**Video Metni**

Blockchain Açıklaması

Blockchain'i anlamak için şu an Mikronezya'da bulunan Yap adasında MS 500 yılına dönelim. Yap halkı her yerde buna benzer taşlara sahipti. Bu bir Yap sikkesi. Onların parasıydı buydu. Yaklaşık 200 kilo olduğundan, şimdiki madeni paralar gibi asılması biraz sorun oluşturuyordu. Adalılar bu sorunu sikkeyi fiziksel olarak yanlarında taşımayarak çözdüler. Sikkeler küçük adalarında son derece görünür yerlere yerleştiriliyordu. Her yetişkin Yaplı her bir sikkenin sahibinin kim olduğunu biliyordu. İki insan alışveriş yapmak istediklerinde sahipliğin el değiştireceğini Yap halkına duyuruyor ve tüm halkın sikkenin kime ait olduğuna dair bilgilerini güncellemesini sağlıyorlardı. İşte bu şekilde para alışverişi tamamlanıyordu.

Yap halkı (bizim deyimimizle) dağıtık bir defter kullanıyordu. Bu, her Yaplının tüm sikkelerin kime ait olduğunu ezbere bildiği bir defterdi. Ve yapılan her işlemde bu defteri zihinlerinde güncellerlerdi. Dağıtık olmasının nedeni defterin tek bir kişi değil, tüm insanlar tarafından biliniyor olmasıydı.

Yap halkı, tek bir kişiden sikkenin zihinden tutulan kaydını takip etmesini isteyebilirdi. Bu kişi hem dürüstlüğü hem yönetim becerileri bakımından gerçekten güvenilir biri olurdu. Bu kişinin işlem aktivitesi üzerinde sahip olduğu bu tekel, bir ücret talep edilmesine veya kimin ne zaman işlem yapabileceğine ilişkin kurallar koyulmasına neden olabilirdi. Üstelik bu kişi hastalandığında, taşınmak istediğinde veya dürüstlüğü bir şekilde riske girdiğinde birtakım sorunlar oluşabilirdi. Bu merkezdeki kişi bir banka olacaktı. Dağıtık defterler, merkezi bir noktada güveni gerektirmeden banka işlevleri benzeri birçok işlevi gerçekleştirebilir.

Yap örneğinde hiç kimse deftere müdahale edemez ve kendine ait olmayan bir taşı sahiplenemez; çünkü tüm Yap halkının gelip bu iddiasını çürütmesinden çekinir. Dolayısıyla dolandırıcılık işlemleri de olası değildir. Ayrıca kabilenin bir üyesi müsait değilse veya başka bir yere taşınırsa (bu şekilde defterin bir kopyası kaybolursa) işlemler yine de diğer Yap halkı tarafından doğrulanabilir. Bu da sistemin hataya dirençli olduğu anlamına gelir.

Belki de en ilginci bir sikkenin zarar görmesi veya kaybolması durumunda olanlar. Bir keresinde büyük bir taş çıkarıldığı adadan getirilirken denize düştü. Yap halkı herhangi bir sorun olmadığına karar verdi. Paranızın orada, okyanusta yerleşik olduğunu hayal edebiliriz. Bunun için size kredi verecek ve tıpkı diğerleri gibi bunu da işlemler için zihinlerimizde kullanacağız. Her ne kadar uygulamada kullanılsa da para ortada yok, ancak yine de işlemlerde onu kullanabiliyorlar.

Dağıtık defterler blockchain'i anlamanız için gerekli iki temel kavramdan biri haline geldi. Ancak blockchain'i daha ayrıntılı açıklamadan önce, *Savaş ve Barış* kitabını yalnızca 20 harfle özetlemenin bir yolunu size söylemek isterim. Görünen o ki her kitabın benzersiz ve izlenemeyen bir parmak izi var. Bilgisayarların kullandığı matematiksel denklemler gibi bazı fonksiyonlar var ve bu denklemlerde bir kitabı veya karakter dizesini girdiğinizde diğer tarafta 20 - 30 basamaklı benzersiz bir kod elde ediyorsunuz. Bu kod her bir giriş için benzersizdir. Dolayısıyla *Savaş ve Barış* yazdığınızda 20 basamaklı, anlaşılmaz bir kod alırsınız. *Savaş ve Barış*'ın aynı kopyasını yalnızca bir virgül değişikliğiyle girdiğinizde tamamen farklı bir 20 basamaklı kod üretilir. Bu kodlar o kadar farklı olur ki birbiri arasında veya *Savaş ve Barış*'ın orijinal versiyonlarıyla bağlantı kuramazsınız.

Bunu yapan fonksiyonların bazı mükemmel kullanımları vardır. Bilgilerin doğrulanması için bunları kullanabilirsiniz. Bir kontrat imzalamak üzere olduğunuzu ve mülk sahibiyle aynı kopyayı imzaladığınızdan emin olmak istediğinizi varsayalım. Sizdeki versiyonu ve diğerini fonksiyona bırakabilirsiniz ve tek bir virgül farkı olduğunda bir bile 20 basamaklı farklı kodlar oluşturulur. Kimliğinizi

gizlemek için de bunun gibi fonksiyonları kullanabilirsiniz. Adınız, doğum tarihiniz, saç renginiz gibi kişisel bilgilerinizi bir metin dizesinde birleştirebilir ve metni fonksiyona girerek 20 basamaklı benzersiz bir kod oluşturabilirsiniz. Çevrimiçi ortamda iş yaparken internet kimliğiniz olarak bu kodu kullanabilir ve böylece kimsenin sizinle yeniden bağlantı kuramayacağından emin olabilirsiniz. Ancak daha sonra kodun size ait olduğunu doğrulamak isteyen biri olursa, yalnızca o kodu yeniden oluşturabilen tek giriş kombinasyonunu bildiğinizi gösterebilirsiniz.

Bunu yapan fonksiyonlar, kriptografik hash fonksiyonları olarak bilinir. Bunlar blockchain'in anlaşılması için bilinmesi gereken ikinci kavramdır. Ancak önce görünmeyen para olayına dönelim. Ada örneğinden biliyoruz ki dağıtık bir defter, ortada para olmasa da, paralarla işlem yapmanızı sağlar. Tıpkı okyanusun dibindeki para gibi... Paraların çalınmasının neredeyse imkansız olduğunu da gördük. Bunun nedeni Yap halkının bir paranın kime ait olduğunu ve sahipliği değiştiren herhangi bir işlem yapılıp yapılmadığını biliyor olmasıydı.

Şimdi bu defterlerin insanların akıllarında saklanmak yerine, dünyanın her yerinde çevrimiçi olarak bilgisayarlarda depolandığını ve teşvik edilmiş gönüllüler tarafından yönetildiğini düşünelim. İşler tıpki adada olduğu gibi yürürdü. Her bilgisayarda, paraların sahiplerini gösteren ve herkes tarafından görülüp bilinen bir defter kopyası olurdu. Bir işlem yapılmak istendiğinde kişi bilgisayar ağına yalnızca paraları başka birine gönderme niyetini duyururdu. Bu ifadeyi duyan tüm bu bilgisayarlar o kişiden bir parayı alıp diğerine eklemek suretiyle kendilerindeki defteri güncellerdi.

Gerçek hayatta buna işlerlik kazandırmamız için yalnızca iki şey eksik. Bunlardan ilki, genel görünümde adımızı ve işlem geçmişini birçoğumuz koymayacağımız için herkese açık defterde insanların kimliklerini gizlemenin bir yoludur. Bunu bir hash fonksiyonuyla çözebiliriz. Herkesin kimlik detayları, yalnızca sahibinin kodu üretmek için gerekli girişleri bildiği, tanınamayan 20 basamaklı bir koda indirgenebilir. Bu sayede katılımcı anonim olur.

Bu sistemin işleyişi için gereken bir diğer eksik ise işlem geçmişinin aynı versiyonundan başlamalarını sağlamak için bilgisayarlar arasındaki defterleri hızlı bir şekilde karşılaştırabilme yöntemidir. Bunu da bir hash fonksiyonuyla yapabiliriz. Her bilgisayar, yalnızca bilgisayar metni olan defterini 20 basamaklı bir kod haline getirebilir ve diğer bilgisayarlardaki defterlerin kodlarıyla karşılaştırabilir. Tüm kodlar uyuşuyorsa defterlerin aynı olduğu anlaşılır. Aynıysa paranın kime ait olduğunu doğru şekilde gösteriyorlar demektir. Bir yandan deftere müdahale etmeyi de neredeyse imkansız hale getirir, çünkü bunun için dünya genelindeki bilgisayarlarda bağımsız şekilde depolanan diğer binlerce defter kopyasına da müdahale etmek gerekir.

Hakkında çok şey duyduğumuz dijital para Bitcoin'e yatırım yaptık. Bitcoin, görünmeyen paraları transfer etmek için kullanılan, paylaşılan bir dağıtık defterdir. 20 basamaklı kodlanmış bir kimlik oluşturan ve bir işlemde başka kullanıcılardan para alan herkes bu deneyimin bir parçası olabilir. Bu kavramlar yani hash fonksiyonlarıyla birlikte dağıtık defter, genellikle blockchain veya bazen yalnızca dağıtık defter adıyla anılır. İlk blockchain, Bitcoin'i hayata geçirmek için oluşturuldu.

Blockchain çok daha fazlası olabilir. Bunu göstermek için modern uçakların nasıl tıpki iPhone'lar gibi olduğunu görmemiz gerekir. Bir yıl önce bir uçuşum sırasında uçak pistin yarısına kadar ani bir frenle inerek kalkışı durdurmak zorunda kaldı. Kaptan bunun kanatla ilgili küçük bir sorundan kaynaklandığını söyledi. Biliyorsunuz uçağı havada tutan parça kanat. "Endişelenmeyin, teknik ekipler düzeltecek" dedi kaptan.

Ancak bir süre sonra gelip bize mekanik bir sorun olmadığını bildirdi. Bir yazılım hatasıydı. Söylediğine göre önemli bir şey değildi. Bir yazılım yaması yükleniyordu. 20 dakika içinde kalkıyor olacaktık. iPhone'um Apple'dan bir yazılım güncellemesi yüklerken uçağım da üreticilerden "ölmememiz" için birtakım güncellemeler yüklüyordu. Bu, acı bir gerçekle yüzleşmeme yol açtı. Kanat yazılımında sorunlar varsa yakında kanat yazılımı korsanları da türeyebilir. Sürücüsüz otomobiller, cerrah robotlar ve finans danışmanlığı sağlayan bilgisayarların olduğu bir dünyaya giriş yaparken aslında buna benzer endişeler daha yoğun bir hale geliyor.

University of Michigan'daki profesörler kalp pili olan hastaların aygıtlarının kablosuz olarak hack'lenmesiyle bu hastaları ölüme götürme olasılığını gösterdiler. Birçok akıllı insan bu otomatikleşen dünyada blockchain'in bize bir miktar güvenlik kazandırmaya yardımcı olabileceğini düşünüyor.

Uçak senaryosuna dönelim; bir ağ üzerinde birbiriyle iletişim halinde olan, dünya çapında 100 uçağı düşünelim. Kalkıştan öne uçağım, kanat yazılımını alıp kriptografik hash fonksiyonuna atabilir ve 20 basamaklı benzersiz bir kod oluşturabilir. Bu durumda, diğer 99 uçağın her birinin kanat yazılımı için sahip olmaları gereken, uygun 20 basamaklı kod kayıtlarını içeren defterleri olduğunu düşünebilirsiniz.

Uçağım diğer 99 uçaktaki defterlerde saklanan kodla, kalkıştan hemen önce her bir kanadın ürettiği kodu karşılaştırabilir. Kodlar uyuşuyorsa uçağım yazılımına herhangi bir müdahale yapılmadığından emin olabilir. Peki neden? Çünkü kodumun oradaki kod depolarıyla uyuşması için bir korsanın diğer 99 uçaktaki defteri değiştirmesi gerekecektir. Uçaklar otonom olsaydı, diğer 99 uçağın tümü onay vermediği sürece kalkış yapmamaya karar verebilirdi. İşte güvenli ve akıllı aygıtların dünyası. Ve bu, bugünkü çözüm yöntemimizle çelişiyor. Bugün böyle bir durumda uçağın, tek bir arıza noktası olup hatalara ve müdahalelere açık bir merkezi sunucuyla iletişime geçmesi gerekecekti. Bu merkezi sunucu kapalı bir sistemde, bir şirkete ait olabilir ve bu da diğer aygıtlarla birlikte çalışmayı zorlaştırır.

Blockchain tüm bunları değiştirebilir. Güvenilir bir merkezi aracı ihtiyacını ortadan kaldırarak blockchain bugün tahmin etmesi bile zor olan yeni çalışma yöntemlerinin önünü açabilir. Teknolojinin daha hızlı benimsenmesi eğilimiyle birlikte blockchain'in de etkisi çok kısa sürede anlaşılacaktır. Bu videonun size başlangıç için yardımcı olacağını umuyoruz.