# Ethereum Akıllı Kontrat Güvenliği

# Akıllı Kontrat Hackleri ve Güvenilir Kodun Önemine dair

- Güvenilir kod nedir?
- Güvenilir kod yazmak her zaman önemli olmuştur
- Blokzincirlerde güvenilir kod yazmamak kötü sonuçlanır
- 2016 DAO hack'i
- 2020: 4B$, 2021: 4B$, 2022: 1.6B$

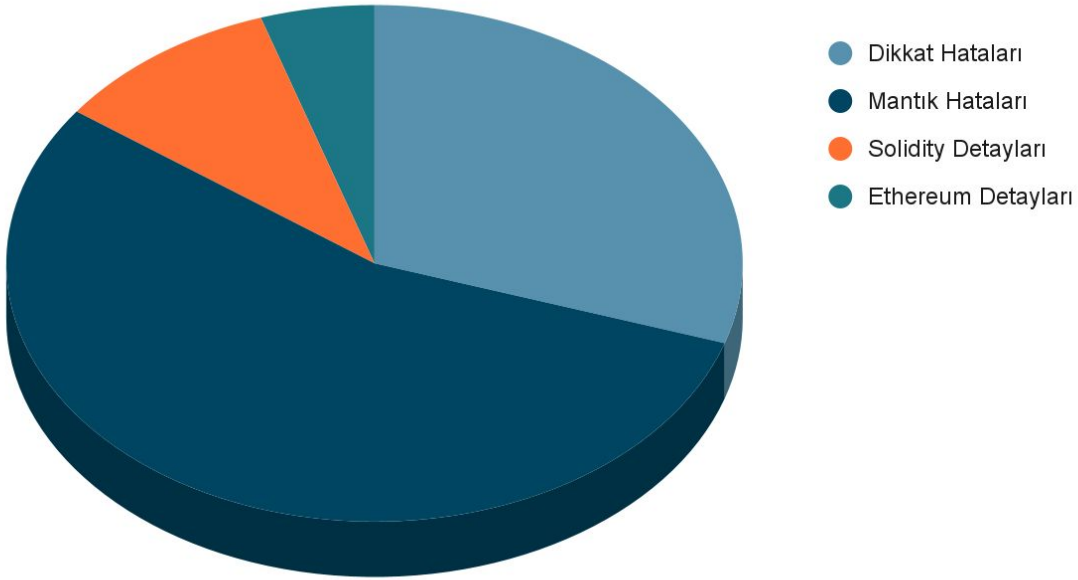
# Yapılabilecek Olası Saldırılar

- Phishing saldırıları ve dolandırıcılıklar
- Projenin serverlarına yapılabilecek saldırılar
- Blok-zincir ağına yapılabilecek saldırılar
- Akıllı kontratlardaki açıklara yapılan saldırılar

# Eğer kodu kimseye göstermezsem hataları bulunur mu?

# Akıllı Kontrat Hataları

- Dikkat hataları
- Mantık hataları
- Yazılan dili anlamamaktan dolayı oluşan hatalar
- Ethereum'un çalışma mantığını anlamamaktan dolayı oluşan hatalar


Dikkat Hataları
Mantık Hataları
Solidity Detayları
Ethereum Detayları

# Dikkat Hataları

- Kodun çalışması yeterli değil
- İşlemler doğru mu yapıldı?
- Kullanıcılar doğru yetkilere sahip mi? Yetkisi olmayanın fonksiyonları çağıramaması için nasıl önlemler alındı?
- Karşılaştırmalar doğru mu?

# Çözümü

- Yetkiler ve işlemler hakkında yapılacak unit-testler

# Dikkat Hatası Örnekleri

- >= yerine > kullanılması
- i++ yerine ++i kullanılması
- Ownable kontratlarda onlyOwner modifier'ının unutulması
- private olması gereken fonksiyonların external/public bırakılması
- Yazılması gerektiği bilinen kodun atlanması

# Hatanın yaşandığı projeler

- Parity Wallet
- Rubixi
- Roco Finance

# Mantık Hataları

- Kod tamamen doğru yazılsa bile istenilen şeyi yapmayabilir
- Kontrat neyi başarmayı amaçlıyor?
- Bu amaç nesnel ölçütlerle nasıl ifade edilir?

# Çözüm

- Kodun spesifikasyonunun hazırlanması
- Spesifikasyona uygun olarak testlerin hazırlanması

# Mantık Hatası Örnekleri

- Whitelist ile satılan bir NFT'nin bazı koşullarda alınabilmesi
- Fiyat formülü iyi yazılmayan DEX'ler
- Mint edilebilen token'ların toplam arzını kontrolsüz arttırabilecek mekaniklerin bulunması

# Hatanın yaşandığı projeler

- Çoğu DeFi protokolü
- Fei Rari
- Saddle Finance
- Fluffy Bears