

Blok Zincirde Güvenlik

Kriptografik Hash Fonksiyonları

- **Hash Değerleri:** Bir blokun içeriğini benzersiz bir şekilde temsil eden, tersine çevrilemez sayı dizileri.
- **Kolizyon Direnci:** İki farklı girdinin aynı hash değerini üretmesinin zor olması.
- **Hash Hızı:** Hash işleminin hızı, blok zincir performansını doğrudan etkiler.
- **SHA-256 ve Diğer Algoritmalar:** Bitcoin gibi sistemlerde kullanılan standart hash algoritması.

Dijital İmzalar

- **Özel Anahtar ile İmzalama:** İşlemlerin sahte olmadığını kanıtlamak için kullanılır.
- **Kamu Anahtarı ile Doğrulama:** İmzanın sadece belirli bir özel anahtarla yapıldığını doğrular.
- **Elips Eğrileri Kriptografisi:** Güçlü güvenlik sunan ve yaygın olarak kullanılan bir kriptoloji yöntemi.
- **İmza Algoritma Seçimi:** Güvenlik düzeyini ve işlem hızını etkiler.

İş Kanıtı (Proof of Work)

- **Zorluk Ayarı:** Ağdaki madencilik gücüne bağlı olarak zorluğun ayarlanması.
- **Nonce Bulma:** Geçerli bir bloğu onaylamak için gerekli sayıyı bulma süreci.
- **Enerji Tüketimi:** Çok fazla hesaplama gücü gerektirir ve enerji tüketimi yüksektir.
- **Çift Harcama Önleme:** İşlemlerin tekrar kullanımını engeller ve güvenliği sağlar.

Pay Kanıtı (Proof of Stake)

- **Token Sahipliği:** Daha fazla token sahibi olanların, daha fazla madencilik gücü ve oylama hakkı.
- **Randomizasyon Süreci:** Blok onay sürecinde rastgele seçim, oyun teorisi kullanarak güvenlik sağlar.
- **Düşük Enerji Tüketimi:** PoW'a kıyasla daha az enerji gerektirir.
- **Zenginlik Konsantrasyonu Riski:** Zenginler daha zengin olabilir, bu da ağın merkezileşmesine yol açabilir.

Dağıtık Ağ Yapısı

- **Noktadan Noktaya Bağlantı:** Her katılımcının eşit yetkisi ve ağ üzerinde kontrolü vardır.
- **Saldırıya Dayanıklılık:** Merkezi olmayan yapı, tek bir hedef noktasının olmamasını sağlar.
- **Veri Doğruluğu ve Şeffaflık:** Her işlem herkes tarafından görülebilir ve doğrulanabilir.
- **Kopya Veri Saklama:** Veriler, ağdaki birden fazla noktada saklanır.

Konsensüs Mekanizmaları

- **Konsensüs Kuralları:** Ağdaki tüm düğümler tarafından kabul edilen kurallar.
- **Çoğunluk Kararları:** İşlemlerin ve blokların geçerliliğini belirlemede çoğunluk kararı esastır.
- **Çatal Yönetimi:** Konsensüs kurallarında bir değişiklik olduğunda ağın nasıl bölüneceği.
- **Yeni Protokol Entegrasyonları:** Güvenlik veya performans iyileştirmeleri için protokol güncellemeleri.

Akıllı Sözleşme Güvenliği

- **Kod Doğrulama:** Akıllı sözleşmelerin, hatalardan ve güvenlik açıklarından arındırılmış olması.
- **Reentrancy Saldırıları:** Aynı fonksiyonun tekrar tekrar çağrılmasıyla ortaya çıkan saldırı türü.
- **Gas Limitleri:** Sözleşme yürütmesi sırasında tüketilebilecek maksimum gas miktarı.
- **Zamanlama Güvenliği:** Sözleşmelerin belirli koşullar altında zamanında yürütülmesi.

51% Saldırısı ve Diğer Saldırı Türleri

- **51% Saldırısı:** Bir madenci veya madenci grubunun ağın çoğunluk hash gücünü kontrol ederek, işlemleri manipüle etmesi.
- **Sybil Saldırısı:** Ağdaki çoğu düğüm üzerinde sahte kimliklerle kontrol sağlama çabası.
- **Çifte Harcama:** Aynı dijital paranın birden fazla kez harcanması.
- **Zaman Damgası Manipülasyonu:** Blokların sırasını ve geçerliliğini etkilemek amacıyla zaman damgalarının manipüle edilmesi.

Özel Anahtar Güvenliği

- **Anahtar Saklama Yöntemleri:** Özel anahtarların güvenli bir şekilde saklanması için kullanılan çeşitli yöntemler.
- **Çoklu İmza Protokolleri:** Bir işlemin birden fazla imza gerektirmesi, güvenliği artırır.
- **Phishing Saldırılarına Karşı Korunma:** Kullanıcıları, özel anahtar bilgilerini çalmaya yönelik saldırılardan koruma.
- **Donanım Cüzdanları:** Özel anahtarların internete bağlı olmayan fiziksel cihazlarda saklanması.

Blok Zinciri Forkları ve Güvenlik Sonuçları

- **Yumuşak Forklar:** Uyumlu değişikliklerin uygulanması, eski düğümlerle uyumlu olmaya devam eder.
- **Sert Forklar:** Radikal değişikliklerin uygulanması, eski düğümlerle uyumsuzdur ve ağı böler.
- **Konsensüs Değişiklikleri:** Forklar sırasında konsensüs kurallarının değişmesi.
- **Topluluk Bölünmeleri:** Forklar nedeniyle topluluk içinde fikir ayrılıkları ve bölünmeler.

Zaman Damgası ve Blok Doğrulama

- **Zaman Damgası Doğruluğu:** Her bloğun doğru bir şekilde zaman damgası alması ve kaydedilmesi.
- **Blok Sıralaması:** Blokların oluşturulma sırasının korunması ve tahrif edilmemesi.
- **Blok İmzaları:** Her bloğun, madenciler tarafından imzalanması ve bu imzaların doğrulanması.
- **Blok Boyutu ve Geçerlilik:** Blokların belirlenen boyut ve kurallara uygun olup olmadığının denetimi.

Merkezi Olmayan Uygulamaların (dApps) Güvenliği

- **Kullanıcı Arayüzü Güvenliği:** Kullanıcıların güvenli bir şekilde etkileşimde bulunabileceği arayüzlerin tasarımı.
- **Bağımlılıkların Yönetimi:** Dış kütüphanelere ve hizmetlere olan bağımlılığın güvenli bir şekilde yönetilmesi.
- **Veri Saklama ve Erişim:** Kullanıcı verilerinin güvenli bir şekilde saklanması ve erişim yönetimi.
- **Yanıltıcı DApp Saldırıları:** Kötü niyetli uygulamalar aracılığıyla kullanıcı bilgilerini çalma veya zarar verme girişimleri.

Katılımcı ve Ağ Kimlik Doğrulaması

- **Kimlik Doğrulama Protokolleri:** Ağ katılımcılarının kimliklerinin doğrulanması.
- **Yetkilendirme Yöntemleri:** Ağ içi kaynaklara erişim yetkilerinin yönetilmesi.
- **Kimlik Avı Saldırılarına Karşı Savunma:** Kimlik bilgilerinin kötüye kullanılmasını önlemek.
- **Anonimlik ve Gizlilik Dengelemesi:** Katılımcıların gizliliğini korurken güvenliği sağlama.

Güvenlik İhlallerine Karşı Korunma Stratejileri

- **Düzenli Güvenlik Denetimleri:** Sistemlerin sürekli olarak denetlenmesi ve güvenlik açıklarının araştırılması.
- **Yedekleme ve Felaket Kurtarma:** Veri kaybını önlemek ve sistem çökmelerinde hızlı toparlanma.
- **Güvenlik Politikaları ve Prosedürler:** Kurumsal güvenlik politikaları ve bunların uygulanması.
- **Eğitim ve Farkındalık Programları:** Kullanıcıları ve yöneticileri eğitmek, güvenlik farkındalığını artırmak.

Mevzuat ve Uyum Sorunları

- **Düzenleyici Çerçeveler:** Farklı yargı bölgelerindeki blockchain teknolojilerine ilişkin yasal düzenlemeler.
- **Uyum Yükümlülükleri:** Yasal gereksinimlere uygun hareket etme yükümlülüğü.
- **Gizlilik Kanunları:** GDPR gibi veri gizliliği kanunlarına uyum.
- **Kripto Para Birimlerinin Denetimi:** Devletlerin kripto para birimlerini denetleme yöntemleri ve yaklaşımları.