üretmek için kullanılan bir algoritmadır. XYO Network, özelleştirilmiş algoritmaların eklenmesine izin verir ve müşterinin hangi algoritmayı kullanacağını belirlemesini sağlar. Bu algoritmanın, aynı veri seti ile herhangi bir Diviner üzerinde çalıştırılması durumunda aynı puanla sonuçlanması gereklidir.

Bound Witness Bound Witness, çift yönlü sezgisel veri noktasının mevcudiyeti ile elde edilen bir konsepttir. Dijital bir kontrata karar vermek için güvenilmeyen bir veri kaynağının (bir oracle) kullanışlı olmadığı gözönüne alınırsa bu tür bir sezgisel veri noktasının oluşturulmasıyla sağlanan verilerin kesinliğini önemli derecede artırabiliriz. Birincil çift yönlü konum sezgisel veri noktası yakınlıktır çünkü her iki taraf da etkileşimi birlikte imzalayarak etkileşiminin oluşumunu ve aralığını doğrulayabilir. Bu, iki düğümün birbirinin yakınında olduğuna dair sıfır bilgi ispatını sağlar.

Bridge Bridge, bir sezgisel veri noktası kopya edicisidir. Sezgisel veri noktası kayıt defterlerini güvenli şekilde Sentinel'lerden Diviner'lara aktarırlar. Bridge'in en önemli özelliği; Diviner'in, Bridge'den alınan sezgisel veri noktası kayıt defterlerinin herhangi bir şekilde değiştirilmediğinden emin olabilmesinin sağlanmasıdır. Bridge'in ikinci en önemli özelliği ise ilave Proof of Origin metaverisi eklemeleridir.

Diviner XYO Network tarafından depolanan geçmiş verileri analiz ederek belirli bir soruya cevap verirler. XYO Network'te depolanan sezgisel veri noktaları, sezgisel veri noktasının geçerliliğini ve doğruluğunu değerlendirmek için yüksek düzeyde Proof of Location'a sahip olmalıdır. Diviner, şahiti Proof of Origin'ini baz alarak

değerlendirerek bir cevap elde eder ve sağlar. XYO Network'ün güvene ihtiyaç duymayan bir sistem olduğu göz önüne alındığında Diviner'lar, sezgisel veri noktalarının güvenilir analizini sağlayacak şekilde teşvik edilmelidir. Sentinel'lerden ve Bridge'lerden farklı olarak Diviner'lar, blok zincirine cevap eklemek için Proof of Work kullanır.

doğruluk Bir veri noktasının veya sezgisel veri noktasının belirli bir hata payı içerisindeki güven ölçüsüdür.

güvene ihtiyaç duymama Bir sistemdeki tüm tarafların, kurallara uygun gerçeğin ne olduğu üzerinde fikir birliğine varmalarıdır. Güç ve güven, tek bir birey veya kuruluşta (ör. bankalar, hükümetler veya finansal kurumlar) toplanmak yerine, ağın paydaşları (ör. geliştiriciler, madenciler ve tüketiciler) arasında dağıtılır (veya paylaşılır). Bu, kolaylıkla yanlış anlaşılabilecek yaygın bir terimdir. Blok zincirleri aslında güveni ortadan kaldırmaz. Yaptıkları iş, bir sistemde tek bir aktör tarafından gereken güven miktarını azaltmaktadır. Bunu; aktörleri, protokol tarafından belirlenen kurallarla işbirliği yapacak şekilde teşvik eden bir ekonomik oyun aracılığıyla güveni, sistemdeki farklı aktörler arasında dağıtarak yapar.

kesinlik Bir veri noktasının veya sezgisel veri noktasının bozulmama veya tahrif edilmeme ihtimalinin bir ölçüsüdür.

kripto lokasyon Kriptografik konum teknolojisinin alanıdır.

kripto ekonomi Malların ve hizmetlerin üretimini, dağıtımını ve tüketimini merkezi olmayan dijital bir ekonomide yöneten protokolleri çalışan bir resmi disiplindir. Kripto ekonomi, bu protokollerin tasarımı ve nitelendirilmesine odaklanan bir pratik bilimdir.

oracle Doğruluk ve kesinliğe sahip bir cevap sağlayarak dijital kontratın karara bağlanmasından sorulmlu olan MOU(merkezi olmayan uygulama) sisteminin bir parçasıdır. "Oracle" terimi, kriptografiden gelir ve orada tamamen rastgele bir kaynağı belirtir (ör. bir rastgele sayı). Bu, kripto denkleminden ötesindeki dünyaya gerekli olan kapıyı sağlar. Oracle'lar, zincirin ötesinden (gerçek dünya veya zincir dışı) akıllı kontrat bilgilerini besler. Oracle'lar dijital dünyadan gerçek dünyaya arayüzlerdir. Marazi bir örnek olarak, Son Arzu ve Vasiyet için yapılan bir kontratı ele alın. Arzu'ların koşulları, vasiyet sahibinin vefat ettiğinin onaylanması üzerine gerçekleştirilir. Bir oracle servisi, resmi kaynaklardan ilgili verileri derleyerek ve toplayarak bir Arzu'yu başlatmak için oluşturulabilir. Oracle bu noktada kişinin vefat edip etmediğini kontrol etmek için akıllı kontratın başvuracağı bir besleme veya son nokta olarak kullanılabilir.

Origin Chain Score Güvenilirliğine karar vermek için Origin Chain tarafından atanan puandır. Bu değerlendirme, boyu, karışıklığı, çakışmayı ve yedekliliği göz önüne alır.

Origin Tree Belirli bir kesinlik seviyesiyle sezgisel veri noktası kayıt defteri girişinin kökenini oluşturmak için çeşitli Origin Chain'lerden alınan kayıt defteri girişlerinin veri setidir.

Proof of Origin Proof of Origin, XYO Network'üne akan kayıt defterlerinin geçerli olup olmadığını doğrulamanın anahtarıdır. Sahtesi yapılabileceğinden dolayı veri kaynağı için benzersiz bir kimlik kullanışlı değildir. XYO Network'ün birçok

bölümünün fiziksel olarak güvenceye alınmasının zor veya imkansız olması nedeniyle özel anahtar imzalaması kullanışlı değildir ve bu nedenle kötü niyetli bir kişinin özel anahtarı çalma potansiyeli fazlasıyla mümkündür. Bunu çözmek için XYO Network, Transient Key Chaining'i kullanır. Bunun faydası, veri için köken zincirinin sahtesinin yapılmasının imkansız oluşudur. Ancak zincir kir kez kırıldığında sonsuza kadar kırılır ve devam ettirilemez.

Proof of Origin Chain Bir dizi Bound Witness sezgisel veri noktası kayıt defteri girişlerini birbirine bağlayan bir Transient Key Chain'dir.

Proof of Work Proof of Work, belirli gereksinimleri sağlayan bir parça veridir; üretmesi zot (yani maliyetli, zaman alıcı) ancak diğerlerinin doğrulaması için basit. Proof of Work üretilmesi, düşük üretme ihtimaliyle rastgele bir süreç olabilir ve bu nedenle, geçerli bir Proof of Work oluşturulmadan önce ortalama olarak titiz deneme ve yanılma gereklidir.

Sentinel Sentinel, bir sezgisel veri noktası şahididir. Sezgisel veri noktalarını gözlemlerler ve geçici kayıt defterleri üreterek sezgisel veri noktalarının doğruluğunu ve kesinliğini teyit ederler. Sentinel'in en önemli özelliği, kayıt deftelerine Proof of Origin ekleyerek Diviner'ların aynı kaynaktan geldiğinden emin olabilmerini sağlayacak şekilde kayıt defterleri üretmeleridir.

sezgisel veri noktası Sentinel'in konumuna göre gerçek dünya ile ilgili bir veri noktasıdır (yakınlık, sıcaklık, ışık, hareket, vb.).

Transient Key Chain Transient Key Chain, Transient Key Cryptography kullanarak bir dizi veri paketini birbirine bağlar.

XY Oracle Network XYO Network.

XYO Network XYO Network, “XY Oracle Network”ü temsil eder. Sentinel'leri, Bridge'leri, Archivist'leri, Diviner'ları kapsayan XYO özellikli bileşen/düğümlerin sistem bütününden oluşur. XYO Network'ün ana işlevi, gerçek dünya coğrafik konum onaylamaları aracılığıyla dijital akıllı kontratların uygulanabileceği bir portal olarak işlev görmesidir.

XYOMainChain Diviner'lar ve onların ilişkili köken puanından toplanan veriyle birlikte sorgu işlemlerini depolayan XYO Network'te değişmez bir blok zinciridir.