Dijitalleşmenin Getirdiği Düzen

Blok Zincirleri

Erdem Ünal [*QNB Finansbank Model Geliştirme Yöneticisi*

Bu dünyada merkezî yönetime, düzen koyuculara veya aracılara ihtiyaç yok. Güvenmenin çağ dışı (güvenin masalsı bir his) olduğu bu yerde tam bir paranoya hâkim. Ama enteresandır ki buranın sakinleri durumlarından hayli memnun, hatta en kritik işlerini bile gönül rahatlığıyla yapıyorlar. Evet, güvensizliğin yarattığı düzene, dijital para Bitcoinin (BTC) doğduğu yere, blok zinciri dünyasına hoş geldiniz.

Blok zincirinin sözlük tanımı "içindeki kayıtların birbirine sırayla bağlı olduğu, sürekli büyüyen dağıtık bir veri tabanı"dır. Dağıtık olması (kayıtların tek bir merkezden ziyade tüm kullanıcılarda olması) bilgilerin yok olma riskini azaltırken, kayıtları içeren blokların birbirine şifrelenmiş şekilde bağlı olması da güvenliği sağlıyor.

Blok zinciri denince akla hemen dijital para birimi Bitcoin gelir. Hiç bir devlete veya kişiye ait olmayan Bitcoin, ülkeler tarafından resmi bir para birimi olarak tanınmasa da hemen hemen her yerde serbestçe kullanılıyor.

Bugün bazı ülkelerde birçok küçük işletmenin yanı sıra Microsoft, Dell, Subway, LOT Polish Airlines gibi büyük ve farklı sektörlerde faaliyet gösteren uluslararası şirketlerin de ödemelerde Bitcoini kabul etmesi bu dijital para biriminin yaygınlaşmasını ve değer kazanmasını sağlıyor.

Blok zinciri teknolojisi hayatımıza 2008'de Satoshi Nakamoto'nun (takma ad) Bitcoini tanıtmasıyla girdi. Bitcoinlerin kullanıcılar arasında transferini ve hesapların güvenliğini sağlayan bu teknoloji, aynı zamanda sistemin güvenli işlemesini sağlayan gönüllü kullanıcılara teşvik olarak Bitcoin dağıtıyor, zaten bu Bitcoin üretmenin tek yolu. Biz de teknolojinin gelişimine uygun olarak, blok zincirinin ne olduğunu ve nasıl çalıştığını Bitcoin transferi örnekleriyle inceleyeceğiz.

Neden Bitcoin?

Toptan satış yapan dünyaca ünlü bir e-ticaret sitesine sahip olduğunuzu düşünün. Yeni müşteriniz Emir bey çok sayıda ayakkabı almak istiyor. Sorun yok, gerekli parayı ödemesi durumunda, siparişi göndermeye hazırsınız. Size para transferi sırasında güvenebileceğiniz birileri lazım. Sanırım dijital ortamda buna en uygun kurumlar bankalar. Emir beyin para transferinin bir banka tarafından onayladığını görürseniz siparişini hemen gönderebilirsiniz. Bankalara güvendiğiniz için bu alışverişte bir tedirginlik duymazsınız.

Genel olarak böyle bir süreçten memnun kalsanız da, birkaç nokta sizi rahatsız edebilir. Örneğin bankalar para transferindeki aracılık hizmeti karşılığında komisyon alır. Ayrıca müşterinizin farklı bir ülkede olması durumunda komisyon oranı çok artarken transfer işleminin onaylanması da zaman alır.

Blok zinciri teknolojisi işte tam da bu noktada bu tip sorunlara çözüm vaadiyle karşınıza çıkıyor. Bir aracıya (örneğin bankalara) olan ihtiyacı ortadan kaldırıyor, komisyonu sıfırlıyor (veya çok düşük komisyon alıyor) ve uluslararası para transferleri gibi uzun zaman alan işlemlerin süresini hayli kısaltıyor.

Örneğin Emir bey transferini blok zinciri teknolojisini kullanarak basitçe şöyle yapabilirdi.

Sipariş tutarı 50.000 TL olsun. Emir bey, size bu tutarı Bitcoin olarak ödeyecek, ki bu tutarın Bitcoin cinsinden karşılığı şu anda yaklaşık 5 BTC. Bunun için Emir beyin yapması gereken tek şey telefonundan veya internetten Bitcoin cüzdanına erişip size 5 BTC göndermek istediğini yazmak, hepsi bu. Hesabınıza transferin geldiğini görmeniz durumunda siz de siparişi gönderebilirsiniz.

Bu yöntem çok basit gibi görünse de işin arka planında hayli karmaşık bir teknoloji var: Blok zinciri. Bu karmaşık teknolojiyi anlamak için onun özelliklerini okumamız yeterli gelmeyebilir, dolayısıyla gelin kendi Bitcoinimizi sıfırdan biz yaratalım.

Amacımız, kimsenin tekelinde olmayan bir para birimi oluşturmak ve bu parayı transfer ederken ve harcarken hiçbir kuruma ihtiyaç duymamak.

Burada anlatacağımız süreç, konunun daha iyi anlaşılması için kurgulanmıştır. Gerçekte Bitcoinin tarihsel gelişimi bu şekilde olmamıştır, mevcut uygulamalarda da bazı ufak farklılıklar vardır.

Bitcoin sisteminde kullanıcılar sadece bir (veya birkaç) hesap numarası olarak görünüyor, bu hesapların gerçekte kime ait olduğu hakkında kimsenin en ufak bir fikri yok. Çünkü hesap açmak bir hesap numarası seçmekten ibaret ve bunun için de kimseyle herhangi bir bilgi paylaşmıyorsunuz.

Yani Bitcoin cüzdan uygulamaları herhangi bir bilgi talep etmeksizin, istediğinizde size (belirli bir formata uymak koşuluyla) rastgele bir hesap numarası oluşturuyor. Bu hesap numarasını Bitcoin ağına duyurmanıza da gerek yok. Size Bitcoin transferi yapacak kişiye söylemeniz yeterli. Diğer kullanıcılar ancak hesabınıza bir transfer yapılırsa, böyle bir hesap numarasından haberdar oluyor. Ama hesabın kime ait olduğunu, hatta bir sahibinin olup olmadığını bile bilmiyorlar (henüz kullanılmayan bir adrese yanlışlıkla para transferi yapılabiliyor).

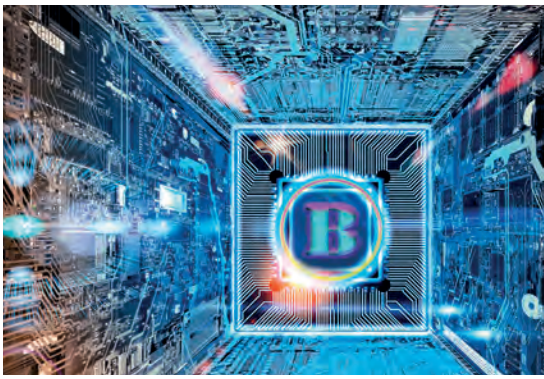
Hesap oluşturma işlemini çevrimdışı yaptığınız için aldığınız hesap numarasının başkası tarafından kullanılıyor olma ihtimali de var. Ancak potansiyel Bitcoin adres havuzu sayısının 2^{160} olması bu ihtimalin gerçekleşmesini neredeyse imkânsız kılıyor.

Bitcoinimizin Doğuşu

Öncelikle bilgisayarımızın başına oturup kendimize, eşe dosta ve akrabalara birer hesap açıyoruz. Bu hesapları şimdilik sadece bizim bilgisayarımızda bulunan birer dosya olarak düşünebiliriz. Ardından bal tutan parmağını yalar deyip kendi hesabımıza +100 BTC yazıyoruz. Sonra isteyen herkesin internet üzerinden bu hesaplarda neler olup bittiğini görmesine, hatta kendi hesaplarını oluşturmasına (ama sadece hesap oluşturmasına, para yazmasına değil) izin veriyoruz. Sistemimizde şimdilik sadece 100 BTC var, o da bizim. Arada akrabalara da 3-5 BTC yolluyoruz. Akrabalar birbirine para yollamak istediğinde, bize söylüyor biz de uygun bulursak transferi yapıyoruz. Herkese bu özel paranın sahibi yok dedik, ama paranın kontrolünün bizde olduğu çok açık. İstediğimiz zaman istediğimiz kadar para üretip dağıtabiliyoruz.

Hesabımızı izleyen ve "açalım dursun" diye hesap açan takipçilerimizin sayısı zamanla artıyor. Önceleri oyun gibi düşünüp seslerini çıkarmasalar da kalabalıklaştıkça işi ciddiye almaya başlıyorlar. Paranın, bizim tekelimizden çıkmasını istiyorlar. Her ne kadar adil olacağımızı, kişisel hesabımıza havadan para yazmayacağımızı söylesek de kimse inanmıyor, çünkü burada güvene yer yok. Şöyle bir talepte bulunuyorlar:

Bizdeki tüm para sisteminin aynısı onlara da yüklenecek ve onların onayı olmadan hiçbir hesapta değişiklik olmayacak. Sahipsiz bir para oluşturmak niyetiyle talebi kabul edip işleme koyuyoruz. Böylelikle merkezî hale gelen veri tabanımız artık herkeste bulunuyor, yani dağıtık hale geliyor.



Para Transferinde Onaylama Süreci

Emir beyin hesap numarası 123 olsun.
Buradan bize 5 BTC göndermek istediğini tüm ağa bildirdikten sonra kullanıcılar iki şeyi kontrol ederek transfer işlemini onaylayabilir:

Transfer talebinin gerçekten 123 no'lu hesaptan geldiğini ve bu hesapta yeterli para olup olmadığını.
İkincisi nispeten daha kolay, her hesapla ilgili bilgiler herkeste olduğu için herkes 123 no'lu hesabın bakiyesini kontrol edip bunu doğrulayabilir.

Biraz daha zor olanı ise talebin gerçekten 123 no'lu hesaptan gelip gelmediğini anlamak.

Bunun için para transferi yapmak isteyenler, transfer talepleri ile birlikte dijital imzalarını da gönderiyor. Diğerleri de imza ile mesajın uyuşup uyuşmadığını kontrol edip talebin gerçekten 123 no'lu hesaptan geldiğinden emin olabiliyor.

Henüz paranın nasıl üretileceğini çözmesek de tüm hesap değişikliklerini kontrol altına almış olduk. Ancak hesap değişikliklerinde herkesin onayını arayarak kontrolü biraz abarttık gibi. Birine para transferi yapmak için herkesin sisteme girmesini ve onay vermesini beklemek hiç de verimli bir yöntem değil. Bunun yerine, sistemde o an kim aktifse onlardan birinin onay vermesi yeterli olsun. Transfere onay veren kişi bunu sistemdeki herkese ilan etsin ve diğerleri de ilk fırsatta bunu kontrol edip kendi kayıtlarına geçirsin. Böylece transfer onayı için uzun uzun beklemeye gerek kalmasın.

Çözümümüz verimliliği artırsa da bazı güvenlik sorunlarını beraberinde getiriyor. Örneğin aynı anda binlerce transfer talebi gelirse önce hangisi değerlendirilecek? İlk bakışta önemsiz gibi gelebilir, ama aslında son derece kritik bir nokta. Zira Emir bey hesabında sadece 5 BTC olmasına rağmen bu parayı hem bize hem de Çin'deki bir satıcıya göndermek için talep açabilir. Banka gibi merkezî bir sistem olsaydı ilk talep onaylanır, ikinci talep hesapta para olmadığı için reddedilirdi. Yeni sistemimizde ise merkezî bir otorite yok, aynı yetkiye sahip çok sayıda kullanıcı var. Bir bilginin tüm kullanıcılara aynı anda ulaşması da mümkün değil. Mesela bazıları bize yapılmak istenen transferi ilk talep olarak görürken, bazıları Çinli satıcı için yapılan talebi ilk talep olarak görebilir. Dolayısıyla her iki talebi de onaylayacak birisi olabilir. Hâlbuki transfer taleplerinden birinin reddedilmesi şart, yoksa çift harcama yapmak mümkün olur!

Sistemin Güvenliği İçin Büyük Tehlike: Aynı Parayı Tekrar Tekrar Harcamak

Çift harcamayı engellemek için bir önerimiz var. Transfer kayıtlarının bir zincirin halkaları gibi birbirine eklenerek ilerlediği bir yapı inşa etmek. Zincirimiz herkesin kullanımına ve yeni halka eklemesine açık olsun. Zincire yeni bir halka eklenmek istendiğinde, hesaplardaki paranın önceden harcanmadığından emin olmak için zincirin önceki halkaları kontrol edilsin.

Sürecimiz kabaca şöyle işleyebilir. Transfer talepleri öncelikle bir havuza alınsın. Talepleri onaylamak isteyen biri havuzdan bir talep seçip yukarıda bahsettiğimiz onaylama sürecini başlatsın. Eğer talep tüm onay kriterlerini karşılıyorsa o talebi zincirin sonuna yeni bir halka olarak eklesin, aksi halde reddetsin. Herkes bu işlem zincirine bakarak onay veya ret vereceği için çift harcamayı engellemiş oluruz. Örneğimizde Emir beyin transferlerinden biri zincirimize önce eklenecek (ve bunu herkes bilecek), diğeri de zincir kontrolü sırasında hesapta para kalmadığı görüleceği için reddedilecek.

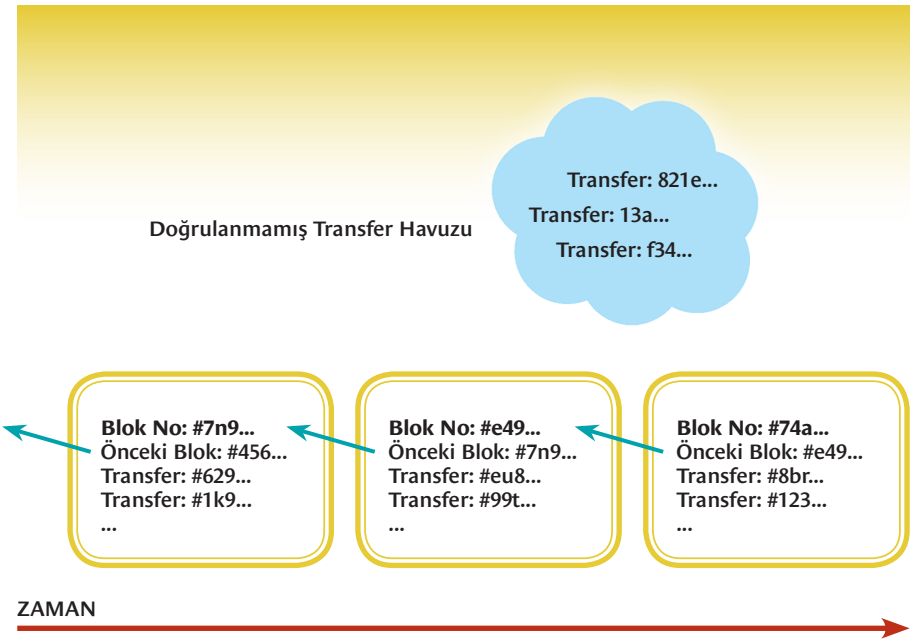
Ancak küçük bir sorunumuz var. Merkezî bir sistemimiz, yani herkesin bakabileceği ortak bir zincirimiz yok. Her kullanıcı kendi zincirini oluşturmak zorunda. Zincir oluşturmak sorun değil, ama herkeste aynı zincir olduğundan nasıl emin olacağız?

Oyunumuza yeni kurallar eklemenin vakti geldi. Bir an için herkeste aynı zincirin olduğunu varsayalım. Birisi bir transferi onaylayıp kendindeki zincire eklerken tüm kullanıcılara şu mesajı göndersin: "Merhaba, elimde son halkasının adı abc olan bir zincir var ve ben buna c23 isimli bir halka (işlem) daha ekliyorum." Bu mesajı alan diğer kullanıcılar herhangi bir sahtekârlığa karşı zincirin son halkasını ve yeni onaylanan c23 işlemini tekrar kontrol edip kendilerindeki zincire eklesin. c23 işlemi onaydan geçmezse, kimse kendi zincirine eklemesin, sahtekâr kullanıcı kendi eklediği ile kalsın. Bunu sağladığımız durumda, herkesin mutabık kalacağı tek bir transfer zinciri elde etmiş oluruz.

Güvenliği sağladık gibi, ama sistemimiz hayli verimsizleşti. Binlerce kullanıcının olduğu bir ortamda zincirin son halkası sürekli değişeceği için süreci takip etmek ve gerekli güncellemeleri yapmak hayli zor olmalı. Son halkanın takibini kolaylaştırmak ve güncelleme işlemini yapmaları için kullanıcılara zaman kazandırmak amacıyla zincire sürekli halka eklenmesine engel olmalıyız. Bunun için halka ekleme işini biraz zorlaştıralım. Örneğin gönüllü kullanıcılar, bir işlemi onaylayıp zincire eklemeden önce çözümü zaman alacak bir soruyla uğraşsın. Sadece soruyu çözenin onayladığı işlem, diğer kullanıcılar tarafından kayıtlara eklensin (tabii doğruluğunu kontrol ettikten sonra).

Zaman Alan Soru

Transfer işlemlerini onaylayan kullanıcıların zincire bir blok eklemeden önce çözmesi gereken bir soru olduğunu söylemiştik. Bu soru en zeki, en kurnaz sahtekârların bile baş edemeyeceği zorlukta olmalı. Bu hedefe ulaşmak için acaba ne kullanılabilir? Tabii ki matematik! Elimizde, hangi girdinin hangi sonucu vereceğini denemeden bilmenin pratikte imkânsız olduğu bir hash fonksiyonu var. Amacımız bu hash fonksiyonuyla ortaya çıkan değerin başında belirli sayıda 0 olmasını sağlayacak bir sayı bulmak. Hash fonksiyonunun parametreleri arasında hem blok içindeki transfer adları ve önceki bloğun adı hem de bize istediğimiz sıfırları verecek ama bilmediğimiz bir sayı var. Bu sayıyı bulmanın kısa bir yolu yok, tek yolu rastgele deneme yapmak. Böyle bir sayıyı, güçlü bir bilgisayarın bulması yıllar alabiliyor. Ancak ağda kendi hash fonksiyonlarını çözmeye çalışan on binlerce bilgisayar olduğu için ortalama her 10 dakikada bir hash fonksiyonu çözülüyor. Dolayısıyla blok zincirine her 10 dakikada 1 blok ekleniyor.



Neden Bloklar Var?

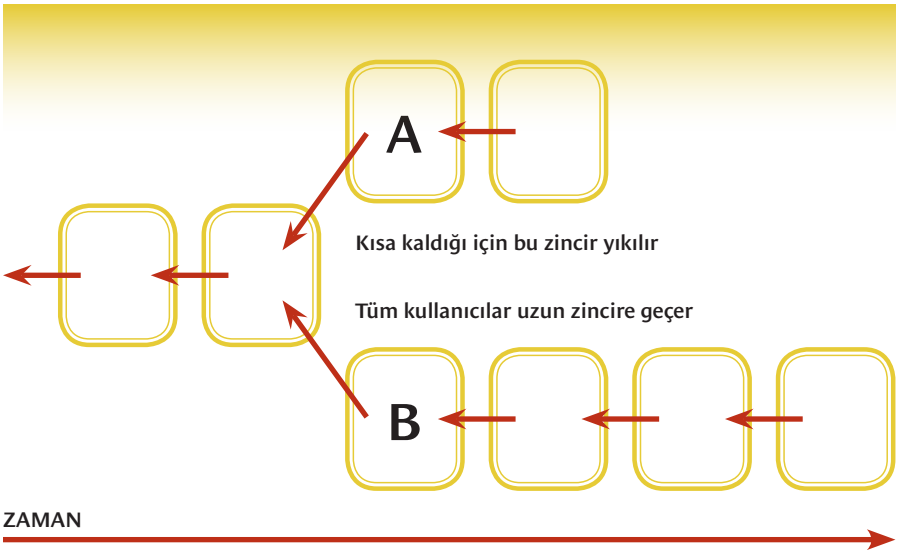
Yeni zincir sistemine soru eklenmesi çok iyi oldu. Ancak bu sefer de başka bir sorunumuz var: Zaman! Her an binlerce transfer talebi yapılan bir dünyada her transfer için bir soru çözülmesini beklemek çok zaman kaybettirir. Kimse transferinin onaylanması için günlerce beklemek istemez. Bu nedenle kullanıcıların transferleri topluca onaylayıp bir blok halinde zincire eklemesine izin verelim. Dolayısıyla kullanıcılar her işlem için tek tek soru çözmek yerine, yüzlerce işlemi barındıran bir blok oluşturup bu blok için tek bir soru çözmekle yetinebilir. Artık elimizde bir transfer zinciri yok, blok zinciri var. İşte bu teknoloji adını böyle alıyor.

Önceki Blok Adı	Yeni Blok İçerisindeki Transfer Adları	Denenerek Aranan Sayı	Hash Sonucu	Başta En Az 2 Adet Sıfır Var mı?
F(#37KAS34...,	transfer#88A..., ..., transfer#C62...,	1000)	= A723882...	✗
F(#37KAS34...,	transfer#88A..., ..., transfer#C62...,	1001)	= A238KCD...	✗
F(#37KAS34...,	transfer#88A..., ..., transfer#C62...,	1002)	= 000BJK12...	✓

Son Dokunuşlar

Gönüllü kullanıcıların öneminin iyi anlaşılması gerekir. Sistemimizin güvenliği bir bakıma onların elinde, çünkü bir bloğun zincire eklenip eklenmemesine onlar karar veriyor. Daha önce bahsettiğimiz gibi her kullanıcının kendi bilgisayarında tuttuğu bir zincir var, merkezî bir zincir yok. Kurallarımız sayesinde, genel olarak herkesteki zincirin hemen hemen aynı olmasını sağlayabiliyoruz. Ancak bazı teknik problemler veya dolandırıcılık girişimleri nedeniyle bazı kullanıcılardaki zincirler farklı olabilir. Farklı zincirler olması hiç istenmeyen bir şey olduğu için acilen bir zincirin kazanması diğerlerinin de ortadan kaldırılması gerekiyor. Bitcoin sisteminde kazanan zincir, kullanıcı sayısı en çok olan zincir oluyor (aslında sayıdan ziyade bilgisayar işlem gücü en çok olan zincir). Diğer zincirler ise atıl kalıyor. Atıl zinciri kullanan kullanıcılar ise kazanan zincirin kopyasını alıp ondan devam etmek zorunda kalıyor.

Gönüllü kullanıcılar (onlara Bitcoin madencisi deniyor), oluşturdukları her blok için belirli bir miktar (onaylama ücreti ve transfer yapmak isteyen bazı kullanıcıların gönüllü olarak ödediği komisyonlar) Bitcoin kazanıyor. Bitcoin üretimi sadece bu yöntemle oluyor, ama üretilebilecek miktar sınırsız değil. Her dört yıllık periyotta, bir önceki dört yıllık periyodun yarısı kadar para üretilecek şekilde tasarlanan sistemde 2140 yılına kadar 21 milyon BTC üretilmiş olacak. 2140 sonrasında ise üretim duracak. Şimdi ücretsiz olan Bitcoin transferi, bu nedenle ileride çok düşük de olsa komisyonlu hale gelebilir.



Haydi, Biraz Para Basalım!

Farklı zincirlerin ortaya çıkması durumunda, üzerinde en çok işlem yapılan zincirin kazandığını gördük. Bu nedenle sistemin toplam işlem gücünün %51'inin kimin veya kimlerin elinde olduğu sorusu çok önemli, çünkü bu kişilerin sistemi yanlış yönlendirme güçleri var. Kötü niyetli kullanıcılar bu gücü elde etmek için yatırım yapabilir, örneğin çok daha güçlü işlemciler satın alabilirler. Sistemi kötülerin eline bırakmamak için blok eklememiz ve onaylamaya istekli, işlem güçlerini artırmak için yatırım yapabilecek iyi kullanıcılar bulmamız gerek. Peki ama iyi kullanıcılar neden zamanlarını ve paralarını sırf sistem güvenli olsun diye harcasın?

Bir sorunumuz daha var. Hiç yeni para basmadık ama artık gerekli.

Peki bir merkez olmadan para nasıl adilce üretilebilir ki?

İtiraf edelim, bunlar çözümü hiç de kolay olmayan sorunlar. Tam da sistemi kurduk işletiyoruz derken, nereden çıktılar! Ama bir dakika, bu sorular birbirinin cevabı olabilir mi? Mesela zincire blok eklemeyi başaran kullanıcılar havadan para kazanabilir! Böylece kullanıcıları blok eklemek için yarışmaya (yani sistemin güvenliğini sağlamaya) teşvik etmiş oluruz, hem de herkes emeğinin karşılığı olarak para ödülü kazanır. Daha nasıl adil olunur ki? Üstelik bu yolla, piyasamıza ne kadar para ekleyeceğimiz bile kontrol altında. Böylece sistemimizi tamamlamış olduk. Artık derin bir nefes alıp iyiliğin baskın gelmesi temennisiyle çayımızı yudumlamaya başlayabiliriz.

Sonuç olarak, hiç kimseye güvenmediğimiz bir dünyada matematik yardımıyla para üretimi ve transferi gibi kritik işlemler yaptık. Blok zincirleri teknolojisinin kullanıldığı en popüler örnek Bitcoin olduğu için burada teknolojiyi Bitcoin üzerinden tanıdık. Ancak yapılabilecekler elbette para transferleri ile sınırlı değil, dijitalleştirilebilen her işlem (seçimlerde oy kullanmaktan tutun da noterlerin belge onaylamasına kadar) yakın gelecekte blok zincirleri ile hayli güvenli bir şekilde yapılabilir. Her şeyin daha güvenli, daha adil olduğu bir dünyada yaşamak dileğiyle. ■

Kaynaklar

https://www.forbes.com/sites/haroldstark/2017/04/21/from-here-to-where-bitcoin-and-the-future-of-cryptocurrency/#56e865ba4367

https://blockgeeks.com/guides/what-is-blockchain-technology/

http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

http://www.huffingtonpost.com/ameer-rosic-/5-blockchain-applications_b_13279010.html