BLOCKCHAIN

Doç. Dr. Mustafa ERGEN
mergen@ku.edu.tr

Blockchain mantalite olarak merkezi sistemler yerine dağıtık mekanizmaların kullanılmasını amaçlayan, yani bir anlamda merkezi bir otoriteye bağımlılığı gideren bir metottur. Örneğin bankacılık sistemimiz şu anda merkezi otorite üzerine kurulu bir sistemdir. Biz banka adı altında akredite bir kuruma güveniriz, onlar kayıt defterlerine kimin ne kadar parası olduğunu yazar ve para transferlerinde o kayıt defterlerini güncellerler. Diyelim ki birisi banka kayıt defterini değiştirdi. Değiştiren iz bırakmazsa geri dönüşü olmayan bir şekilde paramız başka bir hesabın altına taşınmış olur. Bunu banka içinden biri de yapabilir, dışardan bilgisayar sistemlerini kullanarak giren birileri de bu şekilde bir kaos yaratabilir. Ya da örneğin bir şekilde bankanın veri merkezleri ve kopya yerleri zarar gördü veya fiziksel saldırıya uğradı. O bankada paramız olduğunu nasıl ispat ederiz? Yıllarca her yeni geliştirilen teknoloji banka sistemini daha güvenilir yapmak üzere inovasyon yaptı. Devletler banka sistemini daha güvenilir yapmak üzere yasal düzenlemeler çıkarttı. Sistem daha da merkezileşti. Fakat diyelim ki, devletler saldırı altına girdi ve başka devletler tarafından işgal edildi. Vatandaşın parasının güvenliğini nasıl sağlayabiliriz?

Örneğin, bankadaki kayıt defterlerini sadece banka değil de her hesap sahibi tutabilse ileride bankaya olacak bir saldırı akabinde bu defterleri bir hesap sahibi doğrulayabilir. Ama bu sefer bir hesap sahibinin herkesin verilerini bilmesinin önüne geçmemiz gerekir ve her para yatırmada, çekmede veya transferde herkesin elinde bulunan kayıt defterlerini güncellemesi gerekmektedir. Ayrıca bu durumda bu transferi yapan iki kişi işlemin başarılı bir şekilde gerçekleştiğinden emin olmalılar. Bir anlamda ilk olarak kendimizi tanıtıyoruz ve sistem bize belli konular yapma konusunda izin veriyor. Örneğin banka bizim kim olduğumuza kani olursa bankada bizim adımıza olan hesapta işlem yapmamıza izin veriyor. Yani diyor ki, sen gerçekten söylediğin kişi misin? İkinci olarak yapmak istediğin işlem için yetkin var mı? Diyelim ki böyle bir mekanizma yarattık. Bankaya gerek kaldı mı?

Blockchain işte bu kayıt defterini herkesin tutmasını sağlayan Dağıtık Kayıt Defteri (Distributed Ledger Protocol) protokolüdür.

Herhangi bir merkezi otoriteye bağlı olmadan güvenliğin sağlandığı bir mekanizmadır. İlk olarak elektronik para (BitCoin) için kullanılmaya başlanmıştır. Şimdi para transferi yerine akıllı kontrat (Etherium gibi...) mekanizmaları ile hayatın birçok alanında genişletilmeye çalışılmaktadır.

Aslında blockchain bir anlamda hâlihazırda varolan teknolojilerin bir arada kullanılmasıyla oluşturulan bir mekanizmadır. Blockchain'de üç farklı teknoloji kullanılmaktadır: internet, asimetrik şifreleme (public/private key kriptolama) ve özetleme (hash) fonksiyonları.

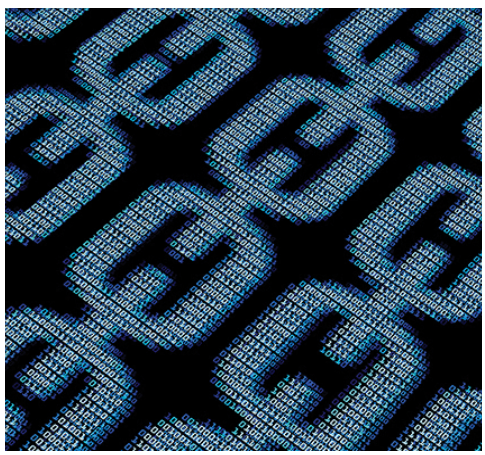
Bir kişi para bekliyor ise yapacağı ilk iş bir adres yaratmak olacaktır. Bu aslında hususi şifreye tekabül eden umumi şifredir. Hususi şifre cüzdanda saklanır. Cüzdan dijital olabileceği gibi bu şifre kağıta da yazılarak saklanabilir. Umumi olan kısmı bir anlamda banka hesabına eşdeğerdir. Burada yalnız bir den fazla hesap vardır. Neredeyse her işlem bir hesapta tutulur. Yani kişilerin birden fazla hususi şifreleri vardır. Ve her şifre kayıt defterinde miktarı gözüken bitcoine işaret eder. Banka hesabı yaratmak için imzalamamız gereken sayfalarca sözleşmeden ziyade bir web sayfasında kimlik bilgisine ihtiyaç olmadan yaratılan umumi/hususi şifreler yeterlidir. Kişi, hususi kısmı kendinde kalacak şekilde yarattığı umumi şifreyi karşı tarafa gönderir. Karşı taraf ise göndereceği para miktarı

ve bu adresi, göndereceği paranın umumi şifresi ile şifreler ve herkese iletir. Herkes bu mesajı alır ve doğruluğunu gönderenin hususi şifresi ile açarak anlar. Herkes yani bir anlamda umumi şifreli bir hesaba ne kadar bitcoin gönderildiğini anlamış olur. Burada kritik kısım bunun kayıt altına alınmasıdır; aksi halde aynı kişi aynı şifre ile birden fazla kişiye aynı parayı gönderebilir. Bunun için kayıt defteri 10 dakikalık zaman damgalı bloklar oluşturur ve dünyanın her yerinden "madenci" diye tabir edilen kişiler bu blokları özetleme algoritmaları ile işlemeye başlar. Her blok, bir önceki bloktaki özetleme sonucunu kullanarak yenisinin yapılarak eklenmesi demektir. Normalde özetleme algoritmaları kolayca işlenebilmesine rağmen blockchain teknolojisinde sonucun belli bir sayıda 0 ile başlaması istenir. Bunun için bir değişken parametre (nonce) girdi olarak konulur. İşte madencilerden hangisi bu özellikte bir sonuç buluyorsa o kazanmış olur ve yeni bloku eskilerine ekleyerek herkese yayınlar. Ödül olarak ise madenciye belli sayıda bitcoin verilir. İlk başta bunun için 50 bitcoin veriliyorken şimdi bu rakam 12.5 bitcoine düşmüştür. Sistem her 210 bin blok sonrası yarıya düşecek şekilde ayarlanmıştır. Bu da toplamda bitcoin sayısının 21 milyonu geçmemesi demektir. Bu şekilde bir anlamda arz yaratılmak istenmiştir. 1 Temmuz 2017 itibariyle 16.4 milyon bitcoin sisteme girmişti. İlk madenciler olmayan bitcoinleri mi özetlediler diye bir soru akla gelebilir. İlk başta sistemi yaygınlaştırmak için örneğin 500 bin USD değerinde bitcoin MİT lisans öğrencilerine dağıtılmıştır.

Son olarak da bu konudaki en önemli meselelerden biri olan "çatallaşmayı" (fork) anlamak önemlidir. Sonuç olarak bu, insan yapısından oluşan bir sistem ve bu sistemin kurallarını bu kullanıcılar koyuyor. Eğer bir grup diğerinden faklı düşünüyor ise blockchain iki farklı yolda ilerleyebilir yani iki farklı kayıt defteri farklı gruplar elinde ilerletilir ve iki ayrı elektronik para birimi tedavülde olmuş olur. Çatallaşma çok normal bir durumdur. Çünkü örneğin madencilikte de iki madenci aynı blok için aynı anda bir başarılı sonuç bulmuştur ama örneğin diğer madenciler bir tanesi üzerine yeni bloklar koyarak ilerlerse diğeri üvey muamelesi görür ve bırakılır. Ama diyelim ki bir grup yazılımın bazı kurallarını değiştirmek istiyor diğerleri istemiyorsa da yeni ama kalıcı bir çatal oluşur. Örneğin Ağustos itibariyle Bitcoin yanında Bitcoin Cash adında yeni bir birim yaratılmak isteniyor. Daha önceleri ise Etherium'dan Etherium Classic çıkmıştır ve alanında büyüklük bakımından altıncı sıradadır. Monero, Bytecoin'den türemiştir. Monera büyüklükte dokuzuncu olmuş, Bytecoin ise eriyip gitmiştir.

Bu blokları çözmek için normalde bilgisayar işlemcisi kullanılırken zaman içinde daha hızlı işlem yapabilen grafik kartları kullanılmaya başlanmıştır. Bir anlamda elektrik parası ve işlemci hızı madenciliğin maliyetidir. Ve aynı altın madenciliğinde olduğu gibi başaramama imkanı da vardır. Şu aralar riski azaltmak için madenciler havuz oluşturarak beraber çözme işlemine başlamıştır. Bu havuzlara birden fazla madenci katılır ve ödül bu madenciler arasında paylaştırılır. Eğer bir havuz sayıca büyürse sistemin güvenirliğini tehlikeye atar çünkü blokları manipüle etme şansı doğar.

Blockchain elektronik para transferinden sonra akıllı kontrat sistemleri ile hayatın birçok alanında yayılmaktadır. Tapu dairesi, mobil operatörler ya da patent ofisi gibi yerlerde olan güven ilişkisini bu sistem ile dijital dünyaya geçmek üzeredir. Örneğin bir ev kiralayacaksınız. Ev ödemesini Bitcoin ile yaptınız ve ödeme yaptığınıza dair bir belge geldi. Bu aslında sizin akıllı kontratınızın başlangıcı. Bunun akabinde ev sahibinin belli zaman içinde evin kapı giriş kodunu size iletmesi gerekiyor. Eğer zamanında bu gelmezse blockchain parayı iade ediyor. Diğer yandan, eğer anahtarı erken gönderilirse sistem anahtarı karşı tarafa göndermek için kira gününe kadar bekliyor. Bu karşılıklı alışveriş bir nevi herkesin gözü önünde oluyor.



> **"Blockchain bir anlamda hâlihazırda varolan teknolojilerin bir arada kullanılmasıyla oluşturulan bir mekanizmadır. Blockchain'de üç farklı teknoloji kullanılmaktadır: internet, asimetrik şifreleme ve özetleme fonksiyonları."**

Bu konuda örneğin Bitcoin sistemi yeterli gelmiyor. SideChains, NXT ve Ethereum gibi blockchain platformları akıllı kontrat için özellikle geliştirilmiş platformlardır. Bitcoin'de 10 dakikalık bloklar varken Etherium'da 12 saniyelik çok daha kısa bir zaman dilimi amaçlanmıştır. Ödül hiçbir zaman yarılanmaz ama her işlemden para alınır. Bunun yanında özetleme daha çok kitle (kitle-kaynak) ile beraber yapılacak şekilde dizayn edilmiştir. Yani sıradan işlemciler yeterlidir ve Bitcoin'de olduğu gibi merkezi güçlü işlemcilere gerek yoktur.

Girişimciler ise blockchain platformunu yatırım almak için kullanmaya başlamışlardır. ICO (Initial Coin Offering) bir anlamda IPO (Initial Public Offering) tarzında bir borsaya açılma hareketidir. Aldıkları elektronik para karşılığı hisseye çevrilecek token ("jeton") vererek para toplama yapmaktadırlar.

Bir startup yatırım almak istiyorsa iş planını yatırımcılara gönderir. Projenin ne olduğu, başarılı olması için ne kadar yatırıma ihtiyacı olacağı gibi konuları belirtir ve alınacak yatırım karşılığı verilecek sanal token miktarı açıklanır. Token burada hisseye tekabül eder. Eğer birçok yatırımcıdan hedeflenen miktar toplanmışsa, yatırım şirkete aktarılır. Aksi halde iade edilir. Bu durumda ICO başarısız olur. Örneğin 2014 yılında Etherium proje aşamasında iken ICO yapmıştır ve Bitcoin kullanarak 18 milyon USD toplanmıştır. Etherium'un tokeni olan Ether'in tanesi $0.4 iken proje 2015'de başarılı olunca $14'a çıkmıştır. Bu şekilde yatırımcısına 35 kat getiri sağlamıştır.

Kısaca özetlersek Blockchain teknolojisi Internet of Value olarak internetin işlem (transaction) katmanı olarak ilerlemektedir.