CAN AHMET DEĞİRMENCİ

KRİPTO PARALARI ANLAMAK

WEB3 ALANINDA
YENİ OLANLAR İÇİN
KAPSAMLI BİR REHBER

Bu kitabı satın almadınız, hiçbir zaman da satılık olmayacak. Amacım bu bilgileri mümkün olduğunca çok kişiye ulaştırmak. Kitabı beğenirseniz yapabileceğiniz en değerli şey onu ihtiyacı olabilecek birine göndermek olur.

Kripto paralara sıfırdan başlayanlar için kusursuz bir rehber. Yazar; teknik terimleri atlamadan, olaylar ve benzetmelerle zenginleştirerek konuyu herkes için anlaşılır kılıyor. Yalnızca yeni başlayanların değil, deneyimli yatırımcıların da temel dinamikleri tazelemek için okuması gereken ufuk açıcı bir kaynak.

— *Furkan Güler*

Kripto paraları anlamak sadece fiyat hareketlerini takip etmekten geçmiyor. Paranın dönüşümünü, blokzincir teknolojisini ve bu ekosistemin hangi sorunlara çözüm sunduğunu kavramaktan geçiyor. Can Ahmet Değirmenci bu kitapta karmaşık kavramları sade bir dille ve günlük hayattan örneklerle anlaşılır hale getiriyor. Oracle ağlarından birlikte çalışabilirliğe, DeFi'dan güvenliğe uzanan bu çalışma yeni başlayanlar için güçlü bir başlangıç sunuyor. Deneyimli okuyucular içinse değerli bir başvuru kaynağı.

— *Samet Dökmeci, Chainlink Community Manager*

Yasal Uyarı

Bu kitapta yer alan bilgiler eğitim ve bilgilendirme amacıyla hazırlanmıştır. Finansal veya yatırım danışmanlığı değildir. Kripto para piyasaları yüksek volatilite ve risk içerir. Herhangi bir yatırım kararı almadan önce kendi araştırmanızı yapmanız ve gerektiğinde bir uzmana danışmanız önerilir. Kitapta paylaşılan görüş ve deneyimler kişiseldir ve gelecekteki sonuçlar için herhangi bir garanti taşımaz.

Her adımımda arkamda duran, sabrını ve desteğini hiç esirgemeyen aileme sonsuz teşekkür ederim. Bu kitabın var olmasının en büyük sebebi bana hep inanmaları.

Bu süreçte fikirlerimi dinleyen, yol arkadaşlığını hiç eksik etmeyen dostum Salih'e de ayrı bir teşekkürü borç bilirim.

Bana inanan herkese, teşekkür ederim.

Önsöz

(Bu hikâyeyi LinkedIn'de zaten okuduysanız doğrudan Bölüm 1'e geçebilirsiniz.)

2023'ün sonbaharıydı. Lise son sınıftaydım ve tam da sınav döneminde her sabah 5'te kalkıyordum. Ama bir kitap yazmak için. Genellikle 1-2 saat kitap yazıyor, sonra da okula hazırlanıyordum. Okuldan gelince ders çalışıp erken yatıyor, ertesi sabah kaldığım yerden devam etmeyi iple çekiyordum. Bu yoğun rutine rağmen hiç yorulduğumu hissetmiyordum. Aksine inanılmaz keyif alıyordum.

Kitabı yazmamdaki temel motivasyon zor yoldan öğrendiğim her şeyi bir yerde toplayıp yeni başlayan birine aktarabileceğim bir kaynağa dönüştürmekti.

O dönemde temel seviye web3 konularını bile epey zorlanarak öğrenmiştim. Bazen İngilizce makaleleri anlayana kadar defalarca okuyor, bazen Reddit'teki başlıkları saatlerce tarıyor, bazen de dolandırılıyordum :)

"*Öğretmek, iki kez öğrenmektir*" sözüne hep inanmışımdır ve bu kitap benim için tam olarak buydu.

Ama bir şeyi geç öğrendim. İşin %40'ı kitabı yazmaksa, %60'ı doğru kitleye ulaştırmakmış. O zamanlar elimde bugünkü kadar bir kitle yoktu. Kitap tamamen ücretsiz olduğu için ücretli tanıtıma da hiç başvurmadım. Dolayısıyla üzerine bu kadar emek verdiğim kitap hedeflediği insanlara hiç ulaşamadı.

Geçenlerde bu kitaba yine baktığımda kendi kendime "Şu anda çok daha büyük bir kitleye ulaşabiliyorken bunu neden yeniden düzenleyip paylaşmıyorum?" dedim.

İşte şu anda okuduğunuz kitap tam olarak bu sorunun cevabı.

Bu sefer **çalışma şeklim biraz değişti.** Sabah beşte kalkmadım ama uzun ve sakin çalışma periyotlarıyla tamamladım :)

Ama amaç hep aynı kaldı. Ücretsiz ve yardımcı bir kaynak olmak.

Hazırsanız başlayalım.

Bölüm 1: Para ve Değer Kavramı

Kripto paraları anlamak için önce paranın kendisini anlamamız gerekir. Çünkü kripto paralar birdenbire ortaya çıkmış yeni bir icattan ziyade insanlığın binlerce yıldır sürdürdüğü arayışın en güncel durağıdır.

Bu bölümde parayı bir örüntü olarak ele alacağız.

Her aşama kendinden öncekinin çözemediği **bir sorunu çözüyor,** ama her çözüm **beraberinde yeni bir sorun getiriyor.**

Bu döngüyü net biçimde gördüğümüzde kripto paraların neden ortaya çıktığını çok daha kolay kavrayacağız.

Takas Sistemi

İnsanlık tarihinin en eski değiş tokuş biçimi takastır. Örnek olarak bir çiftçinin buğdayını, bir çobanın yünüyle takas etmesini düşünün. Kulağa basit ve mantıklı geliyor değil mi? Ama burada ciddi bir sorunu var. Bu soruna **çift rastlantı problemi** diyoruz.

Çift rastlantı problemi takas ekonomisinin en temel sorunlarından biri. Bir takasın gerçekleşmesi için sizin ihtiyacınız olan malı elinde bulunduran kişinin de tam o anda sizin elinizdeki malı istemesi gerekiyor.

Örneğin elinde buğday bulunan bir kişinin ayakkabı almak istemesi durumunda, ayakkabı sahibinin de tam o anda buğdaya ihtiyaç duyması gerekiyor.

Bu denk düşme ne yazık ki her zaman mümkün olmuyor. Bu yüzden de takas sistemi büyüyemiyor, dolayısıyla da ölçeklenemiyor.

Emtia Para

Takasın çift rastlantı sorununu çözmek için topluluklar yeni bir şey yapıyor. Herkesin değerli bulduğu ve ortak kabul gören mallar üzerinde (tahıl, tuz, hayvan, deniz kabuğu gibi), yani emtialar üzerinde, anlaşıyorlar.

Bu mallar artık sadece kendi başlarına bir ihtiyaç değil, aynı zamanda bir değişim aracına dönüşüyor. Herkes tuzun ya da tahılın değerli olduğunu kabul ettiği için elinizdeki malı doğrudan ihtiyacınız olan şeyle değiştirmek zorunda kalmıyorsunuz. Önce bu

ortak kabul gören mala, sonra da asıl istediğiniz şeye ulaşabiliyorsunuz.

Ama tabii emtia paranın da kendi dertleri var. Tahıl bozuluyor. Hayvan hastalanabiliyor, hatta ölebiliyor. Tuz nemden etkileniyor. Üstelik bu mallar için standart bir birim de yok. Bir çuval tahılın kalitesi başka bir çuval tahılınki ile aynı olmayabiliyor. Taşınabilirlik de sınırlı. Özellikle uzun mesafeli ticarette işler iyice zorlaşıyor.

Metal Para

Emtia paranın bozulma ve standart eksikliği sorununa çözüm olarak da altın, gümüş, bakır, vb. metaller devreye giriyor.

Metaller bozulmuyor, bölünebiliyor, eritilip standart ağırlıklarda basılabiliyor ve uzun süre değerini koruyor. Sikke basımı ile birlikte bir topluluğun ürettiği paranın belirli bir ağırlıkta ve saflıkta olduğu garanti altına alınmaya başlıyor. Bu da güveni ciddi ölçüde artırıyor.

Ama her zaman olduğu gibi metal paranın da bir **bedeli**[1] var, o da fiziksel ağırlığı. Büyük miktarlardaki değeri taşımak hem zor hem de riskli. Yol kesenler, hırsızlık ve kaybolma gibi tehditler her zaman kapıda. Büyük miktarda metal parayı güvenli biçimde saklamak da apayrı bir dert.

Kağıt Para

Metal paranın ağırlık ve taşıma sorununu çözmek için kağıt para ortaya çıkıyor. Başta kağıt para kasada duran bir miktar altın ya da gümüşü temsil eden bir makbuz gibi. Yani değerli olan şey aslında kağıdın kendisi değil, vaat ettiği altın ya da gümüş.

Bu sisteme altın standardı diyoruz. Basılan her kağıt paranın karşılığında, kasalarda gerçekten o kadar altın bekliyor. Devlet ne kadar para basacağı konusunda tamamen özgür değil, elindeki altın miktarıyla sınırlı.

1971'de bu denge kırılıyor. ABD'nin dolarını altına bağlayan sistem 1971'de tek taraflı bir kararla sona eriyor.

---

[1] **Trade-off (Bedel):** Bir hedefe ulaşmak için başka bir avantajdan veya imkândan vazgeçilmesini ifade eder. Başka bir deyişle, bir seçim yaparken elde edilen kazancın karşılığında katlanılan maliyet veya verilen ödündür.

Artık kağıt paranın arkasında hiçbir fiziksel varlık olmuyor. Sadece devletin ve merkez bankasının "*bu paraya güvenebilirsiniz*" garantisi var. Buna fiat para diyoruz. **Değeri, birinin ona değer atfetmesinden başka bir şeye dayanmayan para.**

Kağıt paranın çözdüğü sorun inanılmaz büyük. Artık değeri cebinizde taşıyabiliyor, uzak mesafelere kolayca gönderebiliyorsunuz.

Ama beraberinde yeni bir sorun getirmez mi, tabii ki getirir. Altın standardının kalkmasıyla birlikte para arzının önündeki en büyük fren de ortadan kalkmış oluyor. Artık bir devlet elinde fiziksel bir karşılık olmasa bile istediği kadar para basabiliyor. Kısa vadede bu esneklik gibi görünse de uzun vadede ciddi bir riske dönüşüyor. Bir devlet gerektiğinden fazla para bastığında piyasadaki para miktarı artıyor ama üretilen mal ve hizmet miktarı aynı hızda büyümüyor. Sonuç olarak elinizdeki paranın satın alma gücünün erimesi, yani enflasyon ortaya çıkıyor.

Kağıt paranın değeri artık altına değil, onu basan kurumun kararlarına ve disiplinine bağlı. **Parayı kontrol eden otoriteye duyulan güven, artık paranın kendisinden daha önemli hale geliyor.**

Bankacılık Sistemi

Kağıt paranın güvenli saklanması ve büyük miktarlarda transferi için bankacılık sistemi gelişiyor.

Bankalar paranızı fiziksel olarak taşımanıza gerek kalmadan saklama, transfer etme, hatta kredi yoluyla ekonomiye yeniden kazandırma işini üstleniyor. Çek, havale, sonra da dijital bankacılıkla birlikte para artık büyük ölçüde bir kayıt haline geliyor. Yani yalnızca bir rakam.

Bankacılık sistemi pek çok sorunu çözüyor. Ama kendi sorunlarını da beraberinde getiriyor.

Sistem az sayıda büyük kurumun elinde merkezileşiyor. Bu kurumlar veri ihlallerine ve siber saldırılara açık hale geliyor. Her işlem bir komisyon maliyeti taşımaya başlıyor. Dünya nüfusunun büyük bir kesimi çeşitli sebeplerle bankacılık sistemine hiç erişemiyor.

Belki de en önemlisi, **2008 finansal krizinde**[2] gördüğümüz gibi, bu merkezi yapılar ciddi bir risk taşıyor. Birkaç büyük kurumun çöküşü milyonlarca insanın birikimini etkileyebiliyor.

Kripto Paralar

İşte tam bu noktada kripto paralar devreye giriyor. Bankacılık sisteminin **merkezileşme, şeffaflık eksikliği** ve **güven sorununa** karşı bir çözüm önerisiyle ortaya çıkıyor. Merkeziyetsiz, şeffaf ve kimseye güvenmenizi gerektirmeyen bir sistem kurmayı hedefliyor.

Kripto paralarda işlemler tek bir otoritenin kontrolündeki veritabanında değil, dağıtık bir ağda, herkesin doğrulayabileceği bir defterde tutuluyor.

---

[2] **2008 Finansal Krizi:** ABD'de konut piyasasındaki aşırı riskli kredilendirme (subprime mortgage) uygulamalarının çöküşüyle başlayan, büyük bankaların ve finans kurumlarının iflasın eşiğine geldiği küresel ekonomik kriz. Lehman Brothers'ın iflası (2008) krizin simge anı oldu. Milyonlarca insan işini, evini veya birikimini kaybetti, hükümetler bankaları kurtarmak için trilyonlarca dolar harcadı. Kripto para camiasında bu kriz özel bir öneme sahiptir çünkü Bitcoin'in ortaya çıkışı (2009) doğrudan bu krizin yarattığı güvensizlik ortamıyla ilişkilendirilir. Bitcoin'in ilk bloğuna gömülü mesaj bile bir gazete manşetinden alınmıştır ve bankaların kurtarılmasına gönderme yapar.

Buna **blockchain**[3] diyoruz. Kimseye güvenmeniz gerekmiyor çünkü sistemin kendisi matematiksel kurallarla işliyor.

Kripto paraların bu bölümdeki yerini kısa tutuyoruz. Konunun derinine ise bir sonraki bölümde ineceğiz.

Döngü Devam Ediyor mu?

Takas çift rastlantı sorununu çözüyor, emtia para standart eksikliğini çözüyor, metal para bozulmayı çözüyor, kağıt para ağırlığı çözüyor, bankacılık sistemi saklama ve transfer sorununu çözüyor. Fakat her çözüm beraberinde yeni bir sorun getiriyor.

Peki kripto paralar bu resmin neresinde? Bu döngü kripto paralar için de geçerli mi? Yoksa kripto paralar bu zinciri kıran ilk halka mı?

Cevabı bulmak için önce kripto paraların ne olduğunu ve nasıl çalıştığını daha yakından incelememiz gerekiyor. Bir sonraki bölümde tam olarak buradan devam ediyoruz.

---

[3] **Blockchain (Blokzincir):** İşlemlerin kronolojik olarak bloklar halinde kaydedildiği, bu blokların kriptografik yöntemlerle birbirine bağlandığı ve ağdaki katılımcılar tarafından ortaklaşa doğrulanan dağıtık dijital kayıt sistemi.

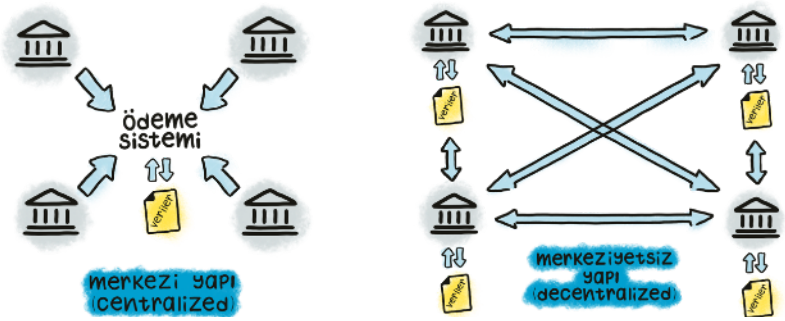
Bölüm 2: Kripto Paralar ve Varlık Sınıfları

Kripto Para Nedir, Nasıl Çalışır?

Bir an için hayal edelim. Elinizde bir defter olsun ve bu defterde herkesin kimden kime ne kadar para gönderdiği yazılı olsun. Şimdi bu defteri tek bir kişiye (mesela bankaya) emanet ettiğinizi düşünün. Ona güvenmek **zorundasınız** değil mi? Çünkü defter onda. Defteri elinde tutan kişi istediği satırı değiştirebilir, yeni para işlemlerini yazmayabilir, olmayan işlemleri uydurabilir veya defteri size hiç göstermeyebilir.

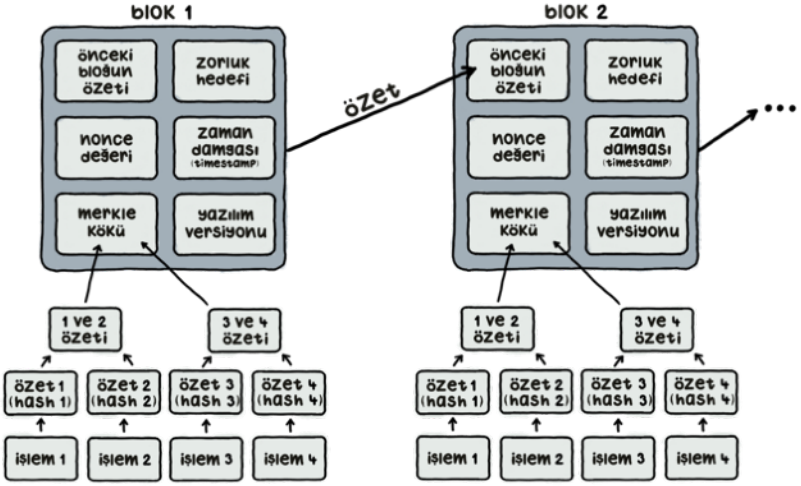
Ya bu defterin tek bir kopyası olmasaydı? Ya binlerce kopyası olsaydı ve her biri ötekinin doğruluğunu kontrol etseydi?

Kripto paralar tam olarak bunu yapıyor. Defter binlerce bilgisayara aynı anda dağılmış durumda ve buna dağıtık defter teknolojisi diyoruz.



Dağıtık defter teknolojilerinin en bilinen türü blockchain. Bir işlem gerçekleştiğinde bu işlem ağdaki katılımcılar tarafından kontrol ediliyor ve onaylanınca bir bloğa ekleniyor. Her blok bir öncekine kriptografik olarak bağlanıyor. Sanki bir zincirin halkaları gibi.

Geçmişe dönüp tek bir halkayı değiştirmeye çalışırsanız zincirin geri kalanı buna izin vermiyor.



Böylelikle sistemde kimseye güvenmeniz gerekmiyor çünkü sistemin kendisi doğrulamayı üstleniyor.

Bundan sonra bu kitapta göreceğiniz varlık sınıfları aslında blockchain (blokzincir) üzerine farklı biçimlerde inşa ediliyor.

O yüzden bu mekanizmayı iyi oturtmak oldukça önemli.

Konsensus Mekanizmaları

Az önce dağıtık bir defter fikrinden bahsettik. Binlerce bilgisayarın aynı kaydı tuttuğu ve kimsenin

patron olmadığı bir sistem. Kulağa güzel geliyor ama aklınıza hemen bir soru takılmış olabilir. Bu kadar çok bilgisayar herhangi bir yönetici olmadan hangi kaydın doğru olduğu konusunda nasıl anlaşıyor? Aralarında kavga çıkmıyor mu? Ya da daha kötüsü, içlerinden birinin yalan söylemesi durumunda ne oluyor?

Bu soru aslında bilgisayar bilimindeki en eski problemlerden birine dayanıyor. Adı da oldukça renkli, Bizans Generalleri Problemi. Hikaye şöyle. Bir şehri kuşatan birkaç general var. Şehirlere farklı yönlerden konuşlanmışlar ve sadece haberci göndererek konuşabiliyorlar. Saldırı için hepsinin aynı anda harekete geçmesi gerekiyor, aksi halde tek tek yenilirler. Sorunumuz şu, generallerden biri ya da birkaçı hain olabilir ve yanlış mesaj gönderip diğerlerini yanıltmaya çalışabilir. Peki birbirine güvenmeyen, hatta içlerinde yalancı olabilecek taraflar nasıl ortak bir karara varır?

Blockchain de tam olarak bu sorunla boğuşuyor. Ağdaki hiçbir bilgisayar diğerine körü körüne güvenmiyor, kimin dürüst kimin kötü niyetli olduğunu bilmiyor. Yine de sistem bir şekilde herkesin üzerinde anlaştığı tek bir doğru kayda ulaşıyor. Bir sistemin,

içindeki bazı katılımcılar kötü niyetli ya da arızalı olsa bile doğru sonuca ulaşabilmesine **Bizans Hata Toleransı**, kısaca **BFT (Byzantine Fault Tolerance)** diyoruz. İşte konsensus mekanizmaları bu hata toleransını pratikte nasıl sağlayacağımızın cevabı.

Bu alanda en popüler olan iki yaklaşım **Proof of Work** ve **Proof of Stake.** İkisi de aynı soruna farklı bir çözüm sunuyor, birini enerji üzerine kuruyor, diğerini sermaye üzerine.

Önce Proof of Work'e bakalım. Bitcoin'in seçtiği yol. Ağdaki bilgisayarlar (yani madenciler) karmaşık bir matematik bilmecesini çözmek için birbiriyle yarışıyor. Bilmeceyi ilk çözen kişi yeni bloğu zincire ekleme hakkını kazanıyor ve karşılığında ödül alıyor.

Peki bu yarış neden güvenilir? Çünkü bilmeceyi çözmek inanılmaz zor ve pahalı. Fakat bir çözümün doğru olup olmadığını kontrol etmek saniyeler sürüyor. Bir madenci hile yapmaya veya sahte bir blok eklemeye kalkarsa ağdaki herkes bunu anında görüyor ve reddediyor. Üstelik o madenci bu bilmeceyi çözmek için ciddi miktarda elektrik ve donanım harcamış oluyor. **Yani dürüst davranmak hile yapmaktan çok daha kârlı hale geliyor.** Aksi durumda hem ödülü

kaybediyorsunuz hem de harcadığınız onca kaynak boşa gidiyor. Buna da oyun teorisi diyoruz. **Kuralları öyle kuruyorsunuz ki en akılcı hareket zaten dürüst olmak oluyor.**

Bu güvenliğin bir bedeli var elbette. Proof of Work ciddi miktarda elektrik tüketiyor. Zaten sistemin en çok eleştirilen yanı da bu.

Proof of Stake ise aynı soruna çok farklı bir çözüm getiriyor. Burada katılımcılar bilmece çözmek yerine kendi kripto paralarını ağa kilitliyor. Buna staking diyoruz. Ağ, kim ne kadar kilitlediğine bakarak yeni bloğu kimin onaylayacağına karar veriyor.

Peki burada dürüstlüğü ne garanti ediyor? Yine oyun teorisi, ama bu sefer enerji yerine doğrudan cebinizden çıkan bir risk üzerinden işliyor. Bir katılımcı ağa zarar verecek şekilde hile yapmaya kalkarsa kilitlediği kripto parasının bir kısmı ya da tamamı yakılıyor. Buna da **slashing** diyoruz. Yani PoW'da ceza boşa harcanmış elektrikken, PoS'ta ceza doğrudan kaybedilen sermaye.

Ama Proof of Stake'in de kendi sorunları var. En çok eleştirilen nokta sistemin doğası gereği "*zengin daha zengin olur*" dinamiğine yatkın olması. Ağa daha fazla

kripto para kilitleyen katılımcı yeni blokları onaylama ve ödül kazanma şansını da artırıyor. Buna bağlı bir başka risk ise merkezileşme. Büyük miktarda varlığı elinde tutan az sayıda katılımcı ya da staking havuzu zamanla ağ üzerinde orantısız bir söz sahibi olabiliyor. Proof of Work'te de benzer bir merkezileşme riski var fakat o tarafta sermaye yerine devasa madencilik donanımları ve ucuz elektriğe erişim belirleyici oluyor.

Yani her iki sistem de kendi ödünleşimini taşıyor. Biri güvenliği enerjiyle satın alıyor. Diğeri aynı güvenliği çok daha az enerjiyle ama farklı bir risk karşılığında sağlıyor. Hangisinin "***daha iyi***" olduğuna dair kesin bir cevap yok. İkisi de farklı bir bedeli tercih ediyor.

Coinler vs Tokenler

Kripto sohbetlerinde en sık karıştırılan iki kavram sanırım coin ve token. Aslında ikisi arasındaki fark oldukça basit.

Bir **“coin”** kendi blockchain ağına sahip olan dijital varlıktır. Bitcoin (BTC) ve Ethereum (ETH) bunlara örnek gösterilebilir.

Token ise kendi blockchain'ine sahip olmayan ve mevcut bir blockchain üzerinde oluşturulan dijital bir varlıktır.

Bunu kendi evi olmayan ancak başka birinin evinde yaşayan bir kiracıya benzetebiliriz.

Örneğin Ethereum ağı üzerinde oluşturulmuş binlerce token bulunur ve bunların büyük bir kısmı ERC-20 adı verilen ortak bir teknik standardı kullanır. USDC, LINK, UNI ve AAVE gibi projeler Ethereum ağı üzerinde çalışan ERC-20 tokenlerine örnek olarak gösterilebilir.

Kısacası **coin** kendi ağına sahipken **token** mevcut bir blockchain'in altyapısından yararlanarak çalışır.

Bir projenin kendi ağını kurması devasa bir mühendislik işi ve büyük bir güvenlik sorumluluğu anlamına gelir. Token olarak kalmak ise daha hızlı, daha ucuz ama var olan ağın kısıtlarına ve risklerine bağımlı kalmak demektir.

Yani token veya coin kavramları için “bu bundan daha iyidir” demek zor. Her iki tarafın da belirli **avantajları** ve **spesifik kısıtlamaları** mevcut.

Stablecoin'ler

Kripto paralara yöneltilen en büyük eleştirilerden biri fiyatındaki oynaklık, yani volatilite. Bitcoin bir günde yüzde beş yükselip ertesi gün yüzde beş düşebiliyor.

Böylesine volatil bir varlığı kullanarak bir bardak kahve satın aldığınızı düşünsenize, kahvenin fiyatı siz onu bitirene kadar değişmiş olabiliyor.

Stablecoin'ler ise bu gibi durumlar için var. Stablecoin'lerin değeri genellikle Dolar, Euro, Japon Yeni veya Çin Yuanı gibi fiat para birimlerine **sabitlenmiş**[4] oluyor. Bu yüzden bir stablecoin her zaman yaklaşık bir dolar civarında kalmaya çalışıyor. USDT ve USDC ise bu alandaki en tanıdık isimler.

Stablecoin'leri kripto dünyası ile geleneksel finans arasında bir liman gibi düşünmek de mümkün. Piyasa dalgalandığında bir yatırımcı varlığını USDT veya USDC'ye dönüştürüp bekleyebilir. Böylelikle banka gibi

[4] **Peg (Sabitleme):** Bir para biriminin veya dijital varlığın değerinin başka bir varlığa sabitlenmesi uygulamasıdır. Bu varlık genellikle ABD doları gibi bir para birimi, altın veya başka bir finansal gösterge olabilir. Örneğin birçok stablecoin değerini yaklaşık 1 ABD dolarında tutmayı hedefleyen bir peg mekanizmasıyla çalışır.

bir kuruluşa geri dönmeden söz konusu varlığın değerini bir bakıma “sabitlemiş” olur.

Yine de kesinlikle uyarmalıyım ki her stablecoin’in güvenlik seviyesi ve rezerv stratejisi aynı değil. Bazı stablecoin'ler gerçek dolar rezervleri ile desteklenirken bazıları algoritmik yöntemlerle ayakta duruyor. İkinci grup biraz daha kırılgan.

Nitekim 2022'de yaşanan Terra/Luna çöküşü bunun bir örneği. Rezerv yerine algoritmik bir mekanizmaya güvenen UST, güven kaybının tetiklediği bir satış dalgasında peg'ini kaybetti ve birkaç gün içinde kardeş tokeni Luna ile birlikte neredeyse sıfırlandı. O hafta piyasadan buharlaşan değer 40 milyar doları aştı. İnanılmaz bir rakam[5]. Bu olaya da değinmeden geçemedim, çünkü "stabil" kelimesi her zaman gerçek bir garanti anlamına gelmiyor.

Peki stablecoin alanındaki bu risk nasıl yönetilebilir? Buradaki yaygın yaklaşım yalnızca tek bir stablecoin'e güvenmek yerine varlığı birkaç farklı stablecoin arasında dağıtmak. Mantık basit. Tüm yumurtalar tek

[5] Bir insanın her gün 100.000 dolar (≈ 4.700.000TL) harcadığı varsayılsa bile 40 milyar doları ($40.000.000.000) tüketmesi yaklaşık 1.100 yıl sürer.

sepette olmayınca bir stablecoin sorun yaşadığında bile elinizdeki değerin tamamı risk altında kalmıyor.

Küçük miktarlarda bu yaklaşımın getirisi göze pek çarpmayabilir, hatta işlem ücretleri bile bu avantajı eritebilir. Fakat miktar büyüdükçe bu dağıtma stratejisi karşılığını fazlasıyla verebiliyor.

Elbette hangi stablecoin'lerin güvenilir bulunduğu ve varlığın nasıl dağıtılacağı tamamen kişisel bir tercih. Önemli olan körü körüne bir seçim yapmak yerine her stablecoin'in arkasındaki teminat yapısını ve şeffaflığını kendi araştırmanızla değerlendirmek.

NFT'ler

Gelelim bir dönem herkesin konuştuğu NFT'lere. NFT, Non-Fungible Token ifadesinin kısaltmasıdır ve Türkçeye "değiştirilemez token" olarak çevrilebilir[6].

Peki neden değiştirilemez (non-fungible) diyoruz, hemen anlatayım.

---

[6] **NFT (Non-Fungible Token):** Türkçede zaman zaman "**nitelikli fikri tapu**" olarak da çevrilir. Ancak yaygın kullanımda İngilizce kısaltma olan **NFT** tercih edilmektedir.

Bir Bitcoin başka bir Bitcoin ile birebir aynı. Sizden bir Bitcoin alsam ve size başka bir Bitcoin versem hiçbir şey fark etmez.

1 Bitcoin = 1 Bitcoin.

Fakat bir NFT öyle değil. Her biri eşsiz ve kendine has bir kimlik taşıyor. Sahipliği ise blockchain üzerinde tartışmasız biçimde kayıtlı.

NFT'ler 2021 yılında adeta bir çılgınlığa dönüşmüştü. Tuvalet kâğıdı resimleri milyonlarca dolara satıldı, herkes bir NFT koleksiyonu çıkarmaya çalıştı, arsalar, tapular, metaverse anlatısı havada uçuştu.

Ama dürüst olmak gerekirse o dönemin oldukça büyük bir kısmı gerçek kullanım alanından ziyade saf bir spekülasyondan ibaretti.

İnsanlar NFT'ler ile ne yapacağından ziyade bir sonraki alıcıya daha pahalıya satıp satamayacağını düşünüyordu. **Hype**[7] söndüğünde fiyatların büyük bölümü de onunla birlikte çöktü.

---

[7] **Hype:** Bir kişi, proje veya varlık hakkında oluşan yoğun ilgi, beklenti ve heyecan ortamını ifade eder. Hype, fiyatların kısa vadede hızla yükselmesine neden olabilse de her zaman gerçek değeri yansıtmayabilir.

Ama tüm bu yaşananlar NFT'lerin işe yaramadığı anlamına da gelmiyor. Tam tersine hype geçtikten sonra geride kalan gerçek kullanım alanları çok daha net görünür hale geldi.

Bununla birlikte bu örüntü NFT'lere ya da kripto dünyasına özgü değil. Yeni bir teknoloji ortaya çıktığında neredeyse hep aynı senaryo tekrar ediyor.

İnternetin ilk yıllarında da benzer bir çılgınlık yaşandı. Hemen hemen her şirket sihirli bir ".com" dokunuşuyla hisse değerini şişirdi, sonra balon patladı ve geriye gerçekten iş yapan Amazon, Google gibi birkaç oyuncu kaldı.

Sanal gerçeklik gözlükleri de benzer bir yol izledi. Önce "herkesin evinde olacak" denildi, hype söndü, şimdi daha dar ama gerçek kullanım alanlarında (oyun, eğitim, endüstriyel simülasyon, vb.) sessizce yoluna devam ediyor.

Aslı önemli olan bir teknolojinin etrafındaki gürültü dindiğinde geride ne kaldığı/ kalacağı.

RWA (Real World Assets)

Elinizde bir gayrimenkul, bir tahvil ya da bir sanat eseri olduğunu düşünün. Bu varlığı blockchain

üzerinde bir token haline getirebilseniz ne olurdu? RWA olurdu.

Ufak bir soru işareti oluşmuş olabilir, RWA az önce anlattığımız NFT'ye benzemiyor mu? Kısmen benziyor. İkisi de gerçek bir şeyi temsil eden bir token. Ama NFT eşsizken (non-fungible, yani iki NFT birbirinin yerine geçmez) RWA genelde bölünebilir ve birbiriyle değiştirilebilir bir değeri temsil eder.

Konuya geri dönelim. Geleneksel piyasalarda bir işlemin sonuçlanması günler sürebiliyor. Blockchain üzerinde ise bu süre çoğu zaman saniyelere iniyor. Üstelik piyasalar yalnızca mesai saatlerinde değil günün her saati erişilebilir durumda.

Bu dönüşümün en önemli sonuçlarından biri yüksek değerli varlıkların çok daha küçük parçalara bölünebilmesi. Normal şartlarda yüz binlerce dolarlık bir ticari gayrimenkule ortak olmak çoğu yatırımcı için mümkün değilken tokenizasyon sayesinde aynı varlığın küçücük bir payına sahip olmak mümkün hale geliyor.

Böylece daha önce yalnızca büyük sermayeye açık olan yatırım fırsatları çok daha geniş bir yatırımcı kitlesine ulaşıyor.

Bu potansiyel yalnızca teori ile kısıtlı değil.

Son yıllarda dünyanın en büyük finans kuruluşları da RWA alanına ciddi yatırımlar yapıyor. Tokenize edilmiş **devlet tahvili fonları**[8] hızla büyürken dünyanın önde gelen varlık yönetim şirketlerinden bazıları da kendi tokenize yatırım ürünlerini piyasaya sürüyor.

Governance Tokenler

Bir projenin geleceğine dair söz hakkınız olsun ister misiniz? Bazı kripto projeleri governance tokenler ile proje içi oylama hakkı sunuyor.

Governance tokene sahip olan bir kişi protokolün nasıl güncelleneceğine dair oy kullanabiliyor. Hangi parametrelerin değişeceğine, hangi yeni özelliklerin ekleneceğine, hatta bazen hazinedeki fonların nasıl kullanılacağına bile karar verebiliyor. Bu yapı **DAO**[9]

---

[8] **Devlet Tahvili Fonu:** Yatırımcıların parasını ağırlıklı olarak devlet tahvillerine yatıran yatırım fonudur. Devlet tahvili, devletlerin borç para toplamak için çıkardığı ve belirli bir vade sonunda faiziyle geri ödediği borçlanma aracıdır. Bu fonlar, hisse senedi fonlarına göre genellikle daha düşük riskli kabul edilir.

[9] **DAO (Decentralized Autonomous Organization):** Kararların tek bir kişi veya kurum yerine topluluk tarafından alındığı bir yönetim modelidir. Kurallar ve karar alma süreçleri büyük ölçüde akıllı sözleşmelerle yürütülür.

dediğimiz merkeziyetsiz otonom organizasyonların temelini oluşturuyor. Uniswap, MakerDAO gibi büyük protokoller bu modelle yönetiliyor.

Bu model kulağa demokratik gelse de işin aslı biraz karışık.

İlk sorun katılım. Çoğu DAO'da oylamalara katılım oranı şaşırtıcı derecede düşük kalıyor.

İkinci sorun ise daha yapısal. Kararların büyük kısmı elinde çok token bulunduran az sayıdaki kişi tarafından şekilleniyor. Buna **whale (balina) dominasyonu** diyoruz. Kağıt üzerinde herkes eşit görünüyor. Ama pratikte klasik bir şirketin hisse yapısından çok da farklı olmayan bir güç dengesi ortaya çıkabiliyor. Ne kadar token, o kadar söz hakkı.

Bu soruna karşı bazı projeler **kuadratik oylama** gibi modelleri deniyor. Bu tarafta da mantık şöyle işliyor, standart sistemde 10 tokeniniz varsa 10 oyunuz oluyor. Oy gücünüz token sayınızla doğru orantılı büyüyor. Kuadratik oylamada ise oy gücünüz token sayısının kareköküyle artıyor. Yani on kat daha fazla tokene sahip olmak size on kat değil, sadece yaklaşık üç kat daha fazla oy gücü kazandırıyor. Küçük yatırımcıların

sesi tamamen bastırılmıyor. Büyük cüzdanların etkisi de yumuşatılmış oluyor[10].

Bir başka çözüm de delegasyon. Kendi başınıza her oylamayı takip etmek istemiyorsanız oy hakkınızı güvendiğiniz birine devredebiliyorsunuz, o kişi de sizin adınıza oy kullanmış oluyor. Bu sayede pasif token sahipleri de en azından dolaylı yoldan sürece dahil olabiliyor.

Yine de gerçekçi olmakta fayda var. Bu çözümler sorunu tamamen ortadan kaldırmıyor, sadece hafifletiyor. DAO'lar halen genç bir yönetim deneyi. Zaman içinde olgunlaşmaya devam etse de şu an için "*tam demokrasi*"den ziyade "*gelişmekte olan bir katılım modeli*" demek daha doğru olur.

Memecoin'ler

Bazı kripto paralar teknolojiden ziyade bir şakadan veya anlatıdan doğuyor. Son yıllarda yeni bir coin

---

[10] Kuadratik oylamanın da bir açığı var. Buna **Sybil saldırısı** diyoruz. Bir kişi token'larını tek bir büyük cüzdanda tutmak yerine yüzlerce küçük cüzdana bölüp her birinden ayrı oy kullanırsa, sistemin "az token, çok oy gücü" mantığını manipüle edilebiliyor. Çünkü sistem farklı cüzdanları farklı kişiler sanıyor ve gerçek kimlik doğrulaması yapmıyor.

çıkarmak o kadar kolaylaştı ki artık her gün yüzlercesi doğuyor ve çoğu **birkaç saat içinde** değersizleşiyor.

Bu projelerin arkasında çoğu zaman somut bir teknoloji ya da kullanım amacı yok, değeri de çoğu zaman topluluk ilgisine ve sosyal medya gündemine bağlı.

Size net bir şey söylemek istiyorum. Memecoin'lere para yatırmak yatırım yapmaktan çok bir kumar masasına oturmaya benziyor. Fiyat hareketleri spekülasyon ve hype tarafından belirleniyor, ki bu da memecoin'leri son derece riskli kılıyor.

"Yatırımın ilk amacı olağanüstü kazanç elde etmek değil, kalıcı sermaye kaybından kaçınmaktır."

— Howard Marks

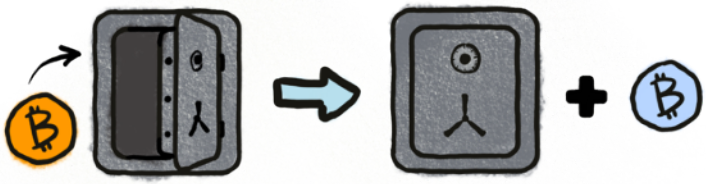
Liquid Staking Tokenler (LST)

Önce staking kavramının tanımı ile başlayalım. **Kripto paranızı belirli bir süre boyunca ağa kilitleyerek karşılığında ödül kazanma yöntemi.** Ancak her zaman olduğu gibi bu ödülün de bir bedeli var. Varlığınız kilitli olarak kaldığı için o süre boyunca

satamaz, transfer edemez veya başka bir amaçla kullanamazsınız.

Liquid staking bu sorunu çözmek için ortaya çıktı. Varlığınızı stake ettiğinizde karşılığında stake edilmiş varlığı temsil eden yeni bir token alırsınız. Bu tokene **Liquid Staking Token (LST) denir.**

Örneğin Ethereum'unuzu stake ettiğinizde elinize **stETH** gibi bir LST geçebilir. Orijinal ETH'niz ağda stake edilmiş halde kalır ve ödül kazanmaya devam eder. Elinizdeki stETH ise satılabilir, transfer edilebilir veya DeFi uygulamalarında kullanılabilir.



LST'leri bankada kasaya koyduğunuz değerli bir eşya karşılığında size verilen makbuza benzetebilirsiniz. Liquid staking'in de temel fikri de budur. Varlığınız getiri üretmeye devam ederken onu temsil eden token sayesinde likiditenizi büyük ölçüde korursunuz.

Wrapped Assets

Her bir blockchain'i kendi kurallarıyla yaşayan izole bir ada gibi düşünebiliriz. Bitcoin adasındaki bir varlığı doğrudan Ethereum adasında kullanamayız. Çünkü bu iki ada birbiriyle aynı dili konuşmuyor. Wrapped assets bu adalar arasına bir köprü kurmak için geliştirildi.

Peki bu köprü tam olarak nasıl çalışıyor? Bir varlık wrap edildiğinde orijinali bir akıllı kontratta kilitleniyor. Bu kilitlenen varlık hiçbir yere gitmiyor, sadece bekliyor. Bunun karşılığında başka bir ağda kilitli varlığın değerini birebir yansıtan yeni bir token basılıyor. En bilinen örnek WBTC, yani wrapped Bitcoin. Elinizdeki bir Bitcoin bir akıllı kontrata kilitleniyor ve karşılığında Ethereum ağında bir WBTC tokeni oluşturuluyor. Bu tokeni istediğiniz gibi

Ethereum'daki DeFi protokollerinde kullanabiliyorsunuz. Oysa normal Bitcoin bunu yapamazdı çünkü Bitcoin ağı DeFi'ın karmaşık akıllı kontrat işlemlerini desteklemiyor.

İşin can alıcı noktası şu, WBTC'nin değeri her zaman gerçek Bitcoin'in değerine bağlı kalıyor. Çünkü elinizdeki her WBTC tokenin karşılığında bir yerlerde gerçek bir Bitcoin kilitli duruyor. WBTC'nizi geri "unwrap" ettiğinizde (yani orijinal haline döndürdüğünüzde) token yakılıyor ve kilitli Bitcoin serbest bırakılıyor.

Peki burada bir risk yok mu? **Var.** Kilitli varlığın güvenliği o kilitleme işlemini yöneten tarafa bağlı. Bazı wrapped asset'lerde bu işlemi merkezi bir kurum yürütüyor, bazılarında ise akıllı kontratlar ve doğrulayıcı ağlar. Kilitleme mekanizması ne kadar merkeziyse, o kurumun elinizdeki gerçek varlığa ne kadar güvenilir davrandığına da o kadar bağlı kalıyorsunuz. Bir sonraki başlıkta konuşacağımız cross-chain köprülerdeki hack riskleri de büyük ölçüde bu noktadan kaynaklanıyor.

Sırada Ne Var?

Tebrik ederim, olabilecek en bilgi bombardımanlı bölümü bitirdin. Bu bölümde kripto paraların temel yapı taşlarını ve karşına çıkabilecek farklı varlık sınıflarını gördük. Ama şunu unutma, bu varlıkların hiçbiri boşlukta yaşamıyor. Hepsi bir ekosistemin içinde ve birbirine bağlı biçimde var oluyor. Katman 1 ve Katman 2 ağlar, oracle'lar, cross-chain köprüler, tüm bu parçaların birbirine nasıl bağlandığını bir sonraki bölümde birlikte keşfediyoruz.

(Ödül: Daha az bilgi bombardımanı içeren Bölüm 3 ⬇ :)

Bölüm 3: Ekosistem Katmanları

Bir önceki bölümde blockchain'leri izole adalara benzetmiştik. Ama hiçbir ada sonsuza kadar yalnız kalmıyor. Bu bölümde o adaların birbirine nasıl bağlandığını, aralarındaki köprülerin nasıl kurulduğunu ve blockchain'in dış dünyayla nasıl konuştuğunu görüyoruz.

Katman 1 ve Katman 2 (L1 & L2)

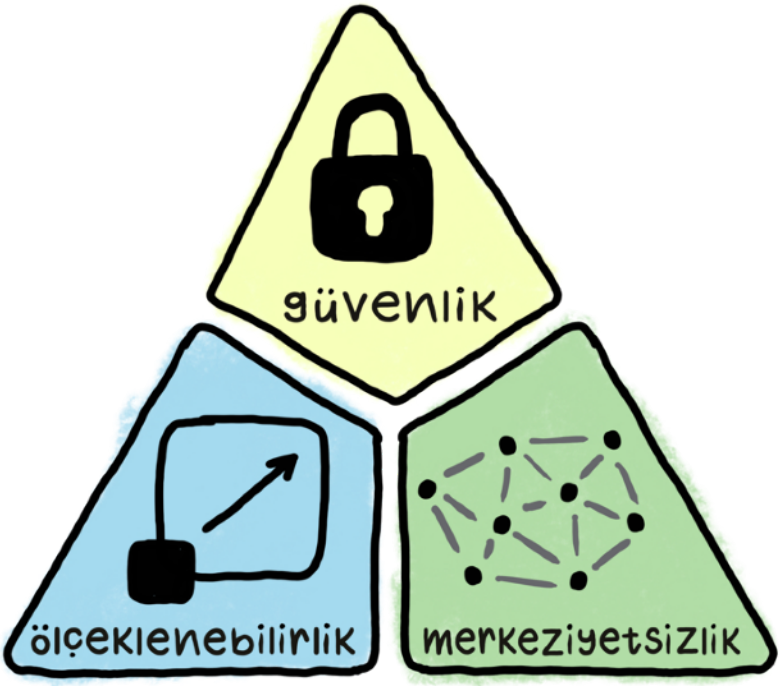
Bir blockchain'in temel katmanına Katman 1 diyoruz. Bitcoin bir Katman 1, Ethereum bir Katman 1, Solana da bir Katman 1.

Bu ağların her biri kendi kurallarını, kendi güvenlik modelini ve kendi konsensus mekanizmasını belirliyor.

Peki neden tek bir mükemmel Katman 1 yapıp işi bitirmiyoruz? Burada karşımıza kripto dünyasının en çok bilinen ödünleşimlerinden (trade-off) biri çıkıyor. Buna **blockchain trilemma** diyoruz.

Bir ağ aynı anda tam olarak üç şeyi sağlamakta zorlanıyor.

Ölçeklenebilirlik, güvenlik ve **merkeziyetsizlik.**



Birini artırmaya çalıştığınızda genelde diğerinden ödün vermeniz gerekiyor[11].

Katman 2 çözümleri de bu noktada devreye giriyor. Katman 1'in güvenliğini kullanan ama işlemlerin büyük kısmını kendi üzerinde çok daha hızlı ve ucuz biçimde işleyen ek bir katman oluşturuyorlar.

İşlemler burada toplanıyor ve işleniyor. Ardından sonuçlar özetlenmiş halde ana ağa, yani Katman 1'e kaydediliyor. Böylece hem hız kazanılıyor hem de temeldeki güvenlikten büyük ölçüde ödün verilmiyor.

---

[11] **Bitcoin**: **Güvenlik** ve **merkeziyetsizlik** konusunda en güçlü blokzincirlerden biri olarak kabul edilir. Ağa binlerce bağımsız düğüm katkı sağlar ve ağı ele geçirmek oldukça zordur. Buna karşılık saniyede gerçekleştirebildiği işlem sayısı düşük olduğu için **ölçeklenebilirlik** açısından sınırlıdır.

EOS: Yüksek işlem kapasitesi sunacak şekilde tasarlanmıştır. Kararlar sınırlı sayıdaki doğrulayıcı tarafından alındığı için işlemler hızlı gerçekleşebilir ve **ölçeklenebilirlik** artar. Ancak bu yapı **merkeziyetsizlik** ve işlem hızı avantajı sağlasa da **güvenlik** açısından daha fazla eleştirilmesine neden olmuştur.

Solana: Çok yüksek işlem hızına ulaşmayı hedefleyen bir blokzincirdir. Bu sayede **ölçeklenebilirlik** konusunda öne çıkar ve güçlü bir **güvenlik** modeli sunmayı amaçlar. Ancak doğrulayıcı olmak için gereken donanım maliyetinin yüksek olması ağa daha az kişinin katılabilmesine yol açar. Bu nedenle **merkeziyetsizlik** açısından sıkça eleştirilir.

Bunu bir banka şubesi gibi düşünebilirsiniz.

Katman 1, bankanın genel merkezi gibi. Tüm resmi kayıtlar burada tutuluyor. Ancak herkes en küçük işlemi bile genel merkeze taşısaydı büyük bir yoğunluk oluşurdu.

Katman 2 ise banka şubeleri gibi çalışıyor. Günlük işlemler şubelerde hızlıca gerçekleştiriliyor. Ardından bu işlemlerin özeti genel merkeze gönderiliyor ve resmi kayıtlara işleniyor. Böylece hem işlemler hızlanıyor hem de tüm sistem tek bir güvenilir kayıt üzerinde çalışmaya devam ediyor.

Oracle Ağları

Şimdi biraz daha ilginç bir soruna geliyoruz. Blockchain'ler kendi başlarına dış dünyadan habersiz. Bir **akıllı kontrat**[12] bugün doların ne kadar olduğunu, yarın hava durumunun ne olacağını ya da bir maçın sonucunu kendi başına bilemiyor. Çünkü blockchain

[12] **Akıllı kontrat (smart contract):** Belirli koşullar gerçekleştiğinde önceden tanımlanmış kuralları otomatik olarak yerine getiren, blokzincir üzerinde çalışan ve sonradan tek taraflı olarak değiştirilemeyen bilgisayar kodlarıdır. Aracı bir kuruma ihtiyaç duymadan işlemlerin güvenli ve şeffaf biçimde yürütülmesini sağlar.

kendi ağının dışına çıkıp bilgi toplayamayan kapalı bir kutu gibi çalışıyor.

Peki örneğin bir **DeFi protokolü**[13] borç verirken teminatın güncel piyasa değerini nereden öğreniyor?

Cevap oracle ağlarında saklı. Oracle'lar blockchain ile dış dünya arasında bir "*çevirmen*" ve "*taşıyıcı*" görevi görüyor. Dışarıdaki veriyi topluyor, doğruluyor ve blockchain'in anlayabileceği bir formatta ağa taşıyor.

Bu alanda en çok bilinen isim Chainlink. Teknik olarak Chainlink birbirinden bağımsız çalışan node (düğüm) ağlarından oluşuyor. Her node kendi kaynağından veri çekiyor. Bu veriler birbiriyle karşılaştırılıyor ve aykırı sonuçlar eleniyor. Sonunda ortaya çıkan tek bir değer ağa "*resmi fiyat*" olarak sunuluyor. Bu sayede tek bir kaynağın yanlış ya da manipüle edilmiş veri vermesi sistemi tek başına yanıltamıyor[14].

---

[13] **DeFi Protokolü:** Banka veya aracı kurum gibi bir kuruluşa ihtiyaç duymadan finansal işlemler yapılmasını sağlayan blokzincir tabanlı uygulamadır. Bu uygulamalar, borç verme, borç alma, alım satım ve faiz geliri elde etme gibi işlemleri akıllı sözleşmeler aracılığıyla gerçekleştirir.

[14] Chainlink'in merkeziyetsiz oracle mimarisi ve düğümlerin (node) nasıl uzlaşmaya vardığıyla ilgili teknik detaylar için projenin resmi dokümantasyonuna (docs.chain.link) veya 2017 tarihli orijinal Whitepaper'ına bakabilirsiniz.

Mesela bir DeFi protokolü Bitcoin'in güncel fiyatını bilmesi gerektiğinde bu tür oracle ağlarına başvuruyor. Oracle'lar sadece fiyat verisi de taşımıyor. Rastgele sayı üretimi, hava durumu, spor sonuçları, hatta gerçek dünyadaki bir olayın gerçekleşip gerçekleşmediği gibi çok çeşitli bilgiler de bu ağlar üzerinden blockchain'e taşınabiliyor.

Bu alan sadece Chainlink'ten ibaret de değil. Pyth Network borsalardan ve yüksek frekanslı işlem firmalarından gelen verileri doğrudan zincire taşıyan farklı bir mimari kuruyor. Band Protocol benzer bir modeli Cosmos ekosisteminde uyguluyor. API3 veri sağlayıcılarının kendi node'larını doğrudan işletmesine imkan tanıyan bir yaklaşım benimsiyor. RedStone ise özellikle düşük maliyetli ve modüler bir oracle altyapısı sunmasıyla dikkat çekiyor. Her birinin kendi mimari tercihleri ve ödünleşimleri var. Hangisinin bir protokol için doğru seçim olduğu o protokolün ihtiyaçlarına göre değişiyor.

Oracle'ların önemi ilk bakışta göz ardı edilebilir. Ama aslında ekosistemin en kritik güvenlik noktalarından biri burası. Yanlış ya da manipüle

edilmiş bir fiyat verisi koca bir protokolü çökertebiliyor.

Nitekim geçmişte birçok saldırgan doğrudan protokolü hacklemek yerine protokolün güvendiği fiyat verisini manipüle ederek haksız kazanç sağlıyor (buna oracle manipülasyonu diyoruz).

Bu yüzden güçlü bir oracle altyapısı günümüzde sağlam bir DeFi projesinin olmazsa olmaz parçalarından biri.

Cross-chain / Interoperability

Bir önceki bölümde wrapped assets'ten bahsederken adalar arasında köprü kurmaktan söz etmiştik. Şimdi bu köprü fikrini biraz daha genişletelim.

Bugün yüzlerce farklı blockchain var ve bunların çoğu birbirinden habersiz şekilde kendi kuralları ve kendi kullanıcı tabanıyla çalışıyor. Bir kullanıcı olarak bu parçalanmışlık bizim için ne anlama geliyor? Ethereum'da tuttuğumuz bir varlığı doğrudan Solana ağında kullanamıyoruz, bu yüzden de arada çeviri bir katmana ihtiyaç duyuyoruz.

Cross-chain teknolojileri ve köprüler bu ihtiyacı karşılıyor. Bir köprü bir ağdaki varlığı kilitleyip başka

bir ağda o varlığı temsil eden yeni bir token oluşturuyor, ya da doğrudan iki ağ arasında mesaj ve veri akışı sağlayarak protokollerin birbiriyle konuşmasına imkan tanıyor.

Ama burada da bir uyarı yapmam gerek. Köprüler kripto dünyasının en sık hacklenen noktalarından biri. Büyük miktarda varlığın tek bir akıllı kontratta kilitlenmesi saldırganlar için son derece cazip bir hedef oluşturuyor. Geçmiş yıllarda birkaç büyük köprü hackinde yüzlerce milyon dolarlık kayıplar yaşandı. **Bu yüzden herhangi bir köprü kullanırken o köprünün güvenlik geçmişine ve denetim raporlarına bakmak yalnızca hız ve ücret avantajına bakmaktan çok daha kritik.**

Sırada Ne Var?

Bu bölümde blockchain ekosisteminin nasıl büyüdüğünü, ölçeklendiğini ve birbirine bağlandığını gördük. Ama tüm bu altyapı boşuna kurulmuyor. Bir sonraki bölümde bu altyapının üzerine inşa edilen DeFi dünyasına, yani merkeziyetsiz finansa geçiyoruz.

Bölüm 4: DeFi (Merkeziyetsiz Finans)

Bir bankaya gitmeden borç almak, borç vermek ya da para takas etmek mümkün olsa nasıl olurdu? Bu bölümde, şimdiye kadar incelediğimiz tüm bu altyapılar sayesinde, bankasız bir finans sisteminin pratikte nasıl işlediğini göreceğiz.

DEX, Lending ve Staking Temelleri

Geleneksel bir borsada işlem yapmak istediğinizde alıcı ve satıcıları eşleştiren bir aracıya ihtiyaç duyarsınız.

DEX, yani merkeziyetsiz borsa, bu aracıyı ortadan kaldırıyor. Peki alıcı ve satıcı olmadan bir takas nasıl gerçekleşiyor? Cevap likidite havuzlarında saklı. Kullanıcılar iki farklı varlığı belirli oranlarda bir havuza kilitliyor. Siz takas yapmak istediğinizde karşınıza bir insan değil, bu havuz çıkıyor. Fiyat, havuzdaki varlıkların oranına göre otomatik olarak hesaplanıyor.

Buna otomatik piyasa yapıcı diyoruz. **Uniswap**[15] bu modelin en bilinen örneği. Havuza varlık kilitleyen kişiler ise karşılığında işlem ücretlerinden pay alıyor. Buna likidite sağlama, bu kişilere de likidite sağlayıcı (LP / Liquidity Provider) diyoruz.

Lending protokolleri[16] ise bankaların kredi işlevini merkeziyetsiz hale getiriyor. Burada önemli bir fark var. Geleneksel bankada kredi verilmeden önce kredi notunuza bakılıyor. DeFi tarafında ise böyle bir şey yok.

Bunun yerine borç almak isteyen kişi aldığı borcun değerinden daha fazla teminatı önceden kilitlemek zorunda. Buna aşırı teminatlandırma diyoruz.

Teminatın değeri düşerse sistem otomatik olarak bu teminatı satışa çıkarıp borcu kapatıyor. Aave ve Compound ise bu alanın öncü isimleri.

---

[15] **Uniswap:** Ethereum ağı üzerinde çalışan en popüler merkeziyetsiz borsalardan (DEX) biridir. 2018 yılında faaliyete geçen Uniswap, alıcı ve satıcıları eşleştirmek yerine likidite havuzlarını kullanan modeliyle DeFi ekosisteminin büyümesinde önemli rol oynamıştır.

[16] **Lending Protokolü:** Kullanıcıların kripto varlıklarını ödünç verebildiği veya teminat göstererek borç alabildiği DeFi uygulamasıdır. Varlığını ödünç veren kullanıcılar faiz geliri elde ederken, borç alan kullanıcılar gösterdikleri teminat karşılığında kripto varlık kullanabilir.

Yield ve Riskleri

DeFi dünyasında sürekli duyacağınız başka bir kelime ise yield. Basitçe elinizdeki varlığı çalıştırıp kazandığınız getiri. Peki bu getiri nereden geliyor? Bazen işlem ücretlerinden, bazen borç alan kişilerin ödediği faizden, bazen de protokolün kendi tokenini dağıtarak kullanıcıyı teşvik etmesinden.

2020 yazında yaşanan ve DeFi Summer olarak anılan dönemde bazı protokoller yüzde binlerle ifade edilen yıllık getiriler vaat etti. Bu rakamlar kulağa her ne kadar harika gelse de gerçekte oldukça sürdürülemezdi.

Böylesine yüksek getiriler genelde ya kısa vadeli bir teşvik, ya da daha kötüsü, bir tuzak işaretidir.

Bunun yanında likidite sağlayanların karşılaştığı özel bir risk daha var, geçici kayıp.

Havuzdaki iki varlığın fiyat oranı değiştiğinde likidite sağlayan kişi varlığını havuza hiç koymamış olsaydı elde edeceğinden daha az değerle karşılaşabiliyor.

Bunun üzerine bir de akıllı kontrat riski eklendiğinde (protokolün koduna gizlenmiş bir hata ya

da açık) tüm havuzun bir gecede boşalmasına yol açabiliyor.

DeFi Tarafında Dikkat Edilmesi Gerekenler

Peki bir protokole güvenip güvenmeyeceğinizi nasıl anlarsınız? Birkaç somut işaret var. Öncelikle denetim raporlarına bakın. Bağımsız güvenlik firmaları tarafından kontrol edilmemiş bir kod üzerine büyük miktarda varlık koymaya değmez. Protokolün ne kadar süredir aktif olduğu da önemli. Yeni çıkmış ve hiç test edilmemiş bir sistemle uzun süredir sorunsuz çalışan bir sistem doğal olarak aynı risk seviyesinde değil. Kilitli toplam değer (yani TVL) bir protokolün ne kadar güven topladığını gösteren kaba bir gösterge olabilir ama tek başına yeterli değil çünkü bu rakam kolaylıkla manipüle edilebiliyor.

En önemlisi, **eğer bir getiri gerçek olamayacak kadar iyi görünüyorsa, muhtemelen gerçek değildir[17].** DeFi bize bankasız bir finans sistemi sunsa da bu özgürlüğün bir eksisi var. **Kişisel güvenliğimizin**

[17] **Too good to be true:** Gerçek olamayacak kadar iyi görünen teklif veya vaatleri ifade eden İngilizce bir deyimdir.

sorumluluğu artık tamamen bizde. Kimse bizi arayıp "bu riskli" demiyor. O kararı biz kendimiz vermek zorundayız.

Sırada Ne Var?

Bu bölümde parayı bir bankaya ihtiyaç duymadan nasıl çalıştırabileceğinizi gördük. Bir sonraki bölümde yatırım yaparken nelere dikkat etmeniz gerektiğine ve temel analize geçiyoruz.

Bölüm 5: Yatırım ve Temel Analiz

Bir önceki bölümde parayı bir bankaya ihtiyaç duymadan nasıl kullanabileceğimizi gördük. Şimdi bir adım geriye çekilme vakti. Elinizde artık kripto paraların ne olduğuna, hangi kategorilere ayrıldığına, ekosistemin nasıl işlediğine ve DeFi'ın ne sunduğuna dair sağlam bir zemin var. Ama tüm bu bilgiler ile ne yapacağız?

Bu bölümde iki şeye odaklanıyoruz, yatırım yaparken gözden kaçırmamanız gereken pratik noktalar ve bir projeyi ciddiye almadan önce sorgulamanız gereken sorular.

Yatırım Yaparken Dikkat Edilmesi Gerekenler

En başa, belki de kitabın en önemli cümlesine koyabileceğim bir prensip ile başlayalım. **Kaybetmeyi göze alamayacağınız parayı bu piyasaya sokmamak.** Kulağa klişe gelse de bu prensibe

uymayan çoğu insan er ya da geç zor bir deneyim yaşıyor. Kripto piyasası geleneksel piyasalara kıyasla çok daha volatil. Bir varlığın bir hafta içinde yarı yarıya değer kaybetmesi sıra dışı bir durumdan ziyade beklenmesi gereken bir ihtimal.

Peki bu oynaklıkla nasıl baş edilir? İlk araç çeşitlendirme (diversifikasyon). Tüm birikiminizi tek bir projeye yatırmak o projenin başarısına kişisel geleceğinizi bağlamak demek. Bunun yerine farklı projelere, farklı risk seviyelerine yayılmış küçük parçalar halinde yaklaşmak tek bir başarısızlığın büyük kayıplara yol açmasını engeller.

İkinci araç zaman ufku. Kripto piyasasına giren pek çok insan birkaç hafta içinde zengin olmayı hayal ediyor. Fakat gerçekte en sağlıklı yaklaşım yıllar ölçeğinde düşünmek. Kısa vadede fiyatlar duyguya, söylentiye ve spekülasyona göre hareket ediyor. Uzun vadede ise gerçek kullanım ve gerçek değer öne çıkma eğiliminde.

Bununla bağlantılı bir başka araç da düzenli alım stratejisi, yani **belirli aralıklarla sabit miktarda alım**

yapmak[18]. Bu şekilde bazen tepede, bazen dipte alım yapıyorsunuz ama zamanla ortalama maliyetiniz dengeleniyor ve tek bir alımın fiyatına bağımlı kalmıyorsunuz.

Bunun tam karşısında durması gereken bir davranış var, o da **kaldıraçlı işlem**[19]. Ödünç para ile pozisyon büyütmek kazancınızı büyütebileceği gibi **kaybınızı da kartopu etkisiyle büyütüyor.** Üstelik piyasa aleyhinize hareket ettiğinde **elinizdeki tüm varlığı bir anda kaybetme riski** de taşıyorsunuz.

Bu kitap boyunca anlattığımız yaklaşım büyük ve hızlı kazançların peşinden koşmak yerine **sermayeyi korumayı önceliklendirip zamanla istikrarlı ve sürdürülebilir bir büyüme yakalamak üzerine kurulu.** Bu bir tavsiye değil, kendi yatırım felsefemin bir özeti.

Kaldıraç ise tam tersini vaat ediyor, hızlı ve büyük kazanç, ama karşılığında sermayenin tamamını bir anda kaybetme ihtimali.

---

[18] **DCA (dollar-cost averaging):** Belirli aralıklarla, fiyatın yükselip düşmesine bakmaksızın sabit miktarda yatırım yapma stratejisi.

[19] **Kaldıraçlı İşlem:** Eldeki paradan çok daha büyük miktarlarla alım satım yapabilmek için borç imkânı kullanma yöntemidir.

Kaldıraçlı işlem severler burada kitabı okumayı bırakmasın. Bu satırların amacı sizi bu araçtan tamamen vazgeçirmek değil. Sadece şunu bilmenizi isterim ki kaldıraç kullananların büyük çoğunluğu zamanla sermayesinin önemli bir kısmını kaybediyor.

Eğer yine de kullanmayı tercih ederseniz riskinizi ne kadar küçük tuttuğunuz ve risk iştahınızı nasıl ayarladığınız büyük fark oluşturuyor. Kaldıracın kendisi değil, **kontrolsüz** ve **bilinçsiz kullanımı** tehlikeli.

Son olarak duygusal karar almaktan bahsetmem gerekiyor. **FOMO**[20] muhtemelen bu piyasada en çok para kaybettiren duygu. Bir varlığın fiyatı hızla yükseldiğinde içinizde "*tam şimdi almalıyım*" hissi uyanıyorsa bu genelde en kötü giriş anlarından biri. Çünkü o noktada zaten yükselişin büyük kısmı gerçekleşmiş oluyor.

Aynı şekilde panik satış da aynı hatayı tersten işlemek gibi. Sağlıklı yatırımın büyük bir kısmı aslında

[20] **FOMO (fear of missing out):** Bir yatırım fırsatını kaçırma korkusuyla, yükselen bir varlığa geç kalma endişesiyle düşünmeden yatırım yapma eğilimi.

piyasayı okumaktan çok kendi duygularınızı yönetmekten geçiyor.

Buraya kadar anlattığım şeyler zaten çoğu kişi tarafından az çok bilinen prensiplerdi.

Şimdi biraz daha sahaya inip bu piyasada kendi tecrübemle işe yaradığını gördüğüm birkaç kuraldan bahsetmek istiyorum. Bunları bir kural listesi olarak değil, benim için işe yarayan bir çerçeve olarak düşünebilirsiniz.

Öncelikle şunu bilin, bu piyasada bir yatırımınız varsa öğrenmeyi bırakmak o yatırımı kendi elinizle öldürmek demek. Piyasa her gün değişiyor, yeni anlatılar doğuyor, dün geçerli olan bir varsayım bir sonraki gün geçersiz kalabiliyor. Bir varlığı aldığınız günkü bilgi ile aylarca aynı pozisyonda kalmak, bir geminin rotasını yalnızca bir kez belirleyip sonra dümeni bırakmaya benziyor.

Portföy ağırlığını yanlış ayarlamak da benzer derecede tehlikeli. "*Bu varlık zaten yüksek piyasa değerine sahip, daha ne kadar yükselebilir ki*" ya da "*bu varlık zaten yükseleceği kadar yükseldi, sıra bu varlıkta*" gibi düşünceler kulağa mantıklı gelse de çoğu zaman sıfıra yaklaşmanın ilk ayak sesleri oluyor. Amacınız

"*hızlıca zengin olmak*" değil, sizi sıfıra götürme potansiyeline sahip davranışlardan olabildiğince uzak durmak olmalı. Hız kazanmak elbette güzel. Zaten sorun orada da değil. Sorun asimetrik riski doğru ayarlamadığınızda o hızın avantaja değil dezavantaja dönüşmesi. Aynı hızı yeşil değil de kırmızı bir mumla yaşayınca asıl hızın ne demek olduğunu çok daha net görüyor insan :)

Ben kendi adıma bir satış protokolü belirlemenin de faydalı olduğunu düşünüyorum. İnanılmaz ucuz bir fiyattan kaliteli bir varlık alabilirsiniz, devamında akıllara zarar bir kârla da karşılaşabilirsiniz. Asıl zor olan çoğu zaman buradan sonrası. Ne zaman çıkacağınızı önceden belirlemediyseniz yükselen fiyatın yarattığı heyecanla o varlığı taşımaya devam edebilir, sonunda neden halen elinizde tuttuğunuzu bile unutabilirsiniz. Yatırım, son durağa kadar gitmeniz gereken bir yolculuk değil. **Sizi gitmek istediğiniz yere götürecek bir biniş bileti.** Dolayısıyla ne zaman satacağınızı önceden belirlemek önemli.

Benzer şekilde elimde belirli bir nakit rezervi tutmak da benim için fazlasıyla işe yarayan bir alışkanlık oldu. Piyasada gerçek bir fırsat gördüğünüz

halde elinizde aksiyon alacak nakit olmaması can sıkıcı bir deneyim olabiliyor. Bu yüzden portföyde bir miktar nakit bulundurmak size esneklik kazandırabilir.

Tüm bunların dışında kendinizi ekrana kilitlemek de pek verimli bir alışkanlık değil bence. Fiyat yükselirken "*satayım mı*" diye, düşerken "*alayım mı*" diye saatlerce grafik izlemek hem yoruyor hem de duygusal kararlar aldırabiliyor. Bunun yerine **limit emir**[21] gibi araçlar o uzun nöbetten sizi kurtarabilir.

Son olarak çeşitlendirme konusunda dengeyi tutturmak da bir o kadar önemli. Portföyünüzü hiç çeşitlendirmemek sizi bitirebilir, ama gereğinden fazla çeşitlendirip elinizdeki tüm sermayeyi niteliksiz varlıklara harcamak da aynı şekilde bitirir. Bunu yalnızca finansal kayıp olarak da görmemek lazım. Fazla çeşitlendirmek **en değerli sermayeniz olan zamanınızı da kaybetmenize** neden olabilir.

Özetle amaç çok sayıda projeye sahip olmak değil, doğru sayıda ve doğru nitelikte projeye sahip olmak.

---

[21] **Limit Emir:** İstediğiniz fiyattan alım veya satım yapmak için sisteme verdiğiniz ön talimattır. Fiyat hedeflediğiniz noktaya ulaşana kadar işlem beklemede kalır.

Temel Analiz

Bu kitapta bilinçli bir tercih olarak teknik analize yer vermiyorum. Kısa vadeli fiyat grafiklerini okuyup örüntü aramak artık büyük ölçüde algoritmaların ve yüksek frekanslı yazılımların domine ettiği bir alan. Bir insanın grafik üzerindeki formasyonlara bakarak bu yazılımlara karşı avantaj elde edebileceğini hiç düşünmüyorum. Dolayısıyla enerjimi ve bu kitabın sayfalarını bu yönde harcamıyorum.

Yine belirtmeliyim ki bu bölümde yer alan şeyler kesin formüllerden ziyade kişisel bir bakış açısı.

Şimdi gelelim bir projeyi değerlendirirken nelere dikkat etmemiz gerektiğine ve hangi soruları sormanın bizim için daha faydalı olabileceğine.

Bir proje ile ilk karşılaştığımda genellikle tokenden önce projenin kendisine bakıyorum. Çünkü piyasada gördüğüm en yaygın hatalardan biri **iyi bir teknoloji** ile **iyi bir tokenin** aynı şey olduğunu varsaymak.

Oysa değiller.

Bir protokol gerçekten harika bir sorunu çözüyor olabilir. İnsanlar onu kullanıyor, teknoloji çalışıyor ve arkasındaki ekip oldukça başarılı olabilir. Ancak tüm bunlara rağmen o projenin tokeni tamamen anlamsız

bir amaca sahip olabilir. Mesela söz konusu token protokolün çalışması için gerçekten gerekli değildir, herhangi bir karar mekanizmasında kullanılmıyordur veya gelir ile arasında gerçek bir bağ yoktur. Sadece insanların alıp satabileceği bir varlık olarak ortada duruyordur.

Bu yüzden kendime ilk olarak **"Tokenin burada gerçekten ne işi var?"** sorusunu soruyorum.

İşlem ücretlerinde kullanılıyor mu? Yönetişimde bir karşılığı var mı? Staking mekanizmasının bir parçası mı? Protokolün ekonomik yapısında gerçekten bir yere sahip mi?

Bazı projeler de tokenlerinde farklı stratejiler izliyor. **Token yakımı**[22] ile dolaşımdaki arzı azaltıyor, **gelir paylaşımı**[23] yapıyor veya **geri alım**[24] mekanizmaları oluşturuyor.

---

[22] **Token Yakımı (Token Burn):** Belirli miktardaki tokenin kalıcı olarak dolaşımdan çıkarılması ve bir daha kullanılamaz hale getirilmesidir. Piyasada bulunan toplam miktarı azaltarak elde kalan varlıkların nadirliğini artırmayı hedefler.

[23] **Gelir Paylaşımı:** Platformun kazandığı gelirin belirli bir kısmını token sahiplerine dağıtma modelidir.

[24] **Geri Alım (Buyback):** Proje ekibinin elde ettiği kazançla piyasadaki kendi tokenlarını satın almasıdır. Piyasaya sürülen miktarı kısarak varlığın değerini korumayı amaçlar.

Bunların hiçbiri tek başına bir projeyi iyi yapmasa da tokenin neden var olduğunu anlamamız noktasında fazlasıyla yardımcı oluyor.

Tokenin işlevini anladıktan sonra ise genellikle gelire göz atıyorum.

"**Bu proje gerçekten para kazanıyor mu?"** sorusu bence kripto piyasasında en çok göz ardı edilen sorulardan biri.

Bir projenin anlatacak çok güzel bir hikâyesi olabilir. Geleceğin finans sistemini değiştireceğini, milyarlarca insana ulaşacağını veya tamamen yeni bir internet altyapısı kuracağını söyleyebilir. Bunların hepsi kulağa hoş da gelebilir. Fakat ortada gerçek bir kullanıcı ve gerçek bir gelir yoksa bir noktada hikâyeyle gerçekliği birbirinden ayırmak gerekiyor.

Gelir varsa bu kez başka bir soru ortaya çıkıyor. **"Bu para nereden geliyor ve nereye gidiyor?"**

Gerçek kullanıcılardan gelen istikrarlı bir ücret akışı ile tek seferlik bir anlaşmanın yarattığı büyük bir gelir rakamı aynı şey değil. Benzer şekilde protokolün kazandığı paranın ekibin cebine gitmesi ile protokolün kendi ekonomisine geri dönmesi arasında da önemli bir fark var.

Rakamların bugün küçük olması da bazen başlı başına kötü bir işaret değil. Eğer bu geliri artırabilecek somut ve gerçekçi bir mekanizma varsa küçük bir başlangıç oldukça normal. Asıl önemli olan bunun doğrulanabilir olması.

Bu noktada zincir üstü (on-chain) veriler ve bağımsız denetim raporları benim için projenin kendi sunumundan çok daha değerli. Çünkü bir ekibin kendisi hakkında ne söylediğinden ziyade zincirde gerçekten ne olduğuna bakmak çok daha sağlıklı.

Bunların dışında teknolojiye de mutlaka göz atıyorum. Fakat burada derin bir mühendislik incelemesi yapmıyorum. Daha çok birkaç temel noktayı anlamaya çalışıyorum.

Kod açık kaynak mı? Ekip projeyi geliştirmeye devam ediyor mu? **GitHub**[25] gibi platformlarda gerçekten bir hareketlilik var mı, yoksa proje aylardır sessiz mi? Hangi blockchain üzerinde çalışıyor? Köklü bir ağın güvenliğinden mi faydalanıyor yoksa kendi zincirini mi kurmuş? Bunların her birinin kendi avantajları ve riskleri var.

---

[25] **GitHub:** Geliştiricilerin kodlarını herkese açık veya özel olarak yayınlayıp güncelledikleri küresel bir sistemdir.

Bir de **“Aynı problemi çözmeye çalışan başka projeler varken bu proje neden var?”** Sorusu da bence çok kritik.

Çünkü aynı şeyi yapan onlarca proje varsa aralarından birini diğerlerinden ayıran somut bir şey olması gerekiyor. Bu bazen teknolojidir, bazen maliyet avantajıdır, bazen kullanıcı deneyimidir. Bazen de sadece çok daha güçlü bir ekosistemin parçası olmaktır.

Buradan da ekip konusuna geliyoruz.

Benim için burada en önemli kelime **şeffaflık**.

Kurucular kim? Geçmişte ne yapmışlar? Daha önce bir proje kurmuşlar mı? Kimlikleri belli mi?

Anonim bir ekip görmek tek başına benim için kırmızı bayrak değil. Kripto dünyasında anonim başlayıp zamanla kendini kanıtlamış projeler var. Fakat anonimlik ile şeffaflığın aynı şey olmadığını da unutmamak gerekiyor. Bir ekibin kimliğini gizlemesi başka, yaptığı iş konusunda hiçbir şekilde hesap vermemesi başka.

Şeffaflığın olmadığı yerde hesap verebilirlik de giderek zorlaşıyor.

Benzer nedenlerle erken yatırımcılara da bakıyorum. Projenin yanında gerçekten sektörde tanınan insanlar var mı yoksa sadece web sitesinde güzel görünmesi için isimler mi sıralanmış? Erken yatırımcılar kim? Ciddi fonların projeye erken aşamada dahil olması elbette başarı garantisi değil ama en azından belirli bir inceleme sürecinden geçilmiş olabileceğine dair bir işaret olabiliyor.

Sonra projenin büyümesine bakıyorum.

Aktif kullanıcı sayısı zaman içinde nasıl değişmiş? Protokolde kilitli değer artıyor mu? İşlem hacmi yükseliyor mu?

Burada benim için **rakamın** kendisinden çok **yönü** önemli.

Aylık, çeyreklik ve yıllık değişim bize tek bir anlık görüntüden çok daha fazla şey anlatıyor. Fakat değişimin neden gerçekleştiğini de anlamak gerekiyor. Kullanıcılar gerçekten geldikleri için mi sayı artıyor, yoksa geçici bir teşvik kampanyası mı insanları kısa süreliğine platforma çekiyor?

Tüm bunların yanında sosyal medya takipçi sayılarına neredeyse hiç güvenmiyorum. Kripto piyasasında şişirilmiş takipçi sayıları ve satın alınmış

etkileşim pek de şaşırılmaması gereken bir durum. Asıl mesele o rakamların arkasında gerçekten insanların olup olmadığı.

Rekabeti de değerlendirmenin bir parçası olarak görüyorum.

Bu projenin karşısında kimler var? Pazarın neresinde duruyor? Payı büyüyor mu, küçülüyor mu? Ve en önemlisi, neden?

Bütün bunların sonunda ise biraz daha tatsız sorulara geliyoruz. **Neler ters gidebilir?**

Proje tek bir merkezi bileşene gereğinden fazla bağımlı olabilir. Kullandığı blockchain veya başka bir altyapı beklenmedik bir sorun yaşayabilir. Regülasyonlar projenin faaliyet gösterdiği bölgede işleri değiştirebilir.

Bunların yanında yol haritasına da bakıyorum.

Önümüzdeki hedefler gerçekten ulaşılabilir mi? Ekip daha önce verdiği sözleri tutmuş mu? Yoksa sürekli ertelenen, her birkaç ayda bir yeniden yazılan bir hedef listesi mi var?

Bütün bunların arasında topluluğu gözlemlemeyi de ihmal etmiyorum. Gerçek bir topluluk var mı? İnsanlar projeyi gerçekten kullanıyor ve hakkında konuşuyor

mu? Yoksa gördüğümüz etkileşimin önemli bir kısmı botlardan mı oluşuyor?

İyi bir topluluk bazen projenin resmi kanallarından daha fazla şey anlatabiliyor. Herkesin sadece projeyi övdüğü bir ortam bana güven vermiyor. İnsanların sorunları tartışabildiği, ekibi eleştirebildiği ve gerektiğinde kötü giden şeyleri açıkça konuşabildiği bir topluluk çok daha değerli.

Bütün bunlar kulağa oldukça fazla kriter gibi gelebilir :)

Fakat zamanla hepsini tek tek kontrol etmekten ziyade projenin genel resmini görmeye başladığınızı fark ediyorsunuz. Temel amaç ise projenin gerçekten anlamlı bir hikâyesi olup olmadığını anlayabilmek.

Burada yaptığımız şey aslında bir melek yatırımcının erken aşamadaki bir girişime bakarken yaptığından çok farklı değil. O da tek bir sinyale güvenmiyor. Ekibe bakıyor, çözülen probleme bakıyor, gelir potansiyelini ve pazarın büyüklüğünü anlamaya çalışıyor, rakipleri inceliyor. Sonra bütün bu parçaları bir araya getirip bir karar veriyor.

Kripto projelerine bakarken de benzer bir düşünce biçimi var diyebiliriz. Tek bir rakama, tek bir habere

veya tek bir güzel hikâyeye kapılmadan biraz geri çekilip resmin tamamını görebilmek.

Günün sonunda sorulması gereken ise **“Bu token yükselecek mi?”** değil, **“Burada gerçekten değer üreten bir şey var mı?”** sorusu.

Sırada Ne Var?

Bu bölümde bir projeyi nasıl değerlendireceğinizi ve piyasada nasıl davranmanız gerektiğini gördük.

Diyelim ki tüm bu adımları tamamladınız ve bir varlığa yatırım yapmaya karar verdiniz. Şimdi çok daha pratik bir soru geliyor, bu varlığı nerede ve nasıl güvenli biçimde saklayacaksınız? Bir sonraki bölümde cüzdanlara ve güvenliğe geçiyoruz.

Bölüm 6: Cüzdanlar ve Güvenlik

Geleneksel bankacılıkta herhangi bir sorun yaşadığınızda müşteri hizmetlerini arayabilirsiniz. Şifrenizi mi unuttunuz, kartınız mı çalındı, hesabınıza yetkisiz bir işlem mi yapıldı? Bankanız sizi bu gibi durumlardan büyük ölçüde kurtarıyor.

Kripto para dünyasında ise bu sorumluluk **%100** sizde. Özel anahtarınızı kaybettiğinizde ya da biri onu ele geçirdiğinde arayabileceğiniz hiçbir kurum, itiraz edebileceğiniz hiçbir merci bulunmuyor.

Kripto camiasında sık duyacağınız bir söz var:

> ***"Not your keys, not your coins."***[26]
> **— Andreas M. Antonopoulos**

---

[26] **"Not your keys, not your coins" (Anahtarlar senin değilse, coinler de senin değildir)** sözü kripto varlıkların gerçek kontrolünün, varlıkları hareket ettirmeye yarayan özel anahtarların kontrolüne bağlı olduğunu anlatır. Bir varlığın borsada veya başka bir platformda tutulması kişinin o varlık üzerindeki erişim yetkisini üçüncü bir tarafa bırakması anlamına gelir. İfade sıklıkla **Andreas M. Antonopoulos**'a atfedilse de ilk kullanımının ona ait olduğu kesin olarak belgelenmiş değildir.

Bu bölümde anlatacağımız her şey aslında bu alıntının etrafında şekilleniyor.

Diğer alt başlığa geçmeden önce hikâye zamanı yapalım :)

Analiz şirketlerinin tahminlerine göre bugüne kadar üretilmiş Bitcoin'lerin yaklaşık %20'si sonsuza dek erişilemez durumda.

Bunun en ünlü örneklerinden biri ise İngiliz mühendis James Howells'in hikâyesi. Bu abimiz içinde 8.000 Bitcoin'in özel anahtarlarının bulunduğu bir sabit diski farkında bile olmadan çöpe atmış ve bu disk bir çöplüğe gömülmüş. Yıllardır belediyeyle çöplüğü kazma izni almak için mahkemelik durumda.

Bir başka örnek ise erken dönem Bitcoin geliştiricilerinden Stefan Thomas'tan geliyor. Kendisi 7.000 Bitcoin'e erişimini sağlayan şifreli bir sabit diskin şifresini unutuyor. Şu anda elinde sadece on deneme hakkı olan bir cihaz var ve şu ana kadar sekiz denemeyi harcamış durumda.

Bu hikâyeleri neden anlattım? **Çünkü bu konu ihmal edildiğinde bunun gibi olaylar herkesin başına gelebiliyor.**

Borsada Varlık Tutmak

Bir kripto borsasına para yatırdığınızda aslında oldukça tanıdık bir şey yapıyorsunuz, paranızı bir üçüncü tarafa emanet ediyorsunuz! Borsa sizin adınıza varlıklarınızın **özel anahtarını**[27] tutuyor. Siz de sadece arayüz üzerinden **temsili bir bakiyeye** bakıyorsunuz.

Dürüst olmak gerekirse bu çok rahat bir deneyim. Eğer şifrenizi unutursanız hesabınızı geri alabiliyorsunuz. Ayrıca alım satım işlemleri de oldukça hızlı ve çok kolay.

Ama bu rahatlığın bir trade-off'u var.

2014 yılında dönemin en büyük Bitcoin borsası olan **Mt. Gox**, bugünkü kur ile ile yaklaşık 55 milyar dolar değerinde 850.000 Bitcoin'in çalındığını açıkladı. Bu miktar o dönem dolaşımdaki tüm Bitcoin'in yaklaşık %7'sine denk geliyordu. Kullanıcılar yıllarca paralarının ufak bir kısmını bile geri alamadı.

Daha yakın bir örnek olarak 2022 sonunda çöken **FTX** borsası var. FTX, dönemin en büyük ve en

---

[27] **Özel Anahtar (Private Key):** Bir kripto cüzdanının gerçek sahibini kanıtlayan ve içindeki varlıklar üzerinde işlem yapma yetkisi veren gizli şifredir. Özel anahtara sahip olan kişi cüzdandaki kripto varlıkları kontrol edebilir. Bu nedenle özel anahtarın kimseyle paylaşılmaması ve güvenli şekilde saklanması gerekir.

güvenilir borsalarından biri olarak kabul ediliyordu. Kurucusu Sam Bankman-Fried dergi kapaklarına çıkıyor, ünlü isimlerle reklam çekiyordu. Ama perde arkasında kullanıcıların borsaya emanet ettiği paralar FTX'in bağlantılı olduğu bir yatırım şirketi tarafından riskli pozisyonlarda kullanılıyordu. Güven bir anda buharlaşınca milyonlarca kullanıcı paralarına erişemez hale geldi.

Bu hikâyeler borsaların hiç kullanılmaması gerektiği anlamına gelmiyor.

Bir varlığı aktif olarak alıp satmak istiyorsanız bir borsada tutmak oldukça pratik. Ama uzun vadede tutmayı planladığınız ve uzun süre dokunmayacağınız bir varlığı da borsada bekletmek gereksiz bir risk almak demek.

Bir varlığı ne kadar süre elinizde tutacaksanız ve varlık ne kadar büyük bir miktarsa, merkezi bir borsaya o kadar az güvenmeniz ve o kadar çok kendi kontrolünüze almanız gerekli.

Bir borsayı seçerken de düzenleyici kayıtlarının olup olmadığına, rezerv kanıtı yayınlayıp yayınlamadığına ve geçmişinde ciddi bir güvenlik ihlali yaşayıp

yaşamadığına bakmak sadece işlem ücretlerine bakmaktan çok daha değerli.

Peki varlıklarımızın kontrolünü nasıl kazanacağız? **Sıcak** ve **soğuk cüzdanlar** ile.

Sıcak Cüzdanlar

İlk durağımız sıcak cüzdanlar. **Sıcak cüzdan internete bağlı herhangi bir cihazda çalışan cüzdan demek.** Bir telefon uygulaması, bir tarayıcı eklentisi ya da bir masaüstü programı olabilir.

Sıcak cüzdanın başlıca avantajı ücretsiz olması, kurulumlarının yalnızca birkaç dakika sürmesi, hem cüzdanın kendisine hem de DeFi uygulamalarına anında erişim sağlanabilmesi, ve tabii en önemlisi, özel anahtarlar tamamen sizin kontrolünüzde olması.

Ama uzun vadeli ve büyük miktarda varlık saklamak için sıcak cüzdanlar çok da ideal değil. Bunun sebebi cüzdanın kendisinin internete bağlı bir cihazda çalışması.

Burada önemli bir noktayı netleştirmek istiyorum. Bu cüzdanlar aslında **güvenli.** Yeter ki cüzdanın bulunduğu cihazı iyi koruyabiliyor olun.

Yani risk cüzdanın kendisinde değil, çoğunlukla yüklü olduğu cihazın güvenliğinde saklı.

Peki kripto özelinde cihaz ve cüzdan güvenliği nasıl sağlanır?

1. Öncelikle cüzdan eklentisinin bulunduğu tarayıcıda başka gereksiz eklentiler bulundurmayın. Hatta mümkünse cüzdanınız için ayrı, kişisel kullanımınız için ayrı bir tarayıcı tercih edin.
2. Korsan yazılımlardan ve crackli programlardan uzak durun. Bu tür dosyalar kötü amaçlı yazılım bulaştırmanın en yaygın yollarından biri.
3. Cüzdan uygulamasını her zaman resmi kaynaklardan indirin ve her zaman için bağlantıları iki kez kontrol edin. (Örneğin apple.com ve apple.com domainleri bire bir aynı gözükse de ikinci domain sizi asla Apple'ın sitesine götürmeyecektir. Bunun nedeni birinci domainde normal "a" kullanılırken ikinci domainde cyrillic "a" kullanılması. Bunun gibi sahtecilik yöntemleri kripto sektöründe oldukça fazla.)

4. **Anahtarlarınızı (seed phrase)**[28] asla kaybetmeyin ve asla dijital ortamda saklamayın. Ekran görüntüsü almayın veya notlar uygulamasına yazmayın. Bu kural **sıcak cüzdanlar** için de, birazdan konuşacağımız **donanım cüzdanlar** için de geçerli.

Donanım Cüzdanlar

Şimdi soğuk cüzdanlara, yani donanım cüzdanlarına geçelim. Donanım cüzdanlar doğru kullanıldığında ve birkaç basit adım tamamlandığında varlıklarınız için inanılmaz derecede güvenli bir saklama aracına dönüşüyor.

Peki donanım cüzdanının arka planında neler oluyor?

İyi bir donanım cüzdanın kalbinde **secure element chip** dediğimiz özel bir çip bulunuyor. Aslında bu çip pasaportlarda ve banka kartlarında da kullanılan çipe benzer bir mantıkla çalışıyor.

---

[28] **Seed Phrase (Kurtarma İfadesi):** Bir kripto cüzdanını kaybetmeniz durumunda yeniden erişmenizi sağlayan 12 veya 24 kelimeden oluşan kurtarma anahtarıdır. Bu kelimelere sahip olan herkes cüzdanı geri yükleyebilir. Bu nedenle çevrim dışı ve güvenli bir yerde saklanması büyük önem taşır.

Özel anahtarı cihazın geri kalanından tamamen izole bir alanda tutuyor ve bu izole alana dışarıdan doğrudan erişim mümkün olmuyor.

Cihazınızı ilk kurduğunuzda da seed phrase'inizi üretmek için **TRNG** dediğimiz **gerçek rastgele sayı üreticisi** kullanılıyor. Bu sayede üretilen kelimelerin bir başkası tarafından tahmin edilmesi ya da aynı kelimelerin tekrar üretilmesi neredeyse imkansız hale geliyor.

Bir işlem yapmak istediğinizde ise süreç şöyle işliyor.

İşlemi telefondaki yazılım üzerinden başlatıyoruz. Ama işlem telefonun içinde gerçekleşmiyor. Kullandığımız telefon bu isteği donanım cihazına iletiyor. İmzalama işlemi ise tamamen cihazın içinde ve izole bir şekilde yapılıyor. Bu noktada sazan gibi atlayıp donanım cüzdan üzerinden işlemi hemen onaylamıyoruz. İşlemi telefon ekranından değil, doğrudan cüzdan cihazının kendi küçük ekranından kontrol ediyoruz. Çünkü telefonumuza veya bilgisayarımıza bulaşmış bir kötü amaçlı yazılım bize ekranda doğru bir adresi, cihazda farklı bir adresi gösteriyor olabiliyor. Dolayısıyla **cihazın kendi ekranı** bu tür işlemlerde **son kontrol noktamız.**

Donanım Cüzdanlar Hakkında Doğru Bilinen Yanlışlar

Bu konuda birkaç önemli yanlış anlaşılmayı netleştirelim.

1. Kripto varlıklarınız cihazın içinde saklanmıyor. Varlıklar daima blockchain üzerinde duruyor, cihaz sadece anahtarları tutuyor. Bu yüzden cihazınız yansa, düşse, suya girse bile sorun değil. Elinizde seed phrase'iniz olduğu sürece bu kelimeleri başka bir uyumlu cihaza aktarıp fonlarınıza yeniden erişebiliyorsunuz.
2. Cihazı üreten şirket batsa bile fonlarınız kaybolmuyor. Bunun nedeni seed phrase standardının spesifik bir şirkete özel olmaması.
3. Bilgisayarınız hacklense bile donanım cüzdanınıza bir şey olmuyor. Bunun nedeni özel anahtarın hiçbir zaman bilgisayara geçmemesi. Bilgisayara sadece imzalanmış işlem geçiyor.

Donanım Cüzdan Firması Nasıl Seçilir?

Firma seçerken birkaç somut kritere kesinlikle bakmak lazım.

1. Öncelikle hem yazılımın hem donanımın açık kaynak kodlu olmasını tercih edin. Bu sayede bağımsız güvenlik araştırmacıları kodu inceleyerek açıkları bulabilir ve bir sonraki güncellemelerle söz konusu zafiyet giderilebilir.
2. Sektörde uzun süredir var olan ve en çok bilinen beş altı firmadan birini tercih etmek makul bir başlangıç noktası. Yine de şunu açıkça söylemem gerekiyor ki **sadece popüler olmak tek başına bir güvenlik garantisi değil.** FTX de **çöktüğü güne kadar sektörün en popüler ve en güvenilir görünen isimlerinden biriydi.** Bilinen büyük donanım cüzdan firmalarından biri olan Ledger çok büyük oranda **kapalı kaynak kodlu** çalışıyor. Bunu bilerek seçim yapmanızda fayda var.
3. Cihazı satın alırken sadece üreticinin kendi resmi sitesinden ya da yine üreticinin kendi sitesinde yayınladığı resmi distribütör listesinden alışveriş yapın. İkinci el bir cihaz

almayın. Kutusu açılmış, önceden müdahale edilmiş ya da içine zararlı bir bileşen yerleştirilmiş bir cihazı fark etmeniz neredeyse imkansız.

"Bu kitabın sponsoru olan XYZ cüzdanını, XYZ kodu ile %10 indirimle alabilirsiniz!" demek oldukça kolay olurdu. Ama bunu yapmıyorum ve ***"şunu alın"*** demiyorum.

Burada amacım ürün satmaktan ziyade küçük bir kıvılcım oluşturup kendi araştırmanızı yapmanızın önünü açmak.

Bugün elimizde inanılmaz güçlü bir araç var. Yapay zeka. Az önce anlattığım kriterleri (açık kaynak kod, sektördeki köklülük, güvenlik geçmişi) alıp herhangi bir yapay zeka aracına sorabilir ve güncel karşılaştırmaları saniyeler içinde görebilirsiniz.

Bu kitabı okuduğunuzda piyasa çoktan değişmiş olabilir. Ama size doğru soruları sormayı öğretebilirsem bu kitabı hangi yıl okursanız okuyun kendi doğru cevabınızı bulabilirsiniz.

Seed Phrase'inizi Nerede Saklamalısınız?

Cüzdanınızı ilk kurduğunuzda size genellikle on iki ya da yirmi dört kelimelik bir seed phrase gösteriliyor. **Bu kelimeler tüm varlığınıza yeniden erişmenin anahtarı. Bu kelimeleri asla dijital ortamda saklamayın. Fotoğrafını çekmeyin, ekran görüntüsü almayın, notlar uygulamasına yazmayın, bir bulut hizmetine yüklemeyin, kendinize mail atmayın.** Dijital olan her şey bir noktada internete temas etme riski taşıyor.

Seed phrase'leri kâğıda yazmak bir başlangıç noktası olabilir. Yine de kâğıt yanabilir, suyla temas edince okunmaz hale gelebilir ve zamanla solabilir.

Ciddi miktarlar için yanmaz ve suya dayanıklı metal yedekleme çözümleri çok daha güvenli bir seçenek. Bu plakalar kelimeleri metale kazıyarak saklıyor ve bir ev yangınında bile okunabilir kalabiliyor.

Passphrase Kullanmak

Ekstra bir güvenlik katmanı isteyenler için passphrase seçeneği var (buna bazen yirmi beşinci

kelime de deniyor). Passphrase, 12 veya 24 kelimelik seed phrase'inizin üzerine kendi belirlediğiniz bir kelime ya da cümle eklemeniz anlamına geliyor. Biri aynı seed phrase'e sahip olsa bile belirlediğiniz ek kelimeyi bilmeyen biri gerçek cüzdanınıza asla ulaşamıyor.

Bunu neden bu kadar güçlü buluyorum? Çünkü farklı bir passphrase girdiğinizde tamamen farklı, hatta boş görünen bir cüzdana ulaşıyorsunuz. Biri seed phrase'inizin fiziksel yedeğinizi ele geçirse bile passphrase'inizi bilmediği sürece seed phrase tek başına işe yaramıyor.

Kısacası seed phrase'iniz çalınsa bile fonlarınız halen güvende kalabiliyor. Bu da onu eklemeye değer kılan asıl sebep.

Dolandırıcılık ve Red Flag'ler

Bu alanda kişisel olarak biriktirdiğim tonlarca tecrübe var çünkü zamanla pek çok dolandırıcılık girişimiyle karşılaştım.

İyi haber, dolandırıcılar sandığınız kadar yaratıcı değil. İsimler ve projeler değişiyor ama kullanılan kalıp genelde aynı kalıyor.

En sık karşılaştığım kalıp rug pull. Bir proje güzel bir görsel kimlikle, aktif bir sosyal medya hesabıyla ve bazen ünlü isimlerin desteğiyle ortaya çıkıyor. Topluluk büyüyor, fiyat yükseliyor, sonra bir gün proje sahipleri likiditeyi çekip ortadan kayboluyor. Elinizde kalan şey ise değeri sıfıra inmiş bir token oluyor.

Bir başka kalıp sabırlı dolandırıcılık dediğim tür. Genelde sosyal medyada ya da mesajlaşma uygulamalarında başlıyor. Karşınızdaki kişi haftalarca sizinle sohbet ediyor, güven inşa ediyor, hatta bazen hiç para konusunu açmıyor. Güven oturduktan sonra "***harika bir fırsat***" ortaya çıkıyor, genelde de bilmediğiniz bir platforma yatırım yapmanız isteniyor. Buradaki asıl silah zaman. Çünkü kimse haftalarca konuştuğu birinden şüphelenmiyor.

Üçüncü kalıp kimlik taklidi. Tanınmış bir borsa, ünlü bir isim ya da resmi bir proje hesabı taklit ediliyor. Genelde bir ödül, bir destek talebi ya da bir "özel fırsat" bahanesiyle sizi platformdan uzaklaştırıp özel bir mesajlaşma kanalına yönlendiriyorlar. Gerçek bir kurum ya da proje sizi asla platform dışına çekip özelden iş yapmaya çalışmıyor.

Son olarak sahte airdrop ve hediye kampanyaları var. "Cüzdanınızı bağlayın, ücretsiz token kazanın" mesajı kulağa çekici geliyor ama genelde bu bağlantı cüzdanınızdaki varlıklara erişim izni istiyor. Bir teklif ne kadar kolay ve bedavaymış gibi görünüyorsa o kadar dikkatli yaklaşmanız gerekiyor.

Tüm bu kalıpların ortak bir noktası var. Hepsi aciliyet ve heyecan üzerine kuruluyor. Gerçek fırsatlar nadiren "hemen şimdi karar ver yoksa kaçırırsın" baskısıyla geliyor.

Bir teklif sizin düşünmenizi bile istemeden sizi hızlıca harekete geçirmeye çalışıyorsa harika bir kırmızı bayraktır.

Sırada Ne Var?

Bu bölümde varlığınızı nasıl koruyacağınızı, elinizdeki farklı yöntemlerin gerçek artılarını ve eksilerini gördük. Şimdi elinizde kripto paraların ne olduğuna, nasıl çalıştığına ve nasıl güvenle saklanacağına dair eksiksiz bir resim var. Peki bütün bu teknoloji nereden çıktı? Bir sonraki bölümde biraz geriye gidip bu hikâyenin nasıl başladığına bakıyoruz.

Bölüm 7: Kripto Paralarda Kilometre Taşları

Bu kitap boyunca kripto paraların ne olduğunu, nasıl çalıştığını ve nasıl kullanılacağını anlattık. Şimdi sırada bu hikâyenin zaman çizgisi var. Çöküşler, mucizeler, gizemli kurucular ve bir pizza siparişinin efsaneye dönüştüğü bir hikâye. Hazırlanın, çünkü sıfır noktasından bugüne geliyoruz.

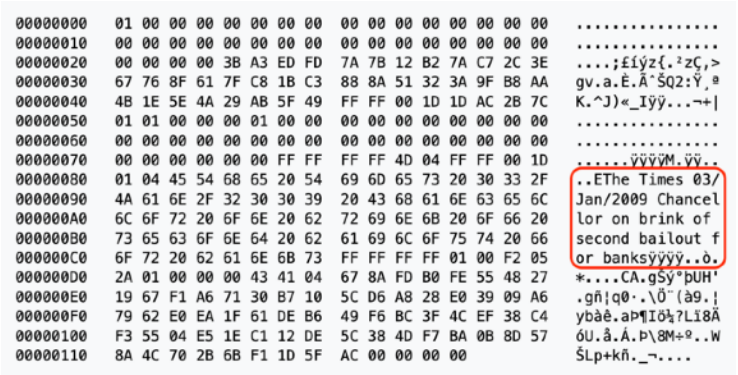
Fitil Ateşleniyor (2008)

Bölüm 1'de anlattığımız 2008 finansal krizini hatırlıyor musunuz? İşte tam o kaosun ortasında (31 Ekim 2008) kimliği hâlâ bilinmeyen bir kişi ya da grup **Satoshi Nakamoto** takma adıyla dokuz sayfalık bir belge yayınladı. Bu belge bir kriptografi e-posta listesine gönderilmişti ve sade bir teknik doküman gibi görünüyordu ama içinde bankasız ve aracısız bir para sistemi önerisi vardı. Belgenin adı ise "Bitcoin, A Peer-to-Peer Electronic Cash System" idi.

Satoshi Nakamoto'nun gerçekte kim olduğunu hâlâ bilmiyoruz. Tek kişi mi, bir ekip mi, hangi ülkeden, hiçbiri net değil. 2010 yılı civarında ortadan kayboldu ve bir daha hiç ortaya çıkmadı. Analistlerin tahminine göre erken dönemde kazdığı yaklaşık bir milyon Bitcoin bugünkü değeri ile onlarca milyar dolar ve hiç dokunulmamış cüzdanlarda duruyor. Yani dünyanın en zengin insanlarından biri olabilecek biri muhtemelen kimliğini hiç açıklamadan ortadan kayboldu. Dolayısıyla kripto dünyasının en büyük gizemi daha çözülmüş değil :)

Genesis (Ocak 2009)

3 Ocak 2009'da Satoshi, Bitcoin ağının ilk bloğunu, yani genesis block'u kendi bilgisayarında kazdı. Ama bu blok sıradan bir başlangıç değildi. İçine küçük ama anlamlı bir mesaj gizlemişti. İngiliz The Times gazetesinin o günkü manşetinden alınma bir cümle. Bankaların ikinci kez kurtarılmanın eşiğinde olduğuna dair. Bu tabii ki tesadüf değildi. Satoshi'nin bu teknolojiyi neden yarattığına dair bıraktığı bir imzaydı.



Bitcoin Genesis Block'un ham verisi. Kaynak: Bitcoin Core / Genesis Block

Bu mesaj artık blockchain'in bir parçası. Yani sonsuza dek orada duracak ve kimse silemeyecek.

Bunu kripto paranın doğum belgesine kazınmış bir protesto notu olarak görebiliriz. O günlerde Bitcoin'in hiçbir parasal değeri yoktu ve kimse alıp satmıyordu.

---

[29] "**Chancellor on brink of second bailout for banks":** Bitcoin'in ilk bloğuna (Genesis Block) yerleştirilen ve **3 Ocak 2009** tarihli *The Times* gazetesinin manşetinden alınan bu ifade Türkçeye "**Maliye Bakanı, bankalar için ikinci kurtarma paketinin eşiğinde**" şeklinde çevrilebilir. Manşet, 2008 küresel finans krizinin ardından hükümetlerin zor durumdaki bankaları kamu kaynaklarıyla kurtarmasını konu alıyordu. Satoshi Nakamoto'nun bu metni ilk bloğa eklemesi bir yandan Bitcoin'in oluşturulduğu tarihi kanıtlarken diğer yandan geleneksel finans sistemine ve devlet destekli banka kurtarmalarına yönelik eleştirel bir mesaj olarak yorumlanır. Bu nedenle söz konusu manşet Bitcoin'in ortaya çıkış felsefesini simgeleyen en önemli ifadelerden biri kabul edilir.

Sadece birkaç meraklı kriptografi hevesçisi bu garip yeni ağı test ediyordu.

İlk Değer Kanıtı (2010)

Bitcoin'in gerçek bir değeri olduğunu kanıtlayan ilk an beklediğinizden çok daha sıradan bir şekilde geldi. 22 Mayıs 2010'da Laszlo Hanyecz adlı bir programcı forumda bir ilan verdi ve on bin Bitcoin karşılığında kendisine iki pizza ısmarlanmasını istedi. Birileri kabul etti, pizzalar geldi, işlem tamamlandı. Bu tarih bugün kripto camiasında Bitcoin Pizza Day olarak her yıl kutlanıyor ve gayet haklı bir sebebi var… O on bin Bitcoin bugünün fiyatlarıyla yüzlerce milyon dolar değerinde. Muhtemelen tarihin en pahalı pizzası.

Aynı yıl bir başka önemli gelişme daha oldu. İlk borsalardan biri olan Mt. Gox kuruldu. Adı da oldukça tuhaf bir hikâyeye sahip. Mt. Gox aslında başlangıçta "Magic the Gathering Online Exchange" kısaltmasıydı. Yani kart oyunu kartlarının takas edildiği bir site olarak kurulmuştu. Sonradan Bitcoin borsasına dönüştürüldü. Birkaç yıl sonra bu ismi tekrar duyacağız, ama bu sefer çok daha kötü bir bağlamda :(

Silk Road ve İlk Patlama (2011-2013)

Şubat 2011'de Bitcoin ilk kez bir doları ($1) gördü. Artık bir Bitcoin bir Amerikan doları değerinde işlem gördü. O yıl aynı zamanda Silk Road adlı bir karanlık ağ pazar yeri açıldı ve ödeme yöntemi olarak Bitcoin'i kullandı. Bu olay hem kripto paraya olan ilgiyi artırdı hem de uzun yıllar boyunca Bitcoin'in imajına gölge düşürdü. **Kripto paranın kötüye kullanılabilir olması ile kötü bir teknoloji olup olmaması arasındaki fark o dönemde pek çok insan tarafından karıştırıldı.** (Nedense aklıma bir anda uranyum teknolojileri geldi :)

2013'e gelindiğinde ilginç bir tetikleyici daha ortaya çıktı. Kıbrıs'ta yaşanan bir bankacılık krizi. Kıbrıslı mevduat sahipleri bankalarının hesaplarına el koyabileceğini görünce bankaya duyulan güvenin ne kadar kırılgan olabileceğini acı bir şekilde öğrendi. Tam da Bölüm 1'de anlattığımız o güven sorununun somut bir örneği. Bu olay Bitcoin'i bankacılık sistemine alternatif olarak görenlerin sayısını artırdı ve yıl sonunda Bitcoin ilk kez 1000 doları geçti. Yıl başında 13 dolar civarında olan bir varlığın yıl sonunda 1200

dolara çıkması o dönem bile akıl almaz bir hikâye olarak anlatılıyordu.

Mt. Gox Çöküşü (2014)

Az önce bahsettiğimiz Mt. Gox'u hatırlıyor musunuz? 2014'e gelindiğinde bu borsa dünyadaki tüm Bitcoin işlemlerinin yaklaşık %70'ini elinde tutan devasa bir oyuncuydu. Şubat 2014'te ise bomba gibi bir haber düştü. Borsa 850.000 Bitcoin'in çalındığını açıkladı. Bu miktar o günün kuruyla yaklaşık 450 milyon dolara denk geliyordu. Anlaşılan o ki hırsızlık bir anda değil yıllar içinde sessizce gerçekleşmiş ve fark edilmemişti.

Bu olay kripto camiasında derin bir travma yarattı ve bugün halen tekrarlanan (ama nedense çoğu kişinin umursamadığı) bir cümlenin doğmasına sebep oldu. Not your keys, not your coins. Bu cümleyi Bölüm 6'dan hatırlıyorsunuzdur. İşte kökeni tam olarak burası. Mt. Gox'un kullanıcıları yıllar süren hukuki süreçlerin ardından kayıplarının ancak bir kısmını geri alabildi.

Ethereum'un Doğuşu (2015)

Şimdi hikâyenin en yaratıcı karakterlerinden birine geliyoruz. Vitalik Buterin. Rus asıllı Kanadalı bir programcı olan Buterin 19 yaşındayken (2013) Ethereum'un whitepaper'ını yazdı. Fikri basitti ama devrimciydi. Bitcoin sadece para transferi yapabiliyorken Ethereum üzerinde herhangi bir programı ,yani akıllı kontratı, çalıştırabilirsiniz. Ethereum kripto dünyasını bir ödeme sisteminden üzerine sonsuz sayıda uygulama inşa edilebilecek bir platforma dönüştürdü.

İlginç bilgi, Buterin'in bu fikirdeki ilham kaynaklarından biri oynadığı bir online oyunda geliştiricilerin kendi karakterinin bir yeteneğini tek taraflı olarak kaldırmasıymış. O an merkezi bir otoritenin dijital bir dünyada dilediği zaman kuralları değiştirebilmesinin ne kadar rahatsız edici olduğunu fark etmiş. Temmuz 2015'te Ethereum ana ağı canlıya alındı ve bugün ikinci en büyük kripto para ağı olarak yoluna devam ediyor.

DAO Hack'i ve Hard Fork (2016)

Ethereum'un ilk büyük sınavı çok geçmeden geldi. 2016'da "The DAO" adında Ethereum üzerinde çalışan ve topluluk oylamasıyla yatırım kararları alan devasa bir merkeziyetsiz fon kuruldu. O dönemin parasıyla 150 milyon doları aşkın bir değer topladı. Ama akıllı kontratın kodunda bir açık vardı. Buna yeniden giriş açığı, yani reentrancy, diyoruz ve bir saldırgan bu açığı kullanarak fonun yaklaşık üçte birini kendi cüzdanına aktardı.

Ethereum topluluğu burada zor bir karar vermek zorunda kaldı. Blockchain'in "***değiştirilemezlik***" ilkesine sadık kalıp çalıntı fonu kabul mü etsinler, yoksa ağı geriye sarıp bu işlemi iptal mi etsinler? Topluluk ikiye bölündü. Bir grup ağı geri sardı ve bugünkü Ethereum'u oluşturdu. Bir grup ise orijinal zincirde ısrar etti ve bu da **Ethereum Classic** adıyla ayrı bir ağ olarak hayatına devam etti.

ICO Çılgınlığı (2017)

2017 kripto dünyasının ilk gerçek çılgınlık yılıydı. ICO, yani ilk coin arzı (Initial Coin Offering), yeni

projelerin token satarak fon toplamasına verilen isim. Bu yıl içinde bazı projeler dakikalar içinde milyonlarca dolar topladı, bazıları ise sadece birkaç sayfalık bir whitepaper ve iddialı bir logo ile yatırımcıları ikna etmeyi başardı. Sonradan yapılan analizlerde o dönemki ICO projelerinin büyük bir kısmının birkaç yıl içinde tamamen değersizleştiği ya da ortadan kaybolduğu ortaya çıktı.

Bu çılgınlığın rüzgârıyla Bitcoin de tarihinde ilk kez 20.000 doları gördü, Aralık ayında ise zirveye ulaştı. Sokaktaki sıradan insanlar bile artık kripto paradan bahsediyordu. Taksi şoförleri hangi coini alacaklarını soruyordu. İnsanlar ise bu tür bir coşkunun genelde bir kırılmanın habercisi olduğunu birkaç ay sonra acı bir şekilde öğrenecekti.

Kripto Kışı (2018-2019)

2018 başladığında parti bitmişti. Bitcoin bir yıl içinde zirvesinden yaklaşık %80 değer kaybetti, ICO ile fon toplayan pek çok proje sessizce ortadan kayboldu. Medya bu döneme "***kripto kışı***" adını taktı ve gazeteler neredeyse her ay ***Bitcoin'in artık öldüğünü ilan eden yazılar yayınladı.***

Eğlenceli gerçek, kripto takipçilerinin tuttuğu gayri resmi bir listeye göre Bitcoin'in medyada "***öldüğü ilan edilme***" sayısı bugüne kadar 475'i geçmiş durumda[30]. Üstelik her seferinde (nasılsa) bir şekilde geri dönmeyi başardı.

Ama fiyatların çökmesi teknolojinin durduğu anlamına gelmiyordu. Bu sessiz dönemde pek çok geliştirici hiçbir şey olmamış gibi çalışmaya devam etti, altyapıyı güçlendirdi ve hataları düzeltti.

Kripto camiasında yine sık duyabileceğiniz bir söz var, en iyi projeler genelde kimsenin bakmadığı ayı piyasalarında inşa edilir. 2018-2019 tam olarak bu dönemdi.

DeFi Summer (2020)

2020 yazında sessizce inşa edilen o altyapı aniden patladı. Compound adlı bir borç verme protokolü kullanıcılarına kendi yönetim tokenini dağıtmaya başladı ve bu da kripto camiasında "***yield farming***"

---

[30] Bitcoin'in kuruluşundan bu yana ana akım medyada çıkan tüm "ölüm ilanlarını", tarihleri ve gazete kupürleriyle birlikte derleyen gayriresmi arşiv için bkz. 99Bitcoins, "Bitcoin Obituaries", erişim adresi: 99bitcoins.com/bitcoin-obituaries/

çılgınlığını tetikledi. Kullanıcılar sadece bir protokole varlık kilitleyerek yüksek getiriler elde etmeye başladı. Para adeta protokolden protokole akmaya başladı. DeFi tarafındaki kilitli toplam değer (TVL) birkaç ay içinde 1 milyar dolardan 15 milyar doların üzerine fırladı.

Bu çılgınlığın komik ama gerçek bir yan etkisi de oldu. Ethereum ağı o kadar yoğunlaştı ki bazı işlemlerin ağ ücreti işlemin kendisinden daha pahalı hale geldi. İnsanlar birkaç dolarlık bir işlem yapmak için 50 dolar ödemek zorunda kaldı.

NFT Çılgınlığı ve Kurumsal Giriş (2021)

2021 kripto dünyasının ana akım medyaya taştığı yıl oldu. Mart ayında dijital sanatçı Beeple'ın bir NFT eseri Christie's müzayede evinde 69 milyon dolara satıldı. Bu haber dünya çapında manşetlere çıktı ve NFT kelimesini bir gecede herkesin diline yerleştirdi. Aynı yıl Tesla 1,5 milyar dolarlık Bitcoin satın aldığını açıkladı, MicroStrategy adlı şirket ise Bitcoin biriktirmeyi neredeyse kurumsal bir stratejiye dönüştürdü.

Belki de yılın en tarihi anı Eylül 2021'de El Salvador'un Bitcoin'i resmi ödeme aracı olarak kabul eden ilk ülke olmasıydı[31]. Bir devlet ilk kez bir kripto parayı doların yanına, yasal para birimi statüsüne yükseltti. Kasım ayına gelindiğinde Bitcoin 69.000 dolar civarında yeni bir zirveye ulaştı. O dönemde herkes bu yükselişin sonsuza kadar süreceğine ikna olmuş gibiydi, ki bu tür bir iyimserliğin kripto tarihinde genelde neyin habercisi olduğunu artık biliyorsunuz.

Büyük Hesaplaşma (2022)

2022 kripto tarihinin en acı derslerinin verildiği yıl oldu. Mayıs ayında Bölüm 2'de detaylı olarak anlattığımız Terra/Luna çöküşü yaşandı. Algoritmik stablecoin UST peg'ini kaybetti ve birkaç gün içinde 40 milyar doları aşkın bir değer buharlaştı. Bu çöküşün dalgaları o kadar büyüktü ki Terra ekosistemine bağlı

[31] Ülke, 2021'de Bitcoin'i resmi para birimi ilan etse de IMF ile yapılan finansal anlaşmalar kapsamında 2025 başında yasada değişikliğe gitti. İşletmeler için Bitcoin kabul etme zorunluluğu kaldırılarak kullanım tamamen gönüllü hale getirildi. Buna karşın El Salvador hazinesinde Bitcoin tutmaya ve düzenli olarak rezerv biriktirmeye devam etmektedir.

kredi veren kuruluşlar da art arda batmaya başladı. Celsius ve Voyager gibi platformlar da iflasını açıkladı.

Yıl kötü bitmedi, daha da kötü bitti. Kasım ayında Bölüm 6'da anlattığımız FTX çöküşü patlak verdi. O güne kadar sektörün en güvenilir isimlerinden biri sayılan borsa aslında müşteri fonlarını kendi bağlantılı şirketinde riske atmıştı. Güven bir gecede yıkıldı. 2022 sonunda toplam kripto piyasa değeri yıl başına göre iki trilyon dolardan fazla erimişti. Bu olay sektörün gördüğü **en büyük** ve **en acı verici** temizlenme dönemiydi.

ETF Dönemi (2023-2024)

Kriz sonrası toparlanma beklenenden daha hızlı ve daha kurumsal bir yoldan geldi. Ocak 2024'te ABD Sermaye Piyasası Kurulu yıllardır reddettiği bir başvuruyu sonunda onayladı. Spot Bitcoin ETF'leri. Bu durum sıradan bir yatırımcının kripto para cüzdanı açmadan doğrudan kendi borsa hesabı üzerinden Bitcoin'e yatırım yapabilmesi anlamına geliyordu. Dünyanın en büyük varlık yönetim şirketlerinden BlackRock'ın piyasaya sürdüğü ürün kısa sürede tarihin en hızlı büyüyen ETF'lerinden biri haline geldi.

Temmuz 2024'te benzer bir onay Ethereum için de geldi. Bu iki gelişme kripto para dünyasının artık kendi kabuğunda yaşayan bir alt kültür olmaktan çıkıp geleneksel finansın resmi bir parçası haline geldiğinin en somut kanıtıydı.

On yıl önce "internet parası" diye alay edilen bir varlık artık emeklilik fonlarının portföylerinde yer alabiliyordu.

Bugüne Doğru (2025-2026)

ETF onaylarından sonraki dönem kripto para dünyasının en hızlı düzenlendiği dönem oldu diyebiliriz.

ABD tarafında en büyük gelişme stablecoin'lerle ilgili. Temmuz 2025'te GENIUS Act yürürlüğe girdi. Bu yasa stablecoin ihraç eden şirketlerin her token karşılığında gerçek nakit ya da kısa vadeli hazine bonosu tutmasını zorunlu kılıyor. Rezerv bileşiminin düzenli olarak açıklanması ve büyük ihraççıların yıllık bağımsız denetimden geçmesi gerekiyor. Bu aslında önceki bölümlerde bahsettiğimiz Terra/Luna çöküşü gibi olayların ardından gelen doğal bir tepki.

RWA tarafında ise büyüme gerçekten çarpıcı. 2026'nın ortasına gelindiğinde tokenize edilmiş gerçek dünya varlıklarının toplam değeri 30 milyar doları aştı. Bu rakam 2025 başına göre yaklaşık beş kat büyüme demek. BlackRock'ın tokenize hazine bonosu fonu BUIDL artık tek bir ağla sınırlı değil. Sekize yakın farklı blockchain'e yayılmış durumda. Hatta bu fonun payları Uniswap gibi merkeziyetsiz borsalarda da işlem görmeye başladı. Yani kurumsal finans ürünleri artık DeFi dünyasıyla doğrudan kesişiyor. Bunun yanında gayrimenkul tokenizasyonu da özellikle Dubai ve Hong Kong'da büyümeye devam ediyor.

Türkiye tarafında da önemli gelişmeler yaşandı. 2024'te kabul edilen 7518 sayılı Kanun ile kripto varlıklar ilk kez hukuki bir tanıma kavuştu. Sermaye Piyasası Kurulu (SPK) kripto varlık hizmet sağlayıcılarını lisanslama yetkisine sahip oldu. 2025 itibarıyla borsaların MASAK'a kayıtlı olması ve kimlik doğrulama (Travel Rule) kurallarına uyması zorunlu hale geldi. Vergilendirme tarafında ise 2026'da yeni bir düzenleme gündeme geldi, SPK lisanslı borsalarda işlem başına binde üç oranında bir işlem vergisi ve kazançlar üzerinden stopaj öngörülüyordu, ama bu

teklif Mart 2026'da TBMM'de geri çekildi ve yasalaşmadı. Yani şu an itibarıyla Türkiye'de kripto paraya özel bir vergi kanunu yürürlükte değil.

Tüm bu gelişmeler bir araya geldiğinde ortaya çıkan tablo şu, kripto paralar artık "*düzenlenmemiş vahşi batı*" imajından çıkıp geleneksel finansla iç içe geçmiş, kuralları netleşen bir alana dönüşüyor ve bu dönüşüm halen devam ediyor. Üstelik oldukça hızlı bir biçimde. **Bu yüzden bu bölümdeki bilgilerin zamanla değişebileceğini unutmamakta fayda var.** Güncel gelişmeleri takip etmek isteyenler için birkaç güvenilir kaynağı da buraya bırakıyorum:

- SPK'nın kripto varlık düzenlemeleri için resmi duyuruları: spk.gov.tr
- ABD'deki stablecoin düzenlemesi (GENIUS Act) için: congress.gov/bill/119th-congress/senate-bill/1582
- RWA piyasasındaki güncel verileri takip etmek için: rwa.xyz

Sonuç

Bu kitabı bir harita gibi düşünebilirsiniz. Paranın tarihinden başlayıp kripto paraların katmanlarına, oradan yatırım ve güvenliğe kadar uzanan bir harita. Ama hiçbir harita, yolu sizin yerinize yürümüyor.

Şimdi elinizdeki bu haritayla ne yapacaksınız? Piyasa yarın da, bir yıl sonra da bugünkünden farklı olacak. Yeni projeler çıkacak, yeni anlatılar doğacak, bugün doğru bildiğiniz bir şey altı ay sonra geçerliliğini yitirebilecek. İşte tam da bu yüzden bu kitap size ezberlemeniz gereken bir bilgi yığını değil, her yeni durumda kullanabileceğiniz bir soru sorma alışkanlığı kazandırmayı hedefledi. Bir proje gördüğünüzde artık kendinize hangi soruları soracağınızı biliyorsunuz. Bir fırsat karşınıza çıktığında o fırsatın gerçek mi yoksa bir tuzak mı olduğunu ayırt edebilecek bilgiye sahipsiniz.

Kripto paralar hâlâ genç bir teknoloji. Bu alanda kesin olan çok az şey var, ama bir şeyi rahatlıkla söyleyebilirim, bilgiyle hareket eden bir yatırımcı olmak, körü körüne hareket eden bir yatırımcı olmaktan her zaman daha güçlü bir konum.

Son Söz

Önsözde bir sabah beşte kalkıp bu kitabı yazmaya başlayan bir hikâyeden bahsetmiştim. O zamanki tek amacım zor yoldan öğrendiğim her şeyi bir yerde toplayıp benim gibi sıfırdan başlayan birine yardımcı olacak bir kaynak bırakmaktı. Şimdi bu son satırları yazarken aynı amacın halen geçerli olduğunu görüyorum. Sadece bu sefer çok daha fazla kişiye ulaşma şansım var.

Bu kitabı yazarken hayal ettiğim okuyucu tam olarak sizdiniz. Umarım şu an kitaba başladığınız andan bir adım değil, çok daha fazla yol kat etmiş biri olarak buradasınız.

Anlamadığınız bir konu ya da aklınıza takılan bir soru olursa çekinmeyin, bana buradan ulaşabilirsiniz.

Telegram: @CanAhmeth
X: @CanAhmeth
LinkedIn: Can Ahmet Değirmenci

Bu satırları okuduğunuz için teşekkür ederim. Yolunuz açık olsun.