Blokzincir 101

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

1.Hafta

İlk hafta, dağıtık sistemleri ve blokzincir teknolojisinin üstüne kurulduğu temel yapıtaşı olan teknolojileri tanımlayacağız. Ayrıca türünün ilk ve en başarılığı örneği olan Bitcoin'in ne olduğunu ve teknik altyapısını tartışacağız.

İçerik

- Dağıtık Defter Teknolojisi
- Dağıtık Sistemli Uygulamalar
- Blokzincir Nedir? Nasıl çalışır?
- Blokzincir karakteristiği
- Blokzincir Tarihçesi
- Çifte harcama (Double Spending)
- Bitcoin
- Kriptografik hash fonksiyonları
- Blokzincir ve madencilik kavramları

Dağıtık Defter Teknolojisi

DLT (Distributed Ledger Technology), verilerin merkezi bir otorite olmadan dağıtık bir ağda saklanmasını ve yönetilmesini sağlayan genel bir teknolojidir.

Kabile metaforu

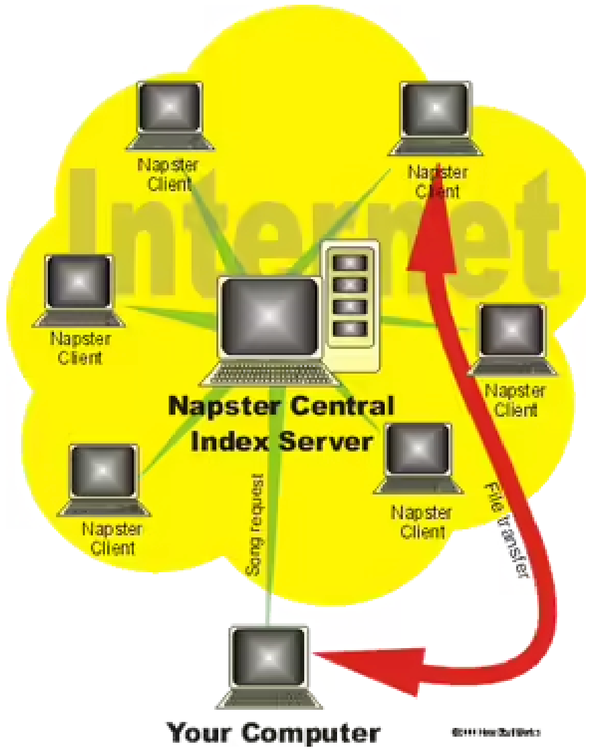
Dağıtık sistemli uygulamalar

Napster (İlk Dönem): Merkezi Yapı
Çalışma Şekli: Kullanıcılar bilgisayarlarındaki müzik dosyalarını merkezi bir sunucuya bildirirlerdi. Başka bir kullanıcı bir şarkı aradığında, merkezi sunucu bu şarkının hangi kullanıcıların bilgisayarında olduğunu listelerdi. İndirme işlemi doğrudan kullanıcılar arasında gerçekleşirdi, ancak arama ve bağlantı merkezi sunucu üzerinden yapılırdı.
Temel Amaç: Öncelikli olarak müzik dosyalarının paylaşımını kolaylaştırmak.
Hukuki Sorunlar: Merkezi yapısı nedeniyle telif hakkı ihlalleri konusunda müzik endüstrisinin doğrudan hedefi haline geldi. Telifli materyalin yaygın bir şekilde izinsiz paylaşımına olanak sağladığı için büyük davalarla karşılaştı ve sonunda kapatılmak zorunda kaldı.
Sonuç: Orijinal Napster kapandı, ancak aynı isimle yasal bir müzik abonelik servisi olarak yeniden doğdu (ancak bu farklı bir platformdur).

Dağıtık sistemli uygulamalar

Limewire: Merkezi Olmayan (Merkezi Sunucusuz) Yapı
Çalışma Şekli: Limewire, Gnutella protokolünü kullanan merkezi olmayan bir P2P istemcisiydi. Bu, kullanıcıların doğrudan birbirleriyle bağlantı kurduğu ve dosya aradığı anlamına geliyordu. Merkezi bir sunucuya ihtiyaç duymuyordu.
Temel Amaç: Müzik başta olmak üzere çeşitli dosya türlerinin (programlar, belgeler, videolar vb.) paylaşımını desteklemek.
Hukuki Sorunlar: Merkezi bir sunucusu olmaması, telif hakkı ihlallerini kontrol etmeyi ve yasal işlem yapmayı zorlaştırdı. Ancak yine de telif hakkı sahiplerinin baskısıyla karşılaştı ve geliştirilmesi durduruldu.
Sonuç: Limewire'ın geliştirilmesi durdurulsa da, Gnutella protokolü ve benzeri merkezi olmayan P2P teknolojileri varlığını sürdürdü.

Dağıtık sistemli uygulamalar

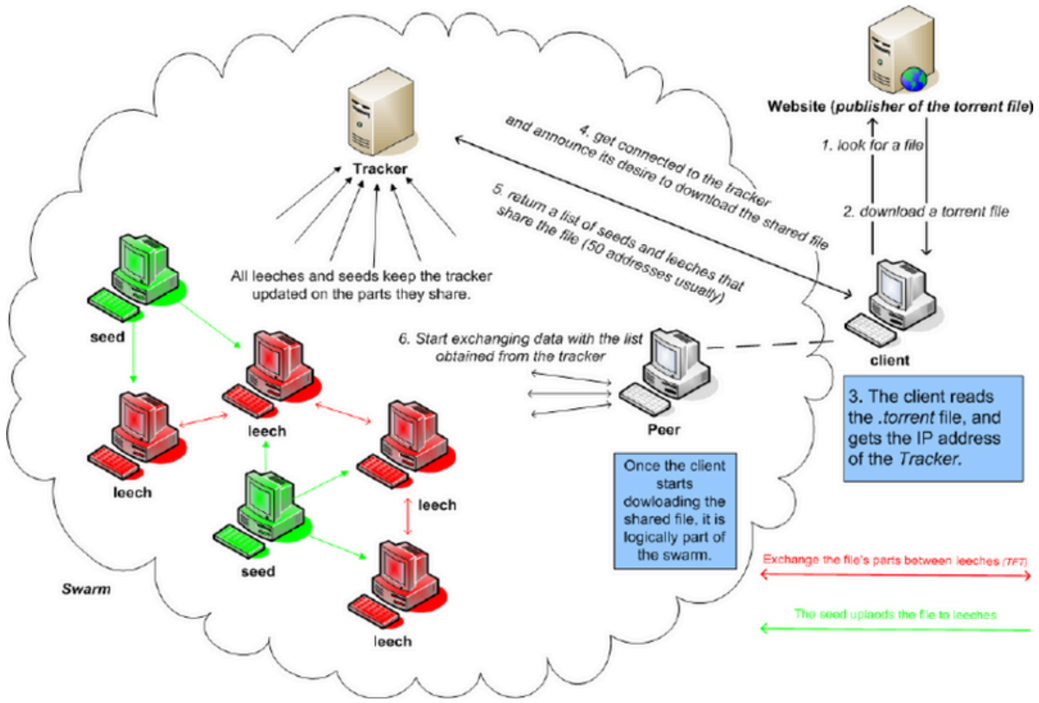


Telif hakları nedeniyle büyük davalarla karşılaştı ve 2001’de kapatıldı.

napster

LimeWire

Dağıtık sistemli uygulamalar

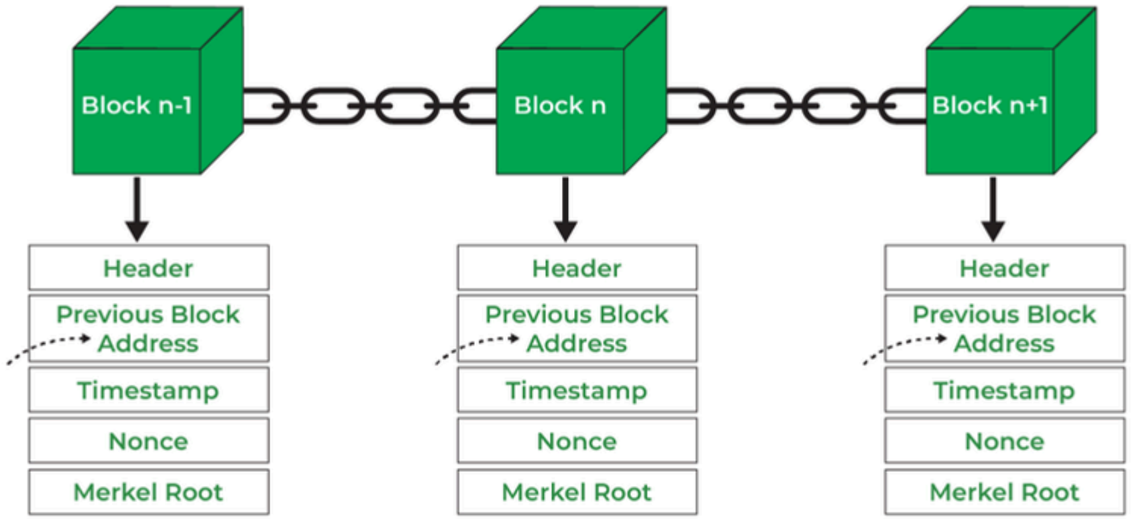


BitTorrent, büyük dosyaları küçük parçalara bölerek ve bu parçaları birçok kullanıcı arasında eş zamanlı olarak indirip yükleyerek daha hızlı ve verimli dosya paylaşımı sağlayan merkezi olmayan bir protokoldür.

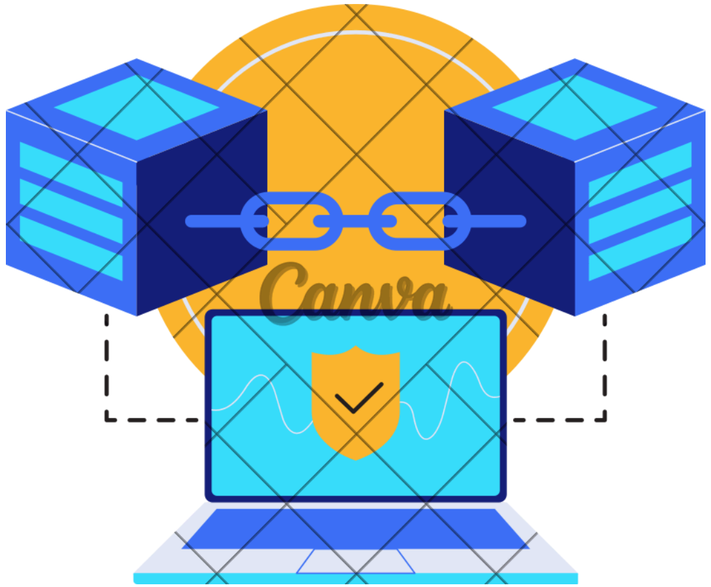
BitTorrent™

Blokzincir nedir? Nasıl çalışır?

Blokzincir (Blockchain), merkezi olmayan, dağıtık (distributed) bir defter teknolojisidir. Veriler bloklar halinde saklanır ve kriptografik olarak zincirleme bir şekilde birbirine bağlanır.
https://blockchaindemo.io/

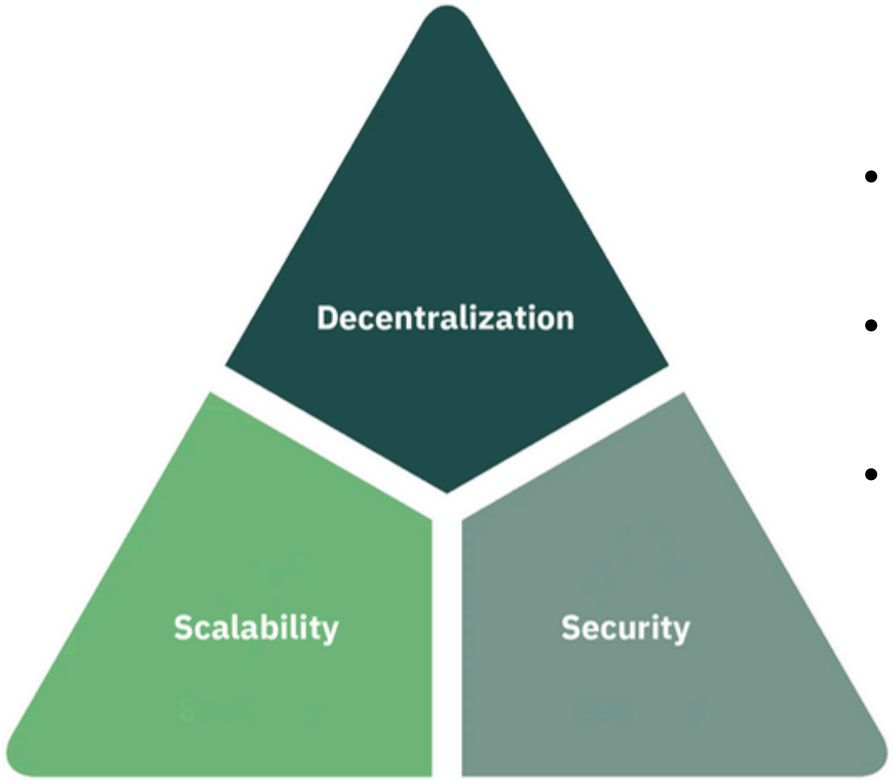


Blokzincir karakteristiği



Merkeziyetsizlik: Veriler, tek bir merkezde değil, tüm ağ katılımcılarında saklanır.
Şeffaflık: İşlemler herkes tarafından görüntülenebilir.
Güvenlik: Kriptografi ve konsensüs mekanizmaları sayesinde sahtecilik yapılması çok zordur.
Değiştirilemezlik: Kaydedilen işlemler geri alınamaz veya değiştirilemez.

Blokzincir karakteristiği



Blockchain Trilemma

Bu üç özellik aynı anda bir blokzincir çözümünde en üst seviyede olamaz, buna blockchain trilemma denir.

- **Merkeziyetsizlik ve Güvenlik Öncelikli:** Merkeziyetsiz ve güvenli blockchainler (örneğin Bitcoin, ilk Ethereum) genellikle ölçeklenebilirlik sorunları yaşar. Çok sayıda katılımcının konsensüse varması zaman alır ve işlem hızını düşürür.
- **Ölçeklenebilirlik ve Güvenlik Öncelikli:** Ölçeklenebilirliği artırmak için bazı blockchainler daha az sayıda ve daha güçlü doğrulayıcıya (daha merkezi bir yapıya) yönelebilir. Bu, güvenlikten ödün verilmesi riskini taşıyabilir.
- **Merkeziyetsizlik ve Ölçeklenebilirlik Öncelikli:** Merkeziyetsizliği korurken yüksek işlem hızı sağlamaya çalışan bazı projeler, güvenlik mekanizmalarında veya konsensüs algoritmalarında karmaşık çözümler uygulamak zorunda kalabilir, bu da potansiyel güvenlik açıklarına yol açabilir.

Blokzincirin tarihçesi ve gelişimi

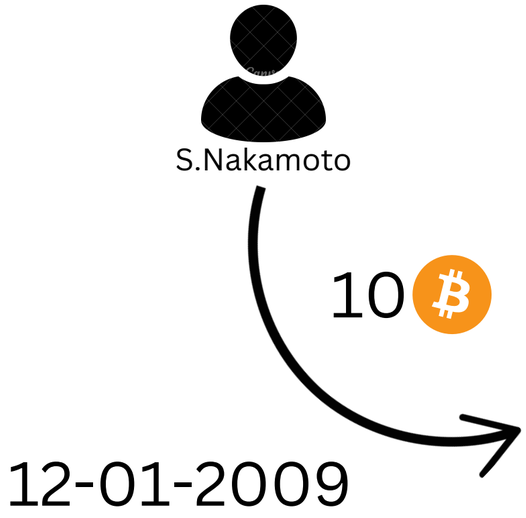
1976: Whitfield Diffie ve Martin Hellman, açık anahtarlı şifreleme (Public Key Cryptography / Asymmetric) kavramını tanıttı.

1979: Ralph Merkle, Merkle Ağacı (Merkle Tree) konseptini geliştirdi. Bu yapı, blokzincirin verileri bütünlükle saklamasını sağlayan temel yapılardan biridir.

1992: Stuart Haber ve W. Scott Stornetta, zaman damgalı (timestamped) değiştirilemez dijital kayıt sistemini tanıttı. Blokzincirin temelini atan fikirlerden biri oldu.

Ralph Merkle

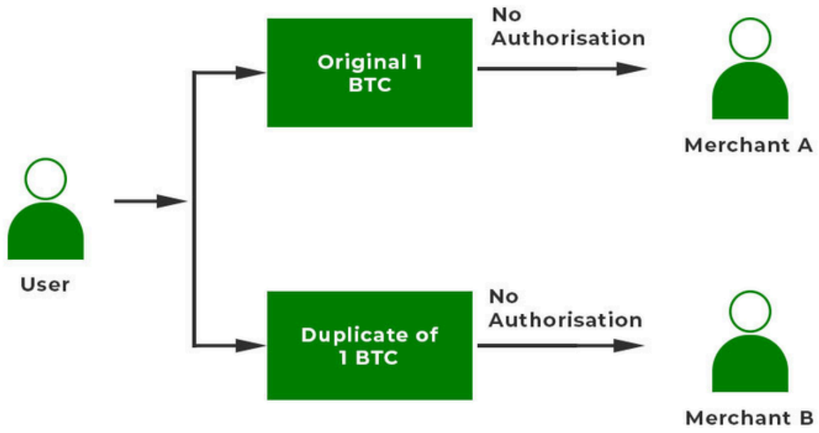
1990: David Chaum, merkezi olmayan dijital para fikrini içeren DigiCash'i geliştirdi.
1997: Adam Back, spam e-postalarla mücadele etmek için Hashcash adlı bir PoW (Proof of Work) algoritması geliştirdi. Daha sonra Bitcoin madenciliğinde kullanılan sistemin temelini oluşturdu.
1998: Wei Dai, merkeziyetsiz para birimi fikrini içeren b-money'yi önerdi.
2004: Hal Finney, yeniden kullanılabilir iş kanıtı (RPoW - Reusable Proof of Work) sistemini geliştirdi.




Hal Finney


David Chaum

Çifte harcama (Double Spending)



Çifte harcama, aynı parayı iki kez harcamadır. Bitcoin dijital olarak bu probleme çözüm getiren ilk projedir.

Bitcoin

🔸 **31 Ekim 2008:**
Satoshi Nakamoto takma adlı kişi veya grup, “Bitcoin: A Peer-to-Peer Electronic Cash System” başlıklı bir whitepaper yayınladı. Bu makale, blokzincir tabanlı merkeziyetsiz dijital para sistemini tanımlıyordu.

🔸 **3 Ocak 2009:**
Bitcoin’in ilk bloğu olan Genesis Block (Blok #0) madencilik yoluyla kazıldı.

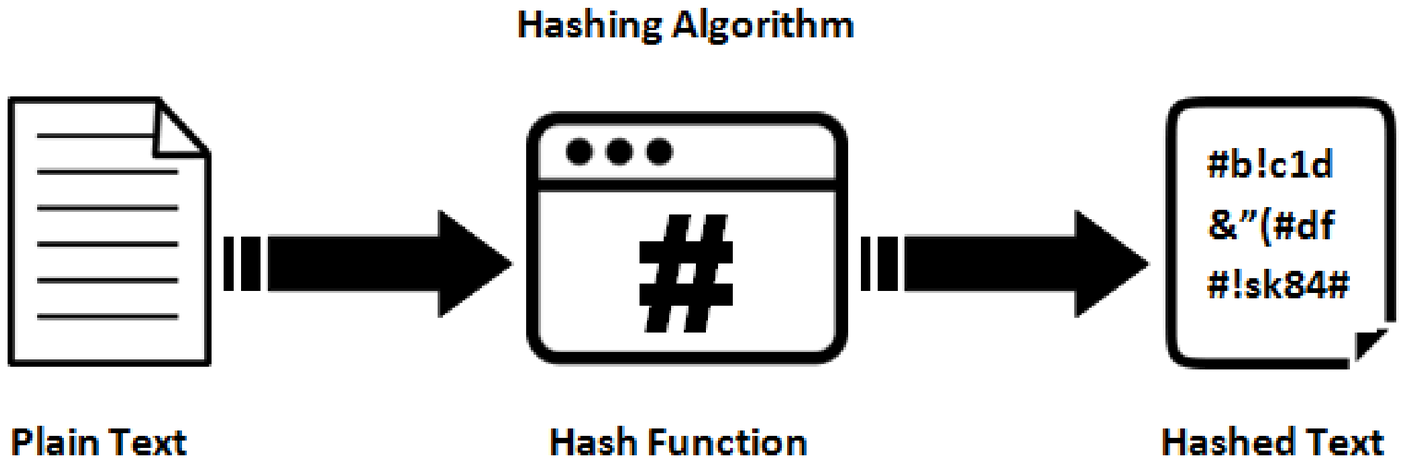
🔸 **12 Ocak 2009:**
İlk Bitcoin transferi gerçekleşti. Satoshi Nakamoto, Hal Finney’e 10 BTC gönderdi.

🔸 **22 Mayıs 2010:**
Tarihte ilk kez bir Bitcoin işlemi gerçek dünyada kullanıldı. Laszlo Hanyecz, 10.000 BTC karşılığında iki pizza satın aldı. Bu olay, her yıl “Bitcoin Pizza Günü” olarak kutlanıyor.

Kriptografik hash fonksiyonları

Hash fonksiyonu, herhangi bir giriş verisini sabit uzunlukta bir çıktıya (hash değeri) dönüştüren matematiksel bir algoritmadır.
Güvenli bir hash fonksiyonu, tek yönlüdür, yani giriş verisinden hash değerini üretmek kolaydır, ancak hash değerinden giriş verisini bulmak imkansıza yakındır.
Aynı giriş verisi her zaman aynı hash değerini üretir. Ancak, giriş verisindeki küçük bir değişiklik bile tamamen farklı bir hash üretir (Avalanche Effect).

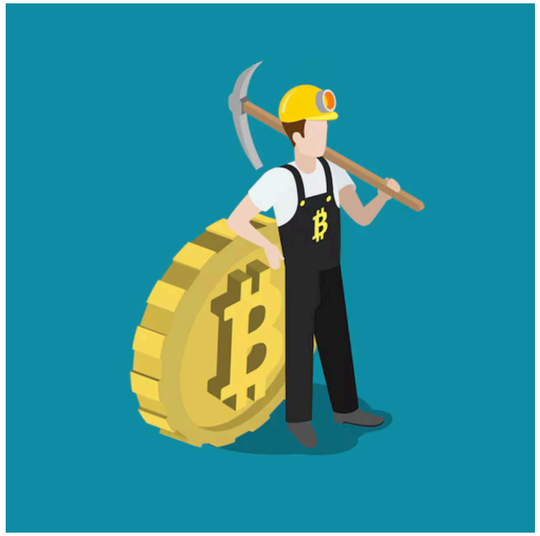
SHA-256, Keccak-256, SHA-3



Blokzincir ve madencilik kavramları

Bitcoin madenciliği, işlemleri bir araya toplayıp Nonce değerini bulmaktır. Bu süreçte brute force ile 0'dan sonraki değerler bulunur. Çok yüksek miktarda enerji harcanır.

SHA-256("Blok Verisi + Nonce") = 0000abcd1234xyz



Okuma: Bitcoin Whitepaper (Satoshi Nakamoto)
https://github.com/durmusgulbahar/blokzincir_egitim/tree/main/1.hafta

Blokzincir ve madencilik kavramları

Bitcoin ağına gönderilen işlemler, mempool (memory pool) adı verilen geçici bir bekleme alanında saklanır.

- Kullanıcılar Bitcoin gönderdiğinde, işlemleri öncelikle madenciler tarafından doğrulanır.
- Madenciler, mempool'daki işlemler arasından genellikle en yüksek işlem ücretine sahip olanları seçerek kendi blok adaylarını (candidate block) oluştururlar.
- İşlemler blok boyutu sınırına (1 MB) göre seçilir.

Blokzincir ve madencilik kavramları

Blok #15234
Önceki Blok Hash: 0000abcd1234xyz
Merkle Kökü: 89abcd567efg
Zaman Damgası: 1707563284
Nonce: 768342
İşlemler:
- Alice, Bob’a 2 BTC gönderdi
- Bob, Charlie’ye 0.5 BTC gönderdi

Bitcoin ağında blok yapısı