# BİLGEM TEKNOLOJİ

Ocak 2020 / Sayı:8

TÜBİTAK BİLGEM Kurumsal Dergisi. Dört ayda bir yayınlanır. Parayla satılamaz.


## Milli Güvenli Bulut Depolama Çözümü: Safir Depo

## Radar ve Elektronik Harp Uygulamaları

# Blokzincir Teknolojisi

## Yazılım Sektöründe Yerlilik ve Millilik

# Başkandan

## *Merhaba,*

TÜBİTAK BİLGEM 2010 yılında kuruldu. Gerçek ve tüzel her oluşumda yaşandığı gibi kuruluşumuz da bazı evrelerden geçmiştir. TÜBİTAK'ın 1963 yılında kurulması ve 5 yıl sonra Elektronik Araştırma Enstitüsü'nün faaliyete geçmesiyle aslında BİLGEM'in temelleri de atılmış oldu. Zamanla sayısı artan enstitüler, 2010 yılında BİLGEM çatısı altında bir araya getirildi. Bugünlere gelmemizde emeği olan herkesi minnetle ve şükranla yad ediyorum.

BİLGEM Teknoloji Dergimizin ilk sayısı Eylül 2009'da UEKAE adıyla yayınlanmıştı. Dergimizin de kurumumuz gibi bir geçmişi ve geleneği bulunmaktadır. Şimdi, kaldığımız yerden 8.sayımızla, yeni ismimizle, taze bir heyecan ve vizyonla sizlere tekrar merhaba demenin mutluluğunu yaşıyorum.

Eskiden olduğu gibi dört ayda bir yayınlayacağımız dergimizle neleri amaçladığımızı siz değerli okuyucularımızla paylaşmak istiyorum:

•Dergimizde BİLGEM'in ürettiği ya da ilgi ve faaliyet alanına giren bilgi ve teknolojilere yer vereceğiz. Dergimiz, siz değerli okuyucularımızla aramızda bir bilgi paylaşım aracı vazifesi görecek.

•Gelecekte bayrağı devredeceğimiz üniversite öğrencilerimize yönelik olarak bilişim alanında içerik oluşturacağız. Ayrıca BİLGEM'in kendi faaliyet alanında ne denli önemli, ulusal bir cazibe merkezi olduğunu kendilerine duyurma imkânı bulacağız.

•Akademik dünya ve iş paydaşlarımızı BİLGEM'de üretilen bilgi ve teknolojilerle ile ilgili daha çok haberdar edecek ve bilgilendireceğiz.

•Dergimiz çoğunlukla personelimizin yazı ve makalelerinden oluşacak. Böylece kurumumuzda üretilen bilgi ve teknolojilerle ilgili bir platform oluşturmuş olacağız.

Her sayıda, projelerimizin kümelendiği, bizim için önemli bir alanı kapak konusu olarak inceleyeceğiz. Bu sayıda Blokzincir teknolojisini ele aldık. Blokzincir, son dönemde ortaya çıkan önemli bir teknoloji ve birçok alanda iş süreçlerini köklü bir biçimde dönüştürmeye aday. BİLGEM'in, bu sahada Türkiye'de öne çıkan önemli bir merkez olduğunu belirtmekte fayda görüyorum.

Kurum olarak bu teknolojiye verdiğimiz önemin derecesi, bünyemizde 3 yıl önce oluşturduğumuz Blokzincir Araştırma Laboratuvarı ve ikincisini geçtiğimiz Eylül ayında düzenlediğimiz Ulusal Blokzincir Çalıştayımızdan anlaşılabilir. Ayrıca koordinatörü olduğumuz ve üniversitelerimizle işbirliği içinde oluşturduğumuz Blokzincir Araştırma Platformundan (BAĞ) bahsetmeliyim. BAĞ, alanla ilgili araştırmacıları biraraya getirip işbirlikleri kurmalarını sağlayan önemli bir platform olma misyonu taşıyor.

İlerleyen sayfalarda araştırmacılarımızın Blokzincir ve diğer bilişim konularında kaleme aldıkları birçok makale okuyacaksınız. Bu makalelerin literatüre de önemli katkıları olacağını düşünüyorum.

Gelecek sayıda buluşana dek sağlıkla kalın.

*Prof. Dr. Hacı Ali Mantar*

# İÇİNDEKİLER

















İletişim Adresi
BİLGEM Teknoloji Dergisi
P.K. 74, 41470 Gebze KOCAELİ

Telefon
(0262) 648 1000

Web
www.bilgem.tubitak.gov.tr

e-posta
bilgemteknoloji@tubitak.gov.tr

Baskı
San Ofset
Tel: (0212) 289 24 24

Baskı Tarihi
Aralık 2019
ISSN 1309-3444

Kısa Kısa

Bertuğ Kayhan - Uzman Yrd / BİLGEM İGBY

## TÜBİTAK BİLGEM Üniversite Öğrencileriyle Bir Araya Geliyor



TÜBİTAK BİLGEM proje yürütücüleri, üniversitelerin Bilgisayar Mühendisliği ve Elektronik Mühendisliği öğrencileriyle, BİLGEM'de yürütülen projelerden öğrencileri haberdar etmek ve mezuniyetleri öncesi ve sonrası muhtemel iş birliği imkânlarını konuşmak üzere bir araya geliyor. Bu kapsamda Ekim-Aralık 2019 döneminde, Yıldız Teknik Üniversitesi, Gebze Teknik Üniversitesi, Sabancı Üniversitesi ve Marmara Üniversitesi'nde BİLGEM Proje Tanıtım Günü düzenlendi.

Tanıtım günlerinde kriptoloji, görüntü kıymetlendirme, tümdevre tasarımı, bulut bilişim ve büyük veri, optik lazer ve e-kimlik alanındaki projelerimizle ilgili sunumlar yapıldı.

Düzenlenen tanıtım ve tanışma etkinliğinin devamı niteliğinde TÜBİTAK BİLGEM'e teknik geziler düzenlendi. Öğrencilerin ilgi alanlarına göre laboratuvarlar gezdirildi ve proje ekipleriyle bir araya gelmeleri sağlandı.

Üniversite öğrencilerine yönelik tanıtım etkinliklerimiz dönemsel olarak devam edecek ve programa daha çok üniversite dâhil edilecek.

## ATAM Anten Ölçüm Laboratuvarı Açıldı

TÜBİTAK Gebze Yerleşkesi'nde bulunan ve BİLGEM'e bağlı Anten Test ve Araştırma Merkezi laboratuvarlarında sürdüren Düzlemsel ve Silindirik Yakın Alan Anten Ölçüm Sistemi'nin açılışı gerçekleştirildi.

Açılışta, halihazırda Avrupa ve Ortadoğu'nun en büyük kapalı alan anten ölçüm sistemi olan laboratuvar katılımcılara tanıtıldı. Ardından yine BİLGEM bünyesinde geliştirilen Milli Gözetim Radarı anteniyle birlikte ilk ölçüm başlatıldı.

Açılışı yapan Başkanımız Prof. Dr. Hacı Ali Mantar, laboratuvarın sağlayacağı katma değerin çok büyük olacağına vurgu yaptı ve "Çalışmalar hem kurumumuzu hem ülkemizi kalkındıracak. Bu laboratuvar şu anda işin yüzde 25'i. Laboratuvarın sağlayacağı katma değer ile kalan yüzde 75'ini de gerçekleştirmiş olacağız." diye konuştu.






## Araca Monte Milli Lazer Sistemi (ARMOL) TSK Envanterine Girdi

TÜBİTAK BİLGEM tarafından milli olarak geliştirilen Araca Monte Lazer Sistemi (ARMOL), Ankara'da gerçekleştirilen geniş katılımlı kabul testlerinden başarıyla geçerek Türk Silahlı Kuvvetleri (TSK) envanterine kabul edilmeye hak kazandı. ARMOL, TSK'nın hizmetine sunulan Türkiye'nin ilk askeri standartlara uygun milli lazer sistemi oldu.

**ARMOL'ün Sağlayacağı Katkılar**

•ARMOL, yüksek güçlü lazer sistemi ile birlikte açık alanda yüksek çözünürlüklü görüntü alabilme yeteneğine sahip. Bu özelliği ile istihbarat amaçlı bilgi toplama, tehdidi önceden tespit edip etkisizleştirme süreci için gerekli planlamaları yapabilme imkânı sağlamaktadır.

• Düşman unsurların bilgi toplamak ve saldırı yapmak üzere kullanacağı drone ve termal kameraların oluşturduğu tehditleri etkisiz hale getirecektir.

•Tel kesme, demir, çelik gibi materyalleri tahrip edebilme yeteneği ile düşman tarafından hazırlanmış tuzakları uzaktan etkisiz hale getirerek askerlerimize büyük kolaylık sağlayacaktır.

• Ayrıca komuta kontrol sistemi ve lazer yönlendirme birimiyle entegre olarak çalışan ARMOL, envanterde bulunan belirli zırhlı araçlara monte edilebilecektir.

## TÜBİTAK Sözleşme Yönetimi Sempozyumu Yapıldı

TÜBİTAK BİLGEM ev sahipliğinde, TÜBİTAK'a bağlı kurumlar arasında düzenlenen Sözleşme Yönetimi Sempozyumu 2-3-4 Eylül 2019 tarihlerinde TÜBİTAK Gebze Yerleşkesi TÜSSİDE tesislerinde yapıldı.

Sözleşme yönetimi ile ilgili konularda TÜBİTAK kuruluşları arasında bilgi birikimi ve tecrübe paylaşımı yapılan sempozyumda, sözleşme yönetimi konularında birim temsilcilerinin, akademisyenlerin ve farklı sektörlerden profesyonellerin katılımıyla sunumlar ve panel oturumları gerçekleştirildi.

Programın açılış konuşması TÜBİTAK BİLGEM Başkanı Prof. Dr. Hacı Ali Mantar tarafından yapıldı. Programın ikinci günü, BİLGEM Başkan Yardımcısı Yusuf Çalık'ın "Proje Yönetimi ve Sözleşmesel Riskler" konulu sunumuyla başladı. Katılımcılara sözleşme hazırlama, müzakere ve saha uygulamaları hakkında bilgi veren Çalık, sözleşme risklerine değindi. Sempozyum, BİLGEM Sözleşme Birimi uzmanları tarafından Teknik Şartname, Sorumluluk ve Cezalar ile Fesih başlıklı eğitimlerin verilmesiyle devam etti.

Programın son gününde TÜBİTAK satın almalarının değerlendirilmesi başlıklı panel gerçekleştirildi. Sempozyum, BİLGEM Sözleşme Birimi ve Gerçekleştirme Bölümü uzmanları tarafından verilen eğitimlerle sona erdi. Sempozyumla TÜBİTAK ve enstitülerinin sözleşme görevlileri, diğer paydaşlar ve sektör yetkilileri arasında bilgi akışı köprüsü kurulmuş oldu.

# II. ULUSAL BLOKZİNCİR ÇALIŞTAYI GERÇEKLEŞTİRİLDİ


**"TÜBİTAK BİLGEM tarafından ikincisi düzenlenen Ulusal Blokzincir Çalıştayı, İstanbul Lütfi Kırdar Uluslararası Kongre ve Sergi Sarayı'nda 25-26 Eylül 2019 tarihlerinde gerçekleştirildi."**

Bertuğ Kayhan - Uzman Yrd. / BİLGEM İGBY

Çalıştayın açılış konuşmalarını, TÜBİTAK Başkanı Prof. Dr. Hasan Mandal, TÜBİTAK BİLGEM Başkanı Prof. Dr. Hacı Ali Mantar, TÜBİTAK BİLGEM İş Geliştirme Başkan Yardımcısı Orhan Muratoğlu, BORSA İSTANBUL Grubu adına Merkezi Kayıt Kuruluşu Başkanı Ekrem Arıkan, Blockchain Türkiye Platformu Yönetim Kurulu üyesi Barış Özistek yaptı. Çalıştaya katılan bürokrasi, iş ve akademi dünyasından binin üzerinde katılımcı ile Blokzincir konusunda Türkiye'nin en kapsamlı zirvesi gerçekleştirildi.


"Blokzincirde Dijital Kimlik" ana temasıyla düzenlenen 2. Ulusal Blokzincir Çalıştayı'nda, blokzincir teknolojisinin bireylerin, kurumların ve sektörlerin hayatını nasıl değiştirebileceği masaya yatırıldı. Çalıştayda ayrıca dijital kimlik konusunun teknik bileşenleri ve özellikle kişisel veri mahremiyeti ile ilişkileri detaylı olarak ele alındı. Yeni nesil dijital kimlik yönetim sistemi önerisi olarak TÜBİTAK liderliğinde, SSI Türkiye adı verilen dijital kimlik platformunun kurulması için çalışmaların başladığı bilgisi paylaşıldı.

TÜBİTAK Başkanı Prof. Dr. Hasan Mandal, Blokzincir teknolojisinin hem dünya hem de Türkiye için önemine ve geleceğin önemli teknolojisi olacağına dikkat çekti. TÜBİTAK olarak blokzincir alanındaki çalışmaların ve desteklerin artırılarak sürdürüleceğini belirtti.

Çalıştaya blokzincir teknolojisi alanında önemli çalışmalar gerçekleştiren duayen isimler de katıldı. Bu kapsamda, dijital kimlik alanında öncü kurumlardan Sovrin Vakfı Yönetim Kurulu Başkanı Dr. Phillip J. Windley, kimlik yönetimi ve yetkilendirme sistemlerinde 20 yıldan fazla deneyime sahip Birleşik Krallık Kent Üniversitesi'nden Prof. Dr. David Chadwick, blokzincir vizyoneri, mimarı ve geliştiricisi Michael Herman, güvenlik uzmanı olarak Sovrin'deki araştırma/geliştirme ve standartlaştırma çalışmalarını yöneten Mike Lodder katıldı.

Çalıştayda ayrıca, Michael Herman'ın "Kurumsal Mimarlar ve Geliştiriciler için Dijital Tanımlayıcı ve Kimlik Bilgilerinin Kullanımı" ve Mike Lodder'ın "Hyperledger Indy ve Aries ile Doğrulanabilir Referans Bilgileri Geliştirme" eğitimlerinin yanısıra Ethereum akıllı kontrat tabanlı uygulama geliştirme ve Hyperledger Fabric konularında uygulamalı eğitimler verildi.

Çalıştayda, üç ayrı seans ile akademik çalışmalar, eğitimler ve sektörden önemli konuşmalar eş zamanlı gerçekleştirildi. Katılımcılar İstanbul Lütfi Kırdar Uluslararası Kongre ve Sergi Sarayı fuaye alanında kurulan firma standlarını ziyaret ederek bilgi aldı.


Prof. Dr. Hasan Mandal

# BLOKZİNCİR



BLOKZİNCİR

# Blokzincir Teknolojsi

Taner Dursun - Başuzman Araştırmacı / BİLGEM UEKAE

> Blokzincir, kripto para olarak kendini göstermiş olsa da çok değişik amaçlarla kullanılabilecek bir teknolojik yeniliktir.

Kripto paralara olan ilgide yaşanan patlamadan sonra, altındaki teknoloji olan Blokzincir, her sektörde merak ve gündem oluşturmuştur. Buna rağmen Blokzincir, hala hem iş hem teknoloji alanlarından pek çok uzmanın bile doğru yorumlamakta zorlandığı bir kavramdır. Bu zorlukların temelinde, Blokzincir'in bir teknolojik buluştan farklı oluşunun yeterince anlaşılamaması ve gündeme gelişinin kendisinin bir uygulaması vasıtasıyla olması sebebiyle yaşanan karmaşa yatar [1]. Blokzincir, kripto para olarak kendini göstermiş olsa da çok değişik amaçlarla kullanılabilecek bir teknolojik yeniliktir. Aracılara olan ihtiyacı ortadan kaldırdığı için yıkıcı bir teknoloji olarak değerlendirilmektedir.

## Blokzincir Teknolojisini Doğuran İhtiyaçlar

Hayatımızdaki süreçler gün geçtikçe hızlanan bir şekilde sanal ortama taşınmaktadır. Bununla birlikte hala bazı süreçler sanallaştırılamamış veya kısmen sanallaştırılabilmiştir. Bu süreçler hala kâğıt, belge, doküman gibi varlıklar veya aracı kişi ve kurumların sürecin işleyişine dâhil olmasını gerektirmektedir. Bunun başlıca nedenlerinden birisi, gün geçtikçe sanal ortamda, kişisel mahremiyet kapsamına giren daha değerli bilgilerin işlenmeye başlanmasına karşın, artan siber tehditlerden dolayı, bireyler lehine gelişen kişisel veri koruma kanunlarının gereklerini yerine getirmede yaşanan zorluklardır. Ayrıca, sahipleri arasındaki güven eksikliği nedeniyle, süreçlerin alt parçalarının çalıştığı, farklı otoritelere ait bilgi işlem sistemlerinin birbiri ile çevrim-içi olarak bağlantılandırılmasına zorunlu olmadıkça da sıcak bakılmamaktadır.





Çünkü bu sistemleri, mahremiyet, güvenlik, güven ihtiyaçlarını karşılayacak şekilde birleştirebilecek teknolojiler henüz olgunlaşmamıştır. Bu nedenle birden fazla bilgi sistemini birlikte ilgilendiren gerçek dünya süreçlerini işletebilmek için, bu birbirinden kopuk sistemler arasındaki güven transferi, aracı kurumlar (noter, banka vb.) oluşturularak sağlanmaya çalışılır.

Bu durum devam ederken, 2008 küresel krizi, tüketicilerin, bankacılık, finans sektörü ve merkezi denetim kurumlarına karşı ciddi bir güven kaybı yaşamasına sebep oldu. Kriz ortamında, ilk kez, bir otoritenin sahipliğine ihtiyaç duymadan yaşayan, hiçbir merkezi sisteme bağlı olmadan çalışabilen, birbirine güven sorunu olan tarafların bile birlikte sorunsuzca kullanabileceği, manipülasyonlara karşı önlemler içeren bir örnek olarak Bitcoin [2] kripto para sistemi ve beraberinde Blokzincir kavramı doğdu. Hızla gelişerek küresel ölçüde kabul gören bir teknolojik kavrama dönüştü. Bitcoin ve diğer kripto paraların gösterdiği dayanıklılık, gereksiz aracıların sürecin içinden çıkması ile güvenlik, hız, maliyet artışlarının gerçeklenebilir olduğu görüşünün de yayılmasını sağladı. Blokzincir teknolojisi ile kripto para dışındaki alanlarda, benzer ihtiyaçları karşılamak üzere harekete geçilmesi uzun sürmedi. Bu ilgi öyle bir noktaya ulaştı ki blokzincir teknolojisi, matbaa, buharlı makinalar ve Internet devrimleri ile eş tutulmaya başlandı.

Aslında, literatüre bakıldığında, kripto paralar ile birlikte popüler hale gelen blokzincir teknolojisine ait fikrin ve yapı taşlarının, aslında kripto paralara özgü olmadığı, bu kavramlar ile ilgili çalışmaların çok daha öncelere uzandığı görülür. David Chaum'ın 1983 yılındaki makalesi [3] ve 1990 yılında kurduğu DigiCash adlı elektronik para firması, öncü çalışmalardandır. İlerleyen yıllardaki çalışmalarda, geriye doğru değiştirilemez veri depolama yapıtaşları geliştirilmiştir [4], [5]. 1997 yılında Adam Back'in tanıttığı hashcash e-posta spam ve DOS saldırılarını engelleme yöntemi, bugünkü pek çok kripto para sisteminde kullanılan bir yapıtaşıdır. 1998'de Nick Szabo, bitgold isimli, merkezi olmayan dijital para, Wei Dai ise b-money isimli başka bir kripto para çalışması yapmıştır. 2004 yılında, Hal Finney, değiştirilemez, özgün, Hashcash tabanlı, kişiden kişiye aktarılabilen RSA imzalı bir token oluşturmuştur. Nihayet, 2008 Aralık ayında, "Bitcoin: A Peer-to-peer Electronic Cash System"[2] başlıklı teknik yazı, Satoshi Nakamoto takma adlı yazar tarafından bir posta listesine gönderilmiş ve akabinde blokzincir teknolojisini dünyaya tanıtacak sistem çalışmaya başlamıştır. Blokzincir teknolojisinin üzerine inşa edildiği kriptografik bileşenler ve merkezi olmayan (decentralized) hesaplama sistemleri bileşenlerinin geçmişi de benzer şekilde eskilere dayanır.

## Blokzincirin Güven Problemine Getirdiği Çözüm

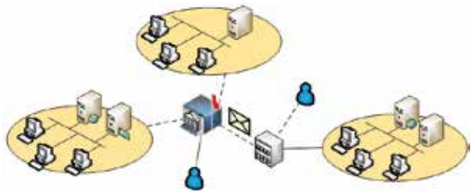
Günümüz bilişim sistemlerinde, dijitalleştirilmiş süreçlere ait otomasyonlar çalıştırılmakta, sürecin taraflarına ait bilgiler depolanmakta ve işlenmektedir. Bu süreçler genellikle merkezi sistemler üzerinde işletilmektedir (Örneğin; eposta sunucu üzerinden posta göndermek, para havalesi için bankaların sunucularının kullanılması vb.). Bu merkezi bilgi sistemleri kullanıcılarının, verilerin işlendiği sistemin sahibine duydukları güven sürdükçe, sistemdeki verilerin doğruluğu hakkında şüphe oluşmadıkça, sistemdeki veriler kaybolmadıkça ve üçüncü kişilerin eline geçmedikçe, bu sistemlerin bir otoritenin kontrolünde olması fazlaca dert edilmemektedir. Bununla birlikte, bu sistemler, kullanıcıları otoritelere bağımlı hale getirirken, depolanan verilere erişimde kesintiler, veri manipülasyonları, veri hırsızlıkları ve siber saldırılar gibi sorunlar da yaşanmaktadır.

> Blokzincir teknolojisi sayesinde merkezi yapılara, otoritelere ihtiyaç duymayan, manipüle edilemeyen, bozulmayan, erişim kesintisi yaşanmayan, güvenli bir veri kayıt sistemi kurmanın mümkün olduğu görülmüştür. Çünkü dijital verilerin sahipliğinin fiziksel dünyadaki varlıklar gibi el değiştirmesi mümkün hale gelmiştir.

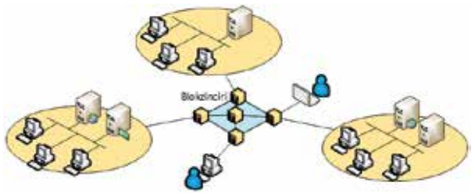
Bir diğer sorunlu konu ise sanallaştırılan süreçlerin işleyişinde gerekebilen, dijital verilerin sahipliğinin, gerçek dünyadaki gibi el değiştirebilmesi senaryolarının gerçekleştirilmesinde birden çok merkezi sistem, otorite ve aracıya bağımlı olunmasıdır. Üstelik bu transferlerde rol alan her bir alt bileşen, ayrı birer güven kaygı noktasıdır. Bu sistemler arasında güven ilişkisinin sağlanması gerekir. Kapsamı gittikçe genişleyen bu sistemlerde, birbirini tanımayan kişi ve yapılar arasındaki ilişkilerin kurallara bağlı hale getirilmesi ve süreçlerin bu kurallara göre işlediğinin, kişisel ilişkilerle oluşan güven duygusu ile değil sistemin kendisi tarafından garanti edilmesi gerekmektedir.

Kriptoloji teknikleri ile bu problemleri çözmek, ilk akla gelen seçenektir. Kriptoloji bilimi, daha çok veri mahremiyetini sağlamak, verinin bütünlüğünü teminat altına almak, veriyi gönderen kişinin kimliğini doğrulamak, inkâr edememezlik sağlamak gibi konularda kullanılmıştır. Varlığın fiziksel dünyadaki benzerleri gibi sahipliğinin el değiştirebilmesi, kriptografi açısından yeni bir uygulama alanıdır. Kriptografik bileşenler içeren Blokzincir teknolojisi sayesinde ise yukarıdaki problemlerin çözülebilmesi ihtimali ortaya çıkmıştır. Merkezi yapılara, otoritelere ihtiyaç duymayan, manipüle edilemeyen, bozulmayan, erişim kesintisi yaşanmayan, güvenli bir veri kayıt sistemi kurmanın mümkün olduğu görülmüştür. Çünkü dijital verilerin sahipliğinin fiziksel dünyadaki varlıklar gibi el değiştirmesi mümkün hale gelmiştir.

Blokzinciri teknolojisi, değer/varlık transferinde merkezi bir sunucunun veya güvenilir bir otoritenin varlığına duyulan ihtiyacı da ortadan kaldırır. Bunun yerine, verilerin kopyası birlikte çalışan binlerce bilgisayarda saklanır ve veriler üzerindeki değişiklikler, düğümler arasında bir mutakabat ile sağlanır. Bu şekilde herkesin doğrulama yapabildiği dağıtık bir veritabanı görüntüsü elde edilmiş olur. Blokzincir teknolojisinde, bir verinin başından geçen her değişiklik, şeffaflık sağlamak üzere, zaman damgalı olarak kayıt altına alınır. Kayıt güncelleme işlemi, sisteme dâhil olan tarafların mutabakatı ile yapılır. Tarafların birbirini tanıması gerekmemektedir. Sistemin paydaşları arasındaki güven, depolanan veriler üzerindeki değişikliklerin, sistemin en başta belirlenmiş kurallarına uyumlu olarak yapılabilmesinin sağlanması, bu değişikliklerin, içeriği şeffaf olan ve kriptografik teknikler ile korunan bir kayıt zincirinde yazılması, bu kayıt zincirinin kopyalarının taraflarda tutulması ile sağlanır.



a)Güven sorunu nedeniyle aracılar üzerinden entegrasyon




b)Blokzinciri üzerinden güven tabanlı entegrasyon

*Şekil 1 Blokzincirin süreçlerin hayata geçirilmesindeki rolü*

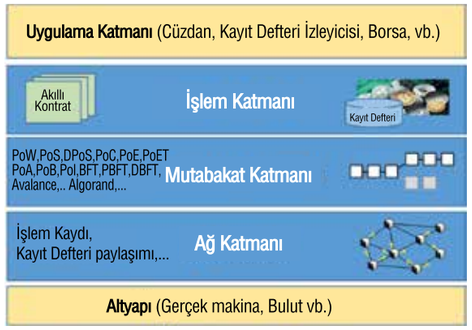
Şimdiye kadar irtibatlandırılmayan mevcut sistemler, artık paydaşı oldukları süreçleri çevrim-içi olarak birlikte gerçekleştirmek üzere, Şekil 1'de gösterildiği gibi, bir blokzincir üzerinden güvenli ve şeffaf bir şekilde irtibatlanabilirler.

## Blokzincir Mimarisi ve Yapıtaşları

Bitcoin'in devrim niteliğinde bir teknoloji olmasını sağlayan en önemli etken, ekonomi, para teorisi, oyun teorisi, bilgisayar bilimi ve kriptoloji disiplinlerinden bileşenleri bir araya getirmiş olmasıdır. Bir blokzincir sisteminin mimarisi temel olarak beş katmanda ele alınabilir:

- Altyapı, blokzincirin düğümlerini oluşturan gerçek veya bulut üzerinde oluşturulmuş bilgisayarlardır. Mutabakat işlemlerinden dolayı, altyapıda genellikle çok çekirdekli bilgisayarlar, GPU, FPGA ve ASIC tabanlı yüksek işlem gücüne sahip donanımlar kullanılır.

- Ağ katmanı, yaygın olarak Gossip protokollerinin [6] kullanıldığı, blokzincir düğümleri arasında hızlıca yayılması, eş düğümlerin bulunması, blokzincir verisinin indirilmesi, blokların ağda yayımlanması işlemlerinin yerine getirildiği seviyedir.
- Mutabakat katmanı, blokzincir düğümlerinin, kendi aralarında, kayıt defterinde doğru ve tutarlı veri yazılmasını garanti altına almak üzere işlettikleri uzlaşma protokollerinin bulunduğu katmandır. Blokzincir'in değiştirelemezliğini sağlayan, kuraldışı transferleri engelleyen hayati bileşendir.




- İşlem (Transaction) katmanı, blokzincirin üzerinde oluşan bilgileri ve bu bilgiler üzerinde güncelleme yapan akıllı kontratları, yapılan güncellemelere ait kayıtları barındırır. Veri katmanı olarak da isimlendirilebilir.
- Uygulama Katmanı, blokzincir üzerinde veri üretme, depolama ve sorgulama yapan uygulamaların bulunduğu katmandır.

## Kriptografik Yapıtaşları

Bir blokzincir platformunun ekosisteminde, sistemden farklı şekilde yararlanan, birbirine güvenmek zorunda olmayan, madenci, onay düğümü sahibi, geliştirici, kullanıcı, yatırımcı, borsa sahibi gibi aktör türleri bulunur. Bu aktörlerin kendi çıkarlarını korumak ve maksimize etmek amacıyla hareket etmesi, sistemin güvenliğini de otomatik olarak sağlar. Buna olanak sağlamak için çeşitli kriptografik bileşenler kullanılır. Kripto paraların ismi, işleyişlerini iki kriptografik yapıtaşına (özet ve elektronik imza) borçlu olmasındandır. Blokzincirlerde kullanılan kriptografik bileşenler, kullanım amaçlarına göre iki gruba ayrılabilir:

- Blokzincir sisteminin kendi güvenliğini sağlayanlar (İmza, özet)
- Blokzinciri kullanıcıları ve verileri için mahremiyet ve anonimlik sağlama amaçlı olanlar (özel imzalar, sıfır bilgi ispat protokolleri, akümülatörler, homomorfik şifreleme, çok taraflı kriptografi vb.)

## Mutabakat Protokolleri

Blokzincir platformunun karakteristiğini oluşturan ve kayıtların bütün düğümlerde aynı şekilde güncellenebilmesini sağlayan bileşendir. Blokzincir ağ bilgisayarlarının kötü niyetli davranabileceği varsayılır. Sistemin bileşenlerinden bazılarının kötü niyetli davranması ile ortaya çıkan arıza türleri, Byzantian Failures/Faults olarak bilinir. Blokzincirlerinde bu tür hataları bertaraf ederek verinin bütün kopyalarının birbiri ile aynı olmasını sağlamak için mutabakat protokolleri kullanılır. Protokollerin çalışma prensibi, genelde çeşitli yetkinliklerine veya özniteliklerine göre (işlem gücü, kripto para miktarı, kimliği, depolama alanı vb.) düğümlerin, ortak kararların alınmasında farklı seviyede söz hakkı almasına dayalıdır. Bilinen yetmişten fazla mutabakat protokolü vardır [9].

> "Bitcoin'in devrim niteliğinde bir teknoloji olmasını sağlayan en önemli etken, ekonomi, para teorisi, oyun teorisi, bilgisayar bilimi ve kriptoloji disiplinlerinden bileşenleri bir araya getirmiş olmasıdır."

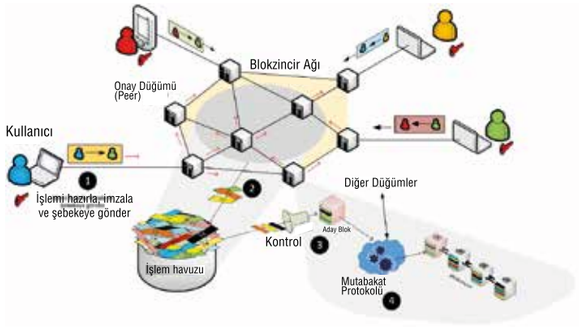
## Akıllı Kontratlar

Akıllı Kontrat (Smart Contract) fikrini 1994 yılında ilk ortaya atan, Nick Szabo'dur. Sözleşmelerin, bilgisayar kodu haline dönüştürülmesi, saklanması ve sistem üzerinde kopyalanması ve blokzinciri çalıştıran bir bilgisayar ağı denetiminde, birçok alanda kullanılabileceği fikrinin ilk örneği Bitcoin'dir. Bununla birlikte, Bitcoin blokzincirin üzerinde depolayabileceği veri yapıları ve üzerlerinde tanımlanabilecek iş kuralları sınırlıdır. Bu sınırlamayı aşmak üzere, Ethereum Foundation, 2014 yılında, akıllı kontrat yeteneği içeren kripto para platformunu ortaya çıkardı. Bu platformda, akıllı kontrat adı verilen program parçalarının içinde tanımlanan kurallara göre eylemler gerçekleştirebilmek mümkündür. Akıllı kontratların kendi hesap adresleri vardır ve içlerinde kripto para tutabilirler. Diğer akıllı kontratlar ve kullanıcı hesapları ile etkileşebilirler. İçlerinde, blokzincirin güvenlik yapısı ile koruma altına alınmış veriler depolayabilen, kopyası her bir blokzincir düğümü üzerinde çalışan, izinsiz olarak durdurulamayan ve değiştirilemeyen kodlar bulunur.

İzleyen yıllarda, Cardano, Hyperledger Fabric, Corda, Quorum gibi, akıllı kontrat destekleyen pek çok blokzincir platformu geliştirilmiştir. Diğer blokzincir türleri, kripto para olarak etkileşim platformu sunarken, akıllı kontrat destekleyen blokzincir türleri ise bunun yanında, güvenilir üçüncü tarafa (merkezi sunuculara ve otoritelere) ihtiyaç duyulmadan, iş mantığı ve işleyişi şeffaf bir şekilde izlenebilen uygulamaları çalıştırma yeteneği sunmaktadır. Bu sayede, blokzincirin para transferi dışında pek çok sektörde kullanımının önü açılmıştır.

## Blokzincirin İşleyişi

Blokzincir sisteminde olaylar, mevcut veriler üzerinde bir güncelleme isteğinin (para aktarma, bir dijital verinin sahipliğini devretme, ortak veriyi güncelleme vb.), kullanıcı tarafından İşlem (Transaction) olarak hazırlanıp, kendisinin ulaşabildiği blokzincir ağının düğümlerinden birisine göndermesi ile başlar (Şekil 2). Kullanıcı bu işlem isteğinin içine, sistemin iş mantığının gerektirdiği kriptografik bileşenleri de (imza, bazı kanıtlar vb.) koymuş olmak zorundadır. Blokzincir ağına aynı anda pek çok kullanıcı, farklı düğümler üzerinden İşlem isteği gönderir. Bu istekleri alan Blokzincir düğümleri, istekleri, kendi komşu düğümlerine yaymak zorundadır. Ağ içinde düğümden düğüme yayılan İşlemler, bazı kontrollerden (gönderenin imzası, kayıt defteri içeriği ile uyumu vb.) geçtikten sonra, sistem genelindeki her düğümde kopyası olan sanal bir İşlem




*Şekil 2: Blokzincir sisteminde veri güncelleme akışı*

Havuzu'nda toplanır. Düğümler, bu işlem havuzundaki işlemleri, diğer düğümler ile işbirliği içinde (mutabakat protokolleri ile) işleyerek, Kayt Defterinin (Blokzinciri), bütün düğümlerde bulunan kopyalarını aynı yapacak şekilde günceller. İşlem havuzundan alınan işlemlerin, öncelikle kayıt defterinin mevcut içeriği ile uyumlu bir istek taşıdığı doğrulanır (işlem yapılmak istenen veri gerçekten var mı ve bu işlemi yapmaya uygun bir durumda mı, işlemi yapmak isteyen kullanıcı bu işlemi yapmaya yetkili mi, vb.).

Bu kontrolleri geçen işlemlerden (sistemden sisteme değişkenlik gösteren sayı ve miktarda) bir kısmı, kayıt defterine eklenmek üzere Blok haline getirilir. Üretilen bu Blok'un kayıt defterine eklenebilmesi için, diğer onay düğümlerini de kapsayan bir mutabakat protokolü çalışır. Mutabakata ulaşılırsa, bu yeni blok, kayıt defterinin en taze zincir halkası olarak herkes tarafından kayıtlara eklenir. Diğer düğümler de işlem havuzlarından, bu blok içindeki işlemleri (artık işlenmiş oldukları için) silerler.

Madenci düğümleri, sürekli olarak blok üretme işi ile meşguldürler. Örneğin Bitcoin vb. blokzincirlerde PoW (Proof-of-Work) tabanlı mutabakat protokolü işletilir [3]. Herhangi bir madenci bilgisayarının, İşlem havuzunu kullanarak hazırladığı aday bloğu, sisteme yeni güncelleme olarak önerebilmesi ve diğer düğümlerce de kabul görmesi için, sistemin o anki zorluk derecesine uygun olarah hash bulmacasını çözmesi gerekir (Bkz. Mutabakat Protokolleri). Hash bulmacası çözülen aday blok, diğer düğümlere de bildirilir.

## Blokzincir Platformları

Açık kaynak kodları ile kullanılabilecek hazır durumda çeşitli Blokzincir platformları vardır. Blokzincir platformları, blokzincir verilerine erişilebilirliğine ve

blokzincir bilgisayarlarını kimin işlettiğine bağlı olarak alt sınıflara bölünmektedir. Açık (Public) blokzincir ağına isteyen herkes katılabilir. Bitcoin ve Ethereum bu türün en çok bilinen örnekleridir. Özel (Private) blokzincirlerinde ise ağa yeni düğümlerin katılımı, ağın kurucularının daveti ve/veya tanımladıkları kurallara göre olabilir. İzinli (permissioned) blokzincir ise Açık ve Özel tipler arasındaki bir hibrit türdür. Her isteyenin girebildiği veya tek bir otoritenin onayı ile ağa dâhil olduğu senaryolar yerine, sınırlı sayıda, önceden belirlenmiş düğüm bulunur. Konsorsiyum (consortium) veya federe (federated) blokzinciri adı da verilir (Örnek Ripple). Mutabakat süreci, önceden seçilmiş düğümler tarafından işletilir. Kullanıcıların hangi tip işlemi (transaction) gerçekleştirebileceği düzenlenebilir.

Bitcoin en çok bilinen kripto para odaklı blokzincir platformudur. Bitcoin platformu üzerinde, amacı kripto para transferinden başka olan yeni özel sistemler oluşturmak için, işlem kayıtları içinde zaman damgası ile depolanan, çeşitli iş senaryolarına ait bilgileri tutmaya dayalı yöntemler kullanılmaktadır.

Ethereum, kripto para olarak kullanılmanın yanında, uygulama geliştiricilerin kendi, merkezi olmayan uygulamalarını geliştirmesine ve çalıştırmasına da olanak ve akıllı kontrat desteği sağlayan açık blokzincir sınıfından bir platformdur. Ethereum, kurumsal dünya içerisinde özel (private) blokzincir yapılarının oluşturulmasında da kullanılabilir. Bu kapsamda "Kurumsal Odaklı Ethereum" olarak nitelendirdiği Quorum adlı platform geliştirilmiştir. Quorum, düğümler üzerindeki Enclave adı verilen kripografik donanım bileşenleri sayesinde, içeriği gizlenebilen işlemler yapılmasına da imkân sağlar.

Hyperledger, Linux Vakfı tarafından Aralık 2015'te başlatılan açık kaynak kodlu bir blokzincir platformudur. Hyperledger kapsamındaki projelerin en bilinenlerinden olan Hyperledger Fabric blokzincir platformu, pek çok kurumsal dönüşüm projesinde kullanıllan izinli bir blokzinciri platformu türüdür. Aynı çatı altında geliştirilmeye devam edilen Hyperledger Indy blokzincir platformu ise merkezi olmayan dijital kimlik yönetimi konusunda özelleşmiş, izinli blokzincir türüdür.

Ripple, temel olarak gerçek zamanlı bir uluslararası para gönderim/ödeme amaçlı blokzincir platformudur. R3 firması liderliğindeki konsorsiyum tarafından geliştirilen Corda platformu, işletmeler arasında yasal sözleşmeleri kaydetmek, yönetmek ve otomatikleştirmek ve finansal piyasalardaki uygulamalara çözümler sunmak için tasarlanmıştır.

## Blokzinciri Teknolojisinin Sorunları

Blokzinciri teknolojisi olgunlaşmakta olan yeni bir teknoloji olması nedeniyle çeşitli konularda çözülmesi gereken problemlere veya iyileştirmelere ihtiyaç duyar. Aşağıdaki maddelerin çoğunda sorun giderici veya azaltıcı çalışmalar zaten yapılmaktadır:





**Mahremiyet (Privacy).** Blokzincirin kayıt defterinde, kimlerin ne zaman işlem yaptığı ve üzerinde işlem yapılan verilerin bütün hayat hikâyesinin izlenebilir olması, mahremiyet açısından istenen özellik değildir. Kripto para blokzincirlerinin büyük çoğunluğunda işlemler herkes tarafından izlenebilir. Hesapların anonim olması yeterli değildir, ifşa olduğunda, geçmiş ve gelecek tüm hareketler de ifşa olabilmektedir. Burada hareketlerin otoritelerce izlenememesi, vergilendirilememesi ve illegal işlerde kullanılma ihtimali vb. nedenlerle mevcut düzene uygun olmadığı kabul edilir.

**Kanun ve Düzenlemelerle Uyum Sorunları:** Kişisel verilerin blokzinciri üzerinde depolanması durumunda, bütün düğümlerin erişimine açılması, özellikle kripto para blokzincirlerinin, ülkelerin politikaları ile uyumu konusu henüz tamamlanmamıştır.

**Ölçeklenebilirlik:** Depolama alanı, haberleşme ve işlem hızı açısından ölçeklenebilirlik bariyerleri vardır. Sürekli büyüyüyen kayıt veritabanı boyu bir sorun teşkil etmektedir. Blokzincirler, mutabakat algoritmaları ve kriptografi yoğun işlemler nedeniyle, günümüzde kullandığımız ödeme sistemlerinin işlem hızından çok daha yavaş bir hıza sahiptir.

**Maliyet, Elektrik Tüketimi:** PoW tipli mutabakat algoritması kullanan kripto para platformları, yüksek elektrik tüketimine sebep olurlar. Örneğin Bitcoin platformu, bir ayda Dünya elektrik tüketiminin %0,3'ünü tek başına gerçekleştirir.

**Siber Tehditler:** Her ne kadar blokzincir düğümlerine saldırılar sınırlı olsa da blokziniciri kullanan dış uygulamalara yönelik siber saldırılar görülmektedir. Cüzdanlardan özel anahtar çalma ve hesap adreslerinin gerçek kişilerle ilişkilendirilebilmesi için ağ izlemesi gibi saldırılar yaşanmaktadır.

**Entegrasyon:** Blokzincir platformlarının geleneksel uygulamalarla ve başka blokzincirleri ile entegrasyonu konusunda hala alınacak çok yol vardır.

**Kullanım Zorluğu:** Sıradan kullanıcıların, kriptografi terimlerini bilerek blokzincirin karmaşık detaylarının farkında olarak kullanması oldukça zordur.

**Quantum Bilgisayar Tehditi:** Kriptografik işlemelere ait izler, her düğüm üzerinde depolandığı için, gelecekte kuantum bilgisayarın hayata geçmesi durumunda, hem geriye doğru bilgilerin deşifre edilmesi hem de varlıkların izinsiz el değiştirebilmesi olasıdır.

**Kanuni Engeller:** Blokzincirin aracıları kaldırarak yerine geçebilmesi için pek çok kanuni düzenlemenin de yapılması gerekmektedir. Örneğin çoğu ülke kanunlarında kripto paraların hangi değer tipi (para, değerli mal, hisse senedi, döviz vb.) olduğu bile tanımlı değildir.

## Blokzinciri Teknolojisinin Geleceği

Blokzinciri teknolojisinin, her kullanım senaryosu ve iş modeli için uygun olduğunu söylemek doğru olmaz. Yönetilecek verinin üzerinde işlem yapan aktör sayısı ve aralarındaki güven ilişkileri irdelenerek bu teknolojinin kullanımına karar verilmelidir. Anlam ve değer içeren herhangi bir varlığın, herhangi bir aracıya ihtiyaç duymadan, güvenli bir şekilde kaydının tutulması ve bu kayıtların sahipliğinin paylaştırılması veya aktarılması ile birlikte, bugüne kadar henüz keşfedilmemiş çok farklı iş modelleri üzerinde çalışmalar devam etmektedir [7],[8].

Öncelikle finansal teknolojiler alanında yorumlanıp değerlendirilmiş olsa da başka pek çok uygulama alanı olacağı görülmektedir. Halen çalışılan uygulama alanları arasına sürekli olarak yenileri eklenmektedir. Günümüzde birçok kurum yeniden kurgulanan kullanım senaryolarıyla ilgili Ar-Ge süreçlerini ve pilot çalışmalarını sürdürmektedir. Blokzincir teknolojisi, yeni uygulama alanları, yeni teknolojik bileşenler ile kendi ekosistemini genişletmeye ve giderek büyüyen kitleler tarafından benimsenmeye devam etmektedir.

*REFERANSLAR*

*[1] Blockchain İçin Kavramsal Mimari, Blockchain Türkiye Platformu Teknoloji Çalışma Grubu Raporu, Mayıs 2019*

*[2] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf, Aralık 2008*

*[3] Blind Signatures for Untraceable Payments, Chaum, David, Advances in Cryptology Proceedings. 82 (3), pp. 199–203, 1983*

*[4] How to Time-Stamp a Digital Document, Stuart Haber, and W. Scot Stornetta, In Advances in Cryptology – Crypto '90, pp. 437–455. LNCS V. 537, Springer-Verlag, 1991.*

*[5] The Eternity Service, Ross J. Anderson. Pragocrypt 1996.*

*[6] Epidemic Algorithms for Replicated Database Maintenance, Demers, Alan; Greene, Dan; and Terry, Doug. Proceedings of the Sixth Annual ACM Symposium on Principles of Distributed Computing. PODC '87, pp. 1–12. doi:10.1145/41840.41841*

*[7] Andreas Antonopoulos Mastering Bitcoin, https://goo.gl/fofWQe, Temmuz 2014.*

*[8] Credit Suisse. Blockchain 2.0, https://goo.gl/GB5ekM, 11 Ocak 2018.*

*[9] Major Blockchain Consensus Algorithms, https://www.tokens-economy.com/2019/06/19/major-blockchain-consensus-algorithms-infographics-version-2019-6/*

# Blokzincir
# UYGULAMA ALANLARI

> "Blokzincir, Bitcoin adlı kripto para sayesinde, dünyanın her tarafından insanların ilgisini üzerinde toplamayı başardı."

Bilal Kılıç – Başuzman Araştırmacı / BİLGEM TDBY

Blokzincir, birkaç yıl önce Bitcoin adlı kripto para bir başka ifadeyle dijital para birimi olarak anılan varlık sayesinde, dünyanın her tarafından insanların ilgisini üzerinde toplamayı başardı. Daha sonra anlaşıldı ki, bu teknoloji, özellikle finans ve kamu başta olmak üzere pek çok alanda, çok büyük değişimlere yol açacak, birçok işletme ve kamu kurumunun işlevini yitirmesine, ortadan kalkmasına veya dönüşmesine yol açacaktır. Geleneksel yöntemlerle verilen hizmetler ve yapılan işler, hem yavaş, hem maliyetli, hem de hataya açıktır. Buna karşılık blokzinciri teknolojisi, daha ucuz, daha şeffaf, daha hızlı ve daha etkili çözümler ortaya koymaktadır. Blokzincir uygulamalarının, 2030 yılına kadar yaygınlaşacağı, devletlerin çoğunun digital paraya geçiş yapacağı, dünya ticaretinin büyük bir kısmının bu platform üzerinde yapılacağı tahmin edilmektedir. Blokzinciri ve akıllı sözleşmeler kullanılarak aşağıdaki alanlarda uygulamalar yapılması mümkündür. Bu uygulamalardan ve gerçekleştiren öncü firmalardan örnekler vereceğiz.

## Uluslararası Ödemeler ve Bankacılık Sistemi

Finans kurumları üzerinden gerçekleştirilen para transferleri, hem daha uzun zaman almakta, hem de yüksek maliyetler içermektedir. Ayrıca yasal düzenlemeler ve mevzuat nedeniyle de bir takım engeller ve zorluklarla karşılaşmakta mümkündür. Blokzincir teknolojisi ve akıllı sözleşmeler kullanılarak, bu ödemelerin daha hızlı ve daha ucuz bir şekilde yapılması söz konusudur. "Barclays" bankası ve daha birçok banka, varlığını devam ettirebilmek ve teknolojik gelişmelere ayak uydurabilmek için, blokzincir ile ilgili projelere yatırım yapmaktadır.

## Kripto Para (Dijital Para)

Blokzincir teknolojisinin ilk uygulama alanı, finans sektöründe dijital paralar ile olmuştur. Bitcoin en çok konuşulan ve en çok bilinen kripto para, yani dijital paradır. Bitcoin den sonra binlerce altcoin de, dijital para olarak sahneye çıkmıştır. Zaman içerisinde muhtemelen fiziksel paranın yerini dijital para alacaktır. Kripto paralar, şu an itibariyle, herhangi bir finansal düzenlemeye tabi değildir. Muhtemelen yakın bir gelecekte pek çok ülke, merkez bankaları üzerinden, blokzincir altyapısını kullanarak, kendi dijital paralarını çıkaracak ve yöneteceklerdir. Blokzincir platformu üzerinde geliştirilen yatırım uygulamaları sayesinde, para havale edilebilir, hisse senedi alınabilir. Hatta bazı işletmelerden ürün ve hizmet satın alınabilir. "Abra" firması bu konu ile ilgili çözüm üretmiştir. "Takasbank" kurumunun geliştirdiği "BİGA" projesi de, dijital ortamda altın alışverişine olanak sağlayacaktır.

## Askeri Güvenli Haberleşme

Askeri güvenli haberleşme, kriptolu yani şifreli olarak yapılır. İletilen bilginin, gizliliği, bütünlüğü, doğru kaynaktan mı geldiği, doğru adrese mi gittiği, inkar edilemezliği, anonim olması, mahrem olması ve güncel olması gibi özellikleri sağlaması gerekir. Blokzincir teknolojisi sayesinde bu şartları daha kolay ve daha güvenli bir şekilde sağlamak mümkündür.

> Geleneksel yöntemlerle verilen hizmetler ve yapılan işler, hem yavaş, hem maliyetli, hem de hataya açıktır. Blokzincir teknolojisi, daha ucuz, daha şeffaf, daha hızlı ve daha etkili çözümler ortaya koymaktadır.

## Tedarik Zinciri Yönetimi

Tedarik zincir yapıları karmaşık ve zor süreçleri içerir. Bu durum kontrolü zorlaştırır. Süreyi ve maliyeti artırır. Verimliliği azaltır. Blokzincir teknolojisi kullanılarak, tarladan müşteriye, imalattan satışa kadar geçen her el değişiminde, ürün ile ilgili işlemler kalıcı, belgelenebilir ve dağıtık bir şekilde kaydedilir. Akıllı sözleşmelerden faydalanarak, iş akışları otomatik olarak gerçekleştirilir. Ayrıca ürünün tüm yaşam döngüsü ve yapılan işlemleri müşteri tarafından izlemek mümkün olur. Böylece şeffaflık artar, süre, maliyet, insan hatası ve israf azalır. "Blockverify", "Everledger", "Openport", "Shipchain", "SyncFab" vb. pek çok firma bu alanda çözümler üretmiştir.

## Talep Tahmini

Blokzincir ve akıllı sözleşmelerin kullanılması ile tüm iş ve işlemlerin doğru bir şekilde kayıt altına alınması sağlanır. Böylece çok sayıda istatistiki veriyi elde etmek, yorumlamak, analiz etmek ve müşteri ihtiyaç ve talepleri ile ilgili isabetli tahminlerde bulunmak mümkün olur. "Augur" firması, Ethereum Blokzincir platformu üzerinde, gerçek zamanlı ve dağıtık olarak çalışan, global piyasalar için talep tahmini yapan protokoller geliştirmiştir.

## Perakende Sektörü

Perakende sektöründe tüketiciler, marketlere ve mağazalara bağımlı kalmaktadır. Blokzincir teknolojisini kullanarak, bu bağımlılığı ortadan kaldırmak, yani tüketiciler ile üreticileri doğrudan, aracısız bir şekilde buluşturmak ve ayrıca aradaki aracılardan kaynaklanan masrafları ortadan kaldırmak mümkündür. Alışverişte güven unsuru, akıllı sözleşmeler ile sağlanır. "openbazaar" ve "ob1" firmaları bu alanda çalışmalar yapmıştır.

## Sigorta İşlemleri

Günümüzde sigorta tazmin sürecinde, zaman kaybı, maliyet, hatalı işlemler, sahtekarlık ve tekrarlanan işlemler gibi pek çok zorlukla karşılaşılmaktadır. Blokzinciri teknolojisi kullanılarak, insan etkisini en aza indirecek şekilde, süreci neredeyse tamamen otomatikleştirmek mümkün olur. Böylece işleyiş daha hızlı, daha güvenli ve daha az maliyetli hale gelir. "Oracle", sigortacılık sektörü için, blokzincir platformu üzerinde çalışan, "AETERNITY" adı verilen bir çözüm geliştirmiştir.

## İnşaat-Emlak

İnşaat Emlak sektöründe, satın alma veya satış yaparken karşılaşılan zorluklar bürokrasi, şeffaflık eksikliği, kayıtlardaki yanlışlıklar ve sahtekarlıklardır. Blokzincir teknolojisi kullanarak gerek kayıtlar ve gerekse alım satım işlemleri, elektronik ortamda olacağı için, işleri hızlı ve güvenli bir şekilde yürütmek mümkün olur. Mülkiyetin sahipliği emin bir şekilde doğrulanmış ve tapu devir işlemi de güvence altına alınmış olur. "Ubitquity" firması, bu alanda çözüm geliştiren firmalardan birisidir.

## Şans Oyunları

Blokzincir teknolojisi kullanarak, dağıtık yapıda, spor başta olmak üzere pek çok alanda, şans oyunları oynamak mümkün olur. Bu sistemde, manipülasyon ve insan hatası ihtimali, geleneksel uygulamalara göre çok daha azdır.

## Nesnelerin İnterneti (IoT)

IBM ve Samsung firmaları, cihazların internet üzerinden güvenli bir şekilde haberleşmesini sağlayabilmek için, blokzincir platformunu kullanan, "otonom, dağıtık ve uçtan uca telemetri" (ADEPT) olarak bilinen, çok sayıda cihaz için kamu defteri işlevi görecek bir sistem geliştirmiştir. İşlemlerin güvenliğini sağlayabilmek için de, mutabakat yöntemi olarak, "emeğin ispatı" ve "sahipliğin ispatı" yöntemlerini kullanmıştır. Böylece, merkezi bir sisteme ihtiyaç duymadan, dağıtık yapıda, bütün cihazlar birbiri ile otonom bir şekilde haberleşebilmekte, hataları yönetebilmekte ve enerji kullanımını izleyebilmektedir.

## Özel Taşımacılık Sektörü

Blokzincir teknolojisi ile, dağıtık yapıda, kişiden kişiye, araç paylaşım uygulamalarını kullanabilmek mümkün olur. Bu işlem, araç sahipleri ile araç talep edenler arasında akıllı sözleşmeler ile güvenli bir şekilde ve aracısız olarak yapılabilir. Buna örnek olarak, "Arcade City" ve "La'zooz" firmalarının uygulamalarını verebiliriz. Bu uygulama ile araçlar daha dolu olarak seyreder. Yakıt ve emek sarfiyatı azalır. Akıllı sözleşmeler ile, otoyol ücreti, park ücreti ve benzin ücreti de, otomatik olarak ödenir. Bunun için "UBS", "ZF" ve "INNOGY" gibi firmalar, Blokzinciri tabanlı uygulamalar geliştirmektedir.





## Veri Depolama

Günümüzde veriler, merkezi sunucu sistemlerinde depolanmaktadır. Merkezi sunucu sistemleri ise, insan hatalarına, siber saldırılara ve veri kayıplarına karşı zayıflıklar içerir. Blokzincir teknolojisi ise, saldırılara karşı daha güvenli ve dayanıklı olan bulut yapısında veri depolamayı sağlar. Veri önce şifrelenir, daha sonra parçalara ayrılır ve ve düğüm noktalarına gönderilir. "Storj" firmasının bu alanda çalışmaları vardır.

## Kredi Uygulamaları ve Girişim Sermayesi Temini

Blokzinciri platformunda, akıllı sözleşmeler kullanarak, aracı kurumları devreden çıkararak, bireylerin birbirine doğrudan kredi vermesi mümkün olur. Aynı şekilde, sendikasyon kredilerini ve mikro kredilerini de, bu sistem ile dağıtmak ve yönetmek mümkündür. Bunlardan farklı olarak, fon sağlamak amacıyla, blokzincir alanında faaliyet gösteren pek çok firma, "Token" adı verilen varlığı, yatırımcılara ihraç ederler. Firmalar bu sayede milyonlarca TL girişim sermayesi elde edebilirler. Altcoin'lerin birçoğu bu şekilde fon tedarik etmektedir.

## Müzik ve Telif Hakları

Müzik endüstrisi sektöründe, telif hakları sıklıkla göz ardı edilir. Blokzincir platformu ve akıllı sözleşmeler kullanarak, kapsamlı, doğru ve dağıtık yapıda bir veri tabanı oluşturarak müzik dinleyen hayranların, müzisyenlere doğrudan ödeme yapabilecekleri altyapıyı kurmak mümkündür. "Mycelia" ve "ujo music" firmaları bu alanlarda çalışmalar yapmaktadır.

## Kamu Yönetimi

Kamu yönetimi, doğası gereği yavaş, hantal ve yolsuzluğa açıktır. Blokzinciri teknolojisi kullanarak,

> Blokzincir teknolojisinin ilk uygulama alanı, finans sektöründe dijital paralar ile olmuştur.

Kamu'daki işlerin şeffaflığını, güvenilirliğini ve verimliliğini artırmak ve bürokrasiyi azaltmak mümkündür. Birleşik Arap Emirlikleri, 2021 yılına kadar, hükümetin yaptığı işlerin yarısını Blokzincir platformu üzerine planlamaktadır. Tüm iş ve işlemler, blokzincir platformuna alındığı takdirde, zamandan, paradan ve işgücünden önemli ölçüde tasarruf elde edilebileceği ve ayrıca vatandaşın hayat kalitesinin ve mutluluğunun artacağı düşünülmektedir. "Consensys" isimli blokzincir firması, bu konularda BAE'ye danışmanlık hizmeti vermektedir.

## Dijital Kimlik

Elektronik dünyada, kimlik belgesi deyince aklımıza sadece nüfus cüzdanı gelmemeli. Pasaport, sürücü belgesi, doğum belgesi, ölüm belgesi, evlilik cüzdanı, işyeri kimlik kartı, dernek üyelik kartı, futbol klübü üyelik kartı vb. tüm belgeler, aslında bir çeşit kimlik belgesidir. Günümüzde kimlik bilgisi, merkezi bir yapı içerisinde muhafaza edilmekte ve dış servislere kontrollü bir şekilde sunulmaktadır. Ancak internet ve mobil teknolojiler geliştikçe, fiziksel kimlikten ziyade, dijital kimliğe olan ihtiyaç iyice artmıştır. Blokzincir teknolojisini kullanarak, merkezi olmayan, dağıtık yapıda, kimlik kayıt ve doğrulama sistemi kurarak, kimlik sahibinin onayına bağlı olarak, kimlik bilgilerinin sadece gerektiği kadarını, gereken yerler ile güvenli bir şekilde paylaşmak mümkündür. Blokzincir üzerinde çalışan mobil dijital kimlik yönetimi ile ilgili "Turkcell" firması bir çözüm geliştirmiştir.

## Sağlık Uygulamaları

Hastanelerin, hastaların mahremiyet içeren sağlık bilgilerini depolaması ve paylaşması için, güvenli bir platforma ihtiyaç vardır. Blokzincir platformu, bu ihtiyacı karşılayabilir. Blokzincirde bu özel veri, güvenli bir şekilde depolanır ve sadece yetkili doktor ve hastaların bu veriye ulaşmasına müsaade edilir. Bu durum teşhisin daha hızlı ve daha doğru şekilde

yapılmasına imkan sağlar. Bunun dışında genel sağlık yönetimi için, ilaçları denetleme, mevzuata uyumluluk, sağlık malzemeleri tedariki gibi alanlarda da kayıtlar oluşturmak ve yönetmek mümkündür. "Gem" ve "Tierion" firmaları bu alanda çalışmalar yapmaktadır.

> "Blokzincir teknolojisi ile Kamu'daki işlerin şeffaflığını, güvenilirliğini, verimliliğini artırmak ve bürokrasiyi azaltmak mümkündür."

### Oy Kullanma

Blokzincir teknolojisi kullanılarak, oy kullanmada ihtiyaç duyulan unsurlar, yani kayıtların anonim olarak tutulması, kimlik doğrulaması ve mükerrer oy kullanılmaması şartlarını gerçekleştirmek mümkündür. Bu sistemde hiçbir oy değiştirilemez ve silinemez. Daha adaletli ve demokratik bir şekilde, seçimlerin yapılabilmesi mümkün olur. Oylama çevrimiçi yapılır ve sonuca hemen ulaşılır. "Democracy.Earth" ve "followmyvote.com" isimli sivil toplum kuruluşları, bu alanda çalışmalar yapmaktadır.

### Müşteri Tanıma (Know Your Customer - KYC)

Bankalar, resmi kurumlar, alışveriş merkezleri vb. pek çok işletme, müşterilerine ait bilgileri toplamak zorundadır. Geleneksel yapıda, bizlere ait bilgiler, her işletme ve kurumda ayrı ayrı toplanmaktadır. Bu durum külfetli, maliyetli ve verimsizdir. Ayrıca müşterilere ait bilgilerin çalınması ve satılması gibi sorunlar da vardır. Blokzincir sisteminde ise, tüm müşterilere ait bilgiler güvenli bir şekilde tutulur. Bu bilgiler, müşterinin onayı ile talep eden kurumlara iletilir. Müşteri bilgilerinde bir değişiklik olduğu takdirde, bu kayda erişme yetkisi olan kurumlara, anlık olarak bu bilgi iletilir. Bu durum, hem işletmeler açısından daha verimli, daha güvenli ve daha az maliyetli olur. "KYC-Chain", "Cambiridge Blockchain", "SelfKey", "uPort" ve "Civic" firmaları bu alanda çalışmalar yapmaktadır.

### Bağış Toplama ve Sosyal Yardımlar

Bağış toplamada karşılaşılan başlıca zorluklar, verimsizlik, bağışın yerine ulaşıp ulaşmadığı endişesi ve kesintilerdir. Blokzincir teknolojisi kullanarak, güvenli, düşük masraflı, verimli ve şeffaf bir bağış toplama sistemini kurmak mümkündür. Bu sistemde, yapılan bağış gideceği yere anında ulaştırılır. Ayrıca bağış yapanlar, bağışlarını takip edip denetleyebilirler. Buna örnek olarak, "BitGive" vakfının uygulamasını verebiliriz. Aynı şekilde, devletin sosyal yardımları da, blokzincir platformu üzerinden dağıtması mümkündür. Böylece zaman kaybı, bürokrasi gibi sorunların üstesinden daha kolay gelinir. "GovCoin" isimli bir firma blokzinciri üzerinde sosyal yardımları dağıtacak bir çözüm geliştirdi. "BARCLAYS" bankası ile birlikte 2016 yılından itibaren İngiltere hükümeti'ne bu alanda hizmet sunmaktadır.

### Vergi Toplama

Nakit paranın kullanılmadığı, tüm parasal işlemlerin dijital ortamda gerçekleştiği bir ortamda, blokzincir platformu üzerinde çalışan akıllı sözleşmeler ile gerçek zamanlı olarak ve doğru bir şekilde vergi hesaplamasını ve vergi tahsilatını yapmak mümkündür. Bütün süreçler elektronik ortamda işleyeceği için, vergi kaçırma ihtimali çok azalır, kayıt dışı ekonomi ortadan kalkar ve vergi toplama işi daha hızlı ve daha düşük maliyetli olur.

### Enerji Yönetimi

Geleneksel yapıda, enerji sektörü de merkezi bir şekilde yönetilen bir sektördür. Günümüzde enerji üreticileri, ürettikleri enerjiyi doğrudan tüketicilere satamıyorlar. Arada, mutlaka aracı olarak kamu şebekesini kullanmak zorunda kalıyorlar. Blokzincir teknolojisini kulanan "TransactiveGrid" firmasının geliştirdiği Etherium üzerinde çalışan, yazılım ve donanım altyapısı ile bu probleme çözüm üretmiştir. Böylece enerji üreticileri, müşterilere dağıtık bir şekilde, doğrudan ulaşabilmektedir. Ayrıca bu yöntemi kullanarak, kişiden kişiye enerji alıp satmakta mümkün olmaktadır.

### Noter İşlemleri

Blockchain teknolojisi kullanarak, noterlerin yaptığı işleri yapmak ta mümkündür. Bu sistemde, pek çok kurum ve işletme gibi, noterlerde işlevlerini yitirme tehlikesi ile karşı karşıyadır.

### Genel Değerlendirme

Birden fazla kişi veya kurum arasında, güven gerektiren kayıtların şifreli bir şekilde doğrulanacağı, tutulacağı, taşınacağı, paylaşılacağı ve yönetileceği her yerde, bu teknolojiden istifade etmek mümkündür. Blokzincirin gelişme evresi, internetin gelişme evresi gibi olabilir. Bu teknolojinin, merkezi otoriteyi önemli ölçüde zayıflatacağını ve pek çok kuruma ve işletmeye olan ihtiyacı ortadan kaldıracağını söylemek mümkündür. Bazı kurumlar ve işletmeler ise, varlığını devam ettirebilmek için, blokzincir teknolojisine uyumlu olacak şekilde yapısını ve işleyişini değiştirmek zorunda kalacaktır. Blokzinciri'nin uygulandığı veya uygulanabileceği bütün alanları anlatmaya kalksak, herhalde kalın bir kitap yazmamız gerekirdi. Bu yazıda, sadece insanları, kurumları ve işletmeleri önemli ölçüde etkileyecek, çarpıcı örnekler verilmiştir.

*Referanslar*
- *http://futurethinkers.org/industries-...*
- *Blockchain 101 Ahmet Usta, Serkan Doğantekin*
- *Bitcoin - https://bitcoin.org/*



TÜBİTAK BİLGEM

Bu bir proje tanıtımıdır.

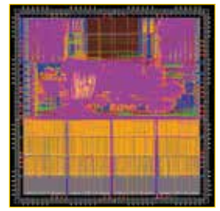
# Çok Amaçlı Açık Kaynak İşlemci (ÇAKIL)

## Proje ile;

- Embedded Linux BSP/ASP geliştirme ve Açık Kaynak Buyruk Kümesi Mimarileri (Open Source ISA) konusunda bilgi birikimi elde edilecektir.
- Tasarımı yapılan işlemcide, TÜBİTAK GİS (Gerçek Zamanlı İşletim Sistemi) desteği sağlanarak GİS'in yaygınlaştırılmasına katkıda bulunulacaktır.
- Proje sonrasında, milli işlemcinin askeri sistemlerde atış kontrol, insansız hava aracı, güdüm, oto pilot, uçuş kontrol, işaret işleme (radar, sonar, video vb.) ve görev yönetimi gibi uygulamalarda kullanılması hedeflenmektedir.
- Projenin başlamasının üzerinden sadece bir yıl geçmesine rağmen ilk prototip tasarım tamamlanmış olup Ocak 2020'de üretimine başlanacaktır. Üretimin ardından GİS entegrasyonu yapılarak 2020 yılının sonunda silah sistemlerinde gösterimi yapılacaktır.

### ÇAKIL İşlemcisi

- RISC-V 64 bit mimari
- İşlemci hızı (~400 Mhz)
- Analog blok tasarımları(PLL)
- Veri yolu tasarımı (Bus)
- Debug & tasarım doğrulama
- GİS & Embedded Linux çalışmaları
- 27 $mm^2$ chip alanı



www.bilgem.tubitak.gov.tr

Fatih Birinci 1995 ODTÜ Matematik mezunudur. ODTÜ Matematik ve GTÜ Bilgisayar Mühendisliği Bölümlerinde yüksek lisans yapmıştır. 1997 yılında TÜBİTAK BİLGEM'de çalışmaya başlamış ve birçok projede görev almıştır. Kriptografi, kriptografik protokoller ve blokzincir konularında uzmanlaşmıştır. Halen TÜBİTAK BİLGEM UEKAE'de Enstitü Müdür Yardımcısı olarak çalışmaktadır.

## BİLGEM UEKAE Enstitü Müdür Yardımcısı Fatih Birinci:

# "Blokzincir yıkıcı değil dönüştürücü bir teknolojidir!"

Dünyada bir taraftan blokzincir teknolojisinin kullanım alanı genişlemekte bir taraftan da ilgili mevzuat çalışmaları sürmektedir.

*Yayın Kurulu olarak Blokzincir teknolojileri ile ilgili UEKAE Enstitü Müdür Yardımcımız Sayın Fatih Birinci ile bir röportaj gerçekleştirdik. Fatih Hocamız alandaki önemli bilgi birikimiyle kafalarımızdaki birçok soru işaretine açıklık getirdi…*

Hamza Özer: **Sıradan bir vatandaşa Blokzincir teknolojisini tanımlamak istersek nasıl bir tanım yapabiliriz? Sizce Blokzincir teknolojisi sıradan bir vatandaşın günlük yaşamına ne zaman girecek veya sıradan bir vatandaş bunu ne zaman ve nasıl hissedecek?**

Blokzincir teknolojisini, güvenilir işlem yapan küresel bir bilgisayara benzetebiliriz. Bilgisayarların en temel bileşenleri hafıza ve işlemci birimleridir. Blokzincirin hafıza kısmını, kayıt defteri olarak da adlandırılan ve genellikle zincir şeklinde birbirine bağlanan veri kümeleri oluşturmaktadır. Bu veriler birbirine kriptografik tekniklerle bağlanmaktadır. Bu mekanizmalar, blokzincire yazılan verilerin silinememesini veya değiştirilememesini sağlamaktadır.

Blokzincirdeki verilerin güncellenmesi için yetkili kişi tarafından işlem yapılması gerekmektedir. İşlem yapabilmek için yetkili olmak yetmemekte ayrıca yapılan işlemin belirli kurallar çerçevesinde olması gerekmektedir. Örneğin para harcayabilmek için hesabın sahibi olmak dışında hesabınızda yeteri kadar para olması gerekmektedir.

Blokzincirin işlemci ayağını ise akıllı kontratlar oluşturmaktadır. Akıllı kontratlar, kurallar dizisi veya bir kod parçası gibi düşünülebilir. Blok zincire yazılan bu kod parçası, daha sonra yapılacak işlemlerde isteğe bağlı veya otomatik olarak tetikle nebilmektedir. Blokzincire önceden kaydedilmiş akıllı kontratlar değiştirilemediği için buna bağlı olarak yapılacak işlemler de güvenilir olacaktır. Blokzincirde veriler birçok noktada dağıtık olarak tutulmaktadır. Bu durum hem verilere erişimi kolaylaştırmakta hem de blokzincirdeki verilerin güvenilirliğini artırmaktadır. Siber saldırı gibi nedenlerle bir uca erişilememesi durumunda başka uçlardan gerekli veriler temin edilerek erişilebilirlik artırılmaktadır. Blokzincirin uçları ademi merkeziyetçi bir tarzda yönetilmektedir, uçlar arasında herhangi bir hiyerarşi yoktur. Bu da sisteme olan güveni artırmaktadır. Tüm yapılan işlemler sistemdeki uçlar tarafından kontrol edilmektedir. Yapılan işlemlerin doğruluğu konusunda bir uzlaşma sağlanarak blokzincire yazılmaktadır. Değişik uzlaşma mekanizmaları vardır. Bunlardan bazılarını işletmek için çok enerji harcandığından eleştiri de almaktadır. Genellikle teknolojinin son kullanıcı tarafından direk hissedilme-si tercih edilmez. Blokzincir teknolojisinin de son kullanıcı tarafından hissedilmemesi, işlerin kolaylaşması, aracıların azalması, sistemin güvenilirliğinin artması veya maliyetlerin düşmesi ile olacaktır.

Ömer Özkan: **Blokzincir alanında dünyada ve Türkiye'de yapılan çalışmalardan bahseder misiniz? Eksik olduğumuz alanlarda öne çıkabilmek adına neler yapmamız gerekir?**

Dünyada bir taraftan bu teknolojinin kullanım alanları genişlemekte bir taraftan da kullanımı için gerekli mevzuat hazırlama çalışmaları sürmektedir. Bu konuda öncü olmaya çalışan ülkeler olmakla birlikte muhafazakâr davranan ve bekle gör stratejisi izleyen ülkeler de vardır. Günümüzde teknolojide hızlı davranıp ilk olmak çok önem kazanmıştır. Bununla birlikte teknolojiyi kullananların da mağdur edilmemesi çok önemlidir. Çiftlikbank gibi örnekler, sermaye piyasaları konusunda mevzuat hazırlama işlerini zorlaştırmakta ve yavaşlatmaktadır.

Halkımızın bu ve benzeri girişimlere yaklaşımı, girişimcilere geniş alan bırakan mevzuatlar oluşturma konusunda karar vericileri zor durumda bırakmaktadır. Dünya'da bir taraftan yeni özellikler taşıyan kripto

paralar/tokenlar ortaya çıkarken diğer taraftan mevcut teknolojide darboğaz oluşturan ve işlem hızlarını sınırlı tutan uzlaşma mekanizmalarının geliştirilmesine yönelik araştırmalar yapılmaktadır. Bunun yanında, ABD NIST kurumunun kuantum bilgisayara karşı güvenli algoritmalar konusunda yürütmekte olduğu yarışma ilerledikçe bu algoritmaları kullanan blokzincirlerle ilgili çalışmaların da hızlanacağı öngörülmektedir.

Türkiye, blokzincir kavram ispatı çalışmaları konusunda dünyadan geri kalmamakla birlikte blok zincir alanında Ar-Ge faaliyetlerini artırmalıdır. Diğer taraftan geliştirilen blokzincir teknolojilerinin kullanımı için gerekli mevzuat çalışmalarının hızlanması da çok önemlidir.

Bilal Kılıç: **Fatih Bey, Blokzincir konusu ile ilgili olarak Kamunun atması gereken somut adımlar sizce neler olmalıdır?**
Kamu kurumları mevzuat oluşturmanın yanısıra bu teknolojinin kullanımı konusunda da ön ayak olabilir. Kamu kurumları genellikle yeni teknolojileri hemen kullanmaz, olgunlaşmalarını bekler. Kamu kurumlarımızın blokzinciri kullanmaya ikna olmaları için bu yeni teknolojiyi daha iyi anlamaya ihtiyaçları olduğunu düşünüyorum. Bu konuda bizim gibi araştırma kurumlarına ve eğitim kurumlarına görevler düşmektedir.

Sanayi ve Teknoloji Bakanlığımızın hazırladığı "2023 Sanayi ve Teknoloji Stratejisi"nde ulusal blokzincir altyapısı hazırlanması hedefi yer almaktadır. Bu hedefi gerçeklemek için yapılması gereken ara faaliyetler bulunmaktadır. Benzer şekilde Merkez Bankası ve Ticaret Bakanlığı'nın da bu konuda hedefler belirlemiş olması sevindirici gelişmelerdir.

Blokzincir konusunda yetkin insan kaynağı yetiştirilmesi çok önemlidir. Üniversitelerimizde bu konuya odaklı programlar açılması ve bu konunun yaşatılacağı topluluklar oluşturmak gerekir. 2. Ulusal Blokzincir Çalıştayımızda TÜBİTAK Başkanımız bu konuyu yakından takip ettiğini ve TÜBİTAK fonları kapsamında gerekli faaliyetlerin yapılmakta olduğunu belirtmiştir.

> **BİLGEM bünyesinde Blokzincir laboratuvarını kurma amacımız, yeni gelişmekte olan bu teknoloji konusunda kamu ve özel sektörümüzü bilinçlendirmek ve dijital kimlik gibi önemli gördüğümüz projelerde öncü rol üstlenmektir.**

## Blokzincir Her Derde Deva Bir İlaç Değildir

Mehmet S.Ekinci: **3 yıl önce BİLGEM çatısı altında Blokzincir laboratuvarı kuruldu. 2 yıldır da uluslararası Blokzincir çalıştayı düzenleniyor. Bu çalışmaların hedefleriyle ilgili bilgi verebilir misiniz?**
Blokzincir laboratuvarını kurma amacımız yeni gelişmekte olan bu teknoloji konusunda kamu ve özel sektörümüzü bilinçlendirmek ve dijital kimlik gibi önemli gördüğümüz projelerde öncü rol üstlenmektir. Bunu çalıştaylar düzenleyerek, kurumlarımızı ziyaret ederek, yaptıkları çalışmalara katılım sağlayarak ve projeler geliştirerek yapmaya çalışıyoruz. Blokzincir her derde deva bir ilaç değildir. Blokzincirle ilgili fizibilite çalışması yapılarak nihayetinde kullanımına gerek olmadığına karar verilen birçok proje çalışması vardır. Dolayısı ile projelendirme ve fizibilite çalışmalarında bunun iyi değerlendirilmesi gerekmektedir. Bu kapsamda da kurumlarımıza yardımcı olabileceğimizi düşünüyoruz.

Çalıştay düzenlememizin bir diğer amacı da blokzincir konusunda çalışan veya bu konuyu merak edenlerin bir araya toplamak ve tanışmalarını sağlamaktır. Dünyada bu konuda çalışan öncü kişileri birinci ağızdan dinleyerek konu hakkında bilgi almaktır. Çalıştaylarımızın önemli bir kısmını da eğitimler oluşturmaktadır. Giriş seviyesindeki bu eğitimlerle amacımız, katılımcılarımızın konu hakkında daha fazla bilgi edinmesidir.

2017 yılından bu yana birçok özel sektör, organizasyon ve kurum ile görüşme fırsatımız oldu. Yeni teknolojileri kullanmayı seven bir millet olmamız bu konuda büyük bir avantaj oluşturmaktadır. Çoğu kurumumuzun bu konuda bilinç sahibi olduğunu görmekle birlikte devletimizin kendilerine tanıdığı özel alanda faaliyet gösteren bazı sektörlerin, bu alanı korumak adına blokzincir teknolojisini görmezden geldiğini görmek de üzücüdür.

## Kripto Paralar

Mehmet S.Ekinci: **Blokzincir ilk çıktığı dönemde yüksek heyecan dalgaları oluşturdu. Spesifik bazı endüstrileri sarsacağı ve köklü değişimlere sebep olacağı söyleniyordu. Bugün ise ilk dönemdeki o coşkuyu göremiyoruz. Ne dersiniz?**
Teknolojiler ilk çıktığında çok fazla beklenti oluştururlar. Bunda yapılan yayınların dilinin de çok önemi vardır. Zamanla bu beklentiler gerçekliğe doğru ilerler, bazen





hayal kırıklıkları da yaşanır. Bu süreç blokzincir için de bu şekilde ilerlemektedir. Bitcoin vb. kripto para birimlerindeki değer artışları ile bunların magazinleştirilmesi blokzincir konusundaki ilgiyi ve beklentiyi olması gerekenden fazla artırmıştır. Bu para birimlerindeki değer düşüşleri ile birlikte yayınlar ve dolayısı ile ilgi de azalmış görünmektedir.

Kripto para dünyasında durum böyle olmakla birlikte blokzincir teknolojisinde araştırma/geliştirme ve kavram ispatı gibi çalışmalar hızla devam etmektedir. Linux Vakfı bünyesinde 197 organizasyonun katılımı ile geliştirilmekte olan Hyperledger açık kaynak projesinin vakfın tarihindeki en hızlı büyüyen proje olduğu bilinmektedir.

Necati Şişeci: **Sayın Hocam, Blokzincir teknolojisinin en yaygın kullanım alanı kripto paralar oldu. Bunu neye bağlıyorsunuz?**
Günümüzde parasal işlemlerin %80'inden fazlası elektronik para şeklinde gerçekleşmektedir. Elektronik para transferleri ise banka ve finans kuruluşları aracılığı ile yapılmaktadır. Özellikle uluslararası para transferleri hem çok kontrollü hem çok yavaş hem de maliyetlidir. Aracıları ortadan kaldıran bir sistem maliyetleri düşürecek ve hızlanma sağlayacaktır. Bu nedenle bu konu ilgi çekici bir alan olmuştur.

Elektronik para kavramı bitcoin ve blokzincirden önce de vardı. 1983 yılında yayınlanan makalesinde David Chaum dijital nakit kavramını ortaya atmıştır. 1990 yılında kurduğu DigiCash şirketi 1998 yılında iflas etmiştir. Bu alandaki en başarılı şirket olan e-Gold 1996 yılında elektronik altın alım ve transferi amacıyla kurulmuş ve beş milyon kullanıcıya kadar ulaşmıştır. Kara para aklama gibi bazı sorunlar nedeniyle Amerikan devleti tarafından yakın takip altına alınmış ve şirket 2009 yılında faaliyetlerini durdurmuştur.

Önceki denemelerden farklı olarak mevcut para birimlerine veya altın gibi değerlere bağlı olmayan, para kavramını felsefi olarak da ele alan, ülke, grup veya şahısların kontrolünün çok zor olduğu, yapılan işlemcilerin bir yarış ve ödül mekanizması ile kayıt altına alındığı Bitcoin sistemi 2008 yılında ortaya çıktı. Bitcoin'in 2017 yılından sonra çok değer kazanması sonucu magazinleştirilmesiyle bu konuya aşina olmayan vatandaşlar arasında kısa yoldan zengin olma aracı olarak görülmeye başlandı. Bu popülerlik sonucu bitcoin benzeri birçok para da ortaya çıktı. Bitcoin'in çok değerliyken yapılan bu haberler neticesince değerliyken alım yapan birçok vatandaş fiyatı düştüğü zaman zarara uğradı.

Kripto paralar dışında Ethereum platformu, bir nevi kitle fonlama aracı olarak kullanılması ile girişimciler için tüm dünyadan kaynak toplayabilecekleri bir araç haline geldi. Bu projelerden bazıları çok başarılı olurken birçoğu ne yazık ki yatırımcısını kandırdı veya zarara uğrattı. Düzenleme ve denetimin olmadığı bir ortamda zaten vatandaşın kendi başına hangi girişime yatırım yapacağını doğru bir şekilde kestirmesi çok zordur. Çoğu şirketin (ortada şirket olmayabilir) başka ülkelerde olması nedeniyle zarara uğrayanlar, haklarını arayabilecekleri veya kapısını çalabilecekleri bir yer de bulamadılar. Bu durum şimdilerde biraz değişmeye başlamıştır. İsviçre, Malta gibi ülkeler bu konudaki mevzuatlarını güncelleyerek kitle fonlama şirketlerinin merkezi olmaya başlamışlardır.

BİLGEM BLOKZİNCİR Araştırma Laboratuvarı

Biz bitcoin gibi spekülatif değerlerle değil blokzincirin arkasında yatan blokzincir teknoloji sinin çok değerli olduğunu düşünüyoruz.

Abdullah Alpaydın: **Blokzinciri yıkıcı bir teknoloji olarak tarif eden gelecek bilimciler var. Siz bu görüşe katılıyor musunuz?**
Blokzincirin yıkıcı bir teknoloji olduğu görüşüne tam olarak katılmıyorum. Blokzincirin yıkıcı bir etkisi olduğu doğrudur. Fakat dönüştürücü etkisini öne çıkarmanın daha doğru olacağını düşünüyorum. Blokzincir teknolojisini en çok araştıran ve çalışan kurumların aslında yıkıcı etkisine maruz kalacak aracılar olduğunu görüyoruz. Böyle bir teknolojinin gelmekte olduğunu görüp buna göre kendilerini dönüştürebilenler, bu teknolojiden zarar değil fayda sağlayacaktır.

Bu teknolojiyi görmezden gelen aracılar ise eninde sonunda bu teknolojinin yıkıcı etkisi ile yüzleşmek durumunda kalacaklardır. Örneğin bankalar, para transferleri ve borç verme gibi işlemlerde aracı durumundadır. Blokzincir teknolojisi konusuna en çok kaynak ayıran sektörlerin başında bankacılık ve finans sektörü gelmektedir. Bankaların da desteklediği birçok Fintek (finansal teknolojiler) girişimi blokzincir konusunda çalışmaktadır. Bankacılık ve finans sektörü, uygun bir değişim geçirmenin (örneğin güven tarafını blokzincire dayandırarak) bir şekilde blokzincir teknolojisi ile birlikte yaşamanın yolunu aramaktadır.

İzzet Karabay: **Blokzincir veya benzeri uygulamalarla ilgili gençlere bir projeksiyon çizecek olsak neler söylememiz gerekir?**
Teknoloji çok hızlı ve değişken, özellikle blokzincir alanı çok haraketli. Az önce de belirttiğim gibi Hyperledger projesi, 197 üyenin katkılarıyla geliştirilmekte ve Linux vakfının tarihindeki en hızlı gelişen ve büyüyen projesidir. Blokzincir, güvenilirlik (şeffaflık) özelliğinin de etkisiyle diğer alanlardan daha fazla açık kaynaklı olarak geliştirilmektedir.

Gençlerimizin yeni çıkan teknolojilerin yüzeysel ve magazinsel yönünden ziyade altında yatan teknolojileri öğrenmesi, açık kaynaklı sistemleri incelemesini öneriyorum. Öğrenmenin en iyi yolu elini bulaştırmaktan geçtiğinden mümkünse açık kaynaklı projelere katkı vermelerinin kendi gelişimleri açısından faydalı olacağını düşünüyorum. Akademik çalışmalar yapan gençlerimiz de çalışmalarını bu alanda yapabilirler.

# Kripto Para Sistemleri

**Kripto para, eşler arası işleyen dağıtık bir sistemde başlıca görevi değer takas aracılığı yapmak olan bir dijital varlıktır.**

Dr. İsa Sertkaya - Başuzman Araştırmacı / BİLGEM UEKAE Araştırma

Toplumların para kavramını kullanmaya başlamalarının tarihsel kökenini tam olarak tespit etmek zordur. Ancak, ilk başlarda gerçek değere sahip emtia para kullanılırken, zaman içerisinde özellikle kolay taşınabilirlik amacıyla, "meta destekli" yani temel emtiayı temsil eden ve aslında öz değeri bulunmayan paralar kullanılmaya başlandı. Günümüzde ise, artık ekonomiler merkezi bir otorite tarafından basılan ve yasal güvence ile taahhüt altına alınan fiat para temelli bir yapıya dönüşmüş durumdadır. Merkezi otoriteye duyulan güvenden hareketle toplum, alışverişlerinde bu parayı kullanmakta ve temelde güven ilişkisi bu sistemi ayakta tutmaktadır. Bu nedenle fiat para sisteminin sürdürülebilirliği için en önemli unsur güvendir.

Yapısı nasıl olursa olsun, geleneksel kullanım alışkanlıkları sonucunda, değişim aracı, hesap birimi ve değer birikimi olarak kullanılmakta olan para; toplum ihtiyaçları ekseninde üretilen, geliştirilen, zamana ve gereklere uyum sağlayan sosyal bir kurum hüviyetine bürünmüştür. Bu bağlamda, paranın son teknolojik gelişmelerden ve internetin yaygın olarak kullanılmasından etkilenmesi şaşırtıcı değildir [1].

## Sanal Para Birimi Nedir?

Avrupa Merkez Bankası 2012 yılında yayınlamış olduğu Sanal Kur Sistemleri raporu, sanal para birimi terimini "genellikle geliştiricileri tarafından verilen ve kontrol edilen ve belirli bir sanal topluluğun üyeleri arasında kullanılan ve kabul edilen, yasal olarak düzenlenmeyen dijital para türü" olarak tanımlamakta ve sanal para sistemlerini üç başlık altında sınıflamaktadır, [1].

Kapalı sanal para birimi sistemleri, bazen "sadece oyun içi" olarak betimlenmekte ve reel ekonomiyle neredeyse hiçbir bağlantısı bulunmamaktadır. Kullanıcılar genellikle bir abonelik ücreti öder ve ardından çevrimiçi performanslarına dayalı olarak sanal para kazanırlar. Sanal para birimi yalnızca sanal topluluk içinde sunulan sanal ürün ve hizmetleri satın alarak harcanabilir ve teoride sanal topluluk dışında alınıp satılamaz.

Tek yönlü akışı olan sanal para birimi sistemleri, doğrudan gerçek para birimini belirli bir döviz kuruyla kullanarak satın alınabilir, ancak orijinal para birimine geri alınamaz. Dönüşüm koşulları, şema sahibi tarafından belirlenir. Bu sistemler, sanal ya da bir kısım gerçek ürün ve hizmetleri satın almak için kullanılsa da tekrar reel paraya dönüştürülemezler.

İki yönlü akışı olan sanal para birimi sistemleri, döviz kurlarına göre döviz cinsinden sanal para alım-satımına imkan tanır. Gerçek dünyayla birlikte çalışabilirliği bakımından diğer herhangi bir dönüştürülebilir para birimine benzer. Bu sistemler hem sanal hem de gerçek mal ve hizmetlerin satın alınmasına izin verir.

Bu noktada, her ne kadar nüans olarak görülse de sisteme etkisi nedeniyle önemli olan bir hususa daha dikkat etmek gerekir. Sanal para ile elektronik para kavramları mevcut yasal düzenlemeler nedeniyle aynı kavramları ifade etmemektedirler. Avrupa Birliği'nde Elektronik Para Direktifi (2009/110/EC), Türkiye'de ise 6493 sayılı Kanun çerçevesinde elektronik para tanımları yapılmakta ve yasal sınırlar açıkça belirtilmektedir. Bu mevzuatlar uyarınca, herhangi bir resmi ya da özel kuruluş tarafından ihraç edilmeyen ve karşılığı için güvence verilmeyen bir sanal para birimi olarak bilinen Bitcoin, mevcut yapısı ve işleyişi itibarıyla Kanun kapsamında elektronik para olarak değerlendirilmemekte, bu nedenle de Kanun çerçevesinde gözetim ve denetimi mümkün görülmemektedir.

## Kripto Para Nedir?

Kripto para, eşler arası işleyen dağıtık bir sistemde başlıca görevi değer takas aracılığı yapmak olan bir dijital varlıktır. Bu dağıtık sistem; işlemleri doğrulamak ve güvence altında tutmak, ve belirli bir kural dahilinde yeni para birimlerinin oluşturulmasını sağlamak için eşler arası ağ yapılarını, dağıtık kayıt defteri teknolojilerinin bir uygulaması olan blokzincir yapılarını ve en önemlisi kriptografik yapıtaşlarını kullanır. Bu bağlamda kripto paralar iki yönlü akışı olan sanal para birimi sistemlerinin en çarpıcı örneklerindendir.

> **"Kullanılabilirliği, güvenirliği gibi tartışmalar tüm hızıyla devam etse de, günümüz teknolojilerinin sanal para sistemine ihtiyaç duyduğunu ve mevcut sistemlerin yetersiz kaldığını söylemek mümkündür."**

Kripto para birimi ekosistemleri esas olarak, daha önceki ödeme sistemlerinde bulunmayan yeni aktör kategorilerini barındırmaktadır [2], bunlardan öne çıkanları şunlardır:

**Mucitler (Inventors),** sanal bir para birimini oluşturur ve çalışacağı ağın teknik bölümünü geliştirir. Bazı durumlarda, bu şahıslar veya kuruluşlar bilinmektedir, diğer durumlarda ise kimlikleri bilinmemektedir.

**İhraççılar (Issuers),** sanal para birimlerini üretebilirler. Tasarıma bağlı olarak, sistemdeki toplam para hacmi önceden veya talebe bağlı olarak belirlenmektedir. Merkezi kripto paralarda ihraççı aynı zamanda kullanım kurallarını belirler ve birimleri dolaşımdan çekme yetkisini elinde bulundurur. Merkezileşmemiş kripto paralarda ise "madenciler" tarafından gerçekleştirilen faaliyetler sonucunda otomatik olarak yeni birimler oluşturulmaktadır.

**Madenciler (Miners),** bazen grup halinde de çalışan, gönüllü olarak sistemin gerektirdiği hesaplama işlemlerini yapan kişilerdir. Kullanıcıların yapmış oldukları para gönderim işlemlerinden (transaction) oluşan bir kümenin onaylanması için oluşturulan ve blok adı verilen veri yapısını oluşturmakta ve doğrulamaktadırlar. Bu bloklar ardı sıra bağlanarak

kayıt defterini yanı blokzincir yapısını oluştururlar. Bu noktada çifte harcama (double-spending) ya da işlem doğruluğu kontrolleri de yapılmaktadır. Madenciler onaylanan blokları için ödül olarak belirli sayıda para biriminin yanı sıra para gönderim ücretlerini de alırlar.

**İşlem Servis Sağlayıcıları (Processing Service Providers)**, bir kısmı madencilerden oluşmakta ve ağ üzerinde bilgi akışının doğruluk teyidi ve yayılımını sağlamaktadırlar.

**Kullanıcılar (Users)**, belirli satıcılardan sanal veya gerçek ürün ve hizmetleri satın almak, kişiden kişiye ödeme yapmak veya yatırım amaçlı kripto para sistemini kullanan aktörlerdir. Kripto para edinmenin beş yolu vardır: satın alma, sanal para birimleriyle ödüllendirilen faaliyetlerde bulunma, madencilik yapma, ödeme veya bağış / hediye olarak kabul etme.

**Cüzdan Sağlayıcılar (Wallet Providers)**, kullanıcılara sanal para birimlerine ait kriptografik anahtarlarını depolama, imzalı para gönderim hazırlama ve tüm bu süreçleri yönetme gibi işlemler için dijital cüzdan hizmeti sunmaktadırlar. Temel olarak, kullanım durumlarına ve siber saldırılara karşı güvenlik sağlama kriterlerine göre farklılık gösteren iki tür cüzdan vardır: çevrimiçi cüzdanlar (sıcak depo) ve çevrimdışı cüzdanlar (soğuk depo). İşlevsel bir bakış açısıyla, masaüstü bilgisayarlar, mobil cihazlar veya bulut bilişim tabanlı uygulamalar üzerinden bu hizmetler sunulmaktadır. Bununla birlikte, kullanıcılar bir cüzdan sağlayıcı kullanmadan, bir cüzdan ayarlayabilir, bakımını ve yönetimini kendileri üstlenebilirler.

**Borsalar (Exchanges)**, kullanıcılara reel para birimlerine karşılık kripto para veya kripto paralar arası alım satım hizmetleri sunmaktadırlar.

**Ticaret Platformları (Trading Platforms)**, sanal olarak alıcı ve satıcıları bir araya getiren pazar olarak işlev görmektedirler. Bununla birlikte, borsaların aksine, işlem platformları alım satım işlemlerine genel itibariyle dahil olmazlar.

## Kripto Para Tarihi

Sanal para sistemlerine yönelik ihtiyaçların giderilmesi konusunda öncü çalışmalardan bir tanesi, David Chaum tarafından 1983 yılında yayınlanan bir makale [3] ile ortaya atılmıştır. Chaum sonrasında bu araştırmalarını temel alarak "DigiCash" adlı elektronik para firmasını 1990 yılında kurmuştur. Kullanıcılar "eCash" adlı paralarını banka tarafından kriptografik olarak imzalanmış dijital bir formatı bilgisayarlarında tutup, bu dijital parayı anlaşmalı her hangi bir kurumda, kredi kartı numarası gibi bir bilgi paylaşımı yapmadan, gizli ve güvenli bir şekilde kullanabiliyorlardı. Bu şirket 1998 yılında yeterli kullanıcı sayısına ulaşamadığından dolayı iflas etmiş olsa da getirdiği kavramlar ve yaklaşımlar ilerideki çözümler için esin kaynağı olmuştur.

Haber ve Stornetta'nın 1991 yılına ait makalelerinde [4], belgelerin, zaman damgalı olarak, kurcalanamaz veya geriye dönük olarak değiştirilemez bir şekilde saklanması için kriptolanmış güvenli bir blokzincir kullanımı önerilmiştir. Sonraki yıl, tasarımlarına blok kavramını da eklemişlerdir. Adam Back, 1997 yılında tanıttığı hashcash sisteminde, e-posta gönderimlerindeki spam ve DOS saldırılarını engellemek için eposta göndericilerin, bugünkü pek

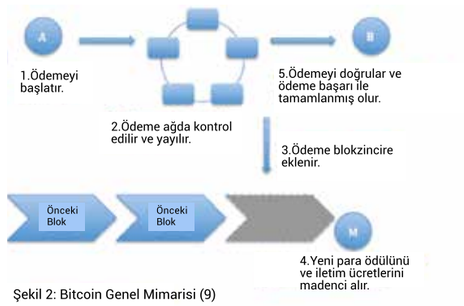
çok kripto para sisteminde de kullanılan özet (hash) algoritması içeren emek ispatı (PoW), yapmalarını önerir, [5]. Wei Dai ise b-money isimli, Nick Szabo, bitgold isimli, kripto para çalışmaları yapmıştır, [6,7]. Bu çalışmalar gerçek hayat uygulamasına dönüşmemiş olsa da günümüzdeki kripto paralarının sistem mimarilerinin temelini atmışlardır.

2008 Aralık ayında, "Bitcoin: A Peer-to-peer Electronic Cash System" başlıklı teknik yazı, Satoshi Nakamoto rumuzu kullanılarak bir kriptografi e-posta listesine gönderilmiş ve akabinde blokzincir teknolojisini dünyaya tanıtacak sistem çalışmaya başlamıştır, [8]. Satoshi 2009 Ocak ayında ilk Bitcoin kripto paralarını üretmeye başlamıştır. Satoshi, daha sonraki açıklamalarında, Bitcoin'in, b-money ve bitgold fikirlerinin bir gerçeklemesi olduğunu ifade etmiştir. 2011 yılında ise sistem kodlarının gelişimini topluluğu devrederek, kenara çekilmiştir. Hala daha gerçek kimliği bilinmemekte ve araştırılmaya devam edilmektedir.

Bitcoin (BTC) üzerine tartışmalar halen devam etse de, kripto para sistemleri içerisinde en popüler ve yaygın olarak kullanılan olma özelliğini devam ettirmektedir. 2017 Aralık ayında 1 Bitcoin'in değeri 70,000.00 Türk Lirası'na ulaşmıştır, 2019 Kasım itibariyle 1 BTC yaklaşık olarak 39,895 Türk Lirası seviyelerinde değerlenmektedir. Coinmarketcap verilerine göre 4,855 farklı kripto para birimi, binlerce işlem borsası bulunmakta ve kripto para piyasa değeri 1 katrilyon Türk Lirası civarında seyretmektedir. Bitcoin, kripto para piyasasının yaklaşık 65,9%'unu oluşturmaktadır. Kripto para sistemlerinin piyasa değerlerine göre mevcut ilk sıralamasını Şekil 1'de bulabilirsiniz.

## Kripto Para Mimarisi ve Yapıtaşları

Kripto para birimi sistem mimarileri farklılık göstermektedir. Buna rağmen, yaygın kullanımı ve öncü olması nedeniyle, Bitcoin sistem mimarisini genel çerçeveyi açıklamak için kullanmak mümkündür. Bitcoin para iletim işleminin gerçeklenmesi ve kayda alınışının genel akışı Şekil 2'de verilmiştir.




Şekil 2: Bitcoin Genel Mimarisi (9)



Bitcoin para iletim işlemi, işlem doğrulaması, ödeme işlemesi ve bitcoin arzını kontrol etmek için şifreleme kullanır. Kriptografi, eskiden beri bilgiyi güvence altına almak için kullanılmıştır; ancak bu özel durumda, para birimlerinin arzını yaratmaya ve kontrol etmeye hizmet eder. Kriptografinin arkasındaki kavram, bir mesajı, bu mesajı deşifre etmek için gerekli bir anahtara sahip olmayan herkes için okunamaz hale getirmek için belirli bir algoritma kullanılarak şifrelenmiş olmasıdır. Bir Bitcoin işlemi temel olarak, göndericinin elektronik adresinden alıcının elektronik adresine bitcoin transferini kolaylaştıran imzalı bir mesajdır.

Bitcoin, dijital imzalar ve kriptografik özet algoritması olmak üzere iki şifreleme yapıtaşı kullanır. Dijital imzalar, alıcının paranın belirli bir göndericiden geldiğini doğrulamasını, gönderenin para gönderimini reddedememesini ve işlem bütünlüğünün korunmasını sağlamaktadır. Kriptografik özet fonksiyonları ise kriptografik anahtarlardan elektronik adres üretilmesini, para gönderim işlemlerinin blok içinde bozulmadan etkin kaydının korunmasını ve oluşturulan blokların değiştirilemez bir şekilde birbirlerine bağlanmasını zorunlu kılar.

Bitcoin sistemi, Bitcoin Protokolü olarak bilinen bir dizi kurala göre çalışır. A kişisi B kişisine belirli miktarda bitcoin ödemek istediğinde, ödeme talimatı diğer ödeme talimatlarıyla birlikte sisteme yerleştirilir. Madenciler, ödemeleri doğrular ve Bitcoin Protokolü tarafından oluşturulan ve belirtilen hesaplama gerektiren zorlu bir matematik problemini çözerek yeni oluşturulan bir bloğa kaydeder. Madenciler hizmetleri için iki şekilde ödül alırlar: para gönderim işlemlerini onaylama sürecinde yaratılan ücretler ve yeni blok ile üretilmesine izin verilen bitcoinler. Madenciler bu ödülleri alabilmek için birbirleriyle yarışmaktadırlar.

Bitcoin, daha önce belirtilen reel ve sanal para sistemi fonksiyon ve özelliklerini karşılaması sebebiyle para olarak ele alınmaktadır. Günümüzde yaygın olarak değerli bir emtia karşılığı olmayan itibari para kullanılmaktadır. Teoride yeni açılacak madenler ve bulunacak rezervlerle dolaşıma çıkabilecek altın miktarını kestirmek mümkün değildir. Bu durum altın gibi güçlü bir emtia için dahi çıkarımındaki zorluk, emek gereksinimi ve arz/talep dengesine dayalı değerlemeyi belirsiz kılmaktadır. Bitcoin'de ise madencilikle elde edilebilecek Bitcoin miktarı toplam 21 milyon Bitcoin ile sabitlenmiştir.

Günümüzde Bitcoin bloklarının elde edilmesi için ciddi miktarda işlem gücü gereksinimi nedeni ile kayda değer bir elektrik tüketimi söz konusudur. İşlem gücü ve enerji olarak yüksek girdi gereksinimi dahi Bitcoin'e değer atfeder niteliktedir. Her 210 bin blokta bir (210 bin blok ortalama 4 senede üretilir) üretilen bitcoin miktarının yarılanmasından ve toplam üretilebilecek bitcoinin 21 milyonla sınırlanmış olmasından yola çıkılarak Bitcoin'in gelecekte daha da büyük değer kazanacağı iddia edilmekte ve tartışmalar devam etmektedir.

| # | Ad | Piyasa Değeri | Fiyat | Hacim (24s) | Dolaşan Arz |
|---|---|---|---|---|---|
| 1 | Bitcoin | ₹720,783,916,262 | ₹39,895.52 | ₹261,581,614,140 | 18,068,787 BTC |
| 2 | Ethereum | ₹90,250,476,161 | ₹830.37 | ₹58,871,040,495 | 108,687,139 ETH |
| 3 | XRP | ₹54,326,901,798 | ₹1.25 | ₹58,112,455,885 | 43,299,885,509 XRP * |
| 4 | Tether | ₹23,744,813,180 | ₹5.78 | ₹185,650,295,952 | 4,108,044,456 USDT * |
| 5 | Bitcoin Cash | ₹21,800,388,995 | ₹1,202.31 | ₹13,387,306,276 | 18,132,150 BCH |
| 6 | Litecoin | ₹16,806,690,719 | ₹263.82 | ₹19,016,783,098 | 63,704,938 LTC |
| 7 | EOS | ₹13,779,730,780 | ₹14.63 | ₹23,289,306,942 | 941,645,678 EOS * |
| 8 | Binance Coin | ₹13,499,494,089 | ₹86.79 | ₹1,279,127,519 | 155,536,713 BNB * |
| 9 | Bitcoin SV | ₹10,923,865,702 | ₹604.56 | ₹3,704,283,447 | 18,068,415 BSV |
| 10 | Stellar | ₹6,689,968,116 | ₹0.333585 | ₹5,912,022,014 | 20,054,779,554 XLM * |

Şekil 1: Piyasa Değerine Göre, ilk 10 Kripto Para Birimi (Kasım 2019, Coinmarketcap.com)

Parasal sistemlerin ortaya çıkardığı en önemli teknoloji dağıtık kayıt defteri teknolojileri (distributed ledger Technologies, DLT) olmuştur. Bir yandan yaygın kullanımına yakın sanal para sistemi geliştirme çabaları devam ederken, bilişim sistemleri ve çözümlerinin DLT ile çözümü yönünde ciddi çalışmalar bulunmaktadır. Tarihsel akışı aksi yönde olsa da, günümüzde kripto para sistemleri artık DLT'nin bir uygulaması konumuna gelmiştir.

Kullanılabilirliği, güvenirliği gibi tartışmalar tüm hızıyla devam etse de, günümüz teknolojilerinin sanal para sistemine ihtiyaç duyduğunu ve mevcut sistemlerin yetersiz kaldığını söylemek mümkündür. Hem kripto para sistemi, hem de dağıtık kayıt defteri tabanlı bilişim çözümlerinin çalışılmasının gerekliliği su götürmeyen bir gerçek olarak karşımızda durmaktadır.

*Kaynakça*
*[1] European Central Bank. (2012). Virtual Currency Schemes. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf*
*[2]European Central Bank. (2015). Virtual currency schemes–a further analysis. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf*
*[3] Chaum, D., Blind signatures for untraceable payments. Advances in Cryptology Proceedings of Crypto 82 (3): 199–203, 1983.*
*[4] Haber S., Stornetta W.S., "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.*
*[5] Back A., "Hashcash - a denial of service counter-measure,"http://www.hashcash.org/papers/hashcash.pdf, 2002.*
*[6] Dai W., "b-money," http://www.weidai.com/bmoney.txt, 1998.*
*[7] Szabo N., "Bit Gold".Unenumerated. Blogspot. http://web.archive.org/web/20151121081112/http://unenumerated.blogspot.com:80/2005/12/bit-gold.html, 2005.*
*[8] Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system. bitcoin.org. https://bitcoin.org/bitcoin.pdf, 2008.*
*[9] Dabrowski, M., & Janikowski, L., Virtual currencies and central banks monetary policy: challenges ahead. https://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf , 2018.*
*[10] Söderberg, G., (2018), "Are Bitcoin and other crypto-assets money?" Economic Commentaries. Sveriges Riksbank. www.riksbank.se/globalassets/media/rapporter/ekonomiska-kommentarer/engelska/2018/arebitcoin-and-other-crypto-assets-money. 2018.*

# BiGA: 1 Gram Altın Projesi

## Ülkemizdeki altına dayalı ilk dijital varlık

İlker Kuşcu - Direktör, Mustafa Atahan - Proje Yöneticisi / Takasbank

**BİGA ile işlemlerin tam mahremiyet altında yapılabilmesi, fiziksel dayanak varlığı esas alması, kendine ait ayrıca bir değeri olmaması ve mevcut regülasyonlara uyumlu olarak gerçekleşebiliyor olması bu projeyi dünyada duyurusu yapılmış birçok projeden ayırmaktadır.**

Blokzincir teknolojisinin popülerliği son yıllarda giderek artmış, finans sektöründe özellikle merkezi konumdaki kurumlar yaygın olarak kullanım alanlarını araştırmaya başlamıştır. İlerleyen yıllarda bu teknolojinin finans sektörüne olabilecek etkilerine yönelik bilgi birikiminin oluşturulması, Takasbank'ın en önemli stratejik hedefleri arasında yer almaktadır.

Bu hedefe yönelik olarak Takasbank Ar-Ge Merkezi, iki yılı aşkın bir süredir blokzincir üzerine detaylı çalışmalar yürütmektedir. Yapılan araştırmalar, blokzincir teknolojilerinin sahip olduğu özelliklerle finans sektöründe kullanılmasına henüz olanak sağlamadığını göstermektedir. Blokzincir teknolojisinin finans sektöründe kullanılabilmesi için, mevcut teknolojilere ek geliştirmeler gerçekleştirilmesi gerektiği ve Takasbank bünyesinde bu çalışmaların oluşturulabileceği öngörülmüştür.

Takasbank tarafından yapılan çalışmalar neticesinde 2017 yılında blokzincir teknolojisi kullanılarak bir platform geliştirme fikri ortaya çıkmıştır. Söz konusu çalışmada fiziksel karşılığı olan dijital altının blokzincir teknolojisiyle taraflararası transferini sağlayan bir platform oluşturulmuştur. Hem dağıtık defter teknolojisi kullanılmış, hem de işlemlerin mahremiyeti tam olarak koruma altına alınmıştır. İşlemlerin tam mahremiyet altında gerçekleştirilmesi, fiziksel dayanak varlığı esas alması, kendine ait ayrıca bir değeri olmaması ve mevcut regülasyonlara uyumlu olarak gerçekleşebiliyor olması bu projeyi dünyadaki duyurulan birçok projeden ayırmaktadır.

Söz konusu çalışmada farklı teknik yetkinlikleriyle ön plana çıkan iki ayrı blokzincir altyapısıyla geliştirmeler yapılmıştır. Yapılan bu geliştirmeler sonucu beş banka ile çok partili test süreci başlamıştır. Albaraka Türk Katılım Bankası, Garanti BBVA, Kuveyt Türk Katılım Bankası, VakıfBank ve Ziraat Bankası ile yapılan testlerin sonucunda BiGA'nın işlevselliği gözlemlenmiş ve yüzde yüz memnuniyetle testler tamamlanmıştır.

### BiGA Projesinin Temelleri

BiGA Projesinin temelleri, Takasbank bünyesinde, 2016 yılının ilk çeyreğinde oluşturulan Takasbank Blokzincir Çalışma Grubu'na dayanmaktadır. Söz konusu tarih itibariyle blokzincir çalışmaları kapsamında sektörel gelişimler yakından takip edilerek Takasbank bünyesinde yapılabilecek projeler hakkında değerlendirmeler yapılmıştır. Ar-Ge vizyonu ile birlikte blokzincir çalışmaları projelendirme aşamasına geçilmiştir. Takasbank, blokzincir hakkında yapılan organizasyonlara gerek ev sahipliği yaparak, gerek aktif katılım sağlayarak üst yönetim seviyesinde katkılar sunmuştur. Takasbank, ülkemizde gelişmekte olan blokzincir finans ekosisteminde bulunan firmalarla çeşitli görüşmeler ve fikir alışverişleri yaparak bu ekosistemin gelişmesine katkılar sağlamıştır. Teknik altyapısı geleneksel yöntemlerle geliştirilen Altın Transfer Sistemi (ATS) Projesi henüz tasarım aşamasındayken blokzincir teknolojisi kullanılarak geliştirilebileceği fikri ortaya çıkmıştır. Bu sayede Altın Transfer Sistemi'nin blokzincir versiyonu olarak değerlendirilebilecek olan BiGA Projesi çalışmalarına başlanmıştır.

Çalışma grubu, öncelikle blokzincir yaklaşımını kavrayarak, güncel gelişmeleri yakından takip etmeye başlamış ve bu teknolojinin Takasbank'ın finans piyasalarında-

**Takasbank; blokzincir altyapısı kullanılarak kurulması planlanan Güvenilir Varlık Transferi Platformu'nun analiz, tasarım, altyapı, sürekli geliştirme ve yönetiminden sorumlu olmayı önümüzdeki dönem hedeflerinden biri olarak belirlemiştir.**


> Her teknoloji ve inovasyon gibi blokzincirin de Ar-Ge projeleri yapılmadan anlaşılması ve somutlaştırılması yakın vadede mümkün görünmemektedir.

ki rolüne etkileri üzerine çalışmalar yürütmüştür. Blokzincir alanında finansal teknoloji ekosistemini güçlendirmek amacıyla, yerli ve yabancı şirketlerle, konu hakkında çalışan akademisyenlerle iletişime geçilmiştir. Takasbank Ar-Ge personeli, akademik çalışmalarını blokzincir konusunda yapmaya teşvik edilmiştir. Finans sektörünü düzenleyici ve denetleyici kamu kurumlarıyla istişareler ve özellikle TÜBİTAK BİLGEM ile araştırma ve destek anlaşmaları yapılmıştır. Yapılan araştırmalar sonucunda finans sektöründe kullanılabilecek blokzincir platformları belirlenmiş ve her bir platform için farklı iş senaryoları üzerine çalışılarak platformlar hakkında bilgi birikimi edinilmiştir. Oluşan bu bilgi birikimiyle blokzincir platformlarının mevcut durumda finansal projelerde kullanılması için bazı şartları sağlaması gerektiği ve farklı bir yaklaşıma ihtiyaç duyulduğu tespit edilmiştir. Bu sebeple sıfır bilgi algoritmalarını da içinde barındıran bir alanda proje odağı belirlenmiştir.

Proje kapsamında, fiziki altınların kasalarda saklanması ve kaydileştirilmesi süreçlerini yöneten ATS (Altın Transfer Sistemi) ile entegrasyon sağlanmış ve kaydi altınların dijitalize edilerek BiGA'ya dönüştürülmesi ve BiGA'dan kaydi altına çevrilmesi işlemleri mümkün kılınmıştır. Bu sayede uçtan uca fiziki varlık ile dijitalize edilmiş varlık arasında bütün bir yapı kurulmuştur.

Geliştirilen blokzincir altyapısıyla, dijital varlıkların transferi, mutabakatı ve raporlanması sağlanmıştır. Bu altyapı, diğer değerli varlıkların da dijitalleştirilerek transferine izin veren, modüler bir yapıda tasarlanmıştır. Bu sistemde dijital varlık için ihraç, itfa ve transfer olmak üzere üç ana kabiliyet sunulmaktadır. Bunların yanı sıra blokzincir sistemi ile ATS arasında entegrasyon, mutabakat yetkinlikleri, izleme ve raporlama gibi ek kabiliyetler de sağlanmaktadır.

## Projenin Teknik Arka Planı

Projede ilk olarak Hyperledger Fabric 1.0 platformu ile çalışmalara başlanmıştır. Bu aşamada hem teknik çalışmalara giriş, hem de finansal teknoloji ekosistemine destek amacıyla, bu alanda örnek çalışmaları bulunan bir fintek firması ile iş birliğine gidilmiştir. Yine çalışmalara başlanırken Zero Knowledge (Sıfır Bilgi) ihtiyaçları göz önünde bulundurularak, TÜBİTAK BİLGEM Blokzincir Araştırma Laboratuvarı ile iş birliği yapılmıştır. Bu işbirlikler ile özellikle blokzincir temel konsepti ve sıfır bilgi ispatı algoritmalarının blokzincir üzerinde uygulanabilirliği teorik olarak çalışılmıştır. Böylece oluşturulan ekosistem ile projenin teknik temelleri farklı disiplinlerden uzmanların bir araya gelmesi ile atılmıştır.

Hyperledger Fabric ile başlayan geliştirmelerden elde edilen deneyimler sonrasında ikinci aşama, Quorum platformuyla devam etmiştir. Burada sadece söz konusu blokzincir platformları üzerinde çalışılmamıştır. Bu kapsamda kapalı devre bir sistem ve sadece platform yöneticisinin yetki vereceği düğümlerin sisteme dâhil olabileceği bir yapı planlandığı için izin gerektiren yapıda platformlar seçilmiştir. BiGA, izin gerektiren (permissoned) ve özel (private) kategorisinde yer alan bir blokzincir ağına sahiptir.

Projede uygulamada kullanılmak üzere seçilen mevcut blokzincir teknolojilerinin sağladığı altyapılar finansal enstrümanlarda kullanılmak istendiğinde, iki önemli kısıt ön plana çıkmaktadır. Bu kısıtlar, bütün işlemlerin görünür olması durumunda, işlem yapan taraflar dışında, diğer düğümlerin de bütün işlemleri görebilmesi nedeniyle oluşacak mahremiyet problemi ve işlemlerin kapalı olması durumunda işlemlerin bir otorite kurum tarafından kontrol ve denetiminin sağlanamaması problemi olarak tanımlanmaktadır.

BiGA Projesi bu iki kısıta da çözüm üreten bir tasarım sunmaktadır. Bu tasarım işlem yapan düğümlerin ilgili işlemleri görebildiği, sistemdeki diğer düğümlerin ise hassas ve kritik verileri göremediği halde yapılan işlemin ve transferin doğruluğunu onayladığı, aynı zamanda otorite düğümün ise istediği zaman istediği işlemleri izleyebildiği çözümü kapsamaktadır. Bu mimari tasarımın teknik olarak sağlanması, mevcut

blokzincir platformlarına sıfır bilgi ispatı algoritmalarının eklenmesi yöntemini içermektedir. Bu yenilikçi yönü ile proje uluslararası düzeyde patentleme sürecine girmiştir.

Projeyle birlikte dağıtık sistemlerin ve mevcut blokzincir altyapılarının çalışma prensiplerini, mahremiyetini, gizlilik ve bütünlüğünü garanti altına almayı sağlayan konsensus algoritmalarından BFT ve RAFT, kriptografik algoritmalardan homomorphic encyription, range proof, equality proof, Diffie Hellman proof, ECDSA ile blokzincir hesap yapıları ve precompiled kontratlar konusunda çalışma yaparak ileri seviye teknik deneyimler elde edilmiştir. Bu teknik detaylar, konunun sadece bir yazılım süreci işi olmaktan öte derin bir matematik ve kriptoloji bilgisi gerektirdiğini göstermiştir.

İlk olarak 2018 yılı Nisan ayında TÜBİTAK tarafından Ankara' da düzenlenen 1. Ulusal Blokzinciri Çalıştayında bahsedilen BiGA Projesinin tamamlanmış hali ise İstanbul'da düzenlenen ve yine TÜBİTAK BİLGEM tarafından düzenlenen 2. Ulusal Blokzincir Çalıştayında duyuruldu. 2020 yılına kadar pilot proje kapsamında kullanıma alınması çalışmaları yürütülmektedir. Projenin ilerleyen fazlarında ise daha verimli, hızlı ve esnek bir yapı oluşturulması için yine öncü çalışmaların devam ettirilmesi planlanmaktadır.

## Sonuç

Takasbank olarak 2016 yılında aktif olarak başladığımız araştırma sürecinin somut bir proje ile bu noktaya gelmiş olması önemli bir dönüm noktası olarak değerlendirilmektedir. Blokzincir üzerine bireylerin ve kurumların bir miktar literatür araştırmaları yapmaları, çıkan haberleri takip etmeleri sonrasında bir proje yapma fikrinin ortaya çıkması doğaldır. Ancak doğru iş senaryosunun belirlenmesi ve proje ekibinin bu işe odaklanmasının sağlanması aynı zamanda üst yönetimlerin bu konularda öncü olması, blokzincir çalışmaları için büyük önem arz etmektedir.

Takasbank, blokzincir konusunda takip eden değil, takip edilen olma vizyonu ile harekete geçerek hem iş modeli hem de teknik çözümüyle katma değeri yüksek bir Ar-Ge projesini tamamlamıştır. Her teknoloji ve inovasyon gibi blokzincirin de Ar-Ge projeleri yapılmadan anlaşılması ve somutlaştırılması yakın vadede mümkün görünmemektedir. Bu noktada değerlendirme aşamasında olan kurum ve girişimciler için, bir an önce pilot projeler ile yola düşmelerinin önemini vurguluyoruz.

En üst yönetim makamından, projede çalışan uzman personele, iş birimi çalışanlarına ve dış paydaşlara kadar ekip çalışmasının önemi, bu projenin sonuçlanmasında öne çıkmaktadır. Takasbank olarak bu teknolojinin finansal alanlarda kullanılmasının önünde en büyük engel olarak görünen tam mahremiyet ve regülasyona uyumluluk konularında yaptığımız çalışmalarla blokzincir alanında çalışmalar yapan kişi ve kurumlara öncülük etmiş olmaktan gurur duymaktayız.

Projeye ait tüm detaylar ve güncel gelişmeler BiGA. takasbank.com.tr web sitemizde ayrıntılı olarak yer almaktadır. Aynı sitede proje teknik dokümantasyonu tüm ilgililerin istifadesine sunulmuştur.

# Blokzincir Tabanlı

# DİJİTAL KİMLİK YÖNETİMİ

Fatih Birinci - Ens.Md.Yrd. - Dr. Oktay Adalıer - Başuzman Araştırmacı / BİLGEM UEKAE

**Kimlik bilgileri sadece nüfus kayıt bilgileri ile sınırlı olmayıp, hayat boyunca edinilen ve bireyle ilişkilendirilen tüm bilgileri kapsamaktadır.**

İnsanlar doğumlarından başlayarak yaşamları boyunca, birçok alanda hizmet almak veya başkaları ile etkileşime geçmek için, çeşitli kimliklere ihtiyaç duyarlar. Söz konusu kimlikler günlük hayatta kullanılırken, içerdikleri kişisel verilerin de paylaşımı gerekmektedir. Bu bilgiler sadece nüfus kayıt bilgileri ile sınırlı olmayıp, hayat boyunca edinilen ve birey ile ilişkilendirilen tüm bilgileri kapsamaktadır. Tren veya uçak seyahatlerinde, bilet sahibi kişi olduğunu ispat etmekten tutun, işe giriş sırasında üniversite diplomasına sahiplik gibi birçok işlemde, kişisel bilgileri paylaşmak ve doğruluğunu ispat etmek ihtiyacı bulunmaktadır. Kanunen reşit olmayan çocukların, engellilerin ve yaşlıların sorumlulukları da ebeveyn veya vasilerine bırakılmıştır.

Bu işlemlerde hali hazırda kimlik kartı ve diploma gibi basılı evraklar kullanılmaktadır. e-Kimlik ve e-Devlet gibi sistemlerin kullanımıyla, bu tip veriler dijital ortama taşınmaktadır. Bu sistemlerde kişi ile ilgili veriler, ilgili kurum tarafından üretilmekte, saklanmakta ve doğrulanmaktadır. e-Devlet tek noktadan verdiği hizmetle, bu verilere erişimi kolaylaştırmaktadır. Teknolojinin getirdiği hareketlilik, internet erişiminin hızlanması ve yaygınlaşmasıyla, kamu ve özel sektörde verilen hizmetler, elektronik ortamda sunulmaya başlamıştır. Bundan dolayı bireyler, çeşitli kimliklerini internet üzerinden kullanmaya ihtiyaç duymaktadırlar.

## Yasal Düzenlemeler

Dijital verilerin gün geçtikçe daha çok kullanılması ve ekonomik boyutunun olması nedeniyle, bilgisayar korsanlarının dikkatini çekmektedir. Her geçen gün daha çok kişisel veri ihlal haberleri duyulmaktadır. Bunun da etkisiyle ülkemizde ve dünyada (KvKK ve GDPR ) kişisel verileri koruma mevzuatı ile kişisel verilere erişim, işleme ve saklama gibi hususlar sıkı kurallara bağlanmıştır. Bu düzenlemeler vatandaşların mahremiyet konusunda daha çok bilinçlenmesini sağlayarak, mahremiyet odaklı sistemler konusundaki beklentilerini de artırmaktadır. Kurumlar ve hizmet sağlayıcılar, yeni yürürlüğe girmekte olan düzenlemelerin yükümlülüklerini yerine getirmekte zorlanmaktadır. Bunun nedeni, kişi hakkında kimlik doğrulamada ihtiyaç duyulandan fazla veri toplanmasından kaynaklanmaktadır. Bunun azaltılması için kuruluşlar ve yetkililer, hem idari olarak hem de teknik olarak çalışmaktadır.

## Kullanıcı Egemen Sistemler

Tüm bu gelişmelerin etkisiyle, dünya genelinde merkezi kimlik yönetim sistemlerinden, kullanıcı egemen sistemlere doğru bir geçiş olmaktadır. Kullanıcı egemen sistemlerde, kişisel verilerin kullanıcının kontrolünde olması hedeflenmektedir. Bu sistemlerde kişi lerin kendileri ile ilgili verileri istediği taraf ile süreli ve yeteri kadar paylaşımına imkân sağlanmaktadır. Örneğin, dijital diploma gibi kişinin ihtiyaç duyduğu doğruluğu kanıtlanabilir bilgileri, ilgili kurumlar hazırlamaya devam edeceklerdir. Bu verilerin ilgili kurumda tutulmasının yanında, bir kopya sının da kişinin kendisine verilerek, kullanım ve paylaşım kontrolünün kendisinde olması sağlanacaktır. Dijital kimlik sistemi, mahremiyet artışı sağlama dışında, iş süreçlerinde hızlanma ve verimlilik artışı da getirecektir.

## Blokzincirin Katkıları

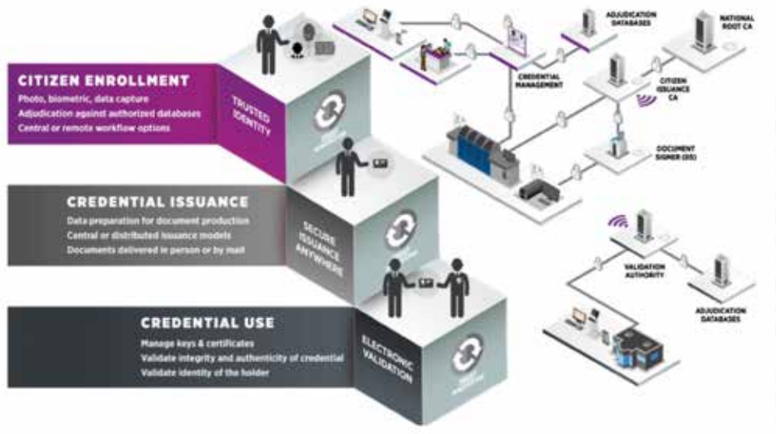
Blokzincir teknolojisinin dijital kimlik sistemlerine sağlayacağı katkılar genel olarak şunlardır:

- Yetkili kişilerce yapılan işlemlerin, gerekli kontrollerden sonra blokzincire uzlaşma ile yazılması,
- Blokzincire kaydedilen verilerin değiştirilememesi, ancak yeni işlemlerle güncellenebilmesi,
- Birden fazla noktada güvenli olarak tutulması ve merkezsiz olması,
- Blokzincire yazılan kurallar ve kod parçacıklarıyla, akıllı sözleşmelerin çalıştırılabilmesine olanak sağlaması.

## Riskler ve Zorluklar

Kişisel bilgilerin özeti dahi olsa yazılan verilerin silinememesi, kişisel verileri koruma mevzuatı açısından blokzincirin dijital kimlikte kullanımını zorlaştırmaktadır. Yazılan verilerin şifreli olması ve ilgili anahtarın silinmesinin yeterli olup olmayacağı konusundaki tartışmalar hala sürmektedir. Blokzincire kişisel verilerin yazılması, kullanıcı egemen sistemlerin prensiplerine de aykırı görünmektedir. Dolayısıyla kişisel bilgilerin kullanıcının kendisinde tutulması, daha uygun bir çözüm olacaktır.

Dijital veriler doğası gereği kolayca oluşturulabilir, değiştirilebilir ve kopyalanabilir. Bu bilgilerin orijinal olduğunun ve sahibinin gerçekten ilgili kişi olduğunun ve kullanımı esnasında da doğru kişi tarafından kullanıldığının kimlik doğrulama sistemi ile kontrol edilmesi gerekmektedir. Bu amaçla parola gibi zayıf kimlik doğrulama yöntemlerinden ziyade, güçlü kriptografik yöntemler kullanılmalıdır. Kullanılan yöntemlerdeki kriptografik anahtarların yönetilmesi gerekmektedir. Blokzincir, verilerin tutulması yerine anahtarların yönetimi için kullanılabilir. Oldukça iyi mahremiyet (pretty good privacy) kapsamında, "web-of-trust"

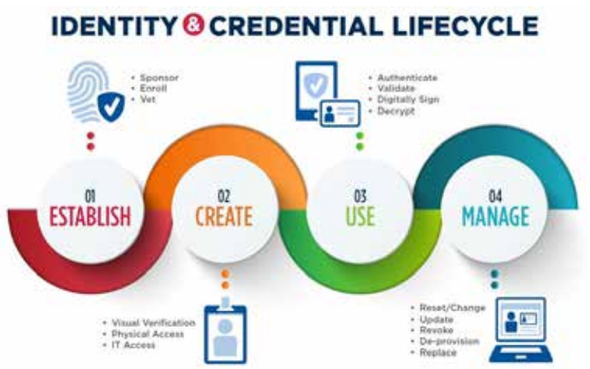



adlı anahtar yönetimi kullanıma sunulmuş, fakat kullanım zorlukları nedeniyle yaygınlaşamamıştır. Blokzincir kapsamında kullanıma sunulacak bir anahtar yönetim sistemi, gelecek vadedebilir mi, bunu zaman içerisinde göreceğiz.

## Anahtar Sistemi ve Zaman Damgası

Günümüz açık anahtar sistemlerinin kullanım açısından bazı zorlukları vardır. Örneğin üniversite tarafından düzenlenen dijital diploma üzerine atılacak nitelikli imzanın geçerliliği, imzada kullanılan anahtarın geçerliliğinin sona ermesi ile bitecektir. Diplomanın geçerliliğinin devam etmesi için, ilgili anahtarın geçerli olduğu sırada, imza işleminin gerçekleştiğini kanıtlamak için, zaman damgası alınması gerekmektedir. Zaman damgasının da bir geçerlilik süresi vardır. Bu süre dolmadan yeni zaman damgası ile uzatılması gerekmektedir.

Kullanıcı egemen sistemlerde, dijital diplomanın kontrolünü kullanıcıya vereceğimiz düşünüldüğünde, diplomanın geçerliliğini zaman damgası ile uzatma gibi işlemleri, kullanıcıdan beklememiz gerekecektir. Kullanıcının bu işleri zamanında yapması çok zor olacaktır. Bu hem maliyetli bir işlemdir, hem de yapılmadığı takdirde diplomanın geçerliliği kalmayacaktır. Bunu yapmak yerine kullanıcının ihtiyacı olduğunda, üniversiteden yeni imzalı bir dijital diploma alması daha kolay o lacaktır. Diplomanın mezuniyetten uzun süre sonra bile gerekli olabileceği dikkate alınırsa, bunun için üniversitedeki ilgili servise kayıt olma gibi zorluklar, kullanıcının kendisini beklemektedir.




Blokzincirde kişiler kendi anahtarını kendisi üretmektedir. Bu anahtarların geçerlilik süresi sınırlandırılmamaktadır. Blokzincirin doğası gereği yapılan işlemler, zaman damgalı olarak kaydedilmektedir. Zaman damgasının uzatılma ihtiyacı da bulunmamaktadır. Dolayısı ile blokzincirden alınan bir anahtar ile imza atılması durumunda, diplomanın geçerliliğinin uzatılması için, herhangi bir işleme gerek olmayacaktır.

Blokzincirde anahtar yönetiminin zorlukları da bulunmaktadır. Üniversite tarafından verilecek bir diplomanın çeşitli nedenlerle iptal edilmesi gerekli olabilecektir. Bunun için verimli bir iptal mekanizmasının blokzincirde kullanımı gerekmektedir.

## Dağıtık Kimlik Tanımlayıcıları *(Decentralized Identifiers-DID)*

Wold Wide Web konsorsiyumu (W3C) bünyesindeki çalışma gruplarında geliştirilen iki standart, bize bu konuda yol göstermektedir. Bunlardan birincisi, dağıtık kimlik tanımlayıcıları olarak çevirisini yapabileceğimiz Decentralized Identifiers (DID), ikincisi ise doğrulanabilir referans bilgisi olarak çevirebileceğimiz Verifiable Credential (VC) standartlarıdır.

Dağıtık kimlik tanımlayıcılarının sistemde tekil olması önemlidir. Tekil olacak şekilde rasgele oluşturulabileceği gibi, kişinin açık anahtarından da elde edilebilir. Bunlar, DID dokümanının yerini gösteren bir işaretçi görevi görürler.

Kullanıcılar tüm anahtarları ve DID'leri kendileri oluşturacaklardır. Dolayısı ile açık anahtara karşılık gelen özel anahtarı, sadece kendileri biliyor olacaktır. Bu nedenle özel anahtar ile yapılan işlemleri, sadece ilgili kişinin yapmış olabileceği varsayımında bulunmamız doğru olacaktır. Dijital kimlik sistemlerinde, kişinin adı yerine DID bilgisi kullanımıyla, kişinin mahremiyetinin artırılması sağlanabilecektir.

## Doğrulanabilir Referans Bilgileri

Bu bilgiler, bir kurum tarafından dağıtık kimlik tanımlayıcıları ile ilişkilendirilerek verilen ve doğruluğu garanti etmek için düzenleyicisi tarafından dijital olarak imzalanan bilgilerdir. Örnek olarak; eğitim sertifikası, diploma, ikametgâh, çalışma ve maaş bilgisi, kimlik, pasaport, kredi kartı ve limit sahipliği, üyelik bilgisi gibi bilgilerdir. Doğrulanabilir bilgilere geçerlilik süresi de verilebilir. Bu bilgiler, düzenleyicisi tarafından gerektiğinde geçerlilik süreleri dolmadan iptal edilebilir olmalıdır.

Sistemde üç temel rol olacaktır. Bunlar, "bilgi sahibi kişi", "düzenleyici" (örneğin üniversite) ve "bilgiyi kullanan" rolleridir. Kişinin üniversiteden dijital diploma aldığı ve bu veriyi iş başvurusu sırasında işveren ile paylaştığı kullanım senaryosunu inceleyelim.

## Dijital Diploma ile İlgili Uygulama Senaryosu

Bu işlemlerin güvenli yapılması son derece önemlidir. Bu işlem öğrencinin üniversiteye gitmesi ile yapılabileceği gibi uzaktan da yapılabilir.

**Diploma düzenlenmeden önce yapılması gerekenler şunlardır.**

- Mezun olan ya da mezuniyeti yaklaşan kişinin öncelikle DID edinmesi ve bu DID'in (açık anahtar ile birlikte) kendisine ait olduğunu üniversiteye bildirmesi gerekmektedir.
- Açık anahtara karşılık gelen özel anahtarı sadece öğrencinin bilmesi gerektiğinden, açık ve özel anahtarı öğrenci oluşturmalıdır.
- Üniversite tarafından, öğrencinin kendisine verdiği DID'e karşılık gelen özel anahtarın öğrenci tarafından bilindiğinin kontrolü yapılmalıdır.
- DID'in karşılığı DID dokümanı da blokzincir'e yazılmalıdır. DID dokümanı blokzincire üniversite tarafından yazılabilir.
- Üniversite, öğrencisinin gerçek kimliğini bildiği için, gerçek kimlik ile dijital diplomanın düzenleneceği DID'i kendi kayıtlarında ilişkilendirir.

**Diploma düzenleme aşamasında üniversite tarafından yapılacak işlemler aşağıdaki gibidir.**

- Üniversite'nin doğrulanabilir bilgi düzenleyicisi olarak, bir DID'e sahip olduğunu varsayalım. (Burada temel rol ler anlatıldığı için, düzenleyici DID'inin nasıl alınacağına değinilmemiştir.)
- Üniversite doğrulanabilir bilgi düzenleyicisi olarak, kişinin DID'i ile ilişkilendirerek bir dijital diploma düzenleyecektir.
- Dijital diploma, üniversitenin DID'ine karşılık gelen özel anahtarı ile imzalanacaktır.
- Dijital diploma ve iptal kontrolü için gerekli bazı bilgiler kişiye verilecektir.
- İptal kontrolü için diğer bazı bilgiler de blokzincire yazılacaktır.

**Üniversite bu belgeyi imzalayarak şunları onaylamış ve kefil olmuş olacaktır.**

- Dijital belgede yazılı DID sahibi kişinin kimliğini doğruladım ve gerçekte kim olduğunu biliyorum.
- Bu kişi hakkında dijital belgede yazan bilgiler doğrudur. Bu bilgiler lisans, yüksek lisans ve doktora derecesi için mezuniyet tarihi ve ortalaması gibi bilgilerdir.
- Dijital belge günceldir. Bu amaçla iptal bilgilerinin kontrolü gereklidir.

Kişi bu diplomayı ve iptal kontrolü için gerekli bilgileri, kendisinde tutacak ve gerekli olduğunda örneğin işvereni ile paylaşabilecektir. İşlemlerin hızlı ve kesintisiz olması için, işverenin üniversite ile iletişime geçmeden diplomanın geçerlilik kontrollerini yapması hedeflenmektedir. Çünkü dijital kimlik sistemi içeriğini oluşturan, üniversite gibi birçok doğrulanabilir bilgi düzenleyicisi olacaktır. Sistem kapsamındaki tüm kurum (örneğin üniversite) sunucularının, her zaman cevap verebilir durumda olmasını garanti etmek zordur. Bu sunu culara yapılacak siber saldırı sonucu hizmet kesintileri yaşanabilir. Bunun yerine blok zincirdeki bilgileri kullana rak doğruluk kontrolü yapılması hedeflenmiştir. Blokzincire doğası gereği birçok noktadan ulaşılabildiği için, hizmet sürekliliği sağlamak çok daha kolay olacaktır.

İş başvurusu sırasında, kişinin dijital diploma ve iptal bilgilerini işverene vermesinin ardından, işve ren tarafından yapılacaklar ise aşağıdaki gibidir. Bu işlemlerin uzaktan yapıldığı varsayılmaktadır.

- Dijital diploma üzerine üniversite tarafından atılan imzanın kontrolü yapılmalıdır. Bu amaçla üniversitenin DID dokümanının blokzincirden alınması gerekmektedir.
- Dijital diplomanın kontrolün gerçekten işe başvuran ve iletişim halinde olunan kişide olduğunun doğrulanması gerekmektedir. Bu adım çok önemlidir. Çünkü dijital veriler çok rahatlıkla kopyalanabilir. İşverenin karşısında gerçekten diplomaya sahip kişinin olduğunu bilmesi önemlidir. Bu doğrulamada temel olarak işe başvuran kişinin DID'ine karşılık gelen özel anahtarın, iletişim halinde olunan tarafta olup olmadığı kontrol edilir.
- Blokzincirden iptal bilgileri alınarak diplomanın iptal edilip edilmediği kontrol edilir.

Doğrulanabilir bilgideki tüm içeriğin karşı tarafa gönderilmesi gerekmeyebilir. Bu mahremiyet açısından da sakıncalıdır. Örneğin bankanın kredi vermek için, kişinin maaşının kaç lira olduğunu bilmesine gerek yoktur. Maaşın belirli bir meblağın üzerinde olduğunu bilmesi yeterlidir. Doğrulanabilir referans bilgileri standardı, sıfır bilgi protokolleri kullanımı ile buna müsaade etmektedir. Kişi, dijital maaş bordrosunun tamamını bankaya göndermeyecek, sadece bordrodaki maaşın bankanın belirlediği limitin yukarısında olduğunu kanıtlayan bir bilgiyi bankaya gönderecektir. Banka kendisine gelen bilgilerin doğruluğunu kontrol ederek ikna olacaktır.

Tüm doğrulanabilir bilgilerde kişinin aynı DID'i kullanması mümkün olmakla birlikte, mahremiyet açısından önerilmemektedir. Mahre miyetin artırılmasını sağlamak amacıyla, kişi farklı doğrulanabilir bilgileri için farklı DID kullanabilir.

Bir kişinin farklı DID'lerle edindiği farklı doğrulanabilir bilgileri (örneğin, çalışma belgesi ve ikametgâh belgesi) birlikte kullanma ihtiyacı doğabilir. Bu farklı DID'leri kontrol eden kişinin aynı kişi olduğunu ispatlaması gereken durumlar olabilir. Detayları doğrulanabilir referans bilgileri standardında yer alan kriptografik tekniklerle, bunu ispat etmek mümkün olabilmektedir.

## Genel Değerlendirme

Blokzincir tabanlı dijital kimlik tanımlama sistemi, dağıtık mimaride kimlik yönetimini desteklemekte olup, kişilere kendi kimliklerini yönetme imkânı tanımaktadır. Merkezi otoriteler aradan çıkartılarak, bireysel bazda kimlik yönetimi sistemi gündeme gelmektedir.

Uluslararası kuruluşlar, bazı durumlardan kendi ülkesi tarafından sahip çıkılmayan ve kimliksiz olan insanlara dijital kimlik vermeyi bile öngörmektedir. Birleşmiş Miletler tarafından kimlik verilme durumunda, gelişmekte olan ülkelerde hangi tür kimliklere insanların yönelebileceği tartışılmaktadır. Bu tür yaklaşımlar, merkezi otoriteyi ve insanların kendi ülkelerine olan bağlarını zayıflatmakta, aidiyet duygusunun ise eksen değiştirmesine yol açmaktadır. Ulusal güvenlik açısından bu gelişmeler takip edilmeli ve yine aynı teknolojiler kullanılarak ulusal çözümler geliştirilmelidir.

# Blokzincirde
## GÜVENLİK VE MAHREMİYET


> Verilerin dağıtık olarak tutulması fikri, merkezi yapılaşmanın sakıncalarını ortadan kaldırsa da güvenlik ve mahremiyetle ilgili potansiyel sorunları da beraberinde getirmektedir.

Dr. Muhammed Ali BİNGÖL - Başuzman Araştırmacı / BİLGEM UEKAE

Geleneksel finansal sistemler, özellikle günümüz bankacılık sistemi, merkezi yetkili otoriteler, arabulucular ve benzeri üçüncü kişilerin tesis etmekte olduğu "güven" olgusuna dayanmaktadır. Bitcoin manifestosu ile birlikte, bu merkezi güven olgusu yerine adem-i merkeziyetçi (decentralized) bir yapı olan blokzincir teknolojisi ortaya çıkmıştır. Böylece dağıtık ağ yapısı sayesinde, blokzincir üzerinde gerçekleştirilen işlemlere ait kayıtların tek bir merkezde tutulması yerine, herhangi bir merkezi yetkiye sahip olmayan düğümler tarafından kayıt altına alınması sağlanmıştır.

Blokzincirler, bu karakteristiği ile güvenin esas tutulduğu pek çok sektörü ve iş süreçlerini derinden etkilemiş ve birçok uygulamanın tekrar bu mantık ile kendini gözden geçirmesine neden olmuştur. Verilerin dağıtık olarak tutulması fikri, merkezi yapılaşmanın sakıncalarını ortadan kaldırsa da güvenlik ve mahremiyet ile ilgili potansiyel sorunları da beraberinde getirmektedir.

### Blokzincirde Mahremiyet

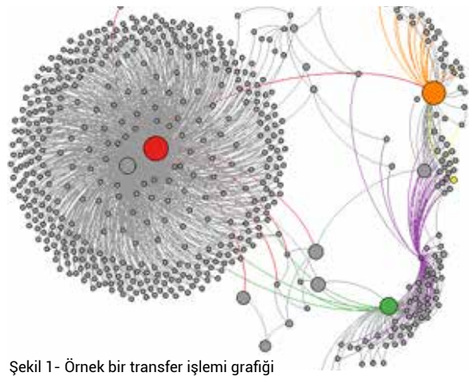
Güncel verilere göre yaklaşık 2350'ye yakın kripto para bulunmaktadır ve bunların yalnızca 65'i mahremiyet sağlama hedefi ile ortaya çıkmıştır. Ayrıca bütçe olarak mahremiyet sağlamayı hedefleyen kripto paralar toplam bütçenin yalnızca %0,8' ini oluşturmaktadır. Bu kripto paraların da mahremiyet özelliklerini tam anlamı ile karşıladığını söylemek oldukça güçtür.

Mahremiyetle ilgili literatüre baktığımızda üç önemli unsur karşımıza çıkmaktadır: Transfer edilecek paranın miktarı, gönderici bilgisi ve alıcı bilgisi. Günümüz bankacılık sistemlerinde bir para transferi işlemi yalnızca gönderici alıcı ve merkezi yapı olan banka tarafından gözlenmesine karşın, mahremiyet sağlamayan örneğin bir kripto para transferinde ise herkes tarafından izlenebilmektedir.

Bunu bir örnekle ifade edecek olursak: merkezi finansal sistem yerine, merkezi olmayan blokzincir tabanlı bir sistem getirdiğimizi ve günlük tüm işlemlerin blokzincir tabanlı yapılar üzerinden yapıldığını hayal edelim. Bir firmanın ya da kurumun, maaşları blokzincir tabanlı bir para ile ödediğini düşünelim. Bu durumda, bu firmanın kaç çalışanının olduğu, çalışanlara hangi ücret aralıklarında maaş ödendiği gibi istatiksel bilgiler, maaş ödeme dönemlerinde herkes tarafından gözlenebilecektir. Gerçek hayattan bir örnek verecek olursak, 06 Eylül 2019 tarihinde blokzincir üzerinde gerçekleştirilmiş en yüksek değerli para transferi duyuruldu. Bu transfer 94.504 BTC olarak gerçekleştirilmiş ve o tarihte yaklaşık 1 milyar dolar seviyesinde bir transfere tekabül etmekteydi.

> Güncel verilere göre yaklaşık 2350'ye yakın kripto para bulunmaktadır ve bunların yalnızca 65'i mahremiyet sağlama hedefi ile ortaya çıkmıştır.

Günümüzdeki hemen hemen bütün kripto paralardaki blokzincir yapılarında, kişilerin gerçek kimlikleri para transferi sürecinde kullanılmaz. Bunun yerine kullanıcılar, sistemden aldıkları "sözde isim" bilgisi (pseudonym) ile para transferi yaparlar. Doğal olarak akıllara sözde isim kullanılmasının mahremiyeti sağlayıp sağlamayacağı gelmektedir. 2011 yılından itibaren yapılan çalışmalar göstermiştir ki eğer belirli bir sayının üzerinde bir yoğunlukla para transferi yapılıyorsa, transfer işlemi grafikleri üzerinde analizler yapılarak para transferleri takip edilebilmektedir. Ayrıca bazı diğer sosyal mühendislik çalışmaları sayesinde, transfer yapan kişilerin kimliklerine kadar ulaşılabildiği gösterilmiştir. Şekil 1'de de örnek bir transfer işlemi grafiği gösterilmiştir.



Şekil 1- Örnek bir transfer işlemi grafiği

Bu örnekler de göstermektedir ki, günümüz finansal sistemi olarak blokzincir teknolojisine tamamen geçilmesi için, öncelikle birçok mahremiyet probleminin çözüme kavuşması gerekmektedir.

Blokzincirlerde mahremiyet sağlama kapsamında, işlemlerin kaynaklarının ve hedeflerinin gerçek kimliklerle bağdaştırılamaması ve birbiri ile ilişkilendirilememesi (anonymity, untraceability), işlemlerdeki içeriklerin gizlenmesi, durum verilerinin gizlenmesi hedefleri, farklı seviyelerde karşılanmaya çalışılır. Blokzincirin doğası gereği, verilerin bütün düğümlerde kopyasının bulunduğu ve işlenmesi gerektiği göz önüne alındığında, mahremiyet hedeflerini sağlamanın güçlüğü de anlaşılabilir. Bu temel bileşenlerin yanında, mahremiyet konusunda da yetenekler eklenmesi hedeflendiğinde, kullanılabilecek yapıtaşlarının sayısı ve kullanım kombinasyonları artmaktadır.

## Blokzincirde Güvenlik

Blokzincirlerde kullanılan güvenlik mekanizmalarının büyük bir kısmı yıllardır kullanılmaktadır. Kripto Teknolojileri kapsamında, Blokzincirin en önemli vizyonu olan güvenlik fonksiyonunu sağlamak için çeşitli bileşenler kullanılır. Özellikle kriptografinin çeşitli bileşenleri, bu amaçla farklı kombinasyonlarda kullanılır. Bitcoin ile tanıştığımız örnekteki özet (hash) [4] ve dijital imza (signature) [5] bileşenleri, neredeyse bütün blokzincir gerçeklemelerinde kullanılan yapıtaşlarıdır.

Özet, blokların değiştirilemezliğini sağlamak ve blok oluşturma işleminde uzlaşma sağlamak için kullanılır. Dijital imza ise, en temel olarak işlemlerin kaynağının doğrulanması için kullanılır. Özet ve Dijital imzanın çeşitli versiyonları, hedeflenen güvenlik ve performans seviyelerine göre tercih edilmektedir. Çoğunluğu Eliptik Eğri Kriptografi (ECC) teknolojisini kullanır. Bunun yanında kuantum kriptoya dayanıklı olduğu bilinen Hash Tabanlı imza teknolojisi de kullanılmaktadır.

> **Günümüz finansal sistemi olarak blokzincir teknolojisine tamamen geçilmesi için öncelikle birçok mahremiyet probleminin çözüme kavuşması gerekmektedir.**

Üzerinde durulması gereken bir diğer popüler konu ise, kuantum teknolojisinin blokzincir üzerindeki etkisidir. Bilindiği üzere blokzincirin temelinde kriptografik algoritmalar yatmaktadır. Günümüz süper bilgisayarları yardımıyla geliştirilen algoritmalar, kuantum bilgisayarlarının kullanımının pratikleşmesi ve yaygınlaşması sonucu, kırılması eskisi kadar zor olmayan algoritmalar durumuna düşecektir. Kriptografik işlemelere ait izler, her düğüm üzerinde depolandığı için, gelecekte, kuantum bilgisayarın hayata geçmesi durumunda, hem geriye doğru bilgilerin ortaya çıkması, hem de varlıkların izinsiz el değiştirebilmesi olasıdır. Ayrıca yaşanabilecek aksilikler geriye dönülmez sonuçlar doğurabilir. Bu yüzden kuantum teknolojisi ile yeni kriptografik algoritmaların geliştirilmesi için ivedilikle hareket edilmesi gerekmektedir.

## Kriptografik Yapıtaşları

Blokzincir'in en önemli özelliği olan güvenlik fonksiyonunu sağlamak için kriptografik bileşenler, çeşitli kombinasyonlarda kullanılır. Bitcoin'in "kripto para" olarak adlandırılmasının sebebi, işleyişini iki kriptografik yapıtaşına borçlu olmasıdır. Bu iki kriptografik temel yapıtaşı, özet (hash) fonksiyonu ve elektronik imzadır (signature). Blokzincirlerde kullanılan kriptografik bileşenler, genel olarak, kullanım amaçlarına göre iki gruba ayrılabilir:

- Blokzincir sisteminin kendi güvenliğini sağlayanlar
- Blokzinciri kullanan kullanıcılar ve verileri için fazladan (mahremiyet ve anonimlik amaçlı) güvenlik sağlayanlar

İlk grupta bulunan özet ve sayısal imza bileşenleri, neredeyse bütün Blokzincir gerçeklemelerinde kullanılan ortak yapıtaşlarıdır. Özet algoritmaları, blokların içindeki işlem kayıtlarını ve blokların kendilerini mühürleyerek değiştirilemez olmasının sağlanması, blok üretme işlemindeki emek ispatı (ing. Proof of Work - PoW) bulmaca hesabı ve bilgileri adresleme amacıyla (hesap, işlem, blok, hesap) kullanılır. Özet algoritmaların bir diğer kullanım amacı ise, blokzincir dışındaki sistemlerde tutulan bilgilerin özet değerlerinin, bu bilgilerin belli tarihte varlığının kanıtı olarak blokzincir üzerinde tutulmasıdır. Sayısal imza algoritmaları ise en temel olarak, işlemlerin kaynağının doğrulanması için kullanılır. Özet ve dijital imzanın çeşitli versiyonları, hedeflenen güvenlik ve performans seviyelerine göre tercih edilmektedir. Çoğunluğu Eliptik Eğri Kriptografi (ECC) teknolojisini kullanır. Ayrıca, kuantum kriptoya dayanıklı olduğu bilinen Hash Tabanlı imza teknolojileri de kullanılmaktadır.



İkinci gruba, Sıfır bilgi ispatları (ing. Zero-knowledge proofs), taahhütler (ing. commitments), akümülatörler (ing. accumulators), simetrik şifreleme ve homomorfik şifreleme teknolojileri, işlemlerin (karşılaştırma, doğrulama, toplama, çıkarma vb.) verinin kendisi yerine gizlenmiş halleri ile yapılmasını sağlamak amacıyla kullanılır. Özel imzalama (Ring-signature ve türevleri, Multi-signature, Blind Signature vb.) teknolojileri ise işlemi başlatan kişilerin kimliklerinin gizlenmesi, imzalanan verinin gizlenmesi vb. mahremiyeti artırıcı amaçlarla kullanılır. Eşik İmza (ing. Threshold Signature) veya Eşik Kriptografi (ing. Threshold Cryptography) teknolojisi ise işlemleri birden fazla kişinin başlatabilmesine olanak vermek amacıyla kullanılır. Blokzincirin güvenliği (bütünlüğü ve işlemlerin orijinini doğrulama) amaçlı yapıtaşları, ön tanımlı olarak zincir içi (ing. on-chain) olarak yerleşmişken, mahremiyet amaçlı olanlar zincir dışı (ing. off-chain) kullanılan bileşenler olarak karşımıza çıkmaktadır.

## Mutabakat Protokolleri

Mutabakat protokolleri blokzincir platformunun karakteristiğini oluşturan ve kayıtların bütün düğümlerde aynı şekilde güncellenebilmesini sağlayan bileşendir. Blokzincir ağ bilgisayarlarının kötü niyetli olabileceği varsayılır. Blokzincir sistemlerinde görülen ve sistemin bileşenlerinden bazılarının kötü niyetli davranması ile ortaya çıkan arıza türleri, Byzantian Failures/Faults olarak adlandırılır. Blokzincirlerinde bu hataları bertaraf ederek verinin bütün kopyalarının birbiri ile aynı olmasını sağlamak için mutabakat protokolleri kullanılır. En çok bilinenleri PoW, PoS, DPoS, PoC, PoE, PoET, PoA, PoB, PoI, BFT, PBFT, DBFT olan yetmişten fazla mutabakat protokolü vardır [6].

Kullanılabilecek mutabakat protokolü, blokzincirin türü ile doğrudan ilişkilidir. Açık bir blokzincirde risk daha yüksek olduğu için PoW (Proof of Work) gibi daha güçlü (ama maliyetli) algoritmalar kullanılır. Emek ispatı olarak adlandırılan PoW tabanlı mutabakat, ilk olarak Bitcoin ile kendisini ispatladığı için Nakamoto konsensüs yöntemi olarak da adlandırılır [7]. Bu yöntemde, sistemin kayıt defterine yeni bir blok üretip eklemek isteyen blokzincir düğümlerinin (madenciler), sistemin belirlediği zorluk derecesindeki bir kriptografik bulmacayı diğer düğümlerden önce çözmeleri gerekir. Bu bulmaca, genellikle üretilen aday blok'un içindeki değişken bir sayıyı (teksa) sürekli değiştirerek bir özet algoritması ile hesaplanan blok özet değerinin, sistemin dinamik olarak belirlediği zorluk derecesiyle belirlenmiş olan belli bir değerden daha küçük olmasını sağlamak üzere, deneme yanılma ile yoğun elektrik sarfiyatına da sebep olacak bir şekilde özet hesaplama şeklindedir.

En basit ifadeyle özet değerinin belirli bir değerden küçük olmasını sağlayan bir "teksa" bulunmasıyla blok, kayıt defterine eklenmeye hazır hale gelir. Bitcoin sistemi, zorluk derecesini (difficulty level), sistemdeki madenci bilgisayarlarının toplam özet alma gücüne göre iki haftada bir adaptif olarak güncelleyerek, bulmacasını çözerek yeni bir blok üretme süresini, ortalama 10 dakika olacak şekilde sabit tutmaya çalışır. Bitcoin gibi bazı kripto para platformları, blok üreten madencilerin hesabına ödül olarak bitcoin ekler. Yaygın olarak madencilik (mining) ismi ile bilinen bu yöntemle sistemde para üretimi de gerçekleşmiş olur. Hash bulmacası çözülen aday blok, diğer düğümlere de bildirilir. Diğer madenci bilgisayarları, aldıkları bu blok duyurusunu, kendileri de bazı kontrollerden geçirirler (kayıt defterinin geçmişi ile uyum, vb.). Bitcoin sisteminin bütün dünyaya yayılmış büyük bir şebeke olması nedeniyle bazen veri iletimindeki gecikmelerden dolayı, şebekenin farklı bölgelerinde, kayıt defterinin farklı blokzincir dallarını içeren sürümleri oluşabilir. Ama mutabakat protokolüne göre, madenci bilgisayarları, kendilerine sonradan ulaşan blok zinciri bilgilerine bakarak, alternatif dallar arasında, farklılaşmanın başladığı noktadan itibaren en uzun olan blok zincirini asıl zincir olarak kabul ederek kendi kayıt defterlerini güncellerler.

Bir diğer yöntem ise PoS (Proof Of Stake), hisse ispatına dayalıdır. Üretilen blokların doğrulaması ve onaylanması işinde, madencilerin, sistemdeki kendi kripto para hisseleri ile orantılı olarak söz hakkı bulunur. Hile yaptığı tesbit edilen madencinin hisseleri elinden alınır.

İzinli blokzincir türlerinde ise oyuncuların daha bilinir olması ve düğümlerin çalışma ortamının nispeten daha kontrollü olması nedeniyle genelde BFT (Byzantine Tault Tolerance) denilen, çoğunlukla düğümler arası etkileşim (oylama vb.) gerektiren mutabakat yönetiminin türevleri kullanılır. Birden fazla çeşitte mutabakat algoritmasını içeren hibrit kullanım örnekleri de vardır. Hibrit olarak en çok PoW ve PoS yöntemleri birlikte kullanılır.

*Kaynakça*
*[1] Coinmarketcap internet sitesi: https://coinmarketcap.com/*
*[2] Privacy Cryptocurrencies: CryptoSlate: https://cryptoslate.com/cryptos/privacy/ ve CoinLore: https://www.coinlore.com/privacy-coins.*
*[3] The Independent: https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-mystery-trade-cryptocurrency-market-transaction-blockchain-a9103611.html*
*[4] NIST 180-4 - Federal Information Processing Standards (FIPS) Publication 180-4, Secure Hash Standard (SHS). National Institute of Standards and Technology (2015).*
*[5] NIST 186-4 - Federal Information Processing Standards (FIPS) Publication 186-4, Digital Signature Standard(DSS). National Institute of Standards and Technology (2013).*
*[6] Major Blockchain consensus algorithms, https://www.tokens-economy com/2019/06/19/major-blockchain-consensus-algorithms-infographics-version-2019-6/*
*[7] Andreas Antonopoulos Mastering Bitcoin, https://goo.gl/fofWQe, Temmuz 2014.*

# Blokzincir Üzerinde Mobil Kimlik Yönetimi

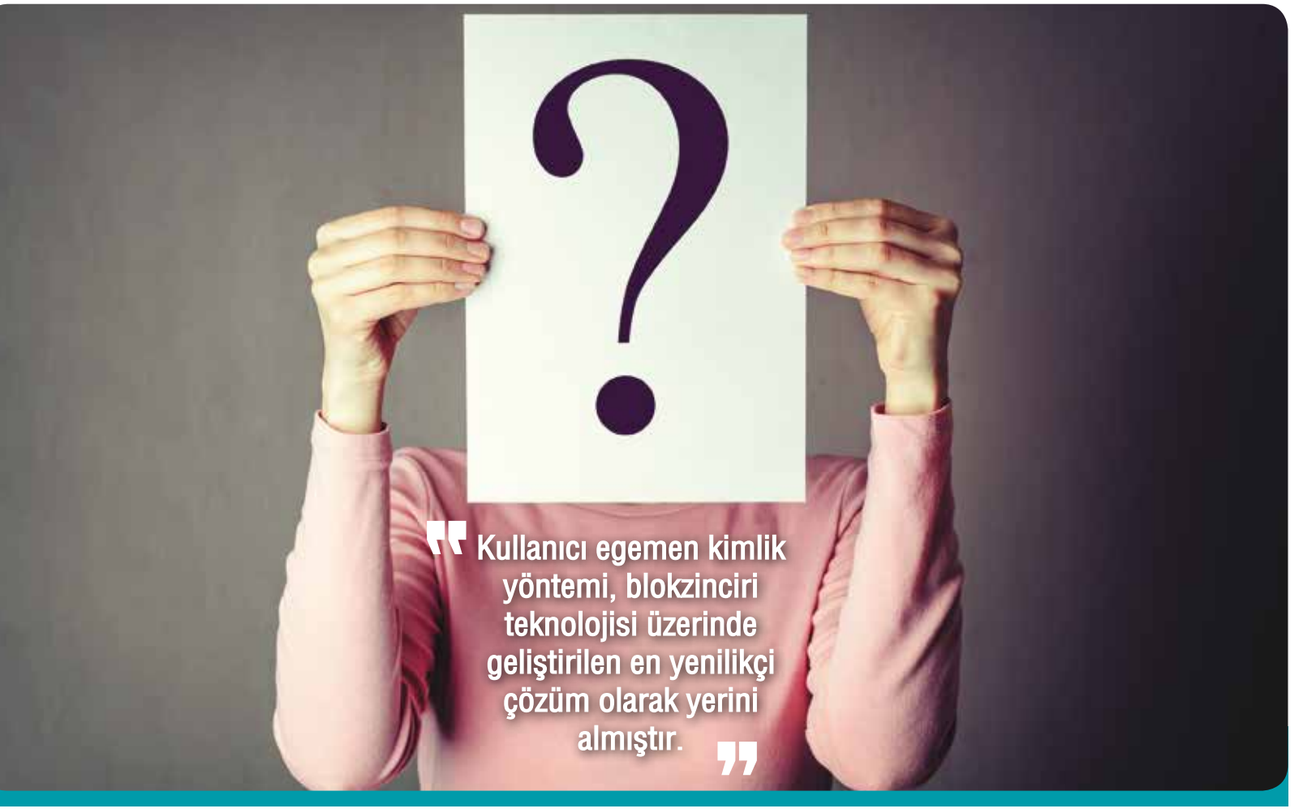
**Kimlik bizi biz yapan sahip olduğumuz özelliklerin bütünüdür.**

Serhan Mert Kır - Recep Yıldız / Turkcell

Kimlik bizi biz yapan sahip olduğumuz özelliklerin bütünüdür. Günlük hayatta yasal yükümlülüğü olan işlemlerde kullandığımız kimlik kartlarımız, kimliğimizin bir parçasıdır. Kimlik kartı, pasaport, sürücü belgesi gibi resmi kimliklerimizin dışında, mezun olduğumuz okulun verdiği mezun kartı, çalıştığımız şirketin giriş kartı, üyesi olduğumuz kurumların sadakat kartları, sanal ve fiziksel ortamlara giriş için kullandığımız kartlar gibi farklı kimlik kartlarımız da bulunmaktadır. Hatta kişisel özelliklerimiz ve sahip olduğumuz yetenekler gibi, bir kart olarak taşımadığımız, ama bize ait olan ve güvenilir kurumlar tarafından onaylanabilen çeşitli niteliklerimiz de, kimliğimizin birer parçasıdır.

Bu özellikler birleşerek bizim kimliğimizi oluşturur. Bu özelliklerin alt kümelerini kullanarak çeşitli firmalarla işlemler yaparız. Örneğin, bir e-ticaret işlemi yaparken ad, soyad, adres ve kredi kartı bilgilerimizi, bankaya giriş yaparken müşteri hesap numarası ve şifremizi, bilet alırken kredi kartı bilgilerimizi, yemek siparişi verirken adres bilgilerimizi paylaşırız. Kimlik kartı bilgilerimizi yüz yüze, çevrimiçi ve çağrı merkezi gibi farklı kanallarda işlem yaptığımız firmalarla paylaşırız.

Günlük hayatımızda kimliğimizi çok farklı amaçlarla kullanırız. Örneğin, bugün başka bir şehirde bir etkinliğe katıldığımızı düşünelim. Evden çıkarken kapıyı kilitleyerek kimlik ile ilgili ilk işlemi yapmaya başlıyoruz. Burada kapı anahtarı sadece kimliği




bilinen yetki verilmiş kişilerin eve girebilmesi için, bir fiziksel yöntem oluşturuyor. Daha sonra havaalanına ulaşım için kullandığımız taksi ücretini kredi kartıyla ödememiz durumunda, kredi kartına sahip olduğumuzu hem fiziksel olarak, hem de girdiğimiz şifre ile doğruluyoruz. Havaalanına girişte güvenlikten geçerken sunduğumuz kimlik ve uçak bileti, yine kimliğimizin bir parçasını oluşturuyor. Bileti kullanarak geçerli bir uçuşta koltuğumuz olduğunu, kimliğimiz ile de bu bilete sahip olduğumuzu kanıtlıyoruz. Daha sonra etkinliğin yapıldığı adrese geldiğimizde, kapıda tekrar bir kimlik doğrulama sürecinden geçiyoruz. Bize gün boyunca o adreste bulunmaya yetkimiz olduğunu gösteren bir yaka kartı veriliyor. Etkinlik sonrası konaklamak için otele gittiğimizde ise, önceden yaptığımız rezervasyon bilgisini doğrulamamız için, rezervasyon numarası ve kimlik kartımız gerekiyor. Kimlik kullanımı, bir gün içerisinde farklı durumlarda sürekli tekrar ediyor.

Fiziksel dünyada sunduğumuz bu kanıtlar için, çeşitli belgeleri cüzdanımızda bulunduruyoruz. İhtiyaç anında kanıt olarak sunuyoruz. Ancak çevrimiçi dünyada bu işlemler bu kadar kolay olmuyor. Kimi zaman yeterli kanıtlama imkanı olmadığı için işlemler yapılamıyor, kimi işlemlerde ise, kullanılan yanlış bilgiler, kullanıcılar veya kurumlar tarafından, para ve zaman kaybına neden olabiliyor. Sahtekarlık önleme çalışmaları nedeniyle, kurumlar daha fazla yatırım yapmak zorunda kalıyor. Bütün bunlar da dolaylı olarak son kullanıcıya olumsuz bir şekilde yansıyor.

## Kimlik Yönetimi Problemleri

Hali hazırda kullanılan kimlik doğrulama yöntemlerinin eksikleri nedeniyle, gereğinden fazla bilgi paylaşılabiliyor. Örneğin, sadece 18 yaşından büyük olduğumuzu kanıtlamamız gereken bir senaryoda, doğum tarihini bile paylaşmamıza gerek yokken, paylaşma yöntemimizin ilkelliği nedeniyle, tüm kimlik bilgilerimizi paylaşmak durumunda kalıyoruz. Daha kötüsü, farklı yerlerle paylaştığımız bu bilgilerimiz, güvenlik açıkları nedeniyle kötü niyetli kişilerin eline geçebiliyor. Bir otel rezervasyonu senaryosunu ele alalım. Bu senaryoda, üç aktörün yaşadığı çeşitli problemler yer almaktadır.

Son kullanıcı olan müşteri açısından bakarsak, şu sorular cevap aramaktadır:

- Neden tüm işletmelere tekrar tekrar kendimi kanıtlıyorum?
- Verilerim nerede ve ne kadar güvenli saklanıyor?
- Bilgilerim başka kimlerle paylaşılıyor?
- İşletmenin gerçek olduğundan nasıl emin olabilirim?

İşletme için de benzer şekilde bazı sorular bulunmaktadır:

- Müşterinin paylaştığı kimlik bilgilerine ne kadar güvenebilirim?
- Aracı firmanın (konaklama sitesinin) müşteriyi doğruladığından nasıl emin olurum?
- Aldığım bilgilerin kanuni gereksinim olduğuna müşteriyi nasıl ikna ederim?

Hizmet sağlayan konaklama sitesi için de şu sorular oluşmaktadır:

- Dijital olarak müşteri ve işletme kimliğini nasıl doğrularım?
- Müşterilerin güvenini nasıl sağlarım?
- Sahte işlemleri nasıl engellerim?

## Kimlik Yönetim Modelleri

Yukarıda sözü edilen sorunları çözmek için, günümüze kadar çeşitli yöntemler geliştirilmiştir. İlk olarak merkezi kimlik yöntemi denenmiştir. Merkezi kimlik, kullanıcıların her kurum için bilgilerini yeniden oluşturdukları merkezi bir yöntemdir. Verilerin her kurum ile tekrar tekrar paylaşılması gerekmektedir. Kullanıcı her kurumdaki şifresini hatırlamalıdır. Zayıf şifreler veya tekrar tekrar kullanılan aynı şifreler, güvenlik açıklarına neden olmaktadır. Verinin birçok yerde kopyasının olması, veri sızıntı riskini artırmaktadır.

İkinci olarak federe kimlik yöntemi kullanılmıştır. Bu yöntem belirli sağlayıcılar aracılığıyla, kimlik bilgilerinin diğer kurumlarla paylaşılması yöntemidir. Kullanıcı birçok kanalla ilişkiyi yönetmek zorunda değildir. Ancak bu durumda tek bir kurumun sahip olduğu bir güç oluşmaktadır. Tam bir merkezi durum olmasa da, çeşitli sağlayıcıların ağırlık kazandığı kısmi bir merkezi yapı söz konusudur. Bilgilerin birleşiminin tek bir kurumda olması da, yeni ve daha ciddi bir risk noktası oluşturmaktadır.

Kullanıcı egemen kimlik yöntemi ise, blokzinciri teknolojisi üzerinde geliştirilen en yenilikçi çözüm olarak yerini almıştır. Bu yöntemde kimlik bilgileri, kimlik sahibinin tam kontrolündedir. Veri paylaşımı, sadece veri sahibinin kontrolü ile mümkündür. Kullanıcı istediği işletmeyle istediği kadar bilgi paylaşabilir. Bilgilerin doğruluğu blokzinciri üzerinden kontrol edilebildiği için, kurumlara da büyük fayda sağlar. Güvenlik konularında en gelişmiş çözümdür.


## Blokzincir Üzerinde Kimlik Yönetimi

Kişi egemen kimlik yönteminde, kimliği doğrulayan kurum, kimlik sahibi ve kimlik sorgulayan kurum olmak üzere üç ayrı aktör vardır. Burada kimliği doğrulayan kurum, blokzinciri ağında herkes tarafından tanınan güvenilir bir kurum olmalıdır. Kimlik sahibi kişi, bu kurumdan kimlik bilgilerini uygulama aracılığı ile talep ettiğinde, kurum bilgileri kişinin kendisine gönderir ve kanıtını da blokzinciri ağına yazar. Blokzincirinde herhangi bir kişisel veri kaydedilmez. Verinin doğruluğunu sağlayan bir nevi imza, blokzinciri üzerinde saklanır. Kimlik sahibi gelen veriyi mobil cihazındaki uygulamada depolar. Bu veriye sadece kimlik sahibinin erişimi vardır. Dolayısıyla veri üzerinde tam kontrole sahiptir. Kimliği sorgulayan kurum kullanıcının verisine ihtiyaç duyduğunda, kullanıcıdan bu bilgileri bir uygulama aracılığı ile talep eder. Sunulacak verilerin hangi kurumlar tarafından doğrulanmış olması gerektiğini de belirtir. Kullanıcının onay vermesi durumunda bilgiler sorgulayan kuruma iletilir. Sorgulayan kurum bilgileri alır ve blokzinciri ağı üzerinden bilgilerin doğruluğunu kontrol eder. Kimliği doğrulama ve sorgulama rolleri ihtiyaca göre kullanılabilir. Bir kurum kimi senaryo için doğrulayıcı olurken, kimi senaryoda ise sorgulayıcı olabilir. Hatta sorgulayan rolündeki kurum, daha önce doğruladığı bir veriyi tekrar sorgulayabilir.

Blokzinciri ağına kanıt yazma ve doğrulama işlemi kabaca şu şekilde olmaktadır. Kimliği doğrulayan kurum, kişiye bilgilerini iletirken, hash algoritması ile bu verinin bir özetini oluşturur. Özel anahtarı ile bu bilgiyi imzalar. İmzalanmış bu bilgiyi, blokzinciri ağına yazar. Daha sonra kimlik sahibi, bilgilerini sorgulayan bir kurumla bilgilerini ve kanıtını paylaşır. İlgili kurum kendisine gelen verinin, hash algoritmasından çıkan özetiyle blokzinciri üzerindeki kanıtı, imzalayan kurumun genel anahtarı ile çözer. Çıkan özeti karşılaştırır ve verinin doğruluğundan emin olur.

## Kullanım Alanları

Bu yapının kullanılabileceği birçok farklı alan bulunmaktadır. Bir kuruma kayıt olurken, hesap açarken, müşteri tanıma (KYC) süreçlerinde, yetki/rol işlemlerinde, ya da veri doğruluğunun dijital ortamda güvenilir bir şekilde paylaşılmasına gerek duyulan işlemlerde, bu yöntem kullanılabilir.

Bir kurumda gerçekleştirdiğimiz KYC süreçlerini, her kurum için tekrar tekrar yapmak zorunda kalmayız. Kişi egemen kimlik yöntemiyle kurumlar için oluşan maliyetler azaltılır. Son kullanıcı için de kayıt olma işlemleri kolaylaştırılmış olur. Bunun yanı sıra, verilerin dijital ortamda kanıtlanması, kişisel verileri koruma kanununa (KVKK) ve genel veri koruma düzenlemesine (GDPR) uyumlu bir şekilde yapılabilir. Çok paydaşlı ekosistemlerin kurulabilmesi, kolaylaşmış olur. Bu da, bugün yapamadığımız birçok senaryoyu, hayata geçirebilmemiz için zemin oluşturur. Müşteriler

açısından bakıldığında ise, kişinin mahremiyeti, bu zamana kadarki en yüksek seviyeye gelmiş olur. Kişi istediği verisini, istediği kurumla, istediği kadar paylaşabilir.

Bir örnek verecek olursak, A takımı taraftarı, X firma müşterisi bir öğrenciye, indirim sunmak istediğimizi düşünelim. Burada öğrenci, okumakta olduğu üniversiteden öğrenci olduğu bilgisini, üyesi olduğu futbol kulübünden üye olduğuna dair kimlik bilgisini, X firmasından da müşteri bilgisini alır. Kullanıcı bu üç kimliği sunarak, indirimi verecek e-ticaret sitesinde sunulan faydadan bu sistem aracılığı ile çok kolay bir şekilde yararlanabilir. Hali hazırda var olan sistemlerle bunu yapmak istediğimizde, her üç kurumun da bu e-ticaret sitesi ile bağlantı kurması ve kullanıcıya kimliğini dijital olarak kanıtlayabileceği, ayrı ayrı yapılar sağlaması gerekiyor. Bunu yaparken her bir kurumun kendi kullanıcılarından, veri paylaşım iznini almış olması gerekiyor. Az sayıda kurumla bu yapılabilir gibi görünse de, kurum sayısı arttıkça pratikte iş içinden çıkılmaz bir noktaya geliyor. Daha da önemlisi kimlik bilgilerini sağlayan bu firmaların, yapılan işlemlerden haberi olmadan, e-ticaret firmasının indirimi uygulaması mümkün olmuyor.

## Neden Dağıtık Kimlik Yönetimi

Blokzinciri teknolojisinin farklı kullanım senaryolarında, farklı özellikleri ön plana çıkabilmektedir. Kimlik senaryosunda da, verinin sadece kanıtının ağda olması ve bu kanıtın da şifrelenmiş ve değiştirilemez bir şekilde dağıtılmış olması, güvenliği ve gizliliği sağlamaktadır. Dijital kimlik doğrulama sistemlerinde, GDPR ve KVKK uyumlu bir yönteme sahip olması nedeniyle, blokzinciri ile kimlik yönetimi büyük faydalar sağlar.

**Kullanıcı açısından faydaları şunlardır:**

- Her kurum için şifre hatırlama ihtiyacı ortadan kalkar.
- Tekrar tekrar yapılan kanıtlamalardan doğan zaman kaybı oluşmaz.
- Kullanıcının verileri bilgisi dışında paylaşılmaz.
- Şifrenin her yerde aynı girilmesi, kağıda yazılması gibi güvenlik açıkları oluşmaz.
- Yüz yüze olamayan ortamlarda, bir kurumdan alıp bir diğer kurum ile paylaşacağı veriler için, fiziksel işlem yapma ihtiyacı ortadan kalkar.
- Adres, soyad, medeni durum gibi değişiklikler sonrasında alınan kanıt, tüm kurumlarla kolayca paylaşılabilir.

**Kurumlar açısından faydaları şunlardır:**

- Müşteriden istenen bilgiler için modern ve kolay bir paylaşım sağlar.
- Paylaşılan verilerin doğruluğu kolaylıkla kontrol edilebilir.
- Sahtekarlığı engellemek için, yapılan harcamalar azalır.
- Kullanıcının kontrolünde, veri paylaşımı sayesinde, KVKK / GDPR kurallarına uyum sağlanır.
- Geçerliliğini kaybeden verilerin işaretlenmesi blokzincirinde yapıldığı için, eski kanıt yeni işlemlerde kullanılamaz.

## Teknik Altyapı

Özel (private) ve izin verilen (permissioned) bir ağ olmasının yanı sıra, ağ'ın yönetiminde farklı roller ile işlemler yapabilmeye imkan sağlaması nedeniyle, Hyperledger Indy dağıtık defterini tercih ettik. Birçok farklı kimlik altyapısında, kişi güvenilirliği (repütasyon) ile işlemler gerçekleştirilirken, Hyperledger Indy'de, bilinirliği olan kurumların güvenilirliği, önem arz etmektedir. Kimlik gibi kritik konularda, doğruluğun teyidi son derece önemli olduğu için, bu yapının blokzinciri ortamında, kimlik yönetiminde en uygun yapı olduğunu düşünüyoruz. Aynı zamanda Hyperledger Indy'nin, Sovrin vakfı gibi, "self-sovrin identity" üzerine çalışan kurumların da destek verdiği, "World Wide Web Konsorsiyum" (W3C) standartlarına uygun olarak geliştirilmiş bir altyapı olması da, tercih nedenimiz oldu.

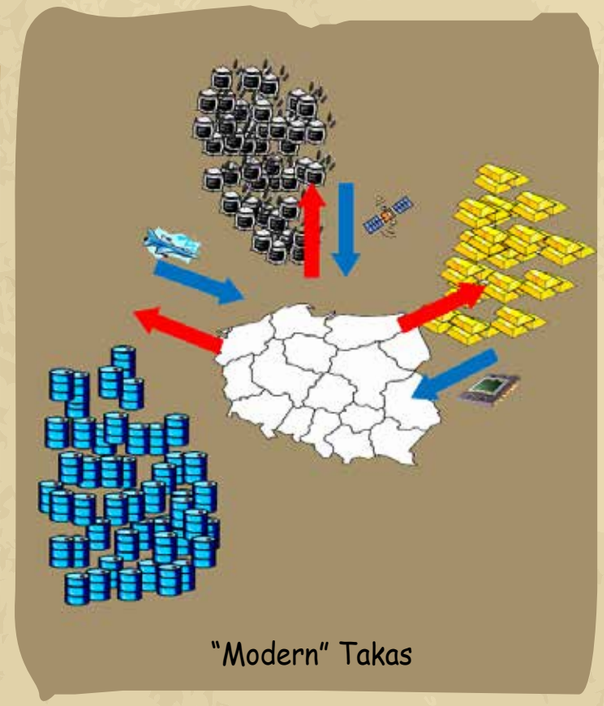
Oluşturduğumuz ağdaki düğüm noktalarımızı, Turkcell Akıllı Bulut altyapısında bulunan "Docker" konteynırları üzerinde konumlandırdık. Mobil uygulamamızı, "React Native" proglamlama çatısı ile geliştirdik. "Indy" ağı ile konuşacak "IOS" ve "Android Native" işletim sistemlerine özel yazılmış programlar, yani yerli kütüphaneler geliştirdik. Var olan sistemlerimizde minimum değişiklikle bu yapıyı kullanabilmek için, "Spring Boot" programlama çatısı üzerinde, vekil sunucu (Proxy) görevi görecek olan, REST standartlarına uyumlu bir programlama arayüzü (Restful API) geliştirdik.




# Kripkatür

Çizer: Umut Uludağ - Başuzman
Araştırmacı / BİLGEM UEKAE





1957 yılında Ankara'da doğdu. İlk ve ortaöğrenimini Ankara ve Erzurum'da tamamladı. Devlet bursuyla gönderildiği İngiltere'de Elektronik Mühendisliği eğitimini şeref derecesiyle 1979 yılında, aynı dalda yüksek lisans eğitimini 1980 yılında tamamlayarak yurda döndü. PTT ARLA, TELETAŞ ve TÜBİTAK'da, araştırma mühendisi ve yönetici olarak çalıştı. TÜBİTAK UEKAE Müdürü ve BİLGEM Başkan Vekili iken 2011 yılında emekliye ayrıldı. Bu tarihe kadar ancak boş zamanlarını ayırabildiği ebrû sanatına zamanının tamamını ayırmaya başlayan Alparslan Babaoğlu, gelenekli ebrû tekniği ve tarihi ile ilgili araştırmalar ve çeşitli kurumlarda ebrû eğitmenliği yapmakta olup evli ve iki çocuk babasıdır.

# Alparslan Babaoğlu: Hayatımın En Güzel Günlerini BİLGEM'de Geçirdim...

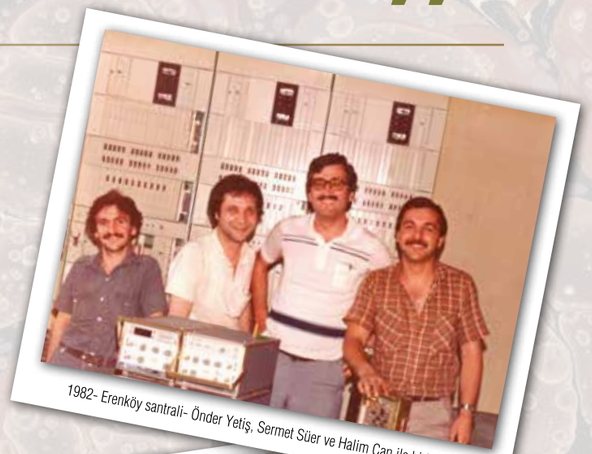




> BİLGEM gibi işlerin rutin olmadığı, çalışılan konuların zamanla değiştiği, zamana karşı yarışılan yerlerde, çalışanların meslekleri dışında faaliyetlerde bulunmaları bir gereklilik.

*Yayın Kurulu olarak Alparslan Babaoğlu Hocamızla bir röportaj gerçekleştirdik. Hocamız BİLGEM'de geçmişte birçok projede yer aldı ve ilklere imza atan ekibin parçası oldu. UEKAE Müdürü ve BİLGEM Başkan Vekili iken 2011 yılında emekliye ayrıldı. Halen BİLGEM Başkan Danışmanı sıfatıyla BİLGEM Ailesinin parçası olmayı sürdürüyor.*

*Resmi kariyerinin dışında Ebrû sanatıyla ciddi olarak ilgilenen ve bu alanda icazet sahibi olan Hocamız, bilim ve sanat birlikteliğini hayatında sağlamış bir isim. Bu bağlamda röportaj boyunca verdiği mesajların ayrı bir değere sahip olduğu düşüncesindeyiz…*



1982- Erenköy santrali- Önder Yetiş, Sermet Süer ve Halim Can ile birlikte

1981- PTT ARLA

Necati Şişeci: **Sayın Hocam, Kurumumuzun geçmişini en iyi bilen kişilerden birisi olmanız sebebi ile yeni başlayacak çalışma arkadaşlarımız için yaşadığınız zorluklardan ve çözüm yollarınızdan örnekler verebilir misiniz?**

Tabii. 1994 senesinde ALCATEL, o dönemde Ar-Ge biriminde çalıştığımız TELETAŞ hisselerinin çoğunluğunu elde etmesiyle Ar-Ge faaliyetlerini durdurma kararı aldı. Önce o zamanki Ar-Ge Direktörümüz Önder YETİŞ ve Sermet SÜER'le birlikte üç kişi, birkaç ay sonra da yanlış hatırlamıyorsam 17 arkadaşımız daha TELETAŞ'tan ayrılarak Marmara Araştırma Merkezi (MAM)'ne bağlı Elektronik Araştırma Ünitesi'ne geçtik. O sırada birimin çalışan sayısı sanıyorum 40 civarında idi.

Elektronik Araştırma Ünitesi, MAM binasının, YİTAL'in bulunduğu kolunda faaliyet gösteriyordu. Bizim üstümüzdeki katta da daha sonra kurulacak olan BTE'nin çekirdeğini teşkil eden Robotik ve Bilişim Teknolojileri Üniteleri vardı.

Çalışan sayısı bugünlere kıyasla çok düşüktü. Dış destekli projelerden yeterli gelir sağlanamaması ve gelirin Başkanlıktan verilen bütçeyle sınırlı olması nedeniyle birimin sürekli maddi sıkıntısı vardı. Fotokopi makinamız yoktu mesela. Fotokopi çektireceğimiz zaman şansımızı önce üst kattaki Robotik biriminin fotokopi makinasında dener, sekreter hanım izin verirse çektirir, makinayı kilitlemişse mecburen MAM Kütüphanesi'ne gider orada çektirirdik.

Birimdeki masaüstü bilgisayar sayısı da yetersizdi. Şimdiki gibi herkesin masasında birkaç bilgisayar değil projelere zimmetli az sayıda bilgisayar vardı. İki tane masaüstü bilgisayar almıştık. Hiç unutmuyorum işlemcisi 486DX266 idi ve 30 MByte hard diski vardı. O günlerde 30 MByte hard disk çok büyük bir bellek alanı idi. İşletim sistemini floppy disketlerde gönderirlerdi ve biz kendimiz yüklerdik. Bir bilgisayara 20-30 diskete yüklenmiş işletim sistemini kurmanız bütün gününüzü alırdı. O bilgisayarlar birimde sıkıntıya sebep olmuştu çünkü herkes bilgisayarı kendi projesi için almak istiyordu.

Zamanla hem teçhizat ve altyapı hem de personel sorununu ancak dış destekli projelerle çözebileceğimizi görünce dış destekli projelere yöneldik. Başlangıçta Silahlı Kuvvetlerimiz için geliştirdiğimiz cihaz ve sistemlerle hem ihtiyaçlarımızı karşılar hem de nitelikli insan gücü istihdam edebilir hale gelmiştik ancak bu defa da kapalı alan sorunu ortaya çıkmıştı. Önce bulunduğumuz binanın çatısını kapatıp sağlı sollu ofisler ve laboratuvarlar oluşturduk. Daha sonra da bildiğiniz gibi, yeteri kadar gelir elde edip de masraflarını karşılayabilir hale gelince ilk ek binamız olan şimdi Başkanlık Binası olarak isimlendirilen binamızı yaptık.

Bilal Kılıç: **Alparslan Bey, geçmişe baktığınızda şunları iyi ki yapmışız güzel oldu dediğiniz şeyler nelerdir? Fakat şunu yapamadık, kısmet olmadı, yapabilseydik ne güzel olurdu diyeceğiniz şeyler var mıdır?**

Hayatımın en güzel günlerini burada geçirdim. Burada yapılan her şey çok güzel, çok özel ve ülkenin acil ihtiyacı olan cihaz ya da sistem olduğu için şunlar güzel oldu şunlar olmadı diye ayıramıyorum her şey çok güzeldi. MİLON-IV, FORMUS ve SIR cihazlarımızla NATO'ya tedarikçi olmaya başlamıştık. MİLOF-I cihazımızla da NATO offline kripto cihazı ihalesinde rakipsiz kalmıştık. Her alanda NATO'ya tedarikçi olabilsek bir de treni kaçırmadan Kuantum Kripto konusuna girebilsek çok güzel olurdu diye düşünüyorum.

> "Burada (BİLGEM) yapılan her şey çok güzel, çok özel ve ülkenin acil ihtiyacı olan cihaz ya da sistemlerdir."

Mehmet S.Ekinci: **Hocam, sizce iyi bir mühendis profili nasıldır?**

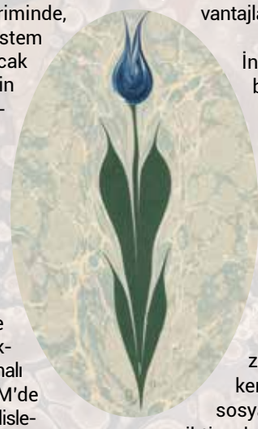
İyi bir mühendisin nitelikleri o mühendisin çalışacağı alana göre farklılık gösterir bana göre. Yani üretimde çalışacak bir mühendisle Ar-Ge biriminde, kalite kontrol biriminde ya da sistem mühendisliği biriminde çalışacak mühendislerin temel niteliklerinin dışında ayırdedici nitelikleri olmalı diye düşünüyorum.

Genel manada temel mühendislik altyapısını edinmiş ve formasyonunu kazanmış bir mühendisin; meraklı, özellikle alanıyla ilgili gelişmeleri takip eden, okumayı seven, hiçbir zaman bildikleriyle yetinmeyen karakter özellikleri olmalı bence. BİLGEM'de çalışacak mühendislerin yani Ar-Ge projelerinde çalışacak mühendislerin en ayırdedici özelliğinin ise sebep sonuç ilişkisinin önemini kavramış kişiler olmaktır diye düşünüyorum. Benim hayatım boyunca kendime en sık sorduğum soru, işler istediğim gibi gitmediğinde "ben bunu böyle olsun istememiştim neden böyle oldu?" sorusudur ve bu sorunun doğru cevabını kısa sürede bulmak iyi bir geliştirme mühendisinin en temel vasfı olmalıdır.

Ömer Özkan: **İnsan hayatı içerisinde iş-aile-sosyal yaşam-akademik ve mesleki gelişim-kültür-sanat nasıl bir dengede tutulmalı? Bu dengeyi büyükşehirde yaşamla birlikte nasıl sağlayabiliriz?**

BİLGEM gibi işlerin rutin olmadığı, çalışılan konuların zamanla değiştiği, zamana karşı yarışılan yerlerde çalışanların meslekleri dışında faaliyetlerde bulunmaları bence bir gereklilik. Bu düzenli olarak sinema, tiyatro, spor karşılaşmaları ya da konserlere gitmek olabilir, bir el becerisi kazanmak amacıyla kurslara katılmak olabilir ya da düzenli olarak sportif faaliyetlerde bulunmak olabilir. İnsan beyninin sürekli aynı konuya odaklanması bir süre sonra insanda algı körlüğüne sebep oluyor kanımca. Rutine bağlanmış işlerde bir süre sonra fark edilmesi gereken şeyler fark edilemez hale geliyor bu da işte başarısızlığa neden oluyor.

Tabii bunların hepsi belli bir programla ve düzen içinde yapıldığında fayda sağlar. Büyükşehirde yaşamak, ulaşımdaki güçlükler ve zaman kaybı gibi nedenlerle zor gibi gözükse de aslında biraz önce saydığım konuların hepsinin bir arada bulunduğu yerlerin insanlara çok fazla seçenek sunması, büyükşehirlerin bütün dezavantajlarına karşılık oluşturduğu avantajlardandır.



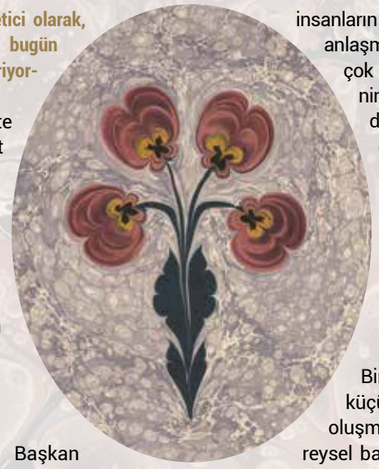
İnsanların hayatlarında işlerinin çok önemli bir yeri olduğu inkâr edilemez bir gerçek. Ancak bence herkesin hayatında her şeyden biraz ama bir denge içinde olmalı. Bu konuda benim gençlere, özellikle çocuk sahibi gençlere bir tavsiyem var. Çocuklarınız yaşça küçükken bacağınıza sarılıp "beni çocuk parkına götür", "birlikte balık tutmaya gidelim" ya da "beni tiyatroya götür" dediğinde iş ya da başka bir nedenle bir mazerete sığınıp onları geri çevirmek yerine onlarla olabildiğince zaman geçirmeye bakın. Büyüdüklerinde kendi arkadaş çevreleri, kendi hobileri ve sosyal faaliyetleri olduğundan ve artık size de ihtiyaçları kalmadığından çocukluklarının tam aksine bu defa siz onların peşinden koşmaya ve birlikte zaman geçirmeye çalışıyorsunuz ama artık iş işten geçmiş oluyor.

Hamza Özer: **Geleneksel Ebrû sanatının önde gelen bir üstadı olduğunuz bilinmektedir. Bir sanat dalı ile ilgilenmek meslek hayatınıza olumlu ve olumsuz olarak nasıl etki etmiştir?**

Estağfurullah... Ebrû yapıyor olmamın meslek hayatıma olumsuz bir etkisinin olduğunu söyleyemem. Tam aksi bütün teknik zorluklarına rağmen akşam eve gidince ebru teknesinin başına geçtiğimde, kafamın içinde dönüp duran işle ilgili ne kadar sorun varsa hepsini unuttuğumu ve ertesi gün işe taptaze bir zihinle gittiğimi, bunun da beni iş hayatımda çok olumlu etkilediğini söyleyebilirim. Bence herkesin akşam uğraşabileceği bir hobisinin olması ruh sağlığı açısından son derece yararlı. Mühendis olmamın ise başarılı ebrû yapmakta, ebrûnun teknik problemle rini çözebilmek için gerekli formasyonu sağlaması ne deniyle çok büyük katkılarının olduğunu söyleyebilirim.



Abdullah Alpaydın: **Eski bir çalışan/yönetici olarak, geçmişle karşılaştırdığınızda BİLGEM'in bugün gelmiş olduğu noktayı nasıl değerlendiriyorsunuz?**



TÜBİTAK'taki çalışma hayatı 1983'te başlamış birisi olarak şunu çok net ifade edebilirim. TÜBİTAK'ın başarı eğrisi sinüzoidal bir eğri. Dönem dönem dış müdahaleler nedeniyle eğri negatif bir eğim gösterse de şu anda eğimin pozitif olduğunu, istikrarın yeniden sağlanmaya başladığını gördüğümü rahatlıkla ifade edebilirim.

İzzet Karabay: **Meslek ile ilginiz devam ediyor mu? Neler yapıyorsunuz?**

Meslekle ilgim TÜBİTAK BİLGEM Başkan Danışmanlığı dışında maalesef devam etmiyor. Sektör değiştirdim. İstanbul Üniversitesi, Edebiyat Fakültesi, Tarih Bölümü, Yeniçağ Tarihi Ana Bilim Dalı'nda ebrû tarihi ile ilgili araştırmalar yapmak amacıyla doktora yapıyorum. Şu anda bilimsel hazırlık dersleri alıyor bir yandan da konumla ilgili arşiv araştırmaları yapıyorum.

İzzet Karabay: **BİLGEM çalışanlarına vermek istediğiniz mesajlarınız, tavsiyeleriniz var mıdır?**

İnsan sosyal bir varlık. Hepimiz BİLGEM'de ya da bir başka yerde başka bireylerle bir arada yaşamak zorundayız. Çevremizdeki insanlarla her zaman frekanslarımız uyuşmayabilir ve her zaman herkesle her konuda tam bir fikir birliği içinde olamayabiliriz. Böyle durumlarda biraz empati yapıp iş arkadaşlarımızın da bizim gibi sorumluluklarının olduğunu, benzer maddi imkanlarla benzer koşullarda yaşamaya ve bizimle benzer sorunlarla başa çıkmaya çalıştıklarını düşünerek anlaşmazlıklar karşısında hoşgörülü olmalarını tavsiye ederim. Bir şekilde hepimiz hayatımızı bir yerde kazanmak zorundayız ve başka yerlerde de çevremizdeki insanların mükemmel olamayacakları ve benzer anlaşmazlıkları oralarda da yaşayacağımız çok açık. Bu nedenle "iş arkadaşım benimle konuşurken sesini yükseltti" ya da "proje yürütücüm bana kötü baktı" gibi argümanların, o kişilerin de bizim gibi sorunlarla başa çıkmak zorunda oldukları ve belki de tam o sırada kafalarının içinde çözmeleri gereken bir sorunla uğraştıklarını, zaman zaman kendimizin de benzer şekilde davrandığımızı düşünerek hoşgörüyle karşılamak gerekir diye düşünüyorum.

Bir başka konu da BİLGEM'in nispeten küçük takımların bir araya gelmesi ile oluşmuş kocaman bir takım olduğunun, bireysel başarının ancak BİLGEM'in başarısıyla mümkün olacağının farkında olmak.

O nedenle nerede bir problem varsa orada olmak, o problemin çözümüne katkıda bulunmak ve "bu benim işim değil" diye düşünmemek de çok önemli.

**Herkesin hayatında dengeli bir şekilde her şeyden biraz olmalı...**

# BİLGEM'den Milli Güvenli Bulut Depolama Çözümü: **Safir Depo**

Safir Depo, dosyalarınızı bulutta güvenli bir şekilde depolayarak, herhangi bir ortamdan kolayca erişebilmenizi sağlayan bir bulut depolama ürünüdür.

Mehmet Zahid Berktaş – Uzman Araştırmacı / BİLGEM BTE

İletişim imkânlarının sürekli arttığı, hızla yeni yöntemlerin popülerlik kazandığı günümüzde, kullanıcı alışkanlıkları da değişmekte ve iletişimde kullanılan araçlar gelişmektedir. Çevrimiçi cihazların yaygınlaşmasıyla birlikte, kullanıcıların dokümanlarına, müziklerine, videolarına; kısacası verilerine farklı cihazlardan kolayca erişme ihtiyacı ortaya çıkmıştır. Yeni çözümlerin, ortaya çıkan ihtiyaçlar sonucu geliştirilmesi geleneği bu noktada da kendisini göstermiş ve "Bulut Bilişim" konseptine temel olmuştur.

## Bulut Bilişim

Ana hatlarıyla değinecek olursak Bulut Bilişim;

- Kaynakların merkezileştirilerek uçbirimlerdeki yatırım maliyetlerini azaltmak
- Merkezi yönetilebilirlik özellikleriyle uçbirimlerdeki bakım maliyetlerini azaltmak
- Yüksek erişilebilirlik özelliği sunarak kaynaklara rahat erişim sağlamak özellikleriyle öne çıkmaktadır.

Bahsedilen özelliklerin her biri Bulut Bilişimin bir temelini oluşturacak şekilde farklı alanlar ortaya çıkmıştır. Bu kapsamda veri ve veri kaynaklarına kolay erişim ihtiyacı da "Bulut Depolama" konseptinin ortaya çıkmasına sebep olmuştur.

## Bulut Depolama

Bulut Depolama, verilerinizin cihazlarınızda ayrı ayrı kopyalar olarak tutulması yerine, uzak lokasyondaki bir veri merkezinde depolandığı ve istenildiği anda istenilen cihazdan (belirli yetkilendirmeler çerçevesinde) 7/24 erişilebilmesinin sağlandığı depolama yöntemidir. Tabii ki bu yöntem, kendisine özgü avantaj ve dezavantajlar getirmektedir. Veriye istenilen yerden ve anda erişebiliyor olmak, merkezi depolama ünitelerinin çok sayıdaki bağımsız ufak depolama seçeneklerinden daha düşük maliyetli olması gibi temel avantajlar sunar. Ancak, verilerin merkezi bir depolama alanında tutuluyor ve her erişim talebinde istemciye ağ üzerinden sunuluyor olması hem veri merkezinde hem de ağ trafiği üzerinde ciddi ek güvenlik tedbirleri gerektirmektedir.

Kullanıcıların bulut depolama ihtiyaçlarına cevap verebilmek adına geliştirilen ticari uygulamalar, son kullanıcı tarafında yoğun talep görmüş ve bu, uygulamaların hızlı bir şekilde popülarite kazanmasını sağlamıştır. Bahsedilen ticari uygulamalar, son kullanıcıların güvenlik kaygılarını gidermek adına gerekli tüm aksiyonları almalarına rağmen, kullanıcı verilerinin ticari firmaya ait veri merkezinde depolanıyor olması ve ticari firmaların bu dosyalar üzerinde kullanıcıları hakkında bilgi sahibi olmaya yönelik analizler çalıştırdıklarını gizlemiyor olmaları kullanıcıların güvenlik endişelerini artırmaktadır.

## Safir Depo

Safir Depo, TÜBİTAK BİLGEM Bulut Bilişim ve Büyük Veri Araştırma Laboratuvarı (B3LAB) tarafından geliştirilen milli ve güvenli bulut nesne depolama uygulamasıdır. Safir Depo üzerinde depolanan dosyalarınıza internet üzerinden; akıllı telefonlar, tabletler veya bilgisayarlar aracılığıyla her an her yerden ulaşabilirsiniz.

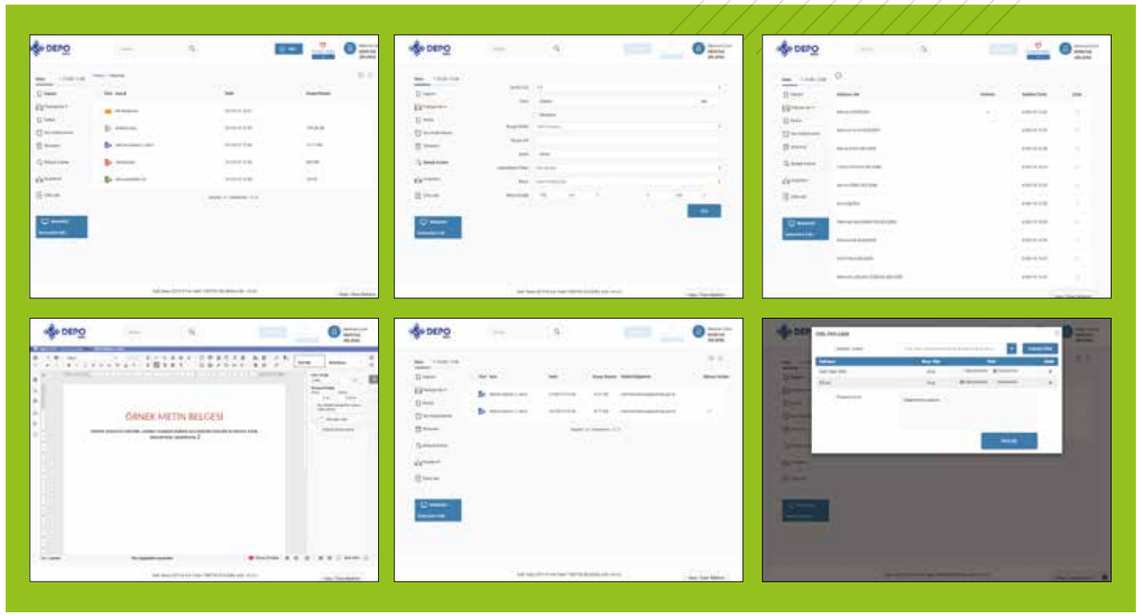
Safir Depo, ticari alternatiflerinde de görülebileceği üzere "Hizmet olarak Yazılım" (SaaS – Software as a Service) yöntemiyle kullanılabileceği gibi, kurumların kendilerine özel bulutları üzerine kurulum yaparak

hizmet verme imkânını da sunmaktadır. Özel bulut (private cloud) seçeneği ile Safir Depo, bulut depolama yazılımlarının yüksek ve kolay erişilebilirlik özelliklerini sağlamaya devam eder. Diğer taraftan müşterilerin kendi veri merkezlerinde barındırılan sunucularına kurulum yapılarak kullanıcılarının dosyalarının kurum içerisinde depolanmasını sağlar.

Tamamen açık kaynak kodlu yazılımlar ve kütüphaneler üzerine geliştirilen Safir Depo, yüksek hesaplama veya depolama kapasiteli özel donanımlar gerektirmemekte, standart sunucular üzerinde çalışabilmekte, yatayda ölçeklenebilir özelliği sayesinde kapasite artışlarına esnek şekilde ayak uydurabilmektedir. Orta ve büyük ölçekli kurulumlarda yük dengeleyici özelliğiyle atanan kaynakları efektif olarak kullanabilir ve müşterilerine veri merkezinden yazılım konfigürasyonuna kadar, "Tek Nokta Hatası" (Single Point of Failure) içermeyecek şekilde tavsiye mimariler sunar. Bu sayede hizmet kesintisi ihtimalini en aza indirgeyerek bulut bilişimin "yüksek erişilebilirlik" özelliğini karşılar.

Muadil ürünlerde yer alan dosya yükleme/indirme, klasör oluşturma, kopyalama, taşıma, silme, isim değiştirme gibi endüstri standardı özelliklerin tamamının yer aldığı Safir Depo, kullanıcı dostu arayüzüyle kullanıcılarının

> Safir Depoda gelişmiş arama özellikleri ile dilediğiniz takdirde seçilen tarih aralığına, belirli doküman tiplerine veya dosya boyutu aralığına göre filtrelemeler yapabilir, ofis ve metin dokümanları içerisinde geçen metinlere göre arama yapabilirsiniz.




yazılımı rahat bir şekilde kullanabilmelerine olanak sağlar. Ofis dokümanlarınızı, resim, video ve müzik dosyalarınızı kullandığınız bilgisayara indirmeden tarayıcınız üzerinde görüntüleyebilir, izleyebilir ve dinleyebilirsiniz.

## Dosyalarda Analiz ve Erişim

Makine öğrenmesi yetenekleri ile akıllı servis eklentileri sunan Safir Depo'da, yüklenen dokümanlar, imajlar ve videolar üzerinde analiz işlemleri gerçekleştirilebilmektedir. Safir Depo'da paylaşılan dokümanlar, kelime yoğunluklarına göre etiketlendirilerek sınıflandırılabilmekte, doküman özetleri çıkarılabilmektedir. Yüklenen çalıştırılabilir dosyalar üzerinde virüs taraması yapılarak virüslü dosyalar indirilmeden önce kullanıcıya bilgi verilebilmektedir. Versiyon karşılaştırma özelliği ile metin dosyalarının farklı versiyonlarında yer alan değişiklikler görüntülenebilmekte ve farklılık yüzdesi belirlenebilmektedir. Safir Depo'da depolanan imaj ve videolar görüntü/sekans içeriklerine göre etiketlenerek sınıflandırılabilmektedir.

Safir Depo, dosyalarınıza hızlı erişebilmeniz için birçok farklı yöntem sunar. Klasik klasör hiyerarşisi içerisinde dosyalarınızı organize edebileceğiniz gibi, son kullanılanlar sekmesinden yakın tarihte işlem yaptığınız dosyalarınıza erişebilirsiniz. Gelişmiş arama seçeneklerini kullanarak sadece belirli türlerde dosyalarınıza, dilediğiniz boyut aralığındaki dosyalarınıza veya içerik arama özelliği sayesinde doküman içerisinde geçen kelimelere göre filtrelemeler yaparak aradığınız dosyaya hızlı bir şekilde ulaşabilirsiniz.

## Dosya Paylaşımı

Bulut depolama yazılımlarının en faydalı özelliklerinden bir tanesi de dosyalarınızı kolaylıkla üçüncü kişilerle paylaşabilmenizi sağlıyor olmasıdır. Halihazırda zaten bulutta depolanan dosyalarınızı, talep ettiğiniz kişilerle ve yetki seviyelerinde, dosyayı tekrar yükleme/gönderme işlemi yapmadan paylaşabilirsiniz. Özellikle hareket halindeyken mobil cihazlarla kullanımlarda ve büyük boyutlu dosyalarda kullanıcılara büyük kolaylık sağlayan paylaşım özelliği Safir Depo'da iki farklı senaryo olarak geliştirilmiştir.

Özel Paylaşım seçeneği, dosyalarınızın diğer Safir Depo kullanıcılarıyla sadece görüntüleyebilir veya düzenleme yapabilir yetkileriyle paylaşabilmenizi sağlar. Kullanıcıların kendi paylaşım gruplarını oluşturarak, grup dâhilindeki tüm kullanıcılara tek seferde kolay paylaşım yapabilmesine de olanak sağlayan bu özellik sayesinde dosyalarınızı saniyeler içerisinde paylaşabilirsiniz.

Bağlantı Paylaşımı seçeneği ise dosyalarınızı Safir Depo kullanıcısı olmayan kişilerle paylaşmanızı sağlar. Paylaşım işlemi sonucunda oluşturulan bağlantı adresini paylaşım yapmak istediğiniz kişiye iletmeniz





> "Safir Depo, standart bulut depolama ürünlerinde yer alan özelliklerin tamamını kullanıcılarına sunarken, kendine özgü yetenekleriyle rakiplerinden ayrılmaktadır."

durumunda, bağlantıya tıklayan kişi Safir Depo'ya üye olmadan ve giriş yapmadan paylaştığınız dosyaya erişebilecektir. Safir Depo, çevrimiçi ofis editörleriyle entegre çalışır. Deponuzda yer alan ofis dokümanlarına çift tıklayarak internet tarayıcı pencerenizde açılacak çevrimiçi ofis editörleriyle açık doküman formatında, yaygın kullanımda olan diğer formatlardaki ofis dokümanlarınız üzerinde düzenleme yapabilirsiniz. Bununla birlikte paylaşımdaki ofis dokümanlarınız üzerinde, paylaştığınız kişilerle simultane çalışabilirsiniz.

Varsayılan kurulumda açık kaynak kodlu OnlyOffice ile entegre çalışacak şekilde ayarlanan Safir Depo, istendiği takdirde yine açık kaynak kodlu LibreOffice Online ile de sorunsuz çalışabilmektedir.

İster dosyanızı kendiniz güncellemiş olun, isterseniz değişiklik yetkisiyle paylaştığınız farklı bir kişi güncellemiş olsun, dosyalarınızdaki her değişiklik Safir Depo'da o dosyanın yeni bir versiyonu olarak depolanır. Dilediğiniz anda dosyalarınızın eski versiyonlarına dönüş yapabilir ve yaptığınız değişiklikleri geri alabilirsiniz.

### Güvenli Depolama

Endüstri standardı güvenlik önlemlerinin entegre edildiği üründe, güvenli HTTPS haberleşme protokolü üzerinden dosya iletimi sağlanmakla birlikte, bu güvenlik seviyesine ek olarak "Güvenli Depolama" özelliği sunar.

Güvenli Depolama özelliği devreye alındığında, Safir Depo'ya gönderilen dosyaların uçtan uca şifreleme yöntemleriyle istemci tarafında (web arayüzü kullanılıyorsa internet tarayıcısında, mobil uygulamalarda cihaz üzerinde, masaüstü uygulamalarında ise istemci bilgisayarda) şifrelendikten sonra internet hattı üzerinden şifrelenmiş olarak iletilmesini sağlar. Bu özellik sayesinde aşağıda sıralı birçok güvenlik zafiyeti çözümlenmiş olur.

- Kullanılan ağ hattı üzerinde gerçekleştirilebilecek "Aradaki Adam" (Man in the Middle) saldırılarında transfer edilen dosyaların açığa çıkması engellenir.
- Sunucu tarafında şifreleme uygulayan sistemlerin aksine, dosyanın sunucuya ulaştığı giriş noktasında oluşabilecek güvenlik açıklarında, şifrelenme öncesi dosyaların ele geçirilmesi tehdidi bertaraf edilmiş olur.
- Ağ izleme ve yönetim, veri merkezi ve sistem yönetim ekiplerinin, dosyaların çözülmüş hallerine hiçbir şekilde erişememesini garanti eder.

Güvenli depolama özelliğinde, dosyalarınızın şifreleme anahtarları dosya sahibinin ve paylaşım yapılan kişilerin anahtarlarıyla zincir anahtar yöntemiyle tekrar şifrelenerek sistemde depolanır. Bu sayede şifrelenmiş bir dosyanın, şifreleme sonrasında farklı kişilerle paylaşılması durumunda, dosyanın istemciye indirilerek uygun kullanıcı anahtarlarıyla tekrar şifrelenmesine gerek kalmaz. Bunun yerine, paylaşım yapılan kişilerde bir değişiklik olduğunda (yeni bir paydaşla paylaşıldığında veya paylaşım yapılan bir kişiyle paylaşım sonlandırıldığında) dosyaya ait şifreleme anahtarı çözülerek güncel paylaşılan kullanıcıların anahtarlarıyla şifrelenerek güncellenir. Bu sayede büyük boyutlu şifrelenmiş dosyaların paylaşım değişikliklerinde dosyanın istemciye indirilerek, yeniden şifrelenip tekrar sunucuya gönderilmesine gerek kalmaz ve bu yöntemle şifrelenmiş dosyalardaki paylaşım değişiklikleri anlık gerçekleşir. Bu, hem işlem süresi hem de ağ trafiği açısından ciddi tasarruf sağlamaktadır.

> "Safir Depo, gelişmiş web tabanlı açık kaynaklı ofis editörleriyle entegre çalışır, dosyalarınız üzerinde aynı anda birden fazla kişiyle birlikte çalışabilirsiniz."

### Safir Depo Kullanımı Yaygınlaşıyor

Veri içeriğinin ve veri güvenliğinin özellikle kritik olduğu kamu kurumlarında ve özel sektörde Safir Depo yaygınlaştırma faaliyetleri hızlanarak devam etmektedir. Cumhurbaşkanlığı Kabinesi 1. 100 Günlük Kalkınma Planı'na dâhil edilerek 3 üniversitede pilot kullanıma açılan Safir Depo, kurulum yapılan ULAKBİM veri merkezi üzerinden 9 üniversitenin kullanımına sunulmuştur. 2018 yılı içerisinde, Gebze veri merkezimiz üzerinden tüm TÜBİTAK personelinin kullanımına açılmış ve aktif olarak kullanılmaktadır.

Kamu kurumlarına özel bulut olarak kavram ispatı kurulumları yapılmış ve bu çalışmalar sonucunda canlı ortam kurulumlarına başlanmıştır. Son olarak Cumhurbaşkanlığı Dijital Dönüşüm Ofisi inisiyatifinde planlanan Milli İletişim Platformu'nun bulut nesne depolama bileşeni olarak entegrasyon çalışmalarına dahil edilmiştir.

Özellikle birden fazla lokasyonda faaliyet gösteren kamu kurumlarının, birimler arası dosya paylaşımlarında önemli bir boşluğu dolduracağını düşündüğümüz Safir Depo ürünümüze yeni özellikler eklemeye devam etmekteyiz. Yaklaşık 3 yıldır analiz, tasarım, geliştirme ve test faaliyetleri gerçekleştirilen projemize emek veren ekip arkadaşlarıma bu vesileyle katkılarından dolayı içtenlikle teşekkür ederim.

# YAPAY ZEKÂ'nın Sinyal İstihbaratındaki Yeri





> Yapay zekâ 1950'lerden bu yana üzerinde çalışılan bir alan olmasına rağmen günümüzde hesaplama kapasitelerinin artmasıyla birlikte kullanımı yaygınlaşmıştır.

Dr. Ali Rıza Ekti - Uzman Araştırmacı, Kadir Günel - Uzman Araştırmacı, Kürşat Tekbıyık - Araştırmacı, Ömer Özdağ - Bursiyer / BİLGEM TDBY

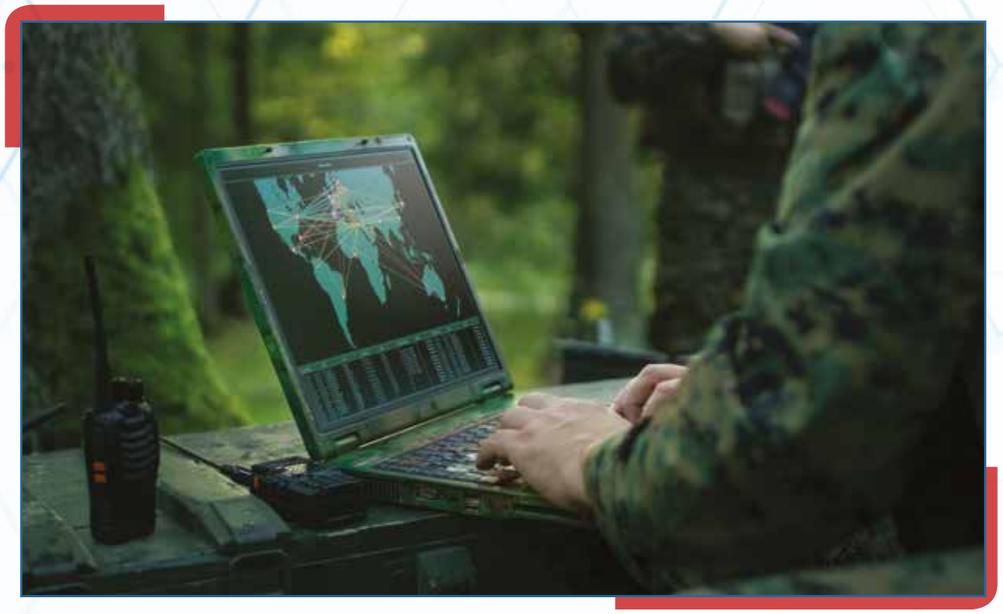
Yapay zekâ insan zekâsıyla ilişkilendirilen bilişsel fonksiyonların makineler tarafından gerçekleştirilmesi temeline dayanmaktadır. Makine öğrenmesi bir yapay zekâ örneğidir ve bilgisayar sistemlerinin herhangi bir açık yönergeye ihtiyaç duymaksızın belirli bir görevi yerine getirmesi için kullanılan algoritmalar sistemidir. Derin öğrenme ise başka bir yapay zekâ örneği olup eldeki verinin hangi özelliklerinin karar verme aşamasında kullanılacağını seçen algoritmalardan oluşur.

Yapay zekâ ve makine öğrenmesi 1950'lerden bu yana üzerinde çalışılan bir alan olmasına rağmen günümüzde hesaplama kapasitelerinin artmasıyla birlikte kullanımı yaygınlaşmıştır. Özellikle grafik işlemci birimlerinin paralel hesaplama yeteneklerinin yapay sinir ağlarında kullanılmasıyla birlikte modellerin hızlı eğitilmesi mümkün olmuştur. Grafik işlemci birimlerinin yaygın kullanılmasının yanı sıra, yüksek kaliteli ve etiketli veri setlerine erişimin kolaylaşmasının ve bu setlerin sayısının artmasının da makine öğrenmesinin gelişmesine ve yaygınlaşmasına katkı sunduğunu belirtmek gerekir. Makine öğrenmesinin günümüzde hızlı yaygınlaşmasının başkaca sebepleri arasında yeni mimarilerin ortaya konulması da sayılabilir.

Bu yazının konusu olan sinyal istihbarat uygulamalarına geçmeden önce makine öğrenmesinin kullanıldığı alanlara kısaca değinelim. Makine öğrenmesi deyince ilk akla gelen uygulamalardan biri el yazısı rakam sınıflandırma ve LeNet mimarisidir. 1998 yılında ortaya çıkan bu mimari bir evrişimsel sinir ağıdır. MNIST veri seti üzerinde başarımı test edilen model bu alanda ses getiren ilk çalışmaların başında gelmektedir.

2012 yılında Alex Krizhevsky tarafından tasarlanan AlexNet bir başka evrişimsel sinir ağı modelidir. Stanford Üniversitesi tarafından hazırlanan Imagenet veri seti üzerinde dikkat çekici başarı sağlayan model birçok farklı alanda kullanılmıştır. Evrişimsel sinir ağlarının yanı sıra tekrarlayan (recurrent) sinir ağları özellikle zaman serileri üzerinde ciddi başarılar göstermiştir. Bunlardan biri olan ve 1997 yılında Münih Teknik Üniversitesi'nden Sepp Hochreiter tarafından ortaya konan uzun-kısa vadeli bellek (LSTM) ağları, uzun dönemli bağımlılıkları öğrenme sürecine dâhil ederek karar verme sürecinde çok daha yüksek performansla veya başka bir deyişle daha az hata ile çıktı üretebilirler.

Uzun-kısa vadeli hafıza ağlarının en fazla uygulamasının bulunduğu alan yapısına da uygunluğu itibariyle doğal dil işleme problemleridir. Metin ve konuşma örüntüleri zaman bağımlılıkları içermektedir ve bu örüntünün takip edilmesiyle gelecek adımın tahmini daha kesin ve doğru bir biçimde belirlenebilmektedir.

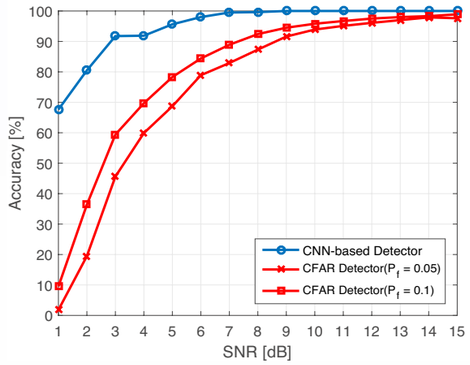


## Sinyal İstihbarat

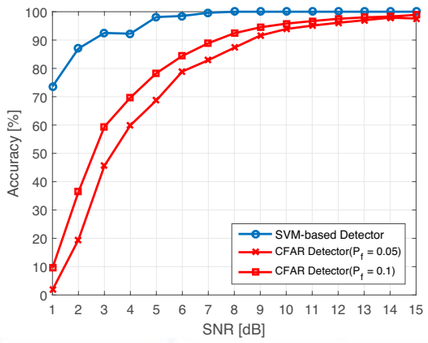
Sinyal istihbarat, telsiz iletişim sistemlerinin kullanılmaya başlanmasının hemen ardından ortaya çıkmış bir savunma teknolojisi alanı olarak kabul edilebilir. Sinyal istihbaratın modern anlamda ilk örneği Japon-Rus savaşı sırasında İngiliz gemisi HMS Diana tarafından Rus denizaltı sinyallerinin Süveyş Kanalı'nda yakalanmasıdır . Daha sonra I. ve II. Dünya Savaşları sırasında sinyal istihbaratın gerekliliği daha iyi anlaşılmış ve bu dönemde bu alana yönelik çalışmalar hız kazanmıştır. Günümüzde hala hem savunma hem de saldırı amaçlı sinyal istihbarat çalışmaları hız kesmeden devam etmekte ve ülkelerin savunma gücünün önemli bir parçası olmayı sürdürmektedir. Sinyal istihbarat temelde sinyalin spektrumda tespiti, tespit edilen işaretin sınıflandırılması ve spektrum kullanımının modellenmesi problemleriyle ilgilenir.

## Sinyal Tespiti

Spektrumda işaretin varlığını tespit etmek amacıyla çeşitli yöntemler önerilmiştir. Bunlar arasında en çok bilinen ve yaygın olanı enerji sezicilerdir. Enerji seziciler, gürültü gücünün bilinmesi durumunda optimum sezici olarak çalışabilmektedir. Fakat gürültü gücünün kestirilmesi zaten işaret tespit probleminin bir başka halidir. Açıkçası bir bant aralığında gürültü gücünün kestirilmesi, işaretin varlığını tespit etmek için yeterli olmasına rağmen gürültü gücünün belirlenmesi ciddi bir problemdir. Bu nedenle enerji seziciler, teoride iyi sonuçlar verse bile gerçek iletim ortamında kanal




Şekil 1 CNN tabanlı sınıflandırıcı klasik CFAR sezicilere göre çok daha yüksek performansla işaret sezimi yapabilmektedir.




Şekil 2 SVM tabanlı sınıflandırıcı klasik CFAR sezicilere göre çok daha yüksek performansla işaret sezimi yapabilmektedir.

karakteristiğinin değişimi ve geniş bantta gürültü varyansının sabit olmayışı gibi nedenlerden dolayı beklenen performansı göstermekten uzaktır.

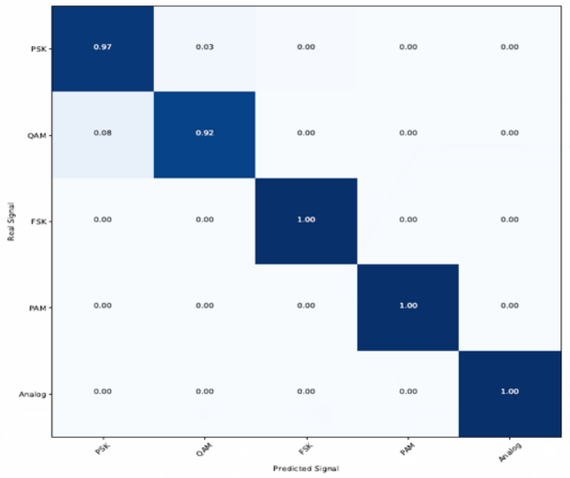
BİLGEM bünyesinde yapılan çalışmalar gösteriyor ki derin öğrenme tabanlı yöntemler, klasik sabit alarm olasılıklı sezicilere nazaran daha iyi performans göstermektedirler. Özellikle düşük işaret-gürültü gücü oranlarında bu fark çok daha belirgin olmaktadır. Yapılan çalışmalara ait çıktılar, Şekil 1 ve Şekil 2'de sırasıyla CNN ve SVM tabanlı sınıflandırıcılar için verilmektedir.

## Sinyal Sınıflandırma

Sinyal modülasyon sınıflandırması askeri ve sivil uygulamalarda çokça kullanılan ve sinyal tespiti ve demodülasyonu arasında bulunan bir aşamadır. Sinyal modülasyon sınıflandırması, gelen sinyalin işlenmesi ve uygun sınıflandırma algoritmasının seçilmesi olmak üzere iki aşamadan oluşur.

Sınıflandırma aşamasında geleneksel yaklaşım ve yapay zekâ yaklaşımı olmak üzere iki yaklaşım bulunur. Geleneksel yaklaşımlar da benzerlik temelli (LB) ve öznitelik temelli (FB) olmak üzere ikiye ayrılır. Benzerlik temelli yaklaşımlar gelen sinyalin benzerlik fonksiyonuna bağlıdır ve sınıflandırma, bu benzerlik oranının bir eşik değerle karşılaştırmasıyla yapılır. Ancak optimum çözüm karmaşık bir hesaplamayla bulunur ve çoğu örnekte bu durum optimal olmayan sınıflandırıcıların elde edilmesine neden olur.

Öznitelik temelli yaklaşımlar önce gelen sinyalin özniteliklerini çıkarır ve belirli bir kritere (eşik değerine) göre karar verir. Sinyalin kullanılan özniteliklerine; sinyalin mutlak genliği, fazı, frekansı, sıfırdan geçiş



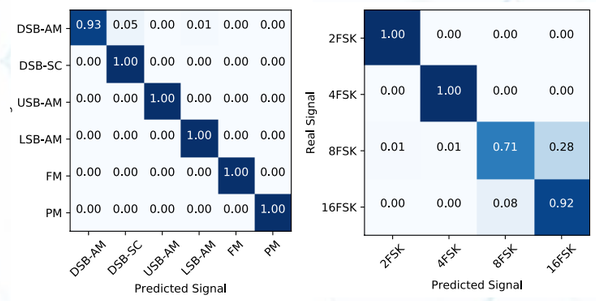

> Grafik işlemci birimlerinin yaygın kullanılması, yüksek kaliteli veri setlerine erişimin kolaylaşması ve bu setlerin sayısının artması günümüzde makine öğrenmesinin hızlı yaygınlaşmasının başlıca sebepleridir.

aralığının varyansı, momentleri, kümülantları ve çevrimsel kümülantları örnek verilebilir. Öznitelik temelli yaklaşımlar, benzerlik temelli yaklaşımlara göre daha az karmaşıktır; ancak bir öznitelik seçimi her işaret kümesi için optimum olmayabilir. Kör tanıma yapılan bir uygulamada işaret kümesi belirlenemediği için öznitelik temelli yaklaşımlar verimli bir sonuç vermeyebilir. Yapay zekâ yaklaşımında ise sınıflandırma modellerine yapay sinir ağları (ANN) ve evrişimsel sinir ağları (CNN) örnek verilebilir.

Derin öğrenme temelli yaklaşımlar manuel öznitelik seçiminden kaçınır. Model işaretin ayırt edici özelliklerini kendisi çıkarabilir. Bu yüzden derin öğrenme temelli yaklaşımlar geleneksel yöntemlere kıyasla çok daha iyi sınıflandırma performansı sergileyebilmektedir. Derin öğrenme, çok sayıda parametre içeren çok büyük sinir ağları kullanarak yüksek boyutlu girdi verisinden doğrudan öznitelik öğrenme kapasitesini ciddi bir biçimde artırmıştır. BİLGEM'de tasarlanan sınıflandırıcı ağın performansı da bu bilgilerle paralellik göstermektedir ve Şekil 3'te görülebilir.

## Spektrum Tahmini

Kablosuz haberleşme teknolojilerinin yaygınlaşmasıyla kablosuz ağa erişimi olan cihaz sayısı artacak ve kullanılabilecek spektrum kaynağı miktarı




*Şekil 3 Evrişimsel sinir ağları (CNN) tabanlı ağın sınıflandırma performansı görülmektedir.*

| GRU | 882-973Mhz | 1701-1792Mhz | 1960-2051Mhz |
|---|---|---|---|
| **Şehir İçi** | 0.94 | 0.744 | 0.90 |
| **Banliyö** | 0.83 | 0.81 | 0.78 |
| **Kırsal Bölge** | 0.98 | 0.76 | 0.95 |

Tablo 1 GRU encoder decoder mimarisi deney sonuçları

| LSTM | 882-973Mhz | 1701-1792Mhz | 1960-2051Mhz |
|---|---|---|---|
| **Şehir İçi** | 0.94 | 0.74 | 0.87 |
| **Banliyö** | 0.83 | 0.81 | 0.79 |
| **Kırsal Bölge** | 0.98 | 0.76 | 0.94 |

Tablo 2 LSTM encoder decoder mimarisi deney sonuçları

azalacaktır. Spektrum kaynaklarının ihtiyaca nazaran az kullanılmasının önüne geçilmesine yarayan teknolojilerden biri spektrum kullanım tahminidir. Spektrum tahmini sayesinde spektrumun uygunluğuna karar verilir, spektrum kaynaklarının kullanım verimliliğiyle beraber kablosuz ağ yapısına erişim kapasitesi de artırılır.

Mevcut spektrum tahmin teknikleri uyumlu filtre tanıması, öznitelik temelli tanıma ve enerji tanıma olmak üzere üçe ayrılır. Uyumlu filtre alıcısı kullanıcı sinyalinin kopyasıyla algılanan sinyali ilişkilendirerek karar verme aşamasında alınan sinyalin işaret-gürültü gücü oranını maksimize eder. Ancak bu yöntemde kullanıcı sinyaline ait tüm bilgiye ihtiyaç vardır ve bu durum bütün gerçek hayat koşullarında sağlanamayabilir.

En bilindik öznitelik temelli tanıma yöntemi, dönemli-durağan öznitelik temelli tanıma yöntemidir. Öznitelik temelli tanıma metodu belli koşullar altında başarılı performans gösterse de sinyale ait ön bilgi eksikliği hesaplama karmaşıklığını artırır ve tanıma performansını düşürür.

Enerji tanıma yöntemi, spektrum tanıma yöntemleri arasında en basitidir ancak sinyalin SNR'ı düşük olduğunda tanıma performansı düşüktür. Mevcut yöntemlere alternatif olarak derin öğrenme metotları, spektrum doluluk tahmininde başarılı sonuçlar verir. BİLGEM'de de yapılan çalışmalarda gördüğümüz üzere kapılı tekrarlayan hücre (GRU) ve LSTM temelli tanıma metotları, mevcut geleneksel yöntemlere kıyasla değişken sinyal ortamlarını daha kolay modelleyebilmektedir ve spektrum tahmininde daha etkilidir (Tablo 1 ve Tablo 2). Hatta düşük işaret-gürültü gücü oranlarında ve yetersiz ön bilgi durumlarında bile iyi sonuçlar vermektedir.

## Sonuç

Donanımların işlem kapasitelerinin artması ve paralel hesaplama yöntemlerinin etkin kullanılmasıyla birlikte yapay zekâ tabanlı sistemler, birçok alanda hızla yer almaktadır. Hiç şüphesiz bu alanlardan biri de gerek çok parametreli sistem kurguları, gerekse yüksek hassasiyet isterleri olan sinyal istihbarat sistemleridir.

BİLGEM bünyesinde yapay zeka tabanlı yöntemler, yıllardır kurum bünyesinde çalışmaları devam eden sinyal istihbarat sistemlerine entegre edilmiş ve sistem performanslarının ciddi ölçüde arttığı görülmüştür. Türk savunma sanayiinin gelişimine ve ilerlemesine katkıda bulunacağı düşünülen yapay zekâ destekli sinyal istihbarat sistemleri üzerine çalışmalar hız kesmeden devam etmektedir.

*Kaynakça*

*[1] .LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. Proceedings of the IEEE, 86(11), 2278-2324.*

*[2] .Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. In Advances in neural information processing systems (pp. 1097-1105).*

*[3] .Report from HMS Diana on Russian Signals intercepted at Suez, 28 January 1904, Naval library, Ministry of Defence, London.*

# TÜRKİYE YAZILIM SEKTÖRÜNDE Yerlilik ve Millilik

> Ekonomik kalkınma yoluyla toplumsal refaha ulaşmada bilişim sektöründe küresel rekabet ve milli politikalar çerçevesinde sanayileşme ihtiyacı bulunmaktadır.

Nuriye Ünlü - Enstitü Md.Yrd., Gizem Kabayel - Araştırmacı, H. Gülin Koçak - Uzman / BİLGEM YTE

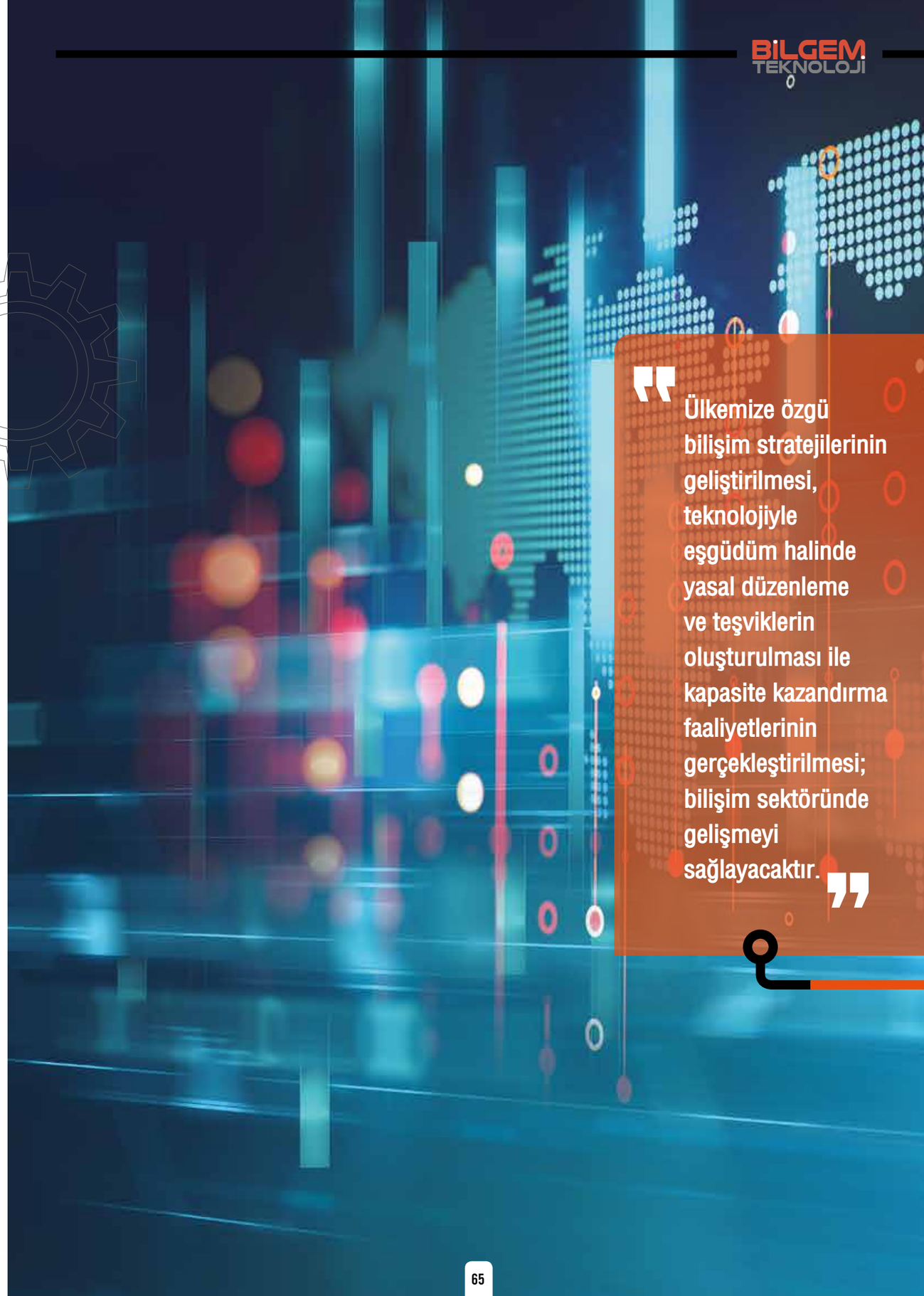
20. yüzyılın ikinci yarısından itibaren Bilgi ve İletişim Teknolojilerinin (BİT) ve bilişim sektörünün gelişimi hızlanmış ve birçok ülkede milli gurur ile özdeşleşmiştir. Ekonomik kalkınma yoluyla toplumsal refaha ulaşmanın önkoşullarından biri küresel rekabetten geçmekte ve milli politikalar çerçevesinde sanayileşme gerekliliği ön plana çıkmaktadır. Yapılan analizler, ülkemizde bilişim sektörünün 1 birim büyümesinin toplam ekonomiye 1,8 birimlik büyüme katkısında bulunacağını göstermektedir. Bununla birlikte, sektörde yer alan varlıklar ve yürütülen faaliyetlerin sahipliği önemli bir husus olarak karşımıza çıkmakta, yerli ve milli kavramları üzerinden politika geliştirilmesi ihtiyacı bulunmaktadır. Bu ihtiyaca yönelik, bilişim sektöründe yerli ürün ve hizmet kullanımının 2023'e kadar % 50'ye çıkarılması hedeflenmiştir. Bilişim sektörünün GSYH'daki payının 160 milyar dolara, yazılım sektörünün de 50 milyar dolara ulaşması hedeflenmektedir.

## Milli Teknoloji Hamlesi ve Açık Kaynak İnisiyatifi

Gerek etkin, etkili ve ekonomik uygulamalar sayesinde tasarruf edilmesi, gerek yeni kabiliyetler geliştirilerek uluslararası pazarlar dâhil yeni ekonomi alanı oluşturulması açısından bilişim sektörünün alt sektörlerinden biri olan yazılım sektörü, ülkenin kalkınmasında ön plana çıkmaktadır. Özgün yazılımlarını geliştiren ve markaya dönüştürebilen ülkeler, uluslararası platformlarda güçlü konuma gelmektedir. Ülke ekonomisi, bağımsızlığı ve güvenliğini etkileyebilecek devlet sırrı, ticari sır, gizli bilgi ve kişisel veri içeren yazılımlar ve diğer stratejik ve kritik yazılımlar üretilerek bu konularda olası tehditlerin ortadan kaldırılması mümkün olmaktadır. Bu motivasyonlarla, ülkeye özgü stratejilerin geliştirilmesi, sektöre uygun ve hızla gelişen teknolojiyle eşgüdüm halinde yasa, düzenleme ve teşviklerin oluşturulması ve kapasite kazandırma faaliyetlerinin gerçekleştirilmesi; sektördeki gelişimin önünü açacaktır.

Milli Teknoloji Hamlesi ve Açık Kaynak Platformu inisiyatifi ile fikrî ve sınai mülkiyet alanında gerekli yasal düzenlemeler hayata geçirilerek açık kaynak kodlamanın yaygınlaştırılması ve yerli açık kaynak çözümlerinin geliştirilmesi, lisanslamadan kaynaklanan kamu ve özel sektör yazılım maliyetlerinin azaltılması, nitelikli yazılım geliştirici sayısının artırılması ile açık kaynak yazılım ürünleri ve bu ürünlerin destek hizmetlerini sunan şirket ve girişimci sayılarının artırılması, kamu yazılım ve bilişim ürünü tedariğinde yerliliği ve açık kaynak kullanımının yaygınlaşmasına yönelik tedarikçi yetkilendirme ve yönetim modeli ile teşvik mekanizmasının geliştirilmesi hedeflenmektedir.

Benzer şekilde, ülkemizde yerli ve milli yazılım konusunda sağlıklı KOBİ ekosisteminin oluşturulması ve



> Yazılımda kritik alanların belirlenerek özellikle yabancı şirketlerin bu alanlardaki konumlarının ülkemizin sahip olduğu/olacağı kabiliyetler dikkate alınarak ihtiyaçlar doğrultusunda yeniden ele alınması ihtiyacı bulunmaktadır.

yazılım sektörüne KOBİ'lerin dahiliyetinin artırılması ve güçlendirilmesi için kolaylaştırıcı ortam oluşturulması, yazılım geliştirme alanında paylaşım ekonomisinin oluşturduğu fırsatlardan faydalanılması amaçlarıyla Açık Kaynak ekosisteminin oluşturularak Açık Kaynak Kodlu yazılım teknolojilerinden yararlanılması ve geliştirilmesine yönelik politikalar geliştirilmiştir.

## Yerli ve Milli Kavramları

Gerek yurtdışında gerekse ülkemizde yerli ve milli yazılım net olarak tanımlanmamış, bu konuda ortak bir anlayış geliştirilmemiştir. Genel kabullerden yola çıkılarak bu tanımlar oluşturulmuştur. Türk Dil Kurumu'nun (TDK) yayımladığı Güncel Türkçe Sözlük'te; "Yerli"; "Yurt içinde yapılan veya bir yurdun kendine özgü niteliklerini taşıyan" şeklinde tanımlanmaktadır. Dolayısıyla, bir ürünün yerli kabul edilebilmesi için söz konusu ürünün fikrî ya da sınai haklarına sahip olunmasına gerek bulunmamaktadır. Ürünün sadece bir ülkede üretilmesi, yerli olabilmesi için yeterlidir. Örneğin; Avrupa menşeli bir şirketin ülkemizde ürettiği herhangi bir ürün yerli olarak nitelendirilebilmektedir. «Milli» sözcüğü ise "Milletle ilgili, millete özgü, ulusal" anlamında kullanılmaktadır. Dolayısıyla, bir ürünün milli olarak kabul edilebilmesi için ülkemize özgü olması, fikrî ya da sınai tüm haklarının ülkemize ait olması gerekmektedir.

## Türk Hukukunda Yerli Malı Kavramı

Yerli bilişim ürününün tanımı net olarak yapılmadığından yerli malı kavramı üzerinden bir tanımlama yapılmaktadır. Ülkemiz açısından «yerli» ürünün sözlük anlamı dışında sahip olması gereken bazı nitelikler de bulunmaktadır. Bu çerçevede, «yerli malı» Türk Hukuku'nda düzenlenerek yerli malı belgesine sahip olma kriterleri özel olarak belirtilmiştir. Nitekim Sanayi ve Teknoloji Bakanlığı'nca hazırlanan 2014/35 sayılı Yerli Malı Tebliği'nde belli şartları sağlayan sanayi ürünlerinin yerli malı olarak kabul edileceği düzenlenmiştir. 1 Temmuz 2017 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren 7033 sayılı Kanun ile de, bilişim teknolojisi ve yazılım üreten işletmeler sanayi işletmesi, sanayi işleri ve sanayici tanımı kapsamına alınarak yazılım sanayi ürünü kapsamına alınmıştır.

Yerli Malı Tebliği'nin "Yerli Malı" başlıklı 4'üncü maddesinde sanayi ürünlerinin yerli malı olarak kabul edilebilmesi için;

- Bakanlık tarafından düzenlenen Sanayi Sicil Belgesine sahip sanayi işletmeleri tarafından üretilmesi ve Sanayi Sicil Belgesindeki "Üretim Konusu" içeriğinde yer alması.
- Tamamen Türkiye'de üretilen veya elde edilen ürünler ile üretim sürecinin önemli aşamalarının ve ekonomik yönden gerekli görülen en son esaslı işçilik ve eylemin Türkiye'de yapılmış olması
- Ürünün yerli katkı oranının en az %51 olması.
- Serbest bölgeler mevzuatı ile gümrük mevzuatı göz önünde bulundurularak, yerli malı kriterlerine ilişkin bu Tebliğde yer alan gerekli şartların sağlanması kaydıyla serbest bölgede faaliyet gösteren işletmelerin ürettikleri ürünlerden olması şartları aranmaktadır.

Yerli katkı oranını belirleyen kriterlerin yazılım için; kurumsal kimlik ve sahipliğin (hissedar yapısı) yerli olma durumu, yabancı ortaklı şirketlerde yabancı ortaklara aktarılan pay dağılımı, nitelikli insan kaynağı maliyetleri cinsinden yerli – yabancı dağılımı, Ar-Ge, inovasyon, tasarım maliyetleri cinsinden yerli – yabancı dağılımı, geliştirme ortamı araç lisans maliyetleri cinsinden yerli – yabancı dağılımı, know-how sahipliğinin yerli – yabancı dağılımı, yazılım geliştirmenin önemli aşamalarının



> Bir ürünün milli olarak kabul edilebilmesi için ülkemize özgü olması, fikrî ya da sınai tüm haklarının ülkemize ait olması gerekmektedir.

ülkemizde yapılma durumu, tasarımın yerli olma durumu, yazılımın fikrî mülkiyet haklarının sahipliğinin yerli olma durumu, yazılım geliştirme ve derleme ayrımında faaliyeti yürütenin yerli olma durumu, yazılım kaynak kodlarından nesne kodlarının üretilebilir olma durumu, yazılım kalitesi ve sürdürülebilir olma durumu, Açık Kaynak yazılım parçası kullanma durumu, Rafta Hazır Ticari Ürün (COTS) haline getirebilme durumu gibi etkenler göz önünde bulundurularak farklılaşmasına ve bu kriterlerin mevzuatla tanımlı hale getirilmesine ihtiyaç bulunmaktadır.

## Ülkemizde Yabancı Yatırımların Durumu

2012'de yapılan değişiklikle ülkemizde yabancı yatırımın artırılması ve kolaylaştırılması amaçlanarak ülkemizde yabancı uyruklu kişilerin şirket kurabilmesi için yönetim kurulundan en az bir kişinin Türk vatandaşı olması veya ülkemizde ikamet etmesi şartı kaldırılmıştır. 6102 sayılı Türk Ticaret Kanunu'na göre yabancılar, ülkemizde her türlü şirketi kurabilme hakkına ve serbestisine sahiptir.

Bu bağlamda, belirlenen kritik alanlar için geçerli olmak üzere yazılım geliştirme konusunda ülkemizin sahip olduğu/olacağı kabiliyetler dikkate alınarak, yabancı şirketlerin konumlarının (özellikle pazarda) ve sağlanacak kolaylıkların yeniden ele alınması gerekmektedir.

## Yerli ve Milli Yazılım Konusunda Uygulanabilecek Politikalar ve Ülke Yaklaşımları

Genel olarak yerli ve milli yazılım konusunda farklı ülke örnekleri bulunmaktadır. Bu örnekler değerlendirildiğinde aşağıdaki yaklaşımların benimsendiği görülmektedir.

- **Kamu yazılımlarının geliştirilmesinde KOBİ'lerin katılımı güvence altına alınmalıdır.** Böylelikle bilişim sektörünün işletme büyüklüğü homojenliği korunarak ekosistemin bütüncül olarak gelişmesi ile bilişim sektöründe sağlıklı bir rekabet ortamı sağlanacaktır. Örneğin; Güney Kore'de büyük bilişim şirketleri (Samsung, LG, SK Telekom vb.) aldığı kamu projelerinin % 10' unu KOBİ'lere yaptırmak ve bu alanda KOBİ'lerin kabiliyetini geliştirmek zorundadırlar.

- **Yazılım sektörünün gelişmesi üst düzey kamu politikası olarak belirlenmeli ve geliştirilen politikalar, regülasyonlarla güvence altına alınmalıdır.** Güney Kore'de ulusal ve endüstriyel kazancı artırmanın anahtarı olduğu düşüncesine dayanarak, küresel rekabet gücünde nispeten zayıf olduğu değerlendirilen yerli yazılım endüstrisinin öne çıkartılması amacıyla Bilgi Ekonomisi Bakanlığı tarafından 2010 yılında Yazılım Gücü Olma Stratejisi hazırlanmıştır. KOBİ'lerin kullanımı için ortak yazılım geliştirme çerçevesi ve platformu oluşturularak, kamu yazılımları geliştirmesinde bu çerçeve, zorunlu hale getirilmiştir.

Estonya'da özellikle 2004 yılındaki AB üyeliği ile yenilikçiliği destekleyen kalkınma politikaları benimsenmiştir. Bilişim sektörü, ülkenin stratejik sektörleri arasında tanımlanmış ve orta öğretimden başlayarak bilişim teknolojileri konusunda yetkinlik artırmaya yönelik planlar yapılmıştır. Estonya'da yerli yazılım sektörünün geliştirilmesi amacıyla 2000 yılında 25 yıllık bir ulusal hedef belirlenmiş ve bu yönde uygulamalara başlanmıştır.

İrlanda'da bilişim teknolojilerinin kullanımının yaygınlaştırılması için 2017 yılında 4 yıllık bir program açıklanmıştır. Program, anahtar kamu hizmetlerinin tamamının 2014/18/EC sayılı Avrupa Birliği Kamu İhale Direktifi ile belirlenen rekabetçi müzakere usulü kullanılarak alınmasını ve yerli yazılım geliştiricilerin ayrıcalıklarını içermektedir.

Çin'de yazılım endüstrilerinin geliştirilmesini teşvik etmek ve yerli yazılım şirketlerine destek sağlamak amacıyla bir genelge yayımlanmıştır. Genelgede yazılım geliştirme ortamının iyileştirilmesi, geliştirme kalitesi ve seviyesinin artırılması hedeflerine yönelik düzenlemeler yapılmıştır. Yanı sıra, 2001-2005 dönemini kapsayan 10. Beş Yıllık Planında yazılım sektörü, ekonomik gelişme ve

ulusal güvenlik açısından kritik ve stratejik sektör olarak tanımlamıştır. Brezilya'da üretilen yerli yazılımın kullanımına yönelik olarak "milli olanı satın al" (Buy National) politikası da önemli destekleyici araçlardan birisi olarak kabul edilmektedir.

• **Kritik sektörlerin ihtiyaçlarının yerli ve milli ürünlerle karşılanması ve bunlar üzerinde fikrî ve sınai hakların korunması için düzenlemeler yapılmalıdır.** Böylelikle yazılım alanında dışa bağımlılığın önüne geçilebilecek, güvenlik tehditleri bertaraf edilebilecektir.

Bilişim sektöründe özel regülasyonları olan Güney Kore, IT Audit standartlarını sektör olgunluk seviyesini dikkate alarak ülkeye özgü prensibiyle geliştirmiştir. Yabancı yatırımcının sektöre girmesi sadece belirli hizmetler / ürünler için mümkündür. Yerli geliştirmede fikrî mülkiyet hakları özellikle takip edilmekte ve bunlara yönelik patent sistemleri bulunmaktadır. 2014 yılında yayımlanan Açık Kaynak Kodlu Yazılım Yenileme Planı ile 2020 yılına kadar açık kaynaklı yazılımlarla Micro-soft işletim sistemi bağımlılığından kurtulmayı hedeflemektedir.

> Kamu yazılımlarının geliştirilmesinde KOBİ'lerin katılımı güvence altına alınmalı, birlikte geliştirme ve rekabet ortamı sağlanmalıdır.

Estonya'da ulusal güvenlik ve milli savunma ile ilgili ürünlere Eston Ürün Uygunluk Kanunu'nun 2'nci maddesi gereğince ayrıcalık tanınmış ve kapsam dışı bırakılmıştır. Bu ayrıcalık ile kamu kurumlarının yerli bilişim güvenlik ürünleri alımıyla ilgili önceliklerinin oluşması sağlanmıştır.

Rusya'da şirketlerin, "yüksek güvenlik riskleri" nedeniyle bazı sektörlerdeki yabancı bilgi teknolojilerini kullanamayacağı belirtilmiş ve yerel olarak geliştirilmiş yazılımların kullanılması için çağrıda bulunulmuştur. Çağrı kapsamında savunma ve enerji sektörü için milli yazılımların kullanılması gerektiği vurgulanmıştır. 2016 yılında yürürlüğe giren Kanunda, kamu kurumlarının yalnızca yurt içi eşdeğerleri bulunmaması durumunda yabancı yazılım satın alabilecekleri düzenlenmiştir.

• **Milli dijital kapasite geliştirilmesine yönelik eğitim programları ve rehberlik mekanizmaları yürütülmelidir.** Güney Kore'de Korean IT and Policy Asistance Programı ile ulusal kabiliyet geliştirilmekte ve sürekli rehberlik sağlanmaktadır.

Kanada'da Yenilikçilik, Bilim ve Ekonomik Kalkınma Bakanlığı tarafından dijital dönüşüm olarak da adlandırılan girişimcilik faaliyetlerinin öne çıkarılması hedeflenmektedir. Bakanlık desteği ile içlerinde anaokulundan başlayarak ilköğretim çağındaki öğrencilere sayısal yetenekler ve kodlama öğretmeyi amaçlayan program da dahil olmak üzere yirmiden fazla program uygulanmaktadır.

Hindistan'da hükümetin eğitim politikaları da BT alanında yetenekli işgücünün oluşmasına büyük katkı sağlamıştır.

Amerika Birleşik Devletleri'nde (ABD) hükümetin izlediği Ar-Ge politikaları ve üniversitelerde Bilgisayar Bilimleri eğitimlerinin erken dönemde gelişmesi, bu ülkede yazılım sektörünün hızla büyümesinde etkili olmuştur. Yazılımın ulusal güvenlik sistemleri için önem teşkil etmesi motivasyonuyla, ABD hükümeti temel ve uygulamalı yazılım araştırmaları desteğini hayata geçirmiştir.

• **Yabancı menşeli yazılımlar milli kabiliyetlerle yerlileştirilerek milli kapasite artırılmalı, farklı iş modelleri geliştirilmelidir.** Örneğin; Japonya'da küresel firmalar yerel firmalar ile işbirliği yaparak hizmetlerini, kurumsal iş modelini ve kültürünü bilen yerli danışmanlar ve kaynaklar üzerinden verebilmektedir. Yerli bilişim ürünleri ve ihtiyaca göre geliştirilmesi yüksek talep görmekte, yerli üreticiler yerli iş modellerine adapte ve yüksek tecrübe sahibi olmaktadır. Hindistan, dünyanın en büyük yazılım ihracatçılarından biri olup, hem yazılım ürünleri hem yazılım hizmetleri ihracatını yoğun şekilde gerçekleştirmektedir. Yazılım ihracatı, Hindistan'da yerel iştiraklerini kurmuş olan çok uluslu şirketlerin yanı sıra gün geçtikçe sayıları artan ve pek çoğu Hindistan dışına açılıp uluslararası şirketler haline gelmiş olan yerel şirketler tarafından yapılmaktadır. Dolayısıyla büyümede hükümet politikalarının ve gittikçe artan oranda gerçekleşen kamu-özel sektör işbirliğinin çok önemli bir etkisi bulunmaktadır.

• **Yerli ve milli yazılım geliştirmeye yönelik teşvik ve destekler artırılmalıdır.** Örneğin; Estonya'da yerli yazılım ürünlerinin sertifikasyonu ile ilgili destekler mevcuttur. Bununla birlikte bu sertifikaların hiçbiri doğrudan 'milli ürün' belgesi olarak tanımlanmamış; ürün geliştirme aşamalarında sadece "yerli ürün" kavramı kullanılmaktadır. Destekler genel olarak yeni girişimci firmalar için vergi avantajları, markalaşma gibi konularda danışmanlık hizmeti şeklindedir. Yazılım ihracatının desteklenmesi ve yazılım ile ilgili hizmet ihracatı yapan firmaların kümeleme yöntemiyle KOBİ'lerle birlikte çalışmalarına olanak sağlayacak yapısal destekler de bulunmaktadır.

İrlanda, son 8-10 yıl içinde önce start-up destekleriyle başlattığı daha sonra 'High Speed Start-up Funding' adını verdikleri yenilikçi projeler için destek programıyla, bilişim projelerini henüz fikir aşamasındayken desteklemeye başlamıştır. Yerli yatırımcıları teşvik edecek şekilde bilişim start-up firmalarının özsermaye yatırımlarıyla ilgili vergi avantajları ve ticarileştirme danışmanlığı sağlanmıştır. Yerli yazılım sektörünü yurtdışı rekabete açabilmek amacıyla pazar araştırması yapılması, yurtdışı firmalarla ortak ofis açılması ve ihracatçı geliştirme desteği sağlanması gibi farklı türde destekler sağlanmaktadır.

• **Yazılım sektöründe yerlileşme teşvik edilirken yabancı yatırımların önünün tamamen kapatılmamasına yönelik yaklaşımlar benimsenerek pazarın dengede tutulması sağlanabilir.** Örneğin; Brezilya'da yazılım sektörünün gelişimi incelendiğinde 1970 ve 1980'li yıllarda ülkede ithal ikameci politikaların ve yabancı sermaye kısıtlamalarının belirleyici olduğu ancak bu sınırlamaların ülkeye yönelik teknoloji transferini olumsuz etkilediği tespit edilmiştir. 1991 yılında uygulamaya konulan vergi ve Ar-Ge destekleri ile 2001 yılında getirilen "Yerli Firma ile Ortaklık Şartı" yazılım endüstrisinin ülke içindeki gelişimi desteklenmiştir. Devlet destek ve teşviklerinin yazılım sektörünün belli bir olgunluğa eriştikten sonra başlamış olması gözlenmektedir.

Estonya'da Mayıs 2010'da AB uyumu çerçevesinde yürürlüğe giren Ürün Uygunluk Kanunu ile start-up firmaları desteklenerek yabancı yatırımcılar da ülkeye çekilmeye çalışılmıştır.

## SONUÇ

Ülkemiz yazılım sektörüne yönelik geliştirilen politikalar değerlendirildiğinde yerli ve milli kavramları net olarak tanımlanmamış olmakla birlikte, farklı kriterlerin mevcut düzenlemelere dercedilmesiyle söz konusu ihtiyaç karşılanabilecektir. Bu çerçevede, yerli ve milli yazılımın ekonomi ve güvenlik açısından önemi gözetilerek, bu alanda ülkemize özgü politika ve yaklaşımların benimsenmesi ile gerekli yasal düzenleme ve regülasyonların yapılması ekosistem bütünlüğü, yabancı yatırım dengesi gözetilerek kolaylaştırıcı ve teşvik edici bir ortam oluşturularak paydaş kurum ve bireylerin hazır bulunurluluğunu sağlayacak kapasite kazandırma çalışmalarının hayata geçirilmesi gerekmektedir.

Milli Teknoloji Hamlesi ve Açık Kaynak İnisiyatifi, söz konusu ihtiyaçların önemli ölçüde karşılandığı bir çerçeve sağlamakta olup uluslararası örnekler ekseninde detaylandırıldığında ülkemiz için hedeflenen ekonomik kazanımların edinilmesinin yanı sıra ülke güvenliği konusunda kontrollü bir ortam oluşturulabilecektir.


*KAYNAKÇA*

- *2023 Sanayi ve Teknoloji Stratejisi, https://www.sanayi.gov.tr/strateji2023/sts-ktp.pdf, 2019*
- *YASAD, Yazılım: Ekonominin Yeni Kalkınma Gücü, 2009, http://www.yasad.org.tr/Content/UserFiles/yasad_rapor.pdf*
- *https://www.rt.com/news/402511-putin-foreign-software-security/*
- *https://sputniknews.com/science/201511171030253524-russian-software-state-organs/*
- *https://www.bofit.fi/en/monitoring/weekly/2016/vw201632_2/s*
- *https://www.chinalawinsight.com/2011/02/articles/intellectual-property/chinas-support-of-domestic-software-industry-strengthened-by-state-council-release-of-prc-government-policies/*
- *https://www.semiconductors.org/clientuploads/directory/DocumentSIA/Public%20Policy%20Committee/State%20Council%20Document%204%202011.pdf*
- *2010 Informatization White Paper, http://unpan1.un.org/intradoc/groups/public/documents/ungc/unpan043363.pdf*
- *Türkiye Bilişim Derneği, Yerli Ve Milli Yazılım Endüstrisi Raporu, Aralık 2018, Ankara, http://www.tbd.org.tr/wp-content/uploads/2018/12/TBD_YERLI_MILLI_YAZILIM_ENDUSTRISI_RAPORU_SURUM1_0.pdf*
- *https://itsfoss.com/linux-national-os/s*
- *http://siliconafrica.com/why-china-and-russia-banned-google-from-their-country/*
- *South Korea Information and Communication Industry, 2011, http://workspace.unpan.org/sites/internet/documents/S2KR11%20South%20Korea%20Information%20and%20Communication%20Industry.pdf*
- *http://english.etnews.com/news/article.html?id=20140627200001*
- *https://www.minttwist.com/2017/03/13/google-vs-naver-googles-struggles-south-korea-focus/*
- *TOBB Yerli Malı Belgesi, https://tobb.org.tr/SanayiMudurlugu/Sayfalar/YerliMaliBelgesi.php*
- *Yerli Malı Tebliği (SGM2014/35), http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=9.5.20049&MevzuatIliski=0&sourceXmlSearch=Yerli%20Mal%C4%B1%20Tebli%C4%9Fi*
- *Sanayinin Geliştirilmesi Ve Üretimin Desteklenmesi Amacıyla Bazı Kanun Ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, http://www.mevzuat.gov.tr/Metin1.*
- *https://www.sabah.com.tr/ekonomi/2018/01/25/yerlilestirme-icin-kurul-olusturuldu*
- *http://www.hurriyet.com.tr/5-sektorde-43-urune-yeni-tesvikler-geliyor-40721561*
- *http://www.turkiyegazetesi.com.tr/ekonomi/516266.aspx*
- *Başbakanlık, Yerlileştirme Yürütme Kurulu Genelgesi, http://www.resmigazete.gov.tr/eskiler/2018/01/20180124-5.pdf*

# RADAR ve ELEKTRONİK HARP UYGULAMALARI

> Radar, gönderdiği radyo dalgalarının hedeflerden yansımasıyla bu hedefleri tespit eden ve ilgili hedeflerin mesafe, hız ve açısal bilgilerini çıkaran sistemdir.

Rıfat Dalkıran – Uzman Araştırmacı, Ömer Ertan Kalyoncu – Araştırmacı, Yılmaz Ütük – Araştırmacı / BİLGEM İLTAREN

Son yıllarda Elektronik Harp (EH) ve uygulamalarının askeri alanda öneminin ciddi olarak artmasıyla bu alanda büyük atılımlar yapılmıştır. Dünya genelinde yaşanan muharebe, çatışma ve krizlerde de EH kritik bir rol almıştır. Bu makalede radar, EH ve uygulamaları genel hatları ile sunulmuştur.

## Elektromanyetik Spektrum

Elektromanyetik spektrum, frekans ve dalga boyuna göre oluşan elektromanyetik dalgaların devamlılığı olarak isimlendirilir. Elektromanyetik spektrum, dalga boylarına göre sıralanmış şekilde X-ışınından radyo dalgalarına kadar birçok ışıma türünü içermektedir. Bütün elektromanyetik dalgalar vakum içerisinde ışık hızıyla hareket eder.

Radyo Dalgaları, 30 Hz'ten 300 GHz'e kadar olan frekans bandında bulunan ve elektromanyetik spektrumda en küçük frekansa, yani en büyük dalga boyuna sahip bir elektromanyetik ışıma türüdür. Yüksek dalga boyuna sahip olmaları sayesinde içerisinde bulunan elektromanyetik enerjiyi kaybetmeden uzun mesafelere gönderebilmektedir. Bu yüzden radyo dalgaları, radar, mobil/uydu haberleşme, navigasyon, kablosuz haberleşme gibi alanlarda sıklıkla kullanılmaktadır.



> Hareketli hedeflerde kullanılan güdümlü mermiler (füzeler), uzaktan güdüm ve hedefle güdüm olmak üzere iki ana başlıkta incelenmektedir.

## Radar

Radar, gönderdiği radyo dalgalarının hedeflerden yansımasıyla bu hedefleri tespit eden ve ilgili hedeflerin mesafe, hız ve açısal bilgilerini çıkaran sistemdir. Genel olarak, radyo dalgalarının gönderilmesi ve alınması işlevini yapan bir sistem olan radar, hava trafik kontrolü, uçuş yönetimi, gemi trafiği, hava savunması, gözetleme gibi amaçlarla kullanılmaktadır. Radarlar, askeri hava savunma sistemlerinde genel olarak dört farklı görevde, şu sırayla kullanılmaktadır:

**Erken Uyarı Radarları:** Gelebilecek hedefleri çok uzun menzillerde, erkenden tespit etmeyi amaçlayan radarlardır.

**Hedef Tespit Radarları:** Erkenden tespit edilen hedeflerin daha dar bir bölgede, detaylı konumlarının tespitinin yapıldığı radarlardır.

**Hedef Takip Radarları:** Konum tespiti yapılan hedeflerin detaylı bir şekilde (mesafe, hız, açısal bilgi vb. verilerin daha hassas bulunmasıyla) izlenmesinin yapıldığı radarlardır.

**Güdüm Radarları:** İzlenilen hedefe fırlatılan füzeleri kontrol etmek için kullanılan radarlardır.

Radarlar, hedefleri vurmak için füze veya hava savunma topu olarak adlandırılan silah sistemlerini ve hedefleri daha kolay takip edebilmek için optik görüntüleme ve takip sistemlerini birlikte kullanabilmektedir.

## Füze / Güdümlü Mermi

Herhangi bir hedefi vurmak için ateşleyici bir sistem yardımıyla fırlatılan nesneye mermi denir. Güdümlü mermi veya aynı anlamda kullanılan füze ise, bir hedefi vurmak için fırlatılan ve uçuş esnasında rotası değiştirilebilen nesnelerdir.

**Güdümlü Mermiler:** Radar güdümlü, kızılötesi güdümlü ve lazer güdümlü olarak üçe ayrılmakta; bu mermiler üzerinde hedefe yönelmek amaçlı arayıcı başlık bulunmaktadır. Bu makalede sadece radar güdümlü mermiler anlatılacaktır.

Hareketli hedeflerde kullanılan güdümlü mermiler, uzaktan güdüm ve hedefle güdüm olmak üzere iki ana başlıkta incelenmektedir. Hedefle güdüm ve uzaktan güdüm de kendi içerisinde alt başlıklara ayrılmaktadır.

**Hedefle Güdüm:** Güdümlü mermi içerisinde bulunan donanımın hedefi algıladığı ve kendisini hedefe yönlendirdiği füze güdüm türüdür.

**Uzaktan Güdüm:** İçerisinde alıcı/verici gibi herhangi bir donanım bulunmayan mermi türü olup mermiyi başka platformlar vasıtasıyla hedefe yönlendiren füze güdüm türüdür. Uzaktan güdümün en sık kullanılan alt türlerinden birisi komuta kontrollü güdümdür.

## Elektronik Harp (EH)

Elektronik Harp (EH), spektrumu kontrol etmek, bir düşmana saldırmak veya düşman saldırılarını engellemek için elektromanyetik spektrum kullanımını içeren eylemler bütünüdür. Düşmanın elektromanyetik spektrumu kullanmasına mani olmak veya kullanma yeteneğini azaltmak, dost kuvvetlerin elektromanyetik spektrumu etkin olarak kullanmasını sağlamak ve elektromanyetik spektrumdan daha fazla yararlanmak maksadıyla yürütülen askeri faaliyetler Elektronik Harp kapsamına girmektedir.

Elektronik Harp, insanlı ve insansız sistemler tarafından havadan, denizden, karadan veya uzaydan uygulanabilmekte; insanları, iletişimi, radarları veya diğer varlıkları hedef alabilmektedir.

Bu makalede genel olarak radarlar üzerine uygulanan EH uygulamalarından söz edilmiştir. Elektronik Harp; Elektronik Destek (ED), Elektronik Taarruz (ET) ve Elektronik Korunma (EK) olmak üzere üç ana başlık üzerinden incelenmektedir.

## Elektronik Destek (ED)

Elektronik Destek (ED) elektromanyetik yayın yapan düşman cihazlarının sinyallerini tespit etmek, sınıflandırmak, kaydetmek, parametrelerini çıkarmak, yerlerini belirlemek ve gerekli durumlarda Elektronik Taarruz (ET) ve Elektronik Korunma (EK) sistemlerine ilgili parametreleri sağlamak amacıyla kullanılan teknolojiler ve yöntemler kümesidir. Amaç, tehditlerin en kısa sürede tanınmasını, önceliklendirilmesini ve hedeflenmesini sağlamaktır.

Elektronik Destek verileri, Sinyal İstihbaratı (SIGINT), Haberleşme İstihbaratı (COMINT), Elektronik İstihbaratı (ELINT) verilerini oluşturmak amacıyla kullanılmaktadır. Sinyal İstihbaratı (SIGINT), radar ve radyo sinyallerinden bilgi toplama ve analiz etme, Haberleşme İstihbaratı (COMINT), askeri radyo trafiği sinyallerini dinleme, analiz etme, kodlarını çözme ve Elektronik İstihbaratı (ELINT), radar, dost-düşman tanıma sistemleri (IFF) ve füze ateşleme sinyallerinden bilgi toplama ve analiz etme süreçlerini içermektedir.

RF ED sistemleri Radar İkaz Alıcısı ve ED Keşif/Gözetleme Sistemleri olarak iki ana sınıfa ayrılmaktadır.

**Radar İkaz Alıcıları:** Basit yapılı, genelde düşük hassasiyetli ED sistemleridir. Kendini koruma amacıyla kullanılmaktadır. Bu nedenle gerçek zamanlı çalışırlar. Temel olarak tehdit sistem ana hüzmesini algılayıp tehdidin tipini, yönünü ve önceliğini takılı olduğu platformun mürettebatına bildirmeyi amaçlar.

RF Karıştırma Sistemleri ile kullanıldıklarında ilgili sisteme tespit ettiği radar parametrelerinin

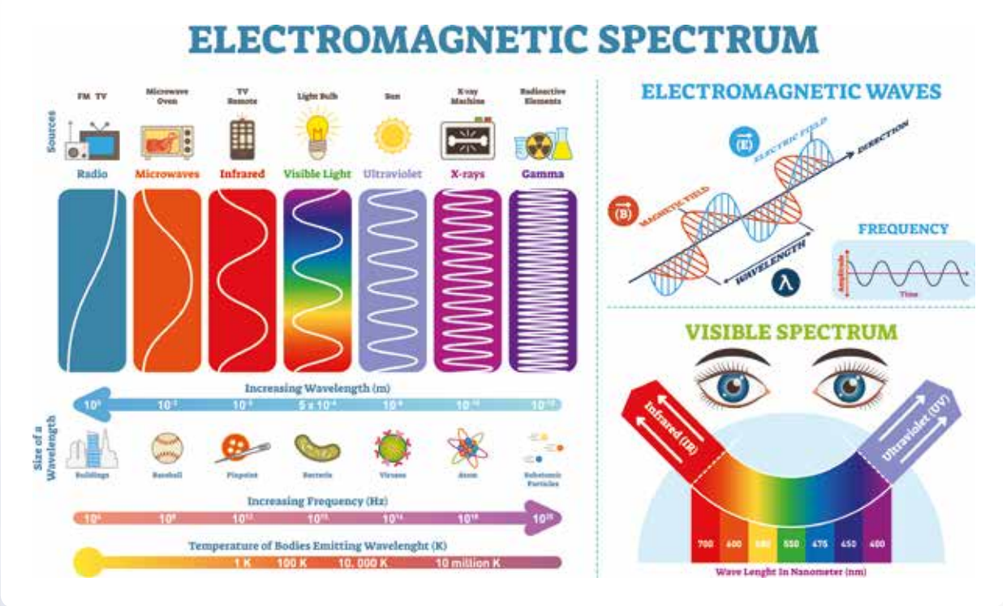
> "Güdümlü mermi veya aynı anlamda kullanılan füze, bir hedefi vurmak için fırlatılan ve uçuş esnasında rotası değiştirilebilen nesnelerdir."

gönderilmesi görevini de üstlenebilirler. Bu sistemler uçak, helikopter, gemi, denizaltı ve yer kuvvetleri tarafından kullanılabilmektedir. Radar İkaz Alıcısının çıkardığı parametrelerden bazıları; frekans, frekans değişim tipi, darbe genişliği (DG), darbe tekrarlama aralığı (DTA), DTA tipi, anten tarama süresi ve anten tarama tipidir.

**ED Keşif / Gözetleme Sistemleri:** Yerel tehditlerin yayınlarını tespit etmek ve güncellemek amacıyla kullanılmaktadır. Bu sistemler neredeyse gerçek zamanlı gibi çalışırlar. Genelde yüksek hassasiyetli ED sistemleridir. Bu sistemlerin temel görevi, haberleşme cihazlarının ve düşman radarlarının yerlerini tespit etmek ve ilgili parametreleri çıkarmaktır. Radar İkaz Alıcılarına göre parametre kestirim özellikleri daha başarılıdır. Ayrıca Radar İkaz Alıcıları tarafından ölçülmeyen ya da ölçülmesine gerek olmayan parametreleri de istihbarat amacıyla belirleyebilirler. Bu parametrelere polarizasyon, darbe şekli ve darbe içi modülasyon örnek gösterilebilir.

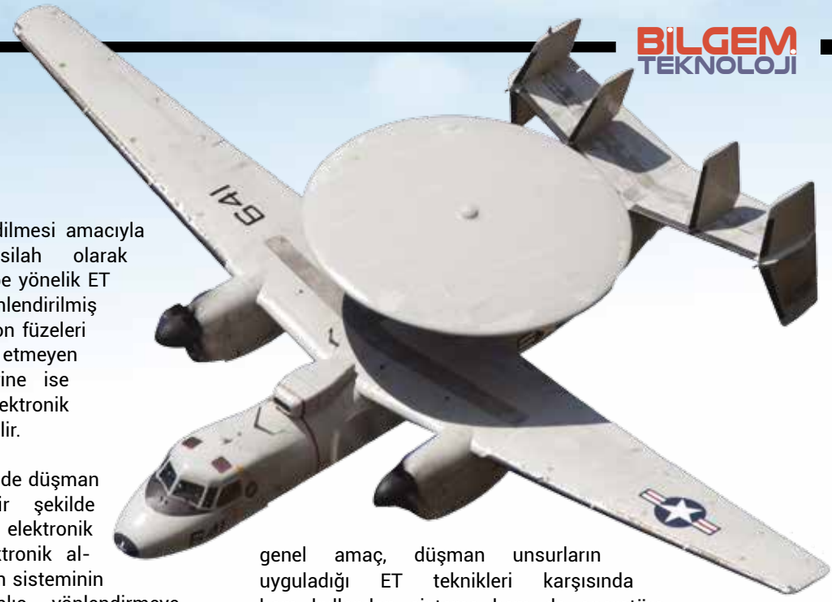
## Elektronik Taarruz (ET)

Elektronik Taarruz, elektromanyetik spektrumda çalışan düşmana ait sistemlerin çalışma performanslarının düşürülmesi, etkisizleştirilmesi, çalışmaz







hale getirilmesi veya tahrip edilmesi amacıyla elektromanyetik enerjinin silah olarak kullanıldığı yöntemlerdir. Tahribe yönelik ET uygulamalarına (Hard Kill) yönlendirilmiş enerji silahları ve anti-radyasyon füzeleri örnek verilebilirken; tahrip etmeyen taarruz (Soft Kill) yöntemlerine ise elektronik karıştırma ve elektronik aldatma teknikleri örnek verilebilir.

Elektronik karıştırma tekniklerinde düşman sisteminin işini düzgün bir şekilde yapmasını önlemeye yönelik elektronik karşı tedbirler uygulanır. Elektronik aldatma tekniklerinde ise düşman sisteminin gerçekleştirdiği faaliyeti yanlış yönlendirmeye yönelik tedbirler uygulanmaktadır. Örneğin bir hedef takip radarı için takip işinin yapıldığı ekranları ET cihazı tarafından yayınlanan gürültü ile doldurulup hedefi gizlemeye çalışmak bir elektronik karıştırma tekniği iken; bu ekranda gerçek hedefe benzer sahte hedefler oluşturmaya yönelik yapılan teknikler elektronik aldatma olarak değerlendirilmektedir.

ET uygulamaları tiplerine göre aktif/pasif ve platform üstü / platform dışı olmak üzere de gruplanabilmektedir. ET uygulamaları açısından aktif sistemler bir enerji kullanarak sinyal yayınlarken pasif sistemler enerji tüketmez ve doğrudan bir sinyal yayını yapmazlar. Platform üstü (onboard) yapılar platform üzerinden ve platformu kullanarak ET uygular; buna karşın platform dışı (offboard) yapılar platformu doğrudan kullanmadan ET uygulamayı amaçlar.

## Elektronik Korunma (EK)

Elektronik Korunma (EK) uygulamaları, RF EH uygulamaları arasında belki de en az bilinen ve dost unsurların uygulanan ET durumunda çalışmasına aksama olmadan devam etmesini amaçlayan yöntemlerdir. Diğer bir adı Elektronik Karşı Karşı Tedbir (EKKT) olan bu uygulamada genel amaç, düşman unsurların uyguladığı ET teknikleri karşısında hem kullanılan sisteme hem de operatöre farklı özellikler kazandırarak normal işleyişine devam etmesini sağlamaktır. ET tekniklerine karşı zafiyeti bilinen sistemlerde yapılacak olan yazılımsal ve donanımsal geliştirmeler, ET karşısında devreye sokulabilecek yeni yöntemler veya ET'ye maruz kalan operatörlerin farklı ET şartlarında eğitilmesi EK'ya örnek olarak verilebilir. Piyasada veya düşman unsur elinde bulunan ET sistemlerinin yetenekleri kapsamında incelenmesi ve bu yetenekleri bertaraf edecek yeni dost radar sistemlerinin tasarlanması da bir EK yöntemi olarak değerlendirilebilir.

### Sonuç

Radarın icadından günümüze kadar geçen sürede radar ve elektronik harp konsepti giderek büyümüş, dost-düşman tespiti, düşman unsurların faaliyetlerinin bastırılması, ülkelerin taktiksel ve stratejik adımlarının belirlenmesine yardımcı olması konularında kritik bir role sahip olmuştur. Milli güvenlik açısından özellikle askeri faaliyetlerde payı her geçen gün artmaktadır. Bu nedenle radar ve elektronik harp alanlarında yapılan yeniliklerin ve gelişmelerin takip edilmesi, uygulanması ve daha ileriye taşınması milli menfaatler için önem arz etmektedir.

# POSTGRESQL: Açık Kaynak Kodlu Veri Tabanı

> PostgreSQL, 1977 yılında akademik ortamda geliştirilmeye başlanmış, popüler, en eski açık kaynak kodlu, platform bağımsız, gelişmiş bir ilişkisel (RDBMS) veri tabanı yönetim sistemidir.

İbrahim Edib Kökdemir - Uzman Araştırmacı / BİLGEM YTE

Dünyada veri internet, bulut ve sosyal medyanın gücüyle üstel bir şekilde artmaktadır. Bu veriyi sağlıklı bir şekilde saklayacak, gerektiğinde hızlı bir şekilde erişilebilir yapacak, istenildiği zaman başka verilerle birleştirecek ve bu verilerden sürekli olarak anlamlar çıkaracak sistemler üretmek de ihtiyaç haline gelmiştir. Bu ihtiyaçlar, bilişim alanında birçok teknolojiyi adreslemektedir.

PostgreSQL, aşağıda sayacağımız özelliklerinden dolayı tüm dünyada küçük ölçekli projelerden büyük ölçekli kurumsal altyapılara kadar güvenle kullanılmaktadır.

- Veri tabanı ve sistem yöneticileri, veri ve sistem mimarları, geliştiriciler ve kurumlar için çekici olan, yenilikçi, sağlam ve kullanışlı birçok özellik sunar.
- Öğrenmesi, kurulumu, konfigürasyonu, yönetimi, izlemesi ve bakımı kolaydır.
- PostgreSQL'in aktif ve güçlü geliştirici topluluğu vardır.
- Tüm dünyadan katılımcıları bulunan ve çekirdek geliştiricilerin yer aldığı topluluk, soru ve sorunlara hızlı geri dönüşlerle çözüm sağlar.
- Hemen her yıl ticari ürünleri kıskandıran yenilikçi ve güncel özellikler içeren yeni bir sürümü yayınlanır.
- Birçok yazılım geliştirme platform ve dillerini destekler ve onlarla uyumlu çalışır.
- Geliştiricilerin işini kolaylaştıran çok geniş bir eklenti havuzu vardır.
- Coğrafi veri yapılarını ve NoSQL veri yapılarını (JSON, JSONB, XML, vb.) destekler. Coğrafi bilgi sistemleri entegrasyonu en başarılı açık kaynak kodlu veri tabanıdır.
- Kod mimarisi iyi tasarlanmış, dokümanları güncel ve yeterlidir. Bu özellikleri ile geliştirici dostudur.
- Bilinen çoğu programlama dili veri tabanı içerisine entegre edip geliştirme yapılabilir.
- Veri dünyasındaki yeni teknolojileri destekler. Büyük veri gibi özellikler PostgreSQL dünyasına kolaylıkla entegre edilebilir.
- Veri tipleri çok geniş ve esnektir.

PostgreSQL, DB-Ranking listesinde en popüler veri tabanları listesinde ilk 4 içindedir. Ayrıca 2017 ve 2018'de yılın veri tabanı seçilmiştir.
PostgreSQL'in bu kurumsal özellikleri, ileri düzey ve çok katmanlı güvenlik yapısından dolayı birçok kritik sistemde, bankalarda, kamu kurumlarında büyük yükler altında aktif olarak kullanılmaktadır.

Açık kaynak lisansı çok esnek olduğundan kopyalama, değiştirme, yeniden lisanslama, sınırsız sayıda ortama kurulum mümkündür. 50'den fazla PostgreSQL'den türetilmiş açık kaynaklı veya kapalı kodlu veri tabanı vardır. Diğer veri kaynaklarına erişim için kullanışlı imkânlar sunmaktadır. Herhangi bir veri kaynağıyla doğrudan veri tabanı içerisinden bağlantı oluşturulabilir.

## PostgreSQL Mimarisi

PostgreSQL güçlü bir ilişkisel veri tabanı sunucusudur ve tüm çok bilinen işletim sistemlerinde çalışır. PostgreSQL kurulumu yapıldığında, ana bir postgres işlemi (process) ve bu işlemde diğer veri tabanı sunucusu yardımcı işlemlerini çalıştırır. Varsayılan olarak 5432 portundan çalışır. Servise cluster adı verilir. Bir istemci postgres servisine bağlandığında her bir bağlantı için yeni bir postgres işlemi başlatılır ve istemci bu işleme bağlanır. İstemci bağlantısı bitince de işlem sonlandırılır.

**Veri Akışı:** Bir veri tabanının en değerli kaynağı bellektir. Belleğin bölümleri değişik işlere göre farklı isimlendirmelere sahiptir. Eğer istemciden gelen istek veride veya yapıda değişiklik gerektiriyorsa (veri ve veri tanımı değişiklikleri) bu bilgi önce ortak belleğe (wal_buffers) yazılır. Bu bellekteki veri de hızlı bir şekilde sıralı olarak diske yazılır ve istemciye 'veri kaydedilmiştir (COMMIT)' mesajı dönülür. Bu değişen veri kaydına PostgreSQL dünyasında WAL (Write Ahead Log) adı verilir. WAL sistemi, kurtarma, VT replikasyon ve yedekleme sistemi için ana yapı taşıdır.

WAL sistemi ile eş zamanlı olarak değişen veri, başka bir ortak bellekte (shared buffers) geçici olarak tutulur ve background writer ve checkpoint işlemleri tarafından belli parametrelere göre düzenli olarak diskteki yerine yazılır ve PostgreSQL kümesi diskte tutarlı hale gelmiş olur.

**Veriyi Sunma:** İstemci işlemlerinin büyük çoğunluğu, veri değişikliğinden ziyade veri okuma amaçlıdır. PostgreSQL istemci tarafından kendisinden istenen veriyi (tuples) saklayan blokları belleğe getirir ve ortak bellekte (shared_buffers) yer olduğu müddetçe veya postgreSQL servisi yeniden başlatılana kadar bu veriyi ortak belleğinde saklar. Ayrıca PostgresSQL işletim sisteminin ön belleğini de ortak bellek olarak kullanabilir. İstemci aynı veriyi tekrar istediğinde eğer veri bellekte varsa diske gitmeden bu veriyi bellekten sunar. Bu, performans açısından büyük bir avantaj sağlar.

PostgreSQL Paralel Sorguları destekler. Paralel sorgular, bir SQL deyimini parçalara bölerek, bu parçaları paralel yürütmeye ve fiziksel kaynakların verimli kullanılmasına yarayan ve sorguları hızlandırmak için kullanılan bir yöntemdir.

**Veri Tipleri:** PostgreSQL, boolean, karakter, sayısal, zamansal, UUID, array ve JSON gibi birçok standart veri tipini desteklerken, CBS (box, line, point, lseg, polygon) ve ağ (inet, macaddr), anahtar-değer (hstore), metin arama (full-text search), diğer sayısal veri tipleri için aralık (range) veri tiplerini de destekler. Ayrıca özel ve birleşik veri tiplerini rahatça üretebilme yeteneği de bulunmaktadır.

**Fonksiyonlar:** PostgreSQL, standart fonksiyonları, tetikleyici fonksiyonları (trigger function) ve saklı yordamları (stored procedure) da desteklemektedir.

**Operatörler:** PostgreSQL, AND, OR, NOT gibi mantıksal, < , >, <=, >=, =, != gibi karşılaştırma, +, - , *, % gibi matematiksel operatörlere ek olarak özel kullanıcı tanımlı operatörleri de destekler.

**Indexing:** PostgreSQL veri tabanı tek-sütun (single-column), çok-sütun (multicolumn), kısmi-indeks (partial index), tekil-indeks (unique index) ifade indeksi (expression index), dâhili indeks (include index), ve eş zamanlı indeksleri (concurrent index) destekler. PostgreSQL, Btree, Hash, Gist, SP-Gist, Bloom, GIN, BRIN, RUM indeks türlerini desteklerken, kullanıcı tanımlı indexlere de izin vermektedir.

**Constraints:** PostgreSQL, Check, Not Null, Unique, Primary key, Foreign key, Exclusion kısıtlamalarını (constraint) kullanabilir.

**Partitioning:** Bir tablonun bütünlüğünü bozmadan belli bir kritere göre parçalanarak performans ve yönetilebilirliğini artırma amaçlı kurulan bir yapıdır. Disk sistemlerinin hızlanmasıyla, veriyi aynı sunucu üzerinde mantıksal olarak ayrıştırarak yönetmek daha sık kullanılır olmuştur.

**Tablespace:** Veri tabanı nesnelerini (veri tabanı, şema, tablo, index ve sequence, temp alanları) için disk(ler)de farklı saklama yerleri belirterek disk IO yükünü dağıtma yöntemidir.

**Views:** PostgreSQL view'ları önceden hazırlanmış sorgular içeren bir veri tabanı nesneleridir. Bir veya daha fazla tablonun verilerini temsil ederek sorgunun karmaşıklığını basitleştirmeye yardımcı olur. View'lar bir SQL sorgusu bulundurur, ancak veri bulundurmazlar. Sanal tablolar da denilebilir.

**Materialized Views:** View kavramının verileri fiziksel olarak depolamasını sağlayacak şekilde genişletilmiş halidir. Karmaşık sorguları belleğe alarak burada depolar, istenildiği zaman güncellenmesine izin verir. Hızlı veri erişimi gerektiren karmaşık ve büyük veri bulunan durumlarda çok kullanışlıdır. Veri ambarı ve raporlamalarda çok kullanılır.

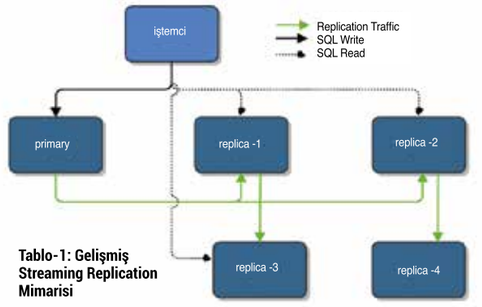
**Postgis:** Postgis PostgreSQL üzerinde, coğrafi özellikleri olan verilerle ilgili işlemlerin hızlı yapılmasını destekleyen bir eklentidir. Postgis, Open Geospatial Consortium'un desteklediği bütün veri tipi ve veri erişim metodlarını destekler.

**Güvenlik:** PostgreSQL ilk kurulduğunda dışardan erişime kapalı olarak çalışır. Sadece VT erişimi için tasarlanmış "pg_hba.conf" dosyasında istemci ip, erişilecek veri tabanı, erişecek kullanıcı ve erişim yöntemi ayarlarına göre erişim tanımlanabilmektedir. İstemci trafiği, SSL ile şifrelenebilir. 256bit şifrelemeyle korunan parola güvenliğini desteklemektedir. VT nesnesi tabanlı yetkilendirme özelliğine sahiptir. Row Based Security özelliğiyle satır ve sütunlara göre erişim denetimi yapılabilmektedir.





> "PostgreSQL'in aktif ve güçlü geliştirici topluluğu vardır. Tüm dünyadan katılımcıları bulunan ve çekirdek geliştiricilerin yer aldığı topluluk, soru ve sorunlara hızlı geri dönüşlerle çözüm sağlar."




**Tablo-1: Gelişmiş Streaming Replication Mimarisi**

**Backup:** Yedekleme, veri tabanı sistemleri için olmazsa olmaz bir özellik olduğundan PostgreSQL yedekleme özelliklerini doğal bir şekilde entegre etmiştir. Mantıksal ve fiziksel olarak 2 tür yedekleme vardır. Mantıksal yedeklemeler genellikle düz metin ve insan tarafından okunabilir biçimde depolanır. Bunun için pg_dump ve pg_dumpall istemci komutları kullanılır. İstenen nesneler seçilerek yedekleme yapılabilir.

Fiziksel yedekleme ile veri dosyaları ve onlarla ilintili WAL dosyaları saklanır. Bütüncüldür. PostgreSQL servisinin tamamı olarak yedeklenir. Parçalı bir şekilde yedeklenmez. Kendi içerisinde hazır olarak gelen pg_basebackup ile ya da aynı yöntemi kullanan harici yedekleme yazılımlarıyla yedeklenebilir.

**Streaming Replication:** Fiziksel replikasyon da denir. Canlı veri tabanının sorgulanabilir bir kopyasının oluşturulması işlemidir. 2 aşamalı çalışır, başlangıçta fiziksel dizinlerin pg_basebackup gibi araçlar kullanılarak kopyalanması ve devamında birincil veri tabanında oluşan WAL kayıtlarının bu yeni PostgreSQL servisi üzerinde otomatik olarak çalıştırılarak verinin tüm taraflarda eşlenmesi mantığı üzerine çalışır.

Bu yöntemde kopya sunucu sadece okunabilir olarak çalışır, veri yazmaya açık değildir. Sadece okuma içeren sorgular bu salt-okunur sunucu üzerinde çalıştırılarak birincil(primary) PostgreSQL sunucusu üzerindeki yük azaltılmış olur. Birden çok sunucuya kopyalanabilir veya hiyerarşik olarak kopya sistemi oluşturulabilir. Senkron ya da asenkron bir mimaride kurgulanabilir.

**Logical Replication:** Fiziksel replikasyonun tüm PostgreSQL servisine bütüncül yaklaştığını belirtmiştik. Mantıksal replikasyonda bu durumdan farklı olarak, Küme üzerinde tutulan veri tabanı, şema veya tablolara ya da tablo üzerindeki belli kayıtlara özel olarak kopyalama ayarlanabilir. Bu sayede istenen bir veri tabanındaki bir tablonun veya tabloların üzerinde gerçekleşen değişiklikler, başka PostgreSQL sunucularına kopyalabilir ve o sunuculardan veri okunabilir.

**Yüksek Erişilebilirlik:** Günümüzde, yazılım ile verilen hizmetlerin ve servislerin yüksek erişilebilir ve ölçeklenebilir olması, hizmet kalitesini çok önemli etkileyen iki köşe taşıdır. Açık kaynak olarak sunulan, kendi ekosisteminin parçası olan harici araçlarla PostgreSQL için failover (otomatik geçiş) süreci kurulabilir. Bunların en popüler olanları, pgpool-II, repmgr, patroni'dir.

**Foreign Data Wrapper:** Postgres içerisinden harici/uzak/farklı veri sistemlerine doğrudan bağlanmanızı, bu dış verileri iç nesnelermiş gibi kullanmanızı sağlayan PostgreSQL özelliğidir. PostgreSQL'in onlarca dış veri kaynağına bağlanabilen FDW eklentisi vardır.

## PostgreSQL Kullanıcıları

PostgreSQL, tüm dünyada, kamu ve özel sektörde önemli hizmetleri sunan uygulama sistemlerinde, finans ve telekom sektörlerinde iş kritik uygulamalarda, önde gelen teknoloji üreticilerinin ürünlerinde, araştırma merkezleri ve üniversitelerde, küçük ölçekli projelerden çok büyük ölçekli kurumsal altyapılarda güvenle kullanılmaktadır.

Türkiye'de Hazine ve Maliye Bakanlığı, TÜBİTAK, TÜİK, TEİAŞ, TKGM, RTÜK, MSB, AFAD, YSK, ÇŞB, İLBANK, TÜRKSAT ve Kuzey Kıbrıs NVI gibi kamu kurumlarında ve Biletix, Trendyol gibi önde gelen e-ticaret firmalarında kullanılmaktadır. Dünyada ise Apple, Fujitsu, Red Hat, Sun Microsystems, Cisco, Juniper Networks, Skype, McAfee, Comodo, Vmware, Instagram, Cloudflare, Adyen, Tomtom, CERN ve Greenpeace çok bilinen kullanıcı örneklerindendir.

### Referanslar


- PostgreSQL derived databases, erişim: 21.10.2019, https://wiki.postgresql.org/wiki/PostgreSQL_derived_databases.
- Foreign data wrappers, erişim: 21.10.2019,https://wiki.postgresql.org/wiki/Foreign_data_wrappers

# NATO MÜŞTEREK SİBER SAVUNMA MÜKEMMELİYET MERKEZİ ESTONYA

> 2016 yılında NATO, hava, kara ve denizden sonra siber alanı yeni bir etki alanı (domain) olarak kabul etmiştir.

*Ensar Şeker – Uzman Araştırmacı / BİLGEM İGBY

2008 yılında gerçekleştirilen Bükreş Zirvesi, NATO'nun siber alan ile ilgili attığı adımlar açısından bir dönüm noktası oldu. NATO, bu zirvede siber alanla ilgili dönüşümün yapılabilmesi adına gerekli adımları atma kararı aldı. Bükreş Zirve'sinin ardından siber savunma ile ilgili iki önemli adım atıldı. Zirveden sonra NATO Siber Savunma Yönetimi Otoritesi'nin (Cyber Defense Management Authority) Brüksel'de kurulmasına karar verildi. Diğer bir önemli adımsa Estonya Tallinn merkezli Müşterek Siber Savunma Mükemmeliyet Merkezinin (Cooperative Cyber Defence Centre of Excellence) kurulması oldu.

Bununla birlikte siber savunma konusu hukuksal olarak, NATO tarafından belki de en ciddi şekilde 8 - 9 Haziran 2016 tarihleri arasında Polonya'da gerçekleştirilen Varşova Zirvesi'nde ele alınmıştır. NATO hava, kara ve denizden sonra siber alanı ilk kez bu zirvede yeni bir etki alanı (domain) olarak kabul etmiştir. Yine bu zirvede müttefik ülkeler Siber Savunma Taahhüdü ile siber savunmayı geliştirme konusunda atılması gereken adımların öncelikli olduğunu kabul etmişlerdir. Buna göre her müttefik ülke kendi ulusal siber savunmasından mesul olmakla birlikte NATO ve diğer NATO üyesi ülkelerle uyumlu olacak şekilde gerekli adımları atmakla mükellef tutulmaktadır.

Ayrıca NATO siber savunma konusunda akademik ve uygulamalı eğitimlerle siber savunma tatbikatlarının daha etkili bir biçimde yaygınlaşması konusunda da karar almıştır. NATO, endüstriyel kuruluşlarla işbirliğini geliştirebilmek adına NATO Endüstri Siber Ortaklığı adı altında yeni bir proje başlatmıştır.

## NATO Mükemmeliyet Merkezleri

NATO Müşterek Siber Savunma Mükemmeliyet Merkezi, Estonya'nın başkenti Tallinn'de bulunmakta ve dünyada NATO akreditasyonu bulunan 24 mükemmeliyet merkezinden biri olarak faaliyetlerini sürdürmektedir. Mükemmeliyet Merkezleri, NATO üyesi ve ortak ülkelerden, liderleri ve uzmanları eğitip yetiştiren uluslararası askeri kuruluşlardır. Söz konusu merkezler,

- doktrin gelişimine yardımcı olur,
- müşterek çalışabilirlik ve yetenekleri geliştirmeye katkı sağlar,
- kazanılan deneyimleri analiz merkezi olarak faaliyet gösterir,
- deneyler yoluyla kavramları test eder ve onaylar.

Mükemmeliyet Merkezleri, muteber nitelikteki uzmanlık ve deneyimlerini müttefik ülkelerin faydasına katkıda bulunacak şekilde paylaşırken, NATO'nun dönüşüm sürecine de destek olmaktadır.

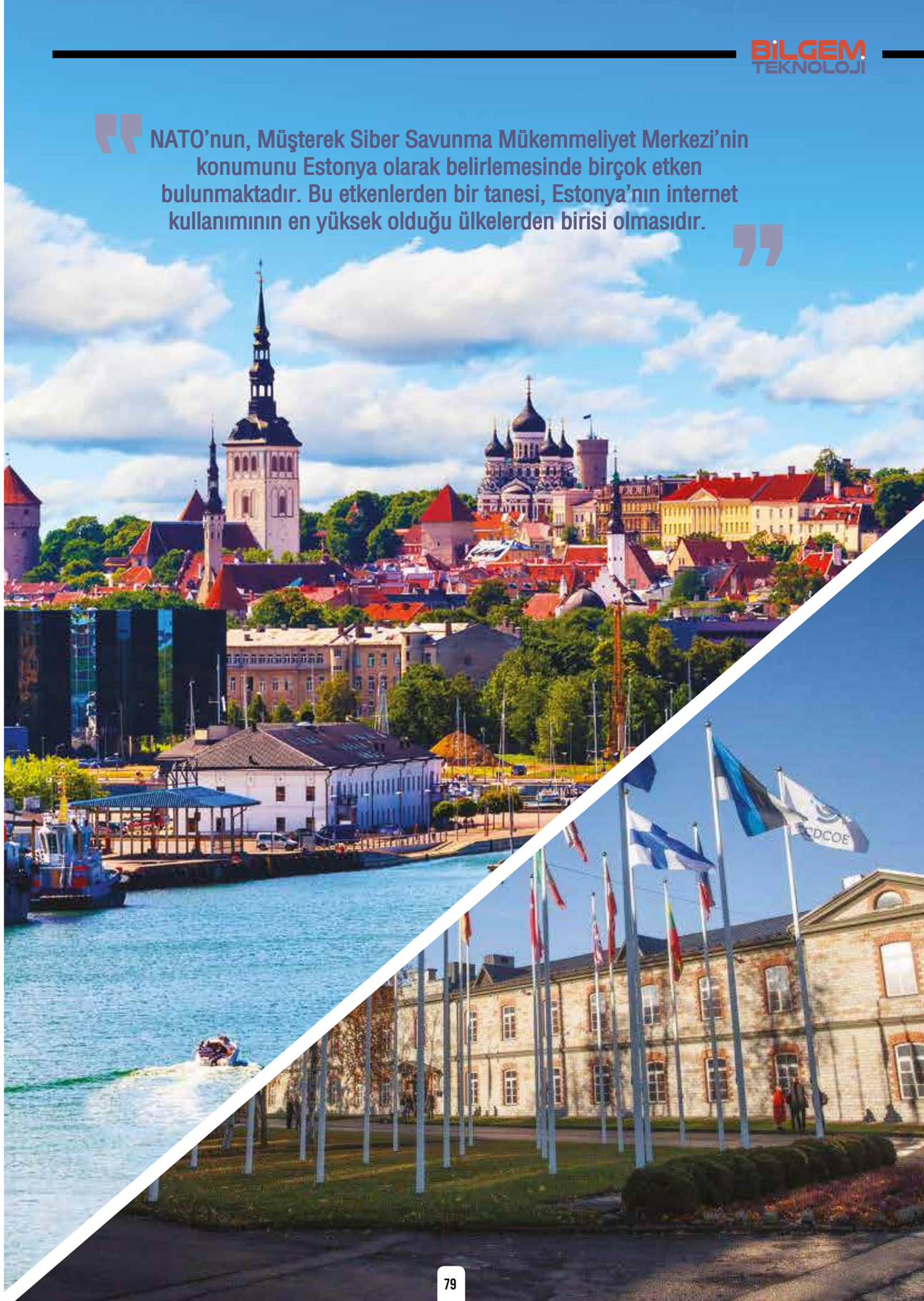
## NATO ve Estonya

NATO'nun, Müşterek Siber Savunma Mükemmeliyet Merkezi'nin konumunu Estonya olarak belirlemesinde birçok etken bulunmaktadır. Bu etkenlerden bir tanesi, Estonya'nın internet kullanımının en yüksek olduğu ülkelerden birisi olmasıdır. Devlet kurumları,





> NATO'nun, Müşterek Siber Savunma Mükemmeliyet Merkezi'nin konumunu Estonya olarak belirlemesinde birçok etken bulunmaktadır. Bu etkenlerden bir tanesi, Estonya'nın internet kullanımının en yüksek olduğu ülkelerden birisi olmasıdır.



bankalar ve günlük hayatla ile ilgili birçok işlemin internet üzerinden güvenli ve kişiye özel bir şekilde yapılmasına imkân veren dijital kimlikler, Estonya'da uzun zamandır kullanılmaktadır. E-devlet ve e-seçim konularında gerek uygulama gerekse de yaygınlık açısından Estonya birçok ilke imza atmıştır.

Estonya'nın internet konusundaki alt yapısı aynı zamanda onun zayıf noktası da olmuş, Rusya ile yaşanan gerginlik sonrasında Estonya, Rusya kaynaklı siber saldırıların hedef noktası haline gelmiştir. Söz konusu gerginlik, Sovyet Rusya işgali sırasında Tallinn'de II. Dünya Savaşı sırasında hayatını kaybeden Sovyet askerlerin anısına yaptırılan 'Bronz Asker Anıtı'nın Eston hükümetince 2007 yılında bulunduğu yerden kaldırılarak Tallinn Askeri Mezarlığına taşınmasıyla had safhaya yükselmiştir. Rusya kökenli siber saldırılar 27 Nisan 2007 tarihinde başlamış olup sonrasında şiddetlenerek devam etmiştir. Bu saldırılar çerçevesinde internet trafiği saniyede 20.000 paketten 4 milyon pakete kadar yükselmiş ve 128'den fazla müstesna DDoS saldırısı gerçekleştirilmiştir. Rusya'da bazı internet sitelerinde bilgisayarla çok içli dışlı olmayan bilgisayar kullanıcılarının dahi adım adım takip ederek siber saldırılara nasıl katkı sağlayabileceklerini açıklayan web forumları kurulmuştur. Bu saldırılar karşısında hazırlıksız yakalanan Eston hükümetinin ilk adımda geliştirebildiği karşı strateji ise internet bant genişliğini 2 Gbps'ten 8 Gbps'e çıkarmak ve sunucuların sayısını artırmak olmuştur.

Estonya'nın internet konusundaki alt yapısı ve bu altyapıya gerçekleştirilen siber saldırılardan elde ettiği kazanım ve tecrübeler, NATO'nun Müşterek Siber Savunma Merkezinin konumunu bu ülkede belirlemesinde önemli bir rol oynamıştır.

## NATO Siber Savunma Mükemmeliyet Merkezi

NATO Siber Savunma Mükemmeliyet Merkezi (NATO Cooperative Cyber Defence Center of Excellence - NATO CCD COE), 14 Mayıs 2008 tarihinde kurulmuş ve 28 Ekim 2008 tarihinde NATO'ya akredite olmuş bir siber güvenlik araştırma ve eğitim merkezidir. Bununla birlikte Merkez, Paris Protokolü çerçevesinde uluslararası askeri bir organizasyon statüsüne sahip olup sponsor ülkeler tarafından görevlendirilen ulusal temsilciler SOFA (A Status of Forces Agreement – Ev sahibi ülke ile temsilci gönderen ülke arasında imzalanan askeri anlaşma) kapsamında görev yapmaktadır.

> NATO Müşterek Siber Savunma Mükemmeliyet Merkezi, Estonya'nın başkenti Tallinn'de bulunmakta ve dünyada NATO akreditasyonu bulunan 24 mükemmeliyet merkezinden biri olarak faaliyetlerini sürdürmektedir.

Merkezin ilgilendiği alanlar arasında eğitim, danışmanlık, akademik çalışmalar ve yayınlar, pratik uygulamalar, Ar-Ge faaliyetleri sıralanabilir. Merkez; siber güvenliğin gerek teknik, gerek stratejik, gerekse hukuki ve uluslararası ilişkileri ilgilendiren konularında çok çeşitli faaliyetler yürütmektedir. NATO CCD COE'nin öne çıkan projeleri arasında; "The Tallinn Manual on the International Law Applicable to Cyber Warfare" çalışması ve her yıl düzenlenmekte olan "International Conference on Cyber Conflict (CyCon)" konferansı ile "Locked Shields" uluslararası siber savunma tatbikatı örnek olarak gösterilebilir. Siber güvenlik hukuku konusunda temel referans kitaplardan biri olduğu uluslararası otoritelerce kabul gören Tallinn Manual kitabının ikinci ve geliştirilmiş hali olan Tallinn Manual 2 kitabının çalışmaları tamamlanmış olup, 2017 yılı Mart ayında yayına sunulmuştur.



Merkez'e üyelik bütün NATO üyesi ülkelere açıktır. Merkez'e üye olan NATO üyesi ülkeler "sponsor" ülke adını alırlar ve Merkez'in faaliyetleri için belirli bir miktar finansal desteği her yıl sağlamayı taahhüt ederler. Merkez'in hali hazırdaki sponsor ülkeleri arasında Belçika, Çek Cumhuriyeti, Estonya, Fransa, Almanya, Yunanistan, Macaristan, İtalya, Letonya, Litvanya, Hollanda, Polonya, Slovakya, İspanya, Türkiye, İngiltere ve ABD bulunmaktadır. Ayrıca Avusturya, Finlandiya ve İsveç NATO üyesi ülkeler arasında bulunmamasına karşın CCD COE üyesi oldukları için katkı sağlayıcı ülke sıfatıyla Merkezin yapmış olduğu faaliyetlere temsilci göndererek katkıda bulunmaktadır.

Merkezin faaliyet ve işleyiş yapısı ile ilgili önemli kararların alındığı Steering Committee (Yönetim Kurulu)' ye sadece sponsor ülkeler temsilci gönderme hakkına sahiptir. Uluslararası askeri bir organizasyon olması sebebiyle NATO CCD COE'ye Türk Silahlı Kuvvetleri (TSK) akredite olmuş olup yönetim kuruluna atanacak temsilci de TSK tarafından görevlendirilmektedir.

NATO Siber Savunma Mükemmeliyet Merkezi, direktörlük ve bu direktörlüğe bağlı Hukuk, Strateji, Teknoloji, Operasyonlar, Eğitim ve Tatbikat ile Destek birimlerinden oluşmaktadır.

## Türkiye Üyeliği

Ülkemiz 3 Kasım 2015 tarihinde sponsor ülke statüsünde Merkez'le Memorandum of Understanding (Mutabakat Sözleşmesi) imzalayarak sponsor ve Merkezde daimi temsilci bulundurma hakkını elde etmiştir. Merkeze üyelik Genelkurmay Başkanlığı üzerinden, Bakanlar Kurulu kararı ile gerçekleşmiştir.

Genelkurmay Başkanlığı ve TÜBİTAK BİLGEM arasında varılan mutabakat gereği Genelkurmay Başkanlığı, Merkezdeki faaliyetlere katılımı TÜBİTAK BİLGEM ile gerçekleştirmektedir. Genelkurmay Başkanlığı ve TÜBİTAK BİLGEM tarafından görevlendirilen personel Merkez'de ulusal temsilci statüsünde görev yapmaktadır. Bununla birlikte, uluslararası askeri organizasyon statüsünde bulunan Merkez ile ilgili konularda insiyatif kullanma ve NATO CCD COE yönetim kuruluna ülkemizi temsilen atama yaptığı personeli ile Merkez'in işleyişi, faaliyetleri ve yönetimsel konularda yapılan oylamalarda oy kullanma ve ülkemizin ilgili konularla ilgili görüş, düsünce ve önerilerini NATO CCD COE yönetim kuruluna aktarma hak ve yetkileri Genelkurmay Başkanlığı'na aittir.

Merkezin altyapı ve idari destek masrafları ev sahibi ülke Estonya tarafından üstlenilmektedir. Buna karşılık, Merkezde görevlendirilen personelin tüm masrafları (maaş, seyahat, konaklama, vb.) gönderen ülkeye aittir. Yıllık üyelik katkı payı, ülkelerin işgal ettikleri pozisyona göre paylaşılmaktadır.

Bu kapsamda TÜBİTAK BİLGEM, Merkezde ulusal temsilci sıfatıyla araştırmacı görevlendirmekte ve Merkez tarafından yapılan araştırma geliştirme faaliyetleri ile uluslararası siber tatbikatlar ve konferanslar ile yine Merkez tarafından verilen siber güvenlik eğitimlerine oldukça önemli katkılar sağlamaktadır. Ayrıca burada görev alan araştırmacılarımız, Merkez'de elde ettikleri bilgi birikimi ve tecrübeleri ülkemize aktarma konusunda önemli adımlar atmaktadır. Merkezde bulundurduğu ulusal temsilcisi dışında TÜBİTAK BİLGEM, bünyesindeki araştırmacılar ile de NATO CCD COE tarafından organize edilen, dünyanın en geniş katılımcı sayısına sahip ve en ileri teknolojileri bünyesinde barındıran Kilitli Kalkan Siber Savunma Tatbikatının yeşil (tatbikat alt yapısından sorumlu takım), kırmızı takım (saldırı takımı) ve mavi takımlarına (savunma takımı) teknik destek sağlamaktadır.

Ayrıca TÜBİTAK BİLGEM yine NATO tarafından organize edilen diğer siber savunma tatbikatları, çalışma grupları ve projelere ilgili uzmanları ile katkılar sağlamaktadır. Bu üstün katkı ve başarılarından ötürü TÜBİTAK BİLGEM, NATO tarafından birçok ödül ve takdir mektubuna layık görülmüştür.

*2016 – 2018 yılları arasında NATO CCD COE'de ulusal temsilci olarak görevlendirilmiştir.

# Göz Görür Beyin Aldanır mı?

**"Sinemada izlediğiniz bol aksiyonlu bir film sonrasında, üzerinizde bıraktığı etkinin ardında yatan gerçeği hiç düşündünüz mü? Biz düşündük..."**

Fatih İmdat – Uzman Yrd. / BİLGEM YTE

Günümüz dünyasında, insanlar, artık gördükleri ve duyduklarının ne kadar gerçek veya gerçekliğe ne kadar yakın olduğuna bakmaktadır. "Ben sadece gözümün gördüğüne inanırım" diyenler, bundan böyle bu cümleyi söylerken iki kere daha düşüneceklerdir. Sosyal medya üzerinde, neredeyse her alan, onlarca manipülasyon ile dolu olabilir.

Dijital dünyamız, gazete manşetlerinden, video görsellerine kadar "clickbait" yani "tık tuzağı"na dönüşmüş durumda. Elbette bu tuzaklar hazırlanırken kullanılan görsellerin ve içeriklerin etkili olması büyük önem arz etmektedir. Hal böyle iken etrafımızın teknolojinin nimetlerinden faydalanmak isteyen, "zeki" ve "aldanmaz" insanlarla dolu olması da biraz tuhaf.

Bu cihetten bakıldığı zaman, günde acaba kaç kez aldatılıyoruz diye bir soru akla gelecektir. Cevabı merak ettiyseniz, bir nebze olsun izlediklerinizi ve gördüklerinize bakış açınızı değiştirecek bir teknolojiden bahsedelim. "GreenBox" veya "ChromaKey", "Greenscreen" isimleri ile bilinen teknolojiden.

## Greenbox Teknolojisi

Sinemaya gittiğiniz ve izlediğiniz filmin aksiyon sahneleri, efektleri ve mekânları sizi bambaşka duygulara sevk etti, değil mi? Yıllar önce çekilmiş meşhur "Avatar" filmini birçoğumuz izlemişizdir. Gösterimde olduğu dönemde, toplanmadık ödül bırakmayan bu filmi insanlar sinema salonlarında izleyip dışarı çıktıklarında, kendilerini boşlukta hissettiklerini söylemişlerdir. Hatta insanların bu film yüzünden depresyona girdiğini ele alan onlarca yazı ve makale kaleme alınmıştır. Burada insanları depresyona soktuğu iddia edilen şey, izleyicilerin filmde sunulan sanal dünyanın büyüsüne öylesine kapılmasıdır ki, film bittiğinde, yani büyünün etkisi geçtiğinde, gerçek dünyanın onlara çok yavan ve sıkıcı gelmeye başlamasından kaynaklanmıştır.

Eğer sizin de etrafınızda böyle psikolojik travma yaşayanlar varsa aşağıdaki resmi gösterin kendilerine. Yani onları, büyüyü bozacak olan gerçeklikle tanıştırın. Çocuklarınıza Örümcek Adam gibi bir binadan aşağı atlayamayacakları veya Superman olup uçamayacakları hakkında sıkı sıkı tembihlerde bulunun.

Çocuklarınıza Örümcek Adam gibi bir binadan aşağı atlayamayacakları veya Superman olup uçamayacakları hakkında sıkı sıkı tembihlerde bulunun.

İngiltere kraliçesi Queen Elizabeth, giydiği yeşil bir elbise sonrasında, muzip grafikerlerin bu resim üzerinde yaptığı değişikliklerle sosyal medyada günlerce konuşulacak resimler ortaya çıkmıştı



"Superman" filminin kamera arkasındaki görüntüden bir kesit

Muhtemelen bu sahneyi görenler koca bir hayal kırıklığı yaşayacaklardır. Bu görüntüleri işleyen ve bu alanda çalışan video grafik tasarımcıları, hayran kalarak izlediğimiz bu sahneleri, teknolojinin tüm nimetlerini kullanarak ve çok ciddi maaşlar alarak yapmaktadır. Genç arkadaşlarımıza, ülkemizde bu alanda yapılan çalışmaların, yurt dışına göre çok da tatminkâr olmadığını hatırlatıp, hâlâ iyi video grafikerlere ihtiyaç olduğunu belirtmek isterim.

Bu görüntüleri işlerken, özel video grafik efektleri kullanılmaz ise, hayran olarak izlediğimiz filmlerin arkasında yatan gerçek, koca bir yeşil (veya mavi) bir perdeden ibaret olacaktır.

## Neden Yeşil veya Mavi?

Lawrence Butler, renkli bir filmde yeşil ekran teknolojisinin (veya mavi ekran teknolojisinin) nasıl kullanılacağını bulan ilk kişidir. Yeşil ekranlar, Lawrence Butler'ın 1940'daki "Bağdat Hırsızı" filmindeki özel efektlerinden dolayı bir akademi ödülü kazanmasından bu yana çok yol kat etmiştir.

Yeşil veya mavi olmasının sebebi, kontrast(zıtlık) renk meselesidir. Belirli bir alanı, diğerinden kusursuz şekilde ayırabilmenin en güzel yöntemi, arka plan renginin bariz şekilde farklı olması ile gerçekleştirilebilir. Ayrıca insanın ten renginde olmayacak renklerin seçilmesi de işin püf noktalarından biridir. Yaygın olarak maviye nazaran yeşil rengin kullanılmasındaki diğer bir faktör de, günümüz gelişmiş dijital kamera sensörlerinin yeşile daha fazla duyarlı olmasıdır.

## Renk Unsurları

Renk konusu, çoğunlukla algılarımızla, yani bizde bulunan görsel sensörlerle ilişkili bir meseledir. Renkleri oluşturan 3 ana renk vardır. Kırmızı (Red), yeşil (Green) ve mavi (Blue). Bu renkler tasarımcıların dünyasında RBG kısaltmasıyla kodlanmıştır. Aslında rengi tam olarak tanımlamak için RGB ve HSV ortak olarak kullanılabilir. Burada HSV, ton (Hue), doygunluk (Saturation) ve değer (Value) olarak tanımlanır.

İnsan teninin parlaklığı, değeri ile orantılıdır, ancak renk tonu ve doygunluk pek değişmemektedir. Bunun için bazı iyi fizyolojik nedenler vardır. Temelde, dış deri katmanımız (epidermis) optik olarak, derimiz üzerinde nötr renkli bir filtre olarak hareket eder. Bu onu büyük oranda perfüze (dokuların, organların kanlanması) eden kanın rengine bağlı olarak kırmızıdır.

> "Özel video grafik efektleri kullanılmaz ise hayran olarak izlediğimiz filmlerin arkasında yatan gerçek, koca bir yeşil (veya mavi) perdeden ibaret olacaktır."

## Yeşil Ekranlar Nasıl Çalışır?

Yeşil ekran, bilinen adıyla "chroma key" nasıl çalışır? Aslında, yeşil perdeler bu işin sadece bir boyutunu ilgilendirir. Bu renkli alanı diğer alanlardan ayırmaya yarayan video üretim yazılımları mevcuttur.

İyi bir renk seçmek için sahnedeki başka hiçbir şeyde bulunmayacak olan renk seçilir. Bununla birlikte, chroma key özelliğine sahip video yazılımı (örneğin, Adobe After Effect) kaldırılacak olan rengi seçmeye imkan verir. Ardından sihirli bir dokunuşla, hayallerinizin sınırlarını zorlayan video içerikleri üretmeye başlayabilirsiniz.

## Yeşil Ekranlar Ne Gibi Kolaylıklar Sağlar?

Bu teknolojinin var olması, hem mali açıdan hem de nihai ürün için ortaya çıkacak çeşitli risk faktörlerini ortadan kaldırmak adına kurtarıcı gibidir. Düşünsenize, iki büyük ordunun savaşma sahnesinde, yüzbinlerce insana ihtiyaç vardır. Fakat askeri kıyafetlerle donattığınız 100 kişilik bir ekibin arkasına koyulacak ucuz yeşil bir perde, size koskoca bir ordu yaratmanıza olanak sağlayabilir.

Game of Trones dizisinde, ak gezenler karakterinin ardında yeşil perde olmasına rağmen, bastığı alanlarda gerçek kar ve buz kütleleri kullanılmıştır.

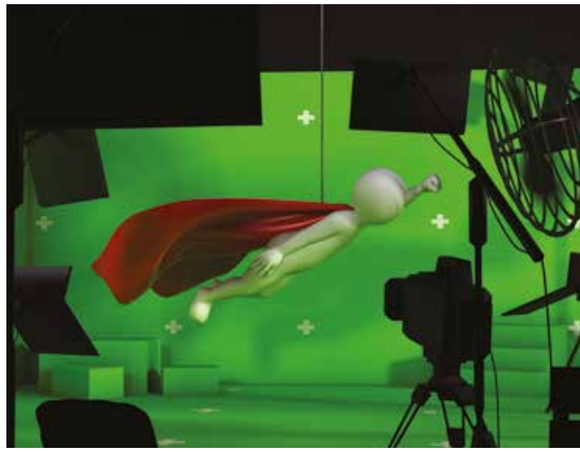
## Yeşil Ekran Efektini Ben de Kullanabilir miyim?

Haber yayını, sinema filmi ve video oyunu endüstrisi bu tekniği kullanarak oldukça etkili işler yapmaktadır. Eğitim öğretim faaliyetlerinde de insanların işini çok kolaylaştırdığı apaçık bir gerçektir. Ayrıca bu yeşilin, sadece ardınızda değil, üzerinizde de olması aynı etkiyi yaratabilir. Emin olun, benzer videoları çok basit yöntemlerle, küçük bir internet araştırması yaparak sizler de yapabilirsiniz. Yeter ki, yeşiliniz ve ışığınız bol olsun. Aman dikkat edin! Çünkü muzip bir arkadaşınız, giydiğiniz yeşil bir elbisenin yerine öyle şeyler koyabilir ki, aklınız hayaliniz durabilir.

Bu teknikle, youtuber dediğimiz birçok içerik üreticisi, artık merdiven altında dünyanın en çok izlenen içeriklerini üretebiliyor.

Hayır, hayır, şaka değil. Gerçekten merdiven altında, kamerası olan herhangi bir cihazla, ardı sıra koyduğu yeşil perde önünde, gayet izlenmesi yüksek (geliri de) içerikler üretebiliyor.

Tabi ki gerçek dekorasyonlar her zaman bu işin vazgeçilmezleridir. Ne yaparsanız yapın, hangi üstün (uzaylı) teknolojisini kullanırsanız kullanın, bazen gerçek dekorasyonun yerini tutturamazsınız.



Bundan dolayı, bu teknolojiyi ileri boyuta taşıyan ve bizim ağzımızı açık bırakarak (yok artık) dedirten mesele tam da budur. Koskoca film ve dizi setleri (şehirleri) kuran yapımcılar neden buna ihtiyaç duyuyor acaba? Madem her şeyi bir yeşil perde ve ışıklarla halledebiliyorlar, neden devasa film setleri kurma ihtiyacı hissediyorlar?

Beynin gördüğü şeylerin gerçekliğine inanmasını sağlayan birçok etken bulunmaktadır. Görünenin ne kadar gerçek olduğu veya olabilme ihtimali gibi iki temel mesele vardır. Eğer kullandığınız teknolojide, gerçek unsurların üzerine kurduğunuz yardımcı unsurlar varsa doğru yoldasınız demektir.

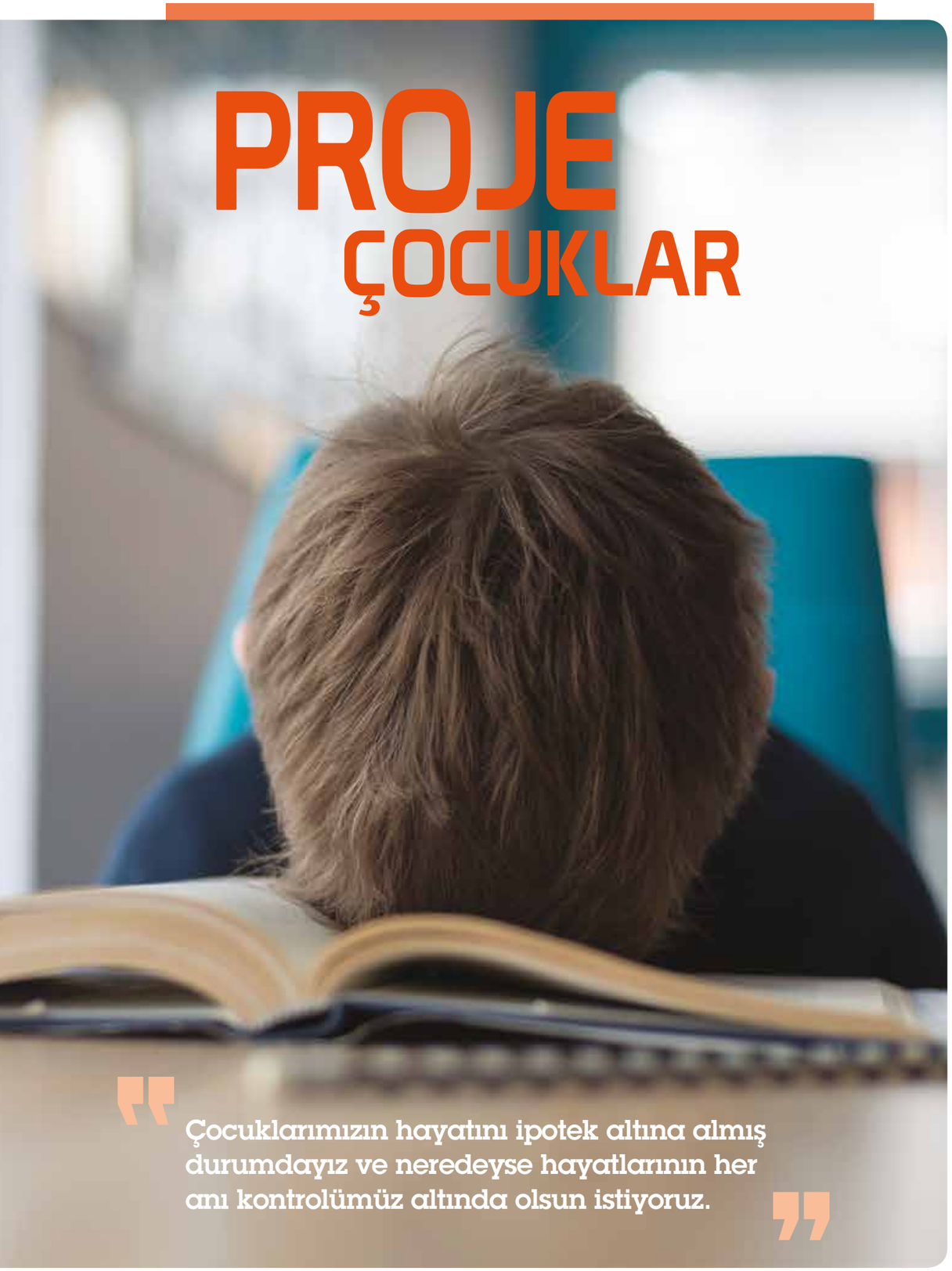
Fakat tamamen gerçek dışı, yani sanal unsurları kullanıyorsanız, insanların aklında her zaman şu ifade çakılı duracaktır: Hadi oradan sende!

Unutulmamalıdır ki, görsel olarak görünen her nesnenin ardında kodlamalar bulunmaktadır. Bunu insanoğlunun görünen bedeninin ardında kodlanmış olan, DNA, hücre ve benzeri birçok özelliğe benzetebilirsiniz. Bu noktadan bakıldığı zaman, insanları hayrete düşüren bu ilginç teknolojinin ardında yatan yazılım ve kodlama sürecini de unutmamak gerekir.

Bu yazımızda, temel olarak yeşil perde hakkında bazı ipuçlarını paylaştık. Artık yeşil bir kıyafet giyerken, bir kez daha düşünmeniz gerekecek...

*Kaynakça :*
*https://www.livescience.com/55814-how-do-green-screens-work.html*
*https://theconversation.com/ive-always-wondered-why-is-a-green-screen-green-92989*
*https://www.jmcacademy.edu.au/news/how-does-a-green-screen-work*
*https://www.techsmith.com/blog/how-to-create-a-diy-green-scre/*

# PROJE ÇOCUKLAR



> Çocuklarımızın hayatını ipotek altına almış durumdayız ve neredeyse hayatlarının her anı kontrolümüz altında olsun istiyoruz.

Abdullah Alpaydın - Danışman / BİLGEM

Eskinin çocukları bugünün birçok imkânından yoksundu. Belki biraz da mecburiyetten tasarruf ve kanaat odaklı olarak yetiştirilir, az şeyle mutlu olmayı öğrenirlerdi. Kişiler arası ilişkiler, bireylerin karşılıklı güven ve samimiyeti esasına dayandığı için daha sahiciydi. Bundan dolayı sokaklar daha güvenilir mekânlardı. Mahalle kendi otokontrolünü sağlar, büyükler sadece kendi çocuklarını değil diğer çocukları da korur, himaye ederlerdi.

Çocuklar ebeveynlerinden daha az ilgi görürlerdi ama bir o kadar da özgürdüler. Kendi başlarına okula gider gelir, özgürce sokağa çıkıp arkadaşlarıyla oynarlardı. Çocuğun sosyal gelişimi ev, sokak ve okul üçgeninde daha sağlıklı ve dengeli şekilde sağlanırdı. Çocukların başarılı olmaları teşvik edilir ama başarı her şeyin üstünde görülmezdi. Aynı sınıfta okuyan komşu çocuğu, alt edilmesi gereken bir rakip olarak değil arkadaş, hatta kardeş olarak görülürdü. Başarıdan ziyade iyi karakterli ve düzgün insan olmak, halk ifadesiyle "adam olmak" daha fazla önemsenir ve değer görürdü.

Eskinin toplumunun sorunsuz ve ideal olduğunu iddia etmiyorum elbette. Lakin bugünle karşılaştırdığımızda, geçmişte başa çıkılması gereken daha az sorun vardı.

## Günümüz Dünyasında Çocuk Olmak!

Bugünün çocuğunun içine doğduğu dünya, eskiyle karşılaştırıldığında sayısız imkân ve zenginlik içeriyor. Lüks evler, arabalar, teknolojik araçlar, envai çeşit oyuncaklar... Velhasıl geçmişe göre oldukça konforlu bir dünya bizimkisi. Konforlu olduğunda şüphe yok ama ne kadar insani, ne kadar doğal? Bu soruya olumlu cevap verebilmek pek mümkün görünmüyor.

Özellikle şehirlerde çocukların yaşantısı içler acısı. Yukarıda bahsetmiş olduğum eski zaman şartlarında büyümüş bizim kuşak, kendi çocuklarına hayatı zindan ediyor ne yazık ki! Bizler, dünün görece özgür şartlarında yetişmiş bireyleri olarak çocuklarımızın hayatını ipotek altına almış durumdayız ve neredeyse hayatlarının her bir anı kontrolümüz altında olsun istiyoruz. Sokağa güvenmediğimiz için çocuklarımızı kendi başlarına sokağa gönderemiyoruz. Güvenilecek bir sokak da kalmadı zaten. Çocuklara yönelik suç oranının had safhaya ulaşmış olması da bu güvensizliği tetikliyor. İnsanlara güvenemiyoruz çünkü birbirimizi yeterince tanımıyoruz. Tanımak için çaba da göstermiyoruz. İnsan tanımadığının düşmanıdır derler ya, tanımayınca sevemiyoruz da...

> İnsanlara güvenemiyoruz çünkü birbirimizi yeterince tanımıyoruz. Tanımak için çaba da göstermiyoruz.

Güvenlikli sitelerde yaşayanlarımız bile çocuklarını gönül rahatlığıyla dışarı gönderemiyor. Okul ve çevresi de eskisi kadar güvenli olmadığı için çocuklarımızı okula ya kendimiz götürüp getiriyor ya da servislerle gönderiyoruz. Kısacası evin dışında hiçbir mekânı çocuklarımız için güvenli bulmadığımız için çocuklarımıza evlerimizde bir nevi hapis hayatı yaşatıyoruz. Odalarında, bilgisayarları

ve oyuncaklarıyla kendi başlarına yaşamaya mahkûm ettiğimiz çocuklarımızın asosyal ya da içe kapanık olduğundan şikâyet ederken, "Yediği önünde, yemediği ardında, bu çocuk niye böyle oldu?" diye serzenişte bulunmaktan da geri durmuyoruz.

## En Başarılı Öğrenci, En Başarılı Sporcu, En Başarılı Sanatçı...

Birey ve toplum boyutunda yaşanan (geri dönüşü artık çok zor görünen) değişimler sebebiyle bugünün toplumu, eski ifadeyle "kahir ekseriyetle" maddiyat ve çıkar odaklı olmuş durumda. Toptancı bir yargıya varmayı doğru bulmamakla birlikte günümüz dünyasında, her şeye sahip olmak arzusuyla gözü dönmüş egoist bireylerin sayısı azımsanmayacak düzeyde.

Her şeyin en iyisi, en büyüğü, en gösterişlisi, en lüksü, en konforlusuna sahip olma gayesiyle hayatlarını ziyan eden acınası insanlar güruhu olduk maalesef. Çocuklarımıza yaklaşımımızı da bu takıntılarımız belirliyor. Öyle ki, onları da sahip olduğumuz diğer metalar gibi algılayıp, her alanda en başarılı bireyler olmalarını sağlamak için müthiş bir baskı kuruyoruz üzerlerinde... Eğitim sistemimizin anlamsız ve bir türlü bitmeyen sınavlarla boğduğu çocuklarımızın sırtlarına bir o kadar da biz yük bindiriyoruz. En başarılı öğrenci, en başarılı sporcu, en başarılı sanatçı vb. her alanda en başarılı olmak gibi irrasyonel hedeflerin altında eziyoruz onları. Çünkü kendimiz ve onlar için hayal ettiğimiz hedefleri gerçekleştirmek için çok başarılı olmaları, en iyi okullardan mezun olup bu sayede en çok para kazandıran meslekler edinerek en kısa zamanda refaha kavuşmaları gerekiyor. Mutluluk mu? O bu süreçte önemli değil. Para nasıl olsa mutluluğu da satın alır(!)

Kısacası, sanki birer proje olarak görüyoruz çocuklarımızı. Onların başarısı, bizim başarı hanemize yazılacak varsayımıyla hareket ediyoruz. Çocuklarımızı kendi çevremizle yürüttüğümüz rekabete kurban

> "Evin dışında hiçbir mekânı çocuklarımız için güvenli bulmadığımızdan onlara, evlerimizde bir nevi hapis hayatı yaşatıyoruz."

ederken gözümüzü bile kırpmıyoruz. Onlar başarınca biz de başarmış olacağız, böylece bizim sosyal statümüz de yükselecek diye düşünüyoruz. Tabii olarak başarısızlıklarını da kendi hanemize yazılmış bir yenilgi olarak algılıyoruz.

Bunlarla da yetinmiyor, geçmişte hayal edip başaramadığımız ya da elde edemediğimiz ne varsa onları da çocuklarımız üzerinden elde etmeye çalışıyoruz. Geçmiş başarısızlıklarımızın hesabını da onlar üzerinden görmeye çalışıyoruz.

Çocuklarımız üzerinden yaptığımız tüm bu mücadele "Ben yaptım, bu benim eserim!" diyebilmek için sanki. Amaç buysa başardık; şimdi eserimizle gurur duyabiliriz(!)

İşin acı tarafı, onlara yaptığımız bunca kötülüğü "Tüm bunları onların iyiliği için yaptığımız" iddiasıyla haklılaştırıyoruz. Bu sayede, suçluluk duygusunu da bastırmış oluyoruz.

Başarıya tapan, başarıyı en üstün değer olarak gören ebeveynlerin yetiştirdiği çocuklar sağlıklı gelişebilir mi? Elbette, hayır! Bu yüzden, psikiyatrlar, psikologlar sorunlu çocuklar üzerine çalışırken ilk olarak çocuk-ebeveyn ilişkilerine odaklanır, sorunun kaynağını ilk olarak orada ararlar. Çünkü sorunlu çocuk yoktur, sorunlu ebeveyn vardır. İşin aslı şu ki; çocuk ebeveyninin müsaade ettiği kadar sağlıklıdır.

# Çok Gezen de Bilir!

**"Seyahat etmenin insana kazandırdığı yetkinlikler saymakla bitmez."**

Petra, Ürdün



"Seyahat etmek cesaretinizi artırır, isteyince ne çok şeyi başarabileceğinizin farkına varırsınız."

Merve KARABUĞA - Uzman Yrd. / BİLGEM İGBY

Seneler evvel, daha henüz ilkokul yıllarında münazara etmeyi öğrenirken ilk münazaramız için verilen konu şuydu: "Çok okuyan mı, yoksa çok gezen mi bilir?" Ta o yıllarda çok gezenin daha çok bileceğini düşünüp, çok gezen bilir diyen grupta yer almayı tercih etmiştim. Aradan yıllar geçti, insan yedisinde ne ise yetmişinde de odur sözünün yansımasıyla yıllık izinlerin ve resmi tatillerin el verdiği sürece dünyayı keşif yolculuğuma başladım.

Tipik bir Türk ailesinin kız çocuğuysanız, dünyayı keşif macerasına atılmak o kadar da kolay olmuyor başlarda. Belki bir memur ailesinin çocuğu olsaydım, yeşil pasaportumla üniversite yıllarında interrail yapmayı zorlayabilirdim ancak böyle bir durumum da yoktu. Hal böyle olunca işe girip para kazanmayı beklemek zorunda kaldım keşif için.

## Gezmeye Başlamak

Yolculuğum, hemen herkes gibi Avrupa kıtasına seyahatle başladı. Yaygın inanış ve coğrafyanın da yakınlığı sebebiyle Avrupa'ya seyahat güvenli olarak algılanıyor toplumumuzda. Öyle biletimi ve valizimi aldım, atladım uçağa gittim gibi de olmadı başlarda. Isınma turlarım tur paketi alarak başladı. İlk seyahatlerimi tur firmalarıyla gerçekleştirdikten sonra bir şeylerin beni tatmin etmediğini fark ettim.

30-40 kişilik gruplarla sürekli koşturmaca halinde bir yerden bir yere sürüklenmek, tur rehberlerinin klişe üslupla "bilmem kaç senesinde şu oldu, bu bina da filanca bina" şeklindeki tekdüze anlatımları, çok hoşuma giden bir yerde istediğim kadar vakit geçirememek, istediğim gibi fotoğraf çekememek, tur programına göre hareket etmek gibi durumlar beni rahatsız etmeye başlamıştı. Geziyordum, ancak ruhu eksikti sanki. Yabancı bir ülkede, farklı kültürden insanlarla birlikte olduğum hissini vere miyordu bana tur paketleri. Bu sebeple tursuz gezme kararı aldım.

İlk tursuz gezimi, yerel bir havayolu şirketimizin yaptığı uçak bileti kampanyasını gördükten sonra "vira Bismillah" deyip, üniversiteden bir arkadaşımla Ürdün'e uçak bileti alarak gerçekleştirdim. Ailem artık yurtdışı seyahatlerime de alışmaya başlamıştı ancak bir Arap coğrafyasına iki kız başımıza gidiyor olmamızın huzursuzluğunu yaşıyor ve bunu da bana hissettiriyorlardı. Annemin birkaç günde bir "Şimdi kesin gidiyor musunuz yani?", "Başka yer yok muydu kızım gidecek?", "Arkadaşının anne babası bir şey dememiş mi?" gibi sorularına da az maruz kalmadım. Ama bu kez farklıydı, bu kez çok daha keyifli geçecek ve farklı tecrübeler edinecektim, biliyordum.

## Seyahat Etmenin Faydaları

Öncesinde bir plan çıkarmak gerekliydi. Hangi şehirde kaç gün kalınacak, şehrin hangi bölgesinde konaklanacak, gidilen şehirlerde nereler görülecek, hangi aktiviteler yapılacak, o ülkenin en meşhur yemeği hangi restoranda yenecek, şehir içi ve şehirlerarası ulaşım nasıl sağlanacak ve bunun gibi daha birçok cevaplanması gereken soruyla baş başa kalıyorsunuz. Ancak bu size ürkütücü gelmesin. Araştırdıkça, rotayı çıkarmaya ve plan şeklini alıp oturmaya başladıkça keşif heyecanınız artıyor ve bir an evvel yola düşmek için sabırsızlanmaya başlıyorsunuz.

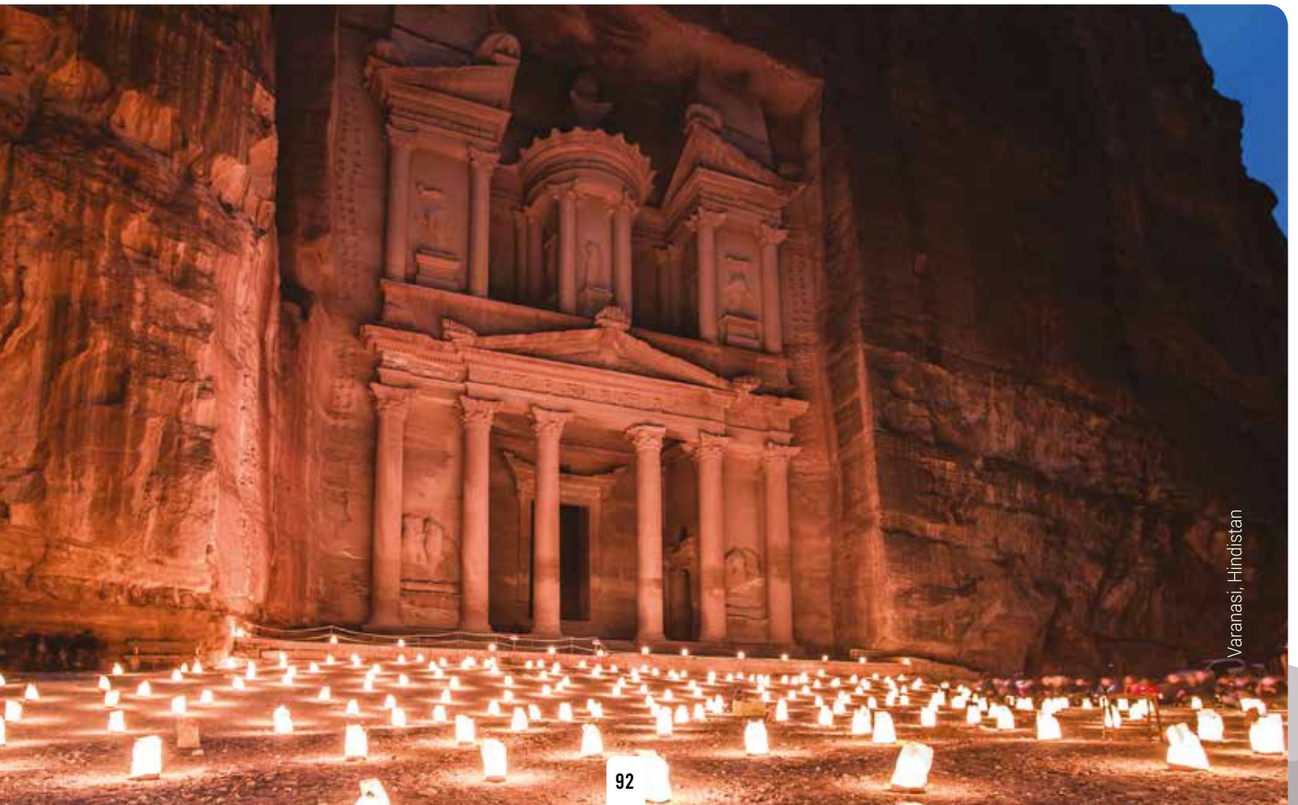
> **Farklı kültürlerden insan tanıdıkça daha açık fikirli, farklılıklara saygılı bir bireye dönüşüyorsunuz.**

Üstelik bunları yaptıkça siz hiç farkına varmadan planlama ve süreyi efektif kullanma beceriniz gelişiyor. Bu deneyimi kazanırken de süreci keyif alarak yönetmek hem sosyal hem de iş hayatınız için kesinlikle çok önemli bir kazanım.

Kendi planlamanızla seyahat etmek, aynı zamanda kriz yönetimi becerinizi de geliştiriyor. Yabancı bir memlekette sınırlı sürelerle ve imkânlarla seyahat ederken karşılaştığınız irili ufaklı problemlerde hızlı ve etkin çözüm üretmek durumunda kalıyorsunuz birçok kez. Bu yaz kuzenimle birlikte gerçekleştirdiğim Asya seyahatimiz sırasında kuzenimin kredi kartı bilgileri çalınmıştı. Üstelik bu olay, wi-fi işimizi görür diye hat almadığımız bir ülkede başımıza geldi ve kendi hattımızı da yurtdışındayken arama yapmaya kapatmıştık, sonrasında sürpriz bir faturayla karşılaşmamak için. Yani bankayı arayamıyorduk kredi kartını iptal ettirmek için. Bu arada bankadan üst üste SMS geliyordu karttan yeni işlemler yapıldığına dair. O an gerçekten bir kriz anıydı ve hızlı aksiyon alarak çözüm üretmemiz gerekiyordu. Türkiye'deki bir yakınımıza sosyal medya üzerinden ulaştık ve onun vasıtasıyla bankaya bildirimde bulunarak sorunu çözebildik. Birebir aynı durumla karşılaşmasanız bile, seyahatleriniz sırasında hiç beklenmedik anlarda can sıkıcı aksiliklerle karşılaşabilirsiniz. Bu tip durumlarla karşılaştıkça, panik yapmadan olabildiğince hızlı ve çözüm odaklı karar verme ve problem çözme gibi yeteneklerinizi geliştiriyorsunuz.

Uzak rotalara, farklı coğrafyalara gittikçe çok farklı kültürlerle, yaşayış ve inançlarla karşılaşıyorsunuz. Gittiğiniz yerin yerel halkıyla vakit geçirdiğinizde ise bunu çok daha iyi hissediyorsunuz. Hindistan'ın en mistik şehri olarak bilinen Varanasi'de yerel bir arkadaş, gezimiz sırasında bize eşlik etmişti. Yıllardır Hinduların ineğe taptığını zannederdik, oysa kendisi ineklerin süt verdiği için onları anne gibi kıymetli gördüklerini ve bundan dolayı ineklere saygı duyduklarını söylemişti. Yerel halkın arasına karışarak onlarla vakit geçirmek, kültürlerini ve inanışlarını kendilerinden dinlemek çok daha keyifli ve o insanlardan dinlediğiniz hikâyeler hep bir anı olarak kalıyor size. Yeri geliyor sizi misafir ediyor, yeri geliyor bir ihtiyacınız olduğunda ellerinden geldiğince koşturuyorlar. En güzeli de, dünyanın her yerinde bir arkadaşınız oluyor ve farklı kültürlerden insan tanıdıkça daha açık fikirli, farklılıklara saygılı bir bireye dönüşüyorsunuz. Ayrıca insan ilişkileri ve iletişim kabiliyetiniz de siz hiç farkına varmadan gelişme gösteriyor. Daha girişken, kendini daha rahat ifade eden bir insan olmaya başlıyorsunuz. En önemlisi, cesaretiniz artıyor ve isteyince ne çok şeyi başarabileceğinizin farkına varıyorsunuz.

Aslına bakarsanız seyahat etmenin insana kazandırdığı yetkinlikler, ne saymakla ne de buraya yazmakla biter. Üstelik bağımlılık yaptığı da bir gerçek! Bir sonraki sayımızda yol hikâyelerine kaldığımız yerden devam etmek üzere, hoşçakalın!



Varanasi, Hindistan

# BİLGEM'de Tiyatro

**"TÜBİTAK Tiyatro Topluluğu (T3), genellikle her yıl Nisan-Mayıs aylarında bir oyun sahnelemektedir."**

Hatice Seçim - Başuzman Araştırmacı, Hediye Coşkun - Başteknisyen / BİLGEM TDBY

TÜBİTAK Tiyatro Topluluğu (T3), 2010 yılında iki BİLGEM çalışanı Hediye Coşkun ve Hatice Seçim tarafından Ozan Erbak yönetiminde kuruldu. Kurulduğu günden bu yana kurum çalışanları tarafından ilgiyle takip edilen ekip, her sezon en az bir oyun çıkarma hedefiyle yola çıkmaktadır.

Şüphesiz tiyatro, tıpkı diğer sanatlar gibi disiplin temelli bir sanat dalıdır. Ekip bu disiplin bilinciyle bütün sezon çalışmakta ve sezon sonunda sözünü sahnede söylemektedir.

Yeni sezon çalışmaları genellikle Eylül-Ekim aylarında başlamaktadır. Çalışmalar haftada iki gün akşam olacak şekilde başlamakta, oyun sahneleme döneminde bu süreler haftada yedi güne kadar çıkabilmektedir.

İlk üç aylık dönemde, yönetmen tarafından temel oyunculuk ve diksiyon dersleri verilmektedir. Oyuncular bu süreçte, yönetmenin de yardımıyla bireysel eksikliklerini fark etmekte ve gidermek için egzersizler yapmaktadır.

Bir taraftan ekibe yeni katılan oyuncular kendilerini yetiştirirken bir taraftan da oyun okuma süreci başlamaktadır. Ekibin sayısına ve yapısına uygun oyun bulma, başlı başına bir süreçtir. Özellikle oyuncuların keyif alacağı ve seyircilerin ilgisini çekebilecek oyun metinleri araştırılmaktadır. Bu süreçte tecrübeli oyunculara ve yönetmene büyük iş düşmektedir.

En uygun oyun metninin seçilmesiyle oyun süreci başlamaktadır. Yönetmen oyun sürecinde de oyunculuk eğitimi vermeye devam etmektedir.

Oyun sürecinde parça parça sahneler çalışıldıktan sonra toplu çalışmalara geçilmektedir. Toplu çalışmalar bazen hafta sonları da yapılabilmektedir. Böyle durumlarda oyuncular bütün günü sahnede geçirmektedir. Oyuncuların çocukları ve eşleri de desteğe gelmektedir. Genellikle bir şenlik havasında geçen provalar, şüphesiz oyun sürecinin en keyifli zamanlarıdır.

Genellikle Nisan-Mayıs aylarında sezon oyununu sahneleyen ekip, oyuncuların takvim uygunluğuna göre bir program belirlemektedir. Bu programa göre, ortalama 4-5 defa aynı oyun sahnelemesi yapılmaktadır.

Zaman zaman dışarıdaki sahnelerde de oyun gösterimi yapan ekip, dışarıdaki tiyatro seyircilerinin de takdirini kazanmayı başarmıştır. Gebze Kent Konseyi Sahnesi, Kadıköy Akla Kara Sahnesi, Ali Poyrazoğlu Sahnesi gibi mekânlarda oyun gösterimi yapan ekip, ilerleyen dönemlerde kurum dışı gösteri sayısını artırmayı hedeflemektedir.

Ekibin bu günlere gelmesinde iki emekçi yönetmenin katkısı çok büyüktür: Ozan Erbak ve Özdemir Çiftçioğlu. Ozan Hoca, ekibin kuruluş döneminde yer almış, birçok temel sorunun giderilmesine ve oyuncu adaylarının ekibe katılmasına büyük katkı sağlamıştır. Yeni kurulan bir ekibin en büyük ihtiyacı oyuncu olduğu için, Ozan Hocanın sunduğu eğlenceli ve eğitici ortam, birçok kurum çalışanının tiyatroya başlamasını sağlamıştır. Özdemir Çiftçioğlu ile ekibin yolu ise 2015 yılında kesişmiştir. Özdemir Hoca gerek tecrübesi, gerekse yüksek sahne disipliniyle ekibe birkaç basamak birden atlatmıştır. Bu durum, hem seyirci beklentisini yükseltmiş hem de oyuncular için itici bir güç olmuştur.

**"Zaman zaman dış sahnelerde de oyun gösterimi yapan TÜBİTAK Tiyatro Topluluğu (T3), Gebze Kent Konseyi Sahnesi, Kadıköy Akla Kara Sahnesi, Ali Poyrazoğlu Sahnesi gibi mekânlarda oyun gösterimi yapmıştır."**

Ekibin mali sponsoru olan TezKoop-İş Sendikası'nın katkısı, sürecin adım adım daha da ileriye götürülmesini sağlamıştır. Sadece sendikal destek değil, yönetimsel olarak da ekibin desteklenmesi, gelişim sürecini hızlandırmıştır. Güvenlik biriminden, yapım işletme birimine, yemekhaneden, servis hizmetlerine kadar, kurumun ilgili bütün birimleri sezon boyunca ekibe ihtiyaç duyduğu desteği vermektedir.

### TÜBİTAK Tiyatro Topluluğu (T3) Oyunları

- Bugün Git, Yarın Gel (2018-2019)
- Fare Kapanı (2017-2018)
- Zalım Tilivizyon (2016-2017)
- Yaşasın Delilik (2015-2016)
- Sevgili Doktor (2014-2015)
- Size Öyle Geliyorsa Öyledir (2013-2014)
- Aristophanes'in Barışı (2012-2013)
- Don Cristobita İle Dona Rosita'nın Acıklı Güldürüsü (2011-2012)
- "www.ailesinden.com" (2010-2011)

Geçen sezon "Bugün Git, Yarın Gel" adlı oyunumuzu izlemeye gelen Prof. Dr. Hasan Mandal'a, Prof. Dr. Hacı Ali Mantar'a ve dokuz yıldır bütün oyunlarda bizi yalnız bırakmayan seyircimize teşekkür ederiz.

# Kriptoloji

*İki kişinin bildiği şey sır değildir derler*
*Öyle ya insanoğlu az mı çiğ süt emmiş*
*Boşuna mı sandınız çığ gibi şüpheler*

*Zaman milattan belki binlerce yıl öncesi*
*Emektar postacı kuşlara güven kalmamış*
*Allah etmeye ya çözülürse kadim kuşdili*
*Serseri sapanla kuşa bir taş atılır belki*
*Elçiye zeval olmaz lafı külliyen yalanmış*

*Kraldan krala haber uçurmak amma zor iş*
*Garibim ulağın saçlarını sıfıra vurmuşlar*
*Dövmeci hattat kesilip metni başına işlemiş*
*Sonra bekle ki yeni baştan uzasın saçlar*
*Öteki kral hele şunun başını tez kazıyın der*
*Başta bir mühür ve bir demet bayat haber*

*Kimi de merdaneye parşömen sarmış*
*Hep börekler açacak değil ya mübarek*
*Şeridin üstüne gizli saklı mesaj yazmış*
*Okuyana aynısından bir merdane gerek*

*Gelin simdi de Sezar'ın hakkını Sezar'a verelim*
*Cenk meydanında ufak tefek matematik hesabı*
*Sezar ne harf yazdıysa bir zahmet sağa öteleyin*

*Vigenere şifresi kasıp kavurmuş geçmişi*
*Şifrenin kasisli yollarında zayiat pek büyük*
*Mevzuyu çok sonradan çakozlamış Kasiski*

*Gel zaman git zaman ne yöntemler gelişmiş*
*Sen simetrik mi istersin yoksa asimetrik mi?*
*Aklın karşısında akıl her zaman galip gelmiş*
*Biri şifreleye dursun öteki çözsün tüm şifreyi*
*Ali yazar Veli bozar hesabına benzer hani*

*Nazilerin Enigması dört yana sürmüş tankları*
*Anlayana kadar ne canlar heba olup gitmiş*
*Anlayanlar da sanki o Nazilerden çok farklı*

*Dur durak bilmeden yarışma üstüne yarışma*
*İki Belçikalı şifrenin ipini göğüsleye dursun*
*NSA parmağı varsa yarışmalar bile muamma*

*İçlerinden biri varmış rahmetli dedemin adaşı*
*Mısırlı El Gamal Dayı kulağıma bir hoş gelir*
*Şahsen tanımam varsa yoksa dedemin hatırı*

*Sanki deli bağlarcasına sımsıkı bağlanmış*
*Zincire vurulmuş bölünmüş mesaj katarı*
*Ya nasip deyip bahtına s kutusu açılmış*
*Üstüne her tur çevirip başka bir anahtarı*

*Bir kadın bir erkek konu komşuya dert olmuş*
*Onların adı gurbet ellerde Alice ve Bob'muş*
*Rusların dediğine bakarsak Natasha ve Boris*
*Bizim memlekette meşhur Ayşe ile Bora ikilisi*
*Kimdir onlar neyin nesidir orası hiç belli değil*
*Ama yakayı ele vermeleri sanki an meselesi*

*Belli ki gençler birbirini sevmiş olmalı*
*Sahi genç olduklarını da nereden çıkarttım*
*Doğru ya aşkta bir milyon yaş bile olası*
*Elektronik kod kitabında geçse de izleri*
*İkisi birbirini hiç gördü mü o bile şüpheli*
*Belki olanlar uzaktan uzağa bir sevdaydı*
*Belki de buluşma yeri bir ağacın altıydı*

*Neyse efendim Ayşe ile Bora birbirini sevmişler*
*Ortak anahtarları sevdadan gelmiş olsa gerek*
*Hem utanmışlar hem ulu orta el âleme demişler*
*İlla bir sertifika makamına sırlarını açacaklar*
*Hiç üçüncü şahsın güveniliri olur mu canım*
*Bir cahillik yapıp her şeyi tehlikeye atacaklar*

*Ah o gözü çıkası ortadaki mendebur adam*
*Kızın babası mıdır, yoksa başka bir talibi mi?*
*Olur, da bir gün atlatıp yüce sertifika makamını*
*Özel anahtarları aşırıp aşkı onlara dar eder mi?*
*Öyle al gülüm ver gülüm hiç kolay olur mu canım*
*Anahtarlar dillere düşmeden değişir mi sandın*

*İsterseniz bütün konunun bir özetini alalım*
*Kriptoloji hakikaten zor zanaatmış azizim*
*Her satırın altına elektronik imzamı atarım*

*Akın Korkmaz - Uzman Araştırmacı / BİLGEM BTE*



TÜBİTAK BİLGEM

Bu bir proje tanıtımıdır.

# Milli Üretim Entegre Sualtı Savaş Yönetim Sistemi Preveze Sınıfı Uygulaması (MÜREN PREVEZE)

Proje kapsamında "denizaltılarımızın savaş yönetim sistemi"nin milli algoritmalara ve yazılıma dayalı olan MÜREN sistemi ile değiştirilmesi planlanmaktadır.

Bu sistemlerin milli olarak geliştirilmesi ve üretilmesi ülkemizin güvenliği açısından hayati derecede kritiktir.

# BLOKZiNCiR Araştırma Ağı

## Blokzincir Araştırma Ağı (BAĞ):

TÜBİTAK BİLGEM ve Üniversitelerimizin
işbirliği ile kurulmuş bir araştırma platformudur.

## Amacı;

- Ülkemizin, hayatımızın her noktasında köklü değişiklikler yapmaya aday blokzincir teknolojileri konusundaki rekabet gücünü yükseltmek
- Ülkemizde konu ile ilgilenen araştırmacıları bir araya getirmek
- Eş güdüm içinde çalışmalarına yardımcı olmak

www.bag.org.tr

TÜBİTAK BİLGEM BAĞ Koordinatörü TÜBİTAK BİLGEM

### Üye Kurumlar

Bahçeşehir Üniversitesi · Antalya Bilim Üniversitesi · Gazi Üniversitesi · Gebze Teknik Üniversitesi · İstanbul Gedik Üniversitesi · İstanbul Ticaret Üniversitesi · Kadir Has Üniversitesi · Konya Teknik Üniversitesi · Necmettin Erbakan Üniversitesi · Yıldırım Beyazıt Üniversitesi