5 SORUDA
BLOKZİNCİRİ

PROF. DR. CEM SAY

BKM
BANKALARARASI
KART MERKEZİ

Tasarım ve Grafik Uygulama
MARJİNAL

Editör
GİZEM GÜNEŞ ERBİL

Baskı
İNCEKARA MATBAACILIK
Maltepe Mahallesi, 1BB5 2. Matbaacılar Sitesi, 34010 Zeytinburnu/İstanbul

5 SORUDA
BLOKZİNCİRİ

EYLÜL 2019

Katkı Sağlayanlar:
Prof. Dr. Cem Say, Dr. Soner Canko, Celal Cündoğlu, Özge Çelik,
Okan Yıldız, Enes Türk

BANKALARARASI
KART MERKEZİ

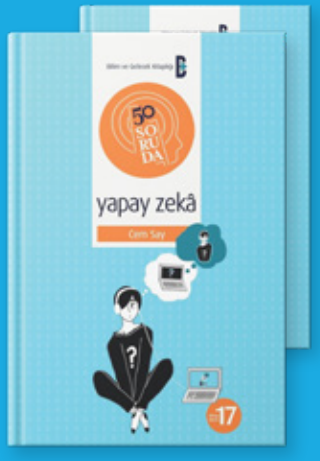
Sorumsuzluk Beyanı

İşbu rapor, yeni nesil teknolojilerden biri olan ve son dönemde birçok sektörde kullanım alanları araştırılan blokzinciriyle ilgili olarak Prof. Dr. Cem Say'ın Herkese Bilim Teknoloji dergisinde yayımlanmış olan yazı dizisi temel alınarak sadece bilgilendirme amacıyla hazırlanmıştır. Kişi ve kurumlara bağlayıcı tavsiye veya görüş niteliği taşımaz. İşbu raporda yer alan bilgilerin güncel ve eksiksiz olduğu taahhüt edilmemektedir. İşbu raporda verilen tüm bilgi ve görüşler zamanla değişkenlik gösterebilir. Bu bağlamda işbu raporun içeriğini okuyan kişilere veya herhangi bir üçüncü kişiye karşı sorumluluğu ve yükümlülüğü bulunmamaktadır.

Prof. Dr. Cem Say

YAZAR HAKKINDA

Prof. Dr. Cem Say, Boğaziçi Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyesi ve Bilişsel Bilim Lisansüstü Programı'nın kurucularındandır. Finansal sahtekarlıkların yapay öğrenme ile büyük hacimli işlem bilgilerinden otomatik tespit edilmesi gibi uygulama projelerinde yer alan Say'ın araştırma konuları arasında, blokzinciri altyapısının mantık ve güvenliğiyle doğrudan ilgili olan kuramsal bilgisayar bilimi, kriptografi ve kuantum hesaplama alanları da bulunmaktadır. Blokzinciri ve derin öğrenme gibi güncel teknik konuları kitlelerin anlayabileceği dilde anlattığı popüler bilim yazıları Herkese Bilim Teknoloji dergisinde yayımlanmakta olan Say, "50 Soruda Yapay Zekâ" kitabının da yazarıdır.



Celal Cündoğlu
BKM Genel Müdür Yardımcısı

SUNUŞ

Prof. Dr. Cem Say'ın ifadesi ile "devrimci bir bilgisayar bilimi fikri" olan blokzincirinin bir güven makinesi olduğunu anladığımızda bu fikir marifeti ile hayata geçirilebilecek farklı blokzinciri çözümlerinin bize sunabileceklerinin potansiyelini hayal eder olduk.

İnsanları diğer canlılardan ön plana çıkartan özelliği, birbirlerini tanımasalar dahi çok büyük kitleler halinde iş birliği yapabilme becerileridir. Bu iş birliklerinin temelini oluşturan güven olgusu ortak lisanlar, ritüeller, inançlar, anlaşmalar, para birimleri, yerel ve uluslararası kanunlar ve yıllar içinde olgunlaşmış süreçler ile besleniyor. Şimdi ise birbirini tanımayan insanların iş birliği yapabilmesini sağlayacak, güven olgusunu iyice pekiştirecek hatta belki eski güven sağlama yöntemlerine alternatif oluşturacak, bunu da matematiğin bilimselliğine yaslayacak blokzinciri adında bir güven makinası çıktı. Bu güven makinası diyor ki; birbirini tanımayan insanlar, işin içinde merkezi güvenilir bir parti olmadan dahi aralarında işbirliği, ticaret ve her türlü değer alışverişi yapabilirler. Sadece blokzincirinin arkasındaki teknolojiye güvenmeleri yeterli. Ancak güven otomatikman ortaya çıkan bir olgu değil. Blokzincirine neden güvenmemiz gerektiğini anlamamız gerekiyor ve zorluk da burada başlıyor. Çünkü ileri matematik, kriptografi, dağıtık kayıt yapıları, algoritmalar gibi kavramlar kitlelerin değil bilim insanlarının uzmanlık alanı.

Birilerinin bu olguları ortalama ilgi seviyesinde okur tarafından anlaşılır kılmasına ihtiyaç var. Prof. Dr. Cem Say'ın elinizde tuttuğunuz yazıları yalın bir anlatım ile blokzincirinin nasıl işlediğini ortaya koyuyor. Güven makinesi blokzincirinin ismini ilk duyurduğu ve kitleler tarafından denenerek kendini ilk kanıtladığı yer, popüler kripto para uygulaması bitcoin oldu. Bu yazı setinde basit sorular cevaplanarak bitcoin blokzincirinin teknik olarak nasıl çalıştığı anlatılıyor. Blokzinciri mekanizmalarının nasıl çalıştığı yeteri derecede anlaşılırsa farklı iş problemlerini bugün olduklarından daha etkin bir şekilde çözmek için farklı blokzinciri ağları kurulabilir. Biz de BKM'nin yerinde Ar-Ge merkezinde dünyada gelişmekte olan farklı blokzinciri uygulamalarını çeşitli kavram ispatı projeleri ile deneyimliyoruz. BKM'nin vizyonu "nakitsiz ödemelerde geleceğin deneyimini yaşatmak". Vizyonumuzun gerçekleşmesinde blokzincirinin önemli katkısı olacağını düşünüyoruz ve teknolojinin potansiyelini araştırıyor, çeşitli kullanım vakalarında deneyimliyor, bulgularımızı kamuoyu ile raporlar aracılığı ile paylaşıyoruz. Kısacası Cem Say Hoca'nın anlattıklarını bir de biz görelim de daha iyi öğrenelim diye elimizi Ar-Ge merkezimizde kirletiyoruz.

Bu bilinç doğrultusunda bugüne kadar iki blokzinciri uygulamasını hayata geçirdik. Bunlardan birisi BKM çalışanları tarafından kullanılan motivasyon ve ödüllendirme uygulaması BBN'di. Hyperledger Fabric üzerinde geliştirilen BBN ile test ettiğimiz kavramlar; dijital kimlik, dijital para, dağıtık kayıt defteri ve akıllı sözleşmeler oldu. BBN'in ardından ise farklı bir platformu tanımaya karar verdik ve Ethereum tabanlı dijital sertifika uygulaması Belgem.io'yu kullanıma sunduk.

Belgem.io kapalı devre bir uygulama değildi ve bu anlamda BBN'den farklılaştı. Katılımcı kurumlardan sertifika almış herkes, belgelerini Belgem.io üzerinden talep edebiliyor. Her iki uygulamamızda öğrendiklerimizi de birer rapor haline getirip kamuoyu ile paylaştık. Olgunlaşmakta olan bir teknolojiyle ilgili paylaşımda bulunmanın çok önemli olduğuna inanıyoruz. Bu tür paylaşımlarda yer verilen her türlü bilgi ve deneyimi, teknoloji bilincinin oluşması ve belirsizliklerin azalması açısından çok değerli buluyoruz.

"Blokzinciri nedir?" sorusuna bulabileceğiniz en yalın yanıtın derlendiği bu yazı setinden faydalanacağınızı umuyor ve bizimle beraber bu teknolojinin potansiyelini hayal etmeye sizi davet ediyoruz.

SESSİZ DEVRİMİN DİP DALGASI: BLOKZİNCİRİ

Dijitalleşme, hayatımızın her alanında köklü değişikliklerin gerçekleşmesini sağlarken teknolojik yenilikler yaşantımızda adeta sessiz devrimler yapıyor. İnternet bu sessiz devrimlerden biriydi. Son dönemde ise akıllı telefonlar benzer etkiyi yaptı. Yaklaşık on yıl önce akıllanmaya başlayan cep telefonlarımız, bilgisayarların cebimize girmesini sağlarken günlük yaşantımızın yanı sıra bilgiye erişme yöntemimizi ve iş yapma biçimimizi de değiştirdi. Bu sessiz devrimlerin en yenilerinden birinin altında ise blokzincirinin imzası olacak gibi görünüyor.

Her ne kadar bitcoin ile zirve yürüyüşüne başlamış olsa da blokzinciri teknolojisinin kökeni çok daha eskilere dayanıyor. Doksanlı yılların başında blokzincirinin alt bileşenlerini ele alan üç makale yazılmıştı. Stuart Haber ve Scott Stornetta'nın 1991 yılında kaleme aldığı makalede anlatılan ve dijital belgelerin zaman damgası ile geriye dönük olarak değiştirilememesini sağlayan çözüm, blokzinciri teknolojisinin ardındaki fikirlerden biri olarak kabul ediliyor. Ross Anderson tarafından 1996 yılında yazılan makalede ise yapılan değişikliklerin silinemeyeceği, merkezi olmayan bir veri kayıt sistemi anlatılmıştı. Bruce Schneier ve John Kelsey'nin 1998 yılında yazdığı makalede ise şifreleme yapısı ele alınmıştı. Blokzincirinin bu bileşenlerinden faydalanan ilk önemli uygulama ise bugün "kripto para" olarak anılan dijital paraların atası olan bitcoin oldu. Satoshi Nakamoto takma adlı kişi veya grup tarafından 2008 yılında hazırlanan makalede anlatılan bitcoin kullanılarak yapılan ilk işlem ise 2009 yılının başında gerçekleşti.

Ne var ki bitcoin'in tüm dünyada bilinen bir kripto paraya dönüşmesi çok hızlı olmadı. 2011 yılının ikinci yarısında fiyatı yükselmeye başlayan bitcoin'in bilinirliği de zaman içerisinde giderek arttı. Ancak kripto paranın bu denli popüler olması, blokzinciri deyince insanların aklına bitcoin'in gelmesine, yani büyük bir yanlış anlaşılmaya mahal verdi.

Oysa blokzinciri, çok daha büyük bir etki yapma potansiyeline sahipti ve bu gerçek, zaman içerisinde fark edilecekti.

Bitcoin, blokzincirinin kullanım alanlarından sadece biriydi ve blokzinciri uygulamaları kripto paralarla sınırlı değildi. Merkezi olmayan yapılar sayesinde kişi ve kurumlar arasında dijital güven ortamı tesis edilmesini sağlayan teknolojinin değerinin anlaşılması kolay olmadı. Bu anlamda blokzinciri ile daha fazlasının yapılabileceğine inanan Vitalik Buterin'in 2015 yılında Ethereum'u kullanıma sunması, teknoloji için önemli kilometre taşlarından biri oldu. Akıllı sözleşme desteğinin yanı sıra bireylere varlıkları veri tabanlarına kaydetme imkânı veren Ethereum, dağıtık uygulamalar geliştirilebilen bir platform olarak hayatımıza girdi ve blokzinciri ekosistemine ilham verdi. Blokzinciri artık konferanslarda konuşulmaya, eğitim içeriklerine konu olmaya başlamıştı. Kurumlar da teknolojiyi gündemlerine alırken vaatlerini ve kullanım alanlarını araştırmaya koyuldular. Farklılaşan ihtiyaçlar doğrultusunda mevcut platformlar iyileştirilirken yeni çözümler de geliştirildi. Artık teknolojiyi test etme zamanı gelmişti.

Yeni nesil girişimlerden dev kurumlara kadar birçok şirket, blokzincirinin çözüm olabileceği alanlarda denemeler yapmaya başladı. Tedarik zinciri yönetimi, dijital kimlik, oylama, sağlık, finans gibi alanlar, yapılan denemelerin ve blokzincirinin katma değerinin yüksek olduğu alanlar olarak öne çıkıyordu.

Yapılan bu denemelerin teknolojinin potansiyelinin yanı sıra geliştirilmesi gereken yönleri de gözlemleniyordu. Bu anlamda yapılan projeler ve araştırmalar sonucunda üretilen raporlar teknolojinin gelişimine ve yaygınlaşmasına katkı sağlamaktadır. Okumakta olduğunuz rapor da bu düşünceden hareketle oluşturulmuş ve Prof. Dr. Cem Say'ın blokzinciriyle ilgili olarak kaleme aldığı beş yazıdan oluşan yazı dizisine yer verilmiştir. Cem Say'ın blokzinciriyle ilgili beş sorunun yanıtını yalın bir dille anlattığı yazılarda teknolojiyle ilgili hap niteliğinde bilgileri bulacaksınız.

CEM SAY İLE BEŞ SORUDA BLOKZİNCİRİ

Bu bölümde Prof. Dr. Cem Say'ın blokzincirinin yapısını ve mantığını anlatmak amacıyla kurguladığı 5 soruyla ilgili Herkese Bilim Teknoloji Dergisi için kaleme aldığı yazıları bulacaksınız.

- SORU 1:
  Merkezden Nasıl Kurtuluruz?
- SORU 2:
  Blokzinciri Nedir?
- SORU 3:
  Birbirini Tanımayan Binlerce Kişi Nasıl İş Birliği Yapabilir?
- SORU 4:
  Zincire Yeni Bloğu Kim Ekleyecek?
- SORU 5:
  Neden Tek Bir Zincir Güvenilir?

Soru 1: Merkezden Nasıl Kurtuluruz?

Son yıllarda ekonomi haberlerinin izleyicileri kripto paralarla ve bu yeni para cinsinin en ünlü örneği olan bitcoin ile karşı karşıya geldiler. Herhalde çoğu kişinin, gerçekten karmaşık bu kavramı ilk seferde anlamadığını söylemek yanlış olmaz. Kripto paraların nasıl çalıştığını açıklamak için üstüne kuruldukları devrimci bilgisayar bilimi fikrinin yani blokzincirinin ne olduğunu anlatmak gerekiyor. Bu kitapçığın amacı sizlere bu blokzinciri konusunu sorularla aktarmak olacak. Hoş geldiniz!

Sanırım en kolayı, blokzincirinin çözmeyi amaçladığı sorunun ne olduğunu ortaya koyarak başlamak. Önemli bilgilerin (söz gelimi kimin kime ne kadar para havale ettiğine ilişkin kayıtların, tapu sicillerinin, vatandaşların farklı hastanelerde yaptırdıkları tahlil sonuçlarının vs.) tutulduğu bir kütük (bilgisayarcılıktaki deyimiyle veri tabanı) düşünün. Bu veri tabanının kimin kontrolünde olduğu çok önemli, değil mi? Ali Veli'ye 1000 TL havale gönderdiğini, Veli ise bu parayı almadığını iddia ederse kimin haklı olduğu Ali veya Veli'nin defterlerine değil, bankadaki merkezî kayda bakılarak anlaşılıyor. Peki ya bu merkezî merciyi aradan kaldırmak istiyorsak?

“Bunu neden isteyelim?” mi dediniz? Bir dizi nedenimiz olabilir. Bilgi güç demektir, bilginin tek muteber kopyasına sahip bir aracının bu gücü haksız şekilde kullanması (mesela bir sabah uyandığınızda bir siber saldırı sonrası tapu kayıtlarıyla oynandığını ve evinizin başka birinin malı olarak görünmesi durumuyla karşılaşsanız) ihtimalinden kaygılanıyor olabilirsiniz. Peki ama bu veriler merkezde tutulmazsa nerede tutulacak?

Her yerde! Daha doğrusu, dünyanın her köşesinde, birbirini tanımayan kişilere ait on binlerce bilgisayarda! Böylece kötü kalpli bir müdahalecinin verinin tek kopyasını değiştirerek indireceği bir darbeden kurtulabiliriz. O kadar bilgisayarın hepsini birden ele geçirecek halleri yok ya bu kötülerin! Yapılan her yeni işlem, kütüğe eklenen her yeni kayıt, işlemi yapan kişinin bilgisayarından diğer tüm bilgisayarlara duyurulsun, her bilgisayar kendi kütük kopyasını güncellesin. Teknik adıyla bir “eş düzeyliler ağı” olan bu düzende herkes bilgilerini herkesle paylaşır (aslında herkes duyduğu her şeyi komşularına söyler, o komşular da kendi komşularına...), yani ha bire her yönde iletişim olur. Merkezi yok etmek için ödediğimiz bedel budur. Ama bir dakika, o zaman karşımıza başka bir dizi sorun çıkıyor:

1. Kimi hassas bilgilerimizi, örneğin bankada ne kadar paramız olduğunu tüm bu bilgisayarların sahibi olan yabancıların görmesini ister miyiz?

2. Kötü niyetli kişilerin müdahalesiyle veya kütüğe yasal değişiklikler (mesela yeni para transferleri) yapıldığına ilişkin mesajların iletişim koşulları nedeniyle değişik bilgisayarlara değişik sırada ulaşmasından ötürü farklı bilgisayarlarda kütüğün farklı kopyaları oluşursa işin tadı kaçmaz mı? Bu çok sayıda bağımsız bilgisayarda tutulan veri tabanlarının tıpatıp aynı içerikte olmasını nasıl garanti edeceğiz? Merkeze güvenmiyorsak bu bilgisayarların hiç tanımadığımız sahiplerine neden güvenelim?

3. Zaten birbirini tanımayan on binlerce kişi neden tüm bu zahmete girsin ki? Başka işleri yok mu?

Sırayla bu problemlerin çarelerini ele alacağız.
Birinci sorun, açık anahtarlı şifrelemeyle çözülüyor. Her kullanıcının herkese duyurduğu bir açık, bir de kimselere söylemediği gizli anahtarı oluyor. (Bu anahtarları kolayca üretebildiğiniz iki sayı olarak düşünün.) Gizli anahtar, bu iş için geliştirilmiş özel bir program aracılığıyla istenen herhangi bir metni imzalamak (yani o metnin altına sadece sizin üretmiş olabileceğiniz bir başka metin eklemek) için kullanılıyor. En ünlü blokzinciri uygulaması olan bitcoin ağındaki diğer kişiler sizin adınızı değil, açık anahtarınızı biliyorlar örneğin. Açık anahtarınız, başka bir program yardımıyla sizin imzalamış olduğunuz iddia edilen bir metni kontrol etmek için kullanılabiliyor. Bir açık anahtar, sadece kendisine karşılık gelen gizli anahtarla imzalanmış bir metni onaylayabiliyor, başka imzalarla karşılaştığında alarm veriyor. Böylece hem gerçek kimliğinizi gizli tutabiliyor hem de "Açık anahtarı filanca olan kişiye kendi hesabımdan 10 bitcoin yolluyorum." gibi mesajları (gizli anahtarınızı bilmeyenlerce) sahtesi yapılamaz şekilde imzalayıp duyurabiliyorsunuz.

Soru 2: Blokzinciri Nedir?

Bu ağın her üyesinin veri tabanının aynı kopyasını tutmasını sağlamamız gerek. Bu zor bir problem! Çünkü sadece sabotajcılar değil, sıradan uyanıklar da bu tekdüzeliği bozarak çıkar elde etmeye çalışabilir. Diyelim Ali ve Veli adında iki kötü kalpli kardeş, Saffet adında saf bir otomobil satıcısını dolandırmaya niyetlendiler. 10 bitcoin'i olan Ali, "Saffet'e 10 bitcoin yolladım." mesajını ağa duyurur. Bunu gören ve artık o paranın kendisine ait olduğunu düşünen Saffet, Ali'ye bunun karşılığında güzel bir araba satar. Fakat Ali tam o sırada bir de "Veli'ye 10 bitcoin yolladım." mesajı yayınlar. Hatlardaki farklı iletişim süreleri nedeniyle ağdaki bilgisayarlar bu iki mesajı farklı sıralarda alabilir. Sistemin mantığı, ağdaki her bilgisayarın kendindeki kütük kopyasına duyurulan yeni bitcoin işleminin bilgilerini eklemeden önce işlemi denetlemesi, yani Ali'nin ilk kaydından bu yana yaptığı bütün alışverişleri tarayarak şu anda bu harcamayı yapacak parası olup olmadığını kontrol etmesini gerektirir. Olayımızda Veli'ye yapılan transfere ilişkin mesajı önce alan bilgisayarlar bunu kayda geçirirlerse, daha sonra ellerine geçen Saffet'e yönelik transfer işlemini "Ali'nin artık bu kadar parası yok." diye reddedeceklerdir. Yani Saffet arabayı vermiş ve karşılığında bir şey alamamış olacaktır. Zaten kayıt defterimizin birbiriyle tutarsız birden farklı kopyasının olması bütün projeyi berbat edecektir. İşte bu problemin çözümü blokzinciri dediğimiz yapıya bağlı. Şimdiye dek kütük, veri tabanı veya kayıt defteri diye andığımız ortak bilgi kümesini, belirli boylarda bloklardan oluşan bir zincir şeklinde yapılandıracağız. Ezelden, daha doğrusu kayıt tutmaya başladığımız andan beri yapılan tüm işlemler, böyle blokların içine gruplanıp zincire eklenecek. Blokları A4 kâğıtları gibi düşünün. Önce bir kâğıda ilk yapılan birkaç işlem yazılıyor. Ayrıca bu kâğıdın adı diyebileceğimiz özel bir sayı (detayını sonra göreceğimiz şekilde) hesaplanıp üstüne yazılıyor. (Blokları neden basitçe 1, 2, 3 diye adlandırmadığımızı göreceksiniz, bu adlandırmanın kolay bir iş olmasını istemiyoruz.)

Bu şekilde hazırlanmış ilk sayfanın kopyaları tüm ağa dağıtılıyor. Sonraki birkaç işlem başka bir kâğıda kaydedilip bu yeni kâğıdın üzerine "bu sayfadan önceki sayfa şuydu" etiketiyle bir önceki sayfanın adı yazılıyor. Tabii bu yeni hazırladığımız sayfanın kendi adı da hesaplanıyor. Bu sayfa da dünya âleme duyuruluyor. Böyle böyle veri tabanımız art arda (bitcoin sisteminde yaklaşık 10 dakika aralıklarla) o arada sistemin kullanıcıları tarafından yayınlanan işlem bildirimlerinden birkaçının bir araya getirilmesiyle hazırlanıp yine tüm sisteme duyurulan sayfaların eklenmesiyle gelişiyor. Hiçbir işlem daha önce hazırlanıp yayınlanmış bir sayfada değişiklik yapmıyor, yeni para transferleri vs. hep yeni sayfalara ekleniyor. Yani veri tabanı geçmişin tüm bilgisini içeriyor.

Soru 3: Birbirini Tanımayan Binlerce Kişi Nasıl İş Birliği Yapabilir?

Kripto para bitcoin için icat edilen ama çok daha geniş ve çarpıcı uygulamalarının da olabileceği şimdiden görülen blokzinciri veri yapısını anlatmaya devam ediyoruz. Önceki bölümlerde kopyaları on binlerce bilgisayarda tutularak merkezî bir merciye tabi olma zorunluluğunu ortadan kaldıran bu yapının art arda eklenen veri bloklarından oluştuğunu, her bloğun içine kendisinden önceki bloğun adının yazıldığını, böylece mesela Ali'nin kaç bitcoin'i olduğunu merak eden bir kişinin tek yapması gerekenin sondan başa bütün zinciri tarayarak Ali'nin tarih boyunca kimden ne kadar alıp kime ne kadar verdiğini okumak olduğunu görmüştük.

Hâlâ her bilgisayarın her zaman blokzincirinin hep aynı kopyasını tutmasını, birbirini tanımayan on binlerce kişinin bilgisayarlarında bu işi, hem de bu dediğimiz kurallara uygun olarak yapmalarını nasıl sağlayacağımızı söylemedik. Aslına bakarsanız, yukarıda bahsettiğimiz blokları ağdaki binlerce bilgisayardan hangisinin hazırladığını da söylemedik. Tek bir bilgisayara bu görevi vermek merkezi yapıyı yok etme fikrimize temelden karşı değil mi?

Zincire eklenecek bir sonraki bloğu hangi bilgisayarın üreteceği bir yarışmayla belirleniyor. Yarışmayı kazanan bilgisayarın sahibi, bundan bir çıkar sağlıyor. Örneğin bitcoin ağında bu işi yapan ve madenci diye anılan bilgisayarlar başarılı olduklarında sahiplerinin hesabına hem yeni ödül bitcoin'leri hem de bu blokta kayda geçen işlemleri yapanların belirtmiş olabilecekleri işlem ücretleri geçiyor ve ağdaki herkes mantıken o kazananın ürettiği bloğu (kontrol ettikten sonra) kendi bilgisayarındaki zincire ekleyip çalışmaya devam etme eğiliminde oluyor. Çünkü bu oyunun kuralları işlemci gücünü onlara uymaya harcayanların hile yapmaya çalışanlardan daha çok para kazanacağı şekilde ayarlanmış. İşte bu nedenle ağın büyük çoğunluğundaki bilgisayarlar hep aynı veri tabanına sahip oluyor.

Bu harika düzenin kurulup işleyebileceğine ikna olmak için birkaç matematiksel tanım gerekecek. Buyurun:

Kriptografik özüt (hash) fonksiyonları

Bilgisayar programlarına verilen bilgiye girdi, programın cevaben çıkardığı bilgiye de çıktı dendiğini hatırlayalım. Özüt fonksiyonu dediğimiz şey, girdi olarak herhangi bir metni verebileceğiniz, verdiğiniz metinlere karşılık gelen çıktılar olarak da size hep aynı sabit uzunlukta (diyelim ki hep 256 karakter boyunda) metinler döndüren hızlı bir programdır. (Bilgisayarcılıkta sadece "bit" adı verilen 0 ve 1 rakamlarını kullanarak her şeyi ifade edebiliriz, özütlerimizi de bit dizileri olarak düşünün.) Girdi olarak aldığı M metni için programın verdiği çıktı metnine, M'nin özütü denir. Fonksiyonunuzun iki farklı girdi metni için aynı özütü döndürmesi olayına çarpışma denir. Ve iyi özüt fonksiyonlarının olabildiğince az çarpışmaya yol açması istenir.

Buraya kadar anlattığım özüt fonksiyonuydu. Peki bu ismin önüne kriptografik sıfatını koymak ne anlama geliyor?

Bazı programların verdikleri çıktıya bakarak almış oldukları girdiyi kolayca hesaplayabilirsiniz. Mesela görevi, kelimeleri ters yüz etmek olan bir program "CAT" çıktısını verdiyse, girdisinin "TAC" olduğunu rahatça bulabiliriz. Bazı programlar içinse ilgilendiğimiz bir metni çıktı olarak çıkartacak bir girdiyi bulmak çok zordur. Hatta aklımıza bütün olası girdileri teker teker programa verip denemekten başka bir yol gelmez. İşte tersinin hesaplanmasının bu anlamda zor olduğu düşünülen özüt fonksiyonlarına kriptografik özüt fonksiyonu denilir.

İyi bir kriptografik özüt fonksiyonu aldığı girdiyi öyle karışık bir şekilde çıktıya dönüştürür ki ona verilen bir metnin özütü (aslında kesin kurallara göre hesaplanmış olsa da) sanki o 256 karakterin tüm olası kombinasyonları arasında piyango çekimiyle belirlenmiş izlenimi verir.

Soru 4: Zincire Yeni Bloğu Kim Ekleyecek?

Bir önceki başlıkta anlattığımız matematiksel özelliklerden yararlanarak, yeni bir bloğun kopyaları on binlerce bilgisayarda tutulan veri tabanına nasıl eklendiğini göreceğiz.

"Ali Veli'ye 3 bitcoin yolladı" gibi işlem bilgilerinin (istenirse kullanıcıların gerçek isimleri kullanılmadan) tüm ağa duyurulduğunu daha önce görmüştük. Böyle bir duyurunun yapılması, işlemin o anda gerçekleştiği anlamına gelmiyor. Paranızın yerine ulaştığından emin olmanız için işlem bilginizin (genelde başkalarınca duyurulmuş başka birkaç işlem bilgisiyle birlikte) bir bloğa yazılmasını, o bloğun adının hesaplanarak zincire eklenmesini, hatta (sonraki bölümlerde göreceğimiz nedenlerden) işi sağlam tutmak için onun da ardına birkaç bloğun daha eklenmesini beklemelisiniz.

Zincire eklenecek her yeni blok için yeni bir ad hesaplandığından söz etmiştik. İşte bu ad bir kriptografik özüt olacak. Her yeni blok, o bloktan bir önceki (yani hâlihazırdaki zincirin sonundaki) bloğun adını, kullanıcılarca duyurulmuş ve henüz zincire eklenmemiş bir dizi işlem bilgisini, bu bloğu üretmeyi başaran madencinin ödülü olacak sanal paranın yaratılış bilgisini ve joker diyebileceğimiz (ne olduğunu az sonra göreceğimiz) bir diğer sayıyı içeriyor. Bloğun adı da bu içeriğin bütününü oluşturan metnin kriptografik özütü olacak. Önceki yazılarda kriptografik özütlerin hızlıca hesaplanabildiklerini, ad hesaplama işininse zor olmasını istediğimizi belirtmiştim. Bu zorluğu sağlamak için blok adlarının uyması gereken ek bir şart koyuyoruz, mesela ilk 30 rakamlarının 0 olması gibi...

Bu şart işi değiştiriyor, çünkü hatırlarsanız bir metnin kriptografik özütü rastgele seçilmiş gibi görünen 0 ve 1 rakamlarından oluşan bir karışım oluyor. Görünürdeki bu rastgele olma hali nedeniyle tipik bir metnin özütünün ilk rakamının 0 olma ihtimali 1/2, ilk iki rakamın ikisinin birden 0 olma ihtimali 1/4, ilk üçününki 1/8 oluyor. Yani ilk 30 rakamın da 0 çıkma ihtimali, hilesiz bir paranın üst üste 30 kere atılıp 30'unda da yazı çıkması ihtimaline eşit. Bu da milyarda birden az bir olasılık.

Blokta joker diye bir sayı olacağından söz etmiştim. Bloğun içindeki her değer gibi o sayı da özütü etkiliyor. Bloğun geri kalanını aynı tutup sadece jokerini değiştirirseniz özütü çok değişik (ve yine rastgele yazılmış izlenimi veren) başka bir sayı oluyor. Madencilerin blok üretirken yaptıkları işlem, joker için art arda bir sürü değer deneyip oluşan blokların özütlerini hesaplayarak istenen "ilk 30 rakam 0" şartına uygun bir ad çıkartmaya çalışmak. Tek bir bilgisayarın böyle bir bulmacayı çözmesi ortalamada çok uzun sürer. Ama bir değil, 10 binlerce madenci bu işi yapmak için aynı anda çalışıyor ve problemin zorluk seviyesi kabaca her 10 dakikada bir ağdaki bilgisayarlardan birinin bir çözüm bulabileceği şekilde sürekli ayarlanıyor.

Bir madenci, hazırladığı paketin aranan şarta uygun bir özütünün olmasına el veren bir joker bulduğunda hemen bloğunu herkese duyuruyor. Ağda kimse kimseye güvenmediği için, bu mesajı alan herkes onu önce bir kontrol ediyor. Eğer yayımlanan bloktaki işlemler geçerliyse, yani imzalar tutuyorsa, harcama yapanların harcadıkları şeylerin gerçek sahipleri oldukları blokzincirinde yazılı geçmiş kayıtlardan teyit edilebiliyorsa ve bu blok içeriğine bu joker değeri eklenip kriptografik özüt hesaplandığında gerçekten bu madencinin duyurduğu blok adı çıkıyorsa o zaman blok sınavı geçiyor. Kurallara göre herkesin böyle bir bloğu kabul edip kendi bilgisayarındaki zincirin sonuna eklemesi gerekiyor.

Peki ama neden bunu yapsınlar? Eğer herkes kendi çıkarını önemsiyorsa, diyelim bir madenci bileğinin hakkıyla yeni bir blok üretmeyi başardığında yukarıda anlattığım kurala uymayıp kendi denemelerini sürdüren, neden sonra bulduğu bir jokerle kendi bloğunu tamamlayıp "Bakın, ben buldum!" deyip kendi zincirini ona göre uzatan madenciler olursa ya da bir dolandırıcı önceden duyurup karşılığında bir mal satın aldığı 5 bitcoin'lik bir ödeme kaydının hiç yer almadığı başka bir blok üretip zincirin bu yeni sürümünü kullanarak aynı 5 bitcoin'i tekrar harcamaya kalkarsa? Yani insanlar herkeste zincirin aynı kopyasının bulunması için hazırlanan bu kural kitabına niye uysunlar ki?

Bu sorunun cevabını bir sonraki bölümde inceleyeceğiz.

Soru 5: Neden Tek Bir Zincir Güvenilir?

Blokzinciri birbirine güvenmeyen binlerce öğeden oluşuyorsa ödüllü blok kurma bulmacasını ilk çözen bilgisayara neden diğerleri uyarak kendi belleklerindeki kütüklere onun duyurduğu bloğu eklesin? Zincirin farklı kopyalarının oluşmasına engel olan nedir?

Önceki bölümlerde önemli işlem bilgilerini (söz gelimi kimlerin kimlere hangi sırayla ne kadar para transfer ettiğini) merkezî bir merciye bel bağlamadan tutup güncelleyebilmek için bir yöntem tarif etmiştik. Veri tabanına yazılmak üzere dünyanın dört bir yanındaki kullanıcılarca ağdaki tüm bilgisayarlara duyurulan yeni işlemlerden birkaç tanesi blok adı verilen bir tür pakete konuluyor. Bu yeni bloğun adının ne olacağının hesaplanması zor bir bulmacayı çözmeyi gerektirdiğinden birbiriyle yarışan binlerce hızlı madenci bilgisayardan biri bunu ortalama 10 dakika içinde başarıyor. "Başardım" diyen bir madencinin ilan ettiği çözümü ağdaki herkes hızlıca kontrol ediyor. Böyle bir çözümün doğru olduğunu gören herkesin de artık bu duyurulan bloğu, zincirin kendi tuttuğu kopyasının ardına eklemesi ve bu bloğun içine yazılmış işlemleri paketleme hevesinden vazgeçip yeni duyurulan birkaç işlemle yeni bir blok yaratma hedefiyle yeni bir bulmacayla uğraşmaya başlaması bekleniyor. Şimdi her biri başına buyruk binlerce farklı kişinin bu kurallara uyup kazananın hakkını teslim etmesini sağlayan gücün ne olduğunu göreceğiz.

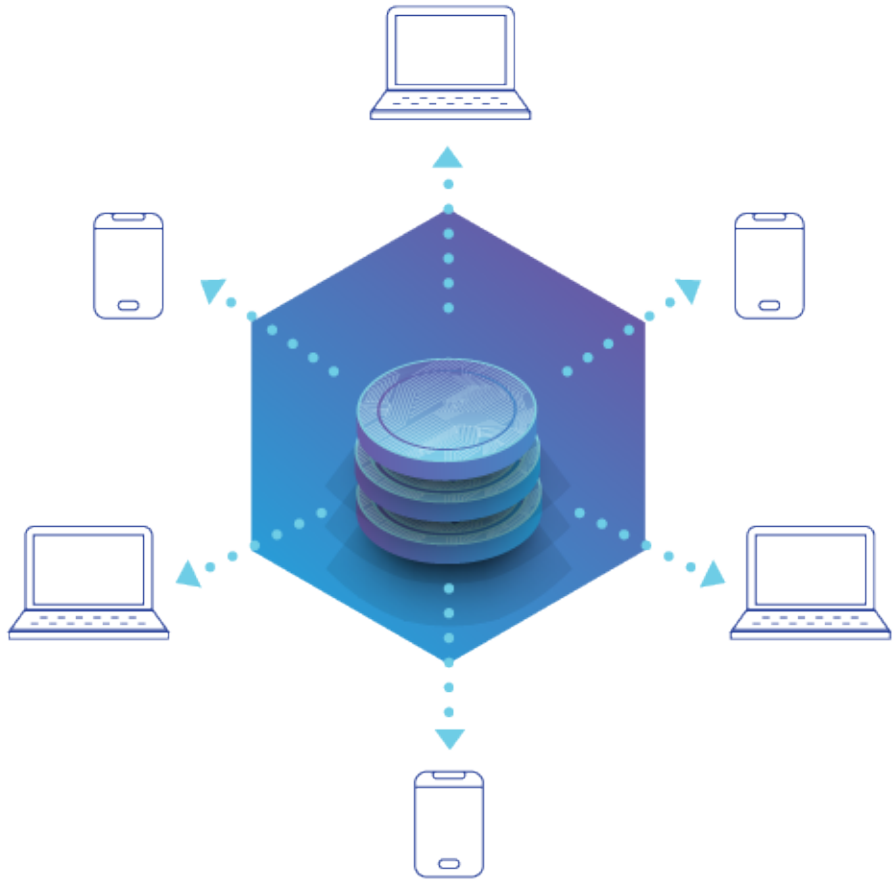
Ağdaki her bilgisayar blokzincirinin kendi tuttuğu kopyasının doğru ve güncel kopya olduğunu iddia edebilir tabii. Blokzinciri oyununun ana kuralı, ortalıkta birden fazla (imza bilgileri doğru) zincir görülüyorsa, muteber olanın (yani sizin de kullanıp güvenmeniz gerekenin) en emek yoğun olanı yani blokların art arda eklenmesi için en çok hesaplama gücünün harcanmış olması gereken olduğunu söylüyor. Daha önce gördüğümüz gibi her bloğun zorluğu adının başındaki 0'ların sayısıyla ilgili, böylece zincirin üretilmesinin toplam zorluğunu hesaplayabiliyoruz. Duyurulan yeni blokları kendi zincir kopyasına eklemeyi ihmal edenlerin (zaten son değişiklikleri de içermeyen) zincirleri bu yüzden itibar görmüyor, kimse yüzlerine bakmıyor. Bu yüzden kendi kopyasına inanılmasını isteyen herkes, en emek yoğun zinciri tutmak zorunda.

Para bir inanç işidir. Bitcoin, kimin kime kaç para verdiği bilgisinin en emek yoğun zincirde yazılı olduğuna inananlar arasında oynanan bir oyundur.

Peki mevcut zincir hangisiyse ondan daha emek yoğununu kendi bilgisayarımda (kendimi zengin edecek uydurma işlem bilgileriyle) kurup yayınlayamaz mıyım? Başkalarının adına hayali işlemler yapamam, söz gelimi bana para havale ettikleri yalanını uyduramam, çünkü gizli anahtarlarını bilmediğimden imzalarını atamam. Ama işlem gücüm yeterse çifte harcama yapabilirim

1. Bunun için önce saf satıcı Saffet'e zincirin mevcut kopyasını inceleyen herkesin halen benim hesabımda olduğunu teyit edebileceği bir miktar para gönderdiğimi anons ederim.

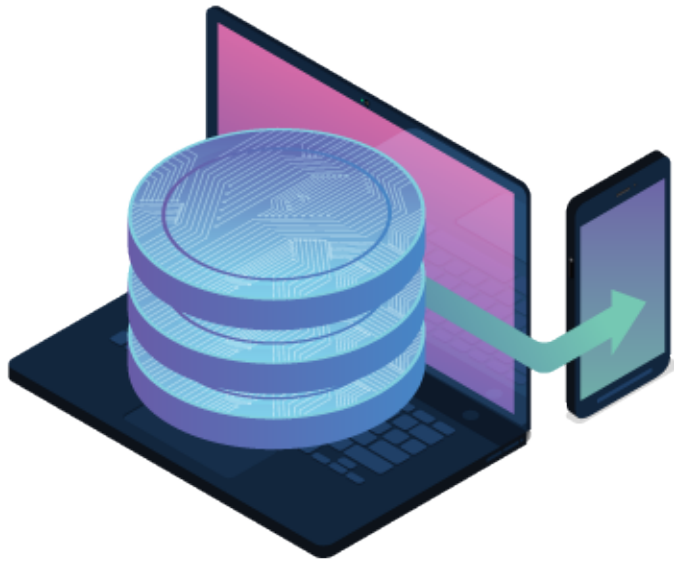
2. Başka bir madenci, Saffet'e yaptığım bu ödemenin bilgisini yeni bir blokta zincire eklemeyi başarıp bunu duyurur. Saffet de paranın artık kendi hesabına geçtiğini dünya âlemin bildiğine güvenerek bana istediğim ürünü teslim eder.



3. Bu noktada ben sanki az önceki anonsu yapmamışım gibi aynı parayı suç ortağım Veli'ye gönderdiğimi duyurur ve bir yandan da üstün güçlü bilgisayarımla Saffet'e yapılan transferi içeren bloğu yok sayarak zincirin eski haline onun yerine Veli'ye yaptığım transfer bilgisini içeren bir blok, onun üstüne de bu sahte zincir daha emek yoğun olup kabul görsün diye bir tane blok daha üretmeyi başarabilirsem yeni muteber zincirde kendisine yapılmış bir ödeme bulunmayan, yani o paraya sahip olduğu kayıtlarda yer almayan Saffet hem ürününü elden çıkarmış hem de karşılığında bir şey alamamış olur.

4. Para bir cebimden diğerine geçmiş durumdadır. Bu yöntemle aynı parayı tekrar tekrar harcayabilirim.

Ama kaygıya gerek yok. Görüldüğü gibi böyle bir hileyi yapmak isteyen kişinin bilgisayarı (ya da bu iş için satın aldığı bilgisayarlar grubu) bu hileden çıkarı olmayan, tam tersine Saffet'e yapılan para transferini kayda geçirerek ödülünü almak isteyen ağdaki tüm diğer bilgisayarlarla yarışıp onları bir değil, iki kez geçmek zorunda. Bunu başarmak için ağdaki toplam işlem gücünün yarısından çoğuna sahip olmak gerek. Blokzincirinin zayıf noktası bu. Gücün yarıdan fazlası bir grubun eline geçerse o grup çifte harcama yapabiliyor. Bu gasp, sisteme ne kadar çok kişi katılırsa o kadar zorlaşan bir iş. Dahası da var: Bu kadar ciddi işlem gücü olan birisi için alnının teriyle dürüstçe madencilik yapmak, yani zincire kurallara uygun yeni bir blok eklemek için yarışa girmek, mevcut blokları arkadan yetişip geçmekten daha kolay bir iş! Madencilikte sürekli başarı da iyi para kazandıran bir iş olduğundan zinciri bozmanın parasal bir getirisi olmuyor.



Bazen bulmacayı aynı anda ya da birbirine çok yakın zamanlarda birden fazla madenci çözebilir. Haberin ağda komşudan komşuya yayılma düzenine göre böyle durumlarda ağın içinde son blokları açısından farklı zincir kopyaları oluşabilir. İşte bu yüzden satıcıysanız size yapılan havalenin son blokta olmasıyla yetinmemek iyi bir fikir olabilir. Yarış sürdüğünden ve bu zincirlerin sonraki bloklarının da aynı anlarda üretilme ihtimali sıfıra yaklaştığından, birkaç adım sonra nasılsa bir zincir diğerleriyle boy (ve dolayısıyla emek yoğunluğu) açısından farkı açacaktır. Bu durumda kısa kalan zincirleri tutan bilgisayarlar için mantıklı hareket, kendi kopyalarını bırakıp uzun zinciri benimsemektir. Ödemenizi içeren blokzincirinin sondan altıncı konumuna vardığında başına böyle bir kaza gelmesi ihtimali rahatlıkla ürününüzü alıcıya verebileceğiniz kadar sıfıra yaklaşmış demektir. Bu da bitcoin'de yaklaşık bir saat sürer.

BITCOIN'İN ÖTESİNDE BİR TEKNOLOJİ

Eşler arasındaki işlemleri şifreleyerek dağıtık bir yapıda kayıt altına alan blokzinciri teknolojisi, "güven makinesi" olma özelliğini ise temelindeki kriptografi ve matematik bilimlerinden alıyor. Prof. Dr. Cem Say'ın beş soruya yanıt vererek blokzinciri teknolojisini tarif ettiği bölümlerde, günümüzün en popüler uygulaması olan bitcoin protokolünden örneklemeler yapılmıştır. Bitcoin protokolü hem karakteristik özellikleri, hem de kullanım alanı olarak ele alındığında blokzinciri teknolojisini yansıtan en saf uygulamalardan biri olsa da farklı ihtiyaçlar doğrultusunda yeni protokoller inşa edilmiş ve farklı kullanım alanları ortaya çıkmıştır.

Blokzinciri protokolleri, zincirde kayıtlı tutulan verinin erişilebilirliği bakımından ikiye ayrılırlar. Bunlar; herkesin erişebileceği "açık" blokzincirleri ve sadece seçilmiş eşler tarafından erişilmesi mümkün olan "özel" blokzincirleridir. Aynı zamanda zincir üzerindeki verinin okunması ve zincire yeni veri yazılması konusunda da bir ayrım vardır. Herkesin veri okuyup yazabildiği yapılara "izin gerektirmeyen" blokzincirleri denirken, okuma ve yazma yetkilerinin sınırlandırıldığı yapılara "izin gerektiren" blokzincirleri denir. Bu sınıflandırmalar düşünüldüğünde yeni bir blok oluşturulması için çözülmesi gereken zorlu matematiksel problemlerin de farklılaştığı mutabakat algoritmalarının kullanılabileceği aşikârdır. Bitcoin protokolünde kullanılan iş kanıtı (Proof-of-Work[1]) mutabakat algoritması, halka açık ve izin gerektirmeyen bir blokzinciri için makuldür ancak ciddi miktarda elektrik enerjisine ihtiyaç duyduğu da bilinmektedir. Kurumsal ihtiyaçları karşılamak üzere tasarlanan özel ve izin gerektiren yapılarda ise zorlu matematiksel problemlerin çözümü yerine, genelde güvenilir eşlerin otoritesine ihtiyaç vardır. BKM'nin gerçekleştirdiği kavram ispatı çalışmalarında faydalandığı bu mutabakat algoritmasına otorite kanıtı (Proof-of-Authority[2]) denir. Günümüzde hem halka açık, hem de özel blokzincirleri için geliştirilmiş, kullanım alanı odaklı mutabakat algoritmaları bulunmaktadır.

[1] Proof of Work: İş kanıtı. Bir ağdaki madenciler yeni bir blok oluşturmak için karışık sayısal bulmacaları çözme konusunda birbirleriyle yarışırlar. Bu bulmacaların çözümleri zordur fakat çözümleri doğrulamak kolaydır. Madenci bulmacanın çözümünü bulduğunda, bloğu ağa yayınlayabilir hale gelir ve ağdaki diğer tüm diğer madenciler çözümün doğru olduğunu doğrular.

[2] Proof of Authority: İtibar kanıtı. PoA mutabakat algoritması ağ içerisindeki blok onaylayıcılarına ait kimliklerin değerini yani itibarını kullanır. Bu nedenle PoA blockchain'lerinin güvenliği, rastgele bir şekilde güvenilir parti olarak seçilen doğrulayıcı düğümler tarafından sağlanmaktadır.

Mutabakat Algoritmalarının Atası: **“Bizans Generalleri Problemi”**

Blokzincirinde yeni bir blok oluşturmak için ağ içerisindeki düğümlerin çoğunluğunun ortak bir karara varması gerekmektedir. Mutabakat algoritmaları ise bir ağın ortak karara varma problemini çözen ve düğümlerin güvenli bir şekilde senkronize çalışmasını sağlayan prosedürler olarak tanımlanabilir. 1982 yılında bir matematik makalesi ile ortaya konulan Bizans Generalleri Problemi, günümüzde blokzinciri teknolojisinde kullanılan mutabakat algoritmalarının temelinde bulunmaktadır. Problem; bir şehri kuşatan Bizans generallerinin bir sonraki hamleleri konusunda aralarında mutabakat sağlamaya çalışırken ortaya çıkabilecek mantıksal ikilemlerden oluşuyor. Generallerden bazıları saldırmayı, bazıları ise geri çekilmeyi savunurlar. Bu durumda belirsizliği çözmek için herkesin aynı kararı uygulaması kritik önem taşımaktadır.. Generaller arasında iletişimi sağlayan ulakların görevi; mesajları hızlı ve eksiksiz bir biçimde iletmeleridir. Dürüst ve art niyetli generallerin bulunduğu bu yapıda toplam N adet dürüst general bulunurken, sistemin tolere edeceği azami art niyetli general sayısı F ile gösterilmektedir. Sistemin hata toleransı N = 3F + 1 ile formüle edilmiştir. Örneğin: 10 generalin bulunduğu bir senaryoda mutabakat yapısının tolere edebileceği art niyetli general sayısı 3’tür. Mesajların vakitli iletimi sayesinde, önceden belirlenmiş formül doğrutusunda oluşan çoğunluğun oyu uygulanacak kararı belirler. Bu problem blokzinciri dünyasında kurgulandığında, her bir general ağ içerisindeki bir düğümü temsil etmektedir. Mutabakat algoritmalarının temel amacı düğümlerin çoğunluğunun ortak karara varmalarını sağlamaktır.

Dağıtık veri kayıt sistemi olan blokzinciri teknolojisi 2015 yılında Ethereum protokolü ile farklı bir boyut kazandı. Blokzinciri 2.0 olarak bilinen Ethereum, sağladığı dağıtık sanal bilgisayar konseptiyle eşler arası mesajlaşmaların belirli şartlar altında gerçekleşmesini sağlayan akıllı sözleşme kavramını hayatımıza soktu.

Akıllı sözleşmeler, blokzinciri ağında yaşayan ve bir işlemin gerçekleşmesi için gerekli şartların yazıldığı kod parçacıklarıdır. Akıllı sözleşmelerin kafanızda canlanması için kira ödeme sürecini ele alabiliriz. Aşağıdaki örnekte her ayın beşinde gerçekleşen bir kira ödeme sürecine ait basitleştirilmiş akıllı sözleşme kodunu görebilirsiniz. KOŞUL1'de ayın beşi şartı sağlandığında sözleşme bir sonraki koşulu kontrol etmek için bir alt satıra geçer. KOŞUL2'de ise gönderici bakiyesinin kira bedelinden büyük olup olmadığı kontrol edilir. Eğer bu koşul da sağlanırsa değer transferi gerçekleştirilir.

```
SÖZLEŞME      :     Kira Ödeme
TANIMLA       :     Alıcı hesabı, Gönderici hesabı, Kira bedeli, tarih
KOŞUL1        :     EĞER (tarih  = ayın 5'i)
KOŞUL2        :     EĞER (gönderici bakiyesi > Kira bedeli)
İŞLET         :     kira bedelini göndericiden alıcıya transfer et
```

Süreçleri otomatikleştirdiği gibi birbirleriyle de haberleşme yetisine sahip akıllı sözleşmeler, belirli bir senaryonun gerçekleşmesi için birleştirildiğinde ise dağıtık uygulamaları oluştururlar. Örneğin BKM'nin hayata geçirdiği Belgem.io; eğitim sertifikalarının güvenli bir şekilde üretilmesi, saklanması ve paylaşılabilmesi için oluşturulmuş bir dağıtık uygulamadır.

Merkezi yapılara bağımlı iş modellerinin yerlerini kolektif çalışmanın hâkim olduğu konsorsiyumlara bıraktığını ve akabinde bunun sağladığı avantajları hissetmeye başladık. Oldukça geniş bir kullanım alanı yelpazesine sahip olan teknoloji, günümüzde bankacılık ve finans, dijital kimlik, tedarik zinciri ve sigortacılık sektörlerinde tercih ediliyor. Her endüstrinin ihtiyaçları farklı olduğu için blokzinciri çözümleri; güvenlik, sürdürülebilirlik ve performans açısından iş alanları bazında farklılıklar gösteriyor. Bu sebeple blokzinciri platformları ve protokolleri arasında bir sıralama yapmak doğru olmayacaktır. Her endüstri kendi çalışma şekillerine göre uygun blokzincir protokollerini tespit edecek veya geliştirecektir. Merkeziyetsizlik odaklı halka açık ve izin gerektirmeyen blokzinciri protokolleri arasında öne çıkanlara ait başlıca bilgiler Tablo 1'de listelenmiştir.

Tablo 1: Halka Açık Protokoller

	bitcoin	ethereum	Stratis	NEO	Quorum	EOS
Programlama Dili	C++	Go,C++,Rust	C#, .NET	C#	C++, Python	C++
Mutabakar Algoritması	PoW	PoW	PoS[3]	dBFT[4]	PoS	DPoS[5]
Blok Süresi	10 dk	15 sn	60 sn	15 sn	120 sn	0,5 sn
Akıllı Sözleşme Desteği	Yok	Var	Var	Var	Var	Var
Akıllı Sözleşme Dili	-	Solidity	C#, .NET	C#, Java, Python, .NET, Kotlin, JavaScript	Solidity, C++, Rust, Python	C++, C

Özel blokzinciri protokolleri ise iş alanının ihtiyaçlarına göre farklılaştırılabilen yapılardır. Kurgulanmak istenen iş akışlarının modüler bir şekilde geliştirilebileceği araçlar sunan bu yapılar, büyük teknoloji sağlayıcıları tarafından destekleniyor ve geliştiriliyor. Günümüzde en çok tercih edilen özel protokoller Tablo 2'de listelenmiştir.

Tablo 2: Özel Protokoller

	ethereum	HYPERLEDGER FABRIC	Quorum	corda	ripple
Hedef Endüstri	Çoklu sektör	Çoklu sektör	Çoklu sektör	Finans	Finans
Kullanım Biçimi	B2B	B2B	Finansal Hizmetler	Finansal Hizmetler	Finansal Hizmetler
Mutabakat Algoritması	PoW / PoA	dBFT / PoA	Raft , Istanbul BFT	PoS	RPCA[8]
Saniye Başına İşlem Performansı	~200	>2000	~100	~170	>1500
Akıllı Sözleşme Desteği	Var	Var	Var	Var	Var
Akıllı Sözleşme Dili	Solidity	Go, JavaScript	Solidity	Java, Kotlin	C++
Sahiplik	Dağıtık	Linux Foundation	Ethereum Komünitesi ve JP Morgan Chase	R3	Ripple Labs

Blokzinciri teknolojisinin geleceğinde, protokollerin birbirleriyle haberleştiği bir dünya hayal edilmektedir. Blokzincirlerinin interneti olarak tanımlayabileceğimiz bu yeni yapıda, zincirler arası çalışacak dağıtık uygulamalar ve yepyeni iş yapma biçimleri hayatımıza girecektir. Bu imkânları sağlayacak blokzinciri altyapıları için çalışmalar sürmektedir.

NASIL BİR YOL İZLENMELİ?

Birçok kişi blokzincirini, internetten sonra en önemli teknolojik inovasyon olarak görüyor. Fakat bir teknolojiden beklentinin bu kadar yüksek olması, başarıya çok hızlı ulaşacağı anlamına gelmiyor. Blokzinciri, halen eksikleri olan ve yapılan denemelerin sayısı arttıkça olgunlaşmaya devam eden bir teknoloji konumunda bulunuyor. Peki, sürekli gelişimin söz konusu olduğu teknolojide bizi bundan sonra neler bekliyor ve nasıl bir yol izlemeliyiz?

Her şeyden önce teknolojinin başarılı olup olmadığıyla ilgili kesin bir hüküm oluşturmak için henüz erken olduğunu düşünüyoruz. Çok hızlı karar vermemek, sabırlı davranıp teknolojiyi tanımak ve geliştirmek için kaynak ayırmamız gerekiyor. BKM olarak bugüne kadar gerçekleştirdiğimiz kavram ispatı çalışmalarında teknolojinin potansiyelini net biçimde gördük. Blokzincirine bakış açısı, sadece mevcut iş süreçlerini blokzincirine uyarlamaktan ibaret olmamalı. Çok daha radikal bir yol izleyip düşünce tarzımızı değiştirmemiz, blokzincirinin imkân verdiği, daha önce teknoloji elvermediği için mümkün olmayan iş yapma şekillerini tespit etmemiz gerekiyor.

Değiştirilemez yapısı, sağladığı şeffaflık ile bilginin doğruluğunu garanti altına alan blokzinciri teknolojisi, önümüzdeki dönemde gündemin üst sıralarındaki yerini korumaya devam edecektir. Finans alanında uluslararası para transferi, ticaret finansmanı, dijital kimlik gibi kullanım alanlarında mesafe kat eden teknoloji, içinde bulunduğumuz dönemde oldukça popüler olan teknoloji şirketleri öncülüğünde hayata geçirilmesi planlanan dijital paraların ve merkez bankalarının dijital para çalışmalarının da temelini oluşturuyor. Biz de hayata geçirdiğimiz blokzinciri inisiyatiflerini çeşitlendirmek için çalışmaya, öğrendiklerimizle hazırladığımız raporları ve Prof. Dr. Cem Say'ın bu eseri gibi paylaşmaya değer bulduğumuz kaliteli içerikleri sizlerle buluşturmaya devam edeceğiz.

BKM

BANKALARARASI
KART MERKEZİ