

# Temel Kavramlar

# Blok Zinciri (Blockchain)

- Tanım: Blok zinciri, işlemlerin kronolojik olarak kaydedildiği ve bir ağ üzerinde dağıtılmış bir defterdir.
- Bloklar: Bir blok zincirinde, işlemler bloklar halinde saklanır ve birbirine zincirleme bağlanır.
- Dağıtık Yapı: Veriler, merkezi bir otorite olmaksızın ağdaki tüm katılımcılar arasında paylaşılır.
- Güvenlik: Kriptografik hash fonksiyonları, işlemlerin güvenliğini ve değiştirilemezliğini sağlar.

# Dağıtık Defter Teknolojisi (DLT)

- Tanım: Birden fazla katılımcının, merkezi bir otorite olmaksızın kayıtları tuttuğu ve paylaştığı bir veri tabanı teknolojisidir.
- İzinli ve İzinsiz Sistemler: Sistemlere erişim kontrolü bazında iki ana tip vardır; izinli (private) ve izinsiz (public).
- Eşler Arası Ağ (P2P): Katılımcılar doğrudan birbirleriyle iletişim kurarak işlemleri gerçekleştirir.
- Consensus Mekanizmaları: Ağdaki tüm katılımcıların veri üzerinde anlaşmaya varmasını sağlayan kurallar bütünüdür.

# Hash Fonksiyonu

- Tanım: Girdi olarak verilen herhangi bir boyuttaki veriyi, sabit boyutta bir çıktı üreten fonksiyondur.
- Değiştirilemezlik: Verinin en küçük bir değişikliği bile çıktıyı tamamen değiştirir.
- Güvenlik: Hash çıktıları, orijinal veriyi geri çıkarmak için kullanılamaz, bu yüzden tek yönlüdür.
- Blok Zinciri Bağlamı: Bloklar bir önceki bloğun hash değeri ile bağlanır, zincirin bütünlüğünü korur.

# Değiştirilemezlik Örneği

- 123456 (String)
  - e10adc3949ba59abbe56e057f20f883e (MD5)
  - 7c4a8d09ca3762af61e59520943dc26494f8941b (SHA1)
- 
- 123457 (String)
  - f1887d3f9e6ee7a32fe5e76f4ab80d63 (MD5)
  - 908f704ccaadfd86a74407d234c7bde30f2744fe (SHA1)

# Sabit Boyutta Çıktı Örneği

- 123457 (String)
  - f1887d3f9e6ee7a32fe5e76f4ab80d63 (MD5)
  - 908f704ccaadfd86a74407d234c7bde30f2744fe (SHA1)
- 
- 1234574567 (String)
  - 9935c1895f78365a7f3ac4a6326f08d1
  - f5e8d2fc5fcea1755df7386f79590999d93c0d0d

# Blok

- Tanım: Blok zincirinde, işlemlerin bir araya getirildiği veri yapılarıdır.
- Blok Başlığı: Her bloğun, önceki bloğun hash değeri, zaman damgası gibi meta verileri içerir.
- İşlem Listesi: Bir blok, birçok işlemi içerir ve bu işlemler blok zincirinde kaydedilir.
- Blok Ödülü: Madenciler, yeni bir blok oluşturduklarında belirli bir miktar kripto para birimi ile ödüllendirilir.

# Madencilik (Mining)

- Tanım: Blok zincirindeki işlemleri doğrulama ve yeni bloklar eklemek için yapılan hesaplama işlemidir.
- Proof of Work: Madenciler, zorlu bir matematiksel problemi çözerek yeni bir blok ekler ve ödül kazanır.
- Hash Oranı: Madencilik gücü, saniyede yapılan hash işlemi sayısı ile ölçülür.
- Enerji Tüketimi: PoW tabanlı sistemlerde madencilik, önemli miktarda elektrik enerjisi tüketir.



# Akıllı Sözleşmeler (Smart Contracts)

- Tanım: Önceden belirlenen koşulların gerçekleşmesi durumunda otomatik olarak uygulanan, programlanabilir sözleşmelerdir.
- Otomatik Uygulanma: Koşullar sağlandığında, akıllı sözleşmeler kendi kendine uygulanır, aracıya gerek kalmaz.
- Güvenlik ve Şeffaflık: İşlemler blok zinciri üzerinde kaydedildiği için değiştirilemez ve doğrulanabilir.
- Kullanım Alanları: Finans, sigorta, tedarik zinciri gibi birçok sektörde kullanılır.

# Kripto Para Birimleri

- Tanım: Dijital veya sanal para birimleri, merkezi bir otoriteye bağlı olmadan işlem görebilen dijital varlıklardır.
- Bitcoin: İlk ve en bilinen kripto para birimi.
- Altcoinler: Bitcoin dışındaki kripto para birimleri; Ethereum, Ripple, Litecoin gibi.
- Kripto Cüzdanlar: Kripto para birimlerinin saklanması, gönderilmesi ve alınması için kullanılan dijital cüzdanlar.

# Merkezi Olmayan Uygulamalar (DApps)

- Tanım: Merkezi bir otoriteye bağlı olmayan, blok zinciri teknolojisi üzerinde çalışan uygulamalardır.
- Şeffaflık: Kodları herkes tarafından incelenebilir, işlemler blok zincirinde kaydedilir.
- Sansüre Direnç: Merkezi bir kontrol noktası olmadığı için, sansüre karşı dirençlidir.
- Kullanıcı Kontrolü: Kullanıcılar, verileri ve varlıkları üzerinde tam kontrol sahibidir.

# ICO (Initial Coin Offering)

- Tanım: Blockchain projelerinin finansman sağlamak amacıyla yeni bir kripto para birimi sunması.
- Yatırımcı Katılımı: Yatırımcılar, projeye erken aşamada yatırım yaparak token satın alır.
- Riskler: ICO'lara yatırım yapmak yüksek risk içerir, projenin başarısız olma ihtimali vardır.
- Düzenlemeler: Birçok ülke, ICO'lar üzerinde düzenlemeler getirmiştir veya getirmeyi düşünmektedir.

# DeFi (Decentralized Finance)

- Tanım: Merkezi finans kurumlarına ihtiyaç duymadan finansal hizmetlerin sunulduğu blok zinciri tabanlı sistem.
- Akıllı Sözleşmeler: DeFi uygulamaları, akıllı sözleşmeler aracılığıyla otomatikleştirilmiş finansal işlemler sunar.
- Ürünler ve Hizmetler: Kredi verme, borç alma, varlık ticareti gibi finansal işlemler DeFi üzerinden gerçekleştirilebilir.
- Erişilebilirlik: Herkesin, coğrafi konum veya ekonomik durum gözetmeksizin DeFi hizmetlerine erişimi vardır.

# NFT (Non-Fungible Token)

- Tanım: Benzersiz, değiştirilemez ve bireysel olarak tanımlanabilen dijital varlıklar için kullanılan tokenler.
- Benzersizlik: Her NFT, sahip olduğu meta veriler ile diğerlerinden farklıdır ve takas edilemez.
- Sanat ve Koleksiyon: NFT'ler, dijital sanat eserleri, koleksiyon objeleri gibi alanlarda popülerdir.
- Sahiplik ve Doğrulanabilirlik: NFT'ler, sahipliği ve orijinalliği blok zinciri üzerinden doğrulanabilir şekilde kaydeder.

# Ölçeklendirme Çözümleri

- Katman 2 Çözümleri (Layer 2 Solutions): Blok zincirinin temel katmanını değiştirmeden işlem kapasitesini artıran çözümler.
- Yan Zincirler (Sidechains): Ana zincirden bağımsız çalışan, ancak ona bağlı olan blok zincirleri.
- Rollups: İşlemleri dışarıda işleyip, sonuçları ana zincire kaydeden bir ölçeklendirme yöntemi.
- Sharding: Ağı bölümlere (shard) ayırarak, her birinin farklı işlemleri işlemesini sağlayan bir yöntem.

# Gizlilik Mekanizmaları

- ZK-Snarks: İşlemin geçerliliğini, içeriğini açığa çıkarmadan doğrulayan bir kriptografi yöntemi.
- Ring Signatures: Göndericiyi anonim tutarak işlem gizliliğini sağlayan bir imza yöntemi.
- Gizli İşlemler: İşlem detaylarını, miktarı ve katılımcıları gizleyen teknikler.
- Gizlilik Odaklı Kripto Para Birimleri: Monero, Zcash gibi, gelişmiş gizlilik özellikleri sunan kripto para birimleri.



# Dağıtık Organizasyonlar (DAOs - Decentralized Autonomous Organizations)

- Tanım: Merkezi bir yönetim olmaksızın, akıllı sözleşmeler aracılığıyla yönetilen, otomatik organizasyonlar.
- Oylama ve Karar Alma: DAO üyeleri, projenin yönetimi üzerinde söz sahibi olurlar ve oylama yoluyla karar alırlar.
- Şeffaflık ve Otomasyon: İşlemler ve kararlar blok zinciri üzerinde kaydedilir, otomatik olarak uygulanır.
- Kullanım Alanları: Fon yönetimi, topluluk projeleri, kar amacı gütmeyen organizasyonlar gibi çeşitli alanlarda kullanılır.

# Kriptografi

- Simetrik Kriptografi: Aynı anahtarın şifreleme ve şifre çözme işlemlerinde kullanıldığı bir yöntem.
- Asimetrik Kriptografi: Bir anahtarın şifrelemek, diğerinin şifreyi çözmek için kullanıldığı, iki farklı anahtar kullanılan yöntem.
- Dijital İmzalar: İşlemlerin sahipliğini ve bütünlüğünü doğrulamak için kullanılan kriptografik imzalar.
- Hash Fonksiyonları: Veriyi sabit boyutlu bir çıktıya dönüştüren, tek yönlü işlemler için kullanılan fonksiyonlar.

# Wallet (Cüzdan) Türleri

- Yazılım Cüzdanları: Bilgisayar veya mobil cihazlarda çalışan, kripto para birimlerini saklamak için kullanılan uygulamalar.
- Donanım Cüzdanları: Fiziksel cihazlar olarak, kripto varlıkların güvenli bir şekilde saklanmasını sağlar.
- Kağıt Cüzdanlar: Kripto para adresleri ve özel anahtarlarının basılı formda saklandığı, fiziksel belgeler.
- Çevrimiçi Cüzdanlar: İnternet üzerinde erişilebilen, kripto para birimlerini saklamak ve işlem yapmak için kullanılan platformlar.

# Blockchain Güvenliği ve Saldırı Türleri

- 51% Saldırısı: Bir madenci veya madenci grubunun, ağın yarısından fazlasının hash gücünü kontrol ederek, işlemleri manipüle etmesi.
- Çift Harcama (Double Spending): Aynı kripto para biriminin birden fazla kez harcanmaya çalışılması.
- Sybil Saldırısı: Ağ, sahte kimliklerle doldurarak, ağın işleyişini bozmaya yönelik bir saldırı.
- Phishing ve Güvenlik İhlalleri: Kullanıcıların özel anahtarlarını ele geçirmeye yönelik dolandırıcılık ve siber saldırılar.