Kuantum Bilişim Bitcoin'i Bitirir mi?

Erman Akdoğan [*Yapay Zeka & Bulut Bilişim Lideri IBM (Şikago, ABD)*

Bitcoin kurunda son birkaç aydır önemli dalgalanmalar oluyor. 2017 yılının Aralık ayında 1 Bitcoin'in fiyatı inanılmaz bir artışla 20.000 dolara ulaştı. Bu sadece 2017'de %2000'den fazla bir artış demek. Böyle bir patlayışla değerlenen bir para biriminin arkasında bir hükümet yok ya da değerli madenle, örneğin altınla da garantilenmiyor. Tüm değeri insanların duyduğu güvenden ve sınırlı sayıda üretilmesinin garanti olmasından geliyor. Peki bu yerinde bir güven mi, Bitcoin'in zayıf yanları yok mu?

Bitcoin Nedir ve Nasıl Üretilir?: Bitcoin 2009 yılında Satoshi Nakamoto takma isimli kişi tarafından yaratılmış bir kripto para birimi. Bu kişinin kim olduğu hâlâ bilinmiyor. Bitcoin hiçbir aracı olmadan kişiden kişiye doğrudan transfer edilebilir. Gönderim kaynağını ve alıcıyı tespit etmek zordur, hesaplarınızı sizden başka kimse kontrol edemez ve hesaplarınıza el koyamaz. Bitcoin üretmek için bilişim madenciliği yapmanız gerekir. Madencilik yapmak için çok iyi bir ekran kartına ve bilgisayara ihtiyaç vardır. CPU yani işlemci ile de madencilik yapılabilir, ancak günümüz şartlarında bu hayli verimsiz olur. Çünkü sadece bu iş için özel makineler üretildi, dünyanın bir çok yerinde büyük "Bitcoin tarlaları" kuruldu. Üretilecek Bitcoin sayısı da belli. Toplam 21 milyon üretilecek ve bugüne kadar yaklaşık 16 milyonu üretildi. Üretim hızını ve enflasyonunu kontrol edebilmek için madenciliğin zorluk seviyesi her gün belirli protokoller çerçevesinde artıyor.

bitcoin

Ana Kurlar		Ana Kurlar - Hesaplama	
1 Bitcoin kaç Türk Lirası	=31.888,3523	100 Bitcoin kaç Türk Lirası	=3.188.835,23
1 Bitcoin kaç Dolar	=8185,3155	100 Bitcoin kaç Dolar	=818.531,55
1 Bitcoin kaç Euro	=6624,3513	100 Bitcoin kaç Euro	=662.435,13
1 Bitcoin kaç Pound	=5872,8820	100 Bitcoin kaç Pound	=587.288,20
1 Bitcoin kaç İsviçre Frangı	=7744,5363	100 Bitcoin kaç İsviçre Frangı	=774.453,63

Bitcoin kurunda son birkaç aydır önemli dalgalanmalar oluyor.

Bu seviyeler ağdaki üretim yoğunluğuna göre belirleniyor.

Kuantum Bilişim Nedir?: Klasik bilişim sistemleri bit'ler üzerine yani 0'lar ve 1'ler üzerine kurulu. Bit yani *binary digit* "ikilik sistemde basamak" demek. Kuantum bilgisayarlarda da ikilik sistem kullanılıyor, ancak bit yerine kubit (qubit=kuantum bit) kullanılıyor. Klasik bilgisayarlarla kuantum bilgisayarlar arasındaki temel fark, klasik fizik ile kuantum fiziği arasındaki temel farka dayalı. Klasik bilgisayarlarda bir bit kesinlikle ve sadece 1 veya 0 olabilirken, kuantum bilgisayarlarda bir kubit 1'in ve 0'ın çok farklı kombinasyonlarından oluşabilir. Kuantum bilgisayarların en basit olanı bile hâlihazırdaki en güçlü süper bilgisayardan kat be kat daha hızlı olacak. IBM bir iki yıl içinde satışa sunulabilir kuantum bilgisayarlar üreteceğini açıkladı. Google da 2000 kubitlik bir kuantum bilgisayar üreteceğini duyurdu.

Kriptografi ve Bitcoin: Kriptografi çok karmaşık bir bilgi şifreleme mekanizmasıdır. Genel olarak asal sayılarla ilgili matematiksel işlemlere ve denklemlere dayanır. Bu matematik işlemlerini bir yönde yapmak kolay, ters yönde yapmak (yani denklemi çözmek) çok ama çok zordur. Kriptografi Bitcoin'in âdeta belkemiğidir. Bitcoin'in kopyalanmasını ya da çalınmasını engelleyen temel iki güvenlik mekanizması vardır ve ikisi de kriptografiye dayanır.

Kuantum bilgisayarlar Bitcoin'in güvenliğini sağlayan ve günümüzdeki bilgisayarlarla çözülemeyen matematiksel denklemleri gayet rahatça çözebilir. Dahası ilk kuantum bilgisayarlar kullanıma açılmaya başladı bile! IBM'in ürettiği kuantum bilgisayara bulut bilişim vasıtası ile erişip işlem yaptırabiliyorsunuz. Mevcut bilgisayarlarla çözülmesi yüz yıllar sürebilecek bir kriptografik denklem, kuantum bilgisayarlarla bir kaç saatte çözülebilecek gibi görünüyor.

Üretim açısından bakıldığında ise bir kuantum bilgisayarın sahte Bitcoin üretilebilecek duruma gelmesine 10 yıl kaldığı düşünülüyor. Tüketim açısından ise durum biraz daha vahim. Bitcoin'i sadece sahibinin harcamasını sağlayan kriptografi mekanizması daha güçsüz. Bu mekanizmanın 2027'den önce kuantum bilgisayarlar tarafından kırılması çok muhtemel. Bu olursa, Bitcoin'lerin harcanma mekanizması çökeceğinden piyasası da tamamıyla çökebilir. Böyle bir durumda üretim tarafının hâlâ güvenlikli olması da tabii hiçbir şey ifade etmez. Bahsettiğimiz riskler hemen hemen tüm kripto para birimleri için geçerlidir. ■

Kaynaklar

https://www.wired.com/2017/03/race-sell-true-quantum-computers-begins-really-exist/

https://www.nature.com/news/d-wave-upgrade-how-scientists-are-using-the-world-s-most-controversial-quantum-computer-1.21353

http://bitcoin.tlkur.com