

Sabancı Üniversitesi

SİBER GÜVENLİK İÇİN BLOK ZİNCİR

Siber Güvenlik, Kriptografi, Blok Zincir

Dr. MUSTAFA AFYONLUOĞLU
Siber Güvenlik, E-Yönetişim ve Dijital Ekonomi Kademeli Uzmanı

2 Ekim 2019
Ankara

Sunum Telif Hakkı: © 2019 Dr. Mustafa AFYONLUOĞLU (afyonluoglu@gmail.com)
Sunumdan alıntı yapılması halinde sunumun başlığı, sunumu hazırlayan ve sunumun yayımlandığı web adresinin referans gösterilmesi zorunludur.

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.

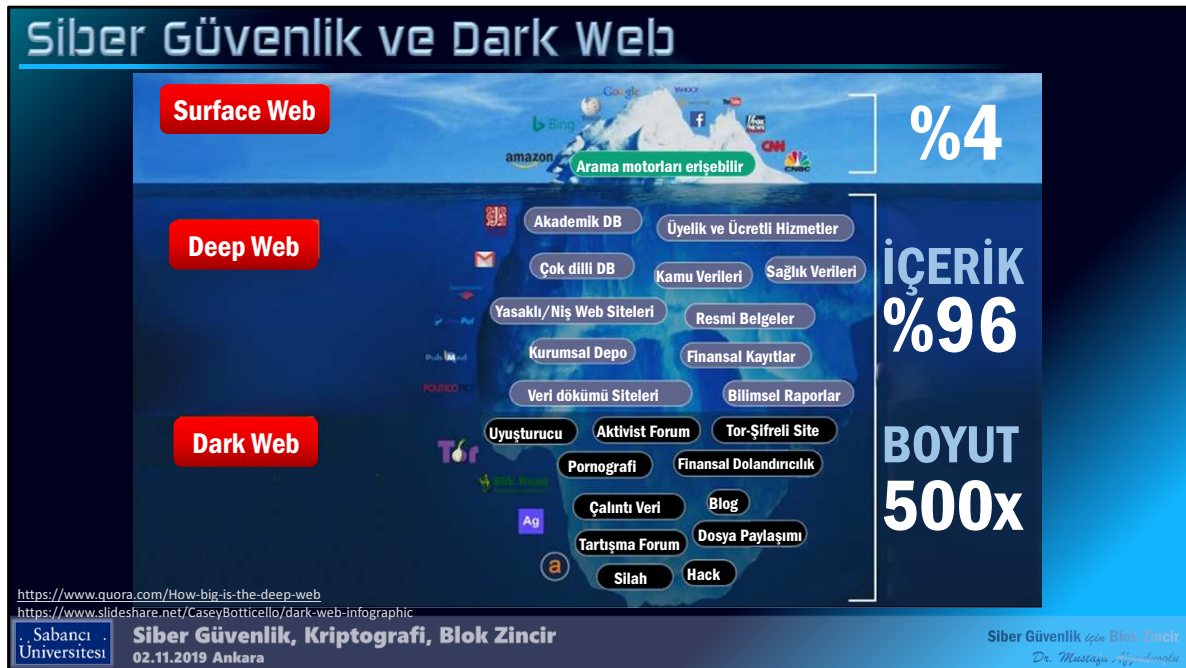
Blokszincir, günümüzde ülkelere önemli fırsatlar vadeden yeni bir teknoloji, siber güvenlik ise dijital hayatımızın vazgeçilmez bir parçası...

Siber güvenlik için blokszincir 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 içtenlikle teşekkür etmek istiyorum.

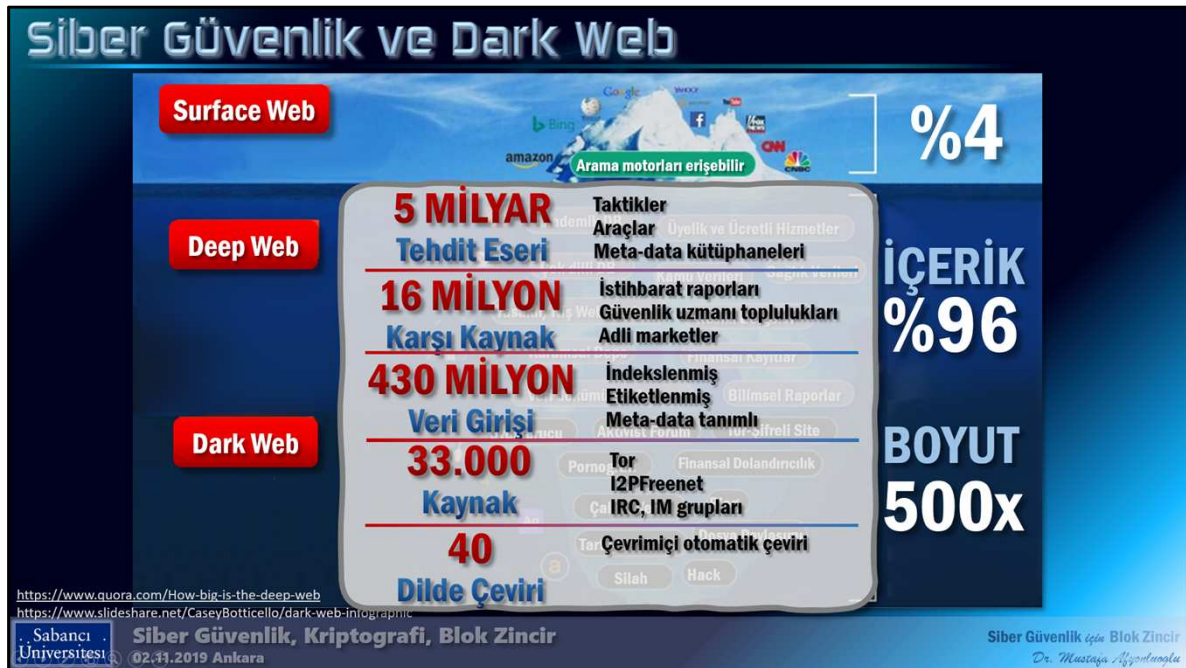
- TEKNİK VERİLER -

Sunum Dosyası Hazırlanma Ortamı:

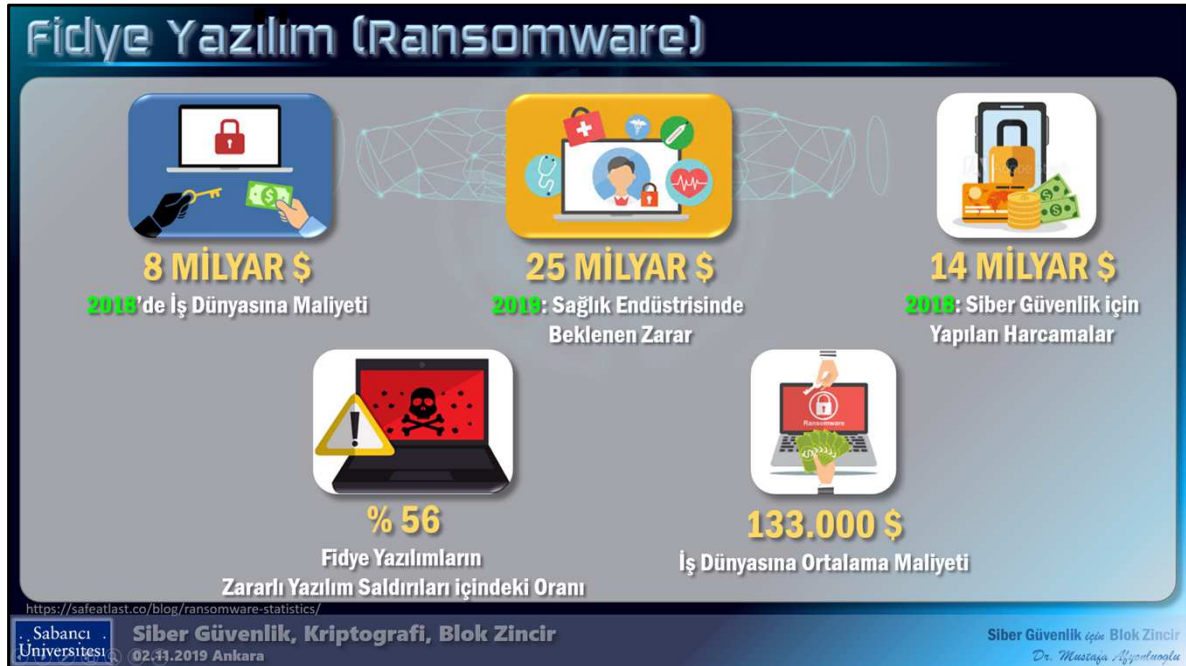
Microsoft Office 365 ProPlus, Microsoft Powerpoint 1908 (Build 1929.20300)



Siber güvenlik dediğimizde aklıma gelen terimlerden birisi karanlık web. Biliyorsunuz, arama motorlarıyla bizim erişebildiğimiz internet kaynakları (yüzeysel web) bugünkü web dünyasının sadece %4'üdür. Geriye kalan %96'lık kısım ise derin web ve karanlık web olarak adlandırılıyor ve yaklaşık boyutunun, yüzeysel 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, birçok 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 ortalama 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 altyapılara** 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 saldırısıdır**. 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 ekonomidir**. 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 \$**'dir. 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 alınır, 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 büyütülmüş 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 ve Güven Gereksinimi

Veri Güvenliği Tehdidini



1

Paydaşlar Arası Güven İhtiyacı

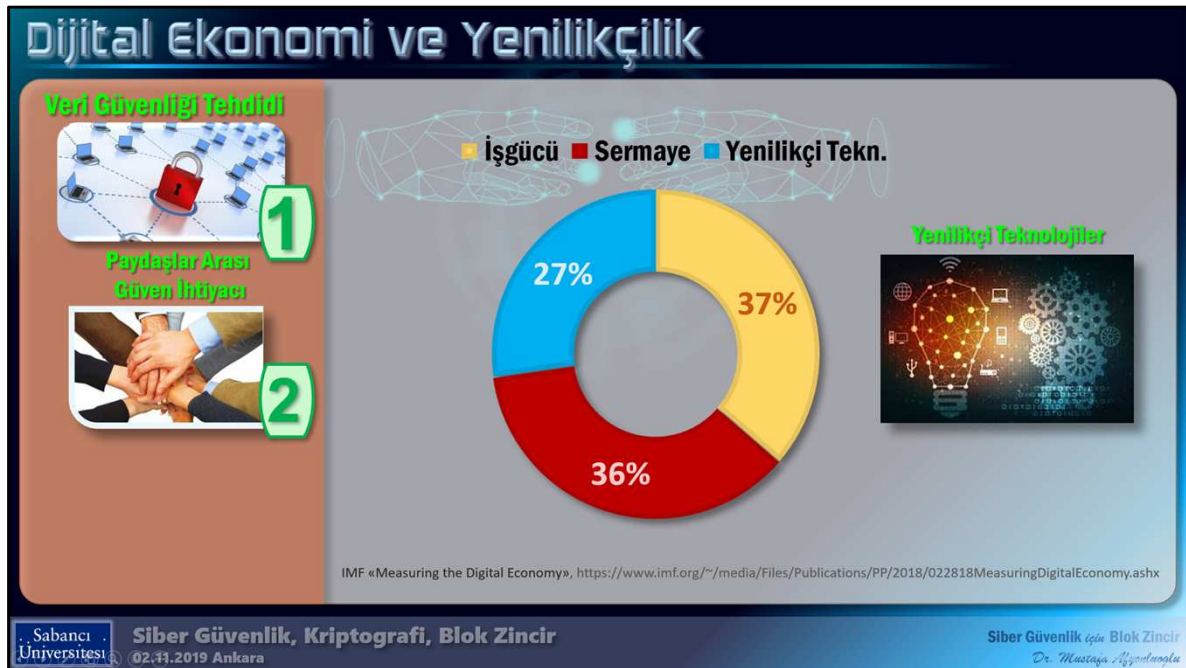


ARACILARIN KALDIRILMASI

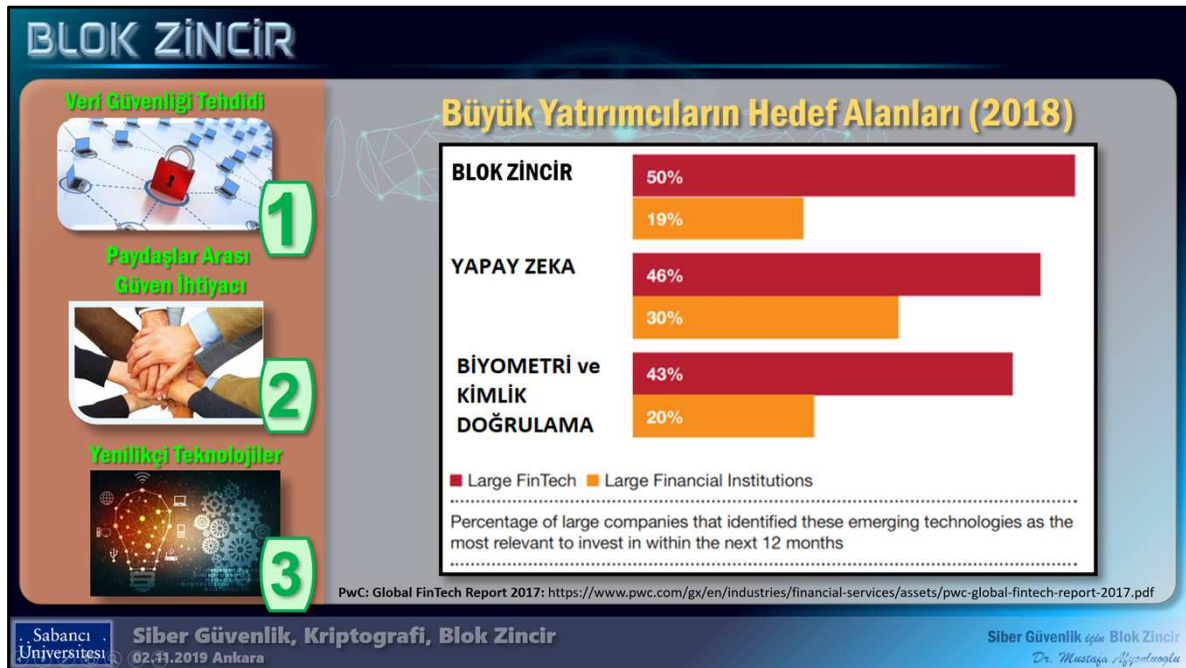
Sabancı Üniversitesi | Siber Güvenlik, Kriptografi, Blok Zincir | 02.11.2019 Ankara

Siber Güvenlik için Blok Zincir
Dr. Mustafa Afyonluoğlu

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 ortamının** oluşturulması ve bu sayede her paydaşın siber problemler yerine kendi asli işine odaklanmasıdır.




Dijital ekonomide bir diğer dikkat çeken husus, IMF'in «**Dijital Ekonomi Ölçümleri**» raporlarında göze çarpmaktadır. Bu güne kadar bir işletme kurmak için sermaye ve işgücü olmak üzere 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.


BLOK ZİNCİR

Veri Güvenliği Tehditli




1

Paydaşlar Arası Güven İhtiyacı



2

Yenilikçi Teknolojiler



3

Büyük Yatırımcıların Hedef Alanları (2018)

GEREKÇELER

1

GÜVEN ve GÜVENLİK

Aracıları Ortadan Kaldırma
Kayıt tahrifatı ile mücadele

2

SADE EKOSİSTEM

Kolay paydaş yönetimi
Basit Paylaşım

3

ŞEFFAF ve DAĞITIK

Tüm süreci anlık izleyebilme
Merkezi veri risklerini kaldırma

4

YÜKSEK HIZ


Bilginin tüm paydaşlara tek adımda ve aynı anda yayılması

5

DÜŞÜK MALİYET

Verinin standart dağılımı sayesinde düşük uygulama ve bakım maliyeti

PwC: Global FinTech Report 2017: <https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2017.pdf>



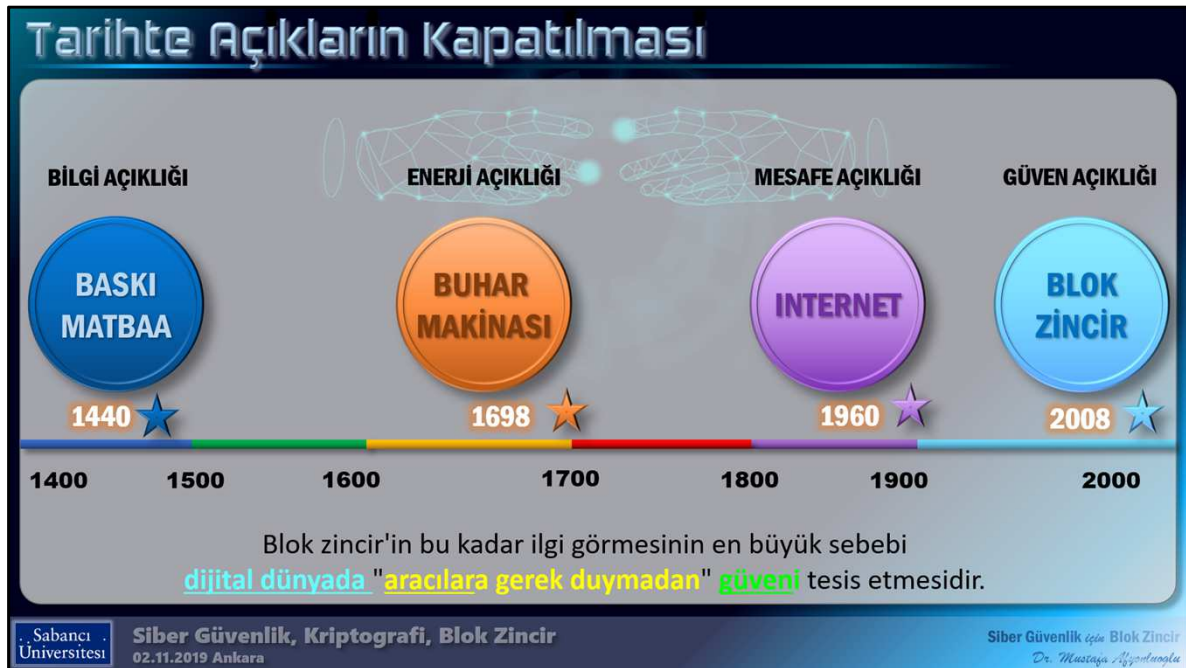
Siber Güvenlik, Kriptografi, Blok Zincir
02.11.2019 Ankara

Siber Güvenlik için Blok Zincir
Dr. Mustafa Afyonluoğlu

Bu tercihin gerekçeleri 5 başlıkta toplanmıştır. Dikkat ederseniz, ilk başlık güven ve (veri) güvenliğidir. Yani tahrifatların önlenmesi, araçların 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.**

"Siber Güvenlik İçin Blok Zincir", Dr. Mustafa Afyonluoğlu,
(<http://afyonluoglu.org>)

10



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 açıklığını kapatmış ve sanayi devrimi başlamış, ilk kez 1960'da ortaya çıkan ve 1990'lı yıllarda vatandaşlara kadar ulaşan internet ile birlikte uzak mesafeler yakın olmuş, iletişim açıkları kapanmıştır. 2000'li yıllarda 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 açıklığını kapattığına inanılmaktadır.

Blok zincir'in bu kadar ilgi görmesinin en büyük sebebi dijital dünyada "araçlara gerek duymadan" güveni tesis etmesidir.

Gelecek: Değerlerin İnterneti (Vol)


"İnternetin iletişim için yaptığını, blok zincir güvenilir işlemler için yapacaktır."

Ginni Rometty, IBM CEO



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.

Kimler Olumsuz Etkilenecek?



Aracı Kuruluşlar



İşlemlerde Güven Tesis Eden Kurumlar
Noterler

AB Kamu Hizmetlerinde Blokzincir Raporu (Aralık 2018)
 «While blockchain is, by nature, one of the most trustworthy notary services available»
 "Blok zincir, doğası gereği en güvenilir noterlik servisedir"



Siber Güvenlik, Kriptografi, Blok Zincir
02.11.2019 Ankara

Siber Güvenlik için Blok Zincir
Dr. Mustafa Afyonluoğlu

Blok zincirin yaygınlaşmasından en çok etkilenecek olanlar şüphesiz ki **aracı kuruluşlar**dır. 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: «

Kamuda ilk Örnek Uygulamalar



Noterler

Mart 2019: Lüksemburg Yönetimi, BLOKZİNCİR tabanlı NOTERLİK sistemini hizmete açtı
 «Avrupanın Blokzincir tabanlı, güvenliği ve işbirliği optimize edilmiş ve düşük maliyetli ilk NOTERLİK sistemi»
 «Sistem, zaman içerisindeki bütünlüğü de koruyacak şekilde her türlü belgeyi kayıt altına alabiliyor»

Bu raporun görüşünün teorik kalmadığına, raporun yayımlanmasından sadece 4 ay sonra Lüksemburg'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 inisiyatifin, arkasında AB raporu da olacak şekilde ilk adımı atması bu alanda çok değerli bir kilometre taşıdır.



Blok zincirin hangi sektörler 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.

AYHAN

ZEYNEP

Blok Zincir İşleyişi

Sabancı Üniversitesi Siber Güvenlik, Kriptografi, Blok Zincir
02.11.2019 Ankara

venlik için Blok Zincir
Dr. Mustafa Afyonluoğlu

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

Domino ve Blok Zincir



DOMİNO bir ZİNCİR oyundur

- Hamle yaptıktan sonra geriye dönüp **HİLE** yapamazsınız.
- **SİLİNEZ** veya **DEĞİŞTİREMEZ**.
- Tüm adımlar **HERKESE AÇIKTIR**.
- **KAZANILIR** kaydedilebilir.

Sabancı Üniversitesi | Siber Güvenlik, Kriptografi, Blok Zincir | 02.11.2019 Ankara | anlık için Blok Zincir | Mustafa Afyonluoğlu

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:

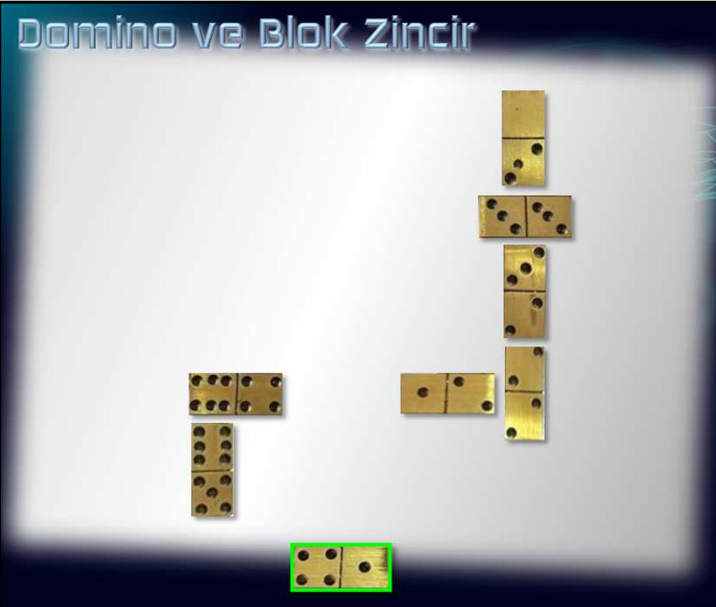
- «bağlı zincir» mantığıyla çalışır . (Bütünlük)
- yapılan tüm hamleler herkese AÇIKTIR (Şeffaflık)

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)

Domino ve Blok Zincir



DOMİNO bir ZİNCİR oyundur

- Hamle yaptıktan sonra geriye dönüp **HİLE** yapamazsınız.
- Tüm adımlar **HERKESE AÇIKTIR**.
- **İZLENEBİLİR**, kaydedilebilir.

Sabancı Üniversitesi | Siber Güvenlik, Kriptografi, Blok Zincir | 02.11.2019 Ankara

anlık için Blok Zincir
Mustafa Afyonluoğlu

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

Domino ve Blok Zincir



DOMİNO bir ZİNCİR oyunudur

- Hamle yaptıktan sonra geriye dönüp **HİLE** yapamazsınız.
- **SİLİNEMEZ** veya **DEĞİŞTİRİLEMEZ**
- Tüm adımlar **HERKESE AÇIKTIR**.
- **ZLENEBİLİR**, kaydedilebilir.
- **HERKES OYNAYABİLİR**, çünkü:
 - Kuralları **BASİT**
 - Oyun formatı **SADE**
 - 1-6 arasındaki sayıları bilmek **YETERLİ**
 - Oyunu öğretecek **ARACILAR**'a gerek yok

Sabancı Üniversitesi | Siber Güvenlik, Kriptografi, Blok Zincir | 02.11.2019 Ankara

anlık için Blok Zincir
Mustafa Afyonluoğlu

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 taş koyacak fiziki yer yoktur. Yeni bir taş sadece zincirin son ucuna ve kurallara uygun bir rakama sahip ise eklenebilir (**Uzlaşma Prensipleri**). Görüldüğü gibi süreç hem şeffaftır hem de o kadar basittir ki bir kullanım kılavuzuna ya da bu işi bilen birisinin yardımına gerek yoktur. Yani **araçlar** zincir sisteminde kendilerine yer bulamazlar.

Avrupa Birliđi ve Blok Zincir

Destek Gerekçeleri / Blok Zincir Gözlemevi ve Forumu

- Küreselleşen **FinTech**
- Markete giren Büyük platformlar (**Platform Ekonomisi**)
- AB Tek Pazar hacmi **0,5 Trilyon \$**, Dijital Ekonomi Pazarı: **8.1 Trilyon \$**
- Dijitalleşen **Bankalar**
- FinTech ile **düzenleyiciler denetleyici kurumlar** arasında artan diyalog
- AB FinTech Eylem Planı 2018:**
 - "yenilikçi iş dünyasını güçlendirmek ve yen teknolojileri desteklemek için, ve siber güvenliği sıkılaştırmak için blok zincir kullanımı"

Zayıf sektörlerde dijitalleşme iki katına çıkarsa 2025'de GDP'de **2.5 Trilyon \$** artış olacağını tahminliyor. Bu sebeple KOBİ'ler 150.000 Euro destekleniyor.

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

Avrupa Birliđi: Neden Blok Zincir

Destek Gerekçeleri

- Dijital ekonomi bakımından **işbirliđi modelleri** nin şart olduđu bu ortamda **GÜVEN** çok öne çıkmaktadır.
- Daha **yüksek kalite** ve **verimlilik** (Blok zincir **veri bütünlüğü** ve **izlenebilirlik** sağlar)
- Dominant platformlara** karşı potansiyel alternatif model (merkezi olmaması sebebiyle)
- Hem **kamu kurumları** hem **özel sektöre** hitap edmektedir.
- AB'nin de kaçırmaması gereken **yeni fırsatları** içermektedir.

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

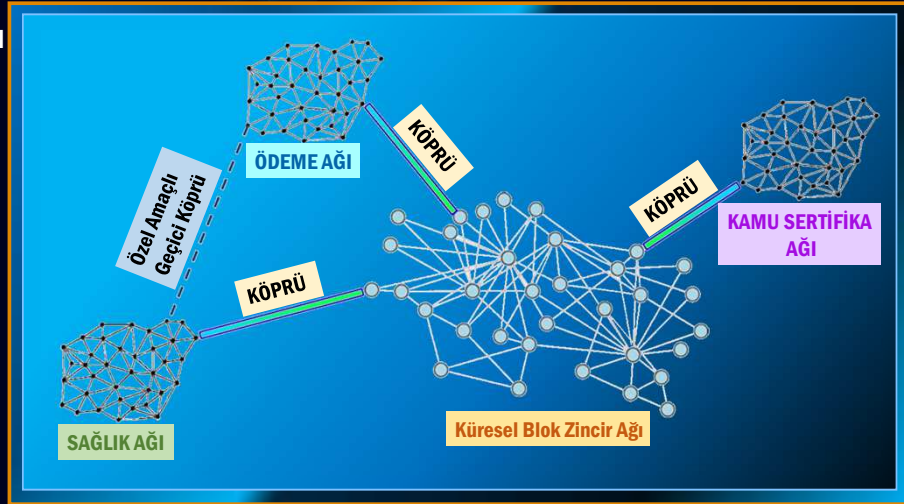


AB, blok zincire verdiği öneme ilaveten, bu alanda, bir çok ülkeden çok daha hızlı yol alabilmiştir. Geçtiğimiz 3 yıla baktığımızda 2016 yılının «**Eğitim Yılı**» ilan edildiğini görüyoruz. AB, 2016 boyunca ekosistemi oluşturmaya çalışmış ve blok zincirin farklı sektörlerdeki etkilerini tespit etmiştir. 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 Blok Zincir Gözlemevi ve Forumu

AYRIK KAMU
BLOKZİNCİR AĞLARININ
ENTEGRASYON MODELİ



Sabancı
Universitesi

Siber Güvenlik, Kriptografi, Blok Zincir
02.11.2019 Ankara

Siber Güvenlik için Blok Zincir
Dr. Mustafa Afyonluoğlu

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 işlemleri 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.

AB'de Blok Zincir Öncelikli Uygulama Alanları

2 YIL'da 660+ proje, workshop, rapor ve eğitim materyali oluşturulmuştur.

EBSI : European Blockchain Service Infrastructure

- 1. Noterlik:** Denetim amaçlı belgelerin onaylanması
- 2. Diploma** sertifikasyonları doğrulama
- 3. eSSIF : European Self-Sovereign Identity Framework – Avrupa Özerk Kimlik tanımlama (SSI) Çerçevesi**
Merkezi idareye gerek duymadan vatandaşların kendi dijital kimliklerini yaratma ve kontrol etmeleri
GDPR uyumluluk dağılama hedefi, mahremiyet sağlama
Blok zincir içim kimlik tanımlama katmanı'nın oluşturulması
- 4. Vergilendirme:** Gümrük ve vergi otoriteleri arasında güvenli şekilde veri paylaşımı
(Trusted Data Sharing)

Sabancı Üniversitesi | Siber Güvenlik, Kriptografi, Blok Zincir | 02.11.2019 Ankara | Siber Güvenlik için Blok Zincir | Dr. Mustafa Afyonluoğlu

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

Blok Zincirin Güvenliđi

- 1** Blok zincir işleyişı geleneksel yaklaşımların dışında:
Veri her yerde, şeffaflık temelli > **Veri Sızıntısı** mümkün değil
- 2** **Veri Bütünlüğü Riski:** 1. **Manipülasyon** (%50 + 1 düğüm noktasının ele geçirilmesi)
2. **Kişisel Veriler** ve Ticari Verilerin **Gizliliđi** > AB Blok zincir Forum Çözümleri
- 3** Özel Blok zincirlerde risk: **AAA sağlanamaması** sebebiyle iç saldırganlara açıklık
> PKI ile uçtan uca şifreleme, cold (offline) storage kullanımı

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

Blok Zincirin Güvenliđi

- 1** Blok zincir işleyişı geleneksel yaklaşımların dışında:
Veri her yerde, şeffaflık temelli > **Veri Sızıntısı** mümkün deđil
- 2** **Veri Bütünlüğü Riski:** 1. **Manipülasyon** (%50 + 1 düđüm noktasının ele geçirilmesi)
2. **Kişisel Veriler** ve Ticari Verilerin **Gizliliđi** > AB Blok zincir Forum Çözümleri
- 3** Özel Blok zincirlerde risk: **AAA sağlanamaması** sebebiyle iç saldırganlara açıklık
> PKI ile uçtan uca şifreleme, cold (offline) storage kullanımı

BİLİNEN PROBLEMLER ve ÇÖZÜMLER

Problem: Cüzdana ait özel anahtarın çalınması

Çözüm: Cold Storage / HSM kullanımı


Problem: Kuantum hesaplama ile kriptografinin çözülmesi
(Adres ve genel anahtar ile özel anahtar çözülür)

Çözüm: Kuantum dirençli algoritmalar
(NSA, SHA-384 önermektedir)

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

Blok Zincirin Güvenliđi

- 1
- 2
- 3



**24.Eylül.2019 - GOOGLE KUANTUM BİLGİSAYARI
54 QBIT'LİK İŞLEMÇİ (SYCAMORE)**
En hızlı süper bilgisayarla **10.000 YIL**'da yapılan işlemi
200 SANİYE'de tamamladığı duyuruldu.

Sabancı Üniversitesi

(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

Blok Zincirin Güvenliđi

- 1 Blok zincir işleyişı geleneksel yaklaşımların dışında:
Veri her yerde, şeffaflık temelli > **Veri Sızıntısı** mümkün deđil
- 2 **Veri Bütünlüğü Riski:** 1. **Manipülasyon** (%50 + 1 düđüm noktasının ele geçirilmesi)
2. **Kişisel Veriler** ve Ticari Verilerin **Gizliliđi** > AB Blok zincir Forum Çözümleri
- 3 Özel Blok zincirlerde risk: **AAA sağlanamaması** sebebiyle iç saldırganlara açıklık
> PKI ile uçtan uca şifreleme, cold (offline) storage kullanımı
- 4 **Oracle:** Güvenilir zincire güvenilmez birçok verinin girilmesi ile zincirdeki veri bütünlüğüne güvenin oluşma riski
- 5 Saldırı veya doğal afet sonrası **bölgesel / Küresel internet kesintisi**
- 6 **Kod Güvenliđi:** Akıllı kontratlarda yazılan kodlarla overflow'a sebep olarak blok yaratma ve onaylama sürecinin etkilenmesi (2016)

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

Siber Güvenlik için Blok Zincir

- Veri Bütünlüğü** 1 **Uzlaşma** (consensus) modeli sayesinde zincirdeki veriyi manipule etmek pratikte mümkün değildir.
- Veri değiştirilememesi, silinememesi ve araya eklenememesi** temel prensiptir. («Kişisel Veriler - Unutulma Hakkı» için özel anahtar kullanılır)
- Siber Saldırıları** 3 **DDoS atağı** merkezi yapılar içindir , blok zincir dağıtık yapıdadır. DDoS'a karşı doğal bağışıklığı vardır. («Single Point of Failure» yoktur)
- Veri Şifreleme**, blok zincirin doğasında mevcuttur.
- Bilgi Güvenliği** 5 Bilgi Güvenliği Temel Şartlarını karşılar (**CIA**)
- 6 Bir blok zincir uygulaması olan bitcoin, son 9 yıldır markette siber güvenliğe karşı en çok **test** edilen ve **saldırlara en iyi dayanan** platformdur.

Sabancı Üniversitesi | Siber Güvenlik, Kriptografi, Blok Zincir | 02.11.2019 Ankara | Siber Güvenlik için Blok Zincir | Dr. Mustafa Afyonluoğlu

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

Siber Güvenlik için Blok Zincir

Veri Bütünlüğü	1	Uzlaşma (consensus) modeli sayesinde zincirdeki veriyi manipule etmek pratikte mümkün değildir.
	2	Veri değiştirilememesi, silinememesi ve araya eklenememesi temel prensiptir. («Kişisel Veriler - Unutulma Hakkı» için özel anahtar kullanılır)
Siber Saldırıları	3	<p>BİLGİ GÜVENLİĞİ TEMEL ŞARTLARI</p> <p>Confidentiality (Gizlilik): Özel blok zincir & Tam-şifreleme</p> <p>Integrity (Bütünlük): Zincirde değiştirilemezlik (#UnutulmaHakkı --> Kişisel Veri şifrelenir ve gerektiğinde anahtarlar imha edilir)</p> <p>Availability (Kullanılabilirlik): Merkezî olmadığından DDoS'a dirençlidir. Bundan dolayı AAA (Authentication, Authorization, Auditing) ve non-repudiation sağlar.</p>
	4	
Bilgi Güvenliği	5	
	6	

Sabancı Üniversitesi Siber Güvenlik 02.10.2019

Siber Güvenlik için Blok Zincir Dr. Mustafa Afyonluoğlu

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

Yakın Gelecek...

- 1 Dijital Ekonomide büyük bir hacim (8.1 Trilyon \$) mevcuttur.
- 2 Türkiye'nin bu hacimden hedef belirleyip hızla çalışmalara başlaması gerekir.
- 3 Blok zincir dijital ekonominin kritik yenilikçi teknolojilerinden birisidir.
- 4 Blok zincir'in, e-Devlet'te şeffaflığı ve güveni artırıcı, çok paydaşlı çalışmayı kolaylaştırıcı etkisini ve özellikle siber güvenlikteki gücünü kullanmak gerekir.

Sabancı Üniversitesi Siber Güvenlik, Kriptografi, Blok Zincir 02.11.2019 Ankara

Siber Güvenlik için Blok Zincir
Dr. Mustafa Afyonluoğlu

(Bu sayfanın açıklaması, sunum metninde yer almaktadır)

Daha çok incelemek isterseniz...

BLOKZİNCİR - ULUSLARARASI RAPORLAR

Toplam Rapor Sayısı: 53
Son Güncelleme: 30.09.2019

Deloitte pwc WORLD ECONOMIC FORUM WORLD BANK HUAWEI ITU McKinsey & Company

AVRUPA BİRLİĞİ
The European Union Blockchain Observatory and Forum

2019 July: NEW Blockchain and the General Data Protection Regulation (GDPR): Can distributed ledgers be squared with European data protection law?

2019 May 2: Blockchain and Digital Identity

2019 March 6: Scalability, Interoperability & Sustainability of Blockchains

2019 : Blockchain for Digital Government: An assessment of pioneering implementations in public services

WORKSHOP REPORTS

2019 May 24: Digital Assets

2019 April 30: Governance and New Organisational Challenges

2019 March 28: Convergence of blockchain

2019 February 19: Supply Chain and Traceability

2018 December 12: Legal Recognition of Blockchains & Smart Contracts

<http://afyonluoglu.org/blokzincir-blockchain/>

Sabancı Üniversitesi **Siber Güvenlik, Kriptografi, Blok Zincir** 02.11.2019 Ankara

Siber Güvenlik için Blok Zincir
Dr. Mustafa Afyonluoğlu

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.



SİBER GÜVENLİK İÇİN BLOK ZİNCİR

TEŞEKKÜR EDERİM

Dr. MUSTAFA AFYONLUOĞLU

Siber Güvenlik, E-Yönetişim ve Dijital Ekonomi Kıdemli Uzmanı

<http://afyonluoglu.org>

2 Ekim 2019
Ankara

Sunum Telif Hakkı: © 2019 Dr. Mustafa AFYONLUOĞLU (afyonluoglu@gmail.com)
Sunumdan alıntı yapılması halinde sunumun başlığı, sunumu hazırlayan ve sunumun yayımlandığı web adresinin referans gösterilmesi zorunludur.

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

Yayın / 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.