

BITCOIN & BLOCKCHAIN - II

İlk videoda verdiğimiz bir örnek vardı; Ali, Bora'ya 2 Bitcoin gönderiyordu.

İşte böyle bir işlem için gönderenin ve alıcının bir hesabı olması gerekiyor. Bitcoin dünyasına adım attığımızda başlangıçta bir hesap oluşturursunuz. Buna dijital cüzdan deniyor. Bu cüzdanın güvenliği de şifre ile yani kriptolojiyle sağlanır. Her cüzdanın iki anahtarı vardır. Biri özel, biri de genel. Özel anahtar size özeldir ve sadece siz kullanabilirsiniz. İmza gibi, ama taklidi imkânsız. Ali, Bora'ya 2 Bitcoin göndereceği zaman bunu önce özel anahtarı ile şifreliyor. Sonra da genel anahtarıyla birlikte Bitcoin ağına gönderiyor. Ağdaki kayıtçılar, genel anahtarı kullanarak işlemin doğruluğunu kontrol eder. Eğer genel anahtar Bitcoin ağında onaylanırsa, gönderilen mesajın herhangi bir Ali'den değil de bizim Ali'den geldiği kanıtlanmış olur. Kimlik kontrolü bu şekilde yapılır.

Peki diyelim ki Ali'nin cüzdanında sadece 2 Bitcoin vardı ve bununla da benden bir araba satın aldı. Sonra da gidip 1 Bitcoin daha harcamaya kalkıştı. Normalde bu işi bankadaki parasıyla yapmaya çalışsaydı, ikinci alışverişe izin verilmezdi çünkü bankacılık sistemi onun sahip olduğu tüm parayı önceden harcadığını bilirdi. Yani paranın kime ait olduğu kadar ne zaman harcandığı da önemli. Bitcoin dünyasında bir harcama ya da başka bir deyişle para transferi yapmak istediğinizde sistem önceki sahip olduğunuz miktarı ve bugüne kadar yaptığınız tüm transferleri kontrol etmek zorunda. Ancak bu şekilde o anda ne kadar Bitcoin sahibi olduğunuzu bilebilir. Dünyada bu kayıtların pek çok yerdeki dijital defterlerde ve çok sayıda tutulduğunu söylemiştik. Aynı anda pek çok transfer yapılıyor ve çeşitli bloklara farklı kayıtlar düşülüyor. Yani dijital defterlerde karmakarışık gerçekleşen kayıtların bir düzene sokulması gerekir. Bu işlemi, çözülmesi oldukça zor bir matematik problemine benzetebiliriz.

Bitcoin dünyasında her bir para işlemi için böyle bir matematik problemi çözülüyor.

Bu problemler kriptografik yani şifreli bir algoritma tarafından üretiliyor. Bu şifrelenmiş problemi çözmek için, uygun donanım ile güçlendirilmiş bir bilgisayar, yaklaşık 10 dakika boyunca çalışır. Fakat buna benzer milyarlarca problemin çözülmesi gerektiğini düşündüğümüzde, bu hiç de kısa bir süre değil. O yüzden şu anda dünyada pek çok kişi donanım gücü çok yüksek bilgisayarları kullanarak daha fazla sayıda problem çözmeye çalışıyor. Buna da Bitcoin madenciliği deniliyor.

Bitcoin madenciliği, oldukça pahalı bir iş. Uygun donanım ve yazılım yatırımının yanında, madencilik için harcadığımız enerjinin maliyeti de oldukça yüksek seviyede. Peki insanlar, neden bu kadar zorlu ve yüksek bir maliyete katlanıyor? Bu işi hayrına mı yapıyorlar?

Tabi ki hayır, Bitcoin sisteminde bir ödül mekanizması var. Eğer bu problemleri çözerek sistemdeki kayıtların güvenli şekilde tutulmasına yardım ederseniz, yeni Bitcoin'ler oluşturuluyor ve hesabınıza aktarılıyor. Aynı altın madeninde yeni altın bulmak gibi. Ancak burada önemli bir durum var. Dünyada altın az bulunduğu için değerli ama daha ne kadar çıkacağı da belli değil. Para da öyle. Basılmaya devam ediliyor. Bitcoin madenciliğindeyse paradan ve altından farklı olarak ne kadar üretilbileceği konusunda kesin ve net bir sınır var. 21 milyon Bitcoin üretilecek. Şu ana kadar 17 milyona yakın Bitcoin üretilmiş ama üretmesi gittikçe zorlaşıyor çünkü sistem bu şekilde tasarlanmış. Tahminlere göre en son Bitcoin 2140 yılında üretilecek. Böyle sınırlı sayıda ve zor üretilbilir olduğu için, şu an inişli çıkışlı bir seyir izlese de uzun vadede belirli bir değeri koruyacağı öngörülmüyor.

Peki bir KOBİ olarak, “Biz bu işin neresindeyiz?” “Bu işten nasıl etkileneceğiz? gibi sorularınıza da şöyle bir yanıt vereyim:

- Blockchain teknolojisi, birçok sektörü derinden etkileyecek. Muhtemelen sizin faaliyet gösterdiğiniz sektör de bundan nasibini alacak. Eğer sektörünüzde iş yapış şekli, araçlarla çalışmayı gerektiriyorsa, ya da siz bizzat aracı olan bir konumdaysanız, noter, emlakçı, komisyoncu gibi, o zaman işinizin dinamiklerinin hızlıca değişmesine hazır olmalısınız.
- Ne mi yapabilirsiniz? İşte size uygulanabilir bir yol haritası:
 - Önce, burada aktardığımız teknolojilerin sağladığı katma değeri iyice kavramalısınız
 - Ardından, bu katma değerın hangi kritik sorunları çözmeye kullanılabileceğini değerlendirmelisiniz.
 - Bulduğunuz kritik sorunların çözümü için sektör temsilcileriyle bir araya gelerek bir komite oluşturabilirsiniz.
 - Komite olarak teknik konular için güvenilir ve yetkin bir çözüm ortağı ile beraber proje geliştirebilirsiniz.
 - Bu konuda kritik olan unsur, geliştireceğiniz projeyi, öncelikle küçük bir bölgede denemeniz ve anlamlı sonuçları aldıktan sonra yaygınlaştırmanızdır.

Bitcoin ve ardından gelen Ethereum, Ripple, Litecoin ve 1400 civarı kripto para biriminin hepsi, içinde bulunduğumuz dijitalleşen ve globalleşen çağın ihtiyaçları sonucu ortaya çıkmış durumda. Ancak burada asıl dikkat çeken unsur, kripto paraların temelindeki Blockchain teknolojisinin, araçları ortadan kaldırarak parayı yeniden tanımlaması. Yani Bitcoin için söylemek zor ama Blockchain teknolojisi, modern dünyanın en önemli buluşlarından birisi olabilir. İçinde bulunduğumuz günlerde Blockchain’e olan yaklaşımı, 1990’ların ortasında hayatımıza giren internete olan yaklaşıma benzetebilirsiniz. O zamanlarda da internete oldukça şüpheli yaklaşıyordu ama şu an geldiğimiz noktada, internetin hayatımıza etkisine baktığımızda, benzer bir etkiyi, çok daha kısa süre içinde Blockchain ve benzeri teknolojilerden görebiliriz.