Blockchain Nedir?

Dağıtık sistemlerin giderek daha fazla yaygınlaştığı günümüzde, blockchain teknolojisi, bu sistemlerin en dikkat çekici uygulamalarından biri haline gelmiştir. Öyle ki, sadece finans değil, tedarik zinciri, sağlık, dijital kimlik ve daha pek çok alanda kullanılmaya başlanmıştır. Bu bölümde, blockchain'in temel yapısını, neden bir dağıtık sistem olarak değerlendirildiğini ve hangi özellikleri sayesinde popüler hale geldiğini ayrıntılı olarak ele alacağız.

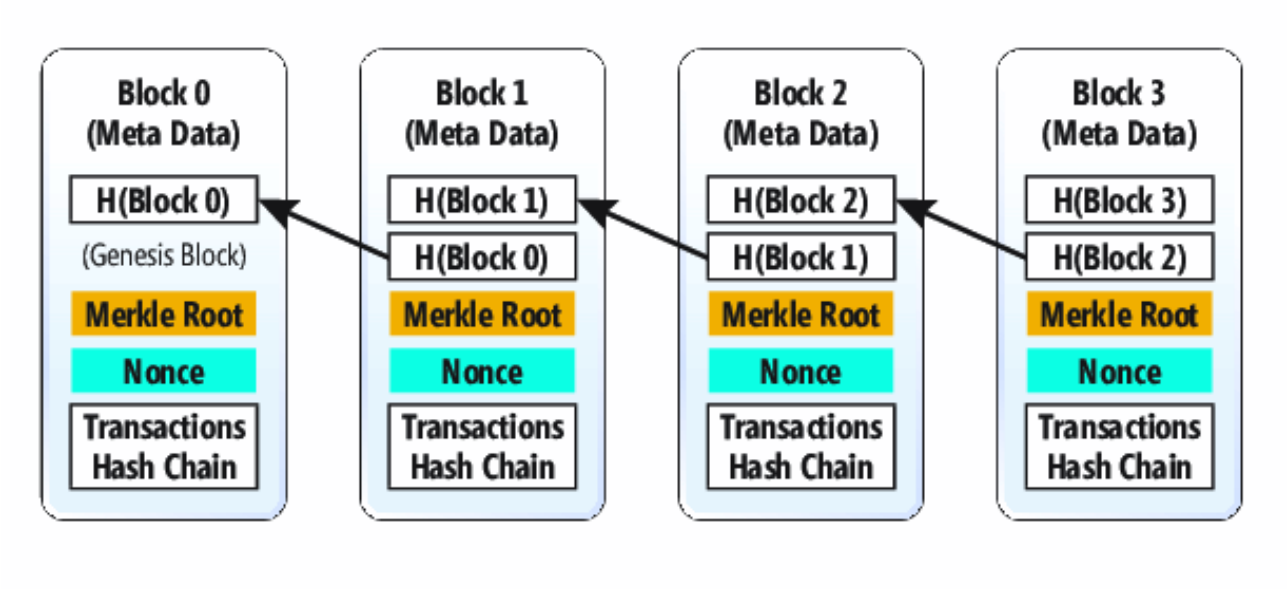
Blockchain, basit bir ifadeyle, dağıtık bir defter sistemidir. Geleneksel veritabanlarından temel farkı, verilerin merkezi bir sunucuda değil, ağdaki her bir katılımcının (düğüm) elinde bulunan kopyalarda saklanmasıdır. Üstelik bu kopyalar sadece bir yedekleme sistemi değildir; her biri sistemin bir parçası gibi tam yetkili şekilde çalışır ve ağ içindeki işlemleri doğrulamakta görev alır.

Bu yapıda bilgiler, blok adı verilen veri yapıları halinde gruplanır ve her blok, kendisinden önce gelen bloğun özet bilgisini yani kriptografik hash değerini içerir. Bu durum bloklar arasında bir zincir oluşmasına neden olur ve zincirin adını buradan alırız: Block-chain.

Bu noktada önemli bir özellik daha ortaya çıkar. Zincirin bir halkasına, yani bloklardan birine sonradan müdahale edilmeye çalışılırsa, hem o bloğun hash değeri, hem de ondan sonra gelen tüm blokların hash değerleri değişmek zorunda kalır. Böylece zincirin geri kalanını etkilemeden bir bloğu değiştirmek pratikte mümkün olmaz. Bu özellik, blockchain'in "değiştirilemezlik" (immutability) özelliğinin temel dayanağıdır.

Burada sistemin güvenliği sadece şifreleme ile değil, aynı zamanda yapının kendisiyle sağlanır. Yani zincirin uzunluğu ve yaygınlığı arttıkça sisteme saldırmak neredeyse imkânsız hale gelir. Dağıtık yapıda çalışan bu sistem, her bir düğümün doğrulama yapmasıyla güvenilirlik kazanır.

Özellikle vurgulamak gerekir ki, blockchain yalnızca bir teknolojik yapı değildir, aynı zamanda merkeziyetsizliği savunan bir felsefeye de sahiptir. Herhangi bir merkezi otoriteye ihtiyaç duymaksızın, sistem kendini sürdürebilir ve karar mekanizmaları dağıtık olarak çalışır. Sistemde her düğüm, veri tabanının güncel bir kopyasını tutar. Bu durum blockchain'in, tek bir düğümün veya sunucunun saldırıya uğraması durumunda bile çalışmaya devam edebilmesini sağlar.



Merkezi Olmayan Yapı

Blockchain'de her düğüm (node), veritabanının tamamının bir kopyasını tutar. Bu kopyalar birbirleriyle sürekli senkronize edilir. Böylece herhangi bir düğüm saldırıya uğrasa ya da devre dışı kalsa bile, sistem çalışmaya devam eder.

Bu yapı aynı zamanda otoriteyi tek bir merkezden alıp, katılımcılar arasında dağıtır. Ağın bütünlüğü, katılımcılar arasında yapılan uzlaşma (konsensüs) mekanizmasıyla sağlanır.

Konsensüs Algoritmaları

Konsensüs algoritmaları, blockchain ağında tüm katılımcıların (düğümlerin) hangi işlemlerin geçerli olduğuna dair ortak karar vermesini sağlayan protokollerdir. Farklı blockchain türlerinde farklı konsensüs algoritmaları kullanılır.

a) Proof of Work (PoW)

PoW algoritmasında, madenciler karmaşık bir matematiksel problemi çözmek için yarışırlar. Bu problem, SHA-256 gibi bir hash fonksiyonunun çıktısının belirli bir koşulu sağlamasını gerektirir:

SHA-256(blok verisi + nonce) < hedef değer

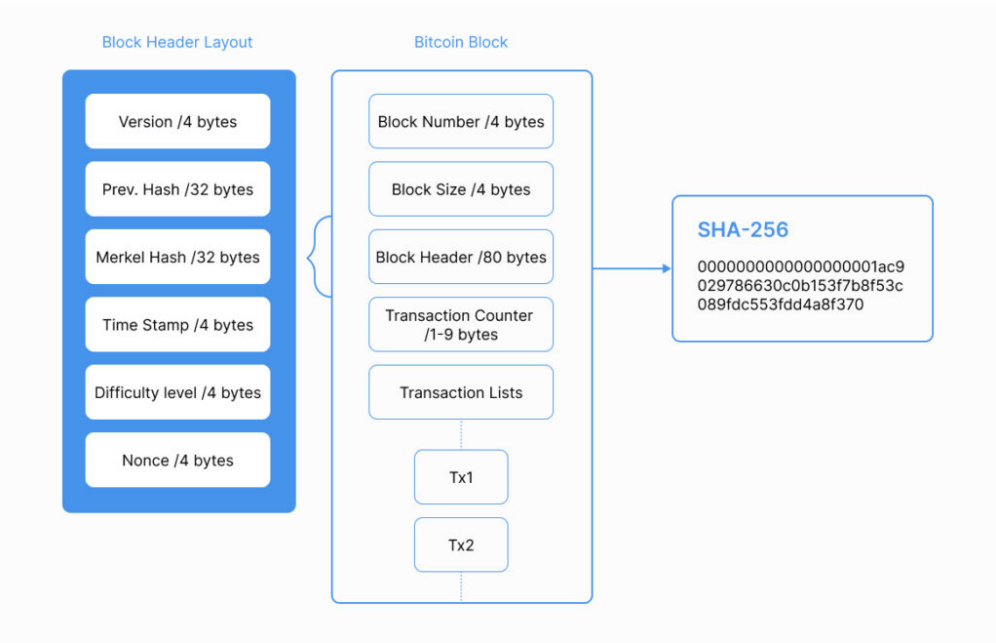
“Blok verisi”, yeni oluşturulacak bloğun içinde yer alacak tüm bilgilerin birleşimidir. Bu veri genellikle şu bileşenlerden oluşur:

1. Önceki Bloğun Hash’i (previous_block_hash): Bu, zincirdeki önceki bloğun SHA-256 hash değeridir. Zincir yapısının korunmasını sağlar.
2. Zaman Damgası (timestamp): Blok oluşturulma zamanını temsil eder. Unix zaman formatında verilir.
3. Merkle Kökü (merkle_root): Blokta yer alan işlemlerin hash’lenerek Merkle ağacında birleştirilmesiyle elde edilen kök hash'tir. Tüm işlemlerin özet bilgisidir.
4. Hedef Zorluk Seviyesi (target difficulty): O anki ağ zorluğunu temsil eden bir değerdir. Blok hash'inin bu değerin altında olması gerekir.

"nonce" değeri, madenciler tarafından sürekli değiştirilerek denenir. Uygun nonce bulunduğunda, blok kabul edilir ve ağın geri kalanına yayılır. Bu işlem hem zaman alıcıdır hem de yoğun hesaplama gücü gerektirir.

Bu zorluk, kötü niyetli bir aktörün ağı manipüle etmesini çok maliyetli hâle getirir. Sahte bir blok oluşturmak isteyen biri, hem mevcut hem de önceki tüm blokların hesaplamasını yeniden yapmak zorundadır. Dolayısıyla sistem, "hesaplama gücü" ile güvenliği garanti eder.

Alternatif olarak kura çekilse olmaz mıydı? Kura sistemi, düşük maliyetli olduğu için kötü niyetli aktörlerin sisteme saldırmasını kolaylaştırırdı. PoW ise saldırganlara karşı ekonomik caydırıcılık sağlar. Eğer biri ağı ele geçirmek istiyorsa, dünya üzerindeki toplam hesaplama gücünün %51’inden fazlasını kontrol etmesi gerekir. Bu da neredeyse imkânsızdır.



b) Proof of Stake (PoS)

PoS, enerji tüketimini azaltmak için geliştirilmiş bir alternatiftir. Bu sistemde madencilik yerine, kullanıcılar sahip oldukları kripto paraları "stake" eder. Stake kelimesi Türkçede *“pay, hisse, ortaya koymak”* anlamlarına gelir. PoS bağlamında bu, bir kullanıcının sahip olduğu kripto paranın bir kısmını ağa teminat olarak kilitlemesi anlamına gelir.

Bu kilitlenen miktar:

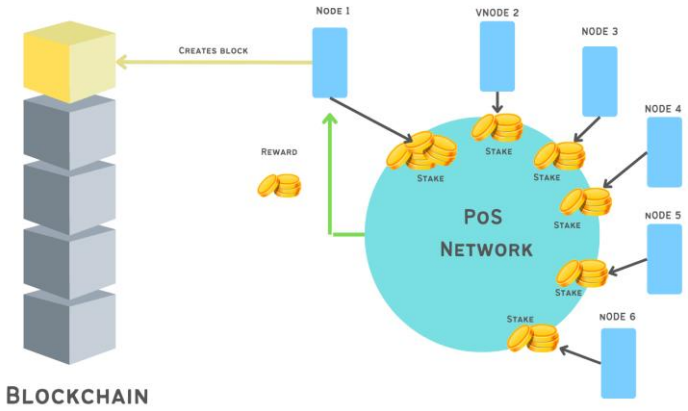
- Blok üretme hakkı kazanmak,
- Ağın güvenliğine katkıda bulunmak,
- Doğrulayıcı (validator) olabilmek

için kullanılır.

Blok üreticisi, stake miktarına göre rastgele seçilir:

Seçilme Olasılığı = Kişinin Stake miktarı / Toplam Stake

PoS sisteminde kötü niyetli davranışlar, stake edilen miktarın kaybıyla cezalandırılır. Böylece ağ katılımcıları dürüst davranmaya teşvik edilir.



c) PBFT (Practical Byzantine Fault Tolerance)

PBFT, özellikle özel (izinli) blockchain sistemlerinde kullanılan bir algoritmadır. Sistem, ağda en fazla hata toleransı için n>= 3f+1 düğüm gerektirir. Düğümler, mesajlaşma yoluyla üç aşamalı bir oylama yapar: pre-prepare, prepare ve commit. Bu protokol sayesinde sistem, bazı düğümler hata yapsa bile doğru kararlara ulaşabilir.

Dağıtık sistemlerdeki Byzantine Hata Problemi, bazı düğümlerin hatalı ya da kötü niyetli olduğu durumda bile sistemin doğru çalışmasını sağlamaya çalışır.

Bu sorun ilk kez "Bizans Generalleri Problemi" olarak ortaya konmuştur:

"Bir kale kuşatılmış. Kale çevresindeki generaller saldırı zamanında uzlaşmak zorunda. Ancak bazı generaller hain. Hainler diğerlerini yanıltmaya çalışıyor. Herkesin aynı kararda birleşmesi gerekiyor ama haberleşme de sadece mesajlarla oluyor."

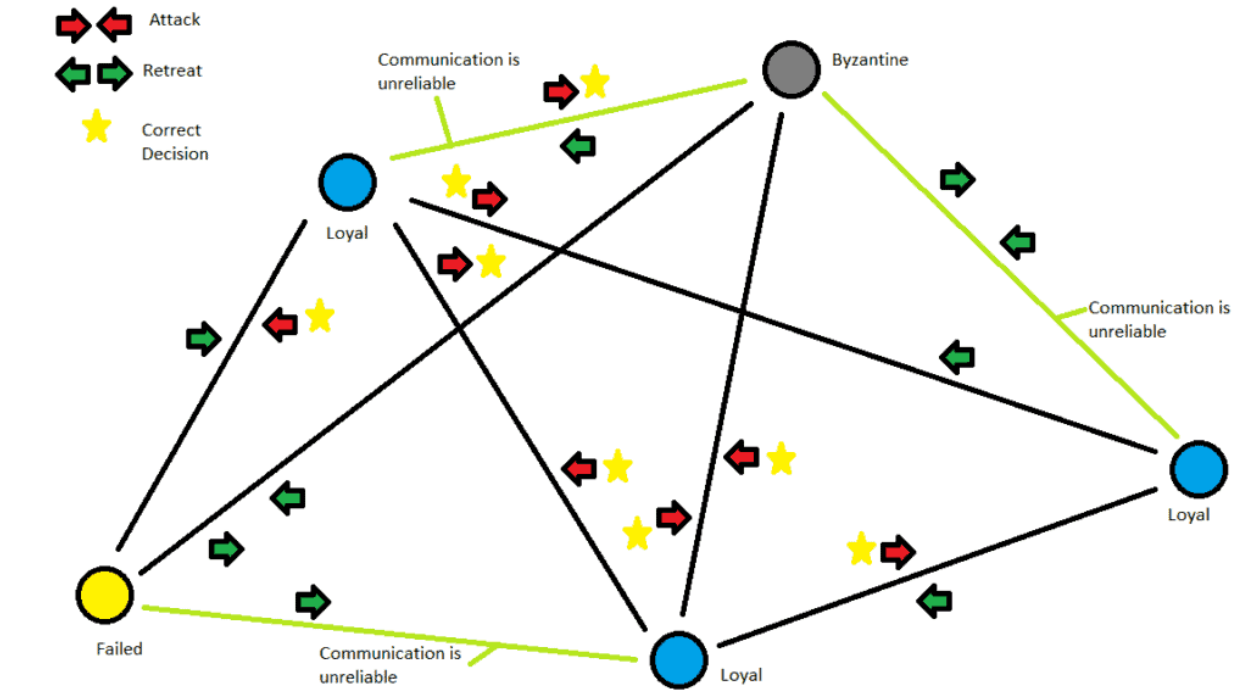
PBFT bu durumu çözmeyi hedefler: Ağda bazı düğümler yanlış bilgi verse bile doğru karara varılabilmesi.

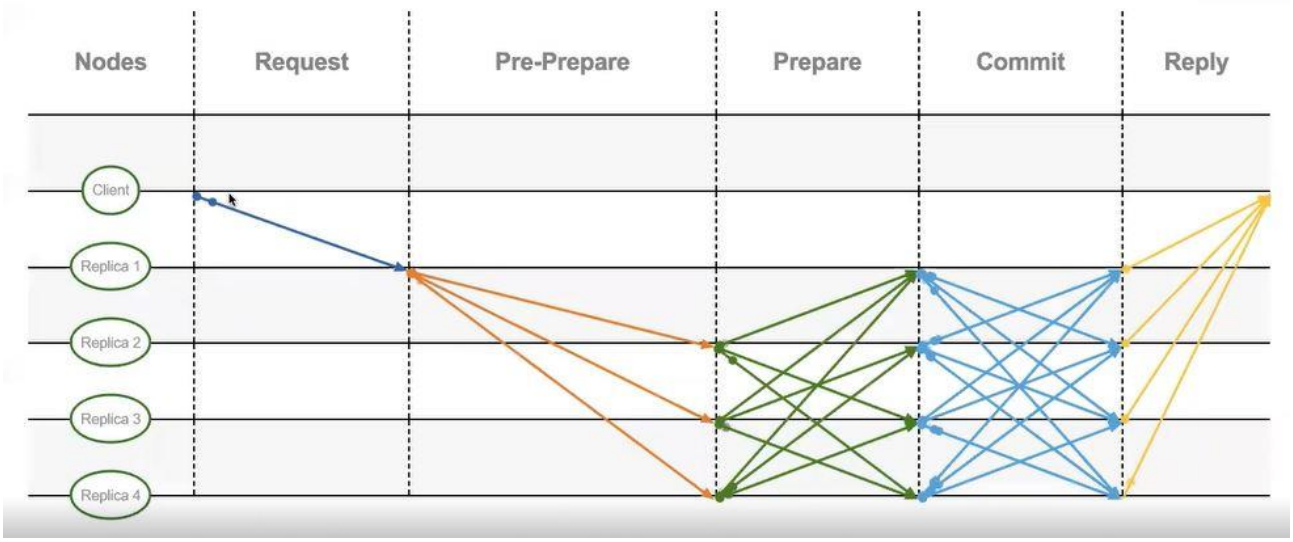
Ağda en fazla 'f' tane Byzantine (yani hatalı veya kötü niyetli) düğüm varsa, PBFT algoritması en az n = 3f + 1 düğüm gerektirir.

Örneğin:

- 1 hata (f = 1) toleransı isteniyorsa → en az 4 düğüm gerekir.
- 2 hata için → 7 düğüm.
- 3 hata için → 10 düğüm.

Bu matematiksel sınır, ağın güvenliğini garanti eder.





Akıllı Sözleşmeler

Akıllı sözleşmeler, blockchain üzerinde çalışan programlanabilir sözleşmelerdir. Belirli koşullar gerçekleştiğinde otomatik olarak işlem yaparlar. Bu sayede güvenilir üçüncü taraflara ihtiyaç kalmadan işlemler yürütülebilir.Akıllı sözleşmeler genellikle Ethereum gibi programlanabilir blockchain platformlarında Turing-tam sanal makineler (örneğin EVM - Ethereum Virtual Machine) üzerinde çalışır.

Bir akıllı sözleşme genellikle şunları içerir:

- Koşullar (if/else blokları)
- İşlemler (token transferi, veri güncelleme vs.)
- Olay kayıtları (events)

Örnek: Dijital Telif Hakkı Ödemesi (Müzik Yayın Platformu)

Diyelim ki blockchain tabanlı bir müzik dinleme platformu kurdun. Kullanıcılar şarkıları dinledikçe, sanatçılara ödeme yapılması gerekiyor. Bu süreci bir akıllı sözleşme ile tamamen otomatikleştirebilirsin.

Senaryo:

- Bir kullanıcı premium üyelik alıyor.
- Sisteme yüklenen her şarkı bir sanatçıya ait.
- Kullanıcının dinlediği her şarkı için sanatçıya mikro ödeme yapılacak.
- Tüm veriler blockchain üzerinde tutuluyor, sansürlenemiyor.

Akıllı Sözleşme Nasıl Olur?

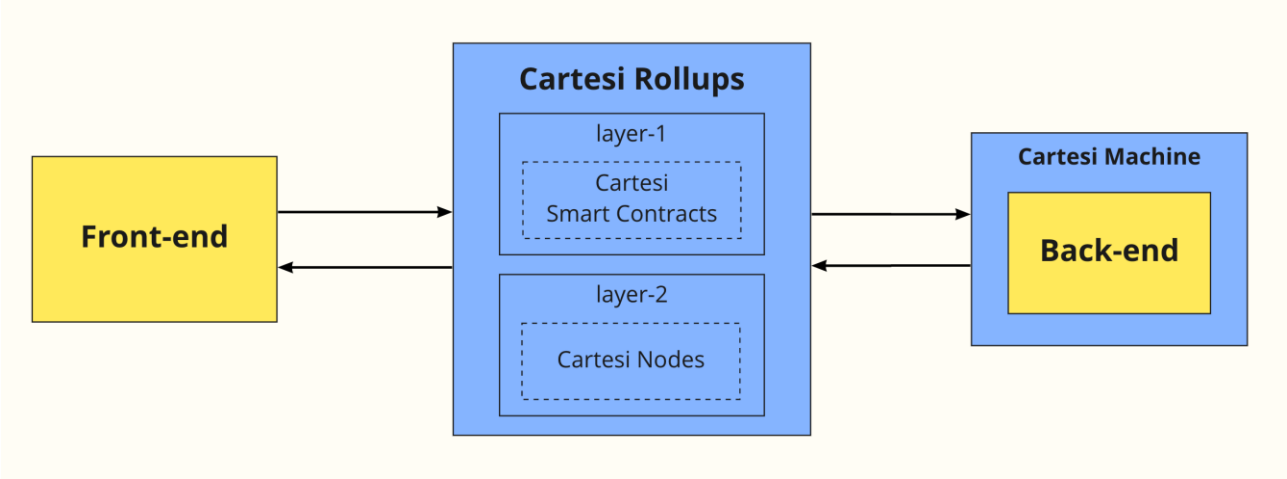
- Şarkı dinlenme sayısı arttıkça bir sayaç artar.
- Ay sonunda toplam dinlenme sayısına göre sistem her sanatçıya doğrudan ödeme yapar.
- Aracı yok, telif gecikmesi yok, itiraz yok.

dApp'ler (Decentralized Applications)

Akıllı sözleşmelerin üzerine inşa edilmiş uygulamalardır. Uniswap, Aave, OpenSea gibi uygulamalar bu tür sistemlere örnektir.

Yapısal Katmanlar

1. Frontend: Web tarayıcısında çalışan kullanıcı arayüzü (React.js, Vue.js vb.)
2. Akıllı Sözleşme Katmanı: Ethereum gibi ağlar üzerinde çalışan mantık.
3. Cüzdan Entegrasyonu: MetaMask gibi araçlarla kullanıcı kimlik doğrulaması ve işlem imzalama yapılır.



Blockchain'in Dağıtık Sistemlerle İlişkisi

Blockchain'in altında yatan yapı, dağıtık sistem prensipleriyle doğrudan ilişkilidir. Bu sistemler, fiziksel olarak farklı yerlerde bulunan bilgisayarların (düğümlerin) ortak bir amaç doğrultusunda birlikte çalışmasını esas alır. Blockchain bu modeli kullanarak verilerin hem yedekli hem de senkronize şekilde tutulmasını sağlar.

Dağıtık Güvenlik Modeli:

Blockchain ağı, her düğümün defterin bir kopyasını tutmasıyla çalışır. Bu sayede sistem, tek bir noktaya yapılacak saldırıya karşı dayanıklıdır. Ayrıca, kriptografi (özellikle dijital imzalar, hash fonksiyonları ve Merkle ağaçları) ile güvenlik sağlanır. Her işlem bir özel anahtarla imzalanır ve bu imza ağ tarafından doğrulanır.

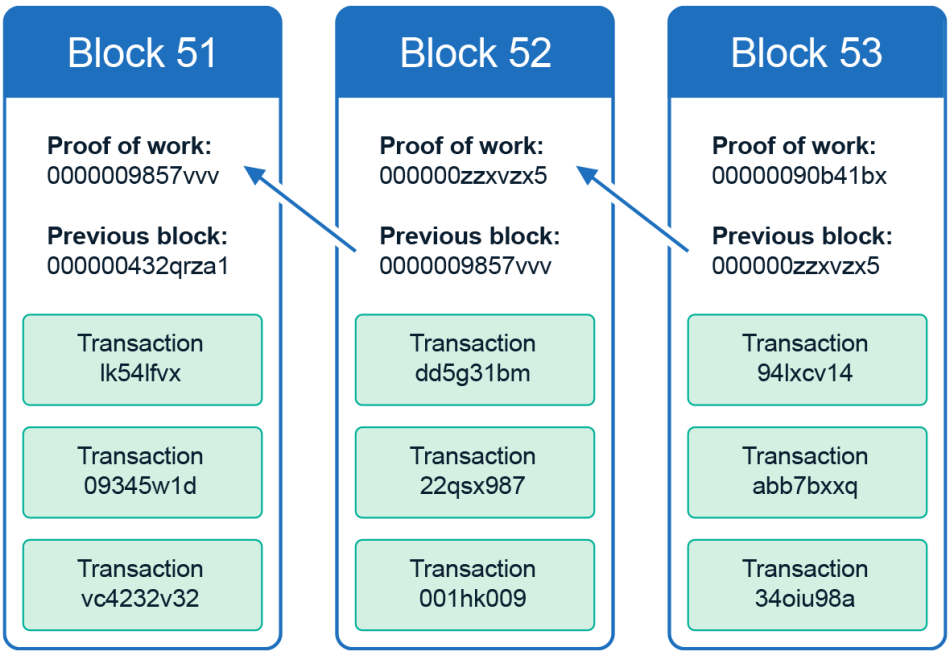
Örnek: Bir kullanıcının cüzdan adresi, onun açık anahtarıyla ilişkilidir. İşlem yapmak için kullanıcı, işlemi kendi özel anahtarıyla imzalar. Diğer düğümler bu imzayı doğrulayarak işlemin gerçekten o kullanıcıya ait olduğunu teyit eder.

Veri Değişmezliği (Immutability)

Blockchain'de veriler bloklara yazılır ve bu bloklar sırasıyla zincirlenir. Her blok, bir önceki bloğun hash değerini içerir:

Bu yapı sayesinde, zincirin ortasındaki herhangi bir veriyi değiştirmek, o bloktan sonraki tüm blokların hash değerlerini değiştirmeyi gerektirir. Bu da çok büyük hesaplama gücü gerektirdiği için pratikte mümkün değildir.

Örnek: Bir saldırgan, 100. bloktaki işlemi değiştirmek isterse, 101, 102, ... tüm blokların yeniden hesaplanması gerekir. Bu, PoW sisteminde neredeyse imkânsızdır.



Gerçek Hayat Kullanım Alanları

Blockchain teknolojisi, yalnızca teorik bir kavram olarak kalmamış; birçok sektörde somut uygulamalarla kendini kanıtlamıştır. Bu bölümde, blockchain'in en yaygın ve etkili kullanıldığı üç temel alanı detaylı şekilde ele alacağız.

Kripto Paralar

Blockchain'in en bilinen uygulaması şüphesiz kripto paralardır. Bitcoin, bu alandaki ilk örnek olup, merkezi bir otoriteye gerek duymadan dijital para transferini mümkün kılmıştır. Ethereum ise daha gelişmiş bir yapıyla yalnızca para transferi değil, programlanabilir sözleşmeler (akıllı sözleşmeler) de sunmuştur.

Bitcoin (BTC):

- 2009 yılında Satoshi Nakamoto tarafından geliştirildi.
- Maksimum arzı 21 milyon ile sınırlandırılmıştır.
- Her 10 dakikada bir yeni blok eklenir.
- Konsensüs algoritması: Proof of Work.
- Amaç: Merkeziyetsiz dijital para transferi.

Ethereum (ETH):

- 2015 yılında Vitalik Buterin ve ekibi tarafından başlatıldı.
- Turing-tam sanal makinesi sayesinde akıllı sözleşmeler çalıştırabilir.
- İlk olarak PoW kullandı, 2022'de Ethereum 2.0 ile PoS'a geçti.
- Amaç: Merkeziyetsiz uygulamalar (dApp) geliştirmek.

Matematiksel Not: Bitcoin'in arzı aşağıdaki formülle yaklaşık olarak hesaplanır:

$$\text{Toplam BTC} = 50 \times \sum_{i=0}^{n} \left(\frac{1}{2}\right)^i$$

Her 210,000 blokta bir ödül yarıya düşer.

Tedarik Zinciri Yönetimi

Tedarik zincirinde ürünlerin üretimden son kullanıcıya kadar olan yolculuğunun takibi oldukça karmaşık ve hataya açık bir süreçtir. Blockchain, bu süreci dijitalleştirip şeffaf ve güvenilir hâle getirir.

Nasıl çalışır?

- Her aşama bir blok olarak zincire eklenir.
- Bu bloklar ürünün hangi üretici, taşıyıcı veya perakendeci elinden geçtiğini belgeler.
- Her işlem, QR kod veya RFID ile gerçek zamanlı izlenebilir.

Örnek: IBM Food Trust, Walmart, Nestlé gibi büyük firmalar tarafından kullanılıyor.

Faydaları:

- Sahte ürünlerin tespiti
- Tüketici güveni
- Soğuk zincir takibi (ilaç, gıda vb.)

Dijital Kimlik Doğrulama

Blockchain, bireylerin kendi kimliklerini merkezi bir otoriteye ihtiyaç duymadan yönetebileceği yeni bir yaklaşım sunar: “self-sovereign identity” (kişisel egemen kimlik).

Geleneksel Sistem:

- Kimlik verisi devlet veya büyük kurumlarca saklanır.
- Bu merkezi sistemler siber saldırılara açıktır.

Blockchain Tabanlı Sistem:

- Kimlik verisi kullanıcının kontrolündedir.
- Veriler, blockchain üzerinde şifreli olarak saklanır.
- Doğrulamalar, “verifiable credentials” ile yapılır.

Örnekler:

- Estonya e-Residency
- Sovrin Network

Faydaları:

- Kimlik hırsızlığının önlenmesi
- KYC işlemlerinde hız ve güven