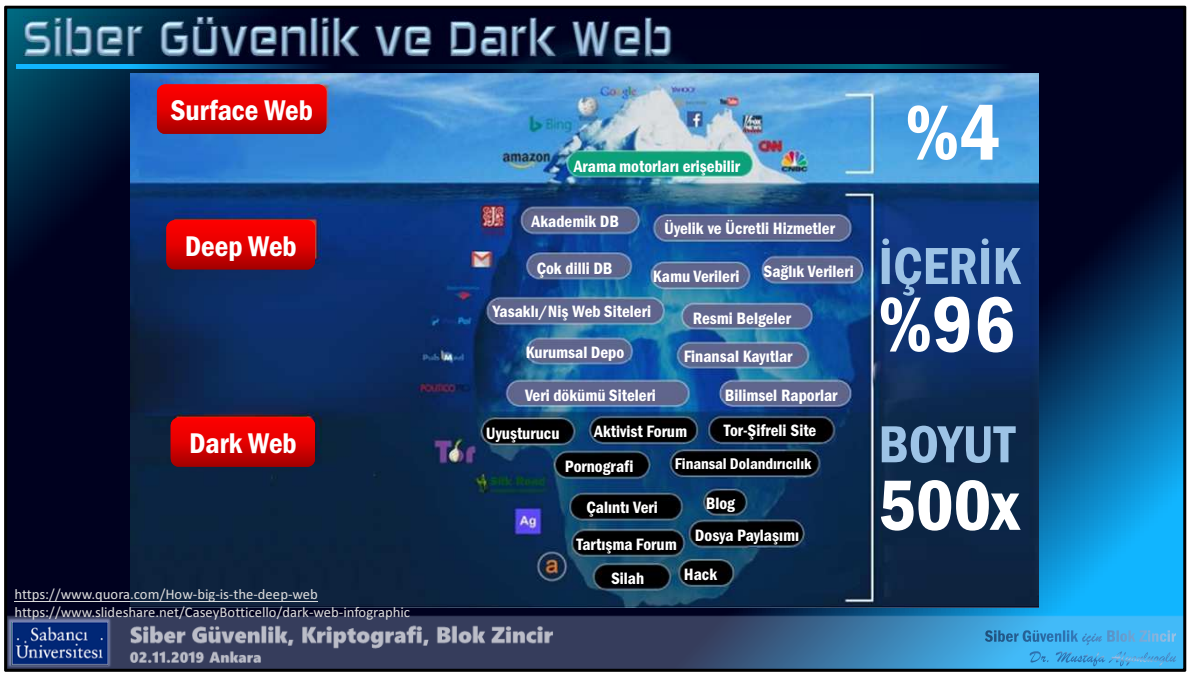
Sunum Tarihi : 02.Ekim.2018
Hazırlayan : Dr. Mustafa AFYONLUOĞLU / Keynote Speaker
Etkinlik : Sabancı Üniversitesi «Siber Güvenlik, Kriptografi, Blok Zincir» Etkinliği
Erişim : http://afyonluoglu.org → KAYNAKLAR → SUNUMLAR
Yayım / Alıntı Şartı : Sunumdan alıntı yapılması için açık referans (Eser Sahibinin Adı Soyadı, Yayımlandığı Web Sayfası Adresi) gösterilmesi zorunludur.
NOT : Bu sunumda herhangi bir kurum temsil edilmemektedir. Tüm görüş ve değerlendirmeler sunumu yapan kişinin uzmanlık değerlendirmeleridir.

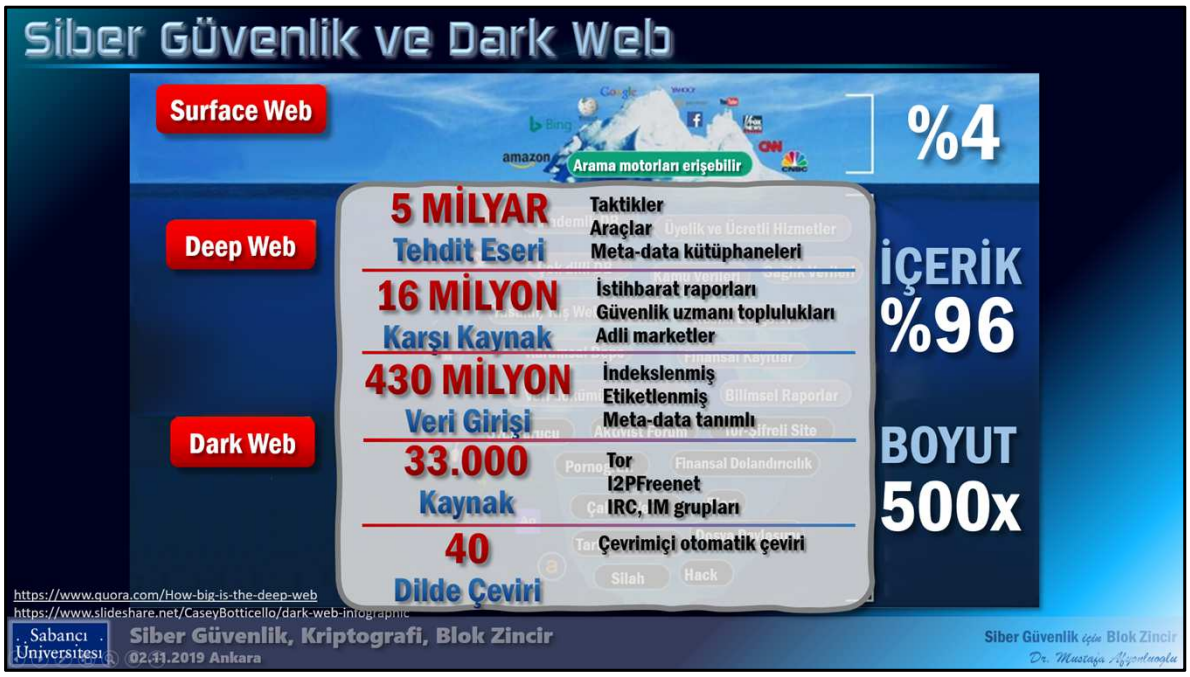
Sayın Rektörüm, Sayın Başkanım, Kıymetli Davetliler,
Hepinizi saygıyla selamlıyorum. Hoşgeldiniz.

Blokzincir, günümüzde ülkelere önemli fırsatlar vadeden yeni bir teknoloji, siber güvenlik ise dijital hayatımızın vazgeçilmez bir parçası…
Siber güvenlik için blokzincir diyebiliyor muyuz yoksa bundan önce «blok zincirin siber güvenliği»ni de tartışmalı mıyız? Bu değerlendirmeyi sizlerle birlikte yapma fırsatı veren Sabancı Üniversitesi Etkinlik Yürütme Kurulu'na öncelikle içntelikle teşekkür etmek istiyorum.

- **TEKNİK VERİLER** ----------
Sunum Dosyası Hazırlanma Ortamı:
Microsoft Ofice 365 ProPlus, Microsoft Powerpoint 1908 (Build 1929.20300)



Siber güvenlik dediğimizde aklıma gelen terimlerden birisi karanlık web. Biliyorsunuz, arama motorlarıyla bizim erişebildiğimiz internet kaynakları (yüzey web) bugünkü web dünyasının sadece %4'üdür. Geriye kalan %96'lık kısım ise derin web ve karanlık web olarak adlandırılıyor ve yaklaşık boyutunun, yüzey web'in 500 katı olduğu tahmin ediliyor. Bu bölümün içeriğinin %65'i yasa dışı veri, belge ve bilgilerden oluşuyor. Özellikle karanlık web'deki içeriğe baktığınızda, bir çok yasa dışı faaliyete hizmet edebilecek içerikler olduğunu göreceksiniz.



Nitekim bugün itibarıyla karanlık web'de 5 milyardan fazla siber tehdit eseri, yani siber saldırı için taktikler, saldırıda kullanılacak araçlar, saldırı için gereken veri kütüphaneleri, yüz milyonlarca endekslenmiş ve kategorilenmiş veri tabloları, on milyonlarca istihbarat raporu ve güvenlik uzmanı yazısı, 30 binden fazla erişim kaynağı var. Üstelik buradaki materyallerin kullanımını kolaylaştırmak ve anlaşılabilirliği arttırmak için, karanlık web'e 40 dilde otomatik çeviri mekanizması entegre edilmiş durumda. Siber saldırılar neticesinde yasa dışı yollarla elde edilen her türlü belge ve bilgi de bu ortamda paylaşılıyor veya satılıyor. Görüleceği üzere, siber güvenlik (ya da siber tehdit) bakımından en riskli kaynaklardan birisi burası…

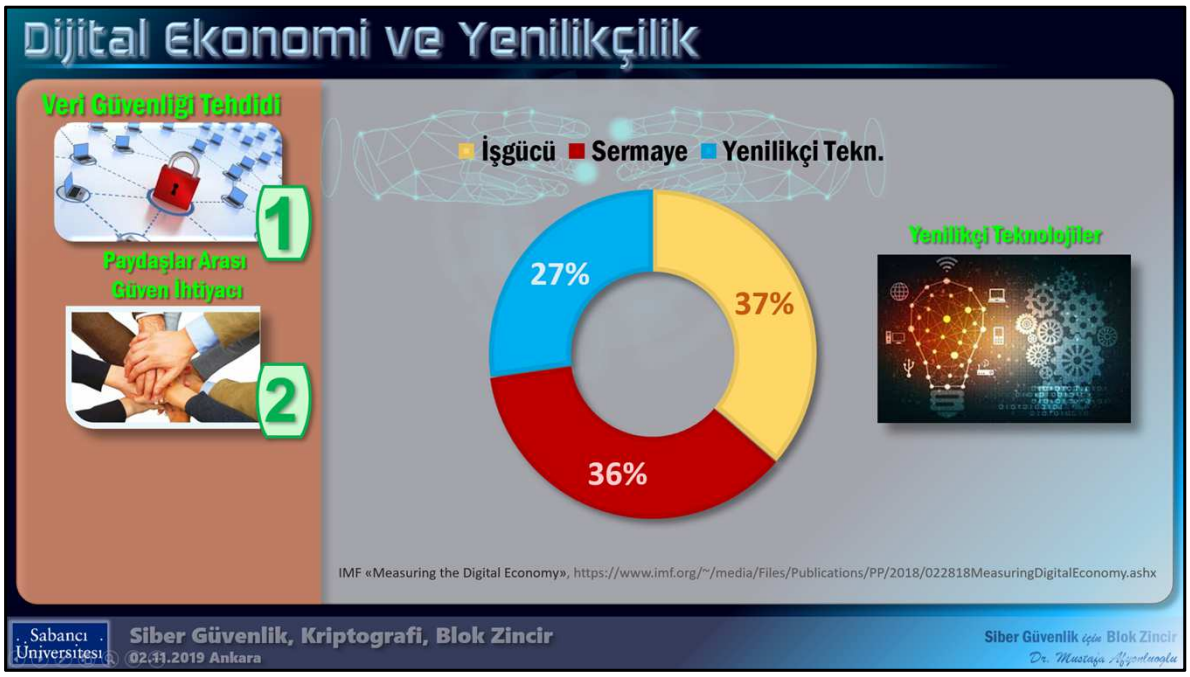
Siber güvenlik deyince halen popülerliğini yitirmeyen bir diğer kavram da «fidye yazılım». Geçen yıl siber güvenlik için yapılan harcamalar toplam 14 milyar $ iken fidye yazılımların sadece bildirilenlerinin iş dünyasına verdiği zarar 8 milyar $ idi. Üstelik bu yıl sadece sağlık sektöründe bu zararın 25 milyar $'a ulaşması bekleniyor. Fidye yazılımlar, zararlı yazılımların yarısından fazla bir büyüklükte (%56) ve ciddi bir siber tehdit olarak özellikle iş dünyasını hedeflemiş durumda.

Siber saldırı için ister karanlık webdeki kaynaklar kullanılsın ister oltalama gibi tekniklere veya fidye yazılım, Truva atı, rootkit ya da virüs gibi zararlı yazılımlara başvurulsun, temelde saldırının hedeflediği 3 ana başlık vardır. Bunların en başında **veri güvenliği tehdidi** gelir. Yani kurumsal verilere, kişisel verilere veya ticari sırlara, kişiler, şirketler veya devletler tarafından bir menfaat elde etmek, manipüle etmek veya saldırı düzenleme amacıyla erişilmeye çalışılır. İkinci temel motivasyon enerji, nükleer, sağlık, ulaşım gibi **kritik altyapılar**a yapılan ve bunların aksamasını ya da imha edilmesini hedefleyen saldırılardır. Bir diğer başlık ise özellikle son yıllarda dikkatimizi çeken ve criptojacking diye bilinen **kaynak kullanım saldırısı**dır. Bu saldırıda, kripto para madenciliğinde kullanılmak üzere sizin bilişim kaynaklarınız, sizin bilginiz ve izniniz olmadan kullanılır.
Başka motivasyonlar mevcut olmakla birlikte tüm bunlar arasında en büyük yer kaplayan, en çok zara veren ve en öncelikli olarak korunması gereken başlık «**veri güvenliği tehdidi**»dir.

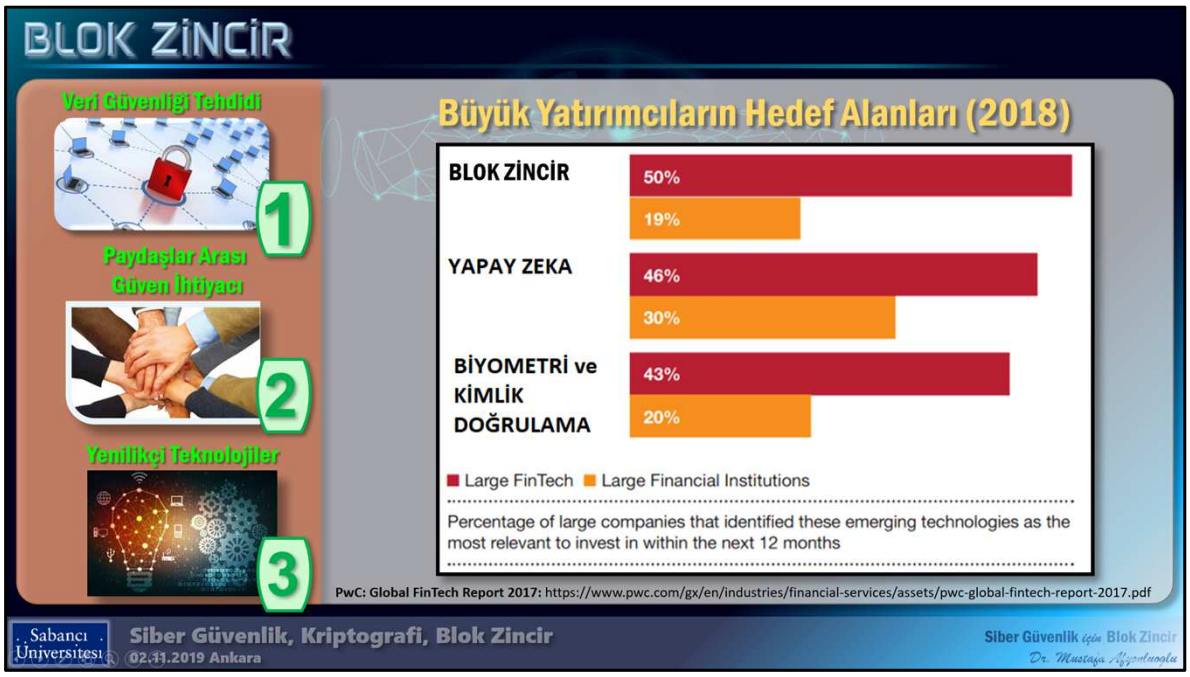
Günümüzde son 5 yıldır tüm ülkelerin dikkatini çeken ve üzerinde yoğun çalışmalar yapılan bir başka başlık **dijital ekonomi**dir. Buradaki yoğun ilginin nereden kaynaklandığını anlamak için, sadece 2 yıl sonrasına ilişkin hacim ekonomik tahminlerine bakmamız yeterlidir. 2021 yılında Çin, dijital ekonomiden **3.8 trilyon dolar** pay beklemektedir. ABD'nin beklentisi **1.2 trilyon $**'dır. Asya pasifik ülkelerinin de bu hacimden hedefledikleri pay aynı seviyededir. Sadece ülkeler değil, birlikler de benzer hedeflere odaklanmış durumdadır. Örneğin bu yıl sonunda nihai hale gelecek olan ve benim ve çekirdek ekibinde yer aldığım dijital ekonomi bölgesel stratejisi kapsamında, Arap Ekonomik Birliği, 2030 yılında **1.5 trilyon dolar** pay hedeflemiştir.

Kuruluş amacı ekonomi olan Avrupa Birliği'nin bile günümüzdeki temel odağı olan **Sayısal Tek Pazar**'daki toplam hacminin sadece **yarım trilyon dolar** olduğu dikkate alınırsa, dijital ekonomideki hacmin büyüklüğü daha iyi anlaşılacaktır. Üstelik sadece bu yılın ocak ayında dijital ekonomi için uluslararası kuruluşlar tarafından raporlanan hacim toplamda 1.15 trilyon $ iken, somut gelişmelere dayanılarak hedef büyültülmüş ve mart ayında 4.5 trilyon $, Temmuz ayında ise 8.1 trilyon dolara yükseltilmiştir. Şahsi kanaatim, özellikle yenilikçi teknolojilerin sektörlerdeki somut çıktılarının ekonomik yansımaları belirginleştikçe bu hacmin daha da artacağı yönündedir.

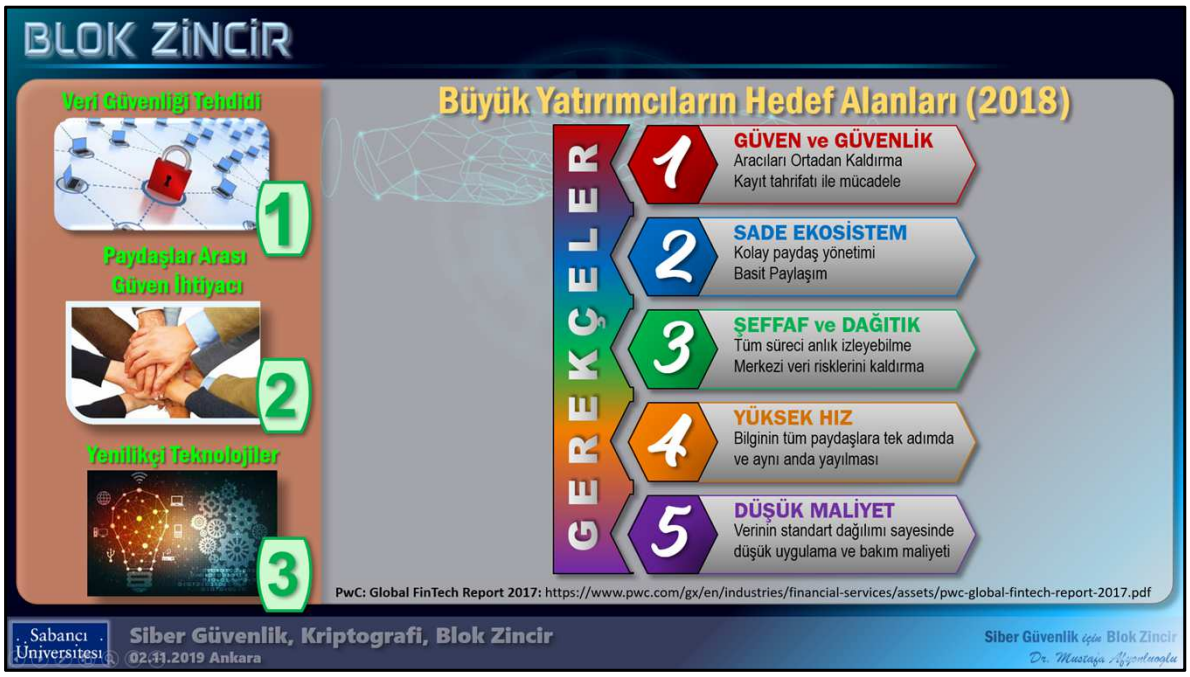
Dijital ekonomi dünyası küresel boyutta olup yatay üretim ve ekonomik yapılanma modeline uygundur, yani tüm ekonomik faaliyetlerde **çok paydaşlılık** söz konusudur. Bu ortamda paydaşların en büyük talebi, **kusursuz güven ortamın**ın oluşturulması ve bu sayede her paydaşın siber problemler yerine kendi asli işine odaklanmasıdır.



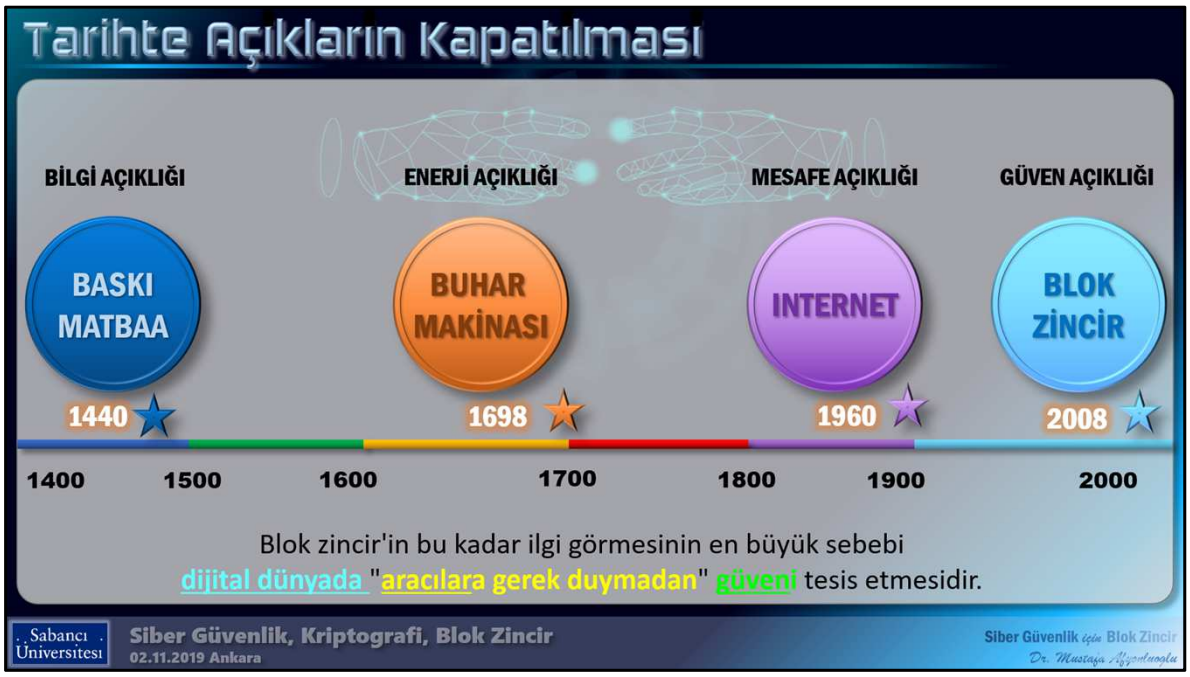
Dijital ekonomide bir diğer dikkat çeken husus, IMF'in «**Dijital Ekonomi Ölçümleme**» raporlarında göze çarpmaktadır. Bu güne kadar bir işletme kurmak için sermaye ve işgücü olmak üzer 2 temel kaynak yeterli iken artık, yenilikçi teknolojilerin kullanımının da neredeyse eşit (%27) oranda önemli olduğu görülmektedir. Dolayısıyla günümüzde başarılı ve sürdürülebilir bir ticari faaliyet için **yenilikçi teknolojiler ve hızlı çözüm oluşturma** ilk plandadır.



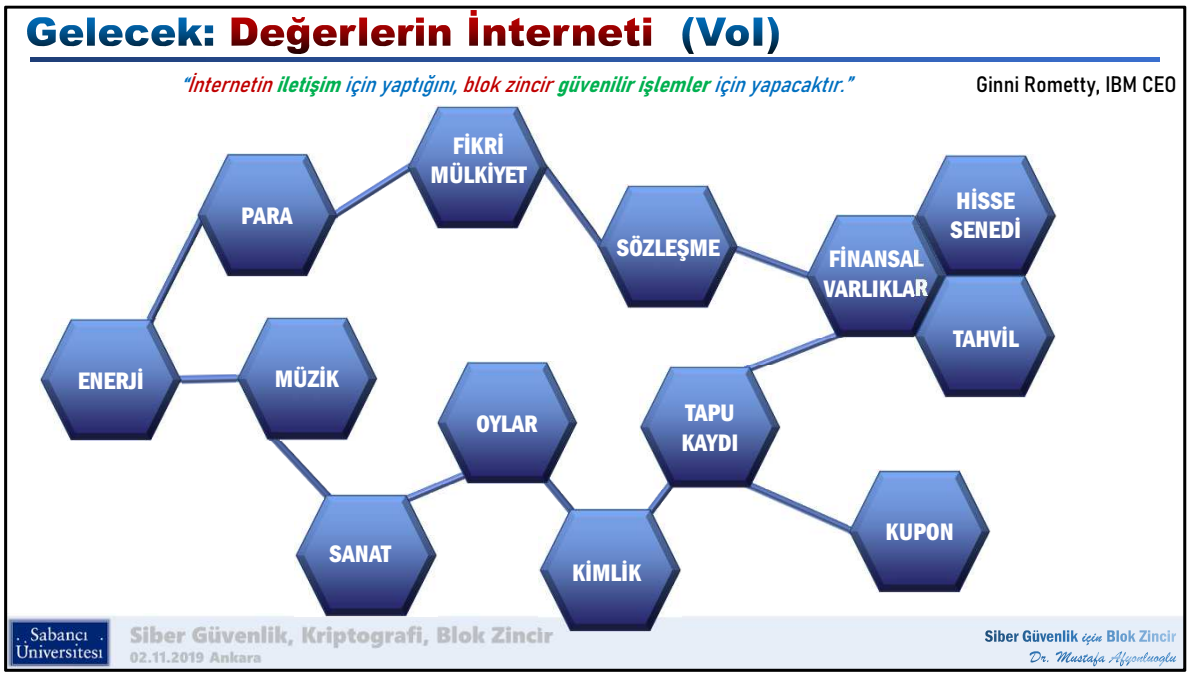
Şu ana kadar tespit ettiğimiz bu üç önemli başlığı (yani veri güvenliğini sağlama ihtiyacı, güven tesis edilmesi ve yenilikçi teknolojilerin esas alınması) masada tutarak PwC'nini geçen yıl yaptığı bir araştırma sonucunu inceleyelim. Bu çalışmada büyük şirketlere hemen şimdi ve yakın gelecekte hangi alanlara yatırım yapmayı planladıkları sorulduğunda, ilk başta **blok zincir** geldiği görülmüştür.



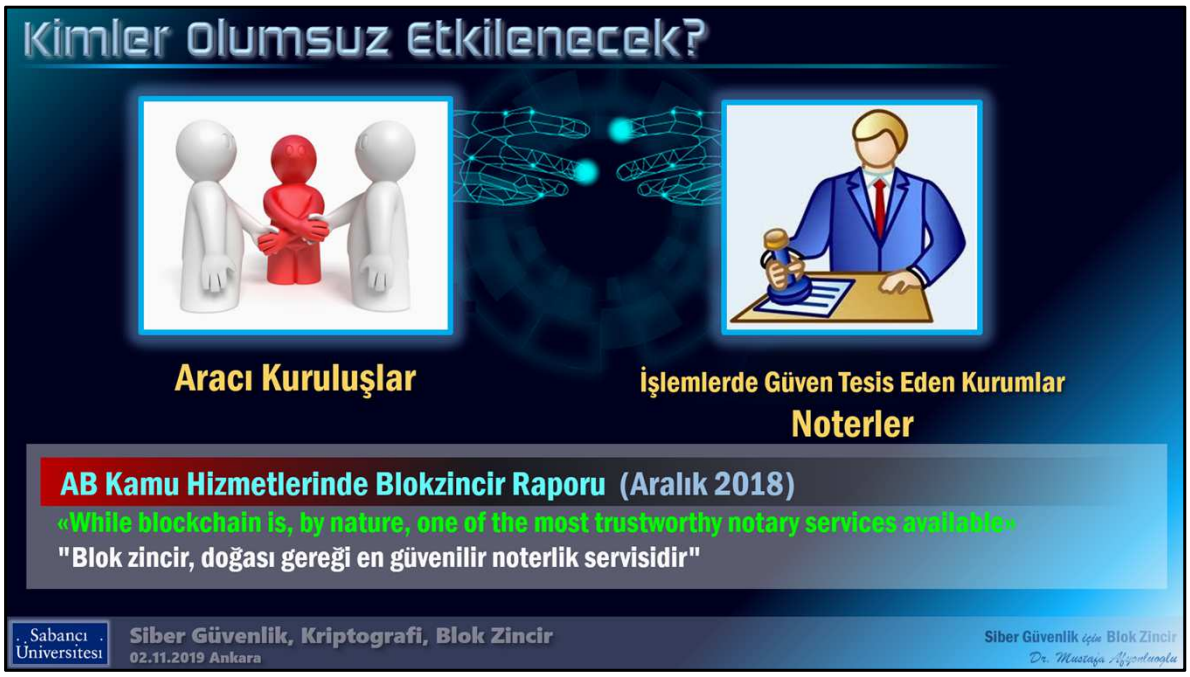
Bu tercihin gerekçeleri 5 başlıkta toplanmıştır. Dikkat ederseniz, ilk başlık güven ve (veri) güvenliğidir. Yani tahrifatların önlenmesi, aracıların ortadan kaldırılması ilk gerekçe (ve en önemli ihtiyaç) olarak sıralanmıştır. Diğer gerekçeler de incelendiğinde kolay paydaş yönetimi, şeffaf olarak tüm süreci izleme ihtiyacı, yüksek hızda işlem, düşük maliyet ve kolay öğrenme süreci, blok zinciri doğrudan tarif ederken, ayrıca bizim tespit ettiğimiz 3 temel ihtiyacı da birebir karşılamaktadır. Yani, **blok zincir, veri güvenliğini sağlama, dijital dünyada güven tesis etme imkanını masaya koyan bir yenilikçi teknolojidir.**



Nitekim tarihteki açıkların kapatılmasına bakıldığında bazı önemli keşiflerin bu açıklığı kapattığı ve yeni bir çağı başlattığı görülür;
Örneğin 1400'lü yılların ortalarında matbaanın keşfi ile bilgi açıklığının kapatıldığı görülmüş, 1700'lü yıllara doğru buhar makinasının keşfi enerji açığını kapatmış ve sanayi devrimi başlamış, ilk kez 1960'da ortaya çıkan ve 1990'lı yıllarda vatandaşa kadar ulaşan internet ile birlikte uzak mesafeler yakın olmuş, iletişim açıkları kapanmıştır. 2000'li yılarda ise, ilk kez 2008'de gündeme gelen ve peşindeki yıl bitcoin isimli finansal alandaki ilk uygulama ile dikkatleri üzerine çeken blok zincirin, dijital dünyada güven açığını kapattığına inanılmaktadır.
Blok zincir'in bu kadar ilgi görmesinin en büyük sebebi **dijital dünyada "aracılara gerek duymadan" güveni** tesis etmesidir.



Nitekim, IBM CEO'su Ginni Rometty, «*nternetin iletişim için yaptığını, blok zincir güvenilir işlemler için yapacaktır.*» diyerek bu inanca vurgu yapmıştır. Günümüzde artık elimizdeki her türlü önem verdiğimiz değer dijital ortama taşınmaktadır. Para, müzik, eserlerimiz, enerji, kullandığımız oylar, fikri mülkiyet haklarımız, sözleşmeler, devletin tapu, kimlik, taşınır ve taşınmaz varlıkları gibi temel kayıtları, finansal varlıklar ve diğer bir çok şey ile birlikte aslında gelecek, «**Değerlerin İnterneti**»ndedir. Dolayısıyla bu değerleri korumak ve yönetmek günümüzün en önemli gereksinimlerinden birisidir. Blok zincir, ilk uygulaması olması sebebiyle her ne kadar finans dünyasına katkı sağlamaya odaklanmış gibi algılansa da, aslında her türlü dijital değeri muhafaza eden, bütünlüğünü koruyan yapısı ile değerler internetinin baş oyuncusudur.



Blok zincirin yaygınlaşmasından en çok etkilenecek olanlar şüphesiz ki **aracı kuruluş**lardır. Akla gelen bir diğer seçenek ise, belgelerde güveni tesis eden **Noterler** olabilir mi?

Bunu için, AB tarafından kurulan «Blok Zincir Gözlemevi ve Forumu»nun 10 ay önce, Aralık 2018'de yayımladığı «**AB Kamu Hizmetlerinde Blok Zincir Raporu**»na bakmak gerekir. Bu raporda çok ilgi çekici bir cümle vardır: «

Bu raporun görüşünün teorik kalmadığına, raporun yayımlanmasından sadece 4 ay sonra Lüxemburg'da şahit oluyoruz. Mart 2019'da Lüksemburg yönetimi, Avrupa'nın blok zincir tabanlı ilk Noterlik sistemini hizmete açmıştır. Benzer yapılar son 2-3 yıldır ticari işletmeler tarafından kullanıma açılmaya başlanmış olsa da, resmi bir insiyatifin, arkasında AB raporu da olacak şekilde ilk adımı atması bu alanda çok değerli bir kilometre taşıdır.

Blok zincirin hangi sektörlere hizmet edeceğini burada eksiksiz olarak saymak mümkün değil. Ancak şunu özellikle belirtmek isterim:

Her alanda blok zincir kullanılabilir mi? Teorik olarak EVET ancak pratikte bazı alanlarda blok zincir kullanmak verimli ve pratik olmayacaktır. Alanlar belirlenirken temel kriterlere uygun işleyiş olup olmadığı önemlidir. Temel kriterler (hatırlatacak olursak), çok paydaşlılık, şeffaflık gereksinimi, tüm paydaşların verilere anında erişim ihtiyacı gibi başlıklardır.

Bununla birlikte blok zincirin önemli fayda sağlayacağı alanların başında hiç şüphesiz hemen tahmin edebileceğiniz gibi finans gelmektedir. Buna ilaveten, e-ticaret, lojistik, sağlık, Enerji, Üretim, Kamu Temel Kayıtları, Dijital Belge Onaylama, Dijital Kimlik Yönetimi, e-Devlet Hizmetleri, e-Seçim, Diploma Servisleri, Sınır ötesi Hizmetler, Vergilendirme gibi alanlar blok zincir için verimli uygulama alanları arasında yer almaktadır.

O zaman kısaca basit şekilde blok zincirin nasıl işlediğine bakalım. Aslında blok zincir ve domino oyunu, **zincir yapıları** sebebiyle birbirlerine çok benzerler.

Domino, «zincir» mantıklı ilerleyen bir oyun ve zincirin kuralı «bir taşın yanına, ancak o taraftaki numara ile başlayan bir başka taş eklenebilir»
Domino oyununun en güzel tarafı bir kez hamle yaptıktan sonra geriye dönüp hile yapamazsınız. Çünkü:

- «bağlı zincir» mantığıyla çalışır . (Bütünlük)
- yapılan tüm hamleler herkese AÇIKTIR (Şeffaflık)

Oyunu herkes oynayabilir çünkü:

- Kuralları basittir.
- Oyun formatı sadedir.
- 1-6 arasındaki sayıları bilmeniz yeterlidir.

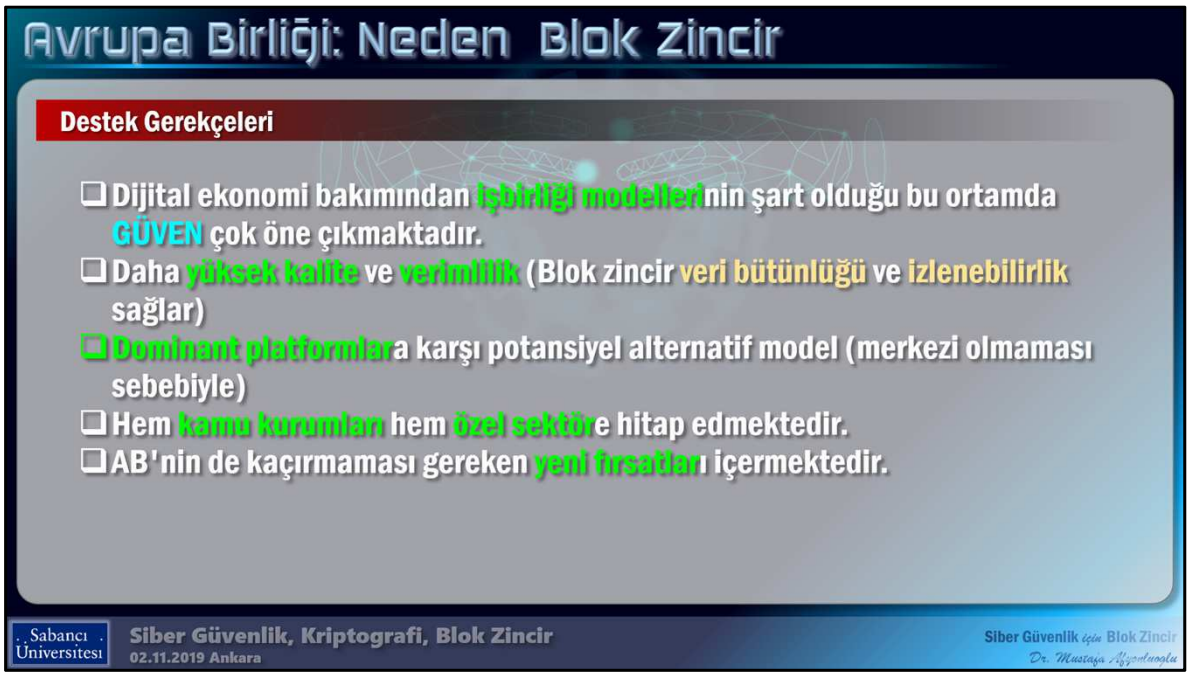
Bu sebeple bir kullanım kılavuzu ya da bilen birisinin yardımı gerekmez (Aracılara ihtiyaç bulunmaması)

Dominoda, eğer zincirin ortasından bir taş eksilirse hemen fark edilir çünkü birbirini izleyen sayılardaki düzen bozulur. Yani taş çalamazsınız. **(Kayıt Silinemez)**

Ya da eğer zincirdeki bir taşı sonradan değiştirmeye kalkarsanız yine hemen fark edilir. **(Kayıt Değiştirilemez)**

Aynı şekilde araya taş da ekleyemezsiniz **(Geçmişe Kayıt Eklenemez)** çünkü taşı koyacak fiziki yer yoktur. Yeni bir taş sadece zincirin son ucuna ve kurallara uygun bir rakama sahip ise eklenebilir **(Uzlaşma Prensibi)**. Görüldüğü gibi süreç hem şeffaftır hem de o kadar basittir ki bir kullanım kılavuzuna ya da bu işi bilen birisinin yardımına gerek yoktur. Yani **aracılar** zincir sisteminde kendilerine yer bulamazlar.

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)



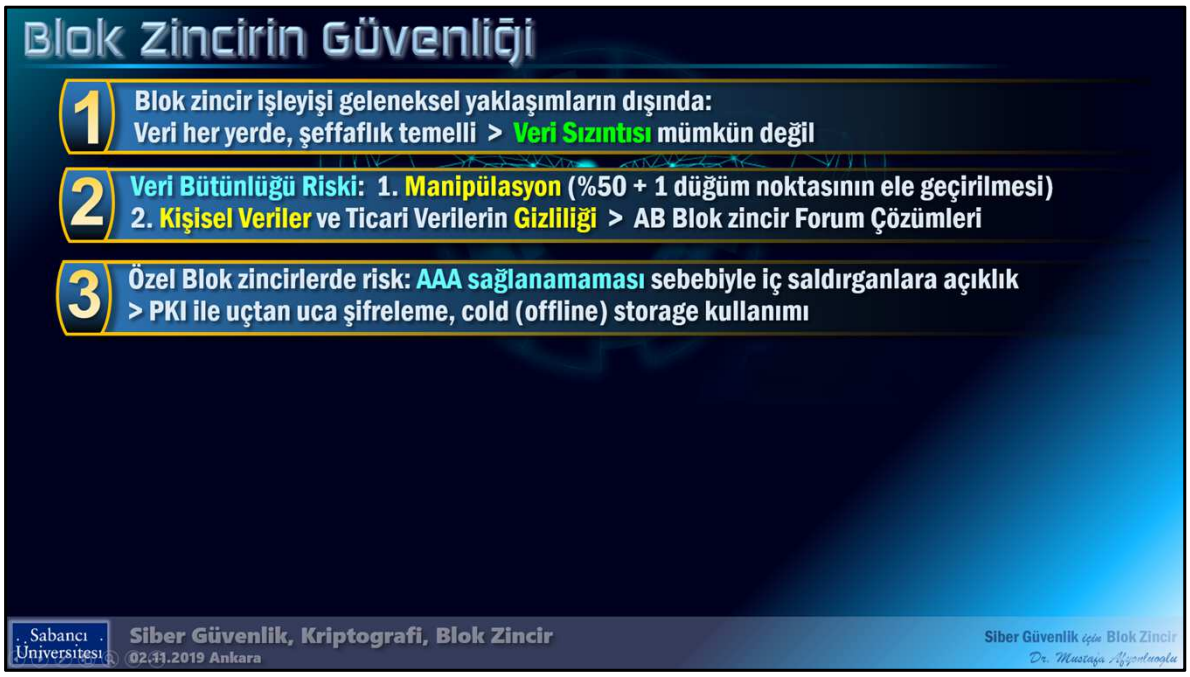
(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

AB, blok zincire verdiği öneme ilaveten, bu alanda, bir çok ülkeden çok daha hızlı yol alabilmiştir. Geçtiğimiz 3 yıla baktığımızda 2016 yılının «**Eğitim Yılı**» ilan edildiğini görüyoruz. AB, 2016 boyunca ekosistemi oluşturmaya çalışmış ve blok zincirin farklı sektörlerdeki etkilerini tespit etmiştir. 2017 yılı, blok zincir tabanlı çözümlerin test edilerek sonuçlarının izlendiği «**Kavram İspat Yılı**» olmuştur. Geçen yıl ise, blok zincirin uygulanabileceği **büyük ölçekli projeler** belirlenmiş ve duyurular yapılarak projeler başlatılmıştır. AB'nin 2019 yılı hedefi ise, büyük ölçekli projelerin en az 10 tanesini tamamlayarak hayata geçirmektir.

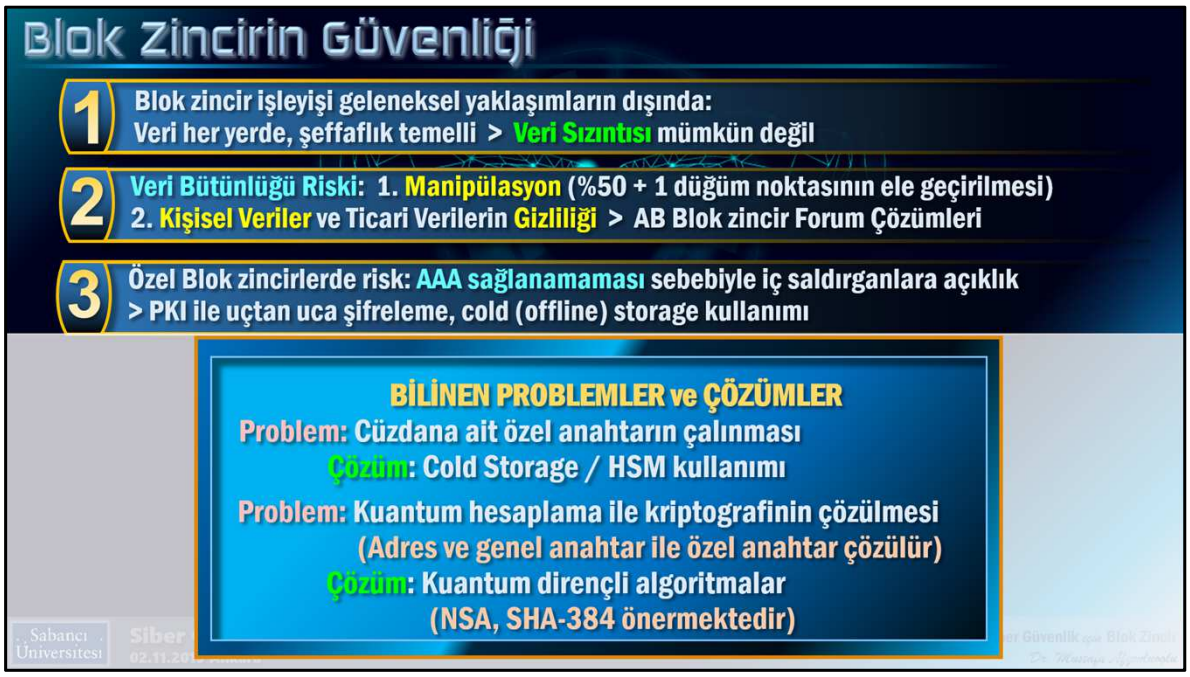
Bununla birlikte bu 3 yıl boyunca yapılan çalışmalar sadece teknik ilerlemeden ibaret değildir. Ayrıca blok zincir konusunda bölgesel ve ulusal politikaların oluşturulması, başta GDPR olmak üzere pratik uyum problemlerinin çözümünün ortaya konulması, hukuki uyumlaştırma modellerinin sağlanması, öncelikli uygulama alanlarının belirlenmesi gibi bir çok başlık neticeye kavuşturulmuştur.

AB'de bu süreçte sonuçlandırılan önemli bir ilerleme de, büyük blok zincirlerdeki **performans** ve **hacim** zaafiyetlerine çözüm bulmak olmuştur. Blok zincirin bir ülkenin çok adetli işlemli yapılarında (örneğin günde üç milyon işlem yapan bir kurum için) kullanılmasından ortaya çıkacak performans ve hızla büyüyen zincir hacmine çare bulmak için özellikle sektörel blok zincirlerin oluşturulması ve bunların birbirleri ile entegrasyonu sayesinde bir bütünmüş gibi çalışmalarını sağlayan modeller oluşturulmuştur.

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)



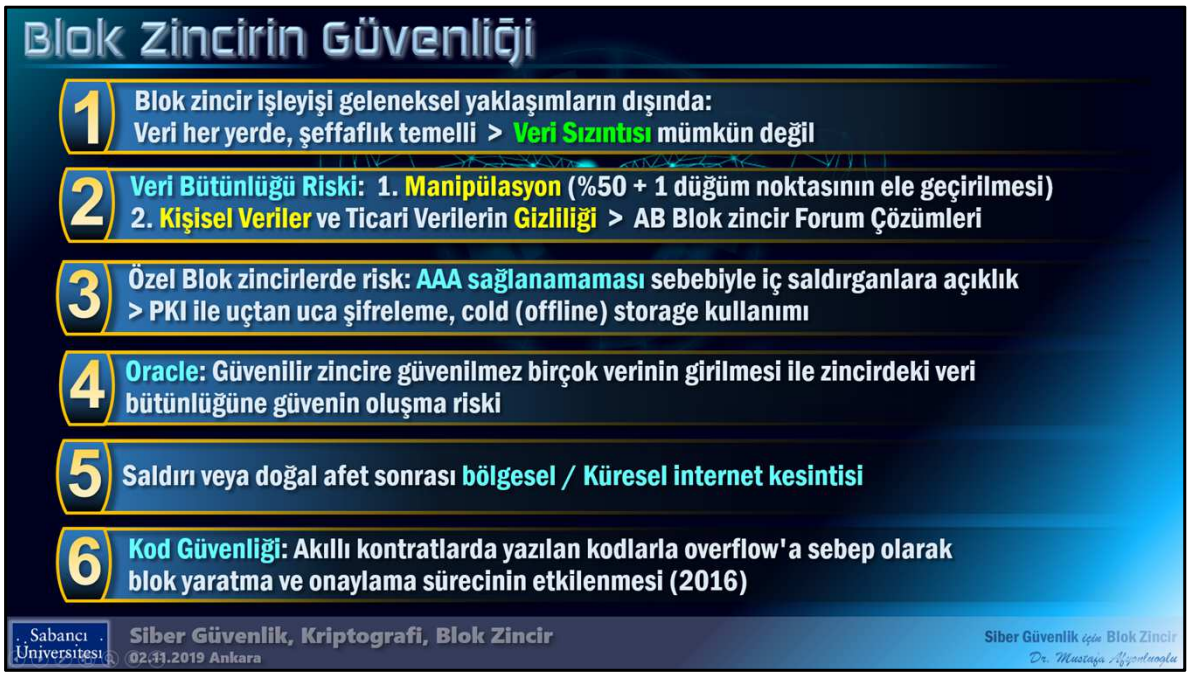
(Bu sayfanın açıklaması, sunum metninde yer almaktadır)



(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

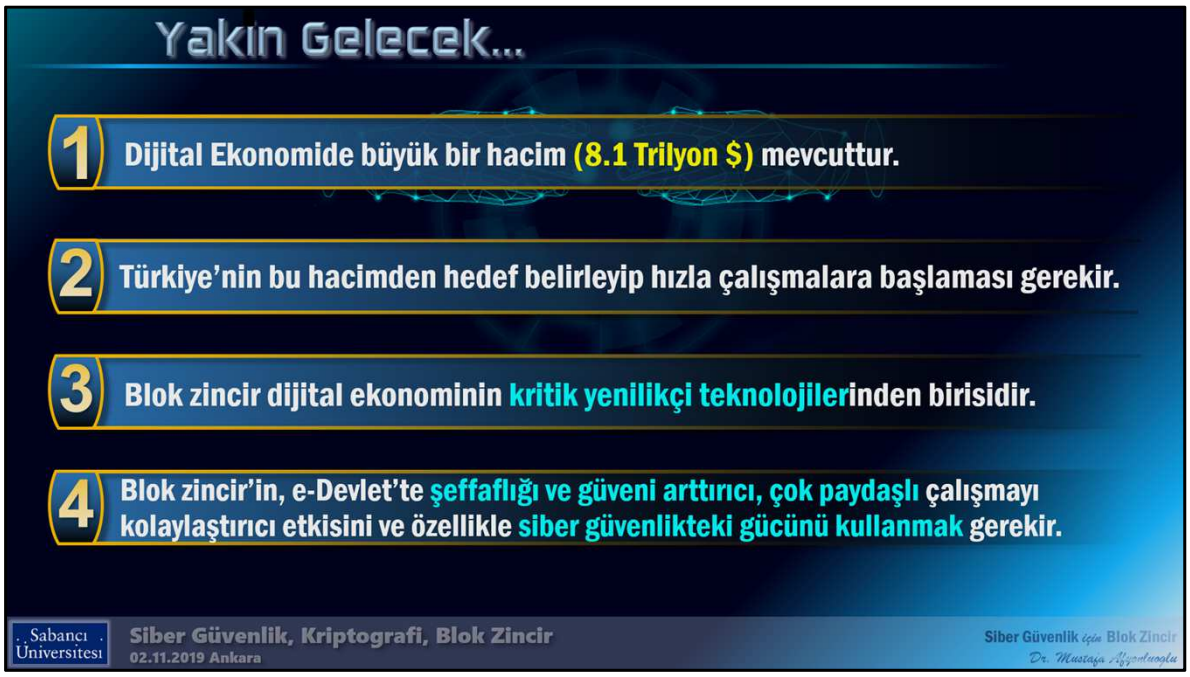
İlgili Haber Adresi:
https://www.wired.com/story/googles-quantum-supremacy-isnt-end-encryption/?mbid=social_twitter&utm_brand=wired&utm_campaign=wired&utm_medium=social&utm_social-type=owned&utm_source=twitter



(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)



(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

Blok zincir dünyası için sadece burada paylaşılan başlıklarla yetinmeyin daha çok incelemek isterseniz, düzenli olarak güncellenen ve bugün (Ekim 2019) itibarı ile 50'den fazla raporu içeren «**Blok Zincir Uluslararası Rapor Kütüphanesi**» ni ziyaret edebilirsiniz. Bu site (**http://afyonluoglu.org**) ayrıca blok zincirin tabanını oluşturan ya da doğrudan birebir ilişkili olan:

- e-Devlet
- Siber Güvenlik
- Kişisel Veriler
- Bilişim Hukuk

başlıklarında, günlük olarak güncellenen 6.000'den fazla ulusal ve uluslararası raporu ücretsiz olarak sunmaktadır. Blok zincir dahil olmak üzere sitede yayımlanan her başlığa ilişkin soru, talep ve önerilerinizi «**afyonluoglu@gmail.com**» adresine gönderebilirsiniz.

Zaman ayırarak bu etkinliğe katıldığınız ve beni dinlediğiniz için sizlere ve bu değerli davet için Sabancı Üniversitesi'ne bir kez daha teşekkür eder, saygılar sunarım.

Sunum Tarihi : 02.Ekim.2018
Hazırlayan : Dr. Mustafa AFYONLUOĞLU / Keynote Speaker
Etkinlik : Sabancı Üniversitesi «Siber Güvenlik, Kriptografi, Blok Zincir» Etkinliği
Erişim : http://afyonluoglu.org → KAYNAKLAR → SUNUMLAR
Yayım / Alıntı Şartı : Sunumdan alıntı yapılması için açık referans (Eser Sahibinin Adı Soyadı, Yayımlandığı Web Sayfası Adresi) gösterilmesi zorunludur.
NOT : Bu sunumda herhangi bir kurum temsil edilmemektedir. Tüm görüş ve değerlendirmeler sunumu yapan kişinin uzmanlık değerlendirmeleridir.