MANAS Sosyal Araştırmalar Dergisi 2020 Cilt: 9 Sayı: 4
MANAS Journal of Social Studies 2020 Volume: 9 No: 4
ISSN: 1694-7215
Review Paper / Derleme Makalesi

Siber Saldırı Önlemede Blokzinciri Teknolojisinin Fayda Maliyet Açısından Değerlendirilmesi

Ömer AYDIN[1] ve Süleyman YÜKÇÜ[2]

Öz

İnternetin hayatımızın her alanına girmesi insan yaşamı için birçok kolaylık ve fayda getirmiştir. Öte yandan internet, doğası gereği sorunlar ve tehditleri de beraberinde getirmiştir. Bireyler bakımından kişisel verilerin izinsiz ele geçirilmesi ve paylaşılması, devlet, şirket ve kurumlar bakımından ise kritik öneme sahip bilgilerin sızdırılması gibi riskler ortaya çıkmıştır. Bu doğrultuda bireyleri, şirketleri, kurumları ve devletleri zarara uğratmak veya bilgilerini ele geçirmek için sanal ordular kurulmakta, saldırılar düzenlenmektedir. Bu saldırıların en yaygınlarından bir tanesi dağıtık olarak farklı kaynaklardan yapılan hizmet durdurma saldırılarıdır. Blokzinciri teknolojisi her alanda ve durumda uygulanabilir olmasa da belli uygulamalar için uygundur. Merkezi olmayan yapısı ile ciddi avantajlar sunmaktadır. Siber saldırılara karşı kurumların, şirketlerin ve devletlerin maliyetlerini düşürebilecek bir çözüm olarak blokzinciri teknolojisi kullanılabilir. Bu çalışmada, blokzinciri teknolojisi ve siber saldırılar hakkında teknik bilgiler, yapılmış siber saldırıların ortaya çıkardığı zararlar paylaşılmış ve belli durumlarda bu saldırıların bir kısmını engellemek için kullanılabilecek blokzincirinin maliyet fayda analizi yapılmıştır. Sonuç olarak blokzincirinin kullanılabileceği uygulamalarda siber saldırıların oluşturduğu maliyetlerden kaçınılabileceği veya maliyetlerinin düşürülmesine fayda sağlayacağı tespit edilmiştir.

Anahtar Kelimeler: Siber saldırı, Blokzinciri, Dağıtık sistemler, Dağıtık hizmet durdurma saldırıları, Maliyet

Assessment of Blockchain Technology in terms of Benefit-Cost in Cyber Attack Prevention

Abstract

The spread of the Internet in all areas of our lives has brought many eases and benefits for human life. On the other hand, the Internet has brought along problems and threats by its nature. Risks such as the seizing and sharing of personal data without permission, and leakage of critical information for government, companies and institutions have emerged. In this direction, cyber armies are set up and attacks are organized in order to damage people, companies, institutions and governments to capture their information. One of the most common of these attacks is denial of service attacks from different sources. Although blockchain technology is not applicable in all areas and situations, it is suitable for certain applications. It offers serious advantages with its decentralized structure. Blockchain technology can be used as a solution to reduce the costs of institutions, companies and governments against cyber-attacks. In this study, technical information about blockchain technology and cyber-attacks, the damages caused by cyber-attacks were shared, and cost benefit analysis of blockchain, which can be used to prevent some of these attacks in certain cases, was made. As a result, it has been determined that in applications where blockchain can be used, the costs caused by cyber-attacks can be avoided or it will benefit the reduction of costs.

Key Words: Cyber attacks, Blockchain, Distributed systems, Distributed denial of service attacks, Cost

Atıf İçin / Please Cite As:

Aydın, Ö. ve Yükçü, S. (2020 Siber saldırı önlemede blokzinciri teknolojisinin fayda maliyet açısından değerlendirilmesi. *Manas Sosyal Araştırmalar Dergisi, 9*(4), 2519-2530.

Geliş Tarihi / Received Date: 20.05.2020 **Kabul Tarihi / Accepted Date:** 04.08.2020

[1] Dr., Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi, İzmir, Türkiye, omer.aydin@deu.edu.tr
ORCID: 0000-0002-7137-4881
[2] Prof. Dr., Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi, suleyman.yukcu@deu.edu.tr
ORCID: 0000-0002-1514-5953

Giriş

Teknolojinin gelişimi ile birlikte güvenlik ve gizlilik gibi iki temel konu, hem kişilerin hem de kurum ve devletlerin başa çıkması gereken konular olarak önemini günden güne arttırmaktadır. Güvenlik, birey, kurum, şirket veya devletlerin mevcut düzen içinde belirlenmiş kurallar çerçevesinde yaşamlarını sürdürmelerine, her türlü tehdit, taciz, salgın ve felakete karşı alınan tedbirlere denilir. Gizlilik ise bir bilginin erişiminin kısıtlanması, bir kimse veya belirlenen bir zümre dışındakilerin bu bilgiye erişememesi anlamına gelmektedir. Bu iki temel kavram günümüzde büyük önem taşımaktadır. Her seviyede organizasyonun bilgilerini internet aracılığı kablolu veya kablosuz olarak iletildiği günümüz dünyasında bu bilgilerin güvenliğinin ve gizliliğinin sağlanması da çok önemlidir. Aksi bir durumda kişiler, kurumlar ve devletler maddi manevi zararlara uğramaktadırlar.

Siber güvenlik kavramı, güvenliğin siber ya da sanal dünya diye adlandırdığımız teknoloji ortamındaki yansımasını karşılamaktadır. İnsan, kurumlar veya devletler her alanda güvende olmak istemektedirler. Günümüz dünyasında bilgi, bu bilginin anlamlandırılması ve güvenliğinin sağlanması büyük önem kazanmıştır. Bu çalışmanın motivasyon noktalarından birincisi budur. İkinci konu ise güvenlik ve gizlilik ihlallerinin doğurduğu maddi ve manevi sonuçlardır. Bu çalışmada daha çok maddi kayıplar üzerinde durulacaktır. Özellikle şirketlerin ve devletlerin maddi anlamda kayıpları değerlendirilecektir. Blokzinciri teknolojisinin dağıtık yapısı nedeni ile kullanılabildiği alanlarda güvenlik ve gizlilik anlamında ciddi kazanımlar sağladığı aşikârdır. Çalışmanın son motivasyon noktası ise bu dağıtık yapının kurum ve devletler için sağlayacağı maddi kazanımlardır.

Siber güvenlik ve blokzinciri ile ilgili genel bilgilerin yer aldığı ilk bölümden sonra ikinci bölümde geçmişten günümüzü yapılan siber saldırılardan bahsedilmiş, ortaya çıkan zararlar verilmiştir. Sonrasında blokzinciri teknolojinin kullanılabileceği uygulama örneklerine yer verilmiş olup güvenlik açısından sunduğu kazanımlar değerlendirilmiştir. Son olarak ise bu kazanımların mali açıdan analizi yapılmıştır. Bu çalışmanın amacı siber güvenliğin şirketler ve ülkeler için önemini vurgulamak, mali açıdan çeşitli uygulama alanlarında ciddi kazanımlar sağlayabilecek blokzinciri teknolojisinin analizlerini yapmaktır.

Siber Güvenlik

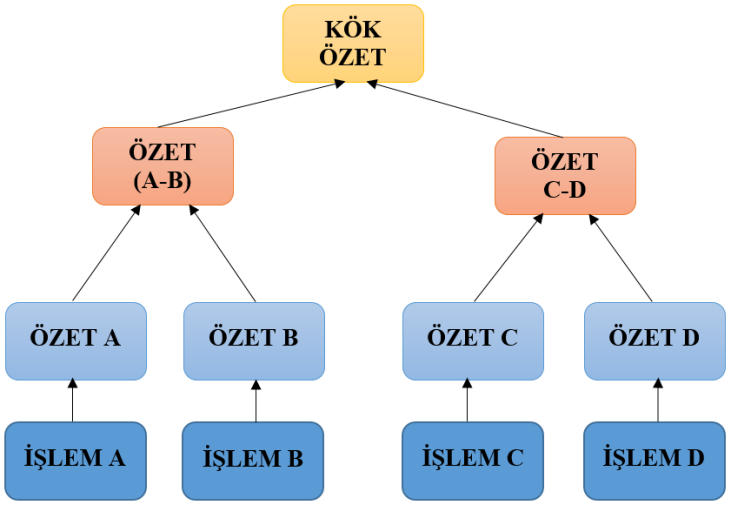
Siber güvenlik, 1990'lı yıllarda, internet ağına bağlı bilgisayarlarda yaşanan güvenlik sorunları ve tehditlerini ifade etmek üzere bilgisayar mühendisleri tarafından oraya atılan bir terimdir (Hansen ve Nissenbaum, 2009, s. 1155). Bu kavram ile siber dünyada yer alan bilginin gizliliğinin, erişilebilirliğinin ve bütünlüğünün sağlanması kastedilmektedir. Gizlilik, bilgiye erişimi kısıtlayan bir anlam ifade etmektedir. Bir başka şekilde ifade edersek bilgiye sadece izin verilen veya yetkisi olan kişiler, gruplar veya makinelerce erişilebilmesidir. Erişim sadece okuma şeklinde olabilecekken, yeni bilgi oluşturma, silme ve güncelleme işlemlerinin hepsi veya belli bir kısmının izin verilmesi şeklinde olabilir. Bütünlük kavramı ise bilginin kısmen veya tamamen değiştirilmemesi anlamına gelmektedir. Bilginin, iletilmek istenen taraflar arasında transfer edilirken veya saklandığı alanda bulunurken bütünlüğünün korunması gereklidir. Erişilebilirlik ise saklanan bilginin erişim iznine sahip kişilerce istenildiğinde erişilebilir olması demektir (Goodrich ve Tamassio, 2011).

Siber saldırılar son dönemde sadece kişisel bilgisayarlara zarar vermemekte aynı zamanda ülkelerin bilgisayar sistemleri, haberleşme altyapıları, askeri üsleri ve silah sistemleri, ulaşım araçları ve altyapıları, enerji sistemleri ve sağlık sistemleri gibi birçok kritik noktayı tehdit etmektedir. Siber tehditler bu anlamda önümüzdeki yıllarda da önemini koruyacaktır (Aytekin, 2015, s. 19). Bu durum göz önünde bulundurulduğunda karşı önlemlerin zaman kaybetmeden planlanması, acil durum senaryolarının hazırlanması ve etkin savunma sistemlerinin kurulması büyük önem taşımaktadır. Saldırılara karşı ulusal veya bölgesel boyutta çeşitli önlemler alınması ve bunun saldırıyı takiben hemen hayata geçirilebiliyor olması gerekmektedir (Goodman, 2008, s. 28).

Devletimiz ve şirketlerimiz son yıllarda siber saldırılara maruz kalmaları nedeni ile bu konuya daha fazla yatırım yapmaktadırlar. Alınan önlemler ve yasa koyucu tarafından yapılan kanunlar teknolojinin hızına dolayısı ile siber tehditlere yetişememektedir. Saldırıların çeşitliliği, büyüklüğü ve etkisi göz önünde bulundurulduğundan kişilerin, kurumların ve hatta devletlerin işbirliği yapmalarını gerektirecek seviyede önlemlere ihtiyaç vardır. Siber güvenlik için yapılan harcamalar, güvensiz bir ortamın getireceği maliyetlerden fazla olmayacaktır (Aslay, 2017, s. 27).

Blokzinciri Teknolojisi

2000 yılların başından itibaren internetin hız ve erişilebilirlik bakımından ülkemiz ve dünyada gelişmesi, mobil bağlantı hız ve imkânlarının artması ile birçok teknolojinin gelişimi mümkün hale gelmiştir. Bu gelişimin bir sonucu olarak ortaya çıkan teknolojilerden biri de blok zinciri yapısıdır. Blokzinciri yapısı bir tarafında şifre bilimi (kriptoloji) diğer tarafında ise veri yapıları bulunmaktadır. Bu yapının geçmişi Merkle ağacı olarak bilinen karma ağaç yapısına dayanmaktadır (Merkle, 1982, s. 2). Şekil 1'de Merkle ağacının yapısı görülebilmektedir. Merkle ağacı uç düğümlerden kök düğüme doğru giden bir ağaç yapısıdır. En uç düğümlerde işlemler yer almaktadır. Bu işlemlerin özetlerinden bir üst düğüm oluşturulur. Özet işlemi için Hash fonksiyonlarından faydalanılır. Daha sonra özetlerin bir araya getirilmesi ile yeni özetler oluşturulur ve bu şekilde üst düğümlere doğru ilerlenir. Son iki düğümün özeti de alınarak kök düğüm oluşturulur.



Şekil 1. *Merkle Ağacı (Karaarslan ve Akbaş, 2017, s. 18)*

Merkle ağacının bir diğer adı da Hash ağacıdır. Hash fonksiyonları, bir veri kümesinin boyundan bağımsız olarak, sabit uzunlukta bir veri kümesi üreten algoritmalara denir. Hash fonksiyonlarının ürettiği metinlerin kaynak metinin bir özeti şeklinde olması ile Merkle ağacındaki özet düğümleri ortaya çıkmaktadır. Bu değerlerin benzersiz olduğu varsayımı ile işlemler yapılmaktadır.

Blokzinciri, gerçek dünyadaki bir zincir gibi yeni halkaların zincirin sonuna eklenmesi ile büyüyen bir veri yapısıdır denilebilir. Eklenen zincir halkaları bir önceki blokun adres bilgisini üzerinde barındırır. Kayıt defteri (Ledger) olarak adlandırılan bir liste vasıtası ile zincirin değiştirilemez listesi tutulur.

Akıllı anlaşmalar (Smat contract) kavramını blokzinciri bakımından mantıksal akışların yazıldığı, blokzincirinin dağıtık yapısı içinde çoğaltılıp dağıtılabilen, çalıştırılıp işletilebilen ve güvenliği bir ağ tarafından doğrulanabilen küçük programlara verilen addır.

Madenci Düğüm (Mining Node): Bu düğümler birer bilgisayar olup işlemler bu bilgisayarlar üzerinde gerçekleşmektedir. İşlemlerin gerçekleşmesi için önceleri ekran kartları veya bu iş için üretilmiş bazı özel kartların işlemcileri kullanılmıştır (Stallings, 2017, s. 19). Günümüzde ise Merkezi İşlem Birimi (CPU), Grafik İşlemci Birimi (GPU), Alan-Programlanabilir Kapı Dizisi (FPGA) ve Uygulamaya Özel Entegre Devre (ASIC) gibi donanımlar yanında bulut hesaplama madencilik işlemlerinde kullanılmaktadır.

Madencilik Gücü: Blokzinciri karmaşık denilebilecek matematiksel hesaplamalar yapılan bir sistemdir. Zincire yeni bir bloğun eklenmesi esnasında hash hesaplanması denilen matematiksel işlemler için bir güce ihtiyaç vardır. Bu güç işlemci gücü olarak karşımıza çıkmaktadır ve genelde saniyede hesaplanan Hash ile ölçülmektedir.

Uzlaşma Protokolleri: Blokzinciri belli kurallara bağlı olarak değiştirilir. Zincirde bulunan düğümler için kimin değişiklik yapabileceği konusundaki kurallar bütünü uzlaşma protokolü olarak adlandırılabilir. Bu aşamada Çalışma Kanıtı (Proof of Work-PoW) ve Hisse İspatı (Proof of Stake-PoS) gibi yaklaşımlardan bahsetmek gerekir. PoW, her bir düğüm için çözülmeyi bekleyen bir bulmaca gibidir ve bulmacayı çözmeden değişiklik önerisi yapabilme hakkı kazanılamamaktadır. PoS ise PoW'dan farklı olarak hesaplamaya bakılmaksızın sisteminde sahip olunan kriptopara zenginliğine yani hissesine bakılarak blok

oluşturma işlemini yapacak kişinin seçildiği bir yaklaşımdır.

Hesap: Klasik anlamda bildiğimiz gibi parayı içinde barındıran, benzersiz (unique) bir değer ile ifade edilen ve her kullanıcı veya bilgisayara özgü olarak oluşturulan hesaptır.

Literatür Taraması

Çetin vd. yaptıkları çalışmada fidye yazılımlarla oluşan siber tehditlerden 2013 ve 2014 yıllarında Türkiye'nin siber tehditlere maruz kalan ülkeler arasında ilk onda yer aldığını belirtmişlerdir. Çalışmalarında e-işletme ve e-ticaret kavramlarını ele almışlardır. Bu kavramların farklı sektör ve alanlardaki etkilerini değerlendirmişler, Dünyada ve ülkemizde gerçekleşen siber güvenlik tehditlerini ortaya koymuşlardır. Ayrıca siber saldırı ve bunların ortaya çıkardığı maliyetler konusunda değerlendirmelere yer vermişlerdir (Çetin vd., 2015, s. 223).

Şentürk ve arkadaşları 2016 yılında yayınlanan çalışmalarında siber güvenlik yatırımlarının stratejileri, maliyetleri, etkisi gibi konularda literatürü incelemişlerdir. Şirketlerin siber güvenlik yatırımı kararları almalarında çeşitli boşluklar tespit etmişlerdir. Çalışmalarında siber güvenlik risklerinin ölçülebilmesi için genel geçer bir model bulunmadığını belirtmişlerdir. Aynı şekilde yatırım kararı alınarak sahip olunan önleyicilerin etkinliğini ölçebilen bir standardın bulunmadığını söylemişlerdir (Şentürk vd., 2016, s. 48).

Irmak ve Erkek'in çalışmalarında farklı bir açıdan bakılarak kritik denilebilecek sistemlere siber saldırı yapan saldırganların profillerine odaklanılmıştır. Saldırı ağacı modelini kullanarak yapılan siber saldırıların başarılı olma ihtimalleri hesaplanmış ve bu hesaplamalar üzerine analizler yapılmıştır. Çalışmanın çıkış noktası literatürde saldırgan profilleri ile ilgili karakteristik özelliklere ait parametrelerde eksiklik olduğu iddia edilmektedir. Eksikliği fark edilen karakteristik özelliklerin saldırgan profillerine dâhil edilmesi ile matematiksel olarak hesaplanan saldırı başarı olasılıklarının gerçeğe yaklaştığı beyan edilmiştir (Irmak ve Erkek, 2016, s. 1).

Literatürde Conoscenti ve arkadaşlarının yaptığı bir çalışmada blokzinciri teknolojisi kullanılan mal ve verilerin ticareti, veri depolama yönetimi, değerlendirme sistemleri ve kimlik denetimi gibi alanlar incelenmiştir. Ayrıca bu çalışmada anonimlik, bütünlük ve uygulanabilirlik gibi blokzincirinin temel özellikleri etkileyen etmenler irdelenmiştir (Conoscenti vd., 2016, s. 1). MedRec adını verdikleri blokzinciri teknolojisi kullanan bir kayı yönetim sistemi Azaria ve arkadaşları tarafından önerilmiştir. Adından da anlaşılacağı üzere sağlık alanında kurgulanan bu sistem ile hastaların bilgilerinin kaydedilmesi ve bunların erişiminin kolaylaştırması amaçlamıştır (Azaria vd., 2016, s. 25). Dijital haklar gibi sözleşmelerin yönetimi için kurgulanan ve daha güvenli bir yapı kurulması için Watanbe ve arkadaşları tarafından bir sistem önerilmiştir (Watanabe vd., 2016, s. 467). Ülke ulusal güvenlik sistemleri için blokzinciri teknolojisinin kullanımının gerekliliğine vurgu yapan Barnas, çalışmasında çeşitli alanlarda blokzincirinin kullanımı ile elde edilecek faydalar vurgulanmıştır (Barnas, 2016, s. 8). Blokzinciri teknolojisinin kullanıldığı bir diğer alan olarak bilgisayar ağları da verilebilir. Bunlara ilk örnek DNSChain (Singh ve Singh, 2016, s.463) verilebilir. Güvenli, merkezi olmayan ve özgür bir çözüm olarak sunulmuştur. Diğer yandan SecureChain ağ cihazlarının bazı kayıtlarının saklanmasına yönelik bir çözüm sunmaktadır (SecureChain, 2020). Özellikle ağ cihazlarında saklanması zorunlu ve değiştirelemezliği güvence altına alınması gereken log vb. kayıtların saklanması için önerilmiştir.

Şenol'un 2016 yılında yayınlamış olduğu makalesinde gelişen teknolojik güçle siber caydırıcılığın sağlanabileceği vurgulanmıştır. Çalışmada Türkiye'de meydana gelen bazı siber saldırılara değinilmiştir (Şenol, 2016, s. 10). Yine aynı yazara ait 2017 yılında yapılmış benzer çalışmada ülkemizdeki siber saldırılara karşı caydırıcılık konusu işlenmiştir. Çalışmada ilk olarak siber güç, saldırı, savaş ve caydırıcılık gibi kavramlar irdelenmiş siber güvenliğin önemine değinilmiştir. Türkiye'de siber saldırılarak karşı caydırıcı olmak için yapılmış strateji ve politikaların yer aldığı çalışmalar incelenmiştir. Siber caydırıcılığın sağlayacağı maliyet ve kolaylıklar açısından sağladığı üstünlüklere dikkat çekilerek çeşitli önerilere yer verilmiştir (Şenol, 2017, s.1).

Karaarslan ve Akbaş 2017 yılında yaptıkları çalışmalarında Blokzinciri tabanlı güvenlik sistemlerini incelemişlerdir (Karaarslan ve Akbaş, 2017, s. 16). Blokzinciri dijital imzalar, şifreleme algoritmaları ve özet (Hash) fonksiyonlarını kullanmaktadır. Güvenlik ve gizlilik gerektiren birçok alanda blokzinciri ile kurulmuş sistemler kullanılabilmektedir (Halpin ve Piekarska, 2017, s. 1).

IoT cihazlarının davranışlarını tayin eden kodlar yazarak bu cihazların yönetiminin blokzinciri ile yapılmasının önerildiği bir çalışmayı Huh ve arkadaşları 2017 yılında yayınlamışlardır. Bu çalışmada platform olarak Ethereum kullanılmıştır (Huh vd., 2017, s. 464). Blokzincirinin IoT cihazlarının güvenlik ve gizlilik ihtiyaçlarını karşılamada kullanılmasını öneren bir çalışmayı Dorri ve arkadaşları yapmıştır.

Kullanılan tekniğin DDoS ve Linking siber saldırıları karşısında etkin olup olmadığı bu çalışmada analiz edilmektedir (Dorri vd., 2017a, s. 173). Bir diğer çalışmada Biswas ve Muthukkumarasamy, akıllı şehirlerde güvenlik sorunlarına çözüm olarak blokzinciri kullanımını önermişlerdir. Bu çalışmada blokzincirinin büyük maliyet gerektirdiği ve bağlantı hızı bakımında yüksek bant genişliği kullandığı için IoT cihazlarının birçoğu için uygun olmadığı belirtilmektedir (Biswas ve Muthukkumarasamy, 2016, s. 1392).

Blokzinciri; kamu kuruluşlarında özel veya halka açık şekilde kullanılabilir. Ödeme sistemleri, dolandırıcılık tespiti, yerel ve merkezi birimlerden gelen belge ve veriyi birbirine bağlama, kayıt yönetimi (patent, akademik kayıtlar, noter kayıtları vb.) kimlik yönetimi, fiziksel varlık (gayrimenkul tapu kayıtları vb.) takibi, vergi takibi, gümrük ve sınır kontrolü (Ølnes vd., 2017, s. 355), dijital pasaportlar(Zhao, 2017), dijital oylama sistemleri, düzenleyici gözetim işlemleri (bağış toplayan kurumların denetimi) gibi birçok alanda uygulabilir bir teknolojidir (Durğay ve Karaarslan, 2018, s. 39).

Dorri ve arkadaşları IoT gibi düşük kaynaklı donanımlar için blokzinciri mimarisini kaynak kullanımı anlamında iyileştirdikleri bir öneride bulunmuşlardır. Bu çözüm ile güvenlik ve gizlilik özellikleri sağlanmaktadır. PoW yerine blok onay zamanını azaltmak için dağıtık güven yöntemi kullanımı önerilmiştir. Hizmet durdurma saldırısı (DoS), ekleme, düşürme ve modifikasyon saldırısı gibi bazı tehditlere karşı koyabildiği iddia edilmiştir (Dorri vd., 2017b, s. 618).

Konacakli ve Karaarslan'ın çalışmalarında siber alanda Komuta ve Kontrol yeteneklerinin güvenlik ve gizliliğini sağlamak için blokzincirinin kullanılabileceğini belirtmişlerdir. Askeri hava operasyonları için blokzincirinin sunduğu faydalar değerlendirilmiş ve bir sistem önerisinde bulunulmuştur (Konacakli ve Karaarslan, 2019, s. 758).

Baygin ve arkadaşlarının yaptığı çalışmada ise avantajları ve dezavantajları ile uygulama bazında yapılan blokzincirleri incelenmiş ve karşılaştırılmıştır (Baygin vd., 2019). Gür ve arkadaşlarının yapmış olduğu diğer bir çalışmada ise elektrik şebekelerinde mikro düzeyde bölgesel veya müşteri bazlı ölçüm, faturalandırma ve izleme işlemleri için IoT ve blokzinciri tabanlı bir system önerilmektedir (Gür vd., 2019, s. 204).

Siber Saldırılar ve Etkileri

İnternetin yaygınlaşması ile birlikte farklı yöntemler ve farklı boyutlarda birçok siber saldırı düzenlenmiş ve birçok şirket ve kurum bunlardan etkilenmiştir. Bazı saldırılar ise devlet sistemlerine yönelik düzenlenmiştir. Bu saldırılardan bilinen büyük boyuttakileri aşağıda verilmiştir.

Moonlight Maze, 1998 yılında başlayan ve ABD askeri sistemlerine sızmayı başaran bir yazılım ile askeri bilgilerinde yer aldığı çok sayıda dosyanın çalındığı bir saldırıdır. Bu yazılım vasıtası ile işlemlerin fark edilmeden 2 yıl boyunca devam ettiği belirlenmiştir. ABD yaptığı araştırmalar sonucunda eski Sovyet birliğine ait bir bilgisayara bilgilerin ulaştırıldığı bilgisine ulaşsa da Rusya bu konuda suçlamaları kabul etmemiştir (Siber Kuvvet, 2015).

Rusya'nın Estonya ile birlikte Nazilere karşı verdiği mücadelenin simgesi olarak Bronz Asker Anıtı, Estonya hükümetinin kararı ile 2007 yılının Nisan ayında yerinden kaldırılmıştır. Bu işlem sonrası büyük tepkiler oluştu. Kısa sürede Estonya hükümetinin kullandığı elektronik sistemlere, bankalara, haber portallarına ve hizmet sağlayıcılara büyük bir siber saldırı düzenlendi. Yapılan servis durdurma atağı nedeni ile uzun süre sistemler çalışamadı (Yener, 2015).

Albert Gonzales 2008 yılında Heartland ödeme sistemlerine saldırmıştır. Albert saldırıyı "Operation Get Rich or Die Tryin" (Zengin ol veya Çabalarken Öl Operasyonu) olarak adlandırmıştır. Bu saldırıda Heartland'a ait yaklaşık 100 milyon kredi kartı bilgisinin ele geçirildiği düşünülmektedir. Bu saldırının şirkete maliyeti yaklaşık olarak 140 milyon dolar olmuştur (Siber Kuvvet, 2015).

2011 yılında Sony PlayStation Network hacklendi ve 77 milyon kullanıcının kişisel bilgilerine erişildi. Dağıtık hizmet durdurma (DDOS) saldırılarıyla sisteme sızan saldırganlar kullanıcıların kredi kartı bilgilerini ele geçirdiler. Bu saldırıda PlayStation servislerine 23 gün boyunca erişim sağlanamadı. Sony, başlangıçta hack'in en az 105 milyon sterline mal olacağını tahmin etti, ancak şirket daha sonra etkinin korktuğu kadar finansal zarara neden olmadığını öne sürdü (Phillips, 2016).

Kanada'nın birçok devlet kurumuna ait IP adreslerine 2011 yılında büyük bir saldırı yapılmıştır. Saldırıyı yapan Internet Protokol (IP) adresleri Çin'e ait olduğu tespit edilmiştir. Saldırı, finans ve savunma gibi alanlarda hizmet veren devlet kurumlarını da içermekte idi. Bu saldırıyı durdurmak için saldırı yapılan birimlerin internet bağlantılarını kesmek zorunda kalmışlardır (Siber Kuvvet, 2015).

Citigroup, 2011 yılında siber saldırılara maruz kalarak müşterilerine ait kişisel verilerini çaldırmıştır. Forbes Global 2000'nin değerlendirmelerine göre dünyadaki en büyük şirket olarak seçilen Citigroup, saldırılar nedeni 2.7 milyar dolar zarara uğrarken iki yüz binin üzerinde müşterisine ait kredi kartını yenilemek zorunda kalmıştır (Naraine, 2011).

İstenemeyen posta (Spam) trafiğinin izlenmesi ve gönderim yapanların takibi amacı ile kurulmuş bir organizasyon olan Spamhaus, elektronik postaların zararlı olup olmadığının belirlenmesinde kullanılan listeler yayınlamaktadır. Spamhaus, 2013 yılında Cyberbunker adlı bir veri merkezinden gelen elektronik postaları zararlı kategorisine aldı. Bundan sonra arkasında Cyberbunker 'in olduğunun iddia edildiği ve internetin o güne kadarki en büyük dağıtık servis durdurma saldırısı gerçekleştirildi. Saldırının 300 Gbps boyutuna ulaştığı bildirilmektedir. Bu saldırı ile çok büyük miktarda veri internet ortamına yayıldı (Dağhan, 2013).

Stuxnet adlı yazılım İsrail ile ABD tarafından ortak olarak İran'ın nükleer alandaki çalışmalarını durdurmak için geliştirilmiştir. Windows işletim sistemine sahip bilgisayarlara bulaşarak Siemens tarafından geliştirilmiş özel bir yazılımı hedef almıştır. Bu yazılım vasıtası ile dış dünyadan izole olarak çalışan İran nükleer santrallerinden iki tanesinin çalışmalarını engellemeyi başarmışlardır. Bu saldırı ile kapalı ve izole ağlarda dahi saldırıların mümkün olabileceği gösterilmiştir (Siber Kuvvet, 2015).

Windows işletim sistemi ile çalışan bilgisayarlar üzerinde etkili olan Flame adlı yazılım aynı ağda yer alan diğer bilgisayarlara da kendi kopyasını göndermeye çalışmaktadır. Ayrıca USB harici bellekler vasıtası ile de bilgisayarlar arasında kendini kopyalatma özelliğine sahiptir. Bulaştığı bilgisayardaki konuşmalar, yazışmalar, şifreler, dosyalar vb. bilgileri almakla kalmaz Bluetooth ile çevredeki bağlı cihazlarında bilgilerini elde etmeye çalışmaktadır. Bu bilgiler belli bir süre sonra saldırgana iletilmektedir. Bu yazılım orta doğu ülkelerinde daha yoğun görülmüştür. Kaspersky antivirus firması çalışanlarından bir tanesi bu yazılımın kullanılan teknik ve içerdiği detaydan dolayı bir devlet tarafından yazılabileceği kanısında olduğunu belirtmiştir (Siber Kuvvet, 2015).

İnternette siber saldırılar ve siber terör ile ilgili olarak 2015 yılında yayınlanmış bir haberde neredeyse her sistemin internete bağlı hale geldiği ve sağlık, güvenlik, devlet kurumları gibi birçok kritik alan gibi kişilerin günlük yaşamlarındaki alanlarında kapsama alanına girdiğine vurgu yapılmıştır. Tüm bu kritik alanlardaki bilgiler ile toplum içinde olağan bir şekilde yaşayan insanların dahi verileri izlenebilmekte ve risk altındadır. Bu haberde de bahsedildiği gibi internete bağlı olarak çalışan evimizdeki buzdolabı saldırganlar tarafından ele geçirilebilmekte ve bu şekilde zombi makinelere dönüşebilmektedir (Öncel, 2014). Bu haberde Siber terör, siber saldırıların nedenleri ve aşağıda detayları yer alan birçok örnek olaya değinilmiştir (Siber Kuvvet, 2015).

Lloyds of London adlı İngiliz sigorta platformu ile Aon adındaki risk yönetim şirketlerinin yaptıkları araştırmaya göre koordinasyon içinde yapılabilecek küresel bir siber saldırı 85 ile 193 milyar dolar arasında bir zarar ortaya çıkarabileceği sonucuna varılmıştır. Bu gibi bir saldırı en büyük etkiyi perakende ve sağlık sektörlerine yapacağı ve bu etkinin her bir sektör için 25 milyar dolar seviyesinde olabileceği öngörülmüştür. Yine bu araştırmada en büyük zararı 89 milyar dolar ile Amerika Birleşik Devletlerinin sonrasında ise 76 Milyar dolar ile Avrupa ülkelerinin ve 19 Milyar dolar ile Asya ülkelerinin göreceği değerlendirilmiştir. Zarar miktarlarının yaklaşık olarak yüzde 86 'lık bölümünün sigortasız olduğunu belirtilmiştir (Kurtaran, 2019).

İnternet kullanıcıları çeşitli kişisel verilerini internet üzerinde barındırmakta ve yaklaşık 4 milyara ulaşan bu kullanıcılar şifreleri ile bilgilerinin güvende olduğunu düşünmektedir. Cybersecurity Ventures adlı ABD merkezli şirketin yaptığı çalışmaya göre 2015 yılında gerçekleştirilen siber güvenlik suçları nedeni ile dünya genelinde 3 trilyon dolar maliyete neden olmuştur. 2021 yılında bu maliyetin 6 trilyon dolar seviyesine çıkması beklenmektedir. 2017-2010 yılları arasında tüm dünyada 1 trilyon dolar güvenlik harcaması yapılacağı araştırma raporunda öngörülmüştür. Accentura isimli Dublin merkezli yönetim danışmanlık şirketinin çalışmasına göre şirketlerin güvenlik yatırımları 2018 yılında 2017 yılına göre ortalama yüzde 23 seviyesinde artış göstermiştir (NTV, 2019).

Birçok firma son yıllarda fidye yazılımlarının tehdidi altına girmiştir. Şirketlerin kritik ve gizli bilgilerinin kullanımını engelleyerek kurbanlardan fidye talep eden yazılımlar yaygınlaşmıştır. Cybersecurity Ventures yaptığı çalışmada dünya üzerinde her 40 saniyede bir şirkete fidye yazılımların tesir ettiği ve verilerinin erişilemez hale getirildiği belirtilmiştir. Fidye yazılımlara yılda ödenen fidye miktarının 1 milyar dolar seviyesinde olduğu FBI tarafından tahmin edilmektedir. 2016 yılında ise Uber şirketinin sistemlerine sızılmış ve sürücülerin kişisel verilerine erişilmiştir. Aynı şekilde Yahoo, Tumblr, Flickr, Fantasy ve

Facebook gibi birçok sosyal medya sitesindeki kullanıcı hesap bilgileri ele geçirilmiştir (NTV, 2019).

Milliyet'in 2020 Ocak ayındaki haberinde Sberbank yöneticisi Stanizlav Kuznetsov'un sözlerini paylaşmıştır. Stanislav, gelecek dönemdeki siber saldırılardan dolayı Rus ekonomisinde kayıpların devam edeceğini söylemiştir. Geçen yılki kaybın ise 2,5 trilyon ruble seviyesinde gerçekleştiğini belirtmiştir. 2019 yılında Sberbank'ta bir siber güvenlik açığı nedeni ile bankanın müşterilerine ait 60 milyon kredi kartı bilgisi çalınmış ve satışa çıkarılmıştı (Milliyet, 2020).

Görüntülü toplantı düzenleme yazlımı olan ve tüm dünyaca bilinen Zoom adlı uygulama ile ilgili ciddi güvenlik problemleri olduğu ve 500 binden fazla Zoom kullanıcı bilgilerinin ele geçirildiği bilgisi Nisan 2020 'de yapılan haberlerle gündeme gelmiştir. Cyble adındaki siber güvenlik şirketi, ele geçirilen kullanıcı bilgilerinin "karanlık web" ve hacker sitelerinde satışa çıkarıldığını bildirmiştir. Her bir hesabın 0.0020 dolar fiyat ile satışa çıkarıldığı belirtilmiştir (Sputnik, 2020).

Blokzinciri Teknolojisi Kullanımının Değerlendirilmesi

Çalışmanın öncesinde açıklandığı üzere blokzinciri teknolojisi bir koruma sistemi olarak kullanılabilmektedir. Devletin ve kurumun bilgi sistemini belli siber saldırılara karşı koruyabileceğinden bu tarz iş ve süreçler için kurulması yerinde olacaktır. Merkezi olmayan yapısı nedeni ile özellikle dağıtık hizmet durdurma saldırılarına karşı koruma sağlayabilmektedir.

Devletin ve kurumların çok gelişmiş bilgi sistemleri olabilir. Bu sistemler ile gizli ve ayrıntı bilgiye yetkiniz ölçüsünde ulaşabilir ve kullanabilirsiniz. Bu bilgi çok değerlidir. Sahibi olan veya erişim hakkı olan bireyin bu bilgiye her ortamda erişebiliyor ve işleyebiliyor olması çok önemlidir. Kötü niyetli kişilerin, rakiplerin sizin kullanmak için ürettiğiniz bilginin en önemsiz görünenine dahi erişemiyor olması gerekmektedir. Örneğin sizin bilgi sisteminizden sizin mal ve hizmetlerinizin fiyat listesine, çalışan sayınıza, maliyet kalemlerinize, indirim opsiyonlarınız gibi bilgilere ulaşılabiliyor olmalıdır. Devletin bilgi sistemi açısından, insansız hava araçları gibi savunma sistemlerinin miktarı, anlık konum bilgileri, askeri birlik konumları, harekât planları, askeri teçhizat sayısı, üretilecek stratejik malların projesi ve üretim takvimi gibi bilgilere yetkisiz kişilerin ulaşamaması gerekir. Hatta bazı önemli bilgiler kurumda çalışan herkesin ulaşamadığı biçimde korunmalıdır. Makina ve Kimya Endüstrisi Kurumu (MKEK) silah fabrikası müdürü o fabrikanın ürettiği silahın projesini bir başka kişiye satarken yakalanmıştı (Aljazeera, 2016). Bazı önemli bilgiler devletin bekası için kritik değerdedir. Bu ve benzer bilgileri rakipleriniz ve kötü niyetli kişilerden (düşman) koruyamaz iseniz, bilgileri ele geçirip onları size karşı kullanarak üstünlük sağlayabileceklerdir. Çok iyi olduğunuz birçok konuda hâkimiyeti rakiplerinize kaptırma ihtimali ortaya çıkacaktır.

Filmlere konu olan bir bilgi edinme olayı veya siber saldırı girişimi ikinci dünya savaşı yıllarında yaşanır. Şifreleme sistemiyle Almanlar ordu güçlerinin nerelerde olduğunu ve ne yapacaklarını birbirlerine bildirmektedirler. Enigma olarak da bilinen şifreleme cihazları ile kurulmuş bu sistem çok başarılıdır. Almanlar savaş boyunca ele geçirilemeyen bu bilgilerin kullanımının avantajı ile düşmanlarına çok zarar vermektedirler. İngilizler Almanların şifreleme sistemini kırmak için bir ekip kurdular. Ekip bugünün bilgisayar teknolojisinden çok ilkel bir sistem olmasına rağmen zamanın en başarılı şifreleme sistemini kırmayı başarır. Çözümledikleri ilk bilgiye göre Almanlar, İngilizlerin küçük bir birliğini bombalayacaklardır. Bu birlikte şifre çözme ekibinde yer alan bir çalışanın kardeşi görev almaktadır. Ekipte görevli bu kişi kardeşini bu durumdan haberdar etmek ister. Ekip lideri, kişiyi durdurur. Bu saldırı küçük bir saldırı olduğu için Almanların şifrenin çözüldüğünü anlamalarını engellemek istemiştir. Aksi halde Almanların şifreleme yöntemini değiştirmesine neden olacak ve ele geçirilen büyük avantaj yitirilmiş olacaktır. Bu küçük saldırıya izin vererek büyük saldırıların önlenmesi sağlanabilecekti. Bu yöntem ile Almanların küçük saldırılarına izin verildi sadece büyük saldırılar önlenmeye çalışıldı. Bu şekilde savaş boyunca üç milyon insanın ölmesi engellenmiş oldu. Burada ekipteki o kişinin kardeşinin ölmesi üç milyon insanın ölümünü engellemiştir.

Blokzinciri Uygulamalarındaki Maliyetler

Blokzinciri uygulaması siber saldırının yapılmasını doğuran nedenlerden birisi olan merkezi yapının yerine dağıtık bir yapı sunmaktadır. Böylece siber saldırıyı önleme faaliyeti olarak kullanılabilir. Siber saldırı sonucunda büyük olumsuzluklar oluşabilir. Bu olumsuzluklar birçok maliyete neden olacaktır. Bu maliyetlere başarısızlık maliyetleri adı verilir. Başarısızlık maliyetleri parasal olarak ölçülebilen veya parasal olarak ölçülmesinde zorluk bulunan maliyetler(İtibar kaybı, iş kaybı, faaliyet sonlandırma vb.) yaratabilir.

Bu tür maliyetlere yönetim muhasebesi açısından kalite maliyetleri adı verilir. Kalite maliyetleri bir iş veya organizasyonda istenilen kaliteyi sağlamak amacıyla katlanılan faaliyetlerin yarattığı maliyetler olarak adlandırılır.

Bir bilgi işlem sisteminin kullanımında karşılaşılabilecek maliyetleri aşağıdaki gibi sınıflayabiliriz (Yükçü, 1999, s.94).

a) Önleme Maliyetleri: Sistemin arızalanması, aksaması, virüs bulaşması, siber saldırıya uğraması vb. gibi durumlar açısından her türlü koruyucu ve önleyici faaliyetin yarattığı maliyetlerdir.

b) Ölçme Değerleme Maliyeti: Bilgi İşlem sisteminin güvenilir ve kaliteli (doğru, kullanılabilir, zamanlı) bilgi üretip üretmediğini ortaya koyabilmek için yapılan kaliteyi ölçmeye yönelik faaliyetlerdir.

c) İçsel Başarısızlık Maliyeti: Bilgi İşlem sisteminin bilgi üretmesi esnasında ortaya çıkan hata, bozukluk, aksaklık nedeni ile yanlış bilgi üretmesinin yarattığı maliyetler, yanlış bilginin düzeltilmesi esnasında yaratılan maliyetler içsel başarısızlık maliyetleridir.

d) Dışsal Başarısızlık Maliyetleri: Bilgi İşlem biriminin ürettiği (yanlış) bilginin bilgi kullanıcısına aktarılmasından sonra, bilgi kullanıcısının yanlış bilgi kullanımı nedeni ile ortaya çıkan zarar, ziyan ve tazminatlardır.

Hemen her sektörde olduğu gibi bilgi işlem sisteminde de başarısızlıkları (içsel, dışsal) önlemek için önleme maliyetlerine önem vermek, katlanmak gerekecektir.

Blokzinciri Uygulamasının Maliyet-Fayda Analizi

Blokzinciri uygulamasının kalite maliyetleri açısından irdelenmesi, sistemin yararını ve varsa zararını açıkça ortaya koyabilir. 30-40 yıl önce ülkemizde ve tüm dünyada işletmelerde ve tüm diğer işlerde kalite furyası vardı. İnsanlık daha iyi yaşamak daha doğru, refah içinde yaşam sürebilmek için kalite konusuna sarılmıştı. Kalite maliyetleri de kalite konusunun açık ara en önemli konusuydu. Günümüzde kalite konusunun coşkusu azalmış olabilir. Ancak otuz yıl önce ifade ettiğim gibi bir gün gelecek insanlar her işte önce kalite maliyetlerine odaklanacaklar. Günümüzde bu konuyu önemseniyor fakat başarısızlık maliyetleri gerçekleştikten sonra bundan yakınma şeklinde bir durum söz konusudur. Bizim önerimizde başarısızlık maliyetlerini azaltmak için önleme maliyetlerine önem verilmiştir.

Blokzinciri uygulamasının bir bilgi işlem sisteminde yaratabileceği kalite maliyetleri aşağıdaki gibi olabilir.

Blokzinciri özelliği gereği bilgi işlem sisteminde çok fazla sayıda düğüm(bilgisayar, sunucu, işlem birimi) ihtiyaç gösterir. Mevcut merkezi sistemlerde bir sunucu varken bu tarz uygulamalardan birden fazla sunucu veya işlem düğümüne ihtiyaç olmaktadır. İşin durumuna göre bu düğüm sayısı 10, 100, 1000 veya daha fazla olabilir. Bu ciddi bir maliyet farkı oluşturmaktadır. Ayrıca bu düğümlerin işletilmesinde ciddi bir elektrik sarfiyatı gerçekleşecektir. Bu nedenle elektrik faturası ciddi oranda artış gösterecektir. Aşırı elektrik kullanımı, donanım sayısı ve işlem kapasitesi arttıkça aşırı ısınma ortaya çıkacaktır. Bu nedenle yalıtım ve soğutma sistemlerine ihtiyaç duyulacaktır. Bunların maliyetleri de çok yükse olabilir. Bu sistemi devamlı ayakta tutacak (çalışır şekilde) deneyimli, donanımlı eleman istihdamına ihtiyaç duyulacaktır.

Blokzinciri uygulamasının yarattığı faydayı ek bir gelir olarak ölçmek, ifade etmek mümkün değildir. Blokzinciri ile üretip, satılıp elde edilen bir gelir söz konusu değildir. Blokzinciri güvenlik zafiyetinin yarattığı zarar, ziyan, kayıp, suiistimali önleyerek kazanım sağlayacaktır. Çalışmanın önceki bölümlerinde verilen örneklerden de görüldüğü üzere kurumlar, kişiler veya devletler siber saldırılar nedeni ile trilyonlarca dolar zarara uğramaktadır ve bu teknolojinin uygulanabilir olduğu çözümlerde bu zarara uğramaktan korunabilir.

Yöneticiler blokzinciri uygulamasından yararlanırken uygulamanın yarattığı güveni çok fazla hissetmeyeceklerdir, önleme faaliyetinin nimeti olan güvenli ortamı "normal" zannederler. Hatta bazılarına bu ortam o kadar normal gelir ki; önleme amaçlı küçük bir maliyet gerekse, bu maliyet yöneticilerin gözüne batar. "Ne gerek var" diye düşünebilirler. Hatta önleme maliyetlerini reddetmek isterler. Ta ki; çok önemli bir başarısızlık maliyeti gerçekleşip önemli bir tutarı ödemek yani göğüslemek zorunda kalana kadar. Böylesinde büyük başarısızlık maliyeti (Örneğin 3,5 milyon TL) ortaya çıktığında da; alt kademedeki görevlilere veryansın ederler. Daha önce bizi neden uyarmadınız da ilgili başarısızlığı önleme faaliyeti için maliyete katlanmadık da bu devasa ceza ve/veya zararı ödüyoruz diye! Alt kademe sorumlusu üstüne "Söyledik, trilyonlarca liralık zarar ve/veya ceza yanına çok küçük bir tutar olan maliyete onay vermemiştiniz" diyemez.

Örnek: X adlı kurum toplamda 50 TL lik bilgi işlem yatırımı yapmış, stratejik olarak önemli mal veya hizmet üretmektedir. Kurumun bilgilerinin güvenle korunabilmesi için blokzinciri sistemi kurulması gerekmektedir. Blokzinciri uygulamasının yaratacağı maliyetlerin aşağıdaki Tablo 1'deki gibi olduğu öngörülmektedir. Sistemin ekonomik ömrü 10 yıl olarak belirlenmiştir.

Tablo 1. *Blokzinciri Uygulamasının Yaratacağı Maliyetler*

Maliyet (Süre)	*Miktar (TL)*
Sunucu maliyeti (10 yıllık)	5
Enerji maliyeti (Yıllık)	1
İzolasyon maliyeti (10 yıllık)	10
Soğutma maliyeti (Yıllık)	1
Yazılım kurulumu (10 yıllık)	1
Personel maaşı (Yıllık)	1

Bilgi İşlem sisteminde blokzinciri kullanılarak sağlanacak güvenlik yapısı olmadığında karşılaşılacak bir dağıtık hizmet durdurma saldırısı ve bilgilerin çalınması veya değiştirilmesi durumunda 2000 TL ceza, 1000 TL tazminat, 10000 TL'lik satış kaybı (%25 karlılık) yaşandığı öngörülmektedir. Kurumun uğrayacağı itibar ve imaj kaybının değeri öngörülememektedir.

Sistemin ömrü on yıl olarak öngörüldüğü için on yıllık veriyi karşılaştırmak gerekmektedir. Karşılaştırmayı paranın zaman değerini ihmal ederek yapıyoruz.

Kurumun yaptığı 50 TL'lik bilgi işlem yatırım maliyeti blokzinciri kullanılsa da kullanılmasa da katlanılacak bir maliyet olduğundan iki seçeneği karşılaştırırken tercihimizi etkilemeyecektir. Bu nedenle yapılacak analizde bu maliyeti dışarıda tutabiliriz.

Tablo 2. *Maliyet Karşılaştırma Tablosu*

	Blokzinciri Teknolojisi kullanılarak kurulan güvenli sistem	*Diğer Sistem*
Sunucu Maliyeti	5	
Enerji Maliyeti	10	
İzolasyon maliyeti	1	
Soğutma maliyeti	10	
Yazılım maliyeti	1	
Personel maliyeti	10	
Ceza	-	2000
Tazminat	-	1000
Satış Kaybı	-	2500
İtibar ve imaj kaybı	-	?
TOPLAM	37	5500 + ?

Tablo 2'de verilen sonuçlar karşılaştırıldığında önleme (Blokzinciri Teknoljisi kullanılarak kurulan güvenli sistem) maliyet ile başarısızlık (diğer sistem) maliyetleri arasında devasa bir fark olduğu görülmektedir. İtibar ve imaj kaybı dikkate alındığında kurum faaliyetlerini sonlandırmak (iflas) zorunda kalabilecektir.

Tartışma, Sonuç ve Öneriler

Siber güvenlik gelişen teknolojinin getirdiği riskler nedeni ile bugün olduğu gibi önümüzdeki dönemin de önemli ve popüler konularının başında gelecektir. Güvenlik ile birlikte kişisel ve kurumsal mahremiyetin korunması da önemlidir. Tüm bunlar aynı zamanda devletlerin de karşı karşıya olduğu risklerdir. Bugüne kadar yaşanan ve yaşanmaya devam eden birçok siber saldırı sistemlerin durmasına, zarar görmesine veya yok olmasına neden olmuş bu şekilde kişiler, kurumlar ve devletler de maddi, manevi zararlar görmüşlerdir. Manevi zararlar aynı zamanda maddi sonuçlar da doğurmaktadır. Öyle ki manevi zarar gören kişiler, saldırganlar tarafından sızılan sistemlerin sahiplerine tazminat davaları açmakta bu şekilde maddi yükümlülükler ortaya çıkmaktadır. Bunların yanında saldırıya uğrayan kurum ve devletler direk olarak da maddi zararlara uğramaktadırlar. Bu durum ciddi maddi kayıplara neden olduğundan kişiler, kurumlar, şirketler ve devletler siber güvenlik ve gizliliğin sağlanması için yatırımlarını arttırmalı güvenli ve sağlam sistemleri tercih etmelidirler.

Bu çalışmada incelenen ve literatürde daha önce yapılmış çalışmalarda siber saldırıların şirketlere büyük maliyetler getirdiği tespit edilmiştir. Siber saldırıları engellemede literatürde farklı çözümler sunulmuş olup bu çözümlerin her bürü uygulama alanına göre faydalar sağlayabilmektedir. Blokzinciri teknolojisinin bir siber güvenlik önleyicisi olarak kullanıldığı çözümler de önerilmiştir. Birçok çalışma sadece güvenlik bakış açısı ile bu uygulamaları incelemiş veya önermiştir. Maliyet-fayda analizi çerçevesinden değerlendirme yapmamışlardır.

Yatırım maliyetleri bakımından güvenlik harcamaları çoğu zaman önemsenmese de saldırılar ile karşı karşıya kalanların bu yatırımların kat kat fazlasını ödemek zorunda kaldıkları bir gerçektir. Tüm bu bilgiler ışığında çalışmada da teknik detayları, kullanım alanları verilmiş olan blokzinciri teknolojisinin güvenli bir

sistem için büyük avantajlar ortaya koyduğu tespit edilmiştir. Blokzinciri sistemi her alanda ve her sistem de kullanılabilen mucizevi bir sistem değildir. Belli alanlar için uygun olup kullanıldığı alanlarda değiştirilemezlik, güvenlik ve gizliliği güvence altına almayı vadeder. Bu çalışmada blokzinciri uygulanabilecek bir alanda bir şirket için bu teknolojiyi kullanmanın getireceği faydalar maliyet anlamında değerlendirilmiştir. Sonuç olarak maliyet bakımından şirketleri çeşitli maliyet kalemlerinden kurtardığı ve genel tabloda ise şirketlerin maliyetlerini düşürdüğü tespit edilmiştir.

Etik Beyan

"Siber Saldırı Önlemede Blokzinciri Teknolojisinin Fayda Maliyet Açısından Değerlendirilmesi" başlıklı çalışmanın yazım sürecinde bilimsel, etik ve alıntı kurallarına uyulmuş; toplanan veriler üzerinde herhangi bir tahrifat yapılmamış ve bu çalışma herhangi başka bir akademik yayın ortamına değerlendirme için gönderilmemiştir

Kaynakça

Aljazeera (2016). MKE Silah Fabrikası Müdürü tutuklandı. Aljazeera Turk. Erişim adresi: http://www.aljazeera.com.tr/haber/mke-silah-fabrikasi-muduru-tutuklandi. Erişim: 14.05.2020.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24-28.

Aytekin, A. (2015). Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi. *Yayımlanmamış Yüksek Lisans Tezi, Bilişim Sistemleri Anabilim Dalı, Gazi Üniversitesi*.

Azaria, A., Ekblaw, A., Vieira, T. ve Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)* (ss. 25-30). IEEE.

Barnas, N. B. (2016). Blockchains in national defense: Trustworthy systems in a trustless world. *Blue Horizons Fellowship, Air University, Maxwell Air Force Base, Alabama*.

Baygin, N., Baygin, M. ve Karakose, M. (2019, November). Blockchain Technology: Applications, Benefits and Challenges. In 2019 1st International Informatics and Software Engineering Conference (UBMYK) (ss. 1-5). IEEE.

Biswas, K. ve Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)* (ss. 1392-1393). IEEE.

Conoscenti, M., Vetro, A. ve De Martin, J. C. (2016, November). Blockchain for the Internet of Things: A systematic literature review. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)* (ss. 1-6). IEEE.

Çetin, H, Gundak, İ. ve Çetin, H. H. (2015). E-işletme güvenliği ve siber saldırılar üzerine bir araştırma. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 6(2), 223-240. Retrieved from Erişim adresi: https://dergipark.org.tr/tr/pub/jiss/issue/25891/272836.

Dağhan (2013). Küresel internet DDos saldırısıyla yavaşladı!. Dağhan Teknoloji ve İnternet. Kaynak: Erişim adresi: https://www.daghan.com/spamhaus-ddos-saldiris.dgn.

Dorri, A., Kanhere, S. S. ve Jurdak, R. (2017a, April*). Towards an optimized blockchain for IoT*. In 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI) (ss. 173-178). IEEE.

Dorri, A., Kanhere, S. S., Jurdak, R. ve Gauravaram, P. (2017b, March). *Blockchain for IoT security and privacy: The case study of a smart home*. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (ss. 618-623). IEEE.

Durğay, Z. ve Karaarslan, E. (2018). *Blokzinciri Teknolojisinin E-Devlet Uygulamalarında Kullanımı: Ön İnceleme*. Akademik Bilişim Konferansı, Karabük, Erişim adresi: https://ab.org.tr/ab18/ab18-ozet-kitapcigi-v5.pdf.

Goodman, S. E. (2008). Critical information infrastructure protection. *NATO Security Through Science Series E Human And Societal Dynamics*, *34*, 24.

Goodrich, M. ve Tamassia, R. (2011), *Introduction to Computer Security*. USA:Pearson Education, Inc..

Gür, A. Ö., Öksüzer, Ş. ve Karaarslan, E. (2019, April). *Blockchain based metering and billing system proposal with privacy protection for the electric network*. In 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG) (ss. 204-208). IEEE.

Halpin, H. ve Piekarska, M. (2017, April). *Introduction to Security and Privacy on the Blockchain*. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (ss. 1-3). IEEE.

Hansen, L. ve Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Huh, S., Cho, S. ve Kim, S. (2017, February). *Managing IoT devices using blockchain platform*. In 2017 19th international conference on advanced communication technology *(ICACT)* (ss. 464-467). IEEE.

Irmak, E. ve Erkek, İ. (2016). Çok Nitelikli Fayda Teorisiyle Saldırgan Profiline Yeni Parametrelerin Eklenmesi. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2(2), 1-9.

Karaarslan, E. ve Akbaş, M. (2017). Blokzinciri Tabanlı Siber Güvenlik Sistemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 3(2) , 16-21. DOI: 10.18640/ubgmd.373297

Konacakli, E. ve Karaarslan, E. (2019, April). *Blockchain-Based Secure Recognized Air Picture System Proposal for NATO Air C2 Capabilities*. In The International Conference on Artificial Intelligence and Applied Mathematics in Engineering (ss. 758-765). Springer, Cham.

Kurtaran, G. (2019). Küresel boyutta siber saldırının maliyeti 193 milyar doları bulabilir. Anadolu Ajansı. Erişim adresi: https://www.aa.com.tr/tr/dunya/kuresel-boyutta-siber-saldirinin-maliyeti-193-milyar-dolari-bulabilir-/1378011, Erişim: 12.03.2020.

Merkle, R. C. (1982). U.S. Patent No. 4,309,569. Washington, DC: U.S. Patent and Trademark Office.

Milliyet (2020). Siber saldırıların Rus ekonomisine maliyeti 2,5 trilyon ruble. Anadolu Ajansı. Erişim adresi: https://www.milliyet.com.tr/ekonomi/siber-saldirilarin-rus-ekonomisine-maliyeti-2-5-trilyon-ruble-6127353. Erişim: 12.03.2020.

Naraine, R. (2011). Citigroup: Customer losses from hack attack reaches $2.7M. ZDNET. Erişim adresi: https://www.zdnet.com/article/citigroup-customer-losses-from-hack-attack-reaches-2-7m/ . Erişim:30.04.2020.

NTV (2019). Dünya 6 trilyon dolarlık siber saldırı riskine karşı hazırlanıyor. Anadolu Ajansı. Erişim adresi: https://www.ntv.com.tr/teknoloji/dunya-6-trilyon-dolarlik-siber-saldiri-riskine-karsi-hazirlaniyor,9eKrA5ZjBEWn_HI7tvrxuw, Erişim: 12.03.2020.

Ølnes, S., Ubacht, J. ve Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly* 34(3), 355-364.

Öncel, Ü. (2014). Siber saldırılarda hackerların yeni silahı buzdolapları olabilir mi?. Webrazzi. Erişim adresi: https://webrazzi.com//2014/01/17/siber-saldiri-buzdolabi/.

Phillips, T. (2016). Five years ago today, Sony admitted the great PSN hack. Eurogamer. Erişim adresi: https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today

SecureChain: A Blockchain Security Gateway for SDN. Erişim adresi: http://www.reply.com/en/content/securechain Erişim:19.05.2020.

Siber Kuvvet, (2015). Siber Saldırılar ve Siber Terör. Erişim adresi: https://siberkuvvet.com/kutuphane/oku/siber-saldirilar-ve-siber-teror.

Singh, S. ve Singh, N. (2016, December). *Blockchain: Future of financial and cyber security*. In 2016 2nd international conference on contemporary computing and informatics (IC3I) (ss. 463-467). IEEE.

Sputnik (2020). Yüz binlerce Zoom kullanıcısının bilgileri 'dark web'de satışa çıktı. Sputnik Türkiye. Erişim adresi: https://tr.sputniknews.com/bilim/202004141041826149-yuz-binlerce-zoom-kullanicisinin-bilgileri-dark-webde-satisa-cikti/

Stallings W. (2017). A blockchain tutorial. *Internet Protocol Journal*, 20(3), 2-24.

Şenol, M. (2016). Siber güçle caydırıcılık ama nasıl. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2(2), 10-17.

Şenol, M. (2017). Türkiye'de siber saldırılara karşı caydırıcılık. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 3(2), 1-9.

Şentürk, H., Çil, C. Z. ve Sağıroğlu, Ş. (2016). Siber güvenlik yatırım kararları üzerine literatür incelemesi. *Politeknik Dergisi*, 19(1), 39-51.

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A. ve Kishigami, J. (2016, January). *Blockchain contract: Securing a blockchain applied to smart contracts*. In 2016 IEEE international conference on consumer electronics (ICCE) (ss. 467-468). IEEE.

Yener, Y.(2015) 8. yılında Estonya Saldırılarına çok boyutlu bir bakış. Siber Bülten. Erişim adresi: https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/

Yükçü, S. (1999). *Kalite maliyetlerinin muhasebeleştirilmesi*; İzmir: Anadolu Matbaacılık.

Zhao, W. (2017). Dubai Plans Digital Passports Using Blockchain Tech. Erişim adresi: https://www.coindesk.com/dubai-plans-gate-less-airport-security-using-blockchain-tech/

EXTENDED ABSTRACT

The spread of the Internet in all areas of our lives has brought many eases and benefits for human life. Along with the development of technology, two basic issues such as security and privacy increase the importance day by day as the subjects that both individuals, institutions and governments should deal with. On the other hand, the Internet has brought along problems and threats by its nature. Risks such as the seizing and sharing of personal data without permission, and leakage of critical information for government, companies and institutions have emerged. The measures taken against individuals, institutions, companies or governments in accordance with the rules determined in the current order, and the measures taken against all kinds of threats, harassment, epidemic and disaster are called "Security". Privacy is the restriction of access to information. It means that people other than a certain person or a group cannot access this information. These two basic concepts are of great importance today. It is also very important to ensure the security and privacy of this information in today's world where the information of the organization at all levels is transmitted wired or wireless via the Internet. Otherwise, individuals, institutions and governments suffer material and moral damages. The concept of cyber security meets the reflection of security in the technology environment, which we call cyber or virtual world. People, institutions or governments want to be safe in

every field. In today's world, information has gained great importance in making sense of this information and ensuring its security. Accordingly, cyber armies are set up and attacks are organized in order to damage individuals, companies, institutions and governments or to seize their information. One of the most common of these attacks is denial of service attacks from distrubuted sources. Although blockchain technology is not applicable in all areas and situations, it is suitable for certain applications. It offers serious advantages with its distributed structure. Blockchain technology can be used as a solution to reduce the costs of institutions, companies and governments against cyber-attacks. In this study, technical information about blockchain technology and cyber-attacks, the damages caused by cyber-attacks were shared and cost benefit analysis of blockchain, which can be used to prevent some of these attacks in certain cases, was made. This is the first of the motivation points of this study. The second issue is the material and moral consequences of security and privacy violations. This study will focus more on material losses. Especially the financial losses of companies and governments will be evaluated. It is obvious that blockchain technology provides significant gains in terms of security and privacy in the areas where it can be used due to its distributed structure. The final motivation point of the study is the financial gains that this distributed structure will provide for institutions and governments. After the first section, which contains general information about cyber security and blockchain, in the second section, cyber-attacks made in the past are mentioned and the damages arising are given. Afterwards, examples of applications where blockchain technology can be used are given and the gains offered in terms of security are evaluated. Finally, financial analysis of these gains was made. The aim of this study is to analyse the blockchain technology that can provide significant gains in various financial application areas, to emphasize the importance of cyber security for companies and countries. As we know, we can classify the costs that may be encountered in using an information system as follows. Prevention Costs: System malfunction, disruption, virus infection, cyber-attack etc. in terms of situations such as all kinds of protective and preventive activities. Measurement Valuation Cost: These are the activities aimed at measuring the quality to determine whether the IT system produces reliable and quality (accurate, usable, timely) information. Internal Failure Cost: Costs caused by producing incorrect information due to errors, defects, and malfunctions that arise during the information production system, and the costs created during the correction of false information are internal failure costs. External Failure Costs: Damages, damages and compensations that arise due to the use of the wrong information by the information user after the (wrong) information produced by the data processing unit is transferred to the information user. As in almost every sector, it will be necessary to pay attention to the costs of prevention and endure in order to prevent failures (internal, external) in the information system. Due to the risks posed by cyber security developing technology, it will be one of the most important and popular topics of the coming period as it is today. Along with security, it is also important to protect personal and corporate privacy. All of these are also the risks faced by states. Many cyber-attacks, which have been and continue to be experienced, have caused systems to stop, damage or disappear, and thus individuals, institutions and states have also suffered material and moral damages. Spiritual damages also have material consequences. So much so that people who are morally damaged bring compensation cases to the owners of the systems infiltrated by the attackers, and material obligations arise in this way. In addition, the attacked institutions and states are also exposed to financial losses directly. Since this situation causes serious financial losses, individuals, institutions, companies and governments should increase their investments in order to ensure cyber security and privacy and prefer safe and robust systems. Although security expenditures are not considered important in terms of investment costs, it is a fact that those who are attacked have to pay many times more of these investments. In the light of all this information, it has been determined that the blockchain technology, whose technical details and usage areas are given, offers great advantages for a safe system. Blockchain system is not a miraculous system that can be used in every field and in every system. It is suitable for certain areas and promises to guarantee immunity, security and privacy in the areas where it is used. In this study, the benefits of using this technology for a company in a field where blockchain can be applied were evaluated in terms of cost. As a result, it has been determined that it saves companies from various cost items in terms of cost and reduces the costs of companies in the general table.