BLOCKCHAIN 101

BLOCKCHAIN 101

YAYINCI: Kapital Medya Hizmetleri A.Ş.
GENEL YAYIN YÖNETMENİ: Pelin Özkan
EDİTÖR: Zeynep Hale Akman
KAPAK TASARIM: Erkan Kocaoğlu
GÖRSEL YÖNETMEN: Sena Altun Çakıroğlu
SATIŞ ve DAĞITIM SORUMLUSU: Salih Şahin
BASKI: Mayıs 2017

YÖNETİM YERİ: Nispetiye Caddesi
Akmerkez E Blok Kat: 6 Etiler/İSTANBUL
Tel: (212) 282 26 40
Faks: (212) 282 26 32
e-posta: kitap@kapital.com.tr

MediaCat
KİTAPLARI

ISBN: 978-605-4584-97-0

Yayıncı Sertifika No: 16190

BASIM ve CİLT: İnkılap Kitabevi Yayın Sanayi ve Ticaret A.Ş. • Çobançeşme Mah. Altay Sok. No: 8 Yenibosna/Bahçelievler/İstanbul Tel: 212 496 11 11 Sertifika No: 10614

BLOCKCHAIN 101

Ahmet Usta
Serkan Doğantekin

İÇİNDEKİLER

2. BÖLÜM

SUNUŞ

Yaşamın temeline baktığımız zaman değişimi görüyoruz. Doğa bu değişimi DNA kodlarına işleyerek yeni nesillere aktarırken, nesiller kendi içinde yaşam döngülerine sahip oluyor. 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 ise sahip olma gayreti ile bizleri daha çok çalışmaya itiyor.

Bu gün işletmelerin ve bireylerin kendilerini yenilemediği bir dünyada var olma mücadelesi içinde 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.

Blockchain kavramı gibi yenilikçi bir kavram için 1990'lı yıllarda internet kavramının bulunduğu noktaya benzer bir noktada olduğumuzu söylemek hatalı bir benzetme olmaz. Daha farklı ifade edecek olursak Blockchain teknolojisi gelecek 25 yılda tüm dünyayı derinden etkileyecek ve en az internetin ge-

leneksel iş dünyasına etkisi kadar yenilikçi modelleri ile günümüz iş dünyasını tekrardan dönüştürecek.

Bankalararası Kart Merkezi (BKM) 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 buluşturmanın gururunu yaşıyoruz.

Paylaştığımız her bilginin ülkemizi, sektörümüzü, şirketimizi ve bizleri geliştireceğine ve değiştireceğine inanıyoruz. Şüphesiz bu yenilenme çabalarımız karşılık bulacak ve bu değişim döngüsünde daha büyük başarıları hedefleyeceğiz.

Dr. Soner Canko
Bankalararası Kart Merkezi Genel Müdürü

ÖNSÖZ

Ahmet Usta

Elinizde tuttuğunuz (veya bir ekranda PDF olarak görüntülediğiniz) bu kitabın temelleri FinTech İstanbul organizasyonunun kurulduğu 2016 yılına dayanıyor. Blockchain dünyası ile alakalı pek çok haberi, kavramı ve makaleyi paylaştığımız FinTechIstanbul.org web 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. 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 pek çok kişinin 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. Yorucu bir maceradan sonra faydalı temel bir kaynağın ortaya çıktığına inanıyoruz. Umarız okuyucularımız da en az bizler kadar bu heyecanı paylaşarak bu kitaptan faydalanır.

Bu süreçte emeği geçen tüm paydaşlara ve bensiz geçirdikleri süre boyunca gösterdikleri hoşgörü ile birlikte tüm huysuzluklarıma katlanmak için gösterdikleri sabır sebebiyle, sevgili eşime ve çocuklarıma, tekrardan teşekkür ediyorum.

Ahmet Usta

ÖNSÖZ

Serkan Doğantekin

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

Bu kitap ile aslında bu heyecanı giriş seviyesinde olsa da mümkün olduğunca geniş kitleler ile paylaşmayı, denize ufakta olsa bir taş atarak dalgalar yaratmayı, yeni düşünce fırtınalarını oluşturmayı, deneyselde 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 sonrasıda Blockchain'in açtığı yeni dünyada yeni kıtalara doğru yelken açarken benzer duygular içinde olursunuz.

Serkan Doğantekin

GİRİŞ

2008 küresel finans krizi yaşandığında gayet köklü yapılar üzerine kurulu olduğuna inanılan bankacılık ve finans sektörü kadar bu yapıları düzenleyen merkezi kurumlara karşı da çok ciddi bir güvensizlik kaçınılmaz olarak ortaya çıktı. Tüketiciler kendilerine satılan finansal ürünleri ve hizmetleri yeterince denetlemediği ve düzenlemediği için küresel merkez bankalarını suçladılar ve bankacılık sisteminde yatırım yapmaya yönelik inançlarının büyük ölçüde yitirdiler.

2008 Eylül ayında Lehman Brothers'ın çöküşünden sadece iki ay sonra gerçek kimliği belirsiz olmakla birlikte "Satoshi Nakamato" takma adını kullanan bir kişi (veya bir grup olma ihtimali de var) "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, bir dijital para birimi olarak karşımıza çıktı. Bu para birimi sanal olmakla birlikte altında yatan güçlü şifreleme (kriptografi) teknikleri,

tek bir merkez yerine tüm kullanıcılarına dağıtılmış veri yapısı ve Blockchain adı verilen kayıt sistemi sayesinde çok hızlı bir şekilde önce teknik camianın ardından tüketicilerin dikkatini üstüne çekti.

Aklımıza gelebilecek her dijital varlığın bir kopyasının çıkartılması sadece zaman problemi iken Blockchain teknolojisi bu durumu tümüyle değiştiriyor ve kopyalanamaması dolayısı ile dijital enflasyona maruz kalmayacak kripto para birimlerinin sunulmasını mümkün hale getiriyordu.

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 gerekli süreyi kısalttı.

Burada okuyucularımız için belirtmemiz gereken önemli bir husus, Blockchain teknolojisine ait kavramsal temellerin ilk olarak 90'lı yıllarda kaleme alınan üç farklı makale ile karşımıza çıkmasıdır:

- 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 sistemini tanımlanır.
- Bruce Schneier ve John Kelsey tarafından hazırlanan

[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.

1998 yılına ait bir makale[3] ise, güvenilmeyen makineler üzerinde tutulan günlük dosyalarının (log files) içerdiği hassas bilgilerin korunması için şifrelemenin nasıl kullanılacağını açıklar.

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 gelecek bölümde tarihsel gelişimleri ile birlikte Blockchain teknolojisini daha iyi anlamamıza imkan sağlayacak kavramları ele alacağız.

İlerleyen bölümlerde teknik detaylara girmeden Blockchain platformları, kullanım alanları gibi konulara değinip sonrasında teknik detaylara yakından göz atacağız.

Kitabımızın içinde pek çok kavramın tekrar edildiğini görebilirsiniz. Bunlar okuyucumuzun hafızasına güvenmediğimiz için değil ancak tekrarlar ile konuların pekişeceğine olan inancımızdan kaynaklanmaktadır.

İnternetten sonraki en büyük dijital ağ teknolojisi olarak tanımlanan Blockchain şimdiden küresel etkilerini göstermeye başlayan bir teknolojidir. Henüz tüm dünyada bu teknoloji açısından yolun çok başında olduğumuzu söylemek zorundayız. Eğer sizlere 20 sene önce interneti anlatan bir kitap yazmış

[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, Januar 1998.

olsak kullanacağımız cümle yapıları çok farklı olmayacaktı. Bu sebeple 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 sunmaktır. İnternetin son çeyrek yüzyılda ticaret, iletişim ve dünyayı nasıl değiştirdiğini göz önüne alarak Blockchain teknolojisinin benzer bir maceranın temellerini oluşturduğunu vurgulamak istiyoruz.

Bitcoin ve diğer kripto para birimlerinin on yıla yakın macerasını değil ancak bunların altında yatan ve kabiliyetleri çok daha geniş olanaklar sunan Blockchain teknolojisi bu kitabın ana konusunu oluşturuyor.

Şüphesiz ki Blockchain, Finansal Teknolojileri ifade etmek için kullanılan FinTech kavramının tamamını değil sadece bir kısmını oluştursa da Blockchain kavramını daha iyi anlamak üzere FinTech kavramını iyi kavramış olmak, bunun için de kavramın etimolojik olarak biraz köklerine inmemiz gerekiyor.

BİRİNCİ BÖLÜM

Blockchain 101:
Blockchain'i Anlamak

1.1. Finans ve Teknolojinin Yeni Birlikteliği: FinTech

Finans kavramı "parasal kaynak" veya "para ile ilişkili" anlamına geliyor. İnsanlığın bireysel veya toplumsal olarak hayatını idame ettirmek için sürdürdüğü ticari ilişkiler tarihin ilk dönemlerinden itibaren takas usulüne dayalı olarak başladığını ancak zamanla bu alışveriş sürecini kolaylaştırmak için para denilen kavramın keşfedildiğini görüyoruz. Çok basit bir ifade ile aslında para; niteliği bakımından ortak bir değer algısı ve kabulü olarak karşımıza çıkıyor.

Uzun çağlar boyunca para kendisi fiziksel bir değer ifade eden altın, gümüş ve bakır sikkeler veya bunların karışımları ile üretilirken teknik imkanların gelişmesi ile birlikte fiziksel olarak değer ifade etmeyen ancak değerinin merkez bankaları tarafından altın rezervleri ile güvence altına alındığı bir metaa haline geldi.

Günümüzün modern olarak tanımlanan dünyasında en önemli küresel ortak para birimi olarak karşımıza Amerikan Doları çıkıyor. Dolar 1970'li yıllardan itibaren ABD merkez

bankasında (FED) altın karşılığı bulundurularak üretilen bir para birimi olmaktan çıkmış ve bu değişim ile birlikte finansal ürünler ve çözümler hızla çeşitlenerek pek çok farklı türevle hayatımıza girmiştir.

Savunma sanayiinden sonra teknolojik altyapılara en çok harcama ve yatırım yapan endüstrilerin açık ara başında bankacılık ve finans sektörü gelmiştir. Tam bu noktada yeni bir soruya cevap vermek gerekiyor;

Teknolojinin Finansla Buluşması

Teknolojinin çok çeşitli tanımları bulunuyor. Temel olarak bu tanımları ortak bir potada erittiğimizde günlük yaşantımızda gerçekleştirdiğimiz işlerin süresini kısaltan ve/veya kalitesini artıran ya da hayatımızda daha önce olmayan bir ürün ve hizmeti yaşantımıza dahil eden yenilikler olarak tanımlanabilir.

Bunun en güzel örneğine 17. yüzyılın sonunda ortaya çıkan buhar makinesi ile tanık oluyoruz. İnsanoğlunun tüm tarihsel gelişim süreci içinde genel olarak ilk kez kas gücünden makineleşmeye geçmesini sağlayan bu teknolojiyi elektriğin hayatımıza girmesi izlemiştir.

Teknolojik gelişim süreci sürekli hızlanmaya devam etmekle birlikte devrimsel olarak kabul edebileceğimiz atılımlar arasındaki süreler de giderek kısalmıştır. Bu pencereden baktığımızda 1990-2000 yılları arasında cep telefonu ile tanışan nesiller için cep telefonu bir teknoloji olarak karşımıza çıkmakta ancak 2000 sonrası doğanlar için artık cep telefonu bir teknoloji olmaktan çıkmış ve hayatın normal bir bileşeni haline gelmiştir. Benzer şekillerde 2005 ve sonrasında hayatımıza giren akıllı

telefonlar artık birer teknoloji olmaktan çıkıp yaşamın vazgeçilmez bir parçası haline dönüşmektedir.

Sahnede FinTech

Finans ve teknolojinin buluşması ile ortaya çıkan FinTech kavramı her ne kadar son yıllarda popüler hale gelse de bugüne kadar parasal işlemler ile alakalı olarak yapageldiğimiz işlemlerin süresini kısaltan veya kalitesini artıran ya da tümüyle yeni bir ürün veya hizmeti hayatımıza sokan bir tanım olarak özetlenebilir.

Bu noktada ülkemizin de finansal teknolojiler açısından yaşadığı dönüşümü dünyada örneğine az rastlanan bir maceraya sahip olduğu için ele almakta fayda görüyoruz.

Türkiye'nin FinTech Dönüşümü

Türkiye'deki bankacılık sisteminin 1960'lı yıllarda küresel sistemler ile bütünleşmeye başladığını ve 1970 yıllarından itibaren dünya ile paralel bir ilerleme kaydederken teknolojik atılımların 1990'larda hız kazandığını görüyoruz. Bu yıllarda yerli sermaye ile kurulmuş özel bankalarda başlayan teknolojik yatırım atılımı ve kurulan AR-GE odaklı bankacılık merkezleri önemli başarılara imza atılmasını sağladı. Türkiye'deki bankaların aynı dönem içinde elde ettikleri yüksek kârları teknolojiye odaklamaları özellikle ödeme sistemleri alanında yapılan atılımcı ve yenilikçi çözümler olarak kendisini bizlere gösterdi.

Ancak 2001 yılında Türkiye'de yaşanan ekonomik kriz üzerine siyasi iradenin bankacılık sektörü üzerinde gerçekleştirdiği düzenleme ve kontroller ile birlikte devrimsel bir adım teşkil

etti. Aynı dönemde Türkiye ekonomisi yeniden yapılanmaya ve ülkede uzun yıllar boyunca devam eden yüksek enflasyon hızla düşmeye başladı. Artık bankaların yüksek faiz gelirleri düşüyor ve bankalar bankacılık hizmetlerinden kâr etmeleri gereken yeni bir döneme giriyordu. Türkiye'de bankalar bu dönem ile birlikte teknolojinin yardımını alarak yenilikçiliği sürdürmek ve verimlilik odaklı projeleri hayata geçirmekten başka seçenekleri kalmadığını hızlı şekilde kabullendiler.

2008 yılına gelinip küresel finansal krizin patlaması ve hemen akabinde FinTech kavramının hızla yükselmesine karşı Türkiye'deki bankacılık sisteminde durum farklı tezahür etti zira batıdaki bankaların hantal yapısına karşı Türkiye'deki bankacılık sistemi gelişmiş bir teknoloji üzerinde ayakları yere sağlam basar hale gelmişti.

Son 15 yılı aşkın süredir FinTech alanında Türkiye'deki bankacılık sistemi, özellikle ödeme çözümleri alanında dünyanın en ileri uygulamalarına ev sahipliği yapmaktadır.

Blockchain Teknolojisinin Yükselişi

2008 yılında yaşanan küresel finansal krizin hemen ardından ortaya çıkan Bitcoin ve altındaki Blockchain teknolojisi özellikle batı dünyasında geleneksel sisteme güveni kalmayan tüketiciler için cazip bir alternatif olarak ortaya çıkmıştır.

Yüzlerce yıllık dönemde gelişen bankacılık sektörüne karşı Blockchain çözümlerinin bir gecede şu anki popüler haline geldiğini söylemek yanlış olur. Üstelik bu yapıyı başarılı kılan tek şey küresel ekonomik kriz de değildir. Bitcoin yapısı itibariyle kullanıcılarının kimliklerinin gizli kalmasını sağlar bu sebeple

yasa dışı gelirler için bir anda uluslararası değer transferi sistemine dönüşmüştür.

Her ne kadar Bitcoin son yıllarda günahların para birimi olmaktan kurtulmuş olsa da altında yatan Blockchain teknolojisi toplumlara ve işletmelere merkez bankaları gibi kontrol mekanizmaları olmaksızın üstelik kimlik denetiminden bağımsız yeni bir uluslararası, hızlı ve güvenilebilir platform sunmayı başarmış ve kendini bu noktada ispatlamıştır.

Tüketicilerin ve işletmelerin hiçbir merkezi kuruma ihtiyaç duymadan ve sistemin kendisinin güvenliği garantilediği bir ortamda değer yaratmasına, takas ve ticaret yapmasına imkan tanıyan Blockchain teknolojisi bu gün işletmeler ve tüketicilerden çok bankacılık ve finans sisteminin ilgisini çekmektedir. Öte yandan kitabımızın ilerleyen bölümlerinde ele alacağımız gibi Blockchain kullanım alanları sadece bankacılık ve finans sektörü ile de sınırlı değildir.

Şimdi sizleri maceramıza çıkacağımız çok eski tarihlere götürelim. Veri kavramının tarihinin ne kadar geçmişe dayandığını ve hatta bizi şaşırtacak şekilde bunun insanlığın bir eseri olmadığı gerçeği ile yüzleşmek için bir sonraki bölümle yolumuza devam edelim.

1.2. Temel Kavramlar

Blockchain teknolojisini anlamak için bazı temel kavramlar konusunda kafamızda soru işaretleri kalmaması gerekiyor. Bu sebeple bu bölümde Veri, Veri Tabanları, Big Data (Büyük Veri), 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 dilimize karışmaya 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 soyutlamadır.

Bir verinin tek başına bir anlamı ve işlevi bulunmamaktadır. Veriler toplandıktan sonra gruplanarak, sıralanarak ve özetlenerek, elle ya da bilgisayarla işlenip enformasyona dönüştürüldüklerinde anlam kazanmakta; ait oldukları bağlamı açıklama gücüne kavuşmaktadır. Problem çözme ya da karar verme gibi bir amaca hizmet edebilecek duruma gelmektedir.[4]

Kayıtlı olmayan veriler 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 kaybetmektedir.

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 veridir.

İnsanlık tarihinin kayıtlı ilk verileri M.Ö 18 ila 20 binli yıllarda hayvan kemikleri üzerine çentikler atılarak oluşturulan rakamsal ifadeler olarak karşımıza çıkıyor. Ishango adı verilen

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

bu kemikler günümüze kadar ulaşmış ve bugün Belçika Kraliyet Doğa Bilimleri Enstitüsünde koruma altında sergilenmektedir.

Yazının keşfedilmesi ile birlikte veri kümelerinin hızla büyüdüğünün ve insanlar arasında aktarılan bilgi miktarının arttığına 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. Maalesef bünyesinde bulunan 150 bin ciltten fazla toplamda ise 900 binden fazla fazla el yazması eserin yer aldığı bu kadim kütüphane 391 yılında yakılarak yok olmuştur.

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 Almanya'da Johannes Gutenberg tarafından geliştirilmiştir.

Verinin insanların kontrolünde ancak makine diline dönüşmesi ise 1801 yılında Fransız bir mucit olan Joseph Jacquard kartlar üzerinde delikler açarak veriyi depolaması 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 metottur. 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 1950 yılında UNITY-

PER isimli ABD merkezli bir şirket ilk olarak manyetik depolama sistemini bilgisayarlar için geliştirmiş ve sonrasında uzun yıllar boyunca finans ve bankacılık sektöründe de kullanılan UNIVAC bilgisayar sistemlerinde kullanmıştır.

UNIVAC ile birlikte manyetik şeritlerde veri depolama teknolojisinin 1951 yılında ticari olarak bilgisayar dünyasıyla buluşması sonrasında 1960 yılında IBM 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 dönemimde disketlerde 1,44 MB gibi kapasiteler konuşulurken bu miktar CD'ler ile birlikte 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 sürekli kapasitesi büyüyen flash bellekler ile birlikte 2010 ve sonrasında artık bilgisayarlardaki optik disk sürücüler bir standart olmaktan çıkmış ve internetin 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 2007 hızla popüler hale gelen bulut depolama çözümü Dropbox servisi 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.

Elbette bunca veriyi depolarken karşımıza yeni bir kavram daha çıkıyor: Veri Tabanları

Veri Tabanları

İnsanlığın çok daha geçmişinden gelen DNA'nın nasıl bir veri sistemi olduğuna ve bunu depolamak için organik yapıların nasıl kullanıldığına geçen bölümde bakarak daha sonra bu hikayeyi günümüzün en modern veri depolama sistemlerine kadar 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.

Bu sefer hikayemize geçen bölümde bahsettiğimiz delikli kartların bir veri tabanı olarak kullanılmasını ele alarak devam edeceğiz.

Delikli kartlar veriyi depolamak kadar aynı zamanda onu organize şekilde saklamak için de kullanılan bir yöntemdi. Pek

çok farklı delikli kart üzerlerinde saklı olan verilerin amacına uygun şekilde kullanılması 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 da 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 veritabanı bilgisayar sistemleri için ilk olarak 1960'lı yıllarda kullanılmaya başlandı. Bu alandaki ilk modern uygulamanın aya gitmek üzere tasarlanan Saturn V roketine ait parçaların listelendiği ve kaydedildiği veritabanı sistemi olarak karşımıza çıkıyor.

1970'lere gelene kadar aslında tüm veritabanı olarak adlandırılan sistemlerin temelde bu gün 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 Veritabanı" tanımını ortaya çıkarmıştır.[5] Codd bu tanımı yaparken kurum içinde gerçekleştirdiği sunumda şöyle bir ifade kullanmıştır: ***"Gelecekte büyük veri kümeleri ile çalışacak kullanıcıların makinelerin bu veriyi nasıl sakladığı konusunda bilgi sahibi olmasına gerek olmamalıdır."***

İlişkisel veritabanları veriyi tablolarda saklar ve bu tablolar arasındaki bağlantıları oluşturur. Kullanıcılar verilerin nasıl

[5] http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/reldb/

saklandığı ile değil kendilerine nasıl sunulduğu ile ilgilenir. Bu sebeple veritabanında kayıtlı verilerin sorgulanması için yine Edgar Codd tarafından geliştirilen SQL (Structured Query Language–Yapılandırılmış Sorgulama Dili) dili kullanılır. SQL 1980'li yıllardan itibaren bir standarda dönüşmüştür.

1980'li yıllarda kişisel bilgisayarların yaygınlaşmaya başlaması ile hayatımıza giren bir diğer düzenli veri depolama çözümü ise Tablolama Uygulamaları olmuştur. İlk olarak Lotus 1-2-3 olarak karşımıza çıkan tablo çözümleri ilerleyen yıllarda Microsoft'un geliştirdiği MS Office ürün ailesi içinde yer alan Excel ile artık temel eğitimden en kompleks şirketlerin finans ve muhasebe servislerinde kullanılan bir çözüme dönüşmüştür.

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

2000'li yıllardan itibaren kullanılmaya başlayan bir diğer veritabanı çözümü ise NoSQL olarak tabir edilen çözümler olmuştur. Bu veritabanlarında ilişkisel tablolar bulunmaz bunun yerine sabit yapıda tekil şemalara sahiptirler ancak bu veritabanlarını güçlü kılan çok büyük veri kümeleri içinde çok hızlı arama yapmaya imkan tanımalarıdır. Örneğin Google arama motorunda bu tarz bir veritabanı kullanılır böylece milyarlarca web sayfası içinde aradığınız bir veya daha fazla kavram için milisaniyeler içinde sonuç almanız mümkün hale gelir.

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

Artık günümüzde 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[6]

Şehir ışıkları ile kirlenmemiş açık bir gökyüzüne bakacak olursanız yıldızların sayısı karşısında hayran kalmamak mümkün değil. Oysa şu ana kadar gözlemlediğimiz yıldızların sayısı tüm evrenin çok ufak bir parçasını oluşturuyor. Bu gün internete bağlanan cihazların insan nüfusunu geçtiğine şahit oluyoruz. Nesnelerin İnterneti (IoT - Internet of Things) adı verilen bu yapı katlanarak büyürken oluşturduğu ekonomi trilyonlarca dolar olarak kabul ediliyor. Bu sistemin bütünü tarafından üretilen verinin dağıtık şekilde kaydedilmesi ve saklanması mümkün olabilir mi?

Aslında bu sorunun cevabı bundan uzun yıllar önce verilmişti. 2000'lerin başında bir birinden 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 sistemlerde veri tek bir merkezde değil sayısı milyonları bulabilecek makine üzerinde bulunur. Bu makinelerden bazıla-

[6] Disney Pixar'a ait Toystory animasyon dizisindeki Buzz Lightyear isimli astronot karakterin sloganı.

rı verinin tamamını bazıları ise kısmen belli bir parçasını içerebilir. Eğer bu veriye ulaşmak isterseniz sistem sizi olabilecek en optimum düzenleme ile bu veriyi farklı makinelerden çekecek şekilde yönlendirir. Siz veriyi kendi bilgisayarınıza çektiğiniz süreç içinde aynı zamanda aldığınız veri için 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 sunar ancak buna rağmen içeriğin şifrelenmemesi, verinin nerelerde saklanacağına dair tercih seçeneği 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) isimli çözümler ortaya çıkmıştır ve kitabımızın ana konusu olan Blockchain teknolojisi de bu çözümün farklı bir uygulaması olarak değerlendirilebilir.

Big Data (Namıdiğer Büyük Veri)

Geride bıraktığımız veri ve veri tabanları konularında gördük ki 1 ve 0'lardan oluşan dijital dünyanın kapıları açıldığı günden bu yana verinin küçük bir değeri ifade ettiği hiçbir dönem olmamıştır. Evet bu gün için 10 MB'lık bir dosyayı internetten indirmek milisaniyeler alıyor olabilir ancak 10 yıl önce çevirmeli bağlantılar ile 10 MB gerçekten indirmek için üzerinde düşünmek durumunda olduğunuz bir büyüklüktü.

Pek çok kez gördüğünüzü düşündüğümüz ve sürekli güncellenen internetin bir dakikası konulu Infografikleri düşünün. Her 60 saniyelik dönemde gönderilen e-posta, atılan tweet, yapılan yorum, verilen beğeni, gerçekleşen sesli ve görüntülü

IBM'in 1956 yılında ürettiği 5 MB büyüklüğündeki sabit disk tören eşliğinde uçağa yükleniyor.

görüşmeler gibi milyonlarca verinin oluşturduğu dev bir dijital nehirden ve bu nehrin döküldüğü okyanustan bahsediyoruz.

Google'ın kurucularından ve tüm Google şirketleri bünyesinde barındıran Alphabet'in İcra Kurulu Başkanı Eric Schmidt yıllar önce bir konuşmasında şöyle demişti: "İnsanlığın var olduğu günden 2003'e kadar beş exabyte veri ürettik. Artık bu veriyi her iki günde bir üretiyoruz ve hızımız giderek katlanıyor."

Tüm bu veri yığınını ifade etmek için kullanılan Big Data kavramı aslında dört temel unsurdan oluşuyor. Bunlar;

Hacim: Verinin toplam büyüklüğü

Hız: Zamana bağlı olarak üretilen veri miktarı ve verinin yayılma hızı (örneğin viral bir Youtube videosu)

Çeşitlilik: Sözel veri, yazılı veri, görsel veri ve bu üçünün dijital olarak ifade edilmesi ile alıcılardan (sensörlerden) gelen veriler

Karmaşa: Twitter'ın zaman akışı, her dakika Youtube'a yüklenen 100 saatlik video, MOBESE kameralarından gelen veriler,

IoT cihazlarının ürettiği alıcı verileri ve aklınıza gelip gelemeyen tüm kaynaklardan akan ne varsa hepsi.

Big Data bu dört temel unsura dayanılarak şu şekilde tanımlanmaktadır: Kullanıcıları için; yaygın olarak kullanılan donanım ve yazılım araçlarının, kabul edilebilir sürede, yakalaması, takip etmesi ve işleyerek anlam vermesinin mümkün olmadığı kadar çok veri üretilmesi sürecidir.

Yukarıdaki tanımı bir kaç kez okumanızı tavsiye ediyoruz.

Yani Big Data bir SÜREÇTİR ve eğer elinizdeki veriye yeterince hızlı şekilde anlam kazandıramıyorsanız buna Big Data denilir.

Veri, veri tabanları ve bunların oluşturduğu Big Data'nın iletişim kanalları içinde taşınması gerekiyor zira artık her şeyin bir birine dijital olarak bağlandığı bir dünyada yaşıyoruz. Ancak bu günümüzün karmaşık gibi görünen iletişim ağlarına ulaşmamız iki yüz yıla yakın zaman almıştır.

Ağ Teknolojilerinin Kısa Tarihi

Teknoloji sayesinde artık yüz yıllık zaman dilimleri bizler daha kısa zamanda daha çok şey yapmamıza rağmen daha hızlı geçiyor. Bu gün 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 kayıtlı veri olan DNA'nın kablosuz şekilde iletilmesi için çiçekler polenlere ve diğer bitkiler çekirdeklere sahip.

İnsanoğlunun modern iletişim teknolojilerini kullanmaya başlaması ile elektriğin keşfi ile benzer dönemlere rast geliyor. 1830 yılında ABD'li Joseph Henry ilk kez elektromıknatıs kullanarak uzaktan zil çalan bir sistem geliştirdi. ABD'li ressam Samuel Morse 1835 yılında ilk kez elektromıknatıslı telgrafı yaptı aynı zamanda tüm dünyada kabul gören Mors alfabesini oluşturdu.

İnsanların birbiriyle sesli olarak uzaktan konuşması için yaklaşık 40 yıl beklemesi gerekti. 1880 yılında Alexander Graham Bell ve Charles Sumner Tainter radyofon isimli aygıtı geliştirdiler.

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 olmuştur.

1960 yılında günümüzün istemci-sunucu (client-server) yapısının temelleri atılmış ve IBM, 1964 yılında ABD hava yolu şirketleri için SABRE adında bir ağ oluşturarak 65 şehirdeki 2.000 terminali bir birine bağlamıştır.

1969 yılında ABD ordusu için geliştirilen ARPAnet aynı anda farklı bilgisayarların bağlanabildiği ilk ağ olarak karşımıza çıkar ve bu gün kullandığımız internetin temelleri de bu yıllarda atılır.

Bu gelişmelerin yaşanırken 1973 yılında Xerox'da çalışan iki mühendis olan Robert Metcalfe ve Dave Boggs, Ethernet teknolojisini geliştirerek bu gün hâlâ bir standart olan bu temel ağ teknolojisinin temellerini atar.

1982 yılında dünyanın ilk Ağ İşletim Sistemi olan Novell NetWare piyasaya sürülür. 1987 yılında mobil GSM standartları oluşturulur.

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

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

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

Günümüzde Gigabit seviyesinde hızlara ulaşan iletişim ağlarımız kitabımızın ana konusu olan Blockchain teknolojisinin mümkün olmasını sağlayan önemli bir bileşeni teşkil ediyor.

Son olarak Blockchain teknolojisinin temelinde yatan çok önemli bir kavram olan Kriptoloji'ye tarihine dalmadan kısaca göz atmamız gerekiyor.

Kriptoloji Kavramı

Eğer veriyi, iletişim ağları üzerinden, geniş ağlara kopyalayıp çoğaltarak dağıtacaksak ve farklı veri tabanlarında saklayacaksak bu verilerin gerçekten gizli kalırken tutarlılığının sağlanması gerekir. Bu amaç içinse kriptoloji kullanılır.

Kriptoloji basit bir şekilde "şifreleme bilimi" olarak tanımlanabilir. Yunanca gizli anlamına gelen **kryptos** ve yazmak anlamına gelen **graphien** sözcüklerinden türetilen, Kriptolojinin

bir alt kolu, "**kriptografi**" (cryptography) verilerin şifrelenmesini ifade etmektedir.

Şifreleme, herhangi bir veri kümesini bir kural yapısı kullanarak rastgele görünen bir veri kümesine dönüştürür. Bu rastgele gibi görünen veri kümesi, şifreleme yapılırken kullanılan anahtar ile sahibi için orijinal anlamlı haline geri dönüştürülebilirken bu anahtara sahip olmayanlar için tekrar orijinal yapısına çevrilemez. Böylece şifrelenmiş veri nerede ve ne şekilde depolanırsa depolansın sadece anahtar sahibi tarafından anlamlı kalmaya devam edecektir. Bu sürecin teknik detaylarına ilerleyen bölümlerde değineceğiz.

Artık veri, veri tabanı, iletişim ağları, Big Data ve kriptografi kavramları hakkında daha çok bilgi sahibi olduğumuza göre; internetten sonraki en büyük ağ devrimi olarak nitelendirilen Blockchain teknolojisine geçiş yapmaya hazırız. O halde "Perde Açılsın!"

1.3. Blockchain Dünyasına Giriş

Şu ana kadar edindiğimiz temel bilgileri şimdi bir bütün olarak düşünmemiz gerekiyor. Artık veriyi tekil sistemlere kaydetmek zorunda değiliz, veriyi bulut gibi uzak bir noktadaki hizmeti kullanarak hatta P2P gibi yapılar üzerinden dağıtarak saklamamız mümkün. Bulut ve P2P yapılarının üzerinde veri tabanları da bulunabilir. Üstelik elimizdeki verinin büyüklüğü onu bir veya pek çok yere dağıtmamız için bir engel de teşkil etmiyor zira çok yüksek hızlı gerek kablolu gerekse kablosuz 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, daha sonra bu kaydın pek çok kopyasını pek çok bilgisayara dağıttık, nihayet her bilgisayar işlemin bir kaydını tutacak hale geldi. Bunun en temel sebebi ise maliyetlerin zaman içinde ciddi şekilde düşmesiydi.

Moore, Metcalfe, Reed hatta Bezos kanunları olarak ifade edilen yaklaşımlar temelde bize hep aynı şeyi söyler: dijital teknolojilerde gelişim süreci o kadar hızlıdır ki her bir kaç yıllık dönemde teknoloji ve maliyetler ters orantılı olarak gelişme kaydeder.

Bu gelişim bizi yukarıdaki şekilde gördüğümüz son aşamaya; yani temel olarak verinin, ucuzlayan iletişim ağları üzerinden, pek çok sayıdaki bilgisayarlara dağıtılmasını pratik açıdan mümkün olduğu noktaya getiriyor. Bu noktada kayıtlarımız tüm sitemlere kopyalanmış oluyor.

Bu yaklaşıma Dağıtık Kayıt Defteri (Distributed Ledger) adı verilmektedir. Bu kavramın yeni bir kavram olmadığını ve geçmişte eDonkey veya Bittorrent gibi ağlarda kullanıldığını anlatmıştık. Ancak bu ağların ortak sorunu üzerinde tutulan verinin şifrelenmemiş olmasıdır. Bu sebeple dileyen herkes bu verilere erişebilir. Bu noktada verileri şifreleyerek (kriptografi) ile dağıtık kayıt defterlerine dağıtmak 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 tutarlılığı ortadan kalkacaktır. Bu durum bizi ikinci aşamaya taşır.

Aşama 2: Dağıtık Kayıt Defterinde Nitelikler ve Süreçler

Bu aşamada elimizdeki iletişim ağına dağıtacağımız verinin tüm dağıtıldığı noktalarda aynı kaldığından emin olmalıyız. Farklı bir ifade ile birden fazla tarafın bulunduğu bir sistemde, sisteme eklenmesi istenen herhangi bir işlemin geçerli olarak kabul edilebilmesi için sistemin geneli tarafından kabul edilmiş kurallara uygunluğunun kontrol edilmesi gerekiyor. Bu kontrol sürecine ve sonunda fikir birliğine varmaya "mutabakat" adı veriliyor.

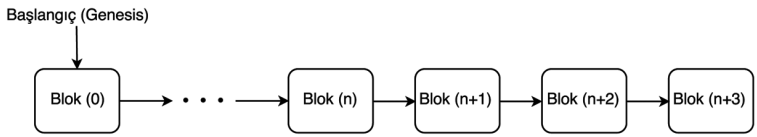
Mutabakat için kontrol işlemi sistem tarafından güvenli olarak tanımlanmış bir dış yapı tarafından yapılabileceği gibi bu işlemi sistem içerisinde de gerçekleştirmek mümkün.

Mutabakatın sistemin kendisi tarafından gerçekleştirilmesi için dağıtık sistem üzerinde kayıt defterini tutan makinelerin bu işlemin geçerliliği konusunda kendi aralarında fikir birliğine varması lazım. Bu fikir birliği gerçekleştiğinde yan mutabakat sağlandığında artık yeni işlemin kayıt defterine yansıtılması için bir engel kalmıyor. Bu yaklaşıma da "mutabakat yapısı" adı veriliyor.

Dijital bir sistem üzerinde mutabakat yapısının sağlanması için bunun yazılımsal açıdan garanti altına alınması lazım. İşte tam bu noktada Blockchain teknolojisi ortaya çıkıyor ve diyor ki; "Ben tüm bu sorunları çözeceğim. Veriyi, iletişim ağları üzerinden, dağıtılmış şekilde saklamanızı ve bu süreç içinde verinin tüm noktalarda aynı kaldığına dair mutabakat yapmanızı sağlayacağım. Hatta bununla da kalmayacağım herkes kendi verisini şifreleyeceği için bu veriyi sadece kendisi kullanacak ve izin verirse diğer taraflar bu veriye erişebilecek."

Bu noktada Blockchain teknolojisi, dijital dünyanın bize sunduğu çok temel bir mantığı yani veriyi dilediğimiz gibi yazıp, silme ve güncelleme imkanına farklı bir bakış açısı getiriyor. Şöyle bir çözüm sunuyor; Veriyi bloklar halinde ele alalım, her bir blok önce belirli kurallara göre oluşturulsun sonra sisteme yazılsın, bu blok tüm dağıtık kayıt defteri yapısındaki uç noktalara yayılsın. Yeni bir blok geldiğinde bir önceki bloğun bir özetini alalım (burada yazılımsal bir kriptoloji yaklaşımı kullanılıyor, ilerleyen bölümlerde bu tekniklerin detaylarına bakacağız) bu özet ile birlikte ikinci bloğu oluşturalım ve zincire ekleyelim. Bu şekilde her bir yeni blok geldiğinde bir öncekinin özeti ile ilişkili olacağı için tüm zincir bir birini tamamlayan bir yapıya sahip olur.

Blockchain kayıtlarını pek çok uç noktaya dağıttığımızı belirtmiştik. Bu durumda tüm noktalar kendi aralarında iletişim halinde kalarak sistemin bozulmadığının teyidini yapabilirler. Eğer Blockchain 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 eder.



İlk Blok (Genesis) kaydından sonra tüm blokların bir birini takip ettiği yapı

Ancak hâlâ birkaç problemimiz var. Blockchain her ne kadar verinin dağıtık bir ağ yapısında şifrelenerek ve bozulmadığı konusunda mutabık kaldığımız bir yapıda depolanmasını sağlasa bile verinin niteliği yani içerik konusunda standartları belirlemedik. Bu aslında büyük bir sorun değil, her bir blok için en fazla 1 MB veri içerecek şekilde diye bir sınırlama getirebilir ve bu nitelikleri çeşitlendirebiliriz. Buna rağmen hâlâ sormadığımız ve cevabını vermediğimiz bir soru var: İnsanlar neden Blockchain sistemini kullansınlar? Cevabını vermeden önce konuya bir bakış açısı daha kazandıralım;

Açık ve Özel Blockchain Ağları

Kısa bir süre için Blockchain dünyasını bir kenara koyalım ve bulut dünyasına yüzümüzü dönelim. Bulut servisleri açık (public) ve özel (private) olarak ikiye ayrılır. Örneğin bir bulut e-posta servisi olan Gmail açık bir servistir. Dileyen herkes uygun bir kullanıcı adı ile @gmail.com uzantılı bir e-posta adresini ücretsiz olarak alabilir. Öte yandan bu servisi sunan Google, Gsuite adını verdiği hizmet ile Gmail bulut altyapısını özel olarak da sunmaktadır. Bedelini ödeyen herkes kendisine ait bir domain adı ile bu bulut altyapısını kullanabilir. Bu durumda sadece bu bedeli ödeyen işletme için kendi domain uzantısı ile Gmail altyapısını kullanmak mümkün olacaktır.

Benzer bir yaklaşım Blockchain dünyası için de geçerlidir.

Blockchain türlerini belirleyen temel ayrışım Blockchain ağının **Açık (Public)** veya Özel **(Private)** olmasıdır. Ancak Blockchain ağlarında ikinci ayrışma katmanını olarak ağ içindeki **mutabakat sistemine dahil olma** izni gelir. Bu kapsamda;

Açık (Public) Blockchain ağlarına dileyen herkes ağa katılabilir. Ancak bu ağlar içinde mutabakat sistemine dahil olmak herkese açık veya izin gerektiren yapıda olabilir.

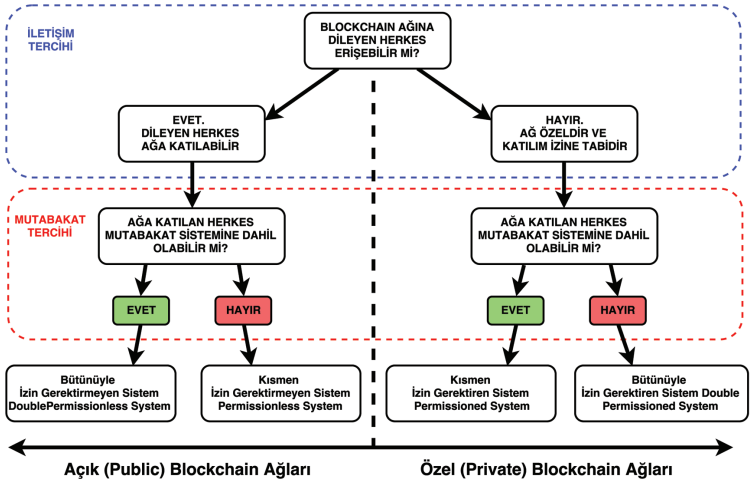
Açık (Public) Blockchain ağlarında katılımcılar eğer **mutabakat sistemine** de izin almadan dahil oluyorsa (blok oluşturabiliyor ve blok doğrulayabiliyorsa) bu sistemlere **Bütünüyle İzin Gerektirmeyen Sistem – Double Permissionless System** adı verilir.

Açık (Public) Blockchain ağlarında katılımcılar eğer **mutabakat sistemine** izin alarak dahil oluyorsa (izin sonrasında blok oluşturabiliyor ve blok doğrulayabiliyorsa) bu sistemlere **Kısmen İzin Gerektirmeyen Sistem – Permissionless System** adı verilir.

Özel **(Private) Blockchain** ağlarında ise sadece izin verilenler ağa katılabilir. Ve yine bu ağlar içinde mutabakat sistemine dahil olmak, ağa katılmasına izin verilen herkese açık veya ikinci kez izin gerektiren yapıda olabilir.

Özel (**Private) Blockchain** ağlarında, izin alarak sisteme giren katılımcılar eğer **mutabakat sistemine** izin almadan dahil oluyorsa (blok oluşturabiliyor ve blok doğrulayabiliyorsa) bu sistemlere **Kısmen İzin Gerektiren Sistem – Permissioned System** adı verilir.

Özel (Private) Blockchain ağlarında, izin alarak sisteme giren katılımcılar eğer **mutabakat sistemine** de izin alarak dahil oluyorsa (blok oluşturabiliyor ve blok doğrulayabiliyorsa) bu sistemlere **Bütünüyle İzin Gerektiren Sistem – Double Permissioned System** adı verilir.



Bu aşamada bir soru sormamız gerekiyor. Blockchain türlerinin bu dört yapısı kime ne fayda sağlayacak? İnsanlar neden sisteme dahil olsunlar? Neden mutabakat sürecine girsinler? Örnekler ile açıklayalım;

Bütünüyle İzin Gerektirmeyen Blockchain ağlarında, ağının bu durumdan kazancı, sisteme dahil olan herkesin mutabakatın garanti altına alınması için eşit ve dengeli rol almasıdır. Ancak bu sisteme dahil olacak insanların da bu işten bir çıkarının olması gerekir. Bu durumda Blockchain ağının kendisi bir değer ifade etmelidir.

İşte bu şekilde açık ve Blockchain ağının kendisinin bir çıkar sağladığı en büyük örnek ve platform **Bitcoin Blockchain** ağının kendisidir. Bitcoin ağında insanlar sisteme dahil olarak Blockchain ağının mutabakat sağlayan bir uç noktası haline gelirler ama bunun karşılığında ağ üzerinde üretilen Bitcoin'lerin

finansal bir değeri vardır ve insanların çıkarı bu değere sahip olmaktır. İlerleyen bölümlerde Bitcoin sisteminin nasıl çalıştığını detayları ile açıklayacağız.

Ancak pek çok insan için Bitcoin kazanmak bir anlam ifade etmeyebilir. Bu durumda Blockchain teknolojisi diğer insanlar için anlamsız ve faydasız mı olacaktır? Elbette hayır.

Kısmen İzin Gerektirmeyen Blockchain ağlarının içinde sisteme dahil olan herkes verilere erişebilir. Erişilen veri, izin almadan bunlara erişenler için bir değer ifade edebilir. Öte yandan mutabakat sistemi ağa yazılan verilerin doğruluğunu ve tekilliğini sağlayabilir.

Bu konuda farazi bir örnek olarak bağımsız müzisyenlerin parçalarını yayınladıkları bir platform düşünelim. Bu durumda sisteme giren herkes tüm müzik parçalarını dinleyebilir ve bunlara erişebilir. Sistemin mutabakatını sağlayanlar izinli kişilerse müzisyenler veya onları temsil eden meslek birlikleri olabilir. Bu durumda bir sanatçı eserini sisteme yazdığında "izin verilen" kişiler **mutabakatı** sağlar. Ağa erişenler için çıkar müzik parçaları olurken, mutabakatı sağlayanlar için çıkar eserlerinin kayıt altına alınmasıdır.

Kısmen İzin Gerektirmeyen Blockchain ağlarına bir diğer güzel örnek ise pek çok farklı amaca hizmet edebilen **Ethereum** Blockchain ağıdır. Ethereum Blockchain ağında **Akıllı Sözleşmeler** adı verilen bir yapı vardır. İlerleyen bölümlerde detayları ile anlatacağımız **Akıllı Sözleşmeler** aslında birer uygulamadır. Akıllı Sözleşmelerin tetikleyeceği işlemlerinin ne olacağı bir işletme, kişi veya grubun belirlediği bir durum olabilir. Ethereum ağına girmek izne tabi değildir ancak Akıllı Sözleşmelerin be-

lirli bir mutabakat ile tetiklediği işlem süreçlerine dahil olmak izin gerektirir.

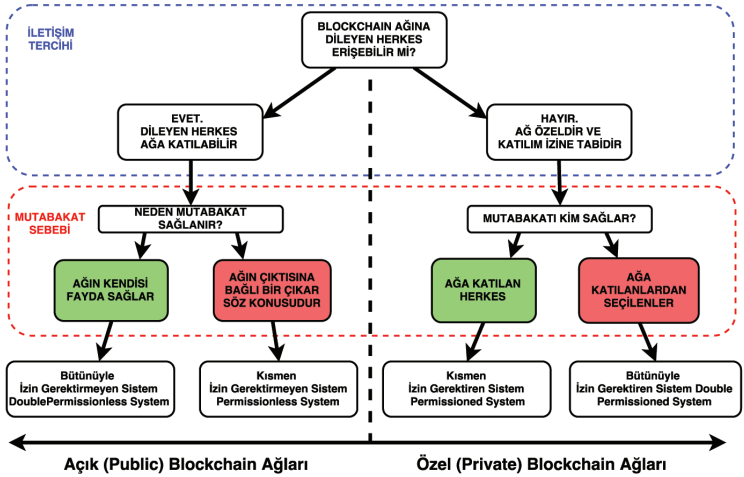
Kısmen İzin Gerektiren Blockchain ağına farazi bir örnek olarak bir bankanın dahili havale sistemini örnek gösterebiliriz. Tüm şubeler bu ağın bir parçası olabilir. Yani bu ağa girmek için izin gereklidir ve bu izni banka sadece şubelerine sağlar. Bir şube içinde veya şubeler arasında yapılan gerçekleşen bir havale işlemi için tüm şubelerin mutabakat sistemine dahil olması gerekmektedir.

Bütünüyle İzin Gerektiren Blockchain ağına farazi bir örnek olarak bankalar arasındaki EFT işlemleri örnek gösterilebilir. Bir EFT işlemi için tüm bankaların kayıt ortak bir Özel Blockchain ağının olduğunu varsayalım. Bu sisteme sadece bankalar girebilmektedir. Bu ağda A bankasından B bankasına bir EFT işlemi gerçekleşsin. Bu işleme ait veriye "gerektiği takdirde" sisteme dahil olan tüm izinli bankalar ulaşabilir. Ancak burada ilgili işlemim mutabakatını sadece A ve B bankası yapmak için izin yetkilendirilmiştir.

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

Bu şema ilk bakışta yukarıda paylaştığımız şemaya benzemekle birlikte Mustabakat Sebebi katmanı ile farklılık göstermektedir. Bu noktaya dikkatinizi çekmek isteriz.

Artık Blockchain ağının ne olduğunu (temelde bir veri saklama sistemi), dağıtık yapısını (dağıtık kayıt defteri), veriyi nasıl koruduğunu (şifreleme, kriptografi), Blockchain ağı üzerindeki işlemler için neden mutabakat gerektiğini, Blockchain ağına



erişimin (açık, özel) ve mutabakata dahil olma (izin gerektirmeyen ve izinli) şeklinde türlerini öğrenmiş bulunuyoruz. O halde gizlilik ve anonimlik konusuna geçebiliriz.

Blockchain Dünyasında Gizlilik ve Anonimlik

Blockchain yapısında temel olarak bloklar ve blok kapsamındaki tüm işlemler ağa katılanların erişimine açık olarak bulunmaktadır. Bu noktada ağ üzerindeki işlemlere ait özel bilgilerin kriptografi tabanlı çözümler ile şifrelenmiş bir şekilde tutulmasının sağlanması Blockchain yapılarında mutlak bir gizlilik ve anonimlik (gerçek kimlikten bağımsızlık) algısının oluşmasına yol açmaktadır. Bu algının önemli nedenlerinden birisi de Bitcoin Blockchain ağının tasarımı gereği üzerinde oluşturulan kişilere ait cüzdan bilgileri için gerçek kimlik bilgileri talep etmemesidir. Farklı bir ifade ile Bitcoin Blockchain ağına giren bir

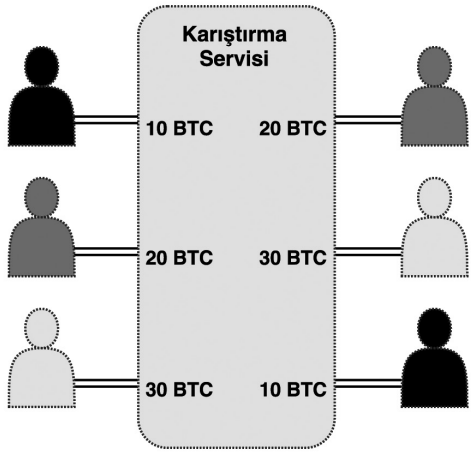
kişinin gerçek hayatta kim olduğunu sadece ağ yapısını inceleyerek pratik olarak bulmak neredeyse imkansızdır.

Bir Blockchain ağı üzerindeki şifrelenmiş bilgilerin temel olarak bir dış gözlemci tarafından orjinal haline çevrilmesi mümkün olmasa da açık olan işlem bilgileri üzerinde çeşitli analiz çalışmaları yapılarak farklı veri modellemeleri oluşturulabilmektedir. Örneğin, Bitcoin Blockchain ağında tüm işlemleri için aynı adres bilgisini kullanan bir kullanıcı için gerçek kimliği bilinmese bile, kullandığı adres ile ilişkili tüm hareketlerin tek bir kişiye ait olduğu yorumlanabilir. Bu hareketlerden birisinin fiziksel dünyada bir karşılığı olması durumunda kişinin kimliğine erişim mümkün olmaktadır (mesela fiziksel bir ürün alımında, ürünün gönderildiği adres bilgisi kullanılarak). Bu tarz bir ilişki kurulduktan sonra kullanıcının haberi olmadan bugüne kadar olmuş ve gelecekte olacak tüm işlemleri takip edilebilmektedir. Tüm dünyada pek çok ülke bu bilgileri analiz etmek ve gerçek kimlikler ile eşleştirebilmek için çalışmalar yürütmektedir zira Bitcoin her ne kadar artık günahların para birimi olmaktan kurtulsa da (ilk dönemlerinin aksine Bitcoin artık yasa dışı değer transferi için çok daha az kullanılmaktadır) devletler kendi kontrolleri dışında bir değer transferinin gerçekleşmesini güvenlik ve istihbarat açısından doğru bulmamaktadır.

Bu tarz durumlar için her kullanım için farklı adres üretimi gibi teknikler geliştirilmiş olsa da bu ancak belirli bir seviye de bağlantısızlık sağlayabilmektedir. Bu tarz çözümler için de kullanıcı tekilleştirmeye gidebilen yaklaşımlar geliştirilmiştir.

Anonimlik özelliği kazanabilmek için ortaya atılan yaklaşımlardan bir tanesi "karıştırma" (mixing) servisleridir. Bu

servisler kendilerine yönlendirilen işlemleri "karıştırarak" yönlendirme yapan kullanıcılar tarafından belirtilen adreslere geri gönderip (basitleştirmek gerekirse servise X birim kripto-para gönderip Y adresine iletilmesini isteyen A kullanıcısı için servis kendisine istekte bulunan diğer kullanıcılardan aktarılan kripto-para işlemleri içerisinden X birimi ayırıp belirtilen Y adresine yönlendirir, bu şekilde A kullanıcısının kripto-para aktardığı hesaptan bağımsız, ilişkisi olmayan kaynaklar tarafından yönlendirilme yapılmış X birim kripto-para içeren yeni bir hesabı olmuş olur) takip sistemlerini engellemeye çalışırlar.



Karıştırma servisleri işlem takibini zorlaştırmak amacı ile arka arkaya karıştırma, sabit işlem miktarı kabulleri, rastlantısal hizmet ücreti, düşük olasılıklı işlem yutma gibi stratejiler uygulayabilirler.

Bu şekilde merkezi karıştırma servislerinin yanı sıra kullanıcıların kendi aralarında oluşturabilecekleri karıştırma proto-

kolleri bulunmaktadır. Bunların en bilinenlerinden CoinJoin protokolü, Bitcoin Blockchain platformu üzerinde kullanıcıların farklı işlemlerini tek bir işlem altında toparlayarak gerçekleştirilmesini, bu sayede kullanıcı bazında girdi-çıktı ilişkisinin takibinin yapılamamasını sağlamaktadır.

Yukarıda belirtilen Blockchain protokolü üstü çözümlerinin dışında Zcash (Zerocash) ve Dash (Darkcoin) gibi kripto-para yaklaşımları Blockchain seviyesinde kriptografik yöntemlerle anonimlik sağlamaktadırlar.

Sebebi ve amacı her ne olursa olsun Bitcoin, Zcash gibi yapılar farklı yöntemler ile gerçek kimlikleri gizlemeyi mümkün kılsalar bile kısmen İzin Gerektiren ve Özel Blockchain uygulamalarında gerçek kimlik bilgisi sistemde gerçekleştirilen uygulamaların ihtiyaç duyduğu oranda sistemde tutulabilmektedir.

İnsanlığın var olduğu günden bu yana yasa dışı ve topluma zararlı faaliyetlerde bulunan suçlular ve suç örgütleri bulunmuştur. Blockchain ağları güçlü şifreleme servisleri ile birlikte kullanıldığında kimlik takibini güçleştirmekte ve kişilerin anonim kalması için cazip bir seçenek sunmaktadır. Ancak devletlerin ve onlara ait resmi kurumların bu suç örgütleri ile mücadele etmesinin yöntemi Blockchain ağlarının sunduğu bu teknik imkanları ortadan kaldırmaya çalışmakla gerçekleşemez. Tam aksine bu imkanlar doğru şekilde kullanıldığında devlet, kurum ve kişilere kişisel ve tüzel verileri korumak için tarihte hiç olmayan yeni imkanları sunmaktadır.

Her ne kadar Blockchain türlerini irdelerken çeşitli uygulama örnekleri vermiş olsak da Blockchain ağlarının pek çok farklı amaca hizmet edebileceğini biliyoruz. Bu amaçları olabildiğince çok başlık altında sıradaki bölümde ele alacağız. Ama

önce bir nefes alıp zihnimizi boşaltmak için Değer Kavramı ve Para üzerine biraz konuşacağız.

1.4. Değer Kavramı ve Paranın Yeni Anlamı

Blockchain kavramının yükselişinde bir kripto para birimi olan Bitcoin'in rolü kesinlikle göz ardı edilemez. Her ne kadar bunu birkaç kere belirtmiş olsak ve Blockchain ağlarının amacı sadece kripto para üretmek ve kullandırmak olmasa da neden fiziksel karşılığı olmayan bir dijital varlığın böylesine değerli hale gelebildiğini, ticari amaçla kullanılabildiğini de bu kitap dahilinde 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.

Giriş bölümünde bir ara başlık olarak "Finans ve Para Nedir?" sorusuna kısaca cevap vermiştik. Hızlıca paranın tanımını hatırlayacak olursak; "Çok basit bir ifade ile niteliği bakımından ortak bir değer algısı ve kabulüdür" diyebiliriz.

Tam bu noktada FinTech dünyasının önemli liderlerinden David Birch'ün "Kimlik: Yeni Para" adı ile Türkçe'ye çevirilen "Identity is the New Money" isimli kitabında yer alan bir kısmı burada paylaşmanın doğru olduğunu düşünüyoruz.

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 çıkartarak beraberlerinde geriye diskler şeklinde yeni taşlar getirirler. Bu diskler bazıları 5-10 santim bazıları ise 3,5 metreye varan genişlikte farklı büyüklüklerde ve ağırlıklara sahiptir. Başarılı bir sefer sonunda şef büyük taşları 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 ederler 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 hafıza 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 batarsa doğal olarak taşlar da denizin dibini boylamaktadır. 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 fikirde karar birliğine varıyorsa buna para denir.

Bitcoin Bu Kadar Değerli Çünkü

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 1.800 doların üstüne ulaştıysa bunun temelinde Bitcoin altyapısında kullanılan teknolojiye güven ve bu ekonominin geniş topluluklar tarafından kabul görmesi yatmaktadır. Bunu ispatlamak için Bitcoin'e ihtiyaç duymamıza da gerek yok. Bu gün dünyanın çeşitli ülkelerinde enflasyon öylesine yüksek ki basılı paralar için üzerindeki yazılı değerler ile değil, kilo ile ağırlığını dikkate alarak işlem yapılıyor. Ülkemizin de benzer bir süreçten altı sıfır atarak geçtiğini bu noktada hatırlamakta fayda var.

Toplumsal olarak değer birliği üzerinde mutabakat yaptığımız her aracı bir para unsuru olarak kullanabiliriz.

Nakitsiz yaşama giden yolda bu temel kabul üzerine kurulabilir. Bu gün kazandığımız parayı teorik olarak hiç elimize almadan yaşantımızı sürdürebileceğimiz bir teknolojiye sahibiz. Banka ve kredi kartları ile yapılan işlemlerde güven unsuru neye dayanmaktadır? 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 de farklı bir kulvarda kendilerine yol açıyorlar. Herhangi bir düzenlemeye tabi olmayan, merkezi bir kontrol birimi olmayan ancak tüm bu kitapta anlatılan Blockchain altyapısının ortak kabul ve mutabakat unsuru üzerine kurulu, elbette gerçek kimliği hâlâ gizliliğini koruyan Satoshi Nakamoto'nun geliştirdiği enflasyondan arındırılmış sınırlı üretim kapasitesi ile Bitcoin hızla değer kazanıyor. Eğer bir gece dünya üzerindeki tüm iletişim ağları çökecek olsa bu değerin bir karşılığı kalmayacaktır ancak aynı durum merkezi kontrol birimleri tarafından üretilen resmi para birimleri için de geçerlidir.

Burada amacımız Bitcoin'i savunmak değil ancak para doğası gereği bir değer mutabakatı ise Bitcoin bunu küresel ölçekte sağlamıştır ve Bitcoin benzeri diğer kripto para birimleri de bunu sağlamak için gayret göstermektedir. Eğer bu yazı kaleme alındığı günlerde Japon hükümeti Bitcoin'i yasal bir alışveriş aracı olarak tanımlamışsa bu yine toplumun ortak değer mutabakatı ile talep ettiği bir adım olmuştur.

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, kağıda basılmış kopyalanması güç banknotlar, silikon bir işlemci içeren kredi kartı veya cep telefonu ekranında takip ettiğiniz yanında BTC yazan bir takım rakamlar olabilir.

Kripto Para Dünyası

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 duyduğu gözlemlenmektedir. Bu ihtiyaçlar gerek oluşturulan kurumlar (merkez bankaları vb.) gerekse geliştirilen fiziksel önlemler (kağıt ve madeni para yapılarında sahtecilik karşıtı özellikler vb.) gibi çeşitli yapılar aracılığı ile karşılanmaktadır.

Internet'in ve Internet tabanlı servislerin yaygınlaşması ile birlikte özellikle son yıllarda hayatımızda yer bulmaya başlayan dijital para, sanal para kavramları içinde bunlara benzer gereksinimler bulunmaktadır. Bu kavramlar gündelik hayatta yakın dönemde popülerlik kazanmış olsa da, geçmişe baktığımızda bu ihtiyaçlar üzerinde uzun süreden bu yana çeşitli araştırmalar ve çalışmalar yapıldığını görmekteyiz.

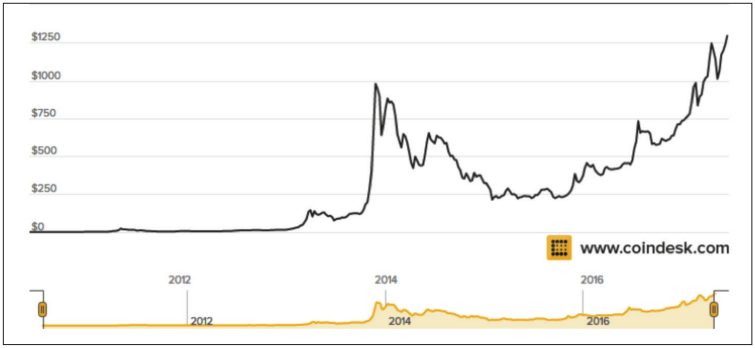
Dijital para kapsamındaki bu ihtiyaçların giderilmesinde kriptoloji kullanımı konusunda öncü çalışmalardan bir tanesi matematikçi David Chaum tarafından 1983 yılında yayınladığı bir akademik makale[7] kapsamında ortaya çıkmıştır. David Chaum sonrasında bu araştırmalarını temel alarak "DigiCash" adlı elektronik para firmasını 1990 yılında kurmuştur. DigiCash

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

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 bir 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 ileride çözümler için esin kaynağı olmuştur. İlginç olan noktalardan bir tanesi, kullanıcı sayısının az olmasının ana nedenlerinden bir tanesinin dönemin çevrimiçi kullanıcı davranış yapısının gizlilik ve güvenlik konularına önem vermemesi olmasıdır.

Günümüzde internet tabanlı servislere sürekli bağlı mobil yaşam modelinin yaygınlaşması birlikte kullanıcıların gizlilik ve güvenlik ihtiyaçları tekrar gündeme gelmiştir. Kripto para kavramı temel olarak dijital dünyada bu ihtiyaçların çözümü için şifrelemenin kullanıldığı dijital para birimleri ifade etmektedir. Kullanılan şifreleme yöntemlerin 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 alanların artışı ile birlikte daha önce hiçbir sanal para birimi tarafında ulaşılamamış bir değerlendirmeye erişmiştir.



Dolar/Bitcoin piyasa değerini veren coindesk.com'un verilerine göre 29 Nisan 2017 tarihinde 1 BTC'nin piyasa değeri 1.320 $

Bitcoin'in başarısı ile birlikte çeşitli kripto-para birimleri ortaya çıkmıştır. Bitcoin ile aynı tasarım yapısına sahip olup tamamı ile farklı bir Blockchain ağı üzerinde yaşam döngüsünü sürdüren bu kripto para birimleri "alt-coin" (alternative coin) adı verilmektedir.

Şu ana kadar yüzlerce alt-coin denemesi yapılmış, bunlardan oldukça az bir kısmı küçük ölçekli de olsa bir pazar başarısı elde edebilmiş, ancak şu ana kadar hiçbiri Bitcoin'in büyüklüğüne yaklaşamamıştır. Bu yazı hazırlandığı tarihte CoinMarketCap verilerine göre 817 farklı kripto para birimi bulunmaktadır. Kripto para piyasalarındaki güncel pazar verilerine ve değerlerine ulaşmak için **https://coinmarketcap.com** adresini kullanabilirsiniz.

Genel olarak bakıldığında alt-coinler Bitcoin tarafından sunulmayan/sunulamayan özelliklerle pazarda yer almaya çalışmaktadır, bunlardan bazıları:

- Mutabakat yaklaşımı
- Kripto para üretimi sürecindeki kullanılan problem
- Kullanılan özetleme algoritması
- Platform kapsamındaki diğer hizmet yeteneklerinin geliştirilmesi
- Blok oluşturma frekansı
- Blok büyüklüğü (örneğin Bitcoin yapısında blok büyüklüğü 1MB ile sınırlandırılmıştır, bundan dolayı bir blok içerisinde yer alabilecek işlem sayısı sınırlıdır)
- Yaratılabilecek kripto para miktarı

Bir örnek vermek gerekirse popüler bir alt-coin olan Litecoin (LTC) kapsamında işlem doğrulamaların daha hızlı yapılabilmesi için blok üretim frekansı 2,5 dakikadır. Bu değer, Blockchain Platformları bölümünde Bitcoin başlığında daha detaylı alacağımız gibi, Bitcoin için ortalama 10 dakika olarak belirlenmiştir. Litecoin ayrıca özel donanım tabanlı kripto para üretimini engelleyip daha dağınık bir madencilik ağına sahip olmak amacı ile geliştirilmiştir. Bunların yanı sıra dolaşımdaki toplam Litecon üst sınırı 84 milyon olacak şekilde tasarlanmıştır. Bitcoin platformunda bu rakam 21 milyon Bitcoin'dir.

Güncel bir alt-coin denemesi olan Zcash, Bitcoin'den farklı olarak işlemleri bir açık Blockchain ağı üzerinde yönetiyor olsa da işlem kayıtları üzerindeki gönderici, alıcı ve tutar bilgilerini gizli olarak tutmaktadır.

Alt-coin'ler genel olarak türedikleri yapılardaki teknik problemlere alternatif getirme iddiasında olsalar da farklı denemeler de yapmaktadırlar. Örneğin 2013 sonunda ortaya çıkan Dogecoin, ilk tasarımında Bitcoin'den farklı olarak blok üretimi

kapsamında rastlantısal bir teşvik ödül yapısı getirmiştir ama bu yapı daha sonra sistemde bulunan bir açık dolayısı ile iptal edilmiştir.

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

Her ne kadar kripto para birimlerin sıfır değerinden binlerce dolara yükselmesi bireysel tasarruflar ve kısa yoldan zengin olma hedefi ile cazip bir yatırım aracı yanılsaması oluştursa da kripto para birimleri merkezi bir denetimden uzak, düzenlemelere tabi olmayan ve spekülatif işlemlerin çok hızlı gerçekleşebileceği oldukça riskli yatırım alanlarıdır. Bu sebeple bu dünyaya bir yatırım alanı olarak değil daha çok teknolojik altyapısının sunduğu imkanlar çerçevesinde yaklaşmak gerekmektedir.

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

1.5. 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 farklıdır.

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

Bir önceki bölümde temel olarak Blockchain türleri ve kısmen aktif kısmen farazi bazı örnekler 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.

Dijital Kimlik

İnternet ve onu takip eden mobil teknolojiler devrimi ile birlikte hayatımıza giren ve hızla yayılan dijital servisler fiziksel dünyadaki kimlik kavramının bir dijital kopyasına olan ihtiyacı ortaya çıkarmıştır. Bu konuda kullanılan çözümler temel olarak merkezi bir yapı içerisinde kimlik bilgilerinin saklanması ve dış servislere kontrollü bir şekilde sunulması şeklinde gerçekleşmektedir. Ancak bu yaklaşım temel olarak bu yeni dijital dünyanın ihtiyaçlarını karşılamamaktadır.

Blockchain ve akıllı sözleşme tabanlı bir altyapı ile merkezi olmayan, kimlik sahibinin onayına bağlı olarak herkese, kısmen veya bütünüyle açık, kullanım ve ihtiyaçlara göre farklı davranışlar sergileyebilen (eğlence servisle için ayrı bir alt-kimlik, kamusal işlemler için ayrı bir alt-kimlik gibi), bu farklı davranışları tanımlı akıllı kontrol akışları kapsamında otomatik olarak gerçekleştirebilen (yaş kontrolü için tüm kimlik bilgileri yerine sadece istek yapan servise doğrulama sağlayan bir akıllı sözleşme gibi) bir yeni nesil dijital kimlik yapısı oluşturulabilir. Bu konu ile alakalı olarak BKM tarafından yayınlanan David Birch'ün "Para: Yeni Kimlik" isimli kitabını okumanızı şiddetle tavsiye ediyoruz.

Müşteri Tanıma (Know Your Customer - KYC)

Başta finansal kurumları olmak üzere pek çok işletme yasal olarak müşteri kazanımı ve kayıt süreçleri kapsamında müşterilerine ait bilgileri toplamak zorundadırlar. Bu bilgiler genellikle temel kimlik bilgilerinin ötesinde müşteriye ait davranışsal ve tercihsel bilgiler olabilir. Müşterinin bilgileri farklı bir kurum-

da 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.

Müşteri bilgilerinin tutulduğu bir Blockchain ağı üzerinde bir müşteriye ait bilgilere ihtiyaç duyulduğu durumlarda, müşteri onayı ile birlikte, bilgiyi talep eden ilgili kuruma aktarılması sağlanabilir. Bu yapı sayesinde müşteri bilgilerinde oluşabilecek den 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 2016 yılında yaklaşık 600 milyar dolar büyüklüğüne ulaşmış 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 yüksek gecikme ve maliyetlere neden olmaktadır. 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 olmaktadır.

Blockchain yaklaşımının ortaya çıkması ile birlikte firmalar sermaye ihtiyaçlarını karşılamak için herhangi bir aracı kuruma ihtiyaç duymadıkları, kendi yönettikleri yeni bir alternatif modele sahip olmuşlardır. Bu modelde temel olarak firmanın kendi tanımladığı bir alt-coin (Bitcoin ilk kripto para birimi olarak kabul edilir, bunun dışında oluşan yeni coinler alt-coin olarak gruplandırılır, kripto para birimleri ile alakalı bölümde detaylarına değineceğiz) yaratıp bunun satışı üzerinden sermaye ihtiyacını karşılayabilir. Örneğin Ethereum platformu, canlı yayına geçmeden önce 42 günlük bir süreç boyunca tüm yatırımcılara açık bir şekilde, henüz karşılığı olmayan bir kripto para birimi olan Ether (ETH) satışı gerçekleştirmiştir. Bu model üzerinde ayrıca Akıllı Sözleşme yapısı (gerçekleşen yatırımların ancak belirli bir sürede belirli bir toplam değere ulaşılınca geçerli kabul edilmesi, yatırımın sonucunda dijital bir ödülün yatırımcıya iletilmesi gibi) getirilerek bir aracı kuruma ihtiyaç olmadan bir kitle fonlama çözümü oluşturmak mümkündür.

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 mümkündür. 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 üzerinden takip ederek gerçekten hedefine uygun bir şekilde kullanıldığını denetleyebilmesi ve bu şekilde kaybolan güven duygusu tekrardan tesis edilmesi sağlanabilir. Ayrıca ilgili mevzuat kapsamında yapılan kontroller çok daha etkili ve verimli bir şekilde gerçekleştirilebilir.

Mal ve Kaza Sigortası Tazmin Süreci

Mal ve kaza sigortası sektör içerisinde yaşam ve sağlık sigortaları sonrasındaki en büyük bölümdür. Beklentilere göre 2018 yılında bu tür sigortaların tahmini toplam büyüklüğü yaklaşık 895 milyar dolar olacaktır. Şu anda mevcut tazmin süreci ince-

lendiğinde özellikle aracılardan kaynaklanan bir yüksek gecikme ve maliyet, taraflar arasında bilgi paylaşım yapılarının yetersizliği nedeni ile dolandırıcılık riski ve tekrarlanan işlemler, bütün bunları 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 uygulamaları ile bu süreç otomatikleştirilebilir), aracı ihtiyacı ortadan kaldırılıp bunların getirdiği gecikme ve maliyet süreçten çıkarılabilir, güvenilir veri kaynaklarına yapılacak entegrasyonla birlikte destek verilerinin oluşturulması en düşük insan kontrolü içeren bir hale getirilebilir, çoğu durum için akıllı sözleşmelerin ödeme işlemine kadar süreci otomatik olarak yönetip tamamlaması sağlanabilir.

Sendikasyon Kredisi

Sendikasyon kredi pazarı 2015 yılı rakamlarına göre yaklaşık 4,7 trilyon dolar büyüklüğündedir. Şu anda mevcut ilgili akış incelendiğinde 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 bilgilerin katılımcı kurumlar tarafından daha açık ve efektif bir şekilde değerlendirilebilir, katılımcı kurumlara ait finansal ve risk to-

lerans bilgilerin Blockchain üzerinde tutulması ile seçim işlemi akıllı bir sözleşme kapsamında otomatikleştirilebilir, akıllı sözleşmelerle aracı kurum ihtiyaçları azaltılıp maliyet ve gecikmeler en düşük hale getirilebilir, 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 yapısı ile birlikte denetleyicilerin ihtiyaç duydukları bilgilere firma kaynaklarını (çalışan gibi) engellemeden erişebilmesi, kurulacak bir entegrasyon yapısı ile denetim yazılımları ile otomatikleştirilmiş denetlemelerin gerçekleştirilmesi, elle yapılan işlemlerin kaldırılması ile birlikte potansiyel hata alanlarının daraltılması sağlanabilir.

Vekaleten Oy Kullanma

Vekaleten oy kullanma yapısı ile birlikte uzak yatırımcılar yıllık hissedar toplantılarında tartışılan konular üzerinde katılım sağlayamasalar bile oy kullanabilmektedir. Bu süreç kapsamında uzak yatırımcıların bilinçli karar vermeleri sağlamak için ge-

rekli bilgilerin sağlanması ilgili firmaların sorumluluğundadır. Bu yapıda gerekli bilgilerin doğru bir şekilde iletimi, yatırımcıların kolay bir şekilde oy kullanma sürecine katılımı, katılım sürecinin şeffaflığı gibi alanlarda çeşitli sıkıntılar gözlemlenmektedir.

Burada oluşturulacak Blockchain ve Akıllı Sözleşme tabanlı yeni bir akış ile birlikte ilgili firmanın hisse yapısını da içeren yatırım kayıtları bir Blockchain üzerinde tutulurken, bu yapı üzerinde çalışan akıllı sözleşmeler tüm yatırımcılara ilgili bilgilerin gönderiminin yönetilmesini, oylamanın farklı kanallardan gerçekleşse bile tek bir ara entegrasyon katmanı ile birlikte Blockchain üzerinde tutulmasını, sonuçların gerçek zamanlı olarak ilgili kurum ve/veya yatırımcılar ile paylaşılmasını 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 konsantre oldukları, zincir boyunca her adımda karışık entegrasyon ve bilgilendirme süreçlerinin yer aldığı, bunlardan dolayı süre, maliyet ve firma verimliliği açısından çeşitli sıkıntılar içeren, kontrolü oldukça zor olan 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 azaltılabilir. 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.

Tapu Kayıt Sistemleri

2010 yılındaki Haiti depreminin ardından yerel hükümetin karşılaştığı problemlerden bir tanesi yıkılan kamu binaları ile birlikte tapu sicil kayıtlarının da tahrip olmasıydı. Haiti gibi her şeyin fiziksel evraklar üzerinden takip edildiği bir sistemde bu durum günümüze kadar devam eden bir sahiplik karmaşasına neden olmuştur.

Günümüzde "e-devlet" yaklaşımının popülerleşmesi ile birlikte bu tarz sistemlerde kayıtların dijital ortama aktarılması ve bu tarz durumlardan minimum hasar ile süreklilik sağlanma-

sı gerçekleştirilmiş olsa bile dijital kayıtlar üzerinde sahtecilik ve onay dışı değişiklik oldukça sık karşılaşılan bir durumdur. Bu noktada Blockchain tabanlı bir çözüm ile birlikte kayıtların dijital parmak izleri Blockchain üzerinde tutularak bu tarz işlemlerin önüne geçilebilir. Ayrıca akıllı sözleşme yapılarınında devreye girmesi ise sahiplik yapısı ve alım-satım gibi sahiplik devri yapılan işlemler çok daha kolay, hızlı ve güvenli bir şekilde gerçekleştirebilir (alıcı ve satıcı arasında gerçekleştirilecek bir akıllı sözleşme ve bu akıllı sözleşmenin içerisindeki akışı kontrol eden kredi veren banka ve sahiplik devri yapan tapu müdürlüğü servisleri gibi).

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 engelleme ve kamusal süreçleri şeffaflaştırmaktadır.

Askeri Emir Komuta Zincirleri

Askeri yapılarda bu gün 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.

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.

Buzdağının Görünmeyen Kısmı Hatta Antarktika Kıtası

Bu bölümde Blockchain teknolojisine yönelik bazı temel potansiyel uygulama alanlarına değinmeye çalıştık, ancak bunlar kelimenin tam anlamı ile sadece buzdağının görünen kısmıdır. Hatta bu kısma ait alt başlıkta belirttiğimiz gibi karşımızda keşfedilmeyi bekleyen, el değmemiş, üstü karlar ve buzlar ile kaplı devasa bir kıta var.

Anlam ve değer içeren herhangi bir varlığın, herhangi bir aracıya ihtiyaç duymadan, güvenli ve otomatik bir şekilde transferinin ve kullanımının sağlanması ile birlikte bugüne kadar olamayacağı düşünülen çok farklı iş modelleri üzerinde dünyanın pek çok noktasında çalışmalar yapılmaktadır.

Günümüzün örnek gösterilen yakın dönem yıkıcı (disruptive) girişimleri dahi Blockchain dalgasının etkisi altındadır,

Ethereum platformunun kurucusu olan Vitalek Buterin'in belirttiği gibi "Çoğu teknoloji, işleri otomatikleştirip çalışanları uzaklaştırırken, Blockchain çözümleri merkezi yapıları ortadan kaldırmaktadır. Uber taksi şoförlerinin işini tehdit edebilir ancak Blockchain Uber'in varlığına ne kadar ihtiyaç kaldığını yeniden düşünmemizi mümkün kılmaktadır."

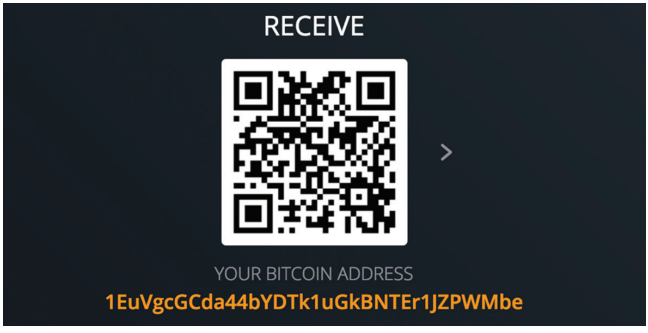
1.6. Blockchain Platformları

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 birisi ama "Amerika'yı yeniden keşfetmeye gerek yok" yaklaşımını takip etmek daha mantıklı olacaktır zira şu anda açık kaynak kodları ile kullanılabilecek hazır durumda çeşitli Blockchain platformları bulunuyor. Bakalım bu platformlar hangileri ve hangi amaçlara hizmet ediyorlar.

Bitcoin

Blockchain kavramının hayatımıza girmesinde en büyük role sahip Blockchain platformu şüphesiz ki 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 yada 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 adresi edinilebilir.



EXODUS isimli birden fazla platformu destekleyen dijital cüzdan uygulamasının Bitcoin için oluşturduğu adres ve bu adrese ait QR kodu.

Oluşturulan her bir cüzdan ile ilişkili olarak sahibi için bir adet açık-özel anahtar çifti oluşturulur (anahtar çiftleri hakkında detaylı bilgi için Kriptoloji bölümünü okuyunuz), açık anahtar ağ içerisindeki diğer herkes ile paylaşılırken gizli anahtar özeldir ve saklı tutulması gerekmektedir.

Bir kullanıcı (Ahmet) başka bir kullanıcıya (Serkan) Bitcoin göndermek istediğinde; gönderim kapsamında kullanılacak Ahmet'in kontrol ettiği Bitcoin hesapları ve Serkan'ın paylaştığı açık anahtar ile oluşturulmuş Bitcoin adresini içerecek şekilde, Ahmet'in gizli anahtarı ile imzalanmış bir işlem oluşturulur.

Böyle bir işlemin gerçekten Ahmet tarafından oluşturulduğu, Ahmet'in 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 dolayı, hangi hesapta ne kadar Bitcoin var sorusunun cevabına ulaşılabilir ve bu şekilde Ahmet'in kontrol ettiği hesaplarda olmayan bir para ile işlem yapmasına izin verilmez. Yine aynı mantık ile Ahmet'in aynı parayı birden fazla kez harcanmasının önüne geçilmiş olunur. Sistemde bulunan ve mutabakat yapan tüm makineler Ahmet'in işlemlerini kontrol eder ve eğer bu sistemdeki kurallara uymayan bir işlem ise buna izin verilmez. Burada mutabakatı yapan sistemdeki tüm mutabakat noktalarıdır, merkezi bir kontrol yoktur ve işlemin onaylanması için sistemde bulunan tüm mutabakat yapısının yüzde 50'sinden fazlasının bu işleme onay vermesi gerekmektedir.

Peki, Bitcoin ağında işlem yapılan kripto para birimi Bitcoin nasıl üretilir?

Bitcoin protokolü kapsamında sistemde yeni Bitcoin yaratılmasının tek yolu Blockchain üzerinde yeni blok üretilmesidir. Bir bloğun üretilebilmesi için sistem üzerinde zorluk seviyesi sisteme dahil olan mutabakat noktalarının sayısına ve bu bilgisayarların işlem gücüne bağlı olarak değişen bir matematiksel problemin çözüm kümesini bulmak gerekmektedir. Her bir blok üretiminde bloğu üreten noktaya sistem tarafından yine miktarı belirli kriterlere bağlı değerde Bitcoin verilmektedir. Bu yaklaşım **teşvik** (**incentive**) yaklaşımı olarak adlandırılmaktadır.

Bitcoin üretmenin zorluğu ve miktarı neden değişkendir?

Gerçek kimliğini bilmediğimiz Satoshi Nakamoto sistemi ilk kez tasarlarken zaman içinde kullanıcı sayısının artabileceğini ve üretilen Bitcoin değerinin yükseleceğini öngörmüştür. Bu sebeple sistemde enflasyona izin vermemek için ortalama her 10 dakikada bir Blok üretilmesi kuralını belirlemiştir.

Sistem, faaliyete geçtiği 3 Ocak 2009'da Blok başına 50 Bitcoin ödül verirken bu değerin her 210.000 Blok üretildiğinde yarılanması öngörülmüştür ve bu süre yaklaşık dört yıla tekabül etmektedir. 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. Bu şekilde en fazla 21 milyon bitcoin üretilebilecek ve sonrasında sistem kapsamında yeni Bitcoin yaratımı yapılamayacaktır.

Nakamoto'nun yaptığı tasarım aynı zamanda sistemde Bitcoin üretmek için matematik problemini çözmeye çalışan nokta ve işlem gücü arttıkça problemi daha zor hale getirerek 10 dakikalık Blok üretim sürecinin de korunmasını sağlamaktadır.

Bu süre içinde birden fazla çözüm bulan noktalar olmasında ne gibi süreçlerin takip edildiğine dair detaylı bilgileri Blockchain hakkında teknik değerlendirme yapılan bölümde bulabilirsiniz.

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

Bitcoin Blockchain ağının yapısı temel olarak; sınırlı ve kontrollü üretilebilen bir kripto para biriminin, kopyalanmadan transfer akışını sağlamaktır. Ancak sistem protokol olarak sahip olduğu betik dil yetenekleri (yazılımsal imkanlar) ile birlikte üzerinde çeşitli iş akışlarında zaman damgasına sahip kılavuz veri taşıyabilen bir yapı olarak da kullanılmaktadır. Blockchain uygulama örneklerinde detaylı olarak bahsedilen Everledger, Bitcoin ağını bu şekilde kullanan ve amacı kripto para transferi olmayan bir uygulamadır. Bitcoin Blockchain kodu açık kaynaklı olup indirilebilir ve yeni alt-coin türleri üretmek veya farklı amaçlara hizmet etmek için değiştirilebilir.

Ethereum

Bitcoin yapısı kripto para yaratımı ve bu kripto para ile ilgili transfer akışlarının yönetimi için yeterli yetkinliklere sahip olsa da yetenekleri farklı alanlar için kullanılmasını sınırlandırmaktadır. Bu kısıtların ötesine geçebilmek için Bitcoin üzerine özel protokollerin hazırlanması gibi yöntemler takip edilmiş ama tüm bu alternatiflerin sadece kendi özel durumlarına çözüm getirip, yüksek maliyet doğurmakta olduğu gözlemlenmiştir. Bu sebeple Ethereum Blockchain platformu bir alternatif olarak doğmuştur.

Ethereum, uygulama geliştiricilerin merkezi olmayan uygulamaları geliştirmesi ve devreye sokmasına olanak tanıyan yenilikçi bir Blockchain teknolojisine dayanan bir platformudur. Ethereum'un yaratıcıları, Bitcoin'i "1. nesil Blockchain", Ethereum'u ise "2. nesil Blockchain" olarak tanımlamaktadırlar.

Ethereum Blockchain 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) ile yazılmış herhangi bir uygulamanın Ethereum Blockchain 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.

Ethereum platformu, Ether (ETH) adı altında kendine ait bir kripto-para birimine sahiptir. Ether, Ethereum platformu kapsamındaki işlemlerin/uygulamaların çalıştırılmasında kullanılmaktadır ve bu yapı bir motorun çalışması için benzin gerekmesi metaforu ile ilişkilendirilebilir.

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

Ethereum üzerinde geliştirilen ve geliştirilmeye devam eden oldukça fazla proje bulunmaktadır. Örneğin ING tarafından Société Générale ile birlikte test edilen bir çözüm; petrol ticare-

ti akışının Ethereum tabanlı bir Blockchain platformu üzerinde yürütülmesini amaçlamaktadır. Deneme kapsamında gerçekleştirilen örnek işlemlerde emtia ticareti için gereken maliyet ve özellikle zamanda ciddi anlamda düşüşler olduğu gözlemlenmiştir. Ethereum Enterprise Alliance ile birlikte özellikle iş dünyasındaki uygulamaların çeşitlenmesi ve artması beklenmektedir.

Öte yandan Ethereum, kitabımızın Zorluklar ve Riskler bölümünde detaylı şekilde ele alınan Blockchain dünyasındaki çatallaşma kavramının üst üste iki kere yaşandığı bir platform olmuş ve 2016 yılında Blockchain camiasının çok önemli tecrübeler kazanmasına vesile olmuştur.

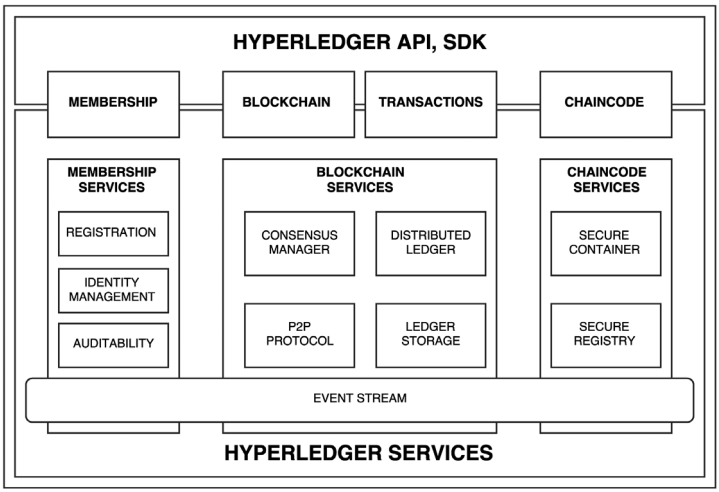
HyperLedger

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 katmanıdır (API: Application Programming Interface – Uygulama Programlama Arayüzü, SDK: Software Development Kit – Yazılım Geliştirme Kiti).

Hyperledger servis katmanı üç ana mantıksal kategori içerisinde değerlendirilmektedir, bunlar: üyelik servisleri, Blockchain servisler ve Chaincode servisleridir. Üyelik servisleri kimlik, gizlilik gibi konularda hizmet verirken Blockchain servisleri sahip olduğu P2P protokolu ile birlikte içerdiği

blockchain ve mutabakat yapısını yönetmektedir. Chaincode servisleri, Hyperledger mimarisi içerisinde akıllı sözleşmelerin yönetim ve işletimini sağlamaktadır. 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 bu gün pek çok Blockchain projesinde kullanılmaktadır. Özel bir röportaj ile sizlere sunduğumuz Bankalararası Kart Merkezi'nin gerçekleştirdiği kavram kanıtlama çalışması olan özel BBN Blockchain projesinde de Hyperledger platformu kullanılmıştır.



Hyperledger kapsamındaki projelerin en bilinenlerinden olan **Fabric** projesi IBM ve Digital Asset tarafından Hyperledger bünyesinde düzenlenen ilk Hackathon kapsamında önerilip

hayat geçmiştir. 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.

Başka bir proje olan **Iroha** ise aslen bir Blockchain projesi değildir, bir dağıtık kayıt defteri projesidir. Bu iki kavram çoğunlukla birbirinin yerine kullanılsa da aralarında farklılıklar bulunmaktadır. Dağıtık kayıt defteri yaklaşımında bloklar yerine zaman damgalı sıralı işlemler bulunmakta, mutabakat yapısı bu sıralı seri üzerinde değişiklik yapılmasını engellemek için kullanılmaktadır. Ayrıca dağıtık kayıt defteri yapılarında tüm düğümlerin eşlenik olmasına gerek duyulmamaktadır. Yapısal olarak bütün blockchain yapıları aynı zamanda bir dağıtık kayıt defteridir, ama bu durumun tersi doğru değildir. Iroha projesinin geniş bir kullanım ağına erişebilmesi için mobil platformlarda (iOS ve Android) ve internet tarayıcılarında kullanımını sağlayacak özel kütüphaneler bulunmaktadır.

Henüz kuluçka döneminde olan **Burrow** projesi ise Hyperledger bünyesinden 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.

Ripple

Ripple, temel olarak gerçek zamanlı bir uluslararası para gönderim/ödeme platformudur. Uluslararası ödeme akışlarında günümüzde kullanılan Swift gibi aracı kurumların gereksinim-

leri ve bunun getirdiği yavaşlık, yüksek maliyet gibi yan etkileri ortadan kaldırmak amacı ile Blockhain tabanlı bir teknoloji kullanılmaktadır.

Ripple, Blockchain platformundan diğer Blockchain platformlarında gördüğümüz "proof-of-work" yada "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 yada Blockchain yapısına ihtiyaç duymamaktadır. Ripple protokolü, üzerinden 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 (yolcu mil puanları gibi) işlem yapılabilmektedir.

Ripple platformu üzerinde kullanıcılar (Ripple entegrasyonu olan finansal kurumlar) güvendikleri kullanıcıları ve bu güven yapısı içerisindeki işlem bilgileri (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 bu bunun için kendi kripto-para birimi üzerinden dönüşüm gerçekleştirir). Bu güvenli yol kurulduktan sonra tüm işlemler atomik yani işlem bütünlüğünün bozulmadığı (işlemlerin ya hepsi gerçekleşir yada hiçbiri 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 işlemlerin 8 saniye içerisinde gerçekleştiği gözlemlenmiştir.

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 ile kurum sistemlerinde değişiklik yapmadan entegrasyonu sağlamaktadır.

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 bir blockchain çözümü değildir, bir dağıtık kayıt defteri (distributed ledger) projesidir. Diğer yaklaşımlardan farklı olarak işletmeler arasında yasal sözleşmeleri kaydetmek, yönetmek ve otomatikleştirmek gibi özel bir iş alanı için 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 geri 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 mutabak 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 yaklaşım açısından 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 kullanılabileceği düşünülmektedir.

Tendermint

Temel olarak Tendermint, bir uygulamayı birçok makinede güvenli ve tutarlı bir şekilde çoğaltmak için kullanılan bir yazılımdır. Ortaya çıkmasındaki temel amaç Bitcoin mutabakat yapısında kullanılan Proof of Work yaklaşımına kıyasla daha efektif ve güvenli bir mutabakat yapısını ortaya koyabilmektir.

Tendermint platformu iki ana parçadan oluşmaktadır, bunlar temelde bulunan blockchain mutabakat moturu (Tendermint Core) ve bunun üzerinde çalışan genel uygulama ara yüzü'dür (ABCI – Application BlockChain Interface). Mutabakat moturu ağ üzerinde bulunan tüm makinelerde aynı işlemlerin aynı sırada kaydedilmesini sağlarken, uygulama ara yüzü bu işlemlerin herhangi bir programlama dili ile işlenmesine olanak sağlamaktadır.

Tendermint yapısında bulunan mutabakat motoru yapısı itibari ile diğer platformlar tarafından kullanılabilecek şekilde tasarlanmıştır. Bu konuda örnek oluşturması amacı ile Tendermint geliştiricileri Ethereum platformuna ait olan EVM (Ethereum Virtual Machine) yapısını alıp Tendermint uygulama arayüzü üzerinde çalıştırmayı başarmışlar ve bu çözümü Ethermint olarak adlandırmışlardır.

Tendermint'in ortaya çıkış amacının Bitcoin yapısına göre daha efektif bir mutabakat yaklaşımı yaratmak olduğunu belirtmiştik, yapılan denemelerde ortalama 1 saniyelik blok üretim hızına eriştiği ve saniyede yaklaşık 10.000 işlem gerçekleştirebildiği gözlemlenmiştir.

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.

1.7. Blockchain Uygulama Örnekleri

Mevcut Blockchain platformlarını kullanarak farklı servisler sunan çözümlerin sayısı bu gün binlere ulaşmıştır. Sadece kripto para birimi olarak 800'e yakın farklı tür bulunurken daha önce Blockchain Uygulama Alanları bölümünde ele aldığımız konularda faaliyet ve çözüm sunan pek çok girişim bulunmaktadır.

Özellikle son yıllarda Blockchain platformlarının yenilikçi yapısı, bu konuda deneyimin ve insan kaynağının kısıtlı olması sebebiyle bu alanda faaliyet gösteren girişimler yatırımcıların ilgisini çekmekte ve çok ciddi yatırımlar alabilmektedir. Yapılan tahminlere göre sadece bankaların 2019 yılına kadar bu teknolojiye 400 milyon dolar yatırım yapması beklenmektedir.

Bu bölümde farklı Blockchain platformlarını kullanan birkaç uygulama örneğini sizler ile paylaşmak istiyoruz.

Everledger

2015 yılında Londra merkezli olarak kurulan bir girişim olan Everledger, elmas ile ilgili bilgileri bir Blockchain ağı üzerinde tutarak değerli taş sahipleri, sigorta firmaları, kanun uygulayıcı

birimler gibi konu ile ilgili tarafların taşlar üzerinde sahiplik ve işlem geçmişini doğrulama işlemlerini geleneksel fiziksel sertifikalara kıyasla güvenli ve hızlı bir şekilde yapmasını 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 oluşturulmaktadır. Bu parmak izi bilgisi belirtilen bilgilerin kendisini değil, belirtilen bilgi kümesini üzerinden üretilen özel ve tekil bir özet değerdir. Bu bilgi Bitcoin Blockchain ağında bir işlemin parçası olarak, Bitcoin platformunun betik dil yetenekleri kullanılarak, saklanabilmektedir. İhtiyaç duyulması halinde ilgili taşa ait dijital parmak izi bilgisi tekrardan oluşturulup Bitcoin Blockchain ağı üzerindeki işlemler kapsamında sorgulama yapılmaktadır.

Everledger şu ana kadar 1 milyondan fazla elmas için Bitcoin Blockchain yapısı üzerine bilgi ekleme işlemi gerçekleştirmiştir. Bu tarz işlemler için Bitcoin'in yapısında bulunan özel bir komut kullanılır (OP_RETURN olarak tanımlanan bu komut ile birlikte 80 byte'lık bir veri kümesi işlem içerisinde tutulabilir). Bu komut ile gerçekleşen işlem çıktıları geçersiz olarak nitelenmektedir, ancak işlemin kendisi geçerli olduğu için Blockchain içerisinde yer alması için düşük değerde bir işlem ücreti ödenmesi gerekmektedir, bu şekilde Everledger değişmeyeceği garantilenmiş bir işlem kaydına sahip olmaktadır.

Factom

Temelleri 2014 yılında atılan Factom, herhangi bir verinin değiştirilemeyen bir şekilde tutulması sağlayan bir kayıt tutma

servisi sağlayıcısıdır. Bu veriler tıbbi kayıtlardan tapu kayıtlarına kadar farklılık gösterebilmektedir.

Factom öncelikli olarak bir veri katmanı oluşturarak kendisine ileten verileri bloklar içine yerleştirir ve blok içerisindeki sıralarını sabitler. Her 10 dakikada bir o zaman aralığında toplanan veri kümesine ait bir özetleme (hash) değeri oluşturulur ve oluşturulan bu değer Bitcoin Blockchain ağı üzerine yazılır. Bitcoin Blockchain ağı üzerine kaydedilen verilerin değiştirilemez yapısından dolayı Factom kendisine emanet edilen kayıt değiştirilmediği sürece bunun orijinalliğini garanti altına almış olur.

Factom ilk başta oluşturduğu özetleme değerlerini Bitcoin Blockchain üzerinde tutuyor olsa da şu anda çoklu Blockchain Platform desteğine sahiptir, oluşturduğu özetleme değerleri Ethereum gibi farklı açık (public) Blockchain platformlarında tutabildiği gibi özel (private) Blockchain yapılarında da tutabilmektedir.

Factom şu ana 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 dolar / 35 TL ve altındaki ödemeleri ifade etmektedir. Nano ödemeler ise bu rakamın çok daha altındaki cent/kuruş seviyesindeki ödemeleri tanımlamak için kullanılmaktadır. Ancak şu anda kullanılan ödeme sistemlerindeki işlem ücretlerinin yapısından dolayı (ücretin ödeme miktarından daha büyük olması) nano

ödemelerin gerçekleştirilmesini pratikte anlamsız hale getirmektedir.

2014 yılında Berlin'de kurulan bir girişim olan SatoshiPay bu soruna Bitcoin Blockchain ağı üzerinde geliştirdiği bir ödeme kanalı ile çözüm sunmaktadır. Bu kanal üzerinde basit bir akıllı sözleşme yapısı ile yönetilmektedir. Bu şekilde kullanıcıya gerekirse anlık olarak bir Bitcoin cüzdanı oluşturulmakta, bu cüzdan üzerinden yapılan ödeme işlemleri kullanıcının oturum süresi boyunca toplanarak sonrasında son ödeme işlemi olarak Bitcoin Blockchain ağına yansıtılmaktadır.

SatoshiPay öncelikli iş alanı olarak web tabanlı içerikler için ödeme çözümü olma üzerine yoğunlaşmış olsa da hedefini web üzerindeki dijital içerikler için bir ödeme standardı olmak olarak belirtmiştir.

Ujo Music

Günümüzde, müzik dağıtım kanalları yapısında geçmişten gelen yapıların içinde bulunduğumuz dijital dünyaya uyumsuzluğundan kaynaklanan çeşitli sorunlar gözlemlenmektedir:

- Yapılan ödemeler (%20-%50) gerçek sahiplerine ulaşamaz.
- Bir sanatçıya ait eserin kullanımı takip edilemez.
- Ödemelerin hak sahiplerine dağıtımında şeffaflık yoktur ve ücretlendirme gibi konuların eser sahibi dışındaki kişiler tarafından yönetilmesi söz konusudur.
- Hak sahiplerinin ödemeleri iki seneye varan çok uzun vadeler ile alması söz konusu olabilmektedir.

Ujo Music bu konuda yaptıkları bir "deney" çalışmasında Ethereum Blockchain ağı üzerinde geliştirdiği 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 sağlamıştır.

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

OpenBazaar

Günümüzde elektronik ticaret akışı temel olarak Amazon, eBay gibi merkezi, internet tabanlı platformlar üzerinde gerçekleştirilmektedir. Bu platformlar sağladıkları hizmet kapsamında belirli ödeme şekilleri, ödeme işlemlerinin maliyetlerinin yansıtılması, kişisel bilgilerin paylaşımı, sınırlı ticari kategori kısıtlamaları 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, tarafların belirlediği kısıtlamalar dışında bir kısıtlama bulunmamaktadır.

OpenBazaar bu yapıda taraflar arasındaki "güven" sorununun aşılması amacı ile Bitcoin Blockchain yapısını 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 ürün aldıktan sonra kendi imzası ile sözleşmeyi onaylamaması durumunda (üç kişiden en az ikisinin onay vermesi durumu gerçekleştiğinden dolayı) gönderimi yapılan Bitcoin satıcı hesabına aktarılmış olur. Bu yapıda bir problem olması durumunda denetci devreye girer, gerekirse sözleşmenin onayı için kendi imzası ile onaylama akışına dahil olur.

Maker

Kripto para birimleri belirli seviyede bilinirlik ve popülerlik kazanmış olsalar da yaygınlaşma konusuna çeşitli sıkıntılar yaşamaktadır. Bu durumun en büyük nedenlerinden birisi fiyat değişkenliğidir. En popüler kripto para birimleri olan Bitcoin (BTC) yada Ether (ETH) bile şu andaki yapısında bireylerin ve şirketlerin uzun vadeli faaliyet planlamasına izin vermek için aşırı değişken ve riskli bir durum sergilemektedirler.

Maker platformu bu durum karşısında Dai adını verdikleri, ortaya çıkan piyasa şartlarına otomatik tepki vererek dünya genelindeki para birimleri karşısındaki değerini dengede tutabilen bir kripto para birimi önermektedir. Bu para birimi, Ethereum Blockchain platformu üzerinde çalışan bir Dai Kre-

di Sistemi tarafından yönetilmektedir. Dai Kredi Sistemi, Dai kripto para biriminin her zaman Ethereum tabanlı diğer dijital varlıklardan oluşan bir teminat portföyü tarafından yeterli seviyede desteklenmesini sağlamaktadır. Bağımsız bir geri bildirim mekanizması ise sürekli olarak Dai borçlanma ve sahipliği teşviklerini güncelleyerek arz-talep dengesini sağlamaktadır. Teminat portföyünün riski Maker (MKR) adlı ayrı bir kripto-para birimi sahipleri tarafından yönetilmektedir. Maker kripto-para biriminin değeri doğrudan risk yönetiminin performansıyla bağlantılıdır, bundan dolayı Maker sahiplerine Dai ödeme yükümlülüğünün ve fiyat istikrarının sorumlu düzenleyicileri olarak davranmak için doğrudan finansal teşvik sağlamaktadır.

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 yüzlerce hatta binlerce farklı uygulama ile karşılaşmanız mümkündür. Bu örneklerden birisi de ülkemizde Bankalararası Kart Merkezi tarafından gerçekleştirilen BBN projesi olmuştur. Şimdi bu projeye bir röportaj eşliğinde yakından bakacağız.

1.8. 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?

Celal Cündoğlu: 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?

Celal Cündoğlu: 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?

Celal Cündoğlu: 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 çalışanlarımız 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?

Celal Cündoğlu: 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 veritabanı yapısı olan ve üzerine kurgulanan modellerle anlamlı çözümler geliştirilen Blockchain'in olmazsa olmazı ise işbirliği. Blockchain, 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 imkanı 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?

Celal Cündoğlu: 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 gün-

cellemelerde 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 bir birine paralel olduğunu söyleyebilir miyiz? Blockchain teknolojisi konusundaki küresel beklentilerin karşılığını bulabileceğini düşünüyor musunuz? İnanıyor musunuz?

Celal Cündoğlu: 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.

1.9. Blockchain Uygulamalarında Zorluklar ve Riskler

Blockchain genel çerçevede ilgili kişiler ve kurumlar tarafından yakın zamanda ortaya çıkmış en heyecan verici ve potansiyeli yüksek teknolojilerden birisi olarak kabul edilse de her yeni teknoloji gibi gelişim aşamasında çeşitli riskler, zayıflıklar ve zorluklar içermektedir.

Şifreleme ve Kuantum Bilgisayarlar

Blockchain platformlarını en güçlü kılan özelliklerin başında kriptografi gelmektedir. Bu kapsamında kullanılan şifreleme yaklaşımlar 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) sistemlerden bahsediyoruz. Ancak kauntum bilgisayarlarda 1 ve 0'ın aynı anda geçerli olduğu üçüncü bir durum daha bulunmakta ve bu üçlü veri Qubit adı verilen yapılarda saklanmaktadır. Bu bilgisayarlar geleneksel ikili sistemlere

karşı milyonlarca kat daha güçlü işlem yapabilme kabiliyetine sahiptir ve bu sistemler her ne kadar şu anda sadece özel laboratuvarlarda kullanılıyor olsalar da ilerleyen on yıllar içinde herkesin erişimine sunulabilirler. Elbette öncelikle savunma ve istihbarat alanında kullanılmaları da kaçınılmaz olacaktır. Bu sistemlerin kabul edilebilir sürelerde günümüzün gelişmiş ikili şifreleme yöntemlerini kırması mümkün olabilecektir. Bu Blockchain dünyası için hemen değil ama uzun vadede bir risk oluşturmaktadır.

Özel Anahtarların Saklanması

Özellikle kripto-para çözümlerinde kullanılan açık-özel anahtar yapısındaki özel anahtarın saklanması kullanıcının sorumluluğunda bulunmaktadır. Bu kullanım şeklinde yaşanacak olan bir özel anahtar kaybetme durumunda, son kullanıcının elinde şifrelenmiş işlemlerin sahipliğini doğrulayacak hiçbir bilgi kalmamaktadır. Özel anahtarın başka bir kullanıcının eline geçmesi ise ilişki 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 ve servislerinin sayısı her geçen artmaktadır. Ancak bu yapılar da yanlarında çeşitli güvenlik sorunlarını getirmektedir (2016 yılında gerçekleşen Bitfinex dolandırıcılığında kullanıcıların kripto-para cüzdan kayıtlarına erişilerek 120.000 Bitcoin çalınmıştır).

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 7.000-8.000 işlem gerçekleştirebilmektedir.

Yüksek Yatırım Gereksinimi

Blockchain, 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 (dünyada Blockchain çalışma mekaniklerine ve akışlarına gerektiğinde kod yapısında güncelleme yapabilecek kadar hakim 8.000 kadar geliştirici olduğu tahmin edilmektedir), deneme yanılma süreçlerinin uzunluğu ve öngörülmeyen yazılımsal riskler toplam sahip olma maliyetini yükseltmektedir.

Dijital Dönüşüm Gereksinimi

Blockchain uygulamaları tarafından ortaya koyulan çözümler mevcut sistemler kapsamında ciddi değişiklikleri beraber getirmektedir. Bu dönüşümün yapılabilmesi için şirketler bir dönüşüm stratejisi oluşturmalıdır.

Enerji Tüketimi

Özellikle "proof-of-work" tipi mutabakat yapıları kullanan Blockchain platformları şu andaki yapıları itibari ile ciddi bir enerji tüketimi ve dolaylı olarak karbon ayak izi etkisi doğurmaktadır.

Sınırlı Teşvik

"Poof-of-Work" tipi mutabakat yaklaşımı kullanan açık Blockchain yapılarında blokların üretilmesi için gerçekleştirilen madencilik (mining) işlemi, genel olarak 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 açıklar tespit edildiği takdirde ciddi ekonomik kayıplar yaşanabilmektedir.

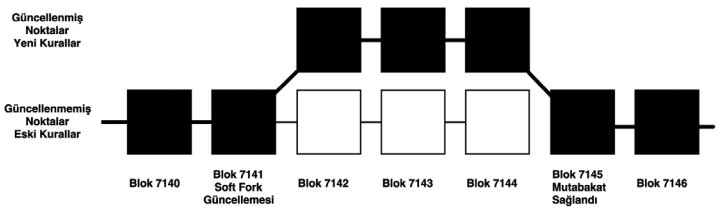
Sahip oldukları açıkların giderilmesi ve yeniliklerin eklenmesi için platformlar üzerinde sürekli güncelleme çalışmaları yürütülmekte, ancak özellikle Açık Blockchain platformlarının merkezi olmayan, demokratik yapısı bu güncellemelerin ger-

çekleştirilmesinde her bir uç noktanın birlikte hareket etmesinde noktasında sıkıntılar yaratabilmektedir. Bu durum çatallaşma (forking) adı verilen bir sonuç doğurabilmektedir.

Çatallaşma (Fork)

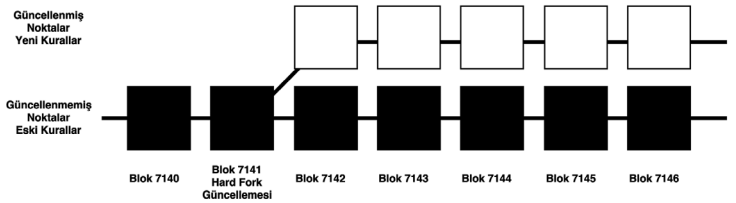
Bir Blockchain ağında tüm katılımcılar ağın kendisine bir yazılım kullanarak ağa dahil olurlar. Bu yazılımlar sürekli olarak sistemi geliştirenler tarafından güncellenir. Bu güncellemeler genellikle ağın yeteneklerini ve imkanlarını geliştirmeye ve performansını artırmaya yönelik gerçekleşir.

Blockchain ağındaki her bir kullanıcı ağının yerel bir kopyasına sahiptir. Bazı istisnai durumlarda yazılımda gerçekleştirilen güncellemeler sonrasında yazılımda güncelleme yapmayanlar sadece genel Blockchain ağındaki verileri okuyabilirken, güncellenmiş yazılıma sahip olanlar Blockchain ağına veri yazmaya devam edebilirler. Bu durumda yazılım güncellemesi yapmayan kullanıcıların sahip oldukları yerel Blockchain ağ kopyası güncellenmediği için genel yapıdan farklılık gösterir. Bu Blockchain ağında bir **Geçici Çatallaşma (Soft Fork)** durumu ortaya çıkarır.



Soft Fork – Geçici Çatallaşma Durumunda Ağdaki Kullanıcıların Yapısı

Bazı yazılım güncelleme durumlarında ise güncelleme almayan eski noktalar Blockchain ağına veri yazamadıkları gibi aynı zamanda verileri okuyamaz duruma düşerler. Yazılım güncellemesi yapanlar Blockchain ağını kullanarak ilerlemeye devam ederlerken yazılım güncellemesi yapmayanlar sadece yerel verileri üzerinde okuma ve yazma işlemi yapabilirler. Ancak bu tarz durumlarda belli bir grup eski yapıyı korumaya karar verebilir ve yeni yapıya itiraz edebilir. Bu durumda ister istemez bir birinden ayrılan iki tane yeni Blockchain ağı oluşur. Bu duruma **Mecburi Çatallaşma (Hard Fork)** adı verilmektedir.



Hard Fork – Mecburi Çatallaşma Durumunda Ortaya Çıkan Yeni Ağ

Blockchain ağlarında yaşanabilen çatallaşma probleminin en büyük örneği "DAO Olayı" olarak adlandırılmaktadır ve Ethereum Blockchain ağında gerçekleşmiştir. Temelinde 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 merkezi olmayan kontrol ile bir yapı oluşturmayı hedeflemektedir. "DAO Olayı" kapsamında Nisan 2016 tarihinde Ethereum üzerinde çalışmak üzere tanımlanmış bir DAO kitlesel fonlamaya açılmış, 11.000 civarında kişinin katı-

lımı ile birlikte 150 milyon dolar değerinde 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) kullanıcı, toplanan fonun yaklaşık 1/3'nü 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.

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 teknik yönleri ile (buna rağmen yine de teknik bir giriş olmanın ötesine geçmeden) Kriptoloji, Blockchain ve Akıllı Sözleşmeleri ele aldığımız bölümler ile devam edebilirsiniz. Bizim yazarken büyük keyif duyduğumuz (tamam bu keyif çok büyük olmayabilir :)) bu bölümleri de okumanızı tavsiye ederiz.

İKİNCİ BÖLÜM

Blockchain 201:
Teknik Detaylar

2.1. Kriptolojinin Teknik Detayları

Temel kavramlar bölümünde kriptoloji kavramına hızlıca göz atmıştık. Bu kısmı tekrardan hatırlayacak olursak; eğer verileri oldukça geniş ağlara kopyalayıp çoğaltarak dağıtacaksak bu verilerin gerçekten gizliliğinin ve aynı zamanda bütünlüğünün sağlanması gerekir bu amaç içinse kriptoloji kullanılır.

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 geçirilseler 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 temel olarak matematiksel işlemler kullanarak büyük bir veriden kıyasla daha küçük bir özet bilgi (bunu kaynak veriye ait dijital bir parmak izi olarak düşünebiliriz) üretilmesidir. 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.

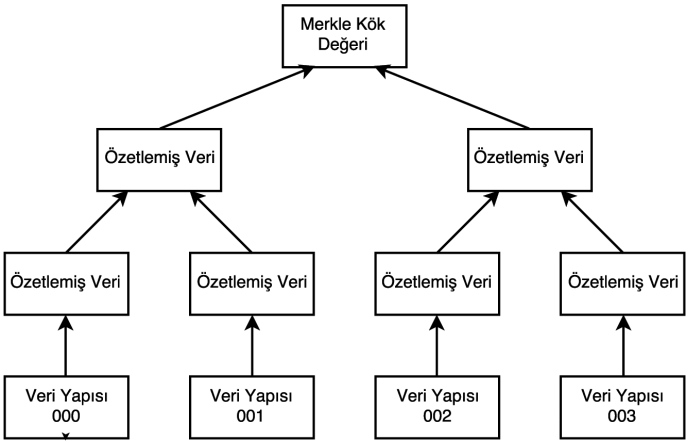
Güvenli özetleme algoritmaları özetledikleri veriden bağımsız olarak sabit uzunlukta özet değer üretirler, örneğin SHA-1 algoritmasının ürettiği özet değerler 160 bit uzunluğunda olurken SHA-256 algoritmasında özet bilgi uzunluğu 256 bit'tir. Algoritma sonuçları sabit uzunlukta olduklarından teorik olarak 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	A7C3962E7BD1F5C65FDD9D97CC993B231CFF60C8296ED9F9590EAD5B0813D1D0
serkan	37B081FA6506D4B937F5A9EB893B45823BDBA49D5DF840B24AF4122BA29E540D
Serkan	508B4498D3A57B759CC171A541CA4F2BBB2DC2B18442665E5EE1E50AF37F7F7A

Merkle Ağaç Yapısı (Merkle Tree)

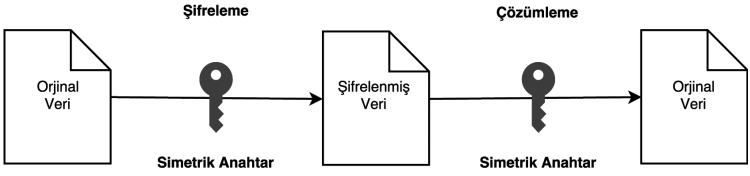
Merkle ağacı, büyük veri kümelerini güvenli ve hızlı bir şekilde doğrulamak için kullanılan, güvenli özetleme yapısı üzerinde geliştirilmiş bir yaklaşımdır. Merkle ağaç yapısında ikili (binary) bir ağaç yapısı oluşturulup, en alt seviyeye veri kümesindeki parçalar yerleştirilir. Sonrasında en alt seviyeden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

Aşağıda 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.

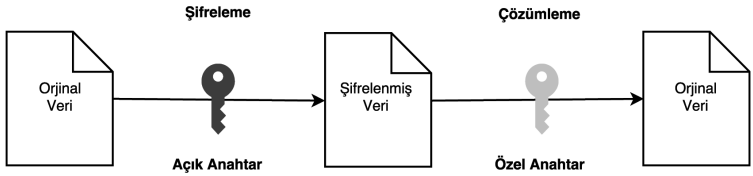


Asimetrik Şifreleme (Asymmetric Encryption)

Bu yaklaşımda şifreleyen ve çözümleyen anahtar bilgileri farklıdır. Temel olarak bu yöntem içerisinde kullanıcının bir adet

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 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.



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.

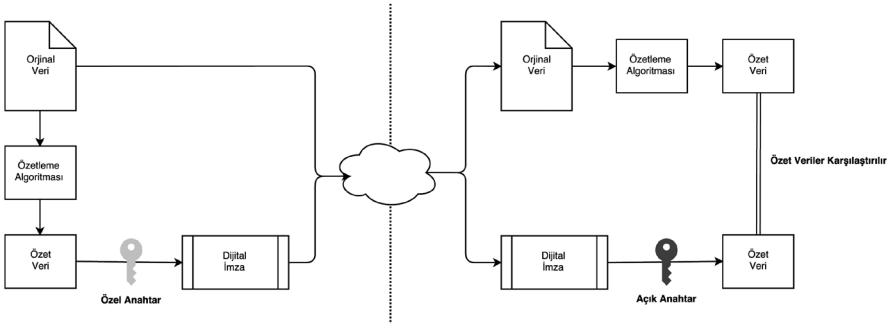
Dijital İmzalama/Doğrulama

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 (yada 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.



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.

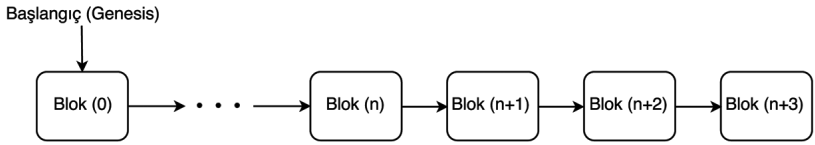
Bu tanımda belirtilen niteliklerin sağlanabilmesi için günümüzde bankalar gibi çeşitli ara kurumlar, kapalı merkezi sistemler kullanırken -örneğin hesabınıza ait bilgilerin bir bankanın merkezi veri yapısında tutulması gibi- Blockchain ağlarının bu ihtiyaçlara karşılık olarak herkese açık, şeffaf, merkezi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

Bu çözüm için temel kavramlar ve bileşenler şu şekildedir;

Blok

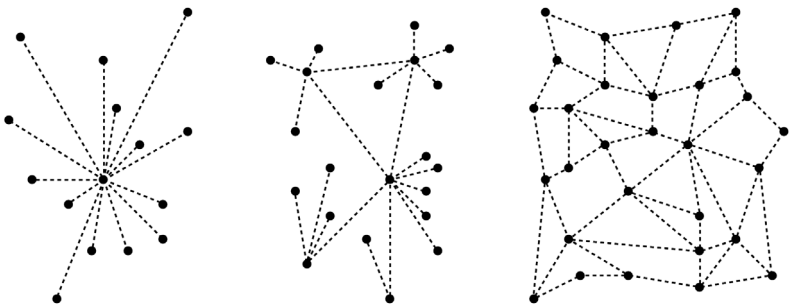
Adından da anlaşılabileceği gibi Blockchain yaklaşımında verilerin saklandığı yapılar blok (block) olarak adlandırılır. Ve bu

blok yapıları bir zincir 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** (bir birinin kopyası) halde tutulmaktadır. Bu şekilde tekil bir ara kuruma ihtiyaç ortadan kalkmakta, bu durumun getirdiği maliyetler ve riskler (single point of failure / tekil kırılma noktası: çalışmaması durumunda içinde bulunduğu tüm sistemin, akışın çalışmasını engel olma) ortadan kaldırılmaktadır.



TEK MERKEZLİ AĞ **ÇOK MERKEZLİ AĞ** **DAĞITIK AĞ**

Mutabakat Mekanizması

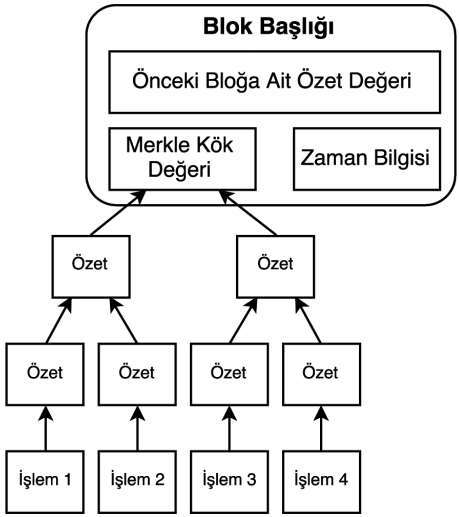
Bir üst madde de ağ yapısı üzerindeki tüm makinelerde Blockchain ağındaki verinin eşlenik bir kopyasını barındırdığını belirtmiştik. Eşleniklik durumunu sağlamak için ağ genelinde **Mutabakat (Consensus)** yapılması gerekir.

Blockchain ağlarında verilerin blok adı verilen yapılarda tutulduğunu biliyoruz. Blockchain ağlarında "güvenlik" tanımı, blokların içerdiği bilgilerin dış dünyadan saklanması değil, oluşturulduktan sonra içerdiği bilgilerin fark edilmeden değiştirilemeyeceğini ifade eder. Bunu sağlamak için **Kriptografik Özetleme** (**Cryptographic Hashing**) ve zaman bilgisi kullanılmaktadır.

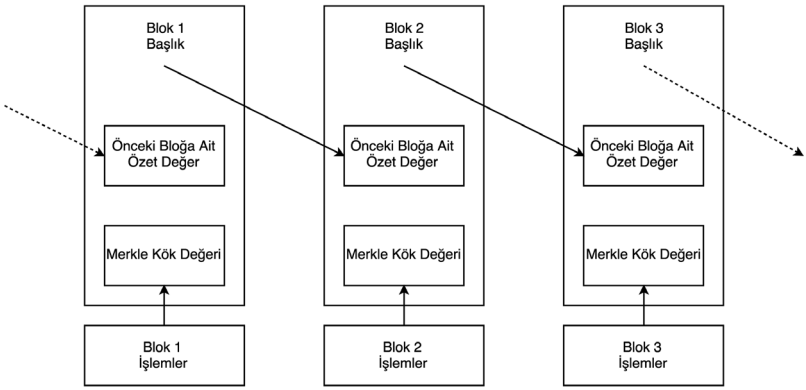
Temel olarak blok iki parçadan oluşur:

- Blok içerisindeki veriler
- Blok içerisindeki veri bütünlüğünü kontrol etmek amaçlı üst bilgi/başlık (**Block Header**). Bir blok başlığı temel olarak aşağıdaki bilgileri içermektedir:
  - 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

Blok başlığı içindeki bilgilerin toplu bir şekilde bir 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.



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 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 incelersek:

Proof of Work

Bu yapıda sistemin bir blok yapısını hazırlayıp, ilgili Blockchain ağına eklenmesinin yönetimi için çözülmesi zor ama çözümün doğruluğun kontrolünün kolay olduğu 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. Basit bir şekilde bu süreci incelersek:

- 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 başlığını 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 hâlâ 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 yapısını bu gereksinimlerin daha elverişli olduğu (ucuz elektrik, düşük maliyetli donanım üretebilme yetkinliği) ortamlara yönlendirmesine ve dağıtık, merkezi olmayan ağ yapısının bu özelliğini zaman içerisinde belirli ölçüde kaybetmesine neden olabilmektedir. Bu durum gerek kullanılan problemlerin farklılaştırılması, gerek enerji tüketimi çıktılarının farklı şekillerde değerlendirilmesi gibi yaklaşımlarla çözülmeye çalışılmaktadır.

Proof of Stake

Bu yaklaşım kapsamında ise blok üretim ve geçerlilik onay mekanizması bloğu üreten makinenin ilgili Blockchain ağı üzerinde sahip olduğu pay ile ilişkilendirilmektedir. 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 temel olarak sahip olunan kripto para miktarına göre hesaplanır.

Pay miktarına göre işlem yapmada farklı davranış şekilleri görülebilmektedir:

- 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 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 kaldırıla-

caktır. Ayrıca katılımcıları platform ile daha derin sahiplik ilişkisine sokarak platformun çıkarına en uygun şekilde çalışmaları için teşvik edilmesi sağlanacaktır. Bu dönüşüm ile birlikte Ethereum platformu daha büyük uygulamaları barındırmak için daha ölçeklenebilir bir hale getirilecektir.

Practical Byzantine Fault Tolerance – PBFT

Bu yapıyı adını Bizanslı generallerin kullandığı bir yöntemden alır. Bizans ordularında generaller, imparatordan gelen emirlerin gerçek olup olmadığını anlamak için oldukça basit ve etkili bir yöntem takip ediyorlardı. İmparator ordusuna bir emir vereceği zaman bunu generallere ulaştırmak için birden fazla ulak yolluyor ve generaller de emri aldıklarında kendi aralarında ulaklar ile bu emirleri paylaşıyorlardı. Bu süreç içinde eğer imparatordan gelen emir ulakların çoğunluğu tarafından doğrulanmış ise bu emrin doğru olduğu kabul ediliyordu. Aksi takdirde tekil emirlere itimat edilmiyordu.

Bu çözümü Blockchain dünyasına getirirsek bu yaklaşımda ağ yapısına dahil her **doğrulayıcı (validator)** rolüne sahip makine için bir açık-özel anahtar ikilisi bulunmaktadır ve her makine diğer makinelerin açık anahtar bilgisine sahiptir.

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, 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 soyutlanmıştır, 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 doğrulayıcı 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 yaklaşım dışında proof of work ve proof of stake'in birlikte uygulanması ile gerçekleşen "proof of activity", blok üretim sürecine dahil olmak için disk alanı tahsis edilmesi gereken "proof of capacity" gibi farklı mutabakat çözümleri bulunmaktadır ancak bu alternatifler daha çok küçük ölçekli denemeler kapsamında kullanılmaktadır.

En Uzun Blockchain Kaydı

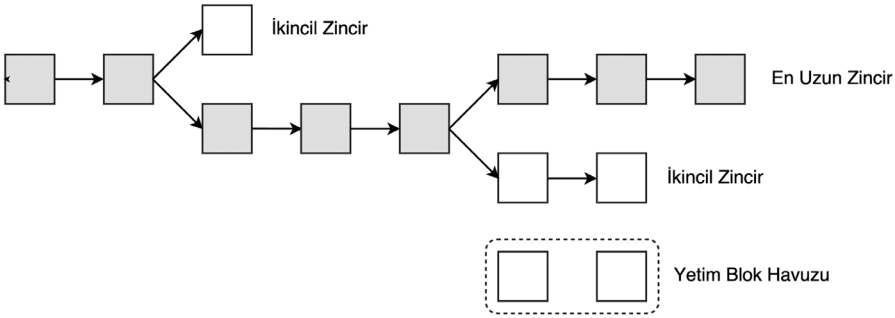
Dağıtık, merkezi olmayan büyük ölçekli bir mimaride bağlı her bir makinedeki blok yapısının her zaman tutarlı olması beklenemez. Sistem içerisinde yakın zamanlı paralel blok üretimi, blokların ağ üzerindeki makinelere farklı zamanlarda iletilmesi gibi nedenlerden dolayı ağa bağlı makineler üzerinde Blockchain ağında farklı blok sıralamasına sahip **düğümlerin (node)** bu-

lunması 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 (bu bilgi ilgili Blockchain ağını oluşturan blokların problem zorluk derecelerinin bir araya getirilmesi ile hesaplanır) Blockchain yapısı "**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 "**ikincil 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 içerisinde belirtilen üst blok tanımı bilinen bir zincir yapısı kapsamında bulunamaz; bu blok-

lar **"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 olayı oluşur. Bu tarz bloklar genel olarak ilgili üst blokları ilgili makineye gelinceye kadar makine üzerinde ayrı bir havuz yapısında tutulurlar.



Blockchain yapılarında çatallaşma sık karşılaşılan bir durumdur, örneğin Bitcoin Blockchain yapısında genel olarak haftada bir tek blokluk çatallaşma görülmektedir, bunun ötesindeki çatallaşmalar çok nadir görülür. Genel olarak 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).

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 - 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 (burada sadece pozitif fark olabilir, toplam çıkış değeri toplam giriş değerinden büyük olamaz) aradaki fark ilgili bloğu üreten makinenin hesabına yansıtılır.

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 aldık ancak teknik olarak hızlıca üzerinden tekrar geçecek olursak;

Soft Fork (Tercihi Çatallaşma): Bu durum genel olarak blok kabul kurallarında yapılan sıkılaştırmalar sonucunda gözlemlenir. Yeni kurallar eski kuralların bir alt kümesi olduğundan dolayı yeni mutabakat kurallarını kullanan makineler tarafından üretilen bloklar, güncelleme yapmamış makineler tarafın-

dan doğrulanabilirler. Güncellenmiş makinelerin ağ üzerinde yüzde 51 ve daha fazla güce kavuşması ile birlikte Blockchain yapısı yeni kural tanımlarına göre oluşan bir yapıya dönüşmeye başlar.

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, güncelleneme yapmamış makineler tarafından, bu şekilde kalmaya devam ederlerse, doğrulanamazlar. Blockchain ağı ikiye bölünerek, Mecburi Çatallaşma ortaya çıkar.

2.3. Teknik Detayları ile Akıllı Sözleşmeler'e Bakış

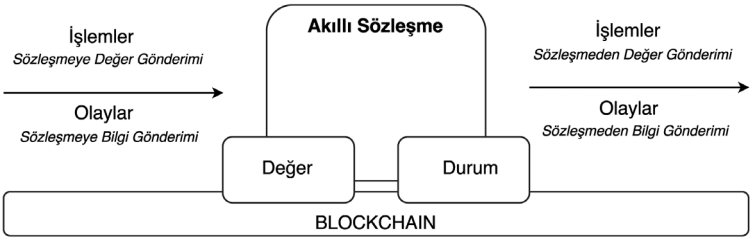
Akıllı Sözleşme kavramı, Blockchain ağlarından bağımsız olarak, 1994 yılında bir bilgisayar bilimcisi olan Nick Szabo tarafından çeşitli taraflar arasındaki etkileşimleri güvenli hale getirip uygun şekilde yürütülmesini sağlayan bilgisayar programlarını/sistemlerini tanımlamak amacı ile ortaya atılmıştır.

Bu yaklaşımı Blockchain bağlamında incelersek, Akıllı Sözleşmeler:

- içinde 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

- üzerinde bulunduğu yapı veya platformda güncellemelere yol açabilen (kripto para ödemeleri/transferleri, yeni akıllı sözleşmelerin yaratılması)

ufak programlardır şeklinde tanımlanabilirler.



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 yada diğer bileşenler sözleşmeye bilgi içeren mesajlar gönderebilir). Bu etkileşim bir işlemin (transaction) başlatılması olabileceği gibi bir bilginin gönderilmesi/teslim alınması şeklinde olabilir. Sözleşme hazırlanırken içerisinden belirlenmiş durumlar oluştuklarında (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.

Akıllı sözleşmeler daha çok Ethereum Blockchain ağı kapsamında öne 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.

Akıllı sözleşmeler, şu anda kullanımda olan geleneksel sözleşme yapılarına karşı çeşitli avantajlar sunmaktadır. Bunların özellikle göze çarpanlarını incelersek:

- 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 risklerini düşürmektedir.
- Akıllı sözleşmeler, "güven" amaçlı aracı kurumlara duyulan ihtiyacı azaltmaktadır.
- Akıllı sözleşmeler, daha az insan girdisine/takibine ihti-

yaç 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 hâlâ emekleme aşamasında olan bir teknolojik yaklaşım olduğu ve çözülmesi gereken temel sorunların olduğu unutulmamalıdır. Bunların bazılarına değinmek gerekirse:

Gecikme Süresi

Şu andaki Blockchain yapıları, işlemlerin doğrulanıp blok mantığında eklenmesi aşamasında yüksek gecikme sürelerine katlanmak zorundadırlar. Blockchain yapısında olmayan veri tabanlarında bu işlemler milisaniye cinsinden ölçümlenirken örneğin Ethereum'da bu değer ortalama 15–17 saniye kadar sürmektedir.

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[8] 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 dünya kullanımlarında olması esneklikler açısından sıkıntı yaratmaktadır.

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

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 olanı 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 mümkün olduğunca Blockchain dünyasını 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 dönemde internetin çıkış noktasından bugün geldiği nokta arasındaki farkı net bir şe-

kilde görebiliyoruz. Blockchain için 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 şöyle 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.

Ortaçağa geri dönecek olursak bir kralın tüm vergilerin toplanmasını beklemesi, pek çok sebeplerden dolayı, çok mantıklı değildi. Kral olabildiğince çabuk şekilde toplanacak vergilerin nakide dönüştürmeliydi. Kral toplanacak vergileri teminat göstererek belli bir faiz karşılığında borç alamazdı zira bu dini ka-

nunlara aykırıydı. Bu sebeple elindeki toplanacak vergiyi gösteren hesap cetvellerini belli bir indirim karşılığında satma fikrini buldu. Böylece vergi çubuklarını satan kral hızlıca nakide ulaşıyor, çubukların yeni sahipleri de vergiler toplandığında kraldan ödemelerini tahsil edebiliyordu. Bu durum bu vergi çubukları için kullanılan "stock" ifadesinin de bu günkü modern devlet tahvili ifadesi olarak kullanımının kökenini oluşturdu. Kraliyet için elindeki tahvilleri belli bir indirim ile satmak, tanrıya ne olduğunu fark ettirmeden borç almak üzere yapılan bir numaraydı.

Kaydı tutulan ticari işlemlerin sayesinde teknoloji hızla dönüşerek yeni bu 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 bulup belli bir indirim karşılığında elindeki çubuklarını satması gerekiyordu. 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 şey 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 Sarayındaki Maliye Bakanlığında, artık kullanılmayan, hesap cetveli dairesinin odasının boşaltmak amacıyla iflas mahkemesine tahsis etti. Ahşap ve Ormancılık Dairesi Londra ofisinde çalışan Asistan Mimar John Phipps, geleneksel garip İngiliz tarihsel sebepleriyle, Krallığın görevlisi olarak sarayda katip olarak çalışan 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 çıkarınca büyük bir yangına sebep oldu ve 16 Ekim 1834'te İngiliz kraliyet sarayı yandı.

Geleceği tahmin etmeye çalışmanın şimdiden bir anlamı yok. Ancak teknik yaklaşımları bir kenara bırakacak olursak 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 bulunur olduğuna 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.

Bankacılık ve finans dünyası bu teknolojiden gelecek yıllarda yoğun şekilde faydalanacak ancak bu teknolojinin nimetlerinden faydalanan tek endüstri bunlar olmayacak. 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'in kendi yapısı bir ağ teknolojisi. O zaman neden siz tekli hareket etmek durumunda olasınız ki? Bu sebeple mutlaka bir ekosistem oluşturun veya mevcut bir ekosistemin parçası olun.
2- Blockchain teknolojisini kurumsal açıdan anlamak için açık ağları incelemek lazım ama en iyi deneyim özel bir altyapı ile anlaşılabilir. 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 hedeflerinizi bu problemleri çözmek olarak belirleyin.
5- Tüm bu önerileri kullanırken teknoloji değil problem odaklı olarak 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 dünyasının sunduğu fırsat ve potansiyeller keşfedilmek üzere müteşebbisleri bekliyor. Zengin kavramlar ile sürekli evrilen bu teknolojinin oluşturduğu dünyada değişim temel unsurlardan birisi. 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. Ancak ilk 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

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://tendermint.com/static/docs/tendermint.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