Sorularla BLOCKCHAIN



Turan Sert

BLOCKCHAIN TÜRKİYE

TBV
TÜRKİYE BİLİŞİM VAKFI


Sorularla
BLOCKCHAIN
NE nasıl ne kadar
NEREDE kim neden nedir
ne zaman neler
ne demek mi mu mü
hangi kaç
?

Turan Sert



Yazan Turan Sert
Editörler Özge Çelik - Ahmet Usta
Tasarım Serdar Şekur

Tüm hakları saklıdır. Bu eserin tamamı ya da bir bölümü, 4110 sayılı Yasa ile degişik 5846 sayılı FSEK uyarınca, kullanılmazdan önce hak sahibinden 52. maddeye uygun yazılı izin alınmadıkça, hiçbir şekil ve yöntemle işlenmek, çogaltılmak, çogaltılmış nüshaları yayılmak, satılmak, kiralanmak, ödünç verilmek, temsil edilmek, sunulmak, telli/telsiz ya da başka teknik, sayısal ve/veya elektronik yöntemlerle iletilmek suretiyle kullanılamaz.

İşbu raporda yer alan bilgi ve görüşler yazarlarına ait olup yazarın çalıştığı kurumların, BCTR'nin ve TBV'nin görüşlerini temsil etmemektedir.
İşbu raporun içeriği, yazarı tarafından her zaman site üzerinde herhangi bir duyuru yapılmadan değiştirilebilir.

SorularlaBLOCKCHAIN
sunuş

Yaşadığımız çağda büyük bir değişim içindeyiz; her geçen gün yeni bir gelişme olmakta, yeni bir çözüm ortaya çıkmakta. Bu değişim o kadar hızlı gerçekleşmekte ki değişimi yakalamak, gelişmelerin gerisinde kalmamak gittikçe zorlaşıyor. Örneğin yeni bir teknolojiden bahsediyorsak bu teknolojinin ne olduğu, neyi farklı yapabildiği, nerelerde kullanılabileceği ve en önemlisi daha önce çözülemeyen hangi problemlere deva olacağını bir an önce anlamak, uygun kullanım alanları belirlemek, kendimizi ve işlerimizi geleceğe hazırlamak kaçınılmaz hale geldi.

İçerisinde bulunduğumuz yoğun tempo içerisinde daha da fazla bilgiye ulaşabilmek için okumak, okuduğunu paylaşmak, araştırmak, yazmak gerekiyor. Merak eden, merak ettiğini araştıran daha sonra da sosyal medyada bunu bir yazı dizisi haline getiren Turan Sert ile de yollarımız bu şekilde kesişti. Elinizde bulunan kitap Turan Sert'in Medium hesabında yalın bir dille uzun zamandır kaleme aldığı yazılarından derlenmiştir.

Blockchain Türkiye Platformu'nun kuruluş amaçlarından bir tanesi de bu teknoloji ile ilgili bir paylaşım ortamı oluşturmaktır. Bu kitap ile bilginin paylaşımına aracılık etmeyi ve daha çok kişiyi yazmaya, üretmeye teşvik etmeyi hedefliyoruz.

Blokzincir ile ilgili pek çok soruya yanıt bulabileceğinize inandığımız bu kitabın herkes için faydalı olmasını diliyoruz.

Dr. Soner Canko
BCTR Yürütme Kurulu Üyesi



Turan Sert

Boğaziçi Üniversitesi İşletme (BA, 1995) ve Harvard Business School (MBA, 2001) mezunu olan Turan Sert, finans ve teknoloji ağırlıklı kariyerine Arthur Andersen'da denetim ve Garanti Bankası'nda yatırım bankacılığı ile başladı.

Booz Allen New York ofisinde üç yıl süren yönetim danışmanlığı sonrası 2005 yılında Türkiye'ye döndü. Çeşitli Fiba Grubu iştiraklerinde murahhas azalık ya da yönetim kurulu üyelikleri ve 2014-16 yılları arasında Özyeğin Üniversitesi'nde CBO'luk görevinde bulundu.

Önce kuruluşundan itibaren içinde yer aldığı Girişim Fabrikası, sonrasında da 2016 yılında kurduğu teknoloji girişimi ile Türkiye'deki ekosistemin büyümesine katkı sağlamaya çalışıyor.
Evli ve iki kız babası.

önsöz

Bu kitabı kendim için yazdım.

Birkaç yıl önce ofiste otururken bir iş arkadaşım "Bitcoin değil ama bak Blockchain önemli" dedi. Boş gözlerle baktım kendisine. Aklımda sorular: "Bitcoin gerçekten ne demek, Blockchain ne demek? Farkları ne? Neden biri değil de diğeri önemli?"

Sonra okumaya başladım: Blockchain, bitcoin, kripto para, dağıtık sistemler... Okudukça tüm terimler birbirine girdi.

Serde danışmanlık var; çok boyutlu bir konuyu kavramanın en kestirme yolu öncelikle bu karmaşayı anlaşılabilir, mantıklı bir çerçeveye oturtmak.

Nasıl yapacaktım bunu? Kendime yazarak. Peki ne yazacaktım? Aklımdaki soruları. Vereceğim cevaplar ortadaki sis perdesini dağıtacak ve konuyu daha anlaşılır kılacaktı.

İlk sorumu sordum: "Sahi nedir bu Blockchain?" Ardından diğer sorular geldi: Önce "İyi güzel ama beni ya da çevremdekileri nasıl etkileyecek?" arkasından "Çok teknik bu konular, acaba bir üniversiteli ya da bir profesyonelin hızlıca kavrayabileceği kadar basitleştirebilir miyiz bu dünyayı?"

Sorular soruları kovaladı. Okunan yüzlerce yazı, dinlenen düzinelerce podcast ve yapılan onlarca konuşma sonrası elinizdeki (ya da ekranınızdaki) bu kitap ortaya çıktı.

Bu sayfayı çevirdiğinizde önünüze gelen içindekiler bölümündeki sorulardan birkaçı sizin de aklınızı kurcalıyor ise devam eden sayfalara bir göz atın. Takıldığınız bir soruya bile cevap bulduysanız kitap amacına ulaşmış demektir...

Kitabın fikir babası Bankalararası Kart Merkezi Üst Yöneticisi Dijital CEO Sn. Soner Canko, süreç sırasında desteklerini esirgemeyen BKM İş Geliştirme Direktörü Sn. Özge Çelik ve Blockchain Türkiye Genel Yayın Yönetmeni Sn. Ahmet Usta'ya teşekkürü borç bilirim. Tabii teşekkürlerin en büyüğü yazıların büyük bir kısmını yayınlanmadan önce dikkatle okuyan ve yorumları ile yönlendiren eşim Doç. Dr. Deniz Sert'e.

Turan Sert

www.turansert.com
@turansert

SorularlaBLOCKCHAIN
index

08 **NEDİR BU BLOCKCHAIN ALLAH AŞKINA?**

09 Üzerimize gelen dalganın farkında mıyız?
09 Önce işin ABC'sinden başlasak?
09 "Web"in kısa tarihine göz atalım mı?
10 Yeni bir dalga varmış Web 3.0 diye?

11 Sahi nedir bu Blockchain Allah aşkına?
12 Peki gayet güzel yürüyen bir sistem var zaten, neden buna ihtiyaç var?
12 Nereden biliyoruz Blockchain'in güvenli olduğunu?
13 Tamam, makineler mutabakat yapıyor. Ne işe yarayacak bu?

14 **BLOCKCHAIN BENİ NASIL ETKİLEYECEK?**

15 Blockchain finans dünyasını nasıl etkileyecek?
16 Peki her tür finansal işlem etkilenecek mi? İlk tehdit altında olanlar hangileri?
17 Başka hangi alanlar?
17 DeFi nedir?

18 Finans dünyasından örnekler neler?
18 Maker DAO nedir?

21 Blockchain tedarik zincirini sağlamlaştırabilir mi?
21 Tedarik zinciri ne demek, Blockchain ne işe yarar burada?
23 Madem bu kadar avantajlı, neden kullanılmıyor hemen?

24 Sağlık için Blockchain çözümleri neler?
24 Sağlık sektörünün sorunları ve sıkıntıları nerede?
25 Blockchain nasıl çözümler sunabilir?

27 Blockchain çevremizi korumamıza yardımcı olabilir mi?
27 Blockchain çevre için neden önemli?
28 Blockchain nerede işe yarayabilir?
29 Çevresel sorunlar neler?
29 Blockchain çevre için hangi alanlarda faydalı olur?
29 Mevcut durumu iyileştirmeye yönelik girişimler var mı?
30 Peki ya ezber bozan girişimler?
32 Bu çözümlerin önündeki engeller neler?

34 Blockchain seyahat sektörünü uçurur mu?
34 Seyahat sisteminin sorunları neler?
35 Blockchain bu sorunları çözmek için neler getirebilir?
35 Sorun çözme yanında yeni fırsatlar da yaratılabilir mi? Örnek: Further Network
36 Başka ne tip girişimler var?

38 Blockchain geleceği tahmin için kullanılabilir mi?
38 Tahmin piyasaları (Prediction Markets) ne demek?
38 Akıllı kontratların tahmin piyasalarına etkisi olur mu?
39 Bireysel tahmin mi konu yoksa daha geniş bakabilir miyiz konuya?

SorularlaBLOCKCHAIN
index

39 Zaten hazırda çözümler var, neden buna ihtiyaç duyuluyor?
40 Tahmin piyasası oyuncuları kimler?

42 **Blockchain'i sosyal fayda için kullanabilir miyiz?**

45 **Blockchain sanat dünyasına ne katabilir?**

45 Sanat sanat için mi… yoksa kimin için?
46 Kripto Kediler... peki var mı başka acayiplikler?
47 CD bitti, yaşasın Spotify... Ya da?

49 **Blockchain her derde deva mı?**

49 Blockchain'in faydalarını özetleyelim mi?
49 Blockchain bir tane mi? Elle tutulur mu?
50 Genel (Açık) ve Özel (Kapalı) Blockchain: Farkları ne?
50 Birkaç örnek verelim mi?
51 Peki girişimciler bu konuda ne kadar tecrübeli?
51 Blockchain bulunduğum sektöre yarar mı?
51 Her güzelin bir kusuru olur, peki Blockchain'in kusurları ne(ler)?
52 Neden ve ne zaman Blockchain'e ihtiyaç duyulur?
53 Peki neden bu kadar şişiriliyor Blockchain balonu?
55 Blockchain hangi sektörlerde başarılı olur? Turnusol kağıdı var mı?

56 **Değişen girişimcilik ve yatırımcılık**

57 Klasik anlamda 'Girişimcilik ve Yatırımcılık' nasıl idi?
57 Yeni anlamıyla 'Girişimcilik ve Yatırımcılık' nasıl yapılıyor peki?
58 Girişimler yeni teknolojiler aracılığıyla nasıl demokratikleşiyor?
59 Girişimciler ve yatırımcılar dışında masada başkaları da var mı?
59 Açık kaynak (Open Source) nedir? Neden önemli?
60 Açık kaynak ile para bir araya gelir mi?

61 **ICO ve Token Dünyası**

61 Aranan kan bulundu mu? - ICO ve Token dünyası
62 Token'ın hisse senedinden farkı ne?
63 Token sadece yatırım için mi kullanılır?

64 **TEKNİK OLARAK BLOCKCHAIN**

65 **Blockchain şifrelemesi ne demek?**

65 Baştan başlayalım: Şifreleme ne demek? Neden önemli?
65 Para, para, para-varlığı bir dert... ya yokluğu?
66 Çok karışık değil mi bu şifreleme?
67 Şifreleme ve öğütme? ne kadar önemli?
71 Peki Blockchain şifrelemesi nasıl çalışıyor?

SorularlaBLOCKCHAIN
index

74 Blockchain nasıl kendi başına hareket ediyor? İpucu: Uzlaşma

75 Bizans generallerinin problemi ne?
77 Blockchain nasıl uzlaşır?
77 Blockchain nasıl çözüm bulmuş bu sorulara?
77 Kısa hatırlatma: Blockchain nasıl çalışıyordu?
78 Blockchain üzerinde uzlaşma nasıl oluyor?
78 Peki bu sistem çok maliyetli değil mi?
79 Başka ne olabilir?

80 Uzlaşma mekanizmaları neler?

80 Satoshi Nakamoto'nun asıl başarısı ne idi?
81 Bitcoin'in meşhur ettiği Proof-of-Work ne, nasıl çalışır?
82 PoW'un en önemli rakibi olan Proof-of-Stake (PoS) nasıl çalışır?
83 Başka ne tip alternatifleri var?

84 **BLOCKCHAIN'İN GELECEĞİ**

85 Blockchain'in geleceği nasıl görünüyor?
86 Peki kısa vadede neler bekleniyor?
87 Blockchain'ler birbirleri ile konuşur mu?

92 **BITCOIN**

93 Bitcoin ne tam olarak?

94 Bitcoin'in kritik püf noktası ne? İpucu: "Uzlaşma Mekanizması"
94 Artık şu Bitcoin'e gelsek mi?
95 Bitcoin'in bir değeri var mı?
96 Bitcoin nasıl başlamış?

97 Bitcoin para mı gerçekten? Nasıl?
97 Paranın ortaya çıkışı nasıl olmuş?
98 Paranın olmazsa olmaz özellikleri neler?: Değer atfedilme ve aracılık etme
98 Her para bir değil. Neler değerini artırır paranın?
99 Peki Bitcoin para mı?

102 Bitcoin işlemi nasıl gerçekleşiyor?

102 Bir Bitcoin işlemi nasıl bir 'şey'?
104 Bitcoin işleminin temel mantığı ne?

106 Bitcoin geniş kitlelere nasıl yayılır?

106 Bitcoin'in geleceği nasıl şekilleniyor?
107 Kahvenizi Bitcoin ile ödemek mi?
107 Mikro ödemeleri Bitcoin üzerinden yapmaya kalkarsak sistem patlar mı?
107 Bitcoin'i nasıl hızlandırırız?

SorularlaBLOCKCHAIN
index

108 Bitcoin üzerinde ışık hızıyla işlem nasıl gerçekleşir? Lightning Network

108 Nedir bu Lightning Network?
109 Nasıl çalışıyor peki bu Lightning Network?

110 Bitcoin üzerinden büyük işlemleri hızlı yapmak mümkün mü? Bir çözüm: Liquid

111 Liquid Network? Nedir o?
112 Nedir sağladığı avantajlar Liquid'in?
112 Var mı sakıncaları?

113 Bakkt kurumsal yatırımcıyı kripto paraya çeker mi?

113 Bakkt'ın sahibi kim?
113 Peki Bakkt tam olarak ne yapmaya çalışıyor?
114 Bakkt konusunda ne tip çekinceler var?

116 Madencilik 2.0: Beyaz yakalıdan madenci olur mu?

116 Yatırımcılık değişiyor, neden?
117 Konu ICO'lar mı? Hayır
117 Girişim Sermayesi'nin faydası ne?
117 Girişim Sermayesi başka neler yapabilir? Madencilik 2.0'a hoş geldiniz!
118 Girişim Sermayesi neden madencilik yapsın?
119 Girişim Sermayeleri artık teknik açıdan da gelişmek zorunda mı yoksa?

120 **ETHEREUM VE DİĞER KRİPTO PARALAR**

121 Dünyanın en büyük bilgisayarı olan Ethereum'un hikayesi ne?

123 Ethereum'un çıkış ve inişi bir döngünün mü parçası?
126 Akıllı kontrat olur mu? Ethereum ve Akıllı Kontratlar

130 Diğer kripto paralar neler?

130 Litecoin, Bitcoin'in zıpır kardeşi olabilir mi?
131 Monero, biraz fazla mı gizli?
131 Dash, biraz fazla mı karanlık?
132 Zcash, sınıfın parlak çocuğu mu yoksa?
132 MimbleWimble aranan mahremiyet büyüsü mü?

143 Nedir bu SabitPara? Var mı böyle bir "şey" gerçekten?
144 En büyük SabitPara Tether neye benzer?
145 Facebook'un SabitParası Libra nedir? Nasıl çalışacak?

151 **BCTR ÇALIŞMA GRUPLARI TARAFINDAN HAZIRLANAN RAPORLAR**

nedir bu BLOCKCHAIN ALLAH aşkına

Üzerimize gelen dalganın farkında mıyız?

New York'taki projemde şirketimin yönetici ortaklarından birinin müşterisine sorduğu en can alıcı soru buydu. "Geceleri uykunuzu ne kaçırıyor?" Dolar/Euro paritesinin değişmesi mi, yoksa önümüzdeki yıl yapılacak seçimler mi? Siz bunlara kafa yorarken, birileri de tutturmuş sinek vızıltısı gibi "Bitcoin" diyor, "Kripto Para, Blockchain" diye bir şeyler sayıklıyor. Bunca derdin sıkıntının arasında bir de bunlar çıktı. Neymiş diye bir baktınız ama size anlatanların bile tam anlamadığını gördüğünüz için vazgeçtiniz.

Haklısınız. Ama inanın bu öyle ötelenecek bir konu değil. Bırakın ülkemizi, dünyada bile bu kavramları tam olarak kavramış insan sayısı şu an çok az. Ama sayı artıyor ve işin içine biraz girenler, yaklaşan dalgayı hissediyor. Bu kuvvetli bir dalga orası kesin. Ama kesin olmayan sizi ne kadar etkileyeceği. Belki hafif bir şekilde sallayacak, belki kroşe ile sersemletecek, ama bir olasılık da sizi nakavt edecek.

Bundan sonraki bölümlerde iş dünyasının içindekilere bu yeni gelen dalgayı, baş aktörlerini ve mevcut sistemi nasıl etkileyeceğini elimizden geldiğince aktarmaya çalışacağım.

Önce işin ABC'sinden başlasak?

Maalesef işe en baştan başlamak gerekiyor. Bu konulara zaten aşina iseniz, birkaç başlık daha beklemeniz gerekecek. Öncesinde, katıldığım bir konferansta konuşmalar başladıktan on dakika sonra konuşmacıların sözünü kesip "Biz Bitcoin diye buraya geldik, siz Blockchain diye bir şeyden bahsediyorsunuz, ben bilmiyorum, etrafıma sordum, onlar da bilmiyor" diyen hatırı sayılır büyük bir kesim için bir başlangıç yapmamız gerekiyor.

Başlangıç noktamız ne olsun? Bitcoin? Hayır, o sonra. Blockchain? Belki. Ama başlangıçta o da çok anlam ifade etmeyebilir. Bu konuda yazanlar genelde paranın ortaya çıkışından başlamayı severler. Ama biz biraz daha farklı açıdan, teknoloji tarafından bakalım, sonra finans (kapital) kısmına uzanırız. Konuyu "Web"in başlangıcına alalım, neler olduğuna çok kısa göz atalım, sonrasında bugüne de geliriz.

"Web"in kısa tarihine göz atalım mı?

"1989 yılında insanlara daha iyi bir hayat için neye ihtiyacınız var diye sorsalar, herhalde hiç kimse 'birbirine üst metin ile bağlı âdem-i merkeziyetçi bir ağ içinde yer alan bilgi noktaları' [yani "Web"] demezdi" *Sep Kamvar*[1]

Web aslında iki katmandan oluşuyor. Birinci katman akademisyenler ve uluslararası standartları oluşturan kurumlar tarafından 1970'lerde oluşturulan açık protokoller örneğin dosya yollamak, epostalar, ya da GPS -uydu ile coğrafi konum belirleme sistemi. Bir nevi Web'in altyapısı diyebileceğimiz bu sistemlerin ortak özelliği herkesin erişimine açık ve ücretsiz olmaları ki bu nedenle buna Web 1.0 diyenler de var.

Web 1.0 pek çok konuda bize kolaylık sağlayan ve bugün hala kullandığımız platformları ücretsiz olarak hizmetimize açtı ancak kimi konularda eksik kaldı. İşte eksik kaldığı bu noktaları 1990'lardan itibaren özel şirketlerin kurduğu platformlar doldurdu. Kullanıcılar tüm Web'e Facebook, Amazon, Google ve Apple'ın oluşturduğu bu merkezi platformlar aracılığı ile ulaşmaya başladılar çünkü bu platformlar hem daha kullanışlı hem de fonksiyonu yüksek hizmetler veriyorlardı. Ticari kâr odaklı bu şirketlerin oluşturduğu ikinci katmana Web 2.0 deniyor.

[1]http://farmerandfarmer.org/mastery/builder.html

Ancak tabii burada ufak bir sorun var. O da bu platformların Web 1.0'da bize ücretsiz hizmet verenler kadar masum olmayışı. Konu sadece kâr etmek değil. Facebook, bize hizmeti ücretsiz veriyor diye düşündüğünüzü sanmıyorum, zira sayfalardaki reklamların sıklığını görüyorsunuz. Olay bunun ötesinde, kişisel verilerimizin tamamen Facebook'un kontrolünde olması, bu kimliği bir başka platforma geçirmenin imkânsızlığı, hatta, neyi ne zaman ve ne şekilde göreceğimize Facebook'un karar vermesi (ABD'de 2016 yılında yapılan seçimlerde kopan yaygarayı hepimiz hatırlıyoruz)



Yeni bir dalga varmış Web 3.0 diye?

İşte konu burada merkezi/âdem-i merkezi (centralized/decentralized) ayrımına geliyor. Bireyler olarak biz sahip olduklarımızı kendimizde tutacak yapılara mı yöneleceğiz (Web 1.0'da olduğu gibi), yoksa bu sahipliği Web 2.0'da yaşandığı gibi başka merkezi yapılara mı devredeceğiz?
Son zamanlarda ortaya çıkan bütün bu yeni kavramların (Blockchain, Bitcoin, Ethereum, Kripto, Dapps, Tokens ki bunlara Web 3.0 da denebilir) temelinde de işte bu Web 2.0'a özgü monopollerin elinde konsolide olmuş olan bu sahipliği, yeniden bireylere geri verme isteği var.
Olayın teknoloji kısmının ana kaynağı bu. Tabii ki kapital işin içine girince bunun çok daha detaylı açılımları var. Örneğin:

• Web 1.0'nın finansmanının Amerikan hükümeti ve ordusunun finansman desteği ile kurulması ve kâr gütmediği için halka açılmasından,

• Web 2.0'in özel fonlar aracılığı ile kurulduğu için kapalı bir sistem içinde bütün yaratılan değeri kendine almasına,

• Web 3.0'ın başlangıçta açık kaynaklar aracılığı ile hobi olarak geliştirilen adem-i merkeziyetçi sistemlerin artık kendilerine yetecek hatırı sayılır derecede finansmanı buluyor olmasına kadar.

Bütün bunlara sonraki bölümlerde değineceğiz. Dediğimiz gibi duyduğunuz bütün bu kavramlar Web 3.0 dalgasının sesleri ve bu dalga ister istemez hepimizi etkileyecek. Ama az, ama çok.

Sahi sizin gece uykularınızı ne kaçırıyor?

Dipnot: Konu ile ilgili olarak Chris Dixon'un: "Why Decentralization Matters?"[2] adlı Medium makalesi ve Steven Johnson'un "Beyond the Bitcoin Bubble"[3] isimli NY Times Magazine yazılarını hararetle tavsiye ederim.

[2]https://medium.com/@cdixon/why-decentralization-matters-5e3f79f7638e

[3]https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html

Sahi nedir bu Blockchain Allah aşkına?

Web 3.0 olarak da adlandırılan yeni dijitalleşme dalgasının içerisinde şu ana kadar en öne çıkan Blockchain konusuna yavaştan başlayalım. Blockchain denince birçoğumuzun ilk aklına gelen kripto para konusuna da değinmeden olmaz. İki kavram aynı değiller anca birbirlerine ayrılmaz biçimde bağlılar. Daha başka örnekler de var, sırasıyla onlara da bakacağız.

İnsan ilişkilerinin temelinde güven yatar. Karşıdakine güven. Ancak biz insanlar karşımızdakinin sadece sözüne bağlı olarak bu güveni sağlayamadığımız için araya aracıların girmesine izin veririz. Pazardan alışveriş yaparken aldığımız domates için verdiğimiz kâğıt para devletin güven teşkil etmek için pazarcı ile aramıza girmesidir örneğin. Ya da birine bir havale yaparken bize ait olan bir varlığın karşı tarafın sahipliğine geçmesine bankanın aracılık etmesi gibi…

Yüzyıllardır bu şekilde kurulan para değiş-tokuş sistemine, işte son zamanlarda adını duymaya başladığınız yeni bir aktör katılıyor: kripto paralar. Ama hemen acele etmeyelim. Kripto para dünyasına dalmadan önce işin felsefi altyapısı için üzerinde durmamız gereken önemli bir konu var. İşte ilk terimimiz: Blockchain.

Hepimiz internete bağlanmak için cep telefonu ya da masaüstü bilgisayarı gibi aracı makineler kullanıyoruz. Bu makineler istediğimiz işlemleri yapabilmek için web olarak adlandırılan geniş bir ağa bağlanıyorlar. Benzer şekilde dünyanın dört bir yanında bulunan bir grup makine de bu ağın içinde özel olarak birbirlerine bağlanmış durumdalar.

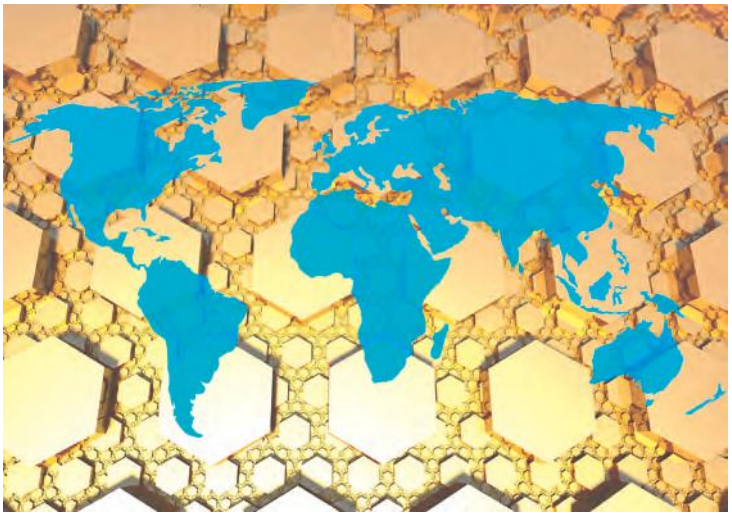
Blockchain ve kripto teknolojisi, işte bu ağa bağlı her makinenin diğerleri ile şifreli olarak konuşmalarını sağlıyor.

Ne konuşuyor bu makineler?

Ana olarak, yapılan herhangi bir işlemi, örneğin bir para transferini ve bu işlem sonucu oluşan son durum bilgisini aralarında paylaşıyorlar. Aynı bir bankanın yapılan bir havale için gönderenin hesabından parayı düşüp, alıcının hesabına gelen parayı eklemesi gibi.

Tabii Blockchain bu makinelere konuşmanın ötesinde kendi aralarında anlık olarak "Evet, bu işlem olmuştur" şeklinde teyit vermelerini sağlayan bir "mutabakat mekanizması" da sunuyor. Bu çok önemli, çünkü daha önceden güveni sağlamak için bir aracıya (ya da otoriteye) ihtiyaç duyulurken, artık bu güven, makineler arası mutabakat sayesinde otomatik olarak sağlanıyor.

Yani Blockchain teknolojisi, yukarıda bahsettiğimiz merkezi yapıların elinde olan "güven" unsurunu, "güvene duyulan ihtiyacın minimize edildiği", merkezi olmayan (adem-i merkeziyetçi) bir yapıya taşıyor. Kripto paralar da, bu teknolojinin tabiri caiz ise ilk çocuğu.



Peki gayet güzel yürüyen bir sistem var zaten, neden buna ihtiyaç var?

İyi de nereden çıktı bu, ne işe yarayacak? Dünyada zaten yeterince miktarda farklı cins para var. İstediğim parayı alıp, istediğimi satıyorum. İstediğim rakamı istediğim yere gönderiyorum? Kredi kartı ile her türlü alışverişi yapıyorum? Neden böyle bir sisteme ihtiyaç duyuldu?
Haklısınız. Ama bir noktayı unutmayın: Dünya nüfusunun şu anda ciddi bir kısmının para sistemine katılımı yok. Yurt dışında yaşamış olanlar bilir ilk yerleştiğinizde oradaki finansal sisteme girmeniz ne kadar sürdü? Ben banka hesabı açtırmak için altı ay uğraştığımı biliyorum üstelik Amerika'da yüksek lisans programına gelmiş "düzenli bir göçmen" olmama rağmen. Bir de zorla yerinden edilmiş ülkesini terk edip başka bir ülkede yaşamaya başlamış özellikle son yıllarda sayıları milyonları aşan insanları düşünün. Bu insanların geride bıraktıkları ya da başka bir ülkede yaşayan ailelerine para göndermek için yaşadıkları sıkıntıları ve girdikleri masrafı (Dünya Bankası göçmenler tarafından ailelerine sadece 2016 yılında yaklaşık 571 milyar ABD Doları gönderildiğini tahmin ediyor). Dolayısı ile hatırı sayılır bir kitlenin temel ihtiyacı aslında bu.

Bu temel problemlerin üzerine birkaç tane birinci dünya problemi de sayabiliriz tabii. Bir ülkeden diğerine yaptığınız para gönderiminin SWIFT sisteminde birkaç gün sürmesi, ortaya çıkan zaman kaybı. Getirdiği onca bürokrasi nedeniyle enerji kaybı. Onlarca dolar tutan yüksek maliyet sonucu oluşan para kaybı gibi…

Söylemeye gerek yok sanırım, Blockchain bazlı şifreli ağlar sayesinde paranız dünyanın neresinde olursa olsun dakikalar içinde bir başka kişinin hesabına geçiyor (nasıl olduğuna sonraki bölümlerde bakacağız).

Özet olarak, bu yeni sistemler şu ana kadar göz ardı edilen ciddi bir kitlenin tam ihtiyaç duyduğu araçlar. Bu piyasa içinde hatırı sayılır bir pay alacaklar. Ancak mevcut sistemi yok edecekler diye düşünmek şu aşamada gerçekçi değil.

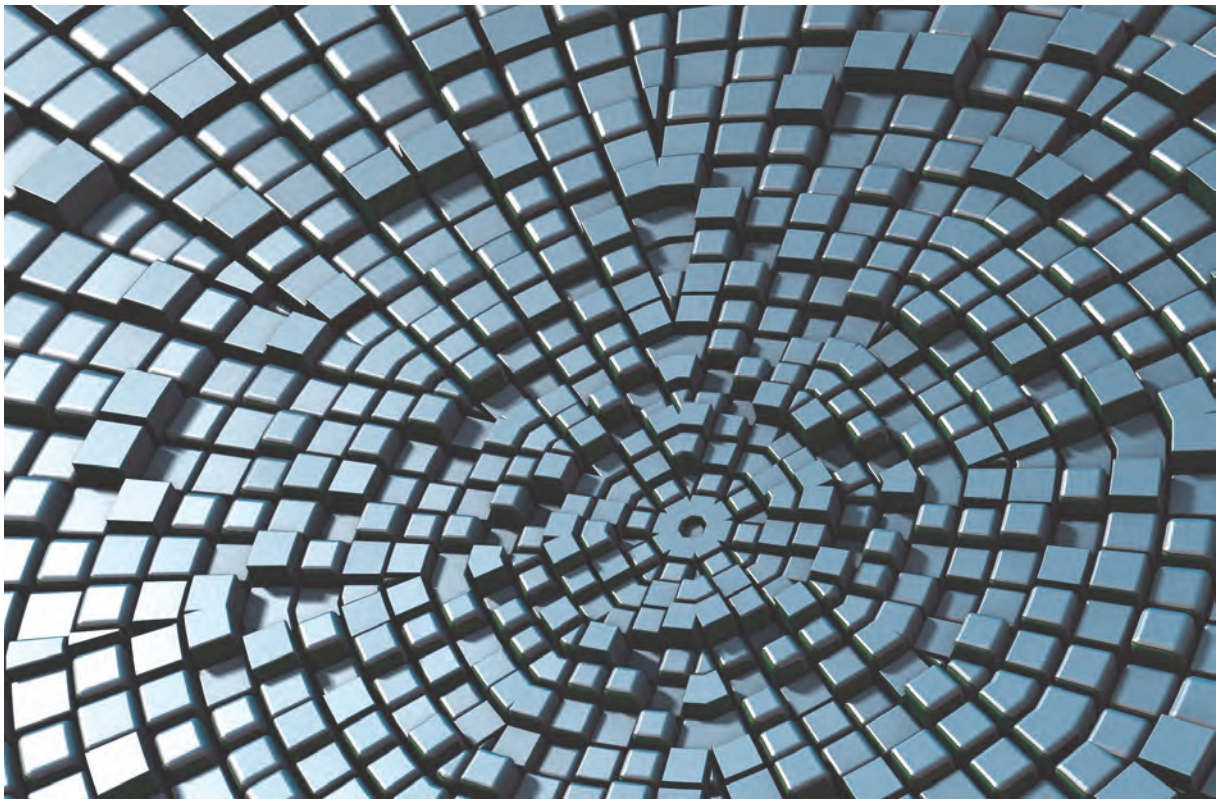
Nereden biliyoruz Blockchain'in güvenli olduğunu?

Aslında bu işin en kolay tarafı. İşin fazla tekniğine girmeden şunu söyleyelim sadece: Blockchain'in ortaya çıkması aslında öyle yazıldığı gibi Satoshi Nakamoto isimli şahıs(lar)ın 2008 yılında bir makale yayınlaması ile olmadı. 70'lerden beri süren 1980 yılında Ralph Merkle'in meşhur makalesi ile başlayan çözülmesi çok zor (imkânsız demek yanlış olur) kripto para ve şifreli ağlar ile başladı.
Özel anahtar, genel anahtar, hash, Bizans Generalleri gibi duymuş olmanız muhtemel teknik detaylara arzu ederseniz sonra bakarız. Bu aşamada şunu bilmek yeterli: Bu sistemleri kripto (şifreleme) sistemleri ile güvenilir kılan en önemli iki özellik şu:

• Sistemin bilgilerinin sistemdeki (ağdaki) tüm üyeler (makineler) tarafından şeffaf bir şekilde tutulması

• Yapılan bir işlemin geriye dönük olarak değiştirilememesi ve zaman geçtikçe böyle bir çabanın daha da imkânsız hale gelmesi

Bunu sürekli örülen bir örümcek ağı gibi düşünün. Bir sinek bir ağa düştükten sonra örümcek sürekli olarak yeni ağlar örüyor ve sineğin kurtulması imkânsızlaşıyor. Yani bir bilgi sisteme kayıt olup teyit edildikten sonra üzerine gelen her bilgi de aynı şekilde kayıt olup teyit ediliyor. Geçmişteki bir bilgiyi değiştirmek için o günden bugüne bütün bilgileri değiştirmek gerekiyor, yani geçmişe dönük değişiklikler gittikçe zorlaşıyor.



İşin teknik detaylarına daha sonraki bölümlerde gireceğiz. Sadece şunu unutmayın: İlk Blockchain uygulaması olarak kabul edilen Bitcoin 2009 yılında başladı ve o günden bugüne bir dakika bile durmadı. Ve 2009 yılında yapılan ilk işlemden bugüne kadar yapılmış bütün işlemleri takip edebilirsiniz. Hiçbiri değişmedi, hepsi şeffaf bir şekilde ortada.

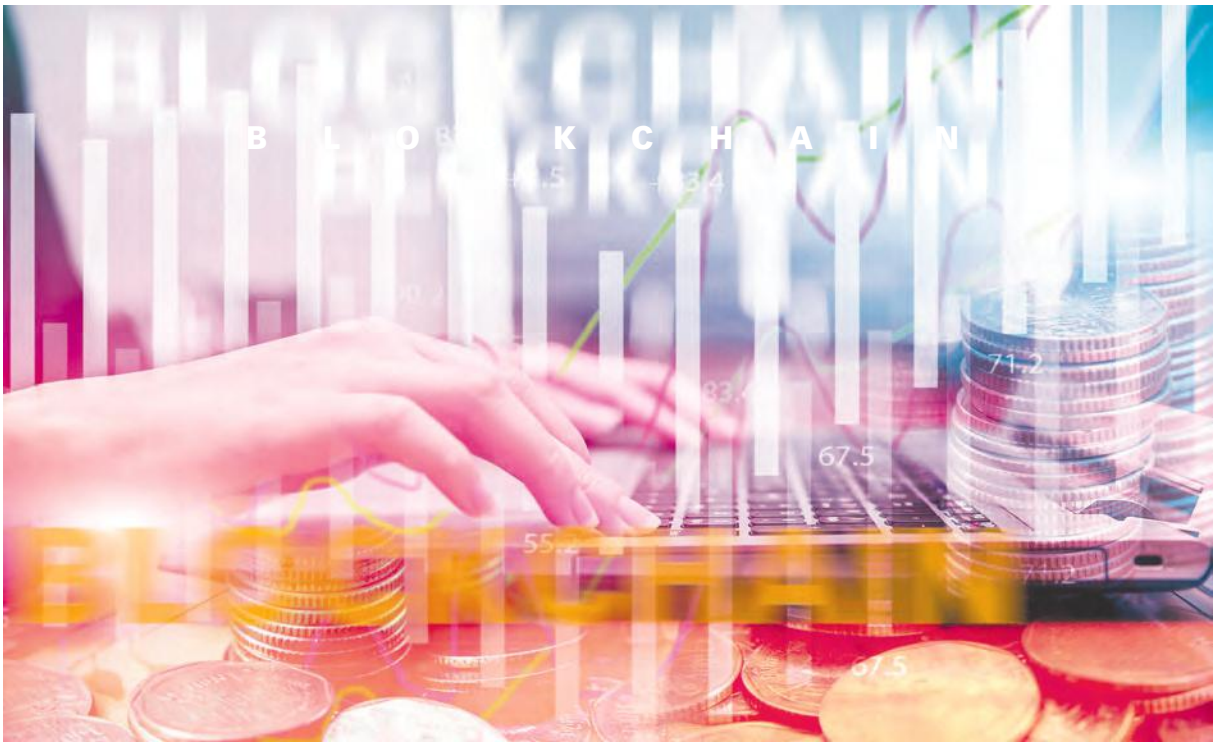
Tamam, makineler mutabakat yapıyor. Ne işe yarayacak bu?

Para burada sadece bir örnek. Güven sağlayan merkezi bir yapının yerini (ya da paralel olarak onunla birlikte) her yere dağılmış makinelerin aldığını düşünelim. Neler yapılabilirdi, bize ne faydası olurdu?

• Online kimliğimiz Blockchain üzerinde tutulsa ve sadece bizim istediğimiz mecralarda bizim istediğimiz kadar gösterilse beğenmediğimiz bir mecrayı anında kesip atsak, bütün bilgilerimizi anında başka bir yere taşısak? Tamam böyle bir kimliğe ortam sağladığı için Facebook bizden para almıyor ama, ya biz bu kimliğimizi kullanıp üstüne bir de para alsak örneğin reklam verenlerden?
• Aracıların olduğu her alana (örneğin Uber'e ya da iTunes App Store'a yüksek komisyon (şu anda %30'larda!) ödeyeceğimize bunu olabildiğince aza (örneğin %1'e) indirsek?
• Yüksek işlem ücreti isteyen her türlü borsanın (örneğin kripto borsaları bu borsalarda işlem yapanlar ne kadar çok aracılık masrafı yaptıklarını çok iyi bilirler) ücretini sıfıra çeksek?

Gelin Blockchain bazlı sistemler bizi ve içinde bulunduğumuz sektörleri nasıl etkileyecek, bir sonraki bölümde buna bakalım...

BLOCKCHAIN beni nasıl etkileyecek?



BLOCKCHAIN finans dünyasını nasıl *etkileyecek?*

Blockchain bazlı sistemlerin en çok etkileyeceği alanlardan birinin finans olduğu ezelden beri söylenir. Gelin neden böyle bir algı var önce ona bakalım sonra da bu alanda son zamanlarda en çok konuşulan konulardan biri olan Decentralized Finance (DeFi-Dağıtık Finans) oluşumuna göz atalım.

Blockchain bazlı sistemlerin ana amacı iki taraf arasında yapılan işlemlerde merkezi bir aracının sağladığı "güven" hizmetini makinelere yaymak. Böylece bu güvene duyulan ihtiyacı tek bir aracının tekelinden kaldırmak.

Bu makineler coğrafi olarak farklı noktalarda ve birbirinden bağımsız. Neden?

Çünkü dağınık olmaları durumda tek bir güç tarafından kontrol edilmeleri neredeyse imkânsız hale geliyor.

Tek bir güç tarafından kontrol edilemeyen makineler kendilerine verilen emirleri gerekli koşullar oluştuğu anda kimseye sormadan otomatik olarak gerçekleştiriyorlar. Hile yok, hurda yok, gecikme yok. Koşul oluştu, işlem de gerçekleşiyor. Bunu da sağlayan bu makineler için yazılmış özel direktifler, bir başka deyişiyle Akıllı Kontratlar.

Finans piyasasındaki mevcut aktörlerin ana rolü işte bu aracıyı oynamaları ve güveni teşkil etmeleri idi. Dolayısıyla Blockchain bazlı sistemler bu aktörler için varoluşsal bir tehdit oluşturuyor; bugün olmasa bile yakın bir gelecekte.

Peki her tür finansal işlem etkilenecek mi? İlk tehdit altında olanlar hangileri?

Bu piyasanın tehdit altında olduğu ilk alan para transferleri oldu. Özellikle de ülkelerarası SWIFT transferleri. Neden? Hem yüksek maliyetli, hem yavaş hem de kimi zaman kimi ülkelerde yaşayanlar için ulaşması imkânsız bir sistem.

Dikkat ederseniz, para transferi kişiler arası gerçekleşen finansal işlemlerin en basiti. Bir kişi kendine ait bir parasal değeri bir diğer kişiye koşulsuz olarak transfer ediyor. Dolayısıyla makineler tarafından yapılması en kolay olanı. Bu nedenle merkezi olmayan yapılar tarafından ilk olarak fethedilmeye çalışan alan burası oldu.

Elbette ileride tüm para transferleri bankalardan alınıp makinelere geçecek demek doğru olmaz. Zira eğer bankadan çok cüzi miktarda para transferini EFT sistemi ile daha hızlı yapabiliyorsanız neden kripto para gibi alternatifler ile uğraşasınız ki? Ama dediğimiz gibi SWIFT gibi yüksek maliyetli bir alana girerseniz işte orada kripto para şimdiden ciddi bir alternatif.

Tabii hemen belirtelim: Kripto paraların bulunduğu Blockchain sistemlerinin hükümetlerin gerekli gördüğü kara para ile mücadele (anti-money-laundry ya da kısaca AML) ve müşterinin kimlik bilgilerinin bilinmesi (know-your-customer ya da kısaca KYC) konularında alacakları bir hayli yol var. Benzer mantıkla Blockchain bazlı yapılar öncelikle basit ve yüksek maliyetli alanlara odaklanacaklar. Teknoloji geliştikçe daha karmaşık alanlara girmeye başlayacaklar.

Aslında belki şöyle demek daha doğru: Blockchain bazlı girişimler finansın her alanında mevcut sistemlere karşı yenilikler çıkaracaklar. Ancak bunlardan basit, yüksek maliyetli ve de geniş kitlelerin kullandığı alanlarda çalışan girişimlerin başarı şansı daha yüksek olacak.

Bir örnek daha verelim: Alışverişlerde kredi kartı yerine kripto para kullanılması.

Bu alanda kendine pay almaya çalışan pek çok girişim var. Örneğin Litecoin ve sonraki bölümlerde bahsettiğimiz Grin bunlardan ikisi. Ancak unutulmaması gereken bir durum var-o da son kullanıcı gözünde Visa ve Mastercard gibi kartlar hem hızlı işlem sağlıyorlar hem de maliyetleri çok düşük. Dolayısıyla özellikle kredi kartı kullanımının yaygın olduğu gelişmiş ülkelerde kripto paralar ile alışveriş yapılması ilk aşamada geniş kitlelerin ilgisini çekecek mi? Zor görünüyor.

Bu demek değil ki bu kripto paralar alışveriş için kullanımda başarısız olacak. Kripto paraların kredi kartına ya da bankacılık sistemine erişimi olmayanlar tarafından kullanılması daha muhtemel. Aynı şekilde mevcut bankacılık sisteminde şu ya da bu şekilde olmak istemeyen gelişmiş dünyadaki küçük bir kitle de bu paraları kullanabilir.



Gelişmiş ülkelerde kripto paraların ödeme amaçlı kullanımı ikinci bir dalga olarak gelebilir. Ancak bunun için iki ön koşul var: birincisi başka ihtiyaçlar nedeniyle kripto para kullanımının artması, ikincisi ise bu paraların üstün bir kullanıcı deneyimi sağlaması.

Başka hangi alanlar?

Peki para transferlerinin ötesinde finansın hangi alanında Blockchain bazlı girişimlerin başarı şansı daha fazla? Decentralized Finance (DeFi) olarak da adlandırılan bu yeni dalgada hangi alanlar göreceli basit ve yüksek maliyetli?

Önce bir DeFi nedir ona bakalım, bir sonraki bölümümüzde ise en yaygın kullanılan üyesine bakacağız bu yeni kavramın.

DeFi nedir?

DeFi, yani Decentralized Finance pek çok girişimin ortaklaşa kurdukları bir protokol ve açık bir topluluk.

Kurucularının ortak özelliği Blockchain sistemleri üzerine girişimler olmaları. Girişimlerin çıkış amacı kurulduktan sonra benzer sıkıntıları paylaşmaları ve vizyonları da silo halinde organize olmuş mevcut finansal altyapıları değiştirmek. Ana prensipleri[4] ise şu üç konu:

• Karşılıklı kullanılabilirlik ve açık kaynak: Bütün projelerin kurulurken karşılıklı kullanılabilir olmasına dikkat etmek. Bunun için de özellikle açık kaynak kullanmak. Böylece bütün projelerin daha kuruluşları sırasında birbirlerini inceleyerek ileri aşamalarda birlikte nasıl çalışabilecekleri ile ilgili ortak bir bilinç oluşturmak.
• Ulaşılabilirlik ve finansal kapsayıcılık: İnternet bağlantısı olan herkesin ulaşabileceği bir finansal sistem hayali. Aynı şekilde "değer"in (ya da bir varlığın) kişinin coğrafi konumundan bağımsız olarak dünyada serbestçe dolaşabilmesi.
• Finansal şeffaflık: Finansal hizmetlerin şeffaf olmayan silolarda tutulması yerine kişilerin gizliliği konusunu saklı tutmak kaydıyla tüm piyasa bilgisinin tüm katılımcılara açık olduğu bir sistem inancı.

[4]https://medium.com/defi-network/opening-defi-42a5afdb71e0

DeFi protokolü üye girişimlerin bazıları Dharma Labs, dy/dx, Compound, CDx, Coinbase Wallet, Kyber Network, bZx, MARKET Protocol, 8x Protocol, Centrifuge, Connext, Loopring. Ama en yaygın kullanılanı Maker DAO.



DeFi kurucu üye platformlar (Kaynak: Dharma)

Sonuç

Özet olarak DeFi yani Decentralized Finance'nin özü Akıllı Kontratlar ile işlemlerin aracısız olarak gerçekleşmesi. Yani herhangi bir güç tarafından kontrol edilmeyen makinelerin verilen işlemleri baştan belirlenen koşullar gerçekleştiğinde otomatik olarak gerçekleştirmesi.

Bu alanda ilk akla gelebilecek uygulamanın para transferi olduğunu belirtmiş ve Bitcoin başta olmak üzere pek çok kripto para ile bu alanda belli yol kat edildiğinden bahsetmiştik. İkinci alan olarak da kredi verme ve almadan bahsedebiliriz.

Bir sonraki bölümde DeFi hareketinin en yaygını olan ve kredi konusunda çalışan MakerDAO'ya bakalım.

finans dünyasından örnekler neler?

Maker DAO nedir?

DeFi-Decentralized Finance (Dağıtık Finans) hareketinin öncülerinden olan MakerDAO[5], Blockchain ile tamamen kendi kendine çalışan yeni bir borçlandırma mekanizması sunuyor. Gelin detaylarına birlikte bakalım.



MakerDAO kişilerin ellerinde duran kripto paraları teminat verip bu teminat karşılığı sistemin parası olan Dai'yi yaratmalarına olanak veren bir dağıtık bir sistem. Ethereum üzerinde kurulu Akıllı Kontratları kullanılıyor bunu yapmak için.
Dai nedir peki? Dai bir ABD Dolarına eşit olan bir SabitPara. SabitParaların ne olduklarına daha sonraki bölümlerde değineceğiz. (Dai kelime anlamı olarak Çince'de borç para vermek[6] anlamı taşıyor bu arada)

[5] https://makerdao.com
[6] https://www.reddit.com/r/MakerDAO/comments/5q98b1/%E8%B2%B8_dai/

Nasıl çalışıyor?

Elinizdeki kripto parayı (şu an için yalnız Ethereum parası ETH geçerli) teminat olarak gösteriyorsunuz, buradaki deyişiyle ETH'lerinizi sistem içine kilitliyorsunuz. Gönderdiğiniz her 150 birim para için 100 birime kadar Dai yaratabiliyorsunuz. Sonrasında bu DAI'yi istediğiniz noktadaki borsada bire bire yakın bir değerden ABD Doları'na çeviriyor ve kullanıyorsunuz. Bu para için bir maliyet ödüyorsunuz, sonrasında ise dilediğiniz noktada tekrar Dai satın alarak yok ediyor ve ETH'nize geri kavuşuyorsunuz.

Neden insanlar kullanıyor?

Diyelim ani olarak paraya ihtiyacınız var, mevcut paranızı da ETH'ye yatırdınız. ETH'nin yükseleceğini düşünüyorsunuz ya da başka herhangi bir nedenle ETH'lerinizden ayrılmak istemiyorsunuz. Bu sistemi kullanarak hem nakit ihtiyacınızı karşılayabilir hem de ETH'nin getireceği kardan yararlanabilirsiniz.

Kredi maliyeti ne?



Bir ara inanılmaz ucuz idi, ancak 2019 yılının ortalarına doğru artmaya başladı. Başlangıçta yıllık %0,5 bir faiz maliyeti olan sistem önce %2,5 seviyelerine çıktı, sonraları ise %14'lere kadar yükseldi (buna stabilize ücreti deniyor ve bu ücreti ayrı bir para ile ödüyorsunuz ama şu aşamada çok da gerekli değil bunu bilmek.

Ya ETH çok düşer de teminatımın altına inerse?

Buna dikkat etmek gerekiyor işte. Zira ETH'nin değeri düşerse ekstra ETH yüklemeniz yapmanız lazım. Ya da baştan ihtiyacınız olan nakitten daha fazla ETH koymakta fayda var. Aksi takdirde sistem ETH'nizi "bozuyor" ve %13 gibi bir ceza sonrası kalan paranızdan borcunuzu düşüp size geri veriyor.

Şu anda sistemde kilitli tutulan teminat rakamının kullanılan krediye oranının yaklaşık %200 olduğunu görüyoruz. Yani insanlar gerekli minimum limit olan %150'nin üzerine bir %50'lik bir ekstra teminat koymuşlar kullandıkları krediler için.

Kim borç veriyor bu sisteme?

Aslında kimse kimseye borç vermiyor. Siz elinizdeki ETH'yi teminat gibi kullanıp Dai yaratıyorsunuz. Buradaki soru şu olabilir? Dai'yi satıp ABD Doları aldınız. Kime satıyorsunuz Dai'yi? Genel olarak SabitPara kullanmak isteyen insanlara (ya da daha önce kredi almış ve şu anda borcunu kapatmak için Dai almak isteyenlere). Neden SabitPara kullanmak ister insanlar konusunu daha detaylı olarak son bölümde bulabilirsiniz.

Dai parası nasıl sabit kalıyor peki?

Dai, bir ABD dolarına sabitlenmiş. Ama alım satım yapıldığı borsada baktığınızda fiyatı aşağı ya da yukarı gidebiliyor. MakerDAO yaratıcıları fiyatın iniş ve çıkış olduğu durumda tekrar 1 ABD dolarına gelmesinin otomatik olacağını düşünüyorlar. Şöyle ki:

Diyelim, Dai fiyatında bir düşüş oldu. Böyle bir durumda geçmişte Dai yaratıp borç almış olanlar, aldıkları borcu yine Dai ile ödeyecekleri için kredilerini ucuza kapatma fırsatı bulabilecekler ve Dai satın alacaklar.

Aynı şekilde Dai fiyatında bir artış olduğunda (1 ABD dolarından daha yüksek bir fiyata geldiğinde) insanlar ellerindeki ETH'leri sisteme gönderip 1 ABD doları karşılığı olacak şekilde Dai yaratacak ve bu Dai'yi piyasada 1 ABD Doları'nın üzerinde bozdurma şansı yakalayacaklar. Bu da piyasada 1 Dai'nin 1 ABD Doları'na yaklaşmasını sağlayacak.

Bunun yanında Dai fiyatında ekstrem bir düşüş olduğu durumlar için de acil durum senaryoları hazırlanmış ama şu aşamada çok teknik kaldığı için ilgilenenleri Tanıtım Yazısı'nı (White Paper)[7] okumaya davet ederek konuyu kapatıyoruz.



Peki başarılı olmuş mu MakerDAO?

MakerDAO tamamen otomatik bir sistem. Arada herhangi bir aracı yok. Karmaşık anlaşmalar yok, kâğıt imza vs yok. Sistem tamamen kodlanmış makineler aracılığıyla işliyor. Teminatınızı koyuyorsunuz, paranızı alıyorsunuz. Teminatınız %150'nin altına düşerse de ETH'niz bozduruluyor ve kredi borcunuzun üzerindeki teminatınız hesabınıza yatıyor. Bu nedenle kredi vermenin getirdiği kâğıt ve bürokrasi masrafından kurtulma sistemin en önemli avantajlarından biri.

[7] https://makerdao.com/en/whitepaper

Şu ana kadar iyi gittiklerini söylemek mümkün. Zira halihazırda iki milyon ETH'e yakın miktar MakerDAO sistemi üzerinden borçlandırılmış (CDP, Collaterized Debt Positions). ETH'nin şu aralar 120 ABD Doları civarında olduğu düşünülürse yaklaşık 240 Milyon ABD doları bir rakama denk geliyor bu. Ethereum'un kullanım olarak en işlevsel platformlarından biri MakerDAO.

Sistem şu ana kadar sıkıntı yaşamadan ilerledi. ETH sene içinde çok ciddi değer kaybetti ama buna rağmen Dai'de ciddi bir sıkıntı olmadı. Bu ileride de olmayacak anlamına gelmiyor tabii. O da bunun riski. ETH'nin aniden %33 değer kaybetmesi durumunda 150 birimlik teminatlar 100 birime düşebilir ve sistem bu ETH'leri satana kadar borç miktarının altına bile inebilir. Şu an için MakerDAO sistemi daha çok küçük ama çok daha büyümesi durumunda tüm ETH değerini bile etkileyecek hale gelebilir olası ani düşüşler.

MakerDAO her derde deva mı?

Tabii ki hayır. Ancak, 'bir ürünü ne kadar basit ve istisnaları dışarıda bırakarak şekillendirirseniz o kadar otomatik (insan eli değmeden) yürütebilirsiniz' tezine güzel bir örnek. Şu anki rakamlar cesaret verici olsa da ileride gerçekten finans piyasalarını sarsıcı bir devrim haline dönüşür mü? Bunu şimdiden tahmin etmek oldukça zor. Neden?

Öncelikle, kriz anlarında test edilmiş bir ürün değil. Test edebilmenin tek yolu da ancak bir kriz yaşamaktan geçiyor, tabii ki stres test benzeri çalışmalar var ama hiçbiri kriz anında ne olacağını tam gösteremiyor. Yukarıda da yazdığımız gibi ETH 2019 yılında değer kaybetti ve MakerDAO'ya hiçbir sıkıntı yaratmadı bu durum. Peki ya ani düşüşler?

En büyük konulardan biri de teminat miktarı. Oldukça yüksek. Ama başta da yazdığımız gibi kredi sisteminin en masraflı ve karmaşık yönlerinden biri kredi derecelendirme ve geri ödememe oranları. Basitlik en başta bu iki özelliği budamaktan geliyor. Tabii ki bunun bir karşı maliyeti olacak, o da yüksek teminat oranları.

MakerDAO için sonraki adımlar neler?

MakerDAO özelinde baktığımızda sonraki adımlarda, sistemin organik olarak büyümesi var. Halihazırda tüm ETH miktarının %2'si MakerDAO sistemine kilitlenmiş durumda, bu da onu Ethereum sisteminin en büyük oyuncularından biri yapıyor. Ancak MakerDAO sadece ETH ile işler diye bir kural yok. Başlangıç noktaları bu ancak diğer altyapı protokolleri ile de çalışabilmek onları daha geniş kitlelere yayacak.

Bunun yanında sistemin daha geniş kitlelere yayılması için aslında farklı yatırımcıların ihtiyaçlarına hitap edecek çözümler üst seviye olarak ortaya çıkabilir (bir nevi Bitcoin üzerine ödemeleri hızlandırmak için kurulan Lightning Network gibi). Örneğin kredi derecelendirmesi gibi daha karmaşık çözümler. Ve bu çözümler merkezi yapılar da olabilir- zira karmaşık çözümler için merkezi yapılar daha efektif olabiliyor. Dolayısıyla altta merkezi olmayan ve bunun getirdiği kolaylıklardan yararlanan ama üstte daha karmaşık isteklere hitap eden merkezi yapılar (DeFi -Decentralized Finance- üzeri CeFi -Centralized Finance-) ilginç açılımlar getirebilir. Tanner Hoban'ın konu ile ilgili makalesi[8] bu anlamda çok daha detaylı bilgi veriyor ilgi duyanlara.



Sonuç

MakerDAO kısa sürede kat ettiği aşama ile büyük bir potansiyel gösteriyor. Büyümesi sürerken yol üzerinde ufak tefek kazalar geçirmesi de olası- ancak ilk yıllarını kazasız bir şekilde atlattılar. Merkezi bir aracıya ihtiyaç duymadan finans dünyasının farklı bir alanında gösterdikleri başarı onları uzun vadede dikkatle izlenmesi gereken girişimlerden biri yapıyor.

[8] https://medium.com/@tehoban/defi-constructing-the-foundation-of-a-new-microeconomy-cb7f21f1c6dd



BLOCKCHAIN tedarik zincirini sağlamlaştırabilir mi?

Değişik sektörlerde Blockchain bazlı teknolojilerin açabileceği vizyon bakmaya devam edeceğiz. Ama şimdi tüm sektörlere dokunan tedarik zincirlerinde Blockchain bazlı olarak nitelendirdiğimiz dağıtık merkezli teknolojiler neler getirebilir kısaca ona bir bakalım…

Tedarik zinciri ne demek, Blockchain ne işe yarar burada?

Tedarik zinciri derken bu bölümün kapsamında bahsettiğimiz şu: bir şirketin müşterilerine sunacağı ürün ya da hizmeti oluşturabilmesi için gerekli alt ürünlerin ilk üreticiden itibaren izlediği zincir.

Blockchain'in hayatımıza getirdiği en önemli yeniliğin 'güvene olan ihtiyacı en aza indirmek' olduğunu daha önce pek çok kez dile getirdik. Verdiğimiz örneklerde güvene duyulan ihtiyacı karşılayan ancak maliyeti yüksek aracılar için güzel günlerin sona ermekte olduğunu yazdık. İlk üreticiden (ki bu hammadde de olabilir) son kullanıcıya kadar pek çok aracının olduğu tedarik zincirleri de aslında buna çok açık bir örnek. Ama bunun yanında aracı olmasa bile aslında bir alıcı ile satıcı arasındaki güvene duyulan ihtiyaç yüksek. Nasıl? Bakalım:

Bir ürün üretmek için tedarikçinizden size bir mal göndermesini istiyorsunuz. Peki tedarikçi ürünü gönderdi mi? Gerçekten iddia ettiği miktarda mı gönderdi? Ürün şu an nerede? Düzgün, işe yarar durumda mı? Bana ne zaman ulaşacak?

Bütün bu sorulara net bir cevap verilememesinin yarattığı belirsizlikler, sizde

• Elinizde olduğundan fazla stok tutmak (ürün ya gelmezse?), ya da
• Kendi ürettiğiniz ürünün müşterinize zamanında ulaşmaması

gibi iki temel risk oluşturuyor. Hele bir de bu belirsizliklerin stok ömrü uzun olmayan sebze, meyve gibi ürünlerde olduğunu düşünün. Maliyetleriniz hepten artacak.

İyi de bunun için Blockchain'e ihtiyaç var mı? Hep söylediğimiz gibi Blockchain her derde deva olacak diye düşünmek doğru değil. Burada söz konusu olan sadece siz ve tedarikçiniz olsa haklısınız. İki taraf arasında olduğunda bir şekilde tedarikçinize dayatacağınız kurallar ile daha şeffaf bir süreç sürdürebilirsiniz. Ancak maalesef ikiniz dışında pek çok taraf var bu işlemin içinde. Taşıyıcı firma, gümrük işleri, sigorta, ithalatçı, ihracatçı… Bunların her birinin süreç içinde bir yeri ve sorumluluğu var. Alelade bir dokümanın bu firmalar arasında döndüğünü düşünün. Avrupa'dan Doğu Afrika'ya giden bir soğutucu için 30'un üzerinde kişi ve kurumdan onay ve 200'ün üzerinde bilgi alışverişi yapıldığını biliyor muydunuz?[9] Neden gerek var bu kadar iletişime? Çünkü taraflar birbirine (maalesef) güvenemiyor ve oluşan hatalar ya da sahtekarlıklar düşünüldüğünde haksız da sayılmazlar.

Peki bütün bu işlemlerin tüm taraflara şeffaf ve geriye dönük değiştirilemez şekilde yapıldığını ve ilgili taraflar ile paylaşıldığını düşününün bir de. Bürokrasinin ve hataların azalmasından sağlanan emek ve zaman tasarrufu hatırı sayılır olacak. Bir de buna düzensiz planlamanın getirdiği ekstra stresi ve aksamalarda oluşan müşterinize ürün ya da hizmeti zamanında verememenin getirdiği prestij kaybı ve potansiyel cezaları ekleyin. Bu iki kazanç bile yeter konuya dikkat kesilmek için.

Hemen belirtelim IBM ve Maersk bu alanda sektöre hitap edecek bir platform oluşturmak için bir ortaklık kurdular[10] ancak sektörün diğer büyükleri bu iki firma tekelindeki girişime şu anda soğuk bakıyorlar.[11]

[9]https://www.reuters.com/article/us-maersk-blockchain-ibm/maersk-ibm-to-launch-blockchain-based-platform-for-global-trade-idUSKBN1F51DE
[10]https://www.reuters.com/article/us-maersk-blockchain-ibm/maersk-ibm-to-launch-blockchain-based-platform-for-global-trade-idUSKBN1F51DE
[11]https://shippingwatch.com/carriers/Container/article10602520.ece

Şeffaflık yalnıza alıcı olarak sizi ilgilendirmiyor. Yapılan işlemlerin doğruluğu ve ürünlerin uygunluğu sizin dışınızdaki dış denetçiler (özel denetim şirketleri ya da hükümetlerin yetkili mercileri) için de önemli. İşlemlerin Blockchain üzerinden şeffaf ve değiştirilemez şekilde tutuluyor olması, dış denetçiler için de büyük kolaylık. Onlar için bu daha az masraf ile çok daha geniş bir alanda işlerin doğru yürüdüğüne emin olmak anlamına geliyor.



Özellikle bozulabilir ürünlerde tedarik zincirini en başından beri takip edebilmenin bir faydası da şu: Özellikle Batı ülkelerinde bir toptancıdan gelen herhangi bir üründe bozukluk olduğunda, müşteriye sunulan bozuk ürünlerin itibara getirdiği hasardan dolayı büyük marketler bu konuda çok katılar-hiçbir risk almak istemiyorlar, sonucunda ürünün tamamı çöpe gidiyor. Halbuki ürünün ilk üreticiden itibaren takibi ve kontrolü yapılabildiğinde bozuk ürünün geldiği alanı nokta atışı belirlemek ve çok daha az ürünü yok ederek israfı engellemek mümkün.

Örneğin, 2017 yılı Kasım-Aralık aylarında ABD ve Kanada'da patlayan E.coli bakterisine bağlı hastalıklardan 60 kişinin hastanelik olup 2 kişinin ölmesinin ardından, bakterinin kaynağını belirlemek için yapılan araştırmalar hem uzun sürdü hem de çelişkili sonuçlar verdi. Kanadalı yetkililer kaynağın marul olduğunu belirtirken, ABD'li yetkililer nedeni 'yeşil yapraklı sebzeler' olarak açıkladı.[12] Bu olay sonrası ABD'de marul satışları bir önceki yıla göre %45 oranında düştü.[13] Aylar sonra ürünün merkezinin Arizona'daki Yuma bölgesi olduğu belirlendi ama ekonomik olarak hasar çoktan gerçekleşti. Böyle bir kriz anında olaya neden olan ürünün tam menşei bölgesi hatta üretim alanı hızlıca belirlense tüketicide böyle bir panik havası yaşanmayacak ve bütün ürün satışlarına yansıyan bir düşüş olmayacaktı.

Bu olay sonrası Walmart, Güney Amerika'da küçük çiftliklerden ithal ettiği dilimlenmiş mangoların geldiği çiftliği mevcut sistemlerinin ne kadar zamanda saptayabildiği ile ilgili bir deneme yaptı[14] ve sonuç: 6 gün, 18 saat, 26 dakika. Eğer Blockchain bazlı bir sistem kurulu olsa bu süre saniyeler ile ölçülecekti.

İşin daha magazinsel tarafına gelirsek bir de son tüketicilerin ellerindeki ürünün hangi aşamalardan geçtiğini görebilmelerine imkân tanıması da avantajlardan biri.

Gayet tabii bu son iki örneği Blockchain olmadan da yapabilirsiniz (marketin kendi dahili kontrol mekanizmaları ile) ancak Blockchain girilen bilginin değiştirilemez olması, bağımsız denetçilerin de ürünün kalitesi ve verinin doğruluğunu rahatça kontrol edebilmeleri nedeniyle marketlerin tüketicilerine daha güvenilir bir ürün sunmasını sağlıyor.

[12] https://newfoodeconomy.org/blockchain-food-traceability-walmart-ibm/
[13] https://www.dallasnews.com/business/retail/2018/06/21/could-blockchain-food-chains-answer-romaine-lettuce-e-coli-outbreaks
[14] https://www.dallasnews.com/business/retail/2018/06/21/could-blockchain-food-chains-answer-romaine-lettuce-e-coli-outbreaks

Madem bu kadar avantajlı, neden kullanılmıyor hemen?

Peki madem bu kadar ciddi getiriler var, neden hemen adapte etmiyor bunu oyuncular? Komik gelecek ama şu an tedarik zincirlerinde Blockchain kullanılmasının önündeki en büyük engel, aslında Blockchain'in minimize etmeye çalıştığı ana konu ile aynı: güven. Blockchain'i kullanacak ve gerekli olan bilgileri girecek olan yukarıda bahsettiğimiz onlarca taraf, kendilerinin ve diğer tarafların doğru bilgiyi gireceklerine şüphe ile bakıyorlar. Bunun yanında, kendine ait özel bir datayı başka tarafların görmesinden dolayı duyulan çekince de var. Ama bu bir süreç. Örnek çalışmalar arttıkça, kurumlar yeni teknolojiye aşina oldukça burada da adaptasyon artacak. Kanuni altyapı düzenlemeleri de önemli tabii. Sadece bir-iki büyük müşterinin dayatması ile belli tarafları Blockchain'e sokabilirsiniz ama tüm taraflar için hükümetlerin gerekli hukuki düzenlemeleri yapması sürecin hızlanmasını ve adaptasyonun artmasını sağlayacak.

Sonuç

Diğer pek çok alanda olduğu gibi burada da yeni teknolojilerin kullanılması konusunda henüz emekleme aşamasındayız. Geniş kesimler tarafından bu teknolojilerin adaptasyonu zaman alacak. Şu anda altyapılar kuruluyor, mevcut oyuncular harıl harıl üzerine kurulacak sistemler oluşturmaya çalışıyorlar. Sektörlerdeki kuşkucu (skeptik) oyuncuları ikna etmeye çalışıyorlar. Zaman alacak. Belki bir on yıl istenen vizyon gerçekleşmeyecek. O zamana kadar aldığımız ürünlerde satıcı kurum ya da kişiye güvenmeye devam…





Sağlık için BLOCKCHAIN neler? çözümleri

Hasta hayatını kurtarabilecek bilginin hızlı paylaşımı ya da maliyet yaratan bürokrasinin azaltılması gibi konularda Blockchain bazlı girişimler sağlık sektörünün oyuncuları olan hasta, hastane, sigorta ve ilaç şirketlerine yeni açılımlar getirebilir.

Sağlık sektörünün sorunları ve sıkıntıları nerede?

2015 yılı Haziran ayında "thedarkoverlord" isimli bir hacker yaklaşık 10 milyon Amerikalı'ya ait medikal veriyi[15] 1 milyon ABD Dolarına yakın bir rakamdan satışa çıkardı. Hacker bu gizli medikal bilgileri dört ayrı şirketin ana bilgisayarlarından almıştı. İşte size merkezi sistemlerin en büyük dezavantajlarından biri: Verilerin bir arada tutulduğu merkezi yapılar her zaman güvenlik açığı tehlikesi taşır.

Öte yandan sağlık kurumlarının kendi özel veritabanlarını tutmaları ve hastaya ait bilgilerin kurumlar arasında paylaşımı ciddi bir sıkıntı. Sistemlerin birbiri ile konuşmaması bir yana bir şekilde iletişim sağlansa bile yaşanan gecikmeler dakikaların bile çok önemli olduğu kimi durumlarda daha ciddi sorunlara hatta ölümlere kadar giden kayıplara yol açabiliyor. Bilgi eğer hastanın kontrolünde olsa acil müdahale gerektiren kritik durumlarda hasta (ya da yakınları) o an ulaşabildikleri ilk sağlık kurumunda yetkili kişilere bu bilgilere erişime izin verebilir ve hastaya gerekli müdahaleler zamanında yapılabilir.

Hemen akla şu soru gelebilir: "Sağlık kurumları kendi aralarında anlaşsa ve bu sistemleri kursa ya? Ya da hükümetler onları zorlasa. Blockchain'e gerçekten gerek var mı?"

[15] https://www.zdnet.com/article/hacker-advertising-huge-health-insurance-database/

Buna üç farklı açıdan bakarak cevap vermek mümkün:

1. Öncelikle bu tip farklı sağlık kurumlarının birbirleri ile konuşmalarını sağlamak için gerekli sistem entegrasyonu ya da iletişimi oldukça zor, karmaşık ve zaman alıcı. Üstelik çok maliyetli. Halbuki bütün hastanelerin bağlanacakları ortak bir platform olsa ve hasta kayıtlarına bu platform aracılığı ile ulaşılsa sağlık kurumları ciddi bir yatırıma girmeden sistemin nimetlerinden faydalanabilirler.
2. Gecikmiş müdahalelerin hastada yol açacağı fiziki tahribat ve sonrasında bu tahribatların tedavisi için yapılacak masrafların büyüklüğü göz önüne alındığında, ortak bir platformun sigorta şirketleri için de ciddi bir tasarruf sağlayacağını öngörmek zor değil.
3. Bir de yukarıda en başta bahsettiğimiz bilginin değişik kurumlara açık olması durumunda yanlış ellere geçmesi ve güvenliğinin sağlanamaması konusu var.

Blockchain nasıl çözümler sunabilir?

Özellikle sağlık alanına hitap eden kişisel bilgilerin korunması, saklanması ve güvenli şekilde paylaşılması konusunda pek çok yeni girişim var. Sadece bununla da sınırlı değil elbette girişimler, özellikle ilaç kullanımı ile ilgili tüm zinciri ilgilendiren konularda çalışanlar da var. İsterseniz sözü daha fazla uzatmadan bu girişimlerden birer cümle ile bahsedelim.

Healthureum[16], Ethereum Blockchain'i kullanarak sizin medikal kayıtlarınız üzerinde tam bir sahipliğiniz olmasını sağlıyor. Yani kayıtlarınız Blockchain üzerinde şifreli olarak saklanıyor. Sizin izin verdiğiniz kuruluşlar sizin izin verdiğiniz ölçüde Healthureum platformu üzerinden bu kayıtlara ulaşabiliyorlar.

[16]https://www.healthureum.io/



Healthureum sistemi nasıl çalışıyor?



Tierion[17] da benzer şekilde hasta verilerinin sağlıklı bir şekilde kayıt edilmesi ve kayıtlarını tutarlılığı (değiştirilemezliği) konusunda çalışıyor ve Philips Blockchain Labs[18] ile iş birliği içinde. Keza MIT altındaki Media Lab merkezinden çıkma girişimlerden MedRec[19] de hastaların verilerini kendi kontrolleri altında izin verdikleri kurumlarla kolayca paylaşabilmesine yoğunlaşmış. Bir başka girişim Factom[20] ise Blockchain altyapısını kullanarak küresel ama özellikle sağlık hizmetlerine erişimin zor olduğu bölgelerde yaşayanların sağlık datalarının dağıtık bir yapıda (Blockchain üzerinde) tutulması ve biyometrik doğrulama ile erişimi konusunda uzmanlaşmış ve 2016 yılında Bill & Melinda Gates Foundation'dan yatırım almış.[21]



ScalaMed[22] ilaçlar ve reçeteler üzerinde yapılan sahteciliği önlemek amacıyla ilaç üreticileri, dağıtıcılar, hastaneler ve eczane zincirlerini bir araya getiren ve ilaçların kayıt, teyit ve transferinin güvenli, kaçağa yol açmayacak şekilde yapılmasını sağlayacak Blockchain altyapılı bir sistem üzerinde çalışıyor. Bu alanda çalışan diğer bir girişim olan MediLedger[23] ise Genentech ve Pfizer'i içine alan bir pilot çalışma ile benzer şekilde ilaçların üreticiden hastaya ulaşımındaki kaçakları önlemek için Blockchain bazlı çözümlere kafa yoruyor.

[17] https://www.tierion.com/
[18] http://www.2.forms.healthcare.philips.com/blockchainlabs
[19] http://medrec.io/
[20] http://www.factom.com
[21] https://www.gatesfoundation.org/How-We-Work/Quick-Links/Grants Database/Grants/2016/11/OPP1159449
[22] https://www.scalamed.com/
[23] https://www.mediledger.com/

Sonuç

Önceki bölümlerimizde de belirttiğimiz gibi, Blockchain tabanlı sistemler henüz emekleme aşamasında. Sağlık alanındaki girişimlerde odak daha çok kişisel bilgilerin korunmasına yoğunlaşmış durumda ve geçmişte yaşanan olaylardan dolayı bu gayet anlaşılır. Ancak hasta hayatını kurtarabilecek bilginin hızlı paylaşımı ve maliyetleri artıran bürokrasinin azaltılması gibi konularda da Blockchain bazlı girişimler sektöre yeni açılımlar getirebilir.

Özellikle sağlık alanında veri paylaşımında herhangi bir standart henüz oturmuş değil ve yukarıdaki örneklerde de gördüğünüz gibi bu alanda dominant oyuncu olmaya aday çok sayıda girişim var. Sağlık, ilaç ve sigorta sektörleri teknolojik yenilikleri yakından takip etseler de organizasyonel değişiklik getirebilecek değişim ve yeniliklerde genelde tutucu davranırlar. Dolayısıyla, özellikle tüm kurumların kullanabileceği ortak bir platforma geçiş konusuna da son derece ihtiyatlı yaklaşacaklarını hatta zorlansalar bile ayak direyeceklerini görmek sürpriz olmaz. Bakalım, Blockchain sağlık alanındaki yaşanan kimi dertlere bir şekilde deva olabilecek mi?





BLOCKCHAIN çevremizi korumamıza yardımcı olabilir mi?

Çevre Blockchain temelli fikirleri hayata geçirmede en mantıklı alanlardan biri. Neden? Blockchain çevre için neden önemli?

İçinde yaşadığımız dünyayı ciddi şekilde kirlettiğimiz ve kaynakları geri döndürülemez biçimde yok ettiğimizin artık belgeli hale gelmesi, hükümetlerin sorunu çözmeye yönelik ortak çabalarına 1990'lardan beri giderek artan bir hız kazandırdı. Bu çabaların sonuçlarını ise yeni yeni görmeye de başlıyoruz.

Örneğin 90'lı yıllarda artan CFC (kloroflorokarbon) gazı nedeniyle yaklaşık %10 seviyesinde incelen ozon tabakası bu gazın kullanımına yönelik alınan tedbirler sonucu 2000 senesinden itibaren her on yılda %3 oranında kalınlık artışı göstermeye başladı.[24] Harika haber. Yeterli mi? Hayır. Bu daha bir başlangıç ve üstelik şu anda Çin dahil kimi ülkelerin hala ürettikleri kimi kimyasallar ile ozon tabakası için bir tehdit olduğu iddia ediliyor.[25]

Çevre sorunlarının hükümetler tarafından koordine edilerek ele alınması doğru bir yöntem. Ancak sistemin karışıklığı, oyuncuların farklı çıkar ilişkileri, çevre konusunda yapılan yatırımların yüksek maliyetinden dolayı daha alınması gereken çok yol var.

[24] https://news.un.org/en/story/2018/11/1024842
[25] https://www.bbc.com/news/newsbeat-46107843

Zira, herhangi bir konuda öncelikle hükümetler anlaşmalı, sonrasında bu anlaşmalara uygun gerekli denetim ve ölçüm/bildirim mekanizmalarını kurulmalı, en sonunda da özel sektör ve kamu oyuncuları bu kurallara uygun davranıp aksiyonlarının sonuçlarını ölçmeli ve ilgili otoritelere bildirmeli. Oldukça yavaş işleyen bir mekanizma bu. Bu yavaşlık önümüzdeki nesillere miras olarak tamir edilemez hasarlara uğramış bir gezegen bırakmamıza yol açabilir.

90'ların başından beri yapılan müzakereler sonucu pek çok alanda hükümetler arası anlaşmalar yapıldı ve ülkelerin önüne özellikle çevre kirliliğini azaltma yolunda ödül/ceza sistemleri ve hedefler konuldu. Ölçümlemeler de uzun süredir yapılıyor. Bu ölçümler sonucu özellikle sera gazında önlenen hasarlar ile ilgili ödül kazanan firmalar bu ödüllerini çevreye zarar veren firmalara satarak çevre ile dost yatırımlarını daha karlı hale getiriyor. Yani yavaş yavaş çark dönmeye başladı.



Ancak henüz daha yolun başındayız. Sistemin doğru işlemesi için daha yapılacak daha birçok iyileştirme var. Ve burada Blockchain bazlı teknolojiler bize yardımcı olabilir. Konuyu sadece mevcut sistemin iyileşmesi olarak düşünmemek lazım. Sıfırdan yepyeni sistemler de kurulabilir. Bu alanda alınabilecek o kadar o kadar aksiyon var ki. Örneğin World Economic Forum çevre alanında uygulanabilecek 65 farklı fikir/girişim içeren bir rapor bile hazırladı.[26] (raporun pdf versiyonu da mevcut).[27] Bölümün kalanında bu raporun içeriğine bakacağız.

[26]https://news.un.org/en/story/2018/11/1024842 https://www.weforum.org/reports/building-block-chain-for-a-better-planet
[27]http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf

Blockchain nerede işe yarayabilir?

PwC ve Stanford Woods Institute ile birlikte hazırlanan bu rapor[26], özellikle iklim değişikliği, doğal çeşitliliğin kaybı ve su arzının kısıtlılığı gibi çevresel problemlerde Blockchain nasıl uygulanabilir konusuna odaklanıyor. Doğru kurgulandığında Blockchain teknolojisinin daha temiz, kaynakları daha doğru kullanan merkeziyetsiz çözümler sunup bu sayede doğal sermayeyi açığa çıkarma ve toplumları güçlendirme potansiyeli olduğundan bahsediliyor.

Bu arada bu sütunlarda daha önce dile getirilen iki konuya burada da dikkat çekiliyor. Birincisi yeni teknolojilerin, mevcut geleneksel ekonomik sistemleri değiştirirken (hatta ters-yüz ederken) yaratılan değeri sadece sermayedarlara değil tüm paydaşlara dağıtma gücü. İkincisi ise bu tip büyük değişimlerin kendiliğinden bir anda olmayacağı. Değişimin gerçekleşebilmesi için teknoloji sağlayıcılardan politika üreten kurumlara kadar farklı her bir paydaşın birlikte çalışma kabiliyeti kazanması gerek. Sadece teknolojik olarak bir platformun uygulanması yeterli değil, sistemlerin de değişmesi gerek bu değişimin kalıcı olması için.



[28]https://www.weforum.org/reports/building-block-chain-for-a-better-planet



Çevresel sorunlar neler?

Dünyada şu anda çevresel olarak sıkıntı yaratan konuları sıralarsak:

• İklim değişikliği: Şu anda sera gazı 3 milyon yılın en yüksek seviyesinde. 2100 yılında sadece Avrupa'da yılda 150.000 kişinin aşırı sıcaktan ölmesi bekleniyor.
• Doğal çeşitliliğin azalması: Mevcut canlı türlerinin beşte biri yok olma tehlikesinde ve yüzyılın sonunda bu oran %50 seviyelerine çıkacak. Amazonlardaki ağaç kesimi 2050 yılında bölgedeki yağış oranını %8 oranında azaltacak ve tüm dünya ekolojik olarak bu durumdan etkilenecek.
• Sağlıklı okyanuslar: Gerek plastik atıklar gerekse okyanusların sera gazını soğurması (absorbe etmesi) sebebiyle okyanuslarda asit oranı ve sıcaklık artışı hem balık sayı ve çeşidini hem de deniz altı zenginliklerini ciddi şekilde azaltacak.
• Temiz suya erişim: Yılda %1 oranında artan temiz su ihtiyacı şu anda 1,9 milyar insan için bir eksiklik ve 2050 yılında bu rakamın 3 milyara çıkması bekleniyor.
• Temiz hava: İnsanların %91'i Dünya Sağlık Örgütü'nün belirlediği değerden daha kötü hava koşullarına sahip bölgelerde yaşıyor. Yılda 7 milyon insan hava kirliliğinden dolayı yaşamını yitiriyor.
• Doğal felaketler: 2017 yılında 710 felaket yaşandı. Bu 1980 yılının tam üç katı. Toplam 330 Milyar ABD Doları hasar meydana geldi ve 23 milyon insan bu felaketler sonucu yer değiştirdi.

Blockchain çevre için hangi alanlarda faydalı olur?

İşte Blockchain bazlı sistemler bu alanlarda ciddi iyileştirmeler sağlayabilir. Neden Blockchain? Çünkü çok fazla oyuncu var. Bu oyuncular arasında tam olmasa da bir güvensizlik var (ve yaşanan pek çok felaketin ihmal ve daha korkuncu gizlemeden dolayı olduğu biliniyor). Denetim/ölçüm mekanizmaları henüz yeterli değil ve kurulması zaman alacak. Blockchain bazlı yenilikler piyasa oyuncuların maliyetlerini azaltabilir, yatırımların tamamlanma süresini kısaltabilir ve koruyucu kurumlara denetimde kolaylıklar sağlayabilir. Özellikle Blockchain teknolojilerinin zaman damgası özelliği ve akıllı kontratların işletileceği mekanizmalar verimli çalışan bir sistem kurulmasına yardımcı olabilir.

Mevcut durumu iyileştirmeye yönelik girişimler var mı?

Rapor mevcut durumu iyileştirmek amacı güden blockchain bazlı girişimleri şu şekilde grupluyor:

• Daha temiz ve verimli, merkezi olmayan sistemlere geçişi sağlayanlar
• Kaynak ya da ruhsatların kişiden-kişiye (Peer-to-peer-P2P) ticareti
• Tedarik zinciri yönetimi ve şeffaflık
• Çevresel sonuçları değerlendirecek finansal modellemeler
• Doğal sermayenin ve finansal olmayan değerlerin ortaya çıkarılması.

Bu girişimler daha çok süreci iyileştirmeye yarayacak getirileri nispeten marjinal fikirler. Bunların üzerinde fazla durmadan vizyon açan başka fikirler de var. Dilerseniz hemen onlara bakalım.



Peki ya ezber bozan girişimler?

Mevcut sistemleri iyileştirmek dışında ezber bozan girişimler de var. Ne demek bu? Mevcut iş yapış biçimlerini değiştirecek, reform yapacak girişimler. Bunu yaparken de bir yandan endüstriyel alandaki son yıllarda yaşanan yenilikleri de içine alacak biraz da onlar sayesinde vizyonlarına ulaşacak fikirler (Ancak hemen hatırlatalım, bu fikirlerin pek çoğu daha test aşamasında?—?henüz yaygın adapte edilecek kadar olgun değiller)

Şeffaf tedarik zinciri:

Pek çok kurum çevresel olarak hükümetlere ve topluma karşı taahhütlerde bulunuyor. Ancak şirketler ne kadar samimi olsalar da bu taahhütlerin ne şekilde yerine getirildiği ile ilgili bir açıklık yok özellikle tedarik zincirlerinde. Kaynaktan son kullanıcıya değiştirilemez ve şeffaf şekilde tutulan Blockchain verisi şirketlere hem riski algılamak ve kendi iç sistemlerini yönetmek hem de dış dünyaya aldıkları bu aksiyonları gösterebilmek açısından yardımcı olabilir. Şirketlere faydasının yanında son tüketici, sivil toplum kuruluşu ve hükümet gibi dış paydaşlara da bu eforu görme, takip ve takdir etme imkânı verebilir.

Merkezi olmayan ve sürdürülebilir kaynak yönetimi:

Mevcut merkezi elektrik-su-doğalgaz hizmet sağlayıcıların arz-talep dengesini sağlayamama, dağıtımda kaçakları önleyememe, tekil arıza noktası olma gibi sorunları var. Evlere yerleştirilecek akıllı alıcı (sensör) gibi endüstriyel yenilikleri kullanacak platformlar son kullanıcıların bu alanda yeni kapılar açıyor. Nasıl? Kullanım bilgisi ve alışkanlıklar konusunda onları daha bilgili ve donanımlı hale getiriyor ve merkezi olmayan yapıları kullanma konusunda ellerini güçlendiriyor. Hangi alanlarda? Kişiden kişiye ticaretten tutun, dinamik fiyatlama yapmaya, arz-talep dengesi içinde kendilerine en optimal hizmet sağlayıcıyı bulmaya kadar. Şu an için çok ütopik gelmekle birlikte bu konuda Brooklyn MicroGrid Project[29] isimli bir projenin New York'ta başlatıldığını hatırlatalım.



[29]https://www.brooklyn.energy/

Sürdürülebilir finans için kaynak sağlama:

Birleşmiş Milletlerin belirlemiş olduğu Sürdürülebilir Gelişim Hedefleri[30]'nin gerçekleştirilebilmesi için gerekli kaynaklar anlamında yıllık 5–7 Trilyon ABD Doları yatırım açığı var ve bunun 2,5 Trilyon ABD Dolarlık kısmı gelişmekte olan ülkelerde. Bu boşa harcanan bir para da değil bu arada. Bu alanda yapılacak yatırımlardan ciddi bir geri dönüş sağlanabilir- yani oldukça karlı yatırımlar ve bu alana yatırım yapmak isteyenler de var. Ancak veri eksikliğinden tutun, finansal karmaşıklığa pek çok sorun nedeniyle yatırımcılar ile ihtiyaç sahipleri bir türlü bir araya gelemiyor. Geldiği durumda başarı hikayeleri de ortaya çıkmıyor değil:



Sun Exchange isimli Afrika bazlı bir proje, evlere ücretsiz güneş enerjisi modülleri takma karşılığında ev sahiplerinin elektrik faturası yerine tasarruf ettikleri paranın bir kısmını kira olarak ödemesi şeklinde bir model geliştirmiş. Kira olarak ödenen rakam, kullanım bazlı olarak sensorlar aracılığıyla bu firmaya gönderiliyor. Eğer evde oturanlar kirayı ödemez ise yine sensörler aracılığıyla hizmet kesiliyor. Hatta bu sistemi Afrika dışında Filipinler'de kurma gibi bir girişimleri de olmuş ancak yabancı para cinsinden para tahsil ve transfer etmede sıkıntı yaşıyorlar. Bunu sorunu çözebilmek için Filipinler'de kripto para kullanımının yaygınlaşmasını beklemek zorundalar :)

[30]https://www.un.org/sustainabledevelopment/sustainable-development-goals/

Döngüsel ekonomileri teşvik:

Geri dönüştürülebilecek pek çok ürün yeterli teşvik mekanizmaları olmadığı için çöp haline geliyor. 2050 yılında okyanuslarda balıktan çok plastik atık olacağı tahmin ediliyor. Bu konuda örneğin plastik atıkları geri dönüşüme sokanlara kripto para veren birkaç girişim mevcut. Bu kripto paraları sonrasında yiyecek, su gibi ihtiyaçlar için kullanabiliyorsunuz. Ne kadar başarılı olur tartışılır. Ama daha ilginç projeler de var: Ormanların yok edilmesine karşı, GainForest isimli girişim çiftçilere ilginç bir finansal teşvik sağlıyor. Ormanlara yerleştirilen uydu sistemleri ile ağaç kesimleri takip edilebiliyor. Ağaçların bulunduğu alanında herhangi bir değişim olmaması durumunda akıllı kontratlar devreye giriyor ve çiftçilerin hesabına belli miktar para yatıyor.

Karbon emisyon pazarlarını değiştirmek:

Karbon emisyon ticaretinin başladığı ilk günlerden bu yana işlemlerin görünür ve izlenebilir olmaması, değişik ülkelerde uygulanan farklı standartlar ve kanunlar ile çifte harcama (double counting) gibi konular bu ticaretin verimliliği konusunda hep şüphe uyandırdı. Bu sorunları gidermeye yönelik IBM ile Energy Blockchain Labs'in ortaklaşa gerçekleştirdiği "Çin'de Karbon Kredi Yönetim Programı" başarılı olursa tüm dünyaya yayılmayı planlıyor.[31]

[31]https://www.ibm.com/case-studies/energy-blockchain-labs-inc

Yeni nesil sürdürülebilirlik izleme ve raporlama sistemleri:

Tedarik zincirine benzer şekilde tüm dünyada önde gelen kurumların sürdürülebilirlik bazında iş modellerini revize etmekle ilgili ciddi taahhütleri var ancak sarf edilen eforu tam layıkıyla gösterebilecekleri mekanizmalar az. Blockchain bazlı sistemler şirketlere kendilerini daha iyi ifade etme imkânı verirken, son kullanıcılara da bu şirketlerin performansını değerlendirme ve tüketim tercihlerini daha doğru yapabilme imkânı veriyor.





Bu çözümlerin önündeki engeller neler?

Yukarıda fikirlerin çoğu henüz ham, daha olgunlaşmamış. Gerçekleşmelerinin önünde engeller de var. Nedir bu engeller?

Öncelikle, bahsettiğimiz değişiklerin birçoğu tüketici alışkanlıklarında bir değişim gerektiriyor. Ekonomik menfaatler bu tip değişimleri hızlandırsa da kimi projeler pratik olmayabilir ve bu nedenle de yaygınlaşmayabilir.

Bunun yanında, bu sistemlerin destek olacak endüstriyel değişimler yeterince hızlı gelişmeyebilir ya da yenilikler Blockchain sistemleri ile uyumlu olmayabilir.

Tedarik zincirleri için Blockchain bölümümüzde belirttiğimiz gibi, çok partinin taraf olduğu sistemlerde oyunculardan bir kısmı hassas bilgileri diğerleri ile paylaşmak istemeyebilir.

Bunun dışında her ülkede kanunların farklı olması özellikle uluslararası nitelikteki projelerde adaptasyon ve canlılığa ket vuracak sıkıntılar doğurabilir.

Teknolojik olarak ise pek çok alanda değişik oyuncular tarafından geliştirilecek farklı Blockchain sistemlerinin birbirleri ile iletişiminin sıkıntı yaratabilir ancak yukarıdaki kültürel ya da kanuni sorunlara göre teknolojik sıkıntıların çok daha kolay şekilde aşılabileceğini düşünüyorum.



Sonuç

Evet, gördüğünüz gibi, kendi içinde bulunduğumuz ülkemiz ve küçük dünyamızı aşıp uluslararası alana baktığımızda, sınır ötesi işlemlerde Blockchain bazlı sistemlerin aracıları ortadan kaldıran yapısının hemen hemen her alanda gerek çevresel kazanç olarak gerekse finansal anlamda sağlayacağı faydalar olduğu çok açık.

Ulusal yapılar ve politik çıkarlar Blockchain ile ortaya çıkabilecek bu faydaları deneyimlememize ne kadar izin verecek bunu hep birlikte yaşayarak göreceğiz.



BLOCKCHAIN *seyahat* sektörünü *uçurur mu?*

Blockchain bize daha rahat, esnek ve ekonomik seyahatler sağlayabilir. Nasıl mı?

Dünyada en dağınık sektörlerden biri seyahat sektörü. Son kullanıcı olarak bizler bu dağınık yapının çok az bir kısmını görüyoruz. Bizim için acente ya da web üzerinden bir bilet almaktan ibaret gibi. Ama perde arkasında pek çok hizmet sağlayıcı bize bu hizmeti vermek için bir araya geliyor. Bileti ayarlayan acente, uçuşu sağlayan havayolu, bağlantı uçuşu varsa diğer uçuşu sağlayan havayolu. Bu işin sadece uçuş kısmı, bir de buna ekstra hizmetler (otel, kiralık araba vb.) eklerseniz iyice karmaşıklaşıyor.

Bunun ötesinde belki İstanbul'dan ya da Londra'dan New York'a uçmak nispeten zahmetsiz. Ama gelin bir de İstanbul'dan Tayland'daki Chang Rai'ye gitmeye kalkın. Mevcut ana havayollarının dışında nispeten az bilinen ve lokal uçuşlar yapan havayollarına binmeye kalkın.

Seyahat sisteminin sorunları neler?

Acenteler, havayolları, oteller her biri kendine özgü sistemler kullanan silolar. Başlangıçta kağıdın olduğu bir dünya üzerine kurulan bu sistemler, zamanla teknoloji gelişip de herşey elektronik olunca afallayıp kalıyorlar. Bu sistemlerden çıkan bilgiler standart değil, çoğu zaman da eksik ya da yanlış bilgi veriyor.

Paylaşılan bilgi doğru olduğunda ve sistemler mutabık kaldığında yolcular için her şey yolunda gidiyor ama istisnalar (iptaller, gecikmeler) olduğunda sorunlar zincirleme şekilde tüm sistemi etkiliyor (müşteriler tarafından yapılan itirazların oranının %5'i bulduğu havayolu şirketleri bile var). Malum, konu seyahat olduğunda bu tip sorunlar da eksik olmadığı için, tüm sektör aslında istisnalardan oluşan sorun yumağını çözmek için ciddi zaman, emek ve para harcıyor.

Sistemlerin birbirinden bağımsız olması nedeniyle oyuncular arasındaki ilişkiler de karmaşık. Bir havayolu bir uçağı uçuşa açtığında sistemlerinde bir ürün yaratıyor. Acentelere bu ürünü satmak için imkân verdiğinde aslında bir nevi acentelere bir tür kredi açmış oluyor. İşte bu kredi nedeniyle acenteler, üye olan havayolları için havayolları birliği olan IATA'ya, üye olmayanlar havayollarından her birine ayrı ayrı kapora ödemesinde bulunmak zorundalar. Ayrıca acenteler ile havayolları arasındaki bu bilet satışının ödemesi için günlerce süren uzun ve yüksek komisyonların ödendiği bir hesaplaşma süreci var. Şöyle söyleyelim: sadece IATA hesaplaşma sistemi yılda 400 milyar ABD Doları işlem yapıyor ve sırf bu işlemler için bankalara 7,7 milyar ABD Doları komisyon ödeniyor.[32]

Blockchain bu sorunları çözmek için neler getirebilir?

Yukarıda yazdığımız sorunların temel nedeni eski birbirinden bağımsız sistemlerin yarattığı veri eksikliği/yanlışlığı ve sistemlerin birbiri ile konuşmaması. Eğer tüm servis sağlayıcılar bir araya gelip bir standart oluşturulabilir ve herkes sistemlerini buna göre güncelleyebilse bunca sorunu çözmek mümkün olabilir. Ama başka öncelikler (gelir artırma gibi), sistem güncellemenin yüksek maliyeti, tüm kurumları bir araya getirecek bir ortak/merkezi irade olmayışı gibi nedenlerle bu çok mümkün görünmüyor.

[32]http://airlines.iata.org/blog/2017/09/blockchain-can-rebalance-the-value-chain-to-benefit-airlines-and-passengers

Blockchain için her zaman söylediğimiz, belli bir merkezi otoritenin varlık nedeni olan güven ihtiyacını minimuma indirebilmesi. Burada da Blockchain herhangi bir partinin güdümünde olmayan ve tüm partilerin güvenle bağlanabilecekleri bağımsız bir platform olarak taraflar arasındaki bilgi paylaşımı ve para ödemelerini rahatlıkla gerçekleştirebilir.

Sorun çözme yanında yeni fırsatlar da yaratılabilir mi? Örnek: Further Network

2016 yılında Türkiye'de kurulan Further Network[33] Blockchain'in olanaklarını kullanarak yukarıda yazdığımız sorunlara çözüm üretmeyi, özellikle yüksek işlem maliyetlerini minimuma indirmeyi hedefliyor. Ancak vizyonları bununla sınırlı değil. Son kullanıcılar için büyük kolaylıklar getirmeyi planlıyorlar. Bunlardan biri uçuş biletini basit bir kâğıt parçasından daha akıllı hale sokmak. Daha önce bahsettiğimiz Akıllı Kontrat haline getirmek. Ne demek bu? Normalde aldığınız bilet size ait bilgiler, uçuşunuzun detayı ve kaç para ödediğinizi yazar. Buna daha başka detaylar eklemek istemez misiniz? Örneğin vejetaryen menü istediğiniz, seyahatte size özel TV programlarının (mesela sadece romantik komedileri) sunulmasını, koltuk arası genişliğinin belli bir cm'den fazla olmasını? Bu ve benzeri bilgileri kendi dijital kimliğinizde paylaşabilir ve dilediğiniz partiye dilediğiniz kadar bilgiyi verebilirsiniz (havayoluna başka, otele başka).



[33]https://further.network/



Geniş koltuk aralığı için ekstra ücret öder misiniz?

Bir başka kolaylık da uçuşları daha değiştirilebilir hale getirmek. Birkaç uçuştan oluşan bir biletini uçuşlarından birini otomatik değiştirmek, uçuşu (ya da bir ayağını) bir başkasına devredebilmek gibi.

Otellere de bakalım: Seyahat acenteleri bir şehirdeki konaklama olanaklarını (otel hatta evleri bile) akıllı bilet haline getirebilirler. Siz de herhangi bir şehirdeki bir fuara gitmeden önce dijital kimliğinizden istediğiniz bilgileri paylaşarak istediğiniz konaklamayı alabilirsiniz. Bunu ödemek için de istediğiniz para cinsini ya da kripto parayı kullanabilirsiniz.

Ödeme demişken, son kullanıcı olarak ödediğimiz bu parayı, Akıllı Kontratımız havayolu, seyahat acentesi ve diğer servis verenler arasında otomatik olarak bölüştürecek, arka plandaki pek çok pürüz yok olacak.

Further Network, yukarıdaki sistemin çalışabilmesi için bir de kendi Token'ı olan Aton'u çıkarıyor. Daha önceki "Değişen Dünyada Girişimcilik" bölümümüzde Token Dünyası'nın nasıl çalıştığından bahsetmiştik . Further Network de sadece bir şirket değil bir ekosistem yaratıyor ve hisse senedi çıkarmak yerine Aton'u çıkararak gerek kendisini fonluyor gerekse de sistemin çalışması için gerekli enerjiyi sağlıyor. Örneğin Blockchain içindeki oyuncuların yeni işlem (örneğin Akıllı Bilet) yaratmak için Aton'a ihtiyacı olacak. Ya da sistem içindeki tüm işlemleri Aton üzerinde tutarak, sistem kullanıcılarına dünyadaki mevcut paralardaki kur değişimlerinden bağımsız bir bakiye ölçme aracı sunacak. Bunun yanında taraflar arasında ödeme için Aton kullanılması durumunda eskiden günlerce süren klasik paralar ile ödeme işlemlerinin anında yapılması sağlanacak. Böyle bir sistemin benimsenmesi durumunda, işlemler anlık olacağı için eskiden olduğu gibi acentelerin IATA ya da havayollarından işlem yapması için gerekli olan yüksek kapora ödemlerine de gerek kalmayacak.

Başka ne tip girişimler var?

Ülkemizden çıkan en prestijli yeni nesil sistemlerden olan Further Network bu alanda rakipsiz değil. İsviçre/Çekya merkezli havayolu taşımacılığını benzer şekilde sarsmayı planlayan Winding Tree[34], keza benzer şekilde çalışan Finlandiya merkezli ETH Travel[35], Çin merkezli otel rezervasyonları üzerine uzmanlaşmış Tripio[36] bu alanda pay almak için çabalayan yüzlerce yeni nesil girişimlerden sadece birkaçı. Sistemin mevcut oyuncuları da elleri kolları bağlı oturmuyor tabii- örneğin IATA mevcut süreçlerini basitleştirmek için pek çok proje[37] deniyor ama bu hantallık ile ne kadar yol alacakları gerçekten meçhul.

[34] https://windingtree.com/
[35] https://ethtravel.io/
[36] http://trip.io/
[37] http://www.iata.org/whatwedo/stb/Pages/index.aspx



Sonuç

Karmaşık ve eskimiş sistemler nedeniyle şu an yalpalamakta olan seyahat sektöründe önümüzdeki on yıl içinde büyük değişimler olması kaçınılmaz. Bu değişimler biz son kullanıcılara daha fazla konfor getirecek. Klişe olacak ama hizmet verenler ise bu değişime ayak uydurdukça sağ kalacaklar- Uyduramayanlar ise hak ettikleri değeri görüp iş hayatının tarihinde kalacaklar. Ülkemizden çıkan ve global bir oyuncu olmayı hedefleyen Further Network ise yeni nesil teknolojileri kullanarak doğacak fırsatlardan pay almak için oldukça avantajlı bir konumda-dileriz doğru ortaklıklar ile bu alanın önde gelen oyuncularından biri olurlar

Dipnot: Uçuş işleminin parçaları*

Seyahat sisteminin oyuncuları 40 yıl tasarlanmış sistemler ile günümüzün hızlı dünyasına ayak uydurmaya çalışıyorlar. Bu ne yazık ki çok mümkün değil. Sistem değiştirmek hem pahalı hem de 7/24 devam ettiği için riskli. Elektronik bilete geçmek bile 15 yılı buldu.

Bir uçuş ve konaklama işlemini üç parçaya ayırmak mümkün:

• Uçuş (ya da konaklama) verisinin ve rezervasyonların sisteme ve son kullanıcıya iletilmesi. Bunu uçuşlar için Sabre, Amadeus, konaklama için Hotelspro ve HotelBeds sağlıyor
• Sistem kullanıcıları arasında bir uçak bileti satın alınması işleminin gerçekleştirilmesi. Burada her servis sağlayıcı kendi sistemini kullanıyor
• Partiler arasında satın alma sonucu ödenen paranın paylaştırılması. Burada da aynı şekilde herkes kendi yağıyla kavruluyor
Yukarıdaki üç parçadan ilki için sistem ile kullanıcı arasındaki bilgiyi IATA (International Air Transport Association) sağlıyor. Ancak mevcut havayolu taşımacılığında senede 3,7 milyar yolcu taşınırken bunun yalnızca %65'i IATA üzerinden geçiyor. Kalanı ise IATA üyesi olmayan 460 havayolu ile taşınıyor ve aralarında standart bir bilgi paylaşımı yok.

*Further Network'un yayınladığı white paper[38]'dan alındı.

[38]http://www.iata.org/whatwedo/stb/Pages/index.aspx

BLOCKCHAIN geleceği *tahmin* için kullanılabilir mi?



Blockchain ile geleceği tahmin etmek mi? Yok, o kadar değil ama burada bile Blockchain belli alanlarda çığır açabilir.

Tahmin piyasaları (Prediction Markets) ne demek?

Geleceği tahmin etmek derken aslında kastettiğimiz "tahmin piyasası" (prediction market). Ne demek bu? Tahmin piyasaları esasında, insanlara gelecek ile ilgili tahminlerin hisselerinin satıldığı piyasalar. Normal bir hisse senedi piyasasından farklı değil, sadece alıp sattığınız bir şirketin hissesinden ziyade bir olayın olma ya da olmama ihtimali üzerine çalışıyor.

Bu tip borsalar şu anda normal olarak var. Özellikle vadeli işlem borsaları bu iş için kurulmuş durumda. Blockchain ile bu tip borsalar merkezi bir yapıdan, adem-i merkezi yani herhangi bir merkezi olmayan dağıtık bir yapıya kavuşacaklar. Bunun ne gibi avantajları var?

Akıllı kontratların tahmin piyasalarına etkisi olur mu?

Blockchain'in ana temellerinden birinin Akıllı Kontratlar olduğuna şu bölümde değiniyoruz. Özetlemek gerekirse, Akıllı Kontratlar içeriği itibariyle aslında akıllı olmayan gayet basit kontratlar.

Ancak Akıllı Kontratları güçlü yapan, hiçbir dış etken etkisinde kalmaması ve eğer gerekli koşullar oluştu ise o kontratın gerektirdiği her türlü sonucu "tak" diye yapması idi.

Bu ne sağlıyor? Bu insanlar için öncelikle "akıl sağlığı" (piece of mind) sağlıyor. Ne demek bu? Şu demek, bir anlaşma yaptığınızda "acaba karşı taraf sözünü yerine getirmezse" diye geceleri uykunuzun kaçmasına gerek yok. İyi yapılmış bir Akıllı Kontrat size otomatik olarak hakkınız olanı verecek.

Peki nasıl çalışacak sistem? Şöyle: Herhangi ama herhangi bir konuda gelecek ile ilgili bir tahmininiz var. Örneğin, İstanbul Şişli'de oturuyorsunuz ve yeni yılın ilk günü saat 12:00 ile 16:00 arasında kar yağacağına eminsiniz. Etrafınızdaki insanlara sordunuz, çoğunun bu konuda bir fikri yok; hatta böyle bir iddiada bulunduğunuz için size deli gözüyle bile bakabilirler. Halbuki, o gün İstanbul'da ya da Türkiye'de ya da dünyanın herhangi bir yerinde sizin gibi başka bir 'deli' İstanbul'da havanın aynı saatler içinde günlük güneşlik olacağını düşünüyor ve iddia ediyor olabilir!

Birincisi böyle bir düşünen bir insanı normal yollardan çevrenizde bulmanız çok zor. O nedenle internet üzerinden ortak bir platform olması mantıklı. Ama daha önemlisi varsayalım çevrenizde böyle bir insan buldunuz ve iddiaya girdiniz, peki o insanın sözüne nasıl güveneceksiniz? Ya cayarsa? Hadi diyelim, oturdunuz noterden bir sözleşme imzaladınız, ya yine ödemez ise? Gidip mahkemeye mi vereceksiniz? Uğraş dur, üç kuruş para alacağım diye tonla masrafa gir. Üstelik eminim hâkim ve savcılar da böyle gereksiz konularda onları uğraştırdığınız için size çok da sevgiyle bakmayacaklardır.

Blockchain üzerindeki bir platformdan aynı işlemi gerçekleştirdiğinizde, öncelikle bu tip tahminlerde bulunan pek çok kişi ile aynı ortamda olduğunuz için tahmininizin tersini düşünen birini bulmanız çok daha kolay. Daha da önemlisi böyle bir kişi bulup anlaşma yaptığınız anda artık rahatsınız. Zira, öncelikle bu tahmininiz Blockchain üzerinde kayıt altına alınıyor ve daha önce de pek çok kez yazdığımız gibi Blockchain üzerindeki kayıtlar hiçbir şekilde hiç kimse tarafından geriye dönük olarak değiştirilemiyor. İkincisi de, Akıllı Kontrat sayesinde yaptığınız tahminin sonucunu aldığınız anda sistem iddiayı kazanan kişiye gerekli ödüllendirmeyi otomatik olarak yapıyor.

Burada kritik konulardan biri, aranızdaki iddianın ne şekilde sonuçlandığına kimin karar vereceği. Bunun için piyasanın güvendiği bir ortak hakem belirleyebilirsiniz (örneğin maç sonuçları için espn.com, hava tahminleri için accuweather.com, belli ekonomik göstergeler için wsj.com gibi), ya da bu iş için özel olarak eğitim almış (bu platformlar için çalışan) aracıları kullanabilirsiniz.

Bireysel tahmin mi sadece yoksa daha geniş bakabilir miyiz konuya?

Tahmin piyasalarını sadece kişilerin istedikleri tahminleri yapacakları bir enstrüman gibi görmemek lazım. Aslında burada önemli konulardan biri de bu tip piyasalar sayesinde gelecek ile ilgili toplumun ne düşündüğü konusunda iyi kötü tahmin yapabilme, yani toplumun nabzını tutabilme imkânı. Bir nevi araştırma ya da anket şirketlerinin yaptığı tahminlerin çok ötesinde insanların ne düşündüğünü ve ne tahmin ettiğini bu piyasalar sayesinde kestirebilirsiniz. Örneğin, bir sonraki seçimlerde Almanya'da Merkel'in iktidarda kalma ihtimali konusundaki tahmini oranlarından (olacağına inananlar bu ihtimali satın alabilir, inanmayanlar da satabilir) ya da bu ihtimal için biçilen değerin zaman içinde artmasından ya da azalmasından kamuoyunun ne düşündüğünü bulabilirler.

Zaten hazırda çözümler var, neden buna ihtiyaç duyuluyor?

Normalde tahmin oyunları için kullanabileceğiniz merkezi yapılar var ve gayet de güzel işliyor. Pek çok vadeli işlem borsası var finansal alanda. Ya da spor karşılaşmaları için örneğin ülkemizde Spor-Toto teşkilatının sunduğu iddaa[39] sayesinde pek çok spor karşılaşması için bahis yapmak mümkün. Tabii böyle yapıların belli kısıtları var: mesela sadece iddaa'nın size sunduğu karşılaşmalara tahminde bulunabiliyorsunuz, üstelik oranları da iddaa belirliyor. Dolayısıyla, sadece iddaa'nın belirlediği alanda onun topuyla oynayabiliyorsunuz.

[39] http://www.iddaa.com/

Pek çok kişi için makul olsa da daha özgür hareket etmek isteyecek bir kesim için çok da tatminkar bir oyun değil bu. “Topumu alıp aşağı mahallede istediğim kurallarla oynarım” demek isteyebilir kimileri.

Bunun yanında merkezi platformların her zaman belli bir otorite tarafından kanuni yaptırımlara tabi olması kimi insanlarda “acaba burada yaptığım bir tahminin sonucunda kazanırsam kanuni bir nedenle hakkımı almama ihtimalim olur mu?” şeklinde bir kuşkuya neden olabiliyor. Merkezi olmayan bir platformda kanuni otoriteler nasıl bir denetim yapacaklar, ya da ne kadar denetim yapılabilir, bunu kestirebilmek için henüz çok erken. Toptan yasaklama genelde çözüm olmuyor. Ne ile karşı karşıya olduğunuzu iyi düşünmek lazım, aksi takdirde bu platformlardaki aktiviteyi illegal yollara düşürmek, kanun koyucu için de ciddi bir vergi kaybı anlamına gelebilir. En doğrusu bu platformlarda belli tahminlerin yapılmasının önüne geçmek olabilir (örneğin kötü bir olayın, bir isyan, suikast ve benzerinin olması gibi).



Bunun yanında bir de merkezi olmayan platformların komisyon miktarı açısından merkezi platformlara göre çok daha maliyetli olduğunu belirtmek lazım. Zira merkezi platformlar tahmin için belirledikleri oranların içine hatırı sayılır miktarda kendi komisyonlarını koyuyor. Merkezi olmayan platformlar ise aslında bir borsa gibi o tahminin alıcısı ile satıcısı arasında aracı oldukları için her iki taraf için de kazanma durumunda alacakları ödül miktarı artıyor.

Tahmin piyasası oyuncuları kimler?

Tahmin piyasasının içindeki en büyük oyuncu şu an itibari ile Augur.[40] Daha önce de bahsettiğimiz Ethereum[41] platformunu kullanarak Reputation (REP) adını verdikleri bir token çıkaran Augur bu alanın öncülerinden biri. Augurun 2019 yılı ortası itibariyle yaklaşık 140 milyon ABD Doları değeri var.



Bu alanda ikinci büyük Gnosis[42] de benzer şekilde Ethereum üzerine kurulmuş, yaklaşık 20 milyon ABD Doları değere sahip bir platform. Gnosis de GNO adını verdiği bir token ile kripto para borsalarında işlem görüyor.

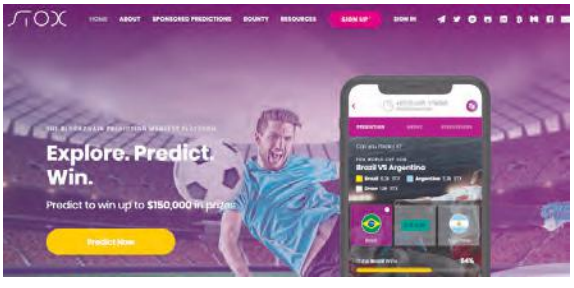


[40] http://www.augur.net/
[41] http://www.ethereum.org/
[42] http://www.gnosis.pm/

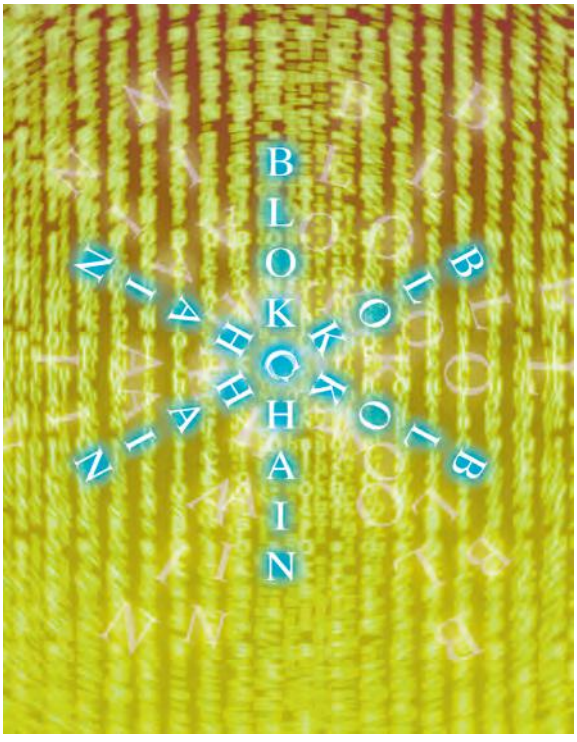
Bir diğer bu alanda çalışmayı planlayan platform Hivemind[43] ise Bitcoin üzerine kurulu ancak şu anda henüz Ar-Ge aşamasında. Bunun yanında Çin piyasasında ön plana çıkan ve Qtum Blockchain platformunu kullanan Bodhi[44] ve Ethereum platformunu kullanan Stox[45] da tahmin piyasaları pazarından pay kapmaya çalışan diğer oyuncular olacak gelecekte.







[43]http://www.bitcoinhivemind.com/
[44]http://www.bodhi.network/
[45]http://www.stox.com



Sonuç

Kişisel olarak gelecek ile ilgili istediğiniz konuda (bir karşı taraf bulabilmek şartıyla) sınırsız şekilde tahmin yapabilme imkânı büyük bir güç. Bunun yanında kişilerin bireysel düşüncelerini toplayarak toplumun (ya da bir kesiminin) kolektif düşüncesini görebilmek/anlayabilmek de belirli olayların nasıl gelişeceğini önceden anlayabilmek için oldukça önemli bir gösterge. Bu alanı şans oyunları gibi dar bir kapsamdan çıkararak çok daha bilimsel tabanlı bir şekilde değerlendirmek gelecek için pek çok konuya daha iyi bakabilme imkânı verecek. Bu alandaki büyük potansiyeli görmek için kâhin olmaya gerek yok :)

BLOCKCHAIN'i *sosyal* fayda için kullanabilir miyiz?



Bu bölümde, finansın soğuk ve rakam dolu dünyasından biraz uzaklaşarak, Blockchain'in dünyayı daha güzelleştirecek filantropi ve insani yardım işleri için nasıl kullanıldığına bakalım dilerseniz.

Blockchain ile ilgili şimdiye kadar yazdıklarımızı tek bir cümle ile özetlemek gerekirse, eski dünyada aracılar tarafından yürütülen her işlem ve bu işlemlerin olmazsa olmazı "güven" ihtiyacı, şifreleme teknolojisi sayesinde aracılardan makinelere geçiyor.

Bu dalga en çok da aracıları (ve güvene) en çok ihtiyaç duyulan finans kesiminin aktörlerini etkileyecek. Ama konu sadece finans sektörü ile sınırlı değil. Aracıların olduğu her sektörü ilgilendiriyor.

Birleşmiş Milletler Dünya Gıda Programı (WFP) geçtiğimiz yıl Mayıs ayında Ürdün'de yeni bir program başlatır. Azrak Göçmen Kampı'nda bulunan mültecilere o bölgede bulunan bir marketten alışveriş yapmaları için kuponlar dağıtır.

WFP, bu kuponları halihazırda kullandığı biyometrik tanımlama teknolojisinin içine Blockchain'i entegre eder, dolayısıyla mülteciler süpermarkette retina okuyucuya bakarak[46] bu kuponları kullanırlar. Bu sayede, mültecilerin bütün işlemleri sorunsuz bir şekilde Blockchain üzerinde tutularak, hem bürokrasi ve kâğıt masrafından hem de bankalara verilen komisyonlardan tasarruf sağlanır. Proje o kadar başarılı olur ki, WFP projeyi tüm Ürdün'e yayarak, ayda 100.000 ABD Doları tasarruf sağlamayı planlamakta[47]…



Suriye'de bir kadın verilen kuponunu kullanmak için göz taramasından geçerken

[46] https://www.wfp.org/news/news-release/wfp-introduces-innovative-iris-scan-technology-provide-food-assistance-syrian refu?_ga=2.69982032.171380775.1522352727-1632756231.1522352727

[47] https://www.wired.com/story/refugees-but-on-the-blockchain/

Blockchain konusundaki iyimserler, mültecilerin işlemlerinin kayıt altına alınması sayesinde insanların bir kredi geçmişi oluşturulabileceğini ve yeni yerleştikleri ülkelerde finans sistemine girişlerinde kolaylık sağlanabileceğini düşünüyorlar.

Benzer şekilde dünyada gelişmekte olan ülkelere yapılan yardımların %30'u heba oluyor[48], ihtiyaç sahiplerine ulaşamıyor. Neden? Aracılara ödenen paralar ve yolsuzluk. İrlanda Kızılhaç'ı bu nedenle Lübnan'da mültecilere gönderdiği kuponları Blockchain teknolojisi ile takip ederek böyle hangi ürünlerde kullanıldığını anlık olarak görme imkânına sahip olur[49]. Bu, onlar için de bir aydınlanma olur, zira normalde nakdi olmayan yardımlar genelde gıda maddeleri ile sınırlı olurken, burada ailelerin genelde temizlik malzemesi satın aldığını fark ederler. Ayrıca kurum, bu sistem sayesinde bağışçılarına yaptıkları bağışların hangi alanlarda kullanıldığını da takip etme olanağı verir. Verdiğiniz yardımın insanların hayatına dokunduğunu görmekten alacağınız manevi tatmini artırmanın yanında, sonra yapacağınız bağışlar için de ciddi bir motivasyon olacağını söylemek doğru olur sanırım.



Sırbistan üzerinden para yardımı şeması



Benzer konuda, Birleşmiş Milletler Kalkınma Programı (UNDP) ülkelerinden uzakta bulunan diasporaların anavatanlarındaki soydaşlarına gönderecekleri paralar için Blockchain altyapısını nasıl kullanır ve yaklaşık %7'lere varan maliyetleri nasıl düşürebiliriz sorularına cevap bulmaya[50] çalışıyorlar. Projenin doğuş nedenlerinden biri gönderilen paraların soydaşlar tarafından ağırlıklı alkole harcanmasının diasporanın canını sıkmış olması. Benzer konuda, Birleşmiş Milletler Kalkınma Programı (UNDP) ülkelerinden uzakta bulunan diasporaların anavatanlarındaki soydaşlarına gönderecekleri paralar için Blockchain altyapısını nasıl kullanır ve yaklaşık %7'lere varan maliyetleri nasıl düşürebiliriz sorularına cevap bulmaya[51] çalışıyorlar. Projenin doğuş nedenlerinden biri gönderilen paraların soydaşlar tarafından ağırlıklı alkole harcanmasının diasporanın canını sıkmış olması.

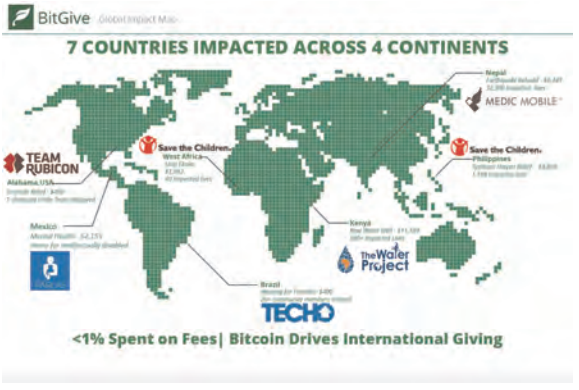
[48] https://www.cgdev.org/blog/how-much-aid-really-lost-corruption
[49] https://medium.com/@DemandASME/as-they-say-follow-the-money-462f00ac16bd

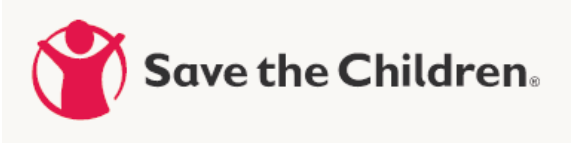
[50] http://altfinlab.org/blog/serbia-sending-remittances-from-serbian-diaspora-to-the-city-of-nis-beneficiaries
[51] http://altfinlab.org/blog/serbia-sending-remittances-from-serbian-diaspora-to-the-city-of-nis-beneficiaries





2013 yılında ABD'de kurulan BitGive[52] kâr amacı gütmeyen ilk Bitcoin bazlı yardım kuruluşu. Bağış kampanyaları düzenleyen bu kuruluş, aynı zamanda ihtiyacı olanlara ulaşması için toplanan paraların izlediği tüm yolu Blockchain üzerinden takip ediyor. Böylece bu bilgiler kesinlikle değiştirilemiyor ve anlık olarak gözlemlenebiliyor. Kurum bağışçılardan Bitcoin toplayarak, Nepal'deki depremde kırsal bölgeler ile merkezler arasında irtibatın kurulumuna yardımcı olacak mobil telefon alınmasından[53], Kenya'daki bir kız okuluna kuyu açılmasına[54]; Filipinler'den[55], Brezilya ve Meksika'ya, küçük ama insanların hayatlarına dokunan projeler için kampanyalar düzenliyor. Bunlar somut, gerçekleşen örnekler ve bu örneklerin benzerleri artarak kullanılmaya devam edecek. Blockchain her derde deva olmayacak ama yine de başarılı birkaç proje bile dünyayı daha güzel ve yaşanır hale getirecek kuşkusuz.







[52]http://www.bitgivefoundation.org
[53]http://www.bitgivefoundation.org/medic-mobile-campaign/
[54]https://thewaterproject.org/community/projects/kenya/a-new-well-in-kenya-4333
[55]https://www.savethechildren.org/us/what-we-do/emergency-response/historical-emergencies/typhoon-haiyan

BLOCKCHAIN *sanat* DÜNYASINA NEkatabilir?



Mona Lisa'nın bir parçasına sahip olmak ister misiniz? Yakın zamanda mümkün olacak gibi görünüyor.

Bir konuyu tekrar vurgulamakta yarar var: Blockchain çok yeni bir teknoloji-dolayısıyla kullanım alanlarına baktığımızda gördüğümüz örnekler genellikle çok yeni ve deneysel. Bu teknolojinin pratik hayatta etkilerinin daha iyi hissedilmesi için bu örneklerin hem çoğalması hem de olgunlaşması gerekiyor. Bu kitaptaki amaç, ilgisi olan okuyuculara bu teknolojinin nasıl kullanılacağı konusundaki vizyona dair fikir vermek. Bu bölümde ise Blockchain'in sanat dünyasının yaratıcı ve tüketicilerine neler sunabileceğine birkaç kullanım örneği üzerinden bakacağız.

Sanat sanat için mi… yoksa kimin için?

Bir resim gördünüz ve çok beğendiniz. Sahip olmak ister misiniz? Tabii. Ama fiyatına baktınız?—?eyvah! Değil aylarca, yıllarca çalışsam almam mümkün değil. Tüh bak kaçırdık! Halbuki şimdi alabilsem, biliyorum ki beş yıl sonra bunu belki de üç-beş katına satabilirim.

Size bu resmin tamamına değil ama bir parçasına sahip olabilirsiniz desem? Üstelik, bu sahip olduğunuz parçayı yatırım olarak tutup sonra istediğiniz zaman satabileceğinizi? İlginizi çekti değil mi? İyi ama nasıl olacak bu?

Hayal gibi ama bir gün bu da olacak. Şu an Blockchain teknolojisini kullanan "start-up"lar size bu imkânı verecek platformlar için çalışıyor. Örneğin Artrium[56] "Art-sharing" denen bir konsepte sahip.

[56] http://artrium.co/

Nasıl çalışıyor sistem? Üç ana adım var: Satın alınacak resim önce eksperler tarafından dikkatlice kontrol ediliyor ve orijinalliği teyit ediliyor. Satın alım sonrası Blockchain üzerinden küçük parçalara bölünüyor ve bu parçalar onlarca müşteriye satılıyor. Daha sonra kendi içinde mini bir borsa ile parçalar yatırımcılar arasında el değiştirebiliyor. Blockchain burada gerek sanat eserinin tümünün gerekse ona ait bölünmüş her bir parçanın tek tek aidiyetini ve alınıp satıldığında yeni sahipliğini hem takip hem de kayıt ediyor.

Yukarıda verdiğimiz örnek, sanat yatırımlarına Blockchain'in getireceği bir yenilik. Peki sanatçılar tarafında durum nasıl? Blockchain'in sanatçılara faydası var mı? Görünüşe göre evet. Yukarıdaki örnekte olduğu gibi sanatçıların yarattığı eserlerin (özellikle dijital sanat eserlerinin) kopyalanması/çalınmasına karşı güzel önlemler var: Örneğin, sanatçı tarafından Blockchain üzerinde yarattığı parçanın hem sahipliğinin hem de yaratılan kopya sayısının kaydının yapılması gibi (hatırlarsanız Blockchain üzerinde yapılan bir kaydın değiştirilmesi mümkün değil). Sahiplik ve kopya sayısına yönelik ilginç bir örnek ile devam edelim.

Kripto Kediler... peki var mı başka acayiplikler?

Dijital sahipliğin ve Blockchain teknolojisinin bir araya geldiği son nokta "Dijital Koleksiyonculuk" olarak da adlandırılan ve dijital bir oyun olan CryptoKitties[57]. Nedir bu diye soracak olursanız: CryptoKitties sitesindeki kedileri inceliyor ve beğendiğinizi satın alıyorsunuz. Aldığınız kedinin pek çok değişik özelliği var almadan önce inceleyebileceğiniz (göz, tüy rengi türü vb.) ancak bilmeniz gereken bir detay: bu kediden sadece bir tane var, başka eşi yok (bir insan gibi her bir kedinin DNA'sı farklı ve Blockchain üzerinde tutularak bu DNA'nın güvenliği sağlanıyor).

[57]https://www.cryptokitties.co/

Sonra bu kediyi bir başka kedi ile "çiftleştirerek" yepyeni bir kedicik yaratabiliyor ve bu kediciği satabiliyorsunuz. Bu kedilerin ilk jenerasyonu sınırlı sayıda yaratıldığı için çok talep görüyor. Çiftleştirme yapılan kediler eğer pahalı bir cinse aitse ise yavrusu da cins ve pahalı olabiliyor ama bir garantisi yok—aynı her ünlünün çocuğunun annesi ya da babası kadar ilgi çekici olmadığı örnekler gibi.

"Hadi canım olur mu öyle şey, çok saçma" demeyin. Geçtiğimiz Kasım ayında faaliyete geçen siteye, daha ilk ayında 180.000 kişi kayıt oldu ve 20 Milyon ABD dolarından fazla para harcadı[58]. Ondan fazla kedicik 100.000 ABD Doları'ndan yüksek fiyata satıldı. Sitenin sahibi şirket Mart ayı başında Anderseen Horowitz (Twitter ve AirBnB'nin ilk yatırımcılarından) ve Union Square Ventures (Zynga, Twitter ve Foursquare'in ilk yatırımcılarından) gibi dünyanın en saygın özel sermaye şirketlerinden 12 Milyon ABD doları yatırım aldı. İnsanlar sırf bu kediciklerden satın alabilmek için kripto para dünyası ile tanışıp Ether satın aldılar. Kripto paraların sanal dünyada en yaygın kullanım gördüğü alanlardan biri oldu CryptoKitties.
Nasıl? Neden? Psikolojik bir yanı olduğu kesin. Sahip olma isteği. Özellikle eşsiz (her bir kedinin ayrı bir DNA'sı var eşi benzeri yok) ve sınırlı sayıda (özellikle ilk yaratılanlardan başka yaratılamayacak olması) olan bir nesneye sahip olma isteği. Üzerine bunu yatırım gibi kullanabilme ve potansiyel para kazanma imkânını koyun. Alın size talep. Bu saydığımız özelliklerin temeli de bir kere işlendi mi değiştirilemeyecek olan Blockchain teknolojisinin insanlarda yarattığı güven.

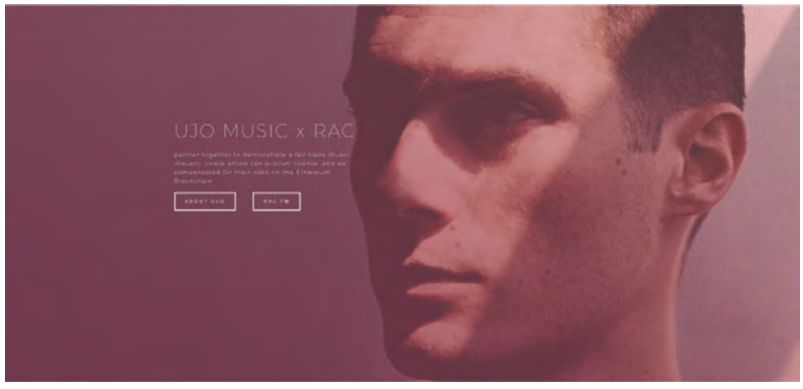


Ünlü CryptoKitty'lerden Twitch

[58]https://www.nytimes.com/2017/12/28/style/cryptokitties-want-a-blockchain-snuggle.html

CD bitti, yaşasın Spotify... Ya da?

2017 yılının Temmuz ayında RAC adıyla dans müziği üreten André Anjos, son albümü EGO'yu bilinen dijital kanallar yanında kendi web sitesinden Ether kripto parası karşılığında da dinleyicilere sundu[59]. Bunu yaparken de Ujo Platormu[60]'nu kullandı.



Biliyorsunuz, müzik dünyası CD'lerden, "streaming" servislerine hızlı bir geçiş yaptı—arada pek çok plakçı/CD satan büyük mağazalar zayi oldu. Artık kimse bir yere gidip CD almıyor, Apple Music ya da Sportify üzerinden istediğimiz müziği istediğimiz kadar dinliyoruz. Kullanıcı için büyük rahatlık. Peki sanatçılar için? Onlar biraz sıkıntılı bu durumdan dolayı. Zira, dinlendikçe para kazanıyorlar ancak bu streaming firmaları tek bir dağıtıcı olarak %30'lara varan ciddi komisyonlar alıyorlar oluşan gelirden. Adeta kartel olmuşlar! Sanatçıların çok söz hakkı yok.

Buna karşı çıkan ve bağımsız sanatçıları koruyan platformlar yok mu? Var tabii. Örneğin Bandcamp[61], müzisyenlerin direkt olarak dinleyiciler ile bir araya gelmesini sağlıyor.

Binlerce müzisyen ve 3.000'den fazla bağımsız müzik şirketini bir araya getiren Bandcamp, 2007 yılından bu yana 287 Milyon ABD Doları bir tutarı müzisyenlere ödemiş. Karşılığında ne almış? %15–20 tutarında bir komisyon. Yukarıda Apple Music'in aldığı oranlara bakınca ciddi bir düşüş oldu bile. Harika. Ama yeterli mi?

Peki o zaman ilk bahsettiğimiz Ujo Music'e dönelim. Ne farkı var? Büyük bir yenilik mi? Tam olarak sayılmaz. Ama iki tane ilerleme saymak mümkün.

Birincisi bahsettiğimiz komisyonlar ciddi olarak düşüyor. İkincisi ise lisans ve dağıtım sistemi içinde yenilikler var. Ujo "global, açık, merkezi olmayan, kimseye ait değil ama aynı anda herkesin sahip olduğu" bir lisans sistemine dayanıyor. Oldukça süslü sözler, peki tam olarak ne demek? Kısacası, sanatçıların a) ürünlerine tamamen sahip oldukları b) ürünlerinin dağıtım politikasını istedikleri biçimde belirledikleri bir sistem. Bu iki noktayı biraz daha açarsak:

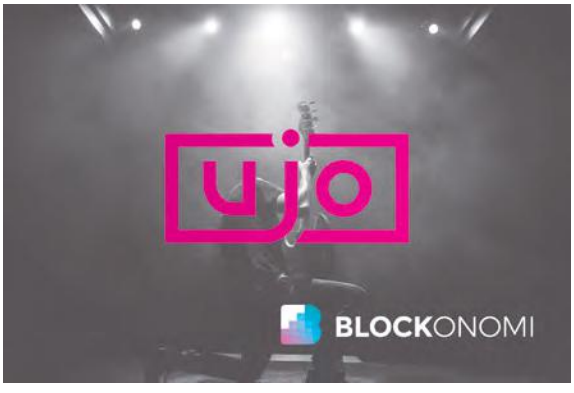


• Bir müzisyen olarak, müziğimi platform bazlı olarak bağlamak yerine platform bağımsız olarak istediğim yere taşıyabileceğim-ne de olsa sahipliği bende, nasıl kullanacağımı da ben belirlerim.
• Özellikle ticari alanda şarkılarımı kullanmak isteyen start-up ya da uygulamaların bu eserleri sanatçı olarak ancak benim belirlediğim lisans hakkı ve dağıtım politikaları çerçevesinde kullanabildikleri bir sistem. Parçayı direkt kullanmanın yanında örneğin bir YouTube fenomeninin müziğimi remix yaparak kendine ait YouTube videosunda kullanma koşullarına da ben karar vereceğim. Eğer müziğim tek bir platforma bağlı olursa bunu yapabilmek uzun zahmetli bir iş. Hem müzisyen olarak benim için hem de müziğimi kullanmak isteyenler için… Bunun yerine, her tür platformda geçen otomatikleştirilmiş bir lisans sistemi olsa aradaki bürokrasi de azalacak.

59http://musically.com/2017/08/04/ujo-music-blockchain-uphill-battle-existing-companies/
60https://ujomusic.com/
61https://bandcamp.com/



Tabii bu konuda şüpheci davranıp müzik alanında yukarıdaki gelişmelerin reklam amaçlı olduğunu, UjoMusic'in "doğru soruları sorduğunu ama henüz cevapları bulamadığını[62]" düşünenler de var.

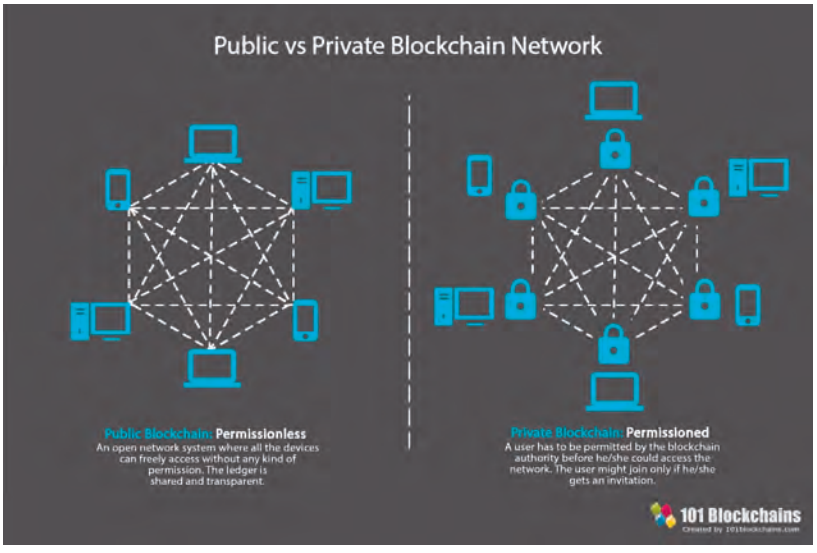


[62]http://www.hypebot.com/hypebot/2017/11/ujo-attempts-music-on-the-blockchain-a-second-time-with-ego-by-rac.html

Sonuç

Başlangıçta da belirttiğimiz gibi Blockchain yeni bir teknoloji. Bu teknolojinin her derde deva olacağını düşünmek yanlış. Ancak bir taraftan da biraz daha çerçevenin dışında düşünmekte fayda var. Sanat alanında gördüğümüz hem dijital sahiplik hem aracıların azalması (dolayısıyla komisyon ve bürokrasinin minimuma indirilmesi), ağırlıklı olarak sanatçılara ama bunun yanında sanata ulaşmak isteyen (ticari ya da kişisel olarak) kitlelere fayda sağlayacak pek çok yeniliğe gebe. Henüz Blockchain'in temellerinin atıldığı şu günlerde son kullanıcı olarak bu teknolojilere erişim için bir süre daha beklememiz gerekecek. Ama işin potansiyeli ve gerçekleştiğindeki faydalarına baktığımızda heyecanlı ve sonunda değecek bir bekleyiş olacağı kesin gibi. Beklerken eğlenmek isterseniz bir kedicik de siz sahiplenebilirsiniz! :)

BLOCKCHAIN her derde *deva mı?*



Elbette değil. Önce bir faydalarına tekrar göz atalım ve değişik türlerini gözden geçirelim sonra da neden bu alandaki girişimlerin çoğu başarısız olacak ona bakalım. Bir sonraki bölümde ise hangi alanlarda başarı şansı daha yüksek ona değineceğiz.

Geçtiğimiz bölümde değişik sektörlerden verdiğimiz örneklere bakıp Blockchain dünyanın tüm dertlerine deva olacakmış gibi bir izlenim çıkmaması için madalyonun diğer tarafına da bir göz atmakta fayda var. Gerçekten Blockchain tüm sorunlarımızı çözebilecek mi?

Blockchain'in faydalarını özetleyelim mi?

Değişik sektörlerde Blockchain ile ilgili uygulamalara baktığımızda genel olarak ağırlık kazanan birkaç ortak tema görmek mümkün. Bunları madde madde bir araya getirirsek:

- Merkezi otoritede yaşanan herhangi bir sıkıntının tüm sistemi etkilemesini (ya da durdurmasını) önlemek
- Aracıları ortadan kaldırarak yüksek komisyonları minimize etmek
- Bürokrasinin getirdiği zaman ve emek kaybını minimuma indirmek
- Geriye yönelik olarak doğru, tutarlı, değiştirilemez kayıt bilgisi oluşturmak
- Bireyler için dijital alanda tüm haklarını ellerinde tuttukları dijital kimlikler oluşturmak.

Blockchain bir tane mi? Elle tutulur mu?

Güzel bir soru. Blockchain bir konsept. Bunun farklı farklı uygulamaları var. Her Blockchain de bir değil. Blockchain aslına bakarsanız, birbiri ile uzaktan bağlı makinelerin, belli işlemleri ortak bir mutabakat yoluyla değiştirilemez biçimde tuttukları bir sistem. (Basit olsun diye sistem diyoruz, başka yerlerde protokol diye görürseniz şaşırmayın, aynı anlamda kullanılıyor). Ama bunun da farklı türleri var. Genel hatları ile ikiye ayrılıyorlar: Genel ve Özel Blockchain'ler (Public ve Private). Önce nedir bunlar, farkları neler ona bir bakalım:



Genel (Açık) ve Özel (Kapalı) Blockchain: Farkları ne?

Genel Blockchain'ler, her tür makinenin izin almadan istediği gibi bağlandığı ve bir parçası olabildiği sistemler. Örneğin, şimdiye kadar konuştuğumuz Bitcoin, Ethereum gibi Blockchain sistemleri bu şekilde. Yani, yarın bir bilgisayar alıp, bir yazılım yükleyip siz de sisteme bağlanabilir ve yapılan işlemleri görüp işlem yapabilirsiniz.

Özel Blockchain ise adından da anlaşıldığı gibi, bir otorite tarafından içeri girişiniz ve içeride işlem yapışınız izne bağlı olan sistemler.

Her iki tür ile ilgili herkesin ayrı bir fikri ve düşüncesi var. Bitcoin taraftarlarına sorarsanız, Özel Blockchain'leri sistemden bile saymazlar -kendilerince haklılar. Zira Bitcoin'in derdi, "merkezi bir otoritenin getirdiği güven ihtiyacını" minimuma indirmek, hatta yok etmek. Halbuki, Özel Blockchain'lerde bu felsefeye taban tabana zıt olacak şekilde, sizin sisteme girişinize ve hareket etmenize izin veren ve gerekirse bu izni yok eden bir otorite var!.

Ama bir taraftan da özellikle kripto para dışındaki girişimlerde her zaman topluma açık sistemler kurmak girişim için en verimli yol olmayabilir. Öncelikle, açıklık demek, gizliliğin olmaması demek. Bahsetmiştik, örneğin Bitcoin'de yapılan işlemleri kimin yaptığı şifreli olarak gizlenmiş durumda ancak bütün işlemler rakamlar ve işlemi yapan partilere ait adresler şeffaf bir şekilde herkes tarafından tutuluyor. Bu kadar açıklık, özellikle ticari iş yapan kurumlar için sakınca yaratabiliyor.

Bunun yanında izne bağlı olmayan açık sistemler, bilginin kayıt edilmesi sırasında kimi partilere fayda sağlayabilecek ancak sisteme yük getirecek ve bilgi kirliliğine yol açabilecek işlemlerin (örneğin spam bildirimler) oluşmasına yapıları gereği engel olamıyorlar.



Birkaç örnek verelim mi?

Elbette. Genel (ya da açık) Blockchain'lere örnekler çok. Hepimizin duyduğu Bitcoin ve Ethereum en bilinen Blockchain örnekleri. Tüm yazılımları halka açık, bütün makinelerin istedikleri gibi bağlanıp parçası olup, istedikleri gibi çıktıkları açık platformlar.

Özel Blockhain'ler ise genelde ticari kurumlar tarafından kuruluyor ve o nedenle ismen çok da bilinmiyorlar. Örneğin IBM'in liderlik ettiği (her ne kadar IBM'in sadece katılımcısı olduğu ve liderliğini Linux Foundation'ın yaptığı söylense de) Hyperledger Fabric[63]. Ya da finansal alanda pek çok finansal kuruluşun üzerine gelişim yaptırdığı Corda Blockchain'i yaratan r3[64]

[63] https://www.ibm.com/blockchain/hyperledger
[64] https://www.r3.com/

Peki girişimciler bu konuda ne kadar tecrübeli?



Hemen hemen her sektörde Blockchain bazlı sistemleri kullanarak sektörü kökünden sarsmak isteyen pek çok yeni girişim var. Ancak, bu girişimlerin birçoğu maalesef hüsranla sonuçlanacak. Neden? Birkaç nedeni var, onları da sıralayalım:

• Henüz Blockchain teknolojisinin altyapısı tam olgunlaşmadı, özellikle genel (public) Blockchain'lerin altyapılarının gelişimi oldukça yavaş bir şekilde ilerliyor. 2000'li yılların başında patlayan Startup balonunda da benzeri olmuştu. O zaman pek çok fikir vizyon olarak iyi ama zamanın çok ötesinde olduğu için başarılı olamadı (şimdi o fikirlerin bir kısmı yeniden hayata geçiriliyor).
• Sırf piyasada bu alana büyük ilgi var diye iş yapmaya çalışan kişiler var—ki bunların bir kısmı PR yapmaya çalışan ve altı boş girişimler. Örnek mi? Sierra Leone'de seçimleri Blockchain üzerinden yaptığını iddia eden[65] Agora ve bunu şiddetle reddeden[66] hükümet.
• "Her ağacın meyvesi olmaz" derler. Her sektörün farklı farklı dinamikleri var. Dolayısıyla Blockchain de her alanda faydalı olacak diye düşünmek doğru değil. Bu nedenle Blockchain' ihtiyaç duyulmayan, böyle bir potansiyelin bulunmadığı sektörlere giren girişimcilerin de hüsrana uğraması kaçınılmaz.

[65] https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/
[66] https://techcrunch.com/2018/03/19/sierra-leone-government-denies-the-role-of-blockchain-in-its-recent-election/

Blockchain bulunduğum sektöre yarar mı?

Blockchain her sektöre uygun değil. Neden? Mevcut sistemlere göre pek çok sıkıntısı var çünkü. Fayda sağlayacağı sektörler de var ama, avantajlarının dezavantajlara üstün geldiği. Nelermiş bunlar bir bakalım.

Geçtiğimiz bölümde, Blockchain'in iki türü olan Özel ve Genel Blockchain kavramından bahsetmiş ve neden bu Blockchain bazlı çoğu projenin geleceğinin parlak olmayacağını göz atmıştık. Şimdi de neden Blockchain bazlı teknolojiler çalışması zor yapılar, başarılı olması için gerekli kriterler neler onlara bakalım dilerseniz.

Her güzelin bir kusuru olur, peki Blockchain'in kusurları ne(ler)?

Bilmemiz gereken en önemli nokta, Blockchain'in aslında çok büyük bir database (veritabanı) olduğu. Bu ne demek? Herhangi bir şekilde sisteme giren bir bilginin, tek bir merkezde tutulması yerine binlerce makinede aynı şekilde tutulması demek. Yeni bir bilgi geldiğinde de yine aynı şekilde bilginin binlerce makineye dağılarak o eski bilginin üzerine eklenmesi demek. Bu sistemin aslında pek çok dezavantajı var. Kısaca bakalım:

• Bilginin binlerce makineye dağılması ve orada tutulması demek öncelikle oldukça yavaş ve hantal bir yapınız var anlamına geliyor. Verilen geliyor, tüm makinelere dağılıyor, makineler bunu kaydediyor, sonra belli aralıklar ile bunların tutarlı olup olmadığını kontrol ediyor. Zaman isteyen bir süreç.
• Aynı zamanda enerji bakımından maliyetli. Merkezi bir sistemde olsa tek bir makine için harcayacağınız elektrik masrafını düşünün, bir de binlerce makinenin aynı bilgiyi tutmasından dolayı gerekecek enerjiyi…

• Bir yandan da oldukça geniş bir bilgi depolama alanına ihtiyacınız var. Bilginin toplam alanını bir makinede tuttuğunuzda gerekli olan depolama alanını düşünün, bir de aynı bilginin binlerce makinada tutulduğunda gerekli olan alanı…
• Binlerce makinayı içeren bir sistemi düşündüğünüzde sistemin yavaş gelişeceğini de kabul etmeniz lazım. Öncelikle sistemi kurarken çok ince elemeli ve sık dokumalısınız. Merkezi bir veritabanı kurarken gerekli olan önlemleri zaten almanız lazım. Ama üzerine bir de binlerce makinenin bağlanacağı bir merkezi olmayan sistemin getireceği sıkıntılara da göğüs gerecek bir sistem olmalı bu.
• Keza, sistemi işletirken sonrasında yaptığınız yenilikler de sistem üzerindeki binlerce makina tarafından kabul edilmeli ve içselleştirilmeli. Sistem doğası gereği adem-i merkezi bir yapı olduğu için hiçbir makineye zorla bir dayatmada bulunamazsınız. Gönüllü olmalı bu iş. Dolayısıyla, yapacağınız her tür değişiklik geriye dönük olarak eski versiyonlarda da kullanılabilmeli. Bu da her yaptığınız değişikliğin tüm sistem tarafından toplu kabulünü oldukça yavaşlatan bir durum.



• Her bir Blockhain sistemi okyanus üzerinde yüzen birer ada gibi. Farklı teknoloji ve altyapılar kullanıyorlar. Birbirleri ile bir iletişimleri yok. Bir Blockchain üzerinde yapılan bir işlemin bir başka Blockhain üzerinde hükmü yok. Bir Blokchain'e dahil kullanıcı ya da madencilerin ellerindeki kripto paraları başka bir Blockchain'de kullanmaları (eğer bir kripto para borsasına gidip al-sat yapmıyorlar ise) mümkün değil.

İşte bu nedenle Blockchain ancak gerekli olduğunda başvurulması gereken bir alan. O nedenle Blockchain üzerine yatırım yapmadan önce iyi düşünmekte fayda var, yoksa…

Neden ve ne zaman Blockchain'e ihtiyaç duyulur?

Hakikaten bir ihtiyaç olmalı Blockchain'e. Geçen bölümden hatırlarsak, neydi bu ihtiyaçlar?

Merkezi otoriteye ya da aracıya güvensizlik

Bilgileri tutacak bir merkezi otoriteye karşı güven bunalımı. Merkezi bir otorite, Nick Szabo'nun da dediği bir "güvenlik açığıdır". Konu gerçekten böyle bir güvenlik açığının olması. Merkezi otoritede yaşanan sıkıntı biz kullanıcıları ne kadar etkiler? Yukarıda saydığımız merkezi olmayan sistemin ağır ve hantal yapısı ile uğraşmaya değer mi? Bunları tartmak lazım.

Bu nedenle belki de Blockchain'in şu ana kadar en başarılı olduğu alan para konusu oldu. Zira, daha önce de bahsettiğimiz gibi ABD'de 2008 yılında yaşanan kriz sonrası, daha önceki yıllarda halkın üzerinden korkunç karlar elde eden ve bu korkunç karlarını daha da büyütmek amacıyla gittikçe daha çok risk alan bankalar, sonrasında "aman kriz daha da büyümesin" açıklaması ile kurtarıldı. Bu kurtarmada Amerikan vatandaşlarının "vergilerinden gelen para" kullanıldı. Üstelik bu kriz nedeniyle enflasyon yaşandı. Üstelik hükümet halka sormadan milyarlarca dolar karşılıksız para bastı. Bunu da "likidite" diyerek halka yutturmaya çalıştı (yeri gelmişken eğer seyretmediyseniz "Too Big To Fail " filmini hararetle tavsiye ederim). Dolayısıyla, bireyler açısından merkezi otoritenin yetkinlikleri ya da yaptıklarının her zaman kendi çıkarlarına olmadığını düşünmelerine sebep olan bu güven bunalımı üzerine Bitcoin'in ortaya çıkması çok da tesadüfi değil.

67https://www.imdb.com/title/tt1742683/

Aracının maliyeti

Bireyler arasındaki işlemlere aracılık ederek bundan komisyon alan her türlü aracı, bu işi kâr için yaptığı noktada işlemin tarafı olan partiler tarafından aracılık için ödenen ücretler yüksek görülecek. Böyle düşünenlerin haklı olduğu alanlar da yok değil. Örneğin, Uber'in sadece bir software olması ve araçlar ile insanlar arasında optimizasyon yapmasına rağmen ödenen ücretin %30'lara varan bir kısmını cebine indiriyor olması tepki çekiyor. Keza, bankacılık sistemine dahil olmayan insanların bir ülkeden diğerine para gönderirken onlar hatta yüzlerce dolar komisyon vermeleri de öyle. İşte dağınık sistemler, ortadaki güven sağladığını iddia ederek (ya da sağlayarak) yüksek miktarda masraf "çakan" aracılara karşı faydalı hatta gerekli.



Aracının hantal yapısı

Evet, dağıtık yapılar hantal olabilirler. Ama gerçekten özellikle geçmişten gelen gerek eski teknoloji gerekse çeşitli bürokratik çıkarlar nedeniyle mevcut sistemi kontrol eden ve yönetenlerin yarattığı bürokratik yapı yanında bu bahsettiğimiz yavaşlığın esamesi okunmaz. Örnek mi? Maersk'e göre, bir soğutucunun Avrupa'dan Afrika'ya ulaşımında 30'dan fazla kişi ya da organizasyon sürece dahil oluyor ve bu aktörlerin birbirleriyle 200'den fazla kez iletişim halinde olmaları gerekiyor. Neden? Bürokrasi, değişik ülkelerdeki kurumların birbirine güvenmemesi, politik ajandalar vb.

Aracılardan bağımsızlık isteği

Merkezi sistemlerin, kişileri bağlamak, elinde tutmak, kişinin üzerinden izinli ya da izinsiz fayda sağlamaya çalışmaları da bireylerde bu tip otoritelerden uzak kalmaya çalışmak, bağımsız olmak dürtüsünü artırdı. Daha önce bahsettiğimiz, Facebook'un bilgilerimizi bizden habersiz (ya da uzun uzun okumadığımız ve evet tuşuna basıp geçtiğimiz kullanım sözleşmeleri aracılığıyla) kurumlara satması gibi. İnsanlar artık, özellikle dijital dünyada kendilerine ait bilgileri kendi kimlikleri gibi ellerinde tutmayı, istedikleri bilgiyi istedikleri yere vermeyi ve istedikleri noktada da o bilgiyi verdikleri kurumdan geri almayı istiyorlar. Merkezi yapılarda ya bu olanak yok, ya da varsa da gerçekten söz verdiklerini yapacaklarına dair bir garanti yok. Dağıtık yapılar bu anlamda bireylere özgürlük getiriyor. Tabii bir de dağıtık yapıların herhangi bir merkezleri olmamasının getirdiği, kanuni olarak hangi otoritenin altında oldukları konusundaki belirsizlik de kimi bu tip otoriter yapıların altında olmak istemeyen kişileri bu yapılara doğru çeken bir başka etken.

Peki neden bu kadar şişiriliyor Blockchain balonu?

Dediğimiz gibi hemen hemen her sektörde gerek yeni girişimler gerekse sistemin içindeki mevcut oyuncular için Blockchain sektörü derinden sarsacak bir olguymuş gibi parlatılıyor. Neden?

Öncelikle bilgi eksikliği diyebiliriz. Daha önce de bahsettiğimiz gibi, Blockchain anlaması ve algılaması oldukça zor bir kavram. Özünde "merkezi olmayan bir veritabanı" olsa da şifreleme, bağımsız makineler, aracıya olan güveni ortadan kaldırma gibi terimler alışık olmadığımız, büyürken bize öğretilen doğrulara kimi zaman taban tabana zıt kavramlar.



Hem anlamakta zorluk çekiyoruz hem de "startup patlamasında" yaşadığımız gibi uzak kalmak ya da etkilenmek istemiyoruz. Büyük kurumların da insanlardan oluştuğunu unutmamamız gerek. Dolayısıyla kurumlar da bu rüzgârdan etkileniyorlar.

Bunun yanında Blockchain'i kullanmaktan çok aslında dışarıda kalmamaya çalışıyor kimi kurumlar. Bir nevi test ortamında deniyorlar kullanışlı olup olmadığını. Havuz kenarına gelip suyun nasıl olduğunu ayağınızın ucuyla dokumak gibi düşünebilirsiniz bunu. Ancak kullandıkları Blockchain teknolojilerin hizmetini verenler bunu piyasada ballandıra ballandıra anlatarak küçük bir olayı bambaşka boyutlarda sunuyorlar. Örnek olarak, şahsen, Ripple Network içinde yer aldığını açıklayan onlarca prestijli bankanın sadece ne olduğunu anlayabilmek için bu ortamda olduklarını düşünüyorum.

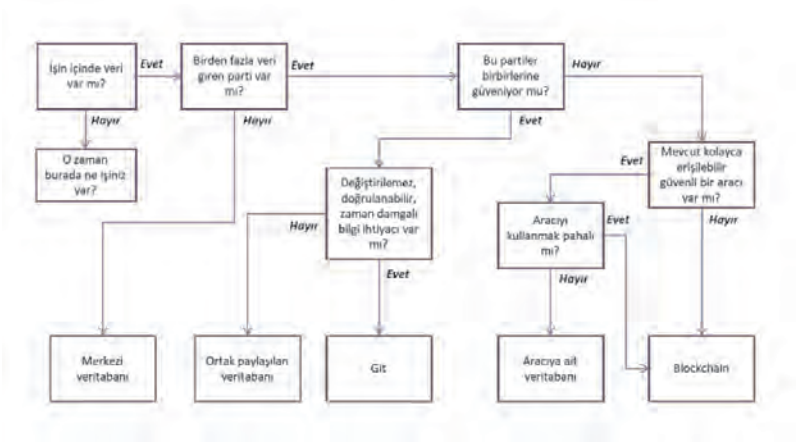
İkincisi, özellikle Bilgi Sistemleri çok önce kurulmuş ve doğası gereği yenilenmeye açık olmayan sektörlerde yeni sistem kurmanın imkânsızlığı ya da yüksek maliyeti, Blockchain sistemlerine olan ilgiyi artıyor. Örnek mi? Geçen bölümlerde bahsettiğimiz havacılık sektörü. Havacılık için böyle bir ihtiyaç var gibi görünüyor ancak başka pek çok sektörde danışman firmalar tarafından da böyle bir ihtiyaç var havası yaratılıyor maalesef.

Bir başka neden de, kurumların kendilerini teknoloji lideri olarak göstermek için Blockchain'den bahsetmeleri. Bir nevi "biz çok akıllıyız, bu teknolojileri anlıyoruz, kullanmaya başlıyoruz" diyerek 'hava atmaları'…

Peki Blockhain sorunlara karşı panzehir geliştirebiliyor mu?

İki bölüm önce Blockchain ile ilgili problemlerden bahsettik: Hantal olması, çok enerji harcaması, geniş bilgi depolama ihtiyacı, güvenlik açıkları olma ihtimali gibi… Peki Blockchain üzerine çalışanlar bu sorunlara bakıp "kader işte yapacak bir şey yok" mu diyorlar? Elbette hayır. Hızlıca bir bakalım arı kovanı gibi çalışan geliştiricilerin yaptıklarına:

• Hantal yapı: Blockchain içinde eğer hantal yapıyı hızlandırmak istiyorsanız, özel Blockchain yapıları kurmak en efektif yöntem. Sisteme giriş çıkışların denetlendiği ya da izne tabi olduğu, yapılan geliştirmelerin makineler tarafından kısmen "zorunlu" tutulduğu yapılar. Halka açık Blockchain yapıları, özel kurulmuş benzerlerini güvenlik ve şeffaflık anlamında zayıf bulduklarını da belirtmek lazım. Ancak her iş ya da her konuda illa tamamıyla şeffaf bir yapı kurmak o kadar da zorunlu değil. Tamam eğer konu bir kripto para ise yani bir değer atfedecek iseniz o zaman güvenlik ve şeffaflıktan bıktıracak kadar hassas olabilirsiniz ama diğer kimi sektörlerde belki o kadar uç noktalara gitmeyecek ama çok daha pratik ve esnek çözümler ile ilerleyebilirsiniz.
• Enerji harcama: Özellikle Bitcoin Blockchain mimarisini kullanan yapılar için kullanılan sistemin çok enerji harcadığı ile ilgili eleştiriler konusunda Bitcoin geliştiricilerinin bir hamle yapmasını beklemek hayal. Zira onlar bu enerji harcamanın sistemin kendi güvenliğini korumak (dış ataklara karşı) için elzem olduğunu düşünüyorlar. Ancak diğer başka Blockchain yapıları gerek Proof-of-Stake gerekse başka tür çalışma kuralları kurarak enerji sorununu çoktan hallettiler bile. Bu konuda detayları şu bölümde bulabilirsiniz.



• Geniş depolama ihtiyacı: Yine özellikle Bitcoin özelinde en çok yapılan eleştirilerden biri işlemlerin tamamının şeffaf bir şekilde sistemde ve her makinede tutulması nedeniyle çok ciddi bir depolama ihtiyacının olması. Yine Bitcoin'de değil ama alternatif yapılarda bunun da çözümü bulunmuş durumda. Örneğin bütün işlemlerin detaylarını tutmak yerine sadece ana başlıklarını tutmak, bilgilerin sıkıştırmak için gelişmiş öğütme mekanizmalarından yararlanmak bunların birkaçı. Bunun yanında gerekli depolama ihtiyacını her bir makinede tutmak yerine şifreleme sistemleri kullanarak bir bilgiyi birkaç makineye paylaştırmak da benzer çözümlerden biri.
• Uyumluluk ve sürdürülebilirlik: Birbirinden farklı yapıdaki Blockchain sistemlerinin birbirleri ile konuşabilmeleri için yapılan pek çok çalışma var. Bundan birkaç yıl önce çalışmaya başlayan Polkadot[68] ve 2018 yılı başlarında sansasyon yaratan Cosmos[69] bu tip çalışmalardan sadece birkaçı. Belki hiçbir zaman tam bir entegrasyon olmasa da, yeni teknolojilerin birbirleri ile hiçbir iletişimi olmayan geçmişteki silo yapılara (Kaç kredi kartı taşıyorsunuz örneğin? Gerçekten gerek var mı bu kadar karta?) oranla çok daha ilişkili olacakları kesin…

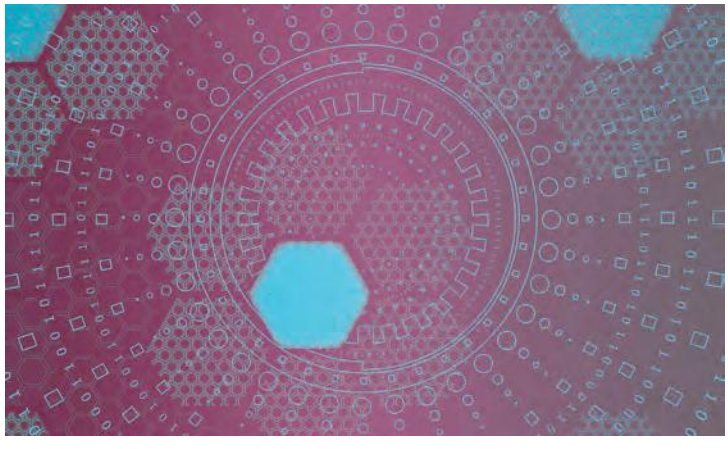
68 https://polkadot.network/
69https://cosmos.network/

Blockchain hangi sektörlerde başarılı olur? Turnusol kağıdı var mı?

Buraya kadar yazdıklarımızın ötesinde daha net olarak içinde bulunduğunuz sektör için Blockchain gerekli mi sorusuna yanıt için aşağıdaki şemayı kullanabilirsiniz (Kaynak: Thomas Ferry-To Blockchain or Not to Blockchain[70] adlı Medium makalesi)

Sonuç

Hep söylediğimizi bir kez daha tekrarlayalım: Blockchain yeni gelişmekte olan bir teknoloji. Güvene dayalı aracıların verimsizleştirdiği her alanda aracıları yıkacak güce ve potansiyele sahip. Şimdi, bu yıl ya da önümüzdeki yıl etkilerini henüz görmeyeceğiz. Ama nasıl internet hiç yokken hayatımıza girdi ve vazgeçilmezimiz oldu Blockchain bazlı teknolojiler de önümüzdeki beş-on yıl aralığında hayatımızı benzer şekilde değiştirecekler. Umuyoruz olumlu yönde olacak bu değişiklikler.



70https://medium.com/causys/to-blockchain-or-not-to-blockchain-aed05bf08150



Değişen **Girişimcilik** *ve* YATIRIMCILIK

Bildiğimiz klasik anlamdaki ‘Girişimcilik ve Yatırımcılık’ yeni teknolojiler ile değişmeye başlıyor. Nasıl mı?

Geçtiğimiz bölümlerde, merkezi olmayan yapılara bakmış ve neden önemli olduklarını anlatmaya çalışmıştık. Özetle, merkezi yapılar, tek bir merkezden yönetildikleri için güvenlik açısından sakıncalar yaşarlar. Tek merkezli yapılar, iç ve dış tehditler için kolayca hedef tahtası haline gelirler. Oysa ki merkezi olmayan sistemler ele avuca sığmayan cıva gibiler, nereye saldıracaksınız ki? İşte bu özellikleri merkezi olmayan yapıları daha sağlam hale getiriyor.

Tabii iki yapı arasındaki farklar bununla sınırlı değil. Bu yeni yapılar kendi ekosistemlerindeki tüm oyuncuların davranış biçimlerini de değiştiriyorlar. Örneğin girişimciler ve yatırımcılar… Merkezi olmayan yapı ile kurulan sistemlerin ortaya çıkışıyla aslında girişim ve yatırım anlamında büyük bir değişimden geçiyoruz. Bildiğimiz klasik anlamdaki bu terimler kökten değişiyorlar. Nasıl mı? Anlatalım.

Klasik anlamda ‘Girişimcilik ve Yatırımcılık’ nasıl idi?

Efendim, normalde girişimcilik (kâr için yapılanı), kaba hatlarıyla şu şekilde çalışır: Bir grup kafadar bir araya gelirler (ya da bir kişi fark etmez). Bir fikir ortaya atarlar. Sonra bu fikir üzerinde kafa yormaya başlarlar. Fikri geliştirir, bu fikir üzerinden bir katma değer yaratmaya başlarlar.



Bir noktada daha fazla katma değer yaratabilmek için dışarıdan birilerinin katkılarına ihtiyaç duyarlar. Örneğin, ekibi büyütmek (ki daha fazla iş ortaya çıkarsınlar), şehir şehir gezmek (ki yeni müşteri bulsunlar), bir ofis kiralamak (ki ekibi bir arada tutsunlar ve verimli çalışsınlar) ve bu sırada kendilerinin ve ekibin karnını doyursunlar. Fikirden elde ettikleri gelir henüz bu masrafları karşılamaya yetmediği durumda ve masrafları bir süreliğine karşılamak için yatırımcılardan finansman sağlamaya çalışırlar (eğer bankadan borç almak için gerekli olacak mal varlığına sahip değillerse).

Yatırımcılar önce girişimcilerin o ana kadar yaptıklarını inceler, sonra ne planladıklarına bakar ve ileride vereceği bu paraya hatırı sayılır bir karşılık alabileceğine inanır ise yatırımcılara para verirler. Karşılığında da kurdukları şirketin bir kısım hissesini alırlar.

Buraya kadar anlattığımız her şeyin kapalı bir sistem olduğunu anlayalım öncelikle. Fikir, girişimcilerin kafasında. Girişimciler bu fikri hayata geçirmek için bir şirket kuruyor ve bu şirketin tamamına sahip oluyorlar önce. Sonra yatırımcılar ile paylaşıyorlar. Fikir ve devamında çalıştıklarında oluşturdukları entelektüel girişimleri olabildiğince patent ve benzeri mekanizmalar ile koruyorlar ki başkaları taklit edemesin.

Burada tüm bu katma değerin merkezinde tek bir yapı var-girişimciler, şirketleri ve yatırımcıları. Şirket belli bir büyüklüğe ulaşınca da yatırımlarını halka arz ediyorlar (İngilizcesi IPO-Initial Public Offering).

Bu, bugün gördüğümüz birçok girişimde, özellikle bizim konumuz olan Web 2.0 dediğimiz 90’ların başından itibaren internette kurulan merkeziyetçi tüm şirketlerde bu şekilde oldu. Facebook Mark Zuckerberg’in fikri olarak çıktı ve Mark hala şirketin tüm karar mekanizmalarından tek başına karar hakkına sahip. Google Sergey Brin ve Larry Page, Amazon Jeff Bezos tarafından kuruldu ve hala onlar tarafından yönetiliyor.

Yeni anlamıyla ‘Girişimcilik ve Yatırımcılık’ nasıl yapılıyor peki?

Ancak Web 3.0 ile gelen yeni merkezi olmayan oluşumlarda bu yapı tamamen değişiyor! Zira burada kurulan sistem bir şirket değil, bir ekosistem… ve bu ekosistemde sadece girişimciler ve yatırımcılar yok. Başka pek çok bileşen var. Girişimciler tabii var ama onlar olayı kurgulayanlar; sonrasında organizma kendi kendine büyüyor. Ne demek bu? Biraz daha açalım.



Hatırlarsanız ilk bölümde, internetin gelişim ve yaygınlaşması ile birlikte ortaya çıkan şirketlerin (Facebook, Google, Amazon ve Apple başta olmak üzere) daha sonra ağırlıklı kâr baskısı sebebiyle monopol haline gelip tüm ekosisteme (kullanıcılar, girişimciler, reklamverenler gibi) nasıl zarar verdiklerinden bahsetmiştik.



2000'li yıllarda çıkan yeni akımın ise işte bu merkeziyetçilik dalgasına bir tepki olarak doğduğundan bahsetmiştik. Dolayısıyla bu akımdan ortaya çıkan yeni yapılar Web 3.0 dediğimiz bu akımın temel felsefesini de benimsemiş olarak ortaya çıktılar. İşte o felsefenin temel noktalarından biri tekellerin kırılması; bilginin, kontrolün kısaca gücün tek bir elde toplanmaması.

Bunun için de öncelikle daha önce bahsettiğimiz gibi, sistemde tek bir merkezden ziyade kontrolün her tarafa dağıldığı bir yapı getiriyorlar ve bunu başarmak için de şifreli bir mekanizma ile kişiye duyulacak güvene olan ihtiyacı ortadan kaldırıyorlar.

Klasik anlamda girişimlerde, bir girişim başarılı olduğunda ortaya çıkan katma değerinin tamamına (ki bu şirket değeri ile ölçülebilir) girişimci ve yatırımcı sahip oluyordu. Bir de belki verilen hisse opsiyonları sayesinde bir kısım çalışan, o kadar. Şimdi ise yukarıda bahsettiğimiz felsefeye paralel olarak, fikrin gelişmesine katkıda bulunan dış geliştiriciler, sistemin çalışmasına yardımcı olan bağımsız dış kaynaklar, hatta son kullanıcılar da yaratılan bu katma değerden pay alıyorlar. Yani gücün yanında getirinin paylaşımı da artık daha demokratik oluyor.

Girişimler yeni teknolojiler aracılığıyla nasıl demokratikleşiyor?

Bu bölümde şu ana yazdıklarımızı hızlıca özetlersek, klasik anlamda girişimlerde, bir girişim başarılı olduğunda ortaya çıkan katma değerin tamamına (genelde şirket değeri ile kendini gösterir) girişimci, yatırımcı ve kısıtlı olarak (hisse opsiyonları ile) çalışanlar sahip oluyordu. Yeni teknolojilerde ortaya çıkan yapılarda, merkeziyetçilikten uzaklaşma felsefesine paralel olarak, fikrin gelişmesine katkıda bulunan dış geliştiriciler, sistemin çalışmasına yardımcı olan bağımsız dış kaynaklar ve hatta verilen hizmetin kullanıcıları da artık bu katma değerden pay alır hale geliyorlar. Yani gücün yanında getirinin paylaşımı da artık daha demokratik oluyor.

Şimdi dilerseniz bunun nasıl başarıldığına bakalım.

Girişimciler ve yatırımcılar dışında masada başkaları da var mı?

90'lar ve 2000'lerin başında ortaya çıkan internet bazlı girişimler (Facebook, Google, Amazon, Apple gibi) ellerindeki büyük güç ile birlikte karlarını artırabilmek için diğer paydaşları zarara sokacak şekilde monopolleşmeye gittiler. 2010'ların başında ise işte bu merkezi yapılara tepki olarak merkezi olmayan yapılar ve sistemler doğdu. Bu sistemlerde girişimci artık bütün gücü elinde tutmuyor, daha demokratik bir yapı var. Artık girişimcinin sahip olduğu bir yapı yok, girişimcilerin kurduğu ekosistemler var.

Ancak burada şöyle bir sorun var. Sonuçta bu sistem içindeki fikirler kendi kendilerine çıkmıyorlar. Birileri bu fikirleri çıkarmalı, üzerinde çalışmalı, yeşertip büyütmeli; yani girişimciler olmalı. Ancak, tüm gücü ve hakları (Web 2.0'da olduğu gibi) girişimcilere (ya da yatırımcılar ile birlikte düşünürsek girişimcinin kurduğu şirkete) verirseniz, gücü yine tek elde toplamış olursunuz. Sonra da kâr odaklı bu şirketler yine monopol olarak güçlerini kâr etmek için kullanmaya başlar ve aynı sarmala girersiniz. Ne yapmalı o zaman? Girişimciler yapıyı kurmalı, büyütmeli ve bunun için de yeterince teşvikleri olmalı ama yapı onlara bağlı olmamalı. İşte bunu başarmak için Web 3.0'in kullandığı önemli bir özelliği açıklamaya geldi sıra:
Açık kaynak (İngilizcesi Open Source).

Açık kaynak (Open Source) nedir? Neden önemli?

Açık kaynak tabii ki Web 3.0 ile gelmedi. Onlarca yıldır var. Bilmeyenler için kısaca bahsedelim. Açık kaynak, (programlama için kullanılsa da özünde) bilginin açık olması ve herkes ile paylaşılması esasına dayanan bir felsefe ve uygulama.

Kısaca şu anlama geliyor. Kişinin elinde olan, emek harcadığı işi tüm toplum ile paylaşması, başka kişilerin de bu yapılan işi emek harcayarak geliştirmesi ve yine toplum hizmetine sunması. Böylece emek ve sonucunda ortaya çıkan iş tüm toplum tarafından ücretsiz olarak kullanılıyor. Aklınıza şu soru gelebilir: "Deli mi bu insanlar, neden hiç para almadan böyle emek harcarlar, hiç mi işleri yok bunların?". Haklılık payı var bu düşüncenin. Kişi bu tip bir emeği gösterirken karşılığında birkaç beklentisi olabilir: Örneğin, burada yaptığı katkıyı tüm topluma göstererek aslında ne kadar maharetli biri olduğunu kanıtlamak ve bir şirkette iş kapmak için referans olarak kullanabilir bunu. Ya da böyle bir işi kullanan birinin daha sonra ihtiyacı olacak hizmetleri (örneğin yan servis, bakım vb.) kullanıcılara sağlayabilir.

Ama bütün bunlar çok küçük bir kitle için geçerli. Ağırlıklı olarak bu işi insanlar hobi olarak ve gönüllülük çerçevesinde yapıyorlar. İşte açık kaynak hareketinin ne kadar büyük olursa olsun, en büyük sorunu da bu. İnsanların gönüllülük hareketi ile yaptığı işler maalesef kâr amacı güden şirketlerin gücü karşısında rekabette zorlanıyor. Zira kâr amacı güden şirketlerin tam zamanlı çalışanları ve neredeyse sınırsız kaynakları var.





Açık kaynaklı projeler bu şirketler ile rekabet için ciddi bir yatırım alıyorlar, (ki o zaman kâr eden bir başka şirkete dönüşüyorlar) bağışlar ile ayakta durmaya çalışıyorlar, (Wikipedia gibi) şirketlerin rakiplerinden destek alıyorlar. Bu bahsettiğimiz son ikisinin sürdürülebilir olması tahmin edersiniz ki çok zor.

Açık kaynak ile para bir araya gelir mi?

İşte Web 3.0 teknolojileri "Açık Kaynak" felsefesinin sürdürülebilir olması için bu işe gönül verenleri ihtiyaçları olan para ile buluşturan bir yenilik getirdi. Artık fikirin gelişmesi bir girişimci ve kurduğu şirket etrafında değil, onun yerine bir girişimci ve girişimcinin kurduğu ekosistem (ağ, ekonomi) üzerinde dönüyor. Bu ekosistem de benzer şekilde bu konuda bağımsız olarak çalışan kişiler ya da hizmet verenler aracılığıyla büyüyor. Bu çok farklı, şimdiye kadar gördüğümüz, alıştığımız anonim şirket, hisse senedi, sermaye piyasaları kavramlarının bambaşka bir hali. Biraz daha açmakta fayda var.

Efendim, kripto bazlı ekonomilerde girişimci bir şirket değil bir sistem kuruyor. Yani? Girişimci yukarıda bahsettiğimiz bir fikri, kendi şirketi altında patentler, telif hakları vb. ticari kılıflar altında saklamak yerine, açık kaynak olarak tüm topluma açıyor.



Sonrasında da olabildiğince çok sayıda geliştiriciyi bu fikir altında çalışmaya ikna ederek kendini bu fikri geliştirmeye adamış bir topluluk oluşturmayı hedefliyor. Bunun ne faydası var. Faydası çok.

En başta, kişilerin ya da şirketlerin gizli saklı tuttuğu hizmetler her zaman o kişilere bağlı kalır. Yarın öbür gün kişiler arasında anlaşmazlık çıktığında ve kişiler işi bıraktığında bu girişimden fayda sağlamayı uman kişiler olarak işiniz çok zor.

2000'lerin başında yatırımcıların en çok zarar ettiği durumlar bu tip ortaklar arası sorunlardan kaynaklanmıştı. Ya da diyelim şirket bir anda bir başka büyük şirkete satıldı ve hizmet vermeyi durdurdu. Başınıza gelmiştir muhakkak. Kullanmayı çok sevdiğiniz bir internet servisi bir gün "kusura bakmayın satıldık, size hizmet veremediğimiz için üzgünüz, ama biz çok para kazandığımız için çok mutluyuz" diye bir not bırakıp ortadan kaybolabiliyor. Yapacak hiçbir şeyiniz yok değil mi? Yeni teknolojiler ile artık öyle değil. Açık kaynak olarak kurulan yapılarda, bütün yapılar ve kurulan sistem herkese açık olduğu için, eğer kurucular bir gün herhangi bir nedenle ayrılırsa, yapılan iş ortada olduğu için (eğer talep varsa) başkaları o işi alıp devam ettirebilir. Özellikle de girişimci bu yapı altında bir topluluk oluşturmayı becerebilmiş ise. Evet ama bu sistemin düzgün çalışabilmesi için kaynağa ihtiyaç var. Doğru. Belki de şimdiye kadar duyduğunuz ama tam adlandıramadığınız, ICO (Initial Coin Offering) ve Token kavramlarını da içeren bu kaynaklar nasıl sağlanıyor? Ona da bir sonraki bölümümüzde bakalım



ICO ve token dünyası:

Yeni dünyada girişimciler için aranan kan bulundu mu?

Yeni dünyada, yaratılan katma değer sadece girişimciler ve yatırımcılar değil tüm kesimler tarafından paylaşılıyor. Bunu sağlayan da Token dediğimiz yeni tip varlıklar. Gelin nedir bir bakalım.

Önceki bölümlerde bildiğimiz anlamda klasik girişimci- yatırımcı ilişkisinin yeni teknolojiler ile birlikte değişmeye başladığını belirtmiştik. Bu değişim ile birlikte girişim tarafından yaratılan katma değerin girişimci-yatırımcı tekelinden çıkıp tüm kesimlere (geliştiriciler, kaynak sağlayıcılar, kullanıcılar gibi) yayıldığını, bu sayede de daha demokratik, daha sağlam ve sürdürülebilir bir yapı (en azından teoride) oluşturulduğuna değinmiştik.

Bu bölümde ise bu katma değerin nasıl bu kesimler tarafından paylaşıldığına bakalım. Ama öncesinde bu sistemi çalıştıran ana öğe olan Token nedir onu bir anlayalım…

Aranan kan bulundu mu? —ICO ve Token dünyası

Yeni teknolojiler ile yaratılan katma değer artık daha eşit şekilde paylaşılıyor. Ama yine de bu katma değeri yaratmak için bir kaynağa ihtiyaç var. Eskiden bu kaynağı yatırımcılar girişimcilere ortak olarak verirdi. Şimdi, pastadan başka pay sahibi olmak isteyenler var. Bu yeni teknoloji ile kurulan yapıların da çalışmak için güce bir nevi yakıta ihtiyacı var. Aynı klasik sistemde şirketlerin hisse senedi adı altında pay satıp yatırımcılardan para almaları gibi. Tek fark, burada bir şirket yok, bir sistem ile kişilerden ve şirketten bağımsız bir yapı var; dolayısıyla neyin payını alacaksınız? İşte yeni terimimiz. "Token". Bütün bu yeni sistemi çalıştırmak için gerekli güç bu Token'lardan geliyor.



Eski günlerdeki (hatırlayana tabii) PTT jetonu



Token'ın hisse senedinden farkı ne?

Klasik anlamda bellediğimiz tipik şirket yapısında, eğer bir şirkete yatırım yapmak isterseniz o şirketin hisselerini sahiplerinden satın alırsınız. Yok eğer şirket halka açık ise, o zaman hisselerinin işlem gördüğü açık pazarlardan o an için fiyatı ne olarak belirlenmiş ise onun üzerinden satın alabilirsiniz. Özel şirketlerin bu şekilde hisselerini açık piyasalarda işleme açmasına yani halka açılmasına Halka Arz işlemi (IPO-Initial Public Offering) denir.

Yeni tip Web 3.0 sistemlerinde ise klasik anlamda bir şirket bulunmadığı için (elbette girişimcilerin kendine ait bir şirketi olabilir ama bu şirket sadece sistemi kurmak ile meşgul, yoksa sistemin sahibi değil), sistemin ihtiyacı olan yakıt, yatırımcılar tarafından Token olarak sisteme konur, bu işleme de ICO (Initial Coin Offering) denir.

Token'ları bir nevi hisse senedi gibi düşünebilirsiniz ancak Token hisse senedinden çok daha kapsayıcı bir kavram. Çünkü sadece hisse senedinden çok daha fazla işlevi var.

Klasik anlamda hisse senedi aldığınızda elinizde iki farklı güç var. Birincisi, hisseniz oranında şirket yönetiminde söz sahibi olursunuz (en basit anlamda). İkincisi yatırım anlamında ya bu hisseler için şirketin her yıl temettü dağıtmasını beklersiniz, ya da şirketin geleceği hakkında spekülasyon yaparak, şirketin hissesini sermaye piyasalarında alır ya da satarsınız.

Token'da ise durum biraz farklı. Yönetiminde söz sahibi olabileceğiniz ya da size temettü verecek bir şirket yok. Token özünde bir ekosistemin parçası. Ama Token eğer kripto para borsalarında işlem görüyor ise alım-satım yaparak o Token'ın ve ilgili ekosistem ile ilgili spekülasyon yapabilirsiniz. Token'lar baştan girişimci tarafından belirlenen bir sistem ile tüm paydaşlara dağıtılır.

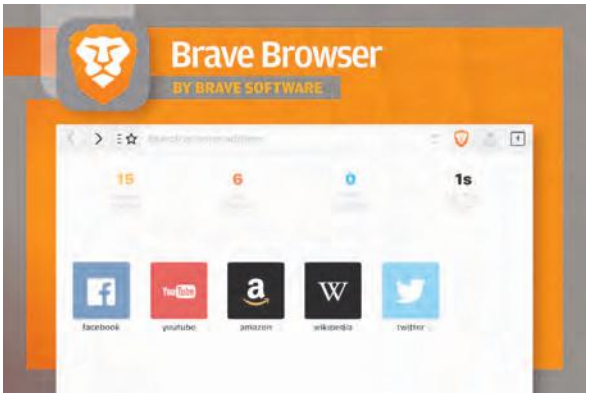
Bir kısmı fikrin sahibi ve sistemin çatışını kuran girişimci grubuna, bir kısmı geliştirme/test aşamasında yardımcı olan bağımsız geliştiricilere (eskiden gönüllü çalışan kişilere), bir kısmı verilecek hizmetin altyapısını sağlayacak olan bağımsız makinelere (aynı Bitcoin'deki madenciler gibi düşünün), bir kısmı da bu hizmeti kullandığı için şirkete para kazandıran (örneğin reklam geliri) kullanıcılara verilir. Her girişim için yukarıdaki paydaşlar, dağıtılacak miktar, dağıtım koşulları vb değişebilir, ancak sistem aşağı yukarı bu şekilde işler.

ICO ile işte bu Token'lar yatırımcılara satılır. Gelir, yukarıda bahsedilen model içinde paylaşılır, sistem büyümeye başladıkça önceden öngörülen miktarda Token'lar değişik paydaşlara bu şekilde dağıtılır. Yani, her bir paydaş katkısı ölçüsünden önceden belirlenmiş Token'a hak kazanır. ICO sonrası da bu Token'lar artık piyasalarda işlem görmeye ve sahipleri tarafından alınıp satılmaya başlarlar.

Token sadece yatırım için mi kullanılır?

Bununla da sınırlı değil Token ile yapabilecekleriniz. Token'lar aynı zamanda, ekosistemin farklı paydaşları tarafından yaratılıp harcanabilir. Örneğin, sistemin çalışması için de yardımcı olabilir ve Token kazanabilirsiniz. Hatırlarsanız, Bitcoin için demiştik ki, A kişisi B kişisine para transferi yaptığında makineler bu transferi yakalıyor, sisteme iletiyor, sistemde bunların kayıtları oluşturuluyor ve her 10 dakikada bir bu kayıtlar mühürleniyor. İşte bu para transferini yakalayan makineler her işlem başına ufak bir komisyon, her 10 dakikada bir kayıtları mühürleme işlemini yapmaya hak kazanan şanslı makine de büyük bir ödül (şu anda yaklaşık 12,5 Bitcoin) kazanıyor. İşte gördüğünüz gibi bulmacayı çözen makine Token (yani Bitcoin) kazandı. Makine sahipleri bu kazandıkları Bitcoin'leri herhangi bir kripto para borsasında satıp ABD Doları, Türk Lirası ne isterler ise onunla değiştirebilirler.

Sistemin çalışmasına yardımın başka çeşitleri de var. Örneğin Brave[71] aynı Chrome, Internet Explorer gibi bir tarayıcı ve kullanıcılarına her kullanım için BAT adında bir Token ödüyor.



Şöyle düşünün, web sitelerine girdiğinizde yukarı, aşağı, sağ, sol bu da yetmez gibi önünüze aniden çıkan (pop-up) reklamlar görüyorsunuz. Evet, bu siteler size içeriklerini parasız sunuyorlar ama karşılığında sizi reklama boğarak hatırı sayılır miktarda reklam geliri elde ediyorlar. İşte Brave o gelirin bir kısmını sizinle paylaşıyor. İsterseniz hiç reklamsız siteleri ziyaret edebiliyorsunuz, isterseniz tercihlerinize göre size uygun reklamlara maruz kalarak BAT Token kazanabiliyorsunuz. Rakamlar çok büyük değil, Token'in değeri ne olacak o da belli olmaz ama hiç yoktan iyidir.

Yukarıda bahsettiğimiz değişik paydaşlar bu ellerine geçen tokeni başka amaçlar için de kullanabilirler. Kazandığınız Token'ı sadece kripto para borsasında satmak yanında, bu ekosistemin yarattığı hizmetleri alır ve bu hizmetler karşılığı ödeme olarak kullanabilirsiniz. Örneğin, Dropbox benzeri bir depolama hizmeti veren Filecoin hizmetini kullandığınızda, dosyalarınızı şifreli biçimde dünyanın çeşitli yerlerindeki bilgisayarlarda güvenli bir şekilde saklayabilir ve bu hizmetin karşılığını Filecoin'in Token'ı ile ödeyebilirsiniz.
Bundan sonraki bölümde değişik değişik tokenlara yine en bildiğimiz örnek olan kripto paralardan başlayarak bakalım isterseniz.



Brave Browser Token'i BAT

[71] https://brave.com/

teknik olarak BLOCKCHAIN

BLOCKCHAIN şifrelemesi NE *demek?*

Baştan başlayalım: Şifreleme ne demek? Neden önemli? Blockchain sistemlerinin güvenli bir şekilde çalışmasının en kritik noktası şifreleme. Peki bu ne anlama geliyor? Neden bu kadar önemli? Aşağıda.



Şifreleme deyince aklımıza çok karışık anlaşılmaz konular geliyor değil mi? Normal. Aslında o kadar da zor değil ama anlayabilmek için biraz çaba sarf etmek gerek-her türlü konuda olduğu gibi. Peki neden önemli bu şifreleme? Çünkü şifreleme bize pek çok kişiye dağılan bilginin doğru ve tam olduğunu anlamamızı sağlıyor. Peki ama ne demek şimdi bu?

Efendim, daha önce de belirtmiştik. 90'larda internet hayatımıza girdi ve her tür dijital bilgi ve verinin yaygınlaşmasını ve bir taraftan diğerine kolayca iletilmesini sağladı. Bu harika bir olay, çünkü masrafsız bir şekilde bilgiyi kopyalayabiliyor ve dağıtabiliyorsunuz. Eğitim, araştırma ve gelişme için bulunmaz nimet. Ancak herhangi bir dijital varlığı internet üzerinden transfer etmeye kalktığınızda önümüze sorunlar çıkıyor.

Zira olur olmaz kopyalanmaması lazım, gerçek sahibinin kim olduğu biliniyor olmalı, o sahip gerçekten bu varlığı birine devretmek istiyor mu onu bilmeli gibi gibi.

İsterseniz internet üzerinden transfer edilebilecek pek çok dijital varlıktan en aşina olduğumuz para üzerinden bir örnek verelim.

Para, para, para-varlığı bir dert... ya yokluğu?



Para ilk zamanlarda fiziki olarak önce madeni para ve kâğıt halinde bulunurken, 60'lı-70'li yıllarda bilgisayarlar ile iletişim başlayınca kurumlar arasında kullanılan elektronik paraya, 90'lardan sonra internet yaygınlaşıp kişiler arasında iletişimin artması ile birlikte de dijital paraya evrildi.

Ancak, paranın alışverişe layık olabilme niteliğini koruyabilmesi için hep bir merkezi otoriteye (merkez bankaları ya da bankalar) ihtiyaç duyuldu. İnsanların güven duyacağı birilerinin kontrol etmesi lazım parayı diye düşünüldü içgüdüsel olarak-normal. Öbür türlü dijital bir nesneyi sonsuz olarak üretebilirsiniz, gerçekten size mi ait nereden bileceksiniz, yabancıların sözlerine nasıl güveneceksiniz?

Ya bir kişi birden fazla kopyalama yapar, sahip olduğu parayı hem size hem başkasına gönderirse? O nedenle, bankalar ve merkezi otoriteler vardı ki bu sorunlara karşı güvence altına alsın.

İşte tam bu sırada 90'ların sonunda Satoshi Nakamoto dediğimiz kişi(ler) para transferi teknolojisini şifreleme ile birleştirdi ve tek bir otoriteye bağlı kalmaksızın, o otoritenin sağladığı güvenin yerini makinelerin aldığı bir yapı oluşturarak adeta bir devrim yarattı. Bu devrim ile işlemlerin arasında yer alan güven abidesi banka gibi kurumlara olan ihtiyaç neredeyse sıfıra indi?-çünkü artık her makine kendi başına bir banka!

Nasıl olur da makineler koskoca bankanın yerini alır derseniz şöyle: Banka kişilere ait banka hesaplarını ve yapılan işlemleri tutarak bir kişinin kendine ait bir varlığı birden fazla kişiye göndermesine engel oluyor. Bunu yaparken doğru ve güvenilir davrandığına emin olmamız için gerek iç organizasyon yapısı gerekse dışarıdan merkezi otorite tarafından dayatılan kontrol ve cezalarına tabii. Blockchain (örneğin Bitcoin sistemi) ise bir kişinin elindeki parayı iki kere harcamasını bütün hesapları ve bütün işlemleri halka açık olarak yaparak önlüyor. İşlemler ve bakiyeler halka açık ama isminiz gibi özel detaylarınız gizli. Dolayısıyla, bir kişiden diğerine Bitcoin gönderildiğinde herkes gönderenin bakiyesinden o paranın düştüğünü alıcının bakiyesinin de o para kadar arttığını görüyor. Yani bankacılık sisteminde ben bankanın yanlış yapmayacağına emin olmak için kendi iç kontrolleri ya da denetleyici kurumlara güvenmek durumunda iken, Blockchain'de her şey açık olduğu için "gözlerime" güvenmem yeterli.

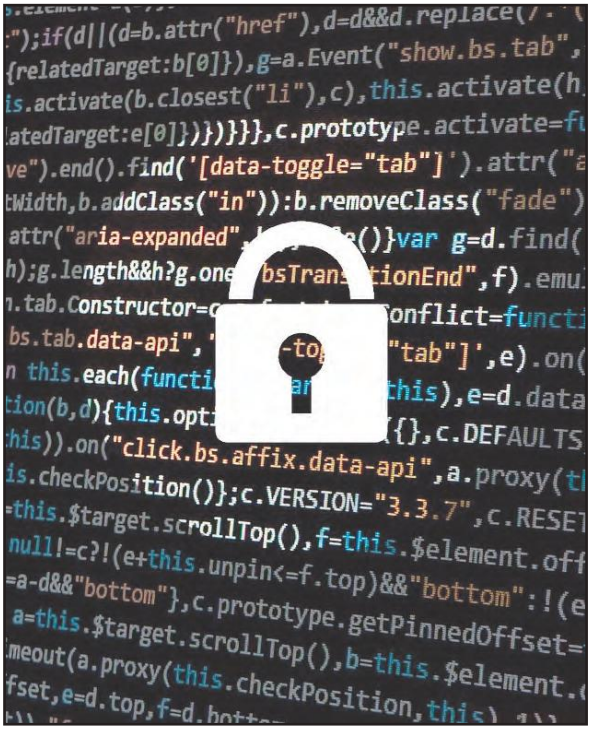
Tekrar edelim: Para örneğini hep konuşulduğu için verdik. Konu sadece para ile sınırlı değil. Bu her tür dijital varlık olabilir: Örneğin noterlerde saklanan bilgi, bir dijital sanat eseri gibi; bana ait olan, başkasının üzerinde hak iddia edemeyeceği, dijital olarak saklanabilen, istediğimde başka birine dijital olarak kısa sürede transfer edebileceğim her tür varlık ya da nesne.

Çok karışık değil mi bu şifreleme?

Yukarıda bahsettiğimiz hem tüm hesap bakiyeleri ve transferler açık olacak hem de hesap sahiplerine ait özel bilgiler gizli kalacak nasıl oluyor dediğimizde bu şifreleme sayesinde.

Şifreleme Blockchain'in temelini oluşturuyor, çünkü Blockchain dağınık bir sistemde çalışıyor, yani bilgi binlerce farklı, birbiri ile ilintili ama birbirini tanımayan makine üzerinde bulunuyor. Dağınık sistemlerin kontrolü olmadığı için bilginin düzgün ve değiştirilmemiş olması son derece önemli-bunu sağlayan da şifreleme sistemi. Yani şifreleme sayesinde herhangi bir bilgi Blockchain üzerindeki her nokta üzerinde hem aynı şekilde tutarlı hem de gizli olarak tutulabiliyor.

Şifreleme teknik ve karmaşık görünse de onu daha iyi anlamak bize günlük hayatımızda Blockchain teknolojisini nasıl daha verimli olarak kullanırız konusunda farklı ipuçları verebilir. Eğer genel yapı olarak ne olduğunu anladıysak, biraz daha teknik olarak nedir şifreleme ona da şimdi bakalım…



Şifreleme ve öğütme ne kadar önemli?

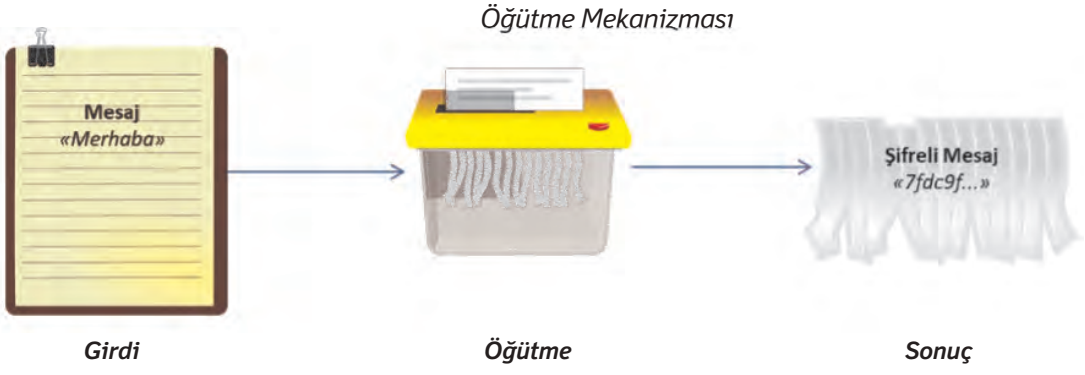
Dijital dünyada bir varlığı bir kişiden diğerine transfer ederken iki önemli konu var dikkat etmemiz gereken:

1. Birincisi, öncelikle varlığın transferi güvenli bir şekilde yapılmalı. Buradan kastedilen bu dijital varlık değiştirilmeden bir taraftan öbürüne geçmeli ve geçtikten sonra bu işlem bir daha değiştirilemez olmalı. Yani herkeste aynı bilgiler olmalı. Herkeste aynı bilgi olursa kimse "eyvah kandırılıyor muyum?" kaygısı yaşamaz, gece evinde rahat uyur. Bu öğütme (hashing) sayesinde başarılıyor.

2. İkincisi, bana ait bir varlığı bir başkasına devredeceksem öncelikle bu varlığın bana ait olduğu ve bu varlığı kendim devretmek istediğim, yani bu işlemi başlatan kişinin gerçekten ben olduğum (orijinal/otantik olduğunun) teyit edilmeli. Ama bunu yaparken bir taraftan da bana ait özel bilgilerin gizliliği kalması da sağlanmalı. İşte bu da şifreleme (encryption/decryption) sayesinde başarılıyor.

Önce bir öğütelim mi?

Kapalı bir kutu (belki de bir kâğıt öğütücü) düşünün. Bir taraftan anlamlı bir sözcük veriyorsunuz, diğer taraftan rakam ve sayılardan oluşan anlamsız rastgele bir sayı/harf dizisi veriyor. İşte buna öğütme deniyor. Bir örnek yapalım dilerseniz:



Siz de deneyebilirsiniz[72]-aynı sonucu bulacaksınız (bu sonuca teknik olarak hash deniyor).

Girdi	Şifreli Sonuç
Merhaba	7fdc9f4717c5fe66df286c700fab969b4d6209d03aa84624c5f8f58c17c9c058

İşte işin özü bu. Değişik öğütme mekanizmalarından en popüler olan SHA-256 böyle çalışıyor. Girin herhangi bir SHA-256 şifreleme sitesine "Merhaba" yazın, yukarıdaki sonucun aynısını verecek size: 64 karakterli bir dizi.

[72]http://www.xorbin.com/tools/sha256-hash-calculator

Peki buraya uzunca bir paragraf koymak istesek ne olur? Mesela,

Girdi	Şifreli Sonuç
Yatağın başından ucuna kadar uzanan mavi damalı yorganın engebeleri, gölgeli vadileri ve mavi yumuşak tepeleriyle örtülü tatlı ve ılık karanlıkta Rüya yüzükoyun uzanmış uyuyordu. Dışarıdan kış sabahının ilk sesleri geliyordu: Tek tük geçen arabalar ve eski otobüsler, poğaçacıyla işbirliği eden salepçinin kaldırıma konup kalkan güğümleri ve dolmuş durağının değnekçisinin düdüğü. Odada, lacivert perdelerin soldurduğu kurşuni bir kış ışığı vardı. Uyku mahmurluğuyla Galip, karısının mavi yorgandan dışarı uzanan başına baktı: Rüya'nın çenesi yastığın kuştüyüne gömülmüştü. Alnının eğiminde, o sırada aklının içinde olup biten harika şeyleri insana korkuyla merak ettiren gerçek dışı bir yan vardı. 'Hafıza,' diye yazmıştı bir köşe yazısında Celâl, 'bir bahçedir.' 'Rüya'nın bahçeleri, Rüya'nın bahçeleri...' diye düşünmüştü o zamanlar Galip, 'düşünme, düşünme, kıskanırsın!' Ama Galip karısının alnına bakarak düşündü.	4144231a09b37be5e58def84d0773802240cb283a3a74dc840bc2d1ae454c723

Ta tam! Bambaşka bir dizi ama yine 64 karakterli. Buraya isterseniz girdi olarak koca bir ansiklopedi koyun, sonuç yine 64 karakterli bir dizi olacak.

Şimdi ilk örneğimize geri dönelim: Merhaba kelimesinin sonuna bir "!" işareti ekleyelim, bakalım ne olacak?

Girdi	Şifreli Sonuç
Merhaba!	b1726b923349fd632fa7ce8b62a06c5a3f785be1db4f6a831eef58d70c7a45cc

Yukarıdaki "Merhaba" da çıkan sonuç ile karşılaştırın bakalım. Tamamıyla değişti!. Bir harf ekledik ama ilk kelimeden tamamen farklı bir sonuç çıktı ortaya. Ama dikkat edin 64 karakterli yine.

Çok güzel de bu kadar girizgahı neden yaptın derseniz? Buraya kadar anlattıklarımızı biraz daha açalım. Aynı girdiler hep aynı sonucu veriyor. Ama girdi içinde bir harf bile değiştirin, çıkan sonuç bambaşka oluyor. Bu ne işe yarıyor? Bu girilen bilginin orijinal ya da otantik (değiştirilmemiş) olup olmadığını anlamamıza yarıyor. Eğer elinizde bir bilgi (girdi) ve bu bilgi sonucu ortaya çıkan şifreli bir sonuç da varsa, bu girdi hakikaten bu sonucu mu veriyor test edebiliyorsunuz. Girin ilk bilgiyi (girdiyi) şifrelemeye aynı sonucu bulacaksınız.

Bu arada şunu da belirtmekte fayda var. Bu şifreleme mekanizmalarının özelliği şu: sonucu biliyor olmanız girdiyi de bildiğiniz anlamına gelmiyor. Yani, girdiyi biliyorsanız sonucu bulabiliyorsunuz ama sonuçtan geriye bilgiye gidemiyorsunuz. Yani, öğütücüden geçmiş kâğıtlara bakarak kâğıtta ne yazıyordu okuyamıyorsunuz. Ancak kağıdın orijinali varsa elinizde onu öğütücüden geçirip önceki öğütülmüş kâğıt demetinin aynısını elde edebiliyorsunuz.

Bilginin tutarlı olduğunu bilmek ne işimize yarıyor? Yukarıda yazdığımız gibi bilgiyi dağıtıp tek bir noktada tutmadığınızda, bilginin dağınık olarak herkeste aynı şekilde durması, bilginin doğruluğu ve kişilerin bu bilgiye olan güvenini sağlayan en önemli etken. Öbür türlü kırk kişide kırk farklı bilgi olursa ona dedikodu denir, kimse de beş kuruş değer vermez.

Harika. Ama yarın öbür gün ben bu mesajı değiştirsem "Yok, yahu ben öyle dememiştim, böyle demiştim" desem? Kusura bakmayın mümkün değil, çünkü mesajınız alındı, güzel bir şekilde öğütüldü ve tüm sistemdeki makineler üzerinde aynı şekilde tutulmaya başladı.

Peki çok güzel. Ama ya bu mesajı ben değil de bir başkası yazdıysa? Onu da şifreleme hallediyor. Şimdi de şifrelemeye bakalım:

Şifrelemeli mi, şifrelememeli mi? Şimdi de şifreleyelim…

Şifreleme bir nevi kilitleme demek. Diyelim bir mesajınız var. Şifreleme derken, bir anahtar ve kilit düşünün, bu anahtar sizin mesajınızı alıyor ve kilidin içine koyup kilitliyor.



Basit (simetrik) Şifreleme

Dolayısıyla sizin yazdığınız bu mesajı sadece anahtarı verdiğiniz kişiler görebiliyor. Buraya kadar güzel. Bu anahtarı bir kişiye verirsem bir sorun yok. Bir taraf mesaj yazar, anahtar ile kilitler, diğeri anahtarın kopyası ile açar mesajı okur, sonra yeni bir mesaj yazar ve anahtarı ile şifreler ve bu böyle sürüp gider. Ancak işin pratiğe geldiğimizde soru(n)lar ortaya çıkmaya başlıyor.

Ya karşı taraf bu anahtarı başka birine daha verirse? O zaman ne olacak? O anahtarı verdiği üçüncü kişi bir mesaj yazarsa? Karşı tarafın bu mesajı yazdığını nereden bileceğim? Anahtarın kopyalanabildiği durumlarda sıkıntı var, mesajı kimin yazdığını anlamak zor.

İşte bu "mesajı kim yazdı, kimler okudu sorununu çözmek için" 1976 yılında yeni bir şifreleme yöntemi ortaya atılmış. "Özel Anahtar" ve "Genel Anahtar" kavramları çıkmış.

"Özel Anahtar" ve "Genel Anahtar"

Yine yukarıdaki anahtar-kilit örneğinden devam edelim. Demiştik ki iki ana problem var. Birincisi benim yazdığım mesajın içeriğini anahtarı olan (ya da anahtarı alan) herkesin görüyor olması, ikincisi de herkesin bu mesajı benim yazdığımdan (kilidi benim kilitlediğimden) emin olması.

Önce ikinciden başlayalım. Şöyle demiş bir akıllı bilim adamı. "Şu kilidin özelliğini bir parça değiştireyim-öyle bir hale getireyim ki, iki tane farklı ama birbiri ile uyumlu anahtarı olsun. Öyle uyumlu olsunlar ki, herhangi biri ile anahtarı kilitlediğimde diğeri açabilsin. Bu anahtarlardan birini çoğaltıp tüm arkadaşlarıma vereyim. Ama diğer uyumlu anahtar sadece bende olsun" İlginç bir mantık. Neye yarıyor peki? İki farklı şekilde kullanabiliriz bu anahtarları.

Birincisi birileri bana bir mesaj göndermek isterse ise mesajı yazıp kilide koyar ve kilitler. Kilidi açan diğer anahtar bende olduğu için, sadece ben açarak bu mesajı okuyabilirim. Böylece bana yazılı mesajın sadece benim tarafımdan okunması garantilenmiş olur.

İkincisi, eğer ben bir mesaj yazıp sadece kendimde bulunan anahtar ile bu kilidi kilitler isem, isteyen herkes benim dağıttığım diğer anahtar ile kilidi açabilir ve içindeki mesajı benden geldiğini bildiği mesajı okur. Böylece, hepimiz yazılan bir mesajın hakikaten benden geldiğine emin oluruz.

İşte bu iki anahtardan bana ait olana "Özel Anahtar", herkese verdiğime de "Genel Anahtar" deniyor.



Mesaj
Özel Anahtar kilitler
Genel Anahtar açar

Özel Anahtar
Sadece bana ait!

Genel Anahtar
Herkese verebilirim

Özel ve Genel Anahtarlar

Yukarıda bahsettiğimiz gibi Özel Anahtar ve Genel Anahtarı farklı ama birbirlerine uyumlu iki anahtar gibi düşünebiliriz. Aradaki tek fark, Özel Anahtarın sadece benim bildiğim (hiç kimse ile paylaşmadığım) bir anahtar olması. Genel Anahtar ise yine bana ait, ama herkes ile paylaştığım tüm dünyanın görebileceği bir anahtar.

İlişkileri ise şu: Benim Özel Anahtarım ile kapadığım kapıyı (şifrelediğim mesajı) Genel Anahtarı bilen herkes açabiliyor (şifreyi açıp mesajı görebiliyor). Ya da benim Genel Anahtarıma sahip birinin kapadığı kapıyı (bana gönderdiği şifreli mesajı) sadece benim açabiliyor olmam (şifreyi açıp mesajı okumam).



Mesajımı Özel Anahtarım ile kilitleyip sana gönderiyorum

Genel Anahtarım ile kilidi açıp mesajı okuyabiliyorsun

Şifreleme Mekanizması

İşte yukarıdaki ilk sorunu çözdük. Mesajın benden geldiğini herkes gördü. İyi de yazının içeriğini tüm dünya görmüş oldu, ben içeriği bilinsin istemiyordum, şimdi ne olacak? İşte burada ilk bölümde anlattığımız öğütme mekanizması ortaya giriyor ve sizin yazınızı okunamaz bir hale getiriyor.

Para ya da başka dijital varlığın Blockchain ile aktarılmasında da işte yukarıdaki sistem kullanılıyor.

• Özel Anahtar ile bana ait olan bir varlığı bir başkasına gönderiyorum, paranın benim bakiyemde olduğu ve bu gönderdiğim paranın miktarını herkes görüyor (Ki kanıtlama işlemine Dijital ya da Sayısal-İmza deniyor).
• Ama aynı zamanda gönderdiğim kişinin Genel Anahtar'ını da ekliyorum ki, hem diğer insanlar o kişinin Genel Anahtarını kullanarak parayı gerçekten ona gönderdiğimi görebilisinler, hem de o kişi sonra bu anahtara uyumlu kendi Özel Anahtarı'nı kullanarak bu parayı sahiplenebilsin ve başkalarına gönderebilirsin.
• Öğütme sayesinde ise bu bakiyenin bana ait olduğunu gizleyebiliyorum.

Para ya da başka dijital varlığın Blockchain ile aktarılmasında da işte yukarıdaki sistem kullanılıyor.

• Özel Anahtar ile bana ait olan bir varlığı bir başkasına gönderiyorum, paranın benim bakiyemde olduğu ve bu gönderdiğim paranın miktarını herkes görüyor. (ki kanıtlama işlemine Dijital (ya da Sayısal) İmza deniyor).
• Ama aynı zamanda gönderdiğim kişinin Genel Anahtar'ını da ekliyorum ki, hem diğer insanlar o kişinin Genel Anahtarı kullanarak parayı gerçekten ona gönderdiğimi görebilisinler, hem de o kişi sonra bu anahtara uyumlu kendi Özel Anahtarı'nı kullanarak bu parayı sahiplenebilsin ve başkalarına gönderebilirsin.
• Öğütme sayesinde ise bu bakiyenin bana ait olduğunu gizleyebiliyorum.

Peki Blockchain şifrelemesi nasıl çalışıyor?

İşte dijital dünyada devrim yaratan şifreleme mekanizması bu şekilde çalışıyor. Bu mekanizma sayesinde dijital varlıkların (örneğin paranın) herhangi bir aracıya ihtiyaç doğmaksızın güvenli bir şekilde bir taraftan öbürüne taşınması sağlanıyor. Dijital olarak bana ait olan her tür varlığı bu şekilde bir başkasına transfer edebilirim bu teknoloji ile. Blockchain teknolojileri önceki bölümde değindiğimiz iki kavramı (öğütme ve şifreleme) kullanarak kendi sistemlerini otomatik güvenli hale getiriyorlar (ya da tek bir kişiye duyulan güven ihtiyacını sıfıra indiriyorlar).

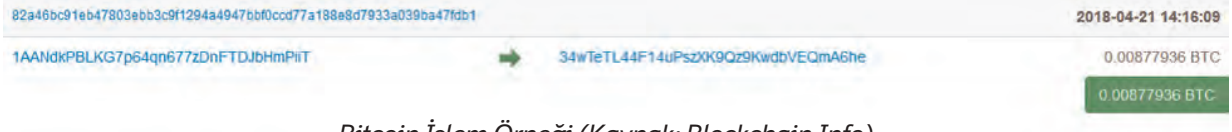
Şifrele ki senden geldiğini anlasınlar

Önce şifreleme kısmına bakalım. Efendim, biliyorsunuz Blockchain sistemi bir dijital varlığın bir kimseden diğerine geçmesini sağlıyor. Burada da bu dijital varlıklardan en bilineni olan dijital para Bitcoin ile konuyu örneklendirelim:

Varsayalım benim bir dijital varlığım, örneğin 1 Bitcoin'im var. Öncelikle, demiştik ki, bütün Blockchain işlemleri aynı şekilde tüm makineler tarafından tutuluyor. Dolayısıyla sistemdeki bütün makineler bu 1 Bitcoin'in bende olduğunu biliyor (o paraya nasıl sahip olduğum ise aşağıda anlatacağımız işlem sonucu daha netlik kazanacak).

Şimdi ben bu parayı Ayşe'ye göndereceğim. Sistem üzerindeki makinelere diyorum ki "Ey ahali, ben 1 Bitcoin'imi Ayşe'ye gönderiyorum". Sistemde "ben" diye bahsettiğim bana ait bir adres. Ayşe de aynı şekilde bir adres. Dolayısı ile diyorum ki, "Ben, bu adresin sahibi kişi şu adrese bu kadar parayı gönderiyorum". Sistem üzerinden görülenler: bana ait hesap numarası, karşı tarafa ait hesap numarası ve ne kadar para gönderildiği.

Merak ediyorsanız nasıl bir şeydir bu diye, işte bir örnek aşağıda: Bunu da kaydedip internet üzerinde yayınlıyorlar.[73]



Bitcoin İşlem Örneği (Kaynak: Blockchain.Info)

Yukarıdaki işlemi yazarken aslında iki küçük ekleme yapıyorum işleme. Birincisi, işlemi sisteme kendi Özel Anahtarım ile kaydediyorum. Böylece herkes bana ait olduğunu anlıyor bu paranın.

[73] https://blockchain.info/block/0000000000000000001c2fa26ad4d4850fe94e688cfccf812c4fbe6d245761eb

İkincisi de, Ayşe'nin Genel Anahtarını da kaydediyorum. Böylece paranın Ayşe'ye gittiğini de anlıyor herkes. Ve bu parayı sadece Ayşe kullanabilir, çünkü bu Genel Anahtara karşılık gelen Özel Anahtar sadece Ayşe'de var.

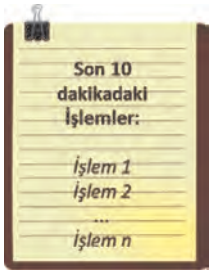
Eğer Ayşe bu parayı bir gün Mehmet'e göndermek isterse, benzer şekilde kendi Özel Anahtarı'nı kullandığında sistem bakacak "Hah tamam bu para zamanından Ayşe'nin Genel Anahtarı kullanılarak gönderilmişti, yani Ayşe'nin malı, şimdi Ayşe Özel Anahtarını kullanarak bu malın kendi sahipliğini ve Mehmet'in Genel Anahtarını kullanarak bu sahipliği Mehmet'e geçirdiğini söylüyor, o zaman yapalım bu transferi" diyecek.

Şimdiye kadar (2009 yılındaki başlangıcından beri) Bitcoin üzerinde yapılmış bütün transferler kayıtlı ve yukarıdaki gibi görülebiliyor. Yani aslında işlemlerin hepsi şeffaf hem de en başından beri. Yani Ayşe'ye gönderdiğim parayı da ben birinden aldım. Bu kişi de bir başkasından. Bu şekilde 2009 yılına kadar gidebilirsiniz. Peki ya en başında ne olmuştu? Bu kadar Bitcoin nasıl çıktı ortaya? Şimdi ona da bakalım:

Öğüt ki, sonsuza kadar kaydedilsin

Hatırlar mısınız, önceki bir bölümde şunu söylemiştik: "Blockchain sisteminde yükü çeken makinelerin bu yaptıkları işlemleri kayıt etme, daha sonra da teyit etme işlemi sonucu aldıkları ödüle (ya da lotaryaya) Bitcoin deniyor. Neden lotarya deniyor? Zira, bu on dakikada bir yapılan teyit işlemi aslında çok zor bir bulmaca. Bir nevi Sudoku oyunu gibi düşünün"
Şimdi dilerseniz bu bulmaca konusunu biraz daha açalım. Ortada tabii ki bir bulmaca yok ama bir öğütme işlemi var. Aynı yukarıda olduğu gibi "girdi" ve "çıktı" kısmı olan bir SHA şifrelemesi.
Girdinin (input) iki parçası var
• Belli bir süre içinde gerçekleşen tüm işlemlerin bir dökümü
• Bir de bir sayı

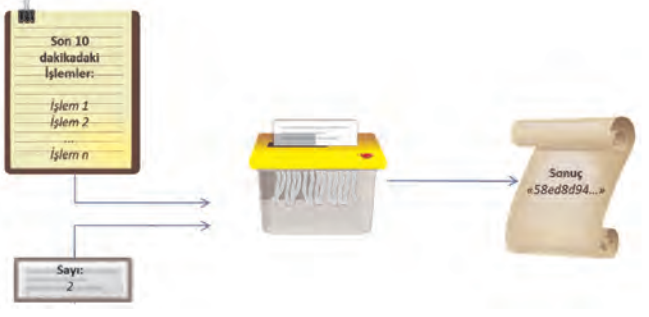
Çıktı (Output) ise yukarıdaki gibi 64 karakterli bir şifre. Sistem söyle çalışıyor.



1. Her 10 dakikada bir Bitcoin ile yapılan bütün işlemler bir araya toplanıyor ve makinelere gönderiliyor
2. Sonra sistem bütün makinelere şunu söylüyor: "Ey makineler, işlemlerin toplam dökümü[74] elinize geçti, şimdi bu işlem dökümünü alın yanına öyle bir sayı ekleyin ki, öğütmeye koyduğunuzda çıkan çıktı (output) beş tane sıfır ile başlasın"
3. Makineler bu çıktıyı alıyor ve sırayla rakamları denemeye başlıyorlar. Önce 1 ekliyor, çıkan sonuca bakıyor,

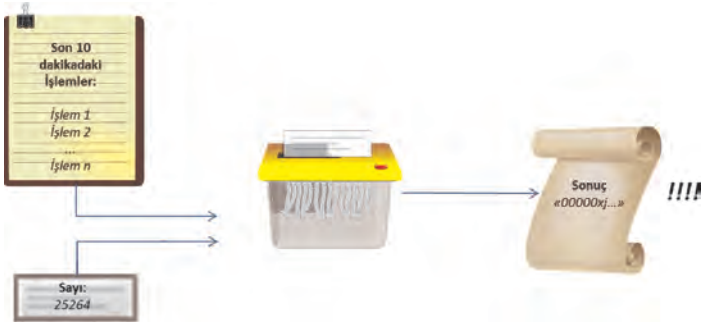


yok olmadı, "370ff8bo…" ile başlayan bir output verdi. Sonra 2 ekliyor, yine bakıyor:



[74]https://blockchain.info/block/00000000000000000 01c2fa26ad4d4850fe94e688cfccf812c4fbe6d245761eb

bu sefer "58ed8d94…" diye başlayan bir sayı verdi… Yine olmadı… Böyle böyle sırayla tüm sayılar deneniyor. Ta ki bir sayı (diyelim "25264") bize "00000…" ile başlayan bir sonuç verene kadar!



4. "00000…" ile başlayan sonucu ilk bulan makine "Buldum!" diyerek bu sonuca ulaştıran sayıyı ("25264") diğer makinelere haber veriyor.
5. Sonucu gören makineler, işlem dökümünü 25264 sayısı ile birlikte şifreye sokuyorlar, bakıyorlar hakikaten çıkan sonuç "00000…" ile başlıyor, "Tamam" diyorlar, "Sonuç doğru" ve bir sonraki 10 dakika için yapılan işlemlere geçiyorlar.
6. "25264" rakamını bulan makine işte bu ödülü (şu anda 12,5 Bitcoin yani 100.000 ABD Doları civari bir rakam) kazanıyor!

İşte bu kadar. Yukarıda anlatılanları görsel olarak izlemek isterseniz, aşağıdaki İngilizce videoyu *("Blockchain nasıl çalışır?— görsel demo" (İngilizce) Kaynak: Anders Brownworth - YouTube)* hararetle tavsiye ederim. Aklınıza yatmayan her konu basit bir şekilde özetlenmiş.

Yukarıdaki süreç her 10 dakikada bir tekrar ediyor ve her 10 dakikada bir 12,5 Bitcoin yaratılarak, sonucu bulan makineye veriliyor yani sisteme sokuluyor (buna İngilizce "mining" deniyor).

İşte yukarıda bahsettiğimiz birbirimize transfer edilen Bitcoin'ler bu şekilde yaratılıyor. Şu ana kadar (Nisan 2017 itibariyle) 17 Milyon Bitcoin yaratıldı. Önümüzdeki 100 yıl boyunca yaklaşık 4 Milyon Bitcoin daha girecek sisteme ve orada 21 Milyonda duracak piyasadaki miktar.

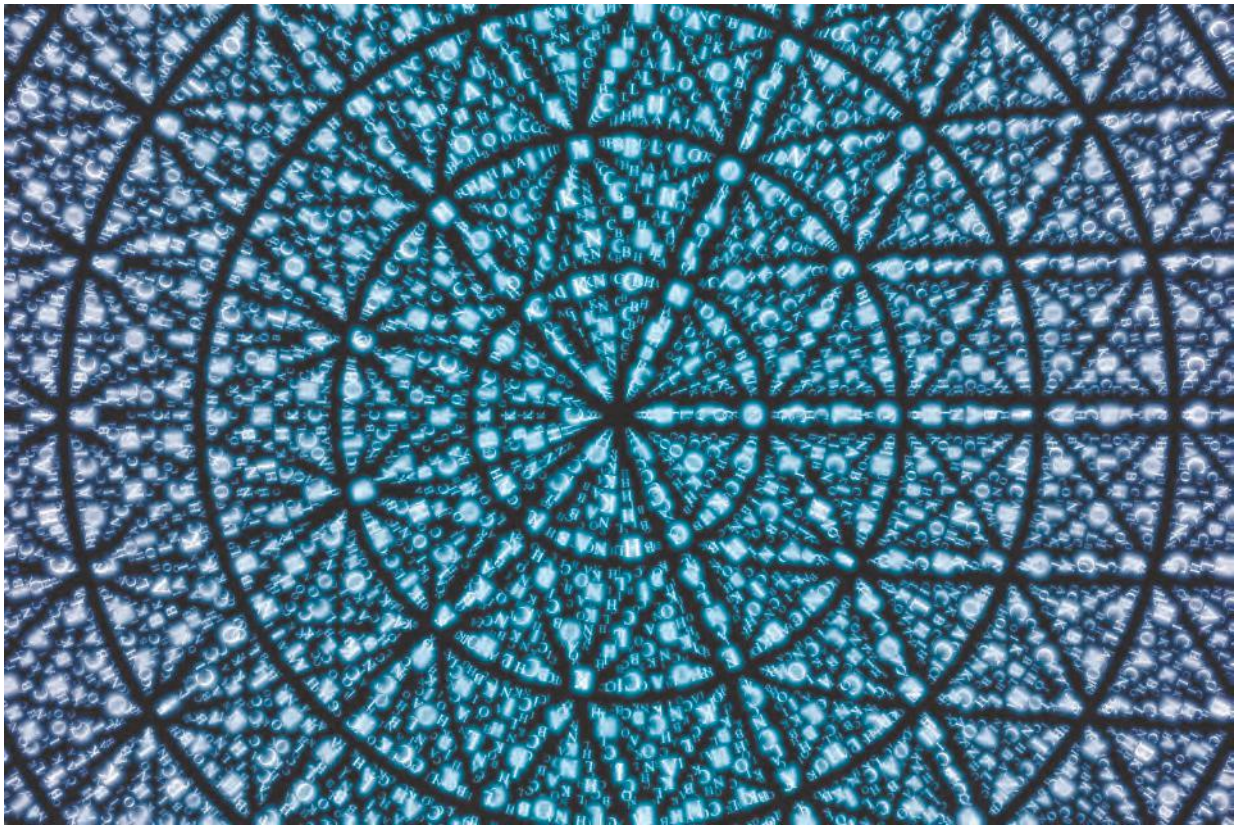
Nasıl oldu da 9 yılda 17 Milyon yaratılırken bundan sonraki 100 yılda 4 Milyona düşecek derseniz, Bitcoin yaratıcıları para enflasyona yenik düşmesin diye her dört yılda bir verilen ödülü yarıya düşürüyorlar. İlk dört yıl 10 dakikada bir 50 Bitcoin verilirken, sonra bu 25'e düştü, şu an 12,5'da, 2021'de 6,25'e inecek. Peki bu madenciler bu ödül ile yaşıyorlar, ödül miktarı düşerse madencilik yapmayı bırakmazlar mı diye akla bir soru gelebilir. Olabilir tabii ama bu yeni para yaratımı ile ilgili bir konu. Madenciler bir de aynı zamanda, yapılan transferler üzerinden bir komisyon almaya devam ediyorlar. Eğer Bitcoin kişiler arası para transferinde sık kullanılmaya devam ederse ya da değeri şimdiki gibi yüksek olursa bir sorun olmaz. Çok düşerse o zaman bir kısım madenci sahneden çekilir, kalanlara pastadan daha büyük bir dilim düşer ve onlar çalışmaya devam ederler.

Bu kadar mı?

Evet, aslında işin özü bu kadar basit. Genel Anahtar aracılığı ile zamanında bana gönderilmiş olan bir varlığı, Özel Anahtarımı kullanarak şifreleyip bir başkasına gönderiyorum. Sistem de bu işlemleri 10 dakikada bir toplayıp öğütüp bir paket haline getiriyor. Şifrelemeyi kullanarak bana ait olduğunu kanıtladığım bir dijital varlığı öğütücü sayesinde bir başkasına kati olarak transfer ediyorum-bunun için de hiç kimsenin onay vermesine ihtiyaç duymuyorum.

Para örneğinden yola çıktık ama tekrar edelim. Dijital olarak bana ait olan her tür varlık ve bilgiyi bu şekilde bir başkasına transfer edebilirim bu teknoloji ile. Seçenekler ve ihtimaller sınırsız-gerisi hayal gücünüze kalmış…

BLOCKCHAIN *nasıl* **kendi** başına *hareket* ediyor? ipucu: **uzlaşma**



Blockchain bazlı sistemlerde binlerce makine ortak bir yerden direktif almadan beraberce hareket ediyor. Nasıl? Anlamak için önce işin temelini anlamak lazım:

Blockchain bazlı şifreli sistemlerin birbirine bağlı ancak birbirinden bağımsız binlerce makineden oluştuğundan daha önceki bölümlerimizde bahsetmiştik. Peki bu makineler merkezi bir otorite olmadan nasıl hep birlikte aynı anda aynı kararı veriyorlar? Aralarında hiç sorun çıkmıyor mu? Eğer çıkıyorsa bu sorunları nasıl çözüp tekrar aynı yolda ilerliyorlar? Birileri sistemi manipüle etmek isterse ne olacak? Olamaz mı? Olur tabii ki…

Sistemin mimarları buna karşı nasıl önlemler almış ona bir göz atalım şimdi. Konuya başlamadan önce Blockchain sistemini kısaca hatırlatmakta yarar var.

Demiştik ki, Blockchain yapılan bir işlemin binlerce makinede kaydının tutulması ve belli aralıklar ile (örneğin Bitcoin'de on dakikada bir) bütün makinelerin ellerindeki kayıtların toplanıp tabiri caiz ise bir balya haline getirilmesi şeklinde çalışan bir sistem idi. Bir araya getirilen bu bilgilerin her makinede aynı şekilde bulunması gerekiyor ki, üzerine yeni bir balya işlem gelebilsin. Dolayısı ile altta kalan balyadaki bilgiler hem tutarlı olsun hem sonradan değiştirilemesin (balya bağlandıktan sonra binlerce makineye dönüp işlem değişikliği yapamazsınız, imkânsıza yakın bu).

Peki ama yukarıda bahsettiğimiz bu on dakikada bir her makinede gerçekleşen işlemler nasıl aynı şekilde bulunuyor? Ya birileri ortama nifak tohumu ekmeye kalkar ve sahte işlem girmeye kalkarsa? Nasıl sağlanacak bu mutabakat? Öncelikle 'mutabakat' derken ne kastediyoruz ona bir bakalım:

Bizans generallerinin problemi ne?

Efendim, ilginçtir, birbirinden bağımsız sistemlerin (bunlara dağıtık sistemler de deniyor) arasındaki ilişkiler ve çıkan anlaşmazlıklar literatüre "Bizans Generalleri Problemi" olarak girmiş.

İlk olarak Prof. Dr. Eralp Akkoyunlu ve ekibi tarafından 1975 yılında yazılan "Some constraints in and tradeoffs in the design of network communications (İletişim ağlarının dizaynı sırasında yapılan -karşılaşılan- bazı kısıtlama ve feragatler)[75]" isimli bir araştırmada bu sorun ortaya atılmış. (New York Üniversitesi Bilgisayar Bölümü'nde kürsü başkanı olan ve 1987 yılında kendi elleri ile yaptığı on iki metrelik teknesi ile bir dünya seyahati gerçekleştiren Prof. Dr. Akkoyunlu 'yu da bu vesile ile saygıyla analım).

[75] http://hydra.infosys.tuwien.ac.at/teaching/courses/AdvancedDistributedSystems/download/1975_Akkoyunlu,%20Ekanadham,%20Huber_Some%20constraints%20and%20tradeoffs%20in%20the%20design%20of%20network%20communications.pdf

Sonrasında da 1982 yılında Bizans Generalleri Problemi[76] adıyla geliştirilmiş. Peki nedir bu problem, kısaca anlatalım:

Vakti zamanında Bizans Ordusu bir şehri kuşatır. Ancak şehrin etrafında vadiler ve dağlar olduğu için ordu parça parça birlikler halinde kuşatmıştır şehri. Birlikler birbirinden uzakta oldukları için aralarındaki haberleşmeyi ulaklar sağlamaktadır. Ancak ordunun asker sayısı oldukça sınırlı, savunmadaki şehir halkı da oldukça dişlidir. Ayrıca birliklerin başındaki generaller içinde (komutan da bunlara dahil) hainlerin bulunma ihtimali vardır. Kale ancak ordu dört bir yandan topluca birlikte hareket ederse alınabilecektir. Aksi takdirde, birliklerin bir kısmı hücum eder diğerleri hücuma katılmazsa saldıranların telef olacağı kuşatma, Bizans ordusunun hezimetiyle sona erecektir.

Komutan ve birliklerin başındaki generallerin birbiri ile anlaşması ve "saat 10:00'da hücum" ya da "geri çekil" emrini ortak bir şekilde gerçekleştirmeleri nasıl sağlanabilir? Yani birbirine güvenmeyen (içlerinde hain ya da hatalı sinyaller verebilecek) parçaların ortak hareket etmesi nasıl sağlanır? Nasıl bir "Mutabakat Mekanizması" olmalı ki aralarında beraberce hareket edebilirler? İşte Bizans Generalleri Problemi bu.



[76] https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/

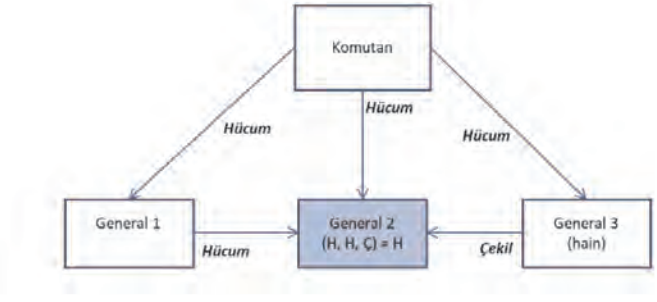
Bu problemi çözmek için oluşturulan sistemin adı ise Bizans Hata Tolerans Sistemi. Bütün hava ulaşım araçlarının motorlarında ve nükleer santrallerde kullanılıyor. Bu sistem, belli bir alana dağılmış ve birbirlerine sinyaller gönderen değişik parçaların gelen çelişkili sinyaller karşısında nasıl doğru hareket etmeleri gerektiğini belirliyor.

Sistem aşağıdaki kurallara bağlı olarak çalışıyor:

1. Oyuncuların en az 2/3'ü doğru çalışıyor olmalı (yalan söylemez);
2. Her bir parça kendisine gelen mesajlar içinde çoğunluğun gönderdiği mesajı uygular;
3. Sistem oyuncuların çoğunluğunun ilerlediği şekilde ilerler. (Burada önemli olan "doğru" bir sonuç çıkması değil "tutarlı bir" sonuç çıkması, ortada bir kararsızlık kalmaması)

Örneğimizden devam edelim:

Öncelikle şu basit duruma bakalım: Bir komutan ve üç general var. Ve bu generallerden biri hain (ya da hatalı bilgi veriyor). Bu durumda komutanın hücum emri vermesi durumunda nasıl bir sonuç çıkıyor aşağıda görelim:

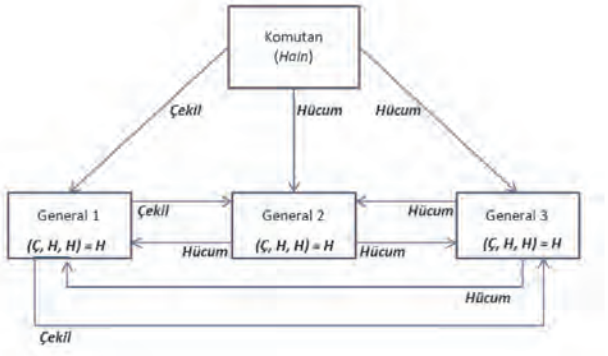


İkinci General gözünden gelen mesajlar: Ne yapmalı generalimiz?

İki numaralı generalin perspektifinden bakalım: Kendisine üç mesaj geliyor. Bunlardan ikisi "hücum", biri "çekil" şeklinde. Bu durumda general, "hücum" emrini uygular, çünkü kendisine gelen hücum emirleri daha fazla.

Bir numaralı general de aynı şekilde hareket eder. Üç numaralı hain general "çekil" emri gereği dursa bile sonuçta iki general (yani çoğunluk) "hücum" emrini verdiği için sistem hücum eder.

Peki ya kumandan hainse? Ve generallere farklı mesajlar yolluyor ise? Bu durumda olaylar şu şekilde gelişir:



Komutan hain ise, generaller ne yaparlar?

Komutan bir emir veriyor, bu emir tüm generallere dağıtılıyor. Generaller de bu emri birbirileri ile paylaşıyorlar. Bu durumda her bir generale iki "hücum" ve bir "çekil" mesajı gelecek. Bu durumda da generaller "hücum" emrini uygulayacaklar.

Konunun teknik açıklaması oldukça uzun ve matematiksel olarak incelemek isterseniz şu harika makaleye[77] göz atabilirsiniz.

Özetle, Blockchain bazlı sistemler genel olarak yukarıda bahsedilen Bizans Hata Tolerans sistemine bağlı "Mutabakat Mekanizması" kullanarak kendi aralarında uzlaşma sağlıyorlar. Tabii yukarıdaki sistemin Blockchain'e uygulanması sırasında pek çok farklı işlem (örneğin Proof-of-Work) söz konusu.

[77] https://marknelson.us/posts/2007/07/23/byzantine.html

BLOCKCHAIN nasıl *uzlaşır?*

Blockchain üzerindeki bağımsız ama birbiri ile konuşan parçaların emir aldıkları bir merkez yok. Peki nasıl oluyor da ortak hareket edebiliyorlar? Geçen bölümde temeline bakmıştık, şimdi Blockchain özelinde nasıl oluyor ona bakalım…



Önceki bölümü kısaca özetlersek: Bizans Hata Tolerans diye adlandırılan bir sistemi kullanan oyuncular, kendilerine gelen mesajların içinde çoğunluğun söylediği mesajı uygulayarak ilerliyorlar, böylece ortada kararsızlık söz konusu olmuyor.

Geçtiğimiz bölümün başlangıcında akla takılabilecek birkaç soru sormuştuk:

• Peki bu makineler merkezi bir otorite olmadan nasıl hep birlikte aynı anda aynı kararı veriyorlar? Aralarında hiç sorun çıkmıyor mu? Eğer çıkıyorsa bu sorunları nasıl çözüp tekrar aynı yolda ilerliyorlar? Birileri sistemi manipüle etmek isterse ne olacak? Olamaz mı? Olur tabii ki…

Bu sorulardan yalnızca ilkine cevap verdik geçtiğimiz bölümde. Şimdi diğer soruların cevaplarını anlamak için bu sistem Blockchain'e nasıl uyarlanmış ona bakalım:

Blockchain nasıl çözüm bulmuş bu sorulara?

Bitcoin'in de içinde bulunduğu Blockchain bazlı sistemlerde de aynı şekilde, makinelerin doğru mesajı verdiğini, arada bir hainin yanlış bilgiyi etrafa verip vermediğini nasıl anlayabiliriz?

Kısa hatırlatma: Blockchain nasıl çalışıyordu?

Efendim bunu anlayabilmek için öncelikle Bitcoin şifrelemesi ile ilgili bölümü hatırlamakta fayda var.

Kısaca tekrar etmek gerekirse: Bitcoin ile yapılmış işlemleri sistemdeki bütün makineler bir araya toplayıp kendi defterlerine yazıyorlar. Sonra da bu işlemleri toplayıp balya haline getiriyorlar (yani madencilik "mining" yapıyorlar)

Peki nasıl bir işlem yapıyordu bu makineler? Hatırlarsanız bahsetmiştik daha önce: Yaptıkları aslında önce üç bilgiyi bir araya getirmek;

1. En son yapılmış balyanın sonucunu al,
2. Sonra son on dakikada yapılmış bütün işlemleri ekle
3. Bir de eğer sonucu kazanırsan kendine bir ödül olacak (hani şu 50 Bitcoin ile başlayan ve şimdilerde 12,5 Bitcoin'e düşmüş olan), o ödülü de yaratılmış gibi ekle.

Sonra bu üç bilgiyi kullanarak sistemin sorduğu bulmacayı çözmeye çalışmak. Bu yaklaşık on dakika süren bir çalışma (Nasıl bir bulmaca bu derseniz detaylarını bu kısmın başında bahsettiğimiz bölümümüzde bulabilirsiniz).

Binlerce makine soruyu çözmeye çalışır ve bunun için de ciddi bir enerji harcar. Çözen makine anında bulmaca sonucunu tüm sisteme yayar. Bilgiyi alan diğer makineler de yukarıdaki üç bilgiyi bir araya getirip sonucu kontrol ederler (bulmacayı çözmek zor ama çözülmüş sonucu kontrol etmek çok basit).

Kontrolün sonunda sonucun doğruluğuna emin oldukları anda sistemdeki bütün makineler bu kazananın sonucunu alıp, yeni balyaya başlar ve yukarıdaki işlemleri tekrar edip yeni bulmacayı çözmeye girişirler. Çoğunluğun üzerinde çalıştığı balya en uzun balya olarak takip edilen zincir olur.

Blockchain üzerinde uzlaşma nasıl oluyor?

İşte bu makinelerin Mutabakat Mekanizması. Bizans Hata Toleransı'nın Blockchain'e uyarlanmış hali. Blockchain yukarıdaki Mutabakat Mekanizması'nı kullanarak, en son yapılan balya sonucunu kimin belirleyeceği (yani bir sonraki akında generalin kim olacağı) konusunda mutabakat sağlıyor. İşte buna Bitcoin özelinde Proof-of-Work deniyor.

Peki bu sistem çok maliyetli değil mi?

Biliyorsunuz Blockchain üzerindeki en bilinen iki sistem Bitcoin ve Ethereum halka açık. Bu şu demek: İsteyen her makine sisteme katılabilir. Ancak sisteme katılabilmek için enerji harcaman lazım. Eğer harcadığın enerji sonrası doğru işlem yaparsan çıkan sonuçtan ödül kazanmaya hakkın var.

Eğer bu makineler herhangi bir şekilde yukarıdaki gibi enerji harcayacakları bir çalışma içine girmeden ilerleme imkânına sahip olsalardı, o zaman kötü niyetli bir grup, sisteme olabildiğince makine sokup, manipüle edebilirdi. Halbuki belli bir maliyet olması ve sistemde çok fazla katılımcı olması nedeniyle bu çok maliyetli bir manipülasyon.

O nedenle "Bitcoin çok enerji harcadı, Bitcoin Sırbistan kadar enerji harcıyor, boşa israf " gibi sözler doğru, ancak işin doğasında var bu. Bitcoin sisteminin yaptığı bu kadar enerji harcayarak kendisini dış tehditlere karşı korunaklı hale getirmek. Bunu boşa bir harcama değil bir güvenlik harcaması gibi düşünün. Kurulduğu 2009 yılından bu yana bir kez bile teklemeyen ve her tür dış tehdidi bertaraf etmiş olmanın bedeli…



Başka ne olabilir?



Peki ya istisnalar olamaz mı? Olabilir. Bakalım ne olabilir ve çözümü var mı?
• Örneğin, bir bulmacayı aynı anda iki makine çözerse ne olur?
Bilgisayarlardan bahsettiğimiz için bu durum söz konusu değil. Milisaniye de olsa bir makine diğerinden önce çözer…
• İyi de bir makine diğerinden 1 milisaniye sonra çözse bulmacayı ve her iki makine de sisteme kendi sonuçlarını verseler? Sistemdeki oyunculardan bir kısmı bir makinenin sonucunu diğerleri ise diğerinin sonucunu önce aldılar (bu olabilir, sonuçta kablolar aracılığıyla dünyanın dört bir ucuna yayılan mesajlardan bahsediyoruz). Dikkat edin, sonuçlar farklı çıkacak çünkü yukarıda yazdığımız üçüncü maddedeki ödülü her iki makine de kendisi için yazdı ve o bilgiyi bulmacaya soktu. Bu durumda sistem ve makineler, en uzun balya (zincir) mantığı ile çalışıyor. İki farklı dal ürüyor ve makineler ya birini ya ötekini seçiyor. Nihayetinde makineler bu dallardan birine doğru evrilmeye başlıyorlar ve o dal ana zincir haline geliyor, diğer daldaki makineler de o dalı bırakıp çoğunluğun olduğu bu dala geliyorlar. (Bulundukları dalı "öksüz"-orphan bırakıyorlar.)
• Peki ya bir makine araya sahte bir işlem sokarsa, ona göre bulmacayı çözerse ve bunu dağıtmaya başlarsa? O zaman, yukarıdaki ikinci maddede yazdığı gibi, diğer makineler sahte işlemi aldıkları anda o işlem kendilerinde olmadığı için bu makinenin yazdığı sonucu kabul etmezler. Bu dediğimiz senaryonun tek istisnası, eğer bir gün bir grup tüm işlem gücünün %51'ini ele geçirir ve içeri bir sahte işlem sokup ondan sonra bu işlemi sistemdeki makinelerin çoğunluğuna doğrulatır ise olabilir. Bu da çok ama çok büyük bir elektrik gücü harcaması demektir ve imkânsız olmasa da çok ama çok güç bir durum.

Sonuç

"Nasıl oluyor da, kendilerine direktif veren bir yönetici olmadan birlikte hareket ediyor" dediğimiz binlerce makine, dışarıdan bakınca bilinmez ve karmaşık gelen ama içine girince matematiksel olarak planlanmış yukarıdaki sistemleri kullanarak Bitcoin örneğinde neredeyse on yıldır tıkır tıkır çalışıyorlar. Şu ana kadar bir sorun olmadı, olursa da teknoloji üzerine çalışanlar bir çözüm yolu bulurlar diye düşünmeden edemiyor insan…

UZLAŞMA mekanizmaları neler?

10 yılını kutlamakta olduğumuz Bitcoin aslında daha önce ortaya çıkmış pek çok teknolojik gelişmenin üzerine kurulmuş. Devrim niteliğindeki yeniliği ise Proof-of-Work aslında. Nedir bu, gelin detaylıca bakalım.

Geçtiğimiz bölümde Blockchain sisteminde aktif rol oynayan birbirinden bağımsız oyuncuların nasıl olup da birlikte hareket ettiklerinin üzerinden geçmiştik. Önce işin sistematiği (mantığı) nasıl çalışıyor sorusunu geçmişte ortaya çıkmış birbirine güvenmeyen Bizans Generalleri'nin düşmana karşı nasıl ortak hareket ettiğine bakmış, sonra da bu problemin Blockchain özelinde nasıl çözüldüğüne göz atmıştık.

2018 yılının Ekim ayında 10. yılını kutladığımız Bitcoin'in yaratıcısı Satoshi Nakamoto'yu bir kez daha analım ve yaptığı devrim niteliğindeki yeniliğe bir kez daha dikkat çekelim.

Satoshi Nakamoto'nun asıl başarısı ne idi?

Bilmemiz gereken kritik nokta şu: Meşhur Satoshi Nakamoto aslında üç parçayı bir araya getirdi. Bu parçalardan ikisi zaten ortada idi. Satoshi, üçüncü kritik parçayı geliştirdi ve bu üç parçanın birbirleri ile sağlam ve durdurulamaz şekilde çalışmasını sağladı. Neydi bu üç parça?

Birinci parça internet idi. Internet sayesinde birbirinde uzakta ve bağımsız makineler birbirleri ile bağlantı kurabildiler.

İkincisi ise şifreleme. Bu dağınık dünyadaki farklı parçaların birbiri ile güvenli iletişimi için şifreleme (Kriptografi) olmazsa olmaz koşuldu.



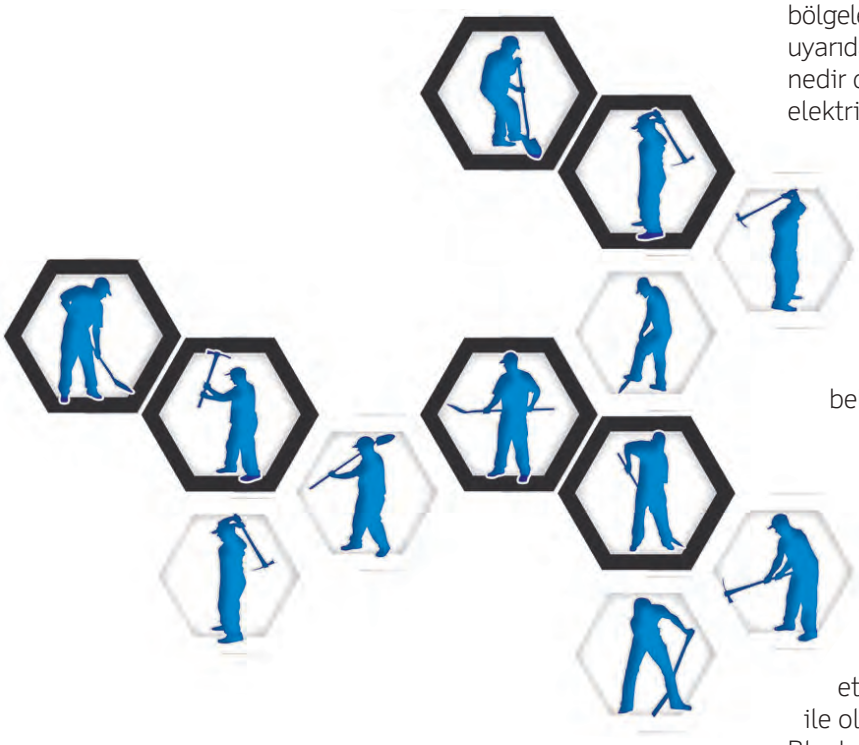
Adı Satoshi Nakamoto ama Bitcoin'i yaratan kişi bu değil!

Bu ilk iki parça yaklaşık 20–30 yıllık bir süreç içinde yavaş yavaş geliştirildi. Eksik olan bu birbirinden uzakta makinelerin ortada bir aracı olmadan nasıl birlikte çalışacağı ve bu şekilde çalışabilmek için nasıl motive edilecekleri (ve nasıl ortak karara varacaklarını) idi.

Satoshi, Bitcoin adını verdiği dijital para fikriyle, kurduğu sistemin altyapısını işletecek oyuncuların bir arada çalışmasını sağlayan bir teşvik sistemi kurdu. İşte bu daha önce yapılmamış olan bulmacadaki eksik son parça idi. İşte Bitcoin bu sorunu çözdü ve aracıya olan ihtiyacı kaldırdı. Bu sayede Satoshi, herhangi bir otoritenin uhdesinde olmadan kendi kendine çalışan, dış tehditlere karşı kendini koruyan ve on yıldır sarsılmadan ayakta duran bir dijital para yarattı. Buna Nakamoto Konsensüsü deniyor.

Bu üçüncü parçayı biraz daha açalım. Nedir ona bakalım, başka ne tip alternatifleri var onlara da bir sonraki bölümde değinelim.

Bitcoin'in meşhur ettiği Proof-of-Work ne, nasıl çalışır?



Nasıl bir uzlaşma mekanizması bu Nakamoto Konsensüsü? Bu bahsettiğimiz parçaların, o an için oluşan Blockchain zincirlerinden en uzununa doğru evrilmesi ve o zincir üzerinde mutabakat sağlanması. Bunun otomatik olması ve bir aracıya ihtiyaç duyulmaması.

Buradaki kritik nokta, makinelerin sistemin içindeyken birlikte nasıl uyumlu bir şekilde çalışacağı ve ötesinde dış tehditlere karşı kendilerini nasıl koruyacakları. Aynı zamanda makinelerin sisteme nasıl gireceğini ve sistemde iken neler yapması gerektiği. İşte bunları belirleyen kuralların en önemlisi Proof-of-Work. Tabii PoW sistemini anlatırken, bunun aslında çok enerji harcayan bir süreç olduğundan bahsetmiştik.

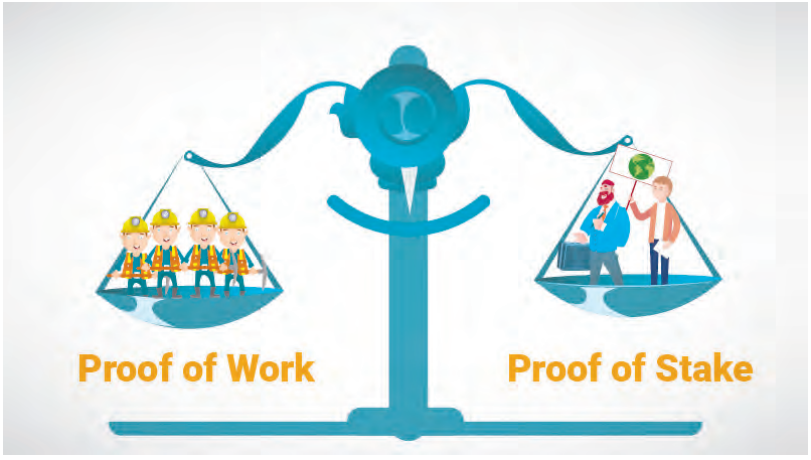
Olaylara maalesef yüzeysel olarak bakan medya, bunu "Bitcoin 159 ülkeden fazla enerji harcıyor" ya da "İzlanda finans bakanı Bitcoin'in ülkede yerleşim bölgelerindekinden fazla tüketimi olduğu konusunda uyarıda bulundu" gibi başlıklar ile veriyor. Hakikaten nedir derseniz, detay yazılar[78] var. Örneğin: Bitcoin elektrik harcaması olarak dünyada 37. sıradaki Avusturya'dan daha fazla.

Bitcoin'in sadık kullanıcıları böyle bir enerji harcamanın uzlaşma mekanizmasının işlemesi için değil ama bu işleyen mekanizmanın dışarıdan sistemi bozmak isteyecek bir tehdide karşı kendini savunma mekanizması olduğunu belirtiyorlar. Zira, uzlaşma mekanizmasının kilit noktası sistem üzerindeki parçaların %51'inin ortak bir kabul üzerinden ilerlemesi şeklinde. Nedir bu kabul? Son 10 dakikada gerçekleşen işlemlerin herkeste aynı şekilde tutulması, tutarlı ve aynı olması.

Eğer sistemin %51'ini ele geçirmek sadece etrafa makine kurmak ve sisteme bağlanmak ile olsaydı (hatırlarsanız kimseye sormadan Blockchain sistemine bağlanıp siz de bir oyuncu olabilirsiniz), o zaman elinin altında (ya da kullanabileceği) büyük bir makine kapasitesi olan biri sistemi ele geçirebilirdi. Halbuki, Bitcoin'in oyunculara sorduğu bilmeceyi çözmek için ciddi bir enerji harcamak gerekiyor. Sistemi ele geçirmek isteyen "dış tehdit" için oldukça maliyetli bir durum bu.

Bitcoin dışında aslında Bitcoin'in küçük kardeşleri diğer alternatif kripto paraların birçoğu da PoW mekanizması kullanıyor. Ethereum (ki değiştirmeyi planlıyor), Litecoin, Monero gibi bütün büyük Bitcoin alternatifleri de PoW'e dayanıyor.

[78] https://www.ofnumbers.com/2018/08/26/how-much-electricity-is-consumed-by-bitcoin-bitcoin-cash-ethereum-litecoin-and-monero/#footnote_0_5656



PoW'un en önemli rakibi olan Proof-of-Stake (PoS) nasıl çalışır?

Peki bu kadar enerji harcamaya gerek var mı? Başka yöntemlerle de makinelerin ortak hareket etmesi sağlanamaz mı? Bu konuda kafa yoranlar var tabii. Onların da geliştirdiği alternatifler var. Gelin dilerseniz bunlara kısaca göz atalım.

Proof-of-Stake, Bitcoin'in Proof-of-Work mekanizmasına en ciddi rakip.
Farkını anlatmak için PoW'nun ne yaptığını tekrar hatırlatalım. Siz eğer Bitcoin'i bozmak gibi bir çabaya girerseniz, tüm Bitcoin'in %51'ini ele geçirecek kadar yatırım ve enerji harcamadıkça yaptığınız çaba sonuçsuz kalır ve yaptığınız tüm masraf boşa gider. Zira sistemin oyuncuları, sizin istediğinizi değil çoğunluğun yolunda giderler, siz de yaptığınız masraf ile geride kalırsınız.

O zaman şöyle bir soru soruyor diğerleri: "İyi çok güzel, bu tip mekanizma kurarak dış tehditleri önlüyorsunuz ama öte yandan iyi niyetli mevcut oyuncular da aynı şekilde bulmaca çözmek zorundalar (Bitcoin kazanmak için gerekli çünkü).

Bu nedenle ortaya çok büyük bir enerji harcaması çıkıyor. Sistemi manipüle edecek birine çok maliyet getirecek ama düzgün çalışan uyumlu oyunculara masraf çıkarmayacak dolayısıyla 'büyük israflara' neden olmayacak bir çözüm bulunamaz mı?"

PoS işte bunun cevabını şu şekilde veriyor. Yapılan işlemlerin teyidi için bir bulmaca çözüp enerji harcamayalım, onun yerine doğru olduğunu düşündüğümüz işlemlerin doğruluğunu teyit için elimizdeki tüm parasal değeri rehin olarak verelim. Elimizi taşın altına koyalım yani. Sistem de bu rehin edenler içinde birine piyango ile yeni blok yaratma ayrıcalığı versin. Ne kadar çok varlık rehin edersek, o kadar çok piyango biletimizin olsun. Sonundaki ödülü kazanmadaki şansımız da o kadar artsın.

Öte yandan eğer sistemi bozmaya çalışan bir dış tehdit isek, (ve eğer çoğunluğa sahip değilsek) yaptığımız manipülasyon nihai olarak sonuçsuz kalacak ve ceza olarak sistem bizim tüm varlığımızı sıfırlayacak-sıkı bir caydırıcı. Bitcoin'in en büyük dezavantajı olarak öne çıkan yüksek enerji sarfiyatı sorununu çözen bir alternatif.

Bu konuda tartışmalar halen devam etmekte. Proof-of-Stake'i kullanacak olan Ethereum geliştiricileri konu üzerinde çalışmaya devam ediyorlar. Bunun dışında Cardano, OmiseGo, QTUM, Ardor PoS kullanıyorlar. Bir de PoS ile PoW'yi karışık şekilde kullananlar var (Decred, Dash, Stratis, HShare, Pivx gibi)

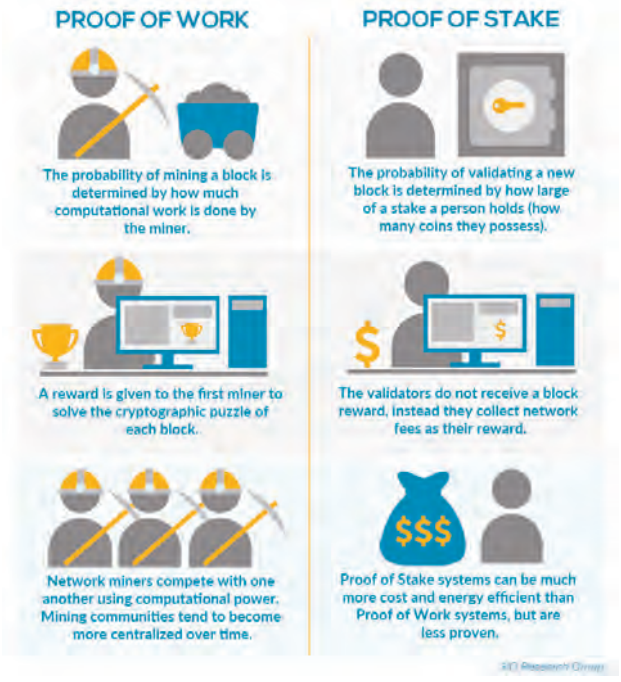


Başka ne tip alternatifleri var?

Blockchain gibi değişik bazlı parçaların birbiri ile nasıl çalışacaklarına ilişkin çalışmalar sadece PoW ve PoS ile sınırlı değil tabii. Teknoloji alanında bir sorun olduğunda onlarca çözüm ortaya çıkar. Neler onlar derseniz, sadece isimlerini ve kimlerin kullandığını belirtelim:

• Proof-of-Authority(Parity) - Ripple, Hyperledger
• Delegated-Proof-of-Stake (DPos)-BitShares, Steemit (sahipleri aynı bu ikisinin), EOS
• DeligatedByzantineFaultTolerance (DBFT)-NEO
• ProofofActivity (PoA)-Digital Note, Vechain
• ProofofCapacity (PoC)-Burstcoin
• ProofofBurn (PoB)-Slimcoin
• ProofofRun (PoR)-Runcoin
• ProofofAssignment-IOTW
• ve diğerleri: DirectedAcyclicGraphs (DAG), ProofofImportance (POI), Proof-of-Elapsed-Time (POET), Leased-Proof-of-Stake (LPos), PracticalByzantineFaultTolerance (PBFT), SimplifiedByzantineFaultTolerance (SBFT)

Bunları bilmek gerçekten önemli mi? Eğer geliştirici değilseniz çok da önemi yok aslında. PoW'un etkili bir sistem olduğu biliniyor. 10 yıldır da sağlam bir şekilde kullanılıyor. Bu alternatifler ağırlıklı olarak PoW'un enerji harcaması konusundaki sıkıntılara çözüm olsun diye çıktı. Bunun yanında farklı farklı mekanizmalar PoW'a kıyasla daha hızlı, madencilerin birden fazla Blockchain'e hizmet verebilme imkanı sağlama ya da PoW'a göre daha dağıtık bir yapıya sahip olma gibi değişik alanlarda uzmanlaşmış durumdalar. Ama bundan on yıl sonra herhalde bu konuda yeterince geliştirme yapılır ve bu konu bir nüans olarak tarihteki yerini alır.



Sonuç

Yeni teknolojiler ile ilgili hep söylediğimizi tekrar edelim. Bu tip teknolojilerin olgunlaşması zaman alıyor ama güzel tarafı, herhangi bir sistemde bir eksiklik görüldüğünde (ya da hissedildiğinde) hemen birileri onun üzerinde çalışmaya başlıyorlar. Sadece eksiklik demeyelim aynı zamanda "daha verimli, daha kolay" bir çözüm arayışı sürekli olarak mevcut. Bu da aslında bu sistemlerin gücü. Zira sürekli bir ilerleme ve gelişme var. Kırk yıldır kullanılan eski sistemlere göre ne kadar büyük bir rahatlık düşünsenize.

BLOCKCHAIN *'in* geleceği

Yurtdışında (özellikle ABD'de) çok rastlarız: İnsanlar gelecek için belli öngörülerde bulunurlar ve sonrasında da bu tahminlerinin gerçekleşip gerçekleşmediğine bakarlar. Hatalarını da göğüslerini gere gere söylerler.

Bizde ise çok görülmez bu; en uzman kişiler bile genellikle hata yapmaktan korktukları için geleceğe yönelik tahmin yapmaktan çekinirler (çoktan seçmeli eğitim sisteminin getirdiği sıkıntılar bunlar aslında - yorumdan çok bilme/ezberlemenin ön planda olduğu ve hata yapıldığında binlerce sıra geriye düşüldüğü bir sistemin çocukları olarak hepimiz böyleyiz)

Hadi gelin biz de Blockchain ile ilgili (muhtemelen bir kısmı yanlış çıkacak) birkaç öngörüde bulunalım, sonuçları gelecekte hep birlikte görürüz:

Blockchain'in geleceği nasıl görünüyor?

Basit olanlardan başlayalım: Web 3.0'ın bize yeni bir dünya getireceği artık bir tahmin bile değil, şimdiden görmeye başladığımız bir durum.

Web 3.0 nedir derseniz, ilk bölümümüze göz atabilirsiniz, ama bir cümle ile özetlersek: Dijital hayatta ekonomik, sosyal, kültürel her tür ikili ya da çoklu ilişkide aracılara olan ihtiyacı ortadan kaldıran ve gücü yeniden kullanıcılara veren teknolojiler.

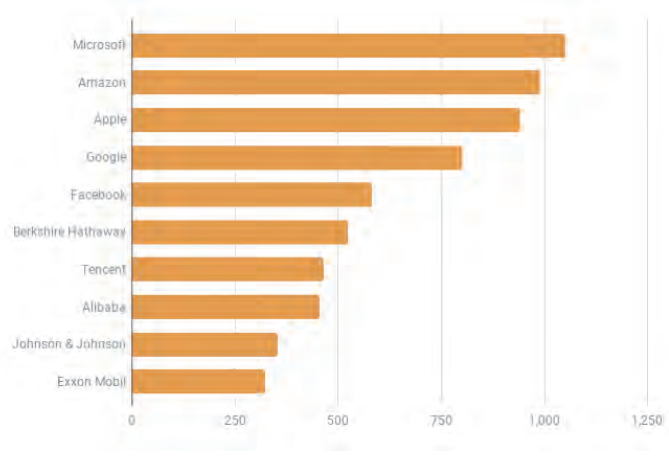
Peki bu teknolojilerin aracılar ile derdi ne?

Aracılar genelde merkezi yapılar. Kullanıcılar ile ilişkilerde güç dengesi hep bu merkezi yapıların tarafında. Bu dengeye karşı çıkan kullanıcı tarafındaki yeni teknolojiler ise adem-i merkeziyetsiz yani gücü kullanıcı da dahil dış oyuncular ile paylaşıyorlar.

Aracılar kullanıcılarının bilgilerini korumada yetersiz kaldıkları ya da parasal faydayı daha ön planda tuttukları için kullanıcı tepkisi çekiyorlar; yeni teknolojiler kullanıcı mahremiyetine daha önem veriyor.

Aracılar merkezi yapılar olarak zamanla genişliyor ve hantal yapılar haline geliyorlar. Bu da maliyetlerini artırıyor. Bir taraftan da bu yapıların hemen hemen tümü halka açık olduğu için her üç ayda bir borsaya kâr bildirmek, üstelik her seferinde bu kârı ciddi miktarda artırmak zorundalar. Dolayısıyla verdikleri hizmet için kullanıcılardan daha çok para isterken yeni teknolojiler daha ucuz ya da ücretsiz.

Web 2.0 bize pek çok yeni şirket ve iş modeli getirdi. 20 yıl önce ortada olmayan şirketler bugün dünyanın en büyüğü oldular. Bakın listeye, piyasa değeri en yüksek on şirketin yedisi teknoloji şirketi ve bunların beşi Web 2.0 sonrası doğdular (Apple biraz daha eski ama esasında onun büyümesi de Web 2.0 sayesinde)



Dünyanın en büyük 10 şirketi - Temmuz 2019 (Milyar ABD Doları)

Yeni girişimlerin uğraş alanı ne olacak?

Bu alanda çalışan binlerce girişim var. Hangisi başarılı olacak şu noktada bilmeye ihtimal yok tabii. Peki bu şirketler ne ile uğraşıyor olacaklar?

Öncelikle güven ihtiyacını minimuma indirmekle meşgul olacaklar. Neden? Son kullanıcının güven ihtiyacını karşılayarak ondan komisyon tırtıklayan her türlü aracıyı yukarıda saydığımız araçlar ile alt edebilmek için.

Bunu yapabilmek için, önlerinde aşmaları gereken uzun ve zahmetli bir yol var. Çünkü karşılarındaki aracıların maddi imkanları çok geniş. Bu gücü kullanarak en iyi yazılımcıları tutup en gelişmiş programları yazdırabilirler. Üstelik bunların bir çoğu müşterilerini çok iyi dinliyorlar, onların taleplerine hızlı cevap veriyorlar.

İşte bu nedenle yeni girişimlerin ucuz oldukları kadar pratik de olmaları gerekiyor. Merkezi olmayan bir yapı oluşturmak başlı başına karmaşık bir işlem. Girişimler şimdiye kadar bu altyapıyı geliştirmek için çaba sarfettiler. Ancak çıkan ürünler ya da hizmetler son kullanıcı açısından oldukça karmaşık; anlaması ve kullanması zor. Bundan sonrasında hem fonksiyon hem de kullanıcı arayüzü anlamında kullanıcı rahatlığına dönük çaba göstermeleri gerekiyor yeni teknoloji girişimlerinin.

Ya "bedava" hizmet veren merkezi aracılar?

Aslında bu mevcut devlerin birçoğu müşteriden para da istemiyor hizmetlerini sunmak için. Bedava her şey! Gerçekten öyle mi? Değil tabii. Evet belki para istenmiyor ama bu çağın artık çok daha önemli geçerli akçesi haline gelen bilgi (hem de kişisel mahrem bilgiler) karşılığında veriliyor bu hizmetler.

İşte son kullanıcılar bu alanda haklarını ve sahibi oldukları bilgileri paylaşmak konusunda ne kadar farkındalık geliştirecekler bunu hep birlikte göreceğiz. Çıkan skandallar hiç kuşkusuz farkındalığı artırıyor ama ne kadar büyük bir kitlenin umurunda bu durum onu bilmiyoruz.

Dolayısıyla eğer girişimler ücretsiz devler ile yarışıyorlar ise, o zaman sadece ekonomik, kullanışlı ve bilginin korunduğu bir hizmet vermek başarı için yeterli olmayabilir. Bunun yanında biraz da gelişen olaylar sonucu son kullanıcıların davranışlarının değişmesi ve gelişmesi için duacı olmak zorundalar. Önümüzdeki dönemde mahremiyet en tartışılan konulardan biri olmaya devam edecek.

Kullanım kolaylığı ile kişisel bilginin paylaşımı savaşını bakalım kim kazanacak?

Hâlâ çoğu aracı bedel istiyor ama...

Yine de pek çok alanda aracılar hâlâ çok güçlü ve kullanıcılardan ciddi rakamlar talep ediyorlar. Aracının olacağı her alanda yeni girişimler mevcut oyunculara gittikçe daha artan bir şekilde rakip olacaklar.

Peki kısa vadede neler bekleniyor?

Öncelikle kısa vadeli olarak baktığımızda, Blockchain dünyasında önümüzdeki aylar ve birkaç yıl boyunca en çok tartışılacak konular şunlar görünüyor:

Yönetim şekli (governance):
Bir Blockchain'in mevcut ve gelecekteki işleyişi üzerindeki karar yetkisinin kimler tarafından hangi durumlarda kullanılacağı konusunda hâlâ çok net değil.

Her bir Blockchain farklı bir yönetim prensibi benimsiyor; açıkçası hangi yönetim biçiminin öne çıkacağına ileride yaşayacağımız olaylar ışık tutacak.

Değişik durum ve gelişen olaylara oyuncuların vereceği tepkiler en kullanışlı yönetim modellerini ortaya çıkaracak.

Tek bir modelden çok birden fazla kullanışlı model olacak - sektör, ihtiyaçlar, oyuncuların beklentileri, Blockchain sisteminin olgunluğu gibi pek çok etkeni göz önüne alan farklı durumlar uygun farklı modeller göreceğiz.

Finansman modellerinde değişim

2017 ve kısmen 2018'de yaşanan Token çıkarıp yatırımcılardan direkt para toplama modeli (ICO) 2019'a geldiğimizde artık eski hızında değil. Bunun yerine kripto para borsaları ile birebir anlaşarak bu borsaların müşterilerine direkt satış yöntemi yaygınlaşıyor. Merkezi olmamak ile övünen Blockchain ruhu ile çelişen bu yöntem daha ne kadar sürdürülebilir önümüzdeki aylarda göreceğiz.

Kripto alanında uzmanlaşmış fonlar aracılığı ile halka açılma öncesi finansman modeli de 2017-2018 öncesine göre evrim geçiriyor. O yıllarda (tıpkı internet balonunun patladığı 2000'ler öncesinde olduğu gibi) önüne gelen girişime neredeyse gördüğünde cebine para sokacakmış gibi kolayca para veren fonlar kalmadı artık. Bunun yerine, seçici davranan ama inandığı girişime çok büyük meblağlı çekler kesen fonlar var artık.

Bu fonlar sadece şirkete yatırımla da kalmıyorlar, bunun yanında ekosistemi geliştirici madencilik ya da yatırım yaptığı ekosisteme destek olacak daha küçük girişimlere yatırım gibi yan alanlara da kaymış durumdalar. Fonlar aktif yatırımcılık yapmaya devam edecekler.

Çeşitlenen özel Blockchain girişimleri

Geçtiğimiz yıl içinde özel/kapalı (private) Blockchain alanında yapılan denemelerde sınırlı başarı elde edildi. Tasarruf odaklı elde edilen kazanımlar yapılan zahmete henüz değmiyor.

Bu da iş çevrelerinde Blockchain ile ilgili genel heyecanı biraz söndürmüş görünüyor.

Bir yandan da sessiz ama derinden devam eden pek çok proje var. IBM bu konuda desteklediği Hyperledger teknolojisi ile hem kendi iç yatırımına hem de ekosistemi geliştirici hamlelerine devam ediyor. Bunu yaparken de potansiyel olduğunu düşündükleri sektörlerde lider şirketler ile işbirliğinde tam gaz ilerliyorlar. Kısa vadede çok büyük bir başarı beklentisi yok, uzun vadeli olarak potansiyel ne kadar gerçek olacak onu da bekleyip göreceğiz.

İşbirliği / karşılıklı çalışılabilirlik (interoperability)

Önümüzdeki dönemin en önemli konularından biri Blockchain'lerin karşılıklı olarak birbirleri ile iletişimde olmaları olacak. Şu an her bir Blockchain kendi dünyası içinde doğuyor ve büyümeye çalışıyor. Bir noktaya kadar bu şekilde belli bir gelişim gösterebilirsiniz. Ancak daha fazla büyüme ve kullanıcı adaptasyonu için mutlaka daha geniş bir alanda oynamalı ve diğer Blockchain'ler ile bilgi alışverişi sağlamalısınız. İşte bu konuda interoperability denen karşılıklı işbirliğini artırıcı altyapı çalışmaları da tam gaz devam ediyor. Gelin dilerseniz bu son maddeye biraz daha detaylı bakalım:

Blockchain'ler birbirleri ile konuşur mu?

Burada ve benzer pek çok yazıda Blockchain üzerine değişik girişimleri okuyoruz. Ancak dikkat ettiniz mi bilmiyorum, bu tip girişimlerin her biri genelde ayrı bir Blockchain kuruyorlar. Ve birbirleri ile pek bir bağlantıları yok. Zaten kullanıcıları çok sınırlı, hatta pek çoğunun sıfıra yakın. Yani bir okyanus üzerine kurulmuş ıssız adalar gibiler. Bu ne kadar sağlıklı?



Blockchain'leri bağlamak ne demek?

Peki bunları neden birleştirmek isteyelim, ya da istesinler? Belli başlı birkaç neden var. Bunlardan en önemlisi kullanıcı sayısını çoğaltmak tabii ki. Blockchain'lerin birbirleri ile bağlantıları olması, kullanıcılara pratik pek çok fayda getiriyor, bu da karşılığında kullanıcı adaptasyonunu artırıyor.

Şu anda kullanılan başka alternatifler var mı?

Tam olarak bire bir olmasa da birçok girişim kendi Blockchain'ini kurmak yerine mevcut bir Blockchain altyapısını kullanıyor. Örneğin önceki bir bölümde bahsettiğimiz CryptoKitties[79] yani Kripto Kedicikler aslında Ethereum üzerine kurulmuş bir oyun.

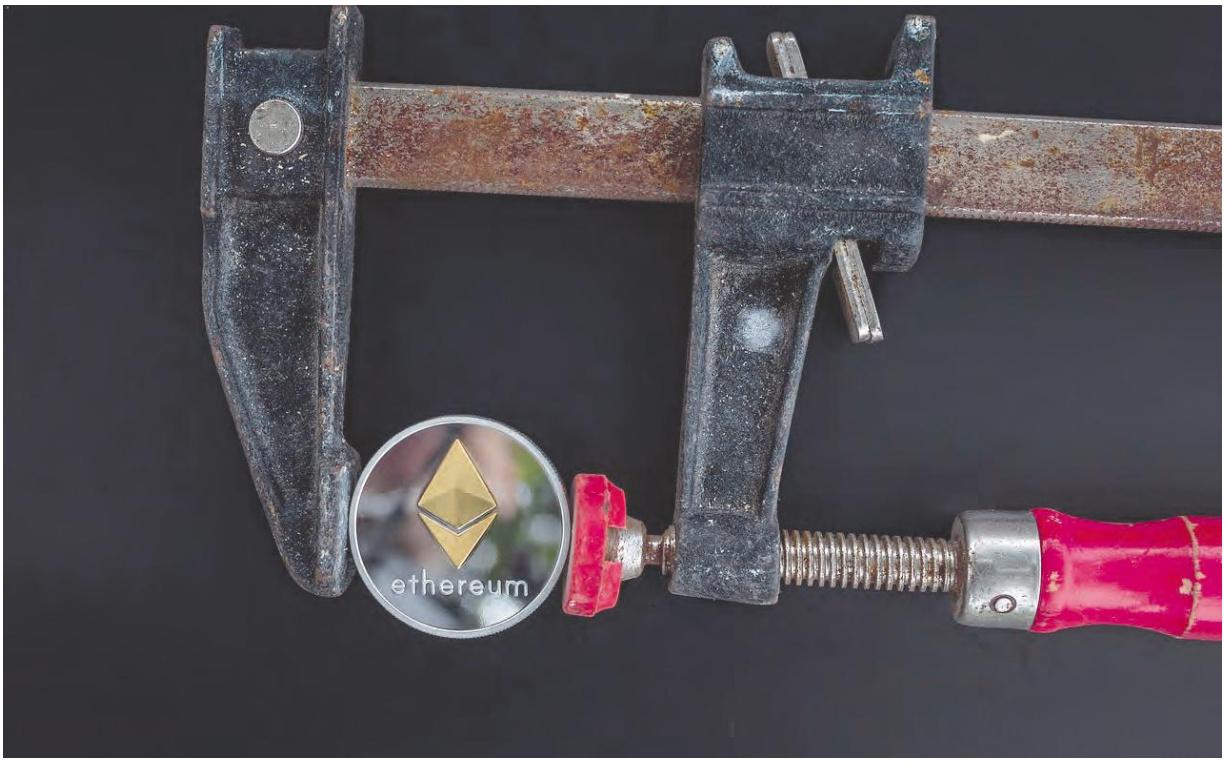
[79] https://www.cryptokitties.co/

Ethereum, değişik alanlarda kullanılabilecek (para dışında) bir altyapı oluşturduğu ve özellikle de Akıllı Kontratlar konusunda üstüne kurulan uygulamalara esneklik getirdiği için bu alanda en rağbet gören Blockchain.

Peki neden Ethereum üzerine dApps yazarsın, ne zaman kendi Blockchain'ini kurarsın?

Ethereum üzerine uygulama yazmanın hayatı kolaylaştırdığı kesin. Bir kere geniş bir ekosistemin içine giriyorsunuz. Yazılımcı bulmanız kolay, kullanıcılara ulaşmak kolay. Strateji derslerinde sık sık söz edilen Küme Etkisi (Cluster Effect) durumu var burada, bir nevi - bütün kuyumcuların bir çarşıda toplanması gibi...

Örneğin geçtiğimiz yazılardan birinde bahsettiğimiz DeFi hareketi, bu şekilde Ethereum üzerine kurulu finans alanında çalışan girişimlerin birbilerini kullanmasına dayanıyor.



Biraz daha açalım. Bu alanın aslında birbirine rakip gibi görünen iki girişimi var: Dharma[80] ve MakerDAO[81]

.

Her ikisi de kişilere kredi hizmeti sağlıyor. Dharma bu hizmeti verirken MakerDAO'nun yarattığı DAI parasını kullanıyor örneğin. Nasıl yapabiliyor bunu? Temelinde her iki uygulamanın da Ethereum üzerinde olması var. Bir kullanıcı Dharma protokolünde MakerDAO'nun parasını kullanıp ETH (Ethereum'un parası) borçlanabiliyor. Sonra da bu ETH ile gidip kendisine CryptoKitty alabiliyor.

Öte yandan Ethereum gibi bir Blockchain üzerine uygulama yazdığınızda normal olarak pek çok alanda özgürlüğünüzden feragat ediyorsunuz. Altyapınızın gelişiminde Ethereum'un hızına uyum sağlamak zorundasınız. Onun getirdiği yazılım dilleri içinde gelişim yapmalısınız.

Onun güvenlik protokollerini kullanmak zorundasınız. Kendinize ait gelişimini ve işleyişini yönetebileceğiniz bir Blockchain olmuyor- Ethereum'a bağlısınız. Ve yine aynı şekilde iletişimde olup birlikte hareket edebileceğiniz girişimlerin de yine Ethereum altyapısını kullanması gerekiyor. Bir başka altyapıyı (örneğin Tezos ya da Stellar) kullanan bir Blockchain ile iletişiminiz kapalı.

Başka bir yol yok mu?

Peki o zaman bir orta yol bulunamaz mı? Hem her türlü hakkına sahip olduğum bir Blockchain'im olsun, hem de diğer Blockchain'ler ile rahatça iletişimde olayım? İşte son birkaç yıldır perde arkasında çalışmasını sürdüren ve bu günlerde görücüye çıkan Interoperatibility konusuna geldi sıra.

[80] https://www.dharma.io/
[81] https://makerdao.com/en/

Interoperability ne demek?

Interoperability Ethereum'un yaptığını bir parça daha genişleten bir kavram aslında. Nasıl Ethereum, kendi üzerine kurulan girişimler (dApps) arasında iletişim sağlıyor ancak başka silolara iletişim konusunda sıkıntı yaşatıyor ise, Interoperability sağlayan girişimler aslında bir nevi bunu da aşacak bir çözüm bulmaya çalışıyorlar. Yani, Ethereum üzerine kurulu bir girişimin, başka bir siloda kurulu (örneğin Tezos) başka bir girişim ile iletişimde olmasını sağlıyor. Ya da bir sistemi kullanan bir kullanıcının başka bir sisteme de angaje olabilmesine olanak veriyorlar.

Bireysel kullanıcılar için ne ifade ediyor bu?

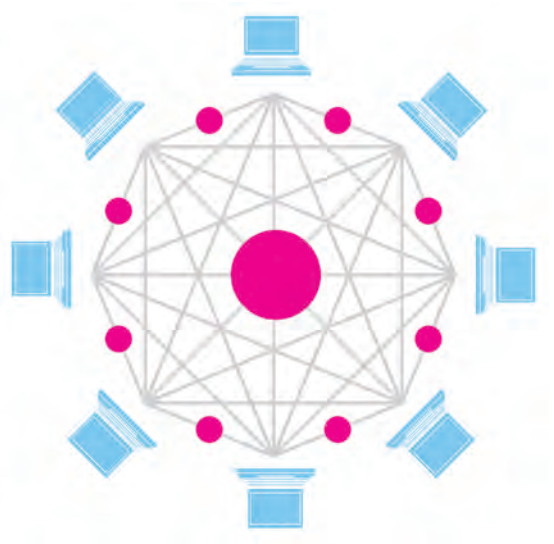
En basit ifadesiyle kullanıcı rahatlığı. Projeler arasında bilgi paylaşımı olması, kullanıcıların kendilerine ait bilgilerinin (kullanıcının izin verdiği kadarının) değişik projelerde kullanılabilmesi anlamına geliyor. Bunu sadece bilginin paylaşılması anlamında değil aynı zamanda bir teyid fonksiyonu olarak da düşünün. 18 yaşından büyük olduğunuz, finansal olarak kabul edilebilir durumda olduğunuz gibi pek çok özelliğiniz ile ilgili detay bilgiyi ayrı ayrı projelere tekrar tekrar vermek yerine, bir projeden alacağınız "yeterlilik belgesini" içeriğindeki detayları paylaşmadan diğer projelerde kullanabilmek gibi.

Bunun yanında Interoperability bir Blockchain içinde yarattığınız bir varlığın bir başka Blockchain içinde de değeri olması demek. Bir Blockchain için kullanılan bir parayı alıp kripto para borsasında satmak ve sonra başka bir Blockchain üzerindeki parayı almak yerine sistemler arasında hızlıca geçiş yapmak anlamına geliyor bu. Bunu yaparken de daha önce de bahsettiğimiz Akıllı Kontratlar kullanılıyor.

Girişimler için ne ifade ediyor?

Girişimciler için temel avantajı bir ekosistemde olmanın getirdiği rahatlık. En önemlilerinden biri, bir Blockhain kurduğunuzda bu Blockchain'in güvenliğini uzlaşma mekanizmalarını da kullanarak bağımsız teyid ediciler ile sağlıyorsunuz (Bitcoin sistemindeki madenciler gibi) Bu teyid edici makinelerin sizin sisteminizde olması ve sisteminizin güvenliğini sağlamaları için onlara bir ödül vermeniz gerek. Ayrıca sizin gibi başka pek çok proje de bu makinelerin peşinde. Interoperability içinde yer alırsanız (örneğin Polkadot) makine bulmak için uğraşmıyor ve ortada bulunan bir havuzdan dilediğiniz gibi yararlanıyorsunuz (ücreti mukabilinde).

Tabii burada şuna da bakmak lazım. Kimi girişimciler için projenin güvenliği hayati önem taşırken, kimileri için o kadar da önemli olmayabiliyor. Normalde bir Bitcoin benzeri değer taşıma üzerine kurulu bir kripto paradan bahsediyor olsak, sistemin güvenliğinin tehlikeye girmesi o kripto paranın değerini sıfıra indirebilir. Dolayısıyla bu kripto paranın geliştiricileri güvenlik için her tür fedakarlığı yapabilir.



Bir de CryptoKitty'leri düşünün. Yani güvenlik iyi güzel de tek özelliği değer taşımak olan bir kripto para kadar değil. Ama baktığınızda CryptoKitty'ler de Ethereum ağı üzerinde bu bahsettiğimiz diğer kripto para da.

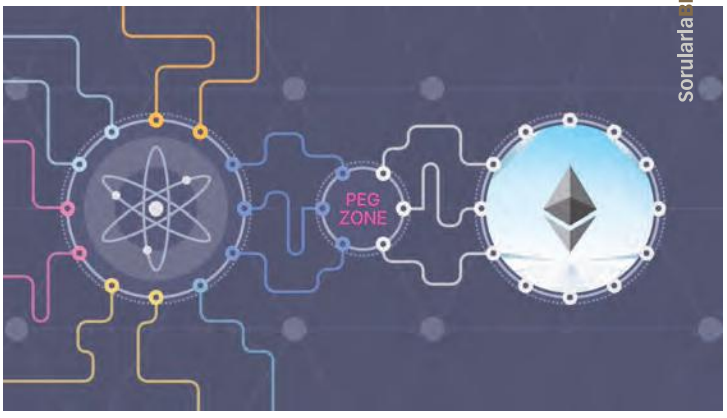
Ethereum kendisini süper güvenli yapmak zorunda ve bundan dolayı ciddi bir maliyeti var. CryptoKitty sırf Ethereum ağında olduğu için aslında gereksiz yere fazladan bu masrafa katlanmak zorunda.

Halbuki Interoperability sağlayan bir ağ üzerinde olsa bu alanda güvenlik için gerektiği kadar kullanıp çok daha ekonomik bir şekilde sürecini yönetebilir.

Interoperability alanında çalışan ve ilerleme sağlamış iki tane girişim bulunmakta. Polkadot[82] ve Cosmos Network[83]. Önümüzdeki yıllarda her iki projeyi de sık sık duyacağız.







Sonuç

Blockchain alanı önümüzdeki yıllarda hem kapalı hem de açık Blockchain'lerde heyecan verici gelişmelere gebe. Girişimler mevcut Web 2.0 devlerini alt edebilecekler mi bunu merakla bekliyor olacağız. Ama kesin olan şu: Yarış artık olması gerektiği gibi son kullanıcıyı memnun etmeye döndü ve bu dönüşümden en kârlı biz son kullanıcılar çıkacağız.

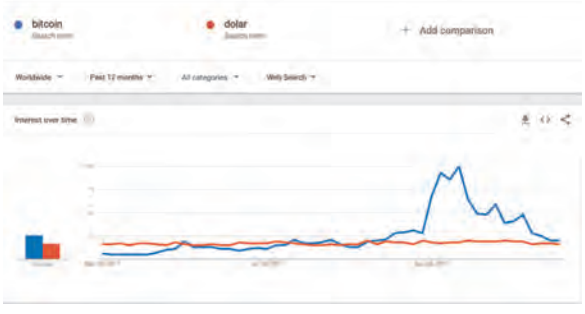
[82] https://polkadot.network/
[83] https://cosmos.network/

Bitcoin



Bitcoin NE *tam* olarak?

Blockchain ile ilgili bir parça okuduysanız, Blockchain teknolojisi üzerine kurulan onlarca hatta yüzlerce kripto para olduğunu göreceksiniz. Ancak herkesin dilinde Bitcoin var.



Baksanıza geçtiğimiz yıl "enflasyon" kelimesinden daha fazla aranmış Google Türkiye'de. (Ama tabii herkes ne olduğunu bildiği için olabilir, örneğin "küresel ısınma" da hiç aranmamış, herkes tehlikenin farkında belli ki.)

Aslında bu normal. Çünkü Bitcoin diğerlerinden farklı-bir nevi bu işin Altın Standardı, tabiri caiz ise 'ağır abisi'. Neden? Anlatalım.

Bitcoin'in kritik püf noktası ne? İpucu: "Uzlaşma Mekanizması"

Geçmiş bölümlerden de hatırlayacağınız gibi, kripto (şifreleme) teknolojisi 1970'lerden beri süregelen araştırmalar sayesinde hatırı sayılır bir olgunluğa erişmişti.

Sonrasında 2008 yılında Satoshi Nakamoto denen kişi(ler), bu kripto teknolojisini kullanarak dünyanın farklı yerlerinde bulunan (adem-i merkezi yapıdaki) makineleri kendi aralarında olabilecek "güven" sorununu en aza indirecek bir "uzlaşma (mutabakat) mekanizması" aracılığıyla birleştirdi. Bu da, merkezi yapıya olan ihtiyacı ortadan kaldıran bir devrim yarattı.

Bu mutabakat mekanizması dünyanın dört bir yanına dağılmış birbirini tanımayan makineler tarafından yapılıyordu. Neden? Çünkü, farklı yerlerde olan makineleri fiziksel olarak kontrol altına almak imkânsız.

Yine hatırlarsak, "uzlaşma mekanizması", taraflar arasında yapılan işlemlerinin makineler tarafından onaylanması idi. Bu basitçe şöyle gerçekleşiyor: İki taraf arasında yapılan işlem, bir makine tarafından "kayda geçiriliyor" ve anında diğer makinelere haber gönderiliyor. Bu şekilde, yapılan bütün işlemler yaklaşık 10 dakikada bir toplanıp tek bir paket haline getiriliyor. Makineler bu paketin doğru olduğunda anlaşırsa, tekrar çalışmaya ve yeni, bir sonraki paketi oluşturmaya başlıyorlar.

Makineler arasında uyumsuzluk genelde olmuyor yani birbirleri ile anlaşıyorlar (istisnalar olabiliyor, sonraki bölümlerde bahsedeceğiz, şimdilik kafamızı karıştırmayalım). Olması durumunda ise çoğunluğun kabul ettiği sonuç ile ilerliyor sistem. Yani makinelerin %51'i ne isterse o oluyor. Peki, dünyanın dört bir yanına dağılmış makineler neden bu sisteme bağlansınlar?

Sonuçta makineler elektrik ile çalışıyor. Karşılığı olmadan gönüllü yapılan hareketler ancak insanlar tarafından, o da ya kişisel gönüllülük ya da ideolojik amaç uğruna yapılıyor.

Üstelik bir sorun daha var. Diyelim makineleri topladık ve bir ağ kurduk. Makineler bu ağa güçleri kadar katkı yapıyorlar. Ya birisi çok güçlü bir makine geliştirir, ya da binlerce makinelik bir ağ kurar ve bu sistemin %51'ini ele geçirirse?
Makinelere "mutabakat mekanizması"nı çalıştırmaları için bir ödül vermek lazım yoksa çalışmayı bırakırlar, bu da bir kişi ya da gücün sistemin %51'ini ele geçirmesine neden olabilir.

Artık şu Bitcoin'e gelsek mi?

İşte geldik Bitcoin'e! Efendim, Blockchain sisteminde yükü çeken makinelerin bu yaptıkları işlemleri kayıt etme, daha sonra da teyit etme işlemi sonucu aldıkları ödüle (ya da lotarya) Bitcoin deniyor.

Neden lotarya deniyor? Zira, bu on dakikada bir yapılan teyit işlemi aslında çok zor bir bulmaca. Bir nevi Sudoku oyunu gibi düşünün. Sistem bu soruyu soruyor, binlerce makine de bu bulmacayı çözmeye çalışıyor. Bulmacanın bir çözümü var-bir makine çözüyor ve sonucu diğerlerine bildiriyor. Yine aynı Sudoku'daki olduğu gibi çözmesi zor ancak başarıldığında çözümün doğru olduğu anında görünebiliyor. Yani diğer makineler çözümü görüyor, mutabık kalıyor ve yeni paket üzerinde çalışmaya başlıyor.

Şimdi diyeceksiniz neden bu kadar zor bir bulmaca var? Çünkü sistemi kuranlar, bu bulmacanın basitçe çözülmesini istemiyorlar. Makinelerin bunu çözerken ciddi bir elektrik harcaması yapmasını özellikle istiyorlar. Ki böylece, yukarıda bahsettiğimiz sistemin %51'ini ele geçirmek inanılmaz pahalı bir hale gelsin.

"Bitcoin çok enerji harcıyor" söylemlerini de duymuşsunuzdur muhakkak. Doğru-çok enerji harcıyor. Ama sistemi dışarıdan gelecek tehlikelere karşı tutmak için ödenen bir bedel bu. Şu anki Bitcoin değeri on binlerce makinenin çalışmasında kullanılan enerji maliyetini karşılamaya yetiyor. Eğer bir gün Bitcoin fiyatları düşerse makineler de çalışmayı bırakabilir ve sistem bir noktada kendi dengesini bulur.

Ha bu arada "bu 10 dakikada bir mutabakat yapma iyi de teknoloji gelişiyor, makineler artık daha güçlü" diyebilirsiniz. Onun da çözümünü bulmuşlar: eğer bir bulmaca 10 dakikadan önce çözülürse, bir sonraki bulmaca zorlaşıyor!

Bitcoin'in bir değeri var mı?

"İyi tamam da, niye Bitcoin'e bir değer atfediliyor" diye bir soru aklınızı kurcalıyor ise, aslında yukarıda elektrik harcaması ile başladığımız değer atfı konusunu "para" terimi üzerinden biraz daha açmaya çalışalım.

Paranın iki ana özelliği var esasında. Bir değer saklama aracı olması, ikincisi değiş tokuşa aracılık etmesi.

Para ya da banknot eğer buna değer atfeden ya da bu kâğıt parçası karşılığı bir hizmet veren varsa bir anlam taşır. Yoksa üzerinde dolar yazan yeşil bir banknot kâğıt parçası olarak arkasında ABD hükümeti olmadıkça bir anlam ifade etmez. Peki ya altın? Alıyor ve satıyorsunuz, yani birileri bu madene bir değer atfediyor (çıkartılması maliyetli diyorsanız, evet doğru aynen Bitcoin'de olduğu gibi)

Bitcoin, para dediğimiz mefhumun bu iki ana özelliğini de taşıyor: Değer depolama ve değişim aracı olmak. Ancak özellikle son zamanlarda, Bitcoin'e talebin çok fazla olması, dolayısıyla çok değerlenmesi nedeniyle depolama özelliği ön plana çıktı.

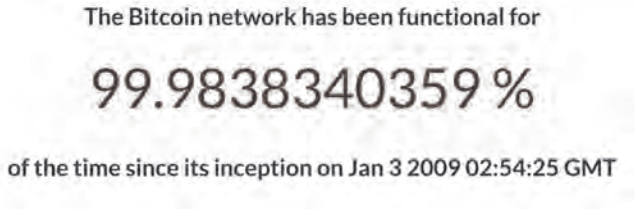
Zira insanlar fiyat yükseleceği beklentisi ile Bitcoin'i herhangi bir alım satım işlemi için kullanmayıp kenarda bekletiyorlar!

O nedenle şu anda Bitcoin'in en çok benzetilebileceği araç altın. Değişim için fazla kullanılmıyor, eskimiyor, daha çok değeri için tutuluyor. Tabii başka avantajları da var, hızlıca el değiştirebilmesi, coğrafi sınırlara bağlı olmaması gibi.

Tabii Bitcoin'in altın ve diğer resmi kâğıt paralardan önemli bir farkı var. O da Bitcoin yaratımı kısıtlı ve bir süre sonra da (tahmini 2140 yılında) bitecek. Dolayısıyla da enflasyonist değil deflasyonist bir sistem ile kurulmuş. Bu da Bitcoin'in değerinin zaman geçtikçe yükseleceği şeklinde bir düşünce yaratıyor. Doğru mu değil mi göreceğiz.

Bitcoin bu alanda ortaya çıkan ilk kripto para olduğu ve yıllarca bir kere bile üzerinde işlem yapılması sekteye uğramadığı (ya da engellenemediği) için dijitalleşen dünyada en çok kabul gören para birimi oldu. Bunun yanında arkasında merkezi bir yapı yok, hatta bir web sitesi bile yok (www.bitcoin.com Bitcoin'e değil onun klonu Bitcoin Cash'e ait, karıştırmayın), bu da tek bir gücün eline geçmesini zorlaştırıyor.

Bitcoin konusunda iyimser olanlar Bitcoin'in gelecekte dünyanın kullanacağı sınırları olmayan, tek bir hâkiminin olmadığı global bir para olacağını düşünüyor. Şimdiden yer kapma amacıyla Bitcoin'e hatırı sayılır bir değer biçiyorlar.





Bitcoin konusundaki karamsarlar ise, dünyanın şu anki hâkimi olan güçlü kuruluşların gelecekte de Bitcoin sistemini aynı şekilde kontrol edeceği görüşündeler. Sonucun ne olacağını hep birlikte göreceğiz.

Bitcoin nasıl başlamış?

Kripto paraların en eskisi, en çok kullanılanı, bir nevi şahı. Diğer bütün paralardan ayrılan birkaç özelliği var. Öncelikle, kurulmak için herhangi bir yatırım almamış. 2008 yılında çıkan kriz sonrası koca koca bankaların batması ihtimali ve devletlerin bu bankaları kurtarmak için (finansal krizi önlemek adına) milyarlarca dolar para basmasına tepki olarak bir grup şifre uzmanı (cypherpunk; cypherpunk denen bir bilimkurgu türünün kelime oyunu ile türetilmiş hali. Cyber yerine şifre anlamındaki cypher kullanılmış) tarafından geliştirilen fikrin meyvesi. Bu dev bankaların batma ihtimali onlarda "acaba paramız mevcut sistemde güvende mi?" sorusunu doğurdu.

Devletlerin finansal krizi önleme adına milyarlarca dolar karşılıksız para basması ise onlarda "mevcut düzenin koruyucusu olan devletler ne kadar sorumlu davranıyorlar?" şeklinde düşünceler ile ilk sorulan sorunun etkisini daha da derinleştirdi. Sonunda da Satoshi Nakamoto tarafından yaratılan Bitcoin ortaya çıktı.

Ancak deneysel bir ürün olan Bitcoin'in Internet üzerinden kuralsız olarak her türlü ürünü satan Silk Road sitesinde kullanıma başlaması (kredi kartı ile ödemede tüm kimlik bilgileri ifşa edilirken Bitcoin'de bir tür gizlilik olması nedeniyle) Bitcoin'e ilgiyi patlattı. Ancak Bitcoin'in (ve Satoshi'nin istediği) istediği normal olarak bu tip bir kötü şöhret değildi. 2010 yılı sonunda ABD hükümeti geçmişte yaptığı gizli işleri ortaya çıkaran Wikileaks'e halk tarafından yapılan yardımları kredi kartı sistemleri üzerinden engellemeye başladı.

Bunun üzerine Wikileaks'in Bitcoin ile bağış toplamaya başladığını açıklaması Bitcoin'e olan talebi iyice yükseltti.

Ancak Bitcoin kurucusu ve o zamana kadar anonim olan Satoshi yazdığı bir yazı ile Bitcoin'in deneysel bir ürün olduğunu henüz gerçek hayatta pratik kullanıma hazır olmadığını belirterek Wikileaks'den Bitcoin ile bağış uygulamasına son vermesini rica etti. Wikileaks'in bunu dinlememesi sonrası ise Satoshi sırra kadem bastı. Şu anda neredediir, kimdir bilen kimse yok. Pardon, bilen bir kişi vardı, o da Bitcoin üzerinden yapılan ilk para transferi ile Satoshi'den $100 alan Hal Finney , o da 2014 yılında hayata veda etti.



Satoshi'yi bildiğine emin olduğumuz tek kişi: Hal Finney

Sonrasında değişik iniş ve çıkışlar yaşayan, defalarca değeri fırlayan, sonra yarıya düşen, her yıl birkaç kere "artık öldü" denilen ama her seferinde daha da güçlü bir şekilde hayatını sürdüren, kurulduğundan beri bir dakika bile işlemleri sekteye uğramamış bir kripto para, Bitcoin hayatımıza girdi. (Bu arada "Bitcoin öldü" haberleri için istatistik bile tutuluyor; şu ana kadar 300'ü geçmiş; sırf bunu takip eden web siteleri var.[84])

[84]https://99bitcoins.com/obituary-stats/

Bitcoin paramı gerçekten nasıl?

"Nasıl para denir bu Bitcoin'e aklım almıyor" diyorsanız buyurun beraber bakalım:

Önceki bölümden kısaca özetlersek, Blockchain yeni çıkan bir altyapı, dijital varlıkların transferine yarıyor ve büyük bir devrim yaratma potansiyeli var. Bitcoin de bu dijital varlıkların sadece biri. Kripto paraların içinde en bilinen ve en kullanılır olanı.

Şimdi burada akılları en çok karıştıran soru şu: "Bitcoin'in para olduğunu nasıl iddia edersin?" Öyle ya, gözle görülmez, elle tutulmaz, arkasında herhangi bir değer yok gibi görünüyor. Nasıl olur da para denir böyle bir "şeye"? Önceki bölümlerimizde basitçe değinmeye çalıştık ama sanki bir miktar daha açmaya ihtiyaç var. Paranın ilk çıkışından başlayalım dilerseniz.

Paranın ortaya çıkışı nasıl olmuş?

İlkçağlarda insanlar alışveriş için değiş-tokuş (takas - barter) yöntemini kullanıyorlardı. Benim ineğimden aldığım bir kilo süt var, senin de bahçenden topladığın iki kilo domates. Ver domatesini al sütümü. Çok güzel ancak her gün domates yenmez ama evdeki çocuğun her gün süt içmesi lazım. Ben senden her gün domates alamam ki? Dolayısıyla takas yöntemi ikili basit alışverişlerde kullanılabilir ama büyük miktarlarda ve hayatın akışında kullanımı pratik değil.

Alışverişler için başlangıçta kullanılan değiş-tokuş yöntemi belli büyüklüklerde işe yaramamaya başlayınca insanoğlunun en içgüdüsel dürtülerinden biri yardıma koşmuş. Biriktirmek?—?özellikle güzel bulduğu ya da az olduğunu düşündüğü nesneleri… Örneğin deniz kabuklarını… Bu kabukları sadece biriktirmekle kalmamış insanlar, bunlardan kolyeler yapmaya başlamışlar. Sonrasında bu kolyeleri birbirlerine hediye etmişler. Birinde bu kolyeyi görüp çok beğenen komşusu ona sahip olabilmek için evinde bulunan yiyecekleri teklif etmiş. Sonra komşu da aldığı bu kolyeyi başka bir ihtiyacını karşılamak için başkasına teklif etmiş. Bu şekilde bir değer transferi aracı olmuş bu kabuklar ve kolyeler.

Yüzyıllar geçtikçe aracılık için kullanılan nesneler daha gelişmiş ve kullanışlı olanlardan seçilmeye başlanmış. Zamanla deniz kabuklarının yerini metaller, bakır ve metal paralar almış. Sonrasında ise altın ön plana çıkmış ve alışverişlerde kullanılan ana öğe olmuş. Ta ki devletler ortaya çıkıp önce altın karşılığı kâğıt para basıp, sonra ise karşılıksız istedikleri kadar para yaratana kadar… (Burada hemen şunu da belirtelim: Eğer hala Merkez Bankalarının altın karşılığı para bastığını düşünüyorsanız, maalesef o günler Vietnam Savaşı sırasında Nixon'un imzaladığı bir emir ile tarih oldu, artık bu basılan paraların rezerv bir karşılığı yok) …



Paranın olmazsa olmaz özellikleri neler?: Değer atfedilme ve aracılık etme

Yukarıda bahsedilen tüm bu nesnelerdeki iki ana öğe paranın esasını oluşturuyor "değer atfedilmesi" ve alışverişlere "aracılık etmesi". Bunlar paranın olmazsa olmazları.

Her para bir değil. Neler değerini artırır paranın?

Ancak tabii burada sorun şu: Hangi nesneleri bu iş için kullanacağım? Doğada her nesneden var. Bu nesnelerden bir ya da birkaçı ön plana çıkacak ama hangisi? Eğer ben diğerlerinden önce bu ön plana çıkacak nesneyi anlarsam, bunları toplarım, sonradan gelenler az bulunan ve talep gören bu nesneleri talep edince değeri yükselir.

Ne gibi özellikler bu nesnenin değerini artırır?

1. Öncelikle ihtiyaçlarım bugün farklı yarın farklı. Yazın farklı kışın farklı. Dolayısıyla elimde tuttuğum bu nesneleri sadece yarın değil önümüzdeki aylarda da kullanabilmeliyim. Hatta benim çocuklarım var onlara iyi bir gelecek sağlamalıyım; eğer aracılık yapacak bu nesneleri çocuklarıma bırakabilsem benim için daha kıymetli olurlar. Dolayısıyla ne kadar dayanırsa o kadar iyi. İşte değerli bir paranın ilk özelliği "Dayanıklı" olması
2. Tabii evde duran nesneler güzel ama eğer ben bunları taşıyıp başka yere götürebilirsem yani "yükte hafif" olursa, bunu nesnenin daha takdir gördüğü yerlerde kullanabilirim. Bu da benim için değerini artırır. Ayrıca yanımda taşıyabilirsem, gönül rahatlığıyla seyahat edebilirim. Evde bırakıp "eve gece yarısı hırsız girerse" diye uykularım kaçmaz. İşte paranın değerini artıran ikinci özellik "Taşınabilir" olması.

3. Elimde tuttuğum nesnelerin şekilleri ve içerikleri benzer hatta aynı olmalı ki el değiştirirken aynı değerden kabul görsün. O nedenle, örneğin altın pırlantaya göre alışveriş yapmak için daha kullanışlı, zira herhangi bir parçası diğerine eşit, pırlanta gibi şekli, kesimi, netliği önemli değil. Kullanışlılık demek değer demek, bunun için nesnenin "Ölçülebilir" olması değerini ciddi olarak artıran bir özellik.
4. Bu nesnelerin bana güzel gelmesi ve benim için özel olması çok da önemli değil. Önemli olan bunun değerinin başkaları tarafından da takdir ediliyor olması. Bunun için en önemlisi, bakan bir kişinin bu nesnenin gerçekten konuştuğumuz nesne olduğunu hemen anlayabilmesi yani "Doğrulanabilir" olması.
5. Herhangi bir eşyanın satıcı ile alıcı tarafından



üzerinde anlaşılan ortak bir değeri oluştuğunda, alışveriş için kullanacağım nesnenin bu değeri tamı tamına karşılayabiliyor olması lazım. Hayatta her zaman bu kadar şanslı olmayacağımız için, genellikle elimizdeki nesnenin tamamı değil sadece bir parçası bu eşyayı almak için yeterli olacak. Aksi halde elimizdeki nesneden fazla miktarda vereceğiz karşı tarafa, bir nevi nesnemizin değeri düşecek. İşte bu nedenle, nesnenin alt parçalara "Bölünebilir" olması, onun değerini artıran özelliklerden biri.
6. Gelelim paranın değerini artıran belki de en önemli ve ilk aklınıza gelen özelliğine. Eğer para olarak kullandığımız bu nesne tabiatta bolca bulunuyorsa o zaman ne olacak? Örneğin deniz kabuğunu alışverişi aracı olarak kullansak, herhalde balıkçılar zengin olurdu! Bu nedenle kullanılan nesne "Kısıtlı" olmalı ya da ünlü bir teorisyenin dediği gibi "üretilmesi ya da taklit edilmesi çok maliyetli[85]" olmalı ki değeri yüksek olsun.

[85] http://nakamotoinstitute.org/shelling-out/

Bunu biraz daha açmakta fayda var:

• Bir maden ne kadar kısıtlı olursa ya da üretmesi zor olursa o kadar değerli olur. Neden? Çünkü taklit edilemez. Taklit edilmesi zor bir nesne, kolayca gerçek olduğu anlaşılacağı için alışverişlerde "güven" içinde kullanılabilir.
• Peki bu madde çıkarması zor ya da pahalı ise niye alışverişte kullanılsın? Haklısınız içgüdüsel olarak "bu masrafa değer mi?" diye düşünüyor olabilirsiniz. Ama şunu unutmayın:
  • Bir nesne, bir alışverişte kullanılır ve bir işe yararsa (değer transferine aracılık ederse) bir değeri olur.
  • Bu nesne, ne kadar çok alışveriş işlemine tabii olursa (yani dolaşıma dahil olursa) değeri o kadar artar!
  • Çok işleme tabii olması için ise insanların güvenini kazanması, yani kullanışlı olması ve taklit edilemez olması (yani değerinin bir sonraki alışverişte düşmemesi) gerekir.
  • Yani bir nevi nesne ne kadar çok işleme tabi olursa çıkarılma masrafını karşılayıp değer yaratmaya başlar.
  • İşte bu nedenle, herhangi bir paranın değeri matematiksel olarak hesaplanırken başka varlıklarda olduğu gibi gelecekte yaratacağı nakit akımlarının toplamına değil, ne kadar sık alışverişte kullanıldığına ve bu alışverişlerde ne değerden işlem gördüğüne bakılır.

Peki Bitcoin para mı?

Şimdi de yukarıda saydığımız özellikleri Bitcoin, altın ve devlet tarafından çıkarılan banknot (ya da bu dünyadaki tanımı ile İtibari ya da Fiat) için karşılaştırmalı olarak değerlendirelim (Vijay Boyapati'nin "Bullish Case for Bitcoin[86]" makalesindeki değerlendirmesinin revize edilmiş hali): Şimdi bu üç aracı nesneye karşılaştırmalı olarak bakalım, farklar ve benzerlikler iyice ortaya çıksın:

[86] https://medium.com/@vijayb_24615/the-bullish-case-for-bitcoin-6ecc8bdecc1



Dayanıklılık

• Bu konuda altın hakikaten bir "altın standart". Bırakın yılları yüzyıllardır hiçbir eskimeye uğramadan nesillerden nesillere aktarılıyor. Notumuz: A+
• İtibari paralar kâğıt formunda eskidikleri durumda, arkalarındaki Merkez Bankaları bunları değiştiriyor. Orada bir sorun yok. Potansiyel sorun, bu paraların arkasındaki Merkez Bankaları bir gün olmazsa? Mesela 1913–1933 yılları arasında var olmuş olan eski Almanya diyebileceğimiz Weimar Cumhuriyeti.[87] 1919 yılında 1 Mark olan bir ekmeğin 1923'de 100 milyar Mark olması ve sonrasında paranın değersiz ve kullanılamaz hale gelmesi gibi canlı bir örnek var önümüzde. Notumuz: B
• Bitcoin'e gelirsek, ilk başladığı 2009 yılından bu yana aynı şekilde devam ediyor. Yapılan her türlü dış atağa karşı şu ana kadar sağlam durdu. İleride ne olacak kimse bilemez ama benzer şekilde bu tür bir bilinmezlik belki çok güçlü birkaç para dışında her ülke parası için de geçerli. Notumuz: B

[87] https://tr.wikipedia.org/wiki/Weimar_Cumhuriyeti

Taşınabilirlik

• Altın, bu üçlü içinde taşınması en zor olanı. Zira bir yerden diğerine taşımak hem maliyetli hem fiziki olarak zor. Bu nedenle daha çok rezervlerde tutuluyor ve sabit duruyor. Notumuz: C
• İtibari paralar, fiziki olarak çok taşınmasalar da, genelde dijital olarak taşınabiliyorlar. Yine de ülkeler arası sistem farklılıkları ya da politikalar nedeniyle uzun süre alabiliyor para transferi, kimi zaman da hiç mümkün olmayabiliyor. Notumuz: B
• Bitcoin bu alanda korkutucu derecede avantajlı. Milyonlarca dolara eşdeğer Bitcoin'i 10 dakika içinde dünyanın öbür ucundaki birine gönderebilmenizin ötesinde, özel kelimelerinizi bir parça kağıda yazarak tüm Bitcoin'inizi bir ülkeden diğerine rahatça cebinizde taşıyabilirsiniz. Notumuz: A+

Ölçülebilirlik/Eşitlik

• Bu alanda altın en önde giden. Altını alıp eritin, parçalara bölün, toplayın altın yine altın. Gramı ne ise kilosu da aynı. Notumuz: A+
• İtibari paralar da fena sayılmazlar. Gerçi yüksek rakamlı banknotlar bazen sıkıntı yaratabiliyor. Örneğin Hindistan hükümetinin kayıt dışını önlemek için 500 ve 1000 rupi banknotlarını azaltmasından sonra bu paralar piyasada iskonto görüyor. Notumuz: B
• Bitcoin de bu alanda itibari paralara benziyor, hatta daha dezavantajlı olabilir. Bitcoin özelliği gereği takip edilebilir. Dolayısıyla örneğin kara para ile ilgisi olan rakamların transferinde?—?özellikle büyük meblağlar söz konusu olduğunda-, Bitcoin çok da elverişli bir araç değil.
Notumuz: B

Doğrulanabilirlik/Sahicilik

• Altın, sahiciliğini kanıtlamada genelde oldukça iyi ama kimi zaman altın kaplamalı sahte madenlerin altın diye yutturulması vakaları mevcut.
Notumuz: B

• İtibari paralar ve banknotların da sahteleri ile insanların kandırıldığı örnekler maalesef hala mevcut. Notumuz: B
• Bitcoin o anlamda altın ve itibari paradan açık ara daha önde. Herkes sahip olduğu Bitcoin'i çok rahat bir şekilde kanıtlayabilir. Hatta, ortada dolaşan ve "Ben Satoshi Nakamoto'yum" diye dolaşan şahıslar eğer gerçekten o kişi ise, kanıtlamaları o kadar kolay ki! Yapılan ilk işlemi kendisinin yaptığını göstersin yeter :) Notumuz: A+

Bölünebilirlik

• Altını ufak parçalara bölsek, en ufağı 1 gram olsa yine de oldukça yüksek bir rakam. Ekmek almak için altın kullanamayız mesela. O nedenle özellikle mikro ödemeler için elverişli değil. Notumuz: C
• İtibari para bu anlamda gayet iyi. Kuruşlara kadar inebiliyorsunuz. Notumuz: A
• Bitcoin ise çok daha küçük parçalara inebildiği için itibari paralardan bir adım önde (gerçi çok ufak paraları transfer etmek komisyon rakamlarından dolayı çok mantıklı olmayabilir). Notumuz: A+

Kısıtlılık

• Altın, şu anda dünyada hatırı sayılır miktarda var ve yeni büyük bir arz beklenmiyor. Yine de teknolojideki değişimler kimi elde edilmesi zor rezervleri ekonomik hale getirip arzda artışa yol açabilir. Notumuz: A
• Maalesef itibari paralar bu alanda sınıfta kaldılar. Zira para musluğu Merkez Bankaları'nın elinde ve para arzı ciddi boyutlara ulaşabiliyor. Notumuz: F
• Bitcoin'in altın ve itibari paralara göre en ayırt edici özelliği bu. Şu anda Bitcoin'in %80'i tedavülde[88]. Kalan %20 ise 2140 yılına kadar her dört yılda bir azalarak tedavüle girecek. Arz belli ve gittikçe azalacağı için deflasyonist bir trend yaşanacağı söyleniyor ama bu Bitcoin fiyatı ileride artacak diye kesin bir hüküm vermeye yeterli değil. Notumuz: A+

[88]http://www.bitcoinblockhalf.com/

Evet-yukarıda saydığımız özelliklere bakınca Bitcoin'in para olduğu konusunda hiçbir kuşku yok. Ne kadar değerlidir, ona da yanıt aradık, yine de en iyisi bu kararı siz verin. Ama eğer topluma bakacak olursanız 22 Mart itibariyle 7.500 ABD Doları adet fiyatı ve 125 milyar ABD Doları toplam piyasa değeri ile Bitcoin dünya tarafından şimdilik değerli bir para olarak kabul edilmiş bile.

Sadede gel? (TL;DR - Too long, did not read)

Efendim, konuyu özetlersek:

• Bir nesneyi para diye adlandırmamız için insanlar arasındaki ticari ilişkilere aracılık etmesi ve insanlar tarafından ona bir değer atfedilmesi olmazsa olmaz koşullar
• Bunun yanında para ne kadar kullanışlı ise ve sirkülasyonu artar ise o kadar değerli oluyor
• Tarihte alışveriş ve değer korunumu için önce altın, sonrasında ise Merkez Bankalarının bastıkları banknotlar kullanılmış
• Bitcoin'i altın ve banknotlar ile karşılaştırdığımızda, dezavantajları olsa da genel olarak kullanışlılık açısından bu iki araçtan bir adım önde görünüyor.

Kripto paralar üzerine bir hayli vakit harcadık. Bundan sonra, Blockchain teknolojisinin bizi ya da kurumları nasıl etkileyeceğine diğer dijital varlıklara bakarak karar vermeye çalışacağız.
- - - - - - - -

Not: Daha detaylı bilgi için aşağıdaki yazılara da göz atmanızı tavsiye ederim:
• Vijay Boyapati'nin uzun ama oldukça açıklayıcı "Bullish Case for Bitcoin[89]" ve
• Nick Szabo'nun 2002 tarihli ağır ve karmaşık ama muhteşem "Shelling Out: The Origins of Money[90]"

[89]https://medium.com/@vijayb_24615/the-bullish-case-for-bitcoin-6ecc8bdecc1
[90]http://nakamotoinstitute.org/shelling-out/

Bitcoin *işlemi* nasıl gerçekleşiyor?

Bitcoin temelinde teknik bir konu. Bu nedenle sıradan kullanıcıya bazı kısımları karmaşık hatta karanlık gelebilir. Halbuki olabilecek en şeffaf sistem bu. Herhangi bir Bitcoin işlemi aslında nasıl gerçekleşiyor anlamak kimi noktaları aydınlatmak için yararlı olabilir.



Eğer kripto paralara ve Bitcoin'e biraz ilgi duyduysanız ya da konuyu biraz araştırdı iseniz mutlaka duymuşsunuzdur aşağıdaki yorumları:

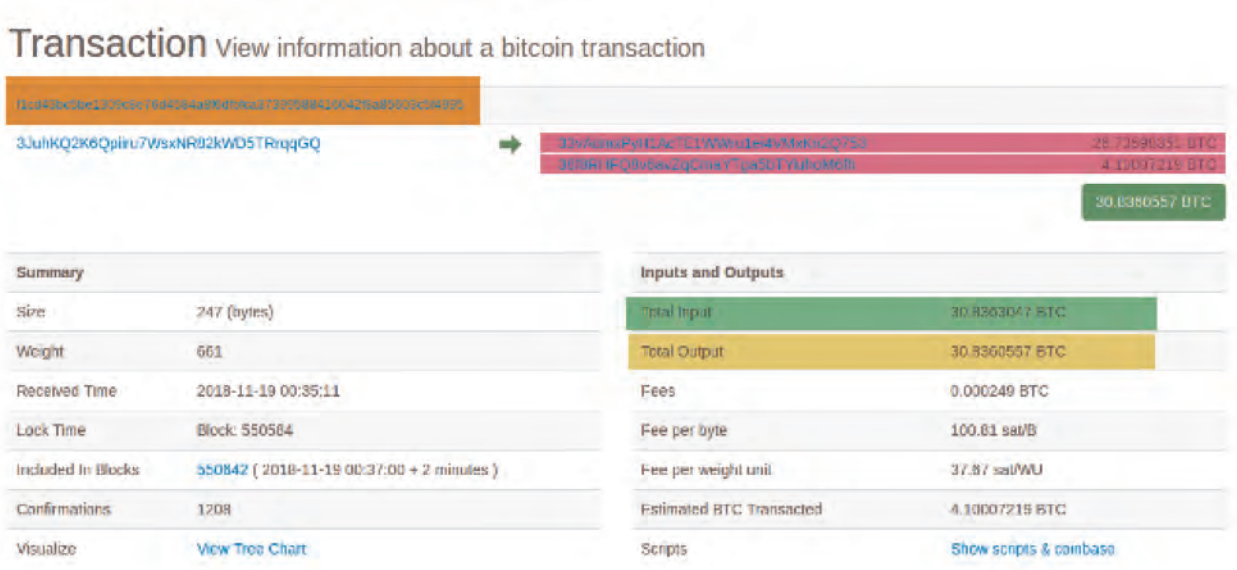
• Bitcoin işlemleri 10 dakika içinde bitiyor, dünyanın öbür ucuna 10 dakika içinde dijital bir varlığı gönderebiliyorsunuz
• Bitcoin, kişilerin ellerindeki varlığı birden fazla kez harcamasına olanak vermez
• Bitcoin üzerindeki bütün işlemler görülebiliyor, öyle ki ilk yapılmış işlem olan 3 Ocak 2009 tarihli işleme kadar geriye gidip görebiliyorsunuz
• Bitcoin üzerindeki işlemler makineler tarafından teyit ediliyor, edilmez ise işlem geçersiz sayılıyor
• Varsayalım biri Bitcoin sistemindeki makinelerin çoğunu ele geçirdi; yapabileceği en tehlikeli iş en son 10 dakikada yapılmış bir işlemi geri çevirmek olur, kişilerin varlıklarına zarar veremez. Bitcoin hiçbir varlığın sahibinin haberi olmadan elden ele dolaşmasına da izin vermez.

Kulağa ilginç gelen hoş söylemler. Peki ama nasıl bir şeydir bu para transferi? Nasıl emin olabiliyoruz bu kadar? Gelin isterseniz gerçek bir Bitcoin işlemi nasıl oluyor bakalım ve yukarıda yazılanların doğru olup olmadığının kararını kendimiz verelim.

Bir Bitcoin işlemi nasıl bir 'şey'?

Bitcoin işlemi özünde herhangi bir miktarda paranın (bu sistemde bu para BTC olarak geçiyor) sahipliğinin bir kişiden diğerine transfer edilmesi demek. Aşağıda bir Bitcoin işlemi görüyorsunuz- dedik ya, bütün işlemler herkese açık diye, bu işlem de öyle. 28 Kasım tarihinde yapılmış herhangi bir işlem linkine istediğiniz zaman ulaşabilirsiniz[91]).

[91] https://www.blockchain.com/btc/tx/f1cd43bc5be1309c8e76d4584a8f6dfbfca37399588416042f8a85603c5f4995



28 Kasım 2018 tarihli gerçek bir işlem (Kaynak: Blockchain.info)

Önemli olan satırlara kısaca bakalım daha iyi anlamak için bu işlemi.

İşlem numarası (Transaction ID): Yapılan her işlemin kendine ait bir numarası var. Yukarıda turuncu ile taranmış alan. Tek bir numara ve sadece bu işlem için kullanılıyor. Ve bu numarayı alın herhangi bir Bitcoin kaydını tutan siteye girin ve o işlem ile ilgili resimde gördüğünüz tüm bilgilere ulaşabilirsiniz.

Örneğin f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16 no'lu hash'i bir siteye (örneğin www.blockchain.info) girin, karşınıza Bitcoin ile yapılmış ilk işlem (2009 Ocak ayından) çıkacak. Boşuna dememişler Bitcoin ile yapılan her işlem kayıt altında diye. Gördüğünüz gibi 2009 yılından itibaren yapılan her işlem tek tek görülebiliyor bu şekilde. Hani hep deniyor ya, bütün bilgisayarlar yapılan işlemlerin tüm kaydını tutuyor diye. İşte bu o.

Alıcının adresi: Gönderdiğiniz parayı alanın adresi. Yukarıda pembe renk ile gördüğünüz alan. Kişi adı yok (gizlilik bu şekilde oluyor) sadece rakam ve harflerden oluşan eşi benzeri olmayan bir başka numara. Gönderilen Bitcoin her zaman bir adrese gider. Burada iki adres görüyorsunuz. Yani para iki adrese gitmiş. Genelde de böyle olur. Neden? Az sonra değineceğiz.

Göndericinin adresi: Aldığınız Bitcoin bir adrese gelir ama siz onu birisine göndermek isterseniz bunun için cüzdanınızı kullanırsınız. Paranın size geldiği adres size ait bir posta kutusu iken, cüzdan size ait bir Özel Anahtar ile açabildiğiniz ve bu sayede bu parayı sadece sizin harcamanıza olanak veren bir oda. Neden bir cüzdan da adres değil? Az sonra örnekte göreceksiniz.

Kullanılan para (Total input): Bu işlemde alıcının cüzdanından gönderilen toplam para miktarı-yeşil renk ile gösterilen yer.

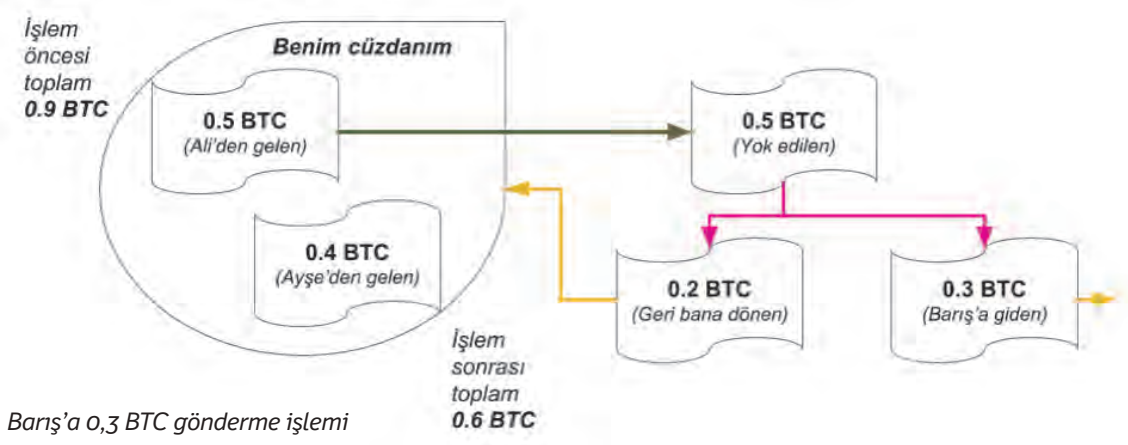
Çıkan (yaratılan) para (Total output): Alıcılara gönderilen toplam para. Hemen yukarıda bahsettiğimiz kullanılan paradan bir miktar daha az, çünkü işlemi gerçekleştiren makinelere ödenen bir komisyon var (Total input'un hemen alt satırında sarı renk ile taranan alanda görüyorsunuz)

Bitcoin işleminin temel mantığı ne?

Bir Bitcoin işlemi gerçekleşirken temel birkaç mantık var. Gelin onlara bir parça değinelim. Bitcoin'in karışmaması, herhangi bir şekilde rahat takip edilebilmesi için temel iki kural var:

1. Öncelikle size gelen Bitcoin'ler her zaman ayrı ayrı dururlar. Hiçbir zaman birbirleri ile karışmazlar.
2. Sonra her Bitcoin yalnızca bir kez kullanılır. Evet, yanlış duymadınız. Her Bitcoin miktarı ne olursa olsun, bir kez kullanılır.

Örnek verelim: Diyelim size Ali'den 0,5 BTC (Bitcoin) ve Ayşe'den de 0,4 BTC geldi. Cüzdanınızda bu iki para ayrı ayrı durur. Birbirine karıştırılmaz. Ve diyelim ki siz şimdi Barış'a 0,3 BTC göndereceksiniz.



Barış'a 0,3 BTC gönderme işlemi

Sistem şöyle çalışır: Ali'den gelmiş 0,5 BTC alınır. Sonrasında bu paranın 0,3 BTC'si Barış'a gönderilir, kalan 0,2 BTC benim adıma yaratılan yeni bir Bitcoin adresine gönderilir (ve benim cüzdanıma geri döner). Yani bir nevi elimde 0,5 BTC bütün banknot var, Barış'a 0,3 BTC verdim, kalan 0,2 BTC de "paranın üstü" olarak bana geri döndü.

Bu ortaya çıkan iki paraya (0,3 BTC ve 0,2 BTC) UTXO Unspent Transaction Amount denir. Yani benim cüzdanımda duran 0,5 BTC yok edildi, yerine bende ve Barış'ta iki parça halinde 0,5 BTC (eksi komisyon) yaratıldı.

İşte bu yüzden yukarıdaki ilk orijinal örnekte de paranın gittiği iki adres görüyorsunuz pembe renkte. Üstteki pembe renkli olan alıcının, alttaki ise gönderici için yaratılan yeni adres. Artık cüzdanımda Ayşe'den gelen 0,4 BTC ve Barış'a gönderdiğim paradan geri dönen 0,2 BTC toplam 0,6 BTC var (yine ayrı ayrı duruyorlar).

İşte bu nedenle para bir adrese geliyor ama çıkarken cüzdandan çıkıyor. Çünkü gönderilen paranın üstünün geri alınması cüzdana (onun için yaratılan yeni adrese) yapılıyor. Gönderilen adres yok oluyor.



Aynı şekilde kimi zaman, gönderilecek para eldeki tek bir adresten değil, birkaç adresten gönderilmek zorunda kalıyoruz. Yukarıdaki durumda 0,7 BTC göndermek zorunda olsaydım hem Ali'den gelen parayı hem de Ayşe'den gelen parayı kullanacaktım. O nedenle de para cüzdandan çıkıyor.

Bu UTXO kavramı önemli. Çünkü bütün UTXO'ları toplarsanız o ana kadar oluşmuş bütün Bitcoin toplamına ulaşıyorsunuz. Bu da birilerinin sahte para ortaya çıkarmasını önlüyor. Çünkü en başından beri çıkan UTXO toplamları belli ve sürekli olarak tutuluyor. Bütün makineler bu UTXO'lara bakarak yapılan işlemlerin doğru olduğunu anlıyorlar. Hani deniyor ya, "Ya birisi çıkar da bütün makinelere ele geçirirse? Kendisine para yaratırsa?" Nasıl yaratacak ki? Bir anda sıfırdan para yaratmak isteseniz yaratamazsınız çünkü para bir adresten gelmek zorunda. Şimdiye kadar yaratılmış bütün paralar belli, hangi adreslerde olduğu belli. O adreslerden o paraları ancak o adresin sahipleri kendi Özel Anahtarları ile çıkarabilirler. (Özellikle öğütme - hashing- ile sistem daha da güvenli hale geliyor. "Özel Anahtar ne, öğütme ne?" diye merak ediyorsanız "Blockchain Şifrelemesi Ne Demek?" bölümüne bakabilirsiniz)

Yarın öbür gün biri çıkar da uzlaşma ile çalışan sistemde makinelerin %51'ini ele geçirerek sistemi sahiplenirse yapabileceği tek hamle, harekete geçtiği anda yapılmış olan son işlemleri reddetmek olabilir. O nedenle zaten hep söylenen bir kural vardır: "Birinden bir Bitcoin alsanız bile onu hemen kendinizin bilmeyin. İşlem önce bir bloğa yazılsın. O blok sistemdeki makineler tarafından doğru kabul edilsin. Üzerine birkaç yeni blok daha konsun. Ancak ondan sonra gönül rahatlığı içinde o para benim diyebilirsiniz".

Diyebilirsiniz ki, "İyi de birisi makinelerin %51'ini ele geçirip UTXO kaydını da değiştirebilir". Yapabilir tabii ama o zaman sahtekarlık yaptığı ortaya çıkar (UTXO listesi anlık olarak takip edilebilir) ve çoğunluk olmasa bile dürüst makineler sistemde yeni bir dal açarak (hard fork) dürüst işlem yapmaya devam ederler. %51'i elde etmiş olan o grup da yaptığı harcama ile kalır.

Sonuç

İşte böyle. Bir Bitcoin işleminin nasıl gerçekleştiğini görmek size bu karmaşık dünyada içinizi biraz daha rahatlatabilir. Bitcoin aslında sahibi olduğuna emin olabileceğiniz belki de tek varlık. Elinizde banknot varsa sahte çıkabilir. Keza altın varsa da öyle; gerçek olup olmadığını anlamak için testten geçirmeniz gerekir. Bitcoin için öyle değil. Gönderin birine parayı sistem reddetmiyor ise gerçektir. Bitcoin'e sahipseniz yapmanız gereken tek kritik konu Özel Anahtarınızı kaybetmemek. Ona sahip oldukça o para siz istediğiniz sürece sizin olacak merak etmeyin.

Bitcoin geniş kitlelere nasıl yayılır?



Bitcoin'in şu anki spekülasyonları bir kenara bırakırsak ileride bir değeri olup olmayacağına geniş kitleler tarafından kullanılıp kullanılmayacağı karar verecek.

Geçtiğimiz bölümde, Bitcoin'in ileride değerli olup olmayacağının iki ana belirleyicisi olacağını belirtmiştik: Birincisi hakikaten insanların işine yarayacak mı, ikincisi de geniş kesimler tarafından kullanılacak mı? Bu iki soruya ne kadar olumlu cevap verebiliyorsak Bitcoin'in değerinin de ileride o kadar artacağını düşünebiliriz.

Bitcoin'in geleceği nasıl şekilleniyor?

Her ne kadar teknoloji hızla gelişiyor olsa da Bitcoin için aynısını söylemek mümkün değil. Bitcoin yavaş gelişen bir sistem bu kasıtlı olarak böyle aslında. Efendim, Bitcoin biliyorsunuz bir dijital para. İşin içine para girdiğinde konu ciddileşiyor. Bitcoin geliştiricileri de bu bilinç ile hareket ediyorlar.

Bu geliştiriciler temel bir prensip var: "Acele işe şeytan karışır", yani ne kadar hızlı gider ve yeterince test ve deneme yapmazsanız hata çıkma ihtimali o kadar artar. O nedenle bu topluluk Bitcoin sistemini özellikle yavaş yavaş tabiri caizse sindire sindire geliştirme yolunu seçiyor.

İkinci bir prensipleri daha var bu topluluğun: "Bir ürüne ne kadar fonksiyon eklerseniz, o kadar güvenlik açığına davet çıkarırsınız[92]" Konu para olunca güvenlik açığının yaratacağı sorunlar daha da dramatik hale gelebiliyor. O nedenle geliştiricilerin Bitcoin'e para dışında yeni fonksiyonlar eklemeleri oldukça zor.

Peki ne olacak o zaman? Bitcoin bu haliyle kör topal devam mı edecek? Tabii ki hayır. Olacak olan ana hatları ile şu: Bitcoin ana (baz) katman olarak fonksiyonunu dijital para şeklinde sürdürecek. Bu ana katmanın üzerine inşa edilecek yeni katmanlar geniş kitlelerin ihtiyacı olan o yeni fonksiyonları sunacaklar.

[92] https://twitter.com/NickSzabo4/status/956507150012026882



Kahvenizi Bitcoin ile ödemek mi?

Bitcoin'in büyümesi ve geniş kitleler tarafından adapte edilmesinin önündeki en büyük engel kendi teknik kısıtları. Nedir onlar? Anlatalım:

Bitcoin ile kıtalararası para gönderme yapabiliyorsunuz diyoruz. Bunun yaparken de maliyetleriniz oldukça düşük. Özellikle yurtdışında yaşayanlar için çok iyi haber. Ama bu göreceli olarak küçük bir kitle ve sınır ötesi para transferini ayda yılda bir yapıyorlar. Bitcoin'in geniş kitlelere yayılması için yeterli değil.

Peki ya gündelik hayatta mikro ödemeler için Bitcoin kullanımı? İşte orada Bitcoin'in kendi iç kısıtlamalarına takılıyoruz. Bitcoin'in saniyede yapabileceği işlem sayısı 7 ile kısıtlanmış. Ethereum için bu sayı 20 işlem. Paypal'in saniyede 450, Visa'nın ise 56.000 işlem yapma kapasitesi olduğunu söylersek Bitcoin'in neden mikro ödemeler için kullanılamayacağını anlayabiliriz sanırım.

Mikro ödemeleri Bitcoin üzerinden yapmaya kalkarsak sistem patlar mı?

İşlem sayısı kısıtlamanın getirdiği ana sorun işlem hızı. Normalde Bitcoin transferi yaptığınızda işlem madenciler tarafından alınıyor ve o anki en son bloğun içine işleniyor. Peki ya bloğun hacminden daha fazla işlem yapıldı ise? O zaman işlem bir sonraki bloğa atılıyor. Her bir blok 10 dakikada bir toplanıp bağlandığı için böyle bir durumda işleminizin gerçekleşmesi 10 dakika sonraya kalıyor. Peki neye göre işleminizin o bloğa ya da sonraki bloğa gireceğine karar veriyor madenciler? O yaptığınız işlem için verdiğiniz (ya da vermek istediğiniz) komisyona göre. İşlem ücretiniz ne kadar yüksek ise o kadar erken işleminiz gerçekleşiyor. Mikro ödemeler zaten kendileri ufak rakamlar oldukları için işlem ücretleri de çok düşük olmak zorunda, bu nedenle de geç gerçekleşme ihtimalleri yüksek.

Bitcoin'i nasıl hızlandırırız?

Aslında bir mikro ödemenin gerçekleşmesi için tüm Bitcoin sisteminin kullanılmasına o kadar da gerek yok. Çünkü biliyorsunuz Bitcoin ile bir işlem yapıldığında binlerce makineye bu işlem yazılıyor. Bir kafeye girip satın aldığınız bir kahvenin işlemi neden binlerce makinede yazılsın ki? Bu işlemler bir bir işlenmek yerine bir araya toplansa?

İşte bu felsefeden yola çıkan geliştiriciler Bitcoin üzerinde mikro işlem yapabilmek için ikinci bir katman yarattılar. Buna da Lightning Network adını verdiler. Bir sonraki bölümümüzde bu Lightning Network nedir biraz daha yakından bakalım.

Bitcoin üzerinde ışık hızıyla işlem nasıl GERÇEKLEŞİR?



Lightning Network

Bitcoin bir gün hayatımızın bir parçası haline gelecekse öncelikle kendi sıkıntılarını aşmalı. Bu konuda çalışan çok. Bunlardan biri de Lightning Network.

Geçtiğimiz bölümde, Bitcoin'in geniş kitlelerce kullanımının önündeki en büyük engelin teknik olarak kısıtlı kapasitesi olduğundan bahsetmiştik. Özetle tekrarlarsak; yapılan her işlem Blockchain üzerine yazılıyor, bunu yapan madenciler ve işlem binlerce makineye yazıldığı ve 10 dakikada bir balya haline getirilip onaylandığı için saniyede maksimum 7 işlem gerçekleşebiliyor.

Ama eğer biz her işlemi Blockchain üzerine yazmak yerine bunları toplayıp bir araya getirsek ve o şekilde yazsak, yani Blockchain'in zinciri üzerine değil zincir dışı işlem yapsak o zaman bu teknik kısıtlardan kurtulabiliriz. Peki ama, biri bana bir Bitcoin yollarsa benim bu Bitcoin'e sahip olduğumu kanıtlamamın tek yolu bu paranın Bitcoin Blockchain'ine işlenmiş olması değil miydi? Nasıl emin olacağım Bitcoin'in benim olduğuma eğer Blockchain zincirini kullanmaz isek? İşte Lightning Network dediğimiz sistem hem zincir dışı hızlı binlerce işlem yapabilen hem de bu binlerce işlemin sadece sonuçlarının Blockchain'e yazıldığı (yani herkesin hak ettiği Bitcoin'i günün sonunda kendi cüzdanında görebildiği) bir yol öneriyor.

Nedir bu Lightning Network?

Önceki bölümde da belirttiğimiz gibi Lightning Network esasında Bitcoin üzerine kurulmuş ikinci bir katman.

Lightning'in ana prensibi Bitcoin üzerindeki işlemlerin zincir üzerinden (yani bloklara yazılması yerine) zincir dışına çıkarılması.
Özündeki prensip ise şu:

• İşlemleri yapmak için ayrı kanallar kuralım.
• Bu kanallar baştan Bitcoin sistemine para yatırsınlar, bir nevi depozito koysunlar.
• Sonrasında bu koydukları parayı geçmemek kaydıyla Bitcoin Blockchain'i dışında kişiler arası para transferi yapılmasına aracılık etmeye yetkili olsunlar (ve aracılık ettikleri bu işlemlerden cüzi bir işlem ücreti alsınlar).
• Birinden alsınlar öbürüne versinler, ama yaptıkları işlemlerin sonundaki net bakiye başta koydukları depozitoyu hiçbir şekilde geçmesin.

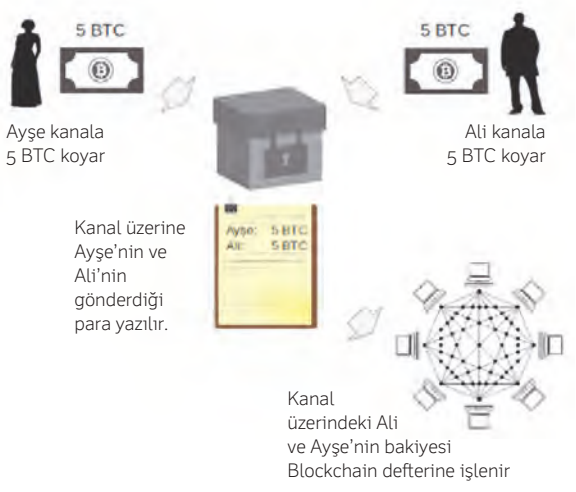
• Böylece madencileri kullanmadan işlemlere aracılık etsinler, dolayısıyla masrafları çok daha az olsun ve bunun sonucunda da sistemi kullanan kullanıcılardan komisyon olarak alacakları çok cüzi rakamlar bile kendilerini kurtarsın.

Nasıl çalışıyor peki bu Lightning Network?

Basit bir örnek ile başlayalım sonra detaylandıralım:

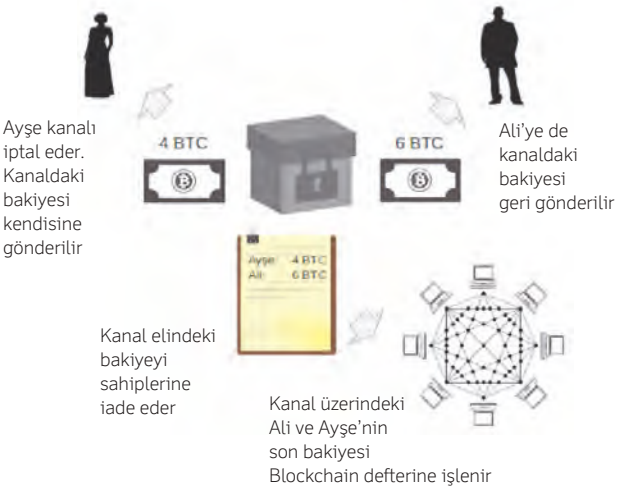
• Ali ve Ayşe ticaret ile uğraşıyor ve birbirlerine sık sık para gönderiyorlar. Bu ikili öncelikle beraberce bir kanal (burada basit olsun diye kilitli bir sandık diyelim) yaratıyorlar. Bu sandığa her ikisi de bir miktar Bitcoin koyuyorlar (örneğin her biri 5 BTC). İlk para koyduklarında bu işlem Bitcoin Blockchain üzerine işleniyor.

• Diyelim bir gün Ali Ayşe'ye 1 BTC gönderiyor, ertesi gün de Ayşe Ali'ye 2 BTC. Bu iki işlemi de Bitcoin ağına binlerce makineye göndermek yerine kendi aralarındaki bu sandık üzerinden gerçekleştiriyorlar. İki gün sonunda Ali'nin sandıktaki hakkı 6 BTC, Ayşe'ninki ise 4 BTC oldu. Sandık orada, iki taraf da kendi bakiyelerini görebiliyor. Ama Bitcoin Blockchain'e herhangi bir bildirimde bulunmuyorlar.





• Eğer iki günün sonunda Ali ya da Ayşe'den biri parayı kendi hesabına çekmek isterse sandığı iptal ediyor. Bu durumda her iki tarafın bakiyesi kendi hesaplarına geri aktarılıyor. Bu örnekte Ali 6 BTC Ayşe ise 4 BTC alıyor.



Özetle iki kişi sandık adını verdiğimiz bir kanal yarattılar. Sandıktaki para da bu kanalın Bitcoin üzerindeki depozitosu, yani bu kanalı kullanacakların güvencesi.

İki kişi üzerinden anlatınca basit görünüyor ama böyle ikili ticaret eden kaç kişi var ki? Peki denkleme bir kişi daha ekleyelim: Örneğin Ayça.

Ayça'nın da Ayşe ile ortak bir sandığı olsun ancak Ali ile daha önce hiçbir para ilişkisi olmasın. Ayça Ali'ye para gönderebilir mi (örneğin 0,5 BTC)? Gayet tabii. Ayça Ali'ye parayı Ayşe aracılığı ile gönderebilir. Ayça'nın Ayşe ile ortak sandığından 0,5 BTC'sini Ayşe'nin yaparsınız, Ayşe'nin Ali ile olan sandığındaki 0,5 BTC'sini de Ali'nin.



Şimdi bu tip sandıklardan (kanallardan) binlerce kişi ve kurumun açtığını düşünün: Bir kahve zincirisiniz. Ali ile Ayşe içtikleri kahve için size ödeme yaptılar. Siz de bu ödemeleri alıp size kahve çekirdeği satın almada kullandınız. Size çekirdeği satan firma dijital reklamlarının dizaynını yapan Ayça'ya bu para ile ödeme yaptı. Ayça da Ali'den aldığı internet hosting hizmeti için kendisine bir miktar para yolladı. İşte tüm sistemi Lightning Network üzerinden döndürebilirsiniz. Binlerce işlemin Bitcoin üzerinden Blockchain bloklarına yazılmadan güvenli bir şekilde gerçekleştirildiği ikinci bir katman yaratmış olursunuz.

Sonuç?

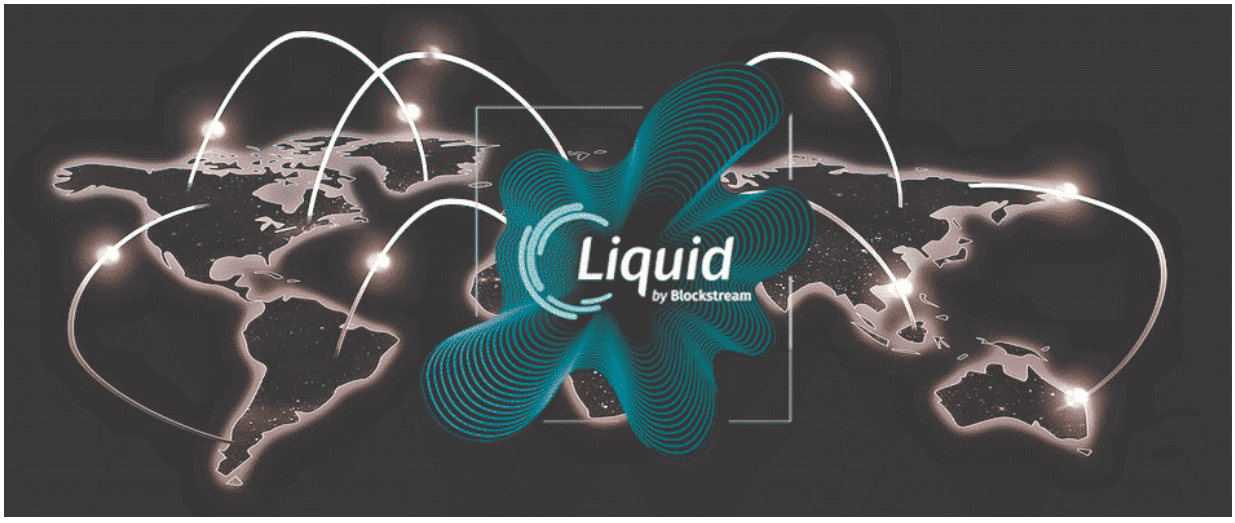
Bitcoin sanal dünyadaki şifreli paralar içinde en kullanılanı. Ancak yine de hala kısıtlı bir kitlenin elinde. Eğer hakikaten bir değer elde edecek ise faydalarının geniş kitlelere yayılması gerekiyor. Bitcoin geliştiricileri Bitcoin'i 'bozma' riski almamak için geniş kitlelerin ihtiyacı olan değişiklikleri çabucak yapmayacaklar. Bu yenilikleri Lightning Network gibi ikinci katmanlar gerçekleştirecek. Başarılı olup olmayacaklarını zaman gösterecek ancak şimdiden söyleyebileceğimiz doğru yolda oldukları.

Bitcoin üzerinden büyük işlemleri hızlı yapmak mümkün mü? Bir çözüm: Liquid

Bitcoin doğası gereği yavaş gelişiyor ama ona eklenen başka teknolojiler çok daha hızlı ilerleyip Bitcoin'in geniş kitlelerce kullanımını kolaylaştırmaya çalışıyorlar. Bunlardan biri de Liquid. Ne olduğu aşağıda:

Geçtiğimiz bölümde Bitcoin'in geniş kitlelere yayılması için üzerinde çalışılan yeniliklerden Lightning Network'den bahsetmiştik. Şimdi de bir başka potansiyel yenilik olan Liquid Network 'e bakalım birlikte.





Liquid Network? Nedir o?

Liquid Network aynı Lightning Network gibi Bitcoin'i üzerine inşa edilmiş bir yenilik. Ama benzerlikleri orada bitiyor.

Kısaca hatırlayacak olursak, Lightning Network Bitcoin üzerine kurulmuş ikinci bir tabaka idi. Bitcoin üzerinde depozito koyup kanal açan aracılar, bu depozitoyu kullanarak birbirleri üzerinden işlem yapabiliyorlar idi. Böylece hem Bitcoin'in sağladığı güvenlik, gizlilik gibi özellikleri kullanabiliyor hem de Bitcoin ağı üzerinde yük yaratmadan binlerce işlem yapabiliyorlar idi.

Liquid hisse alım-satımı yapan kurumlar ve borsalar arasında hızlı işlem yapmaya yarayan özel bir Blockchain. Farkı Lightning Network gibi Bitcoin üzerine kurulmuş bir tabaka değil de Bitcoin'e bağlı bir yan-zincir (side-chain) olması. Ne demek yan zincir? Açıklayalım:
Liquid'in yaratmış olduğu özel bir Blockchain ve buna bağlı olan L-BTC adında bir para var. Kendilerini ABD Doları gibi İtibari paraya bağlayan kimi kripto paralar benzeri L-BTC de kendini Bitcoin'e bağlamış.

Yani hem BTC ile aynı değerde hem de bir L-BTC yaratılması için aynı oranda bir BTC karşılığının olması gerekiyor. Kullanıcılar BTC (Bitcoin'in parası) sahibi olmaya devam ederken L-BTC'nin sağladığı ek avantajlardan yararlanabiliyorlar.

Liquid Network, Bitcoin'den farklı olarak özel bir Blockchain (permissionless). Ne demek bu? Şöyle: Bitcoin açık bir network olduğu için hem kullanıcılar hem madenciler istedikleri gibi girip çıkabiliyorlar. Liquid Network'de ise Bitcoin'deki gibi madenciler yok. Sadece şu an sayısı 15 olan borsalar ve kurumsal aracılar var. Yapılan işlemleri madenciler onaylamıyor, o işi bu borsa ve kurumsal aracılar yapıyor. Bitcoin'de madencilerin çoğunluğunun işlemi onaylaması gerekirken burada üçte iki çoğunluk gerekiyor, yani 11 borsanın işlemi onaylaması gerekli.

Kullanıcılar ise L-BTC ile istedikleri gibi işlem yapabiliyor ama L-BTC'lerini satmak için yine bu borsaları kullanmak zorundalar. Kullanıcı olarak bir borsaya girip L-BTC aldığınızda, bu spesifik bir BTC'ye bağlanıyor ve satmaya kalktığınızda o spesifik BTC üzerinden işlem yapılıyor. Böylece olası sahtekarlıklar önlenmiş oluyor.

Nedir sağladığı avantajlar Liquid'in?

Kullanıcılar için Liquid'in sağladığı en büyük avantaj SabitParalar ile benzer aslında.
Kripto paranızı (buradaki örnekte BTC'nizi) bir borsada tutmak riskli. Neden? Her ne kadar kripto para borsaları her tür güvenlik önlemini alsalar da merkezi yapılar-dış tehdit ve saldırılara açıklar. O nedenle kurumsal yatırımcılar özellikle büyük miktarda parayı borsalarda tutmak istemiyorlar.

Paranızı borsada tutmadığınız durumda ise işlem yapmak istediğinizde çok vaktinizi alıyor. Cüzdanınızdan parayı borsaya göndermek Bitcoin üzerinde en kısasından 10 dakika ama borsanın bunu tam olarak alıp (teyid edip) size işlem yaptırmasına baktığınızda çok daha uzun zaman alıyor. Özellikle çok işlem yapan biri iseniz bu kimi fırsatları kaçırmanıza yol açabilir.

İşte Liquid bu iki soruna çözüm getiriyor. Paranızı L-BTC'de tuttuğunuzda, borsaya 1 dakika içinde gönderebilir ve hemen alım satım yapabilirsiniz. Daha sonrasında L-BTC'inizi isterseniz kendi cüzdanınıza çekersiniz, ya da BTC'ye çevirirsiniz (1'e 1 aynı oranda).

Var mı sakıncaları?

Teoride yukarıda yazılanlar çok güzel görünse de Liquid'e kuşku ile bakanlar da yok değil. Bu kuşkuların ciddi bir kısmı felsefi aslında.

Bitcoin'in bağımsız yapısını ön plana çıkaranlar Liquid Network gibi yapıların özel network olmasına takılıyorlar. Dediğimiz gibi işlemleri onaylayanlar madenci değil özel olarak seçilmiş 15 kurum. Kaldı ki bu seçilmiş kurumların hepsinin sicili de o kadar iyi sayılmaz (a, b, c). Ya bu 15 kurum içinde 11'i birlikte hareket ederse?

Liquid yaratıcıları da böyle bir riski kabul ediyorlar ama karşılaştırmanız gerekenin paranızı (BTC'ninizi) bir borsada tutmanın riski ile 15 farklı borsada tutmanın riski olması gerektiğini söylüyorlar. Tek bir borsanın risklerini almaktansa, riski 15 ayrı borsaya dağıttığınızı belirtiyorlar. Ama nereden bakarsanız bakın, BTC'nin orjinal yaratıcılarının düşlediği özgür dünyadan sapma bu yapı sonuç olarak.

İkinci bir eleştiri ise, Blockstream'e yapılıyor. Kâr güden bir kurum olan Blockstream, kendi kaynaklarını kullanarak bugün için Bitcoin'in geliştiren hatırı sayılır sayıda yazılımcıya iş olanağı sağlıyor. Eleştirenler, bu kişilerin ileride Bitcoin'i geliştirirken de Blockstream'ın istediği alanlara yönelip tarafsızlıklarını kaybedebileceklerinden endişe duyuyorlar. Şahsen çok katılmadığım bir kaygı. Zira Bitcoin geliştiricisi olmak için herhangi bir sertifika ya da izin gerekmiyor. İsteyen yazılımcı Bitcoin'i geliştirmek için katkıda bulunabilir. Blockstream'in bu yazılımcılara iş veriyor olması, başka yazılımcıları da Bitcoin üzerinde çalıştırmaya sevk edebilir, ki bu gayet Bitcoin'in yararına bir durum.

Sonuç

Her ne kadar yukarıdaki eleştirileri yazsak da, özünde Liquid kullanıcılara fayda sağlayan bir yapı. Riskler de katlanılabilir görünüyor. Bitcoin'in kullanan kişilerinin her birinin ondan beklentisi farklı. Kimi hızlı işlem yapmak isterken, kimi gizlilik kimi de baskılara karşı koyabilme özelliğini nedeniyle Bitcoin kullanıyor. Liquid hızlı işlem yapmak ve bu işlemler için yüksek komisyon vermek istemeyenlere uygun bir yapı. Bitcoin'in kurumsal yatırımcılar tarafından daha sık kullanılmasını sağlayacağı bunun sonucu da piyasadaki likiditeyi artırıcı bir faydası olacağı düşünülüyor. Yani özünde aynı Lightning Network gibi Bitcoin'in gelecekte geniş kitlelerce adaptasyonuna yardımcı olmaya çalışan bir araç. Başarılı olacaklar mı hep birlikte göreceğiz.

Bakkt kurumsal yatırımcıyı kripto paraya çeker mi?

Bakkt, kurumsal yatırımcılara Bitcoin üzerinden rahat alım satım yapacakları denetlenebilir bir ortam sunmayı hedefliyor. Başarırsa, kripto paralar geniş kitlelerce adaptasyonda bir eşiği daha atlamış olacak.

Bitcoin'in geniş kitleler tarafından kullanılmasına yardımcı olmaya çalışan iki yenilik Lightning Network ve Liquid'e geçtiğimiz iki bölümde değinmiştik. Şimdi de Ağustos ayında açıklanan ve gecikmeler nedeniyle 2019'un ilk yarısında faaliyete geçmesi planlanan Bakkt nedir ona bakalım.



Bakkt'ın sahibi kim?

Bakkt'ın en ilginç tarafı sahibi: New York Stock Exchange (NYSE)'in sahibi olan Intercontinental Exchange (ICE). Neden ilginç? Çünkü finans dünyasının kalbinin attığı Wall Street perde arkasında kripto paralara ilgi gösterip yatırım yapsa da, genel olarak bu yeniliklere hep şüpheci yaklaştı. Bu yaklaşımın pek çok nedeni var.

Ana nedeni henüz kripto paralar ile ilgili kanuni otoritelerin tavır almamış olması ile ilgili. Bir diğer neden de kripto paralara yatırım yapacak teknik altyapının olmaması (ya da henüz hazır hale gelmemesi). Zira Özel Anahtarlar ile sahipliğin değiştiği kripto paralar Wall Street'de yatırım yapan fonlar için risk barındırıyor ve bu riskleri yok edecek araçlar henüz ortaya çıkmadı.

Ama daha önemli bir nedeni Wall Street'in aslında güven hizmeti veren bir aracı olması. Ve ne diyoruz hep? Blockchain bazlı teknolojiler güven ihtiyacını kurumlardan alıp makinelere vererek aracıları ortadan kaldırmayı planlıyorlar.

Dolayısıyla, Wall Street kendisi için temelden tehdit unsuru olabilecek bu gelişmeye hep defansif bir şekilde yaklaştı. Ancak ICE'in Bakkt ile bu işe adım atması, artık potansiyel kârı kaçırma ve yeniliklerin gerisinde kalma baskısının bu tehdite karşı ağır bastığının bir kanıtı. Tabii, Bakkt'ın bir startup olduğunu unutmamak şartıyla (Bakkt 2019'un ilk günlerinde Boston Consulting Group, Galaxy Digital, Goldfinch Partners, ICE, Pantera Capital, Protocol Ventures and Microsoft'tan 182,5 Milyon ABD Doları yatırım aldığını da belirtelim). Yani ICE havuza balıklama atlamak yerine, şimdilik ayağını suya değdirerek bir nevi ortamı daha iyi anlamaya çalışıyor.

Peki Bakkt tam olarak ne yapmaya çalışıyor?

Temel olarak Bakkt kripto paraları Wall Street'in kullanımına uygun hale getirmeye çalışıyor. Şu anda kurumların kripto para ile işlem yapmaları oldukça zor. Bakkt geliştirdiği enstrümanlar ile kanuni otoriteler tarafından denetlenen bir ortamda kripto para ve diğer dijital varlıkların alım satımını kolaylaştıracak yapılar sunacak.

Bunun ne faydası var? Kanuni altyapıdaki boşluklar ve belirsizlikler nedeniyle kripto para piyasasına giremeyen milyarlarca dolarlık fonun, yönettikleri paranın ufak bir kısmını bile kripto paralara kaydırmasının iki ana faydası var. Birincisi normal olarak böyle bir para girişinin talebi artırıcı ve fiyatları yükseltici etkisi. İkincisi ise piyasaya likidite sağlanması, fiyatlardaki dalgalanmanın bir parça düşmesi. Toplumun yatırım anlamında en önemli kısmının da bu alana adapte olmasının sağlanması.

Peki ne tip bir hizmet sunuyor bu Bakkt derseniz: Öncelikle, Amerika'daki kanuni otoriteler yatırım fonlarının aldıkları varlıkların emanet hesaplarda tutulmasını isterler (ki paralar bir yere kaçıp bu fonlara yatırım yapan-özellikle emeklilik fonları-kişilerin paraları yanmasın diye). Şu anda kripto paralar için böyle bir emanet hesabı sistemi yok henüz. Bakkt, bu anlamda kanuni otoriteleri memnun edecek bir emanetçi/muhafız (custodian) olma yolunda çalışmalar yapıyor. Bu emanetçilik Bakkt'ın projelerinin en önemlisi ve diğer çıkarmayı planladığı ürünler için de bir altyapı olacak.

Bakkt'ın çıkarmayı planladığı bir diğer ürün ise şu: Vadeli işlemleri (Futures) duymuşsunuzdur. İleride belli bir tarihte belli bir varlığı alma ya da satma sözleşmesi. Örneğin "31 Aralık 2020 tarihinde 1 Euro'yu 1,2 ABD Doları karşılığı alacağım" gibi. Bakkt şimdi bu işlemlerin Bitcoin üzerinden yapılmasını da sağlıyor.



Bakkt'ın diğer ürünleri konusunda 2018 yılının Ağustos ayında İsmail Hakkı Polat da güzel bir makale yazmıştı. Bakkt, Starbucks ve Microsoft gibi iş ortaklarına "dijital varlıkların alım satımına" fayda sağlamak hedefine uygun olarak alışveriş sistemlerinde kullanacakları ürünler kurguluyor.

Bakkt konusunda ne tip çekinceler var?

Ancak Bakkt konusunda kripto para piyasalarında ciddi çekinceler var. Aslında çekinceler Bakkt'ın kendisinden ziyade Wall Street'e. Bitcoin'in doğuş nedenlerinden birinin 2008 yılında Wall Street'den kaynaklanan ekonomik kriz olduğunu düşünürsek kuşku duymakta haksız sayılmazlar. En önemli karşı argüman 22 yılını Wall Street'de geçirmiş şimdilerde ise kripto paralar konusunda en saygın isimlerden biri olan Caitlin Long'dan geldi. Biliyorsunuz Wall Street denince aklımıza hisse senedi piyasaları geliyor. Halbuki dünyadaki tüm sermaye piyasalarının toplam değeri 77 Trilyon ABD Doları iken asıl büyük pazar Türev Piyasaları. Bu pazar 532 Trilyon ABD doları ile yaklaşık 7,5 katı sermaye piyasalarının.

Türev piyasaları işlev olarak bir aktifi baz alıp onun üzerine çıkarılan farklı borçlanma araçlarını temsil ediyor. Burası aslında oldukça riskli bir pazar. Zira, aslında paradan para yaratılıyor, ciddi bir genişleme yaratılıyor ve bu pazarın ciddi bir denetleyicisi yok. Bu nedenle riskler çok yüksek, özellikle kriz zamanlarında. 2008 yılında emlak piyasasında başlayan kriz tüm ekonomiyi tehdit eder hale gelirken, özünde emlağa dayalı borçlanma senetleri vardı. Amerika'nın çeşitli yerlerindeki taşınmazlar ve onlara atfedilen değerlere dayanılarak çıkarılan türev enstrümanlar, sonrasında bu taşınmaz değerlerinin şişirilmiş olduğunun anlaşılması ve talebin de azalmasıyla birlikte, çöp haline gelmiş ancak türev ürünler oldukları için ekonomi üzerinde emlak değerlerinin kat be kat fazlası tahribat yaratarak krize neden olmuşlardı.

Türev piyasaları hisse piyasaları ile karşılaştırılmasından da anlayabileceğiniz üzere Wall Street tarafından çok sevilen bir enstrüman. Normalde Wall Street yatırım ya da ticaretini yaptığı enstrümanlar üzerinde hüküm kurmayı sever.

Örneğin halka açık bir şirketin hisselerinin eğer ufak bir payı halka açık ise o hisse gerçek değerini nadiren bulur. Hissenin çoğunluğu halka açık ise o zaman fonların şirketi ele geçirme şansları da artacağı için o şirketin hissesi daha değerlenir. Bu Wall Street'in şirketi kontrol etme ve kâr ettirme yöntemlerinden biri. Bir diğer yöntem de türev piyasalarında hisse ya da herhangi bir varlık üzerinde spekülasyon yapmak.

Bitcoin örneğinde bakarsak, Wall Street'in Bitcoin hisselerinin çoğunluğunu ele geçirmek gibi bir şansı yok. Örneğin hisse senetlerinin sadece NYSE'de işlem görmesini sağlayabilirsiniz ama Bitcoin için bu geçerli değil. Bitcoin satın alarak üzerindeki etkinliğinizi artırmak isteseniz fiyatı arşa çıkar; çok mantıklı değil. Ama işte yukarıdaki gibi vadeli işlem borsasında Bitcoin'i kullanmaya başlarsanız o zaman aslında bir nevi Bitcoin fiyatını daha kontrol eder hale gelebilirsiniz. Hele bir de aşağıda bahsedeceğimiz şekilde bu türev piyasalarını büyütmeye kalkarsanız hem fiyatı kontrol edersiniz hem de Bitcoin'e bağlı riskleri artırmış olursunuz: Türev ürünler belli bir varlığa dayandırılarak yaratılan borçlanma enstrümanları demiştik. Eğer türev ürünleri yaratırken karşılığında gerçekten Bitcoin tutuyorsanız bir sorun yok (ki Bakkt şu an için vadeli işlemlerinde Bitcoin'i karşılık olarak tutacağını belirtiyor).

Ancak Wall Street benzer başka türev ürünlerinde karşılık olarak her zaman bir varlık tutmuyor. Türevi yaratan kurumların bu varlığı elinde tutması yerine, yukarıdaki bahsettiğimiz fonların elinde tuttukları emanet hesaplarındaki varlıkları "ödünç alma"larına olanak veriyor. O zaman da yukarıda bahsettiğimiz 2008 krizi benzeri riskler kat be kat artıyor.

Burada Bitcoin özelinde türev piyasalarının ne kadar etkili olacağı ile ilgili birkaç konuya değinmek gerek: Kanun koyucular diğer varlıklarda olduğu gibi Bitcoin'de de emanet hesaplardaki dijital paraları ödünç alınmasına izin verecekler mi?

Ödünç alma dediğimiz olay Bitcoin için kritik. Zira fiziksel olarak herhangi bir elle tutulur özelliği olmayan Bitcoin'e sahip olmanın tek yolu o Bitcoin'i taşıyan adresin Özel Anahtarı'na sahip olmak. Siz bir fon olarak emanet hesabınızdaki bir varlığı ödünç verdiğinizde Özel Anahtarı da verecek misiniz? Oldukça riskli.

Öte yandan Bitcoin'i şu an elinde tutanların büyük bir kısmının HODL'ler dediğimiz uzun vadeli ve Wall Street ile arası çok da iyi olmayan bir topluluk olduğunu söylersek yukarıdaki gibi emanet hesaplar vasıtasıyla yaratılabilecek türev araçlarının büyüklüğü o kadar da yüksek olmayabilir ve Bitcoin üzerinde korkulduğu gibi bir kontrol ya da risk oluşturmayabilir.

Sonuç

Bakkt, Wall Street'in Bitcoin'i kullanmak (ve belki de kontrol altına almak) için giriştiği ilk adım. Özellikle kurumsal yatırımcılara sağladığı faydalar nedeniyle kısa vadede Bitcoin'e değer katma ihtimali yüksek. Uzun vadede, Wall Street onu kendi dümenine kullanır ve üzerinde yaratacağı türev enstrümanlar ile kontrol altına alıp değerini potansiyel olarak düşürücü aksiyonlara girer mi, onu da hep birlikte göreceğiz. Ne olursa olsun, Bitcoin'in bir köşede duran 'tu kaka' alternatif bir yatırım aracı olarak kalmasındansa, büyük fonların yatırım yapabileceği 'aşina' bir araca dönüşme ihtimali olumlu bir gelişme.



MADENCİLİK 2.0: beyaz *yakalıdan* **madenci** olur mu ?



Yeni nesil teknolojilerin gelişmesi için her kesim çaba gösteriyor. Bunlardan biri de bu alana yatırım yapmış kurumsal yatırımcılar. Özellikle girişim sermayeleri iş yapış biçimlerini değiştiriyorlar. Gelin bir göz atalım neler yaptıklarına:

Yeni teknolojilerin geniş kesimlerce adapte edilebilmesi için pek çok girişim var. Bunlardan Lightning, Liquid ve Bakkt'a geçmiş bölümlerde değinmiştik. Şimdi bu trendlerden gelecekte daha da önem kazanacak olan bir tanesine, kurumsal yatırımcıların kafa yorduğu Generalized Mining (ya da Mining 2.0) kavramına bakalım birlikte.

Yatırımcılık değişiyor, neden?

Hatırlarsanız geçmiş bir bölümde yeni teknolojiler ile değişen girişimcilik ve yatırımcılık tanımlarından bahsetmiştik.

Kısaca özetlersek, değişen teknolojiler ile birlikte bir şirketin yarattığı katma değer artık sadece şirket kurucuları ve yatırımcıları tarafından değil diğer başka aktörler tarafından da paylaşılıyor.

Bunun temel nedeni ise 'artık yeni teknolojiler ile bir şirket değil bir ekosistem (bir ağ) yaratılıyor'. Ve yeni teknolojilerin geçmişe göre devrim niteliği taşıyan ana özelliği, yarattıkları ekosistemdeki tüm oyuncuların oyuna devam etmesini sağlamak için kurdukları teşvik mekanizmaları.

Peki kim bu diğer oyuncular? Madenciler ve son kullanıcılar.

Neden? Öncelikle bir Blockchain sisteminin, birbirinden bağımsız makineler tarafından işletilmesini istiyorsanız bu makinelere harcadıkları efor ve enerjinin karşılığını vermelisiniz, aksi halde neden uğraşsınlar?

Keza benzer şekilde sistemin kullanıcıları da artık harcadıkları vakit karşılığı sadece sistemin sunduğu kolaylıklardan faydalanmak ile yetinmiyorlar. Onlar da ortaya çıkan pastadan pay istiyorlar, ki sistemi kullanmaya devam etsinler ve büyümesine yardımcı olsunlar.



Sonuçta eskiden girişimlere erken yatırım yapan kurumlar (VC'ler-girişim sermayeleri) koydukları para ve aldıkları riskin karşılığı olarak ciddi bir oranda şirket hissesi alarak ortaya çıkan değerin büyük bir kısmını uhdelerine alıyorlar idi. Şimdi ise yeni teknolojiler ile pastadan pay alanlar çoğaldığı için girişim sermayeleri de iş yapma biçimlerini değiştirmek durumunda kalıyorlar.

Konu ICO'lar mı? Hayır

Yukarıda bahsettiğimiz bölümde girişimler için girişim sermayelerine alternatif olarak ortaya çıkan ICO piyasalarından bahsetmiştik. 2018 yılı içinde girişimlere ciddi miktarda finansman sağlayan ICO piyasaları yılın sonuna doğru tabiri caizse kurudu. Bunun pek çok nedeni var: en önemlisi, girişim adı altında ortaya çıkanların çoğunun aslında bu yaratılan heyecanı kullanan hayal tacirleri ya da dolandırıcılar oldukları ortaya çıkması.

Ama benzer durum internet girişimlerinin ilk çıktığı 90'larda da yaşanmıştı, o zaman da çok para battı ancak girişimler yatırım almaya devam ettiler. İlk yaşanan balon söndükten sonra özellikle gerçekten değer yaratan girişimlere uzun vadeli yatırım yapanlar çok ciddi getiriler elde ettiler.

Dolayısıyla şu an ICO pazarı tıkanmış olabilir ancak yeni mekanizmalar ile ileride tekrar canlanması çok muhtemel. Yine de ICO pazarının kuruması klasik anlamdaki risk sermayelerinin artık eskisi gibi at koşturabileceği anlamına gelmiyor. Çünkü oyun değişti. Ne gibi? Bahsedelim.

Girişim Sermayesi'nin faydası ne?

Bir risk sermayesi şirketi girişime sadece para vermez. Bunun dışında pazar bilgisi ile girişimin yönünü etkiler. Ya da organizasyonel tecrübesi ile şirketin büyümesi sırasında kontrolü kaybetmemesi için ne tip insan kaynağı ya da organizasyon yapısına gitmesi gerektiği konusunda girişimciye yardımcı olur.

Ancak yeni teknolojiler ile girişim sermayesi artık sadece girişim ile değil aynı zamanda ekosistemle de ortak oluyor. İşte bu nedenle eskiden şirketi etkilemek ve yönlendirmek için kullandığı çabayı artık ekosistem için de göstermeli.

Girişim Sermayesi başka neler yapabilir? Madencilik 2.0'a hoş geldiniz!

Peki neler yapabilir Girişim Sermayeleri bu alanda? Örneğin madencilik işine girebilirler! Şaşırtıcı değil mi?

Peki yapabilirler mi? Neden yapamasınlar? Eğer açık (public) bir Blockchain sisteminden bahsediyorsak, isteyen herkes madenci olabilir. Girişim Sermayesi şirketi de bu sistem içinde kendisi madencilik yapabilir ya da spesifik girişiminin yarattığı ekosistemde madencilik yapan bir şirkete yatırım yapabilir.



Girişim Sermayesi neden madencilik yapsın?

Girişim sermayeleri neden böyle bir işe kalkışsınlar? Birkaç nedeni var:

Öncelikle, hatırlayalım; madenciler sistem içindeki işlemleri gerçekleştiren ve aynı zamanda çeşitli protokoller ile (PoW gibi) sistemin güvenliğini sağlayan aktörler. Girişim sermayesi açısından eğer uzun vadede bir getiri hedefleniyor ise bu değeri yaratacak olan ekosistemin kesintisiz bir şekilde yaşaması ve dış tehditlerden korunması hayati öneme sahip.

Bir yandan da madenciler ekosistemin gidişatı konusunda sınırlı da olsa söz hakkına sahipler. (genellikle uzlaşma sonucunda tamamlanan blokların içinde yarattıkları tokenlar sayesinde) Birçok ekosistemin nasıl yönetileceğine o sistemin yarattığı token'ları ellerinde tutanlar karar veriyor. Ne kadar token o kadar söz hakkı.

Benzer şekilde, özellikle bu sistemlerin açık kaynaklı olması nedeniyle çok sık rastlanmasa da kimi durumlarda sistemler klonlanarak (hard fork) farklı adlar altında strateji değiştirebiliyor ya da farklı bir grubun kontrolü altına girebiliyorlar. Bu tip hard fork durumlarında ekosistem içindeki her bir aktörün bu iki gruptan hangisinin içinde yer alacağına karar vermesi gerekiyor.

Böyle bir durum ortaya çıktığında oyuncular genelde çoğunluğa uyarlar, bu işin doğası böyle.

Girişim sermayesi de madenciler arasında kendine pay alarak yukarıdaki iki durumda çoğunluğu etkileme ve stratejiyi belirleme konusunda kendisine bir avantaj yaratıyor.

Ama daha da önemlisi, madenciler yaptıkları çalışmaların karşılığını maddi olarak token şeklinde alıyorlar. Girişim Sermayesi de benzer şekilde madencilik yaparak token kazanabiliyor. Kimi durumlarda yaptığı yatırımdan elde ettiği getirinin çok daha fazlasını bu tip madencilik faaliyetinden alabiliyorlar, özellikle token değerinin yükseldiği zamanlarda.



Girişim Sermayeleri artık teknik açıdan da gelişmek zorunda mı yoksa?

Kurumsal yatırımcılar, yeni teknolojiler karşılığında klasik anlamda iş yapış biçimlerini ciddi şekilde değiştirmenin yanında ağır bir teknik bilgi birikimine de ihtiyaç duyuyor.

Örneğin yukarıda bahsettiğimiz madencilik işi öyle basitçe anlaşılacak gibi değil. Daha doğrusu işi layığı ile yapmak istediğinizde ciddi bir teknik donanıma ihtiyacınız var. Kullanacağınız makineler için yüklü bir yatırım yapacaksınız, sonra enerji harcayacaksınız? Sonra yatırımı nereye yapacaksınız, maliyetler nerede düşük?

Ayrıca her Blockchain kendi özelinde farklılık gösteriyor, madencilik olarak da öyle. Gerekli altyapı farklı, enerji ihtiyaçları farklı.

Bunların hepsini iyi anlamak ve hesaplamak gerekiyor. Bu nedenle bu alana yatırım yapan ve akıllı davranan Girişim Sermayeleri ekiplerini artık teknik donanıma sahip (kimi yazılım kökenli) üyeler ile güçlendiriyorlar.

Sonuç

Siz bakmayın öyle "ICO piyasaları kurudu, kripto paraların geleceği yok" gibi söylentilere. Hep söylediğimiz gibi yeni teknolojilerin sunduğu vizyonların birçoğu ulaşılabilir. Ancak bu vizyonlara ulaşmak için gerekli altyapılar henüz yok ve bu alanda çalışmalar tüm hızıyla sürüyor.

Aslında kripto paraların fiyatlarının düşmesi konuya uzun vadeli yaklaşanlar için rahatlatıcı bile oldu. Zira sürekli yükselen fiyatlar, değer yaratmaktan ziyade spekülasyon yapan yatırımcıların piyasayı doldurmasına, yazılımcıların da akıllarının sürekli yükselen fiyatlarda olmasına neden oluyordu. Artık bu spekülatörler piyasadan çekildi (gerçi fiyatlar bir yükselmeye başlasın, ilk onlar geri gelecekler).

Pek çok kurumsal yatırımcı ve girişim sermayesi konuya uzun vadeli bakmaya devam ediyor. Bu yatırımcılar bahsedilen vizyonların gerçekleşmesi için gereken altyapı ve yazılım çalışmaları devam ederken sistemin devamını sağlamak için madencilik dahil her yolu deniyor. Tavsiyem siz de onlar gibi konuya uzun vadeli değer yaratma perspektifinden bakmaya çalışın… ve Çetin Altan'ın dediği gibi "Enseyi karartmayın" …

Ethereum ve diğer kriptoparalar

dünyanın en BÜYÜK *bilgisayarı* Ethereum'un *hikayesi* NE?



Bitcoin dışında en bilinen kripto para Ethereum'un parası olan Ether. Yaratıcısı da 18 yaşında bir genç. Ancak bu genç Ethereum'u kripto para olsun diye yaratmamış. Çok daha iddialı hayalleri var.

"Birbirine bağlı binlerce makine" diyoruz uzun zamandır. Bu makineler bağımsız bir şekilde çalışarak, güvenli tek bir yere bağlı olmayan sistemler içinde kırılıp bükülmeyen, geriye doğru değiştirilemeyen sistemler yaratıyorlar. Bu da güvenin en çok ihtiyaç duyulduğu alan olan para ve onun dijital transferi anlamında dünyada kabul görmüş.

Bu birbirine bağlı binlerce makinenin böyle geniş ortak bir defter ile kayıt tutma dışında başka güçleri de var tabii. İşte bu güçleri kullanmak için yola çıkan sistemin adı Ethereum. Çok kabaca ifade edersek bu binlerce makinenin bağlı olduğu dünyanın en büyük bilgisayarı olma iddiasında Ethereum. Detaylarına bakacağız ama ilginç bir hikayesi var Ethereum'un, kısaca bahsetmekte fayda var.

Vitalik Buterin: 18 yaşında bir dahi mi?

Bitcoin'in ortaya çıkışından birkaç yıl sonra, 2011 yılında Rusya'dan Kanada'ya göç etmiş bir ailenin babası, 17 yaşındaki oğluna Satoshi'nin işlerinden ve Bitcoin'den bahseder. Babasının bahsettiklerinden büyülenen Vitalik Buterin adındaki bu genç kendini bir anda bu dünyanın içinde bulur. Önce arkadaşları ile Bitcoin Magazine diye bir dergi kurarlar. Teknoloji, yazarlık ve matematik konusundaki yetenekleri ile oldukça etkili olur. Zaten rivayete göre üç basamaklı rakamları aklından normal bir insanın iki katı hızda çarpma yeteneğine sahip bu genç, henüz 18 yaşında Uluslararası Enformasyon Olimpiyatları'nda Bronz madalya kazanarak yeteneklerini global platformda da gösterir.

Buterin, öncelikle Bitcoin üzerinde gelişmeler yaparak, Bitcoin transferi dışında daha başka pek çok fonksiyonu (para dışı varlıkları gönderme, dijital kontrat yaratma gibi) bu sisteme geçirmek için uğraşır. Ancak bu konuda oldukça zorlanır.



Zira Bitcoin özelliği itibariyle tek işi (o da para gönderme) iyi yapmak üzere kurgulanır. Geliştiricilerinin aklındaki tek konu "Bitcoin'i nasıl dış tehlikeler karşı daha güvenilir yaparız?" sorusuna cevap bulmaktır, yenilikler öncelikleri arasında değildir (hala da öyle, en gurur duydukları konu bu: Bitcoin 2009'dan beri bir kez bile tökezlemedi ve "hack" edilemedi diye göğüslerini gere gere ortada dolaşıyorlar). Buterin'in kafasında ise paranın bir yerden öbürüne geçtiği işlemleri tutan hesap makinesi benzeri bir fonksiyondan çok, daha pek çok işlemi yapabilecek bir dünya bilgisayarı vizyonu vardır.

Ethereum nasıl ortaya çıkmış?

2013 yılında Buterin 15 yazılımcı arkadaşı ile birlikte Ethereum'u tanıtır. Ama henüz ortada sadece bir konsept tasarım vardır?—?para kazanılacak ya da yatırım alabilecek bir ürün için henüz erkendir. Tam o sırada Peter Thiel (bilenler bilir; PayPal'in kurucularından, Facebook'a ilk para yatıran kişidir kendisi) onlara 100.000 ABD Doları burs verir. Derler ki bu bursu almak ABD'nin en iyi üniversitelerine girmekten bile zordur. Tabii sadece bu da değil, aynı zamanda Buterin, 2014 yılı içinde Etherum ile Dünya Teknoloji Ödülü'nü de alır.

O yıl, Enerji dalında Elon Musk, Medya alanında meşhur Walter Isaacson, Teknoloji alanında ise Buterin ile birlikte bu ödüle layık görülen diğer kişiler olurlar.

Ödüller karın doyurmuyor, var mı yatırım yapacak?

Peter Thiel'in bursu ekibin daha olgun bir ürün oluşturma anlamında yol almasına yardımcı olsa da yeterli olmaz. 2014 Eylül ayında ilginç bir yöntem ile para toplarlar. Derler ki, "ilk iki hafta 2.000 Ether = 1 Bitcoin olacak şekilde para topluyoruz, sonrasında bu rakam yavaş yavaş düşecek en son alanlar 1.337 Ether = 1 Bitcoin şeklinde alacaklar". Daha önce denenmemiş bir yöntem, zira bildiğimiz Dolar ya da Euro para toplamıyorlar, Bitcoin topluyorlar! O zamanlar Bitcoin çok az biliniyor. Herhangi bir regülasyona da tabii değil. Ama zaten ortada satılan bir şirket de yok neye tabii yapacaksınız ki? Karmaşık bir süreç ama nispeten rahat. İsviçre'de bir vakıf kurarak bu vakıf üzerinden satış yaparlar ve o zamanın parası ile 18,5 Milyon ABD Doları toplarlar. Bu bir ether için ortalama 0,31 ABD doları demek. Etherin şu anki fiyatının yaklaşık 500 ABD doları olduğunu söylersek, o zaman yatırım yapanların şu anki karlarını hesaplamak da size kalsın (ya da boşverin biz söyleyelim, koydukları paranın yaklaşık 1.600 katını kazanmış durumdalar).

Yukarıda bahsedilen toplanan paranın tamamının geliştiricilere verilecek ödüller ve maaşlar ile, Ethereum Vakfı'nın destekleyeceği Ethereum ve Kripo dünyası ile ilgili projeler için harcanacağını belirtelim. Bu şekilde satılan etherin yanında, bu miktarın onda biri kadar bir rakam da kurucular için ayrılmış. Yani, daha önceki bölümlerimizde bahsettiğimiz, şirket kurucularının şirketin büyük kısmına sahip olmalarının yerini, bu yeni modelde, para toplamak için satılan etherin ufak bir kısmına baştan sahip olmak almış. Bu da bir yenilik.

İşte bu şekilde etkili bir başlangıç hikayesine imza atar Ethereum. Peki ama ne işe yarar Ethereum? Ona da bir sonraki yazımızda bakalım artık.

Ethereum'un çıkış ve inişi bir döngünün mü parçası?

Girişimlerine para toplayan girişimciler son iki yıldır ağırlıkla Ethereum altyapısını kullandılar. Bu da Ethereum'un parası ETH'yi çılgın seviyelere çıkardı. Ancak sonrası hüsran. Neden böyle oldu?…

Özellikle ICO piyasalarının ve piyasaya çıkan binlerce kripto paranın performansının kötü gitmesi bu alanda konuşan, fikir üretenlerin morallerini bozdu. Kötü gitmesi derken kastettiğimiz şu: 2017 yılında başlayıp 2018 yılında doruk noktasına ulaşan kripto para balonunda (hype da denebilir), balonu oluşturanların büyük kısmı kısa vadeli yatırımcılar oldu. Bu tip yatırımcılar genelde çok detaylı araştırma yapmadan, etraflarında duydukları ya da Twitter benzeri yerlerde gördükleri "gaz" hesaplardan etkilendiler.

Neden bahsediyoruz? Kim bunlar?

Netflix'de izleyebileceğiniz Peaky Blinders dizisinde güzel bir hikaye var. 1920'lerin başında geçen dizinin Cillian Murphy 'nin canlandırdığı baş kahramanı bahis işi yapan Thomas Shelby yarışa sokacağı bir atı bir Çinliye götürerek herkesin ortasında hayvana büyü yaptırır. Aslında Shelby hayvanın zaten iyi olduğu için yarışı kazanacağını biliyordur. Hayvan yarışı kazanır ve insanlar "büyü" yüzünden kazandığını söyler. Olay kulaktan kulağa büyü yavaş yavaş tüm Birmingham'a yayılır. At ikinci yarışında da kazanır bir hafta sonra. Sonra bir daha. Ta ki insanlar ellerinde ne var ne yok satıp bir sonraki yarışta yine aynı ata yatırana kadar… At o hafta kaybeder. İnsanlar tüm varlıklarını yitirirler. Thomas Shelby ise parayı koyacak yer bulamaz. Maalesef ülkemiz de dahil tüm dünyada 2018 yılının başında büyük bir çoğunluk 1920'lerde Birmingham halkının başına gelen bu olayın benzerini yaşadı.

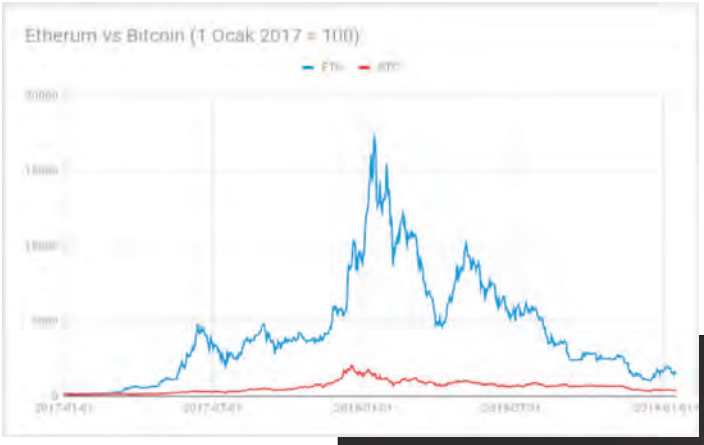
Arkadaşının para kazandığını görenler, hesapsız kitapsız anlamadan para yatırdılar bilmedikleri paralara. Oysa aslında para toplayanların ciddi bir kısmı ponzi scheme benzeri programlar ile insanlardan para toplayan ama ne yapmak istedikleri çok da anlaşılmayan projeler idi. Bu projeleri şimdilik bir kenara bırakalım.



Her projeye de Ponzi denmez ama değil mi?

Performans olarak kötü gitmesine rağmen aslında belli bir vizyona sahip olan pek çok proje de piyasaya geçtiğimiz yıl. Ancak hep söylediğimiz gibi bu projelerin vakte ihtiyacı var. Zira, olgunlaşabilmeleri için hem yazılımcılarının uzunca bir süre bu projeler üzerinde çalışması hem de bu projelerin üzerine inşa edildikleri teknik altyapıların gelişmesi gerekiyor.

Ethereum parası ETH 2017'de neden yükseldi? Bu alanda çalışan pek çok proje özellikle para toplamak konusunda Ethereum'un altyapısını kullandılar. Bu durum özellikle 2017 yılında Ethereum'a korkunç yaradı. Zira, herhangi bir yatırım için token almak isteyen bir yatırımcı elindeki itibari parayı (USD, Euro her ne ise) bozduruyor ve Ethereum alıyordu. Bu da Ethereum'a olan talebi ve para birimi olan ETH'nin fiyatını inanılmaz derecede yükseltti. ETH üzerinden para toplayan girişimler, ETH'deki artışı gördükçe kazandıkları fonları ETH'de tutmaya devam ettiler, çünkü en iyi getiri ETH'de idi! Böylece kendi kendini besleyen bir sanal sarmal oluştu.



Ethereum ve Bitcoin'in son iki yıldaki seyri (Kaynak: Coindesk)



Peki 2018'de neden çakıldı?

Ancak 2018 yılının ikinci yarısında rüzgâr tersine döndü. Yapılan ICO'lar sonrası umduğunu bulamayan yatırımcılar "zararın neresinden dönersek kardır" mantığı ile ellerindeki tokenları sattılar. Bu satışın ETH üzerinde çok etkisi olmadı, zira token satan yatırımcı ya kendi itibari parasına ya da Bitcoin'e döndü. Ama ETH'yi asıl vuran, ICO yaparak ETH toplayan girişimler oldu. Çünkü bu girişimler, bir yandan yatırımcıları çizdiği vizyon karşılığı gelir getirmeyi başaramazken diğer yandan da devam eden masraflarının karşılığı ödeme yapmak zorunda olduklarından yavaş yavaş ellerindeki ETH'leri satmaya başladılar. Bu da ETH üzerinde 2017 yılında yaşananın tam tersi bir sanal sarmal yarattı.



Yukarıdaki tabloya 2018 başından bakınca düşüş daha iyi anlaşılıyor.

Bir sarmal içinde miyiz?

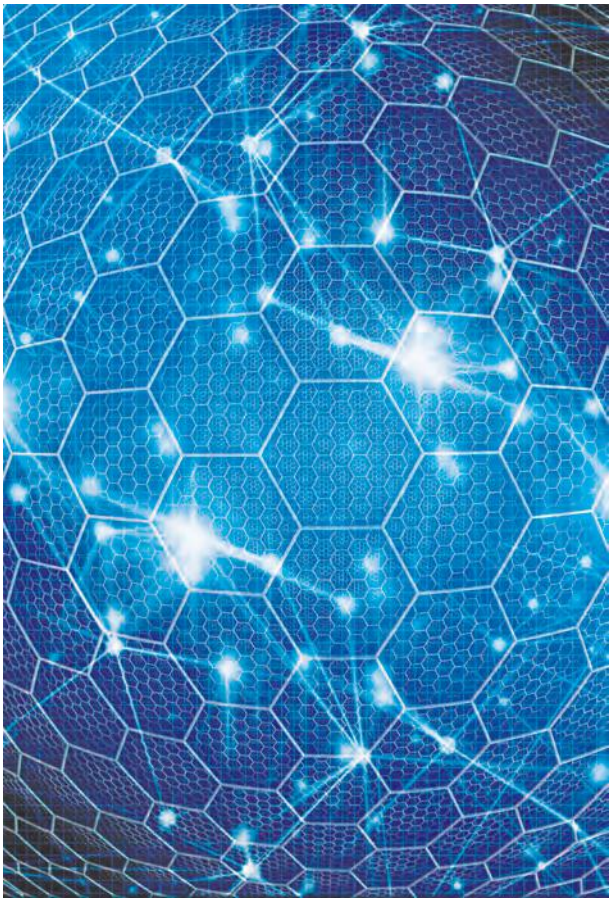
Peki bu böyle mi devam eder. Bu işlerin aslında bir daire çizdiğini söylemek belki daha doğru. Bu alanda yazılmış en iyi kitaplardan Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond'un[93] yazarı Chris Burnske[94]'nin Ocak 2019'da attığı şu tweet dikkat çekici:



Çok geniş bir genelleme bu. Ancak olaya kısa vadeli değil uzun vadeli bakanlar ve işin içinde başından beri bulunanlar için aslında yaşananlar oldukça tanıdık. O nedenle, bu alanda çalışan pek çok kişi "biz bu filmi görmüştük" diyor ve ileride gerçekleşecek yeni döngüyü üst seviyede yakalamak için var güçleriyle çabalıyorlar.

Sonuç

Şu anda Kripto Dünyası hala çok küçük. Tüm piyasa toplam değeri yaklaşık olarak 170 Milyar ABD Doları[95]. Sadece Apple'ın kasasında duran nakit paranın 158 Milyar ABD Doları[96] olduğunu söylersek aslında ne kadar küçük bir pazardan bahsettiğimiz daha anlaşılır oluyor.



O nedenle, bu pazarın bize sunduğu vizyonun bir parçasının bile gerçekleşeceğini düşünsek ileride bu pazarın çok çok daha büyüyeceğini söylemek kâhinlik sayılmaz. Geçtiğimiz yılki çılgınlık sonrası hala girişimleri üzerinde çalışanlar ve daha ötesi yatırım almaya devam edenler, kendi sundukları vizyonun bir şekilde gerçekleşeceğinden eminler. Artık soru daha çok "ne zaman?" üzerine odaklanıyor.

93https://www.amazon.com/Cryptoassets-Innovative-Investors-Bitcoin-Beyond/dp/1260026671/
94https://twitter.com/cburniske
95https://coinmarketcap.com/charts/
96https://www.cultofmac.com/272570/apples-cash-reserves-30x-10-years-ago/



akıllı kontrat OLUR MU?

Ethereum ve Akıllı Kontratlar Ethereum'un dünyayı değiştirme vizyonunu hayata geçirebilmesi için ihtiyaç duyduğu en önemli yardımcılardan biri "Akıllı Kontratlar"

Diğer bölümlerde, Kripto dünyasında hepimizin duyduğu Bitcoin ve benzeri kripto paralar dışında başka konuların da olduğundan bahsediyor ve bu başka dünyaların içinde en önemlisi olan Ethereum'un tarihçesine değiniyoruz. Şimdi ise, Akıllı Kontratlar nedir, ne işe yarar ona bir bakalım arzu ederseniz.

Akıllı Kontrat ne demek?

Ethereum dünyasına girmeden önce bir tanıma daha bakmakta fayda var.

Ofistesiniz, karnınız acıktı. Dışarı çıkıp markete gidecek zamanınız yok. "Alt katta bir otomat var, oradan bir bisküvi alayım açlığımı bastırsın. Şurada bir yerde birkaç bozuk para olacaktı" Gittiniz, parayı otomata attınız, otomat da size istediğiniz bisküviyi attı. Tebrikler! Bir Akıllı Kontrat işlemi gerçekleştirdiniz!

Şaka değil, gerçekten de belki de bir yerde kulağınıza çalınan "Akıllı Kontrat" aslında tam bu. Akıllı denmesinden dolayı çok karmaşık ya da derin bir kavram bekliyorsunuz ama öyle değil. Tam tersine…



Akıllı Kontrat ile bahsedilen, önceden kuralları konmuş, iki tarafın bu kurallara bağlı olarak anlaştıkları koşulların gerçekleşmesi durumunda kendi kendine yürürlüğe giren işlem. Yukarıdaki örnekte, siz biliyorsunuz ki, makineye para attığınızda bisküvi alacaksınız. Makine de benzer şekilde programlanmış ve içine para atılıp seçim yapıldığında otomatik olarak o işlemi gerçekleştiriyor.

Neden akıllı kontrat deniyor o halde? Şu nedenle: İki kişi herhangi bir şekilde aralarında 'normal' bir kontrat yaptığında taraflardan biri "yok efendim, şöyle böyle oldu da ben vazgeçtim" gibisinden bir bahane altına saklanıp sözünü yerine getirmeyebilir. Ondan sonra araya girsin avukatlar, gerekirse yargı ve işin içinden çıkmaya çalışsınlar.

Akıllı kontratın asıl gücü işte burada ortaya çıkıyor. Akıllı kontrat öyle çok karmaşık kurallar vesaire öngörmüyor, tam tersine oldukça basit.

Ama akıllı kontratın asıl gücü, karşı tarafın işlemi yapacağına emin olmamızdan kaynaklanıyor. Zira koşullar otomatik olarak bir yazılım içinde olduğu için, o koşul gerçekleştiği anda, iki taraf için de belirlenen sonuç ne ise, o otomatik olarak gerçekleşiyor.

Bakın Bitcoin ya da diğer Blockchain bazlı teknolojilerde bahsettiğimiz "güven" konusuna yine geldik. Önceki bölümlerde bu yeni sistemler sayesinde, 'güven eksikliğinin neden olduğu merkezi bir otorite ya da aracıya duyulan ihtiyaca' artık gerek kalmadığını yazmıştık. Akıllı kontratlar ile de ikili ilişkilerde karşı tarafın sözünü yerine getireceğine dair duymamız güven ihtiyacı ortadan kalkıyor.

Ethereum dünyasında Akıllı Kontratlar ne gibi bir yer kaplıyor?

Aslında akıllı kontratlar uzun zamandır bilinen bir kavram-aynı otomatların uzun süredir hayatımızda olması gibi. Şu anda en bilinen kripto para Bitcoin de örneğin adı verilen bir akıllı kontrat diline sahip. Ancak bir önceki bölümden hatırlayabileceğiniz gibi, daha çok dijital olarak bir varlığın bir taraftan diğerine transferinde kullanılan Bitcoin ve geliştiricileri sadece Bitcoin'in dijital para özelliğine odaklanmayı tercih etmişlerdi. Ethereum'un kurucusu Vitalik Buterin ise Blockchain sistemlerini sadece para değil daha pek çok fonksiyon için kullanmak istiyordu. Bu fonksiyonlar, dijital bir varlığın bir kişiden diğerine aktarımından tutun, her tür dijital hizmetin değişik yerlerdeki bilgisayarlar aracılığıyla verilmesine kadar uzanan geniş bir yelpazedeler.

Bu tip bilgisayarlar arasında verilecek hizmetler ve bu hizmetler karşılığında bir ödeme yapılabilmesi için bu makinelerin ortak kabul ettikleri bir kurallar bütünü ve sözleşme olması gerekiyordu. İşte, Ethereum bu tip değişik makineler arasında yapılacak işlemler ve bu işlemlerin bağlı olacağı akıllı kontratlar için bir altyapı platformu olarak ortaya çıktı.



Birbirinden uzak ve bağımsız makinelerin kendilerinden uzak olarak verilen işi yapmaları sayesinde Ethereum dünyanın en büyük bilgisayarını insanların emrine veriyor. Yazılımcılar, bu dünyanın en büyük dağılmış bilgisayarı üzerinde çalışacak programlar yazabilecekler. Makineler bu işlemi yaptıklarında ise karşılık olarak ETH denen para birimini alıyorlar-buna yakıt da deniyor (aslında aralarında alışveriş için kullandıkları bu nesneye gas diyorlar ama gas daha çok bilinen ETH'ye bağlı olduğu için basitleştirmek adına bu şekilde bilsek yeter). Yazılımcılar da sistemi kullandıkça ETH ödüyorlar. Bir nevi yazılımcıları basit ve verimli kod yazmaya iten bir sistem, zira ne kadar verimli olursanız sisteme o kadar az para ödeyeceksiniz.





Ethereum üzerine kurulmuş olan yüzlerce yazılım var. Aynı Apple'ın işletim sistemi üzerine Apple Store'dan satın aldığınız uygulamalar gibi…

Bunlara kısaca dApps deniyor. Pek çoğu henüz sahneye çıkmak için hazır değiller. Ama Türkiye'de ve dünyada Blockchain üzerine kurulan girişimlerin büyük çoğunluğunun Ethereum altyapısını kullandığını söylemek mümkün.

Bir yandan da şunu belirtmekte fayda var: Bitcoin genel olarak insanlar arasında parasal bir değerin transferi için kullanılırken, Ethereum bilgisayarlar ve kişiler arasında bilginin ve hizmetlerin gönderilebilmesi amacıyla kurulmuş. Dolayısıyla, "Bitcoin için bir kripto para demek doğru iken Ethereum için bir KriptoEmtia demek daha doğru olacak" der Chris Bunske KriptoVarlıklar (CryptoAssets) adlı kitabında. Bu da oldukça önemli bir ayrım ve şu aralarda da özellikle ABD'de zihinleri meşgul eden konulardan biri. Zira, bir KriptoVarlık'ın para ya da emtia olarak değerlendirilmesi pek çok alanda örneğin vergilendirmede büyük farklılıklar yaratıyor.

Sonuç

Evet-Ethereum dünyası çok büyük bir dünya ve fırsatlar sınırsız. Ancak hep yaptığımız uyarıyı bir kez daha yineleyelim: Ethereum daha henüz emekleme aşamasında-gerekli altyapı henüz tamamlanmış değil. Bu nedenle son kullanıcının Ethereum üzerine kurulan uygulamaları kullanmak için beklemesi gerekiyor. Bitcoin o anlamda basit ve sadece bir konuya (değer transferi) odaklandığı ve güvenlik konusuna ciddi vakit ayırdığı için daha ileride. Ethereum ise koca bir dünya vaat ediyor, bu nedenle olanaklar sınırsız olduğu gibi güvenlik açıkları da oldukça fazla. Bunların kapanması vakit alacak. Kullanırken dikkatli olmanızda kesinlikle fayda var.

diğer kripto paralar neler?

Bitcoin ve Ethereum dışında diğer önemli Blockchain sistemlerine de bakalım kısaca:

Bitcoin temel olarak değer saklama işlevi görmeyi amaçladığı için onu geliştiren yazılımcılar yeniklikten ziyade güvenirliğe önem veriyorlar ve bu nedenle Bitcoin'in yeterince pratik olmadığı ve bu yönde çalışmalarda ağır kaldığı yönünde eleştiriler var. Bir de Bitcoin size tam olarak gizlilik sağlamıyor, bu yönünü eksik bulanlar da bir hayli fazla. İşte altcoinler temel olarak bu eksiklikleri gidermek amacıyla ortaya çıkmış kripto paralar. Genel olarak Blockhain bazlı sistemi kullanıyorlar, ancak detaylarda Bitcoin'den ayrılıyorlar.

Litecoin, Bitcoin'in zıpır kardeşi olabilir mi?



Litecoin, Bitcoin benzeri paralar içinde Bitcoin'e en benzeyeni. Kurucusu, Charlie Lee adında MIT mezunu bir genç. Hatırlarsanız, Bitcoin benzeri sistemler için Açık Kaynak metodunu benimsemişler demiştik. Bu şu demek: İsteyen herhangi biri mevcut sistemi yürüten yazılımı alıp aynısını kurabilir ve çalıştırabilir. İşte Charlie'nin yaptığı da aynen bu.
Litecoin, iki konuda Bitcoin'den ayrışıyor. Birincisi, hani hep diyoruz Bitcoin on dakikada bir bir ödül veriyor. Bu ödül aslında o on dakika içinde yapılmış işlemlerin teyidi anlamına geliyor.

Yani Bitcoin ile bir işlem yaptığınızda örneğin mal satıp Bitcoin aldığınızda, işlemin gerçekten doğrulandığını görmek için on dakika beklemeniz gerekiyor (genelde bu süre ama kimileri daha sağlam olsun diye bu sürenin birkaç katını bekliyorlar). Litecoin ise bu on dakikalık onay süresini 2,5 dakikaya indiriyor. Böylece satıcı olarak aldığınız paranın hakikaten size ait olduğunu yaklaşık 1/4 sürede kesinleştiriyorsunuz.

Litecoin'in ikinci farklılığı ise madenciler alanında. Hani şu işlemleri on dakikada bir teyit eden makineler. Burada ileride bir bölümde daha detaylı ele alacağımız gibi makineler bir bulmaca çözmeye çalışıyorlar. Başlangıçta, evinizdeki laptop aracılığıyla bu bulmacayı çözme ihtimaliniz vardı. Ancak sisteme çok kuvvetli makineler girmeye başladığından beri evde bu işi yapıp bulmacayı çözme ve para kazanma ihtimaliniz çok azaldı. İşte Litecoin, bulmacanın yapısını bu tip büyük makinelerin avantajını azaltarak evde işi yapan küçük oyuncuların avantajına olacak bir hale getirdi. Bu bir nevi, çok kuvvetli makinelerin sistemi tekeline almasının önüne geçmeyi amaçlayan bir yöntem.

İşte bu kadar. Bu iki özellik dışında Litecoin, Bitcoin'in aynısı. Litecoin, Bitcoin ile oldukça yakından çalışıyor, rakipten ziyade küçük kardeş gibi. Litecoin, teknolojik olarak yapılan değişikliklerin laboratuvarı gibi kullanılıyor, bir nevi yeni deneyler burada yapılıyor.

Kısacası, Litecoin yukarıda bahsettiğimiz iki yenilik ile daha pratik olmaya çalışarak paranın iki özelliğinden (değer depolama ve alışveriş aracı olma) yola çıkarak alışveriş için daha pratik ve uygun bir çözüm olmaya çalışıyor.

Monero, biraz fazla mı gizli?



Monero'nun Bitcoin'den farkı gizlilik konusuna verdiği önem.

Konu şu: Normalde Bitcoin ile bir işlem yaptığınızda, satıcı olarak siz Bitcoin'i diğer tarafa gönderiyorsunuz ve kendi Özel Anahtarınız ile bu işlemi onaylıyorsunuz. Dolayısıyla, paranın geldiği adres belli ve açık. Sizin kim olduğunuz bilinmiyor ama size gelen paralar ve sizden giden paralar görülebiliyor.

Pratikte bunun ne önemi var derseniz, kimi durumlarda özellikle kanun dışı aktiviteler içine girmiş kimi hesaplar, eğer kimi borsalar tarafından fark edilirse bloke edilebiliyorlar. Parayı para yapan özelliklerden baktığımız bölümde bahsettiğimiz özelliklerden biri paranın her bir parçasının birbirine eşit olması idi ve orada Bitcoin'in örneğin Altın'a göre dezavantajlı olduğundan bahsetmiştik. İşte ana nedeni bu: Normalde her Bitcoin'in eşit değere sahip olması gerekirken, burada bazı hesaplarda bulunan Bitcoin diğerleri ile aynı değere sahip değil.

Monero ise buna şöyle bir önlem bulmuş. Bir hesaptan diğer hesaba para gönderildiğinde, gönderilen parayı sadece gönderen parti değil onunla birlikte on farklı (rastgele) taraf da imzalıyor. Gerçekten paranın sahibi imzaladığı için işlem gerçekleşiyor ama on kişiden hangisi olduğu bilinmediği için paranın gerçek sahibinin adresini anlamak mümkün değil!

Bunun dışında Monero, Litecoin'e benzer şekilde pratiklik olarak her on dakika yerine iki dakikada bir teyit işlemi yapıyor ve madencilik işinin birkaç büyük aktör elinde toplanmasını önlemek için de Litecoin benzeri bir ödül sistemi kullanıyor. Kısacası Monero, hem Litecoin gibi pratik, hem de ondan daha da gizli bir para sunuyor.

Dash, biraz fazla mı karanlık?

Dash de aynı Monero gibi, hem gönderici/alıcı adreslerini gizliyor, hem de hızlı işlem yapabilmek için teyit sürelerini indirmiş durumda.

Monero'ya göre iki yıl sonra 2014 yılında başlatılan Dash, Evan Duffield adında birinin ürünü. Oldukça iyi bir pazarlama ekibi var, ve bu nedenle son yıllarda paranın değerinde ciddi bir artış yakaladılar. Ancak gizlilik anlamındaki şöhretleri iyi mi kötü mü tartışılır. Örneğin, Doğu Avrupalı yasadışı iş yapan yapıların, son zamanlarda Dash kullanmaya başladıkları söyleniyor (bu yapılar Bitcoin'i yeterince gizli olmadığı için çoktan bıraktılar).

Ancak Dash ile ilgili teknik olarak en büyük soru işareti başlangıcı. Konu şu: Bitcoin (Litecoin ve Monero da aynı şekilde), ilk kurulduğundan itibaren eşit aralıklar ile her on dakikada bir Bitcoin dağıtarak sistemi sürdürdü.



Dash ise ilk 3 yılda yarattığı paranın %30'unu bir "hata" sonucu çalışmaya başladıktan sonraki 24 saat içinde yarattı. Normalde, henüz başlangıçta bu tip sorunlar yaşanabildiği için (zira hepsi deneysel bu paraların) geliştirici sistemi restart edip baştan başlatabilir. Ama Dash öyle yapmadı ve çalışmaya devam etti. Dolayısıyla parayı yaratan kişi ve etrafındaki çok ufak bir ekip, tüm paranın %30'unu en baştan ellerine aldılar. Oldukça şüpheli bir durum ve düpedüz haksız rekabet var.

Kısacası, Dash, Monero gibi gizlilik ve pratiklik alanında ön plana çıkıyor ancak kuşkulu geçmişi nedeniyle onun kadar saygın bir kripto para değil.

Zcash, sınıfın parlak çocuğu mu yoksa?

Zcash, gerek Monero gerekse Dash'den daha sonra, 2016 yılında ortaya çıkan ve büyük ilgi gören bir kripto para. Bunun iki nedeni var.



Birincisi kurucusu Zooko Wilcox'un Dijital Para alanında çok eskiden beri bilinen ve saygın biri olması. İkincisi ise diğer alternatif kripto paralar ilk çıktıklarında çok ufak bir geliştirici topluluk dışında bilinmez iken, son yıllarda artan ilgi nedeniyle Zcash'in daha aktif hale gelmeden hemen hemen bu alandaki herkes tarafından biliniyor olması.

Zcash gizlilik konusunda Monero'dan da ileri gitmiş durumda. Bitcoin'de parayı gönderenin ve alıcının adresleri açıkken, Monero'da bu adresler gizli kalıyor demiştik. Zcash ise kullandığı sistemle gönderilen miktarı bile gizli tutuyor. Bir nevi açık olan hiçbir nokta yok. Sadece bir taraftan (ki kim olduğu belli değil), diğer tarafa (yine kim olduğu belli değil) bir dijital "şey" (ne olduğu belli değil) gönderiyorsunuz.

Zcash, kurucusu ve etrafındaki ekip nedeniyle bu alanda belli bir saygınlığa sahip. Ancak, henüz Monero gibi büyük ve sağlam bir topluluk oluşturmuş ve altyapılarını tamamlamış değiller. Gelecekte neye dönüşeceklerini hep birlikte göreceğiz.

MimbleWimble aranan mahremiyet büyüsü mü?

Bugünlerde kripto dünyasındaki yeni 'hip' konudan bahsedeceğiz bu bölümde. Nedir bu yeni dalga? MimbleWimble!

"Zamanında buralar hep dutluktu" diyenleri bilirsiniz. Hepimiz bu tip kaçırdığımız fırsatlara yanarız. Bundan on yıl önce ortaya çıkan Bitcoin'in ilk yıllarını da benzer şekilde es geçtik. Peki bir sonraki Bitcoin'in çıkışının şu aralar, daha doğrusu 15 Ocak'ta gerçekleştiğini söylesek size? Doğru mu gerçekten bu? Şu andan bunu kesin olarak bilmeye imkân yok tabii, ama belki de öyledir kim bilir? Gelin kararı siz verin. Teknik olduğu için bir parça karışık ama basitleştirmek için üç parçaya ayıralım anlatacağımızı:

• Bu kısımda başlangıç seviyesinde bu teknolojinin teknik olmayan kısmına, felsefi ve ekonomik boyutuna MimbleWimble üzerinden bakacağız.
• İkinci kısımda MimbleWimble üzerine kurulan en heyecanlı uygulama olan Grin parasına değineceğiz.
• Üçüncü kısımda ise, işin teknik kısmına yani diğer iki kısımda felsefi ve ekonomik olarak bahsedilen konuların teknolojik olarak 'nasıl' gerçekleştirildiğine göz atacağız.

Nereden çıktı bu MimbleWimble?

MibleWimble 2016 Ağustos ayında kripto paralar üzerine uğraşan bir grup yazılımcının kendi aralarında yazıştıkları chat ortamına Tom Elvis Jedusor rumuzlu biri tarafından aniden bırakılan bir tanıtım yazısı (White Paper) ile girdi.

MIMBLEWIMBLE
Tom Elvis Jedusor
19 July, 2016

Tom Elvis Jedusor, o yazıyı bıraktıktan sonra kayıplara karıştı. Chat ortamındaki diğer yazılımcılar White Paper'ı incelediler, bahsedilenlerin güvenirliğini, kripto olarak sağlamlığını test ettiler ve gerçekten yeni bir 'olay' ile karşılaştıklarını anladılar.

2016 yılının sonuna doğru Ignotus Peverell rumuzlu bir başka kullanıcı projenin liderliğini ele aldı. MimbleWimble adı verilen o proje Ignotus liderliğinde sayısı gittikçe artan bir yazılımcı ordusu etrafında büyümeye ve gelişmeye başladı. En son 2019 yılının 15 Ocak tarihinde artık perdelerini dünyaya açar hale geldi MimbleWimble'in ilk uygulaması olan Grin.

Ne garip isimler bunlar?

Gerçekten değil mi? Yukarıdaki paragrafta ismi geçen şahısların hiçbiri gerçek değil. Ama hepsinin bir ortak özelliği var. O da Harry Potter ile ilişkili olmaları! Gelin kim kimdir bakalım:

• MimbleWimble:
Yeni teknolojinin altyapısı olan protokol. Harry Potter'ın Deathly Hallows serisinden bir büyü. Amacı bir kişinin dilini bağlayarak büyü yapabilmek için gerekli kelimeleri anlaşılır şekilde söylemesini önlemek.
• Tommy Elvis Jedusor:
MimbleWimble'in kurucusunun rumuzu. Harry Potter'daki kötü karakter Voldemort'un Fransızca karşılığı.
• Grin:
MimbleWimble üzerine kurulu en tanınmış uygulama (detaylar bir sonraki kısımda). Yine Harry Potter öykülerinden birindeki Gringott's büyücülük bankasının adı.
• Ignotus Peverell:
Grin projesinin lideri. Harry Potter'daki görünmezlik pelerinini üreten büyücü
• Luna Lovegood , Seamus Finnigan , Percy Weasley

Grin projesindeki diğer yazılımcıların rumuzları. Hepsi Harry Potter ailesinden karakterler


Luna Lovegood


Seamus Finnigan


Percy Weasley

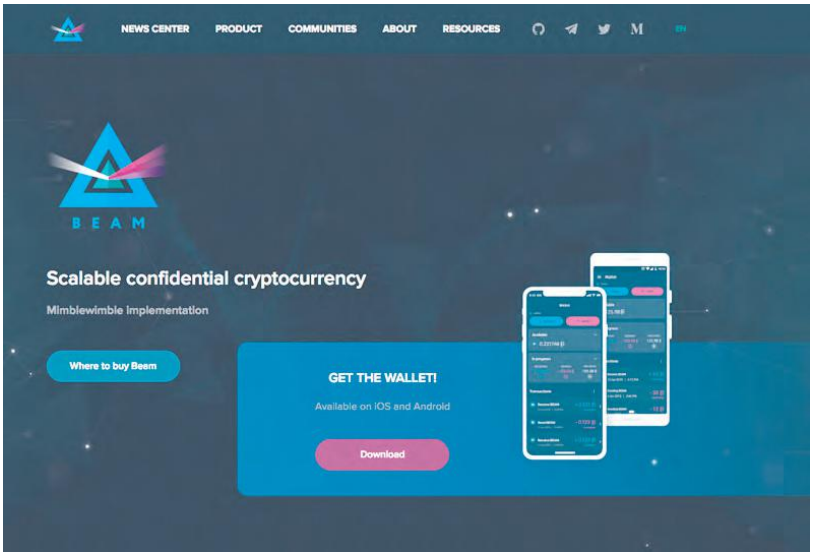
Nedir özünde MimbleWimble?

MimbleWimble özünde Bitcoin'in yaşadığı iki ana sıkıntıyı aşmak için yaratıldı: Gizlilik (mahremiyet) ve hantallık.

Gizli (Mahrem)
Daha önceki bölümlerimizde bahsetmiştik: Bitcoin aslında mahrem bir sistem değil, sözde gizli demek daha doğru. Bitcoin ile yapılan bir işlemde gizli olan kısım sadece kullanıcı adları yerine adresler kullanılması. Ama gizli olmayan kısımları da alabildiğine şeffaf. Örneğin yapılan bir işlemde gönderilen para miktarı. 2009 yılında yapılmış bir işlemde bile ne kadar para transferi yapıldığını görebiliyorsunuz.

Ancak kullanıcı adlarının gizli olması aslında çok da mahremiyet yaratmıyor. Adreslerin gerçekleştirdiği işlemler teknik olarak takip edilebiliyor, dolayısı ile kanunsuz biri ile bir alışveriş yapmanız durumunda hesabınızın mimlenme ihtimali var.





Bunu sadece kanun dışı işlemler olarak düşünmeyin. Baskıcı rejimlerde yaşayanların adreslerinin rejimler tarafından belirlenmesi ve o kişilerin rejim tarafından baskı altına alınması da olası.

İşte Bitcoin üzerindeki bu sıkıntılar, bireylerin özgürlüğünü kendine şiar edinmiş bir grup yazılımcı kesiminin (bunlara 'cypherpunk' da deniyor) tam mahremiyet sağlayacak bir protokol arayışına girmesine neden oldu. Bu şekilde ortaya çıkmış Monero, Dash, Zcash benzeri pek çok kripto para da var (bu paralardan önceki bölümde bahsetmiştik).

MimbleWimble, kuruluş amacı itibariyle tam bir gizlilik sağlamayı amaçlayan bir protokol. MimbleWimble ile yapılan işlemlerde ne işleme taraf olan alıcı ve satıcı ne de işlem miktarı belli. "Öyle olunca hile hurda olmuyor mu?" diye soracak olursanız sizi işin teknik kısmını anlattığımız kısıma bekleriz.

Basit (Hafif)
Bunun dışında MimbleWimble'in diğer temel özelliği ise basit ve hafif bir program olması. Teknik olmayanları çok da ilgilendiren bir konu değil aslında. Hatırlarsanız daha önce Bitcoin'de 2009 yılından bugüne yapılmış bütün işlemleri görebiliyorsunuz demiştik. Bu işlemlerin hepsi Bitcoin sistemindeki tüm makineler tarafından tutuluyor. Bu da her bir makine için gigabaytlarca bilgi demek. Bu kadar çok bilgi tutulması sistemin hantallaşmasına sebep oluyor. MimbleWimble üzerine kurulan uygulamalar burada da güvenlikten ödün vermeden basit bir sistem kurmayı hedefliyorlar.

Ne gibi uygulamaları var?

Yukarıda bahsederken iki uygulaması olduğundan bahsetmiştik. Bu iki uygulama Beam ve Grin. MimbleWimble başka diğer pek çok proje gibi açık kaynak bir yazılım. Açık kaynak yazılımların en önemli özelliği isteyenin istediği noktada projeyi istediği şekilde geliştirebilmesi. Burada da iki farklı grup projeyi birbirinden çok farklı yerlere götürmüş durumda.

MimbleWimble üzerine çıkan iki projeden biri olan Beam[97], İsrailli bir girişimci olan Alexander Zaidelson[98]'un CEO'luk yaptığı bir oluşum. 2018 sonbaharında 400 Bin ABD Doları yatırım alan proje, derli toplu bir şekilde MimbleWimble üzerine Beam adlı kripto parayı kurmak için uğraşıyor. Derli toplu derken, bir ekibe sahip olması, kendilerine çizdikleri bir yol planına sahip olması, yatırım alması, Beam parasını açtıklarında kurucular için kendilerine bir para ayırmaları gibi özellikler. Zcash benzeri ICO yapan bir kripto paranın geçtiği tüm süreçlerin benzerini yapmaya çalışıyorlar. 2019 yılı Ocak ayı başında da paralarını dünyaya açtılar.

[97] https://www.beam.mw/
[98] https://twitter.com/azaidelson

Asıl dikkate değer MimbleWimble uygulaması Grin. Detaylarına bakalım:

Grin nedir?

MimbleWimble'in çıktığı ikinci proje olan Grin, çıkış olarak Bitcoin' çok benziyor.
Örneğin, lideri olan Ignotus Peverell'in kim olduğunu kesinlikle bilinmiyor. Ignotus Peverell geçtiğimiz yıl yapılan Grin konferansına text-to-speech teknolojisi ile katıldı. Katılımcıların sorularını, yazdığı metni seslendiren bir yazılım aracılığı ile cevaplandırdı.[99]

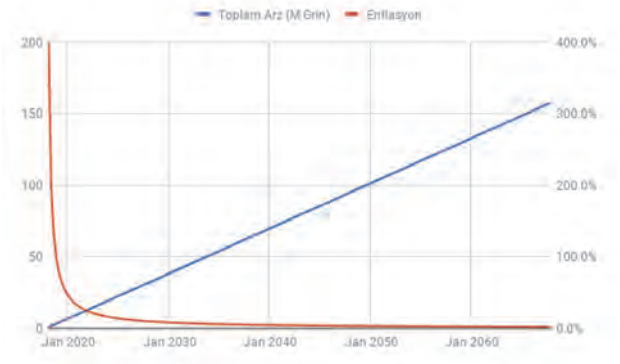
Bunun yanında Grin girişim sermayesi benzeri herhangi bir yatırım almadı, bundan sonra da sadece crowdfunding (kitlesel fonlama) ile yoluna devam etmeyi planlıyor. Bunu özellikle önemsiyorlar zira yatırım aldıklarında aslında gerçekten odaklanmaları gereken gizlilik ve kullanılabilirlik alanları yerine yatırımcıya vaad ettiklerini gerçekleştirebilmek adına değer artırıcı konulara zaman ayırmak zorunda kalmaktan korkuyorlar. Zaten ne bir ofisleri var ne de bir organizasyonları, aynı Bitcoin'in ilk günlerindeki gibiler.

Grin yaratıcıları, Bitcoin'in para saklama aracı olarak piyasanın ağır ağabeyi olarak hâkimiyetini sürdüreceğini, kendi paraları olan Grin'in ise ödeme aracı olarak kullanıcılara pratik ve tam gizlilik sağlayan bir mekanizma kuracağını düşünüyorlar.

Bunu gerçekleştirebilmek için de teknik olarak basit, hafif ve gizli bir para yaratmanın yanında ekonomik olarak da Bitcoin gibi deflasyona yol açan (giderek azalan) bir para yaratım politikası yerine, enflasyonist (sabit olarak aynı hızda artan) bir para yaratım politikası[100] sürdüreceklerini açıklıyorlar.

[99] https://youtu.be/k6tCnw6shgQ
[100] https://www.tokendaily.co/blog/on-grin-mimblewimble-and-monetary-policy

Bu para politikası aslında ilginç bir detay: Para sabit şekilde artacağı için, ikinci yıl ilk yıl piyasaya çıkan kadar para yaratılacak. Üçüncü yıl o ana kadar yaratılmış toplam para stokunun %50'si, dördüncü yıl %33'ü, onuncu yıl 10%u olacak şekilde giderek azalan oranda. Bu nedenle ilk yıllarda para arzı çok fazla olduğu için yani ciddi bir enflasyon yaşayacağı için insanlar parayı ellerinde tutmak yerine (paranın değer saklama özelliği) alışverişte kullanacaklar (paranın ödeme aracı özelliği). Ancak ilk 15–20 yıl sonrası yıllık enflasyon %2'lere inip arz mevcut para miktarına göre iyice azalınca parayı elde tutmak değerli hale gelecek.



Grin Para Politikası

Peki neden popüler oldu bu kadar bu Grin?

Grin'in bu kadar popüler olmasının belki de en önemli nedeni yukarıda da bahsetmeye çalıştığımız Bitcoin benzeri cypherpunk köklere sahip olması. Zira cypherpunk ekibi bireyin özgürlüğünü ve devlet benzeri otoritelere karşı bağımsızlığını savunurken, bunu bir organizasyon altında yapmaları durumunda, otoritelerin uygulayacakları baskılar ile organizasyonlarını ezeceği, kişileri ise hapis de dahil türlü yaptırımlar ile yıldıracağı korkusunu taşıyorlar.

Kişilerin gizliliğini ve bağımsızlığını savunabilmek için kendilerinin de gizli olması gerektiğine inanıyorlar. (Bu nedenle Satoshi ismini gizli tuttu, Wikileaks aracılığıyla Bitcoin ortaya çıktığı anda sırra kadem bastı-tüm hikayesi "Bitcoin ne tam olarak?" adlı bölümümüzde).

Bitcoin benzeri felsefeye sahip bir oluşum olarak başka kripto paralar (Monero, Dash, Zcash) gibi kurucu ekip olarak para yaratımı başlamadan kendilerine baştan bir pay almamaları onları kripto camiası içinde saygın bir yere koyuyor. Çünkü "premine[101]" ya da "founders' share" de denen bu tip bir uygulamanın adil bir paylaşım olmayacağına inanıyorlar.

Bunun yanında Bitcoin'in başlangıcındaki hızlı gelişimi ve fırsatı kaçıran ciddi bir kesim de, şimdi yeni çıkan bu oluşuma erken katılarak oluşacak fırsatlardan olabildiğince çabuk faydalanma peşinde-ama bu kesimin bir sonraki kısmı okumasında fayda var.



On yıl ara ile Hal Finney[102] ile Jameson Lopp[103]

Ama sadece cypherpunk topluluğu değil Grin'i popüler yapan. Her ne kadar dışarıdan yatırım almasa da girişim sermayeleri bir şekilde projeye destek oluyorlar. Nasıl mı? Önceki bir bölümde bahsettiğimiz değişen yatırımcılık kapsamında.

Grin 15 Ocak itibari ile çalışmaya başladı ve işlemler karşılığı madencilere para yaratma hakkı verdi. İşte pek çok girişim sermayesi de şu anda para harcayıp makine satın alarak ve enerji harcayarak madencilik yapıyor. Amaçları Grin parasına rekabet artmadan erkenden sahip olabilmek.

Yine de bu yatırımcıların, benzer şekilde para yaratımına başlamadan önce büyük sükse yapmış "mahremiyet" esaslı diğer paraların yaratılmaya başladıktan sonraki sürede geçirdikleri değer değişimlerini iyi incelemelerinde fayda var. Bakın, Monero, Zcash ve Ravencoin, ilk çıkışlarından sonra değerlerini ne kadar kaybetmiş:



Monero, Zcash ve Ravencoin ilk çıkış sonrası seyirleri-Kaynak ByteSize Capital[104]

Bir başka hipotez ise şu: Bitcoin artık para olarak değer saklama (SoV- Store of Value) konusunda kendini kanıtladı. İnsanlar ona bir değer atfediyor. Üstelik arzın kısıtlı olması değerinin artacağı yönündeki beklentileri de artırıyor aynı zamanda. Ancak Bitcoin teknik kısıtlarından ve yavaş gelişiminden dolayı paranın bir diğer önemli özelliği olan ödeme aracı (MoE- Medium of Exchange) olma konusunda geride kalıyor. (Lightning Network gibi bu alanda çalışan girişimler var tabii).

101https://www.cryptocompare.com/coins/guides/what-is-a-premine/
102https://twitter.com/halfin/status/1110302988
103https://twitter.com/lopp/status/1085203546579128321

104https://twitter.com/ByteSizeCapital/status/1085155010495709184/photo/1

Dolayısıyla pazarda özünde bir ödeme aracı olacak bir başka paraya ihtiyaç hâlâ var gibi. Grin de Bitcoin'e yakın felsefesi ve mahremiyet konusunda ön plana çıkan özellikleri ile bu boşluğu doldurmaya en büyük aday.

Neleri eleştiriliyor?

Grin ile ilgili eleştirilerin ana odak noktası, aslında övünerek bahsettikleri yatırım almama konusu. Bazıları, Grin yaratıcı ekibinin dış bir yatırım almaması nedeniyle kendini baskı altında hissetmeyeceği ve bu nedenle koydukları hedefleri zamanında gerçekleştirmek için kendilerini zorlamayacakları düşüncesinde.

Bunun dışında eleştirilen konulardan biri de ekonomik: Grin'in para yaratma politikası. Bitcoin'in fiyatının artmasındaki en önemli konulardan biri zamanla kullanımı artarken yaratılan Bitcoin'in azalacak olması. Piyasadaki Grin miktarının sürekli artacak olması onu Bitcoin benzeri spekülatif bir değer artışına gitmesini engelleyebilir. Grin'in buna yanıtı şu: "Bitcoin'in başlangıcında fazla fazla yaratılan para, hasbelkader işi başında dalgayı yakalayanlara inanılmaz kazançlar sağladı ancak yaratılan değer ufak bir azınlığın elinde kaldı. Biz bu yaratılacak değeri daha geniş bir kitleye dağıtmak için daha egaliter bir yapı öngörüyoruz, bu nedenle para arzının sürekli olarak artıracağız."

Akla gelen soru işaretlerinden biri de gizlilik ile geniş kitleler tarafından adaptasyon arasındaki çelişki. Biliyorsunuz özellikle kripto para borsaları bu dünyaya adım atmanın en temel yollarından biri. Ancak merkezi çalışan kripto para borsaları otoritelerin denetimi altında olduğu için müşterilerinin gerçek bilinen kişiler olduğunu sıkı takip etmek zorundalar (AML/KYC prosedürleri ile). Grin gibi tam gizli olduğunu iddia eden bir para bu borsalarda nasıl işlem görecek?

İşlem gördüğü durumda gizlilikten ödün vermiş olacak mı? Ya da hiçbir ödün vermeyecek ve geniş kitleler tarafından adapte edilmeyen, sadece baskı altındaki rejimlerde yaşayanlar tarafından kullanılan ufak (niş) bir para olarak mı kalacak? Grin yaratıcıları Bitcoin üzerine inşaa edilen Lightning Network gibi ikinci katman uygulamaların benzerlerinin Grin üzerine kurulabileceğini ve isteyenin bu uygulamalar ile kripto para borsalarında işlem yapabileceğini iddia ediyorlar. Gizlilik ile geniş kitle adaptasyonu bir arada nasıl yürüyecek göreceğiz.

Grin'e teknik olarak bakalım mı?

Kripto para dünyasında her gün yeni değişik bir ortaya çıkıyor. Her ne kadar ICO piyasalarının geçtiğimiz yılın ikinci yarısından bu yana popülerliğini kaybetmiş ve kripto paralara ilgili bir kısım kitlenin hevesini kırmış olsa da, bu alanda çalışan girişimciler üzerinde çalıştıkları projeleri yavaş yavaş ayağa kaldırmaya devam ediyorlar. MimbleWimble ve özellikle Grin, bu alanda Bitcoin'in eksik olduğu düşünülen gizlilik alanında devrim yaratacağını düşünen, Monero, Dash, Zcash benzeri yeni bir para. Eğer işin teknik olarak daha detayına girmek isterseniz, aşağıdaki kısım ilginizi çekebilir.

Gizlilik (Mahremiyet) ne kadar önemli?

Aslında MimbleWimble, Bitcoin'in üzerine kurulduğu teknolojiyi daha gizli hale getirmeye yarayan bir protokol. Ne kastediyoruz bakalım:

MimbleWimble'da ne kullanıcılar ne de işlem miktarları görünecek. Nasıl olacak bu?

Adres yok yaşasın cüzdanlar

Öncelikle sistemde paranın gidip geleceği hesaplar olmayacak. Bunun yerine cüzdanlar kullanılacak. Normalde Bitcoin sisteminde hesaptan para 'input' olarak sisteme girer, input karşılığı da aynı miktarda output çıkardı (bu output'a UTXO denirdi). Sistemdeki makinalar çıkan bu UTXO'ları toplar ve değişmediğini gördüklerinde "tamam" derlerdi "sistemde çifte harcama yapılmamış" (şu bölümde değiniyoruz bu konuya)

Grin sisteminde ise input yok, çünkü input yaratacak adresler kullanılmıyor. Bunun yerine sistemde sadece output'lar yani UTXO'lar var. Bunlar da cüzdanlar aracılığı ile kullanılıyor. Sistem iki kullanıcının bir şekilde (on-line ya da off-line) kendi arasında ne tip bir işlem yapacağı konusunda iletişime geçip anlaşma yapması esasına dayanıyor.

Örnek ile açıklayalım: Ayşe Bora'ya 100 Grin göndermek istiyorsa iki taraf kendi Özel Anahtarlarını kullanarak bir işlem yaratıyor ve bunu sisteme yolluyorlar. Biraz daha açalım: Ayşe bu işlemi başlatırken kendi Özel Anahtarı ile bir adres yaratır ve bunu Bora'ya gönderir. Bora'nın bu sırada online olmasına gerek yok. Bora Ayşe'nin gönderdiği işlemi kendi Özel Anahtarı ile şifreler. Sonrasında bu işlem sisteme girilir. Dolayısıyla sistem sadece iki kullanıcının kendi arasında anlaşarak bir işlem gerçekleştirdiğini görür ama sonuçta sadece para el değiştirdiği ve yeni bir para yaratılmadığı için bir sorun yaşanmaz.

Blok içinde detay bilgi yok

MimbleWimble içinde işlemlerin bir araya getirildiği bloklarda Bitcoin'de olduğu gibi işlemler tek tek görülmüyor. Bunun yerine bütün işlemlerin bir toplamı var-dolayısı ile kim ne işlem yaptı görmek mümkün değil.[105]

Benzer şekilde karıştırma/toplamayı CoinJoin denen bir işlem ile Bitcoin üzerinde ikinci bir katman olarak yapmak da mümkün. MimblewWimble CoinJoin'i kendi ana sisteminin bir parçası olarak kullanıyor.

IP adresleri de gizleniyor

Bitcoin'de adresler belli olduğu için para nereden geldi, nereye gitti biliniyor. Bu nedenle kullanıcıları bir şekilde takip etmek ya da paranın izini sürmek mümkün oluyor (ekstra önlemler alarak bunu engellemeniz mümkün ama bun önlemler ikinci seviye genelde sistemin özünde yok). Çünkü Bitcoin'de bir işlem yaptığınızda bunu sistem ağındaki bir makineye (düğüm-node) gönderiyorsunuz o da tüm sisteme yayıyor. İlk gönderilen node'un biliniyor olması, sizin genelde bu node'u kullanmanız gibi teknik nedenler, aslında bu parayı izi sürülebilir bir hale getiriyor.



Mimblewimble da ise öyle değil. Burada gizlilik çözümü olarak Dandelion[106] adı verilen bir protokol kullanılıyor. (Dandelion kara hindiba çiçeği demek, bu çiçeğin özelliği açmadan önce tek bir sap ve yapraktan oluşup açtıktan sonra serpilmesi).

[105] https://twitter.com/ByteSizeCapital/status/1085155010495709184/photo/1

[106] https://github.com/mimblewimble/grin/blob/master/doc/dandelion/dandelion.md

MimbleWimble'da siz sisteme bir işlem gönderdiğinizde bunu alan makine rastgele bir başka makineye gönderiyor, o bir başkasına ve böyle böyle ilk gönderen makinanın izinin sürülemeyeceği bir "bozma (fluff)" sürecinden geçiliyor.

Peki ya Basitlik/Hafiflik?

Tam güncelleme vs kısmi güncelleme

Bitcoin sisteminin teknik olarak sıkıntılarından biri sistem içindeki makinelerin (node-düğüm) işlemleri teyit etmek için kendi içlerinde tüm blockchain sistemini tutuyor olmaları. Bu data şu anda 200 GB civarında ve giderek artıyor.[107] Herhangi bir bilgisayarın sisteme girmesi için bu datayı yüklemesi oldukça uzun bir zaman.

Grin sisteminde, bir bilgisayar tüm bu datayı tutmak yerine fast sync denen bir metod ile son 2000 bloğu güncelleme (sync) yaparak dakikalar içinde sistemi kullanabilir hale geliyor.

Gizlilik vs hafiflik (ve dolayısıyla ölçeklenmeye)

Gizlilik aslında ölçeklendirme ile çelişkili bir kavram. Neden? Çünkü ne kadar gizlilik isterseniz o kadar işin içine şifreleme mekanizmaları giriyor. Ne kadar şifreleme mekanizması koyarsanız sistem üzerinde saklayacağınız bilgiyi o kadar artırıyorsunuz. Bu da sistemin ağırlaşmasına neden oluyor. Özellikle sistemi büyütmek ve geniş kitlelere yaymak istediğinizde ölçeklendirme (scaling) problemi yaşar hale geliyorsunuz.

Hız vs fonksiyon

Bunun yanında Grin'in Bitcoin'e göre önemli bir eksikliği içinde ayrı kod yazımına (scripting) izin vermemesi. Bitcoin'i genelde para transferi için kullanıyoruz ama aslında herhangi bir dijital varlık ya da bilginin transferi için de kullanabiliriz.

Bunu sağlayan içindeki scripting mekanizması. Ancak bu fonksiyon aynı zamanda ekstra yük getirip blokların büyüklüğünün artmasına ve sisteme yük bindirmesine yol açıyor.

Grin bu tip scripting mekanizması içermiyor. İşe yaradığı tek alan para transferi. Kendisini ödeme aracı olarak konumlandırdığı için daha hızlı olabilmek adına böyle bir farklılaşmaya gitmiş Grin yazılımcıları.

Uzlaşma Mekanizması

Aslında MimbleWimble teknik altyapı olarak Bitcoin'e oldukça benziyor.

Örneğin, aynı Bitcoin gibi uzlaşma mekanizması olarak makinelerin enerji kullanması prensibinden hareket eden Proof-of-Work mekanizmasını kullanıyor (PoW'yi ne olduğu ile ilgili detaylı bilgiyi şu bölümde bulabilirsiniz).

Grin'in kullandığı PoW versiyonunun adı Cuckoo Cycle[108]. Bu versiyonun özelliği Bitcoin sistemini domine etmeye başlayan ASIC tipi madencilik yapan ihtisas makinelerinin etkisini azaltmak. Grin başlangıçta ASIC resistant denen sistemi kullanarak olabildiğince küçük bireysel madencinin sistemin içinde olmasını istiyor. Ancak uzun vadede bunun beyhude bir çaba olduğunu düşünüyorlar ve kademeli olarak ASIC tipi makinelerin de sisteme girmesine izin verecekler.

Öğütme (Hashing)

Aynı zamanda Grin içindeki işlemleri gerçekleştirirken kullanılacak öğütme mekanizmasının, ileride çok kuvvetli makinalar (quantum computers) tarafından kırılacağı iddia edilen Bitcoin mekanizmalarına benzer akibeti yaşamamak için 'quantum resistant' denen çok güçlü mekanizmalar olması planlanıyor.

[107] https://www.blockchain.com/en/charts/blocks-size

[108] https://medium.com/codechain/cuckoo-cycle-c337e30c6c99



Bloklama ve zorluk dereceleri

Bitcoin sistemindeki madencilere sorduğu soruların zorluk derecesini iki haftada bir ayarlıyor. Bu zorluk ayarlamasını yaparken bulmacanın çözülme hızına bakıyor ve hızlı yani 10 dakikadan çabuk çözülüyor ise zorlaştırıyor eğer 10 dakikadan uzun sürüyor ise kolaylaştırıyor. Grin bu zorluk ayarlamasını çok daha hızlı bir şekilde yapacak. Aynı Bitcoin sonrası çıkan başka pek çok Blockchain sisteminin yaptığı gibi.

Bitcoin sisteminde işlemler 10 dakikada bir toplanıp blok oluşturulurken Grin'de bu dakikada bir olacak. Bitcoin şu anda 10 dakikalık blok oluşturma sonrası 12,5 BTC ödül verirken Grin dakikada bir 60 Grin verecek. Grin'de Bitcoin'de dört yılda bir yaşanan azalma da yok, dolayısı ile ileride eğer devam ederse piyasada bol miktarda Grin olacak.

Neden Lightning gibi ikinci bir katman değil de ayrı bir para?

Peki MimbleWimble bir protokol olarak Lightning Network gibi Bitcoin üzerine ikinci bir katman olarak uyarlanamaz mıydı? Ayrı bir paraya ihtiyaç var mıydı? Buna teknik olarak verilen cevap ikinci bir katman olarak yapılacak bir yazılımın geriye dönük olarak da uyumlu olması için çok fazla çalışma gerekeceği.

Yine de çok tatmin edici bir açıklama değil. Bir başka neden bir kısım Bitcoin geliştiricisinin yarın öbür gün Bitcoin'in başına bir 'şey' gelmesi (teknik konular vb.) halinde kendilerine bir B planı araması ve Grin'in de bu alana önemli bir aday olarak görmeleri. Bir başka neden de Bitcoin'in artık genel kabul gören ciddi bir yapı olması nedeniyle üzerine yapılan değişikliklerin çok yavaş olması. Grin yeni bir teknoloji olduğu için (Rust dilinde yazılıyor) hızlı gelişime imkân veren bir yapısı var.

Sorunları sıkıntıları neler?

Grin'in izleyeceği enflasyon yaratan para politikası aslında gelecekte fiyatının çok değerlenmesinin önündeki en büyük engellerden. Peki neden böyle bir para politikası izliyor Grin?

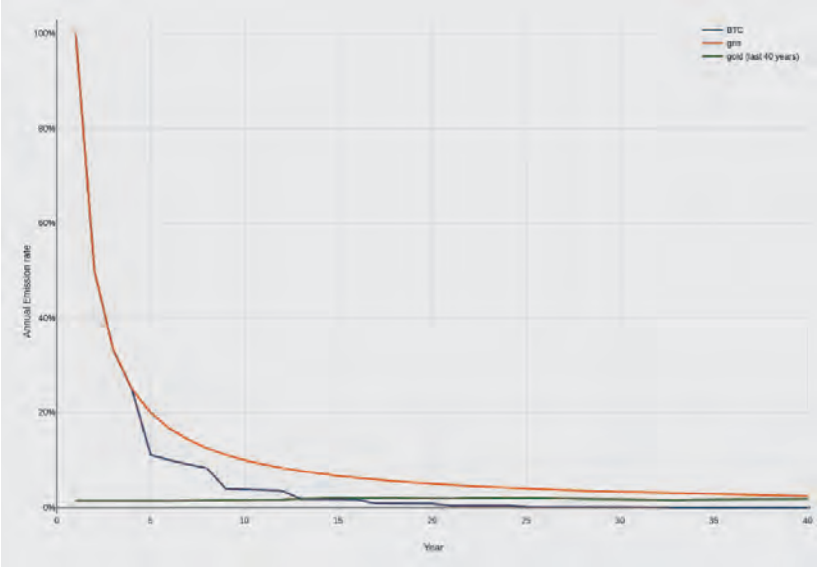
1. Bitcoin'in azalan emisyon özelliği nedeniyle para ödeme aracı değil değer saklama aracı olarak kullanıldığı düşünülüyor. Grin sürekli olarak bir arz yaratarak ödeme aracı olarak kullanılmak istiyor.
2. Bitcoin örneğinde ilk madenci kitlesi sonraki yıllarda yaşanan ciddi değer yükselmesinden dolayı inanılmaz paralar kazandılar. (Örneğin Satoshi Nakamoto'nun hiç kullanmasa bile 1 milyon BTC'si olduğu biliniyor[109]).

[109] http://time.com/money/5002378/bitcoin-creator-nakamoto-billionaire/

Grin, daha 'adil' bir dağıtım süreci öngörüyor ve kendi emisyon hacimlerinin altına benzeyeceğini iddia ediyor.

Grafik bu söylemi doğruluyor.

Bitcoin, Altın ve Grin emisyon hacimleri % olarak (Kaynak: Bobby Digital - Plot.ly[110])

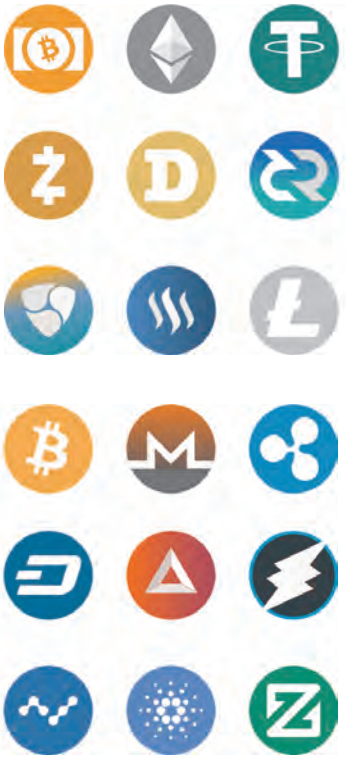


Bunun yanında işlemlere hız katmak amacıyla scripting özelliğini yok etmesi ileride Grin'in sadece para transferi için kullanılacak bir araç olarak kalması ve başka ek fonksiyonlar konusunda sıkıntılar yaratabilir. Ancak üzerine inşaa edilebilecek ikinci seviye katmanlar ve ek yazılımlar ile bu sorun giderilebilir gibi görünüyor.

[110]https://plot.ly/~Bobby_Digital/1/#/

Sonuç

Gördüğünüz gibi kripto para dünyası Bitcoin'den ibaret değil ve pek çok Bitcoin benzeri kripto para var. Muhtemelen daha da çıkmaya devam edecek. Teknoloji geliştikçe, bilinç arttıkça, yeni ihtiyaçlar doğdukça ya da mevcut kripto paralar bu ihtiyaçlara cevap vermekte zorlandıkça yenileri çıkabilir. Peki bu alternatif kripto paralar ya da yeni çıkacaklar Bitcoin'in tahtını sarsabilir mi? Altın gibi kendisine yavaş yavaş saygın bir yer edinen, 2009'dan beri tıkır tıkır çalışan ve basit anlamı ile değer saklama konusunu başarı ile karşılayan Bitcoin'i şu aşamada alt etmeleri zor görünüyor. Ama nasıl dünyada tek bir para birimi yok ise, Kripto Dünyası'nda da sadece Bitcoin olmayacak, bu diğer paralar da pastadan pay almaya devam edecekler.



SabitParalar dalgalı denizler içinde sakin sular sunar mı bize?
Kripto paraların inişli çıkışlı dünyasında sakin bir liman arayanlara-SabitParalar nedir, ne işe yararlar? Aşağıda:

Geçtiğimiz günlerde bir yemekte Bitcoin ile ilgili konuşurken, bir dostum "İyi ama Bitcoin ile bir mal sattın, parayı alıp dolara dönmek istediğinde bir bakıyorsun o sırada paranın değeri değişivermiş, ne anladım bu işten?—?neden Bitcoin kullanayım ki?" şeklinde bir serzenişte bulundu. Haklı mı? Mevcut durumda haklı. Baksanıza Bitcoin'in son bir yıldaki değişimini gösteren grafiğe:



Bitcoin- 2018 yılı içindeki değişim (Kaynak: Coindesk[111])

Sadece Bitcoin değil tabii. Diğer kripto paralar da böyle-hatta onların durumu daha da kötü. Aşağıda son iki ayın grafiği var. İki ay öncesine göre yüzde olarak dört büyük kripto paranın değişimini gösteriyor.

[111]https://www.coindesk.com/price/

Hatırlarsanız bundan önceki bir bölümde "Bitcoin para mıdır, değil midir?" diye uzun uzun tartışmış, Bitcoin'i Altın ve devletler tarafından basılan ve şu an tedavülde olan kâğıt para (itibari para da deniyor) ile karşılaştırmıştık.

Fazla dalga bulantı yapar değil mi?

Bitcoin bir para olarak "değer saklama" işlevini gayet iyi yerine getiriyor ama "alışverişe aracılık etme" konusunda belli yerlerde kullanılsa da hala genel bir kullanıma girmiş değil.

Bunun ana nedeni de, kısa vadeli işlemler için itibari paralara (ülke merkez bankalarının bastıkları) karşı anlık ciddi dalgalanmalar olması nedeniyle pratik olmaması.

Ama bu dalgalanmalar için alınacak çok da bir önlem yok. Zira Bitcoin'in fiyatını diğer tüm paralarda ya da hisse senetlerinde olduğu gibi borsalarda alım satım yapanlar belirliyor. Normalde itibari paralarda parayı basan merkezi otorite (merkez bankaları) piyasada bir oyuncu olarak yer alıp fiyattaki ani zıplamaları önlüyorlar. Kripto para dünyasında böyle arkada duran bir ağır abi yok - kaldı ki zaten böyle bir oyuncunun varlığı, kripto paraların özündeki "merkezi otoriteye olan ihtiyacı sıfırlamak" felsefesine de taban taban zıt bir durum olurdu.

Ani zıplamalar, bu tip paraları al-sat (spekülatif) amacı ile tutan kişiler ve kurumlar için bulunmaz nimet. Piyasaları yakından takip eden, 7/24 bu piyasalardaki eğilimleri (trendleri) izleyenler için çok kârlı fırsatlar sunuyor. Ama bu çok ufak bir kesim. Toplumun kalanının bu tip bir dalgalanmayı takip etmek için ne isteği ne de zamanı var. Eğer kripto paraların günlük hayatımıza girmesi hedefleniyor ise, getirdiği kolaylıklardan faydalanmak için bu paraları kullanmak isteyecek çok büyük bir kesimin daha az dalganan bir araca ihtiyacı var.



Acaba fiyatı sabit olan bir kripto para yapılamaz mıydı? Güzel soru ama kendi içinde o kadar çok çelişki barındırıyor ki. Örneğin sabit para ne demek, neye göre sabit?… Çoğunuzun aklına dolar geldiğine eminim. Peki dolar sabit bir para mı? Yoo, tabii ki hayır!

Stabil bir para aslında kendi içinde oksimoron (zıt şekilde çelişkili) iki ifade. O zaman belki de şu soruyu sormak daha mantıklı: Tamam, öyle stabil olmasın da en azından doların euro karşısında yaşadığı gibi dalgalanmaları hafif olsun, denizde hafif dalgalanmalar hissedelim, öyle her akşam yattığımızda acaba yarın sabah %10 zengin mi uyanacağım yoksa %10 fakir mi diye yüreğimiz ağzımızda olmasın. Bakın bu daha mantıklı bir soru, cevabı için de şu günlerde harıl harıl çalışıyor insanlar… Çalıştıkları konu ise SabitPara (Stable coin) kavramı. Örnekleri uzun zamandır etrafta, ancak kullanım olarak hala gerideler…

Nedir bu SabitPara? Var mı böyle bir "şey" gerçekten?

Efendim, kripto para dünyasındaki dalgalanmanın neden olduğu zararının özünde getireceği pek çok faydaya ağır bastığını ve bunun da bu paraların yaygın kitlelerce kullanımını sekteye uğrattığını fark eden girişimciler uzun zamandır yeni tip daha stabil paralar yaratmak için çalışıyorlar.

Peki nasıl bir zarar veriyor bu dalganmalar? Şöyle bir benzerlik[112] kurmak mümkün: Şu an yaşadığımız ve kâğıt paralardan oluşan dünyayı bir kıta olarak düşünün-her tür ekonomik işlemin kâğıt paralar ile gerçekleştirildiği. Bir de bu kıtaya yakın küçücük bir ada düşünün. İçinde pek çok güzellikler olan bir yer. Adı da Kripto adası olsun. Ancak bu adaya gidip gelmek zor. Botlar var ve bu botlar ile her gün belli sayıda insan oldukça zahmetli bir şekilde bu adaya ulaşıyor. Ama gelmesi zor olduğu gibi geri dönmesi de zor. Peki bu adaya şöyle dört şerit gidiş-dört şerit geliş geniş bir köprü yapılsaydı? O zaman insanlar rahatça gider gelirlerdi. Hatta günde birkaç kere gidip gelebilirlerdi. Ne de olsa ulaşım kolay, o kadar zahmete değer artık…

İşte SabitPara'lar bir nevi bu köprüler aslında… kripto paranız var ise bunu kullanmak çok basit. Daha önce anlattık, elinizdeki Bitcoin ile dünyanın her yerine 10 dakika içinde istediğiniz parayı gönderiyorsunuz. Ama normal kâğıt para dünyasından kripto para dünyasına girmek hem zahmetli, hem masraflı hem de vakit alıyor. Varlığınızı iniş-çıkışlardan dolayı kripto para olarak tutmak istemiyor, ama bir yandan da getirdiği kolaylıklardan faydalanmak istiyorsanız alın bir SabitPara, varlığınız SabitPara'da dursun, istediğinizde istediğiniz başka kripto paraya (örneğin Bitcoin'e) anında çevirin işleminizi yapın. Ya da bir yerden Bitcoin mi geldi, değerini kaybetme riski yaşamadan anında SabitPara'ya çevirin, içiniz rahat olsun.

112https://blog.havven.io/we-need-a-decentralised-stablecoin-b3e13346c74f

SabitParalar neye göre sabit?

Yukarıda yazdığımız sorunlara çözüm bulabilmek için nasıl yapalım da bu parayı sabitleyelim düşünürken, ilk akla gelen fikir "öyle bir para yaratalım ki dolara endekslenmiş olsun, bankada dolar tutmakla borsada bu parayı tutmak birbirinin tıpatıp aynısı olsun" olmuş. Bu düşüncenin sonucu ortaya çıkan pek çok para var.

Mantıklı mı? Bir dereceye kadar evet. Neden mi? Bir kere başta dediğimiz gibi ABD Doları'na bağlı olan bir para, diğer paralar karşısında aynen ABD Doları gibi dalgalanacak. Dolayısı ile çok sabit sayılmaz. Teorik olarak yine Dolar gibi ABD'de yıllık enflasyon ne kadar ise senelik o kadar değer kaybına uğrayacak. Ama bunlar zaten bildiğimiz konular-yine de Bitcoin vb paraya göre daha stabil olacak değil mi? Teorik olarak evet.

Sabitparalar içinde en bilineni ise Tether (USDT). Nedir bu Tether? Nasıl çalışır?[113]

En büyük SabitPara Tether neye benzer?

2015 yılında kurulan Tether'in çalışma mantığı aslında basit. Şöyle demiş kuranlar: Tether'i ABD Doları'na endeksleyelim. Öyle ki her zaman 1 Tether 1 Dolara eşit olsun. Tether satın almak isteyen getirsin dolarını o kadarlık Tether alsın. Bunun için de yaratılan (satılan) her Tether için o kadarlık parayı bir bankada hesaba yatırmışlar. Yani piyasada bulunan her Tetherin karşılığı olarak bankada aynı miktarda dolar bulundurmuşlar. Dolayısıyla, Dolar teminatlı bir SabitPara yaratılmış Tether ile. Ancak yine de başka sorunları yok değil. Örneğin, kripto para dediğimiz dünyanın merkeziyetçilikten uzak olması gerek-neden? Çünkü, (bu işin gurusu Nick Szabo'nun da dediği gibi) merkezi her kurum aslında bir güvenlik açığı yaratır.[114]

[113]https://tether.to/
[114]https://nakamotoinstitute.org/trusted-third-parties/



Halbuki, Tether'de teminat olarak paralar bir bankaya yatırılıyor. O bankada paralar ne kadar güvenli? Ya banka bir gün sıkıntıya girer hatta belki batarsa? Teorik bu tehlikeleri geçtik diyelim-gerçekten bankaya yatırılan ABD Doları karşılığı kadar mı para yaratıldı? Ya daha fazla yaratıldı ise? Kim denetleyecek? Banka ya da bir denetleme kuruluşu. Çalışma prensibini şeffaflık üzerine kurulmuş kripto para dünyasına (örneğin açık kaynak bazlı ekosistem)) oldukça yabancı kavramlar bunlar... Nitekim geçtiğimiz yıl Aralık ayında ABD resmi makamları Tether'e soruşturma açarak[115] bahsedilen rakamların gerçekten teminat altında olup olmadığı ile ilgili inceleme başlattı. Ya yarın öbür gün ABD hükümeti Tether'in varlıklarına el koyarsa? Şu an öyle bir durum yok ama isterse yapma gücü var!

Bunun yanında bir de büyüklük (ölçekleme) sorunu var. Eğer hedeflenen vizyon bir gün bu kripto paranın tüm dünyada kullanılacak hale gelmesi ise bahsettiğimiz milyarlarca dolarlık bir ekonomik büyüklük. Ne yapacaksınız, tüm bu büyüklüğün karşılığı ABD Doları'nı bankaya mı yatıracaksınız? Yatırabilirsiniz tabii bir sorun yok ama bu büyüklüğe ulaşmak için geçeceğiniz yolları hem zorlu hale getirecek bu teminat sistemi hem de oldukça yavaşlatacak. Hızlı bir şekilde bu sistemin büyümesi oldukça zor olacak gibi görünüyor. Sonuç olarak Tether şu anda belli bir işlevi yerine getiriyor. İşe de yarıyor. Ama yine de mevcut dünyada kullanılan bir işlevin Kripto dünyasına adapte edilmeye çalışılmış hali gibi. Şifreli Harikalar Dünyası'nın içindeki vizyona (bağımsız, başta merkez bankaları olmak üzere merkezi otorite etkisinden uzak, dağıtık bir yapı) ise henüz çok uzak. Muhtemelen o vizyona diğer SabitParalar daha yakın olacaklar.

[115]https://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc



Facebook'un SabitParası Libra nedir? Nasıl çalışacak?

Sabit paralar içinde son ortaya çıkan Libra ile Facebook oldu. Hem de ne çıkmak! Nedir nasıl işleyecek gelin hep birlikte bakalım.

Özetle nedir olay?

Bir paragrafta özetleyelim:
• Facebook, 27 diğer kurum[116] ile birlik olarak merkezi Cenevre'de bulunan bir vakıf kuruyor[117].
• Bu vakıf 2020 yılında Libra adında bir Blockchain kurarak aynı adlı bir kripto para çıkaracak.
• Bu para, aslında %100 dolar ve benzeri paralardan oluşan bir sepet ile desteklenen bir SabitPara (stable coin).
• Kişiden kişiye para transferi dışında, Facebook sistemi içindeki pek çok hizmet alımının karşılığında ödeme olarak da kullanılabilecek (ortaklar, örneğin Uber için de geçerli bu).
• Biz bireyler, elimizdeki TL, ABD Doları vb parayı Libra'ya çevirip sistem içinde kullanabileceğiz. Bunu yaparken normal olarak dijital cüzdanlar kullanacağız. Calibra[118], bu cüzdanların Facebook tarafından çıkarılan ilk örneği.

[116] https://libra.org/en-US/partners/
[117] https://libra.org/en-US/association/
[118] https://calibra.com/

Tanıtım Dokümanının İngilizcesi[119] ve Ebru Güven'in çevirisi ile Türkçesi[120] mevcut.

Facebook neden kripto para dünyasına giriyor?

Facebook neden bir kripto para çıkarıyor? Soruyu biraz daha açsak iyi olacak sanki: Facebook neden onlarca farklı kurumu içine alacak geniş bir yapı kurarak bir kripto para çıkarıyor?

Facebook'un derdi ne?

Facebook özünde Google ile birlikte dünyanın en büyük iki reklam ajansından biri. Ve kurduğu benzersiz iş modelinin temeli kullanıcı bilgilerini toplama ve bu bilgiler odağında kullanıcıya nokta atış reklam yapmaya dayanıyor. Ancak Facebook halka açık bir şirket ve Wall Street ondan sürekli olarak kârını artırmasını istiyor. Facebook'un elindeki en büyük varlık ne? 2,3 milyar kullanıcı[121]. Bunlardan bir yere kadar reklam geliri elde edebilir. Ama daha fazlasını vermesi lazım kârâ susamış fonlara, yoksa hisse senedi tepetaklak aşağı gider.

[119] https://libra.org/en-US/white-paper/
[120] https://medium.com/@tasebru/libra-i%CC%87zahnamesi-white-paper-b9662eb7cb3f
[121] https://zephoria.com/top-15-valuable-facebook-statistics/

Fotoğraflarınız, beğendiğiniz makaleler, sevdiklerinizin doğum günlerini kutlamak gibi özel hayatınızla ile ilgili sizi sizden iyi tanıyan Facebook, şimdi Libra ile sizin harcamalarınızı da görmek ve ona etki etmek istiyor.

Kimi örnek alıyor?

Facebook aslında Çin'in dijital anlamdaki en büyük devi olan WeChat'ın yolunu izliyor[122]. Kendi halinde masum bir mesajlaşma programı olarak başlayan WeChat, hükümetin de desteği ile şu anda her tür finansal işlemi dijital olarak gerçekleştirebildiğiniz dev bir platforma dönüşmüş durumda. Benzer şekilde Kore'nin en büyük mesajlaşma uygulaması Kakao da 44 milyon kullanıcısı için bir kripto para cüzdanı geliştirerek kullanıma soktu[123]. Facebook da bu iki kuruluş gibi Whatsapp'ı kullanarak para transferini mesajlaşmanın içine katmayı planlıyor.



Libra, Eski Romalı ağırlık ölçüsü biriminden esinlenme (Kaynak: Pixabay)

Hangi alanlarda sıkışıyor?

Ama bir yandan da şu anki mevcut modelinin bile birçok zayıf karnı var. Bunlar Cambridge Analytica skandalı ile iyice açığa çıktı. İnsanlar artık dijital dünyada kendilerine ait bilgilerin yavaş yavaş önemini kavramaya başladılar. Facebook da bu eğilimin gayet farkında: Mark Zuckerberg "gelecek mahremiyette" temalı ileriye dönük vizyonlarını bizimle paylaştı[124].

[122]https://www.apnews.com/ab55806ba6e54456b4dadadbc795ccc5
[123]https://www.ccn.com/koreas-biggest-messaging-app-kakao-to-integrate-crypto-wallet-for-44-million-users/
[124]https://m.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634

Facebook devasa bir yapı, bir dev. Böyle olduğu için de bütün gözler üzerinde. Monopol yapısı dolayısıyla tepkileri üzerine çekiyor. Geçtiğimiz günlerde şirketin ilk kurucularından Chris Hughes, New York Times'a uzunca bir makale[125] yazarak Facebook'un elinde tuttuğu korkunç güç nedeniyle parçalanmasını istedi.



Kullanıcıların öne plana çıkmaya başlayan hassasiyetleri neler?

Toplumun büyük kesimi bilgilerini paylaşmak konusunda hassas olmayabilir. Ancak bu tip bir genel izlemenin en uç noktası olan Çin aslında işin nerelere gidebileceği konusunda bize ipuçları veriyor. Sosyal medya aktifliğinize göre size bir skor veren ve düşük skorlu olanlara pasaport vermemek gibi yaptırımlar uygulayan baskıcı bir sistem Çin'in planladığı[126]. Geçtiğimiz ay Hong Kong'da yapılan protestolara giden gençlerin kendilerine ait metro kartlarını kullanmayıp, tek kullanımlık kart almaları bir başka örnek. Protestolara katıldıklarının kullandıkları kartlardan ortaya çıkabileceğinden korkuyorlar. Yaşadıkları acı tecrübeler yüzlerce insanı böyle bir önlem almaya itmiş durumda.

Facebook'un iş modeli daha önce de belirttiğimiz gibi kullanıcıların kişisel bilgilerini kullanmak üzerine kurulu. Benzer iş modeli üzerine kurulan Google da aynı şekilde artan kullanıcı tepkisini göğüslemek durumunda. Öte yandan Apple ya da Microsoft kullanıcı verisi üzerine iş modeli inşa etmedikleri için çok rahatlar. Apple CEO'su Tim Cook çıkıp göğsünü gere gere ürün ve hizmetlerinin kişisel bilgilerinizi güvenli ve mahrem tutmak üzerine dizayn edildiğini söylüyor.

[125]https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html
[126]https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4

Bu hamleler bir yandan da Facebook'u daha fazla köşeye sıkıştırmaya yönelik doğal olarak.

Bütün bunlara karşı Facebook ne hamleler planlıyor?

Dolayısıyla Facebook geçmişte yaşanan tepkileri de dikkate alarak bu yeni girişime daha temkinli yaklaşıyor. Yanına pek çok ortak alıyor, bağımsız bir vakıf kurduğunu söylüyor.



Libra kurucuları: Yok yok, kimi ararsan var (Kaynak: The Block)

Bu vakfın Libra'yı yöneteceğini, kendisinin de tüm kurucular gibi vakfın yönetiminde sadece bir oyu olacağını belirtiyor. Bilgilerin mahrem tutulacağı sözünü veriyor. Yeterli mi? Bence hayır.
Şu an yapmak istediği suyu bulandırmaya çalışmaktan başka bir şey değil. Zira Libra para olarak bilgileri tutmayacak ama parayı harcadığınız yere sizin bilgilerinizi verecek. Dolayısıyla bir şekilde harcama bilgileriniz de artık Facebook'un eline geçecek.

Öte yandan vakıf kurup ortakların arkasına sığınarak tekel olarak suçlanma da dahil kurum ve otoritelerden gelecek politik baskıları azaltmayı planlamakta.
2020 yılının ilk yarısında 100 ortak ile hayata geçmesi planlanan Libra projesinin detayları henüz belli değil. Ancak Facebook'un geçmiş sicili bizi Libra konusuna temkinli yaklaşmaya itiyor.

Facebook'un kripto piyasasına girmesi neden önemli?

İşin felsefesine baktığımızda, Libra özünde "para merkez bankaları tarafından basılır" görüşünün antitezi bir enstrüman. Tamam, tabii ki değer olarak arkasında dolar, euro gibi bir varlık var (ki bu şekilde çalışan Hong Kong gibi ülkeler de bulunmakta). Bu nedenle başlı başına "para" özelliği taşıyor mu, tartışılır. Ancak sonuç olarak baktığınızda merkez bankalarından tamamen bağımsız özel kurumların kurduğu bir yapı alışverişte para yerine geçecek bir araç çıkarıyor. Bu bile tek başına hükümetlerin kendi tekellerinde tuttukları ekonomik güce tehdit yaratabilecek bir devrim (eğer başarılı olursa).

Facebook bir dev. Bu devin kripto para piyasasına girmesi bu alanın oyuncuları için de çok önemli. Gelin bir de bu oyunculara bakalım:

Kripto para dünyası için ne gibi etkileri olacak?

Facebook Libra haberlerinin hem kısa hem de uzun vadede kripto para piyasalarına olumlu etkisi olacağını söylemek hiç de zor değil.
Kısa vadede açıklamanın yapılmasının ardından on gün içinde Bitcoin'in yaklaşık %50 oranında yükselmesinden de bu anlaşılıyor. Facebook gibi insanların aşina olduğu bir devin bu alana girmesinin, kripto paralar için en azından üzerine yapışan yaftalar (kara para aklaması ya da uyuşturucu ticaretinde kullanılması gibi) nedeniyle toplumda oluşan olumsuz önyargıların azalmasına yol açtığını şimdiden söyleyebiliriz.

Facebook yeni çıkardığı sistem ile gerçekte kimin rakibi oluyor? Blockchain dünyasının oyuncularına kısaca göz gezdirip birlikte karar verelim:

Bitcoin?

İlk akla gelen şüpheli. Piyasanın ağır ağabeyi şimdi mahalleye yeni taşınan bıçkın gence karşı. Gerçekten öyle mi? Bitcoin ile Libra'nın para transferi için kullanılmak dışında ortak pek bir özelliği yok aslında. Blockchain dünyasının iki ayrı ucundalar:

Dağıtık/Merkezi yapı

Bitcoin, tamamen dağıtık, merkezi ya da lideri olmayan bir yapı. Dolayısıyla sansür edilmesi çok ama çok zor (imkânsız da diyebilirsiniz ama büyük konuşmamak lazım).

Libra ise bir konsorsiyum tarafından yönetiliyor, her ne kadar lideri 2020 yılına kadar Facebook olsa da… Bütün konsorsiyum üyeleri, merkezi yapılar. Libra da benzer şekilde Cenevre merkezi bir yapı. Sansür edilmek ağır bir kelime olsa da, gerek kanunlar gerekse başka politik nedenler ile baskı görmeye hazır. Avrupa Birliği zaten 'dakika bir gol bir' "siz şimdi de bizim başımıza banka mı olmaya kalkıyorsunuz?" diye başladı baskıya[127], keza ABD'de de kaşlar havaya kalktı. En son 2 Temmuz 2019 tarihinde Amerikan Temsilciler Meclisi Finansal Hizmetler Komisyonu Facebook'a resmi bir mektup göndererek[128] Libra geliştirmesini durdumasını istedi. Bundan hemen sonra da Amerikan Kongresi'nde Libra üzerine görüşmeler yapılarak Facebook'un tabiri caiz ise ifadesi alındı[129].

[127]https://www.bloomberg.com/news/articles/2019-06-18/france-calls-for-central-bank-review-of-facebook-cryptocurrency
[128]https://twitter.com/APompliano/status/1146208346543804418
[129]https://www.theguardian.com/technology/2019/jul/17/facebook-libra-cryptocurrency-congress

Açıklık/kapalılık

Bitcoin'de sisteme giriş çıkış (kullanıcılar, yatırımcılar, madenciler) herkes için serbest.

Libra, izne bağlı/kapalı (permissioned) bir Blockchain olarak kuruluyor. İleride beş yıl içinde açık (permissionless) bir sisteme girmek gibi bir hedefleri var, ama bu henüz net değil.

Bu neden önemli? Bir önceki madde ile alakalı aslında. Sisteme giriş çıkışın bir otoriteye bağlı olması sistemi dış tehditlere karşı daha korunaklı hale getiriyor. Ama öte taraftan, otoriteye karşı yapılacak her türlü politik baskı için de zayıf bir karın yaratıyor.

Ayaklarının üstünde durmak / sırtını başkasına yaslamak

Bitcoin kendi değerini kendi yaratan, arkasında herhangi bir varlık ya da güç olmadan bugünlere gelmiş bir para. Altın gibi değer saklama amacıyla kullanılıyor insanlar tarafından. Öte yandan, arkasında bir varlık olmaması nedeniyle değeri arz ve talep ile belirleniyor ve özellikle emekleme aşamasında olduğu ilk on yıl içinde ciddi dalgalanmalar yaşadı.



Libra ise dolar, euro benzeri paraları arkasına alan bir yapı. Yani kendi başına bir değeri olmayacak. Bir sepet kullanacağı için nispeten dalgalanmadan az etkilenecek. Bu da bir kesim insan için cazip olabilir, özellikle parası çok dalgalanan ya da değer kaybeden ülkelerin vatandaşları için varlıklarının değerini korumada bir alternatif sağlayabilir.

Ethereum?

Ethereum daha önce de bahsettiğimiz gibi Akıllı Kontratlar vasıtasıyla üzerine pek çok farklı uygulama geliştirilmiş bir platform.

Facebook'un kurduğu Libra Blockchain'i bu anlamda Ethereum'a bir rakip gibi görülebilir. Zira Libra yalnızca para transferinde kullanılacak bir para olmanın çok ötesinde üzerine yazılacak yazılımlar ile kullanıcıların finans ile ilgili her tür ihtiyacına çözüm getirmeyi amaçlayan bir platform. Facebook bu amaçla geliştiriciler için Libra sistemi üzerinde uygulama yaratmada kullanılacak bir dil de yayınladı[130].

Facebook'un geçmişte platformunu kullanan şirketler (oyun şirketleri, reklam ajansları, dijital analitik firmaları) attığı kazıklar[131] düşünüldüğünde yazılımcılar bu suya atlamak konusunda tereddüt edebilirler. Yazılımcılar için Libra altyapısının en büyük cazibe merkezi ise Facebook'un 2,3 milyar aktif kullanıcısı.

Diğer kripto paralar?

Libra'nın ilk aşamada para transferi işlemi yapacağını öngörürsek, bu alanda etkileyeceği ilk paralardan birinin XRP olduğunu söylemek yanlış olmaz. Zaten bu nedenle Libra açıklamasının yapıldığı gün XRP'nin sahibi Ripple'in para transfer kuruluşu Moneygram'a 50 milyon ABD Dolarına ulaşacak miktarda bir yatırım yapacağı haberi piyasalara düştü[132].

Bunun yanında SabitPara (stable coin) olarak piyasada kendine yer bulmaya çalışan Tether benzeri paralar en büyük tehlike altında olanlar.

[130] https://developers.libra.org/
[131] https://andrewchen.co/why-developers-are-leaving-the-facebook-platform/
[132] https://www.coindesk.com/ripple-could-invest-up-to-50-million-in-moneygram-in-xrp-boosting-deal



Facebook gibi daha geniş kullanıcılı, destekçileri daha güçlü bir rakip karşısında bu yeni yetme SabitPara'ların kullanıcı tabanlarını genişletmek anlamında işlerinin çok zor olacağını söyleyebiliriz.

Biz son kullanıcılar için ne önemi var?

Libra'nın en önemli etkisinin, belki bu yazıyı okuyan kitle için değil ama bankacılık sistemine dahil olmayan 1,7 milyar insan için olacağını[133] söylemek sanırım yanlış olmaz. Bu kadar geniş bir kitlenin birbirleri ile Facebook (ya da Whatsapp) üzerinden ekonomik ilişkiye girebilmeleri çok kritik.

Yalnızca bu değil tabii. Libra'nın merkez bankalarının bastığı paralara bir alternatif getirmesi, bankacılık sistemine dahil bireylerin mali özgürlüğü açısından da önemli. Parası yeterince değerli olmayan ya da izlediği mali politikalar nedeniyle paraları değer kaybına uğrama ihtimali olan merkez bankaları artık karşılarında Libra gibi bir rakip daha bulacaklar.

Elbette bu bireyler şu anda da kendi ülke paraları yerine dolar, euro benzeri varlıkları tutabilirler ancak bu varlıkları alıp satma ya da başkasına transfer etme sırasında ciddi komisyonlar vermek zorundalar. Dijital dünyada aracısız işlem veren Libra benzeri dijital paralar bu maliyetleri neredeyse sıfıra indiriyor.

Benzer şekilde internet üzerinden yapılan alışverişlerde belki sizden değil ama satıcılar tarafından kredi kartı şirketlerine ve bankalara verilen komisyonların düşürülmesi, kuşkusuz tüketici lehine maliyet avantajları getirebilir.

[133] https://globalfindex.worldbank.org/

Ya kripto dünyası dışındaki aktörleri nasıl etkileyebilir?

Facebook'un bu hamlesinin sadece kripto dünyasını etkilemiyor. Aslına bakarsanız, asıl tedirgin olması gerekenler mevcut düzenin koruyucuları olan finansal kurumlar. Kim bunlar? Bankalar, kredi kartı şirketleri, para transferi işi ile uğraşan şirketler ve merkez bankaları.

Bankalar?

İlk aşamada Libra bankalara bir sorun teşkil etmiyor. Peki ya gelecekte?

Sisteme göre Libra kullanabilmek için elinizdeki dolar, euro, TL gibi klasik paraları Libra'ya çevireceksiniz ve Calibra isimli dijital cüzdanda tutacaksınız. Sizin gönderdiğiniz paralar rezerv olarak tutulacak ve riski düşük enstrümanlarda değerlendirilecek. Şu an için böyle. Sisteme giren milyonlarca insandan toplanan bu paralar böyle kuzu kuzu yatacak mı? Sanmıyorum. Bir noktada bu paraları daha iyi değerlendirmek isteyecekler. Yalnızca Facebook değil, diğer konsorsiyum üyeleri de. O zaman ne yapılabilir bu paralar ile? Neden Libra kullananlara kredi vermeyelim?

Bankalar bireylere verdikleri kredilerde, kişinin mali yeterliliklerini göz önüne alarak bir skorlama yaparlar. Ellerindeki bilgi yeterli olmadığında kişiyi kredilendirmeden çekinirler. Peki, ya elinizde Facebook'da olduğu gibi kişi ile ilgili her tür bilgi var ise? Üstelik şu anda sosyal olarak o kişi ile ilgili her tür bilgi mevcut, bundan sonra ekonomik aktivitelerine de (Libra sayesinde) hakim olduğunuzu düşünün. Klasik bir bankaya göre kat be kat iyi tanıyorsunuz bu kişiyi. Riski düşük olan ama bankanın mali varlık açısından yeterli bulmadığı birine kredi vermez misiniz? Vermezseniz, hissedarlarınız sizi sopayla kovalarlar :)

Merkez Bankaları?

Yukarıdaki Libra ile Bitcoin karşılaştırmasında yazdığımız gibi, Libra dolar ve euro gibi paraları arkasına alan bir para olarak, mali olarak güçlük çeken Merkez Bankaları'nın çıkardığı ülke paralarına ciddi bir rakip olma potansiyeline sahip. Ekonomik politikalarınızı iyi düzenleyin, doğru uygulayın, yatırımcılar ve halk nezdinde güveninizi yüksek tutun aksi takdirde kullanıcılar telefonlarındaki bir uygulama kadar kendilerine yakın olan bu paraya gönüllerini kaptırabilirler[134].

Sonuç

Libra ile ilgili hâlâ pek çok bilinmez mevcut. Şimdiye kadar bildiklerimizi varsayımlarımız ile birleştirdiğimizde yukarıdaki tablo çıkıyor. Burada en önemli konulardan biri, değişik ülkelerdeki kanun koyucuların Libra'ya nasıl yaklaşacağı, önüne ne gibi engeller çıkaracağı. Keza, kırk birbirine benzemez kurumu Libra Birliği içinde bir araya getirmek güzel ama bu kuruluşların her birinin ayrı beklentisi, korkusu ve isteği var. Bunları idare etmek de hiç kolay olmayacak Facebook için. Süreç nasıl işleyecek hep birlikte göreceğiz.



[134]https://www.brookings.edu/opinions/why-policymakers-should-fear-libra/

BCTR çalışma grupları tarafından hazırlanan RAPORLAR

BLOCKCHAIN TÜRKİYE

TBV TÜRKİYE BİLİŞİM VAKFI



DÜNYADA BLOKZİNCİRİ REGÜLASYONLARI
VE UYGULAMA ÖRNEKLERİ
Şubat 2019



DİJİTAL KİMLİK RAPORU
Nisan 2019



TEDARİKÇİ TANIMA PLATFORMU
Nisan 2019



BLOCKCHAIN İÇİN
KAVRAMSAL MİMARİ
Mayıs 2019

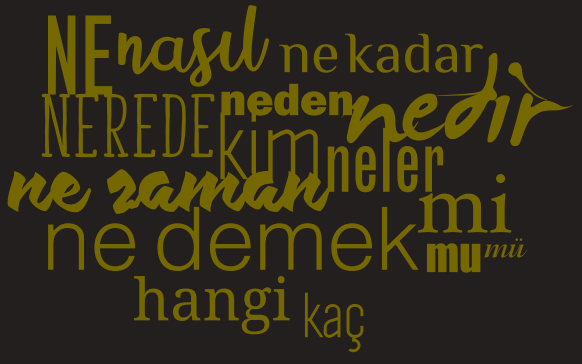


BLOKZİNCİRİ TEKNOLOJİSİ
TERMİNOLOJİ ÇALIŞMASI
Haziran 2019



AÇIK VERİ
Ağustos 2019

Sorularla BLOCKCHAIN





BLOCKCHAIN

TÜRKİYE

TBV

TÜRKİYE BİLİŞİM VAKFI