

# Dağıtık Kayıt Teknolojisi

## Distributed Ledger Technology

Faruk ŞEN\*

ORCID ID : 0000-0001-8012-3219

### Öz

Bilgi, sadece insanlığın sahip olduğu en değerli kaynak değil, aynı zamanda insanın kendisini gerçekleştirmeye çalışırken ihtiyaç duyduğu en önemli enstrümanıdır. Bu anlamda insanlık olarak sahip olduğumuz bilgi birikimini varoluştan beri bu bilgiyi işleyen, kayıt altına alan, paylaşan, sonraki nesillere aktaran ve muhafaza eden yöntemlere borçluyuz. Bu yöntem ve araçlar, insanlığın ulaştığı teknolojik gelişmişlik seviyesine paralel bir şekilde değişmektedir. Bu makalede içinde bulunduğumuz dönemin yeni kayıt teknolojisi olarak adlandırılan Dağıtık Kayıt Teknolojileri genel boyutlarıyla ve kavramsal açıdan irdelenmiştir.

**Anahtar Kelimeler :** Dağıtık Kayıt Teknolojisi, Blokzincir, Toplum 5.0  
**Jel Sınıflandırma Kodları :** O30, O33, O35.

### Abstract

Knowledge is not only the most valuable resource of mankind, but also the most important instrument possessed when trying to realize himself. In this aspect, today we owe our vast knowledge to methods that processes, records, shares, transfers, and preserve this knowledge since its existence. These methods and tools vary in parallel with the level of technological development reached by humanity. In this article the general dimensions of the Distributed Ledger Technology with a conceptual point of view are examined.

**Keywords:** Distributed Ledger Technology, Blockchain, Society 5.0  
**Jel Codes :** O30, O33, O35

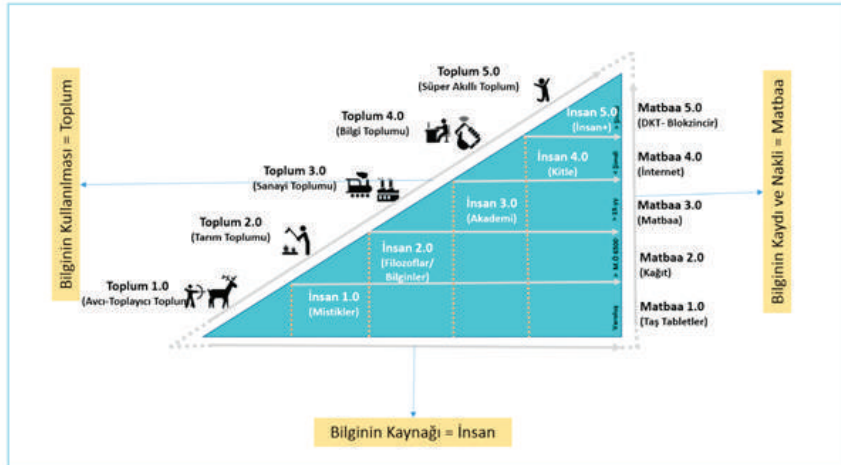
---

\* Ticaret Müfettişi – Ticaret Bakanlığı, f.sen@ticaret.gov.tr

## 1. Giriş

Gerek bilimsel bilgiyi gerekse veri formatında bilgiyi üreten insan bu bilgiyi bir takım enstrümanlar aracılığıyla kayıt altına alarak bunu toplumun kullanımına sunmaktadır. Toplum tarafından kullanılan bu bilgi yeni bir toplumsal düzenin ortaya çıkmasını sağlamakta ve bu döngünün neticesinde toplumlar dönüşmektedir. M.Ö 5000'li yıllara ait Tartaria tabletlerinde (Hood,1967) yada bunlardan yaklaşık iki bin yıl sonra yazılan Sümerlere ait taş yazıtlarda (Kramer,2010) olduğu gibi buralara kaydedilen normların (Speiser,1963) toplumsal hayatı dönüştürdüğü birinci dönemde bilginin kaynağı kabile liderleri, kanaat önderleri, krallar, kahinler gibi belirli, seçkin, sınırlı ve 'mistik' diyebileceğimiz bir insan grubudur ki bunları İnsan 1.0 olarak; bilginin kaydedilmesi ve topluma iletilmesi için kullanılan enstrüman olan kil tabletleri ve taş yazıtları Matbaa 1.0 olarak ve bu şekilde oluşan toplum yapısını da Toplum 1.0 (İlkel Toplum) olarak nitelemek mümkündür.

MÖ. 105 yılında Çinli, Ts'ai Lun kağıdı icat ederek kayıt teknolojisini değiştirmeyi başarmıştır (Hunter,1978). Bu dönemde bilimsel, edebi ve sanatsal bilgi kitaplarda saklandığından kitaplar hem çok stratejik ve hem de pahalı bir emtia niteliğindedir. El yazması kitaplar sayesinde bilgiye erişimin kısmen daha kolay olduğu bu dönemin sonunda yerleşik hayat kurumsallaşmıştır. Bu dönemde bilginin kaynağı filozoflar ve alimler gibi 'bilgin' kimselerdir ki bunları İnsan 2.0 olarak; bilginin kaydedilmesi ve topluma iletilmesi için kullanılan yöntem olan kağıdı ve el yazma kitapları Matbaa 2.0 olarak ve bu şekilde oluşan toplum yapısını da Toplum 2.0 (Yerleşik Toplum) olarak nitelemek mümkündür.



Kaynak: Keidanren'in (Japan Business Federation) kullandığı şablon esas alınarak yazar tarafından oluşturulmuştur.

15. yüzyılın ikinci yarısında Alman mucit Johann Gutenberg tarafından modern anlamda bildiğimiz matbaanın icat edilmesiyle kayıt teknolojisi bir kez daha değişmiştir. Matbaanın icadından önce Batı Avrupa'da üretilen toplam kitap sayısı yaklaşık 5 milyon adet iken bu sayı matbaanın icat edildiği ilk 50 yılda yaklaşık 79 milyon adede ve endüstri devriminin hemen arifesinde 1750-1800 yılları arasında 628 milyon adede ulaşmıştır (Buringh & Zanden, 2009). Bilgiyi stratejik bir kaynak olarak kullanan İngilizler 1803 yılında yaklaşık % 5,7 olan okullaşma oranını 1858'de % 12,9'a yükseltmiş (Umassd, 1861), reformist dönüşümle birlikte bu yeni eğitim sisteminin ön plana çıkarmış olduğu bireysellik (Thomson, 1973, p.79-92) bilimsel çerçeveyi şekillendirerek (Hill, 1969,p.41) endüstri devrimini tetiklemiş ve bu süreç toplumun tarım toplumdan sanayi toplumuna dönüşmesiyle sonuçlanmıştır. Bu dönemde bilginin kaynağı 'akademi' olup bunlar üniversite, manastır ve medreseler de görevli bilim adamlarından teşekkül

olmaktadır ki bunları İnsan 3.0 olarak nitelemek mümkündür. Bilginin kaydedilip çoğaltılmasını ve topluma iletilmesini sağlayan enstrüman olan matbaanın kendisini Matbaa 3.0 olarak ve bu döngünün neticesinde oluşan toplumu da Toplum 3.0 (Sanayi Toplumu) olarak adlandırabiliriz.

1946 yılında bilgisayarın (ENIAC), 1969 yılında ARPANET adı altında bugün modern anlamda bildiğimiz internetin icadı ve 2006 yılı itibariyle bulut depolama teknolojisini ticari olarak kullanılmaya başlanmasıyla birlikte kayıt teknolojisi bir kez daha farklı bir boyut kazanmıştır. (Laudon & Traver, 2014) Bilgisayar ve internetin icadı bilginin işlenmesinin, kaydedilmesinin, depolanmasının ve iletilmesinin önündeki zaman ve mekan kısıdını ortadan kaldırarak toplumun sanayi toplumundan bilgi toplumuna evrilmesini sağlamıştır. Bu dönemde bilginin kaynağı "kitle" dediğimiz toplumdaki her bir bireydir ki bunu İnsan 4.0 olarak; bilginin üretilmesi, işlenmesi, saklanması ve topluma iletilmesi enstrümanı olan interneti ve bilgisayarı Matbaa 4.0 olarak ve bu döngünün neticesinde ortaya çıkan toplum biçimini de Toplum 4.0 (Bilgi Toplumu) olarak tanımlamak mümkündür.

İçinde bulunduğumuz dönem, kayıt teknolojisi açısından yeni bir kırılma noktasıdır. Tarihin hiçbir döneminde bu evrede üretildiği kadar bilgi üretilmemiştir. 1984 yılında tüm dünyada internet üzerinde üretilen toplam aylık ortalama veri yaklaşık 15 gigabayt iken 2014 yılında bu rakam 42 milyar gigabayta ulaşmıştır (WTO,2018). 2018 yılında internette üretilen toplam veri miktarı 33 trilyon gigabayt olup bu rakamın 2025 itibariyle 175 trilyon gigabayta ulaşması beklenmektedir. 175 trilyon gigabayt büyüklüğündeki bir veri mevcut durumda kullanılan DVD'lere kaydedilebilseydi yan yana konulan bu DVD'lerin uzunluğu dünyanın etrafını 222 kez dolaşmaya veya Ay'a 23 kez gitmeye yeterdi. Bu veriyi bir insan 25 Mb/s hızıyla indirmeye çalışsaydı tam 1,8 milyar yılda indirebilirdi (IDC,2018). Böyle muazzam büyüklükteki veriyi güvenli bir şekilde işleyen, kaydeden, paylaşılmasını sağlayan, transfer ve muhafaza eden enstrüman dağıtık kayıt teknolojileri olacaktır. Bunun bir sonucu olarak büyük veri, yapay zeka ve nesnelerin interneti gibi teknolojik enstrümanların toplumsal hayatı şekillendirdiği toplum yapısı da bilgi toplumundan bilgi ötesi topluma (süper akıllı topluma) dönüşecektir ki bu toplum Japonya Bilim Konseyi tarafından 'fiziki alan ile sanal alanın iç içe olduğu bir sistem yapısı çerçevesinde, ekonomik gelişmişliği sosyal sorunların çözümüyle dengeleyen insan merkezli bir toplum' şeklinde tanımlanmaktadır (Cabinet Office, 2019). Bu dönemde bilgi insanın yanı sıra artık makineler, robotlar, bilgisayarlar (AI) ve nesneler (IoT) tarafından da üretilmektedir. Bu durum bilginin kaynağının 'insan+(İnsanArtı/HumanPlus)' olduğu anlamına gelir ki bunu İnsan 5.0 olarak, bu bilginin işlenmesi, kayıt altına alınması, saklanması ve iletilmesi için kullanılan enstrüman Dağıtık Kayıt Teknolojisini (Blokzincir) Matbaa 5.0 olarak ve bu döngünün neticesinde ortaya çıkacak toplum biçimini de Toplum 5.0 (Süper Akıllı Toplum) olarak nitelemek mümkündür.

Bu anlamda, taş yazıtlar ilkel toplumdaki yerleşik topluma geçişte yada kağıdın ve matbaanın icadı tarım toplumundan sanayi toplumuna geçişte veya bilgisayar ve internetin icadı sanayi toplumundan bilgi toplumuna geçişte nasıl bir rol oynamışsa; dağıtık kayıt teknolojilerinin de içinde yaşadığımız toplumun bilgi ötesi (süper akıllı) topluma dönüşmesinde öyle bir rol oynayacağını söyleyebiliriz.

## 2. Dağıtık Kayıt Teknolojisi

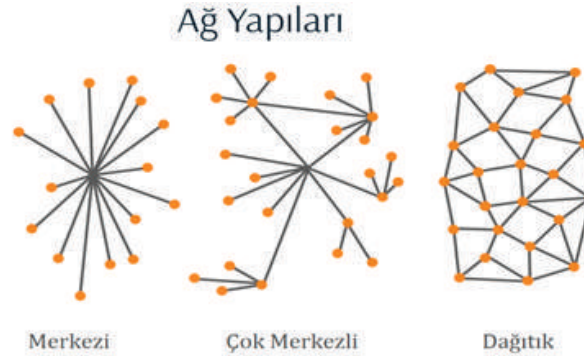
Dağıtık Kayıt Teknolojisi (DKT) genel olarak blokzincir olarak bilinmektedir. Her ne kadar bu iki kavram bir birinin yerine kullanılabilseler de aynı şey değildir. Her Blokzincir bir DKT'dir ancak her DKT bir blokzincir değildir. DTK'nin geçmişi internet üzerinden bilgi, eposta, müzik yada dosya paylaşma gibi uygulamalar kadar eskidir. Ancak modern anlamda bildiğimiz ve kullanıcılar arasında güvenli bir şekilde para, mülkiyet hakkı, kullanım hakkı gibi "değer" transfer eden DKT'nin geçmişi Satoshi Nakamoto'nun 2008 yılında yayımladığı 'Bitcoin: A Peer-to-Peer Electronic Cash System' adlı makaleye dayanmaktadır. Temelde uçtan uca (P2P) ağ yapısı, şifreleme ve oyun teorisine dayalı bu teknoloji, verinin DKT ekosistemi-

ne dahil tüm kullanıcılar arasında dağıtık ve değiştirilemez bir şekilde kayıt altına alınmasını sağlamaktadır.

DKT'nin terminolojisi henüz evrilmeye devam ettiği için evrensel bir tanımlama da yapılamamıştır. Ancak bu teknolojiyi mümkün kılan ayrıntılar 1990'lara kadar uzanmaktadır. Stuart Haber ve W. Scott Stornetta' a ait olan 1990 tarihli dijital belgelerin zaman damgasıyla imzalanması, Ross Anderson'a ait 1996 tarihli merkezi olmayan (dağıtık) veri depolama sistemi ve Bruce Schneier ve John Kelsey'e ait olan 1998 tarihli hassas verilerin güvensiz makineler arasında kripto şifrenmesi konulu makaleleri DKT'nin temel taşlarını oluşturmuştur. Bu anlamda Dağıtık Kayıt Teknolojisi, ekosisteme dahil olan tüm kullanıcılarının her birinin tam olarak aynı veri kaydına sahip olmaları ve bu kaydı topluca ve hep birlikte kendilerine ait bilgisayar sunucularında (dağıtık olarak) saklamaları şeklinde tanımlanabilir. (World Bank Group, 2017).

Dağıtık Kayıt Teknolojilerinin esasında dağıtık ağ yapıları, mutabakat mekanizması ve şifreleme algoritmaları olmak üzere 3 temel niteliği söz konusudur. Bu üç özelliği aynı anda barındırıyor olması sebebiyle Matbaa 5.0 dediğimiz dağıtık kayıt teknolojisi bundan önceki bilgiyi kayıt altına alma yöntemlerinden ayrılmaktadır. İster taş yazıtlara kaydedilmiş isterse internette bulutta kaydedilmiş veri olsun geleneksel kayıt sistemi dediğimiz Matbaa 1.0 ila Matbaa 4.0 arasındaki tüm kayıt enstrümanları merkezi-dir. Bunu anlamak için ağ yapılarına biraz daha yakından bakmak gerekmektedir.

En geniş anlamda üç farklı ağ yapısı söz konusu olup bunlar verinin saklanma biçimine göre farklılık arz etmektedir (Buterik,2017). Merkezi ağ yapısında veri tek bir merkezde saklanmaktadır.



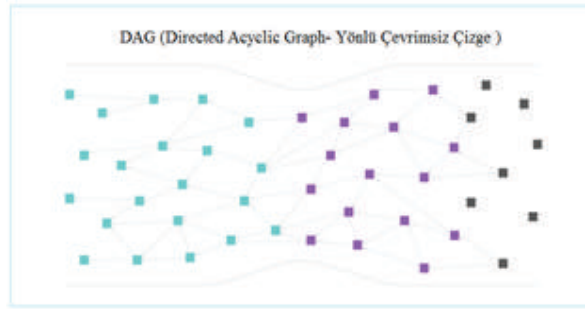
Mevcut durumda kullandığımız ağ yapısı merkezi ağ yapısı olup bu sistemde veri belirli merkezlerdeki veri tabanlarında saklanmaktadır. İnternet kullanıcılarının her an üretmiş oldukları verilerin arama motorlarının yada sosyal medya platformlarının veri tabanlarında saklanması yada Ticaret Bakanlığı'nca üretilen verilerin Bakanlığın kendi sunucularında saklanması gibi. Bu ağ yapısının en önemli özelliği buradaki verilen tam ve eksiksiz olmasından sadece ağın sahibinin sorumlu olmasıdır. Dolayısıyla bu verilerin kullanıcıları açısından güvenilirliği ağ sahibinin aracılığına bağlıdır ki bu durum ağ sahibinin teyidi olmadan buradaki işlemlerin geçerliliği söz konusu olamaması anlamına gelmektedir. İşte bu durum verinin kullanıcıları açısından bir aracıya güvenmeyi zorunlu kılmaktadır ki bu aracının varlığı hem yapılan işlemin maliyetini artırmakta ve hem de işlemin tamamlanması için gerekli olan sürenin uzamasına sebep olmaktadır. Dağıtık ağ yapısında ise veri tek bir merkezde değil ekosisteme dahil olan tüm kullanıcılar tarafından saklanmaktadır. Veri eş zamanlı olarak ilgili tüm kullanıcıların sunucularında saklandığı için ayrıca bir merkezi otoritenin bu kayıtları saklamasına ve bunları teyit etmesine gerek olmadığından yapılan işlemlerde işlem ve zaman maliyeti ortaya çıkmamaktadır.

Dağıtık kayıt Teknolojisinin bir diğer özelliği verilerin şifrenmesidir. Bu şifreleme işleminde bir

takım matematiksel algoritmalar kullanılarak veriler şifrelenmektedir. Bu işlem esnasında genel ve özel olmak üzere iki farklı şifre üretilerek sistemin güvenilirliği özel şifrenin hassasiyetle korunmasına bağlıdır. Geleneksel kayıt sisteminde ise verinin güvenli bir şekilde şifrelenmesi söz konusu olmadığından, gerek transferi esnasında gerekse de transferinden sonra veriye dışarıdan müdahale edilerek aslına uygun olmayan nüshalarının üretilmesi mümkündür. DKT bu sorunu ortadan kaldırarak bilginin naklini güvenli hale getirmektedir.

Mutabakat işlemi ise sisteme girilen her yeni verinin geçerliği ve doğruluğu konusunda ekosistemdeki her bir kullanıcı tarafından önceden belirlenen mutabakat kuralları çerçevesinde fikir birliğine varılması işlemidir (World Bank Group, 2017). Mutabakat mekanizması DKT uygulamalarını birbirinden ayıran en belirgin niteliklerdir. Mutabakatın şekli ve kurallarına bağlı olarak yapılan işlemlerin hızı ve maliyeti de değişmektedir. Bunun bir sonucu olarak da farklı mutabakat mekanizmalarına sahip DKT uygulamaları ortaya çıkmıştır.

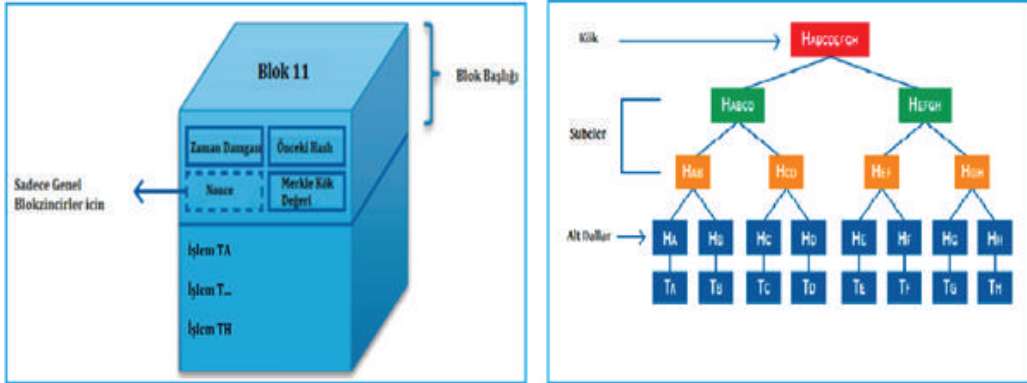
En yaygın olarak bilinen Dağıtık Kayıt Teknolojisi uygulamaları Blokzincir, Tangle, Hashgraph ve Holo-chain adlı uygulamalardır.



Blokzincirde yapılan bir işlem ekosistemdeki tüm kullanıcılar tarafından onaylanarak tek ve eşsiz bir özetleme (hash) numarası olarak bir önceki işlemin özet numarasıyla birlikte saklanmaktadır. Bu şekilde kaydedilen bir verinin daha sonradan değiştirilmesi, tahrif edilmesi ya da silinmesi mümkün değildir. Blokzincirde yapılan her işlemin tek tek her bir kullanıcı tarafından onaylanması gerektiğinden bunun yapılması için öngörülen mutabakat mekanizması uzun sürmektedir. Bu mekanizmada yeni bir bloğun oluşturulması yaklaşık 10 dakika sürmektedir ki bu durum blokzincirde saniyede 7 işlemin (TPS) onaylanması anlamına gelmektedir. Bir ödeme metodu olan Visa sisteminin saniyede işlem kapasitesinin 56.000'e kadar (TPS) çıkabildiği hususu dikkate alınırsa blokzincirin işlem kapasitesinin çok düşük olduğu ortadır (Ganne, 2018). Bu yavaşlamaya sebep olan unsur mutabakat mekanizmasında her bir kullanıcının onayının alınmasında izlenen yöntemdir. Blokzincirin tüm özelliklerini barındıran ancak bloklar olmaksızın çalışan Tangle uygulaması bu yavaşlamanın kaynağı olarak gördüğü mutabakat mekanizmasını değiştirerek bir kullanıcının bir işlemi onaylayabilmesini önceki iki işlemi onaylaması şartına bağlamıştır (Popov, 2016). Bu şekilde işlem sürelerini kısaltarak ve maliyetleri azaltarak daha etkin bir çözüm sunmaktadır. Hashgraph uygulamasındaki 'gossip' adı verilen mutabakat mekanizmasına göre ise her bir işlem tek tek onaylanmak yerine birden fazla işlem aynı anda onaylanmak suretiyle süreç hızlanmakta (Baird, 2016) ve saniyede 250.000 (TPS) işlem kapasitesi yakalanmaktadır. Hem Tangle hem de Hashgraph uygulamaları DAG (Directed Acyclic Graph- Yönlü Çevrimsiz Çizge) teknolojisini kullanmaktadır. DAG yapısı, kullanıcılar (node) ve bunlar arasındaki ilişkilerden oluşmakta olup bu yapıda işlem sadece tek yönlüdür ve geri döndürülmesi mümkün değildir. Aynı anda birden fazla kullanıcının işlem yapması mümkün olduğundan işlem sırasında beklenen süre ve işlemin onaylanması için gerekli süre geleneksel blokzincire göre çok daha kısadır.

Holochain uygulaması ise dağıtık kayıt teknolojisine yeni bir bakış açısı kazandırmıştır. Bu yöntemde de her bir kullanıcının işlemleri tek tek onaylaması söz konusu değildir. Her kullanıcı DNA mutabakat mekanizması adı verilen mekanizma sayesinde başkalarının değil sadece kendisine ait olan işlemleri onaylamak suretiyle onay sürecini hızlandırmaktadır (Harris-Braun, Luck,& Brock,2018). Holochain'i Blokzincir'den ayıran en önemli özelliği, yapılan işlemin güvenilirliğinden taviz vermeden kullanıcıların sadece kendi işlemine ait veriyi saklama ve görüntüleyebilme özelliğine sahip olacak şekilde sınırlandırılmalarına imkan sağlamasıdır (Anwar,2019).

İlk kez 2008 yılında Satoshi Nakamoto tarafından kavramsallaştırılan ancak henüz nihai olarak tanımlanamayan Blokzincir kavramı bir kripto para birimi olan Bitcoin'in kullandığı sanal altyapıdır. 2008 yılında yaşanan finansal kriz neticesinde merkezi para otoritelerine duyulan güven kaybedilmeye başlayınca kim olduğu henüz tam olarak bilinmeyen Satoshi Nakamoto adlı bir kriptoloji fenomeni "Bitcoin: A Peer-to-Peer Electronic Cash System – Bitcoin: Kullanıcılar (eşler) Arası Elektronik Nakit Sistemi" adlı bir makale yayımlayarak, bankaların aracılığına ihtiyaç duyulmaksızın kişiler arasında aynı paranın mükerrer kullanılmasını engelleyerek, güvenli sanal para transferinin mümkün olduğunu ortaya koymuştur (Nakamoto,2008). İşte bunu mümkün kılan teknolojinin adı blokzincir olup; kullandığı matematiksel şifreleme teknikleri sayesinde işlemlerin nerdeyse değiştirilmesi mümkün olmayacak şekilde kaydeden Dağıtık Kayıt Sistemi şeklinde tanımlanmaktadır. Yapılan her işleme ait kayıt bir blok içerisinde saklanmaktadır. Bir blok en fazla 1 MB veriyi saklayabilmektedir. Bundan daha yüksek hacimli veri oluşturan işlemler için ilave blokların oluşturulması gerekmektedir.



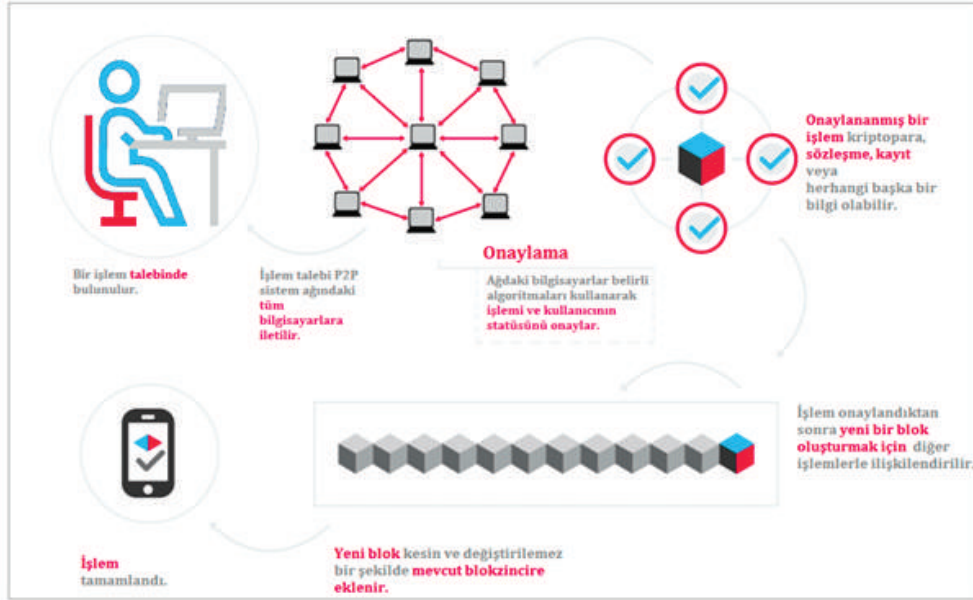
Kaynak: Ganne, Can Blockchain Revolutionize International Trade?

Her hangi bir blok, gövdesinden ve blok başlığından oluşmaktadır. Örneğin yukarıdaki 11 no.lu blok gövdesinde TA ila TH arasındaki işlemler kayıtlıdır. Blok başlığında ise bu işlemler Merkle Kökü olarak özetlenmektedir. En genel anlamda bir Merkle ağacı, çok sayıda veri yığını bir araya getirmenin ve bu veri yığının doğrulanmasının bir yoludur. Bir blok içerisindeki tüm işlemler ikiye bölünür, ortaya çıkan özetler yine kendi aralarında ikiye bölünür, bu işlem tek bir özet elde edilene kadar devam ettirilir. İşlemlerin ikiye bölünmesiyle oluşan ağaç yapısına Merkle Ağacı ve sonuçta ulaşılan tek özete ise Merkle Kökü denir. Yapılan herhangi bir işlemin gerçekte var olup olmadığı kontrol edilirken zincire ekli her bloktaki her bir işlemi tek tek kontrol etmek zaman kaybına sebep olacağından bu işlemler yerine bunların özetleri kontrol edilip zaman tasarrufu sağlanarak işlemler hızlandırılmaktadır. Geriye doğru hareket edilerek kök değerinden işlemin kendisine ulaşmak her zaman mümkündür. Bir bloğa ait herhangi bir işlemde değişiklik yapıldığında, hem o işleme ait Merkle Kök değeri ve hem de bloğun özeti değişmiş olacağından, o bloktan sonraki tüm bloklar doğrulanamaz hale gelecektir. Bu yapı hiç bir işlemin geriye doğru değiştirilememesi anlamına gelir.



Blok başlığında yer alan bir diğer bilgi Zaman Damgasıdır. Bu damga her bir işlemin yapıldığı an itibariyle zaman damgasıyla damgalanması şeklinde gerçekleştirilmekte olup asıl amacı kripto paralarda mükerrer harcama olarak bilinen “double spending” sorununu ortadan kaldırmaktır. Amacı kripto para üretmek olmayan blokzincir uygulamaları açısından bunun anlamı, herhangi bir değer (örneğin aynı taşınmaza ait birden fazla tapu belgesinin üretilmemesi yada aynı konşimento kapsamı gönderi konusu eşyalar için (sahte menşe belgesi üretilmemesi gibi) birden fazla kez transferini engellemektir.

Son olarak blok başlığında bir önceki işlemin Hash değeri yer almaktadır. Hash, herhangi bir uzunluktaki bir girdiyi alarak onu bir dizi matematik algoritması ile şifreli bir çıktı haline dönüştürme işlemine verilen isimdir. Hash fonksiyonları kabaca, farklı büyüklüklerdeki veri kümelerinin sabit uzunlukta bir veri kümesine adresleyen algoritmalarıdır. Aynı girdi her zaman aynı Hash değerini üretecektir ve Hash değerine bakarak girdiyi belirlemek imkânsızdır. Girdide oluşan en ufak bir değişiklik bile Hash değerini tamamen değiştirmektedir.



Blok yapısının genel olarak nelerden oluştuğuna baktıktan sonra şimdi bir blok zincirin nasıl oluşturulduğuna biraz daha yakından bakmak faydalı olacaktır. Temel anlamda bir Blokzincir 3 adımdan oluşmaktadır. İlk olarak ilgili kullanıcı gerçekleştirdiği işlemi ekosisteme dahil tüm kullanıcılara göndererek yaptığı işlemin doğrulanmasını talep eder. İkinci adımda ekosistemdeki tüm kullanıcılar bu işleme ait verileri kendilerine ait bir blokta birleştirerek bu işleme ait daha önceden belirlenen mutabakat mekanizması çerçevesinde (Proof of Work) bir SHA-256 algoritma değerini (şifre) çözerler. Bu şifreyi çözen ilk kullanıcı bunu ekosistemdeki diğer tüm kullanıcılarla paylaşır (Bitcoin’de bu şifreyi ilk çözen kullanıcı belli bir miktar Bitcoin ile ödüllendirilmektedir). Diğer kullanıcılar yeni oluşturulan bloğu, bu blok konusu işlem gerçek ve doğrusya kabul ederek onaylarlar. Bu şekilde onaylanan işlem son adımda zincire eklenerek işlem neticelendirilir (Nakamoto,2008). Blokzincir uygulamaları, ekosisteme dâhil olabilecek kişilerin sınırlandırılıp sınırlandırılmamaları ve sisteme dâhil oluş biçimleri itibariyle farklılık arz etmektedir. Dileyen herkesin ekosisteme dâhil olması mümkünse (Bitcoin gibi) bu durumda genel (açık) blokzincir, sadece belirli kişilerin dahil olabilmesi halinde ise özel blokzincir söz konusudur. Ekosisteme dâhil olunurken bu sistemi işleten mekanizmadan izin alınması gerekmiyorsa izin gerektirmeyen blokzincir, kısmen veya

tamamen izin alınması gerekiyorsa da izin gerektiren blokzincir söz konusudur. Dış ticaret işlemlerinin bu teknoloji üzerinden yürütülmeye başlanması durumunda bir özel blokzincir türü olan izin gerektiren konsorsiyum blokzincir türünün kullanılması en doğru seçim olarak görünmektedir.

Satoshi Nakamoto'nun geliştirmiş olduğu bir kripto para birimi olan Bitcoin'in kullanmış olduğu ve temel özellikleri yukarıda izah olunmaya çalışılan blokzincir uygulaması, birinci jenerasyon blokzincir olarak bilinmektedir (blokzincir 1.0). Bu jenerasyon teknolojinin işlem kapasitesi düşüklüğü, sadece kripto para birimlerinin alt yapısına ilişkin olması ve diğer blokzincir türleriyle birlikte çalışmama gibi bir takım açmazları söz konusudur.

İkinci jenerasyon blokzincir (blokzincir 2.0) olarak bilinen teknoloji yine Ether adında bir kripto para biriminin teknolojisi de olan Ethereum teknolojisidir. Bu teknoloji blokzincir dünyasına Akıllı Sözleşmeler ( Smart Contracts) kavramını getirmiştir ki bu sözleşmeler önceden tanımlanan koşulun meydana gelmesi halinde arzulan sonucu ayrıca bir onaya gerek kalmaksızın gerçekleştiren otomatik talimat şeklinde tanımlanabilir (Buterin, 2014). Birer yazılım kodu olan bu sözleşmeler blokzincir teknolojisini sadece kripto para birimlerinin teknolojik altyapısı olmaktan çıkarmış, ticaret, finans, tarım, sağlık gibi bir çok alanda da kullanılabilir hale gelmesinin sağlamıştır (Anwar, 2018). Ancak bu sözleşmelerin de sadece bir yazılım kodu olarak blokzincirde yer almaları dolayısıyla bunların hukuki bir bağlayıcılıkları yoktur. Başka bir ifadeyle bu sözleşmeler geleneksel anlamda yazılı bir sözleşme niteliğinde olmadığından olası bir uyumsuzluk durumunda hukuki bağlayıcılıkları söz konusu değildir. Bu sorun son dönemler Ricardian Smart Contracts adı verilen Rikardocu Akıllı Sözleşmeler ile çözülmeye başlanmıştır. Bu tarz sözleşmeler hem insan hem de bilgisayar tarafından okunabilir sözleşmeler olduğundan, geleneksel yazılı sözleşmelerin tabi olduğu hukuki bağlayıcılığa sahip akıllı sözleşmelerdir ( Alam,2018; Grigg,2000).

Üçüncü jenerasyon blokzincir (blokzincir 3.0) teknolojisinde ise farklı blokzincir yazılımlarının birlikte çalışabilirliği (interoperability) mümkün hale gelmiştir. Örneğin Ripple farklı blokzincir uygulamalarının karşılıklı iletişimini (Crosschain) mümkün kılan bir teknolojiye sahiptir ( Schwartz, Youngs,& Britto,2014). Bu durum özellikle, dış ticaret açısından, farklı ülkelerde kullanılan farklı blokzincir yazılımlarından karşılıklı veri transferinin mümkün kılınması anlamına geliyor ki bu daha önce mümkün değildi. Avrupa Birliği Blokzincir Formu, blokzincir teknolojisinin ölçeklenebilirliği, birlikte çalışabilirliği ve sürdürülebilirliği olmak üzere üç temel sorunun devam ettiğini belirtmiştir (EUBlockchain,2019). Sigortacılık, uluslararası ticaret, bankacılık, noter, tapu ve nüfus işlemleri gibi birçok alanda kavramsal çerçevede pilot uygulamaları yürütülen bu teknolojinin yaygın kullanılabilir hale gelmesi için daha çok somut projenin uygulamaya geçirilmesine ve bu teknolojinin evrilmesine ihtiyaç olduğu anlaşılmaktadır.

### 3. Sonuç

Dağıtık kayıt teknolojisinin, insanlığın sahip olduğu bilgi stokunu işleme, saklama, paylaşma ve transfer etme biçimini bir kez daha değiştirerek, toplumu dönüştüren en önemli itici faktörlerden birisi olacağını söyleyebiliriz. Bu teknolojiyi mümkün kılan gelişmelerin geçmişi 1990'lara dayansa da bugünkü haliyle kavramsallaştırılmasında en önemli rolü hiç şüphesiz kripto paralar oynamaktadır. Bir çok sebepten dolayı kripto paralara mesafeli yaklaşıldığından, bunların altyapısını oluşturan teknolojinin keşfedilmesi de zaman almıştır. Dağıtık kayıt teknolojisinin kripto para birimi ticaretinden farklı alanlar da kullanım alanının olduğunun fark edilmesiyle birlikte bu teknolojiye çok önemli yatırımlar yapılmaya başlanmıştır. Henüz emekleme aşamasında olan bu teknolojinin tüm yönleriyle olgunlaşması durumunda, ekonomik ve sosyal yaşamda gerçekleştirilen işlemlerde geleneksel anlamda 'güven' ve 'teyit' rolü üstlenen kamu kurumları dahi tüm üçüncü şahıs aracıları ortadan kaldırarak toplumsal hayatı bir kez daha dönüştürebilecek potansiyele sahip olduğu değerlendirilmektedir.



**Kaynakça:**

- Hood, M. (1967). The Tartaria Tablets. *Antiquity*, 41(162), 99-113. doi:10.1017/S0003598X00033032
- Kramer, S. N. (2010). *The Sumerians: Their history, culture, and character*. University of Chicago Press.
- Speiser, E. (1963). Cuneiform Law and the History of Civilization. *Proceedings of the American Philosophical Society*, 107(6), 536-541. Retrieved from <http://www.jstor.org/stable/986110>
- Hunter, D. (1978). *Papermaking: the history and technique of an ancient craft*. Courier Corporation.
- Buringh, E & Zanden, J. (2009). Charting the "Rise of the West": Manuscripts and Printed Books in Europe, A Long-Term Perspective from the Sixth through Eighteenth Centuries. *The Journal of Economic History*. 69. 409-445. 10.1017/S0022050709000837.
- Umassd, (1861) *The Royal Commission on the State of Popular Education in England [Newcastle Commission]*, Parliamentary Papers, 1861, XXI. pp. 293-328; in G. M. Young and W. D. Hancock, eds., *English Historical Documents*, XII(1), 1833-1874 New York: Oxford University Press, 1956, pp. 891-97.
- Thomson. A. (1973), *The Dynamics of Industrial Revolution*, London: Edward Arnold Publisher.
- Hill. C. (1969), *Reformation to Industrial Revolution*, England: Penguin Books.
- Laudon, K. C., & Traver, C. G. (2014), p.123-132. *E-commerce: business, technology, society*.
- WTO, (2018), *World Trade Report 2018*, Retrieved from [https://www.wto.org/english/res\\_e/publications\\_e/world\\_trade\\_report18\\_e.pdf](https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf)
- IDC, (2018), *The Digitization of the World From Edge to Core*, Retrieved from <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>
- Cabinet Office,(2019) *Society 5.0*, Retrieved from [https://www8.cao.go.jp/cstp/english/society5\\_0/index.html](https://www8.cao.go.jp/cstp/english/society5_0/index.html)
- World Bank Group, (2017), *Distributed Ledger Technology (DLT) and Blockchain* Retrieved from: <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>
- Buterik. V, (2017). *The Meaning of Decentralization* Retrieved from: <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>
- Ganne, E. (2018). *Can Blockchain revolutionize international trade?*. World Trade Organization. Retrieved from: <https://tradenews.com.ar/wp-content/uploads/2018/12/Blockchain-OMC.pdf>
- Popov, S. (2016). *The tangle*. cit. on, 131. Retrieved from <http://www.descryptions.com/lota.pdf>
- Baird, L. (2016). *The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance*. Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep. Retrieved from: <http://pages.cpsc.ucalgary.ca/~joel.reardon/blockchain/readings/hashgraph.pdf>
- Harris-Braun, E., Luck, N., & Brock, A. (2018). *Holochain-scalable agentcentric distributed computing*. Alpha, 1,

1-14. Retrieved from: <https://github.com/Holochain/holochain-proto/blob/whitepaper/holochain.pdf>

Anwar. H.,(2019). Distributed Ledger Technology: Where Technological Revolution Starts, Retrieved from: <https://101blockchains.com/distributed-ledger-technology-dlt/>

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash System, Retrieved from: [https://s3.amazonaws.com/academia.edu.documents/54517945/Bitcoin\\_paper\\_Original\\_2.pdf?AWSAccessKeyid=AKIAIWOWYYGZ2Y53UL3A&Expires=1552951723&Signature=ACwvVxb5CCnAUo4nhu8Tv1beiv8%3D&response-content-disposition=inline%3B%20filename%3DBitcoin\\_A\\_Peer-to-Peer\\_Electronic\\_Cash\\_S.pdf](https://s3.amazonaws.com/academia.edu.documents/54517945/Bitcoin_paper_Original_2.pdf?AWSAccessKeyid=AKIAIWOWYYGZ2Y53UL3A&Expires=1552951723&Signature=ACwvVxb5CCnAUo4nhu8Tv1beiv8%3D&response-content-disposition=inline%3B%20filename%3DBitcoin_A_Peer-to-Peer_Electronic_Cash_S.pdf)

Buterin, V. (2014). Ethereum white paper: a next generation smart contract & decentralized application platform. First version. Retrieved from: [http://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf)

Anwar.H, (2018b),The Ultimate Blockchain Technology Guide: A Revolution to Change the World, Retrieved from: (<https://101blockchains.com/ultimate-blockchain-technology-guide/>).

Alam. I,(2018), What are Ricardian Contracts? A Complete Guide, Retrieved from:

<https://101blockchains.com/ricardian-contracts/>

Grigg, I. (2000, February). Financial cryptography in 7 layers. In International Conference on Financial Cryptography (pp. 332-348). Springer, Berlin, Heidelberg. Retrieved from: [https://link.springer.com/chapter/10.1007/3-540-45472-1\\_23](https://link.springer.com/chapter/10.1007/3-540-45472-1_23)

Schwartz, D., Youngs, N., & Britto, A. (2014). The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 5. Retrieved from: [https://www.cryptiaexchange.com/Whitepaper\\_Ripple.pdf](https://www.cryptiaexchange.com/Whitepaper_Ripple.pdf)

EUBlockchain, (2019), Scalability,interopatibility, and sustainability of blockchains. Retrieved from: [https://www.eublockchainforum.eu/sites/default/files/reports/report\\_scalaibility\\_06\\_03\\_2019.pdf](https://www.eublockchainforum.eu/sites/default/files/reports/report_scalaibility_06_03_2019.pdf)