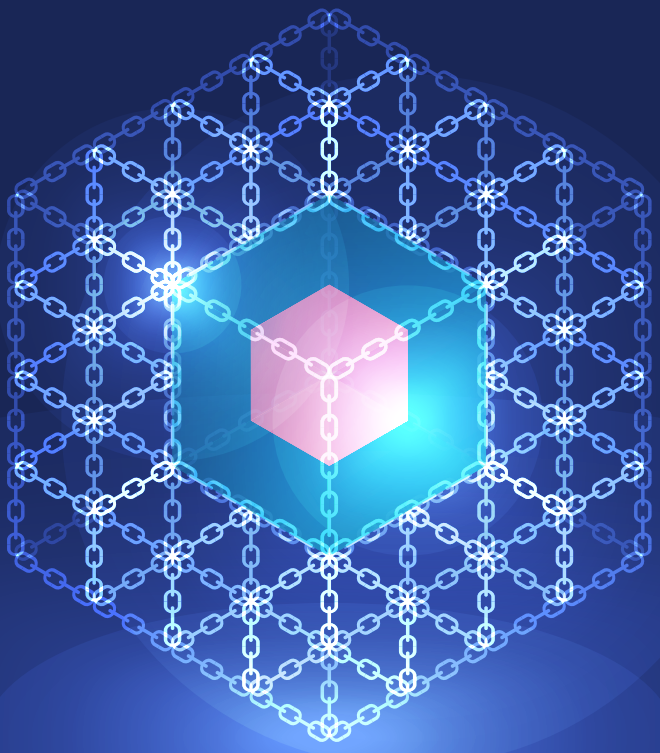
GÜNCELLENMİŞ
v2
VERSİYON



BLOCKCHAIN 101

AHMET USTA

SERKAN DOĞANTEKİN

BKM
BANKALARARASI
KART MERKEZİ

BLOCKCHAIN 101 v2

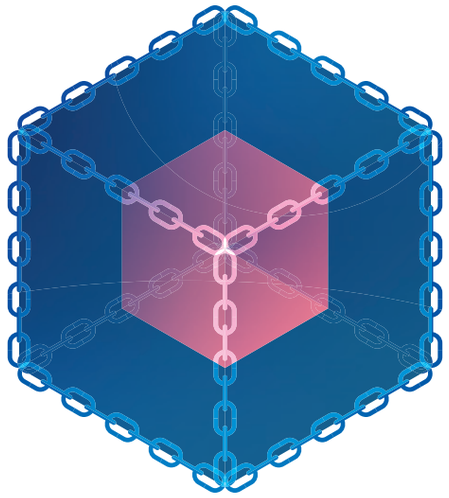
AHMET USTA
SERKAN DOĞANTEKİN

BKM
BANKALARARASI
KART MERKEZİ

İÇİNDEKİLER

BÖLÜM II / BLOCKCHAIN 201: TEKNİK DETAYLAR

BÖLÜM III / BLOCKCHAIN 201: BLOCKCHAIN'İN ÖTESİ



SUNUŞ

Yaşamın temeline baktığımız zaman değişimi görüyoruz. Doğa bu değişimi DNA kodlarına işleyerek yeni nesillere aktarırken, nesiller kendi içinde yaşam döngülerine sahip. Bu döngüler üretim ve tüketim dengesini sağlamak ve bu denge içinde arz ve talep yaratarak üretkenliği körüklemek üzere çalışıyor. İnsanın ruhu yeniliği arzuluyor, bu arzu sahip olma gayreti ile bizleri daha çok çalışmaya itiyor.

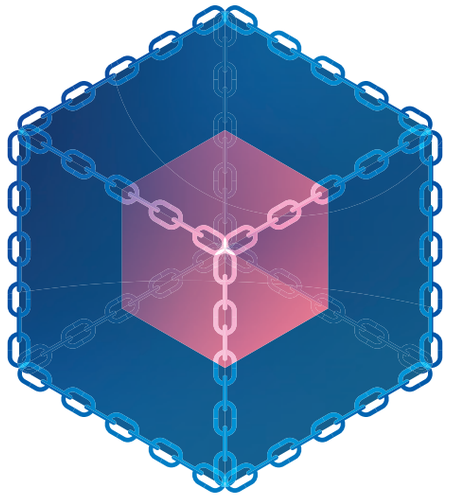
Bugün işletmelerin ve bireylerin, kendilerini yenileyemedikleri bir dünyada var olma mücadelesinde kaybetmeye mahkum olduklarını kesinlikle biliyoruz. Bu yenilenme sürecini, sadece bir topluluğa, bir sektöre hatta gezegenimizin kendisine bile atfedeceğimiz bir zaman dilimindeyiz. Değişimi izlemeli, takip etmeli, kovalamalı, yakalamalı ve tetiklemeliyiz.

Yenilikçi bir teknoloji olarak Blockchain kavramının bugününü, 1990'lı yıllarda internet kavramının bulunduğu noktaya benzetmek yanlış olmaz. Daha farklı bir ifadeyle Blockchain teknolojisinin, gelecek 25 yılda tüm dünyayı derinden etkileyecek ve en az internetin geleneksel iş dünyasına etkisi kadar yenilikçi modelleri ile iş dünyasını tekrardan dönüştürecek bir teknoloji olduğunu söyleyebiliriz.

Bankalararası Kart Merkezi olarak, Blockchain gibi devrimsel bir teknolojiye ait temel kavramları sadece kendi bünyemizde gerçekleştirdiğimiz araştırma, inceleme ve uygulamalar ile sınırlı kalmayarak; çok yönlü şekilde ele alan, yalın bir dil ve örnekler ile aktaran böyle bir eseri okuyucular ile buluşturduğumuz için çok mutluyuz ve gururluyuz.

Kendimize, ülkemize ve insanımıza inanıyoruz. Çok çalışıyoruz ve şüphesiz ki kendimize belirlediğimiz hedeflerimizde başarılı olacağız.

Dr. SONER CANKO
Bankalararası Kart Merkezi
Genel Müdür



ÖNSÖZ

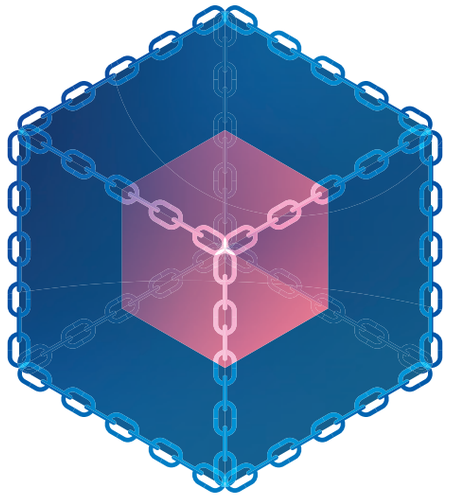
Elinizde tuttuğunuz (veya bir ekranda PDF olarak görüntülediğiniz) bu kitabın temelleri, FinTech İstanbul organizasyonunun kurulduğu 2016 yılına dayanıyor. Blockchain teknolojisi ile alakalı pek çok haberi, kavramı ve makaleyi paylaştığımız FinTechIstanbul.org sitesinde biriken içeriklerin bir araya gelmesi, bu kitabın harcını ve tuğlalarını oluşturdu. Ancak bu temel yapıtaşlarının bir binaya dönüşmesi çok ciddi ince işçilik ve pek çok kişinin katkısı ile mümkün oldu.

Kendisiyle dijital ortamda tanıştığım ve ilk kitabın baskısı elimize geçene dek yüz yüze hiç görüşmediğim Sevgili Serkan Doğantekin'in teknik veriler için altına girdiği büyük yük, Bankalararası Kart Merkezi Genel Müdür Yardımcısı Celal Cündoğlu'nun gösterdiği yol ve bizzat inşaatın içine girerek emek vermesi, Prof. Dr. Selim Yazıcı'nın akademik yönlendirmeleri ve bu kitabın tüm revizyonlarında emeği geçen daha pek çok kişinin bu kitabın oluşumuna katkısı oldu. Elbette tüm bu sürecin tetikleyicisi, motivasyon sağlayıcısı ve destekleyicisi BKM Genel Müdürü Dr. Soner Canko'nun azmi ve ısrarı olmasa, belki de bu yükün altından kalkmak mümkün olmazdı.

Bu ikinci ve genişletilmiş baskı, bir yıldan kısa bir sürede ne denli çok gelişmenin olduğunu bir kere daha bizlere gösterdi. Artık kitabın, bu versiyonundan başlayarak "yeni baskı" uğraşının ötesine geçmesini, kitabın dijital kopyasının sürekli olarak güncellenmesini hedefliyoruz.

Bu süreçte emeği geçen tüm paydaşlara ve bensiz geçirdikleri süre boyunca gösterdikleri hoşgörünün yanı sıra tüm huysuzluklarıma da sabırla katlanmaları sebebiyle sevgili eşime ve çocuklarıma, tekrar teşekkür ediyorum.

AHMET USTA



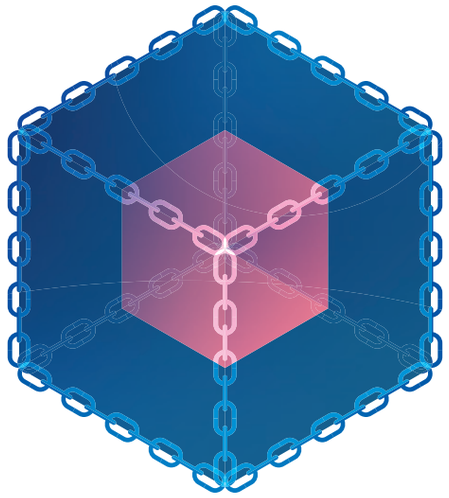
ÖNSÖZ

90'lı yılların ilk yarısında William Gibson'ın Neuromancer adlı kitabını okuyup "Gelecekteki dünya böyle olmalı" diyen bir çocuk olarak, son 20 yılda gerçekleşen bilişim tabanlı devrimler ve bunların dünyayı baştan aşağı değiştiren etkileri, benim için her seferinde bir nevi rüyaların gerçekleşmesi etkisi uyandırıyor. Blockchain devrimi bu zincirin şimdilik son halkalarından biri ve belki de içerdiği potansiyel nedeni ile uzun süreden bu yana en heyecan verici olanı.

İşte bu heyecanı, giriş seviyesinde olsa da bu kitap sayesinde mümkün olduğunca geniş bir kitle ile paylaşmayı, denize ufak bir taş atarak dalgalar yaratmayı, yeni düşünce fırtınalarına vesile olmayı, deneysel de olsa yaratıcı çalışmaları tetiklemeyi hedefledik. Bu süreçte desteklerini her zaman sunan sayın Dr. Soner Canko'ya, Bankalararası Kart Merkezi'ne, Fintech Istanbul ekibine, kitabı birlikte kaleme aldığımız sevgili Ahmet Usta'ya ve bıkkınlık yarattığım o çekilmez anlarımda dahi pozitif enerjilerini benden esirgemeyen hayatımdaki o sevgili kişilere içten teşekkürlerimi sunmak istiyorum.

Bu kitap üzerinde çalışmak benim için çok keyifli ve öğretici bir deneyim oldu, umarım siz okuyucular da hem bu kitabı okurken hem de sonrasında, Blockchain'in açtığı yeni dünyada yeni kıtalara doğru yelken açarken benzer duygular içinde olursunuz.

SERKAN DOĞANTEKİN



GİRİŞ

Modern temelleri 15. Yüzyılda Medici ailesi tarafından Floransa'da atılan bankacılık sektörü, 600 yılı aşkın bir süre boyunca sadece ürünlerini geliştirmekle kalmadı, aynı zamanda müşterilerine karşı güçlü bir güven yapısı da oluşturdu. Ancak 2008 yılında başlayan küresel kriz, gayet köklü yapılar üzerine kurulu olduğuna inanılan bankacılık ve finans sektörüne yönelik tüketici bakış açısında önemli bir değişime neden oldu. Tüketiciler, bankacılık ve finans sektörünün yanı sıra bu yapıları düzenleyen merkezi kurumlara karşı da ciddi bir güven kaybı yaşadılar. Kendilerine satılan finansal ürünleri ve hizmetleri yeterince denetlemediği ve düzenlemediği için küresel merkez bankalarını suçlayan tüketiciler, bankacılık sisteminde yatırım yapmaya yönelik inançlarını büyük ölçüde yitirdiler.

2008 finansal krizini tetikleyen Lehman Brothers'ın iflası, aynı yılın Eylül ayında gerçekleşmişti. Bu olaydan sadece iki ay sonra, bugün dahi gerçek kimliği belirsizliğini sürdüren ve "Satoshi Nakamoto" takma adını kullanan bir kişi (veya bir grup) "Bitcoin: Eşten Eşe Elektronik Nakit Ödeme Sistemi" başlıklı teknik bir çalışma yayınladı.

Bitcoin, hiçbir merkezi sisteme bağlı olmadan çalışabilen, kullanıcılarının ve dışarıdan kişilerin manipülasyona yönelik müdahalelerine karşı gerekli önlemlerin alındığı, dijital bir para birimi olarak bizlere sunuldu. Bu sistem, altında yatan güçlü şifreleme (kriptografi) teknikleri ile mutabakat üzerine kurulu şekilde veriyi kayıt altına alıyor, kaydedilen veriyi tek bir merkez yerine tüm kullanıcılarına birer kopyasını dağıtarak saklıyordu. Nakamoto'nun makalesinde Blockchain kelimesi hiç geçmese de, uygulanan yöntemler ve makalede yer verilen çeşitli şemalar sebebiyle Blockchain kavramı doğdu ve hızla gelişerek küresel ölçüde kabul gördüğü temel bir teknolojik kavrama dönüşmeyi başardı. Aklımıza gelebilecek her dijital veri kaydının bir kopyasının çıkartılması sadece zaman problemi iken Blockchain teknolojisi bu duruma tümüyle yeni bir bakış açısı getiriyordu.

Temel olarak Blockchain teknolojisi, verinin kopyasının çıkartılmasına engel değil. Ancak, kurulan dağıtık veri defteri sistemi dahilinde bu tarz kopyaların barınmasına izin vermiyor. Dolayısıyla, Blockchain platformları kendi içinde dijital enflasyon sorununu ortadan kaldırıyor. Bu durum, öncelikle kripto para adını verdiğimiz uygulamaların hayata geçirilmesini mümkün hale getiriyor.

Blockchain teknolojisini bizlere sunan ve ispatlayan Bitcoin, yapısı itibariyle geleneksel finans dünyasına karşı anarşist bir oluşum iken, bankacılık sisteminin içinden geçtiği büyük kriz, bu yeni oluşumun beyaz atlı prense dönüşmesi için gereken süreyi kısaltmış bulunuyor.

Burada okuyucularımız için belirtmemiz gereken önemli bir husus; Blockchain teknolojisine ait kavramsal temel ve bileşenlerin, sadece Satoshi Nakamoto'nun makalesine özgü olmadığıdır. Bu bileşenler, ilk olarak 90'lı yıllarda kaleme alınan, aşağıda belirttiğimiz üç farklı makale ile karşımıza çıkmaktadır:

- ✔ Stuart Haber ve W. Scott Stornetta tarafından hazırlanan 1991 yılına ait makalede[1], belgelerin zaman damgası ile birlikte kripto imzalarla nasıl kullanılacağı anlatılmaktadır.
- ✔ Ross Anderson'ın hazırladığı 1996 yılına ait bir makalede[2] ise, kaydedilen güncellemelerin silinemeyeceği, merkezi olmayan bir veri depolama sistemi tanımlanır.
- ✔ Bruce Schneier ve John Kelsey tarafından hazırlanan 1998 yılına ait bir makale[3] ise, güvenilmeyen makineler üzerinde tutulan günlük dosyalarının (log files) içerdiği hassas bilgilerin korunması için şifrelemenin nasıl kullanılacağını açıklar.

---

1 *"How to Time-Stamp a Digital Document", Stuart Haber, and W. Scott Stornetta, In Advances in Cryptology – Crypto '90, pp. 437–455. Lecture Notes in Computer Science v. 537, Springer-Verlag, Berlin 1991.*

2 *"The Eternity Service", Ross J. Anderson. Pragocrypt 1996.*

3 *"Cryptographic Support for Secure Logs on Untrusted Machines", Bruce Schneier, and John Kelsey, in The Seventh USENIX Security Symposium Proceedings, pp. 53–62. USENIX Press, January 1998.*

Teknik dünyadan uzak bir okuyucu için bu makalelerde bahsi geçen kavramların kafa karıştırıcı olabileceğinin farkındayız. Depolama sistemleri, veri, veri tabanları ve kriptografi gibi Blockchain teknolojisinin temellerini oluşturan ve herkesin aşina olmak zorunda olmadığı kavramlar ile karşı karşıyayız. Bu sebeple Blockchain kavramını anlatmaya devam etmeden önce, tarihsel gelişimleri ile birlikte Blockchain teknolojisini daha iyi anlamamıza imkân sağlayacak kavramları ilk bölümde ele alacağız. Bu bölümün ilerleyen sayfalarında teknik detaylara girmeden Blockchain platformları, uygulama alanları, uygulama örnekleri ve temelinde Blockchain teknolojisini barındıran ICO gibi konulara değinip, ikinci bölümde ise teknik detaylara yakından göz atacağız.

Kitabımızın içinde pek çok kavramın tekrar edildiğini görebilirsiniz. Bunlar, okuyucumuzun hafızasına güvenmediğimizden değil, sık tekrarlar ile konuların pekişeceğine olan inancımızdan kaynaklanmaktadır.

Kitabımızın bu yeni baskısında, birincisinde olduğu gibi Bitcoin ve diğer kripto para birimlerinin on yıla yakın macerasını değil, bunların altında yatan ve yetenekleri ile çok daha geniş olanaklar sunan Blockchain teknolojisini anlatmaya çalışacağız.

Son yıllarda giderek gündemi işgal eden bu teknolojinin popülerliğine rağmen henüz yolun çok başında olduğunu söylemek zorundayız. Bundan 20 sene önce interneti anlatan bir kitap yazmış olsak, kullanacağımız cümle yapıları bugün Blockchain için yazdıklarımızdan çok farklı olmayacaktı. Dolayısıyla Blockchain teknolojisini, bu teknoloji ile birlikte ortaya çıkan Bitcoin gibi kripto para birimlerini, akıllı sözleşmeleri, dijital kimlik çözümlerini, şimdiden anlamaya ve üzerinde kafa yormaya başlamamız gerekiyor. Bu kitabın amacı, sizlere Türkçe olarak kaleme alınmış ve Blockchain teknolojisine kapı açan temel bir rehber sunmak. İnternetin son çeyrek yüzyılda ticaret, iletişim ve dünyayı nasıl değiştirdiğini göz önüne alarak, Blockchain teknolojisinin de benzer bir maceranın temellerini oluşturduğunu vurgulamak istiyoruz.

Kitabımızın bu ikinci ve genişletilmiş bakısında, bu maceraya daha detaylı bakmak üzere yeniden yolculuğumuza başlayabiliriz.

BÖLÜM I

BLOCKCHAIN 101: BLOCKCHAIN'İ ANLAMAK

Bölüm I

BLOCKCHAIN 101: BLOCKCHAIN'İ ANLAMAK

1.1. Temel Kavramlar

Blockchain teknolojisini anlamak için bazı temel kavramlar konusunda kafamızda soru işaretleri kalmaması gerekiyor. Bu sebeple bu bölümde Veri, Veri Tabanları, Ağ Teknolojileri ve Kriptografi gibi kavramların kısaca tarihsel gelişimlerine ve günümüzdeki modern karşılıklarına göz atacağız.

Eğer bu kavramlar konusunda bilgilerinize güveniyorsanız bu bölümü atlayarak zaman kazanabilirsiniz. Ancak satır aralarında dikkatinizi çekecek bilgileri kaçırmamak adına okumanızı tavsiye ederiz. Başlayalım;

Veri Nedir?

İngilizce ve Latince dillerinde aynı kelime olarak karşımıza çıkan ve artık günlük yaşamda da dilimizde normalleşmeye başlayan "data" kelimesinin Türkçe karşılığıdır. İşlenmemiş, ham bilgi parçacığına verilen isimdir.

Wikipedia'da yer alan açıklamalar ile ilerleyecek olursak veriler; ölçüm, sayım, deney, gözlem ya da araştırma yolu ile elde edilmektedir. Ölçüm ya da sayım yolu ile toplanan ve sayısal bir değer bildiren veriler **nicel veriler**, sayısal bir değer bildirmeyen veriler de **nitel veriler** olarak sınıflandırılmaktadır. Her sembolik gösterim gibi, veri de belirli bir nesne, birey ya da olguya ilişkin bir soyut ifadeler kümesidir.

Bir verinin tek başına bir anlamı ve işlevi bulunmaz. Veriler toplandıktan sonra gruplanarak, sıralanarak ve özetlenerek, elle ya da bilgisayarla işlenip enformasyona dönüştürüldüklerinde anlam kazanırlar. Böylece,

ait oldukları unsuru açıklama gücüne kavuşur ve problem çözme ya da karar verme gibi bir amaca hizmet edebilecek duruma gelirler.[4]

Kayıtlı olmayan verileri ise konuşma esnasında aktarılan kelimeler, müzik notaları veya bir deniz fenerinden görsel olarak iletilen mesajlar olarak ele alabiliriz. Bu tarz veriler vericisi ile alıcısı arasında transfer edildikten sonra varlıklarını kaybetmektedirler.

Düşünülenin aksine veri sadece insanlar tarafından üretilmez. Kayıt altına alamadığımız güneş patlamalarından kaynaklanan kozmik ışınlar ve atomların etrafında dönen elektronlar gibi milyonlarca farklı veri evrende sürekli olarak üretilmektedir. Bundan daha ilginç olanı ise hayatın temelini oluşturan genetik kodlamalar yani DNA insanlığın elinden çıkmamış, hücreler arasında kopyalanarak çoğaltılabilen ve belirli şartlar altında vericisi ve alıcısı arasında transfer edilerek yeniden oluşturulan en temel veri kayıtları arasında yer alır.

İnsanlık tarihine ait bulunabilmiş en eski kayıtlı veri, M.Ö 12 binli yıllarda bir maymun kemiğinin üzerine atılan çentiklerdir. Günümüze kadar ulaşmayı başaran bu örnek, Afrika'nın aynı isimli bölgesinde bulunduğu için Ishango kemiği olarak isimlendirilmiştir. Ishango kemiği, bugün Belçika Kraliyet Doğa Bilimleri Enstitüsünde koruma altında sergilenmeye devam ediyor.

Yazının keşfedilmesi ile birlikte veri kayıtlarının hızla arttığına ve insanlar arasında aktarılan bilgi miktarının çoğaldığına şahit oluyoruz.

Günümüzün modern veri merkezlerinin atası kabul edilebilecek büyük bir kütüphanenin ise ilk olarak M.Ö. 330 yılları civarında Büyük İskender tarafından kurulduğunu biliyoruz. Bünyesinde 150 bini aşkın ciltten oluşan, toplamda 900 binden fazla el yazması eserin yer aldığı bu kadim kütüphane, maalesef 391 yılında yakılarak yok edilmiştir.

Uzun yıllar boyunca el yazmaları şeklinde kaydedilen veriler, 593 yılında Çin'de tahta oyma yöntemi ile geliştirilen ilk matbaa aracılığı ile daha hızlı çoğaltılabilir hale gelmiştir. Metal harfler kullanan ilk modern matbaa ise 1450 yılında

[4] *https://tr.wikipedia.org/wiki/Veri*

Almanya'da Johannes Gutenberg tarafından geliştirilmiştir.

Verinin insanların kontrolünde makine diline dönüşmesi ise 1801 yılında Fransız bir mucit olan Joseph Jacquard'ın karton plakalar üzerinde delikler açması ile gerçekleşir.

Jacquard tarafından icat edilen delikli kart metodu 1832 yılında Rusya'da Semen Korsakov tarafından, verinin depolanması ve hızlı şekilde bulunması için, Homeoskop adı verilen bir cihaza dönüştürülmüştür.

Delikli kartlar ile verinin işlenmesi, 1950'li yıllara kadar popülerliğini korumuş bir yöntemdir. NASA ilk insanlı uzay uçuşunun temellerini oluşturacak hesaplamaların bir kısmını delikli kartlar ile programlanan bilgisayarlar aracılığı ile gerçekleştirmiştir. Ancak, delikli kartların çok fazla yer kaplaması nedeniyle alternatiflerin aranmasına başlanmış ve ilk olarak 1950 yılında, UNITYPER isimli ABD merkezli bir şirket tarafından, bilgisayarlar için manyetik depolama sistemi geliştirilmiştir. Manyetik depolama sistemleri, uzun yıllar boyunca finans ve bankacılık sektöründe de kullanılan UNIVAC bilgisayar sistemlerinin en önemli bileşeni olmuştur.

Manyetik şeritlerde veri depolama teknolojisinin 1951 yılında UNIVAC ile birlikte ticari olarak bilgisayar dünyasıyla buluşmasının ardından, IBM 1960 yılında, ilk 8 inç büyüklüğündeki disketi (Floppy Disk) geliştirmiştir. Bu dönemden sonra çok farklı standartlarda disketler üretilmiştir.

1990'lı yıllarda CD teknolojisinin hayatımıza girmesi ile birlikte manyetik diskler yerlerini optik depolama ünitelerine bırakmış, 1995 yılından itibaren ticari CD kaydedici cihazlar ofis ve evlere girmeye başlamıştır. Bu geçiş döneminde disketlerde 1,44 MB gibi kapasiteler konuşulurken, CD'ler ile birlikte bu miktar 600 MB'ın üstüne çıkmış ve dijital depolamasında devrim niteliğinde bir adım atılmıştır.

90'lı yılların sonuna doğru popüler hale gelmeye başlayan bir diğer teknoloji ise Evrensel Seri Yolu (USB) üzerinden bilgisayarlarımıza bağlanan flash bellekler olmuştur.

90'ların sonundan 2000'li yılların ortalarına kadar önce disk başına 4,7 GB veri depolayan DVD ve sonrasında çok daha yüksek kapasitelere sahip Blu-ray optik diskler hayatımıza girse de USB teknolojisinin yeni versiyonları ve kapasitesi sürekli büyüyen flash bellekler ile birlikte 2010 ve sonrasında artık bilgisayarlardaki optik disk sürücüler bir standart olmaktan çıkmıştır. İnternetin de yaygınlaşmasıyla daha yüksek kapasiteye sahip dahili sürücüleri, USB 3.0 ve üstü bağlantı standardına sahip veya ağ üzerinden kullanılabilen harici disk üniteleri tamamlar hale gelmiştir.

2005 ve sonrasında hayatımıza giren bir diğer önemli veri depolama aracı ise Bulut (Cloud) kavramı ile internet üzerinden sunulan servisler olmuştur. 2006 yılında Amazon Web Servisleri (AWS) tüketicilere sunulmuştur. Bu servisleri kullanarak hızla popüler hale gelen bulut depolama çözümü Dropbox servisi ise 2007 yılında hizmete girmiştir.

2010 yılından itibaren, hiçbir fiziksel bileşen içermeyen SSD (solid state disk) depolama teknolojisi, bilgisayarlarda önemli bir yer edinmeye başlamıştır. Günümüzde bulut servisleri teknolojik ürünlerin vazgeçilmez standart parçaları haline gelmiştir.

Veri Tabanları

Veri kavramını ele aldığımız geçen bölümde, doğanın ürettiği verilerden başlayarak, insanlığın günümüzün en modern veri depolama sistemlerini geliştirmesine dek geçen süreci hızlıca gözden geçirdik. Elimizdeki veriye, bu veri ile üretilmiş bilgiye ve bunları saklayacak ortamlara artık yabancı değiliz.

Bu sefer, veriyi depolarken kullandığımız metodoloji ve sistemlere yakından bakacağız ve geçen bölümde bahsettiğimiz delikli kartların bir veri tabanı olarak kullanılmasını ele alarak hikayemize devam edeceğiz.

Delikli kartlar, veriyi depolamak kadar organize şekilde saklamak için de kullanılan bir yöntemdi. Pek çok farklı delikli kart, üzerlerinde saklı olan verilerin amacına uygun şekilde kullanılabilmesi için düzenli şekilde

dolaplarda saklanıyordu. Amaçları farklı olsa da günün sonunda veri kümeleri organize bir şekilde saklanıyordu.

1950'li yıllardan itibaren analog, manyetik ve sonrasında dijital veri saklama yöntemleri geliştikçe verinin daha düzenli şekilde saklanmasına olan ihtiyaç artmaya başladı. Bu sebeple kökeni yüzlerce yıl öncesine dayanan kütüphanecilik ve arşivcilik teknikleri bilgisayar sistemleri ile buluşmaya ve şekil değiştirerek modernleşmeye başladı.

"Database", yani Türkçe karşılığı ile "veri tabanı" kavramı bilgisayar sistemleri için ilk olarak 1960'lı yıllarda kullanılmaya başlandı. Bu alandaki ilk modern uygulama, aya gitmek üzere tasarlanan Saturn V roketine ait parçaların listelendiği ve kaydedildiği veri tabanı sistemi olarak karşımıza çıkıyor.

1970'lere gelene kadar, aslında veri tabanı olarak adlandırılan tüm sistemlerin, temelde bugün salt metin içerikler oluşturmak için kullandığımız not defteri uygulamalarına benzediğini görüyoruz. 1973 yılında IBM San Jose Araştırma Laboratuvarında çalışan Edgar Codd, devrimsel sayılabilecek bir kavramı, "İlişkisel Veri Tabanı" tanımını ortaya koymuştur.[5] Codd, kurum içinde gerçekleştirdiği sunumda bu tanımı yaparken şöyle bir ifade kullanmıştır: ***"Gelecekte büyük veri kümeleri ile çalışacak kullanıcıların, makinelerin bu veriyi nasıl sakladığı konusunda bilgi sahibi olmasına gerek olmamalıdır."***

İlişkisel veri tabanları, veriyi tablolarda saklar ve bu tablolar arasındaki bağlantıları oluşturur. Kullanıcılar verilerin nasıl saklandığı ile değil, kendilerine nasıl sunulduğu ile ilgilenirler. Veri tabanında kayıtlı verilerin sorgulanması için yine Edgar Codd tarafından geliştirilen SQL[6] dili kullanılır. SQL ,1980'li yıllardan itibaren bir veri tabanı sorgulama standartına dönüşmüştür.

1980'li yıllarda kişisel bilgisayarların yaygınlaşmaya başlaması ile hayatımıza giren bir diğer düzenli veri depolama çözümü ise 90'lı yıllarda Hesap Tablosu olarak da isimlendirilen Tablolama Uygulamaları olmuştur. İlk olarak Lotus 1-2-3 olarak

[5] *http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/reldb/*
[6] *SQL: Structured Query Language – Yapılandırılmış Sorgulama Dili*

karşımıza çıkan tablolama çözümleri, ilerleyen yıllarda Microsoft'un geliştirdiği MS Office ürün ailesi içinde yer alan Excel ile birlikte, temel eğitimden en kompleks şirketlerin finans ve muhasebe servislerine kadar her alanda kullanılan bir çözüme dönüşmüştür.

Tablolama uygulamalarının sınırlı veri depolama ve analiz çözümleri olduğu gözden kaçmamalıdır. Günümüzde devasa veri tabanları trilyonlarca satır veri içerebilir ve boyutları Petabyte düzeyinde olabilir.

2000'li yıllardan itibaren kullanılmaya başlayan bir diğer veri tabanı çözümü ise NoSQL olarak tabir edilen çözümler olmuştur. Bu veri tabanları, ilişkisel tablolar yerine sabit yapıda tekil şemalar içerirler ve bu sayede çok büyük veri kümeleri içinde çok hızlı arama yapmaya imkan tanırlar. Örneğin, Google arama motorunda bu tarz bir veri tabanı kullanılır ve bu sayede milyarlarca web sayfası içinde aradığınız bir veya daha fazla kavram için milisaniyeler içinde sonuç almanız mümkün olur.

Bir önceki bölümde ele aldığımız depolama amaçlı kullanılan bulut servisleri, aynı zamanda veri tabanı hizmetleri için de sunulmaktadır. Örneğin Amazon, bu konuda kendi ürünleri olan RDS, DynamoDB, Redshift gibi farklı çözümler sunmaktadır.

Artık, donanımın uygulamalara ve uygulamaların servislere dönüştüğü bir dönemden geçiyoruz. Bu sebeple bulut çözümleri eşsiz bir maliyet avantajı ile ihtiyaç duyduğumuz altyapıları bize sağlıyor. Ancak bu, teknolojik gelişmenin son noktası değil. Ötesi de var.

Sonsuzluk ve Ötesi[7]

Şehir ışıkları ile kirlenmemiş açık bir gökyüzüne bakacak olursanız, yıldızların sayısı karşısında hayranlık duymamanız mümkün değil. Oysa şu ana kadar gözlemlediğimiz yıldızların sayısı tüm evrenin çok ufak bir parçasını oluşturuyor.

[7] *Disney Pixar'a ait Toy Story animasyon dizisindeki Buzz Lightyear isimli astronot karakterin sloganı.*

Bugün internete bağlanan cihaz sayısı insan nüfusunu geçti. Nesnelerin İnterneti (IoT - Internet of Things) adı verilen bu yapı katlanarak büyürken, oluşturduğu ekonomi trilyonlarca dolar olarak kabul ediliyor. Bütün bu sistem tarafından üretilen verinin dağıtık şekilde kaydedilmesi ve saklanması mümkün olabilir mi?

Aslında bu sorunun cevabı uzun yıllar önce verilmişti. 2000'lerin başında birbirinden bağımsız iki proje olarak karşımıza çıkan eDonkey ve BitTorrent, tam olarak internet üzerinde hiç tanımadığımız ama iletişime geçebileceğimiz diğer kişiler, daha doğrusu makineler üzerinden verinin paylaşılması için geliştirilmiş, uçtan uca "Peer To Peer - P2P" olarak isimlendirilen bir tür veri depolama çözümü olarak karşımıza çıktılar.

Bu sitemlerde veri, tek bir merkezde değil sayısı milyonları bulabilecek makineler üzerinde dağıtılmış veya paylaşılmış şekilde bulunur. Bu makinelerden bazıları verinin tamamını, bazıları ise kısmen belli bir parçasını içerebilir. Ulaşmak istediğinizde sistem size bu veriyi, sunulabilecek en hızlı düzenlemeyle, farklı makinelerden çekecek şekilde yönlendirir. Siz veriyi kendi bilgisayarınıza çekerken, aldığınız veri karşılığında aynı zamanda diğer kullanıcılara bir veri kaynağı olarak hizmet edersiniz. Sistemin kullanıcıları, sisteme verdikleri destek süreci ile doğru orantılı olarak sistemden faydalanabilirler. Bu platformlar, bulutun ötesinde bir çözüm sunmakla birlikte, içeriğin şifrelenmemesi, verinin nerelerde saklanacağına dair seçenek sunmaması gibi nedenlerden dolayı, kurumsal veya mahremiyet içeren kişisel veriler için güvenli bir depolama çözümü değildir.

Bu yaklaşım ile Dağıtık Kayıt Defterleri (Distributed Ledger Systems) adı verilen çözümler ortaya çıkmıştır ve kitabımızın ana konusu olan Blockchain teknolojisi de bu çözümün farklı bir uygulaması olarak değerlendirilebilir.

Ağ Teknolojilerinin Kısa Tarihi

Teknoloji sayesinde artık yüz yıllık zaman dilimleri daha hızlı geçiyor. Bizler daha kısa zamanda daha çok şey yapmamıza rağmen! Bugün iletişimde önemli bir rol oynayan kablosuz iletişim teknolojilerinin, aslında milyonlarca yıldır doğal ekosistemin temel taşlarından birisini oluşturması, belki de bu bölümün en ilginç bilgilerinden birisi olabilir.

Bitkilerin tamamına yakını nesillerini devam ettirmek için kablosuz iletişim teknolojisini milyonlarca yıldır kullanıyor. En eski veri kayıtlarından birisi olan DNA'nın kablosuz şekilde iletilmesi için çiçekler polenlere ve diğer bitkiler çekirdeklere sahiptir.

İnsanoğlunun modern iletişim teknolojilerini kullanmaya başlaması, elektriğin keşfi sayesinde hayatımıza girmeye başlamıştır. ABD'li Joseph Henry, 1830 yılında ilk kez elektromıknatıs kullanarak, uzaktan zil çalan bir sistem icat etti. ABD'li ressam Samuel Morse, 1835 yılında ilk kez elektro mıknatıslı telgrafı geliştirdi ve aynı zamanda tüm dünyada kabul gören Mors alfabesini oluşturdu.

İnsanların birbiri ile sesli olarak uzaktan konuşması içinse yaklaşık 40 yıl geçmesi gerekti. 1880 yılında Alexander Graham Bell ve Charles Sumner Tainter, radyofon isimli aygıtı geliştirdi.

1930 yılının sonuna doğru Almanya'da, metin transferine izin veren, Telex adında yeni bir iletişim teknolojisi geliştirildi.

1949, modern anlamdaki MODEM'in ilk geliştirildiği yıl oldu. 1958 yılına kadar sadece kısıtlı ve askeri projelerde kullanılan MODEM teknolojisi, ilk olarak Bell Telekom tarafından ticarileştirildi. 1958 yılı aynı zamanda telefon ağlarının da ilk kez dijitalleşmeye başladığı sene oldu.

1960 yılında, günümüzün istemci-sunucu (client-server) yapısının temelleri atıldı ve IBM, 1964 yılında ABD hava yolu şirketleri için SABRE adında bir ağ oluşturarak, 65 şehirdeki 2 bin terminali birbirine bağladı.

1969 yılında, ABD ordusu için geliştirilen ARPAnet, aynı anda farklı

bilgisayarların bağlanabildiği ilk ağ olarak tasarlandı ve bugün kullandığımız internetin temelleri de aynı yıllarda atıldı.

1973 yılında, Xerox'da çalışan iki mühendis, Robert Metcalfe ve Dave Boggs, Ethernet teknolojisini geliştirerek, bugün hala bir standart olan ağ teknolojisinin temellerini attı.

1982 yılında, dünyanın ilk Ağ İşletim Sistemi olan Novell NetWare piyasaya sürüldü.

1987 yılında, mobil GSM standartları oluşturuldu.

CERN'de görevli olan Tim Berners-Lee, 1990 yılında HTML (Hypertext Markup Language) dilini yayınlayarak, World Wide Web (WWW) platformunun kurulmasını sağladı.

1991 yılında National Science Foundation (NSF), Internet'i özel bir ağ olmaktan çıkartıp herkesin kullanımına açtı. 1996 yılına gelindiğinde, internet kullanıcı sayısı dünya çapında 36 milyona ulaşmıştı.

2000'li yıllar, kablosuz ağ teknolojilerinin gelişmeye başladığı ve WiFi standartlarının hayatımıza girdiği yıllar oldu. 2009 yılından sonra Mobil Web erişimi artık bir lüks olmaktan çıktı.

Günümüzde çok yüksek hızlara ulaşan iletişim ağları, Blockchain teknolojisinin hızla yaygınlaşmasını sağlayan en önemli bileşenlerden birisidir.

Kriptoloji

Son olarak, Blockchain teknolojisinin temelinde yatan ve büyük öneme sahip Kriptoloji kavramına göz atacağız.

Binlerce yıldır, üretilen veri kayıt altına alınırken ortaya çıkan en önemli ihtiyaçlardan bir tanesi, veriyi istenmeyen gözlerden saklamak olmuştur.

Kriptoloji her ne kadar kulağımıza modern bir kelime gibi gelse de aslında eski bir Yunanca kelime olan **kryptos** kelimesinden türetilmiştir. Kryptos gizlilik anlamına gelirken, kriptoloji gizlilik bilimi anlamına gelmektedir. Kriptoloji'nin bir alt bilim dalı olan Kriptografi de yine eski bir Yunaca kelime olan ve yazı anlamına gelen **graphien** sözcüğü kullanılarak türetilmiştir. **Kriptografi** (cryptography) verilerin (yazıların) şifrelenmesini ifade etmektedir.

Şifreleme, herhangi bir veri kümesini bir kural yapısı kullanarak rastgele görünen bir veri kümesine dönüştürür. Bu rastgele gibi görünen veri kümesi, ancak şifreleme yapılırken kullanılan anahtara sahip olanlar tarafından orijinal ve anlamlı haline geri dönüştürülebilir. Bu anahtara sahip olmayanlar için ise bir anlam ifade etmez. Böylece şifrelenmiş veri nerede ve ne şekilde depolanırsa depolansın, sadece anahtar sahibi tarafından anlamlı kalmaya devam eder. Bu sürecin teknik detaylarına ilerleyen bölümlerde değineceğiz.

Blockchain Teknolojisinin Felsefesi

Tarih boyunca veri kayıtlarının hizmet ettiği önemli ihtiyaçlardan birisi, büyümekte olan topluluklar içinde düzenin sağlanması olmuştur. Büyümekte olan toplumlarda, birbirini tanımayan kişi ve yapılar arasındaki ilişkilerin kurallara bağlı hale getirilmesi ve bu kuralların kayıtlara geçirilmesi her zaman büyük önem taşımıştır. Temel olarak günümüze dek kurulan pek çok organizasyon, dernek, vakıf, şirket ve hatta devletler bu kayıtları oluşturmak, düzenlemek ve işletmek için yine topluluklar ve toplumlar tarafından kurulmuştur.

2008 yılında Lehman Brothers'ın iflasından sadece iki ay sonra ortaya çıkan ve daha önce de belirttiğimiz gibi kimliği hâlâ gizliliğini koruyan Satoshi Nakamoto takma adlı kişi veya grubun yayınladığı "Bitcoin: Eşten Eşe Elektronik Nakit Ödeme Sistemi" başlıklı teknik çalışma, her ne kadar bir dizi matematiksel ve teknolojik uygulamayı bizlere sunsa da, aslında makalede verilen temel mesaj, mealen şöyledir: *"Ey insanlar! Birbirinizi tanıyın veya tanımayın, artık merkezi yapılara ihtiyaç duymadan güvenli bir veri kayıt sistemi kurmak mümkün. Bu sistem, matematik ve teknolojinin imkanlarını kullandığı için manipüle edilemez ve bozulamaz."*

Blockchain felsefesinin verdiği mesajı artık biliyoruz. Bu mesajın özünde yatan, merkezi olmayan ama güvenli veri kayıt sistemlerinin nasıl hayata geçirildiğini anlamak için, veri, veri tabanı, iletişim ağları ve kriptografi kavramları hakkında bilgiye de sahibiz. Şimdi, Blockchain teknolojisinin çalışma süreçlerine geçiş yapabiliriz. O halde "Perde Açılsın!"

1.2. Blockchain Dünyasına Giriş

Şu ana kadar üzerinden geçtiğimiz başlıkları bir bütün olarak ele almanın vakti geldi. Artık veriyi merkezi sistemlere kaydetmek zorunda değiliz, veriyi bulut servisleri gibi hizmetleri kullanarak hatta P2P gibi yapılar üzerinden dağıtarak saklamamız mümkün. Bulut ve P2P yapılarının üzerinde veri tabanları da bulunabilir. Üstelik verinin büyüklüğü pek çok noktaya dağıtılması için bir engel de teşkil etmiyor, zira çok yüksek hızlı iletişim ağlarına sahibiz. Aslında bu Blockchain dünyasına giriş için gerekli olan birinci aşamayı bizlere sunuyor.

Aşama 1: Dijital Kayıtların Evrimi

Tekrarlayacak olursak; önce bir kaydın tek bir kopyasına sahiptik, daha sonra bu kaydı birkaç bilgisayara dağıttık, ardından bu kaydın pek çok kopyasını pek çok bilgisayara dağıttık, nihayet her bilgisayar, -ki burada bilgisayar ifadesinin içine artık akıllı cep telefonları ve internete bağlanabilen diğer elektronik cihazlar da girmektedir-, işlemin bir kaydını tutacak hale geldi. Bunun en temel sebebi ise maliyetlerin zaman içinde ciddi şekilde düşmesiydi.

Şekil 1: **Dijital Kayıtların Evrimi**

Moore, Metcalfe, Reed hatta Bezos kanunları olarak ifade edilen yaklaşımlar, temelde bize aynı şeyi söyler: dijital teknolojilerde gelişim süreci o kadar hızlıdır ki her birkaç yıllık dönemde teknolojik ilerlemeye kıyasla maliyetler ters orantılı olarak düşüş gösterir.

Bu gelişim, bizi Şekil 1'de gördüğümüz son aşamaya; yani temel olarak verinin, ucuzlayan iletişim ağları üzerinden, pek çok sayıdaki bilgisayara dağıtılmasının pratik açıdan mümkün olduğu noktaya getiriyor. Bu noktada kayıtlarımız tüm sistemlere kopyalanmış oluyor.

Bu yaklaşıma Dağıtık Kayıt Defteri (Distributed Ledger) adı veriliyor. Bu kavramın yeni bir kavram olmadığını ve geçmişte eDonkey veya Bittorrent gibi ağlarda kullanıldığını anlatmıştık. Ancak bu ağların ortak sorunu, üzerinde tutulan verinin genellikle şifrelenmemiş olmasıdır. Bu sebeple dileyen herkes bu verilere erişebilir. Bu noktada verileri şifreleyerek (kriptografi ile) dağıtık kayıt defterlerine aktarmak mümkün olabilir. Ancak bu durumda veriyi şifreleyen kişi/taraf dışında hiç kimse bu veriden fayda göremeyecektir. Üstelik, herhangi bir şekilde ağ noktalarının birisinde veri üzerinde bir değişiklik meydana gelirse, verimiz şifrelenmiş olsa bile tutarsız durumlar ortaya çıkabilir. Bu durum bizi ikinci aşamaya taşır.

Aşama 2: Dağıtık Kayıt Defterinde Nitelikler ve Süreçler

Birden fazla tarafın bulunduğu bir sistemde, sisteme eklenmesi istenen her verinin geçerli bir standarda sahip olması beklenir. Böylece sistemin bütünlüğü korunabilecektir. Ancak, dağıtık yapılar birbirini tanımayan taraflardan oluşabileceği için, sistemin geneli tarafından kabul edilmiş kurallara bağlı bir yapı kurgulamak gerekecektir. Bu kurallar, belli bir amaca hizmet edecek sistemlerin tasarım aşamasında belirlenir ve farklı ihtiyaçlara göre değişiklik gösterebilir. Bu kurallar manzumesinin yapısına ve çalışma sürecine, her bir uygulamanın kendisine özel olmak üzere, "**mutabakat yapısı**" adını veriyoruz.

Belli bir mutabakat yapısı ile kurgulanan sistemler içinde, tüm paydaşların uyduğu kuralların işleyiş sürecine de "**mutabakat süreci**" adını veriyoruz.

Sınırlı sayıda birey bir araya geldiklerinde el sıkışarak sözlü veya yazılı bir kayıt ile bir mutabakat sağlayabilirler. Dijital bir sistem üzerinde mutabakat yapısının sağlanması için, bunun yazılım kodları kullanılarak garanti altına alınması gerekir. İşte tam bu noktada Blockchain teknolojisi ortaya çıkıyor ve diyor ki, *"Ben tüm bu sorunları çözeceğim. Baştan mutabakat yapısı (kuralları) belirlenmiş şekilde veriyi kaydetmenizi sağlayacağım. Daha sonra bu kayıtları iletişim ağları üzerinden, pek çok noktaya dağıtacağım. Bu süreç içinde verinin tüm noktalarda aynı kaldığına dair güvenilir bir mutabakat süreci sağlayacağım. Hatta bununla da kalmayacağım tüm kullanıcıların verilerini şifreleyeceği bir çözüm de sunacağım."*

Bu noktada Blockchain teknolojisi, dijital dünyada artık kolaylıkla oluşturabildiğimiz, güncellediğimiz ve hatta silebildiğimiz veri kullanım şekline farklı bir bakış açısı getiriyor; *"Ben dağıtık bir veri kayıt sistemiyim"* diyor ve ekliyor: *"Sunduğum çözümde kaydedilen bir veri sonsuza kadar değiştirilemez, böylece güvenilir bir yapı ortaya çıkar."*

Blockchain Kayıt Yapısı

Blockchain teknolojisinde veri her zaman belirli bir sıralama yaklaşımı ile kayıt altına alınır. Bunu daha iyi anlamak için kurgusal ama basit bir örnek verelim:

Elinizde üzerinde bir deliği bulunan 5 tane minik karton etiketiniz ve bir adet yeterince uzun bir ipiniz olsun. 5 arkadaşınız ile düzenlediğiniz bir parti esnasında bir oyun oynayacaksınız. Oyuna bir etiketin üzerine adınızı yazarak ve bir imza atarak başlıyorsunuz. Sonra bu etiketi ipinize geçirip, bir düğüm atıyorsunuz. Daha sonra yakın bir arkadaşınız bir diğer etikete adını yazarak imza atıyor ve aynı ipe geçirerek düğüm atıyor. Bu işlemi 5 arkadaşınızın hepsi tekrarlıyor. Artık elinizde belirli bir sıra ile ilerleyen, her birinin üstünde bir kişinin adı ve imzası bulunan etiketlerin düğümlendiği bir ipiniz var.

Şekil 2: **Etiket**

Blockchain kayıt sistemi de temelde bu örneğe benziyor. Etiketlerimizi yazdığımız isimlerimiz **veriyi** ifade eder. Verilerin belirli kurallar ile yazıldığı her bir etiket ise **Blok** adı verilen yapıları ifade eder. Her bir blok kendi özel imzasına sahiptir. Blockchain uygulamalarında imzalar, kitabımızın ikinci bölümünde detayları ile ele aldığımız özel bir matematiksel uygulama ile üretilir. İpimizin Blockchain sisteminde karşılığı ise zaman akışıdır, her bir blok oluşturulduğu anda bloğun üzerine tarih ve saat bilgilerini içeren bilgi de eklenir (ipimizde attığımız düğüm). Böylece her biri kendi imzasına sahip, belirli bir zamanda kaydı oluşturulan veri blokları sıra ile arka arkaya dizilir ve bir **blok zincirini** oluşturur. Bu yapıda ilk kayıt başlangıç bloğu olduğu için, bu bloğa özel olarak Genesis adı verilir.

Şekil 3: **İlk Blok (Genesis) kaydından sonra tüm blokların birbirini takip ettiği yapı**

Blockchain Sıra Yapısı

Etiketlerimiz ve ipimiz ile uyguladığımız örneğimiz ile yolumuza devam edelim. Bu ip üzerindeki herhangi bir etiketi aradan çıkartmak için, o etiketi yırtmanız ya da o etikete kadar tüm düğümleri çözerek o etiketi aradan çıkarttıktan sonra diğer etiketleri tekrar ipe sırayla düğümlemeniz gerekecektir. Hatta aradan çıkarttığımız etiketin yerini de değiştirebiliriz. Süreç biraz zahmetli olabilir ancak bunu başarmak mümkün. Bu tehlikeyi fark ettikten sonra, ortadan kaldırmak için, etiket zincirimizi yeni bir kural daha ekleyerek "**mutabakat yapısını**" tekrar oluşturalım ve oyunumuzu tekrar baştan oynayalım.

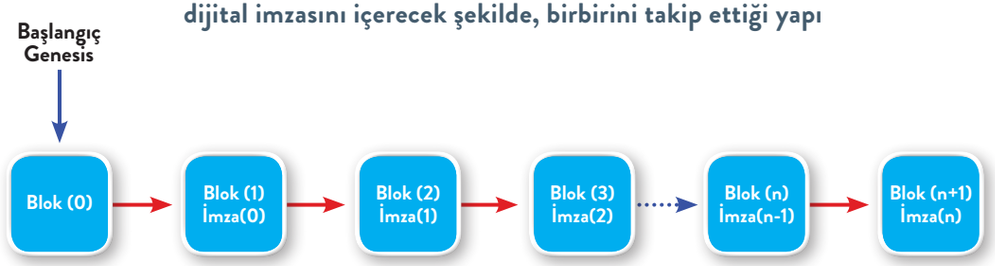
Geçen sefer olduğu gibi adımızı bir etikete yazıp, imzamızı attıktan sonra ipimize geçirip yine düğüm atıyoruz. Bu sefer bir diğer arkadaşımızın kendi adını yazıp imzasını attığı etiketin altına biz de ilk etiketin sahibi olarak kendi imzamızı atalım ve bu şekilde ipe geçirip düğüm atalım. Üçüncü sırada adını yazıp imzasını atan arkadaşımızın etiketine ise ikinci etikete adını yazan arkadaşımız imzasını atsın. Süreç bu şekilde devam ettiğinde ilk etiket hariç olmak üzere her yeni etikette o etikete adını yazıp imza atan arkadaşımız dışında, bir önceki etiketin sahibinin de imzası eklenmiş olacak.

Şekil 4: **Etiket**

Artık bu yeni yapıda, zahmetli bir şekilde ipimizdeki düğümleri açıp, aradan bir etiket çıkartsak veya yerini değiştirsek bile her bir etiket oluşturulduğu esnada kendisinden bir önceki etiketin imzasına da sahip olacağı için, etiket zincirimiz dikkatlice kontrol edildiğinde, rahatlıkla sıranın bozulduğu anlaşılabilecektir.

Blockchain yapısında da benzer bir yaklaşım kullanılır. İlk oluşturulan blok kendisinden önce bir blok olmadığı için Genesis, yani başlangıç bloğu olarak isimlendirilir ve sadece kendi dijital imzasını taşır. Ancak, ardından gelen her bir blok kendisininki ile birlikte, bir öncekinin de benzersiz imzasını içinde taşıyacaktır. Böylece, sıralı bir kayıt yapısı dijital dünyada mümkün hale gelir.

Şekil 5: **İlk Blok (Genesis) kaydından sonra tüm yeni blokların, bir önceki bloğun dijital imzasını içerecek şekilde, birbirini takip ettiği yapı**



Blockchain Dağıtık Yapısı

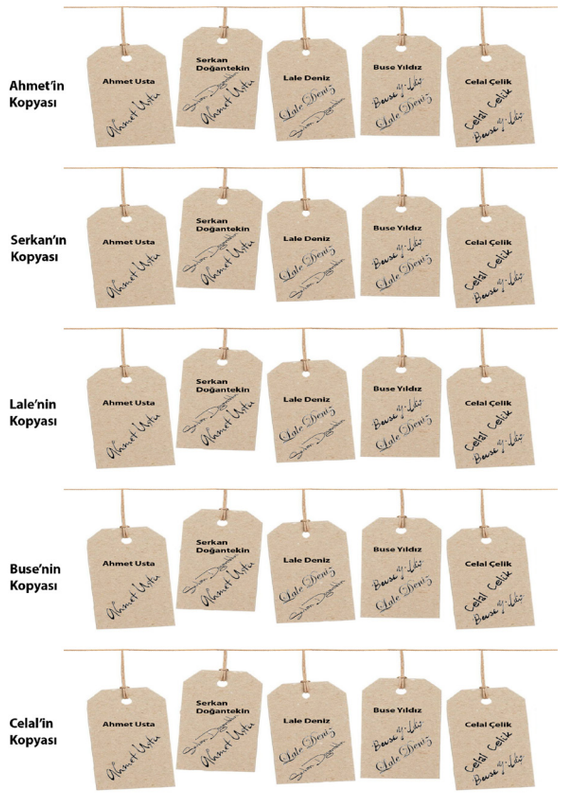
Etiket örneğimizde, arkadaşlarımız gönül rahatlığı ile eşsiz eserimizin sonsuza dek bir hatıra olarak kalacağını düşünerek evlerine gidebilirler ama son sıraya düşen arkadaşımız bu durumdan alınmıştır ve bizim çok iyi bir imza taklitçisi olduğumuzu bildiği için farklı düşünceleri olabilir :)

Teorik olarak bu olasılık imkansız değil. Özellikle dijital dünyada bir kaydın rahatlıkla kopyasının çıkartılabileceğini düşünürsek, bu sıra değiştirme işi çok daha kolay olabilir. Bu sebeple, oluşturduğumuz kayıtların yeni bir "**mutabakat süreci**" yapısına ihtiyacı var.

Neyse ki etiket oyunumuza başlarken bizim imza kopyalama yeteneğimizi bilen bir diğer arkadaşımız bu konuyu gündeme getirmiş ve "**mutabakat sürecimizi**" eşsiz bir hale dönüştürecek bir öneri yapmıştır.

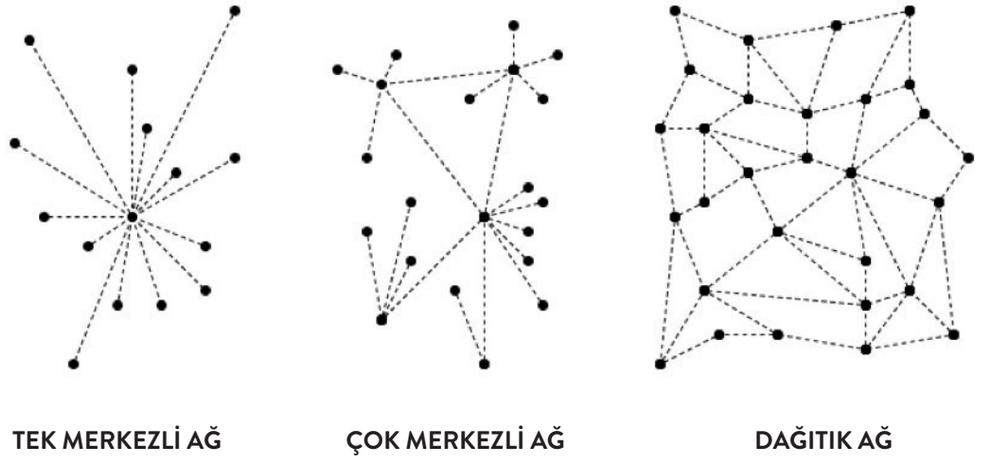
Bu yeni yaklaşımda, artık boş etiketler ve ip parçası sadece bizde değil, tüm arkadaşlarımıza dağıtılacaktır. Biz adımızı bir etikete yazıp imzaladıktan ve ipe geçirip düğüm attıktan sonra, herkes elindeki bir diğer boş etikete bizim adımızı yazacak ve bizden bu etiketi imzalamamızı isteyecektir. Daha sonra bunu kendi iplerine geçirip düğüm atacaktır. İkinci arkadaşımız kendi adını kendi etiketine yazıp imzaladıktan sonra bize imzalatacak ve ipine geçirerek düğüm atacaktır. Diğer herkes ellerindeki bir boş etikete ikinci arkadaşımızın adını yazıp bu arkadaşımız ile birlikte ilk etiketi oluşturduğumuz için bize de imzalattıktan sonra ipe geçirip düğüm atacaktır. Bu şekilde 5 kişi sıralı şekilde baştan belirlediğimiz kurallara uyarak her defasında birbirinin aynı sıraya sahip etiket zincirini oluşturacaktır.

Şekil 6: **Etiket oyununda, artık herkesin elinde etiket zincirinin bir kopyası var.**



Artık belirli bir kayıt (mutabakat yapısı) ve sıraya (mutabakat süreci) sahip ve üretilen zincirin kopyalarının herkese dağıtıldığı bir yapıya sahibiz. Bu durumda herhangi bir kişinin sıralama üzerinde gerçekleştireceği bir manipülasyon veya hile, artık anlamını kaybedecektir. Çünkü çoğunluk, ellerindeki kayıtları birbiri ile karşılaştırıp, çoğunluğun mutabık kaldığı yapıya güvenmeye devam edebilecek ve hile hurda yapmaya çalışanları oyundan atabilecektir.

Şekil 7



Blockchain teknolojisi de tam olarak bizlere aynı yapıyı sunmaktadır. Veri sadece bir merkez veya bir merkez grubu tarafından değil, sisteme dahil olan herkes tarafından kayıt altına alınmaktadır. Burada tarafların bir birini tanıması gerekmediği gibi, güveni sağlayan şey kişiler arasındaki ilişkiler değil, sistemin en başta belirlenen kuralları ve bu kurallar dahilinde üretilen kayıt zincirinin herkese dağıtılmasıdır.

Blok zinciri kayıtlarının dağıtıldığı tüm noktalar, kendi aralarında iletişim halinde kalarak sistemin bozulmadığının teyidini gerçekleştirirler. Eğer veri kayıt zinciri yapısında, aradan bir halka çıkarsa veya değişirse, zincir kırılır ve sistemin geneli kırık/bozuk halkaya sahip noktayı dağıtık kayıt defteri ağından çıkartır. Böylece geriye kalanlar, zincirin kırılmadan devam ettiği noktasında mutabık kalarak sistemi kullanmaya devam ederler.

Blockchain Türleri

Biz de dahil olmak üzere, genellikle Blockchain teknolojisini anlatanlar, bu teknolojiyi internet teknolojisine benzetiyoruz. Bu benzetme, yapısal bir benzerlikten çok, her iki teknolojinin de devrimsel bir tetikleyici olma yönlerini vurgulamayı hedefliyor. Bu rağmen, internet altyapısı üzerinde farklı protokoller ile hizmet veren pek çok internet sitesi gibi, Blockchain teknolojisinin de tekil bir altyapı olduğu ve bunun üzerinde internet sitesi gibi uygulamalar bulunduğu düşünülebilir. Oysa gerçekte, Blockchain soyut olarak bir güvenlik protokolüne benzemekle beraber, aslında birbirinden farklı yaklaşımların kullanılabildiği onlarca farklı platformda, binlerce farklı uygulamanın hayata geçirilebileceği bir teknolojik yaklaşımdır.

Bu yaklaşımın çatısı altındaki tüm platform ve uygulamaları, dört ana tür ile gruplayabilmekteyiz. Şimdi bu türlere göz atarak Blockchain temellerimizi tamamlayalım.

Tür 1: Bütünüyle İzin Gerektirmeyen Blockchain Ağları

Eğer bir Blockchain ağına girerek kayıtlı verileri okumak için izin almanız gerekmiyorsa ve bu ağın "mutabakat yapısına" uyarak, yeni bloklar ekleyebilmek için "mutabakat sürecine" dahil olmak için yine izin gerekmiyorsa, bu tarz ağlara **Bütünüyle İzin Gerektirmeyen Blockchain Ağları** adı verilir.

Bu tarz ağların amacı olabildiğince çok kişinin sisteme dahil olması ve dahil olan herkesin "mutabakat sürecinde" rol almasıdır. Bu şekilde ağa dahil olan kişi sayısı arttıkça, ağın içindeki veri zincirinin bir kopyasına sahip olan nokta sayısı artacak ve ağ her geçen gün daha da güvenli bir hale gelecektir.

Bu durumu, etiket oyunumuzu halka açık bir meydanda oynadığımızı ve isteyen herkesin gelip bize katılabileceğini, yapması gereken tek şeyin sisteme dahil olduğu ana kadar oluşan bir zincirin kopyasını üreterek, hemen sonra sırayla devam eden sürece dahil olması şeklinde örnekleyebiliriz.

Tam bu noktada önemli bir soru sormalıyız? Bu ağa dahil olan insanların çıkarı ya da elde edeceği fayda ne olacaktır? Herhangi bir **Bütünüyle İzin Gerektirmeyen Blockchain Ağına** dahil olacak kişilerin bu işten bir çıkarının olması gerekir. **Bütünüyle İzin Gerektirmeyen Blockchain Ağlarında**, sistemin kendisi bir değer ifade eder.

Bu şekilde **Bütünüyle İzin Gerektirmeyen Blockchain Ağları** için, en popüler ve bize Blockchain teknolojisini de hediye edeni olan Bitcoin platformunu örnek olarak verebiliriz. Bitcoin ağında insanlar sisteme dahil olarak, ağ içinde "mutabakat sürecine" katılan bir uç nokta oluştururlar. Ağın daha güvenli hale gelmesi için veri zincirinin bir kopyasını taşırlar. Kendileri veya ağdaki diğer noktalar yeni bir blok eklediklerinde, bunun "mutabakat yapısına" uyumlu olup olmadığını kontrol ederler. Bu süreç içinde yeni bir blok ekleyenler (elbette ağın kurallarına uygun şekilde), ağın kendisi tarafından belirli bir miktarda Bitcoin ile ödüllendirilirler. İlerleyen bölümlerde, Bitcoin sisteminin nasıl çalıştığını detayları ile açıklayacağız.

Tür 2: Kısmen İzin Gerektirmeyen Blockchain Ağları

Eğer bir Blockchain ağına girerek kayıtlı verileri okumak için izin almanız gerekmiyorsa ama bu ağın "mutabakat yapısına" uyarak yeni bloklar eklemek ve "mutabakat sürecine" dahil olmak için izin gerekiyorsa, bu tarz ağlara **Kısmen İzin Gerektirmeyen Blockchain Ağları** adı verilir.

Bu tarz ağlarda verilere erişenler için bu veriler bir değer sunarken, ağın kendisi genellikle özel amaçlara hizmet etmek amacıyla tasarlanır. Artık, herkesin erişimine açık olan veri kayıtlarının "mutabakat sürecinde" rol alacaklar seçilmektedir.

Bu durumu, etiket oyunumuzu özel bir buluşma esnasında yakın arkadaşlarımız ile oynarken, oluşan kayıtları herkesin diğer arkadaşlarına göstererek "bakın ne güzel bir hatıra yaptık" demesine benzetebiliriz.

Daha anlamlı olması açısından henüz hayata geçmemiş farklı bir örnek daha verelim:

Şu anda dünya üzerindeki en önemli problemlerden birisi haber kaynaklarının güvenliğidir. Sosyal medya kanallarından akan haberler başta olmak üzere zaman zaman çok büyük haber ajansları bile yanılarak hatalı haberler geçebilmektedir.

Bu sorunu çözmek için üretilen bir Blockchain Ağı düşünelim. Ağımızın adı "Güvenli Haber Blockchain Ağı" olsun. Bu ağda her bir haber yeni bir blok olarak kaydedilsin ve dileyen herkes bu ağa erişerek haberleri okuyabilsin. Ancak ağa yeni bir haber eklemek için "mutabakat yapısı" resmi bir haber ajansı olmayı gerektirsin. Resmi bir haber ajansı ağa bir haber gönderdiğinde ise bu haberin bağımsız üç farklı haber ajansı tarafından daha onaylanması mecburi olsun (mutabakat süreci) ve bu onaylar gelince haber bir blok olarak ağa eklensin.

Bir örnek daha verelim: Bağımsız müzisyenlerin parçalarını yayınladıkları bir Blockchain platformu düşünelim. Bu durumda sisteme giren herkes tüm müzik parçalarını dinleyebilir ve bunlara erişebilir. Ancak "mutabakat yapısı" gereği sisteme sadece bağımsız müzisyenlerin parça eklemesine izin verilmektedir. Bu parçaların orijinal ve benzersiz olduğunu ise "mutabakat süreci" gereği meslek birlikleri sağlar. Bu durumda bu ağa erişenlerin çıkarı, müzik parçalarını dinlemek; mutabakatı sağlayanların çıkarı ise eserlerinin kayıt altına alınması (telif ve belki gelir süreçlerini de düşünerek) olur.

Açık (Public) ve Özel (Private) Blockchain Ağları

Yukarıda detayları ve örnekleri ile anlattığımız **Bütünüyle İzin Gerektirmeyen** ve **Kısmen İzin Gerektirmeyen, Blockchain Ağları** herkesin erişimine açık oldukları için **AÇIK (PUBLIC) Blockchain Ağları** olarak gruplandırılırlar.

Öte yandan şirketler, organizasyonlar ve kamu kurumları Açık Blockchain Ağları üzerinde veri bulundurmayı, bu ağlardan faydalanmayı sakıncalı bulabilirler. Evet, verileri şifreleyerek bu tarz ağlara dağıtmak mümkündür, ancak bu şifreler kırılabilir veya anahtarlara sahip kişiler bu bilgileri sızdırabilir. Kısacası güvenlik açısından endişeler olabilir veya bu tarz bir ağın üzerine yazılacak olan verilerin herkese açık olmasını gerektirecek bir durum olmayabilir. Bu noktada Blockchain ağları için ikinci grup kaşımıza çıkar: **ÖZEL (PRIVATE) Blockchain Ağları.**

Özel Blockchain Ağlarının en temel özelliği bu tarz ağlarda kayıtlı verileri okumak için mutlaka ağın kendisinden izin alarak giriş yapılması gerekmesidir. Şimdi bunlara yakından bakalım.

Tür 3: Kısmen İzin Gerektiren Blockchain Ağları

Eğer bir Blockchain ağına girerek kayıtlı verileri okumak için izin almamız gerekiyorsa ama sonrasında bu ağın "mutabakat yapısına" uyarak yeni bloklar eklemek ve "mutabakat sürecine" dahil olmak için izin gerekiyorsa, bu tarz ağlara **Kısmen İzin Gerektiren Blockchain Ağları** adı verilir.

Bu tarz ağların amacı, kaydedilen verileri sadece ilgili tarafların erişimine açmak ancak içeriye giren herkesi "mutabakat sürecine" dahil etmektir. Bu şekilde ağa dahil olanlar arasında güvenli bir veri kayıt sistemi oluşturulur.

Bu durumu etiket oyunumuzu yabancılara kapalı bir mekanda oynarken aramıza sadece davet ettiğimiz arkadaşlarımızın katıldığı senaryo ile açıklayabiliriz. Davetli arkadaşlarımız hemen oyuna girebilecektir.

Gerçek hayattaki farazi bir örnek ise bir bankanın kendi şubeleri arasında gerçekleşen havale sistemi için verilebilir. Bir bankanın şubeleri arasındaki havale işlemlerini tutmak ve bu bankaya özel bir Blockchain ağına erişmek için, Bankanın bir şubesi olmak mecburi olacaktır. Ancak bir şube içeriye giriş yaptıktan sonra artık "mutabakat yapısı" ve "mutabakat sürecine" dahil olacaktır. Böylece herhangi bir şubenin veya bir grup şubenin tüm sistemleri aksayacak olsa bile diğer şubeler arasında havale işlemleri devam edebilecek ve veri kayıtları tüm şubelere dağıtıldığı için gayet güvenli bir altyapı kurulmuş olacaktır.

Tür 4: Bütünüyle İzin Gerektiren Blockchain Ağları

Eğer bir Blockchain ağına girerek kayıtlı verileri okumak için izin almamız gerekiyorsa ve sonrasında bu ağın "mutabakat yapısına" uyarak yeni bloklar eklemek ve "mutabakat sürecine" dahil olmak için tekrardan izin gerekmiyorsa, bu tarz ağlara **Bütünüyle İzin Gerektiren Blockchain Ağları** adı verilir.

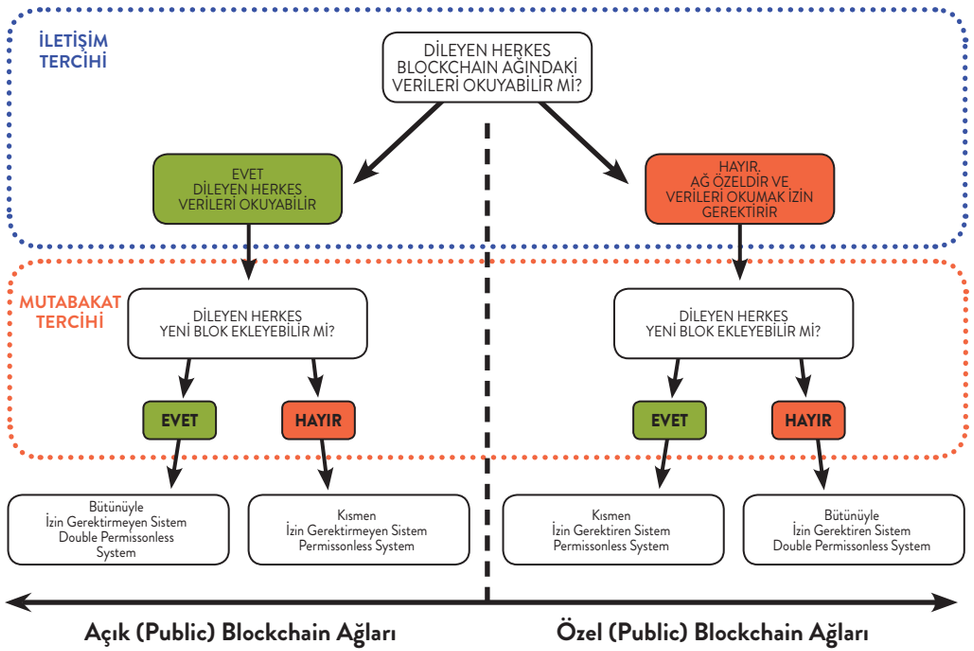
Bu tarz ağların amacı, kaydedilen verileri sadece ilgili tarafların erişimine açmak ve veri erişimine izin verilenler arasından da sadece seçilmiş tarafları "mutabakat sürecine" dahil etmektir. Bu şekilde ağa dahil olanlar arasında çok katmanlı bir güvenli veri kayıt sistemi oluşturulur.

Bu durumu etiket oyunumuzu yabancılara kapalı bir mekanda oynarken aramıza sadece davet ettiğimiz arkadaşlarımızın katıldığı ve bunların içinden de sadece seçilmiş belli sayıda kişinin zincir kaydı tuttuğu bir senaryo ile açıklayabiliriz. Zira arkadaş sayısı arttıkça herkesin her blokta imza atması giderek zorlaşmaktadır ve biz de böyle bir çözüm buluruz :)

Gerçek hayattan farazi bir örnek olarak bankalar arasındaki EFT işlemleri örnek gösterilebilir. Bir EFT işlemi için tüm bankalar arasında kurulan özel bir Blockchain ağına girmek gerekmektedir ve içeriye giriş izni için bir banka olmak gerekmektedir. Sisteme giren bankalar içindense sadece kendi aralarında EFT yapacak iki şubeye veri yazma izni verilmektedir. Böylece bu kayıtlar sadece banka ve şube seviyesinde tutulacaktır. Sisteme izin verilen bankaların ve şubelerin hepsi verileri okuyabilir, ancak "mutabakat yapısı" gereği "mutabakat sürecinde" kayıt oluşturma izni sadece kendi arasında işlem yapan iki şubede olacaktır.

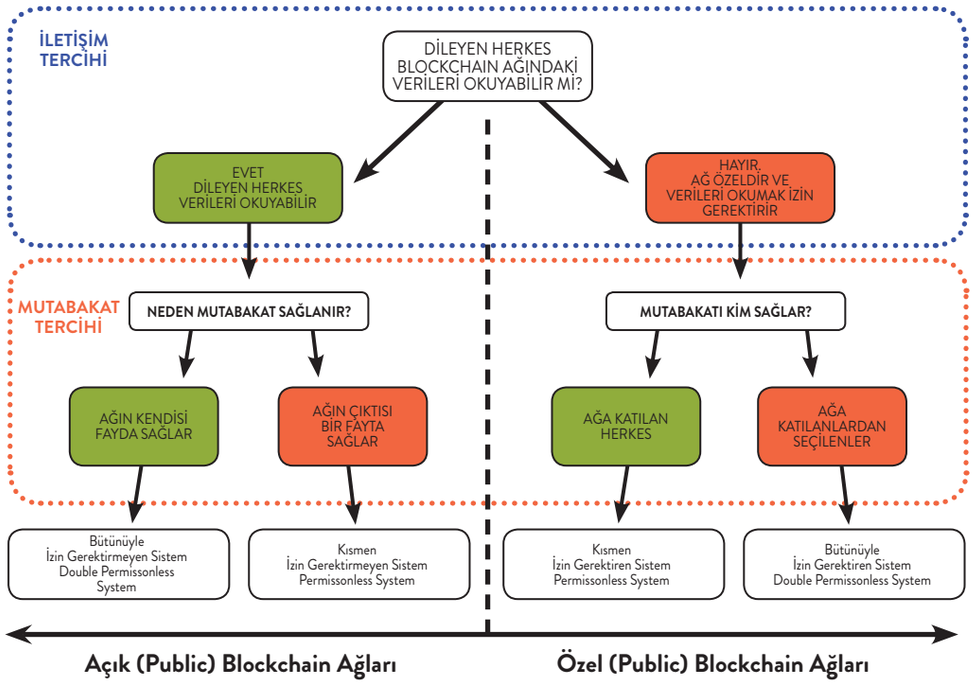
Tüm bu türleri aşağıdaki gibi basit bir şema ile gösterebiliriz.

Şekil 8: **Blockchain Türleri**



Blockchain ağına dahil olmanın, mutabakat sistemine katılmanın çıkar açısından değerlendirildiği yapıyı ise aşağıdaki şema ile görselleştirebiliriz.

Şekil 8: **Mutabakat Çıkarı**



Her iki şema ilk bakışta birbirine benzemekle birlikte Mutabakat Tercihi ve Sebebi katmanı farklılık göstermektedir. Bu noktaya dikkatinizi çekmek isteriz.

Mini Özet

Artık Blockchain teknolojisinin hangi amaca hizmet ettiğini (merkezi yapılara ihtiyaç duymadan güvenilir şekilde veri kaydı tutmak), kaydedilecek veri için kuralların baştan belirlendiğini (mutabakat yapısı), veriler bloklara kaydedilirken bir sürece bağlı ilerlediğini (mutabakat süreci), gerçekleşen tüm kayıtların pek çok noktaya dağıtıldığını (dağıtık kayıt defteri), Blockchain

ağlarına erişmek için izin almak gerekip gerekmediğini (açık veya özel), mutabakat sürecine dahil olmak için amacına göre farklı durumların olduğunu (izin gerektiren ve izin gerektirmeyen), erişim ve mutabakat izinlerine göre iki ana grupta dört farklı türünün olduğunu öğrendik. Şimdi iki önemli kavrama daha sırasıyla bakacağız: **Şifreleme ve Akıllı Sözleşmeler**

Blockchain Ağlarında Şifreleme

Kötü haber: Size bu kitapta şifreleme konusunda çok fazla bilgi veremeyeceğiz. İyi haber: Öğrenmeniz gerektiği kadar temel kavramları öğreneceksiniz zira şifreleme konusu dünyanın en ağır matematik, sayısal sistemler, programlama ve beyin yakan türden kafa yormayı gerektiren işlerinden birisidir.

Temel kavramlardan bahsederken Kriptoloji kelimesinin kökeninin eski bir Yunanca kelime olan Kryptos'dan geldiğini ve gizlilik demek olduğunu belirtmiştik. Tarih boyunca Gizlilik Bilimi (Kriptoloji) çok farklı yöntemler ile kullanılmıştır. Temel amaç bir verinin, istenmeyen birisinin eline geçtiğinde anlaşılamayacak hale getirilmesi ve tekrardan anlamlı hale getirilmesinin mümkün olduğunca zor hatta imkansız hale getirilmesidir.

En temel şifreleme yöntemini bir kasayı anahtar ile kilitlemeye benzetebiliriz. Anahtar sizin elinizde olduğu sürece kasayı sadece siz açabilirsiniz. Bir başkasına anahtarı vermediğiniz sürece veya kaba kuvvet kullanılmadıkça (bu süreç kasanın ne kadar sağlam olduğuna bağlıdır ve dijital dünyada bazı şifreleme yöntemleri gerçekten çok ama çok güçlüdür) açması mümkün olmayacaktır.

Kasa örneği eğer veriyi sadece siz saklayacaksanız anlamlıdır. Ancak veri bir başkasına gönderilecekse kasa ile birlikte anahtarı da göndermek gerekir. Bu da beraberinde anahtarın çalınması, kaybolması gibi farklı sorunları getirir. Anahtarın kaybolmaması için bir kopyasını çıkartmak ise güvenlik açısından daha da fazla probleme yol açabilir. Bu sebeple şifreleme dünyasında daha pratik bir çözüm kullanılır: Anahtarı değil, kilidi karşı tarafa göndermek.

Farz edelim ki siz elinizdeki bir veriyi çok önemli birisine göndereceksiniz. Yukarıda anlattığım problemler ile uğraşmak yerine karşı tarafın size bir kilit göndermesini talep edebilirsiniz. Bu durumda gelen kilit ile kasayı kilitledikten sonra karşı tarafa yollayabilirsiniz. Böylece anahtar hiç el değiştirmemiş olur ve güvenlik artar.

Blockchain ağlarında da bu yöntem kullanılır. Böylece ağların üzerine (ağ ister açık olsun ister özel olsun fark etmez) sadece belirli birisinin erişmesini istediğiniz bir veri ekleyeceğiniz zaman, karşı tarafın kilidi ile veriyi şifrelersiniz ve herkes ağda bu veriyi görse bile şifrelenmiş olacağı için anlamlandıramaz. Alıcısı, yani kilidi size gönderen ve bu kilidi açabilecek anahtara sahip taraf, bu anlamsız veriyi elindeki anahtar ile açarak okuyabilir. Böylelikle, Açık Blockchain Ağları'nda bile şifreli verileri tutmak mümkün hale gelir. Kitabımızın ikinci kısmında bu konuyu daha bilimsel ifadeler ve görselleri ile inceleyebilirsiniz.

Blockchain Ağlarında Akıllı Sözleşmeler

Çok iyi biliyoruz ki bilgisayar sistemleri sadece veriyi kaydetmek için hizmet vermiyorlar. Aynı zamanda pek çok farklı amaca hizmet eden uygulamalar çalıştırıyoruz. Peki, neden benzeri uygulamaları Blockchain Ağları üzerinde de çalıştırmayalım ki? Sonuçta tüm ağlarda verinin kaydını yapan kişiler, bu kayıtlar için yine bilgisayar sistemlerini kullanıyorlar. O zaman, bu sistemler üzerinde programlar da çalıştırabiliriz öyle değil mi? Kesinlikle evet.

Detaylarını kitabımızın ikinci bölümünde bulacağınız "Akıllı Sözleşmeler", Blockchain ağları üzerinde (eğer ağın böyle bir özelliği varsa) çalışan uygulamalardır. Akıllı Sözleşmeler, ağ üzerinde yazılan blokların içinde yer alan verilerin belirli durumları sağlaması durumunda otomatik olarak çalışarak belirli görevleri yerine getirebilirler. Basit bir örnek vererek bu konuyu netleştirelim.

Şu anda bir tapu devri yapmak istediğimizde bu işlemi noter üzerinden gerçekleştiriyoruz. Ancak noterler para transferi için hizmet vermiyor. Bu

hizmeti ya çanta ile parayı taşıyıp teslim ederek veya banka üzerinden işlem talimatı vererek yapmamız gerekiyor. İşte bu iki süreç arasında doğrudan bir kontrol mekanizması olmadığı için gazetelerin üçüncü sayfalarında ve internet haber sitelerinde "para dolu çantayı verdi ve..." şeklinde haberler altında dolandırıcılık olaylarına şahit oluyoruz. Oysa akıllı sözleşmeleri kullanan bir Blockchain ağı üzerinde bu sorunlar ortadan kaldırılabilir. Nasıl mı?

Sadece tapu devri ve tapunun bedelini transfer etme görevine sahip bir Akıllı Sözleşmemiz (uygulama) olsun. Bu akıllı sözleşmenin bulunduğu Blockchain ağına girerken tapuyu devredecek ve parayı ödeyecek taraflar TC kimlik numaraları ve e-devlet şifreleri ile sisteme giriş yaptıktan sonra tapunun kimden kime, hangi bedelle satılacağını sisteme bildirsinler. Bu noktada akıllı sözleşme çalışarak, ilk önce tapu sahibinin bu tapuya sahipliğini ilgili kurum veri tabanından sorup öğrensin, daha sonra da satın alacak kişinin banka hesabında yeterli para var mı yok mu kontrol etsin. Her iki bilgi de doğrulanınca, tarafların onay vermesi ile birlikte otomatik olarak tapu kayıtlarında gerekli değişiklik yapılsın ve bankadan para transferi işlemini gerçekleştirilsin. Tüm bu adımlar, bu akıllı sözleşmenin bulunduğu Blockchain ağında yazılır ve bu sistem bir e-devlet hizmeti olduğu için yasal olarak bir delil niteliği taşır. Bu durumda, tapu kayıt sistemi ve bankanın kendine özel bir Blockchain ağı olmasa bile sistemler kendi aralarında konuşarak, bu sürecin sorunsuz ve insan müdahalesi olmadan çalışmasını sağlayacak ve tüm riskler ortadan kalkacaktır. Elbette bu durumun noterlerin pek hoşuna gideceğini söyleyemeyiz. Belki de noterleri artık işlem yapmaktansa bu Blockchain ağının çalışmasını sağlayan noktalar olarak görevlendirmek bir çözüm olabilir.

Blockchain Ağlarında Gizlilik ve Anonimlik

Dünyadaki ilk ve en popüler Blockchain ağlarından birisi olan Bitcoin Blockchain ağının tasarımı gereği, üzerinde oluşturulan kişilere ait cüzdan bilgileri için gerçek kimlik bilgileri talep edilmez. Farklı bir ifade ile Bitcoin Blockchain ağına giren bir kişinin gerçek hayatta kim olduğunu, sadece ağ yapısını inceleyerek pratik olarak bulmak neredeyse imkânsızdır.

Pek çok farklı Blockchain ağı, üzerindeki işlemlere ait özel bilgileri kriptografi tabanlı çözümler ile şifrelenmiş bir şekilde tutar. Bu durum, genel olarak Blockchain ağlarının yapısında mutlak bir gizlilik ve anonimlik (gerçek kimlikten bağımsızlık) algısının oluşmasına yol açmaktadır. Ancak, bu algının doğruluğunu da tartışabiliriz.

Bir Blockchain ağı üzerindeki gizli yani şifrelenmiş bilgilerin bir dış gözlemci için orijinal haline çevrilmesi mümkün olmasa da açık işlem bilgileri üzerinde çeşitli analiz çalışmaları yapılabilir ve bu işlemler üzerinde farklı veri modellemeleri gerçekleştirilebilir.

Bir sonraki bölümde ele alacağımız kripto paralarda ise alım ve satım işlemleri, tüm kimlik bilgilerinizi en detaylı şekilde sizden alan çeşitli borsalar üzerinde yapıldığı için, gizlilik veya anonimlik diye bir şey söz konusu değildir. Kimliğiniz her zaman kayıt altındadır ve zaten bilinir.

1.3. Para Kavramı ve Kripto Paralar

Blockchain kavramının ortaya çıkışında, bir kripto para birimi olarak tasarlanan Bitcoin'in rolünü göz ardı edemeyiz. Ancak Blockchain ağlarının amacı sadece kripto para üretmek ve kullandırmak değildir. Buna rağmen, Bitcoin ve türevleri gibi fiziksel karşılığı olmayan dijital kayıtların nasıl bu kadar değerli hale gelebildiğini ve ticari amaçla kullanılabildiğini, bu kitap kapsamında sizlere anlatmamız gerekiyor. Bu sebeple kısa bir süre için Blockchain'in zihin yoran kavramlarından uzaklaşıp, derin bir nefes alarak, değer ve para kavramını ele alacağız.

Paranın tanımını, "niteliği bakımından ortak bir değer algısı ve kabulü" ifadesiyle yapabiliriz.

Tam bu noktada, FinTech dünyasının önemli liderlerinden **David Birch**'ün "**Kimlik: Yeni Para**" adı ile Türkçeye çevrilen "**Identity is the New Money**" isimli kitabında yer alan kritik bir bölümü burada paylaşmanın zamanı olduğunu düşünüyoruz:

Paranın Tanımını Anlamak: Yap Adası ve Taş Paraları

Ekonomist Milton Friedman tarafından 1991'de kaleme alınan ünlü 'The Island of Stone Money – Taş Paralar Adası' isimli bir makalede para kavramı yalın bir örnekle açıklanmıştır. Yap, Güney Pasifik okyanusunda yer alan dört adadan oluşan bir ulustur. Adalarda bizim alışkın olduğumuz paranın yerini alabilecek altın, gümüş veya diğer farklı bir maden bulunmaz. Bu sebeple bizlerin bir değer değişim aracı olarak gördüğümüz değerli metallerin yerine Yap sakinleri taşları kullanır. Yap sakinleri, birkaç yüzyıl öncesinde kendilerinden yaklaşık 400 kilometre uzaklıktaki başka bir ada grubunda özel bir kireçtaşı keşfederler. Bu kireçtaşı Yap adalarında bulunmadığı için kaynak oldukça kısıtlıdır. Zaman içinde ada şefleri, bu uzak adalara seferler düzenleyerek madenlerden kireç taşı çıkartırlar ve yanlarında diskler şeklinde yeni taşlar getirirler. Bazıları 5-10 santim bazıları ise 3,5 metreye varan genişlikteki bu diskler, farklı büyüklüklerde ve ağırlıklardadır. Başarılı bir sefer sonunda şef, büyük taşlara ve küçük taşların yüzde 40'ına kendisi el koyar. Geri kalanlar ise sefere katılanlar arasında paylaştırılır. Böylece, uzun süre yaşayan bir şefin evinin dışında pek çok büyük taş birikir.

Adada bir şef, alışveriş yapmak veya bir komşusuna hediye vermek istediğinde bu taşların taşınamayacak kadar büyük olduğunu fark eder ama kimse bunu sorun haline getirmez. Şef, taşın yeni sahibini ilan eder ve artık herkes taşın yeni sahibinin kim olduğunu bilir. Bu tüm ticari işlemler sürecinde bu şekilde işler ve şefler arasında taşların yeri değişmeden sürekli olarak kime ait olduğunun bilgisi dolaşır durur. Herkes mutludur. Yap adalarında para taşlar ile ifade edilen ama günün sonunda insanların hafızalarında saklanan bir değer olmuştur. Ada sakinleri taşların kime ait olduğunu unutmadığı sürece sistem mükemmel şekilde işler.

Sistem o kadar iyi çalışmaktadır ki taşların nerede olduğunu kimse bilmese bile (taşlar kaybolsa bile) işlemeye devam eder. Hatta, zaman zaman taşlar madenlerden çıkartıldıktan sonra adaya geri dönüş yolunda gemiler bir fırtınaya yakalanır ve batar, doğal olarak taşlar da denizin dibini boylar.

Ancak adaya geri döndüklerinde şef taşın yerini herkese söyler. Taş kıyıdan 5-10 kilometre ötede denizin dibinde durmaktadır. Herkes şefe güvendiği için bu kabul görür ve şef bu taşı bir alışverişte kullandığında kabile bu durumu kabul ettiği için sorun oluşmaz. Denizin dibindeki taşın artık yeni bir sahibi olur. Taşlar hiçbir yere gitmediği için ortada hiçbir sorun yoktur. Herkes ortak bir değer üstünde fikir birliğine varmıştır. Friedman'ın hikayesinde vurguladığı nokta şudur: Gerçekten bir taşın söylenen yerde olup olmaması önemli değildir. Eğer herkes ortak bir değer yargısında fikir birliği yapıyorsa, bu değer yargısına para denir.

Paranın ortak bir değeri yargısı için mutabakat aracı olması tanımı en yalın tanımdır ve bundan sonra neye benzeyeceği bir detaydan ibarettir. Bunlar Yap adasında kullanıldığı gibi taş parçaları, masa üstü oyunu Monopoly paraları, kağıda basılmış kopyalanması güç banknotlar, silikon bir işlemci içeren kredi kartı veya Bitcoin Blockchain ağı üzerindeki eşsiz veri kayıtları olabilir.

Neden Bitcoin Bu Kadar Değerli?

Bir sonraki bölümde ele alacağımız Kripto Para kavramı için de durum kesinlikle daha farklı değildir. Eğer Bitcoin 2008 yılında ilk ortaya çıktığı günden bu yana değeri sıfır noktasından 20 bin doların[8] üstüne ulaşmayı başardığına göre, bunun temelinde Bitcoin altyapısında kullanılan teknolojiye güven ve bu ekonominin geniş topluluklar tarafından kabul görmesi yatmaktadır. Ancak Bitcoin'in bu değer artışını tetikleyen bazı süreçleri de göz ardı edemeyiz. Şimdi, bu süreçleri hatırlayalım:

Bitcoin ilk ortaya çıktığı andan itibaren özellikle bilgisayar teknolojisi düşkünleri, programcılar gibi özel bir kitle arasında ilgi görüyordu. Uzun süre bu şekilde yoluna devam eden Bitcoin, belirli bir eşiği aşarak 10 dolarlı değerlerden yüzlerce dolar ile değeri ifade edilen noktaya geldiğinde, Bitcoin

[8] *Bitcoin değeri sürekli değişim göstermektedir. Bu kitap ilk kez kaleme alınırken 1.300 dolar gibi bir rakamdan bahsederken aynı yıl sonuna doğru değeri 20 bin doların geçmeyi başardı ancak daha sonra tekrar gerileyerek 6.500 dolara kadar düştü ve biz bu ikinci baskıyı hazırlarken tekrar yükselme seyri içerisindeydi.*

alım ve satım işlemlerine aracılık yapan Hong Kong merkezli Bitfinex borsası 2016 yılının Ağustos ayında hacklendi ve o günkü değeri ile 70 milyon dolar değerinde Bitcoin çalındı. Bu olayın ardından Bitfinex, Bitcoin sahiplerinin satış yapmasını veya Bitcoin transferlerini engellemedi, fakat satışlardan elde edilen ABD doları gelirlerin mevcut banka hesaplarına transfer edilmesini veya sistem içinde hesaplarında ABD doları olarak para bulunan kullanıcılarının da aynı şekilde mevcut banka hesaplarına transfer gerçekleştirebilmesini askıya aldı. Bu sebeple pek çok kullanıcı Bitcoin satın almaya yöneldi ve bu süreç Bitfinex kaynaklı olarak tüm diğer borsalarda Bitcoin fiyatlarının yükselmesini tetikledi. Bu sürece eş zamanlı olarak, siber korsanlar, ABD Ulusal Güvenlik Teşkilatı'ndan (NSA) çalınan çeşitli bilgiler ile bilgisayarların hacklenmesini sağlayan bir açığı kullanmaya başladılar. WannaCry isimli virüs ile yapılan bu saldırılar sonucunda, pek çok bilgisayar ele geçirildi ve bu bilgisayarlardaki verilerin şifrelenerek geri kurtarılabilmesi için 300 ABD doları değerinde Bitcoin ödemesi yapılması talep edildi. Bu taleplerin oluşturduğu Bitcoin satış işlemleri tüm pazar içinde büyük bir orana sahip olmamakla birlikte, binlerce kişinin farklı borsalarda oluşturduğu talep sayesinde, Bitcoin'in değeri 2017 yılının Şubat ayına kadar 1.200 dolar seviyesine tırmandı. Sadece 6 ay içinde değeri neredeyse ikiye katlanan Bitcoin, bir anda medya kanallarının ilgisini çekti ve "Ne ABD Doları, Ne Altın! En çok o kazandırdı..." şeklinde atılan başlıkların etkisiyle, tüm dünyada Bitcoin'e ciddi bir talep patlaması yaşandı. Bitcoin fiyatı yükseldikçe medya göbeğini kaşıdı, göbek kaşındıkça yeni insanlar Bitcoin satın alma talebi yarattı. Bu süreç içinde yüzlerce irili ufaklı haberin, piyasaları şişiren balinaların (büyük hacimlerde Bitcoin sahiplerinin) ve farklı faktörlerin etkisi ile Bitcoin hızla yükseldiği gibi 2018 yılının Ocak ayından itibaren tekrar geriledi. Bu kitabın yeni baskısını hazırlarken de yükselme yönünde yeni bir hareketlenmenin başladığına şahit oluyoruz.

Değeri Tetikleyen Mutabakat ve Rant

Toplumsal olarak değer birliği üzerinde mutabakat yaptığımız her aracı bir para unsuru olarak kullanabiliriz. Nakitsiz yaşama giden yol da bu temel

kabul üzerine kurulabilir. Bugün, kazandığımız parayı teorik olarak hiç elimize almadan yaşantımızı sürdürebileceğimiz bir teknolojiye sahibiz. Banka ve kredi kartları ile yapılan işlemlerde güven unsuru neye dayanır? POS makinelerinden çıkan bir adet kağıt parçasına mı? Yoksa bu teknolojiyi mümkün kılan bankacılık altyapısı ve bu altyapıyı denetleyen devlete mi?

Bitcoin gibi kripto para birimleri, farklı bir kulvarda kendilerine yol açıyorlar. Herhangi bir düzenlemeye tabi olmayan, merkezi bir kontrol birimi olmayan bir yapıya sahipler. Ancak bu kitapta anlatılan Blockchain teknolojisinin sunduğu mutabakat yapısı ve mutabakat süreci ile eşsiz birer kayıt olarak karşımıza çıkıyorlar. İlk kez Satoshi Nakamoto'nun geliştirdiği enflasyondan arındırılmış sınırlı üretim kapasitesi sayesinde bu eşsiz veri kayıtları ilgi görüyor. Eğer bir gece dünya üzerindeki tüm iletişim ağları çökecek olsa, bu değerin elbette bir karşılığı kalmayacaktır ancak aynı durum merkezi kontrol birimleri tarafından üretilen resmi para birimleri için de geçerlidir.

Bitcoin küresel ölçekte bir mutabakat siteminin kurulmasını sağlamıştır ve Bitcoin benzeri diğer kripto para birimleri de bunu sağlamak için gayret göstermektedir. Bu yapının ilgi çekmesi anormal bir durum değildir, ancak bir önceki bölümde ele aldığımız gibi pek çok faktörün devreye girmesi ile insanların çalışmak yerine kısa yoldan zengin olma arzusu, onların Bitcoin ve benzeri kripto paralara bir rant aracı olarak hücum etmelerini doğurmaktadır. Pek çok insan için Bitcoin'in teknolojisi hiçbir anlam ifade etmiyor. Onlar için önemli olan, bugün yatırdıkları 1.000 doları bir ay sonra 2.000 dolar yapabilmek önemli.

Dijital Para Dünyası ve Kripto Paralar

Paranın insan hayatında kullanımına başlanması ile birlikte geçirdiği evrim süreci incelendiğinde, bir süre sonunda denge sağlama hedefli arz kontrol mekanizmalarına ve dolandırıcılığa engel olmak amacı ile çeşitli güvenlik yaklaşımlarına ihtiyaç duyulduğunu gözlemliyoruz. Bu ihtiyaçlar, gerek oluşturulan kurumlar (merkez bankaları vb.) gerekse geliştirilen fiziksel

önlemler (kağıt ve madeni para yapılarında sahtecilik karşıtı özellikler vb.) gibi çeşitli çözümler ile karşılanmaktadır.

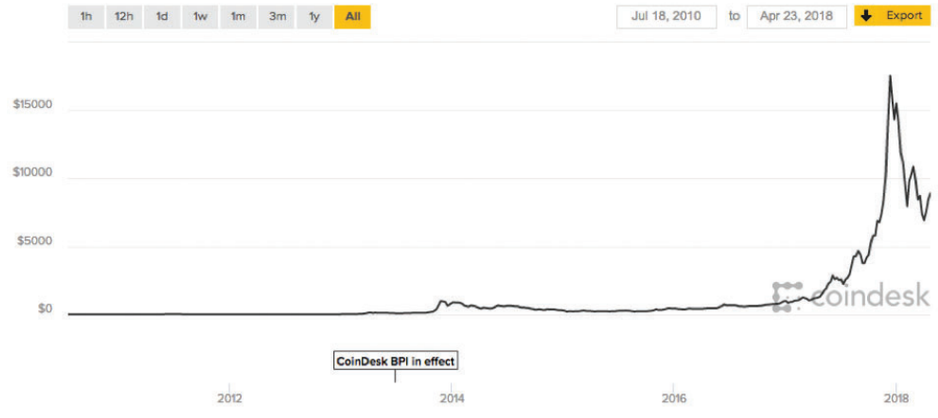
Dijital dünyanın paranın temel niteliklerine hizmet etmesi ve bu nitelikler sayesinde sayısal bir formunun üretilmesi, yeni bir çaba değildir ve sadece Bitcoin ile başlayan Blockchain teknolojisine özel de değildir.

Dijital para kapsamındaki bu ihtiyaçların giderilmesinde kriptoloji kullanımı konusunda öncü çalışmalardan bir tanesi, matematikçi David Chaum tarafından 1983 yılında yayınladığı bir akademik makale[9] kapsamında ortaya çıkmıştır. David Chaum sonrasında bu araştırmalarını temel alarak "DigiCash" adlı elektronik para firmasını 1990 yılında kurmuştur. DigiCash tarafından sunulan yazılım ile birlikte kullanıcılar, paralarını "eCash" adlı, banka tarafından kriptografik olarak imzalanmış dijital bir formatta bilgisayarlarında tutup, bu dijital parayı anlaşmalı her hangi bir kurumda, kredi kartı numarası gibi bir bilgi paylaşımı yapmadan, gizli ve güvenli bir şekilde kullanabiliyorlardı. Bu çalışma 1998 yılında yeterli kullanıcı sayısına ulaşamadığından dolayı iflas etmiş olsa da, getirdiği kavramlar ve yaklaşımlar ilerideki çözümler için esin kaynağı olmuştur. İlginç olan, kullanıcı sayısının az olmasının ana nedenlerinden birinin, dönemin çevrimiçi kullanıcı davranış yapısının gizlilik ve güvenlik konularına önem vermemesi olmasıdır.

Günümüzde İnternet tabanlı servislere sürekli bağlı mobil yaşam modelinin yaygınlaşması ile birlikte, kullanıcıların gizlilik ve güvenlik ihtiyaçları tekrar gündeme gelmiştir. Kripto para kavramı, temel olarak dijital dünyada bu ihtiyaçların çözümü için şifrelemenin kullanıldığı dijital kayıtları ifade etmektedir. Kullanılan şifreleme yöntemlerinin sağladığı güvenlik kapsamında dijital paranın taklit edilmesi, izinsiz kullanılması ve kural dışı bir şekilde oluşturulması mümkün olmamaktadır. Kripto para kavramı özellikle Bitcoin'in ortaya çıkışı ile birlikte genel anlamda bir bilinirliğe kavuşmuş, bilinirliğin getirdiği yaygınlaşma ve kullanım alanlarının artışı ile birlikte daha önce hiç bir sanal para birimi tarafından ulaşılamamış bir değerlendirmeye erişmiştir.

[9] Chaum, David (1983). "Blind signatures for untraceable payments" (PDF). Advances in Cryptology Proceedings. 82 (3): 199–203.

Şekil 10: **Dolar/Bitcoin piyasa değerini veren coindesk.com'un verilerine göre, 23 Nisan 2018 tarihinde 1 BTC'nin piyasa değeri 8.910 $[10] olarak belirtilmiştir.**



Bitcoin'in başarısı ile birlikte çeşitli kripto-para birimleri ortaya çıkmıştır. Bitcoin ile benzer tasarım yapısına sahip olup ancak kendilerine ait bir Blockchain ağı üzerinde yaşam döngüsünü sürdüren bu kripto para birimlerine, "alt-coin[11]" adı verilmektedir.

Şu ana kadar binlerce alt-coin denemesi yapılmıştır. Bitcoin başta olmak üzere kripto paralara olan ilgi, bu piyasaların kısa sürede gelir getirme fırsatı ve yüksek risklere rağmen oluşan rant, milyonlarca kişinin ilgisini çekmeye devam etmektedir.

CoinMarketCap[12] internet sitesi şu anda dolaşıma sunulan tüm kripto paraların listesini sunmaktadır. Verilere göre binlerce farklı kripto para birimi bulunmaktadır.

Alt-coin yapılarında da spekülasyonlar oldukça fazla görülmektedir. Burada özellikle yeni ortaya çıkan ya da düşük değere sahip bir alt-coin'den yüksek

[10] Daha önce de belirttiğimiz gibi bu değer sürekli değişim göstermektedir.

[11] Alt-Coin: Alternative Coin

[12] Kripto para piyasalarındaki güncel pazar verilerine ve değerlerine ulaşmak için https://coinmarketcap.com adresini kullanabilirsiniz.

miktarda alma, çeşitli kanallar aracılığı ile bu satın alma hareketini genel bir topluluk ilgisi olarak gösterme, fiyat yükselmesi ile birlikte elde tutulan alt-coin'leri satma davranışı görülmektedir. Satış sonrası yaratılan yapay ilginin ortadan kaybolması ile birlikte alt-coin değerinde yüksek hareketlilik ve düşüşler gözlemlenmektedir.

Kripto Paralar, Finans ve Bankacılık Dünyasını Tehdit Ediyor mu?

2008 yılında patlak veren küresel finansal krizinin, tüketicilerin bankacılık sistemine olan güvenini sarstığını daha önce belirtmiştik. Bu krizin hemen ardından ortaya çıkan Bitcoin'in merkezi bir yapıya bağlı olmaması, Bitcoin miktarının ve üretiminin enflasyondan arındırılmış olması ve artan ilgi ile birlikte, Bitcoin'in dünya üzerinde devletlerin kontrolünde bulunan para piyasalarını, finans sistemlerini tehdit ettiği yönünde anarşist bir anlayışın da ortaya çıktığına şahit oluyoruz. Acaba bu ne kadar ayakları yere basan bir düşünce şekli?

Tüm alt-coinlerin değerlerini Bitcoin veya daha değerli diğer bazı kripto paralar ile ölçüyoruz. Bitcoin'in değerini ise hâlâ ABD doları ile ölçüyoruz. Bu şekli ile Bitcoin tüm dünyada kabul gören bir değer takası aracına dönüşse bile ki bununla alakalı çok ciddi teknik ve pratik sorunlar bulunuyor, Bitcoin'in değerini ABD doları ile ölçmeye devam ettiğimiz sürece, Bitcoin'in küresel finans sistemine alternatif olduğunu söylemek gerçekten komik bir düşünce şekli olur. Siz değeri bu kadar hareketli bir araçla gidip bir kahve alır mısınız? Bugün kahveye verdiğiniz paranın yarın 300 dolar daha değerli olma ihtimali var. Peki, bir kahve dükkanı bugün size Bitcoin ile kahve satar mı? Zira yarın aldığı ödemenin değeri 300 dolar düşebilir! Elbette şu anda pek çok kişi ve kurum Bitcoin ile ticaret yapıyor, neden mi? Çünkü bu tarz haberlerin çok ciddi bir reklam değeri var. Amaç Bitcoin ile satış yapmak değil, medyada yer bulmak.

Gerçekten Bitcoin ve diğer kripto para birimlerinin değerini ABD doları ile ölçmediğimiz, 0,001 Bitcoin eşittir bir kahve dediğimiz bir dünya mümkün mü?

Teorik olarak mümkün, ancak devletlerin bağımsızlık göstergesi olan ulusal paraların yerine böyle bir sistemin geçmesine izin vermesi ne kadar olası? Ama Bitcoin engellenemez bir sistem! Aslında değil, gayet engellenebilir ve hatta yok edilebilir. Bugün dünya üzerinde Bitcoin Blockchain ağını oluşturan tüm noktaların IP adresleri ve yerleri biliniyor. Bu trafik akışını engellemek bir devlet için ne kadar güç olabilir? Haydi bunu başaramadılar diyelim, NSA gibi kurumların birkaç kripto para borsasını hacklemesi ve 50 milyar dolar değerinde Bitcoin çalmasını kim engelleyebilir? Böyle bir durumda Bitcoin'e olan güvene ne olur? Uzun lafın kısası, Bitcoin ve diğer kripto para birimlerinin geleneksel finans ve bankacılık sistemine bir tehdit oluşturması söz konusu değil, ancak bu durum, Bitcoin ve diğer Blockchain teknolojilerinin bu yapıları ve hatta dünyanın mevcut yapısını değiştirmeyeceği anlamına gelmiyor. Sadece bu süreç, genel olarak düşünülen şekilde gerçekleşmeyecek. En azından bu kitabın yazarı olarak ben böyle düşünüyorum.[13] Ayaklarımızı yerden kesmeyi hedefleyen **Blockchain Teknolojisinin Geleceği** bölümünde bu konuya geri döneceğiz.

Kripto Paraların Birbirinden Farkı Nedir?

Tüm kripto paralar, Bitcoin'in açtığı yoldan ilerlemekte ancak farklı amaçlara hizmet etiklerini belirtmekle birlikte daha farklı özellikler sunmaktadırlar. Bu çerçevede kripto paraların temel özelliklerini şu şekilde listeleyebiliriz:

- ✔ Mutabakat Yaklaşımı
- ✔ Mutabakat Süreci
- ✔ Kripto para üretim sürecinde kullanılan problem
- ✔ Kullanılan özetleme algoritması
- ✔ Platform kapsamındaki diğer hizmet yeteneklerinin geliştirilmesi
- ✔ Her yeni bir Blok oluşturmak için gerekli ortalama süre (frekansı)

[13] *Kitabımızın iki yazarından Ahmet Usta.*

- ✔ Blok büyüklüğü (Bitcoin yapısında blok büyüklüğü 1MB olarak belirlenmiştir.)
- ✔ Yaratılabilecek kripto para miktarı (emisyon hacmi)

Bir örnek vermek gerekirse, popüler bir alt-coin olan Litecoin (LTC) kapsamında mutabakat sürecinin daha hızlı yapılabilmesine hizmet etmek üzere, yeni bir blok oluşturmak için gerekli ortalama süre (blok frekansı) 2,5 dakika olarak belirlenmiştir. Bu değer, Bitcoin için ortalama 10 dakikadır. Litecoin ayrıca özel donanımlar kullanılarak kripto para üretimini engelleyen ve daha dağınık bir madencilik ağına sahip olmayı hedefleyen bir mutabakat yapısı tasarlanarak geliştirilmiştir. Bunların yanı sıra toplam Litecon miktarının üst sınırı 84 milyon olacak şekilde tasarlanmıştır. Bitcoin platformunda bu rakam 21 milyon Bitcoin'dir.

Güncel bir alt-coin denemesi olan Zcash, bütünüyle izin gerektirmeyen bir Blockchain ağı olmakla birlikte, tüm işlem kayıtları üzerindeki gönderici, alıcı ve tutar bilgilerini şifreleyerek gizli tutmaya odaklanmıştır.

Alt-coin'ler genel olarak türedikleri yapılardaki teknik problemlere alternatif getirme iddiasında olsalar da farklı denemeler yapmaktadırlar. Örneğin 2013 sonunda ortaya çıkan Dogecoin, ilk tasarımında Bitcoin'den farklı olarak, blok üretimi kapsamında rastlantısal bir teşvik ödül yapısı getirmiştir. Ancak bu yapı, daha sonra sistemde bulunan bir açık dolayısı ile iptal edilmiştir.

Kripto Para Birimlerine Yatırım Yapalım mı?

KESİNLİKLE YAPIN! Şaşırdınız mı? Büyük harfler ile yazdık, sonuna ünlem koyduk ve şaka yapmıyoruz ciddiyiz. Neden mi?

Bu dünya, yeni şekillenen, keşfedilmesi ve bu keşif boyunca deneyim ve tecrübe kazanılması gereken bir alan. Bu alanı sadece bir kitap okuyarak, birkaç sosyal medya hesabı takip ederek, medyada çıkan haberleri okuyarak tanımanız mümkün değil. Mutlaka içine girmeniz lazım.

Bizim okuyucularımıza tavsiyemiz yatırımlarını belirli kuralları takip ederek yapmaları.

- ✔ Asla ve asla kaybettiğinizde üzüleceğiniz değerler ile yatırım yapmayın. Geçen sene Bitcoin değeri 15.000$ seviyesinde iken, bu artışın hiç bitmeyeceğini düşünen pek çok kişi, evini, arabasını satıp, bankadan kredi çekerek yatırım yaptı. Şu anda bu insanların hayatı kararmış durumda. Pek çok kişi için 1.000$ bile büyük bir tutar. Yatırımlarınızın 50-100 TL seviyesinde de tutulabileceğini unutmayın.
- ✔ Yaptığınız yatırımları 7/24 göz altında tutan; 'hemen satayım', 'şimdi alayım', 'buradan çıkıp şu alt-coine gireyim', 'şu alarmı kurayım'... şeklindeki düşüncelerden her zaman uzak durun. Bu düşünceler sizi içinden çıkılmaz bir takip saplantısına, bu saplantı da geri dönüşü çok zor bir bağımlılığa sürükleyebilir.
- ✔ "Bir fiyatına Beş Bitcoin", "1500 TL yatır, ayda 300 TL madencilik geliri garanti" gibi reklamlara sakın kanmayın! Böyle bir dünya yok ve asla olmayacak.
- ✔ Sadece güvenilir ve referanslı kaynaklardan yatırımlarınızı yapın.
- ✔ Mümkün olan en kısa sürede yatırım yaptığınız ana parayı sistemden alarak, elinizde kalan kripto paraları sadece deneyim ve gözlem için kullanın.

Yukarıdaki kurallara uyduğunuz takdirde, bir borsaya kaydolmak, cüzdan sahibi olmak, kripto para transferi yapmak ve dünyayı takip etmek size bu kitabın veya farklı hiçbir kaynağın veremeyeceği kadar eşsiz bir deneyim ve tecrübe kazandıracaktır.

Kripto Para Birimlerinde ABD Dolarının Ötesine Ulaşmak

Kripto para birimlerinin yapısı, dijital platformlarda çerçevesi belirlenmiş olan verinin üretilmesi, saklanması, kopyalanmaya ve çalınmaya karşı korunması, gizlilik ve anonimlik gibi oldukça kompleks problemlerin çözümlerini

sunmaktadır. Bu yapıların, finans ve bankacılık sisteminin ötesinde paraya bakış açımızı ve şu anda hayatımızda olduğu kadar gelecekte keşfederek hayatımıza dahil edeceğimiz pek çok çözümü ve faydayı sunması kaçınılmaz bir gerçektir. Bu gerçeği görmezlikten gelemeyiz, zaten bu sebeple tüm dünyada başta finans ve bankacılık sistemi olmak üzere, pek çok endüstri ve devletler bu alanlarda araştırmalar yapıyor ve yatırımlar gerçekleştiriyor.

Blockchain ağları, bu ağlar üzerindeki birer uygulama olan kripto paralar, Token çözümleri gibi yapılar, kendilerine pek çok uygulama alanı bulacaklar. Bir saniye! Token mı? O da ne? Haydi şimdi bu soruyu cevaplayalım.

Token Nedir? Kripto Paralardan Farklı mıdır?

Token kelimesi, İngilizce bir kelime ve Türkçe karşılığı "Jeton". Ancak gerek Blockchain dünyasında, gerekse kavramsal olarak kullanıldığı diğer sektörlerde, Token standart bir ifadeye dönüştüğü için biz de Token kelimesini kullanmaya devam edeceğiz.

Token, temel olarak bir aidiyete aracılığı ifade ediyor. Yani herhangi bir şeye sahip olmanın göstergesi olarak ifade edebiliriz. Bu gösterge ile birlikte Token, aynı zamanda el değiştirme imkanı da sağlıyor.

Çocuklar (ya da büyükler için) tasarlanan eğlence salonlarında makineleri kullanmak için para verip jetonlar satın alıyoruz. Daha sonra bu jetonları makinelere atarak onları çalıştırıyoruz. Aslında jetonların hizmet ettiği şey, eğlence makinelerine erişim hakkı sağlamak. Her bir makine için ayrı ayrı hak satın almaktansa bir jeton alarak dilediğimiz makinede kullanabiliyoruz. Eğer jetonlarımızı arkadaşlarımızla paylaşmak istersek bir takas yapabilir veya hediye de edebiliriz.

Dijital dünyada ise Token gerçek dünyada jetonlara benzer hizmetler sağlayan veri kayıtları ve aracıları olarak ele alınabilir. Örneğin Bankalararası Kart Merkezi tarafından sunuluna BKM Express dijital cüzdanı, kendi içinde kredi kartı bilgilerinizi saklamaz. BKM Express cüzdanınız ile çevrimiçi bir

ödeme yapmak istediğinizde sizin hesabınız ve cüzdanınıza bağlı bir Token oluşturulur ve bu Token, BKM sunucularına gönderilir, sunucular üzerindeki uygulama çalışarak kart bilgilerinizi ve bakiyenizi kontrol eder ve alışveriş için tüm şartlar uygunsa satışı yapan şirkete onay bilgisini içeren bir mesaj gönderilir. Kart bilgisi hiçbir zaman transfer edilmez, bunun yerine kart ve sizin kimliğiniz arasında ilişki kuran dijital Token seyahat eder. Bu yöntem, güvenliği en iyi hale getirir.

Token açıklamasını tekrar hatırlayalım; "transfer edilebilen bir aidiyet veya sahiplik aracısı" diyoruz. Bu durumda geçen bölümde detaylı şekilde izah ettiğimiz para kavramı da aslında bir sahiplik ve transfer edilme özelliğine sahip olduğu için Token tanımına uyuyor. Bu durumda tüm para birimleri ve kripto paraların da birer Token olduğunu ifade etmemiz yanlış olmaz. Ancak her Token bir para birimi değildir. Para temel olarak dört niteliği bir arada sunar; bir hesap ölçüsü olmak, bir takas aracı olmak, değer saklamak ve sözleşme aracısı olmak. Tokenlar bu dört niteliğin dördünü de sağlayabilir, ancak her zaman dördünü birden sağlamak zorunda değildir. Farklı amaçlara hizmet etmek için beş farklı Token tipi bulunmaktadır.

Kullanım (Usage) Token: Bir servise ulaşmak, bir ürünü satın almak için kullanılırlar. Hediye Kartları ve yazılım lisansları bu türe örnek verilebilir.

Hak (Equity) Token: Sahiplerine bazı haklar sağlar. Örneğin bir şirketin gelirlerinden kâr almak veya seçimlerde oy vermek gibi.

Çalışma (Work) Token: Sahiplerine bir işe katkı sağlama imkanı verir. Bu katkı karşılığında ise ortaya çıkan sonuçlardan fayda elde edilebilir.

Topluluk (Community) Token: Sahiplerine belli bir topluluk içinde statü sağlar. Topluluğun kurallarını belirleme veya hizmetlerinden faydalanma imkanı verebilir. John Wick filmindeki sikkeler buna örnek gösterilebilir.

Varlık (Asset) Token: Gerçek yaşamda fiziksel bir karşılığı ifade eden Token tipidir. Örneğin bir emlak sahibi olmak, bir araç sahibi olmak gibi. Tapu veya ruhsat gibi çok temel belgeler bu tarz Token yapısına örnek verilebilir.

Blockchain teknolojisi farklı amaçlara hizmet edebilecek bir altyapı sunmaktadır. Bu amaçlar içinde aynı anda hepsine birden veya ayrı ayrı özelliklerine göre farklı Token tiplerine hizmet edebilecek Blockchain çözümleri geliştirmek mümkündür.

Mini Özet

Artık para kavramını, token kavramını, kripto para kavramını ve ne ifade ettiklerini daha iyi biliyoruz. Neden binlerce farklı kripto paranın ortaya çıktığı, birbirlerinden hangi noktalarda farklılaştıkları ve neden bu kadar çok ilgi çektikleri üzerine değerlendirmeler yaptık. Kripto paraların mevcut finansal sistemi tehdit etmediklerini ama dönüştürücü ve değiştirici bir etkiye sahip olacaklarını da daha iyi kavradık. Bu dünyaya uzak kalmayarak yatırım yapmanın ve bu yatırımı yaparken dikkat edilmesi gereken noktaların da üstünden geçtik.
Sürekli ifade ettiğimiz gibi Bitcoin bize Blockchain kavramının doğmasını sağlayan süreci hediye etmiştir. Aynı zamanda Bitcoin sayesinde gayet iyi biliyoruz ki Blockchain teknolojisi sadece bir makale ve önerme olmanın ötesine geçerek, başarıyla çalışan bir çözüm platformu sunmaktadır.
Bu sebeple Blockchain teknolojisinin kullanılabileceği pek çok alan bulunmaktadır. Şimdi birlikte, bu uygulama alanlarına sırasıyla göz atacağız.

1.4. Blockchain Uygulama Alanları

Kökleri 1990'lı yıllara kadar uzanan Blockchain teknolojisinin değeri, Bitcoin ortaya çıkana kadar pek anlaşılamadı. Bitcoin uygulamasının bir kripto-para çözümü olmasından dolayı Blockchain kavramı öncelikli olarak finansal teknolojiler alanında yorumlanıp değerlendirilmiş olsa da, durum bundan biraz farklı.

Artık kesin olarak biliyoruz ki Blockchain yoğun olarak finansal çözümler için kullanılabilir olsa da, bunun ötesinde pek çok farklı uygulama alanına sahiptir.

Bir önceki bölümde, temel olarak Blockchain türleri ve kısmen aktif kısmen farazi bazı örnekleri paylaştık. Bu bölümde Blockchain teknolojisinin kullanılabileceği uygulama alanlarını daha geniş çerçevede ele almak istiyoruz ki bu teknoloji hak ettiği ilgiyi görebilsin.

Şimdi Blockchain teknolojisinin farklı uygulama alanlarına başlıklar halinde birlikte göz atalım. Başlamadan önce belirtmeliyiz ki bu bölümde göreceğimiz uygulama alanlarını, ilerleyen bölümlerde "Blockchain Uygulamaları" başlığı altında gerçek hayattaki örnekleri ile de ele alacağız.

Kripto Para ve Token Çözümleri[14]

Bitcoin ile başlayan ve binlerce farklı kripto para ve Token uygulaması ile popüler hale gelen Blockchain uygulamaları içinde hâlâ en çok konuşulan ve hayata geçirilen uygulama alanı fiziksel paranın dijital dünyaya taşınmasıdır. Temelde aracı kurumların ortadan kalkması ve merkezi olmayan üretim yöntemleri ile bağımsız bir değer üretilmek hedeflense de, Blockchain teknolojisi devletlerin, özel bankalar üzerinden üretimini ve merkez bankaları üzerinden basımını gerçekleştirdikleri resmi para ile ilgili süreçleri de Blockchain altyapısına taşımalarına imkan verecektir. Paranın dijitalleşme sürecini hızlandırma kapasitesi, paraya bağlı bankacılık ve finans hizmetlerini genele yayma ve herkesin erişimine daha çok ulaştırma kapasitesi ile Blockchain, nakitsiz bir yaşama geçişte büyük önem taşımaktadır. Farklı Token çözümleri ise yenilikçi finansal servislerin hayatımıza girmesine olanak sağlamaktadır. Yeni bir sermaye aracı olarak **ICO** (ICO başlıklı özel bölümde detayları ile ele alınacaktır) gibi kavramlar şimdiden hayatımıza girmiştir. İçlerinde Türkiye'nin de bulunduğu pek çok devletin merkez bankaları, özel bankaları ve ilgili kurumları, kripto paralar üzerinde çalışmalar yapmakta ve ICO gibi yenilikçi kavramların güvenli şekilde sunulması için yasal çalışmalar yürütmektedir.

---

[14] *Bu başlık özelinde Bankalararası Kart Merkezi tarafından yayınlanan ve ücretsiz sunulan "Paranın Serüveni" isimli çalışmayı ayrıca okumanızı şiddetle tavsiye ederiz.*

Dijital Kimlik

Internet ve onu takip eden mobil teknolojiler devrimi ile birlikte hayatımıza giren ve hızla yayılan dijital servisler, fiziksel dünyadaki kimlik kavramının bir dijital kopyasına ihtiyaç duyulmasına neden olmuştur. Bu konuda kullanılan çözümler, temel olarak merkezi bir yapı içerisinde kimlik bilgilerinin saklanmasını ve dış servislere kontrollü bir şekilde sunulmasını sağlamaktadır. Ancak bu yaklaşım, bu yeni dijital dünyanın ihtiyaçlarını tam olarak karşılamamaktadır.

Bir örnek ile izah etmek gerekirse şu anda bazı eğlence merkezlerine girmek için kimlik belgemizi gösteriyoruz, bu süreçte tüm kimlik bilgimizi eğlence merkezi ile paylaşmış oluyoruz. Oysa kontrol edilmesi gereken tek şey bizim 18 yaşından büyük olup olmadığımız.

Blockchain teknolojisini ve akıllı sözleşmeleri kullanan, merkezi olmayan bir kimlik kayıt ve doğrulama sistemi kurularak, kimlik sahibinin onayına bağlı olarak kimlik bilgilerinin tamamı veya sadece belirli bir kısmı paylaşılabilir. Farklı bir ifade ile eğlence merkezine, güvenli ve doğrulanmış olarak, sadece yaş bilgimizi sunabiliriz.[15]

Müşteri Tanıma (Know Your Customer - KYC)

Başta finansal kurumlar olmak üzere pek çok işletme, müşteri kazanımı ve kayıt süreçleri kapsamında, yasal olarak müşterilerine ait bilgileri toplamak zorundadırlar. Bu bilgiler genellikle temel kimlik bilgilerinin ötesinde müşteriye ait davranışsal ve tercihlere bağlı bilgiler olabilir. Müşterinin bilgileri farklı bir kurumda tanımlı olsa bile her kurum kendi içerisinde, bağımsız bir şekilde, bu süreci çalıştırmak ve bu bilgileri toplamak zorundadır. Bu durum, "müşteri tanı" sürecini maliyetli ve verimsiz bir duruma çevirmektedir.

[15] Bu konu ile alakalı olarak Bankalararası Kart Merkezi tarafından yayınlanan ve David Birch'ün kaleme aldığı "Kimlik: Yeni Para" isimli kitabını okumanızı şiddetle tavsiye ediyoruz.

Müşteri bilgilerinin tutulduğu bir Blockchain ağı üzerinde, bir müşteriye ait bilgilere ihtiyaç duyulduğu durumlarda, müşteri onayı ile birlikte, bilginin talep eden ilgili kuruma aktarılması sağlanabilir. Bu yapı sayesinde, müşteri bilgilerinde oluşabilecek en ufak bir değişiklik bile bu kayda erişme yetkisine sahip tüm kurumlara gerçek zamanlı şekilde yansıtılabilir. Bu yapı, mevcut duruma göre daha düşük maliyetli, verimli ve yetenekli bir çözüm sağlar.

Küresel Ödeme Sistemleri

Küresel ödeme sistemi pazarı, 2017 yılında yaklaşık 630 milyar dolar büyüklüğüne ulaşmıştır ve ortalama yıllık yüzde 5 büyüme göstermektedir. Şu anda küresel para transferlerinin mevcut yapısı incelendiğinde, özellikle göndericisinden alıcısına giden yoldaki farklı aracı kurumlardan dolayı, küresel para transferleri uzun zaman almakta ve yüksek maliyetler ile gerçekleştirilebilmektedir. Öte yandan mevzuata uyumluluk kontrolü/ raporlaması noktalarında sıkıntılar olduğu gözlemlenmektedir.

Burada oluşturulacak Blockchain ve Akıllı Sözleşme tabanlı yeni bir akış ile birlikte, bu ödemelerin gerçek zamanlı, daha az katılımcı ile daha düşük maliyetli ve Blockchain üzerinde tüm işlemlere erişim yeteneği ile daha basitleştirilmiş, ilgili kurumlar tarafından kolay kontrol edilebilen bir yapıya getirilmesi sağlanabilir.

Girişimler İçin Sermaye İhtiyacı Karşılama

Genel olarak girişimler sermaye ihtiyaçlarını çeşitli seviyedeki yatırımcılar ve fonlar ile yaptıkları çeşitli anlaşmalar ile karşılamakta, bu kapsamda aldıkları yatırım karşılığında çeşitli oranlarda hisse devri yapmakta, çeşitli haklar vermektedirler. Son yıllarda bu duruma bir alternatif olarak kitle fonlama (crowdfunding) modeli ortaya çıkmış, bu modeli uygulayan çeşitli platformlarda (Kickstarter, Crowdcube vb.) milyonlarca dolar ile ifade edilebilecek başarı öyküleri (Pebble, Monzo vb.) gerçekleşmiştir. Ancak

bu modellerde de aracı bir kurum olmasından dolayı, çeşitli ek koşullar ve ücretlendirmeler söz konusudur.

Blockchain yaklaşımının ortaya çıkması ile birlikte firmalar, sermaye ihtiyaçlarını karşılamak için herhangi bir aracı kuruma ihtiyaç duymadıkları, kendi yönettikleri yeni bir alternatif modele sahip oldular.

Bu modelde ilk olarak ilgili firma amacına hizmet edecek niteliklere sahip "**Token**" yaratır. Daha sonra bu Tokenların satışını gerçekleştirip sermaye ihtiyacını karşılayabilir. Bu yeni finansman modeline **ICO** (Initial Coin Offering) adı verilmiştir. ICO konusuna özel bir bölümümüz olduğu için şimdilik bu sürecin detaylarına girmiyoruz.

Bağış Toplama ve Yönetimi

Günümüzde hayır kurumları üzerinden yürütülen işlemlerin büyüklüğü ciddi seviyelere ulaşmıştır. Sadece Amerika Birleşik Devletleri'nde her yıl, 400 milyon dolar seviyesinde bireysel bağış gerçekleşmektedir. Hayır kurumları üzerinden gerçekleştirilen bu bağış akışının kapalı yapısı, özellikle bir güven sıkıntısı ortaya çıkarmakta, insanlar üzerinde bağış yapmaktan uzaklaştırıcı bir etki oluşturmaktadır. Ayrıca ihtiyaç duyulan çeşitli aracı kurumlardan dolayı, bağışların kullanımlarında ciddi kesintiler oluşmakta, kurumlar arası aktarımlar sırasında uzun işlem süreleri yaşanabilmektedir.

Blockchain tabanlı bir bağış yapısı oluşturulması ile daha şeffaf, işlem maliyeti daha düşük bir süreç yaratmak mümkün. Aracı kurumların azaltılması ile birlikte yapılan bağışlar üzerinde çok daha az kesinti yapılması, ihtiyacı olan kişilere/yerlere neredeyse gerçek zamanlı bir şekilde kaynakların ulaştırılması, bunun yanı sıra bağışçıların yaptıkları bağışları herkese açık olan Blockchain platformları üzerinden takip ederek, gerçekten hedefine uygun bir şekilde kullanıldığını denetleyebilmesi ve bu şekilde kaybolan güven duygusunun tekrardan tesis edilmesi sağlanabilir. Ayrıca ilgili mevzuat kapsamında yapılan kontroller, çok daha etkili ve verimli bir şekilde gerçekleştirilebilir.

Vergi Toplama ve Yönetimi

Nakit kullanımının pek çok toplumda hâlâ önemli bir paya sahip olması sebebiyle, ticari ve kişisel faaliyetlere bağlı vergi beyanı ve ödemeleri hâlâ önemli bir süreç gerektirmekte, ticari işletmeler bu süreçler için mali müşavirlerin denetiminde hareket etmek durumunda kalmaktadır. Nakitsiz yaşam politikası ve hedefleri ile fiziksel paradan tümüyle kurtulduğumuz, tüm para süreçlerinin dijital dünyada gerçekleştiği bir ideal senaryoda, Blockchain Platformları üzerinde sunulan akıllı sözleşmeler sayesinde gerçek zamanlı olarak vergi hesaplaması yapılabilir ve hatta tahsilat da aynı şekilde gerçekleştirilebilir. Bu tarz çözümler devletlerin hem kayıt dışı ekonomiyi ortadan kaldırmasını sağlarken hem de vergi toplama süreçlerini hızlandırabilir. Elbette bu tarz bir çözümün, vergi dağılımında daha eşitlikçi ve adaletli politikaların uygulanmasını kolaylaştırma etkisi de olacaktır. Bu tarz bir ideal yapıda, toplum içinde gelir ve hizmet dağılımı da mükemmel hale gelecek ve toplumdaki huzur ve güven katsayısının yükselmesi beklenebilecektir.

Mal ve Kaza Sigortası Tazmin Süreci

Mal ve kaza sigortaları, sigortacılık sektörü içerisinde yaşam ve sağlık sigortaları sonrasındaki en büyük hacmi oluşturmaktadır. Beklentilere göre 2018 yılında bu tür sigortaların tahmini toplam büyüklüğü, yaklaşık 895 milyar dolara ulaşacaktır. Şu anda mevcut tazmin süreci incelendiğinde, özellikle aracılardan kaynaklanan bir yüksek gecikme ve maliyet, taraflar arasında bilgi paylaşım yapılarının yetersizliği nedeni ile dolandırıcılık riski ve tekrarlanan işlemler, bütün bunların yanı sıra üçüncü taraf veri sağlayıcılara bağımlılıktan dolayı süreci destekleyen verileri oluşturmanın zorlukları gibi sıkıntılar olduğu gözlemlenmektedir.

Burada oluşturulacak Blockchain ve Akıllı Sözleşme tabanlı yeni bir akış ile birlikte başvuru süreçleri basitleştirilebilir. akıllı cihazlar ve IoT[16] uygulamaları ile

[16] *Internet Of Things; Nesnelerin Interneti. Sadece tüm cihazların ve eşyaların internete bağlanması değil aynı zamanda bu kaynaklar üzerindeki alıcılardan gelen verilerin kaydedilmesi ve işlenerek anlamlı bilgilere dönüştürülmesi sürecini de ifade etmektedir.*

bu süreç otomatikleştirilebilir, aracı ihtiyacı ortadan kaldırılıp bunların getirdiği gecikme ve maliyet süreçten çıkarılabilir, güvenilir veri kaynaklarına yapılacak bütünleştirme ile birlikte destek verilerinin oluşturulması en düşük insan kontrolü içerecek bir hale getirilebilir, çoğu durum için akıllı sözleşmelerin ödeme işlemine kadar tüm süreci otomatik olarak yönetip tamamlaması sağlanabilir.

Kişiden Kişiye (P2P) Kredi Uygulamaları

Geleneksel yapılarda, kredi hizmetleri ve servisleri için düzenleyici kurumlardan lisans almış bankalar ve çeşitli finans kurumları bu hizmetleri sağlar. Ancak Blockchain güvenli bir veri kayıt sistemi sunduğu için, aracı kurumlara ihtiyaç duyulmadan bireyler arasında kredi verilmesi sağlanabilir. Tüm kayıtlar inkar edilemez şekilde süreci gösterirken, kredi veren ve alan kişilerin davranışları sistem içerisinde saygınlıklarının artması ile birlikte sistemin giderek daha güçlü ve güvenli hale gelmesini sağlayacaktır. Bu tarz P2P kredi servislerinde KYC aşamaları aynı veya farklı Blockchain platformlarında tutulabileceği gibi geleneksel lisanslı kurumlar ile iletişim kurularak da sağlanabilmektedir.

Mikro Finans Hizmetleri

Bankacılık servislerinin bulunmadığı, bu servislere erişimin zor olduğu koşullarda veya geleneksel bir finansman kurumunun ilgi alanına girmeyen çok düşük tutarlarda finansman ihtiyacının olabildiği çeşitli durumlar oluşabilmektedir. Örneğin bir Afrika köyünde sadece iki tavuk alarak bunların bir hafta boyunca ürettiği yumurtaları satarak para kazanmak isteyen bir köylü olabilir. Bu gibi durumlarda 10 doların altında finansman kaynaklarının sağlanması büyük önem taşımaktadır. Blockchain uygulamaları bu tarz kredilerin sağlanmasında rol oynayabilmektedir. P2P krediler veya kurumların mikro finans sağlayabildiği senaryolar dahilinde bu tarz servisler verilebilir. Blockchain teknolojisinin sağladığı imkanlar ile bu tarz servisler bölgesel olmanın ütesinde küresel ölçekte işletilebilir.

Şans ve Bahis Oyunları

Kura ve şansa dayalı oyunlar ve bahisler gibi alanlarda mekanik veya yazılıma bağlı çözümler kullanılmaktadır. Ancak bunların tamamı düzenli olarak takip edilmeli, kontrolleri yapılmalı veya çekilişler noter gibi kurumların gözetiminde gerçekleşmelidir. Oysa Blockchain uygulamaları üzerinde yer alan Akıllı Sözleşmeler ile matematiğin sağladığı rastlantısal hesaplamalar kullanılarak, bu tarz bahis ve şans oyunlarına yönelik servisler sağlanabilmektedir. Bu tarz uygulamaların, eğer yazılım kaynaklı bir açık ve hata yoksa, aldatılması veya manipüle edilmesi, bozulması imkânsızdır.

Sendikasyon Kredisi

Sendikasyon kredi pazarı 2017 yılı rakamlarına göre yaklaşık 5 trilyon doların üstüne çıkmıştır. Şu anda mevcut olan akışa bakıldığında, özellikle kredi talep eden kurumun ve katılımcı kurumların incelenmesinde elle yürütülen işler, hizmet veren aracı kurumların getirdiği maliyetler, sistemler arasındaki iletişim eksikliği ve uyumsuzluk kaynaklı tekrar eden eylemler gibi çeşitli sıkıntılar gözlemlenmektedir.

Burada oluşturulacak Blockchain ve Akıllı Sözleşme tabanlı yeni bir akış ile birlikte, kredi talep eden firmaya ait bilgiler, katılımcı kurumlar tarafından daha açık ve efektif bir şekilde değerlendirilebilir. Aynı şekilde, katılımcı kurumlara ait finansal ve risk tolerans bilgilerinin Blockchain çözümleri üzerinde tutulması ile seçim işlemi akıllı bir sözleşme kapsamında otomatikleştirilebilir, akıllı sözleşmelerle aracı kurum ihtiyaçları azaltılıp, maliyet ve gecikmeler en düşük hale getirilebilir. Ayrıca, mevzuat ile ilgili kontrollerin ilgili kurumlar tarafında daha kolay ve hızlı bir şekilde gerçekleştirilmesi sağlanabilir.

Otomatikleştirilmiş Uyum Mekanizması

Finansal kurumlar, çeşitli mevzuat gereksinimlerine uymak ve gerekli bildirimleri yapmak ile yükümlüdürler. Bu konuda genel olarak denetleme

firmaları ile çalışılmaktadır. Bu yapıda denetleyicilerin ilgili verilere erişimi, bu veriler üzerinde inceleme yapması, geri bildirim akışı içerisinde tekrarlı işlemler, sonuçların entegrasyonu gibi adımlarda süre, maliyet ve firma verimliliği açısından çeşitli sıkıntılar gözlemlenmektedir.

Finansal verilerin tutulduğu bir Blockchain uygulama yapısı ile birlikte denetleyicilerin, ihtiyaç duydukları bilgilere firma kaynaklarını (çalışan gibi) engellemeden erişebilmesi, denetlemelerin kurulacak bir entegrasyon yapısı üzerinde denetim yazılımları ile otomatikleştirilmesi, elle yapılan işlemlerin kaldırılması ile birlikte potansiyel hata alanlarının daraltılması sağlanabilir.

Oy Kullanma ve Vekaleten Oy Kullanma

Blockchain teknolojisinin çözüm sağladığı alanlardan birisi de, oyların toplanması ve kayıtların tutulmasını sağlamak üzere, oylamalarda karşımıza çıkıyor. Blockchain teknolojisi ile geliştirilen oylamaya yönelik uygulamalar; anonim kayıtların tutulması, kimlik doğrulaması ve tekil oy kullanımı gibi gereksinimlere tam olarak cevap verebiliyor.

Vekaleten oy kullanma yapısında ise uzaktaki yatırımcılar, yıllık hissedar toplantılarında tartışılan konular hakkında, katılım sağlayamasalar bile oy kullanabiliyor. Bu süreç kapsamında, uzaktaki yatırımcıların bilinçli karar vermelerini sağlamak için, gerekli bilgilerin iletilmesi ilgili firmaların sorumluluğundadır. Bu yapıda, gerekli bilgilerin doğru bir şekilde aktarımı, yatırımcıların kolay bir şekilde oy kullanma sürecine katılımı, katılım sürecinin şeffaflığı gibi alanlarda çeşitli sıkıntılar gözlemlenmektedir.

Oylama çözümlerinde olduğu gibi, vekaleten oylama süreçlerinde de Blockchain ve Akıllı Sözleşme tabanlı çözümler kullanılabilir. İlgili firmanın hisse yapısını da içeren yatırım kayıtlarını tutan bir platform ve bu yapı üzerinde çalışan akıllı sözleşmeler, tüm yatırımcılara ilgili bilgilerin dağıtılmasını sağlar. Oylama, farklı kanallardan gerçekleşse bile, sonuçlar

tek bir ara entegrasyon katmanı ile birlikte Blockchain uygulamaları üzerinde tutularak, bu sonuçların gerçek zamanlı olarak ilgili kurum ve/veya yatırımcılar ile paylaşılması ve bu sayede yukarıda belirtilen sıkıntıların ortadan kaldırılması sağlanabilir.

Tedarik Zinciri Yönetimi

Günümüzde uygulanan geleneksel tedarik zincir yapısına bakıldığında, üreticilerin ve tüketicilerin silo yaklaşımı kapsamında ağırlıklı olarak kendi iç akışlarına odaklandıkları, tedarik zinciri boyunca her adımda karışık entegrasyon ve bilgilendirme süreçlerinin yer aldığı, bunlardan dolayı süre, maliyet ve firma verimliliği açısından çeşitli sıkıntıların yaşandığı, kontrolü oldukça zor bir yapı ile karşılaşılmaktadır.

Blockchain tabanlı bir yapı ile birlikte, bir ürünün imalattan satışa kadar olan her el değişimi, kalıcı bir ürün geçmişi yaratılarak belgelenebilir. Bu sayede, zaman gecikmelerini, ek maliyetleri ve bugünkü işlemleri engelleyen insan hatalarını önemli ölçüde azaltmak mümkün olabilir. Akıllı sözleşmeler kullanılarak, bir ürünün zincir üzerindeki hareketi sırasında otomatikleştirilmiş kontrol ve eylem akışları gerçekleştirilebilir (bir ürünün X aşamasına gelip Y kontrolünü geçmesini takiben Z birim para transferinin gerçekleştirilmesi gibi). Müşteri gözü ile değerlendirdiğimizde, kullanıcıların aldıkları ürünün kendilerine geliş süreci hakkında bilgi sahibi olup daha bilinçli bir şekilde karar vermeleri sağlanabilir.

Telif Kayıt Sistemleri

Blockchain ağları üzerindeki mutabakat sistemleri sayesinde dijital içeriklerin telif kayıtlarının yapılması, kontrol edilmesi ve kopyalanması durumunda bunun anlaşılması için çözümler oluşturulabilir. Bu şekilde, dijital dünyanın en büyük problemlerinden birisi haline gelen, telif hakları içeren verilerin gerçek sahipleri tarafından tescil edilmesi sorunu ortadan kalkabilecektir.

Kopya Ürün Koruması

Dijital eserler olduğu kadar fiziksel ürünler için de sahteciliğin önüne geçmek için Blockchain teknolojisi kullanılabilir. Fiziksel ürünlere ait tedarik ve üretim süreçleri, Blockchain ağları üzerinden kayıt altına alınırken, tüketiciler satın aldıkları ürünlerin orijinal veya kopya olup olmadığını, ürünlere iliştirilen ve zarar vermeksizin sökülmesi imkansız NFC çipleri ile teyit edebilirler.

Kamu ve Sağlık Kayıtları ile İhaleler

Blockchain ağları her türlü kamusal ve sağlık alanındaki kişisel mahremiyet içeren, acil durumlarda farklı merciler tarafından erişilmesi gereken verilerin saklanması ve tutarlılığının sağlanması için kullanılmaya gayet müsaittir. Benzer şekilde devlet tarafından açılan ihaleler ve bu ihalelerde atılan adımlar Blockchain ağları üzerinde kaydedilebilir. Bu yaklaşımlar, aynı zamanda rüşvet, yolsuzluk gibi süreçleri de engellemekte ve kamusal süreçleri şeffaflaştırmaktadır.

Askeri Emir Komuta Zincirleri

Askeri yapılarda bugün emir komuta zinciri içindeki iletişim ve bilgi teyidi için yüksek kriptografik çözümler kullanılmakta, ancak buna rağmen emir komuta süreçlerinde aksamalar ve yanıltıcı durumlar ortaya çıkabilmektedir. Bir grup askere iletilen bir emrin, merkezi karargâhtan mı geldiği yoksa aradaki bir müdahale ve yanıltma ile mi gerçekleştiği, Blockchain ağları ile kayıt altına alınarak rahatlıkla takip edilebilirken, bu sistemlere bağlanacak Akıllı Sözleşme katmanları ile kolaylıkla kontrol edilebilir ve onaylanabilir.

Güven Protokolü Gerektiren Tüm Alanlar

Blockchain teknolojisi temel olarak bir "Güven Protokolüdür". Birden fazla kişi veya tüzel yapı arasında güven gerektiren tüm kayıtların

tutulması, taşınması, paylaşılması, yetkilendirme ve doğrulama işlemlerinin yapılması için kullanılabilir. Bu alanların belirlenmesi ve bu alanlara göre çözümlerin üretilmesi ise Blockchain mantığını anlayan ve nerelerde kullanılabileceğini iyi bilen uzmanlarca yapılmalıdır. Daha sonra ortaya çıkan planlar yazılım mühendisleri tarafından uygulamalara dönüştürülecektir.

Buzdağının Görünmeyen Kısmı

Bu bölümde Blockchain teknolojisine yönelik bazı temel potansiyel uygulama alanlarına değinmeye çalıştık, ancak bunlar kelimenin tam anlamı ile sadece buzdağının görünen kısmıdır. Hatta bu kısmın üzerinde yuvarlanmakta olan bir kartopudur diyebiliriz. Henüz keşfedilmeyi bekleyen bakir bir kıta ile karşı karşıyayız.

Anlam ve değer içeren herhangi bir varlığın, herhangi bir aracıya ihtiyaç duymadan, güvenli bir şekilde kaydının tutulması ve bu kayıtların sahipliğinin paylaştırılması veya aktarılması ile birlikte bugüne kadar henüz keşfetmediğimiz çok farklı iş modelleri üzerinde çalışmalar devam etmektedir.

Günümüzün örnek gösterilen yakın dönem yıkıcı (distruptive) girişimleri dahi Blockchain dalgasının etkisi altındadır. Ethereum platformunun kurucusu olan Vitalek Buterin'in dediği gibi "Uber, taksi şoförlerinin işini tehdit edebilir, ancak Blockchain, Uber'in varlığına ne kadar ihtiyaç kaldığını yeniden düşünmemizi mümkün kılmaktadır."

1.5. Blockchain Platformları

Artık Blockchain ağlarının yapısını, çalışma mantığını ve bu teknolojinin ne gibi amaçlar için kullanılabileceğini biliyoruz. Bu durumda kafamızdaki bir projeyi hayata geçirmek istediğimizde ne yapmamız gerekecek? Yetenekli yazılımcılardan oluşan bir ekip kurup, kendi Blockchain platformumuzu

mu geliştireceğiz? Elbette bu seçeneklerden herhangi birisi mümkün ama "Amerika'yı yeniden keşfetmeye gerek yok" yaklaşımını takip etmek daha mantıklı olur. Çünkü şu anda açık kaynak kodları ile kullanılabilecek hazır durumda çeşitli Blockchain platformları zaten bulunuyor. Bakalım bu platformlar hangileri ve hangi amaçlara hizmet ediyorlar.

Bitcoin

Blockchain kavramının hayatımıza girmesinde en temel role sahip platform, şüphesiz Bitcoin platformudur. Bitcoin aynı zamanda en çok bilinen ve tanınan Blockchain platformudur. İlk olarak Kasım 2008'de Satoshi Nakamoto adı ile yayınlanan bir makale kapsamında ortaya çıkmış, 2009 yılı başında açık bir ağ olarak faaliyete girmiştir.

Bitcoin, temel olarak P2P (uçtan uca) para transferi konusunda alternatif bir yaklaşım getirmektedir. Günümüz dünyasında para transferi yapabilmek için bankalar ya da bu konuda özelleşmiş ara kurumlar (WesternUnion gibi) hizmet sunmaktadır. Ancak bu servisleri kullanarak gerçekleşen işlemler, hem maliyetli olmakta hem de uzun sürelerde gerçekleşmektedir. Bitcoin platformunda, kripto para birimi Bitcoin (BTC) ve platforma dahil olan kişilerin dijital cüzdanları (Bitcoin adresleri) bulunmaktadır. Dijital cüzdan açmak, ücretsiz ve basit bir işlemdir. Şu anda hazır olarak bulunabilecek pek çok masa üstü veya mobil dijital cüzdan uygulaması ile saniyeler içinde bir dijital cüzdan açılabilir ve adres edinilebilir.

Oluşturulan her bir cüzdan, aslında bir adet açık bir adet gizli anahtar çiftine sahip asimetrik bir şifre sistemidir. (Asimetrik Şifreleme hakkında detaylı bilgi için Kriptolojinin Teknik Detayları bölümünü okuyabilirsiniz), açık anahtar Bitcoin platformundaki diğer herkes ile

Şekil 11: **EXODUS isimli birden fazla platformu destekleyen dijital cüzdan uygulamasının Bitcoin için oluşturduğu cüzdan adresi ve bu adrese ait QR kodu.**

bir cüzdan adresi olarak paylaşılırken gizli anahtar özeldir ve saklı tutulması gerekmektedir.

Bir kullanıcı (Ahmet) başka bir kullanıcıya (Serkan) Bitcoin göndermek istediğinde, Ahmet gizli anahtarını kullanarak bir imza oluşturur. Daha sonra Ahmet, açık cüzdan adresinden Serkan'ın açık cüzdan adresine bir transfer talimatı vererek bu imzayı ekler.

Böyle bir işlemin gerçekten Ahmet tarafından oluşturulduğu, herkes ile paylaşılmış açık anahtar ile doğrulanabilir ama ortada iki temel sorun bulunmaktadır:

✔ Ahmet'in elinde, göndermek istediği kadar Bitcoin var mı?

✔ Ahmet, elindeki Bitcoin'i birden fazla kez gönderebilir/harcayabilir mi?

İşte bu noktada Blockchain yapısı devreye girmektedir.

Bitcoin sistemindeki tüm işlemler, ağ üzerindeki herkese açık, güvenli (değiştirilemez) ve ortak bir Blockchain yapısı üzerinde tutulduğundan, hangi

hesapta ne kadar Bitcoin var sorusunun cevabına ulaşılabilir ve bu şekilde Ahmet'e ait cüzdan içinde yeterli Bitcoin kaydı bulunmuyorsa, bu işlemi yapmasına izin verilmez. Yine aynı mantık ile Ahmet'in aynı kaydı birden fazla kez harcanmasının önüne geçilir. Sistemde bulunan ve mutabakat sürecine dahil tüm diğer noktalar Ahmet'in işlemlerini kontrol eder ve eğer bu, sistemdeki kurallara uymayan bir işlem ise buna izin verilmez. Bu yapıda bir merkez yoktur ve işlemin onaylanması için kuralları baştan belirlenmiş mutabakat yapısına uygun şekilde hareket edilir.

Bitcoin ağında işlem yapılan kripto para birimi Bitcoin nasıl üretilir?

Bitcoin protokolü kapsamında, sistemde yeni Bitcoin yaratılmasının tek yolu, Bitcoin Blockchain Ağı üzerinde, yeni blok kaydının gerçekleştirilmesidir. Her bir yeni blok, ağ içindeki mutabakat sürecine katılan noktalardan birisi tarafından gerçekleştirilir. Bu kaydı gerçekleştiren noktaya, emeğinin ve bu işlemin karşılığı olarak belli bir miktar Bitcoin kaydı verilir. Tüm noktalar bu ödülü elde etmeyi hedefledikleri için, bu işlem özel bir değerin bulunmasına bağlanmıştır. Bu yaklaşım, **teşvik (incentive)** yaklaşımı olarak adlandırılmaktadır.

Satoshi Nakamoto, sistemi ilk kez tasarlarken zaman içinde kullanıcı sayısının artabileceğini ve Bitcoin üretimine ilginin yükseleceğini öngörmüştür. Bu sebeple sistemde enflasyona izin vermemek üzere bazı kurallar belirlemiştir.

Sistemin ilk faaliyete geçtiği 3 Ocak 2009 tarihinde, kaydedilen her yeni Blok başına, 50 Bitcoin üretilmekteydi. Ancak bu değerin, her 210.000 Blok üretildiğinde yarılanması kuralı getirilmiştir. Her bir blok, ortalama 10 dakikada bir üretildiğinden, 210 bin bloğun üretim süresi yaklaşık dört yıla karşılık gelir. Bu işleme yarılanma (halving) adı verilir. Bu sebeple, Bitcoin ağında ilk yarılanma 28 Kasım 2012'de gerçekleşmiş ve her 10 dakikada bir Blok üretimi başına verilen Bitcoin miktarı 25'e düşmüştür. İkinci yarılanma ise 9 Temmuz 2016 tarihinden gerçekleşmiş, ödül miktarı

12,5 Bitcoin'e inmiştir. Her dört yılda bir bu yarılanma devam edecek ve teorik olarak 2140 yılında toplam 21 milyon Bitcoin üretildikten sonra artık sistem üzerinde yeni Bitcoin kaydı gerçekleşmeyecektir, bu açıdan Bitcoin sınırlı bir emisyona sahiptir.

Nakamoto'nun yaptığı tasarım, her yeni bir bloğun oluşturulması için özel bir değer bulmayı gerektirir. Bu ancak, deneme yanılma ile bulunabilen bir değerdir. Zamanla bilgisayar sistemleri hızlandığı için sistem, zorluk seviyesini, sisteme dahil olan mutabakat noktalarının sayısına ve bu bilgisayarların işlem gücüne bağlı olarak değiştirmektedir. Bu zorluk, her 2016 blok üretildiğinde (ortalama iki hafta) yenilenir. Zorluk seviyesi, deneme yanılma işlemleri ile bulunan değerin, ortalama 10 dakikada elde edilmesini sağlayacak şekilde belirlenmiştir. Bu sebeple, her yeni blok ortalama 10 dakikada bir zincire eklenir.

Üretilebilecek toplam Bitcoin miktarı sınırlı olmakla birlikte Bitcoin, kendi içerisinde daha ufak birimlere bölünebilir. Örneğin en küçük Bitcoin birimi, bir Bitcoin'in yüz milyonda biri olan "Satoshi"dir.

Bitcoin Blockchain Ağı'nın yapısı temel olarak; sınırlı ve kontrollü üretilebilen bir veri kaydının (kripto para biriminin) oluşturulması, bu kayıtların kopyalanmadan ve bozulmadan sahipliğinin belirlenmesi, bu sahipliğin başka sahiplere aktarılması üzerine kuruludur. Bununla birlikte, Bitcoin Blockchain Ağı'ndaki kayıtlarda zaman damgası ile beraber çok basit yazılımsal imkanlar sunulmakta ve üzerinde çok kısıtlı da olsa çeşitli iş akışlarının çalışması mümkün olmaktadır. Uygulama örneklerinde detaylı olarak bahsedilen Everledger, Proofstack gibi çözümler, Bitcoin ağını bu şekilde kullanan ve amacı kripto para transferi olmayan birer uygulamadırlar. Bitcoin Blockchain kodu açık kaynaklı olup, indirilebilir ve yeni alt-coin türleri üretmek veya farklı amaçlara hizmet etmek için değiştirilebilir. Ancak dünyada yaygın olarak çalışmakta olan ana Bitcoin Ağı, Bütünüyle İzin Gerektirmeyen bir Blockchain Ağı olarak çalışmaya devam etmektedir.

Ethereum

Bitcoin platformunun sağladığı altyapının belirli bir iş modelinin gerçekleştirilmesi (eşler arası kripto para transferi) için tasarlanmış olması, sahip olduğu yeteneklerin farklı alanlar için kullanılmasını sınırlandırmaktadır. Bu kısıtların ötesine geçebilmek için kod bazında özelleştirilmiş Blockchain yaklaşımları, Bitcoin platformu üzerinde çalışan yeni özel protokollerin hazırlanması gibi yöntemler takip edilmiş ama tüm bu alternatiflerin sadece kendi özel amaçlarına çözüm getirdikleri ve her yeni alternatif için yüksek bir maliyetin karşılanması gerektiği gözlemlenmiştir. "Bitcoin gerçek dünyanın ihtiyaçlarına tam olarak cevap vermekten uzak" diyen Vitalik Buterin, bu ihtiyaçları tanımlayarak daha 19 yaşındayken Ethereum platformunu tasarlamış ve bir alternatif olarak sunmuştur.

Ethereum, uygulama geliştiricilerin hazır senaryoların ötesinde merkezi olmayan uygulamaları geliştirmesine ve devreye sokmasına olanak tanıyan yenilikçi bir Blockchain platformudur. Ethereum'un yaratıcıları, Bitcoin'i "1. Nesil Blockchain", Ethereum'u ise "2. Nesil Blockchain" olarak tanımlamaktadırlar.

Ethereum platformunda, Bitcoin platformundaki "harcanmamış işlem çıktısı" (unspent transaction output – UTXO) yaklaşımından farklı olarak, "hesap" (account) yaklaşımı kullanılmaktadır. Bu sayede hesap yönetiminde alan verimliliği, işlem akışlarında bakiye sorgulama ve hesaplar arasında transfer işlemi gerçekleştirmede avantaj sağlanmaktadır.

Ethereum ağ yapısında her makine Ethereum Virtual Machine (EVM) adı verilen bir sanal makine çalıştırır. Bu sanal makine, Ethereum tarafından sağlanan özel üst seviye programlama dilleri (Solidity, Viper, Serpent gibi) ile yazılmış herhangi bir uygulamanın Ethereum yapısı üzerinde çalışmasına izin vermektedir. Ethereum tarafından sağlanan dil yapıları "Turing-complete" olarak adlandırılan bir özelliğe

sahip olduklarından, teorik olarak gözlemlediğimiz her şey Ethereum içerisinde bir program olarak hazırlanabilmektedir (bu programlara ise temel olarak daha önce izah ettiğimiz "**Akıllı Sözleşmeler**" adı verilir).

Bu programlama yaklaşımı, çeşitli uygulamaların yazılmasına olanak sağlıyor olsa da şu andaki yapısı ile özellikle eşler arasında doğrudan etkileşimi (p2p pazar yerleri gibi) otomatikleştirmeyi veya bir ağ üzerinden koordine edilen grup tabanlı aksiyonları (karmaşık finansal sözleşmeler gibi) kolaylaştırmayı hedefleyen uygulamalar için uygundur.

Ethereum platformu, Ether (ETH) adı altında kendine ait bir kripto-para birimine sahiptir. Ether, Ethereum platformu kapsamındaki işlemlerin/uygulamaların çalıştırılmasında kullanılmaktadır, bu kullanım şekli genellikle bir motorun çalışması için benzin gerekmesi metaforu ile ilişkilendirilir. Bu yaklaşım, ayrıca Ethereum platformunun üzerinde platformun çalışmasına negatif etki yapabilecek hatalı veya kötü niyetli kullanımların etkilerini sınırlamak amaçlı olarak tasarlanmıştır.

Ethereum platformu ilk ortaya çıkışından bu yana sürekli olarak bir gelişim süreci içerisinde olmuş, sürüm planlarını (Frontier, Homestead, Metropolis, Serenity) oluşturup paylaşmıştır. İleride Serenity sürümünün devreye girmesi ile birlikte, mutabakat yapısında Proof of Work'den Proof of Stake'e doğru bir geçiş olacaktır.

Microsoft, Intel, J.P. Morgan gibi kurumlar tarafından kurulan "Enterprise Ethereum Alliance" ile birlikte Ethereum, kurumsal dünya içerisinde özel (private) Blockchain yapılarının oluşturulması adına önemli bir potansiyel sunmaktadır. J.P. Morgan bu kapsamda "Kurumsal Odaklı Ethereum" olarak nitelendirdiği Quorum ve geliştirme ortamı olan Cakeshop projelerini açık kaynak kodlu olarak yayınlamıştır.

Ethereum ayrıca, Microsoft'un bulut çözümü olan Azure üzerinde **Blockchain as a Service (BaaS)** yaklaşımı ile bir servis olarak da

sunulmaktadır. İkinci baskıyı hazırladığımız günlerde **Amazon Web Servisleri (AWS)** üzerinde de bir şablon[17] olarak sunulmuştur.

Ethereum üzerinde geliştirilen ve geliştirilmeye devam eden oldukça fazla proje bulunmaktadır. Her geçen gün büyümekte olan **Ethereum Enterprise Alliance** ile birlikte özellikle iş dünyasındaki uygulamaların çeşitlenmesi ve artması beklenmektedir.

HyperLedger

Hyperledger, Aralık 2015'te Linux Vakfı tarafından başlatılan açık kaynak kodlu bir Blockchain platformudur. Hyperledger tek bir Blockchain yapısı oluşturmak yerine kendi içerisinde farklı alt projelere destek vermektedir.

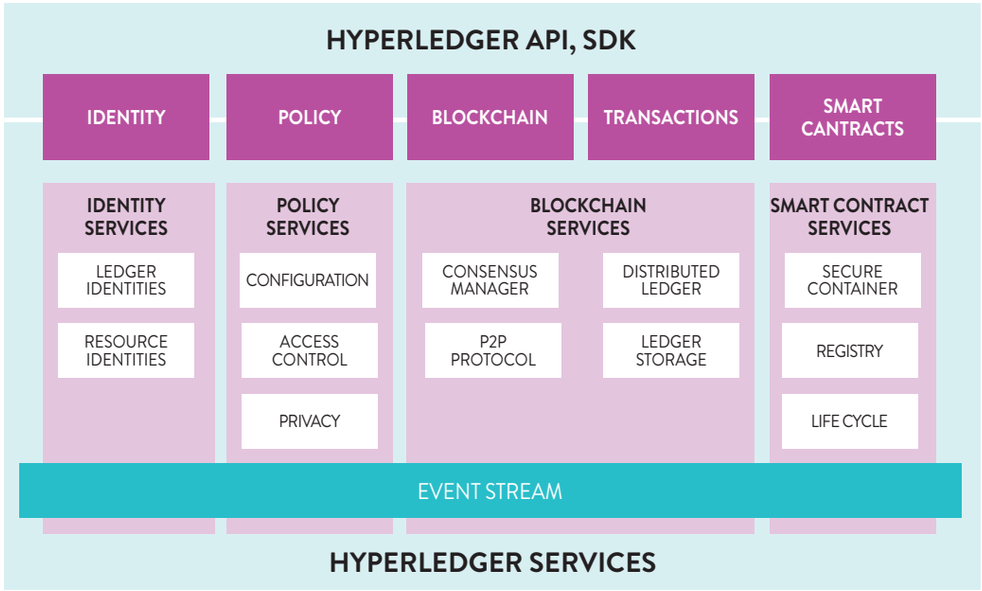
Hyperledger referans mimarisi, iki ana kısımdan oluşmaktadır. Bunlar, Hyperledger servis katmanı ve bu servisleri dış dünyanın kullanımına açmakta kullanılan Hyperledger API/SDK[18] katmanıdır.

Hyperledger servis katmanı sunduğu servisleri dört ana mantıksal kategori içerisinde değerlendirmektedir. Bunlar; Kimlik Servisleri, Hizmet Politikası Servisleri, Blockchain Servisleri ve Akıllı Sözleşme Servisleri'dir. Ayrıca alt seviyede bulunan bir haberleşme katmanı ile birlikte servis katmanı içerisinde olay güdümlü (event driven), çift yönlü etkileşim sağlanabilmektedir. Her ne kadar bu kavramlar ve yapılar kulağa oldukça karışık gelse de Hyperledger, iş dünyasının ihtiyaç duyduğu temel unsurları bünyesinde sağladığı için bugün pek çok Blockchain projesinde kullanılmaktadır. Özel bir röportaj ile sizlere sunduğumuz Bankalararası Kart Merkezinin gerçekleştirdiği kavram kanıtlama çalışması olan özel **BBN Blockchain** projesinde de Hyperledger platformu kullanılmıştır.

[17] AWS üzerinde bir hesap açtıktan sonra yapmanız gereken tek şey Ethereum ağı kurmak için bir komut vermek. Şablon (template) yapısı üzerinden AWS otomatik olarak çalışır durumda bir Ethereum ağı oluşturup size teslim ediyor.

[18] API: Application Programming Interface – Uygulama Programlama Arayüzü
SDK: Software Development Kit – Yazılım Geliştirme Kiti

Şekil 12: **Hyperledger Yapı**



Hyperledger kapsamındaki projelerin en bilinenlerinden olan **Hyperledger Fabric** projesi, IBM ve Digital Asset tarafından Hyperledger bünyesinde düzenlenen ilk Hackathon kapsamında önerilip hayata geçmiştir. Hyperledger Fabric projesinin en önemli özelliklerinden bir tanesi modüler mimarisidir, bu sayede mutabakat, üyelik servisleri gibi Blockchain modülleri ihtiyaçlara göre tak-çalıştır (plug-and-play) felsefesi ile değiştirilebilmektedir.

Henüz kuluçka döneminde olan **Burrow** projesi ise Hyperledger bünyesinde Ethereum'dan türetilmiş bir açık akıllı sözleşme yapısının geliştirilmesini amaçlamaktadır.

Hyperledger platformu giderek büyüyen bir katılımcı kitlesine sahiptir. Bu katılımcı grubu içerisinde IBM, Intel, Red Hat gibi teknoloji firmaları olduğu kadar Wells Fargo, ABN AMRO gibi finansal kurumlar da bulunmaktadır.

Hyperledger platformu da BaaS yapısı ile **Amazon Web Servisleri (AWS)** üzerinde de bir şablon olarak sunulmaktadır.

Ripple

Ripple, temel olarak gerçek zamanlı bir uluslararası para gönderim/ödeme platformudur. Uluslararası ödeme akışlarında günümüzde kullanılan Swift gibi aracı kurumların gereksinimleri ve bunun getirdiği yavaşlık, yüksek maliyet gibi yan etkileri ortadan kaldırmak amacı ile Blockchain teknolojisi kullanılmaktadır.

Ripple, diğer Blockchain platformlarında gördüğümüz "Proof of Work" ya da "Proof of Stake" (Blockchain teknik bölümünde detaylarını okuyabilirsiniz) mutabakat yöntemlerini kullanmak yerine kendisine ait özel bir mutabakat protokolünü (Interledger Protocol) kullanmaktadır. Bu protokol, tasarımı itibari ile küresel bir koordinasyon sistemine ya da Blockchain yapısına ihtiyaç duymamaktadır. Ripple protokolü, üzerinde gerçekleşen işlemler hakkında saniyeler içerisinde mutabakat sağlayabilmektedir.

Ripple, kendi kripto-para birimine sahip olsa da (XRP) yapı itibari ile para birimlerinden bağımsız bir sisteme sahiptir, üzerinde her türlü para birimi (diğer kripto-para birimleri dahil olmak üzere) hatta değer ifade eden herhangi bir birim ile (yolcu mil puanları gibi) işlem yapılabilmektedir.[19]

Ripple platformu üzerinde kullanıcılar (Ripple entegrasyonu olan finansal kurumlar), güvendikleri kullanıcıları ve bu güven yapısı içerisindeki işlem bilgilerini (limit vb.) tanımlamak zorundadırlar. Ripple platformu, iki kullanıcı arasında yapılan bir para transfer işleminde öncelikli olarak bu iki kullanıcı arasında güvenli bir iletişim kanalı kurmaya çalışır. Direk bir iletişim kanalı oluşturamaması durumunda, kullanıcıların güvendikleri diğer yapıları kullanarak bu iletişimi oluşturmaya çalışır (gerekirse bunun için kendi kripto-para birimi üzerinden dönüşüm gerçekleştirir).

[19] *Kripto para borsalarında işlem gören Ripple (XRP), Ripple firmasının geliştirdiği ve kendi servisinde kullandığı kripto para birimi teknolojisidir ancak doğrudan Ripple servisine bağlı değildir. Bu sebeple Ripple firmasının başarısı veya XRP'nin borsalardaki değeri arasında doğrudan bir bağlantı yoktur.*

Bu güvenli yol kurulduktan sonra tüm işlemler atomik yani işlem bütünlüğünün bozulmadığı (işlemlerin ya hepsi gerçekleşir ya da hiç biri gerçekleşmez, parçalı bir gerçekleşme durumu oluşmaz) bir şekilde gerçekleşmektedir.

Ripple platformu küresel anlamda çeşitli finans kurumları tarafından yapılan denemelerde kullanılmaktadır. Örneğin ATB (Kanada) ile Reisebank (Almanya) arasında yapılan Ripple testlerinde, normalde dört gün kadar süren para transfer işlemlerinin 8 saniye içerisinde gerçekleştiği gözlemlenmiştir. Türkiye'de faaliyet gösteren Akbank'ın, Almanya'daki şirketi Akbank AG de Ripple ağına dahil olan bankalar arasında bulunmaktadır.

Ripple finansal kurumları hedefleyen bir platformdur. Bundan dolayı tüm işlemlerin gerçekleştiği Ripple Ağ yapısının yanı sıra, kurumların bu katman ile entegrasyonunu sağlayan Ripple Connect adlı bir ürün sayesinde, kurum sistemlerinde değişiklik yapılmadan entegrasyon sağlanmaktadır.

Corda

80'den fazla finans kurumu ve düzenleyicinin ortaklığı olan R3 (daha doğrusu R3 bu konsorsiyum ortaklığına liderlik eden firmanın adıdır) bünyesinde geliştirilen Corda platformu, aslında tam olarak bir Blockchain çözümü değildir, bir dağıtık kayıt defteri (distributed ledger) projesidir. Diğer yaklaşımlardan farklı olarak işletmeler arasında yasal sözleşmeleri kaydetmek, yönetmek ve otomatikleştirmek ve finansal piyasalardaki uygulamalara çözümler sunmak için özel olarak tasarlanmıştır.

Günümüzde bu tarz sözleşmeler, ilgili her tarafta, farklı sistemlerde, farklı şekillerde saklanmaktadır. Bu farklı ve birbirlerinden kendi aralarındaki mesaj değişimi dışında bağımsız olan sistemlerde tutulan sözleşme verilerinde ortaya çıkabilecek uyumsuzluklar, oldukça yüksek maliyetli düzeltme operasyonlarına gerek duymaktadır. Corda platformu, akıllı sözleşme yaklaşımını kullanarak bu verimsiz ve problemli yapının yerine

geçmek ve gereksiz tekrarlama, teyitleştirme, hatalı eşleme, ihlal gibi kavramları geride bırakmak için tasarlanmıştır.

Corda platformunda veriler, sadece ilgili sözleşmeye dahil olan ve yasal olarak sözleşme ile ilgili bilgilere erişmesi gereken taraflar tarafından görülebilirler, bu veriler ağ üzerindeki diğer makineler ile paylaşılmaz. Mutabakat yapısı sistem genelinde değil, işlem seviyesindedir; işlemlerin doğrulanması yine sadece sözleşmeye dahil olan taraflar tarafından yapılmaktadır. Corda mutabakat yapısı, tak-çalıştır yaklaşımını desteklemektedir. Bu şekilde, gerektiği durumlarda içinde bulunduğu ortamın yerel yönetmeliklere uygun mutabakat yapısını kullanabilmektedir.

Corda platformu, yapısındaki sözleşmeleri uygulama ve doğrulama için, yazılım geliştirme dünyasında bir endüstri standardı olan Java Virtual Machine (JVM)'i kullanmaktadır. Bundan dolayı JVM üzerinde çalışabilen herhangi bir programlama dili (Java, Scala, Groovy gibi) ile sözleşmeler yazılabilmektedir. Bu yaklaşımı ile Ethereum platformunu andırmaktadır.

Corda platformunun, sadece kurumlar arasında değil, kurum içerisindeki farklı sistemlerin aynı işlem için oluşturduğu çoklu kayıt yaklaşımını tekil bir platform üzerinde yöneterek maliyet ve karmaşıklığı azaltmak için de kullanılabileceği düşünülmektedir.

Diğer Blockchain Platformları

Burada anlatılan temel Blockchain platformlarının dışında da pek çok platform bulunmaktadır ve bunların sayısı her geçen gün artmaktadır. Ancak Bitcoin, Ethereum, Hyperledger ve Ripple şu anda gerek açık kaynaklı grupların sahiplenmesi, gerekse kurumsal yapıların sahiplenmesi ile birlikte en çok ilgi duyulan platformlara dönüşmüş durumdalar. Sıfırdan bir Blockchain platformu geliştirmek yerine yüzlerce hatta binlerce farklı kişinin sürekli geliştirdiği ve hatalarını giderdiği platformlar çok daha güvenilir ve popüler hale gelmektedir.

1.6. Blockchain Uygulama Örnekleri

Mevcut Blockchain platformlarını kullanarak veya kendi özel platformunu kurarak farklı servisler sunan çözümlerin sayısı bugün binlere, projelerin sayısı ise on binlere ulaşmıştır.

Bu bölümde değişik Blockchain projelerini anlatarak, Blockchain teknolojisinin ne denli farklı ve geniş bir ekosisteme sahip olduğunu göstermek istiyoruz. Bu projeler arasında özellikle Bankalararası Kart Merkezi'nin gerçekleştirdiği ve Türkiye'nin ilk Blockchain Kavram Kanıtlama Çalışması (Proof of Concept – PoC) olan BBN projesinin; Kadir ve Hasan Kurtuluş kardeşlerin dünya çapında ilgi gören Proofstack (eski adı ile Copyrobo) projesinin ve yine Türkiye merkezli olup sivil havacılık sektörüne yönelik geliştirilen Further Network projesinin, ülkemizde de Blockchain teknolojisi üzerine önemli çalışmaların yapıldığını görmek açısından çarpıcı örnekler olduğunu düşünüyoruz. Bu çalışmaların detaylarını, her bir projeye ait özel başlık altında yer alan, kendi bölümlerinde okuyabilirsiniz.

Everledger

2015 yılında Londra'da kurulan Everledger, elmas ticareti sürecindeki aktörlerin işlem kayıtlarını bir Blockchain ağı üzerinde tutarak süreçleri hızlandırmayı ve tüm taraflar arasındaki güveni artırmayı hedeflemektedir. Elmas sahipleri, sigorta firmaları, düzenleyici kurumlar gibi aktörlerin bir araya geldiği Blockchain platformu, geleneksel sertifika yapısına kıyasla daha güvenli ve hızlı bir süreç sağlamaktadır.

Bu hizmeti verebilmek için öncelikle bir elması tanımlayan; seri numarası, kesim şekli, renk bilgisi gibi temel bilgiler toplanmakta ve bu bilgiler kullanılarak dijital bir parmak izi[20] oluşturulmaktadır. Dijital parmak izi verinin kendisi değil, özet bir bilgiyi ifade etmektedir. Everledger bu dijital

[20] *Dijital parmak izi olarak "Güvenli Özetleme (Secure Hash)" yöntemi kullanılmaktadır. Bu konu ile alakalı daha detaylı bilgiyi kitabımızın 2. Bölümünde bulabilirsiniz.*

özeti Bitcoin Blockchain ağında gerçekleştirilen bir işlemin parçası olarak kaydetmektedir. Böylece, Everledger'in sunduğu hizmeti kullanan elmas ticareti işlemlerinin inkar edilemez ve yok edilemez bir kaydı, Bitcoin ağına işlenmektedir. Everledger şu ana kadar 1 milyondan fazla elmas için Bitcoin Blockchain Ağı üzerine bilgi ekleme işlemi gerçekleştirmiştir.

Factom

Temelleri 2014 yılında atılan Factom, kendisi tarafından saklanan veri kayıtlarının asla değiştirilmeyeceğini garanti ederek bu kayıtları saklama sözü veren bir servis sağlayıcısıdır. Bu veriler tıbbi kayıtlardan tapu kayıtlarına kadar farklılık gösterebilmektedir.

Factom, öncelikle bir veri katmanı oluşturarak kendisine ileten verileri bloklar içine yerleştirir ve blok içerisindeki sıralarını sabitler. Her 10 dakikada bir, bir blok içinde toplanan veri kümesine ait güvenli bir özetleme değeri oluşturulur ve oluşturulan bu değer, Bitcoin Blockchain Ağı üzerine yazılır. Bitcoin Blockchain Ağı üzerine kaydedilen güvenli özet asla değişmeyeceği için, Factom kendisine emanet edilen kayıt değiştirilmediği sürece bunun orijinalliğini garanti altına almış olur.

Factom ilk dönemlerinde oluşturduğu özetleme değerlerini Bitcoin Blockchain Ağı üzerinde tutuyor olsa da şu anda farklı Blockchain Platformlarını da desteklemektedir.

Factom, şu ana kadar yaklaşık olarak 100 milyon belgeyi kayıt altına almıştır. Bu kayıtlar için yaklaşık 80 bin adet özetleme değeri kullanılmıştır.

SatoshiPay

Ödemeler dünyasında ödeme miktarına göre çeşitli sınıflandırmalar bulunur. Örneğin mikro ödemeler genel olarak 10 ABD doları ve altındaki bedellere sahip işlemleri ifade etmektedir. Nano ödemeler ise bu rakamın çok daha

altındaki cent/kuruş seviyesindeki ödemeleri tanımlamak için kullanılmaktadır. Ancak geleneksel ödeme sistemlerinde alınan işlem ücretleri, nano ödemelerin gerçekleştirilmesini maliyetli hale getirmektedir.

2014 yılında Berlin'de kurulan SatoshiPay, bu soruna Bitcoin Blockchain Ağı ile entegre şekilde çalışacak, kendi geliştirdiği bir ödeme kanalı ile çözüm sunmaktadır. Bu özel kanal üzerinde basit bir akıllı sözleşme yapısı bulunmaktadır. Bu şekilde kullanıcıya gerekirse anlık olarak bir Bitcoin cüzdanı oluşturulmakta, bu cüzdan üzerinden yapılan mikro ödeme işlemleri belirli zaman zarfında toplanarak sonrasında tek bir işlem olarak Bitcoin Blockchain Ağı'na yazılmaktadır.

SatoshiPay, öncelikle web tabanlı içerikler için ödeme çözümü olma hedefi üzerine yoğunlaşmış olsa da, web üzerindeki dijital içerikler için bir ödeme standardı haline gelme yolunda ilerlediğini de belirtmiştir.

Ujo Music

Günümüzde, mevcut müzik dağıtım kanalları yapısı ile geçmişten gelen yapıların yer aldığı dijital dünya arasında oluşan uyumsuzluklardan kaynaklanan çeşitli sorunlar yaşanmaktadır:

✔ Yapılan ödemeler (yüzde 20 ila 50'si), gerçek sahiplerine ulaşamaz,

✔ Bir sanatçıya ait eserin kullanımı takip edilemez,

✔ Ödemelerin hak sahiplerine dağıtımında şeffaflık yoktur ve ücretlendirme gibi konular eser sahibi dışındaki kişiler tarafından yönetilir,

✔ Hak sahiplerinin, ödemeleri iki seneye varan çok uzun vadeler ile almaları söz konusudur.

Ujo Music, bu konuda yaptıkları bir "deney" çalışmasında, Ethereum Blockchain Ağı üzerinde geliştirdikleri akıllı bir sözleşme ile, dinleyicilerin bir şarkının indirme, yayınlama ve yeniden düzenleme amaçlı dijital

lisansını satın alabilmelerini ve bunun karşılığında yaptıkları ödemelerin, şarkıcı ve paydaşları arasında otomatik olarak bölünüp dağıtılmasını mümkün kılmıştır.

Bu yapı ile kişisel dinleme için lisanslama yapılabildiği gibi, yayınlama amaçlı lisanslama ile kullanım başına ücretlendirme ya da yeniden düzenleme amaçlı olarak, sadece ilgili bölümün alınması gibi işlemler, herhangi bir aracı kuruma ihtiyaç duyulmadan, gerçeğe yakın zamanlı bir şekilde yapılabilir.

OpenBazaar

Günümüzde elektronik ticaret akışı büyük oranda Amazon, eBay gibi internet tabanlı merkezi platformlar üzerinde gerçekleştirilmektedir. Bu platformlar, sağladıkları hizmet kapsamında belirli sınırlı ödeme yöntemlerini desteklemekte, yüksek işlem komisyonları yansıtmakta, kişisel bilgilerin paylaşımı, sınırlı ticari kategori seçenekleri gibi çeşitli kısıtlamalar getirmektedirler.

2016 yılında faaliyete geçen OpenBazaar bu merkezi yapılara karşı alternatif bir yaklaşım getirip, alıcı ve satıcıları doğrudan birbirine bağlayan bir platform sağlamaktadır. Arada kendisi dahil herhangi bir kurum olmadığından taraflar arasındaki alışveriş kapsamında, kuralları taraflar belirlemekte ve ayrıca bir kısıtlama bulunmamaktadır.

OpenBazaar, bu yapıda taraflar arasındaki "güven" sorununun aşılması amacı ile Bitcoin Blockchain ağını kullanmaktadır. Taraflar bir fiyat üzerinde anlaştıklarında dijital imzaları ile bir sözleşme oluşturup bu sözleşmeyi denetleyici olarak adlandırılan OpenBazaar ağındaki kendi belirledikleri üçüncü kişi ile paylaşırlar. Bu kişi, sözleşmeyi temel alıp Bitcoin Blockchain ağı üzerinde çoklu-imzalı (işlemin gerçekleşmesi için üç kişiden ikisinin onay vermesinin - imzalamasının - yeterli olduğu bir sözleşme yapısı ile) bir hesap oluşturur. Alıcı, Bitcoin hesabına gönderim

yaptığında satıcıya bir bilgilendirme gönderilir, satıcı ürün gönderimini yapıp gizli anahtarı ile sözleşmeyi onaylar. Alıcı, ürünü aldıktan sonra kendi imzası ile sözleşmeyi onaylaması durumunda (üç kişiden en az ikisinin onay vermesi durumu gerçekleştiğinden dolayı) gönderimi yapılan Bitcoin, satıcı hesabına aktarılmış olur. Bu yapıda bir problem olması durumunda denetçi devreye girer, gerekirse sözleşmenin onayı için kendi imzası ile onaylama akışına dahil olur.

Augur

Augur merkezi olmayan bir tahmin borsasıdır. Ethereum platformu üzerinde yazılmış olan Akıllı Sözleşmeler ile çalışır. Dileyen herkesin belirli bir süreye sahip ve sonucu gelecekte belli olacak bir olay için bir kayıt açmasına imkân sağlar. Bu kaydı oluşturan taraf, yetkili hakem; sonucu bildirecek muhabir ve tahmine ait ödeme bedellerini belirler. Daha sonra kullanıcılar bu kayıt için tahminlerini belirterek, vadeli sözleşmeler satın alabilirler. Olay gerçekleştiğinde sonuçlara göre vadeli sözleşme müşterilerinin kazançları veya kayıpları belirlenir. Tüm bu akışlarda Augur adı verilen özel bir Token kullanılır. Sistem üzerinde muhabirler için REP (Reputation – Saygınlık) adı verilen özel bir Token çeşidi daha bulunur. Muhabirler REP Tokenları ile olaylar için bir tartışma ortamı yaratabilirler. Olay netleştiğinde doğru yönde tahmin edenler yatırdıkları REP Tokenlarını belirli bir artış ile geri alırlar. Böylece zaman içinde belirli alanlarda uzmanlar daha yüksek REP Token kazanırlar. REP Token sistemi aynı zamanda bağımsız muhabirlerin olayların sonucunu tarafsız şekilde kanıtlamaları için bir teşvik sistemidir. Sistem üzerinde tüm işlemler akıllı sözleşmelerin tetiklediği süreçler ile yönetildiği için, tahmin borsasında kayıtlı olayların çıktılarına dair bir anlaşmazlık veya haksızlık söz konusu olmaması hedeflenmiştir.

Augur bugüne kadar Ethereum Blockchain platformu üzerinde yazılmış, en büyük, merkezi olmayan uygulamalardan birisidir. Danışmanlar kurulunda bizzat Ethereum'un kurucusu Vitalik Buterin yer almaktadır.

Votem

Oylama süreçleri demokratik yönetimlerde gerek ülke bazında gerekse şirketler ve dernekler gibi daha küçük yapılarda her zaman bir seçim yapmak için kullanılan önemli bir araç olmuştur. Giderek küreselleşen dünyada ise artık oy verecek kişilerin belirli bir oy merkezine gitmeden, uzaktan oy kullanması teknik olarak mümkün olmakla birlikte, kimlik kontrolü, oyun gerçekten sahibi tarafından verildiğinin doğrulanması, mükerrer oyların önlenmesi ve oy kayıtları üzerinde tahrifat yapılmaması gibi farklı ihtiyaçlar kendini göstermektedir. 2014 yılında kurulan Votem, kendisini dünya üzerindeki en geniş Blockchain ağına sahip mobil dijital oy platformu olarak tanıtmaktadır. Bugüne kadar 11 farklı büyük seçimde, 8,2 milyon oy kullanılmasına aracılık yaptığını belirten Votem, kendisine özel geliştirdiği özel bir Blockchain platformu üzerinde çalışan özel bir Token protokolüne sahiptir. Kısmen izin gerektikten bir Blockchain Ağı altında güvenilir noktalardan oluşan altyapısı, aynı zamanda kısmen izin gerektirmeyen açık yan bağlantılar ile güçlendirilmiştir.

Steemit

Steemit, yayıncılara hizmet eden, nitelikli içeriklerin okuyucular tarafından ödüllendirildiği, Blockchain tabanlı bir içerik yayınlama platformudur. Haziran 2016'da aktif şekilde devreye giren platformun şu anda 1 milyona yakın abonesi bulunmakta ve platform üzerinde her ay yaklaşık 1,5 milyondan fazla içerik yayınlanmaktadır. Platform üzerinde bugüne kadar içerik üretenlere 40 milyon dolardan fazla teşvik ödenmiştir.

Steemit platformu kendi Blockchain altyapısına sahiptir. Bu altyapı üzerinde Steem (STM) adı verilen bir Token kullanılmaktadır. Bugüne kadar verilen 40 milyon dolardan fazla ödül nakit olarak değil, Steem

Tokenları ile ödenmiştir ve bu Tokenların kripto para borsalarındaki değeri 40 milyon doların üzerine karşılık gelmektedir.

Platformun, aynı zamanda bir içeriğin kendi Blockchain platformu üzerinde yayınlanması ile birlikte artık yok edilemeyecek bir kayıt haline geldiği için, telif haklarını da koruyabilecek bir niteliğe sahip olduğu belirtilmektedir.

SecureKey

Özellikle bankacılık, finans ve telekomünikasyon gibi sektörlerde, "müşterini tanı" (KYC) süreçleri, maliyetli ve uzun sürebilmektedir. Müşteriler her defasında yeni bir kurum ile ilişki kurarken bu süreçten geçmek zorunda kalırlar. Kanada merkezli SecureKey, Linux Vakfı tarafından geliştirilen Hyperledger platformu üzerinde tekil ve güvenilir bir kimlik kaydı sistemi sağlamak için özel bir çözüm geliştirmektedir. Herhangi bir kurumda gerçekleşen KYC sürecinden geçen bir kimlik kaydı, SecureKey'in sağladığı Blockchain platformunda şifreli ve sadece sahibi ile paylaşıldığı kurum tarafından erişilebilecek şekilde kaydedilir. Kimlik sahibinin daha sonra farklı bir kurumda KYC sürecinden geçmesini gerektiren bir ilişki kurulduğunda, yine kimlik sahibinin izniyle, bu yeni kurum daha önce güvenilir bir diğer kurum tarafından onaylanmış ve KYC sürecinden geçmiş kimlik kaydına ulaşabilir ve müşteri kimlik bilgilerini kullanabilir. Böylece hem müşteri tüm süreci bir daha yaşamak zorunda kalmaz, hem de yeni kurum KYC sürecindeki maliyetten kurtulur. Bu yapı içinde kimlik sahibi, bilginin yöneticisi ve kontrol edenidir. Platform sağlayıcısı SecureKey bilgiyi görmez, kimlik bilgileri yeni bir kurumla paylaşıldığında ilk süreçte kimliği doğrulayarak kaydeden kurum da bundan haberdar olmaz. Herhangi bir kurum KYC maliyeti ile içeri bir kimlik kaydı aldığında da bu veri diğer kurumlar için gizlidir. Bu yapıya **Üç Kör (Three Blind)** adı verilmektedir.

Golem

Golem, yüksek işlem gücü gerektiren makine öğrenmesi, görsel hesaplama gibi hesaplamalar için dağıtık işlem gücü sağlayan küresel ölçekte bir bilgisayar sistemi servisi sunmayı vadetmektedir. Elindeki atıl bilgisayar işlem gücünü Golem ağına dahil etmek isteyenler, bir yazılım indirerek bilgisayarlarındaki bu gücü, Golem ağına tahsis ederler. Diğer taraftan yüksek işlem gücüne ihtiyaç duyanlar yine Golem'in ilgili uygulamasını indirerek, hesaplanacak işlemleri bu ağa gönderebilirler. Tüm işlemlerde hizmet alanlar ve hizmete katılanlar için ödemeler Golem ağındaki özel bir Token olan Golem Network Tokens (GNT) ile yapılır. GNT Token kayıtları ve işlemlerin bilgileri ile yapılacak ve alınacak ödemelere dair süreçler ise Ethereum Blockchain Ağı üzerindeki akıllı sözleşmeler ile sağlanır. Golem sisteminin geliştirmesi devam etmekte ve şu anda oldukça kısıtlı imkanlar dahilinde beta olarak test edilebilmektedir.

iXledger

iXledger sigortacılık sektörüne yönelik geliştirilmekte olan bir Blockchain çözümüdür. Sigorta sektöründe, sigortacılar, resürörler ve aracılar için açık bir pazar ortamında sigorta poliçeleri ve bunlara bağlı ürünlerin satışa çıkartılması, tekrardan satılması, farklı çözümlere dönüştürülmesi için hizmet vermeyi amaçlamaktadır. Şu anda geliştirme aşamasındaki platform, kendine özel IXT adı verilen bir Token ile sigortacılık sektöründeki ticari ürünlerin kendi aralarındaki bu geçişleri ve dönüşümleri sağlamayı hedeflemekte, Blockchain platformu üzerinde kayıtları tutarak küresel bir güvenli sigorta pazar yeri oluşturmayı planlamaktadır.

Mysterium Network

Virtual Private Network (VPN), yani Özel Sanal Ağlar, işletmelerin ve

kurumların güvenlik amacı ile uzak noktadaki merkezleri veya çalışanları ile kendi içlerinde özel bir ağ oluşturmasını sağlayan bir teknolojidir. VPN, aynı zamanda son kullanıcılar için internete çıkış noktalarını değiştirmelerini sağlar. Böylece VPN ağının bir noktasındaki kullanıcı, normal şartlar altında bulunduğu noktadan erişemediği içeriklere, diğer noktada erişim engeli olmayan kişi üzerinden ulaşabilir. Şu anda dünya üzerinde ücretli olarak VPN erişimi sağlayan pek çok şirket bulunmaktadır.

Mysterium Network, dileyen herkesin kendi bilgisayarına küçük bir uygulama indirerek bir VPN noktasına dönüşmesini sağlamayı amaçlamaktadır. Dağıtık bir VPN uygulaması olarak kendisini tanımlayan Mysterium Network, erişimin engellenemediği ve tüm dünyada tüm içeriklere erişimi mümkün kılan bir ağ olmayı hedeflemektedir. Bu amaç için ağa bağlanarak bir erişim noktası haline gelen kişiler ile ağı kullanan kişilerin servis kayıtları bir Blockchain ağı üzerinde tutulacak ve ağ içerisinde ticari işlemler, MYST adı verilen bir Token ile sağlanacaktır. Girişim, kayıtların tutulması ve Token servisinin sağlanması için Ethereum Blockchain ağını kullanmayı planlamaktadır. Proje henüz geliştirme aşamasındadır.

Brave ve BAT

Brave temel olarak bir internet tarayıcısıdır. Reklamları ve kullanıcıyı takip eden diğer yazılım kodlarını engelleyerek, popüler internet tarayıcılar arasında en hızlı olduğunu iddia etmektedir. Brave tarayıcısına entegre olarak çalışan BAT (Basic Attention Token), yani Basit Dikkat Tokeni ise reklam verenlerin, anonim veriler ile Brave kullanıcılarına reklam ulaştırması için tasarlanmıştır. Brave bu yöntemi daha güvenli, sade ve tüketiciyi reklam ile boğmayan bir yapı olarak tanımlar. Elbette BAT akışı reklam verenden tüketicilere doğru olacak şekilde planlanmıştır. Tüketicilerin web sitelerinde gezinmeleri ve dikkatlerini yoğunlaştırmaları karşılığında ise bu performans ölçümlenerek içerik platformlarına

aktarılır. BAT akışı ve süreçlerin tamamı, Ethereum platformu üzerinde akıllı sözleşmeler ile çalışmaktadır. Bu sebeple BAT sahipleri bunları farklı kripto para borsalarında diğer kripto paralara veya nakit paraya dönüştürebilirler.

Filament

Blockchain uygulama alanlarına değindiğimiz bölümde, tedarik zinciri ve kopya ürün koruması gibi alanlarda Blockchain teknolojisinin kullanılabileceğini belirtmiştik. Bu tarz alanlarda Internet of Things yani Nesnelerin İnterneti adını verdiğimiz kavram devreye girmektedir. Pek çok küçük bilgisayar, üzerlerindeki alıcılar ile çevreden bilgi toplamakta ve bu bilgiler internet üzerinden büyük veriye dönüştürülmektedir. Bu veri, daha sonra işlenerek anlamlı hale getirilebilir veya farklı süreçlerin işlemesi için kullanılabilirler.

Filament, IoT dünyasındaki ihtiyaçlara cevap verecek Blockchain çözümleri geliştirmeyi hedeflemek için kurulmuştur. Blocklet Chip adı verilen IoT için tasarlanmış minik donanım çözümü, Blockchain ağlarına bağlanarak veri okuyabilmekte, aynı zamanda veri kaydı yapabilmektedir. Blocklet yazılımı ise Blocklet Chip'lerin üzerindeki veri akışını akıllı sözleşmelere bağlı olarak yönetmek için geliştirilmiştir.

Diğerleri

Bu kitabın kapsamında Blockchain ağları üzerinde koşan sadece sınırlı sayıdaki örnek uygulamaya bakma şansımız bulunuyor. Bu konuda internet üzerinden bir araştırma yapmaya kalktığınızda sayıları binlere ulaşan rakamlarda farklı uygulama ile karşılaşmanız mümkündür.

Bu projelerden pek çoğu henüz tasarım ve geliştirme aşamasındadır. Zaman içinde başarısız olma ihtimalleri bulunduğu gibi henüz ortaya çıkmamış çok başarılı olabilecek projeler de olabilir.

Yönümüzü Türkiye'ye çevirdiğimizde ise Bankalararası Kart Merkezi'nin gerçekleştirdiği ve Türkiye'nin ilk Blockchain Kavram Kanıtlama Çalışması (Proof of Concept – PoC) olan BBN, Kadir ve Hasan Kurtuluş kardeşlerin dünya çapında ilgi gören Proofstack (eski adı ile Copyrobo) projesi ve yine Türkiye merkezli olup sivil havacılık sektörüne yönelik geliştirilen Further Network projesini görmekteyiz. İlerleyen üç bölümde bu projeler için sırasıyla; BKM BBN projesi için BKM Genel Müdür Yardımcısı Celal Cündoğlu ile yaptığımız röportajı, Proofstack projesi için şirket kurucu ortaklarından Kadir Kurtuluş'un ve Further Network için kurucu ortaklarından Gökhan Koç'un kaleme aldığı bölümleri okuyabilirsiniz.

Türkiye'den Bir Örnek: **BKM ve BBN**

Ülkemizde Blockchain teknolojisi alanında test çalışmaları yürüten önemli kurumların başında Bankalararası Kart Merkezi geliyor. "Kavram Kanıtlama" çalışması için Hyperledger platform üzerinde geliştirilen Blockchain projesinin detaylarını BKM Genel Müdür Yardımcısı Celal Cündoğlu'na yönelttiğimiz sorular ile paylaşıyoruz.

Blockchain teknolojisinden ne zaman ve nasıl haberdar oldunuz?

BKM olarak dünyadaki yeni teknolojileri, ürün ve hizmetleri yakından takip ediyoruz. Bu kapsamda 2015 yılında Bitcoin de radarımıza girmişti. Blockchain ile ilk defa Bitcoin'in arkasındaki teknolojiyi anlamaya çalışırken tanıştık. Bitcoin'in arkasındaki teknolojinin faydasının anlaşılması ise biraz zaman aldı. Ancak başta finans olmak üzere birçok sektörde Blockchain'in kullanım alanları son dönemde yoğun biçimde araştırılıyor. Bu tür çalışmaları, teknolojinin sorunlara çözüm üretebilip üretemeyeceğinin netleştirilmesi ve yol haritasının çizilmesi noktasında çok değerli buluyoruz.

Blockchain teknolojisine yönelik bir proje yapma fikri nasıl doğdu ve gelişti?

Blockchain'in finans dünyasına çok katkı sağlayacağına inanıyoruz, burada önemli olan uygun kullanım alanlarını belirleyebilmek. Biz de ilk etapta Blockchain teknolojisi ile ilgili gelişmeleri yakından takip ediyorduk ama bu teknolojiyi daha iyi tanımak, anlamak için de ufak denemeler yapmamız gerektiğinin de farkındaydık. Çokça okuyup, dinleyip, öğrendikten sonra artık proje yapmak için hazırdık. Öncelikle

mevcut altyapıların sunamadığı ancak Blockchain ile bir çözüm yaratılabileceğine inandığımız konuları listeledik ve dijital kimlik konusunda bir kavram kanıtlama çalışması yapamaya karar verdik.

Blockchain projenizde başlangıç, gelişim ve şu anda düşünce ve beklentileriniz nasıl gelişti ve şekillendi? Blockchain projesi ile hedefleriniz nelerdir?

Projeyi hayata geçirmeden önce çok değerli kişiler ve şirketlerle fikir alışverişinde bulunduk. Sonuç olarak şirket içerisinde belirlediğimiz dijital kimlik, dağıtık kayıt yapısı, akıllı sözleşmeler gibi konseptleri deneyebileceğimiz, tüm şirket çalışanlarımızın kullanabileceği bir kurguda karar kıldık ve 2017 yılının başında projemizi hayata geçirdik. Bunun için şirketimizin her katını ayrı bir firma gibi tanımlayıp her kat için farklı mobil uygulamalar geliştirdik. Böylece şirket çalışanlarımızın Blockchain yapısını kullanarak düzenlenen şirket etkinliklerinden puan kazanıp bunları yine mobil uygulamalar üzerinde harcayabildikleri, dijital kimliklerini yönetebildikleri bir sistemi, günlük hayatlarının bir parçası haline getirdik.

Kavram kanıtlama çalışması ile temel hedefimiz bu teknolojinin getirdiklerini, özelliklerini, olumlu ve olumsuz yanlarını daha iyi anlayarak bunun üzerine yeni iş modelleri oluşturabilmek.

Bu projenin sizlere neler kazandırdığını düşünüyorsunuz?

Üzerinde çalışılan platformlar özellikle başlangıçta ihtiyaçlar doğrultusunda sürekli kendilerini geliştiriyor ve geliştiricilerin yeni şeyler yapmasını sağlıyor. Dolayısıyla Blockchain ile bir çırpıda yepyeni bir dünya oluşturmanın mümkün olduğunu söylemek gerçekçi olmaz. Temelinde bir veri tabanı yapısı olan ve üzerine kurgulanan modellerle anlamlı çözümler geliştirilen Blockchain'in olmazsa olmazı ise işbirliği.

Blockchain'in, tek bir kurumun kendi başına uygulaması yerine sağlanacak işbirlikleri ile bugün çözüm bulunamayan pek çok konuya yardımcı olacağına inanıyoruz. Proje bize sunumlarda gördüğümüz bir teknolojiyi çok daha yakından tanıma imkânı verdi. Kavram kanıtlama çalışmamız sona erdiğinde detaylarına hakim olduğumuz bir teknoloji ile yeni iş fikirleri üretebileceğiz.

Proje boyunca yaşadığınız problemlerden bahsedebilir misiniz? Sizce bu tarz projelerdeki en büyük engelleyici/yavaşlatıcı ana unsurlar nelerdir?

Belirttiğim gibi üzerinde çalışılan platformlar, sizinle birlikte gelişip öğreniyorlar. Bu yüzden her istediğinizi hızlı biçimde yapamıyorsunuz. Bu durumun yavaşlatıcı etkisi olduğunu söyleyebiliriz. Bunun yanı sıra bu platformların güncellemelerde eski yapılarından çok farklı bir yapıya geçmesi de yeni yapıya geçiş maliyetlerini arttırabiliyor.

Proje çıktılarını göz önüne aldığımızda Blockchain teknolojisi hakkında mevcut algının ve gerçeklerin birbirine paralel olduğunu söyleyebilir miyiz? Blockchain teknolojisi konusundaki küresel beklentilerin karşılığını bulabileceğini düşünüyor musunuz? İnanıyor musunuz?

Blockchain ile katma değerli çözümler geliştirileceğinden şüphe etmiyoruz. Ancak geliştirilen çözümün kabul görmesi, ülkeden ülkeye değişecektir. Çünkü bir coğrafyada sorunlu olan bir alan, farklı bir pazarda kusursuz biçimde çalışıyor olabilir. İşlem sürelerinin uzun olduğu ve maliyetlerin yüksek olduğu uluslararası para transferleri başarının yakalandığı alanlardan biri oldu. Diğer yandan IoT ile birleştiğinde bugün yeni yeni gelişen akıllı ev, araba gibi pek çok konsept bizlere yeni deneyimler sunacak.

Projemizin ilk fazına ait çıktılarını "Keşif: Blockchain'in Sırları" adını verdiğimiz özel bir raporda topladık. Bu raporu BKM'nin web sitesinden dileyen herkes indirebilir ve gerçekleştirdiğimiz çalışmayı inceleyebilir.

Avukat Kadir Kurtuluş'un kaleminden; **Proofstack**

Blockchain teknolojisinin pek çok farklı alanda devrimsel bir dönüşümü tetikleyebileceğini gözlemliyoruz. Bu alanlardan birisi de Fikri Mülkiyet alanı. Dünya'da yüz doksandan fazla Marka ve Patent ofisi bulunuyor. Maalesef bunca merkezi kurumun kendi aralarında bir entegrasyon bulunmuyor ve pek çok normal sürecin bile zaman zaman aksadığına şahit oluyoruz.

Marka ve patent haklarına benzer şekilde telif haklarında da henüz küresel bir kayıt sistemi yok. Şu anda noterler veya telif hakları ofisleri aracılığıyla hak tespiti yapılmaktadır. Bu tespitlerin yapıldıkları ülkeler dışında ise geçerliliği bulunmuyor. Ayrıca bu süreçlerde de marka ve patent süreçlerine benzer problemler yaşanıyor.

Bahsettiğim tüm bu problemleri, sektörde uzun yıllar boyunca kazandığımız deneyimleri de göz önüne alarak, Blockchain teknolojisi ile çözebileceğimizi gördük. Örneğin geçerliliği resmen kabul görecek açık ya da özel bir Blockchain platformu ve getireceği güvenli kayıt birliği sayesinde; tüm tescil ve diğer işlem verileri tek bir ağda tutulabilir, tek bir ağda anlık izleme ve karşılaştırma yapılabilir, varlık transferleri akıllı sözleşmelerle anlık olarak gerçekleştirilebilir ve zaman tasarrufu bakımından onlarca sözleşme silsilesi tek bir akıllı sözleşme altında yönetilebilir. Ancak böyle küresel bir çözüme giden yol henüz uzun ve oldukça karışık süreçlerin çözümlenmesini gerektiriyor. Bu sebeple biz daha basit ancak benzer faydalar sağlayacak bir çözüm geliştirmeye karar verdik ve ilk adı Copyrobo olan, yeni adı ile Proofstack projesini hayata geçirdik.

Proofstack Nedir? Nasıl Çalışır?

Proofstack, aynı anda farklı ülkelerin yasa ve mevzuatlarına uygun delillerin üretilebileceği, doğrulanabileceği ve yönetilebileceği, güvenli ve devamlı bir platform oluşturmak amacıyla ortaya çıktı.

Proofstack ile işlem, olay, belge gibi içerik ve durumların varlığını gün, saat ve bölge bilgisiyle üstelik reddedilemez biçimde kanıtlayabiliyoruz. Bu işlem için; Nitelikli Zaman Damgası kullanarak eşsiz dijital imzalar üretiyoruz. Daha sonra bu imzaları Bitcoin, Ethereum ve Litecoin Blockchain platformlarında ve eşzamanlı olarak Avrupa Birliği ülkeleri ve diğer ülkelerin yetkilendirdiği sertifika otoritelerinin resmi platformları üzerinde de kayıt altına alıyoruz.

Proofstack ile cep telefonunuzdan ya da web sitesinden tek tuşa basarak birkaç saniye içinde notere gitmeye gerek kalmaksızın; eser, proje, buluş, fikir, belge, fotoğraf, sözleşme, senaryo, beste, tasarım, ses kaydı gibi çalışmanızın tüm haklarının size ait olduğunu, tüm dünyada kanıtlayan bir delil üretebiliyorsunuz. Üretilen deliller telif haklarının ispatında ya da farklı işlem, olay ve belge tespitlerinde kullanılabiliyor. Abim Hasan Kurtuluş ile birlikte gerçekleştirdiğimiz yatırımlar ve 4 yıl süren çalışma sonucunda, 2017 yılında Proofstack'i tüm dünyada kullanıma açtık. Sahaya çıktığımız ilk senemizde, Techcrunch Distrupt San Francisco'da dünyadaki gelecek vadeden üç Blockchain girişiminden biri seçildik. Hemen ardından Dubai'de Jüri özel ödülüne layık görülerek, Dubai'nin 2020 hedeflerinin mimarisini oluşturacak ilk beş şirket arasına girdik. Proofstack şu anda dünya üzerinde hizmet satmaya başlamış olan nadir projelerden birisi.

Proofstack Yasal Deliller Oluşturuyor

Proofstack projesinde mahkemelerde geçerli delili oluşturabilmek için birçok Avrupa ülkesi ve Türkiye elektronik sertifika hizmet sağlayıcılarıyla anlaşma yaptık. 1 Temmuz 2016 'da yürürlüğe giren AB Dijital Tek Pazar ile ilgili eIDAS yasaları ile uyumlu zaman damgalama işlemi yapabiliyoruz. Buna göre Türkiye'de Proofstack aracılığıyla telif hizmeti aldığınız belge, tüm AB mahkemelerinde delil olarak geçerli oluyor. Bu sayede eserinizi tüm AB mahkemelerinde geçerli olacak şekilde tek tıkla korumuş oluyorsunuz. Ayrıca sisteme entegre Bitcoin, Ethereum, Litecoin gibi Blockchain platformlarında gerçekleştirilen kayıtlar sayesinde, bu platformlardaki kayıtların yasal delil teşkil ettiğini kabul eden, Japonya, Hindistan, Avustralya, Kanada, Amerika ve daha bir çok ülkede de geçerli deliller elde etmenizi sağlıyoruz.

Gökhan Koç'un kaleminden **Further Network**

7 trilyon dolarlık global seyahat sektörü, pek çok ülkede ekonominin itici güçlerinden biri konumunda. Tüm paydaşlar, 2020'de hedeflenen 13 trilyon dolarlık pastadaki payını artırmanın yollarını arıyor. Hem sunulan hizmetlerin kalitesi artıyor hem de teknolojik gelişimler sayesinde servis ve ürünlere erişim süreleri gün geçtikçe kısalıyor. Fakat diğer yandan, onlarca yıl önce düzenlenmiş protokollere dayalı ödeme işlemleri, uzun mutabakat sürelerine ve dolayısıyla hantal bir biletleme sürecine yol açıyor.

Havayolları sektörüne odaklandığımızda, 2016 yılında toplam 725 havayolunun bulunduğu ve yaklaşık 1 trilyon dolarlık bir hacim yaratıldığı görülüyor. 1945 yılında kurulmuş olan Uluslararası Hava Taşımacılığı Birliği IATA'ya üye 275 havayolu var ve bu havayolları tüm hacmin 750 milyar dolarlık kısmını yaratıyor. IATA, üye havayolları ve acenteler arasında ödeme ve mutabakat konusunda aracı rolünü üstleniyor. Her ne kadar, bu durum sürece ek maliyetler ve süreler getirse de üye havayolları açısından küresel ve yerel tüm satıcılarla tek tek uğraşma derdi ortadan kalkıyor. Fatura, Mutabakat, Ödeme süreçleri tek bir kanalda yönetiliyor.

IATA üyesi olmayan havayolları açısından ise uçuş envanterini çeşitli acentelere yaymak da, satış sonrası ücretleri sağlıklı bir şekilde toplamak da sıkıntılı bir süreç. Riskleri en alt seviyeye düşürmek için ödenen teminatlar yükseliyor ve vadeler uzuyor. Erişim ağı yüksek acenteler ya bu şartlarla çalışmak istemiyor ya da kısıtlı ve riski düşük olan envanterler için hizmet vermeyi tercih ediyor.

Uzun yıllar boyunca havacılık endüstrisinde deneyim sahibi olan, yazılım teknolojileri, Blockchain, finans ve kullanıcı deneyimi konularında uzman arkadaşlarımız ile mevcut sorunlardan yola çıkarak, Blockchain

teknolojisinin havayolları endüstrisinde ne gibi değişikliklere yol açabileceği üzerine yaptığımız bir tartışma sırasında Further projesi filizlenmeye başladı. Şirketimizin kurucu ortakları Erdem Üney ve Kadir Özgür Oğuz ile birlikte önerimiz şuydu: "Neden acenteler ve havayolları arasında yaşanan ödeme ve mutabakat kaynaklı sıkıntıları Blockchain üzerinde baştan ele almıyoruz? Blockchain sayesinde bu sorunlu alana bir çözüm sunabiliriz." Böylece Further Network'ü seyahat sektöründeki ödeme ve mutabakat süreçlerini Blockchain yapısına taşımayı amaçlayan bir teknoloji girişimi olarak kurduk. Genel olarak tüm seyahat sektörünü hedefliyoruz ama öncelikle kurucu ekibimizin tecrübeli olduğu alanda, havayolları dikeyinde bu teknolojiyi tasarlamaya başladık.

IATA üyesi olmayan havayollarını öncelikli hedef pazar olarak belirledik. Hem IATA üyesi hem de üye olmayan kuruluşların da aslında Blockchain'e dayalı bir envanter yönetimi, biletleme, ödeme ve mutabakat sistemine ihtiyaç duyduğunu biliyoruz. Bu sebeple Further Network, değişik ölçekte ve türde pek çok kuruluşla yoğun şekilde görüşmeler yapıyor.

Dönüşüm Sürecine İhtiyaç Var

Yoğun bir araştırma sürecinin ardından Further Network yol haritasını 5 adımlık bir geliştirme planı olarak belirledik.

Further Network olarak, ilk adımda ödeme ve mutabakat işlemlerinin Blockchain ile gerçek zamanlı olarak gerçekleşmesini sağlamayı hedefliyoruz. Bu kapsamda tasarladığımız network'te, STR (Smart Travel Record - Akıllı Seyahat Kaydı) ile havayolları, Acenteler ve müşteriler arasındaki para akışının ve biletleme işlemlerinin gerçek zamanlı yapılabilmesini sağlayacağız. Hava yolları ve acenteler arasındaki uzun mutabakat süresinden kaynaklı operasyonel iş yükü de ortadan kalkacak. STR içerisinde bilete ilişkin fiyat bilgisi, talep edilen

veya satın alınan servisler ve havayolunun belirlemiş olduğu akıllı kontrat kuralları yer alacak. Ayrıca seyahat ve ek servislerle ilgili ücretlerin bilgisi de STR dahilinde taşınacak.

Further Network'ün tüm bu işlemleri düzenlemek için sistemde kullanılmak üzere geliştirdiği Token'a ise Aton adını veriyoruz. Sistemdeki tüm seyahat ürünlerinin Aton cinsinden bir karşılığı bulunacak. Fakat ödeme resmi para birimleri ve aynı zamanda kripto para birimleriyle de yapılabilecek.

Ödeme ve mutabakat süreçlerinin merkezi bir süreçten P2P ve aracısız bir yapıya taşınmasının ardından Further Network olarak hayata geçirmeyi planladığımız adımlar ise şöyle: Son tüketicilerin seyahat ürün ve servislerini satın alabileceği ve yönetebileceği bir dApp , P2P seyahat ürün dağıtımı ve yönetimi, havayolları için Blockchain'e dayalı bir envanter yönetimi ve biletleme sistemi ile son olarak da ekosistemin üçüncü tarafların kullanımına da açılmasını sağlayacak olan Open Network yapısı. Bu aşamada da sistemdeki uçak bileti ya da otel rezervasyonu veya diğer seyahat ürünlerinden oluşan STR'ların el değiştirilebilmesi için bir pazar yeri de oluşturulacak.

Yaklaşık iki yıllık bir süreçte Further Network yol haritasındaki tüm adımları gerçekleştirmeyi hedefliyoruz.

Son Tüketici Faydası

Further Network'ün temel amaçlarından birisi, tüketicinin seyahat sürecindeki kullanıcı deneyimini geliştirmek ve servis havuzunu zenginleştirecek bir altyapı sağlamak.

Günümüzde bir uçuş bileti satın alırken yaşadığımız opsiyon kısıtlarının çoğu biletleme süreçlerinin komplike yapısından ve ödeme süreçlerinin uzun olmasından kaynaklanıyor. Seyahat şirketleri, ek gelir elde edebilecekleri servisleri tüketicilere sunmaya çalıştıklarında, insan gücü

gerektiren ek süreçler devreye giriyor. Ödemedeki mutabakat sürecine ek yük getirebilecek her adımda, olası finansal riskler de hesaba katıldığında nihai tüketicinin satın almaya değer görmeyeceği fiyatlarda servisler ortaya çıkıyor ve memnuniyetsizlik oluşuyor. Örneğin, mevcut sistemde satın alınan bir biletin kolayca başka birine aktarılması mümkün değil. Pek çok havayolu bu opsiyonu direk kapatıyor. Bu ve benzeri pek çok problem, biletleme sürecinin Blockchain'e taşınmasıyla çözülecek.

1.7. Blockchain Uygulamalarında Zorluklar ve Riskler

Blockchain teknolojisinin çözüm getirdiği problemi, yapısını, uygulamalarını ve platformlarını inceledik. Her ne kadar tüm bu bilgiler bizlere Blockchain teknolojisini sihirli bir değnek gibi gösterse de aslında her yeni teknoloji gibi Blockchain teknolojisi de gelişim aşamasında çeşitli riskler, zayıflıklar ve zorluklar içermektedir. Şimdi bu problemlere göz atacağız.

Dijital Dönüşüm Gereksinimi

Blockchain uygulamaları tarafından ortaya koyulan çözümler, merkezi yapıları ortadan kaldırarak veya yapılarında önemli ölçüde değişimlere yol açarak, mevcut sistemlerin işleyişinde ciddi dönüşümlere ihtiyaç duyar. Bu dönüşümün yapılabilmesi için öncelikle bu sürecin kabullenilmesi ve akabinde ciddi bir dönüşüm stratejisi oluşturularak eyleme geçilmesi gerekmektedir.

Özel Anahtarların Saklanması

Özellikle kripto-para çözümlerinde kullanılan açık-özel anahtar yapısındaki özel anahtarın saklanması, sahibinin sorumluluğundadır. Sahibinin bir özel anahtarı kaybetmesi durumunda, son kullanıcının elinde şifrelenmiş işlemlerin sahipliğini doğrulayacak hiç bir bilgi kalmaz. Özel anahtarın başka bir kullanıcının eline geçmesi ise ilişkili varlıkların sahipliğini kaybetmek ile eşdeğer bir durumdur. Bu gibi problemlerin oluşmasını engellemek amacı ile kullanıcıların anahtar verilerini koruyacak yeni aracı kurum yapılarının oluşması muhtemel bir gelişmedir. Bu sebeple farklı alternatif çözümler sunan kripto para cüzdan uygulamaları, servisleri ve donanımlarının sayısı her geçen gün artmaktadır. Ancak bu yapılar da beraberlerinde farklı güvenlik sorunlarını getirmektedir. Daha uzun vadede özel anahtarların biyometrik verilere bağlanması hedeflenmektedir.

İşlem Performansı

Blockchain platformları alternatif oluşturduğu bazı alanlarda halihazırda kullanılan çözümlere kıyasla daha düşük işlem performansı göstermektedir. Örneğin şu andaki yapısı ile Bitcoin'e ait Blockchain platformu saniyede ortalama 7 işlem gerçekleştirebilirken, modern kredi kartı platformları saniyede 7 ila 8 bin işlem gerçekleştirebilmektedir.

Yüksek Yatırım Gereksinimi

Blockchain teknolojisi, işlem maliyetlerinde ve zaman kullanımında ciddi anlamda tasarruf sağlamaktadır, ancak başlangıçta gereken yüksek yatırım maliyetleri caydırıcı olabilmektedir. Burada açık kaynaklı platformlar ile testlere başlamak kolay görünse bile bu alanda henüz yeterince insan kaynağının olmaması, öğrenme sürecinin uzunluğu ve öngörülmeyen yazılım riskleri, toplam sahip olma maliyetini yükseltmektedir.

Enerji Tüketimi

Özellikle "Proof of Work[23]" tipi mutabakat yapıları kullanan Blockchain platformları, şu anda ciddi bir enerji tüketimi ve dolaylı olarak karbon ayak izi etkisi doğurmaktadır. Bitcoin Blockchain ağında yeni blokların eklenmesi için madenciler tarafından harcanan işlem gücünün tükettiği elektrik, dünya üzerindeki bazı küçük ülkelerin tükettiği elektrik miktarını geçmiş durumdadır. Bu sebeple alternatif mutabakat yapılarının geliştirilmesi ve enerji tüketiminin azaltılması için pek çok çalışma yürütülmektedir.

Sınırlı Teşvik

"Proof of Work" tipi mutabakat yaklaşımı kullanan Açık Blockchain ağlarında yeni blokların üretilmesi için gerçekleştirilen madencilik işlemi, genel olarak

[23] *Bu raporu indirmek için ilgili sayfaya http://bit.ly/BC101-BKM-BBN adresi üzerinden ulaşabilirsiniz.*

teşvik sistemi ile beslenmektedir. Kripto para üretim miktarı sınırlı olan durumlarda teşvik sisteminin sonlanması ile birlikte burada oluşacak madenci davranış şekli konusunda kesin bir yargıya varmak şimdiden mümkün görünmemektedir.

Yazılım Hataları, Açıklar ve Siber Saldırılar

Blockchain teknolojisi oldukça yeni bir teknolojidir, bundan dolayı şu anda kullanılan Blockchain platformları genel olarak "deney" olarak adlandırılmaktadır.

Teknoloji çok yeni olduğu için öngörülemeyen yazılım hataları siber saldırganlara davetiye çıkartmakta ve özellikle Açık Blockchain platformlarındaki bu kusurlar tespit edildiği takdirde ciddi ekonomik kayıplar yaşanabilmektedir.

Sahip oldukları açıkların giderilmesi ve yeniliklerin eklenmesi için platformlar üzerinde sürekli güncelleme çalışmaları yürütülmekte, ancak özellikle Açık Blockchain platformlarının merkezi olmayan, demokratik yapısı bu güncellemelerin gerçekleştirilmesinde her bir uç noktanın birlikte hareket etmesini gerektirmekte, bir anlaşmazlık durumunda ise çatallaşma adı verilen sonuçlar doğabilmektedir.

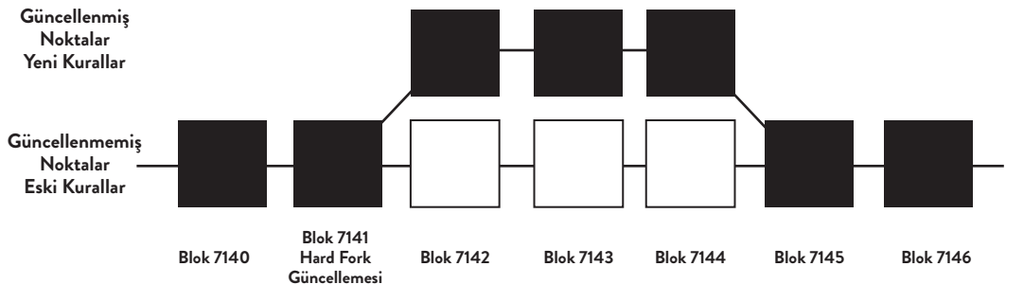
Çatallaşma (Fork) Problemi

Blockchain ağlarında tüm noktalar o ağa özel bir yazılım kullanarak ağa katılır, mutabakat yöntemi ve sürecine dahil olurlar. Bu yazılımlar sürekli olarak sistemi geliştirenler tarafından güncellenir. Bu güncellemeler genellikle ağın yeteneklerini ve imkanlarını geliştirmeye ve performansını artırmaya yönelik gerçekleşir.

Bir Blockchain ağındaki her bir nokta, ağın yerel bir kopyasına sahiptir. Bazı istisnai durumlarda yazılımda gerçekleştirilen güncellemeler sonrasında, güncelleme yapanlar ağa yeni blok eklemeye devam ederken, güncelleme

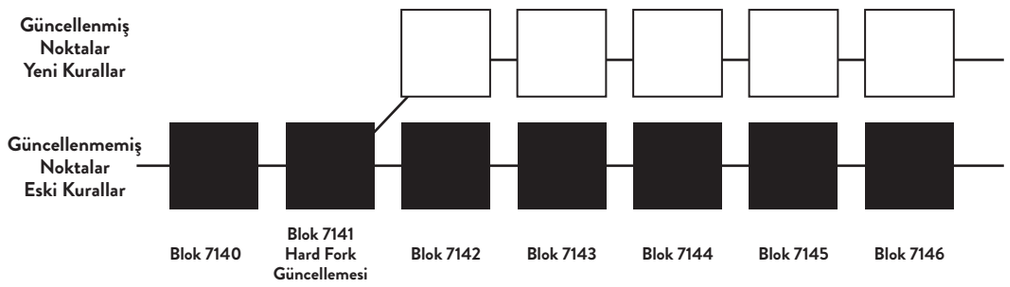
yapmayanlar yeni blok ekleyemezler, ancak mutabakat sürecine dahil olabilirler (eklenen blokları doğrulayabilirler) ve akabinde bu blokları kendi zincirlerine kopyalayabilirler. Bu Blockchain ağında bir **Geçici Çatallaşma (Soft Fork)** durumu ortaya çıkartır.

Şekil 13: **Soft Fork – Geçici Çatallaşma Durumu**



Bazı yazılım güncelleme durumlarında ise güncelleme almayan noktalar artık mutabakat süresine dahil olamazlar. Güncelleme yapan noktaların yazdığı blokları doğrulayamaz, okuyamaz ve kopyalayamazlar. Yazılım güncellemesi yapanlar Blockchain ağında yeni bloklar eklemeye devam ederken yazılım güncellemesini yapmayanlar yeni yapıya katılamamakla beraber, eski mutabakat yapısında yeni bloklar ekleyebilirler. Böyle bir durumda eski yapıdaki noktalardan bazıları yeni yapıya geçmeme kararı alabilir. Bu durumda ister istemez birbirinden ayrılan iki tane yeni Blockchain ağı oluşur. Bu duruma **Mecburi Çatallaşma (Hard Fork)** adı verilmektedir.

Şekil 14: **Hard Fork – Mecburi Çatallaşma Durumu**



Blockchain ağlarında yaşanabilen çatallaşma probleminin en büyük örneği "DAO Olayı" olarak adlandırılmaktadır ve 2016 yılında Ethereum Blockchain ağında gerçekleşmiştir. Gelişmiş bir akıllı sözleşme olan DAO yaklaşımı (Decentralized Autonomous Organization – Merkezi Olmayan Özerk Kurum), herhangi bir insan müdahalesi gerek kalmayacak şekilde, bir kurumun kurallarını ve karar verme mekanizmalarını bir akıllı sözleşme kapsamında tanımlayarak, çözüm sunmayı hedeflemiştir. DAO projesi Nisan 2016 tarihinde Ethereum üzerinde çalışmak üzere tanımlanmış bir şekilde ICO[24] gerçekleştirmiş ve 11.000 civarında kişinin katılımı ile birlikte 170 milyon dolar değerine yakın Ether (ETH) toplanmıştır. Bu toplanan kaynak, girişim sermayesi fonu olarak kullanılmak üzere DAO'nun yönetimine bırakılmıştır. Ancak DAO'un üzerine inşa edildiği akıllı sözleşme yapısındaki bulunan açığı fark eden bir (veya bir grup) siber uzman, toplanan fonun yaklaşık 1/3'ünü[25] kendi hesabına aktarmayı başarmıştır. Buradaki önemli nokta bu işlemin Ethereum ve DAO kurallarına aykırı davranmayarak, herhangi bir ihlal gerçekleştirmemiş olmasıdır.

Bu durum sonrasında, sadece bu olaya özgü işlemlerin iptali için bir **Mecburi Çatallaşma** işlemi gerçekleştirilmiştir. Ancak Ethereum yapısı üzerindeki bazı kullanıcılar, 'kurallara uygun davranan her işlem geçerli bir işlemdir' düşüncesi ile bu değişikliği kabul etmemiştir. Bunun üzerine eski kod yapısı ile devam edenler **Ethereum Classic (ETC)** adını almış ve yeni kod yapısı ile devam edenler **Ethereum (ETH)** şeklinde yoluna devam etmiştir. Bu sebeple şu anda aynı başlangıç noktasından doğan ancak farklılaşarak yoluna devam eden iki farklı Ethereum Blockchain Ağı bulunmaktadır.

Bir diğer mecburi çatallaşma örneği ise yine en popüler Blockchain ağı olan Bitcoin üzerinde yaşanmıştır. 2017 yılında Bitcoin ağındaki blokların en fazla 1 MB büyüklüğünde olması ve bu durumun ağ üzerinde kayıtların birikerek

[24] *Devam eden bölümde detayları ile anlatılmaktadır.*
[25] *3,6 milyon Ether*

gecikmesine yol açması nedeniyle, bu sorunu çözmek isteyenler bir yazılım güncellemesi yapmış ve bu güncelleme sonrası bu noktalar, Bitcoin Cash adı ile yoluna devam etmiştir. Aradan çok uzun bir zaman geçmeden Bitcoin Ağı'nda benzer görüşe sahip noktalar yine bir güncelleme yaparak, Bitcoin Gold ağını ortaya çıkartmıştır. Ancak orijinal Bitcoin ağı varlığını sürdürmeye devam etmektedir. İki farklı mecburi çatallaşma sonrasında orijinal Bitcoin ağı ile birlikte iki farklı türevi ortaya çıkmıştır. Bu ağlarda çatallaşma öncesine ait tüm kayıtlar birbirinin aynısı iken çatallaşma sonrasında her ağ kendi kuralları ile yeni bloklar eklemekte ve artık birbirleri ile hiçbir bağlantıları bulunmamaktadır.

Şifreleme ve Kuantum Bilgisayarlar

Blockchain platformlarını en güçlü kılan özelliklerin başında kriptografi gelmektedir. Bu kapsamında kullanılan şifreleme yaklaşımları oldukça güçlü olsa da, kuantum bilişim (quantum computing) gibi alanlardaki gelişmelerle birlikte bu konuda ilerideki zamanlarda çeşitli zafiyetler görülebileceği düşünülmektedir. Şu anda bilgisayarların sadece 1 ve 0 ile işlem yapabildiği ikili (binary) sistemler kullanıyoruz. Ancak kuantum bilgisayarlarda 1 ve 0 durumlarının birlikte ve aynı anda geçerli olduğu üçüncü bir durum daha bulunmaktadır. 1, 0 ve (1-0) şeklinde ifade edebileceğimiz bu üç farklı durum, Qubit adı verilen yapılarda saklanmaktadır. Bu bilgisayarlar geleneksel ikili sistemlere karşı milyonlarca kat daha hızlı işlem yapabilme kabiliyetine sahiptir ve bu sistemler her ne kadar şu anda sadece özel laboratuvarlarda geliştiriliyor olsalar da ilerleyen on yıllar içinde öncelikle savunma ve istihbarat organizasyonları ve ardından çok daha geniş bir şekilde erişilebilir hale gelecekler. Bu sistemlerin makul sürelerde günümüzün gelişmiş ikili şifreleme yöntemlerini kırması mümkün olabilecektir. Bu durum, mevcut Blockchain platformları için bir risk oluşturmaktadır. Ancak zamanla bu sistemlerin genele yaygınlaşması ile şifreleme işlemleri de kuantum bilgisayarlar ile gerçekleştirilecek ve bu risk ortadan kalkacaktır.

1.8. ICO Kavramı ve Detayları

Token kavramını ele aldığımız **"Token Nedir? Kripto Paralardan Farklı mıdır?"** başlıklı bölümde anlattıklarımızı hatırlıyor musunuz? Eğer hatırlamıyorsanız şimdi dönüp hızlıca bakmanın tam zamanı. Tüm kripto paraların birer Token olduğunu ancak farklı Token çeşitlerinin de bulunduğunu ve bunların hepsinin birer kripto para olmak zorunda olmadığını belirtmiştik. Blockchain teknolojisi kripto paralar başta olmak üzere tüm dijital Token uygulamaları için eşsiz bir platform oluşturuyor. Pek çok farklı amaca hizmet eden ve bu amaçlar için Token sistemlerine sahip çeşitli uygulamalardan uygulama örneklerini ele aldığımız bölümde bahsetmiştik. İşte bu Tokenlar belli bir amaç için ilk olarak üretildiklerinde, henüz hiçbir kullanıcısı olmayan birer uygulamadan ibarettiler, bu sebeple ICO, Initial Coin Offering yani Türkçe karşılığı ile "Öncü Sikke Arzı[26]" gerçekleştirilmektedir.

ICO temel olarak herhangi bir Token için bir Blockchain platformu üzerinde satış veya teklif olarak sunulur. ICO süreçlerinin tamamında arz edilen Tokenlar, Bitcoin veya Ether gibi en popüler kripto paralar karşılığında sahiplerine verilir ve bu işlem Blockchain platformlarının altyapısı üzerinde kaydedilir.

Genelde ICO uygulamalarının ilk olarak 2014'de başladığı düşünülüyor, ancak bu yanlış bir düşünce. İlk ICO, 2009 yılında, Bitcoin platformunun kendisi olmuştur. Bitcoin çekirdeği yazılıp çalışmaya başladıktan sonra ICO olarak, insanlara: "dileyen herkes gelip bu sistemin parçası olabilir ve madencilik yaparak Bitcoin kazanabilir" mesajı verilmiştir. Bugün artık bu öneriyi herkes dikkate alıyor ancak iş işten geçti desek yeridir, zira madencilik yapmak çok zorlaştı. O günlerde bu teklifi ciddiye alanların

[26] Coin kelimesinin Türkçe karşılığı sözlüklerde madeni para veya sikke olarak geçiyor. Çeşitli kaynaklarda Türkçeye Dijital Para olarak çevrilmiş ancak ICO içinde arz edilen unsurun yapısı her zaman bir dijital para olmak zorunda değildir. Bunu Token ile alakalı bölümde detayları ile anlattık. Bu sebeple biz daha iyi bir alternatif önerilene kadar Sikke kelimesi ile Türkçe karşılığı ifade edeceğiz. Genel olaraksa orijinal kısaltma olan ICO'yu kullanmaya devam edeceğiz.

oldukça ciddi kazançlar elde ettiği de malum ancak biz daha yakın tarihlerde popülerleşen ICO kavramına odaklanalım.

Gerçekleşen ICO uygulamaları ile alakalı pazar verilerini yayınlayan Coindesk sitesinde yer alan bilgilere göre[27] 2014 yılının başından, 2018 yılının ilk çeyreği sonuna kadar gerçekleşen ICO'ların pazar değeri 12,11 milyar doları geçmiş durumda. Bu rakamın 7,4 milyar dolarının 2018 yılının ilk çeyreğinde, 5,4 milyar dolarının 2017 yılında, 300 milyon dolarının 2016 yılında ve geri kalan kısmının ise 2015 ve 2014'te gerçekleştiğini görüyoruz. Elbette bu rakamlar ABD doları bazında işlemleri değil, bu değer karşılığında gerçekleşen ve ağırlıklı olarak Bitcoin ve Ether ile yapılan transferleri ifade ediyor.

ICO Satışı Nasıl Yapılıyor?

Kendine ait veya herhangi bir Blockchain platformu üzerinde oluşturulan Tokenlar için farklı satış tipleri ve süreleri ile satış gerçekleştiriliyor. Bunlardan ilki sabit bir fiyat belirlemek. İşin niteliğine göre üretilen Tokenlara bir bedel belirleniyor. Örneğin 1000 UstaCoin için 1 Ether bedel öngörülebiliyor. Bir diğer yaklaşım ise açık artırmaya sunarak fiyatı alıcıların belirlemesi yönünde adım atmak, ancak bu seçenek popüler bir seçenek değil.

Arz edilecek Tokenlar için temel bir bedel belirlendikten sonra, sıra süreye karar vermeye geliyor. Bunun için de iki seçenek mevcut:

Sınırlı Token Satışı (Hard Cap): Satılacak Token adedi için bir üst limit belirleniyor. Satış bu adetteki Token satılınca son buluyor.

Süreli Token Satışı (Soft Cap): Bu senaryoda ise belirli bir süre sınırı konularak, bu süre içinde belli bir adet sınırı olmadan Tokenlar satılıyor.

Genelde uygulanan ise aynı anda hem sınırlı hem de süreli satış modellerini bir arada kullanmak. Örneğin "60 gün süreyle 10 milyon Token satışa sunuldu" deniliyor. Hangisi önce biterse ICO bu süreçte sonuçlanmış oluyor.

[27] http://bit.ly/BC101-ico adresinden Coindesk ICO verilerinin sunulduğu sayfalara ulaşabilirsiniz.

ICO yapacak olan girişimler sıklıkla ICO sürecini daha cazip hale getirmek için bazı ödül mekanizmaları sunuyorlar. Örneğin 60 günlük satışın ilk 10 gününde ICO'dan Token alanlara yüzde 20 bonus vermek, ikinci 10 günlük dönemde yüzde 10 bonus vermek gibi.

Bitcoin'in madencilik odaklı gerçekleşen bir ICO olduğunu belirtmiştik. Günümüzde ise ICO yapan girişimler daha çok belirli bir amaç için kullanılacak Tokenların tamamını, ICO başlamadan önce üretiyorlar ve bunların belli bir kısmını ICO sürecinde arz ediyorlar. Nadiren de olsa ICO için dağıtılacak Tokenlar önceden üretilmiş oluyor ve proje hayata geçtikten sonra yeni Tokenlar madencilik ile üretiliyor.

ICO'nun Faydaları

Yenilikçi bir finansman kaynağı olarak ICO'nun hem yapan taraf hem de yatırımcılar için çeşitli faydaları bulunuyor.

ICO yapanlar için; ortada henüz bir ürün yokken Ethereum gibi platformlar üzerinde Token üretip bunu arz etmek gayet kolay olduğu için hızla müşteri kazanmak, projenin ve ekibin adını duyurmak, hızlı kaynak toplamak, herhangi bir ülkenin finansal ve mali düzenlemelerine bağlı olmadan tüm dünyadan kaynak (kripto para) toplayabilmek gibi faydalar öne çıkıyor. Elbette rakamlara baktığımızda ICO'ların hâlâ çok ciddi şekilde ilgi çektiğini de görüyoruz.

ICO'ya yatırım yapanlar için hâlâ ICO'lardaki Tokenlar çok hızlı değerleniyor, bu yüzden yapılan yatırımı hızlı ve kârlı şekilde elden çıkartmak çok cazip geliyor. Üstelik Token transferi hiçbir düzenlemeye veya kanuna takılmadan hızla gerçekleştirilebiliyor. ICO'ların neredeyse tamamı için hızlı bir viral yayılama durumu söz konusu bu da değeri etkileyen faktörler arasında. Bu durum yatırımcıların ilgisini çekiyor. Büyük ölçüde ICO'larda birbirini tanımayan hatta aynı dili bile konuşmayan binlerce insan yatırım yapıyor ve bu sebeple Token

sahipliği homojen şekilde dağılıyor, geleneksel melek ve risk sermayesi yaklaşımlarında olduğu gibi girişimlerin monopol ellere düşme riski ortadan kalkıyor. Son olarak birkaç sene önce Ether'in piyasa değeri 1-10 dolar arsındayken, Bitcoin'in değeri 300-700 dolar civarındayken yüklü şekilde kripto paralara yatırım yapmış olup, şu anda bu yatırımını 10 ila 1000 kat artırmış olan kripto para zenginleri var. Bu zenginler için ICO'lara yatırım yapmanın hiçbir riski bulunmuyor. Ancak yine de ICO'larda yüksek riskler söz konusu.

ICO'ların Riskleri

Temel olarak dünyanın çok nadir birkaç noktası hariç hiçbir bölgede henüz ICO'lar için başarılı ve koruyucu yasal düzenlemeler bulunmuyor. Bu konuya ayrıca değineceğiz ancak hukuki açıdan sorun olmasa bile başka türlü tehlikeler söz konusu.

Akıllı Sözleşmeler gelişmekte olan bir teknoloji ve bu sebeple yazılımlarda hatalar bulunabiliyor. 2016 yılında gerçekleşen 168 milyon dolar değerinde Ether toplayan **The DAO** isimli ICO, kullandığı akıllı sözleşme üzerindeki bir açık nedeniyle siber saldırganların 70 milyon dolar değerindeki Ether'i ele geçirmesiyle bir felakete dönüştü. Bu olaydan sonra Ethereum platformu bu açığı kapatmak için mecburi çatallaşma yaşamak zorunda kaldı.

ICO'ların neredeyse tümünde (evet tümünde) Token değerlemeleri hiçbir mantıksal temele dayanmıyor. Sadece dayanıyormuş gibi gösteriliyor. Ortada henüz ürün yokken, ekip kendisini kanıtlamamışken gelecekte yapılacağına dair söz verilen bir iş için milyonlarca hatta milyarlarca dolar değer biçilebiliyor. Bu temelsiz yaklaşımlar yatırımcıların bilgisizliği ile buluşunca var olmayan bir işin bir gecede değeri milyarlarca dolara ulaşabiliyor. Ayrıca yatırımcıların cüzdanlarını yönetmek için kullandıkları özel anahtarlarını (private key) kaybetme ve dolayısı ile ICO'dan aldıkları Tokenları sonsuza kadar kaybetme riski bulunuyor.

Elbette temelsiz değerlemeler, ICO'ların aşırı ilgi görmesi, dolandırıcıların da ilgisini çekiyor.

Yüksek fiyat dalgalanmaları, pazar manipülasyonları gibi yaklaşımlar nedeniyle bir gecede yüksek değerlemelere ulaşan veya ICO öncesinde büyük beklenti ile değeri yükseltilen projeler, daha sonra yatırımcıları için bütünüyle bir zarara dönüşebiliyor.

Öngörülemeyen matematiksel tehlikeler her zaman mevcut. Hassas ve kritik şifreleme yaklaşımları bazı projeler için yazılan akıllı sözleşmelerde açıklara sebep olabiliyor. Bir diğer önemli problem ise bu beklenmedik durumların ICO yapılan ağlara zarar vermesi. Örneğin Ethereum Blockchain platformu üzerinde gerçekleştirilen CryptoKitties beklenmedik bir ilgi görünce gerçekleşen işlemler sebebiyle tüm Ethereum Blockchain Ağı bir hafta kadar tıkanma noktasına gelmişti.

ICO Süreçlerinde Hukuki Sorunlar

Temel olarak ICO süreçlerinin hukuki bir dayanağı ve düzenlemesi bulunmuyor. Bir Blockchain ağı üzerinden Bitcoin veya Ether verilerek alınan Tokenlar için ortada gerçek bir para transferi söz konusu olmadığı için hiçbir geleneksel ödeme sistemi üzerinden kayıtlara geçen veya faturalanan bir işlem de söz konusu olmuyor. Kripto para borsaları üzerinden satın alınan Bitcoin ve Ether gibi temel kripto paralarda yüksek hacimli işlemler yine geleneksel bankacılık sistemi üzerinden para transferi yapıldığı için takip edilebiliyor, ancak Bitcoin ve Ether ile bir ICO'ya yapılan yatırımların takip edilmesi çok güç. Bu sebeple anonimlik problemi ortaya çıkıyor.

Anonim işlem yapma şansı, vergiden kaçınma ve potansiyel kara para aklama gibi işlemlere kapı açarken, arka planda yasa dışı süreçlerin işleyip işlemediğini bilmek neredeyse imkânsız hale geliyor.

Ülkeler ICO Uygulamalarına Nasıl Bakıyor?

Çin ve Güney Kore şu anda ICO yapmayı kendi ülkelerinde yasaklamış durumda.

Amerika Birleşik Devletleri'nde, her eyalet kendi kanunlarına göre farklılıklar göstermekle birlikte bir yasaklama söz konusu değil. Ancak ICO'ların lisans alarak ve SEC (Securities and Exchange Comission – Menkul Kıymetler ve Borsa Komisyonu) kurallarına uyularak gerçekleştirilmesi isteniyor. Şu anda ABD'de daha önce gerçekleşen bazı ICO'lar için toplanan kaynakların belirtilen amaçlar için harcanmadığına dair delillere dayanılarak, bu ICO'ları gerçekleştiren kişiler için dava açılmış bulunuyor.

Avrupa Birliği'nin de yaklaşımı ABD'ye benziyor. Henüz bir yasak yok ancak ICO'ların yüksek risk taşıdığı, ICO yapacak firmaların ise KYC/AML[28] süreçlerine uyması gerektiği belirtiliyor ve yatırımcılar bu konuda uyarılıyor.

Kanada, her bir ICO için ayrı ayrı değerlendirme ile hangi yasal düzenlemelere göre işlem yapılacağına dair bir yaklaşım sergiliyor.

Türkiye'de şu anda gerçek paraya dokunmadığınız sürece, ICO yapmayı engelleyen bir kanun yok. Ancak piyasadan gerçek para toplamak ve bu şekilde ICO yapmak mümkün değil. Yaptığı bir ICO için büyük bedeller söz konusu olursa muhtemelen mevcut kanunlar çerçevesinde ifade vermek durumunda kalacak kurumların sayısı da oldukça kabarık. Bu sene içinde gerçekleşen bir ICO, daha sonra BDDK ile görüştüğünü ve mevcut kanunlar çerçevesinde bu işlemin mümkün olmadığını öğrendiklerini belirterek, toplanan tüm kaynakları sahiplerine iade etti.

Bu kitap çerçevesinde tüm ülkelerin kanuni düzenlemelerini teker teker ele almak mümkün değil. Bu çalışma belki kendi başına bir kitap olabilir.[29]

---

[28] KYC: Know Your Customer – Müşterini Tanı Süreçleri
AML: Anti Money Laundering – Kara Para Aklama ile Mücadele Süreçleri
[29] Daha fazla bilgi için şu web sitelerine bakılabilir:
http://bit.ly/BC101-icoreg
http://bit.ly/BC101-ico-wiki

Ancak dünya üzerindeki pek çok gelişmiş ve gelişmekte olan ülke, ICO'ları düzenlemek için ciddi çalışmalar içinde bulunuyor. İsviçre, Singapur, Estonya gibi ülkeler ise bu süreçte öncü olmak için ICO'lara karşı daha izin verici ve himaye edici birer kimlik sergiliyorlar, ancak bu durum düzenlemelerin gelmeyeceği ve ICO'ların başıboş bırakılacağı anlamına gelmiyor.

Gerçekte Neler Oluyor?

ICO yenilikçi bir finansal kaynak ve başarılı bir girişim yakıtı olabilir. Ancak gerçek hayatta durum şu anda biraz daha farklı işliyor. Şu anda yeni bir Token yaratmak için en popüler platform Ethereum Blockchain ağının kendisi. Ethereum Blockchain platformunda yeni bir Token yaratmak için ERC20 adı verilen bir standart bulunuyor. Basit bir akıllı sözleşme ile temel parametreleri belirleyerek bir Token yaratmak gayet basit.[30] Üstelik bu işi yapmak için kodlama bile bilmenize gerek yok, zira bütünüyle ücretsiz. Sadece parametreleri girdiğiniz, arz şeklini, süresini, süreç zarfında öncü avantajlı teklifleri belirlediğiniz ve tek bir tıklama ile kendi Tokenlarınızı yaratabildiğiniz platformlar bulunuyor.

Ücretsiz şekilde Token ve ICO altyapısını temin ettikten sonra güzel görünen bir ICO web sitesi hazırlamanın maliyeti yaklaşık 50 ile 100 dolar arasında değişiyor. Pek çok hazır web sitesi şablonu satan platformda sadece ICO için özel temalar bulunuyor.

Bazı hizmet ve servis sağlayan pazaryeri sitelerinde ise 200 ila 300 dolar arasında profesyonel görünümlü bir ICO WhitePaper (teknik doküman) satın almak, bunu özelleştirmek, hatta tasarımını yaptırdıktan sonra mantık hatalarına karşı kontrol ettirmek bile mümkün.

[30] *http://bit.ly/BC101-ETH-Token adresinden detaylı bilgi alınabilir.*

İyi bir ekip içinse şu anda Rus yazılımcılar çok popüler. İnternet üzerinde biraz araştırma ile sahte profillerden oluşan bir ekip kurmak hiç zor değil.

Geriye sadece biraz duyuru ve reklam yapmak kalıyor. Sonra gelsin Bitcoinler, Etherler, versin elini Maldivler... :)

Kulağa komik geliyor olabilir ancak şu ana dek piyasadaki pek çok ICO için (yüzde 95'in üstünde desek abartmayız) senaryo daha farklı değil.

Nasıl Olmalı? Türkiye için Fırsat mı!

Tokenların sağladığı faydalar, Blockchain teknolojisinin teknolojik altyapısı ile birleşince, ICO'lar kesinlikle yeni girişimlerin fikirlerine kaynak bulması için devrimsel bir yöntem. Yatırım fonlarının elinden gücü alıp, bireylere, üstelik küresel ölçekte veren bir yaklaşım. Ancak kesinlikle düzenlenmesi gerekiyor. Düzenlemelerde farklı yaklaşımlar söz konusu olabilir ancak ICO'ların başarılı şekilde gerçekleşebileceği bir coğrafya, hem küresel bir cazibe merkezi hem de yabancı sermayenin toplanması için bir havuz teşkil edebilir. Umuyoruz ki dünya üzerindeki uygulamalar dikkatlice incelenerek Türkiye'de bu fırsattan en kısa sürede istifade edebilir.

Bu noktada Blockchain'e giriş niteliği taşıyan kitabımızın teorik kısmını tamamlamış bulunuyoruz. Bu süreç zarfında pek çok terim ve kavramdan kaçınmak gibi bir durum söz konusu değildi ve bunların detayları ise teknik bir bilgi ve bakış açısı gerektiriyor. Şu anda mutlaka okumanızı tavsiye ettiğimiz kapanış bölümüne geçiş yapabilir veya temel ölçüde teknik detayları ele aldığımız bölümler ile devam edebilirsiniz.

BÖLÜM II

BLOCKCHAIN 201: TEKNİK DETAYLAR

Bölüm II

BLOCKCHAIN 201: TEKNİK DETAYLAR

2.1. Kriptolojinin Teknik Detayları

Temel kavramlar bölümünde kriptoloji kavramına hızlıca göz atmıştık. Bu kısmı tekrar hatırlayalım: Eğer verileri oldukça geniş ağlara kopyalayıp, çoğaltacak ve dağıtacaksak, bu verilerin gerçekten gizliliğinin ve aynı zamanda bütünlüğünün sağlanması, bunun için de kriptolojiden yararlanılması gerekir.

Kriptoloji basit bir şekilde "şifreleme bilimi" olarak tanımlanabilir. Kriptolojinin bir alt kolu olan "**kriptografi**" (cryptography - Yunanca gizli anlamına gelen **kryptos** ve yazmak anlamına gelen **graphien** sözcüklerinden türetilmiştir) ise verilerin şifrelenmesi kapsamında kullanılan yöntemleri ifade etmektedir. Şifreleme, herhangi bir veri kümesini, bir kural yapısı kullanarak rastgele görünen, geri dönülebilir bir veri kümesine dönüştürür. Bu rastgele gibi görünen veri kümesi, şifreleme ile ilgili anahtar yapısına sahip olmayan kişiler tarafından ele geçirilse bile, orijinal yapısına uygulanabilir bir şekilde geri çevrilemez. Sadece ilgili anahtara sahip olanlar, veriyi tekrar orijinal yapısına dönüştürebilir, yani şifreyi çözebilirler.

Şimdi Blockchain ve kripto-para dünyasında bu alana ait çok kullanılan kavramları inceleyelim.

Güvenli Özetleme (Secure Hash)

Bu yaklaşım, matematiksel işlemler kullanarak büyük bir veriden kıyasla daha küçük bir özet bilgi (bunu kaynak veriye ait dijital bir parmak izi olarak düşünebiliriz) üretilmesine dayanır. Bu üretim yapısı:

✔ Aynı veri kümesi için her zaman aynı özet bilgiyi üretir.

✔ Tek yönlüdür; yani özet bilgiden kaynak veriye geri dönülmesi mümkün değildir. Özet bilgiden kaynağa ulaşmanın tek yolu, kaynak kümesindeki her olası veri yapısı için güvenli özetleme fonksiyonunu çalıştırıp, oluşan özet bilgi ile elimizdeki özet bilgiyi karşılaştırmaktır.

✔ Hızlı olarak gerçekleştirilen işlemlerdir.

✔ Küçük veri değişikliklerinde bile çok farklı özet bilgi üretir ve bu özelliğe "çığ etkisi" adı verilir.

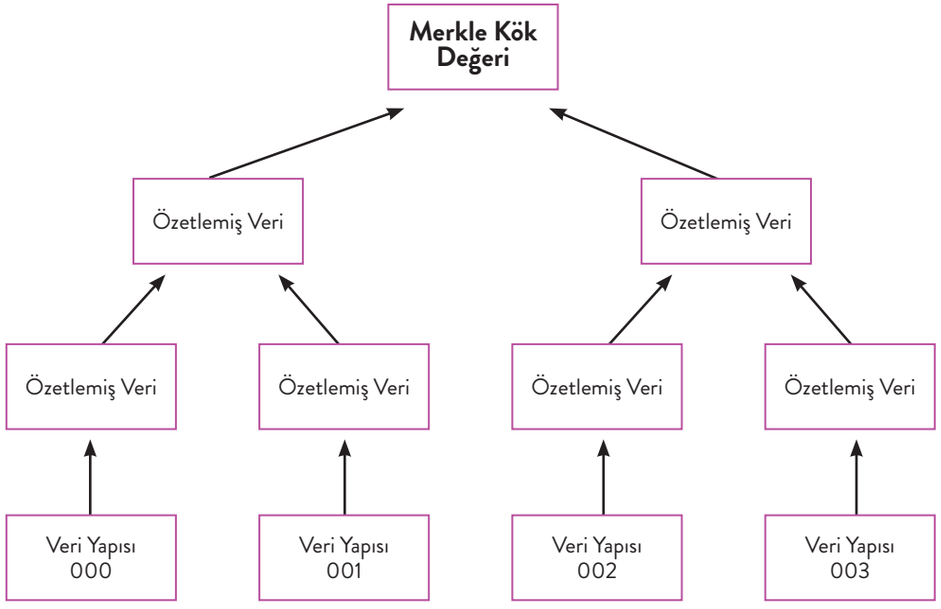
Güvenli özetleme algoritmaları, özetledikleri veriden bağımsız olarak sabit uzunlukta özet değer üretirler, örneğin SHA-1 algoritmasının ürettiği özet değerler 160 bit uzunluğunda olurken, SHA-256 algoritmasında özet bilgi uzunluğu 256 bit'tir. Algoritma sonuçları sabit uzunlukta olduklarından teorik olarak farklı veri kümeleri için özet değerlerinin çakışması mümkündür. Ancak güvenli özetleme algoritmaları kapsamında özet bilgi kümesinin büyüklüğü (SHA-256 algoritmasını düşünürsek, 256 bitlik bir özet yapısının 2^256 farklı değer olabilir, bu ise yaklaşık 10^77 yapmaktadır. Görünür evrendeki atom sayısının 10^80 civarında olduğunu düşünülürse 2^256 sayısının büyüklüğünü hakkında bir fikrimiz olacaktır) gibi nedenlerden dolayı bu göz ardı edilebilecek bir durumdur .

Örnek Veri	SHA-256 Karşılığı (okunabilirlik açısından 16'lık sayı düzeninde gösterilmiştir)
erkan	A7C3962E7BD1F5C65FDD9D97CC993B231CFF60C8296E D9F9590EAD5B0813D1D0
serkan	37B081FA6506D4B937F5A9EB893B45823BDBA49 D5DF840B24AF4122BA29E540D
Serkan	508B4498D3A57B759CC171A541CA4F2BBB2DC2B18442665E 5EE1E50AF37F7F7A

Merkle Ağaç Yapısı (Merkle Tree)

Merkle ağacı, büyük veri kümelerini güvenli ve hızlı bir şekilde doğrulamak için kullanılan, güvenli özetleme yapısı üzerinde geliştirilmiş bir yaklaşımdır. Merkle ağaç yapısında ikili (binary) bir ağaç yapısı oluşturulup, en alt seviyeye veri kümesindeki parçalar yerleştirilir. Sonrasında en alt seviyeden yukarıya doğru ikili bir şekilde özetleme değeri üretilerek ilerlenip, tüm ağaç yapısı için tekil bir özetleme değeri (Merkle kök değeri) üretilmiş olur.

Şekil 15: **Merkle Tree**

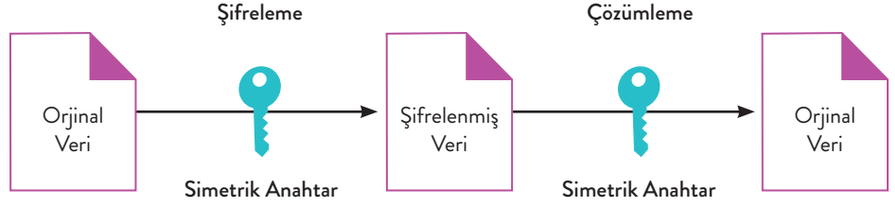


Yukarıda belirttiğimiz gibi temel olarak şifreleme işlemi, şifrelenecek veri kümesi ve şifrelemede kullanılacak bir anahtar veri yapısı ile yapılmaktadır. Burada temel olarak iki teknik kullanılmaktadır:

Simetrik Şifreleme (Symmetric Encryption)

Bu yaklaşımda hem şifreleme hem çözümleme adımlarında aynı anahtar bilgisi kullanılmaktadır. Bundan dolayı anahtar bilgisinin sadece ilgili taraflar arasında paylaşılması gerekmektedir, anahtarı ele geçiren herhangi bir taraf şifrelenmiş veriden orijinal veriye erişebilir.

Şekil 16: **Simetrik Şifreleme**

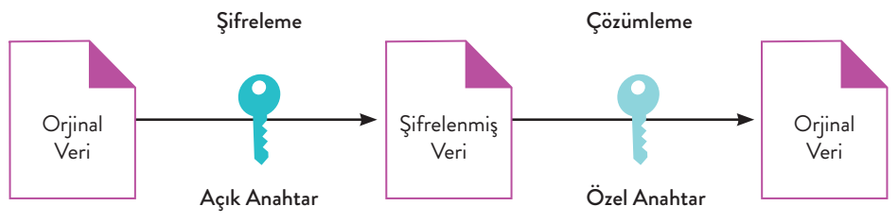


Asimetrik Şifreleme (Asymmetric Encryption)

Bu yaklaşımda şifreleyen ve çözümleyen anahtar bilgileri farklıdır. Temel olarak bu yöntem içerisinde kullanıcının biri herkese açık (public) diğeri ise sadece kendi içerisinde saklı tuttuğu özel (private) anahtar çifti değeri bulunmaktadır. Bu açık anahtar herkese dağıtılabilir, açık anahtardan özel anahtara ulaşmak bunun için gerek duyulan çok yüksek hesap gücünden dolayı "imkansız" olarak nitelenmektedir. Ayrıca açık anahtar ile şifrelenmiş bir veri, ancak ilgili özel anahtar ile çözümlenebilmektedir. Benzer şekilde özel anahtar ile şifrelenmiş veri de ancak ilgili açık anahtar ile çözümlenebilmektedir.

Bu yapı kapsamında verilerin açık anahtar ile şifrelenip özel anahtar ile çözümlenmesi yöntemi, "Açık Anahtar Şifrelemesi" (Public Key Encryption) olarak da adlandırılmaktadır.

Şekil 17: **Asimetrik Şifreleme**



Asimetrik şifreleme genel olarak aşağıdaki temel senaryolar kapsamında kullanılmaktadır:

Şifreleme/Çözme

Bu senaryo bir mesajın sadece ilgili alıcı tarafından okunmasının istendiği durumlarda gerçekleşmektedir. Bu yöntem kapsamında ilgili mesaj başka bir kişi tarafından ele geçirilse bile mesajın içeriği anlaşılamaz.

Örnek olması için A kişisinin B kişisine bu yaklaşımla bir mesaj göndermek istediğini varsayalım, bu durumda akış şu şekilde gerçekleşecektir:

- ✔ A, B'ye ait açık anahtarı elde eder (bu bilgiyi B'den talep edebilir)
- ✔ Göndermek istediği mesajı bu açık anahtar ile şifreler
- ✔ Mesajı B'ye gönderir
- ✔ B sadece kendisinde olan özel anahtar ile şifreyi çözer ve mesajı okuyabilir

İlgili mesaj B'den farklı bir kişi tarafından ele geçirilmiş olsa bile, B'ye ait özel anahtar dış dünya tarafından bilinmediğinden, şifrelenmiş mesajın çözümlenmesi mümkün değildir.

Pratik kullanımlarda, asimetrik şifrelemenin performans konusunda simetrik şifrelemeye göre daha geride olmasından dolayı yukarıda belirtilen akışta mesajın kendisi değil, simetrik şifreleme akışında kullanılacak olan anahtar bilgisi iletilir, mesajın kendisinin gönderimi simetrik şifreleme ile gerçekleştirilir.

Dijital İmzalama/Doğrulama

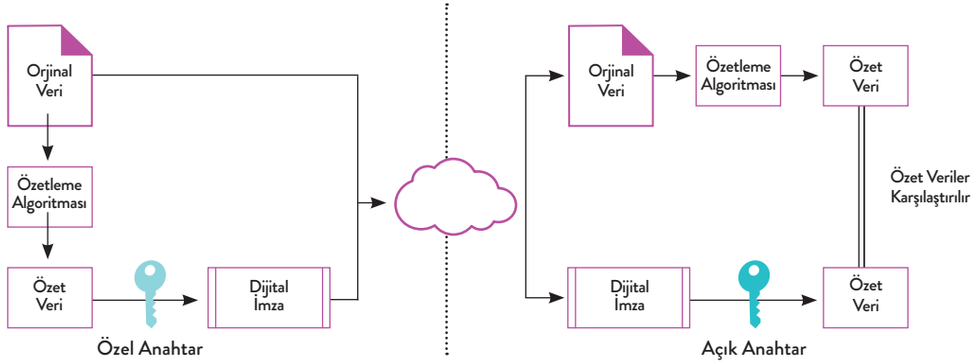
Bu senaryo, alınan bir verinin gerçekten gönderdiği iddia edilen kaynaktan gelip gelmediğini ve transfer edilmesi sırasında içeriğine dış bir kaynak tarafından müdahale edilmediğini kontrol etmek/doğrulamak amacı ile kullanılmaktadır.

Bir önceki senaryoya benzer bir şekilde A kişisinin B kişisine bu yaklaşımla

bir mesaj göndermek istediğini varsayalım, bu durumda akış şu şekilde gerçekleşecektir:

- ✔ A, B ile açık anahtar bilgisini paylaşır (ya da B, A'nın açık anahtar bilgisini güvenilir bir kaynaktan temin eder).
- ✔ A, B'ye göndermek istediği mesajı hazırlar.
- ✔ Bir özetleme algoritması (SHA-256 gibi) mesajın özet değerini oluşturur.
- ✔ Bu özet değerini kendisine ait özel anahtar ile şifreleyip ek bir bilgi olarak mesaja ekler. Bunu bir dokümanı imzalamak olarak düşünebiliriz.
- ✔ Mesajı B'ye gönderir.
- ✔ B, mesajı aldığında;
  - Mesajın özet değerini oluşturur
  - Mesaj içerisinde A tarafından eklenmiş şifreli özet bilgisini A'nın açık anahtarı ile çözümler
  - Kendi oluşturduğu özet bilgisi ile çözümlenmiş özet bilgisini karşılaştırır.
- ✔ Eğer iki özet bilgi karşılaştırıldığında birbirleri ile aynı içeriğe sahip değillerse bunun iki sebebi olabilir:
  - mesajı imzalayan kişi A değildir.
  - mesaj içeriğine transfer sırasında müdahale edilmiştir.

Şekil 18: **Digital imza**



Temel olarak Blockchain dünyasında kullanılan şifreleme yaklaşım ve yöntemlerine dair vereceğimiz teknik bilgiler bu kadar. Şimdi bu bilgilerin de ışığında, teknik açıdan Blockchain ağlarına göz atacağız.

2.2. Teknik Detayları ile Blockchain

Artık daha teknik denizlere girmek için ihtiyaç duyduğumuz tüm temel araçlara ve bilgilere sahibiz. Şimdi önceki bölümlerde ekilen ve filizlenen fikri fidanlarımızı büyütebiliriz.

Blockchain ağlarını, temel olarak değer içeren verilerin (para, kimlik, değerli kağıtlar gibi) **güvenli** ve **emin** bir şekilde **depolanması** ve **yönetilmesi** için tasarlanmış bir teknoloji olarak tanımlamıştık.

Bu tanımda belirtilen niteliklerin sağlanabilmesi için günümüzde bankalar gibi çeşitli ara kurumlar, kapalı merkezi sistemler kullanırken (örneğin hesabınıza ait bilgilerin bir bankanın merkezi veri yapısında tutulması gibi); Blockchain ağlarının bu ihtiyaçlara karşılık olarak herkese açık, şeffaf, merkezi olmayan, ara yapılara ihtiyaç duymayan bir çözüm önerdiğini biliyoruz.

Bu çözüm için temel kavramlar ve bileşenler şöyledir:

Blok

Adından da anlaşılabileceği gibi, Blockchain yaklaşımında verilerin saklandığı yapılar blok (block) olarak adlandırılır. Ve bu blok yapıları bir zincir

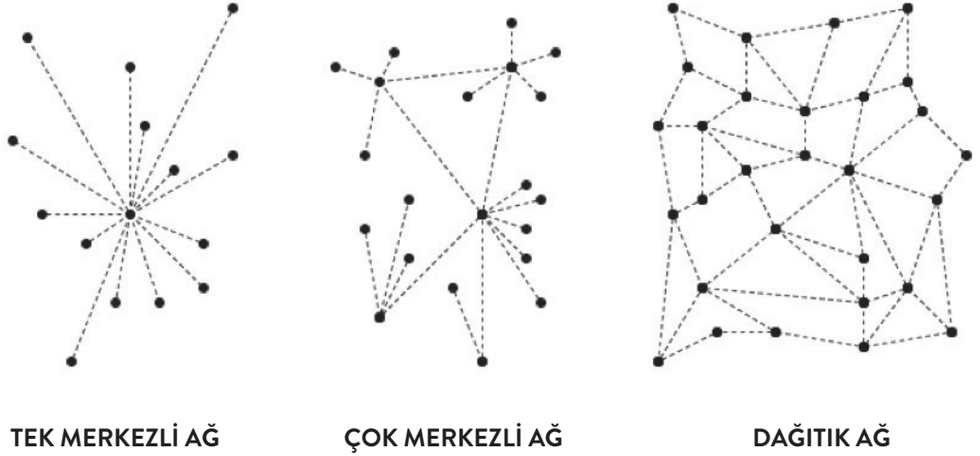
Şekil 3: **İlk Blok (Genesis) kaydından sonra tüm blokların birbirini takip ettiği yapı**

şeklinde (zaman açısından doğrusal bir dizi yapısında) düzenlenir. Bu zincir kapsamındaki ilk blok yapısına "**genesis**" (başlangıç) blok denir.

Dağıtık Ağ Yapısı

Günümüz yaklaşımlarında kapalı merkezi sistemler kullanıldığını belirtmiştik. Blockchain yapısında ise tüm bilgiler dağıtık **(distributed),** katılımcılara açık bir ağ yapısı üzerindeki tüm makinelerde **eşlenik** (birbirinin kopyası) halde tutulmaktadır. Bu şekilde tekil bir ara kuruma ihtiyaç kalmayıp, bu durumun getirdiği maliyetler ve riskler (single point of failure / tekil kırılma noktası: çalışmaması durumunda içinde bulunduğu tüm sistemin, akışın çalışmasına engel olma) ortadan kaldırılmaktadır.

Şekil 7: **Dağıtık Ağ**



Mutabakat Yapısı ve Süreci

Bir üst maddede, Blockchain ağındaki verinin eşlenik bir kopyasının, ağ yapısı üzerindeki tüm makinelerde barındırıldığını belirtmiştik. Bunun sağlanabilmesi için, ağ genelinde **Mutabakat (Consensus)** yapılmasına ihtiyaç vardır.

Blockchain ağlarında verilerin, blok adı verilen yapılarda tutulduğunu biliyoruz. Blockchain ağlarında "güvenlik" yaklaşımı, blokların içerdiği bilgilerin dış dünyadan saklanmasını değil, her bir bloğun içerdiği bilgilerin fark edilmeden değiştirilemeyeceğini vurgular. Bunun sağlanması için de **Kriptografik Özetleme (Cryptographic Hashing)** ve zaman bilgisi kullanılır.

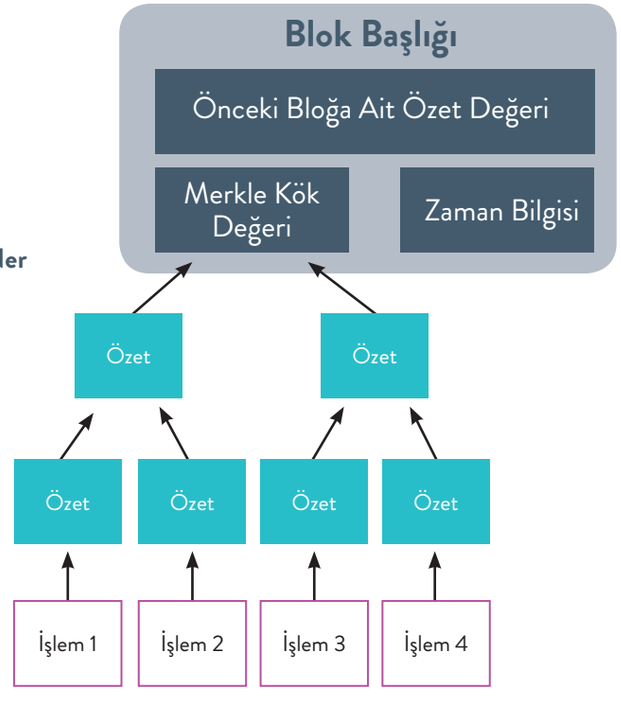
Blok, temel olarak iki parçadan oluşur:

- ✔ Blok içerisindeki veriler.
- ✔ Blok içerisindeki veri bütünlüğünü kontrol etmek amaçlı üst bilgi/başlık **(Block Header).**

Bir blok başlığı, aşağıdaki bilgileri içerir:

- ✔ Bir önceki bloğa **(üst blok)** ait **özet (hash)** değeri.
- ✔ Blok içerisindeki verilere ait **Merkle kök değeri** (bunu kısaca tüm verilerden tek bir özetleme verisine erişme şekli olarak düşünebiliriz).
- ✔ Zaman bilgisi.

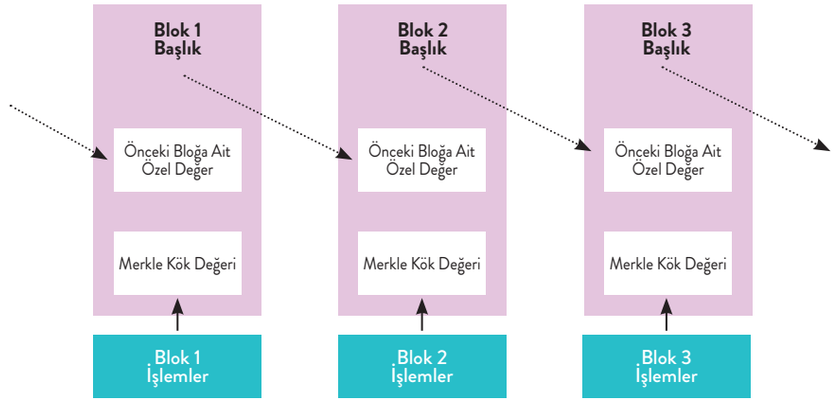
Şekil 19: **Blok Header**



Blok başlığı içindeki bilgilerin, toplu bir şekilde, güvenli özetleme algoritmasından geçirilmesi ile o bloğa ait olan özetleme bilgisine (block hash) ulaşılır.

Fark edebileceğiniz gibi her blok kendisinden önceki bloğa ait özetleme bilgisini içermektedir. Bu bilgiyi içeren bloğun özeti ise bir sonraki blok için kullanılacak özetleme bilgisini elde etmekte kullanılmaktadır.

Şekil 20: **Blok Data**



Bu yapıda, kötü niyetli birisinin, Blockchain ağı üzerinde hedef aldığı bir blok içeriğini değiştirebilmesi için, hem hedef bloğu hem de ondan sonra gelen tüm blokları değiştirmesi gerekmektedir. Blok üretiminin sürekliliği (saldırgan değişim yaparken Blockchain'e yeni blokların katılıyor olması) ve blok üretim yaklaşımlarının yapılarından dolayı, bu senaryo teorik olarak gerçekleştirilebilecek olsa da pratikte gerçekleştirilmesi normal koşullarda mümkün görülmemektedir.

Dağıtık bir mimaride bulunan her bir **düğüm** (alternatif olarak "makine" ifadesi kullanılabilir. İngilizce orijinal kullanımı ise "**node**" kelimesi ile ifade edilir.) üzerindeki blokların eşlenik bir yapıda olabilmesi için, bu makinelerin (düğümlerin) sisteme eklenmek istenen her yeni blok için bir mutabakat yaklaşımı sergilemesi gerekmektedir. Blockchain platformları bu konuda farklı çözümler sunmaktadır.

Bunlardan en çok kullanılan üç tanesini aşağıda inceliyoruz:

Emeğin İspatı: Proof of Work

Bu yapıda sistemin bir blok yapısı hazırlanıp, ilgili Blockchain ağına eklenmesinin yönetimi için, çözülmesi zor ama çözümün doğruluğunun kolay kontrol edildiği bir problem üzerinden ilerlenir. Bu konuda en çok kullanılan problem türü, hazırlanan bloğa ait özetleme (hash) değerinin belirli bir yapıya (tanımlanmış bir değer aralığı içerisinde olma, belirli bir karakter dizisi ile başlama gibi) uymasıdır. Özetleme (hash) fonksiyonları yapı itibari ile tek yönlü olduklarından ve çıktıları tahmin edilemediğinden, uygun bir değer üretilmesi için oldukça fazla sayıda deneme yapılması gerekmektedir. Örneğin Bitcoin yapısında Nisan 2017 itibari ile saniyede ortalama 3,5x10^15 hash işlemi yapılmakta ve ortalama olarak 10 dakikada bir **Proof of Work** yapısına uygun blok üretilebilmektedir. Ancak paylaşılan bir özetleme (hash) değerinin kontrolü için sadece ilgili blok içerisinde özetleme (hash) değerinin bir defa hesaplanması yeterlidir.

Şu andaki en popüler Blockchain platformu olan Bitcoin üzerinde bu mutabakat yaklaşımı kullanılmakta ve ilgili süreç, **madencilik (mining)** olarak adlandırılmaktadır.

Bu süreci, basit bir şekilde aşağıdaki gibi bir akışla ifade edebiliriz:

- ✔ Yeni blok içerisinde yer alması istenen işlemler/veriler seçilir.
- ✔ Bu işlemler/veriler kullanılarak Merkle ağacı yapısı ve Merkle kök değeri oluşturulur.
- ✔ Merkle kök değeri, bir önceki bloğun özetleme değeri, zaman bilgisi ve ardışık olarak artan bir sayaç olarak tanımlanabilecek “nonce” değeri kullanılarak blok başlığı oluşturulur.
- ✔ Blok başlığı özetlenerek (hashing) uygun bir değer (belirli bir karakter kümesi ile mi başlıyor gibi) oluşup oluşmadığı kontrol edilir.
- ✔ Eğer uygun bir blok özetleme değeri oluştu ise yeni blok başarılı bir şekilde oluşturulmuş demektir, bu bilgi ağ üzerindeki tüm makineler ile paylaşılır.
- ✔ Eğer uygun bir blok özetleme değeri oluşmadı ise **nonce** değeri arttırılarak uygun özetleme değeri yaratılmaya çalışılır. Nonce değeri limitine geldiğinde hala geçerli bir blok oluşturulamadı ise (yani geçerli bir özetleme değeri oluşturulamadı ise) bu durumda blok başlığını oluşturan diğer değerlerde (blok içerisinde yer alacak işlemler kümesinin sırası, içeriği gibi) güncelleme yapılır ve akış tekrar baştan ele alınır.

Başka bir popüler Blockchain platformu olan Ethereum da bu yaklaşımı kullanmaktadır. **Proof of Work** yaklaşımı, yapısındaki işlemin özel yapısı ve yüksek frekansta tekrarlanma ihtiyacından dolayı yüksek enerji tüketimi ve özel donanım gereksinimleri ortaya çıkartabilmektedir. Bu durum, çalıştığı ağ yapısının bu gereksinimlerin daha elverişli olduğu (ucuz elektrik, düşük maliyetli donanım üretebilme yetkinliği) ortamlara yönlendirilmesine ve dağıtık, merkezi olmayan ağ yapısı özelliğinin zamanla belirli ölçüde kaybolmasına neden olabilmektedir. Gerek kullanılan problemlerin farklılaştırılması, gerekse enerji tüketimi çıktılarının farklı şekillerde değerlendirilmesi gibi yaklaşımlarla bu sorun çözülmeye çalışılmaktadır.

Sahipliğin İspatı: Proof of Stake

Bu yaklaşım kapsamında blok üretim ve geçerlilik onay mekanizması, bloğu üreten makinenin ilgili Blockchain ağı üzerinde sahip olduğu pay ile ilişkilendirilir. Bu tarz sistemlerde genellikle sistem içerisinde üretilebilecek tüm kripto para miktarı ilk başta üretilir, sistemdeki üyeler yatırımlarına göre paylarına düşen kripto paralarını alırlar, sonradan yeni eklemeler yapılmaz. Sistem kapsamındaki pay değeri, sahip olunan kripto para miktarına göre hesaplanır.

Pay miktarına göre işlem yapma konusunda farklı yöntemler, davranış biçimleri olabilir. İşte bunlardan bazıları:

- ✔ Bir sonraki bloğu üretecek olan makine, sahip olduğu pay ile ilişkilendirilmiş bir rastlantısal fonksiyon ile belirlenebilir, zira payı yüksek olan makinenin seçilme şansı daha yüksektir. İlgili makine belirli bir süre içerisinde uygun bir blok paylaşmaz ise bir sonraki makineye geçilir.
- ✔ Bir makine belirlemesi yapılmaz, ancak pay bilgisi makinenin çözmesi gereken problemin (**Proof of Work** yaklaşımına benzer bir şekilde) zorluk derecesini değiştirir. Örneğin daha fazla pay sahibi olan makine için daha kolay bir problem çözüm aralığı sağlanır.

Tek başına sahip olunan pay değerinin kullanılmasının yüksek pay sahibi makinelere için sürekli bir avantaj yaratmasından dolayı, akış içerisindeki hesaplamalarda kullanılmak üzere bir "**yaş" (age)** kavramı da getirilmiştir. Bu kavram ile birlikte blok üretimi için kullanılan pay kapsamındaki kripto paraların yaş değerleri sıfırlanır, bu kripto paralar ancak belirli bir süre sonunda yaş değeri kazanmaya başlarlar ve yaş değeri işlemlerde öncelik/geçerlilik kazanmada avantaj sağlayıcı olur.

Bu yaklaşım kapsamında blok üretimi süreci, **para basma (forging, minting)** olarak adlandırılmaktadır.

Şu anda "**Proof of Work**" mantığı ile ilerleyen Ethereum ağının, yakın zaman içerisinde "**Proof of Stake**" yapısına geçirilmesi planlanmaktadır. Bu yapı, aslında daha kompleks bir uygulama şekli olsa da, bu geçiş ile birlikte işlemlerin doğrulanma ve blok oluşturma süreci daha hızlı ve kolay bir hale getirilerek, Bitcoin ağında olduğu gibi pahalı ve yüksek güç tüketimine sahip özel madencilik donanımlarına olan ihtiyacı (ve dolaylı olarak oluşan donanım tabanlı merkezciliği) ortadan kaldırılacaktır. Ayrıca katılımcıların platform ile daha derin sahiplik ilişkisi geliştirmesi sağlanarak, platformun çıkarına en uygun şekilde çalışmaları teşvik edilecektir. Bu dönüşüm ile birlikte Ethereum platformu, daha büyük uygulamaları barındırmak için daha ölçeklenebilir bir hale getirilecektir.

Practical Byzantine Fault Tolerance – PBFT

Bu yapı adını, Bizanslı generallerin kullandığı bir yöntemden almaktadır. Bizans İmparatorluğu'nda, imparatordan gelen emirlerin gerçek olup olmadığını anlamak için, generallerin kullandığı oldukça basit ve etkili bir yöntem kullanılmaktaydı. İmparator, ordusuna bir emir vereceği zaman bunu generallere ulaştırmak için birden fazla ulak yollamakta ve generaller de emri aldıklarında kendi aralarında ulaklar ile bu emirleri paylaşmaktaydılar. Bu süreç içinde eğer imparatordan gelen emir ulakların çoğunluğu tarafından doğrulanmış ise bu emrin doğru olduğu kabul edilmekte, aksi takdirde tekil emirlere itimat gösterilmemekteydi.

Bu çözüm, Blockchain dünyasında ise şöyle kullanılmaktadır: Ağ yapısına dahil her **doğrulayıcı (validator)** rolüne sahip makine için özel bir açık-gizli anahtar ikilisi yer almakta ve her makine diğer makinelerin açık anahtar bilgisine sahip bulunmaktadır.

Her makine, kendisine gelen bir **işlem (transaction)** bilgisini, kendi üzerinde tutulan veri yapısını kullanılarak kontrol eder, onayladığı bir işlemi imzalayarak ağ ile paylaşır. Eğer bir işlem belirli bir sayıda (mesela 2n makineden oluşan bir ağ için bu sayı n+1 olabilir) makine tarafından onaylanmış ise mutabakat sağlanmış kabul edilir ve bu işlem ağ tarafından geçerli işlem olarak tanımlanır.

Proof of Work, Proof of Stake gibi yaklaşımlardan farklı olarak, **PBFT** kaynak sahipliği (donanım, pay gibi) akış içerisinde soyutlanmakta, bu sayede en küçük katılımcı bile dahil olduğu ağın yapısında söz sahibi olmaktadır.

Bu yaklaşım kapsamında ağa dahil olan tüm doğrulayıcı makinelerin birbirinden haberdar olması ve ağa dahil olacak yeni bir doğrulayıcının merkezi bir sistem/yapı tarafından onaylanması gerekmektedir. Bu durum Blockchain yaklaşımının temellerinden olan "herkese açık, merkezi olmayan ağ yapısı" kavramı ile çelişmektedir. Bundan dolayı bu mutabakat yaklaşımı, açık (public) yapılar yerine, daha çok özel (private) yapılar içerisinde değerlendirilmektedir.

HyperLedger platformu kapsamında, varsayılan mutabakat yapısı olarak PBFT kullanılmaktadır.

Bu üç yaklaşımın dışında, proof of work ve proof of stake'in birlikte uygulanması ile gerçekleşen "proof of activity"; ayrıca blok üretim sürecine dahil olmak için disk alanı tahsis edilmesini gerektiren "proof of capacity" gibi farklı mutabakat çözümleri de bulunmaktadır. Ancak bu alternatifler, daha çok küçük ölçekli denemeler kapsamında kullanılmaktadır.

En Uzun Blockchain Kaydı

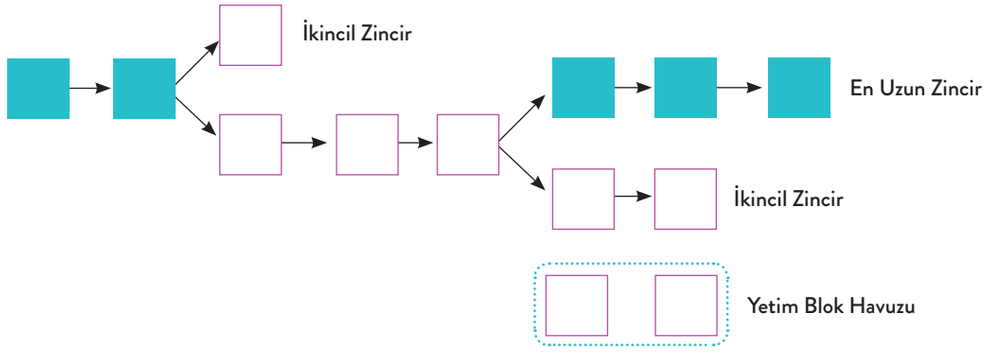
Dağıtık, merkezi olmayan büyük ölçekli bir mimaride, bağlı her bir makinedeki blok yapısının her zaman tutarlı olması beklenemez. Sistem içerisinde yakın zamanlı paralel blok üretimi, blokların ağ üzerindeki makinelere farklı zamanlarda iletilmesi gibi nedenlerden dolayı, ağa bağlı makineler üzerinde Blockchain ağında farklı blok sıralamasına sahip **düğümlerin (node)** bulunması karşılaşılan bir durumdur. Bu durumu çözebilmek için makineler her zaman "**en uzun Blockchain kaydı geçerlidir**" mantığı ile hareket edip, bu Blockchain kaydını genişletmek amacı ile işlem yaparlar. "**En uzun**" yaklaşımı farklı mutabakat yapılarında farklı anlamlara gelebilmektedir, örneğin "Proof-of-Work" yapılarında en fazla Proof of Work'ün gerçekleştiği Blockchain yapısı (bu bilgi ilgili Blockchain ağını oluşturan blokların problem zorluk derecelerinin bir araya getirilmesi ile hesaplanır), "**En Uzun Blockchain Kaydı**" olarak tanımlanmaktadır.

Bir makineye yeni bir blok aday olarak iletildiğinde, öncelikle içeriği incelenerek geçerlilik kontrolü yapılır, sonrasında ise bağlı olduğu üst blok bulunarak Blockchain ağına eklenmeye çalışılır. Bu durumda üç farklı davranış şekli söz konusudur:

- ✔ Gelen blok, en uzun blok yapısının sonuna eklenir (bloğun ilişkili olduğu üst blok, geçerli en uzun Blockchain kaydının son bloğudur). Bunun ile alakalı şemayı aşağıda görebilirsiniz.

- ✔ Gelen blok yapısının bağlı olduğu üst blok, en uzun Blockchain kaydı yapısında sonuncu blok olmadığı durumlarda, ana Blockchain yapısı üzerinde çatallaşmaya **(fork)** yol açar - bu dallara "i**kincil zincir" (secondary chain)** adı verilir. Bir ikincil zincir, o an olmasa da zamanla "en uzun zincir" özelliğine sahip olabilir, bu durumda kendisi ana Blockchain'e dönüşürken o esnada geçerli olan ana Blockchain artık bir ikincil zincir olarak değerlendirilmeye başlanır.
- ✔ Gelen blok yapısının bilinen bir zincir yapısında bağlı olduğu üst blok bulunamaz ve bu durumda söz konusu bloklar **"yetim" (orphan)** olarak adlandırılır. Bu tarz bloklar, genelde birbirini takip eden hızlı blok üretimi durumlarında, blokların ilgili makineye ağ yapısındaki gecikmeler vb. nedenlerden dolayı ters sıralama ile varmasından dolayı oluşur. Bu tarz bloklar, genel olarak ilgili üst blokları ilgili makineye gelinceye kadar, makine üzerinde ayrı bir havuz yapısında tutulurlar.

Şekil 21: **Yetim Zincir**



Blockchain yapılarında çatallaşma sık karşılaşılan bir durumdur. Örneğin Bitcoin Blockchain yapısında, haftada bir, tek blokluk çatallaşma görülmesi normaldir, bunun ötesindeki çatallaşmalar çok nadir görülür. Blok üretim zamanları düşük olan sistemlerde çatal oluşma olasılığı artmaktadır. Ortalama olarak 2.5 dakikada bir blok üretimi yapılan Litecoin'de, Bitcoin'e kıyasla çok daha fazla çatallaşma oluşmaktadır.

Çatallaşma konusundaki en bilinen olaylardan birisi, 2016 yılında Ethereum platformu üzerinde yaşanan Mecburi Çatallaşma olayı olmuştur. Bu olayın detaylarını, Zorluklar ve Riskler bölümünde ele almıştık.

Yukarıda ağa bağlı makinelerin her zaman "en uzun Blockchain kaydı" mantığı ile hareket edip, bu Blockchain ağını genişletmek amacı ile işlem yaptıklarından bahsetmiştik. Makineler için bu şekilde işlem yapmalarının ana motivasyonu kazanç sağlayabilmektir.

Ağa bağlı ve blok üretimi yapan bir makinenin kazanç sağlayabilmesinin yolu, Blockchain üzerinde geçerli bir blok üretebilmesinden geçmektedir ve bu yaklaşıma **teşvik (incentive)** mekanizması denmektedir. Burada iki türlü gelir kazanılabilir:

- ✔ Bazı Blockchain yapıları, blok üretimi yapan makineleri belirli bir kripto para karşılığı ile ödüllendirmektedir. Örneğin Bitcoin, her başarılı blok üretimi için 12,5 BTC ödüllendirme yapmaktadır.
- ✔ Bir bloğa ait giriş ve çıkış değerleri arasında fark olması durumunda, aradaki fark ilgili bloğu üreten makinenin hesabına yansıtılır. Elbette, burada sadece pozitif fark olabilir, toplam çıkış değeri toplam giriş değerinden büyük olamaz.

Bu gelir akışları, üretilen blok içerisinde birer **işlem (transaction)** olarak belirtildiklerinden geçerli olmasının ve sonraki işlemlerde kullanılabilmesinin tek yolu, üretilen bloğun ana Blockchain ağı yapısına dahil olmasıdır. Bundan dolayı ağa bağlı makineler, her zaman geçerli (yani en uzun) Blockchain'i genişletmek amacı ile hareket ederler.

Çatallaşma (Fork)

Bu kavramı Zorluklar ve Riskler bölümünde ele almıştık, ancak teknik olarak hızlıca üzerinden tekrar geçmekte fayda var:

Soft Fork (Tercihi Çatallaşma): Bu durum genel olarak blok kabul kurallarında yapılan düzenlemeler sonucunda gözlemlenir. Yeni kurallar eski kuralların bir alt kümesi olduğundan dolayı, yeni mutabakat kurallarını kullanan makineler tarafından üretilen bloklar, güncelleme yapmamış makineler tarafından doğrulanabilirler ve kendi zincirlerine kopyalanabilirler. Ancak güncelleme yapmayan noktalar mutabakat sürecine katılarak yeni blok yaratamazlar.

Hard Fork (Mecburi Çatallaşma): Bu durum yeni kurallar ile eski kurallar arasında uzaklaşma olduğu durumda gözlemlenir. Eski kural kümesinde olmayan kurallar, artık yeni kural kümesi içerisinde bulunmaktadır. Yeni mutabakat kurallarını kullanan makineler tarafından üretilen bloklar, güncelleme yapmamış makineler tarafından doğrulanamazlar ve kendi zincirlerine eklenemezler. Blockchain ağının ikiye bölünmesiyle, Mecburi Çatallaşma ortaya çıkar.

2.3. Teknik Detayları ile Akıllı Sözleşmelere Bakış

Akıllı Sözleşme kavramı, Blockchain ağlarından bağımsız olarak, ilk kez 1994 yılında, bir bilgisayar bilimcisi ve matematikçi olan Nick Szabo tarafından, çeşitli taraflar arasındaki etkileşimleri güvenli hale getirip uygun şekilde yürütülmesini sağlayan bilgisayar programlarını/sistemlerini tanımlamak amacı ile ortaya atılmıştır[31].

Bitcoin'in ortaya çıkmasından kısa bir süre sonra, arkasındaki Blockchain platformunun eşler arası (p2p) para gönderimi dışındaki farklı senaryolar kapsamında da kullanılabileceği öngörülerek, örnek çalışmalar yapılmaya başlanmıştır. Ancak Bitcoin Blockchain yapısının belirli bir iş modeline göre tasarlanmış olmasının getirdiği kısıtlamalardan dolayı bu denemeler, genel olarak aşağıdaki yöntemlerle gerçekleştirilmiştir:

- ✔ Açık kaynak kodlu olan Bitcoin Blockchain yapısının kod seviyesinde değiştirilmesi ve senaryoya uygun Blockchain alt yapısının oluşturulması,
- ✔ Bitcoin Blockchain platformunu sadece veri tutma amaçlı kullanıp, bir üst uygulama seviyesinde bu veriyi kullanan uygulamaların hazırlanması.

[31] *http://bit.ly/BC101sc*

Ancak bu yöntemlerin uygulaması konusunda çeşitli sıkıntılar gözlemlenmiştir:

- ✔ Kaynak kodu üzerinde her uygulama için değişiklik yapmak ve bu değişikliği yönetebilmek (test, ana kaynak kodu üzerindeki güncellemelerin aktarılması gibi) yüksek bir maliyet getirmektedir.
- ✔ Yeni oluşturulan bir Blockchain alt yapısının kullanılabilir olması için, bir ağ yapısının oluşturulmasına ve katılımcıların ikna edilmesine ihtiyaç duyulmaktadır.
- ✔ Bitcoin Blockchain platformunun kullanılması durumunda, tutulan verinin anlamlandırılmasının başka bir uygulamaya aktarılması, platforma duyulan "güven" duygusunu azaltmaktadır.

Tüm bu gelişmeler devam ederken, 2013 yılının sonuna doğru, **Vitalik Buterin** adlı Rus asıllı Kanadalı bir üniversite öğrencisi, **Ethereum** adını verdiği, genel bir betik dil yapısı ile geliştirilecek uygulamaların çalıştırılmasına izin veren, ortak ve tekil bir Blockchain platformunu anlatan bir çalışma yayınladı. Buterin'in bu çalışma içerisinde uygulamaları tanımlarken "Akıllı Sözleşme" kavramını kullanması, sonrasında geçmişten gelen bu kavramın sıklıkla Blockchain teknolojisi içerisinde kullanılmaya başlamasına neden oldu[32].

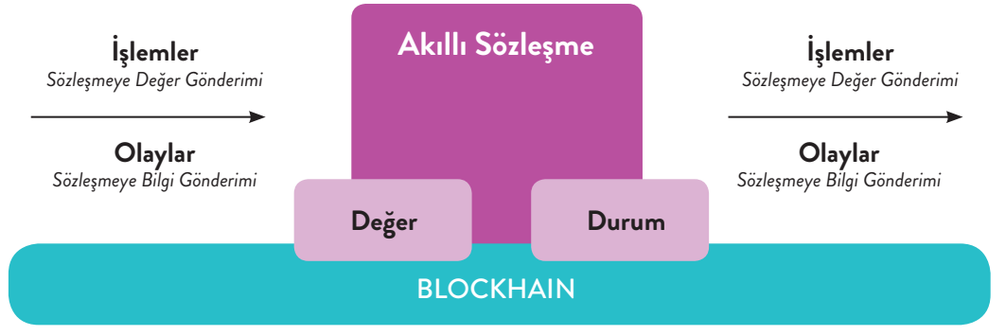
Nick Szabo'nun yaklaşımını Blockchain teknolojisi ile etkileşimli bir şekilde incelersek, Akıllı Sözleşmeler;

- ✔ İçinde mantıksal akışların önceden yazılmış olduğu ('eğer bu olursa şunu yap' tarzı akışlar içeren) bir bilgisayar kod bloğu,
- ✔ Dağıtık, merkezi olmayan bir platform üzerinde saklanıp çoğaltılabilen (Blockchain Ağları),
- ✔ Bir bilgisayar ağı tarafından çalıştırılan/işletilen (Blockchain ağının dağıtıldığı bilgisayar ağı),
- ✔ Güvenilirliği bir bilgisayar ağı (Blockchain ağı) tarafından doğrulanan,

[32] *http://bit.ly/BC101wpe*

- ✔ Üzerinde bulunduğu yapı veya platformda güncellemelere yol açabilen (kripto para ödemeleri/transferleri, yeni akıllı sözleşmelerin yaratılması) ufak programlardır şeklinde tanımlanabilir.

Şekil 22: **Akıllı Sözleşme**



Akıllı Sözleşmeler, ilişkili tarafların kapsam üzerinde anlaşmalarından sonra hazırlanıp, kriptografik olarak imzalanıp, Blockchain ağına yüklenirler. Yüklenmiş sözleşmeler, Blockchain ağı üzerinde olan diğer bileşenlerle etkileşim kurabilirler (kendisi diğer bileşenlere ya da diğer bileşenler sözleşmeye bilgi içeren mesajlar gönderebilir). Bu etkileşim bir işlemin (transaction) başlatılması olabileceği gibi bir bilginin gönderilmesi/teslim alınması şeklinde olabilir. Sözleşme hazırlanırken belirlenmiş durumlar oluştuğunda (bu konuda bir mesaj alınması gibi), akıllı sözleşmeler otomatik olarak içerisinde tanımlanmış olan anlaşma koşullarının çalıştırılmasını sağlar.

Örneğin; bir vadeli işlem ve opsiyon akıllı sözleşmesi, ilişkili hisse senedinin işlem fiyatının önceden belirlenmiş bir değere ulaşması durumunda ilgili taraflar arasında karşılıklı hisse transfer ve ödeme işlemlerini tetikleyebilir.

Bir diğer örnek olarak; bir sigorta akıllı sözleşmesi, hava durumu veri kaynağı ile ilişkiye geçerek yağmur oranının belirli bir seviyenin altına

düşmesi durumunda taraf olan üreticiye ilgili sigorta ödemesinin gerçekleşmesini tetikleyebilir.

Farklı bir örnek ise; bir borç için tahsil tarihi geldiğinde ilişkili tarafa ödeme yapılmasını, ödeme yapılacak hesapta yeterli bakiye olmaması durumunda kendisini oluşturan çek defteri akıllı sözleşmesinin dondurulmasını tetikleyebilir.

Şekil 23: **Örnek Bir Ethereum Akıllı Sözleşmesi**

```
contract BasicBank {
    mapping(address => uint) private balances;
    address public owner;
    event LogDepositMade(address accountAddress, uint amount);

    function BasicBank() public {
        owner = msg.sender;
    }

    function deposit() public payable returns(uint) {
        balances[msg.sender] += msg.value;
        emit LogDepositMade(msg.sender, msg.value);
        return balances[msg.sender];
    }

    function withdraw(uint withdrawAmount) public returns(uint) {
        require(balances[msg.sender] >= withdrawAmount);
        balances[msg.sender] -= withdrawAmount;
        msg.sender.transfer(withdrawAmount))
        balances[msg.sender] += withdrawAmount;
        return balances[msg.sender];
    }

    function balance() public view returns(uint) {
        return balances[msg.sender];
    }
}
```

Akıllı sözleşmeler daha çok Ethereum Blockchain Ağı kapsamında ortaya çıkmış olarak görünüyor olsa da, Bitcoin Blockchain Ağı da para transferinin birden fazla taraf tarafından onaylanması **(multisign)**, para transferinin belirli bir süre sonra devreye girmesi **(check timelock)** gibi

basit anlamda akıllı sözleşmelere destek sunmaktadır. Ayrıca günümüzde özellikle yakın zamanda, ortaya çıkan Blockchain platformlarının çok büyük bir kısmı kendi içlerinde, farklı isimler altında olsa da (Hyperledger Fabric kapsamında "Chaincode" gibi), Akıllı Sözleşme yapılarına destek vermektedir. Platformlar, akıllı sözleşme geliştirme konusunda, mevcut programlama dillerini (C#, Java, Go) kullanabildikleri gibi kendileri tarafından ortaya atılan yeni programlama dillerini de kullanabilmektedirler (Solidity, Viper).

Akıllı sözleşmeler, şu anda kullanımda olan geleneksel sözleşme yapılarına karşı çeşitli avantajlar sunmaktadır. Bunlar arasında özellikle göze çarpan avantajlarını şöyle sıralayabiliriz:

- ✔ Akıllı sözleşmeler genel olarak elle yürütülen süreçleri yazılım tabanlı olarak otomatikleştirdikleri için iş akışlarına hız kazandırır.
- ✔ Akıllı sözleşmeler ile otomatikleşen işlemler, insan kaynaklı hatalara karşı daha dayanıklıdır.
- ✔ Akıllı sözleşmelerin merkezi bir yapı yerine ağ üzerinde dağıtık olarak uygulanması, manipülasyon, yerine getirilmeme gibi riskleri düşürmektedir.
- ✔ Akıllı sözleşmeler, "güven" amaçlı aracı kurumlara duyulan ihtiyacı azaltmaktadır.
- ✔ Akıllı sözleşmeler, daha az insan girdisine/takibine ihtiyaç duyması ve aracı kurumlara daha az bağımlı olmasından dolayı daha düşük maliyetlidir.

Akıllı sözleşmeler konusunda genelde, yukarıda belirttiğimiz noktalar temel alınarak, oldukça pozitif değerlendirmeler yapılsa da hala emekleme aşamasında olan bir teknolojik yaklaşım olduğu ve çözülmesi gereken temel sorunların olduğu unutulmamalıdır.

İşte bunlardan bazıları:

İşlem Süresi

Şu andaki Blockchain yapıları, işlemlerin doğrulanıp blok mantığında eklenmesi aşamasında yüksek işlem sürelerine katlanmak zorundadırlar. Blockchain yapısında olmayan veri tabanlarında performans saniyede binlerce işlem cinsinden ölçümlenebilirken, örneğin Ethereum'da bu değer ortalama saniyede 10-15 işlem kadar sürmektedir. Kurumsal özel Blockchain platformları (Hyperledger Fabric, Corda, Ant Blockchain gibi) bu açıdan daha kabul edilebilir performans değerleri göstermektedir.

Geliştirme Zorluğu

Blockchain platformları oldukça yeni, sürekli gelişen kavramlar ve teknolojik ürünler olduklarından dolayı, akıllı sözleşme geliştirme süreçlerinde olması gereken karmaşık modeller tasarlayabilme, otomatik test yapıları oluşturma, otomatik olarak ağa yükleme gibi konularda geliştiricilerine halihazırdaki yazılım geliştirme platformlarında bulunan kolaylıkları sağlayamamaktadır. Blockchain platformları Truffle (Ethereum), Hyperledger Composer (Hyperledger Fabric) gibi yardımcı geliştirme ortamları, araçları sunarak bu zorlukları minimize etmeye çalışmaktadırlar.

Dış Bilgiye Erişim

Akıllı sözleşmelerin sadece Blockchain ağları üzerindeki bilgilere erişimleri olduğundan dolayı dış sistemlerdeki olayları ve bilgileri Blockchain yapılarına yönlendirecek güvenilir veri servislerine ihtiyaç duyulmaktadır. Bu tarz servislere **Kahin (Oracle)** adı verilmektedir. Yukarıdaki örneklerde, hava durumu bilgisini sağlayan servis bu kapsamda değerlendirilir.

Güvenlik

Blockchain yapıları kriptografik olarak veri güvenliği sağlıyor olsalar da Blockchain ağları üzerinde yapılan akıllı sözleşme tanımlarında, kullanılan platformların yapısının doğru anlaşılmaması kaynaklı hatalı uygulama yapılarının ortaya çıkabildiği gözlemlenmiştir. Singapur Ulusal Üniversitesi (National University of Singapore) tarafından yapılan akademik bir çalışmada[33] Ethereum üzerinde tanımlı 19.366 akıllı sözleşmeden 8.833 tanesinde, sözleşmenin manipüle edilip sonucunda kazanç elde edilebilecek güvenlik açıklarının olduğu tespit edilmiştir.

Esneklik

Blockchain tabanlı akıllı sözleşmelerin "değiştirilemez" yapısından dolayı, geliştiriciler sözleşme üzerinde değişiklik gerekebilecek tüm olası senaryoları önceden düşünmek ve sözleşme tanımına eklemek zorundadırlar. Bu, gerçek dünyada olması gereken esneklikler açısından sıkıntı yaratmaktadır. Bu duruma, bazı kurumsal özel Blockchain platformlarında (Hyperledger Fabric gibi) sağlanan "sözleşme sürümleme/ versiyonlama" gibi yaklaşımlarla çözüm getirilmektedir.

---

[33] *"Making Smart Contracts Smarter" - https://eprint.iacr.org/2016/633.pdf*

BÖLÜM III

BLOCKCHAIN 201: BLOCKCHAIN'İN ÖTESİ

Bölüm II

BLOCKCHAIN 201: BLOCKCHAIN'İN ÖTESİ

3.1. Diğer Dağıtık Kayıt Defteri Teknolojileri

Dağıtık kayıt defteri teknolojisi **(Distributed Ledger Technology - DLT)**, temel olarak birbirinden bağımsız cihazlardan oluşan bir ağ üzerine yayılmış bir veri tabanı olarak nitelendirilebilir. Bu yapıda her katılımcı, bu kayıt defterinin birebir kopyasını çoğaltıp, kendisi üzerinde saklar. Bu teknolojinin çığır açan özelliği, ağ kapsamında merkezi bir yapının bulunmamasıdır; yapılmak istenen güncellemeler (yani yaratılan yeni işlemler) bağımsız olarak her katılımcı tarafından oluşturulup, kaydedilebilir. Sonrasında sistem, merkezi bir yapıya ihtiyaç duymadan, bu güncellemeler üzerinde bir mutabakat süreci sağlar ve bunun sonucunda üzerinde mutabakata varılan kayıt yapısı, katılımcılar üzerinde bağımsız bir şekilde güncellenir.

Bu açıdan değerlendirdiğimizde Blockchain teknolojisi, asıl olarak kısaca DLT olarak tanımlanan bu teknolojinin en çok bilinen, en popüler uygulama şeklidir.

Zaman içerisinde, Blockchain teknolojisinin gerçek hayat içerisindeki uygulamalarında karşılaşılan bazı zorluklardan dolayı (ölçeklenebilirlik, madencilik maliyeti, işlem ücreti gibi), Blockchain teknolojisine alternatif DLT yaklaşımları bir çözüm önerisi olarak ortaya çıkmaya başlamıştır.

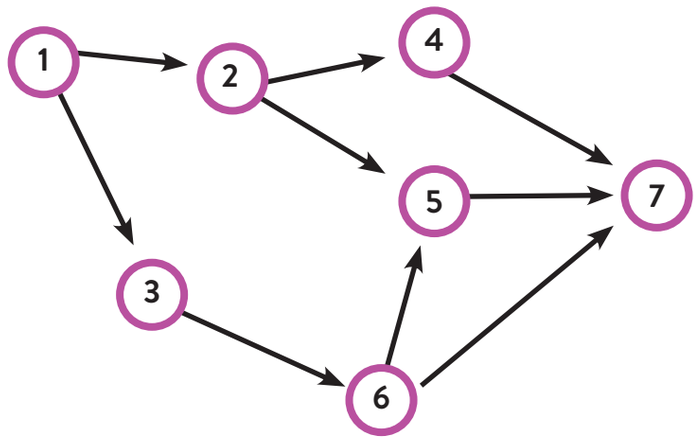
Bu bölümde, en popülerleri olan Tangle ve Hashgraph'i değerlendireceğiz.

Her iki yapıda da Yönlü Çevrimsiz Çizge **(Directed Acyclic Graph—DAG)** yapısını baz aldığından dolayı, bu iki teknolojiye giriş yapmadan önce bu konuya değinmeliyiz.

DAG yapısı düğümler (node) ve bunlar arasındaki ilişkilerden oluşmaktadır. Bu ilişkiler, tek yönlü olarak tanımlanmışlardır (grafik

üzerindeki ok işareti ilişkinin yönünü göstermektedir, örneğin aşağıdaki yapıda 1 → 2 gösterimi ile 1 ve 2 arasında bir ilişki olduğu ve bu ilişkinin yönünün 1'den 2'ye doğru olduğu ifade edilmektedir). Ayrıca, çevrimsiz (acyclic) yapıda olması nedeni ile bir düğümden başka düğüme giden bir yol varsa, aksi yönde bir yol (path) olmaması gerekmektedir (örneğin aşağıdaki yapıda 1'den başlayıp 5'de biten bir yol bulunmaktadır, çevrimsiz yapıdan dolayı bunun tersi yani 5'den başlayıp 1'de biten bir yol olamaz).

Şekil 24: **Directed Acyclic Graph - DAG**



Tangle

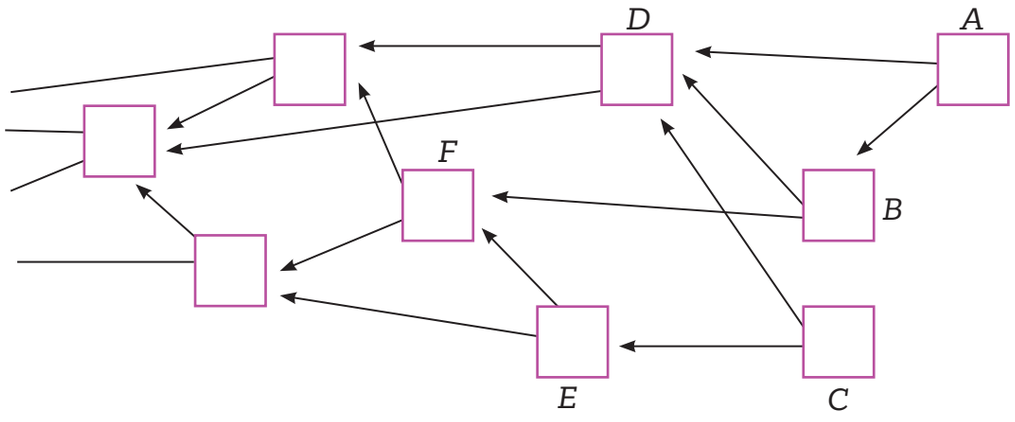
Genel olarak Nesnelerin Internet'i **(Internet of Things—IoT)** ekosistemi için bir kripto para çözümü olarak ortaya çıkarak popülerleşen **IOTA** platformunun arkasındaki teknoloji olarak bilinen Tangle, özellikle mikro ödemeler akışı içerisinde Blockchain teknolojisine alternatif bir DLT yaklaşımıdır.

Tangle'i incelediğimizde, Blockchain teknolojisindeki gibi bir zincir yapısı içerisinde birbiri ile ilişkili bloklar yerine, işlemlerin DAG yapısı içerisinde tutulduğunu görürüz. Bunu en basit şekilde bir ağaç yapısı olarak değerlendirebiliriz. Aslında her DAG için bir ağaç yapısı benzetmesi yapmak doğru değil ama Tangle içerisindeki kök, yani "genesis" işlem

varlığı ve her işlemin direk ya da dolaylı—directed/indirected—olarak bu işlem ile ilişkili olması, bu benzetmeyi doğru kılmaktadır.

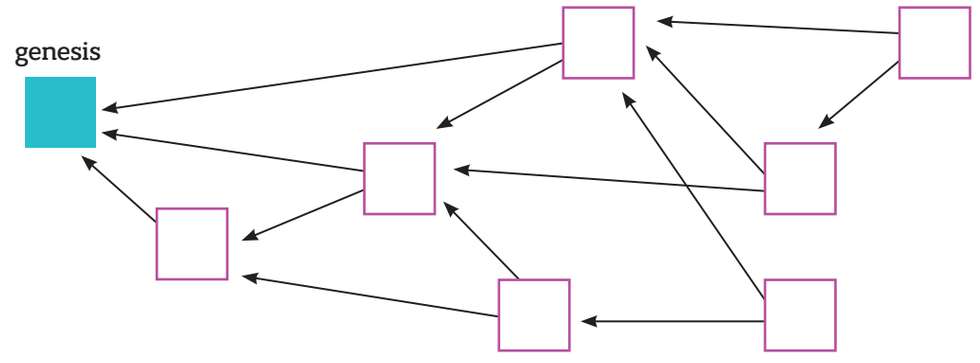
Tangle yapısındaki her işlem, DAG yapısı içerisinde bir düğüm olarak gösterilmektedir (işlemleri basit bir şekilde "A kişisinden B kişisine X birim IOTA gönderimi" olarak düşünebilirsiniz). Yeni bir işlem Tangle'a dahil olurken, daha önceki işlemlerden iki tanesini "onayladığını" **(approval)** belirtmelidir (bu onaylama ilişkisi, DAG yapısında yeni eklenen işlemden onaylanan işlemlere doğru yönlü gösterilir). aşağıdaki örnekte A işlemi (düğümü) Tangle'a dahil olurken, B ve D işlemlerini onaylamaktadır.
İki işlem arasında yönlü bir ilişki bulunmuyorsa ama en az iki birim uzunluğunda yönlü bir yol **(directed path)** bulunuyorsa, bu durum "dolaylı onaylama" **(indirected approval)** olarak adlandırılır. Aşağıdaki örnekte A → B ve B → F ilişkilerinden dolayı "A işlemi F işlemini dolaylı olarak onaylamaktadır" denilir.

Şekil 25: **Tangle1**



Tangle kapsamında "**genesis**" yani "başlangıç" işleminin varlığından bahsetmiştik, bu işlem direk ya da dolaylı bir şekilde diğer tüm işlemler tarafından onaylanmaktadır. Genesis işlemi, sistem içerisindeki tüm tokenların kurucu hesaplara dağıtımını içeren işlemdir.

Şekil 26: **Tangle2**



Tangle kapsamında, Bitcoin Blockchain yapısındaki gibi platform yaşam döngüsü içerisinde tekrardan bir token üretimi yapılması, "madenci" adı verilen sistemlerin parasal ödül kazanmaları gibi bir durum söz konusu değildir. Bitcoin Blockchain'i içerisindeki madencilik ile yapılan işlemlerin doğrulanarak sisteme eklenmesi yaklaşımı, Tangle kapsamında işlemi yayınlayan sistemin doğrulama akışını üstlenmesi ve doğrulamak için seçtiği işlemleri kontrol edip sadece Tangle geçmişi ile çelişkiye düşmeyen işlemleri doğrulaması şeklinde evrimleşmiştir. İşlemi yayınlayan sistem, aynı zamanda doğrulama maliyetini üstlenmiş olduğundan, ayrıca "işlem/transfer ücreti" diye bir maliyet söz konusu değildir, bundan dolayı mikro ödeme akışları için önemli bir çözüm adayıdır.

Bu noktada aklımıza gelmesi en muhtemel soru, yeni bir işlemin önceki işlemlerden hangi ikisini onaylayacağına nasıl karar verdiği olacaktır.

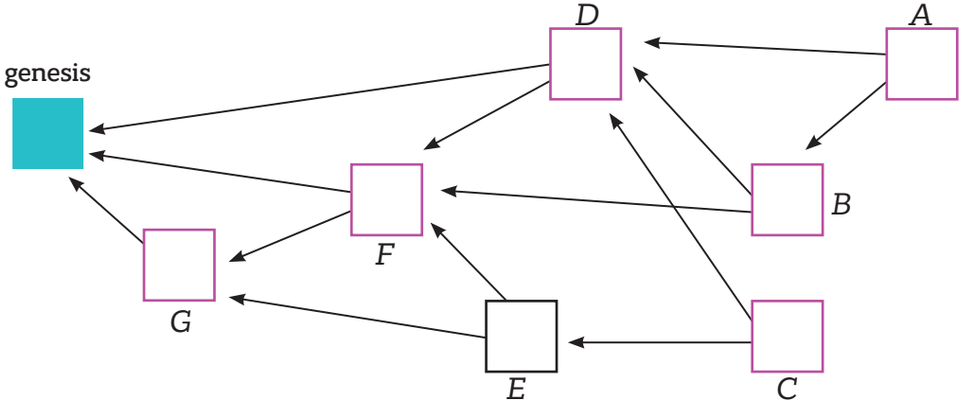
Bu yapıyı ve Tangle'ı daha iyi anlamak için bazı kavramları belirtmemiz gerekiyor:

- ✔ ***Ağırlık (Weight):*** Bir işlemin "ağırlığı", o işlemi yayınlamak isteyen sistemin işlem için harcadığı kaynağı ifade eder. Bitcoin Blockchain platformundaki yapıya benzer bir şekilde (Proof of Work) kriptografik bir problem çözümüne dayanır. Sistem, problemin zorluk derecesiyle oynayarak, işlemin "ağırlık" değerini belirli bir pozitif değer aralığında değiştirebilir. IOTA platformunda ağırlıklar, 3'ün katları şeklinde belirlenmiştir. Aşağıdaki

örnek yapıda basitleştirme amaçlı olarak "ağırlık" değerinin her işlem için "1" olduğu varsayılmıştır.

- ✔ ***Kümülatif Ağırlık (Cumulative Weight):*** Bir işlemin kendi ağırlığı ile kendisini direk ya da dolaylı bir şekilde onaylayan tüm işlemlerin ağırlıklarının toplamıdır. Aşağıdaki örnekte F için (F'yi direk ya da dolaylı onaylayan işlemler : A, B, C, D, E) bu değer, 6'dır.
- ✔ ***Puan (Score):*** Bir işlemin kendi ağırlığı ile kendisinin direk ya da dolaylı bir şekilde onayladığı tüm işlemlerin ağırlıklarının toplamıdır. Aşağıdaki örnekte A için (A tarafından direk ve dolaylı onaylanmış işlemler : B, D, F, G) puan değeri 5'tir.
- ✔ ***Uç (Tip):*** Onaylanmamış işlemlere verilen isimdir. Aşağıdaki örnekte A ve C işlemleri uç işlemlerdir.
- ✔ ***Derinlik (Depth):*** Herhangi bir uç'tan bir işleme gelen en uzun yolun uzunluk değerini ifade eder; aşağıdaki örnekte bu değer G için 4 (G-F-D-B-A), D için 2'dir (D-B-A).
- ✔ ***Yükseklik (Height):*** İşlemden "genesis" işlemine giden en uzun yolun uzunluk değerini ifade eder. Aşağıdaki örnekte bu değer G için 1 (G-Genesis), D için 3'tür (D-F-G-Genesis).

Şekil 27: **Tangle3**



Sadece yukarıda belirttiğimiz onaylama akışı tanımını baz alarak ilerlediğimizde yeni işlemlerin çoğunun onaylamak için eski işlemleri tercih edeceğini düşünebiliriz (bu durum "tembel uç problemi" **-lazy tip problem-** olarak adlandırılmaktadır), bu işlemlerin Tangle geçmişi ile çelişkiye düşmediklerini kontrol etmek çok daha az kaynak gerektirecektir. Bu yaklaşım ise yeni işlemlerin onaylanmaması (yada çok geç onaylanması) ve sonuç olarak Tangle'ın işlevsiz bir yapıya dönüşmesine neden olacaktır. Tangle bu noktada katılımcılarını sadece yeni işlemleri onaylamaya zorlamak gibi merkezi yapılarda görünen bir yaklaşım yerine katılımcılarını belirli kurallar eşliğinde yönlendirmeyi hedefleyen bir yaklaşımı tercih etmiştir.

Tangle yapısında bir işlemi onaylamak için iki işlem seçilirken (ortamda uygun iki işlem olmadığı durumlarda tek bir işlem seçilebilir, örneğin genesis işleminden hemen sonra gelen işlemler), yukarıda tanımlanan değerlerin (özellikle kümülatif ağırlık değerinin) yönlendirme yaptığı bir rastlantısal yapı içerisinde ilerlenmektedir. Bu yaklaşımla, "tembel" davranış sergileyen uçların onaylanma ihtimali düşmekte ve sistem içerisindeki aktörlerin bu davranıştan uzaklaşması sağlanmaktadır.

Bildiğiniz gibi, Bitcoin Blockchain yapısını kendisinden önceki dijital para çözümlerinden ayıran en önemli özelliklerinden bir tanesi, "çift harcama" **(double spending)** problemine getirdiği çözümdür. Tangle'ın dallanmış yapısı, aynı çözümün uygulanmasına izin vermemektedir. Bir kullanıcı bu ağaç yapısının farklı dalları içerisindeyken, hesabındaki parayı tekrar harcayan işlemler tetiklenebilir ve onaylamak için uç arayan işlemler, diğer dallardaki işlemleri bilmediklerinden dolayı, söz konusu işlemleri onaylayabilirler.

Yukarıda belirttiğimiz İşlem Onay Seçim çözümü, yapısı itibari ile (işlemin kendi ve DAG içerisindeki yerine bağlı özelliklerine bağlı rastlantısal seçim) zaman içerisinde bir dal yapısının sistemin geneline göre daha büyümesi ve ağırlaşması ile sonuçlanır. Böylece, daha hafif dallar göz ardı

edilmeye başlanır. Bunu Tangle içerisindeki geçerli işlemler konusunda "mutabakat" (consensus) olarak adlandırabiliriz ve bu durumu, Bitcoin Blockchain'i üzerindeki "en uzun zincir" kavramına benzetebiliriz.

Ancak "A kişisinden B kişisine para gönderimi" işleminde, B'nin ne zaman paranın gerçek sahibi olduğunu anlaması için bu yeterli değildir (bunu Bitcoin Blockchain'i üzerinde işlemin gerçekleşmesini kabul etmek için karşı tarafın işlemin olduğu bloktan sonra "n" blok beklemesi yaklaşımına benzetebiliriz).

Tangle burada, "güven onayı" **(confidence confirmation)** olarak adlandırılan yaklaşımı kullanmaktadır. Temel olarak bir işlemin direk veya dolaylı olarak onay alıyor olması, sistem tarafından daha yüksek bir "güven onayı" ile kabul edildiğini göstermektedir. Tangle, bu değeri uç seçim algoritmasını çoklu bir şekilde çalıştırarak, yüzdelik bir oranda hesaplar. Bir işlem, yüksek bir güven onayı değerine sahipse, mutabakat dışına çıkarılıyor olması oldukça düşük bir ihtimaldir. İşlem kapsamında alıcı taraf, paranın gerçek sahibi olduğu düşüncesi ile hareket edebilir.

Ancak yukarıda belirtildiği gibi "oldukça düşük" bir ihtimal olması, belirtilen durumun olamayacağı anlamına gelmemektedir. Kötü niyetli bir katılımcı, yeterli işlem gücüne de sahip ise çift harcama yapmayı deneyebilir. Bunun için ilk işlemin gerçekleşmesini bekleyip (bir alışveriş akışından eline aldığı ürünün geçmesi gibi), sonrasında kural dışı işlemi onaylayacak çok yüksek sayıda yeni işlem üretip, kural dışı işlemi direk ve dolaylı olarak onaylayarak, kural dışı işlemin olduğu dal yapısının kümülatif ağırlığını arttırabilir ve tüm sistemi bu yeni dal yapısının doğruluğuna ikna edebilir.

Bu durumun gerçekleşebilmesi için kötü niyetli katılımcının diğer tüm katılımcılardan daha fazla işlem yaratabilmesi gerekmektedir. Büyük bir ağ yapısı için bu risk göz ardı edilebilse de günümüzdeki IOTA yapısı için bu risk varlığını korumaktadır. Bu durumu engellemek için geçici olarak "koordinatör" **(coordinator)** adı verilen ek bir mutabakat yapısı eklenmiştir. Bu yapıda belirli aralıklarla (her iki dakikada bir gibi) IOTA platformu tarafından yaratılan bir referans işlemi oluşturulur ve bu işlem tarafından onaylanan

diğer tüm işlemler, otomatik olarak %100 güvenlik onayına sahip olurlar. Merkezi olmayan sistemler düşüncesine aykırı olan bu yaklaşım, IOTA ağının olgunlaşması ve yeterli büyüklüğe ulaşması ile birlikte devre dışı bırakılacaktır.

Tangle, yapı itibari ile kuantum dirençli kriptografik algoritmalar kullandığından dolayı, günümüz Blockchain platformlarına kıyasla, ileride kuantum bilgisayarlarının ortaya çıkması ile gerçekleşebilecek saldırılara karşı çok daha dayanıklıdır.

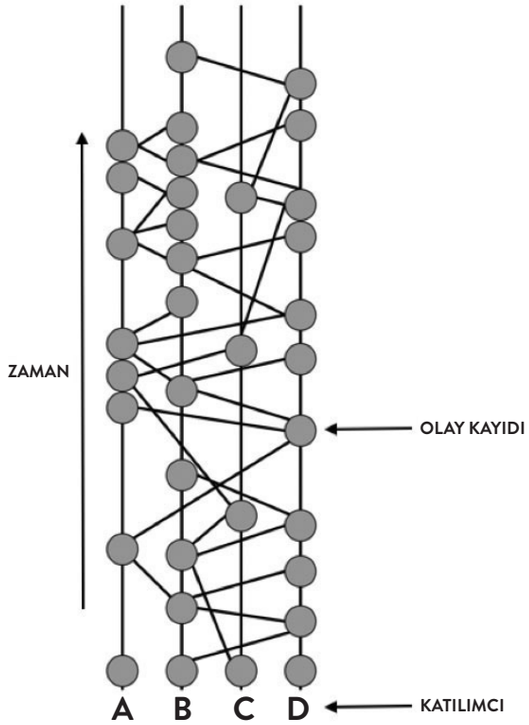
Hashgraph

Leemon Baird tarafından geliştirilmiş olan Hashgraph, genel DLT yaklaşımlarından farklı olarak açık kaynaklı bir teknoloji değildir, yine Leemon tarafından kurulmuş olan Swirlds'in fikri mülkiyetinde bulunmaktadır.

Blockchain teknolojisinin blok yapısını andırır bir şekilde Hashgraph yapısında işlemler "Olay Kaydı" **(Event)** olarak adlandırılan veri yapılarında tutulmaktadır ve olay kayıtları arasında özet değerleri (hash) kullanılarak ilişki kurulmaktadır. Bu veri yapılarının içerisinde zaman bilgisi, işlemler (bu bilginin olması zorunlu değildir) ve ilişkili diğer olay kayıtlarına ait özet bilgisi bulunmaktadır.

Şekil 28: **Olay Kaydı Yapısı**

Şekil 29: **Hashgraph Yapısı**



Hashgraph yapısında, ağı oluşturan tüm katılımcılar birbirleri ile sürekli olarak bildikleri olay kayıtları hakkında iletişim kurmakta ve bu iletişim bir tür olay kayıt ağacı oluşturmaktadır. Bu iletişim sırasında, **"gossip protocol"** adı verilen bir yaklaşım kullanılmaktadır. Bu yapıda katılımcılar, rastlantısal bir şekilde ağ üzerindeki diğer katılımcılar ile iletişime geçerek kendilerinin bilgi sahibi olay kayıtları hakkında bilgi paylaşmaktadırlar. Bu oldukça hızlı bir veri paylaşım modelidir, bir milyon katılımcının olduğu bir sistemde bir olay kaydı yaklaşık 20 senkronizasyon içerisinde tüm ağa yayılabilir. Saniyede 20 senkronizasyon yapan bir sistem için bu bir saniye

içerisinde olay kaydının tüm sisteme yayılması anlamına gelmektedir. Bu modeli toplumsal yapılarda, mesela bir ofis ortamında, herhangi bir dedikodunun yayılma modeline benzetebiliriz.

Hashgraph üzerinde bir katılımcının olay kaydı oluşturması temel olarak başka bir katılımcının kendisi ile irtibata geçmesi ile olur. Bundan dolayı oluşan her olay kaydı üzerinde:

- ✔ Kaydı yaratan katılımcının bir önceki olay kaydını gösteren özet değeri (self-parent),
- ✔ irtibata geçen katılımcının ilettiği son olay kaydını gösteren özet değeri (other-parent) bulunur.

Bu yapının "hashgraph" olarak adlandırılmasının temel nedeni, tüm olay kayıtlarının kriptografik özet değerleri ile birbirilerine bağlı olmasıdır. Bu şekilde bir olay kaydının geçmiş olay kayıtlarına dair referans içeriyor olması ve bu bilginin de diğer katılımcılara iletilmesinden dolayı Hashgraph içerisindeki iletişim yapısı, aynı zamanda **"gossip about gossip"** olarak nitelendirilmektedir.

Hashgraph üzerindeki mutabakat, temel olarak olay kayıtlarının sırası ve zaman bilgisi üzerinde gerçekleşmektedir. Bu mutabakatı gerçekleştirmek için:

- ✔ Hashgraph yapısı, olay kayıtlarının gruplandırıldığı turlara (round) bölünür. Bu turlara "yaratım turu" (round created) denir.
- ✔ Bir tur içerisinde bir katılımcı tarafından yaratılan ilk olay kaydı, "tanık" (witness) olarak adlandırılır (her katılımcının, bir tur içerisinde bir tanık kaydı olması gerekmez).
- ✔ Her "tanık", kendinden sonra gelen turlardaki tanık özelliğine sahip olay kayıtları tarafından değerlendirilir. Bu değerlendirme, olay kayıtları arasında bir yol olup olmamasına göre yapılır. Hashgraph, daha önce belirtildiği gibi bir "Yönlü Çevrimsiz Çizge " yapısıdır.

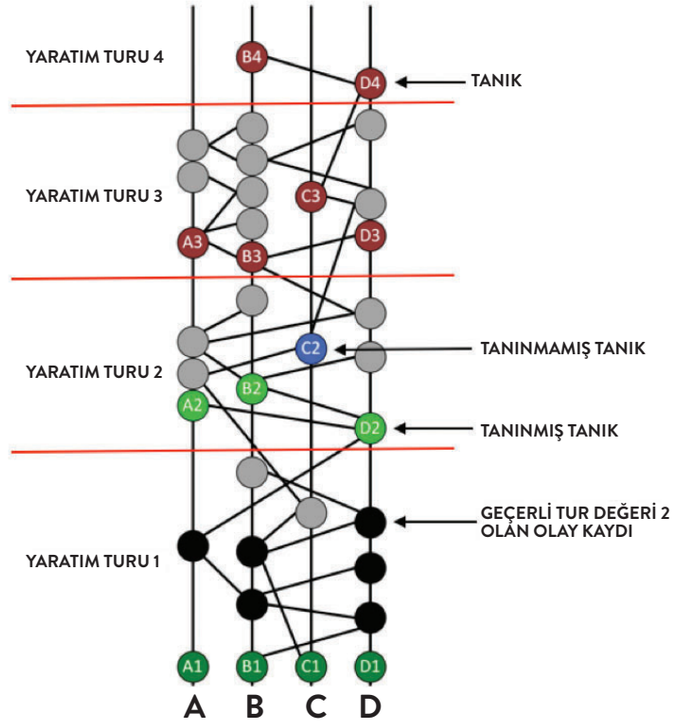
"a" turundaki bir tanık kaydı için:

- ✔ "a + 1" turundaki tanık kayıtlarından ilgili kayda bir yol olup olmaması değerlendirilir (buna "oy verme" denir, yol varsa "evet" yoksa "hayır" olarak tanımlanır).
- ✔ "a + 2" turundaki tanık kayıtlarından "a + 1" turundaki tanık kayıtlarına olan yollar incelerek sistem katılımcılarının çoğunun (tüm katılımcıların 2/3'den fazlasının) kullanılıp kullanılmadığı değerlendirilir (buna "oyların sayılması" denir, "a+1" turundaki tanık kaydının oyunun geçerli olması için bu koşulun sağlanması gerekir).
- ✔ Oyların sayılması sonucunda bu tanık kaydı "evet" oyları çoğunlukta ise **"tanınmış tanık" (famous witness),** "hayır" oyları çoğunlukta ise **"tanınmamış tanık" (infamous witness)** olarak adlandırılır (buna **"karar verme"** denir). Sadece bir sayım yapılması yeterlidir, "a + 2" turundaki tüm tanık kayıtlarının sayım yapmasına gerek bulunmamaktadır.

Bir tur içerisindeki tanık kayıtları ile ilgili karar verildikten sonra önceki olay kayıtları için sıralama ve zaman bilgisi mutabakat yapısı çalıştırılır. Burada önemli olan, incelenen olay kaydı için bir sonraki tur kapsamında tüm tanınmış tanıklardan bir yol olmasıdır (bir sonraki tur kapsamında bu sağlanamazsa sonraki tura ait tanınmış tanıklar incelenir). Bu şekilde bir yol bulunduğu zaman, tanık kayıtlarının yaratım turu değeri bu olay kaydı için "geçerli tur" (round received) değeri olarak kabul edilir ve mutabakat yapısında olay kaydının geçerli olduğu sırayı belirler. Zaman bilgisi konusundaki mutabakat ise, bu olay kaydına bağlı, geçmiş olay kayıtlarının zaman bilgilerinin medyan değerinin hesaplanması ile belirlenir.

Hashgraph içerisindeki mutabakat akışı karmaşık görünüyor olsa da asıl kaynak gerektiren işlemlerin sadece belirli olay kayıtları için (tanık kayıtlar) gerçekleştiriliyor olması ve karar yapılarında ilgili tüm

Şekil 30: **Hashgraph Mutabakat Yapısı**



kayıtlar için kontrol etmeden sadece bir kaydın sonucuna göre hareket edebilmesi sayesinde (matematiksel olarak diğer tüm kayıtlar aynı sonucu oluşturacağından dolayı), günümüz Blockchain platformlarına kıyasla çok daha yüksek bir performans vaat etmektedir. Bu konuda yapılan bazı çalışmalarda saniyede 250.000 işlem görüldüğü belirtilmiş olsa da, bu çalışmalar hep özel, dışarıya kapalı ağ yapılarında gerçekleştirilmiştir. Yakın zamanda duyurusu yapılan ve açık bir platform olan Hedera platformu, bu anlamda gerçek bir deneme ortamı olacaktır[34].

[34] *http://bit.ly/BC101hg*

SONUÇ VE GENEL DEĞERLENDİRME

Bu kısa sayılabilecek kitap ile öncelikle Blockchain teknolojini anlamak için gerekli olan temel kavramları tarihsel gelişimleri ile birlikte ele aldık. Ardından Blockchain dünyasının kavramsal ve teorik mantığına giriş yaparak, türleri, uygulama örnekleri, platformları, önemli bir kullanım alanı olan kripto para birimleri gibi konulara göz attık. Sonrasında, zorluk ve riskleri değerlendirdik. Son olarak, tüm teorik kavramları teknik yaklaşımlar ile tekrar gözden geçirdik.

Amacımız, Blockchain dünyasını, mümkün olduğunca popülist yaklaşımlardan arındırarak, yalın bir şekilde ve okuyucularımızın bu yeni kavram için temel bilgiler edinmesini hedefleyerek anlatmaktı.

Blockchain, her ne kadar internetten sonraki en büyük devrim olarak nitelendirilse de henüz yolun çok başındayız. Bu süreci, 1980'li yıllarda internetin geliştirilme aşamasına benzetebiliriz. Aradan geçen 30 senelik dönem sonunda, internetin çıkış noktasından bugüne geldiği nokta arasındaki farkı net bir şekilde görebiliyoruz. Blockchain için de durum çok farklı değil ve olmayacak.

Öte yandan bu mucizevi gibi görünen teknolojinin de kendine göre riskleri bulunuyor. Kitabımızda bu konuya kısa bir bölüm ayırarak, okuyucularımızı bunaltmadan ve endişeye sevk etmeden bu hususların altını da çizmeye çalıştık.

Tam bu noktada FinTech dünyasının en keyifli fikir önderlerinden biri olan David Birch'ün "Kimlik: Yeni Para" isimli kitabından bir kısmı da sizler ile paylaşmamız gerektiğini düşünüyoruz:

Vergi Tahsil Çubuklarının Beklenmedik Sonucu

Teknoloji, yakın bir gelecekte öngörülmemiş karakteristik özelliklerini bize göstermeye başlayacak. Genel olarak, bu tüm teknolojiler için geçerli olan ve onların varlığının kalıcı olmasını sağlayan bir durumdur. Her şey bir gecede olup bitmez. Tarihçi David Edgerton, The Shock of The Old isimli teknolojik değişim üzerine yaptığı olağanüstü çalışmasında, teknolojilerin kültürleri değiştirmesinin uzun zaman aldığını ve genellikle mucitlerinin düşündüğünden daha farklı şekilde etkilerini gösterdiğini anlatır. Para da farklı değildir. Edgerton söyle der: "Modern dünya, farklı teknolojilerden türemiş melez bir sonuçtur, teknolojiler ortaya çıktıkları noktalardan daha büyük olabilecekleri başka alanlara doğru nakledilmişlerdir" ve bu tespit nakit parayı dönüştüren teknolojiler için de geçerlidir.

İngiltere'nin geçmiş dönemlerinde vergi kayıtlarını tutmak için kullanılan tahta çubukların hikayesi, Edgerton'un bu tespitini harika bir şekilde bize gösteriyor. Vergi çubukları ilk olarak 1066 yılında gerçekleşen Norman istilasından hemen sonra kullanılmaya başlanan bir teknolojidir. İstila sonrasında Britanya adasının çeşitli bölgeleri için vergiler belirlendi ve bunların toplanarak kraliyete sunulması için birer vergi memuru görevlendirildi. Hem kraliyetin hem de vergi memurunun doğru işlem yaptığını anlamak için tahta çubuklara çentik atılan bir kodlama yöntemi geliştirildi. Daha sonra bu çubuklar, belirli noktadan biri uzun diğeri kısa olmak üzere iki parçaya bölünüyordu. Böylece her iki tarafın da elinde işlem ile alakalı bir kayıt oluşuyordu. Daha sonra toplanan vergilerin sayım zamanı geldiğinde vergi memurunun elindeki kısa çubuk ile krallığın elindeki uzun çubuk birbiri ile eşleştiriliyor ve hesabın doğru olduğu kontrol ediliyordu. Bu yeni teknoloji iş görüyordu. Çubuklar uzun süre bozulmadan kalıyor (hatta bu gün elimize ulaşan örnekleri vardır), kolayca saklanabiliyor, taşınabiliyor ve konuyu bilen birisi tarafından rahatlıkla çözümlenebiliyorlardı.

Ancak krallığın harcamalarını yaparken tüm vergilerin toplanmasını beklemesi, pek çok sebeplerden dolayı, çok mantıklı değildi. Kral,

toplanacak vergileri olabildiğince çabuk şekilde nakde dönüştürmeliydi. Toplanacak vergiler teminat gösterilerek belli bir faiz karşılığında borç alınamazdı, zira b,u dini kanunlara aykırıydı. Bu sebeple, toplanacak vergiyi gösteren hesap cetvellerini belli bir indirim karşılığında satma fikri doğdu. Böylece vergi çubuklarını satan kral, hızlıca nakde ulaşıyor, çubukların yeni sahipleri de vergiler toplandığında kraldan ödemelerini tahsil edebiliyordu. Bu durum, bu vergi çubukları için kullanılan "stock" ifadesinin de bugünkü modern devlet tahvili ifadesi olarak kullanımının kökenini oluşturdu. Kraliyet için elindeki tahvilleri belli bir indirim ile satmak, ne olduğunu tanrıya fark ettirmeden borç almak üzere yapılan bir numaraydı.

Kaydı tutulan ticari işlemler sayesinde teknoloji hızla dönüşerek, yeni bir fonksiyon oluşturan, ani bir sonuç yaratmıştır. Bağımsız vergi çubuklarının değeri, artık sahibinin elinde tuttuğu sabit bir vergi miktarına bağlı olmaksızın, piyasanın talebine göre şekillenmeye başladı ve piyasa hızla evrimleşti. Bristol'da toplanacak vergiler için vergi çubuğunu elinde tutan ve York'da yaşayan birisi, ya zamanı geldiğinde Bristol'e giderek toplanan vergiden alacağını tahsil etmeli veya oraya gidip bunu zaten yapacak birini bulu,p belli bir indirim karşılığında elindeki çubuklarını satmalıydı. Böylece çubukların piyasası büyüdü. Piyasanın sürekli değişen talepleri ve sınırları içinde indirimlerin miktarı da değişti. Modern bankacılıktan önceki dönemlerde, ekonomik kaynakların mekan ve zaman içindeki değişimi sayesinde bu fonksiyonlar gelişmeye başladı. Londra para piyasası, yeni bir oluşum değildir. Bu piyasanın etkinliği sayesinde, krallık kendi yapabileceğinden daha makul maliyetler ile nakit akışı sağlamış ve Maliye Bakanlığının kayıtlarından anladığımız kadarıyla, bu piyasa gayet akıcı ve sağlıklı şekilde çalışmıştır.

İlginç bir şekilde hesap cetvelleri, 19. Yüzyıla kadar kullanılmaya devam etti. Bu çubukların nasıl işleneceğini bilen son kişi de 1826 yılında öldü ve biriktirilen çubuklar 1834 yılına kadar bir köşede unutuldu. Daha sonra Hazine, Westminster Sarayı'ndaki Maliye Bakanlığı'nda bulunan Hesap Cetveli Dairesi'nin artık kullanılmayan odasını, boşaltmak amacıyla iflas mahkemesine tahsis etti. Ahşap ve Ormancılık Dairesi Londra ofisinde çalışan Asistan Mimar John Phipps, Krallık görevlisi olarak sarayda katiplik yapan Richard Woebley'e, hesap cetvellerini dışarı çıkarmasını ve Thames nehri kenarında yakmasını söyledi. Ancak Woebley daha güzel bir fikir ortaya sundu ve çubukların merkezi ısıtma sisteminin kazanında yakılmasını önerdi. Hesap cetvelleri güzelce dev kazanlara yüklendi ve yakıldı. Ancak çubukların reçineli yapısı, ortaya gerekenden daha büyük alevler çıkardı ve büyük bir yangına sebep oldu. İngiliz Kraliyet Sarayı, bu olay nedeniyle, 16 Ekim 1834 tarihinde yandı.

Geleceği tahmin etmeye çalışmanın şimdiden bir anlamı yok. Ancak teknik yaklaşımları bir kenara bırakıp şunu söyleyebiliriz: Blockchain dünyasının şimdiden çok önemli bir problemi var ve bu problem küresel ölçekte kendini hissettiriyor: İnsan Kaynağındaki noksanlık.

Teknolojinin çok yeni olması, henüz bu alanda çalışan yazılımcıların tecrübe elde etmesi için yeterli olamadı. Bu sebeple eğer bir Blockchain projesi yapmaya kalkarsanız, gerek yazılımcı gerekse bu alanda servis verebilecek tecrübeli insan kaynağının çok zor bulunduğuna şahit olabilirsiniz.

İnsan kaynağındaki kıtlık, Blockchain dünyasını girişimciler için bir cazibe noktası haline getiriyor. İşin ilginç yanı, bir teknolojinin öylesine erken dönemlerinden bahsediyoruz ki bu alanda çalışan girişimler ve girişimciler için yatırım bulmak çok zor olmuyor, zira problem-çözüm ilişkisinden çok teknolojinin potansiyeline yatırım yapmayı hedefleyen yatırımcılar bu fırsatı kaçırmak istemiyorlar. Bu sebeple girişimciler için oldukça cazip ancak bir o kadar çetrefilli ve zor bir alandan bahsediyoruz.

Kolaylıkla içine düşülebilecek bir hata ise Blockchain teknolojisinin sadece FinTech dünyasına hitap ettiğini düşünmek olur. Kripto para birimleri ve ödeme çözümleri alanında Blockchain'in önemli bir rol oynadığını inkar edemeyiz, ancak bu, teknolojinin çok daha geniş alanlardaki kullanım imkanları göz önüne alındığında, teknolojinin kendisine haksızlık olur.

Kesinlikle bankacılık ve finans dünyası bu teknolojiden gelecek yıllarda yoğun şekilde faydalanacaktır, ancak bu teknolojinin nimetlerinden faydalanan tek endüstri onlarla sınırlı kalmayacaktır. Lojistik, regülasyon, perakende gibi çok farklı alanlarda Blockchain uygulamalarını görmeye devam edeceğiz.

Kurumlar İçin Kısa Bir Reçete

Kitabımızın son paragraflarına geçmeden önce bu dünyaya adım atmak isteyen işletmelere de reçete niteliğinde çok kısa tavsiyelerimiz olacak. Bu tavsiyeleri dikkate almanız bu maceralı dünyada işinizi oldukça kolaylaştıracaktır.

1- Tek başınıza bu dünyaya girmeye kalkmayın. Blockchain teknolojisi pek çok tarafı bir araya getiren bir yapıya sahip. Sizin tek başınıza ilerlemenizi gerektiren sebep olmadığına göre, mutlaka bir ekosistem oluşturun veya mevcut bir ekosistemin parçası olun.

2- Blockchain teknolojisini kurumsal açıdan anlamak için açık ağları incelemek gerekiyor ama en iyi deneyim özel bir altyapı ile anlaşılabiliyor. Bu adımı ihmal etmeyin.

3- Blockchain teknolojisini nerede kullanabileceğinize dair hedefler belirleyin. Bu hedefler için mutlaka özel altyapınızda kavram kanıtlama (Proof of Concept) çalışması gerçekleştirin.

4- Gerçek dünyadaki işletme ve süreçlere dair problemleri, Blockchain ile nasıl çözebileceğinize dair kafa yorun. İkinci ve üçüncü önerilerdeki çalışmalarınızda, hedefinizi bu problemleri çözmek olarak belirleyin.

5- Tüm bu önerileri kullanırken, teknoloji değil problem odaklı başlamayı unutmayın. Eğer teknoloji odaklı olarak başlarsanız, bir süre sonra "Elinde çekiç olan, her şeyi çivi sanır" sözünde tarif edildiği gibi, uygun olmayan problemleri Blockchain yaklaşımı ile çözmeye çalışıp, kendiniz yanlış bir yolda giderken bulabilirsiniz.

Blockchain teknolojisinin sunduğu fırsat ve potansiyeller, keşfedilmek üzere müteşebbisleri bekliyor. Zengin kavramlar ile sürekli gelişen bu teknolojinin oluşturduğu dünyada "değişim", temel unsurların başında geliyor. Bu sebeple okuduğunuz bu kitap, temel kavramları korumakla birlikte demode olmaya mahkûm. Amacımız, okuyucularımızdan gelecek geri bildirimler ve gelişen dünyanın dinamiklerini göz önünde bulundurarak bu kitap içeriğini de güncel tutmak.

Blok 0{

İlk Genesis kaydını oluşturmanın verdiği gurur ile şimdilik burada okuyucumuz ile vedalaşmamız gerektiğini düşünüyoruz.

Bir sonraki kayda kadar umarız tüm okuyucularımıza değer ve fayda sağlayabilmişizdir.

Serkan Doğantekin ve Ahmet Usta / 30 Nisan 2017 – İstanbul

Prev: 0000000000000000000000000000000000000000000000000000000000000000

Hash: 000068173a9d5e49ade66103e79a0239bcdb43b8c13e0d62f0c13b27deb13138

Nounce: 33788

}

Blok 1{

Aradan tam bir yıl geçtikten sonra ikinci Blok kaydını da gerçekleştirmenin mutluluğunu yaşıyoruz. Nice bloklara diyelim.

Serkan Doğantekin ve Ahmet Usta / 30 Nisan 2018 – İstanbul

Prev: 000068173a9d5e49ade66103e79a0239bcdb43b8c13e0d62f0c13b27deb13138

Hash: 0000d5e1f277cbea9d6f18995c4563dc3a4c2ff21daf1d0b52d4580fb00df4f3

Nounce: 17430

}

BAŞVURU VE KAYNAKLAR

Bu kitabı hazırlarken, engin bir dünyadaki pek çok farklı kaynaktan faydalandık. Ancak bu süreç, kitap özelinde gerçekleşmedi. Kitap boyunca okuduğunuz içeriklerin bazıları farklı zaman dilimlerinde farklı yerlerde yayınlanmak üzere kaleme aldığımız makalelerden oluşuyordu. Bu makalelerin özel kaynaklarını olabildiğince kitabın akışı içinde dip notlar olarak paylaştık. Ayrıca aşağıdaki kaynakları da kısmen kullandık ve Blockchain ile alakalı bilgisini artırmak isteyenler için bir başvuru listesi olarak paylaşıyoruz.

http://www.fintechistanbul.org/blog

https://bitcoin.org/bitcoin.pdf

https://www.ethereum.org/

https://github.com/ethereum/wiki/wiki/White-Paper

https://wiki.hyperledger.org/groups/whitepaper/whitepaper-wg

https://ripple.com/files/ripple_consensus_whitepaper.pdf

https://interledger.org/interledger.pdf

Coursera - Bitcoin and Cryptocurrency Technologies

https://www.coursera.org/learn/cryptocurrency

World Economic Forum - The Future Of Financial Infrastructure

http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

https://blockchain.berkeley.edu/

https://www.edx.org/course/blockchain-business-introduction-linuxfoundationx-lfs171x

BKM
BANKALARARASI
KART MERKEZİ