Blokzincir 101

Prof.Dr. Ali Hakan IŞIK
Res.Assist. Durmuş Gülbahar

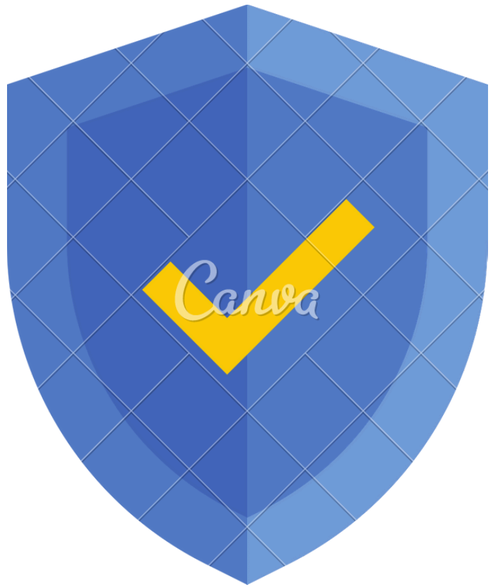
5.Hafta

Eğitimimizin beşinci haftasında blokzincir güvenliği ile ilgili kavramlar incelenecek ve akıllı kontratlarda yaygın güvenlik açıklarını tartışacağız. Dünya çapında meydana gelen kripto hırsızlıklarından bahsedeceğiz ve sebeplerini inceleyeceğiz. Eğitim sonunda uygulamalı olarak bir kontrata Reentrancy saldırısı yapacağız.

İçerik

- Blokzincirde Güvenlik
- Konsensus Mekanizmaları
- Akıllı Kontratlarda Güvenlik
- Yaygın Güvenlik Açıkları
- Dünya Çapında Kripto Hırsızlıkları
- Bridge nedir?
- **Uygulama**: Reentrancy Saldırısı

Blokzincirde Güvenlik



Blokzincir güvenliği, kriptografik algoritmalar, merkeziyetsizlik ve mutabakat mekanizmaları ile sağlanmaktadır. Verilerin değiştirilemezliği, işlemlerin her düğümde tutulması gibi blokzinciri doğasında bulunan özellikler blokzinciri yüksek seviye güvenlikli bir alt yapı haline getirmektedir.

Konsensus Mekanizmaları

Bu mekanizmalar, ağdaki tüm düğümlerin (node) işlemler üzerinde mutabakata varmasını sağlar.

Proof Of Work	Proof of Stake	Byzantine Fault Tolerance
İşlem Gücü	Sahip olunan varlıklar	Özel ağlar
Bitcoin	Ethereum 2.0	Kötü katılımcı

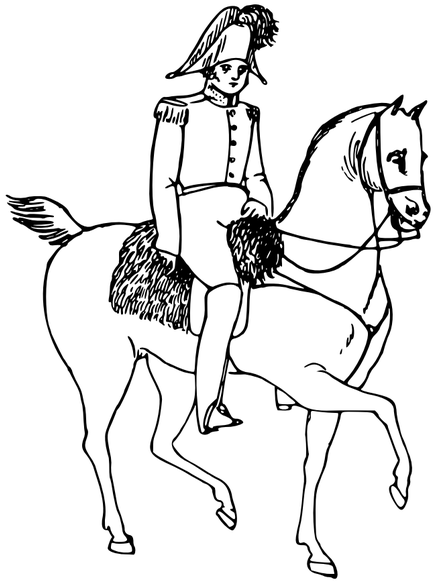
Konsensus Mekanizmaları - PoW

PoW, blockchain ağlarında işlemlerin güvenli bir şekilde doğrulanmasını ve yeni blokların merkeziyetsiz bir yapıda oluşturulmasını sağlayan bir konsensüs algoritmasıdır. Çalışma prensibi oldukça basittir: ağ katılımcıları, karmaşık matematiksel bir problemi çözerek belirli bir "iş" yaptıklarını kanıtlarlar. Bu zorlu bulmacayı ilk çözen madenci, çözümü ve yeni bloğu ağa sunar. Ağdaki diğer düğümler bu kanıtın geçerliliğini kolayca teyit eder ve blok zincire eklenir.
PoW'un en önemli noktaları arasında sağladığı yüksek güvenlik düzeyi ve merkeziyetsiz yapısı yer alır. Ağın manipüle edilebilmesi için çok büyük bir işlem gücüne ihtiyaç duyulması, kötü niyetli girişimleri pratik olarak imkansız kılar. Ancak, bu güvenlik seviyesinin bedeli yüksek enerji tüketimidir ki bu da PoW'un en çok eleştirilen yönüdür. Ayrıca, bulmacanın zorluk seviyesinin ağdaki işlem gücüne göre otomatik olarak ayarlanması, blok oluşturma süresinin dengede tutulmasını sağlar.
Bitcoin gibi öncü kripto paraların kullandığı bu ilk nesil konsensüs mekanizması, blockchain teknolojisinin temelini oluşturmuş olsa da, enerji verimliliği konusundaki endişeler nedeniyle farklı konsensüs mekanizmaları da geliştirilmeye devam etmektedir.

Konsensus Mekanizmaları - PoS

Proof of Stake (PoS), blockchain ağlarında işlemleri doğrulamak ve yeni bloklar oluşturmak için kullanılan, Proof of Work'e (PoW) alternatif bir konsensüs mekanizmasıdır. Temel prensibi, ağ katılımcılarının işlem gücü yerine sahip oldukları kripto para birimini "stake" ederek ağın güvenliğine katkıda bulunmalarıdır. Stake edilen miktar, doğrulayıcı seçimi ve blok oluşturma sürecinde önemli bir rol oynar. Başarılı doğrulayıcılar ödüllendirilirken, kötü niyetli davranışlar ise stake edilen varlıkların kaybıyla sonuçlanabilir. PoS, PoW'a kıyasla daha enerji verimli, potansiyel olarak daha hızlı işlem süreleri sunan ve daha düşük giriş bariyerine sahip bir alternatif olarak öne çıkmaktadır.

Konsensus Mekanizmaları - BFT



Byzantine Fault Tolerance (BFT), dağıtık sistemlerin, arızalı veya kötü niyetli düğümlerin varlığına rağmen tutarlı ve doğru bir şekilde çalışabilme yeteneğini ifade eder. Bizans Generalleri Problemi'nden ilham alan bu kavram, bir grup katılımcının, bazıları yanıltıcı bilgi verse bile ortak bir karar üzerinde anlaşmasını hedefler. BFT algoritmaları, belirli sayıda hatalı düğüme kadar tolerans göstererek sistemin güvenilirliğini ve hataya karşı direncini artırır ve özellikle yüksek güvenlik gerektiren blockchain ağları için kritik bir öneme sahiptir.

Akıllı Kontratlarda Güvenlik

Akıllı kontratlar ağa yüklenmeden önce yoğun bir test sürecinde geçirilmelidir. Bunun sebebi, akıllı kontratların ağ üzerinde sonradan değiştirilemezliğidir.

Kod Denetimi (Audit)
Erişim Kontrolleri
Hata Kontrolü
Acil Durdurma (Circuit Breaker)
Güvenli Kütüphaneler(SafeMath)

Yaygın Güvenlik Açıkları

Reentrancy

Bir akıllı kontrat, başka bir kontratı çağırdığında (örneğin fon transferi için) ve bu çağrı tamamlanmadan önce durum değişkenlerini güncellemezse, kötü niyetli bir kontrat aynı fonksiyonu tekrar tekrar çağırarak kontrattan fon çalabilir.

The DAO hack (2016). Saldırgan, bir yeniden giriş açığından faydalanarak 50 milyon dolar değerinde ether çaldı.

Yaygın Güvenlik Açıkları

Access Control Issues

Kontrat fonksiyonlarına kimlerin erişebileceğinin yanlış yapılandırılması. Örneğin, kritik bir fonksiyonun herkes tarafından çağrılabilir olması. Önlem ise public fonksiyonların onlyOwner gibi metotlarla kısıtlanmasıdır.

Parity Wallet bug'ı (2017). Bir kütüphane kontratındaki yanlış erişim kontrolü, 30 milyon dolarlık ether kaybına neden oldu.

Yaygın Güvenlik Açıkları

Flash loan vulnerability

Teminatsız olarak alınabilen ve aynı işlem içinde geri ödenmesi gereken bir kredi türüdür. Atomik bir yapıdadır, aynı işlem içerisinde aldığın borcu ödemek durumundasınızdır. Eğer bir adım başarısız olursa işlem hiç olmamış gibi kabul edilir ve zincire yazılmaz.

Cream Finance Hack (2021)
Ağustos 2021'de, bir DeFi borç verme platformu olan Cream Finance, bir flash kredi açığı nedeniyle 180 milyon dolar kaybetti. Saldırganlar, flash kredileri kullanarak token çifti fiyatlarını manipüle etti ve sistemden fonları boşalttı

Bridge Nedir?

Farklı ağlar arasında varlık ve veri transferini mümkün kılarak çapraz zincir (cross-chain) uyumluluğunu sağlayan protokollerdir.

Uygulama: Reentrancy Saldırısı

Araçlar:

- RemixIDE (Online Editor for Solidity)
- OpenZeppelin (Smart contract kütüphanesi)
- Solidity (Smart contract programlama dili)