

Mutabakat Protokolleri

Mutabakat Protokolleri

1. Proof of Work (PoW) - İş Kanıtı
2. Proof of Stake (PoS) - Pay Kanıtı
3. Delegated Proof of Stake (DPoS) - Temsilci Pay Kanıtı
4. Proof of Authority (PoA) - Otorite Kanıtı
5. Byzantine Fault Tolerance (BFT) - Bizans Arıza Toleransı

Her bir mutabakat protokolünün avantajları ve dezavantajları vardır. Seçim, genellikle **kullanım durumuna**, **güvenlik** gereksinimlerine, **ölçeklenebilirlik** ihtiyaçlarına ve **enerji** verimliliğine bağlı olarak yapılır.

1. Proof of Work (PoW) - İş Kanıtı

- **Bitcoin** gibi ilk nesil blockchainlerde kullanılan PoW, düğümlerin yeni blokları oluşturmak ve işlemleri onaylamak için **karmaşık bir matematiksel bulmacayı** çözmesini gerektirir.
- Bu bulmacayı çözen **ilk düğüm**, bloğu ağa ekleyebilir ve bu süreçte **ödül** (yeni coinler ve işlem ücretleri) kazanır.
- PoW, **yüksek enerji tüketimi** nedeniyle eleştirilir.

1. Proof of Work (PoW) - İş Kanıtı

Karmaşık Bulmacalar: Madenciler, belirli bir kriptografik bulmacayı çözmek için **rekabet** ederler.

Bu bulmaca genellikle bir hash fonksiyonunun çıktısını hedef bir değerden daha küçük yapacak bir girdi bulmayı içerir.

Madencilik Zorluğu: Bulmacanın **zorluğu**, ağın üretim **hızını** kontrol etmek için **dinamik** olarak ayarlanır.

Bitcoin ağında, örneğin, her 2016 blokta bir (yaklaşık iki hafta) zorluk seviyesi yeniden ayarlanır. Bu, blok üretim hızını her 10 dakikada bir sabit tutmayı amaçlar.

1. Proof of Work (PoW) - İş Kanıtı

Ödüller: Bir **madenci** bulmacayı çözüp yeni bir blok oluşturduğunda, belirli miktarda kripto para birimi ile **ödüllendirilir**. Bu ödül, yeni dövüşülen tokenler ve **işlem ücretlerini** içerir.

Güvenlik: PoW, ağı 51% saldırısı gibi kötü niyetli girişimlere karşı korur. Bu tür bir saldırıyı başarılı bir şekilde gerçekleştirebilmek için, ağın yarısından fazlasının hash gücünü kontrol etmek gerektirir, bu da **maliyet** açısından oldukça **yüksektir**.

Enerji Tüketimi: PoW'un eleştirilen yönlerinden biri, **özellikle büyük kripto para ağlarında**, çözümü bulmak için gereken yoğun hesaplama gücünün **büyük miktarlarda enerji** tüketmesidir.

2. Proof of Stake (PoS) - Pay Kanıtı

- PoS, düğümlerin yeni bloklar oluşturmak için belirli bir miktarda coin'i "**bahis**" olarak kilitlediği bir mekanizmadır.
- Sahip olunan **coin miktarı** ve coinlerin **ne kadar süredir** kilitli olduğu gibi faktörlere bağlı olarak, bir düğümün yeni blok oluşturma ve **ödül kazanma şansı artar**.
- PoS, daha **az enerji tüketimi** ile daha **çevreci** bir alternatif olarak görülür.

2. Proof of Stake (PoS) - Pay Kanıtı

Enerji Verimliliği: PoS, PoW'a kıyasla çok daha **az enerji** tüketir çünkü karmaşık matematiksel bulmacaları çözmek için büyük miktarda **işlemci gücü gerektirmez**.

Daha Fazla Güvenlik: PoS, ağa saldırmak isteyenlerin **büyük miktarda kripto para** birimine sahip olmalarını ve bu **yatırımı riske atmalarını** gerektirir, bu da **saldırıların maliyetini** artırır.

2. Proof of Stake (PoS) - Pay Kanıtı

Daha Fazla Ölçeklenebilirlik: Daha **düşük** işlem onay **maliyetleri** ve **enerji** gereksinimleri nedeniyle, PoS sistemleri daha **yüksek işlem hacimlerini** ve daha **hızlı onay sürelerini** destekleyebilir.

Daha Adil Ödül Dağılımı: PoS, zenginleşme eğilimi yerine daha adil bir **ödül dağılımı** sağlayabilir, çünkü ödüller sahip olunan **miktar ve süreye** göre dağıtılır.

3. Delegated Proof of Stake (DPoS) - Temsilci Pay Kanıtı

- DPoS, coin sahiplerinin temsilcileri (delegeleri) **oylama** yoluyla seçtiği bir sistemdir.
- Bu temsilciler, **ağdaki işlemleri onaylamak ve yeni bloklar oluşturmak** için sorumludur.
- DPoS, daha **hızlı işlem onay süreleri** ve ölçeklenebilirlik sunar.

3. Delegated Proof of Stake (DPoS) - Temsilci Pay Kanıtı

Oylama ve Delege Seçimi: DPoS sistemi, token sahiplerinin, **belirli bir süre için** ağın işlem doğrulama sürecini yönetecek temsilcileri (delegeleri) seçmek üzere **oylarını kullanmalarına** izin verir.

Token sahiplerinin **oylama gücü**, sahip oldukları **token miktarına** bağlıdır.

Bu, sahiplerin ağ üzerindeki **paylarına orantılı olarak söz sahibi** olmalarını sağlar.

3. Delegated Proof of Stake (DPoS) - Temsilci Pay Kanıtı

Blok Üretimi ve Doğrulama: Seçilen delegeler, ağdaki işlemleri **doğrulamak** ve blokları **üretmekle** sorumludur.

Her delegenin, **belirli bir zaman** diliminde bir **blok üretme sırası** vardır.

Bu, blok üretiminin daha **öngörülebilir ve düzenli** olmasını sağlar.

3. Delegated Proof of Stake (DPoS) - Temsilci Pay Kanıtı

Ödüller ve Cezalar: Doğru şekilde blokları üreten ve işlemleri **doğrulayan delegeler**, ağ tarafından **ödüllendirilir**.

Bu **ödülleri**, genellikle yeni üretilen tokenler ve **işlem ücretlerinden** oluşur.

Delegelerin kötü davranışları veya **görevlerini yerine getirmemeleri** durumunda, token sahipleri onları oy kullanarak **görevden alabilirler**.

Bu, delegelerin ağın sağlığı ve güvenliği için **sorumlu davranmalarını** teşvik eder.

3. Delegated Proof of Stake (DPoS) - Temsilci Pay Kanıtı

DPoS'un Avantajları

Enerji Verimliliği: DPoS, PoW'un aksine, madencilik için **büyük miktarda elektrik tüketimine ihtiyaç duymaz**, bu da onu daha **çevre dostu** bir alternatif yapar.

Ölçeklenebilirlik: DPoS, işlemleri daha **hızlı doğrulayabilir** ve blokları daha **hızlı üretebilir**, bu da ağı daha **yüksek işlem hacimlerini** desteklemesine olanak tanır.

Daha Fazla Kullanıcı Katılımı: Token sahipleri, ağdaki değişiklikler ve güncellemeler hakkında **oy kullanarak** doğrudan **söz sahibi** olabilirler.

3. Delegated Proof of Stake (DPoS) - Temsilci Pay Kanıtı

DPoS'un Dezavantajları

Merkezileşme Riski: Çok sayıda tokena sahip olan kullanıcılar, daha fazla oylama gücüne sahip olabilir ve bu da ağ üzerinde aşırı bir etkiye yol açabilir.

Delege Seçiminde Taktikler: Oylama sistemi, belirli delegelerin manipülasyonuna veya kartel oluşturmaya açık olabilir.

4. Proof of Authority (PoA) - Otorite Kanıtı

- PoA, güvenilir ve **önceden onaylanmış düğümlerin** (yetkililerin) ağdaki işlemleri **onayladığı** bir sistemdir.
- Bu protokol, özellikle özel blockchainlerde popülerdir ve **hızlı işlem** onay süreleri ile **düşük enerji** tüketimi sağlar.

4. Proof of Authority (PoA) - Otorite Kanıtı

- Temel Özellikler
- **Güvene Dayalı:** PoA, belirli doğrulayıcıların (validatorların) **kimliklerinin açık ve şeffaf** olmasına dayanır. Bu doğrulayıcılar genellikle **kimlikleriyle tanınır** ve yüksek **güvenilirliğe** sahip bireylerdir veya kuruluşlardır.
- **Enerji Verimliliği:** PoA, Proof of Work (PoW) gibi enerji yoğun konsensüs mekanizmalarına kıyasla **çok daha az enerji tüketir** çünkü karmaşık matematiksel problemleri çözmek yerine **güvenilir doğrulayıcıların onayıyla** işlemler gerçekleştirilir.

4. Proof of Authority (PoA) - Otorite Kanıtı

- Temel Özellikler
- **Performans ve Ölçeklenebilirlik:** PoA, işlem onay süreçlerinin hızlı olması nedeniyle yüksek **işlem hızları** ve **düşük gecikme süreleri** sunar.
- Bu, özellikle **işlem hacminin yüksek olduğu uygulamalarda** önemlidir.

4. Proof of Authority (PoA) - Otorite Kanıtı

Avantajları

- Yüksek **işlem hızı** ve düşük **gecikme süresi**.
- **Enerji** verimliliği ve **çevresel** sürdürülebilirlik.
- Güvenilir ve **şeffaf** doğrulayıcılar aracılığıyla **yüksek güvenlik** seviyesi.

Dezavantajları

- Merkeziyetçilik: Güvenilir **doğrulayıcıların seçilmesi**, sistemde belirli bir derecede **merkeziyetçiliğe yol açabilir**.
- Sınırlı katılım: Doğrulayıcı olarak hizmet vermek için **önceden seçilmiş** olmak gerektiğinden, ağa **katılım sınırlıdır**.

5. Byzantine Fault Tolerance (BFT) - Bizans Arıza Toleransı

- BFT, ağdaki düğümlerin **bir kısmı kötü niyetli** olsa bile, ağın doğru bir şekilde **çalışmaya devam edebilmesini** sağlayan bir protokoldür.
- **BFT varyasyonları** arasında Practical Byzantine Fault Tolerance (**PBFT**) ve Federated Byzantine Agreement (**FBA**) bulunur.

5. Byzantine Fault Tolerance (BFT) - Bizans Arıza Toleransı

BFT'nin Temel Prensipleri

- **Konsensüs:** Sistemdeki **tüm düğümler** (örneğin, bilgisayarlar, sunucular), bir karara (örneğin, bir işlemin geçerliliği) varmak için **birlikte çalışmalıdır**.
- **Güvenilirlik:** BFT mekanizmaları, **birkaç düğüm arızalı** olsa veya kötü niyetli davranırsa bile, **sistem genelinde doğru çalışmayı** sürdürebilmelidir.
- **Esneklik:** Sistem, **çeşitli arıza türlerine** (yazılım hataları, donanım arızaları, kötü niyetli saldırılar vb.) karşı **dayanıklı** olmalıdır.