thinktech
STM Teknolojik Düşünce Merkezi

Zaman Makinesi İcat Olmak Üzere: Kuantum Blok Zincir

Blok zincirleri, üzerinde, geçmişe ait kayıtların tutulduğu bir veritabanıdır. Örneğin finansal işlemler gibi arşivlerin, sistemdeki diğer zincirler üzerinde merkezi bir kurum gerektirmeden etkileşime geçtiği bir ağ olarak da adlandırılabilir. Blok zincirlerin adını en sık duyduğumuz uygulaması Bitcoin'dir. Ancak bugün yeni kurulan teknoloji şirketlerinde ve mevcut büyük teknoloji kurumlarında bu veritabanının diğer potansiyel kullanım alanları da araştırılıyor.

IEEE Spectrum sitesindeki bir habere göre, Yeni Zelanda Wellington Üniversitesinden teorik fizikçi yazar Del Rajan, "Küresel sermayenin yüzde 10'luk kısmının 2027 yılına kadar blok endüstrisi üzerinde depolanması bekleniyor" diyor[1].

Süreç şimdilik blok zincirler için olumlu ilerlese de yakın zamanda blok zincirlerinin güvenliğini tehdit edebilecek diğer bir teknoloji olan kuantum bilgisayarlar da hızla gelişmeye devam ediyor. Günümüzde kullandığımız klasik bilgisayarlar veriyi transistörlerinde ancak 0 ve 1 olarak sembolize ediyor, bir nevi açıp kapıyor. Kuantum bilgisayarlarda ise durum farklı, kuantum fiziğinin sürreal doğasına göre çalışan sistemde aynı anda hem 1 hem 0 durumunda olabilen kuantum bitleri (kübitler) bir süperpozisyon yaratıyor.

Süperpozisyon Nedir?
Süperpozisyon kısaca bir kuantum sisteminin aynı anda birden farklı halde olabilme yeteneği olarak adlandırılabilir. Bu yetenek sistem bir gözlemci (bu bir sensör olabilir) tarafından gözlemlenene kadar geçerlidir.

Süperpozisyonun bu yeteneği bir kübitin aynı anda iki işlem yapabilmesine olanak tanıyor. Bu bitler "dolaşıklık" etkisi ile birbirine bağlandığında örneğin iki kübit, 2 üzeri 2 işlemi aynı anda yapabiliyor. Üç kübit 2 üzeri 3, yani 8 işlemi aynı anda gerçekleştiriyor. Bu prensipten hareketle 300 kübitli bir kuantum bilgisayar görülebilir evrendeki atomlardan bile daha fazla sayıda işlemi anında gerçekleştirebilir hale geliyor. Yeterince güçlü bir kuantum bilgisayar bugünün geleneksel şifreleme yöntemlerini ya da blok zincirlerini istendiğinde başarıyla kırabilir.

Kuantum Blok Zinciri Korsanlara Karşı Koyabiliyor
Yeni Zelanda'daki araştırmacılar bu sistemleri deneysel olarak çalıştırarak bazı bulgular elde ediyor. Araştırmalara göre bir kuantum blok zinciri, kuantum bilgisayarlarca denenecek korsanlık girişimlerine karşı koyabiliyor.

1 https://spectrum.ieee.org/tech-talk/computing/networks/quantum-blockchains-could-act-like-time-machines

Fizikçi Rajan IEEE Spectrum'a verdiği demeçte, "Kuantum operasyonlarıyla uyumlu çalışan blok zincirler zaten mevcuttu ancak ilk kez saf bir kuantum blok zinciri geliştirildi" diyor[2].

Kuantum blokları, teorik olarak dolaşıklık prensibine dayanıyor. Bu prensipte örneğin foton parçacıkları gibi iki ya da daha çok parçacık ne kadar uzakta olurlarsa olsunlar birbirine etki edebiliyor. Einstein bu fenomeni "uzaktaki ürküten eylem" olarak adlandırmıştı.

Dolaşıklık prensibi kriptografi için iki tarafı da keskin bir bıçak. Gelecekte kuantum bilgisayarlar, günümüzün en güçlü kriptografisini kırabilme potansiyeline sahip olacak. Kuantum bilgi teknolojisi, ABD ve Çin gibi hükümetler ve IBM, Intel ve Microsoft gibi teknoloji devleri, büyük bütçeli kuruluşlar tarafından sürekli takip ediliyor.

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından 2018'in Ocak ayında yayınlanan "Blok Zinciri Teknolojisine Genel Bakış" adlı raporda, yakın zamanda geliştirilebilecek kuantum bilgisayarların, mevcut kriptografik algoritmaları büyük ölçüde zayıflatabileceği ve bazı durumlarda yararsız hale getirebileceği belirtiliyor.

Bloklar Zaman İçinde Dolaşımla Bağlanıyor

Kuantum teknolojileri, genellikle bilinen uzayda bir dolaşıma dayanıyor, buna mesafeler arası parçacık etkileşimi de denebilir. Kuantum blok zincirleri ise zaman içinde dolaşlıklığı hedefliyor, iki parçacık zamanda birbirlerinden ne kadar uzak olurlarsa olsunlar bu yeni durumda etkileşime geçebilirler.

Geleneksel blok zinciri veriyi kronolojik olarak şifreliyor. Bir siber korsan belirli bir bloğu kurcalayıp şifreyi kırmaya çalıştığında blok zincirin yapısı, kurcalanmış bloğu takip eden tüm gelecek bloklar geçersiz kılınacak şekilde tasarlanıyor.

Kuantum blok zincirinde, bir bloktaki kayıt birbiriyle dolaştırılmış bir dizi foton içine kodlanıyor ve bu bloklar zaman içinde dolaşım yoluyla kronolojik sırada bağlanıyor. İşin içine zaman kavramı girince durum biraz karışıyor ancak şöyle söylenebilir: Kuantum blok zincirini oluşturan bloklar, bir kuantum ağı içine transfer edilince her bloğu kodlayan yeni fotonlar oluşuyor. Daha sonra foton parçacıkları ağ tarafından absorbe ediliyor ve zaman düzleminde farklı noktalara yayılıyorlar. Rajan, "Geçmiş işlemlere ilişkin veri kayıtları zamana yayılan bir kuantum halinde kodlanır" diye ekliyor[3]. Bu açıdan bakıldığında bir korsan geçmişte yer alan bir foton kaydına müdahale edemiyor çünkü bu fotonlar ağ tarafından absorbe edilmiş oluyor. Bilgisayar korsanlarının bu noktada yapabilecekleri en güncel foton kaydına yani en güncel bloğa ulaşabilmek ve onu kırmaya çalışmak olabilir. Bu da sadece o bloğu geçersiz kılmasına yol açar.

Kuantum blok zincirini oluşturan bloklar bir kuantum bilgisayar ağı içinde transfer edildiğinden, her bloğu kodlayan fotonlar oluşturulur ve daha sonra ağı oluşturan düğümler tarafından emilir. Bununla birlikte, dolanma, bu fotonları zamana bağlar, hatta aynı anda hiç bulunmayan fotonları bile.

Araştırmacılara göre bir bloktaki son fotonun ölçülmesi ve üzerinde işlem yapılması bu bloğun birinci fotonunu henüz o foton ölçülmese de etkileyecek. Aslında bir kuantum blok zincirindeki kayıt, bloğun kendi geçmişiyle bağlı olmaktan ziyade, geçmişte bir ana bağlı oluyor ki o an artık var olmadığına göre bu çalışma prensibi bir zaman makinesine benzetiliyor.

[2] https://spectrum.ieee.org/tech-talk/computing/networks/qbitcoin-making-bitcoin-quantumcomputer-proof
[3] https://spectrum.ieee.org/tech-talk/computing/networks/quantum-blockchains-could-act-like-time-machines