Hydro Raindrop

Blok Zincirinde Kamusal Kimlik Doğrulama

Ocak 2018

İngilizceden çeviren: M. Talha Altınkaya

Özet

HYDRO: Etimolojisi Antik Yunandaki ὑδρο- (hudro-)'dan ve ὕδωρ (húdōr , "water")'dan gelmektedir.

Hydro yeni ve mevcut özel [private] sistemlerin, uygulama ve belge güvenliğini, kimlik yönetimini, işlemleri/hareketleri ve yapay zekâyı geliştirmek için kamusal bir blok zincirinin değişmez ve şeffaf dinamiklerini kullanarak kusursuz şekilde bir entegrasyona ve bunlardan yararlanılmasına olanak verir.

Bu çalışmada, API'lar (Uygulama Program Arabirimi) gibi özel sistemler için, kamusal kimlik doğrulama yoluyla güvenliği artırmak için Hydro Kamusal Blok Zincirinin kullanılmasına yönelik bir durum ortaya konulacaktır.

Önerilen bu teknoloji "Raindrop" olarak adlandırılır – ve bu özel sistemde işlemler erişimini herkese açık bir şekilde onaylayan ve hali hazırdaki kimlik doğrulama yöntemlerini tamamlayıcı/bütünleyici bir akıllı sözleşme aracılığıyla gerçekleştirilir. Bu teknoloji saldırı ve ihlallerden dolayı giderek daha fazla risk taşıyan hassas finansal veriler için ek güvenlik sağlamayı amaçlamaktadır.

Hydro Raindrop'un ilk uygulaması Hidrojen API Platformu üzerinde gerçekleştirilir. Bu modüler API'ler gelişmiş finansal teknoloji platformlarını ve ürünlerini prototip hale getirmek, inşa etmek, test etmek ve dağıtmak için küresel olarak işletmeler ve geliştiriciler için kullanılabilir.

Bu anlamda Hydro Raindrop geliştiricilerin Hydro Raindrop'u herhangi bir REST API ile entegre etmelerini sağlamak için açık kaynaklı bir yazılım olarak dünya geliştirici topluluğuna sunulacaktır.

Blok Zinciri & Ethereum

Hydro Ethereum ağı üzerinden çalışır. Proje hakkında daha fazla ayrıntı vermeden önce, Blok Zinciri ve Ethereum hakkında bazı temel fikirleri anlamak önem arz eder.

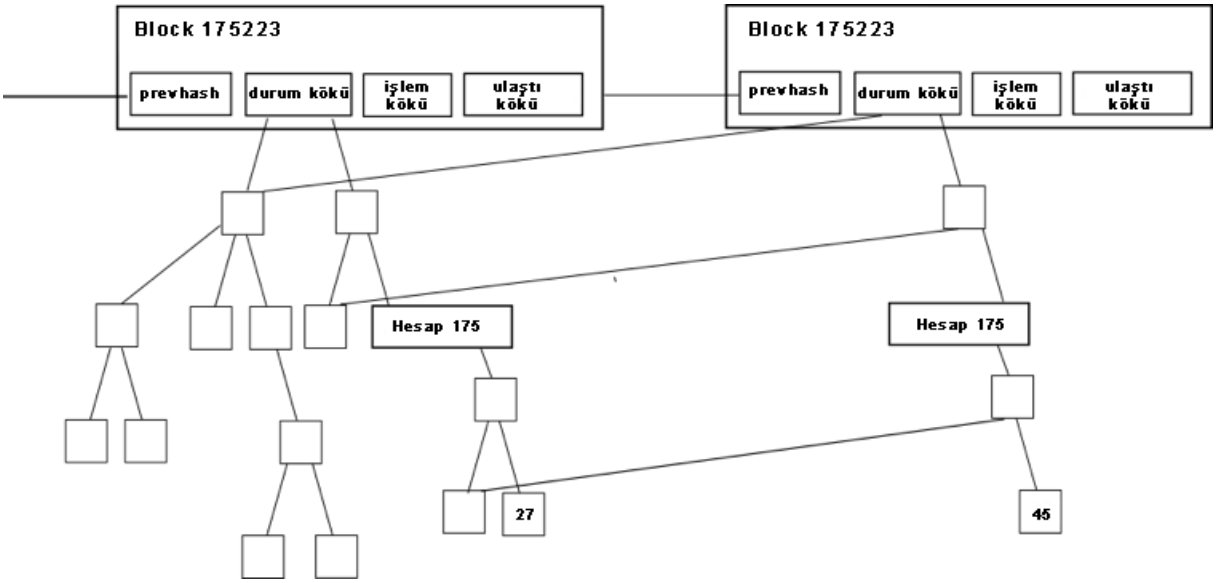
Ethereum Üzerine İnşa Etmek

Nasıl ki Snapchat gibi uygulamalar Swift ve Apple iOS platformu üzerinde sunulan diğer araçlarla oluşturulduysa, Blok Zinciri uygulamaları da Ethereum ağı üzerine inşa edilebilir. Snap şirketi'nin yeni bir iOS oluşturması gerekmiyordu. Şirket iOS'u yenilikçi bir sosyal medya uygulamasını piyasaya sürmek için alt yapı olarak kullandı.

Hydro Projesi de Snapchat örneğine benzerdir. Hydro, temelde Blok Zinciri teknolojisini daha hızlı, daha güçlü hale getirmek için çalışan dünya çapındaki binlerce geliştiriciye dayanır. Hydro sürekli gelişen bu altyapıyı, finansal hizmet uygulamalarına [application] somut faydalar sağlayabilecek Blok Zinciri teknolojisi etrafında ürün odaklı etkileşimler geliştirerek güçlendirir.

Merkle Ağaçları

Merkle ağaçları etkili bir veri doğrulama için dağılmış sistemlerde kullanılır. Onlar tüm dosyalar yerine hash'leri kullandığı için etkilidir. Hash'ler asıl dosyanın kendisinden çok daha küçük olan dosyaları kodlamanın yollarıdır. Ethereum ağındaki her bir blok başlığı İşlemler, Okundu/Alındı Bilgisi [Receipts] ve Durumlar [States] için üç Merkle Ağacı içerir:



Kaynak: Ethereum'da Merkling; Vitalik Buterin, Ethereum Kurucusu

Bu, bir hafif istemcinin [light client] sorgulamalarına karşı doğrulanabilir cevaplar almasını kolaylaştırır, örneğin:

- Bu hesap var mı?
- Mevcut bakiye nedir?
- Bu işlem belirli bir bloğa dahil edilmiş mi?
- Bugün bu adreste belirli bir olay oldu mu?

Akıllı Sözleşmeler

Ethereum ve diğer Blok Zinciri tabanlı ağlar tarafından devreye sokulmuş bir diğer anahtar kavram akıllı sözleşmelerdir. Akıllı sözleşmeler birçok tarafın/şahsın etkileşimde bulunabileceği, güvenilir aracılara duyulan ihtiyacı ortadan kaldıran, kendi kendini uygulayan kod bloklarıdır. Akıllı bir sözleşmedeki kod, geleneksel bir kâğıt sözleşmedeki yasal hükümlere benzer şekilde görülebilir fakat aynı zamanda daha geniş kapsamlı işlevselliklere de ulaşabilir. Sözleşmeler kurallara, koşullara, karşı gelme/uymamaya yönelik cezalara sahip olabilir ya da diğer işlemleri harekete geçirebilir. Sözleşmeler başlatıldığında kamu zinciri [public chain] üzerinde dağıtım sırasındaki başlangıçta belirtildiği gibi, değişmezlik ve merkeziyetsizliğin [decentralization] yerleşik [built-in] unsurlarını sunarak yürütülür.

Akıllı sözleşme, Ethereum altyapısı üzerinde bir şeyi temellendirmek için hayati bir araçtır. Hydro blok zinciri katmanının esas işlevselliği bu belgede daha sonra ele alınacağı gibi, özel sözleşmeler yoluyla elde edilir.

Ethereum Sanal Makinesi

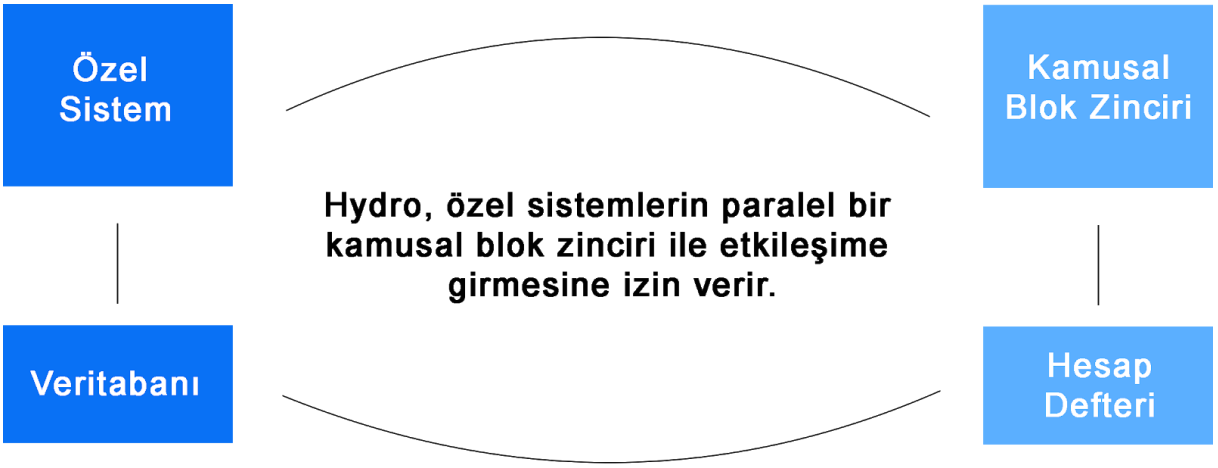
Ethereum Sanal Makinesi (ESM), Ethereum'daki akıllı sözleşmeler için bir çalıştırma ortamıdır. ESM, hizmeti engelleme saldırılarını (DoS) önlemeye yardımcı olur, programların durumbilgisiz [stateless] kalmasını ve kesintisiz iletişimi sağlar. ESM üzerindeki hareketler gerekli olan hesaplama kaynaklarına bağlı bir şekilde, gaz[gas] olarak adlandırılan maliyetlerle ilişkilidir. Her işlem bir gaz limiti olarak bilinen, kendisine paylaştırılan maksimum miktarda gaza sahiptir. Eğer bir işlem tarafından tüketilen gaz limite ulaşırsa, işleme devam etmeyecektir.

Kamusal Muhasebe Defteri

Özel Sistemler İçin Kamusal Bir Muhasebe Defteri

Finansal hizmet platformlarına, web sitelerine ve uygulamalarına güç sağlayan sistemler genellikle veri akışının araçları olarak tanımlanabilir. Bu verilerin niteliği ve daha genel olarak finansal hizmetler nedeniyle bu sistemler genellikle karmaşık işlemleri gizli ve merkezi bir şekilde barındırır. Özel yapılara duyulan güven, sırayla, iç sistemin erişimini aşan dış güçleri birleştirerek çeşitli güvenlik, şeffaflık ve verimlilik kazanımları için kapıyı açar.

Hydrogen'in API platformunda da durum böyledir. Hydro, Hydrogen kullanıcılarının öncelikle özel Hydrogen ekosistemine sorunsuzca entegre edilmiş bir şekilde bir blok zincir ile arayüz oluşturmasına izin vererek, yukarıda belirtilen kazanımlara ulaşmalarını amaçlamaktadır.

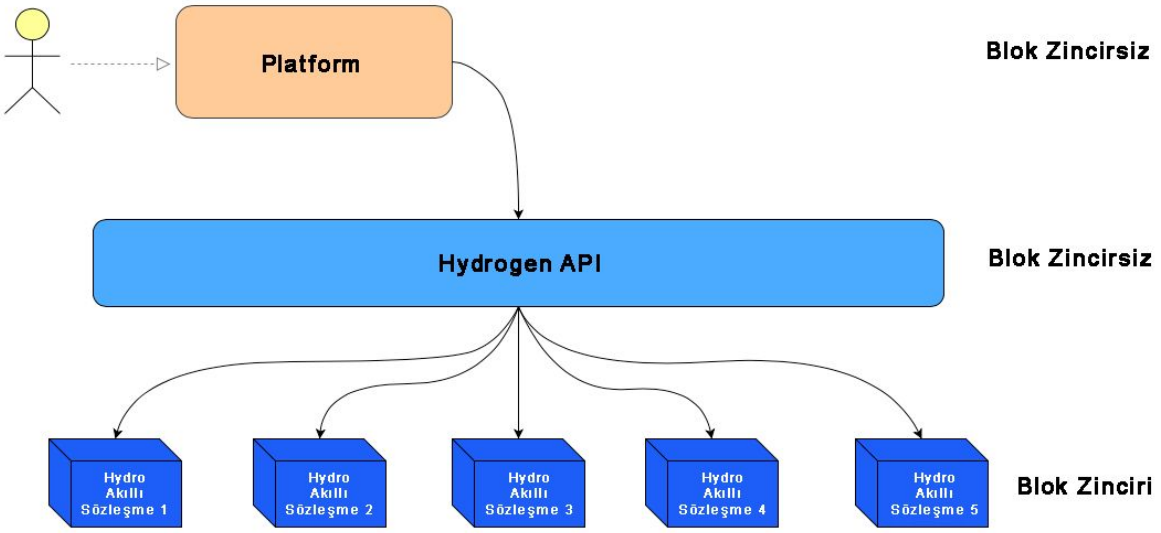


Kamusal blok zinciri tabanlı işlemler, özel işlemlerden önce, özel işlemler sırasında ya da sonrasında meydana gelebilir. Özel ve Kamusal unsurlar arasındaki etkileşim bir ekosistem içindeki süreçleri onaylamak, damgalamak, kaydetmek veya geliştirmek için hizmet edebilir.

Bu modelin ethosu, özellikle en olumlu etkiyi üretebileceği blok zinciri teknolojisinin faydalarını kullanarak işlemleri daha sağlam hale getirmektir. Bu melez yapı tüm platformlar için geçerli olmayabilir ancak Hydro, içinde bulunduğu durumlara değer sağlamaya odaklanır.

Mimarinin Benimsenmesi

Hydro hali hazırda bulunan birçok blok zinciri girişiminden farklıdır çünkü bağımsız olarak var olabilir ve dizgisel [systemic] değişim gerektirmeden yeni veya mevcut sistemlerin etrafında katman oluşturabilir. Hydro değiştirmek yerine arttırmayı hedefler. Hydrogen API'lerine bağlanan platformlar ve kurumlar blok zincirine otomatik olarak erişebilir.



Finansal hizmet platformlarının kapsamı Hydrogen'in genişliğini [broad] geliştirebilir. Bu platformlar aslında herhangi bir deneyime güç sağlayabilir, herhangi bir özel hizmete ev sahipliği yapabilir, herhangi bir özel veri işlemini gerçekleştirebilir ve herhangi bir ortamda kullanılabilir. Bu, Hydrogen'in yapısal modülerliği ile sağlanır ve mimarinin tamamlayıcı bir etmeni olarak hareket eden Hydro ile sinerjiktir.

Raindrop

Raindrop, Hydro Kamusal Hesap Defteri üzerine inşa edilen ve "Yağmur Damlası" [Raindrop] olarak adlandırılan blok zinciri tabanlı bir kimlik doğrulama servisidir. Bu servis erişim isteğinin yetkili bir kaynaktan geldiğini doğrulayan, belirgin, değişmeyen, küresel olarak görüntülenebilir bir güvenlik katmanı sunar.

Açık Yetkilendirme [OAuth] 2.0 gibi özel kimlik doğrulama protokolleri, var olan kullanım durumları spektrumu için çeşitli seviyelerde sağlamlık ve kullanışlılık sunar. Bu protokollerle rekabet etmek veya bu protokolleri değiştirmeye çalışmak için çok az şey gerekir ki Hydro da buraya kimlik doğrulama prosedürünün bir bileşeni olarak blok zinciri mekaniğini dahil ederek doğrulama protokollerini geliştirmenin bir yolunu sunar. Bu yol, sistem ihlallerini ve verilerin bozulmalarını önlemeye yardımcı olacak kullanışlı bir güvenlik katmanı ekleyebilir.

Raindrop'un teknik yönlerini incelemeden önce, çözmeye çalıştığı soruna bir göz atalım.

Finansal Güvenliğin Durumu

Veri çağının yükselişi zafiyet konusunda da bir artışa sebep oldu ve bu konu finansal hizmetler için özellikle önemlidir. Finansal platformlar genellikle devlet kimlik numaraları, hesap bilgileri ve işlem geçmişleri gibi büyük miktarlarda özel ve hassas verilere ağ geçitliği/aracılık yaparlar. Bu veriler ciddi derecede öneme sahip olduğundan, onlara kanunsuz erişim genellikle felaketle sonuçlanır.

Endüstri araştırma şirketi Trend Micro, doğrudan Kişisel Kimlik Bilgileri'nin (PII) çalındığını ve ilgili kalemlerin Deep Web'de 1$ gibi düşük bir fiyata, pasaportlar gibi belgelerin görüntülerinin 10$ gibi bir fiyata, banka giriş kimlik bilgilerinin ise 200$ gibi bir fiyata satıldığı ve çalınan verilerin dağılımının giderek parçalara ayrıldığı ve takip edilemez hale geldiği ile ilgili bir rapor yayınladı.

Ne yazık ki, mevcut finansal sistemin ve paydaşlarının veri ihlallerini önleme, teşhis etme ve iletme konusunda tertemiz bir sicili bulunmamaktadır.

- Javelin Strategy & Research tarafından "2017 yılı Kimlik Dolandırıcılığı" üzerine yapılmış olan yakın tarihli bir araştırmaya göre, finansal sistemin Kişisel Kimlik Bilgilerini (PII) korumadaki

güvenliğe yönelik başarısızlığı nedeniyle 2016 yılında ABD'li 15.4 milyon tüketiciden 16 milyar dolar çalındı.

- Nisan 2017'de Symantec firması, 2016 yılı boyunca çeşitli kapasitelerdeki 1,1 milyar adet Kişisel Kimlik Bilgisinin (PII) risk altında olduğunu tahmin eden İnternet Güvenliği Tehdit Raporu'nu yayınladı.
- Riske Dayalı Güvenlik tarafından 2016 Yıl Sonu Veri İhlali İncelemesi, 2016 yılında dünya genelinde 4,149 veri ihlali meydana geldiğini ve 4,2 milyardan fazla ihlal rekorunun ortaya çıktığını tespit etti.
- Profesyonel hizmetlerde çalışan küresel bilişim teknolojisi (IT) uzmanları tarafından yapılan bir anket olan 2017 Thales Veri Tehdit Raporu -Finansal Hizmetler Baskısı-, finansal hizmet kuruluşlarının %49'unun geçmişte bir güvenlik ihlali geçirdiğini, %78'inin kendilerini korumak için daha fazla harcama yaptığını, ancak %73'ünün uygun güvenlik çözümlerini hazırlamadan önce (Yapay Zeka) AI, (Nesnelerin İnterneti) IoT ve bulut teknolojileriyle ilgili yeni girişimler başlattığını tespit etti.

Equifax İhlali

29 Temmuz 2017'de, 118 yıllık bir ABD kredi raporlama kuruluşu olan Equifax heklendi. Sosyal Güvenlik Numaraları da dahil olmak üzere 143 milyon tüketicinin Kişisel Kimlik Bilgisi açığa çıktı. 209,000 müşterinin kredi kartı verileri tehlikeye atıldı.

Bu ihlalin nedeni neydi?

Saldırı Equifax tarafından kullanılan sunucu uygulama teknolojilerinin biriyle başladı. Strust, Apache Software Foundation tarafından oluşturulan, Java programlama dilinde web uygulamaları geliştirmek için açık kaynaklı bir sistemdir. CVE-2017-9805, XML yüklerini işlemek için XStream işleyicisiyle Struts REST eklentisinin kullanılmasıyla ilgili Apache Struts'taki bir güvenlik açığıdır. Uzaktan kimliği doğrulanmamış bir saldırganın [hacker] eğer isterse, makineyi ele geçirmek veya daha fazla saldırı başlatmak için uygulama sunucusunda kötü amaçlı kod çalıştırmasına izin verir. Bu durum Equifax ihlalinden iki ay önce Apache tarafından düzeltildi [patched].

Apache Struts, REST Eklentisi XStream'de, programın XML taleplerinde kullanıcı tarafından sağlanan girişi güvenli bir şekilde seriden paralele çevirmeden tetiklediği bir hatayı içerir. Daha spesifik olarak, sorun XStreamHandler'in toObject () yönteminde gerçekleşir çünkü XStream seriden

paralele çevirme işleminin bir nesnedeki kullanımına yönelik herhangi bir kısıtlama getirmez ve bu da rastgele kod yürütme güvenlik açıklarına neden olur.

Bu REST eklentisi tehlikeye atılmış olsa bile bunun bir önemi var mıdır? Hala yerleşik REST API ve Java tabanlı sistemlere bel bağlayan bu 143 milyon müşterinin finansal bilgilerini güvence altına almak için blok zinciri teknolojisini kullanmanın bir yolu var mıdır?

Bir Blok Zinciri Katmanı Eklemek

Finansal veri ağ geçitlerinin bütünlüğünün geliştirilebileceği açıktır. Şimdi, Hydro ile ek bir güvenlik katmanının nasıl elde edileceğini inceleyelim.

Ethereum ağının temel mutabakat mekanizmaları işlemin geçerliliğini sağlar çünkü katılımcılar uygun bir şekilde imzalanmış işlemleri topluca işlerler. Bu gerçeklik, merkeziyetsizliğe ve değişmezliğe yol açar fakat daha da önemlisi, hassas verileri işleyen bir ağ geçidine yetkisiz erişimi azaltmak için bir vektör sağlar.

Hydro ile birlikte, kimlik doğrulama blok zincirindeki işlem hareketleri üzerine dayandırılabilir. Örneğin bir API, blok zincirindeki belli adresler arasında standart bir kimlik doğrulama protokolünü başlatan bir önkoşul olarak belirli veri taşıma kapasitesiyle, belirli işlemleri başlatmayı zorunlu kılarak geliştiricileri ve uygulamaları doğrulamayı seçebilir.

Hydro Raindrop

Yağmur, 0.0001 ile 0.005 santimetre çap aralığında yoğunlaştırılmış su paketlerini içerir. Tipik bir yağmur fırtınasında her biri rastgele büyüklükte, hızda ve şekilde olan milyarlarca su paketi vardır. Bu nedenle kimse yağmurun gerçek doğasını eksiksiz bir biçimde tahmin edemez. Benzer şekilde, her Hydro kimlik doğrulama işlemi benzersizdir ve tesadüfen gerçekleşmesi neredeyse imkansızdır ki biz bu yüzden onlara Raindrop diyoruz.

Finansal hizmet platformları, müşteri hesaplarını doğrulamak için genellikle mikro depozit doğrulama kullanır. Konsept gayet basittir: platform, kullanıcının talep ettiği banka hesaplarına küçük depozitolar şeklinde rastgele miktarlarda para yatırır. Kullanıcının gerçekten sahip olduğu hesabı kanıtlaması için -erkek ya da kadın- depozito miktarını platforma geri gönderme gerekir ki daha sonra onaylanır. Kullanıcının geçerli tutarları

(tahmin etmenin yanı sıra) bilmesinin tek yolu, söz konusu banka hesaplarına ulaşmaktır.

Hydro ile Raindrop tabanlı doğrulama da yukarıdaki örneğe benzerdir. Kullanıcıya bir miktar göndermek ve geri gönderilmek yerine bir işlem tanımlanır ve kullanıcının bu işlemi bilinen bir cüzdandan yürütmesi gerekir. Kullanıcının geçerli bir işlem yapabilmesinin tek yolu, söz konusu cüzdana erişmektir.

Raindrop kullanılarak hem sistem hem de erişimci, değişmez bir kamu defterinde yetkilendirme girişimlerini izleyebilir. Bu blok zinciri tabanlı işlem, temel sistem işlemlerinden ayrıştırılır, dağıtılmış bir ağ üzerinde gerçekleşir ve özel anahtarların [private key] mülkiyetine bağlıdır. Bu nedenle, faydalı bir doğrulama vektörü olarak hizmet eder.

Detaylı Bir Bakış

Hydro kimlik doğrulama sürecinde yer alan dört eleman vardır:

1. Erişimci - Bir sisteme erişmeye çalışan taraf. Hydrogen örneğinde erişimci, kendi temel dijital altyapısı için Hydrogen API'lerini kullanan bir finansal kurum ya da uygulamadır.
2. Sistem - Erişimci tarafından erişilen sistem veya ağ geçidi. Hydrogen için, sistem Hydrogen API'sidir.
3. Hydro – Blok zinciri ile iletişim kurmak ve arayüz oluşturmak için Sistem tarafından kullanılan modül.
4. Blok Zinciri – HYDRO işlemlerini işleyen ve bilginin yürütülüp desteklenebileceği ya da başka bir şekilde işletilebileceği Hydro akıllı sözleşmelerini içeren, dağıtılmış kamusal muhasebe defteri.

Her Raindrop bütünüyle, beş işlemsel parametre kümesidir:

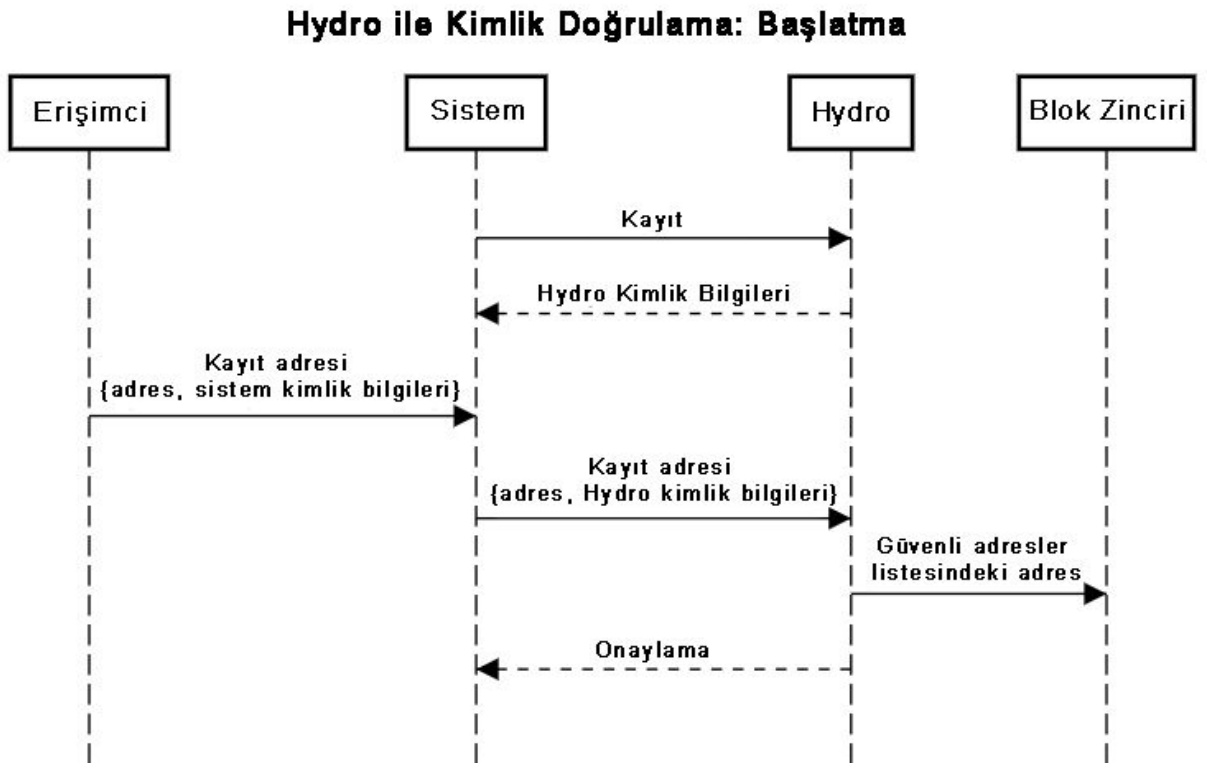
1. Gönderen - İşlemi başlatması gereken adres.
2. Alıcı - İşlemin hedefi. Bu, bir Hydro akıllı sözleşmesinde bir yöntemin çağrılmasına karşılık gelir.
3. Kimlik [ID] - Sistem ile ilişkilendirilmiş bir tanımlayıcı.
4. Miktar – Gönderilecek kesin bir HYDRO sayısı.
5. Görev - Rastgele oluşturulmuş bir alfasayısal dizge.

Aşağıda genellikle üç aşamada sınıflandırılabilen kimlik doğrulama sürecinin bir taslağı bulunmaktadır:

1. Başlatma

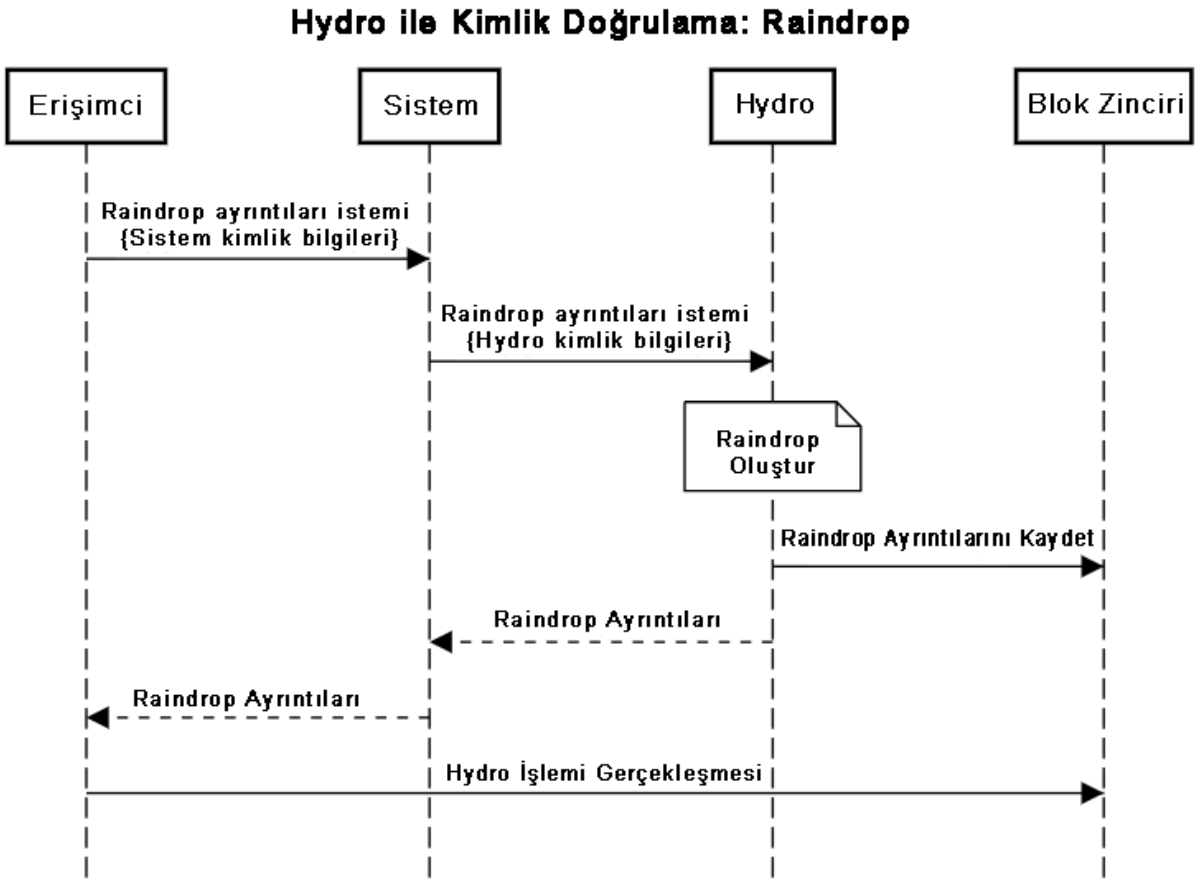
2. Raindrop
3. Doğrulama

Başlatma, Hydro'nun kullanılması ve kimlik bilgilerinin elde edilmesi için bir sistem (örn., Hyrogen) tesciliyle başlar ve sistemin Hydro-modül yoluyla blok zinciri ile iletişim kurmasını sağlar. Sistem, genel bir adresi kaydeden ve daha sonra kayıtlı adresi Hydro'ya geçiren bir erişimci (örneğin bir finans kurumu) içerir. Bu adres, blok zinciri üzerinde Hydro akıllı sözleşmesinde saklanan bir güvenli adresler listesine değişmez şekilde yazılır. Sistem, adresin güvenli adresler listesinde bulunduğunu ve bunun da kamusal bir şekilde görüntülenebilir bir etkinlik olarak doğrulanabileceğini onaylar. Sistem kaydının sadece bir kez yapılması gerekir, ancak Erişimci güvenli adresler listesi, Erişimci başına sadece bir kez oluşturulur.

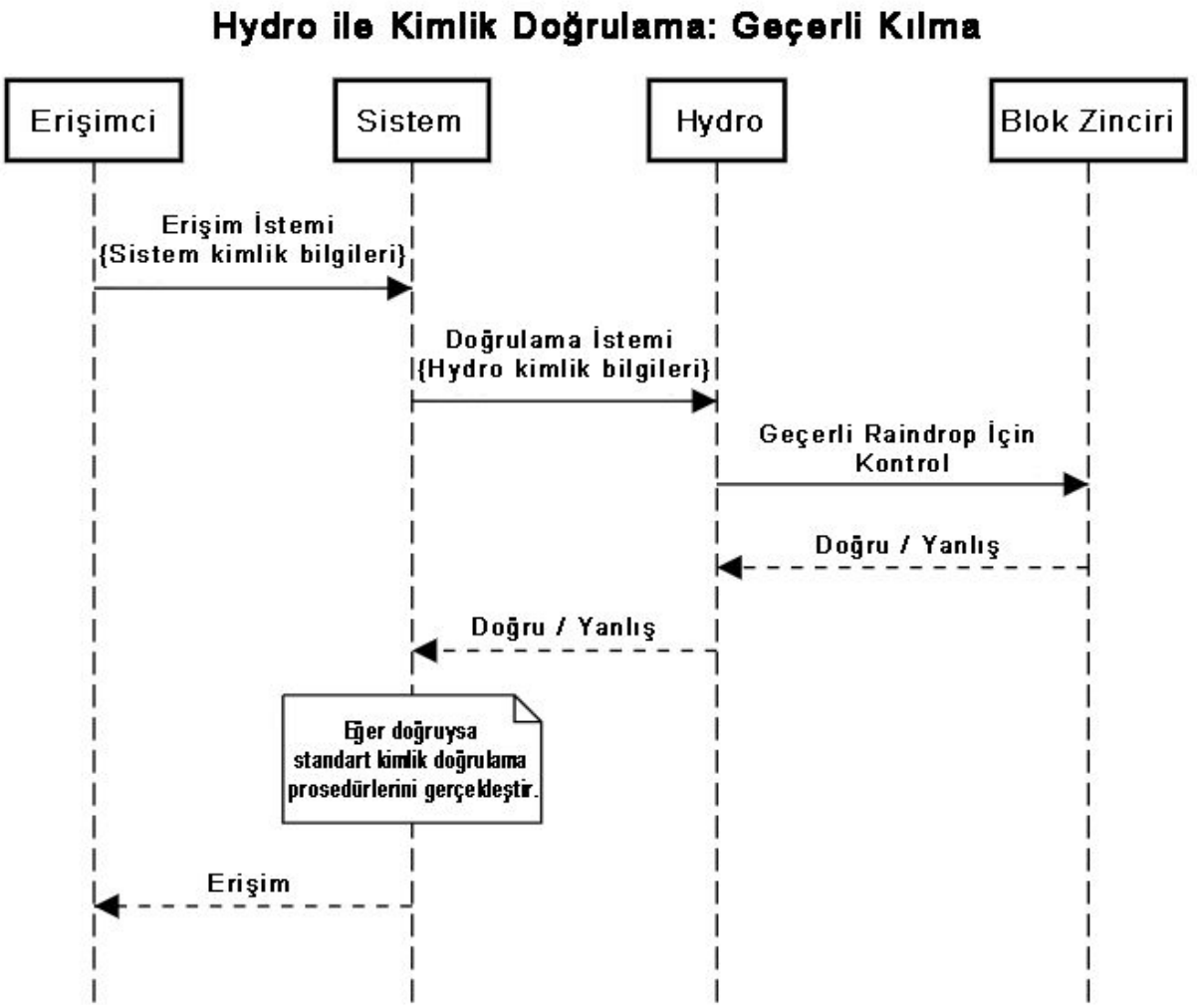


Başlatma tamamlandıktan sonra Hydro kimlik doğrulama işleminin çekirdeği start verir. Bir Raindrop işlemi yürütmesi gereken Erişimci, Sistemden Raindrop detaylarını talep ederek bu süreci hızlandırır ve sistem, talebi Hydro'ya yönlendirir. Hydro yeni bir Raindrop üretir, bazı detayları blok zincirinde değişmez bir şekilde saklar ve tüm detayları sistem üzerinden Erişimciye geri gönderir. Gerekli tüm bilgilerle donatılmış olan Erişimci, kayıtlı adresinden Hydro akıllı sözleşmesindeki bir yönteme bir işlem gerçekleştirir. Adres güvenli adresler listesinde bulunmuyorsa, eylem reddedilir - aksi halde akıllı sözleşmeye kaydedilir. Bu işlemin, sistemin

dışında, Erişimcinin özel anahtarı (yalnızca erişimcinin alabileceği) ile imzalanması gerektiği için, doğrudan erişimciden blok zincirine doğru gerçekleşmesi önemlidir.



Sürecin son adımı doğrulamadır. Bu adımda, Erişimci, Sistem'in yerleşik mekanizması aracılığıyla Sisteme erişimi resmen talep eder. Standart kimlik doğrulama protokollerinden herhangi birini uygulamadan önce Sistem, Erişimcinin geçerli bir Raindrop işlemi gerçekleştirip gerçekleştirmediğini Hydro'dan ister. Hydro, akıllı sözleşme ile arayüz oluşturur, geçerliliği kontrol eder ve doğru / yanlış bir tanımlama ile cevap verir. Sistem, bu atamaya göre nasıl devam etmesi gerektiğine karar verebilir – örneğin eğer yanlış ise, erişimi reddedebilir ve eğer doğruysa, erişim izni verebilir.



Eğer biz temel Sistem kimlik bilgilerinin (ya da mevcut sistem protokolü ne olursa olsun) geniş kapsamlı bir kimlik doğrulama faktörü olduğunu düşünürsek, Hydro katmanının yararlı bir ikinci faktör sağlaması önemlidir. İki temel saldırı vektörünü inceleyerek, bu katmanın yararlılığını kolayca teyit edebiliriz:

- Vektör 1 - Saldırgan Erişimcinin temel sistem kimlik bilgilerini çaldı

    - Saldırgan, geçerli sistem kimlik bilgileri ile sisteme erişim elde etmeye çalışır
    - Sistem, blok zincirinde geçerli bir işlem yapılıp yapılmadığını belirlemek için Hydro ile kontrol gerçekleştirir
    - Hydro yanlış erişimi geri çevirir ve sistem erişimi reddeder
- Vektör 2 - Saldırgan Erişimcinin cüzdanındaki özel anahtarı çalar
    - Saldırgan, gerekli Raindrop ayrıntıları olmadan kayıtlı bir adresten bir Hydro işlemi gerçekleştirmeye çalışır.
    - Saldırgan geçerli bir blok zinciri işlemi yapamaz
    - Ayrıca saldırgan doğru sistem kimlik bilgileri olmadan sisteme erişim talep edemez.

Saldırganın sisteme erişmek için hem temel sistem kimlik bilgilerini hem de erişimcinin özel cüzdan anahtarını/anahtarlarını çalması gerektiği açıktır. Bu bağlamda Hydro, ek bir kimlik doğrulama faktörünü başarıyla ekler.

Raindrop'un Kamuya Açılması

Bu blok zinciri tabanlı kimlik doğrulama hizmeti Hydrogen API ekosisteminin güvenliğini sağlamak için yapılandırılmış olsa da farklı platformlar ve sistemlere de yaygın şekilde uygulanabilir. Başkalarının bu doğrulama katmanından potansiyel olarak yararlanabileceğini düşündüğümüz için, onu kullanıma açıyoruz.

Tıpkı Hydrogen'in kendi API ekosistemine erişim için bir ön koşul olarak entegre edeceği gibi, herhangi bir sistem de mevcut prosedürlere ve protokollere bu sistemi ekleyebilir. Herhangi bir platform -bu bir API olabilir, uygulama, kurumsal yazılım, oyun platformu olabilir, vb.- kimlik doğrulama amacıyla Hydro'dan yararlanabilir. Bu blok zinciri katmanını bir kimlik doğrulama sistemi veya REST API'sine dahil etmek isteyenler için resmi belgeler, GitHub'da mevcut olacaktır.

Örnek Olay - OAuth 2.0 ile Raindrop

Raindrop sürümünün özel kuruluşlar tarafından kullanılabileceği düzinelerce yol vardır. Özel API'ler, veri tabanları ve ağlar, hassas verileri güvence altına almak için son on yılda, jetonlar [tokens], anahtarlar, uygulamalar ve protokoller oluşturdu. Örneğin Google. Google Authenticator uygulamasıyla pazardaki en popüler ürün sağlayıcılarından biri oldu. Daha önce de belirtildiği gibi, mevcut protokollerle rekabet etmek ya da onları değiştirmek için çok sebep var.

Bir örnek olay çalışması olarak burada, Hydrogen'in genel API güvenlik sisteminde bir güvenlik katmanı olarak Hydro kimlik doğrulamasını nasıl uyguladığı hakkında kısa bir özet yapacağız:

1. Hyrogen API iş ortakları, öncelikle güvenli adresler listesine alınan çeşitli ortamların IP adreslerine sahip olmalıdır.
2. İş ortakları, genel bir Hydro adresini güvenli adresler listesine eklemeyi talep etmelidir.
3. Hidrojen API'lerine yapılan tüm çağrılar ve verilerin aktarımı, HTTPS protokolü aracılığıyla şifrelenir ve iletilir.
4. İş ortakları, kayıtlı Hydro adresinden geçerli bir Hydro Raindrop işlemini tamamlamalıdır.
5. İş ortakları OAuth 2.0 doğrulamasını kullanmalıdır. OAuth (Açık Yetkilendirme), jeton tabanlı kimlik doğrulama ve yetkilendirme için açık bir standarttır. Hyrogen "Kaynak Sahibi Şifre Kimlik Bilgileri" ve "İstemci Kimlik Bilgileri" onay türlerini destekler ve her bir API kullanıcısı bir kimlik doğrulama talebi için kimlik bilgisi sağlamalıdır.
6. Eğer yukarıdaki beş öğeden hiçbiri ihlal edilmediyse, Hydrogen iş ortağına her bir API çağrısının kontrol edilmesi ve doğrulanması için benzersiz [unique] bir jeton verilir.
7. Jeton 24 saat boyunca geçerlidir, 24 saatten sonra iş ortağı kendilerini tekrar doğrulamalıdır.

Bu adımlardan herhangi biri ihlal edilirse, kullanıcı hemen API erişiminden uzaklaştırılır. Bir saldırgan, rastgele tahminde bulunarak bu güvenlik faktörlerini baypas edemez, çünkü trilyonlarca benzersiz kombinasyon vardır.

Hydro blok zinciri tabanlı kimlik doğrulama, Hydrogen güvenlik protokolünün önemli bir bileşenidir. Hidrojen ekibi, iş ortaklarını çoklu imza cüzdanları kurmaya ve özel anahtarlarını da diğer kimlik bilgilerinden bağımsız olarak birden çok güvenli konumda depolamaya teşvik eder. Böylece tek bir başarısızlık noktası kalmaz. Bu durumda düzgün bir şekilde oluşturulmuş güvenli bir çoklu imza cüzdanını çalmak zor olmakla kalmaz, aynı zamanda blok zincirinin kamusal yapısı da API'nin güvenliği ile ilgili herhangi bir hırsızlığın hızlı bir şekilde tanınmasını sağlar.

Herkes, Hydro akıllı sözleşmesindeki bir kimlik doğrulama girişimini görüntüleyebilir ki bu da aylar boyunca platformların ele geçirildiği günlerin, geçmişte kaldığı anlamına gelir. API hacker'ları artık beklenmedik yetkilendirme girişimlerini gerçek zamanda, dünyanın herhangi bir yerinden

tespit etme yeteneği nedeniyle artık daha dolaysız bir şekilde engellenebilir.

Riskler

Sosyal medyanın, e-posta'nın ve yayın uygulamalarının (çevirmeli bağlantıya dayanan) ilk günleri gibi her yeni teknolojiye benzer şekilde, çekirdek ekibin (geliştirme ekibi), Ethereum işlem hızlarında ve hacimlerindeki yeni gelişmeleri yakından takip etmesi önemlidir. Youtube'un 1995 yılında lansman yapmayı denediğini düşünsenize? Ya Instagram'ın ilk kez Blackberry'de sunulduğunu?

Vitalik Buterin ve Joseph Poon gibi önemli Ethereum geliştiricileri Plazma'yı önerdi: Ölçeklendirilebilir Özerk Akıllı Sözleşmeler, Ethereum protokolünde bir üst seviyeye geçer:

> Plazma, blok zincirinin dünya çapında önemli miktarda merkezi olmayan finansal uygulamaları temsil edebilmesini mümkün kılan, saniyede önemli miktarlarda durum güncellemesi (potansiyel olarak milyarlar) ile ölçeklendirilebilen akıllı sözleşmelerin teşvik edilmesi ve yürütülmesi için önerilen bir sistemdir. Bu akıllı sözleşmeler, işlemsel durum geçişlerini zorunlu kılmak için sonuçta temel blok zincirine (ör., Ethereum) bağımlı olan ağ işlem ücretleri yoluyla otonom olarak çalışmaya devam etmek için teşvik edilir.

Raiden Ağı gibi diğerleri ise, daha hızlı işlem ve daha düşük ücret sağlamak için tasarlanmış bir ardışık zincir çözümü önerirler. Fakat Raindrop Ethereum sistemine çok az bir yük getirecek ve böylece ölçeklenebilirlik, teknolojinin başarısı için çok küçük bir risk halini alacaktır.

Sonuç

Halka açık bir blok zincirinin değişmezliği, API'ler gibi özel sistemlerin güvenliğini artırmak için yeni yollar sunar.

Bu yazıda üç önemli şey gösterilmiştir:

1. Kamusal blok zinciri finansal hizmetlere değer katabilir.
2. Hydro Raindrop, özel sistemlerin güvenliğini artırabilir.
3. Hydrogen API platformunda Hydro Raindrop'un hazır uygulamaları vardır.

Hydro ekibi, ortaya konan sistemin finansal hizmet endüstrisinde ve ötesinde tüm paydaşlara fayda sağlayacak yeni bir hibrid özel-kamu sistemi modeli için standart güvenlik altyapısı olabileceğine inanır.

Kaynaklar:

Ethereum; Merkling in Ethereum
Trend Micro; What Do Hackers Do With Your Stolen Identity?
Javelin Strategy & Research; *The 2017 Identity Fraud Study*
Symantec; *Internet Security Threat Report*
Risk Based Security; *2016 Data Breach Trends – Year in Review*
Thales; *2017 Thales Data Threat Report – Financial Services Edition*
Apache.org; Apache Struts 2 Documentation - S2-052
Joseph Poon and Vitalik Buterin; Plasma: Scalable Autonomous Smart Contracts