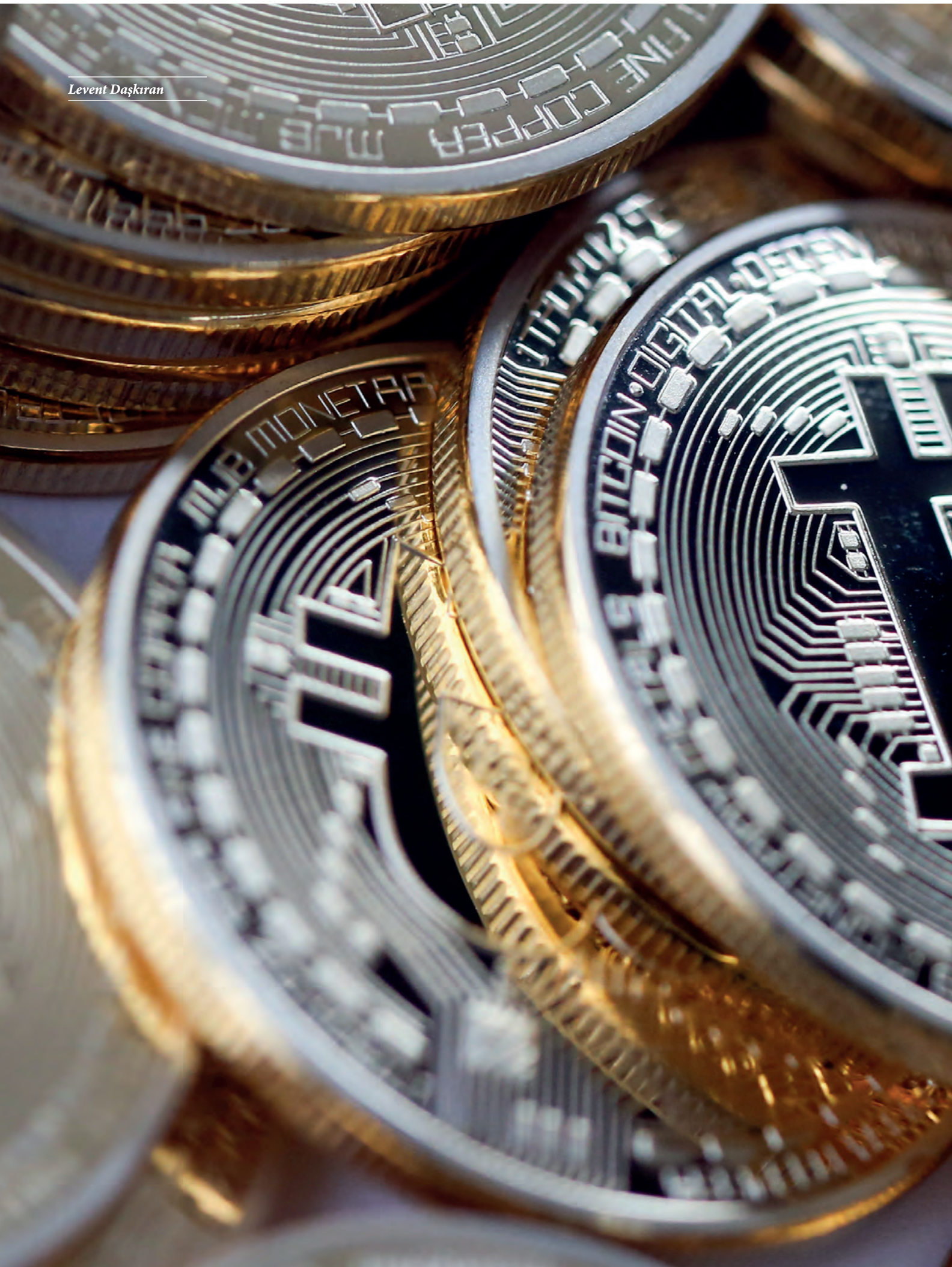
*Levent Daşkıran*



# Bitcoin

## Dijital Dünyanın Finansal Otoriteye Başkaldırısı

Her şeyin dijitale dönüştüğü bir dünyada, karmaşık matematiksel formülleri temel alan yapısıyla geleneksel para birimlerinin dezavantajlarını ortadan kaldırmak üzere kurgulandı.

Hiçbir merkezi otoriteye bağlı değil, kendi kurallarını kendi koyuyor ve milyonlarca kullanıcı tarafından denetleniyor. Arkasında ne bir merkez bankası var, ne de bir hükümet. Ama yine de değerli, yine de yaygın ve popüler. Dijital dünyanın dijital para birimi Bitcoin'le ilgili tüm merak edilenleri bir araya getirdik.

ABD'de 2006 yılında başlayan konut krizi, 2008 yılında büyük bir ekonomik krize yol açtı. Ülkenin finansal sistemi çöktü, dev bankalar ardı ardına iflaslarını açıkladı, borsa çakıldı, işsizlik aldı yürüdü ve dev ülke II. Dünya Savaşı'ndan beri gördüğü en büyük ekonomik buhranın içine düştü. Kriz ABD'de yani dünya ekonomisine yön veren ve dünyanın en yaygın para birimine sahip olan ülkede patlayınca, etkilerinin dünyanın diğer bölgelerine dalga dalga yayılması kaçınılmaz oldu.

Geçmişte pek çok kez yaşandığı üzere geleneksel finans sisteminin krize girdiği böyle bir dönemde Bitcoin'in ortaya çıkışı bir hayli anlamlı olsa gerek. 2009 yılının başlarında Satoshi Nakamoto takma adıyla tanınan kriptoloji uzmanının (veya uzmanlarının) ilkelerini ortaya koyduğu, tamamen dijital ortamda doğan, kendi kuralları çerçevesinde kendi ekonomisini oluşturan ve hiçbir merkezi yönetime bağlı olmayan yeni bir kripto para birimi anlayışı, acaba geleneksel finans yaklaşımının neden olduğu sorunları ortadan kaldırabilir miydi?

Uzmanların uzun süredir üzerinde tartıştığı yeni nesil dijital para birimlerinin ilk örneği olan Bitcoin, işte böyle bir ortamda dünyaya merhaba dedi.

## Satoshi Nakamoto: 750 Milyon Dolarlık Bir Sırrın Hikâyesi

2015 yılının son aylarında dünya, Bitcoin'in yaratıcısı olan ve Satoshi Nakamoto takma adıyla bilinen kişinin gerçek kimliğinin ortaya çıktığı haberleriyle çalkalandı. Avustralyalı güvenlik ve kripto uzmanı Craig Wright, 2009 yılında Bitcoin para biriminin temel ilkelerini ortaya koyan ve 2011 yılında ortadan kaybolan Satoshi Nakamoto olduğunu iddia ediyor ve bunu kanıtlamaya hazır olduğunu söylüyordu. Üstelik Bitcoin dünyasının kökeninde yer alan isimlerden, eski Bitcoin Foundation üyesi Jon Matonis ve Bitcoin'in ilk programcıları arasında yer alan Gavin Andresen'in Wright'ın iddiasına inanan isimler arasında yer alması, iddiaların gerçek olabileceğini düşündürüyordu.

Bununla birlikte Bitcoin camiasında Wright'ın senaryosundaki açıkları işaret eden ve yalnızca ilgi çekmeye çalışan biri olduğunu düşünenlerin sayısı da az değildi. 2016 yılının Mayıs ayında iddiasını ispatlayacak sağlam delillerle ortaya çıkacağını söyleyen Wright, zamanı geldiğinde iddialarını ispatlamak yerine web sitesinden Matonis ve Andresen'e hitaben bir özür yazısı yayımladı ve Satoshi Nakamoto olduğunu ispatlayacak cesarete sahip olmadığını açıkladı.

Bitcoin'in yaratıcısının kendisine uygun bulduğu takma isim olan Satoshi Nakamoto, Japonya'da Ahmet Korkmaz veya Mehmet Yılmaz kadar yaygın bir isim. Bu nedenle gerçek kimliğini saklamak isteyenler tarafından sıkça kullanılıyor. Peki, Satoshi Nakamoto'nun kim, hatta belki de kimler olduğunu bilmek neden bu kadar önemli?

Sanırım Nakamoto'nun yalnızca Bitcoin'in mucidi ve tasarımcısı değil, aynı zamanda 1 milyon civarında Bitcoin'in sahibi olduğunu söylersek bu anlaşılır. Nakamoto'ya ait birden fazla Bitcoin cüzdanı içinde, "Genesis Block" adlı ilk Bitcoin bloğu üzerinden keşfedilen Bitcoin'ler de dâhil olmak üzere 1 milyon civarında Bitcoin bulunduğu tahmin ediliyor (birinin gerçekten Satoshi Nakamoto olduğunu ispatlaması için yapması gereken şeylerden biri de bu ilk Bitcoin'leri hareket ettirmek). Bu o kadar yüksek bir değer ki, 2140 yılında sistemdeki 21 milyon Bitcoin'in tamamı keşfedildiğinde bile Nakamoto'nun elindeki miktar dolaşımdaki toplam miktarın yüzde 5'inden fazlasına denk gelecek. Ben bu yazıyı yazarken günlük Bitcoin kuruyla Nakamoto'nun elindeki servet yaklaşık 760 milyon dolara karşılık geliyordu. Gerçekten iyi para.

## Dijital Dünyada, "Dijital Doğan" Para Birimi

Bitcoin ve benzer kripto para birimlerini herhangi bir üçüncü şahsın, şirketin, bankanın veya hükümetin müdahil olmadığı, tamamen matematiksel işlemler sonucunda dijital ortamda üretilen ve harcanan bir para birimi olarak özetlemek mümkün. Baştan belirlenmiş kendi kuralları haricinde hiçbir merkezi otoritenin denetimi altında değil. Yapılan harcamalara dair kayıtlar da yine bir banka veya hükümet tarafından tutulmak yerine, kurulduğu ilk günden itibaren yapılan tüm işlemler, Bitcoin sistemine dâhil olan herkesin ilk andan sahip olduğu açık bir deftere tek tek yazılıyor. Bitcoin ile yapılan her alışveriş sonucunda el değiştiren Bitcoin miktarı bu deftere kaydediliyor ve güncel kayıtlar Bitcoin kullanıcıları arasında paylaşılıyor. Tüm bunları işler hale getiren kodlar tamamen açık kaynak yapısında, dolayısıyla sistem olabildiğince şeffaf.

Bu sistemin, geleneksel para birimlerine kıyasla, beraberinde getirdiği kendine özgü bazı avantajlar var. Örneğin Bitcoin ile ödeme yaparken herhangi bir aracı kullanmak, dolayısıyla yüksek komisyonlar ödemek zorunda değilsiniz (bu yönüyle özellikle küçük işletmeler ve uluslararası girişimciler açısından gayet cazip).Bitcoin kullanmak için gereken cüzdana sahip olmak sadece birkaç dakikalık bir iş ve herhangi bir bürokrasiye ihtiyaç duyulmuyor. Ayrıca hiç kimse herhangi bir sebeple cüzdanınızdaki varlığa el koyamıyor. Kendi kuralları haricinde herhangi bir düzenlemeye tabi değil, işlemler tamamen şeffaf. Dünyada var olabilecek toplam Bitcoin sayısı 21 milyonla sınırlandırıldığı için aşırı arz sonucunda enflasyon riski de taşımıyor.

İnternette Bitcoin ve benzer kripto para birimlerinin tanımına baktığınızda genel olarak karşılaşacağınız bilgiler bu şekilde. Her şey gayet açık ve net görünüyor, ta ki ilk soruları sormaya başlayana kadar. Örneğin Bitcoin nasıl elde ediliyor? Kim dağıtıyor, nasıl keşfediliyor? Dijital ortamda üretilen bir para biriminin sınırsız bir şekilde kopyalanmasının veya defalarca kullanılmasının önündeki engel nedir? Sadece matematik işlemler sonucu elde edilen bir para biriminin bugün 10 milyar dolara ulaşan toplam piyasa değeri nereden kaynaklanıyor? Merkezi denetimin söz konusu olmadığı bir ortamda, sistemin sahip olduğu temel kuralların doğru işleyip işlemediğini kim, nasıl denetliyor?

Bu soruların önemli bir bölümünün cevabını bulmak için, yeni Bitcoin'lerin keşfedilmesini sağlayan süreç olan Bitcoin madenciliği konusunun derinlerine inmekte yarar var.

Tek bir kişinin bu kadar çok Bitcoin'e sahip olması, bazı çevrelerce Bitcoin'in ortaya çıkış nedeni ve ilkeleri açısından bir tehdit olarak gösteriliyor. Çünkü merkezi para yönetim anlayışından uzaklaşmayı hedefleyerek kurgulanmış bir sistemde bir kişinin elinde bu kadar Bitcoin'in olması, fiyatlar üzerinde dilediği gibi hileli yönlendirme yapabilmesi demek. Ayrıca Bitcoin'in internetin yeraltı ekonomisindeki popüleritesini hesaba katarsanız, değeri 1 milyar dolara yaklaşan bir kripto servetin internetteki suç dünyası için ne kadar iştah kabartıcı olduğunu tahmin edebilirsiniz.

Ancak sahip olduğu servete ve güce rağmen, Bitcoin'in ortaya koyduğu ilkelere en bağlı kişi de Nakamoto gibi görünüyor. Çünkü Bitcoin'in herkese açık olan kayıtları, Nakamoto'nun sahip olduğu Bitcoin'lere edindiği günden beri bir kez bile dokunmadığını gösteriyor. Bazıları Nakamoto'nun 1 milyona yakın Bitcoin'i kayıp olarak sistemin dışına itip diğer Bitcoin'lerin değerinin artmasını sağladığı, böylece ortadan kaybolmadan önce kendi kurduğu sistemi enflasyondan korumaya yardımcı olacak son bir hediye bıraktığı inancında.

Nakamoto'nun kim olduğu belli değil. Ama herkes, kim olduğu ortaya çıkacak olursa böylesine ince planlanmış bir sistem kurgulamanın cezasını bir şekilde çekeceğine inanıyor. Muhtemelen kendisi de bunun farkında.

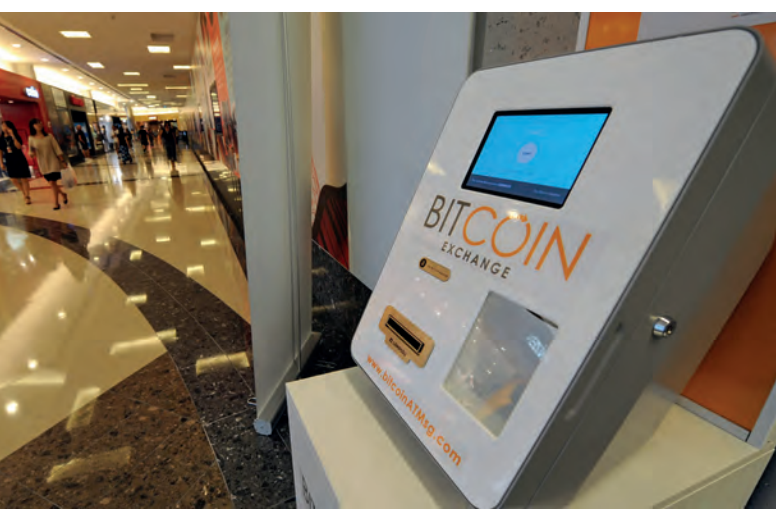
Ama gerçek bambaşka da olabilir. Örneğin Nakamoto'nun hikâyesini okurken aklıma *Ghost in the Shell: Stand Alone Complex* anime tv dizisinin 2003 yılında yayınlanan *Automated Capitalism* adlı bölümü geldi. Bu bölümde kahramanlarımız, borsadan elde ettiği büyük kazançlarla dikkat çeken matematik dehası multimilyarder Kanemoto Yokose'yi öldürmek için bir suikastçı tutulduğunu öğrenir ve olayın peşine düşerler. Bölümün sonunda yalnız yaşayan Yokose'nin zaten haftalar önce doğal sebeplerle öldüğü ortaya çıkar. İşin ilginç tarafı, kurduğu borsa otomasyon sistemi Yokose'nin ölümünden sonra da kendi kendine çalışmaya, servetine servet eklemeye devam etmiştir.

Öyle görünüyor ki Wright'ın yarım bıraktığı girişimin ardından Nakamoto'nun gerçekten kim olduğunu öğrenmek için biraz daha bekleyeceğiz.

Aslında belki de hiç öğrenmesek daha iyi.

## Bitcoin'in Karanlık Madenlerine Yolculuk

Dünya üzerinde on milyonlarca bilgisayarın yeni Bitcoin'leri keşfetmek için birbiriyle yarıştığı Bitcoin madenciliği denilen kavram, birçok kişinin ilk anda düşündüğünün aksine altın bulmak için toprağı kazar gibi mevcut bir veri yumağı içinde, giderek daha karmaşık bir hal alan problemleri ilk çözen olup karşılığında ödüllendirilmekten ibaret değil. Aslında Bitcoin madenciliği yapan herkes, sistemin güvenliğini sağlamak için çalışan, dünya geneline dağılmış dev bir dağıtık süper bilgisayar ağının parçasına dönüşüyor. Peki nasıl?




Bitcoin ve benzeri kriptoya dayalı para birimlerinde ilk akla gelen risklerin başında dolandırıcılık gelir. Zira harcanan para elektronik bir kaydın bir taraftan diğer bir tarafa aktarılmasından ibaret olduğu için, tıpkı bir yazılımı kopyalar gibi aynı parayı üst üste iki kez harcamak elektronik para birimlerinin işleyişi açısından büyük bir risk oluşturur. Örneğin ben 1 Bitcoin karşılığında gidip Ahmet'ten bir bilgisayar satın alıyorum. Hemen arkasından da dönüp aynı Bitcoin ile Ayşe'den bir televizyon almaya yelteniyorum. Bu durumda sistem, yaptığım harcamalardan hangisinin gerçek hangisinin dolandırıcılık girişimi olduğuna nasıl karar verecek?

Bitcoin bunun için Blockchain, yani bizim zincir dizilimi adını verebileceğimiz bir sistem kullanıyor. Bunu da şöyle yapıyor: Yapılan alışverişlere anında onay vermek yerine, işlemleri bir zincir halkası üzerinde biriktiriyor ve yapılan alışverişlerin doğrulama işini Bitcoin madencilerinin sahip olduğu işlem gücüne devrediyor. Yani siz Bitcoin madenciliği yaparken aslında yapılan harcamaların doğruluğunu ve güvenilirliğini onaylamak üzere başlatılan bir sürece destek vermiş oluyorsunuz. Dünya genelinde milyonlarca bilgisayar aynı anda kim, hangi Bitcoin parçasına sahip, bunu hangi anda, nereye harcamış, aynı parayı iki kere harcamaya yeltenen olmuş mu, birileri kayıtlarla oynamaya çalışmış mı diye kontrol ediyor ve elde ettikleri sonuçları diğerlerinin sonuçlarıyla karşılaştırarak yapılan harcamaların geçerli olup olmadığına hükmediyor.

## Bitcoin Hakkında Merak Edilenler

### Bitcoin dijital bir para birimi olduğuna göre, mevcut Bitcoin'leri elektronik ortamda istediğimiz kadar çoğaltmak mümkün değil mi?

Hayır. Sistemin kurgusu Bitcoin para birimini enflasyona ve aynı parayı birçok kez harcama gibi dolandırıcılık girişimlerine karşı koruyacak katı kurallar içeriyor. Ayrıca henüz dolaşıma girmemiş Bitcoin'lerin ne zaman dağıtılacağı ve toplamda en fazla kaç Bitcoin olacağı baştan itibaren belirlenmiş durumda.

Bitcoin'ler yaklaşık 10 dakikada bir dağıtılıyor ve yine yaklaşık her 4 yılda bir 10 dakika içinde dağıtılacak Bitcoin'lerin sayısı yarıya düşüyor. İlk dönem olan 2009-2012 yılları arasında sistem her 10 dakikada bir 50 Bitcoin dağıtıyordu. 2013'te başlayıp 2016 yılının Temmuz ayına kadar süren ikinci dönemde bu rakam 25'e düşmüştü. 9 Temmuz'dan itibaren kazanılacak ödül, sistem tarafından önümüzdeki dört yıl için 12,5 Bitcoin'e indirildi (bir sonraki düşüşün ne zaman olacağını www.bitcoinblockhalf.com adresinden de takip edebilirsiniz). Bu süreç 2140 yılında 21 milyon Bitcoin'in tümü sisteme katılana kadar devam edecek. Dağıtılan toplam Bitcoin adedi 21 milyonu asla geçmeyecek.

### Şu an piyasada kaç Bitcoin var ve bunların değeri ne kadar?

Bugüne kadarki tüm Bitcoin işlemlerinin ortalaması alındığında Bitcoin başına 415 dolar gibi bir ortalama fiyat çıkıyor. Bitcoin fiyatları talebe bağlı olarak değiştiği için gün içinde yüzlerce dolara varan fiyat oynamalarıyla karşılaşılabiliyor. Ben bu yazıyı yazarken dolaşımda olan Bitcoin adedi 15 milyon 691 bin idi ve birim fiyat da 621 dolardı. Bu da Bitcoin piyasasının toplamda yaklaşık 9,5 milyar dolarlık değeri olduğunu gösteriyor. 29 Kasım 2013'te Bitcoin'in ulaştığı 1242 dolarlık değer bugüne dek gördüğü en büyük değer olarak biliniyor.

### Bu kadar değerliyken Bitcoin'i bozdurup harcamak mümkün mü?

Evet. Bitcoin'i en küçük birimi olan Satoshi'ye dönüştürerek parça parça harcamak mümkün. 1 Satoshi, Bitcoin'in yüz milyonda birine karşılık geliyor. Ayrıca milyonda biri mikro Bitcoin, binde biri mili Bitcoin olarak adlandırılıyor.

### Bitcoin madencilerinin ortaya koyduğu işlem gücü ve harcadığı enerji hangi ölçekte?

Tahmin etmek zor. 2015 yılı sonunda çıkan haberlerde küresel ölçekteki Bitcoin madencilerinin toplam işlem gücünün dünyanın en iyi 500 süper bilgisayarının toplam işlem gücünün 11 bin katına ulaştığına dair haberler çıkmıştı. Motherboard sitesinden Sebastiaan Deetman'ın 2016 yılı Mart ayında yaptığı hesaplamalara göre dünya genelindeki Bitcoin madencileri 350 megavat, yani ABD'de 280 bin evin enerji ihtiyacını karşılamaya yetecek kadar enerji harcıyor. Deetman süreç böyle devam ederse Bitcoin ağının enerji ihtiyacının 2020 yılında 14 gigavata ulaşacağına, bunun da Danimarka'nın toplam enerji ihtiyacına eşit olacağına işaret ediyor. Bu nedenle bu işte kâr zarar hesabı yaparken harcayacağınız zaman ve enerjiyi göz ardı ederseniz, ciddi zarara girebilirsiniz.

Bu durum, Bitcoin'e haklı eleştiriler yöneltilmesine neden oluyor. Bitcoin, zaman içinde yeni Bitcoin üretimini yavaşlatmak amacıyla işlemleri yapay olarak zorlaştırdığı için, milyonlarca bilgisayarın bu işe ayrılmasının yanı sıra sırf bu işe özel işlemcilerin ve hesaplama sistemlerinin geliştirilmesine neden oldu. Günümüzde normal bilgisayarların Bitcoin madenciliği için özel tasarlanmış işlemciler ve cihazlar karşısında neredeyse hiç şansı yok. Ayrıca işleri zorlaştırmak için yapay olarak kurgulanan bu sistem, çok ciddi bir enerji israfına yol açıyor.

### Bu kadar işlem gücü ve enerji tüketimi sadece yeni Bitcoin'ler bulmak için mi?

Bitcoin madenciliği şu an muhtemelen dünyanın en güçlü dağıtık bilgisayar ağına sahip. Gönül isterdi ki bu işlem gücü kanser ve diğer hastalıkların tedavisi için işe yarayacak molekül alternatifleri keşfetmekten uzayda akıllı yaşamın izlerini aramaya kadar, başka amaçlar için de kullanılabilsin. Maalesef olmuyor. Bitcoin madenciliğinin temelini oluşturan hesaplama yaklaşımı, sistemin farklı bir amaç için kullanılmasına izin vermiyor. Ne kadar büyük bir kayıp...

### Ben de Bitcoin madenciliği yapabilir miyim?

İsterseniz tabii ki, neden olmasın. Ama şu an dünya genelinde yeni Bitcoin'leri keşfetmek için öylesine büyük bir rekabet var ki, belki bu iş ilk çıktığında günde 100 Bitcoin toparlamaya yetecek olan bilgisayarınız aynı seviyeyi tutturmak için artık


belki de milyonlarca yıl uğraşmak zorunda. Bu nedenle bu işe tek başınıza girmek yerine Bitcoin madencilerinin oluşturduğu havuzlara katılmayı deneyebilirsiniz. Binlerce kullanıcıyı bir araya toplayarak birlikte aramaya çıkan bu havuzlar, havuzda yer alan herhangi birinin sıradaki Bitcoin'leri keşfetmesi durumunda ganimeti uygun şekilde tüm üyeler arasında paylaştırıyor. Bu şekilde daha fazla şansınız olabilir.
Diğer yandan bu havuzların başa dert olduğu durumlar da var. Bitcoin'de eski bir kaydı değiştirerek sistemi kandırmak isteyen herhangi birinin bunu sistemde yer alan tüm bilgisayarlardan daha hızlı yapması gerektiğinden, bunun da tek kişi için neredeyse imkânsız olduğundan bahsetmiştik. Ama olur da sistemdeki madencilerin yarısından fazlasını ortak bir havuzda toplayabilirseniz, bir anda merkezi yönetime sahip olmamak üzere kurgulanmış bir sistemde karar verici çoğunluğa dönüşebilirsiniz.
Bitcoin platformunun yüreğini ağzına getiren ve "%51 Krizi" adı verilen bu durumun bir örneği 2014 yılında yaşandı. GHash adlı bir madenci grubu bir süre için sistemde %50'nin üzerinde ağırlığa sahip oldu ve tüm sistemi risk altında bıraktı. Sorun grupta yer alan bazı madencilerin gönüllü olarak diğer gruplara geçmesiyle çözüldü.

**Bitcoin fiyatları neden bu kadar değişken?**

Bitcoin gün içinde bile yüzlerce dolarla ifade edilen fiyat değişimleri yaşayabiliyor. Bu tamamen arz talep meselesi. Belli bir zamanda Bitcoin almak isteyenlerin sayısı artarsa fiyat yükseliyor, azalırsa fiyat düşüyor. Değişimin bu kadar hızlı olmasının sebebi Bitcoin para biriminin toplam piyasa değerinin diğer geleneksel para birimlerine kıyasla düşük olması. Örneğin trilyonlarca dolar değere sahip bir piyasada yaprak kımıldatmayacak bir hareket, 10 milyar dolarlık Bitcoin piyasasında büyük dalgalanmalara neden olabiliyor. Bitcoin piyasasının değeri arttıkça bu dalgalanmaların azalacağı düşünülüyor.

**Bazı Bitcoin işlemlerinden komisyon alındığını duydum. Bu komisyon merkezi bir yönetime bağlı olmayan bir sistemde kimlere gidiyor?**

Bitcoin madencilerinin yaptığı işin aslında boş bir iş olmadığından ve yapılan her hesaplamanın sistemin güvenliğini artırdığından bahsetmiştik. Bu yüzden madenciler emeklerinin karşılığını sadece 10 dakikada bir dağıtılan yeni Bitcoin'ler olarak değil, bazen de işlem komisyonu olarak alıyor. Bunun nasıl olacağına da yine sistem karar veriyor. Örneğin yaptığınız bir alışveriş karşılığında elinize geçen Bitcoin'i aynı gün harcamaya yeltenirseniz sistemin size komisyon kesme olasılığı artıyor. Neden? Bitcoin'in işleyişi gereği bir işlemin kayıt defterindeki yeri ne kadar eskiyse, birilerinin bu işleme dair hile yapabilme olasılığı o kadar azalıyor. Böylece sistem sizi bundan caydırmaya çalışıyor. Bir süre sonra dağıtılan Bitcoin sayısı iyice azaldığında, dağıtılan komisyonların madencilerin en büyük gelir kapısına dönüşeceği öngörülüyor. 2140 yılından itibaren ise sistemde komisyon hariç gelir elde etme imkânı kalmayacak. O zamana kadar sistem kalırsa tabii.

**Bitcoin çalınmaya karşı güvenli mi?**

Pek sayılmaz. Bir Bitcoin'in size ait olduğunu ispatlamak için, herkese açık şifreleme anahtarının yanında bir de sadece sizde olan ve başka hiç kimsenin bilmediği bir özel anahtar göstermeniz gerekir. Böylece sistem elinizdeki varlığın geçerli olduğuna karar verir. Eğer bu anahtarı kaptırırsanız varlığınızı da kaptırmış olursunuz. Mesela FBI tarafından Silk Road operasyonunda ele geçirilen ve açık artırmayla satılan 1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55 kodlu anahtar 30 bin Bitcoin içeriyordu. Yani şu dizilim daha önce sizin elinize geçmiş olsaydı 20 milyon dolar cebinizdeydi.

Bu durum bilgisayar korsanlarını Bitcoin madenciliğiyle uğraşmak yerine doğrudan kişilerin cüzdanında, hatta Bitcoin aracı kuruluşlarında bulunan Bitcoin'leri çalmaya itiyor. Çünkü daha zahmetsiz ve karşılığında gelen ödül de bir o kadar cazip. Dünyanın en büyük Bitcoin borsalarından Mt. Gox'a yapılan ve şirketin iflasına sebep olan 460 milyon dolarlık vurgun bunun en acı ve çarpıcı örneğiydi. Bugün elinde hatırı sayılır miktarda Bitcoin varlığı olan çoğu kişi, bunu çevrimiçi veya cep telefonu gibi kolay ele geçirilecek bir platformda saklamak yerine USB belleğe yazıp banka kasasına kilitlemeyi veya yazıcıdan kodun çıktısını alıp kâğıdı bir yerlere saklamayı tercih ediyor.

**Elimdeki Bitcoin varlığına dair özel anahtarı kaybedersem ne olur?**

Söz konusu Bitcoinler üzerindeki kontrolünüzü kaybedersiniz ve kimse bunları bir daha geri getiremez. Bir anlamda ilgili tutar kimsenin işine yaramayan zombi varlığa dönüşür. İnternet içinde Bitcoin olduğunu unutup sabit diskine format atan kişilerin hikâyeleriyle dolu. 7500 Bitcoin'lik cüzdanını barındıran sabit diskini çöpe atan James Howells bunun en çarpıcı örneklerinden.


**Sık sık Bitcoin'in suçluların gözde para birimi olduğunu duyuyorum. Gerçekten de öyle mi?**

Olaya neresinden baktığınıza bağlı. Bitcoin merkezi bir yönetime sahip olmadığı için paranıza el koyulması, ödemelerin en son kişiye kadar takip edilmesi gibi, klasik finansal kuralların dışında bir yapısı var. Bu sebeple araya aracı koymadan, kendilerini ele vermeden alışveriş yapmak veya fidye toplamak isteyen siber suçluların özellikle tercih ettiği bir ödeme alternatifi olduğu doğru. Diğer yandan bazı uzmanlar sistemin kara para aklama ve benzer amaçlarla kullanıldığı görüşünün abartılı olduğunu düşünüyor. Suçla ve uyuşturucuyla küresel ölçekte mücadele etmek için kurulan UNODC verilerine göre dünyada her yıl aklanan kara para miktarı 800 milyar dolarla 2 trilyon dolar arasında değişiyor. Bugün tüm Bitcoin'leri tek bir elde toplasanız (ki bu mümkün değil), aklayabileceğiniz kara para en fazla 10 milyar dolar olurdu. Bu da dikkat çekici olmakla birlikte küresel suç ekonomisinin büyüklüğüne kıyasla hayli küçük bir meblağ.

**Bitcoin ile neler satın alabilirim?**

Ödeme sistemi olarak Bitcoin kabul eden dükkânlarda satılan hemen hemen her şeyi. Kahve, bilgisayar, otomobil, çiftlik evi, hatta uzay turu...

**Bitcoin'in alternatifleri var mı?**

Evet. 10 milyar dolara yaklaşan piyasa değerine sahip olan Bitcoin'i 1 milyar 230 milyon dolarlık Ethereum ve 249 milyon dolarlık Litecoin takip ediyor. Bu alternatifler Bitcoin'in getirdiği ilkeleri daha ideal koşullarda sunduklarını dile getirseler de mükemmel değiller. Geçtiğimiz ay siber suçluların Ethereum'a saldırarak 50 milyon dolar değerinde vurgun yapması, para biriminin temelinden sarsılmasına neden oldu.

**Bitcoin kullanmaya nasıl başlayabilirim?**

Bunun için önce kendinize bir Bitcoin cüzdanı oluşturmanız gerekiyor. Başlangıç için ihtiyacınız olan tüm bilgileri bitcoin.org adresinde bulabilirsiniz.

Ama iş burada bitmiyor. Bir zincir halkası içinde yer alan harcamaların Bitcoin kayıt defterine kalıcı olarak işlenebilmesi için bu halkanın bir de kendinden önceki zincire bağlanması lazım. Yani elinizdeki zincir halkasının bağlantısını bir şekilde gevşetmeniz gerekiyor ki, götürüp kendinden önceki uzun zincire bağlayarak zincirin kalıcı bir parçası haline getirebilesiniz.

İşte bu noktada *hash* adlı verilen bir kavram devreye giriyor.

## Milyonları Peşinden Koşturan Yarış

*Hash* kavramını en basit şekilde son derece karmaşık bir problemin çözülmesi sonucunda elde edilen, doğrulaması kolay ama geri döndürülmesi ve tahmin edilmesi zor bir işlemin sonucu olarak tanımlamak mümkün. Mesela size "iki rakamı topladım ve sonuç 22 oldu" dediğimi varsayın. Bu sonuca ulaşmak için pek çok ihtimal ortaya atabilirsiniz. Örneğin 1 ile 21'i ya da 13 ile 9'u toplamış olabilirim. Ama size "8 ile 14'ü toplayın" dersem bulduğum sonucu kolayca doğrulayabilirsiniz.

İşte sistemde üretilen Bitcoin zincirine ait her halka, karmaşık bir matematiksel işlem sonucunda ortaya çıkan *hash* değeriyle birlikte geliyor. Bu değer aslında tamamen gelişigüzel değil. Biraz içerdiği Bitcoin aktarma bilgilerine, biraz da zincirin kendinden bir önceki halkasının *hash* değerine bağlı. Bitcoin bulmak için uğraşan bilgisayarlar bir yandan işlemleri doğrularken bir yandan da bu zinciri diğer zincirlere bağlayacak olan bu *hash* değerini ortaya koyan doğru işlemi bulabilmek için hesaplama yapıyor. En nihayetinde biri doğru sonucu veren işlemi buluyor, diğer bilgisayarlara "ben buldum" diye mesaj gönderiyor. Diğer bilgisayar işlemi ve sonucu doğruladığında işlemi bulan kişi zincirin bu halkasına atanmış olan Bitcoin'leri ödül olarak alıyor. Ardından halka uzun zincire bağlanıyor, içeriğindeki tüm kayıtlar deftere işleniyor ve kalıcı hale geliyor.

Sistemin mucidi Satoshi Nakamoto bunu öylesine kurgulamış ki, ilgili *hash* değerine ulaşmak için çözülmesi gereken işlemin zorluğu o an dünyada Bitcoin bulmak için uğraşan bilgisayarların toplamının işlem gücüne uyum sağlamak için sürekli değişiyor. 2009 yılında yalnızca birkaç tane kişisel bilgisayar bu iş üzerinde çalışırken de problemin çözülmesi için gereken süre yaklaşık 10 dakikaydı, bugün dünyanın ilk 500 süper bilgisayarının toplam işlem gücünün on binlerce katına sahip küresel bir bilgisayar ağı bu iş üzerinde uğraşırken de süre yine 10 dakika.

Tüm bu zahmetin bir sebebi de kayıt defterine yazılı olan geçmiş harcamaları değiştirmeye yönelik olası müdahaleleri zorlaştırarak imkânsız hale getirmek. Düşünün ki bir halkadaki kaydı değiştirerek kendiniz için bundan fayda elde etmek, yani işlem tarihçesini değiştirerek sistemi menfaat sağlamak üzere kandırmak istiyorsunuz. Bunu yapabilmek için sadece o halkadaki değil, o halkaya gelene kadarki tüm zincirde sistemin kurallarına göre yeniden bir *hash* formülü bulmak zorundasınız. Üstelik de bunu tüm Bitcoin camiasından daha hızlı yapmak zorundasınız.

Kimsenin elinde böyle bir sistem olmadığı gibi, bunu gerçekleştirmek için harcanacak zaman ve enerji elde edilecek faydanın kat be kat üzerine çıkıyor. Bir örnekte, sadece tek bir işlem kaydını değiştirmek için ihtiyaç duyulacak güçte bir sistemi kurgulamanın yüz milyonlarca dolara mal olacağından bahsediliyordu. Özetle sistemde ne kadar çok madenci varsa, sistem saldırı ve suistimallere karşı o kadar iyi korunuyor.

## Bitcoin'in Değeri Nereden Geliyor?

Gelelim bir diğer merak uyandıran konu olan Bitcoin'in değerinin nereden geldiği sorusuna. Bu aslında cevap vermesi zor bir soru. Örneğin Hazine'nin ve Türkiye Cumhuriyeti Merkez Bankası'nın kontrolünde olan Türk Lirası'nı ele alın. Türk lirası değerli. Neden? Çünkü emeğinizin karşılığını onunla alıyorsunuz, verginizi onunla ödüyorsunuz, alışverişlerinizi onunla yapıyorsunuz. Altın deseniz, Dünya üzerinde sınırlı miktarda bulunan parlak ve değerli bir maden. Küresel piyasalarda para olarak daima bir karşılığı var. Petrol, çağdaş dünyanın enerji ihtiyacının karşılanmasında çok önemli bir yere sahip. Peki ama bir dizi bilgisayarın kafa kafaya vererek çözdüğü matematiksel işlemlerin sonucunda dağıtılan şifreli bir karakter dizisine neden bu kadar değer biçiliyor?

Bunu daha iyi anlamak için Bitcoin'e sadece bir para birimi olarak bakmamak lazım. Bitcoin sergilediği özellikler itibarıyla üç kavramın kesişim noktasını simgeliyor: Para birimi, hisse ve sosyal medya. İşin para birimi kısmını anlamak kolay, geleneksel para birimlerine kıyasla sunduğu avantajlara da daha önce değinmiştik. Hisseye olan benzerliği, Bitcoin ekosisteminin büyüklüğü arttıkça Bitcoin piyasasının toplam değerinin artması ve birim fiyatın hisse senetlerinde olduğu gibi sürekli dalgalanmasıyla açıklanıyor.

Ancak belki de Bitcoin'e değer verilmesinin en büyük sebebi, yapısının sosyal medyayla olan benzerliği. Bitcoin değerli, çünkü çok fazla kişi tarafından kullanılıyor ve talep görüyor. Son dönemlerde dünyayı değiştiren her teknoloji arkasına kullanıcıları alarak büyüdü. Napster da böyleydi, Facebook da böyle büyüdü. Günümüzde güçlü bir sosyal etkiyi arkasına alan her platform hızla değer buluyor. Kendisinden sonra gelen Ethereum gibi platformların daha iyi işlevsellik sunma vaatlerine rağmen Bitcoin'in Ethereum'a oranla 10 kat daha değerli olmasının nedeni, çok daha fazla sayıda kullanıcının Bitcoin ekosisteminde yer alması.

Neticede arkasında yer alan teknik ne kadar etkileyici olursa olsun, kullanan olmadığı sürece herhangi bir teknolojinin anlamı yok.

Şimdiki soru şu: Acaba Bitcoin bu sosyal etkiyi daha ne kadar devam ettirebilecek?

**Kaynaklar**
- http://www.coindesk.com/
- http://www.cnbc.com/2014/01/23/cnbc-explains-how-to-mine-bitcoins-on-your-own.html
- http://codinginmysleep.com/bitcoin-mining-in-plain-english/
- http://www.economist.com/bitcoinexplained
- http://www.reuters.com/article/us-bitcoin-criminals-insight-idUSBREA2D09820140314
- http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin
- http://arstechnica.com/security/2014/06/bitcoin-security-guarantee-shattered-by-anonymous-miner-with-51-network-power/