Börteçin Ege

Sanal Dünyanın Gerçek Parası

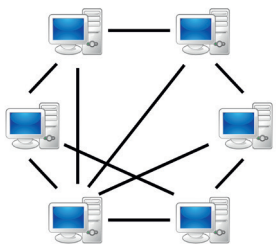
Bitcoin

İnternetin dünyamızı her yönüyle değiştirdiği biliniyordu, fakat sadece internet ortamında üretilen ve internet ortamı dışında da geçerli bir sanal paraya henüz hiç kimse, tam anlamıyla hazırlıklı değildi açıkçası. Üretiminden dağılımına ve kur değerine kadar hemen hemen her şeyinden devlet ve bankalar yerine internetteki bazı borsa ve kullanıcıların sorumlu olduğu bu sanal para birimi, birçok sürpriz de barındırmıyor değil. Sadece sınırlı miktarda fakat son derece karmaşık yöntemlerle üretilen Bitcoin adlı bu para birimini nasıl bir geleceğin beklediği konusunda gerçekçi bir tahminde bulunmak zor olsa bile, bu türdeki sanal para birimleri şimdiden internetten sonra dünyayı değiştirecek en önemli icatlardan biri olmaya aday. Son zamanlarda yaşanan bazı gelişmeler sonrası Bitcoin, ABD ve Almanya gibi birçok gelişmiş ülkenin hükümetlerini telaşa düşürmüş durumda. Gerçekten de şu sıralar hükümetlerden normal internet kullanıcısına kadar hemen hemen herkesin kafasında aynı soru var: Bitcoin gerçekten geleceği olan masum bir para ödeme aracı mı, yoksa bazı internet çevrelerinin şişirmek üzere olduğu yeni bir balon mu? Gelin şimdi, bu yılın Ekim ayı başı itibarıyla bir birimi 137 doları bulmuş olan bu sanal para biriminin tarihçesine ve işleyiş biçimine bir göz atalım.

>>>

Bitcoin Nedir?

Esasında her şey Bitcoin üzerine oluşturulan ilk taslağın 2008 yılında kendine Satoshi Nakamoto adını veren bir şahıs veya grup tarafından bir e-posta listesinde yayımlamasıyla başladı. Günümüzde bile, özellikle üretimi hakkındaki detayları konunun gerçek uzmanları dışında hemen hemen hiç kimse tarafından tam olarak anlaşılamayan bu taslağa göre, Bitcoin bankaların, merkez bankalarının ve hükümetlerin dahi söz sahibi olmadığı, merkezi olmayan bir yapı üzerinden sadece sanal ortamda üretiliyor ve yine sanal ortamda yönetilmesi planlanıyor. Elektronik bir para birimi olan Bitcoin, sanal ortamda bir bilgisayar ağ sistemine dâhil olan kullanıcılar arasında, istendiği gibi havale edilerek paylaşılabiliyor ve gerçekleştirilen her elektronik işlem sistem tarafından dijital bir imzayla imzalanarak merkezi bir veri tabanına kaydediliyor. Bu arada hatırlatmakta fayda var: Bitcoin aynı zamanda bu para biriminin oluşturulmasını sağlayan yazılım sisteminin de adı. Şimdi, dünyaya gözlerini yeni açan ve hayli karmaşık bir üretim ve işleyiş süreci olan bu sanal para biriminin nasıl işlediğini hep beraber anlamaya çalışalım.



Geleneksel istemci-sunucu modelinden farklı olarak, bir P2P ağına bağlı bilgisayarlar herhangi bir merkezi koordinasyona ihtiyaç olmadan kaynaklarını birbirlerine kullandırtabilir.

Başlıca Kullanım Alanları

İlke olarak ister fiziksel ortamda olsun isterse internet ortamında, Bitcoin'i geçerli bir para birimi olarak kabul eden her yerde (restoranlar, kafeler, özel doktorlar, kuaförler, oteller, sanal para borsaları vb.) bu para kullanılabiliyor. Listeyi dilediğimiz gibi uzatmamız mümkün. Daha şimdiden Bitcoin'in başkenti olarak adlandırılan Berlin'de (Almanya) aralarında kuaförlerin, barların ve özel doktorların da bulunduğu en az 30-40 ticari işletmenin, Silikon Vadisi'ndeki bazı emlakçıların, Londra ve Toronto'daki bazı işletmelerin ve İsrail'deki avukatlık bürolarının Bitcoin'i geçerli para birimi olarak kabul edip kullandığı biliniyor. Fakat yine de Bitcoin denilince genelde akla gelen ilk isim internetteki Mt. Gox adlı Bitcoin borsası. Tokyo merkezli olarak 2010 yılında kurulan ve dünyanın en büyük Bitcoin borsası olan Mt.Gox, hem Bitcoin'lerin dolar ve euro gibi geleneksel para birimlerine bozdurulmasına hem de dolar ve euro gibi para birimleri karşılığında Bitcoin satın alınmasına imkân tanıyor.

Bitcoin Üretimi

Eğer Bitcoin kimler tarafından ve nasıl üretiliyor diye soracak olursanız, buna verilecek en basit cevap üretiminde kullanılan sistemin belki de dünyadaki en karmaşık sistemlerden biri olduğu ve üretim sürecinin konuya yabancı insanlar tarafından anlaşılmasının neredeyse imkânsız olduğudur. Buna göre, üretilecek olan para yani Bitcoin miktarı Bitcoin yazılımının beynini oluşturan bir algoritma tarafından, belirli bir zorluk derecesine sahip bazı matematiksel problemlerin çözülmesiyle hesaplanıyor. Fakat bu süreç o kadar karmaşık ki hesaplamalar için ihtiyaç duyulan bilgisayar gücü çok fazla olduğundan bu ihtiyacın sadece normal birkaç bilgisayarla karşılanması mümkün değil. Bitcoin, açık kaynak kod tabanlı bir hareket olduğundan ve bu tabanın - en azından şimdilik - yüksek kapasiteli süper bilgisayarlara sahip olması imkânsız olduğundan, hesaplamalar için gerekli işlem gücü, bir bilgisayar ağına (tam olarak bir Peer-to-Peer-Network, kısaca P2P) bağlı çok yüksek kapasiteli bilgisayarlar tarafından ortaklaşa yaratılıyor (Mining Pool). Belirli bir zorluk seviyesindeki her bir matematiksel problemin çözümünde bilgisayarlarını bu ağın hizmetine vermiş olan her Bitcoin Madencisi'ne (*Miner*) Bitcoin yazılımı tarafından ortalama 25 Bitcoin'lik (yaklaşık 3500 dolar) bir ödül veriliyor.

Bitcoin Hakkında Bilmeniz Gerekenler

Teknik Özellikler

- Bir Bitcoin, ağ içinde olmak şartıyla istenilen yere transfer edilebilir.
- Bitcoin ile yapılan işlemlerin geri dönüşü yoktur, dolayısıyla yapılmış olan bir işlem iptal edilemez.
- Bir Bitcoin sadece bir defa harcanabilir.
- Bitcoin ile işlemler sadece saniyeler içinde gerçekleşir, fakat sistem tarafından onaylanması ancak 10 dakika ile bir saat arasında gerçekleşir.
- İşlemlerin geçekleştirilmesi ve para ihracı madencilik sırasında topluca gerçekleştirilir.
- Kullanıcı kendisine gelen işlemleri her an alabilir, o sırada bilgisayarının açık veya kapalı olmasının bir önemi yoktur.

Ekonomik Kurallar

- Tedavüle çıkabilecek Bitcoin miktarı en fazla 21 milyon Bitcoin olarak belirlenmiştir.
- Bitcoin'ler 8 ondalık basamağa kadar bölünebilir.
- Bitcoin ile yapılan işlemler ucuz, hatta genelde bedavadır.
- Bitcoin değeri hayli değişkendir, dolayısıyla bir Bitcoin'in değeri kısa sürede kestirilemeyecek kadar artıp azalabilir.
- Bitcoin hâlâ gelişim aşamasında bulunan deneysel bir para birimidir.

İstatistikler

- Bitcoin ağı dört yıldan bu yana sürekli çalışmaktadır.
- Bitcoin Vakfı, dünyanın en büyük bilgisayar ağlarından birine sahiptir (65 Terahash/saniye).
- Bitcoin ile günlük işlem hacmi tutarı daha şimdiden milyonlarca dolara ulaşmıştır.
- Bitcoin bilgisayar ağında yapılan günlük işlem sayısı 50.000 civarındadır.
- Günümüzde tedavüldeki bütün Bitcoin'lerin değeri 1,5 milyar dolardan fazladır.
- Bitcoin bilgisayar ağındaki en son güvenlik sorunu Ağustos 2010'da yaşanmıştır, söz konusu güvenlik açığı fark edildikten kısa bir sonra giderilmiştir.

ABD ve Almanya hükümetleri başta olmak üzere ekonomileri gelişmiş birçok hükümet, Bitcoin gibi internet ortamında üretilen sanal paralarla kara para aklanması ve yasadışı ticari etkinliklerde bulunulması konusunda hayli hassas. Son olarak, internetteki başka bir sanal para birimi olan Liberty Reserve bu kurallara uymamanın cezasını kapatılarak ödedi.

Bitcoin, Satoshi Nakamoto takma adlı yaratıcısı tarafından, tedavüldeki miktarı toplam 21 milyon Bitcoin'i geçmeyecek şekilde tasarlanmış olsa da Ekim 2013 itibarıyla, öngörülen bu miktarın neredeyse yarısı (yaklaşık 11.750.000 Bitcoin) şimdiden üretilmiş ve tedavüle çıkmış durumuda. Fakat uzmanlara göre, Bitcoin üretiminde kullanılan matematiksel problemlerin zorluk düzeyi, her bir çözümden sonra Bitcoin üreticileri tarafından kademeli olarak artırıldığı için, bundan sonraki hesaplamaların ve dolayısıyla Bitcoin üretim sürecinin bugüne kadarkinden çok daha zorlu geçmesi ve uzun zaman alması bekleniyor. Böylece Satoshi Nakamoto tarafından yapılan plana göre 21 milyon Bitcoin'in tamamı ancak 2034'te üretilmiş olacak. Görüldüğü kadarıyla 2034'ten sonrası için ortada henüz bir plan yok. Dolayısıyla Bitcoin'in dünya ekonomisine 2034'ten sonraki etkisi üzerine herhangi bir yorumda bulunmak için henüz çok erken.

Bitcoin üretim süreci üzerine akla gelen başka bir soru ise şu: Normal bir internet kullanıcısının çok yüksek kapasiteli bir bilgisayar ile Bitcoin Madencisi (*Miner*) olarak Bitcoin üretimine katılması ne derece akıllıca? Yukarıda da belirtildiği gibi normal kullanıcıların söz konusu üretim sürecine PC ve Notebook gibi normal bilgisayarlarla katılması, bunların kapasite açısından yetersiz olması nedeniyle anlamsız. Bir Bitcoin Madencisi'nin yüksek performanslı donanıma yapacağı yatırım, üretim için harcayacağı elektrik ve diğer olası altyapı ve bakım masrafları düşünüldüğünde, ortalama bir internet kullanıcısının bu sürece katılması hiç de akıl kârı değil gibi. Sonuç olarak en azından içinde bulunduğumuz aşamada Bitcoin'i yatırım veya ödeme aracı olarak görüp kullanmayı düşünenlerin doğrudan Mt. Gox gibi bir internet borsasına giderek Bitcoin satın alması daha ucuz ve mantıklı bir çözüm yolu gibi görünüyor.

>>>

Bitcoin Kullanımı Gerçekten Anonim mi?

Bitcoin hakkındaki şehir efsanelerinden biri de kullanımının normalde yüzde yüz anonim olduğu. Bu, her ne kadar kuramsal olarak mümkün olsa da günlük hayattaki uygulamalarda gerçekten çok da istenen bir durum değil. İşlemlerin anonim olarak yapılması sonucunda Bitcoin'in özellikle para aklama gibi yasal olmayan alanlarda da kullanılması olasılığı, en başta ABD hükümeti olmak üzere dünyadaki birçok hükümeti endişelendiren bir husus. Örneğin dünyanın en büyük Bitcoin borsası olan Mt. Gox, bu yılın Mayıs ayının sonlarına doğru aldığı bir kararla, borsada açılmış ve açılacak tüm Bitcoin hesaplarına her kullanımda doğrulanma zorunluluğu getirdi. Dolayısıyla kendi hesabından Bitcoin çekmek isteyen veya elindeki Bitcoin'leri dolar ve euro gibi geleneksel para birimlerine bozdurmayı amaçlayan her kullanıcı bu yeni kurala uymak zorunda. Mt. Gox yöneticileri, bu gelişmeyle beraber Bitcoin'in para aklama ve buna benzer, yasal olmayan başka ticari işlerde kullanılmasının zorlaşacağını hatta imkânsız hale geleceğini, böylece Bitcoin üzerindeki endişe ve baskıların azalacağını düşünüyor.

coin

Facebook'un patronu Mark Zuckerberg ile giriştikleri hukusal mücadele ile tanınan Winklevoss kardeşler Bitcoin yatırımcısı olarak geri dönüyor.

Ayrıca söz konusu yeni kuralın, kullanımı tamamen anonim olan Liberty Reserve adlı sanal para biriminin ABD hükümeti tarafından yasaklanmasından hemen sonra konulması, Bitcoin üzerindeki politik baskıların arttığının bir işareti olarak görülüyor.

Bitcoin Transfer Sistemi Nasıl İşliyor?

Bitcoin bilgisayar ağında gerçekleştirilen her Bitcoin işlemi, bazı kullanıcı bilgileriyle beraber, açık olarak ve bir daha silinmemek üzere kayıt altına alınıyor. Bu, aynı zamanda herhangi bir Bitcoin adresi tarafından gerçekleştirilen tüm işlemlerin ve söz konusu Bitcoin adresine ait güncel bakiyenin tüm kullanıcılar tarafından da görülebileceği anlamına geliyor. Fakat kullanıcı bunları yaparken, tüm kişisel bilgilerini sistemde açıkça paylaşmak zorunda değil. Her ne kadar tüm bu işlemler sırasında güvenlik nedenlerinden dolayı bazı kriptolojik sistemler kullanılıyor olsa bile, Liberty Reserve'dekinin aksine, Bitcoin'de -bazı ek sistemler kullanılmadığı sürece- işlem yapan kullanıcının gerçek kimliğine en azından güvenlik birimleri tarafından eninde sonunda ulaşılabiliyor. Bundan dolayı Bitcoin Vakfı gerçekten anonim kalmak isteyen kullanıcılara bazı ek güvenlik sistemleri ve her alım işlemi için ayrı bir Bitcoin adresi kullanmalarını tavsiye ediyor. Dolayısıyla genel olarak kullanıcıların isteğine göre hâlen anonim işlem yapmak mümkün. Bu durum tabii ki Bitcoin ile yapılan tüm işlemleri takip etmek isteyen hükümetler açısından bazı endişeleri de beraberinde getiriyor.

Madalyonun Diğer Yüzü

Uzmanlara göre, Bitcoin üretiminde kullanılan ve yine Bitcoin olarak adlandırılan yazılım gerçekten son derece güvenli. Hatta iddialara göre açık kod olarak internette bulunan yazılımda, konunun birçok uzmanı ve bilgisayar korsanı tarafından yapılan incelemelere rağmen tek bir teknik açığa ve hataya rastlanamamış. Fakat genelde Bitcoin kullanımı sırasında ortaya çıkan sorunlar, zaten hayli sağlam matematiksel denklemler üzerine kurulmuş olan bu sistemin kendisinden değil aksine her zamanki gibi bu sistemi kötüye kullanmaya çalışan bazı insanlardan kaynaklanıyor. Bundan dolayı, Bitcoin kendi yaratıcılarına, bilgisayar korsanlarına ve özellikle de yeraltı dünyasında mutlak anonim bir para birimi peşinde koşan bazı kişilere harika bir ödeme aracı gibi görünse de bazı potansiyel problemleri de beraberinde getiriyor.

Gerçekten de genel olarak Bitcoin sisteminin doğasında yatan bazı zayıflıklar, neredeyse insanın saçlarını yoldurtacak türden desek abartmış olmayız. Tipik bir örnek olarak Facebook kurucusu Mark Zuckerberg ile giriştikleri hukuksal mücadeleden tanıdığımız ve yakın bir zaman önce büyük Bitcoin yatırımcısı olarak geri dönen ünlü Winklevoss kardeşleri gösterebiliriz. Winklevoss'lar bile sisteme -en azından şu an için- tam olarak güvenemediklerinden, ellerinde bulunan büyük miktardaki Bitcoin'leri (tahminen 90.000 Bitcoin, yaklaşık 12,5 milyon dolar) bilgisayarlar yerine banka kasalarındaki USB cihazlarında saklıyor. (Son zamanlarda bazı bilgisayar korsanları tarafından Bitcoin kullanıcılarına verilen bazı büyük zararlardan sonra çok da haksız olmadıkları düşünülebilir). Şimdi, şu ana kadar bilgisayar korsanları tarafından bazı Bitcoin kullanıcılarına verilen zararlardan birkaç tanesine göz atalım:

Haziran 2011'de dünyanın en büyük Bitcoin borsası olan Mt. Gox'a, Hong Kong IP adresli bilgisayarlarla düzenlenen siber saldırı sonucu, bilgisayar korsanları kısa bir süreliğine de olsa piyasada bulunan Bitcoin'lerin yaklaşık yüzde 7,7 gibi hatırı sayılır miktarını ele geçirdi. Saldırı sonrasında Bitcoin borsası neredeyse çöktü ve güncel Bitcoin kurunda büyük düşüşler yaşandı. Mt. Gox tarafından yapılan açıklamada korsanlar tarafından gerçekleştirildiği tespit edilen binlerce işlemin iptal edileceği ve düşen kur değerinin yeniden eski değerine çekileceği belirtildi.

Mart 2012'de yeterli düzeyde güvenlik sistemine sahip olmayan bir sunucuya sızan bilgisayar korsanları, sunucuda bulunan toplam 230.000 dolar değerindeki Bitcoin'i çalarak kayıplara karıştı.

Eylül 2012'de New York merkezli ünlü Bitcoin borsalarından biri olan Bitfloor'a bir siber saldırı gerçekleştiren bilgisayar korsanları yaklaşık 250.000 dolar değerinde Bitcoin ele geçirdi ve ortadan kayboldu.

Fakat işin doğrusu Bitcoin ile ortaya çıkan problemler birkaç örnekle sınırlı değil. Sistemin hayli yeni olmasından ve doğasından kaynaklanan ve bir an önce hukuksal açıdan açıklığa kavuşturulması gereken başka sorunları da var. Örneğin Bitcoin'lerin saklandığı bilgisayarların sabit disklerinin aniden bozularak Bitcoin'lerin kaybolması durumunda veya uzun süren elektrik kesintilerinde neler yapılabileceği, bilgisayarınıza sızdıktan sonra elinizdeki Bitcoin'leri kopyalayarak sadece saniyeler içinde dünyanın öbür ucundaki anonim bir alıcıya gönderen olası virüslerle teknik ve hukuksal yönden nasıl baş edilebileceği gibi konular hâlen belirsiz.

İstihbarat Teşkilatlarının Bitcoin Fobisi

Tüm bu belirtilenlerin dışında bir sorun daha var ki bugünlerde hükümetlerin ve en başta CIA olmak üzere birçok istihbarat örgütünün hayli canını sıkıyor: Gelecekte, aynı Liberty Reserve'de olduğu gibi, Bitcoin'in de yeraltı dünyası ve terör örgütleri tarafından sistemli bir şekilde kara para aklamada, uyuşturucu kaçakçılığında, silah alımında ve buna benzer diğer yasal olmayan faaliyetlerde kullanılma olasılığı. Bu konu üzerindeki huzursuzluk hayli büyük boyutlara varmış olmalı ki iddialara göre bu yılın Haziran ayında Bitcoin'in kurucusu Satoshi Nakamoto'nun halefi ve şimdiki patronu Gavin Andresen, CIA tarafından bilgi verme amaçlı bir sunum için CIA merkezine çağrılmış. Kısacası Bitcoin ile ilgili her gelişme sadece normal kullanıcılar, finans dünyası ve bilgisayar korsanları tarafından değil, aynı zamanda istihbarat teşkilatları tarafından da çok dikkatli bir şekilde takip ediliyor.

Google'ın patronu Eric Schmidt ve Google'ın *Ideas* bölümünün kurucusu ve başkanı Jared Cohen

Sonuç

İnternet ortamındaki sanal kimliğimizin ve sanal toplulukların giderek daha fazla ağırlık kazandığı ve hatta geleneksel kimliğimizin ve geleneksel toplulukların önüne geçmeye başladığı bir dönemde yaşıyoruz. İnternetin de katkısıyla küreselleşme süreci tüm hızıyla devam ediyor ve insanlar artık neredeyse gerçek dünyadan çok sanal ortamda yaşıyor. Hatta Google'ın patronu Eric Schmidt ile yine Google'ın *Ideas* bölümünün kurucusu ve başkanı Jared Cohen tarafından da iddia edildiği gibi, tüm bu süreci gelecekte internet üzerinde kurulacak sanal devletler izleyecek. Doğal olarak son dönemlerde sanal ortamda yaşanan bu gelişmeler ekonomileri ve ekonomilerin ana ödeme aracı olan parayı ve geçerli para politikalarını da etkilemeye başladı. Ekonomi uzmanlarının açıklamalarına göre günümüzde sanal ortamdaki devletlere ait para miktarı, yine devletler tarafından basılan kâğıt para miktarının zaten kat kat üstüne çıkmış durumda. Bu gerçeklerden yola çıkarsak, tarihi kayıtlara göre ilk defa MS 806 yılında Çin'de ortaya çıkan kâğıt paranın da artık yavaş yavaş ömrünü doldurmaya başlaması ve bir zamanlar tahtını devraldığı madeni para, deri para, altın ve başka değerli madenler gibi, uzun vadede yerini Bitcoin türündeki sanal ödeme araçlarına bırakması artık kaçınılmaz görünüyor.

Kaynaklar
- Voss, O., "Internet Geld – Bitte ein Bitcoin", Wirtschaftswoche, s. 6-8, 13 Mayıs 2013.
- Kannenberg A., "Coins für alle Fälle-Wie sich die Kryptowährung Bitcoin langsam etabliert", *c't magazin für computer technik*, s. 78-81, 26 Ağustos 2013.
- Schmidt, E., ve Cohen J., *Die Vernetzung der Welt-Einblick in unsere Zukunft*, Rowohlt Verlag GmbH, 1. Basım, s. 150-153, Mayıs 2013.
- Oate,s J., "Mt. Gox bans anonymous currency deals", **coindesk.com**, 30 Mayıs 2013.
- Bernau, V., "Millionenschwere USB-Sticks in Schließfächern", **Süddeutsche.de**, 13 Nisan 2013.
- Reißmann, O., "Handelsplattform lahmgelegt: Angreifer pulverisiert Bitcoin Kurs", **spiegel.de**, 20 Haziran 2011.
- Knoke, F., "Hacker stehlen Bitcoins im Wert von 170.000 Euro", **spiegel.de**, 2 Mart 2012.
- Bitcoin Vakfı, "Bitcoin Hakkında", **bitcoin.org**, 3 Ekim 2013.
- Blockchain, "Bitcoin çizelgeleri ve döviz istatistikleri", **blockchain.info**, 5 Ekim 2013.