

# ZELDHASH PROTOKOLÜ

**Bitcoin'in En Nadir İşlemlerini Avlayın ve ZELD Kazanın.**

Yazan: Ouziel Slama

## 1 Motivasyonlar

- Avın heyecanı için. Her işlem, nadir bir şey keşfetme fırsatına dönüşür — blockchain'de herkesin gözü önünde gizlenmiş dijital bir hazine.
- Bu öncü sıfır kalıpları sadece nadir değil — aynı zamanda sıkıştırmayı geliştirebilir, potansiyel olarak blockchain depolama ve işleme verimliliğini optimize edebilir.
- Herkes nadir işlemleri avlayarak ZELD kazanabilir — Bitcoin blok madenciliğindeki gibi blok başına tek kazanan yok. Av herkese açık.
- Başarılı olursa, ZELD tokenleri sonunda işlem ücretlerini geri ödeyebilir — en nadir bulguları ortaya çıkarılan avcılar ödülünlendirir!

## 2 ZELD Madenciliği

ZELD madenciliği yapmak için txid'i en az 6 sıfırla başlayan bir Bitcoin işlemi yayımlamalısınız. Ödül, işleminizin bloktaki en iyi işlemle nasıl karşılaşıldığını göre hesaplanır:

- Belirli bir blokta, en çok sıfırla başlayan işlemler 4096 ZELD kazanır
- En iyi işlemlerden bir sıfır daha az olan işlemler 4096/16 veya 256 ZELD kazanır
- İki sıfır daha az olan işlemler 4096 / 16 / 16 veya 16 ZELD kazanır
- vb.

Bu nedenle kullanılan formül şu şekildedir:

```
reward = 4096 / 16 ^ (max_zero_count - zero_count)
```

Burada `max_zero_count` en iyi işlemi başlatan sıfır sayısına eşittir ve `zero_count` ödülünü hesapladığımız işlemi başlatan sıfır sayısıdır.

**Not:** Coinbase işlemleri ZELD ödülleri için uygun değildir.

## 3 ZELD Dağıtıımı

6 veya daha fazla sıfırla başlayan bir işlemle kazanılan ZELD'ler UTXO'lara dağıtilır. Dağıtım şu şekilde yapılır:

- Tek bir OP\_RETURN olmayan UTXO varsa, tüm ödülü alır.
- İki veya daha fazla OP\_RETURN olmayan UTXO varsa, ödül sonucusu hariç tüm UTXO'lara her UTXO'nun değeriyle orantılı olarak dağıtılır
- Hesaplamlar yalnızca tam sayılarla yapıldığından, bölümün olası kalanı ilk OP\_RETURN olmayan UTXO'ya dağıtılır.

Örneğin, 256 ZELD kazanan bir işlem sırasıyla 500, 500, 500 ve 2000 Satoshi içeren 4 çıktı içeriyorsa, ilk çıktı ödülün 86 ZELD’ini, ikinci ve üçüncüsü 85 ZELD alır.

## 4 ZELD Taşıma

Ekli ZELD’leri olan UTXO’lar harcanırken, ZELD’ler işlemdeki yeni UTXO’lara dağıtılr. ZELD’leri taşırken dağıtmak için iki yöntem vardır:

### 4.1 Yöntem 1: Otomatik Orantılı Dağıtım

Varsayılan olarak, dağıtım ödüllerle tamamen aynı şekilde yapılır – çıktı UTXO’larının Bitcoin değerlerine göre orantılı olarak, birden fazla çıktı varsa son çıktı hariç tutulur.

### 4.2 Yöntem 2: OP\_RETURN ile Özel Dağıtım

Özel dağıtım verileriyle işleminize bir OP\_RETURN çıktısı ekleyerek ZELD’lerin tam olarak nasıl dağıtılması gerektiğini belirtebilirsiniz. Bu, ZELD transferleri üzerinde hassas kontrol sağlar.

#### 4.2.1 OP\_RETURN Formatı:

- OP\_RETURN betiği 4 baytlık “ZELD” önekiyle başlayan veriler içermelidir
- Önekten sonra veriler CBOR formatında kodlanmalıdır
- CBOR verileri işaretsiz 64-bit tam sayı vektörünü (Vec) temsil etmelidir
- Her tam sayı, ilgili çıktı UTXO’suna kaç ZELD gönderileceğini belirtir

#### 4.2.2 Dağıtım Kuralları:

- Dağıtım dizisindeki değer sayısı, OP\_RETURN olmayan çıktı sayısıyla eşleşecek şekilde otomatik olarak ayarlanır
- Dizi çok uzunsa, fazla değerler kaldırılır
- Dizi çok kısaysa, sıfırlar eklenir
- Dağıtım değerlerinin toplamı, harcanmakta olan toplam ZELD miktarını aşamaz
- Bu toplam, genel toplamdan azsa, fark ilk çıktıya eklenir
- Bu toplam, genel toplamı aşarsa, işlem orantılı dağıtıma geri döner
- Yeni madencilik yapılan ZELD ödülleri her zaman orantılı olarak dağıtılır ve ardından özel dağıtımla birleştirilir

#### 4.2.3 Örnek:

3 çıktıya dağıtmak için 1000 ZELD’iniz varsa ve birincisine 600, ikincisine 300 ve üçüncüsüne 100 göndermek istiyorsanız, OP\_RETURN’ınız “ZELD” ve ardından [600, 300, 100]’ün CBOR kodlamasını içerecektir.

#### Notlar:

- Geçerli bir OP\_RETURN dağıtımını bulunamazsa, işlem otomatik olarak orantılı dağıtım yöntemini kullanır.
- Bir işlem yalnızca bir OP\_RETURN çıktısı içeriyorsa, işlem girdilerine ekli herhangi bir ZELD **ve** yeni kazanılan herhangi bir ödül kalıcı olarak yakılır çünkü bunları alacak harcanabilir çıktılar yoktur.

- Birden fazla OP\_RETURN çıktısı mevcut olduğunda, dağıtım için yalnızca işlemde en son görünen ve geçerli ZELD+CBOR yükü taşıyan çıktı dikkate alınır.