₿ITCOIN REHBERİ

KRİPTO PARALAR HAKKINDA
BİLMEK İSTEDİĞİNİZ HER ŞEY

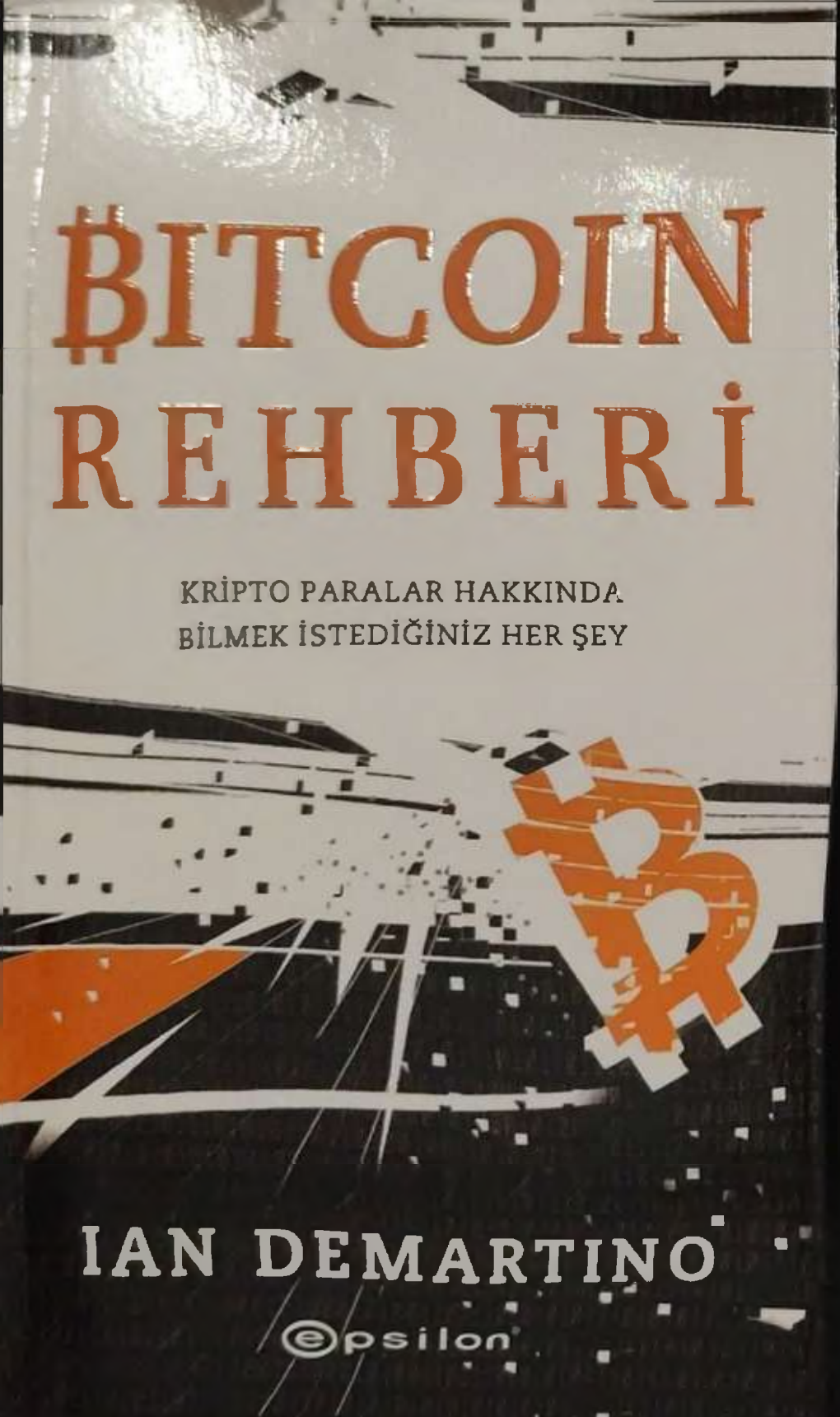


IAN DEMARTINO

Epsilon

BITCOIN REHBERİ

KRİPTO PARALAR HAKKINDA
BİLMEK İSTEDİĞİNİZ HER ŞEY



IAN DEMARTINO

Epsilon

İNTERNETİN İLETİŞİM VE MEDYA KONUSUNDAKİ AÇILIMININ AYNISINI, BITCOIN DE FİNANS DÜNYASINDA UYGULUYOR: ÜLKE SINIRLARINDAN ETKİLENİLMEDEN 'EŞLER ARASI' İŞ YAPILMASINI SAĞLIYOR VE BÖYLECE ÖNÜMÜZE YİNE BİR SÜRÜ YENİ OLASILIK SUNULUYOR. BITCOIN'İN ARDINDAKİ BLOKZİNCİRİ TEKNOLOJİSİYSE DÜNYAYI BİZİM HENÜZ HAYAL EDEMEDİĞİMİZ ŞEKİLDE DEĞİŞTİRECEK. PARA YALNIZCA BAŞLANGIÇ.

BITCOIN REHBERİ

Kripto Paralar Hakkında Bilmek İstediğiniz Her Şey

BITCOIN REHBERİ

Orijinal Adı: The Bitcoin Guidebook /How To Obtain, Invest and Spend The World's First Decentralized Cryptocurrency

Yazan: Ian DeMartino
Genel Yayın Yönetmeni: Meltem Erkmen
Çeviri: Kübra Tekneci
Editör: Mert Doğruer
Düzelti: Melis Özbakır
Kapak Uygulama: Dilara Kavaklıoğlu

1. Baskı: Nisan 2018

ISBN: 978-605-173-405-7

YAYINEVİ SERTİFİKA NO: 34590

© 2016 Ian DeMartino

Türkçe Yayım Hakkı: Anatolialit Ajans aracılığıyla
© Epsilon Yayınevi Ticaret ve Sanayi A.Ş.

Baskı ve Cilt: Mega Basım Yayın Sanayi ve Tic. A.Ş.
Cihangir mah. Güvercin cad. No: 3/1
Baha iş merkezi A Blok Kat: 2 34310
Haramidere/ İstanbul/TURKEY
Tel: 212 412 17 00
Sertifika No: 12026

Yayımlayan:
Epsilon Yayınevi Ticaret ve Sanayi A.Ş.
Osmanlı Sk. Osmanlı Iş Merkezi No: 18 / 4-5 Taksim/Istanbul
Tel: (0212) 252 38 21 Faks: 252 63 98
Internet adresi: www.epsilonyayinevi.com
e-mail: epsilon@epsilonyayinevi.com

BITCOIN REHBERİ

Kripto Paralar Hakkında Bilmek İstediğiniz Her Şey

Ian DeMartino

Çeviri
Kübra Tekneci

epsilon®

Beni her zaman destekleyen ebeveynlerim Jon ve Tamah'ya,
Bana nasıl çalışıp yaşayacağımı öğreten kız arkadaşım Laura'ya,
Bana tahammül ettikleri için editörlerim Jon, Erica,
Olga ve Joe'ya,
Dünyanın en iyi öğretmenleri olan internetteki bütün ezik ve zeki asosyallere,

Teşekkür ederim.

İÇİNDEKİLER

Önsöz 9
Anahtar Sözcükler 13
Kim Kimdir 21

BİRİNCİ KISIM
Bitcoin Nedir? 25

1. BÖLÜM
Bitcoin 101: Blok Zinciri Teknolojisi 27

2. BÖLÜM
Bitcoin Satın Almak, Biriktirmek ve Harcamak Üzerine Pratik Bir Rehber 42

3. BÖLÜM
Öncüler, Tarih ve Yaradılış Satoshi'nin Makalesi 49

4. BÖLÜM
Bitcoin'i Kim Yönetiyor? 67

5. BÖLÜM
Bitcoin'e Değerini Veren Ne? 83

6. BÖLÜM
Bitcoin: Anonim mi Yoksa Takma İsimli mi? 101

7. BÖLÜM
Bitcoin ve Suç Unsurları 121

8. BÖLÜM
Mt 60 x: Bitcoin'in Dönüm Noktası mı? 148

9. BÖLÜM
Diğer Bitcoin Hileleri ve Yaygın Taktikler 167

İKİNCİ KISIM
Bitcoin'le Yatırım Yapmak 197

10. BÖLÜM
Banka Hesabı, Nakit ve Paypal ile Bitcoin Satın Almak 199

11. BÖLÜM
Bitcoin İçin Çalışmak 212

12. BÖLÜM
Madencilik 221

13. BÖLÜM
Hodl! 237

14. BÖLÜM
Gün İçi İşlemler 244

15. BÖLÜM
Aitcoin Ticareti ve Şişirme Boşaltmalar 253

16 BÖLÜM
Eşler Arası Kredi Verme 262

17. BÖLÜM
Bitcoin Kullanarak Diğer Emtialara Yatırım Yapmak 269

ÜÇÜNCÜ KISIM
Bitcoin Benim İçin Ne Yapabilir? 281

18. BÖLÜM
Para Havalesi 283

19 BÖLÜM
Mikro İşlemler 298

20. BÖLÜM
Başlangıç Fonu 307

DÖRDÜNCÜ KISIM
Bitcoin'in Geleceği 315

21. BÖLÜM
Aitcoinler ve Bitcoin 2.0 Projeleri 317

22. BÖLÜM
Yaygın Otonom Şirketler Denetim ve Niş Pazarlar 351

Önsöz

Bu benim ilk kitabım, o nedenle bu işlerin nasıl yürüdüğü konusunda uzmanmışım gibi davranamam. Tek bildiğim, bir kitap yazmak için oturduğunuzda, dinleyici kitlenizi tanıdığınızdan emin olmanız gerektiğidir. Bu her konu hakkında ama özellikle de 80.000 kelime yazmak için oturduğunuzda geçerli. Hiç kimse bütün o çabaya bakıp kendi kendine, *Hepsi ne içindi?* diye sormak istemez.

O nedenle, bu kitabın kime hitap etmesi gerektiği üzerine bir süre düşündüm. Programcılara hitap etmeyeceğini en başından beri biliyordum; ben bir programcı değilim ve onlar Bitcoin'in 'kaportasının altında' ne olduğunu benden daha iyi anlıyorlar, bu yüzden onlarla konuşmaya çalışmamın hiç anlamı yok. Andreas M. Antonopoulos'un yazdığı *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* programcılar için daha iyi bir kitap. Hedefimde yatırımcıların da olmayacağını biliyordum. Kripto paralarla gün içi ciddi işlem yapacak kadar harcanabilir gelirim hiçbir zaman olmadı. Bu alanda benden daha tecrübeli olan eski

Wall Street yatırımcılarının ve mevcut Bitcoin ile günlük işlem yapan kişilerin yazdığı onlarca e-kitap var.

Profesyonel olarak Bitcoin hakkında yazmaya başlamadan önce, 2012'de Bitcoin'le ilgili bir kitap alsaydım okumak isteyebileceğim türden bir kitap yazmaya karar verdim.

O zamanlar, bana merak ettiklerimi anlayabileceğim terimlerle açıklayan ama muhtemel sonuçlar hakkında da benden hiçbir şey gizlemeyen bir kitap istiyordum. Kripto paraların hem iyi hem de kötü yanları hakkında bilgi sahibi olmayı istiyordum. Bana öyle geliyor ki, Bitcoin taraftarları topluluğun negatif yönlerini genellikle geçiştiriyorlar ve bu kitapta bütün foyaları ortaya çıkarmayı amaçladım.

Bir kitap vardı, *BitCon: The Naked Truth About Bitcoin* (Bit-Üçkâğıt: Bitcoin Hakkındaki Çıplak Gerçekler) ama oldukça kısaydı ve dürüst bir bakış açısı sunmak yerine ideolojik bir noktaya parmak basmaya kararlı gibiydi. Foyalarla doluydu, hepsi bu.

Bu kitap Bitcoin'in yaptığı kötü şeylerden ve karşı karşıya olduğu tehlikelerden uzak durmuyor, ama mecazi ufukta beliren ışığı, umutlanmak için verdiği sebepleri de göz ardı etmiyor.

Bu kitabı bitirdiğinizde, siz, okuyucuların Bitcoin'in tüm detayları –geçmişinden günümüze ve potansiyel geleceği– hakkında herhangi biriyle sohbet edebilmenizi istiyorum. Bu kitabı okuduktan sonra bir sonraki muhteşem Bitcoin hizmetini programlamayacaksınız, ama bir dahaki sefere bir akşam yemeğinde birinin Bitcoin'den bahsettiğini duyduğunuzda, sohbete ayak uydurabileceğinizi garanti ediyorum.

Bu kitap Bitcoin'in yönleri konusunda uzmanlaşmanızı sağlamayacak. Daha ziyade, Bitcoin'de 'ticaret konusunda yetenekli' ya da 'ortanın üstü düzeyde bir öğrenci' olmanız için tasarlandı. Onun doğasını ve onu nasıl kullanacağınızı anlayacaksınız, nereden geldiğini bileceksiniz ve nereye doğru gittiğine dair bir fikriniz olacak.

Bu kitap elinize nasıl geçmiş olursa olsun, vaktinizi ayırıp okuduğunuz için teşekkür ederim. Umarım bir şekilde faydalı bulursunuz. Yazara bağışta bulunmak isterseniz, aşağıdaki kare kodla yapabilirsiniz:

Bitcoin Adresi: 3Bi1fhng5LfoDzue5MTfGw9PgHNKKgRkVt



Uyarı: Bu kitabın mümkün olduğunca doğru olması için uğraşmış olsam da, kripto paralar karmaşık ve sürekli gelişen bir konu. O yüzden baştan söylemek en iyisi:

Kendi araştırmanızı yapın. İşler bir aydan diğerine, hatta bir haftadan diğerine değişebilir. Ayrıca, bu kitapta geçen şirketlerin meşruluğu hakkında hiçbir iddiada bulunmuyorum, çünkü statüleri her an değişebilir.

ANAHTAR SÖZCÜKLER

%51 saldırısı: Bitcoin'de blokzincirini doğrulamak için çalışma ispatı (PoW) kullanılır. İşlemleri doğrulamak ve onaylamak bilgisayımsal güç gerektirir. Bir işlemi değiştirmek onu izleyen bütün işlemlerdeki doğrulanabilir veriyi de değiştirir. Bu nedenle, eğer farklı işlem geçmişleri olan iki rakip blokzinciri varsa, uzun olan 'gerçek' blokzinciri olarak kabul edilir, çünkü ardında daha fazla bilgisayımsal güç vardır. Kötü niyetli oyuncular genellikle tek başlarına çalıştıkları için herhangi bir grubun gerçek blokzincirine kıyasla değiştirilmiş blokzincirinin ardına daha fazla bilgisayımsal güç koyması olası değildir. Ancak, biri gerçek blokzincir üzerinde çalışan bütün madencilerin kombine hash oranından daha yüksek bir hash oranını kontrol ederse, o grup geçerli zincirden üstün gelip kendi blokzincirini geçerli olarak onaylayabilir. Buna %51 saldırısı denir.

açık anahtarlı şifreleme: açıkça belirlenebilen bir anahtar kullanarak bilginin açığa vurulmadan bir dış kul-

lanıcı tarafından doğrulandığı bir yöntem. Bu anahtar, onunla ilişkili özel anahtarı elinde bulunduran birinden gelen mesajı özel anahtarın ayrıntılarını açığa çıkarmadan doğrulamak için kullanılabilir.

açık kaynak: açık olan ve halk tarafından değiştirilebilen herhangi bir kod.

ağ cüzdanı: Başka bir şirketin sunuculuğunu yaptığı bir web sitesinde kontrol edilen ve tutulan bir cüzdan. Sunuculuğunu yapan şirket kadar güvenli ve güvenilirdir. Genellikle, sadece para harcamaya uygundur ama bazı servisler ekstra güvenlik sağlamalarıyla ve kısa-orta vadeli saklamaya uygun çevrimdışı anahtar üreten multisig teknolojisine sahip olmakla övünüyorlar.

altcoin: 'alternatif kripto para'nın kısaltması; Bitcoin benzeri başka bir kripto para. Şu anda binin üstünde altcoin mevcut; çoğu da kendilerinden daha başarılı kripto paraların neredeyse bire bir kopyası. Bununla birlikte, hayli yenilikçi versiyonlar da üretiliyor.

ASIC: Uygulamaya özgül tüm devre. Tek bir şey yapmak için tasarlanmış bir donanım parçası. Kripto para dünyasında, belirli bir algoritmayı araştırıp bulur (SHA256, Scrypt, vb.).

baş geliştirici: Hangi geliştiricilerin git commit erişimi olduğuna karar veren geliştirici.

BFGMiner: İkinci en popüler Bitcoin madencilik yazılımı.

Bitcoin XT: İlk olarak Gavin Andresen ve Mike Hearn tarafından ortaya çıkarılan Bitcoin'in mevcut ana uygulamasıyla uyumlu Bitcoin kodunun alternatif bir uygulaması. Yeni özellikleri test etmek için kullanılıyor ve blok

boyutu tartışmasındaki farklı gruplar uzlaşmaya varamazlarsa, Bitcoin-Qt'nin yerini alabilecek gözüyle bakılıyor. Ana özellik olarak 20MB boyutunda bloklar sundu.

Bitcoin/bitcoin: Büyük B ile yazılan Bitcoin, Bitcoin sistemini, ağını ya da para birimini ifade eder; küçük b ile yazılan bitcoin bireysel bitcoin'leri ifade eder, "Beş bitcoin'im var," gibi.

Bitcoin-Qt: Bitcoin Core (Bitcoin Çekirdeği) olarak da ifade edilir, Bitcoin, diğer bütün cüzdanlar ve hizmetlerin bağlı olduğu ana uygulamadır.

blok gezgini: Kullanıcıların blokzinciri aracılığıyla Bitcoin işlemlerini gözlemlemeleri ve takip etmelerine imkân tanıyan bir web sitesi ya da yazılım. Altcoin'lerin blokzincirleri için kurulmuş benzer sistemlerin tanımlanması için de kullanılabilir.

blok: Blokzincirindeki işlemler yaklaşık olarak her on dakikada bir madenciler tarafından doğrulanan bloklar halinde gruplanırlar. Şu an 1MB boyutuyla sınırlılar ama bunun yakın gelecekte değişmesi olası.

blokzinciri: Bitcoin'in çalışmasını sağlayan merkezsizleşmiş hesap defteri. Bütün işlemlerin ve hesapların kaydı burada tutulur. Web sitesi blockchain.info ya da ana kuruluşu Blockchain ile karıştırılmaması gerekir. Ayrıca, dijital değerin kaydını tutmak için umumi bir hesap defteri kullanan her yeni teknoloji de ifade eder. Örneğin, "Kendi blokzinciri teknolojilerini geliştiriyorlar."

CGMiner: En popüler Bitcoin madenciliği yazılımı.

cüzdan: İşlemleri gerçekleştirmek için Bitcoin adresinizi kullanarak Bitcoin ağıyla iletişim kuran yazılıma verilen genel isim.

çatallanma: Açık kaynak kodu kopyalayıp üzerinde değişiklikler yapmak. Kripto para birimleri bağlamında, aynı zamanda madencilerin yanlışlıkla ya da kötü niyetle bir sahte blokzincirini kazmaya başlamaları anlamına gelir.

çekirdek geliştirici: Sitenin GitHub sayfasındaki git komutlarına erişimi olan kripto para geliştiricisi.

Derin Ağ: Banka bilgilerinden yasadışı uyuşturucu pazarlarına kadar sıradan ağ tarayıcılar tarafından görülmeyen internetteki bütün bilgiler.

e-nakit/e-para: Resmi para birimlerinden ayrı, her türlü dijital para; genellikle, Bitcoin öncesi dijital para birimlerinden bahsedilirken kullanılır.

full node: Bütün blokzincirini saklayan, madencilerin onayladığı işlemleri doğrulamaya ve yaymaya yardım eden yerel bir Bitcoin cüzdanı. Madencilerin aksine, full node'ların belli bir amaç için üretilmiş donanıma gereksinimleri yoktur, ayrıca ödül de almazlar.

git commit: GitHub sitesindeki açık kaynak kodu üzerinde olası bir değişiklik.

GitHub: Kod üzerinde ortak çalışmak için açık kaynak koduna sunuculuk yapan bir web sitesi.

GUIMiner: Grafiksel kullanıcı arayüzü olan en popüler Bitcoin-madencilik yazılımı.

hash gücü: Hash oranı demenin bir başka yolu.

hash oranı: Bir ağa aktarılan toplam hash sayısı. Toplam hash sayısı Bitcoin (ya da diğer kripto para) ağında gerçekleşen bilgisayımsal denkliklerin sayısına eşittir. 1/THs hash oranı, ağın saniyede bir trilyon hesaplama yapabildiği anlamına gelir.

hash: Bir ağa ne kadar bilgisayımsal gücün aktarıldığını ölçen bir ölçü birimi.

kâğıt cüzdan: Basılabilen ya da bir kâğıt parçasına yazılabilen özel ya da kamusal anahtarınız.

Karanlık Ağ: Derin Ağ'ın belirli hizmetler vermesi amacıyla kurulan bölümü. Uyuşturucu aktiviteleri de buna dahildir, ama karanlık ağ bununla sınırlı değildir, gazetecilerin kaynaklarla anonim ve güvenli bir şekilde buluşabildikleri, anonim tanışma grupları ve anonimliğin korunmasını gerektiren diğer aktivitelerin de gerçekleştiği yerdir.

kripto para: Sistemini ya da kullanıcılarının kimliklerini ve hesap bilgilerini güvenceye almak için kriptografi kullanan her dijital para birimi.

madenci: Bitcoin ağını güvenli kılan karmaşık matematiksel hesaplamalar yaparken, aynı zamanda kriptografi aracılığıyla bütün işlemleri onaylayan Bitcoin ağının bir katılımcısı. İşi yapan bilgisayar donanımını ya da donanımın sahibi olan kişileri, şirketleri ifade edebilir.

madencilik öncesi: altcoin'lerin bazıları ilk yaratıldıklarında, yaratıcılar bazen ağ çalıştırılmadan önce birkaç para üretirler ve insanlar onları adil bir şekilde çıkarırlardı. Genel olarak dolandırıcılığa işaret eder ama eğer az sayıda paradan söz ediliyorsa dürüst bir para programının bir parçası olabilir ve şeffaf bir şekilde ya da paranın türü gerektirdiği için yapılır.

madencilik: Karmaşık matematiksel hesaplamaları çözüp işlemleri ağın geri kalanına gönderen bloklar adı verilen gruplardaki Bitcoin işlemlerini doğrulama süreci. Bunu yaptıkları için madenciler küçük bir miktar Bitcoin ile ödüllendirilirler ve yeni bitcoin'ler bu şekilde üretilir. Madenciler aynı zamanda her işleme bağlı olan küçük üc-

retleri de alırlar ve 2140 yılında olması öngörülen, 21 milyon bitcoin çıkarıldığında bununla geçinmek zorunda kalacaklar. Madenciler birbirleriyle sürekli yarış halindedir.

merkezsizleşme: Merkezi bir kırılma noktası olmaksızın, bir ağ, hizmet ya da şirket sahipliğinin geniş bir grup insan arasında dağıtılma fikri. Örn.: "İnternet küresel ve merkezsiz bir iletişim ağıdır."

Mt. Gox: Aslen 'Magic: The Gathering' kartları satması planlanan ama en sonunda ilk merkezi serbest piyasayı oluşturarak ilk ve en büyük Bitcoin borsası haline gelen internet sitesidir. Çok sayıda güvenlik sorunu ve dolandırıcılık suçlamalarından sonra, 2014'ün başında çökerek, o sırada tarihi zirvesinde olan Bitcoin'in fiyatını düşürdü. Bitcoin'in fiyatı hâlâ tam olarak toparlanamadı.

musluk: Reklam izlemek gibi küçük işleri yerine getiren kullanıcılara düşük miktarda Bitcoin'i ücretsiz veren internet hizmetleri. Bitcoin pahalı değilken, tam bitcoin'ler veriyorlardı. Günümüzde, daha önceki tam bitcoin'lerde olduğu gibi, bir sentin çok az bir bölümüne karşılık gelen küçük miktarlarını veriyorlar.

node runner: Bitcoin ağında bütün blokzinciri indiren ve madencinin işini çifte kontrol eden ama madencilik yarışına girmeyen, ödül almayan ama yine de Bitcoin ağını güvenceye almanın önemli bir parçası olan bir katılımcı. Blokzincirlerin boyutu arttıkça ve daha az kişi bütün bloğu indirmek istedikçe, node runner'lar için teşvik edici şeylerin geliştirilmesi düşünüldü.

proof of burn (PoB): Blokzincir kullanarak Bitcoin ya da başka bir kripto paranın harcanamaz bir adrese gönderildiğini ve etkili bir şekilde sistemden çıktığını kanıtlamaktır.

proof of stake (PoS): Bilgisayımsal güçten ziyade para stoklarına bağlı olarak bir paranın oylarını tartan blokzincirini güvenceye alan bir tür kriptografik kanıt.

proof of work (PoW): Bilgisayımsal güce bağlı olarak oyları ölçen blokzincirini güvenceye alan bir tür kriptografik kanıt.

Scrypt: Litecoin ve diğer birçok alternatif kripto para biriminin ağlarını güvenceye almak için kullandıkları bilgisayar algoritması. ASIClere karşı daha dirençli olması için tasarlandı.

SHA256: Bitcoin ve diğer birçok kripto para biriminin ağlarını güvenceye almak için kullandıkları bilgisayar algoritması.

sıcak cüzdan: İnternete bağlı, çevrimiçi bir cüzdan. Bilgisayar ya da cüzdan şifresi güvenli değilse, bitcoin'ler çalınma riskiyle karşı karşıyadır. Para harcamaya ve kısa süreli saklamaya uygundur. Bütün ağ cüzdanları sıcak cüzdanlardır.

soğuk depo cüzdanı: İnternete bağlı olmayan bir bilgisayar ya da disk bellekteki cüzdan, işlem gerçekleştirmek için geçici olarak internete bağlanıp sıcak cüzdana dönüştürülmelidir. Daha sonra tekrar soğuk cüzdana dönüştürülebilir.

X11: Dash ve diğer birkaç para birimi tarafından kullanılan algoritma. 11 farklı algoritmadan faydalanır, ve ismi buradan gelir.

yan zincir: Bitcoin ölçeklendirmek için olası bir çözüm. Çok sayıda işlemin kaydını tutan blokzincirine benzer hesap defterleri sıkıştırılmış formatta son blokzincire eklenecek.

yerel cüzdan: Bilgisayarınızda bulunan sıcak cüzdan ya da soğuk depo cüzdanı.

yumuşak çatallanma: Güvenlik ya da başka bir sebepten ötürü cüzdan yazılımının güncellenmesi 'gerekliliğinden', eski yazılımla alım-satım yapmayı ve işlemleri doğrulamayı sağlayacak ve yanlışlıkla alternatif bir blokzincirini doğrulamaya başlamasını önleyecek olan kripto paranın kodu üzerinde önemli bir değişiklik.

zorunlu çatallanma: Katılımcıların güncellenmiş istemcilerle çalışabilmeleri için yazılımlarını güncellemelerini gerektiren kripto para kodundaki değişiklik. Kullanıcıların çoğu güncelleme yapmazlarsa, eski yazılım kendi blokzincirinde madencilik yapmaya devam eder; sonuç olarak daha yüksek bir hash oranı olan daha uzun bir blokzinciri ortaya çıkacağı için paranın ağı ikiye bölünür, ki bu potansiyel bir felaket demektir. Ancak, başarılı sert çatallar kripto paranın kodu üzerinde önemli değişiklikler yapmanın genellikle tek yoludur.

KİM KİMDİR

Gavin Andressen: Satoshi Nakamoto'nun Bitcoin'in güvenlik anahtarlarını teslim ettiği çekirdek geliştirici.

Andreas Antonopoulos: Yazar, Bitcoin savunucusu ve güvenlik uzmanı.

Bitcoin Vakfı: Bir zamanlar çekirdek geliştiriciler için ana fon sağlayıcı olan bir ticaret organizasyonu.

Dijital Ticaret Odası: Bitcoin yanlısı bir lobicilik grubu.

Hal Finney: PGP'yi yaratmaya yardım eden ilk kriptograf. İlk Bitcoin destekçilerinden biri, ilk Bitcoin transferi ona yapıldı.

Mike Hearn: Bitcoin geliştiricisi ve Google çalışanı; Lighthouse'u yarattı ve Bitcoin XT'yi savunuyor.

Olivier Janssens: Bitcoin'i ilk benimseyenlerden, zamanla melek yatırımcı olmuştur. Bitcoin'in çekirdek koduna kitle kaynak güncellemeler yapması için tasarlanan bir program olan Lighthouse'un yaratılışına kaynak sağladı, ama şimdiye kadar çoğunlukla ilgisiz projelere kitlesel fon sağlamak için kullanıldı.

Mark Karpelès: Borsa çöktüğünde Mt. Gox'un yönetim kurulu başkanı ve sahibiydi.

Wladimir van der Laan: Bitcoin'in mevcut baş geliştiricisi.

Jed McCaleb: Mt. Gox'un kurucusu ve eski sahibi, Ripple'ın ve Stellar'ın kurucu ortağı.

Satoshi Nakamoto: Bitcoin'in anonim yaratıcısı, bir kişi ya da birden fazla kişi olmasından şüpheleniliyor.

Dread Pirate Roberts: Kötü şöhretli Silk Road (İpek Yolu) yer altı borsasının lideri. Bir grup insan ya da bir kişiden diğerine geçen bir isim olabilir.

Amir Taaki: Dark Wallet'ın kurucu ortağı ve daha sonra Açık Pazar'a dönüşen karaborsanın baş geliştiricisi.

Peter Todd: Bitcoin çekirdek geliştiricisi.

Ross Ulbricht: Dread Pirate Roberts olmakla suçlanıp mahkûm edildi; davası temyizde.

Roger Ver: Melek yatırımcı ve Bitcoin savunucusu; Bitcoin'i kabul eden ilk sitelerden biri olan Memorydealers.com'un yönetim kurulu başkanı ve Blockchain şirketinin kurucusu.

Cody Wilson: Dark Wallet'ın kurucu ortağı ve üç boyutlu yazıcılarla üretilebilen bir silahın tasarımcısı.

Craig Wright: Satoshi Nakamoto arayışına yeni eklenen bir isim. *Wired* dergisi kısa bir süre önce onun 'muhtemelen' Bitcoin'in yaratıcısı olduğunu (ya da dünyanın öyle sanmasını istediğini) belirtti. Mayıs 2016'da, Satoshi Nakamoto'yla ilişkilendirilmiş bir hesabı kullanarak bir mesaj imzalayıp Bitcoin'i yarattığını kanıtlamaya çalıştı. O noktada, Gavin Andresen de dahil olmak üzere birçok kişi ikna olmuştu. Ancak, topluluğun büyük bir bölümü şüpheci kaldı. Daha fazla kanıt sunacağına söz verdikten sonra, Wright sözünü tutmadı. Bu gelişmeler çok kısa süre önce yaşandığı için onları bu kitapta doğru düzgün bir şekilde ele almak mümkün değil.

BİRİNCİ KISIM:
Bitcoin Nedir?

Birinci Bölüm:

Bitcoin 101: Blokzinciri Teknolojisi

Hepimiz bunu, bu Siber İsa anını bekliyorduk. Artık FED'e karşı koymaya çalışan aktivistler kazanacaklar.

— Max Keiser, gazeteci, *Russia Today*

"Bitcoin nedir?" sorusuna birbirleriyle bağlantılı olsa da farklı iki yaklaşım var: Birincisi, Bitcoin'in gerçekte ne olduğu ve ikincisi, Bitcoin'in neler yapabileceği. Ayrıca, insanlar bunu sorduklarında kastettikleri şey genellikle "Bitcoin nasıl çalışıyor?" oluyor. Bu kitapta bu üç soruyu yanıtlamaya çalışacağım.

Basitçe açıklamak gerekirse: Bitcoin yeni bir para birimi –aşina olduğumuz avro ya da dolar gibi– ve nakit paranın dijital karşılığı. Herhangi biri dünyanın farklı bir noktasında ya da aynı odada bulunan başka birine bir bitcoin, birden çok bitcoin ya da bitcoin'in çok küçük bir bölümünü dijital olarak 'aktarabilir.' Bu, birine nakit para vermek gibidir; eski dijital finans sistemlerinin aksine, para bir ban-

ka ya da başka bir şirket gibi aracı bir kurumdan geçmek zorunda değildir. Bitcoin'i değerli kılan şey, daha sonra değineceğim üzere, Bitcoin kullanmanın avantajlarıdır.

Bitcoin aynı zamanda bir hesap defteri, şöyle ki, her işlemin ve her Bitcoin cüzdanının bakiyesinin kaydı tutulan bir sistem (cüzdanı şimdilik bir hesap gibi düşünebilirsiniz). Bu hesap defterine aynı zamanda blokzinciri adı veriliyor. Bir bankanın veritabanında tutulması yerine, her cüzdan bu hesap defterinde bulunuyor; her cüzdanın bir özel anahtarı ve bir ortak anahtarı var. Ortak anahtara aynı zamanda Bitcoin adresi deniyor. 25 ila 36 alfanumerik karakterden oluşan bu adres, 1 ya da 3 ile başlıyor. Bu adres herkese gösterilebilir ve herhangi birinin size bitcoin göndermesine imkân tanır. Bir elektronik posta adresi gibi, Bitcoin cüzdanları anında yaratılabilir ve aynı şekilde ortadan kaldırılabilir.

Özel anahtar, 5JJqKVLu29gfafXvCjva9zBtVapjrE8qNerXWt9RTAv4ebbDX4E gibi bir şeye benzer ve her ne pahasına olursa olsun korunmalıdır. "Hukukun onda dokuzu mülkiyettir," denir. Bitcoin'de bütün hukuk özel anahtardır. Özel anahtarı elinde bulunduran kişi başka bir cüzdana dilediği gibi bitcoin gönderebilir. Bir Bitcoin transferini geri çevirmek mümkün değildir, o nedenle, özel anahtarı güvenli bir şekilde saklamak Bitcoin ilkelerinin en önemlisidir. Bu noktada aklınız biraz karışmış olabilir; fiziksel bir varlığı olmayan yeni bir para birimi yaratmanızın gerektiği varsayımsal bir durumda, bunu anlamanız daha kolay olabilir.

19 kişiyle birlikte ıssız bir adada mahsur kaldığınızı düşünün. Hayatta kalmanıza yetecek kadar yiyecek ve temiz su var ama kurtarılmak ya da kaçmak söz konusu değil.

Hayatta kalmak için hepiniz birlikte çalışmalısınız. Güçlerinizi adil bir şekilde dağıtmak için kimin kim için ve ne kadar süreyle çalıştığını takip etmek isteyebilirsiniz. Durum böyle olsaydı, bir tür parasal sistem yaratmanız gerekirdi. Deniz kabukları, parlak taşlar ya da benzer şekilde nadir bulunan bir şey kullanabilirsiniz ama hiç şüphesiz biri sistemi kandırma becerisine sahip olacaktır. İki deniz kabuğu bulana kadar kumsalda yürüyebilecekken, neden iki deniz kabuğu karşılığında arkadaşınıza bir kulübe inşa etmesinde yardım edesiniz? İnsanların rahatlıkla çalışıyormuş gibi yapabilecekleri bir ortamda, saatlerce çalışmanın karşılığında dürüstçe para kazanmalarını sağlayan bir sistemi nasıl kuracaksınız?

Bir hesap defteri ya da liste oluşturmak çözüm olabilir. Bu hesap defterinde kimin ne kadar çalıştığının kaydı tutulabilir ve bu 'çalışma birimi' olarak ölçülebilir. Hesap defteri her kişinin ne kadar parası olduğunu kayıt altına alır ve bir diğer katılımcının hesabına para aktarmasına olanak sağlar. Eğer hesap defteri herkesin birim stokunu ve gerçekleşen her takası takip ederse, hiç kimse sistemin dışından deniz kabuğu, parlak taşlar ya da başka 'çalışma birimleri' ekleyerek bakiyesini şişiremez. Hesap defteri çözümünün yarattığı sorun, bütün katılımcıları hesap defterine sahip kişinin dürüst oynayacağına güvenmek zorunda bırakmasıdır. Eğer hesap defteri bir kişi ya da grubun elindeyse, sonuçta herkesin ne kadar parası olduğunu onlar kontrol ederler ve bu en iyi niyetli insanlar için bile baştan çıkarıcı bir konumdur.

Bu sorunun çözümü merkezsizleştirmedir. Gruptaki güvenilen iki kişiye hesap defterinin iki kopyasını verebilirsiniz. Böylece her bir defteri çapraz kontrolden geçirip

kayıtların birbirine uyduğundan emin olabilirler. Yine de, katılımcıların bu kez bir yerine iki kişiye güvenmesi beklenmektedir. Bütün gücü hesap defterini elinde bulunduran tek kişiye vermekten daha iyi olsa da, yine de ideal bir düzenleme değildir.

En iyi çözüm hesap defterinin 20 kopyasını çıkarıp onları adadaki herkese dağıtmaktır. Günün sonunda, herkes başkalarının arasında gerçekleşen alım-satımları çapraz kontrol edebilir ve merkez otorite olmadan bir mutabakat sağlanır. Eninde sonunda, adada sağ kalanlar deniz kabuklarına gerek olmadığını, önemli olan tek şeyin hesap defteri olduğunu fark edebilirler. Adadaki bütün deniz kabukları toplatılsa bile önemi olmaz; hesap defteri kimin ne kadar deniz kabuğu olduğunu ve kiminle neyi takas ettiğini hatırlar. Hatta deniz kabuklarının ticarete ayak bağı olduğu bile iddia edilebilir; ne de olsa onları toplamak, güvenli bir yerde saklamak ve hangilerinin meşru olduğunun kaydını tutmak için harcanan vakit ve enerji başka bir şekilde değerlendirilebilir. Eğer bir hesap defteri bunu zaten yapıyorsa, deniz kabukları konu dışı olurlar. Asıl para birimi hesap defterindeki 'çalışma birimi'dir. Deniz kabukları ya da diğer fiziksel nesneler işin kaydını tutmayı sağlayan şeylerdir ama asıl para birimi işin kendisidir.

Bitcoin'i para birimi ve blokzincirini hesap defteri olarak düşünebilirsiniz. İnternetin mümkün kıldığı neredeyse anlık iletişim bu kapıyı açtı, ama Satoshi Nakamoto olarak bilinen anonim bir kişi herkesin inceleyebileceği bir hesap defteri oluşturdu. Bitcoin'e tam katılım gösteren herkeste hesap defterinin bir kopyası var; herkes diğer hesap defterlerine karşı kendi kopyasını kontrol edebilir ve

doğruluğundan emin olabilir. Bu doğruluğun nasıl onaylandığını açıklamak bundan biraz daha karışık, ama temel prensip bu.

Örneğimiz ve Bitcoin arasındaki bariz farklılık Bitcoin'in küresel ölçekte işlemesi ve adanın 20 kişiyle sınırlı olması; Bitcoin ancak bilgisayarlar ve internet aracılığıyla mümkün olabilir. Ayrıca, internette fiziksel bir alan yoktur; bir fiber optik kablo aracılığıyla deniz kabukları gönderemezsiniz. Bu nedenle, dijital bir para birimi fiziksel olamaz.

Pratik bir dijital para birimi yaratmanın asıl zorluğu bu; gerçekte, en azından varlığını düşünmeye alışık olduğumuz şekilde bir varlık sürdürmüyor. Varoluş konsepti geçmişte daha kolay tanımlanabiliyordu. Bir şey ya vardı ya yoktu. Elinizle tutabilirdiniz ya da tutamazdınız. Ama sanal dünyanın yaratılışıyla, varoluşu ne tanımlıyor? Bir kitap kâğıda basıldığında daha mı gerçek oluyor? Varlığı aynı kitabın elektronik halinden daha mı geçerli? Fiziksel dünyada daha somut bir şekilde 'var olduğu' kesin ama çok az kişi kitabın fiziksel varlığının elektronik varlığından daha geçerli olduğunu iddia edebilir. Sonuçta, ikisi de aynı hikâyeyi anlatıyor.

Bir bakıma, para kendi hikâyesini, yani çalışmanın hikâyesini temsil ediyor. Ama para bu hikâyeyi anlatması için bir kâğıt parçasına basılmıyor. Bir parça kâğıda basılıyor, bir parça metale işleniyor ya da kolaylık olması için bir bilgisayar sunucusunda saklanıyor. Amerikan dolarından avroya, yuana kadar, paranın büyük bir bölümü elektronik ortamda bulunuyor. Hiç kimse banka hesabında milyonlarca doları olan ama üzerinde çok fazla nakit parası

olmayan birinin fakir olduğunu söyleyemez. Eğer fiziksel paranın elektronik temsili fiziksel para kadar geçerliyse, o halde sadece elektronik olarak temsil edilen bir para birimi bu denkleme nasıl sığar? Ayrıca, geleneksel paranın dijital temsillerine zaten sahip olduğumuza göre, Bitcoin gibi sadece dijital bir para birimine ihtiyacımız var mı?

İnternet üzerinden alışveriş yeni bir alışkanlık. 2012 yılında e-ticarette 289 milyar dolar harcanmışken[1] 1990'ların başında internetten herhangi bir şey satın almak birçok tüketici için düşünülemez bir şeydi.

Çevrimiçi ticaretin doğumu, ilk 'güvenli' alışverişin – Netmarket web sitesinden satın alınan 12,48 dolarlık Sting albümü *Ten Summoner's Tales*– yapıldığı 1994 yılına uzanıyor.[2] CD'yi satın almak için kullanılan kredi kartı numarası şifrelenmişti; tüketici toplumu yavaşça internetin geçerli bir pazar olduğunu anlamaya başladı. Bir sonraki sene, Amazon ve eBay kuruldu, gerisini anlatmaya da gerek yok.

Yine de, insanlar bu olayların herhangi biri gerçekleşmeden çok önce internet ekonomisinin lojistiği hakkında teoriler üretiyorlardı. Bu soruların Nikola Tesla'nın küresel kablosuz 'merkezi sinir merkezleri' irdelemesine uzanabileceği iddia edilse de, asıl övgüyü Marshall McLuhan hak ediyor. 1964'te yayınlanan kitabı *Medyayı Anlamak*'ta, McLuhan internete ve hatta sanal gerçekliğe şaşırtıcı derecede benzeyen, birbirine bağlı ve birbirini etkileyen bir medya biçimini tarif ediyor. Daha önce, *Gutenberg Galak-*

[1]"Statistics and Facts about Online Shopping." Statista. June 2014. Erişim Tarihi 19 Mayıs 2015. http://www.statista.com/topics/2477/online-shopping-behavior/

[2]Lewis, Peter H. "Attention Shoppers: Internet Is Open." Editorial. *The New York Times*. August 12, 1994: n. pag. Erişim tarihi 19 Mayıs, 2015. http://www.nytimes.com/1994/08/12/business/attention-shoppers-internet-is-open.html.

sisi'nde, günümüzde hâlâ interneti tarif etmekte kullanılan 'küresel köy' terimini uydurdu. McLuhan aynı zamanda, toplumda bilginin iletilme şeklinin bilginin kendisinden daha güçlü bir etkisi olduğu anlamına gelen, "Araç mesajdır," ifadesini ortaya attı. Bu konseptler kültürün elektronik olarak bağlı bir toplumda nasıl işleyeceği sorusuyla çatışmaya başladı ama McLuhan öncelikli olarak ekonomiyle değil, iletişim ve medyayla ilgileniyordu. Ona daha sonra sıra gelecekti.

Yaşlı okuyucular 1970'lerin sonunda evden alışveriş yapmayı mümkün kılan alışveriş ağlarını hatırlayabilirler. Kullanıcılar ilk ev bilgisayarlarında elektronik mönüleri doldurup onları telefon aracılığıyla diledikleri eczaneye ya da marketlere iletirlerdi.

O günler için kötü bir fikir olmasa da, internet büyüdükçe bu ilk ağlar işe yaramaz oldu. Yine de, bu örnek bilgisayarınız aracılığıyla bir şeyler sipariş etme fikrinin 1994'te bile yeni olmadığını gösteriyor. Sadece, bunu güvenli ve kullanışlı bir şekilde yapmanın yolunu henüz hiç kimse bulmamıştı.

Netmarket o ilk satışı yaptığında, bu olayı takip eden herkes yeni bir çağın başlangıcına tanıklık ettiğini biliyordu. Mesele birinin internet üzerinden bir şey satın almış olması değildi. Alıcının kredi kartı bilgilerinin güvenli olduğundan emin olduğu ilk satış olduğu gerçeğiydi. Netmarket'ten önce, internetten bir şey satın alan insanlar öteki uçtaki kişinin bu bilgiyi çalmayacağına güvenmek zorundaydılar.

Netmarket'le birlikte, müşterilerin o zaman bile efsane olan PGP programını temel alan özel yazılımı indirmeleri

gerekiyordu. 'Pretty Good Privacy'nin (Oldukça Sağlam Gizlilik) kısaltması olan PGP, internet üzerinde şifreleme kullanarak iki taraf arasında gizli ve güvenli iletişimi sağlayan bir teknolojidir. Kriptografi için çok büyük bir adımdı, şifreleme algoritmaları onlarca yıl boyunca endüstrinin temeli olarak hizmet etti; onu baz alan açık kaynak yazılımlar günümüzde hâlâ kullanılıyorlar.

Netmarket alışverişinden sonra internet üzerinden bir şeyler satın almak kolaylaştı ama her zaman aynı güvenlik seviyesine sahip olmadı. Anlaşılan, bir kredi kartının bilgilerini şifrelemek, internet üzerindeki en güvenli alışveriş yöntemi değilmiş. İlk e-ticaret dönemi, sahtekârlıklar ve kredi kartı dolandırıcılıklarıyla doluydu. 1999'da yanlışlıkla yaklaşık bir milyon siparişin bilgilerini sızdırdığında Netmarket de bu anlaşmazlığın içine girdi.[3]

Kişisel bilgi sızıntıları günümüzde de devam ediyor. Bu korku, gelecekçileri ve geliştiricileri o satıştan ve PayPal gibi hizmetlerden önce, internetin kendi para birimine ihtiyacı olup olmadığını merak etmeye zorladı.

Bu, kulağa geldiği kadar çılgınca bir fikir değil. Geçmişte, para birimleri belirli ülkeler ve bölgelerle sınırlıydı. Bu düzenleme yüzyıllar boyunca sorunsuz bir şekilde işledi, çünkü dünyanın bir tarafındaki yerel para birimine sahip bir kişinin, dünyanın öteki tarafında farklı bir para birimine sahip başka biriyle işlem yapma ihtimali oldukça düşüktü. Ancak, internetin gelişmesi, insanların sadece siyasi sınırları değil, coğrafi sınırları da aşmalarına imkân tanıdı.

---

[3]Wolverton, Troy. "Netmarket Exposes Customer Order Data." CNET News. CBS Interactive, May 10, 1999. Erişim tarihi 19 Mayıs 2015. http://www.cnet.com/news/ netmarket-exposes-customer-order-data/

Birdenbire, dünyanın bir ucundaki kişinin öteki ucundaki biriyle iletişim kurması sıradanlaştı. Ve insanlar küresel bir şekilde iletişim kurmaya başlayınca, kaçınılmaz olarak ticaretle uğraşmayı istediler.

Sorun şuydu ki, hiç kimse bilgisayar ekranının diğer tarafındaki kişiye güvenmek için sağlam bir zemine sahip değildi. Farklı bir adli yargılama alanındaki birine kredi kartınızın numarasını vermek hiç mantıklı değildi. Finansal kuruluş uyumluluk sorunlarına ek olarak –Amerikan kredi kartınız satıcının Rus bankasıyla uyumlu olacak mıydı?– süreç oldukça güvensizdi. Kredi kartı numaranızı, çoğunlukla şifrelenmemiş ortamda, herhangi bir yerde olabilecek isimsiz birine göndermenizi gerektiriyordu. İnternetin ilk günlerinden bu yana çevrimiçi alışveriş hiç şüphesiz daha güvenli olsa da, güvenlik en büyük endişe olarak kaldı ve internet para birimi ya da 'e-paranın' kullanımı için asıl gerekçe oldu. Para havalesi, dağınık fonlar, mikro ödemeler ve erişilebilir yatırım, Bitcoin'in günümüzde büyük gelişme gösterdiği alanlar olarak sık sık işaret edilse de, elektronik paranın ilk tekrarlarının arkasındaki asıl amaç bu güvenlik endişelerini ele almaktı.

1994'de yayınlanan kitabı *Out of Control: The New Biology of Machines, Social Systems, and the Economic World*'de, *Wired* dergisi editörü Kevin Kelly, internet ekonomisinin tam anlamıyla kalkışa geçmesi için neye ihtiyacı olduğunu düşündüğüne değiniyor. Kelly'ye göre, "Oldukça iyi bir toplumun anonimlikten daha fazlasına ihtiyacı vardır. Bir çevrimiçi medeniyetin çevrimiçi anonimliğe, çevrimiçi kimlik tespitine, çevrimiçi belgelemeye, çevrimiçi itibara, çevrimiçi güvenilir kişiye, çevrimiçi imzalara, çevrimiçi

gizliliğe ve çevrimiçi erişime ihtiyacı vardır. Hepsi açık toplumların vazgeçilmez malzemeleridir." Kelly'ye göre, internetin gizlilik ve kimlik saptama, doğrulama, itibar sağlamak için anonimliğe ve güvenlik sağlamak için imzalara ihtiyacı var. Bu iki arzu temelde birbirleriyle çelişiyor gibi görünüyor. Aynı anda hem gizliliğe hem de kimlik saptamaya nasıl sahip olabilirsiniz?

Kevin Kelly ve dönemin 'şifrepunklarının' doğru bir şekilde öngördükleri gibi, yanıt kriptografi ve şifrelemede gizli:

> Bana öyle geliyor ki, şifreleme teknolojisi ağ sistemlerinin oluşturduğu bilgi ve veri akınını bir yerde dizginliyor, medenileştiriyor. Bu evcilleştiren ruh olmadan, Net kendi hayatını kapana kıstıran bir ağa dönüşür. Çabuk üreyen bağlantılarıyla kendi kendini boğar. Bir şifre, ağın yang'i için bir yin'dir, merkezsizleşmiş, yaygın sistemlerden doğan patlayıcı ara bağlantıları evcilleştirebilen küçük gizli bir güçtür. Şifreleme, düğüm iyice karışırken çevik ve hızlı kalabilmesi için bir kovan kültürünün gerektirdiği lüzumlu kontrolsüzlüğe izin verir.

Özellikle açık anahtar şifreleme bu etkiyi gösterebilirdi. Açık anahtar, kullanıcıların kimliklerinin saptanmasına gerek kalmadan doğrulanmasına izin verir. Geleneksel şifreleme, bir mesajı çözen önceden belirlenmiş bir anahtara dayanır. Bu güvenilir bir ikinci kişiyle işe yarayabilir ama elbette kalabalık gruplar ya da anonim kaynaklarla uğraşırken ideal değildir, çünkü anahtar kolaylıkla ele geçirilebi-

lir. Açık anahtar şifrelemeyle, her kullanıcının iki anahtarı bulunur: bir açık anahtar ve bir özel anahtar. Açık anahtar açıkça paylaşılabilir ve herhangi birinin sadece özel anahtarınızın çözebileceği bir mesajı şifrelemesine yarar. Açık anahtar özel anahtarı keşfetmek için kullanılamaz, o nedenle paylaşılması güvenlidir ama dijital imzalama denilen bir teknikle işlem ters bir şekilde çalışabilir. Özel anahtarınızı kullanarak bir mesajı şifrelerseniz –bir başka kullanıcının açık anahtarınızı kullanarak bir mesajı şifrelemesi yerine– sadece açık anahtarınızla çözülebilen bir mesaj yaratırsınız. Bu kullanıcıların, taklit edilemeyecek bir şekilde, bir mesajı ya da dokümanı dijital olarak imzalamalarına imkân sağlar. Ancak Bitcoin'in gelişimi için daha da önemlisi, bir kişinin dijital olarak imzaladığı bir şeyi göndermediğini ya da postalamadığını iddia etmesini imkânsız kılmasıdır. Bu doğrulanabilir ek güvenlik katmanı herhangi bir dijital para biriminin doğru düzgün bir şekilde işlemesi için son derece önemlidir.

Issız adada mahsur kalan 20 kişi örneğine geri dönecek olursak, farz edelim ki aralarında bir anlaşmazlık çıktı. Bir kişi başka birine mal ya da hizmet karşılığında ödeme yaptığını iddia ediyor ama ikinci kişi alışverişin gerçekleştiğini inkâr ediyor. O sırada söz konusu alışverişin kaydını tutabilecek biri olmadığı için kimse hangi hesap defterinin doğru olduğunu bilmiyor. Bizim senaryomuzda, kimin doğruyu söylediği kimin yalan söylediğini kararlaştırmak zor olur. Bitcoin ağı her katılımcıyı her işlem yaptığında dijital imzaya zorlayarak bu işlemin çok daha güvenilir olmasını sağlıyor, 'imzanızın' kredi kartı işleminizi ya da çekinizi güvenceye almasından pek farklı değil.

Bitcoin dünyasında, açık hesap defterine blokzinciri

denir. Bitcoin ağında, cüzdan denen her hesap blokzinciri üzerinde takip edilir. Ağa her işlem gönderildiğinde, gönderici onu dijital olarak imzalar ve işlemin bir tarih damgası yaratılır. Daha sonra birlikte işlenen bir grup işleme dahil edilir ve bir önceki işlem grubunun sıkıştırılmış bir versiyonu gruba eklenir. Her yeni işlem grubu bir önceki grubun sıkıştırılmış bir versiyonunu içerdiği için sıra boyunca herhangi bir şeyi değiştirmek işlem geçmişini değiştirip zinciri geçersiz kılar. Biri geri gidip eski bir işlemi silmek ya da değiştirmek isterse, o noktaya kadar hesap defterini oluşturan matematiksel hesaplamaları yeniden yapmak zorunda kalır.[4] Bu da blokzincirinin neredeyse değişmez olduğu anlamına geliyor.

Ağa bir işlem gönderildiğinde, blokzincirinde sonsuza kadar saklanır. Topluluğun geri kalanı iki katılımcıdan herhangi birinin sözüne güvenmek zorunda değildir. Blokzincirine –ya da hash adındaki sıkıştırılmış versiyonuna– kaydedilen işlem ya kriptoyla doğrulanır ya da doğrulanamaz. Tartışmaya yer yoktur.

Bu ağın sorunsuz bir şekilde işlemesi için birinin her işlemin hash'lerini doğrulayan karmaşık matematiksel denklemler işlemesi gerekir. Bu katılımcılara madenciler deniyor; bu işlemleri gerçekleştirip blokzincirine eklemenin karşılığında, madenciler yeni yaratılmış bitcoin'lerin yanı sıra her işlemden alınan küçük miktardaki madenci ücretinin kazancıyla ödüllendirilirler.

Daha sonra madencilik hakkında daha detaylı konuşacağız, ama blokzincirinin blok adı verilen yaklaşık 10 daki-

[4]Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Directory System." The Cryptography Mailing List (2008). Erişim tarihi 18 Mayıs 2015. https://bitcoin.org/bitcoin.pdf

kalık segmentlere kaydedildiğini söylemekte yarar var. Bir madenci bir grup işlemi uygun biçimde her doğruladığında ödüllendirilir.

Blokzinciri her işlemin ve bakiyenin kaydedilmesine, izlenmesine ve doğrulanmasına imkân tanır. Bu sırada, kriptografi ve merkezsizleştirme oldukça basit becerileri olan kullanıcıların işlemleri sırasında makul bir şekilde anonim kalmalarına izin vererek güvenliği mahremiyetle birleştirir. Yasadışı malların internette satılmasıyla ilgili hissedilen küçük endişeleri itibarsızlaştırmaya hevesli Bitcoin hayranları, Bitcoin'in anonim değil, takma isimli olduğuna dikkat çekeceklerdir. Aradaki fark şudur: 'Anonim' herhangi bir kimliğinizin olmadığı anlamına gelirken, 'takma isim' çevrimiçi işleyici ya da bir Bitcoin adresi gibi gerçek kimliğinizi doğrudan teslim etmeyen bir kimlikleyici anlamına gelir.

Bu tartışma kelime anlamlarından ibarettir, çünkü giriş seviyesinden biraz üstün Bitcoin tekniğine sahip biri için takma ad rahatlıkla anonimliğe dönüşür. Yine de, Bitcoin özünde o 1990'ların başındaki gelecekçiler ve ekonomistlerin hem arzuladığı hem de korktuğu şeydir. İnternet para birimlerinin anonim ya da takip edilebilir olup olmayacağı üzerine çelişen görüşler vardı. İkisi birden oldu: Her şey takip ediliyor ama kullanıcılar gerçek kimliklerini gizleyebiliyorlar.

Kullanışlı bir e-para biçimi yaratılmadan çok önce, dijital para birimlerinin potansiyel tehlikeleri hakkında uyarılar vardı. Bazıları bu para birimlerinin teröristlere, uyuşturucu satıcılarına, rüşvetçilere, pedofillere ve diğer suçlulara yardımcı olacağından korkuyordu. 1994'te *Jour-*

nal of Criminal Justice Education'da yer alan makalesinde, o zaman Georgetown Üniversitesi'nde bilgisayar bilimi başkanı olan Dorothy Denning, bu tehlikelerin biri hakkında şöyle yazdı:

"[Kriptografi] izi sürülemez nakit ve anonim, izi sürülemez işlemleri mümkün kılabilir. Bu tür hizmetler birçok gizlilik faydası sunsa da, aynı zamanda para aklama ve dolandırıcılığa da olanak sağlayabilir."[5]

Bu tür endişeleri dile getiren tek kişi Denning değildi. Aralık 1994 *Wired* dergisi makalesinde, Steven Levy, Amerikan Bankacılar Birliği üyesi Kawika Daguio'dan alıntı yapıyor:

> Kendim için konuşacak olursam, izi sürülemez ve sınırsız miktarda dijital para biriminin üretilmesi tehlikeli ve güvenilmez bir kamu düzeni yaratır... Suçluların şu an elinde olmayan suistimal etme fırsatlarını açığa çıkarır. Fiziksel dünyada, para büyük hacimlidir. Fiziksel dünyada, insanları takip etmek mümkündür, bu nedenle para işaretlenirse, para dışarıda gözlemlenirse ya da seri numaraları kaydedilirse, adam kaçıran biri yakalanabilir. Tamamen anonim bir para sahtecilik ve dolandırıcılık fırsatlarına izin verir.[6]

Daguio'nun anonim dijital para birimlerinin potansi-

[5]Denning, Dorothy E. "Crime and Crypto on the Information Superhighway." *Journal of Criminal Justice Education* 6.2 (1995): 323-36. Erişim tarihi 28 Ekim 2015. http://www.tandfonline.com/doi/abs/10.1080/10511259500083501?journalCode=rcje20

[6]Levy, Steven. "E-money (That's What I Want)." *Wired* 1 Dec. 1994: n. pag. Wired.com. Erişim tarihi 28 Ekim 2015. http://www.wired.com/1994/12/emoney/

yelleri üzerine eleştirisi günümüzde Bitcoin'in karşı karşıya olduğu eleştirilere; suçluların, adam kaçıranların ve rüşvetçiler tarafından kullanıldığı iddialarına çok benziyor. Bu tür şeylerin de olduğunu inkâr etmeyeceğim.

Nakit paranın suç faaliyetlerinde dijital para birimlerinden çok daha sık ve uzun bir süredir kullanıldığını tartışmayacağım bile, çünkü açıkçası dijital para birimleri belirli suç faaliyetlerine nakit paradan daha uygun. Bitcoin kullanışlı bir araç ve insanlar hem iyi hem de kötü amaçla onu kullanma imkânı bulacaklar. Dijital para birimlerini etrafını kuşatan suç faaliyetlerinin gelecekte daha ileri düzeyde olacaklarını düşünüyorum, ama aynı şekilde, meşru yatırımlar ve yenilikler de gelişim gösterecek.

Bitcoin birçok şey. O bir çevrimiçi para birimi, yaygın bir hesap defteri ve merkezsizleşmiş bir ağ. Ama buna rağmen, internetin ilk öncülerinin öngörülerini, arzularını ve hatta korkularını gerçekleştiren şey olabilir.

İkinci Bölüm:

Bitcoin Satın Almak, Biriktirmek ve Harcamak Üzerine Pratik Bir Rehber

Paramızı ve inancımızı politika ve insan hatasından muaf olan matematiksel bir yapıya emanet etmeyi seçtik.

– Tyler Winklevoss, girişimci ve Olimpiyat sporcusu

Demek birkaç bitcoin istediğinize karar verdiniz. Kulağa yeterince basit geliyor ama şimdi ne yapacaksınız? En önemlisi, elde ettiğiniz bitcoin'lerle tam olarak ne yapmak istediğinize karar vermenizdir.

Öncelikle, bol miktarda bitcoin'i ücretsiz almayı unutun. Daha sonraki bölümlerde açıklayacağım sebeplerden ötürü, ortalama kullanıcıların madencilikle –daha fazla bitcoin üreten işlem– bitcoin elde etmesi artık makul değil. Küçük miktarda bitcoin'leri ücretsiz ya da reklam izleme karşılığında dağıtan musluk denen şeyler var, ama bunlar her defasında bir sentin çok küçük bir parçasını veriyorlar.

Bitcoin'leri satın almak çok daha iyi bir fikir. Sırada onları nereden ve nasıl satın alacağınız ve sahip olduktan sonra onlarla ne yapmak istediğiniz gibi sorular var.

İlk soruyu ele alalım. Bitcoin'leri ya başka birinden ya da bir borsadan satın alabilirsiniz. Şu anda, Birleşik Devletler'deki en saygın borsalar Circle ve Coinbase'dir. Bu borsalara üye olmak, ilgili mevzuatlara, bir diğer deyişle Müşterini Tanı [Know-Your-Customer (KYC)] ve Kara Para Aklamayı Önleme [Anti-Money Laundering (AML)] mevzuatlarına uymak zorunda olduğunuz anlamına geliyor. Bu genellikle taranmış bir resmi kimlik ve ikamet yerinizi kanıtlayan bir fatura gibi belirli bir düzeyde kimlik doğrulama olacağı anlamına geliyor.

Borsalardan biri, Circle ya da Coin, banka hesabınız, kredi kartınız ya da her ikisiyle bağlantı kuracak. Kimliğinizi doğruladıktan sonra bitcoin satın alabilirsiniz. Genellikle hesabınıza anında aktarılırlar, ama borsalardan biri alımı şüpheli bulursa ya da çok büyük bir tutarsa birkaç gün sürebildiği bilinmektedir.

Her iki borsa da –yasal para ve bitcoin arasındaki işlemlere imkân tanıyan diğer birçoğu gibi– size ağ cüzdanı denen bir cüzdan tanımlayacak. Bu tür işlemler durumunda, Bitcoin bankaları olarak görev görüyorlar. Sizin için özel anahtarlarınızı, yani sahibinin belirli bir cüzdandan bitcoin göndermesine izin veren benzersiz ve rastgele belirlenmiş karakterleri tutacaklar. Dilediğiniz yere bitcoin göndermekte serbest olsanız da, herhangi bir borsa teorik olarak hesabınızı kilitleyebilir. Bu borsalardan biri batarsa, bitcoin'leriniz büyük ihtimalle kaybolur.

Bu uzak olasılığa rağmen, birçok kullanıcı hâlâ bit-

coin'lerini bu borsalarda tutuyorlar. Coinbase ve Circle yakın zamanda herhangi bir yere kaybolacak gibi görünmüyor. İkisinin de de girişim sermayesi fonuna milyonlar akıtıldı ve ikisi de onlarca yıl boyunca Bitcoin dünyasında lider olmayı amaçlıyorlar.

Her halükarda, ağ cüzdanlarının en büyük avantajı, sunduğu rahatlık. Bilgisayardan ya da cep telefonundan rahatlıkla erişilebilirler ve ikisinin de kullanıcı dostu arayüzleri var. Olumsuz tarafı gizlilik ve güvenlikten taviz vermek zorunda olmak. Her iki hizmet için de iki faktörlü kimlik doğrulama mevcut ve şiddetle tavsiye ediliyor. 'İki faktörlü kimlik doğrulama' iki ayrı bilgi; bir şifre ve başka bir şey gerektiren her güvenlik sistemini tanımlamak için kullanılan bir terimdir. O 'başka şey' genellikle kısa mesaj ya da Authy ve Google Authenticator gibi popüler cep telefonu uygulamaları aracılığıyla teslim edilir.

Artık bitcoin'lerimiz olduğuna göre, onlarla ne yapacağız? Eğer bol miktarda bitcoin satın almayı planlıyorsanız, muhtemelen onları Coinbase ve Circle'dan daha güvenli bir yere taşımak isteyeceksiniz. Kullanıcılar için kullanışlı ve biraz daha fazla güvenlik sağlayan çoklu imzalı ağ cüzdanları var. Coinkite ve BitGo kusursuz güvenlik önemleri olan iki popüler site. Tecrübe sahibi olduğum BitGo, anahtarınızı belirlemeniz için birkaç seçenek sunuyor. Tarayıcınız aracılığıyla rastgele belirlenebilir, üçüncü bir parti onu üretebilir, bir uygulamaya –şu anda sadece iOS'te mümkün– ürettirebilir ya da kendiniz üretebilirsiniz. Üçüncü parti hizmet kullanmak anahtarınızı kaybederseniz geri alabileceğiniz anlamına gelir. Ancak, bu üçüncü partinin anahtarınızı doğru düzgün koruyacağına güvenmenizi gerektirir.

Çevrimdışı üretme, bir diğer deyişle internete bağlı değilken şifreli bir anahtar üretme hariç, yukarıdaki seçeneklerin hepsi anlaşılır sayılır. Bu durumda, BIP32 anahtar üreten bir yazılım bulmanız gerekecek. Bit32.org'u öneririm. Talimatları takip ederek anahtarınızı üretin, BIP32 uzun anahtarınızı alıp BitGo'ya kopyalayın. En iyi güvenlik için bu son adım normalde kullandığınız bilgisayar dışında bir bilgisayar üzerinde yapılmalıdır.

Artık çoklu imzalı bir ağ cüzdanıyla silahlandığınıza ve özel anahtarınız üzerinde biraz olsun kontrol sahibi olduğunuza göre, bir sonraki aşama Circle ya da Coinbase cüzdanınızdan o cüzdana bitcoin'ler göndermek olacak. 3 ile başlayan ve şöyle 3Bi1fhng5LfoDzue5MTfGw9PgHNKKgRkVt bir şeye benzeyen –insanlarla paylaşmakta özgür olduğunuz ve insanların size bitcoin göndermelerine izin veren– 'açık anahtarınızı' alın. (Circle ya da Coinbase açık anahtarınız, varsayılan haliyle çok imzalı olmayan, benzer görünür ama 1 ile başlar.) 'Gönder' butonuna ya da Coinbase, Circle cüzdanınızda 'bitcoin gönder' butonuna tıklayın ve sonra 'Alıcı:' kısmına BitGo, Coinkite ya da kâğıt cüzdan adresinizi kopyalayıp 'gönder' butonuna tıklayın.

Orada, bitcoin'lerinizi oldukça güvende tutarken, başka Bitcoin adresine bitcoin gönderebilir ya da başka adreslerden bitcoin alabilirsiniz. Bu sadece harcamak isteyebileceğiniz ama çabucak yasal paraya dönüştürmek istemeyeceğiniz orta ölçekli –bu size ne ifade ediyorsa– para tutarı için kabul edilebilir.

Coinbase yakınlarda Vault adı verilen kendi çoklu imzalı cüzdan hizmetini başlattı. Başkalarına ya da kendinize anahtarlar vermenizi sağlayan kullanıcı dostu bir seçenek.

BitGo'nun bu alanda birkaç yıl daha fazla tecrübesi ve itibarı var, ama bu da uygulanabilir bir seçenek.

Eğer o bitcoin'leri paraya dönüştürmek isterseniz, nakit karşılığında birine satabilir (bitcoin'leri ticari olarak satmayı planlamıyorsanız PayPal ya da diğer geri çevrilebilir işlemleri önermiyorum) ya da tekrar Coinbase'e, Circle'a koyup oradan satabilirsiniz ve para birkaç iş günü içerisinde banka hesabınıza aktarılır.

Para ve diğer ödeme yöntemleri karşılığı bitcoin alım-satım işlemini onuncu bölümde anlatacağım.

Uzun vadeli yatırım için 'kâğıt cüzdan' yazdırmak iyi bir fikir. Bunu yapmak için bana kalırsa en güvenli ve kullanışlı yazılım bitaddress.org. Tarayıcınızda gerçekleştirdiğiniz rastgele hareketleri (fareyi hareket ettirmek, tuşlara basmak, vs.) temel alarak Bitcoin adresleri oluşturuyor ve daha sonra bunlardan bir adres yaratmanıza izin veriyor. Daha güvenli bir cüzdan için yazılımı indirmeniz önerilir (buna izin veren sitede bir link mevcut).

Daha sonra, cüzdanı yazdırın ve daha önce yarattığınız ağ cüzdanını kullanıp kâğıt cüzdanınız için yaratılan açık adrese kare kodu kullanarak (ya da açık adresi elle girerek) bitcoin gönderin.

Elbette, her şeyi kendi kendinize yapma seçeneğiniz mevcut. Ne de olsa, Bitcoin bundan ibaret: üçüncü şahıslar olmadan para. Bitcoin Core ve blokzinciri kopyanızı indirerek –birazdan buna değineceğiz– bulunduğu bilgisayar kadar güvenli olan bir Bitcoin cüzdanına sahip olabilir ve bu sırada Bitcoin ağını güvenceye almaya yardımcı olabilirsiniz. Buna yerel cüzdan deniyor. İnternete bağlı olmayan bir yerel cüzdan çevrimdışı cüzdandır ve genellikle 'soğuk depo' olarak ifade edilir.

Bu, pek de kullanıcı dostu bir işlem değil ve birine ilk Bitcoin cüzdanı için yapmasını önerebileceğim bir şey değil. Bununla birlikte, Bitcoin'i uzun vadeli tutmayı planlayan her Bitcoin kullanıcının en az bir kez yapması gereken bir şey. Emeklilik için para biriktirmek amacıyla yüklü miktarda para biriktirmeyi planlayan herkes –uzun vadeli birikimleri bir kâğıt cüzdana koymayacaklarsa– mutlaka yerel bir cüzdan ve çevrimdışı bir cüzdan oluşturmalı.

Çevrimdışı ve yerel cüzdanlar için çoklu imza hizmeti sunan Bitcoin Core ve Armory en popüler yerel cüzdanlardan ikisidir. Onları bitcoin.org ve bitcoinarmory.com sitelerinden indirip programları kurun. Programı açınca, uzun süren (50GB'dan büyük) Bitcoin blokzinciri indirme işlemine başlayacaksınız. Tamamlanınca, tam düğüm denen bir şey olarak Bitcoin ağının meşru bir parçası olacaksınız. Blokzincirinin sürekli güncellenen bir versiyonunu tutacak ve madenciler tarafından doğrulanan işlemleri dağıtacaksınız (madenciliğe daha sonraki bölümlerde değineceğiz). Tam düğüm olmak gerekli değildir –bu işlem, bant genişliğinde büyük yer işgal eder– ama her düğüm Bitcoin ağının sorunsuz ve güvenli çalışmasına yardımcı olur. Yazılım her şeyi kendi kendine halleder ama herhangi bir sorunla karşılaşırsanız 8333 bağlantı noktasının açık olduğundan emin olun. Bunu yapabilmek için kendi yönlendirici ayarlarınızı kontrol etmeniz gerekecek.

Bu noktadan sonra, işlem yine oldukça açık ve bir ağ cüzdanı kullanmaktan pek farklı değil. Cüzdanı çevrimdışı bir cüzdana dönüştürmek isterseniz, programın klasöründe 'wallet.dat' dosyasını bulun ve onu USB çubuğuna ya da benzer bir depolama aygıtına taşıyın.

Bahsetmeye değer son bir seçenek ise 'donanım cüzdan.' Farklı şirketler tarafından yaratılan bu cüzdanlar insanların Bitcoin ağına mümkün olduğunca az bağlanarak bitcoin'lerini saklama ve harcama imkânı tanıyor. Ne yazık ki bunlardan birini kullanmadım ve faydaları hakkında kesin konuşamam. KeepKey, TREZOR ve Ledger şu anda endüstrinin liderleri.

Artık bitcoin'leri nasıl elde edeceğinizi, saklayacağınızı ve harcayacağınızı biliyorsunuz. Ama bunu neden isteyesiniz? Bunu açıklamak biraz daha uzun sürecek. Bitcoin'in kısa bir tarihiyle başlayacağım.

Üçüncü Bölüm:

Öncüler, Tarih ve Yaratılış, Satoshi'nin Makalesi

Bir süredir, tamamen eşler arası olan, üçüncü bir partiden bağımsız yeni bir elektronik para sistemi üzerinde çalışıyorum.
Makaleye şu adresten ulaşabilirsiniz: http://www.bitcoin.org/bitcoin.pdf
Ana özellikleri şöyle:

Eşler arası ağ sayesinde çift harcama önleniyor.
Darphane ya da başka bir güvenilir kuruluş yok.
Katılımcılar anonim olabilirler.
Yeni paralar Hashcash tarzı çalışma ispatıyla (PoW) yapılır.
Yeni para üretiminde gereken çalışma ispatı aynı zamanda ağa güç sağlayacak ve mükerrer harcamayı önleyecek.

— Satoshi Nakamoto'nin Bitcoin duyurusu,
The Cryptography and Cryptography Policy Posta Listesi, 1 Kasım 2008

Bu mesajla birlikte, Satoshi Nakamoto adı altında yazan anonim bir kişi ya da grup günümüzde Bitcoin olarak bilinen devrimi başlattı.

İnternet toplum bilincine ilk girdiğinde, insanlar hemen internet ticaretinin nasıl idare edileceğini merak etmeye başladılar. Birçok kişi internet aracılığıyla mal satma potansiyelini görebiliyordu, ne de olsa –daha önce değindiğim gibi– 1970'lerden beri bilgisayarlar aracılığıyla evden alışveriş yapmayı mümkün kılan sistemler vardı. Asıl sorun internet üzerindeki işlemleri güvenli kılan bir sistemin olmamasıydı. Eğer birinden bir şey satın almak istiyorsanız, onlara e-posta aracılığıyla kredi kartı numaranızı göndermek ve sizden fazla para çekmemelerini ya da e-postanın engellenmemesini ya da başka birinin eline geçmemesini ummak zorundaydınız. Bu durum hiç ideal değildi ve köklü, meşru şirketler çevrimiçi ticaret yapmıyorken, kredi kartı bilgilerinizi internetteki isimsiz birine verme fikri en hafif tabiriyle saflık, en kötü ihtimalle çılgınlık olarak görülürdü.

İnternetin yaygın kullanımından önce bile, insanlar bu sorunun çözümü üzerinde çalışıyorlardı. Ortak teklif, internet için resmi dünyadan (ya da hükümetin bastığı bir para biriminden) muaf olarak çalışan bir para birimi üretmekti. Bitcoin böyle bir para birimi yaratmak için ilk çaba değildi. Satoshi Nakamoto Bitcoin tanıtım yazısını 2008'de yayınlamadan önce birkaç dijital para birimi daha yaratılmaya çalışıldı.

Bitcoin de dahil olmak üzere, bütün dijital para birimlerinin asıl amacı işlemin güvenli olmasını sağlamaktır. Kopyalanabilen, aynı anda iki farklı yerde harcanan ya da

kişinin yasal olarak sahip olduğundan daha fazlasını harcayabilmesini sağlayan bir dijital para biriminin hiç anlamı yoktur. Dijital paranın işlevini yerine getirebilmesi için insanların paranın değerine inancı olmalıdır ve güvenlik kusurları varsa, insanlar ona güven duymazlar.

Bu endişe ancak katılımcılar için bir tür yükümlülük olursa giderilebilir. Kullanıcıların kötü niyetle hareket etmediklerinden emin olan bir şey olmalıdır. İşlemlerimize gözcülük yapan bir varlık şart değil ama ağın her hesabın harcamaya çalıştığı değere sahip olduğundan emin olması gerekir.

David Chaum ilk kısmen başarılı internet para birimi Digicash'i yarattı. Chaum ilk internet öncülerindendi ve 1983'te, ilk ağ tarayıcısı halka sunulmadan yıllar önce, elektronik para kavramıyla ilgili yazılar yazdı. Chaum'un elektronik para sistemi için kritik gördüğü üç özellik vardı ve en sonunda Digicash'e dahil edildiler. *Advances in Cryptology: Proceedings of Crypto 82*'de yayınlanan 'İzlenemez Ödemeler için Kör İmzalar' başlıklı yazısında, elektronik para sistemi için ana gereksinimler olarak gördüğü şeyleri özetliyor:

1) Üçüncü kişilerin bir kişi tarafından yapılan ödemenin kime, ne zaman ya da ne kadar yapıldığını belirleyememesi
2) Sıra dışı hallerde, şahısların ödeme kanıtı sunabilmesi ya da ödemeyi alan kişinin kimliğini saptayabilmesi
3) Medyanın çalıntı olarak bildirdiği ödemeleri kullanma olanağı

Bu ana gereksinimlerde eksik olan şey merkezsizleşme kavramı. Aslına bakılırsa, Bitcoin merkezi bir sistemden ziyade merkezsizleşmiş bir sisteme dayanan ilk elektronik para sistemi oldu. Chaum'un icadı Digicash ağırlıklı olarak merkezi yapılara dayanıyordu.

Chaum'un 1983'te hakkında yazdığı kör imza fonksiyonu şu şekilde çalışıyordu: Bir kullanıcı dijital bir token talep eder, yani temelde önceden belirlenmiş bir değerde bir bankada paraya çevrilebilen eşsiz bir belirleyicisi olan bir dizi kod. Banka kullanıcıya token'ı dijital olarak verir ve kullanıcı ona bankanın görmeyeceği bir kör seri numarası (ya da imza) iliştirir. Banka seri numarasının ne olduğunu görmeden token'ı imzalar. Kullanıcı ancak o zaman onu bir satıcıya göndermeden önce seri numarasını açığa çıkarır. Satıcı onu veren bankaya götürür ve bankada verilen bütün seri numaralarının olduğu bir hesap defteri bulunur.

Ne yazık ki, bu süreç korkulan çift harcama saldırısını güvenilir bir biçimde önleyemezdi. Bir kullanıcı, teoride, bir satıcıda harcadığı token'ı daha sonra başka birinde harcayabilirdi. Satıcı token'ı bankaya gönderip onun hesap defterinde olduğunu öğrenemeden satın aldığı ürün kullanıcının yanına kâr kalırsa, kullanıcı o token'ı başarılı bir şekilde iki kez harcamış olur.

Digicash şirketi 1990'da faaliyete başlayıp Chaum'un 'e-para' konseptini hayata geçirdiğinde, bu olası soruna önerilen çözüm ödeme yapılan kişi eğer kötü niyetli davranıyorsa, o kişinin anonimliğini ortadan kaldırmaktı. Kullanıcı kişisel bilgileri bankaya gönderecek ve şifrelenen bilgiler token'la ilişkilendirilecekti. Satıcı bilgiyi göreme-

yecekti ama token iki kez harcandıysa, ikinci token biraz farklı olacaktı. Banka çift harcayan kullanıcıyı ortaya çıkarmak için bu bilgiyi kullanabilirdi. Bu sistemin kusuru, para ödenen tarafın savunmasızlığıydı. Çalıntı hesap ya da hileli hareket eden bir banka gibi durumlarda, masum kişi sadece parası çaldırmakla kalmayıp, aynı zamanda hırsızlıkla suçlandığı için itibarı zedelenecekti.

Bu sistem yayılmadığı ve David Chaum herkes tarafından tanındığı için Digicash'in yasal sistemin belirlediği sınırlar içinde işlemekten başka seçeneği yoktu. Hükümetlerin desteğini ve onayını kazanmak için e-parayı izi sürülebilir kılmak zorunluydu. Şantaj, kara para aklama ve teröristleri fonlama hakkında endişeler vardı, o nedenle Digicash e-parasını belirli durumlarda anonimliği ortadan kaldırmaya izin veren bir biçimde çalıştırmak zorundaydı.

Yetkili bir üçüncü partinin anonimliği ortadan kaldırma fikri günümüz Bitcoin topluluğunda kutsal değerlere hakaret olarak görülür. Ama Chaum'a fazla yüklenmemek gerek. O, farklı bir dönemdi. Anonimlik ikinci plandaydı, asıl önemli olan Digicash'in işlediğinden emin olmaktı. Ve suç faaliyetleri durumunda başvuracak bir yer isteyen bankaların ve hükümetlerin desteği olmadan işlemesi imkânsızdı.

Digicash ve e-parası bir süre dayandı ama asla popüler olmadı, yine de birkaç kez çok yaklaştı. Raporlara göre, Citibank, Visa ve Microsoft'la anlaşma yapmaya çok yaklaşmıştı.[1] Hatta Microsoft'un Digicash'in Windows 98'e da-

[1]Vigna, Paul, and Michael J. Casey. The Age of Cryptocurrency: *How Bitcoin and Digital Money Are Challenging the Global Economic Order*. New York: St. Martin's Press, 2015. 56-59.

hil edilmesi için şirkete 180 milyon dolar teklif ettiği bile söyleniyordu, ama bunu doğrulayan güvenilir kaynaklar bulamadım. Sonuçta, teknik başarısızlıklardan ziyade ticari başarısızlıklardan ötürü bu anlaşmalar gerçekleşmedi.[2]

Sebebi ne olursa olsun, Digicash'in e-parası hiçbir zaman yükselişe geçmedi. Yeterli sayıda satıcı kabul etmedi, yeterli sayıda banka onu kullanmadı ve şifreleme yöntemleri insanların kredi kartlarıyla çevrimiçi ticaret yapmalarına imkân verirken, tüketiciler onu pek faydalı bulmadılar.

Digicash anlaşılmazlık içinde çaba gösterdi, sönük kaldı ve teknolojisinin diğerlerinden daha üstün olduğu konusunda kendisine fazlasıyla güvendi. Bu sırada, internet ilerlemeye devam edip onsuz gelişim gösterdi. 1998'de Digicash iflasını açıklayıp kapatıldığında, e-ticaret büyük bir işe dönüşmüştü ve PayPal'a benzer ağ cüzdanları öne çıkmak üzereydi.[3]

Digicash'in başarısızlığından sonra, kripto para birimi dünyasında pek fazla şey olmadı. Aksine, bir bankayla doğrudan uğraşmadan birbirlerine para gönderme imkânını kullanıcılarına sunan PayPal gibi hizmetler yükselişe geçti. Kullanıcıların yine de PayPal aracılığıyla işlemlerini yapmaları gerekiyordu ama bu süreç daha kullanışlıydı ve PayPal bunu kolaylaştırdı. Bankanın aktarımını ve hesap numaralarını kaydetmek için upuzun rastgele haneler yazmak zorunda değildiniz; tek ihtiyacınız olan bir e-posta adresiydi. Ve kişisel detaylarınızı diğer taraflara ifşa etmek

[2]Clark, Tim."Digicash Files Chapter 11." CNET News. November 4, 1998. Erişim tarihi 21 Haziran 2015. http://news.cnet.com/2100-1001-217527.html

[3]"E-Stats." United States Department of Commerce. March 7, 2001. doi:10.1021/ cen-v077n034.p028

zorunda değildiniz. PayPal'ın ortaya çıkması çok önemliydi, çünkü kredi kartı bilgilerinizi çevrimiçi ortamda paylaşabileceğiniz şirket sayısı artıyor olsa da, küçük işletmelerin, özellikle de eBay gibi hızla büyüyen hizmetler aracılığıyla, internette bir güç olarak kalacakları belliydi.

Tabii birkaç kripto para teşebbüsü daha oldu, bunlardan en önde geleni de E-gold'du. E-gold –tahmin ettiğiniz üzere– altın tarafından desteklenen bir dijital para birimiydi. Şirket, dijital para birimini destekleyen gerçek altın külçeler bulunduruyordu.

Şirket, Douglas Jackson adında eski bir onkolog tarafından 1995'te kuruldu; son nefesini 2009'da verdi.[4] Bitcoin'den önce E-gold hiç şüphesiz internetin en başarılı para birimiydi ama her şey Jackson'a bağlıydı. Kendisi kara para aklama ve lisanssız para transferi faaliyeti suçlarını kabul ettiğinde, para birimi öldü. Yasalara uyma şartıyla ev hapsinden serbest bırakıldıktan sonra parayı tekrar canlandırmaya çalıştı ama artık çok geçti.

2009 yılından bir *Wired* makalesi, Jackson'ın para birimi öngörüsünü şöyle tarif ediyor:

> Jackson'ın öngördüğü gibi, E-gold hükümet kontrollerinden bağımsız bir şekilde dolaşımda olan ve borsaların yükselmesi ya da düşmesinden etkilenmeyen özel, uluslararası bir para birimiydi. Ateşli bir hevesle dolup taşan Jackson, onun modern para sisteminin hastalıkları için bir çare olduğunu iddia etti ve bir noktada 'insanoğlunun

[4] Jackson, Douglas. "E-gold Update: Value Access." e-gold Blog. November 2, 2009. Erişim tarihi 21 Haziran 2015. http://blog.e-gold.com/2009/11/egold-update-value-access.html.

kaderinde çığır açan bir değişiklik... insanlık için düşünülmüş muhtemelen en büyük fayda' olarak tanımladı.[5]

Bu, kulağa Bitcoin heveslilerinin kendi para birimleri hakkında söylediklerinden pek farklı gelmiyor. Hatta, E-gold'a ilk olarak çekilen kitle Bitcoin'i ilk benimseyen insanlara çok benzerdi: altın tutkunları, özgürlükçüler, mahremiyet savunucuları ve evet, suçlular.

2005 yılında çalıntı kredi kartları satan çevrimiçi suçlular hakkında yazılan bir *New York Times* makalesinde E-gold'dan bahsediliyor. Makaleye göre, global erişimi ve anonim hesapları nedeniyle ödeme yöntemi olarak E-gold'u tercih ediyorlarmış.[6] O sırada, E-gold en büyük ikinci çevrimiçi ödeme hizmetiydi, hızla büyüyen PayPal'ı takip ediyordu.

E-gold'a kapılanlar sadece kredi kartı hırsızları değildi. Saadet zincirleri de E-gold'la çalışıyorlardı. Jackson yetkililerle işbirliği yaptı ve hükümetin kullanıcı hesapları hakkında bilgi taleplerini yerini getirdi. Anlaşılan, Jackson bir kullanıcının kimliğini açığa çıkarmak istediğinde, E-gold anonim değildi. Ama çalıntı kredi kartı numaralarını araştıran Gizli Servis Jackson'la işbirliği yapmamaya karar verdi ve E-gold'u MoneyGram ve Western Union gibi benzerleriyle birlikte düzenlenmiş alana getirmeye çabaladı.

---

[5]Zetter, Kim. "Bullion and Bandits: The Improbable Rise and Fall of E-Gold." Wired.com. June 6, 2009. Erişim tarihi 21 Haziran 2015. http://www.wired.com/2009/06/e-gold/

[6]Zeller Jr, Tom. "Black Market in Stolen Credit Card Data Thrives on Internet." Nytimes.com. June 21, 2005. Erişim tarihi 21 Haziran 2015.

http://www.nytimes.com/2005/06/21/technology/black-market-in-stolen-credit-card-data-thrives-on-Inter- net.html

Ancak, Jackson şirketinin bu tür düzenlemelere boyun eğmemesi gerektiğini düşünüyordu.[7]

Hükümet onunla aynı fikirde değildi; Jackson lisanssız para aktarma hizmeti ve kara para aklama tezgâhı kurmakla suçlandı. Ve bu E-gold'un sonu oldu.

Bu sırada küçük bir 'sonradan görme' teknoloji ortaya çıkıyordu: Bitcoin. Ama Bitcoin yaratılmadan önce, çözülmesi gereken birkaç sorun vardı. 2008'de, Nakamoto Bitcoin'i tanımlayan tanıtım yazısını yayınlamadan aylar önce, Nick Szabo bit altın adını verdiği oldukça benzer bir şey sundu.

Bit altın hiçbir zaman yaratılmadı. Aksine, Bitcoin'in neredeyse bütün ana özelliklerini bünyesinde bulunduran bir öneriydi.[8] Nick Szabo'yu Satoshi Nakamoto'nun gerçek kimliği olabilecek inanılır adaylardan biri yapan şey bu benzerlik.

E-gold, Digicash ve daha önceki elektronik para birimi girişimlerinin aksine, bit altın merkezsizleştirilecekti. Zaman damgalı bir açık hesap defteri ve sınırlı sayıda somut defterleri olacaktı. Hiç kimsenin çözemediği merkezsizleşmiş hesap defteri sorununa Bizans Generalleri problemi denir. Bilindik açıklamasının gereksiz bir biçimde karışık olduğunu düşünüyorum.[9] Sorun şundan ibaret: içinde bilginin katılımcıları tarafından yayılması gereken bir ağ,

[7]Condon, Stephanie. "Judge Spares E-Gold Directors Jail Time." CNET. November 20, 2008. Erişim tarihi 21 Haziran 2015. http://www.cnet.com/news/judge-spares-e-gold-directors- jail-time/

[8]Szabo, Nick J. "Unenumerated." December 27, 2005. Erişim tarihi 21 Haziran 2015. http://unenumerated.blogspot.com/2005/12/bit-gold.html.

[9]Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine Generals Problem." In Programming Languages and Systems. 3rd ed. Vol. 4. Association for Computing Machinery, 1982. Erişim tarihi 21 Haziran 2015. http://research.microsoft.com/ en-us/um/people/lamport/pubs/byz.pdf

bu katılımcıların dürüstlüğüne itimat eder. Eğer dürüst değillerse, dürüst aktörlere dürüst olmayanlar tarafından verilen yanlış bilgiler ağda yayılabilir.

Nick Szabo'nun öncüsü olduğu ve Nakamoto'nun kusursuzlaştırdığı proof-of-work (PoW - çalışma ispatı) bu sorunu ele alıyor. Her işlem zaman damgalı ve öncesindeki işlemin bir hash'ini içeriyor, tabii o da kendisinden bir önceki işleminkini. Bu nedenle, eğer kötü niyetli oyuncu yeni bir zincir yaymak istiyorsa, hesap defterinde değiştirmek istediği işlemi bulması ve sonrasındaki işlemleri silip o noktadan sonra gerçekleşen bütün çalışmaları yeniden hesaplaması gerekir. Yoksa, sonradan ortaya çıkan her işlemin hash'i matematiksel olarak eşleşmez.

O nedenle, eğer o kötü niyetli parti meşru zinciri yakalamak istiyorsa, matematiksel denklemlerde meşru zincir üzerinde çalışan bir grup insandan daha hızlı olmalıdır.

Gerçek dünya bağlamında bunun anlamı, sahte bir blokzinciri oluşturup onu kabul ettirmeye çalışan bir madencinin meşru zincir üzerinde çalışan madencilerden daha fazla bilgisayımsal gücü olması gerektiğidir. Güvenli kalmak için meşru blokzinciri üzerinde tek bir sahte zincir üzerinde çalışan kötü niyetli oyunculardan daha fazla bilgisayımsal güç olmalıdır. Teorik olarak, aşağıda açıklık getirdiğim '%51 saldırısı' bu noktada devreye giriyor.

Bit altın çözümünün sorunlarından biri, bir hesap defterinin geçerliliğini belirlemek için ardındaki bilgisayımsal güç miktarından ziyade katılımcı sayısını kullanacak olmasıydı. Bu, bit altın önerisindeki her para birimini, kötü niyetli aktörlerin çok sayıda takma isim ürettikleri ve daha sonra bunları üzerinde değişiklik yapılmış hesap defterini

yaymakta kullandıkları Sybil saldırısı'na[10] maruz bırakırdı. Aksine, Bitcoin hesap defterinin ardında ne kadar bilgisayımsal güç olduğuna dayanıyor ve bu sadece kötü niyetli aktörlerin doğru olmayan hesap defterini yaymak için ağın hash gücünün %51'inden daha fazlasından sorumlu olmak zorunda olduğu %51 saldırısına karşı maruz olduğu anlamına geliyor. Bu tür bir bilgisayımsal gücü bir araya getirmek gerçekte mümkün değildir ve yüzlerce milyon dolara mal olur. Ayrıca, ağdaki hash gücü sürekli artıyor ve ağ büyüdükçe %51 saldırısı ihtimali giderek düşüyor.

Bu oldukça küçük farka rağmen, Nick Szabo'nun bit altınına bazen Bitcoin için başlangıç noktası denir. 2005'teki blog yazısında, Szabo anonimlikten bahsetmedi, ama günümüzde Bitcoin'in ekonomi felsefesinin ana ilkeleri olarak görülen iki fikirden söz etti: merkezsizleştirme ve enflasyona karşı direnç. Yazı bu fikirlerle başlayıp bitiyor:

> Uzun zaman önce bit altın fikrini keşfettim. Sorun kısaca şu ki, paramızın değeri şu anda üçüncü bir partiye olan güvene bağlı. Yirminci yüzyılda görülen çok sayıda enflasyonist ve hiperenflasyonist dönemler düşünüldüğünde, bu ideal bir gidişat değil. [...] Özetle, insanlığın kullandığı bütün para birimleri öyle ya da böyle güvensizdi. Bu güvensizlik sahtekârlıktan hırsızlığa kadar birçok şekilde dışa vuruldu. Bit altın bize bu tehlikelerden eşi benzeri görülmemiş bir şekilde korunan bir para sağlayabilir.

[10]Tschorsch, Florian, and Björn Scheuermann. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies." The Digital Currency Challenge. Erişim tarihi 21 Haziran 2015. doi:10.1057/9781137382559.0014

Aslına bakılırsa, daha önceki blog yazılarında 'bit altın' terimini kullanmamış olsa da, Szabo bu konsepte 2005 yılından önce yaklaştı. 1999'da, Wei Dai'in B-money önerisinden fazlasıyla ödünç aldığı bir konsept olan 'Tanrı Protokolü' üzerine yazısını paylaştı.[11] Bu, 1998'de Cypherpunk (Şifrepunkları) e-posta listesinde Dai tarafından sunulmuştu.[12] Günümüzde Bitcoin'de kullanılan en önemli özelliklerden biri olan, kripto para birimlerinde nadirliği yaratmak için hashcash kullanmayı öneriyordu: e-posta göndermek için ekstra bilgisayımsal güç gerektirerek istenmeyen e-postaların pahalıya mal olmasına neden olarak onları engelleyen bir sistem. Nadirliği, Bitcoin'in arz talep dinamiğine sahip olmasına imkân tanıyor.

Tanrı Protokolü, üçüncü parti merkezi sunucunun yerini otomatikleştirilmiş bir sanal üçüncü partinin almasını öneriyordu. Bulut bilişimin ilk konseptlerini kullanıyordu ve yürürlülüğe geçmiş olsaydı, muhtemelen günümüzün otonom –çok az ya da hiç insan girdisi olmadan işlevini yerine getirebilen dijital şirket– kuruluşunun bir proto-versiyonu olurdu. Birçok kişi Bitcoin'de *sırada* bunun olduğunu hayal ediyor. Tanrı Protokolü akıllı kontratlar – Bitcoin tarafından canlandırılan başka bir kavram– için bir çözüm olarak planlanmıştı. Szabo bloğunda şöyle yazıyor:

> [Ağ güvenliği teorisyenleri] iki ya da daha fazla parti arasında sanal bilgisayarlar yaratan protokoller geliştirdiler. Çok partili güvenli hesaplama herhan-

[11]Dai, Wei. "Bmoney." Weidai.com. 1998. Erişim tarihi 21 Haziran 2015. http://www. weidai.com/bmoney.txt

[12]Dai, Wei."PipeNet 1.1 and B-money." November 26, 1998. Cypherpunks. Erişim tarihi 21 Haziran 2015. http://marc.info/?l=cypherpunks&m=95279516022393&w=2

gi bir sayıdaki partinin bir hesaplamayı paylaşmasını mümkün hale getiriyor, her biri sadece kendi girdisinden ve hesaplamanın çıktısından çıkarılabilecek şeyi öğreniyor. Bu sanal bilgisayarların heyecan verici bir özelliği var; her partinin girdisi diğer partilerden katı bir şekilde saklanıyor. Program ve çıktılar partiler tarafından paylaşılıyor.

Örneğin, bu sanal bilgisayar üzerinde internette bir hesap çizelgesi çalıştırabiliriz. Bir dizi formülü kararlaştırıp sanal bilgisayarın kurulumunu bu formüllerle yapabiliriz.

Her katılımcının kendi girdi hücreleri olacak ve bunlar diğer katılımcıların bilgisayarlarında boş kalacaklar. Katılımcılar çıktı hücre(lerini) paylaşacaklar. Her katılımcı kendi özel verisini girdi hücrelerine giriyor. Alice diğer katılımcıların girdi hücrelerinden ancak kendi girdileri ve çıktılarından çıkarabileceği kadarını öğrenebilir.

Bu kavramın blokzincirine benzer bir şeye nasıl dönüşebileceğini görebilirsiniz. PGP'nin ve Digicash'in jetonlarının kriptografi kavramını ve B-money'nin enderlik yaratmak için ana işlemcinin bilgisayımsal gücünü kullanma konseptiyle birleştirdiğinizde, Bitcoin'e benzer bir kripto paranın yaklaştığını görmeye başlıyorsunuz.

Nick Szabo'nun bit altın yazısına kadar bu fikirler bir araya getirilmemişti. Ama bazı sorunlar vardı. Daha önce bahsettiğim Sybil saldırısı ele alınmamıştı, (Szabo'nun deyimiyle) 'dövülemez zinciri' her istemcinin (ya da en azından yeterli sayıda istemcinin) kişisel bilgisayarına koyma fikrini henüz kimse düşünememişti. Bunun yerine, 'bir-

kaç farklı zaman damgalı hizmet' tasarladı, belki de Tanrı Protokolü'nde tanımlandığı gibi otomatikleşmiş olacaktı, ayrıca eşler arası sistemden de bahsedilmemişti.

Sonuç olarak, 1990'ların ortasından 2000'lerin ortasına kadar kripto para alanında çok fazla gelişme yaşanmadı. Bu gelişim eksikliği mantıksız değil. O dönemde bu konu üzerinde çalışan yeterince insan yoktu. Digicash ya da E-gold tarafından hayal kırıklığına uğrayan birçok kişi bunu boş bir hayal olarak görüyordu. Bazıları ise, altın ya da gümüş gibi bir emtiayla desteklenmeyen bir para biriminin uzun ömürlü olmayacağını düşünüyordu. Böyle bir girişimin katı devlet direnişiyle karşı karşıya kalmasından korkanlar da vardı.

Bu son nokta konusunda yanılmıyorlardı. E-gold en sonunda Amerikan hükümeti tarafından kapatıldı. Digicash kapatılmadı ama tüketici talebi hiçbir zaman yüksek hedeflerine yetişemedi ve merkezi yanıyla ilgili sorunlar bir konsept olarak birçok kriptocu çekici gelmedi: Yeniden canlandırılsa bile, çok az kişi onunla çalışıyordu.

1 Kasım 2008'de, Bitcoin'le birlikte kripto para/elektronik para hareketi yeniden doğdu. İlk başta şüpheyle karşılandı. Bitcoin topluluğu günümüzde de birleşmiş değil, en başından beri durum böyleydi. Satoshi Nakamoto, her kim ya da her kimseler, her soruya ve eleştiriye sakince yanıt vererek iyi bir iş çıkardı.

Satoshi Nakamoto'nun gerçek kimliği hakkındaki spekülasyonlara çok fazla girmek istemiyorum, çünkü bu konuda *bıkkınlık getirecek kadar* çok yazı yazıldı. Hiçbir sonuca varılmadı ve Nakamoto kimliğini açıklayana kadar bu gizem muhtemelen sürecek. Ve o zaman bile, internetin bazı köşelerinde tartışmanın süreceğini tahmin ediyorum.

Baş şüphelilerin arasında, Szabo'nun bit altın önerisinde bahsedilen çok kullanımlık çalışma ispatını e-para fikrine uygulamakta etkili olan kriptocu Hal Finney var. Kendisi aynı zamanda ilk Bitcoin transferinin alıcısıydı. Daha önce bahsi geçen Wei Dai B-money önerisinden sonra kriptografiyle ilgilenmeye devam ettiği için o da baş şüphelilerden. Bir de, elbette, uzun süredir ortada dolaşan Satoshi Nakamoto'nun, Bitcoin'e çok benzeyen kavramlar hakkında açıkça yazılar yazan Nick Szabo olduğu teorisi var. Ayrıca, gerekli tecrübeye kesinlikle sahip olan ve belki de dünyaya elektronik paranın uygulanabilir olduğunu göstermek isteyen David Chaum var. Adam Back hashcash'i icat etti ve Cypherpunk e-posta listesinde B-money önerisi hakkında yorumda bulunduğu için o da elenemez.

Kaliforniya'da küçük bir evde yaşayan Dorian Prentice Satoshi Nakamoto adında bir adam, bir keresinde *Newsweek* tarafından oldukça tartışmalı bir kapak hikâyesinde gerçek Satoshi Nakamoto olarak "ortaya çıkarıldı."[13] Makale yayınlandığında, Satoshi Nakamoto'nun e-postası tekrar dirildi ve Bitcoin geliştirici e-posta listesine "Dorian Nakamoto olmadığını" yazdı. Ancak e-posta dijital olarak imzalanmamıştı, yani Nakamoto'nun kendisi tarafından değil, muhtemelen Nakamoto'nun e-posta hesabına sahip biri tarafından gönderilmişti.

Bütün popüler adaylar gerçek Satoshi Nakamoto olduklarını inkâr ettiler.

Ana şüpheliler arasında, bana kalırsa en olası aday Szabo ve Dorian Nakamoto'nun olması ise en düşük ihtimal.

[13]Goodman, Leah McGrath. "The Face Behind Bitcoin." Newsweek, March 6, 2014. Erişim tarihi 21 Haziran 2015. http://www.newsweek.com/2014/03/14/face-behind-bit- coin-247957.html

Ama Nakamoto'nun Szabo, Finnery, Dair ve Adam Back'in bir tür kombinasyonu olduğuna inanıyorum. Onların Bitcoin'in yaratıcıları olduğunu söylemiyorum, sadece bu kişilerin Bitcoin'e benzer bir şeye doğru en aktif şekilde çalışan ve bunu yapabilecek araçlara sahip kişiler olduklarını söylüyorum. Bu kişilerden herhangi birinin olmaması da mümkün, ne de olsa, o sırada Cyperpunk e-posta listesine yazan sayısız isimsiz kişi vardı ve birkaçı bu konuyla ilgilendiklerini belirttiler.

Nakamoto'nun kimliği Bitcoin tanıtım yazısının yayınlanması gerçeğinin gölgesinde kaldı. 2008 yazısının üzerinden çok zaman geçmeden, Bitcoin hayata geçirildi.

Nakamoto kodu çoktan hazırlamıştı ve tanıtım yazısını yayınlamadan önce iki senedir üzerinde çalıştığını iddia etti.

3 Ocak 2009'da, Bitcoin'in başlangıç bloğu (blokzincirindeki ilk blok) oluşturuldu. 9 Ocak'ta, kriptografi e-posta listesi aracılığıyla Bitcoin'in v0.1'i yayınlandı. 12 Ocak'ta, Satoshi Nakamoto ve Hal Finney arasındaki ilk transfer gerçekleşti ve Bitcoin devrimi yol almaya başladı.

Bahsetmeye değer birkaç dönüm noktası daha var. 5 Ekim 2009'da, New Liberty Standard web sitesi tarafından o zamanki 'zorluk derecesine' göre madencilik süreciyle bitcoin yaratırken harcanan elektriğin bedeli temel alınarak Bitcoin'in ilk takas oranı belirlendi. (Zorluk derecesi bir bilgisayarın Bitcoin'i çalıştıran hesaplamaları çözerken ne kadar zorlandığını kastediyor; buna madencilikle ilgili bölümde daha fazla değineceğim.) Bir dolar 1,309.03 bitcoin'e (BTC'ye) eşdeğerdi, o nedenle algoritmalarına göre her bitcoin yaklaşık olarak 0.00076 dolara eşitti. Bazı Bitcoin kullanıcıları fiyatın çok yüksek olduğunu söyleyerek karşı çıktılar.

Bitcoin topluluğunda 'pizza günü' olarak sevgiyle isimlendirilen 22 Mayıs 2010'da, somut bir mal karşılığında ilk açık Bitcoin transferi gerçekleşti. BitcoinTalk kullanıcısı laszlo, jercos adlı kullanıcıya 10,000 BTC gönderdi ve jercos kredi kartını kullanarak laszlo'ya 25$ değerinde pizza gönderilmesini sağladı.

Temmuz 2010'da, kullanıcılara çabucak bitcoin almak ve satmak için merkezi bir yer sunan ancak kısa süre sonra kötü bir şekilde anılacak Mt. Gox borsası kuruldu ve sonuç olarak fiyatın 0,06$'a yükselmesine neden oldu. Bir sene geçmeden, 9 Şubat 2011'de, Bitcoin Amerikan dolarıyla eşitlendi ve çok sayıda medya kuruluşunun yeni para birimi hakkında haber yapmalarını sağlayıp yeni bir dalga kullanıcı kazandırdı.

26 Temmuz 2011'de, Berlin'de "sıcak bira, soğuk kadınlar ve yavaşça hazırlanan fast food" vaat eden Room77 adında bir bar Bitcoin kabul etmeye başladı ve günümüzde bu hâlâ devam ediyor. Mart 2013'te, bitcoin'in fiyatı 100 dolara ulaştı ve Bitcoin'in piyasa değeri 1 milyar doları geçti. O noktada, hiç kimse Bitcoin'in geleceğinden emin değildi ama daha fazla hayran yakın zamanda hiçbir yere gitmeyeceğinden emindi.

En sonunda, fiyat bir kez daha fırladı. Ne yazık ki, bu olay kötü şöhretli Mt. Gox'un başarısızlığıyla aynı döneme denk geldi ve bu, fiyatı tekrar aşağı çekti. İlerleyen bölümlerin birinde buna daha fazla değineceğim. O zamandan beri, Bitcoin Mt. Gox döneminde olduğundan daha sabit ama fiyatında istikrarlı bir yükselişin başladığı 2015'in sonlarına doğru aynı hızda düştü. 2015 Ocak ayının başında fiyat kısa bir süreliğine 200 doların altına indi

ama sonra toparlandı ve aylar boyunca 220 ile 250 dolar arasında tutunduktan sonra Kasım 2015'te birdenbire 450 doların üzerine çıktı. Bu kitabı okuduğunuzda, mevcut yükseliş hiç şüphesiz geçmiş olacak, ama kitabı yazdığım sırada herkes bunun bir sonraki dev sıçrayış olup olmadığını merak ediyor.

Ama Bitcoin'in geçmişi bize bir şey söyleyecekse, herhangi bir fiyat seviyesinde işlevini sürdürebileceğidir. İnsanlar Bitcoin'e yatırım yapıyorlar ve PayPal ve Apple Pay'in dokunamadıkları küçük niş ekonomiler bile olsa, gelecekte bunun kullanılabildiğini görecekler. Bu fikir yatırımcıların hoşuna gitmeyecek; Bitcoin'in herkes tarafından her yerde kullanılmasını istiyorlar. Bu olabilir. Bitcoin ya da bir tür blokzinciri teknolojisinin finans dünyasının modernleşmesi için kullanılması neredeyse kaçınılmaz görünüyor, ama aynı zamanda ters yöne de gidebilir ve sadece buna kesinlikle ihtiyacı olan insanlar tarafından kullanılabilir. Bu durumda, fiyat Bitcoin hayranlarının yüksek tahminlerine asla ulaşamaz. Ancak, teknoloji yoluna devam edecek; birine bir dolar değerinde bitcoin göndermek 1000 dolar değerinde bitcoin göndermek kadar kolay.

Her halükarda, teknoloji bu görevi yerine getirebilecek. Çok yönlü olduğunu kanıtladı ve bunun değişeceğini düşünmek için çok az sebep var.

Dördüncü Bölüm:

Bitcoin'i Kim Yönetiyor?

Bitcoin 'kontrolsüz' değil. Hükümet bürokrasileri yerine algoritma tarafından kontrol ediliyor. Yozlaşmamış.

— Andreas Antonopoulos, yazar,
Bitcoin savunucusu ve güvenlik uzmanı

Bitcoin hakkında çok fazla yanlış fikir var. Özellikle de ilk başta, alışılmadık orijini ve varlığı nedeniyle medya kuruluşları Bitcoin hakkında doğru bir biçimde haber yapmakta zorlandılar. Daha önceki bölümlerde ele aldığım gibi, geçmişte bir internet para birimi oluşturmak için birkaç girişim oldu. Bu tekrarların merkezi bir güç tarafından çıkarılmak gibi ölümcül bir kusuru vardı. Bitcoin medyanın ilgisini ilk çektiğinde ve sonraki yıllar süresince, haber kuruluşları hatalı bir şekilde bir 'Bitcoin yönetim kurulu başkanı'ndan bahsettiler. Örneğin, Bitcoin borsası First Meta'nın yönetim kurulu başkanı Autumn Radtke intihar ettiğinde, *New York Daily News* Bitcoin'in yönetim kurulu

başkanının intihar ettiği haberini duyurdu.[1] Böyle bir şey mümkün değil, çünkü Bitcoin'in bir yönetim kurulu başkanı yok.

Bu bölümün başlığındaki sorunun en net yanıtı Bitcoin'i kimsenin "yönetmediğidir." Bitcoin'in varlığı herhangi bir organizasyona bağlı değil ve 'başında' olan biri yok. Satoshi Nakamoto 2008'de Bitcoin'i faaliyete geçirdiğinde, diğer hiçbir organizmaya benzemeyen, yaşayan, büyüyen ve gelişen bağımsız bir varlık doğurmuş oldu. İyi bir ebeveyn gibi Nakamoto yanından ayrılmayıp Bitcoin'e rehberlik etti ama ortadan kaybolduğunda, Bitcoin geride kaldı. BitcoinTalk forumlarındaki (bu kitabı yazdığım an itibariyle) son yazısıyla Nakamoto baş geliştirici statüsünü Gavin Andresen'e transfer etti.

Bu unvan Andresen'in her şeyin başında olduğu anlamına gelmiyor. Bitcoin'e kimin katıldığını, birinin kaç bitcoin'i olduğunu ya da kimin kime ne gönderdiğini hiç kimse kontrol edemez. Bitcoin'i doğrudan etkileyebilen tek bir şey var: kod. Andresen'e –ve daha sonra yerini alan Wladimir van der Laan'a– kod üzerinde kontrol verildi ama yaptığı değişiklikler topluluğun büyük bir kesimi tarafından benimsenmek zorunda değil ve benimsenmezlerse, muhtemelen unutulurlar.

Farklı rolleri sebebiyle Bitcoin endüstrisinde etkili birkaç grup var. Para birimini kullananlar (sıradan Bitcoin kullanıcıları), ağın işlemesini sağlayanlar (madenciler),

[1]Moran, Lee. "Bitcoin CEO Researched Suicide before Taking Her Own Life: Coroner." NY Daily News. September 16, 2014. Erişim tarihi 21 Haziran 2015.

http://www.nyda- ilynews.com/news/world/bitcoin-ceo-researched-suicide-life-coroner-article-1.1941010

Bitcoin'le ilgili hizmet sunanlar (Bitcoin hizmetleri sunan kuruluşlar ve web siteleri), Bitcoin'in kodunu devam ettirenler (geliştiriciler) ve kodu devam ettirmeleri için geliştiricilere para ödeyen insanlar, hepsinin Bitcoin'in gidişatı üzerinde etkisi var.

"Bitcoin'i kim yönetiyor?" sorusuna Bitcoin savunucularının verdiği en popüler yanıt 'topluluk' olur. Topluluğun büyük bir etkisi var. Bu terim genellikle, harcama ya da yatırım amaçlı Bitcoin kullanan insanlardan bahsederken kullanılıyor. Başka bir zincir ya da paraya geçerlerse, endüstrinin geri kalanı onları takip eder. Ancak, elbette topluluk görüşleri konusunda birleşmiş değil, o nedenle, rağbet görmeyen bir değişikliği önlemek dışında, herhangi bir gerçek yönlendirme ya da değişikliğin bu alandan gelmesi pek olası değil.

Bu arada, işlerin yürümesini sağlayan insan grubu madenciler. Madenciler blokzincirindeki işlemleri doğrulamazlarsa, her şey aniden durur. Bu grup Bitcoin topluluğundan biraz daha birleşmiş durumda, çünkü bütün üyeler aynı şeyi istiyorlar: Bitcoin madenciliğinin mümkün olduğunca kârlı olmasını. Ama genel topluluk gibi, madenciler de dünyanın dört bir yanına dağılmış durumdalar ve ağın hash gücünün büyük bir bölümü Çin'den çıkıyor. Belirli sorunlar ya da değişiklikler hakkında ne düşündüklerini anlamak zor. Yine de, Bitcoin'de büyük bir potansiyel güç yapısını temsil ediyorlar. Anahtarlar onların elinde değil, ama anahtarları onlardan başka çevirebilecek kimse yok.

Her endüstride olduğu gibi, şirketler güçlerine bağlı olarak nüfuz sahibi olabilirler. Coinbase, Bitstamp, Circle

ya da Blockchain.info gibi şirketlerin devasa kullanıcı temelleri var ve onlar nereye giderse, endüstri de oraya gitmeye meyilli. Ama Bitcoin'i 'yönettiklerini' ya da ondan sorumlu olduklarını söylemek, Apple ya da Samsung'un cep telefonu endüstrisinden sorumlu olduklarını söylemek gibi olur. Trendleri belirliyorlar ama standartları zorla kabul ettirmiyorlar.

Öyleyse, geriye Bitcoin ekosistemindeki en etkili ve güçlü iki grup kaldı: geliştiriciler ve geliştiricilere para ödeyen gruplar. Gavin Andresen ve Wladimir van der Laan, Bitcoin'in çekirdek geliştiricileri arasında en öne çıkanlar. Bitcoin dünyasındaki en etkili kişiler oldukları söylenebilir, ama Bitcoin onlar olmadan da devam edebilir.

Bütün açık kaynak projelerinde olduğu gibi, Bitcoin kodu en nihayetinde tek bir kişi tarafından kontrol ediliyor. Andresen 2014'ün başında van der Laan'dan GitHub sayfasının anahtarını aldığından beri bu konumda.[2] (GitHub işbirlikçi açık kaynak projeleri için bir forum.) Ancak bu onun bütün kontrole sahip olduğu anlamına gelmiyor, ne de olsa herkes her an –çatallanma denen hareket– kodu yayıp kopyalar ve Bitcoin madencileri ile kullanıcılarının bu yeni versiyona geçmelerini sağlayabilirse, kabul gören o olur. Van der Laan Bitcoin'in çekirdek koduna (Bitcoin'in işlevini sağlayan ve her Bitcoin cüzdanının bir şekilde temel aldığı ve uyumlu olduğu) yapılan değişikliklerin bütün kontrolünü elinde bulundursa da, topluluğun bu değişiklikleri desteklemesine bağlı.

[2] Shubber, Kadhim. "Gavin Andresen Steps Down as Bitcoin's Lead Developer." CoinDesk. April 8, 2014. Erişim tarihi 21 Haziran 2015. http://www.coindesk.com/ gavin-andresen-steps-bitcoins-lead-developer/

Çekirdek geliştiricilerin, en azından tam zamanlı çalışanların, ücretsiz çalışmadıkları göz önünde bulundurulmalıdır. Ücretleri ödenmelidir ve ücretlerini kimin ödeyeceği sorusuna yanıt vermek her zaman kolay değildir. Teorik olarak, ücretleri Bitcoin kullanıcıları tarafından ödenmelidir, ama çekirdek geliştiricilere yapılan bağışlar hiç etkileyici değil ve bunun yerine geliştiriciler farklı şekillerde destekleniyorlar.

Andresen ve diğer çekirdek geliştiricilerin maaşları daha önce, kendisini Bitcoin'in benimsenmesi, kabul görmesi ve gelişiminin sürmesine adayan ticari bir grup olan Bitcoin Vakfı tarafından ödeniyordu.

2013'te ve 2014 başlarındaki hareketli günlerde, Bitcoin Vakfı kendini para içinde yüzerken buldu. Daha önce yapılan küçük bağışlar Bitcoin'in değerindeki artış sayesinde fazlasıyla takdir gördü.

Ancak o noktada, Bitcoin Vakfı skandallarla çalkalanıyordu. 2013'ün sonunda Mt. Gox fiyaskosu son sürat devam ediyordu ve eski Bitcoin Vakfı yönetim kurulu başkanı Mark Karpelès hâlâ vakfın yöntem kurulundaydı. O sıralar raporlar, şirketi yanıp kül olurken Karpelès'in umursamaz bir tavrı olduğuna işaret ediyordu ve vakıftan ayrılması için teşvik edilmesi gerekti.[3] Savaşa giren ve neredeyse evrensel olarak nefret edilen yönetim kurulu başkanı geri çekildikten kısa bir süre sonra, Bitcoin Vakfı yönetim kurulu üyesi ve BitInstant'ın yönetim kurulu başkanı Charlie Shrem tutuklandı. Karaborsa Silk Road'un kullanıcılarının

[3]McMillan, Robert. "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster." Wired.com. March 3, 2014. Erişim tarihi 21 Haziran 2015. http://www.wired.com/2014/03/ bitcoin-exchange/

Bitcoin kullanarak paralarını aklamaya yardım etmek için şirketini kullanmakla suçlanıyordu. Shrem en sonunda daha küçük bir suçu kabul etti ve iki sene hapse mahkûm edildi.[4]

2014'ün ortalarında, vakfı gerçekten destekleyen birini bulmak zordu. Skandallar vakfın imajına onarılamaz bir hasar vermişti ve Bitcoin çekirdek kodu gelişiminin merkezileştirilmesine dair endişeler giderek artıyordu. Çekirdek kodu geliştirme süreci, ağırlıklı olarak vakıf tarafından finanse ediliyordu ve topluluktakilerin bazıları bu düzenin suiistimale imkân sağlamasından endişeleniyorlardı.

Duruma karşılık verme çabalarından biri, risk sermayedarı, ilk Bitcoin benimseyenlerden, kripto-sever olduğu iddia edilebilecek Olivier Janssens'ten geldi. Bitcoin Vakfı'nın Bitcoin çekirdek kodu gelişimi üzerinde potansiyel kontrol edinmesinden endişelendiği için çekirdek kodu gelişimi finanse etmenin alternatif bir yolunu bulan kişiye 40,000 dolar ödül teklif etti; diğer ödüllerde bir de 60,000 dolar vardı. Bu teşvik, eski Bitcoin geliştiricisi Mike Hearn tarafından geliştirilen Lighthouse'un yaratılışıyla sonuçlandı.[5] İnsanların Bitcoin platformundaki projelere bağış yapmalarına imkân tanıyacaktı, gelişimcilerin düzeltmeleri gereken sorunu ya da eklemeleri gereken özelliği tarif

[4] Cook, James. "'Bitcoin Millionaire' Charlie Shrem Sentenced To 2 Years In Prison." Business Insider. December 22, 2014. Erişim tarihi 21 Haziran 2015. http://www.businessin- sider.com/bitcoin-millionaire-charlie-shrem-sentenced-to-2-years-in-prison-2014-12

[5] Higgins, Stan. "Mike Hearn Wins $40k Bounty for Bitcoin Core Crowdfunding Platform." CoinDesk RSS. July 02, 2014. Erişim tarihi 21 Haziran 2015. http://www.coindesk.com/mike-hearn-wins-40000-bounty-bitcoin-core-crowdfunding/

ettikleri bir yazı yazmaları ve Bitcoin kullanıcıları ya da şirketlerin bu projeleri finanse etmeleri fikrine dayanıyordu.

Lighthouse çekirdek kodu gelişimi finanse eden güvenilir bir yöntem olarak hiçbir zaman Bitcoin Vakfı'nın yerini almadı. Aksine, ağırlıklı olarak kriptoyla ilgili projeleri finanse etmek için kullanıldı. Yine de, yaratılışı Bitcoin Vakfi'nın çekirdek kodu gelişimi üzerinde ne kadar kontrol sahibi olması gerektiği konusunda tartışmaları başlattı.

Gavin Andresen Bitcoin Vakfi'nın Bitcoin'in çekirdek kodu gelişimi üzerinde kontrol sahibi olmadığını ileri sürdü.[6] Andresen'e göre, Bitcoin'in çekirdek kodunun ne içermesi gerektiği hakkındaki kararlarını etkilemeye kalkışmamıştı. Bu güvenceye rağmen, topluluğun büyük bir bölümü ikna olmadı. Mesele Andresen'in sözlerine inanmaları değildi; asıl mesele çoktan gerçekleşen gerçek kötüye kullanmadan ziyade potansiyel kötüye kullanma olasılığıydı.

Bir ticaret kuruluşu olan Bitcoin Vakfı, kurumsal ortaklarının onu finanse etmesine bağlıydı. Bu ortakların muhtemelen Bitcoin'in kodunun nasıl geliştiğini görmeyi istediklerine dair fikirleri vardı.

Andresen dürüst görünüyordu ve Bitcoin Vakfı'nın yönetim kurulu çekirdek kodu bağımsızlığının önemini anlamış görünüyorlardı, peki ama gelecekteki baş geliştiriciler ne olacaktı? Onlar da Andresen kadar dürüst olacaklar

[6]Higgins, Stan. "Gavin Andresen: Bitcoin Core Development." CoinDesk RSS. November 20, 2014. Erişim tarihi 21 Haziran 2015.
http://www.coindesk.com/gavin-andresen-bitcoin-foundation-pivot-centralize-development/

mıydı? Ya Bitcoin Vakfı'nın gelecekteki yönetim kurulu üyeleri? Sonsuza kadar hep böyle iyi niyetli olacak ve her şeyden çok Bitcoin'in sağlığı için endişelenecekler miydi?

Skandallar nedeniyle kullanıcı bağışları kesilmişken ve gelişim üzerine etkileri tartışılırken, Bitcoin Vakfı kurumsal bağışlara giderek daha çok bağlı olmaya başladı. Bitcoin'in fiyatı Mt. Gox skandalı ve onu izleyen panik nedeniyle hızla düştüğü için vakfın rezervi de azalmaya başladı. İronik bir şekilde, Bitcoin mevcut doruk noktasına –29 Kasım 2013'te gördüğü 1.124,76 $– Mt. Gox borsası çökmeden kısa bir süre önce ulaşmıştı. İnsanlar dört basamaklı bitcoin fiyatına çok sevinseler de, olacakların korkusu sevinçlerine gölge düşürüyordu. Bitcoin endüstrisi Mt. Gox'a benzer bir şeyi hiç tecrübe etmemişti. Merkezsiz bir sistemin en büyük merkezi noktası dağılırsa ne olacaktı?

Toplulukta bu kadar belirsizlik varken, Bitcoin Vakfı, Bitcoin'i terk ediyormuş gibi görünemez, yani rezervlerini satamazdı. Eğer vakfın bitcoin'lerini paraya dönüştürdüğü haberi yapılsaydı, endüstride büyük paniğe neden olurdu.

Ayrıca, ana akım medya Bitcoin'in başında kimin olduğuna dair bu kadar kafa karışıklığı yaşarken, Bitcoin Vakfı isimli bir organizasyon para birimini terk ediyormuş gibi görünürse, peşinden gelecek negatif başlıkları tahmin etmek hiç zor değildi.

Belki de, vakfın iddialarını biraz sınırlayıp varlıklarının daha fazlasını paraya dönüştürmesi gerekirdi, ama bu kararı almak hiç kolay değildi. Birçok gözlemci Bitcoin'in fiyatının, daha önceki çıkışlardan sonra olduğu gibi, düşmeye mahkûm olduğunu söyleyebilirdi, ama aynı zamanda bunun Bitcoin'in 'engeli aşacağı' ve genel kabul göreceği

an olduğuna dair bir his vardı. Bu safça bir umuttu –vakıf muhtemelen farkındaydı– ama bu olasılığa şüphe düşürmeyen bir şey yapmak hem vakıf hem de Bitcoin için kötü bir itibar çalışması olurdu.

2014 sonbaharın başında, vakıftan duman çıkıyordu. Bağışların çoğu kesilmişti. Vakfın halka açık bağış adresine Ekim 2014'te sadece yaklaşık 0.3BTC bağış yapılmıştı[7] ama bu rakam kurumsal bağışları ve üyelik aidatlarını yansıtmıyordu.

Bitcoin'in fiyatı 2014 kışı sonunda çıktığı noktadan çok aşağıdaydı ve vakıf hakkında hevesli insanlar bulmak zordu.

Bitcoin Vakfı bu noktada reforma başladı. Çekirdek kodu gelişiminin en önemli görev olduğuna karar verdi. O sırada, topluluğun daralan odak noktasının arkasında durması umut ediliyordu ve Bitcoin'in çekirdek kodunu korumak herkesin destekleyebileceği bir sebepti.

Yine de, topluluğun büyük bir bölümü bunu desteklemedi ve bağışlar önemli ölçüde, en azından vakfın maddi endişelerini çözecek kadar artmadı.

Bu sırada, Bitcoin Vakfı'nın çekirdek kodu gelişimi üzerindeki potansiyel kontrolüne dair endişeler artmaya devam ediyordu.

Vakıf Karpelès ve Shrem'in boşalan koltuklarını doldurmak için bir seçim düzenlediğinde, topluluk hoşnutsuzluğunu dile getirme fırsatı buldu. Adayların arasında, vakfın finanse edilme biçimine alternatif bir yöntem geliştirmek için 100,000 dolarını ortaya koyan Olivier Janssens

[7]https://blockchain.info/address/1BTCorgHwCg6u2YSAWKgS17qUad6kHmtQW

de vardı. Sadece Bitcoin Vakfi'nın paralı üyeleri oy verebiliyordu ama onların fikirleri Reddit ve Bitcoin Talk gibi halka açık forumlarda dile getirilenleri yansıtıyordu. Fazlasıyla tartışmaya açık bir seçimden sonra, Olivier Janssens ve –vakfın çekirdek kodu gelişiminin finanse edilmesine karşı bir başka aday– Jim Harper açık iki yer için seçildiler. Çekirdek kodu gelişim geçişinin yanı sıra, iki aday vakfın mali durumuna şeffaflık getireceklerine söz verdiler.[8]

Seçim vakıf üyelerinin gelişimin kesesinin iplerini elinde tutan vakfın yönetim kurulundan memnun olmadıklarının açık bir işaretiydi. Seçimden birkaç hafta sonrasına kadar açıkça hiçbir şey olmadı. Sonra, Janssens bombayı patlattı. Reddit ve Bitcoin Vakfi forumlarında yazan Janssens, vakfın tamamen parasız olduğunu belirtti. Ayrıca, onunla yaptığım röportajda bana Andresen ve diğer çekirdek geliştiricilerin maaş çeklerinin kesildiğini açıkladı.[9]

Vakıf hasar kontrolü moduna girdi, çoktan silinen bir yazıda, Janssens'in sorunu ele almak için bir plan oluşturduktan bir iki hafta sonra açıkladığı bilginin aynısını yayınladılar. Vakıf, ayrıca, sorunun Janssens'in iddia ettiği kadar kötü olmadığında ısrarcıydı.[10] Bu açıklamalar doğru olabilir de, olmayabilir de, ama afişe olan birinin *her şeyi açıklamak üzere* olduğunu iddia etmesi kolaydır.

---

[8]Englund, Jinyoung Lee. "Election Runoff." The Bitcoin Foundation. February 20, 2015. Erişim tarihi 21 Haziran 2015. http://blog.bitcoinfoundation.org/election-runoff/

[9]Janssens, Olivier. "The Truth about the Bitcoin Foundation." Reddit. 4 Nisan 2015. R/Bitcoin. Erişim tarihi 21 Haziran 2015. http://www.reddit.com/r/Bitcoin/comments/31c6jh/ the_truth_about_the_bitcoin_foundation/

[10] "The Facts About the Bitcoin Foundation." The Bitcoin Foundation. 7 Nisan 2015. Erişim tarihi 21 Haziran 2015.

https://web.archive.org/web/20150407230759/https://blog.bit- coinfoundation.org/the-facts-about-the-bitcoin-foundation/. (Silindi, sadece archive.org üzerinden ulaşılabilir)

Janssens'in yazısından sonra bir an önce ele alınması gereken iki sorun vardı. Birincisi ve en acili, çekirdek kodu gelişimine mali desteğe nasıl devam edileceğiydi. Janssens başka bir çözüm bulunana kadar gelişimi kendisi finanse etmeyi teklif etti.[11] İkinci sorun Bitcoin Vakfı varlığını sürdürecekse, yoluna nasıl devam edeceğiydi.

İkinci soruna tamamen çözüm getirilemedi. Bitcoin Vakfı varlığını hâlâ sürdürüyor ve artık gelişimden ziyade daha çok benimsenmeye odaklandı, ama nasıl finanse edildiği belirli değil ve finansal olarak rahat olup olmadığı bilinmiyor. Vakfın gönüllü kapasiteyle çalışan yeni yönetici müdürü, Bruce Fenton, reform sözü verdi.[12]

Büyük sorun şimdilik çözülmüş görünüyor ama bazı insanlar hâlâ endişeliler. Çekirdek geliştiriciler Janssens'in çekirdek kodu gelişimini finanse etme teklifine hiçbir zaman açıkça yanıt vermediler, bunun bir sebebi başka bir çözümün oldukça hızla ortaya çıkmasıydı. The MIT (Massachusetts Teknoloji Enstitüsü) Digital Currency Initiative (Dijital Para Girişimi) çekirdek kodu gelişimini finanse edeceğini duyurdu ve o zamandan beri bunu kısmen yapıyor, geri kalanı ise topluluk ve farklı şirketlerden geliyor.[13]

Birçok kişi bir öncekine kıyasla durumun geliştiği konusunda hemfikir. Bitcoin'in çekirdek kodunun kurumsal

---

[11]DeMartino, Ian M. "First Interview With Olivier Janssens After 'The Truth About BTC Foundation' Post." Mining Pool. 6 Nisan 2015. Erişim tarihi 21 Haziran 2015. http://www.miningpool.co.uk/first-interview-with-olivier-janssens-after-the-truth-about-btc-foundation-post/.

[12]Rizzo, Pete. "New Bitcoin Foundation Director Bruce Fenton Pledges Fiscal Reform." CoinDesk RSS. 13 Nisan 2015. Erişim tarihi 21 Haziran 2015. http://www.coindesk.com/bruce-fenton-bitcoin-foundation-executive-director/

[13]Prisco, Giulio. "Gavin Andresen and Other Core Developers Join MIT's Digital Currency Initiative." Bitcoin Magazine. 22 Nisan 2015. Erişim tarihi 21 Haziran 2015. https://bitcoinmagazine.com/20132/gavin-andresen-core-developers-join-mits-digital-currency-initiative/

ticari bir grup tarafından sürdürülmesi ve güncellenmesine kıyasla akademik bir enstitü tarafından sürdürülmesi ve güncellenmesinin bariz avantajları var. Akademik bir enstitünün dış kaynaklardan etkilenerek geliştiricileri Bitcoin'deki büyük kuruluşların tercihlerine göre kod yazmaya zorlaması daha az olası görünüyor.

Ancak, yine de endişeleri olan birçok insan var. Gelişim fonu hâlâ merkezi. Öncekine kıyasla daha iyi bir yerde merkezileştirilmiş olabilir ama yine de merkezi. Gelecekteki MIT proje yöneticilerinin ve onların gelecekteki geliştiriciler üzerindeki etkileri hakkındaki endişeler hâlâ geçerliliklerini koruyor. Şu anda Bitcoin'le ilgili insanlar para biriminin hiç şüphesiz ilk benimseyenleri olarak görülecekler ve insan doğası kendinden önce gelenleri üstün görmeye meyillidir.

Bitcoin'i kontrol eden mekanizmalar henüz değiştirilemez değil. Çekirdek geliştiriciler arasında ne yapılması ve işin başında kimin olması gerektiğine dair fikir birliği bile yok. Bu kitabı yazdığım sırada, toplulukta Bitcoin'in gelecekte nasıl ölçeklendirileceği üzerine büyük bir tartışma sürüyor.

Bu tartışma, çekirdek geliştiricilerin arasında bir ayrılığa yol açmaya ve Bitcoin'i çatallanmaya sebep olmakla tehdit etti. Bir tarafta, madencilik yapabilmek için daha büyük blokları işlemek ve daha büyük blokzincirlerini yedeklemek zorunda olan madenciler vardı. Diğer tarafta, Bitcoin işlemleri için giderek artan talepleri karşılayabilecek daha büyük bloklara ihtiyaçları olduğunu öne süren ödeme işlemcileri vardı. Bu tartışmanın sonucu Bitcoin politikasında gücün gerçekten nerede olduğunu gösteriyor.

Tartışma çıkmasının nedeni, ağın bir seferde kaldırabi-

leceği işlem sayısının bir sınırının olması. Her blok, boyutu şu anda 750KB ile 1MB arasında ve ancak belirli sayıda işlem saklayabilir. Bunun hiçbir zaman kesin sınır olması gerekmiyordu, ama Satoshi Nakamoto bir dizi anlamsız işlemle ağa hücum etmeye çalışan kötü niyetli oyuncuların zorlanmaları için onu bu şekilde inşa etti. İlk başta sorun oluşturmadı, çünkü Bitcoin daha büyük ya da hızlı blokları gerektirecek kadar popüler değildi. Yaklaşık 10 dakikalık sıklıkla 1MB, o sırada ağın üstesinden gelmesi gereken hacim için fazlasıyla yeterliydi.

Günümüzde Bitcoin çok daha popüler ve blok boyut sınırı bir sorun olmaya başlıyor. Birçok blok henüz dolmamış olsa da, bazıları doldu ve işlemler aniden yükseldiğinde, bazı kullanıcılar anormal derecede uzun işlem sürelerinden şikâyet ettiler. Bitcoin Visa ya da Mastercard seviyesine ulaşmak istiyorsa, şu anda olduğundan çok daha fazla işlemi kaldırması gerekecek. İşlemler teklemeye başlarsa, kullanıcılar panikleyebilir ve gönderilmeden önce aynı bitcoin'leri harcamaya kalkabilirler, bu da bekleyen işlemlere yük olmanın yanı sıra potansiyel olarak madencilik çatışmalarına sebep olup işleri daha çok yavaşlatabilir.

Tartışma devam ediyor. Büyük ihtimalle, bir tür uzlaşma göreceğiz. Ama açıkçası, Bitcoin'de olması gerekenlere karar verenler tam olarak yerleşmiş değiller ve mevcut durum işin içinde olanlar için bile kafa karıştırıcı. Ve milyonlarca dolar söz konusu olduğunda, "Bitcoin'i kim kontrol ediyor?" sorusunun yanıtı çok önemli. Bitcoin hayranları için "Topluluk karar veriyor," demek çok kolay, ama aslında ne tür değişiklikler yapılacağına topluluk karar vermiyor. Blok boyutu tartışmasında ne kadar söz sahibi olabildiler?

Bitcoin kullanıcıları teorik olarak yeni bir çatala atlayabilirler ve teknik olarak herkes kendininkini yapabilir, ama bunu yakın zamanda görmemiz zor. Bitcoin'in çekirdek kodu topluluğa minnettar olan bir grup geliştirici tarafından kodlanıyor, ama topluluk onlara emir yağdırmıyor. Eklenecek bir sonraki özellikler ya da en kritik hata düzeltmesinin hangisi olduğu üzerinde kimse söz sahibi değil. Evet, topluluk ağ üzerindeki katılımıyla oy veriyor ama kontrol burada son buluyor. Mevcut zincirin nasıl değiştiği ve bu değişikliklere kimin karar verdiği hâlâ belirsiz. En nihayetinde, son kararı baş geliştirici veriyor, ama ne kadar kontrole sahip olmalılar ve topluluklarını ne kadar dinlemeliler? Andresen diğer açık kaynak projelerindeki baş geliştiricilerden farksız olması ve idareyi ele alması gerektiğini iddia ediyor. Van der Laan onunla aynı görüşte değil. Ancak, uzlaştığımız şeyin sonuçları Bitcoin'de bu ikilinin katılımından daha uzun ömürlü olabilir.

Henüz Bitcoin'e atlamamış ve bu kitabı okuduktan sonra girişmek isteyecek olsanız da, gelecekteki insanlar tarafından onu ilk benimseyenlerden biri olarak görüleceksiniz. Eğer Bitcoin gerçekten yarının para birimiyse, o halde fazlasıyla büyümesi gerek. Satoshi'nin tanıtım yazısını yayınlamasından sadece sekiz sene sonra, 2015 ya da 2016'da onu benimseyenler, gelişmekte olan bir teknolojiden yararlanma fırsatına balıklama atlayarak riske giren cesur insanlar olarak görülecekler.

Amerikalılar uzun zamandır kurucularını idealize ediyorlar ve o on sekizinci yüzyıl adamlarının anlamalarının mümkün olmayacağı sorunlarda hâlâ onların rehberliğine başvuruyorlar. Aynı şekilde, Bitcoin topluluğundaki insan-

lar da Satoshi Nakamoto'yu idealize ediyorlar ve herhangi bir tartışmanın ondan yapılan bir alıntıyla bittiğini ya da bir Bitcoin alternatifinin Nakamoto'nun icadının daha saf bir hali olduğunun iddia edildiğini sıklıkla görebiliriz.

Gelecekte, sadece Nakamoto olmayacak. Çekirdek geliştiriciler ve günümüz Bitcoin topluluğunun diğer etkili üyelerinin düşünceleri hakikat olarak alıntılanacak. Bu talihsiz bir durum –çünkü onlar da herkes gibi yanılabilir– ama kaçınılmaz görünüyor. Bir topluluk olarak yapabileceğimiz en iyi şey geleceğin Bitcoincilerine örnek olmak ama neredeyse herkes bunun olası sonuçları konusunda çelişiyor.

Eğer çekirdek kodu gelişiminin merkezi olarak finanse edilmesini sorun olarak görmeyerek emsal teşkil edersek, geleceğin Bitcoin kullanıcıları buna dikkat çekerek merkeziliğin bir sorun olmayacağını söylemeye devam ederler. Yirmi ya da otuz sene sonra, biri fonu geri çekmekle tehdit ederek Bitcoin çekirdek kodu gelişim ekibi üzerinde etkili olmaya çalışabilir. O zaman nasıl bir yol izleyeceğiz? İnsanlar, gelişim fonu her zaman merkezi oldu diyecekler. Fonlamayı nüfuza dönüştürmek pek de abartı olmaz. Kurallar, ancak biri bu yönde uğraşırsa, hiç kimse fark etmeden zamanla tersine çevrilebilir. Bu tür işler yapan insanlar genellikle art niyetlilerdir.

Şimdi oluşturacağımız örneğin gelecekte kullanılacağı şüphesiz. Aynı zamanda, bu sistemi kendi çıkarlarına göre çevirmeye çalışacak insanlar da olacak. Mevcut düzenleme seçmeli olabilir, ama bu konuda hararetli bir tartışma olmadı. Janssens ve Harper'ın seçilmeleri –Bitcoin Vakfı'nın üyesi olmak için para ödeyenlere (oy verebilen insanlara)

bile– topluluğun çekirdek gelişimin kesesinin iplerini onların tutmalarını istemediğini kanıtladı.

Topluluk MIT Digital Currency Initiative fon gelişimi hakkında ne düşünüyor? Bilmiyorum, onlara soran biri olduğunu da sanmıyorum.

Beşinci Bölüm:
Bitcoin'e Değerini Veren Ne?

Ekonomistler ve gazeteciler sık sık şu soruya takılıp kalıyorlar: Bitcoin'in neden değeri var? Yanıtı çok kolay. Çünkü faydalı ve ender bulunan bir şey.

— Eric Voorhees, Bitcoin şirketi Coinapult'un kurucu ortağı

Birçok insan Bitcoin'e değerini veren şeyin ne olduğunu merak ediyor. Birçok kişinin sorabileceği ilk soru Bitcoin'in herhangi bir şey tarafından desteklenip desteklenmediği. Yanıt: Bitcoin'i kodu ve yararlılığı, yani yapabilecekleri destekliyor. Eğer Bitcoin faydalı olmayı bırakırsa, değerini kaybeder.

İnsanlar sık sık Bitcoin'in değerinin insanların ona biçtiği değerle ilgili olduğunu iddia ediyorlar. Bu her şey için söylenebilir, yine de tam olarak doğru değil. Bir şişe suya bir dolar ya da o su şişesinin değerini nasıl algıladığınıza bağlı olarak iki dolar ödemeye razı olabilirsiniz. O neden-

le, evet, bir şeye biçtiğimiz değerin onun değeri üzerinde doğrudan etkisi vardır. Ama su şirketi piyasaya filtrelenmemiş ve kısmen çamurla dolu su sürmeye başlarsa, ürün kalitesini kaybettiği, sağlığa faydası olmadığı için insanlar aynı miktarda para ödemeye istekli olmazlar.

Bitcoin'in kullanılabilirliği diğer her şeyin üzerine kurulduğu bir temeldir. Bu kullanılabilirlik olmazsa, her şeyi çöker. Spekülatif gün içi işlemler sadece kuru gürültü. Az bulunur olması çok önemli bir etken ama en nihayetinde her şey kullanılabilirliğe dayanıyor. Bitcoin'in yaratılacak para sayısı üzerinde katı bir sınırı var. Sadece 21 milyon bitcoin var olacak. Madenciler yeni bir bloğu çözüp girdikleri zahmetin karşılığında yeni para kombinasyonları ve madenci ücretiyle ödüllendirildiklerinde yeni bitcoin'ler yaratılıyor. (Bilgisayarınız –bu işe adanan madenci yazılımı– karmaşık bitcoin gönderen hesapların bitcoin'leri olduğunu ve işlemlerini dijital olarak imzaladıklarını doğrulayan matematiksel problemleri çözümlediğinde 'yeni bir blok çözüyorsunuz.' Her blok şu anda 750KB ila 1MB'lık işlem değerine sahip.) 21 milyon bitcoin yaratılana kadar yaklaşık her dört senede bir, blok başına yaratılan yeni coin sayısının yarısı azalacak; o noktada, madenciler tamamen madencilik ücretleriyle geçinmek zorunda kalacaklar. Bunun önümüzdeki yüzyılda olması öngörülüyor. Bitcoin'in parametrelerini önceden bilmek Bitcoin'i spekülatif bir yatırım ve para birimi olarak daha faydalı kılıyor.

Altın standardının taraftarları ikna edici konuşmalarını yaparken, genellikle altının kullanılabilirliğine işaret ederler. Bir dolar sadece bir kâğıt parçasıdır. Altının bir emtia, elektronik eşyalar için değerli bir mineral ve –binlerce se-

nedir olduğu gibi– mücevherler için cazip bir madde olarak gerçek bir değeri olduğunu öne sürerler. Ama bir emtianın desteklediği para birimi bile onu dağıtan zümrenin sözüne bağlıdır. Altın ve diğer değerli maddelerin her zaman belirli bir değeri olacak olsa da, bütün devlet daireleri kapanırsa, üzerinde değerinin bir ons altın olduğu yazan bir kâğıt parçası sadece bir kâğıt parçasıdır. Birleşik Devletler'de yaşıyorsanız, hükümetin bir gecede ortadan kaybolması fikri pek gerçekçi olmayabilir, ama üçüncü dünya ülkelerinin vatandaşları, ya da Yunanistan gibi ekonomik sorunları olan geleneksel gelişmiş ülkelerinin vatandaşları için bile bu korku daha somuttur.

Bitcoin değerini onu düzenleyen bir zümre olmadan başarabileceklerinden alır. Bu, fiyatını nereden aldığını söylemekten farklı bir şey. Bitcoin'in fiyatını birçok şey etkiliyor: benimsenme, spekülasyon ve değer, hepsi bu denklemin büyük parçalarını oluşturuyorlar. Ama asıl değerini kullanılabilirliğinden alıyor. Spekülasyonun Bitcoin'in fiyatını etkilemediği teorik bir dünyada, bir bitcoin'in fiyatı değeri ve nadir bulunmasından dolayı olması gereken noktada olur ve bu değer tamamen kullanılabilirliğinden oluşur. Ayrıca, bu değer olmadan, her şey kâğıttan bir ev gibi yıkılır.

O kullanılabilirlik hâlâ geliştiriliyor. Bitcoin'in şimdiden birçok kullanım alanı var ve daha sonraki bir bölümde onlara değineceğim, ama en belirgin olanları kısaca belirtmeme izin verin. Öncelikle, Bitcoin oldukça küçük bir tutar karşılığında –genellikle 0,02 dolar– dünyanın herhangi bir yerine gönderilmesi para havalesi için büyük fırsatlar açıyor.

Ayrıca, Bitcoin ve blokzincirini temel alan diğer teknolojiler programlanabilirler ve bu onlara henüz akıl edilmemiş kullanım alanları veriyor. Örneğin, insanlar tahviller, hisse senetleri, değerli madenler ve hatta dünyanın dört bir yanındaki diğer para birimlerine yatırım yapabiliyorlar, üstelik ücretler ve bu alanlara geleneksel yöntemlerle yatırım yapılırken alınan yüksek giriş masrafları olmadan.

Ekonomik açıdan paranoyaklar için, Bitcoin aynı zamanda idari kuruluşların doğrudan etkisinin olmadığı bir tasarruf aracı sunmanın yanı sıra utanç verici ya da yasadışı hizmetler için anonimlik imkânı sunuyor.

Bir satıcı gözüyle bakıldığında, Bitcoin'in kârlarını azaltan kredi kartı şirketlerinin yüksek ücretlerine sahip olmaması gibi bir avantajı var. Kredi kartı şirketleri her işlemden genellikle yüzde üç ya da dört komisyon alırlar ve bu ücreti genellikle satıcı üstlenir. Küçük kâr oranları olan satıcılar için bu ücret her kredi ya da bankamatik kartıyla yapılan işlemin kârının yarısı ya da daha fazlasını silip süpürmesiyle sonuçlanabilir. Daha önce belirttiğim gibi, buna karşı, Bitcoin'in yaklaşık 0,02 dolar olan bir madenci ücreti var ve bu nedenle Bitcoin satıcıların kâr oranını fazlasıyla artırabilir.

İnternet hayatının başında, birçok öncü tamamen çevrimiçi yürütülen bir ekonomi hayal etti. 1990'ların başında, internetten alışveriş birçok şirketin üzerine uzun uzun düşündüğü bir şey olmadan çok önce, yazar Bill Eager internetten alışveriş hakkında kitaplar yazıyordu. O sırada, çevrimiçi bir şeyler, özellikle de fiziksel eşyalar satın almak alışılmamış olmaktan öteydi. Birçok ürün için bu imkânsızdı.

1994'te, Eager çarpıcı bir tahminde bulundu. *The In-*

formation Superhighway Illustrated adlı kitabında, "İnternetten alışveriş 1998 yılına kadar yıllık 4,8 milyar dolara ulaşma potansiyeli olan 200 milyon dolarlık bir ticaret," diye yazdı.[1]

Anlaşılan, Eager'ın tahmini pek abartı değildi. 1998 yılı, teknolojiye meraklı tüketicilerden genel tüketicilere geçiş yapan çevrimiçi alışveriş için bir dönüm noktası oldu.

Boston Consulting Group'un Aralık 1998'de yayınladığı raporuna göre, o yılın sadece ilk altı ayında internetten yapılan alışverişler 4,4 milyar dolara ulaşmıştı. Bu sayının yıl bitene kadar ve yeni yıl alışverişleri hesaba katıldığında, 13 milyar dolara ulaşması bekleniyordu.

1990'ların sonu ve 2000'lerin başı dot-com balonunun nihayet patladığı dönem olarak hatırlanıyor. Ama bu her sene büyümeye devam eden çevrimiçi perakende satış mağazaları için geçerli değildi. Geleneksel perakende mağazaları internette yer edinmeye başlayıp sadece çevrimiçi satış yapan web sitelerine meydan okurken suda çok fazla kan vardı, ama toplam harcama arttı ve günümüzde birçok kişinin yirmi sene önce hayal etmesinin mümkün olmadığı bir oranda artmaya devam ediyor. 1999 yılında, internet alışverişi iki katına çıkıp 27 milyar dolara, 2000 yılında tekrar artış gösterip 45 milyar dolara ulaştı.[2] 2013 yılında, işletmeden tüketiciye çevrimiçi perakende satışları 803,76 milyar dolar kazanç getirdi. Bu, çevrimiçi işletmeden işletmeye işlemleri de hesaba kattığınızda iki katına ulaşan bir rakamdı.[3]

[1]Eager, Bill. The Information Superhighway Illustrated. (Indianapolis, Que Pub, 1994)

[2]Abdelmessih, Nina, Michael Silverstein, and Peter Stanger. "Winning The Online Consumer: The Challenge of Raised Expectations." The Boston Consulting Group, 2001. Erişim tarihi 15 Mart 2015. http://www.bcg.com/documents/file13692.pdf

[3]"Statistics and facts about Online Shopping" Statista. Erişim tarihi 15 Mart 2015. http://www.statista.com/topics/871/online-shopping/

İnternet ekonomisinin ilk hayalleri gerçekleşti. Giysilerden müziğe, arabalara ve hatta evcil hayvanlarımıza kadar birçok şey internetten satın alıyoruz. İnternetten alışveriş yapmak artık tuhaf değil; beklenen bir şey. İnternetten hiç alışveriş yapmamış insanlar giderek eşine ender rastlanan bir tür haline geliyorlar. Yaşlıların bile büyük bir bölümü internetten bir şey satın almışlardır.[4]

İnternet öncülerinin çoğu kendi para birimi olan bir internet hayal ettiler. "İnternet küreseldir," diye iddia ettiler. Küresel, anlık ve dijital bir ekonominin doğru düzgün işlemesi için onu destekleyebilecek küresel, anlık ve dijital bir para birimine ihtiyacımız var. Eğer Bitcoin daha fazla gelişmezse bile, bu şeylerin hepsi olacak. Şimdiden anlık bir küresel para birimi ve internet gibi, hemen herkesin kullanımına açık. İnternetin öncüleri Bitcoin ekosisteminin günümüzde takıntı haline getirdiği spekülatif olasılıklar hakkında konuşmuyorlardı. Bitcoin kültürünün bu talihsiz yanı fiyatın çılgınca yükselip alçalmasından sonra ortaya çıktı.

Wired dergisinin ilk genel yayın yönetmeni Kevin Kelly, elektronik para sisteminin gelişimini ve dünyamız üzerindeki etkisini 1994'te yazdığı *Out of Control: The New Biology of Machines, Social Systems and the Economic World* adlı kitapta öngördü. Kelly şöyle yazıyor:

Merkezi olmayan, yaygın yapısı sebebiyle şifrelenmiş e-para yönetimi iletişim yapısını revizyondan geçiren ki-

[4] "E-COMMERCE: Evolution Or Revolution In The Fast-Moving Consumer Goods World?" Nielsen. Ağustos 2014. Erişim tarihi 19 Mayıs 2015. http://www.nielsen.com/con- tent/dam/corporate/us/en/reports-downloads/2014%20Reports/nielsen-global-e-com-merce-report-august-2014.pdf

şisel bilgisayarlar gibi ekonomik yapıyı değiştirme potansiyeline sahip. En önemlisi de, e-paranın ihtiyacı olan gizlilik/güvenlik yenilikleri bilgiye dayalı bir toplumda uygulanabilir karmaşıklığın seviyesini geliştirmekte aracı olacak. Hatta biraz daha ileri gidip gerçek dijital paranın –daha doğrusu, gerçek dijital para için gereken ekonomik mekanizmaların– ekonomi, iletişim ve bilgi yapımızı yeniden şekillendireceğini söyleyebilirim.[5]

Çevrimiçi ne kadar vakit geçireceğimiz ve para harcayacağımızla ilgili tahminler doğru çıkmış olsa da, internetin hiçbir zaman kendi para birimi olmadı. Bazı girişimler oldu ama parayı tedavüle çıkaran birimlerin merkezi yapısı e-parayı her zaman internetin merkezi olmayan yapısıyla bağdaştırmadı. Bazı para birimleri başarısız oldular, çünkü onları ortaya çıkaran şirketler para işlemcileri olarak hareket edip gereksiz aracıları ortadan kaldırmak yerine yeni bir aracı eklediler. Diğerleri ise, parayı yayan kişi onun gücünü kötüye kullandığı ve satın alanları dolandırdığı için başarısız oldular.[6] Bir kısmı hükümet düzenlemelerine ters düştüler. Merkezsizleşme sayesinde bu sorunlardan kaçınılabilir.

Satoshi Nakamoto dağıtık hesap defteri ve çalışma ispatı kavramlarını birleştirerek blokzincirini icat ettiğinde, internet için uzun zamandır düşünülen işlenebilir, dağıtılabilir, merkezsizleştirilmiş para birimi hayalini gerçekleş-

[5]Kelly, Kevin. Out of Control: The New Biology of Machines, Social Systems and the Economic World. (New York, Basic Books, 1994, Reprint 1995)

[6]Zetter, Kim. "Bullion and Bandits: The Improbable Rise and Fall of E-Gold." Wired.com. 6 Eylül 2009. Erişim tarihi 20 Mayıs 2015. http://www.wired.com/2009/06/e-gold/

tirdi. Bununla, herkes birkaç sent ya da daha az bir miktar karşılığında dilediği kadar transfer yapabilir. Blokzinciri her işlemi kaydediyor ve yaygın yapısı hiçbir resmi kurumun onu kapatmamasını sağlıyor. Bunun nasıl işlediğiyle ilgili detaylara başka bir bölümde değineceğim. Ama Bitcoin ve blokzincirinin ilk kullanım durumu internette e-posta yollamak kadar kolay ve neredeyse o kadar ucuz bir şekilde değer transferi yapabilmektir. Blokzinciri için her geçen gün daha fazla kullanım alanı geliştiriliyor ama bu en bariz olanı. Birçok uzman blokzincirinin ilk 'uygulamasının' para transferi olduğunu söylediler; ancak bu tek uygulamanın bile neredeyse sonsuz kullanımı var.

Bu kitabın başında bulunan kare kodu kullanarak Bitcoin cüzdanı olan herhangi bir okuyucu bana, yazara bitcoin gönderebilir. Hiçbir bankanın bunu onaylamasına gerek yok; nerede olduğunuzun ya da bunu ne zaman okuduğunuzun önemi yok. Cüzdana erişimim olduğu sürece parayı alabilirim. Hatta, o cüzdana erişimimin olmasına bakılmaksızın, Bitcoin blokzinciri varlığını sürdürdüğü sürece herhangi bir kullanıcı o adrese para transfer edebilir.

Bu, kulağa pek de etkileyici gelmeyebilir. Ne de olsa, bankalar da para transferi yapabiliyorlar. Bankalar komisyonlarını alırlar, ama insanların eski sistemi kullanarak dijital olarak para gönderebilecekleri yöntemler de mevcut. Ancak, izin istemekle izin istememek arasındaki fark hiç de küçük değil. Bitcoin kullanan herhangi bir kullanıcı hiçbir kısıtlama olmadan dünyanın herhangi bir yerinde Bitcoin cüzdanı olan herhangi bir işletme ya da şahsa dilediği miktarda para gönderebilir.

Rusya'daki biri, bir kitlesel fonlama projesi başlatmak

istiyorsa, parayı Rusya'daki bir banka hesabına yatıracak bir hizmet bulmalı ve sonra projesini onaylayacak ya da reddedecek kitlesel fonlama sitesine taşımalıdır. Sonra, bu site yatırımcıları ve yaratıcıları buluşturduğu için kendi komisyonunu alacak. Bitcoin tüm bu aracıları ortadan kaldırabilir. Bitcoin kullanarak, insanlar hiç kimseden izin almadan başka birine para yollayabilirler.

Bu aynı zamanda bir özgürlük sorunu. Merkezi ve yasal sistemler kullanıcıların belirli oluşumlara para göndermelerini yasaklıyorlar. Örneğin, Amerikan helikopter pilotlarının sivil görünen kişileri vururken şakalaşmalarını gösteren, bilinmeyen bir kaynaktan sızmış video üzerine tartışmalar sürerken, ispiyoncu web sitesi Wikileaks, PayPal ve kredi kartı desteğini kaybetti.[7]

Bu tür bir yasaklama için yasal bir temel şart olmasa da, bireysel şirketler insanların inandıkları amaçları desteklemek için para göndermelerini engelleyebilirler. Bitcoin, güçlü bir yasal savunmayla birlikte, bu kişilerin bu tür yasaklamaları atlatmanın bir yolunu bulmalarına yardım etti. Kullanıcıların belirli bir kişiye para göndermelerine engel olan merkezi bir güç olmadığında, kullanıcılar bitcoin'lerini diledikleri amaç için başkalarına gönderebilirler.

Bitcoin'in sadece internet tabanlı aracıları değil, gerçek dünyadakileri de gölgede bırakma potansiyeline sahip. Walmart Çin'den çok fazla mal satın alıyor. Walmart'ın kâr oranının yüksek kalması için ürünlere fazlasıyla zam yapılıyor. Peki onlara gerçekten ihtiyacımız var mı? İnternet

[7]Barnes, Julian and Jeanne Whalen. "PayPal Drops WikiLeaks Donation Account." The Wall Street Journal, 4 Aralık 2010. Erişim tarihi 10 Mart 2015. http://www.wsj.com/articles/SB10001424052748704767804575654681242073308

ve Bitcoin'i kullanarak, Çin'deki herhangi birine rahatlıkla para gönderebilirim. Alıcının Amerikan kredi kartlarını kabul eden ve Çin banka hesabına parayı yatıran bir sistem kurulması hakkında endişelenmesine gerek yok. Dolarla bitcoin satın alıp Çin'deki işletme sahibine gönderebilirim ve alıcı onu yuana çevirebilir. Ücretler, olsa bile, Western Union ya da kredi kartı aracılığıyla para göndermekten çok düşük olur. Hatta, en büyük ücret potansiyeli eski bankacılık sistemiyle muhatap olunduğunda –Amerikan dolarını bitcoin'e ve sonra bitcoin'i yuana dönüştürürken– ortaya çıkıyor.

Bunun küresel ekonomiyi nasıl değiştirebileceğini düşünün. Geçmişte, dünya liderleri –iyisiyle kötüsüyle– bizi küreselleşmeye doğru itiyorlardı. Serbest ticaretin gümrük vergilerini ortadan kaldırmasıyla, işgücü hızlı bir şekilde bölgeselden küresele doğru hareket etti. Bunun birçok Amerikan işçi için kötü olduğunu çok az kişi inkâr edebilir. O işçiler Latin Amerika ve Asya'daki ucuz işgücünden kötü etkilendiler. Sömürüye dayalı işgücü ve Amerikan tüketicileri arasındaki anlaşmaları yürüten aracılara kalan kâr giderek daha da artıyor.

Serbest ticaret hakkındaki düşünceleriniz ne olursa olsun, masrafları artıran –ekonomi uzmanları tarafından genellikle sürtünme olarak adlandırılan– engellerin hiçbir faydası yok. Eğer küresel bir ekonomimiz olacaksa, küresel bir para birimine ihtiyacımız var. Aracıları ortadan kaldırıp paranın üreticiden doğrudan tüketiciye aktarılmasını sağlamak bu süreci oldukça hızlandırır. Aynı zamanda, aracılar olmadan doğrudan dünya çapındaki tüketicilere satış yapmalarına imkân tanıyarak küçük ölçekli üretim sana-

yiye güç verir. Umarım, bunlar çalışanlarına adil davranan sürdürülebilir endüstrilere dönüşür, bölgelerinde ve en nihayetinde dünya çapında işgücünü artırırlar.

Daha temel ve orta seviyede, Bitcoin düşük maliyetli havaleye imkân tanıyor. Bankacılığın nispeten erişilebilir olduğu gelişmiş ülkelerden rahatlıkla erişilebilir olmayan üçüncü dünya ülkelerine para göndermek oldukça pahalı olabilir. En yüksek ücretler neredeyse yüzde elli ve ortalama ücretler yüzde dokuz civarında. 2009 yılında, göçmenlerin ülkelerine 316 milyar dolar gönderdiği düşünülürse, aracıların emdiği bu ücretler yerel ekonomiye katkı sağlayabilecek milyarlarca dolara ulaşıyor.[8] Bitcoin bu aracıların yerini alabilir.

Bitcoin'in nasıl fark yaratacağına bir başka örnek borç vermek olabilir. Mikro krediler küçük yatırımcıların şahısların kredi şirketlerinin aldığı yüksek faiz oranlarından kaçınmalarını sağlarken paralarını artırmalarının bir yolu olarak internette oldukça popüler olmaya başladı.

BTCJam ve benzer hizmetler yatırımcıların ticari planlardan kişisel projelere kadar her şey için kredi alan kişileri finanse etmelerini sağlıyor. Krediler hem bitcoin hem de dolar olarak gösterilebilirler. BTCJam bir aracı olmasına rağmen, kredi kartı ve para transferini yapan aracıları ortadan kaldırarak çalışırken, kredi alanlardan sadece yüzde bir ila beş oranında ücret kesiyor. Sürtünmenin giderilmesi daha fazla yatırımcıya ve daha fazla paraya olanak tanır.

Kripto paranın teorik olarak sağlayabileceği bir başka hizmet herhangi bir işlemde arabulucu rolü üstlenmek-

[8]"Transfer fees." The Economist. 15 Aralık 2010. Erişim tarihi 15 Mart 2015. http://www.economist.com/blogs/dailychart/2010/12/remittances

tir. BlackHalo'nun Bitcoin yarısı BitHalo, yasal güç yerine bilgisayar kodu tarafından düzenlenen uygulanabilir akıllı sözleşmelerin ilk örneğiydi. Akıllı sözleşmeler iki tarafın da birbirlerine güvenmelerine gerek kalmadan somut mal satışına imkân tanıyor. BlackHalo, yirmi birinci bölümde değineceğim alternatif kripto para Blackcoin için tasarlandı. BitHalo'nun benzer işlevselliği var ama Bitcoin'le birlikte çalışıyor. İki para birimi arasında hızlı transfere imkân tanıyor.

En önemlisi, BitHalo eBay ya da Paypal gibi üçüncü bir arabulucuya gerek kalmadan merkezi olmayan bir pazar sunuyor. Bitcoin tek başına malın satıcıdan alıcıya doğrudan satılmasına imkân tanırken, insanların anlaşmazlıkları ortadan kaldırmalarının bir yolu yok. Bitcoin bir kez gönderildikten sonra, alıcının kontrolündedir ve eğer satıcı ürünü göndermeyi ya da hizmeti sağlamayı ihmal ederse, alıcının bu konuda yapabileceği çok az şey vardır. BitHalo insan doğasını hesaba katarak bu sorunu çözüyor. Her iki tarafın da asıl işlemden ayrı bir depozito yatırması beklenir. Hem depozitolar hem de alıcının parası program tarafından emanete alınır. İki taraf da işlemi onayladıktan sonra, alıcının parası satıcıya transfer edilir ve depozitolar iki kullanıcıya geri iade edilir. Eğer iki kullanıcı da işlemi iptal etmeye karar verirse, para alıcıya transfer edilir ve depozitolar sahiplerine iade edilir. Ancak, iki taraf önceden belirlenmiş bir tarihe kadar anlaşamazsa, depozitolarını kaybederler ve meblağ, geri alınabilir bir adresi olmayan bir cüzdana gönderilir. Fonlar Bitcoin ekosisteminden çıkarılır.

Düzgün bir şekilde kullanıldığında, BitHalo alıcı ve sa-

tıcılara diğer tarafın işlemin makul bir şekilde gerçekleşeceğinden emin olduğuna dair güven verir. Eğer depozito asıl işlemin üç katı değerindeyse, iki taraf da diğerini dolandırmaya çalışarak hiçbir yere varamaz. Dolandırma ve göz korkutma taktikleri hâlâ ara sıra kullanılsa da, bu sistem merkezi olmayan bir pazarda güven oluşturmak için uygulanabilir bir yöntem sunuyor.

BitHalo'nun tek sorunu onu kullanan kimsenin olmaması. Pazar yerini dolduran insanlar olmayınca, alıcı ve satıcıların yazılımı indirmeleri için hiçbir sebep yok. Güzel fikirler her zaman güzel bir şekilde uygulanmazlar. Bitcoin'le ilgili bazı projelerin sorunu bu.

OpenBazaar, Silk Road'un gelişmişi olarak tarif edilen ve ümit vaat eden bir proje. Silk Road'un aksine, OpenBazaar Bitcoin gibi merkezsizleştirilmiş; bir diğer deyişle hükümetin onu durdurmak için kapatabileceği bir sunucusu yok. Amir Taaki ve bir grup gelişimcinin yarattığı Darkmarket denen koda dayanıyor. Brian Hoffman, çatallandırdığı Darkmarket'i aynı prensipleri kullanan ama görünürde kendisini Silk Road'dan ayıran OpenBazaar'a dönüştürdü. Bununla beraber, herhangi bir şeyin satışını engelleyen bir kural yok, yazılımla da olamaz. OpenBazaar'a sonuçta ne olacağı –merkezsizleştirilmiş bir Amazon ya da eBay mi, ya da daha alışılmışın dışında, merkezsizleştirilmiş Silk Road mu– belirsizliğini koruyor. Proje şu anda ilk aşamasında ve ortalama tüketici tarafından kullanılamaz ama bu kitap raflardaki yerini aldığında, durum farklı olabilir.

Yine de, Bitcoin'in kişiler arası transfer dışında birçok yanı var. Daha önce de bahsettiğim gibi, Bitcoin banka eri-

şimi olmayanlara temel banka işlemlerini ulaştırmakla kalmıyor; aynı zamanda dünyanın her yanındaki kullanıcılara ileri bankacılık işlemlerini getirme potansiyeli de var.

Genellikle adlandırıldıkları gibi, Bitcoin 2.0 projeleri Bitcoin ya da diğer kripto paraları içerebilirler. Bu projelerin arkasındaki ana fikir, blokzinciri ve blokzinciri teknolojilerinin Bitcoin ya da diğer dijital para birimleri dışındaki değerli malların transferini yapmak ve kaydını tutmak için kullanılabilecek olmaları. Bir 2.0 projesi Bitcoin kökenli olmasa bile –Ethereum gibi– kripto paralara yatırımı ve ilgiyi artırırsa, Bitcoin'in değerini de artırmaya eğilimlidir.

İlk '2.0' kripto para örneği Namecoin'di ve bir para birimi olmanın yanı sıra, herhangi bir hükümetin kontrolünden bağımsız yaygın bir alan adı yazmanı görevi görüyordu. Kullanıcıların Namecoin protokolünü kullanarak kaydolan siteleri ziyaret edebilmeleri için Namecoin blokzincirini indirmeleri gerekiyor. Namecoin ağındaki siteler .bit alan adı uzantısını kullanırlar. İnternette genelde gördüğünüz, .com, .net, .org ya da diğer alan adı uzantılarının aksine, .bit kayıtları merkezi bir kuruluş tarafından verilmez ve kontrol edilmez.

Namecoin bir Bitcoin 2.0 projesinin ilk örneğiydi ama başkaları da oldu. Counterparty, Ethereum, Masterparty ve Nxt kitlesel fonlama ve 'kitlesel yatırım'da ön plandalar. Bu platformların hepsi farklı olsa da, özünde aynı şeye imkân tanıyorlar: kullanıcılar bir şirket mülkiyeti de dahil olmak üzere para dışında birçok şeyi temsil eden kendi varlıklarını kullanabiliyorlar.

Birçok varlık şimdiye kadar geleneksel kitlesel fonla-

ma ya da yatırıma benzer şekilde kullanılmış olsa da, başka birçok seçenek var. *Distributed Automated Corporations* (DAC – Yaygın Otomasyonlu Şirketler) neredeyse bütün kripto para topluluğunu heyecanlandıran bir şey. Bütün şirketler gibi, DAC'ler da para kazanmak için var olan oluşumlar. Ancak, birçok şirketin aksine, DAC'lerin çalışanları yok. Çalışanlar yerine, bir DAC kod kullanarak kendini idare eder. İnternette reklam izlemek gibi kâr getirebilecek bir aktivite bulur ve bunu tekrar tekrar yapar. Mülkiyeti, Bitcoin ya da başka bir kripto para aracılığıyla DAC'ın varlığını elinde tutan şahıslara kriptoyla bağlı ve kârı onlara dağıtılıyor. Bir DAC birçok şey olabilir; ancak bir kez kurulduktan sonra, asgari ya da sıfır dış müdahaleyle çalışabilmelidir. Teknoloji geliştikçe, çok sayıda insanın DAC'lere sahip olması son derece olası ve bunlar sahiplerine ek ya da pasif bir gelir sağlayabilirler. Bunun sürdürülebilir olup olmadığı belirsizliğini koruyor; 'bedava' para nadiren bedavadır ve toplumumuzun gerçek iş olmayan bir dünyaya hazır olduğunu sanmıyorum; yine de DAC'ler ilginç olasılıklar sunuyorlar.

Bitcoin ve blokzinciri teknolojileri bize sadece internette yaratılan, yatırıma elverişli şirketler vermediler. Geleneksel finans da daha önce bu bağlantılardan ve yatırım yapabilecek fonlardan yoksun kişilere açılıyor. Eskiden Bitreserve adıyla bilinen Uphold, BitGold ve birkaç hizmet kullanıcılara değerli madenlere ve hatta başka yasal paralara yatırım yapma ve bulundurma imkânı veriyor. Uphold durumunda, yirmi yedi yasal para ve değerli madenin yanı sıra dört dijital para birimi (Bitcoin, Litecoin, Ether ve Uphold'un kendi para birimi Voxelus) destek-

leniyor. Uphold, yüklü miktarda başlangıç yatırımı yapabilecek ve yüksek ücretlerin üstesinden gelebilecek kadar harcanabilir gelire sahip olmayan ortalama tüketiciler için başka türlü mümkün olmayacak yatırım fırsatları sunuyor. Uphold kısa bir süre önce bütün doğrulanmış müşterilerinden –kişisel belgelerini yükleyerek kimliğini kanıtlayanlardan– yasal para dönüşümü için ücret almayı kesti.

Yukarıda bahsettiğim iki hizmet değerli madenler ya da yasal para ve Bitcoin arasında hızlı transfere imkân tanıyor. Diğer şirketler Bitcoin'i teminat olarak kullanarak kullanıcıların hisse alım satım yapmasına izin veriyor. Borsa artık yatırım bankerleri ve farklı sitelerin gerektirdiği yüksek minimum depozitoları karşılayabilen kişilerle sınırlı değil.

Bitcoin kullanıcılara daha önce üst orta sınıf ve üzerine mahsus olan bir yatırım aracı sunuyordu. Bitcoin kullanıcıları birikimleriyle neredeyse anında birçok emtiaya yatırım yapabilirler. Eğer bir kullanıcı yatırımından vazgeçmeye ya da bir kısmını harcamaya karar verirse, fahiş ücretlere maruz kalmadan bunu neredeyse anında yapabilir. Ayrıca, bir kuruştan daha az bir tutarla 'yatırım yapmak' bile mümkün.

Şimdiye kadar anlattığım kullanım biçimlerinin hepsi katı bir biçimde para transferi yapmayı içermese de, tabiatları gereği parasallar. Ama blokzinciri bundan çok daha fazlasını yapabilir. Güvenli kriptolu bir şekilde dokümanları saklayabilir. Bir kullanıcı pasaportunun dijital kopyasını şifreleyebilir ve o dosyanın hash'ini blokzincirinde saklayabilir ve sonra yedek olarak o kopyayı kullanabilir. İki kullanıcı evliliklerini blokzincirine kaydedebilir; hatta bu

çoktan yapıldı.[9] Neredeyse bütün resmi belgeler ya da sözleşme blokzincirinde saklanabilir ve –yasal olarak tanınmasa da– noter onaylı bir dokümana kıyasla bir blokzinciri işlemini taklit etmek çok daha zordur.

Kullanılabilirlik potansiyel olarak parasal olmanın çok ötesine gidebilir. Blokzinciri teknolojisini kullanarak merkezsizleştirilmiş bulut depolama da bir olasılık. Storj Bitcoin blokzincirinde çalışmıyor; Bitcoin blokzincirinden ayrı ama ona dayalı üretilen bir para ve parasal hizmetler seti olan CounterParty sistemi üzerinde çalışıyor. Storj Bitcoin'in öncülük ettiği açık hesap defteri ve kriptolu araçlar kullanarak bir depolama sistemi kurmayı amaçlıyor.

Bu sırada, eski Megaupload.com ve mevcut Mega.co.nz adlı siteleriyle tanınan kötü şöhretli Kim Dotcom, bir şekilde blokzinciri ya da Bitcoin teknolojisi kullanacak 'IP'siz' internet üzerinde çalışıyor, ama bu konuda sızan haberler yavaşlamaya başladı.[10]

Bilgisayarın bütün faydalarını sıralamanın imkânsız olması gibi, Bitcoin'in bütün faydalarını sıralamak da imkânsızdır. Tıpkı programlanabildiği için sonsuz faydası olan bir bilgisayar gibi, programlanabilen bir para olarak Bitcoin de çok yönlüdür. Bunu okuduğunuzda, hiç şüphesiz Bitcoin için daha fazla kullanım alanı olacak.

---

[9] Vigna, Paul, ve Michael Casey. "BitBeat: Wedding Bells on the Blockchain." MoneyBeat. 26 Eylül 2014. Erişim tarihi 20 Mayıs 2015. http://blogs.wsj.com/moneybeat/2014/09/26/bitbeat-wedding-bells-on-the-blockchain/

[10] Cuthbertson, Anthony. "Kim Dotcom's Blockchain MegaNet and Bitcoin ATMs Stolen." International Business Times RSS. 17 Şubat 2015. Erişim tarihi 20 Mayıs 2015. http://www.ibtimes.co.uk/cryptocurrency-round-kim-dotcoms-blockchain-meganet-bitcoin-atms-stolen-1488393

Her gün Bitcoin blokzincirinde ya da onunla bağlantılı teknoloji üzerinde kullanılmak üzere yeni araçlar geliştiriliyor. Ve Bitcoin var olan binlerce kripto paradan sadece biri. Ancak, onların ilkiydi ve o hâlâ bütün dijital paralar içinde en değerli, popüler ve faydalı olan. Bitcoin'in kullanılabilirliği sadece geliştiricilerinin yeteneği ve üzerinde çalışabilmeleri için onlara zaman tanıyan fonlamayla sınırlı. En nihayetinde, değerini belirleyen de bu.

Eğer Bitcoin Apple Pay, PayPal, Google Wallet ve diğerleriyle yarışmak istiyorsa, açık kaynak geliştiricileri –sadece çekirdek kodu geliştiricileri değil, bağlantılı projeler üzerinde çalışan bütün geliştiricileri kastediyorum– Bitcoin'e tüketici için herhangi bir biçimde şu anda mevcut olandan daha fazla kullanım alanı sağlamalılar. Teknoloji her zaman bundan ibaretti. Bitcoin'in farklı olduğunu düşünmek için hiçbir sebep yok.

Altıncı Bölüm:

Bitcoin: Anonim Mi, Yoksa Takma İsimli mi?

Şahıslar hakkında ortalıkta o kadar çok bilgi dolaşacak ki, mahremiyeti mümkün olduğunca korumak isteyeceğiz... Ama bankacıların bir kısmı isimsiz sistemin asla başarılı olamayacağını, *daha da önemlisi kendilerinin çözemeyeceği bir oluşuma dönüşeceğini hissediyor.*

— İlk kriptoculardan Ernie Brickell, Aralık 1994, Wired

Bitcoin sık sık isimsiz dijital para olarak adlandırılıyor, aslında bu onu tanımlamanın en kötü yolu değil. Ancak her cüzdana bir açık anahtar ya da kimlik verilir. Bu nedenle, ağa isimsiz demek yerine, 'takma isimli' demek daha doğru olur. Bu önemli bir ayrım ve bu bölümde nedenine ve yasal olarak ne anlama geldiğine değineceğim.

Birinci bölümde bahsettiğim gibi, blokzinciri ağ üzerindeki bütün işlemleri ve bakiyeleri kayıt altına alıyor. Her cüzdan, kullanıcının Bitcoin kimliği ya da takma ismi

görevi gören uzun bir dizi sayıyla tanımlanıyor. Bu kimlik gerçek hayattaki kimliğinizden ayrı tutulduğu sürece, işlemlerin kredi kartı ekstresi gibi size ulaşacak şekilde geriye doğru izi sürülemez.

Sorun şu ki, bir Bitcoin hesabını çevrimiçi bir kimlikle ilişkilendirmenin birçok farklı yolu var. Ve oradan, 'çevrimiçi' kimlikten 'gerçek hayattaki' kimliğe ulaşmak genellikle hiç zor değil. Bitcoin ağında anonim kalmanın en büyük zorluğu Bitcoin ağına girmektir. Bitcoin'de çalışmıyorsanız ya da size para karşılığı bitcoin satacak birini bulamıyorsanız, eninde sonunda bir banka havalesi yapmak, kredi kartı ya da PayPal hesabı kullanmak ya da girişimci bir üçüncü partinin kim olduğunuzu, ne kadar Bitcoin satın aldığınızı ve onu hangi cüzdana koyduğunuzu bilmesine izin vermek için bir şey yapmak zorundasınız.

Bunu bir kez yapınca, işlemlerinizi blokzincirinde takip edebilirler. Ağ üzerinde hareket eden gerçek veri parçaları ya da başka bir 'fiziksel' şey olmamasına rağmen, blokzinciri hesabınızdan çıkan her şeyi ve ağ üzerinde ona tekabül eden depozitoyu kaydediyor.

Eğer Bob, Jack'e beş bitcoin verirse, ağ Bob'ın hesabından beş bitcoin eksilip Jack'in hesabına geçtiğini görecek. Aslında internet üzerinde hiçbir şey 'seyahat etmiyor'; sadece Bob'ın cüzdanında beş bitcoin daha az ve Jack'inkinde beş bitcoin daha fazla var. Eğer Jack güvenilmez biriyse, Bob bütün dünyanın Jack'e beş bitcoin verdiğini görmesini istemeyebilir ama işlem bakmak isteyenler için blokzincirine kaydedilir. Daha önce bahsettiğim gibi, Bitcoin ağı işlemleri şahıs isimleriyle takip etmez; sadece cüzdan adreslerini takip eder.

Normal bir Bitcoin işlemi şöyle görünür:

18xAMYmeDHqmtPvM76VwECqzcEC7oCST15 0.02BTC---> 38ccq12hPFoiSksxUdr6SQ5VosyjY7s9AU

Bu size ya da bana hiçbir şey ifade etmez. Görebileceğiniz tek şey 18xAMYme... adlı cüzdanın 38ccq12... adlı cüzdana 0.02BTC göndermiş olduğudur. Ancak, ilk adresi benim kontrol ettiğimi ve ikinci adresin Bitcoin'in evsizler destek programı Sean's Outpost tarafından kontrol edildiğini biliyorsanız, o halde 22 Haziran 2014'te Sean's Outpost'a 0.02 bitcoin gönderdiğimi rahatlıkla çözebilirsiniz.

Şimdi, yaptığım bağışı herkesten saklamak istediğimi farz edelim. Bitcoin'leri kredi kartıyla satın aldıktan sonra o parayı başka bir kullanıcıya göndermek yeterli değil; bir aracı olmalı ve o aracı belirli şekilde davranmalı.

Eğer cüzdan A cüzdan B'ye beş bitcoin gönderir ve sonra cüzdan B cüzdan C'ye beş bitcoin gönderirse, cüzdan A'nın niyetinin cüzdan C'ye beş bitcoin göndermek olduğundan emin olabilirsiniz. Bu, özellikle de cüzdan B'nin ilk başta hiç bitcoin'i yoksa ya da varlığı süresince sadece cüzdan A'dan bitcoin aldıysa doğrudur.

Eğer meraklı bir taraf cüzdan A'nın sahibi olduğumu ve cüzdan C'nin Sean's Outpost'a ait olduğunu biliyorsa, o halde asıl niyetimin Sean's Outpost'a bitcoin göndermek olduğundan şüphelenebilirler.

Yasal bir açıdan bakıldığında, makul şüphe seviyesinin herhangi bir suç işlendiğinde birini temize çıkarıp çıkarmayacağına dair bazı sorular var. Eğer daha önce bitcoin'i olmayan bir cüzdana bitcoin gönderirsem ve o cüzdan aynı miktarda parayı bir uyuşturucu satıcısıyla ilişkili hesaba yollarsa, bu durum uyuşturucu satın almaktan suç-

lu bulunmam için yeterli seviyede makul kanıt oluşturur mu? Ya aracı cüzdanın, yani bu örnekteki cüzdan B'nin, önceden bitcoin'i varsa? Ya o bitcoin farklı kaynaklardan gelmişse? Ya ona üç bitcoin gönderirsem ve o cüzdan C'ye iki bitcoin gönderirse? Ya kalan bitcoin'i daha sonra bana geri gönderirse? Ya göndermezse? Bu tür soruların önümüzdeki yıllarda mahkemeler tarafından yanıtlanacağını düşünüyorum.

Ancak, söz konusu kişisel gizlilik olduğunda, el altındaki sorun her zaman yasal konular değil. Kamuoyunun görüşleri yasal makamların görüşlerinden daha sert olabilir ve paranızı nasıl, ne zaman harcadığınızın bilgisi reklamcılar ya da daha kötüsü: Dolandırıcılar, takipçiler ve psikopatlar tarafından kullanılabilir.

Basında kişisel gizliliği koruma çabalarının bir suçmuş gibi resmedilmesi endişe verici boyutlara gelmeye başladı. Her nedense, her şeyi herkesle paylaşmamak bir suç unsuru olmakla ilişkilendirilmeye başlandı. Kişisel işlemlerinizi gizli tutmayı istemenizin birçok mantıklı sebebi var, suç faaliyetleriyle hiçbir ilgisi olmayan sebepler.

Bana bitcoin'le ödeme yapan CoinJournal'da yazıyorum. Aynı zamanda kişisel blogumda insanların bana bağış yapabileceklerini belirtiyorum, o nedenle Bitcoin adresim herkese açık. Eğer bir rakip web sitesi beni CoinJournal'dan kapmak isterse, her hafta CoinJournal'dan bana ne kadar para gönderildiğine bakabilir ve bana daha fazla para teklif edebilir.

Rekabetçi çalışan kapma birçok iş yeri için ciddi bir mesele ve çalışanların maaşlarının herkese açık bir bilgi olması pek ideal bir durum olmayabilir.

Ayrıca, hedef olma endişesi var. Eğer insanlar yüklü

miktarda para kazandığınızı fark ederlerse, bu birçok soruna yol açabilir.

Her şeyden çok, gizlilik bir insan hakkı meselesidir. İlk bölümlerin birinde bahsettiğim, Bitcoin öncesi dijital para girişimlerinden Digicash'le ilgili bir makalede, *Wired* dergisinden Steven Levy, kriptocu ve o dönem Digicash çalışanı olan Niels Ferguson'dan şöyle alıntı yapıyor:

> Ah, gizliliğe ihtiyaçları olduğunu söylediğim insanlarla kaç kez tartıştığımı bilemezsiniz! "Paramı nerede harcadığımı bilmen umurumda değil!" diyorlar. Onlara genellikle, "Seni bütün gün takip edecek özel bir dedektif tutsam? Sinirlenir misin?" diye soruyorum. Ve yanıt her zaman, "Evet, elbette, çok sinirlerim," oluyor. Bunun üzerine, "Parasal işlemlerimizde gizlilik olmazsa, her ödemeyi görebilirim. İçtiğin her fincan kahveyi, aldığın her çikolatayı, içtiğin her kutu kolayı, açtığın her kapıyı, yaptığın her telefon görüşmesini görebilirim. Eğer bunları görebilirsem, özel dedektife ihtiyacım olmaz. Görev yerimde oturup seni bütün gün takip edebilirim," diyorum. İnsanlar ancak o zaman gizliliğin gerçekten önemli olduğunu anlıyorlar. Bilginin herhangi bir kısmı muhtemelen önemsiz olabilir. Ama asıl önemli olan bilgiyi toplamaktır.[1]

Mesele şu ki, maddi durumunuzdan daha özel olan çok az şey var; o halde Bitcoin'in bir açık defter kullanmasıyla

[1]Levy, Steven. "Emoney (That's What I Want)." Wired. 1 Aralık 1994. Erişim tarihi 22 Haziran 2015. http://archive.wired.com/wired/archive/2.12/emoney_pr.html

nasıl baş edeceksiniz? Takma isimli işlemlerinizi Bitcoin ağında gerçek hayattaki kimliğinizden nasıl tamamen ayrı tutacaksınız?

Bitcoin'lerin Bitcoin ağını oluşturan kod dışında gerçekten var olmadığını unutmamanız çok önemli. Bitcoin'leri takip etmek imkânsızdır, çünkü birini diğerinden ayıran hiçbir şey yok. Onlar sadece bireysel cüzdanlardaki değişken bakiyeler. Cüzdan A'dan cüzdan B'ye bir işlem gönderildiğinde, aslında hiçbir şey hareket etmiyor; cüzdan A'nın bitcoin sayısı azalırken, cüzdan B'ninki ona eşit miktarda artıyor.

Takip edilenler sadece işlemler. İşlem miktarınızın çeşitlendirip onları çok sayıda adres arasında bölerseniz, bu işlemlerin takibini A noktasından B noktasına doğrudan para göndermeyi takip etmekten daha çok zorlaştırırsınız. Yine de, bu teknik karışıklığa bir kat daha ekliyor. İşi yapmaya istekli olan biri iki durum arasındaki bağlantıyı kurabilir.

Günümüz teknolojisiyle Bitcoin işlemlerini takip etmeyi neredeyse imkânsızlaştıran hizmetler var. Bunu işlemleri birbirleriyle karıştırarak başarıyorlar. Bir grup farklı insanın işlemlerini alıp onları tek bir cüzdana yollar ve sonra orijinal katılımcıların kontrol ettiği ama ilişkilendirilmediği adreslere dağıtırsanız, blokzinciri kullanarak kimin neye sahip olduğunu kanıtlamak neredeyse imkânsız olur.

Bunu başarmanın birkaç yolu var. En açık olanı, Bitcoin ana akım medyanın ilgisini çeker çekmez ortaya çıkan bir para 'aklama' hizmeti. Bu gruplar farklı kullanıcıların işlemlerini alıp birbirleriyle karıştırıyorlar ve sonra onları müşterilerin istediği hesaplara yolluyorlar. Anonimliği artırmak için, paralar en az birkaç saat hesaplarda tutuluyor

ve ilgili tarafların işlemler arasında bağlantı kurmalarını zorlaştırmak için farklı ve rastgele ücretler içeriyor.

Ancak bu yöntemin bazı dezavantajları var. İşin doğası gereği anonim kalması gereken ve dükkânı her an kapatabilecek birine güvenmek zorundasınız.

Altcoin'ler de kasıtlı olmadan 'aklama' hizmeti sunuyorlar. Belirli bir işlemden gerçek kimliğini ayrı tutmak isteyen biri her zaman 'blokzincirine atlayabilir.' Daha sonraki bir bölümde değineceğim altcoin'ler, Bitcoin'den ayrı ve kendi açık hesap defterleri olan dijital paralardır. Bir kullanıcı bir borsadan altcoin satın alabilir ve onları borsa tarafından kontrol edilmeyen borsa dışındaki kendi cüzdanına aktarabilir, sonra onları başka bir borsaya aktarıp bitcoin karşılığında satabilir ve daha sonra onları yeni, ayrı bir cüzdana aktarabilir.

Bu yaklaşım blokzincir üzerinde takip edilemeyeceği için etkilidir ama borsalara bağlanmak genellikle bir tür kimlik ve olası bir IP adresi kaydı gerektirir. Ancak aynı yöntem, nadiren kimlik bilgisi soran ve yıllardır kasti olmayan karıştırma hizmeti sunan kumar sitelerinde uygulanabilir.

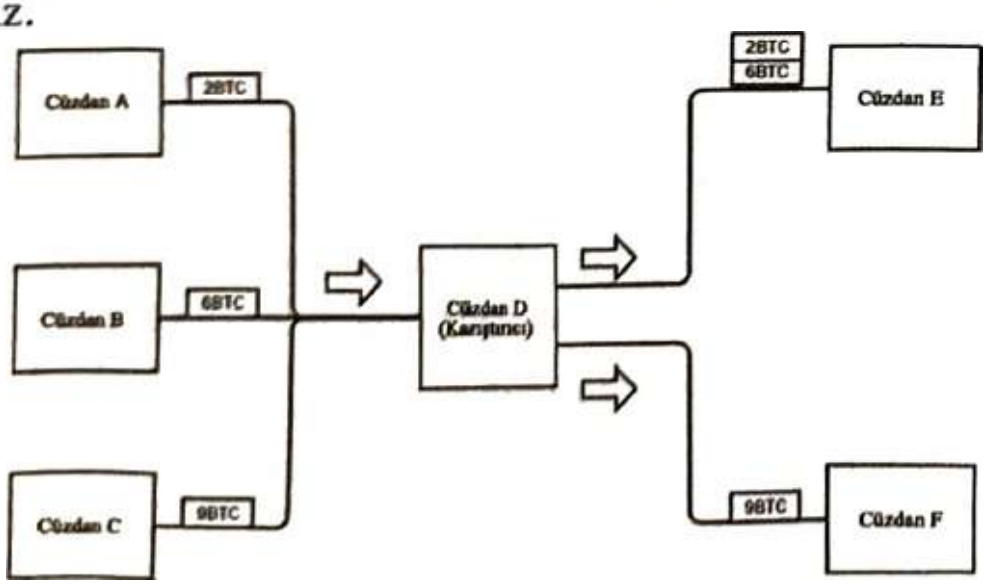
Son zamanlarda, bu hizmet yazılıma şifrelenerek bazen güvenilmez olabilen üçüncü şahıslara güven duyma zorunluluğunu ortadan kaldırdı. Bu konsept, artık birçok hizmetin kullandığı, CoinJoin adı verilen bir teknolojiyle doğdu. Uygun bir şekilde kullanıldığında, CoinJoin anonimliği otomatik olarak artırmak için paraları karıştırıyor. Ancak, kullanıcının belirlediği parametrelere bağlı olarak, CoinJoin işlemleri anonim yapmıyor, çünkü başarılı bir bir karıştırma, yukarıda anlatılan işlemi izlemeye bağlı. Kullanıcılar sık sık, ya bilerek ya da bilmeyerek, kolaylığı

gizliliğe tercih ediyor ve paralarını gerçek anlamda anonimlik sağlayacak kadar karıştırmamayı seçiyorlar.

Yukarıdaki örneği düşünün. Eğer cüzdan A cüzdan B'ye beş bitcoin gönderir ve sonra cüzdan B cüzdan C'ye beş bitcoin gönderirse, cüzdan A'nın cüzdan B'yi aracı olarak kullanarak cüzdan C'ye beş bitcoin göndermek istediğini çözmek hiç zor olmaz.

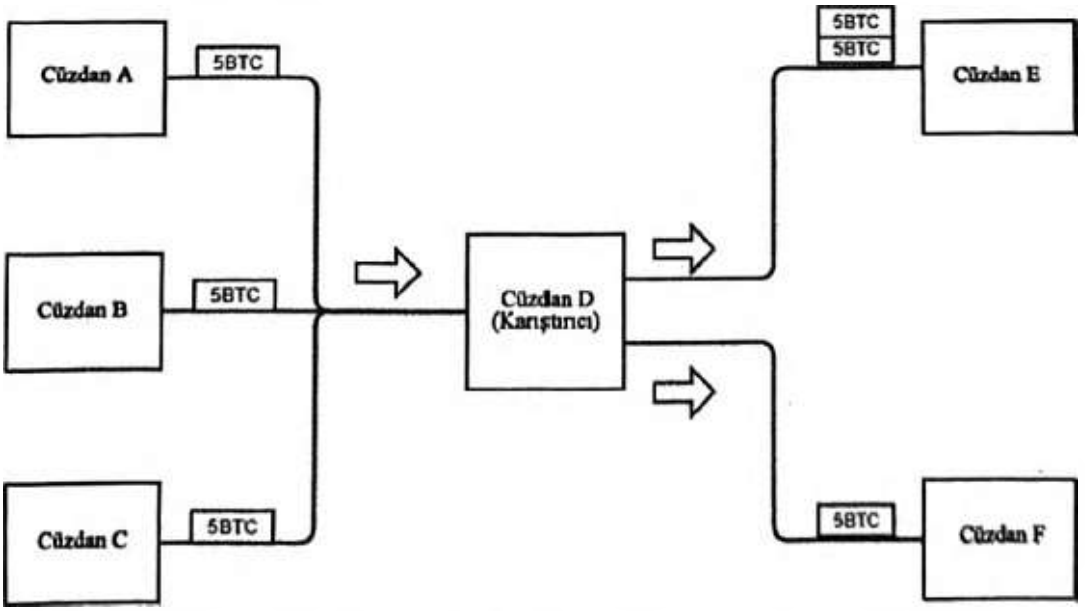
Birkaç Bitcoin kullanıcısının işlemlerini birleştirmek, takip etmeyi imkânsızlaştırmasa da oldukça zorlaştırır. Eğer cüzdan A, cüzdan B ve cüzdan C bir aracı hizmet (cüzdan D'ye) bitcoin gönderir ve sonra o parayı cüzdanlar E ve F'ye aktarırlarsa ama dış kaynakların kimin kime ne kadar gönderdiğini bilmelerini istemiyorlarsa, bitcoin'lerini cüzdan D'ye göndermeleri yeterli olmaz.

Eğer CoinJoin cüzdanına cüzdan A iki bitcoin koyar, cüzdan B altı bitcoin koyar ve cüzdan C dokuz bitcoin koyarsa –ve sonra tek işlemde cüzdan E'ye iki bitcoin, ikinci işlemde cüzdan E'ye altı bitcoin ve cüzdan F'e dokuz bitcoin gönderilirse– o zaman cüzdan A'nın cüzdan E'ye iki bitcoin, cüzdan B'nin cüzdan E'ye altı bitcoin ve cüzdan C'nin cüzdan F'e dokuz bitcoin gönderdiğini farz edebiliriz.



Blockchain.info'nun popüler Bitcoin ağ cüzdanında CoinJoin'in özelliğinden yararlanmaya çalışan kullanıcılara bu oluyordu.[2] Blockchain.info gizliliğe odaklanan bir şirket değil; o sadece alınması ve vazgeçilmesi kolay olan Bitcoin cüzdanı ve Bitcoin adresleri hakkında bilgi veriyor. Site, CoinJoin'i bir özellik olarak ekledi ama kullanıcılarını onu nasıl kullanacakları konusunda serbest bıraktı. Birçoğu işlemleri benzer işlemlerle karıştırma sürecinin otomatik olmadığını anlamadılar ve üçüncü bir partinin işlemlerini takip etmesinin ne kadar kolay olduğunu fark edince üzüldüler.

Birçok Bitcoin işlemi o sırada yasal paranın değerine bağlıydı. Hangi Bitcoin ödeme işlemcisinin kullanıldığına bağlı olarak sürekli değişen bir takas oranı varken, işlemler şöyle genellikle şöyle görünüyordu: 0.04534051BTC. Bu da kolaylıkla eşleştirilebilen bir tutar değildi. Paraları doğru düzgün karıştırabilmek için giden ve gelen miktarlar benzer olmalıdır.



[2] Southurst, John. "Blockchain's SharedCoin Users Can Be Identified, Says Security Expert." CoinDesk RSS. 10 Haziran 2014. 22 Haziran 2015. http://www.coindesk.com/blockchains-sharedcoin-users-can-identified-says-security-expert/

Yukarıdaki şema basit bir başarılı karışımı gösteriyor. Bir kanun uygulama kurumu ya da başka bir ilgili taraf cüzdan C'nin cüzdan F'ye beş bitcoin gönderdiğinden güçlü bir şekilde şüphelenecek olsa da, cüzdan C'nin o bitcoin'leri cüzdan F yerine cüzdan E'ye göndermediğini kanıtlayamaz. Sorun şu ki, bu yöntem cüzdan A, B ve C'nin aynı miktarı gönderebilmeleri için birlikte çalışmasını gerektiriyor. Bu genellikle bir tür merkezileşme gerektirir. Bitcoin'leri aklayan popüler hizmetler var ve ne kadar popüler olurlarsa, karışım hizmeti o kadar güçlüdür. En iyi hizmetler kullanıcılarına karışım hizmetlerinin etkisini maksimuma çıkarmak için uymaları gereken kurallar koyar.

Yukarıdaki şema para karıştırmanın temel ilkelerini gösteriyor ama birçok hizmet işlemleri kademelendirerek ve alınan ücreti rastgeleleştirerek yöntemi bir adım ileri götürüyor. Birçok karıştırma hizmeti yüzde 0,1 ila 0,25 arası küçük bir ücret alıyorlar ama bu yöntemi basit bir şekilde resimlemek için yuvarlak sayılar kullanacağız. O nedenle, karıştırma hizmetlerinin karıştırma işlemi başına 0, 1, 2 ya da 3 bitcoin aldığını ve bu miktarın rastgele seçildiğini farz edelim.

Üç cüzdanın (A, B, C) bir karıştırma hizmeti (cüzdan D) kullanarak üç cüzdana (E, F, G) üç farklı miktarda bitcoin göndermek istediğini düşünelim. Bu grafikte, aşamalandırılmış bir şekilde gönderildiklerini göstermek için işlemleri birbirlerinden ayıracağım.

Kullanıcılara ya 4BTC ya da 2BTC göndermeleri talimatı verilir ve karışan bitcoin'lerini 1BTC ya da 3BTC olarak alacakları söylenir. Ayrıca, kullanıcılara rastgeleleş-

tirilmiş 0BTC, 1BTC, 2BTC ya da 3BTC ücrete tekabül etmesi için her karışım için fazladan üç BTC gönderilmeleri söylenir. 1BTC ya da 2BTC ücret alırlarsa, fazla bitcoin'ler hedef adrese gönderilecektir. Genellikle, amaç bitcoin'leri karıştırma hizmeti aracılığıyla son duraklarına göndermek değil, sahip olduğunuz başka bir hesaptaki paralarla karıştırmaktır.

Bu noktada blokzinciri meraklıları için işler daha zorlaşır. Yukarıdaki şemadan çıkarılabilecek tek şey cüzdan B'nin cüzdan F'ye muhtemelen para göndermediğidir, çünkü cüzdan B'nin gönderdiği toplam miktar cüzdan F'nin aldığı miktardan daha azdır. Ancak, cüzdan C'nin cüzdan E, G ya da F'den herhangi birine para göndermek istemiş olabileceği iddia edilebilir ve bu işleri iyice karıştırır.

Ama cüzdanların birden çok ve ortak varış noktaları olabileceği ihtimalini göz ardı etsek bile –çünkü birbirlerinden bağımsız hareket eden kişilerin aynı anda aynı miktarları göndermeleri olasılık dışı olurdu– blokzinciri kullanarak kesin bir kanıt sunmak oldukça zor oluyor. Cüzdanlar A ve C üç alıcı hesaptan herhangi birine 7BTC göndermeye çalışmış olabilirler. Cüzdan B cüzdan G ya da cüzdan E'ye 5BTC göndermeye çalışmış veya 1BTC ödemiş ya da şansı yaver gidip hiç ücret ödememiş olabilir.

Yeterince sınırlandırma ve mantıksal çıkarım yaparak, bu senaryodaki bir ya da daha fazla oyuncuyu bulmak mümkün olabilir. Cüzdan B en büyük riski taşıyor, çünkü toplam işlem miktarı cüzdan C ve A ile eşleşmiyor. Ancak, işler iyice karışırken, kimin ne yaptığının izini sürmek giderek zorlaşıyor. Karıştırma hizmetleri kullanıcı sayısı

arttıkça daha etkili oluyor. Yukarıdaki senaryoyu yüzlerce gönderici ve onlara eş değerde olan alıcı cüzdanla hayal edin. Cüzdan B'nin eşleşmesi gereken üç cüzdan değil, yüzlerce cüzdan olurdu. Düzinelerce cüzdan B cüzdanı gibi aynı anda 8BTC gönderebilirdi.

Gördüğünüz gibi, insanlar Bitcoin'in anonim olduğunu söylediklerinde bu tam olarak doğru değil. Anonim olabilir ama takma isimli olduğunu söylemek daha doğru olur. Her cüzdana bir kimlik verilir ve o kimliğin sizin hakkınızda neler söyleyebileceği değişir. Cüzdan adresi sahibinin gerçek hayatındaki kimliğinden tamamen ayrı olsa da, kendini işine adamış bir kişi bir kullanıcının internette dolaşma alışkanlıklarını gözlemleyerek bir bağlantı kurabilir ve en nihayetinde bir işlemi IP adresiyle eşleştirebilir. Bu çoğumuzun –Microsoft, Apple ya da Google'ın bize verdiği varsayılan ayarları kullanarak– ağda dolaşma biçimimizden kaynaklanan bir savunmasızlık.

Kimliklerini ve işlemlerini gizlemeye kararlı dikkatli Bitcoin kullanıcıları Tor gibi anonim ağ tarayıcıları kullanabilirler. Bir zamanlar *The Onion Router*'ın kısaltması olan Tor, Bitcoin'den daha kötü şöhrete sahip birkaç teknolojiden biri.

Tor ağına bağlandığınızda, düğüm denilen bir giriş noktasından geçersiniz. Orada bilgi talebiniz o sırada düğümden geçmeye çalışan bütün kullanıcıları talepleriyle karışır. Bilgi daha sonra şifrelenir ve birkaç düğüme aktarıldıktan sonra çıkış düğümü denen yere varır. Çıkış düğümü bilginin şifresini çözer ve onu 'sıradan' internete aktarır. Tor daha sonra talep edilen bilgiyi internetten alır, onu şifreler ve iç düğüme gönderir, iç düğüm onu başka bir iç düğüme

gönderir ve en sonunda çıkış düğümüne vardığında bilginin şifresini çözüp kullanıcıya verir.

Bu şekilde, eğer düğüm ele geçirilirse, bilgiyi kimin istediğini 'bilir' ama ne istediğini bilemez. Çıkış düğümü kimlerin ne istediğini çözebilir ama kime ait olduğunu çözemez.

Tor tarayıcısı olan bir bilgisayarla yaratılan ve erişilen bir Bitcoin adresi dışarıdan neredeyse takip edilemez. Eğer bilgisayarınıza kötü amaçlı bir yazılım ya da virüs bulaşırsa, hiçbir önlem takip edilmenizi engelleyemez. Popüler işletim sistemleri, özellikle de Windows, gözetlenmelere ve saldırılara karşı oldukça hassastır. Linux işletim sistemleri genelde daha güvenlidir ama hiçbir şey yüzde yüz güvenli değildir.

Kısa süre önce, Birleşik Devletler Ulusal Güvenlik Teşkilatı ve Birleşik Krallık'ın Hükümet İletişim Merkezi'nin tüketici elektronik ürünlerine gizli erişim geçişleri yerleştirdikleri ortaya çıktı. Eğer sizin donanımınızda da bu geçerliyse, izlenmenizi önlemek için yapabileceğiniz pek fazla şey yok.[3]

Bitcoin'i ister takma isimli ister anonim görün, ağda kime bitcoin aktardığınızı gizlemeniz mümkündür. Bunun iyi bir şey olup olmadığı tartışmaya açık.

Bitcoin temelde internet dünyasının para birimidir. Birine nakit para verirsem ve bana karşılığında verdikleri üründen ya da hizmetten memnun kalmazsam, para iadesi isterken tamamen onların merhametinde olurum; başvu-

[3]Gallagher, Ryan, and Glenn Greenwald. "How the NSA Plans to Infect 'Millions' of Computers with Malware." The Intercept. 12 Mart 2014. Erişim tarihi 22 Haziran 2015. https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions- computers-malware/

rabileceğim üçüncü bir parti olmaz. Ayrıca, alışverişin gerçekleştiğini kanıtlamanın bir yolu da olmaz.

Söz konusu hesapların gerçek dünyadaki herhangi bir kimlikle bağlantılı olmadığını düşünürsek, Bitcoin de aynı şekildedir. Blokzinciri bir işlemin gerçekleştiğini kanıtlamayı mümkün kılıyor ama gerçek dünyadaki kimliklerle bir bağlantı olmadan, sadece blokzincirindeki verilere dayanarak kimin ne gönderdiğini kanıtlamak mümkün değildir.

Sonuçta, karıştırma hizmetleri dijital dünyaya sadece gerçek dünyada para transferlerinin işleyiş biçimini getiriyor. Güven sağlamaya yardımcı olmak için her türlü emanet hizmeti var. Ancak, en nihayetinde, bitcoin'ler hesabınızdan çıktıktan sonra, tıpkı para gibi onları verdiğiniz kişiye aitler ve nakit para transferlerinin izini sürmek için yapılabilecek çok az şey var. Düzenleyiciler ve felaket tellalları Bitcoin'i mevcut durumu yok eden bir araç gibi göstermeye çalışsalar da, açıkçası bu sadece elektronik işlemler ortaya çıkmadan binlerce senedir var olan mevcut durumu güçlendiriyor.

Bitcoin ekosistemindeki bu belirli oyuğun en umut vaat edici teknolojilerinden biri Darkwallet'tı, ama görüşüne bakılırsa, fazlasıyla para toplamış olmalarına rağmen geliştiricilerin parasız kalmasıyla projenin gelişimi durdu. Şu anda kullanılabilir bir durumda değil.

Üç boyutlu yazıcılarla basılabilen silahın yaratıcısı Cody Wilson ve Darkmarket'in yaratıcısı Amir Taaki tarafından icat edilen Darkwallet, merkezi olmayan bir karıştırma hizmetidir. Yaratıcılarının her ikisinin de otorite karşıtı, bireysel özgürlük yanlısı geçmişleri ve politikaları var.

Yine de, projeleri ana akım medya tarafından sık sık resmedildiği gibi onlar kadar radikal görülmemeli. Darkwallet terörizmi finanse edecek, uyuşturucu satın alınabilecek ve para aklanabilecek bir şeymiş gibi gösteriliyor.[4]

Açıkçası, Darkwallet sadece bir araç olmasına rağmen, hem suçlular hem de masum insanlar tarafından kullanılabilir. Kişisel finansı gizlemek ya da gizli tutmayı tercih edebileceğiniz alımları gizlemek için kullanılabilir. Porno satın almak birinin yasal sebeplerden ötürü gizlemek isteyebileceği alımlar için harika bir örnek. Porno yasa dışı değil –en azından genellikle– ama birçok insanın bu bilgiyi gizli tutmak için fazlasıyla sebebi var.

Bitcoin'in blokzinciri herkesin görebileceği şekilde açık. Bunun sebep olduğu kişisel gizlilik meselelerini hafifletmek tam olarak kötü bir şey değil. Visa ya da MasterCard'ın beni ne tür görüntülerin tahrik ettiğini bilmeleri gerekiyor mu? Bu benden başka birini ilgilendirir mi? Peki bu bilgiyi gizli tutmak beni bir suçlu mu yapar? Blokzincirinde, mesele Visa ve MasterCard'ın bu tür şeyleri görmesine izin vermek değil, potansiyel olarak bütün dünyanın onları görmesine izin vermektir. Bu tek örnek gizliliğe meraklı Bitcoin uygulamalarının ana akım medya tarafından neden 'suçlu aracı' olarak gösterilmemeleri gerektiğini açıklıyor.

Elbette, Darkwallet, ana akım medyanın bahsettiği birçok şey de dahil olmak üzere her türlü yasa dışı amaç için kullanılabilir. Geliştiriciler muhtemelen bu suçların daha

[4]Copestake, Jen. "Hiding Currency in the Dark Wallet." BBC News. 19 Eylül 2014. Erişim tarihi 22 Haziran 2015. http://www.bbc.com/news/technology-29283124

önce de var olduklarına dikkat çekerek karşılık vereceklerdir. Yasal para sistemi suçlulara çok iyi olanaklar tanıdı. Uyuşturucu satıcıları her zaman mallarını satıp kârlarını saklamanın bir yolunu buldular. Terör örgütleri her zaman, genellikle dost hükümetler tarafından, geleneksel yöntemlerle finanse edilmenin bir yolunu buldular.

Para aklamaya gelince, bu aklamayı kimin yaptığına ve ne kadarını akladığına bağlıdır. Kimliğinizi açıklamadan Bitcoin ağına para aktarmak gerçekten zordur; buna karşın, daha önce de değindiğim gibi, kimliğinizi ortadan kaybetmek oldukça kolaydır ama aynı zamanda ne yaptığınız bellidir.

Eğer halka açık bir şirketin yönetim kurulu başkanı Bitcoin kullanarak zimmetine para geçirmek isterse, parayı Bitcoin ağına aktarmak zorundadır; bir diğer deyişle Bitcoin karşılığında birine nakit para vermek gibidir ve bu eninde sonunda kişisel ya da şirket hesabını Bitcoin satan bir şirketle ilişkilendirmesini gerektirir. Halka açık şirketin finansal kayıtları ve Bitcoin blokzinciri de halka açık olduğu için Bitcoin yüklü miktarda parayı zimmete geçirmek için son derece kötü bir araç olur. Para karıştırıcıya gönderildiği anda kaybolur ama bu gerçekleşir gerçekleşmez ikaz işaretleri yanar. Karıştırma hizmetlerini fark etmek kolaydır, çünkü çok sayıda Bitcoin transferi yapmak zorundadırlar.

Blokzincirine yüklü miktarda para koyan ve sonra onu ortadan kaybeden geleneksel bir şirket, iyi muhabirleri ve araştırmacıları meraklandırır. Hiç kimse fark etmezse bile, ortada resmi kayıtlar vardır ve söz konusu suç olduğunda bu asla iyi bir şey değildir.

Suç içeren işlemlerde Bitcoin'i kullanmanın kilit noktası şudur: kayıt sonsuza kadar herkesin görebileceği şekilde ortadadır. Mevcut karıştırma teknikleri blokzincirindeki işlemleri gizleyebilir, hatta işlemleri belirli bir hesapla ilişkilendirmenin imkânsız olabileceği noktaya kadar götürebilir. Ama bu Bitcoin blokzinciri dışındaki takip tekniklerini ya da gelecekte geliştirilecek teknikleri açıklamaz.

Bitcoin şu anda gelişmekte olan tek teknoloji değildir. Büyük veri bir diğer önemli teknoloji ve bir şekilde blokzinciriyle birleşmesi kaçınılmaz. Eğer biri devasa internet takip operasyonlarındaki verileri kullanırsa, birinin gerçek hayattaki kimliğiyle Bitcoin cüzdanını ilişkilendirmek çok daha kolaylaşır.

Blockchain Factory'nin (ağırlıklı olarak blokzincirinde bulunan işe yarar verileri yaymaya odaklanan kurumlar arası bir hizmet) kurucu ortağı Nathan Wosnack şöyle diyor:

> Halka açık ve kayıtları sabit, ayrıca [blokzincir gibi] herkes tarafından denetlenebilen bir hesap defteri üzerindeki anonimlik hakkındaki yorumların modern şehir efsanelerinden öteye gitmeyen saçmalıklar olduğunu düşünüyorum. [...] Karıştırıcı kullanmak yardımcı oluyor ama bunların bile hedeflenen kişileri ya da büyük veriyi analiz etmek ve tarafların kimler ve nerede olduklarını ve ne alıp sattıklarını kabaca çözmek için güvenlik güçleri tarafından kullanılan ve geliştirilen karmaşık adli hesap araçlarından birini kurtarabileceğine henüz ikna olmadım.

Geleceği yüzde yüz doğrulukla öngörmek imkânsız-

dır. Gelecekte blokzincirini ne tür araçlarla tarayacağımızı bilmiyoruz. Bu sebepten, ciddi suçların takibi mümkün olmayan nakit parayla gerçek dünyada işlenmeleri muhtemelen daha iyi olacak. Kredi kartı ya da banka havalesi yerine Bitcoin kullanmak daha avantajlı görünebilir, ki birçok açıdan öyle, ama geleneksel işlemlerin kayıtları eninde sonunda silinebilir ya da örtbas edilebilir. Bankaların kayıtları sadece beş sene tutmaları gerekiyor. Bundan daha uzun süre tutabilirler ama tutmamaları mümkün. Bitcoin'le, o işlemler hiçbir zaman kaybolmayacaklar. İşlemlere dahil olan insanlar isteseler de istemeseler de, sonsuza kadar Bitcoin tarihinin birer parçası olacaklar. Kripto paraların sözünün geçeceği gelecekte, rakipleri ya da medya dedektifleri tarafından siyasi adayların Bitcoin geçmişlerinin ortaya dökülmesini beklemek hiç mantıksız olmaz.

İpucu arayacakları tek yer blokzinciri olmayacak. Blokzinciriyle etkileşim içinde olmak genellikle internetle etkileşim içinde olmak anlamına gelir. Her etkileşim sızıntılı bir tarayıcı, gizlenmemiş bir IP adresi ya da bir düzine farklı yöntem aracılığıyla kullanıcının kimliğini ortaya çıkarma potansiyeli taşır. İnternet anonim değildir, o nedenle kimliğinizden ödün vermeden –Bitcoin ekosistemiyle etkileşim içinde olmak da buna dahildir– herhangi bir şey yapmanız zordur. Şu anda bir insanın yapabileceği en güvenli şey, sadece bir flash bellekte ya da diğer depolama araçlarında var olan ve üst üste veri yazan bir işletim sistemi olan (her kullanıldığında işletim sisteminin dışındaki veriyi silen) TailsOS kullanmaktır. Diğer gizlilik teknikleriyle birlikte kullanıldığında, TailsOS hükümeti ya da diğer casusları bile atlatabilir. Günümüzde Snowden Bel-

geleri olarak bilinen verileri sızdırırken gizliliğini korumasına yardımcı olan TailsOS Edward Snowden tarafından övüldü.[5]

Hükümet onayı olmadan ülke dışına para çıkarmak için Bitcoin'den yararlanabilen insanlar zaten çaktırmadan hareket eden kişiler. Bir insanın başka bir ülkeye göç etmeden önce bütün birikimlerini vergi ödemeden ülkenin dışına çıkarmasını önlemek birçoğumuzun önüne geçmek için endişelendiği maddi suçlardan biri değil. Yine de, Bitcoin ağının küçük işlemlerin yanı sıra, en çok bu tür orta ölçekli işlemlere olanak sağlaması mümkün. Bitcoin normal insanların 'para aklama' kelimelerini duyduklarında düşündükleri multi milyon dolarlık işlemler için nakit paradan daha az etkili olacak. Elbette, para aklandıktan sonra, nakit dolu bir evrak çantasında taşımaktan daha kolay olur. Ama asıl mesele, o paranın gerçek bir kişi ya da şirket kimliğiyle ilişkilendirilmeden ağa nasıl taşınacağıdır.

Nakit karşılığı yüzlerce bin dolarlık Bitcoin satmak için bekleyen çok sayıda insan olduğu söylenemez. Böyle bir balina bulmak için çevrimiçi olmalısınız ve çevrimiçi olmak kayıt yaratır.

Potansiyel olarak, Bitcoin'in sözünün geçtiği bir dünya yüklü miktarda para aklayanlar için çok zor olur. Bitcoin gibi bir para birimi geleneksel yasal para birimlerinin yerini alır ya da onları önemli ölçüde tamamlarsa, halka açık şirketlerin kamu harcamalarını blokzincirinde tutmaları

[5]Higgins, Parker. "The 7 Privacy Tools Essential to Making Snowden Documentary CITIZENFOUR." Electronic Frontier Foundation. 29 Ekim 2014. Erişim tarihi 22 Haziran 2015. https://www.eff.org/deeplinks/2014/10/7-privacy-tools-essen- tial-making-citizenfour

mantıklı olur. Seçme şansınız olsa, bütün harcamalarını halkla paylaşan bir şirkete mi, yoksa parasını karıştırma hizmetine aktarıp işlemlerini halktan ve hissedarlarından gizleyen bir şirkete mi yatırım yaparsınız?

Aynı şey hayır kuruluşları için de geçerli. İnsanlar parasını nasıl harcadığı konusunda dürüst ve açık olan bir hayır kuruluşuna mı, yoksa blokzinciri kayıtlarını gizlemeye çalışan bir hayır kuruluşuna mı daha çok yardımda bulunurlar?

Sonuçta, Bitcoin hem takma isimli hem de tamamen izi sürülebilir. Bir kullanıcının takip edilebilirliğinin kolaylığı o kullanıcının kendini gizlemek için ne kadar uğraştığına bağlıdır. Görünürdeki bu çelişkiye rağmen, Bitcoin'in takip edilebilirliğinin ve artan gizliliğinin teknolojik gelecekte oynayacak rolleri var.

Yedinci Bölüm

Bitcoin ve Suç Unsurları

Herkes internetin hayatlarımızı değiştirdiğini biliyor, çünkü 1993'ten beri her gün medyadan biri aynı sözü söyleyip duruyor. Ancak, görünüşe bakılırsa, internetin başardığı en büyük şeylerden biri amatör pornoyu normalleştirmesi. World Wide Web üzerindeki çıplak insan sayısını meşru kılmak mümkün değil, birçoğunun da bunu maddi sebeplerden ötürü yapmadığı çok açık (hem de çok!). Bu insanlar on beş sene önce neredeydiler? 1986'da kocalarına dönüp, "Bilirsin, titanyum dildoyu ağzıma sokarken çekilen resimlerime bakarak yabancıların kendilerini tatmin etmelerini çok isterim, ama ne yazık ki, bu tür bir eğlence aracı yok. Sanırım burada oturup yine Şahin Tepesi'ni izlemek zorundayız," diyen milyonlarca kadın gerçekten var mıydı?

— Chuck Klosterman, *Sex, Drugs, and Cocoa Puffs: A Low Culture Manifesto*

Suç unsurlarından bahsetmeden Bitcoin hakkında dü-

rüstçe konuşamazsınız. Bazı Bitcoin savunucuları bu ilişkiyi önemsiz gibi gösterseler de –ve bunun için mantıklı iddiaları olsa da– suç dünyasının Bitcoin'le olan ilişkisi göz ardı edilemez.

Bitcoin suç oluşturan işlemleri kolaylaştırmaya yardımcı oluyor. Bunu inkâr etmenin bir anlamı yok, çünkü uyuşturucu ve diğer yasa dışı mallar ve hizmetler sunan Derin Ağ pazarlarında birkaç dakika geçirmek Bitcoin'in bu tür şeylerdeki rolünü anlamak için yeterlidir. (Derin Ağ, internetin geleneksel arama motorları tarafından indekslenmeyen kısmıdır.) Ancak, aynı şekilde nakit paranın da suç oluşturan işlemlere yardımcı olduğunu söylemek doğru olur. Nakit paranın yasa dışı mal ve hizmetlerin alım-satımında hâlâ başlıca yöntem olduğunu anlamak için herhangi bir metropolün merkezindeki belirli bir caddede bir süre vakit geçirmek yeterlidir.

Bu bölümü nasıl ele alacağım konusunda kendi kendime uzun uzun tartıştım. İnternetin suç unsurları Bitcoin'in ilk fiyat belirlemesinde ve benimsenmesinde hiç şüphesiz önemli rol oynadı, ama olanak sağladığı suçların Bitcoin olmadan çevrimiçi ya da sokakta olmayacağını ima etmek istemiyorum. Bitcoin kullanıcılarının hepsinin –ya da büyük bir bölümünün– Derin Ağ'da ya da başka bir yerde suç faaliyetlerine karıştıklarını da ima etmek istemiyorum. Bitcoin'in göreceli olarak daha anonim olması sebebiyle, Derin Ağ'daki gizli işlemler ilk kullanım alanlarından biriydi ama o zamandan bu yana para birimi yasal müşterilerin, serbest çalışanların ve personellerin kullandığı yasalara uygun bir ödeme yöntemi haline geldi.

Yine de, suç Bitcoin'in hayatının ilk döneminde etkiliydi ve gelecekte de etken olmaya devam edecek.

Silk Road (İpek Yolu)

'Açık ağ' adı verilen şey internetin sadece küçük bir bölümünü oluşturur. Açık ağın altında çok az kişinin görebileceği bir veri denizi bulunur. Bu banka işlemleri, şirket işlemleri, elektronik postalar, IRC sohbet odaları, Usenet toplulukları, akademik ve kurumsal dahili ağlar, Google ya da diğer büyük arama motorunun indekslemediği diğer birçok şeyden oluşur ve buna Derin Ağ denir.

Bitcoin'in popüler olmasının ilk nedenlerinden biri dijital para birimi olarak Karanlık Ağ olarak bilinen –Derin Ağ'ın küçük bir bölümü– internetin kasten gizlenen kısmında bir grup suçlunun Amerikan gençliğine uyuşturucu satmasına olanak tanımasıdır. Birkaç yayımın dışında, ilk haberlerin büyük bir bölümü panik dolu "internette uyuşturucu satılıyor" ve "tuhaf bir internet parası bunu gerçekleştiriyor" iddialarına odaklanmıştı.

İkinci düşünce yanlış. İnternet her zaman uyuşturucu ve yasa dışı mallar satmak için kullanıldı. Uyuşturucu tarayıcılar ortaya çıkmadan önceki Usenet günlerinde bile internet aracılığıyla satılıyordu. Federaller farklı sistemlerdeki uyuşturucu işlemlerini önlemek için her ne kadar uğraşsalar da, bazı uyuşturucular her zaman gözden kaçmayı başardılar. Günümüzde bile, uyuşturucu satışları Derin Ağ'la sınırlı değil. Doğru sayılara ulaşmak imkânsız ama açık internetin de –'internet' sözcüğünü duyan birçok insanın düşündüğü şey– uyuşturucu satışı için en az Derin Ağ kadar kullanıldığı iddia edilebilir. Silk Road gibi çevrimiçi piyasalarda milyarlar harcansa da, birçok uyuşturucu satıcısı onlardan faydalanabilecek kadar teknoloji meraklısı değildir. Ancak Facebook, Instagram, Craigslist ve di-

ğer birçok siteyi kullanacak kadar teknolojiden anlıyorlar. Eylül 2014'te, *Venture Beat*'ten Fletcher Babb, "Instagram uyuşturucu ticareti için bir altın çağ başlattı," iddiasıyla bir makaleye başladı.[1]

Aynı şey ilk kez popüler akıma ve farkındalığa girdiklerinde Silk Road ve Bitcoin için de söylendi. Babb Instagram hakkında böyle bir şey söylediğinde abartıydı ama Silk Road için aynı şeyi söylemek o kadar abartı sayılmasa da, internetteki uyuşturucu ticaretinin yükselişi yüzünden bu hizmetleri suçlamak abartı olur.

Instagram uyuşturucu satmak için kullanılıyor. Diğer birçok şey için de kullanılıyor: kısa süre önce pişirilen bir yemek için inceden böbürlenmek ya da milyonlarca formsuz ziyaretçiye çekici spor gurularına arzuyla bakma fırsatı vermek için. Aynı zamanda uyuşturucu satmak için de kullanılıyor ama Şubat 2014'te Bitcoin'in yasaklanması için çağrıda bulunan Batı Virginia Senatör'ü Joe Manchin gibi, hiç kimse kapatılması ya da yasaklanması için çağrıda bulunmuyor.[2]

Bitcoin ve Derin Ağ aynı zamanda tamamen yasal amaçlar için kullanılıyorlar. Derin Ağ'ın boyutu hakkında sağlam tahminler yok ama her gün dolaştığımızı internetten daha büyük bir ölçekte olduğu konusunda herkes

---

[1]Babb, Fletcher. "Instagram Has a Drug Problem." VentureBeat. 19 Eylül 2014. Erişim tarihi 22 Haziran 2015. http://venturebeat.com/2014/09/19/instagram-has-a-drug-problem/

[2]Fung, Brian. "Sen. Joe Manchin Calls for a Bitcoin Ban as Regulators Seek 'Accelerated Push'." Washington Post. 26 Şubat 2014. Erişim tarihi 22 Haziran 2015. http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/26/sen-joe-manchin-calls-for-a-bitcoin-ban-as-regulators-seek-accelerated-push/

hemfikir. Verilerin çoğu dış taraflar için işe yaramaz ama bu engin bilgi denizinde, insanlar internetin ana akım kullanıcılarından ve emniyet teşkilatlarından gizli ağlar ve hizmetler inşa etmeye başladılar. Bu sitelerin çoğu .onion alan uzantısını kullanıyor ve görünürde rastgele harfler ve sayılardan oluşan uzun URL'ları var.

Derin Ağ'ı kullananların sayısı derinlere gittikçe hiç şüphesiz artsa da, Derin Ağ yasal amaçlara da hizmet ediyor. Wikileaks bir Derin Ağ hizmeti olarak ortaya çıktı. Gazetecilerin bilgiyi anonim bir şekilde yayınlayabilmeleri için kaynaklarla, muhbirlerle iletişim kurabilmeleri ne pahasına olursa olsun özgürlük adına korunması gereken önemli bir araç.

Elbette, gizlilik şifrepunkları, Bitcoin meraklıları ve suçlular dışındaki insanlar için de büyük bir endişe. Dünyanın en büyük kurumları şifrelemenin sadece belirli gruplar için değil, aynı zamanda özgürlük için de vazgeçilmez olduğunu bize hatırlatıyorlar. Mayıs 2015'te, Birleşmiş Milletler şifreleme hakkında gizliliği insani bir hak olarak açıkça doğrulayan özel bir rapor yayınladı.

> Şifreleme ve anonimlik, bunların ardındaki güvenlik kavramlarıyla birlikte, dijital çağda düşünce ve ifade özgürlüğü hakkını uygulayabilmek için gerekli olan gizlilik ve güvenliği sağlıyorlar. Bu tür bir güvenlik ekonomik haklar, gizlilik, yargı süreci, barışçı toplantı ve birleşme özgürlüğü, yaşam ve vücut bütünlüğü hakları da dahil olmak üzere başka birçok hakkı uygulamak için vazgeçilmez olabilir. Düşünce ve ifade özgürlüğü haklarının önemi nedeniyle, şif-

> releme ve anonimlik kısıtlamaları yasallık, gereklilik, orantılılık ve tarafsızlıkta meşruiyet ilkelerine göre katı bir şekilde sınırlandırılmalıdır.

BM Özel Raportörü David Kaye kısa bir süre önce, sözde 'Beş Göz' (gözetimi paylaşma anlaşmasının birer parçası olan Birleşik Devletler, Birleşik Krallık, Avustralya, Yeni Zelanda ve Kanada) tarafından desteklenen politikalara ve şifrelemeye saldırılarına açıkça karşı çıktı. Kaye şöyle diyor:

> Devletlerin güçlü şifrelemeyi ve anonimliği desteklemesi gerekir. Ulusal kanunlar bireylerin dijital iletişimlerini çevrimiçi anonimliğe imkân tanıyan şifreleme teknolojileri ve araçları kullanarak korumakta özgür olduklarını kabul etmelidir. [...] Devletler, gizli erişimler, zayıf şifreleme standartları ve anahtar emaneti gibi bireylerin çevrimiçi sahip oldukları güvenliği zayıflatan bütün önlemlerden kaçınmalılardır.

İnternet savunucuları ve bilgisayar kurtlarının şifrelemenin gizlilik için ne kadar önemli olduğu hakkında konuştuklarını duymayı bekleyebiliriz, ama aynı şey BM gibi eski kafalı, ana akım ve uluslararası bir oluşum tarafından yankılandığında mesele gerçekten anlaşılıyor.[3]

Peki, bunun Bitcoin ve suç unsurları konusuyla ne ilgisi var?

---

[3]Kaye, David. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. United Nations' Human Rights Council, 22 Mayıs 2015

Görünüşe bakılırsa, çok ilgisi var, çünkü Bitcoin için vazgeçilmez olan şifreleme teknikleri 1990'ların başından beri toplumsal tartışmanın odağı oldu ve bu tartışma şifreleme konusuyla ilgili her şeyi suç faaliyetleri şemsiyesinin altına yerleştirmekle son buldu. Bitcoin ve suç unsurlarının ilişkilendirilmesi bundan kaynaklanıyor.

1995'te, günümüzde var olmayan ancak ilk internet kriptografi şirketlerinden biri olan Cygnus Solutions'ın ofisini ziyaret eden yazar Steven Levy, o dönemin ilk Şifrepunklarının başarmaya çalıştıkları şeyi şöyle anlatıyor:

> Bu odadaki insanlar bir bireyin bilgisel izlerinin –kürtaj hakkındaki görüşünden gerçek bir kürtajın tıbbi kaydına kadar her şeyin– ancak kişi onları açıklamak isterse takip edilebileceği; anlaşılabilir mesajların ağ ve mikrodalga aracılığıyla gezegende dolaşabildiği, ama onları sisin içinden çekip çıkaran davetsiz misafirlerin ve federallerin hiçbir şey anlamayacağı; gözetleme araçlarının gizlilik araçlarına dönüştürüldüğü bir dünya ümit ediyorlar.
>
> Bu hayalin gerçekleşmesinin sadece tek yolu var: şifrelemenin yaygın bir şekilde kullanılması. Bu teknoloji mümkün mü? Kesinlikle. Engeller siyasi: Hükümetteki en etkili kuvvetlerin bazıları bu araçları kontrol etmeye adanmışlar. Kısacası, kriptoyu özgürleştirmek isteyenler ve onu baskı altında tutmak isteyenler arasında bir savaş yaşanıyor. Bu konferans salonuna dağılan görünürde tehlikesiz insanlar kripto yanlısı güçlerin öncü birliklerini temsil ediyorlar. Savaş alanı uzak görünse de, tehlike değil: bu müca-

delenin sonucu toplumumuzun yirmi birinci yüzyılda bize bahşedeceği özgürlüğün miktarını belirleyebilir. Şifrepunkları için özgürlük riske girmeye değer bir meseledir.

"Kalkın," diye teşvik ediyor onlardan biri. "Dikenli tellerinizden başka kaybedecek hiçbir şeyiniz yok."[4]

İnternet ortaya çıkmadan önce, sıradan bir insanın kriptografiye pek ihtiyacı yoktu. Elbette, telefon görüşmeleri dinlenebilir ve kriptoyla güvenceye alınan bir telefon harika olurdu ama hedeflenmiş hükümet gözetiminin üzerlerinde olmasından endişelenen çok az kişi vardı.

Yıllar boyunca, Ulusal Güvenlik Teşkilatı kriptografi konusunda tekeldi. Genellikle, iletişimlerinin diğer hükümetler tarafından izlenmesinden endişelenmek için geçerli sebepleri olan hükümet ajanları kullanırdı. Elektronik iletişimin yükselişte olduğu 1975'te, Whitfield Diffie ilk 'açık anahtar' sistemini icat etti, potansiyel olarak, kriptografi işini yapabilecek bir bilgisayara erişimi olan dünyadaki herkesin dünyadaki herhangi biriyle güvenli olarak iletişim kurmasına olanak sağlıyordu.

Bu sistem en nihayetinde, şirketlerin ve Phil Zimmerman'ın PGP şifreleme programı gibi hizmetlerin doğmasına neden oldu. Ulusal Güvenlik Teşkilatı'nın hükümete Birleşik Devletler şirketleri tarafından satılan her telefon ve bilgisayara gizli erişim sağlaması için tasarlanan dona-

[4]Levy, Steven. "Crypto Rebels." Wired 1.02. 1 Mayıs 1993. Erişim tarihi 22 Haziran 2015. http://archive.wired.com/wired/archive/1.02/crypto.rebels.html

nım tabanlı kriptografi çözümü Clipper Chip'iyle baş başa gidiyordu.

Clipper Chip'in güvensiz olduğu gösterilirken, PGP ve şifrepunkları savaşı kazandılar. Hükümet destekli gizli erişim kavramı kriptografi topluluğundan silindi. Ancak, bu, Ulusal Güvenlik Teşkilatı'nın güvenlik şirketi RSA'ya gözetleme operasyonlarında faydalanacağı güvenlik açıklarını koruması için para öderken yaptığı gibi kendi gizli erişimlerini sinsice eklemesine engel olmadı.[5][6] Ancak, en sonunda halkın –kalbi olmasa da– zihniyle girdikleri savaşı kaybettikleri söylenebilir. Halk iletişimlerini gizli tutma şansını geri kazansa da, büyük bir bölümü buna gerek olduğunu düşünmedi.

1990'ların ortasından Edward Snowden'in hükümetin yaygın ve yasa dışı bir şekilde casusluk yaptığını ifşa etmesine kadar, halk interneti, elektronik postayı ve diğer elektronik iletişim biçimlerini tamamen şifrelenmemiş bir şekilde kullandı ve birçoğu doğal risklerden habersizdi. Bu sırada, hükümet casusluk yazılımları tasarladı ve teknolojimize gizli erişimler yerleştirdi.

Günümüzde bile, Snowden'in açıklamalarından sonra, kullanıcıların büyük bir bölümü elektronik postalarını hâlâ şifrelenmemiş bir şekilde gönderiyor ve Firefox, Chrome ya da Internet Explorer kullanarak ağda dolaşıyor;

---

[5]Higgins, Parker. "On the Clipper Chip's Birthday, Looking Back on Decades of Key Escrow Failures." Electronic Frontier Foundation. 16 Nisan 2015. Erişim tarihi 22 Haziran 2015. https://www.eff.org/deeplinks/2015/04/clipper-chips-birthday-looking-back-22-years-key-escrow-failures.

[6]Snyder, Brian. "Exclusive: NSA Infiltrated RSA Security More Deeply than Thought- Study." Reuters. 31 Mart 2014. Erişim tarihi 12 Kasım 2015. http://www.reuters.com/article/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331

nadiren ekstra güvenlik özellikleri ekliyorlar. Güvenlik düşünülerek tasarlanan tarayıcılar bütün internet kullanımının yüzde birinden daha azını oluşturuyor.

90'lı yılların başındaki şifrepunkları ve kriptocular gizlilik araçlarını kullanma hakkımız için mücadele verdiler; günümüzün korsanları ve tamircileri bunu genişlettiler. Onlar için mücadele sadece gizlilik araçlarını kullanma hakkından ibaret değildi, aynı zamanda matematik yardımıyla yaratılan her aracı kullanma hakkını kapsıyordu.

Bitcoin topluluğunda ortak bir görüşe benzer bir şey olmadığının altı çizilmelidir. Basının topluluğu radikal özgürlükçüler olarak tanımlamasına rağmen, farklı inanç sistemleri ve bağlantıları olan çok sayıda kullanıcı var.

Aynı şekilde, özgürlükçülerin büyük bir bölümü kripto para topluluğundaki bazı insanlar kadar radikal değiller. Ama kripto özgürlükçülerin arasında da yazılımı belirli bir yöne doğru iten tutarlı ve açık ilkeleri olan bir grup var.

Bu gruba genellikle özgürlükçü deniyor, ama bu isim tam olarak doğru değil. Son gelişmeler göz önüne alındığında, bu tür tanımlar kullanmak anlamsız olabilir. Ekim 2014'te CoinTelegraph'ın serbest kürsü sayfasında, kapitalizm ve komünizmin karşılaştırıldığı eski argümanların neden sona ermek üzere olduğuna dair görüşümü açıkladım:

> Blokzinciri geleceğine doğru ilerlerken, her ikisinden de [hem kapitalizm hem de komünizm] daha üstün olan yeni hükümet sistemleri yükselişe geçecek.
>
> Serbest piyasa ekonomisinin bireysel özgürlüğü-

nü sağlarken, her vatandaşın temel ihtiyaçlarını karşılayacak kadar ekstra servet üreten [bir blokzinciri hükümeti] görebiliriz.

O nedenle, hükümetten ziyade matematiğin onlara getirdiği sınırlardan endişelenen bu gruba özgürlükçü değil, kriptocu demeyi tercih ediyorum. Açık kaynak yazılımlar arayışlarında güçlü bir araç çıktı.

Alex Winter'ın yönettiği belgesel *Derin Ağ*, OpenBazaar geliştiricisi Amir Taaki'den bir alıntıyla başlıyor: "Faşistlerin kaynakları olabilir, ama bizim hayal gücümüz var. Bağımsızlığımızı geri almak için araçlar yapıyoruz."[7]

Silk Road'un arkasında da benzer bir felsefe vardı. Aynı zamanda, Brian Hoffman'ın OpenBazaar'ını, Cody Wilson'ın üç boyutu yazıcıda bastığı silahını, Darkwallet'ı ve bütün hayatlarını mevcut durumu korumaya adayan insanları korkutan diğer bir düzine aracı motive etmeye devam ediyor.

Silk Road kontrolsüz bir pazar ve birçoğu *Derin Ağ* belgeselinde Amir Taaki'nin anlattığı felsefeye inanan benzer görüşte insanların buluşma yeriydi. FBI ajanları 2 Ekim 2013'te Ross William Ulbricht'i tutukladılar ve onu internetin en büyük yer altı pazarı Silk Road'un ele geçirilmesi zor idarecisi, kötü şöhretli Dread Pirate Roberts olmakla suçladılar. 4 Şubat 2015'te, narkotik madde dağıtmak için kumpas kurmak, para aklamak, korsanlık yapmak ve 'bir suç girişimini devam ettirmek' –normalde uyuşturucu çeteleri ve mafya gibi suç örgütlerinin liderlerine ayrılan

[7]Deep Web. Yönetmen Alex Winter. Anlatıcılar Cindy Cohn, Andy Greenberg. Epix, 2015.VoD.

'en nüfuzlu kişi' olarak bilinen konum– dahil olmak üzere kendisine yöneltilen yedi suçlamanın hepsinden suçlu bulundu. Ardından, 29 Mayıs'ta kefaletle serbest bırakılma şansı olmadan ömür boyu hapse mahkûm edildi. Yargıç Katherine B. Forrest genç adamı ibret olsun diye cezalandırdığını ima etti.

> Kanunsuzluğa tahammül edilmeyeceğinden hiç kimsenin şüphesi olmasın. Eğitimi ya da ayrıcalıklarına bakılmaksızın hiç kimsenin kanundan daha üstün olmadığından şüpheniz olmasın. Kanun önünde herkes eşittir. Devasa bir suç müessesesini yönetilemeyeceği ve her şeyin internet üzerinde olmasının işlenen suçun hafiflemeyeceğinden kimsenin şüphesi olmasın.[8]

Ancak, Ulbricht'e karşı açılan davadaki bazı iddialar o kadar kolay açık değildi. Ulbricht'in Silk Road'la bağlantısının olmadığını iddia etmek zor olsa da, kanıtların nasıl ve kimler tarafından toplandığına ve tam olarak neyi kanıtladıklarına dair bazı sorular var.

Ulbricht'in davasını ele almadan önce, Silk Road pazarını kısaca özetleyeceğim. Daha önce de bahsettiğim gibi, Silk Road Derin Ağ'da gizli bir hizmetti. Birçok Derin Ağ hizmeti gibi, sadece, aslen ya Birleşik Devletler Donanma-

[8]"Dread Pirate Roberts takma adıyla bilinen Ross Ulbricht, Manhattan Federal Mahkemesi tarafından ömür boyu hapse mahkûm edildi." FBI. 29 Mayıs 2015. Erişim tarihi 22 Haziran 2015. https://www.fbi.gov/newyork/press-releases/2015/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison

sı ya da CIA tarafından geliştirilen –hangi kaynağa inandığınıza bağlı– Tor ağ tarayıcısı kullanılarak ulaşılabiliyordu. Rahatlıkla takip edilebilen normal internet üzerinden mesaj göndermeden güvenilir bir iletişim yolu sağlaması için geliştirilmişti.

Zaman içerisinde açık kaynağa dönüştü ve güvenli anonim iletişime imkân tanırken kontrol edilemeyecek boyuta ulaştı. Tor şu anda gazeteciler, gizlilik savunucuları, taciz kurbanları ve anonim kalmak isteyen insanlar tarafından kullanılıyor.

Bunun hükümet için teşkil ettiği sorun, Tor gibi hizmetlerin güvenlik teşkilatlarının faaliyetlerini baltalamasıdır. *Derin Ağ* yönetmeni Alex Winter'a göre, bu etki ancak dev bürokrasilerde mümkün olan bir tür çıkar çatışmasına sebep oldu. Filmin ilk gösteriminden sonra Epix'te yönetmenle sohbet sırasında, Winter hükümetin belirli bölümleri Tor'un kriptosunu baltalamak için uğraşırken, diğer bölümlerinin Tor'un gizlilik özeliklerini artırmak için çabaladıklarını iddia etti.

Buna inanan tek kişi Winter değil. Tor yöneticisi Roger Dingledine, Ulusal Güvenlik Bakanlığı ve Birleşik Krallık İstihbarat Kurumu'nun Tor'u baltalamak için bir yazılım yaydıklarını ileri sürdü. Bu sırada, Birleşik Devletler hükümeti Tor'u geliştirme fonunu 2013'te 1.8 milyon dolara yükseltti.[9]

Silk Road'a geri dönelim. Derin Ağ'a gizli bir pazar olarak hizmet veriyordu ve sadece Tor aracılığıyla ulaşılabili-

[9]Kelion, Leo. "NSA and GCHQ Agents 'leak Tor Bugs', Alleges Developer - BBC News." BBC News. 22 Ağustos 2014. Erişim tarihi 22 Haziran 2015. http://www.bbc.com/news/ technology-28886462

yordu. İnsanların neredeyse her şeyi almalarına ve satmalarına imkân tanıyordu ama en çok yasa dışı ve gri borsa ilaçların satışı için kullanılıyordu. Alıcılar ve satıcılar PGP teknolojisi kullanarak iletişim kuruyor ve Bitcoin kullanarak işlemleri tamamlıyorlardı. İnternet anonimliğinin kalesiydi ve ilk başta yetkililer bu konuda ne yapacaklarını bilemediler.

New York Senatörü Charles Schumer harekete geçip federal hükümetten siteyi kapatmasını talep etti ve sonra gidip izleyen bütün gençlere çevrimiçi uyuşturucu sipariş etmenin ne kadar kolay olduğunu gösterdi.[10]

Polis teşkilatı ilk başta Silk Road'a da diğer suç örgütlerine sızdıkları gibi –örgütün bir üyesiymiş gibi yaparak– sızdılar. Kullanıcı adı Chronicpain olan bir satıcıyı bulmayı başardılar; onun ve diğer satıcıların hesaplarını ele geçirdiler ama bu hesapların sahiplerini tutuklamadılar. Daha sonra, Dread Pirate Roberts'la iletişime geçmeyi başardılar ve çok sayıda suçla ilgisi olduğunu gösterdiler.

Basının en çok ilgi gösterdiği ve Ross Ulbricht'in kefaletle serbest bırakılmasının reddedilmesi için kullanılan suç sözde sipariş edilen üç cinayetti. Hükümetin kayıtlarına göre, Dread Pirate Roberts üç kişinin ölmesini emretmişti: Birincisi hırsızlık yapan biri, ikincisi tanık olan eski bir satıcı ve üçüncüsü bir şantajcıydı.

En sonunda toplam kiralık katil sayısı altıya yükseldi ve Ulbricht'in 'toplum için tehdit oluşturduğuna' karar verildi, kefaletle serbest kalma talebi reddedildi. Çok geç-

[10]"Schumer Pushes to Shut Down Online Drug Marketplace." NBC New York. Erişim tarihi 6 Şubat 2016. http://www.nbcnewyork.com/news/local/Schumer-Calls-on-Feds-to-Shut-Down-Online-Drug-Marketplace-123187958.html

meden, hükümet kiralık katil tutma suçlamalarını düşürdü ama yine de Ulbricht'in şartlı tahliye edilmesine engel olmayı başardılar ve onu alenen acımasız bir katil olarak gösterdiler.

Birçok kişi hükümetin suçlamaları düşürmesinin sebebinin tutma ihtimallerinin olmaması olduğundan şüphelendi.

Silk Road davasını araştırmaktan ciddi ölçüde sorumlu iki hükümet ajanının davranışları ve Dread Pirate Roberts'la doğrudan iletişimde olmaları davaya gölge düşürdü. Mart 2015'te, Gizli Servis Ajanı Shaun Bridges ve Narkotik Ajanı Carl Mark Forve IV tutuklandılar, kara para aklamak ve elektronik dolandırıcılıkla suçlandılar. Force, ayrıca, kamu malı hırsızlığı ve çıkar çatışmasıyla suçlandı. Bridges'ın 800,000 dolar değerinde bitcoin çaldığı ve onu şahsi hesabına aktardığı iddia edildi. Force'un da bitcoin çaldığı ve Dread Pirate Roberts'tan ödeme almak, Silk Road'dan çalmak ve Dread Pirate Roberts/Ulbricht'e soruşturma hakkında bilgi satmak da dahil olmak üzere çok daha fazla suça karıştığı iddia edildi. Ayrıca, farklı bir kimlik altında Dread Pirate Roberts'a şantaj yapmaya çalıştığı öne sürüldü. Buna ek olarak, Dread Pirate Roberts'ın kiralık katil ya da cinayet için arabulucu olarak tutmaya çalıştığı ajan Force'tu.

Buradaki sorunu anlamış olabilirsiniz. Bridges'in Silk Road'dan para çaldığı ve sonra Force'un parayı çaldığını iddia ettiği kişiyi –bir Silk Road çalışanını– öldürmek için Dread Pirate Roberts'dan ödeme aldığı söyleniyor. Force'un ayrıca tanık olan satıcıyı öldürmesi için de para aldığı ve ölümünü tertiplemeye yardım ettiği söyleniyor. Daha sonra Dread Pirate Roberts'a şantaj yaptığı ve hayali şan-

tajcıyı öldürmek için ondan para aldığı iddia ediliyor. Bu parayı amirlerine vermek yerine, Force'un çoğunu elinde tuttuğu söyleniyor.

Force'a karşı yeminli ifadede, Dread Pirate Roberts'ı PGP kullanmaya teşvik ettiği ve amirlerine özel anahtarı vermediği belirtiliyor. Durum bundan daha da kötüye gidiyor. Force'un Silk Road'da tek bir kimliğinin olmasına izin verilmişti: Nob. Soruşturmacılar artık sitede birden fazla 'çorap kukla' hesabı olduğuna ve onları ve emniyet teşkilatındaki bağlantılarını kişisel çıkarları için kullandığına inanıyorlar.[11]

Adalet Bakanlığı'nın basın duyurusunda şöyle ifade ediliyor:

> Force'un soruşturmanın hedefindeki kişiye hükümetle ilgili bilgiler sattığı iddia edildi. Şikâyet dilekçesi aynı zamanda Force'un Uyuşturucu ile Mücadele Dairesi'nde çalışırken yatırım yaptığı bir dijital para birimin borsa şirketinde de çalıştığını ve şirketi hiçbir yasal dayanağı olmadan bir müşterinin hesabını dondurmaya zorladığını ve sonra müşterinin fonlarını kendi hesabına aktardığını öne sürüyor. Dahası, Force'un çevrimiçi bir ödeme hizmetine kişisel hesabının blokesini kaldırması için Adalet Bakanlığı'ndan yetkisiz bir celp gönderdiği iddia ediliyor.

Özetle, şartlı tahliye talebi reddedilen Ross Ulbricht, basında bir katil olarak resmedildi, çünkü çevrimiçi kişi

[11]Jeong, Sarah. "Criminal Charges Against Agents Reveal Staggering Corruption in the Silk Road Investigation." Forbes. 31 Mart 2015. Erişim tarihi 22 Haziran 2015. http:// www.forbes.com/sites/sarahjeong/2015/03/31/force-and-bridges/

Dread Pirate Robert ya gerçekte hiç olmayan ya da hükümet ajanlarının eylemleri olan suçların karşılığında var olmayan iki kişiyi öldürmesi için hayali bir kiralık katil tutmuştu. Tutuklanmasından sorumlu iki ajan –hükümetin itiraflarına göre– tamamen ahlaksızdı ve aktif olarak davadaki kanıtları saklamak için uğraşıyorlardı. Kiralık katil tutma suçlaması mahkemede hiçbir zaman kanıtlanmadı ama yine de, hem görünürde tarafsız olan yargıcın hem de halkın görüşünü etkiledi.

Ekim 2013'te tutuklandığı gün, Ross Ulbricht San Francisco kütüphanesinde diz üstü bilgisayarı açık bir şekilde oturuyordu. Yetkililer bilgisayarını kapatmasına izin verirlerse, verinin şifreleneceğini ve onun izini süremeyeceklerini düşündüler. (Jacob Müller-Maguhn'un dikkat çektiği gibi, "Kişi kriptografi söz konusu olduğunda şiddetin bir matematik problemini çözmeyeceğini kabullenmelidir.[12]) Dikkatini dağıttıktan sonra, ajanlar diz üstü bilgisayarını kapatamadan Ulbricht'i ondan ayırdıklarını söylüyorlar. İddialara göre Silk Road'da yönetici hesabına bağlıymış; Ulbricht suçüstü yakalanmış gibi görünüyordu.

Ama 2013'te *Forbes*'un Dread Pirate Roberts'la yaptığı bir röportajda, yönetici –*Prenses Gelin* adlı filmdeki bir karakterden gelen– takma ismin eski bir yöneticiden kendisine devredildiğini ve daha sonra onun da başkasına devredeceğini açıkladı.[13]

---

[12]Assange, Julian, Jacob Appelbaum, Andy Müller-Maguhn ve Je´re´mie Zimmermann. Cypherpunks: Freedom and the Future of the Internet. New York: OR Books, 2012.

[13]Greenberg, Andy. "An Interview With A Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A)." Forbes. 14 Ağustos 2013. Erişim tarihi 22 Haziran 2015. http:// www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-

Ulbricht'un savunma avukatları, Ulbricht'in bir zamanlar Silk Road'un başında olduğunu ama popülerliği artınca ayrıldığını iddia etmeye çalıştılar.

Savunma suçlu olarak tuzak kurulabilmesi için cezbedilerek geri çekildiğini iddia etti. Açıklama göründüğü kadar inanılmaz değil. Force (iddialara göre) gerçek Dread Pirate Roberts'a içeriden bilgi sızdırıyordu. Suçlandı ve en sonunda Dread Pirate Roberts'la konuşmalarının belirli içeriklerini gizlediğini, para aldığını itiraf etti.

Gerçek Dread Pirate Roberts'ın Force'la işbirliği yaparak Ross Ulbricht'i Silk Road'a geri dönmeye ikna edip bilgisayarına bu bilgiyi yerleştirmiş olması mümkün mü? Ulbricht'in dizüstü bilgisayarında iddia edilen suç faaliyetlerinin detaylı bir kaydı bulunmuş, ama onun gibi eğitimli birinin böyle bir kaydı şifrelenmemiş bir şekilde bırakması ne kadar olası? Ulbricht'in avukatları onun müvekkillerinin bilgisayarına yerleştirilmiş olabileceğini iddia ettiler.

Akranlarından oluşan bir jüri Ulbricht'i kendisine yöneltilen bütün suçlamalardan onu suçlu buldu ama savunmasının iki ajanın görevlerini kötü kullanmalarından ya da *Forbes* röportajından jüriye bahsetmesi engellendi. Hükümet Silk Road sunucularının yerini bulduğunu ve böylece Silk Road'daki 'güvenlik kodu açığı' sayesinde bütün kanıtlara ulaştığını iddia etti. (Güvenlik kodu robot olmadığınızı kanıtlamanız için bir web sitesine girmek zorunda olduğunuz bir dizi harf ya da sayıdır; güvenlik kodu açığı ise site hakkında tanımlayıcı bilgiler verir.) Bu iddia birçok çevrimiçi güvenlik uzmanı tarafından geçersiz sayıldı[14] ama savunmanın bu açıklamayla çelişecek olan

[14]Cubrilovic, Nik. "Analyzing the FBI's Explanation of How They Located Silk Road." New Web Order. 7 Eylül 2014. Erişim tarihi 22 Haziran 2015. https://www.nik- cub.com/posts/analyzing-fbi-explanation-silk-road/

tanıklarının ifade vermelerine izin verilmedi. Son olarak, hükümetin kendi soruşturmaları zaman zaman birçok insanın Dread Pirate Roberts olduğundan şüphelendiklerini gösteriyor.

Silk Road Dread Pirate Roberts siteye katılmadan önce faaliyete geçti ve davadaki kanıtlar sitenin liderleri arasındaki bir tartışmanın ardından 'korsan' efsanesinin hızla ortaya çıktığına işaret ediyor. Bu bir spekülasyon, ama anonim ve sürekli değişen bir 'lider' yaratmak domino taşları devrilmeye başladığında bir adamı tuzağa düşürmek için harika bir yol.

Amacım Ross William Ulbricht'i suçlu ya da masum göstermeye çalışmak değil. Bitcoin dünyasındaki diğer birçok skandalda olduğu gibi, sırf bu konu hakkında kocaman bir kitap yazılabilir, yazılmalıdır. Bu kitabı yazdığım sırada, Ulbricht'in temyiz süreci devam ediyor. Söylemeye çalıştığım şey şu: Ulbricht'in gerçek bir savunma sunduğunu görmek güzel olurdu.

Ayrıca, Ulbricht'e mümkün olan en ağır, savcıların istediğinden daha ağır bir ceza verildi. Benzer suçlardan yargılanan bir başka Silk Road satıcısına sadece on yedi ay ceza verildi. O sanık suçunu kabul ettiği için daha kısa bir ceza almasını beklemek mantıklı; ama bu zıtlık çok orantısız. Ulbricht'in cezası anayasal hakkı olan yargılanmayı uygulamaya çalıştığı için ödediği büyük bir bedeldi. Aldığı ceza katillerin ve çocuk istismarcılarının aldığı cezalardan çok daha ağır ve savunma avukatlarının dikkat çektiği gibi, ancak Charles Manson ve benzeri suçlulara layık.

Ulbricht'in ağır cezası sadece işlediği suçlardan kaynaklanıyor gibi görünmüyor. Silk Road ve ardındaki felsefe,

hükümetin gücünü elinden alan bir teknoloji kullanıyor. Hükümet bu tür araçlara sahip olamayacağınızı söylüyor. Silk Road kapatıldı ama yerini Silk Road 2, Sheep Marketplace ve Agora gibi kapanan sitelerden halen işleyen Valhalla, Alpha Bay ve Dream Market gibi onlarca site aldı. Bu siteler de arada sırada kapatılıyorlar, ama ikinci nesil, açık kaynak ve tamamen merkezsizleştirilmiş alternatifler hemen köşede bekliyorlar. Çok yakında, bireysel satıcılar dışında tutuklayabilecekleri kimse olmayacak. Peki hükümet o zaman ne yapacak? Bireysel satıcıları tutuklamak onlarca yıldır sokakta uyuşturucuyla savaşın stratejisi oldu ve sadece en sadık uyuşturucu savaşçıları bunun başarılı olduğunu iddia edebilirler. Çevrimiçi korsanlıkla ele alabileceğimiz doğrudan bir ilişkisi var. Napster kapatıldığında, korsan topluluğu sekteye uğradı. Merkezi sistemler zayıf birer nokta oldular. Merkezi olmayan torrent siteleri ortaya çıktığından bu yana, hükümet ve diğer örgütlerin korsanlığı önlemek için yapabilecekleri pek fazla şey yoktu. Bireysel yükleyicileri hedef aldılar ama bu, çevrimiçi korsanlığın büyümesini yavaşlatmaya yardımcı olmadı.

Diğer Tor Hizmetleri ve Onları Kullanma Yöntemleri

Silk Road'un kapatılması ve Ross Ulbricht'in müebbet hapisle cezalandırılması insanları Tor kullanmaktan vazgeçirmedi ve Bitcoin'in suç faaliyetlerine devam etmesini engelleyemedi. Benzer tasarımlara sahip siteler ve benzer kurallar hâlâ var. Bu kitabı yazdığım sırada, Valhalla ve AlphaBay en popüler ve saygın siteler ama durumları her

an değişebilir. Deepdotweb.com ve Reddit'in altforumları r/Darkmarkets ve r/DarkmarketNoobs Derin Ağ'dan bir şeyler sipariş etmek isteyen insanlar için harika kaynaklardır.

Bu sitelerden sipariş vermek PGP ve Bitcoin kullanmayı gerektiriyor. Bitcoin'in nasıl kullanılacağını bu kitaptan ve internetteki birçok kaynaktan öğrenebilirsiniz. GnuPG (ya da kısaca GPG, genellikle hâlâ PGP denir) GPG yayınlanana kadar dünyanın en popüler ve muhtemelen en güçlü kişisel şifreleme yazılımı olan PGP'nin açık kaynak versiyonudur. Phil Zimmerman tarafından icat edildi ve 2010'da Symantec satın alana kadar PGP Corporation'ın bünyesindeydi.[15]

Windows'un güvensizliği ve Tor'un barındırdığı tehlikeler bilindiği için, gizlilik ve anonimlik hakkında güçlü endişeleri olan kullanıcılar daha önce bahsettiğim TailsOS'yi kullanmak için fazladan çaba harcamalılar.

Bütün olası önlemler alınmasına rağmen, emniyet teşkilatı bu pazarlardaki alıcı ve satıcıların kimliklerini ortaya çıkarmak için elinden gelen her şeyi yapacaktır. Örnek uygulamalardan bazılarını takip ederek belirli bir özgüven edinilse de, bugün güvenli olan bir şey gelecekte güvenli olmayabilir.

Ayrıca, birçok para karıştırma hizmeti Derin Ağ'da gerçekleşiyor. Coin Laundry bir süredir kullanılıyor, ama anonim biri tarafından yönetilen her merkezi Tor hizmetinde olduğu gibi, bu da her an değişebilir.

---

[15]Duncan, Geoff. "Symantec PGP'yi 300 milyon dolara satın aldı." Digital Trends. 29 Nisan 2010. Erişim tarihi 22 Haziran 2015. http://www.digitaltrends.com/computing/symantec-buys-pgp-for-300-million/

Derin Ağ'da uyuşturucu, sahte pasaportlar ve genelde Silk Road'un varislerinde bulunan Netflix hesaplarından çok daha karanlık olan başka yasadışı hizmetler de var. Orada çocuk pornosundan gerçek şiddet ve ölüm sahnelerini içeren filmlere kadar her şey bulunabilir. Bu hizmetlerin Bitcoin topluluğuyla hiçbir ilgisi yok ve neredeyse evrensel olarak üyeleri tarafından kınanırlar. Bitcoin'le olan tek bağlantıları bazen işlemleri gerçekleştirmek için Bitcoin kullanmalarıdır. 2014'ün sonunda, Birleşik Krallık İnternet Gözetim Vakfı çocuk pornosu teşvik eden iki yüzü aşkın sitenin Bitcoin'le ödeme kabul ettiğini ve bunların otuzunun tek ödeme yönteminin Bitcoin olduğunu bulduklarını duyurdu.[16]

Kredi kartı ya da PayPal kabul eden bu tür birçok site var. Emniyet teşkilatı için MasterCard ya da PayPal'ın suçlunun fonlarını dondurmasını ve ödemelerini durdurmasını sağlamak yeterince kolaydır. Ancak merkezi bir yetkilinin olmadığı Bitcoin'de bu imkânsızdır. Bitcoin'in bu özelliği nedeniyle, paranın kullanımındaki potansiyel problemlere rağmen, gelecekte ödeme yöntemi olarak Bitcoin'i kabul eden daha fazla itibarsız site görmeyi bekleyebilirsiniz.

Uzun vadede, Bitcoin'in benimsenmesi suçlularla mücadelede işe yarayabilir. Blokzinciri analiz teknolojisi ilerledikçe, gelecekte bundan öğrenilebilecekleri kestirmek imkânsızdır ve kendini işine adamış bir dedektifin işlemlerden kocaman bir ağaç oluşturması tek bir hataya bakabilir. Bir başka deyişle, tek bir işlemle kimliğinizi bir

[16]Hern, Alex. "Pedofililer Bitcoin Karşılığında Çocuk İstismarı Görüntüleri Satıyorlar." The Guardian. 14 Nisan 2015. http://www.theguardian.com/technology/2015/apr/14/paedophiles-sell-child-abuse-images-for-bitcoin

kez açığa çıkarırsanız –paralarınızı karıştırmayabilir, IP adresinizi açığa vurabilir ya da bir cüzdan oluşturmaya kalkabilirsiniz– bir dedektif diğer cüzdanların düzinelerce işlemini takip ederek bağlantı kurmaya başlayabilir ve sonuçta işlemlerinize ulaşabilir.

Gri bölgede varlığını sürdüren siteler de var. Bitcoin karıştırma hizmetleri ve daha önce bahsettiğim yasal ama politik, ahlaki ya da kültürel olarak tartışılabilir olan forumlar gibi.

Ama Tor ve Derin Ağ'ın toplum için yaptıkları iyi şeyleri de unutmamalıyız. En karanlık köşelerindeki çirkin ve iğrenç unsurlara rağmen, Derin Ağ gizliliğin yoksun olduğu bir dijital dünyada onun kalesi oldu.

Derin Ağ toplulukları devrim niteliğinde kitap kulüpleri, hafif cinsel fetiş blogları, '90'lı yılların başı ve ortasında hüküm süren ilk sohbet odalarını hatırlatan anonim sohbet odaları, anonim sosyal iletişim ağları, toplu kupon satıcıları ve (sandığınızdan daha zararsız) anonim itiraf siteleri içeriyor. Hatta Virginia Tech'in buhar tünellerini keşfe çıkmanın kurbansız suçu hakkında bir blog bile var.

Bunlar küçük şeyler gibi görünebilirler ama onlar kültürümüzün başka bir şekilde var olma ihtimali olmayan altkümeleri. Bazı şeyler yasal olsa da utanç verici olabilir. Herkes Yahoo! Answers'a girip hemoroidi hakkında soru sormak, en derin paranoyalarını ya da rağbet görmeyen siyasi düşüncelerini paylaşmak istemiyor.

Derin Ağ aynı zamanda baskı altındaki insanların hükümetleri aleyhinde konuşmalarına yardımcı oldu. Türkiye, Twitter ve YouTube'u kapatmaya kalkıştığında, Tor hükümetin güvenlik duvarını aşmanın en iyi yoluydu. Çok

sayıda ana akım basın kuruluşu muhbirlerin kimliklerini açığa vurmadan bilgi sızdırabilecekleri gizli Tor hizmet siteleri kurdular.

Derin Ağ'da balık tutma tecrübesi Google işimizi kolaylaştırmadan önce internette dolaşmaya benziyor. Gerçek anonimlikle birlikte gelen özgürlük hem güçlü hem de iyi ve kötü sonuçları olabiliyor ve bu yakın gelecekte değişmeyecek.

Bitcoin'in suç faaliyetleriyle olan bağlantısı Derin Ağ'la sınırlı değil. Bitcoin kötü amaçlı yazılım, fidye yazılım ve gri pazar hizmetlerinde giderek büyük bir rol oynuyor.

Çevrimiçi kumar, Bitcoin'in ilk ve en açık kullanım alanlarından biriydi, bu trend ilk kumar siteleri internette belirdiğinden beri bütün hızıyla devam etti. Günümüzde, neredeyse her etkinlik için Bitcoin kullanılarak bahse girilebilir ve neredeyse her kumar oyunu oynanabilir. Belirli etkinlikler üzerine bahse girmenize imkân tanıyan eşler arası bahis siteleri bile var. Başkanlık seçimi sonuçlarından tutuklanan bir sonraki ünlünün kim olacağı ya da ertesi gün Las Vegas'ta yağmur yağıp yağmayacağı gibi. Sizinle bu bahse girecek birini bulduğunuz sürece, üçüncü parti emanet sistemi kullanarak bir Bitcoin bahsine girmeniz mümkün.

Yasal porno alanında Bitcoin çok sık kullanılıyor ve bu alan büyümeye devam ediyor. Artık daha fazla porno sitesi Bitcoin kabul ediyor, içerikleri yasa dışı olduğu için değil, Bitcoin müşterilerin olası bir utanç verici kredi kartı ekstresiyle karşılaşmalarını engelleyip kredi kartlarından fazla para çekilmesi riskini önlediği için.

Ama internetteki en sık rastlanan yasa dışı Bitcoin faa-

liyeti insanları bitcoin için dolandırmaktır. Birçok kişinin düşüncesine göre, bu Bitcoin ekosistemi için en büyük tehlikeyi oluşturuyor. Bitcoin sürekli yeni insanların ilgisini çekiyor ve bu insanların kripto topluluğu hakkındaki ilk düşünceleri genelde negatif oluyor.

Bitcoin odaklı kötü amaçlı yazılımların popülerliği artıyor. En sık başvurulan taktikler gizli madencilik yazılımı yüklemek ve önemli dosyaları şifreleyip onları fidye karşılığında tutmayı içeriyor.

Son örnek en korkutucu olanıdır. Kötü amaçlı yazılım –bu tür 'fidye yazılım' olarak bilinir– kripto yöntemiyle kurbanın dosyalarını şifreler ve dokümanlar ve fotoğraflar gibi önemli gördüğü şeylere odaklanır. Ardından, o dosyaları açan şifre karşılığında Bitcoin'le ödeme talep eder. Yazılım genellikle bir geri sayım aracı içerir ve kurbanı geri sayım sıfıra ulaşırsa dosyaları açma ücretinin yükseleceğiyle tehdit eder.

Güvenlik bloglarına göre, fidyeyi ödeyen kurbanlar dosyalarındaki şifreleri kaldırtmakta genellikle başarısız oluyorlar. Dosyaların üzerindeki şifreleri ücretsiz bir şekilde kaldırmak için çoktan keşfedilen şifreleri kullanan bazı siteler var ama fidye yazılımı neredeyse kırılamaz görülüyor.

Bir başka dolandırma yöntemi, saldırganın bir siteye kaldıramayacağı kadar talep göndererek sitenin kapanmasına neden olduğu (DDOS) dağınık hizmet aksatma saldırısıdır. Bu eski bir yöntem ama saldırganların bitcoin ödemesi talep etmelerine daha sık tanık oluyoruz. Örneğin, kötü şöhretli korsan/şantaj grubu DD4BC kumar sitelerinden başlayıp –yapılan şantajı kamuya ilk duyuran site

nitrogensports.eu da dahil olmak üzere– ve Bitcoin medya siteleri ve diğer hizmetlere geçerek çok sayıda siteye saldırdılar.

Beklendiği gibi, Bitcoin'de de Nijerya prensi dolandırıcılık hikâyeleri var. Bunları genellikle 'gerçek olmayacak kadar iyi' teklifleri sayesinde fark etmek çok kolay. Bitcoin sisteminde kurbanın paralarını ikiye katlayacak bir açık bulduklarını iddia ediyorlar. Elbette, kurban bitcoin'lerini gönderdikten sonra onları bir daha geri alamıyor.

Daha zeki dolandırıcılıkları anlamak o kadar kolay değil. Yeni bir Bitcoin kullanıcısı neyin meşru neyin onları bitcoin'lerinden ayırmak için tasarlandığını çözmekte zorlanabilir, o nedenle her zaman temkinli olmakta fayda var.

Suç unsurları fiyatının belirlenmesinde ve ilk kullanım alanlarını bulmasında Bitcoin'e yardımcı oldular. Geri çevrilemeyen işlemlerde, göreceli anonimlik ve küresel erişim onu belirli suçlar için benzersiz bir şekilde faydalı kılıyor. Ama bir kez daha vurgulamakta fayda var, Bitcoin bu kullanım alanlarını aştı. Yine de, yasal Bitcoin kullanımının yasa dışı alternatiflerinden daha hızlı bir şekilde artmasını beklesem de, daha fazla suçlunun Bitcoin kullanacağını düşünüyorum. Her para birimi suçluları kendine çeker ve Bitcoin de farklı olmadığını kanıtladı.

Bitcoin'i öne çıkaran şey suçlulara olanak tanıması ve aynı zamanda onları engellemesidir. Açık blokzincirine ve her işlemin –suç faaliyetlerine karışanlar da dahil– kaydedilmesine ek olarak, Bitcoin'in suçlular için işleri zorlaştırmasının başka yolları da var.

Kredi kartı sahtekârlığı ve dolandırıcılığı Bitcoin ekosisteminde yer alamaz. Kişisel bilgilerinizi teslim etmek

zorunda olmamanız en büyük avantajlarından biridir. Bitcoin'le çevrimiçi bir şey satın alırsanız ve satıcı bitcoin'lerinizi elinde tutmak isteyen bir dolandırıcı çıkarsa, siparişi iptal edemezsiniz. Ancak, o kişinin sizden başka bir şey alabilme ihtimali hakkında endişelenmenize gerek yok. Kredi kartınızı iptal etmenize ve satıcının söylediğinden daha fazla para çekeceğinden endişelenmenize gerek yok.

Doğru düzgün emanet sistemleri ve cüzdan güvenliğiyle, çevrimiçi alışverişleriniz tamamen güvenli olabilir. Satıcıya, bankaya ya da kredi kartı şirketine güvenmek zorunda değilsiniz. Target'in 2013'te yaptığı gibi,[17] eğer satıcı yüzlerce milyonluk müşteri kaydını kaybederse, bu Target'e korsanların kullanabileceği bilgiler vermemiş olan Bitcoin kullanıcılarını etkilemez.

Yüklü miktarda bitcoin'i güvence altına almanın zorluğu gibi dezavantajlar Bitcoin'in avantajlarını bir nebze gölgeliyor ama daha fazla hizmet geliştikçe, her şey kolaylaşacak.

Kısacası, Bitcoin tam olarak duyurulduğu şey: bir çevrimiçi para birimi. Suçlular için güçlü bir araç olabildiği gibi, finansal gizliliklerini Target ve Apple gibi şirketlere emanet etmek istemeyenler için de güçlü bir araç.

[17]Wallace, Gregory. "Target Credit Card Hack: What You Need to Know." CNNMoney. 23 Aralık 2013. http://money.cnn.com/2013/12/22/news/companies/ target-credit-card-hack/

Sekizinci Bölüm:

Mt. Gox: Bitcoin'in Dönüm Noktası mı?

'Magic: The Gathering Çevrimiçi Borsası' Bitcoin için sistemik bir risk, tacirler için bir ölüm tuzağı ve hiçbir fikri olmayan insanların idare ettiği bir işletmedir.

— Andreas Antonopoulos, BitcoinTalk forum, Nisan 2013

Aslında, bu bölümü üst düzey Bitcoin dolandırıcılıklarına adayacaktım ama çok geçmeden Mt. Gox fiyaskosunu geçiştirmenin okuyuculara haksızlık olacağını anladım. Mt. Gox basit bir hırsızlıktan çok daha fazlasıydı; Bitcoin tarihinde bir dönüm noktasıydı. Hâlâ genç olan para birimi için, olumlu ya da olumsuz, muhtemelen şimdiye kadarki en önemli olaydı. Bitcoin tarihindeki alenen en görünür olay olduğundan hiç şüphe yok, bu başlı başına önemli bir faktör.

Mt. Gox fiyaskosu –gerçek bir fiyaskoydu– hakkında söylenebilecek en iyi şey Bitcoin'i öldürmemiş olmasıdır.

Birçok resmi açıklamaya ve öngörüye rağmen, fiyatı çöküşten önceki zirveye kıyasla sönük kalsa da, Bitcoin daha geniş kitleler tarafından benimsenmeye, geçerli görülmeye ve finanse edilmeye devam etti. Bu istikrar paranın direncini göstermekle kalmıyor, aynı zamanda çok sayıda zengin ve güçlü insanın Bitcoin'e inandıklarını gösteriyor.

Tokyo merkezli Mt. Gox dünyanın en büyük Bitcoin borsasıydı, ancak aylarca süren teknik sorunlardan sonra, borsa kendine ait birkaç yüz bin bitcoin'in yanı sıra, müşterilerinin çoğunun bitcoin'lerini kaybettiğini açıkladı. Toplam kayıp o sıralar 480 milyon dolar değerinde olan 850.000 bitcoin'di. Başarısızlığı öncesinde ve süresince, Mt. Gox borsasını, Jeb McCaleb'den satın alan Mark Karpelès idare ediyordu. Karpelès'in finansal ve teknik suçlardan oluşan bir geçmişi vardı. Bu gerçekleri hiçbir zaman gizlemedi ve herkese açık olan blogunda sık sık onlardan bahsetti ama aynı zamanda geçmişi büyük ölçüde fark edilmedi.

28 Şubat 2014'te, hayatı boyunca hiç olmadığı kadar pişman görünen, bir zamanlar dünyanın en büyük Bitcoin borsasının sıkışan yönetim kurulu başkanı Tokyo yerel mahkemesinde oturmuş 480 milyon dolar değerinde dünyadaki birçok kişinin duymadığı bir para birimini nasıl kaybettiğini açıklıyordu. Mark Karpelès'in şirketi iflas ilan ediyordu ve bilerek ya da bilmeyerek Bitcoin tarihinde bir sayfayı kapatıyordu.[1] 2000'lerin ortasında dahi teknoloji gurularını harekete geçiren ve neredeyse her toplum önüne çıkışında tişört ve kot pantolon giyen Karpelès nihayet

[1]McMillan, Robert. "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster." Wired.com. Conde Nast Digital, 3 Mart 2014. Erişim tarihi 19 Mayıs 2015. http://www. wired.com/2014/03/bitcoin-exchange/

bir takım elbise giymişti. Görünüşündeki bu değişiklik ufak olabilir ama sadece Mt. Gox'un değil aynı zamanda Karpelès'in –ve birçok açıdan Bitcoin topluluğunun– küstahlığının sonunu temsil ediyordu.

Kendisini bir daha asla başarılı bir teknoloji girişimcisi olarak sunamayacaktı. Karpelès, Mt. Gox'un düşüşünden sonra kafasını belirsizlik denizinden birkaç kez çıkarmaya çalışsa da, istikrarlı bir nefret korosuyla sesi bastırıldı.

Doğrusunu söylemek gerekirse, dava hâlâ adalet ve cezanın tatmininden yoksun olsa da, bu merhametli bir sondu. 2012'den bu yana, Mt. Gox'tan yavaş para çekme hakkında ara ara şikâyetler duyuluyordu. Sitenin nihayet kapatıldığı Şubat 2014'te şikâyetler doruğa çıktı. 7 Şubat'ta para çekme resmi olarak durduruldu, ocak ayının ortasında da tamamen kesildi.[2] Anlaşılan, Mt. Gox para çekmeyi resmen durdurmadan çok önce iflas etmişti. Artık anlaşılıyor ki, bir yıl boyunca yavaşça hırsızlık yapılmış ve bu Mt. Gox'un düzeltmeye yeterli ya da istekli olmadığı gevşek güvenlik uygulamaları yüzünden mümkün olmuştu.

Mt. Gox hayatının sonunda Bitcoin'in başına açtığı bütün sorunlara rağmen, borsa Bitcoin'in ilk gelişim dönemi için vazgeçilmezdi. Mt. Gox dijital Magic: The Gathering kartlarının alım-satımı için tasarlanan bir siteden Bitcoin alım-satımı yapılan bir siteye geçiş yapınca, Bitcoin için bir pazar geliştirmede ve fiyat belirlemede etkili oldu. Mt. Gox'tan önce, birçok Bitcoin ticareti pazarın dışında gerçekleşiyordu. Genellikle çevrimiçi buluşan iki kişiden biri,

[2]Southurst, Jon. "Mt. Gox Halts ALL Bitcoin Withdrawals, Price Drop Follows - CoinDesk." CoinDesk.com. 7 Şubat 2014. Erişim tarihi 18 Mayıs 2015. http://www.coin-desk.com/mt-gox-halts-bitcoin-withdrawals-price-drop/

"Sana iki dolar karşılığında 500 bitcoin veririm," der ve diğer kişi bunun ya çok yüksek ya da çok düşük olduğunu söyler; daha sonra pazarlık ederler. Mt. Gox gibi merkezi bir borsa varken, gerçek fiyat keşfi için bir fırsat ve likit piyasa ortaya çıktı.

İki kişinin bir bitcoin'in onlar için ne kadar değerli olduğuna karar vermeye çalışmalarından ziyade, başkalarının bir bitcoin için ne kadar para ödemeye razı olduklarını ve geçmişte bir bitcoin için ne ödendiğini görebileceklerdi. Bu bitcoin'lerin gerçek bir fiyat noktası ve gerçek değer edinmesine olanak sağladı.

Bununla birlikte, Mt. Gox'ta bir şeylerin yolunda gitmediğine dair uyarı işaretleri her yerdeydi. Bu olaydan alınabilecek en büyük ders uyarı işaretlerinin göz ardı edilmemesidir.

Bitcoin oynak bir para birimi olarak görülür ve birçok yasal parayla karşılaştırıldığında bu doğrudur. Ama günümüzde, 2011'de bir haftadan kısa bir süre içinde 1 dolardan 30 dolara sıçradığında olduğundan çok daha dengeli. O sıralar, belirsiz ve çoğunlukla değersiz bir para biriminden teknoloji departmanı olan bütün basın kuruluşlarının yer verdiği bir şeye geçiş yapıyordu. Muhtemelen Avrupa para biriminden bu yana en başarılı ve kesinlikle en göze çarpan yeni para birimi olmuştu. Değerindeki ve halkın ilgisindeki bu artışa Mt. Gox'un artırılmış bir güvenlikle karşılık vermesi gerekirdi ama bunu yapmadı. Haziran 2011'de binlerce bitcoin kayboldu. Ortalıkta birçok suçlama dolaştı ve en sonunda kaybın şirketin eski sahibinin hesabının ele geçirilmesi sonucunda gerçekleştiği keşfedildi. O hesabı kontrol eden kullanıcı Mt. Gox'un siste-

minde yapay bitcoin'ler yaratıp onları borsaya bırakarak fiyatı bir doların altına çekti. Sonra ucuzlayan bitcoin'leri satın alıp onları Mt. Gox'un sisteminden geri çekti. En sonunda, kayıp bitcoin sayısının 2.500 olduğu tahmin edildi. Borsada 500.000 bitcoin 'satılmış' olmasına rağmen, Mt. Gox satışları tersine çevirdi, o nedenle sadece birkaç bin bitcoin geri alınamadı.

Mt. Gox bu darbeye rağmen devam edebildi. Yine de, büyüyen pazarda güçlü bir konumu olan dünyanın en büyük Bitcoin borsasıydı. Bazı şeyleri değiştirip güvenlikle yakından ilgilenmek yerine, Mt. Gox yanlışlıkla binlerce bitcoin'i var olmayan Bitcoin adreslerine göndererek esasında onları Bitcoin ekosisteminden sonsuza kadar çıkardı.

Güvenlik blogu WizSec sayesinde, Mt. Gox'un 2011 ve 2012 boyunca yavaşça bitcoin'leri sızdırdığını ve 2012'nin sonunda fiilen iflas ettiğini keşfettik.

Mt. Gox'un bitcoin'lerini kimin çaldığını kimse bilmiyor. Her birinin çok sayıda destekleyici makul kanıtı varmış gibi görünen birkaç teori var.

Mt. Gox ve Mark Karpelès'in sunduğu açıklama Bitcoin dünyasında yinelenip duruyor: Bir korsan, Mt. Gox cüzdanlarına erişmeyi ve uzun bir süre içinde yüz binlerce bitcoin çalmayı başardı. Mt. Gox ekibi hırsızlığı fark edemedi. Bu açıklama aslında çok mantıklı, çünkü böyle bir soygunun başarılı olabilmesi için gereken bütün insan dinamiklerini içeriyor. Yüklü miktarda paraya yaslanan, konumlarına güvenen ama görevlerinde yetersiz olan bir grup insan vardı. Karpelès ve şirketinin Bitcoin'in değeri ve ona gösterilen ilgideki ani yükselişe hazırlıksız yakalandıklarını düşünüyorsanız bu son derece anlaşılabilir bir durum.

Aynı zamanda, internet suçu kavramı halkın aklında yer ettiğinden beri neredeyse medyanın her betimlemesinde yer alan bir karikatür olan, karanlık ve bilinmeyen, sınırsız becerilere sahip bir korsan var. Bu korsan bir klişe, ama gerçeğe bağlı biri. Gerçekten de, haberlerde okuduğumuz şeyleri yaparak kendilerine bir kariyer edinen neredeyse sınırsız becerilere sahip karanlık ve bilinmez korsanlar var. Bu insanlar Bitcoin'e özel değiller. Target'e sorabilirsiniz.

İkinci teori muhtemelen en popüler olanı, çünkü Karpelès'ten nefret etmek çok kolay. Bu teori gayet basit: Karpelès herkesi dolandırıyor. Bu fikrin savunucuları Karpelès'in kendi şirketinden para çaldığı, yasal sürecin ve kamu ilgisinin geçmesini beklediğinde ısrarcılar. Bu olduğunda, gizlice kontrol ettiği yüz binlerce bitcoin'i anonim bir şekilde paraya dönüştürecek. Bu teorinin gerçek olması için Karpelès'in hem çok cüretkâr hem de son derece aptal olması gerekir. Bitcoin'de yüzlerce milyon dolar kaybettiğinizde, halkın ilgisi kolay kolay azalmaz. Karpelès'in hayatı tehlikede ve internetin hafızası sonsuzdur. Yine de, kimse Karpelès'in cüretkâr ve aptal olmadığını söylemedi. Ödeme yeterliliği testinin –üçüncü bir partinin bir şirketin iddia ettiği fonlara sahip olduğunu doğruladığı bir hesap denetimi– tamamlanmasının hemen ardından başlayan Bitcoin sızıntısının başlangıcının şüpheli zamanlaması bu teoriyi destekliyor, birkaç sayfa sonra değineceğim Willy ve Markus adı verilen botların davranışları da destekleyici.

Bir başka teori daha makul görünüyor, ama ortada sağlam bir fail yok. Başka Mt. Gox çalışanlarının borsanın iç güvenlik işleyişine erişimlerinin olması olası ve bitcoin'leri herhangi biri boşaltmış olabilir. Çalışanların müdahale-

si Mt. Gox'un neredeyse bir sene boyunca neden hiçbir şey fark etmediğini açıklayabilir. Karpelès dışında bariz bir şüpheli olmadığı için bu açıklama pek tatmin edici değil. Sonuç olarak, yönetim kurulu başkanı Karpelès'e kıyasla düşük profilli bir çalışanın fark edilmeden sıvışması daha kolay olur.

Yeni ortaya çıkan teori, bir önceki bölümde tanıştığımız iki hükümet görevlisini içeriyor. Hatırlayacağınız gibi, 2015'te, Narkotik Ajanı Carl Mark Force IV ve Gizli Servis ajanı Shaun Bridges Silk Road soruşturmasına dahil olmuş ve soruşturma sırasında Derin Ağ pazarından yüz binlerce bitcoin çalmak da dahil olmak üzere birkaç suça karıştıkları için tutuklanmışlardı.[3] Savcılara göre, Force soruşturma sırasında Mark Karpelès ile temas halindeydi. Mahkeme belgelerinde bulunan elektronik postalara göre, Karpelès yetkililere ulaşıp yasa dışı kaynaklardan borsaya giren bitcoin'leri soruşturmalarına yardımcı olmak istediğini belirtmişti.

Aksine, Force'un Mt. Gox yönetim kurulu başkanını onunla işbirliği yapmaya zorladığı iddia ediliyor. Karpelès reddedince, hükümet şans eseri Mt. Gox'un iki milyon yasal para rezervine el koydu. Paraya el koyulduktan kısa bir süre sonra Force'un Karpelès'e, "Sana benimle işbirliği yapman gerektiğini söylemiştim!" diye bir mesaj gönderdiği öne sürülüyor. Force ya da Bridges'in Mt. Gox hırsızlığıyla doğrudan bağlantılı olduklarını gösteren açık

[3]Popper, Nathaniel. "Goldman and IDG Put $50 Million to Work in a Bitcoin Company." The New York Times. 29 Nisan 2015. Erişim tarihi 19 Mayıs 2015. http://www. nytimes.com/2015/04/30/business/dealbook/goldman-and-idg-put-50-million-to-work-in-a-bitcoin-company.html?_r=0

bir kanıt olmamasına rağmen, iki memurun bu aşikâr yolsuzluğa bir şekilde dahil olmuş olabileceklerine dair spekülasyonlar mevcut. İki ajan aynı zamanda Karanlık Ağ'ın üyelerine Karpelès'in onlarla işbirliği yaptığını açıklayarak hırsızlığı yapan kişinin –Karpelès internetin yeraltı dünyasında kendine güçlü düşmanlar edindiği için muhtemelen bir Mt. Gox çalışanıyla birlikte hareket eden– bir korsan olduğu teorisini güçlendirdiler.

Mt. Gox davasında birine suç atmak bu kitapta yapılabilecek bir şey değil. Dava John F. Kennedy suikastının komplo teorileri ve karışıklığı seviyesine yaklaşıyor. Olanlar, iddia edilenler ve yaşanmış olabilecek şeyler hakkında rahatlıkla birkaç kitap yazılabilir. Duruşmalar tamamlanıp soruşturmacılar bildikleri her şeyi açıkladıklarında, o kitapların ortaya çıkacaklarını düşünüyorum. Bu arada, suçluyu saptama işini davayla yakından ilgilenen soruşturmacılara bırakacağım.

Ancak, bir çevrimiçi güvenlik araştırmacısı Wizsec soruşturmasından bazı bilgiler edinilebilir. Bitcoin Mt. Gox'un sıcak cüzdanından 2011'de sızmaya başladı; bu süreç 2012'ye kadar devam etti. O coin'ler öncelikle geçici adreslere gönderildikten sonra daha büyük bir toplama adresine ve ardından ya karıştırılmak ya da satılmak üzere borsalara gönderildi. Hatta coin'lerin bir kısmı Mt. Gox'a geri aktarıldı.[4]

Farklı bir borsa, Kraken, Mt. Gox davasında arabulucu statüsü verildi. Bu kalan fonları kontrol edebileceği ve nasıl dağıtılmaları konusunda yetkililerle birlikte çalışaca-

[4]Nilsson, Kim, Daniel Kelman, ve J. Maurice. "WizSec: The Missing Mt. Gox Bitcoins." WizSec.jp. N.p., 19 Nisan 2015. Erişim 19 Mayıs 2015. http://blog.wizsec.jp/2015/04/the-missing-Mt.Gox-bitcoins.html

ğı anlamına geliyordu. Kraken bağımsız soruşturmacılara karşı detaylar ve kayıtlar hakkında tam olarak açık sözlü olmadı, bu sıra dışı değil, hatta yasal bir zorunluluk bile olabilir. Ayrıca, Mt. Gox kayıtlarının ne kadar düzgün olduğu belli değil. Yine de, kapsamlı blokzinciri analizi, Mt. Gox veritabanı sızıntısında bulunan bilgiler ve Mt. Gox tarafından 2011'de tamamlanan ödeme yeterliliği testi sayesinde, WizSec o zamandan 2014'te iflas edene kadar Mt. Gox'un varlıklarının izini sürebildi.

Biri tamamen izi sürülebilen bir para biriminin en büyük cüzdanlarından hiç kimseye fark ettirmeden nasıl para sızdırabilmişti? Raporlar, Mt. Gox'un soğuk cüzdanlarını (internete bağlı olmayan ve bu nedenle teorik olarak hırsızlıktan korunan Bitcoin cüzdanları) sürekli takip etmediğini, günlük işlemlerdeki normal değişiklik sebebiyle azalan sıcak cüzdanlarını belirli aralıklarla doldurduğunu gösteriyordu.

WizSec, Mt. Gox'un iç güvenliğinin dikkatini çekmeden bu durumun cüzdanlardan yavaşça nasıl sızıntıya sebep olabileceğini web sitesinde açıkladı:

> Depolamayı takip etmeyen ya da gelen ve giden miktarları karşılaştırmayan Mx. Gox çalışanları sık yaşanan depozito ve coin çekim dalgalanmalarıyla uğraştıklarını düşünerek körü körüne soğuk depo cüzdanlarını sızdıran sıcak cüzdanlarına aktarmış ve soğuk depo cüzdanlarını neredeyse sızıntı hızında doldurulmuş olabilirler.

Her halükarda, Mt. Gox'un müşterilerinin sandığından

daha az Bitcoin'i bulunuyordu. 2012 yılında, rezervleri tükendi ve daha sonra işler iyice kötüye gitti.

2013'te, bir dizi tuhaf işlem Mt. Gox'da bir botun sıra dışı miktarda işlem yapmasından şüphelenilmesine yol açtı. Botlar farklı borsalarda Bitcoin satın alan ve satan komut dizileridir. Bot işlemleri günümüzde Bitcoin işlemlerinde sık rastlansa da, bu botların faaliyetleri ilgi çekiciydi. İşlem yapan botlar genellikle sahiplerinin isteklerini yerine getirirler: Bitcoin belirli bir fiyata gelince alım yapmak ve belirli bir fiyata çıkarsa satmak gibi. Aslında bundan biraz daha karışıktır, botlar gün içinde sürekli alım satım yapabilmek için belirli parametreler dahilinde karar verirler. Kısacası, botlar günün yirmi dört saatini uyanık geçirebilecek mantıklı işlemciler gibi davranmaya programlanırlar. Ancak bu botlar mantıklı günlük işlemciler gibi davranmıyorlardı. Aniden rastgele fiyatlarda gruplar halinde bitcoin satın alıyorlardı. Doğrulanmamış olsa da, artık bunun müşterilerin sahip olduğundan daha az paranın olduğu sistemde kısmi yedekle çalışmanın etkilerini hafifletmek için yapılmış olmasından şüpheleniliyor. Botlardan birinin aktivitesi o kadar şüpheliydi ki ona lakap takıldı: Bot Willy.

Bu sıra dışı bot faaliyetlerindeki içeriden müdahale kanıtı 2013'ün sonunda sızan işlem detaylarından geliyor. Şüpheli bot hareketleriyle bağlantılı hesaplar sadece teker teker harekete geçtiler. Birden ortaya çıkıp 2.5 milyon dolar değerinde bitcoin satın alır ve bir daha asla işlem yapmazlardı. Bu hesaplar 112 milyon dolarlık işlemden sorumlulardı. Botlar satın aldıkları 270,000 BTC'yi hiçbir zaman satmadılar.

Botların tek şüpheli özelliği bu işlem değildi. İlk bilinen bot Willy hesabının düzenli müşterilerin mevcut seviyesinden daha yüksek bir müşteri numarası olması normal kullanıcı hesabı yaratma sisteminin dışında yaratıldığına işaret ediyordu. Bu bazılarının biraz daha derinlere inmelerine sebep oldu ve kâşifi tarafından Markus adı verilen öncü botun keşfedilmesini sağladı, onun da normalden daha yüksek bir kullanıcı numarası vardı ve benzer şekilde hareket ediyordu.

Bot Markus, Mt. Gox'a hiçbir işlem ücreti ödemeden çalıştı. Bölgesi olarak Japonya'yı seçmiş olmasının yanı sıra, botun Mt. Gox gibi Tokyo merkezli bir IP adresi vardı, ama IP adresleri rahatlıkla taklit edilebilirdi. Ancak en tuhaf olan şey botun Bitcoin için mevcut satış tekliflerine bağlı değişken bir fiyat yerine statik bir fiyattan yüklü miktarda alım yapmış olmasıydı. Bu detay Willy'den önceki botların –ve muhtemelen bot Willy'nin de– aslında bitcoin satın almadıklarına dair sağlam bir spekülasyona sebep oldu.

Bot hareketlerinin hırsızlıkla hiç ilgisi yoktu. WizSec kayıp Mt. Gox bitcoin'lerinin botlar ortalığa çıktığında çoktan kaybolmuş olduklarını kanıtladı. Ancak bu Mt. Gox'daki birinin 2012'nin başından itibaren bir şeylerin üstünü örtmeye çalıştığına işaret ediyor görünüyor.

Daha önce de bahsettiğim gibi, bot Markus'un sıra dışı olabilecek kadar yüksek bir kimlik numarası vardı: 698630. 2014 sızıntısında, Nisan 2013 işlem kaydının iki versiyonu bulunuyordu: kullanıcı isimlerinin çıkarıldığı sıkıştırılmış ama değiştirilmediği kanıtlanabilir bir versiyon ve kullanıcı isimlerini içeren ama değiştirilmiş olabilecek sıradan bir

versiyon. Birinci versiyonda, işlemleri kullanıcı isimlerini içeren ikinci versiyondaki işlemlerle kıyaslanarak Markus yine de tanımlanabilir. Botun sıra dışı alım fiyatları bekleneceği şekilde şartlara uygun bir şekilde değiştirilmiş görünüyor ve yüksek kimlik numarası 634 olarak değiştirilmiş. 2011'te yaşanan sızıntıda, 634 numaralı bir kullanıcı vardı. 'MagicalTux' adlı kullanıcıya aitti. Mark Karpelès'in BitcoinTalk'ta, blogunda ve Twitter'da kullandığı kullanıcı adıyla aynıydı.

Bot Markus işlem yapmayı kestikten sonra, işlemlere Bot Willy devam etti ve zaman zaman bir saat içindeki toplam işlem hacminin yüzde doksanını sadece o oluşturuyordu.[5] Ancak alım-satım hareketlerindeki benzerlik dışında Bot Markus ve Bot Willy arasında kesin bir bağlantı kurulamadığı unutulmamalıdır.

Çok geçmeden, durum iyice kötüye gitti. Bot alım-satım hareketleriyle kayıplarının üstünü örter gibi görünen Mt. Gox'un Wells Fargo ve Dwolla (PayPal'a benzer bir hizmet) hesaplarına Birleşik Devletler hükümeti tarafından el koyulmasıyla rezervlerinden birkaç milyon dolar daha eksildi.

Bu el koyma para çekiminin ilk kez resmen durdurulmasına sebep oldu. Arada sırada kesintiye uğrasa da, en nihayetinde para çekimi tekrar başladı.

2013'ün sonunda ve 2014'te kısa bir süreliğine, Mt. Gox yaşadığı sorunlardan Bitcoin protokolünde bilinen bir hatayı sorumlu tuttu: işlem işlenebilirliği istismarı. Şöyle işliyordu: Madenci ya da tam düğüm rolü oynayan

[5]Nilsson, Kim. "WizSec: Mt. Gox Investigation Update and Preliminary Release." WizSec.jp. 14 Şubat 2015. Erişim tarihi 19 Mayıs 2015. http://blog.wizsec.jp/2015/02/Mt.Gox-investigation-release.html

kötü niyetli bir oyuncu farklı bir varış yeri numarasıyla diğer kullanıcıların işlemlerinin sahte versiyonlarını gönderir. Sistemin işlem numarasının hash'ini ve gönderen kişinin imzasını kontrol ederek bunu önleyebilmesi gerekir; ama Bitcoin'in eski versiyonlarında bunu yapmayı ihmal ediyordu. Eğer kötü niyetli bir oyuncu kullanıcı kimliğini değiştirip işlemin değişime uğramış versiyonunu gerçek işlemden önce blokzincirinde doğrulatırsa, o zaman kötü niyetli oyuncu Bitcoin işlemlerini engelleme ve yeniden yönlendirme becerisini kazanır.

İşlem işlenebilirliği hatası gerçek bir sorun olmasına rağmen, ondan Mt. Gox iflası sırasında kaybolan bitcoin'lerin küçük bir bölümünden bile sorumlu olabilecek kadar faydalanılmadı. Rakamlar akla yatmıyor. arXiv.org'da yayınlanan bir bildiri işlem işlenebilirliği hatasının Mt. Gox'un finansal sorunlarına sebep olduğuna dair resmi iddiayı tamamen çürüttü.[6] Bildiri Mt. Gox kullanıcılarının çekim yapmasını engellemeden önce, bütün Bitcoin ekosisteminde sadece 386 coin'in olası başarılı işlem işlenebilirliği istismarı teşebbüslerine karışmış olabileceğini belirtti. Bunun Mt. Gox'un iflasına önemli ölçüde katkıda bulunup bulunmadığını tahmin etmenin imkânı yok.

Suçlamalar artarken ve daha fazla müşteri memnuniyetsizliğini dile getirirken, Karpelès nihayet Bitcoin Vakfi'ndaki görevinden ayrıldı[7] fakat birçok kişi bunu yapmakta

[6]Decker, Christian, ve Roger Wattenhofer. "Bitcoin Transaction Malleability and Mt. Gox." Computer Security - ESORICS 2014 Lecture Notes in Computer Science (2014): 313-26. ArXiv.org. 26 Mart 2014. Erişim tarihi 18 Mayıs 2015. http://arxiv.org/ abs/1403.6676

[7]Sidel, Robin. "Mt. Gox Resigns From Bitcoin Foundation." The Wall Street Journal. 24 Şubat 2014. Erişim tarihi 19 Mayıs 2015. http://www.wsj.com/articles/SB10001424052702303426304579401883794330454

geciktiğini düşünüyordu. Daha fazla müşterinin her gün çekim hakkında şikâyetlerini dile getirdiği 2014'ün başı oldukça çalkantılıydı. Şubat ayında, birçok kişi Mt. Gox'un artık yasal para ya da Bitcoin ödemesi yapamayacağını düşünüyordu. Bir Amerikalı Karpelès'ten parasını şahsen istemek için Indiana'dan Japonya'ya uçtu. Bu belki de Bitcoin'le ilgili internet dışında yaşanan ilk politik tiyatroydu.[8]

Artık Şubat 2014'ün son gününe ve Japon Yerel Mahkemesi'nin önünde üzerinde takım elbisesiyle yenilgiye uğramış ve keyifsizce oturmuş, iflasını açıklayan Karpelès'e geri dönebiliriz. Mt. Gox kapatılacaktı ve o ya da yönetim kurulu başkanı için bir kurtuluş hikâyesi olmayacaktı. Çalışanlarını kendisine 'kral' diye hitap etmeye zorladığı söylenen adam krallığını kaybetmişti. Rüya sona ermişti ve Karpelès bunun farkındaymış gibi görünüyordu. Eğer Karpelès hırsızlığın failiyse, soluğu orada almayı bekliyormuş gibi görünmüyordu.

Mt. Gox'un son nefesi ana akım bilince dalan dev bir dalgalanma etkisi yarattı ve birçok kişinin Bitcoin'le ilgili algısını şekillendirdi. Bu algılar günümüzde de Bitcoin'in itibarını renklendirmeye devam ediyor.

The Weekly Standard 'Bitcoin Öldü' başlıklı bir makale yayınladı.[9]

Salon'un Mt. Gox'un uğradığı saldırı hakkında yazdığı

---

[8]Southurst, Jon. "Watch This Man Confront CEO of Mt. Gox Over Missing Bitcoins." CoinDesk.com. 14 Şubat 2014. Erişim tarihi 19 Mayıs 2015. http://www.coin-desk.com/watch-man-confront-ceo-mt-gox-missing-bitcoins/

[9]Last, Jonathan V. "Bitcoin Is Dead." The Weekly Standard. weeklystandard.com. 5 Mart 2014. Erişim tarihi 19 Mayıs 2015. http://www.weeklystandard.com/bitcoin-is-dead/ article/784187

yazı –ve Kaliforniyalı bir adamın Satoshi Nakamoto olarak 'kimlik bilgilerine ulaştıklarını' (ifşa ettikleri) sahte haber– para birimi için felaket anlamına geliyordu.[10] Reuters'dan[11] Yahoo'ya[12] herkes Bitcoin'in ölümünü bekliyor gibi görünüyordu. Birkaçı bir umut ışığı[13] görse de, çoğu bunun son olduğunu düşünüyordu. Batı Virginia Senatörü Joe Manchin, Bitcoin'in yasaklanması çağrısında bulundu.[14] Uzun zamandır Bitcoin blogunda yazan güvenlik araştırmacısı ve kripto para savunucusu twobitidot (gerçek adı Ryan Selkis) haberi alınca 'Bitcoin'in Kıyamet ânı' için sızlandı.[15]

---

[10]Leonard, Andrew. "Sorry, Libertarians: Your Dream of a Bitcoin Paradise Is Officially Dead and Gone." Salon.com. 7 Mart 2014. Erişim tarihi 19 Mayıs 2015. http://www.salon.com/2014/03/07/sorry_libertarians_your_dream_of_a_bitcoin_paradise_is_officially_dead_and_gone/

[11]Hadas, Edward. "An Early Obituary for Bitcoin." Reuters.com. 8 Ocak 2014. Erişim tarihi 19 Mayıs 2015. http://blogs.reuters.com/edward-hadas/2014/01/08/an-early-obituary-for-bitcoin/

[12]Lyster, Lauren. "Mt. Gox on Verge of Collapse, Bitcoin Plunges: Is This the End for the Virtual Currency?" Yahoo Finance. Daily Ticker, 25 Şubat 2014. Erişim tarihi 19 Mayıs 2015. http://finance.yahoo.com/blogs/daily-ticker/bitcoin-mt--gox-deleted-141110461. html

[13]Carson, Biz. "This Week in Bitcoin: Mt. Gox's Meltdown May Prove Bitcoin Is a Real Currency." Gigaom.com. Gigaom, 28 Şubat 2014. Web. 19 Mayıs 2015. http://finance.yahoo.com/blogs/daily-ticker/bitcoin-mt--gox-deleted-141110461.html

[14]Fung, Brian. "Sen. Joe Manchin Calls for a Bitcoin Ban as Regulators Seek 'accel- erated Push'." The Washington Post. 26 Şubat 2014. Erişim tarihi 19 Mayıs 2015. https://www.washingtonpost.com/news/the-switch/wp/2014/02/26/sen-joe-manchin-calls-for-a-bitcoin-ban-as-regulators-seek-accelerated-push/

[15]Selkis, Ryan. "Bitcoin's Apocalyptic Moment: Mt. Gox May Have Lost 750,000 Bitcoins." TBI's Daily Bit. Tumblr, 24 Şubat 2014. Erişim tarihi 19 Mayıs 2015.http://two-bit-idiot.tumblr.com/post/77745633839/bitcoins-apocalyptic-moment-mt-gox-may-have

Endişelerin yerinde olduğunu söylemek gerekir. 2014 Mt. Gox çöküşünün para biriminin sonu olacağını düşünenler hoş görülebilirler. Mt. Gox hırsızlığında var olabilecek bütün bitcoin'lerin yüzde 3,5'i ortadan kayboldu. Bunun Bitcoin'in sonu olduğunu sanmak hiç zor değildi.

2014 Mart ortasında, Mt. Gox'un sahip olduğu 200.000 bitcoin unutulan bir cüzdanda keşfedildi.[16] Bu zararlarının karşılanmasını bekleyen insanlara biraz umut verdi ama Mt. Gox'u dirileceğine dair hiç umut yok.

Borsanın çöküşünden sonraki yasal süreç acı verici bir şekilde yavaştı ve artan harcamaların 200.000 BTC zulasını eriteceği kesindi. Eski Mt. Gox müşterilerinin ödeme talebi süreci iflastan bir seneden uzun bir süre sonra başladı. Kimse bu ödeme talebi sürecinin tamamlanıp tamamlanmayacağını bilmiyor. Bu sırada, kalan sermayeden büyük yatırımcılara ve Mark Karpelès'in mahkeme masraflarına nakit akıyordu. Fonlar böylesine tükenmişken Mt. Gox müşterilerine bir şey kalmış olması pek mümkün görünmüyor.

Yine de, Bitcoin ölmedi. Kalıcı bir şekilde lekelendiğini söylemek mümkün ama yoluna devam etmeyi başardı. Mt. Gox çöküşü topluluğun geri kalanı için bir uyarı oldu ve Bitcoin'in altyapısını şekillendirmeye yardım etti.

Bitcoin, merkezi olmayan bir para birimi olduğundan, topluluğun o coin'leri tuttuğu yeri merkezileştirmek Bitcoin'in avantajlarını yok eder. Mt. Gox esasında herkesin parasını elinde tutan bir banka görevi görerek merkezi

[16]Lyne, James. "$116 Million Bitcoins 'Found' At Mt. Gox And How To Protect Your Wallet." Forbes Magazine. 21 Mart 2014. Erişim tarihi 19 Mayıs 2015. http://www.forbes.com/sites/jameslyne/2014/03/21/116-million-bitcoins-found-at-Mt.Gox-and-how-to-protect-your-wallet/ - 1501b9419695

olmama yönünü ortadan kaldırıyordu. Bankalar ve suistimalleri sık sık insanların Bitcoin'e ilgi göstermelerinin ardındaki itici güç olarak gösteriliyorlar. Ne yazık ki, bankaların aksine, Mt. Gox denetimlerden muaftı ve sigortası bulunmuyordu. Bankaların bütün negatif yanlarını bünyesinde bulundururken, on yıllar boyunca uyguladıkları gözetime sahip değildi.

Böylesine çok sayıda bitcoin tek bir yerde toplandığı için Mt. Gox kötü niyetli insanlar için büyük bir hedef haline geldi ve başarısızlığın odak noktası oldu. Yine de, insanların bitcoin alıp satabilecekleri merkezi bir pazar, fiyat keşfi ve en nihayetinde bütün Bitcoin ekosistemi için vazgeçilmezdir.

Bu çıkmaz, merkezi olmayan bir borsa yaratmak için farklı proje girişimlerine sebep oldu. Birkaçı tamamlandı: BitHalo, Nxt borsası ve Blocknet piyasaya sunulmak üzereler ya da bu kitap yayınlandığında büyük güncellemeler yapacaklar. Onları kullanan kişilerin olup olmayacağını – ya da piyasaya sunulup sunulmayacaklarını– bekleyip göreceğiz.

Merkezi olmayan bir borsa kullanıcıların üçüncü bir partiye gerek duymadan yasal para karşılığında bitcoin alıp satmalarına imkân tanır. Borsa dışı satışların aksine, merkezi olmayan bir borsanın bir sipariş defteri ve pazar talebine göre değişen bir fiyatı olabilir. Merkezi olmayan borsa fikri Mt. Gox çöküşünden önce de var olsa da, bu olay onu neredeyse herkesin yapılacaklar listesinin en tepesine itti. Ne yazık ki, günümüzdeki birçok Bitcoin işlemi hâlâ merkezi sunucular kullanılarak yapılıyor. Kullanılabilirlik, güvenlik ve gizlilik ihtiyaçlarına hitap eden, merkezi olmayan bir hizmet geliştirilemedi. Bu geliştirildiğinde,

merkezi olmayan borsayı geleneksel finans sistemlerine entegre etme sorunu yine var olacak.

Merkezsizleşmeye doğru çabalamaktan daha önemli olan şey Bitcoin'in kısa çocukluk döneminin bitmiş olduğunu fark etmekti. Sisteme gerçek para akıtılıyordu ve gerçek paraya gerçek suçlar eşlik ediyordu. Bitcoin hükümetlerin ya da bankaların değil, onu çekici bulan insanların bir hedefi haline geldi. Teknolojiye eğilimli kişiler Bitcoin'in en büyük değeri ve en büyük tehdidi olarak duruyorlar. Bitcoin'in değeri kullanılabilirliğine ve bu kullanılabilirlik tamamen güvenliğine bağlı. Bitcoin'in temel protokolü ne kadar güçlü olursa olsun, üçüncü partiler itibarına gölge düşürebilirler. Bir korsanın bitcoin zulalarını ele geçirmesi inşa etmesi yıllar süren güveni ve iyi niyeti mahvedebilir.

Bununla birlikte, Mt. Gox fiyaskosundan sonra bile akıllı para Bitcoin'e yatırım yapmaya devam etti. 2014'ün geri kalanı ve 2015'in ilk üç çeyreği boyunca fiyat sabit düşüşte olsa da, risk sermayedarı parası daha önce hiç olmadığı kadar akmaya başladı. 2014 kripto para yatırımı için rekor kıran bir yıl oldu[1] ve bu kitabı yazdığım sırada, 2015 o rekoru kırma yolunda ilerliyordu. Kısa bir süre önce, finans devleri Goldman Sachs[17], USAA[18] ve NASDAQ[19],

---

[17]DeMartino, Ian M. "Smart Money Bets On Bitcoin: Top Three Investments In Bitcoin History Occurred In 2015." Coin Journal. 1 Mayıs 2015. Erişim tarihi 19 Mayıs 2015. http://coinjournal.net/smart-money-bets-on-bitcoin-top-three-investments-in-bitcoin-history-occurred-in-2015-op-ed/

[18]Popper, Nathaniel. "Goldman and IDG Put $50 Million to Work in a Bitcoin Company." The New York Times. 29 Nisan 2015. Erişim tarihi 19 Mayıs 2015. http://www. nytimes.com/2015/04/30/business/dealbook/goldman-and-idg-put-50-million-to-work-in-a-bitcoin-company.html

[19]Rocham, M. "Financial Services Giant USAA to Study Use of Bitcoin Technology." International Business Times. 9 Mayıs 2015. Erişim tarihi 19 Mayıs 2015. http://www.ibtimes.co.uk/financial-services-giant-usaa-study-use-bitcoin-technology-1500514

Bitcoin'e katılacaklarını ve blokzincirine dayalı teknolojileri inceleyeceklerini duyurdular. Bitcoin kabul eden satıcı listesi de büyümeye devam etti ve artık Microsoft, PayPal'ın Braintree'si, Dell, DishNetwork, Expedia, Overstock.com, Amerikan Kızılhaçı, RE/MAX Londra, Save The Children, Edward Snowden'ın yasal savunma fonu ve diğer birçok kuruluşu içeriyor.[20] [21] Circle adlı Bitcoin borsası New York Mali Hizmetler Departmanı'na kayıtlı ve yönetmeliğine uygun olarak çalışıyor. 2016 Birleşik Devletler başkanlık yarışı sırasında, Cumhuriyetçilerin baş adaylarından biri olan Rand Paul Bitcoin bağışlarını kabul ediyordu.

Bitcoin'in geleceğinin nasıl olacağını biliyormuş gibi davranamam. Ancak, Mt. Gox muhtemelen Bitcoin'in başına gelen en kötü şey olmasına rağmen para biriminin sonunu getirmedi. Bitcoin hayatına devam etti ve şimdi 2013'ün sonunda olduğundan daha güçlü görünüyor. Bunun bir önemi olmalı.

---

[20]Franzen, Carl. "Newegg Now Accepts Bitcoin." The Verge. Vox Media. 1 Temmuz 2014. Erişim tarihi 19 Mayıs 2015. http://www.theverge.com/2014/7/1/5860556/newegg-now-accepts-bitcoin

[21]Chansanchai, Athima. "Now You Can Exchange Bitcoins to Buy Apps, Games and More for Windows, Windows Phone and Xbox." Microsoft. 11 Aralık 2014. Erişim tarihi 19 Mayıs 2015. https://blogs.microsoft.com/firehose/2014/12/11/now-you-can-exchange-bitcoins-to-buy-apps-games-and-more-for-windows-windows-phone-and-xbox/

Dokuzuncu Bölüm:

Diğer Bitcoin Hileleri ve Yaygın Taktikler

Evrende bundan daha rezil ve sefil başka bir yer yoktur. Dikkatli olmalıyız.

— Obi-Wan (Ben) Kenobi, *Yıldız Savaşları Bölüm 4: Yeni Bir Umut*

Güvenli bir şekilde Bitcoin'e yatırım yapmak istiyorsanız, bunu yapmanın basit bir yolu var. Bir borsadan ya da tanıdığınız birinden Bitcoin satın alın, onu yerel cüzdana çekin ve bir kâğıt cüzdana yazdırın. Daha sonra, yatırımınızı artırmak istediğinizde o cüzdandaki kare kodu kullanarak fon ekleyebilirsiniz. Bitcoin'lerinizi her çekmek istediğinizde, hepsini çekmek zorunda kalacaksınız ve cüzdan artık el değmemiş bir kâğıt cüzdan kadar güvenli olmayacak.

Harcamak ya da başka girişimlere yatırım yapmak istiyorsanız bitcoin'inizi tutmanın en uygun yolu bu değil, ama dolandırılmadan Bitcoin'e yatırım yapmanın en güvenli yolu budur.

Eğer bir adım daha ileri gidip yeni teknolojilere ya da şirketlere yatırım yapmak isterseniz, kripto para topluluklarına dalmaya başlamanız gerekecek. Bunu yaptığınız zaman, en azından bu kitabı yazdığım sırada, topluluğun en kötü unsurlarıyla karşı karşıya kalacağınızı neredeyse garanti edebilirim. Her kültürel ve ekonomik furyada olduğu gibi, Bitcoin de her türlü insanı kendisine çekti. Bu karışımda suçlular, genel nüfusa kıyasla orantısız bir şekilde olsa da, kesinlikle yer alıyorlar. Ve suçlular ortama yeni giren insanları avlamayı severler.

Birçok büyük kültürel fenomen bu dezavantaja sahip görünüyor. Bitcoin'in ortaya çıkışını hippi akımıyla karşılaştırabiliriz. 1967'de, birkaç ana akım medya kuruluşu San Francisco'nun Haight-Ashbury bölgesinde giderek artan asit dalgasını haber yaptılar; dönemin popüler müziği –Scott McKenzie'nin *San Francisco* (*Saçlarınıza çiçek takmayı unutmayın*) adlı şarkısı– orada gelişen hayatı tanıtıyordu. Halkın bu ilgisi haklarından mahrum edilen bir dizi gencin bedava kalacak yer, yiyecek, uyuşturucu ve aşk bulmak için şehre akın etmelerine neden oldu. Ama binlerce insanın her şeyi bedava istemesinin ve giderek az sayıda insanın onları bedava vermeye razı olmasının ekonomisi uzun vadede işe yaramadı. En sonunda, Haight-Ashbury'nin olgun ve deneyimli sakinlerinden bazıları yeni gelenlerin yanı sıra bölgeyi ziyaret eden turistleri avlamaya başladılar.

Haight-Ashbury'de ortaya çıkan hippi akımının neden uzun ömürlü olmadığına dair birçok teori var ve ben onları yargılayabilecek bir konumda değilim. Akım hakkında yazan herkesin açıkça gördüğü şey şuydu ki; kalabalık bir

insan akını toplum üzerinde stres oluşturmuştu. 1969'da Haight-Ashbury'de hippi bulmaya çalışan birinin en azından akımın şanından faydalanma niyetinde olan hippi kılığına girmiş birini bulma ihtimalinin olduğunu söylemek yerinde olur.

Bitcoin ve Haight-Ashbury arasında birçok benzerlik kurulabilir. 2011'de ve daha sonra 2013 sonu-2014 başında Bitcoin'in fiyatı fırladığında, para birimi ana akım medyanın ilgisini çekti ve onlar aracılığıyla dijital zenginliğin bir sonraki dalgasını yakalamak isteyen yüz binlerce kısmen ve özenti teknoloji hastasını kendisine çekti. Ama Bitcoin ekonomisinde zaten binlerce insan vardı ve tecrübenin son derece nadir olduğu bir âlemde yılların birikimine sahiplerdi.

1960'ların sonunda ortaya çıkan, parayı ve maddi eşyaları reddeden hippi akımının aksine, Bitcoin akımı tamamen parayla ilgiliydi. Ne de olsa, bitcoin bir para birimi. Haight-Ashbury dolandırıcılarının davranışı hippilerin felsefesine ters olsa da, Bitcoin 'akımı' paranın etrafında döner, o nedenle Hunter S. Thompson'ın 'Açgözlüler' olarak tanımlayacağı kişilerin ilgisini çekmesi hiç şaşırtıcı değil.

Her biri bir noktada 'Bitcoin Mesih'i' olarak adlandırılan konuşmasını bilen Bitcoin savunucuları Andreas Antonopoulous ve Roger Ver gibi insanların süslü sözleri sayesinde Bitcoin birçoğumuzun ilgisini çekti, hatta bazılarımızı büyüledi. Açgözlülük ve hırsızlığa daha az bağlı olan yeni bir ekonomik sistem vaat ettiler.

Ama aksine, günümüzde insanların kripto para topluluklarında çeşit çeşit entrikalar ve birçok sebepten ötürü

başarısızlığa mahkûm para türleri bulması olası. Bazı durumlarda, paraların geliştiricileri giderek daha rekabetçi olan pazarla rekabet edecek beceriye sahip değiller. Diğer durumlarda, entrikalar en başından beri dolandırma amaçlı. Ve bazıları da, bir noktada her büyük kripto para birimi şirketini vuran teknolojik saldırıları atlatmalarını sağlayacak güvenlik düzeyine sahip değiller.

Bu bölüm sizi Bitcoin'de karşılaşabileceğiniz her sahtekârlığa karşı doğru düzgün hazırlamayacak. Aksine, kripto para pazarını vuran en büyük sahtekârlıklara genel bir bakış atacağız ve böylece daha önce neler olduğu hakkında bir fikriniz olacak, günümüzde dönen sahtekârlıkları tanıma becerisi kazanacaksınız.

Bitcoin topluluğunda iki tür sahtekârlıkla karşılaşabilirsiniz ama ne kadar derine indiğinize bağlı olarak onlardan sadece birini görebilirsiniz. Birincisi apaçık bir sahtekârlık: genellikle bir kumar ya da borsa hizmeti sunan bir web sitesi, insanlar bitcoin'lerini yatırdıktan sonra kapanır ve müşteriler birikimlerini bir daha göremezler. Bazı durumlarda, bu olay bir korsan saldırısı sonucu gerçekleşir; diğer durumlarda, kaçan kişi sitenin yaratıcısıdır. Bitcoin ekonomisi kuvvetlendikçe, bu tür dolandırıcılıklardan kaçınmak kolaylaşıyor. 'Güvenli' borsalar bitcoin'lerini saklamak ve harcamak isteyenler için oldukça güvenli pozisyonlar sunan sigortası ve denetimi olan yerlerdir. Bitcoin'de hiçbir şey garanti olmasa da, Mt. Gox benzeri olaylar gittikçe azalıyor; popüler 'çoklu kripto para' borsalarının hâlâ anlaşmazlıkları ve sorunları olsa da, sadece Bitcoin alım-satımı yapılan borsalar –Circle, Coinbase, vs.– küçük ve orta ölçekli Bitcoin varlıkları için oldukça güvenlidir.

Yine de, uzun vadeli birikimlerin çevrimdışı bir cüzdanda tutulması daha iyidir, ama saf Bitcoin borsalarının her birkaç ayda bir iflas etme dönemi geride kalmış görünüyor. Bu dolandırıcılıklar/olaylar gri market –Bitcoin aklayıcılar, porno siteleri, kumar siteleri– hizmetlerinin yanı sıra karaborsa hizmetleri için de hâlâ bir risk oluşturuyor ama ortalama bir kullanıcı oldukça güvende.

İkinci dolandırıcılık türü biraz daha karışık ve tanıması daha zor. Unutmamanız gereken en önemli prensip saadet zinciri gibi görünmesidir ve muhtemelen öyledir. Bitcoin bunu değiştiremez.

Şirketler, sık sık bir paravan olarak 'bulut madencilik' kullanarak (sizin yerinize madencilik yapan ve donanımı onlardan 'kiraladığınız') bir hizmet sunarlar ve kullanıcılara para öderler. Madencilik kârından ödeyeceklerini iddia ederler ama para genellikle yeni yatırımcılardan gelir. Kısa bir süre önce, bulut madencilik çok sayıda dolandırıcılık sebebiyle popülerliğini yitirirken, yeni dolandırıcılık yöntemleri türedi. Bazı dolandırıcılar Bitcoin günlük işlemcileri ya da en iyi borsalardan biri olacağına *emin* oldukları yeni bir borsayı piyasaya sürecekmiş gibi davranıyorlar. En çok test edilip onaylanan dolandırıcılıklardan biri yeni bir para birimi yaratıp onun Bitcoin'e rakip olacağını iddia etmektir. Bu tür şeyleri yapan çok sayıda şirket olduğunu unutmamalısınız.

Toplulukların büyük bir bölümünün kullandığı yerleşik borsalar olduğu için yeni bir borsanın kâr getirmeden önce önünde uzun ve zorlu bir yol vardır.

Madencilik blokzincirinde rahatlıkla doğrulanabilir. Bu hizmet, sahip olduğunu iddia ettiği hash gücüyle is-

tikrarlı yeterli coin tabanı girdisi –madencilikle yeni para yaratılışını tanımlayan girdiler– olan bir adres sunamazsa, ona güvenilmemelidir. Bana kalırsa, bulut madencilikten tamamen kaçınmak en iyisidir. Blokzincirinde doğrulanamayan bir şeyse, aklınızı kullanmak zorundasınız. Unutmayın, herhangi bir şeyin 'Bitcoin işletmesi' olması, diğer işletmelerden daha avantajlı olduğu anlamına gelmez. Diğer işletmelerle olduğu gibi, çevrimiçi itibarı iyi olmalıdır. Bu itibar en önemli etken değildir ama size bir şirketin müşterisi olmaya değer olup olmadığını söyler.

Eğer bir şirket yatırımcıların kazancını ödemek için yeterince mal, 'fiziki bitcoin' –ya da başka bir şey– sattığını iddia ediyorsa, resimli müşteri yorumlarına bakın. Alexa.com'dan sitenin ziyaret edilme sıklığını kontrol edin ve ziyaretçi trafiğinin ticaret miktarıyla tutarlı olup olmadığına bakın. Whois.com bir web sitesinin alan adının kime ait olduğunu görmenize izin verir. Gerçek bir isim ve adres yerine eğer 'WhoisGuard' ya da benzeri bir hizmet varsa, bu işletmenin kim olduklarını müşterilerinin bilmesini istemediğine dair kesin bir işarettir. Çevrimiçi kumar sitesi gibi bir işletme söz konusu olduğunda, bu mantıklı olabilir; diğer durumların yüzde 99'unda, hiç mantıklı değildir ve o şirketten uzak durmanız gerekir.

Unutulmaması gereken en önemli şey şu: Eğer bir şey kulağa dolandırıcılık gibi geliyorsa, muhtemelen öyledir. Yatırımınız karşılığında anlık ya da gerçekçi olmayan geri dönüşler vaat eden herkesten sakının. Saadet zincirinin temel prensipleri diğer her alanda olduğu gibi kripto parada da aynı şekilde işliyor. Eğer eski yatırımcılara yeni yatırımların sermayesiyle ödeme yapılıyorsa, bir saadet zinciriyle

karşı karşıyasınız demektir. İnsanlar kâr başka bir yerden geliyormuş gibi göstermek için her türlü iddiada bulunurlar, o nedenle kendi araştırmanızı yapıp paranızı her neye yatırmak istiyorsanız derinine inmeniz gerekecek.

Aşağıda sıraladığım suçlular Bitcoin spektrumunun her yanından geliyorlar. Birçoğu yokuş aşağı gitmeden önce topluluğun en önemli üyeleri olarak görüldüler. Davasına bütün bir bölümü ayırmam gerektiği için listede olmayan Mt. Gox'tan Mark Karpelès, bir zamanlar Bitcoin Vakfı'nın yönetim kurulu üyeleri arasındaydı. Topluluğun o anki saygısı bir kişinin itibarlı ya da güvenilir olduğunu garantilemez. Bir zamanlar, daha sonra değineceğim bir şirket olan GAW Miners, madencilik endüstrisinin devi olarak görülüyordu. Daha önce de bahsettiğim gibi, işler somutlaşıyor ve güvenilebilir şirketler daha belirgin olmaya başlıyorlar, ama dolandırıcılığa hâlâ sık rastlanıyor.

Detaylı listeye başlamadan önce, unutmamanız gereken birkaç noktaya değinmek istiyorum:

- Eğer başka bir şirket ya da kişi özel anahtarınıza sahipse, esasında bitcoin'leriniz onların elinde demektir. Bitcoin'in cazip olmasının en büyük etkeni hiçbir bankanın paranızı bloke edememesidir, ama eğer özel anahtarınızı birine verirseniz, o kişiye onu dilediği şekilde kullanma yetkisini vermiş sayılırsınız.
- Altcoin alanında sık sık 'şişir ve boşalt' manipülasyonu görülür. Bir coin'in geliştirici ekibinin ya da topluluğun her duyurusuna temkinli bir şekilde yaklaşmak gerekir. Amaçları her zaman net değildir

ve coin'in yaratıcısı olarak, ellerinde muhtemelen yüklü miktarda coin bulunduruyor olmalılar, o nedenle fiyatı şişirmek onların yararınadır. Bir özelliğin (piyasaya sunulup sunulmayacağı kesin olmayan) heyecan verici duyurusunun sonucu olarak fiyatı birkaç sent yükseltseler bile, fiyat yükselişinin ardından coin'leri sattıklarında yüklü miktarda para kazanacaklar.

Bunun dışında, küçük miktarda alımlar yaparak zamanla toplam varlıkları pazarı hareketlendirecek küçük hacimli altcoin bulan –coin geliştiricilerinden bağımsız– gruplar var. Topluluğun geri kalanı tarafından genellikle üçkâğıtçı olarak görülen bu kişiler, önce bir coin'in değerini artırır ve ardından önceden belirlenmiş bir zamanda onu satarlar. İşleri iyice karıştırmak için gruptaki kişiler coin'lerden aynı anda kurtulmak için liderlerinin sözünü beklerler. Üyelerinin arasında 'içeriden gerçek bilgi alan' küçük bir zümre olduğu için grupların suçlanması duyulmamış değildir.

- Bitcoin ve diğer paraların yüklü miktarda toplanması dolandırıcılar ve korsanların ilgisini çeker. Borsalar korsanların hedefi haline geldi ve en iyi niyetli şirketler bile, onlara altı ya da yedi haneli bir sayıya mal olan bir saldırıyı atlatmakta zorlanabilirler.
- Çeşitlilik önemlidir. Bütün paranızı tek bir borsada tutarsanız ve o borsa saldırıya uğrarsa, bütün varlığınızı kaybedersiniz. Ama paranızı birkaç borsaya yayarsanız, sadece bir kısmını kaybedersiniz. Eğer Bitcoin akımının ardında bir düstur olursa, mer-

kezsizleşme fikri olur. Bitcoin'lerinizin merkezileştirilmesi için hiçbir sebep yok. Aynı şey çevrimdışı ve kâğıt cüzdanlar için de geçerli. Bir cüzdan güvenli olsa bile, içinde her şeyi bulundurmamalısınız. Her şeyi kâğıt cüzdanlarda tutmakta ısrarcı olursanız, hepsini aynı yerde tutmadığınızdan emin olun. Fiziksel hırsızlık ve zarar görme potansiyeli hâlâ büyük bir risk oluşturuyor.

- Altcoin'ler tam bir fiyaskodur. Hepsinin ya da çoğunun sahtecilikle ilgili olduğunu söylemeye çalışmıyorum. Sadece pazarın destekleyemeyeceği kadar çok var. En iyi altcoin'lerin bile en az yüzde doksan beşi başarısız olacak. Mevcut mahsullerin sadece birkaçı kripto para tarihinde bir sonraki aşamaya geçmeyi başaracaklar ama birçoğu filizlenirken ölecek. Ölmek üzere olan bir coin'in geliştiricisi olmak korkunç bir gerçek, özellikle de teknolojinizi kullanarak dünyayı değiştirmeyi hayal eden iyi niyetli bir geliştiriciyseniz. Yıllarca çalışıp kendisini adayan bir kişinin her şeyin bir hiç uğruna olduğunu anlaması çaresiz hissetmesine neden olabilir. Ve çaresiz insanlar ahlak kurallarından taviz vermek gibi çaresizce şeyler yaparlar.
- Bitcoin ortamında birçok dolandırıcı var ve teknik açıdan oldukça yetenekliler. Herkes iddia ettiği kadar iyi bir korsan olmayabilir –buna daha sonra detaylı bir şekilde değineceğim– ama ortalıkta iyi sayılabilecek yeterince korsanın olması, onlarla sık sık karşılaştığınız anlamına gelir. Sonuç olarak, güvenlik uygulamalarınızda her zaman dikkatli olun.

Bir çevrimiçi cüzdanda yüklü miktarda paranız varsa, o halde iki aşamalı doğrulama (şifre ve tek kullanımlık özel bir kod gibi bir çift doğrulama) kullanmalısınız.

- Genel olarak internette işe yarayan dolandırıcılık yöntemleri, bazen biraz daha sofistike bir şekilde, kripto para dünyasına da taşındı. Oltalama yöntemine çok sık rastlanıyor ve hırsızlar meşru Bitcoin şirketlerinin e-posta adreslerini kullanarak kandırma konusunda yetenekliler. Oltalama yöntemi teşebbüslerinin devam edeceğinden emin olabilirsiniz. Aklınızı kullanın, asla hesap linklerine tıklayıp oturum açmayın ve "bitcoin'lerinizi buradan ikiye katlayın!" gibi vaatlerde bulunan e-postalarına inanmayın. Linkin diğer ucunda Nijeryalı bir prens ya da gökkuşağının diğer ucunda bir çanak dolusu altın yok.

Dolandırıcılık ve korsanlık farklı şeylerdir. E-dolandırıcılık, ya asıl plan ya sitenin sahibinin kaybını kapatmak için daha sonradan yapmaya karar verdiği bir şey ya da başka bir nedenden ötürü kullanıcıların parasını çalan bir hizmettir. Korsanlık güvenlik açığı sebebiyle bir dış kaynak tarafından bitcoin hırsızlığı yapılmasıdır. Aşağıdaki iki durumda olduğu gibi, birçok dolandırıcılıkta kaybın bir korsanlık sonucu olduğu iddia edilir.

MintPal

MintPal çok sayıda para birimi destekleyen profesyonel görünümlü bir kripto para borsasıydı. Ne yazık ki, dış görünüş aldatıcı olabilir.

MintPal skandalı, Mt. Gox fiyaskosu da dahil olmak üzere, kripto para tarihindeki diğer dolandırıcılıklar kadar karışıktır. Sinema için neredeyse biçilmiş kaftan olan bu skandal sahte kimlikler, kurumsal devir ve bir arkası yarın içeriyor.

MintPal'ın sorunu Temmuz 2014'te meşru bir saldırı gibi görünen bir durumla başladı. Saldırı esasen sekiz milyon VeriCoin kaybını içeriyordu. VeriCoin işlemleri doğrulamak için proof-of-stake (PoS) algoritması kullanır. PoS algoritmaları kripto paradan yüklü miktarda bulunduranlara önem verir ve kısmen istikrarlı bir faiz yüzdesine sebep olur. Coin'e bağlı olmak üzere genellikle yüzde bir ila beştir. Bitcoin gibi iş ispatı (PoW) kullanan coin'lerin aksine, PoS algoritması kullanan coin'ler tam düğüm çalıştıran ve stake denen bir süreçle işlemleri doğrulayan hesaplara bağlıdır.

Eğer bir oyuncu herhangi bir anda cüzdanına geçirilen (*stake*) coin'lerin toplamının yüzde 51'ini kazanırsa, diğer oyuncuları geçersiz kılıp coin'lerini çifte harcayabilir. (İşlemi gerçekleştirenler, Bitcoin madencilerinin proof-of-stake coin'lerinin versiyonudur. Daha detaylı açıklama için anahtar sözcük bölümünde proof-of-stake'in tanımına bakın.) Çalınan VeriCoin miktarı mevcut toplam VeriCoin'in yüzde otuzunu oluşturuyordu ve birçok kullanıcı coin'lerini onaylatmaya gerek duymadığı için, çalınan coin'ler cüzdana aktarılırsa, ağda rahatlıkla baskın çıkabilirlerdi.

Bu durum en sonunda VeriCoin'in kripto para topluluğunda yapılması en tartışmalı ve zor şeylerden biri olan sert çatallanma yaratmasına ve blok zincirinin değişmesine neden oldu.[1]

Blokzincirinin güvenilir olması gerekiyor; coin'in geçmişinin tartışılmaz hesabı olduğu için dini metin gibi saygı gösteriliyor. Kripto para savunucuları sık sık onu değiştirmenin imkânsız olduğunu söylerler.

Ama mümkün ve VeriCoin bunu kanıtladı. Katılımcıların yüzde ellisinin değişimi kabul etmesini sağlamak yeterlidir. Eğer değişime uğrayan blok zincirinde orijinal blok zincirinde olduğundan daha fazla madencilik yapan insan varsa, yenisi geçerli zincir olur. Herkes bunun farkındaydı, ama birçok kişi topluluğun böyle bir şeyi kabul etme olasılığını göz ardı etti. MintPal saldırısı VeriCoin topluluğunu zor bir karar vermeye zorladı. Coin'in kayıtlarını yeniden yazdılar, çünkü yazmasalardı, geleceği olmayacaktı. Çok sayıda kullanıcının varlıklarını kaybetmesinin yanı sıra, coin'e olan güven de kayboldu, çünkü bilinmeyen bir dolandırıcı, teorik olarak olsa bile, ağ üzerinde mutlak kontrol edindi.

Ama MintPal saldırısında VeriCoin'in aldığı ikincil zarar MintPal dolandırıcılığı girişinde sadece bir dipnot olabilir. Saldırının ardından, Moolah adında bir şirketin yönetim kurulu başkanı olan Alex Green aniden sıkıntıya düşen borsanın yardımına koştu. Şirket MintPal'ın sadece yüzde otuzunu satın aldı ve kontrol ona verildi. Daha son-

[1]Higgins, Stan. "8 Million VeriCoin Hack Prompts Hard Fork to Recover Funds." CoinDesk. 14 Temmuz 2014. Erişim tarihi 22 Haziran 2015. http://www.coindesk.com/bitcoin-protected-VeriCoin-stolen-MintPal-wallet-breach/

ra gerçek adının Ryan Kennedy olduğu ortaya çıkan Green kendisini bir güvenlik uzmanı olarak tanıttı ve borsanın eksiklerini giderdikten sonra onu daha güvenli yapacağına söz verdi.

Site yeniden açıldığında, sorunlarla doluydu ve birçok kullanıcı fonlarına ulaşmak için oturum açamadı. En sonunda, sıcak depo cüzdandaki fonlar Kennedy'nin kontrolünde olduğu iddia edilen bir cüzdana taşındı. Kennedy Moolah'tan istifa edip gerçek kimliğini açıklamadan ortadan kayboldu.

Sonunda, ortağı Chelsea Hopkins'le birlikte Birleşik Krallık yetkilileri tarafından tutuklandığında tekrar ortaya çıktı. Kefaletle serbest bırakıldılar ve bu kitabı yazdığım sırada duruşma henüz karara bağlanmamıştı.[2]

MintPal başarısızlığından alınabilecek en önemi ders dış görünüşün meşruluk göstergesi olmadığıdır. Ana akım 'çoklu kripto para' borsaları arasında, MintPal en güzel tasarıma sahip olanlardan biriydi. Bir keresinde bir arkadaşıma MintPal'ın, bana göre, en 'uygun' görünüme sahip olduğunu söylemiştim ama o görünüm aldatıcı çıktı. Söylemek istediğim şu, bir borsanın güvenlik kapasitesine değer biçmek için bir web sitesinin tasarımından daha derinine bakmalısınız. İnsanlar 'Alex Green'in' kimliğini derinlemesine inceleselerdi, birçok kişi yüklü miktarda parasını kurtarabilirdi.

Sheep Marketplace (Koyun Pazarı)

Sheep Marketplace federal yetkililer Silk Road'u kapat-

[2]Riley, Duncan. "MintPal Scammer Ryan Kennedy Arrested in U.K. over Theft of 3,700 Bitcoins." SiliconANGLE. 23 Şubat 2015. Erişim tarihi 22 Haziran 2015. http:// siliconangle.com/blog/2015/02/23/MintPal-scammer-ryan-kennedy-arrested-in-u-k-over-theft-of-3700-bitcoins/

tıktan sonra sitenin yerini alması için inşa edildi. Silk Road 2 de kısa bir süre önce kapatılmış ve sahibi sistemdeki bitcoin'lerle kaçmıştı.

Birçok kişi Sheep Marketplace'in de aynı yolu izleyeceğinden şüphelendi ve korkularında haklı çıktılar. Sheep Marketplace'teki çekim işlemleri durdu ve sitenin lideri dolandırıcılığın suçlusu olarak tek bir kişiye işaret etti. Birçok kişi ise sitenin sahibini sahtekârlığın faili olmakla suçladı.

En sonunda, Çek haber siteleri sayesinde Sheep Marketplace'in eski sahibi Thomas Jiřikovský'in, Silk Road yönetici Ross Ulbricht gibi uyuşturucu ve organize suçtan ötürü değil, lüks bir ev alıp çaldığı bitcoin'lerin geri kalanını kurduğu paravan şirketler vasıtasıyla kız arkadaşının banka hesabına yatırarak para aklamaktan ötürü tutuklandığı ortaya çıktı.

Bu haberler hiçbir zaman doğrulanmadı ve Sheep Marketplace'in eski kullanıcılarının, sitedeki ticaretin doğası düşünüldüğünde, kaybettikleri fonları geri alma umutları suya düştü.[3] Bu olaydan alınması gereken ders çok açık: bitcoin'lerinizle kanunsuz bir şey yapıyorsanız, işler ters gittiğinde başvurabileceğiniz çok az yer var.

Paycoin/GAW

Paycoin eski madencilik şirketi GAW Miners'ın yarattığı bir kripto paradır. GAW Miners ve kardeş şirketi ZEN Miners, Josh Garza adıyla bilinen Homero Joshua Garza adında bir adama aitlerdi. Garza, müşterilerini terk etme-

[3] "Breaking: Sheep Marketplace Owner Arrested." Deep Dot Web. 27 Mart 2015. Erişim tarihi 22 Haziran 2015. https://www.deepdotweb.com/2015/03/27/breaking-sheep-marketplace-owner-arrested/

den önce kazıklamakla suçlanan ve halen soruşturma altında olan bir geniş bantlı internet şirketini idare ettikten sonra kripto para işine girdi.[4]

GAW Miners esasında madencilik donanımı satıyordu. İlk başta, başarılı görünüyor. Butterfly Labs ve KnCMiner'la birlikte bir zamanlar madencilik pazarındaki 'Büyük Üçlü'nün' bir parçası olarak görülüyordu. Bir noktada, gönderiler hakkında şikâyetler ve kullanılmış donanım göndermekle suçlalar ortaya çıktı, ama bu o sırada Bitcoin madencilik şirketleri için sıra dışı değildi, KnCMiner ve özellikle de Butterfly Labs benzer suçlamalar ve sorunlarla karşı karşıyaydılar.[5] [6]

GAW Miners en sonunda o dönem için kuşkusuz yenilikçi olan bazı özellikler barındıran 'bulut madencilik' şirketi olmaya geçiş yaptı. Müşteriler hash gücü satın alıp o sırada hashpoint olarak bilinen bir dahili dijital para birimiyle onu temsil ettirebiliyorlardı. Hashpointler, kullanıcıları için Bitcoin üretmenin yanı sıra –her hashpointin madencilik gücünü temsil etmesi gerekiyordu– satın alınıp diğer müşterilere satılabiliyorlardı. Bitcoin madenciliği daha kârlı olursa, hashler de olacaktı. Uzun 'bulut madencilik' kontratları riskine girmeden insanların madenciliğe girmelerinin kolay bir yolunu temsil ediyorlardı. Bir sü-

[4]Mansfield, Erin. "SEC Investigates Vt. Broadband Company Founder." VTDigger. 8 Temmuz 2015. Erişim tarihi 11 Ocak 2016. http://vtdigger.org/2015/07/08/sec-investigates- vermont-internet-service-company-founder/

[5]Maina, John Weru. "FTC Shuts Down Butterfly Labs... Finally." CCN Financial Bitcoin News. 23 Eylül 2014. Erişim tarihi 22 Haziran 2015. https://www.cryptocoins-news.com/ftc-shuts-down-butterfly-labs-finally/

[6]Gillis,RickMac."TimelineofKncMiner'sStruggleWiththe20nmASICBitcoinMiners." CCN Financial Bitcoin News. 22 Temmuz 2014. Erişim tarihi 22 Haziran 2015. https://www.cryptocoinsnews.com/ccn-reveals-timeline-kncminers-struggle-20nm-asic-bitcoin-miners/

reliğine, GAW'ın pazarından hashpoint satın almak teorik olarak Bitcoin ağında madencilik gücü almanın en ucuz yoluydu. Güvenlik ve Borsa Komisyonu (Security and Exchange Commission - SEC) GAW Miners ve Garza'dan şikâyetçi olunca, GAW'ın aşırı hashpoint satışı yaptığı ve üreteceklerini iddia ettikleri bitcoin sayısına ulaşmak için yeterli donanıma sahip olmadıkları söylendi.

Güvenlik ve Borsa Komisyonu'na göre, madencilik ödemelerinin çoğu yeni yatırımcıların parasıyla ödenmişti.[7]

Birçok medya kuruluşu, özellikle de kripto paralara odaklananlar, Aralık 2014'te Paycoin'in ilk satışından sonra GAW hakkında yeterince haber yapmış olsalar da, ilk incelemenin büyük bir kısmı en popüler Bitcoin mesaj panosu olan BitcoinTalk kullanıcıları tarafından yapıldı. Suchmoon adlı bir kullanıcının başlattığı genel konu başlığına atıfta bulunuldu ama bireysel katkılara değinilmedi. Bu konu başlığı, doğru düzgün bir şekilde referans gösterilemeyecek kadar dağınıktı ve bazı üyeler bu ilgiden hoşlanmadılar. Bununla birlikte, katkısı paha biçilmezdi.[2]

GAW'da işler göründüğü gibi değildi ve ödemeler yavaşlamaya başladı. En sonunda, hashpointlerin madenciliği bırakacağı ve GAW'ın vaadine göre, kullanıcıların onları devrimsel olacak yepyeni bir kripto paraya dönüştürebilecekleri duyuruldu. Bu, dolandırıcıların onlarca yıldır baş-

[7]"SEC Charges Bitcoin Mining Companies." SEC.gov. Securities and Exchange Commission. 1 Aralık 2015. Erişim tarihi 11 Ocak 2016. http://www.sec.gov/news/ pressrelease/2015-271.html

[8]Suchmoon, Miaviator, and More "GAW / Josh Garza Discussion Paycoin XPY Btc.com Bitcoin'ist. ALWAYS MAKE MONEY :)." Bitcointalk Post. 14 Kasım 2014. GAW / Josh Garza Discussion Paycoin XPY CPIG BTCLend Xpyerr. ALWAYS MAKE MONEY :). Erişim tarihi 22 Haziran 2015. https://bitcointalk.org/index.php?topic=857670. msg11401660%3Btopicseen#msg11401660

vurduğu sıradan bir yöntemdir: Sahtekârlığın doğal akışı sona erdiğinde, onu genellikle bir diğeri izler.

Birkaç adayı gözden geçirdikten sonra, şirket ve topluluk en sonunda Paycoin ismine karar verdiler ve altcoin temelli tartışmasız en büyük sahtekârlık başlamış oldu.

Güvenlik ve Borsa Komisyonu soruşturmasından edinilen sızmış e-postalar aşağıdaki suçlamaları doğrulasa da, yasal sebeplerden ötürü Homero Joshua Garza'nın henüz suçlu bulunmadığına dikkat çekmek gerekir. Ama yolsuzluklar ve yalanların upuzun listesine bakılırsa, okunurluğun hatırına, bunu şimdi aradan çıkarmak istiyorum: Aşağıdaki suçlamalar mahkeme tarafından doğrulanmadı; kanıtların ezici olmasına rağmen, yasal açıdan bakıldığında hepsi iddia durumunda.

Paycoin'in ilk sitesi birçok vaatte bulunuyordu. İddialara göre, Paycoin'in çok ciddi yatırımcıları vardı. Büyük bir ticari destek vaat ediyordu ve Amazon, Target ve diğer büyük tacirlerin logolarını bulunduruyor ve görünürde bu sitelerin Paycoin ile ödemeleri kabul edeceğini ima ediyordu. Sitenin iddialarına göre, Paycoin kullanıcıları Paycoin kullanarak faturalarını ödeyebileceklerdi.[9]

Her şeyden önemlisi, en azından yatırımcılar için, $20 taban fiyat vaat ediyordu. GAW piyasaya sunulduktan sonra Paycoin'in fiyatının hiçbir zaman $20 altına düşmeyeceğini belirtti. Bunu desteklemek için sözde $100.000.000 değerinde bir 'Topluluk Eylem Fonu' yaratıldı ve bu benimsenme, geliştirme ve fiyat yirmi doların altına her düştüğünde şişirmek için kullanılacaktı.

---

[9]"Paycoin Is Here | Paycoin Digital Currency." Paycoin Is Here | GAW-Miners, Republished by Archive.org. 17 Mayıs 2014. Erişim tarihi 22 Haziran 2015. https://archive. is/01HEwd. http://paycoins.biz/paycoin/

Paycoin ilk başta bir coin'i dört dolardan 'ilk benimseyenlere' sunuldu. Aralık 2014 sunumu yaklaşırken, bu belirli aralıklarla yükseldi ve en sonunda bir coin on iki dolar oldu. On iki dolarlık bir coin yirmi dolardan oldukça düşüktü, o nedenle hikâyeye inanan yatırımcılar hâlâ riske girmeden kazanabilecekleri yüklü miktarda para olduğunu düşündüler. Paycoin'le ilgili ilk hashtalk.org yazıları Josh Garza'nın Noel'lerini nasıl kurtardığıyla ilgili heyecanlı açıklamalar içeriyordu.

GAW Paybase adında bir site açtı. Paycoin satın almanın başlıca yolu ve müşterilerin faturalarını ödeyip Paycoin'in diğer sözde özelliklerinden faydalanabilecekleri bir site olacaktı. Aynı zamanda müşteriler coin'lerini $20 karşılığında bozdurabileceklerdi. GAW'ın Bittrex gibi diğer borsalarda coin'lerin fiyatı üzerinde kontrolü olmasa da, Paybase'de $20 ödemeyi vaat ediyordu. Bu, elbette, ancak Bittrex gibi borsalarda fiyat $20 ya da üzerinde, ya da arbitraj fırsatı önemsiz olabilecek kadar yakınında (örneğin, $19,95) kalırsa makuldü. Doğal talep, fiyatı yeterince yüksek tutmadıkça, GAW'ın Paycoin alım-satımı yapan her borsadaki fiyatı desteklemesi gerekecekti. İnsanlar Bittrex'te Paycoin alıp onları Paybase'de GAW'a satabilirler ve sonra o parayı daha fazla Paycoin almak için kullanabilir ve fiyat $20'a yükselene ya da GAW parasız kalana kadar bitmek bilmeyen bir döngüyü tamamlayabilirlerdi. Görünürde $100.000.000'lık Topluluk Eylem Fonu bunun için kullanılacaktı. Gerçekten inananlar, özellikler teker teker sunuldukça ve tacirler teker teker gemiye bindikçe fiyatın doğal olarak $20 üzerinde kalacağını düşündüler. Daha sonra, böyle bir fonun hiç olmadığı, özelliklerin sunulma-

yacağı ve vaat edilen tacirlerin Paycoin'le bağlantılarının olmadığı ortaya çıktı.

Garza ve GAW hakkında olumlu düşünmeye çalışıp bir an için bu planın işe yaraması için ellerinden geleni yaptıklarını, bunun heyecan yaratıp milyonları ceplerine indirmenin bir yolu olmadığını söylesek dahi, her şey kusursuz bir şekilde gitmiş olsaydı bile, planın bir sorunu vardı.

GAW Paycoin'in $4, $8 ve $12 fiyatlarında fazlasıyla reklamını yapıyordu. *The Wall Street Journal*'ın MoneyBeat blogunda bir makalesi yayınlandı.[10]

İnternetteki bütün büyük kripto para medya kuruluşlarına reklam ücreti ödediler ve büyük bir kongrenin sponsoru oldular. Paycoin'e ilk başta ilgi gösterebilecek herkes onu duymuştu ve o düşük fiyatlardan Paycoin satın alma imkânları vardı. Neden tipik bir Cryptsy ya da Bittrex kullanıcısı Paycoin'i $12 ya da daha düşük bir fiyattan satın alabilecekken $20'dan satın alsın ki?

Paycoin'in bu fiyat etiketini hak ettiğini göstermek için son derece başarılı bir şekilde faaliyete geçirilmesi gerekiyordu, özellikle de GAW'ın ön satış ve piyasaya sürülme döneminde coin'i o fiyattan satarak pazarı düşük tutmuş olması düşünülürse. Kripto para topluluğunda Paycoin'i duymayan ve $20'ın altındaki farklı fiyatlardan satın alma fırsatını kaçırmayan çok az kişi vardı. Birçoğu Paycoin'in Garza'nın sattığı fiyata değer olmadığını düşünüyorlardı ve o fiyata değer olduğunu düşünenler ise çoktan satın almışlardı.

[10]Casey, Michael J. "BitBeat: GAW Miners to Launch Bitcoin Challenger, Paycoin." MoneyBeat RSS. 25 Kasım 2014. Erişim tarihi 22 Haziran 2015. http://blogs.wsj.com/moneybeat/2014/11/25/bitbeat-gaw-miners-to-launch-bitcoin-challenger-paycoin/

Başarılı bir faaliyete geçiş yerine, her adımda sorunlarla karşılaştılar. Öncelikle, Paybase Noel sonrasına ertelendi. Bu esasen çocuklarına Noel hediyesi almak için ayırdıkları paralarını buna yatıran yatırımcıların şikâyet etmelerine neden oldu. Paycoin Visa'yla bir anlaşma yapacağını söyleyerek heyecan yaratmıştı; bu gerçekleşmeyince, Garza Paycoin'in aleyhinde konuşanları Visa'yı korkutup kaçırmakla suçladı. Bu sırada, Amazon, Walmart ve Target Garza'yla bağlantıları olduğunu inkâr ettiler ve Paycoin'le ilgili soruları yanıtlamadılar. Garza bir anlaşma üzerinde çalıştıklarına dair iddialarını kanıtlamak için hiçbir şey sunamadı. Daha sonra, sızan bir e-posta sorunu aydınlattı ve Paycoin/GAW çalışanları ve söz konusu şirketler arasında hiçbir iletişim olmadığını ve hatta buna hiçbir zaman kalkışılmadığını ortaya çıkardı. Ayrıca, Visa kartları basmaya izni olmayan bir şirketle gönülsüzce ve aceleye getirilmiş bir ortaklık yapılmıştı. Daha sonra Garza, MasterCard damgalı hesap kartı için bir anlaşmaya varmak üzere olduklarını iddia etti, ama MasterCard bu iddiayı kesin olarak reddetti.[11]

Kısacası, Garza ve GAW'ın vaat ettiği özelliklerin hiçbiri gerçekleşmedi. Kayda değer siteler tarafından benimsenme, hesap kartı, fatura ödeme özelliği ve PayFlash (sözde 'dünyadaki en büyük e-ticaret sitelerinde kullanılabilir fon' için anında Paycoin'e dönüştürme) yoktu; ayrıca Paycoin resmi olarak hizmete girdiğinde, gördüğü en yüksek seviye $13,50'ti. GAW daha sonra $20 taban fiyatı korumaya çalıştığını ve $20'dan bir miktar Paycoin satın

[11]Johnson, Mike. "MasterCard Denies PayCoin Partnership." Coin Fire. 25 Şubat 2015. Erişim tarihi 22 Haziran 2015. http://coinfire.io/2015/02/25/mastercard-denies-paycoin-partnership/

aldığını iddia etse de, serbest piyasa fiyatı $14 bile bulmadı. Paybase bir Paycoin karşılığında $20 ödediyse bile, bu sadece çok kısa bir süre için geçerliydi. İnsanlar Garza'nın başarmasını beklerken işler bir süre daha dayandı. Hatta bazıları bu 'düşük' fiyattan coin alma ihtimali karşısında heyecanlı görünüyordu.

Zemin hiçbir zaman desteklenmemişti ve her şey hızla yıkılmaya başladı. Kullanıcıların Paybase'e Paycoin yatırabilecekleri ve GAW'ın bir coin'in $20 olacağı vaadini yerine getireceği bir 'Onur' programı duyuruldu, ama bunu ayda sadece belirli sayıda Paycoin için yapabilecekti. Bu, geçici bir fiyat toparlanması için yeterince iyiydi ama fiyat tekrar kırıldı. Ancak, çok geçmeden medya kuruluşları piyasaya sürülme anında satın alınan Paycoin'lerin ödenmesi planının onlarca yıl süreceğine; kullanıcıların serbest piyasadan satın aldıkları Paycoin'leri (aylar sonra bile) Paybase'de satarak sonsuz bir döngü içinde Paycoin'leri hareket ettirebilecekleri için planın makul olmadığına ve işe yarasa bile muhtemelen yasa dışı olacağına dikkat çekti.

Her şey yıkılmadan önce bile, topluluk o kadar kızgındı ki, Garza Miami'de düzenlenen Kuzey Amerika Bitcoin Konferansı'ndaki (The North American Bitcoin Conference – TNABC) konuşmasını iptal etmek zorunda kaldı. İnsanların öfkesi TNABC liderlerinin topluluğun ona zor sorular yöneltebilmesi için konuşmasına izin vermeye karar vermelerine neden olacak kadar güçlüydü. Ama Garza bu planı ve organizatörleri son anda yüzüstü bıraktı.[12]

---

[12]DeMartino, Ian M."Last Minute TNABC Changes: Garza Cancels, Robot Roger Ver and More." CoinTelegraph. 16 Ocak 2015. Erişim tarihi 22 Haziran 2015. http://cointelegraph.com/news/113314/last-minute-tnabc-changes-garza-cancels-robot-roger-ver-and-more

O sırada, Baş Kontrolörler bir sorun haline geldi. Baş Kontrolörler Paycoin'in sözde özelliklerinden biriydi. Her proof-of-stake coin gibi, Paycoin'in işlemleri de cüzdanlarını açık tutan ve onları cüzdana aktaran kullanıcıları tarafından doğrulanıyordu. Daha sonra ağ için işlemlerini doğrulayıp coin'lerine faiz oluşturuyorlardı. Paycoin'de belirlenen faiz oranı oldukça yüksekti: %5. Ama en yüksek teklifi sunan kişilere verildiği iddia edilen bu Baş Kontrolör hesapları yüzde onluk bir stake oranı belirlediler. Esasında, bu Baş Kontrolörlerin sıradan stake işleminden daha zor görevleri yerine getirip getirmeyecekleri net değildi, ama daha sonra sıradan cüzdan aktarımcılarından daha farklı bir şey yapmadıkları ve sadece daha fazla para ödedikleri için ödüllendirildikleri kanıtlandı.

Ne olursa olsun, çoğu hâlâ GAW tarafından kontrol edilen Baş Kontrolörlerin birçoğunun aslında yüzde ondan daha yüksek oranda stake işlemi uyguladıkları ortaya çıkınca işler iyice kötüye gitti. Blok zincirinin gözden geçirilmesi sonucunda, belirli Baş Kontrolörlerin günde birkaç kez birleştirildiğinde toplam yüzde 3,500 faiz oranına eşit olan yüzde 350 gibi çılgınca bir oranla cüzdanlara aktardıkları ortaya çıktı.

Paycoin'in kripto para topluluğunda biraz güvenilirliği kaldıysa bile, bu skandal onu öldürdü. Kripto paraların en cazip özelliklerinden biri merkezsizleştirilmiş olmaları ve tek bir kişinin kontrolünde olmamalarıdır. Eğer Paycoin rahatlıkla basılabilirse –ve Baş Kontrolörler hiç şüphesiz dijital para basma makineleriydiler– onu bir merkez bankasının desteklediği para biriminden ayıran pek fazla bir şey olmaz. Aradaki tek büyük fark, güçlü bir hükümet

tarafından desteklenmek yerine, Paycoin Homero Josh Garza ve kurduğu şirketin sözleriyle destekleniyordu ve güvenilir olmadığı çabucak kanıtladı.

Çok geçmeden, büyük haber duyuldu: Güvenlik ve Borsa Komisyonu GAW Miners ve Josh Garza hakkında bir soruşturma açmıştı. Garza ilk başta bu iddiayı yalanladı ve bu haberi yapan siteye karşı yasal işlem başlatmayı düşündüğünü söyledi.

Ama en sonunda GAW, Güvenlik ve Borsa Komisyonu ve diğer yetkililer arasında bir şeyler olduğu ve olmaya devam ettiği, diğer medya kuruluşları ve gerçek Güvenlik ve Borsa Komisyonu dokümanlarıyla doğrulandı.[13] Bu soruşturma hâlâ sürüyor ve kitabı yazdığım sırada Güvenlik ve Borsa Komisyonu'nun dava hakkında kamuyla paylaşabileceği çok az şey vardı. Ayrıca, GAW'a dava açıldığı sırada $130,000'ın üzerinde elektrik faturasını ödemeyi ihmal ettiği ortaya çıktı. GAW mahkemeye çıkmadı.[14]

Garza ve birçok GAW çalışanının e-postaları sızınca işler iyice çirkinleşti. Her şey ortadaydı ve neredeyse GAW ve Paycoin hakkındaki bütün şüpheler doğrulanmış görünüyordu.

E-postalar Garza'nın düzenli yatırımcılara Harry Potter serisinde büyücülük yeteneği olmayan karakterlere verilen isimden esinlenerek *muggles* (beceriksizler) diye hitap ettiğini gösteriyordu. Ayrıca, Visa ya da MasterCard'la hiç-

[13]Johnson, Mike."Coin Fire+: GAW Miners Catches SEC, FTC, IRS, DHS Attention." Coin Fire. 5 Mart 2015. Erişim tarihi 22 Haziran 2015. http://coinfire.io/2015/03/06/coin-fire-gaw-miners-catches-sec-ftc-irs-dhs-attention/

[14]Higgins, Stan. "GAW Miners Absent in Ongoing Mississippi Court Case." CoinDesk. 18 Haziran 2015. Erişim tarihi 11 Ocak 2016. http://www.coindesk.com/gaw-miners-absent-court-case/

bir görüşme olmadığını; Garza'nın şirketinin yüzde yüzünden fazlasını taahhüt ettiğini; saygın bir yatırım şirketi olan Cantor Fitzgerald'ın ortağı Stuart Fraser'dan muazzam miktarda borç aldığını gösteriyordu.

Garza hem Fraser hem de onun şirketinden para çalmış, çalışanlarını kandırmış, karısı kıskandığı için gönül ilişkisi olan çalışanını kovmuş, bir emlak satışı yaptıktan sonra ortadan kaybolmuş, üç arabasını satmış ve e-postasında bir fatura bulunmasına rağmen o arabaları nasıl aldığı konusunda insanlara yalan söylemiş (Tesla'dan "Elon Musk'ın bir hediyesi" diye bahsetmişti), iş ortaklarının ödemelerini yapmakta zorlanmış ve daha birçok yolsuzluğa karışmış görünüyordu.

Birçok senaryoda, bu şirketin sonu olurdu. Her şey sona erer ve herkes kendi yoluna giderken müşterilerin elinden SEC soruşturmasının onlara yatırımlarını geri döndürmesini ummaktan başka bir şey gelmezdi. Sorun şu ki, bir coin'in güvenilmez biri tarafından yaratılması ve dönüştürülebilir özelliğinin olmaması, o coin'in ortadan kaybolması anlamına gelmez.

Bütün bu olaylar süresince, Paycoin'in fiyatı düştü. Bu kitabı yazdığım sırada, fiyatı 0,05 dolardı. Bu vaat edilen $20 taban fiyatından çok uzak ama yine de birçok meşru ve işe yarar altcoin'den çok daha yüksekte ve bu çok para ödeyen bazı insanların –değersiz olduğu kanıtlansa da– yatırımlarına tutunmaya razı olduklarını gösteriyor. Çok az kişi Paycoin'i $20'dan satın almak istedi, çünkü daha ucuza satıldığını biliyorlardı; bu psikolojinin tersi coin'in tamamen ölmesine engel oldu. Ama hiçbir yere gitmiyor. Paycoin kripto paranın geleceği ve hatta önemli bir oyun-

cusu bile olmayacak. Ona bulaşan herkes vazgeçene ya da sıkılana kadar altcoin dünyasının derinliklerinde debelenecek.

İnsanlar Paycoin için çok para ödediler. O kadar çok ki, onu $5 ya da $1'dan satmak onlar için büyük bir kayıp olacaktı. Coin'in değeri $0.50 ve $0.25 kilometre taşlarını gördüğünde de yatırımlarına tutunmaya devam ettiler; ama sonra durum daha da kötüye gitti. Paycoin'i $12'dan alan yatırımcıların o fiyatlardan satmakta tereddüt etmeleri anlaşılabilir, ama o zaman karşılığında alacakları küçük tutar bile, tutunmaya devam ettikleri şeyden daha iyi olabilirdi.

Soğuk algınlığı için size $12'dan yılan yağı satsam ve daha sonra iddia edildiği gibi çıkmadığını ya da pek etkisi olmadığını keşfetseniz, onu bir dolara satmaya razı olur musunuz? Peki ya $0,50'a? Ya da $0,25 ve $0,01?

Söylemek istediğim şu: İşe yaramadığını bildiğiniz yılan yağını elinize geçen herhangi bir meblağ karşılığında satmalısınız. Ama yatırımcılar duruma bu açıdan bakmakta zorlandılar. Onlara göre, coin'e $12 ödemişlerdi ve $12,01'in aşağısında bir fiyata satmak başarısızlık anlamına geliyordu.

Bu bir başarısızlık olabilir, ama $10'dan satmak $0.10'dan satmaktan daha az başarısızlıktır; tıpkı $0,10'dan satmanın $0,01'dan satmaktan ve $0,01'dan satmanın $0.0001'dan satmaktan daha az başarısız olacağı gibi (kripto paralarda bu mümkün).

Çok fazla para yatıran bir kişinin düşük fiyattan elindeki coin'leri satmak yerine bekleyip görmeye karar vermesi anlaşılabilir. Genel olarak, fiyat düşükken satış yapmak

hiçbir zaman iyi bir yatırım hamlesi değildir ama $14'dan muhteşem düşüşüne rağmen, Paycoin aşırı değerliydi. Paycoin, Nxt gibi bir para biriminden daha fazla toplam coin'e ve daha kötü ve muhtemelen kötü niyetli bir geliştirici ekibine sahip. Para birimini mahvetmek için her an etkinleştirilebilecek Baş Kontrolörleri var. Ne yaptığını bilen çok az kişi 'Paycoin Vakfi'nın' ne yaptığını dikkate alıyor. Paycoin'in itibarı bir zamanlar ortaklık yapacağını iddia ettiği şirketleri kendisinden uzaklaştırdı, coin'in yaratıcıları SEC tarafından soruşturuluyor ve Baş Kontrolörleri hesaba katmazsak bile, sıra dışı olabilecek kadar yüksek bir faiz oranı var. Her NXT yaklaşık olarak bir buçuk sent değerindedir. Daha önce bahsettiğim gibi, bu kitabı yazdığım sırada, bir Paycoin yaklaşık beş sent değerindeydi. Bu kitabı okuduğunuz sırada muhtemelen daha düşük olacak, ama bir Paycoin birkaç yüz satoshi'den daha yüksek olduğu sürece (bir sentin yüzde biri), Paycoin aşırı değerli sayılır.

Birçok vaatte bulunuldu ve hiçbiri gerçekleşmedi. Coinstand kullanıcıların Amazon ürünleri satın alırken her biri $20 değerindeki Paycoin'lerini kullanabilecekleri bir hizmet olarak tanıtıldı. En nihayetinde bu yüzde beş düşürüldü, ama bunun Paycoin sahiplerinin çoğu için önemi yoktu, çünkü sistem sadece, muhtemelen Garza'nın seçtiği, küçük bir grup 'beta sınayıcılarına' açıktı. (Bir iki hafta topluluğa en sadık üyelerini aday göstermelerini isteyen bir mesaj yayınlamıştı.) Gruptaki birkaç kişinin siparişleri teslim edildi ama çok geçmeden ürünlerin gönderimi durdu, günümüzde site çalışmıyor ve yeniden canlandırılması hakkında hiçbir görüşme yok.

GAW çökerken liderlik bölündü ve yeni kurulan Paycoin Vakfı Garza'yla arasına mesafe koymaya çalıştı. Başka bir geliştirici, Coinstand'den sorumlu olan Phil Vadala her iki gruptan da ayrıldı ve iddialara göre Garza'dan birkaç Baş Kontrolör çaldı ama Garza'nın sözde özel yatırımcılara satılan Baş Kontrolörlere nasıl sahip olduğu net değil. Daha sonra, ilk başta siteyle hiçbir ilgisi olmadığını iddia etmesine rağmen, Coinstand'i Garza'nın finanse ettiği ortaya çıktı.

Bu eylem Garza'nın Baş Kontrolörlerin Rusya'da organize suç unsurlarına ve sinirlendirilmemesi gerektiğini söylediği Orta Doğulu bir yatırımcıya ait olduklarını iddia ettiği Vadala'yla yaptığı Skype görüşmesini yayınlamasına neden oldu.[15]

Suç örgütleriyle anlaşma yaptığını itiraf etmenin bir hata olabileceği Garza'nın aklına gelmemiş gibi görünüyordu. Ayrıca, eski geliştiricilerinden birini üstü kapalı bir şekilde tehdit etmesinin ve topluluğun çıkarından ziyade sözde ilk yatırımcılara –hem de suça meyilli yatırımcılara– öncelik verdiğini açıklamanın topluluğun geri kalanı için endişe verici olacağını akıl edememişti.

Bu konu hakkında Garza'yla röportaj yaptığımda, Vadala'nın işlediği iddia edilen hırsızlık suçundan ziyade sözlerinin beni daha çok endişelendirmiş olmasına şaşırmış görünüyordu.[16]

---

[15]DeMartino, Ian M."Josh Garza Breaks Down, Admits To Working With Mobsters, Going To Dubai In Bizarre Post." Mining Pool. 6 Mayıs 2015. Erişim tarihi 22 Haziran 2015. http://coinjournal.net/josh-garza-breaks-down-admits-to-working-with-mobsters-going- to-dubai-in-bizarre-post/

[16]DeMartino, Ian M. "The Josh Garza Interview." Mining Pool. 11 Mayıs 2015. Erişim tarihi 22 Haziran 2015. http://coinjournal.net/the-josh-garza-interview-organized- crime-threats-and-is-he-in-america/

Ama bahsettiğim gibi, Paycoin teknik olarak hâlâ hayatta. Hâlâ farklı borsalarda alınıp satılabilir ve topluluğunda kalan birkaç kişi var. Garza, GAW Miners ve ZEN Miners'ın hepsi süregelen SEC soruşturmalarının hedefleri olmalarına rağmen, oldukça durgun bir şekilde olsa da coin hayatına devam ediyor.

Topluluğun son iki üyesi de çekilip borsalar onu satışa sunmayı bıraktığında, Paycoin ölecek. Birçok kişi muhtemelen ölümünü kaçınılmaz son olarak görse de, bu gerçek kripto paraların ne kadar dayanıklı olduğunu gösteriyor. Paycoin kripto paranın değer verdiği neredeyse her prensibi (merkezi olmayan kontrol, sınırlı arz, şeffaflık) çiğnedi ve onu yaratmak için kötü niyetle yola çıkan, ortalıktan kaybolan ve yetkililerle süregelen bir davası olan muhtemel bir dolandırıcı tarafından yönetildi; ama bunlara rağmen ağ işlevini yerine getirmeye devam ediyor. Bu dürüst geliştirici ekipleri olan ve özellikle de Bitcoin gibi bütün ekonomisiyle onu desteklemeye yardım eden para birimleri için iyiye işaret.

Paycoin'den alınması gereken ders şu: bir şirketin ana akım medya kuruluşları tarafından haberlerinin yapılması, güvenilir olduğu anlamına gelmez. Bütün dolandırıcılar gibi, Bitcoin dolandırıcıları da bir projeden diğerine geçmeye meyillidirler; eğer bir şirket yeni bir girişime geçiş yapıyorsa, hızla çökmekte olan bir saadet zincirine taze para çekmeye çalışmadığından emin olun. Eğer biri size yatırımınızı yüzde 500 artırmayı vaat ediyorsa, yalan söylüyordur. Ve 'HODL' (evet, 'HOLD', yani *tutmak* sözcüğünün komik bir yanlış telaffuzu) Bitcoin'de uzun vadeli yatırım yaparken iyi bir strateji olması, ihtilaf çıktığında

toparlanma umudu olmadan neredeyse bütün değerini hızla kaybeden altcoin'ler için beklemek uygulanabilir bir strateji değildir.

Bitcoin dünyası dolandırıcılarla dolu. Bu onun bir sahtekârlık ve kaçınılması gereken bir şey olduğu anlamına gelmez. Aynı şekilde, internet de dolandırıcılıklarla dolu. Ama Nijeryalı prens skandalı ve sahte Bank of America oltalama e-postalarına alışmamızın biraz zaman alması gibi, kripto para dünyasına bulaşan sahtekârlıklara alışmamız da zaman alacak. Paranın olduğu yerde, dolandırıcılar eksik olmaz. Bitcoin *paradır*, o nedenle dolandırıcıların ilgisini çekmesi çok doğal. Bütün bunlar şu anlama geliyor: dikkatli olun. Araştırmanızı yapın ve kaybetmeyi göze aldığınız miktardan daha fazlasıyla asla yatırım yapmayın. Bu noktada bunu söylemek neredeyse klişe, ama Bitcoin gerçekten Vahşi Batı, tek farkı düzeni sağlayan bir şerifin olmaması.

İKİNCİ KISIM:
Bitcoin'e Yatırım Yapmak

Onuncu Bölüm:

Banka Hesabı, Nakit ve PayPal ile Bitcoin Satın Almak

Normalde size borsada nasıl para kazanacağınızı söyleyen bir kitap önermem. Bu kitapların çoğu saf insanlara yöneliktir ve genellikle yatırım yapan insanlardan ziyade yazarlarına para kazandırırlar.

— *Financial Times* yazarı Gavyn Davies

İnsanlar Bitcoin'e bir ağ, dağıtık hesap defteri ve birçok şey dediler, haksız da değiller. Bitcoin her şeyden çok bir para birimi, *değerin* izini sürmenin ve transfer etmenin bir yolu. Söz konusu para birimi olduğunda, insanlar kaçınılmaz olarak nasıl daha fazlasına sahip olabileceklerini sorarlar.

Size Bitcoin'le nasıl zengin olacağınızı öğretemem. Dört dörtlük bir planım olsaydı, bu kitabı yazmak yerine onu uygulardım. Ama sizi doğru şekilde yönlendirmeyi

umarak sizin için manzaraya basit bir genel bakış ve Bitcoin'le çalışmak için temel teknikler sunabilirim.

Gün içi işlemler, oynak menkul değerlerden kâr etmek için günlük alım-satım yapma işi, bazıları için hiç şüphesiz çok kazançlı. İnsanlar her gün Bitcoin ve diğer para birimlerinden alıp satarak para kazanıyorlar. Ben bunu yapmıyorum. Bir sebebi, harcanabilir gelirimin olmaması ve potansiyel kazancın harcayacağım vakte ve çabaya değeceğini düşünmemem. Ama tek sebebi bu değil.

Gün içi kripto para işlemleri acımasızdır. Bitcoin ve diğer birkaç büyük altcoin ve projeler dışında, neredeyse her kripto para uzun vadede kötü bir görünüme sahip ve potansiyel kâr genellikle uydurma spekülatif baloncuklara binerek elde edilebilir. Uzun vadede kötü görünmelerinin sebebi çoğunun masaya yeni bir şey getirmemesi, bazen ise getirseler bile yeterli olmamasıdır. Ethereum ana akım şirketlerin bazıları tarafından kabul gördü, UBS ve Barclays gibi büyük bankalar teknolojiyle yaptıkları deneyleri duyurdular, ama bu kullanım son derece nadir.[1] Altcoin'lerin sadece küçük bir bölümü masaya yeni bir şey getirir, onların da sadece çok küçük bir kısmı uzun vadede finansal kapasite gösterir ve *onların* çok küçük bir kısmı kripto para topluluğu dışında ilgi görür. Kripto para alanının yenilik ve iyi niyetli geliştiricilerle dolu olmadığını söylemiyorum. Ama gelişmekte olan teknolojiler düşünüldüğünde, yarı güvenli yatırımlar olduklarını bile söyleyemem. Bir-

[1]Allison, Ian. "UBS and Barclays Are Front Runners with Bitcoin 2.0 Technology Ethereum." International Business Times RSS. IBTimes, 5 Ağustos 2015. Erişim tarihi 29 Ekim 2015. http://www.ibtimes.co.uk/ubs-barclays-bnp-paribas-are-front-runners-bitcoin-2-0-technology-ethereum-1514138

çoğu sadece şişirme ve boşaltma amacıyla var. Buna daha sonra değineceğim.

Bu kitabı yazdığım sırada, kripto para dünyası büyük ölçüde kontrolsüzdü. New York eyaletindeki BitLicense gibi kanunlar uygulamaya konulacak ama yetkililer şimdilik borsaların kara para aklanmasının önlenmesi (AML) ve müşterini tanı (KYC) düzenlemelerini uyguladıklarını denetlemeye odaklanmış görünüyorlar. İçeriden bilgi ticaretini, piyasa manipülasyonunu ya da pek bilinmeyen altcoin'lerde ve kontrolsüz menkul kıymetler borsalarındaki sık görülen diğer şamataları önlemekle pek ilgilenmiyor gibi görünüyorlar.

Sorunların büyük bir kısmından Bitcoin ve belki birkaç altcoin'den şaşmayarak kaçınılabilir. Bir piyasa ne kadar büyükse, düzenleyiciler olsun ya da olmasın, onu manipüle etmek o kadar zordur. Herhangi bir piyasayı manipüle etmenin en sık görülen yolu piyasayı yükseliyor gibi göstermek için kademeli olarak artan küçük alımlar yapmaktır. Piyasa yeterince yükseldiğinde, manipülatör bütün kripto parasını –hisse senetlerini ya da diğer menkul değerlerini– yarattığı yeni fiyattan satar. Bunlar herhangi bir 'şişir ve boşalt' planının temelleridir. Büyük piyasalarda bunu yapmak daha zordur, çünkü manipülatörün fiyatı etkilemek için daha çok alım yapması gerekir.

Bitcoin gün içi işlemcileriyle ilk doğrudan deneyimim 2014'te Washington, DC'deki Bitcoin in the Beltway Konferansı'ndaydı. Bitcoin danışmanlığına ve gün içi işlemciliğine geçiş yapan birkaç eski Wall Street taciriyle tanıştım. İki gün boyunca neredeyse on iki saat süren konferansların ardından, onlarla bir partide buluştum. Parti sona erer-

ken, biri bana başarılı bir gün içi işlemci olmak için gereken bağlılığa sahip olmadığımı anlamamı sağlayan bir şey söyledi. Saat sabah bire yaklaşıyordu ve iki tam gün süren konferansların, partilerin ardından herkes sızmaya hazırdı; bu kişi bana "Japon borsaları birkaç saat içinde uyanacağı" ve bu eylemle kâr etmeyi planladığı için bir süre daha takılmak isteyip istemediğimi sordu.

O anda Bitcoin gün içi tacirlerinin hayvanlar olduğunu anladım. Aynı ölçüde takıntılı olmadıkça onlarla baş edemezsiniz. O seviyeye gelmek için bu kitaptan daha fazlasına ihtiyacınız var. Hiç çalışmadan para kazanılan sektörler son derece rekabetçi ve ironik bir şekilde, çok fazla çalışmayı gerektiriyor. Menkul kıymetler borsalarının aksine, Bitcoin borsaları asla kapanmıyor ve uyandığınızda önceki gün harcadığınız bütün çabanın sabahın erken saatlerindeki bir fiyat dalgalanmasıyla tamamen silindiğini görebilirsiniz.

Bitcoin'e uzun vadeli yatırım yapmanızı öneririm. Bitcoin satın alın, onu güvenli bir yere koyduktan sonra bekleyin ve fiyatların önünüzdeki beş, on ya da on beş senede yükselmesini ümit edin. Bitcoin satın almak oldukça kolay; tek yapmanız gereken size onu satmaya razı olan birini bulmanız. Bu kısmın ilk birkaç bölümünde uzun vadeli elde tutma amacıyla nasıl bitcoin satın alıp saklayacağınızı açıklayacağım. Gün içi işlemlere girmeye kararlıysanız, bu kitap size temel prensipleri öğretebilir ama hiç çalışmadan ya da daha deneyimli birinden bir şeyler öğrenmeden yüz binlerce dolar kazanmayı beklemeyin. Sadece gün içi Bitcoin alım-satımı üzerine değil, geleneksel hisselerin temelleri hakkında da rehberler bulmak için internette

araştırma yapmanızı öneririm. Benzer prensiplerin çoğu Bitcoin dünyasında da geçerli ve onlar üzerinde uzmanlaşamazsanız, ileri düzeydeki tacirlerin hep bir adım gerisinde kalırsınız.

Nakit Parayla Bitcoin Satın Almak

Bitcoin satın almak neredeyse her ülkede mümkün, ama bazı ülkelerde diğerlerine kıyasla daha kolay. Nakit parayla doğrudan bitcoin satın almanın en güvenilir ve gizli yolu LocalBitcoins (localbitcoins.com) kullanmaktır. Bunun için siteye girip ödeme seçenekleri kısmında 'şahsen' altındaki 'nakit' seçeneğini tıklayın, konumunuzu belirtin ve yakınınızda nakit karşılığı bitcoin satmak isteyen biri olup olmadığına bakın. Kendi adınıza bir satın alma siparişi girip bekleyebilir ya da var olan bir satış talimatını bulup o bitcoin'leri satın alabilirsiniz. Beklerseniz, bitcoin'lerini bir an önce satmak isteyen biriyle iyi bir pazarlık edebilirsiniz. Satış emri veren birinden bitcoin satın alırsanız, piyasa fiyatının biraz üzerinde bir değer ödemeniz gerekebilir. Daha sonra satıcıyla bir buluşma ayarlamalısınız, o nedenle kendisine bırakılan yorumları okuduğunuzdan ve buluşmak için bir kafe gibi umumi bir yer seçtiğinizden emin olun.

İşlemi gerçekleştirmek için bir Bitcoin cüzdanına ihtiyacınız olacak. Mobil uygulaması olan bir ağ cüzdanı kâğıt cüzdana tercih edilir, çünkü nakit parayı satıcıya vermeden önce işlemin gerçekleştiğini kolayca kontrol etmeyi isteyeceksiniz. Daha sonra bitcoin'leri çevrimdışı bir cüzdana ya da kâğıt cüzdana transfer edebilirsiniz.

Asıl işlem çok basit ama sizin için yeni bir deneyim ola-

cağı için tekrar açıklayacağım. Öncelikle, tercihen akıllı telefonunuza yüklü bir Bitcoin cüzdanına ihtiyacınız var. Yanınıza onu ve biraz nakit alarak internet bağlantısı olan herhangi bir yerde satıcıyla buluşabilirsiniz. Her cüzdan uygulaması farklıdır, ama bu kitabın başındaki siyah-beyaz kutuya benzeyen bir kare kod oluşturmanın bir yolunu bulmalısınız. Satıcı kendi akıllı telefonunun kamerasıyla onu tarayacak ve sonra kararlaştırılan sayıda bitcoin'i size gönderecek. Sizin uygulamanızda görünmesi çok uzun sürmemeli. Eğer yüklü miktarda alım yapmıyorsanız, o noktada parayı verebilirsiniz ve işleminiz tamamlanmış olur.

Teorik olarak, blok zincirinde üç ile altı doğrulama beklemelisiniz. Madencilik bölümünde doğrulamaya daha çok değineceğim ama şimdilik, Bitcoin ağının işlemin geçerli olduğundan emin olmak için bir madenci ya da tam düğüme onu kaç kez kontrol ettirdiğini gösterdiğini bilmeniz yeterli. Birçok cüzdan uygulaması size bir işlemin güvenli sayılması için doğrulanmasına ne kadar zaman kaldığını gösterir. Bu sadece işlem oldukça büyükse gereklidir; küçük işlemler için bir doğrulama genellikle yeterlidir. Bir kişinin ağ ilk işlemi doğrulamadan aynı bitcoin'leri satmaya çalıştığı çifte harcama saldırısı bu kitapta bahsettiğim nedenlerden ötürü oldukça zordur ama imkânsız değildir; o nedenle büyük alımlar için işlem doğrulanana kadar beklemek en iyisidir.

LocalBitcoins'te birinin banka hesabına para yatırmak ya da birine hediye çeki almak da dahil olmak üzere nakit parayla bitcoin satın almanın birkaç yolu daha var. Aklınıza gelen her türlü elektronik ödeme yöntemini kullanarak

bitcoin satın alabilirsiniz: Western Union, Walmart-2-Walmart, Skrill ve çok daha fazlası. LocalBitcoins dolandırıcılığı en aza indirmek için üçüncü parti emanet sunuyor, ama satıcılar meşru olduklarını kanıtlamak için alıcılara genellikle yüksek şartlar belirliyorlar. Sonuç olarak, LocalBitcoins yerel borsalar dışındaki alıcının fazlasıyla güvenmesini gerektiriyor. Ayrıca, anlaşılan Birleşik Devletler emniyet teşkilatı siteyi takip ediyor ve arada sırada lisanssız para transferi hizmeti sunmakla suçladığı satıcıları tutukluyor. Alıcıların hiçbiri herhangi bir suçla suçlanmadı, sadece satıcılar suçlandılar; ama bu hizmeti kullanarak düzenli bir şekilde bitcoin alım-satımı yapmayı planlıyorsanız, bu da göz önünde bulundurmanız gereken bir şey.

Bitquick.co sitesi de nakit karşılığında bitcoin sunuyor ve bir emanet sistemi kullanıyor. Tek yapmanız gereken yaşadığınız bölgedeki bir bankayla çalışan bir kullanıcı seçmek ve verilen bilgilerle o bankaya gidip kişinin hesabına parayı yatırmak. Üç saat sonra, belirttiğiniz Bitcoin adresine bitcoin'leriniz teslim edilir.

Nakit parayla anonim olarak bitcoin satın almanın bir yolu daha var: Bitcoin ATM'leri. Bu yöntem büyük ölçüde yaşadığınız yere bağlı, çünkü Bitcoin ATM'leri ülkede ve dünyada yeni yeni görülmeye başladı. Bazıları anonim değil ve kullanılmadan önce bir telefon numarası ya da taranmış bir kimlik kartı gerektiriyor ama diğerleri oldukça erişilebilir. Bu makinelerin ücretleri makul ile fahiş arasında değişiyor; o nedenle uzunca yol gitmeden önce araştırmanızı yapın. Bu ATM'leri bulmanıza yardımcı olmak için bulunan bazı çevrimiçi araçlar var. Örneğin, Coinmap.org Bitcoin ATM'lerinin yanı sıra bitcoin ile ödeme

kabul eden işletmeleri bulmak için bir açık kaynak çözüm. Coinatmradar.com ücretler ve dönüştürme türleri hakkında bilgi veren bir başka iyi hizmet. Bazı Bitcoin ATM'leri sadece yasal para kabul ediyor ve bitcoin veriyorlar; diğerleri iki türlü işlem yapıyor ama genelde ücretleri oldukça yüksek.

Ancak, Bitcoin bir dijital para birimi, o nedenle onu çevrimiçi satın almak daha mantıklı. Bitcoin'i fiziksel olarak satın almanın sadece birkaç yolu olsa da, dijital olarak satın almanın sayısız yolu var. Aşağıda en güvenli ve saygın hizmetleri bulabilirsiniz. Birçoğu son derece emniyetli, güvenilir ve saygın olan başka birçok yöntem olsa da, hepsini burada listelemek imkânsız.

Verebileceğim tek tavsiye, bir şey kulağa gerçek olmayacak kadar iyi geliyorsa, muhtemelen öyledir. Diğer borsalardan çok daha iyi bir fiyat sunan herhangi bir site muhtemelen bir sahtekârlık peşindedir. Bitcoin fiyatından birkaç sent düşük fiyat sunulması makul komisyondur, ama alış-satış arasında büyük fiyat farkı olan borsalar arbitraj fırsatı arayan tacirler tarafından hemen elenirler. Eğer bir sitenin alış-satış farkı çok yüksekse, ne iddia ettiğine bakılmaksızın, tuhaf bir şey döndüğünden emin olabilirsiniz.

Kredi Kartıyla Bitcoin Satın Almak

Bir kredi kartı ya da banka kartıyla bitcoin satın almak Birleşik Devletler'de bitcoin satın almanın en hızlı ve muhtemelen en hesaplı yoludur, ama aynı zamanda Bitcoin hesabınız ve gerçek kimliğiniz arasında bariz bir bağlantı yaratır. Birleşik Devletler'deki saygın hizmetlerin çoğu

KYC (*know your customer* – müşterini tanı) ve AML (*anti-money laundering* – kara para aklamayı önleme) kanunlarına uyarlar; kimliğiniz hakkında bilgi vererek muhtemelen bu kanunlara uymaya zorlanacaksınız. Söz konusu yetki alanının Bitcoin'e özel kanunları olmasa bile, yerel hükümetin finansal hizmet kanunlarına tabi olabilir. Dahası, birçok borsa erken davranıp kendi kendini düzenleyerek beklemede olan kanunların önüne geçmeye çalışıyor.

Daha önce de bahsettiğim gibi, kredi kartı kullanarak bitcoin almanıza imkân tanıyan düzinelerce şirket var. Ancak endüstrinin üç devi Coinbase, Bistamp ve Circle'dır. Bitstamp 2015'in başında bir saldırıya maruz kaldı ve daha sonra sigorta şirketiyle olan bir duruşmada utanç verici detaylar sızdı ama hiçbir müşterinin fonları kaybolmadı. Coinbase ve Circle'ın şu anda güvenlik kayıtları tertemiz ama kredi kartı bilginizi paylaşmadan önce yeni gelişmeler hakkında her zaman Google'da araştırma yapmalısınız.

İşlem ücretleri değişken. Tacire bağlı olmak üzere, ücretler haftada ilk birkaç bin dolar için yüzde sıfırdan yüzde bire kadar değişiyor.

Birçok site kimlik doğrulaması istiyor, o nedenle kimliğinizin bir fotokopisinin yanı sıra banka ekstresi ya da ikametgâh belgesi göndermeniz gerekecek. Hatta bazı siteler iki farklı kimlik bile isteyebilirler. Doğrulama seviyesi ne kadar satın aldığınıza bağlı olarak değişir. Hareketleriniz şüpheli görülürse, sizden daha fazla doğrulama istenebilir.

Bunlara ek olarak, bu sitelerin bazıları –özellikle de Coinbase– kullanıcılarının Bitcoin hareketlerini takip ettiği (ve bazılarının iddialarına göre) onlara karşı katı bir tedbir aldığı için kötü şöhret edindi. Örneğin, eğer bir kulla-

nıcının bitcoin'lerini yasa dışı ya da kumar gibi yarı yasal eylemler için kullanıyorlarsa, o hesabı dondurabilirler. Bu nedenle, kumar oynamayı ya da LocalBitcoins'te çok fazla ticaret yapmayı düşünenler altıncı bölümde tarif edilen yöntemleri kullanarak coin'lerini karıştırmalılar. Daha da iyisi, coin'leri borsadan çekip işlemleri gerçekleştirmek için yerel bir bilgisayar cüzdanı kullanın.

PayPal ile Bitcoin Satın Almak

PayPal ile satın almanın satıcı için bazı riskleri var. Google araştırmalarınızda bazı sitelerin iddia ettiklerinin aksine, itibarlı borsaların hiçbiri direk olarak PayPal kabul etmez. LocalBitcoins'teki birkaç satıcı PayPal kabul ediyor, ama bu kolaylık için genellikle ekstra ücret talep ediyorlar ve sadece sitede itibarı olan hesaplarla işlem yapabilirler.

Bu güçlüğün sebebi, Bitcoin işlemlerinin aksine PayPal işlemlerinin geri çevrilebilir olmasıdır. Teknik olarak bu kredi kartları için de geçerli, ama henüz çok büyük bir sorun olmadı. En büyük sorun, kullanıcı hatasından ötürü (zayıf şifre, vs.) PayPal hesaplarının ele geçirilmeye müsait olmasıdır. Eğer biri ele geçirilmiş bir PayPal hesabıyla bitcoin satın alırsa, PayPal işlemi geri çevirir, ama usulüne uygun bir şekilde Bitcoin satıcısının çoktan göndermiş olduğu coin'lerini geri almasının bir yolu yoktur.

Ama bu PayPal ile bitcoin satın alamayacağınız anlamına gelmez. Sadece biraz yaratıcı olmalısınız. İnternette vakit geçiriyorsanız, Second Life adı verilen çevrimiçi oyun ve topluluğu duymuş olmalısınız. Second Life'ın Linden Doları adı verilen kendi sanal para birimi var. Linden Doları kripto para birimi olmamasının yanı sıra, gerçek bir

dijital para birimi bile değil; o sadece insanların gerçek parayla satın almaya razı oldukları oyunda kullanılan bir para birimi.[2]

Second Life'ın arkasındaki şirket Linden Labs, sanal dünyada var olan gerçek bir ekonomi yaratmak gibi dâhice bir fikir üretti. Linden Doları kullanıcıların her şeyi Linden Labs'tan satın almak yerine birbirlerinden mal, hizmet ve sanal emlak alıp satmalarına imkân tanıyor. Linden Doları tamamen merkezi olsa da ve Linden Labs dilediği zaman dijital olarak sınırsız sayıda Linden Doları 'basabilse de', yeni benimseyenlere ekonomiye girmelerinin bir yolunu sunarken, doğru miktarda enderliği korumakta övülmeye değer bir iş çıkardı. Sanal Second Life ekonomisi Linden Doları satmaya yetkili kullanıcıların olduğu bir noktaya ulaştı. Kripto paralarda olduğu gibi, Linden Doları'nın değeri de değişken, hatta bazı insanlar onlarla gün içi işlem yapıyorlar. Yetkili satıcılardan biri VirWox ve burada bitcoin'e çevirme seçeneği var. PayPal à Linden Doları à Bitcoin zincir işlemleri yaklaşık yüzde altı oranında ücret ödemenize sebep olur, ama PayPal ile bitcoin satın almanın muhtemelen en güvenli yoludur.

Hediye Çekiyle Bitcoin Satın Almak

Yukarıda bahsettiğim gibi, hediye çeki satın alıp LocalBitcoins'te onları satmak bir seçenek ama başka seçenekler de var. Cardforcoin.com oldukça yeni bir hizmet. Starbucks hediye çeki almanıza imkân vererek başladı ve en sonunda kullanıcıların Starbucks kartları da dahil olmak

[2]"Linden Dollar Definition." Investopedia. 28 Ağustos 2011. Erişim tarihi 22 Haziran 2015. http://www.investopedia.com/terms/l/linden-dollar.asp

üzere belirli dükkânlardan bitcoin'lerle hediye çeki alıp satmalarına imkân tanıdı. Her zamanki gibi, araştırmanızı yapın, özellikle de bu kitabı ilk kez yayınlandıktan yıllar sonra okuyorsanız.

Uzun lafın kısası, Bitcoin ekosisteminin en zor yanı o ekosisteme girmektir. Bir kez girdikten sonra, sunulan bütün hizmetlerden faydalanmak –kullandığınız şirketlerin güvenilir olduğundan emin olmanız dışında– neredeyse zahmetsizdir.

Ancak Bitcoin ana akım olacaksa, topluluğun insanların katılmasını kolaylaştırması gerekiyor. Circle gibi hizmetler Bitcoin'in profesyonel görünmesini sağlamak için çok faydalılar, ama yine de ilk kez bitcoin satın alacak kullanıcılar için hâlâ çok zor. Bir kez başladıktan sonra, her şey genellikle daha kolay ama o ilk zorluğu aşmak hâlâ zor, çünkü kimse kişisel belgelerini bir siteye yüklemek ya da sadece merak ettiği bir şeyi satın almak için bir kafede bir yabancıyla buluşmak istemez. Bitcoin'in ana akım olması için topluluğun ya da bir şirketin bu soruna bir çözüm bulması gerekiyor.

Purse.io

Purse.io hızla endüstrinin bir esas unsuru haline geldi. Bitcoin kullanıcılarına Amazon'dan bitcoin ile satın aldıkları ürünlerde yüzde beş ya da daha fazla indirim sunuyor. Madalyonun diğer yüzünde kredi kartlarını, Amazon hediye çeklerini ya da PayPal hesaplarını Bitcoin'e dönüştürmek isteyen insanlar var. Bir Purse.io Bitcoin kullanıcısı Amazon'dan satın almak istediği bir ürünü sipariş eder, sonra bitcoin almak isteyen ve ücreti ödemeyi sorun et-

meyen biri onun için ürünü satın alıp Bitcoin kullanıcısının adresine gönderir. Purse, ürünler Bitcoin kullanıcısına ulaşana kadar bitcoin'leri havuz hesabında tutar. Şu anda, bu hizmet Bitcoin kullanıcılarının tasarruf etmeleri ve üçüncü şahısların hızla Bitcoin'e girmeleri için en iyi yollardan biri.

On Birinci Bölüm:

Bitcoin İçin Çalışmak

Bitcoin hesap defteri yeni bir ödeme sistemidir. Dünyadaki herhangi biri başka birine hesap defterinde dilediği değer miktarına tekabül eden tasarrufunu transfer ederek Bitcoin ile ödeme yapabilir. Değeri belirleyin, onu transfer edin, alıcı da herhangi bir izne gerek duymadan ve çoğunlukla ücretsiz olarak onu alsın.

— Marc Andreessen

Bitcoin ile ödeme almak, vergi dönemi karışıklığı hariç, çok kolay bir iş. Bunu yıllardır yapıyorum. Ayrıca, bitcoin'le ya da bitcoin satarak edindiğim dolarlarla kiramı ve faturalarımı da ödedim.

Pazarlanabilir beceri sahibi olan herkes için kazançlı bir seçenek. Çevrimiçi yapılan neredeyse her şey Bitcoin ile ödenebilir ve iş piyasası yüz yüze işler açısından da hızla

[1] "Top Investor Tuesday - Bitcoin." PitchBook News. 10 Aralık 2015. Erişim tarihi 13 Ocak 2016. http://pitchbook.com/newsletter/top-investor-tuesday-bitcoin

büyüyor. 2014'te Bitcoin'e toplam 301 milyon dolar girişim sermayesi fonu yatırıldı ve bu sayı 2015'te 314 milyon dolara yükseldi[1] 2016'da bu sayı tekrar yükselirse çok az kişi şaşıracak. Bu birçok açığı doldurmak isteyen çok sayıda yeni şirket demek.

Bir Bitcoin şirketinde çalışmak düzenli bir şekilde bitcoin kazanmanın kesin bir yoludur, ama hızlı ve kolay serbest işler yapmak da aynı şekilde etkilidir.

Bitcoin ile Ödeme Yapan İş Bulmak

Bitcoin ile ödeme yapan bir iş bulmanın ilk adımı nereye bakmanız gerektiğini bilmenizdir. Coinality internette en uzun süredir hizmette olan ve muhtemelen en kapsamlı Bitcoin iş ilanı sitesidir. Şirketlerin sitelerinden, Elance ve Reddit'in alt forumu r/Jobs4Bitcoin gibi serbest çalışma sitelerinden iş bulup internetteki neredeyse her Bitcoin ile ödeme yapan iş ilanını bünyesinde topluyor.

En sık rastlanan eleman açıklığının kodlayıcılar olması hiç şaşırtıcı değil. Bitcoin kodlayıcıları, web tasarımcılar, mobil uygulama geliştiriciler: Bu beceriler endüstride çok revaçta.

Yazı yazmak iyi seçeneklerden bir diğeri. Birçok Bitcoin haber sitesi yeni öneriler kabul eder. Bu siteler CoinDesk, DeepDotWeb, Bitcoin Magazine, CryptoCoinsNews ve newBTC'yi içeriyor. Hepsi yazarlarına bitcoin ile ödeme yapıyor. Grafik tasarım sanatçıları ve metin yazarlarının da Bitcoin alanında birçok iş bulmaları olası.

Deneyimsiz ve yetersiz yazarlar için bitcoin kazanmanın bir yolu olumlu yorumlar yazarak bir şirketin piyasasını kızıştırmaktır, ama topluluk genellikle bu tür işleri onaylamaz. Yine de, eğer çaresizce bitcoin kazanmak is-

tiyorsanız, bazı insanları sinirlendirmeyi ve itibarsız şirketleri savunmayı umursamıyorsanız, deneyebileceğiniz yollardan biridir, ama sahtekâr bir şirket için çalışmanın o sahtekârlığa ortak olmak olarak görüleceğini unutmayın, o nedenle dikkatli olmanızı öneririm.

Ancak Bitcoin istihdamı sadece programcılar ve içerik yaratıcılarıyla sınırlı değil. Endüstride genel ticaret ve pazarlama için giderek artan bir talep var. uBITquity'nin operasyon direktörü ve Blockchain Factory'nin kurucu ortağı/uyum müdürü Nathan Wosnack şöyle söylüyor:

Sadece teknolojiden anlamak yeterli olmayacak; mesleğe yabancı olanların dilini de konuşabilmelisiniz. En büyük ihtiyacın pazarlama ve tanıtım elemanları olduğunu düşünüyorum. Kripto para alanında halkla nasıl konuşulması gerektiğini bilen, pazarlama kampanyaları yaratabilen ve halka ulaşabilen insanlara ihtiyaç var.

Bitcoin şirketlerinin aynı zamanda kriptonun ötesinde becerileri olan, genel teknoloji pazarlamasıyla ilgilenen kendilerini adamış iş geliştirme elemanlarına ihtiyaçları var. Teknolojiyi ve gerçek hayattaki kullanım gerekliliklerini anlayabilmeliler. Çünkü eninde sonunda; ürününüzü ya da hizmetinizi müşterilere satamazsanız, fikriniz işe yaramazdır.

Tecrübelerime göre, (Bitcoin ve blok zinciri gibi) yeni teknolojilerin gelişmesiyle ticaretin zamanla test edilmiş kurallarının geçerli olmayacağına dair insanların aptalca ve genellikle tehlikeli bir düşüncesi var. Ne yazık ki, yanılıyorlar.

Bir şirket için çalışmak seçeneklerden sadece biri. Bir diğeri de bahşişle çalışmak. Kâr etmenin en hızlı yolu bu olmayabilir, ama kaliteli işler çıkardıktan sonra insanların bağış yapmalarını beklemek kesinlikle bitcoin toplamanın bir yoludur. Sesli yayıncılardan müzisyenlere, blog yazarlarına ve sanatçılara kadar herkes dinleyicilerinden projelerini finanse etmelerini istediler. Birkaçı tam zamanlı işler kapmayı başardılar. Bu yolu seçmeyi planlayanlara diğer para birimlerinde de ödeme kabul etmelerini öneririm, ama Bitcoin bu gelirin büyük ve büyüyen bir kısmı olabilir.

Bitcoin Karşılığında Mal Satmak

Bitcoin karşılığında mal, ürün ya da hizmet satmak Bitcoin ekosistemine doğrudan girmenin bir diğer yoludur. Bir işletme sahibiyseniz ve müşterilerinizin Bitcoin ile ödemelerine imkân tanımak istiyorsanız ya da sadece evinizde duran eşyaları satmak istiyorsanız, ödeme seçeneği olarak Bitcoin'i kabul etmenin sayısız yolu vardır.

Şu anda, Bitcoin kullanabileceğiniz en büyük açık artırma sitesi CryptoThrift'tir. eBay'e benzer bir formatı var ve bütün satışlarda 30 günlük havuz hesabı sunuyor (satıcı bunu sunmak zorunda ve faydalanıp faydalanmayacağına alıcı karar verir). 2014'te, CryptoThrift güvenlik endişelerini öne sürerek birkaç aylığına havuz hesabı hizmetini iptal etti. Daha sonra bu sorunlar ortadan kalktı ve havuz hesabı bütün alıcılara şiddetle tavsiye edilir.[2] Satıcılar için bu özellik fonlarının otuz güne kadar bloke edilebilece-

[2]DeMartino, Ian M. "CryptoThrift Suffers Security Breach, 15 BTC Stolen, Escrow Service Suspended." CoinTelegraph. 7 Ekim 2014. Erişim tarihi 22 Haziran 2015. http://cointelegraph.com/news/112691/cryptothrift-suffers-security-breach-15-btc-stolen-escrow-service-suspended

ği anlamına geliyor, ama pratikte fonlar, bir anlaşmazlık çıkmadığı takdirde, alıcıların ürünlerini teslim almalarının ardından serbest bırakılır.

Glyde bir diğer eşler arası pazardır. CryptoThrift'in aksine, Amazon gibi sabit fiyatla çalışır. Burada genellikle cep telefonu, tablet ve video oyunları satıyor. Sigortalı gönderi ve paketleme sunuluyor ve satıcıların banka havalesi, posta çeki ya da Bitcoin olarak ödeme almalarına imkân tanınıyor. Ne yazık ki, ürün satın almak için doğrudan Bitcoin kullanamazsınız.

Ayrıca, r/Bitcoinmarket ve BitcoinTalk forumları gibi açık pazarlar da var. Bu seçenekler son derece riskli olabilir, çünkü dahili bir havuz hesabı yok, ama topluluğun saygın bir üyesini –küçük bir ücret karşılığında– emanet hizmeti olarak kullanmak riskin bir bölümünü ortadan kaldırabilir.

Eğer bir işletmeniz varsa, çok az bir masrafla bitcoin elde edebilir ve bütün Bitcoin ekosistemine faydalı olabilirsiniz. Bitcoin kabul etmek kolaydır ve işinizi paralarını kendi tercih ettikleri ödeme biçimiyle kabul eden hevesli kullanıcılardan oluşan kocaman bir dünyaya açabilir.

Sonuçlar değişken olabilir. Bazı şirketler Bitcoin satışlarının etkileyici olmadığını belirttiler; diğerleri rakamlardan oldukça memnundu. Netice ne olursa olsun, Bitcoin'i kabul edilen ödeme biçimlerine eklemenin neredeyse hiç masrafı yok ve suya balıklama dalmak ya da sadece ayaklarını sokmakla yetinmek istediklerine satıcılar karar verebilirler.

Bitcoin kabul eden işletmeler için iki seçenek var: Bitcoin işlemlerini ya kendileri ya da başka biri onlar için

halledebilir. PayPal'in Braintree'si artık satıcıların dijital ürünler için Bitcoin kabul etmelerine olanak tanıyor; Square satıcıların Bitcoin kabul etmelerine imkân tanıyor ve hem Bitcoin hem de Apple Pay'i kabul eden bir yazarkasa üzerinde çalışıyor; Shopify da satıcıların Bitcoin kabul etmesine imkân tanıyor. Ancak, bu siteler otomatik olarak alıcının bitcoin'lerini yasal para karşılığında satıyorlar, o nedenle kendi bitcoin'lerini kazanmak ve tutmak isteyen satıcılar için uygun bir seçenek değiller.

Bu hizmet Coinbase ve Bitstamp gibi şirketler tarafından sağlanıyor. Bu şirketler satıcıların ne kadarını Bitcoin'de tutmak, ne kadarını yasal paraya dönüştürmek istediklerine karar vermelerine olanak tanıyor. Örneğin bir satıcı, dükkânının yasal parayla her zaman masraflarını karşılayacak şekilde bir miktar belirleyip kâr marjını Bitcoin olarak tutabilir.

Alternatif olarak, bir dükkân sadece Bitcoin kabul etmeye karar verebilir. Yerel bir cüzdan kurup, bir kare kod gösterebilir ve gelen siparişleri takip etmek için bir bilgisayar ya da tabletten yararlanabilir. Bir ağ cüzdanı ve işlemleri kabul etmek için akıllı cihaz kullanmak daha basit bir çözüm olur. Her halükarda, satıcı Bitcoin'in ne kadarını, ne zaman yasal paraya dönüştürmek istediğine karar verebilir.

Şirketle Bitcoin kabul ederek, sadece teknolojiye meraklı, antisosyal küçük bir gruba hitap etmiyorlar; aynı zamanda işlerini bütün dünyaya açıyorlar. Çin'den bir müşteri, banka uyumluluğu ya da fahiş ücretler hakkında endişelenmeden Birleşik Devletler merkezli bir şirketten Bitcoin kullanarak bir ürün satın alabilir. İşlemin tersine

çevrilemez olması satıcı açısından avantajlıdır ve genellikle yüzde iki ila dört arasında değişen kredi kartı komisyonundan kaçınmış olur. Birçok şirket, özellikle de perakende şirketleri, son derece küçük kâr marjıyla çalışıyor; yüzde üç oranında bir ücret kârlarının yarısını alıp götürebilir. Ücreti genellikle $0,02'nin altında olan Bitcoin onlar için gerçekten ezber bozan bir sistemi temsil ediyor. Her kuruşun hesabını yapan şirketler için Bitcoin'in kullanılabilirliği benzersizdir.

Bitcoin Karşılığında Çalışmak İstemenin Nedenleri

İnsanların Bitcoin karşılığında çalışmayı seçmelerinin birkaç sebebi var. Bu Bitcoin elde etmenin kolay bir yoludur. Serbest çalışanlar için, bitcoin ile ödeme almak müşteri tabanlarını genişletir ve gereksiz aracıları ortadan kaldırır.

Freelancer ve Elance gibi siteler her işin ödemesinden belli bir komisyon alırlar. Bu uygulama hem müşteriyi hem de serbest çalışan kişiyi incitir, ama bu potansiyel işverenlerle bağlantı halinde olmanın ve istifade edilmekten korunmanın bedelidir. Bitcoin sadece aracıyı ortadan kaldırmıyor; anonim ya da neredeyse anonim bir şekilde iş yapmayı daha güvenli kılıyor.

Ayrıca, potansiyel hizmetinizin erişimini büyük ölçüde artırıyor. Bitcoin kabul ederseniz, dünyadaki herkes size iş verebilir. Para dönüşümü ücretleri, banka ücretleri ya da diğer ülkenin sizin ülkenizle e-ticaret yapmaya izin verip vermediği hakkında endişelenmenize gerek yok.

Bu kazançlara rağmen, Bitcoin karşılığında çalışmanın henüz ortadan kaldırılmayan bazı sorunları var.

Bitcoin Karşılığında Çalışmanın Sorunları

Bitcoin ve diğer kripto paralar için akıllı kontratlar –bir kontrata uyulduğundan emin olan bilgisayar protokolü– geliştirildi ve sürekli daha da güçleniyorlar. Havuz hesabı çok kullanışlı, çünkü işveren kontrata uymamaya karar verse bile çalışana kontratın yerine getirileceğine dair güvenebileceği üçüncü bir parti sunuyor. Bu durum her zaman ideal değil ve işveren ve çalışan arasındaki güç dengesi birçok faktöre bağlı olarak çılgınca değişim gösterebilir.

Akıllı kontratların arkasındaki asıl amaç güven ihtiyacını ortadan kaldırmaktır. Henüz oraya varmadılar. Ve havuz hesabı programlanabilir olsa da, sonuçta kontrattaki tarafların dürüst davranmalarına dayanıyor. Örneğin, iş kalitesi öznel olduğu için programın bir sitenin müşterinin belirttiği şekilde tasarlanıp tasarlanmadığına karar vermesi zordur.

Ancak, programlanabilir bazı kriterler var ve bu çok değerli. Örneğin, bir arama motoru optimizasyonu (SEO) uzmanı belirli seviyede tıklama vaat edebilir ve kontrat Alexa.com'dan istatistikleri alıp ödemeyi site ancak o sayıya ulaştığında yapabilir.

Elbette, insanlar her zaman sistemi kandırmaya çalışacaklar. Bu insan doğasının bir parçası gibi görünüyor. Yukarıdaki örnekte, arama motoru optimizasyonu uzmanı ödemeyi bıraktığı anda kesilecek ucuz, yapay trafik satın alabilir. Hem müşteri hem de SEO uzmanı trafiğin meşru ve organik olacağı anlaşmasına varmış olabilirler, ama bunu anlaşmaya kodlamanın bir yolu olmadan, müşteri rahatlıkla aldatılabilir.

Mevcut tehlikelere ve engellere rağmen, Bitcoin karşılığı çalışmanın birçok avantajı var. CoinTelegraph'ta yazarken, Rusya'da yaşayan insanlar ve Birleşik Krallık merkezli bir site için yazıyordum. Vietnam, Meksika'dan, Avrupa'nın her yerinden ve Birleşik Devletler'den yazarları vardı. CoinTelegraph'ın bütün o ülkelerdeki mali kurumlarla çalışacak kadar kaynağı yoktu. CoinTelegraph geleneksel mali kurumlara ya da PayPal'a bağlı olsaydı, faaliyete geçip geçmeyeceği bile net değildi. Ancak, global erişim ve Bitcoin'in izinsiz yapısı sonucunda CoinTelegraph bunu başarabildi.

Bitcoin çevrimiçi çalışan insanlara dünyayı açtı. İnternet bu insanlarla iletişimi mümkün kıldı, ama Bitcoin icat edilene kadar size değer temsil eden bir şey göndermiyorlardı. İnternet dünyayı küresel bir topluluk haline getirdi. Bitcoin dünyayı gerçek bir küresel ekonomi yaptı.

On İkinci Bölüm:

Madencilik

Ağın iyiliği için GPU (grafik işleme birimi) silahlanma yarışını mümkün olduğunca erteleyeceğimize dair centilmenlik anlaşması yapmalıyız. GPU sürücüleri ve uyumluluk için endişelenmeleri gerekmeyen yeni kullanıcılar gelişmelerden haberdar etmek daha kolay olur. CPU'su (merkezi işlemci birimi) olan herhangi birinin şu anda oldukça eşit ölçüde rekabet edebilmesi çok güzel.

— Satoshi Nakamoto, 12 Aralık 2010
Nakamoto hesabının 'son' mesajını yayınladığı gün

Bir zamanlar Bitcoin madenciliği yapmak hiçbir yatırım yapmadan anında zengin olmanın en kısa yolu olarak görülüyordu. İnsanlar buna benzer bir şey olduğunu keşfettikleri anda, böyle olmayı bıraktı. Günümüzde, madencilik Bitcoin elde etmenin ve yatırım yapmanın muhtemelen en etkisiz yoludur.

Daha önce de belirttiğim gibi, madencilik Bitcoin iş-

lemlerini doğrulama sürecidir. Ağdaki katılımcılar yaklaşık olarak her on dakikada bir 'blok' denen giderek zorlaşan matematiksel denklemleri çözerler. Her blokta bir grup işlem ve bir önceki bloğun sıkıştırılmış bir versiyonu bulunur. Blok zincirinde herhangi bir şey değişirse, bir sonraki bloğun hash'ini değiştirir ve bu nedenle kendisinden sonraki bütün blokları değiştirir. O nedenle, eski bir işlemi değiştirmek kolay bir iş değildir ve o noktadan itibaren bütün zinciri yeniden hesaplamayı gerektirir. Bu yüzden, katılımcılar en uzun zincirin doğru olduğundan emin olabilirler. Bitcoin bu şekilde çalışır ve bu madenciler bir bloğu her doğru şekilde çözdüklerinde işlem ücretleri ve yaratılan yeni bitcoin'lerden (21 milyon bitcoin sınırına ulaşılana kadar) oluşan bir kombinasyonla küçük bir miktar bitcoin ile ödüllendirilirler.

Matematiksel denklemlerin ne kadar karışık olduğunu ağdaki toplam hesaplama gücü –hash gücü– belirler. Madenciliğin gücü son 2016 bloğun ne kadar hızlı çözüldüğüne bağlı olarak her 2016 blokta bir düzeltilir. Bir kez bu internet parasının sihirli olduğu anlaşılınca, insanlar atlayıp sürekli gelişen donanımlarla madencilik yapmaya başladılar. Çok geçmeden bir silahlanma yarışına dönüştü ve ilk silah oyun odaklı video kartları biçiminde ortaya çıktı, sonra özellikle madencilik için tasarlanan bilgisayarlar geliştirildi ve en sonunda ASIC (uygulamaya özgül tüm devre) denen, madencilik için üretilen çipler çıktı.

Bitcoin hızla herkesin madencilik yapabileceği ve Satoshi Nakamoto'nun "bir CPU bir oya eşittir" talimatının (bilgisayarı olan herkesin blok zinciri doğrulamasında eşit söze ve bitcoin ile ödüllendirilmek için eşit şansa sahip ol-

duğu) şekillendirdiği dağınık dijital para biriminden, oldukça merkezi ve sadece maddi gücü yetenlerin rekabete girebildiği son derece rekabetçi bir ortama dönüştü.

Bitcoin'in Nakamoto'nun orijinal hayalini gerçekleştirmeyi başaramadığını söylemiyorum, sadece madenciliğin belirli yanları Bitcoin'in yaratıcısının umutlarına ulaşmadı. 2010'da bile, Nakamoto ve topluluğun geri kalanı yaklaşan silahlanma yarışının farkındaydılar. Günümüz madencilik piyasasını domine eden ASIC çiftlikleri hakkında Nakamoto'nun ne düşündüğünü bilmiyoruz, ama mevcut madencilik durumunun asıl Bitcoin tanıtım yazısında belirtilen orijinal bir CPU-bir oy umudundan çok uzakta olduğu açık.

Teknik olarak hâlâ herkes madencilik yapabilir, ama yüksek güçlü bilgisayar kullanılsa bile herhangi bir ödül getirmesi pek olası değil. Aksine, madenci çok fazla elektrik tüketir ve aşırı çalıştırdığı bilgisayarın CPU ya da GPU'suna hasar verir. Bu uyarı temkin bolluğundan kaynaklanmıyor. Ben de bir süre masaüstü bilgisayarımla CPU-madencilik yaptım ve o zamandan beri bilgisayarımın CPU'sunun aşırı ısınma sorunu var. Bu deneyimde yalnız değilim. Kullanıcılar tam düğüm çalıştırarak katkıda bulunabilirler. Bu, bütün Bitcoin blok zincirinin indirilmiş olduğu bir Bitcoin cüzdanıdır ve madenciler tarafından doğrulanan işlemleri çifte kontrol etmeye yardımcı olur. Bu kişiler silahlanma yarışına katılmadıkları için madencilik ödüllerini toplayamazlar, ama onlar için de teşvik edici bir ödülün eklenmesi konuşuluyor.

Bitcoin ağına yardımseverlikle katkıda bulunmak isteyenler için tam düğüm çalıştırmak tavsiye edilir. Ayrıca,

mahremiyete önem veren insanlar için bazı avantajları var. Kendi düğümünüzü çalıştırırsanız, üçüncü bir partiye güvenmek yerine kendi işlemlerinizi ağa sunacağınız için o düğümün kötü amaçla hareket etmediğinde emin olabilirsiniz.

Madencilikse cüzdanı dolgun olmayanlara göre bir şey değil. Dört ya da beş basamaklı bir yatırım gerektiriyor ve buna rağmen silahlanma yarışı yüzünden yatırımınızı telafi edememe ihtimaliniz var. Bunu başarsanız bile, çok az kâr edebilirsiniz ve donanım, güç ya da bağlantı sorunları gibi herhangi bir aksilik kârınızı iyice düşürebilir. Zorluk sürekli artarken, kâr etmek için gereken yatırım da artıyor. Bu uyarıları aklınızda bulundurun.

Yine de elektriği Bitcoin'e dönüştürmeye kararlıysanız, bunu yapabilirsiniz ve bunu yapmanın birkaç farklı yolu var.

Öncelikle, elektrik ucuz değilse, madenciliğe kalkışmayın. Ucuz ve hatta bedava elektrikle bile madenciliği kâra dönüştürmek yeterince zor. Bunu elektriğin yanına yaklaşılmaz bir şekilde pahalı olduğu bir yerde yapmak imkânsızdır. Madencilik rekabetten ibarettir ve masrafları daha düşük olan insanlarla rekabet etmek zordur.

Potansiyel madencilere açık olan yollar her geçen gün kısıtlanıyor. Teknik olarak üç seçenek var: solo madencilik, havuz madenciliği ve bulut madenciliği. Dokuzuncu bölümde değindiğim ve daha sonra detaylı bir şekilde ele alacağım bulut madenciliği, başka birine sizin için madencilik yapması karşılığında para ödediğinizi söylemenin aslında süslü bir yoludur. Solo madencilik bir havuza katıldıklarında edinecekleri devasa hash gücü olmadan bir

bloğu çözmek gibi neredeyse imkânsız bir işe girişmeyi tercih eden sadece kararlı mazoşistlere göredir.

Birçok madencilik havuzlarda yapılır. Havuz madenciliği bir grup madencinin hash güçlerini birleştirip ödüllerini paylaşmaya karar vermelerine denir. Bu yaklaşım güvene dayanır, ne de olsa bireysel madencilerin havuz operatörünün ödülleri eşit olarak paylaştıracağına güvenmeleri gerekir. Ancak, sahtekârlık hemen fark edilir ve havuzun itibarına telafisi mümkün olmayan bir zarar verir. Hatta havuz bir gecede buharlaşabilir ve katılımcılar daha saygın bir havuza geçebilirler.

Havuz madenciliği ve solo madencilik hem Windows hem de Linux'ta komut satırında çalışan teknik olarak zor bir yazılıma dayanır. Hoş bir kullanıcı ara yüzü ekleyen başka yazılımlar da var, ama genel fikir madencinizi bilgisayımsal gücü mümkün olduğunca az tüketen bir yazılımla çalıştırmaktır. CGMiner en popüler versiyondur. Kullanmak için biraz bilgi gerektiriyor ama çok zor bir iş değil.

İlk adım yazılımın güvenilir ve emniyetli bir versiyonunu bulmak. Madencilik yazılımları bazen virüs tarayıcılarda yanlış pozitif verir. Bu yüzden, madencilik yazılımları genellikle üçüncü partiler tarafından kötü amaçlı yazılımlarla paketlenirler. Bu nedenle, madencilik yazılımınızın resmi ve güvenilir sitelerden indirmeniz çok önemlidir.

Evde bir madenci kurmadan önce, her şeyin şartnamelerine uygun olduğundan emin olmak için seçtiğiniz havuzdan bir çevrimiçi rehber okumalısınız. Madencilik çok kolay olsa da, bilgisayardan hiç anlamayan kişilere göre olmadığını unutmayın. Toplulukta madenciliğin ge-

nel kullanıcılar için kolaylaştırılmaması yönünde bir görüş hâkim, ne de olsa, daha fazla insan daha fazla rekabet ve zorluk demek ve bu madencilerin mevcut donanımlarıyla edindikleri kârı düşürür.

Ama madencilik gerçekten hiç zor değil. Birkaç basit adımı izleyerek hemen herkes bunu yapabilir. Ancak her şeyi kolaylaştıran güzel bir kullanıcı arayüzü beklemeyin. Birçok POW coin madenciliği çok benzer yöntemlere dayalı çalışır ama havuzunuzun rehberine danıştığınızdan emin olun.

Birinci adım madencilik yazılımını indirmek: CGMiner ya da BFGMiner. Açıklamak amacıyla CGMiner'a odaklanacağım ama BFGMiner süreci de neredeyse aynı. Önce Windows yöntemini ele alacağım.

Yazılımı indirdikten sonra bir havuza katılın, bir 'işçi' yaratın ve ona havuzun web sitesinde bir isim verin. Sitenin madencilik IP adresini bulun; havuzun web sitesinde zaten görünüyor olmalı. Onu bulamazsanız, sitenin SSS sayfasına göz atın. Bir TCP adresi olmalı.

Sonra, not defterinde bir metin belgesi ya da benzer bir program açıp aşağıdakini yazın:

cgminer -o stratum+tcp://[buraya havuz URL'i girin]:[buraya bağlantı noktası numarasını girin] -u [havuz kullanıcı adı].[havuz işçi adı] -p [buraya havuz hesabı şifrenizi girin]

'Farklı Kaydet'e tıklayın ve dosya uzantısını .txt'ten 'bütün dosyalar'a dönüştürün. Ona 'StartMining.bat' adını verin ve CGMiner'ın bulunduğu klasöre kaydedin. Artık o dosyaya tıkladığınızda madenciniz otomatik olarak çalışmaya başlayacak.

İlerlemenizin ve hash oranınızın bir özetinden olu-

şan, sürekli güncellenen bir kayıt dosyası göreceksiniz. Bu ekrandan, madencilik detaylarınızı da güncelleyebilir ve hangi havuzlara madencilik yaptığınızı yönetebilirsiniz.

Bir havuza madencilik yapmak yerine tek başınıza madencilik yapmayı tercih ederseniz, bu süreç de basit (donanım gereksinimi hariç). Öncelikle, Bitcoin Core, ya da Bitcoin-Qt'yi indirmelisiniz. Bu bütün blok zincirini indirmeyi gerektiriyor ve hızlı bir süreç olmayacak. Blok zinciri hızla büyüyor ve şu anda 52GB boyutunu aşmış durumda. Bu kitap yayınlandığında, blok zinciri çok daha büyümüş olacak.[1] Süreç eşler arası, ama ağdan indirerek muhtemelen kaynak sayısı yüksek torrentlerin hızına yetişemediğinizi göreceksiniz. Bir sunucudan ilk 20GB'yi indirerek işleri hızlandırabilirsiniz, ama indirmenin bir ya da iki gün sürebileceğini unutmayın.

Blok zincirini indirdikten sonra, madenciliğe başlamak için Bitcoin yazılımında küçük bir ayar yapmanız gerekecek.

Teknik olarak sadece CPU ve bir cüzdanla madencilik yapabilirsiniz ama bu CPU'nuzu (Bitcoin gibi GPU odaklı coin'ler için) yakmanın hızlı bir yoludur. Ancak, bu süreçle ilgilenenlere (ya da CPU odaklı bir altcoin'de tek başına madencilik yapmak isteyenlere) anlatmak gerekirse, şöyle yapılır:

Not defterinde 'Bitcoin.conf' adında bir dosya açın ya da oluşturun. Onu programlar klasöründe \APPDATA\ Roaming\Bitcoin bulabilirsiniz. Aşağıdaki sekiz satırı ekleyin:

---

[1] "Blockchain Size." Chart. Blockchain.info. Erişim tarihi 22 Haziran 2015. https://block-chain.info/charts/blocks-size

server=1
listen=1
daemon=1
rpcuser=[istediğiniz herhangi bir isim]
rpcpassword=[istediğiniz herhangi bir şifre]
rpcallowip=localhost
rpcport=127.0.0.1
port=[Bitcoin ağına bağlanmak için kullanmak istediğiniz bağlantı noktası; 8332 işe yarar]

Artık cüzdanınız tamamen senkronize olduğuna ve Bitcoin.config dosyası doğru bir şekilde düzenlendiğine göre, cüzdan yazılımını açıp Yardım'a, ve sonra Debug Window ve ardından Konsol'a tıklayın.

Konsol komut satırı açıkken, *setgenerate true – 1* yazarsanız madencilik başlayacak. Doğru düzgün çalıştığını kontrol etmek için *getmininginfo* yazın ve mevcut coin zorluğu, mevcut blok ve hash oranınız görüntülenecek.

Teknolojiye meyilli olmayanlar için başka bir seçenek daha var. GUIMiner madenciliği biraz daha kullanıcı dostu yapan küçük bir yazılım. Blok zincirini yine bilgisayarınıza indirmek zorundasınız ama indirme işleminden sonra, kullanıcıların tek yapması gereken GUIMiner'ı indirip programı çalıştırmak ve programın gözler önüne serdiği basit adımları takip etmek. CGMiner rehberindeki bilgilerden yararlanarak programın madencilik için kullanmak istediğiniz GPU'yu tanıdığından emin olmak için Araçlar bölümünü kontrol edin.

Madencilikle –solo ya da havuz madenciliği– ciddi bir şekilde ilgilenmek istiyorsanız donanıma birkaç bin do-

lar yatırım yapmanız gerekecek. Buna rağmen, kolayca kâr edeceğinizin bir garantisi yok ve bedava ya da oldukça ucuz elektrik tüketmiyorsanız, paranızı farklı bir şekilde harcamanız daha iyi olur.

Ucuz elektrik kullanıyorsanız, bazı donanımlar satın almalısınız. Bir dizi anlaşmazlığın ardından hem ButterFly Labs hem de GAW Miners kapatıldığı için KnCMiner ve Spondoolies meraklı seviyesine hizmet veren kalan Bitcoin madencilik şirketlerinden ikisidir. Ancak kalan bu iki şirket hakkında da anlaşmazlıklar çıktı. Kripto parayla ilgili her konuda olduğu gibi genel bir tavsiye olarak yüklü miktarda para yatırmadan önce araştırmanızı yapmanızı öneririm.

Donanım satın almadan önce, kârlılığa ulaşma ihtimalinizi çözmek için Bitcoin madenciliği zorluk hesaplamasını kontrol etmeniz şarttır. Bunlar elektrik masrafınızı, beklenen hash gücünüzü ve beklenen zorluğu girmenizi isteyen, beklenen kârlılığı hesaplayan web siteleri ve uygulamalardır. Google'da 'Bitcoin madenciliği hesaplayıcı' diye aratmanız birkaç uygun seçenek bulmanız için yeterli olur.

İkinci el donanım satın almanızı önermiyorum. Madencilik donanımı oldukça yıpratan bir iş ve satıcının web sitesindeki resimlere bakarak aletlerin CPU ve GPU'suna ne kadar zarar gördüğünü anlamak mümkün değil. Beklenenden daha kısa yaşam süresi olan bir donanım yatırımı mahvedebilir.

Bulut Madenciliği

Bütün bu zorlukları atlamanızı sağlayan bir Bitcoin

madencilik yöntemi var. Ama o da bazı riskler içeriyor ve, her madencilik yöntemi gibi, tavsiye edilmez. Çok az kripto para savunucusu bunu madencilik olarak görüyor. Daha önce bahsettiğim bu yönteme bulut madenciliği adı veriliyor.

Bulut madenciliği, hem popülerliği hem de kötü şöhreti hızla artan bir düzen. Genellikle bu fikri satmaya çalışan şirketlerden oluşan bulut madenciliğinin savunucuları, yatırımcıların tek başlarına madencilik yapmanın sıkıntıları hakkında endişelenmeden Bitcoin madenciliği yapabilmelerine imkân tanıdığını söylerler. Elektrik masrafı, makine bakımı ve teknik sorunlar gibi şeylerle şirketler ilgilenirler.

Bulut madenciliği şöyle işliyor: madencilik şirketleri depo büyüklüğünde devasa madencilik çiftlikleri kuruyorlar, bu çiftliklerin küçük parçalarını şirketlere satıyor ya da kiralıyorlar ve teoride –kendi ücretlerini aldıktan sonra– sahip oldukları hash oranına dayanarak müşterilere ödeme yapıyorlar.

Esasen, sizin için madencilik yapması karşılığında başkasına para ödüyorsunuz. Bu noktada, kendiniz madencilik yapmıyorsunuz. Aksine, bulut madenciliği müşterileri başka birinin madencilik operasyonuna yatırım yapıyorlar ve operasyonun ödediği komisyonlardan daha fazla kâr getirmesini ve madencilik şirketinin sahibinin paranın kaymağını almamasını ummak zorundalar.

Elbette, şirketin madencilik yaptığından emin olamazsınız. Bulut madenciliği şirketlerinin gerçekten madencilik yaptıklarını kanıtlamak için blok zincirini kullanmaları ve o karı müşterilere ödemeleri mümkün, ama bazıları

bunu yapmıyor. Eğer şirket iddia ettiği hash gücüne sahip değilse, yanına bile yaklaşmayın. Kanıt olmadan, yatırım yaptığınız şeyin gerçek bir madencilik operasyonu mu, yoksa bir saadet zinciri mi olduğunu bilmenize imkân yok. Bulut madenciliği şirketleri eski yatırımcılara yeni yatırımcıların alımlarıyla ödeme yaparken yakalandılar ve buna saadet zinciri denir.[2]

Bazı insanlar bulut madenciliğinin mantıklı olmadığını iddia ediyorlar. Eğer madencilik müşterilerden toplanan ücretlerden daha kârlıysa, şirketlerin kârı müşterilere aktarmak yerine o donanımlarla neden kendilerinin madencilik yapmadıkları sorulması gereken en mantıklı sorudur. Bulut madencilik şirketleri sık sık parayı başlangıç sermayesi olarak kullandıklarını söylerler, ama çok azı bu iddiayı destekleyecek kanıt gösterebildiler. Genellikle, bulut madencilik şirketleri siparişleri almadan çok önce donanımlara sahipler. Ve eğer durum buysa, neden mevcut donanımla madencilik yapmıyorlar? Eğer şirket Bitcoin madenciliği ve uzun vadede kârlılığına inanıyorsa –satış konuşmalarında öyle söylüyorlar– ticaret açısından o kârı başka bir yere göndermek hiç mantıklı değil.

Ancak, bütün bulut madencilik şirketlerinin sahtekâr olduklarını ima etmek istemiyorum. Ben sadece iş modellerinin biraz tartışmaya açık olduğunu ve birçoğunun gerçekten sahtekâr olduklarını söylüyorum. O halde neden bunu yapıyorlar? Çok fazla seçenek yok. Solo madencilik söz konusu bile olamaz ve hatta havuz madenciliği bile tüketici sınıfı sayılamayacak donanımlar gerektiriyor.

---

[2]Madore, Paul H. "Scam Alert: Bitcoin Cloud Services." CCN Financial Bitcoin News. 11 Haziran 2015. Erişim tarihi 22 Haziran 2015. https://www.cryptocoinsnews.com/scam-alert-bitcoin-cloud-services/

Bir kez daha, yeni kullanıcıların madencilikten uzak durmalarını öneriyorum. Kâr etmek için fazla rekabetçi bir ortam ve zorluk sürekli artıyor.

Bitcoin madenciliği çok zor, hatta bazı madencilik şirketleri bir süreliğine ara verdiler. Ocak 2015'te, 2013'ten bu yana fiyatlar ilk kez $200'ın altına düştüğünde, madenciliğin zorluğu fiyatla ve çoktan zayıflayan kârlılıkla örtüşmeyince, madencilerin çoğu kayboldular. Birçok bulut madenciliği şirketi müşterilerin hesaplarına kaydedilen bakım masraflarının muhtemel ödülleri aştığını belirterek kullanıcılarının hesaplarını kapattı.[3] Fiyatlar tekrar yükselirken, madencilik kârlılığı da arttı ve o zamandan beri her şey yoluna girmiş görünüyor. Yine de, bu olay Bitcoin madenciliğinin herkesin kaldırabileceği bir şey olmadığını açıkça ortaya koydu. Sadece değişken piyasayla uğraşacak kadar kaynağı ve sağduyusu olanlar bu işe girmeli. Sonuçta, fiyatlar düşük kalsaydı, zorluk seviyesi inerdi, ama fiyat çok geçmeden toparlandı.

Madenciliğin ortalama bir kullanıcı için erişilmez olduğunu söylemeye çalışmıyorum, sadece *Bitcoin* madenciliği artık makul değil. Elektriği Bitcoin'e dönüştürmenin bir yolu zorluk seviyesi daha düşük olan alternatif bir para biriminde madencilik yapmak ve sonra o para birimini Bitcoin'e dönüştürmektir. Bu yaklaşım yine de çabuk zengin olmanın bir yolu değil, ama kârlılık potansiyeli Bitcoin madenciliğinden daha yüksek. İlk Bitcoin madencileri

[3]DeMartino, Ian M. "Interview with CEX.io's Jeffrey Smith on Why They Paused Mining and the Future of the Industry." CoinTelegraph. 14 Ocak 2015. Erişim tarihi 22 Haziran 2015. http://cointelegraph.com/news/113302/interview-with-cexios-jeffrey-smith-on-why-they-paused-mining-and-the-future-of-the-industry

Bitcoin'in hash gücündeki artıştan ziyade fiyatındaki artıştan kâr ettiler; aynı durum altcoin'ler için de geçerli.

Bitcoin gibi, birçok altcoin de iş ispatı (PoW) ile güvenceye alınmış durumda. Coin'lerin işlediği üç ana algoritma var ve bir coin için tasarlanan donanım aynı algoritmayı kullanan her coin için kullanılmak üzere değiştirilebilir. En popüler üç algoritma SHA-256, Scrypt ve X11'dir. SHA-256 Bitcoin'in algoritmasıdır ve kripto paralar için temel algoritma olarak görülebilir ama öyle olsa da, kesinlikle basit değildir. Scrypt topluluğun GPU madencilik teçhizatlarının (birden çok, güçlü grafik işleme birimleri olan madencilik donanımları) ve ASIC'lerin yolunu kesmek için ilk girişimiydi; şu anda Litecoin ve diğer bir düzine para birimi tarafından kullanılıyorlar. Bütün çabalarına rağmen, Scrypt ASIC'ler piyasaya sürülmeyi başardı. Yan ürünleri X5, X6, X12 ile birlikte X11, ASIC madencilerinin gelişimini yavaşlatmak için tasarlanan bir CPU/GPU melezidir ve en popüler coin'i Dash'tir (eskiden Darkcoin olarak bilinirdi).

Pahalı ama modası geçmiş donanımları olan birçok insan var ve çoğu hash gücünün önemine dikkat çekmeye çalışıyorlar. Altcoin madenciliği alanının giderek daha rekabetçi olmasının bir sebebi de bu. Artık Bitcoin madenciliğinde etkisiz olan SHA-256 ASIC'ler daha küçük ağı olan ve zorluk seviyesi düşük para birimlerine yönlendirilebilirler. Sorun şu ki, makine Bitcoin ağı için yeterince güçlü olmasa da, daha küçük altcoin'ler için aşırı güçlü olabilir. Bu çeşitli coin'lerin madencilik operasyonlarında genellikle geçici merkezileşmeye sebep olabilir ve oldu. Çok daha az güvenli ağlarda %51 saldırısı korkusunun ya-

yılmasına neden olsa da, henüz bu tür bir saldırı bildirilmedi.

Altcoin madenciliğinin zorluk seviyesindeki artışın bir diğer sebebi çoklu havuzların artışıydı. Bu madencilik havuzları belirli bir algoritması olan bütün coin'lere odaklanırlar (SHA-256, Scrypt, vs.) ve sonra en iyi fiyat ve zorluk kombinasyonuna sahip olan coin için madencilik yaparlar. Bir başka coin daha kârlı olduğunda havuz otomatik olarak ona geçiş yapar. Genel olarak, bu havuzlar daha sonra o coin'leri Bitcoin ya da kullanıcının tercih ettiği başka bir dijital para karşılığında satarlar.

Bu tür eylemler, bazen blok zincirindeki madencilik gücünde geçici ve devasa artış yüzünden zorluk seviyeleri alt üst olduğundan, geliştiriciler ve bu küçük coin'lerin toplulukları tarafından her zaman hoş karşılanmazlar. Küçük coin'lerin üzerine binen yükü hafifletmek için yazılımlar geliştirildikçe bu tür şikâyetler büyük ölçüde azaldı. Bu sırada, coin geliştiricileri insanları coin'lerinde madencilik yapmaktan vazgeçirmeye çalışmanın onları durdurmakta etkisiz olmasının yanı sıra kripto para topluluğunun politik ideolojilerine karşı olduğunu keşfettiler.

Madencilik yapılacak bir coin seçerken, göz önünde bulundurulması gereken birkaç şey var. Birincisi, coin'de ön çıkarım yapılmış mı, eğer öyleyse, bu makul bir ön çıkarım mı? Ön çıkarım tam olarak kulağa geldiği gibidir. Bir coin piyasaya sürülmeden önce, geliştirici o coin'den bol miktarda üretir ve onu kendi kişisel kontrolü altına alır. Geliştiricilerin ödemelerinde ya da topluluğu genişletmekte kullanmak gibi bu fon için birkaç kullanım alanı var.

Eğer o fon gerçekten coin gelişimini finanse etmekte kullanılacaksa ve makul bir miktarsa, başlangıç bloğundan –bir coin'in blok zincirindeki ilk blok– önce kenara biraz coin ayırmakta yanlış bir şey yok. Ön çıkarım miktarı yüzde birkaç noktadan daha fazlaysa, o halde geliştiricinin 'şişir ve boşalt' planı uygulama ihtimali yüksektir. Tipik bir şüpheli ön çıkarım coin'in toplam dağılımının yüksek bir yüzdesini içerir ve böylece düşük fiyatta bile yaratıcıya önemli ölçüde kâr getirmeyi garantiler.

Ön çıkarım 'hilesi' artık o kadar sık kullanılmıyor, çünkü topluluğun büyük bir kısmı bunun farkına vardı. Blok zinciri yalan söylemez, coin'in büyük sahiplerini ve ellerinde ne kadar bulunduğunu açığa çıkarır. Bazı geliştiriciler ön çıkarımı başlangıç bloğunda gizlemeye ve sonra *o blokta* madencilik yapmayı garantilemeye çalıştılar, ama bu eski bir taktiktir ve günümüzde BitcoinTalk forumu üyeleri tarafından hemen fark edilir.

Bir coin'de ön çıkarım yapılmadığından ya da ön çıkarımın şeffaf ve makul olduğundan emin olduktan sonra bakılacak bir sonraki şey coin'in bir borsaya sokmanın ne kadar olası olduğuna bakmaktır. Saf proof-of-stake coin'lerde para birimini harekete geçirmek için ön çıkarım yapılması gerekir. Birçok altcoin'ler büyük bir borsaya girip insanların ilgisini çektiklerinde değerlerinde ani bir sıçrayış olur. Genellikle, ilk madenciler bu noktada coin'lerini satarlar ve bir altcoin'in çıktığı o ilk zirveye tekrar ulaşması çok nadirdir. Bu nedenle, madencilik yapmak için bir coin ararken, borsa desteği olmayan bir coin'de madencilik yapmak ve büyük bir piyasaya girdikten sonra onu Bitcoin karşılığında satmak iyi bir taktiktir.

Aktif bir geliştirme ekibi ve borsa sahiplerine Tweet göndererek coin'i tanıtmaktan ve coin'i sitelerine koymalarını istemekten çekinmeyen sadık bir topluluğu olan coin'lerin borsalar tarafından kabul görmeleri daha olasıdır. Borsa sahiplerini taciz etmeyi önermesem de, sosyal medyayı takip etmek eklenecek bir sonraki coin'leri öngörmek için iyi bir yoldur.

Eğer büyük borsalara girecek kadar başarılı olan bir coin'in ilk madencilerindenseniz, onu Bitcoin karşılığında satmanın ardından kâr etmeniz mümkündür.

Bitcoin henüz başlangıç dönemindeyken, madencilik yaparak işlemleri doğrulamak Bitcoin elde etmenin en kolay ve ucuz yoluydu. Günümüzde, bu muhtemelen en zor ve pahalı yöntem. Bitcoin ya da altcoin, hangi madenciliği yaparsanız yapın, madencilik vakit, elektrik ve teknik bilgi gerektirir. Coin satın almak elektrikle bitcoin yaratmaya çalışmaktan daha etkilidir. Bedava elektrik tüketmiyorsanız, dolgun bir banka hesabınız yoksa ya da bir bulut madenciliği şirketine güvenmiyorsanız, madencilik muhtemelen size göre değil.

Satoshi Nakamoto bunu amaçlamamış olmayabilir, ama elimizde olan bu.

On Üçüncü Bölüm:

HODL!

biraz viski içtim
aslına bakarsanız şişede vski yazıyordu
her neyse
öyleyse *beni mahkemeye verin*
(ama sadece BTC'yle ödenebiliyorsa)

— BitcoinTalk üyesi ve farkında olmadan Bitcoin'in 'HODL' sloganını yaratan, GameKyuubi, Aralık 2013

Bitcoin'e giren birçok kişi yatırım amacıyla giriyor. Bitcoin'i ilk benimseyen ve çok fazla kâr edenler hakkında yazılan hikâyeleri okuyan potansiyel yatırımcılar sürüler halinde para birimine hücum ettiler. Hepsi tek bir şeyi bilmek istiyordu: "Bitcoin'le nasıl köşeyi dönerim?"

Ciddi finansal tavsiyeler için dikkate alınması gereken biri değilim. Ancak, Bitcoin'le çok fazla deneyimim oldu ve potansiyel Bitcoin yatırımcılarına verebileceğim sağlam bir tavsiye var: Fiyat düşerken coin'lerinizi elinizde tutun,

fiyat yükselirken de coin'lerinizi elinizde tutun. Coin'lerinizi tutun ve bekleyin.

Bitcoin'in fiyatının yükseleceğini garanti edemem ama yükselirse, Bitcoin'in fiyatı ve günlük durağanlığa dair endişelerin hepsi konu dışı olur. Sadece 21 milyon bitcoin olacak. Uluslararası ticaretin kayda değer bir bölümü Bitcoin kullanmaya başlarsa, para biriminin fiyatı astronomik olur. Potansiyel borsa işlemlerini, gayrimenkul tapularını ve Bitcoin'in diğer muhtemel kullanım alanlarını da eklersek, Bitcoin'in finansın geleceğinde bir yeri olduğuna inanıyorsanız, şimdiki fiyatının oldukça düşük olduğu anlaşılır.[1]

Bu yüzden Bitcoin'e yatırım yapmaya özenen herkese satın alıp beklemelerini öneririm. Yaygın bir şekilde 'HODL' ('HOLD' – tutmak sözcüğünün eğlenceli bir yanlış telaffuzu) adı verilen Bitcoin'lerinizi elinizde tutma taktiği Bitcoin'e sadık olanların başlıca prensibidir. Bitcoin topluluğundaki bu neredeyse dini inançtan nefret etsem de, doğruluk payı olduğu için bu ilkeyi seve seve kabul ediyorum.

Bitcoin'in fiyatında en az üç kez büyük bir sıçrayıp oldu ve hepsi aynı modeli izlediler. Öncelikler, coin fiyatı biraz düşer; sonra hızla öngörülemez seviyelere fırlar. Ardından, kayda değer miktarda düşüş görülür –değerinin yarısı ya da daha azına iner– ama daima bir önceki sıçrayışın zirvesinin üzerinde kalır. Sonra, tekrar, bir önceki sıçrayışın yanında küçük kaldığı seviyelere çıkar.

Bu düzen 2009'dan Bitcoin fiyatının 'kurallarından'

[1]Hong, Euny. "Could One Bitcoin Come To Be Worth $1 Million? Q&A." Investopedia. 14 May 2014. Erişim tarihi 22 Haziran 2015. http://www.investopedia.com/articles/investing/051414/could-one-bitcoin-come-be-worth-1-billion-qa.asp

birinin nihayet çiğnendiği 2014'e kadar kendini tekrarladı. 2015'in başında, Bitcoin'in fiyatı $200'ın altına düştü; 2013'ün sonu, 2014'ün başındaki yükselişinden önceki değerinden bile düşüktü.[2]

Ancak bu istisna ani çıkış modelinin sona erdiği anlamına gelmez. Bu kitabı okuduğunuz sırada, aynı şey tekrarlamış olabilir. Belki de olmaz. Ocak 2015'teki düşüşün kanıtladığı tek şey bu yeni piyasada hiçbir şeyin öngörülemez olduğu ve fiyatı tahmin etmek için kullanılan herhangi bir yöntemin işe yarar olur olmaz çiğneneceğidir.

Deneyimli insanlar onlarca yıldır borsada bir model arasalar da başarısız oldular ve borsa (sözde) akıllı yatırımcılarla doludur. Ayrıca, günün belirli saatlerinde açıktır ve genellikle çalıştığı ülkeyi kapsar. Bitcoin alım-satımı yedi gün yirmi dört saat devam eder, dünyanın her yanında milyonlarca öngörülemez amatör yatırımcısı var ve nispeten daha kontrolsüzdür. Bu kadar karışık bir şeyin fiyatını öngörmek Nostradamus benzeri bir yetenek gerektirir.

Bununla birlikte, Bitcoin internet ekonomisinde giderek büyüyen bir rol oynadıkça –eninde sonunda ve uzun vadede– fiyatı artacaktır. Bu 'eğer' oldukça büyük: Blok zinciri teknolojisi giderek daha çok kullanılacak olsa da, Bitcoin'in tercih edilen para birimi olacağını garantilemek mümkün değil.

Beşinci bölümde değindiğim gibi, Bitcoin'e değerini belirleyen çok şey var. Talep ve nadirliğinin ardından, en önemli faktörlerden biri bitcoin yaratmanın zorluğudur.

---

[2]Samman, George."Bitcoin Price Drops Below $200: Have We Reached the Bottom?" CoinTelegraph. January 14, 2015. Erişim tarihi 22 Haziran 2015. http://cointelegraph.com/ news/113299/bitcoin-price-drops-200-how-we-reached-the-bottom

Bitcoin'in Ekim 2009'da ilk takas oranı belirlendiğinde, bir bitcoin yaratılırken madencilik operasyonunun harcadığı elektrik baz alınarak hesaplandı.

Bitcoin'in fiyatını belirleyen başka faktörler olsa da, yaratılış masrafı Bitcoin'in gerçek değeri için bir zemin oluşturuyor. Bir bitcoin yaratmanın bedeli iki dolarsa (çok daha fazlaya mal oluyor, ama rakamları basit tutup iki dolar olduğunu varsayalım), o halde bitcoin satan birinin karşılığında en az iki dolar isteyeceğini düşünebiliriz.

Bu değerinin hiçbir zaman iki doların altına düşmeyeceği anlamına gelmez, çünkü spekülatif işlemler ve artan tacir kabulü –tacir varlıklarında buna eş değer artış olmadan– fiyatın geçici bir süreliğine madencilerin Bitcoin'lerini satmak istedikleri fiyatın altına düşmesine neden olabilir. Bitcoin yeterince dağınık bir para birimi ve takas oranı üzerinde etkili olan tek grup madenciler değil.

Ama oran en nihayetinde onlardan geliyor. Eğer bir bitcoin'i üretmek bugün iki dolara ve yarın on dolara mal olur ama benimsenme, kullanılabilirlik ve talep aynı kalırsa, o zaman fiyatın yükselmesi kesindir. Bu uzun vadeli Bitcoin yatırımcıları için iyi haber, çünkü Bitcoin'i yaratmak sürekli zorlaşıyor ve yaklaşık her altı senede bir yeni bitcoin sayısı eskiye nazaran iki kat nadirleşecek.

Bir bloğu çözen madenciler Bitcoin ile ödüllendirilirler. Her bloğun değeri 50BTC'ydi ama birkaç sene önce 25BTC'ye düştü. Blok çözme ödülünün yarıya ineceği bir sonraki 'blok yarılama'nın 2016'da, muhtemelen Haziran ayında olması bekleniyor ve ödül blok başına 12.5 bitcoin'e düşecek. Bu nedenle, blok çözme zorluğunun artışına ek olarak, bitcoin üretmek de giderek zorlaşıyor.

'Blok yarılama' Bitcoin'in fiyatındaki sıçrayışla doğrudan örtüşmeyecek. Spekülatif tacirler Bitcoin için ödemeye razı oldukları fiyata karar verirken 'blok yarılama' gibi kazanma şansı yüksek durumları hesaba katmaya çalışıyorlar. Ancak, daha önce de bahsettiğim gibi, Bitcoin'in fiyatı üzerinde etkisi olan tek grup spekülatif tacirler değiller. Bitcoin'in fiyatına kıyasla bitcoin yaratmanın maliyetinden başka hiçbir şeyi düşünmeyen madencilerle sürekli anlaşmazlık halindeler. Fiyat öngörülerinden ziyade, mevcut gerçeklikle mücadele ediyorlar. Eğer bir bitcoin'i üretmek on dolara mal oluyorsa, en azından bazı madenciler satıp zarar etmektense fiyatın yükselmesini beklerler. Spekülatif tacirler Bitcoin'in fiyatında ayı ya da boğa –finansal piyasalarda düşüş ya da yükseliş trendini ya da tahminleri belirtmek için kullanılan terimler– olabilir ve bu öngörüyle alım-satım yapabilirler. Öte yandan, madenciler sadece elektrik faturalarını düşünmek zorundalar.

Spekülatif tacirleri kötülemeye çalışmıyorum. Onların işi dünyanın gelecekte –ister yirmi dakika, ister yirmi sene sonra olsun– nasıl olacağını öngörmek ve bu öngörülere göre karar vermektir. Madencilerin böyle bir lüksü yok ve gelecekte olabileceklere değil, şu anda olanlara dayanarak soğukkanlı ve yerinde öngörülerde bulunuyorlar.

Spekülatif tacirler blok ödülü yarılanmasından sorumlu olabilirler, birçok açıdan da öyleler. Herkes bunun yaklaştığının farkında ve beklentilerine bunu da dahil ediyor. Ama öngörülen gelecek, 'ânı düşünen' madencilerle buluştuğunda işler değişecek. Bu gelişmenin Bitcoin'in fiyatında tam olarak ne zaman artışa sebep olacağı belli değil. Artış bitcoin blok ödülü yarılanmasından kısa süre önce

veya aylar sonra olabilir. Hatta, öncesinde öngörülemez bir sorunun Bitcoin'in fiyatını düşürmesi ya da şişirmesi nedeniyle hiç gelmeyebilir. Kesin olan bir şey var ki, Bitcoin'i üretmek daha zor olacak ve bu madencilerin bitcoin'lerini en azından masraflarını çıkaracak kadar değerli olana kadar ellerinde tutmalarına sebep olacak.

Söz konusu Bitcoin'e yatırım yapmak olduğunda, sayısız strateji mevcut. Herkesin kendi sistemi var ve Bitcoin'in fiyatındaki oynaklığa kapılarak kazanılabilecek çok şey var. Sonuçta, en güvenilir tavsiye şu: Bir miktar Bitcoin satın alın, onu güvenli bir (kâğıt cüzdan gibi) yere koyun ve sonra onu unutun. Beş sene sonra geri dönün ve tekrar değerlendirin.

2014'ün Bitcoin'in en kötü yılı olduğu iddiasına yanıt veren Bitcoin savunucusu Andreas Antonopoulos bir keresinde yatırım heveslilerine Bitcoin'e zaman tanımalarını söyledi. Bitcoin şirketlerine beş yüz milyon dolarlık risk sermayesi yatırımı olduğuna dikkat çektikten sonra şöyle söyledi:

> Bize iki sene verin. Sorunla ilgilenmesi için 500 şirket ve 10.000 geliştiriciyi seferber ettiğinizde ne olur? İki yıl sabredin ve bitcoin konusunda nasıl inanılmaz gelişmeler olacağını görün.[3]

Antonopoulos'un ortaya attığı iki yıllık zaman dilimine katılmıyorum, ama sözlerinin arkasındaki genel düşünceye katılıyorum. İki sene gerçekçi olmayabilir; kripto para

[3]Bundrick, Hal M. "Andreas Antonopoulos: 'Give Bitcoin Two Years.'" Inside Bitcoins. 8 Şubat 2015. Erişim tarihi 22 Haziran 2015. http://insidebitcoins.com/news/andreas-antonopoulos-give-bitcoin-two-years/29708

ekosisteminde bu süre sonsuzluk gibi görünse de, halk – özellikle de finansal piyasalar– aynı hızda hareket etmiyor.

Ama Bitcoin'in büyüdüğü inkâr edilemez. Aynı zamanda, iki sene içinde daha fazla büyümesi olası ve daha fazla geleneksel finans şirketi katılacak ve daha fazla belirsiz kullanıcı çitin Bitcoin tarafına düşecek. Bütün bunlar olurken, başka bir sebepleri yoksa bile sırf kendi blok zinciri hizmetlerini yükseltmek için, Bitcoin elde etmenin bir yolunu arayan çok fazla şirket olacak.

Ancak, genel olarak Antonopoulos'un yarı öngörüsüne karşı değilim. 2016'daki blok yarılanması, benimsenme ve yatırımdaki sürekli artış muhtemelen haklı olduğuna işaret ediyor. Ama 2017'nin bir tür süre sonunu (bazıları Antonopoulos'un yorumundan bunu çıkarabilirler) simgelediğini iddia ederken dikkatli olmak gerekir. Bitcoin hiçbir şey değilse bile öngörülemez oldu.

Bitcoin dünyasında değişmeyen tek bir şey oldu: Bitcoin üretimi istikrarlı bir şekilde zorlaşıyor. Para birimi kullanılmaya ve benimsenmeye devam ettiği sürece, fiyat onu izlemek zorunda.

Kısacası, biraz Bitcoin alın, biraz viski için (ya da duruma göre vski) ve HODL (elinizde tutun).

On Dördüncü Bölüm:

Gün İçi İşlemler

Bizimle takılmak istemediğinden emin misin? Japon piyasaları birkaç saat sonra uyanacak, o zaman hareketlilik olur.

— İsmini unuttuğum bir günlük işlemci,
bir Bitcoin kongresi sonrasındaki partide
saat sabah birden sonra söyledi

Bitcoin ile gün içi işlem yapmak iradesiz ya da gönülsüzlere göre değildir. Bunu hiç tavsiye etmem. Ben de pek yapmıyorum. Sistemi alt edebilen her insana karşılık alt edemeyen birçok insan var. Altına hücum zamanında, satabileceğiniz en iyi şey kürektir. Son derece değişken bir emtia varken, bazı gün içi işlemciler zengin olur ve bazıları gömleklerini bile kaybeder ve piyasa her halükarda komisyonlarla yolunu bulur.

Ayrıca, gün içi işlemleri Bitcoin topluluğunun geri kalanının felsefesi ve motivasyonuna neredeyse zıt yapan bir

şey var. Günlük işlemciler piyasadaki oynaklığa bayılırlar. Topluluğun diğer üyelerinin hiçbiri oynaklığı sevmez. Madenciler, satıcılar, ödeme işlemcileri, uzun vadeli yatırımcılar, ödemelerini Bitcoin ile alanlar: Bu grupların her biri oynaklık değil, durağanlık ister.

Aynı zamanda, topluluğun günlük işlemlere ihtiyacı vardır. Bu para biriminin meşru kullanımı ve hacminin büyük bir bölümünü oluşturur. Ayrıca, fiyatın kısa sürede bu kadar yükselmesinin bir sebebidir. O sıçrayışlar, hem yasal para olarak hem de Bitcoin'i daha değerli kılarak Bitcoin ekosistemine çok fazla gerçek kıymet getirdi. İlk benimseyenlerin çoğu yatırımlarının yüzde 9,000 ya da daha fazla değer kazandığını görünce, kazandıkları paranın en azından bir kısmını Bitcoin'le ilgili işlere yatırdılar.

Herhangi bir emtianın yüksek hacimli alım-satımında, bir süre sonra bir tür 'meta' olur. Görünürde, herkes Bitcoin'in ulaşacağını düşündükleri değer için bahse giriyorlar ama asıl bahse girdikleri bu değil. Asıl bahse girdikleri şey halkın, başlıca diğer günlük işlemcilerin, fiyatın bir saat, yarım saat ya da on dakika sonra geleceğini sandıkları noktadır.

Bitcoin'in teorik değerine dayanarak değil, ortalama günlük işlemcinin teorik acemiliğine dayanarak halkın düşüneceği bir sonraki şeyi tahmin etmek için belirli stratejiler izlenebilir.

Bu bölümü okuduktan sonra sadece bu kitapla silahlanarak bütün birikimleriniz ve hayallerinizle Bitcoin'in neredeyse kontrolsüz günlük işlem dünyasına dalmanızı tavsiye etmiyorum. Ben bunu yapmadım. Dürüst olmak gerekirse, tecrübeli bir günlük işlemci değilim ve öyleymiş

gibi davranmayacağım. Bu bölümde bazı temel ipuçlarını ve teorileri açıklamanın yanı sıra, daha fazla bilgi edinebileceğiniz kaynakları sunacağım. Bu kapsamlı bir rehber anlamına gelmez. Bunu "yasal olarak kendimi korumak, ama aslında, hazırsanız, harekete geçin," anlamında bir feragat olarak söylemiyorum. Günlük işlem dünyasında, en iyi ihtimalle yürümeyi yeni öğrenen bir çocuğum. O nedenle, sunduğum bilgileri okuyun, ama kaybetmeyi göze aldığınız bir yatırımda bulunmadan önce gidip bir bilenden öğrenin.

Gerçek hayvanlarla rekabet edeceksiniz. Birçoğu, en başarılı olanları, borsanın emektarlarıdır. Onlar bile yedi gün yirmi dört saat açık küresel bir piyasanın eskiden borsa kurlarıyla yaşayan bağımlıların üzerindeki etkileri konusunda endişeliler. Bu bölümün başındaki sözler doğrudan bana söylendi. Tacirin adını unutmuş olsam da, bu sözleri söylerkenki hevesini asla unutamam. Çok ciddiydi. Ayrıca, beni zorlamıyordu; son on yedi saattir kongreyi takip etmiş olmama rağmen, Japonlar uyanmaya başlarken saat sabahın üçüne kadar Bitcoin piyasasında çalışmakla gerçekten ilgilenebileceğimi düşünüyordu.

Bitcoin günlük işlemlerine girerken, bu tür adamlarla rekabet edeceğinizi bilmeniz gerekir. Onun gibi adamları yenmek zorunda değilsiniz ama kâr etmek konusunda ciddiyseniz, kendinizi en az onun kadar adamanız gerekir. Öte yandan, neredeyse diğer bütün emtialara kıyasla –hisse senetleri, değerli madenler, para birimleri– Bitcoin oldukça değişken, o nedenle, olumlu havadan yeterince faydalanabilirseniz, çok para kazanabilirsiniz.

Elbette, günlük işlemlerle ilgileniyorsanız, ister uzun

vadeli, ister kısa vadeli yatırım yapın, şimdiye kadar yatırımın her zaman altın kuralı olan, 'düşük fiyattan al, yüksek fiyattan sat,' ilkesini duymuş olmalısınız. Bu stratejiyi herkes bilir ama günlük işlemlerin işe yaramasının tek sebebi birçok kişinin buna bağlı kalmamasıdır.

Bu kurala uymak isterler, hatta muhtemelen uyduklarını düşünüyorlar ama uymuyorlar. Asıl sorun fırsatı kaçırma korkusudur. Ortalama bir günlük işlemci fiyatta hızlı bir yükseliş görünce, "Ah, beklediğimiz sıçrama bu, bunu kaçıramam!" diye düşünür. Ama, elbette, günlük işlemci fırsatı çoğunluklu kaçırmıştır, olmadı zirveden ya da zirveye yakın bir yerden satın alıyordur. Daha sonra, fiyat düştüğünde, tekrar yükselmesini beklemek yerine, ortalama bir günlük işlemci aşırı tepki verip bunun bir sonraki büyük düşüş olduğunu düşünüp satış yapar. Elbette, bütün profesyonel tacirler ve balinalar –yüklü miktarda Bitcoin sahiplerine verilen isim– fiyat düşükken satın almış ve yükseldiğinde satmışlardır.

İşin en önemli kısmı sakin olmak, belirli göstergeleri kullanarak coin'in mevcut fiyatına kıyasla piyasanın gerçekliği hakkında bir fikir edinmek. Öncelikle, nereden bilgi edineceğinizi bilmelisiniz. Ciddi bir şekilde Bitcoin alım-satımı yapmayı planlıyorsanız, en popüler kaynak ve kesinlikle okumanız gereken şey BitcoinWisdom.com'dur. Web sitesi Bitcoin ve bütün büyük borsalardaki diğer büyük altcoin'ler hakkında bilgi veriyor. Sipariş defterinin yanı sıra, alım-satım fırsatlarını tanımak için işe yarar temel araçlar sunuyor.

Aynı anda birden çok sitede alım-satım yapmanıza imkân tanıyan ve profesyonel borsacıların kullandıklarına

benzeyen araçlar sunan Coinigy gibi başka siteler de var. Şu anda ücretsiz deneme imkânı veriyor, sonrasında oldukça yüksek bir ücret alıyor. Günlük işlemlerinize ayırmak istediğiniz hacme bağlı olarak, onu bu ücrete değer bulabilir ya da bulmayabilirsiniz.

Günlük hisse senedi ya da döviz alım-satımında geçerli olan ilkeler burada da geçerli: olası alım-satım noktalarını belirlemek için piyasa göstergelerinden yararlanın ve sonra onları sermayeye dönüştürün. Günlük işlemler biraz sörf yapmaya benzer: Düşer, hatalar yapar ve çoğunlukla yanılırsınız. Sörfte olduğu gibi, birçok kez tahtanızdan düşeceksiniz; bu sporun bir parçasıdır. Daha sık başarılı olana kadar vazgeçmemek ve piyasayı tanıyana kadar küçük miktarlarda alım-satım yapmak işin püf noktasıdır. Bitcoin bu konuda çok yardımcı, çünkü önemsiz miktarlarla – beş dolar ya da daha az– 'alıştırma' yapabilirsiniz ve sonra hazır olduğunuzda daha büyük miktarlara geçebilirsiniz.

Bakmanız gereken asıl şey göstergelerinizin fiyatın olması gerektiğini söylediği yer ve piyasadaki fiyatın olduğu yer arasındaki değişkenliktir. Genel olarak, piyasa daha önce bulunduğu noktaya geri dönmeye meyillidir. Genel düşme ya da yükselme trendleri görülür, ama bunların hepsi fiyat dibi ya da zirveyi test ederken 'asansör' sıçrayışı yerine 'basamak' sıçrayışında olur.

Bilmeniz gereken ilk kavram çift diptir. Bir ayı piyasası (düşüş) boğa piyasasına (yükseliş) geçiş yapmak üzereyken, çift diple test yapar. Bu şu demek oluyor; fiyat yeni bir dibe ulaşır ulaşmaz küçük ama hızlı bir yükseliş olur ve onu genellikle eşit ya da bir öncekinden daha düşük başka bir düşüş izler.

Bu bazı insanların yeni düşük fiyattan aldıklarının ve yakında bir tepki geleceğinin göstergedir. Alım-satım yaparken göz önünde bulundurulması gereken tek modelin bu olmadığını aklınızda bulundurun, çünkü çift dipler bazen büyük bir düşüşe giderken geçici mola noktaları olabilirler.

Her tacirin bilmesi gereken başka esas göstergeler de var. Onlar hareketli ortalama (MA), hareketli ortalama göstergesi (MACD), relatif güç indeksi (RSI) ve denge işlem hacmidir (OBV). Ayrıca, göstergeden ziyade faydalı görseller olan Fibonacci düzeltme seviyelerine de değineceğim.

Coinigy ve Brian Beamish –The Rational Investor olarak bilinir– kendi araçlarını kullanarak Bitcoin günlük işlemleriyle ilgili bir dizi harika videolar oluşturdular. O videoları izlemenizi şiddetle öneririm. Onları Coinigy'nin YouTube kanalında bulabilirsiniz.

Beamish'in sistemi şöyle işliyor: göstergeler bir 'M' çizdiğinde, bu boğa piyasasına işaret eder. Buna karşılık, 'W' gösterdiklerinde, ayı piyasasına işarettir. Beamish bunu bir alım-satım fırsatı olarak görmeden önce en az üç bağımsız göstergeyi tanımanızı tavsiye ediyor.

Hareketli Ortalama (MA)

Hareketli ortalama belirlenen bir süre için ortalama fiyattır. Fiyat dalgalanmalarını düzleştirerek paraziti azaltır. Hareketli ortalamanın en sık görülen iki türü basit hareketli ortalama (SMA) ve üssel hareketli ortalamadır (EMA). Basit hareketli ortalama tekabül ettiği zaman dilimlerinin ortalamasıdır; üssel hareketli ortalama daha ziyade son göstergelere ağırlık verir.

Hareketli Ortalama Göstergesi (MACD)

MACD yeni EMA fiyatlarını geçmiş EMA fiyatlarıyla karşılaştırarak fiyat dalgalanmalarının göreceli gücünü ölçer. Tipik bir MACD planı 12 günlük EMA ortalamasını alıp ondan 26 günlük EMA'yı çıkarmayı içerir.[1]

Relatif Güç İndeksi (RSI)

Relatif güç indeksi, ortalama fiyata göre aşırı satın alma ve aşırı satma koşullarına değer biçmek için son kayıpları ve kazanımları karşılaştırır.[2]

Denge İşlem Hacmi

Denge işlem hacmi bir piyasanın mevcut hacmini eski hacmine kıyaslayarak takip eder. Teoride, artan hacme eşlik eden bir fiyat artışı yoksa –yine teoride– kısa süre içinde bir fiyat artışının olacağını haber verir.[3]

Fibonacci Düzeltme Seviyeleri

Fibonacci düzeltme seviyeleri bir gösterge olmasa da, yine de faydalı bir araçtır. Oranlar kullanarak olası toparlanma seviyeleri ve tavan fiyatları resmeden bu grafikler bir coin yatırımına girmeye ya da yatırımdan çıkmaya karar verirken faydalı bir rehber olabilirler. Genellikle kullanılan oranlar yüzde 23,6, yüzde 38,2, yüzde 50, yüzde 61,8

---

[1] "Moving Average (MA) Definition" Investopedia. 24 Kasım 2003. Erişim tarihi 22 Haziran 2015. http://www.investopedia.com/terms/m/movingaverage.asp

[2] Bitcoin RSI Tutorial. Yönetmen Brian Beamish. Anlatıcı Brian Beamish. Youtube.com/coinigy.April 25, 2015. https://www.youtube.com/watch?v=Vq2EC7OinQQ

[3] "On-Balance Volume (OBV) Definition" Investopedia. 24 Kasım 2003. Erişim tarihi 22 Haziran 2015. http://www.investopedia.com/terms/o/onbalancevolume.asp

ve yüzde 100'dür. Coin'in en yüksek fiyatından en düşük fiyatına doğru Fibonacci düzeltme seviyelerini takip edin (değerlendirmek istediğiniz zaman dilimi için) ve yüzde 23,6 ya da yüzde 38,2 dışında kalan hiçbir kutudan satın almayın. Her zaman yüzde 61,8 ve yüzde 100 kutularındaki fiyatlardan satış yapın. Hamleleri tahmin eden bir şeyden ziyade, temel 'yüksekten sat, düşükten al' ilkesine sadık kalmanıza yardımcı olan işe yarar bir araçtır ve önünüzde açık olduğunu görmek kullanışlı olabilir.[4]

Bu konuda uzman olmadığımı bir kez daha vurguluyorum. Kendi araştırmanızı yapın ve bir ders almayı göz önünde bulundurun. En azından, ücretsiz olan her şeyi okuyun ve izleyin.

En nihayetinde, biraz alıştırma ve adanmışlıkla, Bitcoin oynaklığından kâr edebildiğinizi görebilirsiniz. Başarınız sizi diğer piyasalara girmek için cezbedebilir. Günlük işlemler en az kumar oynamak kadar heyecan vericidir ve özellikle de yirmi dört saat alım-satım için müsait olan yüzlerce altcoin piyasası olduğu düşünülürse, bağımlılık gerçek bir sorun haline gelebilir.

Bitcoin kullanıcılarının sadece Bitcoin'e, altcoin'lere ve onlarla ilişkili hizmetlere yatırım yapmalarına imkân tanımakla kalmaz; internet bağlantısı olan herkese kocaman bir yatırım dünyasının kapılarını açar.

Finansal hizmetler basit banka hesaplarının ötesindedir. Finansal hizmetler varlığınızı artırmakla, ya da çalışmayı bıraktığınızda en azından bir kısmının elinizde olmasını garantilemenizle ilgilidir. Bu birikimden çok daha fazla-

[4]Bitcoin Fib Tutorial - Fibonacci Retracements. Yönetmen Brian Beamish. Anlatıcı Brian Beamish. Youtube.com/coinigy. 25 Nisan 2015. https://www.you tube.com/watch?v=9Wj9ITc0444

sını ifade eder; bu yatırım demektir. Yatırım hizmetlerinden genellikle Amerika'daki insanlar yararlanabilirler, ama ya bir aracıya danışmalı ya da E*TRADE gibi hizmetlerin minimum hesap seviyelerini karşılayacak kadar zengin olmanız gerekir. Eğer yatırımcılığa girmek istemiyorsanız ama altının yükseleceğine (ya da düşeceğine) dair içinizde bir his varsa, Bitcoin her halükarda kâr etmenizi sağlar.

Bitcoin bu bariyerleri sadece gelişmiş ülkelerin vatandaşları için değil, herkes için indiriyor. Bitcoin blok zinciri değer transfer etmek için geliştirildi ve bu değerin sadece Bitcoin olması için bir sebep yok. Gelecekte, blok zincirinde hisse senetleri ve tahvillerin de alım-satımlarının yapılmasını beklemek oldukça makul. Bu neredeyse kaçınılmaz görünüyor. Ama henüz oraya varmadık.

Bu süre içerisinde, Bitcoin günlük işlemleri var. Bunun Bitcoin üzerinde negatif etkisi olduğu tartışılır, çünkü sebep olduğu değişkenlik değer deposu olarak faydasını azaltarak para birimine zarar verebilir. Ancak, spekülatif işlemler Bitcoin'in en büyük kullanım alanlarından biri ve bir gecede ortadan kalkarsa bu hacim özlenebilir. Aptal altını olsa da, hızla zengin olma vaadi para birimine daha fazla insanın ilgisini çekmekte başarılı oldu. Spekülatif işlemler ve Bitcoin muhtemelen birkaç sene daha dost olacaklar. Bu birliktelik sadece Bitcoin'e özgü değil.

On Beşinci Bölüm:

Aitcoin Ticareti ve Şişirme-Boşaltmalar

Kendinizden utanmalısınız, çocuklar. Bir yandan Bitcoin ve getirdiği devrimsel değişiklikleri savunurken, diğer yandan gülünç altcoin'leri şişirmekle uğraşamazsınız.

— Blog yazarı Matt Branton,
The Branton Bits, 7 Nisan 2014

Bitcoin için geçerli olan stratejiler altcoin'lere de uygulanabilir; prensipler aynıdır. Ancak, altcoin'ler –özellikle de piyasa değeri olan birkaçı dışındakiler– şişirme ve boşaltma taktiklerine daha müsaitlerdir.

Şişirme ve boşaltma sadece kripto paralara özgü değildir. Menkul kıymetler borsalarında ve özellikle de düşük likiditeli borsalarda hep var oldular. Aynı model altcoin'ler için de geçerli. Piyasa likiditesi ne kadar düşükse (alan ve satan insan sayısı), şişirme ve boşaltma taktiklerini uygulamak o kadar kolay ve etkilidir.

Bu eski bir taktiktir. Temel düşünce yatırımda olanla

aynı: fiyat düştüğünde satın al ve yükseldiğinde sat. Tek farkı –ve bu taktiğe kötü şöhret veren şey– şişir ve boşalt planını uygulayan insanların fiyat artışının sebebi olmalarıdır. Planın bir parçası olan 'boşaltma' gerçekleştiğinde, ihale her şeyden habersiz yatırımcılara kalır.

Bu süreç bazen coin'in uzun vadede sağlığı için zararlı olabilir. Algılanan değerin yapaylıkla aşılanması, bir coin'in uzun vadeli görünümüyle ilgilenenlere tatsız bir iniş çıkış gibi gelebilir. Aynı zamanda, bunları idare edebilen coin'ler için, kendilerini şişirmenin yanlış tarafında bulan yatırımcılar hariç, 'şişir ve boşalt' taktiği genellikle zararsızdır.

Geleneksel olarak, 'şişir ve boşalt' aynı genel modeli izler. Öncelikle, bir grup yatırımcı fazla likiditesi olmayan bir coin'i düşük fiyattan sessizce satın alırlar. Bazen coin'i yüklü miktarda satın almak şişirme hamlesi için yeterlidir ama daha karışık planlar mevzubahis olduğunda dedikodu yaparak başlarlar. BitcoinTalk topluluk sitesinde, insanlar geliştirici ekibinin, ya da topluluğun ne kadar iyi olduğundan ya da buna benzer şeyler söyleyerek coin'i övmeye başlarlar. Hatta kripto para haber sitelerinde bir iki makale bile yayınlatabilirler. Sonra yatırımcılar ve bu oldukça erken evrede onlara katılmayan ama sonradan ikna ettikleri kişiler bir anda yüklü miktarda alım yaparlar. Her büyük alımla birlikte fiyat artar ve daha önce de değindiğim gibi, fırsatı kaçırma korkusu da piyasadaki gelgite yardımcı olur. Coin'in fiyatının arttığını gördüklerinde, alıcılar değerinin gerçekten arttığını düşünerek alım yaparlar.

Daha sonra, sözde yatırımcılar artık daha değerli olan coin'lerini satarlar, fiyat dibe vurur ve oyuna geç katılan

yatırımcılar ellerinde kendileri piyasaya girmeden önce olduğundan daha değersiz bir emtiayla kalırlar.

Bu tür taktikler düşük likiditeli her türlü emtiayı etkiler. Sadece piyasada geleneksel emtialara kıyasla daha fazla sayıda düşük likiditeli kripto para var. Ve kripto para dünyası neredeyse kontrolsüz olduğu için 'şişir ve boşalt' taktiklerine çok sık rastlanıyor.

Bu planların arkasındaki gruplar taktikleri konusunda oldukça yüzsüzler. İçlerinde en kötü şöhretli olan Bob-Surplus gruptur. Kripto para dünyasındaki en büyük 'şişir ve boşalt' oyunlarının arkasında oldular ve çabaları konusunda oldukça açık sözlüler.

Grubun arkasındaki adam 'yatırımcılardan' grubuna katılmaları için 2BTC alıyor. Piyasa materyallerine göre, bu şanslı yatırımcılara şişireceği bir sonraki coin'i söylüyor. 'Yatırımcılar' bu coin'i satın alarak fiyatı yükseltiyorlar. Sonrasında, coin boşaltılarak bu heyecana kapılanların elinde kalıyor.

SurplusBob'ın fiyatı yükseltmediğine, aksine üyelik ücretlerini cebe indirip heyecandan yararlanarak coin'in büyümesini sağladığına dair çok sayıda suçlama var. Kârın vaat edildiği kadar yüksek olmadığından şikâyet eden grubun birkaç eski üyesiyle ilgili haberler çıkmıştı.[1]

Uygulanabilir o kadar çok söylenti var ki, birini seçmek imkânsız. Yılanlarla aynı yatağa girmek sözü yerinde olur.

'Şişir ve boşalt' taktiği kripto paranın kısa tarihi boyunca birçok kez tekrarlandı. Ancak, en çok zarar veren örnekler,

[1]Fury, The Sound And. "The Story of Bob Surplus." Bitcoin Talk. 17 Aralık 2014. Erişim tarihi 22 Haziran 2015. https://bitcointalk.org/index.php?topic=896480.0

en başından beri 'şişir ve boşalt' planlarında kullanılmak üzere tasarlanan coin'lerdir.

Günümüzde piyasaya bir coin sürmenin popüler bir yolu ilk dijital para arzıdır (*initial coin offering* - ICO). Her dijital para arzına şüpheyle yaklaşılması gerekir, çünkü bu, coin'in yaratıcısına yüklü miktarda para akıtma potansiyeline sahiptir. Bu şekilde piyasaya sürülen bir coin'de ön çıkarım yapılması gerekir. Arz edilebilecek coin'ler olmadıkça 'arz etmek' diye bir şey olamaz. İlk arz edilen coin'lerin ağı ilk güvenceye alanlara gittiği tamamen adil bir dağılımda, söz konusu coin'in yaratıcılarına menfaat sağlamak dışında, iş ispatı (PoW) gerektiren bir coin'in ilk ön çıkarımına gerek yoktur.

Ancak proof-of-stake (PoS) coin'lerin ilk başta küçük miktarda dağıtılması gerekir. Ağa getirdikleri hash gücüne bağlı olarak madencilerin ödüllendirildikleri iş ispatına (PoW) dayanan coin'lerin aksine, proof-of-stake coin'ler madencilere ne kadar coin bulundurduklarına bağlı olarak verilir, genellikle bir ila beş faiz oranıyla. Elinde coin bulunan biri yoksa, faiz verilmesi gereken biri de yoktur. O nedenle, coin'i başlatmak için küçük miktarda ön çıkarım yapılmalıdır.

Birçok coin iş ispatına (PoW) dayanarak piyasaya sürülür ve belirli sayıda blok işlendikten sonra proof-of-stake'e geçiş yapar. Ön çıkarım olmadığı düşünülürse, yatırım yaptığınız coin'in adil bir ilk dağılımı olduğunu garantilemenin en kesin yolu budur. Elbette, serbest piyasada işlem görmeye başladıktan sonra şişirme-ve-boşaltma unsurları olmayacağından emin olamazsınız. Büyük ihtimalle olacak ve bir coin'in piyasaya sürüldüğü an 'şişir ve boşalt' taktiği için oldukça iyi bir zamandır.

Ama saf proof-of-stake coin'leri dağıtmanın adil yolları da var. Potansiyel yatırımcıların sadece daha iyi araştırmaları gerekiyor. Göz önünde bulundurulması gereken bazı şeyler var. Coin'ler 'ilk dağıtım' yoluyla serbest bırakılırlar ve bu tam da kulağa geldiği gibidir: Cüzdana geçirme işlemi için kullanılacak ilk coin grubunun insanlara nasıl dağıtıldığıdır. Unutmayın, proof-of-stake coin'ler hâlâ işlemleri doğrulamak için dünya çapındaki kullanıcılarının çalıştırdığı bilgisayar ağlarını kullanıyorlar. Aradaki fark, proof-of-stake'in ağa ne kadar bilgisayımsal güç getirdiğinizi önemsememesi ve elinizde bulunan coin sayısına göre ödüllendirilmenizdir. Bu fikir ağdaki varlığınıza ve coin'lerinizi elinizde tutmaya ne kadar istekli olduğunuza bağlı olarak ödüllendirilmekten ibarettir. Ama ortada henüz coin yoksa, stake edilebilecek coin'lerin olması için ilk coin grubu yaratılıp dağıtılmalıdır. Bazı coin'ler bunu kısa süreli iş ispatı evresiyle yapıyorlar ve bu hiç şüphesiz proof-of-stake coin piyasaya sürmesi gereken ilk coin'leri en adil şekilde dağıtma yoludur.

İlk dağıtım yüzde birkaç puanı geçmemelidir; tercihen piyasaya sürülecek coin'lerin sadece yüzde biri olmalıdır. Bu şekilde, coin dağıtılırken büyümek için zamanı olur. Unutmayın, bunun bir coin'in doğumu olması gerekiyor, yaşam döngüsünün daha sonraki evreleri değil. İlk etapta yüksek miktarda dağıtım yapılması, para biriminin büyük ihtimalle birkaç kişinin ellerinde kalarak merkezileşeceği anlamına gelir. İlk dağıtımdan yüklü miktarda bulundurarak 'şişir ve boşalt' taktiğini rezervleri tükenene kadar birçok kez uygulayabilirler. Buna ek olarak, eğer bir kişi elinde çok fazla coin bulunduruyorsa ve onları stake ediyorsa, teorik olarak blok zincirini değiştirebilir.

Yüzdenin nasıl bölündüğünün de önemi var. Katı kurallar yok ama ilk dağıtımın önemli bir bölümü halk için ayrılmalıdır. Geliştiriciler için kenara küçük bir miktar ayırmak makul olmaz. Ama şunu unutmayın: henüz bir coin'i piyasaya sürmedikleri için kendilerini kanıtlamış değiller.

İdeal olarak, ilk dağıtılan coin'ler ücretsiz olmalıdır. İnsanlar e-posta ya da ona benzer bir şey göndererek coin'den kendi paylarına düşeni almalılar. Ama eğer bir şirket büyükse, tanınmışsa ve alenen sergilediği bir teknolojiye sahipse, o halde ücret talep etmesi tam olarak oyunu bozmaz. Ama geliştiriciler ilk 'piyasa' fiyatından bahsederken –Josh Garza'nın Paycoin'le yaptığı gibi– özel yatırımcıların farklı bir fiyattan alacaklarını ima ediyorlarsa, bu kesinlikle bir kırmızı alarmdır.

Unutmayın, fiyat bir coin'in yapabileceklerine bağlıdır. Eğer bir coin henüz hiçbir şey yapmadıysa, bir fiyatı olmamalıdır. Paycoin piyasaya sürüldüğünde, 'halk' için belirlediği fiyat $20'dan piyasaya sürmeden önce birkaç farklı fiyattan yatırımcılara ve GAW madencilik operasyonlarının eski müşterilerine coin'in haklarını çoktan satmıştı.[2] Paycoin serbest piyasada hiçbir zaman o fiyata ulaşmadı. Ama coin'i ücretsiz ya da ucuza alan insanlar umut dolu yatırımcılar taban yapan coin'i hızla satın alırken servet yaptılar.

Buna rağmen, ilk dağıtım neredeyse hiçbir zaman bir coin'i almak için doğru an değildir. Fiyat neredeyse her zaman belirli bir noktadan sonra düşer, meşru coin'lerde bile bu böyledir. En iyi strateji piyasaya sürüldükten son-

[2]"Paycoin Is Here | Paycoin Digital Currency." 17 Mayıs 2014. Erişim tarihi 22 Haziran 2015. https://archive.is/0HEwd. http://paycoins.biz/paycoin/

ra bir coin'in ne yapacağını bekleyip görmektir. Bitcoin'in günümüzde olduğu noktaya gelmesi neredeyse sekiz sene sürdü ve henüz zirveyi görmedi. Bir sonraki büyük altcoin'i piyasaya sürüldüğünde satın almayanların hiçbiri ilk benimseyenlerden olma fırsatını 'kaçırmayacak'; yatırım yapmak için yeterince vakit var.

Her ne kadar faydası olsa da, bir coin'in Paycoin gibi piyasaya sürülmeden önce isminin tanınır olmasına ve basın tarafından ilgi görmesine gerek yok. 'Şişir ve boşalt' yönteminin başarılı olmasının tek sebebi topluluktaki heyecandı.

Eğer bir 'şişir ve boşalt' taktiğinin kurbanı olmaktan kaçınmak istiyorsanız, temel kural sadece gerçekliği kanıtlanabilir olan şeyler üzerine bahse girmektir. Sadece koda gerçekten bağlı olan coin'lere –geliştiricisi sürekli kodun üzerinde çalışan ve açık kaynak olan coin'ler– yatırım yapın. Kendiniz programlayamasanız bile, GitHub sayfasının ne kadar aktif olduğuna bakarak bir geliştiricinin ne kadar aktif olduğuna dair fikir edinebilirsiniz.

Sadece git komutalarına (önerilen değişiklikler) bakmak yeterli değildir. Bir geliştirici, aktif gibi göstermek için kod üzerinde hiç etkisi olmayan küçük 'git pull' komutları (uygulanmış değişiklikler) yapabilir. Ama biraz kurcalayarak değişikliklerin önemli olup olmadığını anlayabilirsiniz. Kod anlaşılmaz görünebilir ama bir coin'e önemli miktarda para yatırmadan önce, kodunu çatallandığı coin ile karşılaştırmalısınız. (Bir coin'i çatallaştırmak değişiklik yapma amacıyla kodu yeni bir Git'e kopyalamak demektir.) Bunu GitHub'a bakıp iki projeyi karşılaştırarak yapabilirsiniz. Bazı geliştiriciler coin'in geldiği yeri gizlemeye çalışabilirler.

Çok az coin sıfırdan yaratılır, o nedenle her zaman bir şeyin referansı olmalıdır. Eğer yoksa, o halde geliştiriciler çok az çalıştıklarını gizlemeye çalışıyor olabilirler. İki coin'i karşılaştırmak becerinizi aşıyorsa, o halde kodu kontrol etmek için bir uzmana danışabilirsiniz, ama denetçiyi de araştırdığınızdan emin olun. Çok az emek verilen coin'lere 'geliştirici kanıtı' sertifikası veren web siteleri var. Geliştirici kanıtı sertifikası genellikle geliştiricinin koda ne kadar emek sarf ettiğiyle değil, gerçek kimliği hakkında ne kadar açık olduğuyla ilgilidir.

Kodun kaynağını bulursanız ve ismi dışında birkaç değişiklik varsa ya da hiç değişiklik yoksa, pek fazla çaba gösterilmemiş demektir. Bu coin'i tamamen elemeniz gerektiği anlamına gelmez ama yatırım yapmak için kanıtlanabilir gelişim olana kadar beklemelisiniz. Eğer bir coin açık kaynaklı değilse, olana kadar yatırım yapmayı aklınızdan bile geçirmemelisiniz.

Unutmayın, coin'lerin büyük bir bölümü popüler borsalara geçer geçmez elden çıkarılırlar. Bir 'şişir ve boşalt' planının parçası bile olmayabilirler. Madenciler ve ilk benimseyenler serbest piyasada ilk erişime sahipler, o nedenle mümkün olduğunda yatırımlarını paraya dönüştürmeleri çok doğal. Coin kötü niyetli olsun ya da olmasın, madencilerden biri değilseniz, o kaçınılmaz ilk elden çıkarmadan önce yatırım yapmak için nadiren bir sebep olabilir.

Bir sonraki maaş gününüzde yeni altcoin'ler peşinde koşmanızı tavsiye etmiyorum. Ya bir sahtekârlık kurbanı ya da sürdürülebilir bir şeye dönüşme ihtimali çok düşük olan iyi niyetli bir coin'e yatırım yapmış olursunuz. Daha oturmuş altcoin'lerden bazılarını araştırmak, uzun vadede hangisinin hayatta kalma şansı olduğunu düşündüğünüze

karar vermek ve sonra gözünüz gelecekte –yatırımın birkaç sene içinde yok olabileceğini bilerek– o coin'lere küçük miktarda yatırım yapmak iyi bir fikir olabilir.

Yeni coin'ler aracılığıyla kâr peşinde koşmak saçma bir iştir. O coin'lerden bazılarında etkili bir şekilde madencilik yapabilecek donanıma sahipseniz, madencilik yapıp daha sonra ilk borsaya çıktıklarında onları elinizden çıkarmanızın bir mahsuru yok, ama bunu yapmak için yeni donanım almaya değmez. En iyi ihtimalle, zaten sahip olduğunuz Bitcoin madencilik donanımından birkaç raunt daha kazanç elde etmenin bir yolu olur.

On Altıncı Bölüm:

Eşler Arası Kredi Verme

Gerçek dünyaya bakarsanız, fakirlerin deneyimsiz ya da eğitimsiz oldukları için değil, emeklerinin karşılığını alamadıkları için fakir olduklarını görürsünüz. Sermaye üzerinde kontrolleri yoktur ve insanlara fakirlikten kurtulma gücünü veren sermaye üzerinde kontrol sahibi olmaktır.

— Muhammad Yunus, *Banker to the Poor: Micro-Lending and the Battle Against World Poverty*'nin yazarı

Mikrokrediler yıllardır internet ekonomistleri ve gelişmekte olan ülkelerin savunucularının odak noktasında oldu. Bu eski bir fikir: hayırseverlik iyi olsa da, desteklemek daha iyidir. 'Bir adama balık tutmayı öğretirseniz, her gün doyar,' sözünde olduğu gibi.

Mikrokredi ve mikrofinans siteleri yıllardır var. Kiva, Opportunity Fund ve Accion en popülerleri arasında yer alıyorlar. Farklı boşlukları doldurup farklı amaçlara hizmet ediyorlar ama en nihayetinde hepsi aynı şeye dayanıyor;

ya hayırseverlikle ya da finansal yatırım olarak birbirlerine kredi veren bireylere. Amaç fazla paranın büyük değişiklik yaratabileceği alanlar yaratmak. Birine verdiğim ya da yatırdığım yirmi doların pek fazla etkisi olmayabilir ama onu yüzlerce kullanıcının yirmi dolarıyla birleştirince, birden o kadar da önemsiz bir miktar gibi görünmez; özellikle de, ödünç alan kişi genellikle yaşam maliyeti çok daha düşük olan bir üçüncü dünya ülkesinde olduğu için.

Bitcoin'in bu piyasada iki faktörden ötürü çok fazla potansiyeli var. Birincisi, neredeyse olmayan işlem ücreti onu mikrokrediler için uygun kılıyor. Birçok mikrokredi ve mikrofinans sitesi kredi verenleri olarak orta sınıf ve üstünü hedef alsa da, Bitcoin destekli mikrokredi siteleri yoksulların bile başkalarına yatırım yaparak kıt birikimlerini artırmaları için imkân sunuyor. Paranın faiziyle birlikte geri ödeneceğine dair makul bir beklentiyle elli dolar, beş dolar ve hatta beş sent bile yatırım yapılabilir. Geleneksel para yöntemini kullanarak böylesine küçük miktarlarda yatırım yapmak, sıra borcu ödemeye geldiğinde borç verenler için can sıkıcı olabilir. Ya onlar ya da aracılar her ay yavaş ve etkisiz eski sistemleri kullanarak düzinelerce küçük para transferi yapmak zorunda kalırlar. Yatırımcılara Bitcoin ile basit ve ucuz bir şekilde anında ödeme yapılabilir. İnternet erişimli ama yasal paraya dayanan eşler arası borç programları çok hızlı ve basit sistemler yarattılar, ama yine de eski sistemi kullanmak zorundalar ve bu yüzden yüklü miktarda ücretler ödüyorlar. Kendisi hiçbir ücret almayan ve işletme giderlerini karşılamak için ayrı bağışlara bağlı olan hayırsever eğilimli mikrokredi sitesi Kiva gibi sitelerde bile bütün para kredi alanların eline geçmiyor.

Çünkü paranın kredi alanların eline geçmesine yardımcı olan 'saha ortakları' bazen komisyon alıyorlar.

Güçlü bir yatırımcı olmasam da, Bitcoin'e dayanan en büyük mikrokredi/mikrofinans sitesi BTCJam aracılığıyla yatırım yapmak konusunda deneyimliyim. Tecrübelerim çoğunlukla olumlu. Bitcoin dünyasındaki birçok şeyde olduğu gibi bu tür yatırımlarda yeterince dolandırıcı çekiyor. Ama bunun gözünüzü korkutmasına izin vermeyin. BTCJam riski sergilemekte iyi bir iş çıkarıyor ve kredi alanların çoğu borçlarını ödemek konusunda ciddiler. Ayrıca, BTCJam fotoğraflı kimlik, sosyal medya hesapları bağlantıları, gelir belgesi, banka hesapları ve hatta eBay ve PayPal hesapları gibi şeyler sorarak kredi alanların kimliklerini doğrulamak için elinden geleni yapıyor. Sonra, verdikleri bilgilere bağlı olarak her kredi alana bir derece veriyor.

Yüksek dereceli krediler çoğunlukla borcu tamamen kapatırlar. Düşük dereceli kredilerin geri ödeme riski daha fazla olduğu için faiz oranı da yüksektir. Unutmamanız gereken birkaç hile var. Birçok dolandırıcı bazı belirli kalıpları izler. Paranızın bu tür bir borçlanıcıya gittiğini görürseniz çok dikkatli olun. Herkes bir yerden başlamak zorunda olsa da, diğer yatırımcıların bu ilk riski almasına izin vermeyi isteyebilirsiniz. BTCJam'de bir krediyi ödememenin sonuçları olsa da, bir an önce para bulmak isteyen birçok kişi bu köprüyü yakmaya razıdır. Borcunu ödediğini kanıtlayan birine yatırım yapmak borcunu ödemeyen birine yatırım yapmaktan daha güvenlidir.

Aynı şekilde, borç alan kişinin geçmişine dikkat edin. Birçok dolandırıcı kredi verenlerin büyük borçları finanse etmekte tereddüt ettiklerini bilir ve kredi alıp küçük mik-

tarlarda ödeyerek güven kazanmaya çalışır. Sonrasında asla ödemeyi düşünmedikleri yüklü miktarda bir kredi alırlar. Birkaç küçük krediyi başarılı bir şekilde ödeyen ve artık beş ya da altı bitcoin isteyen borçlanıcılara karşı şüpheyle yaklaşın.

Yukarıdaki iki tüyo borç vermenin sadece en nadir durumlarda çiğnenmesi gereken katı kuralları olarak görülmelidir. Yatırım yapmak için borçlanıcı seçerken aklınızda bulundurmanız gereken bir diğer kural şudur: bir kişi sizden ne kadar uzaksa, borcunu ödemediğinde izini sürmeniz o kadar zordur. BTCJam kredi verenlere mahkemede kullanılabilecekleri bir tahkim kararı veren dış arabulucuya bütün bilgileri gönderse de, 200 dolarlık bir borç için (örneğin) Hindistan'daki birinin peşine düşüp onu bir Hint mahkemesine çıkarmak ne makul ne de buna değer olur.

Kredi verenlerin diğer ülkelerdeki kişilere yatırım yapmamalarını önermek istemiyorum, çünkü gelişmekte olan ülkelerdeki girişimcilere fırsat sağlamak mikrokredi ve mikrofinansın en büyük toplumsal faydalarından biridir. Daha ziyade, sizinle aynı adli yargılama bölgesinde olmayan, özellikle de bahsettiğim katı kuralları çiğneyen, borçlanıcılara yatırım yaparken dikkatli olmanız için uyarıda bulunuyorum.

Kredi vermeyi düşünürken, BTCJam'in değerlendirme sistemine, daha deneyimli borç veren kişilerin yorumlarına ve borç alan kişinin geri ödeme planının makul olup olmadığına dikkat edin. Tüyolarımdan birini ya da hepsini göz ardı etmek istiyorsanız, hiç çekinmeyin. Hatta kârlı bile çıkabilirsiniz. Unutmamanız gereken en önemli

strateji çeşitliliktir; farklı sayıda borçlanıcıya kredi verdiğinizden emin olun. Yeterli çeşitlilikle, BTCJam kredilerinin geri ödemelerini alabilirsiniz, riskli kredilere yatırım yapmadığınız sürece.

BTCJam'deki kredilerin çoğu ya Amerikan doları ya da borçlanıcının para birimi üzerinden belirlenir. Bu borçlanıcı ve kredi veren kişiyi arada sırada görülen Bitcoin'in fiyatındaki devasa dalgalanmadan korumak amaçlıdır. Kredilerin Bitcoin kullanılarak alınmasına ve ödenmesine rağmen, kredi ve geri ödeme için gereken Bitcoin genellikle borç alanın seçtiği yasal para biriminin dönüşüm oranına bağlıdır. Bu sistem kredi veren kişinin kısmen güvenilir –doğru düzgün bir araştırmanın yapıldığını varsayarsak– bir gelir akışı sürdürmesine ve parasını 'aktif' tutarken Bitcoin fiyatındaki dalgalanmalara karşı kendisini korumasına imkân tanır.

Bazı krediler yasal para fiyatına bağlı değildir, ama bunlar sadece Bitcoin ile para kazanan borçlanıcılara tavsiye edilir. Boğa piyasasında olan ya da Bitcoin fiyatını elverişli bulan ama yine de paranın bir cüzdanda durmasına izin vermekten başka bir şey yapmak isteyenler için faydalı olabilir. Ancak, Bitcoin kredi seçenekleri yasal paraya bağlı kredilerden daha sınırlıdır.

Bir borçlanıcının bakış açısından bakıldığında, BTCJam –ve gelecekte ona benzer hizmetler– bir bankanın nazını çekmeye gerek kalmadan makul bir oranda kredi alma fırsatı sunuyor. Bir banka ya da risk sermayedarına yeterince yüksek getiri sunmayan iş modelleri birden uygulanabilir hale geliyor. Aynı zamanda, borçlanıcılar borçlarını kapatmak için kredi alıp onları kalabalıktan topladıkları tek bir

düşük faizli krediye dönüştürerek geleneksel kredicilerin hâkimiyetinden kurtulmak için BTCJam'i kullanabilirler. Ancak, dürüst olmak gerekirse, Kiva gibi geleneksel eşler arası sitelere kıyasla burada daha fazla risk varmış gibi görünüyor, çünkü Bitcoin bağlantısı borçlanıcıların kredilerini geri ödememenin yanlarına kâr kalacağını düşünmelerine neden oluyor. Yine de, kredilerin büyük bir bölümü geri ödeniyor, özellikle de yüksek dereceli olanlar.

Bankacılığın icat edilmesinden bu yana kredi vermek bankacılar için en kârlı eylemlerden biri oldu. İnternetin geleneksel plak şirketlerinin etkisini azaltması gibi, Bitcoin'in de geleneksel bankacılık endüstrisinin gücünü azaltma potansiyeli var. Bankalar ve bankacılar Bitcoin'in takdimini ve gelişimini atlatmak için muhtemelen evrim geçirecek olsalar da, kredi vermek konusunda tekel olmaları hızla sona eriyor. İnsanlar banka olduklarında, geleneksel bankacılık sistemine daha az ihtiyaç olacak.

Mikrokrediler ve mikrofinans Bitcoin'in –ve genel olarak internetin– büyük bir etkide bulunabileceği önde gelen alanların arasındalar. Bitcoin'in diğer birçok fonksiyonunda olduğu gibi, mikrofinans ve mikrokrediler yasal para birimleriyle de başarılabilir. Ama Bitcoin'i önemli kılan şey bunu daha iyi yapabilecek olmasıdır. Mikrokrediler ve mikrofinans her iki tarafında yararına olabilecek biçimde bireylerin başka bireylere yardım etmesiyle ilgilidir. Bu eşler arası işlemde, geleneksel finansal aracıları kullanmak için hiçbir sebep yok. Parayı borçlanıcıya göndermek için başka bir bankaya yollayacak Kiva'ya ya da başka bir hizmete para yollamak için bir banka –bu sırada ücretler birikecek– kullanmak yerine, kredi verenler parayı direk

borçlanıcıya gönderebilirler. En kötü ihtimalle, sadece yüzde bir ila dört komisyon alan BTCJam gibi bir aracıyla uğraşmak zorundalar.

Bazıları internet yüzünden müzik endüstrisinin başının dertte olduğunu iddia etse de, doğrusu internet birçok sanatçı için harika oldu. Kaybeden sanatçılar sadece listelerin en tepesinde yer alan ve tek bir hit şarkı sayesinde milyonlarca albüm satanlar oldu. Daha az görünür sanatçılar ve gruplar için internet dünya çapında keşfedilmeleri için bir yol oldu ve bu keşfedilme fırsatı, barların ve garaj konserlerinin bilinmezliğinden kurtulmalarını sağladı. Müzik endüstrisinde internetin gerçekten incittiği tek topluluk, gerçek sanatçıların yaratıcı çabalarından milyonlarca dolar para kazanan plak şirketleri oldu. Dağıtım –eskiden şirketlerin kontrolünde olurdu– internete geçer geçmez, birçok sanatçının artık onlara ihtiyacı kalmadı.

Bitcoin ve mikrokrediler de bankalarla aynı şeyi yapıyorlar. Bankaların sabit masrafları var: çalışanlar, elektrik, reklam ve bir işi yönetmenin getirdiği diğer her şey. Bunların hepsi bir kredinin masraflarına dahil ediliyor. Kitlesel fonlanan krediler, özellikle de Bitcoin kullanan kitlesel fonlanan krediler, bu masrafların hiçbirini karşılamak zorunda değil ve bankalardan daha iyi faiz oranları sunabilir. Büyük ölçüde azalan sabit maliyetler hem borçlanıcıya hem de kredi verene fayda sağlar.

Bundan faydalanmayan tek grup kredi tekelini elinde tutan gruptur. Son cümledeki 'tutmak' anahtar sözcük oluyor.

On Yedinci Bölüm:

Bitcoin Kullanarak Diğer Emtialara Yatırım Yapmak

Çeşitliliğin güzelliği, yatırımda bedava öğle yemeğine olabildiğince *yaklaşabilmenizi sağlamasıdır.*

— Finans yazarı Barry Ritholtz

Bitcoin kullanıcılarına sadece Bitcoin'e, altcoin'lere ve ilgili hizmetlere yatırım yapmalarına olanak sağlamakla kalmaz. Aynı zamanda, internet bağlantısı olan herkese kocaman bir yatırım dünyasının kapılarını açar.

On dördüncü bölümün sonuna doğru söylediğim bir şeyi tekrarlamak istiyorum: Finansal hizmetler basit banka hesaplarının ötesindedir. Söylediğim gibi, finansal hizmetler varlığınızı artırmak ya da çalışma hayatınız bittiğinde en azından bir kısmının hâlâ elinizde olmasını garantilemenizle ilgilidir. Bu birikim yapmaktan daha fazlasıdır; bu yatırım demektir. Yatırım hizmetlerinden Amerika'daki insanlar yararlanabilirler, ama genellikle bir aracıyla uğraşmak ya da E*TRADE gibi minimum hesap seviyesi olan

hizmetleri maddi olarak karşılayabilecek durumda olmak zorundasınız.

Bitcoin bu sınırları ortadan kaldırıyor. Bitcoin blok zinciri değer transfer etmek için tasarlandı ve bu değerin Bitcoin formunda olması gerekmiyor. Teorik olarak, blok zinciri herhangi bir şeyi transfer edebilir. Belgeler, doğum sertifikaları, evlilik sertifikaları ve pasaportlar şifrelenerek, güvenli bir şekilde blok zincirine işlenip kaydedilebilir. Gelecekte, blok zincirinde hisse senetleri ve tahvillerinin alım-satımının yapılmasını beklemek oldukça mantıklıdır.

Ama blok zincirinde her şeyin alım-satımının yapıldığı zaman henüz gelmedi. Altcoin Ripple bu hedefe ulaşmak için çok yol kat etti. Kullanıcılarının altının yanı sıra –hem yasal hem de kripto para– farklı para birimlerini satın almalarına imkân tanırken 'güvenli ağ geçitleri' kullanıyor. Güvenli ağ geçitleri, değerli maden yatırım şirketleri gibi, Ripple ağına koydukları varlıkları koruyacağına güvenilen oluşumlardır. Ağ geçidi emtia için bir borç senedi düzenler. Bu, istenen Ripple kullanıcısına transfer edilebilir ve kullanıcı istediği zaman onu başka birine satabilir ya da emtianın o anki değeri karşılığında Ripple almak için ağ geçidine geri transfer edebilir. Bir değerli maden şirketinin piyasaya bir 'gümüş para' sürdüğünü ve onu 10.000 ons gümüşle desteklediğini varsayalım. 100.000 gümüş para piyasaya sürerek her paranın bir gümüş onsun onda biri değerinde olmasını sağlar. A Yatırımcısı piyasa fiyatından 10 gümüş para satın alır ve gümüşün değeri yüzde on artar. A Yatırımcısı bunun üzerine değerli maden şirketine gidip yüzde on faiz alır –şirketin alacağı ücretler hariç– ya da onu gümüşün daha çok yükseleceğini düşünen B Yatırımcısı'na satar. B Yatırımcısı gümüş paraları hiçbir

ücret ödemeden A Yatırımcısı'ndan alıp gümüşün değeri yükselene kadar onları elinde tutabilir. Daha sonra, A Yatırımcısı'nın ödediğinden daha yüksek bir ücrete onları değerli maden şirketine götürebilir. Elbette, tersi de geçerli: gümüşün fiyatı düşerse, gümüş paraların değeri de düşer.

Kripto topluluğunun büyük bir bölümünün bu sistemle olan sorunu güvenli ağ geçitlerine güven duymanın zorunlu olmasıdır. Basitçe izah etmek gerekirse, insanlar bir aracıyı başka biriyle değiştiriyorlar. Güvenli ağ geçitlerinin isimlerindeki 'güveni' boşa çıkarmaları sonucunda bazı sorunlar yaşadılar, ama hâlâ ilginç bir sistem olma özelliğini koruyor.

Hisse senetleri ve benzer menkul değerler henüz Ripple ağına eklenmedi. Yokluklarının başlıca sebebi yönetmelik. Birleşik Devletler'de 'kredisiz' yatırımcıların menkul değerlere ve hisselere yatırım yapmalarına karşı çıkan kanunlar var. Bu potansiyel piyasayı öyle ya da böyle yavaşlattı.

Ripple ağı şimdilik yüksek hacimli günlük işlemler için çok yavaş olsa da, biraz tavizle yapılabilir. Teoride, ağ geçidine güvendiğiniz sürece Ripple ağında her şey transfer edilebilir. Ama Ripple herhangi bir yasanın ayaklarına basmamaya her zaman özen gösterdi. Diğer kripto paralardan daha merkezileşmiş olan Ripple Labs Ripple ağına eklentilerden muhtemel bir şekilde sorumlu tutulabilir. Hatta, bir keresinde yönetmeliğe ters düştü ama iş mahkemeye varmadan çözüldü.[1]

[1]Todd, Sarah, ve Ian McKendry. "What Ripple's Fincen Fine Means for the Digital Currency Industry." American Banker. 6 Mayıs 2015. Erişim tarihi 14 Ocak 2016. http://www.americanbanker.com/news/bank-technology/what-ripples-fincen-fine-means-for-the-digital-currency-industry-1074195-1.html

Karanlık Ağ piyasalarında Bitcoin karşılığında sunulan hisseler oldu ama geçerlilikleri tartışılır. Karanlık Ağ'dan 'hisse senedi' satın almak bir Karanlık Ağ satıcısından ödeme senedi aldığınız anlamına gelir ve bu tavsiye edebileceğim bir şey değildir. Mesleklerinin genellikle uyuşturucu ve çalıntı hesapları satmayı da içerdiği düşünülürse, ödeme senetlerinin muhtemelen pek anlamı olmaz.

Bir karanlık piyasadan herhangi bir 'hisse senedi' almanızı kesinlikle tavsiye etmeyeceğim gibi bir sohbet odası ya da mesaj panosunda tanıştığınız birinden de almamalısınız.

Söylemeye çalıştığım şey şu, yasalar engel olmasaydı, blok zinciri kullanarak hisse senedi alım-satımı yapmak mümkün olabilirdi. Ya Ripple ya başka bir altcoin ya da Bitcoin'in kendisi aracılığıyla çok yakında bu muhtemelen olacak. Wall Street'de olmayan piyasalar her geçen sene daha popülerleşiyor. Eninde sonunda, kripto paralar kod ve kriptografi dışında hiçbir aracının olmadığı tamamen eşler arası bir borsa yaratabilirler. Bu tür bir sistemde, insanlar hisselerini satın almak isteyen yatırımcılara varlıklarını kriptoyla imzalayarak devredebilirler ve yatırımcılar, hiçbir ücret ödemeden, dünyanın farklı noktalarındaki yatırımcılarla alım-satım yapabilirler. Serica adlı şirket teorik olarak, hisse senetleri ve tapular da dahil olmak üzere, hemen hemen her emtianın satın alınmasına imkân tanıyan bir eşler arası piyasa üzerinde çalışıyor ama bu özellikler şu anda özel beta sürecinde (özel olarak test ediliyor) ve henüz halkın erişimine açık değil. Ayrıca, hiç kimse nasıl çalışacağını bilmiyor.

Buna ek olarak, uzun zamandır Bitcoin'in savunucu-

luğunu yapan Overstock.com yönetim kurulu başkanı Patrick Byrne şu anda Wall Street'i değiştirecek bir piyasa üzerinde çalışıyor. Birçok kripto paraya bağlı 'borsa' projelerinin aksine, Overstock yasalara uygun olmak için doğru kanallar aracılığıyla hareket ediyor. Öncelikle, Overstock sadece kendi şirketinin hisselerini satışa sunacak, ama başka şirketlerin de onu izleyeceği umuluyor.[2]

Ancak, bu bölüm gelecekle ilgili değil. Bitcoin'in bugünkü yatırımlarınızı çeşitlendirmenize nasıl yardımcı olabileceğiyle ilgili. Her an iflas etme ihtimali olan kâr amaçlı kuruluşların bazılarından bahsedeceğim.

Bütün Bitcoin kuruluşlarında olduğu gibi, bir sene, hatta altı sene sonra bile ortalıkta olacaklarını garanti edemem. Onlara bu kitapta yer vermem için hiçbiri bana para ödemedi; sadece en güvenilir bulduklarımı seçtim. Bununla birlikte, bir şirkete para verirken, her zaman onu iyice kontrol etmelisiniz. Güvenilir bilgiler genellikle hızla değişir, o nedenle bu kitap yayınlandığından beri hiçbir şeyin değişmediğinden emin olmak için kontrol edin.

Altın tutkunları için onlarca yıldır güven bir sorun oldu. 1933'teki Altın Rezervi Yasası'ndan beri, kimlerin altın bulundurup satabileceği hakkında katı kontroller oldu. Bu düzenleme yatırımcıların altınlarını fiziksel olarak saklamaları için bir üçüncü partiye güvenmelerini gerektiriyor. Bu riskli olabilir, çünkü şeffaflık olmadan şirketin kendisini aşırı genişletip genişletmediğini bilmek imkânsızdır. Elbette, bir kasa dairesinde yirmi altın külçe saklayabilir

[2]Leising, Matthew. "Discount Retailer Overstock Has New Target: Upending Wall Street." Bloomberg.com. 14 Ocak 2016. Erişim tarihi 14 Ocak 2016. http://www.bloomberg.com/news/articles/2016-01-14/discount-retailer-overstock-has-new-target-upending-wall-street

ama ya müşterilerine iki yüz altın külçe borcu varsa? Ya müşterilerin hepsi aynı anda altınlarını geri almak isterse? Zamanla, düzenlemeler bu riski azalttı ama banka iflası altınlarını evlerindeki bir kasada saklamayan herkes için bir endişe olarak kalmaya devam etti.

Tıpkı yasal para yatırımlarında olduğu gibi, birçok Bitcoin altın yatırımı da gerçek bir altın külçesi bulundurmayı içermiyor. Size bunu satacak siteler bulabilirsiniz, özellikle de Birleşik Devletler dışında yaşıyorsanız ama birçok site, külçe altın hizmeti sunan sertifikalı bir şirkette altına sahip olarak çalışır.

Kripto para dünyasına geçmek riski artırır. Riski artıran Bitcoin'in kendisi değil; daha ziyade, Bitcoin'i altına (gümüşe ya da başka bir emtiaya) dönüştüren şirket potansiyel bir başarısızlık noktası olabilir. Artık sadece altını elinde bulunduran tarafın ayakta kalıp dürüst olmasına güvenmeniz yetmeyecek, aynı zamanda Bitcoin'inizi alıp sizin yerinize o altını satın alan şirkete de güvenmeniz gerekecek.

Bu alanda lider Uphold'dur. Bu hizmet farklı yasal paralara ve emtialara yatırım yapmanıza olanak sağlıyor. Bitcoin'lerinizi Uphold hesabınıza emanet ediyor (ya da gönderiyorsunuz) ve sonra onları her biri farklı bir para birimini ya da emtiayı temsil eden hesabınızdaki farklı 'kartlara' transfer ediyorsunuz. Eğer o para birimi ya da emtianın fiyatı Bitcoin'in fiyatına kıyasla yükselirse, hesabınızda daha fazla bitcoin oluyor.

Ancak, Uphold'un basit bir yatırım aracından çok daha fazlası. Bitcoin'deki fiyat dalgalanması yüzünden birikimlerinin silinmesine maddi gücü yetmeyecek olanlara kripto paranın faydalarını getiriyor. Kullanıcılar Bitcoin'lerini

farklı emtialar ya da para birimlerinde tutabilirler. Fiziksel emtiaları alıp satmak küçük bir ücretin, genellikle yüzde 0,5 ve 2, ödenmesini gerektirir. Ancak kimliklerini doğrulayan kullanıcılar farklı para birimlerini ve Bitcoin'i ücretsiz bir şekilde alıp satabilirler.

Uphold'un bir diğer faydalı özelliği ise kullanıcıların, hangi döviz ya da emtiada olursa olsun, Bitcoin'in kabul edildiği her yerde ürünlerin bedelini ödemek için bakiyelerini kullanabilmeleridir. Uphold'un sunucu uygulamasında, Bitcoin'in fiyatına bağlı olarak emtia ya da para birimine karşılık uygun miktarda Bitcoin gönderir ve sonra ona eş değerde emtia ya da dövizi satıp rezervlerini doldurmak için tekrar Bitcoin satın alır.

Şu anda, Uphold kullanıcılarının Bitcoin'lerini Amerikan doları, avro, Japon yeni, İsveç frankı, Çin yuanı, Hint rupisi ve Meksika pezosunun yanı sıra, altın, gümüş, platin ve paladyum olarak tutmalarına imkân tanıyor. Petrolün de Uphold'un desteklediği emtialar listesine eklenmesi planlanıyor.[3]

Çok çeşitli emtialar ve dövizler bulundurmasının yanı sıra, Uphold şeffaflık konusunda da eşsiz. Uphold'un halihazırda bulundurduğu bütün varlıklarını ve yaptığı bütün işlemler hakkındaki bilgileri –ne kadar Bitcoin satıldığı, her emtianın ne kadar satılıp alındığını, vs.– gösteren blok zincirinin 'rezerv zinciri' adı verilen bir uzantısını barındırıyor. Finansal dünyada bu düzeyde bir şeffaflık duyulmamıştır ve Uphold'un bunu sunmak için iyi sebepleri var.

---

[3]DeMartino, Ian M. "Bitreserve Wants You To Hold - and Spend - Oil." CoinTelegraph. 12 Aralık 2014. Erişim tarihi 22 Haziran 2015. http://cointelegraph.com/ news/113085/bitreserve-wants-you-to-hold-and-spend-oil

Uphold CNET'in kurucusu Halsey Minor tarafından başlatıldı. CNET'i internette kâr eden pornografik olmayan ilk basın şirketi yapan Minor bir zamanlar milyarderdi. Oldukça başarılı Salesforce.com ve Grand Central Communications'ın kurucu ortağı oldu. Grand Central Communications daha sonra Google tarafından satın alınıp Google Voice olarak yeniden isimlendirildi.

Birkaç kötü ticari gayrimenkul yatırımı, güzel sanat bağımlılığı, 2008 finansal krizi ve kendisinin açtığı ve ona açılan çeşitli davalardan sonra, 2000'lerin sonuna doğru Minor meteliksiz kaldı. 2013'te, –internet çağının ilk başarı hikâyelerinden biri olan– Minor Chapter 7 iflas başvurusu yaptı. Uphold Minor'un geri dönme çabasıdır. Diğer kripto para temelli kuruluşlardan daha emniyetli olduğuna dair insanlara güven vermenin yanı sıra, Uphold'un şeffaflığı kullanıcıları fonlarının Minor'un alacaklılarını ya da güzel sanat bağımlılığını beslemeyeceğini garanti ediyor.[4]

Bu kulağa kural dışı bir vuruş gibi gelebilir ve eğer öyle hissediyorsa Halsey Minor'dan özür dilerim, ama doğru. İnsanlar paralarını, tamamen kendi suçu olsun ya da olmasın, milyarlarını tüketen birine emanet etmek konusunda tereddüt ederler. Rezerv zinciri paralarının sorumlulukla saklandığını kanıtlıyor. Minor'a göre, Uphold'un felsefesi şöyle, "Üyelerimizin paralarıyla ne yaptıkları onları ilgilendirir, ama bizim onların paralarıyla ne yaptığımız herkesi ilgilendirir." Rezerv zinciri bunun teknolojik bir şekilde somut örneği. Minor bu tür bir şeffaflığın sadece

[4]Stone, Brad. "Halsey Minor Returns, Bearing Bitcoins, via Bitreserve." Bloomberg.com. 15 Mayıs 2014. Erişim tarihi 22 Haziran 2015. http://www.bloomberg.com/bw/articles/2014-05-15/halsey-minor-returns-bearing-bitcoins-via-bitreserve

Uphold için değil, müşterilerinin kontrol edebilecekleri şekilde emtialarını tutmak için Uphold'u kullanmak isteyen şirketler için de şeffaflığa imkân tanıyan işletmeler arası hizmetler için yepyeni bir endüstri açacağına inanıyor. Kasım 2014'te Minor'la röportaj yaptığımda, büyüyen fırsatlar hakkında konuştu:

> [Uphold'a yaklaşan] bir şirket iş ortaklarının (A) yatırdıkları paranın güvende olduğunu ve (B) şeffaflık istediklerini söyledi. [...] Yatırımcılar bitcoin olmayan sistemin yükünü kullanıyorlar, [neler olduğunu göremiyorlar ama] herkes neler olduğunu görmek istiyor ve bunu sağlayabiliriz. Hiçbir banka bunu yapamaz. Şeffaflık içeren bir banka sistemi yok. Görünen o ki, şeffaflığın iş modelinin bir parçası olmasını isteyen birçok işletme var.
>
> Bu doğrulanabilir şeffaflık günümüzde var olandan daha fazla iş modeline olanak sağlayacak.[5]

Doğrulanabilir şeffaflık sıradan yatırımcılar için de önemlidir. Herhangi bir şirket size altın sattığını iddia edebilir ve hatta Bitcoin'inizi altın fiyatı üzerinden belirleyebilir.

Ama itibarlı bir altın sağlayıcısının desteklediği gerçek rezervler olmadan, fiyata yatırım yapmaktan ziyade aslında şirketin size altın fiyatı üzerinden para ödeyeceği vaadine yatırım yapıyorsunuz.

---

[5]DeMartino, Ian M. "Halsey Minor's Bitreserve Is Designed To Fix Bitcoin Volatility, But It Is Doing Much More." CoinTelegraph. 21 Kasım 2014. Erişim tarihi 22 Haziran 2015. http://cointelegraph.com/news/112966/halsey-minors-bitreserve-is-designed-to-fix-bitcoin-volatility-but-it-is-doing-much-more

Bu en sonunda Uphold için de geçerli olabilir; birdenbire kapanırsa, bünyesinde bulunan bütün para buharlaşır. Yine de, Bitcoin ekosisteminde altın için muhtemelen en emniyetli yer olabilir. Altınını dünyadaki en saygın altın satıcılarından biri olan Gold Bullion International'da tutuyor. Bunun altınınızı saklamak için elektronik transfer fonundan (EFT) daha güvenli olduğunu duydum. Bunu rezerv zinciriyle birleştirdiğinizde, kullanıcılar Uphold'da tuttukları varlıklarının gerçek ve oldukça güvende olduğundan emin olabilirler.

BitGold da –Nick Szabo'nun Bitcoin öncesi 'bit gold' önerisiyle karıştırmayın– altının Brinks teminatlı somut yerlerde dönüştürülebilir dijital versiyonlarını satıyor. Uphold'da olduğu gibi, BitGold'un web sitesine üye olduktan sonraki süreç de oldukça basit. Adımları teker teker açıklamaya gerek yok, çünkü yeterince basitler ve web sitesinin tasarımı zamanla mutlaka değişecek. Dikkate değer bir özelliği BitGold'un BitGold'un sisteminde tutulan altınla finanse edilebilecek MasterCard destekli bir bankamatik kartı sunuyor.

Başka seçenekler de var. Örneğin, BitGild geleneksel postala fiziksel paralar ya da altın, gümüş ve platin külçeleri gönderiyor. VeldtGold aynı şeyi altınla yapıyor ve Birleşik Devletler merkezli. Bunlar itibarlı hizmetlerden sadece birkaçı.

Emtia satın almak ve birikimleri farklı para birimlerine dönüştürmek eskiden sadece bunlara maddi gücü yetenlerin faydalanabildiği finansal araçlardı. Ama artık, Bitcoin sayesinde, isteyenlere finansal güvenlik dünyasının kapıları açılıyor. Bitcoin kendi para biriminize karşı birikimle-

rinizi garantiye alabilir –örneğin, Ukrayna'da yaşadığınızı varsayarsak, bu fena bir fikir sayılmaz– ama yine kendi dalgalanmasını yaşar.

Rus rublesinin değeri düştüğünde, birçok Bitcoin meraklısı biriktirdikleri paralarının değerini kaybetmemesi için Bitcoin'in Ruslar tarafından kullanılabileceğini iddia ettiler. Ne yazık ki, o aylarda rublenin performansı çok kötü olsa da, Bitcoin'inki çok daha kötüydü ve Ruslar paralarını Bitcoin olarak saklasalar bile pek kazançlı çıkmazlardı. Yine de, mantıklı bir düşünceydi ve Bitcoin kısa tarihinin en kötü gerilemesinin ortasında olmasaydı, işe yarayabilirdi. Söylemeye çalıştığım şey şu, Bitcoin Rus hükümetinin dünya sahnesindeki eylemlerine karşı o kadar kırılgan bir tasarruf aracı olmayabilirdi. Ayrıca, Bitcoin Rus rublesinden Bitcoin'e, altına ya da başka bir güvenilir varlık birikimine değer transferini gerçekleştirmek için kullanılabilirdi.

Haziran 2015'te, ekonomik krizin ortasında olan Yunanistan, vatandaşlarının avrolarını ülke dışına çıkarmasını önlemek için bazı önlemler aldı. Basında Bitcoin'in bu tür önlemleri atlatabileceğinden bahsediliyordu.[6] Günümüzde, Bitcoin'in bir insanın birikimlerini saklamasının güvenilir bir yolu olamayacak kadar değişken olduğu iddia edilebilir. Ancak, ara bir adım olarak kullanılabilir ve insanların birikimlerini dolar, altın, gümüş ya da Bitcoin kullanılarak satın alınabilen diğer sayısız emtiada saklama-

[6]Kelly, Jemima. "Fearing Return to Drachma, Some Greeks Use Bitcoin to Dodge Capital Controls." Reuters. 3 Temmuz 2015. Erişim tarihi 14 Ocak 2016. http://www.reuters.com/article/us-eurozone-greece-bitcoin-idUSKCN0PD1B420150703

larına olanak tanıyabilir. Ve bu, genelde son derece yüksek olan minimum alım seviyelerine ulaşmak zorunda olmadan ya da Yunanistan'ın durumundan örnek vermek gerekirse, paranızla ne yaptığınızı kısıtlayan kanunlarla uğraşmadan başarılabilir.

Mesele Yunan hükümetinin Bitcoin'in sermaye kontrolleri hakkında yapabileceklerinden endişelenmemesi değildi; isteseler bile pek bir şey yapamazlardı. Bitcoin'ler cep telefonlarında rahatlıkla transfer edilebilirken, teknoloji dostu Yunanların avrolarını bitcoin formunda ülke dışına çıkarmalarına engel olmaları için fiziksel ve dijital bir ambargo yapmalarını gerektirirdi.

Birkaç sene öncesine kadar, değerli maden yatırımı sadece varlıklı ve bağlantıları olan kişilerle sınırlıydı. Bitcoin'le, neredeyse herkes varlıklarını diledikleri biçimde saklayabilir. Sınırlar, siyaset ve yasaların canı cehenneme.

ÜÇÜNCÜ KISIM:

Bitcoin Benim İçin Ne Yapabilir?

On Sekizinci Bölüm:

Para Havalesi

Dünya çapında 215 milyondan fazla insan anavatanları olarak bildikleri ülkelerinin dışında yaşıyorlar. Ama para havalesine muhtaç ailelerin çoğu dünyadaki finans sisteminin dışında yaşamlarını sürdürüyor. *Elektronik para transferinin küresel yaygınlığına rağmen, birçok göçmen işçi kırsal kesimde yaşayan alıcıların uzun yollar kat etmesini gerektiren masraflı para havalelerine bağlı modern bankacılık hizmetlerinin kolaylığından mahrum kalıyor.*

— Kanayo F. Nwanze, Uluslararası Tarımsal Kalkınma Fonu başkanı

Bitcoin kullanmanın birinci sebebi her zaman spekülatif yatırım oldu. Öyle ya da böyle, Bitcoin alım-satımı Bitcoin işlemlerinin arkasındaki en sık rastlanan nedendir. Daha önce de belirttiğim gibi, fiyattaki büyük dalgalanmalar dijital parayı günlük işlemciler için oldukça çekici kılıyor.

Silk Road piyasası ortaya çıktığında, Bitcoin'e başka bir kullanım alanı verdi: kredi kartı şirketlerinin ya da yetkililerin bilmesini istemediğiniz şeyleri satın alma. En sonunda, para birimi ana akım satıcılar tarafından kabul edildi ve maaş ödeme, ürün ve hizmet satın alma ve benzeri şeylerde yasal bir ödeme yöntemi olarak giderek daha fazla kullanılır oldu. Bunların her biri yasal para birimleriyle yapılabilir ve genellikle öyle yapılıyor. Kiranızı, eğitiminizi ya da market masraflarınızı ödemek için yasal para kullanabilirsiniz. Ama nakit ve diğer para biçimlerinin aynı zamanda sayısız kullanım alanı var. Onu yatırım yapmak, birikim yapmak ve daha milyonlarca şey yapmak için kullanabilirsiniz. İlk başta, kripto para birimleri birkaç kullanımla sınırlıydı ve, Silk Road gibi, birçoğu sıradan insanlar için pek çekici değildi.

Bitcoin'i ve blokzinciri teknolojisini doğası gereği çekici kılan şeyler, diğer para birimlerine kıyasla üstün oldukları taraflardır: Bitcoin ve diğer dijital para birimleri, bir kişinin genellikle yurtdışında olan başka birine para göndermesi için kusursuz biçimde tasarlanmıştır. İnsanların şu anda bitcoin'i yasal bir para birimine dönüştürmekte karşılaştıkları zorlukları bir kenara ittiğimizde, Bitcoin hiç şüphesiz para havalesi için mevcut diğer hizmetlerden daha iyidir.

Bu kitabın ilk bölümünde ele aldığım gibi, bu blokzinciri teknolojisi herhangi bir merkezi otorite tarafından kontrol edilmiyor ve internet gibi dağıtık bir ağ olarak varlığını sürdürüyor. Dağıtık sistemi kullanarak, dilediğiniz miktarda bitcoin'i ağdaki herhangi birine (başka bir Bitcoin adresine) göndermek neredeyse sürtünmesizdir; ko-

misyonlar ve gecikmeler gibi işlemi aksatan herhangi bir şeyin olmamasını kastediyorum. İnsanlar geleneksel yöntemleri kullanarak birbirlerine para gönderebilirler, ama onları kullanmak genellikle hem yavaş hem de pahalıdır. Western Union ve diğer para aktarıcılar daha hızlılar, ama her işlemden yüklü miktarda komisyon alıyorlar ve bunu yaparken dünya çapında milyarlar tahsil ediyorlar.[1]

Bitcoin sadece madencilere giden küçük bir işlem ücreti alıyor. Bu ücret genellikle bir sent ila birkaç sentin çok küçük bir bölümüdür. Miktarın işlemin boyutuyla hiçbir ilgisi yok, aksine Bitcoin'in mevcut değeri ve ağın ne kadar aktif olduğuyla ilgilidir. Kullanıcılar blok zincirinde onlarca milyon dolar transfer ettiler ve her defasında bu birkaç sent ya da daha aza mal oldu.

Para havalesi büyük bir iştir. Dünya Bankası küresel para havalesinin bu sene (2016) 681 milyar dolara ulaşacağını tahmin ediyor[2] ve paranın büyük bir bölümü gelişmekte olan ülkelere gidiyor. Bitcoin, tıpkı e-postanın telekomünikasyon şirketlerine ve posta hizmetlerine yaptığı gibi, kullanıcılarının aracıyı ortadan kaldırmasına imkân tanıyor. Artık gezegenin diğer ucundaki birine istediğim değeri gönderebilirim, hem de neredeyse ücret ödemeden.

Equibit'in yeminli mali müşaviri ve sertifika yetkilisi Chris Horlacher, Bitcoin'in benimsenmesinin dünyanın

[1] Anderson, Marc. "Global Remittance Industry Choking Billions out of Developing World." The Guardian. 18 Nisan 2014. Erişim tarihi 22 Haziran 2015. http://www. theguardian.com/global-development/2014/aug/18/global-remittance-industry-choking-billions-developing-world

[2] "Remittances to Developing Countries to Stay Robust This Year, despite Increased Deportations of Migrant Workers, Says WB." 4 Nisan 2011. Erişim tarihi 22 Haziran 2015. http://www.worldbank.org/en/news/press-release/2014/04/11/remittances-developing-countries-deportations-migrant-workers-wb

her yanındaki insanların hayatlarını nasıl geliştireceğine dikkat çekti.

> Dünya Bankası havale masraflarını yüzde beş puan indirmenin yılda 16 milyar dolar tasarruf sağlayacağını belirtti. Yüzde yüze ne dersiniz? Bu dünyadaki muhtaç insanların hayatlarını nasıl etkiler? Yıllık toplam havaleler şimdiden hükümet yardımlarını aşıyor ve hiçbir politik bağlantı olmadan doğrudan yoksulların cebine gidiyor. Bu kaynakları serbest bırakmanın yaşam kalitesi üzerinde büyük bir etkisi olur ve yoksulluğun eziciliğinden nihayet kalıcı bir şekilde kurtulabilinir.

İşler henüz bu evrede değil. Bitcoin'in küresel çapta bu tür bir etkisi olması için alıcının onu hızlı bir şekilde yaşadığı ülkenin para birimine dönüştürebilmesi gerekir. Bitcoin ağı neredeyse her yere ulaşıyor ama fiziksel görünümü, yani bitcoin karşılığında yasal para alabileceğiniz yerler sınırlı. Birçok alanda, özellikle de gelişmekte olan ülkelerin kırsal kesimlerinde. Bu dönüşümü makul bir oranda yapmanın bir yolunu bulmak genellikle çok zor.

2013 itibariyle, Dünya Bankası'nın raporuna göre, 60 milyar dolarlık yıllık Afrika havale piyasasında havale masrafları 4 milyar doları buluyor. Bu göçmen işçiler ve ailelerinin cebine girmeyen çok büyük bir miktar demektir. Göçmenlerin gönderdiği parayla yerel ekonomilerine büyük ölçüde katkıda bulunabilecekken, bunun gelişmekte olan ekonomiler üzerinde fazlasıyla negatif bir etkisi var. 2014'teki bir *Guardian* makalesi şöyle açıklıyor:

> Yüzde yirmiden yüksek komisyonu olan beş 'koridor' –ülkeler arası transfer– var ve hepsi de Afrika'da. Örneğin, Güney Afrika'daki göçmen işçiler 2012 yılında Botswana'ya gönderdikleri para üzerinden ortalama yüzde 23 komisyon ödeyerek onu dünyadaki en pahalı havale kanalı yaptılar. Transferlerin üzerine ortalama yüzde 22 komisyon koyulan Güney Afrika'dan Mozambik'e para göndermek ikinci en pahalı kanaldı. Uzmanlar para göndermenin bedelinin küresel endüstriyi ikili tekellerine alan şirketler –Western Union ve MoneyGram– tarafından şişirildiğini söylüyorlar.[3]

Bu ikili tekel, iki para transferi şirketinin fazlaca şımarmasına sebep oldu. Bazı Afrika ülkelerinden istenen yüzde yirmiyi aşan ücretler bu ikili tekelin en kötü örnekleridir; ama nispeten daha ucuz havale ücretleri bile Bitcoin'in madencilik ücretinin yanında astronomik kalır. Western Union havale ücretleri $4,99'ten başlıyor; bu kitap yayınlandığında bu ücret değişmiş olabilir. Ayrıca, transfer edilen tutara ve havale yapılan ülkelere bağlı olarak ek ücretler olabilir. Müşteriler işlemi gerçekleştirene kadar ücreti görmüyorlar bile.

Öte yandan, Bitcoin kullanıcıları yaklaşık iki bitcoin sentine eş bir madencilik ücreti bekleyebilirler, ama bu değişkendir ve genellikle ücretsizdir. Kasım 2013'te, Bitcoin ağında işlemden hiçbir ücret alınmadan 194.993 bitcoin

[3]Anderson, Mark. "Global Remittance Industry Choking Billions Out of Developing World." The Guardian. 18 Ağustos 2014. Erişim tarihi 13 Şubat 2016. http://www.theguardian.com/global-development/2014/aug/18/global-remittance-industry-choking-billions-developing-world

transfer edildi. Madencilik ücreti ödemek şart değil ama madencinin işlemi daha hızlı yayınlama ihtimalini artırmak için tavsiye edilir. Bu işlemin yasal para değerinin 147 milyon dolar olduğu tahmin ediliyor.[4] [5] Kimse bunu kimin ya da neden gönderdiğini bilmiyor ama uygulamada önemi yok. Yani, biri tek sent ücret ödemeden 147 milyon dolar havale gönderdi. Para dünyanın diğer ucunda ya da yan odada olan birine ve hatta göndericinin kontrolünde olan başka bir cüzdana gitmiş olabilir. Paranın gönderildiği yerin işlemin masrafı üzerinde hiçbir etkisi olmadı.

Geleneksel yöntemler kullanarak yurtdışına 147 milyon dolar göndermenin lojistiği karışıktır. Western Union gibi hizmetler kullanmak söz konusu bile olamaz ve IRS (Milli Gelirler İdraresi) ücretleri ve vergileri muhtemelen toplamdan büyük bir parça koparır.

Herhangi bir miktarda –büyük, orta ya da küçük– transfer yapmak isteyenler geleneksel hizmetler yerine Bitcoin kullanarak çok fazla şey kazanabilirler. Ancak şu anda, Bitcoin'in havale piyasasında büyük bir oyuncu olmasının önünde duran iki büyük engel var: müşteri bilgisi ve altyapı.

Bitcoin'in, özellikle de Çin ve Birleşik Devletler'de, giderek artan popülerliğine rağmen, dünya nüfusunun büyük bir bölümü hâlâ Bitcoin'in ne olduğunu bilmiyor. Eğer Bitcoin havale şirketleri 681 milyon dolarlık havale piyasasının bir kısmında pay sahibi olmak istiyorlarsa, bilgi

[4] "Transaction1c12443203a48f42cdf7b1acee5b4b1c1fedc144cb909a3bf5edbffafb0cd204" Blockchain, 11 Kasım 2013. https://blockchain.info/tx/1c12443203a48f42cdf7b1acee5b4b1c1fedc144cb909a3bf5edbffafb0cd204

[5] Southurst, Jon. "194,993 BTC Transaction worth $147 Million Sparks Mystery and Speculation." CoinDesk. 22 Kasım 2013. Erişim tarihi 22 Haziran 2015. http://www. coindesk.com/194993-btc-transaction-147m-mystery-and-speculation/

dağılımının zor olduğu yerlerde insanları bilgilendirmek için çalışmalılar. Alternatif olarak, müşterilerin havale yaparken hizmetin işlemi gerçekleştirmek için Bitcoin kullandığını bilmelerine bile gerek kalmadan Bitcoin'i otomatik olarak kullanabilecekleri bir yöntem geliştirmeliler.

Bir Bitcoin havale şirketi iki ülkede birer ofis kurup müşterilerini arka planda işlemleri gerçekleştiren Bitcoin teknolojisi hakkında eğitmek zorunda kalmadan insanların o ofisler aracılığıyla para göndermelerine imkân tanıyabilir. Bitcoin'in neredeyse olmayan ücreti sayesinde, şirket sadece gerekli masrafları ücretlendirebilir. Bitcoin ATM'leri bu noktada işe yarayabilir, ne de olsa küçük bir makineyi idare etmek çalışanları ve diğer her şeyi olan kocaman bir binayı idare etmekten daha ucuz olur. Ortalama bir evde 2,43 televizyonun olduğu ve evlerin yüzde 86'sından daha fazlasında internet erişiminin olduğu Birleşik Devletler gibi ülkelerde bile halkı Bitcoin hakkında eğitmenin zor olduğu görüldüğü için ATM'ler ilgi çekmek için popüler bir yol olabilir. Evlerin yüzde ikisinden daha azında internet erişiminin olduğu Etiyopya gibi ülkelerde bilgi erişimi çok daha sınırlı.[6] Sorun şu ki, ATM'lerle bile masraf çok fazla ve havale piyasasında ilerleme kaydetmek için ücretleri yeterince düşük tutmak zor olabilir. İdeal olarak, hem gönderici hem de alıcının Bitcoin'i diledikleri yasal paraya dönüştürebilecekleri erişilebilir ve ucuz bir yol olmalı.

Bitcoin'in Western Union ve MoneyGram ile farklı ülkelerde geniş ölçekte rekabet edebilmesi için altyapının havalenin 'son aşama' denilen kısmı için elverişli olması

[6] "Internet Users by Country (2014)." Chart. Internet Live Stats. Erişim tarihi 22 Haziran 2015. http://www.Internetlivestats.com/Internet-users-by-country/

gerekiyor. Birinin Etiyopya, Nijer ya da başka bir yerdeki birine Bitcoin göndermesi yeterince kolay bir şey.

Sorun, alıcı o Bitcoin'i kendi yerel para birimine dönüştürmek istediğinde başlıyor. Fiziksel Bitcoin dönüşümleri tam olarak yaygın değil ve çevrimiçi döviz büroları, varsa bile, gelişmekte olan ülkelerde açması zor olabilecek bir banka hesabına erişim gerektiriyorlar.

Bu sorunun iki olası çözümü var. Birincisi bu altyapıyı zaman içinde yavaşça inşa etmek; ikincisi bu son aşamayı bitirmek için halihazırda olan hizmetlerin sırtından geçinmek. Bu tür bir altyapıyı sıfırdan kurmak birçok Bitcoin şirketinin yapabileceği bir şey değil. Her ulusun ve, birçok açıdan şirketin ticaret yapmayı umduğu her bölgenin mevzuat çerçevelerine uymayı gerektiriyor. Birleşik Devletler'de, örneğin, ulusal çapta hizmet vermek isteyen şirketlerin 50 eyaletten mevzuata ilişkin izin almaları gerekiyor.[7]

Yabancı bir ülkede bir finans şirketi açmanın karışık mevzuatını hallettikten sonra bile, ücretlerin geleneksel hizmetlere kıyasla düşük olması için masrafları olabildiğince düşük tutarak ülkede bir varlık oluşturmak gerekir.

Bu taktik, başta makinelerini oldukça düşük ücretlerle kurabilen Bitcoin ATM şirketleri olmak üzere, birkaç şirket tarafından denendi. Bu ATM'ler havale için uygun olsalar da, nispeten yüksek ücretleri Bitcoin kullanmanın avantajını eledi.[8]

---

[7]DeMartino, Ian M. "Igot Founder Rick Day: Regulation Has 'Absolutely' Hindered Bitcoin In The US." MiningPool. 22 Nisan 2015. Erişim tarihi 22 Haziran 2015. http://coinjournal.net/interview-with-igot-founder-rick-day-regulation-has-absolutely-hindered-bitcoin-in-the-us

[8]Wile, Rob. "Think Fees On Normal ATMs Are Expensive? Check Out What It Costs To Use A Bitcoin ATM." Business Insider. 10 Mart 2014. Erişim tarihi 22 Haziran 2015. http:// www.businessinsider.com/using-a-bitcoin-atm-is-actually-pretty-expensive-2014-3

Rebit.ph ikinci yaklaşımı deneyen Bitcoin temelli bir havale şirketidir. Tek bir piyasaya odaklanan Rebit.ph, yurtdışında yaşayan Filipinliler için Filipinler'e Bitcoin havalesini elverişli bir seçenek yapmaya çalışıyor.[9] Rebit.ph'nin kurucu ortağı Luis Nuenaventura bu hizmetin arkasındaki stratejiyi şöyle açıklıyor:

> Bu hizmetler yurtdışından gönderilen bitcoin'i kabul edip pezoya, dinara ya da şiline dönüştürüyor ve sonra bu fonları farklı yurtiçi transfer yöntemleri aracılığıyla nihai faydalanıcıya ulaştırıyor. Faydalanıcının o fonların bitcoin aracılığıyla iletildiğini bilmesine gerek yok, onlar sadece göndericinin havale yaparken daha az para ödediğini biliyorlar. Alıcı bitcoin'e hiç dokunmadığı için oynaklık riski yok; bütün risk hizmet tarafından idare ediliyor.
>
> Son aşama üzerinde uzmanlaşarak, gayriresmi koridorlar oluşturmaları için diğer ülkelerdeki bitcoin girişimcilerini davet ediyoruz. Hong Kong'daki bir müşterinin Hong Kong dolarını son aşama hizmetine göndermeden önce Bitcoin'e dönüştürmesi gerekiyor. Onlara bu hizmeti verirken oldukça kârlı bir iş kurulabilir.[10]

---

[9] Balea, Judith. "Bitcoin Remittance Service Rebit Rolls out Zero Transaction Fees, KYC Policy." Tech in Asia. 15 Ocak 2015. Erişim tarihi 22 Haziran 2015. https://www.techinasia.com/bitcoin-rebit-philippines-zero-fees-remittances-kyc/

[10] Buenaventura, Luis. "The Bootstrapper's Guide To Bitcoin Remittances." TechCrunch. 30 Ocak 2015. Erişim tarihi 22 Haziran 2015. http://techcrunch.com/2015/01/30/the-bootstrappers-guide-to-bitcoin-remittances/

Bitcoin havalesi alıcı ülkenin mevzuatına uygunluk gerektiriyor. Yerel bankalarla iletişim halinde olan fiziksel ya da dijital varlık kurmak isteyen her hizmet söz konusu ülkenin mevzuatlarına uygun hareket etmek zorunda olsa da, bu şirketler göndericilere sadece Bitcoin bulmak konusunda endişelenmeleri gerektiğini söylüyor. Sonra şirket göndericinin Bitcoin kullandığını bilmesine bile gerek olmadan alıcının o Bitcoin'i yerel para birimine ucuz bir şekilde dönüştürmesini kolaylaştırmaya odaklanabilir. Bu noktada biraz masraf çıkabilir ama en azından bu işlemin sadece bir tarafında olacak. Dolayısıyla, geleneksel sistemlerdeki ücretler ve gecikmeler atlandığı için yine de oldukça hesaplı olabilir.

Bir müşteri Western Union kullanarak para gönderdiğinde, alıcı bu parayı bir Western Union ofisinden almak zorundadır. İki rakip para transfer hizmeti yerine farklı bankaları kullanmakta biraz daha sinerji var. Ancak, yine, bu iki katılımcının da banka hesabı olup olmadığına bağlı ve o zaman bile bankalar aynı ağın (SWIFT, SEPA, vs.) üzerindeyse işe yarar.

Bitcoin ağı gönderici ve alıcının hangi ülkede yaşadıklarını ya da katılımcıların hangi Bitcoin cüzdanını kullandıklarını önemsemez. Bir Gmail hesabından Microsoft Outlook hesabına e-posta göndermekte hiçbir zorluk olmadığı gibi, bir Bitcoin hizmetinden diğerine Bitcoin göndermekte de zorluk yoktur. Bu şirketlerin iletişim kurma sıklığı, aralarında ne kadar mesafe ya da kaç siyasi sınır olduğu önemsizdir.

Tahmin edebileceğiniz gibi, bu insanların Bitcoin'in gelecekteki fiyatından bahsederken konuştukları bir şey.

Eğer Bitcoin o havale piyasasının bir kısmını ele geçirirse, fiyatının önemli ölçüde yükseleceğini düşünüyorlar. Bunda hiç şüphesiz doğruluk payı var ama 60 milyar dolarlık Afrika havale piyasasına bakıp Bitcoin onun yüzde 10'una sahip olursa, piyasa değerinin 6 milyar dolar artacağını düşünmek o kadar kolay değil.

Havalenin arkasında, elbette, alıcılar bitcoin'lerini alır almaz onları bozduracakları varsayımı var. Bu mantıklı; işlem alıcının eline bitcoin değil para iletmek için tasarlandı. Her havale işlemi için bire bir sıçrayışa yakın bir şey olmayacak. Alıcının eline geçen bitcoin'lerin hepsini olmasa da çoğunu yasal paraya dönüştüreceği ve potansiyel olarak ona eş alımın Bitcoin'in toplam piyasa değeri üzerindeki etkisini geçersiz kılacağı neredeyse kesin.

Bu, yatırımcıların kazancını kesinlikle azaltır, o nedenle Bitcoin dev havale piyasasına girerse fiyatında potansiyel bir yükselme olacağı düşüncesiyle bu bölümü salyalarınızı akıtarak okuyorsanız sizi uyarmak isterim. Bitcoin havale işlemlerinin toplamda 1 milyar doları bulması Bitcoin'in piyasa değerini 1 milyar dolar artırmaz. Bu, özellikle de paranın neredeyse geldiği hızla gittiği havale işlemlerinde, konulanın alındığı bir korelasyon değil.

Ancak, bu Bitcoin işlemleri sayısında büyük bir yükselişe sebep olur. Dolayısıyla Bitcoin'e olan talep artar, çünkü yedi gün yirmi dört saat çalışan küresel havale piyasası sürekli takas halinde olduğu için potansiyel olarak daha değerli olacak. Bu piyasalarda daha az Bitcoin olacağı ve dolayısıyla bir fiyat artışı görüleceği anlamına gelir.

Dahası, bir havale aracı olarak Bitcoin'e maruz kalmak Bitcoin'e olan ilgiyi muhtemelen artıracak. Birleşik Dev-

letler'de ya da diğer gelişmiş ülkelerde yaşayan insanların hatırlaması zor olabilir, ama temel banka hizmetlerine erişimi olmayan büyük kitleler var. İki buçuk milyar insanın, ya da dünyadaki yetişkin nüfusunun yarısının, büyük bir bölümünün finansal hizmetleri kullanmadığı ve banka hesabı olmadığı tahmin ediliyor. Bitcoin banka hesabı olmayanlara bu hizmetleri sağlayabilir; üçüncü parti araçlarla banka erişimi olmayanlara şimdiden çok şey sunuyor.[11]

İnsanlar göçmen ailelerinden çift haneli ücretler ödemeden para almaya başladıklarında, bazıları hiç şüphesiz Bitcoin'e ilgi gösterecekler. Bitcoin hakkında daha fazla bilgi edindikçe, onu sadece değer transfer eden bir mekanizma olarak görmek yerine onun değer saklamak için de kullanışlı olduğunu görebilirler.

Her geçen gün, Bitcoin dünyanın her yanındaki insanlar için daha erişilebilir oluyor. Bu kitabı yazdığım sırada, LocalBitcoins.com 244 ülkeye ve 8,000'den fazla şehre ulaştı.[12]

Bütün o piyasalarda onu herkes için yeterli bir havale aracı yapacak kadar likidite –insanların alım-satımı– olmasa da, likiditenin olduğu yerlerle baş etmek için hazır araçlar var.

Bitcoin'in mevcut değişkenliği birikimi elverişsiz yapsa da, Uphold gibi hizmetler kullanıcıların düzinelerce farklı para birimini Bitcoin ekosisteminin sınırları içinde tutmalarına imkân tanıyor. Uphold emtialarını ve dövizle-

[11]"Box 0.1." Global Financial Development Report 2014. N.p.: World Bank, n.d. 3. Print. ISBN: 978-0-8213-9990-3

[12]Localbitcoins.com Statistics. Program documentation. Erişim tarihi 22 Haziran 2015. https://localbitcoins.com/statistics

rini emtia ya da dövizin gerçeğiyle tutuyor, ama her işlem Bitcoin aracılığıyla yapılıyor. Henüz bütün dünyaya açık olmasa da, Uphold ve benzeri hizmetler hızla büyüyor ve bir banka hesabına gerek duymadan gelişmekte olan ülkelerdeki insanların bile, her ne kadar küçük olsa da, birikimlerinin bir kısmını kenara koymalarına olanak tanıyor.

2012 itibarıyla, günde iki dolardan az para kazanan insanların yüzde yetmiş beşini banka hizmetlerinden yararlanamadıkları için bir banka hesabına gerek duymamak büyük bir avantaj.[13] Başlıca sebep yoksulluk. Çok az para kazananların birikim yapması ve asgari hesap gereksinimlerini karşılaşması zor. Bitcoin bu sorunu çözüyor, çünkü bir Bitcoin sekiz ondalık noktaya bölünebilir (0,00000001BTC, 0,00000002BTC, vs.) ve sistem, her ne kadar küçük olsa da, her boyutta işlemi barındırabilir. Dahası, Bitcoin hesaplarının (cüzdanların) asgari miktarı yok.

Bir diğer sebep ise, kırsal kesimde yaşayanların bir bankaya ulaşmak için genellikle çok uzun yol kat etmek zorunda olmalarıdır. Bitcoin sadece cep telefonu ve internet sinyalleriyle sınırlı ve onların erişimindeki alanlar sürekli genişliyor. Banka hizmeti almak için seyahat etmek zorunda kalmamak banka hizmetlerinden mahrum kalanların bu eksiklerini gidermek için oldukça etkili oldu. M-Pesa, Kenya'nın en büyük cep telefonu operatörü Safaricom tarafından kurulan bir mobil bankacılık çözümüdür. Kenya içinde (şehirdeki göçmenlerden kırsaldaki kasabalara) havale yapmak ve Kenya'nın düşük sınıflarına temel bankacılık hizmetleri götürmek için vazgeçilmez oldu.

---

[13] Renzenbrink, Anne. "World Bank: 75 Percent of Poor Don't Have Bank Accounts." CNN. 19 Nisan 2011. Erişim tarihi 22 Haziran 2015. http://www.cnn.com/2012/04/19/business/ poor-bank-accounts/index.html

M-Pesa kripto para gibi değil; merkezi ve kendi para biriminde hareket etmek yerine yasal paraların dengelerini takip ediyor. PayPal AT&T tarafından yaratılmış ve sadece cep telefonlarında var olmuş olsaydı ve ülkenin her yanında hesabınızdan para çekebileceğiniz ya da faturalarınızı ödeyebileceğiniz döviz büroları olsaydı, onun gibi olurdu.

Bu nüfuz Bitcoin havale şirketleri tarafından M-Pesa'nın başarısından faydalanma çabalarına ve onu Kenya'da Bitcoin havalesinin son aşaması olarak kullanmalarına sebep oldu. Hem igot hem de BitPesa M-Pesa'yla birleştiler ve yurtiçi havalede sundukları avantajları uluslararası olacak şekilde genişlettiler. İnsanlar bu ülkelerdeki ailelerine cep telefonlarını kullanarak Bitcoin gönderebilirler; alıcılar da kendi telefonlarını kullanarak parayı M-Pesa parasına dönüştürüp daha sonra normalde olduğu gibi yasal paraya çevirebilirler.[14] [15]

Bitcoin'in spekülatif işlemler ve karaborsa, 'gri borsa' ürünleri satın alımı dışında da kullanım alanlarına ihtiyacı var. Kullanım alanları aynı zamanda Bitcoin'in yasal para seçeneklerinden daha iyi yaptığı şeyleri içermeli. Havale bariz bir aday. Yasal para birimlerinin yaptığı şeyleri daha hesaplı ve hızlı yapabilir. Aynı zamanda, küçük ya da oldukça büyük miktarda para yollamak ya da daha önce

[14] Torpey, Kyle. "Bitcoin Exchange Igot Launches in Kenya via M-Pesa Integration." Inside Bitcoins. 25 Şubat 2015. Erişim tarihi 22 Haziran 2015. http://insidebitcoins.com/news/bitcoin-exchange-igot-launches-in-kenya-via-m-pesa-integration/30194

[15] Vigna, Paul. "Kenya's BitPesa Launches Beta Test of Remittance Service." MoneyBeat RSS. 23 Mayıs 2014. Erişim tarihi 22 Haziran 2015. http://blogs.wsj.com/moneybeat/2014/05/23/kenyas-bitpesa-launches-beta-test-of-remittance-service/

bankacılık hizmetlerinden yararlanamayan kişilere ileri düzeyde yatırım hizmetleri sağlamak gibi müşterilerin geleneksel hizmetler kullanarak yapmalarının mümkün olmadığı işleri yapabilir.

Ayrıca, dünyayı değiştirme potansiyeline sahip bir şey. Zengin ülkelerden alınan yardımlardan ziyade havale ekonomisi gelişmekte olan ülkeler için çok daha önemli bir kurtarıcı haline geldi. Bir avuç şirket milyonları ceplerine indirirken hem gelişmiş hem de gelişmekte olan ülkelerin paralarını ekonomiden çekiyor. Bu şirketleri süreçten uzaklaştırmak bütün ülkelerin ekonomisi için faydalı olur ama en büyük fayda ciddi ölçüde göçmenlerin havalelerine bel bağlayan gelişmekte olan ülkelerin ekonomilerine olacak.

Bitcoin dünyayı değiştirebilir mi? Havale yoluyla ellerine geçen paraya muhtaç insanların hayatlarını değiştirme potansiyeline sahip. Ve bir kez insanların hayatını değiştirmeye başladığınızda, dünyayı değiştirmeye başlarsınız.

On Dokuzuncu Bölüm:

Mikro İşlemler

İnternet halkın kullanımına ilk açıldığında, insanların birbirlerine benzemekten kurtulmalarına yarayacak, tutku, yaratıcılık, yenilik ve bilgi özgürlüğünün hükmettiği, değişken bir dünya olduğunu düşündürerek sevinç yarattı. Önce reklamcılık ve sonra ticaret tarafından gasp edildiğindeyse teslim olmuş, insan açgözlülüğü ve hırsıyla hizaya getirilmiş bir havadaydı artık.

— Neil Strauss, yazar ve gazeteci

Mikro işlemler birkaç sent ila beş dolar arasında değişen işlemlerdir. Bir zamanlar internet ekonomisinin kurtarıcısı olan ama dotcom balonu sırasında sürdürülebilir gelir getirmeyi başaramayan reklamcılık dalaverelerinin yerini alabilecek, mantıklı bir seçenek olarak görüldüler. Düşünceye göre –bu hâlâ geçerli– sitenin ziyaretçileri her ziyaret ya da üyelik için küçük miktarlar ödeyerek siteleri finanse edeceklerdi. Mikro işlemlerin insanlara çevrimiçi içeriğe doğrudan ödeme yapmaları için bir yol sunacağı ve

reklamcıları televizyon, radyo ve reklam panolarının dünyasına geri dönmeye zorlayacağı düşünüldü.

Elbette, buna herkes inanamadı ve internetteki reklamcılık en sonunda, sürdürülebilir değilse bile, mevcut dünyamızda en azından uygulanabilir bir modele dönüştü.

Mikro işlemler henüz reklamcılığın yerini almasa da, internet ekonomisinin büyük bir parçası oldular. Şu anda, başlıca video oyunları şirketleri tarafından kullanıcılara video oyunlarının içindeki ürünleri satmak için kullanılıyorlar. Ancak, Bitcoin eski sistem kullanıldığında oluşan ücretleri ortadan kaldırarak mikro işlemleri kolaylaştırma potansiyeline sahip. Eski sistemle gerçekleştirilen mikro işlemler genellikle etkisizdir, çünkü yarısı ya da daha fazlası aracı ve ücretlerle kesilir. Şirketlerin bu ücretleri önemli biçimde azaltmak için anlaşmalar yaptığı nadir durumlarda bile, alıcının (ya da göndericinin) bankasının kendi komisyonunu almamasına bağımlıdırlar.

Mikro işlemlerin çok büyük bir potansiyeli var. Bir kişinin diğerinden bir şey satın aldığı geleneksel ticarette, tek belirleyici faktör alıcının ürüne biçtiği paha ve satıcının o ürünü elinden çıkarmak için talep ettiği asgari fiyattır. Ekonomiler büyüdüğünde milyonlarca insan aynı şeyleri istemeye başlar ve işler karmaşıklaşır. Geniş bir ekonomide bir malın –örneğin bir müzik albümünün– fiyatı sadece alıcının ne kadar ödemek istediğine ya da satıcının ne kadara satmak istediğine bağlı değildir; dağıtım, pazarlama, yasal masraflar, gönderi ücretleri gibi unsurlar da belirleyicidir. Bir sanatçı albümünü beş dolara satmaya razı olabilir ama gerçekten beş dolar kazanmak istiyorsa, ondan çok daha fazlasına satmak zorundadır.

İnternet bu duvarların çoğunu yıktı. Tower Records'un insanların almayı isteyebileceği bütün albümleri kataloğunda bulundurmasına ihtiyacımız yok. CD'lerin basımı ya da tanıtımı için Sony'nin para ödemesine ihtiyacımız yok. Günümüzde yapılması gereken tek şey bir sanatçının albümünü internetten sunması ve insanların ona neredeyse doğrudan ödeme yapmasıdır. Plak şirketleri ve müzik mağazaları bu denklemden kesildiler. Günümüzde daha önce hiç olmadığı kadar düşük maliyetli müziğe erişebiliyoruz. Mikro işlemlerin önemi bu: Satıcılara ürünlerini gerçekten satmak istedikleri fiyattan listelemelerine imkân tanıyor. Ürünlerin zahmetsizce kopyalanabildiği ve satıcının bir ürünü satmak için onu 'elinden çıkarmasına' gerek olmayan dijital dünyada bu ücret son derece küçük olabilir.

Günümüzde, bir sanatçı müziğini kendi web sitesine koyarsa ve onu beş dolara satın alırsam, o beş dolardan pay alan tek aracı kredi kartı şirketi ya da komisyonunu alan bankadır. Bu, otuz sent ya da bir dolar olabilir. Kastettiğim şey eğer saf dışı edilirse daha fazlası üretilip tüketilebilir.

Bitcoin bu zorlu görevi karşılaması için eşsiz olarak tasarlandı. O küresel, hızlı ve oldukça düşük işlem ücretlerine sahip, bu nedenle birkaç sent ve hatta bir sentin çok küçük bir bölümünü göndermek bile sorun değil. PayPal ve Apple Pay de dahil olmak üzere başka hiçbir hizmet bu üç şeyi bünyesinde bulundurduğunu iddia edemez. Bir mikro işlem şirketinin başarılı olabilmesi için bu üç özellik gereklidir.

Bitcoin mikro işlemleri tamamen bir eşler arası hizmet olarak başladı ve öyle kalabilir. Daha önce de birçok kez

söylediğim gibi, herkes dilediği miktarda Bitcoin gönderebilir. Dünyanın diğer ucundaki birine iki sent değerinde Bitcoin gönderebilirim ve o kişi bana karşılığında yirmi yen değerinde Bitcoin gönderebilir. Eski sistemleri kullanan hizmetlerde sık sık olduğu gibi, işlem ücretlerini düşürmek için mikro işlemleri gruplandıran merkezi bir hizmete gerek yok. Bitcoin kullanırken işlem ücretleri zaten yeterince düşük.

Her mikro işlem müzik albümü gibi ürünler satmak için kullanılmaz. Genellikle bir şeyin takdir edildiğini göstermek için kullanılırlar. Reddit ve Twitter gibi sosyal ağlarda, insanlar beğendikleri yazılar ya da icat ettikleri sebep her neyse birbirlerine Bitcoin'le bahşiş vererek ödüllendirirler.

Bu işlemleri bir arada gruplandırmak zor olur, çünkü genellikle farklı insanlardan gelir ve farklı insanlara giderler ve bu kesik kesiktir. Kullandıkları banka ve kredi kartı şirketlerinin farklı kombinasyonları ve insanların bahşişlerine hemen erişebilmeyi istedikleri düşünüldüğünde, onları bir araya toplamak neredeyse imkânsızdır. Eğer biri bir yaratıcıya yarattığı resmi beğendiği için $0,20 bahşiş vermek istiyor ama bankanın $0,19'unu alacağını biliyorsa, o kişinin parasını harcamaya daha az istekli olması mantıklıdır.

Bitcoin ile gönderdiğiniz miktar alıcıya ulaşan miktardır. Bitcoin cüzdanları kullanarak insanlar kullanıcılara ve hizmetlere herhangi bir şeye para öder gibi bahşiş verebilirler. Bu işlemi kolaylaştırmak için birkaç hizmet oluşturuldu.

ChangeTip uygulanabilir ilk hizmetti ve hâlâ en popü-

lerlerinden biri. ChangeTip bünyesinde Twitter, Reddit, Facebook, GitHub, YouTube ve yaklaşık bir düzine daha fazlası da dahil olmak üzere sayıları giderek artan sosyal medya ve içerik yaratma siteleri barındırıyor. ChangeTip'le, kullanıcılar yasal para ya da Bitcoin'le belirtilen miktarda parayı desteklenen bir siteden başka birine ücretsiz olarak gönderebilirler. ChangeTip alıcıyı bahşiş aldığı konusunda uyarır. Alıcının daha sonra bahşişi alabilmesi için üye olması gerekir. Bahşiş kabul edildikten sonra, ChangeTip'te saklanabilir ya da kullanıcının Bitcoin cüzdanına ya da bir hediye çekine aktarılabilir.

ChangeTip kolay ve kullanışlı bir hizmet ama şirketin sosyal medya sitelerinden topladığı bilgileri satabileceğinden korkan bazıları gizlilikle ilgili endişelerini dile getirdi. Şu anki yönetim kurulu başkanı Nick Sullivan bunu asla yapmayacağına söz verdi[1] ama ChangeTip eleştirmenleri şirketin satılması durumunda olabilecekler hakkında hâlâ endişeliler. Birkaç yorumcunun dikkat çektiği gibi, veri satmadan ChangeTip'in kâr potansiyeli oldukça düşük.[2] Ama o zamandan bu yana hediye çeki seçeneği gibi yeni gelir kaynakları eklendi.

Bazı Bitcoin kullanıcılarının kuruntularına rağmen, ChangeTip Bitcoin'in benimsenmesinde oldukça etkili oldu. Birine ChangeTip aracılığıyla Bitcoin vermek onların Bitcoin hakkında herhangi bir şey bilmelerini gerek-

---

[1]Rizzo, Pete. "ChangeTip CEO Nick Sullivan: We Won't Sell User Data." CoinDesk. 18 Aralık 2014. Erişim tarihi 22 Haziran 2015. http://www.coindesk.com/changetip-ceo-nick-sullivan-wont-sell-user-data/

[2]Sirer, Emin Gün. "Tips for ChangeTip." Tips for ChangeTip. 29 Aralık 2014. Erişim tarihi 22 Haziran 2015. http://hackingdistributed.com/2014/12/29/tips-for-changetip/?v=01

tirmiyor. Ama o Bitcoin'i ChangeTip hesaplarından alıp yasal paraya dönüştürmek istediklerinden cüzdanlar, özel anahtarlar ve Bitcoin ekosisteminin farklı yanlarını öğrenmeye başlıyorlar.

ChangeTip kullanıcıların en sevdikleri içerik yaratıcısına katkıda bulunmalarını sağlayan tek hizmet değil. Bir başka hizmet, ProTip, Christopher Ellis tarafından yaratıldı ve Kickstarter'da kitleler tarafından finanse edildi.

Bitcoin bağışlarını kabul etmeyi bir web sitesinde herhangi bir yere Bitcoin adresi koymak kadar kolay yapmayı amaçlıyor.

Bu, faydalı bir hedef, çünkü ChangeTip'in sorunlarından biri içerik yaratıcılarının dahil olmalarının kolay olmaması. ChangeTip, Reddit ya da Twitter gibi, kullanıcı için her şeyin düşünüldüğü ortamlarda en yüksek verimi sağlıyor. Ama web siteleri ya da YouTube kanalları için işler daha zor olmaya başladı. Web sitesi yaratıcılarının biraz kod girmeleri gerekiyor. Çok değil ama bu, birçok web sitesi sahibinin uğraşmak istemediği bir sorun.

Süreç şu anda olması gerektiği kadar kolay değil ve içerik yaratıcısı tarafından biraz çaba harcamayı gerektiriyor. ProTip web sitesi yaratıcısının özel bir çaba harcamasını gerektirmiyor. Eğer bir sitede bir Bitcoin adresi varsa, ProTip onu bulup izini sürüyor (buna birazdan değineceğim). Web sitesi yaratıcıları bir ProTip komut dizisi ekliyorlar (ve ProTip'in gelecek versiyonları üyelikler ve ödeme duvarları gibi özelliklere olanak sağlayacak) ama onların da ProTip'i kullanmalarına gerek yok.

Bağışçıların bu hizmeti kullanabilmeleri için, ProTip kullanıcının tarayıcısına bir uzantı yükleyecek, otomatik

olarak Bitcoin adresleri olan web sitelerini tarayıp onları bir haftalığına kaydedecek. O hafta boyunca, Bitcoin adresleri olan en çok ziyaret edilen beş site (ya da kullanıcı kaç site belirlerse) haftanın başında kullanıcının kenara ayırdığı Bitcoin'in bir kısmını alacak. Eğer bir sayfada üç adresten fazlası varsa, ProTip bulduğu ilk üçü seçecek. Aynı zamanda, kullanıcılar web sitelerini ve bazı adresleri 'kara listeye' alabilirler. Böylece Twitter'da postalanan gelişigüzel adresler ya da insanların mesajlarının imza kısmındaki adresler göz ardı edilebilir, tabi kullanıcının yapmak istediği buysa.

Her hafta bir bütçe belirlenir; kullanıcı bağışın otomatik olarak ya da alıcılara göz gezdirdikten sonra yapılmasına karar verebilir. Kullanıcıya zorluk çıkarmayan, 'finanse et ve bırak' tarzı bir program olmayı hedefliyor.

İçerik yaratıcıları Bitcoin adreslerini sitelerinde diledikleri yere koyabilirler ve ProTip onları belirleyip hatırlar.

Bitcoin icat edilmeden önce bu bağış modelinin internetteki başarısı tartışmalıydı. Sadık hayran kitlesi olan popüler sesli yayınlar ve YouTube kanalları ayakta durmayı başardılar, hatta dinleyicilerinin iyiliği sayesinde büyüdüler, ama çok azı reklam modelini tamamen kenara itebildi.

Ancak, potansiyel bağışçıların da önünde çok sayıda engel var. Öncelikle, bağış yapabilmek için çok uğraşmaları gerekiyor, bu PayPal ya da benzer bir hizmete üye olmayı ve neredeyse birkaç web sayfasına tıklamayı gerektiren bir süreç. İkincisi, küçük miktarda bağışlar yasal para birimleri için makul değil. $0,25 ya da daha az miktarda bir düzine bağış yapmak kullanışlı değil. Alıcıyla aynı ülkede yaşadığınızı ve PayPal'a o kişinin bir arkadaşınız olduğunu

söylediğinizi varsayarsak, bunu PayPal aracılığıyla yapabilirsiniz, yoksa PayPal'ın komisyonu çok fazla olacağı için bağış yapmaya değmeyebilir.

ProTip ve Bitcoin, birlikte, bağışları otomatik yaparak bu engelleri ortadan kaldırıp gerçek mikro bağışlara, bir sentin altında olanlara bile, olanak tanıyorlar.

İnsanların uygulanabilir mikro işlemlere nasıl tepki göstereceklerini bilmiyoruz. Bu, yıllardır internetteki içerik yaratılışını finanse etmek için önerilen bir çözümdü ama henüz popüler olmadı. Reklamcılığın içerik yaratıcılarına ayırabileceği çok fazla parası var ve içerik tüketicileri o içeriğe ücretsiz ulaşmaya alıştılar. Sık sık aldatıcı görülen reklamcılığa aşırı bel bağlamak, Chris Ellis'in içeriği doğrudan finanse etmeyi sağlayan ProTip'i yaratmasının arkasındaki asıl sebepti:

> Benim gibi insanların para kazanmalarına ve tekrar video hazırlamaya başlamama yardım edecek bir uygulama yapabilmek için içerik oluşturmaya ara verdim.
>
> Dürüstlüğün fayda sağlamasını istiyorum, çünkü Satoshi orijinal tanıtım yazısında bunu sergiledi. Bitcoin'in orijinal kapsamında olan bir proje üzerinde çalışmak istedim.
>
> Dürüstlüğün sahtekârlıktan daha fazla fayda sağladığı bir araç geliştirirsek ne olur? Sanatçılara, yazarlara, video grafikerlere izleyici kitleleriyle bağlantı kurmaları için 'Beğen' düğmelerinden daha anlamlı bir şekilde ihtiyaç duydukları araçları verebiliriz.

Taylor Swift'e Twitter'da yazılan cevaplara bakın. Çoğunda hayranları, "Aman Tanrım beni takip et," diyorlar. İnsanlar bağlantı, deneyim ve yeni bir şeyin şaşkınlığını istiyorlar. Taylor yetenekli ama aynı zamanda şanslıydı ve bu birçok sanatçı için geçerli değil.

Çok satmayanlar doğru şeyi yapıp yapmadıklarını ya da yeterince iyi olup olmadıklarını sorgulayarak eziyet dolu bir hayat yaşıyorlar.

Çok satanlar pazarlama ve halkla ilişkilere yöneliyorlar. Bu insanların karar verme biçimini manipüle etmek için tasarlanmış bir endüstridir.[3]

Reklamcılıktan uzaklaşarak bağımsız basını destekleyebiliriz. Reklamcılık basın kuruluşlarını önemli haberleri göz ardı etmeye ikna ediyor ve bize onların ürünleri olmadan yetersiz olduğumuzu hissettirip ticari propagandayla sanatı yozlaştırıyor. Bir zamanlar insanların internetin bu kaderden kaçınacağını umdular; ama kaçınamadı. Sadece kısmen makul bir alternatif önerildi: bahşiş ekonomisini besleyen mikro işlemler.

Bağış temelli bir ekonominin uygulanabilir olduğunu kimse garanti edemez, ama Bitcoin başarılı olması için ona elinden geldiğince şans veriyor.

---

[3]DeMartino, Ian M. "Interview With ProTip's Chris Ellis On Saving Media." CoinTelegraph. 19 Mart 2015. Erişim tarihi 22 Haziran 2015. http://cointelegraph.com/ news/113741/interview-with-protips-chris-ellis-on-saving-media

Yirminci Bölüm:

Başlangıç Fonu

Eğer bir fikriniz varsa, bugün başlayın. Başlamak için bundan daha iyi bir zaman olamaz. Bu, işinizi bırakıp aklınızdaki fikre ilk günden itibaren yüzde yüz atılmanız anlamına gelmiyor, ama harekete geçmek için her zaman küçük ilerlemeler kaydedilebilir.

— Kevin Systrom, Instagram'ın kurucu ortağı

Bitcoin'deki en ilginç gelişmelerden biri başlangıç fonuydu. Kitlesel fonlama dünyayı kasıp kavurdu. Bu başarı hikâyeleri ve endüstri yaratan devlerle dolu. En sonunda iki milyar dolara Facebook tarafından satın alınan ve tek başına sanal gerçeklik endüstrisini canlandıran Oculus'ta Kickstarter'da başladı. Aynı şekilde, akıllı saat şirketi Pebble o kadar başarılıydı ki, LG'den Samsung'a, Google'dan Apple'a kadar birçok şirket endüstriye girdi.

Bir de eşitliğe dayalı kitlesel fonlama var, normal kitlesel fonlama gibi, ancak fon sağlayıcılar bir ürün ya da tipik kitlesel fonlama kampanyalarındaki ödüllerden biri

yerine şirketin hisselerini alıyorlar. Sıkı mevzuatlar nedeniyle Birleşik Devletler'de uygulanabilir olmasa da, başka yerlerdeki şirketler şirketin bölümlerini kitlesel fonlamaya katılanlara satarak projelerini ve şirketlerini finanse ediyorlar. Esasında, bu kitlesel fonlanmış yatırım sermayesidir. Oculus Rift hızla demode olan gelişim kitleri yerine kendisini destekleyenlere eşitlik sunmuş olsaydı, fonlayıcıları yüklü miktarda para kazanmış olacaklardı. (Oculus daha sonra sanal gerçeklik gözlüğü piyasaya sürüldüğünde onları en başından beri destekleyenlere tüketici versiyonunun verileceğini açıkladı.) Birkaç kez bahsettiğim Uphold eşitliğe dayanan bir kampanya yürüttü ve Birleşik Devletler'deki müşterilere açılmadan 9 milyon dolardan fazla para topladı.[1]

Ama bunlar yasal para dünyasının çözümleri. Kripto para dünyasında, işletmeleri finanse etmenin daha doğrudan bir yolu var: blok zincirinde dağıtılan varlık token'ları. Varlık token'ları, bir şirketin hisseleri gibi, blok zinciri üzerinden gönderilebilen Bitcoin dışında bir şeyin sahipliğini temsil eden token'lardır. Potansiyel yatırımcıların ve yeni kurulan şirketlerin sahiplerinin bu alanın şu anda sahtekârlıklar ve saadet zincirleriyle dolu olduğunu unutmamaları gerekir.

Bu sürpriz olmamalı. Kripto para kullanarak eşitlik fonlaması yeni ve henüz tam olarak anlaşılmamış doğru düzgün denetimi olmayan bir teknoloji. Birkaçı hariç şim-

[1]Parsa, Tim. "Series B Closes with $9.6M Raised via Crowdcube and Venovate." Bitreserve. 13 Ocak 2015. Erişim tarihi 22 Haziran 2015. https://bitreserve.org/en/blog/posts/bitreserve/series-b-closes-with-9-6m-raised-via-crowdcube-and-venovate

diye kadar finanse edilen işletmelerin hepsi gelir kaynağı belirsiz kripto para temelli işletmelerdir.

Ama mevcut durum meşru işletmeler için ciddi bir fırsat. Kripto finansçılar, ağı dolduran sahtekârlardan ve dalaverelerden bıktılar. Eğer meşru bir işletme sahibiyseniz –bir pizza restoranınızın olduğunu ve bunu kanıtlamak için resimler yayınladığınızı varsayalım– restoran üzerindeki hakkınızın bir kısmından (örneğin yüzde beşinden) ikinci bir restoran açmak için yeterli para toplamak umuduyla vazgeçebilirsiniz. Elde ettiğiniz token'ların şirketinizin yüzde beşini temsil ettiğini belirten bir sözleşme ya da bir tür yasal doküman oluşturduktan sonra onları piyasaya koyabilirsiniz. Yatırımcılar iş planınızı değerlendirebilir ve yatırım yapmak isteyip istemediklerine karar verdikten sonra token'larınızın bir kısmını sizden satın alabilirler. Yatırımcılara kâr payı vererek ya da onlara gelecekteki mekânlar hakkında oy hakkı vererek ödeme yapabilirsiniz ve yatırımcılar diledikleri zaman token'ları serbest piyasada satabilirler.

Ama aceleci davranıyorum. Şirketinizi ya da ürününüzü kripto para birimleriyle finanse etmeden önce hangi hizmetlerin mevcut olduğunu ve benzer projelerin ne kadar başarılı olduğunu bilmelisiniz.

Şirketinizin mülkiyetinin küçük bir kısmını temsil eden kendi token'ınızı çıkarmak için kullanabileceğiniz dört büyük platform var: Counterparty, Omni/Mastercoin, Ethereum ve Nxt. Başkaları da var ama ya hâlâ gelişim aşamasındalar ya da küçük bir topluluğun parçası oldukları için potansiyel yatırımcı sayınızı sınırlandırabilirler.

Counterparty Bitcoin blok zinciri üzerine kuruldu, o

nedenle potansiyel yatırımcı havuzunuz Bitcoin kullanan herkesi içeriyor. Öte yandan, Nxt'in kendi teknolojisi ve Bitcoin'inkinden oldukça küçük bir topluluğu var. Ancak, Nxt'in varlık borsası –token piyasasına verilen isim– çekirdek istemcisine kuruluyken, Counterparty özel bir cüzdan gerektiriyor. Temelde, Counterparty Bitcoin topluluğunun bir altkümesine erişmenize izin verip geri kalanına potansiyel erişim sunarken, Nxt en başından itibaren, küçük olmasına rağmen, bütün topluluğuna erişmenize izin veriyor.

Omni/Mastercoin blok zinciri üzerine kurulu bir platform. Diğer kripto para 2.0 projelerinde olduğu gibi, yaratmaya, satmaya ve varlık takasına imkân tanıyor.

Ethereum kısa bir süre önce piyasaya sürüldü ve her geçen gün popülerleşiyor. O da bir işletmeyi finanse etmek için kullanılabilir ama buna ek olarak ilginç projeler yaratmak için bünyesinde ekstra programlama barındırıyor. Ancak, bunun tecrübeli kişilere bırakılması en iyisi.

Alıcılara bir tür ödül sunan bir varlığı piyasaya sürmek esasında her platformda aynı şekilde işliyor. Pizza restoranı örneğine geri dönelim. Buradaki ödül toplam kârınızın yüzde beşi, toplam kripto para satışının yüzde yirmi beşi, ya da restoranda bozdurulan her token için 'ücretsiz' bir dilim pizza olabilir. Varlık tipini, kaç tane olduğunu, daha fazla yaratıp yaratamayacağınızı ve bölünebilir olup olmadığını seçebilirsiniz. Onu bölünebilir yapmanızı şiddetle öneririm; bölünemeyen varlıkları serbest piyasada alıp satmak daha zor ve o nedenle bazı yatırımcıları caydırması mümkün.

Sonra, bir iş planı oluşturup parayı nasıl kullanmayı

düşündüğünüzü, varlığınızı neden piyasaya sürdüğünüzü ve yatırımcılarınızı nasıl ödüllendirmeyi beklediğinizi açıklamalısınız. İşletmenizin olduğunu ve kitlesel fonlama kampanyasını gerçekten sizin yürüttüğünüzü kanıtlayan bir web sitesi hazırlamanızın işiniz için faydası olabilir.

Ardından, birkaç duyuru yapın: biri kullandığınız platformun mesaj panosunda, biri onun Reddit sayfasında ve biri de kullandığınız platforma bağlı olarak ya NXTforum ya da BitcoinTalk'ta.

Bu şekilde para toplamaktan daha fazlasını yapabilirsiniz. Aynı zamanda, yatırımcılarınızın –ve muhtemelen en sadık müşterilerinizin– istediği bir sonraki şeyi öğrenebilirsiniz. İlk pizza restoranı kampanyanızın çok ilgi gördüğünü ve ikinci restoranın da aynı şekilde iyi durumda olduğunu varsayalım. Hatta işler o kadar iyi gidiyor ki, başka bir yere üçüncü restoranı açmayı düşünüyorsunuz.

Ama üçüncü bir mekân eklemek çok masraflı olacak, o nedenle siz kâra geçene kadar yatırımcılarınız kâr paylarını alamayacaklar. Öte yandan, planınıza uyarlarsa, üçüncü bir restoranın kârlarını fazlasıyla artırma şansı var. Token/hisse sahiplerinin bu konuda oy vermelerine izin verebilirsiniz.

Daha neşeli bir örnek olarak, token sahiplerinin restoranınızda yer alan bir sonraki 'ayın pizzası'nı seçmesine izin verebilirsiniz. Haftalık ya da aylık kampanyalar gibi şeylerde oy kullanmak basit kâr payı olasılıklarının ardındaki büyük teşviklerdir. Bu da Birleşik Devletler güvenlik yönetmeliğiyle ters düşmeden bağış toplamanın bir başka yoludur.

Kitlesel fonlama platformları müşterilerinizi dahil et-

mek için oylama seçeneklerini bünyelerinde bulundururlar. Nxt en sınırsız özelliklere sahip oylama mekanizmasına sahip. Yüklü miktarda yatırım yapan insanlara daha fazla ağırlık vermek ya da hisse oranına bakılmaksızın her adrese eşit oy hakkı vermek gibi oyu düzene sokan farklı kurallar belirleyebilirsiniz.

Counterparty'yle oy vermek pek ideal değil ama yine de mümkün. Token'ınıza 'PİZZA' adını verdiğinizi ve 100 PİZZA token'ı sahibi olduğunu varsayalım. 'PİZZAOYU' adı verilen yeni bir token piyasaya sürüp onu 'PİZZA' sahiplerine kâr payı olarak dağıtın. Daha sonra, her biri farklı bir oyu temsil eden coin'lerin gönderilebileceği birkaç Bitcoin adresi belirleyin. Token sahipleri oy token'larını vermeyi istedikleri oyu temsil eden adreslere gönderirler; oyları toplar ve çıkan sonuca bağlı olarak kararınızı verirsiniz (ama unutmayın, sonuçları herkes görebilecek).

Kontrolsüz bir piyasaya, özellikle de Birleşik Devletler'de faaliyet gösteren işletmeler için, kâr payı üreten varlık sürmenin yasallığı hakkında endişeler olduğu unutulmamalıdır. Bu birçok coin topluluğunun pazarlama materyallerinde 'varlık' ve 'kâr payı' sözcüklerinden itinayla kaçınmalarına neden oldu, sanki Güvenlik ve Borsa Komisyonu (SEC) kapılarını çalarsa bu onları koruyabilirmiş gibi. Bana kalırsa, SEC buna verdiğiniz ismi önemsemiyor; bence onu yatırımcıları aldatmak için kullanıp kullanmadığınızı önemsiyorlar. Kripto topluluğuna yasal olarak tutamayacağınız herhangi bir taahhütte bulunmadan önce bir avukata danışmanızı tavsiye etsem de, yasal işletmelerin şeffaf ve açık bir şekilde bağış toplamalarının SEC'i çok fazla endişelendireceğini sanmıyorum, özellikle

de birçok yasadışı işletmenin aynı şeyi yaptığı düşünülürse. Ancak, şirketinizin mülkiyetini hisse ya da emtia olarak satmanız kesinlikle yasadışıdır. Birleşik Devletler'deki işletme sahipleri için oy verme hakkı sunmak uygulanabilir bir seçenektir.

Bir diğer seçenek ise, Kickstarter'a benzer ödüller vermek. SEC 'token' sahiplerine ücretsiz pizza, ya da sattığınız ürün her neyse, vermenizi umursamaz.

Bitcoin'e verilen çok sayıda isimden biri 'programlanabilir paradır' ve bu Bitcoin ve diğer kripto paraların kritik özelliğini tanımlıyor. Onlara genellikle 'internetin para birimi' deniyor. Bu bir ülkenin kendi para birimi olduğunu söylememizden daha derin bir anlam taşıyor. İnternet tamamen dijital; hiçbir yerde mevcut değil ama aynı zamanda her yerde. Dolar, avro ve yuanı oldukça belirli koridorlarda zorluyoruz. Bitcoin sadece bu engelleri yıkmakla kalmıyor, aynı zamanda neredeyse hayal edilebilir her kullanım alanı için uygun hale getirilebilir. Blok zinciri her şeyin adil olmasını sağlıyor ve tek sınır programcının hayal gücü ve becerisidir.

Bitcoin iş kurmanıza ve yeni iş modelleri yaratmanıza yardımcı olabilir. Ve tıpkı internetin birkaç bin sadık hayranın bağışlarıyla küçük sanatçıların ayakta kalmasına imkân tanıdığı gibi, kripto paralar da kendini idame ettiren mini ekosistemler yaratma potansiyeline sahip. İşletmeler için bağış toplamak kripto para birimlerinin kolaylaştırabileceği şeylerden sadece biri ve gerçekten de bazı işletmeler onlar olmadan varlığını sürdüremez.

DÖRDÜNCÜ KISIM
Bitcoin'in Geleceği

Yirmi Birinci Bölüm:

Aitcoin'ler ve Bitcoin 2.0 Projeleri

Milyonlarca altcoin'imiz olacak.

— Andreas Antonopoulos, Nisan 2014

Şimdiye kadar Bitcoin'den, geçmişinden, kullanım alanlarından ve tekniğinden bahsettim. Ama Bitcoin var olan tek dijital para değil. O kullanılabilir ve hiç şüphesiz en başarılı ilk dijital para birimi olsa da, her gün yüzlercesi takas edilen bini aşkın dijital para birimi mevcut. Ve en azından birkaçı başarılı bir gelecek şansına sahip olacak gibi görünüyor.

Dijital devrimin başarılı olup olmayacağından ya da Bitcoin'in değerini artıracak şekilde gelişme göstereceğinden kimse emin olmadığı için Bitcoin riskli bir yatırımdır. Bir altcoin'e, herhangi birine, yatırım yapmak en az iki kat daha risklidir. Yatırımcı dijital para birimi devriminin bir bütün olarak başarılı olacağına bahse girer. Ama sadece

Bitcoin'in değil, seçtiği altcoin'in değerini de artıracak *kadar* başarılı olacağına bahse giriyordur.

Her spekülatif yatırımda geçerli olduğu gibi, yatırım yapmak her zaman inanmakla aynı şey değildir. Günlük işlemlerden de para kazanılabilir. Ancak, farklı coin'leri uzun vadeli ellerinde tutanlar, coin geliştiriciler ve serbest piyasacıların diğer altcoin'lerin denizinde batmayacaklarına ve insanların Bitcoin yerine tercih edeceği yeterince benzersiz özellikler sunacakları üzerine bahse girerler.

Bitcoin popülerleştikçe, farklı geliştiriciler göz kamaştırıcı yükselişini kendi para birimleriyle taklit edip edemeyeceklerini görmek istediler. 2011'de, Namecoin Bitcoin'e ilk alternatif olarak piyasaya sürüldü. .bit ismi için merkezi olmayan kaydı getirdi ve blok zincirinde rahatlıkla veri saklanmasına imkân tanıdı. (Genellikle, bir web sitesini kaydettirirken, ICANN denen bir organizasyona başvurur ya da ICANN'a başvuran GoDaddy.com gibi bir şirketten faydalanırsınız ve o sunucunuzun IP adresini bir alan adı sisteminde (DNS) URL'nizle birleştirir. Bir kripto para olmanın yanı sıra, Namecoin blok zincirinde çalışan ve ICANN ya da diğer düzenleyici kuruluşlara bağlı olmayan, yaygın, merkezsizleşmiş bir DNS'dir.) O zamandan beri, çoğu başarılı coin'lerin neredeyse değersiz kopyaları olan binlerce coin piyasaya sürüldü. Çok azı Namecoin'in 2011'de masaya getirdiği yeniliğe sahipti.

Geliştirilebilir olmak için çok fazla altcoin var. Genel tavsiyem, bıçak ağzında olmakla gerçekten ilgilenmiyorsanız, altcoin'lerin hepsinden uzak durmanız yönündedir. Birçok kişi, önümüzdeki birkaç sene içinde altcoin'ler için büyük bir kan kaybı olacağını öngörüyor. Çoğu sadece

spekülatif alım-satımlar ve 'şişir ve boşalt' taktikleri sayesinde ayakta tutuluyor. Uzun vadede hiçbir faydaları yok ve bu nedenle hayatta kalma ihtimalleri düşük.

Altcoin'lerin sorunu onları yaratmanın çok kolay olmasıdır. Ars Technica bu konu hakkında bir makale yayınladı. Yazarı, Cyrus Farivar, sürecin basitliğine dikkat çekmek için bir coin yaratıp piyasaya sürdü. Artık kullanılmayan bir hizmet olan Coingen.io'yu kullandı. 0.2BTC'ye Arscoin adında bir ısmarlama Scrypt coin yaratmayı başardı.[1] (Scrypt kripto para birimleri için popüler bir algoritmadır.) Farivar şöyle yazıyor:

> Ödemeyi yapıp bekledik. İşlem sadece birkaç dakika sürdü. En sonunda, GUI ve kaynak koduyla birlikte Windows ve Linux uygulamalarını hazırladık ve Arscoin doğdu. Artık tek yapmamız gereken birkaç coin çıkarmak ve onları harcamanın bir yolunu bulmaktı.

Kaynak kodunu derlemek ve piyasaya bir yazılım sürmek aslında coin oluşturmaz. Teoride coin'ler olsa da, bir ağ kurulup kod çalıştırılana kadar hiçbir coin yaratılamaz ve kullanılamaz. O sırada, Arscoin sadece ondan 42 milyon yaratılabileceğini söyleyen pasif bir yazılım parçası olarak varlığını sürdürüyordu. Aslında hiç coin yaratılmamıştı. Farivar Arscoin'in varsayımsal bir coin'den gerçek bir coin'e dönüşmesi sürecini şöyle anlatıyor:

---

[1]Farivar, Cyrus. "Behold Arscoin, Our Own Custom Cryptocurrency!" Ars Technica. 5 Mart 2014. Erişim tarihi 21 Haziran 2015. http://arstechnica.com/business/2014/03/behold-arscoin-our-own-custom-cryptocurrency/

Bana yol göstermesi için Coingen yaratıcısı Corallo'yu aradım. Öncelikle, meslektaşlarımdan birinin eş olarak eklenebilmesi için uygulamayı yükselmesi gerektiğini söyledi. Çok geçmeden, büyük deneye Peter Bright katıldı ve Arscoin-qt konsolunu açıp 'addnode [Peter'ın IP adresi] add,' yazmamı sağladı. Ve bam! Birden Arscoin'in iki kişilik eşler arası ağı oluştu.

Bir sonraki adım 'setgenerate true' komutuyla madenciliğe başlamaktı. Arscoin uygulamasının Windows versiyonunda, görev çubuğunda çok geçmeden başarılı bir şekilde çözülen bir bloğu belirten bir pencere açıldı. Ödül mü? Elli Arscoin. Artık Arscoin resmen doğmuştu.

Bu işe yaramaz matematiksel kütürtü olsa da, 'coin' çıkarma heyecanı hızla başka çalışanları çekti. Arscoin düğümlerinden oluşan ağımız üç katına çıktı. Grup 120 blok çözdüğünde, 'olgunluğa' erişen o ilk coin'ler artık harcanabilirlerdi. Beş eşle, o kadar bloğu çözmek sadece birkaç saat aldı.

O noktada, birbirimize coin gönderebiliyorduk. Birinin Arscoin cüzdan adresi görevini gören rakam ve harflerden oluşan uzun diziyi kopyalayıp yapıştırmak kolaydı ve başkalarına coin göndermeyi tamamlamak sadece birkaç dakika sürüyordu. İşe yaramaz coin'lerimizin artık işe yaramaz bir ekonominin esaslarına sahipti.

Bu coin'ler işe yaramaz görünseler de, onlara talep vardı, o nedenle 'sıfırdan fazla' değere sahiptiler. Makale

yayınlandıktan sonra, Ars Technica okuyucuları Arscoin'e ilgi duydular ve basın kuruluşlarının eline birdenbire oldukça başarılı bir kripto para birimi geçti. Okuyucuların Arscoin'lerini harcayabilecekleri bir dükkân açtı. Dükkânda sadece orijinallik satıyordu –web sitesindeki makalelerin altında yorumlardaki kullanıcı isimlerine eşlik eden küçük süslü şapkalar– ama bu da bir şey sayılırdı.

Bir anda, Arscoin çok az altcoin'in sahip olmayı başardığı üç şeye sahip oldu: medya ilgisi, bir topluluk ve bir kullanım alanı. Rekabetçi bir gelişim ekibi, kalıcı bir ekonomi yaratmak için uzun vadeli planlar ve merkezsizleştirilmiş bir piyasa gibi birkaç şeyi eksikti. Ama kusurları isimlerinin yanında süslü şapkalar isteyen sayısız Ars Technica okuyucusunu caydırmadı. Kulağa aptalca gelse de, süslü şapkaları sadece Arscoin ile satın alabilirsiniz. Çok az altcoin benzer bir iddiada bulunabilir. Bitcoin'i bile, Karanlık Ağ piyasaları dışında çok az ürün ya da hizmet kabul ediyor.

Elbette, başarı özneldir, ama para birimi klonlanmış ve kendinden menkul tuhaf bir paranın görmesi gerektiğinden daha fazla ilgi gördü. (Klonlanmış para kopyala-yapıştır kod içerir. İsmi, toplam coin sayısı ve blok ödülü gibi kolaylıkla değiştirilebilen birkaç değişken dışında hiçbir değişikliği olmayan para birimidir.) 11 Nisan 2014'te Ars Technica ekibi Arscoin'i öldürdü ve ona ayrılan bütün bilgisayımsal güç dijital giderden akıp gitti. Çok geçmeden süslü şapkalar da onu izledi.

Bu kararı açıklayan bir makalede, yazar Lee Hutchinson para biriminin birkaç dönüm noktasına değindi:

7 Nisan 2017 itibarıyla, toplam 1,103,600 Arscoin oluşturuldu (gerçi birkaç blok değerinde coin havuz sorunları nedeniyle kaybedildi). Cüzdanları için otomatik ödemeyi hiç yapılandırmayan kullanıcılar tarafından çıkarılan o coin'lerin yaklaşık 81,600'ü havuz sunucusunda dağıtılmadan duruyor.

Arscoin dükkânında toplam 864 satın alma oldu; buna ilk şapka alımları, pişmanlıkla şapka alımları ve renkli kullanıcı isimleri dahil. Bu alımlar dükkânda toplam 572,565 Arscoin harcandığını gösteriyor.

Tümüyle ele alındığında, 3005 kullanıcı havuz sunucusuna kaydoldu ve toplam 5108 havuz çalışanı yaratılıp kullanıldı.[2]

Arscoin altcoin yaratmanın ne kadar kolay olduğunu gösterdi ve bilerek ya da bilmeden, bütün altcoin ekosisteminin gülünçlüğüne dikkat çekti. Ama bu deney günün birinde gerçekten değerli olma şansı olan gerçek kullanım alanlarına sahip coin'lerin olmadığı anlamına gelmez.

Bu bölümün geri kalanında, piyasa değerine göre en bilinen altcoin'lerin –hâlâ ICO (ilk dijital para arzu) evresinde olan coin'ler hariç– yanı sıra, ya geçmişte başarılı olan ya da bahsetmeye değer gördüğüm eşsiz özellikleri olan diğer altcoin'leri ele alacağım. Herhangi bir coin gelişti-

[2]Hutchinson, Lee. "Farewell to Arscoin: Preparing to Kill Our Cryptocurrency." Ars Technica. 7 Nisan 2014. Erişim tarihi 21 Haziran 2015. http://arstechnica.com/information-technology/2014/04/farewell-to-arscoin-preparing-to-kill-our-cryptocurrency/

rici bu listede ona yer vermem için bana para ödemedi ve hiçbirine bol miktarda sahip değilim. Bu piyasadaki faydalı altcoin'lerin hepsinin olduğu kapsamlı bir liste olmaktan çok uzak. Bu sadece altcoin piyasasının genel manzarasını kısaca ve gerçekçi bir şekilde sergilemek için benim dürüstçe bir çabam.

Litecoin
Algoritma: Scrypt
Madencilik Türü: İş ispatı (PoW — proof-of-work)
Blok süresi: 2.5 dakika
Zorluk Yeniden Hesaplaması: 2016 blok
Blok Ödülü (güncel): 25 LTC
Ödül Eğrisi: Her 840,000 blokta yarılanma
Toplam LTC Sayısı: 84 milyon

Litecoin kabul görme seviyesi ve marka tanınırlığına bakılırsa, muhtemelen Bitcoin'den sonra en popüler kripto paradır. Charlie Lee tarafından yaratıldı. Teknik olarak, çok kötü bir dağılımı olan, ilk Scrypt coin Tenebrix'in bir çatalıdır. İlk başta, 'Bitcoin altınsa, Litecoin gümüştür' diye pazarlanan Litecoin, madencilerin giderek daha karışık madencilik ekipmanları kurdukları Bitcoin'in büyüyen donanımı ve ASIC yarışının önüne geçmek için bir teşebbüstü. Amaç madenciliği onun için özellikle tasarlanmış donanımlardan uzaklaştırıp ev bilgisayarlarına geri döndürmek için CPU'ya dayanan bir algoritma kullanmaktı.

Bu bir süre işe yaradı. Litecoin evde madencilik yapmak isteyenler için hâlâ kullanışlı bir seçenek. Ancak, Bitcoin'in karşılaştığı sorunlarla karşılaştı ve bu yüzden evde

madencilik yapmanız tavsiye edilmez, yine de Bitcoin madenciliğinden daha makul.

En sonunda Scrypt madenciliği yapması için tasarlanan ASICler piyasaya sürüldü ve Litecoin'in popülerliği arttıkça, zorluk seviyesi Bitcoin'inkine benzer bir eğri izledi. Fiyatı son birkaç senede düşmesine rağmen, Litecoin'in zorluğu artmaya devam etti ve en yeni teknoloji donanımlarla bile madencilik kârlılığı çok düşük. Ev bilgisayarında madencilik yapmak size Litecoin kazandırmaktan ziyade büyük ihtimalle donanımınıza zarar verir. Bununla birlikte, eğer kullandığınız elektrik ücretsiz ya da oldukça ucuzsa, evde bir ölçüde madencilik yapmak mümkün olabilir. Evde Bitcoin madenciliği yapmaktan daha makul olduğu kesin olsa da ortalama bir kullanıcıya önerilmez.

Günümüzde, Litecoin büyük ölçüde tasarlandığı şekilde kullanılıyor: tıpkı Bitcoin gibi, sadece daha ucuz. Bu kitabı yazdığım sırada, bir Litecoin $2.93 değerindeydi. Bu Bitcoin ve yasal para birimleri dışında (diğer kripto para birimlerinin takas edildiği para birimi) en sık takas edilen paradır. Aynı zamanda, ya Coin Merchants gibi popüler işleme şirketleri ya da 'tacirden tacire' ilkesiyle bağımsız olarak çalışan tacirler tarafından kabul görüyor.

Litecoin'i başlatan Charlie Lee, aynı zamanda Bitcoin'e giden Amerika merkezli en popüler kestirme yol Coinbase'in ilk yatırımcılarındandı. Coinbase'le olan ilişkisi Coinbase'in bir noktada Litecoin'i kabul edeceğine dair sürekli spekülasyona neden oldu. Coinbase bir ödeme işleyicisi ve yasal para dünyasıyla bir köprü olarak statüsü düşünüldüğünde, onun tarafından kabul görmek Litecoin için çok faydalı olur. Ancak Charlie Lee'nin bağlantısı dı-

şında, Coinbase'in Litecoin'i kabul edeceğine dair hiçbir işaret yok.

Teknik bir açıdan bakıldığında, Litecoin Bitcoin'den daha hızlı. Bitcoin'le aynı blok boyutuna ama çok daha kısa blok süresine sahip olduğu için ağ her saniye Bitcoin'in güncel biçiminde olduğundan daha fazla işlem yapabilir. Bitcoin'in blok boyutu sabit değil ve blokların boyutunu değiştirmek konusunda süregelen bir tartışma var ama şimdilik Litecoin daha hızlı.

Kısa bir süre önce, Litecoin Dogecoin ile karışık madenciliği (aynı algoritmaya sahip iki coin'i aynı anda çıkarmayı) başlattı. İkisi de Scrypt kullanıyorlar, o nedenle hash oranları aynı anda iki coin'e aktarılabilir. Litecoin madencileri için bir dezavantaj yoktu ve birleşim Litecoin madencilerini Dogecoin ağına taşıyarak onu güvenceye almayı sağladı.

Dogecoin
Algoritma: AuxPoW ile Scrypt
Madencilik Türü: İş ispatı (PoW — proof-of-work)
Blok süresi: 1 dakika
Zorluk Yeniden Hesaplaması: Digishield (değişken)
Blok Ödülü (güncel): 10,000 Doge
Ödül Eğrisi: Her 840,000 blokta yarılanma
Toplam LTC Sayısı: 100 milyon [hedef, değişken]

Eğer Litecoin en popüler ciddi kripto paraysa, Dogecoin en 'viral' olanıdır; sorduğunuz kişiye bağlı olarak ya 'Dogi Coin' ya da 'Douci Coin' olarak telaffuz edilir. Esasında, bir şaka olarak başlayan Dogecoin, ortalamadan daha iyi dayanma gücüyle büyük bir hit oldu. Dogecoin'in

ilk başarısının sırrı maskotuydu. İnternette popüler olan Shiba Inu cinsi bir köpeğin resmi en başından beri para biriminin maskotu oldu. İlk benimseyenlere faydalı olması için en başından yüksek ödüller sunduğu için teknik açıdan coin'in uzun süre ayakta kalması beklenmiyordu. Dogecoin'in bir 'şişir ve boşalt' coin'i olarak piyasaya sürülmüş olması tartışılabilir.

Ama bu yanı bir para birimi olarak büyümesine engel olmadı. Bir coin'in topluluğu son derece önemli olabilir, Dogecoin'in topluluğu da birinci sınıftı. Doğal, viral pazarlamada harika olan topluluk 'şakayı' devam ettirmek için çok uğraştı. Erken girenler büyük kâr ettiler. Dogecoin, 'doge dili' ile interneti neredeyse ele geçirmesinin yanı sıra, bir NASCAR pilotuna sponsor olduğunda da ün kazandı. Topluluk, resmin arabaya yerleştirilmesi için tamamen bağışlarla toplanan, $55,000'dan daha fazla para ödedikten sonra Josh Wise üzerinde Dogecoin Shiba Inu olan bir araba kullandı.[3] Üstelik, egzoz borusunun yanındaki küçük bir logodan bahsetmiyorum. Arabanın kaportasına boyanan bir resimdi. Josh Wise bir 'Dogecoin Arabası' sürüyordu.

Daha sonra, John Candy'nin hayaletinin bile içini ısıtabilecek bir hikâyede, topluluk Jamaika kızak takımına sponsor olarak takımın Sochi 2014 Kış Olimpiyatları'na gitmesini sağladı.[4]

---

[3]"Dogecoin to Sponsor Josh Wise at Talladega." NASCAR.com. 22 Mayıs 2014. Erişim tarihi 22 Haziran 2015. http://www.nascar.com/en_us/news-media/articles/2014/5/22/josh-wise-dogecoin-sponsorship-talladega-sprint-fan-vote.html

[4]Davidson, Kavitha A. "Jamaican Bobsledders Ride Dogecoin Into Olympics." BloombergView.com. 4 Şubat 2014. 22 Haziran 2015. http://www.bloombergview.com/articles/2014-02-04/jamaican-bobsledders-ride-dogecoin-into-olympics

Ancak, daha önce de bahsettiğim gibi, Dogecoin hiçbir zaman uzun vadede ayakta durması için tasarlanmadı, o nedenle –orijinal geliştiricileri de dahil olmak üzere– herkesin beklediğinden daha uzun süre dayanmış olmasına rağmen, bazı sorunlarla karşılaştı. Dogecoin, coin yaratımının ilk döneminde madencilik ödüllerinin yüzde doksanını alarak onu ilk kullanıcılarına faydalı olacak şekilde tasarlandı. Dogecoin'lerin arzı azalırken, madencilik ödülü, hash oranı ve en nihayetinde, güvenliği de azaldı. Madencilik ödülü azalınca, daha çok madenci donanımlarını daha kârlı para birimlerine yönlendirdiler. Ağ zorluğunun bir coin'e olan ilginin azalmasını ya da coin'in değerinin düşmesini telafi etmesi gerekse de, Dogecoin'in madencilik ödülünde aşırı düşüş kolaylıkla idare edilemezdi. Dogecoin büyük bir piyasa değeri kazandı ve hash oranı hızla düşerken, %51 saldırısı gerçek bir olasılık haline geldi.

Çözüm Litecoin aracılığıyla geldi. Her iki toplulukta uzun uzun tartışıldıktan sonra, Litecoin Dogecoin ile birlikte madenciliği birleştirmeye karar verdi. Dogecoin ağındaki oldukça düşük ödüllere rağmen, Litecoin madencileri bu karardan yine de karlı çıktılar. Aynı algoritmayı kullandıkları için her iki coin de, çıkarımlarında düşüş olmadan, aynı anda çıkarılabilir.[5] Bu Dogecoin ağının Litecoin madencileri tarafından güvenceye alınmasını sağladı ve %51 saldırısı aracılığıyla çifte harcama yapmak isteyen birinin hep Litecoin'in ağının hash oranı hem de

[5]Higgins, Stan. "Dogecoin Community Celebrates as Merge Mining with Litecoin."

Dogecoin'inkiyle boy ölçüşmesi gerekecekti. Sonrasında, madencilik birleşimi birçok küçük kripto para da popüler bir özellik oldu.

En şiddetli savunucularının bile kabul ettiği gibi, Dogecoin internet para biriminin geleceği değil. Ama bu, bu esnada bir yeri olmadığı anlamına gelmez. Şimdiden birçok beklentiyi karşıladı ve kripto para dünyasının geri kalanı Dogecoin'in topluluğu ve başarılarından çok şey öğrenebilirler.

Ripple/Stellar

Teknik olarak, Ripple Labs Bitcoin'den çok önceden beri vardı. Aslında PayPal'dan pek farklı olmayan bir ödeme işlemcisiydi. Satoshi Nakamoto'nun tanıtım yazısı yayınlandıktan ve Bitcoin'in yükselişinin ardından, şirket Ripple adı verdiği kendi kripto para birimini piyasaya sürmeye karar verdi.

Ripple Bitcoin ve birçok kripto paradan farklıdır. Topluluktaki birçok merkezi yapısı nedeniyle kişi onun 'gerçek' bir kripto para olmadığını iddia ediyor ve haklı da olabilirler. Ancak bu, Ripple'ın yasal para dünyasıyla birlikte çalışmak konusunda çok becerikli olduğunu kanıtladığı ve bankalarla ve geleneksel finans endüstrisinin diğer yönleriyle etkileşim içinde olmaya önderlik ettiği gerçeğini değiştirmez.

Ripple, Mt. Gox kurucusu Jeb McCaleb Mt. Gox'u eski yönetim kurulu başkanı Mark Karpelès'e sattıktan sonra McCaleb ve Chris Larsen tarafından yaratıldı. Ripple Bitcoin ile aynı kodu paylaşmıyor ve Bitcoin'in üçüncü parti yazılım olmadan rahatlıkla yapamayacağı birkaç şeyi yapa-

bilecek şekilde tasarlandı. Bu özelliklerin ne kadar yararlı olduğu tartışılır, ama yine de Ripple'ın dikkat çekmesini başardılar.

Ripple, ortak hesap defterinde her türlü emtianın satın alınabilmesine imkân tanıyan ağ geçidi denen bir konsept kullanarak çalışıyor. Ağ geçitleri emtia sahibi olan bireyler ya da şirketlerdir ve söz konusu emtia için piyasaya esasında bir IOU sürebilirler. Örneğin, bir değerli maden şirketi bir IOU değerinde bir ons altın satabilir. Onu Ripple ağında satın alan kişi, teoride, o IOU'yu şirketin fiziki konumlarından birinde fiziki altına dönüştürebilir.

Tacir daha sonra dünyanın farklı noktalarındaki diğer güvenilir tacirlerle ortaklık yaparak insanların dijital altın token'ları alıp satabilecekleri dünya çapında bir ağ oluşturabilir. Bu sistem güvene dayanır ve bu, Bitcoin sonrası dijital para birimlerinin çoğunun ortadan kaldırmaya çalıştığı bir şeydir. Bitcoin'in bu kadar başarılı olmasının sebebi üçüncü partilere güvenmeye gerek duymamasıdır. Ripple'ın ağ geçidi sistemi, aslına bakılırsa, kullanıcıların ağ geçitlerinin sisteme sürdükleri IOU'ların karşılığını ödemelerini gerektiren bir üçüncü parti sistemidir. Bu bir takas ama sistemde neredeyse her emtianın ticaretini kolaylaştıran özelliklere imkân tanıyan bir takas. (On yedinci bölümde güvenilir partilere ve nasıl işlediklerine daha detaylı bir şekilde değindim.)

Ripple adı verilen ve para birimi kodu XRP olan Ripple'ın kendi para birimini herhangi bir üçüncü partinin göndermesi gerekmiyor. Bitcoin ve diğer kripto paralarda olduğu gibi, para bir kuruştan az bir ücret karşılığında dünyanın herhangi bir yerindeki başka bir Ripple kullanı-

cısına gönderilebilir. Ama topluluktaki bazı kişileri asıl endişelendiren ve Ripple'ın gerçek bir kripto paradan farklı olduğunu düşünmelerine neden olan şey paranın dağılımı.

Ripple Ripple Labs tarafından ön çıkarımı yapılan bir para birimi, bu var olması planlanan bütün Ripple'ın zaten var olduğu ve çoğuna Ripple Labs'ın sahip olduğu anlamına geliyor. Ripple Labs gelişim için 20 milyar Ripple'ı elinde tutacağına ve bir 50 milyarı da mümkün olduğunca adilce dağıtacağına söz verdi, ama özünde bu Ripple Labs'ın para birimini kontrol ettiği anlamına gelir. Dilerse, fiyatın dibe vurmasına izin verecek kadar Ripple'a sahip. Ayrıca, merkezsizleştirilmiş madencilikle ağı güvenceye alan biri olmadığı için Ripple'ın açık hesap defteri üzerinde ne kadar kontrole sahip olduğu da belli değil. Yüklü miktarda Ripple'ı dağıtmış olsa da, hâlâ elinde milyarlarcası var ve eğer Ripple şirketi yarın kaybolursa, varlıklarına ne olacağı belli değil. Bu ön çıkarım aynı zamanda Ripple'ın aşırı şişen piyasa değerinden de sorumlu. Ripple'ın belirli bir değere sahip olması ve ağda 100 milyar Ripple olması, toplam ağın onun 100 milyar katı değerinde olduğu anlamına gelmez. Eğer Ripple Labs bütün Ripple coin'lerini tek seferde satarsa, fiyatı arz talebe bağlı olarak dibe vurur. Ripple'ın gerçek değeri fiyatına karşılık ne kadar satılmış olduğudur, ama bu hesaplanamayacak kadar zor bir sayı.

Jeb McCaleb'e göre, Ripple'ı bırakıp Stellar'ı başlatmasının bir sebebi bu tür endişelerdi. Stellar da esasında Ripple gibi işliyor, ama daha şeffaf ve adil bir dağılım hedefliyor. Stripe yatırımla piyasaya sürüldü (Stripe insanların kredi kartı ve Bitcoin de dahil olmak üzere diğer

ödeme yöntemlerini cep telefonlarıyla kabul etmelerini sağlayan bir şirkettir) ve daha şeffaf bir dağılım vaat ediyor, ama piyasaya sürülmesi sorunlarla doluydu ve para birimi henüz Ripple'ın başarısını yakalayamadı.

Ripple Bitcoin topluluğunun çekirdek ilkelerinin çoğunu reddetmesine rağmen, ya da belki de bu yüzden, geleneksel finansal kuruluşlarla ilerleme kaydetti. Fidor Bank Ripple kullanıyor, Saldo.mx Birleşik Devletler müşterilerinin Meksika'daki ailelerinin faturalarını ödemelerine imkân tanıyor ve Amerika'daki birkaç küçük banka da Ripple'la projeleri olduğunu açıkladı. Bu listeyle Ripple önemli bir başarıya imza atmış görünmeyebilir, ama yine de yasal para dünyasına adımını bile atamayan birçok altcoin'den çok daha ileride.

Dash/Dark
Algoritma: X11
Madencilik Türü: İş ispatı (PoW — proof-of-work)
Blok süresi: 2.5 dakika
Zorluk Yeniden Hesaplaması: 2016 blok
BlokÖdülü(güncel):2222222/(((Zorluk+2600)/9) ^ 2)
Toplam Dash Sayısı: ~22 milyon

Dash'ın adı — Dashcoin ile karıştırmayın — ilk olarak Darkcoin'di, ama yaratıcıları suçla bağlantıları olduğu algısından uzaklaşmak amacıyla onu yeniden isimlendirmeye karar verdiler. Dash, Bitcoin'in takma isimli yapısından elektronik paranın anonim vaadine son sıçrayışı yapmayı hedefleyen gizliliğe önem veren bir kripto paradır.

Dash bunu Tor ağını çalıştıran düğümlerden pek fark-

lı olmayan bir ana düğümle etkileşimde kalarak yapmaya çalışıyor (Tor Derin Ağ'a kurulu ve sadece aynı ismi taşıyan özel tarayıcısıyla erişilebilen bir şebekedir. Tor hakkında daha fazla bilgi için altıncı bölüme bakın.) Temel fikir her işlemin başka bir işlemle gruplandırıldığı bir ana düğüme gönderilmesi ve kriptoyla blokzincirine kaydedilmesidir. Çıktılar kapatılır, böylece kimin kime ne kadar gönderdiğini hiçbir dış gözlemci göremez; sadece farklı kullanıcılardan bir grup coin'in ana düğüme gittiğini ve aynı miktarda coin'in çıkıp diğer üyelere gittiği görülebilir. Darksend adı verilen bu teknoloji kökenini ve varış yerini gizlemek için Bitcoin işlemlerini karıştıran Bitcoin teknolojisi CoinJoin'e dayanıyor.

Dash'in Bitcoin'den daha anonim olduğu tartışılmaz olsa da, Derin Ağ tarayıcısı Tor'u uğraştıran aynı sorunla mücadele ediyor: düğümlerin güvenilir olmasına bağlı olmak. Düzenli hissedarların alımlarını gizlemek için muhtemelen yeterlidir, ama aklama sürecinin kullanıcıların Dash'lerini nasıl harcadıklarını çözmeye kararlı iyi finanse edilmiş bir oluşumu engelleyebileceğinin hiçbir garantisi yok.

Birçok 'anonim' kripto para biriminde olduğu gibi, karanlık piyasaların yüksek gizlilik özellikleri sebebiyle Dash'i benimseme ihtimali insanları heyecanlandırdı. Yasadışı mal satın almakla ilgilenmeyenler için bile, karanlık piyasaların Dash'i benimseme düşüncesi umut vericiydi, çünkü Bitcoin'in ilk döneminde olduğu gibi aktif yer altı piyasasının talebi genel talebi artırıp fiyatın yükselmesini sağlayabilir. Ancak, karanlık piyasaların çoğu daha fazla kişi tarafından benimsenen Bitcoin'i tercih ettikleri için bu henüz gerçekleşmedi.

Günümüzde, Dash kendisini bu algıdan uzak tutmaya çalışıyor. Geliştiricilerinin hiç vakit kaybetmeden gizlilik istemenin suç olmadığına dikkat çektiği gibi, finansal işlemlerinizi gözlerden uzakta tutmayı istemek için birçok geçerli sebep var. Dash'in en önemli özelliği hâlâ artırılmış gizlilik seçenekleri, ama 'ana akım' kripto kitlesiyle flört etmeye devam ediyor gibi görünüyor.

NuBits

NuBits ilginç bir coin, çünkü topluluğun büyük bir kısmının nefret ettiği bir para birimiyle bağlantılı. NuBits değer her zaman bir dolar olacak şekilde tasarlandı. Döviz kontrolü mü? Enflasyonist bir para birimine fiyat sabitlemek mi? İnsanların kripto paralara sığınmalarının sebebi bundan uzaklaşmak değil miydi?

Öyle olabilir, ama değişken olmayan bir kripto para arzusu var ve NuBits bunu sağlıyor. Herkes NuBits'in blok zinciriyle birlikte bir cüzdan indirip varlığını bilgisayarında tutabileceği için hâlâ merkezsizleştirilmiş durumda, ama fiyatını bir dolar seviyesinde tutmak için perde arkasında çok fazla çaba harcanıyor.

NuBits fiyatı kontrol altında tutmak için farklı borsalarda NuBits alım-satımı yapan robotlar kullanıyor. Bu da fiyat sabitlemesinin geliştirici desteğine bağlı olduğu ve onların sonsuza kadar yanlarında olup olmayacaklarını bilmenin imkânsız olduğu anlamına geliyor, ama –fiyatın bir doların oldukça altına indiği bir örnek dışında– fiyatı olması gerektiği yerde tutarak harika bir iş çıkardılar.

NuBits, Bitcoin'in fiyatına karşı bir çit olarak faydalı olmasının yanı sıra, yatırımınızı riske atmadan kripto pa-

ralara giriş yapmanın da bir yoludur. Elbette, fiyatı sabitlemek spekülatif yatırımı engelliyor ama NuShares –NuBits yaratıcılarının bir diğer kripto parası– insanlara teknoloji üzerine bahse girmeleri için imkân verdi. Geliştiricilere göre, neredeyse bağımsız hareket eden fiyat kontrolünün para birimini uzun vadede sabit tutup tutamayacağını görmek ilginç olacak.

Nxt
Algoritma: Uygulanmaz, imzalamak için SHA256 kullanır
Madencilik Türü: Proof-of-stake (PoS)
Blok süresi: 1 dakika
Blok Ödülü (güncel): %1

Telaffuzu *nekst* olan Nxt, mevcut coin'ler arasında en güçlü olan "Crypto 2.0" (gelecek nesil) coin'dir. En aktif geliştirici topluluklarından birine sahip ve 2.0 özellikleri en sık kullanılanlar arasında. Nxt dijital ürünler için merkezsizleştirilmiş bir piyasa, bir dijital 'token' ya da varlık borsası, Nxt blok zincirinde güvenceye alınan para birimlerinin kolayca yaratılmasına imkân tanıyan bir parasal sistem, bir mesajlaşma sistemi ve bir takma ad sistemi içeriyor. Ayrıca, birkaç blok zincirini birleştirip iletişim kurmalarına imkân tanıyan SuperNET sisteminde en önemli coin'dir.

Bu özellikler 2013'te para biriminin piyasaya sürülmesinden sonra zaman içinde ortaya çıktı ve sürekli yeni özellikler ekleniyor. Bitcoin'in Satoshi Nakamoto'su gibi, Nxt'in yaratıcısı da anonim kalmayı seçti ve BCNext ismiyle tanındı ama sonra Nakamoto gibi ortadan kayboldu.

Nxt topluluğu coin'in en güçlü varlıklarından biri olsa da, aynı zamanda en büyük engellerinden biri olduğunu kanıtladı. Tarihinin ilk döneminde, topluluk hâlâ net olmayan sebeplerden ötürü bölündü. Bu bölünme iki mesaj panosunun yaratılmasına neden oldu ve bu durum yeni katılanların hâlâ kafalarını karıştırıyor. Ayrıca, topluluğun üyelerini ya da eski üyelerini içeren coin'in itibarını zedeleyen birkaç sahtekârlık yaşandı.

Nxt, ayrıca, birkaç Bitcoin tarzı korsanlığın hedefi oldu. Bütün bunların coin'in güvenliğinden ziyade borsa güvenliği ya da kullanıcı hatasıyla ilgisi olmasına rağmen, Nxt tamamen çevrimiçi depolanır ve bazen sorunun sebebi olarak kolaylıkla çevrimdışı depolanabilir cüzdanların olmaması gösteriliyor. 2014'te, Nxt'in en büyük borsalarından biri, Bter, 50 milyon Nxt kaybetti.[6] Topluluk saldırısının etkisini tersine çevirmek için sert çatallanma yapmayı düşündü ama bunun saldırı ve sert çatallanma arasındaki süre boyunca meşru işlemler yapan insanlar için adil olmayacağına karar verdi. Bunun toplulukta kötü bir örnek olacağı düşünüldü.

Bazıları ise, sorunun Nxt'in dağılımı olduğuna dikkat çektiler. Nxt bir proof-of-stake coin, yani 'para bastığı' sürece her hesabın bulundurduğu coin kadar yıllık yaklaşık yüzde bir faiz alır. Nxt'in ilk dağılımının Bitcoin'inkinden daha kötü olmadığı iddia edilse de, Nxt'in oluşumunu cüzdan sahibinin 'zenginliğine' bağlı kılan proof-of-stake coin'ler 'zengin daha da zenginleşir' dinamiğini sürekli pekiştiriyor. Bu yüzden, proof-of-stake coin'ler için ilk

[6]DeMartino, Ian M. "Breaking: Bter Hacked, 50M NXT Stolen." CoinTelegraph. 15 Ağustos 2014. Erişim tarihi 22 Haziran 2015. http://cointelegraph.com/news/112278/breaking-bter-hacked-50m-nxt-stolen

dağılım büyük bir endişedir. Yine de, Bitcoin'in iş ispatına dayanan mekanizması ücretsiz ve eşit coin oluşumu mekanizmasıyla sonuçlanmadı ve proof-of-stake'in de kendine göre avantajları var.

En nihayetinde, Nxt son derece güçlü ve eşsiz bir teknoloji parçası olduğu için bu ve diğer karşıtlıklara rağmen ayakta kalmayı başardı. Coin'in ilk sahiplerinin çoğu onları eşantiyon olarak ve yazılım hatalarını bulan kişilere ödül veren programlarla (yazılım geliştiricilerinin programlarında hata bulan kişilere para teklif ettiği) dağıtıyorlardı, ama belki de başkalarının istediği kadar hızlı değillerdi. Ağırlıklı olarak Bitcoin'in kodunu ödünç alan birçok coin'in aksine, Nxt Javascript kullanılarak sıfırdan yaratıldı. Bu yüzden, geliştiricileri kullanıcı dostu bir ara yüz yaratmayı ve Bitcoin'in koduna dayanan coin'lere dahil etmenin kolay olmadığı özellikleri eklemeyi başardılar.

Nxt'in geliştirici topluluğu Bitcoin, Ethereum ve Counterparty'yle birlikte en iyiler arasında ve varlık borsası yüksek riskli yatırımlar için eğlenceli bir yer. Bazı özellikler pek başarılı olmadı. Örneğin parasal sistemi aceleye getirilmiş –hiçbir yenilik ve değer getirmeyen– hiçbir amaca hizmet etmeyen ve kimsenin satın almadığı kripto paralarla dolu. Aynı şekilde, dijital ürün mağazası çok etkileyici ama kullanıcılar ürünlerin değiştiğini nadiren görüyorlar.

Bu pek başarılı olmayan özelliklerine rağmen, Nxt Bitcoin'i hükümsüz kılma hakkındaki tartışmalarda yer edinen birkaç alternatif para biriminden biri. Ancak, bunun olası olduğunu sanmıyorum, çünkü hiçbir coin'in Bitcoin'in yerine geçebileceğini düşünmüyorum.

Counterparty

Counterparty bir başka Bitcoin 2.0 projesidir, ama Bitcoin blok zincirinde çalışarak Bitcoin ağının güvenliği ve hash gücünü alır. Varlık oluşumu ve akıllı kontratlara imkân tanır. Varlık ihraç edenler, varlıktan daha fazla oluşturulup oluşturulamayacağı da dahil olmak üzere birçok farklı parametre belirleyebilir ve kâr payını, Counterparty ya da Bitcoin, varlığı biçiminde dağıtabilirler.

Counterparty, piyasaya sürüldüğünde Counterparty coin'leri almak isteyen insanların doğrulanabilir harcanamaz bir adrese bitcoin göndererek o bitcoin'leri Bitcoin ekosisteminden sonsuza kadar çıkardıkları proof-of-burn (yakma) yöntemi aracılığıyla yaratıldı. Bu bir genel algılama değeri oluşturmak için yapıldı. Geliştiriciler de dahil olmak üzere, insanların Counterparty almak için para harcamaları gerekiyordu. İnsanların adil piyasa değeri ödemek zorunda olmaları kripto paralar için her zaman doğru olabilse de, bu para genellikle madencilere gider. Counterparty gibi madencilik yapılamayan para birimleri durumunda (Bitcoin'in aksine madencilik yapılamayan paralar), o para geliştiricilere gider. Proof-of-burn (yakma ispatı) geliştiricilerin projeyi desteklemek için bitcoin'lerini yakacak kadar kendilerini işlerine adadıklarını kanıtlarken, coin'lerin adilce dağıtılması için bir yöntem olarak görüldü.

Bu yaklaşım tartışmalıydı, çünkü kullanımda olacak bitcoin sayısı sınırlıdır. Uzun vadede var olup olmayacağı kesin olmayan bir para birimine değer algısı kazandırmak için onları yakmak birçok Bitcoin hayranını rahatsız etti. Teoride, bitcoin'leri yakmak geriye daha az kalacağı için

kullanımda olan bitcoin'leri daha değerli kılacak olsa da, sınırlı stoğu azaltmak herkes tarafından sevilen bir fikir olmadı.

Counterparty daha sonra Overstock'un sunuculuğunda Medici adında 'Bitcoin'e benzer' bir borsa kurmak için Overstock.com ile sözleşme yaptı. Overstock'un başkanı Patrick Byrne Bitcoin'in en büyük destekçilerinden biridir. Ne yazık ki, Counterparty'nin geliştiricileri ve Overstock duyurudan sadece dört ay sonra Şubat 2015'te ayrıldılar. Medici hiçbir zaman piyasaya sürülmedi ve Overstock kendi borsasını geliştiriyor.

Aynı zamanda, Counterparty'nin özelliklerinin çoğunun, hiç şaşırtıcı olmasa da, Dogeparty adı verilen Dogecoin sistemine kurulan başka bir platforma taşındığını belirtmekte fayda var.

Counterparty onun çevresine birkaç sistem kurdu ve sürekli daha fazlası ekleniyor.

Master/Omni

Counterparty gibi, Master/Omni de Bitcoin blok zinciri üzerine kuruldu. Ocak 2015'te, Mastercoin hem piyasaya sürülüşünü lekeleyen anlaşmazlıktan uzaklaşmak hem de projenin yeni bir sayfa olduğunu göstermek için Omni olarak yeniden isimlendirildi.

Mastercoin/Omni kripto para tabanlı varlık borsası yaratması için Overstock.com tarafından görevlendirildi ama Overstock en sonunda Mastercoin/Omni geliştiricilerinin yardımı olmadan projeye devam etmeye karar verdi.[7] An-

[7]Rizzo, Pete. "Lead Developers Leave Overstock's Medici Project." CoinDesk. 4 Şubat 2015. Erişim tarihi 22 Haziran 2015. http://www.coindesk.com/lead-developers-leave-overstocks-medici-project/

cak, işe yararlılığını kanıtlamak için Omni/Mastercoin sistemine kurulu üç proje var: Maidsafe, Tether ve Factom.

Maidsafe: Maidsafe merkezsizleştirilmiş bir internettir. Web sitelerini ve diğer dosyaları bütün internete hizmet eden tek bir sunucuda depolamak yerine dosyalar şifrelenir, bölünür ve dünyanın farklı noktalarındaki bilgisayarlara gönderilir. Sabit sürücülerinin kullanmadıkları kısımlarını bağışlayan katılımcılar Maidsafe coin'leri/token'larıyla ödüllendirilirler. Mevcut haliyle, Maidsafe daha ziyade merkezsizleştirilmiş bir dosya deposu ve kayda değer bir karışıklığa sebep oluyor. Eğer hükümet kontrolünden muaf yeni bir internet olmayı başarırsa, geleceğimizi büyük ölçüde değiştirebilir.

Tether: Tether insanları Bitcoin'in oynaklığına karşı korumak için tasarlanan bir token. Bu haliyle, NuBits'e benziyor ama daha fazla para birimi destekliyor. Örneğin, TetherUSD, Amerikan dolarına bağlıdır.

Ancak, NuBits'in aksine, harcanabilir değil ve –Bitcoin'in eklentisi –Omni'nin bir eklentisi olarak kendi blok zincirine sahip değil. Daha ziyade, günlük işlemciler ya da Bitcoin'in değişkenliğinden geçici bir süreliğine uzaklaşmayı düşünenler tarafından kullanılır.

Factom: Factom dosyaları Bitcoin blok zincirine kriptolu güvenli bir şekilde işleyen bir doküman yedekleme hizmetidir. Pasaportlar, tapular ve hatta vasiyetler bile tamamen güvenli ve değiştirilemez bir şekilde depolanabilirler. Bir mahkemenin blok zincirine yedeklenmiş bir kopyayı

belgenin aslı olarak kabul edip etmeyeceğine dair bazı sorular var, ama doküman işlenmeden önce doğru düzgün bir şekilde noterden onaylandığı sürece kabul etmemeleri için bir sebep olamaz.

Peercoin
Algoritma: Uygulanmaz
Madencilik Türü: Proof-of-Stake
Blok süresi: 10 dakika
Ödül (güncel): yıllık %1

Peercoin ilk meşru proof-of-stake coin'di. Peercoin'in çatallandırıldığı daha eski bir coin vardı, ama kocaman bir gizli ön çıkarım içeriyordu. Ön çıkarımlar bütün kripto paralarda kabul edilemezdir, ama özellikle de proof-of-stake coin'lerde rahatsız edicidir. Proof-of-stake algoritmalar stake işlemini gerçekleştirenlere –proof-of-stake'in madenci versiyonu– bulundurdukları coin sayısına bağlı olarak daha fazla değer katarlar. Bitcoin ve iş ispatına dayanan coin'lerin hash gücüne ağırlık vermeleri gibi, –ağın hash gücünün %51'ini kontrol ettiğinizde blok zinciri değiştirebileceğiniz Bitcoin gibi– aynı şey bir oluşumun ağı güvenceye almak için cüzdanda mevcut coin'lerin yüzde 51'ini elinde bulundurduğu proof-of-stake coin'ler için de geçerli.

İlk uygulanabilir proof-of-stake coin olan Peercoin daha sonra Nxt, Bitcoin ve çok daha fazlasının kullandığı yöntemi kullandı. İş ispatına dayanan coin'lerde uygulanan madencilik yerine, Peercoin kullanıcıları yıllık yüzde bir faiz oranıyla yeni Peercoin'ler 'basıyorlar.' Madenciler

gibi bu para basan kişiler de ağı güvenceye alıyorlar. Ama madencilerin aksine, birbirleriyle yarış halinde değiller ve iş ispatına dayanan (proof-of-work) coin'lerin tartışmasız bir şekilde yaptıkları gibi çok fazla bilgisayımsal güç tüketmiyorlar. Hatta, Raspberry Pi mikrobilgisayar gibi hafif bir sistemde bir tam düğüm ve cüzdan depolanabilir.

Peercoin topluluğu birçok ilerlemeye önderlik eden yenilikçi bir topluluk. Peercoin'in üzerine kurulu token/varlık dağıtımına imkân tanıyan bir sistem olan Peershares de dahil olmak üzere kendi '2.0' projeleri var.

Ancak, coin bir süredir durgun. Her git commit arasında aylar geçiyor ve bir süredir hiç haber yok. Özellikle de, daha sonra piyasaya sürülen proof-of-stake coin'lerin daha aktif geliştirici toplulukları olduğu düşünülürse, dünyanın ilk proof-of-stake coin'ine geleceğin neler getireceğini merak etmek hiç zor değil.

Bytecoin/Monero
Algoritma: CryptoNote
Madencilik Türü: İş ispatı (PoW — proof-of-work)
Blok süresi: 2 dakika
Zorluk Yeniden Hesaplaması: 1 blok
Blok Ödülü: zorluğa bağlı olarak değişken

Bytecoin ve Monero, CryptoNote coin'lerdir, yani SHA-256 ya da Scrypt yerine CryptoNote algoritması kullanırlar. Başka CryptoNote coin'ler de var; esasında hepsi aynı, sadece farklı parametrelere ve markalaştırmalara sahipler. Ancak bu ikisi en önemlileri.

CryptoNote teknolojisi sadece başka bir algoritma

değil. Aksine, tamamen anonim ya da en azından Bitcoin'den daha anonim işlemlere imkân tanıyan bir anahtar imzası kullanıyor. Halka imzası olarak bilinen bir teknoloji kullanıyor. Bu işlemlerin doğru kişi tarafından gönderildiğini doğrulamak için bir resmin matematiksel dengini kullanıyor ama bu anahtar, dışarıdan bilgi olmadan o kişiyi doğrulamak için kullanılamaz. Ayrıca, her işlem yeni bir adres oluşturuyor, o nedenle sadece gönderici nereye gittiğini biliyor.

Bytecoin (BCN) –uzun zaman önce ölen doğrudan Bitcoin klonu olan Bytecoin (BTE) ile karıştırmayın– CryptoNote teknolojisinin ilk uygulamasıydı. Piyasaya sürülüşü hâlâ gizemini koruyor. Muhtemelen Doğu Avrupa ya da Rusya kökenli olan paranın 2012'den beri Derin Ağ'da gizli bir şekilde çalıştığı söyleniyor. Topluluğun büyük bir kısmı bu resmi hikâyeden şüpheli ve Bytecoin'in geçmişi CyrptoNote'un şu anki itibarı üzerinde bir leke olarak kaldı. Buna ek olarak, Bytecoin'de ciddi ölçüde gizlice ön çıkarım yapılmış olması, birçok Bitcoin kullanıcısının onu göz önünde bulundurmayı dahi elemesine neden oldu.

Monero piyasaya sürüldüğünde, Bytecoin'in neredeyse karbon kopyasıydı ama Bytecoin'e sorun çıkaran ön çıkarımı terk etti. Anonim yapıları gereği CryptoNote coin'lerinin dağılımını görmek imkânsız olsa da, Monero en başından yenilik getirmemesine rağmen, genellikle iki coin'in daha 'adil' olanı olarak görülüyor.

Namecoin

Algoritma: SHA256

Madencilik Türü: İş ispatı (PoW — proof-of-work)

Blok süresi: 10 dakika
Zorluk Yeniden Hesaplaması: 2016 blok
Blok Ödülü (güncel): 25NMC
Toplam Dash Sayısı: 21 milyon

Namecoin ilk 'Bitcoin 2.0' ya da 'Cyrptopara 2.0' projesiydi. Nisan 2011'de piyasaya sürüldü ve internette bazılarının endişelendiği isim tescili merkeziyetçiliği ve sansür sorunları konusunda özgün bir çözümdü.

Ancak, bir Bitcoin 2.0 projesinin başarılı olması için tek gereken, faydalı ve kullanılabilir bir sistem değildir. Namecoin büyük ölçüde bir başarısızlık ya da en azından potansiyelini asla gerçekleştiremeyecek bir şey olarak görüldü. Geleneksel sistemlere özgü mevzuatlardan ve sansürden muaf, merkezsizleştirilmiş isim tescili gazetecilerin, aktivistlerin ve internetin yasal saçaklarında bulunanların işine yarayabilir. Ama Namecoin'in kullanıcılarının erişimine verdiği .bit alan adı daha sonra kâr etmek için satmayı uman adreslerin üzerinde oturan şirketler dışında çok fazla insan tarafından ilgi görmedi. Bu internetin ilk günlerinde .com web adreslerine yerleşen şirketler ve bireylerden pek farklı bir durum değil.

İşe yarar .bit alan isim kombinasyonları park şirketleri tarafından tutulurdu (başka şirketlere satmak için alan adı satın alan şirketler) ve sırf .bit sitelerini taramak için göz korkutucu Namecoin blok zincirini indirme zorunluluğu .bit sitelerini gezen insan sayısında çok az artışa neden oldu. Birçok gizli hizmet o grupların gizliliği açısından daha güvenli ve daha fazla erişime sahip olan Tor'u kullanmayı tercih ediyor. Yine de Namecoin kullanım alanını

bulabilir. Birçok kişi onu çoktan silmiş olsa da, bunu yapmak için o kadar aceleci davranmazdım. Birleşik altcoin piyasası şu anda sahip olduğu piyasa büyüklüğünü destekleyemiyor. Bitcoin'in yerini dolduramadığı faydalı özellikleri ya da piyasa talebi olan yeterince para birimi yok. Bu bir spekülasyon; ama ben mantıklı olduğunu düşünüyorum: işe yaramaz ve çok az işe yarar coin'ler tükenene kadar altcoin piyasası küçülmeye devam edecek. Topluluk 'tükenmenin' tam olarak ne olduğunu tanımlamadı ama bu tanımın yakında yazılacağına inanıyorum.

Toz duman dağıldığında, ister yavaş bir kan kaybı ister hızlı ve kesin bir yıkım olsun, sadece işe yarar coin'ler ayakta kalacak. Fiyatın, bir coin'in uzun vadeli finansal kapasite göstergesi olduğuna inanmıyorum. Kulağa idealistlik gibi geliyor ama en nihayetinde bir coin'in ayakta kalması üç şeye bağlıdır: topluluğunun fedakârlığı, geliştiricilerinin yeteneği ve eşsizliğinin cazibesi.

Namecoin, birçok coin'in sahip olmadığı bir avantaja sahip: İlk ortaya çıkan altcoin'lerden biri olduğu için, teknolojinin ayakta kaldığını görmek isteyen geliştiricilik geçmişine sahip çok sayıda bilgili yatırımcıları var.

Eski Namecoin geliştiricisi ve savunucusu Michael Dean teknolojinin 'öldüğünü' söyleyerek karşı çıkıyor. Birçok şeyin yanı sıra, geliştiricileri benimsenmesi ve kullanılabilirliğine odaklanmadığı için coin'in hiçbir zaman beklendiği gibi bir çıkış yapmayacağına inanıyor:

Popülerleşmek için neredeyse dört senesi vardı, ama hiç benimsenmedi. Yüz binlerce oturan alan adı var ama sadece 30 gelişmiş Nokta-Bit sitesi var. Bunların hepsi Nok-

ta-Com, Nokta-Net ya da Nokta-Org sitelerinin (sansüre karşı çokluk ve koruma sağlaması için muhtemelen öyle olmalı) ikizleri ve o 30 sitenin yarısı benim.

MeowBit ve FreeSpeechMe yüklemelerine dayanarak, Dünyada Nokta-Bit sitelerini ziyaret etmek için gerekli yazılımı kuran muhtemelen beş binden daha az insan var. Namecoin'in madenciliği ve alım-satımı fazlasıyla yapıldı, bekleyen birçok alan adı var ama alan inşa etme ya da çözücü kullanımı neredeyse hiç yok.

Dean birçok iyi noktaya dikkat çekiyor ve geliştiricilerin genel görünümden ziyade ufak şeyler hakkındaki bariz ısrarları coin'e ciddi ölçüde zarar vermiş olabilir. Ama bu uzun vadede önemi olmayabilir. Düşmanca bir ICANN (şu anda internetteki alan adı kaydını kontrol eden oluşum) idaresiyle ilgili endişelerinde haklılık payı olsa da, daha yetenekli biri onu hayata döndürmeye çalışana kadar Namecoin'in ayakta kalacağını düşünüyorum.

İşe yarar adresler park şirketleri tarafından satın alınmış olsa bile, sonuçta .bit adreslerinin hakkı Namecoin'in elinde. Bu değerli, çünkü .bit kötü bir alan adı sistemi değil; akılda kalır ve birçok şirketle ilgili. .bit adreslerinin sıradan tarayıcılara eklendiğinde, her ne kadar küçük ya da büyük olursa olsun, dünya sansürsüz bir internete kavuşacak.

Bu gerçekleşecek mi? Emin değilim. Bu konuda bahse girmezdim. Öte yandan, Namecoin'i Dean kadar kolay bir şekilde silip atamazdım. Dürüst olmak gerekirse, son birkaç senedir coin'i yükselişe geçirmeye çalışırken, ben sadece bir dış gözlemciyim. Kopya coin'lerin bile .bit adreslerini toplamaları yasaklandı, o nedenle hem açık kay-

naklı olup hem de daha düşük dereceli bir coin tarafından doğrudan kopyalanması önlenen Namecoin kripto paralar arasında son derece nadir bir konuma sahip. Başka biri benzer bir sansürsüz internet yaratabilir ama bunu yapmak içim kullanılmamış başka bir alan adı uzantısı düşünmek zorundalar.

Namecoin, altcoin'lerin bu çağında kötü performans gösterdi, çünkü bu çağ tamamen spekülatif alım-satıma odaklandı. Altcoin'lerin bir sonraki çağında bunun önemi olmayacak. Asıl önemli olan Namecoin'in ayakta kalmak için bir sebebinin olup olmaması ve bunu başarıp başarmaması. Bu, *ayakta kalacağı* anlamına gelmez ama hiçbir coin'in sahip olmadığı bir avantaja sahip. Geliştiricilerinden bazıları bunu unutmuş olabilirler ama ben hâlâ bunun önemli olduğunu düşünüyorum.

Blackcoin
Algoritma: Uygulanmaz
Madencilik Türü: Proof-of-Stake '3.0' (PoW/PoS ilk dağılım için kısa melez dönem)
Blok süresi: 1 dakika 4 saniye
Blok Ödülü: yıllık %1
Maksimum Blok Boyutu: 1 MB
Toplam Sayı: Sınırsız; güncel ~74.5 milyon + <%1 yıllık faiz

Blackcoin, yenilikleri fiyatına yansımasa da, kripto para topluluğuna getirdiği çok sayıda özellik nedeniyle etkileyici oldu. Blackcoin'in fiyatı 2014'ün başından beri gerileme halindeydi ama topluluğu yakın gelecekte hiçbir yere gidecek gibi görünmüyor.

Blackcoin'in para sistemine diğer kripto para birimlerinden daha az bağlı olan ve ağı güvenceye almayı amaçlayan kendi proof-of-stake ('Proof-of-Stake 3.0' ismi verilen) versiyonu var. Ayrıca, Blackcoin'in geliştiricilerinin kripto paraları güvenceye almak için proof-of-stake yöntemi üzerinde çalıştıkları söyleniyor.

Blackcoin'in en önemi başarıları büyük potansiyeli olan iki yazılım BlackHalo ve NightTrader'dır. BlackHalo çifte depozito havuz sistemi olan bir akıllı kontrat sistemidir. NightTrader, indirilebilir oyunlar ve e-kitaplar gibi dijital ürünler için merkezsizleştirilmiş bir pazardır. Bir aracıya bağlı olmayan işleyen bir havuz sistemi olan merkezsizleştirilmiş bir dijital ürün pazarında buluşuyorlar ve BlackHalo havuz sistemi görevi görüyor. Çift depozito sistemi oluşturulduğu zaman bir yenilikti. Kullanıcı deneyimi açısından hâlâ kat etmesi gereken uzun bir yol var. Belki de bu yüzden ve kullanıcıların tam Blackcoin düğümü çalıştırmalarındaki ısrarı nedeniyle, teknolojinin benimsenmesi yavaş oldu.

BlackHalo'nun baş geliştiricisi David Zimbeck'in Bob-Surplus adındaki kötü şöhretli bir 'şişir ve boşalt' grubu ve BTER'le birlikte bir coin oluşturup fiyatını artırarak yapay olarak coin'in ilk satış fiyatını şişirdikleri BTER/Baybit skandalına karışması işleri iyice zora soktu. Zimbeck proje hayata geçene kadar bunun farkında olmadığını iddia ediyor ama onun itibarına ve Blackcoin'e ciddi ölçüde zarar verdi.[8]

[8]DeMartino, Ian M."Chat Logs Allegedly Show Bter Creating and Pumping Its Own Coin." CoinTelegraph. 3 Ocak 2015. Erişim tarihi 22 Haziran 2015.

Ancak Blackcoin'in hâlâ sadık bir topluluğu ve, Zimbeck olsun ya da olmasın, oldukça rekabetçi bir geliştirici ekibi var. Nxt'inki kadar geniş değil ve Bitcoin'in devasa topluluğunun yanına yaklaşmıyor, ama bünyesindeki geliştiriciler yetenekli olduklarını kanıtladılar.

Blackcoin, coin'in düğümlerinin büyük kısmının bulunduğu Çin'de de ilerleme kaydetti.

Bir altcoin'in fiyatı önemlidir, çünkü çok düşerse insanların ilgisini çekmez. Aksi takdirde, günlük işlemlerin dışında fiyatını takip etmenin pek anlamı yoktur. Önemli olan piyasa oturana kadar bir coin'in ayakta durup durmayacağıdır. Şu anda, piyasa meşru ve sahtekârlık coin'leriyle dolup taşmış durumda. Eninde sonunda bu aşırı doygunluk altcoin ekosisteminin çökmesine neden olacak. Ayakta kalmayı başaran coin'ler avantajlı konumda olacaklar.

Blackcoin'in bunu başarma şansı var, çünkü geliştirici ekibi insanları bir süre daha oyalayacak kadar yetenekli. Önünde uzun bir yol var, çünkü görünen o ki, işe yaramaz sahtekârlık coin'leri bile kolay kolay bitmiyor.

Ethereum

Algoritma: Ethash
Madencilik Türü: İş ispatı (PoW) (Yeni proof-of-stake yöntemine geçme planları olan Proof-of-Work)
Blok süresi: Ortalama 20 saniye
Blok Ödülü: 5 Ether
Maximum Blok Boyutu: 1 MB
Toplam Sayı: Limitsiz

Bitcoin'den sonra belki de en heyecan verici kripto

parayla bitiriyorum. Ethereum bir coin'den daha fazlası, kendisini şöyle tanımlıyor: "Ethereum akıllı kontratlar işleten merkezsizleştirilmiş bir platformdur: aksama süresi, sansür, sahtekârlık ya da üçüncü parti müdahalesi ihtimali olmadan programlandığı şekilde çalışan uygulamalar. Ethereum internetin işlemesi gerektiği gibidir."

Nxt ve CounterParty'de olduğu gibi, varlık/token oluşturmaya imkân tanıyor. Dahası Ethereum'un kendi programlama dili var ve bu, fazlasıyla heyecan verici projeler meydana getirdi. Aralarında Augur coin'i olanların bir öngörünün gerçekleşip gerçekleşmeyeceği üzerine oy kullanmaya teşvik edildiği, kalabalığa dayanan öngörü piyasası Augur var. (Bunun nasıl işlediği ve insanların dürüst olmalarının nasıl sağlandığı, bu bölümün kapsamı dışında.)

Ethereum'da sistemin işlemesini sağlayan, ağı güvenceye alan ve kontratları bağlayan Bitcoin'e benzeyen Ether adında bir coin var.

Ancak, manşetlerde daha çok yer alan, dünyanın farklı yerlerindeki büyük teknoloji şirketleri, bankalar ve finansal kuruluşların Ethereum kullanarak projeler üzerinde çalıştıklarını duyurmalarıydı. Bu noktada detaylar zayıf, ama UBS ve Barclays Ethereum'la ilgilendiklerini duyurdular ve Microsoft bulut bilişim hizmetinde belirli bir kapasitede Ethereum sunarak geliştiricilerin Ethereum uygulamaları yaratmalarını kolaylaştırıyor.

Dış dünyadan Bitcoin dışında bir kripto paranın böylesine bir destek gördüğü duyulmamıştır ve Ethereum'un ileride başarılı olacağının en büyük işaretidir. Topluluğun hem içinden hem de dışından gördüğü destek konusunda çok ileride olan Bitcoin gibi olması için önünde uzun bir yol var.

Ethereum altcoin dünyasındaki diğer coin'lerden çok daha üstün olduğunu kanıtladı. Ürünün piyasaya sürülmesi beklenenden daha uzun sürünce, bazıları onu eledi. Ama piyasaya sürüldüğünde, ana akım dünyanın ilgisini çekmiş görünüyordu. Diğer coin'lerin güçlü özellikleri var, ama Ethereum kendi programlama diline sahip. Bu, programlama tecrübesi olmayan birçok insana pek fazla bir şey ifade etmiyor ama anlaşılan onunla ilgilendiğini belirten büyük oluşumlar için durum farklı.

Bir kripto paranın özelliğinin kullanılabilirliği doğrudan onu kullanan insanların sayısı ve kalitesine bağlantılıdır. Eğer bir varlık piyasasını kullanan biri yoksa ya da sadece dolandırıcılar kullanıyorsa, pek işe yarar olduğu söylenemez.

Ethereum'un dış dünyadan ilgi görmesi, bana kalırsa, altcoin dünyasının nihayet sağlamlaştığının bir işaretidir. Birçok altcoin başarısız olacak; aslına bakılırsa, çoğu çoktan başarısız oldu. Çünkü sayıları çok fazla. Ama birkaçı kullanım alanı bulacak, hatta günün birinde bir ya da ikisi ana akım ekonomimizin bir parçası bile olabilir. Ethereum dışındaki altcoin'lere cebinizdeki bozuk paralarınızdan daha fazla para yatırmamanızı öneririm. Ama bu altcoin'lerin dikkate değer olmadıkları anlamına gelmez. Anonim coin'ler, varlık oluşturan Bitcoin 2.0 coin'leri ve Ethereum gibi merak uyandıran teknolojiler gelecekte ekonomimizde bir tür rol oynayacaklar.

Yirmi İkinci Bölüm:

Yaygın Otonom Şirketler, Denetim ve Niş Pazarlar

Son yirmi senenin en heyecan verici icatlarından biri ve finansal hizmetler, ticaret ve yönetim için merkezsizleştirilmiş güvenilir uygulamalar kuran bir platform olduğuna inandığım için bitcoin'e tutkunum. Bir para biriminden çok daha fazlası olan bitcoin, paranın internetidir. Para birimi sadece ilk uygulama!

— Andreas Antonopoulos, 15 Ocak 2015,
Reddit AMAA (Ask Me Almost Anything)

Bitcoin'in geleceğini tahmin etmek zor. Savunucuları, ben de dahil, Bitcoin'in *gelece*ğin ta kendisi olduğunu söylerler.

Bitcoin'in mevcut projelerinin çoğunu çoktan ele aldım. Yakın gelecekte bu araçların gelişiminin yanı sıra daha kullanıcı dostu hizmetler göreceğiz ve umarım farklı cüzdanlar ve ödeme işlemcilerinin müşterek çalışmaları artar.

Blok boyutu hakkında süregelen tartışmalar bu kitabı

okuduğunuz sırada çözülmüş olabilir ya da olmayabilir, ama Bitcoin blok zincirinin boyut sınırının artıp artmayacağı ya da yan zincirler geliştirmeye ihtiyaç olup olmayacağı konusunda kalıcı çıkarımlar olacak. (Yan zincirler Bitcoin'i daha fazla insan tarafından kullanılır yapmak için bir tekliftir. Onlar Bitcoin blok zincirinden ayrı olarak işlemlerin izini sürmeleri için tasarlanan blok zinciri türleridir. Yan zincirler işlemleri daha sonra kriptolu bir şekilde kontrol edilebilen sıkıştırılmış biçimde Bitcoin blok zincirine tek seferde eklerler.)

Bu sorunlar bir şekilde er ya da geç çözülecek ama Bitcoin ayakta kalacak. Sonucunda zarar görebilir, hatta birkaç sene geride kalabilir ama Bitcoin devam edecek. İnsanlar ona o kadar çok yatırım yaptılar ki, ilerlememesi için bir sebep yok. Bir bitcoin'e $800 ödeyen insanlar ondan sekiz sente vazgeçmeyecekler. Bitcoin'in bir fiyatı olduğu sürece, ağ işlevini sürdürebilir. Hakkında birçok ölüm ilanı yazıldı[1] ve tekrar yazılacak. Ama fiyatına ne olursa olsun, ağ ayakta kalacak.

Uzak gelecekte olabilecekleri yakın gelecekte olabileceklerden daha ilginç bir soru.

Daha genel anlamda bakacak olursak, beş sene göz açıp kapayıncaya kadar geçer, ama kripto para dünyasında, bu bir ömürdür. Andreas Antonopoulos Bitcoin'e iki sene verilmesini söyledi.[2] Bu değerlendirmeye katılmıyorum,

---

[1]Last, Jonathan V. "Bitcoin Is Dead." 5 Mart 2014. Erişim tarihi 22 Haziran 2015. http:// www.weeklystandard.com/blogs/bitcoin-dead_784187.html

[2]Bundrick, Hal M. "Andreas Antonopoulos: 'Give Bitcoin Two Years.'" 8 Şubat 2015. Erişim tarihi 22 Haziran 2015. http://insidebitcoins.com/news/andreas-antonopoulos-give-bitcoin-two-years/29708

çünkü Bitcoin beş ya da on sene boyunca bir niş ürün olarak var olabilir ve sonra doğru ürün ya da uygulama yaratıldığında patlayabilir. Bu çeyrekte ya da yılda kâr bekleyen yatırımcılar için bu iyi bir haber olmayabilir ama bu gerçekleşebilir. Apple Pay ve PayPal kumar, porno ve diğer gri ya da kara borsa ürünler açısından hiçbir zaman Bitcoin kadar iyi olmayacaklar. Bu pek de sevilen bir iddia değil –ve Bitcoin'in, mevcut biçiminde bile, bundan çok daha faydalı olduğunu düşünüyorum– ama hiç olmazsa, bunlara sahip. Ve bunlara her zaman sahip olacağı için insanlar onu hep kullanacaklar. İnsanlar onu kullandığı sürece, bazı yenilikler ve onun için daha fazla ya da daha iyi kullanım alanları yapacak bir kodlayıcı, bir kurcalayıcı olacak.

Bu olduğu sürece, Bitcoin'in her zaman bir şansı var.

Ama Antonopoulos'un öngörüsü bir noktayı açıklıyor: kripto para dünyasında her şey çok hızlı ilerliyor. İki sene onda yer edinen insanlar için neredeyse akıl almaz bir süre. Biraz daha sabırlı olmanızı öneririm ama mesele açık: O zamana kadar birçok şey belirlenecek. Yeni bir teknoloji konusunda herhangi bir öngörüde bulunmak çok zor, çünkü geriye dönüp bakıldığında bariz kullanımlar mevcutken değişiklikler köklü bir şekilde güçlendiriliyor. Ağ tarayıcılar ortaya çıkmadan önce AltaVista, Geocities ve ICQ'yu tahmin etmeye çalıştığınızı düşünün ve sonra AltaVista, Geocities ve ICQ hâlâ internetin ana dayanak noktaları olduğu 2000'de Facebook, Reddit ve Google Earth'ü öngörmeye çalışın.

Haklı olduğum kadar sık bir şekilde yanılacağımı farz edersek, kripto para harikalar diyarında ne tür hizmetlerin gelişeceğini görüyorum?

İnanılmaz hizmetler.

Altcoin'ler şu anda spekülatif yatırım tarafından rahatsız ediliyorlar. Alandaki her şeyi iten bu. Fiyat düşerse, topluluk geliştiricilerin bir şey duyurmasını talep ediyor. Her coin'in topluğu bir sonraki 'devrimsel' özelliğin getireceğinden emin oldukları büyük sıçrayışı bekliyor gibi görünüyor.

Bu fiyatı yukarı çekmekte genellikle başarısız oluyor ve sonra topluluklar ve geliştiriciler cesaretlerini yitirebiliyorlar.

Bana kalırsa, altcoin alanından gelen en önemli ve ilginç yenilikler –hem alternatif kripto paralar hem de Bitcoin üzerine kurulan 'coin'ler'– fiyat peşinde koşmanın faydasız olduğunu fark eden topluluklardan gelecek.

Daha önce popüler teknoloji sitesi Ars Technica'nın yarattığı Arscoin hakkında konuştum. Kısacası, gerçekten kötü bir coin'di. Merkeziydi, kopyala ve yapıştır kodu kullanılmıştı ve iyi planlanmamıştı. Ama hiçbir zaman olmadığı bir şey gibi yapmadı ve bir grup insanın önemsediği bir kullanım alanı vardı: yorumlarındaki isimlerinin renklerini değiştirebilmelerinin yanı sıra, yanına koyabilecekleri küçük sanal şapkalar almalarına imkân tanıyordu.

Hepsi bu. Arscoin'i diğer Arscoin kullanıcılarına göndermek dışında onunla yapabileceğiniz en iyi şey bu. Ama işe yaradı ve hak ettiğinden çok daha popüler oldu. Coin en sonunda kapatıldı, çünkü Ars Technica kaynaklarını ve zamanını bir kripto parayı idare etmek için harcamak istemedi, ama bu deney insanların gerçekten istediği bir işleve sahip olmanın hızla başarıya götürdüğünün bir kanıtıydı.

Bu insanların kullanmak istediklerini *söyledikleri* bir iş-

levden farklıdır. Herkes merkezsizleştirilmiş bir piyasa istediğini söyledi ama mevcut olanları kaç kişi kullanıyor? Belki de, bir sonraki Mt. Gox benzeri fiyaskodan sonra, insanlar onun için daha fazla kullanım alanı bulacaklar, ama insanlar piyasaların hızlı ve özelliklerle dolu olmalarını bekliyorlar. Ana akım topluluk ve sabit fikirli amatörlerin bir kripto paradan istedikleri şeyler arasında çok büyük fark var.

Yapılabilecek en mantıklı şey biraz fazla hırslı ve belki de zamanının ötesinde olan ama yine de büyüleyici bir teknoloji ve konseptle sergilenebilir.

Counterparty kullanılarak kurulan LTBCoin çizelgelerde yukarı fırlamıyor. Fiyatı sönük ve işlem hacmi düşük, ama ilginç bir konseptti ve hâlâ öyle. Kripto para kullanılarak kendini idame ettiren bir ekonomi yaratmak için belki de ilk gerçek girişimdi.

$30,000'dan biraz daha yüksek bir piyasa değerine sahipken artık ekonomisinin 'kendini idame ettirdiği' söylenemez.[3] Hiç kimsenin kirasını LTBCoin ile ödediğini sanmıyorum. Ama bir konsept ve gelecek projesi olarak büyüleyici. Counterparty platformuna kurulmuş olması Bitcoin blok zinciriyle güvenceye alındığı anlamına gelir. Eğer popülerliği azalırsa, ağ güvenliği için endişelenmeye gerek olmaz.

LTBCoin Let's Talk Bitcoin'in resmi token'ıdır. Let's Talk Bitcoin Bitcoin odaklı popüler bir sesli yayın olarak başladı. Popüleritesi arttıkça, yayın sayısı arttı ve en sonunda LTBCoin denilen sosyal deneye başlandı.

[3]"Crypto-Currency Market Capitalizations – LTBCoin." Chart. CoinMarket Cap. Erişim tarihi 22 Haziran 2015. http://coinmarketcap.com/assets/ltbcoin/

Coin'ler belirlenen bir zamanda içerik yaratıcılarına ve dinleyicilere/izleyicilere dağıtılıyor. LTBCoin'den piyasada 510 milyon bulunuyor ve 2014'te piyasaya sürüldükten yaklaşık beş sene sonra hepsi dağıtılmış durumda.

2019'da LTBCoin'in nerede olacağını bilmiyorum ama şu anda bulunduğu nokta çok ilginç. LTBCoin'in bir parçası olan sesli yayınlarda her hafta sihirli bir kelime veriyorlar. Dinleyiciler daha sonra sihirli kelimeyi girerek o haftalık LTBCoin stoklarını alabiliyorlar. O LTBCoin'ler Bitcoin satın almak, LTBCoin ağında reklam alanı satın almak ya da ağda kendi blogunuzu satın almak için kullanabilirsiniz. Ayrıca, makale yayınlayarak ya da kendi açık artırmalarınızı düzenleyerek coin kazanabilirsiniz.

Bu kitabı yazdığım sırada, LTBCoin cephesi oldukça sessiz ama daha fazla izleyici çekeceği umulan yeni bir web sitesi geliştiriliyor. Bu sadece coin'le birlikte satın alınabilen reklam alanı sayesinde coin'i değerlendirecek.

Yine de, başka hiçbir yerin sunmadığı bir şey sunduğu için değerli olan kendi kendini idame ettiren bir ekonomi fikri büyüleyici bir şey. 2014'te, bir coin'in spor dünyasında ne yapacağını düşünerek bu konseptle ilgili bir yazı yazdım.

Bildiğiniz gibi, spor dünyası ateşli insanlarla doludur. Her takımın bütün sporların taraftarlarının geniş alt kültüründe yer alan spor türünün taraftarlarının da alt kültüründe bulunan kendi küçük alt kültürü vardır.

Takımların aynı zamanda taraftarlara hitap eden kendilerine özel ürünler yapmak için neredeyse müstesna bir yeteneği var. Bir oyuncu ya da antrenöre bir şey imzalatmak kadar kolay. Bazı takımlar çoktan benzer fikir-

leri deneyip sık uçan yolcu miline benzer ürünler markalaştırdılar. 2014'de yazdığım makalemde, maçlara erken gelen sezon bileti sahiplerine, kalabalık belirli bir gürültü seviyesine her ulaştığında ya da takımın resmi maç sonrası şovunu izleyenlere verilecek 'Jet Puan' planını açıklayan New York Jetleri'nden ilham aldım. Jet Puan'ı sezon bileti satın almak için gereken nefret edilen ve pahalı Kişisel Koltuk Lisansı'na (KKL) değer kazandırmak için ortaya çıkarıldı. Bunun bir kripto para olarak nasıl görüneceği hakkında şöyle yazdım:

> Jetler anlık para değeri olan ama sadece [Jet Coin ile] alınabilen özel ürünler satabilirler. Bu Jet Coin'e (ya da adını her ne koyarlarsa) anlık değer kazandırır. Eğer değerli bir koleksiyon ürünü –örneğin [Onur Listesi'nde yer alan Oyun Kurucu] Joe Namath'ın giydiği bir üniforma gibi– piyasaya sürülürse yüz binlerce Jet taraftarı onu ister ve KKL sahiplerine onu satın almak için gerekli olan Jet Coin'leri ödemeye razı olurlar. Özünde, Jetler ve taraftarları kendi para birimlerine sahip olacaklar ve takımı (parasal olarak) en çok destekleyenler bunun faydasını görecekler. Ama bu aynı zamanda çok uzakta yaşayan Jet taraftarlarına bir koleksiyon parçasına sahip olmaları ya da Jetlerin sahibi Woody Johnson'la akşam yemeği yemek gibi hayatta bir kez karşılaşılan bir fırsatı satın alabilmeleri için güvenli bir seçenek sunacak.[4]

[4]DeMartino, Ian M. "How Bitcoin Could Change How We Interact With Sports." CoinTelegraph. 13 Nisan 2014. Erişim tarihi 22 Haziran 2015. http://cointelegraph.com/ news/112268/op-ed-how-bitcoin-could-change-how-we-interact-with-sports

Bilet sahipleri sadece izlemek istemedikleri maçların biletlerini satabilecekleri için değil, aynı zamanda mümkün olduğunca çok maça gitmenin karşılığında kripto parayla ödüllendirilecekleri için birdenbire KKL bir yatırım aracı olur. Bu para birimi kişiye özel bir koleksiyon parçası kazandırmanın yanı sıra, o koleksiyon parçası serbest piyasada isteyen insanlara satılabilir. Gerçek Jet Puanları transfer edilemez ama bir potansiyel Jet Coin'i transfer edilebilir.

Zamanla LTBCoin gibi daha fazla niş ekonominin ortaya çıkacağına inanıyorum. Bu kitabı tamamlamadan kısa bir süre önce, Uphold sanal gerçeklik içerik yaratmada para birimi olması için tasarlanan kripto para Voxel'i duyurdu. Gelecekte başka neler olacak?

Bitcoin'in etrafını saran en çarpıcı konseptlerden biri merkezsizleştirilmiş yönetim fikridir. Demokraside insanların yönetimlerini seçtiği söylenir ama bu tam olarak doğru değil, özellikle de Birleşik Devletler gibi demokratik cumhuriyetlerde. İnsanların asıl kastettikleri hükümetlerinin bakış açılarının seçilebilmesidir. Bir ABD vatandaşı, hükümetini Fransız yönetimine dönüştürmek için oy veremez. İdeal bir durumda, hükümeti Fransız yönetimine –ya da hangi yönetimi tercih ediyorlarsa– *benzer* bir şeye dönüştürmek için oy kullanabilirler, ama yine de ellerindeki hükümete mecburlardır.

Bu çok kötü, çünkü baskıcı rejimlerde yaşayan insanların tek suçu yanlış yerde doğmuş olmalarıdır. Dünyamız giderek globalleşiyor ve sınırlar zamanla daha az anlam ifade ediyor. Onları önce ulaşım yıktı. Arabalar ve uçaklar sayesinde sınırlar hiç olmadığı kadar hızlı geçiliyor. Daha

sonra, sınırlar arasındaki iletişimi internet yıkarak çizgiyi iyice belirsizleştirdi. Günümüzde, Bitcoin sınırlar arasındaki finansal ayrılığı belirsizleştiriyor. Gelecekte, blok zinciri idaresi bu sınırları tamamen ortadan kaldırmaya yaklaşabilir.

Neden yönetimimi seçemiyorum? *Gerçekten* yönetimimi seçmeyi kastediyorum. Ben özgürlükçü ya da anarşist değilim; birilerinin yollar, hastaneler ve, evet, ordu için bile para ödemesi gerektiğini anlıyorum, o nedenle hükümetlere muhtemelen her zaman vergi ödeyeceğiz.

Ama bütün diğer şeyler bir seçenek olamaz mı? Sosyal Güvenlik için maaşımın bir kısmını hükümete vermek yerine, onu bir Bitcoin hesabına göndersem ne olur? O Bitcoin hesabına yüz binlerce insan katkıda bulunsa ne olur? Emekli olduğumda o parayı geri alacağımı garantileyen bir program yazılabilir. Bana kalırsa, birçok kişi Birleşik Devletler hükümeti ve Sosyal Güvenlik idaresinden ziyade ona güvenir.

Oy verme mekanizması kurularak ilk kez uygulanabilir doğrudan bir demokrasi yaratılabilir. Hatta sigorta bile idare edilebilir; biri işteyken yaralanır ve çalışmayı bırakmak zorunda kalırsa, grubun geri kalanı o kişinin erken emekli olmayı hak edip etmediğine ve emekliliğin nasıl idare edileceğine karar verebilir.

İnsanların böyle bir durumda her zaman 'hayır' oyunu vereceğini düşünebilirsiniz, ama ben insan ruhuna bundan daha çok güveniyorum. Ayrıca, rakip yönetimler olacak; eğer A Yönetimi zor durumdaki vatandaşlarıyla ilgilenmiyorsa, insanlar B Yönetimi'ne katılmaya karar verebilirler.

Rekabetçi sistemler kurulabilir: bir kişi bütün katkı-

ların yüzde beşini sosyal güvenlik ağı için kenara ayrılan bir hükümete katılırken, daha özgürlükçü sistemler yüzde bir, hatta yüzde sıfır bile katkıda bulunabilirler.

Söylemek istediğim şu: İnsanlar istedikleri yönetim biçimini seçebilirler. Bölgesel yönetiminize karşı her zaman bazı yükümlülükleriniz olacak, çünkü global bir hükümetin karşılayamayacağı belirli yerel ve bölgesel ihtiyaçlar var. Ama hükümetin idare ettiği yerel ya da bölgesel düzeyde olmayan sayısız görev var ve bu hizmetler işbirlikçi ve gönüllü olarak halledilebilir. Bitcoin'den önce, özgürlükçü olmaktan ziyade sosyalisttim. Ama artık kripto paralarla kurulan sistemlerin özgürlükçü ideallerin bireysel özgürlüklerini ve ilerici insanların arzuladığı sosyal güvenlik ağlarını tatmin ettiğini öngörebiliyorum.

Uzak bir gelecekte, yerel ve bölgesel ihtiyaçlar blok zincirinde idare edilebilir. Bireysel kasabaların kendi blok zincirleri ve coin'leri olabilir. Vatandaşlar okullara, yollara, polise ve diğer her şeye ne kadar para ayrılması gerektiği konusunda cep telefonlarıyla, bilgisayarlarıyla ya da gelecekte ne tür tuhaf teknoloji kullanacaklarsa onunla doğrudan oy verebilirler. Böyle bir şey olacaksa bile, bundan onlarca yıl sonra olabilir ya da daha yakın gelecekte küçük topluluklarda denenebilir.

Sanal gerçeklik Bitcoin'in yanında büyürken başka bir olasılık ortaya çıkıyor. Sohbet odalarının sanal gerçeklik versiyonlarında şimdiden topluluklar gelişiyor. Sanal 'yerler' giderek daha kalıcı olurken, tam gelişmemiş yönetimlerin ortaya çıkmasını öngörmek mantık dışı olmaz. Eğer böyle bir şey olursa, onları blok zincirinde idare etmek çok akıllıca olur. Bu toplulukların eninde sonunda bir para bi-

rimine ihtiyaçları olacağından ve kripto paraların dijital dünyada çalışacak şekilde tasarlandıklarından bahsetmeye bile gerek yok.

Geleneksel hükümetlerin tamamen ortadan kalkacaklarını söylemiyorum; çok az kişi bu kadar iyimser olabilir. Nathan Wosnack iNation'ın –bu konsept üzerinde çalışan birkaç şirketten biri– kurucu ortaklarından biri ve gelecek için umutlu olsa da, temkinli olmayı elden bırakmamayı öneriyor:

> Hükümetin Belgeler/Tapular, Eğitim, Pasaportlar ve Evliliklerden tamamen elini çekeceğine inanıyor muyum? Elbette hayır, kontrolü sağlamak istiyorlar. Daha az güvene ve hükümet tarafından idare edilen merkezi sistemlerden uzaklaşmaya ve eşler arası, bilginin demokratikleştirildiği merkezsizleştirilmiş ağlara doğru agorist ve özgürlükçü bir hareket var. Doğal olarak, daha fazla güvenlik (şifreleme), blok zincirinin doküman doğrulaması ve düşük genel giderlere karşı (iNation) gibi alternatif sistemlerin sunduğu ücretlerle, hükümetin özel rekabetin idare alanına girdiğini kabullenmekten başka seçeneği olmayacak. Bunun ilk olarak gelişmiş ülkelerde olduğunu görüyoruz ve gelişmekte olan ülkeler de eninde sonunda onları izleyecekler.

Aslına bakılırsa, gelişmiş ülkelerin vatandaşları merkezsizleştirilmiş yönetimleri pek kullanışlı bulmayabilirler. Onların gözüne, sigortanızı sigortalamak kadar gereksiz bir lüks gibi görünebilir. Ama sosyal güvenlik ağının var

olmadığı ülkelerde, bürokratlar ve zorbalardan ziyade matematiğin güvenceye aldığı merkezsizleştirilmiş güvenlik ağlar daha fazla kullanım imkânı bulabilir.

'Hükümetinizin sonu' sigortası olarak bile faydası olabilir. Emekli olduğunuzda Sosyal Güvenliğin geçerli olup olmayacağından emin değil misiniz? 401(k)'nin en sonunda işe yarayacağını vaat eden bankacılara güvenmiyor musunuz? Bitcoin fiyatını sabitlerse, felaket getiren hükümet yıkımlarına karşı uygulanabilir bir koruma sağlayabilir.

Bu hükümetleri kimlerin idare edeceği, kimlerin dijital krallıkların kralları ve kraliçeleri olacağı gibi soruların yanıtları henüz belli değil. Onların matematikle kurulan ve sonra serbest bırakılan doğrudan demokrasiler olacaklarını tahmin ediyorum. Ne zaman ve ne hakkında oy kullanılacağı gibi bütün sistemi etkileyen sorunlar kullanıcı girdisi ve kod kombinasyonuyla otomatik olarak kararlaştırılabilir. Bu ilginç bir fikir, ama şimdi bulunduğumuz yerle o potansiyel gelecek arasında çok mesafe var. Yine de, diğer projeler insanlara –yönetim biçiminde olmasa da– bir tür doğrudan demokrasi getirebilirler. Dağınık otonom şirketler kripto paralardan çıkan heyecan verici konseptlerden biri. Amaç bir programın, neredeyse hiç insan katkısı olmadan, kendi kendini işletmesini ve internette başıboş dolaşırken kâr etmesini sağlamak.

Bunların ne tür kurumlar olacağı hakkında bazı fikirler öne sürüldü. Fikirlerin bazıları pek uygun değil, ama yine de bir noktaya dikkat çekiyorlar. Örneğin, bir istenmeyen e-posta robotu, token'ı ya da coin'ini satın alarak gelişimine katkıda bulunan birden fazla kullanıcının bilgisayarında dağınık bir şekilde çalıştırılabilir. Daha sonra elde ettiği

kârı, herhangi birinin ödemeyi onaylaması ya da denetlemesi gerekmeden, otomatik olarak sahiplerine dağıtabilir.

Muhtemelen, istenmeyen e-posta robotlarından daha faydalı programlar olacak. Daha karışık tekliflerden biri hem kripto paraların depolanabileceği hem de kredi alınabilecek bir bankayı içeriyordu. Banka borçlanıcının kredi notuna, gelir belgesine ve diğer yönlerine baktıktan sonra kredi verip vermeyeceğine karar verebilir. Eğer borçlanıcı kredisini ödemezse, kara listeye alınabilir. Kredilerden elde edinen kâr, parasını bu otomatikleştirilmiş bankalara yatıran katılımcıların faizini ödemek için kullanılabilir.

Bu son derece karışık bir girişim olur ve muhtemelen şu anda mevcut olan yapay zekâdan daha karmaşık bir şeye gereksinim duyabilir. Ancak, gelecekte otomatik bir programın insan katkısı olmadan risk hesaplaması ve kimlik doğrulaması mümkün olabilir. Büyük bir kredi alan kişi borcunu ödemediğinde mahkemeler için de ilginç bir durum olur. Bir dağınık otonom şirket ve bir kişi arasındaki sözleşme geçerli sayılabilir mi? Banka katılımcılarının toplu dava açarak o kişinin peşine düşmeleri mi gerekir?

Bütün bunlar o noktaya vardığımızda geçmesi oldukça ilginç köprüler olacaklar.

İstenmeyen e-posta robotları ve bankalar dışında, bir diğer ilginç fikir ise dağıtık şekilde işleyen ve reklam gelirlerini kripto paraya dönüştürüp bütün kullanıcılarına dağıtan bir sosyal ağ olabilir. Ağın nasıl kâr etmeyi planladığını başlangıç programına yerleştirmek ağın sahiplerine bağlıdır ama geleneksel işletmelerden daha düşük masraflarla, bu o kadar zor olmayabilir.

Bir diğer fikir ise, merkezsizleştirilmiş, Uber'e benze-

yen, halka açıkça işletilen sürücüsüz arabalardır. Bir grup insan coin satarak para toplayabilir ve daha sonra o parayı sürücüsüz araba filosu satın almak ve arabaları çağıran bir uygulama tasarlamak için kullanabilir, sonra bütün araçları bir metropole salabilirler.

Gelecekte, insanların küçük bir kısmına sahip oldukları birden fazla dağınık otonom şirket olabilir ve onlardan düzenli olarak artık gelir elde edebilirler. Bunun otomatikleşmenin artmasıyla yükselen ve yükselmeye devam edecek olan işsizlik sorunlarını azaltmaya faydası olabilir.

Bu bir klişe, ama teknoloji çok hızlı ilerliyor. Bitcoin teknolojisi de istisna değil. Bitcoin, yaklaşan bütün teknolojik gelişmelere entegre edilecek ve dünyada bundan faydalanacak tüm para birimlerinin arasında eşsiz bir yere sahip.

Bitcoin'in sağladığı finansal özgürlük internetin sağladığı eğitimsel ve bilgisel özgürlük kadar devrimsel olacak. Eğer Bitcoin potansiyeline ulaşırsa, milyarlarca insanın ekonomik hayatı kripto para birimlerinin gelişiminden etkilenecek. Ekonomik merdivenleri asla hayal etmedikleri bir şekilde tırmanmalarını sağlayacak bir ekonomik özgürlük kazanacaklar. Kısacası, Bitcoin finansal seçkinler ve diğer herkes arasındaki oyun alanını dengeleyecek.

IAN DEMARTINO,
COINJOURNAL'IN
KURUCU ORTAĞI
VE COINDESK'TE
SERBEST YAZARDIR.
BITCOIN'E
İLGİ DUYMADAN
ÖNCE FARKLI
SİTELERDE TEKNOLOJİ
YAZARI OLARAK ÇALIŞTI.

BITCOIN REHBERİ

KRİPTO PARALAR HAKKINDA BİLMEK İSTEDİĞİNİZ HER ŞEY

Bitcoin yeni bir ödeme birimi değil. İnternet gibi, Bitcoin de dağılmış ağda çalışan bir teknoloji. Onu kimse kontrol edemez, kimse kapatamaz. 'İnternetin para birimi' denen Bitcoin bundan çok daha güçlü: akıllı gözlemcilerin deyimiyle, para biriminin interneti.

- *Dijital paranın kökeni, geçmişi, şimdiki durumu, geleceği;*
- *Bitcoin'in arkasındaki devrimsel blokzinciri teknolojisi;*
- *Bitcoin'i elde etme ve onunla yatırım yapma yöntemleri;*
- *Bitcoin'i nasıl ve nerede harcayabileceğiniz;*
- *Bitcoin'in internetin yeraltı dünyasıyla ilişkisi;*
- *Alternatif dijital paralar hakkında bilmek istediğiniz her şey.*

Yeni teknoloji devrimini yakalamak isteyenler için yazılan Bitcoin Rehberi, küresel kripto para fenomenini size çok daha yakın kılacak.

ISBN 978-605-173-405-7
9 "786051" 734057"
₺29,50
/epsilonyayinevi
www.epsilonyayinevi.com
online alışveriş: kitap365.com

IAN DEMARTINO, COINJOURNAL'IN KURUCU ORTAĞI VE COINDESK'TE SERBEST YAZARDIR. BITCOIN'E İLGİ DUYMADAN ÖNCE FARKLI SİTELERDE TEKNOLOJİ YAZARI OLARAK ÇALIŞTI.

₿ITCOIN REHBERİ

KRİPTO PARALAR HAKKINDA BİLMEK İSTEDİĞİNİZ HER ŞEY

Bitcoin yeni bir ödeme birimi değil. İnternet gibi, Bitcoin de dağılmış ağda çalışan bir teknoloji. Onu kimse kontrol edemez, kimse kapatamaz. 'İnternetin para birimi' denen Bitcoin bundan çok daha güçlü: akıllı gözlemcilerin deyimiyle, para biriminin interneti.

- *Dijital paranın kökeni, geçmişi, şimdiki durumu, geleceği;*
- *Bitcoin'in arkasındaki devrimsel blokzinciri teknolojisi;*
- *Bitcoin'i elde etme ve onunla yatırım yapma yöntemleri;*
- *Bitcoin'i nasıl ve nerede harcayabileceğiniz;*
- *Bitcoin'in internetin yeraltı dünyasıyla ilişkisi;*
- *Alternatif dijital paralar hakkında bilmek istediğiniz her şey.*

Yeni teknoloji devrimini yakalamak isteyenler için yazılan Bitcoin Rehberi, küresel kripto para fenomenini size çok daha yakın kılacak.

ISBN 978-605-173-405-7
9 786051 734057

₺29,50

/epsilonyayinevi

www.epsilonyayinevi.com
online alışveriş: kitap365.com